Windows 2000 Server

Chapter 4 - IP Multicast Support

Microsoft® Windows® 2000 provides support for the sending, receiving, and forwarding of IP multicast traffic. The IP multicast components of the Routing and Remote Access service allow you to send and receive IP multicast traffic from remote access clients and multicast-enabled portions of the Internet or a private intranet.

In This Chapter

Related Information in the Resource Kit

- For more information about IP multicast basics, see "Introduction to TCP/IP" in the Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide.
- For more information about IP multicast support in TCP/IP for Windows 2000, see "Windows 2000 TCP/IP" in the Windows 2000 TCP/IP Core Networking Guide.
- For more information about remote access, see "Remote Access Server" in this book.
- For more information about the Windows 2000-based routers, see "Routing and Remote Access Service" in this book.

IP Multicasting Overview

In addition to unicast and broadcast support, IP also provides a mechanism to send and receive IP multicast traffic. IP multicast traffic is sent to a single destination IP address but is received and processed by multiple IP hosts, regardless of their location on an IP internetwork. A host listens for a specific IP multicast address and receives all packets to that IP address.

IP multicast is more efficient than IP unicast or broadcast for one-to-many delivery of data. Unlike unicast, only one copy of the data is sent. Unlike broadcast, the traffic is only received and processed by computers that are listening for it.

The additional elements of IP multicast include the following:

- The set of hosts listening on a specific IP multicast address is called a host group.
- Host group membership is dynamic, and hosts can join and leave the group at any time.
- There are no limitations to the size of a host group.
- A host group can span IP routers across multiple network segments. This configuration requires IP multicast support on IP routers and the ability for hosts to register themselves with the router. Host registration is accomplished using the Internet Group Management Protocol (IGMP).
- A host can send traffic to an IP multicast address without belonging to the corresponding host group.

IP multicast addresses, also known as group addresses, are in the class D range of 224.0.0.0 to 239.255.255.255 as defined by setting the first four high order bits to 1110. In network prefix or Classless Inter-Domain Routing (CIDR) notation, IP multicast addresses are summarized as 224.0.0.0/4. Multicast addresses in the range 224.0.0.0 to 224.0.0.255 (224.0.0.0/24) are reserved for the local subnet and are not forwarded by IP routers regardless of the Time to Live (TTL) in the IP header.

The IP multicast addresses from 224.0.1.0 to 238.255.255.255 are either reserved or assigned to a multicasting application. The addresses from 239.0.0.0 to 239.255.255.255 (239.0.0.0/8) are reserved for applications that can be administratively scoped. For more information about these addresses, see "Multicast Boundaries" later in this chapter.

The following are examples of reserved IP multicast addresses:

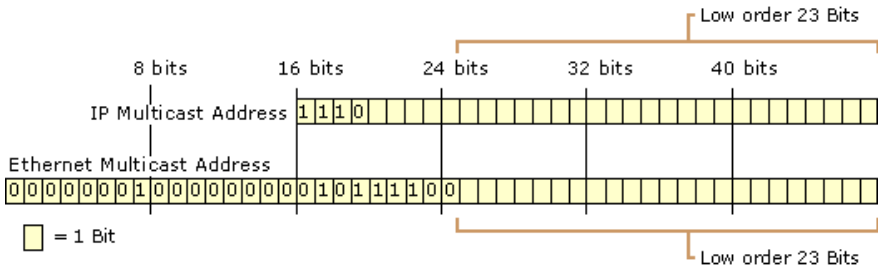
- 224.0.0.1 - all hosts on this subnet.
- 224.0.0.2 - all routers on this subnet.
- 224.0.0.5 - Open Shortest Path First (OSPF) Version 2, designed to reach all OSPF routers on a network.
- 224.0.0.6 - OSPF Version 2, designed to reach all OSPF designated routers on a network.
- 224.0.0.9 - Routing Information Protocol (RIP) Version 2.
- 224.0.1.1 - Network Time Protocol.

For the latest list of reserved multicast addresses, see the Information Sciences Institute link at http://windows.microsoft.com/windows2000/reskit/webresources.

For more information about IP multicast support, see Internet Engineering Task Force (IETF) Request for Comments (RFC) 1112.

Mapping IP Multicast to MAC-Layer Multicast

To support IP multicasting, the Internet authorities have reserved the multicast address range of 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF for Ethernet and Fiber Distributed Data Interface (FDDI) media access control (MAC) addresses. As shown in Figure 4.1, the high order 25 bits of the 48-bit MAC address are fixed and the low order 23 bits are variable.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.1 Mapping IP Multicast Addresses to Ethernet and FDDI MAC Addresses

To map an IP multicast address to a MAC-layer multicast address, the low order 23 bits of the IP multicast address are mapped directly to the low order 23 bits in the MAC-layer multicast address. Because the first 4 bits of an IP multicast address are fixed according to the class D convention, there are 5 bits in the IP multicast address that do not map to the MAC-layer multicast address. Therefore, it is possible for a host to receive MAC-layer multicast packets for groups to which it does not belong. However, these packets are dropped by IP once the destination IP address is determined.

For example, the multicast address 224.192.16.1 becomes 01-00-5E-40-10-01. To use the 23 low order bits, the first octet is not used, and only the last 7 bits of the second octet is used. The third and fourth octets are converted directly to hexadecimal numbers. The second octet, 192 in binary is 11000000. If you drop the high order bit, it becomes 1000000 or 64 (in decimal), or 0x40 (in hexadecimal). For the next octet, 16 in hexadecimal is 0x10. For the last octet, 1 in hexadecimal is 0x01. Therefore, the MAC address corresponding to 224.192.16.1 becomes 01-00-5E-40-10-01.

Token Ring uses this same method for MAC-layer multicast addressing. However, many Token Ring network adapters do not support it. Therefore, by default, the functional address 0xC0-00-00-04-00-00 is used for all IP multicast traffic sent over Token Ring networks. For more information about Token Ring support for IP multicasting, see RFC 1469.

Note Microsoft® Windows NT® version 4.0 and earlier do not support IP multicast on Token Ring network adapters.

IP Multicast-Enabled Intranet

In an IP multicast-enabled intranet, any host can send IP multicast traffic to any group address, and any host can receive IP multicast traffic from any group address regardless of their location. To facilitate this capability, IP multicast must be supported by the hosts and routers of the intranet.

Hosts

A host supports IP multicast at one of the following levels:

- Level 0 - No support to send or receive IP multicast traffic.
- Level 1 - Support exists to send but not receive IP multicast traffic.
- Level 2 - Support exists to both send and receive IP multicast traffic.

TCP/IP for Windows 2000 supports all levels of IP multicasting and by default is configured for level 2 support for IP multicast traffic. For information about changing the level of multicast support, see "Windows 2000 TCP/IP" in the TCP/IP Core Networking Guide.

For a host to send IP multicast packets, it must:

- Determine the IP multicast address to use.

  To determine the IP multicast address to use, the application must first determine whether to create a new host group or use an existing host group. To join an existing group, the application can use a service location protocol to determine the group address for a specific service.

  The multicast address for a new group can either be determined by the application or obtained through a mechanism that allocates a unique multicast address such as Multicast Address Dynamic Client Allocation Protocol (MADCAP). MADCAP is an extension to the Dynamic Host Configuration Protocol (DHCP) protocol standard that you can use to support dynamic assignment and configuration of IP multicast addresses on TCP/IP-based networks.

  Ordinarily, you use DHCP scopes to provide client configurations by allocating ranges of unicast IP addresses. MADCAP scopes can be used to allocate ranges of IP multicast addresses. For more information about MADCAP and its support in Windows 2000, see "Dynamic Host Configuration Protocol" in the TCP/IP Core Networking Guide.

- Place the IP multicast packet on the medium.

