Home

Home > My courses > Network Defense and Remote Access Configuration > 05 [Enter Module Title Here] > Lesson Proper for Week 5

Lesson Proper for Week 5

TCP/IP III

IPv6 Core Protocols

You have probably read brief descriptions of IPv6, but most networking books and articles have not explored it in detail until recently. Although you might be a whiz at IPv4, IPv6 has some major differences in its core architecture and functions, and uses some different core protocols. For example, IPv4 uses Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages to manage node-to-node communications, but IPv6 uses the Neighbor Discovery protocol. The next few sections explain the core architecture and protocols of IPv6.

IPv6 is a connectionless, unreliable datagram protocol used mainly for addressing and routing packets between hosts. Being connectionless, IPv6 does not establish a session before data is exchanged, and delivery is not guaranteed. IPv6 makes a concerted attempt to deliver a packet but relies on higher-layer protocols, such as TCP, if acknowledgement and recovery of lost packets are required.

An IPv6 datagram consists of the IPv6 header and the IPv6 payload. The IPv6 header is made up of the IPv6 base header and IPv6 optional extension headers. For functional purposes, the optional extension headers and upper-layer protocols are considered part of the IPv6 payload.

As you can see in Figure 2-8, an IPv6 header is more streamlined than an IPv4 header.

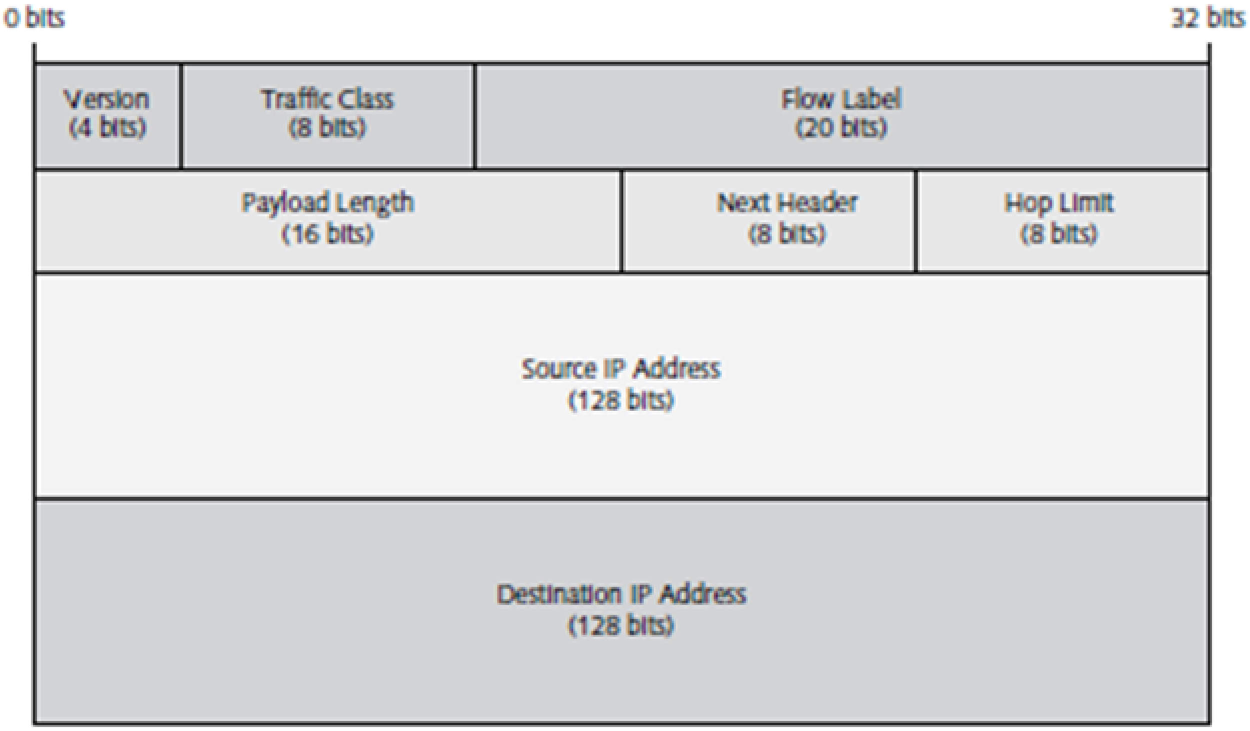


Figure 2-8 IPv6 header structure

The fields in the IPv6 header are as follows:

- *Version*—This field specifies the IP version number (6 for IPv6). Note that the Internet Header Length (IHL) field has been removed in IPv6.

