

# [MS-RRASM]: Routing and Remote Access Server (RRAS) Management Protocol Specification

---

## Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft [Open Specification Promise](#) or the [Community Promise](#). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights.** All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

**Tools.** The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

## Revision Summary

Date	Revision History	Revision Class	Comments
06/20/2008	0.01		Initial Availability
07/25/2008	0.01.1	Editorial	Revised and edited the technical content.
08/29/2008	0.2	Minor	Updated the technical content.
10/24/2008	0.2.1	Editorial	Revised and edited the technical content.
12/05/2008	1.0	Major	Updated and revised the technical content.
01/16/2009	2.0	Major	Updated and revised the technical content.
02/27/2009	3.0	Major	Updated and revised the technical content.
04/10/2009	3.0.1	Editorial	Revised and edited the technical content.
05/22/2009	4.0	Major	Updated and revised the technical content.
07/02/2009	5.0	Major	Updated and revised the technical content.
08/14/2009	6.0	Major	Updated and revised the technical content.
09/25/2009	7.0	Major	Updated and revised the technical content.
11/06/2009	7.0.1	Editorial	Revised and edited the technical content.
12/18/2009	7.0.2	Editorial	Revised and edited the technical content.
01/29/2010	8.0	Major	Updated and revised the technical content.
03/12/2010	9.0	Major	Updated and revised the technical content.
04/23/2010	10.0	Major	Updated and revised the technical content.
06/04/2010	11.0	Major	Updated and revised the technical content.
07/16/2010	12.0	Major	Significantly changed the technical content.
08/27/2010	13.0	Major	Significantly changed the technical content.
10/08/2010	13.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	13.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	14.0	Major	Significantly changed the technical content.
02/11/2011	14.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/25/2011	14.1	Minor	Clarified the meaning of the technical content.

<b>Date</b>	<b>Revision History</b>	<b>Revision Class</b>	<b>Comments</b>
05/06/2011	14.1	No change	No changes to the meaning, language, or formatting of the technical content.
06/17/2011	14.2	Minor	Clarified the meaning of the technical content.

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>17</b>
1.1	Glossary .....	17
1.2	References.....	23
1.2.1	Normative References.....	23
1.2.2	Informative References .....	26
1.3	Overview .....	27
1.3.1	Interface Object.....	29
1.3.2	Transport Object .....	30
1.3.3	Management Information Base (MIB).....	30
1.3.4	Ports Object .....	31
1.3.5	Connection Object .....	32
1.4	Relationship to Other Protocols.....	32
1.5	Prerequisites/Preconditions .....	32
1.6	Applicability Statement.....	32
1.7	Versioning and Capability Negotiation.....	33
1.8	Vendor-Extensible Fields.....	33
1.9	Standards Assignments .....	33
<b>2</b>	<b>Messages.....</b>	<b>34</b>
2.1	Transport.....	34
2.1.1	Dimsvc Security Settings.....	34
2.1.1.1	Server Security Settings .....	34
2.1.1.2	Client Security Settings .....	34
2.1.2	Rasrpc Security Settings .....	34
2.1.2.1	Server Security Settings .....	34
2.1.2.2	Client Security Settings .....	35
2.2	Common Data Types .....	35
2.2.1	RRASM RPC Common Messages .....	35
2.2.1.1	Data Types, Enumerations, and Constants .....	35
2.2.1.1.1	ROUTER_INTERFACE_TYPE.....	35
2.2.1.1.2	ROUTER_CONNECTION_STATE .....	36
2.2.1.1.3	RAS_QUARANTINE_STATE.....	36
2.2.1.1.4	RAS_PORT_CONDITION .....	37
2.2.1.1.5	RAS_HARDWARE_CONDITION .....	37
2.2.1.1.6	DIM_HANDLE.....	38
2.2.1.1.7	FORWARD_ACTION .....	38
2.2.1.1.8	MIB_IPFORWARD_TYPE .....	38
2.2.1.1.9	MIB_IPFORWARD_PROTO.....	38
2.2.1.1.10	MIB_IPSTATS_FORWARDING .....	40
2.2.1.1.11	MIB_TCP_STATE .....	40
2.2.1.1.12	TCP_RTO_ALGORITHM .....	41
2.2.1.1.13	IP_NAT_DIRECTION.....	41
2.2.1.1.14	OSPF_PARAM_TYPE .....	42
2.2.1.1.15	OSPF_FILTER_ACTION .....	42
2.2.1.1.16	RASDEVICETYPE .....	43
2.2.1.1.17	RASMAN_STATUS.....	44
2.2.1.1.18	ReqTypes .....	44
2.2.1.1.19	RASMAN_STATE .....	45
2.2.1.1.20	RASMAN_DISCONNECT_TYPE .....	45
2.2.1.1.21	RASMAN_USAGE .....	46



2.2.1.2	Structures .....	46
2.2.1.2.1	DIM_INFORMATION_CONTAINER .....	46
2.2.1.2.2	DIM_INTERFACE_CONTAINER.....	48
2.2.1.2.3	RTR_INFO_BLOCK_HEADER.....	49
2.2.1.2.4	RTR_TOC_ENTRY .....	49
2.2.1.2.5	FILTER_DESCRIPTOR.....	54
2.2.1.2.6	FILTER_INFO .....	55
2.2.1.2.7	FILTER_DESCRIPTOR_V6 .....	57
2.2.1.2.8	FILTER_INFO_V6.....	57
2.2.1.2.9	GLOBAL_INFO .....	59
2.2.1.2.10	IN6_ADDR.....	59
2.2.1.2.11	INTERFACE_ROUTE_INFO.....	60
2.2.1.2.12	PRIORITY_INFO .....	62
2.2.1.2.13	PROTOCOL_METRIC.....	63
2.2.1.2.14	RTR_DISC_INFO .....	63
2.2.1.2.15	MCAST_HBEAT_INFO .....	64
2.2.1.2.16	MIB_MCAST_LIMIT_ROW .....	65
2.2.1.2.17	IPINIP_CONFIG_INFO .....	65
2.2.1.2.18	INTERFACE_STATUS_INFO .....	66
2.2.1.2.19	DIM_MIB_ENTRY_CONTAINER .....	66
2.2.1.2.20	MIB_IPDESTROW .....	68
2.2.1.2.21	MIB_IPDESTTABLE .....	68
2.2.1.2.22	MIB_ROUTESTATE .....	69
2.2.1.2.23	MIB_BEST_IF.....	69
2.2.1.2.24	MIB_BOUNDARYROW .....	69
2.2.1.2.25	MIB_ICMP .....	70
2.2.1.2.26	MIBICMPINFO .....	70
2.2.1.2.27	MIBICMPSTATS .....	71
2.2.1.2.28	MIB_IFNUMBER.....	72
2.2.1.2.29	MIB_IFROW .....	72
2.2.1.2.30	MIB_IFSTATUS.....	74
2.2.1.2.31	MIB_IFTABLE .....	75
2.2.1.2.32	MIB_IPADDRROW.....	76
2.2.1.2.33	MIB_IPADDRTABLE.....	77
2.2.1.2.34	MIB_IPFORWARDNUMBER .....	77
2.2.1.2.35	MIB_IPFORWARDROW .....	77
2.2.1.2.36	MIB_IPFORWARDTABLE .....	79
2.2.1.2.37	MIB_IPMCAST_BOUNDARY .....	79
2.2.1.2.38	MIB_IPMCAST_BOUNDARY_TABLE.....	80
2.2.1.2.39	MIB_IPMCAST_GLOBAL .....	81
2.2.1.2.40	MIB_IPMCAST_IF_ENTRY .....	81
2.2.1.2.41	MIB_IPMCAST_IF_TABLE.....	81
2.2.1.2.42	MIB_IPMCAST_MFE .....	82
2.2.1.2.43	MIB_IPMCAST_OIF .....	83
2.2.1.2.44	MIB_IPMCAST_MFE_STATS.....	83
2.2.1.2.45	MIB_IPMCAST_OIF_STATS .....	85
2.2.1.2.46	MIB_IPMCAST_SCOPE.....	86
2.2.1.2.47	MIB_IPNETROW .....	87
2.2.1.2.48	MIB_IPNETTABLE .....	87
2.2.1.2.49	MIB_IPSTATS.....	88
2.2.1.2.50	MIB_MCAST_LIMIT_ROW .....	90
2.2.1.2.51	MIB_MFE_STATS_TABLE .....	90
2.2.1.2.52	MIB_MFE_TABLE .....	91

2.2.1.2.53	MIB_OPAQUE_INFO .....	91
2.2.1.2.54	MIB_OPAQUE_QUERY .....	95
2.2.1.2.55	MIB_PROXYARP .....	102
2.2.1.2.56	MIB_TCPROW .....	102
2.2.1.2.57	MIB_TCPSTATS .....	103
2.2.1.2.58	MIB_TCPTABLE .....	104
2.2.1.2.59	MIB_UDPROW .....	104
2.2.1.2.60	MIB_UDPSTATS .....	104
2.2.1.2.61	MIB_UDPTABLE .....	105
2.2.1.2.62	MPR_SERVER_0 .....	105
2.2.1.2.63	MPR_SERVER_1 .....	106
2.2.1.2.64	MPR_SERVER_2 .....	107
2.2.1.2.65	PPP_NBFCP_INFO .....	108
2.2.1.2.66	PPP_IPCP_INFO .....	108
2.2.1.2.67	PPP_IPCP_INFO2 .....	109
2.2.1.2.68	PPP_IPXCP_INFO .....	109
2.2.1.2.69	PPP_IPV6_CP_INFO .....	110
2.2.1.2.70	PPP_ATCP_INFO .....	110
2.2.1.2.71	PPP_CCP_INFO .....	111
2.2.1.2.72	PPP_LCP_INFO .....	112
2.2.1.2.73	PPP_INFO .....	115
2.2.1.2.74	PPP_INFO_2 .....	115
2.2.1.2.75	PPP_INFO_3 .....	116
2.2.1.2.76	RASI_PORT_0 .....	116
2.2.1.2.77	RASI_PORT_1 .....	118
2.2.1.2.78	RASI_CONNECTION_0 .....	119
2.2.1.2.79	RASI_CONNECTION_1 .....	120
2.2.1.2.80	RASI_CONNECTION_2 .....	121
2.2.1.2.81	RASI_CONNECTION_3 .....	122
2.2.1.2.82	MPRI_INTERFACE_0 .....	122
2.2.1.2.83	MPRI_INTERFACE_1 .....	124
2.2.1.2.84	MPRI_INTERFACE_2 .....	125
2.2.1.2.85	MPRI_INTERFACE_3 .....	133
2.2.1.2.86	MPR_DEVICE_0 .....	141
2.2.1.2.87	MPR_DEVICE_1 .....	141
2.2.1.2.88	MPR_CREDENTIALSEX_1 .....	142
2.2.1.2.89	IFFILTER_INFO .....	142
2.2.1.2.90	MPR_FILTER_0 .....	143
2.2.1.2.91	IPX_GLOBAL_INFO .....	143
2.2.1.2.92	IPX_IF_INFO .....	144
2.2.1.2.93	IPXWAN_IF_INFO .....	144
2.2.1.2.94	IPX_STATIC_ROUTE_INFO .....	144
2.2.1.2.95	IPX_STATIC_SERVICE_INFO .....	145
2.2.1.2.96	IPX_STATIC_NETBIOS_NAME_INFO .....	146
2.2.1.2.97	IPX_ADAPTER_INFO .....	146
2.2.1.2.98	IPX_TRAFFIC_FILTER_GLOBAL_INFO .....	147
2.2.1.2.99	IPX_TRAFFIC_FILTER_INFO .....	147
2.2.1.2.100	IF_TABLE_INDEX .....	149
2.2.1.2.101	ROUTING_TABLE_INDEX .....	149
2.2.1.2.102	STATIC_ROUTES_TABLE_INDEX .....	150
2.2.1.2.103	SERVICES_TABLE_INDEX .....	150
2.2.1.2.104	STATIC_SERVICES_TABLE_INDEX .....	151
2.2.1.2.105	IPX_MIB_INDEX .....	151

2.2.1.2.106	IPX_MIB_GET_INPUT_DATA.....	152
2.2.1.2.107	IPXMIB_BASE.....	152
2.2.1.2.108	IPX_IF_STATS.....	153
2.2.1.2.109	IPX_INTERFACE.....	154
2.2.1.2.110	IPX_ROUTE.....	157
2.2.1.2.111	IPX_MIB_ROW.....	158
2.2.1.2.112	IPX_MIB_SET_INPUT_DATA.....	158
2.2.1.2.113	SAP_SERVICE_FILTER_INFO.....	159
2.2.1.2.114	SAP_IF_FILTERS.....	160
2.2.1.2.115	SAP_IF_CONFIG.....	160
2.2.1.2.116	SAP_MIB_BASE.....	161
2.2.1.2.117	SAP_IF_STATS.....	161
2.2.1.2.118	SAP_INTERFACE.....	162
2.2.1.2.119	SAP_MIB_GET_INPUT_DATA.....	162
2.2.1.2.120	SAP_MIB_SET_INPUT_DATA.....	163
2.2.1.2.121	IPX_SERVICE.....	163
2.2.1.2.122	SAP_IF_INFO.....	163
2.2.1.2.123	RIPMIB_BASE.....	164
2.2.1.2.124	RIP_IF_STATS.....	165
2.2.1.2.125	RIP_INTERFACE.....	165
2.2.1.2.126	RIP_MIB_GET_INPUT_DATA.....	166
2.2.1.2.127	RIP_MIB_SET_INPUT_DATA.....	166
2.2.1.2.128	EAPTLS_HASH.....	166
2.2.1.2.129	EAPTLS_USER_PROPERTIES.....	167
2.2.1.2.130	MPRAPI_OBJECT_HEADER_IDL.....	168
2.2.1.2.131	PPP_PROJECTION_INFO_1.....	169
2.2.1.2.132	IKEV2_PROJECTION_INFO_1.....	173
2.2.1.2.133	PROJECTION_INFO_IDL_1.....	174
2.2.1.2.134	RAS_CONNECTION_EX_1_IDL.....	175
2.2.1.2.135	RAS_CONNECTION_EX_IDL.....	177
2.2.1.2.136	CERT_BLOB_1.....	178
2.2.1.2.137	IKEV2_TUNNEL_CONFIG_PARAMS_1.....	178
2.2.1.2.138	IKEV2_CONFIG_PARAMS_1.....	179
2.2.1.2.139	PPTP_CONFIG_PARAMS_1.....	179
2.2.1.2.140	L2TP_CONFIG_PARAMS_1.....	180
2.2.1.2.141	SSTP_CERT_INFO_1.....	180
2.2.1.2.142	SSTP_CONFIG_PARAMS_1.....	181
2.2.1.2.143	MPR_SERVER_EX_1.....	182
2.2.1.2.144	MPR_SERVER_EX_IDL.....	182
2.2.1.2.145	MPRAPI_TUNNEL_CONFIG_PARAMS_1.....	182
2.2.1.2.146	MPR_SERVER_SET_CONFIG_EX_1.....	183
2.2.1.2.147	MPR_SERVER_SET_CONFIG_EX_IDL.....	183
2.2.1.2.148	RAS_UPDATE_CONNECTION_1_IDL.....	184
2.2.1.2.149	RAS_UPDATE_CONNECTION_IDL.....	184
2.2.1.2.150	IPBOOTP_GLOBAL_CONFIG.....	184
2.2.1.2.151	IPBOOTP_IF_CONFIG.....	185
2.2.1.2.152	IPBOOTP_MIB_GET_INPUT_DATA.....	186
2.2.1.2.153	IPBOOTP_MIB_GET_OUTPUT_DATA.....	187
2.2.1.2.154	IPBOOTP_IF_STATS.....	187
2.2.1.2.155	IPBOOTP_IF_BINDING.....	188
2.2.1.2.156	IPBOOTP_IP_ADDRESS.....	189
2.2.1.2.157	DHCPV6R_MIB_GET_OUTPUT_DATA.....	189
2.2.1.2.158	DHCPV6R_GLOBAL_CONFIG.....	189

2.2.1.2.159	DHCPV6R_IF_STATS .....	190
2.2.1.2.160	DHCPV6R_IF_CONFIG .....	191
2.2.1.2.161	DHCPV6R_MIB_GET_INPUT_DATA .....	192
2.2.1.2.162	IPRIP_MIB_GET_INPUT_DATA .....	192
2.2.1.2.163	IPRIP_MIB_GET_OUTPUT_DATA .....	193
2.2.1.2.164	IPRIP_GLOBAL_STATS .....	194
2.2.1.2.165	IPRIP_GLOBAL_CONFIG .....	194
2.2.1.2.166	IPRIP_IF_STATS .....	195
2.2.1.2.167	IPRIP_IF_CONFIG .....	196
2.2.1.2.168	IPRIP_ROUTE_FILTER .....	201
2.2.1.2.169	IPRIP_IF_BINDING .....	202
2.2.1.2.170	IPRIP_IP_ADDRESS .....	202
2.2.1.2.171	IPRIP_PEER_STATS .....	203
2.2.1.2.172	IGMP_MIB_GET_INPUT_DATA .....	203
2.2.1.2.173	IGMP_MIB_GET_OUTPUT_DATA .....	204
2.2.1.2.174	IGMP_MIB_GLOBAL_CONFIG .....	206
2.2.1.2.175	IGMP_MIB_IF_CONFIG .....	206
2.2.1.2.176	IGMP_MIB_IF_GROUPS_LIST .....	209
2.2.1.2.177	IGMP_MIB_GROUP_INFO .....	210
2.2.1.2.178	IGMP_MIB_IF_STATS .....	211
2.2.1.2.179	IGMP_MIB_GROUP_IFS_LIST .....	214
2.2.1.2.180	IGMP_MIB_GROUP_INFO_V3 .....	214
2.2.1.2.181	INTERFACE_ROUTE_ENTRY .....	215
2.2.1.2.182	IP_NAT_MIB_QUERY .....	216
2.2.1.2.183	IP_NAT_ENUMERATE_SESSION_MAPPINGS .....	217
2.2.1.2.184	IP_NAT_SESSION_MAPPING .....	217
2.2.1.2.185	IP_NAT_INTERFACE_STATISTICS .....	219
2.2.1.2.186	IP_DNS_PROXY_MIB_QUERY .....	219
2.2.1.2.187	IP_DNS_PROXY_STATISTICS .....	220
2.2.1.2.188	IP_AUTO_DHCP_MIB_QUERY .....	220
2.2.1.2.189	IP_AUTO_DHCP_STATISTICS .....	221
2.2.1.2.190	MIB_DA_MSG .....	221
2.2.1.2.191	IP_AUTO_DHCP_GLOBAL_INFO .....	225
2.2.1.2.192	IP_AUTO_DHCP_INTERFACE_INFO .....	226
2.2.1.2.193	IP_DNS_PROXY_GLOBAL_INFO .....	227
2.2.1.2.194	IP_DNS_PROXY_INTERFACE_INFO .....	228
2.2.1.2.195	IP_NAT_GLOBAL_INFO .....	228
2.2.1.2.196	IP_NAT_TIMEOUT .....	229
2.2.1.2.197	IP_NAT_INTERFACE_INFO .....	229
2.2.1.2.198	IP_NAT_ADDRESS_RANGE .....	231
2.2.1.2.199	IP_NAT_PORT_MAPPING .....	232
2.2.1.2.200	IP_NAT_ADDRESS_MAPPING .....	232
2.2.1.2.201	IP_ALG_GLOBAL_INFO .....	232
2.2.1.2.202	RIP_GLOBAL_INFO .....	233
2.2.1.2.203	RIP_ROUTE_FILTER_INFO .....	234
2.2.1.2.204	RIP_IF_FILTERS .....	234
2.2.1.2.205	RIP_IF_INFO .....	235
2.2.1.2.206	RIP_IF_CONFIG .....	236
2.2.1.2.207	SAP_GLOBAL_CONFIG .....	236
2.2.1.2.208	OSPF_ROUTE_FILTER .....	237
2.2.1.2.209	OSPF_ROUTE_FILTER_INFO .....	237
2.2.1.2.210	OSPF_PROTO_FILTER_INFO .....	238
2.2.1.2.211	OSPF_GLOBAL_PARAM .....	238

2.2.1.2.212	OSPF_AREA_PARAM .....	239
2.2.1.2.213	OSPF_AREA_RANGE_PARAM .....	239
2.2.1.2.214	OSPF_VIRT_INTERFACE_PARAM .....	240
2.2.1.2.215	OSPF_INTERFACE_PARAM .....	241
2.2.1.2.216	OSPF_NBMA_NEIGHBOR_PARAM .....	242
2.2.1.2.217	RequestBuffer .....	242
2.2.1.2.218	DeviceConfigInfo .....	244
2.2.1.2.219	RAS_DEVICE_INFO .....	244
2.2.1.2.220	GetSetCalledId .....	245
2.2.1.2.221	RAS_CALLEDID_INFO.....	247
2.2.1.2.222	GetNdiswanDriverCapsStruct .....	247
2.2.1.2.223	RAS_NDISWAN_DRIVER_INFO .....	247
2.2.1.2.224	GetDevConfigStruct .....	248
2.2.1.2.225	Enum .....	248
2.2.1.2.226	RASMAN_PORT_32 .....	249
2.2.1.2.227	Info .....	250
2.2.1.2.228	RASMAN_INFO .....	250
2.2.1.2.229	RASRPC_PBUSER.....	252
2.2.1.2.230	RASRPC_CALLBACKLIST .....	254
2.2.1.2.231	RASRPC_STRINGLIST.....	256
2.2.1.2.232	RASRPC_LOCATIONLIST .....	256
2.2.2	File Format for Phonebook.....	256
2.2.2.1	RRAS entry section name .....	257
2.2.2.2	Phonebook entry settings .....	257
2.2.2.2.1	Encoding .....	258
2.2.2.2.2	PBVersion.....	258
2.2.2.2.3	Type.....	258
2.2.2.2.4	Autologon .....	258
2.2.2.2.5	UseRasCredentials.....	258
2.2.2.2.6	LowDateTime.....	258
2.2.2.2.7	HighDateTime.....	258
2.2.2.2.8	DialParamsUID .....	258
2.2.2.2.9	Guid .....	258
2.2.2.2.10	BaseProtocol .....	259
2.2.2.2.11	VpnStrategy .....	259
2.2.2.2.12	ExcludedProtocols.....	259
2.2.2.2.13	LcpExtensions .....	259
2.2.2.2.14	DataEncryption .....	260
2.2.2.2.15	SwCompression.....	260
2.2.2.2.16	NegotiateMultilinkAlways .....	260
2.2.2.2.17	SkipNwcWarning .....	260
2.2.2.2.18	SkipDownLevelDialog.....	260
2.2.2.2.19	SkipDoubleDialDialog .....	260
2.2.2.2.20	DialMode .....	261
2.2.2.2.21	DialPercent .....	261
2.2.2.2.22	DialSeconds.....	261
2.2.2.2.23	HangupPercent.....	261
2.2.2.2.24	HangupSeconds .....	261
2.2.2.2.25	OverridePref .....	261
2.2.2.2.26	RedialAttempts.....	261
2.2.2.2.27	RedialSeconds.....	262
2.2.2.2.28	IdleDisconnectSeconds.....	262
2.2.2.2.29	RedialOnLinkFailure .....	262

2.2.2.2.30	CallbackMode.....	262
2.2.2.2.31	CustomDialDll .....	262
2.2.2.2.32	CustomDialFunc .....	262
2.2.2.2.33	CustomRasDialDll .....	262
2.2.2.2.34	ForceSecureCompartment .....	262
2.2.2.2.35	DisableIKENNameEkuCheck .....	263
2.2.2.2.36	AuthenticateServer .....	263
2.2.2.2.37	ShareMsFilePrint.....	263
2.2.2.2.38	BindMsNetClient .....	263
2.2.2.2.39	SharedPhoneNumbers .....	263
2.2.2.2.40	GlobalDeviceSettings .....	264
2.2.2.2.41	PrerequisitePbk .....	264
2.2.2.2.42	PrerequisiteEntry .....	264
2.2.2.2.43	PreferredPort .....	264
2.2.2.2.44	PreferredDevice.....	264
2.2.2.2.45	PreferredBps .....	264
2.2.2.2.46	PreferredHwFlow .....	264
2.2.2.2.47	PreferredProtocol.....	265
2.2.2.2.48	PreferredCompression .....	265
2.2.2.2.49	PreferredSpeaker .....	265
2.2.2.2.50	PreferredMdmProtocol .....	265
2.2.2.2.51	PreviewUsePw .....	265
2.2.2.2.52	PreviewDomain .....	265
2.2.2.2.53	PreviewPhoneNumber .....	265
2.2.2.2.54	ShowDialingProgress.....	266
2.2.2.2.55	ShowMonitorIconInTaskbar.....	266
2.2.2.2.56	CustomAuthKey .....	266
2.2.2.2.57	CustomAuthData .....	266
2.2.2.2.58	AuthRestrictions .....	266
2.2.2.2.59	TypicalAuth .....	267
2.2.2.2.60	IpPrioritizeRemote .....	267
2.2.2.2.61	IpInterfaceMetric.....	267
2.2.2.2.62	fCachedDnsSuffix .....	267
2.2.2.2.63	IpHeaderCompression .....	267
2.2.2.2.64	IpAddress.....	267
2.2.2.2.65	IpDnsAddress .....	267
2.2.2.2.66	IpDns2Address.....	268
2.2.2.2.67	IpWinsAddress .....	268
2.2.2.2.68	IpWins2Address .....	268
2.2.2.2.69	IpAssign .....	269
2.2.2.2.70	IpNameAssign .....	269
2.2.2.2.71	IpFrameSize .....	269
2.2.2.2.72	IpDnsFlags .....	269
2.2.2.2.73	IpNBTFflags .....	270
2.2.2.2.74	TcpWindowSize .....	270
2.2.2.2.75	UseFlags .....	270
2.2.2.2.76	IpSecFlags.....	270
2.2.2.2.77	IpDnsSuffix .....	270
2.2.2.2.78	IpCachedDnsSuffix .....	270
2.2.2.2.79	Ipv6Assign .....	270
2.2.2.2.80	Ipv6PrefixLength .....	271
2.2.2.2.81	Ipv6PrioritizeRemote .....	271
2.2.2.2.82	Ipv6InterfaceMetric .....	271

2.2.2.2.83	Ipv6NameAssign .....	271
2.2.2.2.84	Ipv6DnsAddress .....	271
2.2.2.2.85	Ipv6Dns2Address .....	271
2.2.2.2.86	Ipv6Prefix .....	272
2.2.2.2.87	Ipv6InterfaceId .....	272
2.2.2.2.88	DisableClassBasedDefaultRoute .....	272
2.2.2.2.89	DisableMobility .....	272
2.2.2.2.90	NetworkOutageTime .....	272
2.2.2.2.91	ProvisionType .....	272
2.2.2.2.92	PreSharedKey .....	272
2.2.2.2.93	NETCOMPONENTS .....	272
2.2.2.2.94	ms_msclient .....	272
2.2.2.2.95	ms_server .....	272
2.2.2.2.96	MEDIA .....	272
2.2.2.2.97	Port .....	273
2.2.2.2.98	Device .....	273
2.2.2.2.99	ConnectBPS .....	273
2.2.2.2.100	DEVICE .....	273
2.2.2.2.101	Terminal .....	274
2.2.2.2.102	Name .....	274
2.2.2.2.103	Script .....	275
2.2.2.2.104	X25Pad .....	275
2.2.2.2.105	X25Address .....	275
2.2.2.2.106	UserData .....	275
2.2.2.2.107	Facilities .....	275
2.2.2.2.108	PhoneNumber .....	275
2.2.2.2.109	AreaCode .....	276
2.2.2.2.110	CountryCode .....	276
2.2.2.2.111	CountryID .....	276
2.2.2.2.112	UseDialingRules .....	276
2.2.2.2.113	Comment .....	276
2.2.2.2.114	FriendlyName .....	277
2.2.2.2.115	LastSelectedPhone .....	277
2.2.2.2.116	PromoteAlternates .....	277
2.2.2.2.117	TryNextAlternateOnFail .....	277
2.2.2.2.118	HwFlowControl .....	277
2.2.2.2.119	Protocol .....	277
2.2.2.2.120	Compression .....	278
2.2.2.2.121	Speaker .....	278
2.2.2.2.122	MdmProtocol .....	278
2.2.2.2.123	LineType .....	278
2.2.2.2.124	Fallback .....	278
2.2.2.2.125	EnableCompression .....	279
2.2.2.2.126	ChannelAggregation .....	279
2.2.2.2.127	Proprietary .....	279
2.2.3	Registry Keys .....	279
2.2.3.1	Transport Configuration .....	279
2.2.3.1.1	ProtocolId .....	280
2.2.3.1.2	GlobalInfo .....	280
2.2.3.1.3	GlobalInterfaceInfo .....	280
2.2.3.2	Interface Configuration .....	280
2.2.3.2.1	Common Interface Configuration Values .....	281
2.2.3.2.1.1	InterfaceName .....	281

2.2.3.2.1.2	Type .....	281
2.2.3.2.1.3	Enabled .....	281
2.2.3.2.1.4	DialOutHours .....	281
2.2.3.2.2	Transport-specific Configuration .....	281
2.2.3.2.2.1	ProtocolId .....	282
2.2.3.2.2.2	InterfaceInfo .....	282
2.2.3.3	Ports Configuration .....	282
2.2.3.3.1	Non-modem Device Port Configurations .....	282
2.2.3.3.1.1	ComponentId .....	282
2.2.3.3.1.2	DriverDesc .....	283
2.2.3.3.1.3	EnableForOutboundRouting .....	283
2.2.3.3.1.4	EnableForRas .....	283
2.2.3.3.1.5	EnableForRouting .....	283
2.2.3.3.1.6	CalledIDInformation .....	283
2.2.3.3.1.7	MaxWanEndpoints .....	283
2.2.3.3.1.8	WanEndpoints .....	283
2.2.3.3.2	Modem device Port Configurations .....	283
2.2.3.4	Miscellaneous Configuration Information .....	284
2.2.3.4.1	RouterType .....	284
2.2.3.4.2	IKEv2 Tunnel Configuration Settings .....	284
2.2.3.4.2.1	idleTimeout .....	285
2.2.3.4.2.2	networkBlackoutTime .....	285
2.2.3.4.2.3	saDataSize .....	285
2.2.3.4.2.4	saLifeTime .....	285
2.2.3.4.2.5	TrustedRootCert .....	285
2.2.3.4.3	SSTP Tunnel Configuration Settings .....	285
2.2.3.4.3.1	UseHttps .....	285
2.2.3.4.3.2	IsHashConfiguredByAdmin .....	285
2.2.3.4.3.3	SHA256CertificateHash .....	286
2.2.3.4.3.4	SHA1CertificateHash .....	286
2.2.3.4.4	QuarantineInstalled .....	286
2.2.3.4.5	LoggingFlags .....	286
2.2.3.4.6	ServerFlags .....	286
2.2.3.4.7	ConfigurationFlags .....	288
2.2.3.4.8	AllowNetworkAccess .....	288
2.2.3.4.9	EnableIn .....	288
2.2.3.4.10	EnableNetbtBcastFwd .....	288
2.2.3.4.11	IpAddress .....	288
2.2.3.4.12	IpMask .....	289
2.2.3.4.13	NetworkAdapterGUID .....	289
2.2.3.4.14	UseDhcpAddressing .....	289
2.2.3.4.15	StaticAddressPool .....	289
2.2.3.4.16	AdvertiseDefaultRoute .....	289
2.2.3.4.17	StaticPrefixPool .....	290
2.2.3.4.18	Accounting Settings .....	290
2.2.3.4.18.1	AcctGroupName .....	290
2.2.3.4.18.2	ActiveProvider .....	290
2.2.3.4.18.3	RADIUS-based Accounting Settings .....	290
2.2.3.4.18.3.1	Score .....	290
2.2.3.4.18.3.2	AcctPort .....	290
2.2.3.4.18.3.3	Timeout .....	291
2.2.3.4.18.3.4	EnableAccountingOnOff .....	291
2.2.3.4.19	Authentication Settings .....	291



2.2.3.4.19.1	AuthGroupName .....	291
2.2.3.4.19.2	CRPName .....	291
2.2.3.4.19.3	ActiveProvider .....	291
2.2.3.4.19.4	RADIUS-based Authentication Settings .....	291
2.2.3.4.19.4.1	Score .....	292
2.2.3.4.19.4.2	AuthPort .....	292
2.2.3.4.19.4.3	Timeout .....	292
2.2.3.4.19.4.4	SendSignature .....	292
2.2.4	Error Codes .....	292

### 3 Protocol Details ..... 294

3.1	DIMSVC Interface Server Details .....	294
3.1.1	Abstract Data Model .....	294
3.1.2	Timers .....	295
3.1.3	Initialization .....	295
3.1.4	Message Processing Events and Sequencing Rules .....	295
3.1.4.1	RMprAdminServerGetInfo (Opnum 0) .....	298
3.1.4.2	RRasAdminConnectionEnum (Opnum 1) .....	299
3.1.4.3	RRasAdminConnectionGetInfo (Opnum 2) .....	301
3.1.4.4	RRasAdminConnectionClearStats (Opnum 3) .....	302
3.1.4.5	RRasAdminPortEnum (Opnum 4) .....	303
3.1.4.6	RRasAdminPortGetInfo (Opnum 5) .....	305
3.1.4.7	RRasAdminPortClearStats (Opnum 6) .....	307
3.1.4.8	RRasAdminPortReset (Opnum 7) .....	307
3.1.4.9	RRasAdminPortDisconnect (Opnum 8) .....	308
3.1.4.10	RRouterInterfaceTransportSetGlobalInfo (Opnum 9) .....	309
3.1.4.11	RRouterInterfaceTransportGetGlobalInfo (Opnum 10) .....	311
3.1.4.12	RRouterInterfaceGetHandle (Opnum 11) .....	313
3.1.4.13	RRouterInterfaceCreate (Opnum 12) .....	314
3.1.4.14	RRouterInterfaceGetInfo (Opnum 13) .....	317
3.1.4.15	RRouterInterfaceSetInfo (Opnum 14) .....	319
3.1.4.16	RRouterInterfaceDelete (Opnum 15) .....	321
3.1.4.17	RRouterInterfaceTransportRemove (Opnum 16) .....	322
3.1.4.18	RRouterInterfaceTransportAdd (Opnum 17) .....	323
3.1.4.19	RRouterInterfaceTransportGetInfo (Opnum 18) .....	327
3.1.4.20	RRouterInterfaceTransportSetInfo (Opnum 19) .....	328
3.1.4.21	RRouterInterfaceEnum (Opnum 20) .....	332
3.1.4.22	RRouterInterfaceConnect (Opnum 21) .....	334
3.1.4.23	RRouterInterfaceDisconnect (Opnum 22) .....	335
3.1.4.24	RRouterInterfaceUpdateRoutes (Opnum 23) .....	336
3.1.4.25	RRouterInterfaceQueryUpdateResult (Opnum 24) .....	337
3.1.4.26	RRouterInterfaceUpdatePhonebookInfo (Opnum 25) .....	338
3.1.4.27	RMIBEntryCreate (Opnum 26) .....	339
3.1.4.28	RMIBEntryDelete (Opnum 27) .....	342
3.1.4.29	RMIBEntrySet (Opnum 28) .....	344
3.1.4.30	RMIBEntryGet (Opnum 29) .....	347
3.1.4.31	RMIBEntryGetFirst (Opnum 30) .....	352
3.1.4.32	RMIBEntryGetNext (Opnum 31) .....	355
3.1.4.33	RMIBGetTrapInfo (Opnum 32) .....	356
3.1.4.34	RMIBSetTrapInfo (Opnum 33) .....	358
3.1.4.35	RRasAdminConnectionNotification (Opnum 34) .....	359
3.1.4.36	RRasAdminSendUserMessage (Opnum 35) .....	360
3.1.4.37	RRouterDeviceEnum (Opnum 36) .....	361

3.1.4.38	RRouterInterfaceTransportCreate (Opnum 37)	362
3.1.4.39	RRouterInterfaceDeviceGetInfo (Opnum 38)	364
3.1.4.40	RRouterInterfaceDeviceSetInfo (Opnum 39)	365
3.1.4.41	RRouterInterfaceSetCredentialsEx (Opnum 40)	367
3.1.4.42	RRouterInterfaceGetCredentialsEx (Opnum 41)	368
3.1.4.43	RRasAdminConnectionRemoveQuarantine (Opnum 42)	369
3.1.4.44	RMprAdminServerSetInfo (Opnum 43)	370
3.1.4.45	RMprAdminServerGetInfoEx (Opnum 44)	372
3.1.4.46	RRasAdminConnectionEnumEx (Opnum 45)	373
3.1.4.47	RRasAdminConnectionGetInfoEx (Opnum 46)	374
3.1.4.48	RMprAdminServerSetInfoEx (Opnum 47)	375
3.1.4.49	RRasAdminUpdateConnection (Opnum 48)	376
3.1.4.50	RRouterInterfaceSetCredentialsLocal (Opnum 49)	377
3.1.4.51	RRouterInterfaceGetCredentialsLocal (Opnum 50)	378
3.1.5	Timer Events	379
3.1.6	Other Local Events	379
3.1.6.1	Invoke DIMSVC Method	380
3.1.6.2	Start DIMSVC	380
3.1.6.3	Stop DIMSVC	380
3.2	DIMSVC Interface Client Details	380
3.2.1	Abstract Data Model	380
3.2.2	Timers	380
3.2.3	Initialization	380
3.2.4	Message Processing Events and Sequencing Rules	381
3.2.4.1	RMprAdminServerGetInfo (Opnum 0)	381
3.2.4.2	RRasAdminConnectionEnum (Opnum 1)	381
3.2.4.3	RRasAdminConnectionGetInfo (Opnum 2)	381
3.2.4.4	RRasAdminConnectionClearStats (Opnum 3)	381
3.2.4.5	RRasAdminPortEnum (Opnum 4)	381
3.2.4.6	RRasAdminPortGetInfo (Opnum 5)	381
3.2.4.7	RRasAdminPortClearStats (Opnum 6)	381
3.2.4.8	RRasAdminPortReset (Opnum 7)	382
3.2.4.9	RRasAdminPortDisconnect (Opnum 8)	382
3.2.4.10	RRouterInterfaceTransportSetGlobalInfo (Opnum 9)	382
3.2.4.11	RRouterInterfaceTransportGetGlobalInfo (Opnum 10)	382
3.2.4.12	RRouterInterfaceGetHandle (Opnum 11)	382
3.2.4.13	RRouterInterfaceCreate (Opnum 12)	382
3.2.4.14	RRouterInterfaceGetInfo (Opnum 13)	382
3.2.4.15	RRouterInterfaceSetInfo (Opnum 14)	382
3.2.4.16	RRouterInterfaceDelete (Opnum 15)	382
3.2.4.17	RRouterInterfaceTransportRemove (Opnum 16)	382
3.2.4.18	RRouterInterfaceTransportAdd (Opnum 17)	382
3.2.4.19	RRouterInterfaceTransportGetInfo (Opnum 18)	382
3.2.4.20	RRouterInterfaceTransportSetInfo (Opnum 19)	383
3.2.4.21	RRouterInterfaceEnum (Opnum 20)	383
3.2.4.22	RRouterInterfaceConnect (Opnum 21)	383
3.2.4.23	RRouterInterfaceDisconnect (Opnum 22)	383
3.2.4.24	RRouterInterfaceUpdateRoutes (Opnum 23)	383
3.2.4.25	RRouterInterfaceQueryUpdateResult (Opnum 24)	383
3.2.4.26	RRouterInterfaceUpdatePhonebookInfo (Opnum 25)	383
3.2.4.27	RMIBEntryCreate (Opnum 26)	383
3.2.4.28	RMIBEntryDelete (Opnum 27)	383
3.2.4.29	RMIBEntrySet (Opnum 28)	383

3.2.4.30	RMIBEntryGet (Opnum 29) .....	383
3.2.4.31	RMIBEntryGetFirst (Opnum 30) .....	384
3.2.4.32	RMIBEntryGetNext (Opnum 31) .....	384
3.2.4.33	RRasAdminSendMessage (Opnum 35) .....	384
3.2.4.34	RRouterDeviceEnum (Opnum 36) .....	384
3.2.4.35	RRouterInterfaceTransportCreate (Opnum 37) .....	384
3.2.4.36	RRouterInterfaceDeviceGetInfo (Opnum 38) .....	384
3.2.4.37	RRouterInterfaceDeviceSetInfo (Opnum 39) .....	384
3.2.4.38	RRouterInterfaceSetCredentialsEx (Opnum 40) .....	384
3.2.4.39	RRouterInterfaceGetCredentialsEx (Opnum 41) .....	384
3.2.4.40	RRasAdminConnectionRemoveQuarantine (Opnum 42) .....	384
3.2.4.41	RMprAdminServerSetInfo (Opnum 43) .....	384
3.2.4.42	RMprAdminServerGetInfoEx (Opnum 44) .....	384
3.2.4.43	RRasAdminConnectionEnumEx (Opnum 45) .....	385
3.2.4.44	RRasAdminConnectionGetInfoEx (Opnum 46) .....	385
3.2.4.45	RMprAdminServerSetInfoEx (Opnum 47) .....	385
3.2.4.46	RRasAdminUpdateConnection (Opnum 48) .....	385
3.2.4.47	RRouterInterfaceSetCredentialsLocal (Opnum 49) .....	385
3.2.4.48	RRouterInterfaceGetCredentialsLocal (Opnum 50) .....	385
3.2.5	Timer Events .....	385
3.2.6	Other Local Events .....	385
3.3	RASRPC Interface Server Details .....	385
3.3.1	Abstract Data Model .....	385
3.3.2	Timers .....	386
3.3.3	Initialization .....	386
3.3.4	Message Processing Events and Sequencing Rules .....	386
3.3.4.1	RasRpcDeleteEntry (Opnum 5) .....	387
3.3.4.2	RasRpcGetUserPreferences (Opnum 9) .....	388
3.3.4.3	RasRpcSetUserPreferences (Opnum 10) .....	389
3.3.4.4	RasRpcGetSystemDirectory (Opnum 11) .....	390
3.3.4.5	RasRpcSubmitRequest (Opnum 12) .....	391
3.3.4.6	RasRpcGetInstalledProtocolsEx (Opnum 14) .....	395
3.3.4.7	RasRpcGetVersion (Opnum 15) .....	396
3.3.5	Timer Events .....	397
3.3.6	Other Local Events .....	397
3.3.6.1	Invoke RASRPC Method .....	397
3.3.6.2	Start RASRPC .....	398
3.3.6.3	Stop RASRPC .....	398
3.4	RASRPC Interface Client Details .....	398
3.4.1	Abstract Data Model .....	398
3.4.2	Timers .....	398
3.4.3	Initialization .....	398
3.4.4	Message Processing Events and Sequencing Rules .....	398
3.4.4.1	RasRpcDeleteEntry (Opnum 5) .....	399
3.4.4.2	RasRpcGetUserPreferences (Opnum 9) .....	399
3.4.4.3	RasRpcSetUserPreferences (Opnum 10) .....	399
3.4.4.4	RasRpcGetSystemDirectory (Opnum 11) .....	399
3.4.4.5	RasRpcSubmitRequest (Opnum 12) .....	399
3.4.4.6	RasRpcGetInstalledProtocolsEx (Opnum 14) .....	400
3.4.4.7	RasRpcGetVersion (Opnum 15) .....	400
3.4.5	Timer Events .....	400
3.4.6	Other Local Events .....	400

<b>4 Protocol Examples</b>	<b>401</b>
4.1 Querying Server Configuration Information	401
4.2 Disconnecting a Particular User Connection	401
4.3 Creating a Demand Dial Interface on RRAS with Filters	403
4.4 Enumerating Interfaces and Connecting "dd1"	406
4.5 Querying Interface Status Through MIB	406
4.6 Updating the Connection Endpoint of an IKEv2-Based Connection	407
4.7 Retrieving the Rasrpc Server Version Info	408
4.8 Retrieving Device Configuration Information	409
4.9 Retrieving Specific Port Information	410
4.10 Sample Phonebook File for a Demand-dial Connection	411
4.11 Registry Configuration	415
4.11.1 Transport Configuration	415
4.11.2 Interface Configuration	416
4.11.3 Ports Configuration	417
4.11.4 Other Miscellaneous Configuration Information	418
<b>5 Security</b>	<b>421</b>
5.1 Security Considerations for Implementers	421
5.1.1 Security Considerations Specific to the RRAS Management Protocol	421
5.2 Index of Security Parameters	421
<b>6 Appendix A: Full IDL</b>	<b>422</b>
<b>7 Appendix B: Product Behavior</b>	<b>480</b>
<b>8 Change Tracking</b>	<b>497</b>
<b>9 Index</b>	<b>499</b>

# 1 Introduction

The **Routing and Remote Access Service (RRAS) Server** management (RRASM) protocol enables remote management (configuration and monitoring) of an RRAS implementation. The RRAS implementation here refers to the components that can be configured to provide the following functionality:

- Routing
- Remote access service
- Site-to-site connectivity

The RRASM protocol is a client/server protocol based on **remote procedure call (RPC)**. It comprises RPC methods that enable the remote management of an RRAS implementation.

This document also specifies the registry information that can be used to specify the overall RRAS configuration. These registry settings can be managed remotely using the [\[MS-RRP\]](#) protocol. Additionally, for site-to-site connectivity, the settings to be used to connect to a remote site are specified in the form of a **phonebook file**. This document also specifies the format of the phonebook file used by RRAS server.

As a part of remote management of RRAS implementation, a management application should use the RPC methods to manage the RRAS implementation actively (while RRAS is running). When RRAS is not active, the configurations should be managed through the registry information. The management application can use the phonebook file format to specify the connection configuration to be used for site-to-site connections.

## 1.1 Glossary

The following terms are defined in [\[MS-GLOS\]](#):

**administrator**  
**Advanced Encryption Standard (AES)**  
**American National Standards Institute (ANSI) character set**  
**authentication**  
**authentication level**  
**Authentication Service**  
**binary large object (BLOB)**  
**broadcast**  
**certificate**  
**client**  
**credential**  
**cyclic redundancy check (CRC)**  
**Data Encryption Standard (DES)**  
**device**  
**domain**  
**domain name (2, 3)**  
**Dynamic Host Configuration Protocol (DHCP) server**  
**endpoint**  
**Extensible Authentication Protocol (EAP)**  
**filter**  
**globally unique identifier (GUID)**  
**Interface Definition Language (IDL)**

interface identifier (IID)  
key (1)  
little-endian  
marshal  
named pipe  
NetBIOS  
Network Access Protection (NAP)  
network byte order  
Network Data Representation (NDR)  
opnum  
process identifier (PID)  
Remote Access Service (RAS) server  
remote procedure call (RPC)  
registry  
RPC protocol sequence  
security identifier (SID)  
service principal name (SPN)  
smart card  
subkey  
Unicode  
universally unique identifier (UUID)  
UTC (Coordinated Universal Time)  
value  
Windows registry

The following terms are specific to this document:

**adapter:** The hardware that connects to a particular network segment. A bound LAN card is one example of an **adapter**. Similarly, a computer with two modems, each capable of connecting to a remote network, has two **adapters**, one to represent each modem.

**adapter GUID:** A GUID type identifier that refers uniquely to a particular **adapter**.

**autonomous system (AS):** A group of routers that share a single administrative policy. These routers all use the same **routing protocol**, called an Interior Gateway Protocol, to communicate.

**autostatic route:** A route that is dynamically obtained from a **routing protocol**. After a route is obtained in this manner, it behaves as a **static route**.

**best route:** The optimal route to a network **destination**, based on specified criteria. This concept is based on the fact that there is a certain "cost" involved in taking a route across a network. The **best route** to take is the one with the lowest cost, based on specified criteria. This criteria can include the number of networks crossed, the type of network crossed (for example, public or private), or a monetary or bandwidth limit.

**CalledId:** Originating address of a call.

**callback:** The mechanism through which a remote access client gets called back by the server in order to establish connectivity.

**connection:** The successful completion of necessary protocol arrangements (authentication, network parameters negotiation, and so on) between a remote client computer and the RRAS server to set up a dial-up or **virtual private networking (VPN)** association. **Connection** enables the remote client computer to function on the RRAS server network as if it were connected to the server network directly.

**Compression Control Protocol (CCP):** Allows two computers that communicate through Point-to-Point Protocol (PPP) [\[RFC1661\]](#) to negotiate compatible algorithms for sending and receiving compressed PPP frames. The two computers may not use CCP until the network-control-protocol phase of the PPP connection. For more information, see [\[RFC1962\]](#).

**demand-dial:** Dialing a preconfigured connection only when there is traffic to be sent. Interfaces configured to do so are called demand dial or dial-on-demand (DOD) interfaces.

**destination:** A network entry in the **routing table** represented by a network address and a network mask.

**dial in interface:** The **interface** on the RRAS server that corresponds to all the modem dial-up and virtual private networking clients connected to the RAS server. This is also referred to as an **internal interface**.

**dialing rule:** The rule that specifies the correct sequence of numbers to dial on a modem device. This includes rules that specify the long distance operator and international prefix that is dialed before domestic long distance or international phone numbers.

**Exterior Gateway Protocol (EGP):** Distributes routing information to the routers that connect autonomous systems to a backbone.

**forwarder:** The **forwarder** is the kernel-mode component of the router that is responsible for forwarding data from one router **interface** to the others. The **forwarder** also decides whether a packet is destined for **local** delivery, whether it is destined to be forwarded out of another **interface**, or both. There are two kernel-mode **forwarders**: **unicast** and **multicast**.

**IKEv2-based tunneling protocol:** Tunneling protocol that uses IKEv2 [\[RFC4306\]](#) and IPsec encapsulation using ESP [\[RFC4303\]](#) to provide VPN functionality.

**interface:** Represents a network that can be reached over an **adapter**. Each **interface** has a unique **interface** identifier also known as an **interface** index. **interfaces** that are active have an **adapter** that is providing connectivity to the network they represent. **interfaces** that are inactive do not have an **adapter** providing connectivity unless an administrator disabled the **interface** after it already had an **adapter**. Routing a packet to a network represented by an **interface** will cause the router to allocate an **adapter** for that **interface**, and will establish a wide area network (WAN) connection to the remote network. Allocating an **adapter** to an **interface** is referred to as binding. In the case of a local area network (LAN) **interface**, the **interface** corresponds to an actual physical device in the computer, a LAN **adapter**. In the case of a WAN interface, the **interface** is mapped to a port at the time that a connection is established. The port could be a COM port, a parallel port, or a virtual port (for tunnels such as **PPTP** [\[RFC2637\]](#) and **L2TP** [\[RFC2661\]](#)). WAN interfaces have the additional quality that they typically receive a network address only at the time that a connection is established. For example, a WAN interface using PPP [\[RFC1661\]](#) receives its network layer address from the remote peer during the connection process. Receiving a network address as part of the connection process is sometimes referred to as late-binding.

**Interior Gateway Protocol (IGP):** A protocol that forwards routing information to the other routers in the autonomous system.

**IPX packet filtering:** Input and output filters for each **interface**, configured using key fields in the IPX header.

**IPX route filtering:** Filtering for incoming routes and for the announcement of routes.

**key value pair (KVP):** A set of two linked data items: a key that is an identifier for some data item, and a value that is a value associated with the data item for the identifier represented by the key.

**L2TP:** Layer 2 Tunneling Protocol as specified in [\[RFC2661\]](#).

**local computer (local):** In case of a remote access client connection endpoint on the RRAS server, the **local computer** is the RRAS machine whereas **remote computer (remote)** is the machine from which the client has connected.

**Management Information Base (MIB) APIs:** APIs for RRAS that make it possible to query and set the values of the MIB entries exported by the transport or any of the **routing protocols** on RRAS.

**metrics:** Each route has an administrative **preference** and a client-dependent metric. The router uses this information to determine which is the better route to a **destination**. Routes with lower **preference** are better routes (one being lowest and therefore the best). If two routes have the same **preference**, the route with the lower metric is the better route.

**multicast:** Allows a host to send data to only those **destinations** that specifically request to receive the data. In this way, **multicasting** differs from sending broadcast data, because broadcast data is sent to all hosts. **multicasting** saves network bandwidth because **multicast** data is received only by those hosts that request the data, and the data travels over any link only once. **multicasting** saves server bandwidth because a server has to send only one **multicast** message per network instead of one **unicast** message per receiver. Examples of popular **multicast** applications are online meetings and Internet radio.

**multicast group:** An IP address (that is, in the range of 224.0.0.0- 239.255.255.255). **Multicast** data that is sent to an address in this range is not destined for a single target. Instead, this data can be received by any host that makes a request to join a specific group. A **multicast group** is referred to by either the symbol *G* or *g*.

**multicast heartbeat:** The ability of the router to listen for a regular **multicast** notification to a specified group address. **Multicast heartbeat** is used to verify that IP **multicast** connectivity is available on the network. If the heartbeat is not received within a configured amount of time, the **multicast heartbeat** status of the configured **interface** is set to inactive.

**multicast routing protocol:** A protocol that manages group membership and controls the path that **multicast** data takes over the network. Examples of **multicast routing protocols** include Protocol Independent Multicast (PIM), Multicast Open Shortest Path First (MOSPF), and Distance Vector **multicast routing protocol** (DVMRP). The Internet Group Management Protocol (IGMP) is a special **multicast routing protocol** that acts as an intermediary between hosts and routers.

**multicast source:** The IP address of the host from which the **multicast** data originated. A source is referred to by either the symbol *S* or *s*.

**multilink phonebook entry or multilink:** A dial-up phonebook entry that can connect to the RAS server using multiple configured devices (or channels, in the case of an ISDN device).

**NetBEUI:** NetBIOS Enhanced User Interface. **NetBEUI** is an enhanced NetBIOS protocol for network operating systems, originated by IBM for the LAN Manager server and now used with many other networks.

**NetBIOS Broadcast propagation:** The forwarding of **NetBIOS** over IPX broadcasts flexibly configured over LANs and **demand-dial** interfaces.



**Network Address Translator (NAT):** An IPv4 router defined in [\[RFC1631\]](#) that can translate the IP addresses and TCP/UDP port numbers of packets as they are forwarded.

**next hop:** The next router on the path toward a **destination**. Packets from a source are forwarded to a **destination** on a hop-by-hop basis.

**next hops:** Routes have one or more **next hops** associated with them. If the **destination** is not on a directly connected network, the **next hop** is the address of the next router (or network) on the outgoing network that can **best route** data to the **destination**. Each **next hop** is uniquely identified by the address of the **next hop** and the **interface** index used to reach the **next hop**. If the **next hop** itself is not directly connected, it is marked as a "remote" **next hop**. In this case, the **forwarder** must perform another lookup using the **next hop's** network address. This lookup is necessary to find the "local" **next hop** used to reach the remote **next hop** and the **destination**.

**phone book:** A file maintained by RRAS to store telephone numbers, and security and network settings used for RAS connections.

**point-to-point interface:** An **interface** that provides communication between a single source and a single **destination**, such as a PPP link.

**point-to-multipoint interface:** An **interface** that provides communication between a single host and multiple **destinations**. Point-to-multipoint **interfaces** can be thought of as a collection of point-to-point links with a single termination, such as an ATM link.

**port:** The logical endpoint of a remote access connection on the client or server.

**ppp-based tunneling protocol:** A protocol such as **PPTP**, **L2TP**, and **SSTP** that uses the PPP protocol to provide VPN functionality.

**PPPoE:** Specifies a method for transmitting PPP frames over Ethernet as specified in [\[RFC2516\]](#).

**PPTP:** Point-to-point tunneling protocol as specified in [\[RFC2637\]](#).

**preserved key:** A shared secret agreed upon by two authenticating entities (**routing and remote access service (RRAS) server** or client in this document).

**preference:** Normally used to indicate priority between **routing protocols**. For example, an administrator can assign Open Shortest Path First (OSPF) a lower (better) **preference** than Routing Information Protocol (RIP). In this case, OSPF routes are preferable to RIP routes.

**RAS port:** The logical endpoint of a remote access connection on the client or server.

**RIP for IPX:** Routing Information Protocol (RIP) for IPX, is the primary **routing protocol** used in IPX internetworks.

**REG\_DWORD:** A registry value type defined to be a **REG\_VALUE\_TYPE** of 4 as defined in [\[MS-RRP\]](#).

**REG\_SZ:** A registry value type defined to be a **REG\_VALUE\_TYPE** of 1 as defined in [\[MS-RRP\]](#).

**REG\_VALUE\_TYPE:** DWORD values used to indicate the format of the data associated with a value.

**route:** A "network path" to a **destination** that has a certain cost associated with it. The cost is represented by its administrative **preference** and its protocol-specific metric.

**router:** A server that handles data forwarding and runs **routing protocols**.

**routing and remote access service (RRAS) server:** A server implementation that is managed by the RRAS protocol and provides routing and remote access service functionality.

**routing protocol:** Used to exchange information regarding routes to a **destination**. **Routing protocols** are either **unicast** or **multicast**. **Routing protocols** advertise routes to a **destination**. A **unicast** route to a **destination** is used by a **unicast routing protocol** to forward **unicast** data to that **destination**. Examples of **unicast routing protocols** include RIP, OSPF, and Border Gateway Protocol (BGP). A **multicast** route to a **destination** is used by some **multicast routing protocols** to create the information that is used to forward **multicast** data from hosts on the **destination** network of the route (known as reverse-path forwarding).

**routing table:** Consists of **destinations**, routes, and **next hops**. These entries define a route to a **destination** network.

**RRAS entry name:** The display name for the RRAS entry.

**RRAS entry/RRAS phonebook entry/RRAS phonebook section:** A grouping of the demand dial connection name and the settings associated with the demand dial connection stored as key value pairs.

**RRAS entry section:** A grouping of the **RRAS entry name** and the settings associated with the RRAS entry stored as key value pairs.

**RRAS Entry Subsection:** Refers to a group of related key value pairs in the RRAS Phonebook Entry.

**RRAS phonebook file/phonebook file:** An ANSI-encoded text file containing the settings for the RRAS entries.

**RRAS phonebook path:** Refers to the location of the phonebook file.

**RRASM client:** The RPC client-side implementation of the RRASM protocol, which can be used to develop management software to remotely manage the RRAS server.

**RRASM server:** The RPC server-side implementation of the RRASM protocol, which provides the server endpoint for remote management of the RRAS server implementation.

**static route:** A route that is manually added to the **routing table**. A **static route** is associated with an **interface** that represents the remote network. Unlike dynamic routes, **static routes** are retained even if the router is restarted or the **interface** is disabled. Typically, routes to remote networks are obtained dynamically through **routing protocols**. However, the administrator can also seed the **routing table** by providing routes manually. These routes are referred to as **static**.

**SSTP:** Secure Socket Tunneling Protocol as specified in [\[MS-SSTP\]](#).

**Service Advertising Protocol (SAP) for IPX:** The mechanism by which the names and addresses of services running on IPX nodes are collected and distributed for NetWare clients.

**SAP filtering:** The filtering of incoming service names and the announcement of service names.

**static SAP service names:** The names that are advertised using SAP.

**static NetBIOS names:** The names that can be configured so that NetBIOS over IPX name query broadcasts for specific NetBIOS names can be forwarded using specific **interfaces**.

**subentry:** Specifies the portion of the phonebook entry that comprises the settings associated with the device configured for the RRAS entry.

**subInterface:** For each RAS client connection in RRAS, one is created and has an index similar to **interface index** called a **subInterface index**. Different RAS clients on the server are associated with different subInterfaces identified by their subInterface index.

**switch:** A logical device type that provides options to run a **terminal window** or a custom script for a dial-up connection. This device type is not used for dialing a connection.

**TAPI:** Telephony Application Programming Interface. A set of functions that allows programming of telephone line-based devices in a device-independent manner.

**terminal window:** An ANSI text-only window in a graphical user interface that emulates a console. This is also referred to as a hyper terminal.

**transport:** A routable **transport** that fits into the router architecture, for example, IPv4, IPv6, or IPX.

**unicast:** The process of sending traffic to a unique address. Unicast traffic is destined for a unique address. **Unicast** routing is the process of forwarding unicast traffic from a source to a **destination** on an internetwork.

**view:** A subset of the **routing table** and contains a group of related routes (for example, **multicast** routes). **Views** are sometimes called routing information bases (RIBs).

**virtual private networking (VPN):** A private data network that makes use of the public telecommunication infrastructure.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as specified in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## 1.2 References

References to Microsoft Open Specification documents do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

### 1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information. Please check the archive site, <http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624>, as an additional source.

[C706] The Open Group, "DCE 1.1: Remote Procedure Call", C706, August 1997, <http://www.opengroup.org/public/pubs/catalog/c706.htm>

[IANA-EAP] Internet Assigned Numbers Authority, "Extensible Authentication Protocol (EAP) Registry", October 2006, <http://www.iana.org/assignments/eap-numbers>

[IANAIfType] Internet Assigned Numbers Authority, "IANAIfType-MIB Definitions", January 2007, <http://www.iana.org/assignments/ianaiftype-mib>

[MS-DTYP] Microsoft Corporation, "[Windows Data Types](#)".

[MS-ERREF] Microsoft Corporation, "[Windows Error Codes](#)".

[MS-L2TPIE] Microsoft Corporation, "[Layer 2 Tunneling Protocol \(L2TP\) IPsec Extensions](#)".

[MS-RNAP] Microsoft Corporation, "[Vendor-Specific RADIUS Attributes for Network Access Protection \(NAP\) Data Structure](#)".

[MS-RPCE] Microsoft Corporation, "[Remote Procedure Call Protocol Extensions](#)".

[MS-RRP] Microsoft Corporation, "[Windows Remote Registry Protocol Specification](#)".

[MS-SSTP] Microsoft Corporation, "[Secure Socket Tunneling Protocol \(SSTP\) Specification](#)".

[MS-TRP] Microsoft Corporation, "[Telephony Remote Protocol Specification](#)".

[RFC950] Mogul, J., and Postel, J., "Internet Standard Subnetting Procedure", STD 5, RFC 950, August 1985, <http://www.ietf.org/rfc/rfc950.txt>

[RFC1002] Network Working Group, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications", STD 19, RFC 1002, March 1987, <http://www.ietf.org/rfc/rfc1002.txt>

[RFC1058] Hedrick, C., "Routing Information Protocol", RFC 1058, June 1988, <http://www.ietf.org/rfc/rfc1058.txt>

[RFC1172] Perkins, D., and Hobby, R., "The Point-to-Point Protocol (PPP) Initial Configuration Options", RFC 1172, July 1990, <http://www.ietf.org/rfc/rfc1172.txt>

[RFC1256] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991, <http://www.ietf.org/rfc/rfc1256.txt>

[RFC1301] Armstrong, S., Freier, A., and Marzullo, K., "Multicast Transport Protocol", RFC 1301, February 1992, <http://www.ietf.org/rfc/rfc1301.txt>

[RFC1334] Lloyd, B., and Simpson, W., "PPP Authentication Protocols", RFC 1334, October 1992, <http://www.ietf.org/rfc/rfc1334.txt>

[RFC1354] Baker, F., "IP Forwarding Table MIB", RFC 1354, July 1992, <http://www.ietf.org/rfc/rfc1354.txt>

[RFC1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993, <http://www.ietf.org/rfc/rfc1542.txt>

[RFC1570] Simpson, W., Ed., "PPP LCP Extensions", RFC 1570, January 1994, <http://www.ietf.org/rfc/rfc1570.txt>

[RFC1631] Egevang, K., and Francis, P., "The IP Network Address Translator (NAT)", RFC 1631, May 1994, <http://www.ietf.org/rfc/rfc1631.txt>

[RFC1634] Allen, M., "Novell IPX Over Various WAN Media (IPXWAN)", RFC 1634, May 1994, <http://www.ietf.org/rfc/rfc1634.txt>

[RFC1661] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994, <http://www.ietf.org/rfc/rfc1661.txt>

[RFC1700] Reynolds, J., and Postel, J., "Assigned Numbers", RFC 1700, October 1994, <http://www.ietf.org/rfc/rfc1700.txt>

[RFC1723] Malkin, G., "RIP Version 2 Carrying Additional Information", RFC 1723, November 1994, <http://tools.ietf.org/html/rfc/rfc1723.txt>

[RFC1850] Baker, F., and Coltun, R., "OSPF Version 2 Management Information Base", RFC 1850, November 1995, <http://www.ietf.org/rfc/rfc1850.txt>

[RFC1962] Rand, D., "The PPP Compression Control Protocol (CCP)", RFC 1962, June 1996, <http://ietf.org/rfc/rfc1962.txt>

[RFC1974] Friend, R., and Simpson, W., "PPP Stac LZS Compression Protocol", RFC 1974, June 1996, <http://www.ietf.org/rfc/rfc1974.txt>

[RFC1990] Sklower, K., Lloyd, B., McGregor, G., et al., "The PPP Multilink Protocol (MP)", RFC 1990, August 1996, <http://www.ietf.org/rfc/rfc1990.txt>

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/rfc/rfc2119.txt>

[RFC2125] Richards, C., and Smith, K., "The PPP Bandwidth Allocation Protocol (BAP) and The PPP Bandwidth Allocation Control Protocol (BACP)", RFC 2125, March 1997, <http://www.ietf.org/rfc/rfc2125.txt>

[RFC2284] Blunk, L., and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998, <http://www.ietf.org/rfc/rfc2284.txt>

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998, <http://www.ietf.org/rfc/rfc2328.txt>

[RFC2365] Meyer, D., "Administratively Scoped IP Multicast", BCP 23, RFC2365, July 1998, <http://www.ietf.org/rfc/rfc2365.txt>

[RFC2433] Zorn, G., and Cobb, S., "Microsoft PPP CHAP Extensions", RFC 2433, October 1998 <http://www.ietf.org/rfc/rfc2433.txt>

[RFC2459] Housley, R., Ford, W., Polk, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999, <http://www.ietf.org/rfc/rfc2459.txt>

[RFC2637] Hamzeh, K., Pall, G., Verthein, W., et al., "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999 <http://www.ietf.org/rfc/rfc2637.txt>

[RFC2661] Townsley, W., Valencia, A., Rubens, A., et al., "Layer Two Tunneling Protocol L2TP", RFC 2661, August 1999, <http://www.ietf.org/rfc/rfc2661.txt>

[RFC2865] Rigney, C., Willens, S., Rubens, A., and Simpson, W., "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000, <http://www.ietf.org/rfc/rfc2865.txt>

[RFC3315] Droms, R., Bound, J., Volz, B., et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003, <http://www.ietf.org/rfc/rfc3315.txt>

[RFC3376] Cain, B., Deering S., Kouvelas, I., et al., "Internet Group Management Protocol, Version 3", RFC 3376, October 2002, <http://www.ietf.org/rfc/rfc3376.txt>

[RFC4292] Haberman, B., "IP Forwarding Table MIB", RFC 4292, April 2006, <http://www.ietf.org/rfc/rfc4292.txt>

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005, <http://www.ietf.org/rfc/rfc4303.txt>

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005, <http://www.ietf.org/rfc/rfc4306.txt>

[RFC4555] P. Eronen, Ed., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006, <http://www.ietf.org/rfc/rfc4555.txt>

[RFC5072] Varada, S., Ed., Haskins, D., and Allen, E., "IP Version 6 over PPP", RFC 5072, September 2007, <http://www.ietf.org/rfc/rfc5072.txt>

## 1.2.2 Informative References

[E164] ITU-T, "The International Public Telecommunication Numbering Plan", Recommendation E.164, February 2005, <http://www.itu.int/rec/T-REC-E.164/e>

**Note** There is a charge to download the specification.

[MS-CHAP] Microsoft Corporation, "[Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol \(CHAP\) Specification](#)".

[MS-GLOS] Microsoft Corporation, "[Windows Protocols Master Glossary](#)".

[MS-PEAP] Microsoft Corporation, "[Protected Extensible Authentication Protocol \(PEAP\) Specification](#)".

[MSDN-NAP] Microsoft Corporation, "Network Access Protection", [http://msdn.microsoft.com/en-us/library/aa369712\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa369712(VS.85).aspx)

[MSDN-RAS] Microsoft Corporation, "RASENTRY Structure", <http://msdn.microsoft.com/en-us/library/aa377274.aspx>

[MSFT-NAQC] Microsoft Corporation, "Network Access Quarantine Control in Windows Server 2003", 2004, <http://technet.microsoft.com/en-us/library/bb726973.aspx>

[MSFT-ROUTING] Microsoft Corporation, "Routing Technologies", <http://technet.microsoft.com/en-us/library/cc786023.aspx>.

[MSFT-RRAS] Microsoft Corporation, "Routing and Remote Access", <http://technet.microsoft.com/en-us/network/bb545655.aspx>.

[OB930E] ITU-T, "List of ITU-T Recommendation E.164 Assigned Country Codes", Complement to ITU-T Recommendation E.164, April 2009, [http://www.itu.int/dms\\_pub/itu-t/opb/sp/T-SP-E.164D-2009-PDF-E.pdf](http://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.164D-2009-PDF-E.pdf)

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996, <http://www.ietf.org/rfc/rfc1994.txt>

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., et al., "A Method for Transmitting PPP over Ethernet (PPPoE)", RFC 2516, February 1999, <http://www.ietf.org/rfc/rfc2516.txt>

[RFC2759] Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000, <http://www.ietf.org/rfc/rfc2759.txt>

[RFC2761] Dunn, J., and Martin, C., "Terminology for ATM Benchmarking", RFC 2761, February 2000, <http://www.ietf.org/rfc/rfc2761.txt>

[RFC3629] Yergeau, F., "UTF-8, A Transformation Format of ISO 10646", STD 63, RFC 3629, November 2003, <http://www.ietf.org/rfc/rfc3629.txt>

[RFC4022] Raghunathan, R., Ed., "Management Information Base for the Transmission Control Protocol (TCP)", RFC 4022, March 2005, <http://www.ietf.org/rfc/rfc4022.txt>

[SPNNAMES] Microsoft Corporation, "Name Formats for Unique SPNs", <http://msdn.microsoft.com/en-us/library/ms677601.aspx>

[X.25] ITU-T, "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit", Recommendation x.25, October 1996, <http://www.itu.int/rec/T-REC-X.25-199610-I/en>

### 1.3 Overview

The RRASM protocol enables remote management (configuration and monitoring) of RRAS. This protocol exposes the RRAS management data objects (described in sections [1.3.1](#), [1.3.2](#), [1.3.3](#), [1.3.4](#), and [1.3.5](#)) and the methods to manage these objects remotely. An RRAS implementation that exposes its configuration in the form of these objects and methods can be managed remotely using the RRASM protocol. The RRASM protocol is responsible for providing the remote management capability only. The way the management objects are used in order to provide RRAS functionality, is specific to the RRAS implementation and is outside the scope of this protocol.

The RPC protocol provides the mechanism to define methods and data structures that are passed as parameters to these methods. It also provides the underlying transport with which these methods can be invoked remotely as well as the data passed as parameters.

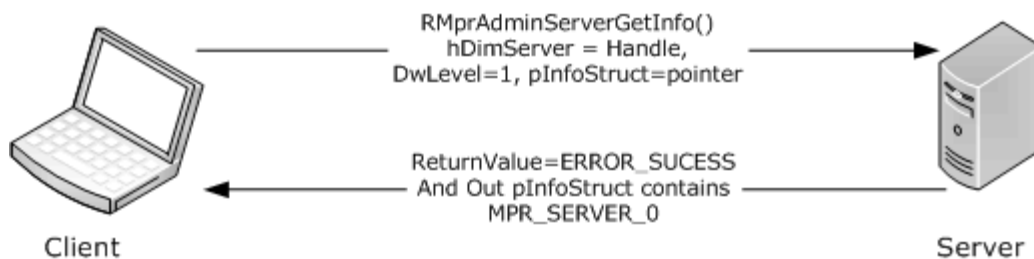
This document, in addition, specifies the registry keys and values that can be used to specify an RRAS server configuration. These registry keys can be remotely configured using the [\[MS-RRP\]](#) protocol. They form the initial configuration for the RRAS implementation. Runtime configuration changes are done through the RPC protocol itself. An RRAS implementation that understands these registry keys and realizes their intended semantics can then be configured remotely using the [\[MS-RRP\]](#) protocol.

This document also specifies the format of the phonebook file that can be used to specify site-to-site connection settings. An RRAS implementation that understands the semantics of this phonebook file can then be configured to provide site-to-site connectivity. The phonebook file can be created remotely at a well-known location using any remote file management mechanism such as the Server Message Block protocol. The RRAS implementation can read the settings and realize the configuration based on the semantics specified.

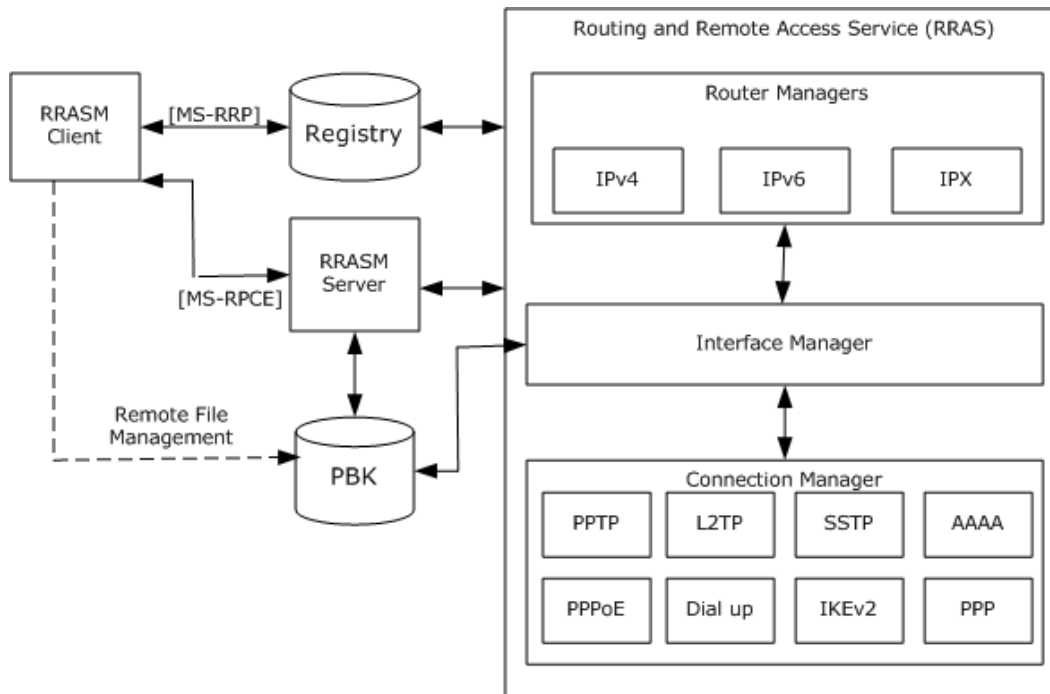
The interaction between a RRASM client and a RRASM server itself is stateless and is accomplished through RPC method invocation. Each RPC method request is independent of others and no context is maintained by RRASM pertaining to the sequence of operations. Each method involves passing of certain parameters from the RRASM client to the RRAS implementation through the RRASM RPC server. The RRAS server should perform the required operation locally in response to the RPC method request and provide the result of the operation to the RRASM server in the form of result information and associated data. The RRASM server is responsible for transporting the result information and the data associated, back to the client that originated the request. This request-response mechanism is provided by the RPC protocol as defined in [\[MS-RPCE\]](#). In a nutshell, the RRASM client and server act as the endpoints providing remote communication to the RRAS implementation which already has these objects defined and managed locally.

The following two figures respectively show the Client/server message exchange and the RRAS conceptual model.





**Figure 1: Client/server message exchange**



**Figure 2: RRAS conceptual model**

The RRASM client and server interact with each other using RPC interfaces. There are two RPC interfaces supported by RRASM: DIMSVC and RASRPC. These interfaces are specified in section [3](#).

The RRAS implementation can be viewed as comprising the following components:

- Interface Manager
- Router Manager
- Connection Manager

The Interface Manager is the component responsible for managing the various interfaces (LAN/WAN) on the RRAS server. The LAN interface refers to the Ethernet interfaces that can participate in routing. The WAN interface can be a dial-in interface (the interface that collectively represents all the remote access clients that are connected to the RRAS server), or a demand dial interface (a WAN interface that is connected on demand to realize secure site-to-site router-level connectivity). For demand dial interfaces, the Interface Manager is responsible for initiating the connection. The connection settings are managed by the Interface Manager using the phonebook file format. The



manager reads the phonebook entry for the demand dial connection settings and passes it to the Connection Manager to perform the task of setting up the connection using a particular protocol.

The Router Managers are responsible for managing various routing protocols. The Router Managers start as a part of the RRAS server initialization. The RRAS server will read the router configuration as specified in the registry store and will initialize the Router Managers with their configuration. There is one Router Manager per transport (for example, the IPv4 Router Manager). The Router Manager in turn is responsible for configuring the various routing protocols (for example, RIP for IPv4 transport) for which the configuration is available. The Router Manager interacts with Interface Manager to monitor the various interfaces and their status. This in turn enables the Router Manager (and the routing protocols) to apply the routing configuration on the various interfaces. The Router Manager is also responsible for providing status and statistical information in the form of a Management Information Base (MIB).

The Connection Manager is the component responsible for managing remote access connections. It provides the implementation of the various protocols as mentioned in the conceptual model (such as PPTP, L2TP, PPP, and so on). It is also responsible for providing authentication, accounting, auditing, and authorization (AAAA) support for the remote access connections. This provides connection-specific detailed information for monitoring purposes.

These three components of RRAS server implement their own providers for configuration and monitoring tasks based on the defined objects and semantics. RRASM can then be used to perform these tasks remotely. The way these tasks are actually realized is outside the scope of the RRASM protocol itself.

The high-level data objects defined for an RRAS implementation to understand and operate on, and remotely managed by the RRASM protocol, are as follows:

- Interface
- Transport
- Management Information Base
- Port
- Connection
- Server

The RRAS implementation is defined to be the provider of these methods and objects for local management. These methods and objects should be made available for the RRASM server to call into. The RRASM protocol makes these objects and methods available remotely over RPC interfaces, thereby enabling remote management.

### 1.3.1 Interface Object

This object provides the interface-specific information and the routing protocol configurations associated with the interface. The interfaces on the RRAS server can be enumerated using [RRouterInterfaceEnum](#). Each interface is associated with a handle that can be used to refer to a particular interface. This handle can be obtained through the [RRouterInterfaceEnum](#) or through [RRouterInterfaceGetHandle](#). For new interfaces, creating the interface through [RRouterInterfaceCreate \(Opnum 12\)](#) will also provide the reference handle. With the interface handle, specific tasks on the interface can be performed, which are as follows:

- [RRouterInterfaceDelete](#)

- [RRouterInterfaceGetInfo](#)
- [RRouterInterfaceSetInfo](#)
- [RRouterInterfaceUpdatePhonebookInfo](#)
- [RRouterInterfaceDeviceGetInfo](#)
- [RRouterInterfaceDeviceSetInfo](#)
- [RRouterInterfaceSetCredentialsEx](#)
- [RRouterInterfaceGetCredentialsEx](#)
- [RRouterInterfaceSetCredentialsLocal](#)
- [RRouterInterfaceGetCredentialsLocal](#)

An interface object corresponding to a demand dial interface can also be used to perform tasks like connect and disconnect using the [RRouterInterfaceConnect](#) and [RRouterInterfaceDisconnect](#) methods.

### 1.3.2 Transport Object

The transports are the various protocols that participate in the routing operation. The transport configurations are realized by the router managers and the routing protocols that are part of the router managers. Each transport is identified by a well-known transport identifier that specifies the protocol for which a certain operation needs to be performed. The transport-specific configuration can be managed through the following methods by specifying the appropriate transport identifier:

- [RRouterInterfaceTransportSetGlobalInfo](#)
- [RRouterInterfaceTransportGetGlobalInfo](#)
- [RRouterInterfaceTransportCreate](#)

Additionally, the transport configurations can be managed for a specific interface using the following methods by specifying the transport identifier and the interface handle.

- [RRouterInterfaceTransportRemove](#)
- [RRouterInterfaceTransportGetInfo](#)
- [RRouterInterfaceTransportSetInfo](#)
- [RRouterInterfaceTransportAdd](#)

For the routing functionality, the route configuration can be updated on the interfaces for a particular transport by using the following methods.

- [RRouterInterfaceUpdateRoutes](#)
- [RRouterInterfaceQueryUpdateResult](#)

### 1.3.3 Management Information Base (MIB)

A number of statistics are collected as a part of the routing functionality of the various routing protocols. The MIB object provides methods and data structures with which this information can be

gathered from the router managers and the routing protocols. The following methods enable these monitoring operations:

- [RMIBEntryCreate](#)
- [RMIBEntryDelete](#)
- [RMIBEntrySet](#)
- [RMIBEntryGet](#)
- [RMIBEntryGetFirst](#)
- [RMIBEntryGetNext](#)
- [RMIBGetTrapInfo](#)
- [RMIBSetTrapInfo](#)

Each of these methods takes the transport identifier and the routing protocol identifier for which the MIB operations are performed.

### 1.3.4 Ports Object

The remote access and site-to-site connection functionality is associated with connectivity. In turn, connectivity is provided by physical devices, such as a modem or ISDN (dial-up), or by virtual devices, such as **PPTP**, **L2TP**, **PPPoE**, **IKEv2**, and **SSTP**. For the RRAS server to accept connectivity, the devices (physical or virtual) need to be configured to accept connections. This is specified through the port configuration. A port is associated with each device type supported. The ports can be used for various connectivity purposes like remote access or demand dial routing connectivity. There can be miscellaneous configurations associated with a particular device type. Configurations of the devices can be set or retrieved through the following methods:

- [RMprAdminServerSetInfo](#)
- [RMprAdminServerGetInfo](#)
- [RMprAdminServerGetInfoEx](#)
- [RMprAdminServerSetInfoEx](#)
- [RRouterDeviceEnum](#)

The following request types, used by [RasRpcSubmitRequest](#), also enable these operations.

- REQTYPE\_GETDEVICECONFIGINFO
- REQTYPE\_SETDEVICECONFIGINFO
- REQTYPE\_GETCALLEDID
- REQTYPE\_SETCALLEDID
- REQTYPE\_GETDEVCONFIG
- REQTYPE\_GETNDISWANDRIVERCAPS

Each port is associated with a port handle that can be retrieved using [RRasAdminPortEnum](#) or the `RasRpcSubmitRequest` with `REQTYPE_PORTENUM`. This handle can be used to perform tasks or queries specific to a port using this handle as reference. For each configured port there are runtime information and statistics obtainable through [RRasAdminPortGetInfo](#). The specific request type `REQTYPE_GETINFO` of the `RasRpcSubmitRequest` method also enables these operations. Other than these get and set operations, there are other port-specific operations possible such as [RRasAdminPortClearStats](#), [RRasAdminPortReset](#), and [RRasAdminPortDisconnect](#).

### 1.3.5 Connection Object

The ports represent an endpoint of the remote access or demand dial connectivity. As a part of the individual device process of establishing the underlying connectivity, there is data available at runtime. The data is represented as connection objects. The connections can be enumerated using [RRasAdminConnectionEnumEx](#) or [RRasAdminConnectionEnum](#). Each connection is associated with a connection handle that can be used to refer to a specific connection instance. This can be obtained through the [RRasAdminPortEnum](#) or [RRasAdminPortGetInfo](#) methods. [RRasAdminConnectionGetInfo](#) or [RRasAdminConnectionGetInfoEx](#) enable the retrieval of the connection-specific information. Other than these, the connection-specific tasks that can be performed are as follows:

- [RRasAdminConnectionClearStats](#)
- [RRasAdminConnectionNotification](#)
- [RRasAdminUpdateConnection](#)
- [RRasAdminConnectionRemoveQuarantine](#)
- [RRasAdminSendUserMessage](#)

## 1.4 Relationship to Other Protocols

The RRAS Management Protocol relies on RPC [\[MS-RPCE\]](#) as a transport. It is used to remotely manage RRAS server implementations. For more information about RRAS, see [\[MSDN-RAS\]](#).

This protocol uses RPC over named pipes as specified in section [2.1](#). The support for the RPC protocol sequence using named pipes is as specified in the [\[MS-RPCE\]](#) section 2.1.1.2.

The registry values that the RRASM client uses for configurations are handled using the [\[MS-RRP\]](#) protocol. Any RRAS server implementation can use these registry settings to initialize the RRAS server configuration.

## 1.5 Prerequisites/Preconditions

This protocol is implemented on top of RPC. The pre-requisites specified in [\[MS-RPCE\]](#) are applicable.

The RRAS Management Protocol assumes that a client has obtained the name or the IP address of the RRAS server that implements this protocol suite before the protocol is invoked.

## 1.6 Applicability Statement

This protocol is applicable when an application needs to remotely configure, manage, or monitor an RRAS server implementation.

## 1.7 Versioning and Capability Negotiation

- **Supported Transports:** The RRAS Management Protocol uses the RPC protocol as a transport and the **RPC protocol sequence** as specified in section [2.1](#).
- **Protocol Versions:** This protocol has two interfaces named DIMSVCS and RASRPC. Each interface has only one interface version. The interfaces have been extended by adding additional methods at the end. The use of these methods is specified in section [3.1](#) and section [3.3](#).
- **Security and Authentication Methods:** **Authentication** and security for the transport used by this protocol are specified in [\[MS-RPCE\]](#). For the RPC interfaces, the security and authentication mechanisms are described in section [5](#).
- **Localization:** This protocol passes text strings in various methods. Localization considerations for such strings are specified where relevant.
- **Capability Negotiation:** The RRAS Management Protocol does not support negotiation of the interface version to use for the RPC interfaces. Instead, this protocol uses only the interface version number specified in the **Interface Definition Language (IDL)** for versioning and capability negotiation.

## 1.8 Vendor-Extensible Fields

This protocol uses error codes as defined in [\[MS-ERREF\]](#) section 2.2. Additional error codes are defined in section [2.2.4](#). Vendors SHOULD reuse those values with their indicated meaning. Choosing any other value runs the risk of a collision in the future.

## 1.9 Standards Assignments

The following parameters are private Microsoft assignments.

Parameter	Value	Reference
RPC interface <b>UUID</b> for dimsvc interface	8f09f000-b7ed-11ce-bbd2-00001a181cad	<a href="#">[C706]</a> section A.2.5
RPC interface UUID for Rasrpc interface	20610036-fa22-11cf-9823-00a0c911e5df	<a href="#">[C706]</a> section A.2.5
<b>Named pipe</b> name	\\PIPE\\ROUTER	

## 2 Messages

### 2.1 Transport

RRASM uses RPC over named pipes, with the named pipe-name as \PIPE\ROUTER.

The protocol MUST use the following UUID for the RPC interfaces.

- 8f09f000-b7ed-11ce-bbd2-00001a181cad for the dimsvc interface
- 20610036-fa22-11cf-9823-00a0c911e5df for the rasrpc interface

#### 2.1.1 Dimsvc Security Settings

##### 2.1.1.1 Server Security Settings

The server interface MUST be identified by the UUID 8f09f000-b7ed-11ce-bbd2-00001a181cad version 0.0. The server MUST specify RPC over SMB as the RPC protocol sequence to the RPC implementation, as specified in [\[MS-RPCE\]](#). The dimsvc RPC server MUST specify "Simple and Protected GSS-API Negotiation Mechanism" (0x09) as the RPC authentication service as specified in [\[MS-RPCE\]](#) section 2.2.1.1.7. The dimsvc RPC SHOULD [<1>](#) support RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY (0x06) as the RPC authentication level. This enables clients requiring data confidentiality to be able to connect to the RPC server interface with data confidentiality.

The dimsvc RPC server, to perform its task, MUST impersonate the RPC identity and ensure that the client belongs to the Administrators group on the server, as specified by the RPC method (described in section [3.1.4](#)).

##### 2.1.1.2 Client Security Settings

The RPC client for the dimsvc RPC interface MUST use ncacn\_np as the RPC protocol sequence. The client MUST specify "Simple and Protected GSS-API Negotiation Mechanism" (0x09) as the authentication service, as specified in [\[MS-RPCE\]](#) section 2.2.1.1.7. The client SHOULD supply a service principal name (SPN) (for more information, see [SPNNAMES]) of "host/hostname" where hostname is the actual name of the server to which the client is connecting and "host/" is the literal string "host/". The RPC client MUST first bind to the named pipe mentioned in section [2.1](#) and use the binding handle obtained (as a part of the binding process) to further communicate with the server, as specified in section 2 of [\[C706\]](#). The RPC client MAY also negotiate RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY as the authentication level in order to ensure the communication to the RPC server is also protected with data confidentiality. The client MUST enable the server to impersonate the client identity by specifying RPC\_C\_IMPL\_LEVEL\_IMPERSONATE as the impersonation level, as specified in [\[MS-RPCE\]](#) section 2.2.1.1.9.

#### 2.1.2 Rasrpc Security Settings

##### 2.1.2.1 Server Security Settings

The server interface MUST be identified by the UUID 20610036-fa22-11cf-9823-00a0c911e5df version 1.0. The server MUST specify RPC over SMB as the RPC protocol sequence to the RPC implementation, as specified in [\[MS-RPCE\]](#). The Rasrpc RPC server SHOULD [<2>](#) specify "Simple and Protected GSS-API Negotiation Mechanism" (0x09) as the RPC Authentication service, as specified in [\[MS-RPCE\]](#) section 2.2.1.1.7. The Rasrpc RPC server SHOULD specify "NT LAN Manager (NTLM)" and

"Kerberos" [\[3\]](#) as additional authentication services supported, as specified in [\[MS-RPCE\]](#) section 2.2.1.1.7. The Rasrpc RPC server SHOULD [\[4\]](#) support all authentication levels up to RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY (0x06) to enable clients to use data confidentiality as required. It SHOULD allow clients to connect only with an authentication level of at least RPC\_C\_AUTHN\_LEVEL\_CONNECT. [\[5\]](#) Additionally, the RPC server MUST allow only clients that are part of the administrators group on the server.

### 2.1.2.2 Client Security Settings

The RPC client for Rasrpc RPC interface MUST use ncacn\_np as the RPC protocol sequence. The client SHOULD [\[6\]](#) specify "Simple and Protected GSS-API Negotiation Mechanism" (0x09) as the authentication service, as specified in [\[MS-RPCE\]](#) section 2.2.1.1.7. The client MAY [\[7\]](#) use "NT LAN Manager (NTLM)" or "Kerberos" as the authentication services specifically to connect to the server. The client SHOULD supply a service principal name (SPN) (for more information, see [\[SPNNAMES\]](#)) of "host/hostname" where "hostname" is the actual name of the server to which the client is connecting. "host/" is the literal string "host/". The RPC client MUST first bind to the named pipe mentioned in section [2.1](#) and use the binding handle obtained (as a part of the binding process) to further communicate with the server, as specified in section 2 of [\[C706\]](#). The client SHOULD negotiate RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY [\[8\]](#) as the authentication level in order to have a secure connection to the RPC server with data confidentiality also. The client MUST enable the server to impersonate the client identity by specifying RPC\_C\_IMPL\_LEVEL\_IMPERSONATE as the impersonation level as described in [\[MS-RPCE\]](#) section 2.2.1.1.9.

## 2.2 Common Data Types

### 2.2.1 RRAS RPC Common Messages

In addition to RPC base types and definitions specified in [\[C706\]](#) and [\[MS-RPCE\]](#), additional data types are defined in this section.

All multi-byte integer values in the messages declared in this section use **little-endian** byte order.

#### 2.2.1.1 Data Types, Enumerations, and Constants

##### 2.2.1.1.1 ROUTER\_INTERFACE\_TYPE

The **ROUTER\_INTERFACE\_TYPE** type enumerates the different kinds of **interfaces** on the RRAS server.

```
typedef enum _ROUTER_INTERFACE_TYPE
{
    ROUTER_IF_TYPE_CLIENT,
    ROUTER_IF_TYPE_HOME_ROUTER,
    ROUTER_IF_TYPE_FULL_ROUTER,
    ROUTER_IF_TYPE_DEDICATED,
    ROUTER_IF_TYPE_INTERNAL,
    ROUTER_IF_TYPE_LOOPBACK,
    ROUTER_IF_TYPE_TUNNEL1,
    ROUTER_IF_TYPE_DIALOUT
} ROUTER_INTERFACE_TYPE;
```

**ROUTER\_IF\_TYPE\_CLIENT:** The interface is for a remote access client.

**ROUTER\_IF\_TYPE\_HOME\_ROUTER:** The interface is for a home RRAS server or a one-way initiated **demand-dial** interface. With one-way initiated **connections**, one **router** is always the answering router and the other router is always the calling router [\[MSFT-ROUTING\]](#).

**ROUTER\_IF\_TYPE\_FULL\_ROUTER:** The interface is for a full router or a two-way initiated demand-dial interface. With two-way initiated connections, either router can be the answering router or the calling router, depending on which router initiates the connection [\[MSFT-ROUTING\]](#).

**ROUTER\_IF\_TYPE\_DEDICATED:** The interface is always connected. It is a LAN interface, or the interface is connected over a leased line.

**ROUTER\_IF\_TYPE\_INTERNAL:** The interface is an internal-only interface.

**ROUTER\_IF\_TYPE\_LOOPBACK:** The interface is a loopback interface.

**ROUTER\_IF\_TYPE\_TUNNEL1:** The interface is an IP in an IP tunnel. [<9>](#)

**ROUTER\_IF\_TYPE\_DIALOUT:** The interface is a demand-dial interface [\[MSFT-ROUTING\]](#).

#### 2.2.1.1.2 ROUTER\_CONNECTION\_STATE

The **ROUTER\_CONNECTION\_STATE** type enumerates the possible states of an interface on the RRAS server.

```
typedef enum
{
    ROUTER_IF_STATE_UNREACHABLE,
    ROUTER_IF_STATE_DISCONNECTED,
    ROUTER_IF_STATE_CONNECTING,
    ROUTER_IF_STATE_CONNECTED
} ROUTER_CONNECTION_STATE;
```

**ROUTER\_IF\_STATE\_UNREACHABLE:** The interface is unreachable.

**ROUTER\_IF\_STATE\_DISCONNECTED:** The interface is reachable, but disconnected.

**ROUTER\_IF\_STATE\_CONNECTING:** The interface is in the process of connecting.

**ROUTER\_IF\_STATE\_CONNECTED:** The interface is connected.

#### 2.2.1.1.3 RAS\_QUARANTINE\_STATE

The **RAS\_QUARANTINE\_STATE** enumerated type indicates the quarantine state of a client connection [\[MS-RNAP\]](#). For more information, see [\[MSDN-NAP\]](#).

```
typedef enum _RAS_QUARANTINE_STATE
{
    RAS_QUAR_STATE_NORMAL,
    RAS_QUAR_STATE_QUARANTINE,
    RAS_QUAR_STATE_PROBATION,
    RAS_QUAR_STATE_UNKNOWN
} RAS_QUARANTINE_STATE;
```

**RAS\_QUAR\_STATE\_NORMAL:** The connection state is normal.



**RAS\_QUAR\_STATE\_QUARANTINE:** The connection is quarantined, meaning that the client did not meet the health requirements [MS-RNAP] and therefore, its access is restricted to specific servers.

**RAS\_QUAR\_STATE\_PROBATION:** The connection is in probation, meaning that the client is not healthy [MS-RNAP] and needs to become healthy within a specified duration.

**RAS\_QUAR\_STATE\_UNKNOWN:** The connection state is unknown.

#### 2.2.1.1.4 RAS\_PORT\_CONDITION

The **RAS\_PORT\_CONDITION** enumerated type specifies information regarding the connection condition of a given **RAS port**.

```
typedef enum _RAS_PORT_CONDITION
{
    RAS_PORT_NON_OPERATIONAL,
    RAS_PORT_DISCONNECTED,
    RAS_PORT_CALLING_BACK,
    RAS_PORT_LISTENING,
    RAS_PORT_AUTHENTICATING,
    RAS_PORT_AUTHENTICATED,
    RAS_PORT_INITIALIZING
} RAS_PORT_CONDITION;
```

**RAS\_PORT\_NON\_OPERATIONAL:** The **port** is non-operational.

**RAS\_PORT\_DISCONNECTED:** The port is disconnected.

**RAS\_PORT\_CALLING\_BACK:** The port is in the process of a calling back a dialed connection.

**RAS\_PORT\_LISTENING:** The port is listening for incoming calls.

**RAS\_PORT\_AUTHENTICATING:** The user connected to the port is being authenticated.

**RAS\_PORT\_AUTHENTICATED:** The port has authenticated a user.

**RAS\_PORT\_INITIALIZING:** The port is initializing.

#### 2.2.1.1.5 RAS\_HARDWARE\_CONDITION

The **RAS\_HARDWARE\_CONDITION** enumeration type specifies hardware status information about a given RAS port.

```
typedef enum _RAS_HARDWARE_CONDITION
{
    RAS_HARDWARE_OPERATIONAL,
    RAS_HARDWARE_FAILURE
} RAS_HARDWARE_CONDITION;
```

**RAS\_HARDWARE\_OPERATIONAL:** The hardware attached to this RAS port is operational and is ready to receive client calls.

**RAS\_HARDWARE\_FAILURE:** The hardware attached to this RAS port has failed.

#### 2.2.1.1.6 DIM\_HANDLE

The **DIM\_HANDLE** is a [handle\\_t](#) used by methods specified in section [3.1.4](#); details of how it is obtained are specified in section [3.1.3](#).

This type is declared as follows:

```
typedef handle_t DIM_HANDLE;
```

#### 2.2.1.1.7 FORWARD\_ACTION

The **FORWARD\_ACTION** enumeration type specifies the type of action to be taken in a **filter**.

```
typedef enum _FORWARD_ACTION
{
    FORWARD = 0,
    DROP = 1
} FORWARD_ACTION;
```

**FORWARD:** Allows the traffic to pass through the filter.

**DROP:** Does not allow the traffic to pass through the filter: drops the traffic.

#### 2.2.1.1.8 MIB\_IPFORWARD\_TYPE

The **MIB\_IPFORWARD\_TYPE** enumeration type specifies the type of the IP **route**.

```
typedef enum
{
    MIB_IPROUTE_TYPE_OTHER = 1,
    MIB_IPROUTE_TYPE_INVALID = 2,
    MIB_IPROUTE_TYPE_DIRECT = 3,
    MIB_IPROUTE_TYPE_INDIRECT = 4
} MIB_IPFORWARD_TYPE;
```

**MIB\_IPROUTE\_TYPE\_OTHER:** Other than the type specified in [\[RFC1354\]](#).

**MIB\_IPROUTE\_TYPE\_INVALID:** An invalid route is deleted.

**MIB\_IPROUTE\_TYPE\_DIRECT:** A local route where the **next hop** is the final destination (a local interface).

**MIB\_IPROUTE\_TYPE\_INDIRECT:** The remote route where the next hop is not the final destination (a remote destination).

#### 2.2.1.1.9 MIB\_IPFORWARD\_PROTO

The **MIB\_IPFORWARD\_PROTO** enumeration indicates which protocols have updated routes.

```
typedef enum
{
    MIB_IPPROTO_OTHER = 1,
```

```

MIB_IPPROTO_LOCAL = 2,
MIB_IPPROTO_NETMGMT = 3,
MIB_IPPROTO_ICMP = 4,
MIB_IPPROTO_EGP = 5,
MIB_IPPROTO_GGP = 6,
MIB_IPPROTO_HELLO = 7,
MIB_IPPROTO_RIP = 8,
MIB_IPPROTO_IS_IS = 9,
MIB_IPPROTO_ES_IS = 10,
MIB_IPPROTO_CISCO = 11,
MIB_IPPROTO_BBN = 12,
MIB_IPPROTO_BGP = 13,
MIB_IPPROTO_OSPF = 14,
MIB_IPPROTO_NT_AUTOSTATIC = 10002,
MIB_IPPROTO_NT_STATIC = 10006,
MIB_IPPROTO_NT_STATIC_NON_DOD = 10007
} MIB_IPFORWARD_PROTO;

```

**MIB\_IPPROTO\_OTHER:** A route added by a protocol not specified in [\[RFC1354\]](#).

**MIB\_IPPROTO\_LOCAL:** A route added locally on an interface.

**MIB\_IPPROTO\_NETMGMT:** A static route. This value is used to identify route information for IP routing set through network management such as DHCP, the Simple Network Management Protocol (SNMP), or by any other API to create routes.

**MIB\_IPPROTO\_ICMP:** A route added as a result of an Internet Control Message Protocol (ICMP) redirect.

**MIB\_IPPROTO\_EGP:** A route added by the Exterior Gateway Protocol (EGP), a dynamic **routing protocol**.

**MIB\_IPPROTO\_GGP:** A route added by the Gateway-to-Gateway Protocol (GGP), a dynamic routing protocol.

**MIB\_IPPROTO\_HELLO:** A route added by the Hellospeak protocol, a dynamic routing protocol. This protocol is not supported and MUST NOT be used.

**MIB\_IPPROTO\_RIP:** A route added by the Berkeley Routing Information Protocol (RIP) or RIP-II, a dynamic routing protocol. See [\[RFC1058\]](#) and [\[RFC1723\]](#).

**MIB\_IPPROTO\_IS\_IS:** A route added by the Intermediate System-to-Intermediate System (IS-IS) protocol, a dynamic routing protocol. The IS-IS protocol was developed for use in the Open Systems Interconnection (OSI) protocol suite.

**MIB\_IPPROTO\_ES\_IS:** A route added by the End System-to-Intermediate System (ES-IS) protocol, a dynamic routing protocol. The ES-IS protocol was developed for use in the Open Systems Interconnection (OSI) protocol suite.

**MIB\_IPPROTO\_CISCO:** A route added by the Cisco Interior Gateway Routing Protocol (IGRP), a dynamic routing protocol.

**MIB\_IPPROTO\_BBN:** A route added by the Bolt, Beranek, and Newman (BBN) Interior Gateway Protocol (IGP) that used the Shortest Path First (SPF) algorithm, a dynamic routing protocol.

**MIB\_IPPROTO\_BGP:** A route added by the Border Gateway Protocol (BGP), a dynamic routing protocol.

**MIB\_IPPROTO\_OSPF:** A route added by the Open Shortest Path First (OSPF) protocol, a dynamic routing protocol.

**MIB\_IPPROTO\_NT\_AUTOSTATIC:** A route that was originally generated by a routing protocol, but now is static.

**MIB\_IPPROTO\_NT\_STATIC:** A route added as a **static route** from the routing user interface or a routing command.

**MIB\_IPPROTO\_NT\_STATIC\_NON\_DOD:** A route added as a static route from the routing user interface or a routing command. These routes do not cause demand-dial.

#### 2.2.1.1.10 MIB\_IPSTATS\_FORWARDING

The **MIB\_IPSTATS\_FORWARDING** enumerates different forwarding possibilities.

```
typedef enum
{
    MIB_IP_FORWARDING = 1,
    MIB_IP_NOT_FORWARDING = 2
} MIB_IPSTATS_FORWARDING,
*PMIB_IPSTATS_FORWARDING;
```

**MIB\_IP\_FORWARDING:** Forwarding-enabled.

**MIB\_IP\_NOT\_FORWARDING:** Not forwarding-enabled.

#### 2.2.1.1.11 MIB\_TCP\_STATE

The **MIB\_TCP\_STATE** enumerates different possible TCP states.

```
typedef enum
{
    MIB_TCP_STATE_CLOSED = 1,
    MIB_TCP_STATE_LISTEN = 2,
    MIB_TCP_STATE_SYN_SENT = 3,
    MIB_TCP_STATE_SYN_RCVD = 4,
    MIB_TCP_STATE_ESTAB = 5,
    MIB_TCP_STATE_FIN_WAIT1 = 6,
    MIB_TCP_STATE_FIN_WAIT2 = 7,
    MIB_TCP_STATE_CLOSE_WAIT = 8,
    MIB_TCP_STATE_CLOSING = 9,
    MIB_TCP_STATE_LAST_ACK = 10,
    MIB_TCP_STATE_TIME_WAIT = 11,
    MIB_TCP_STATE_DELETE_TCB = 12
} MIB_TCP_STATE;
```

**MIB\_TCP\_STATE\_CLOSED:** The TCP connection is closed.

**MIB\_TCP\_STATE\_LISTEN:** The TCP connection is in the listen state.

**MIB\_TCP\_STATE\_SYN\_SENT:** A SYN packet has been sent.

**MIB\_TCP\_STATE\_SYN\_RCVD:** A SYN packet has been received.

**MIB\_TCP\_STATE\_ESTAB:** The TCP connection has been established.

**MIB\_TCP\_STATE\_FIN\_WAIT1:** The TCP connection is waiting for a FIN packet.

**MIB\_TCP\_STATE\_FIN\_WAIT2:** The TCP connection is waiting for a FIN packet.

**MIB\_TCP\_STATE\_CLOSE\_WAIT:** The TCP connection is in the close wait state.

**MIB\_TCP\_STATE\_CLOSING:** The TCP connection is closing.

**MIB\_TCP\_STATE\_LAST\_ACK:** The TCP connection is in the last ACK state.

**MIB\_TCP\_STATE\_TIME\_WAIT:** The TCP connection is in the time wait state.

**MIB\_TCP\_STATE\_DELETE\_TCB:** The TCP connection is in the delete TCB state.

#### 2.2.1.1.12 TCP\_RTO\_ALGORITHM

The **TCP\_RTO\_ALGORITHM** enumerates different TCP retransmission time-out algorithms.

```
typedef enum
{
    MIB_TCP_RTO_OTHER = 1,
    MIB_TCP_RTO_CONSTANT = 2,
    MIB_TCP_RTO_RSRE = 3,
    MIB_TCP_RTO_VANJ = 4
} TCP_RTO_ALGORITHM,
*PTCP_RTO_ALGORITHM;
```

**MIB\_TCP\_RTO\_OTHER:** Other.

**MIB\_TCP\_RTO\_CONSTANT:** Constant time-out.

**MIB\_TCP\_RTO\_RSRE:** MIL-STD-1778. See [\[RFC4022\]](#).

**MIB\_TCP\_RTO\_VANJ:** Van Jacobson's algorithm.

#### 2.2.1.1.13 IP\_NAT\_DIRECTION

This enumeration contains **network address translation (NAT)** directions.

```
typedef enum
{
    NatInboundDirection = 0,
    NatOutboundDirection
} IP_NAT_DIRECTION,
*PIP_NAT_DIRECTION;
```

**NatInboundDirection:** The packet was received from a public address and is to be sent to private address.

**NatOutboundDirection:** The packet was received from a private address and is to be sent to public address.

#### 2.2.1.1.14 OSPF\_PARAM\_TYPE

This enumeration contains an OSPF parameter type that defines the type of information in the following structures.

- [OSPF\\_ROUTE\\_FILTER\\_INFO \(section 2.2.1.2.209\)](#)
- [OSPF\\_PROTO\\_FILTER\\_INFO \(section 2.2.1.2.210\)](#)
- [OSPF\\_GLOBAL\\_PARAM \(section 2.2.1.2.211\)](#)
- [OSPF\\_AREA\\_PARAM \(section 2.2.1.2.212\)](#)
- [OSPF\\_AREA\\_RANGE\\_PARAM \(section 2.2.1.2.213\)](#)
- [OSPF\\_VIRT\\_INTERFACE\\_PARAM \(section 2.2.1.2.214\)](#)

```
typedef enum
{
    OSPF_END_PARAM_TYPE = 0,
    OSPF_GLOBAL_PARAM_TYPE,
    OSPF_AREA_PARAM_TYPE,
    OSPF_AREA_RANGE_PARAM_TYPE,
    OSPF_INTF_PARAM_TYPE,
    OSPF_NEIGHBOR_PARAM_TYPE,
    OSPF_VIRT_INTF_PARAM_TYPE,
    OSPF_ROUTE_FILTER_PARAM_TYPE,
    OSPF_PROTOCOL_FILTER_PARAM_TYPE
} OSPF_PARAM_TYPE;
```

**OSPF\_END\_PARAM\_TYPE:** Specifies that there is no more configuration information and marks the end of the configuration.

**OSPF\_GLOBAL\_PARAM\_TYPE:** Mapped to the OSPF\_GLOBAL\_PARAM structure.

**OSPF\_AREA\_PARAM\_TYPE:** Mapped to the OSPF\_AREA\_PARAM structure.

**OSPF\_AREA\_RANGE\_PARAM\_TYPE:** Mapped to the OSPF\_AREA\_RANGE\_PARAM structure.

**OSPF\_INTF\_PARAM\_TYPE:** Mapped to the OSPF\_INTF\_PARAM\_TYPE structure.

**OSPF\_NEIGHBOR\_PARAM\_TYPE:** Mapped to the OSPF\_NEIGHBOR\_PARAM\_TYPE structure.

**OSPF\_VIRT\_INTF\_PARAM\_TYPE:** Mapped to the OSPF\_VIRT\_INTF\_PARAM\_TYPE structure.

**OSPF\_ROUTE\_FILTER\_PARAM\_TYPE:** Mapped to the OSPF\_ROUTE\_FILTER\_PARAM\_TYPE structure.

**OSPF\_PROTOCOL\_FILTER\_PARAM\_TYPE:** Mapped to the OSPF\_PROTOCOL\_FILTER\_PARAM\_TYPE structure.

#### 2.2.1.1.15 OSPF\_FILTER\_ACTION

This enumeration is used to determine whether or not a route is added to the OSPF database.

```
typedef enum _OSPF_FILTER_ACTION
{
```

```

ACTION_DROP = 0,
ACTION_ACCEPT = 1
} OSPF_FILTER_ACTION,
*POSPF_FILTER_ACTION;

```

**ACTION\_DROP:** The route is not added to the OSPF database.

**ACTION\_ACCEPT:** The route is added to the OSPF database.

### 2.2.1.1.16 RASDEVICETYPE

The **RASDEVICETYPE** type enumeration defines the different **device** types on the RRAS server.

```

typedef enum _RASDEVICETYPE
{
    RDT_Modem = 0,
    RDT_X25,
    RDT_Isdn,
    RDT_Serial,
    RDT_FrameRelay,
    RDT_Atm,
    RDT_Sonet,
    RDT_Sw56,
    RDT_Tunnel_Pptp,
    RDT_Tunnel_L2tp,
    RDT_Irda,
    RDT_Parallel,
    RDT_Other,
    RDT_PPPOE,
    RDT_Tunnel_Sstp,
    RDT_Tunnel_Ikev2,
    RDT_Tunnel = 0x00010000,
    RDT_Direct = 0x00020000,
    RDT_Null_Modem = 0x00040000,
    RDT_Broadband = 0x00080000
} RASDEVICETYPE;

```

**RDT\_Modem:** Modem device

**RDT\_X25:** X.25 device

**RDT\_Isdn:** ISDN device

**RDT\_Serial:** Serial port device

**RDT\_FrameRelay:** Frame relay device

**RDT\_Atm:** Asynchronous transfer mode (ATM) device

**RDT\_Sonet:** Sonet device

**RDT\_Sw56:** Switched 56K access device

**RDT\_Tunnel\_Pptp:** PPTP device

**RDT\_Tunnel\_L2tp:** L2TP device

**RDT\_Irda:** Infrared Data Association (IrDA) device.

**RDT\_Parallel:** Parallel port device.

**RDT\_Other:** Any other device.

**RDT\_PPPE:** PPPoE device [<10>](#)

**RDT\_Tunnel\_Sstp:** SSTP device [<11>](#)

**RDT\_Tunnel\_Ikev2:** IKEv2 device [<12>](#)

**RDT\_Tunnel:** Specifies the tunnel device class like PPTP, L2TP, SSTP, IKEv2.

**RDT\_Direct:** Specifies the direct device class like Serial, Parallel.

**RDT\_Null\_Modem:** Specifies modem device class like Modem, Isdn, Irda.

**RDT\_Broadband:** Specifies broadband device class like PPPoE. [<13>](#)

The final four values (RDT\_Tunnel, RDT\_Direct, RDT\_Null\_Modem, RDT\_Broadband) are used to specify the class of the device.

#### 2.2.1.1.17 RASMAN\_STATUS

The **RASMAN\_STATUS** type enumerates the status of the Port.

```
typedef enum _RASMAN_STATUS
{
    OPEN = 0,
    CLOSED = 1,
    UNAVAILABLE = 2,
    REMOVED = 3
} RASMAN_STATUS;
```

**OPEN:** Port is in open state for a connection.

**CLOSED:** Port is in closed state and is available for connection.

**UNAVAILABLE:** Port is in the process of being removed and is not available for connection.

**REMOVED:** Port is removed and is not available for connection.

#### 2.2.1.1.18 ReqTypes

The **ReqTypes** enumerations indicate the different types of message requests that can be passed in the **RB\_ReqType** field of [RequestBuffer](#) structure.

```
typedef enum _ReqTypes
{
    REQTYPE_PORTENUM = 21,
    REQTYPE_GETINFO = 22,
    REQTYPE_GETDEVCONFIG = 73,
    REQTYPE_SETDEVICECONFIGINFO = 94,
    REQTYPE_GETDEVICECONFIGINFO = 95,
    REQTYPE_GETCALLEDID = 105,
    REQTYPE_SETCALLEDID = 106,
```



```

    REQTYPE_GETNDISWANDRIVERCAPS = 111
} ReqTypes;

```

**REQTYPE\_PORTENUM:** Request to enumerate all the port information on the RRAS.

**REQTYPE\_GETINFO:** Request to get information about a specific port on the RRAS.

**REQTYPE\_GETDEVCONFIG:** Request to get device information on the RRAS.

**REQTYPE\_SETDEVICECONFIGINFO:** Request to set device configuration information on RRAS.

**REQTYPE\_GETDEVICECONFIGINFO:** Request to get device configuration information on RRAS.

**REQTYPE\_GETCALLEDID:** Request to get CalledId information for a specific device on RRAS.

**REQTYPE\_SETCALLEDID:** Request to set CalledId information for a specific device on RRAS.

**REQTYPE\_GETNDISWANDRIVERCAPS:** Request to get the encryption capabilities of the RRAS.

#### 2.2.1.1.19 RASMAN\_STATE

The **RASMAN\_STATE** enumeration indicates the connection condition of a given RAS port.

```

typedef enum _RASMAN_STATE
{
    CONNECTING = 0,
    LISTENING = 1,
    CONNECTED = 2,
    DISCONNECTING = 3,
    DISCONNECTED = 4,
    LISTENCOMPLETED = 5
} RASMAN_STATE;

```

**CONNECTING:** The port is in the process of connecting.

**LISTENING:** The port is listening for connection requests.

**CONNECTED:** The port is connected.

**DISCONNECTING:** The port is in the process of disconnecting.

**DISCONNECTED:** The port is disconnected.

**LISTENCOMPLETED:** The port has completed listening for connection requests.

#### 2.2.1.1.20 RASMAN\_DISCONNECT\_TYPE

The **RASMAN\_DISCONNECT\_TYPE** enumeration indicates different types of disconnection requests for a given RAS port.

```

typedef enum _RASMAN_DISCONNECT_TYPE
{

```

```

    USER_REQUESTED = 0,
    REMOTE_DISCONNECTION = 1,
    HARDWARE_FAILURE = 2,
    NOT_DISCONNECTED = 3
} RASMAN_DISCONNECT_TYPE;

```

**USER\_REQUESTED:** The local user requested the disconnect action.

**REMOTE\_DISCONNECTION:** The remote dial-up or VPN client requested the disconnect action.

**HARDWARE\_FAILURE:** The hardware attached to this RAS port has failed.

**NOT\_DISCONNECTED:** The port is not disconnected.

#### 2.2.1.1.21 RASMAN\_USAGE

**RASMAN\_USAGE** enumerates the usage for a port. It can be any combination of the following values.

```

typedef enum _RASMAN_USAGE
{
    CALL_NONE = 0x00,
    CALL_IN = 0x01,
    CALL_OUT = 0x02,
    CALL_ROUTER = 0x04,
    CALL_LOGON = 0x08,
    CALL_OUT_ONLY = 0x10,
    CALL_IN_ONLY = 0x20,
    CALL_OUTBOUND_ROUTER = 0x40
} RASMAN_USAGE;

```

**CALL\_NONE:** Port is not configured for any usage.

**CALL\_IN:** Port is configured for incoming connection requests.

**CALL\_OUT:** Port is configured for outgoing connection requests

**CALL\_ROUTER:** Port is configured for demand dial connection requests.

**CALL\_LOGON:** Port is configured for connection during logon.

**CALL\_OUT\_ONLY:** Port is configured only for outgoing connection requests.

**CALL\_IN\_ONLY:** Port is configured only for incoming connection requests.

**CALL\_OUTBOUND\_ROUTER:** Port is configured for outgoing demand dial connection requests.

#### 2.2.1.2 Structures

##### 2.2.1.2.1 DIM\_INFORMATION\_CONTAINER

The **DIM\_INFORMATION\_CONTAINER** specifies a generic information container used by certain methods to store and retrieve information.

```

typedef struct _DIM_INFORMATION_CONTAINER {

```

```

    DWORD dwBufferSize;
    [size_is(dwBufferSize)] LPBYTE pBuffer;
} DIM_INFORMATION_CONTAINER,
*PDIM_INFORMATION_CONTAINER;

```

**dwBufferSize:** This MUST be set to the size, in bytes, of the data being pointed to by **pBuffer**.

**pBuffer:** A pointer to a buffer of size **dwBufferSize** that contains the information. The information contained in this buffer is specific to the API in which this structure is used.

This information can be any of the following structures:

- [MPR\\_SERVER\\_0](#)
- [MPR\\_SERVER\\_1](#)
- [MPR\\_SERVER\\_2](#)
- [RASI\\_CONNECTION\\_0](#)
- [RASI\\_CONNECTION\\_1](#)
- [RASI\\_CONNECTION\\_2](#)
- [RASI\\_CONNECTION\\_3](#)
- [RASI\\_PORT\\_0](#)
- [RASI\\_PORT\\_1](#)
- [MPRI\\_INTERFACE\\_0](#)
- [MPRI\\_INTERFACE\\_1](#)
- [MPRI\\_INTERFACE\\_2](#)

**DIM\_INFORMATION\_CONTAINER** specifies a generic information container used by the following methods to store and retrieve information:

- [RMprAdminServerGetInfo \(section 3.1.4.1\)](#)
- [RRasAdminConnectionEnum \(section 3.1.4.2\)](#)
- [RRasAdminConnectionGetInfo \(section 3.1.4.3\)](#)
- [RRasAdminPortEnum \(section 3.1.4.5\)](#)
- [RRasAdminPortGetInfo \(section 3.1.4.6\)](#)
- [RRouterInterfaceCreate \(section 3.1.4.13\)](#)
- [RRouterInterfaceGetInfo \(section 3.1.4.14\)](#)
- [RRouterInterfaceSetInfo \(section 3.1.4.15\)](#)
- [RRouterInterfaceEnum \(section 3.1.4.21\)](#)

- [RRouterInterfaceDeviceInfo \(section 3.1.4.39\)](#)
- [RRouterInterfaceDeviceSetInfo \(section 3.1.4.40\)](#)
- [RRouterInterfaceSetCredentialsEx \(section 3.1.4.41\)](#)
- [RRouterInterfaceGetCredentialsEx \(section 3.1.4.42\)](#)

#### 2.2.1.2.2 DIM\_INTERFACE\_CONTAINER

The **DIM\_INTERFACE\_CONTAINER** specifies a generic structure used by certain methods to set, create, or retrieve information from the RRAS server.

```
typedef struct _DIM_INTERFACE_CONTAINER {
    DWORD fGetInterfaceInfo;
    DWORD dwInterfaceInfoSize;
    [size_is(dwInterfaceInfoSize)] LPBYTE pInterfaceInfo;
    DWORD fGetGlobalInfo;
    DWORD dwGlobalInfoSize;
    [size_is(dwGlobalInfoSize)] LPBYTE pGlobalInfo;
} DIM_INTERFACE_CONTAINER,
*PDIM_INTERFACE_CONTAINER;
```

**fGetInterfaceInfo:** This field is used to get interface information from the server. This MUST be set to TRUE when the client needs to retrieve interface information from the server while calling the [RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#) and [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#) methods.

**dwInterfaceInfoSize:** This MUST be set to the size of *pInterfaceInfo*.

**pInterfaceInfo:** This MUST point to a buffer that specifies the default client interface information for the **transport**. The buffer MUST contain [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) with a valid info type of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#).

**fGetGlobalInfo:** This field is used to get or set global information. This field MUST be set to TRUE when the client needs to retrieve global information from the server while calling [RRouterInterfaceTransportGetGlobalInfo](#).

**dwGlobalInfoSize:** This MUST be set to the size of *pGlobalInfo*.

**pGlobalInfo:** This MUST point to a buffer that specifies global information for the transport. The buffer MUST contain a **RTR\_INFO\_BLOCK\_HEADER** with a valid info type of [RTR\\_TOC\\_ENTRY](#).

The **DIM\_INTERFACE\_CONTAINER** specifies a generic structure used by the following methods to set, create, or retrieve information from the RRAS server.

- [RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)
- [RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)
- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

### 2.2.1.2.3 RTR\_INFO\_BLOCK\_HEADER

The **RTR\_INFO\_BLOCK\_HEADER** specifies information pertaining to the protocol using a set of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) structures. These structures are encapsulated by an **RTR\_INFO\_BLOCK\_HEADER**.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version																															
Size																															
TocEntriesCount																															
TocEntry (variable)																															
...																															

**Version (4 bytes):** A 32-bit, unsigned integer in **network byte order** that MUST be set to 0x00000001. No other versions are defined.

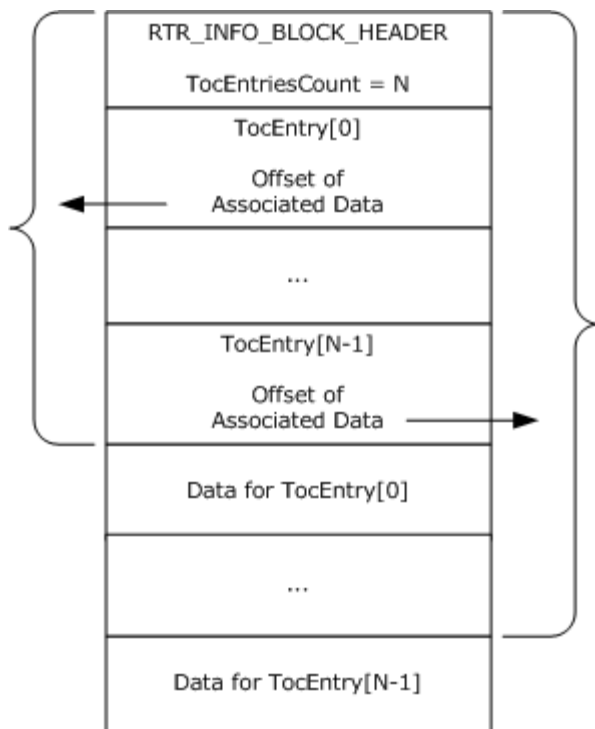
**Size (4 bytes):** A 32-bit, unsigned integer in network byte order that MUST specify the size of the structure in bytes including the **Version**, **Size**, **TocEntriesCount**, and entries (**TocEntry**). The size MUST be at least 28 bytes. The total size depends on the number and type of the entries. This value MUST be the size of the blob represented by the structure. This MUST be the sum of the **InfoSize** of each element of **TocEntry** and **TocEntriesCount** times the size of RTR\_TOC\_ENTRY.

**TocEntriesCount (4 bytes):** A 32-bit, unsigned integer in network byte order that MUST specify the number of entries. It MUST be greater than 0.

**TocEntry (variable):** A list of consecutive entries, **TocEntriesCount** in number, each of which MUST be formatted as defined in RTR\_TOC\_ENTRY.

### 2.2.1.2.4 RTR\_TOC\_ENTRY

The RTR\_TOC\_ENTRY structure specifies the format in which information pertaining to the type of data is stored in [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#). The following figure shows the relationships between the block header and the entries.