  The sending host must construct an IP packet containing the wanted destination IP multicast address and place it on the medium. In the case of shared access technologies such as Ethernet, FDDI, and Token Ring, the destination MAC address is created from the IP multicast address as previously described.

For a host to receive IP multicast packets, it must:

- Inform IP to receive multicast traffic.

  To determine the IP multicast address to use, the application must first determine whether to create a new host group or use an existing host group. To join an existing group, the application can use a service location protocol to determine the group address for a specific service.

  After the group address is determined, an application must inform IP to receive multicasts at a specified destination IP multicast address. If multiple applications are using the same IP multicast address, then IP must pass a copy of the multicast to each application. IP must track which applications are using which multicast addresses as applications join or leave a host group. Additionally, for a multihomed host, IP must track the application membership of host groups for each subnet.

- Register the multicast MAC address with the network adapter.

  If the network technology supports hardware-based multicasting, then the network adapter is told to pass up packets for a specific multicast address. In the case of shared access technologies such as Ethernet, FDDI, and Token Ring, the NdisRequest function is used to program the network adapter to respond to a multicast MAC address corresponding to the wanted IP multicast address.

- Inform local routers.

  The host must inform local subnet routers that it is listening for multicast traffic at a specific group address. The protocol that registers host group information is the Internet Group Management Protocol (IGMP).

  IGMP is required on all hosts that support level 2 IP multicasting. The IGMP Host Membership Report message is sent by a host to register membership in a specific host group. TCP/IP for Windows 2000 supports IGMP version 2. For more information about IGMP, see "IGMP v1" and "IGMP v2" later in this chapter.

Routers

To forward IP multicast packets to only those subnets for which there are group members, an IP multicast router must be able to:

- Receive all IP multicast traffic.
- Forward IP multicast traffic.
- Receive and process IGMP Host Membership Report messages.
- Query attached subnets for host membership status.
- Communicate group membership to other IP multicast routers.

Receive All IP Multicast Traffic

For shared access technologies, such as Ethernet and FDDI, the normal listening mode for network adapters is unicast listening mode. The listening mode is the way that the network adapter analyzes the destination MAC address of incoming frames to decide to process

them further. In unicast listening mode, the only frames that are considered for further processing are in a table of interesting destination MAC addresses on the network adapter. Typically, the only interesting addresses are the broadcast address (0xFF-FF-FF-FF-FF-FF) and the unicast address, also known as the media access control (MAC) address, of the adapter.

However, for an IP multicast router to receive all IP multicast traffic, it must place the network adapter in a special listening mode called multicast promiscuous mode. Multicast promiscuous mode analyzes the Institute of Electrical and Electronics Engineers (IEEE)-defined multicast bit to determine whether the frame requires further processing. The multicast bit for Ethernet and FDDI addresses is the last bit of the first byte of the destination MAC address.

The values of the multicast bit are the following:

- If the multicast bit is set to 0, then the address is a unicast or individual address.
- If the multicast bit is set to 1, then the address is a multicast or group address. The multicast bit is also set for the broadcast address.

When the network adapter is placed in multicast promiscuous listening mode, any frames with the multicast bit set to 1 are passed up for further processing.

Multicast promiscuous mode is different than promiscuous mode. In promiscuous mode, all frames-regardless of the destination MAC address-are passed up for processing. Promiscuous mode is used by protocol analyzers, also known as network sniffers, such as the full version of Microsoft Network Monitor that is part of the Microsoft® Systems Management Server.

Multicast promiscuous mode is supported by most network adapters. A network adapter that supports promiscuous mode might not support multicast promiscuous mode. Consult your network adapter documentation or manufacturer for information about whether your network adapter supports multicast promiscuous mode.

Forward IP Multicast Traffic

The ability to forward IP multicast packets is a capability of the TCP/IP protocol, and the Windows 2000 implementation of TCP/IP includes this functionality. When multicast forwarding is enabled, non-local subnet IP multicast packets are analyzed to determine over which interfaces the packet is forwarded. The analysis is done by comparing the destination group address to entries in the IP multicast forwarding table. Upon receipt of a non-local IP multicast packet, the Time to Live (TTL) in the IP header is decremented by 1. If the TTL is greater than 0 after decrementing, then the multicast forwarding table is checked. If an entry in the multicast forwarding table is found that matches the destination IP multicast address, the IP multicast packet is forwarded with its new TTL over the appropriate interfaces.

The multicast forwarding process does not distinguish between hosts on locally attached subnets who are receiving multicast traffic or hosts on a network segment that are downstream from the locally attached subnet across another router on the subnet. In other words, a multicast router might forward a multicast packet on a subnet for which there are no hosts listening. The multicast packet is forwarded because another router on that subnet indicated that a host in its direction is receiving the multicast traffic.

The multicast forwarding table does not record each host group member or the number of host group members; only that there is at least one host group member for a specific group address.

For information about how to view the IP multicast forwarding table on a Microsoft® Windows® 2000 Server-based computer running the Routing and Remote Access service, see "IP Multicast Troubleshooting Tools" later in this chapter.

Multicast forwarding is enabled by setting the value of the EnableMulticastForwarding registry entry (HKEY_LOCAL_MACHINE \System \CurrentControlSet \Services \Tcpip) \Parameters to 1. This registry entry is created and set to 1 when you install the Routing and Remote Access service.

Caution Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

Receive and Process IGMP Host Membership Report Messages

Multicast routers receive IGMP Host Membership Report messages from all hosts on all locally attached subnets. This information is used to track host group membership by placing entries in the multicast forwarding table. Because all multicast routers are listening in multicast promiscuous mode, they receive all IGMP Host Membership Report messages sent to any group address.

For the Windows 2000 Routing and Remote Access service, this functionality is provided by adding the IGMP routing protocol and enabling IGMP router mode on an interface. For more information, see "IGMP Protocol" later in this chapter.

Query Attached Subnets for Host Membership Status

On a specific subnet, there can be a mixture of IGMP v1 hosts and IGMP v2 hosts. When an IGMP v1 host stops receiving IP multicast traffic for a specific group address (the host leaves the group), it does not send a specific message to inform the local routers. Consequently, the host can leave the group; if it is the last member on the subnet, then the local routers continue to forward multicast traffic for that group to the subnet.

To improve the leave latency, the time between when the last host on a subnet has left the group and when no more multicast traffic for that group is forwarded to that subnet, multicast routers periodically send IGMP Host Membership Query messages to the local subnet for host membership information. A host that is still a member of a multicast group responds to the query with an IGMP Host Membership Report message. To keep multiple hosts on a particular subnet from sending IGMP Host Membership Report messages for the same group, a random response is used on the hosts to delay the transmission of the IGMP Host Membership Report message. If the message is sent by another host on that subnet before the response timer expires, a message is not sent.

To further improve leave latency, an IGMP v2 host that is the last host of a group on a subnet sends an IGMP Leave Group message. After sending group-specific queries to the group being left and receiving no response, the IGMP v2 router can determine that there are no more group members on that subnet.

Communicate Group Membership to Other IP Multicast Routers

To create multicast-enabled IP internetworks containing more than one router, multicast routers must communicate group membership information to each other so group members can receive IP multicast traffic regardless of their location on the IP internetwork.

Multicast routers exchange host membership information using a multicast routing protocol such as Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), or Protocol Independent Multicast (PIM). Group membership is either communicated explicitly, by exchanging group address and subnet information, or implicitly, by informing upstream routers whether or not group members exist downstream from the source of the multicast traffic.

The goals of a multicast routing protocol include the following:

- Forward traffic away from the source to prevent loops.
- Minimize or eliminate multicast traffic to subnets that do not need the traffic.

- Minimize CPU and memory load on the router for scalability.
- Minimize the overhead of the routing protocol.
- Minimize the join latency, the time it takes for the first host member on a subnet to begin receiving group traffic.