- *Traffic Class*—Also known as the priority field, this field identifies traffic subject to flow control. A value of 1 to 7 indicates lower-priority transmissions that can be slowed down when encountering congestion. Values from 8 to 15 represent real-time traffic that must have a constant sending rate.

- *Flow Label*—This experimental field has not yet been implemented fully, but it can support labeling of some groups of packets as a "flow" and thus improve performance of time-sensitive content such as multimedia. For example, a connection could be specified as "no delay allowed on this connection."

- *Payload Length*—This field indicates the length of the IPv6 payload, which includes the extension headers as well as the upper-layer content. (Extension headers are not shown in Figure 2-8.) The Payload Length field replaces the IPv4 Total Length field and is expressed in 16 bits, indicating a payload of up to 65,535 bytes. If a larger payload is present, this field is set to zero and the Jumbo Payload option is specified in the Hop-by-Hop Options extension header.

- *Next Header*—This field identifies the first extension header. If no extension header is present, the field identifies the name of the transport protocol handler for that packet (for example, TCP or UDP). The port numbers used in the second case are the same as those used in IPv4.

- *Hop Limit*—This field indicates the maximum number of hops the packet is allowed before it is dropped. This number is decreased by 1 each time the packet is transmitted by a router. When the value in this field reaches 0, the packet is dropped. This field replaces the IPv4 Time to Live field.

- *Source IP Address*—This field contains the 128-bit address of the packet source.

- *Destination IP Address*—This field contains the 128-bit address of the packet's intended recipient. It might not be the final destination if a routing extension header is present.

Extension headers are not normally found in a typical IPv6 packet. If needed, however, the sending host adds the appropriate extension header(s). IPv6 extension headers include the following:

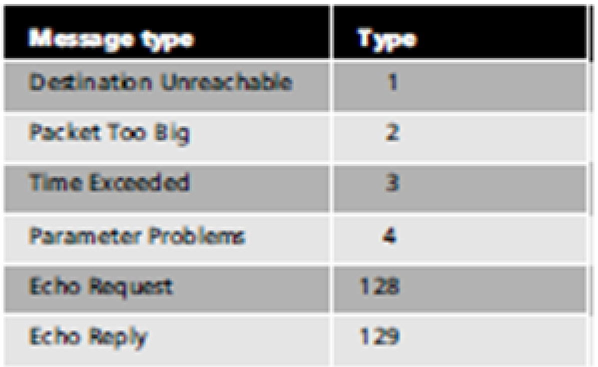
- *Hop-by-Hop* Options header—This header carries information that every node along the delivery path must examine and process. It can specify a Jumbo Payload option for payloads greater than 56,535 bytes and up to about 4.2 gigabytes. It also supports the Router Alert option used in Multicast Listener Discovery, which is explained later in this chapter.
- *Destination Options header*—This header carries optional information used by intermediate destinations or by the final destinations. A Next Header value of 60 indicates this header's presence.
- *Routing header*—Similar to IPv4's loose source and record routing (lsrr) option, this header is used to list one or more intermediary nodes (particularly routers) to which the packet is to be forwarded. A Next Header value of 43 indicates that a Routing header is present.
- *Fragment header*—This header is used to send a packet larger than the maximum transmission unit (MTU) value allows. For example, the MTU of Ethernet is 1500 bytes, so larger payloads need to be fragmented. The source node divides large packets into fragments and generates an identification value. (Fragmentation in IPv6 is performed only by source nodes, not by routers along the delivery path.) A Next Header value of 44 indicates a fragment header's presence, but only the destination node processes this header, using it to reassemble fragmented packets on receipt.
- *Authentication header (AH)*—This header provides data authentication and integrity for IPv6 packets. It is algorithm-independent and supports many authentication techniques. The Authentication header is part of the IPsec (IP Security) standard and provides a field for the Security Parameters Index (SPI), which identifies the Security Association (SA) required by IPsec. A value of 51 in the Next Header field specifies the Authentication header.
- *Encapsulating Security Payload (ESP) header*—This field provides data integrity, authentication, and confidentiality to the encapsulated payload (the data portion of the datagram). Also, a foundational protocol of IPsec, the ESP header, includes an SPI field.

Remember that IPv4 and IPv6 headers are not interoperable. A host or router must be configured to support both so that it can recognize and process both formats.

Internet Control Message Protocol for IPv6 ICMPv6

An integral component of IPv6 communications, is used by IPv6 nodes for reporting errors and for diagnostic purposes. As in ICMPv4, ICMPv6 uses the ping and tracert commands as well as other diagnostics you already know.

ICMPv6 messages are grouped into two classes: error messages and informational messages. Error messages are identified by message type codes 0 to 127, and informational messages are identified by message type codes 128 to 255. Table 2-11 shows common message type codes for ICMPv6.