**Figure 3: Block header and entries**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
InfoType																															
InfoSize																															
Count																															
Offset																															

**InfoType (4 bytes):** A 32-bit, unsigned integer in network byte order that MUST indicate the type of data contained in the list. The value MUST be one of the following when the transport is IPv4 or IPv6. [<14>](#)

Value	Meaning	Structure pointed to at offset
0xffff0001 IP_IN_FILTER_INFO	This is the input filter that is applied to the IP packets sent to the RRAS server.	<a href="#">FILTER_DESCRIPTOR (section 2.2.1.2.5)</a>
0xffff0002 IP_OUT_FILTER_INFO	This is the output filter that is applied to the IP packets sent from the	FILTER_DESCRIPTOR (section 2.2.1.2.5)

Value	Meaning	Structure pointed to at offset
	RRAS server.	
0xffff0003 IP_GLOBAL_INFO	Global IP filtering information.	<a href="#">GLOBAL_INFO (section 2.2.1.2.9)</a>
0xffff0004 IP_INTERFACE_STATUS_INFO	IPv4 interface status information.	<a href="#">INTERFACE_STATUS_INFO (section 2.2.1.2.18)</a>
0xffff0005 IP_ROUTE_INFO	Routing information is added. If bV4 of INTERFACE_ROUTE_INFO is set, an IPv4 route is added; otherwise, an IPv6 route is added.	<a href="#">INTERFACE_ROUTE_INFO (section 2.2.1.2.11)</a>
0xffff0006 IP_PROT_PRIORITY_INFO	Protocol priority information.	<a href="#">PRIORITY_INFO (section 2.2.1.2.12)</a>
0xffff0007 IP_ROUTER_DISC_INFO	Router discovery information.	<a href="#">RTR_DISC_INFO (section 2.2.1.2.14)</a>
0xffff0009 IP_DEMAND_DIAL_FILTER_INFO	The IP traffic that matches this filter indicates that a demand-dial connection is available and all the IP packets matching this filter MUST be routed into the connection.	FILTER_DESCRIPTOR (section 2.2.1.2.5)
IP_MCAST_HEARTBEAT_INFO 0xffff000a	This specifies the multicast heart beat configuration for an interface.	<a href="#">MCAST_HBEAT_INFO (section 2.2.1.2.15)</a>
0xffff000b IP_MCAST_BOUNDARY_INFO	Multicast boundary information.	<a href="#">MIB_BOUNDARYROW (section 2.2.1.2.24)</a>
0xffff000c IP_IPINIP_CFG_INFO	IP in IP configuration information.	<a href="#">IPINIP_CONFIG_INFO (section 2.2.1.2.17)&lt;15&gt;</a>
0xffff000d IP_IFFILTER_INFO	IPv4 interface filter information.	<a href="#">IFFILTER_INFO (section 2.2.1.2.89)</a>
0xffff000e IP_MCAST_LIMIT_INFO	Multicast configuration information.	<a href="#">MIB_MCAST_LIMIT_ROW (section 2.2.1.2.16)</a>
0xffff000f IPV6_GLOBAL_INFO	Global IPv6 filtering information.	GLOBAL_INFO (section 2.2.1.2.9)<16>
0xffff0011 IP_IN_FILTER_INFO_V6	This is the input filter that MUST be applied to the IPv6 packets sent to the RRAS server.	<a href="#">FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7)&lt;17&gt;</a>

Value	Meaning	Structure pointed to at offset
0xffff0012 IP_OUT_FILTER_INFO_V6	This is the output filter that MUST be applied to the IPv6 packets sent from the RRAS server.	FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7) <a href="#">&lt;18&gt;</a>
0xffff0013 IP_DEMAND_DIAL_FILTER_INFO_V6	IPv6 traffic that matches this filter indicates that a site-to-site connection MUST be available and all the IPv6 packets matching this filter MUST be routed into the connection.	FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7) <a href="#">&lt;19&gt;</a>
0xffff0014 IP_IFFILTER_INFO_V6	IPv6 interface filter information.	IFFILTER_INFO (section 2.2.1.2.89) <a href="#">&lt;20&gt;</a>
0x0000270f MS_IP_BOOTP	IP BOOTP global or interface information depending on the method that calls.	<a href="#">IPBOOTP GLOBAL CONFIG (section 2.2.1.2.150)</a> <a href="#">IPBOOTP IF CONFIG (section 2.2.1.2.151)</a>
0x4137000a MS_IP_IGMP	IGMP global or interface information depending on the method that calls.	<a href="#">IGMP MIB GLOBAL CONFIG (section 2.2.1.2.174)</a> <a href="#">IGMP MIB IF CONFIG (section 2.2.1.2.175)</a>
0x00000008 MS_IP_RIP	IP RIP global or interface information depending on the method that calls.	<a href="#">IPRIP IF CONFIG (section 2.2.1.2.167)</a> <a href="#">IPRIP GLOBAL CONFIG (section 2.2.1.2.165)</a>
0x81372714 MS_IP_DHCP_ALLOCATOR	DHCP allocator global or interface information depending on the method that calls.	<a href="#">IP_AUTO_DHCP GLOBAL INFO (section 2.2.1.2.191)</a> <a href="#">IP_AUTO_DHCP INTERFACE INFO (section 2.2.1.2.192)</a>
0x81372713 MS_IP_DNS_PROXY	DNS Proxy global or interface information depending on the method that calls.	<a href="#">IP_DNS_PROXY GLOBAL INFO (section 2.2.1.2.193)</a> <a href="#">IP_DNS_PROXY INTERFACE INFO (section 2.2.1.2.194)</a>
0x81372715 MS_IP_NAT	IP NAT global or interface information depending on the method that calls.	<a href="#">IP_NAT GLOBAL INFO (section 2.2.1.2.195)</a> <a href="#">IP_NAT INTERFACE INFO (section 2.2.1.2.197)</a>
0x0000000d MS_IP_OSPF <a href="#">&lt;21&gt;</a>	OSPF global or interface information depending on the method that calls.	<a href="#">OSPF_ROUTE_FILTER_INFO (section 2.2.1.2.209)</a> <a href="#">OSPF_PROTO_FILTER_INFO (section 2.2.1.2.210)</a> <a href="#">OSPF_GLOBAL_PARAM (section 2.2.1.2.211)</a> <a href="#">OSPF_AREA_PARAM (section</a>



Value	Meaning	Structure pointed to at offset
		<a href="#">2.2.1.2.212)</a> <a href="#">OSPF AREA RANGE PARAM (section 2.2.1.2.213)</a> <a href="#">OSPF VIRT INTERFACE PARAM (section 2.2.1.2.214)</a> <a href="#">OSPF INTERFACE PARAM (section 2.2.1.2.215)</a> <a href="#">OSPF NBMA NEIGHBOR PARAM (section 2.2.1.2.216)</a>
0x000003E7 MS_IPV6_DHCP	DHCPv6 Relay global or interface information depending on the method that calls.	<a href="#">DHCPV6R_IF_CONFIG (section 2.2.1.2.160)</a> <a href="#">DHCPV6R_GLOBAL_CONFIG (section 2.2.1.2.158)</a>

The value MUST be one of the following when the transport is IPX. <22>

Value	Meaning	Structure pointed to at offset
0x00000001 IPX_INTERFACE_INFO_TYPE	Specifies the IPX interface data.	<a href="#">IPX_IF_INFO (section 2.2.1.2.92)</a>
0x00000002 IPX_STATIC_ROUTE_INFO_TYPE	Specifies the route information for an IPX interface.	<a href="#">IPX_STATIC_ROUTE_INFO (section 2.2.1.2.94)</a>
0x00000003 IPX_STATIC_SERVICE_INFO_TYPE	Specifies information about the transport layer protocol that is being multiplexed.	<a href="#">IPX_STATIC_SERVICE_INFO (section 2.2.1.2.95)</a>
0x00000006 IPX_IN_TRAFFIC_FILTER_INFO_TYPE	Specifies the filter data for an IPX interface.	<a href="#">IPX_TRAFFIC_FILTER_INFO (section 2.2.1.2.99)</a>
0x00000007 IPX_ADAPTER_INFO_TYPE	Specifies the adapter information for the IPX.	<a href="#">IPX_ADAPTER_INFO (section 2.2.1.2.97)</a>
0x00000008 IPXWAN_IF_INFO	Specifies whether IPXWAN negotiation is to be disabled or enabled.	<a href="#">IPXWAN_IF_INFO (section 2.2.1.2.93)</a>
0x00000009 IPX_GLOBAL_INFO_TYPE	Specifies global IPX information. See IPX_GLOBAL_INF O for the actual	<a href="#">IPX_GLOBAL_INFO (section 2.2.1.2.91)</a>

Value	Meaning	Structure pointed to at offset
	information.	
0x0000000a IPX_STATIC_NETBIOS_NAME_INFO_TYPE	Specifies the NetBIOS name of an IPX interface.	<a href="#">IPX_STATIC_NETBIOS_NAME_INFO (section 2.2.1.2.96)</a>
0x0000000b IPX_IN_TRAFFIC_FILTER_GLOBAL_INFO_TYPE	Specifies the action for a filter match.	<a href="#">IPX_TRAFFIC_FILTER_GLOBAL_INFO (section 2.2.1.2.98)</a>
0x0000000c IPX_OUT_TRAFFIC_FILTER_INFO_TYPE	Specifies the filter data for an IPX interface.	IPX_TRAFFIC_FILTER_INFO (section 2.2.1.2.99)
0x0000000d IPX_OUT_TRAFFIC_FILTER_GLOBAL_INFO_TYPE	Specifies the action for a filter match.	IPX_TRAFFIC_FILTER_GLOBAL_INFO (section 2.2.1.2.98)
0x00020000 IPX_PROTOCOL_RIP	RIP global or interface information depending on the method that calls.	<a href="#">RIP_GLOBAL_INFO (section 2.2.1.2.202)</a> <a href="#">RIP_IF_CONFIG (section 2.2.1.2.206)</a>
0x00020001 IPX_PROTOCOL_SAP	SAP global or interface information depending on the method that calls.	<a href="#">SAP_GLOBAL_CONFIG (section 2.2.1.2.207)</a> <a href="#">SAP_IF_CONFIG (section 2.2.1.2.115)</a>

**InfoSize (4 bytes):** A 32-bit, unsigned integer, in network byte-order, that MUST specify the number of bytes in an information structure of this type in this entry.

**Count (4 bytes):** A 32-bit, unsigned integer in network byte order that MUST specify the number of information structures of this type in this entry.

**Offset (4 bytes):** A 32-bit, unsigned integer in network byte order that MUST specify the offset of start of the first structure for this entry.

### 2.2.1.2.5 FILTER\_DESCRIPTOR

The **FILTER\_DESCRIPTOR** is the structure that MUST be used while specifying IPv4 filters.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwVersion																															
dwNumFilters																															
faDefaultAction																															

fiFilter (variable)
...

**dwVersion (4 bytes):** A 32-bit integer in network byte order used to specify the version. It MUST be 0x00000001. No other versions are defined.

**dwNumFilters (4 bytes):** A 32-bit integer in network byte order used to specify the number of filters. It MUST be greater than 0.

**faDefaultAction (4 bytes):** A 32-bit integer in network byte order used to specify the action for the filter. It MUST be [FORWARD ACTION \(section 2.2.1.1.7\)](#).

**fiFilter (variable):** This MUST contain the actual five tuple filters as specified in section [2.2.1.2.6](#).

When this structure is used as an embedded structure in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **infoType** of RTR\_TOC\_ENTRY MUST have the value 0xffff0001, 0xffff0002, or 0xffff0009 to specify an IPv4 in filter, an IPv4 out filter, or an IPv4 demand-dial filter respectively.

This structure is used in the following methods:

- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)
- [RRouterInterfaceTransportCreate \(section 3.1.4.38\)](#)

## 2.2.1.2.6 FILTER\_INFO

The **FILTER\_INFO** structure MUST specify the five tuple filter to be used in [FILTER\\_DESCRIPTOR \(section 2.2.1.2.5\)](#).

```
typedef struct _FILTER_INFO {
    DWORD dwSrcAddr;
    DWORD dwSrcMask;
    DWORD dwDstAddr;
    DWORD dwDstMask;
    DWORD dwProtocol;
    DWORD fLateBound;
    WORD wSrcPort;
    WORD wDstPort;
} FILTER_INFO,
*PFILTER_INFO;
```

**dwSrcAddr:** A 32-bit, unsigned integer in network byte order that MUST contain the IPv4 source address for which the filter applies. A value of 0x00000000 in this field signifies ANY.

**dwSrcMask:** A 32-bit, unsigned integer in network byte order that MUST contain the subnet mask for the source address. See [\[RFC950\]](#).

**dwDstAddr:** A 32-bit, unsigned integer in network byte order that MUST contain the IPv4 destination address for the filter. A value of 0x00000000 in this field signifies ANY.

**dwDstMask:** A 32-bit, unsigned integer in network byte order that MUST be the subnet mask for the destination address in network byte order. See [\[RFC950\]](#).

**dwProtocol:** A 32-bit, unsigned integer in little-endian byte order that MUST be the protocol number (such as TCP or UDP) for the filter.

Possible values include the following.

Value	Meaning
0x00000000	ANY
0x00000001	ICMP
0x0000003A	ICMPv6
0x00000006	TCP
0x00000011	UDP

The complete list is specified in [\[RFC1700\]](#).

**fLateBound:** A 32-bit, unsigned integer in little-endian byte order that indicates to the RRAS server if the fields in the filter may be dynamically replaced by the RRAS server with values for specific **endpoints** at the time those endpoints request network access.

This MUST be a combination of one or more of the following values:

Value	Meaning
0x00000000	No source or destination address or mask replacement.
0x00000001	Source address replaceable with a new address.
0x00000004	Destination address replaceable with a new address.
0x00000010	Source address mask replaceable with a new mask.
0x00000020	Destination address mask replaceable with a new mask.

**wSrcPort:** If the protocol is TCP or UDP, this MUST be a 16-bit, unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the protocol is ICMP or ICMPv6, this MUST be a 16-bit, unsigned integer in little-endian byte order that specifies a type indicator for ICMP or ICMPv6 correspondingly. For all other protocol values, this MUST be set to 0 (byte order does not matter).

**wDstPort:** If the protocol is TCP or UDP, this MUST be a 16-bit, unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the protocol is ICMP or ICMPv6, this MUST be a 16-bit, unsigned integer in little-endian byte order that specifies a code indicator for ICMP or ICMPv6 correspondingly. For all other protocol values, this MUST be set to 0 (byte order does not matter).

### 2.2.1.2.7 FILTER\_DESCRIPTOR\_V6

The **FILTER\_DESCRIPTOR\_V6** is the structure that MUST be used while specifying IPv6 filters.

This structure is used in the following methods:

- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)
- [RRouterInterfaceTransportCreate \(section 3.1.4.38\)](#)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwVersion																															
dwNumFilters																															
faDefaultAction																															
fiFilter (variable)																															
...																															

**dwVersion (4 bytes):** A 32-bit integer in network byte order used to specify the version. It MUST be 0x00000001. No other versions are defined.

**dwNumFilters (4 bytes):** A 32-bit integer in network byte order used to specify the number of filters. It MUST be greater than 0.

**faDefaultAction (4 bytes):** A 32-bit integer in network byte order used to specify the action for the filter. It MUST be [FORWARD ACTION \(section 2.2.1.1.7\)](#).

**fiFilter (variable):** This is defined in [FILTER\\_INFO\\_V6 \(section 2.2.1.2.8\)](#).

When this structure is used as an embedded structure in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** of RTR\_TOC\_ENTRY MUST be 0xffff0011, 0xffff0012, or 0xffff0013. [<23>](#)

### 2.2.1.2.8 FILTER\_INFO\_V6

The **FILTER\_INFO\_V6** structure MUST specify the five tuple filters to be used in [FILTER\\_DESCRIPTOR\\_V6 \(section 2.2.1.2.7\)](#). [<24>](#)

```
typedef struct _FILTER_INFO_V6 {
    BYTE ipv6SrcAddr[16];
    DWORD dwSrcPrefixLength;
    BYTE ipv6DstAddr[16];
    DWORD dwDstPrefixLength;
    DWORD dwProtocol;
    DWORD fLateBound;
    WORD wSrcPort;
```

```

WORD wDstPort;
} FILTER_INFO_V6,
*PFILTER_INFO_V6;

```

**ipv6SrcAddr:** A 128-bit, unsigned integer in network byte order that MUST contain the IPv6 source address for which the filter applies. A value of zero in this field signifies ANY.

**dwSrcPrefixLength:** A 32-bit, unsigned integer in network byte order that MUST be the prefix length for the source address. A value of zero in this field signifies ANY source address.

**ipv6DstAddr:** A 128-bit, unsigned integer in network byte order that MUST contain the IPv6 destination address for the filter. A value of zero in this field signifies ANY.

**dwDstPrefixLength:** A 32-bit, unsigned integer in network byte order that MUST be the prefix length for the destination address. A value of zero in this field signifies ANY destination address.

**dwProtocol:** A 32-bit, unsigned integer in network byte order that specifies the protocol number (such as TCP or UDP) for the filter.

Possible values include the following.

Value	Meaning
0x00000000	ANY
0x00000001	ICMP
0x0000003A	ICMPv6
0x00000006	TCP
0x00000011	UDP

**fLateBound:** A 32-bit, unsigned integer in network byte order that indicates if the fields in the filter may be dynamically replaced by the network access server (NAS) with values for specific endpoints.

The value MUST be one of the following values, or a bit-wise OR a combination of the following values.

Value	Meaning
0x00000000	No source or destination address or mask replacement.
0x00000001	Source address replaceable with a new address.
0x00000004	Destination address replaceable with a new address.
0x00000010	Source address mask replaceable with a new mask.
0x00000020	Destination address mask replaceable with a new mask.

**wSrcPort:** If the protocol is TCP or UDP, this MUST be a 16-bit, unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the protocol is ICMP

or ICMPv6, this MUST be a 16-bit, unsigned integer in network byte order that specifies a type indicator for ICMP or ICMPv6 correspondingly. For all other protocol values, this MUST be set to 0 (byte order does not matter).

**wDstPort:** If the protocol is TCP or UDP, this MUST be a 16-bit, unsigned integer in network byte order that specifies a port number for the corresponding protocol. If the protocol is ICMP or ICMPv6, this MUST be a 16-bit, unsigned integer in network byte order that specifies a code indicator for ICMP or ICMPv6 correspondingly. For all other protocol values, this MUST be set to 0 (byte order does not matter).

#### 2.2.1.2.9 GLOBAL\_INFO

The **GLOBAL\_INFO** structure is used to set logging levels and enable filtering on the RRAS server.

This structure is used in the following methods:

- [RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)
- [RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

```
typedef struct _GLOBAL_INFO {  
    BOOL bFilteringOn;  
    DWORD dwLoggingLevel;  
} GLOBAL_INFO,  
*PGLOBAL_INFO;
```

**bFilteringOn:** This MUST be set to 0x00000001; filtering is always enabled.

**dwLoggingLevel:** This MUST be set to the logging levels so that if the RRAS server has different levels of logging information this field specifies the logging level and MUST be one of the following values.

Value	Meaning
0x00000000	Log no messages.
0x00000001	Log all errors.
0x00000002	Log all warnings and errors.
0x00000003	Log all errors, warnings, and information.

When this structure is used, the **InfoType** of [RTR TOC ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff0003 or 0xffff000f.

#### 2.2.1.2.10 IN6\_ADDR

The **IN6\_ADDR** structure represents an IPv6 address.

```
typedef struct in6_addr {  
    union {  
        UCHAR Byte[16];  
        USHORT Word[8];  
    } u;
```

```

} IN6_ADDR,
*PIN6_ADDR,
*LPIN6_ADDR;

```

**Byte:** An IPv6 address represented as an array of 16 UCHAR values.

**Word:** An IPv6 address represented as an array of USHORT values.

#### 2.2.1.2.11 INTERFACE\_ROUTE\_INFO

The **INTERFACE\_ROUTE\_INFO** <25> structure or **MIB\_IPFORWARDROW** (section 2.2.1.2.35) <26> MUST be used to specify the routes to be added or deleted on the RRAS server. Whenever this structure is used, the **InfoType** of **RTR\_TOC\_ENTRY** (section 2.2.1.2.4) MUST be 0xffff0005. <27>

This structure is used in the following methods:

- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```

typedef struct _INTERFACE_ROUTE_INFO {
    union {
        struct {
            DWORD dwRtInfoDest;
            DWORD dwRtInfoMask;
            DWORD dwRtInfoPolicy;
            DWORD dwRtInfoNextHop;
            DWORD dwRtInfoAge;
            DWORD dwRtInfoNextHopAS;
            DWORD dwRtInfoMetric1;
            DWORD dwRtInfoMetric2;
            DWORD dwRtInfoMetric3;
        };
        struct {
            IN6_ADDR DestinationPrefix;
            DWORD DestPrefixLength;
            IN6_ADDR NextHopAddress;
            ULONG ValidLifeTime;
            DWORD Flags;
            ULONG Metric;
        };
    };
    DWORD dwRtInfoIfIndex;
    DWORD dwRtInfoType;
    DWORD dwRtInfoProto;
    DWORD dwRtInfoPreference;
    DWORD dwRtInfoViewSet;
    BOOL bV4;
} INTERFACE_ROUTE_INFO,
*PINTERFACE_ROUTE_INFO;

```



**dwRtInfoDest:** This MUST be the destination IPv4 address of the route. An entry with an IPv4 address of 0.0.0.0 is considered a default route. This member cannot be set to a **multicast** IPv4 address.

**dwRtInfoMask:** This MUST be the IPv4 subnet mask to be logically ANDed with the destination IPv4 address before being compared to the value in the **dwRtInfoDest** member. See [\[RFC950\]](#).

**dwRtInfoPolicy:** This MUST be set to the conditions that would cause the selection of a multipath route (the set of **next hops** for a given destination). This member is typically in IP TOS format. The encoding of this member is specified in [\[RFC1354\]](#).

**dwRtInfoNextHop:** This MUST be the IPv4 address of the next system in the route. Otherwise, this member SHOULD be an IPv4 address of 0.0.0.0.

**dwRtInfoAge:** This MUST be the number of seconds since the route was added or modified in the network **routing table**.

**dwRtInfoNextHopAS:** This MUST be the autonomous system number of the next hop. When this member is unknown or not relevant to the protocol or routing mechanism specified in **dwRtInfoProto**, this value SHOULD be set to 0. This value is documented in [\[RFC1354\]](#).

**dwRtInfoMetric1:** This MUST be the primary routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwRtInfoProto** member. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

**dwRtInfoMetric2:** This MUST be an alternate routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwRtInfoProto** member. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

**dwRtInfoMetric3:** This MUST be an alternate routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwRtInfoProto** member. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

**DestinationPrefix:** This MUST be the IPv6 address prefix for the destination IP address for this route.

**DestPrefixLength:** The length, in bits, of the site prefix or network part of the IP address specified in **DestinationPrefix**. Any value greater than 128 is an illegal value. A value of 255 is commonly used to represent an illegal value.

**NextHopAddress:** This MUST be the IPv6 address of the next system or gateway for a remote route. If the route is to a local loopback address or an IP address on the local link, the next hop is unspecified (all zeros). For a local loopback route, this member SHOULD be an IPv6 address of 0::0.

**ValidLifeTime:** The maximum time, in seconds, the IP route entry is valid. A value of 0xffffffff is infinite.

**Flags:** Reserved. This MUST be set to 0.

**Metric:** The route metric offset for this IP route entry. The semantics of this metric are determined by the routing protocol specified in **dwRtInfoProto**. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC4292\]](#).

**dwRtInfoIfIndex:** This MUST be the index of the local interface through which the next hop of this route is reachable.

**dwRtInfoType:** This MUST be the route type as specified in [\[RFC1354\]](#).

The following list shows the possible values for this member. [<28>](#)

Value	Meaning
MIB_IPROUTE_TYPE_OTHER 0x00000001	A type other than what is specified in <a href="#">[RFC1354]</a> .
MIB_IPROUTE_TYPE_INVALID 0x00000002	An invalid route is logically deleted.
MIB_IPROUTE_TYPE_DIRECT 0x00000003	A local route where the next hop is the final destination (a local interface).
MIB_IPROUTE_TYPE_INDIRECT 0x00000004	The remote route where the next hop is not the final destination (a remote destination).

**dwRtInfoProto:** The protocol or routing mechanism that generated the route. It MUST be one of the values specified in MIB\_IPFORWARD\_PROTO.

**dwRtInfoPreference:** Specifies the route preference as determined by the routing protocol in **dwRtInfoProto**.

**dwRtInfoViewSet:** Specifies the Route Information Table **views**. It MUST be a combination of the following values, or a combination of RTM\_VIEW\_MASK\_UCAST and RTM\_VIEW\_MASK\_MCAST.

Value	Meaning
RTM_VIEW_MASK_ANY 0x00000000	This value is used to define or set the mask for the Route Information Table view. This value is a mask for any type of route.
RTM_VIEW_MASK_UCAST 0x00000001	This value is used to define or set the mask for Route Information Table view. This value is a mask for <b>unicast</b> routes.
RTM_VIEW_MASK_MCAST 0x00000002	This value is used to define or set the mask for the Route Information Table view. This value is a mask for multicast routes.
RTM_VIEW_MASK_ALL 0xFFFFFFFF	This value is used to define or set the mask for the Route Information Table view. This value is a mask for all types of routes.

**bV4:** Set to 1 if it is an IPV4 route; set to 0 to indicate an IPV6 route. For an IPV4 route, the first structure in the union is used. For an IPV6 route, the second structure in the union is used.

#### 2.2.1.2.12 PRIORITY\_INFO

The **PRIORITY\_INFO** structure MUST be used to set **preferences** to different protocols on the RRAS server.

This structure is used in the following methods:

- [RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

- [RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumProtocols																															
ppmProtocolMetric (variable)																															
...																															

**dwNumProtocols (4 bytes):** This MUST be the number of protocols for which metric information is given in this structure [PROTOCOL\\_METRIC \(section 2.2.1.2.13\)](#).

**ppmProtocolMetric (variable):** This MUST be an array of **PROTOCOL\_METRIC** structures with **dwNumProtocols** specifying the number of elements in the array.

When this structure is used, the **InfoType** of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff0006. Multiple instances of this structure may be present. If multiple instances are present, and there are overlapping protocol IDs, the metric specified in the last instance will be set.

#### 2.2.1.2.13 PROTOCOL\_METRIC

The **PROTOCOL\_METRIC** structure MUST be used to specify the metric of a protocol in [PRIORITY\\_INFO \(section 2.2.1.2.12\)](#).

```
typedef struct _PROTOCOL_METRIC {
    DWORD dwProtocolId;
    DWORD dwMetric;
} PROTOCOL_METRIC,
*PPROTOCOL_METRIC;
```

**dwProtocolId:** The protocol ID. This SHOULD be one of the values specified in [MIB\\_IPFORWARD\\_PROTO<29>](#).

**dwMetric:** The metric for **dwProtocolId**.

#### 2.2.1.2.14 RTR\_DISC\_INFO

The **RTR\_DISC\_INFO** is used to set and retrieve router discovery information according to [\[RFC1256\]](#).

This structure is used in the following methods.

- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)
- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)

```
typedef struct _RTR_DISC_INFO {
    WORD wMaxAdvtInterval;
    WORD wMinAdvtInterval;
    WORD wAdvtLifetime;
    BOOL bAdvertise;
```

```

    LONG lPrefLevel;
} RTR_DISC_INFO,
*PRTR_DISC_INFO;

```

**wMaxAdvtInterval:** This MUST be set to the maximum time allowed between sending multicast Router Advertisements from the interface, in seconds. It MUST be no less than 4 seconds and no greater than 1800 seconds.

**wMinAdvtInterval:** This MUST be the minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. It MUST be no less than 3 seconds and no greater than **wMaxAdvtInterval**.

**wAdvtLifetime:** This MUST be the value to be placed in the **Lifetime** field of Router Advertisements sent from the interface, in seconds. It MUST be no less than **wMaxAdvtInterval** and no greater than 9000 seconds.

**bAdvertise:** This MUST be the flag indicating whether or not the address is to be advertised.

**lPrefLevel:** This MUST be the preference of the address as a default router address, relative to other router addresses on the same subnet. A 32-bit, signed, twos complement integer, with higher values meaning more preferable. The minimum value (hex 80000000) is used to indicate that the address, even if advertised, is not to be used by neighboring hosts as a default router address.

When this structure is used, the **InfoType** of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff0007.

#### 2.2.1.2.15 MCAST\_HBEAT\_INFO

The **MCAST\_HBEAT\_INFO** is used for multicast heartbeat information. See [\[RFC1301\]](#) and [\[RFC3376\]](#) for more details.

```

typedef struct _MCAST_HBEAT_INFO {
    WCHAR pwszGroup[64];
    BOOL bActive;
    ULONG ulDeadInterval;
    BYTE byProtocol;
    WORD wPort;
} MCAST_HBEAT_INFO,
*PMCAST_HBEAT_INFO;

```

**pwszGroup:** A null-terminated **Unicode** string containing the name and address of the multicast group.

**bActive:** Indicates whether or not the heartbeat is active.

**ulDeadInterval:** The dead interval in minutes.

**byProtocol:** Specifies how the heartbeat is being carried out. This MUST have one of the following values:

Value	Meaning
RAW (0xFF)	A non-UDP based protocol is specified for use as multicast heartbeat. wPort specifies the identifier for the protocol.
UDP (0x11)	UDP-based protocol is specified for use as multicast heartbeat. wPort specifies the UDP port number.

**wPort:** The port or protocol for which the heartbeat is being carried out.

When this structure is used, the **InfoType** of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff000a.

#### 2.2.1.2.16 MIB\_MCAST\_LIMIT\_ROW

The **MIB\_MCAST\_LIMIT\_ROW** is used to specify the configuration information for a multicast interface.

This structure is used in the following method:

- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```
typedef struct {
    DWORD dwTtl;
    DWORD dwRateLimit;
} MIB_MCAST_LIMIT_ROW,
*PMIB_MCAST_LIMIT_ROW;
```

**dwTtl:** The Time to Live (TTL) value for a multicast interface.

**dwRateLimit:** The rate limit for a multicast interface.

When this structure is used, the **InfoType** of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff000e.

#### 2.2.1.2.17 IPINIP\_CONFIG\_INFO

The **IPINIP\_CONFIG\_INFO** structure is used to specify configuration information for an IP in an IP tunnel. [<30>](#)

```
typedef struct _IPINIP_CONFIG_INFO {
    DWORD dwRemoteAddress;
    DWORD dwLocalAddress;
    BYTE byTtl;
} IPINIP_CONFIG_INFO,
*PIPINIP_CONFIG_INFO;
```

**dwRemoteAddress:** The destination address of the IP in the IP packet.

**dwLocalAddress:** The source address of the IP in the IP packet.

**byTtl:** The **TTL** field for the IP in the IP packet.

When this structure is used, the **InfoType** of [RTR TOC ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff000c.

#### 2.2.1.2.18 INTERFACE\_STATUS\_INFO

The **INTERFACE\_STATUS\_INFO** structure contains the administrative status of an interface.

This structure is used in the following methods:

- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```
typedef struct _INTERFACE_STATUS_INFO {  
    DWORD dwAdminStatus;  
} INTERFACE_STATUS_INFO,  
*PINTERFACE_STATUS_INFO;
```

**dwAdminStatus:** The administrative status of the interface. It MUST be one of the following values.

Value	Meaning
IF_ADMIN_STATUS_UP 0x00000001	Interface is administratively enabled
IF_ADMIN_STATUS_DOWN 0x00000002	Interface is administratively disabled

When this structure is used, the **InfoType** of [RTR TOC ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff0004.

#### 2.2.1.2.19 DIM\_MIB\_ENTRY\_CONTAINER

The **DIM\_MIB\_ENTRY\_CONTAINER** structure contains the size and the data for the management information base (MIB) entries that are either set or retrieved from the MIB variables.

This structure is used in the following methods:

- [RMIBEntryCreate \(section 3.1.4.27\)](#)
- [RMIBEntryDelete \(section 3.1.4.28\)](#)
- [RMIBEntrySet \(section 3.1.4.29\)](#)
- [RMIBEntryGet \(section 3.1.4.30\)](#)
- [RMIBEntryGetFirst \(section 3.1.4.31\)](#)
- [RMIBEntryGetNext \(section 3.1.4.32\)](#)

```
typedef struct _DIM_MIB_ENTRY_CONTAINER {
    DWORD dwMibInEntrySize;
    [size_is(dwMibInEntrySize)] LPBYTE pMibInEntry;
    DWORD dwMibOutEntrySize;
    [size_is(dwMibOutEntrySize)] LPBYTE pMibOutEntry;
} DIM_MIB_ENTRY_CONTAINER,
*PDIM_MIB_ENTRY_CONTAINER;
```

**dwMibInEntrySize:** This field gives the size of the MIB entry data being input. It represents the size of the data contained in **pMibInEntry**.

**pMibInEntry:** A pointer to a protocol-specific structure that contains input data.

**dwMibOutEntrySize:** This field gives the size of the MIB entry data being output. It represents the size of the data contained in **pMibOutEntry**.

**pMibOutEntry:** This member points to the protocol-specific structure that points to the MIB.

The contents of pMibInEntry and pMibOutEntry are based on the transport and the routing protocol for which the MIB information is requested.

Transport	Routing Protocol	pMibInEntry	pMibOutEntry
PID_IP 0x000000 21	IPRTRMGR_PID 0x00002710	<a href="#">MIB_OPAQUE_QUERY (section 2.2.1.2.54)</a>	MIB_OPAQUE_QUERY (section 2.2.1.2.54)
PID_IP 0x000000 21	MS_IP_BOOTP 0x0000270F	<a href="#">IPBOOT MIB GET INPUT DATA (section 2.2.1.2.152)</a>	<a href="#">IPBOOTP MIB GET OUTPUT DATA (section 2.2.1.2.153)</a>
PID_IP 0x000000 21	MS_IP_NAT 0x81372715	<a href="#">IP NAT MIB QUERY (section 2.2.1.2.182)</a>	<b>IP_NAT_MIB_QUERY</b> (section 2.2.1.2.182)
PID_IP 0x000000 21	MS_IP_DNS_PROXY 0x81372713	<a href="#">IP_DNS_PROXY MIB QUERY (section 2.2.1.2.186)</a>	IP_DNS_PROXY_MIB_QUERY (section 2.2.1.2.186)
PID_IP 0x000000 21	MS_IP_DHCP_ALLOCA TOR 0x81372714	<a href="#">IP_AUTO_DHCP MIB QUERY (section 2.2.1.2.188)</a>	<b>IP_AUTO_DHCP_MIB_QUERY</b> (section 2.2.1.2.188)
PID_IP 0x000000 21	MS_IP_OSPF 0x0000000d	<a href="#">MIB_DA_MSG (section 2.2.1.2.190)</a>	<b>MIB_DA_MSG</b> (section 2.2.1.2.190)
PID_IP 0x000000 21	MS_IP_RIP 0x00000008	<a href="#">IPRIP MIB GET INPUT DATA (section 2.2.1.2.162)</a>	<a href="#">IPRIP MIB GET OUTPUT DATA (section 2.2.1.2.163)</a>
PID_IP 0x000000 21	MS_IP_IGMP 0x4137000a	<a href="#">IGMP MIB GET INPUT DATA (section 2.2.1.2.172)</a>	<a href="#">IGMP MIB GET OUTPUT DATA (section 2.2.1.2.173)</a>

Transport	Routing Protocol	pMibInEntry	pMibOutEntry
PID_IPV6 0x000000 57	MS_IPV6_DHCP 0x000003E7	<a href="#">DHCPV6R MIB GET INPUT DATA (section 2.2.1.2.161)</a>	<a href="#">DHCPV6R MIB GET OUTPUT DATA (section 2.2.1.2.157)</a>
PID_IPV6 0x000000 57	IPRTRMGR_PID 0x00002710	MIB_OPAQUE_QUERY (section 2.2.1.2.54)	MIB_OPAQUE_QUERY (section 2.2.1.2.54)
PID_IPX 0x000000 2B	IPX_PROTOCOL_BASE 0x0001FFFF	<a href="#">IPX MIB GET INPUT DATA (section 2.2.1.2.106)</a>	<b>IPX_MIB_GET_INPUT_DATA</b> (section 2.2.1.2.106)
PID_IPX 0x000000 2B	IPX_PROTOCOL_RIP 0x00020000	<a href="#">RIP MIB GET INPUT DATA (section 2.2.1.2.126)</a>	<b>RIP_MIB_GET_INPUT_DATA</b> (section 2.2.1.2.126)
PID_IPX 0x000000 2B	IPX_PROTOCOL_SAP 0x00020000	<a href="#">SAP MIB GET INPUT DATA (section 2.2.1.2.119)</a>	<b>SAP_MIB_GET_INPUT_DATA</b> (section 2.2.1.2.119)

#### 2.2.1.2.20 MIB\_IPDESTROW

The **MIB\_IPDESTROW** contains information about how a destination can be reached. In addition to the route information, this structure contains preference and view information. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPDESTROW {
    MIB_IPFORWARDROW ForwardRow;
    DWORD dwForwardPreference;
    DWORD dwForwardViewSet;
} MIB_IPDESTROW,
*PMIB_IPDESTROW;
```

**ForwardRow:** Contains the [MIB\\_IPFORWARDROW \(section 2.2.1.2.35\)](#) structure that contains the route information.

**dwForwardPreference:** This MUST be the preference value of the **ForwardRow**. While routing packets for two routes, if the prefix length is the same, the packet with the lower **dwForwardPreference** is chosen.

**dwForwardViewSet:** This MUST be the view information of the **ForwardRow**. This member describes the type of route, for example a multicast route. For more information, see the **dwRtInfoViewSet** member of [INTERFACE\\_ROUTE\\_INFO \(section 2.2.1.2.11\)](#).

#### 2.2.1.2.21 MIB\_IPDESTTABLE

The **MIB\_IPDESTTABLE** structure contains a table of [MIB\\_IPDESTROW \(section 2.2.1.2.20\)](#) structures containing the interface entries.



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumEntries																															
table (variable)																															
...																															

**dwNumEntries (4 bytes):** The number of interface entries in the table.

**table (variable):** An array of **MIB\_IPDESTROW** structures containing the interface entries.

#### 2.2.1.2.22 MIB\_ROUTESTATE

The **MIB\_ROUTESTATE** structure contains information as to whether the route needs to be added to the **forwarder** or not. Typically, only the **best routes** are added to the forwarder.

```
typedef struct _MIB_ROUTESTATE {
    BOOL bRoutesSetToStack;
} MIB_ROUTESTATE,
*PMIB_ROUTESTATE;
```

**bRoutesSetToStack:** This MUST be set to 0x00000001 to set routes to the forwarder.

#### 2.2.1.2.23 MIB\_BEST\_IF

The **MIB\_BEST\_IF** structure stores the index of the interface that has the best route to a particular destination IPv4 address.

```
typedef struct _MIB_BEST_IF {
    DWORD dwDestAddr;
    DWORD dwIfIndex;
} MIB_BEST_IF,
*PMIB_BEST_IF;
```

**dwDestAddr:** Specifies the IPv4 address of the destination address.

**dwIfIndex:** Specifies the index of the interface that has the best route to the destination address specified by the **dwDestAddr** member.

#### 2.2.1.2.24 MIB\_BOUNDARYROW

The **MIB\_BOUNDARYROW** structure contains the IPv4 group address value and mask for a multicast boundary. Whenever this structure is used, the **InfoType** of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff000b.

This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

This structure is used in the following methods:

- [RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)
- [RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)
- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```
typedef struct {
    DWORD dwGroupAddress;
    DWORD dwGroupMask;
} MIB_BOUNDARYROW,
*PMIB_BOUNDARYROW;
```

**dwGroupAddress:** The 32-bit integer representation of the IPv4 group address which, when combined with the corresponding value in **dwGroupMask**, identifies the group range for which the scoped boundary exists.

**Note** Scoped addresses must come from the range 239.\*.\*.\* as specified in [\[RFC2365\]](#).

**dwGroupMask:** The 32-bit integer representation of the IPv4 group address mask which, when combined with the corresponding value in **dwGroupAddress**, identifies the group range for which the scoped boundary exists.

#### 2.2.1.2.25 MIB\_ICMP

The **MIB\_ICMP** structure contains the ICMP statistics. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_ICMP {
    MIBICMPINFO stats;
} MIB_ICMP,
*PMIB_ICMP;
```

**stats:** An [MIBICMPINFO \(section 2.2.1.2.26\)](#) structure that contains the ICMP statistics.

#### 2.2.1.2.26 MIBICMPINFO

The **MIBICMPINFO** structure that contains the incoming and outgoing statistics for the ICMP.

This structure is used in [MIB\\_ICMP \(section 2.2.1.2.25\)](#).

```
typedef struct _MIBICMPINFO {
    MIBICMPSTATS icmpInStats;
    MIBICMPSTATS icmpOutStats;
} MIBICMPINFO;
```

**icmpInStats:** An [MIBICMPSTATS \(section 2.2.1.2.27\)](#) structure that contains the statistics for incoming ICMP messages.

**icmpOutStats:** An **MIBICMPSTATS** structure that contains the statistics for outgoing ICMP messages.

#### 2.2.1.2.27 MIBICMPSTATS

The **MIBICMPSTATS** structure that contains statistics for the ICMP messages on a particular computer. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#) and [MIBICMPINFO \(section 2.2.1.2.26\)](#).

```
typedef struct _MIBICMPSTATS {  
    DWORD dwMsgs;  
    DWORD dwErrors;  
    DWORD dwDestUnreachs;  
    DWORD dwTimeExcds;  
    DWORD dwParmProbs;  
    DWORD dwSrcQuenchs;  
    DWORD dwRedirects;  
    DWORD dwEchos;  
    DWORD dwEchoReps;  
    DWORD dwTimestamps;  
    DWORD dwTimestampReps;  
    DWORD dwAddrMasks;  
    DWORD dwAddrMaskReps;  
} MIBICMPSTATS;
```

**dwMsgs:** The number of ICMP messages received or sent.

**dwErrors:** The number of errors that occurred while sending or receiving ICMP messages.

**dwDestUnreachs:** The number of destination-unreachable messages received or sent. A destination-unreachable message is sent to the originating computer when the destination address in a datagram cannot be reached.

**dwTimeExcds:** The number of TTL-exceeded messages received or sent. A TTL-exceeded message is sent to the originating computer when a datagram is discarded because the number of routers it has passed through exceeds its TTL value.

**dwParmProbs:** The number of parameter-problem messages received or sent. A parameter-problem message is sent to the originating computer when a router or host detects an error in a datagram's IP header.

**dwSrcQuenchs:** The number of source quench messages received or sent. A source quench request is sent to a computer to request that it reduce its rate of packet transmission.

**dwRedirects:** The number of redirect messages received or sent. A redirect message is sent to the originating computer when a better route is discovered for a datagram sent by that computer.

**dwEchos:** The number of echo requests received or sent. An echo request causes the receiving computer to send an echo reply message back to the originating computer.

**dwEchoReps:** The number of echo replies received or sent. A computer sends an echo reply in response to receiving an echo request message.

**dwTimestamps:** The number of time stamp requests received or sent. A time stamp request causes the receiving computer to send a time stamp reply back to the originating computer.

**dwTimestampReps:** The number of time stamp replies received or sent. A computer sends a time stamp reply in response to receiving a time stamp request. Routers can use time stamp requests and replies to measure the transmission speed of datagrams on a network.

**dwAddrMasks:** The number of address mask requests received or sent. A computer sends an address mask request to determine the number of bits in the subnet mask for its local subnet.

**dwAddrMaskReps:** The number of address mask responses received or sent. A computer sends an address mask response in response to an address mask request.

#### 2.2.1.2.28 MIB\_IFNUMBER

The **MIB\_IFNUMBER** structure stores the number of interfaces on a particular computer.

```
typedef struct _MIB_IFNUMBER {
    DWORD dwValue;
} MIB_IFNUMBER,
*PMIB_IFNUMBER;
```

**dwValue:** The number of interfaces on the computer.

#### 2.2.1.2.29 MIB\_IFROW

The **MIB\_IFROW** structure stores information about a particular interface.

```
typedef struct _MIB_IFROW {
    WCHAR wszName[256];
    DWORD dwIndex;
    DWORD dwType;
    DWORD dwMtu;
    DWORD dwSpeed;
    DWORD dwPhysAddrLen;
    BYTE bPhysAddr[8];
    DWORD dwAdminStatus;
    DWORD dwOperStatus;
    DWORD dwLastChange;
    DWORD dwInOctets;
    DWORD dwInUcastPkts;
    DWORD dwInNUcastPkts;
    DWORD dwInDiscards;
    DWORD dwInErrors;
    DWORD dwInUnknownProtos;
    DWORD dwOutOctets;
    DWORD dwOutUcastPkts;
    DWORD dwOutNUcastPkts;
    DWORD dwOutDiscards;
    DWORD dwOutErrors;
    DWORD dwOutQLen;
    DWORD dwDescrLen;
    BYTE bDescr[256];
} MIB_IFROW;
```

**wszName:** A pointer to a Unicode string that contains the name of the interface.

**dwIndex:** The index that identifies the interface. This index value may change when a network adapter is disabled and then enabled, and is not persistent.

**dwType:** The interface type as defined by the Internet Assigned Names Authority (IANA) [\[IANAifType\]](#).

The following table lists common values for the interface type, although many other values are possible.

Value	Meaning
IF_TYPE_OTHER 0x00000001	Another type of network interface.
IF_TYPE_ETHERNET_CSMACD 0x00000006	An Ethernet network interface.
IF_TYPE_ISO88025_TOKENRING 0x00000009	A token ring network interface.
IF_TYPE_PPP 0x00000017	A PPP network interface.
IF_TYPE_SOFTWARE_LOOPBACK 0x00000018	A software loopback network interface.
IF_TYPE_ATM 0x00000027	An ATM network interface.
IF_TYPE_IEEE80211 0x00000047	An IEEE 802.11 wireless network interface.
IF_TYPE_TUNNEL 0x00000083	A tunnel type encapsulation network interface.
IF_TYPE_IEEE1394 0x00000090	An IEEE 1394 (FireWire) high-performance serial bus network interface.

**dwMtu:** The maximum transmission unit (MTU) size in bytes.

**dwSpeed:** The speed of the interface in bits per second.

**dwPhysAddrLen:** The length, in bytes, of the physical address specified by the **bPhysAddr** member.

**bPhysAddr:** The physical address of the adapter for this interface.

**dwAdminStatus:** The administrative status of the interface. It can be either enabled or disabled.

**dwOperStatus:** The operational status of the interface.

This member can be one of the following values.

Value	Meaning
IF_OPER_STATUS_NON_OPERATIONAL	LAN adapter has been disabled, for example, because of

Value	Meaning
0x00000000	an address conflict.
IF_OPER_STATUS_UNREACHABLE 0x00000001	WAN adapter that is not connected.
IF_OPER_STATUS_DISCONNECTED 0x00000002	For LAN adapters: network cable disconnected. For WAN adapters: no carrier.
IF_OPER_STATUS_CONNECTING 0x00000003	WAN adapter that is in the process of connecting.
IF_OPER_STATUS_CONNECTED 0x00000004	WAN adapter that is connected to a remote peer.
IF_OPER_STATUS_OPERATIONAL 0x00000005	Default status for LAN adapters.

**dwLastChange:** The length of time, in hundredths of seconds, starting from the last computer restart, when the interface entered its current operational state. [<31>](#)

**dwInOctets:** The number of octets of data received through this interface.

**dwInUcastPkts:** The number of unicast packets received through this interface.

**dwInNUcastPkts:** The number of nonunicast packets received through this interface. **Broadcast** and multicast packets are included.

**dwInDiscards:** The number of incoming packets that were discarded even though they did not have errors.

**dwInErrors:** The number of incoming packets that were discarded because of errors.

**dwInUnknownProtos:** The number of incoming packets that were discarded because the protocol was unknown.

**dwOutOctets:** The number of octets of data sent through this interface.

**dwOutUcastPkts:** The number of unicast packets sent through this interface.

**dwOutNUcastPkts:** The number of nonunicast packets sent through this interface. Broadcast and multicast packets are included.

**dwOutDiscards:** The number of outgoing packets that were discarded even though they did not have errors.

**dwOutErrors:** The number of outgoing packets that were discarded because of errors.

**dwOutQLen:** The transmit queue length. This field is not currently used.

**dwDescrLen:** The length, in bytes, of the **bDescr** member.

**bDescr:** A null-terminated ASCII string containing the description of the interface.

### 2.2.1.2.30 MIB\_IFSTATUS

The **MIB\_IFSTATUS** structure stores status information for a particular interface.

```
typedef struct _MIB_IFSTATUS {
    DWORD dwIfIndex;
    DWORD dwAdminStatus;
    DWORD dwOperationalStatus;
    BOOL bMHbeatActive;
    BOOL bMHbeatAlive;
} MIB_IFSTATUS,
*PMIB_IFSTATUS;
```

- dwIfIndex:** The index that identifies the interface.
- dwAdminStatus:** The administrative status of the interface, that is, whether the interface is administratively enabled or disabled.
- dwOperationalStatus:** The operational status of the interface. This member can be one of the values defined in the [ROUTER CONNECTION STATE \(section 2.2.1.1.2\)](#).
- bMHbeatActive:** Specifies whether multicast heartbeat detection is enabled. A value of TRUE indicates that heartbeat detection is enabled. A value of FALSE indicates that heartbeat detection is disabled.

Value	Meaning
TRUE	Heartbeat detection is enabled.
FALSE	Heartbeat detection is disabled.

**bMHbeatAlive:** Specifies whether the multicast heartbeat dead interval has been exceeded. A value of FALSE indicates that the interval has been exceeded. A value of TRUE indicates that the interval has not been exceeded.

Value	Meaning
TRUE	Heartbeat dead interval has not been exceeded.
FALSE	Heartbeat dead interval has been exceeded.

2.2.1.2.31 MIB\_IFTABLE

The **MIB\_IFTABLE** structure contains a table of interface entries. This structure is used in [MIB OPAQUE INFO \(section 2.2.1.2.53\)](#).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumEntries																															
table (variable)																															
...																															

**dwNumEntries (4 bytes):** The number of interface entries in the table.

**table (variable):** An array of [MIB\\_IFROW \(section 2.2.1.2.29\)](#) structures containing interface entries.

### 2.2.1.2.32 MIB\_IPADDRROW

The **MIB\_IPADDRROW** specifies information for a particular IPv4 address. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPADDRROW {
    DWORD dwAddr;
    DWORD dwIndex;
    DWORD dwMask;
    DWORD dwBCastAddr;
    DWORD dwReasmSize;
    unsigned short unused1;
    unsigned short wType;
} MIB_IPADDRROW,
*PMIB_IPADDRROW;
```

**dwAddr:** The IPv4 address.

**dwIndex:** The index of the interface associated with this IPv4 address.

**dwMask:** The subnet mask for the IPv4 address. See [RFC950](#).

**dwBCastAddr:** The broadcast address. A broadcast address is typically the IPv4 address with the host portion set to either all zeros or all ones.

**dwReasmSize:** The maximum reassembly size for received datagrams.

**unused1:** This member is reserved and SHOULD be set to 0.

**wType:** The address type or state. [<32>](#)

Value	Meaning
MIB_IPADDR_PRIMARY 0x0001	Primary IP address.
MIB_IPADDR_DYNAMIC 0x0004	Dynamic IP address.
MIB_IPADDR_DISCONNECTED 0x0008	Address is on disconnected interface.
MIB_IPADDR_DELETED 0x0040	Address is being deleted.
MIB_IPADDR_TRANSIENT 0x0080	Transient address.



### 2.2.1.2.33 MIB\_IPADDRTABLE

The **MIB\_IPADDRTABLE** structure contains a table of IPv4 address entries. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumEntries																															
table (variable)																															
...																															

**dwNumEntries (4 bytes):** The number of IPv4 address entries in the table.

**table (variable):** A pointer to a table of IPv4 address entries implemented as an array of [MIB\\_IPADDRROW \(section 2.2.1.2.32\)](#) structures.

### 2.2.1.2.34 MIB\_IPFORWARDNUMBER

The **MIB\_IPFORWARDNUMBER** structure stores the number of routes in a particular IP routing table.

```
typedef struct _MIB_IPFORWARDNUMBER {
    DWORD dwValue;
} MIB_IPFORWARDNUMBER,
*PMIB_IPFORWARDNUMBER;
```

**dwValue:** Specifies the number of routes in the IP routing table.

### 2.2.1.2.35 MIB\_IPFORWARDROW

The **MIB\_IPFORWARDROW** structure contains information that describes an IPv4 network route. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPFORWARDROW {
    DWORD dwForwardDest;
    DWORD dwForwardMask;
    DWORD dwForwardPolicy;
    DWORD dwForwardNextHop;
    DWORD dwForwardIfIndex;
    union {
        DWORD dwForwardType;
        MIB_IPFORWARD_TYPE ForwardType;
    };
    union {
        DWORD dwForwardProto;
        MIB_IPFORWARD_PROTO ForwardProto;
    };
    DWORD dwForwardAge;
    DWORD dwForwardNextHopAS;
    DWORD dwForwardMetric1;
```

```

    DWORD dwForwardMetric2;
    DWORD dwForwardMetric3;
    DWORD dwForwardMetric4;
    DWORD dwForwardMetric5;
} MIB_IPFORWARDROW,
*PMIB_IPFORWARDROW;

```

**dwForwardDest:** The destination IPv4 address of the route. An entry with an IPv4 address of 0.0.0.0 is considered a default route. This member MUST NOT be set to a multicast (class D) IPv4 address.

**dwForwardMask:** The IPv4 subnet mask to be logically ANDed with the destination IPv4 address before being compared to the value in the **dwForwardDest** member; see [\[RFC950\]](#).

**dwForwardPolicy:** The set of conditions that would cause the selection of a multipath route (the set of next hops for a given destination). This member is typically in IP TOS format. The encoding of this member is specified in [\[RFC1354\]](#).

**dwForwardNextHop:** For remote routes, the IPv4 address of the next system in the route. Otherwise, this member SHOULD be an IPv4 address of 0x00000000.

**dwForwardIfIndex:** The index of the local interface through which the next hop of this route is reachable. This MUST be an interface index of one of the interfaces on RRAS.

**dwForwardType:** The route type as specified in [\[RFC1354\]](#). The enum [MIB\\_IPFORWARD\\_TYPE \(section 2.2.1.1.8\)](#) describes the possible values for this member. In addition, **dwForwardType** can also be IP\_PRIORITY\_MAX\_METRIC (0x000000ff) or IP\_PRIORITY\_DEFAULT\_METRIC (0x0000007f).

**ForwardType:** The route type as specified in [\[RFC1354\]](#).<33>

**dwForwardProto:** The protocol or routing mechanism that generated the route. It can take one of the values specified in [\[RFC1354\]](#). The enum [MIB\\_IPFORWARD\\_PROTO \(section 2.2.1.1.9\)](#) describes the possible values for this member.

**ForwardProto:** The protocol or routing mechanism that generated the route.<34>

**dwForwardAge:** The number of seconds since the route was added or modified in the network routing table. The **dwForwardAge** member is also used if the RRAS server is running for routes of type PROTO\_IP\_NETMGMT as defined on the Protocol Identifiers reference page. When **dwForwardAge** is set to INFINITE (-1) when running the RRAS server, the route will not be removed based on a time-out value.

**dwForwardNextHopAS:** The autonomous system number of the next hop. When this member is unknown or not relevant to the protocol or routing mechanism specified in **dwForwardProto**, this value SHOULD be set to 0. This value is documented in [\[RFC1354\]](#).

**dwForwardMetric1:** The primary routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwForwardProto** member. If this metric is not used, its value SHOULD be set to MIB\_IPROUTE\_METRIC\_UNUSED (-1). This value is documented in [\[RFC1354\]](#).

**dwForwardMetric2:** An alternate routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwForwardProto** member. If

this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

**dwForwardMetric3:** An alternate routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwForwardProto** member. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

**dwForwardMetric4:** An alternate routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwForwardProto** member. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

**dwForwardMetric5:** An alternate routing metric value for this route. The semantics of this metric are determined by the routing protocol specified in the **dwForwardProto** member. If this metric is not used, its value SHOULD be set to -1. This value is documented in [\[RFC1354\]](#).

### 2.2.1.2.36 MIB\_IPFORWARDTABLE

The **MIB\_IPFORWARDTABLE** structure contains a table of the IP route entries.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumEntries																															
table (variable)																															
...																															
reserved																															
...																															

**dwNumEntries (4 bytes):** Specifies the number of route entries in the table.

**table (variable):** Pointer to a table of route entries implemented as an array of [MIB\\_IPFORWARDROW \(section 2.2.1.2.35\)](#) structures.

**reserved (8 bytes):** An array of 8 bytes that SHOULD be set to 0 and ignored on receipt.

### 2.2.1.2.37 MIB\_IPMCAST\_BOUNDARY

The **MIB\_IPMCAST\_BOUNDARY** structure contains a router's scoped IPv4 multicast address boundaries. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct {
    DWORD dwIfIndex;
    DWORD dwGroupAddress;
    DWORD dwGroupMask;
    DWORD dwStatus;
} MIB_IPMCAST_BOUNDARY,
```

\*PMIB\_IPMCAST\_BOUNDARY;

**dwIfIndex:** The index value for the interface that applies to this boundary. Packets with a destination address in the associated address/mask range are not forwarded with this interface.

**dwGroupAddress:** The 32-bit integer representation of the IPv4 group address which, when combined with the corresponding value in **dwGroupMask**, identifies the group range for which the scoped boundary exists.

**Note** Scoped addresses must come from the range 239.\*.\*.\* as specified in [\[RFC2365\]](#).

**dwGroupMask:** The 32-bit integer representation of the IPv4 group address mask which, when combined with the corresponding value in **dwGroupAddress**, identifies the group range for which the scoped boundary exists.

**dwStatus:** A status value that describes the current status of this entry in a multicast forwarding entry (MFE) boundary table.

Value	Meaning
0x00000001	The entry has active status.
0x00000002	The entry has notInService status.
0x00000003	The entry has notReady status.
0x00000004	The entry has createAndGo status.
0x00000005	The entry has createAndWait status.
0x00000006	The entry has destroy status.

2.2.1.2.38 MIB\_IPMCAST\_BOUNDARY\_TABLE

The **MIB\_IPMCAST\_BOUNDARY\_TABLE** structure contains a list of a router's scoped IPv4 multicast address boundaries. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumEntries																															
table (variable)																															
...																															

**dwNumEntries (4 bytes):** The number of [MIB\\_IPMCAST\\_BOUNDARY \(section 2.2.1.2.37\)](#) structures listed in **table**.

**table (variable):** An array of **MIB\_IPMCAST\_BOUNDARY** structures that collectively define the set of scoped IPv4 multicast address boundaries on a router.

#### 2.2.1.2.39 MIB\_IPMCAST\_GLOBAL

The **MIB\_IPMCAST\_GLOBAL** structure stores global information for IP multicast on a particular computer.

```
typedef struct _MIB_IPMCAST_GLOBAL {
    DWORD dwEnable;
} MIB_IPMCAST_GLOBAL,
*PMIB_IPMCAST_GLOBAL;
```

**dwEnable:** Specifies whether or not IP multicast is enabled on the computer. This value is set to 1 if IP multicast is enabled on the computer and is set to 2 if IP multicast is not enabled on the computer.

#### 2.2.1.2.40 MIB\_IPMCAST\_IF\_ENTRY

The **MIB\_IPMCAST\_IF\_ENTRY** structure stores information about an IP multicast interface.

```
typedef struct _MIB_IPMCAST_IF_ENTRY {
    DWORD dwIfIndex;
    DWORD dwTtl;
    DWORD dwProtocol;
    DWORD dwRateLimit;
    ULONG ulInMcastOctets;
    ULONG ulOutMcastOctets;
} MIB_IPMCAST_IF_ENTRY,
*PMIB_IPMCAST_IF_ENTRY;
```

**dwIfIndex:** The index of this interface.

**dwTtl:** The TTL value for this interface.

**dwProtocol:** The multicast routing protocol that owns this interface.

**dwRateLimit:** The rate limit of this interface.

**ulInMcastOctets:** The number of octets of multicast data received through this interface.

**ulOutMcastOctets:** The number of octets of multicast data sent through this interface.

#### 2.2.1.2.41 MIB\_IPMCAST\_IF\_TABLE

The **MIB\_IPMCAST\_IF\_TABLE** structure contains a table of IP multicast interface entries. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPMCAST_IF_TABLE {
    DWORD dwNumEntries;
    MIB_IPMCAST_IF_ENTRY table[dwNumEntries];
} MIB_IPMCAST_IF_TABLE,
*PMIB_IPMCAST_IF_TABLE;
```

**dwNumEntries:** Specifies the number of interface entries in the table.

**table:** A pointer to a table of interface entries implemented as an array of [MIB\\_IPMCAST\\_IF\\_ENTRY \(section 2.2.1.2.40\)](#) structures.

#### 2.2.1.2.42 MIB\_IPMCAST\_MFE

The **MIB\_IPMCAST\_MFE** structure stores the information for an IP multicast forwarding entry (MFE). This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPMCAST_MFE {
    DWORD dwGroup;
    DWORD dwSource;
    DWORD dwSrcMask;
    DWORD dwUpStrmNgbr;
    DWORD dwInIfIndex;
    DWORD dwInIfProtocol;
    DWORD dwRouteProtocol;
    DWORD dwRouteNetwork;
    DWORD dwRouteMask;
    ULONG ulUpTime;
    ULONG ulExpiryTime;
    ULONG ulTimeOut;
    ULONG ulNumOutIf;
    DWORD fFlags;
    DWORD dwReserved;
    MIB_IPMCAST_OIF rgmioOutInfo[ulNumOutIf];
} MIB_IPMCAST_MFE,
*PMIB_IPMCAST_MFE;
```

**dwGroup:** The range of IPv4 multicast groups for this MFE. A value of zero indicates a wildcard group.

**dwSource:** The range of IPv4 source addresses for this MFE. A value of zero indicates a wildcard source.

**dwSrcMask:** The IPv4 subnet mask that corresponds to **dwSource**. The **dwSource** and **dwSrcMask** members are used together to define a range of sources.

**dwUpStrmNgbr:** The upstream neighbor that is related to this MFE.

**dwInIfIndex:** The index of the interface to which this MFE is related.

**dwInIfProtocol:** The routing protocol that owns the incoming interface to which this MFE is related.

**dwRouteProtocol:** The protocol that created the route. This is the enum [MIB\\_IPFORWARD\\_PROTO \(section 2.2.1.1.9\)](#).

**dwRouteNetwork:** The IPv4 address associated with the route referred to by **dwRouteProtocol**.

**dwRouteMask:** The IPv4 mask associated with the route referred to by **dwRouteProtocol**.

**ulUpTime:** The time, in seconds, that this MFE has been valid. This value starts from zero and is incremented until it reaches the **ulTimeOut** value, at which time the MFE is deleted.

**ulExpiryTime:** The time, in seconds, that remains before the MFE expires and is deleted. This value starts from **ulTimeOut** and is decremented until it reaches zero, at which time the MFE is deleted.

**ulTimeOut:** The total length of time, in seconds, that this MFE remains valid. After the time-out value is exceeded, the MFE is deleted.

**ulNumOutIf:** The number of outgoing interfaces that are associated with this MFE.

**fFlags:** Reserved. This member SHOULD be NULL.

**dwReserved:** Reserved. This member SHOULD be NULL.

**rgmioOutInfo:** A pointer to a table of outgoing interface statistics that are implemented as an array of [MIB\\_IPMCAST\\_OIF \(section 2.2.1.2.43\)](#) structures.

2.2.1.2.43 MIB\_IPMCAST\_OIF

The **MIB\_IPMCAST\_OIF** structure stores the information required to send an outgoing IP multicast packet.

```
typedef struct _MIB_IPMCAST_OIF {
    DWORD dwOutIfIndex;
    DWORD dwNextHopAddr;
    PVOID pvReserved;
    DWORD dwReserved;
} MIB_IPMCAST_OIF,
*PMIB_IPMCAST_OIF;
```

**dwOutIfIndex:** The index of the interface on which to send the outgoing IP multicast packet.

**dwNextHopAddr:** The destination address for the outgoing IPv4 multicast packet.

**pvReserved:** Reserved. This member MUST be NULL.

**dwReserved:** Reserved. This member MUST be zero.

2.2.1.2.44 MIB\_IPMCAST\_MFE\_STATS

The **MIB\_IPMCAST\_MFE\_STATS** structure stores the statistics associated with an MFE.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwGroup																															
dwSource																															
dwSrcMask																															
dwUpStrmNgbr																															

dwInIfIndex
dwInIfProtocol
dwRouteProtocol
dwRouteNetwork
dwRouteMask
ulUpTime
ulExpiryTime
ulNumOutIf
ulInPkts
ulInOctets
ulPktsDifferentIf
ulQueueOverflow
rgmiosOutStats (variable)
...

**dwGroup (4 bytes):** The multicast group for this MFE. A value of zero indicates a wildcard group.

**dwSource (4 bytes):** The range of source addresses for this MFE. A value of zero indicates a wildcard source.

**dwSrcMask (4 bytes):** The IPv4 subnet mask that corresponds to the **dwSource**. The **dwSource** and the **dwSrcMask** members are used together to define a range of sources.

**dwUpStrmNgbr (4 bytes):** The upstream neighbor that is related to this MFE.

**dwInIfIndex (4 bytes):** The index of the incoming interface that is related to this MFE.

**dwInIfProtocol (4 bytes):** The routing protocol that owns the incoming interface that is related to this MFE.

**dwRouteProtocol (4 bytes):** The protocol that created the route. It is the enum [MIB\\_IPFORWARD\\_PROTO \(section 2.2.1.1.9\)](#).

**dwRouteNetwork (4 bytes):** The address associated with the route referred to by the **dwRouteProtocol**.



**dwRouteMask (4 bytes):** The mask associated with the route referred to by the **dwRouteProtocol**.

**ulUpTime (4 bytes):** The time, in 100ths of a second, since the MFE was created.

**ulExpiryTime (4 bytes):** The time, in 100ths of a second, until the MFE will be deleted. A value of zero is specified if the MFE is not subject to aging requirements.

**ulNumOutIf (4 bytes):** The number of interfaces in the outgoing interface list for this MFE.

**ulInPkts (4 bytes):** The number of packets that have been forwarded that matched this MFE.

**ulInOctets (4 bytes):** The number of octets of data forwarded that match this MFE.

**ulPktsDifferentIf (4 bytes):** The number of packets matching this MFE that were dropped due to an incoming interface check.

**ulQueueOverflow (4 bytes):** The number of packets matching this MFE that were dropped due to a queue overflow. There is one queue per MFE.

**rgmiosOutStats (variable):** A pointer to a table of outgoing interface statistics that are implemented as an array of [MIB\\_IPMCAST\\_OIF\\_STATS \(section 2.2.1.2.45\)](#) structures. The number of entries in the table is specified by the value of the **ulNumOutIf** member.

#### 2.2.1.2.45 MIB\_IPMCAST\_OIF\_STATS

The **MIB\_IPMCAST\_OIF\_STATS** structure stores the statistics that are associated with an outgoing multicast interface.

```
typedef struct _MIB_IPMCAST_OIF_STATS {  
    DWORD dwOutIfIndex;  
    DWORD dwNextHopAddr;  
    PVOID pvDialContext;  
    ULONG ulTtlTooLow;  
    ULONG ulFragNeeded;  
    ULONG ulOutPackets;  
    ULONG ulOutDiscards;  
} MIB_IPMCAST_OIF_STATS,  
*PMIB_IPMCAST_OIF_STATS;
```

**dwOutIfIndex:** Specifies the outgoing interface to which these statistics are related.

**dwNextHopAddr:** Specifies the address of the next hop that corresponds to **dwOutIfIndex**.

The **dwOutIfIndex** and **dwNextHopIPAddr** members uniquely identify a next hop on point-to-multipoint interfaces, where one interface connects to multiple networks. Examples of point-to-multipoint interfaces include non-broadcast multiple-access (NBMA) interfaces, and the internal interface on which all dial-up clients connect. For Ethernet and other broadcast interfaces, specify zero. Also specify zero for point-to-point interfaces, which are identified by only **dwOutIfIndex**.

**pvDialContext:** Reserved. This member MUST be NULL.

**ulTtlTooLow:** Specifies the number of packets on this outgoing interface that were discarded because the packet's TTL value was too low.

**ulFragNeeded:** Specifies the number of packets that required fragmentation when they were forwarded on this interface.

**ulOutPackets:** Specifies the number of packets that were forwarded out of this interface.

**ulOutDiscards:** Specifies the number of packets that were discarded on this interface.

#### 2.2.1.2.46 MIB\_IPMCAST\_SCOPE

The **MIB\_IPMCAST\_SCOPE** structure contains a multicast scope name and the associated IPv4 multicast group address and mask that define the scope. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct {
    DWORD dwGroupAddress;
    DWORD dwGroupMask;
    WCHAR snNameBuffer[256];
    DWORD dwStatus;
    BYTE reserved[492];
} MIB_IPMCAST_SCOPE,
*PMIB_IPMCAST_SCOPE;
```

**dwGroupAddress:** A 32-bit integer representation of the IPv4 group address which, when combined with the corresponding value in **dwGroupMask**, identifies the group range for which the multicast scope exists.

**Note** Scoped addresses must come from the range 239.0.0.0 to 239.255.255.255 as specified in [RFC2365](#).

**dwGroupMask:** A 32-bit integer representation of the IPv4 group address mask which, when combined with the corresponding value in **dwGroupAddress**, identifies the group range for which the multicast scope exists.

**snNameBuffer:** A Unicode string, suitable for display to multicast application users, that contains the text name associated with the multicast scope.

If no name is specified, the default name is the string representation of the scoped address in **dwGroupAddress** with the address and mask length appended and separated by a backslash "/" character, of the form "239.\*.\*.\*x/y", where **x** is the address length and **y** is the mask length.

**dwStatus:** A status value that describes the current status of this row in an MFE scope table.

Value	Meaning
0x00000001	Row has active status.
0x00000002	Row has notInService status.
0x00000003	Row has notReady status.
0x00000004	Row has createAndGo status.
0x00000005	Row has createAndWait status.

Value	Meaning
0x00000006	Row has destroy status.

**reserved:** An array of 492 bytes that SHOULD be set to 0 and ignored on receive.

#### 2.2.1.2.47 MIB\_IPNETROW

The **MIB\_IPNETROW** structure contains information for an Address Resolution Protocol (ARP) table entry for an IPv4 address. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPNETROW {
    DWORD dwIndex;
    DWORD dwPhysAddrLen;
    BYTE bPhysAddr[8];
    DWORD dwAddr;
    DWORD dwType;
} MIB_IPNETROW,
*PMIB_IPNETROW;
```

**dwIndex:** This MUST be the interface index of an adapter.

**dwPhysAddrLen:** The length, in bytes, of the physical address.

**bPhysAddr:** The physical address.

**dwAddr:** The IPv4 address.

**dwType:** The type of ARP entry. This type MUST be one of the following values.

Value	Meaning
0x00000004	Static
0x00000003	Dynamic
0x00000002	Invalid
0x00000001	Other

#### 2.2.1.2.48 MIB\_IPNETTABLE

The **MIB\_IPNETTABLE** structure contains a table of ARP entries for IPv4 addresses.

```
typedef struct _MIB_IPNETTABLE {
    DWORD dwNumEntries;
    MIB_IPNETROW table[dwNumEntries];
    BYTE reserved[8];
} MIB_IPNETTABLE,
*PMIB_IPNETTABLE;
```

**dwNumEntries:** The number of ARP entries in the table.

**table:** A pointer to a table of ARP entries implemented as an array of [MIB\\_IPNETROW \(section 2.2.1.2.47\)](#) structures.

**reserved:** An array of 8 bytes that SHOULD be set to 0 and ignored on receipt.

#### 2.2.1.2.49 MIB\_IPSTATS

The **MIB\_IPSTATS** structure stores information about the IP protocol running on a particular computer. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_IPSTATS {
    union {
        DWORD dwForwarding;
        MIB_IPSTATS_FORWARDING Forwarding;
    };
    DWORD dwDefaultTTL;
    DWORD dwInReceives;
    DWORD dwInHdrErrors;
    DWORD dwInAddrErrors;
    DWORD dwForwDatagrams;
    DWORD dwInUnknownProtos;
    DWORD dwInDiscards;
    DWORD dwInDelivers;
    DWORD dwOutRequests;
    DWORD dwRoutingDiscards;
    DWORD dwOutDiscards;
    DWORD dwOutNoRoutes;
    DWORD dwReasmTimeout;
    DWORD dwReasmReqds;
    DWORD dwReasmOks;
    DWORD dwReasmFails;
    DWORD dwFragOks;
    DWORD dwFragFails;
    DWORD dwFragCreates;
    DWORD dwNumIf;
    DWORD dwNumAddr;
    DWORD dwNumRoutes;
} MIB_IPSTATS,
*PMIB_IPSTATS;
```

**dwForwarding:** Specifies whether IP forwarding is enabled or disabled. This value MUST be 0xffffffff or one of the following values. If set to 0xffffffff, [RMIBEntrySet](#) does not change the current value of **dwForwarding**.

Value	Meaning
0x00000001	IP Forwarding enabled.
0x00000002	IP Forwarding not enabled.

**Forwarding:** Specifies whether IP forwarding is enabled or disabled. [<35>](#)

**dwDefaultTTL:** The default initial TTL for datagrams originating on a particular computer. This value MUST be 0xffffffff or a value less than or equal to 255.

**dwInReceives:** The number of datagrams received. This is a read-only field and MUST be ignored while writing.

**dwInHdrErrors:** The number of datagrams received that have header errors. This is a read-only field and MUST be ignored while writing.

**dwInAddrErrors:** The number of datagrams received that have address errors. This is a read-only field and MUST be ignored while writing.

**dwForwDatagrams:** The number of datagrams forwarded. This is a read-only field and MUST be ignored while writing.

**dwInUnknownProtos:** The number of datagrams received that have an unknown protocol. This is a read-only field and MUST be ignored while writing.

**dwInDiscards:** The number of received datagrams discarded. This is a read-only field and MUST be ignored while writing.

**dwInDelivers:** The number of received datagrams delivered. This is a read-only field and MUST be ignored while writing.

**dwOutRequests:** The number of outgoing datagrams that the IP is requested to transmit. This number does not include forwarded datagrams. This is a read-only field and MUST be ignored while writing.

**dwRoutingDiscards:** The number of outgoing datagrams discarded. This is a read-only field and MUST be ignored while writing.

**dwOutDiscards:** The number of transmitted datagrams to be discarded. This is a read-only field and MUST be ignored while writing.

**dwOutNoRoutes:** The number of datagrams for which this computer did not have a route to the destination IP address. These datagrams were discarded. This is a read-only field and MUST be ignored while writing.

**dwReasmTimeout:** The amount of time allowed for all pieces of a fragmented datagram to arrive. If all pieces do not arrive within this time, the datagram is discarded. This is a read-only field and MUST be ignored while writing.

**dwReasmReqds:** The number of datagrams that require reassembly. This is a read-only field and MUST be ignored while writing.

**dwReasmOks:** The number of datagrams that were successfully reassembled. This is a read-only field and MUST be ignored while writing.

**dwReasmFails:** The number of datagrams that cannot be reassembled. This is a read-only field and MUST be ignored while writing.

**dwFragOks:** The number of datagrams that were fragmented successfully. This is a read-only field and MUST be ignored while writing.

**dwFragFails:** The number of datagrams that have not been fragmented because the IP header specifies no fragmentation. These datagrams are discarded. This is a read-only field and MUST be ignored while writing.

**dwFragCreates:** The number of fragments created. This is a read-only field and MUST be ignored while writing.

**dwNumIf:** The number of interfaces. This is a read-only field and MUST be ignored while writing.

**dwNumAddr:** The number of IP addresses associated with this computer. This is a read-only field and MUST be ignored while writing.

**dwNumRoutes:** The number of routes in the IP routing table. This is a read-only field and MUST be ignored while writing.

#### 2.2.1.2.50 MIB\_MCAST\_LIMIT\_ROW

The **MIB\_MCAST\_LIMIT\_ROW** structure contains the configurable limit information from a corresponding [MIB\\_IPMCAST\\_IF\\_ENTRY \(section 2.2.1.2.40\)](#) structure. Whenever this structure is used, the **InfoType** of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) MUST be 0xffff000e.

This structure is used in the following methods.

- [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)
- [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)
- [RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```
typedef struct {
    DWORD dwTtl;
    DWORD dwRateLimit;
} MIB_MCAST_LIMIT_ROW,
*PMIB_MCAST_LIMIT_ROW;
```

**dwTtl:** The TTL value for a multicast interface.

**dwRateLimit:** The rate limit for a multicast interface. This MUST be set to 0.

#### 2.2.1.2.51 MIB\_MFE\_STATS\_TABLE

The **MIB\_MFE\_STATS\_TABLE** structure stores statistics for a group of MFEs. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#) and in the following methods.

- [RMIBEntryGet \(section 3.1.4.30\)](#)
- [RMIBEntryGetFirst \(section 3.1.4.31\)](#)
- [RMIBEntryGetNext \(section 3.1.4.32\)](#)

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
dwNumEntries																															
table (variable)																															
...																															

**dwNumEntries (4 bytes):** The number of MFEs in the table.

**table (variable):** A pointer to a table of MFEs that are implemented as an array of [MIB\\_IPMCAST\\_MFE\\_STATS \(section 2.2.1.2.44\)](#) structures.

#### 2.2.1.2.52 MIB\_MFE\_TABLE

The **MIB\_MFE\_TABLE** structure contains a table of MFEs. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwNumEntries																															
table (variable)																															
...																															

**dwNumEntries (4 bytes):** The number of MFEs in the table.

**table (variable):** A pointer to a table of MFEs implemented as an array of [MIB\\_IPMCAST\\_MFE \(section 2.2.1.2.42\)](#) structures.

#### 2.2.1.2.53 MIB\_OPAQUE\_INFO

The **MIB\_OPAQUE\_INFO** structure contains information related to an MIB entry. This structure is used to handle MIB data in MIB methods such as the following:

- [RMIBEntryCreate \(section 3.1.4.27\)](#)
- [RMIBEntrySet \(section 3.1.4.29\)](#)
- [RMIBEntryGet \(section 3.1.4.30\)](#)
- [RMIBEntryGetFirst \(section 3.1.4.31\)](#)
- [RMIBEntryGetNext \(section 3.1.4.32\)](#)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwId																															
ullAlign																															
rgbyData																															

**dwId (4 bytes):** MIB ID for the type of information being submitted or returned.

IPX does not use this structure.

For IP transport, the MIB ID MUST be one of the following.

<b>dwId Value</b>	<b>Meaning</b>	<b>Structure to be pointed to by rgbyData.</b>
0x00000000 IF_NUMBER	Information about number of interfaces on the server.	<a href="#">MIB_IFNUMBER (section 2.2.1.2.28)</a>
0x00000001 IF_TABLE	Table of interface entries.	<a href="#">MIB_IFTABLE (section 2.2.1.2.31)</a>
0x00000002 IF_ROW	Information about a particular interface.	<a href="#">MIB_IFROW (section 2.2.1.2.29)</a>
0x00000003 IP_STATS	Information about the IP protocol.	<a href="#">MIB_IPSTATS (section 2.2.1.2.49)</a>
0x00000004 IP_ADDRTABLE	Table of IPv4 address entries.	<a href="#">MIB_IPADDRTABLE (section 2.2.1.2.33)</a>
0x00000005 IP_ADDRROW	Information for a particular IPv4 address.	<a href="#">MIB_IPADDRROW (section 2.2.1.2.32)</a>
0x00000006 IP_FORWARDNUMBER	Information about number of routes in a particular IP routing table.	<a href="#">MIB_IPFORWARDNUMBER (section 2.2.1.2.34)</a>
0x00000007 IP_FORWARDTABLE	Table of IPv4 route entries.	<a href="#">MIB_IPFORWARDTABLE (section 2.2.1.2.36)</a>
0x00000008 IP_FORWARDROW	Information that describes an IPv4/IPv6 network route.	<a href="#">MIB_IPFORWARDROW (section 2.2.1.2.35)</a> for IPv4, <b>INTERFACE ROUTE ENTRY (section 2.2.1.2.181)</b> for IPv6 based on the transport
0x00000009 IP_NETTABLE	Table of ARP entries for IPv4 addresses.	<a href="#">MIB_IPNETTABLE (section 2.2.1.2.48)</a>
0x0000000a IP_NETROW	Information about an ARP table entry for an IPv4 address.	<a href="#">MIB_IPNETROW (section 2.2.1.2.47)</a>
0x0000000b ICMP_STATS	Statistics for ICMP messages on a particular computer.	<a href="#">MIB_ICMP (section 2.2.1.2.25)</a>
0x0000000c TCP_STATS	Statistics for the TCP protocol running on the local computer.	<a href="#">MIB_TCPSTATS (section 2.2.1.2.57)</a>
0x0000000d TCP_TABLE	Table of IPv4 TCP connections.	<a href="#">MIB_TCPTABLE (section 2.2.1.2.58)</a>



<b>dwId Value</b>	<b>Meaning</b>	<b>Structure to be pointed to by rgbyData.</b>
0x0000000e TCP_ROW	Information for an IPv4 TCP connection.	<a href="#">MIB_TCPROW (section 2.2.1.2.56)</a>
0x0000000f UDP_STATS	Statistics for the UDP running on the local computer.	<a href="#">MIB_UDPSTATS (section 2.2.1.2.60)</a>
0x00000010 UDP_TABLE	Table of address information for sending and receiving UDP datagrams.	<a href="#">MIB_UDPTABLE (section 2.2.1.2.61)</a>
0x00000011 UDP_ROW	Information for a UDP session.	<a href="#">MIB_UDPROW (section 2.2.1.2.59)</a>
0x00000012 MCAST_MFE	Information for an IP multicast forwarding entry.	<a href="#">MIB_MFE_TABLE (section 2.2.1.2.52)</a> . <i>rgbyData</i> SHOULD be specified as NULL when the requested IP multicast forwarding entry is not found when using the RMIBEntryGet, RMIBEntryGetFirst, and RMIBEntryGetNext methods. These methods return ERROR_SUCCESS even if they do not find the requested IP multicast forwarding entry.
0x00000013 MCAST_MFE_STATS	Statistics associated with an MFE.	<a href="#">MIB_MFE_STATS_TABLE (section 2.2.1.2.51)</a>
0x00000014 BEST_IF	Information about the interface that has the best route to a particular destination IPv4 address.	<a href="#">MIB_BEST_IF (section 2.2.1.2.23)</a>
0x00000015 BEST_ROUTE	Information about a particular route.	<a href="#">INTERFACE_ROUTE_INFO (section 2.2.1.2.11)</a>
0x00000016 PROXY_ARP	Information for a Proxy Address Resolution Protocol (PARP) entry.	<a href="#">MIB_PROXYARP (section 2.2.1.2.55)</a>
0x00000017 MCAST_IF_ENTRY	Information about an IP multicast interface.	<a href="#">MIB_IPMCAST_IF_ENTRY (section 2.2.1.2.40)</a>
0x00000018 MCAST_GLOBAL	Global information for IP multicast on a particular computer.	<a href="#">MIB_IPMCAST_GLOBAL (section 2.2.1.2.39)</a>

<b>dwId Value</b>	<b>Meaning</b>	<b>Structure to be pointed to by rgbyData.</b>
0x00000019 IF_STATUS	Status information for a particular interface.	<a href="#">MIB_IFSTATUS (section 2.2.1.2.30)</a>
0x0000001a MCAST_BOUNDARY	Information about a router's scoped IPv4 multicast address boundaries.	<a href="#">MIB_IPMCAST_BOUNDARY (section 2.2.1.2.37)</a>
0x0000001b MCAST_SCOPE	Information about a multicast scope.	<a href="#">MIB_IPMCAST_SCOPE (section 2.2.1.2.46)</a>
0x0000001c DEST_MATCHING	Route information about a matching destination.	<a href="#">MIB_IPDESTTABLE (section 2.2.1.2.21)</a>
0x0000001d DEST_LONGER	Information about all the possible routes to a destination.	MIB_IPDESTTABLE (section 2.2.1.2.21)
0x0000001e DEST_SHORTER	Information about the best matching routes to a destination.	MIB_IPDESTTABLE (section 2.2.1.2.21)
0x0000001f ROUTE_MATCHING	Information about a matching IP route.	MIB_IPDESTTABLE (section 2.2.1.2.21)
0x00000020 ROUTE_LONGER	Information about all the possible routes to a destination.	MIB_IPDESTTABLE (section 2.2.1.2.21)
0x00000021 ROUTE_SHORTER	Information about the best matching routes to a destination.	MIB_IPDESTTABLE (section 2.2.1.2.21)
0x00000022 ROUTE_STATE	Information about whether the route needs to be added to the forwarder or not.	<a href="#">MIB_ROUTESTATE (section 2.2.1.2.22)</a>
0x00000023 MCAST_MFE_STATS_EX	Statistics associated with an MFE.	<b>MIB_MFE_STATS_TABLE</b> (section 2.2.1.2.51)

**ullAlign (4 bytes):** The number of bytes that align the information returned. This is used to align the field to a long boundary so that the structure is aligned.

**rgbyData (4 bytes):** A pointer to the information returned from the opaque query.

### 2.2.1.2.54 MIB\_OPAQUE\_QUERY

The **MIB\_OPAQUE\_QUERY** structure contains the MIB ID and the corresponding index of the MIB object. This structure is used in the following methods:

- [RMIBEntryGet \(section 3.1.4.30\)](#)
- [RMIBEntryDelete \(section 3.1.4.28\)](#)
- [RMIBEntryGetFirst \(section 3.1.4.31\)](#)
- [RMIBEntryGetNext \(section 3.1.4.32\)](#)

The same structure is also used as a blob for querying MIB if **dwPid** is PID\_IPX, or if **dwPid** is PID\_IP and **dwRoutingPid** is not IPRTRMGR\_PID in the parameter of the methods using this structure.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwVarId																															
rgdwVarIndex (variable)																															
...																															

**dwVarId (4 bytes):** The identifier of the MIB object while querying IPv4 or IPv6 MIB variables. The value MUST be the same as **dwId** for [MIB\\_OPAQUE\\_INFO](#).

**rgdwVarIndex (variable):** Place holder for data of the blob as previously mentioned. If **dwRoutingPid** is IPRTRMGR\_PID, then this MUST indicate the index of the MIB object to query as shown in the following table.

dwVarId	rgdwVarIndex	Structure that needs to be retrieved	Meaning of rgdwVarIndex
0x00000000 IF_NUMBER	Not used.	<a href="#">MIB_IFNUMBER (section 2.2.1.2.28)</a>	Not used.
0x00000001 IF_TABLE	Not used.	<a href="#">MIB_IFTABLE (section 2.2.1.2.31)</a>	Not used.
0x00000002 IF_ROW	Index of the interface.	<a href="#">MIB_IFROW (section 2.2.1.2.29)</a>	The instance of the structure whose interface index matches with the value specified in <b>rgdwVarIndex</b> .
0x00000003 IP_STATS	Not used.	<a href="#">MIB_IPSTATS (section 2.2.1.2.49)</a>	Not used.
0x00000004 IP_ADDRTABLE	Not used.	<a href="#">MIB_IPADDRTABLE (section 2.2.1.2.33)</a>	Not used.

<b>dwVarId</b>	<b>rgdwVarIndex</b>	<b>Structure that needs to be retrieved</b>	<b>Meaning of rgdwVarIndex</b>
0x00000005 IP_ADDRROW	IP address.	<a href="#">MIB_IPADDRROW (section 2.2.1.2.32)</a>	The instance of the structure whose dwAddr matches the value specified in rgdwVarIndex.
0x00000006 IP_FORWARDNUMBER	Not used.	<a href="#">MIB_IPFORWARDNUMBER (section 2.2.1.2.34)</a>	Not used.
0x00000007 IP_FORWARDTABLE	Not used.	<a href="#">MIB_IPFORWARDTABLE (section 2.2.1.2.36)</a>	Not used.
0x00000008 IP_FORWARDROW	This MUST be of 4 DWORDS size (rgdwVarIndex[4]) for IPV4. For IPV6 this MUST be index.	<a href="#">MIB_IPFORWARDROW (section 2.2.1.2.35)</a> for IPv4, <a href="#">INTERFACE_ROUTE_ENTRY (section 2.2.1.2.181)</a> for IPv6	For IPv4, the instance of the structure whose dwForwardDest matches rgdwVarIndex[0], dwForwardProto matches rgdwVarIndex[1], dwForwardPolicy matches rgdwVarIndex[2], and dwForwardNextHop matches rgdwVarIndex[3]. For IPv6, the instance of the structure whose dwIndex matches rgdwVarIndex.
0x00000009 IP_NETTABLE	MUST be of size one DWORD (rgdwVarIndex[1]) or two DWORDS (rgdwVarIndex[2]).	<a href="#">MIB_IPNETTABLE (section 2.2.1.2.48)</a>	If one DWORD is passed, an instance of the structure whose <b>dwIndex</b> matches the value specified in rgdwVarIndex[0] is returned. If two DWORDs are passed, an instance of the structure whose <b>dwIndex</b> matches the value specified in rgdwVarIndex[0] and whose <b>dwAddr</b> matches rgdwVarIndex[1] is returned.
0x0000000a	This MUST be of	<a href="#">MIB_IPNETROW (section</a>	If one DWORD is

<b>dwVarId</b>	<b>rgdwVarIndex</b>	<b>Structure that needs to be retrieved</b>	<b>Meaning of rgdwVarIndex</b>
IP_NETROW	size one DWORD (rgdwVarIndex[1]) or two DWORDS (rgdwVarIndex[2]).	<a href="#">2.2.1.2.47</a>	passed, an instance of the structure whose dwIndex matches the value specified in rgdwVarIndex[0] is returned.  If two DWORDs are passed, an instance of the structure whose dwIndex matches the value specified in rgdwVarIndex[0] and whose dwAddr matches rgdwVarIndex[1] is returned.
0x0000000b ICMP_STATS	Not used.	<a href="#">MIB_ICMP (section 2.2.1.2.25)</a>	Not used.
0x0000000c TCP_STATS	Not used.	<a href="#">MIB_TCPSTATS (section 2.2.1.2.57)</a>	Not used.
0x0000000e TCP_ROW	This MUST be of 4 DWORDS size (rgdwVarIndex[4]) for IPV4.	<a href="#">MIB_TCPROW (section 2.2.1.2.56)</a>	The instance of the structure whose dwLocalAddr matches rgdwVarIndex[0], dwLocalPort matches rgdwVarIndex[1], dwRemoteAddr matches rgdwVarIndex[2], and dwRemotePort matches rgdwVarIndex[3].
0x0000000f UDP_STATS	Not used.	<a href="#">MIB_UDPSTATS (section 2.2.1.2.60)</a>	Not used.
0x00000010 UDP_TABLE	Not used.	<a href="#">MIB_UDPTABLE (section 2.2.1.2.61)</a>	Not used.
0x00000011 UDP_ROW	This MUST be of size one DWORD (rgdwVarIndex[1]) or two DWORDS (rgdwVarIndex[2]).	<a href="#">MIB_UDPROW (section 2.2.1.2.59)</a>	If one DWORD is passed, an instance of the structure whose dwLocalAddr matches the value specified in rgdwVarIndex[0] is returned.  If two DWORDs are passed, an instance

<b>dwVarId</b>	<b>rgdwVarIndex</b>	<b>Structure that needs to be retrieved</b>	<b>Meaning of rgdwVarIndex</b>
			of the structure whose dwLocalAddr matches the value specified in rgdwVarIndex[0] and whose dwLocalPort matches the value specified in rgdwVarIndex[1]. Both dwLocalAddr and dwLocalPort MUST be specified for RMIBEntryGet.
0x00000012 MCAST_MFE	This MUST be of 3 DWORDS size (rgdwVarIndex[3]).	<a href="#">MIB_MFE_TABLE (section 2.2.1.2.52)</a>	The instance of the structure whose dwGroup matches rgdwVarIndex[0], dwSource matches rgdwVarIndex[1], dwSrcMask matches rgdwVarIndex[2] is returned, and rgdwVarIndex[2] MUST be 0xffffffff.
0x00000013 MCAST_MFE_STATS	This MUST be of 3 DWORDS size (rgdwVarIndex[3]).	<a href="#">MIB_IPMCAST_MFE_STATS (section 2.2.1.2.44)</a>	The instance of the structure whose dwGroup matches rgdwVarIndex[0], dwSource matches rgdwVarIndex[1], dwSrcMask matches rgdwVarIndex[2] is returned, and rgdwVarIndex[2] MUST be 0xffffffff.
0x00000014 BEST_IF	MUST be of 1 DWORDS size (rgdwVarIndex[1]).	<a href="#">MIB_BEST_IF (section 2.2.1.2.23)</a>	The interface having the best route for the destination specified in rgdwVarIndex[0] is returned.
0x00000015 BEST_ROUTE	MUST be of 2 DWORDS size (rgdwVarIndex[2]).	<a href="#">INTERFACE_ROUTE_INFO (section 2.2.1.2.11)</a>	The best route information for the destination specified in rgdwVarIndex[0] is returned. rgdwVarIndex[1] MUST be set to 0.
0x00000017 MCAST_IF_ENTRY	MUST be of 1 DWORDS size (rgdwVarIndex[1]).	<a href="#">MIB_IPMCAST_IF_ENTRY (section 2.2.1.2.40)</a>	The instance of the structure whose interface index matches with the

<b>dwVarId</b>	<b>rgdwVarIndex</b>	<b>Structure that needs to be retrieved</b>	<b>Meaning of rgdwVarIndex</b>
			value specified in <b>rgdwVarIndex</b> .
0x00000018 MCAST_GLOBAL	Not used.	<a href="#">MIB_IPMCAST_GLOBAL (section 2.2.1.2.39)</a>	Not used.
0x00000019 IF_STATUS	MUST be of 1 DWORDS size (rgdwVarIndex[1]).	<a href="#">MIB_IFSTATUS (section 2.2.1.2.30)</a>	The instance of the structure whose interface index matches with the value specified in rgdwVarIndex.
0x0000001a MCAST_BOUNDARY	MUST be of 3 DWORDS size (rgdwVarIndex[3]).	<a href="#">MIB_IPMCAST_BOUNDARY (section 2.2.1.2.37)</a>	The instance with <b>dwIfIndex</b> equal to rgdwVarIndex[0], <b>dwGroupAddress</b> equal to rgdwVarIndex[1], and <b>dwGroupMask</b> equal to rgdwVarIndex[2] is returned.
0x0000001b MCAST_SCOPE	MUST be of size one DWORD (rgdwVarIndex[1]) or two DWORDS (rgdwVarIndex[2]).	<a href="#">MIB_IPMCAST_SCOPE (section 2.2.1.2.46)</a>	If one DWORD is passed, an instance of the structure whose <b>dwGroupAddress</b> matches the value specified in rgdwVarIndex[0] is returned.  If two DWORDs are passed, an instance of the structure whose <b>dwGroupAddress</b> matches the value specified in rgdwVarIndex[0] and whose <b>dwGroupMask</b> matches rgdwVarIndex[1] is returned.  Both <b>dwGroupAddress</b> and <b>dwGroupMask</b> MUST be specified for <b>RMIBEntryGet</b>
0x0000001c DEST_MATCHING	MUST be of 4 DWORDS size (rgdwVarIndex[4]).	<a href="#">MIB_IPDESTTABLE (section 2.2.1.2.21)</a>	The instance of the structure whose ForwardRow fields of <b>dwForwardDest</b>

<b>dwVarId</b>	<b>rgdwVarIndex</b>	<b>Structure that needs to be retrieved</b>	<b>Meaning of rgdwVarIndex</b>
			matches rgdwVarIndex[0], <b>dwForwardMask</b> matches rgdwVarIndex[1], <b>dwForwardViewSet</b> matches rgdwVarIndex[2], and whose <b>dwForwardProto</b> matches rgdwVarIndex[3].
0x0000001d DEST_LONGER	MUST be of 4 DWORDS size (rgdwVarIndex[4]).	<b>MIB_IPDESTTABLE</b> (section 2.2.1.2.21)	The instance of the structure whose ForwardRow fields of <b>dwForwardDest</b> matches rgdwVarIndex[0], <b>dwForwardMask</b> matches rgdwVarIndex[1], <b>dwForwardViewSet</b> matches rgdwVarIndex[2], and whose <b>dwForwardProto</b> matches rgdwVarIndex[3].
0x0000001e DEST_SHORTER	MUST be of 4 DWORDS size (rgdwVarIndex[4]).	<b>MIB_IPDESTTABLE</b> (section 2.2.1.2.21)	The instance of the structure whose ForwardRow fields of <b>dwForwardDest</b> matches rgdwVarIndex[0], <b>dwForwardMask</b> matches rgdwVarIndex[1], <b>dwForwardViewSet</b> matches rgdwVarIndex[2], and whose <b>dwForwardProto</b> matches rgdwVarIndex[3].
0x0000001f ROUTE_MATCHING	This MUST be of 4 DWORDS size (rgdwVarIndex[4]).	<b>MIB_IPDESTTABLE</b> (section 2.2.1.2.21)	The instance of the structure whose ForwardRow fields of dwForwardDest matches rgdwVarIndex[0], dwForwardMask matches rgdwVarIndex[1], dwForwardViewSet



<b>dwVarId</b>	<b>rgdwVarIndex</b>	<b>Structure that needs to be retrieved</b>	<b>Meaning of rgdwVarIndex</b>
			matches rgdwVarIndex[2], and whose dwForwardProto matches rgdwVarIndex[3].
0x00000020 ROUTE_LONGER	MUST be of 4 DWORDS size (rgdwVarIndex[4]).	<b>MIB_IPDESTTABLE</b> (section 2.2.1.2.21)	The instance of the structure whose ForwardRow fields of <b>dwForwardDest</b> matches rgdwVarIndex[0], <b>dwForwardMask</b> matches rgdwVarIndex[1], <b>dwForwardViewSet</b> matches rgdwVarIndex[2], and whose <b>dwForwardProto</b> matches rgdwVarIndex[3].
0x00000021 ROUTE_SHORTER	MUST be of 4 DWORDS size (rgdwVarIndex[4]).	<b>MIB_IPDESTTABLE</b> (section 2.2.1.2.21)	The instance of the structure whose ForwardRow fields of <b>dwForwardDest</b> matches rgdwVarIndex[0], <b>dwForwardMask</b> matches rgdwVarIndex[1], <b>dwForwardViewSet</b> matches rgdwVarIndex[2], and whose <b>dwForwardProto</b> matches rgdwVarIndex[3].
0x00000022 ROUTE_STATE	Not used.	<a href="#">MIB_ROUTESTATE (section 2.2.1.2.22)</a>	Not used.
0x00000023 MCAST_MFE_STATS_EX	MUST be of 3 DWORDS size (rgdwVarIndex[3]).	<a href="#">MIB_MFE_STATS_TABLE (section 2.2.1.2.51)</a>	The instance of the structure whose <b>dwGroup</b> field matches rgdwVarIndex[0], and <b>dwSource</b> matches rgdwVarIndex[1]. rgdwVarIndex[2] is not used.

### 2.2.1.2.55 MIB\_PROXYARP

The **MIB\_PROXYARP** structure stores information for a Proxy Address Resolution Protocol (PARP) entry. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_PROXYARP {
    DWORD dwAddress;
    DWORD dwMask;
    DWORD dwIfIndex;
} MIB_PROXYARP,
*PMIB_PROXYARP;
```

**dwAddress:** The IPv4 address that acts as a proxy.

**dwMask:** The subnet mask for the IPv4 address specified by the **dwAddress** member. See [\[RFC950\]](#).

**dwIfIndex:** The index of the interface that acts as a proxy for the address specified by the **dwAddress** member.

### 2.2.1.2.56 MIB\_TCPROW

The **MIB\_TCPROW** structure contains information for an IPv4 TCP connection. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_TCPROW {
    union {
        DWORD dwState;
        MIB_TCP_STATE State;
    };
    DWORD dwLocalAddr;
    DWORD dwLocalPort;
    DWORD dwRemoteAddr;
    DWORD dwRemotePort;
} MIB_TCPROW,
*PMIB_TCPROW;
```

**dwState:** The state of the TCP connection. This member can be one of the enums in [MIB\\_TCP\\_STATE \(section 2.2.1.1.11\)](#).

**State:** The state of the TCP connection. [<36>](#)

**dwLocalAddr:** The local IPv4 address for the TCP connection on the local computer. A value of zero indicates the listener can accept a connection on any interface.

**dwLocalPort:** The local port number in network byte order for the TCP connection on the local computer.

**dwRemoteAddr:** The IPv4 address for the TCP connection on the remote computer.

**dwRemotePort:** The remote port number in network byte order for the TCP connection on the remote computer.

### 2.2.1.2.57 MIB\_TCPSTATS

The **MIB\_TCPSTATS** structure contains statistics for the TCP protocol running on the local computer. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_TCPSTATS {
    union {
        DWORD dwRtoAlgorithm;
        TCP_RTO_ALGORITHM RtoAlgorithm;
    };
    DWORD dwRtoMin;
    DWORD dwRtoMax;
    DWORD dwMaxConn;
    DWORD dwActiveOpens;
    DWORD dwPassiveOpens;
    DWORD dwAttemptFails;
    DWORD dwEstabResets;
    DWORD dwCurrEstab;
    DWORD dwInSegs;
    DWORD dwOutSegs;
    DWORD dwRetransSegs;
    DWORD dwInErrs;
    DWORD dwOutRsts;
    DWORD dwNumConns;
} MIB_TCPSTATS,
*PMIB_TCPSTATS;
```

**dwRtoAlgorithm:** The retransmission time-out (RTO) algorithm in use. This member can be one of the enum values in [TCP\\_RTO\\_ALGORITHM \(section 2.2.1.1.12\)](#).

**RtoAlgorithm:** The RTO algorithm in use. [<37>](#)

**dwRtoMin:** The minimum RTO value in milliseconds.

**dwRtoMax:** The maximum RTO value in milliseconds.

**dwMaxConn:** The maximum number of connections. If this member is -1, the maximum number of connections is variable.

**dwActiveOpens:** The number of active open connections. In an active open, the client is initiating a connection with the server.

**dwPassiveOpens:** The number of passive open connections. In a passive open, the server is listening for a connection request from a client.

**dwAttemptFails:** The number of failed connection attempts.

**dwEstabResets:** The number of established connections that were reset.

**dwCurrEstab:** The number of currently established connections.

**dwInSegs:** The number of segments received.

**dwOutSegs:** The number of segments transmitted. This number does not include retransmitted segments.

**dwRetransSegs:** The number of segments retransmitted.

**dwInErrs:** The number of errors received.

**dwOutRsts:** The number of segments transmitted with the reset flag set.

**dwNumConns:** The number of connections that are currently present in the system. This total number includes connections in all states except listening connections.

#### 2.2.1.2.58 MIB\_TCPTABLE

The **MIB\_TCPTABLE** structure contains a table of IPv4 TCP connections on the local computer.

```
typedef struct _MIB_TCPTABLE {
    DWORD dwNumEntries;
    MIB_TCPROW table[dwNumEntries];
    BYTE reserved[8];
} MIB_TCPTABLE,
*PMIB_TCPTABLE;
```

**dwNumEntries:** The number of entries in the table.

**table:** A pointer to a table of TCP connections implemented as an array of [MIB\\_TCPROW \(section 2.2.1.2.56\)](#) structures.

**reserved:** An array of 8 bytes that SHOULD be set to 0 and ignored on receipt.

#### 2.2.1.2.59 MIB\_UDPROW

The **MIB\_UDPROW** structure contains address information for sending and receiving User Datagram Protocol (UDP) datagrams. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_UDPROW {
    DWORD dwLocalAddr;
    DWORD dwLocalPort;
} MIB_UDPROW,
*PMIB_UDPROW;
```

**dwLocalAddr:** The IPv4 address on the local computer.

**dwLocalPort:** The port number on the local computer.

#### 2.2.1.2.60 MIB\_UDPSTATS

The **MIB\_UDPSTATS** structure contains statistics for the UDP running on the local computer. This structure is used in [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).

```
typedef struct _MIB_UDPSTATS {
    DWORD dwInDatagrams;
    DWORD dwNoPorts;
    DWORD dwInErrors;
    DWORD dwOutDatagrams;
    DWORD dwNumAddrs;
} MIB_UDPSTATS,
```

\*PMIB\_UDPSTATS;

**dwInDatagrams:** The number of datagrams received.

**dwNoPorts:** The number of datagrams received that were discarded because the port specified was invalid.

**dwInErrors:** The number of erroneous datagrams received. This number does not include the value contained by the **dwNoPorts** member.

**dwOutDatagrams:** The number of datagrams transmitted.

**dwNumAddrs:** The number of entries in the UDP listener table.

#### 2.2.1.2.61 MIB\_UDPTABLE

The **MIB\_UDPTABLE** structure contains a table of address information for sending and receiving UDP datagrams on the local computer.

```
typedef struct _MIB_UDPTABLE {  
    DWORD dwNumEntries;  
    MIB_UDPROW table[dwNumEntries];  
    BYTE reserved[8];  
} MIB_UDPTABLE,  
*PMIB_UDPTABLE;
```

**dwNumEntries:** The number of entries in the table.

**table:** Pointer to an array of [MIB\\_UDPROW \(section 2.2.1.2.59\)](#) structures.

**reserved:** An array of 8 bytes that SHOULD be set to 0 and ignored on receipt.

#### 2.2.1.2.62 MPR\_SERVER\_0

The **MPR\_SERVER\_0** structure contains configuration information for a router.

```
typedef struct MPR_SERVER_0 {  
    BOOL fLanOnlyMode;  
    DWORD dwUpTime;  
    DWORD dwTotalPorts;  
    DWORD dwPortsInUse;  
} MPR_SERVER_0,  
*PMPR_SERVER_0;
```

**fLanOnlyMode:** This is of type BOOL. It specifies whether the RRAS server is running in LAN only mode or not. If the value is 1, the RRAS server is not routing; if the value is 0, then the RRAS server is functioning as a router.

Value	Meaning
0	The RRAS server is functioning as a router.
1	The RRAS server is not routing.

**dwUpTime:** Specifies the elapsed time (in seconds) since the router was started.

**dwTotalPorts:** Specifies the number of ports on the router.

**dwPortsInUse:** Specifies the number of ports on the router currently in use.

#### 2.2.1.2.63 MPR\_SERVER\_1

The **MPR\_SERVER\_1** structure is used to get and set the number of Point-to-Point Tunneling Protocol/Layer Two Tunneling Protocol (PPTP/L2TP) ports configured on the RRAS server. It is also used to get and set the RRAS functionality and router functionality enabled on those ports.

```
typedef struct MPR_SERVER_1 {
    DWORD dwNumPptpPorts;
    DWORD dwPptpPortFlags;
    DWORD dwNumL2tpPorts;
    DWORD dwL2tpPortFlags;
} MPR_SERVER_1,
*PMPR_SERVER_1;
```

**dwNumPptpPorts:** Specifies the number of ports configured on that (PPTP) device. This value cannot exceed the server port limit. [<38>](#)

**dwPptpPortFlags:** Indicates the RRAS server and/or router functionality configured on the PPTP device.

Possible flag values are as follows.

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote access is enabled for PPTP.
MPR_ENABLE_ROUTING_ON_DEVICE 0x00000002	Routing is enabled for PPTP.

**dwNumL2tpPorts:** Specifies the number of ports configured on that (L2TP) device. This value cannot exceed the server port limit. [<39>](#)

**dwL2tpPortFlags:** Indicates the RAS and/or router functionality configured on the L2TP device.

Possible flag values are as follows.

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote access is enabled for L2TP.

Value	Meaning
MPR_ENABLE_ROUTING_ON_DEVICE 0x00000002	Routing is enabled for L2TP.

#### 2.2.1.2.64 MPR\_SERVER\_2

The **MPR\_SERVER\_2** structure is used to get and set the number of Point-to-Point Tunneling Protocol/Layer Two Tunneling Protocol/Secure Socket Tunneling Protocol (PPTP/L2TP/SSTP) ports configured on the RRAS server. It also gets and sets the RRAS functionality and router functionality enabled on the server. [<40>](#)

```
typedef struct MPR_SERVER_2 {
    DWORD dwNumPptpPorts;
    DWORD dwPptpPortFlags;
    DWORD dwNumL2tpPorts;
    DWORD dwL2tpPortFlags;
    DWORD dwNumSstpPorts;
    DWORD dwSstpPortFlags;
} MPR_SERVER_2,
*PMPR_SERVER_2;
```

**dwNumPptpPorts:** Specifies the number of ports configured on that (PPTP) device. This value cannot exceed the server port limit. [<41>](#)

**dwPptpPortFlags:** Indicates the RRAS server and/or router functionality configured on the PPTP device.

Possible flag values are as follows.

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote access is enabled for PPTP.
MPR_ENABLE_ROUTING_ON_DEVICE 0x00000002	Routing is enabled for PPTP.

**dwNumL2tpPorts:** Specifies the number of ports configured on that (L2TP) device. This value cannot exceed the server port limit. [<42>](#)

**dwL2tpPortFlags:** Indicates the RRAS server and/or router functionality configured on the L2TP device.

Possible flag values are as follows.

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote access is enabled for L2TP.
MPR_ENABLE_ROUTING_ON_DEVICE 0x00000002	Routing is enabled for L2TP.

**dwNumSstpPorts:** Specifies the number of ports configured on that (SSTP) device. [<43>](#) This value cannot exceed the server port limit. [<44>](#)

**dwSstpPortFlags:** Indicates the RRAS server and/or router functionality configured on the SSTP device. [<45>](#)

Possible flag values are as follows.

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote access is enabled for SSTP.

#### 2.2.1.2.65 PPP\_NBFCP\_INFO

The **PPP\_NBFCP\_INFO** structure contains the result of a PPP NetBEUI Framer (NBF) projection operation. [<46>](#)

```
typedef struct _PPP_NBFCP_INFO {  
    DWORD dwError;  
    WCHAR wszWksta[17];  
} PPP_NBFCP_INFO;
```

**dwError:** Specifies the result of the PPP control protocol negotiation. A value of zero indicates success. A nonzero value indicates failure and is the actual fatal error that occurred during the control protocol negotiation.

**wszWksta:** Specifies a null-terminated Unicode string that is the local workstation's computer name. This unique computer name is the closest **NetBIOS** equivalent to a client's NetBEUI address on a remote access connection.

#### 2.2.1.2.66 PPP\_IPCP\_INFO

The **PPP\_IPCP\_INFO** structure contains the result of a PPP control protocol negotiation for IP.

```
typedef struct _PPP_IPCP_INFO {  
    DWORD dwError;  
    WCHAR wszAddress[16];  
    WCHAR wszRemoteAddress[16];  
} PPP_IPCP_INFO;
```

**dwError:** Specifies the result of the PPP control protocol negotiation. A value of zero indicates success. A nonzero value indicates failure and is the actual fatal error that occurred during the control protocol negotiation.

**wszAddress:** Specifies a null-terminated Unicode string that holds the local computer's IP address for the connection. This string has the form a.b.c.d; for example, "10.102.235.84".

If a remote access client is connecting to a RRAS server, this member holds the IP address of the server.



**wszRemoteAddress:** Specifies a null-terminated Unicode string that holds the IP address of the remote computer. This string has the form a.b.c.d. If the address is not available, this member is an empty string.

If a remote access client is connecting to a RRAS server, this member holds the IP address of the client.

#### 2.2.1.2.67 PPP\_IPCP\_INFO2

The **PPP\_IPCP\_INFO2** structure contains the result of a PPP control protocol negotiation for the IP.

```
typedef struct _PPP_IPCP_INFO2 {  
    DWORD dwError;  
    WCHAR wszAddress[16];  
    WCHAR wszRemoteAddress[16];  
    DWORD dwOptions;  
    DWORD dwRemoteOptions;  
} PPP_IPCP_INFO2;
```

**dwError:** See **dwError** in [PPP\\_IPCP\\_INFO \(section 2.2.1.2.66\)](#).

**wszAddress:** See **wszAddress** in PPP\_IPCP\_INFO.

**wszRemoteAddress:** See **wszRemoteAddress** in PPP\_IPCP\_INFO.

**dwOptions:** Specifies IP Configuration Parameters (IPCP) options for the local computer.

When set to PPP\_IPCP\_VJ (0x00000001), indicates that IP datagrams sent by the local computer are compressed using Van Jacobson compression. Otherwise, set to 0x00000000.

**dwRemoteOptions:** Uses the same values as **dwOptions**, but applies to datagrams received by the local computer.

#### 2.2.1.2.68 PPP\_IPXCP\_INFO

The **PPP\_IPXCP\_INFO** structure contains the result of a PPP IPX projection operation. [<47>](#)

```
typedef struct _PPP_IPXCP_INFO {  
    DWORD dwError;  
    WCHAR wszAddress[23];  
} PPP_IPXCP_INFO;
```

**dwError:** Specifies the result of the PPP control protocol negotiation. As value of zero indicates success. A nonzero value indicates failure and is the actual fatal error that occurred during the control protocol negotiation.

**wszAddress:** Specifies a null-terminated Unicode string that holds the client's IPX address on the RRAS server connection. This address string has the form of "net.node" (for example, "1234ABCD.12AB34CD56EF").

### 2.2.1.2.69 PPP\_IPV6\_CP\_INFO

The **PPP\_IPV6\_CP\_INFO** structure contains the result of a PPP control protocol negotiation for IPv6. [<48>](#)

```
typedef struct _PPP_IPV6CP_INFO {
    DWORD dwVersion;
    DWORD dwSize;
    DWORD dwError;
    BYTE bInterfaceIdentifier[8];
    BYTE bRemoteInterfaceIdentifier[8];
    DWORD dwOptions;
    DWORD dwRemoteOptions;
    BYTE bPrefix[8];
    DWORD dwPrefixLength;
} PPP_IPV6_CP_INFO,
*PPPP_IPV6_CP_INFO;
```

**dwVersion:** Specifies the version of the **PPP\_IPV6\_CP\_INFO** structure used. Currently this field is not used and MUST be set to zero.

**dwSize:** This SHOULD be set to 0. This MAY be used to specify the size, in bytes, of this **PPP\_IPV6\_CP\_INFO** structure.

**dwError:** Specifies the result of the PPP control protocol negotiation. A value of zero indicates success. A nonzero value indicates failure and is the actual fatal error that occurred during the control protocol negotiation.

**bInterfaceIdentifier:** Specifies the 64-bit **interface identifier** of the IPv6 server **interface**.

**bRemoteInterfaceIdentifier:** Specifies the 64-bit interface identifier of the IPv6 client interface.

**dwOptions:** Currently this is not used and MUST be set to zero.

**dwRemoteOptions:** Currently this is not used and MUST be set to zero.

**bPrefix:** Specifies the address prefix of the IPv6 client interface.

**dwPrefixLength:** The length, in bits, of the address prefix.

### 2.2.1.2.70 PPP\_ATCP\_INFO

The **PPP\_ATCP\_INFO** structure contains the result of a PPP AppleTalk projection operation. [<49>](#)

```
typedef struct _PPP_ATCP_INFO {
    DWORD dwError;
    WCHAR wszAddress[33];
} PPP_ATCP_INFO;
```

**dwError:** Specifies the result of the PPP control protocol negotiation. A value of zero indicates success. A nonzero value indicates failure and is the actual fatal error that occurred during the control protocol negotiation.

**wszAddress:** Specifies a null-terminated Unicode string that holds the client's AppleTalk address on the RRAS server connection.

#### 2.2.1.2.71 PPP\_CCP\_INFO

The **PPP\_CCP\_INFO** structure contains information that describes the results of a **Compression Control Protocol (CCP)** negotiation.

```
typedef struct _PPP_CCP_INFO {  
    DWORD dwError;  
    DWORD dwCompressionAlgorithm;  
    DWORD dwOptions;  
    DWORD dwRemoteCompressionAlgorithm;  
    DWORD dwRemoteOptions;  
} PPP_CCP_INFO;
```

**dwError:** Specifies an error if the negotiation was unsuccessful. Zero indicates success.

**dwCompressionAlgorithm:** Specifies the compression algorithm used by the local computer.

The following table shows the possible values for this member.

Value	Meaning
0x00000000	The local computer has not negotiated any compression algorithm.
RASCCPCA_MPPC 0x00000006	Microsoft Point-to-Point Compression (MPPC) Protocol.
RASCCPCA_STAC 0x00000005	STAC LZS data compression algorithm <a href="#">[RFC1974]</a> option 4.

**dwOptions:** Specifies the compression options on the local computer.

The following options are supported.

Value	Meaning
0x00000000	No additional compression options are available.
PPP_CCP_COMPRESSION 0x00000001	Compression without encryption.
PPP_CCP_HISTORYLESS 0x01000000	Microsoft Point-to-Point Encryption (MPPE) in stateless mode. The session key is changed after every packet. This mode improves performance on high-latency networks, or networks that experience significant packet loss.
PPP_CCP_ENCRYPTION40BIT 0x00000020	MPPE using 40-bit keys.
PPP_CCP_ENCRYPTION56BIT 0x00000080	MPPE using 56-bit keys.
PPP_CCP_ENCRYPTION128BIT	MPPE using 128-bit keys.

Value	Meaning
0x00000040	

**dwRemoteCompressionAlgorithm:** Specifies the compression algorithm used by the remote computer.

The following table shows the possible values for this member.

Value	Meaning
0x00000000	The remote computer has not negotiated any compression algorithm.
RASCCPCA_MPPC 0x00000006	MPPC Protocol.
RASCCPCA_STAC 0x00000005	STAC option 4.

**dwRemoteOptions:** Specifies the compression options on the remote computer.

The following options are supported.

Value	Meaning
0x00000000	No additional compression options are available.
PPP_CCP_COMPRESSION 0x00000001	Compression without encryption.
PPP_CCP_HISTORYLESS 0x01000000	MPPE in stateless mode. The session key is changed after every packet. This mode improves performance on high-latency networks, or networks that experience significant packet loss.
PPP_CCP_ENCRYPTION40BIT 0x00000020	MPPE using 40-bit keys.
PPP_CCP_ENCRYPTION56BIT 0x00000080	MPPE using 56-bit keys.
PPP_CCP_ENCRYPTION128BIT 0x00000040	MPPE using 128-bit keys.

### 2.2.1.2.72 PPP\_LCP\_INFO

The **PPP\_LCP\_INFO** structure contains information that describes the results of a PPP Link Control Protocol (LCP) negotiation.

```
typedef struct _PPP_LCP_INFO {
    DWORD dwError;
    DWORD dwAuthenticationProtocol;
    DWORD dwAuthenticationData;
    DWORD dwRemoteAuthenticationProtocol;
    DWORD dwRemoteAuthenticationData;
    DWORD dwTerminateReason;
    DWORD dwRemoteTerminateReason;
```

```

DWORD dwOptions;
DWORD dwRemoteOptions;
DWORD dwEapTypeId;
DWORD dwRemoteEapTypeId;
} PPP_LCP_INFO;

```

**dwError:** Specifies the error that occurred if the negotiation was unsuccessful. Zero indicates success.

**dwAuthenticationProtocol:** Specifies the authentication protocol used to authenticate the local computer. The following table shows the possible values for this member.

Value	Meaning
0x00000000	Either no authentication was negotiated by the local end, or no LCP settings are applicable for the connection (for example, an IKEv2 connection).
PPP_LCP_PAP 0x0000C023	Password Authentication Protocol (PAP) <a href="#">&lt;50&gt;</a>
PPP_LCP_SPAP 0x0000C027	Shiva Password Authentication Protocol (SPAP) <a href="#">&lt;51&gt;</a>
PPP_LCP_CHAP 0x0000C223	Challenge Handshake Authentication Protocol (CHAP) <a href="#">&lt;52&gt;</a>
PPP_LCP_EAP 0x0000C227	<b>Extensible Authentication Protocol (EAP)</b>

**dwAuthenticationData:** Specifies additional information about the authentication protocol specified by the **dwAuthenticationProtocol** member. The following table shows the possible values for this member.

Value	Meaning
0x00000000	No additional authentication data applies.
PPP_LCP_CHAP_MD5 0x00000005	MD5 CHAP <a href="#">&lt;53&gt;</a>
PPP_LCP_CHAP_MS 0x00000080	Microsoft CHAP <a href="#">&lt;54&gt;</a>
PPP_LCP_CHAP_MS2 0x00000081	Microsoft CHAP version 2

**dwRemoteAuthenticationProtocol:** Specifies the authentication protocol used to authenticate the remote computer. See the **dwAuthenticationProtocol** member for a list of possible values.

The following table shows the possible values for this member.

Value	Meaning
0x00000000	Either no authentication was negotiated by the remote end, or no LCP settings are applicable for the connection (for example, an IKEv2 connection).
PPP_LCP_PAP 0x0000C023	Password Authentication Protocol (PAP) <a href="#">&lt;55&gt;</a>
PPP_LCP_SPAP 0x0000C027	Shiva Password Authentication Protocol (SPAP) <a href="#">&lt;56&gt;</a>
PPP_LCP_CHAP 0x0000C223	Challenge Handshake Authentication Protocol (CHAP) <a href="#">&lt;57&gt;</a>
PPP_LCP_EAP 0x0000C227	Extensible Authentication Protocol (EAP)

**dwRemoteAuthenticationData:** Specifies additional information about the authentication protocol specified by **dwRemoteAuthenticationProtocol**. See the **dwAuthenticationData** member for a list of possible values.

**dwTerminateReason:** Specifies the reason the connection was terminated by the local computer. This member always has a value of zero.

**dwRemoteTerminateReason:** Specifies the reason the connection was terminated by the remote computer. This member always has a value of zero.

**dwOptions:** Specifies information about the LCP options in use by the local computer. This member is a combination of the following flags.

Value	Meaning
0x00000000	No flag is set.
PPP_LCP_MULTILINK_FRAMING 0x00000001	The connection is using multilink.
PPP_LCP_PFC 0x00000002	Protocol Field Compression (see <a href="#">[RFC1172]</a> ).
PPP_LCP_ACFC 0x00000004	Address and Control Field Compression (see <a href="#">[RFC1172]</a> ).
PPP_LCP_SSHF 0x00000008	Short Sequence Number Header Format (see <a href="#">[RFC1990]</a> ).
PPP_LCP_DES_56 0x00000010	<b>Data Encryption Standard (DES)</b> 56-bit encryption.
PPP_LCP_3_DES 0x00000020	Triple DES encryption.
PPP_LCP_AES_128 0x00000040	128-bit <b>AES</b> encryption. <a href="#">&lt;58&gt;</a>
PPP_LCP_AES_256 0x00000080	256-bit AES encryption. <a href="#">&lt;59&gt;</a>

**dwRemoteOptions:** Specifies information about the LCP options in use by the remote computer. See **dwOptions** member for a list of possible values.

**dwEapTypeId:** Specifies the type identifier of the EAP used to authenticate the local computer. MUST be one of the values specified in Method Types of [\[IANA-EAP\]](#). The value of this member is valid only if **dwAuthenticationProtocol** is PPP\_LCP\_EAP.

**dwRemoteEapTypeId:** This field MUST be zero and has no significance.

### 2.2.1.2.73 PPP\_INFO

The **PPP\_INFO** structure is used to report the results of the various PPP projection operations for a connection.

```
typedef struct _PPP_INFO {
    PPP_NBFCP_INFO nbfc;
    PPP_IPCP_INFO ip;
    PPP_IPXCP_INFO ipx;
    PPP_ATCP_INFO at;
} PPP_INFO;
```

**nbfc:** A [PPP\\_NBFCP\\_INFO \(section 2.2.1.2.65\)](#) structure containing information about the NetBEUI Frammer (NBF) for a connection.

**ip:** A [PPP\\_IPCP\\_INFO \(section 2.2.1.2.66\)](#) structure containing the IPv4 PPP information for a connection.

**ipx:** A [PPP\\_IPXCP\\_INFO \(section 2.2.1.2.68\)](#) structure containing the IPX information [<60>](#) for a connection.

**at:** A [PPP\\_ATCP\\_INFO \(section 2.2.1.2.70\)](#) structure containing the AppleTalk [<61>](#) information for a connection.

### 2.2.1.2.74 PPP\_INFO\_2

The **PPP\_INFO\_2** structure is used to report the results of the various PPP projection operations for a connection. [<62>](#)

```
typedef struct _PPP_INFO_2 {
    PPP_NBFCP_INFO nbfc;
    PPP_IPCP_INFO2 ip;
    PPP_IPXCP_INFO ipx;
    PPP_ATCP_INFO at;
    PPP_CCP_INFO ccp;
    PPP_LCP_INFO lcp;
} PPP_INFO_2;
```

**nbfc:** A [PPP\\_NBFCP\\_INFO \(section 2.2.1.2.65\)](#) structure containing information about the NetBEUI Frammer (NBF) for a connection.

**ip:** A [PPP\\_IPCP\\_INFO2 \(section 2.2.1.2.67\)](#) structure containing the IPv4 information for a connection.

**ipx:** A [PPP\\_IPXCP\\_INFO \(section 2.2.1.2.68\)](#) structure containing the IPX information [<63>](#) for a connection.

**at:** A [PPP\\_ATCP\\_INFO \(section 2.2.1.2.70\)](#) structure containing AppleTalk [<64>](#) information for a connection.

**ccp:** A [PPP\\_CCP\\_INFO \(section 2.2.1.2.71\)](#) structure containing compression information details for a given PPP connection.

**lcp:** A [PPP\\_LCP\\_INFO \(section 2.2.1.2.72\)](#) structure containing the PPP information related to the Link Control Protocol (LCP) for a given connection.

### 2.2.1.2.75 PPP\_INFO\_3

The **PPP\_INFO\_3** structure is used to report the results of the various PPP projection operations for a connection. [<65>](#)

```
typedef struct _PPP_INFO_3 {
    PPP_NBFCP_INFO nbfc;
    PPP_IPCP_INFO2 ip;
    PPP_IPV6_CP_INFO ipv6;
    PPP_CCP_INFO ccp;
    PPP_LCP_INFO lcp;
} PPP_INFO_3;
```

**nbfc:** A [PPP\\_NBFCP\\_INFO \(section 2.2.1.2.65\)](#) structure containing information about NetBEUI Framer (NBF) for a connection.

**ip:** A [PPP\\_IPCP\\_INFO2 \(section 2.2.1.2.67\)](#) structure containing the IPv4 information for a connection.

**ipv6:** A [PPP\\_IPV6\\_CP\\_INFO \(section 2.2.1.2.69\)](#) structure containing the IPv6 [<66>](#) information for a connection.

**ccp:** A [PPP\\_CCP\\_INFO \(section 2.2.1.2.71\)](#) structure containing the compression information details for a given connection.

**lcp:** A [PPP\\_LCP\\_INFO \(section 2.2.1.2.72\)](#) structure containing the compression information related to the Link Control Protocol (LCP) for a given connection.

### 2.2.1.2.76 RASI\_PORT\_0

The **RASI\_PORT\_0** structure contains general information regarding a specific RRAS port, such as the port condition and the port name.