Multicast routing is more complex than unicast routing. With unicast routing, unicast traffic is forwarded to a globally unique destination. Unicast routes summarize ranges of globally unique destinations. Unicast routes in the network are comparatively consistent and only need to be updated when the topology of the IP internetwork changes.

With multicast routing, multicast traffic is forwarded to an ambiguous group destination. Group addresses represent individual groups, and in general, cannot be summarized in the multicast forwarding table. The location of group members is not consistent, and the multicast forwarding tables of multicast routers might need to be updated whenever a host group member joins or leaves a host group.

Just as unicast routing protocols update the unicast IP routing table, multicast routing protocols update the IP multicast forwarding table. The Windows 2000 Routing and Remote Access service does not include any multicast routing protocols, although it provides a platform on which third-party protocols can run. The only component provided with Windows 2000 that can update entries in the multicast forwarding table is IGMP.

MBone

The Internet Multicast Backbone, or MBone, is the portion of the Internet that supports multicast routing and forwarding of Internet-based IP multicast traffic. The MBone structure consists of a series of multicast-enabled islands, collections of contiguous networks, connected together using tunnels. Multicast traffic is passed from one island to another by tunneling: encapsulating the IP multicast packet with an additional IP header addressed from one router in a multicast island to another router in another multicast island. Tunneling allows the multicast traffic to travel across portions of the Internet that do not support multicast forwarding.

The MBone is used for audio and video multicasts of Internet Engineering Task Force (IETF) meetings, the National Aeronautics and Space Administration, and the United States House of Representatives and Senate, among others. Support for the MBone might vary among Internet service providers (ISPs).

IGMP

Internet Group Management Protocol (IGMP) is used between hosts and their local multicast router. IGMP messages are encapsulated by IP and use the IP protocol number 0x02.

There are two versions of IGMP:

- IGMP version 1 is supported by TCP/IP for Windows NT version 4.0 Service Pack 3 and earlier and Microsoft® Windows® 95.
- IGMP version 2 is supported by TCP/IP for Microsoft Windows NT 4.0 Service Pack 4 and later, Microsoft® Windows® 98, and Windows 2000.

IGMP version 2 is backward compatible with IGMP version 1. The differences between the two versions are discussed in the following sections.

Note IGMP is only used to maintain host group membership on a local subnet. IP multicast traffic is not sent using an IGMP header. Typical IP multicast traffic uses a User Datagram Protocol (UDP) header.

IGMP v1

IGMP version 1 is a simple protocol consisting of two messages. The structure of IGMP version 1 messages is shown in Figure 4.2.

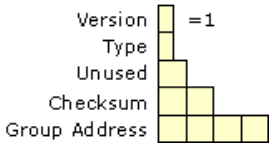


Figure 4.2 IGMP Version 1 Message Structure

Version A 4-bit field set to the value of 0x1 for IGMP v1.

Type A 4-bit field containing either 0x1 or 0x2. 0x1 indicates a Host Membership Query sent by an IP multicast router to query a subnet for current host membership. 0x2 indicates a Host Membership Report sent by IP multicast hosts when joining a group or in response to a Host Membership Query.

Unused An unused 1-byte field set to the value of 0x00 by the sender and whose value is ignored by the receiver.

Checksum A 2-byte field set to the value of the 16-bit checksum calculation on the IGMP message. The IGMP checksum does not include the IP header.

Group Address A 4-byte field set to either 0.0.0.0 for a Host Membership Query, or the specific group address for a Host Membership Report.

Host Membership Report

When a host joins a multicast group, it sends an IGMP Host Membership Report message to the specific group address, regardless of whether there are already other hosts on its subnet that are host group members. Unlike a multicast router, a host does not keep track of the host group membership of other hosts on its subnet. Because a multicast router is listening in multicast promiscuous mode, it receives and processes IGMP Host Membership Report messages sent to any multicast address.

For a Windows 2000 Routing and Remote Access service configured with the IGMP routing protocol and an interface running in IGMP router mode, if this is the first host to join a host group on a particular subnet, the IGMP routing protocol creates an entry in the interface group table. If needed, an entry in the IP multicast forwarding table is created, containing the group address being registered and the interface on which the IGMP Host Membership Report message was received.

Host Membership Query

An IGMP v1 multicast router periodically sends an IGMP Host Membership Query message to 224.0.0.1 (the all hosts group) to refresh its knowledge of host members on the subnet. For each host group for which there are members on the subnet, one host group member responds with an IGMP Host Membership Report message. As previously discussed, a random response timer is used to stagger and randomly distribute the individual host group member who sends the IGMP Host Membership Report message for each group.

Upon receiving a response from a host group, the Windows 2000 Routing and Remote Access service updates the IGMP interface group table with a new expiry time, and the existing entry for the host group remains in the IP multicast forwarding table. If no hosts respond to the query for the host group and the expiry time for the entry in the IGMP interface group table becomes 0, then IGMP removes the host group entry from the multicast forwarding table.

Table 4.1 summarizes the values of the source and destination IP addresses and the TTL in the IP header and the value of the Group Address in the IGMP header for the two different types of IGMP v1 messages.

Table 4.1 Addresses and TTLs Used for IGMP v1 Messages

Address	IGMP Host Membership Query	IGMP Host Membership Report
Source IP Address	[Router interface IP address]	[Host interface IP address]
Destination IP Address	224.0.0.1	[Group address]
TTL	1	1
Group Address	0.0.0.0	[Group address]

For more information, see Appendix I of RFC 1112.

IGMP v2

IGMP version 2 extends the functionality of IGMP while maintaining backward compatibility with IGMP v1.

With IGMP v1, the router that sends the periodic queries is elected by the multicast routing protocols. IGMP v2 uses a simple election process to choose the multicast querier, the single router on each subnet that sends the periodic IGMP Host Membership Query messages. The router with the numerically lowest IP address is elected the multicast querier. The election process consists of listening for IGMP queries from other routers. If a query is received with a lower source IP address, the listening router remains a non-querier. If no query is received from other routers, the listening router becomes a querier.

IGMP v2 adds two new message types, an IGMP v2 Host Membership Report and a Leave Group message. It also adds a variation on the Host Membership Query called the Group-Specific Host Membership Query. The details of these new message types are discussed in the following sections.

The structure of IGMP version 2 messages is shown in Figure 4.3.

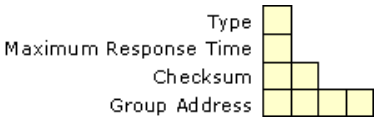


Figure 4.3 IGMP Version 2 Message Structure

Type Specifies the type of IGMP packet. IGMP v2 combines the two 4-bit IGMP v1 Version and Type fields into a single 8-bit Type field.

Table 4.2 lists the defined IGMP v2 message types.

Table 4.2 IGMP v2 Message Types

Hexadecimal Value	Decimal value	Message Type and Description
0x11 (The IGMP v1 Version field of 0x1 and IGMP v1 Type field 0x1 become the IGMP v2 Type field of 0x11.)	17	Host Membership Query For a general query, the Group Address field is set to 0.0.0.0. For a group-specific query, the Group Address field is set to the host group address.
0x12 (The IGMP v1 Version field of 0x1 and IGMP v1 Type field 0x2 become the IGMP v2 Type field of 0x12.)	18	Host Membership Report The Group Address field is set to the host group.
0x16	22	Version 2 Host Membership Report The Group Address field is set to the host group.
0x17	23	Leave Group The Group Address field is set to the host group.

Maximum Response Time A 1-byte field that specifies the maximum time allowed in 1/10's of a second before sending a Host Membership Report after receiving a Host Membership Query. The Maximum Response Time field is only used in general or group-specific query messages. The Maximum Response Time is configured as the value for the Query response interval setting from:

- The Router tab on the properties of an IGMP interface in the Routing and Remote Access snap-in.
- The netsh routing ip igmp set interface command.