Message type	Type
Destination Unreachable	1
Packet Too Big	2
Time Exceeded	3
Parameter Problems	4
Echo Request	128
Echo Reply	129

Table 2-11 Common ICMPv6 message type codes

ICMPv6 is specified in RFC 4443 and updated by RFC 4884.

An ICMPv6 message is preceded by an IPv6 header and sometimes by extension headers. An ICMPv6 header follows the IPv6 header and is identified by a Next Header value of 58 in the IPv6 header. An ICMPv6 header has the format shown in Figure 2-9.

The Type field in Figure 2-9 contains the value for a type of ICMPv6 message; for example, a value of 128 indicates an Echo Request message. The Code field specifies additional parameters for the message. For example, if a Destination Unreachable (type 1) message is received, the Code field might contain 1, indicating that the firewall configuration or other security protocol denied packet access, thus prohibiting communication with the destination. The Checksum field is used to detect data corruption in the ICMPv6 message and parts of the IPv6 header.

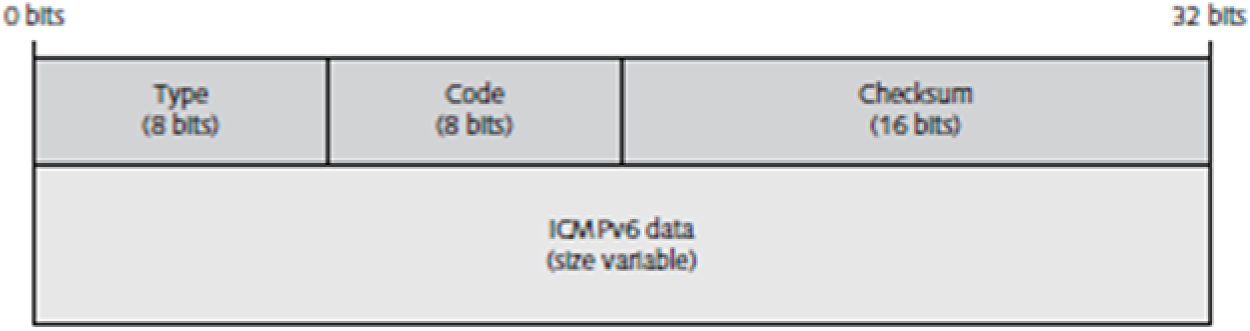
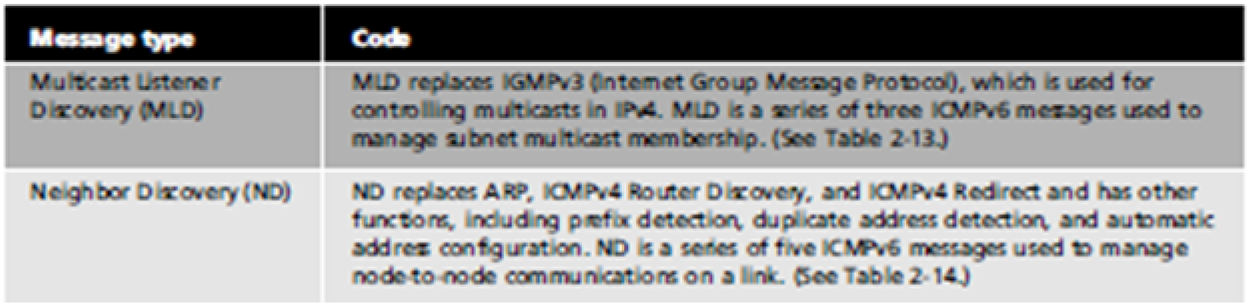


Figure 2-9 ICMPv6 header structure

ICMPv6 also provides the framework for additional IPv6 features, as shown in Table 2-12. The following sections discuss these features in more detail.