```
typedef struct _RASI_PORT_0 {
    DWORD dwPort;
    DWORD dwConnection;
    RAS_PORT_CONDITION dwPortCondition;
    DWORD dwTotalNumberOfCalls;
    DWORD dwConnectDuration;
    WCHAR wszPortName[17];
    WCHAR wszMediaName[17];
    WCHAR wszDeviceName[129];
    WCHAR wszDeviceType[17];
}
```



```

} RASI_PORT_0,
*PRASI_PORT_0;

```

**dwPort:** A unique identifier for the port.

**dwConnection:** A unique identifier that specifies the connection.

**dwPortCondition:** A [RAS\\_PORT\\_CONDITION \(section 2.2.1.1.4\)](#) value indicating the condition of a port specified in **dwPort**.

**dwTotalNumberOfCalls:** Specifies the cumulative number of calls that this port has serviced.

**dwConnectDuration:** Specifies the duration of the current connection on this port, in seconds.

**wszPortName:** Specifies the port name.

**wszMediaName:** Specifies the media name.

**wszDeviceName:** Specifies the device name.

**wszDeviceType:** Specifies the device type.

This member can be one of the following string constants.

Value	Meaning
MPRDT_Modem "Modem"	A modem that is accessed through a Component Object Model (COM) port.
MPRDT_Isdn "Isdn"	An ISDN adapter with the corresponding NDISWAN driver installed.
MPRDT_X25 "x25"	An X.25 adapter with the corresponding NDISWAN driver installed.
MPRDT_Vpn "Vpn"	A virtual private network (VPN) connection.
MPRDT_Pad "Pad"	A packet assembler/disassembler.
MPRDT_Generic "GENERIC"	Generic.
MPRDT_Serial "SERIAL"	Direct serial connection through a serial port.
MPRDT_FrameRelay "FRAMERELAY"	Frame relay.
MPRDT_Atm "ATM"	Asynchronous transfer mode (ATM).
MPRDT_Sonet "SONET"	Sonet.

Value	Meaning
MPRDT_SW56 "SW56"	Switched 56K access.
MPRDT_Irda "IRDA"	An Infrared Data Association (IrDA)-compliant device.
MPRDT_Parallel "PARALLEL"	Direct parallel connection through a parallel port.

### 2.2.1.2.77 RASI\_PORT\_1

The **RASI\_PORT\_1** structure contains information about a RRAS port.

```
typedef struct _RASI_PORT_1 {
    DWORD dwPort;
    DWORD dwConnection;
    RAS_HARDWARE_CONDITION dwHardwareCondition;
    DWORD dwLineSpeed;
    DWORD dwBytesXmited;
    DWORD dwBytesRcvd;
    DWORD dwFramesXmited;
    DWORD dwFramesRcvd;
    DWORD dwCrcErr;
    DWORD dwTimeoutErr;
    DWORD dwAlignmentErr;
    DWORD dwHardwareOverrunErr;
    DWORD dwFramingErr;
    DWORD dwBufferOverrunErr;
    DWORD dwCompressionRatioIn;
    DWORD dwCompressionRatioOut;
} RASI_PORT_1,
*PRASI_PORT_1;
```

**dwPort:** A unique identifier that specifies the port.

**dwConnection:** A unique identifier that specifies the connection.

**dwHardwareCondition:** A [RAS\\_HARDWARE\\_CONDITION \(section 2.2.1.1.5\)](#) value that specifies the condition of a port specified in **dwPort**.

**dwLineSpeed:** Specifies the line speed of the port, represented in bits per second.

**dwBytesXmited:** Specifies the bytes transmitted on the port. This value is the number of bytes of compressed data.

**dwBytesRcvd:** Specifies the bytes received on the port. This value is the number of bytes of compressed data.

**dwFramesXmited:** Specifies the frames transmitted on the port.

**dwFramesRcvd:** Specifies the frames received on the port.

**dwCrcErr:** Specifies the **cyclic redundancy check (CRC)** errors on the port.

**dwTimeoutErr:** Specifies the time-out errors on the port.

**dwAlignmentErr:** Specifies the alignment errors on the port.

**dwHardwareOverrunErr:** Specifies the hardware-overrun errors on the port.

**dwFramingErr:** Specifies the framing errors on the port.

**dwBufferOverrunErr:** Specifies the buffer-overrun errors on the port.

**dwCompressionRatioIn:** Specifies a percentage that indicates the degree to which data received on this connection is compressed. The ratio is the size of the compressed data divided by the size of the same data in an uncompressed state.

**dwCompressionRatioOut:** Specifies a percentage indicating the degree to which data transmitted on this connection is compressed. The ratio is the size of the compressed data divided by the size of the same data in an uncompressed state.

### 2.2.1.2.78 RASI\_CONNECTION\_0

The **RASI\_CONNECTION\_0** structure contains general information regarding a specific connection, such as user name or **domain**.

```
typedef struct _RASI_CONNECTION_0 {
    DWORD dwConnection;
    DWORD dwInterface;
    DWORD dwConnectDuration;
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    DWORD dwConnectionFlags;
    WCHAR wszInterfaceName[257];
    WCHAR wszUserName[257];
    WCHAR wszLogonDomain[16];
    WCHAR wszRemoteComputer[17];
} RASI_CONNECTION_0,
*PRASI_CONNECTION_0;
```

**dwConnection:** Contains the connection handle that specifies a unique identifier of the connection.

**dwInterface:** Contains the interface handle and specifies a unique identifier of the interface through which the connection exists.

**dwConnectDuration:** Specifies the duration of the current connection, in seconds.

**dwInterfaceType:** A [ROUTER\\_INTERFACE\\_TYPE](#) value specifying the interface type of the current connection.

**dwConnectionFlags:** Specifies certain attributes of the connection.

This member can contain the following flags.

Value	Meaning
RAS_FLAGS_PPP_CONNECTION 0x00000001	The connection is using PPP.

Value	Meaning
RAS_FLAGS_MESSENGER_PRESENT 0x00000002	The messenger service is active on the client, and messages can be sent to the client using <a href="#">RRasAdminSendUserMessage (section 3.1.4.36)</a> .
RAS_FLAGS_RAS_CONNECTION 0x00000004	The connection is a NetBIOS connection.
RAS_FLAGS_QUARANTINE_PRESENT 0x00000008	The connection is currently in quarantine. See <a href="#">RRasAdminConnectionRemoveQuarantine (section 3.1.4.43)</a> for more information.
RAS_FLAGS_ARAP_CONNECTION 0x00000010	The connection is using AppleTalk Remote Access Protocol (ARAP). <a href="#">&lt;67&gt;</a>

**wszInterfaceName:** Specifies a null-terminated Unicode string that contains the name of the interface for this connection.

**wszUserName:** Specifies a null-terminated Unicode string that contains the name of the user logged on to the connection.

**wszLogonDomain:** Specifies a null-terminated Unicode string that contains the domain on which the connected user is authenticated.

**wszRemoteComputer:** Specifies a null-terminated Unicode string that contains the name of the remote computer.

### 2.2.1.2.79 RASI\_CONNECTION\_1

The **RASI\_CONNECTION\_1** structure contains detailed statistical information regarding a specific connection, such as error counts and bytes received.

```
typedef struct RASI_CONNECTION_1 {
    DWORD dwConnection;
    DWORD dwInterface;
    PPP_INFO PppInfo;
    DWORD dwBytesXmited;
    DWORD dwBytesRcvd;
    DWORD dwFramesXmited;
    DWORD dwFramesRcvd;
    DWORD dwCrcErr;
    DWORD dwTimeoutErr;
    DWORD dwAlignmentErr;
    DWORD dwHardwareOverrunErr;
    DWORD dwFramingErr;
    DWORD dwBufferOverrunErr;
    DWORD dwCompressionRatioIn;
    DWORD dwCompressionRatioOut;
} RASI_CONNECTION_1,
*PRASI_CONNECTION_1;
```

**dwConnection:** See **dwConnection** in [RASI\\_CONNECTION\\_0 \(section 2.2.1.2.78\)](#).

**dwInterface:** See **dwInterface** in [RASI\\_CONNECTION\\_0](#).

**PppInfo:** A [PPP\\_INFO \(section 2.2.1.2.73\)](#) structure giving the connections details.

**dwBytesXmited:** Specifies the bytes transmitted on the current connection.

**dwBytesRcvd:** Specifies the bytes received on the current connection.

**dwFramesXmited:** Specifies the frames transmitted on the current connection.

**dwFramesRcvd:** Specifies the frames received on the current connection.

**dwCrcErr:** Specifies the CRC errors on the current connection.

**dwTimeoutErr:** Specifies the time-out errors on the current connection.

**dwAlignmentErr:** Specifies the alignment errors on the current connection.

**dwHardwareOverrunErr:** Specifies the number of hardware-overrun errors on the current connection.

**dwFramingErr:** Specifies the number of framing errors for the current connection.

**dwBufferOverrunErr:** Specifies the number of buffer-overrun errors.

**dwCompressionRatioIn:** Specifies a percentage that indicates the degree to which data received on this connection is compressed. The ratio is the size of the compressed data divided by the size of the same data in an uncompressed state.

**dwCompressionRatioOut:** Specifies a percentage that indicates the degree to which data transmitted on this connection is compressed. The ratio is the size of the compressed data divided by the size of the same data in an uncompressed state.

#### 2.2.1.2.80 RASI\_CONNECTION\_2

The **RASI\_CONNECTION\_2** structure contains information for a connection, including the **GUID** that identifies the connection, as defined in [\[MS-DTYP\]](#) section 2.3.2.

```
typedef struct _RASI_CONNECTION_2 {
    DWORD dwConnection;
    WCHAR wszUserName[257];
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    GUID guid;
    PPP_INFO_2 PppInfo2;
} RASI_CONNECTION_2,
*PRASI_CONNECTION_2;
```

**dwConnection:** See **dwConnection** in [RASI\\_CONNECTION\\_0 \(section 2.2.1.2.78\)](#).

**wszUserName:** See **wszUserName** in **RASI\_CONNECTION\_0**.

**dwInterfaceType:** A [ROUTER\\_INTERFACE\\_TYPE \(section 2.2.1.1.1\)](#) that specifies the interface type of the current connection.

**guid:** A GUID uniquely identifying the connection.

**PppInfo2:** A [PPP\\_INFO\\_2 \(section 2.2.1.2.74\)](#) structure that contains information about the PPP negotiation for this connection.

### 2.2.1.2.81 RASI\_CONNECTION\_3

The **RASI\_CONNECTION\_3** structure contains information for a connection, including the GUID that identifies the connection, the **Network Access Protection (NAP)**, and the PPP-related data for the connection. [<68>](#)

```
typedef struct _RASI_CONNECTION_3 {
    DWORD dwVersion;
    DWORD dwSize;
    DWORD dwConnection;
    WCHAR wszUserName[257];
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    GUID guid;
    PPP_INFO_3 PppInfo3;
    RAS_QUARANTINE_STATE rasQuarState;
    FILETIME timer;
} RASI_CONNECTION_3,
*PRASI_CONNECTION_3;
```

**dwVersion:** Determines the version of the **RASI\_CONNECTION\_3** structure used.

**dwSize:** This SHOULD be set to 0. This MAY be used to specify the size, in bytes, of this **RASI\_CONNECTION\_3** structure.

**dwConnection:** Contains the connection handle that specifies a unique identifier of a connection.

**wszUserName:** Specifies a null-terminated Unicode string that contains the name of the user on this connection.

**dwInterfaceType:** A [ROUTER\\_INTERFACE\\_TYPE](#) value that specifies the type of interface.

**guid:** Specifies a GUID that identifies the connection. For an incoming connection, this GUID is valid only as long as the connection is active.

**PppInfo3:** Specifies a [PPP\\_INFO\\_3](#) structure that contains information about the PPP negotiation for this connection. [<69>](#)

**rasQuarState:** Specifies the NAP quarantine state for the connection through the [RAS\\_QUARANTINE\\_STATE \(section 2.2.1.1.3\)](#) that contains the quarantine state of this connection.

**timer:** Specifies the NAP probation time for the connection in the UTC. This value is valid only if the **rasQuarState** has a value of RAS\_QUAR\_STATE\_PROBATION (see [RAS\\_QUARANTINE\\_STATE](#)).

### 2.2.1.2.82 MPRI\_INTERFACE\_0

The **MPRI\_INTERFACE\_0** structure contains information for a particular router interface. This structure is used in the [RRouterInterfaceCreate \(section 3.1.4.13\)](#), [RRouterInterfaceGetInfo \(section 3.1.4.14\)](#), [RRouterInterfaceSetInfo \(section 3.1.4.15\)](#), and [RRouterInterfaceEnum \(section 3.1.4.21\)](#) methods.

```
typedef struct _MPRI_INTERFACE_0 {
    WCHAR wszInterfaceName[257];
```

```

DWORD dwInterface;
BOOL fEnabled;
ROUTER_INTERFACE_TYPE dwIfType;
ROUTER_CONNECTION_STATE dwConnectionState;
DWORD fUnReachabilityReasons;
DWORD dwLastError;
} MPRI_INTERFACE_0,
*PMPRI_INTERFACE_0;

```

**wszInterfaceName:** A null-terminated Unicode string that contains the name of a valid interface. This value **MUST** be specified during the call to RRouterInterfaceCreate and cannot be modified after the interface is created.

**dwInterface:** Specifies a unique identifier of the interface. This is a read-only field that cannot be set or modified.

**fEnabled:** Specifies whether the interface is enabled. The value is greater than 0 (zero) if the interface is enabled, and 0 (zero) if the interface is disabled by **administrators**.

This member can have one of the following values.

Value	Meaning
TRUE >0	The interface is enabled.
FALSE 0	The interface is disabled.

**dwIfType:** A [ROUTER\\_INTERFACE\\_TYPE \(section 2.2.1.1.1\)](#) value that specifies the interface type. This value **MUST** be specified during the call to RRouterInterfaceCreate and cannot be modified after the interface is created.

**dwConnectionState:** A [ROUTER\\_CONNECTION\\_STATE \(section 2.2.1.1.2\)](#) value that specifies the current state of the interface (for example: connected, disconnected, or unreachable). This is a read-only field that cannot be set or modified.

**fUnReachabilityReasons:** Specifies a value that represents a reason the interface cannot be reached. This is a read-only field that cannot be set or modified.

The following table lists constant values that indicate why an interface is unreachable.

Value	Meaning
MPR_INTERFACE_OUT_OF_RESOURCES 0x00000001	No ports or devices are available for use.
MPR_INTERFACE_ADMIN_DISABLED 0x00000002	The administrator has disabled the interface.
MPR_INTERFACE_CONNECTION_FAILURE 0x00000004	The previous connection attempt failed. Look at the dwLastError member for the error code.
MPR_INTERFACE_DIALOUT_HOURS_RESTRICTION	Dialing out is not allowed at the current time.

Value	Meaning
0x00000010	
MPR_INTERFACE_SERVICE_PAUSED 0x00000008	The RRAS is paused.
MPR_INTERFACE_NO_MEDIA_SENSE 0x00000020	The network cable is disconnected from the network card.
MPR_INTERFACE_NO_DEVICE 0x00000040	The network card has been removed from the machine.

**dwLastError:** Specifies a nonzero value if the interface fails to connect. The value is a Win32 error code as specified in [\[MS-ERREF\]](#). This is a read-only field that cannot be set or modified.

### 2.2.1.2.83 MPRI\_INTERFACE\_1

The **MPRI\_INTERFACE\_1** structure contains configuration and status information for a particular router interface. [<70>](#) This structure is used in [RRouterInterfaceGetInfo \(section 3.1.4.14\)](#) and in [RRouterInterfaceSetInfo \(section 3.1.4.15\)](#).

```
typedef struct _MPRI_INTERFACE_1 {
    WCHAR wszInterfaceName[257];
    DWORD dwInterface;
    BOOL fEnabled;
    ROUTER_INTERFACE_TYPE dwIfType;
    ROUTER_CONNECTION_STATE dwConnectionState;
    DWORD fUnReachabilityReasons;
    DWORD dwLastError;
    DWORD dwDialOutHoursRestrictionOffset;
    WCHAR lpwsDialoutHoursRestriction;
} MPRI_INTERFACE_1,
 *PMPRI_INTERFACE_1;
```

**wszInterfaceName:** The same as **wszInterfaceName** in [MPRI\\_INTERFACE\\_0 \(section 2.2.1.2.82\)](#).

**dwInterface:** The same as **dwInterface** in [MPRI\\_INTERFACE\\_0](#).

**fEnabled:** The same as **fEnabled** in [MPRI\\_INTERFACE\\_0](#).

**dwIfType:** The same as **dwIfType** in [MPRI\\_INTERFACE\\_0](#).

**dwConnectionState:** The same as **dwConnectionState** in [MPRI\\_INTERFACE\\_0](#).

**fUnReachabilityReasons:** The same as **fUnReachabilityReasons** in [MPRI\\_INTERFACE\\_0](#).

**dwLastError:** The same as **dwLastError** in [MPRI\\_INTERFACE\\_0](#).

**dwDialOutHoursRestrictionOffset:** Indicates whether **lpwsDialoutHoursRestriction** is specified. It MUST be set to a nonzero value if **lpwsDialoutHoursRestriction** is specified. Otherwise, it MUST be set to 0.

**lpwsDialoutHoursRestriction:** Pointer to a Unicode string that specifies the times during which dial-out is restricted. The format for this string is as follows.



<day><space><time range><space><time range>. . .<NULL><day>. . .<NULL><NULL>

Where <day> is a numeral that corresponds to a day of the week.

Value	Meaning
0	Sunday
1	Monday
2	Tuesday
3	Wednesday
4	Thursday
5	Friday
6	Saturday

<Time range> is of the form HH:MM-HH:MM, using 24-hour notation.

<space> denotes a space character. <NULL> denotes a null character.

The restriction string is terminated by two consecutive null characters.

Example:

```
2 09:00-12:00 13:00-17:30<NULL>4 09:00-12:00 13:00-17:30<NULL><NULL>
```

The preceding string restricts dial-out to Tuesdays and Thursdays from 9:00 A.M. to 12:00 P.M. and from 1:00 P.M. to 5:30 P.M.

#### 2.2.1.2.84 MPRI\_INTERFACE\_2

The **MPRI\_INTERFACE\_2** structure contains data for a router demand-dial interface.<71> This structure is used in [RRouterInterfaceGetInfo \(section 3.1.4.14\)](#) and [RRouterInterfaceCreate \(section 3.1.4.13\)](#).

```
typedef struct _MPRI_INTERFACE_2 {
    WCHAR wszInterfaceName[257];
    DWORD dwInterface;
    BOOL fEnabled;
    ROUTER_INTERFACE_TYPE dwIfType;
    ROUTER_CONNECTION_STATE dwConnectionState;
    DWORD fUnReachabilityReasons;
    DWORD dwLastError;
    DWORD dwfOptions;
    WCHAR szLocalPhoneNumber[129];
    DWORD dwAlternateOffset;
    DWORD ipaddr;
    DWORD ipaddrDns;
    DWORD ipaddrDnsAlt;
    DWORD ipaddrWins;
```

```

DWORD ipaddrWinsAlt;
DWORD dwfNetProtocols;
WCHAR szDeviceType[17];
WCHAR szDeviceName[129];
WCHAR szX25PadType[33];
WCHAR szX25Address[201];
WCHAR szX25Facilities[201];
WCHAR szX25UserData[201];
DWORD dwChannels;
DWORD dwSubEntries;
DWORD dwDialMode;
DWORD dwDialExtraPercent;
DWORD dwDialExtraSampleSeconds;
DWORD dwHangUpExtraPercent;
DWORD dwHangUpExtraSampleSeconds;
DWORD dwIdleDisconnectSeconds;
DWORD dwType;
DWORD dwEncryptionType;
DWORD dwCustomAuthKey;
DWORD dwCustomAuthDataSize;
DWORD dwCustomAuthDataOffset;
GUID guidId;
DWORD dwVpnStrategy;
} MPRI_INTERFACE_2,
*PMPRI_INTERFACE_2;

```

**wszInterfaceName:** Specifies a Unicode string that contains the name of a valid interface. This value **MUST** be specified during the call to the [RRouterInterfaceCreate<72>](#) method and cannot<73> be modified after the interface is created.

**dwInterface:** Specifies a unique identifier of the interface. This is a read-only field and cannot be set or modified.

**fEnabled:** Specifies whether the interface is enabled. The value is greater than zero (0) if the interface is enabled, and zero (0) if the interface is disabled by administrators.

Value	Meaning
TRUE >0	The interface is enabled.
FALSE 0	The interface is disabled.

**dwIfType:** A [ROUTER INTERFACE TYPE \(section 2.2.1.1.1\)](#) value that specifies the type of interface.

**dwConnectionState:** A [ROUTER CONNECTION STATE \(section 2.2.1.1.2\)](#) value that specifies the current state of the interface (for example: connected, disconnected, or unreachable). This is a read-only field and cannot be set or modified.

**fUnReachabilityReasons:** A value that describes the reason that the interface is unreachable. This is a read-only field and cannot be set or modified. The following is the list of possible values.

Value	Meaning
MPR_INTERFACE_ADMIN_DISABLED 0x00000002	The administrator has disabled the interface.
MPR_INTERFACE_CONNECTION_FAILURE 0x00000004	The previous connection attempt failed.
MPR_INTERFACE_DIALOUT_HOURS_RESTRICTION 0x00000010	Dial-out is not allowed at the current time.
MPR_INTERFACE_OUT_OF_RESOURCES 0x00000001	No ports or devices are available for use.
MPR_INTERFACE_SERVICE_PAUSED 0x00000008	The service is paused.
MPR_INTERFACE_NO_MEDIA_SENSE 0x00000020	The network cable is disconnected from the network card.
MPR_INTERFACE_NO_DEVICE 0x00000040	The network card has been removed from the machine.

**dwLastError:** Contains a nonzero value if the interface fails to connect. This value is a Win32 error code as defined in [\[MS-ERREF\]](#). This is a read-only field and cannot be set or modified.

**dwfOptions:** A value that specifies the bit flags that are used to set connection options.

This value MUST be a combination of the flags listed in the following table.

Value	Meaning
MPRIO_SpecificIpAddr 0x00000002	If this flag is set, the RRAS server attempts to use the IP address specified by the <code>ipaddr</code> field as the IP address for the dial-up connection. If this flag is not set, the value of the <code>ipaddr</code> member is ignored.
MPRIO_SpecificNameServers 0x00000004	If this flag is set, the RRAS server uses the <b>ipaddrDns</b> , <b>ipaddrDnsAlt</b> , <b>ipaddrWins</b> , and <b>ipaddrWinsAlt</b> members to specify the name server addresses for the dial-up connection. If this flag is not set, the RRAS server ignores these members.
MPRIO_IpHeaderCompression 0x00000008	If this flag is set, the RRAS server negotiates to use the IP header compression on PPP connections. The IP header compression can significantly improve performance.  If this flag is not set, the IP header compression is not negotiated.
MPRIO_RemoteDefaultGateway 0x00000010	If this flag is set, the default route for the IP packets is through the dial-up adapter when the connection is active. If this flag is cleared, the default route is not modified.
MPRIO_DisableLcpExtensions 0x00000020	If this flag is set, the PPP LCP extensions defined in <a href="#">[RFC1570]</a> are disabled for the connection associated with the interface. This flag MUST not be set, unless interoperating with some older PPP implementations that do not support LCP extensions.
MPRIO_SwCompression	If this flag is set, software compression is negotiated on the link.

Value	Meaning
0x00000200	Setting this flag causes the PPP to attempt to negotiate a Compression Control Protocol (CCP) with the server. This flag SHOULD be set by default, but clearing it can reduce the negotiation period if the server does not support a compatible compression protocol.
MPRIO_RequireEncryptedPw 0x00000400	If this flag is set, only secure password schemes can be used to authenticate the client with the server. This prevents the PPP from using the PAP plaintext authentication protocol to authenticate the client. However, the <a href="#">[MS-CHAP]</a> , MD5-CHAP, and SPAP authentication protocols are supported. For increased security, set this flag. For increased interoperability, clear this flag.
MPRIO_RequireMsEncryptedPw 0x00000800	If this flag is set, it prevents the PPP from using the PAP plaintext authentication protocol, MD5-CHAP, or SPAP. For increased security, set this flag. For increased interoperability, clear this flag. This flag takes precedence over MPRIO_RequireEncryptedPw.
MPRIO_RequireDataEncryption 0x00001000	If this flag is set, data encryption must be negotiated successfully or the connection is dropped. This flag is ignored unless MPRIO_RequireMsEncryptedPw is also set.
MPRIO_UseLogonCredentials 0x00004000	If this flag is set, the RRAS server uses the user name, password, and domain of the currently logged-on user when dialing this entry. This flag is ignored unless MPRIO_RequireMsEncryptedPw is also set.
MPRIO_PromoteAlternates 0x00008000	This flag has an effect when alternate phone numbers are defined by the szAlternates member. If this flag is set, an alternate phone number that connects successfully becomes the primary phone number, and the current primary phone number is moved to the alternate list.
MPRIO_SecureLocalFiles 0x00010000	If this flag is set, the RRAS server checks for an existing remote file system and remote printer bindings before making a connection with this entry. Typically, this flag is set on phone book entries for public networks to remind users to break connections to their private network before connecting to a public network.
MPRIO_RequireEAP 0x00020000	If this flag is set, Extensible Authentication Protocol (EAP) must be supported for authentication.
MPRIO_RequirePAP 0x00040000	If this flag is set, Password Authentication Protocol (PAP) must be supported for authentication.
MPRIO_RequireSPAP 0x00080000	If this flag is set, Shiva's Password Authentication Protocol (SPAP) must be supported for authentication. <a href="#">&lt;74&gt;</a>
MPRIO_SharedPhoneNumbers 0x00800000	This flag is not used.
MPRIO_RequireCHAP 0x08000000	If this flag is set, the Challenge Handshake Authentication Protocol (CHAP) must be supported for authentication.

Value	Meaning
MPRIO_RequireMsCHAP 0x10000000	If this flag is set, the Microsoft Challenge Handshake Authentication Protocol [MS-CHAP] must be supported for authentication. <a href="#">&lt;75&gt;</a>
MPRIO_RequireMsCHAP2 0x20000000	If this flag is set, version 2 of the [MS-CHAP] must be supported for authentication.
MPRIO_IpSecPreSharedKey 0x80000000	Configured the demand-dial interface to use preshared key.

**szLocalPhoneNumber:** A null-terminated Unicode string that contains the local telephone number or the destination IP, IPv4, or IPv6 address.

**dwAlternateOffset:** Offset from the beginning of this structure where the alternate phone numbers are stored. If no alternate phone number is available, this value MUST be set to 0. Alternate phone numbers are a list of consecutive null-terminated Unicode strings. The last string is terminated by two consecutive null characters. The strings are alternate phone numbers that the router dials, in the order listed, if the primary number fails to connect. For more information, see the description of **szLocalPhoneNumber**. The alternate phone numbers MUST be stored after the CustomAuthData field that is appended at the end of this structure.

**ipaddr:** A value that specifies the IP address to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificIpAddr flag.

**ipaddrDns:** A value that specifies the IP address of the DNS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**ipaddrDnsAlt:** A value that specifies the IP address of a secondary or backup DNS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**ipaddrWins:** A value that specifies the IP address of the WINS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**ipaddrWinsAlt:** A value that specifies the IP address of a secondary WINS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**dwfNetProtocols:** A value that specifies the network protocols to negotiate. This member can be a combination of the following flags.

Value	Meaning
MPRNP_Ipx 0x00000002	Negotiate the IPX protocol. <a href="#">&lt;76&gt;</a>
MPRNP_Ip 0x00000004	Negotiate the TCP/IPv4 protocol.
MPRNP_Ipv6 0x00000008	Negotiate the TCP/IPv6 protocol. <a href="#">&lt;77&gt;</a>

**szDeviceType:** A value that specifies a null-terminated Unicode string that indicates the RRAS server device type that is referenced by **szDeviceName**. This is a read-only field that is computed based on the value of **szDeviceName**.

This member can be one of the following string constants.

Value	Meaning
MPRDT_Modem "Modem"	A modem that is accessed through a COM port.
MPRDT_Isdn "Isdn"	An ISDN adapter with the corresponding NDISWAN driver installed.
MPRDT_X25 "x25"	An X.25 adapter with the corresponding NDISWAN driver installed.
MPRDT_Vpn "Vpn"	A virtual private network (VPN) connection.
MPRDT_Pad "Pad"	A packet assembler/disassembler.
MPRDT_Generic "GENERIC"	Generic.
MPRDT_Serial "SERIAL"	Direct serial connection through a serial port.
MPRDT_FrameRelay "FRAMERELAY"	Frame relay.
MPRDT_Atm "ATM"	Asynchronous transfer mode.
MPRDT_Sonet "SONET"	Sonet.
MPRDT_SW56 "SW56"	Switched 56K access.
MPRDT_Irda "IRDA"	An Infrared Data Association (IrDA)-compliant device.
MPRDT_Parallel "PARALLEL"	Direct parallel connection through a parallel port.

**szDeviceName:** Specifies a null-terminated Unicode string that contains the name of a telephony application programming interface (TAPI) device to use with this phone book entry, for example, "Fabrikam Inc 28800 External". To enumerate all available RAS-capable devices, use the [RRouterDeviceEnum \(section 3.1.4.37\)](#) function.

**szX25PadType:** A data type that contains a null-terminated Unicode string that identifies the X.25 PAD type. This value SHOULD be set to an empty string ("") unless the entry dials using an X.25 PAD. [<78><79>](#)

**szX25Address:** Contains a null-terminated Unicode string that identifies the X.25 address to connect to. This value SHOULD be set to an empty string (""), unless the entry SHOULD dial using an X.25 PAD or native X.25 device. [<80>](#)

**szX25Facilities:** Contains a null-terminated Unicode string that specifies the facilities to request from the X.25 host at connection time. This member is ignored if **szX25Address** is an empty string ("").

**szX25UserData:** Contains a null-terminated Unicode string that specifies additional connection data supplied to the X.25 host at connection time. This member is ignored if **szX25Address** is an empty string ("").

**dwChannels:** Not used and MUST be set to zero.

**dwSubEntries:** A value that specifies the number of multilink subentries associated with this entry. This is a read-only field that cannot be set or modified. Multilink subentries can be added and configured as described in [3.1.4.40](#). Multilink subentries can be removed by updating the Media section of the phonebook file as specified in [2.2.2.2.96](#).

**dwDialMode:** Indicates whether the RRAS server dials all of this entry's multilink subentries when the entry is first connected.

This member can be one of the following values.

Value	Meaning
0x00000000	Dial the first available device only.
MPRDM_DialAll 0x00000001	Dial all subentries initially.
MPRDM_DialAsNeeded 0x00000002	Adjust the number of subentries as bandwidth is required. The RRAS server uses the <b>dwDialExtraPercent</b> , <b>dwDialExtraSampleSeconds</b> , <b>dwDialHangUpExtraPercent</b> , and <b>dwHangUpExtraSampleSeconds</b> members to determine when to dial or disconnect a subentry. <a href="#">&lt;81&gt;</a>

**dwDialExtraPercent:** A value that specifies the percentage of the total bandwidth that is available from the currently connected subentries. The RRAS server dials an additional subentry when the total bandwidth that is used exceeds the percentage limit (**dwDialExtraPercent**) of the available bandwidth for at least **dwDialExtraSampleSeconds** seconds.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwDialExtraSampleSeconds:** A value that specifies the time, in seconds, for which current bandwidth usage must exceed the threshold that is specified by **dwHangUpExtraSampleSeconds** before the RRAS server dials an additional subentry.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwHangUpExtraPercent:** A value that specifies the percentage of the total bandwidth that is available from the currently connected subentries. The RRAS server terminates (hangs up) an existing subentry connection when the total bandwidth used is less than the percentage limit, indicated by **dwHangUpExtraPercent**, of the available bandwidth for at least **dwHangUpExtraSampleSeconds** seconds.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwHangUpExtraSampleSeconds:** A value that specifies the time, in seconds, for which current bandwidth usage must be less than the threshold that is specified by **dwHangUpExtraPercent** before the RRAS server terminates an existing subentry connection.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwIdleDisconnectSeconds:** A value that specifies the time, in seconds, after which an idle connection is terminated. Unless the idle time-out is disabled, the entire connection is terminated if the connection is idle for the specified **dwIdleDisconnectSeconds**. This member can specify either a time-out value or one of the following values.

Value	Meaning
MPRIDS_Disabled 0xffffffff	There is no idle time-out for this connection.
MPRIDS_UseGlobalValue 0x00000000	Use the user preference value as the default.

**dwType:** A value that specifies the type of phone book entry. This is a read-only field and specifies the type of entry based on the value of the **szDeviceType** member.

This member can be one of the following types.

Value	Meaning
MPRET_Phone 0x1	Phone line (for example: modem, ISDN, or X.25).
MPRET_Vpn 0x2	Virtual private network (VPN).
MPRET_Direct 0x3	Direct serial or parallel connection. <a href="#82">&lt;82&gt;</a>

**dwEncryptionType:** A value that specifies the type of encryption to use for Microsoft Point-to-Point Encryption (MPPE) with the connection.

This member can be one of the following values.

Value	Meaning
MPR_ET_None 0x0	Do not use encryption.
MPR_ET_Require 0x1	Use encryption.
MPR_ET_RequireMax 0x2	Use maximum-strength encryption.



Value	Meaning
MPR_ET_Optional 0x3	If possible, use encryption.

The value of the **dwEncryptionType** does not affect how passwords are encrypted. Whether passwords are encrypted and how passwords are encrypted is determined by the authentication protocol (for example: PAP, [MS-CHAP], or EAP).

**dwCustomAuthKey:** A value that specifies the authentication key to be provided to an EAP vendor.

**dwCustomAuthDataSize:** A value that specifies the size of the data pointed to by the **lpbCustomAuthData** member.

**dwCustomAuthDataOffset:** Offset from the beginning of this structure where the CustomAuthData is stored. If CustomAuthData is not specified, it MUST be set to 0. CustomAuthData is the authentication data to use with EAP. CustomAuthData MUST be appended to the end of this structure.

**guidId:** The GUID that represents this phone book entry. This member is read-only.

**dwVpnStrategy:** The VPN strategy to use when dialing a VPN connection.

This member can have one of the following values.

Value	Meaning
MPR_VS_Default 0x0	The RRAS server dials the PPTP first. If the PPTP fails, the L2TP is attempted. The protocol that succeeds is tried first in subsequent dialing for this entry.
MPR_VS_PptpOnly 0x1	The RRAS server dials only the PPTP.
MPR_VS_PptpFirst 0x2	The RRAS server always dials the PPTP first and the L2TP second.
MPR_VS_L2tpOnly 0x3	The RRAS server dials only the L2TP.
MPR_VS_L2tpFirst 0x4	The RRAS server dials the L2TP first and the PPTP second.

#### 2.2.1.2.85 MPRI\_INTERFACE\_3

The **MPRI\_INTERFACE\_3** structure contains data for a router demand-dial interface. [<83>](#) This structure is used in [RRouterInterfaceCreate \(section 3.1.4.13\)](#) and [RRouterInterfaceGetInfo \(section 3.1.4.14\)](#).

```
typedef struct _MPRI_INTERFACE_3 {
    WCHAR wszInterfaceName[257];
    DWORD dwInterface;
    BOOL fEnabled;
    ROUTER_INTERFACE_TYPE dwIfType;
    ROUTER_CONNECTION_STATE dwConnectionState;
    DWORD fUnReachabilityReasons;
```

```

DWORD dwLastError;
DWORD dwfOptions;
WCHAR szLocalPhoneNumber[129];
DWORD dwAlternateOffset;
DWORD ipaddr;
DWORD ipaddrDns;
DWORD ipaddrDnsAlt;
DWORD ipaddrWins;
DWORD ipaddrWinsAlt;
DWORD dwfNetProtocols;
WCHAR szDeviceType[17];
WCHAR szDeviceName[129];
WCHAR szX25PadType[33];
WCHAR szX25Address[201];
WCHAR szX25Facilities[201];
WCHAR szX25UserData[201];
DWORD dwChannels;
DWORD dwSubEntries;
DWORD dwDialMode;
DWORD dwDialExtraPercent;
DWORD dwDialExtraSampleSeconds;
DWORD dwHangUpExtraPercent;
DWORD dwHangUpExtraSampleSeconds;
DWORD dwIdleDisconnectSeconds;
DWORD dwType;
DWORD dwEncryptionType;
DWORD dwCustomAuthKey;
DWORD dwCustomAuthDataSize;
DWORD dwCustomAuthDataOffset;
GUID guidId;
DWORD dwVpnStrategy;
ULONG AddressCount;
IN6_ADDR ipv6addrDns;
IN6_ADDR ipv6addrDnsAlt;
IN6_ADDR* ipv6addr;
} MPRI_INTERFACE_3,
*PMPRI_INTERFACE_3;

```

**wszInterfaceName:** A pointer to a Unicode string that contains the name of the interface. This value **MUST** be specified during the call to the RRouterInterfaceCreate<84> method and cannot<85> be modified after the interface is created.

**dwInterface:** Specifies a unique identifier of the interface. This is a read-only field and cannot be set or modified.

**fEnabled:** Specifies whether the interface is enabled. The value is greater than 0 (zero) if the interface is enabled, and 0 (zero) if the interface is disabled by administrators.

Value	Meaning
TRUE >0	The interface is enabled.
FALSE 0	The interface is disabled.

**dwIfType:** A [ROUTER\\_INTERFACE\\_TYPE \(section 2.2.1.1.1\)](#) value specifying the type of interface.

**dwConnectionState:** A [ROUTER\\_CONNECTION\\_STATE \(section 2.2.1.1.2\)](#) value specifying the current state of the interface (for example: connected, disconnected, or unreachable). This is a read-only field and cannot be set or modified.

**fUnReachabilityReasons:** A value that describes the reason why the interface is unreachable. This is a read-only field and cannot be set or modified.

The following table has the list of possible values.

Value	Meaning
MPR_INTERFACE_ADMIN_DISABLED 0x00000002	The administrator has disabled the interface.
MPR_INTERFACE_CONNECTION_FAILURE 0x00000004	The previous connection attempt failed.
MPR_INTERFACE_DIALOUT_HOURS_RESTRICTION 0x00000010	Dial-out is not allowed at the current time.
MPR_INTERFACE_OUT_OF_RESOURCES 0x00000001	No ports or devices are available for use.
MPR_INTERFACE_SERVICE_PAUSED 0x00000008	The service is paused.
MPR_INTERFACE_NO_MEDIA_SENSE 0x00000020	The network cable is disconnected from the network card.
MPR_INTERFACE_NO_DEVICE 0x00000040	The network card has been removed from the machine.

**dwLastError:** A value that contains a nonzero value if the interface fails to connect. This value is a Win32 error code as defined in [\[MS-ERREF\]](#). This is a read-only field and cannot be set or modified.

**dwfOptions:** A value that specifies bit flags used to set connection options.

MUST be a combination of the flags listed in the following table.

Value	Meaning
MPRIO_SpecificIpAddr 0x00000002	If this flag is set, the RRAS server attempts to use the IP address specified by the <b>ipaddr</b> field as the IP address for the dial-up connection. If this flag is not set, the value of the <b>ipaddr</b> member is ignored.
MPRIO_SpecificNameServers 0x00000004	If this flag is set, the RRAS server uses the <b>ipaddrDns</b> , <b>ipaddrDnsAlt</b> , <b>ipaddrWins</b> , and <b>ipaddrWinsAlt</b> members to specify the name server addresses for the dial-up connection. If this flag is not set, the RRAS server ignores these members.
MPRIO_IpHeaderCompression 0x00000008	If this flag is set, the RRAS server negotiates to use the IP header compression on the PPP connections. The IP header

Value	Meaning
	compression can significantly improve performance. If this flag is not set, the IP header compression is not negotiated.
MPRIO_RemoteDefaultGateway 0x00000010	If this flag is set, the default route for the IP packets is through the dial-up adapter when the connection is active. If this flag is cleared, the default route is not modified.
MPRIO_DisableLcpExtensions 0x00000020	If this flag is set, the RRAS server disables the PPP LCP extensions defined in <a href="#">RFC1570</a> . Disabling the PPP LCP extensions may be necessary to connect to certain older PPP implementations, but it interferes with features such as server callback. This flag MUST NOT be set unless it is specifically required.
MPRIO_SwCompression 0x00000200	If this flag is set, software compression is negotiated on the link. Setting this flag causes the PPP to attempt to negotiate the CCP with the server. This flag SHOULD be set by default, but clearing it can reduce the negotiation period if the server does not support a compatible compression protocol.
MPRIO_RequireEncryptedPw 0x00000400	If this flag is set, only secure password schemes can be used to authenticate the client with the server. This prevents the PPP from using the PAP plaintext authentication protocol to authenticate the client. However, the <a href="#">MS-CHAP</a> , MD5-CHAP, and SPAP authentication protocols are supported. For increased security, set this flag. For increased interoperability, clear this flag.
MPRIO_RequireMsEncryptedPw 0x00000800	If this flag is set, only the Microsoft secure password schemes can be used to authenticate the client with the server. This prevents the PPP from using the PAP plaintext authentication protocol, MD5-CHAP, or SPAP. For increased security, set this flag. For increased interoperability, clear this flag. This flag takes precedence over MPRIO_RequireEncryptedPw.
MPRIO_RequireDataEncryption 0x00001000	If this flag is set, data encryption must be negotiated successfully or the connection is dropped. This flag is ignored unless MPRIO_RequireMsEncryptedPw is also set.
MPRIO_UseLogonCredentials 0x00004000	If this flag is set, the RRAS server uses the user name, password, and domain of the currently logged-on user when dialing this entry. This flag is ignored unless MPRIO_RequireMsEncryptedPw is also set.
MPRIO_PromoteAlternates 0x00008000	This flag has an effect when alternate phone numbers are defined by the szAlternates member. If this flag is set, an alternate phone number that connects successfully becomes the primary phone number, and the current primary phone number is moved to the alternate list.
MPRIO_SecureLocalFiles 0x00010000	If this flag is set, the RRAS server checks for an existing remote file system and remote printer bindings before making a connection with this entry. Typically, this flag is set on phone book entries for public networks to remind users to break connections to their private network before connecting to a public network.

Value	Meaning
MPRIO_RequireEAP 0x00020000	If this flag is set, Extensible Authentication Protocol (EAP) must be supported for authentication.
MPRIO_RequirePAP 0x00040000	If this flag is set, Password Authentication Protocol (PAP) must be supported for authentication. <a href="#">.&lt;86&gt;</a>
MPRIO_RequireSPAP 0x00080000	If this flag is set, Shiva's Password Authentication Protocol (SPAP) must be supported for authentication. <a href="#">.&lt;87&gt;</a>
MPRIO_SharedPhoneNumbers 0x00800000	If this flag is set, phone numbers are shared.
MPRIO_RequireCHAP 0x08000000	If this flag is set, the Challenge Handshake Authentication Protocol (CHAP) must be supported for authentication. <a href="#">.&lt;88&gt;</a>
MPRIO_RequireMsCHAP 0x10000000	If this flag is set, the Microsoft Challenge Handshake Authentication Protocol [MS-CHAP] must be supported for authentication. <a href="#">.&lt;89&gt;</a>
MPRIO_RequireMsCHAP2 0x20000000	If this flag is set, version 2 of the [MS-CHAP] must be supported for authentication.
MPRIO_IpSecPreSharedKey 0x80000000	Configured the demand-dial interface to use preshared key.

**szLocalPhoneNumber:** A value that specifies a null-terminated Unicode string that contains a telephone number.

**dwAlternateOffset:** The offset from the beginning of this structure where the alternate phone numbers are stored. If no alternate phone number is available, this value MUST be set to 0. Alternate phone numbers are a list of consecutive null-terminated Unicode strings. The last string is terminated by two consecutive null characters. The strings are alternate phone numbers that the router dials, in the order listed, if the primary number fails to connect. For more information, see **szLocalPhoneNumber**. The alternate phone numbers MUST be stored after the custom data that is appended to this structure.

**ipaddr:** A value that specifies the IP address to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificIpAddr flag.

**ipaddrDns:** A value that specifies the IP address of the DNS server to be used while this connection is active. This member is ignored unless dwfOptions specifies the MPRIO\_SpecificNameServers flag.

**ipaddrDnsAlt:** A value that specifies the IP address of a secondary or backup DNS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**ipaddrWins:** A value that specifies the IP address of the WINS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**ipaddrWinsAlt:** A value that specifies the IP address of a secondary WINS server to be used while this connection is active. This member is ignored unless **dwfOptions** specifies the MPRIO\_SpecificNameServers flag.

**dwfNetProtocols:** A value that specifies the network protocols to negotiate.

This member can be a combination of the following flags.

Value	Meaning
MPRNP_Ipx 0x00000002	Negotiate the IPX protocol.
MPRNP_Ip 0x00000004	Negotiate the TCP/IPv4 protocol.
MPRNP_Ipv6 0x00000008	Negotiate the TCP/IPv6 protocol.

**szDeviceType:** A value that specifies a null-terminated Unicode string that indicates the RRAS server device type that is referenced by **szDeviceName**. This is a read-only field that is computed based on the value of the **szDeviceName** member. The possible values for this member are the same as the **wszDeviceName** defined in **RASI\_PORT\_0**.

**szDeviceName:** Contains a null-terminated Unicode string that contains the name of a TAPI device to use with this phone book entry (for example, "Fabrikam Inc 28800 External"). To enumerate all available RAS-capable devices, use the [RRouterDeviceEnum](#) function.

**szX25PadType:** A data type that contains a null-terminated Unicode string that identifies the X.25 PAD type. This value SHOULD be set to an empty string (""), unless the entry dials using an X.25 PAD. [<90><91>](#)

**szX25Address:** Contains a null-terminated Unicode string that identifies the X.25 address to connect to. This value SHOULD be set to an empty string (""), unless the entry dials using an X.25 PAD or native X.25 device. [<92>](#)

**szX25Facilities:** Contains a null-terminated Unicode string that specifies the facilities to request from the X.25 host at connection time. This member is ignored if **szX25Address** is an empty string ("").

**szX25UserData:** Contains a null-terminated Unicode string that specifies the additional connection data supplied to the X.25 host at connection time. This member is ignored if **szX25Address** is an empty string ("").

**dwChannels:** Reserved for future use.

**dwSubEntries:** A value that specifies the number of multilink subentries associated with this entry. This is a read-only field and cannot be set or modified. Multilink entries SHOULD be specified by updating the Media section of the phonebook file as specified in [2.2.2.2.96](#).

**dwDialMode:** Indicates whether the RRAS server needs to dial all of this entry's multilink subentries when the entry is first connected.

This member can be one of the following values.

Value	Meaning
0x00000000	Dial the first available device only.
MPRDM_DialAll	Dial all subentries initially.

Value	Meaning
0x00000001	
MPRDM_DialAsNeeded 0x00000002	Adjust the number of subentries as bandwidth is required. The RRAS server uses the <b>dwDialExtraPercent</b> , <b>dwDialExtraSampleSeconds</b> , <b>dwDialHangUpExtraPercent</b> , and <b>dwHangUpExtraSampleSeconds</b> members to determine when to dial or disconnect a subentry. <a href="#93">&lt;93&gt;</a>

**dwDialExtraPercent:** A value that specifies the percentage of the total bandwidth that is available from the currently connected subentries. The RRAS server dials an additional subentry when the total bandwidth that is used exceeds **dwDialExtraPercent** percent of the available bandwidth for at least **dwDialExtraSampleSeconds** seconds.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwDialExtraSampleSeconds:** A value that specifies the time, in seconds, for which current bandwidth usage must exceed the threshold that is specified by **dwDialExtraPercent** before the RRAS server dials an additional subentry.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded.

**dwHangUpExtraPercent:** A value that specifies the percentage of the total bandwidth that is available from the currently connected subentries. The RRAS server terminates (hangs up) an existing subentry connection when the total bandwidth used is less than **dwHangUpExtraPercent** percent of the available bandwidth for at least **dwHangUpExtraSampleSeconds** seconds.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwHangUpExtraSampleSeconds:** A value that specifies the time, in seconds, for which current bandwidth usage must be less than the threshold that is specified by **dwHangUpExtraPercent** before the RRAS server terminates an existing subentry connection.

This member is ignored unless the **dwDialMode** member specifies the MPRDM\_DialAsNeeded flag.

**dwIdleDisconnectSeconds:** A value that specifies the time, in seconds, after which an inactive connection is terminated. Unless the idle time-out is disabled, the entire connection is terminated if the connection is idle for the specified interval.

This member can specify either a time-out value or one of the following values.

Value	Meaning
MPRIDS_Disabled 0xffffffff	There is no idle time-out for this connection.
MPRIDS_UseGlobalValue 0x00000000	Use the user preference value as the default.

**dwType:** A value that specifies the type of phone book entry. This is a read-only field that is calculated based on the value of the **szDeviceType** member.

This member can be one of the following types.

Value	Meaning
MPRET_Phone 0x00000001	Phone line (for example: modem, ISDN, or X.25).
MPRET_Vpn 0x00000002	Virtual private network (VPN).
MPRET_Direct 0x00000003	Direct serial or parallel connection.

**dwEncryptionType:** A value that specifies the type of encryption to use for Microsoft Point-to-Point Encryption (MPPE) with the connection.

This member can be one of the following values.

Value	Meaning
MPR_ET_None 0x00000000	Do not use encryption.
MPR_ET_Require 0x00000001	Use encryption.
MPR_ET_RequireMax 0x00000002	Use maximum-strength encryption.
MPR_ET_Optional 0x00000003	If possible, use encryption.

The value of **dwEncryptionType** does not affect how passwords are encrypted. Whether passwords are encrypted and how passwords are encrypted is determined by the authentication protocol, for example: PAP, MS-CHAP, or EAP.

**dwCustomAuthKey:** A value that specifies the authentication key to be provided to an EAP ([\[MS-PEAP\]](#)) vendor.

**dwCustomAuthDataSize:** A value that specifies the size of the data pointed to by the **lpbCustomAuthData** member.

**dwCustomAuthDataOffset:** The offset from the beginning of this structure where the CustomAuthData is stored. If CustomAuthData are not specified, this member MUST be set to 0. CustomAuthData is the authentication data to use with EAP [MS-PEAP]. CustomAuthData MUST be appended to the end of this structure.

**guidId:** The GUID that represents this phone book entry. This member is read-only.

**dwVpnStrategy:** The VPN strategy to use when dialing a VPN connection.

This member can have one of the following values.

Value	Meaning
MPR_VS_Default	The RRAS server dials the PPTP first. If the PPTP fails, the L2TP is attempted.



Value	Meaning
0x00000000	The protocol that succeeds is tried first in subsequent dialing for this entry.
MPR_VS_PptpOnly 0x00000001	The RRAS server dials only the PPTP.
MPR_VS_PptpFirst 0x00000002	The RRAS server always dials the PPTP first and the L2TP second.
MPR_VS_L2tpOnly 0x00000003	The RRAS server dials only the L2TP.
MPR_VS_L2tpFirst 0x00000004	The RRAS server dials the L2TP first and the PPTP second.

**AddressCount:** Not used.

**ipv6addrDns:** A value that specifies the IP address of the DNS server to be used while this connection is active.

**ipv6addrDnsAlt:** A value that specifies the IP address of a secondary or backup DNS server to be used while this connection is active.

**ipv6addr:** Not used.

#### 2.2.1.2.86 MPR\_DEVICE\_0

The **MPR\_DEVICE\_0** structure stores information about a device used for a link in a multilinked demand-dial interface.

```
typedef struct _MPR_DEVICE_0 {
    WCHAR szDeviceType[17];
    WCHAR szDeviceName[129];
} MPR_DEVICE_0,
*PMPR_DEVICE_0;
```

**szDeviceType:** Specifies a null-terminated Unicode string that indicates the RRAS server device type referenced by **szDeviceName**. See [MPRI INTERFACE 2 \(section 2.2.1.2.84\)](#) for a list of possible device types.

**szDeviceName:** Specifies a null-terminated Unicode string that contains the name of the TAPI device to use with this phone book entry.

#### 2.2.1.2.87 MPR\_DEVICE\_1

The **MPR\_DEVICE\_1** structure stores information about a device used for a link in a multilinked demand-dial interface. In addition to the information in [MPR\\_DEVICE\\_0 \(section 2.2.1.2.86\)](#), **MPR\_DEVICE\_1** contains phone number information.

```
typedef struct _MPR_DEVICE_1 {
    WCHAR szDeviceType[17];
    WCHAR szDeviceName[129];
    WCHAR szLocalPhoneNumber[129];
    PWCHAR szAlternates;
```

```

} MPR_DEVICE_1,
*PMPR_DEVICE_1;

```

**szDeviceType:** Specifies a null-terminated Unicode string that indicates the device type referenced by **szDeviceName**. See [MPRI INTERFACE 2 \(section 2.2.1.2.84\)](#) for a list of possible device types.

**szDeviceName:** Specifies a null-terminated Unicode string that contains the name of the TAPI device to use with this phone book entry.

**szLocalPhoneNumber:** Specifies a null-terminated Unicode string that contains a telephone number. The router uses the **szLocalPhoneNumber** string as the entire phone number.

**szAlternates:** Pointer to a list of consecutive null-terminated Unicode strings. The last string is terminated by two consecutive null characters. The strings are alternate phone numbers that the router dials in the order listed if the primary number (see **szLocalPhoneNumber**) fails to connect.

### 2.2.1.2.88 MPR\_CREDENTIALSEX\_1

The **MPR\_CREDENTIALSEX\_1** structure contains extended credentials information (other than username/password), such as the information used by Extensible Authentication Protocols (EAPs) or a preshared key based on the level being passed in by the methods that use this structure. This structure is used in [RRouterInterfaceSetCredentialsEx \(section 3.1.4.41\)](#) and [RRouterInterfaceGetCredentialsEx \(section 3.1.4.42\)](#). If a preshared key is being used **dwSsize** MUST be less than 257. Note that the preshared key here is used to specify the credential for the connection endpoint on the RRAS server. The other end of the connection endpoint MUST be configured with the same preshared key in order for the connection to be successful.

```

typedef struct _MPR_CREDENTIALSEXI {
    DWORD dwSize;
    DWORD dwOffset;
    BYTE bData[1];
} MPR_CREDENTIALSEX_1,
*PMPR_CREDENTIALSEX_1;

```

**dwSize:** Specifies the size of the data pointed to by the **bData** member. If dwSize is zero in a call to [RRouterInterfaceSetCredentialsEx](#) and the key is a preshared key, the key is deleted.

**dwOffset:** Offset where the data starts in the structure.

**bData:** Pointer to the credential information. Note that bData[1] is only a placeholder and the actual data of size **dwSize** is stored at the end of the structure. The actual value stored here can be either a preshared key or the EAP information [EAPTLS\\_USER\\_PROPERTIES \(section 2.2.1.2.129\)](#).

### 2.2.1.2.89 IFFILTER\_INFO

The **IFFILTER\_INFO** structure is used to specify the filter settings for an interface. When this structure is encapsulated within the [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) structure, the **InfoType** value used MUST be 0xffff000d or 0xffff00014.

```
typedef struct _IFFILTER_INFO {
    BOOL bEnableFragChk;
} IFFILTER_INFO,
*PIFFILTER_INFO;
```

**bEnableFragChk:** When this field is set to TRUE, the fragmented packets are filtered at the interface and dropped. If this field is set to FALSE, the fragment checking is not done at the interface.

Value	Meaning
TRUE	Fragment checking is done at the interface.
FALSE	Fragment checking is not done at the interface.

#### 2.2.1.2.90 MPR\_FILTER\_0

The **MPR\_FILTER\_0** structure is used to specify whether RRAS server filtering is enabled or not. When this structure is encapsulated within [RTR TOC ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0xffff0015 or 0xffff0016.

```
typedef struct _MPR_FILTER_0 {
    BOOL fEnable;
} MPR_FILTER_0,
*PMPR_FILTER_0;
```

**fEnable:** This MUST be set to 0x00000001 to enable filtering on the RRAS server and MUST be set to 0x00000000 to disable filtering.

Value	Meaning
0x00000000	Disable filtering.
0x00000001	Enable filtering.

#### 2.2.1.2.91 IPX\_GLOBAL\_INFO

The **IPX\_GLOBAL\_INFO**<sup><94></sup> structure is used to give the global IPX information for the RRAS server. When this structure is encapsulated in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0x00000009.

```
typedef struct _IPX_GLOBAL_INFO {
    ULONG RoutingTableHashSize;
    ULONG EventLogMask;
} IPX_GLOBAL_INFO,
*PIPX_GLOBAL_INFO;
```

**RoutingTableHashSize:** The hash size of the IPX routing table.

**EventLogMask:** Mask to manage event logging on the IPX interface on the RRAS server.

#### 2.2.1.2.92 IPX\_IF\_INFO

The **IPX\_IF\_INFO** [<95>](#) structure is used to specify the IPX interface data. When this structure is encapsulated in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0x00000001.

```
typedef struct _IPX_IF_INFO {
    ULONG AdministratorState;
    ULONG NetbiosAccept;
    ULONG NetbiosDeliver;
} IPX_IF_INFO,
*PIPX_IF_INFO;
```

**AdministratorState:** This MUST be set to the desired state of the interface. A value of 0x00000001 disables the interface and a value of 0x00000002 enables the interface.

**NetbiosAccept:** This MUST be set to 0x00000001 for the interface to accept NetBIOS broadcast packets.

**NetbiosDeliver:** This MUST be set to 0x00000001 on a LAN interface and 0x00000000 on a WAN interface.

Value	Meaning
0x00000000	WAN interface
0x00000001	LAN interface

#### 2.2.1.2.93 IPXWAN\_IF\_INFO

The **IPXWAN\_IF\_INFO** [<96>](#) structure is used to specify the IPX interface data for the WAN interface. When this structure is encapsulated in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0x00000008.

```
typedef struct _IPXWAN_IF_INFO {
    ULONG Adminstate;
} IPXWAN_IF_INFO,
*PIPXWAN_IF_INFO;
```

**Adminstate:** This MUST be set to the desired state of the interface. A value of 0x00000001 disables the interface, and a value of 0x00000002 enables the interface. This enables or disables the IPXWAN negotiation.

#### 2.2.1.2.94 IPX\_STATIC\_ROUTE\_INFO

The **IPX\_STATIC\_ROUTE\_INFO** [<97>](#) structure carries the route information for an IPX interface. When this structure is encapsulated within the [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0x00000002.

```
typedef struct _IPX_STATIC_ROUTE_INFO {
    union {
        ULONG DwordAlign;
        UCHAR Network[4];
    };
    USHORT TickCount;
    USHORT HopCount;
    UCHAR NextHopMacAddress[6];
} IPX_STATIC_ROUTE_INFO,
*PIPX_STATIC_ROUTE_INFO;
```

**DwordAlign:** This field of the union MUST NOT be used.

**Network:** This member MUST be the 4-byte IPX network number in hexadecimal (8 hexadecimal digits). For example, 1abe32.0000.0c33.2331. The first 32 bits represent the network address and the remaining bits represent the node address; that is, the format is network.node.

**TickCount:** This MUST be the number of ticks to get to the network number. One unit of tick count is approximately 1/18 seconds.

**HopCount:** This MUST be the number of routers to be traversed to get to the network number.

**NextHopMacAddress:** This MUST be the 6-byte MAC address of the next hop in hexadecimal (12 hexadecimal digits).

#### 2.2.1.2.95 IPX\_STATIC\_SERVICE\_INFO

The **IPX\_STATIC\_SERVICE\_INFO**[<98>](#) structure carries the IPX server information. When this structure is encapsulated in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0x00000003.

```
typedef struct _IPX_SERVER_ENTRY {
    USHORT Type;
    UCHAR Name[48];
    UCHAR Network[4];
    UCHAR Node[6];
    UCHAR Socket[2];
    USHORT HopCount;
} IPX_SERVER_ENTRY,
*PIPX_SERVER_ENTRY,
IPX_STATIC_SERVICE_INFO,
*PIPX_STATIC_SERVICE_INFO;
```

**Type:** The **Type** field indicates the contents of the payload portion of the IPX packet. It allows a number of client protocols to use the IPX and be identified by the IPX router.

Routers can filter the IPX traffic based on the Packet **Type** field. For example, some routers by default do not propagate NetBIOS over IPX broadcast traffic and must be manually configured to enable packets with a packet type value of 20.

The following table lists some common defined values of the IPX packet type.

Value	Meaning
0x0000	Unspecified
0x0001	RIP
0x0004	SAP/Normal IPX
0x0005	SPX
0x0014	IPX WAN broadcast (used for NetBIOS over IPX broadcasts)

**Name:** A null-terminated Unicode string giving the name of the interface.

**Network:** This MUST be the 4-byte IPX network number in hexadecimal (8 hexadecimal digits).

**Node:** The **Node** field identifies a node on an IPX network. The 6-byte fields can be used to store physical addresses, also known as media access control (MAC) addresses.

**Socket:** The **Socket** field identifies the software process addresses of the destination and source applications. With multiple processes communicating between the same two computers, the IPX network and node numbers are the same. The IPX socket number is a software process identifier that is used to forward the IPX payload to the proper process.

**HopCount:** This MUST be the number of routers to be traversed to get to the network number.

#### 2.2.1.2.96 IPX\_STATIC\_NETBIOS\_NAME\_INFO

The **IPX\_STATIC\_NETBIOS\_NAME\_INFO** structure contains the static NetBIOS name for an IPX interface. When this structure is encapsulated in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value MUST be 0x0000000a. [<99>](#)

```
typedef struct _IPX_STATIC_NETBIOS_NAME_INFO {
    union {
        ULONG DwordAlign;
        UCHAR Name[16];
    };
} IPX_STATIC_NETBIOS_NAME_INFO,
*PIPX_STATIC_NETBIOS_NAME_INFO;
```

**DwordAlign:** This field of the union MUST NOT be used.

**Name:** **Static NetBIOS names** MUST be used to confine NetBIOS over IPX broadcast traffic in environments where client-side NetBIOS applications need to access a small set of server-side NetBIOS applications.

#### 2.2.1.2.97 IPX\_ADAPTER\_INFO

The **IPX\_ADAPTER\_INFO** [<100>](#) structure contains the adapter information for the IPX. When this structure is encapsulated in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be 0x00000007.

```
typedef struct _IPX_ADAPTER_INFO {
    ULONG PacketType;
```

```

    WCHAR AdapterName[MAX_ADAPTOR_NAME_LEN];
} IPX_ADAPTER_INFO,
*PIPX_ADAPTER_INFO;

```

**PacketType:** The **PacketType** field indicates the contents of the payload portion of the IPX packet. It allows a number of client protocols to use the IPX and be identified by the IPX router.

The following table lists some common defined values of the IPX packet type.

Value	Meaning
0x0000	Unspecified
0x0001	RIP
0x0004	SAP/Normal IPX
0x0005	SPX
0x0014	IPX WAN broadcast (used for NetBIOS over IPX broadcasts)

**AdapterName:** Name of the adapter. The MAX\_ADAPTER\_NAME\_LEN value is defined as follows.

```
#define MAX_ADAPTOR_NAME_LEN 48
```

#### 2.2.1.2.98 IPX\_TRAFFIC\_FILTER\_GLOBAL\_INFO

The **IPX\_TRAFFIC\_FILTER\_GLOBAL\_INFO** [<101>](#) structure specifies the filter action to be taken when any IPX interface filter condition is met. When this structure is encapsulated in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value MUST be 0x0000000b or 0x0000000d. If the value in **InfoType** is 0x0000000b, the filter is applied to incoming traffic and if the value is 0x0000000d, the filter is applied to outgoing traffic.

```

typedef struct _IPX_TRAFFIC_FILTER_GLOBAL_INFO {
    ULONG FilterAction;
} IPX_TRAFFIC_FILTER_GLOBAL_INFO,
*PIPX_TRAFFIC_FILTER_GLOBAL_INFO;

```

**FilterAction:** This specifies the action if there is a match with any filter on the interface. This MUST be set to 0x00000001 to permit traffic and to 0x00000002 to deny traffic.

#### 2.2.1.2.99 IPX\_TRAFFIC\_FILTER\_INFO

The **IPX\_TRAFFIC\_FILTER\_INFO** structure [<102>](#) specifies the filter data for an IPX interface. When this structure is encapsulated in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value MUST be 0x00000006 or 0x0000000c. If the value of **InfoType** is 0x00000006, the filter is applied to incoming traffic, if the value of **InfoType** is 0x0000000c, the filter is applied to outgoing traffic.

```
typedef struct _IPX_TRAFFIC_FILTER_INFO {
    ULONG FilterDefinition;
    UCHAR DestinationNetwork[4];
    UCHAR DestinationNetworkMask[4];
    UCHAR DestinationNode[6];
    UCHAR DestinationSocket[2];
    UCHAR SourceNetwork[4];
    UCHAR SourceNetworkMask[4];
    UCHAR SourceNode[6];
    UCHAR SourceSocket[2];
    ULONG PacketType;
} IPX_TRAFFIC_FILTER_INFO,
*PIPX_TRAFFIC_FILTER_INFO;
```

**FilterDefinition:** Flags that specify relevant IPX address fields to filter on. The values MUST be one of the following.

Value	Meaning
IPX_TRAFFIC_FILTER_ON_SRCNET 0x00000001	Apply filter on source network.
IPX_TRAFFIC_FILTER_ON_SRCNODE 0x00000002	Apply filter on source node.
IPX_TRAFFIC_FILTER_ON_SRC_SOCKET 0x00000004	Apply filter on source socket.
IPX_TRAFFIC_FILTER_ON_DSTNET 0x00000010	Apply filter on destination network.
IPX_TRAFFIC_FILTER_ON_DSTNODE 0x00000020	Apply filter on destination node.
IPX_TRAFFIC_FILTER_ON_DST_SOCKET 0x00000040	Apply filter on destination socket.
IPX_TRAFFIC_FILTER_ON_PKTTYPE 0x00000100	Apply filter based on packet type.
IPX_TRAFFIC_FILTER_LOG_MATCHES 0x80000000	Apply filters based on log matches.

**DestinationNetwork:** The **DestinationNetwork** field identifies the network (a segment of the IPX internetwork bounded by the IPX routers) to which an IPX node is connected.

**DestinationNetworkMask:** The mask that must be logically ANDed with **DestinationNetwork**.

**DestinationNode:** Identifies a node on an IPX network. The 6-byte fields can be used to store physical addresses, also known as MAC addresses.

**DestinationSocket:** Identifies the software process addresses of the destination and source applications respectively. With multiple processes communicating between the same two computers, the IPX network and node numbers are the same. The IPX socket number is a software process identifier that is used to forward the IPX payload to the proper process.



**SourceNetwork:** Identifies the network (a segment of the IPX internetwork bounded by the IPX routers) to which an IPX node is connected.

**SourceNetworkMask:** The mask that must be logically ANDed with **SourceNetwork**.

**SourceNode:** Identifies a node on an IPX network. The 6-byte fields can be used to store physical addresses, also known as MAC addresses.

**SourceSocket:** Identifies the software process addresses of the destination and source applications respectively. With multiple processes communicating between the same two computers, the IPX network and node numbers are the same. The IPX socket number is a software process identifier that is used to forward the IPX payload to the proper process.

**PacketType:** The **PacketType** field indicates the contents of the payload portion of the IPX packet. It allows a number of client protocols to use the IPX and be identified by the IPX router.

The following table lists some common defined values of the IPX packet type.

Value	Meaning
0x0000	Unspecified
0x0001	RIP
0x0004	SAP/Normal IPX
0x0005	SPX
0x0014	IPX WAN broadcast (used for NetBIOS over IPX broadcasts)

#### 2.2.1.2.100 IF\_TABLE\_INDEX

The **IF\_TABLE\_INDEX** structure specifies the index within the Interface Table. It is used in [IPX MIB INDEX \(section 2.2.1.2.105\).<103>](#)

```
typedef struct _IF_TABLE_INDEX {
    ULONG InterfaceIndex;
} IF_TABLE_INDEX,
*PIF_TABLE_INDEX;
```

**InterfaceIndex:** The local index value for the network interface. This index value MAY change when a network adapter is disabled and then enabled, or under other circumstances, and need not be persistent.

#### 2.2.1.2.101 ROUTING\_TABLE\_INDEX

The **ROUTING\_TABLE\_INDEX** structure specifies the index within the routing table. It is used in [IPX MIB INDEX \(section 2.2.1.2.105\).<104>](#)

```
typedef struct _ROUTING_TABLE_INDEX {
    UCHAR Network[4];
} ROUTING_TABLE_INDEX,
*PROUTING_TABLE_INDEX;
```

**Network:** This MUST be the 4-byte IPX network number in hexadecimal (8 hexadecimal digits).

#### 2.2.1.2.102 STATIC\_ROUTES\_TABLE\_INDEX

The **STATIC\_ROUTES\_TABLE\_INDEX** structure specifies the index within the static routes table. It is used in [IPX MIB INDEX \(section 2.2.1.2.105\).<105>](#)

```
typedef struct _STATIC_ROUTES_TABLE_INDEX {
    ULONG InterfaceIndex;
    UCHAR Network[4];
} STATIC_ROUTES_TABLE_INDEX,
*PSTATIC_ROUTES_TABLE_INDEX;
```

**InterfaceIndex:** The local index value for the network interface. This index value MAY change when a network adapter is disabled and then enabled, or under other circumstances, and need not be persistent.

**Network:** This MUST be the 4-byte IPX network number in hexadecimal (8 hexadecimal digits).

#### 2.2.1.2.103 SERVICES\_TABLE\_INDEX

The **SERVICES\_TABLE\_INDEX** structure specifies the index within the services table. It is used in [IPX MIB INDEX \(section 2.2.1.2.105\).<106>](#)

```
typedef struct _SERVICES_TABLE_INDEX {
    USHORT ServiceType;
    UCHAR ServiceName[48];
} SERVICES_TABLE_INDEX,
*PSERVICES_TABLE_INDEX;
```

**ServiceType:** The type of service (for example: file server, print server, or application server).

Commonly used types are described in the following table.

Service type (hexadecimal)	Server
0x00	Unknown
0x00 — 0x04	NetWare file server
0x00 — 0x07	NetWare print server
0x06 — 0x40	Microsoft RPC server
0xFF	General SAP request

**ServiceName:** The name of the server hosting the service.

#### 2.2.1.2.104 STATIC\_SERVICES\_TABLE\_INDEX

The **STATIC\_SERVICES\_TABLE\_INDEX** structure specifies the index within the static services table. It is used in [IPX MIB INDEX \(section 2.2.1.2.105\)](#).<107>

```
typedef struct _STATIC_SERVICES_TABLE_INDEX {
    ULONG InterfaceIndex;
    USHORT ServiceType;
    UCHAR ServiceName[48];
} STATIC_SERVICES_TABLE_INDEX,
*PSTATIC_SERVICES_TABLE_INDEX;
```

**InterfaceIndex:** The local index value for the network interface. This index value MAY change when a network adapter is disabled and then enabled, or under other circumstances, and need not be persistent.

**ServiceType:** The type of service (for example: file server, print server, or application server).

Commonly used types are described in the following table.

Service Type (Hexadecimal)	Server
0x00	Unknown
0x00 — 0x04	NetWare File Server
0x00 — 0x07	NetWare Print Server
0x06 — 0x40	Microsoft RPC Server
0xFF	General SAP Request

**ServiceName:** The name of the server hosting the service.

#### 2.2.1.2.105 IPX\_MIB\_INDEX

The **IPX\_MIB\_INDEX** structure is used in [IPX MIB GET INPUT DATA \(section 2.2.1.2.106\)](#) to specify the MIB index for which the query is made.<108>

```
typedef struct _IPX_MIB_INDEX {
    IF_TABLE_INDEX InterfaceTableIndex;
    ROUTING_TABLE_INDEX RoutingTableIndex;
    STATIC_ROUTES_TABLE_INDEX StaticRoutesTableIndex;
    SERVICES_TABLE_INDEX ServicesTableIndex;
    STATIC_SERVICES_TABLE_INDEX StaticServicesTableIndex;
} IPX_MIB_INDEX,
*PIPX_MIB_INDEX;
```

**InterfaceTableIndex:** Gives the MIB index within the interface table, as specified in section [2.2.1.2.100](#).

**RoutingTableIndex:** Gives the MIB index within the routing table, as specified in section [2.2.1.2.101](#).

**StaticRoutesTableIndex:** Gives the MIB index within the static routes table, as specified in section [2.2.1.2.102](#).

**ServicesTableIndex:** Gives the MIB index within the services table, as specified in section [2.2.1.2.103](#).

**StaticServicesTableIndex:** Gives the MIB index within the static services table, as specified in section [2.2.1.2.104](#).

#### 2.2.1.2.106 IPX\_MIB\_GET\_INPUT\_DATA

The **IPX\_MIB\_GET\_INPUT\_DATA** structure is used to retrieve IPX MIB entries. [<109>](#) This structure is used in [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _IPX_MIB_GET_INPUT_DATA {
    ULONG TableId;
    IPX_MIB_INDEX MibIndex;
} IPX_MIB_GET_INPUT_DATA,
*PIPX_MIB_GET_INPUT_DATA;
```

**TableId:** Specifies the type of table. Values MUST be one of the following.

Value	Meaning
IPX_BASE_ENTRY 0x00000000	IPX base. See <a href="#">IPXMIB_BASE (section 2.2.1.2.107)</a> .
IPX_INTERFACE_TABLE 0x00000001	IPX interface table. See <a href="#">IPX_INTERFACE (section 2.2.1.2.109)</a> .
IPX_DEST_TABLE 0x00000002	IPX destination table. See <a href="#">IPX_ROUTE (section 2.2.1.2.110)</a> .
IPX_SERV_TABLE 0x00000004	IPX service table. See <a href="#">IPX_SERVICE (section 2.2.1.2.121)</a> .
IPX_STATIC_SERV_TABLE 0x00000005	IPX static service table. See <a href="#">IPX_STATIC_SERVICE_INFO (section 2.2.1.2.95)</a> .

**MibIndex:** Specifies the MIB index for the query. See section [2.2.1.2.105](#).

#### 2.2.1.2.107 IPXMIB\_BASE

The **IPXMIB\_BASE** structure contains basic information about the IPX protocol. [<110>](#) This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _IPXMIB_BASE {
    ULONG OperState;
    UCHAR PrimaryNetNumber[4];
    UCHAR Node[6];
    UCHAR SysName[48];
    ULONG MaxPathSplits;
```

```

ULONG IfCount;
ULONG DestCount;
ULONG ServCount;
} IPXMIB_BASE,
*PIPMIB_BASE;

```

**OperState:** The operational status of the interface. This member can be one of the following values.

Value	Meaning
OPER_STATE_DOWN 0x00000001	Nonoperational.
OPER_STATE_UP 0x00000002	Operational and can pass packets.
OPER_STATE_SLEEPING 0x00000003	Operational but has to connect to pass packets.

**PrimaryNetNumber:** Every IPX WAN router has a "primary network number". This is an IPX network number unique to the entire internet. This number will be a permanently assigned network number for the router.

A 32-bit number assigned by the network administrators; set to 0 on the local network.

**Node:** A 48-bit number that identifies the LAN hardware address. If the node number is FFFF FFFF, it means broadcast. If the node number is 0000 0000 0001, that means it is the server.

**SysName:** An administratively assigned name for this managed node. By convention, this is the node's fully qualified **domain name**.

**MaxPathSplits:** The maximum number of path splits implies the number of network interface boards in the server that are connected to the network or the number of ports in the server that are connected to a switch. The highest possible number is 8.

**IfCount:** Indicates the number of available interfaces.

**DestCount:** This value indicates the maximum destinations (networks) that the user expects the router to learn. This is used to pre-allocate table sizes for network tables. Changing this value can greatly affect the memory used by the IPX, but it can also speed learning times.

**ServCount:** This value indicates the maximum services that the user expects the router to learn. This is used to pre-allocate table sizes for service tables. Changing this value can greatly affect the memory used by the IPX, but it can also speed learning times.

#### 2.2.1.2.108 IPX\_IF\_STATS

The **IPX\_IF\_STATS** structure is used to gather the IPX interface statistics. [<111>](#) This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _IPX_IF_STATS {
```

```

ULONG IfOperState;
ULONG MaxPacketSize;
ULONG InHdrErrors;
ULONG InFiltered;
ULONG InNoRoutes;
ULONG InDiscards;
ULONG InDelivers;
ULONG OutFiltered;
ULONG OutDiscards;
ULONG OutDelivers;
ULONG NetbiosReceived;
ULONG NetbiosSent;
} IPX_IF_STATS,
*PIPX_IF_STATS;

```

**IfOperState:** The operational status of the interface. This member can be one of the following values.

Value	Meaning
OPER_STATE_DOWN 0x00000001	Nonoperational.
OPER_STATE_UP 0x00000002	Operational and can pass packets.
OPER_STATE_SLEEPING 0x00000003	Operational but has to connect to pass packets.

**MaxPacketSize:** The size of the MAX size packet received on the interface.

**InHdrErrors:** The number of packets received with header errors.

**InFiltered:** The number of incoming packets filtered.

**InNoRoutes:** The number of packets received with no matching routes.

**InDiscards:** The number of incoming packets discarded.

**InDelivers:** The number of incoming packets delivered.

**OutFiltered:** The number of outgoing packets filtered.

**OutDiscards:** The number of outgoing packets discarded.

**OutDelivers:** The number of outgoing packets delivered.

**NetbiosReceived:** The number of NetBIOS packets received.

**NetbiosSent:** The number of NetBIOS packets sent.

## 2.2.1.2.109 IPX\_INTERFACE

The **IPX\_INTERFACE** structure describes the MIB Row for **IPX\_INTERFACE\_TABLE**.[<112>](#) This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```

typedef struct _IPX_INTERFACE {
    ULONG InterfaceIndex;
    ULONG AdministratorState;
    ULONG AdapterIndex;
    UCHAR InterfaceName[48];
    ULONG InterfaceType;
    ULONG MediaType;
    UCHAR NetNumber[4];
    UCHAR MacAddress[6];
    ULONG Delay;
    ULONG Throughput;
    ULONG NetbiosAccept;
    ULONG NetbiosDeliver;
    ULONG EnableIpxWanNegotiation;
    IPX_IF_STATS IfStats;
} IPX_INTERFACE,
*PIPX_INTERFACE;

```

**InterfaceIndex:** The local index value for the network interface. This index value MAY change when a network adapter is disabled and then enabled, or under other circumstances, and need not be persistent.

**AdministratorState:** This MUST be set to the desired state of the interface. A value of 0x00000001 disables the interface and a value of 0x00000002 enables the interface.

**AdapterIndex:** The interface index associated with the network adapter.

**InterfaceName:** A null-terminated Unicode string that contains the name of the adapter.

**InterfaceType:** The type of the interface. The type MUST be one of the following.

Value	Meaning
IF_TYPE_OTHER 0x00000001	Other.
IF_TYPE_LAN 0x00000002	LAN.
IF_TYPE_WAN_ROUTER 0x00000003	WAN router.
IF_TYPE_WAN_WORKSTATION 0x00000004	Remote workstation dialing in.
IF_TYPE_INTERNAL 0x00000005	The internal (virtual) interface.
IF_TYPE_PERSONAL_WAN_ROUTER 0x00000006	Personal WAN router.
IF_TYPE_ROUTER_WORKSTATION_DIALOUT 0x00000007	Local workstation dialing out.
IF_TYPE_STANDALONE_WORKSTATION_DIALOUT 0x00000008	Stand-alone workstation dialing out.

**MediaType:** The type of media. This MUST one of the following values.

Value	Meaning
NdisMedium802_3 0x0000000	An Ethernet (802.3) network.
NdisMedium802_5 0x0000001	A Token Ring (802.5) network.
NdisMediumFddi 0x0000002	A Fiber Distributed Data Interface (FDDI) network.
NdisMediumWan 0x0000003	A wide area network (WAN). This type covers various forms of point-to-point and WAN NICs and variant address/header formats that must be negotiated between the protocol driver and the underlying driver after the binding is established.
NdisMediumLocalTalk 0x0000004	A LocalTalk network.
NdisMediumDix 0x0000005	An Ethernet network for which the drivers use the DIX Ethernet header format.
NdisMediumArcnetRaw 0x0000006	An ARCNET network.
NdisMediumArcnet878_2 0x0000007	An ARCNET (878.2) network.
NdisMediumAtm 0x0000008	An ATM network. Connection-oriented client protocol drivers can bind themselves to an underlying miniport driver that returns this value. Otherwise, legacy protocol drivers bind themselves to the system-supplied LanE intermediate driver, which reports its medium type as either NdisMedium802_3 or NdisMedium802_5, depending on how the network administrator configures the LanE driver.
NdisMediumWirelessWan 0x0000009	A wireless network. NDIS 5.x miniport drivers that support wireless LAN (WLAN) or wireless WAN (WWAN) packets declare their medium as NdisMedium802_3 and emulate Ethernet to higher-level NDIS drivers.<113>
NdisMediumIrda 0x000000a	An infrared (IrDA) network.
NdisMediumBpc 0x000000b	A broadcast computer network.
NdisMediumCoWan 0x000000c	A wide area network (WAN) in a connection-oriented environment.
NdisMedium1394 0x000000d	An IEEE 1394 (FireWire) network.
NdisMediumInfiniBand 0x000000e	An InfiniBand network.
NdisMediumTunnel 0x000000f	A tunnel network.



Value	Meaning
NdisMediumNative802_11 0x0000010	A native IEEE 802.11 network.
NdisMediumLoopback 0x0000011	An NDIS loopback network.

**NetNumber:** The IPX network number that is matched to the destination network number in a packet's IPX header.

**MacAddress:** The destination MAC address of the IPX packet when it is forwarded to the next hop. For directly attached networks, the Forwarding MAC Address field is blank.

**Delay:** Link delay indicated in milliseconds.

**Throughput:** Throughput of the interface indicated in bits per second.

**NetbiosAccept:** This MUST be set to 0x00000001 for the interface to accept NetBIOS broadcast packets.

**NetbiosDeliver:** This MUST be set to 0x00000001 on the LAN interface and 0x00000000 on the WAN interface.

**EnableIpxWanNegotiation:** A value of 0x00000001 disables the WAN negotiation, and a value of 0x00000002 enables the WAN negotiation.

**IfStats:** The interface statistics. See [IPX\\_IF\\_STATS \(section 2.2.1.2.108\)](#).

### 2.2.1.2.110 IPX\_ROUTE

The **IPX\_ROUTE** structure specifies the details for an IPX route in the RRAS server. [<114>](#)

```
typedef struct _IPX_ROUTE {
    ULONG InterfaceIndex;
    ULONG Protocol;
    UCHAR Network[4];
    USHORT TickCount;
    USHORT HopCount;
    UCHAR NextHopMacAddress[6];
    ULONG Flags;
} IPX_ROUTE,
*PIPX_ROUTE;
```

**InterfaceIndex:** The local index value for the network interface. This index value MAY change when a network adapter is disabled and then enabled, or under other circumstances, and need not be persistent.

**Protocol:** The protocol that added the route. The value MUST be one of the following.

Value	Meaning
IPX_PROTOCOL_LOCAL 0x0000000	Local route

Value	Meaning
IPX_PROTOCOL_STATIC 0x0000001	Static route
IPX_PROTOCOL_RIP 0x0000002	Added by RIP
IPX_PROTOCOL_NLSP 0x0000004	Added by NLSP

**Network:** This MUST be the 4-byte IPX network number in hexadecimal (8 hexadecimal digits).

**TickCount:** The number of ticks it takes to reach the destination network where one tick is approximately 1/18 of a second. This estimate is based on ongoing RIP requests and replies and is determined by the transmission speed of network segments. LAN links are typically one tick, and WAN links, such as a T1 link, are usually six or seven ticks. The tick count is an estimated, not precise, measurement of the delay.

**HopCount:** This MUST be the number of routers to be traversed to get to the network number.

**NextHopMacAddress:** This MUST be the 6-byte MAC address of the next hop in hexadecimal (12 hexadecimal digits).

**Flags:** Indicates the type of route being added. It MUST be one of the following.

Value	Meaning
GLOBAL_WAN_ROUTE 0x0000001	Global route.
DO_NOT_ADVERTISE_ROUTE 0x0000002	This route is not advertised.

#### 2.2.1.2.111 IPX\_MIB\_ROW

This structure contains **IPX\_MIB\_ROW** information. [<115>](#)

```
typedef struct _IPX_MIB_ROW {
    IPX_INTERFACE Interface;
    IPX_ROUTE Route;
    IPX_SERVICE Service;
} IPX_MIB_ROW,
*PIPX_MIB_ROW;
```

**Interface:** The [IPX\\_INTERFACE \(section 2.2.1.2.109\)](#) structure.

**Route:** The [IPX\\_ROUTE \(section 2.2.1.2.110\)](#) structure.

**Service:** The [IPX\\_SERVICE \(section 2.2.1.2.121\)](#) structure.

#### 2.2.1.2.112 IPX\_MIB\_SET\_INPUT\_DATA

The IPX\_MIB\_SET\_INPUT\_DATA structure is used in [RMIBEntrySet \(section 3.1.4.29\)](#). [<116>](#)

```
typedef struct _IPX_MIB_SET_INPUT_DATA {
    ULONG TableId;
    IPX_MIB_ROW MibRow;
} IPX_MIB_SET_INPUT_DATA,
*PIPX_MIB_SET_INPUT_DATA;
```

**TableId:** Specifies the type of tables. It MUST be one of the following values.

Value	Meaning
0x00000000	IPX_BASE_ENTRY
0x00000001	IPX_INTERFACE_TABLE
0x00000002	IPX_DEST_TABLE
0x00000003	IPX_STATIC_ROUTE_TABLE
0x00000004	IPX_SERV_TABLE
0x00000005	IPX_STATIC_SERV_TABLE

**MibRow:** An [IPX MIB ROW \(section 2.2.1.2.111\)](#) structure.

#### 2.2.1.2.113 SAP\_SERVICE\_FILTER\_INFO

The **SAP\_SERVICE\_FILTER\_INFO**[<117>](#) structure MUST be used when the **InfoType** in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#) is 0xffff0004.

```
typedef struct _SAP_SERVICE_FILTER_INFO {
    union {
        USHORT ServiceType;
        ULONG ServiceType_align;
    };
    UCHAR ServiceName[48];
} SAP_SERVICE_FILTER_INFO,
*PSAP_SERVICE_FILTER_INFO;
```

**ServiceType:** A field that indicates the type of the service. Service types are assigned uniquely by Novell, Inc. Some commonly defined SAP service types are listed in the following table.

Service type (hexadecimal)	Server
0x00	Unknown
0x00 — 0x04	NetWare file server
0x00 — 0x07	NetWare print server
0x06 — 0x40	Microsoft RPC server
0xFF	General SAP request

**ServiceType\_align:** Ensures alignment.

**ServiceName:** Stores the name of the server advertising the service. The combination of server name and service type uniquely identifies a service on an IPX internetwork. Server names that are fewer than 48 bytes are terminated with the ASCII NULL character.

#### 2.2.1.2.114 SAP\_IF\_FILTERS

This structure contains information about the SAP interface filters. [<118>](#)

```
typedef struct _SAP_IF_FILTERS {
    ULONG SupplyFilterAction;
    ULONG SupplyFilterCount;
    ULONG ListenFilterAction;
    ULONG ListenFilterCount;
    SAP_SERVICE_FILTER_INFO ServiceFilter[1];
} SAP_IF_FILTERS,
*PSAP_IF_FILTERS;
```

**SupplyFilterAction:** This MUST be set to 0x00000001 to permit data and to 0x00000002 to deny data.

Value	Meaning
0x00000001	Permit data
0x00000002	Deny data

**SupplyFilterCount:** The count of supply filters.

**ListenFilterAction:** This MUST be set to 0x00000001 to permit data and to 0x00000002 to deny data.

Value	Meaning
0x00000001	Permit data
0x00000002	Deny data

**ListenFilterCount:** The count of listen filters.

**ServiceFilter:** This must be a [SAP\\_SERVICE\\_FILTER\\_INFO \(section 2.2.1.2.113\)](#).

#### 2.2.1.2.115 SAP\_IF\_CONFIG

The **SAP\_IF\_CONFIG** structure contains SAP InterfaceConfiguration Information. [<119>](#) This structure MUST be used when the <InfoType> in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#) is 0x00020001.

```
typedef struct _SAP_IF_CONFIG {
    SAP_IF_INFO SapIfInfo;
    SAP_IF_FILTERS SapIfFilters;
} SAP_IF_CONFIG;
```

```
*PSAP_IF_CONFIG;
```

**SapIfInfo:** This MUST be a [SAP\\_IF\\_INFO \(section 2.2.1.2.122\)](#) structure.

**SapIfFilters:** This must be a [SAP\\_IF\\_FILTERS \(section 2.2.1.2.114\)](#) structure.

#### 2.2.1.2.116 SAP\_MIB\_BASE

The **SAP\_MIB\_BASE** structure contains the operation status.<120> This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _SAP_MIB_BASE {
    ULONG SapOperState;
} SAP_MIB_BASE,
*PSAP_MIB_BASE;
```

**SapOperState:** Contains the operational status of the SAP. It MUST be one of the following values.

Value	Meaning
OPER_STATE_DOWN 0x00000001	Nonoperational.
OPER_STATE_UP 0x00000002	Operational and can pass packets.
OPER_STATE_SLEEPING 0x00000003	Sleeping.
OPER_STATE_STARTING 0x00000004	Starting the router.
OPER_STATE_STOPPING 0x00000005	Stopping the router.

#### 2.2.1.2.117 SAP\_IF\_STATS

The **SAP\_IF\_STATS** structure contains the SAP MIB Interface Table Entry.<121> This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _SAP_IF_STATS {
    ULONG SapIfOperState;
    ULONG SapIfInputPackets;
    ULONG SapIfOutputPackets;
} SAP_IF_STATS,
*PSAP_IF_STATS;
```

**SapIfOperState:** Indicates the operation status of the SAP on the interface. It MUST be one of the following values.

Value	Meaning
OPER_STATE_DOWN 0x00000001	Nonoperational.
OPER_STATE_UP 0x00000002	Operational and can pass packets.
OPER_STATE_SLEEPING 0x00000003	Sleeping.

**SapIfInputPackets:** Counts the SAP input packets on the interface.

**SapIfOutputPackets:** Counts the SAP output packets on the interface.

#### 2.2.1.2.118 SAP\_INTERFACE

The **SAP\_INTERFACE** structure contains information about an SAP interface.[<122>](#) This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _SAP_INTERFACE {  
    ULONG InterfaceIndex;  
    SAP_IF_INFO SapIfInfo;  
    SAP_IF_STATS SapIfStats;  
} SAP_INTERFACE,  
*PSAP_INTERFACE;
```

**InterfaceIndex:** This MUST be the interface index of the interface.

**SapIfInfo:** This MUST be a [SAP\\_IF\\_INFO \(section 2.2.1.2.122\)](#) structure.

**SapIfStats:** This MUST be a [SAP\\_IF\\_STATS \(section 2.2.1.2.117\)](#) structure.

#### 2.2.1.2.119 SAP\_MIB\_GET\_INPUT\_DATA

The **SAP\_MIB\_GET\_INPUT\_DATA** structure is used to retrieve the SAP MIB information.[<123>](#)

```
typedef struct _SAP_MIB_GET_INPUT_DATA {  
    ULONG TableId;  
    ULONG InterfaceIndex;  
} SAP_MIB_GET_INPUT_DATA,  
*PSAP_MIB_GET_INPUT_DATA;
```

**TableId:** This MUST be set to 0x00000000 if the table refers to a [SAP\\_MIB\\_BASE \(section 2.2.1.2.116\)](#) and this MUST be set to 0x00000001 if the table refers to a [SAP\\_INTERFACE \(section 2.2.1.2.118\)](#).

**InterfaceIndex:** MUST be the interface index of the interface.

The **SAP\_MIB\_GET\_INPUT\_DATA** structure is used in the following APIs to retrieve the MIB information of the TableId and specified InterfaceIndex:

- [RMIBEntryGet \(section 3.1.4.30\)](#)
- [RMIBEntryGetFirst \(section 3.1.4.31\)](#)
- [RMIBEntryGetNext \(section 3.1.4.32\)](#)

#### 2.2.1.2.120 SAP\_MIB\_SET\_INPUT\_DATA

The **SAP\_MIB\_SET\_INPUT\_DATA** structure is used in the [RMIBEntrySet \(section 3.1.4.29\)](#) method to set information corresponding to the **TableId** and the **SapInterface**.<124>

```
typedef struct _SAP_MIB_SET_INPUT_DATA {
    ULONG TableId;
    SAP_INTERFACE SapInterface;
} SAP_MIB_SET_INPUT_DATA,
*PSAP_MIB_SET_INPUT_DATA;
```

**TableId:** This MUST be set to 0x00000001.

**SapInterface:** This MUST be a [SAP\\_INTERFACE \(section 2.2.1.2.118\)](#) structure.

#### 2.2.1.2.121 IPX\_SERVICE

This structure contains information about the IPX service<125> and is part of [IPX MIB ROW \(section 2.2.1.2.111\)](#).

```
typedef struct _IPX_SERVICE {
    ULONG InterfaceIndex;
    ULONG Protocol;
    IPX_SERVER_ENTRY Server;
} IPX_SERVICE,
*PIPX_SERVICE;
```

**InterfaceIndex:** This MUST be the interface index.

**Protocol:** This MUST be the protocol from which knowledge of the service was obtained.

**Server:** This MUST be an [IPX\\_SERVER\\_ENTRY \(section 2.2.1.2.95\)](#) structure.

#### 2.2.1.2.122 SAP\_IF\_INFO

The **SAP\_IF\_INFO** structure contains information about the SAP interface.<126> This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _SAP_IF_INFO {
    ULONG AdminState;
    ULONG UpdateMode;
    ULONG PacketType;
    ULONG Supply;
```

```

ULONG Listen;
ULONG GetNearestServerReply;
ULONG PeriodicUpdateInterval;
ULONG AgeIntervalMultiplier;
} SAP_IF_INFO,
*PSAP_IF_INFO;

```

**AdminState:** This MUST be the desired state of the interface. A value of 0x00000001 disables the SAP on the interface, and a value of 0x00000002 enables the SAP on the interface.

**UpdateMode:** This MUST be the SAP update mechanism used on the interface.

**PacketType:** This MUST be the SAP packet type used on this interface.

**Supply:** This MUST be set to a value of 0x00000001 to disable sending SAP updates on this interface and to a value of 0x00000002 to enable.

**Listen:** This MUST be set to a value of 0x00000001 to disable listening to SAP updates on this interface and to a value of 0x00000002 to enable.

**GetNearestServerReply:** Set to a value of 0x00000001 to disable GetNearestServer and to a value of 0x00000002 to enable.

**PeriodicUpdateInterval:** This MUST be the interval, in seconds, at which the information is periodically updated. The default value is 60.

**AgeIntervalMultiplier:** Each time a periodic update is done at the server, **PeriodicUpdateInterval** is multiplied by **AgeIntervalMultiplier**. The default value is 3.

#### 2.2.1.2.123 RIPMIB\_BASE

The **RIPMIB\_BASE** structure contains information about the RIP MIB base. This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```

typedef struct _RIPMIB_BASE {
    ULONG RIPOperState;
} RIPMIB_BASE,
*PRIPMIB_BASE;

```

**RIPOperState:** **RIPOperState** MUST be one of the following values.

Value	Meaning
OPER_STATE_DOWN 0x00000001	Nonoperational.
OPER_STATE_UP 0x00000002	Operational and can pass packets.
OPER_STATE_SLEEPING 0x00000003	Sleeping.



Value	Meaning
OPER_STATE_STARTING 0x00000004	Starting the router.
OPER_STATE_STOPPING 0x00000005	Stopping the router.

#### 2.2.1.2.124 RIP\_IF\_STATS

The **RIP\_IF\_STATS** contains the RIP interface statistics. This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _RIP_IF_STATS {
    ULONG RipIfOperState;
    ULONG RipIfInputPackets;
    ULONG RipIfOutputPackets;
} RIP_IF_STATS,
*PRIP_IF_STATS;
```

**RipIfOperState:** This MUST be one of the following values.

Value	Meaning
OPER_STATE_DOWN 0x00000001	Nonoperational.
OPER_STATE_UP 0x00000002	Operational and can pass packets.
OPER_STATE_SLEEPING 0x00000003	Sleeping.

**RipIfInputPackets:** The count of the RIP interface input packets.

**RipIfOutputPackets:** The count of the RIP interface output packets.

#### 2.2.1.2.125 RIP\_INTERFACE

The **RIP\_INTERFACE** structure contains information about a particular RIP interface. This structure is returned as part of [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _RIP_INTERFACE {
    ULONG InterfaceIndex;
    RIP_IF_INFO RipIfInfo;
    RIP_IF_STATS RipIfStats;
} RIP_INTERFACE,
*PRIP_INTERFACE;
```

**InterfaceIndex:** This MUST be the interface index of the interface.

**RipIfInfo:** This MUST be the [RIP\\_IF\\_INFO \(section 2.2.1.2.205\)](#) structure.

**RipIfStats:** This MUST be the [RIP\\_IF\\_STATS \(section 2.2.1.2.124\)](#) structure.

#### 2.2.1.2.126 RIP\_MIB\_GET\_INPUT\_DATA

The **RIP\_MIB\_GET\_INPUT\_DATA**[<127>](#) structure is used to retrieve information from the IPX RIP MIB.

```
typedef struct _RIP_MIB_GET_INPUT_DATA {
    ULONG TableId;
    ULONG InterfaceIndex;
} RIP_MIB_GET_INPUT_DATA,
*PRIP_MIB_GET_INPUT_DATA;
```

**TableId:** This MUST contain 0x00000000 if the table refers to [RIPMIB\\_BASE \(section 2.2.1.2.123\)](#) and it MUST contain 0x00000001 if the table refers to [RIP\\_INTERFACE \(section 2.2.1.2.125\)](#).

**InterfaceIndex:** The interface index.

#### 2.2.1.2.127 RIP\_MIB\_SET\_INPUT\_DATA

The **RIP\_MIB\_SET\_INPUT\_DATA**[<128>](#) is used to set information in the IPX RIP MIB.

```
typedef struct _RIP_MIB_SET_INPUT_DATA {
    ULONG TableId;
    RIP_INTERFACE RipInterface;
} RIP_MIB_SET_INPUT_DATA,
*PRIP_MIB_SET_INPUT_DATA;
```

**TableId:** This MUST contain 0x00000000 if the table refers to [RIPMIB\\_BASE \(section 2.2.1.2.123\)](#) and it MUST contain 0x00000001 if the table refers to [RIP\\_INTERFACE \(section 2.2.1.2.125\)](#).

**RipInterface:** This MUST be the **RIP\_INTERFACE** structure.

#### 2.2.1.2.128 EAPTLS\_HASH

The **EAPTLS\_HASH** structure contains the **certificate** hash.

```
typedef struct _EAPTLS_HASH {
    DWORD cbHash;
    BYTE pbHash[20];
} EAPTLS_HASH;
```

**cbHash:** This MUST contain the number of bytes in the hash.

**pbHash:** This MUST contain the hash of the certificate.

### 2.2.1.2.129 EAPTLS\_USER\_PROPERTIES

The structure **EAPTLS\_USER\_PROPERTIES** is used to store the EAP Transport Layer Security (TLS) user properties.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	30	1
reserved																															
dwVersion																															
dwSize																															
fFlags																															
Hash																															
...																															
...																															
...																															
...																															
...																															
pwszDiffUser																															
dwPinOffset																															
pwszPin																															
usLength																usMaximumLength															
ucSeed								awszString (variable)																							
...																															

**reserved (4 bytes):** This MUST be 0x00000000.

**dwVersion (4 bytes):** This MUST be 0x00000001.

**dwSize (4 bytes):** This MUST be the number of bytes in this structure.

**fFlags (4 bytes):** Unused; it MUST be set to 0x00000000.

**Hash (24 bytes):** An [EAPTLS HASH \(section 2.2.1.2.128\)](#) structure that MUST contain the hash for the user certificate.

**pwszDiffUser (4 bytes):** Pointer to a null-terminated Unicode string that contains the EAP identity to send. The string SHOULD be stored starting at **awszString**.

**dwPinOffset (4 bytes):** Offset from the end of this structure to where the PIN is stored. This SHOULD be set to sizeof(pwszDiffUser).

**pwszPin (4 bytes):** Pointer to a null-terminated Unicode string that contains the **smart card** PIN.

**usLength (2 bytes):** Unused; it MUST be set to zero.

**usMaximumLength (2 bytes):** Unused; it MUST be set to zero.

**ucSeed (1 byte):** Unused; it MUST be set to zero.

**awszString (variable):** Storage for **pwszDiffUser** and **pwszPin**.

### 2.2.1.2.130 MPRAPI\_OBJECT\_HEADER\_IDL

The **MPRAPI\_OBJECT\_HEADER\_IDL** structure [<129>](#) defines the version of the structure that needs to be used by the following methods and structures:

- [RRasAdminConnectionEnumEx \(section 3.1.4.46\)](#)
- [RRasAdminConnectionGetInfoEx \(section 3.1.4.47\)](#)
- [RAS\\_CONNECTION\\_EX\\_1 IDL \(section 2.2.1.2.134\)](#)
- [MPR\\_SERVER\\_EX\\_1 \(section 2.2.1.2.142\)](#)
- [MPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_1 \(section 2.2.1.2.145\)](#)
- [RAS\\_UPDATE\\_CONNECTION\\_1 IDL \(section 2.2.1.2.148\)](#)

```
typedef struct _MPRAPI_OBJECT_HEADER_IDL {  
    UCHAR revision;  
    UCHAR type;  
    USHORT size;  
} MPRAPI_OBJECT_HEADER_IDL,  
*PMPRAPI_OBJECT_HEADER_IDL;
```

**revision:** This represents the version of the structure that is being used depending on the **type** field. The following is the current supported value.

Value	Meaning
MPRAPI_RAS_CONNECTION_OBJECT_REVISION_1 0x01	Represents revision 1 of the structure <a href="#">RAS_CONNECTION_EX_1_IDL</a> (section 2.2.1.2.134) if <b>type</b> is 0x01.
MPRAPI_MPR_SERVER_SET_CONFIG_OBJECT_REVISION_1 0x01	Represents revision 1 of the structure <a href="#">MPR_SERVER_SET_CONFIG_EX_1</a>

Value	Meaning
	( <a href="#">section 2.2.1.2.146</a> ) if <b>type</b> is 0x01.
MPRAPI_MPR_SERVER_OBJECT_REVISION_1 0x01	Represents revision 1 of the structure <a href="#">MPR_SERVER_EX_1</a> ( <a href="#">section 2.2.1.2.143</a> ) if <b>type</b> is 0x01.
MPRAPI_RAS_UPDATE_CONNECTION_OBJECT_REVISION_1 0x01	Represents revision 1 of the structure <b>RAS_UPDATE_CONNECTION_1_IDL</b> ( <a href="#">section 2.2.1.2.148</a> ) if <b>type</b> is 0x05.

**type:** The following represents the type of structure being used.

Value	Meaning
MPRAPI_OBJECT_TYPE_RAS_CONNECTION_OBJECT 0x01	Represents a <a href="#">RAS_CONNECTION_EX_IDL</a> ( <a href="#">section 2.2.1.2.135</a> ) structure.
MPRAPI_OBJECT_TYPE_MPR_SERVER_OBJECT 0x02	Represents a MPR_SERVER_EX_1 ( <a href="#">section 2.2.1.2.143</a> ) structure.
MPRAPI_OBJECT_TYPE_MPR_SERVER_SET_CONFIG_OBJECT 0x03	Represents a MPR_SERVER_SET_CONFIG_EX_1 structure.
MPRAPI_OBJECT_TYPE_UPDATE_CONNECTION_OBJECT 0x05	Represents a <b>RAS_UPDATE_CONNECTION_1_IDL</b> ( <a href="#">section 2.2.1.2.148</a> ) _IDL structure.

**size:** Size of the BLOB (structure) being passed based on the type and revision.

### 2.2.1.2.131 PPP\_PROJECTION\_INFO\_1

The **PPP\_PROJECTION\_INFO\_1** structure<sup><130></sup> contains information obtained during the PPP negotiation for the PPP-based tunnels.

```
typedef struct {
    DWORD dwIPv4NegotiationError;
    WCHAR wszAddress[16];
    WCHAR wszRemoteAddress[16];
    DWORD dwIPv4Options;
    DWORD dwIPv4RemoteOptions;
    ULONG64 IPv4SubInterfaceIndex;
    DWORD dwIPv6NegotiationError;
    UCHAR bInterfaceIdentifier[8];
    UCHAR bRemoteInterfaceIdentifier[8];
    UCHAR bPrefix[8];
    DWORD dwPrefixLength;
    ULONG64 IPv6SubInterfaceIndex;
    DWORD dwLcpError;
    DWORD dwAuthenticationProtocol;
    DWORD dwAuthenticationData;
    DWORD dwRemoteAuthenticationProtocol;
    DWORD dwRemoteAuthenticationData;
    DWORD dwLcpTerminateReason;
```

```

DWORD dwLcpRemoteTerminateReason;
DWORD dwLcpOptions;
DWORD dwLcpRemoteOptions;
DWORD dwEapTypeId;
DWORD dwRemoteEapTypeId;
DWORD dwCcpError;
DWORD dwCompressionAlgorithm;
DWORD dwCcpOptions;
DWORD dwRemoteCompressionAlgorithm;
DWORD dwCcpRemoteOptions;
} PPP_PROJECTION_INFO_1,
*PPPP_PROJECTION_INFO_1;

```

**dwIPv4NegotiationError:** Same as **dwError** in [PPP\\_IPCP\\_INFO \(section 2.2.1.2.66\)](#).

**wszAddress:** Same as **wszAddress** in PPP\_IPCP\_INFO.

**wszRemoteAddress:** Same as **wszRemoteAddress** in PPP\_IPCP\_INFO.

**dwIPv4Options:** Same as **dwOptions** in PPP\_IPCP\_INFO.

**dwIPv4RemoteOptions:** Same as **dwIPv4Options**.

**IPv4SubInterfaceIndex:** Specifies the index of the **subinterface** corresponding to the connection on the server.

**dwIPv6NegotiationError:** Specifies the result of PPP\_IPv6. Network control protocol negotiation. A value of zero indicates that either IPv6 was not negotiated or Ipv6 has been negotiated successfully. A nonzero value indicates failure, and is the actual fatal error that occurred during the control protocol.

**bInterfaceIdentifier:** If **dwIPv6NegotiationError** is zero and IPv6 was negotiated, this MUST be the 64-bit interface identifier of the IPv6 address of the server interface. If **dwIPv6NegotiationError** is zero, a value of zero for this indicates that IPv6 was not negotiated. It MUST be zero when **dwIPv6NegotiationError** is nonzero.

**bRemoteInterfaceIdentifier:** If **dwIPv6NegotiationError** is zero and IPv6 was negotiated, this MUST be the 64-bit interface identifier of the IPv6 address of the client interface. If **dwIPv6NegotiationError** is zero, a value of zero for this indicates that IPv6 was not negotiated. It MUST be zero when **dwIPv6NegotiationError** is nonzero.

**bPrefix:** Specifies the prefix of the IPv6 address of the client interface.

**dwPrefixLength:** The length, in bits, of the address prefix.

**IPv6SubInterfaceIndex:** Specifies the index of the subInterface corresponding to the connection on the server.

**dwLcpError:** Specifies the error that occurred if the PPP negotiation was unsuccessful and it MUST be one of the following.

Value	Meaning
ERROR_NO_LOCAL_ENCRYPTION 0x000002E5	The local computer does not support the required data encryption type.

Value	Meaning
ERROR_NO_REMOTE_ENCRYPTION 0x000002E6	The remote computer does not support the required data encryption type.
ERROR_CHANGING_PASSWORD 0x000002C5	There was an error changing the password on the domain. The password might have been too short or might have matched a previously used password.
ERROR_PPP_NO_PROTOCOLS_CONFIGURED 0x000002D0	The PPP controlled protocols were not configured.
ERROR_AUTHENTICATION_FAILURE 0x000002B3	The connection was denied because the user name or password specified is not valid or because the selected authentication protocol is not permitted on the remote server.
ERROR_MORE_DATA 0x000000EA	More data is available.
ERROR_PROTOCOL_NOT_CONFIGURED 0x000002DC	The received control protocol of the PPP is not configured.
ERROR_AUTH_INTERNAL 0x00000285	There was an internal error while processing authentication.
ERROR_NO_DIALIN_PERMISSION 0x00000289	The user does not have permission to dial in.
ERROR_SERVER_POLICY 0x0000032C	The connection was prevented because of a policy configured on the RRAS.
ERROR_PEER_REFUSED_AUTH 0x00000397	The connection could not be established because the authentication protocol used by the RRAS to verify user name and password could not be matched with the one proposed by the client.
ERROR_UNKNOWN_FRAMED_PROTOCOL 0x0000031A	The Framed Protocol RADIUS <a href="#">[RFC2865]</a> attribute for this client is not PPP.
ERROR_WRONG_TUNNEL_TYPE 0x0000031B	The Tunnel Type RADIUS <a href="#">[RFC2865]</a> attribute for this user is not correct.
ERROR_UNKNOWN_SERVICE_TYPE 0x0000031C	The Service Type RADIUS <a href="#">[RFC2865]</a> attribute for this user is neither Framed nor Callback Framed.
ERROR_RESTRICTED_LOGON_HOURS 0x00000286	The user is not permitted to log on at this time of day.
ERROR_ACCT_DISABLED 0x00000287	The account is disabled.
ERROR_PASSWD_EXPIRED 0x00000288	The password for this account has expired.
ERROR_ILL_FORMED_PASSWORD 0x0000052C	Unable to update the password. The value provided for the new password contains values that are not allowed in passwords.

**dwAuthenticationProtocol:** The same as **dwAuthenticatedProtocol** in [PPP\\_LCP\\_INFO](#).

**dwAuthenticationData:** The same as **dwAuthenticatedData** in PPP\_LCP\_INFO.

**dwRemoteAuthenticationProtocol:** Specifies the authentication protocol used to authenticate the remote computer. This will be different from **dwAuthenticationProtocol** in the case of demand-dial if the authentication protocol used by the two ends are different. See the **dwAuthenticationProtocol** member for a list of possible values.

**dwRemoteAuthenticationData:** Specifies additional information about the authentication protocol specified by *dwRemoteAuthenticationProtocol*. This will be different from **dwAuthenticationData** in the case of demand-dial if the authentication protocol used by the two ends are different. See the **dwAuthenticationData** member for a list of possible values.

**dwLcpTerminateReason:** Specifies the reason the connection was terminated by the local computer. This member always has a value of zero.

**dwLcpRemoteTerminateReason:** Specifies the reason the connection was terminated by the remote computer. This member always has a value of zero.

**dwLcpOptions:** The same as **dwOptions** in PPP\_LCP\_INFO.

**dwLcpRemoteOptions:** Specifies information about the LCP options in use by the remote computer. See the **dwLcpOptions** member for a list of possible values.

**dwEapTypeId:** Specifies the type identifier of the EAP used to authenticate the local computer. The value of this member is valid only if **dwAuthenticationProtocol** is PPP\_LCP\_EAP. The valid values are defined in [\[IANA-EAP\]](#).

**dwRemoteEapTypeId:** MUST be zero. This value has no significance.

**dwCcpError:** Specifies an error if the negotiation is unsuccessful.

**dwCompressionAlgorithm:** The same as **dwCompressionAlgorithm** in PPP\_LCP\_INFO.

**dwCcpOptions:** The same as **dwCcpOptions** in PPP\_LCP\_INFO.

**dwRemoteCompressionAlgorithm:** Specifies the compression algorithm used by the remote computer. The values are the same as those for **dwCompressionAlgorithm**.

**dwCcpRemoteOptions:** Specifies the compression options on the remote computer. The following options are supported.

Value	Meaning
PPP_CCP_COMPRESSION 0x00000001	Compression without encryption.
PPP_CCP_HISTORYLESS 0x01000000	MPPE in stateless mode. The session key is changed after every packet. This mode improves performance on high-latency networks, or networks that experience significant packet loss.
PPP_CCP_ENCRYPTION40BITOLD 0x00000010	PPE using 40-bit keys.
PPP_CCP_ENCRYPTION40BIT 0x00000020	MPPE using 40-bit keys.



Value	Meaning
PPP_CCP_ENCRYPTION56BIT 0x00000080	MPPE using 56-bit keys.
PPP_CCP_ENCRYPTION128BIT 0x00000040	MPPE using 128-bit keys.
ERROR_PPP_NOT_CONVERGING 0x000002DC	The remote computer and RRAS could not converge on address negotiation.

### 2.2.1.2.132 IKEV2\_PROJECTION\_INFO\_1

The **IKEV2\_PROJECTION\_INFO\_1** structure [<131>](#) contains information obtained during Internet key exchange (IKE) negotiation.

```
typedef struct IKEV2_PROJECTION_INFO_1 {
    DWORD dwIPv4NegotiationError;
    WCHAR wszAddress[16];
    WCHAR wszRemoteAddress[16];
    ULONG64 IPv4SubInterfaceIndex;
    DWORD dwIPv6NegotiationError;
    UCHAR bInterfaceIdentifier[8];
    UCHAR bRemoteInterfaceIdentifier[8];
    UCHAR bPrefix[8];
    DWORD dwPrefixLength;
    ULONG64 IPv6SubInterfaceIndex;
    DWORD dwOptions;
    DWORD dwAuthenticationProtocol;
    DWORD dwEapTypeId;
    DWORD dwCompressionAlgorithm;
    DWORD dwEncryptionMethod;
} IKEV2_PROJECTION_INFO_1,
*PIKEV2_PROJECTION_INFO_1;
```

**dwIPv4NegotiationError:** Specifies if an Internal IPv4 address [\[RFC4306\]](#) has been successfully assigned. A value of zero indicates success. A nonzero value indicates failure.

**wszAddress:** The same as **wszAddress** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**wszRemoteAddress:** The same as **wszRemoteAddress** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**IPv4SubInterfaceIndex:** The same as **IPv4SubInterfaceIndex** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**dwIPv6NegotiationError:** The same as **dwIPv5NegotiationError** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**bInterfaceIdentifier:** The same as **bInterfaceIdentifier** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**bRemoteInterfaceIdentifier:** The same as **bRemoteInterfaceIdentifier** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**bPrefix:** The same as **bPrefix** in [PPP\\_PROJECTION\\_INFO\\_1](#).

**dwPrefixLength:** The same as **dwPrefixLength** in PPP\_PROJECTION\_INFO\_1.

**IPv6SubInterfaceIndex:** The same as **IPv6SubInterfaceIndex** in PPP\_PROJECTION\_INFO\_1.

**dwOptions:** Not used.

**dwAuthenticationProtocol:** Specifies the authentication protocol used to authenticate the remote computer. It MUST be one of the following.

Value	Meaning
MPRAPI_IKEV2_AUTH_USING_CERT 0x00000001	Using x.509 machine certificate <a href="#">[RFC2459]</a> .
MPRAPI_IKEV2_AUTH_USING_EAP 0x00000002	Extensible Authentication Protocol (EAP).

**dwEapTypeId:** Specifies the type identifier of the EAP used to authenticate the local computer. The value of this member is valid only if **dwAuthenticationProtocol** is MPRAPI\_IKEV2\_AUTH\_USING\_EAP [\[IANA-EAP\]](#).

**dwCompressionAlgorithm:** Not used.

**dwEncryptionMethod:** Specifies the encryption method used in the connection. It MUST be one of the following values.

Value	Meaning
IPSEC_CIPHER_TYPE_3DES 2	Specifies 3DES encryption.
IPSEC_CIPHER_TYPE_AES_128 3	Specifies AES-128 encryption.
IPSEC_CIPHER_TYPE_AES_192 4	Specifies AES-192 encryption.
IPSEC_CIPHER_TYPE_AES_256 5	Specifies AES-256 encryption.

### 2.2.1.2.133 PROJECTION\_INFO\_IDL\_1

The **PROJECTION\_INFO\_IDL\_1** structure is used in [RAS\\_CONNECTION\\_EX\\_1\\_IDL \(section 2.2.1.2.134\)](#) as a placeholder for [PPP\\_PROJECTION\\_INFO\\_1 \(section 2.2.1.2.131\)](#) or [IKEV2\\_PROJECTION\\_INFO\\_1 \(section 2.2.1.2.132\)](#).

```
typedef struct _PROJECTION_INFO_IDL_1 {
    UCHAR projectionInfoType;
    union {
        PPP_PROJECTION_INFO_1 PppProjectionInfo;
        IKEV2_PROJECTION_INFO_1 Ikev2ProjectionInfo;
    } ProjectionInfoObject;
} PROJECTION_INFO_IDL_1,
*PPROJECTION_INFO_IDL_1;
```

**projectionInfoType:** Specifies if the projection is for a PPP-based or IKEv2-based tunnel.

Value	Meaning
MPRAPI_PPP_PROJECTION_INFO_TYPE 0x01	Data corresponds to <b>PPP_PROJECTION_INFO_1</b> .
MPRAPI_IKEV2_PROJECTION_INFO_TYPE 0x02	Data corresponds to <b>IKEV2_PROJECTION_INFO_1</b> .

**PppProjectionInfo:** Contains a **PPP\_PROJECTION\_INFO\_1** for a PPP-based tunnel.

**Ikev2ProjectionInfo:** Contains an **IKEV2\_PROJECTION\_INFO\_1** for an IKEv2-based tunnel.

#### 2.2.1.2.134 RAS\_CONNECTION\_EX\_1\_IDL

The **RAS\_CONNECTION\_EX\_1\_IDL** structure contains information for a connection, including the GUID that identifies the connection, the NAP, and the PPP or the IKEv2 related data for the connection.

```
typedef struct _RAS_CONNECTION_EX_1_IDL {
    MPRAPI_OBJECT_HEADER_IDL Header;
    DWORD dwConnectDuration;
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    DWORD dwConnectionFlags;
    WCHAR wszInterfaceName[257];
    WCHAR wszUserName[257];
    WCHAR wszLogonDomain[16];
    WCHAR wszRemoteComputer[17];
    GUID guid;
    RAS_QUARANTINE_STATE rasQuarState;
    FILETIME probationTime;
    DWORD dwBytesXmited;
    DWORD dwBytesRcvd;
    DWORD dwFramesXmited;
    DWORD dwFramesRcvd;
    DWORD dwCrcErr;
    DWORD dwTimeoutErr;
    DWORD dwAlignmentErr;
    DWORD dwHardwareOverrunErr;
    DWORD dwFramingErr;
    DWORD dwBufferOverrunErr;
    DWORD dwCompressionRatioIn;
    DWORD dwCompressionRatioOut;
    DWORD dwNumSwitchOvers;
    WCHAR wszRemoteEndpointAddress[65];
    WCHAR wszLocalEndpointAddress[65];
    PROJECTION_INFO_IDL_1 ProjectionInfo;
    ULONG hConnection;
    ULONG hInterface;
} RAS_CONNECTION_EX_1_IDL,
*PRAS_CONNECTION_EX_1_IDL;
```

**Header:** A [MPRAPI\\_OBJECT\\_HEADER\\_IDL \(section 2.2.1.2.130\)](#) whose revision field MUST be 0x01 and type field MUST be 0x01.

**dwConnectDuration:** Specifies the duration in seconds for which the current connection is active.

**dwInterfaceType:** Specifies a [ROUTER\\_INTERFACE\\_TYPE \(section 2.2.1.1.1\)](#) value specifying the interface type of the current connection.

**dwConnectionFlags:** Specifies certain attributes of the connection.

This member MUST contain one of the following flags.

Value	Meaning
0x00000000	No flag is set.
RAS_FLAGS_PPP_CONNECTION 0x00000001	The connection is using the Point-to-Point Protocol (PPP).
RAS_FLAGS_MESSENGER_PRESENT 0x00000002	The messenger service is active on the client and messages can be sent to the client using <a href="#">RRasAdminSendMessage (section 3.1.4.36)</a> .
RAS_FLAGS_QUARANTINE_PRESENT 0x00000008	The connection is currently in quarantine. See <a href="#">RRasAdministratorConnectionRemoveQuarantine (section 3.1.4.43)</a> for more information.
RAS_FLAGS_ARAP_CONNECTION 0x00000010	The connection is using the AppleTalk Remote Access Protocol (ARAP).<132>
RAS_FLAGS_DORMANT 0x00000020	The connection is using the IKEv2 and the server is not reachable.<133>

**wszInterfaceName:** Specifies a null-terminated Unicode string that contains the name of the interface for this connection.

**wszUserName:** Specifies a null-terminated Unicode string that contains the name of the user logged on to the connection.

**wszLogonDomain:** Specifies a null-terminated Unicode string that contains the domain on which the connected user is authenticated.

**wszRemoteComputer:** Specifies a null-terminated Unicode string that contains the name of the remote computer.

**guid:** A GUID uniquely identifying the connection.

**rasQuarState:** Specifies the NAP quarantine state for the connection through the type [RAS\\_QUARANTINE\\_STATE \(section 2.2.1.1.3\)](#) that contains the quarantine state of this connection.

**probationTime:** Specifies the NAP probation time for the connection in UTC. This value is valid only if the **rasQuarState** has a value of RAS\_QUAR\_STATE\_PROBATION (see [RAS\\_QUARANTINE\\_STATE](#)).

**dwBytesXmited:** Specifies the bytes transmitted on the current connection.

**dwBytesRcvd:** Specifies the bytes received on the current connection.

**dwFramesXmited:** Specifies the frames transmitted on the current connection.

**dwFramesRcvd:** Specifies the frames received on the current connection.

**dwCrcErr:** Specifies the CRC errors on the current connection.

**dwTimeoutErr:** Specifies the time-out errors on the current connection.

**dwAlignmentErr:** Specifies the alignment errors on the current connection.

**dwHardwareOverrunErr:** Specifies the number of hardware-overrun errors on the current connection.

**dwFramingErr:** Specifies the number of framing errors for the current connection.

**dwBufferOverrunErr:** Specifies the number of buffer-overrun errors.

**dwCompressionRatioIn:** Specifies a percentage that indicates the degree to which data received on this connection is compressed. The ratio is the size of the compressed data divided by the size of the same data in an uncompressed state.

**dwCompressionRatioOut:** Specifies a percentage that indicates the degree to which data transmitted on this connection is compressed. The ratio is the size of the compressed data divided by the size of the same data in an uncompressed state.

**dwNumSwitchOvers:** Specifies the number of MOBIKE [\[RFC4555\]](#) switches that happened on the connection. Valid only if **dwConnectionFlags** is RAS\_FLAGS\_IKEV2\_CONNECTION.

**wszRemoteEndpointAddress:** Specifies a null-terminated Unicode string that holds the remote computer's IP address for the connection. This string has the form a.b.c.d; for example, "10.102.235.84".

**wszLocalEndpointAddress:** Specifies a null-terminated Unicode string that holds the local computer's IP address for the connection. This string has the form a.b.c.d or a::1234; for example, "10.102.235.84" or 2ffe::1234.

**ProjectionInfo:** This is a [PROJECTION\\_INFO\\_IDL 1](#) structure.

**hConnection:** A handle to the connection.

**hInterface:** A handle to the interface.

#### 2.2.1.2.135 RAS\_CONNECTION\_EX\_IDL

The **RAS\_CONNECTION\_EX\_IDL** structure contains a placeholder for [RAS\\_CONNECTION\\_EX\\_1\\_IDL \(section 2.2.1.2.134\)](#). This structure is used in [RRasAdminConnectionGetInfoEx \(section 3.1.4.47\)](#).

```
typedef
union _RAS_CONNECTION_EX_IDL switch (UCHAR revision) ConnObject {
    case 1: RAS_CONNECTION_EX_1_IDL RasConnection1;
} RAS_CONNECTION_EX_IDL;
*PRAS_CONNECTION_EX_IDL;
```

**RasConnection1:** This MUST be the structure **RAS\_CONNECTION\_EX\_1\_IDL**.

### 2.2.1.2.136 CERT\_BLOB\_1

The **CERT\_BLOB\_1** is a generic structure that contains x.509 [\[RFC2459\]](#) certificate information.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
cbData																															
pbData (variable)																															
...																															

**cbData (4 bytes):** Size (in bytes) of the certificate information present in **pbData**.

**pbData (variable):** Pointer to the information of the certificate. This information depends on the structure in which this is used. In [IKEV2\\_TUNNEL\\_CONFIG\\_PARAMS\\_1](#), this points to the subject name of the certificate. In [SSTP\\_CERT\\_INFO\\_1](#), **pbData** contains a SHA-1 hash.

### 2.2.1.2.137 IKEV2\_TUNNEL\_CONFIG\_PARAMS\_1

The **IKEV2\_TUNNEL\_CONFIG\_PARAMS\_1** structure is used to get or set configured parameters for IKEv2 devices [\[RFC4306\].<134>](#)

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
dwIdleTimeout																															
dwNetworkBlackoutTime																															
dwSaLifeTime																															
dwSaDataSizeForRenegotiation																															
dwConfigOptions																															
dwTotalCertificates																															
certificateNames (variable)																															
...																															

**dwIdleTimeout (4 bytes):** Duration, in seconds, after which the connection will be disconnected if there is no traffic. This value **MUST** be between 300 and 17,279,999.

**dwNetworkBlackoutTime (4 bytes):** Retransmission timeout, in seconds, for IKEv2 Request packets [\[RFC4306\]](#). IKEv2 expects a response for every request packet sent, this value specifies the time after which the connection is deleted incase response is not received. This value **MUST** be greater than or equal to 120.

**dwSaLifeTime (4 bytes):** Lifetime of a security association (SA), in seconds, after which the SA is no longer valid [\[RFC4306\]](#). This value MUST be between 300 and 17,279,999.