Checksum A 2-byte field set to the value of the 16-bit checksum calculation on the IGMP message. The IGMP checksum does not include the IP header.

Group Address A 4-byte field set to either 0.0.0.0 for a general Host Membership Query message or the specific group address for the Host Membership Report, Leave Group, and group-specific Host Membership Query messages.

IGMP v2 Host Membership Report

The IGMP v2 Host Membership Report has the same function as the IGMP v1 Host Membership Report except that it is intended to be received by IGMP v2 routers.

Leave Group Message

The Leave Group message is used to reduce the time it takes for the multicast router to stop forwarding multicast traffic when there are no longer any members in the host group. If a host responds to the last IGMP query, it might be the last or only member of the host group. When this host leaves the group it sends an IGMP Leave Group message to 224.0.0.2 (the all routers group). Upon receipt of the Leave Group message, the router sends a series of group-specific queries for the host group. If no host responds to the group-specific queries, the router determines that there are no more members of that host group on that particular subnet and removes the entry from the IGMP interface group table.

IGMP Group-Specific Query

An IGMP Host Membership Query is sent to 224.0.0.1 (the all hosts group) to query for the group membership of all hosts on the subnet. IGMP v2 routers can also send a group-specific query, a query for a specific multicast group sent to the group address.

Table 4.3 summarizes the values of the source and destination IP addresses and the TTL in the IP header and the value of the Group Address in the IGMP header for the two additional types of IGMP v2 messages.

Table 4.3 Addresses and TTLs Used for IGMP v2 Messages

Address	IGMP Group-Specific Query	IGMP Leave Group Message
Source IP Address	[Router interface IP address]	[Host interface IP address]
Destination IP Address	[Host group being queried]	224.0.0.2
TTL	1	1
Group Address	[Host group being queried]	[Host group being left]

For more information, see RFC 2236.

Routing and Remote Access Service IP Multicast Support

IP multicast support provided by the Windows 2000 Routing and Remote Access service consists of the following elements:

- The IGMP protocol
- Multicast boundaries
- Multicast heartbeat
- IP-in-IP tunnels
- Multicast static routes

IGMP Protocol

Because there are no multicast routing protocols provided with Windows 2000, the maintenance of entries in the IP multicast forwarding table is a function of IGMP, a component that is added as an IP routing protocol. After the IGMP routing protocol is added, router interfaces are added to IGMP. Each interface added to the IGMP routing protocol can be configured in one of two operating modes: IGMP router mode and IGMP proxy mode. The operating modes are discussed in more detail in the following sections.

While the IGMP protocol provides some limited ability to create or extend multicast-enabled IP internetworks, it is not the equivalent of a multicast routing protocol, such as DVMRP or PIM. Do not use the Windows 2000 IGMP routing protocol to create a multicast-enabled IP internetwork of an arbitrary size or topology. For more information about how Windows 2000 routers with the IGMP routing protocol component can be used, see "Supported Multicast Configurations" later in this chapter.

IGMP Router Mode

When an IGMP routing protocol interface is configured in IGMP router mode, it performs the following functions:

- Listens in multicast promiscuous mode.

  The IGMP router mode interface is enabled for multicast promiscuous mode. If multicast promiscuous mode is not supported by the network adapter, then IP Router Manager event number 20157 is logged.
- Listens for IGMP Host Membership Report messages and Leave Group messages.

  The IGMP router mode interface listens for IGMP Host Membership Report messages and Leave Group messages sent by hosts on the subnet.
- Sends IGMP Host Membership Queries.

  The IGMP router mode interface sends periodic general queries and group-specific queries after receiving a Leave Group message.
- Elects an IGMP querier.

  As an IGMP multicast router, the IGMP router mode interface elects an IGMP querier for the subnet.
- Maintains entries in IP multicast forwarding table.

  Based on the current group membership for hosts on the subnet, IGMP maintains the appropriate entries in the IP multicast forwarding table.

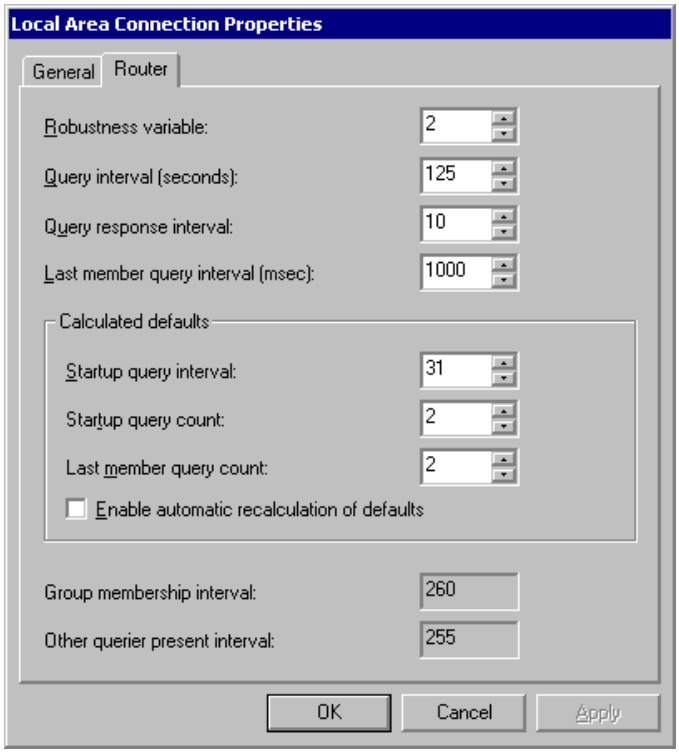
IGMP router mode can be enabled on multiple interfaces. For each interface, either version of IGMP can be configured. The default version is IGMP v2.

IGMP Router Mode Settings

The operation of IGMP v2 running in IGMP router mode is configurable for each interface. You can modify the operation of IGMP router mode using:

- The Router tab on the properties of an IGMP interface in the Routing and Remote Access snap-in.
- The netsh routing ip igmp set interface command.

Figure 4.4 shows the IGMP router mode settings for the Local Area Connection interface in the Routing and Remote Access snap-in.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.4 IGMP v2 Router Properties

Robustness Variable The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.

Query Interval The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). You can also click the scroll arrows to select a new setting. The default query interval is 125 seconds.

Query Response Interval 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. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. You can also click the scroll arrows to select a new setting. The default query response interval is 10 seconds and must be less than the query interval.

Last Member Query Interval The last member query interval is the amount of time in seconds 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. You can also click the scroll arrows to select a new setting. The default last member query interval is 1 second.

Calculated Defaults IGMP variables can be manually configured or automatically calculated based on the values of the robustness variable and the query interval. For automatic calculation, select the Enable automatic recalculation of defaults check box.

Startup Query Interval The startup query interval is the amount of time in seconds between successive General Query messages sent by a querier during startup. You can also click the scroll arrows to select a new setting. The default startup query interval is one-fourth of the value for the query interval.

Startup Query Count The startup query count is the number of general query messages sent at startup. You can also click the scroll arrows to select a new setting. The default startup query count is 2.

Last Member Query Count The last member query count is the number of Group-Specific Query messages sent before the router assumes that there are no members of the host group being queried on this interface. You can also click the scroll arrows to select a new setting. The default last member query count is 2.

Enable Automatic Recalculation of Defaults Specifies whether the values in startup query interval, startup query count, and last member query count are calculated automatically based on the following:

- The startup query interval is one-fourth of the value for the query interval.
- The startup query count is the same value as the robustness variable.
- The last member query count is the same value as the robustness variable.

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 calculated as the (robustness variable) * (query interval) + (query response interval). The group membership interval is a calculated value and is not configurable.

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 takes precedence as the querier. The other querier present interval is the robustness variable multiplied by the query interval plus the query response interval divided by two. The other querier present interval is a calculated value and is not configurable.

Note For more information about these settings and their relationship to each other, see RFC 2236.