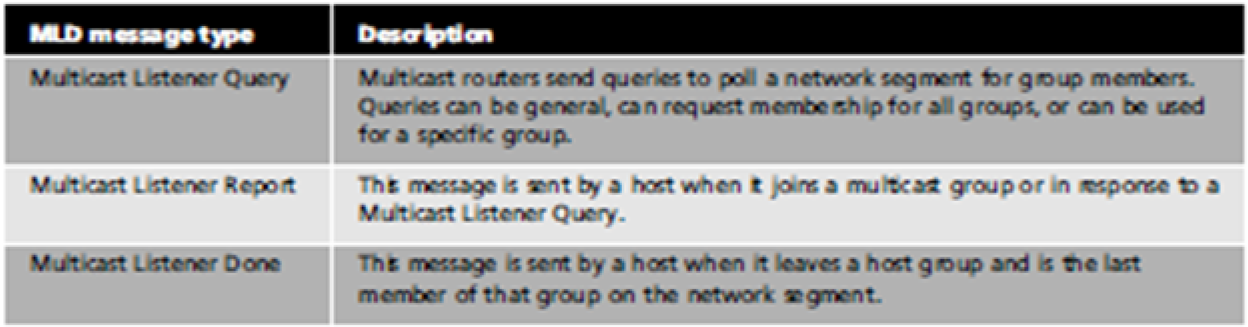
Message type	Code
Multicast Listener Discovery (MLD)	MLD replaces IGMPv3 (Internet Group Message Protocol), which is used for controlling multicasts in IPv4. MLD is a series of three ICMPv6 messages used to manage subnet multicast membership. (See Table 2-13.)
Neighbor Discovery (ND)	ND replaces ARP, ICMPv4 Router Discovery, and ICMPv4 Redirect and has other functions, including prefix detection, duplicate address detection, and automatic address configuration. ND is a series of five ICMPv6 messages used to manage node-to-node communications on a link. (See Table 2-14.)

Table 2-12 ICMPv6 features

Multicast Listener Discovery Multicasts are used for a variety of network functions and connectionless delivery of information to multiple subscribers at the same time. Unlike conventional data streaming, which uses one stream per recipient, multicasting has a single stream on any link with at least one recipient. Instead of consuming bandwidth to distribute multiple copies, routers track subscribers (group members) and create copies only as needed.

IP multicast traffic is sent to a single address but is processed by all members of a multicast group. Hosts listening on a specific multicast address are part of the multicast group. Group membership is dynamic, with hosts joining and leaving the group at any time. A host does not need to be a group member to send messages to the group. The group size is unlimited, and members can be on different subnets as long as the connecting routers support multicast message forwarding between those subnets. Multicast group members can be members of multiple groups simultaneously.

Multicast addresses can be permanent or transient. A permanent multicast address has an administratively assigned IP address. However, the address is permanent, not the group members. In IPv6, Multicast Listener Discovery (MLD) enables IPv6 routers to discover multicast listeners on a directly connected link and decide which multicast addresses are of interest to the nodes. MLD uses a series of ICMPv6 messages to track membership, as shown in Table 2-13.



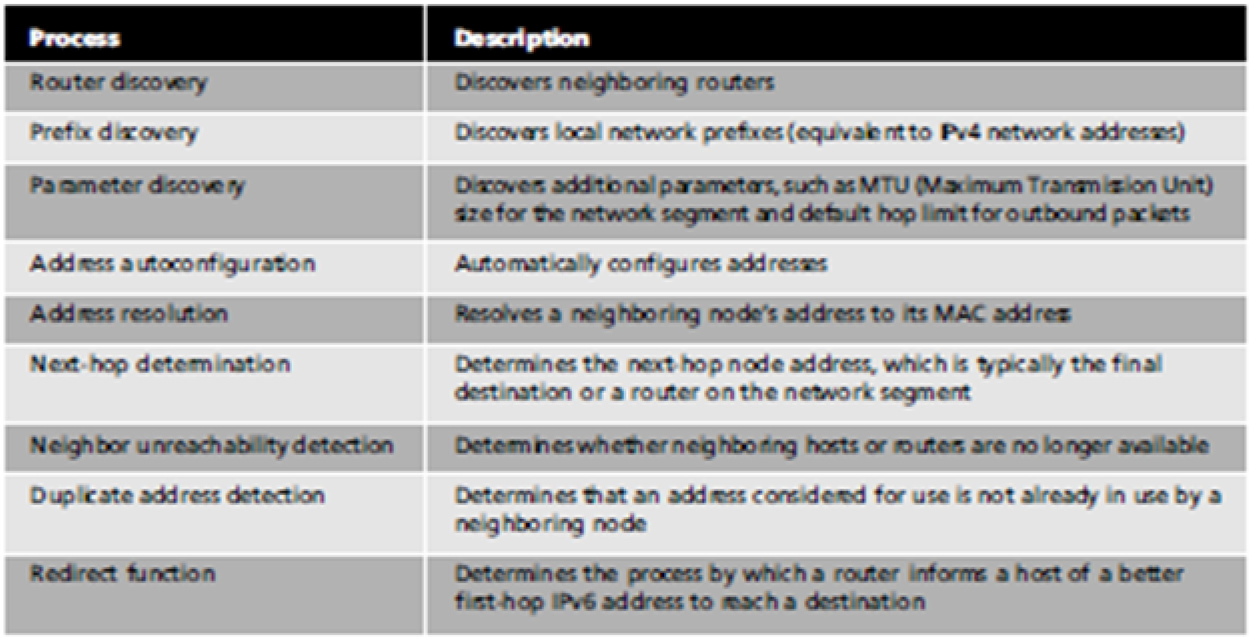
MLD message type	Description
Multicast Listener Query	Multicast routers send queries to poll a network segment for group members. Queries can be general, can request membership for all groups, or can be used for a specific group.
Multicast Listener Report	This message is sent by a host when it joins a multicast group or in response to a Multicast Listener Query.
Multicast Listener Done	This message is sent by a host when it leaves a host group and is the last member of that group on the network segment.