**dwSaDataSizeForRenegotiation (4 bytes):** Number of Kilobytes that are allowed to transfer using a SA. After that the SA will be renegotiated [\[RFC4306\]](#). This value MUST be greater than or equal to 1024.

**dwConfigOptions (4 bytes):** Unused and must be set to 0.

**dwTotalCertificates (4 bytes):** Total number of certificates in member variable **certificateNames**.

**certificateNames (variable):** An array of [CERT\\_BLOB\\_1](#).

#### 2.2.1.2.138 IKEV2\_CONFIG\_PARAMS\_1

The **IKEV2\_CONFIG\_PARAMS\_1** structure is used to get or set configured parameters for IKEv2 devices. [<135>](#)

```
typedef struct _IKEV2_CONFIG_PARAMS_1 {
    DWORD dwNumPorts;
    DWORD dwPortFlags;
    DWORD dwTunnelConfigParamFlags;
    IKEV2_TUNNEL_CONFIG_PARAMS_1 TunnelConfigParams;
} IKEV2_CONFIG_PARAMS_1,
*PIKEV2_CONFIG_PARAMS_1;
```

**dwNumPorts:** Specifies the number of ports configured on RRAS to accept IKEv2 connections. This value cannot exceed the server port limit. [<136>](#)

**dwPortFlags:** Specifies the type of port configured on IKEv2 devices. Possible flags are:

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote Access is enabled for IKEv2.

**dwTunnelConfigParamFlags:** SHOULD be set to 0x00000001 when sent and SHOULD be ignored on receipt.

**TunnelConfigParams:** IKEv2 tunnel related parameters. MUST be an [IKEV2\\_TUNNEL\\_CONFIG\\_PARAMS\\_1](#) structure.

#### 2.2.1.2.139 PPTP\_CONFIG\_PARAMS\_1

The **PPTP\_CONFIG\_PARAMS\_1** structure is used to get or set the device configuration for PPTP on the RAS Server. [<137>](#)

```
typedef struct _PPTP_CONFIG_PARAMS_1 {
    DWORD dwNumPorts;
    DWORD dwPortFlags;
} PPTP_CONFIG_PARAMS_1,
*PPPTP_CONFIG_PARAMS_1;
```

**dwNumPorts:** Specifies the number of ports configured on that (PPTP) device. This value cannot exceed the server port limit.<138>

**dwPortFlags:** Specifies the type of port configured on PPTP devices. The possible flags are.

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	PPTP is enabled to accept Remote Access client connection.
MPR_ENABLE_ROUTING_ON_DEVICE 0x00000002	PPTP is enabled to accept Demand dial connections.

#### 2.2.1.2.140 L2TP\_CONFIG\_PARAMS\_1

The **L2TP\_CONFIG\_PARAMS\_1** structure is used to get or set the device configuration for L2TP on RAS Server.<139>

```
typedef struct _L2TP_CONFIG_PARAMS_1 {
    DWORD dwNumPorts;
    DWORD dwPortFlags;
} L2TP_CONFIG_PARAMS_1,
*PL2TP_CONFIG_PARAMS_1;
```

**dwNumPorts:** Specifies the number of ports configured on the (L2TP) device. This value cannot exceed the server port limit.<140>

**dwPortFlags:** Specifies the type of port configured on L2TP devices. Possible flags are:

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	L2TP is enabled to accept Remote Access client connection.
MPR_ENABLE_ROUTING_ON_DEVICE 0x00000002	L2TP is enabled to accept Demand dial connections.

#### 2.2.1.2.141 SSTP\_CERT\_INFO\_1

The **SSTP\_CERT\_INFO\_1** structure contains the subject name of the x.509 certificates that will be configured by the RRAS to be used in SSL/TLS negotiation as a part of the [\[MS-SSTP\]](#) protocol.<141>

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
isDefault																															
certBlob (variable)																															



...
-----

**isDefault (4 bytes):** This value specifies how the SSTP certificate hash values are configured. Possible values are:

Value	Meaning
TRUE	RRAS server should choose a certificate hash on its own automatically.
FALSE	The SSTP certificate hash values are configured by the administrator.

This value SHOULD be set to FALSE when sent. The RRAS server specifies TRUE for this value if administrator has not configured the certificate and default certificate selection logic is used. This value is FALSE if the administrator has configured the certificate.

**certBlob (variable):** This MUST be a [CERT\\_BLOB\\_1](#). This contains the Certificate HASH Length and Certificate Hash. It accepts ONLY SHA256 HASH as the valid HASH. Thus, the value of the length field SHOULD always be 32 [\[RFC2459\]](#). Specifying a value 0 for the cbData member of CERT\_BLOB\_1 removes the certificate configuration. In this case, RRAS server uses its default certificate selection logic.

#### 2.2.1.2.142 SSTP\_CONFIG\_PARAMS\_1

The **SSTP\_CONFIG\_PARAMS\_1** structure is used to get or set the device configuration for SSTP on a RAS Server [\[MS-SSTP\].<142>](#)

```
typedef struct _SSTP_CONFIG_PARAMS_1 {
    DWORD dwNumPorts;
    DWORD dwPortFlags;
    BOOL isUseHttps;
    DWORD certAlgorithm;
    SSTP_CERT_INFO_1 sstpCertDetails;
} SSTP_CONFIG_PARAMS_1,
*PSSTP_CONFIG_PARAMS_1;
```

**dwNumPorts:** Specifies the number of ports configured on that (SSTP) device. This value cannot exceed the server port limit. [<143>](#)

**dwPortFlags:** Specifies the type of port configured on SSTP devices. Possible flags are:

Value	Meaning
MPR_ENABLE_RAS_ON_DEVICE 0x00000001	Remote Access is enabled for SSTP.

**isUseHttps:** MUST be set to TRUE if HTTPS used, MUST be set to FALSE if HTTPS is not used.

**certAlgorithm:** MUST be set to 0x0000800C.

**sstpCertDetails:** MUST be a [SSTP\\_CERT\\_INFO\\_1](#) structure.

#### 2.2.1.2.143 MPR\_SERVER\_EX\_1

The **MPR\_SERVER\_EX\_1** structure is used to get or set the configuration of a RAS server. [<144>](#)

```
typedef struct _MPR_SERVER_EX_1 {
    MPRAPI_OBJECT_HEADER_IDL Header;
    DWORD fLanOnlyMode;
    DWORD dwUpTime;
    DWORD dwTotalPorts;
    DWORD dwPortsInUse;
    DWORD Reserved;
    MPRAPI_TUNNEL_CONFIG_PARAMS_1 ConfigParams;
} MPR_SERVER_EX_1,
*PMPR_SERVER_EX_1;
```

**Header:** This specifies the version of the MPR\_SERVER\_EX\_1 structure; and MUST be a [MPRAPI\\_OBJECT\\_HEADER\\_IDL \(section 2.2.1.2.130\)](#) whose revision field MUST be 0x01, and whose type field MUST be 0x02.

**fLanOnlyMode:** Specifies whether RRAS is running on the router. If TRUE, RRAS is not running as the router; if FALSE, RRAS is running as router.

**dwUpTime:** Specifies the elapsed time, in seconds, since the router was started.

**dwTotalPorts:** Specifies the number of ports on the system.

**dwPortsInUse:** Specifies the number of ports currently in use.

**Reserved:** Unused, MUST be set to 0.

**ConfigParams:** This MUST be a [MPRAPI\\_TUNNEL\\_CONFIG\\_PARAMS\\_1](#) structure.

#### 2.2.1.2.144 MPR\_SERVER\_EX\_IDL

The **MPR\_SERVER\_EX\_IDL** structure is a place holder for [MPR\\_SERVER\\_EX\\_1](#). [<145>](#)

```
typedef
union _MPR_SERVER_EX_IDL switch (UCHAR revision) ServerConfigObject {
    case 1: MPR_SERVER_EX_1 ServerConfig1;
} MPR_SERVER_EX_IDL,
*PMPR_SERVER_EX_IDL;
```

**ServerConfig1:** MUST be a **MPR\_SERVER\_EX\_1** structure.

#### 2.2.1.2.145 MPRAPI\_TUNNEL\_CONFIG\_PARAMS\_1

The **MPRAPI\_TUNNEL\_CONFIG\_PARAMS\_1** structure is used to get or set configuration of various tunnels on RAS server. [<146>](#)

```
typedef struct _MPRAPI_TUNNEL_CONFIG_PARAMS_1 {
    IKEV2_CONFIG_PARAMS_1 IkeConfigParams;
    PPTP_CONFIG_PARAMS_1 PptpConfigParams;
    L2TP_CONFIG_PARAMS_1 L2tpConfigParams;
    SSTP_CONFIG_PARAMS_1 SstpConfigParams;
```

```

} MPRAPI_TUNNEL_CONFIG_PARAMS_1,
*PMPRAPI_TUNNEL_CONFIG_PARAMS_1;

```

**IkeConfigParams:** MUST be a [IKEV2 CONFIG PARAMS 1](#) structure and is used to get or set IKEv2 tunnel parameters.

**PptpConfigParams:** MUST be a [PPTP CONFIG PARAMS 1](#) structure and is used to get or set PPTP tunnel parameters.

**L2tpConfigParams:** MUST be a [L2TP CONFIG PARAMS 1](#) structure and is used to get or set L2TP tunnel parameters.

**SstpConfigParams:** MUST be a [SSTP CONFIG PARAMS 1](#) structure and is used to get or set SSTP tunnel parameters.

#### 2.2.1.2.146 MPR\_SERVER\_SET\_CONFIG\_EX\_1

The **MPR\_SERVER\_SET\_CONFIG\_EX\_1** structure is used to set the configuration parameters for the RRAS. [<147>](#)

```

typedef struct _MPR_SERVER_SET_CONFIG_EX_1 {
    MPRAPI_OBJECT_HEADER_IDL Header;
    DWORD setConfigForProtocols;
    MPRAPI_TUNNEL_CONFIG_PARAMS_1 ConfigParams;
} MPR_SERVER_SET_CONFIG_EX_1,
*PMPR_SERVER_SET_CONFIG_EX_1;

```

**Header:** This MUST be [MPRAPI\\_OBJECT\\_HEADER\\_IDL \(section 2.2.1.2.130\)](#), the revision field MUST be 0x01, and the type field MUST be 0x03.

**setConfigForProtocols:** This MUST be one of the following values that specify the type of tunnel.

Value	Meaning
MPRAPI_SET_CONFIG_PROTOCOL_FOR_PPTP 0x00000001	PPTP device configuration parameters are present in the structure.
MPRAPI_SET_CONFIG_PROTOCOL_FOR_L2TP 0x00000002	L2TP device configuration parameters are present in the structure.
MPRAPI_SET_CONFIG_PROTOCOL_FOR_SSTP 0x00000004	SSTP device configuration parameters are present in the structure.
MPRAPI_SET_CONFIG_PROTOCOL_FOR_IKEV2 0x00000008	IKEv2 device configuration parameters are present in the structure.

**ConfigParams:** This MUST be a MPRAPI\_TUNNEL\_CONFIG\_PARAMS\_1.

#### 2.2.1.2.147 MPR\_SERVER\_SET\_CONFIG\_EX\_IDL

The **MPR\_SERVER\_SET\_CONFIG\_EX\_IDL** structure is used to get or set configured parameters for PPTP, L2TP, SSTP, and IKEv2 devices.

```
typedef struct _MPR_SERVER_SET_CONFIG_EX_IDL switch (UCHAR revision) ServerSetConfigObject
{
    case 1: MPR_SERVER_SET_CONFIG_EX_1 ServerSetConfig1;
} MPR_SERVER_SET_CONFIG_EX_IDL,
*PMPR_SERVER_SET_CONFIG_EX_IDL;
```

**ServerSetConfig1:** This MUST be a [MPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_1](#).

#### 2.2.1.2.148 RAS\_UPDATE\_CONNECTION\_1\_IDL

The **RAS\_UPDATE\_CONNECTION\_1\_IDL** structure contains information about the tunnel endpoint address on an IKEv2 connection. [<148>](#)

```
typedef struct _RAS_UPDATE_CONNECTION_1_IDL {
    MPRAPI_OBJECT_HEADER_IDL Header;
    DWORD dwIfIndex;
    WCHAR wszRemoteEndpointAddress[65];
} RAS_UPDATE_CONNECTION_1_IDL,
*PRAS_UPDATE_CONNECTION_1_IDL;
```

**Header:** MUST be a [MPRAPI\\_OBJECT\\_HEADER\\_IDL](#).

**dwIfIndex:** MUST be set to the index of the local interface to which the connections has to be switched and on which MOBIKE [\[RFC4555\]](#) is to be sent.

**wszRemoteEndpointAddress:** Specifies a null-terminated Unicode string that holds the remote IP address to which connections has to be switched and on which MOBIKE is to be sent for the connection. This string has the form a.b.c.d in case of IPv4 address and a::b:c in case of IPv6; for example, "10.102.235.84" or "2001::a456".

#### 2.2.1.2.149 RAS\_UPDATE\_CONNECTION\_IDL

The **RAS\_UPDATE\_CONNECTION\_IDL** is used to send the MOBIKE [\[RFC4555\]](#) on an IKEv2 connection. [<149>](#)

```
typedef
union _RAS_UPDATE_CONNECTION_IDL switch (UCHAR revision) UpdateConnection {
    case 1: RAS_UPDATE_CONNECTION_1_IDL UpdateConnection1;
} RAS_UPDATE_CONNECTION_IDL,
*PRAS_UPDATE_CONNECTION_IDL;
```

**UpdateConnection1:** This MUST be an [RAS\\_UPDATE\\_CONNECTION\\_1\\_IDL](#) structure.

#### 2.2.1.2.150 IPBOOTP\_GLOBAL\_CONFIG

The **IPBOOTP\_GLOBAL\_CONFIG** structure is used to set or retrieve global configuration for the IPBOOTP. This is used in the following methods:

RRouterInterfaceTransportSetGlobalInfo

## RRouterInterfaceTransportGetGlobalInfo

```
typedef struct _IPBOOTP_GLOBAL_CONFIG {
    DWORD GC_LoggingLevel;
    DWORD GC_MaxRecvQueueSize;
    DWORD GC_ServerCount;
} IPBOOTP_GLOBAL_CONFIG,
*PIBOOTP_GLOBAL_CONFIG;
```

**GC\_LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
IPBOOTP_GLOBAL_CONFIG 0x00000000	No Logging is done.
IPBOOTP_LOGGING_ERROR 0x00000001	Only errors are logged.
IPBOOTP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IPBOOTP_LOGGING_INFO 0x00000003	Errors, warnings, and information are logged.

**GC\_MaxRecvQueueSize:** Specifies the maximum size in bytes of messages in the receive queue while processing.

**GC\_ServerCount:** The number of BOOTP server IP addresses.

### 2.2.1.2.151 IPBOOTP\_IF\_CONFIG

The **IPBOOTP\_IF\_CONFIG** structure is used to set or retrieve the per-interface configuration. This is used in the following methods:

- [RRouterInterfaceTransportAdd](#)
- [RRouterInterfaceTransportGetInfo](#)
- [RRouterInterfaceTransportSetInfo](#)

All IP address are in network order.

```
typedef struct _IPBOOTP_IF_CONFIG {
    DWORD IC_State;
    DWORD IC_RelayMode;
    DWORD IC_MaxHopCount;
    DWORD IC_MinSecondsSinceBoot;
} IPBOOTP_IF_CONFIG,
*PIBOOTP_IF_CONFIG;
```

**IC\_State:** Contains the status of the IPBOOTP. This member is read only.

Value	Meaning
IPBOOTP_STATE_ENABLED 0x00000001	The interface is enabled.
IPBOOTP_STATE_BOUND 0x00000002	The socket is bound and can listen to the IP BOOTP packets <a href="#">[RFC1542]</a> .

**IC\_RelayMode:** Contains the IPBOOTP relay mode status. It MUST be one of the following.

Value	Meaning
IPBOOTP_RELAY_DISABLED 0x00000000	The relay is configured.
IPBOOTP_RELAY_ENABLED 0x00000001	The relay is not configured.

**IC\_MaxHopCount:** The maximum number of DHCP relay agents that will handle the DHCP relayed traffic. It MUST be less than 17.

**IC\_MinSecondsSinceBoot:** The number of seconds the relay agent waits before forwarding the DHCP messages; no validation is done while setting this value.

#### 2.2.1.2.152 IPBOOTP\_MIB\_GET\_INPUT\_DATA

The **IPBOOTP\_MIB\_GET\_INPUT\_DATA** structure is passed as input data for [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _IPBOOTP_MIB_GET_INPUT_DATA {
    DWORD IMGID_TypeID;
    DWORD IMGID_IfIndex;
} IPBOOTP_MIB_GET_INPUT_DATA,
*PIPBOOTP_MIB_GET_INPUT_DATA;
```

**IMGID\_TypeID:** This MUST be one of the following.

Value	Meaning
IPBOOTP_GLOBAL_CONFIG_ID 0x00000000	The global configuration for the IPBOOTP.
IPBOOTP_IF_STATS_ID 0x00000001	The per-interface statistics.
IPBOOTP_IF_CONFIG_ID 0x00000002	The per-interface configuration.
IPBOOTP_IF_BINDING_ID 0x00000003	The IP addresses to which each interface is bound.

**IMGID\_IfIndex:** The index of the interface.

### 2.2.1.2.153 IPBOOTP\_MIB\_GET\_OUTPUT\_DATA

The **IPBOOTP\_MIB\_GET\_OUTPUT\_DATA** structure is passed as output data for [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.2.4.31\)](#), and [RMIBEntryGetNext \(section 3.2.4.32\)](#).

**Note** At the end of a table RMIBEntryGetNext wraps to the next table.

```
typedef struct _IPBOOTP_MIB_GET_OUTPUT_DATA {
    DWORD IMGOD_TypeID;
    DWORD IMGOD_IfIndex;
    BYTE IMGOD_Buffer;
} IPBOOTP_MIB_GET_OUTPUT_DATA,
*PIPBOOTP_MIB_GET_OUTPUT_DATA;
```

**IMGOD\_TypeID:** It MUST be one of the following.

Value	Meaning
IPBOOTP_GLOBAL_CONFIG_ID 0x00000000	The global configuration for the IPBOOTP, <a href="#">IPBOOTP_GLOBAL_CONFIG</a>
IPBOOTP_IF_STATS_ID 0x00000001	The per interface statistics, <a href="#">IPBOOTP_IF_STATS</a>
IPBOOTP_IF_CONFIG_ID 0x00000002	<a href="#">IPBOOTP_IF_CONFIG</a>
IPBOOTP_IF_BINDING_ID 0x00000003	The IP addresses to which each interface is bound, <a href="#">IPBOOTP_IF_BINDING</a> .

**IMGOD\_IfIndex:** The index of the interface.

**IMGOD\_Buffer:** One of the structures in the previous table based on **IMGOD\_TypeID**.

### 2.2.1.2.154 IPBOOTP\_IF\_STATS

The **IPBOOTP\_IF\_STATS** structure is an MIB entry, stores per interface statistics for the IPBOOTP. All of the IP addresses are in network order. This structure is read-only.

```
typedef struct _IPBOOTP_IF_STATS {
    DWORD IS_State;
    DWORD IS_SendFailures;
    DWORD IS_ReceiveFailures;
    DWORD IS_ArpUpdateFailures;
    DWORD IS_RequestsReceived;
    DWORD IS_RequestsDiscarded;
    DWORD IS_RepliesReceived;
    DWORD IS_RepliesDiscarded;
} IPBOOTP_IF_STATS,
*PIPBOOTP_IF_STATS;
```

**IS\_State:** Contains status of the IPBOOTP. This member is read-only.

Value	Meaning
IPBOOTP_STATE_ENABLED 0x00000001	The interface is enabled.
IPBOOTP_STATE_BOUND 0x00000002	The socket is bound and can listen to the IPBOOTP packets <a href="#">[RFC1542]</a> .

**IS\_SendFailures:** The number of relay messages that could not be sent.

**IS\_ReceiveFailures:** The number of times errors were encountered in receiving relay messages.

**IS\_ArpUpdateFailures:** The number of times errors were encountered while updating the ARP cache.

**IS\_RequestsReceived:** The number of IP BOOTP requests received.

**IS\_RequestsDiscarded:** The number of IP BOOTP requests discarded.

**IS\_RepliesReceived:** The number of IP BOOTP replies received.

**IS\_RepliesDiscarded:** The number of IP BOOTP replies discarded.

#### 2.2.1.2.155 IPBOOTP\_IF\_BINDING

In the **IPBOOTP\_IF\_BINDING** structure, the MIB entry contains the table of IP addresses to which each interface is bound. All of the IP addresses are in network order. The base structure contains the field **IB\_AddrCount**, which gives the number of IP addresses to which the indexed interface is bound. The IP addresses themselves follow the base structure and are given as [IPBOOTP\\_IP\\_ADDRESS \(section 2.2.1.2.156\)](#) structures.

```
typedef struct _IPBOOTP_IF_BINDING {
    DWORD IB_State;
    DWORD IB_AddrCount;
} IPBOOTP_IF_BINDING,
*PIPBOOTP_IF_BINDING;
```

**IB\_State:** The state of the IPBOOTP. It MUST be one of the following.

Value	Meaning
IPBOOTP_STATE_ENABLED 0x00000001	The interface is enabled.
IPBOOTP_STATE_BOUND 0x00000002	The socket is bound and can listen to the IP BOOTP packets <a href="#">[RFC1542]</a> .

**IB\_AddrCount:** The number of IP addresses to which the indexed interface is bound.



### 2.2.1.2.156 IPBOOTP\_IP\_ADDRESS

The **IPBOOTP\_IP\_ADDRESS** structure is used for storing interface bindings. A series of structures of this type follows the [IPBOOTP\\_IF\\_BINDING](#) structure. Both fields are IP address fields in network order.

```
typedef struct _IPBOOTP_IP_ADDRESS {  
    DWORD IA_Address;  
    DWORD IA_Netmask;  
} IPBOOTP_IP_ADDRESS,  
*PIPBOOTP_IP_ADDRESS;
```

**IA\_Address:** The IP address in network byte order.

**IA\_Netmask:** The network mask in network byte order. See [\[RFC950\]](#).

### 2.2.1.2.157 DHCPV6R\_MIB\_GET\_OUTPUT\_DATA

The **DHCPV6R\_MIB\_GET\_OUTPUT\_DATA** structure is passed as output data for [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _DHCPV6R_MIB_GET_OUTPUT_DATA {  
    DWORD IMGOD_TypeID;  
    DWORD IMGOD_IfIndex;  
    BYTE IMGOD_Buffer[1];  
} DHCPV6R_MIB_GET_OUTPUT_DATA,  
*PDHCPV6R_MIB_GET_OUTPUT_DATA;
```

**IMGOD\_TypeID:** It MUST be one of the following:

Value	Meaning
DHCPV6R_IF_STATS_ID 0x00000001	The interface statistics data, <a href="#">DHCPV6R_IF_STATS (section 2.2.1.2.159)</a> , is specified in the location that starts with IMGOD_Buffer.

**IMGOD\_IfIndex:** The index of the interface.

**IMGOD\_Buffer:** This specifies the output data corresponding to the type specified by IMGOD\_TypeID.

### 2.2.1.2.158 DHCPV6R\_GLOBAL\_CONFIG

The **DHCPV6R\_GLOBAL\_CONFIG** structure contains the global configuration of the DHCPV6 Relay Agent. This structure is used in the following methods:

[RRouterInterfaceTransportSetGlobalInfo](#)

[RRouterInterfaceTransportGetGlobalInfo](#)

This structure is variable length, after the base structure there will be an array of GC\_ServerCount in6\_addr, each of which contains an IPv6 address of a DHCP server to which packets will be sent. All IPv6 address fields MUST be in network order.

```
typedef struct _DHCPV6R_GLOBAL_CONFIG {
    DWORD GC_LoggingLevel;
    DWORD GC_MaxRecvQueueSize;
    DWORD GC_ServerCount;
} DHCPV6R_GLOBAL_CONFIG,
*PDHCPV6R_GLOBAL_CONFIG;
```

**GC\_LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
DHCPV6R_LOGGING_NONE 0x00000000	No logging is done.
DHCPV6R_LOGGING_ERROR 0x00000001	Only errors are logged.
DHCPV6R_LOGGING_WARN 0x00000002	Errors and warnings are logged.
DHCPV6R_LOGGING_INFO 0x00000003	Errors, warnings, and information are logged.

**GC\_MaxRecvQueueSize:** Specifies the maximum size in bytes of messages in the receive queue while processing

**GC\_ServerCount:** The number of the IPv6 addresses of DHCP servers.

#### 2.2.1.2.159 DHCPV6R\_IF\_STATS

The **DHCPV6R\_IF\_STATS** structure stores per interface statistics for the DHCPv6 relay agent. This structure is read-only. This structure is part of [DHCPV6R\\_MIB\\_GET\\_OUTPUT\\_DATA \(section 2.2.1.2.157\)](#).

```
typedef struct _DHCPV6R_IF_STATS {
    DWORD IS_State;
    DWORD IS_SendFailures;
    DWORD IS_ReceiveFailures;
    DWORD IS_RequestsReceived;
    DWORD IS_RequestsDiscarded;
    DWORD IS_RepliesReceived;
    DWORD IS_RepliesDiscarded;
} DHCPV6R_IF_STATS,
*PDHCPV6R_IF_STATS;
```

**IS\_State:** Contains the status of the DHCPv6 relay agent. This member is read-only and MUST be a combination of one or more of the following flags:

Value	Meaning
DHCPV6R_STATE_ENABLED 0x00000001	The interface is enabled.
DHCPV6R_STATE_BOUND 0x00000002	The socket is bound and can listen to the DHCPv6 relay agent packets <a href="#">[RFC3315]</a> .

**IS\_SendFailures:** The number of relay messages that could not be sent.

**IS\_ReceiveFailures:** The number of times errors were encountered while receiving relay messages.

**IS\_RequestsReceived:** The number of DHCPV6 relay requests received.

**IS\_RequestsDiscarded:** The number of DHCPV6 relay requests discarded.

**IS\_RepliesReceived:** The number of DHCPV6 relay replies received.

**IS\_RepliesDiscarded:** The number of DHCPV6 relay replies discarded.

#### 2.2.1.2.160 DHCPV6R\_IF\_CONFIG

The **DHCPV6R\_IF\_CONFIG** structure is an MIB entry and describes the per-interface configuration. The field **IC\_State** is read-only. This structure is used in [DHCPV6R MIB GET INPUT DATA \(section 2.2.1.2.161\)](#) and [DHCPV6R MIB GET OUTPUT DATA \(section 2.2.1.2.157\)](#).

```
typedef struct _DHCPV6R_IF_CONFIG {
    DWORD IC_State;
    DWORD IC_RelayMode;
    DWORD IC_MaxHopCount;
    DWORD IC_MinSecondsSinceBoot;
} DHCPV6R_IF_CONFIG,
*PDHCPV6R_IF_CONFIG;
```

**IC\_State:** Contains the status of the DHCPV6 relay. This member is read-only and MUST be a combination of one or more of the following flags:

Value	Meaning
DHCPV6R_STATE_ENABLED 0x00000001	The interface is enabled
DHCPV6R_STATE_BOUND 0x00000002	The socket is bound and can listen to the DHCPv6 relay agent packets <a href="#">[RFC3315]</a> .

**IC\_RelayMode:** Contains the DHCPV6 relay mode status. It MUST be one of the following.

Value	Meaning
DHCPV6R_RELAY_DISABLED 0x00000000	The relay is configured.
DHCPV6R_RELAY_ENABLED	The relay is not configured.

Value	Meaning
0x00000001	

**IC\_MaxHopCount:** The maximum number of DHCPv6 relay agents that will handle the DHCPv6 relayed traffic. It MUST be less than 33.

**IC\_MinSecondsSinceBoot:** The number of seconds the relay agent waits before forwarding the DHCPv6 messages.

#### 2.2.1.2.161 DHCPV6R\_MIB\_GET\_INPUT\_DATA

The **DHCPV6R\_MIB\_GET\_INPUT\_DATA** structure is passed as input for [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _DHCPV6R_MIB_GET_INPUT_DATA {
    DWORD IMGID_TypeID;
    DWORD IMGID_IfIndex;
} DHCPV6R_MIB_GET_INPUT_DATA,
*PDHCPV6R_MIB_GET_INPUT_DATA;
```

**IMGID\_TypeID:** This MUST be one of the following.

Value	Meaning
DHCPV6R_IF_STATS_ID 0x00000001	Interface statistics data

**IMGID\_IfIndex:** The index of the interface for which Get has to be performed.

#### 2.2.1.2.162 IPRIP\_MIB\_GET\_INPUT\_DATA

The **IPRIP\_MIB\_GET\_INPUT\_DATA** structure is passed as input data for [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#). All of the IP addresses MUST be in network order.

```
typedef struct _IPRIP_MIB_GET_INPUT_DATA {
    DWORD IMGID_TypeID;
    union {
        DWORD IMGID_IfIndex;
        DWORD IMGID_PeerAddress;
    };
} IPRIP_MIB_GET_INPUT_DATA,
*PIPRIP_MIB_GET_INPUT_DATA;
```

**IMGID\_TypeID:** This MUST be one of the following.

Value	Meaning
IPRIP_GLOBAL_STATS_ID	The global statistics for the Microsoft Internet Protocol Routing

Value	Meaning
0x00000000	Information Protocol (IPRIP).
IPRIP_GLOBAL_CONFIG_ID 0x00000001	The global configuration for the IPRIP.
IPRIP_IF_STATS_ID 0x00000002	The per-interface statistics for the IPRIP.
IPRIP_IF_CONFIG_ID 0x00000003	The per-interface configuration.
IPRIP_IF_BINDING_ID 0x00000004	The table of IP addresses to which each interface is bound.
IPRIP_PEER_STATS_ID 0x00000005	The statistics kept about neighboring routers.

**(unnamed union):** The interface index or peer IP address for which data specified by **IMGID\_TypeID** needs to be retrieved.

### 2.2.1.2.163 IPRIP\_MIB\_GET\_OUTPUT\_DATA

The **IPRIP\_MIB\_GET\_OUTPUT\_DATA** structure is populated by [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

```
typedef struct _IPRIP_MIB_GET_OUTPUT_DATA {
    DWORD IMGOD_TypeID;
    union {
        DWORD IMGID_IfIndex;
        DWORD IMGID_PeerAddress;
    };
    BYTE IMGOD_Buffer[1];
} IPRIP_MIB_GET_OUTPUT_DATA,
*PIPRIP_MIB_GET_OUTPUT_DATA;
```

**IMGOD\_TypeID:** This MUST be one of the following.

Value	Meaning
IPRIP_GLOBAL_STATS_ID 0x00000000	The global statistics for the IP RIP, <a href="#">IPRIP GLOBAL STATS (section 2.2.1.2.164)</a> .
IPRIP_GLOBAL_CONFIG_ID 0x00000001	The global configuration for the IP RIP, <a href="#">IPRIP GLOBAL CONFIG (section 2.2.1.2.165)</a> .
IPRIP_IF_STATS_ID 0x00000002	The per-interface statistics for the IP RIP, <a href="#">IPRIP IF STATS (section 2.2.1.2.166)</a> .
IPRIP_IF_CONFIG_ID 0x00000003	The per-interface configuration, <a href="#">IPRIP IF CONFIG (section 2.2.1.2.167)</a> .
IPRIP_IF_BINDING_ID	The table of IP addresses to which each interface is bound,

Value	Meaning
0x00000004	<a href="#">IPRIP_IF_BINDING</a> .
IPRIP_PEER_STATS_ID 0x00000005	The statistics kept about neighboring routers, <a href="#">IPRIP_PEER_STATS (section 2.2.1.2.171)</a> .

**(unnamed union):** The interface index or peer IP address for which data specified by **IMGOD\_TypeID** needs to be retrieved.

**IMGOD\_Buffer:** One of the structures in the previous table based on the **IMGOD\_TypeID**.

#### 2.2.1.2.164 IPRIP\_GLOBAL\_STATS

The **IPRIP\_GLOBAL\_STATS** structure contains global statistics for the IP RIP. There is only one instance, so this entry has no index. This structure is read-only. This structure is used in [IPRIP\\_MIB\\_GET\\_INPUT\\_DATA \(section 2.2.1.2.162\)](#) and [IPRIP\\_MIB\\_GET\\_OUTPUT\\_DATA \(section 2.2.1.2.163\)](#).

```
typedef struct _IPRIP_GLOBAL_STATS {
    DWORD GS_SystemRouteChanges;
    DWORD GS_TotalResponsesSent;
} IPRIP_GLOBAL_STATS,
*PIPRIP_GLOBAL_STATS;
```

**GS\_SystemRouteChanges:** The number of global route changes due to the IPRIP.

**GS\_TotalResponsesSent:** The count of global RIP responses sent.

#### 2.2.1.2.165 IPRIP\_GLOBAL\_CONFIG

The **IPRIP\_GLOBAL\_CONFIG** structure contains global configuration for the IPRIP. This structure is used in [IPRIP\\_MIB\\_GET\\_INPUT\\_DATA \(section 2.2.1.2.162\)](#), [IPRIP\\_MIB\\_GET\\_OUTPUT\\_DATA \(section 2.2.1.2.163\)](#), and the following methods:

- [RRouterInterfaceTransportSetGlobalInfo](#)
- [RRouterInterfaceTransportGetGlobalInfo](#)

There is only one instance of this entry in the MIB. Following it is an array of **GC\_PeerFilterCount** DWORDs, each of which contains an IP address which is a peer which will be accepted or rejected depending on the value of **GC\_PeerFilterMode**. If the **GC\_PeerFilterMode** is set to **IPRIP\_FILTER\_EXCLUDE**, routes will be rejected which come from the routers whose addresses are in the peer array, and all other routers will be accepted.

Likewise, if the **GC\_PeerFilterMode** is set to **IPRIP\_FILTER\_INCLUDE**, routes will be only be accepted if they are from the routers in the peer array.

```
typedef struct _IPRIP_GLOBAL_CONFIG {
    DWORD GC_LoggingLevel;
    DWORD GC_MaxRecvQueueSize;
    DWORD GC_MaxSendQueueSize;
    DWORD GC_MinTriggeredUpdateInterval;
    DWORD GC_PeerFilterMode;
```

```

    DWORD GC_PeerFilterCount;
} IPRIP_GLOBAL_CONFIG,
*PIPRIP_GLOBAL_CONFIG;

```

**GC\_LoggingLevel:** Specifies the logging level. This MUST be one of the following values.

Value	Meaning
IPRIP_LOGGING_NONE 0x00000000	No logging is done.
IPRIP_LOGGING_ERROR 0x00000001	Only errors are logged.
IPRIP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IPRIP_LOGGING_INFO 0x00000003	Errors, warnings, and information is logged.

**GC\_MaxRecvQueueSize:** The maximum queue size of outstanding RIP messages that need to be processed.

**GC\_MaxSendQueueSize:** The maximum queue size for outstanding RIP messages that have been sent out.

**GC\_MinTriggeredUpdateInterval:** The minimum amount of time router waits before it sends triggered updates.

**GC\_PeerFilterMode:** Specifies whether route changes from all the IP addresses are accepted. It MUST be one of the following:

Value	Meaning
IPRIP_FILTER_DISABLED 0x00000000	Updates from all the IP addresses are accepted.
IPRIP_FILTER_INCLUDE 0x00000001	Updates only from the IP addresses specified in this structure after GC_PeerFilterCount are accepted.
IPRIP_FILTER_EXCLUDE 0x00000002	Ignores updates from the IP addresses specified in this structure after GC_PeerFilterCount.

**GC\_PeerFilterCount:** The number of IP addresses in this structure after this field.

#### 2.2.1.2.166 IPRIP\_IF\_STATS

The **IPRIP\_IF\_STATS** structure contains per-interface statistics for the IPRIP. This structure is read-only. This structure is used in [IPRIP MIB GET INPUT DATA \(section 2.2.1.2.162\)](#) and [IPRIP MIB GET OUTPUT DATA \(section 2.2.1.2.163\)](#).

```

typedef struct _IPRIP_IF_STATS {
    DWORD IS_State;
    DWORD IS_SendFailures;
}

```

```

DWORD IS_ReceiveFailures;
DWORD IS_RequestsSent;
DWORD IS_RequestsReceived;
DWORD IS_ResponsesSent;
DWORD IS_ResponsesReceived;
DWORD IS_BadResponsePacketsReceived;
DWORD IS_BadResponseEntriesReceived;
DWORD IS_TriggeredUpdatesSent;
} IPRIP_IF_STATS,
*PIPRIP_IF_STATS;

```

**IS\_State:** The IP RIP state on the interface. It MUST be a combination of one or more of the following values.

Value	Meaning
IPRIP_STATE_ENABLED 0x00000001	IP RIP is enabled.
IPRIP_STATE_BOUND 0x00000002	The socket is bound.

**IS\_SendFailures:** The number of send failures on the interface.

**IS\_ReceiveFailures:** The number of receive failures on the interface.

**IS\_RequestsSent:** The number of requests sent on the interface.

**IS\_RequestsReceived:** The number of requests received on the interface.

**IS\_ResponsesSent:** The number of responses sent on the interface.

**IS\_ResponsesReceived:** The number of responses received on the interface.

**IS\_BadResponsePacketsReceived:** The number of bad response packets received.

**IS\_BadResponseEntriesReceived:** The number of bad response entries received.

**IS\_TriggeredUpdatesSent:** The number of triggered updates sent.

#### 2.2.1.2.167 IPRIP\_IF\_CONFIG

The **IPRIP\_IF\_CONFIG** structure contains the per-interface configuration. This structure is used in [IPRIP\\_MIB\\_GET\\_INPUT\\_DATA \(section 2.2.1.2.162\)](#), [IPRIP\\_MIB\\_GET\\_OUTPUT\\_DATA \(section 2.2.1.2.163\)](#), and the following methods:

[RRouterInterfaceTransportAdd](#)

[RRouterInterfaceTransportGetInfo](#)

[RRouterInterfaceTransportSetInfo](#)



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	30	1
IC_State																															
IC_Metric																															
IC_UpdateMode																															
IC_AcceptMode																															
IC_AnnounceMode																															
IC_ProtocolFlags																															
IC_RouteExpirationInterval																															
IC_RouteRemovalInterval																															
IC_FullUpdateInterval																															
IC_AuthenticationType																															
IC_AuthenticationKey																															
...																															
...																															
...																															
IC_RouteTag																IC_Padding															
IC_UnicastPeerMode																															
IC_AcceptFilterMode																															
IC_AnnounceFilterMode																															
IC_UnicastPeerCount																															
IC_AcceptFilterCount																															
IC_AnnounceFilterCount																															
IC_UnicastPeer (variable)																															

...
IC_AcceptFilter (variable)
...
IC_AnnounceFilter (variable)
...

**IC\_State (4 bytes):** Specifies the IP RIP state on the interface. This field **MUST** be read-only and **MUST** be ignored if modified. It **MUST** be a combination of one or more of the following values.

Value	Meaning
IPRIP_STATE_ENABLED 0x00000001	The IP RIP is enabled.
IPRIP_STATE_BOUND 0x00000002	The socket is bound.

**IC\_Metric (4 bytes):** Specifies the metric of the interface.

**IC\_UpdateMode (4 bytes):** Specifies whether the update mode is periodic or on demand.

Value	Meaning
IPRIP_UPDATE_PERIODIC 0x00000000	The RIP updates are done periodically.
IPRIP_UPDATE_DEMAND 0x00000001	The RIP updates are done only when there is change.

**IC\_AcceptMode (4 bytes):** Specifies the type of routes that are accepted.

Value	Meaning
IPRIP_ACCEPT_DISABLED 0x00000000	Does not accept routes.
IPRIP_ACCEPT_RIP1 0x00000001	Accepts RIPv1 routes.
IPRIP_ACCEPT_RIP1_COMPAT 0x00000002	Accepts RIPv1 compatible routes (RIPv1 was designed to be compatible with future versions of the RIP. If a RIPv1 router receives a message and if the RIP version indicated in the RIP header is not 1, the RIPv1 router does not discard the RIP announcement, but instead processes only the RIPv1 defined fields.)
IPRIP_ACCEPT_RIP2 0x00000003	Accepts RIPv2 routes. See <a href="#">RFC1723</a> .

**IC\_AnnounceMode (4 bytes):** Specifies the type of routes that are announced.

Value	Meaning
IPRIP_ANNOUNCE_DISABLED 0x00000000	Does not announce routes.
IPRIP_ANNOUNCE_RIP1 0x00000001	Announces RIPv1 routes.
IPRIP_ANNOUNCE_RIP1_COMPAT 0x00000002	Accepts RIPv1 compatible routes. (RIPv1 was designed to be compatible with future versions of the RIP. If a RIPv1 router receives a message and if the RIP version indicated in the RIP header is not 1, the RIPv1 router does not discard the RIP announcement, but instead processes only the RIPv1 defined fields.)
IPRIP_ANNOUNCE_RIP2 0x00000003	Announces RIPv2 routes. See <a href="#">[RFC1723]</a> .

**IC\_ProtocolFlags (4 bytes):** Specifies which routes are included or excluded from RIP announcements.

Value	Meaning
IPRIP_FLAG_ACCEPT_HOST_ROUTES 0x00000000	Specifies whether host routes in received RIP announcements are accepted.
IPRIP_FLAG_ANNOUNCE_HOST_ROUTES 0x00000002	Specifies whether host routes are included in RIP announcements.
IPRIP_FLAG_ACCEPT_DEFAULT_ROUTES 0x00000004	Specifies whether host routes are included in RIP announcements.
IPRIP_FLAG_ANNOUNCE_DEFAULT_ROUTES 0x00000008	Specifies whether default routes are included in RIP announcements.
IPRIP_FLAG_SPLIT_HORIZON 0x00000010	Enables split-horizon processing. Specifies whether routes learned on a network are not announced in RIP announcements sent on that network.
IPRIP_FLAG_POISON_REVERSE 0x00000020	Enables the poison-reverse processing. Specifies whether routes learned on a network are announced with a metric of 16 (unreachable) in RIP announcements sent on that network.
IPRIP_FLAG_GRACEFUL_SHUTDOWN 0x00000040	Sends cleanup updates when shutting down. Specifies whether, if the RIP is stopping on this interface, the RIP sends an announcement with all routes that are marked with a metric of 15. This enables neighboring routers to immediately update their routing tables to indicate that the routes available through the router that is stopping are no longer reachable.
IPRIP_FLAG_TRIGGERED_UPDATES	Enables triggered updates processing.

Value	Meaning
0x00000080	Specifies whether new routes and metric changes trigger an immediate update that includes only the changes. This is called a triggered update.
IPRIP_FLAG_OVERWRITE_STATIC_ROUTES 0x00000100	Overwrites the static routes on the interface.
IPRIP_FLAG_NO_SUBNET_SUMMARY 0x00000200	Specifies that subnet routes are not summarized in the form of the class-based network ID when announced on a network that is not a subnet of the class-based network ID. By default, subnet summarization is disabled.

**IC\_RouteExpirationInterval (4 bytes):** The lifetime (in seconds) of a route that is learned through the RIP before it expires.

**IC\_RouteRemovalInterval (4 bytes):** The amount of time (in seconds) after which a RIP-learned route that has expired is removed from the routing table.

**IC\_FullUpdateInterval (4 bytes):** The number of seconds between full RIP updates.

**IC\_AuthenticationType (4 bytes):** One of the following values.

Value	Meaning
IPRIP_AUTHTYPE_NONE 0x00000001	No authentication is used.
IPRIP_AUTHTYPE_SIMPLE_PASSWORD 0x00000002	Password authentication is used. Plain comparison of text is made.
IPRIP_AUTHTYPE_MD5 0x00000003	This is unused.

**IC\_AuthenticationKey (16 bytes):** The authentication data being sent depending on IC\_AuthenticationType. This MUST be a write-only field and MUST be ignored on receive.

**IC\_RouteTag (2 bytes):** A tag number for the routes advertised on this interface. Use this option if to have all packets sent over this interface to include a tag in RIP version 2 announcements. See [\[RFC1723\]](#).

**IC\_Padding (2 bytes):** This is a padding field and MUST be set to 0 and ignored on receive.

**IC\_UnicastPeerMode (4 bytes):** This MUST be one of the following values.

Value	Meaning
IPRIP_PEER_DISABLED 0x00000000	RIP packets will not be sent to peers.
IPRIP_PEER_ALSO 0x00000001	RIP packets will be sent to peers, as well as being sent via broadcast or multicast.
IPRIP_PEER_ONLY 0x00000002	RIP packets will only be sent to the peers specified in the structure.

**IC\_AcceptFilterMode (4 bytes):** This MUST be one of the following values.

Value	Meaning
IPRIP_FILTER_DISABLED 0x00000000	Updates from all IP addresses are accepted.
IPRIP_FILTER_INCLUDE 0x00000001	Updates are only accepted from the IP addresses specified by the IC_AcceptFilter.
IPRIP_FILTER_EXCLUDE 0x00000002	Ignores updates from the IP addresses specified by the IC_AcceptFilter.

**IC\_AnnounceFilterMode (4 bytes):** This MUST be one of the following values.

Value	Meaning
IPRIP_FILTER_DISABLED 0x00000000	Updates from all IP addresses are accepted.
IPRIP_FILTER_INCLUDE 0x00000001	Updates are only accepted from IP addresses specified by the IC_AnnounceFilter.
IPRIP_FILTER_EXCLUDE 0x00000002	Ignores updates from the IP addresses specified by the IC_AnnounceFilter.

**IC\_UnicastPeerCount (4 bytes):** The number of peer IP addresses specified in **IC\_UnicastPeer** array.

**IC\_AcceptFilterCount (4 bytes):** The number of accept filters specified in **IC\_AcceptFilter**.

**IC\_AnnounceFilterCount (4 bytes):** The number of announce filters specified in **IC\_AnnounceFilter**.

**IC\_UnicastPeer (variable):** This specifies an array of IPv4 address of the peers in network byte order. The array MUST have **IC\_UnicastPeerCount** number of elements in it.

**IC\_AcceptFilter (variable):** This specifies an array of [IPRIP\\_ROUTE\\_FILTER \(section 2.2.1.2.168\)](#) entries. The array MUST have **IC\_AcceptFilterCount** number of elements in it. The default filter action to be applied for these filters is specified by **IC\_AcceptFilterMode**.

**IC\_AnnounceFilter (variable):** This specifies an array of **IPRIP\_ROUTE\_FILTER** (section 2.2.1.2.168) entries. The array MUST have **IC\_AnnounceFilterCount** number of elements in it. The default filter action to be applied for these filters is specified by **IC\_AnnounceFilterMode**.

#### 2.2.1.2.168 IPRIP\_ROUTE\_FILTER

The **IPRIP\_ROUTE\_FILTER** structure is used to specify a route filter for use in the **IC\_AcceptFilter** and **IC\_AnnounceFilter** fields of the [IPRIP\\_IF\\_CONFIG \(section 2.2.1.2.167\)](#) structure.

```
typedef struct _IPRIP_ROUTE_FILTER {  
    DWORD RF_LoAddress;  
    DWORD RF_HiAddress;  
} IPRIP_ROUTE_FILTER,
```

```
*PIPRIP_ROUTE_FILTER;
```

**RF\_LoAddress:** The starting IPv4 address of the route filter specified in network byte order.

**RF\_HiAddress:** The ending IPv4 address of the route filter specified in network byte order.

### 2.2.1.2.169 IPRIP\_IF\_BINDING

The **IPRIP\_IF\_BINDING** structure is an MIB entry that contains the table of IP addresses to which each interface is bound. This structure is used in [IPRIP MIB GET INPUT DATA \(section 2.2.1.2.162\)](#) and [IPRIP MIB GET OUTPUT DATA \(section 2.2.1.2.163\)](#).

All IP addresses are in network order. This structure is variable length.

The base structure contains the field **IB\_AddrCount**, which gives the number of IP addresses to which the indexed interface is bound. The IP addresses themselves follow the base structure and are given as [IPRIP\\_IP\\_ADDRESS \(section 2.2.1.2.170\)](#) structures. This MIB entry is read-only.

```
typedef struct _IPRIP_IF_BINDING {  
    DWORD IB_State;  
    DWORD IB_AddrCount;  
} IPRIP_IF_BINDING,  
*PIPRIP_IF_BINDING;
```

**IB\_State:** The IP RIP state on the interface. It MUST be a combination of one or more of the following values.

Value	Meaning
IPRIP_STATE_ENABLED 0x00000001	The IP RIP is enabled.
IPRIP_STATE_BOUND 0x00000002	The socket is bound.

**IB\_AddrCount:** The number of IPRIP\_IP\_ADDRESS structures present at the end of this structure.

### 2.2.1.2.170 IPRIP\_IP\_ADDRESS

The **IPRIP\_IP\_ADDRESS** structure is used for storing interface bindings. A series of structures of this type follows the [IPRIP\\_IF\\_BINDING \(section 2.2.1.2.169\)](#) structure. This structure is used in **IPRIP\_IF\_BINDING**. Both fields are IP address fields in network-order.

```
typedef struct _IPRIP_IP_ADDRESS {  
    DWORD IA_Address;  
    DWORD IA_Netmask;  
} IPRIP_IP_ADDRESS,  
*PIPRIP_IP_ADDRESS;
```

**IA\_Address:** The IP address.

**IA\_Netmask:** The net mask. See [\[RFC950\]](#).

#### 2.2.1.2.171 IPRIP\_PEER\_STATS

The **IPRIP\_PEER\_STATS** structure is an MIB entry that describes the statistics kept about neighboring routers. All IP addresses are in network order. This structure is read-only. This structure is used in [IPRIP\\_MIB\\_GET\\_INPUT\\_DATA \(section 2.2.1.2.162\)](#) and [IPRIP\\_MIB\\_GET\\_OUTPUT\\_DATA \(section 2.2.1.2.163\)](#).

```
typedef struct _IPRIP_PEER_STATS {
    DWORD PS_LastPeerRouteTag;
    DWORD PS_LastPeerUpdateTickCount;
    DWORD PS_LastPeerUpdateVersion;
    DWORD PS_BadResponsePacketsFromPeer;
    DWORD PS_BadResponseEntriesFromPeer;
} IPRIP_PEER_STATS,
*IPRIP_PEER_STATS;
```

**PS\_LastPeerRouteTag:** The route tag last received from the peer.

**PS\_LastPeerUpdateTickCount:** The number of updates received from peer.

**PS\_LastPeerUpdateVersion:** The RIP version of the last update received from peer.

**PS\_BadResponsePacketsFromPeer:** The number of bad response packets received from peer.

**PS\_BadResponseEntriesFromPeer:** The number of bad entries in responses received from peer.

#### 2.2.1.2.172 IGMP\_MIB\_GET\_INPUT\_DATA

The **IGMP\_MIB\_GET\_INPUT\_DATA** structure is passed as input data for [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#). All IP addresses MUST be in network order.

```
typedef struct _IGMP_MIB_GET_INPUT_DATA {
    DWORD TypeID;
    USHORT Flags;
    USHORT Signature;
    DWORD IfIndex;
    DWORD RasClientAddr;
    DWORD GroupAddr;
    DWORD Count;
} IGMP_MIB_GET_INPUT_DATA,
*PIGMP_MIB_GET_INPUT_DATA;
```

**TypeID:** Specifies the type of entry being requested. It MUST be one of the following, otherwise an error is returned.

Value	Meaning
IGMP_IF_STATS_ID 0x00000004	The Internet Group Management Protocol (IGMP) statistics for an interface. If <b>TypeID</b> is set to this value, <b>Count</b> MUST be non-zero.
IGMP_IF_GROUPS_LIST_ID 0x00000005	The list of multicast group members on an interface. If <b>TypeID</b> is set to this value, <b>Count</b> MUST be non-zero.
IGMP_GROUP_IFS_LIST_ID 0x00000006	The list of interfaces joined for a group. If <b>TypeID</b> is set to this value, <b>Count</b> MUST be non-zero and <b>GroupAddr</b> MUST match a valid existing IGMP group address.
IGMP_PROXY_IF_INDEX_ID 0x00000007	Returns the index of the interface owned by the IGMP proxy. <b>RMIBEntryGetNext</b> is invalid as there is only one proxy interface and ERROR_NO_MORE_ITEMS is returned.

**Flags:** This MUST be one of the following combinations, otherwise an error is returned.

Value	Meaning
IGMP_ENUM_FOR_RAS_CLIENTS 0x00000001	Enumerate for RAS clients only.
IGMP_ENUM_ONE_ENTRY 0x00000002	Return only one interface group entry.
IGMP_ENUM_ALL_INTERFACES_GROUPS 0x00000004	Enumerate all interfaces. If enumeration reaches end of an interface, it will go to the next interface.
IGMP_ENUM_ALL_TABLES 0x00000010	Enumerate all tables.
IGMP_ENUM_SUPPORT_FORMAT_IGMPV3 0x00000010	Set if IGMPv3 is supported.

**Signature:** This MUST be set to zero.

**IfIndex:** The index of the interface for which information needs to be retrieved.

**RasClientAddr:** The address of the RAS client for which information needs to be retrieved.

**GroupAddr:** The IGMP group address for which information needs to be retrieved.

**Count:** The count of entries that need to be retrieved.

## 2.2.1.2.173 IGMP\_MIB\_GET\_OUTPUT\_DATA

The **IGMP\_MIB\_GET\_OUTPUT\_DATA** structure is written into the output data on calling [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
TypeID																															



Flags
Count
Buffer (variable)
...

**TypeID (4 bytes):** Specifies the type of entry being populated.

Value	Meaning
IGMP_IF_STATS_ID 0x00000004	Returns the statistics for an interface, see <a href="#">IGMP MIB IF STATS</a> for more details.
IGMP_IF_GROUPS_LIST_ID 0x00000005	Returns the list of multicast group members on an interface, <a href="#">IGMP MIB IF GROUPS LIST</a> .
IGMP_GROUP_IFS_LIST_ID 0x00000006	Returns the list of interfaces joined for that group, <a href="#">IGMP MIB GROUP IFS LIST</a> .
IGMP_PROXY_IF_INDEX_ID 0x00000007	Returns the index of interface owned by the IGMP proxy.

**Flags (4 bytes):** This MUST be a combination of the following flags.

Value	Meaning
IGMP_ENUM_FOR_RAS_CLIENTS 0x00000001	Enumerate for RAS clients only.
IGMP_ENUM_ONE_ENTRY 0x00000002	Returns only one interface group entry.
IGMP_ENUM_ALL_INTERFACES_GROUPS 0x00000004	Enumerate all interfaces. If the enumeration reaches the end of an interface, it will go to the next interface.
IGMP_ENUM_ALL_TABLES 0x00000010	Enumerate all tables.
IGMP_ENUM_SUPPORT_FORMAT_IGMPV3 0x00000010	Set if IGMPv3 is supported.
IGMP_ENUM_INTERFACE_TABLE_BEGIN 0x00000100	Indicates the beginning of the table.
IGMP_ENUM_INTERFACE_TABLE_CONTINUE 0x00000200	The enumeration for the interface has to continue.
IGMP_ENUM_INTERFACE_TABLE_END 0x00000400	End of the enumeration for the interface.
IGMP_ENUM_FORMAT_IGMPV3 0x00001000	A set of IGMPv3 information is present.

**Count (4 bytes):** The number of entries being returned.

**Buffer (variable):** One of the structures specified previously depending on the **TypeId**.

#### 2.2.1.2.174 IGMP\_MIB\_GLOBAL\_CONFIG

The **IGMP\_MIB\_GLOBAL\_CONFIG** structure contains the global configuration for the IGMP. This structure is used in the following methods.

[RRouterInterfaceTransportSetGlobalInfo \(Opnum 9\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(Opnum 10\)](#)

```
typedef struct _IGMP_MIB_GLOBAL_CONFIG {  
    DWORD Version;  
    DWORD LoggingLevel;  
} IGMP_MIB_GLOBAL_CONFIG,  
*IGMP_MIB_GLOBAL_CONFIG;
```

**Version:** It MUST be one of the following.

Value	Meaning
IGMP_VERSION_1_2 0x00000201	IGMPv1 or IGMPv2
IGMP_VERSION_3 0x00000301	IGMPv3

**LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
IGMP_LOGGING_NONE 0x00000000	No logging is done.
IGMP_LOGGING_ERROR 0x00000001	Only errors are logged.
IGMP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IGMP_LOGGING_INFO 0x00000003	Errors, warnings, and information is logged.

**RasClientStats:** If **RASClientStats** is nonzero, then per RAS client statistics are maintained.

#### 2.2.1.2.175 IGMP\_MIB\_IF\_CONFIG

The **IGMP\_MIB\_IF\_CONFIG** structure contains per-interface configuration. This structure is used in the following methods:

[RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)

[RRouterInterfaceTransportGetInfo \(section 3.2.4.19\)](#)

[RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

All IP address fields MUST be in network order.

```
typedef struct _IGMP_MIB_IF_CONFIG {
    DWORD Version;
    DWORD IfIndex;
    DWORD IpAddr;
    DWORD IfType;
    DWORD Flags;
    DWORD IgmpProtocolType;
    DWORD RobustnessVariable;
    DWORD StartQueryInterval;
    DWORD StartQueryCount;
    DWORD GenQueryInterval;
    DWORD GenQueryMaxResponseTime;
    DWORD LastMemQueryInterval;
    DWORD LastMemQueryCount;
    DWORD OtherQuerierPresentInterval;
    DWORD GroupMembershipTimeout;
    DWORD NumStaticGroups;
} IGMP_MIB_IF_CONFIG,
*PIGMP_MIB_IF_CONFIG;
```

**Version:** It MUST be one of the following.

Value	Meaning
IGMP_VERSION_1_2 0x00000201	IGMPv1 or IGMPv2
IGMP_VERSION_3 0x00000301	IGMPv3

**IfIndex:** The index of the interface, it is read-only.

**IpAddr:** The IP address of the interface, it is read-only.

**IfType:** The type of the interface, it is read-only. It MUST be one of the following.

Value	Meaning
IGMP_IF_NOT_RAS 0x00000001	The interface is connected to a LAN.
IGMP_IF_RAS_ROUTER 0x00000002	The interface is connected to another router over RAS.
IGMP_IF_RAS_SERVER	The entry corresponds to a RAS server if it contains statistics, then it

Value	Meaning
0x00000003	represents summarized statistics.
IGMP_IF_RAS_CLIENT 0x00000004	The entry corresponds to a RAS client.
IGMP_IF_PROXY 0x00000008	One of the first four flags will still be set to enable the switch from the proxy to an IGMP router.

**Flags:** It MUST be one of the following.

Value	Meaning
IGMP_INTERFACE_ENABLED_IN_CONFIG 0x00000001	The interface is enabled in this configuration.
IGMP_ACCEPT_RTRALERT_PACKETS_ONLY 0x00000002	Can accept only router alerts.

**IgmpProtocolType:**

Value	Meaning
IGMP_PROXY 0x00000000	The interface is an IGMPv2 proxy.
IGMP_ROUTER_V1 0x00000001	The interface is an IGMPv1 router.
IGMP_ROUTER_V2 0x00000002	The interface is an IGMPv2 router.
IGMP_ROUTER_V3 0x00000003	The interface is an IGMPv3 router.
IGMP_PROXY_V3 0x00000010	The interface is an IGMPv3 proxy.

**RobustnessVariable:** The robustness variable is a way of indicating the lossy nature of the subnet to which this interface is attached. The IGMP can recover from lost IGMP packets (robustness variable is set to 1). The robustness variable SHOULD be set to a value of 2 or greater.

**StartQueryInterval:** The startup query interval is the amount of time in seconds between successive general query messages sent by a querier during startup.

**StartQueryCount:** The startup query count is the number of general query messages sent at startup.

**GenQueryInterval:** The query interval is the amount of time, in seconds, between the IGMP general query messages sent by the router (if the router is the querier on this subnet).

**GenQueryMaxResponseTime:** The query response interval is the maximum amount of time, in seconds, that the IGMP router waits to receive a response to a general query message.

**LastMemQueryInterval:** The last member query interval is the amount of time, in milliseconds, that the IGMP router waits to receive a response to a group-specific query message. The last member query interval is also the amount of time, in seconds, between successive group-specific query messages.

**LastMemQueryCount:** The last member query count is the number of group-specific query messages sent before the router assumes there are no members of the host group being queried on this interface.

**OtherQuerierPresentInterval:** Displays the calculated other querier present interval. The other querier present interval is the number of seconds that must pass before a multicast router determines that there is no other multicast router that should be the querier. The other querier present interval is  $(\text{robustness variable}) * (\text{query interval}) + (\text{query response interval}) / 2$ .

**GroupMembershipTimeout:** Displays the calculated group membership interval. The group membership interval is the number of seconds that must pass before a multicast router determines that there are no more members of a host group on a subnet. The group membership interval is  $(\text{robustness variable}) * (\text{query interval}) + (\text{query response interval})$ .

**NumStaticGroups:** The number of static groups. This value MUST be zero when calling RRouterInterfaceTransportAdd and RRouterInterfaceTransportSetInfo.

### 2.2.1.2.176 IGMP\_MIB\_IF\_GROUPS\_LIST

The **IGMP\_MIB\_IF\_GROUPS\_LIST** structure is an MIB entry, stores the list of multicast groups which are members on that interface. This structure has variable length. The structure is followed by **NumGroups** number of [IGMP\\_MIB\\_GROUP\\_INFO \(section 2.2.1.2.177\)](#) structures.

```
typedef struct _IGMP_MIB_IF_GROUPS_LIST {  
    DWORD IfIndex;  
    DWORD IpAddr;  
    DWORD IfType;  
    DWORD NumGroups;  
    BYTE Buffer[1];  
} IGMP_MIB_IF_GROUPS_LIST,  
*IGMP_MIB_IF_GROUPS_LIST;
```

**IfIndex:** Index of the interface

**IpAddr:** IP address of the interface

**IfType:** Type of the interface, MUST be one of the following.

Value	Meaning
IGMP_IF_NOT_RAS 0x00000001	The interface is connected to a LAN
IGMP_IF_RAS_ROUTER 0x00000002	The interface is connected to another router over RAS
IGMP_IF_RAS_SERVER 0x00000003	The entry corresponds to a RAS server if it contains stats, then it represents summarized stats

Value	Meaning
IGMP_IF_RAS_CLIENT 0x00000004	The entry corresponds to a RAS client
IGMP_IF_PROXY 0x00000008	then one of the 1st 4 flags still will be set to enable switch from proxy to IGMP router

**NumGroups:** Number of **IGMP\_MIB\_GROUP\_INFO** structures

**Buffer:** MUST point to **IGMP\_MIB\_GROUP\_INFO**

### 2.2.1.2.177 IGMP\_MIB\_GROUP\_INFO

The **IGMP\_MIB\_GROUP\_INFO** structure is used in [IGMP MIB IF GROUPS LIST \(section 2.2.1.2.176\)](#). If the interface is of type RAS\_SERVER then the group membership of all the RAS clients is summarized, and the **GroupUpTime** and **GroupExpiryTime** is the maximum over all member RAS clients, while the **V1HostPresentTimeLeft** is set to 0. If the interface is of type RAS\_CLIENT, the **IpAddr** is the next hop IP address of the RAS client. The membership is summarized over the RAS clients unless the IGMP\_ENUM\_FOR\_RAS\_CLIENTS\_ID flag is set in **Flags**.

```
typedef struct _IGMP_MIB_GROUP_INFO {
    union {
        DWORD IfIndex;
        DWORD GroupAddr;
    } IfIndex/ GroupAddr;
    DWORD IpAddr;
    DWORD GroupUpTime;
    DWORD GroupExpiryTime;
    DWORD LastReporter;
    DWORD V1HostPresentTimeLeft;
    DWORD Flags;
} IGMP_MIB_GROUP_INFO,
*IGMP_MIB_GROUP_INFO;
```

**IfIndex/ GroupAddr:** The index of the interface or group address.

**IpAddr:** The IP address of the interface.

**GroupUpTime:** The time, in seconds, since the group is up.

**GroupExpiryTime:** The time, in seconds, before the group expires.

**LastReporter:** The IP address of the last reporter.

**V1HostPresentTimeLeft:** The time left for the present IGMPv1 hosts.

**Flags:** It MUST be one of the following.

Value	Meaning
IGMP_GROUP_TYPE_NON_STATIC 0x00000001	The IGMP group is not static.

Value	Meaning
IGMP_GROUP_TYPE_STATIC 0x00000002	The IGMP group is static.
IGMP_GROUP_FWD_TO_MGM 0x00000004	The IGMP group needs to be forwarded to the multiple multicast routing protocols.
IGMP_GROUP_ALLOW 0x00000010	Allows IGMP groups.
IGMP_GROUP_BLOCK 0x00000020	Blocks IGMP groups.
IGMP_GROUP_NO_STATE 0x00000040	There is no IGMP group state.

### 2.2.1.2.178 IGMP\_MIB\_IF\_STATS

The **IGMP\_MIB\_IF\_STATS** structure contains statistics about an interface.

```
typedef struct _IGMP_MIB_IF_STATS {
    DWORD IfIndex;
    DWORD IpAddr;
    DWORD IfType;
    BYTE State;
    BYTE QuerierState;
    DWORD IgmpProtocolType;
    DWORD QuerierIpAddr;
    DWORD ProxyIfIndex;
    DWORD QuerierPresentTimeLeft;
    DWORD LastQuerierChangeTime;
    DWORD V1QuerierPresentTimeLeft;
    DWORD Uptime;
    DWORD TotalIgmpPacketsReceived;
    DWORD TotalIgmpPacketsForRouter;
    DWORD GeneralQueriesReceived;
    DWORD WrongVersionQueries;
    DWORD JoinsReceived;
    DWORD LeavesReceived;
    DWORD CurrentGroupMemberships;
    DWORD GroupMembershipsAdded;
    DWORD WrongChecksumPackets;
    DWORD ShortPacketsReceived;
    DWORD LongPacketsReceived;
    DWORD PacketsWithoutRtrAlert;
} IGMP_MIB_IF_STATS,
*PIGMP_MIB_IF_STATS;
```

**IfIndex:** The index of the interface.

**IpAddr:** The IP address of the interface. If the interface is a RAS interface, then the **IpAddr** is set to the **NextHopAddress** of the RAS client.

**IfType:** The type of the interface. It MUST be one of the following.

Value	Meaning
IGMP_IF_NOT_RAS 0x00000001	The interface is connected to a LAN.
IGMP_IF_RAS_ROUTER 0x00000002	The interface is connected to another router over RAS.
IGMP_IF_RAS_SERVER 0x00000003	The entry corresponds to a RAS server if it contains statistics and it represents summary statistics.
IGMP_IF_RAS_CLIENT 0x00000004	The entry corresponds to a RAS client.
IGMP_IF_PROXY 0x00000008	The interface is an IGMP PROXY. One of the first four flags will still be set to enable the switch from the proxy to the IGMP router.

**State:** It MUST be a combination of one or more of the following values.

Value	Meaning
IGMP_STATE_BOUND 0x01	The socket is bound.
IGMP_STATE_ENABLED_BY_RTRMGR 0x02	The interface is enabled by router.
IGMP_STATE_ENABLED_IN_CONFIG 0x04	The interface is enabled in the configuration.
IGMP_STATE_ENABLED_BY_MGM 0x08	The interface is enabled by component that aggregates multiple routing protocols.

**QuerierState:** It MUST be one of the following.

Value	Meaning
RTR_QUERIER 0x10	The interface is the IGMP querier.
RTR_NOT_QUERIER 0x00	The interface is not the IGMP querier.

**IgmpProtocolType:** Takes one of the following values.

Value	Meaning
IGMP_PROXY 0x00000000	The interface is an IGMPv2 proxy. Specifies that the IGMPv2 proxy mode is enabled on this interface. An interface in IGMP proxy mode acts as a host, forwarding the IGMP host membership messages for all the IGMP host membership messages received on all other interfaces on which the IGMP router mode is enabled. Additionally, all nonlocal multicast traffic received on all other interfaces (on which the IGMP router mode is enabled) is forwarded over the IGMP proxy mode interface.



Value	Meaning
IGMP_ROUTER_V1 0x00000001	The interface is an IGMPv1 router. Specifies that IGMPv1 router mode is enabled on this interface. An interface in IGMP router mode listens for IGMP messages from hosts and updates the TCP/IP multicast forwarding table.
IGMP_ROUTER_V2 0x00000002	The interface is an IGMPv2 router. Specifies that IGMPv2 router mode is enabled on this interface. An interface in IGMP router mode listens for IGMP messages from hosts and updates the TCP/IP multicast forwarding table.
IGMP_ROUTER_V3 0x00000003	The interface is an IGMPv3 router. Specifies that IGMPv3 router mode is enabled on this interface. An interface in IGMP router mode listens for IGMP messages from hosts and updates the TCP/IP multicast forwarding table.
IGMP_PROXY_V3 0x00000010	The interface is an IGMPv3 proxy. Specifies that IGMPv3 proxy mode is enabled on this interface. An interface in IGMP proxy mode acts as a host, forwarding IGMP host membership messages for all IGMP host membership messages received on all other interfaces on which IGMP router mode is enabled. Additionally, all nonlocal multicast traffic received on all other interfaces (on which IGMP router mode is enabled) is forwarded over the IGMP proxy mode interface.

**QuerierIpAddress:** The IP address of the querier.

**ProxyIfIndex:** The **IfIndex** of the IGMP proxy.

**QuerierPresentTimeLeft:** If no IGMPv2 queries are heard on this interface within this interval, the local router will take over the querier on the IP subnet to which this interface is attached.

**LastQuerierChangeTime:** The number of seconds since igmpInterfaceQuerier was last changed.

**V1QuerierPresentTimeLeft:** The time remaining until the host assumes that there are no IGMPv1 routers present on the interface. While this is nonzero, the host will reply to all queries with version 1 membership reports.

**Uptime:** The time, in seconds, the interface has been activated.

**TotalIgmpPacketsReceived:** The total IGMP packets received.

**TotalIgmpPacketsForRouter:** The total IGMP packets received for a router.

**GeneralQueriesReceived:** The total queries received.

**WrongVersionQueries:** The count of wrong version queries received.

**JoinsReceived:** The count of IGMP joins received.

**LeavesReceived:** The count of IGMP leaves received.

**CurrentGroupMemberships:** The count of current group memberships.

**GroupMembershipsAdded:** The count of group memberships received.

**WrongChecksumPackets:** The count of packets with wrong checksum received.

**ShortPacketsReceived:** The count of short packets received.

**LongPacketsReceived:** The count of long packets received.

**PacketsWithoutRtrAlert:** The count of packets with router alerts received.

#### 2.2.1.2.179 IGMP\_MIB\_GROUP\_IFS\_LIST

The **IGMP\_MIB\_GROUP\_IFS\_LIST** structure is an MIB entry and stores the list of interfaces that have received joins for that group. This structure has variable length. The structure is followed by the **NumInterfaces** number of structures of type [IGMP\\_MIB\\_GROUP\\_INFO](#) or [IGMP\\_MIB\\_GROUP\\_INFO\\_V3](#).

This structure is read only.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
GroupAddr																															
NumInterfaces																															
Buffer (variable)																															
...																															

**GroupAddr (4 bytes):** The address of the IGMP group.

**NumInterfaces (4 bytes):** The number of structures in the buffer.

**Buffer (variable):** If IGMP\_ENUM\_FORMAT\_IGMPV3 is set, then **Flags** of [IGMP\\_MIB\\_GET\\_OUTPUT\\_DATA](#) contains IGMP\_MIB\_GROUP\_INFO\_V3 structures otherwise. Otherwise, it contains IGMP\_MIB\_GROUP\_INFO structures.

#### 2.2.1.2.180 IGMP\_MIB\_GROUP\_INFO\_V3

The **IGMP\_MIB\_GROUP\_INFO\_V3** provides information about a group.

```
typedef struct _IGMP_MIB_GROUP_INFO_V3 {
    union {
        DWORD IfIndex;
        DWORD GroupAddr;
    };
    DWORD IpAddr;
    DWORD GroupUpTime;
    DWORD GroupExpiryTime;
    DWORD LastReporter;
    DWORD V1HostPresentTimeLeft;
    DWORD Flags;
    DWORD Version;
    DWORD Size;
    DWORD FilterType;
}
```

```

    DWORD V2HostPresentTimeLeft;
    DWORD NumSources;
    DWORD Sources;
} IGMP_MIB_GROUP_INFO_V3,
*IGMP_MIB_GROUP_INFO_V3;

```

**IfIndex:** The interface for which this entry contains information for an IP multicast group address.

**GroupAddr:** The IP multicast group address for which this entry contains information.

**IpAddr:** The IP address of the interface.

**GroupUpTime:** The time, in seconds, since the group membership was up.

**GroupExpiryTime:** The time, in seconds, before the group membership expires.

**LastReporter:** The IP address of the source of the last membership report received for this IP multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.

**V1HostPresentTimeLeft:** The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. While this time remaining is nonzero, the local router ignores any IGMPv1 leave messages for this group that it receives on this interface.

**Flags:** This MUST be 0x1000 if IGMPv3 information is available and a **IGMP\_MIB\_GROUP\_INFO\_V3** structure MUST be used. All other values have no meaning.

**Version:** The IGMP version. It MUST be 3.

**Size:** The size of the structure.

**FilterType:** Indicates whether the sources specified need to be included or excluded. It MUST be either 0x00000000 (EXCLUSION) or 0x00000001 (INCLUSION).

**V2HostPresentTimeLeft:** The time remaining until the local router will assume that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. Upon hearing any IGMPv2 membership report, this value is reset to the group membership timer. While this time remaining is nonzero, the local router ignores any IGMPv2 leave messages for this group that it receives on this interface.

**NumSources:** The number of entries of IGMP\_MIB\_GROUP\_SOURCE\_INFO\_V3

**Sources:** The IGMP\_MIB\_GROUP\_SOURCE\_INFO\_V3 structure.

#### 2.2.1.2.181 INTERFACE\_ROUTE\_ENTRY

The **INTERFACE\_ROUTE\_ENTRY** structure is used to store and retrieve entries of the IPv6 ForwardRow based on the dwIndex.

```

typedef struct _INTERFACE_ROUTE_ENTRY {
    DWORD dwIndex;
    INTERFACE_ROUTE_INFO routeInfo;
}

```

```

} INTERFACE_ROUTE_ENTRY,
*INTERFACE_ROUTE_ENTRY;

```

**dwIndex:** The index to the table of [INTERFACE\\_ROUTE\\_INFO](#) structures defined on RRAS.

**routeInfo:** This MUST be **INTERFACE\_ROUTE\_INFO**.

#### 2.2.1.2.182 IP\_NAT\_MIB\_QUERY

The **IP\_NAT\_MIB\_QUERY** structure is passed to [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBGetEntryFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#) to retrieve the Network Address Translation (NAT) information.

```

typedef struct _IP_NAT_MIB_QUERY {
    ULONG Oid;
    union {
        ULONG Index;
        UCHAR Data;
    };
} IP_NAT_MIB_QUERY,
*PIP_NAT_MIB_QUERY;

```

**Oid:** This is an index of the NAT MIB. It MUST be one of the following values.

Value	Meaning
IP_NAT_INTERFACE_STATISTICS_OID 0x00000000	NAT interface statistics information is retrieved. When <b>RMIBEntryGet</b> , <b>RMIBGetEntryFirst</b> , and <b>RMIBEntryGetNext</b> return pMibOutEntry or pInfoStruct it MUST be typecast to <a href="#">IP_NAT_INTERFACE_STATISTICS (section 2.2.1.2.185)</a> .
IP_NAT_INTERFACE_MAPPING_TABLE_OID 0x00000001	NAT interface mapping table information. When <b>RMIBEntryGet</b> , <b>RMIBGetEntryFirst</b> , and <b>RMIBEntryGetNext</b> return pMibOutEntry or pInfoStruct it MUST be typecast to <a href="#">IP_NAT_ENUMERATE_SESSION_MAPPINGS (section 2.2.1.2.183)</a> .
IP_NAT_MAPPING_TABLE_OID 0x00000002	NAT mapping table information. Retrieves the session mappings of an interface. When <b>RMIBEntryGet</b> , <b>RMIBGetEntryFirst</b> , and <b>RMIBEntryGetNext</b> return pMibOutEntry or pInfoStruct it MUST be typecast to IP_NAT_ENUMERATE_SESSION_MAPPINGS.

**Index:** This MUST be the index of the interface when Oid is 0x00000000.

**Data:** This MUST be IP\_NAT\_ENUMERATE\_SESSION\_MAPPINGS if Oid is not 0x00000000.

### 2.2.1.2.183 IP\_NAT\_ENUMERATE\_SESSION\_MAPPINGS

The **IP\_NAT\_ENUMERATE\_SESSION\_MAPPINGS** structure is used for enumerating **NAT** session mappings and is part of [IP NAT MIB QUERY \(section 2.2.1.2.182\)](#).

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Index																															
EnumerateContext																															
...																															
...																															
...																															
EnumerateCount																															
EnumerateTotalHint																															
EnumerateTable (variable)																															

**Index (4 bytes):** This MUST be the index of the interface.

**EnumerateContext (16 bytes):** This is represented by an array of 4 [ULONG](#) values. On the first call (to [RMIBEntryGet \(section 3.1.4.30\)](#) or [RMIBEntryGetFirst \(section 3.1.4.31\)](#)) **EnumerateContext** should be zeroed out. It will be filled by the NAT with the information to be passed back down as the enumeration continues. To indicate there are no items remaining, the NAT will set **EnumerateContext[0]** to 0. In [RMIBEntryGetNext \(section 3.2.4.32\)](#), **EnumerateContext** MUST be returned to the value returned in the previous calls.

**EnumerateCount (4 bytes):** Contains the number of enumerations returned and the number of [IP NAT SESSION MAPPING \(section 2.2.1.2.184\)](#) structures being returned.

**EnumerateTotalHint (4 bytes):** Count of the total number of entries.

**EnumerateTable (variable):** This MUST be IP\_NAT\_SESSION\_MAPPING structures.

**Note** The **EnumerateTable** field is of variable size depending on the value of **EnumerateCount**. While calculating the structure size, the size of **EnumerateTable** MUST NOT be added if value of **EnumerateCount** is zero.

### 2.2.1.2.184 IP\_NAT\_SESSION\_MAPPING

The **IP\_NAT\_SESSION\_MAPPING** structure holds information for a single NAT mapping and is part of [IP NAT ENUMERATE SESSION MAPPINGS \(section 2.2.1.2.183\)](#).

```
typedef struct _IP_NAT_SESSION_MAPPING {
    UCHAR Protocol;
    ULONG PrivateAddress;
```

```

USHORT PrivatePort;
ULONG PublicAddress;
USHORT PublicPort;
ULONG RemoteAddress;
USHORT RemotePort;
IP_NAT_DIRECTION Direction;
ULONG IdleTime;
} IP_NAT_SESSION_MAPPING,
*PIP_NAT_SESSION_MAPPING;

```

**Protocol:** This MUST be one of the following.

Value	Meaning
NAT_PROTOCOL_ICMP 0x01	ICMP Protocol
NAT_PROTOCOL_IGMP 0x02	IGMP Protocol
NAT_PROTOCOL_TCP 0x06	TCP Protocol
NAT_PROTOCOL_UDP 0x11	UDP Protocol
NAT_PROTOCOL_IP6IN4 0x29	IPv6 in IPv4
NAT_PROTOCOL_PPTP 0x2F	PPTP Protocol
NAT_PROTOCOL_IPSEC_ESP 0x32	IPSec ESP
NAT_PROTOCOL_IPSEC_AH 0x33	IPSec AH
NAT_PROTOCOL_PGM 0x71	PGM

**PrivateAddress:** The private address of the NAT entry.

**PrivatePort:** The private port of the NAT entry.

**PublicAddress:** The public address of the NAT entry.

**PublicPort:** The public port of the NAT entry

**RemoteAddress:** The remote address of the NAT entry.

**RemotePort:** The remote port of the NAT entry.

**Direction:** This MUST be IP\_NAT\_DIRECTION.

**IdleTime:** The time, in seconds, since the last packet matching this entry was sent or received.

### 2.2.1.2.185 IP\_NAT\_INTERFACE\_STATISTICS

The **IP\_NAT\_INTERFACE\_STATISTICS** structure holds statistics for an interface and is part of [IP\\_NAT\\_MIB\\_QUERY \(section 2.2.1.2.182\)](#).

```
typedef struct _IP_NAT_INTERFACE_STATISTICS {
    ULONG TotalMappings;
    ULONG InboundMappings;
    ULONG64 BytesForward;
    ULONG64 BytesReverse;
    ULONG64 PacketsForward;
    ULONG64 PacketsReverse;
    ULONG64 RejectsForward;
    ULONG64 RejectsReverse;
} IP_NAT_INTERFACE_STATISTICS,
*IP_NAT_INTERFACE_STATISTICS;
```

**TotalMappings:** The count of the total number of mappings present in the NAT table.

**InboundMappings:** The count of the total number of inbound mappings present in the NAT table.

**BytesForward:** The count of the total bytes forwarded.

**BytesReverse:** The count of the total bytes reversed.

**PacketsForward:** The count of the packets forwarded.

**PacketsReverse:** The count of the packets reversed.

**RejectsForward:** The count of the forward packets rejected.

**RejectsReverse:** The count of the reverse packets rejected.

### 2.2.1.2.186 IP\_DNS\_PROXY\_MIB\_QUERY

The **IP\_DNS\_PROXY\_MIB\_QUERY** structure is passed to [RMIBEntryGet \(section 3.1.4.30\)](#) to retrieve the DNS proxy information.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Oid																															
Index																															
Data (variable)																															
...																															

**Oid (4 bytes):** This MUST be set to 0x00000000.

**Index (4 bytes):** This MUST be the index of the interface.

**Data (variable):** This MUST be an [IP\\_DNS\\_PROXY\\_STATISTICS](#) structure.

**Note** Note that the **Index** and **Data** are of variable size and while calculating the structure size, the size of **Index** or **Data** needs to be added. **Data** is unused, and has been kept for extensibility.

### 2.2.1.2.187 IP\_DNS\_PROXY\_STATISTICS

The **IP\_DNS\_PROXY\_STATISTICS** structure contains the IP DNS proxy statistics.

```
typedef struct _IP_DNS_PROXY_STATISTICS {
    ULONG MessagesIgnored;
    ULONG QueriesReceived;
    ULONG ResponsesReceived;
    ULONG QueriesSent;
    ULONG ResponsesSent;
} IP_DNS_PROXY_STATISTICS,
*IP_DNS_PROXY_STATISTICS;
```

**MessagesIgnored:** The count of the DNS proxy messages ignored.

**QueriesReceived:** The count of the DNS proxy queries received.

**ResponsesReceived:** The count of the DNS proxy responses received.

**QueriesSent:** The count of the DNS proxy queries sent.

**ResponsesSent:** The count of the DNS proxy responses sent.

### 2.2.1.2.188 IP\_AUTO\_DHCP\_MIB\_QUERY

The **IP\_AUTO\_DHCP\_MIB\_QUERY** structure is passed to [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#) to retrieve the DNS proxy information.

```
typedef struct _IP_AUTO_DHCP_MIB_QUERY {
    ULONG Oid;
    union {
        ULONG Index;
        UCHAR Data;
    };
    ULONG Reserved;
} IP_AUTO_DHCP_MIB_QUERY,
*PIP_AUTO_DHCP_MIB_QUERY;
```

**Oid:** This MUST be set to 0x00000000.

**Index:** This MUST be index of the interface.

**Data:** This MUST be an [IP\\_AUTO\\_DHCP\\_STATISTICS](#) structure.

**Note** Index and Data are variable-sized arrays. While calculating the structure size, the size of Index or Data is added. Data is unused, and has been kept for extensibility.



**Reserved:** MUST be set to zero when sent and MUST be ignored on receipt.

#### 2.2.1.2.189 IP\_AUTO\_DHCP\_STATISTICS

The **IP\_AUTO\_DHCP\_STATISTICS** structure contains the DHCP auto-discovery statistics. This structure defines the statistics kept by the DHCP allocator, and is accessible to [RMIBEntryGet \(section 3.2.4.30\)](#), [RMIBEntryGetFirst \(section 3.2.4.31\)](#), and [RMIBEntryGetNext \(section 3.2.4.32\)](#).

```
typedef struct _IP_AUTO_DHCP_STATISTICS {
    ULONG MessagesIgnored;
    ULONG BootpOffersSent;
    ULONG DiscoversReceived;
    ULONG InformReceived;
    ULONG OffersSent;
    ULONG RequestsReceived;
    ULONG AcksSent;
    ULONG NaksSent;
    ULONG DeclinesReceived;
    ULONG ReleaseReceived;
} IP_AUTO_DHCP_STATISTICS,
*PIP_AUTO_DHCP_STATISTICS;
```

**MessagesIgnored:** The count of the messages ignored.

**BootpOffersSent:** The count of the IPBOOTP offers sent.

**DiscoversReceived:** The count of the discover messages received.

**InformReceived:** The count of the INFORM messages received.

**OffersSent:** The count of the OFFER messages sent.

**RequestsReceived:** The count of the REQUEST messages received.

**AcksSent:** The count of the acknowledge control packets (ACKs) sent.

**NaksSent:** The count of the negative acknowledge (NAK) messages sent.

**DeclinesReceived:** The count of the DECLINE messages received.

**ReleaseReceived:** The count of the RELEASE messages received.

#### 2.2.1.2.190 MIB\_DA\_MSG

This structure<150> is used in [RMIBEntryGet \(section 3.1.4.30\)](#), [RMIBEntryGetFirst \(section 3.1.4.31\)](#), and [RMIBEntryGetNext \(section 3.1.4.32\)](#) for retrieving OSPF MIB entries.

```
typedef struct MIB_DA_MSG {
    UINT32 op_code;
    UINT32 ret_code;
    UINT32 in_snmp_id[44];
    UINT32 obj_id[17];
    UINT32 attr_id;
    UINT32 inst_id[23];
    UINT32 next_snmp_id[44];
    UINT32 creator;
```

```

UINT32 attr_type;
UINT32 inst_cnt;
UINT32 map_flag;
ULONG_PTR data[32];
} MIB_DA_MSG;

```

**op\_code:** This MUST have one of the following values.

Value	Meaning
ASN_RFC1157_GETREQUEST 0x000000A0	MIB get request: <b>RMIBEntryGet</b> (section 3.1.4.30)
ASN_RFC1157_GETNEXTREQUEST 0x000000A1	MIB get next request: <b>RMIBEntryGetNext</b> (section 3.1.4.32)
ASN_RFC1157_SETREQUEST 0x000000A3	MIB set request: <a href="#">RMIBEntrySet (section 3.1.4.29)</a>

**ret\_code:** This contains a return value which MUST be one of the following.

Value	Meaning
MIB_OK 0x00000000	The call was successful.
All other values	The call was not successful.

**in\_snmp\_id:** Contains the index of the entry that needs to be retrieved.

in\_snmp\_id[0] contains the length (excluding the zeroth element) of the data passed in **in\_snmp\_id**. in\_snmp\_id[1] onwards contains the MIB object identifier [\[RFC1850\]](#)

Value in_snmp_id[1] and beyond	Meaning [RFC 1850]
g_oidOspfAreaEntry { 4, 1, 18, 3, 5, 3, 2, 3, 2, 1 }	Open Shortest Path First (OSPF) area entry. See ospfAreaEntry, section 3.2 in <a href="#">[RFC1850]</a> .  Information describing the configured parameters and cumulative statistics of one of the router's attached areas.
g_oidOspfLsdbEntry { 4, 1, 18, 3, 5, 3, 2, 3, 3, 1 }	A single link state advertisement. See ospfLsdbEntry, section 3.4 in <a href="#">[RFC1850]</a> .
g_oidOspfNbrEntry { 4, 1, 18, 3, 5, 3, 2, 3, 7, 1 }	The information regarding a single neighbor. See OspfNbrEntry, section 3.10 in <a href="#">[RFC1850]</a> .
g_oidOspfVIFEntry { 4, 1, 18, 3, 5, 3, 2, 3, 6, 1 }	The information about a single Virtual Interface. See OspfVirtIfEntry, section 3.9 in <a href="#">[RFC1850]</a> .
g_oidOspfAreaState	Retrieves the state. This value indicates the state of the OSPF

Value in _snmp_id[1] and beyond	Meaning [RFC 1850]
{ 4, 1, 18, 3, 5, 3, 2, 3, 2, 1, 3 }	Area, either up(0x00000001), or down(0x00000002). See ospfAreaStatus, section 3.2 in <a href="#">[RFC1850]</a> .
g_oidOspfAreaSpfCount { 4, 1, 18, 3, 5, 3, 2, 3, 2, 1, 9 }	Retrieves the number of times the SPF algorithm has run for the area. See ospfSpfRuns, section 3.2 in <a href="#">[RFC1850]</a> .
g_oidOspfLsdbAge { 4, 1, 18, 3, 5, 3, 2, 3, 3, 1, 6 }	Retrieves the age of the link state advertisement in seconds. See ospfLsdbAge, section 3.4 in <a href="#">[RFC1850]</a> and section 12.1.1 LS age in <a href="#">[RFC2328]</a> .
g_oidOspfLsdbSequence { 4, 1, 18, 3, 5, 3, 2, 3, 3, 1, 5 }	Retrieves the sequence. The OSPF Sequence Number is a 32-bit signed integer. It starts with the value '80000001'h, or '7FFFFFFF'h, and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative. The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number the more recent the advertisement. See ospfLsdbSequence, section 3.4 of <a href="#">[RFC1850]</a> and LS sequence number, section 12.1.6 in <a href="#">[RFC2328]</a> .
g_oidOspfNbrRtrId { 4, 1, 18, 3, 5, 3, 2, 3, 7, 1, 7 }	Retrieves the router ID. A 32-bit integer uniquely identifying the neighboring router in the autonomous system. See ospfNbrRtrId, section 3.10 in <a href="#">[RFC1850]</a> .
g_oidOspfNbrState { 4, 1, 18, 3, 5, 3, 2, 3, 7, 1, 3 }	Retrieves the state. The state of the Virtual Neighbor Relationship. It can be down (0x00000001), attempt (0x00000002), init (0x00000003), twoWay (0x00000004), exchangeStart (0x00000005), exchange (0x00000006), loading (0x00000007), and full (0x00000008) See ospfNbrState, section 3.10 in <a href="#">[RFC1850]</a> .
g_oidOspfNbrPriority { 4, 1, 18, 3, 5, 3, 2, 3, 7, 1, 9 }	Retrieves the priority. The priority of this neighbor in the designated router election algorithm. The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network. See ospfNbrPriority, section 3.10 in <a href="#">[RFC1850]</a> .
g_oidOspfNbrEvents { 4, 1, 18, 3, 5, 3, 2, 3, 7, 1, 10 }	Retrieves the event count. The number of times this neighbor relationship has changed state, or that an error has occurred. See ospfNbrEvents, section 3.10 in <a href="#">[RFC1850]</a> .
g_oidOspfNbrLSRetransQLen { 4, 1, 18, 3, 5, 3, 2, 3, 7, 1, 11 }	Retrieves the queue length. See ospfNbrLsRetransQLen, section 3.10 in <a href="#">[RFC1850]</a> .
g_oidOspfVIFState { 4, 1, 18, 3, 5, 3, 2, 3, 6, 1, 3 }	Retrieves the state. See ospfVirtIfState, section 3.9 in <a href="#">[RFC1850]</a> .
g_oidOspfVIDrops { 4, 1, 18, 3, 5, 3, 2, 3, 6, 1, 21 }	The number of OSPF packets dropped on Virtual Interfaces. The data returned is a 32-bit integer.
g_oidOspfVIRxHellos	The number of OSPF Hello packets received on Virtual Interfaces.

Value in _snmp_id[1] and beyond	Meaning [RFC 1850]
{ 4, 1, 18, 3, 5, 3, 2, 3, 6, 1, 16 }	Data returned is a 32 bit integer.
g_oidOspfVITxHellos { 4, 1, 18, 3, 5, 3, 2, 3, 6, 1, 11 }	The number of OSPF Hello packets transmitted on the Virtual Interfaces. The data returned is a 32 bit integer.
g_oidOspfIfArea { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 6 }	See ospfIfAreaId, section 3.7 in <a href="#">[RFC1850]</a> .
g_oidOspfIfType { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 7 }	See ospfIfType, section 3.7 in <a href="#">[RFC1850]</a> .
g_oidOspfIfState { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 3 }	See ospfIfState, section 3.7 in <a href="#">[RFC1850]</a> .
g_oidOspfIfRxDBDescriptors { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 24 }	The number of OSPF DataBase Description packets received. The data returned is a 32-bit integer.
g_oidOspfIfRxLinkStateAcks { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 27 }	The number of OSPF Link State Acknowledgements received. The data returned is a 32-bit integer.
g_oidOspfIfRxLinkStateReqs { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 25 }	The number of OSPF Link State Requests received. The data returned is a 32-bit integer.
g_oidOspfIfRxLinkStateUpds { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 26 }	The number of OSPF Link State Updates received. The data returned is a 32-bit integer.
g_oidOspfIfTxDBDescriptors { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 19 }	The number of OSPF DataBase Description packets transmitted. The data returned is a 32-bit integer.
g_oidOspfIfTxLinkStateAcks { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 22 }	The number of OSPF Link State Update packets transmitted. The data returned is a 32-bit integer.
g_oidOspfIfTxLinkStateReqs { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 20 }	The number of OSPF Link State Request packets transmitted. The data returned is a 32-bit integer.
g_oidOspfIfTxLinkStateUpds { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 21 }	The number of OSPF Link State Update packets transmitted. The data returned is a 32-bit integer.
g_oidOspfIfDrops { 4, 1, 18, 3, 5, 3, 2, 3, 5, 1, 1 }	The number of OSPF packets dropped because of invalid information in the packet. The data returned is a 32-bit integer.

Value in_snmp_id[1] and beyond	Meaning [RFC 1850]
28 }	

**obj\_id:** Unused and MUST be set to zero.

**attr\_id:** Unused and MUST be set to zero.

**inst\_id:** Unused and MUST be set to zero.

**next\_snmp\_id:** Unused and MUST be set to zero.

**creator:** Unused and MUST be set to zero.

**attr\_type:** Unused and MUST be set to zero.

**inst\_cnt:** Unused and MUST be set to zero.

**map\_flag:** Unused and MUST be set to zero.

**data:** Contains the data returned by the OSPF MIB based on the entry requested in the previous table. See [\[RFC1850\]](#) for more information about how to interpret the returned data. The length of the data returned is specified in **dwMibOutEntrySize** of *pInfoStruct* in the call to **RMIBEntryGet**, **RMIBEntryGetFirst**, and **RMIBEntryGetNext**.

#### 2.2.1.2.191 IP\_AUTO\_DHCP\_GLOBAL\_INFO

This structure holds the global configuration for the DHCP allocator and is used in the following methods.

- [RRouterInterfaceTransportSetGlobalInfo](#)
- [RRouterInterfaceTransportGetGlobalInfo](#)

The configuration consists of two things:

1. The network and mask from which addresses are to be allocated.
2. An optional list of addresses to be excluded from allocation. Thus, this structure is of variable length.

```
typedef struct _IP_AUTO_DHCP_GLOBAL_INFO {
    ULONG LoggingLevel;
    ULONG Flags;
    ULONG LeaseTime;
    ULONG ScopeNetwork;
    ULONG ScopeMask;
    ULONG ExclusionCount;
    ULONG ExclusionArray[0];
} IP_AUTO_DHCP_GLOBAL_INFO,
*PIP_AUTO_DHCP_GLOBAL_INFO;
```

**LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
IPNATHLP_LOGGING_NONE 0x00000000	No logging is done.
IPNATHLP_LOGGING_ERROR 0x00000001	Only errors are logged.
IPNATHLP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IPNATHLP_LOGGING_INFO 0x00000003	Errors, warnings, and information is logged.

**Flags:** This MUST be set to 0.

**LeaseTime:** The lease time, in minutes.

**ScopeNetwork:** The scope of the network from which addresses are to be allocated.

**ScopeMask:** The mask used to identify the subnet portion of the address. See [\[RFC950\]](#). The value obtained by logically ANDing ScopeMask and ScopeNetwork MUST equal ScopeNetwork. Any ScopeMask that produces a different ANDed result is invalid.

**ExclusionCount:** The number of IP addresses that need to be excluded from being allocated. This also indicates the size of the *ExclusionArray*.

**ExclusionArray:** An array of IP addresses that need to be excluded. The size of the array is given by *ExclusionCount*.

### 2.2.1.2.192 IP\_AUTO\_DHCP\_INTERFACE\_INFO

This structure holds per-interface configuration for the DHCP allocator. This structure is used in the following methods:

- [RRouterInterfaceTransportAdd](#)
- [RRouterInterfaceTransportGetInfo](#)
- [RRouterInterfaceTransportSetInfo](#)

The configuration only allows the DHCP allocator to be disabled on the given interface. Since the allocator runs in promiscuous-interface mode, it is enabled by default on all interfaces. Thus, the only interfaces that require any configuration are those on which the allocator is to be disabled.

```
typedef struct _IP_AUTO_DHCP_INTERFACE_INFO {
    ULONG Flags;
} IP_AUTO_DHCP_INTERFACE_INFO,
*PIP_AUTO_DHCP_INTERFACE_INFO;
```

**Flags:** Specifies whether or not the DHCP allocator is enabled.

Value	Meaning
0x00000000	The DHCP allocator is enabled.
IPNATHLP_INTERFACE_FLAG_DISABLED 0x00000001	The DHCP allocator is disabled.

### 2.2.1.2.193 IP\_DNS\_PROXY\_GLOBAL\_INFO

This structure holds global configuration for the DNS proxy and is used in the following methods:

[RRouterInterfaceTransportSetGlobalInfo](#)

[RRouterInterfaceTransportGetGlobalInfo](#)

```
typedef struct {
    ULONG LoggingLevel;
    ULONG Flags;
    ULONG TimeoutSeconds;
} IP_DNS_PROXY_GLOBAL_INFO;
```

**LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
IPNATHLP_LOGGING_NONE 0x00000000	No logging is done.
IPNATHLP_LOGGING_ERROR 0x00000001	Only errors are logged.
IPNATHLP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IPNATHLP_LOGGING_INFO 0x00000003	Errors, warnings, and information is logged.

**Flags:** It MUST be one of the following.

Value	Meaning
IP_DNS_PROXY_FLAG_ENABLE_DNS 0x00000000	DNS is enabled.
IP_DNS_PROXY_FLAG_ENABLE_WINS 0x00000001	WINS is enabled.

**TimeoutSeconds:** It MUST be the number of seconds that entry is maintained in the cache.

### 2.2.1.2.194 IP\_DNS\_PROXY\_INTERFACE\_INFO

This structure holds per-interface configuration for the DNS proxy. The configuration currently only allows the proxy to be disabled on a given interface. The proxy runs in promiscuous-interface mode so that all interfaces are added to it and it is enabled on all of them by default. Hence, the configuration need only be present for those interfaces on which the proxy is not to be run.

```
typedef struct {
    ULONG Flags;
} IP_DNS_PROXY_INTERFACE_INFO;
```

**Flags:** It MUST be a combination of the following.

Value	Meaning
DNS_INTERFACE_FLAG_DELETED 0x80000000	The DNS proxy is disabled on the interface.
DNS_INTERFACE_FLAG_BOUND 0x40000000	The DNS proxy socket is bound on the interface.
DNS_INTERFACE_FLAG_ENABLED 0x20000000	The DNS proxy is enabled on the interface.
DNS_INTERFACE_FLAG_CONFIGURED 0x10000000	The DNS proxy is configured on the interface.

### 2.2.1.2.195 IP\_NAT\_GLOBAL\_INFO

This structure holds the global configuration information for NAT. This structure is used in the following methods:

[RRouterInterfaceTransportSetGlobalInfo](#)

[RRouterInterfaceTransportGetGlobalInfo](#)

```
typedef struct {
    ULONG LoggingLevel;
    ULONG Flags;
    RTR_INFO_BLOCK_HEADER Header;
} IP_NAT_GLOBAL_INFO;
```

**LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
IPNATHLP_LOGGING_NONE 0x00000000	No logging is done.
IPNATHLP_LOGGING_ERROR	Only errors are logged.



Value	Meaning
0x00000001	
IPNATHLP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IPNATHLP_LOGGING_INFO 0x00000003	Errors, warnings, and information is logged.

**Flags:** This MUST be set to 0.

**Header:** This MUST be [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#). The **InfoType** field of header MUST be either 0x00000000 or 0xffff0001. If it is 0x00000000, there is no other information beyond the header and the rest of the fields MUST be zero. If the **InfoType** is 0xffff0001, the Offset MUST point to a structure of type [IP\\_NAT\\_TIMEOUT \(section 2.2.1.2.196\)](#).

### 2.2.1.2.196 IP\_NAT\_TIMEOUT

This structure is used to amend the default timeouts for TCP and UDP session mappings.

```
typedef struct {
    ULONG TCPTimeoutSeconds;
    ULONG UDPTimeoutSeconds;
} IP_NAT_TIMEOUT;
```

**TCPTimeoutSeconds:** The number of seconds that a dynamic mapping for a TCP session remains in the translation table.

**UDPTimeoutSeconds:** The number of seconds that a dynamic mapping for a UDP session remains in the translation table.

### 2.2.1.2.197 IP\_NAT\_INTERFACE\_INFO

This structure is used to configure the NAT on an interface. This structure is used in the following methods:

[RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

The configuration information uses the [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) structure.

```
typedef struct {
    ULONG Index;
    ULONG Flags;
    RTR_INFO_BLOCK_HEADER Header;
} IP_NAT_INTERFACE_INFO;
```

**Index:** This MUST be set to the interface index that identifies the interface to be configured.

**Flags:** This specifies the logging level. It MUST be a combination of one or more of the following values.

Value	Meaning
IP_NAT_INTERFACE_FLAGS_BOUNDARY 0x00000001	Set to mark the interface as a boundary-interface.
IP_NAT_INTERFACE_FLAGS_NAPT 0x00000002	Set to enable address-sharing via port-translation.
IP_NAT_INTERFACE_FLAGS_DISABLE_PPTP 0x00000004	The PPTP is disabled.
IP_NAT_INTERFACE_FLAGS_FW 0x00000010	Set to enable the firewall mode on the interface. This works with all other flags. An interface in the firewall mode is much more strict on what inbound packets it will allow to propagate up the stack; in general, it will only allow packets that are part of a locally initiated connection flow (for example, packets for which a mapping or ticket exists).
IP_NAT_INTERFACE_FLAGS_DIALUP 0x00000040	This is a dial-up interface.
IP_NAT_INTERFACE_FLAGS_ALL 0x0000007f	All of the above.

**Header:** This MUST be RTR\_INFO\_BLOCK\_HEADER. The **InfoType** field of the header MUST be one of the following and the offset MUST point to a structure specified in the following table.

Value	Meaning
IP_NAT_PORT_MAPPING_TYPE 0xffff0003	<a href="#">IP_NAT_PORT_MAPPING (section 2.2.1.2.199)</a> .
IP_NAT_ADDRESS_RANGE_TYPE 0xffff0002	<a href="#">IP_NAT_ADDRESS_RANGE (section 2.2.1.2.198)</a> .
IP_NAT_ADDRESS_MAPPING_TYPE 0xffff0004	<a href="#">IP_NAT_ADDRESS_MAPPING (section 2.2.1.2.200)</a> .
IP_NAT_ICMP_CONFIG_TYPE 0xffff0005	There is no structure for IP_NAT_ICMP_CONFIG; it's just a <b>ULONG</b> . The flags in the following table define the behavior.

The values for IP\_NAT\_ICMP\_CONFIG\_TYPE are as follows:

Value	Meaning
IP_NAT_ICMP_ALLOW_OB_DEST_UNREACH 0x00000008	The data sent over the Internet that fails to reach this computer due to an error will be discarded and acknowledged with a destination unreachable message explaining the failure.
IP_NAT_ICMP_ALLOW_OB_SOURCE_QUENCH	When this computer's ability to process incoming

Value	Meaning
0x00000010	data cannot keep up with the rate of a transmission, data will be dropped and the sender will be asked to slow down.
IP_NAT_ICMP_ALLOW_REDIRECT 0x00000020	The data sent from this computer will be rerouted if the default path changes.
IP_NAT_ICMP_ALLOW_IB_ECHO 0x00000100	The messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.
IP_NAT_ICMP_ALLOW_IB_ROUTER 0x00000200	This computer will respond to requests for information about the routes it recognizes.
IP_NAT_ICMP_ALLOW_OB_TIME_EXCEEDED 0x00000800	When this computer discards an incomplete data transmission because the entire transmission required more time than allowed, it will reply to the sender with a time-expired message.
IP_NAT_ICMP_ALLOW_OB_PARAM_PROBLEM 0x00001000	When this computer discards data it has received due to a problematic header, it will reply to the sender with a bad-header error message.
IP_NAT_ICMP_ALLOW_IB_TIMESTAMP 0x00002000	The data sent to this computer can be acknowledged with a confirmation message indicating the time that the data was received.
IP_NAT_ICMP_ALLOW_IB_MASK 0x00020000	This computer will listen for and respond to requests for more information about the public network to which it is attached.

#### 2.2.1.2.198 IP\_NAT\_ADDRESS\_RANGE

Holds a range of addresses that are part of the address-pool for a boundary interface. An address pool consists of a list of these structures. Overlapping address ranges are not supported. Noncontiguous subnet masks are also unsupported.

```
typedef struct {
    ULONG StartAddress;
    ULONG EndAddress;
    ULONG SubnetMask;
} IP_NAT_ADDRESS_RANGE;
```

**StartAddress:** The starting IP address of the address pool.

**EndAddress:** The end IP address of the address pool.

**SubnetMask:** The subnet mask of the address pool; see [\[RFC950\]](#).

#### 2.2.1.2.199 IP\_NAT\_PORT\_MAPPING

Holds a static mapping that ties a public-side port on this NAT interface to a particular private machine's address or port. In the case of an interface with a pool of addresses, the "PublicAddress" should specify which of those addresses this static mapping applies to.

```
typedef struct {
    UCHAR Protocol;
    USHORT PublicPort;
    ULONG PublicAddress;
    USHORT PrivatePort;
    ULONG PrivateAddress;
} IP_NAT_PORT_MAPPING;
```

**Protocol:** Specifies the protocol used for data reception and transmission.

**PublicPort:** Specifies the destination port number of incoming public traffic.

**PublicAddress:** Specifies the public IPv4 address.

**PrivatePort:** The destination port number of the private traffic.

**PrivateAddress:** Specifies the private IPv4 address.

#### 2.2.1.2.200 IP\_NAT\_ADDRESS\_MAPPING

Holds a static mapping that ties an address from this NAT interface's address pool to a particular private-machine's address.

**Note** This address must fall within one of the ranges comprising the pool as specified by the [IP NAT ADDRESS RANGE](#) structures.

```
typedef struct {
    ULONG PrivateAddress;
    ULONG PublicAddress;
    BOOLEAN AllowInboundSessions;
} IP_NAT_ADDRESS_MAPPING;
```

**PrivateAddress:** The private IP address of the translation.

**PublicAddress:** The public IP address of the translation.

**AllowInboundSessions:** Specifies whether sessions from public networks are allowed.

#### 2.2.1.2.201 IP\_ALG\_GLOBAL\_INFO

The IP\_ALG\_GLOBAL\_INFO [<151>](#) structure holds the global configuration for the Application Layer Gateway transparent proxy and is used in the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

```
typedef struct {
    ULONG LoggingLevel;
    ULONG Flags;
} IP_ALG_GLOBAL_INFO;
```

**LoggingLevel:** Specifies the logging level. It MUST be one of the following values.

Value	Meaning
IPNATHLP_LOGGING_NONE 0x00000000	No logging is done.
IPNATHLP_LOGGING_ERROR 0x00000001	Only errors are logged.
IPNATHLP_LOGGING_WARN 0x00000002	Errors and warnings are logged.
IPNATHLP_LOGGING_INFO 0x00000003	Errors, warnings, and information is logged.

**Flags:** This MUST be set to 0.

#### 2.2.1.2.202 RIP\_GLOBAL\_INFO

The RIP\_GLOBAL\_INFO structure [<152>](#) is used to give the global IPX RIP information for the RRAS server. When this structure is encapsulated in [RTR TOC ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be set to 0x00020000. This structure is used in the following methods:

[RRouterInterfaceTransportSetGlobalInfo](#)

[RRouterInterfaceTransportGetGlobalInfo](#)

```
typedef struct {
    ULONG EventLogMask;
} RIP_GLOBAL_INFO;
```

**EventLogMask:** The mask to manage event logging on the RIP interface on the RRAS server. This MUST be set as combination of one or more of the following flags.

Value	Meaning
0x0000	Nothing will be logged.
EVENTLOG_ERROR_TYPE (0x0001)	Only errors will be logged.
EVENTLOG_WARNING_TYPE 0x0002	Only warnings will be logged.

Value	Meaning
EVENTLOG_INFORMATION_TYPE 0x0004	Only information will be logged.

### 2.2.1.2.203 RIP\_ROUTE\_FILTER\_INFO

This structure contains the information about a route filter to which the filter actions specified in [RIP\\_IF\\_FILTERS \(section 2.2.1.2.204\)](#) are applied. This structure is used in **RIP\_IF\_FILTERS**.

```
typedef struct {
    UCHAR Network;
    UCHAR Mask;
} RIP_ROUTE_FILTER_INFO;
```

**Network:** The network to which this filter is to be applied.

**Mask:** The mask that must be ANDed with the network and with the IP address of the packet to establish a filter match. See [RFC950](#).

### 2.2.1.2.204 RIP\_IF\_FILTERS

The RIP\_IF\_FILTERS structure [<153>](#) specifies the filter data for a RIP for IPX interface. This structure is used in [RIP\\_IF\\_CONFIG \(section 2.2.1.2.206\)](#). Supply filters are applied to the RIP updates supplied by the interface, while the listening filters are applied to the RIP updates being listened to by the interface.

```
typedef struct {
    ULONG SupplyFilterAction;
    ULONG SupplyFilterCount;
    ULONG ListenFilterAction;
    ULONG ListenFilterCount;
    ULONG RouteFilter;
} RIP_IF_FILTERS;
```

**SupplyFilterAction:** This MUST be set to 0x00000001 to permit data and to 0x00000002 to deny data.

Value	Meaning
0x00000001	Permit data.
0x00000002	Deny data.

**SupplyFilterCount:** The count of supply filters.

**ListenFilterAction:** This MUST be set to 0x00000001 to permit data and to 0x00000002 to deny data.

Value	Meaning
0x00000001	Permit data.
0x00000002	Deny data.

**ListenFilterCount:** The count of listen filters.

**RouteFilter:** This must be a [RIP\\_ROUTE\\_FILTER\\_INFO \(section 2.2.1.2.203\)](#).

### 2.2.1.2.205 RIP\_IF\_INFO

The `RIP_IF_INFO`<sup><154></sup> structure contains information about the RIP for IPX interface. This structure is used in [RIP\\_IF\\_CONFIG \(section 2.2.1.2.206\)](#) and [RIP\\_INTERFACE \(section 2.2.1.2.125\)](#).

```
typedef struct {
    ULONG AdminState;
    ULONG UpdateMode;
    ULONG PacketType;
    ULONG Supply;
    ULONG Listen;
    ULONG PeriodicUpdateInterval;
    ULONG AgeIntervalMultiplier;
} RIP_IF_INFO;
```

**AdminState:** This MUST be set to the desired state of the interface. A value of 0x00000001 disables the interface, and a value of 0x00000002 enables the interface.

**UpdateMode:** This MUST be set to the RIP update mechanism used on the interface. It can have one of the following values.

Value	Meaning
0x00000001	Periodic update.
0x00000002	No update.
0x00000003	AutoStatic triggered update.

**PacketType:** Indicates the RIP packet type used on this interface and MUST be one of the following values:

Value	Meaning
IPX_STANDARD_PACKET_TYPE 0x00000001	IPX standard packet
IPX_RELIABLE_DELIVERY_PACKET_TYPE 0x00000002	IPX reliable packet

**Supply:** Determines whether to send RIP updates on this interface. A value of 0x00000001 disables sending of a RIP updated on this interface, and a value of 0x00000002 enables sending of a RIP updated on this interface.

**Listen:** Determines whether to listen for RIP updates on this interface. A value of 0x00000001 disables listening for a RIP updated on this interface, and a value of 0x00000002 enables listening for a RIP updated on this interface.

**PeriodicUpdateInterval:** This MUST be the interval at which the information is updated periodically, in seconds. The default value is 60.

**AgeIntervalMultiplier:** Each time a periodic update is done at the server, PeriodicUpdateInterval is multiplied by AgeIntervalMultiplier. The default value is 3.

#### 2.2.1.2.206 RIP\_IF\_CONFIG

The RIP\_IF\_CONFIG structure<155> is used to specify the configuration information of a RIP for IPX interface. When this structure is encapsulated in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be set to 0x00020000 and the transport MUST be PID\_IPX.

```
typedef struct {
    DWORD RipIfInfo;
    DWORD RipIfFilters;
} RIP_IF_CONFIG;
```

**RipIfInfo:** This MUST be a [RIP\\_IF\\_INFO \(section 2.2.1.2.205\)](#) structure.

**RipIfFilters:** This MUST be a [RIP\\_IF\\_FILTERS \(section 2.2.1.2.204\)](#) structure.

#### 2.2.1.2.207 SAP\_GLOBAL\_CONFIG

The SAP\_GLOBAL\_INFO structure<156> is used to give the global SAP information for the RRAS server. When this structure is encapsulated in [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#), the **InfoType** value used MUST be set to 0x00020001 and the transport MUST be PID\_IPX.

```
typedef struct {
    DWORD EventLogMask;
} SAP_GLOBAL_INFO;
```

**EventLogMask:** The mask to manage event logging on the SAP interface on the RRAS server. This MUST be set as combination of one or more following flags.

Value	Meaning
0x0000	Nothing will be logged.
EVENTLOG_ERROR_TYPE (0x0001)	Only errors will be logged.
EVENTLOG_WARNING_TYPE 0x0002	Only warnings will be logged.



Value	Meaning
EVENTLOG_INFORMATION_TYPE 0x0004	Only information will be logged.

### 2.2.1.2.208 OSPF\_ROUTE\_FILTER

This structure [<157>](#) is used as part of OSPF\_ROUTE\_FILTER\_INFO.

```
typedef struct {
    DWORD dwAddress;
    DWORD dwMask;
} OSPF_ROUTE_FILTER;
```

**dwAddress:** The IPV4 address or subnet.

**dwMask:** The IP subnet mask. See [\[RFC950\]](#).

### 2.2.1.2.209 OSPF\_ROUTE\_FILTER\_INFO

This structure [<158>](#) contains OSPF route filter information and is used by the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
type																															
ofaActionOnMatch																															
dwNumFilters																															
pFilters (variable)																															
...																															

**type (4 bytes):** This MUST be set to **OSPF\_ROUTE\_FILTER\_PARAM\_TYPE**.

**ofaActionOnMatch (4 bytes):** Set to 0 or 1 as mentioned in [OSPF\\_FILTER\\_ACTION \(section 2.2.1.1.15\)](#).

**dwNumFilters (4 bytes):** Set to the number of route filters present in the **pFilters** field.

**pFilters (variable):** List of route filters. This points to a buffer that contains a list of structures of type [OSPF\\_ROUTE\\_FILTER \(section 2.2.1.2.208\)](#).

### 2.2.1.2.210 OSPF\_PROTO\_FILTER\_INFO

This structure [<159>](#) contains the OSPF protocol filter information is used by the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

```
typedef struct {
    DWORD type;
    OSPF_FILTER_ACTION ofaActionOnMatch;
    DWORD dwNumFilters;
    DWORD pdwProtoId[1];
} OSPF_PROTO_FILTER_INFO;
```

**type:** This MUST be set to OSPF\_PROTO\_FILTER\_INFO\_TYPE.

**ofaActionOnMatch:** Set to 0 or 1 as mentioned in [OSPF\\_FILTER\\_ACTION \(section 2.2.1.1.15\)](#).

**dwNumFilters:** The number of protocol filters present in the **pFilter** field.

**pdwProtoId:** A list of protocol IDs. This list MUST contain one or more values defined in [MIB\\_IPFORWARD\\_PROTO \(section 2.2.1.1.9\)](#). All other values are ignored.

### 2.2.1.2.211 OSPF\_GLOBAL\_PARAM

This structure [<160>](#) contains the OPSF global parameters and is used by the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

```
typedef struct {
    DWORD type;
    DWORD create;
    DWORD enable;
    DWORD routerId;
    DWORD ASBrdrRtr;
    DWORD logLevel;
} OSPF_GLOBAL_PARAM;
```

**type:** This MUST be set to OSPF\_GLOBAL\_PARAM\_TYPE.

**create:** Set to 1 if the configuration needs to be created or set to 2 if it needs to be deleted.

**enable:** Set to 1 if the configuration needs to be enabled or set to 2 if it needs to be deleted.

**routerId:** This can be any value, or the IP address of the router, and MUST NOT be zero.

**ASBrdrRtr:** If it is the boundary router set to 1, otherwise set to 2.

**logLevel:** Set to 0 if no logging, 1 if an error, 2 if a warning, and 3 if information.

#### 2.2.1.2.212 OSPF\_AREA\_PARAM

This structure [<161>](#) contains the OSPF area parameters and is used by the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

When calling **RRouterInterfaceTransportSetGlobalInfo** (section 3.1.4.10) you MUST NOT delete the area with the areaId set to 0.0.0.0, which works as the backbone area for the OSPF, otherwise the method will return a failure.

```
typedef struct {
    DWORD type;
    DWORD create;
    DWORD enable;
    DWORD areaId;
    DWORD authType;
    DWORD importASExtern;
    DWORD stubMetric;
    DWORD importSumAdv;
} OSPF_AREA_PARAM;
```

**type:** This MUST be set to **OSPF\_AREA\_PARAM\_TYPE**.

**create:** Set to 1 if the configuration needs to be created or set to 2 if it needs to be deleted.

**enable:** Set to 1 if the configuration needs to be enabled or set to 2 if it needs to be deleted.

**areaId:** Set to 0 if it is border. Otherwise, set to any nonzero value.

**authType:** Set to 1 if there is no password or set to 2 for a simple password.

**importASExtern:** Set to 1 if yes, 2 for no.

**stubMetric:** Stub area metric. It MUST be set to a value between 1 and USHORTMAX/2.

**importSumAdv:** The import summary advertisement. Set to 1 if yes, 2 for no.

#### 2.2.1.2.213 OSPF\_AREA\_RANGE\_PARAM

This structure [<162>](#) contains the OSPF area range parameters. This structure is used by the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

```
typedef struct {
    DWORD type;
    DWORD create;
    DWORD enable;
    DWORD areaId;
    DWORD rangeNet;
    DWORD rangeMask;
} OSPF_AREA_RANGE_PARAM;
```

**type:** This MUST be set to **OSPF\_AREA\_RANGE\_PARAM\_TYPE**.

**create:** Set to 1 if the configuration needs to be created, or set to 2 if it needs to be deleted.

**enable:** Set to 1 if the configuration needs to be enabled, or set to 2 if it needs to be deleted.

**areaId:** Set to 0 if it is a border. Otherwise, set it to any nonzero value.

**rangeNet:** The IP address of the subnet.

**rangeMask:** The mask of the IP address subnet.

#### 2.2.1.2.214 OSPF\_VIRT\_INTERFACE\_PARAM

This structure [<163>](#) contains the OSPF virtual interface parameters and is used by the following methods:

[RRouterInterfaceTransportSetGlobalInfo \(section 3.1.4.10\)](#)

[RRouterInterfaceTransportGetGlobalInfo \(section 3.1.4.11\)](#)

```
typedef struct {
    DWORD type;
    DWORD create;
    DWORD enable;
    DWORD transitAreaId;
    DWORD virtNeighborRouterId;
    DWORD transitDelay;
    DWORD retransInterval;
    DWORD helloInterval;
    DWORD deadInterval;
    BYTE password[8];
} OSPF_VIRT_INTERFACE_PARAM;
```

**type:** This MUST be set to **OSPF\_VIRT\_INTF\_PARAM\_TYPE**.

**create:** Set to 1 if the configuration needs to be created or set to 2 if it needs to be deleted.

**enable:** Set to 1 if the configuration needs to be enabled or set to 2 if it needs to be deleted.

**transitAreaId:** The transit area ID. It MUST not be set to 0; it MUST be set to an IP address.

**virtNeighborRouterId:** The virtual neighbor router ID (for example, the IP address).

**transitDelay:** This MUST be set to a value a value between 1 and 3600.

**retransInterval:** This MUST be set to a value between 1 and 3600.

**helloInterval:** This MUST be set to a value between 1 and USHORTMAX/2.

**deadInterval:** This MUST be set to a value between 1 and USHORTMAX/2.

**password:** The password.

#### 2.2.1.2.215 OSPF\_INTERFACE\_PARAM

This structure [<164>](#) contains the OSPF Non-Broadcast Multiple Access (NBMA) neighbor parameters and is used in the following methods:

[RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)

[RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)

[RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```
typedef struct {
    DWORD type;
    DWORD create;
    DWORD enable;
    DWORD intfIpAddress;
    DWORD intfSubnetMask;
    DWORD areaId;
    DWORD intfType;
    DWORD routerPriority;
    DWORD transitDelay;
    DWORD retransInterval;
    DWORD helloInterval;
    DWORD deadInterval;
    DWORD pollInterval;
    DWORD metricCost;
    BYTE password[8];
    DWORD mtuSize;
} OSPF_INTERFACE_PARAM;
```

**type:** This MUST be set to **OSPF\_INTF\_PARAM\_TYPE**.

**create:** This MUST be set to 1 if the configuration needs to be created or set to 2 if it needs to be deleted.

**enable:** This MUST set to 1 if the configuration needs to be enabled or set to 2 if it needs to be deleted.

**intfIpAddress:** The interface address on which the OSPF is enabled.

**intfSubnetMask:** The interface subnet address on which the OSPF is enabled. See [\[RFC950\]](#).

**areaId:** The area ID of the OSPF area of which the interface is a part.

**intfType:** Set to 1 for broadcast, set to 2 for NBMA, and set to 3 for point-to-point.

**routerPriority:** This MUST be set to a value between 1 and 255.

**transitDelay:** This MUST be set to a value between 1 and 3600.

**retransInterval:** This MUST be set to a value between 1 and 3600.

**helloInterval:** This MUST be set to a value between 1 and USHORTMAX/2.

**deadInterval:** This MUST be set to a value between 1 and USHORTMAX/2.

**pollInterval:** This MUST be set to a value between 1 and USHORTMAX/2.

**metricCost:** This MUST be set to a value between 1 and USHORTMAX/2.

**password[8]:** The password.

**mtuSize:** This MUST be set to a value between 1 and 10000.

#### 2.2.1.2.216 OSPF\_NBMA\_NEIGHBOR\_PARAM

This structure [<165>](#) contains the OSPF NBMA neighbor parameters and is used in the following methods:

[RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#)

[RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#)

[RRouterInterfaceTransportSetInfo \(section 3.1.4.20\)](#)

```
typedef struct {
    DWORD type;
    DWORD create;
    DWORD enable;
    DWORD neighborIpAddr;
    DWORD intfIpAddr;
    DWORD neighborPriority;
} OSPF_NBMA_NEIGHBOR_PARAM;
```

**type:** This MUST be set to **OSPF\_NEIGHBOR\_PARAM\_TYPE**.

**create:** Set to 1 if the configuration needs to be created or set to 2 if it needs to be deleted.

**enable:** Set to 1 if the configuration needs to be created or set to 2 if it needs to be deleted.

**neighborIpAddr:** The neighbor IP address.

**intfIpAddr:** The interface IP address.

**neighborPriority:** The priority of the neighbor.

#### 2.2.1.2.217 RequestBuffer

The RequestBuffer is a generic information container used by the [RasRpcSubmitRequest \(section 3.4.4.5\)](#) method to set or retrieve information on RRAS server.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
RB_PCBIndex																															
RB_Rectype																															
RB_Dummy (optional)																															
RB_Done																															
Alignment																															
...																															
RB_Buffer (variable)																															
...																															

**RB\_PCBIndex (4 bytes):** A unique identifier for the port.

**RB\_Rectype (4 bytes):** A [ReqTypes \(section 2.2.1.1.18\)](#) enumeration value indicating the request type sent to the server.

**RB\_Dummy (4 bytes):** MUST be set to the size of the ULONG\_PTR on the client. [<166>](#)

**RB\_Done (4 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**Alignment (8 bytes):** MUST be set to zero when sent and MUST be ignored on receipt.

**RB\_Buffer (variable):** A pointer to the buffer that contains the information specific to the **RB\_Rectype** request type.

This information MUST be one of the following structures depending upon the **RB\_Rectype ReqTypes**.

Structure	ReqTypes
<a href="#">DeviceConfigInfo (section 2.2.1.2.218)</a>	REQTYPE_SETDEVICECONFIGINFO
<a href="#">DeviceConfigInfo (section 2.2.1.2.218)</a>	REQTYPE_GETDEVICECONFIGINFO
<a href="#">GetSetCalledId (section 2.2.1.2.220)</a>	REQTYPE_GETCALLEDID
<a href="#">GetSetCalledId (section 2.2.1.2.220)</a>	REQTYPE_SETCALLEDID
<a href="#">GetNdiswanDriverCapsStruct (section 2.2.1.2.222)</a>	REQTYPE_GETNDISWANDRIVERCAPS
<a href="#">GetDevConfigStruct (section 2.2.1.2.224)</a>	REQTYPE_GETDEVCONFIG
<a href="#">Enum (section 2.2.1.2.225)</a>	REQTYPE_PORTENUM
<a href="#">Info (section 2.2.1.2.227)</a>	REQTYPE_GETINFO

### 2.2.1.2.218 DeviceConfigInfo

The DeviceConfigInfo structure contains information specific to the **REQTYPE\_SETDEVICECONFIGINFO** and **REQTYPE\_GETDEVICECONFIGINFO** [ReqTypes](#) ([section 2.2.1.1.18](#)).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
retcode																															
dwVersion																															
cbBuffer																															
cEntries																															
abdata (variable)																															
...																															