IGMP Proxy Mode

While the purpose of IGMP router mode is to act as a multicast router, the purpose of IGMP proxy mode is to act as a multicast proxy for hosts on interfaces on which IGMP router mode is enabled. When an IGMP routing protocol interface is configured in IGMP router mode, it performs the following functions:

- Forwards IGMP Host Membership Reports

All IGMP Host Membership Reports received on IGMP router mode interfaces are retransmitted on the IGMP proxy mode interface.

- Registers multicast MAC addresses

  For shared access technologies such as Ethernet, the network adapter is left in unicast listening mode. For each unique group registered by IGMP Host Membership Reports forwarded on the IGMP proxy mode interface, the network adapter is programmed to pass up frames with the corresponding multicast MAC address. Each additional multicast MAC address is an entry in the table of interesting destination MAC addresses on the network adapter. Each network adapter has a maximum number of entries it can store. If the maximum number of entries is used, then the IGMP routing protocol enables multicast promiscuous listening mode on the network adapter.

- Adds entries to the multicast forwarding table

  When non-local multicast traffic is received on an IGMP router mode interface, the IGMP routing protocol adds or updates an entry to the multicast forwarding table to forward the multicast traffic out the IGMP proxy mode interface. The end result of this process is that any non-local multicast traffic received on IGMP router mode interfaces is flooded, or copied, to the IGMP proxy mode interface.

- Receives multicast traffic received on IGMP proxy mode interfaces

  Multicast traffic received on the IGMP proxy mode interface corresponding to the groups registered by hosts on IGMP router mode interfaces are forwarded to the appropriate interfaces using the IP protocol and the multicast forwarding table.

The purpose of IGMP proxy mode is to connect a Windows 2000 router to a multicast-enabled IP internetwork, such as the MBone, or a private intranet that is using multicast routing protocols, such as DVMRP and PIM. The IGMP proxy mode interface acts like a host and joins host groups on behalf of hosts on its IGMP router mode interfaces. Multicast traffic sent to host members on IGMP router mode interfaces are received on the IGMP proxy mode interface and forwarded by the IP multicast forwarding process. Multicast traffic sent by hosts on IGMP router mode interfaces are flooded on the IGMP proxy mode interface where a downstream IP multicast-enabled router can either forward the traffic or ignore it.

IGMP proxy mode can only be enabled on a single IGMP routing protocol interface. The correct interface on which to enable IGMP proxy mode is the interface attached to a subnet containing a multicast router running multicast routing protocols. In other words, the IGMP proxy mode interface "points" to the multicast-enabled intranet.

Router Mode vs. Proxy Mode

Table 4.4 summarizes the features and behavior of IGMP router mode and IGMP proxy mode.

Table 4.4 IGMP Router Mode and IGMP Proxy Mode

Behavior	IGMP Router Mode	IGMP Proxy Mode
Listening mode	Multicast promiscuous mode.	Unicast listening mode.
IGMP router or host	Acts as an IGMP-based multicast router and listens for IGMP Host Membership Report messages.	Acts as an IGMP-based host by forwarding IGMP Host Membership Reports and responding to IGMP queries. Listens for IGMP Host Membership Report messages as a host, not as a router.
Updating of IP multicast forwarding table	Updates the IP multicast forwarding table based on IGMP traffic.	Updates the IP multicast forwarding table to flood non-local multicast traffic received on IGMP router mode interfaces.
Sends IGMP queries	Sends IGMP queries to maintain a current forwarding table.	Sends no IGMP queries.

Multicast Boundaries

Multicast boundaries are configurable administrative barriers that limit the extent of the IP internetwork over which multicast traffic can be forwarded. Without boundaries, an IP multicast router forwards all appropriate IP multicast traffic. With a Windows 2000-based router, you can define multicast boundaries by a range of IP addresses known as a multicast scope, by the value of the TTL field in the IP header, or by the rate of multicast traffic.

Multicast boundaries are configured per interface from the Multicast Boundaries tab from the properties of an interface in the General node under IP Routing in the Routing and Remote Access snap-in.

Scope-Based Boundaries

The 239.0.0.0/8 range of IP multicast addresses is defined as the administratively scoped IP multicast address space. Multicast addresses in this range can be prevented from propagating in either direction (send or receive) through the use of scope-based boundaries. A scope-based boundary defines the edge or boundary beyond which a multicast packet for a specified range is not forwarded.

To configure a scope (a range of IP multicast addresses) for address-based boundaries, you must first add the scope from:

- The Multicast Scopes tab of the properties of the General node under IP Routing in the Routing and Remote Access snap-in.
- The netsh routing ip set scope command.

You must enter the address range corresponding to the scope as an IP address and mask. However, the Local Scope of 239.255.0.0/16 is excluded. Therefore, configured scopes must be in the range of 239.0.0.0 to 239.254.255.255. For a range of IP multicast addresses, determine the appropriate IP address and mask that define the range. For a single group address, the IP address is the group address being scoped and the mask is 255.255.255.255.

Once the scopes are created, scope-based boundaries are configured per interface.

For more information about administrative scoping for IP multicast traffic, see RFC 2356.

TTL-Based Boundaries

TTL-based boundaries prevent the forwarding of IP multicast traffic with a TTL less than a specified value. TTL-based boundaries apply to all multicast packets regardless of the multicast group. Typically used TTL thresholds are listed in Table 4.5.

Table 4.5 TTL Thresholds and Their Scope

TTL Threshold	Scope
0	Restricted to the same host.
1	Restricted to the same subnet.
15	Restricted to the same site.

63	Restricted to the same region.
127	Worldwide.
191	Worldwide; limited bandwidth.
255	Unrestricted in scope.

Therefore, setting a TTL scope of 15 on an interface prevents the forwarding of IP multicast traffic that is intended to be restricted to the site. Only regional or beyond traffic is forwarded.

TTL-based boundaries are less effective than scope-based boundaries due to interactions with multicast routing protocols. For more information, see RFC 2365.

Multicast Rate Limiting

With multicast rate limiting, you can restrict multicast traffic forwarding for traffic beyond a specified rate in kilobytes per second.

Multicast Heartbeat

Multicast heartbeat is the ability of the Windows 2000-based 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. To detect that the multicast heartbeat is missing, you must create a polling mechanism that periodically checks the multicast heartbeat status. If the status becomes inactive, then you can create a notification event. For more information, see the Microsoft Platform SDK link at http://windows.microsoft.com/windows2000/reskit/webresources.

For example, you could create a mechanism that sends a Simple Network Management Protocol (SNMP) trap to the configured SNMP management station when the multicast heartbeat status becomes inactive. This requires the creation of an SNMP sub-agent; the SNMP agent on the Windows 2000 router must be configured with the SNMP community name and the destination to send traps. For more information, see "Simple Network Management Protocol" in the TCP/IP Core Networking Guide.

A common protocol used for multicast heartbeat is Simple Network Time Protocol (SNTP). SNTP uses the reserved IP multicast address 224.0.1.1 and is used for time synchronization. If the source of the heartbeat traffic (the SNTP server) is strategically placed, the loss of the heartbeat indicates a problem with the IP multicast routing infrastructure. Windows 2000 includes an SNTP server called the Windows Time Synchronization service (W32Time) and an SNTP client. For more information about SNTP, see RFC 1769.

You can configure multicast heartbeat from the Multicast Heartbeat tab of the properties of the General node under IP Routing in the Routing and Remote Access snap-in.

IP-in-IP Tunnels

IP-in-IP tunnels are used to forward information between endpoints acting as a bridge between portions of an IP internetwork that have differing capabilities. A typical use for IP-in-IP tunnels is the forwarding of IP multicast traffic from one area of the intranet to another area of the intranet, across a portion of the intranet that does not support multicast forwarding or routing.

With IP-in-IP tunneling, an IP datagram is encapsulated with another IP header addressed to and from the endpoints of the IP-in-IP tunnel, as shown in Figure 4.5. An IP-in-IP tunnel is indicated by setting the IP Protocol field to 4 in the outer IP header. For more detailed information about IP-in-IP tunneling, see RFC 1853.

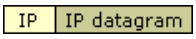


Figure 4.5 IP-in-IP Tunnel Packet Structure

IP-in-IP Interfaces

An IP-in-IP interface is a logical interface that sends IP packets in a tunneled mode. To create an IP-in-IP interface, in the Routing and Remote Access snap-in, right-click Routing Interfaces, click New, and then click Tunnel (IP only). After the tunnel is created, add it as an IP routing interface by right-clicking the General node under IP Routing, and then clicking New Interface.

After IP-in-IP interfaces are created and added as an IP routing interface, you must configure the tunnel endpoints. Then, you can configure them the same as any other IP interface, including setting packet filters to confine the traffic that is allowed into and out of the interface, and multicast scopes and boundaries.

Multicast Static Routes

When an IP multicast packet is received on an interface of a Windows 2000 multicast-enabled router, the source and destination IP address of the IP multicast packet is compared to the entries in the IP multicast forwarding table. If an entry is found, the IP multicast packet is forwarded according to the found entry. If there are no downstream host group members, the packet is eventually discarded.

If an entry is not found, an entry must be created. An entry in the IP multicast forwarding table consists of the multicast group address, the source IP address, a list of interfaces to which the traffic is forwarded (next hop interfaces), and the single interface on which the traffic must be received in order to be forwarded (the previous hop interface). The multicast group and source IP addresses are obtained from the multicast packet. The next hop interfaces are determined by the registration of multicast group members using IGMP (and any multicast routing protocols, if present).

The previous hop interface is the interface that is closest-in terms of routing metrics-to the source of the IP traffic. To determine the previous hop interface, a multicast routing table is checked. Based on the entries in the multicast routing table, a single interface is chosen as the previous hop interface based on the best route back to the source of the IP multicast packet. The best route is the closest matching multicast route with the best metric.

The multicast routing table is logically separate from the unicast routing table. In the Routing and Remote Access service, the Route Table Manager (RTM) keeps a master list of routes. Each route is flagged as either a unicast route, a multicast route, or both. Therefore, the list of routes that you obtain depends on your view. The set of unicast routes in the RTM route table is called the unicast view. The set of multicast routes in the RTM route table is called the multicast view. The multicast view of the RTM routing table is used to determine the previous hop interface and the previous hop neighbor, which is needed for multicast diagnostic utilities, such as mtrace.

By default, all unicast routes obtained by the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) routing protocols, and static routes manually configured with the Routing and Remote Access snap-in, are flagged as appearing in both views. If your unicast routers are also your multicast routers, no other modifications are necessary.

However, in some configurations, the unicast infrastructure and multicast infrastructure are different. For example, to balance the load between unicast and multicast traffic, a different set of routers is used. In these configurations, you might need to override the default behavior of adding all routes as both a unicast and multicast route by creating multicast static route using the netsh routing ip add rtmroute command.

An example is a Windows 2000 router with two interfaces; Interface 1 is connected to a unicast router, Interface 2 is connected to a multicast router. For simplicity, assume that a single static default route is used to forward all non-local unicast IP traffic to a downstream router using Interface 1. Because the static route was configured using the Routing and Remote Access snap-in, it is

flagged as both a unicast and multicast route. Consider what happens when an IP multicast packet is received on Interface 2:

- To create the IP multicast forwarding table entry, the previous hop interface must be determined. Based on the multicast view of the RTM route table, the previous hop interface is determined to be Interface 1, not Interface 2 (Interface 1 is closest to the multicast source in terms of routing metrics). Because the previous hop interface is the only interface on which IP multicast packets for the group and source IP address can be received, subsequent IP multicast packets received on Interface 2 for the group and source IP address are silently discarded.

To fix this multicast forwarding problem, use the netsh routing ip add rtmroute command to create a multicast static default route that uses Interface 2 and has a lower metric. This new route overrides the manually configured static default route.

Supported Multicast Configurations

Because the IGMP router and IGMP proxy component of the Windows 2000 Routing and Remote Access service are not designed to be a substitute for a multicast routing protocol such as DVMRP or PIM, the following sections describe recommended and supported configurations of a Windows 2000 router using the IGMP routing protocol, IGMP router mode, and IGMP proxy mode.

Single Router Intranet

The Windows 2000 router can provide full multicast capabilities in a single router intranet. In this configuration, all interfaces are added to the IGMP routing protocol and each interface is configured for IGMP router mode. Any host on any subnet can both send and receive multicast traffic from any other host. All multicast traffic is forwarded to subnets where there are host members.

The single router intranet configuration is shown in Figure 4.6.

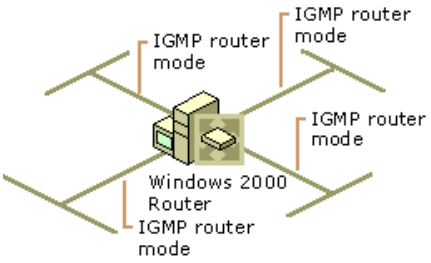


Figure 4.6 Single Router Intranet

Single Router Intranet Connected to the MBone

The Windows 2000 router can provide multicast capabilities in a single router intranet connected to the Internet MBone. In this configuration, all interfaces on are added to the IGMP routing protocol. All private subnet interfaces are configured for IGMP router mode and the Internet interface is configured for IGMP proxy mode.

Hosts joining multicast groups send IGMP Host Membership Reports, which are then copied on the Internet interface. Multicast traffic from the Internet is sent to the Internet interface. When received, the multicast traffic is forwarded to the host on the appropriate subnet. Multicast traffic sent by a host on an intranet subnet is copied to the Internet interface. The multicast router at the ISP either ignores or forwards the multicast traffic.

In this configuration, multicast traffic sent between two hosts on the private intranet is still copied to the Internet interface, resulting in inefficient use of the bandwidth of the link to the ISP. To prevent intranet multicast traffic from being copied to the Internet interface, configure the applications or the ranges of multicast addresses on your MADCAP servers on the intranet to use IP multicast addresses from the administratively scoped range of 239.0.0.0 to 239.254.255.255, and configure the appropriate scope-based boundary on the Internet interface.

The single router intranet connected to the MBone configuration is shown in Figure 4.7.

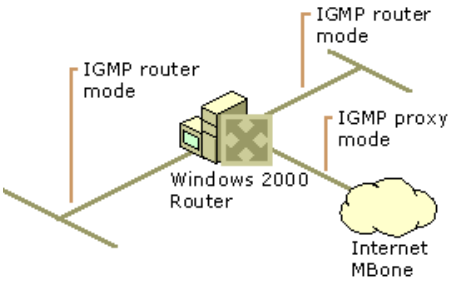


Figure 4.7 Single Router Intranet Connected to the MBone

Peripheral Router in a Multicast-Enabled Intranet

In a configuration very similar to the single router intranet connected to the MBone, a Windows 2000-based router can provide multicast capabilities as a peripheral router connected to a multicast-enabled private intranet. A peripheral router is a router attached to multiple subnets; however, only a single attached subnet contains another router. In this case, the other router is a multicast core router, a multicast router running routing protocols that is part of the multicast-enabled intranet.

In this configuration, all interfaces are added to the IGMP routing protocol. All interfaces not containing the multicast router are configured for IGMP router mode and the interface connected to the subnet containing the multicast core router is configured for IGMP proxy mode.

Hosts joining multicast groups send IGMP Host Membership Reports, which are copied on the interface attached to the subnet containing the multicast core router. Multicast traffic from the intranet is forwarded to the IGMP proxy mode interface subnet. When received, the multicast traffic is forwarded to the host on the appropriate subnet. Multicast traffic sent by a host on an attached subnet is copied to the IGMP proxy mode interface subnet. The multicast core router either ignores the multicast traffic or forwards it to downstream host group members.