**retcode (4 bytes):** A 32-bit, unsigned integer value that indicates return status. A return value ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, specified in [\[MS-ERREF\]](#) or in [2.2.4](#).

**dwVersion (4 bytes):** Specifies the version of the server. [<167>](#)

**cbBuffer (4 bytes):** This MUST be set to the size, in bytes, of the buffer passed in **abdata**.

**cEntries (4 bytes):** Specifies the number of device entries as returned by the server.

**abdata (variable):** This refers to the buffer containing the array of [RAS\\_DEVICE\\_INFO](#) ([section 2.2.1.2.219](#)) structures as returned by the server.

### 2.2.1.2.219 RAS\_DEVICE\_INFO

The **RAS\_DEVICE\_INFO** structure contains device information.

```
typedef struct _RAS_DEVICE_INFO {
    DWORD dwVersion;
    BOOL fWrite;
    BOOL fRasEnabled;
    BOOL fRouterEnabled;
    BOOL fRouterOutboundEnabled;
    DWORD dwTapiLineId;
    DWORD dwError;
    DWORD dwNumEndPoints;
    DWORD dwMaxOutCalls;
    DWORD dwMaxInCalls;
    DWORD dwMinWanEndPoints;
    DWORD dwMaxWanEndPoints;
    RASDEVICETYPE eDeviceType;
    GUID guidDevice;
    CHAR szPortName[17];
}
```



```

    CHAR szDeviceName[129];
    WCHAR wszDeviceName[129];
} RAS_DEVICE_INFO,
*PRAS_DEVICE_INFO;

```

**dwVersion:** Specifies the version of the Rasrpc server. [<168>](#<168>)

**fWrite:** If set to 1, specifies that device information needs to be stored on RRAS. If set to 0, specifies that the device information does not need to be stored.

**fRasEnabled:** If set to 1, specifies that the device is enabled for incoming connections. If set to 0, specifies that the device is not enabled for incoming connections.

**fRouterEnabled:** If set to 1, specifies that the device is enabled for both incoming and outgoing **Demand dial** connection. If set to 0, specifies that the device is not enabled for both incoming and outgoing **Demand dial** connection.

**fRouterOutboundEnabled:** If set to 1, specifies that the device is enabled for outgoing Demand dial connection. This can be set to 1 only when fRouterEnabled is set to 0. [<169>](#<169>)

**dwTapiLineId:** Unique **TAPI** identifier for the device.

**dwError:** Specifies the return status as explained in section [2.2.1.2.218](#2.2.1.2.218) for the **retcode** field.

**dwNumEndPoints:** Specifies the number of WAN end points available for the device.

**dwMaxOutCalls:** Specifies the maximum number of outgoing connections allowed on the device.

**dwMaxInCalls:** Specifies the maximum number of incoming connections allowed on the device.

**dwMinWanEndPoints:** Specifies the minimum number of WAN **end points** allowed on the device.

**dwMaxWanEndPoints:** Specifies the maximum number of WAN **end points** allowed on the device.

**eDeviceType:** Specifies the **RASDEVICETYPE** enumeration type.

**guidDevice:** A **GUID** uniquely identifying the device. This value MUST NOT be used when eDeviceType is RDT\_Modem.

**szPortName:** Specifies a null-terminated ASCII string specifying the Port Name.

**szDeviceName:** Specifies a null-terminated ASCII string specifying the Device Name.

**wszDeviceName:** Specifies a null-terminated Unicode string specifying the Device Name. [<170>](#<170>)

## 2.2.1.2.220 GetSetCalledId

The **GetSetCalledId** structure contains information specific to the REQTYPE\_GETCALLEDID and REQTYPE\_SETCALLEDID [ReqTypes](#ReqTypes).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
retcode																															
fWrite																															
dwSize																															
guidDevice																															
...																															
...																															
...																															
rdi																															
...																															
...																															
...																															
...																															
...																															
...																															
...																															
...																															
(rdi cont'd for 110 rows)																															
rciInfo (variable)																															
...																															

**retcode (4 bytes):** Specifies the return status as explained in section [2.2.1.2.218](#) for the retcode field.

**fWrite (4 bytes):** If set to 1, specifies that **CalledID** information MUST be stored on RRAS. If set to 0, CalledId information MUST not be stored.

**dwSize (4 bytes):** Specifies the size, in bytes, of the rciInfo structure, including the rciInfo.bCalledId buffer, which is specified by the **dwSize** member of the [RAS\\_CALLEDID\\_INFO](#) structure.

**guidDevice (16 bytes):** This value MUST be set to 0 when sent and ignored on receipt.

**rdi (472 bytes):** Specifies the RAS\_DEVICE\_INFO structure as defined in section [2.2.1.2.219](#)

**rciInfo (variable):** Specifies the RAS\_CALLEDID\_INFO structure as defined in section [2.2.1.2.221](#)

#### 2.2.1.2.221 RAS\_CALLEDID\_INFO

The **RAS\_CALLEDID\_INFO** structure contains the TAPI CalledId information.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
dwSize																															
bCalledId (variable)																															
...																															

**dwSize (4 bytes):** Specifies the size in bytes of the bCalledId buffer.

**bCalledId (variable):** Specifies the buffer containing the null-terminated Unicode string representing the called device phonenummer information.

#### 2.2.1.2.222 GetNdiswanDriverCapsStruct

The **GetNdiswanDriverCapsStruct** structure contains the information specific to the REQTYPE\_GETNDISWANDRIVERCAPS **ReqTypes**

```
typedef struct GetNdiswanDriverCapsStruct {
    DWORD retcode;
    RAS_NDISWAN_DRIVER_INFO NdiswanDriverInfo;
} GetNdiswanDriverCapsStruct;
```

**retcode:** Specifies the return status as explained in section [2.2.1.2.218](#) for retcode field.

**NdiswanDriverInfo:** The **RAS\_NDISWAN\_DRIVER\_INFO** structure.

#### 2.2.1.2.223 RAS\_NDISWAN\_DRIVER\_INFO

The RAS\_NDISWAN\_DRIVER\_INFO structure contains the encryption capabilities of the RRAS server.

```
typedef struct _RAS_NDISWAN_DRIVER_INFO {
    ULONG DriverCaps;
    ULONG Reserved;
} RAS_NDISWAN_DRIVER_INFO,
 *P_NDISWAN_DRIVER_INFO;
```

**DriverCaps:** Specifies the encryption capabilities of the RRAS. It MUST be one of the following values.

Value	Meaning
RAS_NDISWAN_40BIT_ENABLED 0x00000000	40-bit encryption supported
RAS_NDISWAN_128BIT_ENABLED 0x00000001	128-bit encryption supported

**Reserved:** MUST be set to zero when sent and MUST be ignored on receipt.

#### 2.2.1.2.224 GetDevConfigStruct

The GetDevConfigStruct structure contains information specific to the **REQTYPE\_GETDEVCONFIG** [ReqTypes \(section 2.2.1.1.18\)](#).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
retcode																															
devicetype																															
...																															
...																															
...																															
...										size																					
...										config (variable)																					
...																															

**retcode (4 bytes):** Specifies the return status as explained in section [2.2.1.2.218](#) for retcode field.

**devicetype (17 bytes):** Specifies a null-terminated ASCII string that indicates the RRAS server device type as specified for the **wszDeviceType** field in the [RASI\\_PORT\\_0 \(section 2.2.1.2.76\)](#) structure.

**size (4 bytes):** Specifies the size in bytes of the configuration data as specified by **config**.

**config (variable):** Tapi device configuration blob as specified by **GetDevConfig.IpDeviceConfig** in section 2.2.4.1.3.33 of [\[MS-TRP\]](#).

#### 2.2.1.2.225 Enum

The Enum structure contains information specific to the **REQTYPE\_PORTENUM** [ReqTypes \(section 2.2.1.1.18\)](#) value.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
retcode																															
size																															
entries																															
buffer (variable)																															
...																															

**retcode (4 bytes):** Specifies the return status as explained in section [2.2.1.2.218](#) for the **retcode** field.

**size (4 bytes):** Specifies the size in bytes of the **buffer**.

**entries (4 bytes):** Specifies the number of port entries as pointed by the **buffer**.

**buffer (variable):** Points to the array of [RASMAN\\_PORT\\_32 \(section 2.2.1.2.226\)](#) structures.

#### 2.2.1.2.226 RASMAN\_PORT\_32

The **RASMAN\_PORT\_32** structure contains information regarding a specific RAS port, such as port status and port name.

```
typedef struct _RASMAN_PORT_32 {
    DWORD P_Port;
    CHAR P_PortName[16];
    RASMAN_STATUS P_Status;
    RASDEVICETYPE P_rdtDeviceType;
    RASMAN_USAGE P_ConfiguredUsage;
    RASMAN_USAGE P_CurrentUsage;
    CHAR P_MediaName[16];
    CHAR P_DeviceType[16];
    CHAR P_DeviceName[129];
    DWORD P_LineDeviceId;
    DWORD P_AddressId;
} RASMAN_PORT_32;
```

**P\_Port:** A unique identifier for the port.

**P\_PortName:** Specifies a null-terminated ASCII string specifying the port name.

**P\_Status:** Specifies the status of the port as defined in the [RASMAN\\_STATUS \(section 2.2.1.1.17\)](#) enumeration type.

**P\_rdtDeviceType:** Specifies the device type of the port as defined in the [RASDEVICETYPE \(section 2.2.1.1.16\)](#) enumeration type.

**P\_ConfiguredUsage:** Specifies the configured usage of the port as defined in section [2.2.1.1.21](#).

**P\_CurrentUsage:** Specifies the usage for the port currently being used as defined in section [2.2.1.1.21](#).

**P\_MediaName:** A null-terminated ASCII string specifying the name of the media associated with the port.

**P\_DeviceType:** Specifies a null-terminated ASCII string that indicates the RRAS server device type as specified for the **wszDeviceType** field of the [RASI\\_PORT\\_0 \(section 2.2.1.2.76\)](#) structure.

**P\_DeviceName:** A null-terminated ASCII string specifying the name of the device associated with the port.

**P\_LineDeviceId:** Specifies a unique identifier for the device.

**P\_AddressId:** MUST be set to zero when sent and ignored on receipt.

### 2.2.1.2.227 Info

The **Info** structure contains information specific to the **REQTYPE\_GETINFO** [ReqTypes \(section 2.2.1.1.18\)](#) value.

```
typedef struct Info {
    union {
        DWORD retcode;
        HANDLE paddingField;
    };
    RASMAN_INFO info;
} Info;
```

**retcode:** Specifies the return status as explained in section [2.2.1.2.218](#) for the **retcode** field.

**paddingField:** Reserved field to provide proper alignment of the structure.

**info:** Specifies the port information as defined in the [RASMAN\\_INFO \(section 2.2.1.2.228\)](#) structure.

### 2.2.1.2.228 RASMAN\_INFO

The **RASMAN\_INFO** structure contains general information regarding a specific RRAS port, such as port status and port name.

```
typedef struct _RASMAN_INFO {
    RASMAN_STATUS RI_PortStatus;
    RASMAN_STATE RI_ConnState;
    DWORD RI_LinkSpeed;
    DWORD RI_LastError;
    RASMAN_USAGE RI_CurrentUsage;
    CHAR RI_DeviceTypeConnecting[16];
    CHAR RI_DeviceConnecting[129];
    CHAR RI_szDeviceType[16];
    CHAR RI_szDeviceName[129];
    CHAR RI_szPortName[17];
    RASMAN_DISCONNECT_TYPE RI_DisconnectType;
    DWORD RI_OwnershipFlag;
```

```

    DWORD RI_ConnectDuration;
    DWORD RI_BytesReceived;
    CHAR RI_Phonebook[261];
    CHAR RI_PhoneEntry[257];
    HANDLE RI_ConnectionHandle;
    DWORD RI_SubEntry;
    RASDEVICETYPE RI_rdtDeviceType;
    GUID RI_GuidEntry;
    DWORD RI_dwSessionId;
    DWORD RI_dwFlags;
    GUID RI_CorrelationGuid;
} RASMAN_INFO;

```

**RI\_PortStatus:** Specifies the status of the port as defined in [RASMAN STATUS \(section 2.2.1.1.17\)](#) enumeration type.

**RI\_ConnState:** Specifies the connection state of the port as defined in [RASMAN STATE \(section 2.2.1.1.19\)](#).

**RI\_LinkSpeed:** Specifies the link speed in bits per second (bps) of the connection using port as specified by **RI\_szPortName**.

**RI\_LastError:** Specifies the return status as explained in section [2.2.1.2.218](#) for **retcode** field.

**RI\_CurrentUsage:** Specifies the current usage of the port as defined in section [2.2.1.1.21](#).

**RI\_DeviceTypeConnecting:** Specifies a null-terminated ASCII string that indicates the RRAS server device type as specified for the **wszDeviceType** field of a [RASI\\_PORT\\_0 \(section 2.2.1.2.76\)](#) structure.

**RI\_DeviceConnecting:** Specifies a null-terminated ASCII string containing the name of the device associated with the port.

**RI\_szDeviceType:** Specifies a null-terminated ASCII string containing the RRAS server device type as specified for the **wszDeviceType** field of RASI\_PORT\_0 structure.

**RI\_szDeviceName:** Specifies a null-terminated ASCII string containing the name of the device associated with the port.

**RI\_szPortName:** Specifies a null-terminated ASCII string containing the port name.

**RI\_DisconnectType:** Specifies the disconnect type of the port as defined by the [RASMAN\\_DISCONNECT\\_TYPE \(section 2.2.1.1.20\)](#) enumeration type.

**RI\_OwnershipFlag:** Specifies the **PID** of the **client** application that has opened the port.

**RI\_ConnectDuration:** Specifies the duration of the current connection on this port, in milliseconds.

**RI\_BytesReceived:** Specifies the number of bytes received on this port.

**RI\_Phonebook:** Specifies the **RRAS Phonebook path** for the connection associated with this port.

**RI\_PhoneEntry:** Specifies the **RRAS Phonebook entry** name for the connection associated with this port.

**RI\_ConnectionHandle:** Specifies a unique 32-bit unsigned integer identifying the connection associated with this port.

**RI\_SubEntry:** Specifies an index to the **multilink** subentry associated with this port.

**RI\_rdtDeviceType:** Specifies a value giving the [RASDEVICETYPE \(section 2.2.1.1.16\)](#) enumeration type.

**RI\_GuidEntry:** Specifies a GUID uniquely identifying the connection associated with the port.

**RI\_dwSessionId:** Specifies the unique session ID associated with the port.[<171>](#)

**RI\_dwFlags:** Specifies the configuration option of the connection associated with this port.[<172>](#)

The value MUST be one of the following values or a bit-wise OR combination of the following values.

Value	Meaning
0x00000001	Connection associated with this port is configured to store the credentials for everyone.
0x00000002	Connection associated with this port is configured as outgoing connection.

**RI\_CorrelationGuid:** Specifies a GUID that uniquely identifies the connection associated with this port.[<173>](#)

## 2.2.1.2.229 RASRPC\_PBUSER

The RASRPC\_PBUSER structure contains configuration information of Demand Dial connection.

```
typedef struct _RASRPC_PBUSER {
    BOOL fOperatorDial;
    BOOL fPreviewPhoneNumber;
    BOOL fUseLocation;
    BOOL fShowLights;
    BOOL fShowConnectStatus;
    BOOL fCloseOnDial;
    BOOL fAllowLogonPhonebookEdits;
    BOOL fAllowLogonLocationEdits;
    BOOL fSkipConnectComplete;
    BOOL fNewEntryWizard;
    DWORD dwRedialAttempts;
    DWORD dwRedialSeconds;
    DWORD dwIdleDisconnectSeconds;
    BOOL fRedialOnLinkFailure;
    BOOL fPopupOnTopWhenRedialing;
    BOOL fExpandAutoDialQuery;
    DWORD dwCallbackMode;
    [unique] LPRASRPC_CALLBACKLIST pCallbacks;
    WCHAR pszLastCallbackByCaller[129];
    DWORD dwPhonebookMode;
    WCHAR pszPersonalFile[260];
    WCHAR pszAlternatePath[260];
    [unique] LPRASRPC_STRINGLIST pPhonebooks;
    [unique] LPRASRPC_STRINGLIST pAreaCodes;
```



```

    BOOL fUseAreaAndCountry;
    [unique] LPRASRPC_STRINGLIST pPrefixes;
    [unique] LPRASRPC_STRINGLIST pSuffixes;
    [unique] LPRASRPC_LOCATIONLIST pLocations;
    DWORD dwXPhonebook;
    DWORD dwYPhonebook;
    WCHAR pszDefaultEntry[257];
    BOOL fInitialized;
    BOOL fDirty;
} RASRPC_PBUSER,
*LPRASRPC_PBUSER;

```

**fOperatorDial:** It is unused and can be set to any value.

**fPreviewPhoneNumber:** It is unused and can be set to any value.

**fUseLocation:** It is unused can be set to any value.

**fShowLights:** It is unused and can be set to any value.

**fShowConnectStatus:** It is unused and can be set to any value.

**fCloseOnDial:** It is unused and can be set to any value.

**fAllowLogonPhonebookEdits:** It is unused and can be set to any value.

**fAllowLogonLocationEdits:** It is unused and can be set to any value.

**fSkipConnectComplete:** It is unused and can be set to any value.

**fNewEntryWizard:** It is unused and can be set to any value.

**dwRedialAttempts:** It is unused and can be set to any value.

**dwRedialSeconds:** It is unused and can be set to any value.

**dwIdleDisconnectSeconds:** It is unused and can be set to any value.

**fRedialOnLinkFailure:** It is unused and can be set to any value.

**fPopupOnTopWhenRedialing:** It is unused and can be set to any value.

**fExpandAutoDialQuery:** It is unused and can be set to any value.

**dwCallbackMode:** It is unused and can be set to any value.

**pCallbacks:** A pointer to a linked list of callback information specified by [RASRPC\\_CALLBACKLIST \(section 2.2.1.2.230\)](#) structures. Each member of the linked list specifies the callback information for a particular port associated with a device.

**pszLastCallbackByCaller:** A null-terminated Unicode string specifying the callback phone number last used.

**dwPhonebookMode:** It is unused and can be set to any value.

**pszPersonalFile:** It MUST be set to an empty string("").

**pszAlternatePath:** It MUST be set to an empty string("").

**pPhonebooks:** It is not used and can be set to NULL.

**pAreaCodes:** It is not used and can be set to NULL.

**fUseAreaAndCountry:** It is unused and can be set to any value.

**pPrefixes:** It MUST be set to NULL.

**pSuffixes:** It MUST be set to NULL.

**pLocations:** It MUST be set to NULL.

**dwXPhonebook:** It is unused and can be set to any value.

**dwYPhonebook:** It is unused can be set to any value.

**pszDefaultEntry:** It MUST be set to an empty string ("").

**fInitialized:** If set to 1, specifies that the RASRPC\_PBUSER structure is initialized if set to 0 specifies that the RASRPC\_PBUSER structure is not initialized.

**fDirty:** If set to 1, specifies that the RASRPC\_PBUSER structure needs to be stored on server. If set to 0, specifies that the RASRPC\_PBUSER structure need not be stored on RRAS.

#### 2.2.1.2.230 RASRPC\_CALLBACKLIST

The **RASRPC\_CALLBACKLIST** structure specifies the callback information such as the callback device name and the callback phonenumber.

```
typedef struct _RASRPC_CALLBACKLIST {
    WCHAR pszPortName[RASRPC_MaxPortName + 1];
    WCHAR pszDeviceName[RASRPC_MaxDeviceName + 1];
    WCHAR pszNumber[RASRPC_MaxPhoneNumber + 1];
    DWORD dwDeviceType;
    [unique] struct _RASRPC_CALLBACKLIST* pNext;
} RASRPC_CALLBACKLIST,
*LPRASRPC_CALLBACKLIST;
```

**pszPortName:** A null-terminated Unicode string specifying the port name on which callback is made.

**pszDeviceName:** A null-terminated Unicode string specifying the device name on which callback is be made.

**pszNumber:** A null-terminated Unicode string specifying the phone number to which callback is be made.

**dwDeviceType:** Specifies the device type to which callback is to be made.

This MUST take one of the following values:

Value	Meaning
PBDT_None 0	No device.
PBDT_Null 1	Serial or parallel port device.
PBDT_Other 2	Device other than mentioned in the table.
PBDT_Modem 3	A modem device.
PBDT_Pad 4	An X.25 <a href="#">[X.25]</a> packet assembler/disassembler. <a href="#">&lt;174&gt;</a>
PBDT_Switch 5	Switch device.
PBDT_Isdn 6	An ISDN device.
PBDT_X25 7	An X.25 [X.25] device. <a href="#">&lt;175&gt;</a>
PBDT_ComPort 8	Generic COM port device.
PBDT_Irda 10	An Infrared Data Association (IrDA)-compliant device.
PBDT_Vpn 11	A virtual private network (VPN) device
PBDT_Serial 12	Serial port device.
PBDT_Atm 13	Asynchronous Transfer Mode (ATM) device.
PBDT_Parallel 14	Parallel port device.
PBDT_Sonet 15	Sonet device.
PBDT_Sw56 16	Switched 56K Access.
PBDT_FrameRelay 17	Frame Relay device.
PBDT_PPPE 18	PPPoE device. <a href="#">&lt;176&gt;</a>

**pNext:** Specifies the pointer to the next RASRPC\_CALLBACKLIST structure. The last member of the linked list of RASRPC\_CALLBACKLIST structures MUST have the **pNext** field set to NULL.

#### 2.2.1.2.231 RASRPC\_STRINGLIST

The **RASRPC\_STRINGLIST** structure contains a null-terminated Unicode string.

```
typedef struct _RASRPC_STRINGLIST {
    WCHAR psz[256];
    [unique] struct _RASRPC_STRINGLIST* pNext;
} RASRPC_STRINGLIST,
*LPRASRPC_STRINGLIST;
```

**psz:** Specifies a null-terminated Unicode string.

**pNext:** Specifies the pointer to the next RASRPC\_STRINGLIST structure.

#### 2.2.1.2.232 RASRPC\_LOCATIONLIST

The **RASRPC\_LOCATIONLIST** structure contains information related to the TAPI location identifier.

```
typedef struct _RASRPC_LOCATIONLIST {
    DWORD dwLocationId;
    DWORD iPrefix;
    DWORD iSuffix;
    [unique] struct _RASRPC_LOCATIONLIST* pNext;
} RASRPC_LOCATIONLIST,
*LPRASRPC_LOCATIONLIST;
```

**dwLocationId:** Specifies the TAPI location id.

**iPrefix:** It is unused and if set MUST be ignored by RRAS.

**iSuffix:** It is unused and if set MUST be ignored by RRAS.

**pNext:** Specifies the pointer to the next RASRPC\_LOCATIONLIST structure.

### 2.2.2 File Format for Phonebook

The Phonebook is an 8-bit ASCII-encoded text file that contains the names and settings for the demand dial connections. It includes the connection settings that can be used for establishing the demand dial connections. The RRAS client can remotely configure this file on the RRAS server at a well-known name and location using any remote file management protocol (such as SMB). RRAS can read the file from this location [177](#) for gathering the demand dial connection settings.

The name and the settings for a single demand dial connection is known as an **RRAS phonebook section** (also known as RRAS phonebook entry or RRAS entry). An RRAS entry begins with the name of demand dial connection, which MUST be unique. The name is followed by settings as a sequence of **key value pairs**. The phonebook file can have zero (when there are no demand dial connections) or more RRAS entry sections.

Each RRAS entry section in the phonebook file can have the following four **RRAS entry subsections**: NETCOMPONENTS, MEDIA, DEVICE, and PhoneNumber. The NETCOMPONENTS and PhoneNumber subsections are optional, whereas MEDIA and DEVICE subsections MUST be present. There can be multiple MEDIA subsections within a single RRAS entry section. Each MEDIA subsection can have multiple DEVICE subsections and each DEVICE subsection in turn can have multiple

PhoneNumber subsections. When there are multiple MEDIA subsections, each subsection corresponds to a physical device.

RRASM uses the list of phonebook entries to validate the WAN interface name as a part of specific RPC methods as specified in section [3.1.1](#). In order for the WAN interface name to be valid, there has to be a RRAS phonebook entry with the specified name.

### 2.2.2.1 RRAS entry section name

An RRAS entry section is identified by a unique RRAS entry section name. The RRAS entry section name **MUST** be a minimum of one (1) character in length.

The RRAS entry section name **MUST** be enclosed within an open square bracket "[" and a closing square bracket "]", followed by a line-feed and carriage return. An RRAS entry section extends from the beginning of one RRAS entry section name to the start of the next RRAS entry section or the end of file. Consider the following example.

```
[Remote Router]\LF\CR
```

"[Remote Router]\LF\CR" is the beginning of a RRAS entry section with the name "Remote Router".[<178>](#)

### 2.2.2.2 Phonebook entry settings

Each RRAS entry section **MUST** consist of a sequence of key value pairs separated by line-feed and carriage return. A key-value pair **MUST** be a key name followed by an equal sign "=" with the value after the equal sign.

For example:

```
Encoding=1\LF\CR
```

Encoding is the name of the key and 1 is its value.

In cases where the value is optional, the key is followed by an equal sign "=" and a line-feed and carriage return. The value is not specified for the key.

For example:

```
Encoding=\LF\CR
```

Here, Encoding is the name of key and it does not take a value. The implementation can assume a default value for the key or ignore it.

The following sections provide descriptions for each key used in the phonebook file and their possible values. All the keys **MUST** appear in the same order in the phonebook file as they appear here, unless explicitly specified.

In the following sections, if an optional key is absent or for any key the value is not one of the specified valid values, the behavior of the RRAS is implementation-specific and outside the scope of this document. For example, if the "Encoding" key is not present, or the value of the key is not "0" or "1", then a compliant implementation may decide to assume the value of an encoding is "1".

#### 2.2.2.2.1 Encoding

This key specifies the encoding format for all the string values in the current RRAS entry. This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	All strings in the RRAS entry are encoded in 8-bit ASCII format.
1	All strings in the RRAS entry are encoded in UTF-8 format <a href="#">[RFC3629]</a> .

#### 2.2.2.2.2 PBVersion

This key specifies the version of the RRAS entry. This key is optional. If the key is present, the value SHOULD be "1".

#### 2.2.2.2.3 Type

This key specifies the type of the RRAS entry. This key SHOULD take one of the values in the following table. [<179>](#)

Value	Meaning
1	Dial-up connection
2	VPN connection
5	Broadband connection <a href="#">&lt;180&gt;</a>

#### 2.2.2.2.4 Autologon

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.5 UseRasCredentials

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.6 LowDateTime

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.7 HighDateTime

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.8 DialParamsUID

This key specifies a unique identifier (an 8-bit ASCII-encoded string representation of a decimal number) to be used on RRAS for use as a credential key for demand-dial connection. This key is optional.

#### 2.2.2.2.9 Guid

This key specifies a unique identifier (GUID) for this RRAS entry. This key is optional.

#### 2.2.2.2.10 BaseProtocol

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.11 VpnStrategy

This key specifies the order in which the RRAS attempts the tunnel protocol until the demand-dial connection succeeds. This key is optional. If the key is present, it is used only if the key **Type** has the value "2" and SHOULD take one of the values in the following table.

Value	Meaning
0	Try a series of tunnel protocols.<181>
1	RRAS attempts PPTP only.
2	RRAS attempts PPTP first. If PPTP fails, L2TP is tried. If L2TP fails, demand-dial connection fails.
3	RRAS attempts L2TP only.

#### 2.2.2.2.12 ExcludedProtocols

This key specifies the protocols not to be negotiated by the RRAS. This key is an 8-bit ASCII-encoded string representation of a decimal number used as a bit field. The bits are defined in the following table. This key is optional.

Bit number (From LSB)	Network Protocol	Meaning
0 (LSB)	NetBEUI	0 – Negotiate NetBEUI 1 – Don't negotiate NetBEUI <182>
1	IPX <183>	0 – Negotiate IPX 1 – Don't negotiate IPX <183>
2	IPv4 <184>	0 – Negotiate IPv4 1 – Don't negotiate IPv4
3	IPv6 [RFC5072]	0 – Negotiate IPv6 1 – Don't negotiate IPv6 <184>

#### 2.2.2.2.13 LcpExtensions

This key specifies whether the option for LCP extensions, as defined in <185>, is enabled for the RRAS entry. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	Do not configure LCP extensions.
1	Configure LCP extensions.

#### 2.2.2.2.14 DataEncryption

This key specifies the encryption type to be negotiated by the RRAS. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	RRAS will not negotiate encryption.
8	RRAS requests encryption during negotiation. Negotiation will succeed even if remote RRAS does not support encryption.
256	RRAS requires encryption to be negotiated.
512	RRAS requires maximum strength encryption to be negotiated.

#### 2.2.2.2.15 SwCompression

This key specifies whether the option for software compression, as defined in [\[RFC1962\]](#), is enabled on the RRAS entry. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	Do not use software compression.
1	Use software compression.

#### 2.2.2.2.16 NegotiateMultilinkAlways

This key specifies whether the option for **multilink** is enabled on the RRAS entry. This key is optional. If the key is present, it is used only if the key Type has the value "1" and SHOULD take one of the values in the following table.

Value	Meaning
0	RRAS will not negotiate multilink.
1	RRAS will negotiate multilink.

#### 2.2.2.2.17 SkipNwcWarning

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.18 SkipDownLevelDialog

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.19 SkipDoubleDialDialog

This key is optional and if present MUST be ignored by RRAS.



#### 2.2.2.2.20 DialMode

This key specifies the dialing mode for the RRAS entry. This key is optional. If the key is present, it is used only if the key **Type** has the value "1" and SHOULD take one of the values in the following table.

Value	Meaning
0	RRAS dials first available subentry
1	RRAS dials all the subentries
2	RRAS dials subentries as needed <a href="#">&lt;185&gt;</a>

#### 2.2.2.2.21 DialPercent

This key specifies a percent of the total bandwidth available through the currently connected **subentry**, or subentries, for the demand-dial connection. If the bandwidth actually consumed exceeds this value, then RRAS will dial an additional subentry. This key is optional; if present, it is used only if the key **Type** has the value "1" and the key DialMode has the value "2". The value for this key SHOULD be a decimal number in the range 0 to 100. [<186>](#)

#### 2.2.2.2.22 DialSeconds

This key specifies the number of seconds that current bandwidth usage must exceed the threshold specified by **DialPercent** before RRAS dials an additional subentry. This key is optional. If the key is present, it is used only if the key **Type** has the value "1" and the key DialMode has the value "2". The value for this key SHOULD be a decimal number in the range 0 to 3600. [<187>](#)

#### 2.2.2.2.23 HangupPercent

This key specifies a percent of the total bandwidth available from the currently connected subentries for a demand-dial connection. RRAS terminates a currently connected subentry when the total bandwidth used is less than this value. The key is optional; if present, it is used only if the key **Type** has the value "1" and the key **DialMode** has the value "2". The value for this key SHOULD be a decimal number in the range 0 to 100. [<188>](#)

#### 2.2.2.2.24 HangupSeconds

This key specifies the time, in seconds, that the current bandwidth usage must be less than the threshold specified by **HangupPercent**, after which RRAS terminates a currently connected subentry. This key is optional; if present, it is used only if its key **Type** has the value "1" and its key **DialMode** has the value "2". The value for this key SHOULD be a decimal number in the range 0 to 3600. [<189>](#)

#### 2.2.2.2.25 OverridePref

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.26 RedialAttempts

This key specifies the number of times RRAS attempts to redial a connection. This key is optional. If the key is present, it SHOULD be a decimal number in the range 0 to 99.

#### 2.2.2.2.27 RedialSeconds

This key specifies the number of seconds to wait between redial attempts. This key is optional. If the key is present, it SHOULD be a decimal number in the range 1 and 600.

#### 2.2.2.2.28 IdleDisconnectSeconds

This key specifies the number of seconds after which the demand-dial connection is terminated due to inactivity. This key is optional. If the key is present, the value SHOULD be a number in the range 0 to 4294967296.

#### 2.2.2.2.29 RedialOnLinkFailure

This key indicates whether RRAS automatically attempts to re-establish the demand-dial connection if it is lost. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	RRAS does not re-establish the demand-dial connection if it is lost.
1	RRAS Server establishes the demand-dial connection if it is lost.

#### 2.2.2.2.30 CallbackMode

This key specifies whether the option for callback is enabled on the RRAS entry. This key is optional. If the key is present, it is used only if the key **Type** has the value "1" and SHOULD take one of the values in the following table.

Value	Meaning
0	Do not negotiate callback.
1	Negotiating callback is optional.
2	Callback is negotiated.

#### 2.2.2.2.31 CustomDialDll

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.32 CustomDialFunc

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.33 CustomRasDialDll

This key specifies the file path to a custom dialer dynamic link library. This key is optional.

#### 2.2.2.2.34 ForceSecureCompartment

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.35 DisableIKENNameEkuCheck

This key specifies whether the option for verifying the name of the RRAS certificate is enabled on the RRAS entry. [190](#) This key is optional. If the key is present, it is used only if the key **Type** has the value "2". It SHOULD take one of the values in the following table.

Value	Meaning
0	Verify that the name of RRAS certificate is the same as the value specified for the key PhoneNumber.
1	Do not verify the name of the RRAS certificate.

#### 2.2.2.2.36 AuthenticateServer

This key specifies whether the RRAS authenticates the remote RRAS when making a demand-dial connection. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	Do not authenticate the remote RRAS.
1	Authenticate the remote RRAS.

#### 2.2.2.2.37 ShareMsFilePrint

The value for this key indicates whether the option of file and printer sharing is enabled on the RRAS entry. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	Disable file and printer sharing on the RRAS entry.
1	Enable file and printer sharing on the RRAS entry.

#### 2.2.2.2.38 BindMsNetClient

This key indicates whether the option for NetBT is enabled on the RRAS entry. This key is optional. If the key is present, it SHOULD be set either to "0" or "1". This key, along with the value of the keys **ShareMsFilePrint** and **IpNBTFIags**, specifies whether NetBT is enabled or not. [191](#)

#### 2.2.2.2.39 SharedPhoneNumbers

This key specifies whether RRAS uses the same set of phone numbers for all the subentries in the RRAS entry. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0	Do not use same phone numbers for all subentries in the RRAS entry.
1	Use same phone numbers for all subentries in the RRAS entry.

#### 2.2.2.2.40 GlobalDeviceSettings

This key specifies whether the modem device settings are read from the RRAS entry or not. This key is optional. If the key is present, it is used only if the key **Type** has the value "1" and SHOULD take one of the values in the following table.

Value	Meaning
0	Do not use the modem device settings from the RRAS entry.
1	Use the modem device settings from the RRAS entry.

#### 2.2.2.2.41 PrerequisitePbk

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.42 PrerequisiteEntry

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.43 PreferredPort

This key specifies the name of the preferred port to be used by the RRAS server for the demand-dial connection. This key contains a string. This key is optional. If this key is present its value SHOULD be the same as that of the **Port** key.

#### 2.2.2.2.44 PreferredDevice

This key specifies the name of the preferred device to be used by RRAS server for the demand-dial connection. This key contains a string. This key is optional. If this key is present its value SHOULD be the same as that of the **Device** key.

#### 2.2.2.2.45 PreferredBps

This key specifies the maximum connection speed for a modem, in bits per second, associated with the preferred port. For example, it can be 115200 bits per second. The value of this key SHOULD be a valid modem connection speed in the range 0 to 4294967296. This key is optional. This key is ignored unless the **DEVICE** key is set to "modem".

#### 2.2.2.2.46 PreferredHwFlow

This key specifies whether to enable hardware flow control for the modem associated with the preferred port. This key is optional. If the key is present, it SHOULD take one of the values given in the following table. This key is ignored unless the **DEVICE** key is set to "modem".[<192>](#192)

Value	Meaning
0	Disable hardware flow control.
1	Enable hardware flow control.

#### 2.2.2.2.47 PreferredProtocol

This key specifies whether the modem associated with the preferred port performs a cyclic redundancy check on the inbound and outbound data stream. This key is optional. If the key is present, it SHOULD take one of the values in the following table. This key is ignored unless the **DEVICE** key is set to "modem".<193>

Value	Meaning
0	Do not perform (CRC) error checking.
1	Perform (CRC) error checking.

#### 2.2.2.2.48 PreferredCompression

This key specifies whether to compress the modem-to-modem data stream for the modem associated with the preferred port. This key is optional. If the key is present, it SHOULD take one of the values in the following table. This key is ignored unless the **DEVICE** key is set to "modem".<194>

Value	Meaning
0	Disable hardware compression.
1	Enable hardware compression.

#### 2.2.2.2.49 PreferredSpeaker

The value for this key specifies whether the modem dial tone and connections sounds are heard for modem associated with the preferred port. This key is optional. If the key is present, it SHOULD take one of the values given in the following table. This key is ignored unless the **DEVICE** key is set to "modem".<195>

Value	Meaning
0	Disable modem speaker.
1	Enable modem speaker.

#### 2.2.2.2.50 PreferredMdmProtocol

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.51 PreviewUsePw

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.52 PreviewDomain

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.53 PreviewPhoneNumber

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.54 ShowDialingProgress

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.55 ShowMonitorIconInTaskbar

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.56 CustomAuthKey

This key specifies the Extensible Authentication Protocol (EAP) method type to be used when making a demand-dial connection. This key is optional. If the key is present, it is used only if the **AuthRestrictions** key is configured to negotiate EAP. It SHOULD be an 8-bit ASCII string representation of a decimal number as defined by [\[IANA-EAP\]](#) section 1.2.1.

#### 2.2.2.2.57 CustomAuthData

This key specifies the configuration blob associated with an EAP method. This key is optional. If the key is present, it is used only if **AuthRestrictions** key is configured to negotiate EAP. This key contains data specific to the EAP method specified in the key **CustomAuthKey**.

#### 2.2.2.2.58 AuthRestrictions

This key specifies the authentication protocols configured for the RRAS entry. This key is optional. If the key is present, the value is a decimal number used as a bit field. The bits are defined in the following table.

Bit number (From LSB)	Authentication Protocol	Meaning
4	Password Authentication Protocol (PAP) <a href="#">[RFC1334]</a>	0 – Do not negotiate PAP 1 – Negotiate PAP.
5	Shiva Password Authentication Protocol (SPAP) <a href="#">[RFC1334]</a>	0 – Do not negotiate SPAP. 1 – Negotiate SPAP <a href="#">&lt;196&gt;</a>
6	MD-5 Challenge Handshake Protocol (CHAP) <a href="#">[RFC2433]</a>	0 – Do not negotiate MD5-CHAP. 1 – Negotiate MD5-CHAP.
7	Microsoft Challenge Handshake Protocol Version 1 (MSCHAPv1) <a href="#">[RFC2433]</a>	0 – Do not negotiate MSCHAPv1. 1 – Negotiate MSCHAPv1. <a href="#">&lt;197&gt;</a>
8	Extensible Authentication Protocol (EAP) <a href="#">[RFC2284]</a>	0 – Do not negotiate EAP. 1 – Negotiate EAP.
10	Microsoft Challenge Handshake Protocol Version 2 (MSCHAPv2) <a href="#">[RFC2759]</a>	0 – Do not negotiate MSCHAPv2. 1 – Negotiate MSCHAPv2.
11	Microsoft Challenge Handshake Protocol (Microsoft Windows® 95 operating system compatible MSCHAP)	0 – Do not negotiate MSCHAP Windows 95 compatible. 1 – Negotiate MSCHAP

Bit number (From LSB)	Authentication Protocol	Meaning
		Windows 95 compatible. <a href="#">.&lt;198&gt;</a>

#### 2.2.2.2.59 TypicalAuth

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.60 IpPrioritizeRemote

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.61 IpInterfaceMetric

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.62 fCachedDnsSuffix

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.63 IpHeaderCompression

This key specifies whether the option for IP header compression is enabled on the RRAS entry. This key is optional. If the key is present, it is used only if the key **Type** has the value "1" and SHOULD take one of the values in the following table.

Value	Meaning
0	Disable TCP/IP header compression.
1	Enable TCP/IP header compression.

#### 2.2.2.2.64 IpAddress

This key specifies a static IPv4 address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0.0.0.0	RRAS ignores this key
A valid IPv4 address. For ex: 10.10.10.1	If the key <b>IpAssign</b> has the value "2", RRAS requests the configured IPv4 address for the demand-dial connection when connecting to a remote RRAS endpoint. Otherwise RRAS ignores this key.

#### 2.2.2.2.65 IpDnsAddress

This key specifies a static IPv4 address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0.0.0.0	RRAS ignores this key.
A valid IPv4 address. For ex: 10.10.10.1	If the key <b>IpNameAssign</b> has the value "2", RRAS requests the configured IPv4 address as the primary DNS server address from the remote RRAS endpoint when making a demand-dial connection. Otherwise RRAS ignores this key.

#### 2.2.2.2.66 IpDns2Address

This key specifies a static IPv4 address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0.0.0.0	RRAS ignores this key.
A valid IPv4 address. For ex: 10.10.10.1	If the key <b>IpNameAssign</b> has the value "2", RRAS requests the configured IPv4 address as the secondary DNS server address from the remote RRAS endpoint when making a demand-dial connection. Otherwise RRAS ignores this key.

#### 2.2.2.2.67 IpWinsAddress

This key specifies a static IPv4 address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0.0.0.0	RRAS ignores this key.
A valid IPv4 address. For ex: 10.10.10.1	If the key <b>IpNameAssign</b> has the value "2", RRAS requests the configured IPv4 address as the primary WINS server address from the remote RRAS endpoint when making a demand-dial connection. Otherwise RRAS ignores this key.

#### 2.2.2.2.68 IpWins2Address

This key specifies a static IPv4 address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
0.0.0.0	RRAS ignores this key.
A valid IPv4 address such as 10.10.10.1	If the key <b>IpNameAssign</b> has the value "2", RRAS requests the configured IPv4 address as the secondary WINS server address from the remote RRAS endpoint when making a demand-dial connection. Otherwise RRAS ignores this key.



### 2.2.2.2.69 IpAssign

This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
1	RRAS when making a demand-dial connection does not request a specific IPv4 address from the remote RRAS endpoint.
2	RRAS requests a specific IPv4 address as specified by the value of the key <b>IpAddress</b> for the demand-dial connection when connecting to a remote RRAS endpoint.

### 2.2.2.2.70 IpNameAssign

This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
1	RRAS, when making a demand-dial connection, does not request a specific IPv4 address for the DNS and WINS servers from the remote RRAS endpoint.
2	RRAS, when making a demand-dial connection, requests a specific IPv4 DNS and WINS server's address as specified in keys <b>IpDnsAddress</b> , <b>IpDns2Address</b> , <b>IpWinsAddress</b> , and <b>IpWins2Address</b> respectively from a remote RRAS endpoint.
3	Same as the value 1.

### 2.2.2.2.71 IpFrameSize

This key is optional and if present MUST be ignored by RRAS.

### 2.2.2.2.72 IpDnsFlags

This key specifies the DNS configuration settings on the RRAS entry. The value is a decimal number used as a bit field. The bits are defined as in the following table.

Bit number (From LSB)	DNS flag	Meaning
0	This bit determines whether RRAS registers IPv4 and IPv6 addresses for the demand-dial connection with DNS server.	0 – Do not register with DNS. 1 – Register with DNS.
1	This bit specifies whether RRAS registers DNS suffixes specified as the value of the key <b>IpDnsSuffix</b> in the RRAS entry with the DNS server.	0 – Do not register DNS suffix with DNS. 1 – Register DNS suffix with DNS.
2	This bit specifies whether RRAS registers DNS suffixes obtained when making a demand-dial connection with the DNS server.	0 – Do not register DNS suffix with DNS. 1 – Register DNS suffix with DNS.

#### 2.2.2.2.73 IpNBTFlags

This key specifies whether the option for **NetBT** is enabled on the RRAS entry. This key is optional. If the key is present, it SHOULD be set either to "0" or "1". The meaning of these values is implementation-specific. [<199>](#)

#### 2.2.2.2.74 TcpWindowSize

This key specifies the TCP window size for all TCP sessions created over the demand-dial connection. This key is optional. If the key is present, it SHOULD be set to a decimal number in the range 0 to 1073725440. [<200>](#)

#### 2.2.2.2.75 UseFlags

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.76 IpSecFlags

This key specifies if a pre-shared key is configured on the RRAS entry. This key is optional. If the key is present, it is used only if **Type** is "2" and the demand-dial connection is made using L2TP. It SHOULD take one of the following values.

Value	Meaning
0	No pre-shared key configured for the RRAS entry
1	Pre-shared key configured for the RRAS entry

#### 2.2.2.2.77 IpDnsSuffix

This key specifies the DNS suffix configured for the RRAS entry. The key is optional; if present, it is used only if the **IpDnsFlags** key is configured to use it. This key SHOULD be in the domain name (3) format.

#### 2.2.2.2.78 IpCachedDnsSuffix

This key is optional and if present is ignored by RRAS.

#### 2.2.2.2.79 Ipv6Assign

This key is optional. If the key is present, it SHOULD take one of the values in the following table. [<201>](#)

Value	Meaning
1	RRAS when making a demand-dial connection does not request a specific IPv6 address from the remote RRAS endpoint.
2	RRAS requests a specific IPv4 address as specified as the value for the keys <b>Ipv6PrefixLength</b> and <b>Ipv6Address</b> for the demand-dial connection when connecting to a remote RRAS endpoint.

#### 2.2.2.2.80 Ipv6PrefixLength

This key specifies a static IPv6 prefix length configured for the RRAS entry. RRAS requests the configured prefix length when making a demand-dial connection to the remote RRAS endpoint. This key is optional. If the key is present, it SHOULD be a decimal number in the range 0 to 128.<202>

#### 2.2.2.2.81 Ipv6PrioritizeRemote

This key is optional and if present is ignored by RRAS.

#### 2.2.2.2.82 Ipv6InterfaceMetric

This key is optional and if present is ignored by RRAS.

#### 2.2.2.2.83 Ipv6NameAssign

This key is optional. If the key is present, it SHOULD take one of the values in the following table.

Value	Meaning
1	RRAS when making a demand-dial connection does not request a specific IPv6 address for the DNS servers from the remote RRAS endpoint.
2	RRAS when making a demand-dial connection requests a specific IPv6 DNS server addresses as specified in keys <b>Ipv6DnsAddress</b> and <b>Ipv6Dns2Address</b> from a remote RRAS endpoint.

#### 2.2.2.2.84 Ipv6DnsAddress

This key specifies a static primary IPv6 DNS server address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.<203>

Value	Meaning
::	RRAS ignores this key.
A valid IPv6 address. For example: 3ffe::1	If the key Ipv6NameAssign has the value "2", RRAS requests the configured IPv6 address as the primary DNS server address from the remote RRAS endpoint when making a demand-dial connection. Otherwise RRAS ignores this key.

#### 2.2.2.2.85 Ipv6Dns2Address

This key specifies a static secondary IPv6 DNS server address. This key is optional. If the key is present, it SHOULD take one of the values in the following table.<204>

Value	Meaning
::	RRAS ignores this key.
A valid IPv6 address. For example: 3ffe::1	If the key <b>Ipv6NameAssign</b> has the value "2", RRAS requests the configured IPv6 address as the secondary DNS server address from the remote RRAS endpoint when making a demand-dial connection. Otherwise RRAS ignores this key.

#### **2.2.2.2.86 Ipv6Prefix**

This key specifies a 64-bit prefix length of the IPv6 address of the demand-dial connection. This key is optional. This key SHOULD be initialized to 0000000000000000 and MUST be ignored on receipt. When RRAS connects to a remote RRAS endpoint, the prefix length for the IPv6 address of the demand-dial connection is cached as a value for this key. [<205>](#205)

#### **2.2.2.2.87 Ipv6InterfaceId**

This key specifies a 64-bit interface identifier for the IPv6 address of the demand-dial connection. This key is optional. This key SHOULD be initialized to 0000000000000000 and MUST be ignored on receipt. When RRAS connects to a remote RRAS endpoint, the interface identifier for the IPv6 address of the demand-dial connection is cached as a value for this key. [<206>](#206)

#### **2.2.2.2.88 DisableClassBasedDefaultRoute**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.89 DisableMobility**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.90 NetworkOutageTime**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.91 ProvisionType**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.92 PreSharedKey**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.93 NETCOMPONENTS**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.94 ms\_msclient**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.95 ms\_server**

This key is optional and if present is ignored by RRAS.

#### **2.2.2.2.96 MEDIA**

This **key** specifies the name of the media. This is also the beginning of the MEDIA RRAS Entry subsection (henceforth called MEDIA subsection). A MEDIA subsection can contain one or more **DEVICE** RRAS Entry subsections (section [2.2.2.2.100](#2.2.2.2.100)). For a Multilink phonebook entry there are multiple **MEDIA** subsections, where each subsection corresponds to a physical device. All the keys in the RRAS phonebook entry starting from the MEDIA key until the beginning of another MEDIA subsection, or another **RRAS entry** or the end of RRAS phonebook file are part of a MEDIA

subsection. This key **MUST** be present and it is case sensitive. This key **SHOULD** take one of the string values given in the following table.

String	Meaning
Isdn	The device type is isdn.
x25	The device type is x25.
Serial	The device type is modem, pad, or switch.
Rastapi	For other device types.

If the key is absent, the demand-dial connection cannot be made for this RRAS entry.

#### 2.2.2.2.97 Port

This key specifies the name of the port to be used by RRAS server for the demand-dial connection. This key is a string. This key **MUST** be present. In case the key is not present, RRAS will discard this RRAS entry. [<207>](#207)

#### 2.2.2.2.98 Device

This key specifies the name of the device to be used by the RRAS server for the demand-dial connection. This key contains a string. This key is optional.

#### 2.2.2.2.99 ConnectBPS

This key specifies the maximum connection speed for a modem, in bits per second. An example speed would be 115200 bits per second. The value of this key **SHOULD** take a valid modem connection speed in the range 0 to 4294967296. This key is optional. This key is ignored unless the **DEVICE** key is set to "modem".

#### 2.2.2.2.100 DEVICE

This key specifies the name of the device type associated with a port. This key **MUST** be present and it is case sensitive. This key **MUST** take one of the string values given in the following table.

String	Meaning
Modem	A modem accessed through a COM port.
Isdn	An ISDN card.
X25	An X.25 card.
Vpn	A virtual private network connection.
Pad	A Packet Assembler/Disassembler.
Generic	Generic.
FrameRelay	Frame Relay.
Atm	Asynchronous Transfer Mode (ATM).

String	Meaning
Sonet	Sonet.
SW56	Switched 56K Access.
Irda	Infrared Data Association (IrDA) compliant device.
PPPoE	Point-to-Point Protocol over Ethernet.
Switch	A pre-connect switch or post-connect switch.
Rastap	For other devices. This is allowed only if the MEDIA key is Rastapi.
Serial	A serial device.

This key is also the beginning of DEVICE RRAS entry subsection (henceforth called DEVICE subsection). There can be multiple DEVICE subsections within a single **MEDIA** subsection. For serial media, there can be one to four DEVICE subsections, representing a pre-connect switch, modem, X.25 PAD, and post-connect switch, and MUST appear in the same order within the RRAS phonebook entry. If the switch is used before dialing a connection it is known as a pre-connect switch. If it is used after dialing a connection it is known as post-connect switch. For all other media, there MUST be exactly one DEVICE subsection. If this key is missing, then RRAS will ignore the DEVICE subsection settings.

All the keys in the RRAS phonebook entry (from the DEVICE key to the beginning of another DEVICE subsection, or another MEDIA subsection, or another RRAS entry, or the end of RRAS phonebook file) are part of a DEVICE subsection. Some of the following keys will be relevant only to specific device types. Unless explicitly specified, a key will be applicable to all the device types. If a key is not applicable to a device type it can be absent. [<208>](#208)

#### 2.2.2.2.101 Terminal

This key specifies whether to use a **Terminal window** for dialup connections. For example, before connecting to the remote server, a terminal window opens in which the user can type modem setup commands and view the modem's responses. This key is ignored unless the **DEVICE** key is set to "switch". This key is optional. If the key is present, it SHOULD be used only with a pre-connect switch and SHOULD take one of the values given in the following table. [<209>](#209)

Value	Meaning
0	Do not display Terminal window for user input.
1	Display Terminal window for user input.

#### 2.2.2.2.102 Name

This key specifies the name of the path of the custom script file that the RRAS server executes during the demand dial connection. This key is ignored unless the **DEVICE** key is set to "switch". This key is optional. If the key is present, it SHOULD be used only with a post-connect switch.

### 2.2.2.2.103 Script

This key specifies whether a script can run. This key is ignored unless the **DEVICE** key is set to "switch". This key is optional. If the key is present, it SHOULD be used only with a post-connect switch and SHOULD take one of the values given in the following table.

Value	Meaning
0	Do not run the script.
1	Run the script.

### 2.2.2.2.104 X25Pad

This key identifies the X.25 PAD type. This key contains a string. This key is ignored unless the **DEVICE** key is set to "Pad". This key SHOULD be present with a valid X.25 PAD type for making a X.25 demand dial connection. [<210>](#)

### 2.2.2.2.105 X25Address

This key identifies the X.25 address to which to connect. This key contains a string. This key is ignored unless the **DEVICE** key is set to "Pad" or "X25". This key SHOULD be present with a valid X.25 address for making a X.25 demand dial connection. [<211>](#)

### 2.2.2.2.106 UserData

This key specifies additional connection information supplied to the X.25 host at connection time. This key contains a string. The value for this key is ignored if the **X25Address** key is empty. This key is ignored unless the **DEVICE** key is set to "Pad" or "X25". This key is optional. [<212>](#)

### 2.2.2.2.107 Facilities

This key specifies the facilities to request from the X.25 host at connection time. For example, some providers support **/R** to specify reverse charging. The value of this key is ignored if the value is not an **X25Address** key. This key contains a string. This key is ignored unless the **DEVICE** key is set to "Pad" or "X25". This key is optional. [<213>](#)

### 2.2.2.2.108 PhoneNumber

This key specifies a device-type specific destination string to dial a connection. This key is ignored if the **DEVICE** key is set to "Pad", "X25" or "Switch". This key contains a string. This key SHOULD be present with a valid value for making a demand dial connection. This key is optional if the **Type** key is set to "5". The following table describes the contents of the **PhoneNumber** key for various device types.

DEVICE	PhoneNumber
Modem	Telephone number <a href="#">[E164]</a>
Isdn	Telephone number <a href="#">[E164]</a>
Atm	Virtual Path Identifier (VPI) and Virtual Channel Identifier <a href="#">[RFC2761]</a> (VCI) values of a permanent virtual circuit. Use the following format: p(vpi),(vci)

DEVICE	PhoneNumber
	Example: "P0,40"
PPPoE	Service name <a href="#">[RFC2516]</a>
Vpn	DNS name, IPv4 address, or IPv6 address

There can be one or more phone number subsections within in a DEVICE subsection when the **Type** key is set to "1". The phone number subsection contains the following keys only—**PhoneNumber**, **AreaCode**, **CountryCode**, **CountryID**, **UseDialingRules**, **Comment**, and **FriendlyName**. If there are multiple phone number subsections then the first subsection is for the primary phone number and the others are for the alternate phone numbers.

#### 2.2.2.2.109 AreaCode

This key specifies the telephonic area code. The value of key is ignored unless the **UseDialingRules** key is set to "1". This key is ignored unless the **Type** key is set to "1". This key is also ignored if the **DEVICE** key is set to "Pad", "X25", or "Switch". This key is optional. If the key is present, it SHOULD be a string representation of an area code.

#### 2.2.2.2.110 CountryCode

This key specifies the country/region code portion of the phone number, as specified in [\[OB930E\]](#). The value of the key is ignored unless the **UseDialingRules** key is set to "1". This key is ignored unless the **Type** key is set to "1". This key is also is ignored if the **DEVICE** key is set to "Pad", "X25", or "Switch". This key is optional. If the key is present, it SHOULD be a string representation of a country/region code.

#### 2.2.2.2.111 CountryID

This key specifies the telephony application programming interface (**TAPI**) country/region identifier. The value of the key is ignored unless the **UseDialingRules** key is set to "1". This key is ignored unless the **Type** key is set to "1". This key is also is ignored if the **DEVICE** key is set to "Pad", "X25", or "Switch". This key is optional. If the key is present, it MUST be a string representation of TAPI country/region identifier.

#### 2.2.2.2.112 UseDialingRules

This key specifies whether the **CountryID**, **CountryCode**, **AreaCode** keys and the custom **dialing rules** are used to construct the phone number. This key is ignored unless the **Type** key is set to "1". This key is also is ignored if the **DEVICE** key is set to "Pad", "X25", or "Switch". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Do not use <b>CountryID</b> , <b>CountryCode</b> , <b>AreaCode</b> keys and custom dialing rules.
1	Use <b>CountryID</b> , <b>CountryCode</b> , <b>AreaCode</b> keys and custom dialing rules.

#### 2.2.2.2.113 Comment

This key is optional and if present MUST be ignored by RRAS.



#### 2.2.2.2.114 FriendlyName

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.115 LastSelectedPhone

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.116 PromoteAlternates

This key specifies whether to make the alternate phone number that connects successfully the primary phone number and move the primary phone number to the alternate list. This key is ignored unless the **Type** key is set to "1". It is also ignored if the **DEVICE** key is set to "Pad", "X25", or "Switch". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Do not promote alternate phone numbers.
1	Promote alternate phone numbers.

#### 2.2.2.2.117 TryNextAlternateOnFail

This key specifies whether to dial the alternate phone numbers when the primary phone number fails to connect to the remote RRAS server. This key is ignored unless the **Type** key is set to "1". It is also ignored if the **DEVICE** key is set to "Pad", "X25", or "Switch". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Do not try next alternate phone number on fail.
1	Try next alternate phone number on fail.

#### 2.2.2.2.118 HwFlowControl

This key specifies whether to enable hardware flow control for the modem. This key is ignored unless the **DEVICE** key is set to "modem". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Disable hardware flow control.
1	Enable hardware flow control.

#### 2.2.2.2.119 Protocol

This key specifies whether the modem performs cyclic redundancy checks on the inbound and outbound data stream. This key is ignored unless the **DEVICE** key is set to "modem".

This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Do not perform (CRC) error checking.
1	Perform (CRC) error checking.

#### 2.2.2.2.120 Compression

This key specifies whether to compress the modem-to-modem data stream. This key is ignored unless the **DEVICE** key is set to "modem". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Disable hardware compression.
1	Enable hardware compression.

#### 2.2.2.2.121 Speaker

This key specifies whether the modem dial tone and connection sounds are heard. This key is ignored unless the **DEVICE** key is set to "modem". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Disable modem speaker.
1	Enable modem speaker.

#### 2.2.2.2.122 MdmProtocol

This key is optional and if present MUST be ignored by RRAS.

#### 2.2.2.2.123 LineType

This key specifies the type of ISDN line. This key is ignored unless the **DEVICE** key is set to "Isdn". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	64K Digital (highest quality)
1	56K Digital
2	56K Analog (lowest quality)

#### 2.2.2.2.124 Fallback

This key instructs RRAS to communicate at the selected line type but to negotiate a lower quality line type if necessary. This negotiation depends on the condition of the ISDN line (for example, noise on the line affects negotiation). This key is ignored unless the **DEVICE** key is set to "Isdn".

This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Do not Negotiate Line Type.
1	Negotiate Line Type.

#### 2.2.2.2.125 EnableCompression

This key specifies whether an ISDN card will compress the data before transmitting. The value of this key is ignored unless the **Proprietary** flag is set to "1". This key is ignored unless the **DEVICE** key is set to "Isdn". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Disable hardware compression.
1	Enable hardware compression.

#### 2.2.2.2.126 ChannelAggregation

This key specifies the number of ISDN channels. The value of this key is ignored unless the **Proprietary** flag is set to "1". This key is ignored unless the **DEVICE** key is set to "Isdn". This key is optional. If the key is present, it SHOULD take values ranging from 1 to 999999999 only.

#### 2.2.2.2.127 Proprietary

This key specifies whether the keys **EnableCompression** and **ChannelAggregation** are ignored. This key is ignored unless the **DEVICE** key is set to "Isdn". This key is optional. If the key is present, it SHOULD take one of the values given in the following table.

Value	Meaning
0	Ignore <b>EnableCompression</b> and <b>ChannelAggregation</b> flags.
1	Do not ignore <b>EnableCompression</b> and <b>ChannelAggregation</b> flags.

### 2.2.3 Registry Keys

The following are the various registry keys that can be configured on the RRAS server to control RRAS server behavior. [<214>](#) These registry configurations can be performed remotely, by using the [\[MS-RRP\]](#) protocol. RRAS reads these registry values during the initialization process, and uses the registry values to initialize RRASM as specified in section [3.1.1](#).

#### 2.2.3.1 Transport Configuration

The various transport-specific generic configurations that are not associated with any particular interface MUST be stored under the registry key

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\RouterManagers

Under this key, there MUST be one registry key per transport with the name denoting the transport itself. Each name MUST be either of the values IP, IPv6, [215](#) or IPX. [216](#) For example, the IPv4 transport configuration will be specified under the registry key

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\RouterManagers\IP

The registry values defined under these keys are given in the following sections.

#### 2.2.3.1.1 ProtocolId

This value MUST be defined for each supported transport. This registry value MUST be of type REG\_DWORD. This represents the numeric protocol identifier corresponding to the transport protocol name.

Transport Name	ProtocolId Value
IP	0x00000021
IPv6	0x00000057
IPX	0x0000002b

#### 2.2.3.1.2 GlobalInfo

This value SHOULD be defined for each transport supported. This registry value when defined MUST be of type REG\_BINARY. This represents the global transport configuration and any specific global information for the various routing protocols and configuration that might be supported for the specific transport. The contents of this registry value MUST be in the form of RTR\_INFO\_BLOCK\_HEADER as described in section [2.2.1.2.3](#).

#### 2.2.3.1.3 GlobalInterfaceInfo

This value SHOULD be defined for each transport supported. [217](#) This registry value when defined MUST be of type REG\_BINARY. This represents the default configuration that will be applied for each interface that is added to the specific transport. In the absence of per-interface transport configuration, this will be the configuration applied on the interface. The contents of this registry value MUST be in the form of RTR\_INFO\_BLOCK\_HEADER as described in section [2.2.1.2.3](#).

#### 2.2.3.2 Interface Configuration

The interfaces that are present on the RRAS server MUST be stored under the registry key

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces

with each subkey representing the configuration information pertaining to one interface. The subkeys MUST be named with a 0-based index in a monotonically increasing order. For example if there are 3 interfaces in the system, the registry keys will be as follows.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces\0

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces\1

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces\2

Under each interface-specific registry key, there SHOULD be transport-specific subkeys that contain the interface-specific configuration information pertaining to the transport. For example, the IPv4

transport-specific information for an interface with index 4 will be stored under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces\4\IP.

#### **2.2.3.2.1 Common Interface Configuration Values**

These are the registry values that define the common properties of an interface.

##### **2.2.3.2.1.1 InterfaceName**

For each interface, InterfaceName MUST be specified. This MUST be of type REG\_SZ and MUST be a null-terminated string. This represents the name of the interface.

##### **2.2.3.2.1.2 Type**

For each interface, Type MUST be specified. This MUST be of type REG\_DWORD. This represents the type of the interface. The value for this MUST be as defined in the [ROUTER\\_INTERFACE\\_TYPE \(section 2.2.1.1.1\)](#).

##### **2.2.3.2.1.3 Enabled**

For each interface, Enabled SHOULD be specified. This MUST be of type REG\_DWORD. This represents whether the interface is enabled or not. The value MUST be either 0 or 1. A value of 0 MUST be interpreted as the interface is disabled and a value of 1 MUST be used to indicate the interface is enabled. If the value is not specified, it MUST be treated as the interface is enabled (1).

##### **2.2.3.2.1.4 DialOutHours**

This is applicable only for interfaces of type ROUTER\_IF\_TYPE\_HOME\_ROUTER or ROUTER\_IF\_TYPE\_FULL\_ROUTER. This SHOULD be used to specify the dialing restrictions for the demand dial interfaces. This represents the times during which the dialing and connecting of the demand dial interface is allowed. This MUST be of type REG\_MULTI\_SZ as specified in [\[MS-RRP\]](#) section 2.2.6. It MUST be specified in the following format: <day><space><time range> <time range>...\0<day><space><time range>\0\0

where

<day> is a numeral that corresponds to the day of the week starting with 1 representing Monday.

<space> is the literal corresponding to one blank space.

<time range> represents the dialing hours allowed during the particular <day> and is represented in the form "HH:MM-HH:MM" using 24-hour notation.

There can be a number of time ranges within a single day and each day's dialing hours is separated by a \0. The last of the dialing information is followed by an additional \0 as defined for REG\_MULTI\_SZ.

#### **2.2.3.2.2 Transport-specific Configuration**

The following are the registry values that can be configured for a given interface, and which represent transport and routing protocol-specific configuration for the interface.

#### 2.2.3.2.2.1 ProtocolId

This is similar to the ProtocolId as described in ProtocolId 2.4.1.2. The protocolId MUST be the value corresponding to the transport protocol subkey for which the interface information is being specified.

#### 2.2.3.2.2.2 InterfaceInfo

This value MUST be used to specify the transport-specific configuration for the interface. This also includes the various routing protocol configurations applicable to the specific transport. This MUST be of type REG\_BINARY. The contents of this registry value MUST be in the form of RTR\_INFO\_BLOCK\_HEADER as specified in section [2.2.1.2.3](#).

### 2.2.3.3 Ports Configuration

An RRAS server implementation can support a number of device types for remote access requirements. Each device type can be configured with a number of ports as well as the usage of the ports.

#### 2.2.3.3.1 Non-modem Device Port Configurations

The port configuration for various device types given in the following table MUST be stored under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}.

The device types for which the configuration information is stored here are PPTP, L2TP, SSTP, IKEv2, and PPPoE. This registry MUST include subkeys that are numbered from 000 and monotonically increasing. Under each subkey, the value ComponentId MUST be used to denote the protocol for which the (numbered) key has the configuration information. The following table specifies the ComponentId value and the protocol the configuration corresponds to.

ComponentId Value	Device Type	Driver Description
ms_sstpminiport	SSTP	WAN Miniport (SSTP)
ms_agilevpnminiport	IKEv2	WAN Miniport (IKEv2)
ms_l2tpminiport	L2TP	WAN Miniport (L2TP)
ms_pptpminiport	PPTP	WAN Miniport (PPTP)
ms_pppoemiport	PPPoE	WAN Miniport (PPPoE)
ms_ptimiport	Direct Parallel Connection	Direct Parallel

For example, if the subkey having name 008 has ms\_sstpminiport as the ComponentId value, the registry path storing SSTP information will be HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0008.

##### 2.2.3.3.1.1 ComponentId

This value specifies the protocol for which the key (under which the value is defined) comprises the configuration information. The value for this name MUST be one of the values mentioned in the preceding table. This value MUST be of type REG\_SZ. This value MUST be null-terminated.

#### **2.2.3.3.1.2 DriverDesc**

This value specifies the name of the device. This value MUST be of type REG\_SZ. If this value is not specified, the device MUST be considered as an invalid device for routing and remote access.

#### **2.2.3.3.1.3 EnableForOutboundRouting**

This value MUST be used to specify whether the ports of the device type can be used for outbound demand dial interface connections. This value MUST be of type REG\_DWORD. This MUST be configured with a value of either 0 or 1. The value 0 MUST be interpreted as the device type is not enabled for outbound routing. The value 1 MUST be interpreted as the device type is enabled for outbound routing.

#### **2.2.3.3.1.4 EnableForRas**

This value MUST be used to specify whether or not the ports for the device type can be used for remote access. This value MUST be of type REG\_DWORD. This MUST be configured with a value of either 0 or 1. The value 0 MUST be interpreted as the device type is not enabled for remote access, and a value of 1 MUST be interpreted as the device type is enabled for remote access.

#### **2.2.3.3.1.5 EnableForRouting**

This value MUST be used to indicate whether the ports for the device type can be used for demand dial (or site-to-site) connectivity. This value MUST be of type REG\_DWORD. This MUST be configured with a value of 0 if the device type has to be disabled for demand dial usage and MUST be configured with a value of 1 if the device type has to be enabled for demand dial usage.

#### **2.2.3.3.1.6 CalledIDInformation**

This value SHOULD be used to specify the phone number of the device to be passed to the client as the called station ID in Bandwidth Allocation Protocol (BAP)-enabled connections. This MUST be of type REG\_MULTI\_SZ as specified in [\[MS-RRP\]](#) section 2.2.6. Each string in the REG\_MULTI\_SZ represents one phone number. For VPN device types where a phone number is not applicable, this SHOULD be the IP address of the server configured as the called ID.

#### **2.2.3.3.1.7 MaxWanEndpoints**

This value MUST be used to specify the maximum number of endpoints or ports that the device type can support. This MUST be of type REG\_DWORD and can take any valid 32-bit integer value.

#### **2.2.3.3.1.8 WanEndpoints**

This value MUST be used to specify the number of endpoints or ports that the device type is configured with. This MUST be of type REG\_DWORD and can take any valid 32-bit integer as its value. It MUST be lesser than or equal to MaxWanEndpoints value.

#### **2.2.3.3.2 Modem device Port Configurations**

The modem devices can be used for dial-up networking. The modem devices that are present on the RRAS server MUST be registered under the registry key  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E96D-E325-11CE-BFC1-08002BE10318}.

Under this registry key, for each modem, the modem-specific information MUST be present under its own subkey. The subkey MUST be a monotonically increasing number starting with 0000. For

example, HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E96D-E325-11CE-BFC1-08002BE10318}\0005 can be the subkey under which modem device information is present. Under this registry key, the value FriendlyName MUST be defined to specify the friendly name for the particular modem device. This MUST be of type REG\_SZ, which comprises the friendly name for the modem device. This value MUST be null-terminated.

The device usage configuration itself MUST be present under the subkey Clients\Ras. For example, if HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E96D-E325-11CE-BFC1-08002BE10318}\0005 represents a valid modem device information, the device usage information will be present in the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E96D-E325-11CE-BFC1-08002BE10318}\0005\Clients\Ras key. The registry values, EnableForOutboundRouting, EnableForRas, EnableForRouting, and CalledIDInformation specify the device usage and these values are the same as described in sections [2.2.3.3.1.3](#), [2.2.3.3.1.4](#), [2.2.3.3.1.5](#), and [2.2.3.3.1.6](#) respectively.

## 2.2.3.4 Miscellaneous Configuration Information

These registry keys specify information relevant for the RRAS server configuration that does not fall under the previous categories.

### 2.2.3.4.1 RouterType

This defines the mode in which the RRAS server needs to be running. This MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters. This MUST be of type REG\_DWORD. This MUST be a combination of the following flag values.

Flag Value	Description
ROUTER_TYPE_RAS 0x00000001	RRAS is enabled for remote access connections providing connectivity using IPv4 protocol as transport.
ROUTER_TYPE_LAN 0x00000002	RRAS is enabled for IPv4 routing over Ethernet interfaces only.
ROUTER_TYPE_WAN 0x00000004	RRAS is enabled for IPv4 routing over Ethernet as well as demand dial interfaces.
IPV6_ROUTER_TYPE_RAS 0x00000008	RRAS is enabled for remote access connections providing connectivity using IPv6 protocol as transport.
IPV6_ROUTER_TYPE_LAN 0x00000010	RRAS is enabled for IPv6 routing over Ethernet interfaces only.
IPV6_ROUTER_TYPE_WAN 0x00000020	RRAS is enabled for IPv6 routing over Ethernet as well as demand dial interfaces.

### 2.2.3.4.2 IKEv2 Tunnel Configuration Settings

IKEv2 tunnel configuration settings MUST be stored under the registry path HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\IKEV2.



#### 2.2.3.4.2.1 idleTimeout

This value specifies the idle Timeout value in seconds to be used with IKEv2 protocol. This MUST be of type REG\_DWORD. This is the duration in seconds after which the connection will be disconnected if there is no traffic. This value MUST be at least 300 and have a maximum supported value of 17,279,999.

#### 2.2.3.4.2.2 networkBlackoutTime

This value specifies the retransmission timeout value in seconds to be used with IKEv2 protocol. This MUST be of type REG\_DWORD. This value MUST be greater than or equal to 120 seconds.

#### 2.2.3.4.2.3 saDataSize

This value specifies the life time of the security association (SA) for IKEv2 [\[RFC4306\]](#) in terms of the data transfer size in kilobytes, after which the SA has to be renegotiated. This value MUST be of type REG\_DWORD. This value MUST be at least 1024.

#### 2.2.3.4.2.4 saLifeTime

This value specifies the life time of the security association for IKEv2 [\[RFC4306\]](#) in seconds after which the SA has to be renegotiated. This value MUST be of type REG\_DWORD. This value MUST be at least 300 seconds.

#### 2.2.3.4.2.5 TrustedRootCert

This is a registry value specifying the subject name of the certificate that will be trusted by the server for IKEv2 certificate authentication. This value MUST be of type REG\_BINARY. The value itself is the binary representation of the subject name of the **certificate**. This registry value is defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\IKEV2\AllowedTrustedRootCerts\nnnn, where nnnn is a monotonically increasing number starting with 0000 with each such entry representing a unique trusted root certificate to be supported for IKEv2 peer authentication.

#### 2.2.3.4.3 SSTP Tunnel Configuration Settings

SSTP Tunnel configuration settings MUST be stored in the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\SstpSvc\Parameters.

##### 2.2.3.4.3.1 UseHttps

This value specifies whether the SSTP should be using HTTP or HTTPS as the underlying transport. This value MUST be of type REG\_DWORD. The valid values for this are 0 and 1. A value 0 implies the use of HTTP transport and 1 implies the use of HTTPS transport. If the value not specified, a default usage of HTTPS (value 1) MUST be assumed.

##### 2.2.3.4.3.2 IsHashConfiguredByAdmin

This value specifies whether the SSTP certificate hash values are configured by the administrator, or if the RRAS server should choose a certificate hash on its own automatically. This value MUST be of type REG\_DWORD. The valid values for this are 0 and 1. A value 0 implies automatic certificate configuration and 1 implies the certificate was configured by the administrator. If the value is not

specified for this registry value, or if this registry value is not present, the default setting of automatic certificate configuration is assumed.

#### 2.2.3.4.3.3 SHA256CertificateHash

This value specifies the SHA 256 hash of the X.509 certificate to be used with SSTP. This value MUST be of type REG\_BINARY. It MUST be of length 32 bytes. This registry value is used only if the registry value [IsHashConfiguredByAdmin](#) is present with the value of 1; otherwise, this value is ignored.

#### 2.2.3.4.3.4 SHA1CertificateHash

This value specifies the SHA1 hash of the X.509 certificate to be used with SSTP. This value MUST be of type REG\_BINARY. It MUST be of length 20 bytes. This registry value is used only if the registry value [IsHashConfiguredByAdmin](#) is present with the value of 1; otherwise, this value is ignored.

#### 2.2.3.4.4 QuarantineInstalled

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This represents whether Quarantine Service [\[MSFT-NAQC\]](#) is installed or not. A value 0 SHOULD be used to denote that quarantine service is not installed and a value 1 SHOULD be used to denote that quarantine service is installed.

#### 2.2.3.4.5 LoggingFlags

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters. This MUST be of type REG\_DWORD. This SHOULD be from 0 to 3. This represents the logging level for events for the RRAS server.

Value	Description
0x00000000	Logging SHOULD be disabled.
0x00000001	Log all the error category events only.
0x00000002	Log all the warning and error category events only.
0x00000003	Log all the informational, warning, and error category events.

#### 2.2.3.4.6 ServerFlags

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters. This MUST be of type REG\_DWORD. This SHOULD be a combination of the various flag values given in the following table. This specifies a number of configuration settings for the RRAS server implementation.

Value	Description
0x00000001	This specifies that for Callback Control Protocol (CBCP) <a href="#">[RFC1570]</a> in PPP, there needs to be a delay before the RRAS server performs the actual callback.

Value	Description
0x00000002	Use the Microsoft Point-to-Point Compression (MPPC) protocol to compress data sent on the remote access or demand dial connections.
0x00000004	NetBEUI Framing is enabled.
0x00000008	RRAS server is enabled for IPv4 traffic to be tunneled.
0x00000010	RRAS server is enabled for IPX traffic to be tunneled.
0x00000020	RRAS server is enabled for AppleTalk protocol traffic to be tunneled.
0x00000040	Shiva Password Authentication Protocol (SPAP) can be negotiated for remote access and demand dial connection authentication.
0x00000080	Packets between the WAN endpoints should be encrypted.
0x00000100	MSCHAP protocol can be negotiated for remote access and demand dial connection authentication.
0x00000200	The use of LCP extensions as defined in <a href="#">[RFC1570]</a> is allowed.
0x00000400	Multilink negotiation <a href="#">[RFC1990]</a> is allowed for remote access and demand dial connections.
0x00000800	PPP peer needs to be authentication.
0x00001000	Packets between WAN endpoints should be encrypted using the strongest possible algorithm. The exact algorithm is RRAS implementation-dependent.
0x00002000	Bandwidth Allocation Control Protocol (BACP) <a href="#">[RFC2125]</a> is allowed for remote access connections.
0x00004000	Remote access connections without authentication are allowed on the RRAS server.
0x00008000	EAP protocol can be negotiated for remote access and demand dial connection authentication.
0x00010000	Password Authentication Protocol (PAP) <a href="#">[RFC1334]</a> can be negotiated for remote access and demand dial connection authentication.
0x00020000	MD5-CHAP <a href="#">[RFC1994]</a> can be negotiated for remote access and demand dial connection authentication.
0x00040000	IPsec needs to be negotiated for L2TP <a href="#">[MS-L2TPIE]</a> tunnel type connections.
0x00080000	Packets between WAN endpoints may be unencrypted.
0x00100000	MOBIKE <a href="#">[RFC4555]</a> extension support is not allowed for IKEv2 remote access connections.
0x00200000	Use of LAN Manager passwords <a href="#">[RFC2433]</a> is allowed for remote access and demand dial connection authentication.
0x00400000	Connections to the RRAS server using directly connected serial ports may be accepted without authentication.
0x00800000	MSCHAPv2 <a href="#">[MS-CHAP]</a> can be negotiated for remote access and demand dial connection authentication.
0x01000000	Callback functionality using CBCP <a href="#">[RFC1570]</a> is enabled.

Value	Description
0x02000000	Machine authentication is allowed on the RRAS server.
0x04000000	Authentication using certificates is allowed on the RRAS server.
0x08000000	RRAS server is enabled for IPv6 traffic to be tunneled.
0x10000000	Preshared key can be used for authentication using L2TP over IPsec [MS-L2TP-IE].

#### 2.2.3.4.7 ConfigurationFlags

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This specifies whether the RRAS functionality is enabled or not. A value 0 SHOULD be used to specify that RRAS is disabled and a value 1 SHOULD be used to denote that RRAS is enabled.

#### 2.2.3.4.8 AllowNetworkAccess

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip or HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ipv6 based on whether it is specifying the setting for IPv4 or IPv6. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This specifies whether RRAS can route packets between interfaces or not. A value of 0 SHOULD be used to specify that routing should not be allowed and a value of 1 SHOULD be used to specify that routing should be allowed.

#### 2.2.3.4.9 EnableIn

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip or HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ipv6 based on whether it is specifying the setting for IPv4 or IPv6. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This specifies whether remote access is enabled for the specific protocol (IPv4 or IPv6) or not. A value of 0 SHOULD be used to specify that remote access is not enabled for the data traffic and a value of 1 SHOULD be used to specify that the remote access is enabled for the data traffic.

#### 2.2.3.4.10 EnableNetbtBcastFwd

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip or HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ipv6 based on whether it is specifying the setting for IPv4 or IPv6. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This specifies whether remote access clients can use NETBIOS over TCP/IP (NETBT) [\[RFC1002\]](#) to perform broadcast name resolution or not. A value of 0 SHOULD be used to specify that this service is disabled and a value of 1 SHOULD be used to specify that this service is enabled.

#### 2.2.3.4.11 IpAddress

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip. This MUST be of type REG\_SZ. This specifies a valid IPv4 address in dotted notation which along with

IpMask specifies the static address pool to be used to configure remote access clients and demand dial peers. This registry value specifies the static address range if the [StaticAddressPool](#) registry is not configured.

#### **2.2.3.4.12 IpMask**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip. This MUST be of type REG\_SZ. This specifies a valid IPv4 address mask in dotted notation specifying the subnet mask or the prefix which along with IpAddress specifies the static address pool to be used to configure remote access clients and demand dial peers; see [RFC950](#). This registry value specifies the static address range if [StaticAddressPool](#) registry is not configured.

#### **2.2.3.4.13 NetworkAdapterGUID**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip. This MUST be of type REG\_SZ. This specifies the GUID associated with the adapter that should be used to obtain IP addresses, the DNS and WINS servers to be assigned to the remote access, and demand dial IPv4 remote endpoints.

#### **2.2.3.4.14 UseDhcpAddressing**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This specifies whether the RRAS server should use a DHCP server to obtain IP addresses to be assigned for remote access and demand dial connections. A value of 0 SHOULD be used to specify that IP addresses for IPv4 should be assigned from the static IP address pool. A value of 1 SHOULD be used to specify that IP addresses for IPv4 should be obtained from a DHCP server.

#### **2.2.3.4.15 StaticAddressPool**

This registry subkey MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip. This in turn MUST comprise of subkeys numbered from 0, with each subkey specifying the values that form a static address range. For example, there can be a registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip\StaticAddressPool\0 which provides one static IPv4 address range to be used to assign IPv4 addresses to remote access and demand dial interfaces.

Each range MUST be specified using the values "From" and "To". These values MUST be of type REG\_DWORD. The "From" value MUST specify the starting of the IPv4 address range and the "To" value MUST specify the ending of the IPv4 address range.

#### **2.2.3.4.16 AdvertiseDefaultRoute**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ipv6. This MUST be of type REG\_DWORD. This SHOULD be either 0 or 1. This specifies whether the default route should be advertised over IPv6 router advertisement for remote access or demand dial based tunnels. A value of 0 SHOULD be used to specify that the default route should not be advertised and a value of 1 SHOULD be used to specify that the default route should be advertised.

#### 2.2.3.4.17 StaticPrefixPool

This key MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ipv6. There MUST be a subkey for each IPv6 prefix and the subkey SHOULD be numbered from 0. For example, the registry path for an IPv6 prefix could be HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ipv6\StaticPrefixPool\0. Under this subkey, the values "From" and "To" MUST be defined of type REG\_BINARY which specify the prefix to be used for IPv6 as a 16 byte value.

#### 2.2.3.4.18 Accounting Settings

The accounting settings for the RRAS server SHOULD be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Accounting.

##### 2.2.3.4.18.1 AcctGroupName

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Accounting. This value MUST be of type REG\_SZ. This specifies the name of the RADIUS server or server group that provides accounting.

##### 2.2.3.4.18.2 ActiveProvider

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Accounting\Providers. This MUST be of type REG\_SZ. This defines a GUID corresponding to the current accounting provider. This SHOULD be either {1AA7F846-C7F5-11D0-A376-00C04FC9DA04} to specify the default accounting provider, or {1AA7F840-C7F5-11D0-A376-00C04FC9DA04} to specify RADIUS accounting provider.

##### 2.2.3.4.18.3 RADIUS-based Accounting Settings

For RADIUS accounting, the RADIUS server information SHOULD be specified under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Accounting\Providers\{1AA7F840-C7F5-11D0-A376-00C04FC9DA04}\Servers.<218> There SHOULD be one subkey for each RADIUS server and the RADIUS server-specific settings SHOULD be present under this subkey as registry values. For example, the accounting settings specific to a RADIUS server Server1 SHOULD be present under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Accounting\Providers\{1AA7F840-C7F5-11D0-A376-00C04FC9DA04}\Servers\Server1.

##### 2.2.3.4.18.3.1 Score

This value specifies the initial responsiveness score of the RADIUS server. This MUST be of type REG\_DWORD. This can be any valid positive integer.

##### 2.2.3.4.18.3.2 AcctPort

This value specifies the UDP port that the RADIUS server is waiting on, for processing accounting requests. This MUST be of type REG\_DWORD. This can be any valid UDP port number on which the RADIUS server is configured to listen for accounting messages.

#### **2.2.3.4.18.3.3 Timeout**

This value specifies the time in seconds that the RRAS server waits for a response from the RADIUS server before trying the next configured RADIUS server. This MUST be of type REG\_DWORD. This can be any valid positive integer.

#### **2.2.3.4.18.3.4 EnableAccountingOnOff**

This value specifies whether RADIUS Accounting-On and Accounting-Off messages are to be sent by the RRAS server when it starts up and shuts down respectively. This MUST be of type REG\_DWORD. It SHOULD be either 0 or 1. A value 0 SHOULD be used to specify that the Accounting On/Off messages need not be sent by RRAS server and a value 1 SHOULD be used to specify that these messages need to be sent by RRAS server.

#### **2.2.3.4.19 Authentication Settings**

The authentication settings for the RRAS server SHOULD be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Authentication.

##### **2.2.3.4.19.1 AuthGroupName**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Authentication. This value MUST be of type REG\_SZ. This specifies the name of the RADIUS server or server group that provides authentication services.

##### **2.2.3.4.19.2 CRPName**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Authentication. This value MUST be of type REG\_SZ. This specifies the connection request policy (CRP) name which will designate whether connection requests are processed locally or forwarded to a remote RADIUS server.

##### **2.2.3.4.19.3 ActiveProvider**

This value MUST be defined under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Authentication\Providers. This MUST be of type REG\_SZ. This defines a GUID corresponding to the current authentication provider. This SHOULD be either {1AA7F841-C7F5-11D0-A376-00C04FC9DA04} to specify the default authentication provider or {1AA7F83F-C7F5-11D0-A376-00C04FC9DA04} to specify the RADIUS authentication provider.

##### **2.2.3.4.19.4 RADIUS-based Authentication Settings**

For RADIUS authentication, the RADIUS server information SHOULD be specified under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Authentication\Providers\{1AA7F83F-C7F5-11D0-A376-00C04FC9DA04}\Servers.[<219>](#) There SHOULD be one subkey for each RADIUS server and the RADIUS server specific settings SHOULD be present under this subkey as registry values. For example, the authentication settings specific to a RADIUS server Server1 SHOULD be present under the registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Authentication\Providers\{1AA7F840-C7F5-11D0-A376-00C04FC9DA04}\Servers\Server1.



#### 2.2.3.4.19.4.1 Score

This value specifies the initial responsiveness score of the RADIUS server. This MUST be of type REG\_DWORD. This can be any valid positive integer.

#### 2.2.3.4.19.4.2 AuthPort

This value specifies the UDP port that the RADIUS server is waiting on, for processing authentication requests. This MUST be of type REG\_DWORD. This can be any valid UDP port number on which the RADIUS server is configured to listen for authentication messages.

#### 2.2.3.4.19.4.3 Timeout

This value specifies the time in seconds that the RRAS server waits for a response from the RADIUS server before trying the next configured RADIUS server. This MUST be of type REG\_DWORD. This can be any valid positive integer.

#### 2.2.3.4.19.4.4 SendSignature

This value specifies whether a message authenticator need to be sent with each RADIUS authentication message or not. This MUST be of type REG\_DWORD. It SHOULD be either 0 or 1. A value 0 SHOULD be used to specify that the message authenticator need not be sent with each RADIUS message and a value 1 SHOULD be used to specify that message authenticator need to be sent with each RADIUS message.

### 2.2.4 Error Codes

This section lists additional error codes that can be used to convey specific error conditions to the RRASM client. These codes have been implemented in addition to the common error codes defined in [\[MS-ERREF\]](#).

Return value	Description
0x00000258 PENDING	An operation is pending.
0x00000259 ERROR_INVALID_PORT_HANDLE	An invalid port handle was detected.
0x0000025B ERROR_BUFFER_TOO_SMALL	The caller's buffer is too small.
0x00000260 ERROR_DEVICE_DOES_NOT_EXIST	The specified device does not exist.
0x00000267 ERROR_PORT_NOT_FOUND	The specified port was not found.
0x0000026A ERROR_PORT_NOT_OPEN	The specified port is not open.
0x0000026D ERROR_CANNOT_OPEN_PHONEBOOK	The phonebook file could not be opened.



Return value	Description
0x0000026E ERROR_CANNOT_LOAD_PHONEBOOK	The phonebook file could not be loaded.
0x0000026F ERROR_CANNOT_FIND_PHONEBOOK_ENTRY	The phonebook entry for the specified connection could not be found.
0x00000386 ERROR_UNKNOWN_PROTOCOL_ID	The specified protocol identifier is not known to the router.
0x00000387 ERROR_DDM_NOT_RUNNING	The Demand-dial Interface Manager is not running.
0x00000388 ERROR_INTERFACE_ALREADY_EXISTS	An interface with this name is already registered with the router.
0x00000389 ERROR_NO_SUCH_INTERFACE	An interface with this name is not registered with the router.
0x0000038A ERROR_INTERFACE_NOT_CONNECTED	The interface is not connected.
0x0000038C ERROR_INTERFACE_CONNECTED	The interface cannot be deleted, because it is connected.
0x0000038E ERROR_ALREADY_CONNECTING	The interface is already in the process of connecting.
0x0000038F ERROR_UPDATE_IN_PROGRESS	An update of routing information on this interface is already in progress.
0x00000394 ERROR_INTERFACE_DISABLED	The interface is in a disabled state.
0x0000039D ERROR_INTERFACE_HAS_NO_DEVICES	There are no routing enabled ports available for use by this demand-dial interface.
0x000003A0 ERROR_SERVICE_IS_PAUSED	The Demand-dial Interface Manager is in a paused state. The request could not be processed.
0x000003B4 ERROR_PROTOCOL_ALREADY_INSTALLED	The transport is already installed with the router.

## 3 Protocol Details

There are three components to the RRAS management - the RPC interfaces, the phonebook file settings, and the registry settings.

The RPC interfaces enable remote management of the RRAS runtime. It comprises two RPC interfaces – DIMSVC and RASRPC.

The phonebook file specifies the site-to-site connection settings and RRAS validates the phonebook entries used as a part of RRAS RPC methods using the phonebook file. The phonebook entries (specified through the RPC methods) are valid if there are corresponding phonebook entry sections that have the same name. The phonebook file format is described in section [2.2.2](#).

The registry settings specify the RRAS configuration. RRAS initializes its runtime configuration using the registry settings described in section [2.2.3](#). Subsequently the RRAS RPC interfaces provide the remote management of these runtime configuration settings. RRAS is responsible for updating the configuration changes back to the registry store. RRAS initializes the RRAS RPC interfaces as given in section [3.1.6.2](#) and [3.3.6.2](#). RRAS server passes the value of two of the registry keys that impacts RRAS protocol behavior as a part of this initialization as defined in section [3.1.6](#). RRAS stores these values in the ADM variables as defined in section [3.1.1](#). The other registry settings do not impact the RRAS protocol behavior and only impact the configuration used by RRAS. Both RRAS and RRAS reside on the same server. That portion of the server which implements the management semantics, which the RRAS protocol remotely makes available remotely, is referred to as the RRAS server or RRAS implementation.

### 3.1 DIMSVC Interface Server Details

For the list of methods supported by this interface, refer to [Appendix A: Full IDL \(section 6\)](#).

#### 3.1.1 Abstract Data Model

This section describes a conceptual model that an implementation can maintain to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model, as long as their external behavior is consistent with that described in this document.

RRAS protocol provides the remoting capability to the underlying RRAS implementation's management objects and methods. The following data variables affect the protocol behavior.

**RouterType:** This 4-byte variable specifies the currently defined RRAS role type. It is a combination of the flags as specified under section [2.2.3.4.1](#). As a part of the initialization, the RRAS server specifies this value for the RRAS server to initialize with **Start DIMSVC**, as defined in section [3.1.6](#). This value remains the same and will be refreshed only when the RRAS server is shut down and initialized again.

**SupportedTransportsList:** This specifies the list of transport identifiers that are supported by RRAS. Each transport identifier is a 4-byte value and can be one of the following values. As a part of the initialization, RRAS specifies this value for the RRAS server to initialize with **Start DIMSVC** as defined in section [3.1.6](#). This list remains static and will be refreshed only when the RRAS server is shut down and initialized again.

Value	Meaning
PID_IPX	IPX protocol <a href="#">&lt;220&gt;</a>

Value	Meaning
0x0000002B	
PID_IP 0x00000021	IPv4 protocol
PID_IPV6 0x00000057	IPv6 protocol <a href="#">&lt;221&gt;</a>

**PhonebookEntryNameList:** This specifies the list of **phonebook entry names** (section [2.2.2.1](#)). The RRASM server loads the phonebook file and regenerates this list when any of the following methods are called:

RRouterInterfaceCreate (section [3.1.4.13](#))

RRouterInterfaceGetInfo (section [3.1.4.14](#))

RRouterInterfaceSetInfo (section [3.1.4.15](#))

RasRpcDeleteEntry (section [3.3.4.1](#))

**InterfaceList:** This specifies the list of interfaces configured in the RRAS server. Each entry in this list is comprised of an interface name of type LPWSTR and an interface handle of type DWORD. This list is populated using the InterfaceName registry value (section [2.2.3.2.1.1](#)) for each interface as specified in section [2.2.3.2](#). As a part of the initialization, RRAS specifies this list with the interface name and handle specified for each entry. The interface handle is an opaque value for RRASM. This list is specified as a part of Start DIMSVC as defined in section [3.1.6](#). This list is updated when the following methods are called:

RRouterInterfaceCreate (section [3.1.4.13](#))

RRouterInterfaceDelete (section [3.1.4.16](#))

There are no additional states maintained by RRASM other than those maintained by [\[MS-RPCE\]](#).

### 3.1.2 Timers

No timers are required beyond those used internally by the RPC to implement resiliency to network outages, as specified in [\[MS-RPCE\]](#) section 3.2.3.2.1.

### 3.1.3 Initialization

The DIMSVC RPC interface of RRASM server MUST be initialized by RRAS as described in the Start DIMSVC abstract interface defined in section [3.1.6](#). As a part of the initialization process, the RRASM protocol server MUST register the RPC interface as specified in section [2.1.1](#).

### 3.1.4 Message Processing Events and Sequencing Rules

To receive incoming remote calls for this interface, the server MUST implement an RPC endpoint using the UUID, 8f09f000-b7ed-11ce-bbd2-00001a181cad. As a part of the message processing, RRASM performs validation parameters as specified under the methods in this section. It then passes the information to the actual RRAS implementation using **Invoke DIMSVC Method**. The **Invoke DIMSVC Method** will return any data required and the completion status of the operation is sent back to the client over the DIMSVC interface of RRASM protocol.

The RRASM server MUST perform a strict **Network Data Representation (NDR)** data consistency check at target level 5.0, as specified in [\[MS-RPCE\]](#) section 3.

In the following table, the term "Reserved for local use" means that the clients MUST NOT send the **opnum**, and the server behavior is undefined because it does not affect interoperability.

All methods MUST NOT throw exceptions. No exceptions are thrown beyond those thrown by the underlying RPC protocol [MS-RPCE].

Methods in RPC Opnum Order

Method	Description
<a href="#">RMprAdminServerGetInfo</a>	Retrieves port-related configuration information for the specified RRAS server. Opnum: 0
<a href="#">RRasAdminConnectionEnum</a>	Opnum: 1
<a href="#">RRasAdminConnectionGetInfo</a>	Opnum: 2
<a href="#">RRasAdminConnectionClearStats</a>	Opnum: 3
<a href="#">RRasAdminPortEnum</a>	Opnum: 4
<a href="#">RRasAdminPortGetInfo</a>	Opnum: 5
<a href="#">RRasAdminPortClearStats</a>	Opnum: 6
<a href="#">RRasAdminPortReset</a>	Opnum: 7
<a href="#">RRasAdminPortDisconnect</a>	Opnum: 8
<a href="#">RRouterInterfaceTransportSetGlobalInfo</a>	Opnum: 9
<a href="#">RRouterInterfaceTransportGetGlobalInfo</a>	Opnum: 10
<a href="#">RRouterInterfaceGetHandle</a>	Opnum: 11
<a href="#">RRouterInterfaceCreate</a>	Opnum: 12
<a href="#">RRouterInterfaceGetInfo</a>	Opnum: 13
<a href="#">RRouterInterfaceSetInfo</a>	Opnum: 14
<a href="#">RRouterInterfaceDelete</a>	Opnum: 15
<a href="#">RRouterInterfaceTransportRemove</a>	Opnum: 16
<a href="#">RRouterInterfaceTransportAdd</a>	Opnum: 17
<a href="#">RRouterInterfaceTransportGetInfo</a>	Opnum: 18
<a href="#">RRouterInterfaceTransportSetInfo</a>	Opnum: 19
<a href="#">RRouterInterfaceEnum</a>	Opnum: 20
<a href="#">RRouterInterfaceConnect</a>	Opnum: 21

Method	Description
<a href="#">RRouterInterfaceDisconnect</a>	Opnum: 22
<a href="#">RRouterInterfaceUpdateRoutes</a>	Opnum: 23
<a href="#">RRouterInterfaceQueryUpdateResult</a>	Opnum: 24
<a href="#">RRouterInterfaceUpdatePhonebookInfo</a>	Opnum: 25
<a href="#">RMIBEntryCreate</a>	Opnum: 26
<a href="#">RMIBEntryDelete</a>	Opnum: 27
<a href="#">RMIBEntrySet</a>	Opnum: 28
<a href="#">RMIBEntryGet</a>	Opnum: 29
<a href="#">RMIBEntryGetFirst</a>	Opnum: 30
<a href="#">RMIBEntryGetNext</a>	Opnum: 31
<a href="#">RMIBGetTrapInfo</a>	Opnum: 32
<a href="#">RMIBSetTrapInfo</a>	Opnum: 33
<a href="#">RRasAdminConnectionNotification</a>	Opnum: 34
<a href="#">RRasAdminSendUserMessage</a>	Opnum: 35
<a href="#">RRouterDeviceEnum</a>	Opnum: 36
<a href="#">RRouterInterfaceTransportCreate</a>	Opnum: 37
<a href="#">RRouterInterfaceDeviceGetInfo</a>	Opnum: 38
<a href="#">RRouterInterfaceDeviceSetInfo</a>	Opnum: 39
<a href="#">RRouterInterfaceSetCredentialsEx</a>	Opnum: 40
<a href="#">RRouterInterfaceGetCredentialsEx</a>	Opnum: 41
<a href="#">RRasAdminConnectionRemoveQuarantine</a>	Opnum: 42
<a href="#">RMprAdminServerSetInfo</a>	Opnum: 43
<a href="#">RMprAdminServerGetInfoEx</a>	Opnum: 44
<a href="#">RRasAdminConnectionEnumEx</a>	Opnum: 45
<a href="#">RRasAdminConnectionGetInfoEx</a>	Opnum: 46
<a href="#">RMprAdminServerSetInfoEx</a>	Opnum: 47
<a href="#">RRasAdminUpdateConnection</a>	Opnum: 48
<a href="#">RRouterInterfaceSetCredentialsLocal</a>	Opnum: 49
<a href="#">RRouterInterfaceGetCredentialsLocal</a>	Opnum: 50

### 3.1.4.1 RmprAdminServerGetInfo (Opnum 0)

The **RmprAdminServerGetInfo** method retrieves port-related configuration information for the specified RRAS server using the handle *hDimServer*. The *dwLevel* defines the type of information requested. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#). The caller SHOULD free the memory pointed to by *pInfoStruct*.

```
DWORD RmprAdminServerGetInfo(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD dwLevel,  
    [out] PDIM_INFORMATION_CONTAINER pInfoStruct  
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to one of the following values.

Value	Meaning
0	After the function returns, the memory pointed by pInfoStruct->pBuffer is interpreted as <a href="#">MPR_SERVER_0 (section 2.2.1.2.62)</a> .
1	After the function returns, the memory pointed by pInfoStruct->pBuffer is interpreted as <a href="#">MPR_SERVER_1 (section 2.2.1.2.63)</a> .<222>
2	After the function returns, the memory pointed by pInfoStruct->pBuffer is interpreted as <a href="#">MPR_SERVER_2 (section 2.2.1.2.64)</a> .<223>

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER**.

DIM\_INFORMATION\_CONTAINER.dwBufferSize SHOULD be initialized to zero. Upon successful return, the pInfoStruct->pBuffer is typecast to **MPR\_SERVER\_0**, **MPR\_SERVER\_1**,<224> or **MPR\_SERVER\_2**<225> based on the *dwLevel* value.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or in section [2.2.4](#). All values not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 0.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a **client** that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those specified in the previous table.

- If *dwLevel* is not supported, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server processes the request successfully, populate *pInfoStruct* with the information returned by the RRAS server. Return ERROR\_SUCCESS.
- Otherwise return the error provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.2 RRasAdminConnectionEnum (Opnum 1)

The **RRasAdminConnectionEnum** method retrieves the list of active connections for a specified RRAS server identified by the handle *hDimServer*. The *dwLevel* specifies the type of information requested. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), where **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. After the function returns, the caller SHOULD free the memory pointed to by **pInfoStruct**.

```
DWORD RRasAdminConnectionEnum(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in] DWORD dwPreferredMaximumLength,
    [out] LPDWORD lpdwEntriesRead,
    [out] LPDWORD lpdwTotalEntries,
    [in, out, unique] LPDWORD lpdwResumeHandle
);
```

**hDimServer:** A handle to the RRAS server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to one of the following values.

Value	Meaning
0	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as an array of <a href="#">RASI_CONNECTION 0 (section 2.2.1.2.78)</a> . The size of the array is determined by <i>lpdwEntriesRead</i> .
1	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as an array of <a href="#">RASI_CONNECTION 1 (section 2.2.1.2.79)</a> . The size of the array is determined by <i>lpdwEntriesRead</i> .
2	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as an array of <a href="#">RASI_CONNECTION 2 (section 2.2.1.2.80)</a> . The size of the array is determined by <i>lpdwEntriesRead</i> .
3	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as an array of <a href="#">RASI_CONNECTION 3 (section 2.2.1.2.81)</a> . The size of the array is determined by <i>lpdwEntriesRead</i> .

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER**, and **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. Upon successful return, the *pInfoStruct->pBuffer* is a typecast array of **RASI\_CONNECTION\_0**,

**RASI\_CONNECTION\_1**, **RASI\_CONNECTION\_2**, or **RASI\_CONNECTION\_3**,[<226>](#) based on the *dwLevel* value. The array size is determined by the value in memory pointed to by *lpdwEntriesRead*.

**dwPreferedMaximumLength:** This is of type **DWORD** and SHOULD specify the preferred maximum length of the returned data (*pInfoStruct->pBuffer*) in bytes.

**lpdwEntriesRead:** This is a pointer to type **DWORD** and upon a successful function-call return specifies the total number of connections enumerated from the current resume position given by *lpdwResumeHandle*.

**lpdwTotalEntries:** This is a pointer to type **DWORD** and receives the total number of connections that could have been enumerated from the current resume position given by *lpdwResumeHandle*.

**lpdwResumeHandle:** This is a pointer to type **DWORD** and specifies a resume handle that is used to continue the enumeration. The *lpdwResumeHandle* parameter is zero on the first call and left unchanged on subsequent calls. The caller MUST pass the same returned value in the next call to this function; otherwise, an error is returned. If the return code is **ERROR\_MORE\_DATA**, another call can be made using this handle to retrieve more data. If the return code is not **ERROR\_MORE\_DATA**, the handle returned SHOULD be ignored. A return value of **ERROR\_SUCCESS** indicates a successful completion of the enumeration. Any return value other than **ERROR\_SUCCESS** or **ERROR\_MORE\_DATA** indicates the failure of the enumeration.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of **ERROR\_SUCCESS** (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or in section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges as specified in section <a href="#">2.1.1.1</a> .
0x000000EA ERROR_MORE_DATA	Not all of the data was returned with this call. To obtain additional data, call the function again using the handle that was returned in the <i>lpdwResumeHandle</i> parameter.

The *opnum* field value for this method is 1.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error **ERROR\_ACCESS\_DENIED** (0x00000005).
- If the [RouterType \(section 2.2.3.4.1\)](#) is **ROUTER\_TYPE\_LAN**, return an error other than those in the preceding table.
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.



- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server processes the request successfully, populate the information returned by RRAS server in *pInfoStruct*, along with *lpdwEntriesRead*, *lpdwTotalEntries*, and *lpdwResumeHandle*, and return `ERROR_SUCCESS`.
- Otherwise return the failure error that the RRAS server returns.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.3 RRasAdminConnectionGetInfo (Opnum 2)

The **RRasAdminConnectionGetInfo** method retrieves the connection information for a particular connection identified by the passed handle of the connection given in *hDimConnection*. The RRAS server is identified by the server handle passed in *hDimServer*. The *dwLevel* defines the type of information requested. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), where **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. The caller SHOULD free the memory pointed to by *pInfoStruct*.

```
DWORD RRasAdminConnectionGetInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in] DWORD hDimConnection,
    [out] PDIM_INFORMATION_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to one of the following values.

Value	Meaning
0	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">RASI_CONNECTION 0 (section 2.2.1.2.78)</a> .
1	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">RASI_CONNECTION 1 (section 2.2.1.2.79)</a> .
2	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as an array of <a href="#">RASI_CONNECTION 2 (section 2.2.1.2.80)</a> structures.
3	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">RASI_CONNECTION 3 (section 2.2.1.2.81)</a> .<227>

**hDimConnection:** This is of type **DWORD** and SHOULD be set to a particular connection identifier for which the connection information is required. Obtain this handle by calling [RRasAdminConnectionEnum \(section 3.1.4.2\)](#). Since RRASM server does not maintain connection handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER**, and **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. Upon successful return, the *pInfoStruct->pBuffer* is a cast to an array of **RASI\_CONNECTION\_0**,

**RASI\_CONNECTION\_1**, or **RASI\_CONNECTION\_3** structures, [<228>](#) based on the *dwLevel* value.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 2.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If not, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If the [RouterType](#) is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, populate the *pInfoStruct* with the information returned by the RRAS server and return ERROR\_SUCCESS.
- Otherwise return the error provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.4 RRasAdminConnectionClearStats (Opnum 3)

The **RRasAdminConnectionClearStats** method resets the statistics counters for the connection identified by the passed handle in *hDimConnection*. The *hDimServer* handle specifies the RRASM server on which the call is executed.

```
DWORD RRasAdminConnectionClearStats(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hDimConnection  
);
```

**hDimServer:** A handle to the RRAS server where the call is executed, see section [3.1.3](#).

**hDimConnection:** This is of type **DWORD** and SHOULD be set to the particular connection identifier for which the connection statistics have to be cleared. Obtain this handle by calling [RRasAdminConnectionEnum \(section 3.1.4.2\)](#). Because RRASM server does not maintain

connection handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or in section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 3.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, return error ERROR\_ACCESS\_DENIED (0x00000005).
- If the **RouterType** is ROUTER\_TYPE\_LAN, return an error other than one of the errors listed in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- If the operation completed successfully, return ERROR\_SUCCESS.
- Otherwise, return the error provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.5 RRasAdminPortEnum (Opnum 4)

The **RRasAdminPortEnum** method retrieves the list of all ports on a RRAS server, or the ports for a specified connection determined by *hRasConnection*. The *hDimServer* handle specifies the RRAS server on which the call is executed. The *dwLevel* defines the type of information requested. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), where **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. The caller SHOULD free the memory pointed to by *pInfoStruct*.

```
DWORD RRasAdminPortEnum(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD dwLevel,  
    [in] DWORD hRasConnection,  
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,  
    [in] DWORD dwPreferredMaximumLength,  
    [out] LPDWORD lpdwEntriesRead,  
    [out] LPDWORD lpdwTotalEntries,  
    [in, out, unique] LPDWORD lpdwResumeHandle  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to the following value.

Value	Meaning
0	After the function returns, the memory pointed by pInfoStruct->pBuffer is interpreted as an array of <a href="#">RASI_PORT_0 (section 2.2.1.2.76)</a> . The size of the array is determined by <i>lpdwEntriesRead</i> . This includes information related to the Port object during runtime. The port objects SHOULD be initialized based on the port configurations defined by <a href="#">WanEndpoints (section 2.2.3.3.1.8)</a> . The Device Name is also returned as a part of each port information.

**hRasConnection:** This is of type **DWORD** and SHOULD be set to a particular connection identifier for which the connection information is required. Obtain this handle by calling [RRasAdminConnectionEnum \(section 3.1.4.2\)](#). If this parameter is passed as **INVALID\_HANDLE\_VALUE** (0xffffffff), the function enumerates all the active ports configured on the RRAS server. Since RRAS server does not maintain connection handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1), and **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. Upon successful return, the pInfoStruct->pBuffer is typecast to an array of **RASI\_PORT\_0**, and the array size is determined by the value to pointer *lpdwEntriesRead*.

**dwPreferedMaximumLength:** This is of type **DWORD** and SHOULD specify the preferred maximum length of returned data (pInfoStruct->pBuffer) in bytes. If *dwPreferedMaximumLength* is -1 then all existing port entries for the specified connection are returned in the buffer.

**lpdwEntriesRead:** This is a pointer to type **DWORD**. Upon successful return, this determines the total number of ports enumerated from the current resume position given by *lpdwResumeHandle*.

**lpdwTotalEntries:** This is a pointer to type **DWORD** and receives the total number of ports that could have been enumerated from the current resume position given by *lpdwResumeHandle*.

**lpdwResumeHandle:** This is a pointer to type **DWORD** and specifies a resume handle that is used to continue the enumeration. The *lpdwResumeHandle* parameter is zero on the first call and left unchanged on subsequent calls (the caller MUST pass the same returned value in the next call to this function; otherwise, an error is returned). If the return code is **ERROR\_MORE\_DATA** (0x000000EA), another call may be made using this handle to retrieve more data. If the handle is NULL upon return, the enumeration is complete. This handle is invalid (-1) for other types of error returns.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of **ERROR\_SUCCESS** (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not listed in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005	The calling application does not have sufficient privileges.

Return value/code	Description
ERROR_ACCESS_DENIED	
0x000000EA ERROR_MORE_DATA	Not all of the data was returned with this call. To obtain additional data, call the function again using the handle that was returned in the <i>lpdwResumeHandle</i> parameter.

The *opnum* field value for this method is 4.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).

If the [RouterType](#) (section [2.2.3.4.1](#)) is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.

- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, populate *pInfoStruct* with the information returned by the RRAS server and return ERROR\_SUCCESS.
- Otherwise return the failure error status returned by RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.6 RRasAdminPortGetInfo (Opnum 5)

The **RRasAdminPortGetInfo** method retrieves the port information for a particular port given in *hPort* for a specified RRAS server using the handle *hDimServer*. The *dwLevel* defines the type of information requested. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER](#) (section [2.2.1.2.1](#)), where DIM\_INFORMATION\_CONTAINER.dwBufferSize is initialized to zero. The caller SHOULD free the memory pointed to by *pInfoStruct*.

```

DWORD RRasAdminPortGetInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in] DWORD hPort,
    [out] PDIM_INFORMATION_CONTAINER pInfoStruct
);

```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to any of the following values.

Value	Meaning
0	After the function returns, the memory pointed to by <code>pInfoStruct-&gt;pBuffer</code> is typecast to <a href="#">RASI_PORT_0 (section 2.2.1.2.76)</a> . The size of the array is determined by <code>lpdwEntriesRead</code> .
1	After the function returns, the memory pointed to by <code>pInfoStruct-&gt;pBuffer</code> is typecast to <a href="#">RASI_PORT_1 (section 2.2.1.2.77)</a> . The size of the array is determined by <code>lpdwEntriesRead</code> .

**hPort:** This is of type **DWORD** and MUST be set to the particular port identifier for which the port information is required. Obtain this handle by calling [RRasAdminPortEnum \(section 3.1.4.5\)](#). Since RRASM server does not maintain any port handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER**, and `DIM_INFORMATION_CONTAINER.dwBufferSize` is initialized to zero. Upon successful return, the `pInfoStruct->pBuffer` is typecast to an array of the **RASI\_PORT\_0** or **RASI\_PORT\_1** structures, based on the `dwLevel` value.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of `ERROR_SUCCESS` (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not listed in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section 2.1.1.1.

The `opnum` field value for this method is 5.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section 2.1.1.1, whether this method was called by a client that has access to the method. If the client does not have access, then return error `ERROR_ACCESS_DENIED` (0x00000005).
- If the **RouterType** is `ROUTER_TYPE_LAN`, return an error other than those in the preceding table.
- If `pInfoStruct` is `NULL`, return an error other than those in the preceding table.
- If `dwLevel` is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, populate `pInfoStruct` with the information returned by RRAS server. Return `ERROR_SUCCESS`.
- Otherwise return the error status returned by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.7 RRasAdminPortClearStats (Opnum 6)

The **RRasAdminPortClearStats** method resets the counters for the specified port on the given server *hPort*. The *hDimServer* handle specifies the RRASM server on which the call is to be executed.

```
DWORD RRasAdminPortClearStats(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hPort  
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**hPort:** This is of type **DWORD** and MUST be set to the particular port identifier for which the port information is required. Obtain this handle by calling [RRasAdminPortEnum \(section 3.1.4.5\)](#). Since RRASM server does not maintain port handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of *ERROR\_SUCCESS* (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 6.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error *ERROR\_ACCESS\_DENIED* (0x00000005).
- If **RouterType** is *ROUTER\_TYPE\_LAN*, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error that the RRAS server may return while processing this request. Otherwise return *ERROR\_SUCCESS*. No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.8 RRasAdminPortReset (Opnum 7)

The **RRasAdminPortReset** function performs no action and always returns *ERROR\_SUCCESS* if the access validation succeeds.

```

DWORD RRasAdminPortReset (
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hPort
);

```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**hPort:** This is of type **DWORD** and SHOULD be set to the particular port identifier for which the port information is required. Obtain this handle by calling [RRasAdminPortEnum \(section 3.1.4.5\)](#). This parameter is not used. Because RRASM server does not maintain port handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or in section [2.2.4](#). All values not in the following table MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 7.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If **RouterType** is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error that the RRAS server may return while processing this request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.9 RRasAdminPortDisconnect (Opnum 8)

The **RRasAdminPortDisconnect** method initiates the disconnect of the connection on a specified port. The port SHOULD have been associated with a connection. For the disconnection to be successful, the connection SHOULD have been in the connected state. The connection is the established dial-up or VPN connection that has the RRAS server as its endpoint.

```

DWORD RRasAdminPortDisconnect (
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hPort
);

```



);

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**hPort:** This is of type **DWORD** and MUST be set to the port identifier of the port that is to be disconnected. Obtain this handle by calling [RRasAdminPortEnum \(section 3.1.4.5\)](#). Since RRASM server does not maintain port handle information, the validation of this handle SHOULD be done by the RRAS server implementation.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 8.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If **RouterType** is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- Use the **RRasAdminPortEnum** method to ensure that *hPort* is a valid port handle of an active connection. If it is not, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error that the RRAS server may return as a part of processing this request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.10 RRouterInterfaceTransportSetGlobalInfo (Opnum 9)

The **RRouterInterfaceTransportSetGlobalInfo** method [<229>](#) is used to set global information, for the specified transport (IPv4, IPv6, or IPX), such as disabling IPv6 filtering.

```
DWORD RRouterInterfaceTransportSetGlobalInfo(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD dwTransportId,  
    [in] PDIM_INTERFACE_CONTAINER pInfoStruct  
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwTransportId:** Specifies the transport for which the information is set (IPv4, IPv6, or IPX). It MUST be one of the following values.

Value	Meaning
PID_IPX 0x0000002B	IPX protocol <a href="#">&lt;230&gt;</a>
PID_IP 0x00000021	IPv4 protocol
PID_IPV6 0x00000057	IPv6 protocol <a href="#">&lt;231&gt;</a>

**pInfoStruct:** Specifies the pointer to a [DIM\\_INTERFACE\\_CONTAINER \(section 2.2.1.2.2\)](#).

The **fGetGlobalInfo** member of the **DIM\_INTERFACE\_CONTAINER** MUST be set to 0.

The **pGlobalInfo** and **dwGlobalInfoSize** of **DIM\_INTERFACE\_CONTAINER** MUST be set. The rest of the fields SHOULD not be set.

The **dwGlobalInfoSize** field MUST be set to the size of the information passed in **pGlobalInfo**.

The **pGlobalInfo** member MUST point to a valid [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) and [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#). Otherwise, an error code is returned. The acceptable RTR\_TOC\_ENTRY values depend on the transport and the RRAS server implementation support; hence the RRAS server implementation SHOULD check that *InfoType* of RTR\_TOC\_ENTRY is supported.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 9.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than one of the errors specified in the preceding table.
- If *dwTransportId* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.

- If the **dwGlobalInfoSize** information in *pInfoStruct* is not the same as the **Size** field of **RTR\_INFO\_BLOCK\_HEADER**, or if the **RTR\_INFO\_BLOCK\_HEADER** is not constructed properly according to section [2.2.1.2.3](#), return an error other than one of the errors in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- Return any error value returned as a part of the RRAS server processing. Otherwise return **ERROR\_SUCCESS**.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.11 RRouterInterfaceTransportGetGlobalInfo (Opnum 10)

The **RRouterInterfaceTransportGetGlobalInfo** method [<232>](#) is used to get the entire global information for the specified transport.

```
DWORD RRouterInterfaceTransportGetGlobalInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwTransportId,
    [in, out] PDIM_INTERFACE_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwTransportId:** Specifies the transport for which the information is set (IPv4, IPv6, or IPX). It MUST be one of the following values.

Value	Meaning
PID_IPX 0x0000002B	IPX protocol <a href="#">&lt;233&gt;</a>
PID_IP 0x00000021	IPv4 protocol
PID_IPV6 0x00000057	IPv6 protocol <a href="#">&lt;234&gt;</a>

**pInfoStruct:** Pointer to [DIM\\_INTERFACE\\_CONTAINER \(section 2.2.1.2.1\)](#). This pointer MUST NOT be NULL when calling this method and is allocated to the size of the **DIM\_INTERFACE\_CONTAINER** structure. On successful completion, the structure is populated with a **DIM\_INTERFACE\_CONTAINER** structure having valid values for **dwGlobalInfoSize** and **pGlobalInfo** fields which the caller SHOULD free when done using it.

The **fGetGlobalInfo** of **DIM\_INTERFACE\_CONTAINER** MUST be set to 1. The rest of the **DIM\_INTERFACE\_CONTAINER** fields SHOULD not be set.

The **pGlobalInfo** and **dwGlobalInfoSize** members of **DIM\_INTERFACE\_CONTAINER** will be populated on successful completion of this method.

The **pGlobalInfo** member will point to a valid [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) and [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#).

On successful completion **dwGlobalInfoSize** will be set to the size of the information being passed in **pGlobalInfo**.

If *dwTransportId* is PID\_IP or PID\_IP6 and if the **InfoType** field in the RTR\_TOC\_ENTRY structure is one of the following, **pGlobalInfo** MUST be interpreted as the structure in the following table.

InfoType value	Meaning	Structure pointed to by pGlobalInfo
MS_IP_BOOTP 0x0000270f	IP BOOTP global configuration information.	<a href="#">IPBOOTP GLOBAL CONFIG (section 2.2.1.2.150)</a>
MS_IP_IGMP 0x4137000a	IGMP global configuration.	<a href="#">IGMP MIB GLOBAL CONFIG (section 2.2.1.2.174)</a>
MS_IP_RIP 0x00000008	IP RIP global configuration information.	<a href="#">IPRIP GLOBAL CONFIG (section 2.2.1.2.165)</a> (values specified are overwritten)
MS_IP_DHCP_ALLOCATOR 0x81372714	DHCP global configuration information.	<a href="#">IP AUTO DHCP GLOBAL INFO (section 2.2.1.2.191)</a> (values specified are overwritten)
MS_IP_DNS_PROXY 0x81372713	DNS proxy global configuration information.	<a href="#">IP DNS PROXY GLOBAL INFO (section 2.2.1.2.193)</a> (values specified are overwritten)
MS_IP_OSPF<235> 0x0000000d	OSPF global configuration information specified is retrieved. The type field is the first field in each of the structures and this defines which of the structures MUST be used. The type field MUST be OSPF_PARAM_TYPE (section 2.3.1.1.13) and the value MUST be corresponding to the structures specified.	<a href="#">OSPF ROUTE FILTER INFO (section 2.2.1.2.209)</a> <a href="#">OSPF PROTO FILTER INFO (section 2.2.1.2.210)</a> <a href="#">OSPF GLOBAL PARAM (section 2.2.1.2.211)</a> <a href="#">OSPF ROUTE FILTER (section 2.2.1.2.208)</a>
MS_IP_ALG<236> 0x8137271A	Application layer gateway global configuration.	<a href="#">IP ALG GLOBAL INFO (section 2.2.1.2.201)</a>
MS_IPV6_DHCP 0x000003E7	DHCPv6 Relay global configuration information.	<a href="#">DHCPV6R GLOBAL CONFIG (section 2.2.1.2.158)</a>
MS_IP_NAT 0x81372715	IP NAT global configuration information.	<a href="#">IP NAT GLOBAL INFO (section 2.2.1.2.195)</a>

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 10.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than one of the errors specified in the preceding table.
- If *dwTransportId* is not specified in **SupportedTransportsList**, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, populate the returned information in the *pInfoStruct* with the information returned by the RRAS server and return ERROR\_SUCCESS.
- Otherwise return the error value provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.12 RRouterInterfaceGetHandle (Opnum 11)

The **RRouterInterfaceGetHandle** method [<237>](#) retrieves the handle of the specified interface *lpwsInterfaceName* among all the ROUTER\_INTERFACE\_TYPES. The *hDimServer* handle determines the RRAS server on which the call is made.

```
DWORD RRouterInterfaceGetHandle(
    [in] DIM_HANDLE hDimServer,
    [in, string] LPWSTR lpwsInterfaceName,
    [in, out] LPDWORD phInterface,
    [in] DWORD fIncludeClientInterfaces
);
```

**hDimServer:** A handle to the RRAS server where the call is executed, see section [3.1.3](#).

**lpwsInterfaceName:** Pointer to a null-terminated Unicode string that specifies the name of the interface to be retrieved.

**phInterface:** This is a pointer to a **DWORD** that receives the unique identifier of the interface specified by *lpwsInterfaceName*.

**fIncludeClientInterfaces:** Specifies whether the method includes client interfaces while searching. If this parameter is 0, interfaces of type ROUTER\_IF\_TYPE\_CLIENT are ignored in the search for the interface with the name specified by *lpwsInterfaceName*. If this parameter

is a non-zero value and an interface with the specified name exists, **RRouterInterfaceGetHandle** returns a handle to an interface of type ROUTER\_IF\_TYPE\_CLIENT. Since it is possible that there are several interfaces of type ROUTER\_IF\_TYPE\_CLIENT, the handle returned references the first interface that is found with the name ROUTER\_IF\_TYPE\_CLIENT specified by *lpwsInterfaceName*.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section 2.1.1.1.