The peripheral router in a multicast-enabled intranet configuration is shown in Figure 4.8.

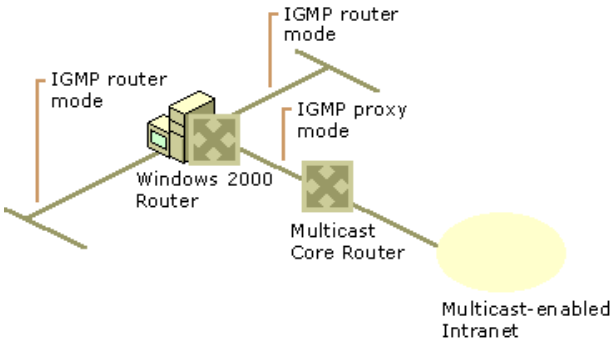


Figure 4.8 Peripheral Router in a Multicast-Enabled Intranet

Multicast Support for Remote Access Clients

A common use for the Windows 2000 IGMP routing protocol is to provide multicast services to dial-up or virtual private network (VPN) remote access clients. As in the previously discussed configurations, the remote access or VPN server is acting as a peripheral router to a multicast-enable IP internetwork.

There are two possible configurations, depending on the connectivity provided to the remote access clients:

- MBone access for dial-up clients by an ISP.
- Access to a private multicast-enabled intranet for dial-up or VPN clients.

MBone Access for ISP Dial-Up Clients

If you are using the Windows 2000 Routing and Remote Access service to provide Internet access to dial-up clients as an ISP:

1. Add the Internal interface, and the interface connecting to the rest of the Internet, to the IGMP routing protocol. The Internal interface represents all remote access clients.
2. Configure the Internal interface for IGMP router mode.
3. Configure the Internet interface for IGMP proxy mode.

Connected remote access clients joining multicast groups send IGMP Host Membership Reports, which are copied on the Internet interface. Multicast traffic from the Internet is sent to the Internet interface. When received, the multicast traffic is forwarded to the connected host. Multicast traffic sent by a connected host is forwarded to other connected host group members and copied to the Internet interface. The downstream multicast router in the Internet either ignores the multicast traffic or forwards it to downstream group members.

The MBone access configuration for ISP dial-up clients is shown in Figure 4.9.

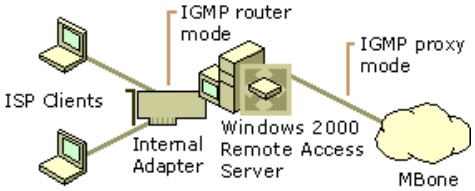


Figure 4.9 Mbone Access for ISP Dial-Up Clients

Private Intranet Access for Dial-Up or VPN Clients

If you are using the Windows 2000 Routing and Remote Access service to provide intranet access for dial-up or VPN remote access clients, perform the following steps:

1. Add the Internal interface and the interface connecting to the private intranet to the IGMP routing protocol. The Internal interface represents all remote access clients. The private intranet interface must be attached to a subnet containing a multicast core router.
2. Configure the Internal interface for IGMP router mode.
3. Configure the private intranet interface for IGMP proxy mode.

Connected remote access clients joining multicast groups, send IGMP Host Membership Reports, which are copied on the intranet interface. Multicast traffic from the intranet is sent to the IGMP proxy mode interface subnet. When received, the multicast traffic is forwarded to connected group members. Multicast traffic sent by a connected host is forwarded to other connected host group members and copied to the IGMP proxy mode interface subnet. The multicast core router either ignores the multicast traffic or forwards it to downstream group members.

The private intranet access for dial-up or VPN clients configuration is shown in Figure 4.10.

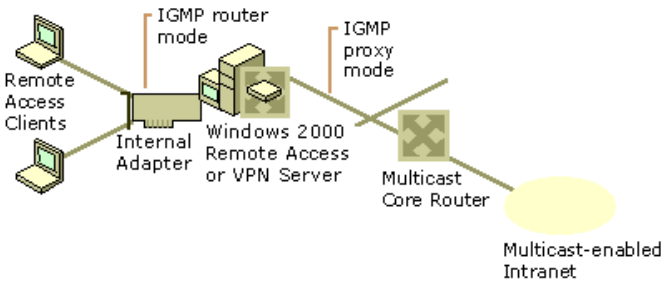


Figure 4.10 Private Intranet Access for Dial-Up or VPN Clients

For more information about multicast support for the remote access server, see "Remote Access Server" in this book.

Multicast Support for Branch Office Networks

The Windows 2000 router can provide full multicast capabilities for single router branch offices connected to a hub office with a

multicast-enabled intranet. This configuration requires proper configuration of both the branch office and hub office router.

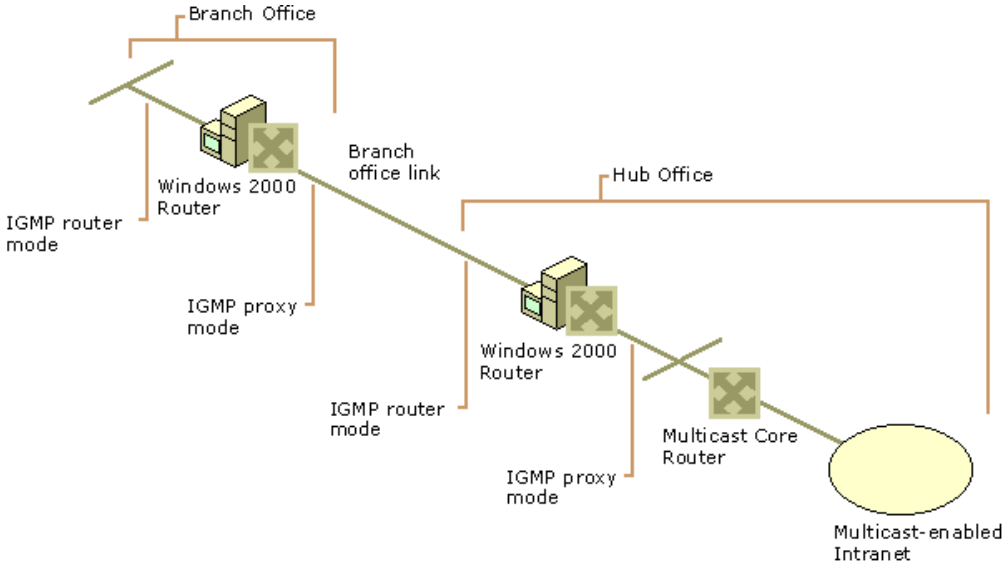
For the branch office router, all interfaces are added to the IGMP routing protocol and the interfaces for the branch office subnets are configured for IGMP router mode. The interface that connects to the hub office router is configured for IGMP proxy mode. The interface that connects to the hub office router can be a LAN interface (such as when using a T-Carrier or Frame Relay connection) or a demand-dial interface (such as when using dial-up analog phone lines, ISDN, or a router-to-router VPN connection). A demand-dial interface can be either on-demand or persistent. For more information about demand-dial interfaces and configuration, see "Demand-Dial Routing" in this book.

For the hub office router, all interfaces are added to the IGMP routing protocol and the interface connected to the branch office is configured for IGMP router mode. The interface that connects to the branch office router can be a LAN interface (such as when using a T-Carrier or Frame Relay connection) or a demand-dial interface (such as when using dial-up analog phone lines, ISDN, or a router-to-router VPN connection). The interface that connects the multicast core router subnet is configured for IGMP proxy mode.

IGMP Group Membership Report messages for group members are copied across the branch office link to the multicast core router subnet. Multicast traffic from branch office hosts is flooded from the branch office subnet across the branch office link to the multicast core router subnet.