The opnum field value for this method is 11.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section 2.1.1.1, whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *lpwsInterfaceName* is NULL, return an error other than those specified in the preceding table.
- If the interface name of any entry in InterfaceList is not the same as *lpwsInterfaceName*, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC** Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server has successfully processed the request, populate the interface handle in *phInterface*. This interface handle is the same as the one present as a part of the interface-specific entry in InterfaceList. Return ERROR\_SUCCESS.
- Otherwise return the error provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.13 RRouterInterfaceCreate (Opnum 12)

The **RRouterInterfaceCreate** method creates an interface on a specified RRAS server, *hDimServer*.<238>

```
DWORD RRouterInterfaceCreate(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in, out] LPDWORD phInterface
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section 3.1.3.

**dwLevel:** This is of type **DWORD** and MUST be set to any of the following values.

Value	Meaning
0	The pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_0 (section 2.2.1.2.82)</a> .
1	The pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_1 (section 2.2.1.2.83)</a> .
2	The pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_2 (section 2.2.1.2.84)</a> .
3	The pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_3 (section 2.2.1.2.85)</a> .

**pInfoStruct:** This is a pointer of type [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) and MUST be set to following, based on *dwLevel*.

dwLevel	pInfoStruct->size	pInfoStruct->pBuffer
0	This MUST be set to the size of <b>MPRI_INTERFACE_0</b> (section 2.2.1.2.82). Otherwise, an error is returned.	This MUST be set to point to <b>MPRI_INTERFACE_0</b> . Only the <b>wszInterfaceName</b> , <b>fEnabled</b> , and <b>dwIfType</b> fields of <b>MPRI_INTERFACE_0</b> can be set. Setting other values has no effect.
1	This MUST be set to the size of <b>MPRI_INTERFACE_1</b> (section 2.2.1.2.83). Otherwise, an error is returned.	This MUST be set to point to <b>MPRI_INTERFACE_1</b> . Only the <b>wszInterfaceName</b> , <b>fEnabled</b> , <b>dwIfType</b> fields of <b>MPRI_INTERFACE_1</b> can be set. Setting other values has no effect.
2	This MUST be set to the size of <b>MPRI_INTERFACE_2</b> (section 2.2.1.2.84). Otherwise, an error is returned.	This MUST be set to point to <b>MPRI_INTERFACE_2</b> . The <b>dwIfType</b> of <b>MPRI_INTERFACE_2</b> SHOULD be set to <b>ROUTER_IF_TYPE_FULL_ROUTER</b> . The <b>dwAlternateOffset</b> of <b>MPRI_INTERFACE_2</b> MUST be set to 0.
3	This MUST be set to the size of <b>MPRI_INTERFACE_3</b> (section 2.2.1.2.85). Otherwise, an error is returned.	This MUST be set to point to <b>MPRI_INTERFACE_3</b> . The <b>dwIfType</b> of <b>MPRI_INTERFACE_3</b> SHOULD be set to <b>ROUTER_IF_TYPE_FULL_ROUTER</b> . The <b>dwAlternateOffset</b> of <b>MPRI_INTERFACE_3</b> MUST be set to 0. The values of the <b>ipv6addrDns</b> and <b>ipv6addrDnsAlt</b> members of the <b>MPRI_INTERFACE_3</b> structure SHOULD be ignored by the server.

If **dwIfType** is set to **ROUTER\_IF\_TYPE\_TUNNEL1** or **ROUTER\_IF\_TYPE\_DIALOUT** in **MPRI\_INTERFACE\_0**, **MPRI\_INTERFACE\_1**, **MPRI\_INTERFACE\_2**, or **MPRI\_INTERFACE\_3**, an error is returned. [<239>](#)

If **dwIfType** is set to **ROUTER\_IF\_TYPE\_DEDICATED**, **ROUTER\_IF\_TYPE\_INTERNAL**, or **ROUTER\_IF\_TYPE\_LOOPBACK**, and if **fEnabled** is set to **FALSE**, an error other than one of the errors specified in the table that follows MUST be returned.

If the **dwIfType** in **MPRI\_INTERFACE\_0**, **MPRI\_INTERFACE\_1**, **MPRI\_INTERFACE\_2**, or **MPRI\_INTERFACE\_3**, is set to **ROUTER\_IF\_TYPE\_CLIENT**, **ROUTER\_IF\_TYPE\_HOME\_ROUTER**,

or ROUTER\_IF\_TYPE\_FULL\_ROUTER, and if the **RouterType** is ROUTER\_TYPE\_LAN, an error SHOULD be returned.

If **dwIfType** in MPRI\_INTERFACE\_0 is set to ROUTER\_IF\_TYPE\_FULL\_ROUTER, phonebook information for the interface MUST have already been configured in the phonebook file.

If **dwLevel** is either 2 or 3 and none of the authentication protocol-related flags MPRIO\_RequireMsCHAP2, MPRIO\_RequireCHAP, and MPRIO\_RequireEAP are specified in the **dwfOptions** member, then the **dwEncryptionType** member of the MPRI\_INTERFACE\_2 or MPRI\_INTERFACE\_3 structures SHOULD be initialized to MPR\_ET\_Require and the value of the **dwfOptions** member SHOULD be modified to enable the following flags by default:

- MPRIO\_RequireEncryptedPw
- MPRIO\_RequireDataEncryption
- MPRIO\_RequireCHAP
- MPRIO\_RequireMsCHAP2

**phInterface:** This is a pointer to a **DWORD** that specifies the unique identifier of the interface that is created. This is the same as the **dwInterface** in MPRI\_INTERFACE\_0, MPRI\_INTERFACE\_1, MPRI\_INTERFACE\_2, or MPRI\_INTERFACE\_3.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 12.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- If the interface name of any entry in InterfaceList is the same as **wszInterfaceName** specified as a part of MPRI\_INTERFACE\_0, MPRI\_INTERFACE\_1, MPRI\_INTERFACE\_2, and MPRI\_INTERFACE\_3, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable the RRAS server to perform the required management task.



- If the RRAS server processes the request successfully, populate the *phInterface* with the interface handle returned by the RRAS server, add an interface entry to the InterfaceList comprising the interface name to be the **wszInterfaceName** (present as a part of the MPRI\_INTERFACE\_0, MPRI\_INTERFACE\_1, MPRI\_INTERFACE\_2, or MPRI\_INTERFACE\_3 structure) and the interface handle to be the value filled in for *phInterface*. If **dwLevel** value is specified as 2 or 3, add the **wszInterfaceName** specified as a part of MPRI\_INTERFACE\_2 or MPRI\_INTERFACE\_3 into **PhonebookEntryNameList** and return ERROR\_SUCCESS.
- Otherwise return the error status that the RRAS server returned.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.14 RRouterInterfaceGetInfo (Opnum 13)

The **RRouterInterfaceGetInfo** method [<240>](#) retrieves information for a specified interface, *hInterface*, on a specified RRAS server, *hDimServer*. This method is used to find information about existing interfaces on the RRAS. The information is returned in *pInfoStruct*. The caller SHOULD free the memory pointed to by *pInfoStruct*.

```
DWORD RRouterInterfaceGetInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in] DWORD hInterface
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to any of the following values.

Value	Meaning
0	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">MPRI_INTERFACE_0 (section 2.2.1.2.82)</a> .
1	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">MPRI_INTERFACE_1 (section 2.2.1.2.83)</a> .
2	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">MPRI_INTERFACE_2 (section 2.2.1.2.84)</a> .
3	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">MPRI_INTERFACE_3 (section 2.2.1.2.85)</a> .

**pInfoStruct:** This is a pointer of type [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), and DIM\_INFORMATION\_CONTAINER.dwBufferSize SHOULD be initialized to zero. Upon successful return, the *pInfoStruct->pBuffer* is cast to an array of **MPRI\_INTERFACE\_0**, **MPRI\_INTERFACE\_1**, **MPRI\_INTERFACE\_2**, or **MPRI\_INTERFACE\_3** structures based on the *dwLevel* values.

The **dwfOptions** member of **MPRI\_INTERFACE\_2** and **MPRI\_INTERFACE\_3** SHOULD be updated as follows:

- If the **dwfOptions** member has neither MPRIO\_RequirePAP nor MPRIO\_RequireEAP, then enable MPRIO\_RequireEncryptedPw.

- If the **dwfOptions** has none of the following flags set, then enable MPRIO\_RequireMsEncryptedPw:
  - MPRIO\_RequireCHAP
  - MPRIO\_RequirePAP
  - MPRIO\_RequireEAP
- If the **dwEncryptionType** member is not set to MPR\_ET\_None or MPR\_ET\_Optional, enable the MPRIO\_RequireDataEncryption flag.

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). The interface MUST be of type ROUTER\_IF\_TYPE\_FULL\_ROUTER if **dwLevel** is set to 2 or 3. Because the RRAS server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle value represents a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not listed in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 13.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- If the *hInterface* value specified is not associated with an interface entry in InterfaceList that has a matching interface handle (value being the same), return an error other than one of the errors specified in the preceding table.
- If *dwLevel* value is specified as 2 or 3 and *lpEntry* is not present in **PhonebookEntryNameList**, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server has processed the request successfully, populate the *pInfoStruct* with the information returned by the RRAS server and return ERROR\_SUCCESS.

- Otherwise return the error status returned by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.15 RRouterInterfaceSetInfo (Opnum 14)

The RRouterInterfaceSetInfo method [<241>](#) sets information for a specified interface, *hInterface*, on a specified server, *hDimServer*.

```
DWORD RRouterInterfaceSetInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in] DWORD hInterface
);
```

**hDimServer:** A handle to the RRASM server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and SHOULD be set to any of the following values.

Value	Meaning
0	pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_0 (section 2.2.1.2.82)</a> .
1	pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_1 (section 2.2.1.2.83)</a> .
2	pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_2 (section 2.2.1.2.84)</a> .
3	pInfoStruct->pBuffer MUST be set to point to a <a href="#">MPRI_INTERFACE_3 (section 2.2.1.2.85)</a> . <a href="#">&lt;242&gt;</a>

**pInfoStruct:** This is a pointer of type [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) and MUST be set to the following, based on *dwLevel*.

dwLevel	pInfoStruct->size	pInfoStruct->pBuffer
0	This MUST be set to the size of the data being passed in <b>MPRI_INTERFACE_0</b> (section 2.2.1.2.82).	This MUST be set to point to <b>MPRI_INTERFACE_0</b> . Only the <b>fEnabled</b> field of this structure can be modified; the rest of the fields MUST be populated as returned by <a href="#">RRouterInterfaceGetInfo (section 3.1.4.14)</a> .
1	This MUST be set to the size of the data being passed in <b>MPRI_INTERFACE_1</b> (section 2.2.1.2.83).	This MUST be set to point to <b>MPRI_INTERFACE_1</b> . In addition to the fields for <b>MPRI_INTERFACE_0</b> , <b>lpwsdialoutHoursRestriction</b> can be set. Setting other values has no effect. The values MUST be populated as returned by RRouterInterfaceGetInfo.
	This MUST be set to the size of <b>MPRI_INTERFACE_2</b> (section 2.2.1.2.84). Otherwise, an error is returned.	This MUST be set to point to <b>MPRI_INTERFACE_2</b> . The <b>dwIfType</b> of <b>MPRI_INTERFACE_0</b> MUST be set to <b>ROUTER_IF_TYPE_FULL_ROUTER</b> . The <b>dwAlternateOffset</b> of <b>MPRI_INTERFACE_2</b> MUST be set to 0.

dwLevel	pInfoStruct->size	pInfoStruct->pBuffer
3	This MUST be set to the size of MPRI_INTERFACE_3 (section 2.2.1.2.85). Otherwise, an error is returned.	This MUST be set to point to MPRI_INTERFACE_3. The <b>dwIfType</b> of MPRI_INTERFACE_3 MUST be set to <b>ROUTER_IF_TYPE_FULL_ROUTER</b> . The <b>dwAlternateOffset</b> of <b>MPRI_INTERFACE_0</b> MUST be set to 0. The values of the ipv6addrDns and ipv6addrDnsAlt members of MPRI_INTERFACE_3 SHOULD be ignored by the server.

If the interface type, specified at the time the interface was created using [RRouterInterfaceCreate \(section 3.1.4.13\)](#), is either **ROUTER\_IF\_TYPE\_DEDICATED** or **ROUTER\_IF\_TYPE\_INTERNAL** and if **fEnabled** is set to FALSE, an error is returned.

When the **dwLevel** value is either 2 or 3 and the **dwfOptions** member does not contain any of the flags MPRIO\_RequirePAP, MPRIO\_RequireCHAP, MPRIO\_RequireMsCHAP2, or MPRIO\_RequireEAP, then the **dwfOptions** value SHOULD be modified to enable MPRIO\_RequireMsCHAP2, MPRIO\_RequireCHAP, and **MPRIO\_RequirePAP**.

**hInterface:** The unique identifier of an interface. This can be obtained from **RRouterInterfaceCreate** or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM does not manage the interface handles, the RRAS server SHOULD check to ensure that this handle is a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 14.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- If the *hInterface* value specified is not associated with an interface entry in **InterfaceList** that has a matching interface handle (value being the same), return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.

- Return any error that the RRAS server may return while processing this request. Otherwise return ERROR\_SUCCESS. No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.16 RRouterInterfaceDelete (Opnum 15)

The **RRouterInterfaceDelete** method [<243>](#) deletes an interface on a specified server. The interface MUST have been created with the [RRouterInterfaceCreate \(section 3.1.4.13\)](#) method.

```
DWORD RRouterInterfaceDelete(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hInterface
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** A unique identifier of an interface. This can be obtained from **RRouterInterfaceCreate** or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Because the RRAS server does not maintain the interface handles, the RRAS server SHOULD check to ensure that this handle is a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates the return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not listed in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .
0x0000038c ERROR_INTERFACE_CONNECTED	The interface is connected and therefore cannot be deleted. This error is returned if the interface is of type <b>ROUTER_IF_TYPE_CLIENT</b> , <b>ROUTER_IF_TYPE_HOME_ROUTER</b> , or <b>ROUTER_IF_TYPE_FULL_ROUTER</b> .

The opnum field value for this method is 15.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If the interface is of type **ROUTER\_IF\_TYPE\_CLIENT**, **ROUTER\_IF\_TYPE\_HOME\_ROUTER**, or **ROUTER\_IF\_TYPE\_FULL\_ROUTER**, and if the interface is not connected, the RRAS implementation MUST return ERROR\_INTERFACE\_CONNECTED (0x0000038c).

- If the *hInterface* value specified is not associated with an interface entry in **InterfaceList** that has a matching interface handle (value being the same), return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server returns successfully removing the interface context from its runtime configuration settings, and if the interface is **ROUTER\_IF\_TYPE\_FULL\_ROUTER**, get the interface name present in the interface entry (from the **InterfaceList**) that has the same interface handle as *hInterface*, remove the phone book entry with the specified interface name, and remove the interface name from **PhonebookEntryNameList**. Remove the interface entry from the **InterfaceList** to complete the removal of the interface.
- Return any error status provided by the RRAS server. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.17 RRRouterInterfaceTransportRemove (Opnum 16)

The **RRRouterInterfaceTransportRemove** method [<244>](#) is used to remove an existing transport (IPv4, IPv6 [<245>](#), or IPX [<246>](#)) from the RRAS server on an interface.

```
DWORD RRRouterInterfaceTransportRemove(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hInterface,
    [in] DWORD dwTransportId
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** A unique identifier of an interface. This can be obtained from [RRRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Because the RRASM server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle represents a valid interface handle.

**dwTransportId:** Specifies the transport (IPv4, IPv6, or IPX). It must be one of the following values. Otherwise an error other than those in the returned values table is returned.

Value	Meaning
PID_IPX 0x0000002B	IPX protocol <a href="#">&lt;247&gt;</a>
PID_IP 0x00000021	IPv4 protocol
PID_IPV6 0x00000057	IPv6 protocol <a href="#">&lt;248&gt;</a>

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

The return value is one of the following error codes. All other values must be treated the same.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 16.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *dwTransportId* is not specified in the **SupportedTransportList**, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status that the RRAS server returns as a result of its processing. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.18 RRouterInterfaceTransportAdd (Opnum 17)

The **RRouterInterfaceTransportAdd** method [<249>](#) adds a transport (IPv4, IPv6, or IPX) to a specified interface. Note that if a transport already exists on an interface it cannot be added.

```
DWORD RRouterInterfaceTransportAdd(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hInterface,  
    [in] DWORD dwTransportId,  
    [in] PDIM_INTERFACE_CONTAINER pInfoStruct  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Because the RRASM server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle represents a valid interface handle.

**dwTransportId:** Specifies the transport (IPv4, IPv6, or IPX) and MUST be one of the following values. Otherwise an error, other than those in the return values table, is returned.

Value	Meaning
PID_IPX	IPX <a href="#">&lt;250&gt;</a>

Value	Meaning
0x0000002B	
PID_IP 0x00000021	IPv4
PID_IPV6 0x00000057	IPv6< <a href="#">251</a> >

**pInfoStruct:** This is a pointer of type [DIM\\_INTERFACE\\_CONTAINER \(section 2.2.1.2.2\)](#).

**pInterfaceInfo** and **dwInterfaceInfoSize** of **DIM\_INTERFACE\_CONTAINER** MUST be set to valid values. All other fields of **DIM\_INTERFACE\_CONTAINER** are ignored.

**pInterfaceInfo** points to a valid [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) and [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#). Otherwise, an error is returned. The RRAS server does not store the interface configurations for the various transports that the RRAS server supports. As part of its processing, the RRAS server SHOULD check that **InfoType** of **RTR\_TOC\_ENTRY** is supported.

Only a combination of the following entries MUST be present in **pInterfaceInfo**.

Value	Meaning and conditions (interface means the one identified by hInterface)	Structure pointed to at offset
IP_IN_FILTER_INFO 0xffff0001	This is the input filter that MUST be applied to IP packets sent to the RRAS server. The information is overwritten. The interface MUST NOT be of type <b>ROUTER_IF_TYPE_INTERNAL</b> , <b>ROUTER_IF_TYPE_LOOPBACK</b> , or <b>ROUTER_IF_TYPE_DIALOUT</b> .	<a href="#">FILTER_DESCRIPTOR (section 2.2.1.2.5)</a>
IP_OUT_FILTER_INFO 0xffff0002	This is the output filter that MUST be applied to IP packets sent from the RRAS server. The information is overwritten. The interface MUST NOT be of type <b>ROUTER_IF_TYPE_INTERNAL</b> , <b>ROUTER_IF_TYPE_LOOPBACK</b> , or <b>ROUTER_IF_TYPE_DIALOUT</b> .	<a href="#">FILTER_DESCRIPTOR (section 2.2.1.2.5)</a>
IP_INTERFACE_STATUS_INF O 0xffff0004	The interface IP status info is overwritten.	<a href="#">INTERFACE_STATUS_INFO (section 2.2.1.2.18)</a>
IP_ROUTER_DISC_INFO 0xffff0007	Router discovery information is overwritten.	<a href="#">RTR_DISC_INFO (section 2.2.1.2.14)</a>
IP_MCAST_BOUNDARY_INFO 0xffff000b	Multicast boundary information is added.	<a href="#">MIB_BOUNDARYROW (section 2.2.1.2.24)</a>
IP_IFFILTER_INFO 0xffff000d	IP interface filter information is overwritten. Interface MUST NOT be	<a href="#">IFFILTER_INFO (section 2.2.1.2.89)</a>



Value	Meaning and conditions (interface means the one identified by hInterface)	Structure pointed to at offset
	of type <b>ROUTER_IF_TYPE_INTERNAL</b> , <b>ROUTER_IF_TYPE_LOOPBACK</b> , or <b>ROUTER_IF_TYPE_DIALOUT</b> .	
IP_MCAST_LIMIT_INFO 0xffff000e	Multicast configuration information.	<a href="#">MIB_MCAST_LIMIT_ROW (section 2.2.1.2.50)</a>
IP_IN_FILTER_INFO_V6 0xffff0011	This is the input filter that MUST be applied to IPv6 packets sent to the RRAS server. The information is overwritten. The interface MUST NOT be of type <b>ROUTER_IF_TYPE_INTERNAL</b> , <b>ROUTER_IF_TYPE_LOOPBACK</b> , or <b>ROUTER_IF_TYPE_DIALOUT</b> .	<a href="#">FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7)&lt;252&gt;</a>
IP_OUT_FILTER_INFO_V6 0xffff0012	This is the output filter that MUST be applied to IPv6 packets sent from the RRAS server. The information is overwritten. The interface MUST NOT be of type <b>ROUTER_IF_TYPE_INTERNAL</b> , <b>ROUTER_IF_TYPE_LOOPBACK</b> , or <b>ROUTER_IF_TYPE_DIALOUT</b> .	<a href="#">FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7)&lt;253&gt;</a>
IP_DEMAND_DIAL_FILTER_I NFO_V6 0xffff0013	IPv6 traffic that matches this filter indicates that a site-to-site connection MUST be available and all IPv6 packets matching this filter MUST be routed into the connection. The interface MUST be of type <b>ROUTER_IF_TYPE_FULL_ROUTE R</b> or <b>ROUTER_IF_TYPE_HOME_ROUTE R</b> and the filters are overwritten	<a href="#">FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7)&lt;254&gt;</a>
IP_IFFILTER_INFO_V6 0xffff0014	IPv6 interface filter information is overwritten. The interface MUST NOT be of type <b>ROUTER_IF_TYPE_INTERNAL</b> , <b>ROUTER_IF_TYPE_LOOPBACK</b> , or <b>ROUTER_IF_TYPE_DIALOUT</b> .	<a href="#">IFFILTER_INFO (section 2.2.1.2.89)&lt;255&gt;</a>
MS_IP_BOOTP 0x0000270f	IP BOOTP interface, information depending.	<a href="#">IPBOOTP_IF_CONFIG (section 2.2.1.2.151)</a>
MS_IP_IGMP 0x4137000a	IGMP interface information.	<a href="#">IGMP_MIB_IF_CONFIG (section 2.2.1.2.175)</a>
MS_IP_RIP 0x00000008	IP RIP interface information.	<a href="#">IPRIP_IF_CONFIG (section 2.2.1.2.167)</a>
MS_IP_DHCP_ALLOCATOR	DHCP allocator interface	<a href="#">IP_AUTO_DHCP_INTERFACE INFO (section</a>

Value	Meaning and conditions (interface means the one identified by hInterface)	Structure pointed to at offset
0x81372714	information. Used only with <a href="#">RRouterInterfaceTransportSetGlobalInfo</a> (section 3.1.4.10).	<a href="#">2.2.1.2.192</a> )
MS_IP_DNS_PROXY 0x81372713	DNS proxy interface information.	<a href="#">IP_DNS_PROXY_INTERFACE_INFO</a> (section 2.2.1.2.194)
MS_IP_NAT 0x81372715	IP NAT interface information.	<a href="#">IP_NAT_INTERFACE_INFO</a> (section 2.2.1.2.197)
MS_IP_OSPF<256> 0x0000000d	OSPF interface information is added.	<a href="#">OSPF_INTERFACE_PARAMETER</a> (section 2.2.1.2.215)
MS_IPV6_DHCP 0x000003E7	DHCPv6 Relay interface information.	<a href="#">DHCPV6_RELAY_INTERFACE_CONFIG</a> (section 2.2.1.2.160)

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values not in the following table MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in <a href="#">2.1.1.1</a> .

The opnum field value for this method is 17.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwTransportId* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status provided by the RRAS server processing. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.19 RRouterInterfaceTransportGetInfo (Opnum 18)

The **RRouterInterfaceTransportGetInfo** method<257> retrieves information about a transport running on a specified interface. The information retrieved is of the type [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#), encapsulated within a [DIM\\_INTERFACE\\_CONTAINER \(section 2.2.1.2.2\)](#).

```
DWORD RRouterInterfaceTransportGetInfo(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hInterface,  
    [in] DWORD dwTransportId,  
    [in, out] PDIM_INTERFACE_CONTAINER pInfoStruct  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle is a valid interface handle.

**dwTransportId:** Specifies the transport for which the information is retrieved (IPv4, IPv6, or IPX). It MUST be one of the following values. Otherwise an error other than those in the return values table is returned.

Value	Meaning
PID_IPX 0x0000002B	IPX<258>
PID_IP 0x00000021	IPv4
PID_IPV6 0x00000057	IPv6<259><260>

**pInfoStruct:** This is a pointer of type **DIM\_INTERFACE\_CONTAINER**. It MUST NOT be NULL.

**fGetInterfaceInfo** of **DIM\_INTERFACE\_CONTAINER** MUST be set to 1.

On completion of the method, **pInterfaceInfo** and **dwInterfaceInfoSize** of the *pInfoStruct* fields are set. **pInterfaceInfo** points to a valid [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#), and [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) on return.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of [ERROR\\_SUCCESS \(0x00000000\)](#) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 18.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwTransportId* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server processing returns successfully, populate the interface information returned by RRAS server in *pInfoStruct* and return ERROR\_SUCCESS.
- Otherwise return the error result provided by RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.20 RRouterInterfaceTransportSetInfo (Opnum 19)

The **RRouterInterfaceTransportSetInfo** method [<261>](#) sets information about a transport running on a specified interface. The information is overwritten using the type [RTR\\_INFO\\_BLOCK\\_HEADER](#) (section [2.2.1.2.3](#)), encapsulated within a [DIM\\_INTERFACE\\_CONTAINER](#) (section [2.2.1.2.2](#)).

```
DWORD RRouterInterfaceTransportSetInfo(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hInterface,  
    [in] DWORD dwTransportId,  
    [in] PDIM_INTERFACE_CONTAINER pInfoStruct  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate](#) (section [3.1.4.13](#)) or [RRouterInterfaceGetHandle](#) (section [3.1.4.12](#)). Because the RRASM server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle represents a valid interface handle.

**dwTransportId:** Specifies the transport for which the information is set (IPv4, IPv6, or IPX). It MUST be one of the following values. Otherwise an error other than those in the return values table is returned.

Value	Meaning
PID_IPX 0x0000002B	IPX <a href="#">&lt;262&gt;</a>
PID_IP 0x00000021	IPv4

Value	Meaning
PID_IPV6 0x00000057	IPv6<263>

**pInfoStruct:** This is a pointer of type DIM\_INTERFACE\_CONTAINER.

**pInterfaceInfo** and **dwInterfaceInfoSize** of PDIM\_INTERFACE\_CONTAINER MUST be set. The rest of the fields are ignored. The RRAS server does not store the interface configurations for the various transports that the RRAS server supports. The RRAS server SHOULD check that the **InfoType** field of [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) is supported.

Only a combination of the following entries of RTR\_TOC\_ENTRY MUST be present in **pInterfaceInfo**.

Value	Meaning and conditions (interface means the one identified by hInterface)	Structure pointed to at offset
IP_INTERFACE_STATUS_INFO 0xffff0004	Interface IP status information is overwritten.	<a href="#">INTERFACE_STATUS_INFO (section 2.2.1.2.18)</a>
IP_ROUTER_DISC_INFO 0xffff0007	Router discovery information is overwritten.	<a href="#">RTR_DISC_INFO (section 2.2.1.2.14)</a>
IP_MCAST_BOUNDARY_INFO 0xffff000b	Multicast boundary information is added.	<a href="#">MIB_BOUNDARYROW (section 2.2.1.2.24)</a>
IP_IFFILTER_INFO 0xffff000d	IP interface filter information is overwritten. The interface MUST NOT be of type ROUTER_IF_TYPE_INTERNAL, ROUTER_IF_TYPE_LOOPBACK, or ROUTER_IF_TYPE_DIALOUT.	<a href="#">IFFILTER_INFO (section 2.2.1.2.89)</a>
IP_MCAST_LIMIT_INFO 0xffff000e	Multicast configuration information.	<a href="#">MIB_MCAST_LIMIT_ROW (section 2.2.1.2.16)</a>
IP_ROUTE_INFO 0xffff0005	The dwAdminStatus MUST be IF_ADMIN_STATUS_UP if the route information is added. If bV4 of <a href="#">INTERFACE_ROUTE_INFO</a> is set, it indicates an IPv4 route is added; otherwise, an IPv6 route is added.	INTERFACE_ROUTE_INFO (section 2.2.1.2.11)<264>
IP_IN_FILTER_INFO 0xffff0001	This is the input filter that MUST be applied to IP packets sent to the RRAS server. The information is overwritten. The interface MUST NOT be of type ROUTER_IF_TYPE_INTERNAL, ROUTER_IF_TYPE_LOOPBACK, or ROUTER_IF_TYPE_DIALOUT.	<a href="#">FILTER_DESCRIPTOR (section 2.2.1.2.5)</a>

<b>Value</b>	<b>Meaning and conditions (interface means the one identified by hInterface)</b>	<b>Structure pointed to at offset</b>
IP_OUT_FILTER_INFO 0xffff0002	This is the output filter that MUST be applied to IP packets sent from the RRAS server. The information is overwritten. The interface MUST NOT be of type ROUTER_IF_TYPE_INTERNAL, ROUTER_IF_TYPE_LOOPBACK, or ROUTER_IF_TYPE_DIALOUT.	FILTER_DESCRIPTOR (section 2.2.1.2.5)
IP_DEMAND_DIAL_FILTER_INFO 0xffff0009	IPv4 traffic that matches this filter indicates that there is a site-to-site connection available into which all the IPv4 packets (matching this filter) are routed. The information is overwritten. The interface MUST be of type ROUTER_IF_TYPE_FULL_ROUTE R or ROUTER_IF_TYPE_HOME_ROUTER.	FILTER_DESCRIPTOR (section 2.2.1.2.5)
IP_IN_FILTER_INFO_V6 0xffff0011	This is the input filter that MUST be applied to IPv6 packets sent to the RRAS server. The information is overwritten. The interface MUST NOT be of type ROUTER_IF_TYPE_INTERNAL, ROUTER_IF_TYPE_LOOPBACK, or ROUTER_IF_TYPE_DIALOUT.	<a href="#">FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7)&lt;265&gt;</a>
IP_OUT_FILTER_INFO_V6 0xffff0012	This is the output filter that MUST be applied to IPv6 packets sent from the RRAS server. The information is overwritten. The interface MUST NOT be of type ROUTER_IF_TYPE_INTERNAL, ROUTER_IF_TYPE_LOOPBACK, or ROUTER_IF_TYPE_DIALOUT.	FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7) <a href="#">&lt;266&gt;</a>
IP_DEMAND_DIAL_FILTER_INFO_V6 0xffff0013	IPv6 traffic that matches this filter indicates that a site-to-site connection MUST be available and all IPv6 packets matching this filter MUST be routed into the connection. The interface MUST be of type ROUTER_IF_TYPE_FULL_ROUTE R or ROUTER_IF_TYPE_HOME_ROUTER. The filters are overwritten.	FILTER_DESCRIPTOR_V6 (section 2.2.1.2.7) <a href="#">&lt;267&gt;</a>
IP_IFFILTER_INFO_V6	The IPv6 interface filter	IFFILTER_INFO (section

Value	Meaning and conditions (interface means the one identified by hInterface)	Structure pointed to at offset
0xffff0014	information is overwritten. The interface MUST NOT be of type ROUTER_IF_TYPE_INTERNAL, ROUTER_IF_TYPE_LOOPBACK, or ROUTER_IF_TYPE_DIALOUT.	2.2.1.2.89) <a href="#">&lt;268&gt;</a>
MS_IP_BOOTP 0x0000270f	IP BOOTP interface information.	<a href="#">IPBOOTP_IF_CONFIG (section 2.2.1.2.151)</a>
MS_IP_IGMP 0x4137000a	IGMP interface information. It can only be set once.	<a href="#">IGMP_MIB_IF_CONFIG (section 2.2.1.2.175)</a>
MS_IP_RIP 0x00000008	IP RIP interface information.	<a href="#">IPRIP_IF_CONFIG (section 2.2.1.2.167)</a>
MS_IP_DHCP_ALLOCATOR 0x81372714	DHCP allocator interface information.	<a href="#">IP_AUTO_DHCP_INTERFACE_I NFO (section 2.2.1.2.192)</a>
MS_IP_DNS_PROXY 0x81372713	DNS proxy interface information.	<a href="#">IP_DNS_PROXY_INTERFACE_IN FO (section 2.2.1.2.194)</a>
MS_IP_NAT 0x81372715	IP NAT interface information.	<a href="#">IP_NAT_INTERFACE_INFO (section 2.2.1.2.197)</a>
MS_IP_OSPF <a href="#">&lt;269&gt;</a> 0x0000000d	OSPF interface information is set. This MUST end the configuration buffer by OSPF_END_PARAM_TYPE. If passed with any other structure, it will return an error.	<a href="#">OSPF_INTERFACE_PARAM (section 2.2.1.2.215)</a> , <a href="#">OSPF_NBMA_NEIGHBOR_PARA M (section 2.2.1.2.216)</a>
MS_IPV6_DHCP 0x000003E7	DHCPv6 Relay interface information. It can only be set once.	<a href="#">DHCPV6R_IF_CONFIG (section 2.2.1.2.160)</a>

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The Opnum field value for this method is 19.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If **pInfoStruct** is NULL, return an error other than those in the preceding table.
- If **dwTransportId** is not specified in **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- Return any processing error that the RRAS server fails with. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.21 RRouterInterfaceEnum (Opnum 20)

The **RRouterInterfaceEnum** method [<270>](#) Retrieves the list of all the interfaces from the specified server. The *hDimServer* handle specifies the RRAS server on which the call is to be executed. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), where **DIM\_INFORMATION\_CONTAINER.dwBufferSize** is initialized to zero. The caller SHOULD free the memory pointed to by *pInfoStruct*.

```
DWORD RRouterInterfaceEnum(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in] DWORD dwPreferredMaximumLength,
    [out] LPDWORD lpdwEntriesRead,
    [out] LPDWORD lpdwTotalEntries,
    [in, out, unique] LPDWORD lpdwResumeHandle
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and SHOULD be set to zero (0).

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER**.

**pInfoStruct.dwBufferSize** SHOULD be initialized to zero. Upon successful return, the *pInfoStruct->pBuffer* is cast to an array of [MPRI\\_INTERFACE\\_0 \(section 2.2.1.2.82\)](#), and the array size is determined by the value to pointer *lpdwEntriesRead*.

**dwPreferredMaximumLength:** This is of type **DWORD** and SHOULD specify the preferred maximum length of returned data (*pInfoStruct->pBuffer*) in bytes. If this parameter is -1, the buffer returned is large enough to hold all available information.

**lpdwEntriesRead:** This is a pointer to type **DWORD**. Upon successful return, this determines the total number of connections enumerated from the current resume position given by *lpdwResumeHandle*.

**lpdwTotalEntries:** This is a pointer to type **DWORD** and receives the total number of connections that could have been enumerated from the current resume position given by *lpdwResumeHandle*.



**lpdwResumeHandle:** This is a pointer to type **DWORD** and specifies a resume handle used to continue the enumeration. The *lpdwResumeHandle* parameter is zero on the first call and left unchanged on subsequent calls (the caller MUST pass the same returned value in the next call to this function). If the return code is ERROR\_MORE\_DATA (0x000000EA), another call MAY be made using this handle to retrieve more data. If the handle is NULL upon return, the enumeration is complete. This handle is invalid for other types of error returns.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client. This error code value can correspond to a RRAS Management Protocol-specific failure, which takes a value between 600 and 975, or any generic failure.

The return value is one of the following error codes. All other error values must be treated the same.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section 2.1.1.1.
0x000000EA ERROR_MORE_DATA	More information is available; the enumeration can be continued.

The opnum field value for this method is 20.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section 2.1.1.1, whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS Server processes the request successfully, populate the interface information in *pInfoStruct* and fill the values for *lpdwResumeHandle*, *lpdwEntriesRead*, and *lpdwTotalEntries* as returned by the RRAS server. If the RRAS server has updated the resume handle and there are more entries to be enumerated, return ERROR\_MORE\_DATA. Otherwise, return ERROR\_SUCCESS.
- Otherwise return the error status provided by RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.22 RRouterInterfaceConnect (Opnum 21)

The **RRouterInterfaceConnect** method [<271>](#) establishes a connection for the specified interface *hInterface* if it is not already connected. The *hDimServer* handle specifies the RRASM server on which the call is to be executed.

```
DWORD RRouterInterfaceConnect(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hInterface,  
    [in] ULONG_PTR hEvent,  
    [in] DWORD fBlocking,  
    [in] DWORD dwCallersProcessId  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle is a valid interface handle.

**hEvent:** The calling application MUST specify NULL for this.

**fBlocking:** If this parameter is set to 1, the function does not return until the connection attempt has completed.

If this parameter is set to 0, the function will return immediately. A return value of PENDING (0x00000258) indicates that the connection attempt was successfully initiated.

**dwCallersProcessId:** This is for internal use and SHOULD be ignored by the server.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .
0x00000258 PENDING	An operation is pending.

The opnum field value for this method is 21. Whether the call returns immediately or is blocked is decided by *fBlocking* as previously described.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).

- If *RouterType* is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status or PENDING status that the RRAS server may return as a part of its processing. The RRAS server MUST return PENDING if fBlocking is set to FALSE and the task of connecting the interface is not complete. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.23 RRouterInterfaceDisconnect (Opnum 22)

The **RRouterInterfaceDisconnect** method disconnects the specified interface, *hInterface*. The *hDimServer* handle specifies the RRASM server on which the call is to be executed.

```
DWORD RRouterInterfaceDisconnect(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hInterface
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle is a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 22.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *RouterType* is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status that the RRAS server returns while processing this request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.24 RRouterInterfaceUpdateRoutes (Opnum 23)

The **RRouterInterfaceUpdateRoutes** method [<272>](#) updates routing information for a given transport on a specified interface on the RRAS server. If a routing protocol like RIP is running ([\[RFC1058\]](#)), the new routes learned are updated on the interface. This interface **MUST** be called only when the interface state is ROUTER\_IF\_STATE\_CONNECTED, otherwise an error is returned.

```
DWORD RRouterInterfaceUpdateRoutes(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hInterface,  
    [in] DWORD dwTransportId,  
    [in] ULONG_PTR hEvent,  
    [in] DWORD dwClientProcessId  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM server does not maintain the interface handles, the RRAS server **SHOULD** check and ensure that this handle represents a valid interface handle.

**dwTransportId:** Specifies the transport for which routing information needs to be updated. This **MUST** be one of the following.

Value	Meaning
PID_IPX 0x0000002B	IPX <a href="#">&lt;273&gt;</a>
PID_IP 0x00000021	IPv4

**hEvent:** The calling application **MUST** specify NULL for this parameter.

**dwClientProcessId:** The current process identifier where the function is called from. If this is a nonexistent process the method will fail with an error code, as specified in [\[MS-ERREF\]](#). Otherwise the process specified is notified.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or in section [2.2.4](#). All values that are not in the table that follows **MUST** be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 23.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If **RouterType** is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- If *dwTransportId* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status the RRAS server returns while processing this request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.25 RRouterInterfaceQueryUpdateResult (Opnum 24)

The **RRouterInterfaceQueryUpdateResult** method [<274>](#) returns the result of the last **RRouterInterfaceUpdateRoutes** (section [3.1.4.24](#)) request of the RRAS server for a specified transport to update its routes for an interface. This method MUST be called only once after **RRouterInterfaceUpdateRoutes**.

```
DWORD RRouterInterfaceQueryUpdateResult(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hInterface,  
    [in] DWORD dwTransportId,  
    [out] LPDWORD pUpdateResult  
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This identifier can be obtained from **RRouterInterfaceCreate** (section [3.1.4.13](#)) or **RRouterInterfaceGetHandle** (section [3.1.4.12](#)). Because the RRAS server does not maintain interface handles, the RRAS server SHOULD check and ensure that this handle represents a valid interface handle.

**dwTransportId:** Specifies the transport for which routing information needs to be updated. This MUST be one of the following values. Otherwise an error is returned.

Value	Meaning
PID_IPX 0x0000002B	IPX <a href="#">&lt;275&gt;</a>
PID_IP 0x00000021	IPv4

**pUpdateResult:** A pointer to a **DWORD** variable. This variable receives the result of the last call to **RRouterInterfaceUpdateRoutes**; see the return values of **RRouterInterfaceUpdateRoutes**.

**Return Values:** A-32 bit, unsigned integer value that indicates return status. A return value of `ERROR_SUCCESS` (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 24.

When processing this call, the RRAS server MUST do the following.

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error `ERROR_ACCESS_DENIED` (0x00000005).
- If `dwTransportId` is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server processes the request successfully, update the `pUpdateResult` with the information provided by RRAS server and return `ERROR_SUCCESS`. Otherwise return the error status that the RRAS server returns.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.26 RRouterInterfaceUpdatePhonebookInfo (Opnum 25)

The **RRouterInterfaceUpdatePhonebookInfo** method [<276>](#) forces the router to pick up changes made on a specified demand-dial interface, `hInterface`. The `hDimServer` handle specifies the RRAS server on which the call is to be executed. Call this method after changes are made to a phone-book entry for a demand-dial interface, such as `ROUTER_IF_TYPE_HOME_ROUTER` or `ROUTER_IF_TYPE_FULL_ROUTER`.

```
DWORD RRouterInterfaceUpdatePhonebookInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hInterface
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Because the RRAS server does not maintain the interface handles, the RRAS server SHOULD check and ensure that this handle is a valid interface handle.

**Return Values:** A-32 bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section 2.1.1.1.

The opnum field value for this method is 25.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section 2.1.1.1, whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error result the RRAS server might return while processing this request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.27 RMIBEntryCreate (Opnum 26)

The **RMIBEntryCreate** method [<277>](#) creates an MIB entry that is used by the RRAS to create a route entry in the IPv4 routing table.

```
DWORD RMIBEntryCreate(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
    [in] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the transport protocol.

**dwRoutingPid:** Specifies the routing protocol. The value of this parameter MUST be set to IPRTMGR\_PID (0x2710.) The method MUST return an error other than those specified in the return value table for any other value.

**pInfoStruct:** This is a pointer to a [DIM\\_MIB\\_ENTRY\\_CONTAINER \(section 2.2.1.2.19\)](#) structure with valid **dwMibInEntrySize** and **pMibInEntry** fields. The **dwMibOutEntrySize** and **pMibOutEntry** of the structure are ignored by the server for this method. **dwMibInEntrySize** MUST be set to the size of data being passed in **pMibInEntry**. If *pInfoStruct* is NULL, an error other than those specified in the return value table is returned. Otherwise, the pointer is treated as a pointer to the DIM\_MIB\_ENTRY\_CONTAINER structure.

Because the *dwRoutingPid* parameter of this method MUST take the value `IPRTRMGR_PID`, the **pMibInEntry** field of **pInfoStruct** MUST be a pointer to [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#). The **dwId** and **rgbyData** fields of `MIB_OPAQUE_INFO` must be set to one of the values in the following table.

dwId Value	Structure that MUST be pointed to by rgbyData	Remarks
ROUTE_MATCHING 0x0000001f	<a href="#">MIB_IPDESTROW (section 2.2.1.2.20)</a>	<p>A route corresponding to data in <b>rgbyData</b> is added in the IPv4 route table.</p> <p>The route is created with the following fields specified in <b>MIB_IPDESTROW</b> and the <b>ForwardRow</b> member of <b>MIB_IPDESTROW</b>:</p> <ul style="list-style-type: none"> <li>▪ dwForwardDest</li> <li>▪ dwForwardMask</li> <li>▪ dwForwardPolicy</li> <li>▪ dwForwardNextHop</li> <li>▪ ForwardType</li> <li>▪ ForwardProto</li> <li>▪ dwForwardAge</li> <li>▪ dwForwardNextHopAS</li> <li>▪ dwForwardIfIndex</li> <li>▪ dwForwardProto</li> <li>▪ dwForwardMetric1</li> <li>▪ dwForwardMetric2</li> <li>▪ dwForwardMetric3</li> <li>▪ dwForwardMetric4</li> <li>▪ dwForwardMetric5</li> <li>▪ dwForwardPreference</li> </ul> <p>and the <b>dwForwardViewSet</b> field of <b>MIB_IPDESTROW</b>:</p> <ul style="list-style-type: none"> <li>▪ dwRtInfoDest</li> <li>▪ dwRtInfoMask</li> <li>▪ dwRtInfoNextHop</li> <li>▪ dwRtInfoIfIndex</li> <li>▪ dwRtInfoProto</li> </ul>



dwId Value	Structure that <b>MUST</b> be pointed to by rgbyData	Remarks
		<ul style="list-style-type: none"> <li>dwRtInfoMetric1</li> <li>dwRtInfoMetric2</li> <li>dwRtInfoMetric3</li> </ul> <p>The following fields are set to these values irrespective of the values specified in the <b>pMibInEntry</b>:</p> <ul style="list-style-type: none"> <li><b>dwForwardPolicy</b> is set to 0.</li> <li><b>dwForwardMetric4</b> and dwForwardMetric5 are set to MIB_IPROUTE_METRIC_UNUSED (-1).</li> <li><b>dwForwardPreference</b> is set to IP_PRIORITY_DEFAULT_METRIC (0x0000007f).</li> </ul>

If **pMibInEntry** is NULL, an error other than those specified in the return values table is returned. Otherwise the pointer to **pMibInEntry** is cast to a pointer to MIB\_OPAQUE\_INFO.

If **dwMibInEntrySize** does not match the size of MIB\_IPDESTROW an error other than those specified in the return values table is returned.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows **MUST** be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 26.

When processing this call, the RRASM server **MUST** do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.

- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error that the RRAS server may return while processing this request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.28 RMIBEntryDelete (Opnum 27)

The RMIBEntryDelete method [<278>](#) deletes a MIB entry in an IPv4 forwarding table. This causes the IPv4 routing table entry to be deleted.

```
DWORD RMIBEntryDelete(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
    [in] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the transport. The value of this field must be one of the following.

Value	Meaning
PID_IP 0x00000021	An IPv4 MIB entry is to be deleted.

**dwRoutingPid:** Specifies the routing protocol. This MUST be 0x2710 (10000) and indicates that *pInfoStruct* MUST point to [MIB\\_OPAQUE\\_QUERY \(section 2.2.1.2.54\)](#). Otherwise an error other than those specified in the return values table is returned.

**pInfoStruct:** This parameter MUST be a pointer to the structure [DIM\\_MIB\\_ENTRY\\_CONTAINER \(section 2.2.1.2.19\)](#) with valid **dwMibInEntrySize** and **pMibInEntry** fields. The parameters *dwMibOutEntrySize* and *pMibOutEntry* are ignored by the server. **dwMibInEntrySize** MUST be set to the size of data being passed in **pMibInEntry**.

**pMibInEntry** MUST be a pointer to MIB\_OPAQUE\_QUERY. **dwVarId** and **rgdwVarIndex** of MIB\_OPAQUE\_QUERY MUST be set to one of the following values that need to be deleted.

dwVarId Value	Structure that MUST to be pointed by rgdwVarIndex	Remarks
ROUTE_MATCHING 0x0000001f	<a href="#">MIB_IPDESTROW (section 2.2.1.2.20)</a> <ul style="list-style-type: none"> <li>▪ rgdwVarIndex[0] MUST be dwForwardDest</li> <li>▪ rgdwVarIndex[1] MUST be dwForwardMask</li> <li>▪ rgdwVarIndex[2] MUST</li> </ul>	A route with the following matching fields specified in ForwardRow and MIB_IPDESTROW is deleted from the IPv4 route table: <ul style="list-style-type: none"> <li>▪ dwForwardDest</li> <li>▪ dwForwardMask</li> <li>▪ dwForwardIfIndex</li> </ul>

dwVarId Value	Structure that MUST to be pointed by rgdwVarIndex	Remarks
	be dwForwardIfIndex <ul style="list-style-type: none"> <li>rgdwVarIndex[3] MUST be dwForwardNextHop</li> <li>rgdwVarIndex[4] MUST be dwForwardProto</li> </ul>	<ul style="list-style-type: none"> <li>dwForwardNextHop</li> <li>dwForwardProto</li> </ul>
IP_NETTABLE 0x00000009	<a href="#">MIB_IPNETTABLE (section 2.2.1.2.48)</a> rgdwVarIndex[0] MUST be dwIfIndex rgdwVarIndex[1] MUST be dwAddr	An entry is deleted<279> whose interface index matches the <b>dwIfIndex</b> and whose IPv4 address matches the specified <b>dwAddr</b> .

If **pMibInEntry** is NULL, an error other than those specified in the return value table is returned. Otherwise, the pointer to **pMibInEntry** is cast to a pointer to a MIB\_OPAQUE\_QUERY.

If *pInfoStruct* is NULL, an error other than those specified in the following return value table is returned.

If **dwMibInEntrySize** does not match the size of **MIB\_IPDESTROW** (section 2.2.1.2.20) an error other than those specified in the return value table is returned.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the following table MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 27.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- Validate that the *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.

- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status returned by the RRAS server while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.29 RMIBEntrySet (Opnum 28)

The **RMIBEntrySet** method [<280>](#) modifies an MIB entry in the IPv4 forwarding table.

```
DWORD RMIBEntrySet(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
    [in] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the transport protocol. The value of this parameter MUST be PID\_IP. The method MUST return an error other than those specified in the return value table for any other value.

Value	Meaning
PID_IP 0x00000021	An IPv4 MIB entry is to be deleted.

**dwRoutingPid:** Specifies the routing protocol. This MUST be 0x2710 (10000) and indicate that *pInfoStruct* MUST point to [MIB\\_OPAQUE\\_QUERY \(section 2.2.1.2.54\)](#). Otherwise, an error other than those specified in the return table value is returned.

**pInfoStruct:** This MUST be a pointer to the structure [DIM\\_MIB\\_ENTRY\\_CONTAINER \(section 2.2.1.2.19\)](#) with valid **dwMibInEntrySize** and **pMibInEntry** fields. The **dwMibOutEntrySize** and **pMibOutEntry** of the structure are ignored by the server for this method.

**dwMibInEntrySize** MUST be set to the size of data being passed in **pMibInEntry**. If *pInfoStruct* is NULL, an error other than those specified in the return value table is returned. Otherwise, the pointer is treated as a pointer to the structure DIM\_MIB\_ENTRY\_CONTAINER.

Since the *dwRoutingPid* parameter of this method MUST take a value IPRTRMGR\_PID, the **pMibInEntry** field of *pInfoStruct* MUST be a pointer to [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#). The **dwId** and **rgbyData** fields of MIB\_OPAQUE\_INFO MUST be set to one of the values in the following table.

dwId Value	Structure that MUST be pointed to by rgbyData	Remarks
ROUTE_MATCHING 0x0000001f	<a href="#">MIB_IPDESTROW (section 2.2.1.2.20)</a>	A route corresponding to data in <b>rgbyData</b> is added in the IPv4 route table.  The route is created with the following fields specified in MIB_IPDESTROW and the <b>ForwardRow</b> member of MIB_IPDESTROW:

dwId Value	Structure that <b>MUST</b> be pointed to by rgbyData	Remarks
		<ul style="list-style-type: none"> <li>▪ dwForwardDest</li> <li>▪ dwForwardMask</li> <li>▪ dwForwardPolicy</li> <li>▪ dwForwardNextHop</li> <li>▪ ForwardType</li> <li>▪ ForwardProto</li> <li>▪ dwForwardAge</li> <li>▪ dwForwardNextHopAS</li> <li>▪ dwForwardMetric1</li> <li>▪ dwForwardMetric2</li> <li>▪ dwForwardMetric3</li> <li>▪ dwForwardMetric4</li> <li>▪ dwForwardMetric5</li> <li>▪ dwForwardPreference</li> <li>▪ dwForwardViewSet</li> <li>▪ dwRtInfoDest</li> <li>▪ dwRtInfoMask</li> <li>▪ dwRtInfoNextHop</li> <li>▪ dwRtInfoIfIndex</li> <li>▪ dwRtInfoProto</li> <li>▪ dwRtInfoMetric1</li> <li>▪ dwRtInfoMetric2</li> <li>▪ dwRtInfoMetric3</li> </ul> <p>The following fields are set to these values irrespective of the values specified:</p> <ul style="list-style-type: none"> <li>▪ <b>dwForwardPolicy</b> is set to 0.</li> <li>▪ <b>dwForwardMetric4</b> and <b>dwForwardMetric5</b> are set to MIB_IPROUTE_METRIC_UNUSED (-1).</li> <li>▪ <b>dwForwardPreference</b> is set to IP_PRIORITY_DEFAULT_METRIC (0x0000007f).</li> </ul>

<b>dwId Value</b>	<b>Structure that MUST be pointed to by rgbyData</b>	<b>Remarks</b>
IF_ROW 0x00000002	<a href="#">MIB_IFROW (section 2.2.1.2.29)</a>	Only <b>dwAdminStatus</b> can be set to IF_ADMIN_STATUS_DOWN or IF_ADMIN_STATUS_UP (see <b>dwAdminStatus</b> of <a href="#">INTERFACE_STATUS_INFO (section 2.2.1.2.18)</a> ).
MCAST_IF_ENTRY 0x00000017	<a href="#">MIB_IPMCAST_IF_ENTRY (section 2.2.1.2.40)</a>	<b>dwTtl</b> MUST be set to less than or equal to 255. <b>dwRateLimit</b> MUST NOT be set to 0. <b>dwIfIndex</b> MUST be set to the index of the interface for which the entries are being updated. The following entries can be set only if the operational status of the interface is IF_OPER_STATUS_OPERATIONAL (see <b>dwOperStatus</b> of MIB_IFROW: <b>ulInMcastOctets</b> <b>ulOutMcastOctets</b>
MCAST_BOUNDARY 0x0000001a	<a href="#">MIB_IPMCAST_BOUNDARY (section 2.2.1.2.37)</a>	If <b>dwStatus</b> is set to ROWSTATUS_CREATEANDGO, the boundary information specified in MIB_IPMCAST_BOUNDARY is created. If <b>dwStatusfield</b> is set to ROWSTATUS_DESTROY, the boundary information specified in MIB_IPMCAST_BOUNDARY is deleted.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client.

<b>Return value/code</b>	<b>Description</b>
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

All error values MUST be treated the same and as long as ERROR\_SUCCESS is not returned, the call should be deemed failed.

The opnum field value for this method is 28.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).

- If *pInfoStruct* is NULL, return an error other than specified those in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status that the RRAS server might return while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.30 RMIBEntryGet (Opnum 29)

The **RMIBEntryGet** method [<281>](#) retrieves the value of a RRAS MIB entry that corresponds to the transport and that matches the information specified in *pInfoStruct*.

```
DWORD RMIBEntryGet(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
    [in, out] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the transport protocol. The value of this parameter MUST be one from the following table. The method MUST return an error for any other values.

Value	Meaning
PID_IP 0x00000021	An IPv4 MIB entry is to be retrieved.
PID_IPX 0x0000002B	An IPX <a href="#">&lt;282&gt;</a> MIB entry is to be retrieved.
PID_IPV6 0x00000057	IPv6. <a href="#">&lt;283&gt;</a>

**dwRoutingPid:** If *dwPid* is PID\_IP and if *dwRoutingPid* is 10000, then **pMibInEntry** MUST point to [MIB\\_OPAQUE\\_QUERY](#) (section [2.2.1.2.54](#)). The **dwVarId** field of MIB\_OPAQUE\_QUERY MUST be one of the following values. **pMibOutEntry** MUST be interpreted as a pointer to MIB\_OPAQUE\_QUERY.

See section [2.2.1.2.54](#) for details on the structure retrieved by the **rgdwVarIndex** field of MIB\_OPAQUE\_QUERY for different **dwVarId** values.

dwVarId Value	Meaning
IF_NUMBER 0x00000000	Number of interfaces on the machine.
IF_TABLE	Information about interface table.

<b>dwVarId Value</b>	<b>Meaning</b>
0x00000001	
IF_ROW 0x00000002	Information about a particular interface.
IP_STATS 0x00000003	Information about the IP protocol.
IP_ADDRTABLE 0x00000004	Table of IPv4 address entries.
IP_ADDRROW 0x00000005	Information for a particular IPv4 address.
IP_FORWARDNUMBER 0x00000006	Information about number of routes in a particular IP routing table.
IP_FORWARDTABLE 0x00000007	Table of IPv4 route entries.
IP_NETTABLE 0x00000009	Table of ARP entries for IPv4 addresses.
IP_NETROW 0x0000000a	Information about an ARP table entry for an IPv4 address.
ICMP_STATS 0x0000000b	Statistics for ICMP messages on a particular computer.
TCP_STATS 0x0000000c	Statistics for the TCP protocol running on the local computer.
UDP_STATS 0x0000000f	Statistics for the UDP running on the local computer.
MCAST_MFE 0x00000012	Information for an IP multicast forwarding entry.
MCAST_MFE_STATS 0x00000013	Statistics associated with an MFE.
MCAST_IF_ENTRY 0x00000017	Information about an IP multicast interface.
ROUTE_MATCHING 0x0000001f	Information about a matching IP route.
BEST_IF 0x00000014	Index of the interface that has the best route to a particular destination IPv4 address.
MCAST_GLOBAL 0x00000018	Global information for IP multicast on a particular computer.



dwVarId Value	Meaning
IF_STATUS 0x00000019	Status information for a particular interface.
MCAST_BOUNDARY 0x0000001a	Information about a router's scoped IPv4 multicast address boundaries.
MCAST_SCOPE 0x0000001b	Information about a multicast scope.

If *dwPid* is `PID_IPv6` and *dwRoutingPid* is 10000, then **pMibInEntry** MUST point to `MIB_OPAQUE_QUERY` (section 2.2.1.2.54). The **dwVarId** field of **pMibInEntry** MUST be one of the following values. **pMibOutEntry** MUST be interpreted as a pointer to `MIB_OPAQUE_QUERY`.

See section [2.2.1.2.54](#) for details on the structure retrieved by the **rgdwVarIndex** field of `MIB_OPAQUE_QUERY` for different **dwVarId** values.

dwVarId Value	Meaning
0x00000001 IF_TABLE	Information about interface table.
0x00000008 IP_FORWARDROW	Information about an IPv6 network route.

If *dwPid* is `PID_IP` and if *dwRoutingPid* is not `IPRTRMGR_PID` (0x00002710), then *dwRoutingPid* MUST be one of the entries in the **Value** column and *pMibInEntry* MUST be the corresponding entry in the **Structure to be pointed to by pMibInEntry** in the following table. The routing protocols specified in the following table are valid only if the protocol is already initialized by RRAS for IPv4. RRAS initializes a protocol when a `RTR_TOC_ENTRY` with the **InfoType** corresponding to the protocol is present in the global configuration. The [RRouterInterfaceTransportSetGlobalInfo](#) method enables specifying the global configuration through the **pGlobalInfo** member of **pInfoStruct**.

Value	Meaning	Structure to be pointed to by pMibInEntry.	Remarks
MS_IP_BOOTP 0x0000270f	An entry in <code>IBOOTPMIB</code> needs to be retrieved.	<code>IPBOOTP_MIB_GET_INPUT_DATA</code>	See section <a href="#">2.2.1.2.153</a> for details on how to populate <code>IPBOOTP_MIB_GET_INPUT_DATA</code> to retrieve different types of MIB entries.  When this method returns <b>pMibOutEntry</b> , <i>pInfoStruct</i> MUST be cast to <a href="#">IPBOOTP_MIB_GET_OUTPUT_DATA</a> . See section <a href="#">2.2.1.2.158</a> on how to interpret the data returned.
MS_IP_NAT 0x81372715	An entry in the NAT MIB	<code>IP_NAT_MIB_QUERY</code>	See <a href="#">IP_NAT_MIB_QUERY</a> (section 2.2.1.2.182) for details on how to populate this

Value	Meaning	Structure to be pointed to by pMibInEntry.	Remarks
	needs to be retrieved.		structure to retrieve the entries required. The values are returned in IP_NAT_MIB_QUERY.
MS_IP_DNS_PROXY 0x81372713	An entry in DNS Proxy MIB needs to be retrieved.	IP_DNS_PROXY_MIB_QUERY	See section <a href="#">2.2.1.2.186</a> for details on how to populate IP_DNS_PROXY_MIB_QUERY. The values are returned in IP_DNS_PROXY_MIB_QUERY.
MS_IP_DHCP_ALLOCA TOR 0x81372714	An entry in auto DHCP MIB is retrieved.	IP_AUTO_DHCP_MIB_QUERY	See section <a href="#">2.2.1.2.188</a> for details on how to populate IP_AUTO_DHCP_MIB_QUERY. The values are returned in the same structure.
MS_IP_OSPF< <a href="#">284</a> > 0x0000000d	An entry in OSPF MIB needs to be retrieved.	MIB_DA_MSG MIB_DA_MSG OSPF_GLOBAL_PARAM OSPF_ROUTE_FILTER_INFO OSPF_PROTO_FILTER_INFO OSPF_AREA_PARAM OSPF_AREA_RANGE_PARAM OSPF_VIRT_INTERFACE_P ARAM OSPF_NBMA_NEIGHBOR_PA RAM	

If *dwPid* is PID\_IPV6 and if *dwRoutingPid* is not IPRTRMGR\_PID (0x00002710), then *dwRoutingPid* MUST be one of the entries in the **Value** column and **pMibInEntry** MUST be the corresponding entry in the **Structure to be pointed to by pMibInEntry** in the following table. The routing protocols specified in the following table are valid only if the protocol is already initialized by RRAS for IPv6. RRAS initializes a protocol when a RTR\_TOC\_ENTRY with the **InfoType** corresponding to the protocol is present in the global configuration. The **RRouterInterfaceTransportSetGlobalInfo** method enables specifying the global configuration through the **pGlobalInfo** member of **pInfoStruct**.

Value	Meaning	Structure to be pointed to by pMibInEntry	Remarks
MS_IPV6_DHC P 0x000003E7	An entry in DHCPv6 Relay agent MIB needs to be retrieved	DHCPV6R_MIB_GET_INPUT_DATA	See section <a href="#">2.2.1.2.161</a> on how to populate DHCPV6R_MIB_GET_INPUT_DATA. The values are returned in DHCPV6R_MIB_GET_OUTPUT_DATA.

Value	Meaning	Structure to be pointed to by pMibInEntry	Remarks
	.		

**pInfoStruct:** This MUST be a pointer to the structure [DIM\\_MIB\\_ENTRY\\_CONTAINER \(section 2.2.1.2.19\)](#) with valid **dwMibInEntrySize** and **pMibInEntry** fields. **dwMibInEntrySize** MUST be set to the size of data being passed in **pMibInEntry**. **dwMibOutEntrySize** and **pMibOutEntry** are populated by the server. The caller should free the memory pointed to by *pInfoStruct*.

If *dwPid* is `PID_IPX`, *dwRoutingPid* MUST be one of the entries in the Value column and *pMibInEntry* MUST be the corresponding entry in the Structure to be pointed to by *pMibInEntry* in the return values table.

Value	Meaning	Structure to be pointed to by pMibInEntry.	Remarks
IPX_PROTOCOL_BASE 0x00000000	IPX related information. The call was successful.	IPX_MIB_GET_INPUT_DATA	See section <a href="#">2.2.1.2.106</a> for details on how to populate <code>IPX_MIB_GET_INPUT_DATA</code> to retrieve different types of MIB entries and how to interpret the data returned.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of `ERROR_SUCCESS` (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 <code>ERROR_SUCCESS</code>	The call was successful.
0x00000005 <code>ERROR_ACCESS_DENIED</code>	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 29.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error `ERROR_ACCESS_DENIED` (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.

- Return any error status returned by the RRAS server while processing the request. Otherwise, fill the MIB information returned by the RRAS server in the *pInfoStruct* and return `ERROR_SUCCESS`.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.31 RMIBEntryGetFirst (Opnum 30)

The **RMIBEntryGetFirst** method [<285>](#) retrieves the first value of an entry corresponding to the transport, protocol, and the MIB entry specified in *pInfoStruct*.

```
DWORD RMIBEntryGetFirst(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
    [in, out] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the transport protocol. The value of this parameter **MUST** be one from the following table.

Value	Meaning
PID_IP 0x00000021	An IPv4 MIB entry is to be retrieved.
PID_IPX 0x0000002B	An IPX MIB entry is to be retrieved. <a href="#">&lt;286&gt;</a>
PID_IPV6 0x00000057	An IPv6 entry is to be retrieved. <a href="#">&lt;287&gt;</a>

**dwRoutingPid:** If *dwPid* is `PID_IP` and if *dwRoutingPid* is 10000, then **pMibInEntry** **MUST** point to [MIB\\_OPAQUE\\_QUERY](#) (section 2.2.1.2.54). The **dwVarId** field of `MIB_OPAQUE_QUERY` **MUST** be one of the following values. **pMibOutEntry** **MUST** be interpreted as a pointer to `MIB_OPAQUE_QUERY`.

See section [2.2.1.2.54](#) for details on the structure retrieved by the **rgdwVarIndex** field of `MIB_OPAQUE_QUERY` for different **dwVarId** values.

dwVarId Value	Meaning
IF_ROW 0x00000002	Information about a particular interface.
IP_ADDRROW 0x00000005	Information for a particular IPv4 address.
IP_NETROW 0x0000000a	Information about an ARP table entry for an IPv4 address.
MCAST_MFE	Information for an IP multicast forwarding entry.

dwVarId Value	Meaning
0x00000012	
MCAST_MFE_STATS 0x00000013	Statistics associated with an MFE.
MCAST_IF_ENTRY 0x00000017	Information about an IP multicast interface.
IF_STATUS 0x00000019	Status information for a particular interface.
MCAST_BOUNDARY 0x0000001a	Information about a router's scoped IPv4 multicast address boundaries.
MCAST_SCOPE 0x0000001b	Information about a multicast scope.

If *dwPid* is `PID_IPv6` and *dwRoutingPid* is 10000, then **pMibInEntry** MUST point to `MIB_OPAQUE_QUERY` (section 2.2.1.2.54). The **dwVarId** field of **pMibInEntry** MUST be one of the following values. **pMibOutEntry** MUST be interpreted as a pointer to `MIB_OPAQUE_QUERY`.

See section [2.2.1.2.54](#) for details on the structure retrieved by the **rgdwVarIndex** field of `MIB_OPAQUE_QUERY` for different **dwVarId** values.

dwVarId Value	Meaning
0x00000008 IP_FORWARDROW	Information about an IPv6 network route.

If *dwPid* is `PID_IP` and if *dwRoutingPid* is not `IPRTRMGR_PID` (0x00002710), then *dwRoutingPid* MUST be one of the entries in the **Value** column and *pMibInEntry* MUST be the corresponding entry in the **Structure to be pointed to by pMibInEntry** in the following table. The following specified routing protocols are valid only if the protocol is already initialized by RRAS for IPv4. RRAS initializes a protocol when an `RTR_TOC_ENTRY` with the **InfoType** corresponding to the protocol is present in the global configuration. The [RRouterInterfaceTransportSetGlobalInfo](#) method enables specifying the global configuration through the **pGlobalInfo** member of **pInfoStruct**.

Value	Meaning	Structure to be pointed to by pMibInEntry.	Remarks
MS_IP_BOOTP 0x0000270f	An entry in <code>IBOOTPMIB</code> needs to be retrieved.	<code>IPBOOTP_MIB_GET_INPUT_DATA</code>	See section <a href="#">2.2.1.2.153</a> for details on how to populate <code>IPBOOTP_MIB_GET_INPUT_DATA</code> to retrieve different types of MIB entries.  When this method returns <b>pMibOutEntry</b> , <i>pInfoStruct</i> MUST be cast to <a href="#">IPBOOTP_MIB_GET_OUTPUT_DATA</a> . See section <a href="#">2.2.1.2.158</a> on how to interpret the data

Value	Meaning	Structure to be pointed to by pMibInEntry.	Remarks
			returned.
MS_IP_NAT 0x81372715	An entry in the NAT MIB needs to be retrieved.	IP_NAT_MIB_QUERY	See <a href="#">IP_NAT_MIB_QUERY (section 2.2.1.2.182)</a> for details on how to populate this structure to retrieve the entries required. The values are returned in IP_NAT_MIB_QUERY.
MS_IP_DNS_PROXY 0x81372713	An entry in DNS Proxy MIB needs to be retrieved.	IP_DNS_PROXY_MIB_QUERY	See section <a href="#">2.2.1.2.186</a> for details on how to populate IP_DNS_PROXY_MIB_QUERY. The values are returned in IP_DNS_PROXY_MIB_QUERY.
MS_IP_DHCP_ALLOCA TOR 0x81372714	An entry in auto DHCP MIB is retrieved.	IP_AUTO_DHCP_MIB_QUERY	See section <a href="#">2.2.1.2.188</a> for details on how to populate IP_AUTO_DHCP_MIB_QUERY. The values are returned in the same structure.
MS_IP_OSPF< <a href="#">288</a> > 0x0000000d	An entry in OSPF MIB needs to be retrieved.	MIB_DA_MSG MIB_DA_MSG OSPF_GLOBAL_PARAM OSPF_ROUTE_FILTER_INFO OSPF_PROTO_FILTER_INFO OSPF_AREA_PARAM OSPF_AREA_RANGE_PARAM OSPF_VIRT_INTERFACE_P AM OSPF_NBMA_NEIGHBOR_P ARAM	

If *dwPid* is `PID_IPV6` and if *dwRoutingPid* is not `IPRTRMGR_PID` (0x00002710), then *dwRoutingPid* MUST be one of the entries in the **Value** column and **pMibInEntry** MUST be the corresponding entry in the **Structure to be pointed to by pMibInEntry** in the following table. The following specified routing protocols are valid only if the protocol is already initialized by RRAS for IPv6. RRAS initializes a protocol when an `RTR_TOC_ENTRY` with the **InfoType** corresponding to the protocol is present in the global configuration. The **RRouterInterfaceTransportSetGlobalInfo** method enables specifying the global configuration through the **pGlobalInfo** member of **pInfoStruct**.

Value	Meaning	Structure to be pointed to by pMibInEntry	Remarks
MS_IPV6_DHC P 0x000003E7	An entry in DHCPv6 Relay agent	DHCPV6R_MIB_GET_INPUT_DATA	See section <a href="#">2.2.1.2.161</a> on how to populate DHCPV6R_MIB_GET_INPUT_DATA. The values are returned in DHCPV6R_MIB_GET_OUTPUT_DATA

Value	Meaning	Structure to be pointed to by pMibInEntry	Remarks
	MIB needs to be retrieved		A.

**pInfoStruct:** The same as in [RMIBEntryGet \(section 3.1.4.30\)](#).

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 30.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status returned by the RRAS server while processing the request. Otherwise fill the MIB information returned by the RRAS server in the *pInfoStruct* and return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.32 RMIBEntryGetNext (Opnum 31)

The **RMIBEntryGetNext** method [<289>](#) retrieves the next (to the previous call) entry corresponding to the transport, protocol, and the MIB entry specified in *pInfoStruct*.

```
DWORD RMIBEntryGetNext(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
```

```
[in, out] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** The same as in [RMIBEntryGet \(section 3.1.4.30\)](#).

**dwRoutingPid:** The same as in [RMIBEntryGetFirst \(section 3.1.4.31\)](#).

**pInfoStruct:** The same as in [RMIBEntryGet \(section 3.1.4.30\)](#).

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .
0x00000103 ERROR_NO_MORE_ITEMS	No more data available.

The opnum field value for this method is 31.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status returned by the RRAS server while processing the request. Otherwise fill the MIB information returned by the RRAS server in the *pInfoStruct*. If there are no more MIB entries to be returned, the RRAS server MUST return ERROR\_NO\_MORE\_ITEMS [<290>](#); otherwise, return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.33 RMIBGetTrapInfo (Opnum 32)

The **RMIBGetTrapIn** method [<291>](#) queries the module that set a trap event for more information about the trap. This method cannot be called remotely.

```
DWORD RMIBGetTrapInfo(
```



```

[in] DIM_HANDLE hDimServer,
[in] DWORD dwPid,
[in] DWORD dwRoutingPid,
[in, out] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);

```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the transport protocol. The value of this parameter MUST be one from the following table.

Value	Meaning
PID_IP 0x00000021	An IPv4 MIB entry is to be retrieved.
PID_IPX 0x0000002B	An IPX MIB entry is to be retrieved. <a href="#">&lt;292&gt;</a>
PID_IPV6 0x00000057	An IPv6 entry is to be retrieved. <a href="#">&lt;293&gt;</a>

**dwRoutingPid:** Specifies the routing protocol that exported the variable.

**pInfoStruct:** Pointer to an opaque data structure [DIM\\_MIB\\_ENTRY\\_CONTAINER \(section 2.2.1.2.19\)](#). The data structure's format is determined by the router manager or router manager client that is servicing the call. The data structure MUST contain information that specifies the variable being created and the value to assign to the variable.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 32.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If not, then return error ERROR\_ACCESS\_DENIED.
- If *pInfoStruct* is NULL, return an error other than one of the errors specified in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than those specified in the preceding table.

- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, return the information in pInfoStruct and with the information provided by the RRAS server and return ERROR\_SUCCESS. Otherwise return the error result provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.34 RMIBSetTrapInfo (Opnum 33)

The **RMIBGetTrapInfo** method [<294>](#) specifies a handle to an event that is signaled whenever a TRAP needs to be issued. [<295>](#)

```
DWORD RMIBSetTrapInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwPid,
    [in] DWORD dwRoutingPid,
    [in] ULONG_PTR hEvent,
    [in] DWORD dwClientProcessId,
    [in, out] PDIM_MIB_ENTRY_CONTAINER pInfoStruct
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwPid:** Specifies the protocol ID that exported the variable.

**dwRoutingPid:** Specifies the routing protocol that exported the variable.

**hEvent:** A handle to an event that is signaled when a trap needs to be issued. This MUST be a handle to an event on the RRAS server which is created within the process specified by **dwClientProcessId** which can be signaled whenever a TRAP needs to be issued. Otherwise the method SHOULD fail with an appropriate error code as specified in [\[MS-ERREF\]](#).

**dwClientProcessId:** The current process identifier.

**pInfoStruct:** Pointer to an opaque data structure [DIM MIB ENTRY CONTAINER \(section 2.2.1.2.19\)](#). The data structure's format is determined by the router manager or router manager client that is servicing the call. The data structure MUST contain information that specifies the variable being created and the value to assign to the variable.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

Return value/code	Description
0x0000007A ERROR_INSUFFICIENT_BUFFER	

The opnum field value for this method is 33.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If not, then return error ERROR\_ACCESS\_DENIED.
- If *pInfoStruct* is NULL, return an error other than one of the errors specified in the preceding table.
- If *dwPid* is not specified in the **SupportedTransportsList**, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, return ERROR\_SUCCESS. Otherwise return the error result provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.35 RRasAdminConnectionNotification (Opnum 34)

The **RRasAdminConnectionNotification** method [<296>](#) registers an event object with the RRAS server so that, if an interface connects or disconnects, the event is signaled. The *hDimServer* handle specifies on which RRAS server the call is to be executed. [<297>](#)

```
DWORD RRasAdminConnectionNotification(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD fRegister,
    [in] DWORD dwClientProcessId,
    [in] ULONG_PTR hEventNotification
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**fRegister:** This is of type **DWORD** and SHOULD be set to 1, if notifications are required when an interface is connected or disconnected. Set to 0 to unregister notifications.

**dwClientProcessId:** The current process identifier that determines where the function is called from.

**hEventNotification:** A handle to an event that is signaled after the connection is connected or disconnected. This MUST be a handle to an event on the RRASM server which is created within the process specified by **dwClientProcessId** which can be signaled on interface connect and disconnect events. Otherwise the method SHOULD fail with an appropriate error code as specified in [\[MS-ERREF\]](#).

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully;

otherwise, it contains an error code, as specified in [MS-ERREF] or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 34.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If not, then return error ERROR\_ACCESS\_DENIED.
- If *hEventNotification* is NULL, return an error other than those specified in the preceding table.
- If *RouterType* is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status the RRAS server might return while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.36 RRasAdminSendUserMessage (Opnum 35)

The **RRasAdminSendUserMessage** method [<298>](#) sends a message to the user connected on the connection specified by *hDimServer*. [<299>](#)

```
DWORD RRasAdminSendUserMessage(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD hDimConnection,  
    [in, string] LPWSTR lpwszMessage  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hDimConnection:** This is of type **DWORD** and MUST be set to a particular connection identifier for which the connection information is required. Obtain this handle by calling [RRasAdminConnectionEnum \(section 3.1.4.2\)](#). Since RRASM server does not maintain the connection handles, the RRAS server SHOULD check and ensure that this handle represents a valid interface handle.

**lpwszMessage:** A pointer to a Unicode string that specifies the message to the user. It MUST NOT be NULL.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 35.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *RouterType* is ROUTER\_TYPE\_LAN, return an error other than those specified in the preceding table.
- If *lpwszMessage* is NULL, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status the RRAS server might return while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.37 RRouterDeviceEnum (Opnum 36)

The **RRouterDeviceEnum** method [<300>](#) retrieves the list of all the devices from the specified server. The *hDimServer* handle specifies the RRAS server on which the call is executed. The caller MUST pass a pointer to a valid [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), where DIM\_INFORMATION\_CONTAINER.dwBufferSize is initialized to zero. The caller SHOULD free the memory pointed to by pInfoStruct->pBuffer.

```

DWORD RRouterDeviceEnum(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in, out] LPDWORD lpdwTotalEntries
);

```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to the following value.

Value	Meaning
0	After the function returns the memory pointed to by pInfoStruct->pBuffer it should be interpreted as array of <a href="#">MPR_DEVICE 0 (section 2.2.1.2.86)</a> . The size of the array is determined by <i>lpdwEntriesRead</i> .

**pInfoStruct:** This is a pointer of type **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1), and pInfoStruct.dwBufferSize is initialized to zero. Upon successful return, the pInfoStruct->pBuffer is a typecast array of **MPR\_DEVICE\_0** (section 2.2.1.2.86) and the array size is determined by the value to pointer *lpdwTotalEntries*.

**lpdwTotalEntries:** This is a pointer to type **DWORD** and receives the total number of devices that have been enumerated.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of **ERROR\_SUCCESS** (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 36.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section 2.1.1.1, whether this method was called by a client that has access to the method. If the client does not have access, then return error **ERROR\_ACCESS\_DENIED** (0x00000005).
- If *pInfoStruct* is NULL, return an error other than one of the errors in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server completes the request successfully, place the returned information in **pInfoStruct** and set *lpdwTotalEntries* to the number of entries returned by RRAS server and return **ERROR\_SUCCESS**.
- Otherwise return the error status provided by RRAS Server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.38 RRouterInterfaceTransportCreate (Opnum 37)

The **RRouterInterfaceTransportCreate** method [<301>](#) is used to create a new transport on the RRAS server.

```
DWORD RRouterInterfaceTransportCreate(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwTransportId,
    [in, string] LPWSTR lpwsTransportName,
    [in] PDIM_INTERFACE_CONTAINER pInfoStruct,
    [in, string] LPWSTR lpwsDLLPath
```

);

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwTransportId:** Specifies the transport for which the information is set (IPv4, IPv6, or IPX).

It MUST be set to one of the following values.

Value	Meaning
PID_IPX 0x0000002B	IPX protocol <a href="#">&lt;302&gt;</a>
PID_IP 0x00000021	IPv4 protocol
PID_IPV6 0x00000057	IPv6 protocol <a href="#">&lt;303&gt;</a>

**lpwsTransportName:** Pointer to a null-terminated Unicode string that specifies the name of the transport being added. If this parameter is not specified, the *dwTransportId* parameter is converted into a string and used as the transport name.

**pInfoStruct:** Pointer to a [DIM\\_INTERFACE\\_CONTAINER \(section 2.2.1.2.2\)](#). This MUST NOT be NULL. The **pGlobalInfo** member of the **DIM\_INTERFACE\_CONTAINER** MUST NOT be NULL and MUST point to a valid [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) and [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#).

If *dwTransportId* is PID\_IP or PID\_IPV6, one or more of the following entries MUST be set in the **InfoType** field in the RTR\_TOC\_ENTRY (section 2.2.1.2.4) structure while passing to the method.

Value	Meaning and conditions	Structure pointed to at offset
IP_PROT_PRIORITY_INFO 0xffff0006	IPv4 and IPv6 route priority information is specified.	<a href="#">PRIORITY_INFO (section 2.2.1.2.12)</a>
IPV6_GLOBAL_INFO 0xffff000f	Global IPv6 logging and filtering information.	<a href="#">GLOBAL_INFO (section 2.2.1.2.9)</a>
IP_GLOBAL_INFO 0xffff0003	Global IPv4 logging and filtering information.	GLOBAL_INFO (section 2.2.1.2.9)

**lpwsDLLPath:** Pointer to a null-terminated Unicode string that specifies the name of the router manager DLL for the specified transport. If this name is specified, the function sets the DLL path for this transport to this name. [<304>](#)

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 37.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than one of the errors specified in the preceding table.
- If *dwTransportId* is not specified in the **SupportedTransportsList**, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status returned by the RRAS server. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.39 RRouterInterfaceDeviceGetInfo (Opnum 38)

The **RRouterInterfaceDeviceGetInfo** method [<305>](#) retrieves information for a specified device, *dwIndex*, for a specified interface *hInterface*, on a specified server, *hDimServer*.

```

DWORD RRouterInterfaceDeviceGetInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in] DWORD dwIndex,
    [in] DWORD hInterface
);

```

**hDimServer:** A handle to the RRAS server where the call is executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to any of the following values.

Value	Meaning
0	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">MPR_DEVICE 0 (section 2.2.1.2.86)</a> .
1	After the function returns, the memory pointed to by <i>pInfoStruct-&gt;pBuffer</i> is interpreted as <a href="#">MPR_DEVICE 1 (section 2.2.1.2.87)</a> .



**pInfoStruct:** This is a pointer of type [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) and pInfoStruct.dwBufferSize SHOULD be initialized to zero. Upon successful return, the pInfoStruct->pBuffer is a typecast array of [MPR\\_DEVICE\\_0](#) or [MPR\\_DEVICE\\_1](#), based on the dwLevel value.

**dwIndex:** Specifies the one-based index of the device. A multilinked demand-dial interface uses multiple devices.

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM server does not maintain interface handles, the RRAS server SHOULD check and ensure that this handle represents a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values not in the following table MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 38.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If pInfoStruct is NULL, return an error other than those in the preceding table.
- If dwLevel is not supported, return an error other than those in the preceding table.
- Call the abstract interface Invoke DIMSVC Method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, fill the returned information in pInfoStruct and return ERROR\_SUCCESS. Otherwise return the ERROR\_STATUS returned by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.40 RRouterInterfaceDeviceSetInfo (Opnum 39)

The **RRouterInterfaceDeviceSetInfo** method [<306>](#) sets the information for a specified device, dwIndex, for a specified interface, hInterface, on a specified server, hDimServer.

```
DWORD RRouterInterfaceDeviceSetInfo(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD dwLevel,  
    [in] PDIM_INFORMATION_CONTAINER pInfoStruct,
```

```

[in] DWORD dwIndex,
[in] DWORD hInterface
);

```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to one of the following values.

Value	Meaning
0	pInfoStruct->pBuffer MUST be set to point to <a href="#">MPR_DEVICE_0 (section 2.2.1.2.86)</a> .
1	pInfoStruct->pBuffer MUST be set to point to <a href="#">MPR_DEVICE_1 (section 2.2.1.2.87)</a> .

**pInfoStruct:** This is a pointer of type [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) and MUST be set to the following, based on *dwLevel*. The *szDeviceName* MUST be one of the devices as specified by [RRouterDeviceEnum](#). The **szDeviceType** specified in the structure SHOULD be validated against the actual type of the device specified by *szDeviceName*. If the **szDeviceType** is incorrect, the actual device type SHOULD be used by the server instead.

dwLevel	pInfoStruct->size	pInfoStruct->pBuffer
0	Should be set to the size of <b>MPR_DEVICE_0</b> (section 2.2.1.2.86).	This MUST be set to point to <b>MPR_DEVICE_0</b> .
1	Should be set to the size of <b>MPR_DEVICE_1</b> (section 2.2.1.2.87).	This MUST be set to a point to <b>MPR_DEVICE_1</b> .

**dwIndex:** Specifies the 1-based index of the device. A multilinked demand-dial interface uses multiple devices. If the device information specified for *dwIndex* 1 is either a PPPoE interface or a VPN interface, any other device information, specified (with *dwIndex* > 1), SHOULD be ignored. If the device information specified for *dwIndex* 1 is a serial or ISDN device, the connection SHOULD be treated as a multilink-capable connection. Any other device information, specified (with *dwIndex* > 1), SHOULD be treated as device information for the individual links. Device information with type **szDeviceType**, which is neither modem nor ISDN, SHOULD [<307>](#) be ignored.

**hInterface:** The unique identifier of an interface. This can be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). Since the RRASM server does not maintain the interface handles, the RRAS server implementation SHOULD check and ensure that this handle represents a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005	The calling application does not have sufficient privileges.

Return value/code	Description
ERROR_ACCESS_DENIED	

The opnum field value for this method is 39.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED.
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- Return the error status that may be returned by the RRAS server while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.41 RRouterInterfaceSetCredentialsEx (Opnum 40)

The **RRouterInterfaceSetCredentialsEx** method [<308>](#) is used to set extended **credentials** (other than username and password) information for an interface. This function is used to set credentials information used for the EAP methods or used as a key that is shared between two routers (a preshared key).

```
DWORD RRouterInterfaceSetCredentialsEx(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in] PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in] DWORD hInterface
);
```

**hDimServer:** A handle to the RRASM server where the call should be executed, see section [3.1.3](#).

**dwLevel:** Specifies the format of the credentials information. This parameter MUST be one of the following values: 0x00000000, 0x00000001, 0x00000002, or 0x00000003. A value of zero indicates that this is EAP information, and the [MPR\\_CREDENTIALSEX\\_1](#) structure MUST contain [EAPTLS\\_USER\\_PROPERTIES \(section 2.2.1.2.129\)](#). A value of one, two, or three (these can be used interchangeably) indicate that the credentials information is a preshared key and is formatted as an MPR\_CREDENTIALSEX\_1 structure. The preshared key specifies the preshared key to be used with IPsec for L2TP over IPsec connections.

**pInfoStruct:** Pointer to the [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#), the **pBuffer** pointer of which points to the MPR\_CREDENTIALSEX\_1 structure that contains the credential information to be set for the interface.

**hInterface:** Handle to the interface. This may be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). If *dwLevel* is 0x00000002 and *hInterface* is NULL, the preshared key is used for L2TP. Since the RRASM server does not

maintain the interface handles, the RRAS server SHOULD check and ensure that this handle is a valid interface handle.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 40.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- Return any error the RRAS server may return while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.42 RRouterInterfaceGetCredentialsEx (Opnum 41)

Use the **RRouterInterfaceGetCredentialsEx** method [<309>](#) to retrieve extended (other than the user name or password) credentials information for the specified interface.

```
DWORD RRouterInterfaceGetCredentialsEx(  
    [in] DIM_HANDLE hDimServer,  
    [in] DWORD dwLevel,  
    [in, out] PDIM_INFORMATION_CONTAINER pInfoStruct,  
    [in] DWORD hInterface  
);
```

**hDimServer:** A handle to the RRASM server where the call should be executed, see section [3.1.3](#).

**dwLevel:** Specifies the format of the credentials information. This parameter takes values 0x00000000, 0x00000001, 0x00000002, or 0x00000003. An error other than one of the errors in the return values table is returned for other values. A value of 0x00000000 indicates that the credentials information is about the EAP configuration. If the interface does not have EAP information, the **dwSize** field of the [MPR\\_CREDENTIALSEX\\_1](#) structure MUST be set to

zero. Otherwise, the MPR\_CREDENTIALSEX\_1 structure MUST contain [EAPTLS\\_USER\\_PROPERTIES \(section 2.2.1.2.129\)](#). A value of 0x00000001, 0x00000002, or 0x00000003 indicates that the credentials information is a preshared key. If the interface does not have a preshared key configured, an error other than one of the errors in the return values table is returned. Otherwise, the preshared key is formatted as an MPR\_CREDENTIALSEX\_1 structure.

**pInfoStruct:** Pointer to a MPR\_CREDENTIALSEX\_1 structure that contains the preshared key or EAP information for the interface. When the method completes successfully, the client SHOULD free this memory.

**hInterface:** A handle to the interface. This may be obtained from [RRouterInterfaceCreate \(section 3.1.4.13\)](#) or [RRouterInterfaceGetHandle \(section 3.1.4.12\)](#). The interface MUST be of type ROUTER\_IF\_TYPE\_FULL\_ROUTER if **dwLevel** is 0x00000000.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .

The opnum field value for this method is 41.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error the RRAS server may return while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.43 RRasAdminConnectionRemoveQuarantine (Opnum 42)

The **RRasAdminConnectionRemoveQuarantine** method [<310>](#) removes quarantine filters on a dialed-in RRAS client if the filters were applied as a result of Internet Authentication Service (IAS) policies. This function does not remove the IPv6 quarantine filters. The *hDimServer* handle specifies the RRASM server on which the call is to be executed. [<311>](#)

```
DWORD RRasAdminConnectionRemoveQuarantine(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hRasConnection,
```

```
[in] BOOL fIsIpAddress
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**hRasConnection:** This is of type **DWORD** and SHOULD be set to a particular connection identifier for which the connection information is required. Obtain this handle by calling [RRasAdminConnectionEnum \(section 3.1.4.2\)](#). Since the RRAS server does not maintain the connection handles, the RRAS server SHOULD check and ensure that this handle is a valid connection handle.

Alternatively, this parameter specifies the IP address of the RRAS client for which to remove the quarantine filter. The IP address MUST be specified as a **DWORD** in network byte order. Obtain the IP address by calling **RRasAdminConnectionEnum**. If this parameter specifies an IP address, the *fIsIpAddress* parameter MUST specify a TRUE value.

**fIsIpAddress:** Specifies a Boolean value that indicates whether the *hRasConnection* parameter specifies the IP address of the client for which to remove the quarantine filters. If this parameter is a TRUE value, *hRasConnection* specifies an IP address. Otherwise, *hRasConnection* specifies a handle to a connection.

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 42.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that is a member of the "Administrator Group". If not, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error the RRAS server may return while processing the request. Otherwise return ERROR\_SUCCESS.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

#### 3.1.4.44 RMprAdminServerSetInfo (Opnum 43)

The **RMprAdminServerSetInfo** method [<312>](#) sets ports information on a specified server *hDimServer*.

```

DWORD RMprAdminServerSetInfo(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD dwLevel,
    [in] PDIM_INFORMATION_CONTAINER pInfoStruct
);

```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**dwLevel:** This is of type **DWORD** and MUST be set to any of the following values.

Value	Meaning
1	pInfoStruct->pBuffer MUST be a pointer to a <a href="#">MPR_SERVER_1 (section 2.2.1.2.63)</a> .
2	pInfoStruct->pBuffer MUST be a pointer to a <a href="#">MPR_SERVER_2 (section 2.2.1.2.64)</a> .

**pInfoStruct:** This is a pointer of type [PDIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) and MUST be set to the following, based on *dwLevel*.

dwLevel	pInfoStruct->size	pInfoStruct->pBuffer
1	This MUST be set to the size of <b>MPR_SERVER_1</b> (section 2.2.1.2.63).	This MUST be set to a pointer to a <b>MPR_SERVER_1</b> (section 2.2.1.2.63).
2	This MUST be set to the size of <b>MPR_SERVER_2</b> (section 2.2.1.2.64).	This MUST be set to a pointer to a <b>MPR_SERVER_2</b> (section 2.2.1.2.64).

**Return Values:** A 32-bit, unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not listed in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.
0x00000BC2 ERROR_SUCCESS_REBOOT_REQUIRED	A system reboot is required for such a change to take effect. <a href="#">&lt;313&gt;</a>

The opnum field value for this method is 43.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED.
- If *pInfoStruct* is NULL, return an error other than those in the preceding table.
- If *dwLevel* is not supported, return an error other than one of the errors listed in the preceding table.

- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server completes the processing successfully return either ERROR\_SUCCESS or ERROR\_REBOOT\_REQUIRED<314> based on the impact of the configuration change as indicated by the RRAS server. Otherwise return the error status.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.45 RMprAdminServerGetInfoEx (Opnum 44)

The **RMprAdminServerGetInfoEx** method<315> gets the device configuration information for PPTP, L2TP, SSTP, and IKEv2 on a specified server , *hDimServer*.

```
DWORD RMprAdminServerGetInfoEx(
    [in] DIM_HANDLE hDimServer,
    [in, out] PMPR_SERVER_EX_IDL pServerConfig
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**pServerConfig:** A valid pointer to an MPR\_SERVER\_EX\_IDL structure (section [2.2.1.2.144](#)). This MUST NOT be NULL. On successful return this parameter contains port information for RRAS.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 44.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- When the RRAS server processes the request successfully, populate pServerConfig with the information returned by RRAS server and return ERROR\_SUCCESS. Otherwise return the error status provided by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).



### 3.1.4.46 RRasAdminConnectionEnumEx (Opnum 45)

The **RRasAdminConnectionEnumEx** method [<316>](#) retrieves the list of all active connections for a specified RRAS server using handle *hDimServer*. The caller SHOULD free the memory pointed to by *pRasConections*.

```
DWORD RRasAdminConnectionEnumEx(  
    [in] DIM_HANDLE hDimServer,  
    [in] PMPRAPI_OBJECT_HEADER_IDL objectHeader,  
    [in] DWORD dwPreferedMaxLen,  
    [out] LPDWORD lpdwEntriesRead,  
    [out] LPDWORD lpdNumTotalElements,  
    [out, size_is(*lpdwEntriesRead)]  
        PRAS_CONNECTION_EX_IDL* pRasConections,  
    [in, out, unique] LPDWORD lpdwResumeHandle  
);
```

**hDimServer:** The handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**objectHeader:** The pointer to an MPRAPI\_OBJECT\_HEADER\_IDL structure (section [2.2.1.2.130](#)). In the structure, the **revision** field MUST be **MPRAPI\_RAS\_CONNECTION\_OBJECT\_REVISION\_1**, type filed MUST be **MPRAPI\_OBJECT\_TYPE\_RAS\_CONNECTION\_OBJECT**, and size MUST be size of [RAS\\_CONNECTION\\_EX\\_IDL](#).

**dwPreferedMaxLen:** This parameter is of type [DWORD](#) and SHOULD specify the preferred maximum length of returned data (*pRasConections*) in bytes. If *dwPreferedMaxLen* is -1, the buffer returned is large enough to hold all available information. The number of entries returned is zero in the case that *dwPreferedMaxLen* is less than the size of one item; otherwise, the number of entries returned is one more than what could be accommodated in *dwPreferedMaxLen* bytes.

**lpdwEntriesRead:** This is a pointer to type **DWORD**. Upon a successful function call return, this parameter determines the total number of connections enumerated from the current resume position given by *lpdwResumeHandle*.

**lpdNumTotalElements:** This is a pointer to type **DWORD** and receives the total number of connections that could have been enumerated from the current resume position given by *lpdwResumeHandle*.

**pRasConections:** Upon successful return, this is a pointer array of **RAS\_CONNECTION\_EX\_IDL** (section 2.2.1.2.135) structures and the array size is determined by value pointed to by *lpdwEntriesRead*.

**lpdwResumeHandle:** This is a pointer to type **DWORD** and specifies a resume handle used to continue the enumeration. The *lpdwResumeHandle* parameter is NULL on the first call, and left unchanged on subsequent calls (caller MUST pass the same returned value in the next call to this function). If the return code is ERROR\_MORE\_DATA, another call MAY be made using this handle to retrieve more data. If the handle is NULL upon return, the enumeration is complete. This handle is invalid for other types of error returns.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section <a href="#">2.1.1.1</a> .
0x000000EA ERROR_MORE_DATA	Not all of the data was returned with this call. To obtain additional data, call the function again using the resume handle.

The *opnum* field value for this method is 45.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error `ERROR_ACCESS_DENIED` (0x00000005).
- If *RouterType* is `ROUTER_TYPE_LAN`, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, populate *pRasConnections* with information about the active connections returned by the RRAS server. For successful processing, the *lpdwEntriesRead*, *lpdwNumTotalElements*, and *lpdwResumeHandle* will be filled with the values returned by the RRAS server. If there are more entries to be enumerated, the RRAS implementation MUST return `ERROR_MORE_DATA`. If all the entries have been enumerated, the RRAS implementation MUST return `ERROR_SUCCESS`.
- Otherwise, return the failure error status that is returned by the RRAS server.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.47 RRasAdminConnectionGetInfoEx (Opnum 46)

The **RRasAdminConnectionGetInfoEx** method [<317>](#) retrieves the connection information for a particular connection given in *hDimConnection* for a specified RRAS server using handle *hDimServer*. The caller SHOULD free the memory pointed to by *pRasConnection*.

```

DWORD RRasAdminConnectionGetInfoEx (
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hDimConnection,
    [in] PMPRAPI_OBJECT_HEADER_IDL objectHeader,
    [out] PRAS_CONNECTION_EX_IDL pRasConnection
);

```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**hDimConnection:** This is of type [DWORD](#) and MUST be set to a particular connection identifier for which the connection information is required. Obtain this handle by calling [RRasAdminConnectionEnumEx \(section 3.1.4.46\)](#). Because the RRASM server does not maintain the connection handles, the RRAS server SHOULD check and ensure that this handle represents a valid connection handle.

**objectHeader:** A pointer to [MPRAPI\\_OBJECT\\_HEADER\\_IDL \(section 2.2.1.2.130\)](#). In the structure, the **revision** field MUST be MPRAPI\_RAS\_CONNECTION\_OBJECT\_REVISION\_1, the **type** field MUST be MPRAPI\_OBJECT\_TYPE\_RAS\_CONNECTION\_OBJECT, and the **size** MUST be the size of RAS\_CONNECTION\_EX\_IDL.

**pRasConnection:** Upon successful return, this is a pointer to a [RAS\\_CONNECTION\\_EX\\_IDL \(section 2.2.1.2.135\)](#) structure.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section 2.2.4. All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges, as specified in section 2.1.1.1.

The opnum field value for this method is 46.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section 2.1.1.1, whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If *RouterType* is ROUTER\_TYPE\_LAN, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server successfully processes the request, populate *pRasConnection* with information specific to the connection that was requested in *hDimConnection*. Return ERROR\_SUCCESS to the caller. If the RRAS server doesn't complete the request successfully, return the error status returned.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.48 RMprAdminServerSetInfoEx (Opnum 47)

The **RMprAdminServerSetInfoEx** method<318> sets the device configuration information for PPTP, L2TP, SSTP, and IKEv2 on a specified server *hDimServer*.

```
DWORD RMprAdminServerSetInfoEx(  
    [in] DIM_HANDLE hDimServer,  
    [in] PMPR_SERVER_SET_CONFIG_EX_IDL pServerConfig  
);
```

**hDimServer:** The handle to the RRASM server where the call is to be executed, see section 3.1.3.

**pServerConfig:** This is a pointer to a structure PMPR\_SERVER\_SET\_CONFIG\_EX\_IDL (section 2.2.1.2.147) which contains the information required to set values on the RAS server.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of `ERROR_SUCCESS` (0x00000000) indicates the operation was completed successfully; otherwise, it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 <code>ERROR_SUCCESS</code>	The call was successful.
0x00000005 <code>ERROR_ACCESS_DENIED</code>	The calling application does not have sufficient privileges.
0x00000BC2 <code>ERROR_SUCCESS_REBOOT_REQUIRED</code>	A system reboot is required for such a change to take effect.
0x00000BC3 <code>ERROR_SUCCESS_RESTART_REQUIRED</code>	A remote access service restart is required for such a change to take effect.

The `opnum` field value for this method is 47.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error `ERROR_ACCESS_DENIED` (0x00000005).
- If `pServerConfig` is NULL, return an error other than those in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS server completes the processing successfully, it MUST return either `ERROR_SUCCESS`, `ERROR_REBOOT_REQUIRED` [<319>](#), or `ERROR_RESTART_REQUIRED` [<320>](#) based on the impact of the configuration change. Otherwise return the error status.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.49 RRasAdminUpdateConnection (Opnum 48)

The **RRasAdminUpdateConnection** method [<321>](#) updates the endpoint by sending MOBIKE on a connection specified by `hDimConnection` on a specified server, `hDimServer`.

```
DWORD RRasAdminUpdateConnection(
    [in] DIM_HANDLE hDimServer,
    [in] DWORD hDimConnection,
    [in] PRAS_UPDATE_CONNECTION_IDL pServerConfig
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**hDimConnection:** This is of type [DWORD](#) and SHOULD be set to a particular IKEv2 connection identifier for which the endpoint needs to be updated. Obtain this handle by calling `RRasAdminConnectionEnum` (see section [3.1.4.2](#)). Since the RRAS server does not maintain connection handles, the RRAS server should validate this handle.

**pServerConfig:** This is a pointer to a RAS\_UPDATE\_CONNECTION\_IDL structure (section [2.2.1.2.149](#)) that contains the information required to set values on the RRAS server.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates that the operation was completed successfully; otherwise, the return value contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not included in the table that follows MUST be treated the same by the RRASM client

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The Opnum field value for this method is 48.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status the RRAS server may return. Otherwise return ERROR\_SUCCESSFUL.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.50 RRouterInterfaceSetCredentialsLocal (Opnum 49)

The **RRouterInterfaceSetCredentialsLocal** method [<322>](#) is used to set credentials information for an interface. Specifically, the user name, domain name, and password that are used in user authentication are set using this method.

```
DWORD RRouterInterfaceSetCredentialsLocal(  
    [in] DIM_HANDLE hDimServer,  
    [in, string] LPWSTR lpwsInterfaceName,  
    [in, string] LPWSTR lpwsUserName,  
    [in, string] LPWSTR lpwsDomainName,  
    [in, string] LPWSTR lpwsPassword  
);
```

**hDimServer:** A handle to the RRASM server where the call is to be executed, see section [3.1.3](#).

**lpwsInterfaceName:** A pointer to a null-terminated Unicode string that contains the name of the interface for which credentials need to be set. The length of the string MUST NOT be more than 256 characters, otherwise an error is returned.

**lpwsUserName:** A pointer to a null-terminated Unicode string that contains the name of the user on this connection. The string length MUST NOT be more than 256 characters, otherwise an error is returned.

**lpwsDomainName:** A pointer to a null-terminated Unicode string that contains the domain name. The string length MUST NOT be more than 16 characters, otherwise an error is returned.

**lpwsPassword:** A pointer to a null-terminated Unicode string that contains the password of the user on this connection. The string length MUST NOT be more than 256 characters, otherwise an error is returned.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRAS client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 49.

When processing this call, the RRAS server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If an interface with the name *lpwsInterfaceName* does not exist on the server, return an error other than those described in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status the RRAS server may return. Otherwise return ERROR\_SUCCESSFUL.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.4.51 RRouterInterfaceGetCredentialsLocal (Opnum 50)

The **RRouterInterfaceGetCredentialsLocal**[<323>](#) method[<324>](#) is used to get credentials information for an interface. Specifically the user name, domain name, and password used in user authentication are retrieved with this method.

```
DWORD RRouterInterfaceGetCredentialsLocal(  
    [in] DIM_HANDLE hDimServer,  
    [in, string] LPWSTR lpwsInterfaceName,  
    [out, string] LPWSTR* lpwsUserName,  
    [out, string] LPWSTR* lpwsDomainName,  
    [out, string] LPWSTR* lpwsPassword  
);
```

**hDimServer:** A handle to the RRAS server where the call is to be executed, see section [3.1.3](#).

**IpwsInterfaceName:** A pointer to a null-terminated Unicode string that contains the name of the interface for which credentials need to be set. The length of the string MUST NOT be more than 256 characters, otherwise an error is returned. The client SHOULD free this memory.

**IpwsUserName:** A pointer to a null-terminated Unicode string that contains the name of the user on this connection. The string length MUST NOT be more than 256 characters. The client SHOULD free the memory pointed to by *IpwsUserName*.

**IpwsDomainName:** A pointer to a null-terminated Unicode string that contains the domain name. The string length MUST NOT be more than 16 characters. The client SHOULD free the memory pointed to by *IpwsDomainName*.

**IpwsPassword:** A pointer to a null-terminated Unicode string that contains the password of the user on this connection. The string length MUST NOT be more than 256 characters. The client SHOULD free the memory pointed to by *IpwsPassword*.

**Return Values:** A 32-bit unsigned integer value that indicates return status. A return value of ERROR\_SUCCESS (0x00000000) indicates the operation was completed successfully; otherwise it contains an error code, as specified in [\[MS-ERREF\]](#) or section [2.2.4](#). All values that are not in the table that follows MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.
0x00000005 ERROR_ACCESS_DENIED	The calling application does not have sufficient privileges.

The opnum field value for this method is 50.

When processing this call, the RRASM server MUST do the following:

- Validate, as specified in section [2.1.1.1](#), whether this method was called by a client that has access to the method. If the client does not have access, then return error ERROR\_ACCESS\_DENIED (0x00000005).
- If an interface with the name *IpwsInterfaceName* does not exist on the server, return an error other than one of the errors listed in the preceding table.
- Call the abstract interface **Invoke DIMSVC Method** specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Return any error status the RRAS server may return. Otherwise return ERROR\_SUCCESSFUL.

No exceptions are thrown beyond those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

### 3.1.5 Timer Events

None.

### 3.1.6 Other Local Events

Apart from the underlying [\[MS-RPCE\]](#) specified events there are no special events for RRASM. However the RPC interface interacts with the underlying RRAS implementation through the following interfaces.

### 3.1.6.1 Invoke DIMSVC Method

The RRASM server provides the remote management capability to the RRAS implementation. The RRAS implementation refers to the actual task of configuring and providing the routing and remote access functionality that is outside the scope of the RRASM protocol. In order to keep the implementation aspects separated from the semantics of the RRASM methods, this abstract interface is defined with the RRAS implementation. With this, any RPC method request received by the RRASM server, after the required validations done by the RRASM server, are passed to the RRAS server through the interface. As a part of the callback, the Opnum and data structures are passed as-is to the RRAS server. The RRAS as a part of this processing, will perform the actual management task as defined by the semantics of the RRASM method, and will return any information requested by the RRASM server on behalf of the remote RRASM client and return the status of the operation requested by the RRASM server (on behalf of the RRASM client). The RRASM server then relays these return values and data back to the remote RRASM client. The RRAS understands the data structures that the RRASM server requires and can process and provide information in the same manner.

### 3.1.6.2 Start DIMSVC

This interface is invoked by RRAS when it is started to initialize the DIMSVC interface of RRASM. RRAS reads the settings from the registry store – the configuration information in registry are explained in section [2.2.3](#). RRAS passes the initialization parameters to RRASM. RRASM stores these parameters in the corresponding ADM variables, that is, in RouterType, InterfaceList, and SupportedTransportsList as specified in section [3.1.1](#).

### 3.1.6.3 Stop DIMSVC

This interface is invoked by RRAS when it is getting stopped. This will stop the DIMSVC interface of RRASM server and no further RPC requests should be processed. RRAS in turn should ensure that the runtime configuration settings are stored back to the registry store. This way the registry setting will be consistent with the active configuration that RRAS was having when the RRASM interface was running.

## 3.2 DIMSVC Interface Client Details

### 3.2.1 Abstract Data Model

This section describes a conceptual model that an implementation can maintain to participate in this protocol. The described organization is provided to facilitate the explanation of protocol behavior. This document does not mandate that implementations adhere to this model, as long as their external behavior is consistent with that described in this document.

The client is not required to maintain any information during this protocol.

### 3.2.2 Timers

No protocol timers are required beyond those used internally by the RPC method to implement resiliency to network outages, as specified in [\[MS-RPCE\]](#).

### 3.2.3 Initialization

The client creates an RPC binding handle to the server RPC method endpoint when an RPC method is called. For more information on binding handles, see [\[C706\]](#). The client MAY create a separate



binding handle for each method invocation, or it MAY reuse a binding handle for multiple invocations. The client MUST create an authenticated RPC binding handle.

If the RPC interface is available, the client MUST use the RPC interface to configure the RRAS server remotely. The client SHOULD use the registry store configuration using [\[MS-RRP\]](#) to configure RRAS server as defined in section [2.2.3](#) when the RPC interface is not available.

### 3.2.4 Message Processing Events and Sequencing Rules

The client MUST pass any error received from the invocation of an RPC method to the application that issued the RPC call. For all the methods, if `ERROR_ACCESS_DENIED` (0x00000005) is returned, the client needs to make sure it has administrative privileges on the RRAS.

#### 3.2.4.1 RMprAdminServerGetInfo (Opnum 0)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### 3.2.4.2 RRasAdminConnectionEnum (Opnum 1)

If the return code is **ERROR\_MORE\_DATA**, then call [RRasAdminConnectionEnum \(Opnum 1\)](#) ([section 3.1.4.2](#)) with the handle passed in *lpdwResumeHandle*. If *lpdwResumeHandle* is NULL, the enumeration cannot be continued.

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### 3.2.4.3 RRasAdminConnectionGetInfo (Opnum 2)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### 3.2.4.4 RRasAdminConnectionClearStats (Opnum 3)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.5 RRasAdminPortEnum (Opnum 4)

If the return code is **ERROR\_MORE\_DATA**, then call [RRasAdminPortEnum \(Opnum 4\)](#) ([section 3.1.4.5](#)) with the handle passed in *lpdwResumeHandle*. If *lpdwResumeHandle* is NULL, the enumeration cannot be continued.

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### 3.2.4.6 RRasAdminPortGetInfo (Opnum 5)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### 3.2.4.7 RRasAdminPortClearStats (Opnum 6)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.8 RRasAdminPortReset (Opnum 7)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.9 RRasAdminPortDisconnect (Opnum 8)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.10 RRouterInterfaceTransportSetGlobalInfo (Opnum 9)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.11 RRouterInterfaceTransportGetGlobalInfo (Opnum 10)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer **pGlobalInfo** pointer of the *pInfoStruct*.

#### 3.2.4.12 RRouterInterfaceGetHandle (Opnum 11)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.13 RRouterInterfaceCreate (Opnum 12)

If **dwIfType** in [MPRI\\_INTERFACE\\_0](#) is set to **ROUTER\_IF\_TYPE\_FULL\_ROUTER**, the phone book information for the interface MUST have already been configured.

#### 3.2.4.14 RRouterInterfaceGetInfo (Opnum 13)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### 3.2.4.15 RRouterInterfaceSetInfo (Opnum 14)

None beyond those specified in section [3.2.4.<325>](#).

#### 3.2.4.16 RRouterInterfaceDelete (Opnum 15)

If **ERROR\_INTERFACE\_CONNECTED** (0x0000038c) is returned, [RRouterInterfaceDisconnect \(section 3.1.4.23\)](#) SHOULD be called before [RRouterInterfaceDelete \(section 3.1.4.16\)](#) can succeed.

#### 3.2.4.17 RRouterInterfaceTransportRemove (Opnum 16)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.18 RRouterInterfaceTransportAdd (Opnum 17)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.19 RRouterInterfaceTransportGetInfo (Opnum 18)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer **pInterfaceInfo** of the *pInfoStruct* structure.

### 3.2.4.20 RRouterInterfaceTransportSetInfo (Opnum 19)

None beyond those specified in section [3.2.4](#).

### 3.2.4.21 RRouterInterfaceEnum (Opnum 20)

If the return code is **ERROR\_MORE\_DATA**, then the call [RRouterInterfaceEnum \(section 3.1.4.21\)](#) with the handle passed in *lpdwResumeHandle*. If *lpdwResumeHandle* is NULL, the enumeration cannot be continued.

If the method completes successfully and returns a value of either **ERROR\_MORE\_DATA** or **ERROR\_SUCCESS**, the client MUST free the returned buffer *pInfoStruct*.

### 3.2.4.22 RRouterInterfaceConnect (Opnum 21)

If the return value is **PENDING** (0x00000258), call [RRouterInterfaceGetInfo \(section 3.1.4.14\)](#) to find out if the connection was successful or not.

### 3.2.4.23 RRouterInterfaceDisconnect (Opnum 22)

None beyond those specified in section [3.2.4](#).

### 3.2.4.24 RRouterInterfaceUpdateRoutes (Opnum 23)

None beyond those specified in section [3.2.4](#).

### 3.2.4.25 RRouterInterfaceQueryUpdateResult (Opnum 24)

None beyond those specified in section [3.2.4](#).

### 3.2.4.26 RRouterInterfaceUpdatePhonebookInfo (Opnum 25)

None beyond those specified in section [3.2.4](#).

### 3.2.4.27 RMIBEntryCreate (Opnum 26)

None beyond those specified in section [3.2.4](#).

### 3.2.4.28 RMIBEntryDelete (Opnum 27)

None beyond those specified in section [3.2.4](#).

### 3.2.4.29 RMIBEntrySet (Opnum 28)

None beyond those specified in section [3.2.4](#).

### 3.2.4.30 RMIBEntryGet (Opnum 29)

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### **3.2.4.31 RMIBEntryGetFirst (Opnum 30)**

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### **3.2.4.32 RMIBEntryGetNext (Opnum 31)**

When the method completes with either **ERROR\_SUCCESS** or **ERROR\_NO\_MORE\_ITEMS** as the return value, the client MUST free the returned buffer *pInfoStruct*. If **ERROR\_NO\_MORE\_ITEMS** is returned, the client MUST NOT call [RMIBEntryGetNext](#) for the same MIB table.

#### **3.2.4.33 RRasAdminSendUserMessage (Opnum 35)**

None beyond those specified in section [3.2.4](#).

#### **3.2.4.34 RRouterDeviceEnum (Opnum 36)**

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct->pBuffer*.

#### **3.2.4.35 RRouterInterfaceTransportCreate (Opnum 37)**

None beyond those specified in section [3.2.4](#).

#### **3.2.4.36 RRouterInterfaceDeviceGetInfo (Opnum 38)**

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct->pBuffer*.

#### **3.2.4.37 RRouterInterfaceDeviceSetInfo (Opnum 39)**

None beyond those specified in section [3.2.4](#).

#### **3.2.4.38 RRouterInterfaceSetCredentialsEx (Opnum 40)**

None beyond those specified in section [3.2.4](#).

#### **3.2.4.39 RRouterInterfaceGetCredentialsEx (Opnum 41)**

When the method completes with **ERROR\_SUCCESS** as the return value, the client MUST free the returned buffer *pInfoStruct*.

#### **3.2.4.40 RRasAdminConnectionRemoveQuarantine (Opnum 42)**

None beyond those specified in section [3.2.4](#).

#### **3.2.4.41 RMprAdminServerSetInfo (Opnum 43)**

If the return code is **ERROR\_SUCCESS\_REBOOT\_REQUIRED**, then the server machine needs to be rebooted to make the changes take effect.

#### **3.2.4.42 RMprAdminServerGetInfoEx (Opnum 44)**

None beyond those specified in section [3.2.4](#).

#### 3.2.4.43 RRasAdminConnectionEnumEx (Opnum 45)

If the return code is `ERROR_MORE_DATA`, then the call [RRasAdminConnectionEnumEx \(section 3.1.4.46\)](#) with the handle passed in *lpdwResumeHandle*. If *lpdwResumeHandle* is `NULL`, the enumeration cannot be continued.

When the method completes with either **ERROR\_SUCCESS** or **ERROR\_MORE\_DATA** as the return value, the client **MUST** free the returned buffer *pInfoStruct*.

#### 3.2.4.44 RRasAdminConnectionGetInfoEx (Opnum 46)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.45 RMprAdminServerSetInfoEx (Opnum 47)

If the return code is **ERROR\_SUCCESS\_RESTART\_REQUIRED**, then the RemoteAccess service on the server needs to be restarted to make the changes take effect.

If the return value is `ERROR_SUCCESS_RESTART_REQUIRED`, the RRAS implementation **MUST** be restarted for the changes to take effect.

#### 3.2.4.46 RRasAdminUpdateConnection (Opnum 48)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.47 RRouterInterfaceSetCredentialsLocal (Opnum 49)

None beyond those specified in section [3.2.4](#).

#### 3.2.4.48 RRouterInterfaceGetCredentialsLocal (Opnum 50)

When the method completes with **ERROR\_SUCCESS** as the return value, the client **SHOULD** free the memory pointed to by *lpwsUserName*, *lpwsDomainName*, and *lpwsPassword*.

### 3.2.5 Timer Events

No protocol timer events are required on the client beyond the timers required in the underlying RPC protocol.

### 3.2.6 Other Local Events

No local events are maintained on the client other than the events that are maintained in the underlying RPC protocol.

## 3.3 RASRPC Interface Server Details

For the list of methods supported by this interface, refer to [Appendix A: Full IDL \(section 6\)](#) for `uuid(20610036-fa22-11cf-9823-00a0c911e5df)`

### 3.3.1 Abstract Data Model

This section describes a conceptual model that an implementation can maintain to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model, as long as their external behavior is consistent with that described in this document.

There are no states that are maintained for this RPC interface that would affect the RPC method behavior for this interface.

### 3.3.2 Timers

No timers are required beyond those used internally by RPC to implement resiliency to network outages, as specified in the [\[MS-RPCE\]](#) section 3.2.3.2.1.

### 3.3.3 Initialization

The Rasrpc server MUST be initialized by the RRAS server using Start RASRPC as defined in section [3.3.6](#). As a part of initialization, the RRAS protocol MUST register the RPC interface as specified in section [2.1.2](#).

### 3.3.4 Message Processing Events and Sequencing Rules

The Rasrpc Server interface provides methods that remotely retrieve and set the configuration of the RRAS. The version for this interface is 1.0.

To receive incoming remote calls for this interface, the Rasrpc server MUST implement an RPC endpoint using the UUID, 20610036-fa22-11cf-9823-00a0c911e5df. As a part of the message processing, RRAS validates parameters as specified under the following methods. It then hands over the information to the actual RRAS implementation using the **Invoke RASRPC Method**. The **Invoke RASRPC method** will provide any data required and the completion status of the operation which is sent back to the client over the RASRPC interface of RRAS protocol.

The Rasrpc server MUST perform a strict Network Data Representation (NDR) data consistency check at target level 5.0, as specified in [\[MS-RPCE\]](#) section 3.

This protocol MUST indicate to the RPC runtime that it is to reject a NULL unique or full pointer with nonzero conformant value, as specified in section [3](#) of [\[MS-RPCE\]](#).

In the following table, the term "Reserved for local use" means that clients MUST NOT send the opnum, and the server behavior is undefined because it does not affect interoperability.

The Rasrpc server implementation MUST check that the client invoking the method is an administrator of the RRAS server. If the client invoking the method is not an administrator of the RRAS server, the server MUST indicate the lack of access permission in the form of a specific error code. The server SHOULD [<326>](#) throw an RPC exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client does not have access permission. If the server is not throwing an exception, it MAY [<327>](#) return a status code of **E\_ACCESSDENIED** (0x80070005) to indicate to the client that it does not have the required access.

The RPC methods MUST NOT throw any other exception. The other exceptions allowed are those thrown by the underlying RPC protocol [\[MS-RPCE\]](#).

Methods in RPC Opnum Order

Method	Description
Opnum0NotUsedOnWire	Reserved for local use. Opnum: 0
Opnum1NotUsedOnWire	Reserved for local use. Opnum: 1

Method	Description
Opnum2NotUsedOnWire	Reserved for local use. Opnum: 2
Opnum3NotUsedOnWire	Reserved for local use. Opnum: 3
Opnum4NotUsedOnWire	Reserved for local use. Opnum: 4
<a href="#">RasRpcDeleteEntry</a>	Opnum: 5
Opnum6NotUsedOnWire	Reserved for local use. Opnum: 6
Opnum7NotUsedOnWire	Reserved for local use. Opnum: 7
Opnum8NotUsedOnWire	Reserved for local use. Opnum: 8
<a href="#">RasRpcGetUserPreferences</a>	Opnum: 9
<a href="#">RasRpcSetUserPreferences</a>	Opnum: 10
<a href="#">RasRpcGetSystemDirectory</a>	Opnum: 11
<a href="#">RasRpcSubmitRequest</a>	Opnum: 12
Opnum13NotUsedOnWire	Reserved for local use. Opnum: 13
<a href="#">RasRpcGetInstalledProtocolsEx</a>	Opnum: 14
<a href="#">RasRpcGetVersion</a>	Opnum: 15
Opnum16NotUsedOnWire	Reserved for local use. Opnum: 16

### 3.3.4.1 RasRpcDeleteEntry (Opnum 5)

The **RasRpcDeleteEntry** method deletes a specific RRAS Entry from an **RRAS Phonebook path**.

```

DWORD RasRpcDeleteEntry(
    [in] handle_t h,
    [in, string] LPWSTR lpszPhonebook,
    [in, string] LPWSTR lpszEntry
);

```

**h:** An RPC binding handle as specified in [\[C706\]](#) section 2.

**lpszPhonebook:** A null-terminated Unicode string specifying the RRAS Phonebook path as specified in section [2.2.2](#).

**IpszEntry:** A null-terminated Unicode string specifying the **RRAS Entry name** as specified in section [2.2.2.1](#) to be deleted.

**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#) for **retcode** field.

The return value can be one of the following error codes. All other error values MUST be treated the same by the **RRASM client**.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the **RRASM server**, with access permission to perform the operation. [<328>](#)

The opnum field value for this method is 5.

When processing this call, the RRASM server SHOULD do the following:

- Validate as specified in section [3.3.4](#) whether this method was called by a client which is an administrator of the RRASM server.
- If *IpszEntry* is NULL, return an error other than one of the errors specified in the preceding table.
- If *IpszEntry* is not present in **PhonebookEntryNameList**, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke RASRPC**, with the method that specifies the operation and the parameters necessary to enable the RRASM server to perform the required management task.
- Return any error result that the RRASM server may return as a part of the processing. Otherwise return **ERROR\_SUCCESS**.

### 3.3.4.2 RasRpcGetUserPreferences (Opnum 9)

The **RasRpcGetUserPreferences** method retrieves the configuration information. The configuration information consists of the callback information associated with the various ports, and the number of the last successful callback done by the RRAS. This configuration information is set by [RasRpcSetUserPreferences](#).

```
DWORD RasRpcGetUserPreferences(  
    [in] handle_t h,  
    [in, out] LPRASRPC_PBUSER pUser,  
    [in] DWORD dwMode  
);
```

**h:** An RPC binding handle as specified in [\[C706\]](#) section 2.

**pUser:** Pointer to the [RASRPC\\_PBUSER \(section 2.2.1.2.229\)](#) structure which on successful return contains the configuration information on the RRAS server.

**dwMode:** This MUST be set to 2.



**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#) for the **retcode** field.

The return value can be one of the following error codes. All other error values MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the RRASM server, with access permission to perform the operation. [<329>](#)

The Opnum field value for this method is 9.

When processing this call, the RRASM SHOULD do the following:

- Validate as specified in section [3.3.4](#) whether this method was called by a client that is an administrator of the RRASM server. [<330>](#)
- Call the abstract interface **Invoke RASRPC** method, specifying the operation and the parameters necessary to enable RRAS server to perform the required management task.
- Populate the *pUser* structure with the configuration information returned by the RRAS server and returning **ERROR\_SUCCESS** (0x00000000).

### 3.3.4.3 RasRpcSetUserPreferences (Opnum 10)

The **RasRpcSetUserPreferences** method sets the configuration information. The configuration information consists of the callback information associated with the various ports, and the number of the last successful callback done by the RRAS.

```
DWORD RasRpcSetUserPreferences(  
    [in] handle_t h,  
    [in] LPRASRPC_PBUUSER pUser,  
    [in] DWORD dwMode  
);
```

**h:** An RPC binding handle as specified in [\[C706\]](#) section 2.

**pUser:** Pointer to the [RASRPC\\_PBUUSER \(section 2.2.1.2.229\)](#) structure which on successful return contains the configuration information on the RRAS server.

**dwMode:** This MUST be set to 2.

**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#) for the **retcode** field.

The return value can be one of the error codes that follow. All other error values MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the RRAS server, with access permission to perform the operation. [<331>](#)

The opnum field value for this method is 10.

When processing this call, the RRAS SHOULD do the following:

- Validate as specified in section [3.3.4](#) whether this method was called by a client that is an administrator of the RRAS server.
- Call the abstract interface **Invoke RASRPC** method, specifying the operation and the parameters necessary to enable RRAS server to perform the required management task.
- Provide the configuration information as specified by the *pUser* structure to the RRAS server for further processing and returning **ERROR\_SUCCESS** (0x00000000).

#### 3.3.4.4 RasRpcGetSystemDirectory (Opnum 11)

The **RasRpcGetSystemDirectory** method retrieves the path of the system directory.

```
UINT RasRpcGetSystemDirectory(
    [in] handle_t h,
    [in, out, string, size_is(uSize)]
    LPWSTR lpBuffer,
    [in, range(0, 260)] UINT uSize
);
```

**h:** An RPC binding handle as specified in [\[C706\]](#) section 2.

**lpBuffer:** A null-terminated Unicode string that is populated with the path of the system directory. The length of the string MUST be equal to *uSize*.

**uSize:** Specifies the size of the *lpBuffer* in Unicode characters. This value MUST be equal to 260.

**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#) for **retcode** field.

The return value can be one of the following error codes. All other error values MUST be treated the same by the RRAS client.

Return value	Description
0x00000000	The actual processing to retrieve the system directory on the remote server has failed.
Any other values	Indicate the length of the string in Unicode characters copied to the buffer.

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the RRASM server, with access permission to perform the operation. [<332>](#332)

The Opnum field value for this method is 11.

When processing this call, the RRASM server SHOULD do the following:

- Validate as specified in section [3.3.4](#3.3.4) whether this method was called by a client that is an administrator of the RRASM server. [<333>](#333)
- If *uSize* is less than 260, return an error other than one of the errors specified in the preceding table.
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If all validations are successful, return the processing information result for the RRAS server and populate the *lpBuffer* with the system directory path returned by the RRAS server. Return the length of the string in Unicode characters populated to the *lpBuffer*.

### 3.3.4.5 RasRpcSubmitRequest (Opnum 12)

The **RasRpcSubmitRequest** method retrieves or sets the configuration data on RRAS server.

```
DWORD RasRpcSubmitRequest(  
    [in] handle_t hServer,  
    [in, out, unique, size_is(dwcbBufSize)]  
    BYTE pReqBuffer,  
    [in] DWORD dwcbBufSize  
);
```

**hServer:** An RPC binding handle as specified in [\[C706\]](#C706) section 2.

**pReqBuffer:** A pointer to a buffer of size *dwcbBufSize*. The buffer MUST be large enough to hold the **RequestBuffer** structure (section [2.2.1.2.217](#2.2.1.2.217)) and **RequestBuffer.RB\_Buffer** data. **RequestBuffer.RB\_Reqtype** specifies the request type which will be processed by the server and **RequestBuffer.RB\_Buffer** specifies the structure specific to **RB\_Reqtype** to be processed. The structure that MUST be used for each [ReqTypes](#ReqTypes) value is explained in section [2.2.1.2.217](#2.2.1.2.217). The client MUST NOT send the **ReqType** other than those defined in section [2.2.1.1.18](#2.2.1.1.18). **RequestBuffer.RB\_PCIndex** MUST be set to the unique port identifier whose information is sought for **ReqTypes REQTYPE\_GETINFO** and **REQTYPE\_GETDEVCONFIG**. For other valid **ReqTypes**, **RequestBuffer.RB\_PCIndex** MUST be set to zero.

**dwcbBufSize:** Size in byte of *pReqBuffer*.

**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#2.2.1.2.218) for **retcode** field.

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the RRASM server, with access permission to perform the operation. [<334>](#334)

Validations which SHOULD be done by the RRASM for all **ReqTypes** are:

- Return **ERROR\_SUCCESS** (0x00000000) if one of the following conditions are met without any further processing of the call:

- `dwcbBufSize` is less than the sum of size of `RequestBuffer` and 5000, i.e. if the condition (`dwcbBufSize < size of RequestBuffer + 5000`) is true.
- `pReqBuffer` is NULL
- `pReqBuffer.RB_ReqType` is less than zero or greater than maximum `ReqTypes` [<335>](#335)
- Validate as specified in section [3.3.4](#3.3.4) whether this method was called by a client that is an administrator of the RRAS server.

Specific RRASM behavior for each `ReqTypes` value follows.

#### REQTYPE\_GETDEVICECONFIGINFO:

When processing this request, the RRASM SHOULD do the following:

- The `dwcbBufSize` that is passed in SHOULD be greater than or equal to the sum of the size of `RequestBuffer` (section 2.2.1.2.217) with the **RB\_Buffer** field specifying the `DeviceConfigInfo` (section 2.2.1.2.218) structure, and the size of **DeviceConfigInfo.cbBuffer**. If this is not the case, RRASM MUST return the **ERROR\_SUCCESS** (0x00000000) setting **DeviceConfigInfo.retcode** to **E\_INVALIDARG** (0x80070057).
- If **DeviceConfigInfo.dwVersion** is not set to the version of Rasrpc Server [<336>](#336), RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **DeviceConfigInfo.retcode** to **ERROR\_NOT\_SUPPORTED** (0x00000032).
- Call the abstract interface **Invoke RASRPC** specifying the method and the parameters necessary to enable RRAS server to perform the required management task.
- MUST set the **cEntries** to the number of devices returned by the RRAS.
- MUST check the passed in **cbBuffer** size, and copy the device information details ([RAS\\_DEVICE\\_INFO \(section 2.2.1.2.219\)](#RAS_DEVICE_INFO)) for the devices that fit in the **cbBuffer** size to **abdata** buffer.
- **cbBuffer** MUST be set to the total size in bytes needed to hold all the device information. It MUST be set to the value of **cEntries** multiplied by the size of **RAS\_DEVICE\_INFO**.
- **dwVersion** MUST be set to the version of the Rasrpc server.
- If there is no error, **ERROR\_SUCCESS** (0x00000000) MUST be returned setting **DeviceConfigInfo.retcode** to **ERROR\_SUCCESS** (0x00000000).

#### REQTYPE\_SETDEVICECONFIGINFO:

When processing this request, the RRASM MUST do the following:

- The `dwcbBufSize` that is passed in SHOULD be greater than or equal to the sum of the size of `RequestBuffer` (section 2.2.1.2.217) with the **RB\_Buffer** field specifying the `DeviceConfigInfo` (section 2.2.1.2.218) structure, and the size of **DeviceConfigInfo.cbBuffer**. The `dwcbBufSize` passed in SHOULD be equal to or greater than sum of the size of `RequestBuffer`, size of `DeviceConfigInfo` and **DeviceConfigInfo.cbBuffer**. If not, **ERROR\_SUCCESS** (0x00000000) MUST be returned setting **DeviceConfigInfo.retcode** to **E\_INVALIDARG** (0x80070057).
- The **DeviceConfigInfo.cbBuffer** SHOULD be greater than or equal to size of all the device information (**RAS\_DEVICE\_INFO**) as specified in **DeviceConfigInfo.cEntries**. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) and also set **DeviceConfigInfo.retcode** to **ERROR\_INVALID\_PARAMETER** (0x00000057).

- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If the RRAS implementation does not have any of the devices, **RAS\_DEVICE\_INFO.dwError** for that device MUST be set to **ERROR\_DEVICE\_DOES\_NOT\_EXIST** (0x00000260).
- If **RAS\_DEVICE\_INFO.fWrite** is set and the RRAS implementation could not succeed in storing the device information then **DeviceConfigInfo.retcode** MUST be set to **ERROR\_CAN\_NOT\_COMPLETE** (0x000003EB).
- If **RAS\_DEVICE\_INFO.dwNumEndPoints** or **RAS\_DEVICE\_INFO.dwMaxWanEndPoints** is more than the maximum supported value for the WAN endpoint on the RRAS server, it MUST be set to the maximum supported value.
- If the RRAS server returns no error status, **ERROR\_SUCCESS** (0x00000000) MUST be returned setting **DeviceConfigInfo.retcode** to **ERROR\_SUCCESS** (0x00000000). Otherwise return the error status returned by the RRAS server in **DeviceConfigInfo.retcode**.

#### REQTYPE\_GETINFO:

When processing this request, the RRASM SHOULD do the following:

- The *dwcbBufSize* that is passed in SHOULD be greater than or equal to the size of RequestBuffer (section 2.2.1.2.217) with the **RB\_Buffer** field specifying the size of the **Info** structure. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **Info.retcode** to **E\_INVALIDARG** (0x80070057).
- Since the RRASM server does not manage the list of valid port identifiers, the RRAS implementation SHOULD check if the **RequestBuffer.RB\_PCBIndex** refers to a valid port identifier. If the port identifier is not valid, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) and also set **Info.retcode** to **ERROR\_PORT\_NOT\_FOUND** (0x00000267).
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- SHOULD validate if the passed in **RequestBuffer.RB\_Dummy<337>** is equal to the size of **ULONG\_PTR** on the server. If it is not equal and passed in **RequestBuffer.RB\_Dummy** is equal to the size of **DWORD**, the RRASM server MUST **marshal** the **Rasman\_Info.RI\_ConnectionHandle** from **HANDLE** to **ULONG**.
- If the RRAS server successfully processes the request, the RRASM server MUST populate the **RequestBuffer.RB\_Buffer** (Info) structure with the port information provided by RRAS server and return **ERROR\_SUCCESS** (0x00000000).

#### REQTYPE\_GETCALLEDID:

When processing this request, the RRASM MUST do the following:

- The *dwcbBufSize* that is passed in SHOULD be greater than or equal to the sum of the size of RequestBuffer (section 2.2.1.2.217) with the **RB\_Buffer** field specifying the **GetSetCalledId** (section 2.2.1.2.220) structure, and the size of **GetSetCalledId.rciInfo.dwSize**. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) and also set **GetSetCalledId.retcode** to **E\_INVALIDARG** (0x80070057).
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.

- **GetSetCalledId.dwSize** SHOULD be equal to or greater than the sum of the size of [RAS\\_CALLEDID\\_INFO \(section 2.2.1.2.221\)](#) and the size of CalledId buffer to be returned. If so, fill the **GetSetCalledId.rciInfo** buffer with the CalledId details returned by the RRAS server. Otherwise **GetSetCalledId.rciInfo** buffer is not filled with the CalledId details.
- MUST set the **GetSetCalledId.dwSize** to the sum of the size of RAS\_CALLEDID\_INFO and the size of CalledId buffer to be returned and return **ERROR\_SUCCESS** (0x00000000).

#### REQTYPE\_SETCALLEDID:

When processing this request, the RRASM MUST do the following:

- The *dwcbBufSize* that is passed in SHOULD be greater than or equal to the sum of the size of RequestBuffer (section 2.2.1.2.217) with the **RB\_Buffer** field specifying the GetSetCalledId structure, and the size of **GetSetCalledId.rciInfo.dwSize**. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetSetCalledId.retcode** to **E\_INVALIDARG** (0x80070057).
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If all validation is successful, the RRAS server MUST store the **GetSetCalledId.rciInfo** buffer containing CalledId details.
- Return any error the RRAS server may return while processing the request. Otherwise return **ERROR\_SUCCESS** (0x00000000).

#### REQTYPE\_PORTENUM:

When processing this request, the RRASM MUST do the following:

- The *dwcbBufSize* that is passed in SHOULD be greater than or equal to the sum of the size of the RequestBuffer structure specifying the [Enum \(section 2.2.1.2.225\)](#) structure, and **Enum.size**. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **Enum.retcode** to **E\_INVALIDARG** (0x80070057).
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- MUST set the **Enum.entries** to the number of available port devices returned by the RRAS Server.
- MUST check the passed in **Enum.size** and copy all of the port information details ([RASMAN\\_PORT 32 \(section 2.2.1.2.226\)](#)) for the ports that fit in the **Enum.size** to **Enum.buffer**.
- **Enum.size** MUST be set to the total size in bytes needed to hold all the port information.
- If there is no error, the server MUST return **ERROR\_SUCCESS** (0x00000000).

#### REQTYPE\_GETNDISWANDRIVERCAPS:

When processing this request, the RRASM MUST do the following:

- The *dwcbBufSize* that is passed in SHOULD be greater than or equal to the size of the RequestBuffer structure with the **RB\_Buffer** field specifying the [GetNdiswanDriverCapsStruct \(section 2.2.1.2.222\)](#) structure. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetNdiswanDriverCapsStruct.retcode** to **E\_INVALIDARG** (0x80070057).

- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- If all validation is successful, populate the **GetNdiswanDriverCapsStruct** with the encryption capabilities returned by the RRAS server and set **GetNdiswanDriverCapsStruct.retcode** to **ERROR\_SUCCESS** (0x00000000). If there is any error while retrieving the encryption capabilities of RRAS, set the **GetNdiswanDriverCapsStruct.retcode** with the error. RRASM MUST return **ERROR\_SUCCESS** (0x00000000).

#### REQTYPE\_GETDEVCONFIG:

When processing this request, the RRASM MUST do the following:

- The *dwcbBufSize* that is passed in SHOULD be greater than or equal to the sum of the size of the RequestBuffer structure with the **RB\_Buffer** field specifying the [GetDevConfigStruct \(section 2.2.1.2.224\)](#) structure, and **GetDevConfigStruct.size**. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetDevConfigStruct.retcode** to **E\_INVALIDARG** (0x80070057).
- Because RRASM does not maintain the list of valid port identifiers, the RRAS server SHOULD check that **RequestBuffer.RB\_PCBIndex** is a valid port identifier. If this is not the case, RRAS MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetDevConfigStruct.retcode** to **ERROR\_PORT\_NOT\_FOUND** (0x00000267).
- If the device type specified by **GetDevConfigStruct.devicetype** does not exist on the RRAS server, the RRAS implementation MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetDevConfigStruct.retcode** to **ERROR\_DEVICE\_DOES\_NOT\_EXIST** (0x00000260).
- If the device type associated with the port as identified by **RequestBuffer.RB\_PCBIndex** is a value other than "MODEM", RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetDevConfigStruct.retcode** to **ERROR\_SUCCESS** (0x00000000) and **GetDevConfigStruct.size** to zero.
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- Check if **GetDevConfigStruct.size** is large enough to hold the device information as returned by RRAS. If not, RRASM MUST return **ERROR\_SUCCESS** (0x00000000) setting **GetDevConfigStruct.retcode** to **ERROR\_BUFFER\_TOO\_SMALL** (0x0000025B). Set the **GetDevConfigStruct.size** to the size of the required buffer to hold device information.
- If all validation is successful, the RRAS server MUST get the device configuration information associated with the port identified by **RequestBuffer.RB\_PCBIndex** and fill the **GetDevConfigStruct.config** buffer with the details and set the **GetDevConfigStruct.size** to the size of the buffer copied to **GetDevConfigStruct.config**. Server MUST return **ERROR\_SUCCESS** (0x00000000).

#### 3.3.4.6 RasRpcGetInstalledProtocolsEx (Opnum 14)

The **RasRpcGetInstalledProtocolsEx** method retrieves the protocol information on the RRAS server. The list of protocols is defined in the following return value section.

```
DWORD RasRpcGetInstalledProtocolsEx(
    [in] handle_t h,
    [in] BOOL fRouter,
    [in] BOOL fRasCli,
```



```
[in] BOOL fRasSrv
);
```

**h:** An RPC binding handle as specified in [\[C706\]](#) section 2.

**fRouter:** If set to TRUE, protocols enabled for Demand Dial are retrieved. If set to FALSE, protocols enabled for Demand Dial are not retrieved.

**fRasCli:** This flag is not used and MUST be set to FALSE.

**fRasSrv:** If set to TRUE, retrieves the protocol enabled for RRAS incoming connections. If set to FALSE, protocol for RRAS incoming connections are not retrieved.

**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#) for the **retcode** field.

The return value can be one of the error codes that follow. All other error values MUST be treated the same by the RRASM client.

Return value	Description
0x00000000	There is no protocol installed on the RRAS server or there is some error when RRAS server retrieves the information.
0x00000001 to 0x0000000F	Specifies the protocols enabled on the RRAS server. This value SHOULD be a combination of one or more of the following flags: NP_Nbf (0x00000001): NetBEUI protocol is enabled. <a href="#">&lt;338&gt;</a> NP_Ipx (0x00000002): IPX protocol is enabled. <a href="#">&lt;339&gt;</a> NP_Ip (0x00000004): TCP/IPv4 protocol is enabled. NP_Ipv6 (0x00000008): TCP/IPv6 protocol is enabled. <a href="#">&lt;340&gt;</a>

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the RRASM server, with access permission to perform the operation.[<341>](#)

The opnum field value for this method is 14.

When processing this call, the RRASM server SHOULD do the following:

- Validate as specified in section [3.3.4](#) whether this method was called by a client that is an administrator of the RRASM server.
- Call the abstract interface **Invoke RASRPC** method specifying the operation and the parameters to enable RRAS server to perform the required management task.
- If all validation is successful, return the installed protocol information as provided by the RRAS server.

### 3.3.4.7 RasRpcGetVersion (Opnum 15)

The **RasRpcGetVersion** method retrieves the Rasrpc server interface version.

```
DWORD RasRpcGetVersion(
[in] handle_t h,
```



```
[in, out, ref] LPDWORD pdwVersion  
);
```

**h:** An RPC binding handle as specified in [\[C706\]](#) section 2.

**pdwVersion:** This is a pointer to type **DWORD** which, after a successful function call, specifies the version of the Rasrpc interface.

**Return Values:** Specifies the return status as explained in section [2.2.1.2.218](#) for the **retcode** field

The return value can be one of the error codes that follow. All other error values MUST be treated the same by the RRASM client.

Return value/code	Description
0x00000000 ERROR_SUCCESS	The call was successful.

**Exceptions Thrown:** This method throws an exception with the exception code **RPC\_S\_ACCESS\_DENIED** (0x00000005) if the client is not an administrator on the RRASM server, with access permission to perform the operation. [<342>](#)

The opnum field value for this method is 15.

When processing this call, the RRAM server SHOULD do the following:

- Validate as specified in section [3.3.4](#) whether this method was called by a client that is an administrator of the RRASM server. [<343>](#)
- Call the abstract interface **Invoke RASRPC method** specifying the operation and the parameters to enable the RRAS server to perform the required management task.
- Set the value pointed by pdwVersion to the version of RRAS Server. [<344>](#)
- If there is no error, the server MUST return 0x00000000 (ERROR\_SUCCESS).

### 3.3.5 Timer Events

No protocol timer events are required on the server beyond the timers required in the underlying RPC protocol.

### 3.3.6 Other Local Events

Apart from the underlying [\[MS-RPCE\]](#) specified events there are no special events for RRASM. However the RPC interface interacts with the underlying RRAS implementation through the following interfaces.

#### 3.3.6.1 Invoke RASRPC Method

The RRASM server provides the remote management capability to the RRAS implementation. The RRAS implementation refers to the actual task of configuring and providing the routing and remote access functionality that is outside the scope of the RRASM protocol. For more information about routing and remote access, see [\[MSFT-RRAS\]](#). To keep the implementation aspects separate from the semantics of the RRASM methods, this abstract interface is defined with the RRAS implementation.

With this, any RPC method request received by the RRASM server, after the required validations done by the RRASM server, are passed to the RRAS server through this interface. The Opnum and the data structures are passed as is to the RRAS server. As part of this processing, RRAS will perform the actual management task as defined by the semantics of the RRASM method, and will return any information requested by the RRASM server on behalf of the remote RRASM client and return the status of the operation requested by the RRASM server (on behalf of the RRASM client). The RRASM server then relays these return values and data back to the remote RRASM client. The RRAS understands the data structures that the RRASM server requires and can process and provide information in the same manner.

### 3.3.6.2 Start RASRPC

This interface is invoked by RRAS when it is started to initialize the RASRPC interface of RRASM.

### 3.3.6.3 Stop RASRPC

This interface is invoked by RRAS when it is getting stopped. This will stop the RASRPC interface of RRASM and no further RPC requests are processed.

## 3.4 RASRPC Interface Client Details

### 3.4.1 Abstract Data Model

This section describes a conceptual model that an implementation can maintain to participate in this protocol. The described organization is provided to help explain protocol behavior. This document does not mandate that implementations adhere to this model, as long as their external behavior is consistent with that described in this document.

The client is not required to maintain any information during this protocol.

### 3.4.2 Timers

No protocol timers are required beyond those used internally by the RPC method to implement resiliency to network outages, as specified in [\[MS-RPCE\]](#).

### 3.4.3 Initialization

The client creates an RPC binding handle to the server RPC method endpoint when an RPC method is called. For more information on binding handles, see [\[C706\]](#). The client MAY create a separate binding handle for each method invocation, or it MAY reuse a binding handle for multiple invocations. The client MUST create an authenticated RPC binding handle.

### 3.4.4 Message Processing Events and Sequencing Rules

The client MUST pass any error that is received from the invocation of an RPC method to the application that issued the RPC call. For all of the methods, if `RPC_S_ACCESS_DENIED` (0x00000005) is returned as an exception or `E_ACCESS_DENIED` (0x80070005) [\[345\]](#) is returned as a return value, the client needs to make sure it has administrative privileges on the RRAS server.

The Rasrpc server MUST perform a strict Network Data Representation (NDR) data consistency check at target level 5.0, as specified in [\[MS-RPCE\]](#) section 3.

This protocol MUST indicate to the RPC runtime that it is to reject a NULL unique or full pointer with non-zero conformant value, as specified in section [3](#) of [\[MS-RPCE\]](#).

#### 3.4.4.1 RasRpcDeleteEntry (Opnum 5)

None beyond those specified in section [3.4.4](#)

#### 3.4.4.2 RasRpcGetUserPreferences (Opnum 9)

When the method completes successfully with a return value of ERROR\_SUCCESS, the client SHOULD free the memory allocated by RPC. The following fields of **RASRPC\_PBUSER** MAY contain RPC allocated memory: pCallbacks, pLocations, pPhonebooks, pAreaCodes, pPrefixes, pSuffixes.

#### 3.4.4.3 RasRpcSetUserPreferences (Opnum 10)

None beyond those specified in section [3.4.4](#)

#### 3.4.4.4 RasRpcGetSystemDirectory (Opnum 11)

None beyond those specified in section [3.4.4](#)

#### 3.4.4.5 RasRpcSubmitRequest (Opnum 12)

Before calling the method, the client MUST set the pReqBuffer buffer and dwcbBufSize buffer size to a size at least as large as the sum of the size of RequestBuffer and 5000. Also, thepReqBuffer.RB\_ReqType value MUST be set to one of the valid enumeration values as stated in section [2.2.1.1.18](#).

Client behavior for specific **ReqTypes** is as follows.

##### **REQTYPE\_GETDEVICECONFIGINFO**

Before calling the method, the client MUST set DeviceConfigInfo.dwVersion to the version of Rasrpc server. The version information for the Rasrpc server can be retrieved using RasRpcGetVersion method as described in section [3.3.4.7](#).

Also, the DeviceConfigInfo.cbBuffer value MUST be equal to the size of the DeviceConfigInfo.abdata buffer.

If the returned DeviceConfigInfo.cbBuffer is more than the passed in cbBuffer size, it implies that the passed in buffer is not big enough to hold all the device information. The client SHOULD again call the API with DeviceConfigInfo.cbBuffer set to the size of the returned cbBuffer.

##### **REQTYPE\_SETDEVICECONFIGINFO**

Before calling the method, the client MUST set the DeviceConfigInfo.cbBuffer value equal to the size of DeviceConfigInfo.abdata buffer.

##### **REQTYPE\_PORTENUM**

Before calling the method, the client MUST set the Enum.size value to the size of Enum.buffer.

If the returned Enum.size is more than the passed in Enum.size, it implies that the passed in buffer was not big enough to hold all the ports information. The client SHOULD again call the API with Enum.size set to the size of the returned Enum.size.

##### **REQTYPE\_GETDEVCONFIG**

Before calling the method, the client MUST set the GetDevConfig.size value to the size of the GetDevConfig.config buffer.

If the returned `GetDevConfig.retcode` is set to `ERROR_BUFFER_TOO_SMALL` (0x0000025B), the buffer that was passed in was not big enough to hold the device configuration information. The client SHOULD again call the API with `GetDevConfig.size` set to the size of returned `GetDevConfig.size`.

### **REQTYPE\_GETCALLEDID**

Before calling the method, the client SHOULD set the `RequestBuffer.RB_PCBIndex` to zero.

Also, the client MUST set the `GetSetCalledId.dwSize` to the sum of the size of `RAS_CALLEDID_INFO` and the size of `GetSetCalledId.rciInfo.bCalledId` buffer size.

If the returned `GetSetCalledId.dwSize` is more than the passed in `GetSetCalledId.dwSize`, it implies that the passed in buffer was not big enough to hold all the `CalledId` information. The client SHOULD again call the API with `GetSetCalledId.dwSize` set to sum of the size of `RAS_CALLEDID_INFO` and the returned `GetSetCalledId.dwSize`.

#### **3.4.4.6 RasRpcGetInstalledProtocolsEx (Opnum 14)**

None beyond those specified in section [3.4.4](#)

#### **3.4.4.7 RasRpcGetVersion (Opnum 15)**

None beyond those specified in section [3.4.4](#)

### **3.4.5 Timer Events**

No protocol timer events are required on the client beyond the timers required in the underlying RPC protocol.

### **3.4.6 Other Local Events**

No local events are maintained on the client other than the events that are maintained in the underlying RPC protocol.

## 4 Protocol Examples

### 4.1 Querying Server Configuration Information

This example illustrates the use of the RPC methods defined in this specification. The methods are used to query the configuration of the RRAS server when there are 128 ports each of PPTP, L2TP, and SSTP. [<346>](#) The RRAS server is configured for both routing and remote access.

The client calls the RPC method [RMprAdminServerGetInfo \(section 3.1.4.1\)](#) with the following parameters:

- The [DIM\\_HANDLE \(section 2.2.1.1.6\)](#) that the client obtains during initialization (section [3.1.3](#)).
- The level of information required. In this example, if the client specifies level 3, [<347>](#) it will get the maximum information.
- The pointer to [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) (*pInfoStruct*) into which the server configuration information would be passed back by the RRAS server.

When the client calls the RPC method as previously described, it returns ERROR\_SUCCESS. Additionally, the following parameter values are updated:

- The *dwBufferSize* in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) will contain the size of information being passed; in this case, it will be the size of [MPR\\_SERVER\\_2 \(section 2.2.1.2.64\)](#).
- The *pBuffer* in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) will contain the pointer to a buffer containing **MPR\_SERVER\_2**.
- The *dwNumPptpPorts* in **MPR\_SERVER\_2** will contain 128, the number of PPTP ports configured on the RRAS server.
- The *dwPptpPortFlags* in **MPR\_SERVER\_2** will contain 0x00000003 because both routing and remote access are configured.
- The *dwNumL2tpPorts* in **MPR\_SERVER\_2** will contain 128, the number of L2TP ports configured on the RRAS server.
- The *dwL2tpPortFlags* in **MPR\_SERVER\_2** will contain 0x00000003 because both routing and remote access are configured.
- The *dwNumSstpPorts* in **MPR\_SERVER\_2** will contain 128, the number of SSTP ports configured on the RRAS server. [<348>](#)
- The *dwSstpPortFlags* in **MPR\_SERVER\_2** will contain 0x00000003 because both routing and remote access are configured. [<349>](#)

The client should free the buffer pointed to by *pBuffer* using *midl\_user\_free*.

### 4.2 Disconnecting a Particular User Connection

This example illustrates the use of the RPC methods defined in this specification to enumerate a connection on the RRAS server. This example shows a Windows Server® 2008 operating system server [<350>](#) when 10 remote access connections are active and one of the clients (foo) has connected from a multilink (2-port) machine that is compliant with the policies on the server [\[MS-](#)

[RNAP](#). The connection of foo is enumerated and all the ports (2) of that connection are disconnected.

The client calls the RPC method [RRasAdminConnectionEnum \(section 3.1.4.2\)](#) with the following parameters:

- The [DIM\\_HANDLE \(section 2.2.1.1.6\)](#) that the client obtains during initialization (section [3.1.3](#)).
- The level of information required. In this example, the RRAS server supports level 3. [<351>](#)
- The pointer to [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) (*pInfoStruct*) that the RRAS server uses to pass the information.
- The *dwPreferedMaximumLength* is set to -1, so that the buffer returned is large enough to hold all available information.
- The *lpdwResumeHandle* parameter is zero because this is the first call.

When the client calls the RPC method as previously described, the RRAS server returns ERROR\_SUCCESS. Additionally, the following parameter values are updated:

- The **dwBufferSize** in the pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) will contain the size of information being passed; in this case, it will be 10 times the size of [RASI\\_CONNECTION\\_3 \(section 2.2.1.2.81\)](#).
- The *lpdwEntriesRead* and *lpdwTotalEntries* will point to **DWORD**, which has a value of 10.
- The **pBuffer** in the pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) will contain a pointer to a 10-element array of **RASI\_CONNECTION\_3**.
- The **dwVersion** in **RASI\_CONNECTION\_3** will be 1.
- The **dwSize** in each instance of **RASI\_CONNECTION\_3** will be the size of **RASI\_CONNECTION\_3** in bytes.
- The **dwConnection** in **RASI\_CONNECTION\_3** will be a unique handle to identify the connection.
- The **wszUserName** in one of the 10 instances of **RASI\_CONNECTION\_3** will be "foo".
- The **dwInterfaceType** in **RASI\_CONNECTION\_3** will be ROUTER\_IF\_TYPE\_CLIENT.
- The **guid** in **RASI\_CONNECTION\_3** will be a unique GUID to identify a connection.
- The **PppInfo3** **RASI\_CONNECTION\_3** will contain the PPP information of the connection.
- The **rasQuarState** in **RASI\_CONNECTION\_3** will be RAS\_QUAR\_STATE\_NORMAL because the client is healthy.
- The **timer** in **RASI\_CONNECTION\_3** will not be valid because the client is healthy.

The client then stores the **dwConnection** in **RASI\_CONNECTION\_3**, which has the **wszUserName** "foo" in a local variable *hRasConnection*.

The client should free the buffer pointed to by **pBuffer**.

The client calls the RPC method [RRasAdminPortEnum \(section 3.1.4.5\)](#) with the following parameters:

- The **DIM\_HANDLE** is the same handle that the client obtains earlier during initialization.
- The *dwLevel* is set to 0.
- The *hRasConnection* is the handle that the client obtained in **dwConnection** in **RASI\_CONNECTION\_3** during the previous call **RRasAdminConnectionEnum**.
- The pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) that the RRAS servers uses to pass the information.
- The *dwPreferedMaximumLength* is set to -1, so that the buffer returned is large enough to hold all available information.
- The *lpdwResumeHandle* parameter is zero because all the information required is present.

When the client calls the RPC method as previously described, the RRAS server returns **ERROR\_SUCCESS**. Additionally, the following parameter values are updated:

- The **dwBufferSize** in the pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) will contain the size of information being passed; in this case, it will be the size of [RASI\\_PORT\\_0 \(section 2.2.1.2.76\)](#).
- The **pBuffer** in the pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) will contain a pointer to **RASI\_PORT\_0**.
- The *lpdwEntriesRead* will point to a **DWORD** that contains 2.

The client stores the **dwPort** in each instance of **RASI\_PORT\_0** into a local variable array *hPort[2]*.

The client should free the buffer pointed to by **pBuffer**.

The client then calls the RPC method [RRasAdminPortDisconnect \(section 3.1.4.9\)](#) twice with the following parameters:

- The **DIM\_HANDLE** is the same handle that the client obtains earlier during initialization.
- The *hPort[n]* handle is obtained previously by calling **RRasAdminPortEnum** (*n*= 0,1).

When the client calls the RPC method as described in this section, the method returns **ERROR\_SUCCESS**, and the user connection is disconnected.

### 4.3 Creating a Demand Dial Interface on RRAS with Filters

This example illustrates the use of the RPC methods defined in this specification to create a one-way demand-dial interface named "dd1" on the RRAS on Windows Server® 2008 operating system. Then, IPv4 filtering is enabled on the demand-dial interface so that the demand dial is triggered whenever packets with the source address 1.1.1.1 reach the RRAS server.

The client updates the phone book file *router.pbk* under the file path *C:\Windows\System32* to comprise the phonebook entry for *dd1*, see section [4.10](#) for details.

The client calls the RPC method [RRouterInterfaceCreate \(section 3.1.4.13\)](#) with the following parameters:

- The [DIM\\_HANDLE \(section 2.2.1.1.6\)](#) that the client obtains during initialization (section [3.1.3](#)).
- The level of information required. In this example, the client specifies level 0.
- The pointer to [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) (*pInfoStruct*) that the RRAS server uses to pass the information.
- The **dwBufferSize** in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) will contain the size of information being passed; in this case, it will be the size of [MPRI\\_INTERFACE\\_0 \(section 2.2.1.2.82\)](#).
- The **pBuffer** in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) will contain a pointer to **MPRI\_INTERFACE\_0**.
- The **wszInterfaceName** in the pointer to **MPRI\_INTERFACE\_0** is set to L"dd1".
- The **dwIfType** in the pointer to **MPRI\_INTERFACE\_0** is set to ROUTER\_IF\_TYPE\_HOME\_ROUTER.

When the client calls the RPC method as previously described, it returns ERROR\_SUCCESS. Additionally, the following parameter value is updated:

- The *hInterface* specifies a unique identifier of the newly created interface.

The client stores the *hInterface* returned in **MPRI\_INTERFACE\_0** into a local variable *hInterface*.

The client should free the buffer pointed to by **pBuffer**.

The client then calls the RPC method [RRouterInterfaceTransportAdd \(section 3.1.4.18\)](#) to add with the following parameters:

- The **DIM\_HANDLE** that the client obtains during initialization (section [3.1.3](#)).
- The pointer to [DIM\\_INTERFACE\\_CONTAINER](#) (*pInfoStruct*) that the RRAS server uses to pass the information.
- The *hInterface* is the handle to the interface stored locally.
- The *dwTransportId* will be set to 0x00000021 since IPv4 filters are being added.
- The pointer to DIM\_INTERFACE\_CONTAINER (*pInfoStruct*) that the RRAS server uses to pass the information.
- The **fGetInterfaceInfo** in the pointer to DIM\_INTERFACE\_CONTAINER (*pInfoStruct*) must be set to 0 because the client is setting information.
- The **dwInterfaceInfoSize** in the pointer to DIM\_INTERFACE\_CONTAINER (*pInfoStruct*) must be set to the size of [RTR\\_INFO\\_BLOCK\\_HEADER \(section 2.2.1.2.3\)](#) with one [RTR\\_TOC\\_ENTRY \(section 2.2.1.2.4\)](#) and have the quad memory aligned data for MPR\_FILTER\_0 0x34.
- The **pInterfaceInfo** in the pointer to DIM\_INTERFACE\_CONTAINER (*pInfoStruct*) must be set to **RTR\_INFO\_BLOCK\_HEADER**.
- The **Version** in **RTR\_INFO\_BLOCK\_HEADER** must be set to 1.
- The **Size** must be set to 32.



- The **TocEntriesCount** must be set to 1.
- The **InfoType** of RTR\_TOC\_ENTRY must be set to IP\_FILTER\_ENABLE\_INFO (0xffff0015).
- The **InfoSize** in RTR\_TOC\_ENTRY must be set to 20 (TOC entry 16 byte + 4 bytes mprfilter).
- The **Count** in RTR\_TOC\_ENTRY must be set to 1.
- The **Offset** must be 16 and must point to [MPR\\_FILTER\\_0 \(section 2.2.1.2.90\)](#).
- The **fEnable** in **MPR\_FILTER\_0** is set to 0x00000001 to enable filtering on the RRAS server.

Having enabled filtering on the interface, the client should then add filters on the demand-dial interface. In this example, filtering is enabled on all packets with the source address 1.1.1.1.

The client then calls the RPC method **RRouterInterfaceTransportAdd** with the following parameters:

- The **DIM\_HANDLE** that the client obtains during initialization (section [3.1.3](#)).
- The pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) that the RRAS server uses to pass .
- The *hInterface* is the handle to the interface stored locally.
- The *dwTransportId* will be set to 0x00000021 for IPv4.
- The pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) that the RRAS server uses to pass .
- The **fGetInterfaceInfo** in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) must be set to 0 because the client is setting information.
- The **dwInterfaceInfoSize** in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) must be set to 68 (filter descriptor 40 bytes + TOC entry 16 bytes + **RTR\_INFO\_BLOCK\_HEADER** -Toc 12 bytes).
- The **pInterfaceInfo** in the pointer to **DIM\_INFORMATION\_CONTAINER** (*pInfoStruct*) must be set to **RTR\_INFO\_BLOCK\_HEADER**.
- The **Version** in **RTR\_INFO\_BLOCK\_HEADER** must be set to 1.
- The **Size** must be set to 72 (filter descriptor 40 bytes + TOC entry 32 bytes).
- The **TocEntriesCount** must be set to 1.
- The **InfoType** of RTR\_TOC\_ENTRY must be set to 0xffff0009.
- The **InfoSize** in RTR\_TOC\_ENTRY must be set to 40 (the size of the filter descriptor).
- The **Count** in RTR\_TOC\_ENTRY must be set to 1.
- The **Offset** must be 32 and must point to [FILTER\\_DESCRIPTOR \(section 2.2.1.2.5\)](#).
- The **dwVersion** in **FILTER\_DESCRIPTOR** is set to 0x00000001.
- The **dwNumFilters** in **FILTER\_DESCRIPTOR** is set to 0x00000001.
- The **faDefaultAction** in **FILTER\_DESCRIPTOR** is set to 0x00000000.

- The **fiFilter** must contain [FILTER\\_INFO \(section 2.2.1.2.6\)](#).
- The **dwSrcAddr** in **FILTER\_INFO** is set to 0x01010101 and the rest of the fields in **FILTER\_INFO** are set to 0.

#### 4.4 Enumerating Interfaces and Connecting "dd1"

This example illustrates the use of the RPC methods defined in this specification to enumerate interfaces on the RRAS server that has three demand-dial interfaces and connect dd1.

The client calls the RPC method [RRouterInterfaceEnum \(section 3.1.4.21\)](#) with the following parameters:

- The [DIM\\_HANDLE \(section 2.2.1.1.6\)](#) that the client obtains during initialization (section [3.1.3](#)).
- The level of information required is set to zero.
- The pointer to [DIM\\_INFORMATION\\_CONTAINER \(section 2.2.1.2.1\)](#) (*pInfoStruct*) into which the information is passed by the RRAS server.
- The *dwPreferedMaximumLength* is set to -1, so that the buffer returned is large enough to hold all available information.
- The *lpdwResumeHandle* parameter is zero because this is the first call.

When the client calls the RPC method as previously described, the RRAS server returns **ERROR\_SUCCESS**. Additionally, the following parameter values are updated:

- The **dwBufferSize** in the pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) will contain the size of information being passed. In this case, it will be three times the size of [MPRI\\_INTERFACE\\_0 \(section 2.2.1.2.82\)](#).
- The **pBuffer** in the pointer to **DIM\_INFORMATION\_CONTAINER** (section 2.2.1.2.1) (*pInfoStruct*) will contain the pointer to the three-element array of **MPRI\_INTERFACE\_0**.
- The *lpdwEntriesRead* and *lpdwTotalEntries* will point to the **DWORD** whose value is 3. The client will attempt to match **wszInterfaceName** of each of the entries of **MPRI\_INTERFACE\_0**.

It will store the **dwInterface** of the matched **MPRI\_INTERFACE\_0** in the local variable *hInterface*. After ensuring that the **fEnabled** field is 1, the client calls [RRouterInterfaceConnect \(section 3.1.4.22\)](#) with the following parameters:

- The **DIM\_HANDLE** that the client obtains during initialization (section [3.1.3](#)).
- The *hInterface* that the client has stored locally.
- The *hEvent* is set to NULL and *fBlocking* is set to 1 so that the call is blocked until the connection attempt has completed.

When the client calls the RPC method as previously described, the RRAS server returns **ERROR\_SUCCESS** after the connection is successful.

#### 4.5 Querying Interface Status Through MIB

This example illustrates the use of the RPC methods defined in this specification to get the status information for an interface on the RRAS server on which no multicast protocol is running.

The client calls the RPC method [RMIBEntryGet \(section 3.1.4.30\)](#) with the following parameters:

- The [DIM\\_HANDLE \(section 2.2.1.1.6\)](#) that the client obtains during initialization (section [3.1.3](#)).
- The *dwPid* specifies the protocol ID that exported the variable (0x00000002) because the status is being requested.
- The *dwRoutingPid* specifies the routing protocol that exported the variable (10000) IP.

When the client calls the RPC method as previously described, the RRAS server returns ERROR\_SUCCESS. Additionally, the following parameter values are updated:

- The *pInfoStruct* pointer to an opaque data structure [DIM\\_MIB\\_ENTRY\\_CONTAINER \(section 2.2.1.2.19\)](#).
- The **dwMibOutEntrySize** in the pointer to **DIM\_MIB\_ENTRY\_CONTAINER**.
- The **pMibOutEntry** in the pointer to **DIM\_MIB\_ENTRY\_CONTAINER** will point to [MIB\\_OPAQUE\\_INFO \(section 2.2.1.2.53\)](#).
- The **dwId** in **MIB\_OPAQUE\_INFO** will be set to 0x00000002.
- The **dwIfIndex** in [MIB\\_IFSTATUS \(section 2.2.1.2.30\)](#). The index that identifies the interface.
- The **dwAdminStatus** will indicate the administrative status as UP.
- The **dwOperationalStatus** will indicate the operational status as UP.
- The **bMHbeatActive** will be zero.
- The **bMHbeatAlive** will be zero.

## 4.6 Updating the Connection Endpoint of an IKEv2-Based Connection

This example illustrates the use of the RPC methods defined in this specification to enumerate a connection on the RRAS server. In this example we consider a Windows Server® 2008 R2 operating system [\[352\]](#) when 10 remote access connections are active and one of the clients (user name = joe) has connected using the IKEv2 from a machine that is compliant with the policies on the server [\[MS-RNAP\]](#). The connection of joe is enumerated and the tunnel endpoint is updated to a different interface identified by interface index.

The client calls the RPC method [RRasAdminConnectionEnumEx \(section 3.1.4.46\)](#) with the following parameters:

- The [DIM\\_HANDLE \(section 2.2.1.1.6\)](#) that the client obtains during initialization (section [3.1.3](#)).
- The *objectHeader* contains the pointer to [MPRAPI\\_OBJECT\\_HEADER\\_IDL \(section 2.2.1.2.130\)](#), revision is set to MPRAPI\_RAS\_CONNECTION\_OBJECT\_REVISION\_1, type is set to MPRAPI\_OBJECT\_TYPE\_RAS\_CONNECTION\_OBJECT, and size is set to sizeof(MPRAPI\_OBJECT\_HEADER\_IDL).
- The *dwPreferredMaximumLength* is set to -1, so that the buffer returned is large enough to hold all available information.
- The *lpdwResumeHandle* parameter is zero as this is the first call.

When the client calls the RPC method as described above, the RRAS server returns `ERROR_SUCCESS` and additionally the following parameter values are updated:

- The *lpdwEntriesRead* and *lpdNumTotalElements* will point to `DWORD` whose value is 10.
- The *pRasConections* will contain pointer to 10 element array `RAS_CONNECTION_EX_IDL`.
- The **hConnection** in [RAS\\_CONNECTION\\_EX\\_IDL](#) will be a unique handle to identify the connection.
- The *wszUserName* in one of the 10 instances of `RAS_CONNECTION_EX_IDL` will be "joe".
- The *dwInterfaceType* in `RAS_CONNECTION_EX_IDL` will be `ROUTER_IF_TYPE_CLIENT`.
- The *guid* in `RAS_CONNECTION_EX_IDL` will be a unique GUID to identify a connection.
- The *ProjectionInfo* in `RAS_CONNECTION_EX_IDL` will contain the IKEv2 information of the connection.
- The *rasQuarState* in `RAS_CONNECTION_EX_IDL` will be `RAS_QUAR_STATE_NORMAL` as the client is healthy.

The client then stores the **hConnection** in `RAS_CONNECTION_EX_IDL` whose *wszUserName* is "joe" in a local variable **hRasConnection**.

The client should free the buffer pointed to by **pRasConections**.

The client calls the RPC method [RRasAdminUpdateConnection \(section 3.1.4.49\)](#) with the following parameters:

- The `DIM_HANDLE` (section 2.2.1.1.6) that the client obtains during initialization (section [3.1.3](#)).
- *hDimConnection* contains the previously obtained **hConnection**.
- The pointer to [RAS\\_UPDATE\\_CONNECTION\\_IDL \(section 2.2.1.2.149\)](#) (*pServerConfig*) which contains the interface index of the local interface to which the connection has to be switched.

When the client calls the RPC method as described above, the RRAS server returns `ERROR_SUCCESS` and the IKEv2 connection is switched to the new interface specified in the interface index.

## 4.7 Retrieving the Rasrpc Server Version Info

This example illustrates the use of the Rasrpc Interface method `RasRpcGetVersion` as defined in this specification. The method is used to query the version information of the Rasrpc Server when the version is 6.

The client calls the RPC method `RasRpcGetVersion` (section [3.3.4.7](#)) with the following parameters:

- The handle to the Rasrpc Server, where the call is to be executed that the client obtains during initialization (section [3.3.3](#))
- The pointer to type `DWORD`, which on successful function call return contains the version of the Rasrpc server.

When the client calls the RPC method as previously described, it returns `ERROR_SUCCESS`. *pdwVersion* points to `DWORD` containing 6 as the remote Rasrpc server version.

## 4.8 Retrieving Device Configuration Information

This example illustrates the use of the Rasrpc Interface method **RasRpcSubmitRequest** with ReqTypes REQTYPE\_GETDEVICECONFIGINFO as defined in this specification. The method is used to query all the devices configured on the RRAS server when there are 7 devices on the RRAS - 2 Modem devices, 4 tunnel devices (one each for PPTP, L2TP, SSTP and IKEv2) and 1 PPPoE device.

The client calls the RPC method **RasRpcSubmitRequest** (section [3.3.4.5](#)) with the following parameters:

- The handle to the Rasrpc Server where the call is to be executed that the client obtains during initialization (section [3.3.3](#)).
- pReqBuffer parameter is updated as follows:
  - The pReqBuffer buffer is allocated the size of the sum of the size of RequestBuffer and 5000.
  - pReqBuffer.RB\_PCIndex is set to zero.
  - pReqBuffer.RB\_Reftype is set to 95 (REQTYPE\_GETDEVICECONFIGINFO)
  - pReqBuffer.RB\_Dummy is set to the size of ULONG.
  - pReqBuffer.Done is set to zero.
  - pReqBuffer.Alignment is set to zero.
  - pReqBuffer.RB\_Buffer is interpreted as a DeviceConfigInfo structure and following value for DeviceConfigInfo are set:
    - DeviceConfigInfo.dwVersion is set to the version of Rasrpc Server. The version information can be retrieved using RasRpcGetVersion method (section [3.3.4.7](#))
    - DeviceConfigInfo.cbBuffer is set to zero.
- The dwcbBufSize is set to the size of pReqBuffer.

When the client calls the RPC method as previously described, server returns ERROR\_SUCCESS. Additionally, the DeviceConfigInfo structure as pointed by pReqBuffer.RB\_Buffer is updated as follows:

- DeviceConfigInfo.cEntries will contain 7 as the number of device entries present on the Rasrpc server.
- DeviceConfigInfo.cbBuffer will contain 3304 as the size of DeviceConfigInfo.abdata buffer needed to contain all the device information.
- DeviceConfigInfo.dwVersion will contain 6 as the version of the Rasrpc server.

If DeviceConfigInfo.cbBuffer returned size is greater than the passed in DeviceConfigInfo.cbBuffer size, it implies that the passed in size was not large enough to hold all the devices information in which case, The client should call the **RasRpcSubmitRequest** method again with DeviceConfigInfo.cbBuffer set to the returned value of DeviceConfigInfo.cbBuffer in the first call.

If DeviceConfigInfo.cbBuffer returned size is less than or equal to the passed in DeviceConfigInfo.cbBuffer size, DeviceConfigInfo.abdata contains an array of RAS\_DEVICE\_INFO structure containing information for each device on the server.

The client will call the **RasRpcSubmitRequest** method again with DeviceConfigInfo.cbBuffer set to 3304 and all other parameters being same.

When the client calls the RPC method as described, the server returns ERROR\_SUCCESS. Additionally, the **DeviceConfigInfo** structure as pointed by pReqBuffer.RB\_Buffer is updated as follows by the server:

- DeviceConfigInfo.cEntries will contain 7 as the number of device entries present on the Rasrpc server.
- DeviceConfigInfo.cbBuffer will contain 3304 as the size of DeviceConfigInfo.abdata buffer needed to contain all the device information.
- DeviceConfigInfo.dwVersion will contain 6 as the version of the Rasrpc server.
- DeviceConfigInfo.abdata points to the array of RAS\_DEVICE\_INFO structures containing the device information.

The client should free the memory allocated to the pReqBuffer structure.

## 4.9 Retrieving Specific Port Information

This example illustrates the use of the Rasrpc Interface method RasRpcSubmitRequest with ReqTypes REQTYPE\_GETINFO as defined in this specification. The method is used to query the information of a specific port with port identifier 2 which is a SSTP port.

The client calls the RPC method RasRpcSubmitRequest(section [3.3.4.5](#)) with the following parameters:

- The handle to the Rasrpc Server where the call is to be executed that the client obtains during initialization (section [3.3.3](#))
- pReqBuffer parameter is updated as follows:
  - The pReqBuffer buffer is allocated the size of the sum of the size of RequestBuffer and 5000.
  - pReqBuffer.RB\_PCBIndex is set to 2. (Port identifier information for all the available ports on the server can be retrieved using the RasRpcSubmitRequest with ReqTypes as REQTYPE\_PORTENUM. RASMAN\_PORT\_32.P\_Port contains the unique port identifier for the port.)
  - pReqBuffer.RB\_Reftype is set to 22 (REQTYPE\_GETINFO)
  - pReqBuffer.RB\_Dummy is set to the size of ULONG.
  - pReqBuffer.Done is set to zero.
  - pReqBuffer.Alignment is set to zero.
- The dwcbBufSize MUST be set to the size of pReqBuffer.

When the client calls the RPC method as previously described, the server returns ERROR\_SUCCESS. pReqBuffer.RB\_Buffer is interpreted as Info structure and contains the port information of the port with port ID 2.

## 4.10 Sample Phonebook File for a Demand-dial Connection

This example illustrates the settings associated with a Demand-Dial connection "dd1". The description for each key/value pair is given in the following table. The format of the phonebook file is defined in section 2.2.2. The phonebook entry for "dd1" is stored inside the file router.pbk present under the path %windir%\system32\ras on the RRAS server. The following table describes the sample phonebook settings associated with "dd1". The first column in the following table is the sample phonebook file representing the settings for "dd1" connection. The second column is the description of the values for all of the settings.

Phonebook file	Meaning
[dd1]\LF\CR	Name of the Demand-Dial connection is "dd1"
Encoding=1\LF\CR	Encoding format is UTF-8
Type=1\LF\CR	Type of connection is dial-up
AutoLogon=0\LF\CR	Ignored
UseRASCredentials=0\LF\CR	Ignored
LowDateTime=-300171584\LF\CR	Ignored
HighDateTime=30015653\LF\CR	Ignored
DialParamsUID=700993612\LF\CR	A unique number
Guid=ECFE1B3644EBB744A7562E43091795ED\LF\CR	A unique identifier of the Demand-Dial connection "dd1"
BaseProtocol=1\LF\CR	Ignored
VpnStrategy=0\LF\CR	Ignored for Modem connection type
ExcludedProtocols=0\LF\CR	Negotiate IPv4 and IPv6
LcpExtensions=1\LF\CR	Enable LCP extensions
DataEncryption=8\LF\CR	Request data encryption
SwCompression=1\LF\CR	Enable software compression
NegotiateMultilinkAlways=0\LF\CR	Don't negotiate multilink
SkipNwcWarning=0\LF\CR	Ignored
SkipDownLevelDialog=0\LF\CR	Ignored
SkipDoubleDialDialog=0\LF\CR	Ignored
DialMode=1\LF\CR	Dial all Modems
DialPercent=75\LF\CR	Ignored since DialMode is 1
DialSeconds=120\LF\CR	Ignored since DialMode is 1
HangUpPercent=10\LF\CR	Ignored since DialMode is 1
HangUpSeconds=120\LF\CR	Ignored since DialMode is 1

Phonebook file	Meaning
OverridePref=32\LF\CR	Read CallbackMode from this entry
RedialAttempts=0\LF\CR	Redial attempts is set to 0
RedialSeconds=60\LF\CR	Redial seconds is set to 60
IdleDisconnectSeconds=300\LF\CR	Idle disconnect seconds is set to 300
RedialOnLinkFailure=0\LF\CR	Do not redial the connection on link failure
CallbackMode=0\LF\CR	No callback
CustomDialDll=\LF\CR	The key does not have a value
CustomDialFunc=\LF\CR	Ignored
CustomRRASDialDll=\LF\CR	Ignored
ForceSecureCompartment=0\LF\CR	Ignored
DisableIKENNameEkuCheck=0\LF\CR	Ignored. This is not applicable since Type is "1".
AuthenticateServer=0\LF\CR	Server authentication is disabled
ShareMsFilePrint=0\LF\CR	NetBT is disabled
BindMsNetClient=0\LF\CR	Microsoft Net client is disabled
SharedPhoneNumbers=1\LF\CR	Phone numbers are shared for all the subentries
GlobalDeviceSettings=0\LF\CR	Do not use the device settings present in the phonebook file
PrerequisiteEntry=\LF\CR	Ignored
PrerequisitePbk=\LF\CR	Ignored
PreferredPort=COM3\LF\CR	Preferred port name is "COM3"
PreferredDevice= Compaq 56K USB External Fax Modem \LF\CR	Preferred device name is "Compaq 56K USB External Fax Modem"
PreferredBps=115200\LF\CR	Maximum transfer speed is 115200 bits per second for preferred modem
PreferredHwFlow=1\LF\CR	Hardware flow control is enabled for preferred modem
PreferredProtocol=1\LF\CR	Cyclic Redundancy Check (CRC) is enabled for preferred modem
PreferredCompression=1\LF\CR	Enable hardware compression for preferred modem
PreferredSpeaker=1\LF\CR	Enable modem speaker for preferred modem



Phonebook file	Meaning
PreferredMdmProtocol=0\LF\CR	Ignored
PreviewUserPw=1\LF\CR	Ignored
PreviewDomain=1\LF\CR	Ignored
PreviewPhoneNumber=0\LF\CR	Ignored
ShowDialingProgress=0\LF\CR	Ignored
ShowMonitorIconInTaskBar=1\LF\CR	Ignored
CustomAuthKey=0\LF\CR	Ignored since AuthRestrictions not configured to negotiate EAP
AuthRestrictions=544\LF\CR	Negotiate authentication protocols Challenge Handshake Protocol (CHAP) and Microsoft Challenge Handshake Protocol Version 2 (MSCHAPv2)
IpPrioritizeRemote=1\LF\CR	Ignored
IpInterfaceMetric=0\LF\CR	Ignored
IpHeaderCompression=1\LF\CR	Enable IPv4 header compression
IpAddress=0.0.0.0\LF\CR	Ignored since IpAssign is 1
IpDnsAddress=0.0.0.0\LF\CR	Ignored since IpNameAssign is 1
IpDns2Address=0.0.0.0\LF\CR	Ignored since IpNameAssign is 1
IpWinsAddress=0.0.0.0\LF\CR	Ignored since IpNameAssign is 1
IpWins2Address=0.0.0.0\LF\CR	Ignored since IpNameAssign is 1
IpAssign=1\LF\CR	RRAS assigns the IPv4 address
IpNameAssign=3\LF\CR	RRAS assigns the IPv4 DNS and WINS address
IpDnsFlags=0\LF\CR	Do not register the client IPv4 address with DNS
IpNBTFflags=0\LF\CR	Disable NetBT
TcpWindowSize=0\LF\CR	Ignored
UseFlags=2\LF\CR	Ignored
IpSecFlags=0\LF\CR	Ignored since Type is 1.
IpDnsSuffix=\LF\CR	Ignored
Ipv6PrioritizeRemote=1\LF\CR	Ignored
Ipv6InterfaceMetric=0\LF\CR	Ignored
Ipv6NameAssign=1\LF\CR	RRAS assigns the IPv6 DNS address

Phonebook file	Meaning
Ipv6DnsAddress=::\LF\CR	Ignored since Ipv6NameAssign is 1
Ipv6Dns2Address=::\LF\CR	Ignored since Ipv6NameAssign is 1
Ipv6InterfaceId=0000000000000000\LF\CR	Ignored
NETCOMPONENTS=\LF\CR	Ignored
ms_msclient=0\LF\CR	Ignored
ms_server=0\LF\CR	Ignored
MEDIA=serial\LF\CR	Media name is serial
Port=COM3\LF\CR	Communication port name is COM3
Device=Compaq 56K USB External Fax Modem\LF\CR	Device name is "Compaq 56K USB External Fax Modem"
ConnectBPS=115200\LF\CR	Maximum transfer speed is 115200 bits per second
DEVICE=switch\LF\CR	Device type is pre-connect switch
Terminal=1\LF\CR	Display terminal window
DEVICE=modem\LF\CR	Device type is modem
PhoneNumber=2006034\LF\CR	Primary local phone number to dial is 2006034
AreaCode=\LF\CR	Ignored as UseDialingRules is 0
CountryCode=91\LF\CR	Ignored as UseDialingRules is 0
CountryID=91\LF\CR	Ignored as UseDialingRules is 0
UseDialingRules=0\LF\CR	Do not use the dialing rules
Comment=\LF\CR	Ignored
FriendlyName=\LF\CR	Ignored
PhoneNumber=2006035\LF\CR	Alternate local phone number is 2006035
AreaCode=\LF\CR	Ignored because UseDialingRules is 0
CountryCode=91\LF\CR	Ignored as UseDialingRules is 0
CountryID=91\LF\CR	Ignored as UseDialingRules is 0
UseDialingRules=0\LF\CR	Do not use the dialing rules
Comment=\LF\CR	Ignored
FriendlyName=\LF\CR	Ignored
LastSelectedPhone=0\LF\CR	Ignored
PromoteAlternates=0\LF\CR	Do not promote alternate numbers

Phonebook file	Meaning
TryNextAlternateOnFail=1\LF\CR	Try alternate number on failure of the primary number
HwFlowControl=1\LF\CR	Hardware flow control is enabled
Protocol=1\LF\CR	Cyclic Redundancy Check (CRC) is enabled
Compression=1\LF\CR	Enable hardware compression
Speaker=0\LF\CR	Disable modem speaker
MdmProtocol=0\LF\CR	Ignored

## 4.11 Registry Configuration

This section describes the sample registry settings for the various RRAS settings configured.

### 4.11.1 Transport Configuration

The following is a sample registry setting configuration for the IPv4 transport.

**Key Name:**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\RouterManagers\Ip

**Name:** ProtocolId

**Type:** REG\_DWORD

**Data:** 0x21

**Name:** GlobalInfo

**Type:** REG\_BINARY

**Data:**

```

00000000  01 00 00 00 78 00 00 00 - 02 00 00 00 03 00 ff ff  ....x.....ÿÿ
00000010  08 00 00 00 01 00 00 00 - 30 00 00 00 06 00 ff ff  .....0.....ÿÿ
00000020  34 00 00 00 01 00 00 00 - 38 00 00 00 00 00 00 00  4.....8.....
00000030  00 00 00 00 01 00 00 00 - 06 00 00 00 02 00 00 00  .....
00000040  01 00 00 00 16 27 00 00 - 03 00 00 00 17 27 00 00  ....'.....'..
00000050  05 00 00 00 12 27 00 00 - 07 00 00 00 03 00 00 00  ....'.....
00000060  0a 00 00 00 08 00 00 00 - 78 00 00 00 00 00 00 00  .....x.....
00000070  00 00 00 00 00 00 00 00 -                .....

```

The GlobalInfo is the RTR\_INFO\_BLOCK\_HEADER structure providing the following information:

**GLOBAL\_INFO:** This specifies the transport configuration for IPv4 – specifically the filtering and logging level.

bFilteringOn: FALSE

dwLoggingLevel: 0x00000001 – Log Errors only.

PRIORITY\_INFO: This specifies the priority of the routes added through various methods. The following is the information represented by the GlobalInfo blob. It is organized in terms of the route type and the priority associated with it.

- MIB\_IPPROTO\_LOCAL - 1
- MIB\_IPPROTO\_NT\_STATIC - 3
- MIB\_IPPROTO\_NT\_STATIC\_NON\_DOD - 5
- MIB\_IPPROTO\_NT\_AUTOSTATIC - 7
- MIB\_IPPROTO\_NETMGMT - 10
- MIB\_IPPROTO\_RIP - 120

#### 4.11.2 Interface Configuration

The following is a sample registry setting showing the IPv4 configuration for a demand dial interface with name RR2.

**Key Name:**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces\5

**Name:** InterfaceName

**Type:** REG\_SZ

**Data:** RR2

**Name:** Type

**Type:** REG\_DWORD

**Data:** 0x2

**Name:** Enabled

**Type:** REG\_DWORD

**Data:** 0x1

**Key Name:**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Interfaces\5\Ip

**Name:** ProtocolId

**Type:** REG\_DWORD

**Data:** 0x21

**Name:** InterfaceInfo

**Type:** REG\_BINARY

**Data:**

```

00000000  01 00 00 00 fc 00 00 00 - 04 00 00 00 0a 00 ff ff  ....ü.....ÿÿ
00000010  8c 00 00 00 01 00 00 00 - 50 00 00 00 04 00 ff ff  ....P.....ÿÿ
00000020  04 00 00 00 01 00 00 00 - e0 00 00 00 07 00 ff ff  ....à.....ÿÿ
00000030  10 00 00 00 01 00 00 00 - e8 00 00 00 0d 00 ff ff  ....è.....ÿÿ
00000040  04 00 00 00 01 00 00 00 - f8 00 00 00 00 00 00 00  ....ø.....
00000050  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
00000060  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
00000070  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
00000080  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
00000090  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
000000a0  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
000000b0  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
000000c0  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....
000000d0  00 00 00 00 0a 00 00 00 - 00 00 00 00 00 00 00 00  ....
000000e0  01 00 00 00 00 00 00 00 - 58 02 a4 01 08 07 00 00  ....X.¤....
000000f0  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00  ....

```

The InterfaceInfo is the RTR\_INFO\_BLOCK\_HEADER specifying the following information:

**MCAST\_HBEAT\_INFO:** This specifies the multicast heart beat configuration for the interface. In the preceding configuration, the multicast heart beat is disabled.

**bActive:** FALSE

The rest of the members of the structure MCAST\_HBEAT\_INFO are not applicable since it is not active.

**INTERFACE\_STATUS\_INFO:** This specifies the administrative status of the interface. In the preceding setting, it is set to IF\_ADMIN\_STATUS\_UP.

**dwAdminStatus:** IF\_ADMIN\_STATUS\_UP

**RTR\_DISC\_INFO:** This specifies the router discovery configuration for the interface. The advertisement is disabled in the preceding interface configuration.

**wMaxAdvtInterval:** 600

**wMinAdvtInterval:** 420

**wAdvtLifetime:** 1800

**bAdvertise:** FALSE

**IPrefLevel:** 0

**IFFILTER\_INFO:** This specifies the filter setting for the IP fragments. The specified configuration has the fragment filtering disabled.

**bEnableFragChk:** FALSE

### 4.11.3 Ports Configuration

The following is a sample registry configuration for an SSTP device. The following registry key has the SSTP configured for remote access connections with 128 ports.

**Key Name:** HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0000

**Name:** ComponentId

**Type:** REG\_SZ

**Data:** ms\_sstpminiport

**Name:** DriverDesc

**Type:** REG\_SZ

**Data:** WAN Miniport (SSTP)

**Name:** EnableForRas

**Type:** REG\_DWORD

**Data:** 0x1

**Name:** EnableForRouting

**Type:** REG\_DWORD

**Data:** 0

**Name:** EnableForOutboundRouting

**Type:** REG\_DWORD

**Data:** 0

**Name:** MaxWanEndpoints

**Type:** REG\_DWORD

**Data:** 0x3e8

**Name:** WanEndpoints

**Type:** REG\_DWORD

**Data:** 0x80

#### 4.11.4 Other Miscellaneous Configuration Information

The following registry value specifies the RRAS mode configured.

**Key Name:** HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters

**Name:** RouterType

**Type:** REG\_DWORD

**Data:** 0x1e

The previous value corresponds to the following enumeration flags.

ROUTER\_TYPE\_LAN

ROUTER\_TYPE\_WAN

IPV6\_ROUTER\_TYPE\_RAS

IPV6\_ROUTER\_TYPE\_LAN

This specifies that for IPv4 LAN routing and demand dial is enabled and remote access connections are not enabled. For IPv6, Remote Access connections are enabled but only LAN routing is enabled.

The following registry information specifies the settings to be used for IKEv2. This specifies an idle timeout value of 5 minutes, retransmission timeout of 30minutes, SA life time of 8 hours, and SA datasize lifetime of 100 MB.

**Key Name:**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\IKEV2

**Name:** idleTimeout

**Type:** REG\_DWORD

**Data:** 0x12c

**Name:** networkBlackoutTime

**Type:** REG\_DWORD

**Data:** 0x708

**Name:** saLifeTime

**Type:** REG\_DWORD

**Data:** 0x7080

**Name:** saDataSize

**Type:** REG\_DWORD

**Data:** 0x19000

The following registry configuration specifies the IPv4 static address pool to be used. The address range configured is from 10.1.1.1 to 10.1.1.100.

**Key Name:**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip

**Name:** UseDhcpAddressing

**Type:** REG\_DWORD

**Data:** 0

**Key Name:**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RemoteAccess\Parameters\Ip\StaticAddressPool\0

**Name:** From

**Type:** REG\_DWORD

**Data:** 0xa010101

**Name:** To

**Type:** REG\_DWORD

**Data:** 0xa010164



## 5 Security

### 5.1 Security Considerations for Implementers

The RRAS Management Protocol allows any user to establish a connection to the RPC server. The protocol uses the underlying RPC protocol to retrieve the identity of the caller that made the method call as specified in [\[MS-RPCE\]](#). Clients should create an authenticated RPC connection. Servers should use this identity to perform specific access checks.

#### 5.1.1 Security Considerations Specific to the RRAS Management Protocol

The RRAS data and RRAS operations specified by this implementation should be protected by access checks based on the identity of the RPC client.

Servers implementing this specification should not allow anonymous RPC connections and should protect RRAS access to all data and operations with access control checks based on client identity.

RPC over named pipes should not be used by clients or servers implementing this specification because it is vulnerable to man-in-the-middle attacks. RPC over TCP/IP should be used instead.

Using `RPC_C_AUTHN_LEVEL_PKT_PRIVACY` as the RPC authentication level provides data confidentiality for the communication between client and server. The server implementing this protocol should support clients requesting `RPC_C_AUTHN_LEVEL_PKT_PRIVACY`[<353>](#). The server MAY enforce this in order to protect the privacy of the communication between the client and the server.

### 5.2 Index of Security Parameters

Security parameter	SECTION
<code>RPC_C_AUTHN_GSS_NEGOTIATE</code>	Section <a href="#">2.1.1.1</a>

## 6 Appendix A: Full IDL

For ease of implementation, the full IDL is provided, where "ms-dtyp.idl" refers to the IDL found in [\[MS-DTYP\]](#) Appendix A. The syntax uses the IDL syntax extensions defined in [\[MS-RPCE\]](#) section 2.2.4. For example, as noted in [\[MS-RPCE\]](#) section 2.2.4.9, a `pointer_default` declaration is not required, and `pointer_default` (unique) is assumed.

```
import "ms-dtyp.idl";

#define IN
#define OUT

typedef enum _ROUTER_INTERFACE_TYPE
{
    ROUTER_IF_TYPE_CLIENT,
    ROUTER_IF_TYPE_HOME_ROUTER,
    ROUTER_IF_TYPE_FULL_ROUTER,
    ROUTER_IF_TYPE_DEDICATED,
    ROUTER_IF_TYPE_INTERNAL,
    ROUTER_IF_TYPE_LOOPBACK,
    ROUTER_IF_TYPE_TUNNEL1,
    ROUTER_IF_TYPE_DIALOUT
} ROUTER_INTERFACE_TYPE;

typedef enum
{
    ROUTER_IF_STATE_UNREACHABLE,
    ROUTER_IF_STATE_DISCONNECTED,
    ROUTER_IF_STATE_CONNECTING,
    ROUTER_IF_STATE_CONNECTED
} ROUTER_CONNECTION_STATE;

typedef enum _RAS_QUARANTINE_STATE
{
    RAS_QUAR_STATE_NORMAL,
    RAS_QUAR_STATE_QUARANTINE,
    RAS_QUAR_STATE_PROBATION,
    RAS_QUAR_STATE_UNKNOWN
} RAS_QUARANTINE_STATE;

typedef enum _RAS_PORT_CONDITION
{
    RAS_PORT_NON_OPERATIONAL,
    RAS_PORT_DISCONNECTED,
    RAS_PORT_CALLING_BACK,
    RAS_PORT_LISTENING,
    RAS_PORT_AUTHENTICATING,
    RAS_PORT_AUTHENTICATED,
    RAS_PORT_INITIALIZING
} RAS_PORT_CONDITION;
```

```
typedef enum _RAS_HARDWARE_CONDITION
{
    RAS_HARDWARE_OPERATIONAL,
    RAS_HARDWARE_FAILURE
}
RAS_HARDWARE_CONDITION;
```

```
typedef handle_t DIM_HANDLE;
```

```
typedef enum _FORWARD_ACTION
{
    FORWARD = 0,
    DROP = 1,
}
FORWARD_ACTION;
```

```
typedef enum {
    MIB_IPROUTE_TYPE_OTHER = 1,
    MIB_IPROUTE_TYPE_INVALID = 2,
    MIB_IPROUTE_TYPE_DIRECT = 3,
    MIB_IPROUTE_TYPE_INDIRECT = 4,
} MIB_IPFORWARD_TYPE;
```

```
typedef enum {
    MIB_IPPROTO_OTHER = 1,
    MIB_IPPROTO_LOCAL = 2,
    MIB_IPPROTO_NETMGMT = 3,
    MIB_IPPROTO_ICMP = 4,
    MIB_IPPROTO_EGP = 5,
    MIB_IPPROTO_GGP = 6,
    MIB_IPPROTO_HELLO = 7,
    MIB_IPPROTO_RIP = 8,
    MIB_IPPROTO_IS_IS = 9,
    MIB_IPPROTO_ES_IS = 10,
    MIB_IPPROTO_CISCO = 11,
    MIB_IPPROTO_BBN = 12,
    MIB_IPPROTO OSPF = 13,
    MIB_IPPROTO_BGP = 14,
    MIB_IPPROTO_NT_AUTOSTATIC = 10002,
    MIB_IPPROTO_NT_STATIC = 10006,
    MIB_IPPROTO_NT_STATIC_NON_DOD = 10007,
} MIB_IPFORWARD_PROTO;
```

```
typedef enum {
    MIB_IP_FORWARDING = 1,
    MIB_IP_NOT_FORWARDING = 2,
} MIB_IPSTATS_FORWARDING, *PMIB_IPSTATS_FORWARDING;
```

```

typedef enum {
    MIB_TCP_STATE_CLOSED      = 1,
    MIB_TCP_STATE_LISTEN     = 2,
    MIB_TCP_STATE_SYN_SENT   = 3,
    MIB_TCP_STATE_SYN_RCVD   = 4,
    MIB_TCP_STATE_ESTAB      = 5,
    MIB_TCP_STATE_FIN_WAIT1  = 6,
    MIB_TCP_STATE_FIN_WAIT2  = 7,
    MIB_TCP_STATE_CLOSE_WAIT = 8,
    MIB_TCP_STATE_CLOSING    = 9,
    MIB_TCP_STATE_LAST_ACK   = 10,
    MIB_TCP_STATE_TIME_WAIT  = 11,
    MIB_TCP_STATE_DELETE_TCB = 12,
} MIB_TCP_STATE;

typedef enum {
    MIB_TCP_RTO_OTHER      = 1,
    MIB_TCP_RTO_CONSTANT   = 2,
    MIB_TCP_RTO_RSRE       = 3,
    MIB_TCP_RTO_VANJ       = 4,
} TCP_RTO_ALGORITHM, *PTCP_RTO_ALGORITHM;

//
// IPv6 Internet address (RFC 2553)
// This is an 'on-wire' format structure.
//
typedef struct in6_addr {
    union {
        UCHAR      Byte[16];
        USHORT     Word[8];
    } u;
} IN6_ADDR, *PIN6_ADDR, *LPIN6_ADDR;

typedef struct _DIM_INFORMATION_CONTAINER
{
    DWORD      dwBufferSize;
    [size_is(dwBufferSize)] LPBYTE pBuffer;
}
DIM_INFORMATION_CONTAINER, *PDIM_INFORMATION_CONTAINER;

// RAS_CONNECTION_EX structure are redefined in this IDL to make use of versioning:
// All the Versions of RAS_CONNECTION_EX will be defined here in RPC usable format:

typedef struct _MPRAPI_OBJECT_HEADER_IDL
{
    UCHAR      revision;
    UCHAR      type;
    USHORT     size;
}MPRAPI_OBJECT_HEADER_IDL, *PMPRAPI_OBJECT_HEADER_IDL;

typedef struct _PPP_PROJECTION_INFO_1
{

```

```

// IPv4 Projection Parameters
DWORD          dwIPv4NegotiationError;
WCHAR          wszAddress[16];
WCHAR          wszRemoteAddress[16];
DWORD          dwIPv4Options;
DWORD          dwIPv4RemoteOptions;
ULONG64        IPv4SubInterfaceIndex;

// IPv6 Projection Parameters
DWORD          dwIPv6NegotiationError;
UCHAR          bInterfaceIdentifier[8];
UCHAR          bRemoteInterfaceIdentifier[8];
UCHAR          bPrefix[8];
DWORD          dwPrefixLength;
ULONG64        IPv6SubInterfaceIndex;

// LCP Options
DWORD          dwLcpError;
DWORD          dwAuthenticationProtocol;
DWORD          dwAuthenticationData;
DWORD          dwRemoteAuthenticationProtocol;
DWORD          dwRemoteAuthenticationData;
DWORD          dwLcpTerminateReason;
DWORD          dwLcpRemoteTerminateReason;
DWORD          dwLcpOptions;
DWORD          dwLcpRemoteOptions;
DWORD          dwEapTypeId;
DWORD          dwRemoteEapTypeId;

// CCP options:
DWORD          dwCcpError;
DWORD          dwCompressionAlgorithm;
DWORD          dwCcpOptions;
DWORD          dwRemoteCompressionAlgorithm;
DWORD          dwCcpRemoteOptions;

} PPP_PROJECTION_INFO_1, *PPPP_PROJECTION_INFO_1;

typedef struct IKEV2_PROJECTION_INFO_1
{
    DWORD          dwIPv4NegotiationError;
    WCHAR          wszAddress[16];
    WCHAR          wszRemoteAddress[16];
    ULONG64        IPv4SubInterfaceIndex;

    DWORD          dwIPv6NegotiationError;
    UCHAR          bInterfaceIdentifier[8];
    UCHAR          bRemoteInterfaceIdentifier[8];
    UCHAR          bPrefix[8];
    DWORD          dwPrefixLength;
    ULONG64        IPv6SubInterfaceIndex;

    DWORD          dwOptions;

```

```

        DWORD                dwAuthenticationProtocol;
        DWORD                dwEapTypeId;
        DWORD                dwCompressionAlgorithm;
        DWORD                dwEncryptionMethod;

}IKEV2_PROJECTION_INFO_1, *PIKEV2_PROJECTION_INFO_1;

typedef union _PROJECTION_INFO_IDL_1 switch (UCHAR projectionInfoType) ProjectionInfoObject
{
    case 1:
        PPP_PROJECTION_INFO_1        PppProjectionInfo;
    case 2:
        IKEV2_PROJECTION_INFO_1      Ikev2ProjectionInfo;
}PROJECTION_INFO_IDL_1;

typedef struct _PROJECTION_INFO_IDL_1 *PPROJECTION_INFO_IDL_1;

typedef struct _RAS_CONNECTION_EX_1_IDL{
    MPRAPI_OBJECT_HEADER_IDL        Header;
    DWORD                dwConnectDuration;
    ROUTER_INTERFACE_TYPE           dwInterfaceType;
    DWORD                dwConnectionFlags;
    WCHAR                wszInterfaceName[257];
    WCHAR                wszUserName[257];
    WCHAR                wszLogonDomain[16];
    WCHAR                wszRemoteComputer[17];
    GUID                 guid;
    RAS_QUARANTINE_STATE            rasQuarState;

    // Probation time
    FILETIME              probationTime;

    DWORD                dwBytesXmited;
    DWORD                dwBytesRcvd;
    DWORD                dwFramesXmited;
    DWORD                dwFramesRcvd;
    DWORD                dwCrcErr;
    DWORD                dwTimeoutErr;
    DWORD                dwAlignmentErr;
    DWORD                dwHardwareOverrunErr;
    DWORD                dwFramingErr;
    DWORD                dwBufferOverrunErr;
    DWORD                dwCompressionRatioIn;
    DWORD                dwCompressionRatioOut;

    // Currently valid only for IKEV2:
    DWORD                dwNumSwitchOvers;

    // Endpoint Information
    WCHAR                wszRemoteEndpointAddress[65];
    WCHAR                wszLocalEndpointAddress[65];

    PROJECTION_INFO_IDL_1        ProjectionInfo;

    ULONG                hConnection;
    ULONG                hInterface;

```

```

} RAS_CONNECTION_EX_1_IDL, *PRAS_CONNECTION_EX_1_IDL;

typedef union _RAS_CONNECTION_EX_IDL switch (UCHAR revision) ConnObject
{
    case 1: // RAS_CONNECTION_EX with version 1: (MPRAPI_RAS_CONNECTION_OBJECT_REVISION_1)
        RAS_CONNECTION_EX_1_IDL RasConnection1;
}RAS_CONNECTION_EX_IDL;

typedef struct _RAS_CONNECTION_EX_IDL *PRAS_CONNECTION_EX_IDL;

typedef struct _CERT_BLOB_1
{
    DWORD cbData;
    [size_is(cbData)] BYTE * pbData;
}CERT_BLOB_1,*PCERT_BLOB_1;

typedef struct _IKEV2_TUNNEL_CONFIG_PARAMS_1 {
    DWORD dwIdleTimeout;
    DWORD dwNetworkBlackoutTime;
    DWORD dwSaLifeTime;
    DWORD dwSaDataSizeForRenegotiation;
    DWORD dwConfigOptions;
    DWORD dwTotalCertificates;
    [size_is(dwTotalCertificates)] CERT_BLOB_1* certificateNames;
}IKEV2_TUNNEL_CONFIG_PARAMS_1, *PIKEV2_TUNNEL_CONFIG_PARAMS_1;

typedef struct _IKEV2_CONFIG_PARAMS_1 {

    DWORD dwNumPorts;
    DWORD dwPortFlags;
    DWORD dwTunnelConfigParamFlags;
    IKEV2_TUNNEL_CONFIG_PARAMS_1 TunnelConfigParams;

}IKEV2_CONFIG_PARAMS_1, *PIKEV2_CONFIG_PARAMS_1;

typedef struct _PPTP_CONFIG_PARAMS_1 {

    DWORD dwNumPorts;
    DWORD dwPortFlags;

}PPTP_CONFIG_PARAMS_1, *PPPTP_CONFIG_PARAMS_1;

typedef struct _L2TP_CONFIG_PARAMS_1 {

    DWORD dwNumPorts;
    DWORD dwPortFlags;

}L2TP_CONFIG_PARAMS_1, *PL2TP_CONFIG_PARAMS_1;

#define MAX_SSTP_HASH_SIZE 32

typedef struct _SSTP_CERT_INFO_1
{
    BOOL isDefault;
    CERT_BLOB_1 certBlob;
}

```

```

}SSTP_CERT_INFO_1, *PSSTP_CERT_INFO_1;

typedef struct _SSTP_CONFIG_PARAMS_1 {

    DWORD                dwNumPorts;
    DWORD                dwPortFlags;
    BOOL                 isUseHttps;
    DWORD                certAlgorithm; // Always CALG_SHA_256
    SSTP_CERT_INFO_1    sstpCertDetails;

}SSTP_CONFIG_PARAMS_1, *PSSTP_CONFIG_PARAMS_1;

typedef struct _MPR_API_TUNNEL_CONFIG_PARAMS_1 {

    IKEV2_CONFIG_PARAMS_1    IkeConfigParams;

    PPTP_CONFIG_PARAMS_1     PptpConfigParams;

    L2TP_CONFIG_PARAMS_1     L2tpConfigParams;

    SSTP_CONFIG_PARAMS_1     SstpConfigParams;

}MPR_API_TUNNEL_CONFIG_PARAMS_1, *PMPR_API_TUNNEL_CONFIG_PARAMS_1;

// MPR_SERVER_EX structure are redifed in this IDL to make use of versioning:
// All the Versions of MPR_SERVER_EX will be defined here in RPC usable format:

typedef struct _MPR_SERVER_EX_1
{
    MPR_API_OBJECT_HEADER_IDL    Header;
    BOOL                         fLanOnlyMode;
    DWORD                       dwUpTime;
    DWORD                       dwTotalPorts;
    DWORD                       dwPortsInUse;
    DWORD                       Reserved; // Added so that the structure is 8 byte
aligned
    MPR_API_TUNNEL_CONFIG_PARAMS_1    ConfigParams;

}MPR_SERVER_EX_1, *PMPR_SERVER_EX_1;

typedef union _MPR_SERVER_EX_IDL switch (UCHAR revision) ServerConfigObject
{
    case 1:
        MPR_SERVER_EX_1    ServerConfig1;
}MPR_SERVER_EX_IDL;

typedef struct _MPR_SERVER_EX_IDL *PMPR_SERVER_EX_IDL;

typedef struct _MPR_SERVER_SET_CONFIG_EX_1
{
    MPR_API_OBJECT_HEADER_IDL    Header;
    DWORD                       setConfigForProtocols;
    MPR_API_TUNNEL_CONFIG_PARAMS_1    ConfigParams;

}MPR_SERVER_SET_CONFIG_EX_1, *PMPR_SERVER_SET_CONFIG_EX_1;

```



```

typedef union _MPR_SERVER_SET_CONFIG_EX_IDL switch (UCHAR revision) ServerSetConfigObject
{
    case 1:
        MPR_SERVER_SET_CONFIG_EX_1 ServerSetConfig1;
}MPR_SERVER_SET_CONFIG_EX_IDL;

typedef struct _MPR_SERVER_SET_CONFIG_EX_IDL *PMPR_SERVER_SET_CONFIG_EX_IDL;

typedef struct _RAS_UPDATE_CONNECTION_1_IDL
{
    MPRAPI_OBJECT_HEADER_IDL Header;
    DWORD dwIfIndex;
    WCHAR wszRemoteEndpointAddress[ 65 ];
} RAS_UPDATE_CONNECTION_1_IDL;

typedef struct _RAS_UPDATE_CONNECTION_1_IDL *PRAS_UPDATE_CONNECTION_1_IDL;

typedef union _RAS_UPDATE_CONNECTION_IDL switch (UCHAR revision) UpdateConnection
{
    case 1: // MPR_SERVER_UPDATE_CONNECTION_EX with version 1:
(MPRAPI_RAS_UPDATE_CONNECTION_OBJECT_REVISION_1)
        RAS_UPDATE_CONNECTION_1_IDL UpdateConnection1;
    // New ones update here
}RAS_UPDATE_CONNECTION_IDL;

typedef struct _RAS_UPDATE_CONNECTION_IDL *PRAS_UPDATE_CONNECTION_IDL;

typedef struct _DIM_INTERFACE_CONTAINER
{
    DWORD fGetInterfaceInfo;
    DWORD dwInterfaceInfoSize;
    [size_is(dwInterfaceInfoSize)] LPBYTE pInterfaceInfo;
    DWORD fGetGlobalInfo;
    DWORD dwGlobalInfoSize;
    [size_is(dwGlobalInfoSize)] LPBYTE pGlobalInfo;
}
DIM_INTERFACE_CONTAINER, *PDIM_INTERFACE_CONTAINER;

typedef struct _RTR_TOC_ENTRY
{
    ULONG InfoType;
    ULONG InfoSize;
    ULONG Count;
    ULONG Offset;
}
RTR_TOC_ENTRY, *PRTR_TOC_ENTRY;

typedef struct _RTR_INFO_BLOCK_HEADER
{
    ULONG Version;
    ULONG Size;
    ULONG TocEntriesCount;
    RTR_TOC_ENTRY TocEntry[1]; //1 is a placeholder for TocEntriesCount
}
RTR_INFO_BLOCK_HEADER, *PRTR_INFO_BLOCK_HEADER;

```

```

typedef struct _FILTER_INFO
{
    DWORD    dwSrcAddr;
    DWORD    dwSrcMask;
    DWORD    dwDstAddr;
    DWORD    dwDstMask;
    DWORD    dwProtocol;
    DWORD    fLateBound;
    WORD     wSrcPort;
    WORD     wDstPort;
}
FILTER_INFO, *PFILTER_INFO;

typedef struct _FILTER_DESCRIPTOR
{
    DWORD            dwVersion;
    DWORD            dwNumFilters;
    FORWARD_ACTION   faDefaultAction;
    FILTER_INFO       fiFilter[1];    //1 is a placeholder for dwNumFilters
}
FILTER_DESCRIPTOR, *PFILTER_DESCRIPTOR;

typedef struct _FILTER_INFO_V6
{
    BYTE            ipv6SrcAddr[16];
    DWORD            dwSrcPrefixLength;
    BYTE            ipv6DstAddr[16];
    DWORD            dwDstPrefixLength;
    DWORD            dwProtocol;
    DWORD            fLateBound;
    WORD             wSrcPort;
    WORD             wDstPort;
}
FILTER_INFO_V6, *PFILTER_INFO_V6;

typedef struct _FILTER_DESCRIPTOR_V6
{
    DWORD            dwVersion;
    DWORD            dwNumFilters;
    FORWARD_ACTION   faDefaultAction;
    FILTER_INFO_V6    fiFilter[1];    //1 is a placeholder for dwNumFilters
}
FILTER_DESCRIPTOR_V6, *PFILTER_DESCRIPTOR_V6;

typedef struct _GLOBAL_INFO
{
    IN OUT BOOL       bFilteringOn;
    IN OUT DWORD      dwLoggingLevel;
}
GLOBAL_INFO, *PGLOBAL_INFO;

```

```

typedef struct _INTERFACE_ROUTE_INFO
{
    union
    {
        struct
        { // IPv4 specific
            DWORD      dwRtInfoDest;
            DWORD      dwRtInfoMask;
            DWORD      dwRtInfoPolicy;
            DWORD      dwRtInfoNextHop;
            DWORD      dwRtInfoAge;
            DWORD      dwRtInfoNextHopAS;
            DWORD      dwRtInfoMetric1;
            DWORD      dwRtInfoMetric2;
            DWORD      dwRtInfoMetric3;
        };
        struct
        { // IPv6 specific
            IN6_ADDR    DestinationPrefix;
            DWORD      DestPrefixLength;
            IN6_ADDR    NextHopAddress;
            ULONG      ValidLifeTime;
            DWORD      Flags;
            ULONG      Metric;
        };
    };
    DWORD      dwRtInfoIfIndex;
    DWORD      dwRtInfoType;
    DWORD      dwRtInfoProto;
    DWORD      dwRtInfoPreference;
    DWORD      dwRtInfoViewSet;
    BOOL      bv4;
}
INTERFACE_ROUTE_INFO, *PINTERFACE_ROUTE_INFO;

typedef struct _PROTOCOL_METRIC
{
    IN OUT DWORD      dwProtocolId;
    IN OUT DWORD      dwMetric;
}
PROTOCOL_METRIC, *PPROTOCOL_METRIC;

typedef struct _PRIORITY_INFO
{
    IN OUT DWORD      dwNumProtocols;
    IN OUT PROTOCOL_METRIC ppmProtocolMetric[1];
}
PRIORITY_INFO, *PPRIORITY_INFO;

typedef struct _RTR_DISC_INFO
{
    IN OUT WORD      wMaxAdvtInterval;
    IN OUT WORD      wMinAdvtInterval;
}

```

```

        IN OUT WORD          wAdvtLifetime;
        IN OUT BOOL          bAdvertise;
        IN OUT LONG          lPrefLevel;
    }
    RTR_DISC_INFO, *PRTR_DISC_INFO;

#define MAX_GROUP_LEN 64

typedef struct _MCAST_HBEAT_INFO
{
    WCHAR          pwszGroup[MAX_GROUP_LEN];
    BOOL           bActive;
    ULONG          ulDeadInterval;
    BYTE           byProtocol;
    WORD           wPort;
}
MCAST_HBEAT_INFO, *PMCAST_HBEAT_INFO;

typedef struct
{
    DWORD dwTtl;
    DWORD dwRateLimit;
}
MIB_MCAST_LIMIT_ROW, *PMIB_MCAST_LIMIT_ROW;

typedef struct _IPINIP_CONFIG_INFO
{
    DWORD dwRemoteAddress;
    DWORD dwLocalAddress;
    BYTE  byTtl;
}
IPINIP_CONFIG_INFO, *PIPINIP_CONFIG_INFO;

typedef struct _INTERFACE_STATUS_INFO
{
    IN OUT DWORD dwAdminStatus;
}
INTERFACE_STATUS_INFO, *PINTERFACE_STATUS_INFO;

typedef struct _DIM_MIB_ENTRY_CONTAINER
{
    DWORD dwMibInEntrySize;
    [size_is(dwMibInEntrySize)] LPBYTE pMibInEntry;
    DWORD dwMibOutEntrySize;
    [size_is(dwMibOutEntrySize)] LPBYTE pMibOutEntry;
}
DIM_MIB_ENTRY_CONTAINER, *PDIM_MIB_ENTRY_CONTAINER;

typedef struct _MIB_IPFORWARDROW {
    DWORD dwForwardDest;

```

```

    DWORD dwForwardMask;
    DWORD dwForwardPolicy;
    DWORD dwForwardNextHop;
    DWORD dwForwardIfIndex;
    union {
        DWORD dwForwardType;
        MIB_IPFORWARD_TYPE ForwardType;
    };
    union {
        WORD dwForwardProto;
        MIB_IPFORWARD_PROTO ForwardProto;
    };
    DWORD dwForwardAge;
    DWORD dwForwardNextHopAS;
    DWORD dwForwardMetric1;
    DWORD dwForwardMetric2;
    DWORD dwForwardMetric3;
    DWORD dwForwardMetric4;
    DWORD dwForwardMetric5;
} MIB_IPFORWARDROW,
*PMIB_IPFORWARDROW;

typedef struct _MIB_IPDESTROW
{
    MIB_IPFORWARDROW ForwardRow;
    DWORD dwForwardPreference;
    DWORD dwForwardViewSet;
} MIB_IPDESTROW, *PMIB_IPDESTROW;

typedef struct _MIB_IPDESTTABLE
{
    DWORD dwNumEntries;
    MIB_IPDESTROW table[1]; //1, placeholder for dwNumEntries
} MIB_IPDESTTABLE, *PMIB_IPDESTTABLE;

typedef struct _MIB_ROUTESTATE
{
    BOOL bRoutesSetToStack;
} MIB_ROUTESTATE, *PMIB_ROUTESTATE;

typedef struct _MIB_BEST_IF {
    DWORD dwDestAddr;
    DWORD dwIfIndex;
} MIB_BEST_IF, *PMIB_BEST_IF;

typedef struct {
    DWORD dwGroupAddress;
    DWORD dwGroupMask;
} MIB_BOUNDARYROW,
*PMIB_BOUNDARYROW;

```

```

typedef struct _MIBICMPSTATS {
    DWORD dwMsgs;
    DWORD dwErrors;
    DWORD dwDestUnreachs;
    DWORD dwTimeExcds;
    DWORD dwParmProbs;
    DWORD dwSrcQuenchs;
    DWORD dwRedirects;
    DWORD dwEchos;
    DWORD dwEchoReps;
    DWORD dwTimestamps;
    DWORD dwTimestampReps;
    DWORD dwAddrMasks;
    DWORD dwAddrMaskReps;
} MIBICMPSTATS;

```

```

typedef struct _MIBICMPINFO {
    MIBICMPSTATS icmpInStats;
    MIBICMPSTATS icmpOutStats;
} MIBICMPINFO;

```

```

typedef struct _MIB_ICMP {
    MIBICMPINFO stats;
} MIB_ICMP,
*PMIB_ICMP;

```

```

typedef struct _MIB_IFNUMBER {
    DWORD dwValue;
} MIB_IFNUMBER,
*PMIB_IFNUMBER;

```

```

typedef struct _MIB_IFROW {
    WCHAR wszName[256];
    DWORD dwIndex;
    DWORD dwType;
    DWORD dwMtu;
    DWORD dwSpeed;
    DWORD dwPhysAddrLen;
    BYTE bPhysAddr[8];
    DWORD dwAdminStatus;
    DWORD dwOperStatus;
    DWORD dwLastChange;
    DWORD dwInOctets;
    DWORD dwInUcastPkts;
    DWORD dwInNUcastPkts;
    DWORD dwInDiscards;
    DWORD dwInErrors;
    DWORD dwInUnknownProtos;
    DWORD dwOutOctets;
    DWORD dwOutUcastPkts;
    DWORD dwOutNUcastPkts;
    DWORD dwOutDiscards;
    DWORD dwOutErrors;
}

```

```

        DWORD dwOutQLen;
        DWORD dwDescrLen;
        BYTE bDescr[256];        // 256, placeholder for dwDescrLen
    } MIB_IFROW;

typedef struct _MIB_IFSTATUS {
    DWORD dwIfIndex;
    DWORD dwAdminStatus;
    DWORD dwOperationalStatus;
    BOOL bMHbeatActive;
    BOOL bMHbeatAlive;
} MIB_IFSTATUS,
*PMIB_IFSTATUS;

typedef struct _MIB_IFTABLE {
    DWORD dwNumEntries;
    MIB_IFROW table[1];        //1, placeholder for dwNumEntries
} MIB_IFTABLE, *PMIB_IFTABLE;

typedef struct _MIB_IPADDRROW {
    DWORD dwAddr;
    DWORD dwIndex;
    DWORD dwMask;
    DWORD dwBCastAddr;
    DWORD dwReasmSize;
    unsigned short unused1;
    unsigned short wType;
} MIB_IPADDRROW,
*PMIB_IPADDRROW;

typedef struct _MIB_IPADDRTABLE {
    DWORD dwNumEntries;
    MIB_IPADDRROW table[1];        //1, placeholder for dwNumEntries
} MIB_IPADDRTABLE,
*PMIB_IPADDRTABLE;

typedef struct _MIB_IPFORWARDNUMBER {
    DWORD dwValue;
} MIB_IPFORWARDNUMBER,
*PMIB_IPFORWARDNUMBER;

typedef struct _MIB_IPFORWARDTABLE {
    DWORD dwNumEntries;
    MIB_IPFORWARDROW table[1];        //1, placeholder for dwNumEntries
    BYTE reserved[8];
} MIB_IPFORWARDTABLE,
*PMIB_IPFORWARDTABLE;

```

```

typedef struct {
    DWORD dwIfIndex;
    DWORD dwGroupAddress;
    DWORD dwGroupMask;
    DWORD dwStatus;
} MIB_IPMCAST_BOUNDARY,
*PMIB_IPMCAST_BOUNDARY;

typedef struct {
    DWORD dwNumEntries;
    MIB_IPMCAST_BOUNDARY table[1];    //1, placeholder for dwNumEntries
} MIB_IPMCAST_BOUNDARY_TABLE,
*PMIB_IPMCAST_BOUNDARY_TABLE;

typedef struct _MIB_IPMCAST_GLOBAL {
    DWORD dwEnable;
} MIB_IPMCAST_GLOBAL,
*PMIB_IPMCAST_GLOBAL;

typedef struct _MIB_IPMCAST_IF_ENTRY
{
    DWORD dwIfIndex;
    DWORD dwTtl;
    DWORD dwProtocol;
    DWORD dwRateLimit;
    ULONG ulInMcastOctets;
    ULONG ulOutMcastOctets;
}
MIB_IPMCAST_IF_ENTRY, *PMIB_IPMCAST_IF_ENTRY;

typedef struct _MIB_IPMCAST_IF_TABLE {
    DWORD dwNumEntries;
    MIB_IPMCAST_IF_ENTRY table[1];    //1, placeholder for dwNumEntries
} MIB_IPMCAST_IF_TABLE,
*PMIB_IPMCAST_IF_TABLE;

typedef struct _MIB_IPMCAST_OIF {
    DWORD dwOutIfIndex;
    DWORD dwNextHopAddr;
    PVOID pvReserved;
    DWORD dwReserved;
} MIB_IPMCAST_OIF,
*PMIB_IPMCAST_OIF;

```



```

typedef struct _MIB_IPMCAST_MFE {
    DWORD dwGroup;
    DWORD dwSource;
    DWORD dwSrcMask;
    DWORD dwUpStrmNgbr;
    DWORD dwInIfIndex;
    DWORD dwInIfProtocol;
    DWORD dwRouteProtocol;
    DWORD dwRouteNetwork;
    DWORD dwRouteMask;
    ULONG ulUpTime;
    ULONG ulExpiryTime;
    ULONG ulTimeOut;
    ULONG ulNumOutIf;
    DWORD fFlags;
    DWORD dwReserved;
    MIB_IPMCAST_OIF rgmioOutInfo[1];    //1, placeholder for ulNumOutIf
} MIB_IPMCAST_MFE,
*PMIB_IPMCAST_MFE;

typedef struct _MIB_IPMCAST_OIF_STATS {
    DWORD dwOutIfIndex;
    DWORD dwNextHopAddr;
    PVOID pvDialContext;
    ULONG ulTtlTooLow;
    ULONG ulFragNeeded;
    ULONG ulOutPackets;
    ULONG ulOutDiscards;
} MIB_IPMCAST_OIF_STATS,
*PMIB_IPMCAST_OIF_STATS;

typedef struct _MIB_IPMCAST_MFE_STATS {
    DWORD dwGroup;
    DWORD dwSource;
    DWORD dwSrcMask;
    DWORD dwUpStrmNgbr;
    DWORD dwInIfIndex;
    DWORD dwInIfProtocol;
    DWORD dwRouteProtocol;
    DWORD dwRouteNetwork;
    DWORD dwRouteMask;
    ULONG ulUpTime;
    ULONG ulExpiryTime;
    ULONG ulNumOutIf;
    ULONG ulInPkts;
    ULONG ulInOctets;
    ULONG ulPktsDifferentIf;
    ULONG ulQueueOverflow;
    MIB_IPMCAST_OIF_STATS rgmiosOutStats[1];    //1, placeholder for ulNumOutIf
} MIB_IPMCAST_MFE_STATS,
*PMIB_IPMCAST_MFE_STATS;

typedef struct {

```

```

        DWORD dwGroupAddress;
        DWORD dwGroupMask;
        WCHAR snNameBuffer[256];
        DWORD dwStatus;
        BYTE reserved[492];

    } MIB_IPMCAST_SCOPE,
    *PMIB_IPMCAST_SCOPE;

typedef struct _MIB_IPNETROW {
    DWORD dwIndex;
    DWORD dwPhysAddrLen;
    BYTE bPhysAddr[8];
    DWORD dwAddr;
    DWORD dwType;
} MIB_IPNETROW,
*PMIB_IPNETROW;

typedef struct _MIB_IPNETTABLE {
    DWORD dwNumEntries;
    MIB_IPNETROW table[1];    //1, placeholder for dwNumEntries
    BYTE reserved[8];
} MIB_IPNETTABLE,
*PMIB_IPNETTABLE;

typedef struct _MIB_IPSTATS {
    union {
        DWORD dwForwarding;
        MIB_IPSTATS_FORWARDING Forwarding ;
    };
    DWORD dwDefaultTTL;
    DWORD dwInReceives;
    DWORD dwInHdrErrors;
    DWORD dwInAddrErrors;
    DWORD dwForwDatagrams;
    DWORD dwInUnknownProtos;
    DWORD dwInDiscards;
    DWORD dwInDelivers;
    DWORD dwOutRequests;
    DWORD dwRoutingDiscards;
    DWORD dwOutDiscards;
    DWORD dwOutNoRoutes;
    DWORD dwReasmTimeout;
    DWORD dwReasmReqds;
    DWORD dwReasmOks;
    DWORD dwReasmFails;
    DWORD dwFragOks;
    DWORD dwFragFails;
    DWORD dwFragCreates;
    DWORD dwNumIf;
    DWORD dwNumAddr;
    DWORD dwNumRoutes;
} MIB_IPSTATS,

```

```

*PMIB_IPSTATS;

typedef struct _MIB_MFE_STATS_TABLE {
    DWORD dwNumEntries;
    MIB_IPMCAST_MFE_STATS table[1];    //1, placeholder for dwNumEntries
} MIB_MFE_STATS_TABLE,
*PMIB_MFE_STATS_TABLE;

typedef struct _MIB_MFE_TABLE {
    DWORD dwNumEntries;
    MIB_IPMCAST_MFE table[1];    //1, placeholder for dwNumEntries
} MIB_MFE_TABLE,
*PMIB_MFE_TABLE;

typedef struct _MIB_OPAQUE_INFO {
    DWORD dwId;
    union {
        ULONGLONG ullAlign;
        BYTE rgbyData[1];
    };
} MIB_OPAQUE_INFO,
*PMIB_OPAQUE_INFO;

typedef struct _MIB_OPAQUE_QUERY {
    DWORD dwVarId;
    DWORD rgdwVarIndex[1];
} MIB_OPAQUE_QUERY,
*PMIB_OPAQUE_QUERY;

typedef struct _MIB_PROXYARP {
    DWORD dwAddress;
    DWORD dwMask;
    DWORD dwIfIndex;
} MIB_PROXYARP,
*PMIB_PROXYARP;

typedef struct _MIB_TCPROW {
    union {
        DWORD dwState;
        MIB_TCP_STATE State;
    };
    DWORD dwLocalAddr;
    DWORD dwLocalPort;
    DWORD dwRemoteAddr;
    DWORD dwRemotePort;
} MIB_TCPROW,
*PMIB_TCPROW;

```

```

typedef struct _MIB_TCPSTATS {
    union {
        DWORD dwRtoAlgorithm;
        TCP_RTO_ALGORITHM RtoAlgorithm;
    };
    DWORD dwRtoMin;
    DWORD dwRtoMax;
    DWORD dwMaxConn;
    DWORD dwActiveOpens;
    DWORD dwPassiveOpens;
    DWORD dwAttemptFails;
    DWORD dwEstabResets;
    DWORD dwCurrEstab;
    DWORD dwInSegs;
    DWORD dwOutSegs;
    DWORD dwRetransSegs;
    DWORD dwInErrs;
    DWORD dwOutRsts;
    DWORD dwNumConns;
} MIB_TCPSTATS,
*PMIB_TCPSTATS;

typedef struct _MIB_TCPTABLE {
    DWORD dwNumEntries;
    MIB_TCPROW table[1];    //1, placeholder for dwNumEntries
    BYTE reserved[8];
} MIB_TCPTABLE,
*PMIB_TCPTABLE;

typedef struct _MIB_UDPROW {
    DWORD dwLocalAddr;
    DWORD dwLocalPort;
} MIB_UDPROW,
*PMIB_UDPROW;

typedef struct _MIB_UDPSTATS {
    DWORD dwInDatagrams;
    DWORD dwNoPorts;
    DWORD dwInErrors;
    DWORD dwOutDatagrams;
    DWORD dwNumAddrs;
} MIB_UDPSTATS,
*PMIB_UDPSTATS;

typedef struct _MIB_UDPTABLE {
    DWORD dwNumEntries;
    MIB_UDPROW table[1];    //1, placeholder for dwNumEntries
    BYTE reserved[8];
}

```

```
} MIB_UDPTABLE,  
*PMIB_UDPTABLE;
```

```
typedef struct MPR_SERVER_0  
{  
    BOOL    fLanOnlyMode;  
    DWORD   dwUpTime;  
    DWORD   dwTotalPorts;  
    DWORD   dwPortsInUse;  
}  
MPR_SERVER_0,*PMPR_SERVER_0;
```

```
typedef struct MPR_SERVER_1  
{  
    DWORD   dwNumPptpPorts;  
    DWORD   dwPptpPortFlags;  
    DWORD   dwNumL2tpPorts;  
    DWORD   dwL2tpPortFlags;  
}  
MPR_SERVER_1,*PMPR_SERVER_1;
```

```
typedef struct MPR_SERVER_2  
{  
    DWORD   dwNumPptpPorts;  
    DWORD   dwPptpPortFlags;  
    DWORD   dwNumL2tpPorts;  
    DWORD   dwL2tpPortFlags;  
    DWORD   dwNumSstpPorts;  
    DWORD   dwSstpPortFlags;  
}  
MPR_SERVER_2,*PMPR_SERVER_2;
```

```
typedef struct _PPP_NBFCP_INFO  
{  
    DWORD   dwError;  
    WCHAR   wszWksta[17];  
}  
PPP_NBFCP_INFO;
```

```
typedef struct _PPP_IPCP_INFO  
{  
    DWORD   dwError;  
    WCHAR   wszAddress[16];  
    WCHAR   wszRemoteAddress[16];  
}  
PPP_IPCP_INFO;
```

```

typedef struct _PPP_IPCP_INFO2
{
    DWORD dwError;
    WCHAR wszAddress[16];
    WCHAR wszRemoteAddress[16];
    DWORD dwOptions;
    DWORD dwRemoteOptions;
}
PPP_IPCP_INFO2;

typedef struct _PPP_IPXCP_INFO
{
    DWORD dwError;
    WCHAR wszAddress[16];
}
PPP_IPXCP_INFO;

typedef struct _PPP_IPV6CP_INFO
{
    DWORD dwVersion;
    DWORD dwSize;
    DWORD dwError;
    BYTE bInterfaceIdentifier[8];
    BYTE bRemoteInterfaceIdentifier[8];
    DWORD dwOptions;
    DWORD dwRemoteOptions;
    BYTE bPrefix[8];
    DWORD dwPrefixLength;
}
PPP_IPV6_CP_INFO, *PPPP_IPV6_CP_INFO;

typedef struct _PPP_ATCP_INFO
{
    DWORD dwError;
    WCHAR wszAddress[33];
}
PPP_ATCP_INFO;

typedef struct _PPP_CCP_INFO
{
    DWORD dwError;
    DWORD dwCompressionAlgorithm;
    DWORD dwOptions;
    DWORD dwRemoteCompressionAlgorithm;
    DWORD dwRemoteOptions;
}
PPP_CCP_INFO;

typedef struct _PPP_LCP_INFO

```

```

{
    DWORD dwError;
    DWORD dwAuthenticationProtocol;
    DWORD dwAuthenticationData;
    DWORD dwRemoteAuthenticationProtocol;
    DWORD dwRemoteAuthenticationData;
    DWORD dwTerminateReason;
    DWORD dwRemoteTerminateReason;
    DWORD dwOptions;
    DWORD dwRemoteOptions;
    DWORD dwEapTypeId;
    DWORD dwRemoteEapTypeId;
}
PPP_LCP_INFO;

typedef struct _PPP_INFO
{
    PPP_NBFCP_INFO nbfc;
    PPP_IPCP_INFO ip;
    PPP_IPXCP_INFO ipx;
    PPP_ATCP_INFO at;
}
PPP_INFO;

typedef struct _PPP_INFO_2
{
    PPP_NBFCP_INFO nbfc;
    PPP_IPCP_INFO2 ip;
    PPP_IPXCP_INFO ipx;
    PPP_ATCP_INFO at;
    PPP_CCP_INFO ccp;
    PPP_LCP_INFO lcp;
}
PPP_INFO_2;

typedef struct _PPP_INFO_3
{
    PPP_NBFCP_INFO nbfc;
    PPP_IPCP_INFO2 ip;
    PPP_IPV6_CP_INFO ipv6;
    PPP_CCP_INFO ccp;
    PPP_LCP_INFO lcp;
}
PPP_INFO_3;

typedef struct _RASI_PORT_0
{
    DWORD dwPort;
    DWORD dwConnection;
    RAS_PORT_CONDITION dwPortCondition;
    DWORD dwTotalNumberOfCalls;
}

```

```

        DWORD                dwConnectDuration;
        WCHAR                wszPortName[17];
        WCHAR                wszMediaName[17];
        WCHAR                wszDeviceName[129];
        WCHAR                wszDeviceType[17];
    }
    RASI_PORT_0,*PRASI_PORT_0;

typedef struct _RASI_PORT_1
{
    DWORD                dwPort;
    DWORD                dwConnection;
    RAS_HARDWARE_CONDITION dwHardwareCondition;
    DWORD                dwLineSpeed;
    DWORD                dwBytesXmited;
    DWORD                dwBytesRcvd;
    DWORD                dwFramesXmited;
    DWORD                dwFramesRcvd;
    DWORD                dwCrcErr;
    DWORD                dwTimeoutErr;
    DWORD                dwAlignmentErr;
    DWORD                dwHardwareOverrunErr;
    DWORD                dwFramingErr;
    DWORD                dwBufferOverrunErr;
    DWORD                dwCompressionRatioIn;
    DWORD                dwCompressionRatioOut;
}
    RASI_PORT_1,*PRASI_PORT_1;

```

```

typedef struct _RASI_CONNECTION_0
{
    DWORD                dwConnection;
    DWORD                dwInterface;
    DWORD                dwConnectDuration;
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    DWORD                dwConnectionFlags;
    WCHAR                wszInterfaceName[257];
    WCHAR                wszUserName[257];
    WCHAR                wszLogonDomain[16];
    WCHAR                wszRemoteComputer[17];
}
    RASI_CONNECTION_0,*PRASI_CONNECTION_0;

```

```

typedef struct RASI_CONNECTION_1
{
    DWORD                dwConnection;
    DWORD                dwInterface;
    PPP_INFO             PppInfo;
    DWORD                dwBytesXmited;
    DWORD                dwBytesRcvd;
    DWORD                dwFramesXmited;
    DWORD                dwFramesRcvd;
    DWORD                dwCrcErr;
}

```



```

        DWORD    dwTimeoutErr;
        DWORD    dwAlignmentErr;
        DWORD    dwHardwareOverrunErr;
        DWORD    dwFramingErr;
        DWORD    dwBufferOverrunErr;
        DWORD    dwCompressionRatioIn;
        DWORD    dwCompressionRatioOut;
    }
    RASI_CONNECTION_1,*PRASI_CONNECTION_1;

```

```

typedef struct _RASI_CONNECTION_2
{
    DWORD    dwConnection;
    WCHAR    wszUserName[257];
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    GUID     guid;
    PPP_INFO_2    PppInfo2;
}
RASI_CONNECTION_2,*PRASI_CONNECTION_2;

```

```

typedef struct _RASI_CONNECTION_3
{
    DWORD    dwVersion;
    DWORD    dwSize;
    DWORD    dwConnection;
    WCHAR    wszUserName[257];
    ROUTER_INTERFACE_TYPE dwInterfaceType;
    GUID     guid;
    PPP_INFO_3    PppInfo3;
    RAS_QUARANTINE_STATE rasQuarState;
    FILETIME    timer;
}
RASI_CONNECTION_3,*PRASI_CONNECTION_3;

```

```

typedef struct _MPRI_INTERFACE_0
{
    WCHAR    wszInterfaceName[257];
    DWORD    dwInterface;
    BOOL     fEnabled;
    ROUTER_INTERFACE_TYPE dwIfType;
    ROUTER_CONNECTION_STATE dwConnectionState;
    DWORD    fUnReachabilityReasons;
    DWORD    dwLastError;
}
MPRI_INTERFACE_0,*PMPRI_INTERFACE_0;

```

```

typedef struct _MPRI_INTERFACE_1
{
    WCHAR    wszInterfaceName[257];
    DWORD    dwInterface;
    BOOL     fEnabled;
}

```

```

ROUTER_INTERFACE_TYPE    dwIfType;
ROUTER_CONNECTION_STATE  dwConnectionState;
DWORD                    fUnReachabilityReasons;
DWORD                    dwLastError;
LPWSTR                    lpwsDialoutHoursRestriction;
}
MPRI_INTERFACE_1, *PMPRI_INTERFACE_1;

```

```

typedef struct _MPRI_INTERFACE_2
{
    WCHAR                wszInterfaceName[257];
    DWORD                dwInterface;
    BOOL                 fEnabled;
    ROUTER_INTERFACE_TYPE dwIfType;
    ROUTER_CONNECTION_STATE dwConnectionState;
    DWORD                fUnReachabilityReasons;
    DWORD                dwLastError;
    DWORD                dwfOptions;
    WCHAR                szLocalPhoneNumber[129];
    PWCHAR                szAlternates;
    DWORD                ipaddr;
    DWORD                ipaddrDns;
    DWORD                ipaddrDnsAlt;
    DWORD                ipaddrWins;
    DWORD                ipaddrWinsAlt;
    DWORD                dwfNetProtocols;
    WCHAR                szDeviceType[17];
    WCHAR                szDeviceName[129];
    WCHAR                szX25PadType[33];
    WCHAR                szX25Address[201];
    WCHAR                szX25Facilities[201];
    WCHAR                szX25UserData[201];
    DWORD                dwChannels;
    DWORD                dwSubEntries;
    DWORD                dwDialMode;
    DWORD                dwDialExtraPercent;
    DWORD                dwDialExtraSampleSeconds;
    DWORD                dwHangUpExtraPercent;
    DWORD                dwHangUpExtraSampleSeconds;
    DWORD                dwIdleDisconnectSeconds;
    DWORD                dwType;
    DWORD                dwEncryptionType;
    DWORD                dwCustomAuthKey;
    DWORD                dwCustomAuthDataSize;
    LPBYTE                lpbCustomAuthData;
    GUID                 guidId;
    DWORD                dwVpnStrategy;
}
MPRI_INTERFACE_2, *PMPRI_INTERFACE_2;

```

```

typedef struct _MPR_INTERFACE_3
{
    WCHAR                wszInterfaceName[257];
    DWORD                dwInterface;
    BOOL                 fEnabled;
}

```

```

ROUTER_INTERFACE_TYPE    dwIfType;
ROUTER_CONNECTION_STATE  dwConnectionState;
DWORD                    fUnReachabilityReasons;
DWORD                    dwLastError;
DWORD                    dwfOptions;
WCHAR                    szLocalPhoneNumber[129];
PWCHAR                   szAlternates;
DWORD                    ipaddr;
DWORD                    ipaddrDns;
DWORD                    ipaddrDnsAlt;
DWORD                    ipaddrWins;
DWORD                    ipaddrWinsAlt;
DWORD                    dwfNetProtocols;
WCHAR                    szDeviceType[17];
WCHAR                    szDeviceName[129];
WCHAR                    szX25PadType[33];
WCHAR                    szX25Address[201];
WCHAR                    szX25Facilities[201];
WCHAR                    szX25UserData[201];
DWORD                    dwChannels;
DWORD                    dwSubEntries;
DWORD                    dwDialMode;
DWORD                    dwDialExtraPercent;
DWORD                    dwDialExtraSampleSeconds;
DWORD                    dwHangUpExtraPercent;
DWORD                    dwHangUpExtraSampleSeconds;
DWORD                    dwIdleDisconnectSeconds;
DWORD                    dwType;
DWORD                    dwEncryptionType;
DWORD                    dwCustomAuthKey;
DWORD                    dwCustomAuthDataSize;
LPBYTE                   lpbCustomAuthData;
GUID                     guidId;
DWORD                    dwVpnStrategy;
ULONG                    AddressCount;
IN6_ADDR                 ipv6addrDns;
IN6_ADDR                 ipv6addrDnsAlt;
IN6_ADDR*                ipv6addr;
}

MPRI_INTERFACE_3,*PMPRI_INTERFACE_3;

```

```

typedef struct _MPR_DEVICE_0
{
    WCHAR szDeviceType[17];
    WCHAR szDeviceName[129];
}
MPR_DEVICE_0,*PMPR_DEVICE_0;

```

```

typedef struct _MPR_DEVICE_1
{
    WCHAR szDeviceType[17];
    WCHAR szDeviceName[129];
    WCHAR szLocalPhoneNumber[129];
    PWCHAR szAlternates;
}

```

```
MPR_DEVICE_1,*PMPR_DEVICE_1;
```

```
typedef struct _MPR_CREDENTIALSEX_1
{
    DWORD    dwSize;
    DWORD    dwOffset;
    BYTE     bData[1];
} MPR_CREDENTIALSEX_1, *PMPR_CREDENTIALSEX_1;
```

```
typedef struct _IFFILTER_INFO
{
    BOOL     bEnableFragChk;
} IFFILTER_INFO, *PIFFILTER_INFO;
```

```
typedef struct _MPR_FILTER_0
{
    IN BOOL fEnable;
}
MPR_FILTER_0, *PMPR_FILTER_0;
```

```
typedef struct _IPX_GLOBAL_INFO {
    ULONG    RoutingTableHashSize;
    ULONG    EventLogMask;
} IPX_GLOBAL_INFO, *PIPX_GLOBAL_INFO;
```

```
typedef struct _IPX_IF_INFO {
    ULONG    AdministratorState;
    ULONG    NetbiosAccept;      //
    ULONG    NetbiosDeliver;     // Deliver Netbios broadcast packets
} IPX_IF_INFO, *PIPX_IF_INFO;
```

```
typedef struct _IPXWAN_IF_INFO {
    ULONG    Adminstate;
} IPXWAN_IF_INFO, *PIPXWAN_IF_INFO;
```

```
typedef struct _IPX_STATIC_ROUTE_INFO {
    union {
        ULONG DwordAlign;
        UCHAR Network[4];
    };
    USHORT TickCount;
    USHORT HopCount;
    UCHAR NextHopMacAddress[6];
} IPX_STATIC_ROUTE_INFO, *PIPX_STATIC_ROUTE_INFO;
```

```
typedef IPX_SERVER_ENTRY IPX_STATIC_SERVICE_INFO, *PIPX_STATIC_SERVICE_INFO;
```

```
typedef struct _IPX_SERVER_ENTRY
{
    USHORT Type;
    UCHAR Name[48];
    UCHAR Network[4];
    UCHAR Node[6];
    UCHAR Socket[2];
    USHORT HopCount;
} IPX_SERVER_ENTRY, *PIPX_SERVER_ENTRY;
```

```
typedef struct _IPX_STATIC_NETBIOS_NAME_INFO {
    union {
        ULONG DwordAlign;
        UCHAR Name[16];
    };
} IPX_STATIC_NETBIOS_NAME_INFO, *PIPX_STATIC_NETBIOS_NAME_INFO;
```

```
#define MAX_ADAPTOR_NAME_LEN 48
```

```
typedef struct _IPX_ADAPTER_INFO {
    ULONG PacketType;
    WCHAR AdapterName[MAX_ADAPTOR_NAME_LEN];
} IPX_ADAPTER_INFO, *PIPX_ADAPTER_INFO;
```

```
typedef struct _IPX_TRAFFIC_FILTER_GLOBAL_INFO {
    ULONG FilterAction;
} IPX_TRAFFIC_FILTER_GLOBAL_INFO, *PIPX_TRAFFIC_FILTER_GLOBAL_INFO;
```

```
typedef struct _IPX_TRAFFIC_FILTER_INFO {
    ULONG FilterDefinition;
    UCHAR DestinationNetwork[4];
    UCHAR DestinationNetworkMask[4];
    UCHAR DestinationNode[6];
    UCHAR DestinationSocket[2];
    UCHAR SourceNetwork[4];
    UCHAR SourceNetworkMask[4];
    UCHAR SourceNode[6];
    UCHAR SourceSocket[2];
    UCHAR PacketType;
} IPX_TRAFFIC_FILTER_INFO, *PIPX_TRAFFIC_FILTER_INFO;
```

```

typedef struct _IF_TABLE_INDEX {
    ULONG InterfaceIndex;
} IF_TABLE_INDEX, *PIF_TABLE_INDEX;

typedef struct _ROUTING_TABLE_INDEX {
    UCHAR Network[4];
} ROUTING_TABLE_INDEX, *PROUTING_TABLE_INDEX;

typedef struct _STATIC_ROUTES_TABLE_INDEX {
    ULONG InterfaceIndex;
    UCHAR Network[4];
} STATIC_ROUTES_TABLE_INDEX, *PSTATIC_ROUTES_TABLE_INDEX;

typedef struct _SERVICES_TABLE_INDEX {
    USHORT ServiceType;
    UCHAR ServiceName[48];
} SERVICES_TABLE_INDEX, *PSERVICES_TABLE_INDEX;

typedef struct _STATIC_SERVICES_TABLE_INDEX {
    ULONG InterfaceIndex;
    USHORT ServiceType;
    UCHAR ServiceName[48];
} STATIC_SERVICES_TABLE_INDEX, *PSTATIC_SERVICES_TABLE_INDEX;

typedef union _IPX_MIB_INDEX {
    IF_TABLE_INDEX InterfaceTableIndex;
    ROUTING_TABLE_INDEX RoutingTableIndex;
    STATIC_ROUTES_TABLE_INDEX StaticRoutesTableIndex;
    SERVICES_TABLE_INDEX ServicesTableIndex;
    STATIC_SERVICES_TABLE_INDEX StaticServicesTableIndex;
} IPX_MIB_INDEX, *PIPX_MIB_INDEX;

typedef struct _IPX_MIB_GET_INPUT_DATA {
    ULONG TableId;
    IPX_MIB_INDEX MibIndex;
} IPX_MIB_GET_INPUT_DATA, *PIPX_MIB_GET_INPUT_DATA;

typedef struct _IPXMIB_BASE {
    ULONG OperState;
    UCHAR PrimaryNetNumber[4];
    UCHAR Node[6];
    UCHAR SysName[48];
    ULONG MaxPathSplits;
    ULONG IfCount;
}

```

```

        ULONG        DestCount;
        ULONG        ServCount;
    } IPXMIB_BASE, *PIPMIB_BASE;

```

```

typedef struct _IPX_IF_STATS {
    ULONG IfOperState;
    ULONG MaxPacketSize;
    ULONG InHdrErrors;
    ULONG InFiltered;
    ULONG InNoRoutes;
    ULONG InDiscards;
    ULONG InDelivers;
    ULONG OutFiltered;
    ULONG OutDiscards;
    ULONG OutDelivers;
    ULONG NetbiosReceived;
    ULONG NetbiosSent;
} IPX_IF_STATS, *PIPX_IF_STATS;

```

```

typedef struct _IPX_INTERFACE {
    ULONG        InterfaceIndex;
    ULONG        AdministratorState;
    ULONG        AdapterIndex;
    UCHAR        InterfaceName[48];
    ULONG        InterfaceType;
    ULONG        MediaType;
    UCHAR        NetNumber[4];
    UCHAR        MacAddress[6];
    ULONG        Delay;
    ULONG        Throughput;
    ULONG        NetbiosAccept;
    ULONG        NetbiosDeliver;
    ULONG        EnableIpxWanNegotiation;
    IPX_IF_STATS IfStats;
} IPX_INTERFACE, *PIPX_INTERFACE;

```

```

typedef struct _IPX_ROUTE {
    ULONG InterfaceIndex;
    ULONG Protocol;
    UCHAR Network[4];
    USHORT TickCount;
    USHORT HopCount;
    UCHAR NextHopMacAddress[6];
    ULONG Flags;
} IPX_ROUTE, *PIPX_ROUTE;

```

```

typedef struct _IPX_SERVICE
{
    ULONG        InterfaceIndex;
    ULONG        Protocol;
    IPX_SERVER_ENTRY Server;
}

```

```

} IPX_SERVICE, *PIPX_SERVICE;

typedef union _IPX_MIB_ROW {
    IPX_INTERFACE Interface;
    IPX_ROUTE Route;
    IPX_SERVICE Service;
} IPX_MIB_ROW, *PIPX_MIB_ROW;

typedef struct _IPX_MIB_SET_INPUT_DATA {
    ULONG TableId;
    IPX_MIB_ROW MibRow;
} IPX_MIB_SET_INPUT_DATA, *PIPX_MIB_SET_INPUT_DATA;

typedef struct _SAP_SERVICE_FILTER_INFO {
    union {
        USHORT ServiceType;
        ULONG ServiceType_align; // Ensures alignment
    };
    UCHAR ServiceName[48];
} SAP_SERVICE_FILTER_INFO, *PSAP_SERVICE_FILTER_INFO;

typedef struct _SAP_IF_FILTERS {
    ULONG SupplyFilterAction;
    ULONG SupplyFilterCount;
    ULONG ListenFilterAction;
    ULONG ListenFilterCount;
    SAP_SERVICE_FILTER_INFO ServiceFilter[1];
} SAP_IF_FILTERS, *PSAP_IF_FILTERS;

typedef struct _SAP_IF_INFO {
    ULONG AdminState;
    ULONG UpdateMode;
    ULONG PacketType;
    ULONG Supply;
    ULONG Listen;
    ULONG GetNearestServerReply;
    ULONG PeriodicUpdateInterval;
    ULONG AgeIntervalMultiplier;
} SAP_IF_INFO, *PSAP_IF_INFO;

typedef struct _SAP_IF_CONFIG {
    SAP_IF_INFO SapIfInfo;
    SAP_IF_FILTERS SapIfFilters;
} SAP_IF_CONFIG, *PSAP_IF_CONFIG;

typedef struct _SAP_MIB_BASE {

```



```

        ULONG      SapOperState;
    } SAP_MIB_BASE, *PSAP_MIB_BASE;

typedef struct _SAP_IF_STATS {
    ULONG      SapIfOperState;
    ULONG      SapIfInputPackets;
    ULONG      SapIfOutputPackets;
} SAP_IF_STATS, *PSAP_IF_STATS;

typedef struct _SAP_INTERFACE {
    ULONG      InterfaceIndex;
    SAP_IF_INFO SapIfInfo;
    SAP_IF_STATS SapIfStats;
} SAP_INTERFACE, *PSAP_INTERFACE;

typedef struct _SAP_MIB_GET_INPUT_DATA {
    ULONG TableId;
    ULONG InterfaceIndex;
} SAP_MIB_GET_INPUT_DATA, *PSAP_MIB_GET_INPUT_DATA;

typedef struct _SAP_MIB_SET_INPUT_DATA {
    ULONG TableId;
    SAP_INTERFACE SapInterface;
} SAP_MIB_SET_INPUT_DATA, *PSAP_MIB_SET_INPUT_DATA;

typedef struct _RIPMIB_BASE {
    ULONG RIPOperState;
} RIPMIB_BASE, *PRIPMIB_BASE;

typedef struct _RIP_IF_STATS {
    ULONG      RipIfOperState;
    ULONG      RipIfInputPackets;
    ULONG      RipIfOutputPackets;
} RIP_IF_STATS, *PRIP_IF_STATS;

typedef struct _RIP_IF_INFO {
    ULONG      AdminState;
    ULONG      UpdateMode;
    ULONG      PacketType;
    ULONG      Supply;
    ULONG      Listen;
    ULONG      PeriodicUpdateInterval;
}

```