In this configuration, multicast traffic sent between two hosts on the branch office intranet is copied to the branch office link, resulting in inefficient use of the bandwidth of the link to the hub office. To prevent intra-branch office multicast traffic from being copied to the branch office link, configure the applications or the ranges of multicast addresses on your MADCAP servers on the intranet to use IP multicast addresses from the administratively scoped range of 239.0.0.0 to 239.254.255.255, and configure the appropriate scope-based boundaries on the interface to the hub office.

The multicast support for branch office networks configuration is shown in Figure 4.11.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.11 Multicast Support for Branch Office Networks

IP Multicast Troubleshooting Tools

To troubleshoot IP multicast problems, the Windows 2000 Routing and Remote Access service provides the following tools:

- Routing and Remote Access snap-in tables
- Mrinfo command
- Mtrace support
- Netsh commands
- IGMP event logging
- Tracing

For more information about general multicast troubleshooting, see the Internet Draft titled "Multicast Debugging Handbook."

Routing and Remote Access Snap-In Tables

There are three tables containing IP multicast information that can be viewed with the Routing and Remote Access snap-in:

- Multicast forwarding table
- Multicast statistics
- IGMP interface group table

Their location within the Routing and Remote Access snap-in depends on the component that maintains the table.

Multicast Forwarding Table

The multicast forwarding table is the table used by IP to forward IP multicast traffic. Each entry records a specific host group and the source of the traffic. The Type column is set to Active for the entry if packets for the host group are being forwarded and set to Negative if the traffic is seen on the network but the router is not forwarding because no hosts have registered for this group.

To view the multicast forwarding table, right-click the General node under IP Routing, and then click Show Multicast forwarding table.

Multicast Statistics

Multicast statistics are counters and other information compiled by IP for each multicast group being forwarded. An entry for multicast statistics records the group address, the IP address of the multicast source, the interface on which it was received, the number of packets received, and other information.

To view multicast statistics, right-click the General node under IP Routing, and then click Show Multicast statistics.

IGMP Group Table

The IGMP group table displays IGMP host group membership information for all host groups registered on all interfaces configured for IGMP router mode. Each entry records uptime (number of seconds since the group was first registered), expiry time (the number of seconds left before the group expires if no hosts send host membership reports for this address), and other information.

To view the IGMP Group Table, right-click the IGMP node under IP Routing, and then click Show group table.

IGMP Interface Group Table

The IGMP interface group table displays IGMP host group membership information for host groups registered on a specific interface configured for IGMP router mode. Each entry records uptime (number of seconds since the group was first registered), expiry time (the number of seconds left before the group expires if no hosts send host membership reports for this address), and other information.

To view the IGMP Interface Group Table, right-click the interface in the IGMP node under IP Routing, and then click Show interface group table.

Mrinfo Command

Windows 2000 includes the mrinfo tool, which you can use to display the configuration of a multicast router. The configuration information can be used to aid in the troubleshooting of multicast forwarding and routing problems.

mrinfo queries a specified multicast router with a special message. The response to the query contains a version number, the list of interfaces and the neighbors on each interface, metrics, Time-to-Live (TTL) thresholds, and flags. mrinfo syntax includes:

```
mrinfo [ -d debug_level ] [ -r retry_count ] [ -t timeout_count ] multicast_router
```

Table 4.6 Mrinfo Command Options

Option	Description
-d	Specifies the debug level. The default value is 0. When debug leve1 is set to 1, all packet warnings are displayed. When debug leve1 is set to 2, downed network notifications and all level 1 messages are displayed. When debug leve1 is set to 3, packet time-out notifications and all level 2 messages are displayed.
-r	Specifies the neighbor query retry limit. The default value is 3.
-t	Specifies how long in seconds mrinfo waits for a neighbor query reply. The default value is 4.

Example of using mrinfo:

```
C:\>mrinfo 10.1.0.1
10.1.0.1(test1.ntdev.microsoft.com) [version 20.50,mtrace,snmp]:
10.1.0.1 -> 0.0.0.0 (local) [1/0/querier/leaf]
10.2.0.1 -> 10.2.0.2 (test2.ntdev.microsoft.com) [1/0]
10.2.0.1 -> 10.2.0.3 (test3.ntdev.microsoft.com) [1/0]
10.3.0.1 -> 0.0.0.0 (local) [1/0/querier/leaf]
```

In the previous example, mrinfo is run against a multicast router at 10.1.0.1. The first line shows the multicast router configuration: version number (for Windows 2000 routers, the version number reflects the build number of Windows 2000) and flags (mtrace and SNMP supported).

Each additional line displays the interfaces on the multicast router and the neighbors on each interface. Interfaces 10.1.0.1 and 10.3.0.1 have no neighbors. Interface 10.2.0.1 has two neighbors, 10.2.0.2 and 10.2.0.3. For each line, mrinfo displays the interface and neighbor, the domain name for the neighbor, the multicast routing metric, the TTL threshold, and flags indicating its role on the network such as the IGMP querier of the network (querier) or whether it has no neighbors (leaf).

Mtrace Support

Although Windows 2000 does not provide a version of the multicasting tracing utility called mtrace, the Windows 2000 multicast router does respond to mtrace queries from third-party mtrace utilities.

Netsh Commands

To view multicast tables and gather information to aid in the troubleshooting of multicast routing and forwarding problems, use the following netsh command lines:

- netsh routing ip show mfe

  Displays the entries in the multicast forwarding table. This is equivalent to the multicast forwarding table available from the Routing and Remote Access snap-in.

- netsh routing ip show mfestats

  Displays packet statistics and input and output interface information for entries in the multicast forwarding table. This is equivalent to the multicast statistics window available from the Routing and Remote Access snap-in.

- netsh routing ip igmp show grouptable

  Displays IGMP host group membership information for all host groups registered on all interfaces configured for IGMP router mode. This is equivalent to the IGMP group table in the Routing and Remote Access snap-in.

- netsh routing ip igmp show ifstats

  Displays IGMP statistics for each interface.

- netsh routing ip igmp show iftable

  Displays host group membership information for host groups registered on a specific interface configured for IGMP router mode. This is equivalent to the IGMP interface group table in the Routing and Remote Access snap-in.

- netsh routing ip igmp show rasgrouptable

  Displays the group table for the Internal interface used by the remote access server.

- netsh routing ip igmp show proxygrouptable

  Displays the group table for the IGMP proxy mode interface.

IGMP Event Logging

The level of event logging for events recorded in the Windows 2000 system event log for the IGMP routing protocol is set:

- Through the properties of the IGMP routing protocol under IP Routing in the Routing and Remote Access snap-in.
- The netsh routing ip igmp set global command.

- The logging levels are:
- Log errors only
- Log errors and warnings
- Log the maximum amount of information
- Disable event logging

The default level is Log errors only. When troubleshooting a problem with the IGMP routing protocol, set the logging level to Log the maximum amount of information. Once the appropriate information is obtained, set the logging level back to Log errors only.

Tracing

Tracing records the sequence of programming functions called during a process to a file. To record detailed information about IGMP routing protocol processes in the log file SystemRoot\tracing\IGMPv2.log, set the value of the EnableFileTracing registry entry (HKEY_LOCAL_MACHINE \Software \Microsoft \tracing \IGMPV2) to 1. After you are done viewing the traced information, set EnableFileTracing back to its original setting of 0.

The tracing information can be complex and very detailed. This information is predominantly useful only to Microsoft support professionals, or to network administrators who are very experienced with the Windows 2000 Routing and Remote Access service. The tracing information can be saved as files and sent to Microsoft support for analysis. For more information about the tracing facility, see "Routing and Remote Access Service" in this book.

Additional Resources

For more information about IP multicast, see Deploying IP Multicast in the Enterprise by Thomas A. Maufer, 1998, Upper Saddle River, NJ: Prentice Hall PTR.