```

        ULONG    AgeIntervalMultiplier;
    } RIP_IF_INFO, *PRIP_IF_INFO;

typedef struct _RIP_INTERFACE {
    ULONG    InterfaceIndex;
    RIP_IF_INFO    RipIfInfo;
    RIP_IF_STATS    RipIfStats;
} RIP_INTERFACE, *PRIP_INTERFACE;

typedef struct _RIP_MIB_GET_INPUT_DATA {
    ULONG TableId;
    ULONG InterfaceIndex;
} RIP_MIB_GET_INPUT_DATA, *PRIP_MIB_GET_INPUT_DATA;

typedef struct _RIP_MIB_SET_INPUT_DATA {
    ULONG TableId;
    RIP_INTERFACE RipInterface;
} RIP_MIB_SET_INPUT_DATA, *PRIP_MIB_SET_INPUT_DATA;

typedef struct _EAPTLS_HASH
{
    DWORD    cbHash;
    BYTE    pbHash[20];
} EAPTLS_HASH;

typedef struct _EAPTLS_USER_PROPERTIES
{
    DWORD    reserved;
    DWORD    dwVersion;
    DWORD    dwSize;
    DWORD    fFlags;
    EAPTLS_HASH Hash;
    WCHAR*    pwszDiffUser;
    DWORD    dwPinOffset;
    WCHAR*    pwszPin;
    USHORT    usLength;
    USHORT    usMaximumLength;
    UCHAR    ucSeed;
    WCHAR    awszString[1];
} EAPTLS_USER_PROPERTIES;

typedef struct _IPBOOTP_GLOBAL_CONFIG {
    DWORD    GC_LoggingLevel;
    DWORD    GC_MaxRecvQueueSize;
    DWORD    GC_ServerCount;
} IPBOOTP_GLOBAL_CONFIG, *PIPBOOTP_GLOBAL_CONFIG;

typedef struct _IPBOOTP_IF_CONFIG {
    DWORD    IC_State;

```

```

        DWORD        IC_RelayMode;
        DWORD        IC_MaxHopCount;
        DWORD        IC_MinSecondsSinceBoot;
    } IPBOOTP_IF_CONFIG, *PIBOOTP_IF_CONFIG;

typedef struct _IPBOOTP_MIB_GET_INPUT_DATA {
    DWORD        IMGID_TypeID;
    DWORD        IMGID_IfIndex;
} IPBOOTP_MIB_GET_INPUT_DATA, *PIBOOTP_MIB_GET_INPUT_DATA;

typedef struct _IPBOOTP_MIB_GET_OUTPUT_DATA {
    DWORD        IMGOD_TypeID;
    DWORD        IMGOD_IfIndex;
    BYTE        IMGOD_Buffer[1];
} IPBOOTP_MIB_GET_OUTPUT_DATA, *PIBOOTP_MIB_GET_OUTPUT_DATA;

typedef struct _IPBOOTP_IF_STATS {
    DWORD        IS_State;
    DWORD        IS_SendFailures;
    DWORD        IS_ReceiveFailures;
    DWORD        IS_ArpUpdateFailures;
    DWORD        IS_RequestsReceived;
    DWORD        IS_RequestsDiscarded;
    DWORD        IS_RepliesReceived;
    DWORD        IS_RepliesDiscarded;
} IPBOOTP_IF_STATS, *PIBOOTP_IF_STATS;

typedef struct _IPBOOTP_IF_BINDING {
    DWORD        IB_State;
    DWORD        IB_AddrCount;
} IPBOOTP_IF_BINDING, *PIBOOTP_IF_BINDING;

typedef struct _IPBOOTP_IP_ADDRESS {
    DWORD        IA_Address;
    DWORD        IA_Netmask;
} IPBOOTP_IP_ADDRESS, *PIBOOTP_IP_ADDRESS;

typedef struct _DHCPV6R_MIB_GET_OUTPUT_DATA {
    DWORD        IMGOD_TypeID; // Type of the data received
    DWORD        IMGOD_IfIndex;
    BYTE        IMGOD_Buffer[1];
} DHCPV6R_MIB_GET_OUTPUT_DATA, *PDHCPV6R_MIB_GET_OUTPUT_DATA;

typedef struct _DHCPV6R_IF_STATS {
    DWORD        IS_State;
    DWORD        IS_SendFailures;
    DWORD        IS_ReceiveFailures;
    DWORD        IS_RequestsReceived;
    DWORD        IS_RequestsDiscarded;
    DWORD        IS_RepliesReceived;
    DWORD        IS_RepliesDiscarded;
} DHCPV6R_IF_STATS, *PDHCPV6R_IF_STATS;

typedef struct _DHCPV6R_MIB_GET_INPUT_DATA {
    DWORD        IMGID_TypeID; // Type of the data to get
    DWORD        IMGID_IfIndex;
} DHCPV6R_MIB_GET_INPUT_DATA, *PDHCPV6R_MIB_GET_INPUT_DATA;

```

```

typedef struct _DHCPV6R_GLOBAL_CONFIG {
    DWORD      GC_LoggingLevel;
    DWORD      GC_MaxRecvQueueSize;
    DWORD      GC_ServerCount;
} DHCPV6R_GLOBAL_CONFIG, *PDHCPV6R_GLOBAL_CONFIG;

typedef struct _DHCPV6R_IF_CONFIG {
    DWORD      IC_State;
    DWORD      IC_RelayMode;
    DWORD      IC_MaxHopCount;
    DWORD      IC_MinElapsedTime;
} DHCPV6R_IF_CONFIG, *PDHCPV6R_IF_CONFIG;

typedef struct _IPRIP_MIB_GET_INPUT_DATA {
    DWORD      IMGID_TypeID;
    union {
        DWORD   IMGID_IfIndex;
        DWORD   IMGID_PeerAddress;
    };
} IPRIP_MIB_GET_INPUT_DATA, *PIPRIP_MIB_GET_INPUT_DATA;

typedef struct _IPRIP_MIB_GET_OUTPUT_DATA {
    DWORD      IMGOD_TypeID;
    union {
        DWORD   IMGOD_IfIndex;
        DWORD   IMGOD_PeerAddress;
    };
    BYTE       IMGOD_Buffer[1];
} IPRIP_MIB_GET_OUTPUT_DATA, *PIPRIP_MIB_GET_OUTPUT_DATA;

typedef struct _IPRIP_GLOBAL_STATS {
    DWORD      GS_SystemRouteChanges;
    DWORD      GS_TotalResponsesSent;
} IPRIP_GLOBAL_STATS, *PIPRIP_GLOBAL_STATS;

typedef struct _IPRIP_GLOBAL_CONFIG {
    DWORD      GC_LoggingLevel;
    DWORD      GC_MaxRecvQueueSize;
    DWORD      GC_MaxSendQueueSize;
    DWORD      GC_MinTriggeredUpdateInterval;
    DWORD      GC_PeerFilterMode;
    DWORD      GC_PeerFilterCount;
} IPRIP_GLOBAL_CONFIG, *PIPRIP_GLOBAL_CONFIG;

typedef struct _IPRIP_IF_STATS {
    DWORD      IS_State;
    DWORD      IS_SendFailures;
    DWORD      IS_ReceiveFailures;
    DWORD      IS_RequestsSent;
    DWORD      IS_RequestsReceived;
    DWORD      IS_ResponsesSent;
    DWORD      IS_ResponsesReceived;
    DWORD      IS_BadResponsePacketsReceived;
    DWORD      IS_BadResponseEntriesReceived;
    DWORD      IS_TriggeredUpdatesSent;
} IPRIP_IF_STATS, *PIPRIP_IF_STATS;

typedef struct _IPRIP_IF_CONFIG {
    DWORD      IC_State;

```

```

        DWORD        IC_Metric;
        DWORD        IC_UpdateMode;
        DWORD        IC_AcceptMode;
        DWORD        IC_AnnounceMode;
        DWORD        IC_ProtocolFlags;
        DWORD        IC_RouteExpirationInterval;
        DWORD        IC_RouteRemovalInterval;
        DWORD        IC_FullUpdateInterval;
        DWORD        IC_AuthenticationType;
        BYTE         IC_AuthenticationKey[ 16];
        WORD         IC_RouteTag;
        DWORD        IC_UnicastPeerMode;
        DWORD        IC_AcceptFilterMode;
        DWORD        IC_AnnounceFilterMode;
        DWORD        IC_UnicastPeerCount;
        DWORD        IC_AcceptFilterCount;
        DWORD        IC_AnnounceFilterCount;
    } IPRIP_IF_CONFIG, *PIPRIP_IF_CONFIG;

typedef struct _IPRIP_ROUTE_FILTER {
    DWORD        RF_LoAddress;
    DWORD        RF_HiAddress;
} IPRIP_ROUTE_FILTER, *PIPRIP_ROUTE_FILTER;

typedef struct _IPRIP_IF_BINDING {
    DWORD        IB_State;
    DWORD        IB_AddrCount;
} IPRIP_IF_BINDING, *PIPRIP_IF_BINDING;

typedef struct _IPRIP_IP_ADDRESS {
    DWORD        IA_Address;
    DWORD        IA_Netmask;
} IPRIP_IP_ADDRESS, *PIPRIP_IP_ADDRESS;

typedef struct _IPRIP_PEER_STATS {
    DWORD        PS_LastPeerRouteTag;
    DWORD        PS_LastPeerUpdateTickCount;
    DWORD        PS_LastPeerUpdateVersion;
    DWORD        PS_BadResponsePacketsFromPeer;
    DWORD        PS_BadResponseEntriesFromPeer;
} IPRIP_PEER_STATS, *PIPRIP_PEER_STATS;

typedef struct _IGMP_MIB_GROUP_SOURCE_INFO_V3 {
    DWORD        Source;
    DWORD        SourceExpiryTime;    //not valid for exclusion mode
    DWORD        SourceUpTime;
    DWORD        Flags;
} IGMP_MIB_GROUP_SOURCE_INFO_V3, *PIGMP_MIB_GROUP_SOURCE_INFO_V3;

typedef struct _IGMP_MIB_GET_INPUT_DATA {
    DWORD        TypeId;
    USHORT       Flags;
    USHORT       Signature;
    DWORD        IfIndex;
    DWORD        RasClientAddr;
    DWORD        GroupAddr;
    DWORD        Count;
} IGMP_MIB_GET_INPUT_DATA, *PIGMP_MIB_GET_INPUT_DATA;

```

```

typedef struct _IGMP_MIB_GET_OUTPUT_DATA {
    DWORD      TypeId;
    DWORD      Flags; //IGMP_ENUM_FORMAT_IGMPV3 set if v3 struct
    DWORD      Count;
    BYTE       Buffer[1];
} IGMP_MIB_GET_OUTPUT_DATA, *PIGMP_MIB_GET_OUTPUT_DATA;

typedef struct _IGMP_MIB_GLOBAL_CONFIG {
    DWORD      Version;
    DWORD      LoggingLevel;
    DWORD      RasClientStats;
} IGMP_MIB_GLOBAL_CONFIG, *PIGMP_MIB_GLOBAL_CONFIG;

typedef struct _IGMP_MIB_GLOBAL_STATS {
    DWORD      CurrentGroupMemberships;
    DWORD      GroupMembershipsAdded;
} IGMP_MIB_GLOBAL_STATS, *PIGMP_MIB_GLOBAL_STATS;

typedef struct _IGMP_MIB_IF_BINDING {
    DWORD      IfIndex;
    DWORD      IfType;
    DWORD      State;
    DWORD      AddrCount;
} IGMP_MIB_IF_BINDING, *PIGMP_MIB_IF_BINDING;

typedef struct _IGMP_MIB_IF_CONFIG {
    DWORD      Version;
    DWORD      IfIndex; //read only:index
    DWORD      IpAddr;  //read only
    DWORD      IfType;  //read only
    DWORD      Flags;
    DWORD      IgmpProtocolType;
    DWORD      RobustnessVariable;
    DWORD      StartupQueryInterval;
    DWORD      StartupQueryCount;
    DWORD      GenQueryInterval;
    DWORD      GenQueryMaxResponseTime;
    DWORD      LastMemQueryInterval;
    DWORD      LastMemQueryCount;
    DWORD      OtherQuerierPresentInterval; //read only
    DWORD      GroupMembershipTimeout;      //read only
    DWORD      NumStaticGroups;
} IGMP_MIB_IF_CONFIG, *PIGMP_MIB_IF_CONFIG;

typedef struct _IGMP_MIB_IF_GROUPS_LIST {
    DWORD      IfIndex;
    DWORD      IpAddr;
    DWORD      IfType;
    DWORD      NumGroups;
    BYTE       Buffer[1];
} IGMP_MIB_IF_GROUPS_LIST, *PIGMP_MIB_IF_GROUPS_LIST;

typedef struct _IGMP_MIB_GROUP_INFO {
    union {
        DWORD      IfIndex;
        DWORD      GroupAddr;
    };
    DWORD      IpAddr;

```

```

        DWORD      GroupUpTime;
        DWORD      GroupExpiryTime;
        DWORD      LastReporter;
        DWORD      V1HostPresentTimeLeft;
        DWORD      Flags;
    } IGMP_MIB_GROUP_INFO, *PIGMP_MIB_GROUP_INFO;

typedef struct _IGMP_MIB_IF_STATS {
    DWORD      IfIndex;                // same as in MIB_IF_CONFIG
    DWORD      IpAddr;                // same as in MIB_IF_CONFIG
    DWORD      IfType;                // same as in MIB_IF_CONFIG
    BYTE      State;                // bound/enabled
    BYTE      QuerierState;            // (not)querier
    DWORD      IgmpProtocolType;        // router/proxy, and ver(1/2/3)
    DWORD      QuerierIpAddr;
    DWORD      ProxyIfIndex;            // IfIndex of proxy(req by mib)
    DWORD      QuerierPresentTimeLeft;
    DWORD      LastQuerierChangeTime;
    DWORD      V1QuerierPresentTimeLeft; //obsolete
    DWORD      Uptime;                // seconds it has been activated
    DWORD      TotalIgmpPacketsReceived;
    DWORD      TotalIgmpPacketsForRouter;
    DWORD      GeneralQueriesReceived;
    DWORD      WrongVersionQueries;
    DWORD      JoinsReceived;
    DWORD      LeavesReceived;
    DWORD      CurrentGroupMemberships;
    DWORD      GroupMembershipsAdded;
    DWORD      WrongChecksumPackets;
    DWORD      ShortPacketsReceived;
    DWORD      LongPacketsReceived;
    DWORD      PacketsWithoutRtrAlert;
} IGMP_MIB_IF_STATS, *PIGMP_MIB_IF_STATS;

typedef struct _IGMP_MIB_GROUP_IFS_LIST {
    DWORD      GroupAddr;
    DWORD      NumInterfaces;
    BYTE      Buffer[1];
} IGMP_MIB_GROUP_IFS_LIST, *PIGMP_MIB_GROUP_IFS_LIST;

typedef struct _IGMP_MIB_GROUP_INFO_V3 {
    union {
        DWORD      IfIndex;
        DWORD      GroupAddr;
    };
    DWORD      IpAddr;
    DWORD      GroupUpTime;
    DWORD      GroupExpiryTime;

    DWORD      LastReporter;
    DWORD      V1HostPresentTimeLeft;
    DWORD      Flags;

    //v3 additions
    DWORD      Version; //1/2/3
    DWORD      Size;    //size of this struct
    DWORD      FilterType; //EXCLUSION/INCLUSION
    DWORD      V2HostPresentTimeLeft;
    DWORD      NumSources;

```

```

        //IGMP_MIB_GROUP_SOURCE_INFO_V3        Sources[0];

} IGMP_MIB_GROUP_INFO_V3, *PIGMP_MIB_GROUP_INFO_V3;

typedef struct _INTERFACE_ROUTE_ENTRY
{
    DWORD                dwIndex;
    INTERFACE_ROUTE_INFO routeInfo;
}INTERFACE_ROUTE_ENTRY, *PINTERFACE_ROUTE_ENTRY;

typedef struct _IP_NAT_MIB_QUERY {
    ULONG Oid;
    union {
        ULONG Index;
        UCHAR Data;
    };
} IP_NAT_MIB_QUERY, *PIP_NAT_MIB_QUERY;

typedef enum _IP_NAT_DIRECTION {
    NatInboundDirection = 0,
    NatOutboundDirection
} IP_NAT_DIRECTION, *PIP_NAT_DIRECTION;

typedef struct _IP_NAT_SESSION_MAPPING {
    UCHAR Protocol;           // see NAT_PROTOCOL_* above
    ULONG PrivateAddress;
    USHORT PrivatePort;
    ULONG PublicAddress;
    USHORT PublicPort;
    ULONG RemoteAddress;
    USHORT RemotePort;
    IP_NAT_DIRECTION Direction;
    ULONG IdleTime;           // in seconds
} IP_NAT_SESSION_MAPPING, *PIP_NAT_SESSION_MAPPING;

typedef struct _IP_NAT_ENUMERATE_SESSION_MAPPINGS {
    IN ULONG Index;
    IN OUT ULONG EnumerateContext[4];
    OUT ULONG EnumerateCount;
    OUT ULONG EnumerateTotalHint;
    OUT IP_NAT_SESSION_MAPPING EnumerateTable[1];
} IP_NAT_ENUMERATE_SESSION_MAPPINGS, *PIP_NAT_ENUMERATE_SESSION_MAPPINGS;

typedef struct _IP_NAT_INTERFACE_STATISTICS {
    OUT ULONG TotalMappings;
    OUT ULONG InboundMappings;
    OUT ULONG64 BytesForward;
    OUT ULONG64 BytesReverse;
    OUT ULONG64 PacketsForward;
    OUT ULONG64 PacketsReverse;
    OUT ULONG64 RejectsForward;
    OUT ULONG64 RejectsReverse;
} IP_NAT_INTERFACE_STATISTICS, *PIP_NAT_INTERFACE_STATISTICS;

typedef struct _IP_DNS_PROXY_MIB_QUERY {
    ULONG Oid;
    union {
        ULONG Index;
        UCHAR Data;
    };
}

```



```

    };
} IP_DNS_PROXY_MIB_QUERY, *PIP_DNS_PROXY_MIB_QUERY;

typedef struct _IP_DNS_PROXY_STATISTICS {
    ULONG MessagesIgnored;
    ULONG QueriesReceived;
    ULONG ResponsesReceived;
    ULONG QueriesSent;
    ULONG ResponsesSent;
} IP_DNS_PROXY_STATISTICS, *PIP_DNS_PROXY_STATISTICS;

typedef struct _IP_AUTO_DHCP_MIB_QUERY {
    ULONG Oid;
    union {
        ULONG Index;
        UCHAR Data;
    };
    ULONG Reserved;
} IP_AUTO_DHCP_MIB_QUERY, *PIP_AUTO_DHCP_MIB_QUERY;

typedef struct _IP_AUTO_DHCP_STATISTICS {
    ULONG MessagesIgnored;
    ULONG BootpOffersSent;
    ULONG DiscoversReceived;
    ULONG InformReceived;
    ULONG OffersSent;
    ULONG RequestsReceived;
    ULONG AcksSent;
    ULONG NaksSent;
    ULONG DeclinesReceived;
    ULONG ReleasesReceived;
} IP_AUTO_DHCP_STATISTICS, *PIP_AUTO_DHCP_STATISTICS;

typedef struct _MIB_DA_MSG {
    UINT32 op_code; /* IN: MIB manager operation code */
    UINT32 ret_code; /* OUT: MIB manager return code */
    UINT32 in_snmp_id[44]; /* IN: SNMP ID array (get_next) */
    UINT32 obj_id[17]; /* IN: object ID array (get, set) */
    UINT32 attr_id; /* IN: attribute ID (set) */
    UINT32 inst_id[23]; /* IN: instance ID array (get, set) */
    UINT32 next_snmp_id[44]; /* OUT: SNMP ID array (get_next) */
    UINT32 creator; /* OUT: creator of instance (get, get_next) */
    UINT32 attr_type; /* OUT: for resolveVarBind */
    UINT32 inst_cnt; /* OUT: # of insts for caching (get_next) */
    UINT32 map_flag; /* IN: flag - is this request mapped? */
    ULONG_PTR data[32]; /* IN: attribute value (set) */
                        /* OUT: entire record (get, get_next) */
} MIB_DA_MSG;

typedef struct _IP_AUTO_DHCP_GLOBAL_INFO {
    ULONG LoggingLevel;
    ULONG Flags;
    ULONG LeaseTime;
    ULONG ScopeNetwork;
    ULONG ScopeMask;
    ULONG ExclusionCount;
    ULONG ExclusionArray;

```

```

} IP_AUTO_DHCP_GLOBAL_INFO, *PIP_AUTO_DHCP_GLOBAL_INFO;

typedef struct _IP_AUTO_DHCP_INTERFACE_INFO {
    ULONG Flags;
} IP_AUTO_DHCP_INTERFACE_INFO, *PIP_AUTO_DHCP_INTERFACE_INFO;

typedef struct _IP_DNS_PROXY_GLOBAL_INFO {
    ULONG LoggingLevel;
    ULONG Flags;
    ULONG TimeoutSeconds;
} IP_DNS_PROXY_GLOBAL_INFO, *PIP_DNS_PROXY_GLOBAL_INFO;

typedef struct _IP_DNS_PROXY_INTERFACE_INFO {
    ULONG Flags;
} IP_DNS_PROXY_INTERFACE_INFO, *PIP_DNS_PROXY_INTERFACE_INFO;

typedef struct _IP_NAT_GLOBAL_INFO {
    ULONG LoggingLevel; // see IPNATHLP.H (IPNATHLP_LOGGING_*).
    ULONG Flags;
    RTR_INFO_BLOCK_HEADER Header;
} IP_NAT_GLOBAL_INFO, *PIP_NAT_GLOBAL_INFO;

typedef struct _IP_NAT_TIMEOUT {
    ULONG TCPTimeoutSeconds;
    ULONG UDPTimeoutSeconds;
} IP_NAT_TIMEOUT, *PIP_NAT_TIMEOUT;

typedef struct _IP_NAT_INTERFACE_INFO {
    ULONG Index;
    ULONG Flags;
    RTR_INFO_BLOCK_HEADER Header;
} IP_NAT_INTERFACE_INFO, *PIP_NAT_INTERFACE_INFO;

typedef struct _IP_NAT_ADDRESS_RANGE {
    ULONG StartAddress;
    ULONG EndAddress;
    ULONG SubnetMask;
} IP_NAT_ADDRESS_RANGE, *PIP_NAT_ADDRESS_RANGE;

typedef struct _IP_NAT_PORT_MAPPING {
    UCHAR Protocol;
    USHORT PublicPort;
    ULONG PublicAddress; // OPTIONAL - see IP_NAT_ADDRESS_UNSPECIFIED
    USHORT PrivatePort;
    ULONG PrivateAddress;
} IP_NAT_PORT_MAPPING, *PIP_NAT_PORT_MAPPING;

typedef struct _IP_NAT_ADDRESS_MAPPING {
    ULONG PrivateAddress;
    ULONG PublicAddress;
    BOOLEAN AllowInboundSessions;
} IP_NAT_ADDRESS_MAPPING, *PIP_NAT_ADDRESS_MAPPING;

typedef struct IP_ALG_GLOBAL_INFO {
    ULONG LoggingLevel;
    ULONG Flags;

```

```

} IP_ALG_GLOBAL_INFO, *PIP_ALG_GLOBAL_INFO;

typedef struct _RIP_GLOBAL_INFO {
    DWORD        EventLogMask;
} RIP_GLOBAL_INFO,
*PRIP_GLOBAL_INFO;

typedef struct _RIP_ROUTE_FILTER_INFO {
    UCHAR        Network[4];
    UCHAR        Mask[4];
} RIP_ROUTE_FILTER_INFO,
*PRIP_ROUTE_FILTER_INFO;

typedef struct _RIP_IF_FILTERS {
    ULONG        SupplyFilterAction;
    ULONG        SupplyFilterCount;
    ULONG        ListenFilterAction;
    ULONG        ListenFilterCount;
    RIP_ROUTE_FILTER_INFO  RouteFilter[1];
} RIP_IF_FILTERS,
*PRIP_IF_FILTERS;

typedef struct _RIP_IF_CONFIG {
    RIP_IF_INFO    RipIfInfo;
    RIP_IF_FILTERS RipIfFilters;
} RIP_IF_CONFIG,
*PRIP_IF_CONFIG;

typedef struct _SAP_GLOBAL_INFO {
    DWORD        EventLogMask;
} SAP_GLOBAL_INFO,
*PSAP_GLOBAL_INFO;

typedef struct _OSPF_ROUTE_FILTER
{
    DWORD        dwAddress;
    DWORD        dwMask;
}OSPF_ROUTE_FILTER, *POSPF_ROUTE_FILTER;

typedef enum _OSPF_FILTER_ACTION
{
    ACTION_DROP = 0,
    ACTION_ACCEPT = 1
}OSPF_FILTER_ACTION, *POSPF_FILTER_ACTION;

typedef struct _OSPF_ROUTE_FILTER_INFO
{
    DWORD        type;
    OSPF_FILTER_ACTION  ofaActionOnMatch;
    DWORD        dwNumFilters;
    OSPF_ROUTE_FILTER  pFilters[1];
}OSPF_ROUTE_FILTER_INFO, *POSPF_ROUTE_FILTER_INFO;

typedef struct _OSPF_PROTO_FILTER_INFO
{
    DWORD        type;
    OSPF_FILTER_ACTION  ofaActionOnMatch;
    DWORD        dwNumFilters;
    DWORD        pdwProtoId[1];

```

```

}OSPF_PROTO_FILTER_INFO, *POSPF_PROTO_FILTER_INFO;

typedef struct _OSPF_GLOBAL_PARAM
{
    DWORD    type;
    DWORD    create;
    DWORD    enable;
    DWORD    routerId;
    DWORD    ASBrdrRtr;
    DWORD    logLevel;
}OSPF_GLOBAL_PARAM, *POSPF_GLOBAL_PARAM;

typedef struct _OSPF_AREA_PARAM
{
    DWORD    type;
    DWORD    create;
    DWORD    enable;
    DWORD    areaId;
    DWORD    authType;
    DWORD    importASExtern;
    DWORD    stubMetric;
    DWORD    importSumAdv;
}OSPF_AREA_PARAM, *POSPF_AREA_PARAM;

typedef struct _OSPF_AREA_RANGE_PARAM
{
    DWORD    type;
    DWORD    create;
    DWORD    enable;
    DWORD    areaId;
    DWORD    rangeNet;
    DWORD    rangeMask;
}OSPF_AREA_RANGE_PARAM, *POSPF_AREA_RANGE_PARAM;

typedef struct _OSPF_VIRT_INTERFACE_PARAM
{
    DWORD    type;
    DWORD    create;
    DWORD    enable;
    DWORD    transitAreaId;
    DWORD    virtNeighborRouterId;
    DWORD    transitDelay;
    DWORD    retransInterval;
    DWORD    helloInterval;
    DWORD    deadInterval;
    BYTE    password[8];
}OSPF_VIRT_INTERFACE_PARAM, *POSPF_VIRT_INTERFACE_PARAM;

typedef struct _OSPF_INTERFACE_PARAM
{
    DWORD    type;
    DWORD    create;
    DWORD    enable;
    DWORD    intfIpAddr;
    DWORD    intfSubnetMask;
    DWORD    areaId;
    DWORD    intfType;
    DWORD    routerPriority;
    DWORD    transitDelay;
}

```

```

        DWORD    retransInterval;
        DWORD    helloInterval;
        DWORD    deadInterval;
        DWORD    pollInterval;
        DWORD    metricCost;
        BYTE     password[8];
        DWORD    mtuSize;
}OSPF_INTERFACE_PARAM, *POSPF_INTERFACE_PARAM;

typedef struct _OSPF_NBMA_NEIGHBOR_PARAM
{
    DWORD    type;
    DWORD    create;
    DWORD    enable;
    DWORD    neighborIpAddr;
    DWORD    intfIpAddr;
    DWORD    neighborPriority;
}OSPF_NBMA_NEIGHBOR_PARAM, *POSPF_NBMA_NEIGHBOR_PARAM;

typedef enum _RASDEVICETYPE
{
    RDT_Modem = 0,
    RDT_X25,
    RDT_Isdn,
    RDT_Serial,
    RDT_FrameRelay,
    RDT_Atm,
    RDT_Sonet,
    RDT_Sw56,
    RDT_Tunnel_Pptp,
    RDT_Tunnel_L2tp,
    RDT_Irda,
    RDT_Parallel,
    RDT_Other,
    RDT_PPpOE,
    RDT_Tunnel_Sstp,
    RDT_Tunnel_Ikev2,
    RDT_Tunnel = 0x00010000,
    RDT_Direct = 0x00020000,
    RDT_Null_Modem = 0x00040000,
    RDT_Broadband = 0x00080000
} RASDEVICETYPE;

typedef enum _RASMAN_STATUS {
    OPEN      = 0,
    CLOSED    = 1,
    UNAVAILABLE = 2,
    REMOVED   = 3
} RASMAN_STATUS;

typedef enum _ReqTypes {
    REQTYPE_PORTENUM= 21,
    REQTYPE_GETINFO= 22,
    REQTYPE_GETDEVCONFIG= 73,
    REQTYPE_SETDEVICECONFIGINFO= 94,
    REQTYPE_GETDEVICECONFIGINFO= 95,
    REQTYPE_GETCALLEDID= 105,
    REQTYPE_SETCALLEDID= 106,

```

```

REQTYPE_GETNDISWANDRIVERCAPS= 111
} ReqTypes;

typedef enum _RASAN_STATE {
    CONNECTING    = 0,
    LISTENING     = 1,
    CONNECTED     = 2,
    DISCONNECTING = 3,
    DISCONNECTED  = 4,
    LISTENCOMPLETED = 5,
} RASAN_STATE;

typedef enum _RASAN_DISCONNECT_TYPE {
    USER_REQUESTED = 0,
    REMOTE_DISCONNECTION = 1,
    HARDWARE_FAILURE = 2,
    NOT_DISCONNECTED = 3
} RASAN_DISCONNECT_TYPE;

typedef enum _RASAN_USAGE {
    CALL_NONE = 0x00,
    CALL_IN = 0x01,
    CALL_OUT = 0x02,
    CALL_ROUTER = 0x04,
    CALL_LOGON = 0x08,
    CALL_OUT_ONLY = 0x10,
    CALL_IN_ONLY = 0x20,
    CALL_OUTBOUND_ROUTER = 0x40
} RASAN_USAGE;

typedef struct _RequestBuffer {
    DWORD      RB_PCIndex;
    ReqTypes    RB_Rectype;
    DWORD      RB_Dummy;
    DWORD      RB_Done;
    LONGLONG    Alignment;
    BYTE       RB_Buffer[1];
} RequestBuffer;
typedef struct DeviceConfigInfo
{
    DWORD      retcode;
    DWORD      dwVersion;
    DWORD      cbBuffer;
    DWORD      cEntries;
    BYTE       abdata[1];
} DeviceConfigInfo;
typedef struct _RAS_DEVICE_INFO
{
    DWORD      dwVersion;
    BOOL       fWrite;
    BOOL       fRasEnabled;
    BOOL       fRouterEnabled;
    BOOL       fRouterOutboundEnabled;
    DWORD      dwTapiLineId;
    DWORD      dwError;
    DWORD      dwNumEndPoints;
    DWORD      dwMaxOutCalls;
    DWORD      dwMaxInCalls;
    DWORD      dwMinWanEndPoints;

```

```

        DWORD           dwMaxWanEndPoints;
        RASDEVICETYPE   eDeviceType;
        GUID            guidDevice;
        CHAR             szPortName[17];
        CHAR             szDeviceName[129];
        WCHAR           wszDeviceName[129];
    } RAS_DEVICE_INFO, *PRAS_DEVICE_INFO;

typedef struct _RAS_CALLEDID_INFO
{
    DWORD           dwSize;
    BYTE            bCalledId[1];
} RAS_CALLEDID_INFO, *PRAS_CALLEDID_INFO;

typedef struct GetSetCalledId
{
    DWORD           retcode;
    BOOL            fWrite;
    DWORD           dwSize;
    GUID            guidDevice;
    RAS_DEVICE_INFO rdi;
    RAS_CALLEDID_INFO rciInfo;
} GetSetCalledId;

typedef struct _RAS_NDISWAN_DRIVER_INFO
{
    ULONG           DriverCaps;
    ULONG           Reserved;
} RAS_NDISWAN_DRIVER_INFO, *P_NDISWAN_DRIVER_INFO;

typedef struct GetNdiswanDriverCapsStruct
{
    DWORD           retcode;
    RAS_NDISWAN_DRIVER_INFO NdiswanDriverInfo;
} GetNdiswanDriverCapsStruct;

typedef struct GetDevConfigStruct
{
    DWORD           retcode;
    CHAR            devicetype[17];
    DWORD           size;
    BYTE            config[1];
} GetDevConfigStruct;

typedef struct Enum
{
    DWORD           retcode;
    DWORD           size;
    DWORD           entries;
    BYTE            buffer[1];
} Enum;

typedef struct _RASMAN_PORT_32 {
    DWORD P_Port;
    CHAR P_PortName[16];
    RASMAN_STATUS P_Status;
    RASDEVICETYPE P_rdtDeviceType;

```

```

    RASMAN_USAGE P_ConfiguredUsage;
    RASMAN_USAGE P_CurrentUsage;
    CHAR P_MediaName[16];
    CHAR P_DeviceType[16];
    CHAR P_DeviceName[129];
    DWORD P_LineDeviceId;
    DWORD P_AddressId;
} RASMAN_PORT_32;

typedef struct _RASMAN_INFO {
    RASMAN_STATUS    RI_PortStatus;
    RASMAN_STATE     RI_ConnState;
    DWORD            RI_LinkSpeed;
    DWORD            RI_LastError;
    RASMAN_USAGE     RI_CurrentUsage;
    CHAR             RI_DeviceTypeConnecting [16];
    CHAR             RI_DeviceConnecting [129];
    CHAR             RI_szDeviceType[16];
    CHAR             RI_szDeviceName[129];
    CHAR             RI_szPortName[17];
    RASMAN_DISCONNECT_TYPE RI_DisconnectType;
    DWORD            RI_OwnershipFlag;
    DWORD            RI_ConnectDuration;
    DWORD            RI_BytesReceived;
    CHAR             RI_Phonebook[261];
    CHAR             RI_PhoneEntry[257];
    HANDLE           RI_ConnectionHandle;
    DWORD            RI_SubEntry;
    RASDEVICETYPE    RI_rdtDeviceType;
    GUID             RI_GuidEntry;
    DWORD            RI_dwSessionId;
    DWORD            RI_dwFlags;
    GUID             RI_CorrelationGuid;
} RASMAN_INFO;

typedef struct Info
{
    union {
        DWORD            retcode;
        HANDLE           paddingField;
    };
    RASMAN_INFO    info;
} Info;

#define RASRPC_MaxEntryName    256
#define RASRPC_MaxPortName    16
#define RASRPC_MaxDeviceName  128
#define RASRPC_MaxPhoneNumber 128
#define RASRPC_MAX_PATH      260

typedef struct _RASRPC_CALLBACKLIST
{
    WCHAR pszPortName[RASRPC_MaxPortName + 1];
    WCHAR pszDeviceName[RASRPC_MaxDeviceName + 1];
    WCHAR pszNumber[RASRPC_MaxPhoneNumber + 1];
    DWORD dwDeviceType;
    [unique] struct _RASRPC_CALLBACKLIST *pNext;
} RASRPC_CALLBACKLIST, *LPRASRPC_CALLBACKLIST;

```



```

typedef struct _RASRPC_STRINGLIST
{
    WCHAR psz[256];
    [unique] struct _RASRPC_STRINGLIST *pNext;
} RASRPC_STRINGLIST, *LPRASRPC_STRINGLIST;

typedef struct _RASRPC_LOCATIONLIST
{
    DWORD dwLocationId;
    DWORD iPrefix;
    DWORD iSuffix;
    [unique] struct _RASRPC_LOCATIONLIST *pNext;
} RASRPC_LOCATIONLIST, *LPRASRPC_LOCATIONLIST;

typedef struct _RASRPC_PBUUSER
{
    BOOL fOperatorDial;
    BOOL fPreviewPhoneNumber;
    BOOL fUseLocation;
    BOOL fShowLights;
    BOOL fShowConnectStatus;
    BOOL fCloseOnDial;
    BOOL fAllowLogonPhonebookEdits;
    BOOL fAllowLogonLocationEdits;
    BOOL fSkipConnectComplete;
    BOOL fNewEntryWizard;
    DWORD dwRedialAttempts;
    DWORD dwRedialSeconds;
    DWORD dwIdleDisconnectSeconds;
    BOOL fRedialOnLinkFailure;
    BOOL fPopupOnTopWhenRedialing;
    BOOL fExpandAutoDialQuery;
    DWORD dwCallbackMode;
    [unique] LPRASRPC_CALLBACKLIST pCallbacks;
    WCHAR pszLastCallbackByCaller[129];
    DWORD dwPhonebookMode;
    WCHAR pszPersonalFile[260];
    WCHAR pszAlternatePath[260];
    [unique] LPRASRPC_STRINGLIST pPhonebooks;
    [unique] LPRASRPC_STRINGLIST pAreaCodes;
    BOOL fUseAreaAndCountry;
    [unique] LPRASRPC_STRINGLIST pPrefixes;
    [unique] LPRASRPC_STRINGLIST pSuffixes;
    [unique] LPRASRPC_LOCATIONLIST pLocations;
    DWORD dwXPhonebook;
    DWORD dwYPhonebook;
    WCHAR pszDefaultEntry[257];
    BOOL fInitialized;
    BOOL fDirty;
} RASRPC_PBUUSER, *LPRASRPC_PBUUSER;

[
    uuid(8f09f000-b7ed-11ce-bbd2-00001a181cad),
    version(0.0),
    pointer_default(unique)

```

]

```
interface dimsvc
{
```

```
    DWORD
    RMprAdminServerGetInfo (
        [in]          DIM_HANDLE          hDimServer,
        [in]          DWORD                dwLevel,
        [out]         PDIM_INFORMATION_CONTAINER pInfoStruct
    );
```

```
    DWORD
    RRasAdminConnectionEnum (
        [in]          DIM_HANDLE          hDimServer,
        [in]          DWORD                dwLevel,
        [in,out]     PDIM_INFORMATION_CONTAINER pInfoStruct,
        [in]          DWORD                dwPreferedMaximumLength,
        [out]         LPDWORD              lpdwEntriesRead,
        [out]         LPDWORD              lpdwTotalEntries,
        [in,out,unique] LPDWORD              lpdwResumeHandle
    );
```

```
    DWORD
    RRasAdminConnectionGetInfo (
        [in]          DIM_HANDLE          hDimServer,
        [in]          DWORD                dwLevel,
        [in]          DWORD                hDimConnection,
        [out]         PDIM_INFORMATION_CONTAINER pInfoStruct
    );
```

```
    DWORD
    RRasAdminConnectionClearStats (
        [in]          DIM_HANDLE          hDimServer,
        [in]          DWORD                hDimConnection
    );
```

```
    DWORD
    RRasAdminPortEnum (
        [in]          DIM_HANDLE          hDimServer,
        [in]          DWORD                dwLevel,
        [in]          DWORD                hRasConnection,
        [in,out]     PDIM_INFORMATION_CONTAINER pInfoStruct,
        [in]          DWORD                dwPreferedMaximumLength,
        [out]         LPDWORD              lpdwEntriesRead,
        [out]         LPDWORD              lpdwTotalEntries,
        [in,out,unique] LPDWORD              lpdwResumeHandle
    );
```

```

DWORD
RRasAdminPortGetInfo (
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in]          DWORD               hPort,
    [out]         PDIM_INFORMATION_CONTAINER pInfoStruct
);

DWORD
RRasAdminPortClearStats (
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hPort
);

DWORD
RRasAdminPortReset (
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hPort
);

DWORD
RRasAdminPortDisconnect (
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hPort
);

DWORD
RRouterInterfaceTransportSetGlobalInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwTransportId,
    [in]          PDIM_INTERFACE_CONTAINER pInfoStruct
);

DWORD
RRouterInterfaceTransportGetGlobalInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwTransportId,
    [in,out]      PDIM_INTERFACE_CONTAINER pInfoStruct
);

DWORD
RRouterInterfaceGetHandle(
    [in]          DIM_HANDLE          hDimServer,
    [in,string]   LPWSTR              lpwsInterfaceName,
    [in,out]      LPDWORD              phInterface,
    [in]          DWORD               fIncludeClientInterfaces
);

```

```
);
```

```
DWORD
RRouterInterfaceCreate(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in]          PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in,out]      LPDWORD              phInterface
);
```

```
DWORD
RRouterInterfaceGetInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in,out]      PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]          DWORD               hInterface
);
```

```
DWORD
RRouterInterfaceSetInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in]          PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]          DWORD               hInterface
);
```

```
DWORD
RRouterInterfaceDelete(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface
);
```

```
DWORD
RRouterInterfaceTransportRemove(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface,
    [in]          DWORD               dwTransportId
);
```

```
DWORD
RRouterInterfaceTransportAdd(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface,
    [in]          DWORD               dwTransportId,
    [in]          PDIM_INTERFACE_CONTAINER pInfoStruct
);
```

```

DWORD
RRouterInterfaceTransportGetInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface,
    [in]          DWORD               dwTransportId,
    [in,out]      PDIM_INTERFACE_CONTAINER pInfoStruct
);

DWORD
RRouterInterfaceTransportSetInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface,
    [in]          DWORD               dwTransportId,
    [in]          PDIM_INTERFACE_CONTAINER pInfoStruct
);

DWORD
RRouterInterfaceEnum (
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in,out]      PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]          DWORD               dwPreferedMaximumLength,
    [out]         LPDWORD              lpdwEntriesRead,
    [out]         LPDWORD              lpdwTotalEntries,
    [in,out,unique] LPDWORD              lpdwResumeHandle
);

DWORD
RRouterInterfaceConnect(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface,
    [in]          ULONG_PTR           hEvent,
    [in]          DWORD               fBlocking,
    [in]          DWORD               dwCallersProcessId
);

DWORD
RRouterInterfaceDisconnect(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface
);

DWORD
RRouterInterfaceUpdateRoutes(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hInterface,
    [in]          DWORD               dwTransportId,

```

```

        [in]          ULONG_PTR          hEvent,
        [in]          DWORD              dwClientIdProcessId
    );

```

```

DWORD
RRouterInterfaceQueryUpdateResult(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD              hInterface,
    [in]          DWORD              dwTransportId,
    [out]         LPDWORD             pUpdateResult
);

```

```

DWORD
RRouterInterfaceUpdatePhonebookInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD              hInterface
);

```

```

DWORD
RMIBEntryCreate(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD              dwPid,
    [in]          DWORD              dwRoutingPid,
    [in]          PDIM_MIB_ENTRY_CONTAINER pInfoStuct
);

```

```

DWORD
RMIBEntryDelete(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD              dwPid,
    [in]          DWORD              dwRoutingPid,
    [in]          PDIM_MIB_ENTRY_CONTAINER pInfoStuct
);

```

```

DWORD
RMIBEntrySet(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD              dwPid,
    [in]          DWORD              dwRoutingPid,
    [in]          PDIM_MIB_ENTRY_CONTAINER pInfoStuct
);

```

```

DWORD
RMIBEntryGet(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD              dwPid,
    [in]          DWORD              dwRoutingPid,

```

```

        [in,out]          PDIM_MIB_ENTRY_CONTAINER    pInfoStuct
    );

DWORD
RMIBEntryGetFirst(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwPid,
    [in]          DWORD               dwRoutingPid,
    [in,out]      PDIM_MIB_ENTRY_CONTAINER    pInfoStuct
);

DWORD
RMIBEntryGetNext(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwPid,
    [in]          DWORD               dwRoutingPid,
    [in,out]      PDIM_MIB_ENTRY_CONTAINER    pInfoStuct
);

DWORD
RMIBGetTrapInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwPid,
    [in]          DWORD               dwRoutingPid,
    [in, out]     PDIM_MIB_ENTRY_CONTAINER    pInfoStruct
);

DWORD
RMIBSetTrapInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwPid,
    [in]          DWORD               dwRoutingPid,
    [in]          ULONG_PTR          hEvent,
    [in]          DWORD               dwClientProcessId,
    [in, out]     PDIM_MIB_ENTRY_CONTAINER    pInfoStruct
);

DWORD
RRasAdminConnectionNotification(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               fRegister,
    [in]          DWORD               dwClientProcessId,
    [in]          ULONG_PTR          hEventNotification
);

DWORD
RRasAdminSendMessage(
    [in]          DIM_HANDLE          hDimServer,

```

```

        [in]                DWORD                hDimConnection,
        [in, string]        LPWSTR               lpwszMessage
    );

DWORD
RRouterDeviceEnum(
    [in]                DIM_HANDLE                hDimServer,
    [in]                DWORD                    dwLevel,
    [in, out]           PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in, out]           LPDWORD                  lpdwTotalEntries
);

DWORD
RRouterInterfaceTransportCreate(
    [in]                DIM_HANDLE                hDimServer,
    [in]                DWORD                    dwTransportId,
    [in, string]        LPWSTR                   lpwsTransportName,
    [in]                PDIM_INTERFACE_CONTAINER pInfoStruct,
    [in, string]        LPWSTR                   lpwsDLLPath
);

DWORD
RRouterInterfaceDeviceGetInfo(
    [in]                DIM_HANDLE                hDimServer,
    [in]                DWORD                    dwLevel,
    [in, out]           PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]                DWORD                    dwIndex,
    [in]                DWORD                    hInterface
);

DWORD
RRouterInterfaceDeviceSetInfo(
    [in]                DIM_HANDLE                hDimServer,
    [in]                DWORD                    dwLevel,
    [in]                PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]                DWORD                    dwIndex,
    [in]                DWORD                    hInterface
);

DWORD
RRouterInterfaceSetCredentialsEx(
    [in]                DIM_HANDLE                hDimServer,
    [in]                DWORD                    dwLevel,
    [in]                PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]                DWORD                    hInterface
);

DWORD

```



```

RRouterInterfaceGetCredentialsEx(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in,out]      PDIM_INFORMATION_CONTAINER pInfoStruct,
    [in]          DWORD               hInterface
);

DWORD
RRasAdminConnectionRemoveQuarantine(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hRasConnection,
    [in]          BOOL               fIsIpAddress
);

DWORD
RMprAdminServerSetInfo(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               dwLevel,
    [in]          PDIM_INFORMATION_CONTAINER pInfoStruct
);

DWORD
RMprAdminServerGetInfoEx(
    [in]          DIM_HANDLE          hDimServer,
    [in, out]      PMPR_SERVER_EX_IDL pServerConfig
);

DWORD
RRasAdminConnectionEnumEx (
    [in]          DIM_HANDLE          hDimServer,
    [in]          PMPRAPI_OBJECT_HEADER_IDL objectHeader,
    [in]          DWORD               dwPreferredMaxLen,
    [out]         LPDWORD             lpdwEntriesRead,
    [out]         LPDWORD             lpdwNumTotalElements,
    [out, size_is(*lpdwEntriesRead)] PRAS_CONNECTION_EX_IDL *pRasConnections,
    [in,out,unique] LPDWORD             lpdwResumeHandle);

DWORD
RRasAdminConnectionGetInfoEx (
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hDimConnection,
    [in]          PMPRAPI_OBJECT_HEADER_IDL objectHeader,
    [out]         PRAS_CONNECTION_EX_IDL pRasConnection
);

DWORD
RMprAdminServerSetInfoEx (
    [in]          DIM_HANDLE          hDimServer,
    [in]          PMPR_SERVER_SET_CONFIG_EX_IDL pServerConfig);

```

```

DWORD
RRasAdminUpdateConnection(
    [in]          DIM_HANDLE          hDimServer,
    [in]          DWORD               hDimConnection,
    [in]          PRAS_UPDATE_CONNECTION_IDL pServerConfig);

DWORD
RRouterInterfaceSetCredentialsLocal(
    [in]          DIM_HANDLE          hDimServer,
    [in,string]   LPWSTR              lpwsInterfaceName,
    [in,string]   LPWSTR              lpwsUserName,
    [in,string]   LPWSTR              lpwsDomainName,
    [in,string]   LPWSTR              lpwsPassword);

DWORD
RRouterInterfaceGetCredentialsLocal(
    [in]          DIM_HANDLE          hDimServer,
    [in,string]   LPWSTR              lpwsInterfaceName,
    [out] [string] LPWSTR              *lpwsUserName,
    [out] [string] LPWSTR              *lpwsDomainName,
    [out] [string] LPWSTR              *lpwsPassword);
}

[
    uuid(20610036-fa22-11cf-9823-00a0c911e5df),
    version(1.0)
]

interface rasrpc
{

    void Opnum0NotUsedOnWire(void);

    void Opnum1NotUsedOnWire(void);

    void Opnum2NotUsedOnWire(void);

    void Opnum3NotUsedOnWire(void);

    void Opnum4NotUsedOnWire(void);

    DWORD
    RasRpcDeleteEntry(
        [in] handle_t h,
        [in, string] LPWSTR lpszPhonebook,
        [in, string] LPWSTR lpszEntry
    );

    void Opnum6NotUsedOnWire(void);

    void Opnum7NotUsedOnWire(void);

    void Opnum8NotUsedOnWire(void);

    DWORD

```

```

RasRpcGetUserPreferences (
    [in] handle_t h,
    [in, out] LPRASRPC_PBUSER pUser,
    [in] DWORD dwMode
);

DWORD
RasRpcSetUserPreferences (
    [in] handle_t h,
    [in] LPRASRPC_PBUSER pUser,
    [in] DWORD dwMode
);

UINT
RasRpcGetSystemDirectory (
    [in] handle_t h,
    [in, out, string, size_is(uSize)] LPWSTR lpBuffer,
    [in, range(0, RASRPC_MAX_PATH)] UINT uSize
);

DWORD
RasRpcSubmitRequest (
    [in] handle_t h,
    [in, out, unique, size_is(dwcbBufSize)] PBYTE pReqBuffer,
    [in] DWORD dwcbBufSize
);

void Opnum13NotUsedOnWire(void);

DWORD
RasRpcGetInstalledProtocolsEx (
    [in] handle_t h,
    [in] BOOL fRouter,
    [in] BOOL fRasCli,
    [in] BOOL fRasSrv
);

DWORD
RasRpcGetVersion (
    [in] handle_t h,
    [in, out, ref] LPDWORD pdwVersion
);

void Opnum16NotUsedOnWire(void);
}

```

## 7 Appendix B: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft Windows® 2000 operating system
- Microsoft Windows® 2000 Server operating system
- Windows® XP operating system
- Windows Server® 2003 operating system
- Windows Vista® operating system
- Windows Server® 2008 operating system
- Windows® 7 operating system
- Windows Server® 2008 R2 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

[<1> Section 2.1.1.1:](#) Not available in Windows 2000 Server.

[<2> Section 2.1.2.1:](#) In Windows 2000 Server no authentication service registration is specified.

[<3> Section 2.1.2.1:](#) Not supported in Windows 2000 Server.

[<4> Section 2.1.2.1:](#) Not available in Windows 2000 Server.

[<5> Section 2.1.2.1:](#) Windows 2000 Server supported clients connecting with `RPC_C_AUTHN_LEVEL_NONE`.

[<6> Section 2.1.2.2:](#) Not available in Windows 2000 Server

[<7> Section 2.1.2.2:](#) In Windows 2000 Server no authentication service is specified.

[<8> Section 2.1.2.2:](#) Not supported in Windows 2000 Server.

[<9> Section 2.2.1.1.1:](#) Only defined in Windows Server 2000 and not defined for Windows Server 2008 and Windows Server 2003.

[<10> Section 2.2.1.1.16:](#) Not defined in Windows 2000 Server

[<11> Section 2.2.1.1.16:](#) Not defined in Windows 2000 Server and Windows Server 2003

[<12> Section 2.2.1.1.16:](#) Not defined in Windows 2000 Server, Windows Server 2003, and Windows Server 2008.

- [<13> Section 2.2.1.1.16:](#) Not defined in Windows 2000 Server
- [<14> Section 2.2.1.2.4:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<15> Section 2.2.1.2.4:](#) Only defined in Windows 2000 Server.
- [<16> Section 2.2.1.2.4:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<17> Section 2.2.1.2.4:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<18> Section 2.2.1.2.4:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<19> Section 2.2.1.2.4:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<20> Section 2.2.1.2.4:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<21> Section 2.2.1.2.4:](#) Windows 2000 Server and Windows Server 2003 only.
- [<22> Section 2.2.1.2.4:](#) IPX-related information and features are only defined in Windows 2000 Server.
- [<23> Section 2.2.1.2.7:](#) Only defined in Windows Server 2008.
- [<24> Section 2.2.1.2.8:](#) IPv6-related information and features are only defined in Windows Server 2008.
- [<25> Section 2.2.1.2.11:](#) Only defined in Windows Server 2008.
- [<26> Section 2.2.1.2.11:](#) Only defined in Windows Server 2003 and Windows Server 2008.
- [<27> Section 2.2.1.2.11:](#) Only defined in Windows Server 2008.
- [<28> Section 2.2.1.2.11:](#) Windows implementations always return 0x00000000 for this field when `INTERFACE_ROUTE_INFO` is queried using the [RRouterInterfaceTransportGetInfo \(section 3.1.4.19\)](#) method.
- [<29> Section 2.2.1.2.13:](#) Windows does not validate the **dwProtocolId** member of **PROTOCOL\_METRIC** to be one of the values specified in the **MIB\_IPFORWARD\_PROTO**. A set operation (using [RRouterInterfaceTransportSetGlobalInfo](#)) with a value specified outside of the **MIB\_IPFORWARD\_PROTO** will be accepted, and the same will be returned when a get operation (using [RRouterInterfaceTransportGetGlobalInfo](#)) is performed.
- [<30> Section 2.2.1.2.17:](#) Windows 2000 Server only.
- [<31> Section 2.2.1.2.29:](#) The **dwLastChange** member is not currently supported by the Network Driver Interface Specification (NDIS). On Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, NDIS returns zero for this member. On other versions, an arbitrary value is returned in this member for the interfaces supported by NDIS. For interfaces supported by other interface providers, an appropriate value might be returned.
- [<32> Section 2.2.1.2.32:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<33> Section 2.2.1.2.35:](#) Only defined in Windows Server 2008.

[<34> Section 2.2.1.2.35:](#) Only defined in Windows Server 2008.

[<35> Section 2.2.1.2.49:](#) Only defined beginning with Windows Server 2008.

[<36> Section 2.2.1.2.56:](#) Only defined beginning with Windows Server 2008.

[<37> Section 2.2.1.2.57:](#) Only defined beginning with Windows Server 2008.

[<38> Section 2.2.1.2.63:](#) The port limit is determined by the Windows server license.

[<39> Section 2.2.1.2.63:](#) The port limit is determined by the Windows server license.

[<40> Section 2.2.1.2.64:](#) Defined only in Windows Server 2008.

[<41> Section 2.2.1.2.64:](#) The port limit is determined by the Windows server license.

[<42> Section 2.2.1.2.64:](#) The port limit is determined by the Windows server license.

[<43> Section 2.2.1.2.64:](#) Only defined in Windows Server 2008.

[<44> Section 2.2.1.2.64:](#) The port limit is determined by the Windows server license.

[<45> Section 2.2.1.2.64:](#) Only defined in Windows Server 2008.

[<46> Section 2.2.1.2.65:](#) Only defined in Windows 2000 Server and not defined in Windows Server 2003 and Windows Server 2008.

[<47> Section 2.2.1.2.68:](#) Only defined in Windows 2000 Server.

[<48> Section 2.2.1.2.69:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<49> Section 2.2.1.2.70:](#) Only defined in Windows 2000 Server.

[<50> Section 2.2.1.2.72:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<51> Section 2.2.1.2.72:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<52> Section 2.2.1.2.72:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<53> Section 2.2.1.2.72:](#) Windows 2000 Server and Windows Server 2003 only.

[<54> Section 2.2.1.2.72:](#) Windows 2000 Server and Windows Server 2003 only.

[<55> Section 2.2.1.2.72:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<56> Section 2.2.1.2.72:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<57> Section 2.2.1.2.72:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<58> Section 2.2.1.2.72:](#) Only defined in Windows Server 2008.

[<59> Section 2.2.1.2.72:](#) Only defined in Windows Server 2008.

[<60> Section 2.2.1.2.73:](#) Only defined in Windows 2000 Server.

[<61> Section 2.2.1.2.73:](#) Only defined in Windows 2000 Server.

[<62> Section 2.2.1.2.74:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<63> Section 2.2.1.2.74:](#) Only defined in Windows 2000 Server.

[<64> Section 2.2.1.2.74:](#) Only defined in Windows 2000 Server.

[<65> Section 2.2.1.2.75:](#) Only defined in Windows Server 2008.

[<66> Section 2.2.1.2.75:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<67> Section 2.2.1.2.78:](#) Only defined in Windows 2000 Server.

[<68> Section 2.2.1.2.81:](#) Only defined beginning with Windows Server 2008.

[<69> Section 2.2.1.2.81:](#) Only defined beginning with Windows Server 2008.

[<70> Section 2.2.1.2.83:](#) Only defined beginning with Windows Server 2003.

[<71> Section 2.2.1.2.84:](#) Only defined beginning with Windows Server 2003.

[<72> Section 2.2.1.2.84:](#) Windows implementations also require that the interface be registered in the registry as specified in [2.2.3.2.1](#); otherwise, the interface will not be available for managing after the Remote Access Service is restarted.

[<73> Section 2.2.1.2.84:](#) In Windows Server implementations, specifying a new value for **wszInterfaceInfo** with MPRI\_INTERFACE\_2 in calls to [RRouterInterfaceSetInfo](#) results in a new phonebook entry being created; that new entry will not be available for management.

[<74> Section 2.2.1.2.84:](#) Only defined in Windows 2000 Server and Windows Server 2003.

[<75> Section 2.2.1.2.84:](#) Only defined in Windows 2000 Server and Windows Server 2003.

[<76> Section 2.2.1.2.84:](#) Windows 2000 Server only.

[<77> Section 2.2.1.2.84:](#) Windows Server 2008 only.

[<78> Section 2.2.1.2.84:](#) This feature is only supported in Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2.

[<79> Section 2.2.1.2.84:](#) In Windows 2000 and Windows NT the szX25PadType string maps to a section name in PAD.INF.

[<80> Section 2.2.1.2.84:](#) This feature is only supported in Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2.

[<81> Section 2.2.1.2.84:](#) This feature is only supported in Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2. On Windows Server 2008 and Windows Server 2008 R2, this value is ignored and treated identically to MPRDM\_DialAll.

[<82> Section 2.2.1.2.84:](#) Supported only in Windows 2000 Server.

[<83> Section 2.2.1.2.85:](#) Only defined in Windows Server 2008.

[<84> Section 2.2.1.2.85:](#) Windows implementations also require that the interface be registered in the registry as specified in [2.2.3.2.1](#); otherwise, the interface will not be available for managing after the Remote Access Service is restarted.

[<85> Section 2.2.1.2.85:](#) In Windows Server implementations, specifying a new value for **wszInterfaceInfo** with MPRI\_INTERFACE\_3 in calls to [RRouterInterfaceSetInfo](#) results in a new phonebook entry being created; that new entry will not be available for management.

[<86> Section 2.2.1.2.85:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<87> Section 2.2.1.2.85:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<88> Section 2.2.1.2.85:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<89> Section 2.2.1.2.85:](#) Only defined in Windows Server 2003 and Windows Server 2008.

[<90> Section 2.2.1.2.85:](#) This feature is only supported in Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2.

[<91> Section 2.2.1.2.85:](#) In Windows 2000 and Windows NT, the szX25PadType string maps to a section name in PAD.INF.

[<92> Section 2.2.1.2.85:](#) This feature is only supported in Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2.

[<93> Section 2.2.1.2.85:](#) This feature is only supported in Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2. On Windows Server 2008 and Windows Server 2008 R2, this value is ignored and treated identically to MPRDM\_DialAll.

[<94> Section 2.2.1.2.91:](#) Only defined in Windows 2000 Server.

[<95> Section 2.2.1.2.92:](#) Only defined in Windows 2000 Server.

[<96> Section 2.2.1.2.93:](#) Only defined in Windows 2000 Server.

[<97> Section 2.2.1.2.94:](#) Only defined in Windows 2000 Server.

[<98> Section 2.2.1.2.95:](#) Only defined in Windows 2000 Server.

[<99> Section 2.2.1.2.96:](#) Only defined in Windows 2000 Server.

[<100> Section 2.2.1.2.97:](#) Only defined in Windows 2000 Server.

[<101> Section 2.2.1.2.98:](#) Only defined in Windows 2000 Server.

[<102> Section 2.2.1.2.99:](#) Windows 2000 Server only.

[<103> Section 2.2.1.2.100:](#) Only defined in Windows 2000 Server.

[<104> Section 2.2.1.2.101:](#) Only defined in Windows 2000 Server.

[<105> Section 2.2.1.2.102:](#) Only defined in Windows 2000 Server.

[<106> Section 2.2.1.2.103:](#) Only defined in Windows 2000 Server.

[<107> Section 2.2.1.2.104:](#) Only defined in Windows 2000 Server.

[<108> Section 2.2.1.2.105:](#) Only defined in Windows 2000 Server.

[<109> Section 2.2.1.2.106:](#) Only defined in Windows 2000 Server.

[<110> Section 2.2.1.2.107:](#) Only defined in Windows 2000 Server.



[<111> Section 2.2.1.2.108:](#) Only defined in Windows 2000 Server.

[<112> Section 2.2.1.2.109:](#) Only defined in Windows 2000 Server.

[<113> Section 2.2.1.2.109:](#) This media type is available only in versions of Windows before Windows Vista.

[<114> Section 2.2.1.2.110:](#) Only defined in Windows 2000 Server.

[<115> Section 2.2.1.2.111:](#) Only defined in Windows 2000 Server.

[<116> Section 2.2.1.2.112:](#) Only defined in Windows 2000 Server.

[<117> Section 2.2.1.2.113:](#) Only defined in Windows 2000 Server.

[<118> Section 2.2.1.2.114:](#) Only defined in Windows 2000 Server.

[<119> Section 2.2.1.2.115:](#) Only defined in Windows 2000 Server.

[<120> Section 2.2.1.2.116:](#) Only defined in Windows 2000 Server.

[<121> Section 2.2.1.2.117:](#) Only defined in Windows 2000 Server.

[<122> Section 2.2.1.2.118:](#) Only defined in Windows 2000 Server.

[<123> Section 2.2.1.2.119:](#) Only defined in Windows 2000 Server.

[<124> Section 2.2.1.2.120:](#) Only defined in Windows 2000 Server.

[<125> Section 2.2.1.2.121:](#) Only defined in Windows 2000 Server.

[<126> Section 2.2.1.2.122:](#) Only defined in Windows 2000 Server.

[<127> Section 2.2.1.2.126:](#) Only defined in Windows 2000 Server.

[<128> Section 2.2.1.2.127:](#) Only defined in Windows 2000 Server.

[<129> Section 2.2.1.2.130:](#) Windows Server 2008 R2 only.

[<130> Section 2.2.1.2.131:](#) Windows Server 2008 R2 only.

[<131> Section 2.2.1.2.132:](#) Windows Server 2008 R2 only.

[<132> Section 2.2.1.2.134:](#) Only defined in Windows 2000 Server.

[<133> Section 2.2.1.2.134:](#) Windows Server 2008 R2 only.

[<134> Section 2.2.1.2.137:](#) This is available only in Windows Server 2008 R2.

[<135> Section 2.2.1.2.138:](#) This is available beginning with Windows Server 2008 R2.

[<136> Section 2.2.1.2.138:](#) The port limit is determined by the Windows server license.

[<137> Section 2.2.1.2.139:](#) This is available beginning with Windows Server 2008 R2.

[<138> Section 2.2.1.2.139:](#) The port limit is determined by the Windows server license.

[<139> Section 2.2.1.2.140:](#) This is available beginning with Windows Server 2008 R2.

[<140> Section 2.2.1.2.140:](#) The port limit is determined by the Windows server license.

[<141> Section 2.2.1.2.141:](#) This is available beginning with Windows Server 2008 R2.

[<142> Section 2.2.1.2.142:](#) This is available beginning with Windows Server 2008 R2.

[<143> Section 2.2.1.2.142:](#) The port limit is determined by the Windows server license.

[<144> Section 2.2.1.2.143:](#) This is available beginning with Windows Server 2008 R2.

[<145> Section 2.2.1.2.144:](#) This is available beginning with Windows Server 2008 R2.

[<146> Section 2.2.1.2.145:](#) This is available beginning with Windows Server 2008 R2.

[<147> Section 2.2.1.2.146:](#) This is available beginning with Windows Server 2008 R2.

[<148> Section 2.2.1.2.148:](#) This is available beginning with Windows Server 2008 R2.

[<149> Section 2.2.1.2.149:](#) This is available beginning with Windows Server 2008 R2.

[<150> Section 2.2.1.2.190:](#) Windows 2000 Server and Windows Server 2003 only.

[<151> Section 2.2.1.2.201:](#) Not available in Windows 2000 Server.

[<152> Section 2.2.1.2.202:](#) Only defined in Windows Server 2003.

[<153> Section 2.2.1.2.204:](#) Only defined in Windows Server 2003.

[<154> Section 2.2.1.2.205:](#) Only defined in Windows 2000 Server.

[<155> Section 2.2.1.2.206:](#) Only defined in Windows Server 2003.

[<156> Section 2.2.1.2.207:](#) Only defined in Windows Server 2003.

[<157> Section 2.2.1.2.208:](#) Windows 2000 Server and Windows Server 2003 only.

[<158> Section 2.2.1.2.209:](#) Windows 2000 Server and Windows Server 2003 only.

[<159> Section 2.2.1.2.210:](#) Windows 2000 Server and Windows Server 2003 only.

[<160> Section 2.2.1.2.211:](#) Windows 2000 Server and Windows Server 2003 only.

[<161> Section 2.2.1.2.212:](#) Windows 2000 Server and Windows Server 2003 only.

[<162> Section 2.2.1.2.213:](#) Windows 2000 Server and Windows Server 2003 only.

[<163> Section 2.2.1.2.214:](#) Windows 2000 Server and Windows Server 2003 only.

[<164> Section 2.2.1.2.215:](#) Windows 2000 Server and Windows Server 2003 only.

[<165> Section 2.2.1.2.216:](#) Windows 2000 Server and Windows Server 2003 only.

[<166> Section 2.2.1.2.217:](#) Not defined in Windows 2000 Server.

[<167> Section 2.2.1.2.218:](#) 5 for Windows 2000 Server, 6 for Windows Server 2003, Windows Server 2008, Windows Server 2008 R2

[<168> Section 2.2.1.2.219:](#) 5 for Windows 2000 Server, 6 for Windows Server 2003, Windows Server 2008, Windows Server 2008 R2

[<169> Section 2.2.1.2.219:](#) Not defined in Windows 2000 Server

[<170> Section 2.2.1.2.219:](#) Not defined in Windows 2000 Server

[<171> Section 2.2.1.2.228:](#) Not defined in Windows 2000 Server

[<172> Section 2.2.1.2.228:](#) Not defined in Windows 2000 Server

[<173> Section 2.2.1.2.228:](#) Not defined in Windows 2000 Server and Windows Server 2003

[<174> Section 2.2.1.2.230:](#) Defined in Windows 2000 Server and Windows Server 2003

[<175> Section 2.2.1.2.230:](#) Defined in Windows 2000 Server and Windows Server 2003

[<176> Section 2.2.1.2.230:](#) Not defined in Windows 2000 Server

[<177> Section 2.2.2:](#) The phonebook file used by Windows is router.pbk present under the directory System32 under the Windows folder. For example C:\Windows\System32\ras\router.pbk is the file used on RRAS server where Windows folder is C:\Windows

[<178> Section 2.2.2.1:](#) On Windows 2000 Server, Windows Server 2003 the number of characters in RRAS entry section name MUST NOT exceeds 256 bytes.

On Windows Server 2008 and Windows Server 2008 R2, the numbers of characters in the RRAS entry section name MUST NOT exceed 1536 bytes.

[<179> Section 2.2.2.2.3:](#) On Windows Server 2008 R2 Type key is optional. On Windows 2000 Server, Windows Server 2003, and Windows Server 2008 Type key must be present

[<180> Section 2.2.2.2.3:](#) This option is not available on Windows 2000 Server

[<181> Section 2.2.2.2.11:](#) On Windows 2000 Server, Windows Server 2003, and Windows Server 2008, RRAS attempts L2TP first. If L2TP fails, PPTP is tried. If PPTP fails, demand-dial connection fails.

On Windows Server 2008 R2, RRAS attempts PPTP first. If PPTP fails, L2TP is tried. If L2TP fails, demand-dial connection fails

[<182> Section 2.2.2.2.12:](#) Available only on Windows 2000 Server

[<183> Section 2.2.2.2.12:](#) Available only on Windows 2000 Server

[<184> Section 2.2.2.2.12:](#) Available only on Windows Server 2008 and Windows Server 2008 R2

[<185> Section 2.2.2.2.20:](#) On Windows 2000 and Windows Server 2003, RRAS adjusts the number of subentries configured for the connection as bandwidth is needed. RRAS uses **DialPercent**, **DialSeconds**, **HangupPercent**, and **HangupSeconds** to determine when to dial or disconnect a subentry.

On Windows Server 2008 and Windows Server 2008 R2, RRAS ignores this key and assumes the value to be 1.

[<186> Section 2.2.2.2.21:](#) This key is ignored on Windows Server 2008 and Windows Server 2008 R2.

[<187> Section 2.2.2.2.22:](#) This key is ignored on Windows Server 2008 and Windows Server 2008 R2.

[<188> Section 2.2.2.2.23:](#) This key is ignored on Windows Server 2008 and Windows Server 2008 R2.

[<189> Section 2.2.2.2.24:](#) This key is ignored on Windows Server 2008 and Windows Server 2008 R2.

[<190> Section 2.2.2.2.35:](#) This key is ignored on Windows 2000 Server and Windows Server 2003

[<191> Section 2.2.2.2.38:](#) On Windows 2000 Server and Windows Server 2003 the option to enable NetBT on the RRAS entry is based on the values for the keys **ShareMsFilePrint** and **BindMsNetClient**. The following table specifies the behavior on Windows 2000 Server and Windows Server 2003:

ShareMsFilePrint	BindMsNetClient	Meaning
0	0	Disable NetBT.
0	1	Enable NetBT.
1	0	Enable NetBT.
1	1	Enable NetBT.

On Windows Server 2008 and Windows Server 2008 R2, RRAS relies on the keys **ShareMsFilePrint**, **BindMsNetClient**, and **IpNBTFIags** to configure NetBT on the RRAS entry.

[<192> Section 2.2.2.2.46:](#) This key is ignored on Windows 2000 Server.

[<193> Section 2.2.2.2.47:](#) This key is ignored on Windows 2000 Server.

[<194> Section 2.2.2.2.48:](#) This key is ignored in Windows 2000 Server.

[<195> Section 2.2.2.2.49:](#) This key is ignored in Windows 2000 Server.

[<196> Section 2.2.2.2.58:](#) SPAP is not present only on Windows Server 2008 and Windows Server 2008 R2.

[<197> Section 2.2.2.2.58:](#) MSCHAPv1 is not present only on Windows Server 2008 and Windows Server 2008 R2.

[<198> Section 2.2.2.2.58:](#) MSCHAP Windows 95 compatible is present only on Windows 2000 Server and Windows Server 2003.

[<199> Section 2.2.2.2.73:](#) **IpNBTFIags** key is present only on Windows Server 2008 and Windows Server 2008 R2. The meaning for the combination of values for keys **IpNBTFIags**, **BindMsNetClient**, and **ShareMsFilePrint** is given in the following table.

Value	Meaning
0	Disable NetBT.
1	Disable NetBT if the value for the keys <b>ShareMsFilePrint</b> and <b>BindMsNetClient</b> is set to "0".
1	Enable NetBT if the value for either of the keys <b>ShareMsFilePrint</b> and <b>BindMsNetClient</b> is "1".

[<200> Section 2.2.2.2.74:](#) This key is ignored on Windows Server 2008 and Windows Server 2008 R2.

[<201> Section 2.2.2.2.79:](#) This key is ignored on Windows 2000 Server, Windows Server 2003, and Windows Server 2008.

[<202> Section 2.2.2.2.80:](#) This key is ignored on Windows 2000 Server, Windows Server 2003, and Windows Server 2008.

[<203> Section 2.2.2.2.84:](#) This key is ignored on Windows 2000 Server and Windows Server 2003.

[<204> Section 2.2.2.2.85:](#) This key is ignored on Windows 2000 Server and Windows Server 2003.

[<205> Section 2.2.2.2.86:](#) This key is ignored on Windows 2000 Server, Windows Server 2003, and Windows Server 2008.

[<206> Section 2.2.2.2.87:](#) This key is ignored on Windows 2000 Server, Windows Server 2003, and Windows Server 2008.

[<207> Section 2.2.2.2.97:](#) On Windows Server 2008 R2, if the key **PBVersion** is present and is set to "1", and the **Type** key is present, then this key is optional.

[<208> Section 2.2.2.2.100:](#)

1. X25 and Pad device types are supported in Windows 2000 Server and Windows Server 2003.
2. PPPoE device type is not supported in Windows 2000 Server.
3. In Windows 2000 Server the value of DEVICE key is same as that of MEDIA key for all the device types other than isdn, x25, Pad, modem, and switch.

[<209> Section 2.2.2.2.101:](#) This key is available only in Windows Server 2003.

[<210> Section 2.2.2.2.104:](#) X25 and Pad device types are ignored in Windows Server 2008 and Windows Server 2008 R2.

[<211> Section 2.2.2.2.105:](#) X25 and Pad device types are ignored in Windows Server 2008 and Windows Server 2008 R2.

[<212> Section 2.2.2.2.106:](#) X25 and Pad device types are ignored in Windows Server 2008 and Windows Server 2008 R2.

[<213> Section 2.2.2.2.107:](#) X25 and Pad device types are ignored in Windows Server 2008 and Windows Server 2008 R2.

[<214> Section 2.2.3:](#) Windows clients use these registry keys to manage RRAS configuration when the RRAS server is offline.

[<215> Section 2.2.3.1:](#) Available beginning in Windows Server 2008

[<216> Section 2.2.3.1:](#) Available only in Windows 2000 Server.

[<217> Section 2.2.3.1.3:](#) Windows defines GlobalInterfaceInfo only for the IPX transport, which is available only in Windows 2000.

[<218> Section 2.2.3.4.18.3:](#) Windows defines this registry key only on Windows 2000 Server and Windows Server 2003.

[<219> Section 2.2.3.4.19.4:](#) Windows defines this registry key only on Windows 2000 Server and Windows Server 2003.

[<220> Section 3.1.1:](#) Windows 2000 only.

[<221> Section 3.1.1:](#) Not available in versions before Windows Server 2008.

[<222> Section 3.1.4.1:](#) Only defined beginning with Windows Server 2003.

[<223> Section 3.1.4.1:](#) Only defined beginning with Windows Server 2008.

[<224> Section 3.1.4.1:](#) Only defined beginning with Windows Server 2003.

[<225> Section 3.1.4.1:](#) Only defined beginning with Windows Server 2008.

[<226> Section 3.1.4.2:](#) Only defined in Windows Server 2008.

[<227> Section 3.1.4.3:](#) Only defined beginning with Windows Server 2008.

[<228> Section 3.1.4.3:](#) Only defined beginning with Windows Server 2008.

[<229> Section 3.1.4.10:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<230> Section 3.1.4.10:](#) Windows 2000 Server only.

[<231> Section 3.1.4.10:](#) Not available in versions before Windows Server 2008.

[<232> Section 3.1.4.11:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<233> Section 3.1.4.11:](#) Windows 2000 Server only.

[<234> Section 3.1.4.11:](#) Not available before Windows Server 2008.

[<235> Section 3.1.4.11:](#) Windows 2000 Server and Windows Server 2003 only.

[<236> Section 3.1.4.11:](#) Not available in Windows 2000 Server.

[<237> Section 3.1.4.12:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<238> Section 3.1.4.13:](#) Not supported in Windows 2000, Windows XP, Windows Vista, and Windows 7.

[<239> Section 3.1.4.13:](#) No error is returned in Windows 2000 Server if **dwIfType** is set to ROUTER\_IF\_TYPE\_TUNNEL1.

[<240> Section 3.1.4.14:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<241> Section 3.1.4.15:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<242> Section 3.1.4.15:](#) Not available before Windows Server 2008.

[<243> Section 3.1.4.16:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<244> Section 3.1.4.17:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<245> Section 3.1.4.17:](#) Not available before Windows Server 2008.

[<246> Section 3.1.4.17:](#) Windows 2000 Server only.

[<247> Section 3.1.4.17:](#) Windows 2000 Server only.

[<248> Section 3.1.4.17:](#) Not available before Windows Server 2008.

[<249> Section 3.1.4.18:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<250> Section 3.1.4.18:](#) Windows 2000 Server only.

[<251> Section 3.1.4.18:](#) Not available before Windows Server 2008.

[<252> Section 3.1.4.18:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<253> Section 3.1.4.18:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<254> Section 3.1.4.18:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<255> Section 3.1.4.18:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<256> Section 3.1.4.18:](#) Windows 2000 Server and Windows Server 2003 only.

[<257> Section 3.1.4.19:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<258> Section 3.1.4.19:](#) Windows 2000 Server only.

[<259> Section 3.1.4.19:](#) Not available before Windows Server 2008.

[<260> Section 3.1.4.19:](#) IPV6\_ROUTE\_INFO and [FILTER\\_DESCRIPTOR\\_V6 \(section 2.2.1.2.7\)](#) can only be retrieved beginning with Windows Server 2008 R2.

[<261> Section 3.1.4.20:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<262> Section 3.1.4.20:](#) Windows 2000 Server only.

[<263> Section 3.1.4.20:](#) Not available before Windows Server 2008.

[<264> Section 3.1.4.20:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<265> Section 3.1.4.20:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<266> Section 3.1.4.20:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<267> Section 3.1.4.20:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<268> Section 3.1.4.20:](#) IPv6-related information and features are only defined in Windows Server 2008.

[<269> Section 3.1.4.20:](#) Windows 2000 Server and Windows Server 2003 only.



[<270> Section 3.1.4.21:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<271> Section 3.1.4.22:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<272> Section 3.1.4.24:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<273> Section 3.1.4.24:](#) Windows 2000 Server only.

[<274> Section 3.1.4.25:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<275> Section 3.1.4.25:](#) Windows 2000 Server only.

[<276> Section 3.1.4.26:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<277> Section 3.1.4.27:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<278> Section 3.1.4.28:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<279> Section 3.1.4.28:](#) Not supported in Windows Server 2008 and Windows Server 2008 R2.

[<280> Section 3.1.4.29:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<281> Section 3.1.4.30:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<282> Section 3.1.4.30:](#) Windows 2000 Server only.

[<283> Section 3.1.4.30:](#) The method does not support PID\_IPV6 in Windows Server 2008 and earlier.

[<284> Section 3.1.4.30:](#) Windows 2000 Server and Windows Server 2003 only.

[<285> Section 3.1.4.31:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<286> Section 3.1.4.31:](#) Windows 2000 Server only.

[<287> Section 3.1.4.31:](#) Not available before Windows Server 2008.

[<288> Section 3.1.4.31:](#) Windows 2000 Server and Windows Server 2003 only.

[<289> Section 3.1.4.32:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<290> Section 3.1.4.32:](#) Windows returns ERROR\_SUCCESS when the global configuration for IPBOOTP is requested. Since only one global configuration is available for IPBOOTP, RMIBEntryGetNext is treated same as RMIBEntryGetFirst and the global configuration is always returned with return value ERROR\_SUCCESS.



[<291> Section 3.1.4.33:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<292> Section 3.1.4.33:](#) Windows 2000 Server only.

[<293> Section 3.1.4.33:](#) Not available before Windows Server 2008.

[<294> Section 3.1.4.34:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<295> Section 3.1.4.34:](#) This method is not invoked by Windows remotely.

[<296> Section 3.1.4.35:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<297> Section 3.1.4.35:](#) This method is not invoked by Windows remotely.

[<298> Section 3.1.4.36:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<299> Section 3.1.4.36:](#) Only defined in Windows Server 2003.

[<300> Section 3.1.4.37:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<301> Section 3.1.4.38:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<302> Section 3.1.4.38:](#) Windows 2000 Server only.

[<303> Section 3.1.4.38:](#) Not available in versions before Windows Server 2008.

[<304> Section 3.1.4.38:](#) For Windows, iptrmgr.dll MUST be present in the %systemroot%\system32 folder.

[<305> Section 3.1.4.39:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<306> Section 3.1.4.40:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<307> Section 3.1.4.40:](#) Windows does not validate the type of devices being added for a connection. Thus, if the devices specified are valid serial, ISDN, PPPoE, or VPN devices (as provided by the [RRouterDeviceEnum](#) method), the addition of the VPN/PPPoE devices still succeeds and the method returns ERROR\_SUCCESS, though the functionality itself is not supported.

[<308> Section 3.1.4.41:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<309> Section 3.1.4.42:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<310> Section 3.1.4.43:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<311> Section 3.1.4.43:](#) Only defined in Windows Server 2003.

[<312> Section 3.1.4.44:](#) Not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<313> Section 3.1.4.44:](#) For each VPN Tunnel Type, Windows maintains the port configuration by using the registry keys **MaxWanEndpoints** and **WanEndpoints** as specified in sections [2.2.3.3.1.7](#) and [2.2.3.3.1.8](#), respectively. **WanEndpoints** corresponds to the number of ports being configured through the **MPR\_SERVER\_1** and **MPR\_SERVER\_2** structures. When **WanEndpoints** configured is more than **MaxWanEndpoints**, a reboot is required for the configuration change to be applied by the RRAS implementation. In such a case, Windows returns the error code **ERROR\_SUCCESS\_REBOOT\_REQUIRED**.

[<314> Section 3.1.4.44:](#) Windows returns the error value **ERROR\_REBOOT\_REQUIRED** when the configuration change requires a reboot of the machine for the settings to be applied. One such implementation requirement is when the number of ports configured is more than the maximum number of ports that the tunneling protocols are configured to support initially.

[<315> Section 3.1.4.45:](#) This method is introduced in Windows Server 2008 R2 and Windows 7.

[<316> Section 3.1.4.46:](#) This method is introduced in Windows Server 2008 R2 and Windows 7.

[<317> Section 3.1.4.47:](#) This method is introduced in Windows Server 2008 R2 and Windows 7.

[<318> Section 3.1.4.48:](#) This method is introduced in Windows Server 2008 R2. It is not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<319> Section 3.1.4.48:](#) Windows returns the error value **ERROR\_REBOOT\_REQUIRED** when the configuration change requires a reboot of the machine for the settings to be applied. One such instance is when the number of ports configured is more than the maximum number of ports that the tunneling protocols are configured to support initially.

[<320> Section 3.1.4.48:](#) Windows returns the error value **ERROR\_SUCCESS\_RESTART\_REQUIRED** when a configuration change is being done for SSTP or IKEv2, such as when the value for the `setConfigForProtocols` member of [MPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_1](#) in `pServerConfig` is specified as `MPRAPI_SET_CONFIG_PROTOCOL_FOR_SSTP (0x00000004)` or `MPRAPI_SET_CONFIG_PROTOCOL_FOR_IKEV2 (0x00000008)`.

[<321> Section 3.1.4.49:](#) This method is introduced in Windows Server 2008 R2. It is not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<322> Section 3.1.4.50:](#) This method is introduced in Windows Server 2008 R2. It is not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<323> Section 3.1.4.51:](#) Not available before Windows Server 2008 R2.

[<324> Section 3.1.4.51:](#) This method is introduced in Windows Server 2008 R2. It is not available on Windows 2000, Windows XP, Windows Vista, or Windows 7.

[<325> Section 3.2.4.15:](#) Windows implementation calls [RRouterInterfaceGetInfo \(section 3.2.4.14\)](#) in order to construct and fill the structures with which [RRouterInterfaceSetInfo](#) will be called. After the structure is retrieved using [RRouterInterfaceGetInfo](#), the necessary configuration modifications are applied to the structure before calling [RRouterInterfaceSetInfo](#).

[<326> Section 3.3.4:](#) Windows 2000 does not throw an exception to indicate the client does not have access.

[<327> Section 3.3.4:](#) Windows 2000 returns the status value of **E\_ACCESSDENIED** (0x80070005).

[<328> Section 3.3.4.1:](#) Windows 2000 Server does not throw an RPC exception. Instead it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<329> Section 3.3.4.2:](#) Windows 2000 Server does not throw an RPC exception. Instead it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<330> Section 3.3.4.2:](#) Windows 2000 Server does not perform access permission validation.

[<331> Section 3.3.4.3:](#) Windows 2000 Server does not throw an RPC exception. Instead, it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<332> Section 3.3.4.4:](#) Windows 2000 Server does not throw an RPC exception. Instead, it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<333> Section 3.3.4.4:](#) Windows 2000 Server does not validate access permission.

[<334> Section 3.3.4.5:](#) Windows 2000 Server does not throw an RPC exception. Instead, it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<335> Section 3.3.4.5:](#) Maximum ReqTypes enumeration is 141 for Windows Server 2008 R2, 137 for Windows Server 2008, 129 for Windows Server 2003, 122 for Windows 2000 Server.

[<336> Section 3.3.4.5:](#) The version is 5 for Windows 2000 Server, 6 for Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2

[<337> Section 3.3.4.5:](#) Not in Windows 2000 Server.

[<338> Section 3.3.4.6:](#) Valid only Windows 2000 Server

[<339> Section 3.3.4.6:](#) Valid only Windows 2000 Server

[<340> Section 3.3.4.6:](#) Not valid for Windows 2000 Server and Windows Server 2003

[<341> Section 3.3.4.6:](#) Windows 2000 Server does not throw an RPC exception. Instead, it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<342> Section 3.3.4.7:](#) Windows 2000 Server does not throw an RPC exception. Instead, it returns an error value of **E\_ACCESSDENIED** (0x80070005).

[<343> Section 3.3.4.7:](#) Windows 2000 Server does not validate access permission.

[<344> Section 3.3.4.7:](#) 5 for Windows 2000 Server, 6 for Windows Server 2003, Windows Server 2008, Windows Server 2008 R2.

[<345> Section 3.4.4:](#) Windows 2000 Server will return a status of E\_ACCESS\_DENIED if the client is not an administrator of the RRAS server.

[<346> Section 4.1:](#) Only defined in Windows Server 2008.

[<347> Section 4.1:](#) Only defined in Windows Server 2008.

[<348> Section 4.1:](#) Only defined in Windows Server 2008.

[<349> Section 4.1:](#) Only defined in Windows Server 2008.

[<350> Section 4.2:](#) Only defined in Windows Server 2008.

[<351> Section 4.2:](#) Only defined in Windows Server 2008.

[<352> Section 4.6:](#) This section applies only to Windows Server 2008 R2.

[<353> Section 5.1.1:](#) Supported beginning in Windows Server 2003

## 8 Change Tracking

This section identifies changes that were made to the [MS-RRASM] protocol document between the May 2011 and June 2011 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact [protocol@microsoft.com](mailto:protocol@microsoft.com).

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
<a href="#">1.2 References</a>	Added explanatory statement regarding the removal of the publishing year from Microsoft Open Specification document references.	N	Content updated.

## 9 Index

### A

Abstract data model  
  client  
    [DIMSVC interface](#) 380  
    [RASRPC interface](#) 398  
  server  
    [DIMSVC interface](#) 294  
    [RASRPC interface](#) 385  
[Applicability](#) 32

### C

[Capability negotiation](#) 33  
[CERT\\_BLOB\\_1 packet](#) 178  
[Change tracking](#) 497  
Client  
  abstract data model  
    [DIMSVC interface](#) 380  
    [RASRPC interface](#) 398  
  initialization  
    [DIMSVC interface](#) 380  
    [RASRPC interface](#) 398  
  local events  
    [DIMSVC interface](#) 385  
    [RASRPC interface](#) 400  
  message processing  
    [DIMSVC interface](#) 381  
    [RASRPC interface](#) 398  
  security settings  
    [dimsvc](#) 34  
    [Rasrpc](#) 35  
  sequencing rules  
    [DIMSVC interface](#) 381  
    [RASRPC interface](#) 398  
  timer events  
    [DIMSVC interface](#) 385  
    [RASRPC interface](#) 400  
  timers  
    [DIMSVC interface](#) 380  
    [RASRPC interface](#) 398  
[Common data types](#) 35  
[Common messages](#) 35  
[Configuration example](#) 418  
[Connection object](#) 32  
[Constants](#) 35  
[Creating demand dial interface with filters example](#) 403

### D

Data model - abstract  
  client  
    [DIMSVC interface](#) 380  
    [RASRPC interface](#) 398  
  server  
    [DIMSVC interface](#) 294  
    [RASRPC interface](#) 385

[Data types](#) 35  
[DeviceConfigInfo packet](#) 244  
[DHCPV6R\\_GLOBAL\\_CONFIG structure](#) 189  
[DHCPV6R\\_IF\\_CONFIG structure](#) 191  
[DHCPV6R\\_IF\\_STATS structure](#) 190  
[DHCPV6R\\_MIB\\_GET\\_INPUT\\_DATA structure](#) 192  
[DHCPV6R\\_MIB\\_GET\\_OUTPUT\\_DATA structure](#) 189  
[DIM\\_INFORMATION\\_CONTAINER structure](#) 46  
[DIM\\_INTERFACE\\_CONTAINER structure](#) 48  
[DIM\\_MIB\\_ENTRY\\_CONTAINER structure](#) 66  
[DIMSVC interface - server](#) 294  
[Disconnecting particular user connection example](#) 401

### E

[EAPTLS\\_HASH structure](#) 166  
[EAPTLS\\_USER\\_PROPERTIES packet](#) 167  
[Enum packet](#) 248  
[Enumerating interfaces and connecting dd1 example](#) 406  
[Enumerations](#) 35  
Events  
  local - client  
    [DIMSVC interface](#) 385  
    [RASRPC interface](#) 400  
  local - server  
    [DIMSVC interface](#) 379  
    [RASRPC interface](#) 397  
  timer - client  
    [DIMSVC interface](#) 385  
    [RASRPC interface](#) 400  
  timer - server  
    [DIMSVC interface](#) 379  
    [RASRPC interface](#) 397  
Examples  
  [configuration](#) 418  
  [creating demand dial interface with filters](#) 403  
  [disconnecting particular user connection](#) 401  
  [enumerating interfaces and connecting dd1](#) 406  
  [interface configuration](#) 416  
  [ports configuration](#) 417  
  [querying interface status through Management Information Base \(MIB\)](#) 406  
  [querying server configuration information](#) 401  
  [registry configuration](#) 415  
  [retrieving device configuration information](#) 409  
  [retrieving specific port information](#) 410  
  [retrieving the Rasrpc server version info](#) 408  
  [sample phonebook file for a demand-dial connection](#) 411  
  [transport configuration](#) 415  
  [updating connection endpoint of IKEv2-based connection](#) 407

### F

[Fields - vendor-extensible](#) 33

[FILTER\\_DESCRIPTOR packet](#) 54  
[FILTER\\_DESCRIPTOR\\_V6 packet](#) 57  
[FILTER\\_INFO structure](#) 55  
[FILTER\\_INFO\\_V6 structure](#) 57  
[FORWARD\\_ACTION enumeration](#) 38  
[Full IDL](#) 422

## G

[GetDevConfigStruct packet](#) 248  
[GetNdiswanDriverCapsStruct structure](#) 247  
[GetSetCalledId packet](#) 245  
[GLOBAL\\_INFO structure](#) 59  
[Glossary](#) 17

## I

[IDL](#) 422  
[IF\\_TABLE\\_INDEX structure](#) 149  
[IFFILTER\\_INFO structure](#) 142  
[IGMP\\_MIB\\_GET\\_INPUT\\_DATA structure](#) 203  
[IGMP\\_MIB\\_GET\\_OUTPUT\\_DATA packet](#) 204  
[IGMP\\_MIB\\_GLOBAL\\_CONFIG](#) 206  
[IGMP\\_MIB\\_GLOBAL\\_CONFIG structure](#) 206  
[IGMP\\_MIB\\_GROUP\\_IFS\\_LIST packet](#) 214  
[IGMP\\_MIB\\_GROUP\\_INFO](#) 210  
[IGMP\\_MIB\\_GROUP\\_INFO structure](#) 210  
[IGMP\\_MIB\\_GROUP\\_INFO\\_V3](#) 214  
[IGMP\\_MIB\\_GROUP\\_INFO\\_V3 structure](#) 214  
[IGMP\\_MIB\\_IF\\_CONFIG structure](#) 206  
[IGMP\\_MIB\\_IF\\_GROUPS\\_LIST](#) 209  
[IGMP\\_MIB\\_IF\\_GROUPS\\_LIST structure](#) 209  
[IGMP\\_MIB\\_IF\\_STATS structure](#) 211  
[IKEV2\\_CONFIG\\_PARAMS\\_1 structure](#) 179  
[IKEV2\\_PROJECTION\\_INFO\\_1 structure](#) 173  
[IKEV2\\_TUNNEL\\_CONFIG\\_PARAMS\\_1 packet](#) 178  
Implementer - security considerations  
    [overview](#) 421  
    [RRAS Management Protocol-specific](#) 421  
[IN6\\_ADDR structure](#) 59  
[Index of security parameters](#) 421  
[Info structure](#) 250  
[Informative references](#) 26  
Initialization  
    client  
        [DIMSVC interface](#) 380  
        [RASRPC interface](#) 398  
    server  
        [DIMSVC interface](#) 295  
        [RASRPC interface](#) 386  
[Interface configuration example](#) 416  
[Interface object](#) 29  
[INTERFACE\\_ROUTE\\_ENTRY](#) 215  
[INTERFACE\\_ROUTE\\_ENTRY structure](#) 215  
[INTERFACE\\_ROUTE\\_INFO structure](#) 60  
[INTERFACE\\_STATUS\\_INFO structure](#) 66  
Interfaces - server  
    [DIMSVC](#) 294  
    [RASRPC](#) 385  
[Introduction](#) 17  
[IP\\_ALG\\_GLOBAL\\_INFO structure](#) 232  
[IP\\_AUTO\\_DHCP\\_GLOBAL\\_INFO structure](#) 225

[IP\\_AUTO\\_DHCP\\_INTERFACE\\_INFO structure](#) 226  
[IP\\_AUTO\\_DHCP\\_MIB\\_QUERY structure](#) 220  
[IP\\_AUTO\\_DHCP\\_STATISTICS structure](#) 221  
[IP\\_DNS\\_PROXY\\_GLOBAL\\_INFO structure](#) 227  
[IP\\_DNS\\_PROXY\\_INTERFACE\\_INFO structure](#) 228  
[IP\\_DNS\\_PROXY\\_MIB\\_QUERY packet](#) 219  
[IP\\_DNS\\_PROXY\\_STATISTICS](#) 220  
[IP\\_DNS\\_PROXY\\_STATISTICS structure](#) 220  
[IP\\_NAT\\_ADDRESS\\_MAPPING structure](#) 232  
[IP\\_NAT\\_ADDRESS\\_RANGE structure](#) 231  
[IP\\_NAT\\_DIRECTION enumeration](#) 41  
[IP\\_NAT\\_ENUMERATE\\_SESSION\\_MAPPINGS packet](#) 217  
[IP\\_NAT\\_GLOBAL\\_INFO structure](#) 228  
[IP\\_NAT\\_INTERFACE\\_INFO structure](#) 229  
[IP\\_NAT\\_INTERFACE\\_STATISTICS](#) 219  
[IP\\_NAT\\_INTERFACE\\_STATISTICS structure](#) 219  
[IP\\_NAT\\_MIB\\_QUERY structure](#) 216  
[IP\\_NAT\\_PORT\\_MAPPING structure](#) 232  
[IP\\_NAT\\_SESSION\\_MAPPING structure](#) 217  
[IP\\_NAT\\_TIMEOUT structure](#) 229  
[IPBOOTP\\_GLOBAL\\_CONFIG structure](#) 184  
[IPBOOTP\\_IF\\_BINDING structure](#) 188  
[IPBOOTP\\_IF\\_CONFIG structure](#) 185  
[IPBOOTP\\_IF\\_STATS structure](#) 187  
[IPBOOTP\\_IP\\_ADDRESS structure](#) 189  
[IPBOOTP\\_MIB\\_GET\\_INPUT\\_DATA structure](#) 186  
[IPBOOTP\\_MIB\\_GET\\_OUTPUT\\_DATA structure](#) 187  
[IPINIP\\_CONFIG\\_INFO structure](#) 65  
[IPRIP\\_GLOBAL\\_CONFIG structure](#) 194  
[IPRIP\\_GLOBAL\\_STATS structure](#) 194  
[IPRIP\\_IF\\_BINDING structure](#) 202  
[IPRIP\\_IF\\_CONFIG packet](#) 196  
[IPRIP\\_IF\\_CONFIG structure](#) 195  
[IPRIP\\_IP\\_ADDRESS structure](#) 202  
[IPRIP\\_MIB\\_GET\\_INPUT\\_DATA structure](#) 192  
[IPRIP\\_MIB\\_GET\\_OUTPUT\\_DATA structure](#) 193  
[IPRIP\\_PEER\\_STATS](#) 203  
[IPRIP\\_PEER\\_STATS structure](#) 203  
[IPRIP\\_ROUTE\\_FILTER structure](#) 201  
[IPX\\_ADAPTER\\_INFO structure](#) 146  
[IPX\\_GLOBAL\\_INFO structure](#) 143  
[IPX\\_IF\\_INFO structure](#) 144  
[IPX\\_IF\\_STATS structure](#) 153  
[IPX\\_INTERFACE structure](#) 154  
[IPX\\_MIB\\_GET\\_INPUT\\_DATA structure](#) 152  
[IPX\\_MIB\\_INDEX structure](#) 151  
[IPX\\_MIB\\_ROW structure](#) 158  
[IPX\\_MIB\\_SET\\_INPUT\\_DATA structure](#) 158  
[IPX\\_ROUTE structure](#) 157  
[IPX\\_SERVER\\_ENTRY structure](#) 145  
[IPX\\_SERVICE structure](#) 163  
[IPX\\_STATIC\\_NETBIOS\\_NAME\\_INFO structure](#) 146  
[IPX\\_STATIC\\_ROUTE\\_INFO structure](#) 144  
[IPX\\_STATIC\\_SERVICE\\_INFO](#) 145  
[IPX\\_TRAFFIC\\_FILTER\\_GLOBAL\\_INFO structure](#) 147  
[IPX\\_TRAFFIC\\_FILTER\\_INFO structure](#) 147  
[IPXMIB\\_BASE structure](#) 152  
[IPXWAN\\_IF\\_INFO structure](#) 144

## L



[L2TP\\_CONFIG\\_PARAMS\\_1 structure](#) 180

#### Local events

##### client

[DIMSVC interface](#) 385

[RASRPC interface](#) 400

##### server

[DIMSVC interface](#) 379

[RASRPC interface](#) 397

[LPIN6\\_ADDR](#) 59

[LPRASRPC\\_CALLBACKLIST](#) 254

[LPRASRPC\\_LOCATIONLIST](#) 256

[LPRASRPC\\_PBUSER](#) 252

[LPRASRPC\\_STRINGLIST](#) 256

## M

[Management Information Base \(MIB\) object](#) 30

[MCAST\\_HBEAT\\_INFO structure](#) 64

#### Message processing

##### client

[DIMSVC interface](#) 381

[RASRPC interface](#) 398

##### server

[DIMSVC interface](#) 295

[RASRPC interface](#) 386

#### Messages

[RPC common](#) 35

[transport](#) 34

[MIB\\_BEST\\_IF structure](#) 69

[MIB\\_BOUNDARYROW structure](#) 69

[MIB\\_DA\\_MSG structure](#) 221

[MIB\\_ICMP structure](#) 70

[MIB\\_IFNUMBER structure](#) 72

[MIB\\_IFROW structure](#) 72

[MIB\\_IFSTATUS structure](#) 74

[MIB\\_IFTABLE packet](#) 75

[MIB\\_IPADDRROW structure](#) 76

[MIB\\_IPADDDRTABLE packet](#) 77

[MIB\\_IPDESTROW structure](#) 68

[MIB\\_IPDESTTABLE packet](#) 68

[MIB\\_IPFORWARD\\_PROTO enumeration](#) 38

[MIB\\_IPFORWARD\\_TYPE enumeration](#) 38

[MIB\\_IPFORWARDNUMBER structure](#) 77

[MIB\\_IPFORWARDROW structure](#) 77

[MIB\\_IPFORWARDTABLE packet](#) 79

[MIB\\_IPMCAST\\_BOUNDARY structure](#) 79

[MIB\\_IPMCAST\\_BOUNDARY\\_TABLE packet](#) 80

[MIB\\_IPMCAST\\_GLOBAL structure](#) 81

[MIB\\_IPMCAST\\_IF\\_ENTRY structure](#) 81

[MIB\\_IPMCAST\\_IF\\_TABLE structure](#) 81

[MIB\\_IPMCAST\\_MFE structure](#) 82

[MIB\\_IPMCAST\\_MFE\\_STATS packet](#) 83

[MIB\\_IPMCAST\\_OIF structure](#) 83

[MIB\\_IPMCAST\\_OIF\\_STATS structure](#) 85

[MIB\\_IPMCAST\\_SCOPE structure](#) 86

[MIB\\_IPNETROW structure](#) 87

[MIB\\_IPNETTABLE structure](#) 87

[MIB\\_IPSTATS structure](#) 88

[MIB\\_IPSTATS\\_FORWARDING enumeration](#) 40

[MIB\\_MCAST\\_LIMIT\\_ROW structure](#) ([section 2.2.1.2.16](#) 65, [section 2.2.1.2.50](#) 90)

[MIB\\_MFE\\_STATS\\_TABLE packet](#) 90

[MIB\\_MFE\\_TABLE packet](#) 91

[MIB\\_OPAQUE\\_INFO packet](#) 91

[MIB\\_OPAQUE\\_QUERY packet](#) 95

[MIB\\_PROXYARP structure](#) 102

[MIB\\_ROUTESTATE structure](#) 69

[MIB\\_TCP\\_STATE enumeration](#) 40

[MIB\\_TCPROW structure](#) 102

[MIB\\_TCPSTATS structure](#) 103

[MIB\\_TCPTABLE structure](#) 104

[MIB\\_UDPROW structure](#) 104

[MIB\\_UDPSTATS structure](#) 104

[MIB\\_UDPTABLE structure](#) 105

[MIBICMPINFO structure](#) 70

[MIBICMPSTATS structure](#) 71

[MPR\\_CREDENTIALSEX\\_1 structure](#) 142

[MPR\\_DEVICE\\_0 structure](#) 141

[MPR\\_DEVICE\\_1 structure](#) 141

[MPR\\_FILTER\\_0 structure](#) 143

[MPR\\_SERVER\\_0 structure](#) 105

[MPR\\_SERVER\\_1 structure](#) 106

[MPR\\_SERVER\\_2 structure](#) 107

[MPR\\_SERVER\\_EX\\_1 structure](#) 182

[MPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_1 structure](#) 183

[MPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_IDL structure](#) 183

[MPRAPI\\_OBJECT\\_HEADER\\_IDL structure](#) 168

[MPRAPI\\_TUNNEL\\_CONFIG\\_PARAMS\\_1 structure](#) 182

[MPRI\\_INTERFACE\\_0 structure](#) 122

[MPRI\\_INTERFACE\\_1 structure](#) 124

[MPRI\\_INTERFACE\\_2 structure](#) 125

[MPRI\\_INTERFACE\\_3 structure](#) 133

## N

[Normative references](#) 23

## O

[OSPF\\_AREA\\_PARAM structure](#) 239

[OSPF\\_AREA\\_RANGE\\_PARAM structure](#) 239

[OSPF\\_FILTER\\_ACTION enumeration](#) 42

[OSPF\\_GLOBAL\\_PARAM structure](#) 238

[OSPF\\_INTERFACE\\_PARAM structure](#) 241

[OSPF\\_NBMA\\_NEIGHBOR\\_PARAM structure](#) 242

[OSPF\\_PARAM\\_TYPE enumeration](#) 42

[OSPF\\_PROTO\\_FILTER\\_INFO structure](#) 238

[OSPF\\_ROUTE\\_FILTER structure](#) 237

[OSPF\\_ROUTE\\_FILTER\\_INFO packet](#) 237

[OSPF\\_VIRT\\_INTERFACE\\_PARAM structure](#) 240

[Overview \(synopsis\)](#) 27

## P

[P\\_NDISWAN\\_DRIVER\\_INFO](#) 247

[Parameters - security index](#) 421

[PDHCPV6R\\_GLOBAL\\_CONFIG](#) 189

[PDHCPV6R\\_IF\\_CONFIG](#) 191

[PDHCPV6R\\_IF\\_STATS](#) 190

[PDHCPV6R\\_MIB\\_GET\\_INPUT\\_DATA](#) 192

[PDHCPV6R\\_MIB\\_GET\\_OUTPUT\\_DATA](#) 189

[PDIM\\_INFORMATION\\_CONTAINER](#) 46

[PDIM\\_INTERFACE\\_CONTAINER](#) 48

[PDIM\\_MIB\\_ENTRY\\_CONTAINER](#) 66

[PFILTER\\_INFO](#) 55  
[PFILTER\\_INFO\\_V6](#) 57  
[PGLOBAL\\_INFO](#) 59  
 Phonebook  
     [entry\\_settings](#) 257  
     [file\\_format](#) 256  
[PIF\\_TABLE\\_INDEX](#) 149  
[PIFFILTER\\_INFO](#) 142  
[PIGMP\\_MIB\\_GET\\_INPUT\\_DATA](#) 203  
[PIGMP\\_MIB\\_IF\\_CONFIG](#) 206  
[PIGMP\\_MIB\\_IF\\_STATS](#) 211  
[PIKEV2\\_CONFIG\\_PARAMS\\_1](#) 179  
[PIKEV2\\_PROJECTION\\_INFO\\_1](#) 173  
[PIN6\\_ADDR](#) 59  
[PINTERFACE\\_ROUTE\\_INFO](#) 60  
[PINTERFACE\\_STATUS\\_INFO](#) 66  
[PIP\\_AUTO\\_DHCP\\_GLOBAL\\_INFO](#) 225  
[PIP\\_AUTO\\_DHCP\\_INTERFACE\\_INFO](#) 226  
[PIP\\_AUTO\\_DHCP\\_MIB\\_QUERY](#) 220  
[PIP\\_AUTO\\_DHCP\\_STATISTICS](#) 221  
[PIP\\_NAT\\_MIB\\_QUERY](#) 216  
[PIP\\_NAT\\_SESSION\\_MAPPING](#) 217  
[PIPBOOTP\\_GLOBAL\\_CONFIG](#) 184  
[PIPBOOTP\\_IF\\_BINDING](#) 188  
[PIPBOOTP\\_IF\\_CONFIG](#) 185  
[PIPBOOTP\\_IF\\_STATS](#) 187  
[PIPBOOTP\\_IP\\_ADDRESS](#) 189  
[PIPBOOTP\\_MIB\\_GET\\_INPUT\\_DATA](#) 186  
[PIPBOOTP\\_MIB\\_GET\\_OUTPUT\\_DATA](#) 187  
[PIPINIP\\_CONFIG\\_INFO](#) 65  
[PIPRIP\\_GLOBAL\\_CONFIG](#) 194  
[PIPRIP\\_GLOBAL\\_STATS](#) 194  
[PIPRIP\\_IF\\_BINDING](#) 202  
[PIPRIP\\_IF\\_STATS](#) 195  
[PIPRIP\\_IP\\_ADDRESS](#) 202  
[PIPRIP\\_MIB\\_GET\\_INPUT\\_DATA](#) 192  
[PIPRIP\\_MIB\\_GET\\_OUTPUT\\_DATA](#) 193  
[PIPRIP\\_ROUTE\\_FILTER](#) 201  
[PIPX\\_ADAPTER\\_INFO](#) 146  
[PIPX\\_GLOBAL\\_INFO](#) 143  
[PIPX\\_IF\\_INFO](#) 144  
[PIPX\\_IF\\_STATS](#) 153  
[PIPX\\_INTERFACE](#) 154  
[PIPX\\_MIB\\_GET\\_INPUT\\_DATA](#) 152  
[PIPX\\_MIB\\_INDEX](#) 151  
[PIPX\\_MIB\\_ROW](#) 158  
[PIPX\\_MIB\\_SET\\_INPUT\\_DATA](#) 158  
[PIPX\\_ROUTE](#) 157  
[PIPX\\_SERVER\\_ENTRY](#) 145  
[PIPX\\_SERVICE](#) 163  
[PIPX\\_STATIC\\_NETBIOS\\_NAME\\_INFO](#) 146  
[PIPX\\_STATIC\\_ROUTE\\_INFO](#) 144  
[PIPX\\_STATIC\\_SERVICE\\_INFO](#) 145  
[PIPX\\_TRAFFIC\\_FILTER\\_GLOBAL\\_INFO](#) 147  
[PIPX\\_TRAFFIC\\_FILTER\\_INFO](#) 147  
[PIPXMIB\\_BASE](#) 152  
[PIPXWAN\\_IF\\_INFO](#) 144  
[PL2TP\\_CONFIG\\_PARAMS\\_1](#) 180  
[PMCAST\\_HBEAT\\_INFO](#) 64  
[PMIB\\_BEST\\_IF](#) 69  
[PMIB\\_BOUNDARYROW](#) 69  
[PMIB\\_ICMP](#) 70  
[PMIB\\_IFNUMBER](#) 72  
[PMIB\\_IFSTATUS](#) 74  
[PMIB\\_IPADDRROW](#) 76  
[PMIB\\_IPDESTROW](#) 68  
[PMIB\\_IPFORWARDNUMBER](#) 77  
[PMIB\\_IPFORWARDROW](#) 77  
[PMIB\\_IPMCAST\\_BOUNDARY](#) 79  
[PMIB\\_IPMCAST\\_GLOBAL](#) 81  
[PMIB\\_IPMCAST\\_IF\\_ENTRY](#) 81  
[PMIB\\_IPMCAST\\_IF\\_TABLE](#) 81  
[PMIB\\_IPMCAST\\_MFE](#) 82  
[PMIB\\_IPMCAST\\_OIF](#) 83  
[PMIB\\_IPMCAST\\_OIF\\_STATS](#) 85  
[PMIB\\_IPMCAST\\_SCOPE](#) 86  
[PMIB\\_IPNETROW](#) 87  
[PMIB\\_IPNETTABLE](#) 87  
[PMIB\\_IPSTATS](#) 88  
[PMIB\\_MCAST\\_LIMIT\\_ROW](#) ([section 2.2.1.2.16](#) 65,  
     [section 2.2.1.2.50](#) 90)  
[PMIB\\_PROXYARP](#) 102  
[PMIB\\_ROUTESTATE](#) 69  
[PMIB\\_TCPROW](#) 102  
[PMIB\\_TCPSTATS](#) 103  
[PMIB\\_TCPTABLE](#) 104  
[PMIB\\_UDPROW](#) 104  
[PMIB\\_UDPSTATS](#) 104  
[PMIB\\_UDPTABLE](#) 105  
[PMPR\\_CREDENTIALSEX\\_1](#) 142  
[PMPR\\_DEVICE\\_0](#) 141  
[PMPR\\_DEVICE\\_1](#) 141  
[PMPR\\_FILTER\\_0](#) 143  
[PMPR\\_SERVER\\_0](#) 105  
[PMPR\\_SERVER\\_1](#) 106  
[PMPR\\_SERVER\\_2](#) 107  
[PMPR\\_SERVER\\_EX\\_1](#) 182  
[PMPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_1](#) 183  
[PMPR\\_SERVER\\_SET\\_CONFIG\\_EX\\_IDL](#) 183  
[PMPRAPI\\_OBJECT\\_HEADER\\_IDL](#) 168  
[PMPRAPI\\_TUNNEL\\_CONFIG\\_PARAMS\\_1](#) 182  
[PMPRI\\_INTERFACE\\_0](#) 122  
[PMPRI\\_INTERFACE\\_1](#) 124  
[PMPRI\\_INTERFACE\\_2](#) 125  
[PMPRI\\_INTERFACE\\_3](#) 133  
[Ports configuration example](#) 417  
[Ports object](#) 31  
[PPP\\_ATCP\\_INFO\\_structure](#) 110  
[PPP\\_CCP\\_INFO\\_structure](#) 111  
[PPP\\_INFO\\_structure](#) 115  
[PPP\\_INFO\\_2\\_structure](#) 115  
[PPP\\_INFO\\_3\\_structure](#) 116  
[PPP\\_IPCP\\_INFO\\_structure](#) 108  
[PPP\\_IPCP\\_INFO2\\_structure](#) 109  
[PPP\\_IPV6\\_CP\\_INFO\\_structure](#) 110  
[PPP\\_IPXCP\\_INFO\\_structure](#) 109  
[PPP\\_LCP\\_INFO\\_structure](#) 112  
[PPP\\_NBFCP\\_INFO\\_structure](#) 108  
[PPP\\_PROJECTION\\_INFO\\_1\\_structure](#) 169  
[PPPP\\_IPV6\\_CP\\_INFO](#) 110  
[PPPP\\_PROJECTION\\_INFO\\_1](#) 169  
[PPPTP\\_CONFIG\\_PARAMS\\_1](#) 179

[PProjection Info IDL 1](#) 174  
[PProtocol Metric](#) 63  
[PPTP Config Params 1 structure](#) 179  
[PRAS Connection Ex 1 IDL](#) 175  
[PRAS Device Info](#) 244  
[PRAS Update Connection 1 IDL](#) 184  
[PRASI Connection 0](#) 119  
[PRASI Connection 1](#) 120  
[PRASI Connection 2](#) 121  
[PRASI Connection 3](#) 122  
[PRASI Port 0](#) 116  
[PRASI Port 1](#) 118  
[Preconditions](#) 32  
[Prerequisites](#) 32  
[Priority Info packet](#) 62  
[PRIP IF Stats](#) 165  
[PRIP Interface](#) 165  
[PRIP MIB Get Input Data](#) 166  
[PRIP MIB Set Input Data](#) 166  
[PRIPMIB Base](#) 164  
[Product behavior](#) 480  
[Projection Info IDL 1 structure](#) 174  
[Protocol Metric structure](#) 63  
[PROUTING TABLE INDEX](#) 149  
[PRTR Disc Info](#) 63  
[PSAP IF Config](#) 160  
[PSAP IF Filters](#) 160  
[PSAP IF Info](#) 163  
[PSAP IF Stats](#) 161  
[PSAP Interface](#) 162  
[PSAP MIB Base](#) 161  
[PSAP MIB Get Input Data](#) 162  
[PSAP MIB Set Input Data](#) 163  
[PSAP Service Filter Info](#) 159  
[PServices Table Index](#) 150  
[PSSTP Config Params 1](#) 181  
[PStatic Routes Table Index](#) 150  
[PStatic Services Table Index](#) 151

## Q

[Querying interface status through Management Information Base \(MIB\) example](#) 406  
[Querying server configuration information example](#) 401

## R

[RAS CALLEDID Info packet](#) 247  
[RAS Connection Ex 1 IDL structure](#) 175  
[RAS Device Info structure](#) 244  
[RAS Hardware Condition enumeration](#) 37  
[RAS NDISWAN Driver Info structure](#) 247  
[RAS Port Condition enumeration](#) 37  
[RAS Quarantine State enumeration](#) 36  
[RAS Update Connection 1 IDL structure](#) 184  
[RASDEVICETYPE enumeration](#) 43  
[RASI Connection 0 structure](#) 119  
[RASI Connection 1 structure](#) 120  
[RASI Connection 2 structure](#) 121  
[RASI Connection 3 structure](#) 122  
[RASI Port 0 structure](#) 116

[RASI Port 1 structure](#) 118  
[RASMAN\\_DISCONNECT\\_TYPE enumeration](#) 45  
[RASMAN\\_INFO structure](#) 250  
[RASMAN\\_PORT\\_32 structure](#) 249  
[RASMAN\\_STATE enumeration](#) 45  
[RASMAN\\_STATUS enumeration](#) 44  
[RASMAN\\_USAGE enumeration](#) 46  
[RASRPC interface](#) 385  
[RASRPC\\_CALLBACKLIST structure](#) 254  
[RASRPC\\_LOCATIONLIST structure](#) 256  
[RASRPC\\_PBUSER structure](#) 252  
[RASRPC\\_STRINGLIST structure](#) 256  
[RasRpcDeleteEntry method](#) 387  
[RasRpcGetInstalledProtocolsEx method](#) 395  
[RasRpcGetSystemDirectory method](#) 390  
[RasRpcGetUserPreferences method](#) 388  
[RasRpcGetVersion method](#) 396  
[RasRpcSetUserPreferences method](#) 389  
[RasRpcSubmitRequest method](#) 391  
[References](#)  
     [informative](#) 26  
     [normative](#) 23  
[Registry configuration example](#) 415  
[Registry keys](#) 279  
[Relationship to other protocols](#) 32  
[ReqTypes enumeration](#) 44  
[RequestBuffer packet](#) 242  
[Retrieving device configuration information example](#) 409  
[Retrieving specific port information example](#) 410  
[Retrieving the Rasrpc server version info example](#) 408  
[RIP GLOBAL\\_INFO structure](#) 233  
[RIP IF Config structure](#) 236  
[RIP IF FILTERS structure](#) 234  
[RIP IF INFO structure](#) 235  
[RIP IF STATS structure](#) 165  
[RIP INTERFACE structure](#) 165  
[RIP MIB GET INPUT DATA structure](#) 166  
[RIP MIB SET INPUT DATA structure](#) 166  
[RIP ROUTE FILTER INFO structure](#) 234  
[RIPMIB BASE structure](#) 164  
[RMIBEntryCreate method \(\[section 3.1.4.27\]\(#\) 339, \[section 3.2.4.27\]\(#\) 383\)](#)  
[RMIBEntryDelete method \(\[section 3.1.4.28\]\(#\) 342, \[section 3.2.4.28\]\(#\) 383\)](#)  
[RMIBEntryGet method \(\[section 3.1.4.30\]\(#\) 347, \[section 3.2.4.30\]\(#\) 383\)](#)  
[RMIBEntryGetFirst method \(\[section 3.1.4.31\]\(#\) 352, \[section 3.2.4.31\]\(#\) 384\)](#)  
[RMIBEntryGetNext method \(\[section 3.1.4.32\]\(#\) 355, \[section 3.2.4.32\]\(#\) 384\)](#)  
[RMIBEntrySet method \(\[section 3.1.4.29\]\(#\) 344, \[section 3.2.4.29\]\(#\) 383\)](#)  
[RMIBGetTrapInfo method](#) 356  
[RMIBSetTrapInfo method](#) 358  
[RMprAdminServerGetInfo method \(\[section 3.1.4.1\]\(#\) 298, \[section 3.2.4.1\]\(#\) 381\)](#)  
[RMprAdminServerGetInfoEx method \(\[section 3.1.4.45\]\(#\) 372, \[section 3.2.4.42\]\(#\) 384\)](#)

[RMprAdminServerSetInfo method \(section 3.1.4.44 370, section 3.2.4.41 384\)](#)  
[RMprAdminServerSetInfoEx method \(section 3.1.4.48 375, section 3.2.4.45 385\)](#)  
[ROUTER\\_CONNECTION\\_STATE enumeration 36](#)  
[ROUTER\\_INTERFACE\\_TYPE enumeration 35](#)  
[ROUTING\\_TABLE\\_INDEX structure 149](#)  
[RPC common messages 35](#)  
[RRAS entry section name 257](#)  
[RRasAdminConnectionClearStats method \(section 3.1.4.4 302, section 3.2.4.4 381\)](#)  
[RRasAdminConnectionEnum method \(section 3.1.4.2 299, section 3.2.4.2 381\)](#)  
[RRasAdminConnectionEnumEx method \(section 3.1.4.46 373, section 3.2.4.43 385\)](#)  
[RRasAdminConnectionGetInfo method \(section 3.1.4.3 301, section 3.2.4.3 381\)](#)  
[RRasAdminConnectionGetInfoEx method \(section 3.1.4.47 374, section 3.2.4.44 385\)](#)  
[RRasAdminConnectionNotification method 359](#)  
[RRasAdminConnectionRemoveQuarantine method \(section 3.1.4.43 369, section 3.2.4.40 384\)](#)  
[RRasAdminPortClearStats method \(section 3.1.4.7 307, section 3.2.4.7 381\)](#)  
[RRasAdminPortDisconnect method \(section 3.1.4.9 308, section 3.2.4.9 382\)](#)  
[RRasAdminPortEnum method \(section 3.1.4.5 303, section 3.2.4.5 381\)](#)  
[RRasAdminPortGetInfo method \(section 3.1.4.6 305, section 3.2.4.6 381\)](#)  
[RRasAdminPortReset method \(section 3.1.4.8 307, section 3.2.4.8 382\)](#)  
[RRasAdminSendMessage method \(section 3.1.4.36 360, section 3.2.4.33 384\)](#)  
[RRasAdminUpdateConnection method \(section 3.1.4.49 376, section 3.2.4.46 385\)](#)  
[RRouterDeviceEnum method \(section 3.1.4.37 361, section 3.2.4.34 384\)](#)  
[RRouterInterfaceConnect method \(section 3.1.4.22 334, section 3.2.4.22 383\)](#)  
[RRouterInterfaceCreate method \(section 3.1.4.13 314, section 3.2.4.13 382\)](#)  
[RRouterInterfaceDelete method \(section 3.1.4.16 321, section 3.2.4.16 382\)](#)  
[RRouterInterfaceDeviceGetInfo method \(section 3.1.4.39 364, section 3.2.4.36 384\)](#)  
[RRouterInterfaceDeviceSetInfo method \(section 3.1.4.40 365, section 3.2.4.37 384\)](#)  
[RRouterInterfaceDisconnect method \(section 3.1.4.23 335, section 3.2.4.23 383\)](#)  
[RRouterInterfaceEnum method \(section 3.1.4.21 332, section 3.2.4.21 383\)](#)  
[RRouterInterfaceGetCredentialsEx method \(section 3.1.4.42 368, section 3.2.4.39 384\)](#)  
[RRouterInterfaceGetCredentialsLocal method \(section 3.1.4.51 378, section 3.2.4.48 385\)](#)  
[RRouterInterfaceGetHandle method \(section 3.1.4.12 313, section 3.2.4.12 382\)](#)  
[RRouterInterfaceGetInfo method \(section 3.1.4.14 317, section 3.2.4.14 382\)](#)

[RRouterInterfaceQueryUpdateResult method \(section 3.1.4.25 337, section 3.2.4.25 383\)](#)  
[RRouterInterfaceSetCredentialsEx method \(section 3.1.4.41 367, section 3.2.4.38 384\)](#)  
[RRouterInterfaceSetCredentialsLocal method \(section 3.1.4.50 377, section 3.2.4.47 385\)](#)  
[RRouterInterfaceSetInfo method \(section 3.1.4.15 319, section 3.2.4.15 382\)](#)  
[RRouterInterfaceTransportAdd method \(section 3.1.4.18 323, section 3.2.4.18 382\)](#)  
[RRouterInterfaceTransportCreate method \(section 3.1.4.38 362, section 3.2.4.35 384\)](#)  
[RRouterInterfaceTransportGetGlobalInfo method \(section 3.1.4.11 311, section 3.2.4.11 382\)](#)  
[RRouterInterfaceTransportGetInfo method \(section 3.1.4.19 327, section 3.2.4.19 382\)](#)  
[RRouterInterfaceTransportRemove method \(section 3.1.4.17 322, section 3.2.4.17 382\)](#)  
[RRouterInterfaceTransportSetGlobalInfo method \(section 3.1.4.10 309, section 3.2.4.10 382\)](#)  
[RRouterInterfaceTransportSetInfo method \(section 3.1.4.20 328, section 3.2.4.20 383\)](#)  
[RRouterInterfaceUpdatePhonebookInfo method \(section 3.1.4.26 338, section 3.2.4.26 383\)](#)  
[RRouterInterfaceUpdateRoutes method \(section 3.1.4.24 336, section 3.2.4.24 383\)](#)  
[RTR\\_DISC\\_INFO structure 63](#)  
[RTR\\_INFO\\_BLOCK\\_HEADER packet 49](#)  
[RTR\\_TOC\\_ENTRY packet 49](#)

## S

[Sample phonebook file for a demand-dial connection example 411](#)  
[SAP\\_GLOBAL\\_INFO structure 236](#)  
[SAP\\_IF\\_CONFIG structure 160](#)  
[SAP\\_IF\\_FILTERS structure 160](#)  
[SAP\\_IF\\_INFO structure 163](#)  
[SAP\\_IF\\_STATS structure 161](#)  
[SAP\\_INTERFACE structure 162](#)  
[SAP\\_MIB\\_BASE structure 161](#)  
[SAP\\_MIB\\_GET\\_INPUT\\_DATA structure 162](#)  
[SAP\\_MIB\\_SET\\_INPUT\\_DATA structure 163](#)  
[SAP\\_SERVICE\\_FILTER\\_INFO structure 159](#)  
 Security  
     implementer considerations  
         [overview 421](#)  
         [RRAS Management Protocol-specific 421](#)  
         [parameter index 421](#)  
 Sequencing rules  
     client  
         [DIMSVSVC interface 381](#)  
         [RASRPC interface 398](#)  
     server  
         [DIMSVSVC interface 295](#)  
         [RASRPC interface 386](#)  
 Server  
     abstract data model  
         [DIMSVSVC interface 294](#)  
         [RASRPC interface 385](#)  
         [DIMSVSVC interface 294](#)  
     initialization

- [DIMSVC interface](#) 295
- [RASRPC interface](#) 386
- local events
  - [DIMSVC interface](#) 379
  - [RASRPC interface](#) 397
- message processing
  - [DIMSVC interface](#) 295
  - [RASRPC interface](#) 386
- overview
  - [DIMSVC interface](#) 294
  - [RASRPC interface](#) 385
- [RASRPC interface](#) 385
- security settings
  - [dimsvc](#) 34
  - [Rasrpc](#) 34
- sequencing rules
  - [DIMSVC interface](#) 295
  - [RASRPC interface](#) 386
- timer events
  - [DIMSVC interface](#) 379
  - [RASRPC interface](#) 397
- timers
  - [DIMSVC interface](#) 295
  - [RASRPC interface](#) 386
- [SERVICES\\_TABLE\\_INDEX structure](#) 150
- [SSTP\\_CERT\\_INFO\\_1 packet](#) 180
- [SSTP\\_CONFIG\\_PARAMS\\_1 structure](#) 181
- [Standards assignments](#) 33
- [STATIC\\_ROUTES\\_TABLE\\_INDEX structure](#) 150
- [STATIC\\_SERVICES\\_TABLE\\_INDEX structure](#) 151
- [Structures](#) 46

## T

- [TCP\\_RTO\\_ALGORITHM enumeration](#) 41
- Timer events
  - client
    - [DIMSVC interface](#) 385
    - [RASRPC interface](#) 400
  - server
    - [RASRPC interface](#) 397
- Timer events - server
  - [DIMSVC interface](#) 379
- Timers
  - client
    - [DIMSVC interface](#) 380
    - [RASRPC interface](#) 398
  - server
    - [DIMSVC interface](#) 295
    - [RASRPC interface](#) 386
- [Tracking changes](#) 497
- Transport
  - [overview](#) 34
  - security settings
    - client
      - [dimsvc](#) 34
      - [Rasrpc](#) 35
    - server
      - [dimsvc](#) 34
      - [Rasrpc](#) 34
- [Transport configuration example](#) 415
- [Transport object](#) 30

## U

- [Updating connection endpoint of IKEv2-based connection example](#) 407

## V

- [Vendor-extensible fields](#) 33
- [Versioning](#) 33