Table 2-13 Multicast Listener Discovery message types

MLD for IPv6 is specified in RFC 2710, with updates added in RFCs 3590 and 3810. Be sure to check for other updates because Internet drafts change often.

Neighbor Discovery

In IPv4, ARP is used to resolve IP addresses to MAC (Media Access Control) addresses, and ICMP Router Discovery and ICMP Redirect are used to locate neighboring routers and redirect hosts to better routes to reach destination addresses. IPv6 uses a new protocol, Neighbor Discovery (ND), to handle these tasks and provide additional functions. ND uses ICMPv6 messages to manage node-to-node communications. Table 2-14 summarizes the functions of ND.



Process	Description
Router discovery	Discovers neighboring routers
Prefix discovery	Discovers local network prefixes (equivalent to IPv4 network addresses)
Parameter discovery	Discovers additional parameters, such as MTU (Maximum Transmission Unit) size for the network segment and default hop limit for outbound packets
Address autoconfiguration	Automatically configures addresses
Address resolution	Resolves a neighboring node's address to its MAC address
Next-hop determination	Determines the next-hop node address, which is typically the final destination or a router on the network segment
Neighbor unreachability detection	Determines whether neighboring hosts or routers are no longer available
Duplicate address detection	Determines that an address considered for use is not already in use by a neighboring node
Redirect function	Determines the process by which a router informs a host of a better first-hop IPv6 address to reach a destination

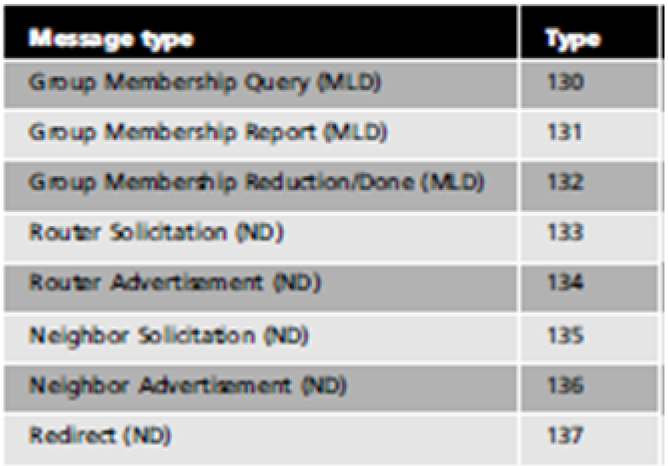
Table 2-14 IPv6 Neighbor Discovery functions

ND for IPv6 is specified in RFC 4861, with updates added in RFC 4311 and RFC 5942.

ND defines five different types of ICMP messages:

- Router Solicitation messages are sent by hosts when an interface is enabled so that they can discover routers on the network. A Router Solicitation message requests that routers send a Router Advertisement message immediately rather than at the next scheduled time.
- Router Advertisement messages inform hosts about router presence and provide additional parameters about the link or services, such as address configuration or suggested hop limits. A Router Advertisement message is sent at defined intervals or in response to a Router Solicitation message.
- Neighbor Solicitation messages are sent by a node to determine the MAC address of a neighbor or to verify that a neighbor is still reachable. Neighbor Solicitation messages are also used for duplicate address detection.
- Neighbor Advertisements are sent in response to a Neighbor Solicitation message or to update neighbors of a MAC address change.
- Redirect messages are sent by routers to tell hosts about better first-hop addresses to reach a destination.

ICMP is an efficient method of managing many underlying networking functions, such as those formerly assumed by Internet Group Management Protocol (IGMP) and ARP. ND and MLD take care of these housekeeping jobs, such as managing group membership and managing node-to-node communications. Each message is identified in the packet header by the corresponding ICMPv6 message type code, as shown in Table 2-15. (In addition to these ICMPv6 message types, remember the common message types in Table 2-11.)



Message type	Type
Group Membership Query (MLD)	130
Group Membership Report (MLD)	131
Group Membership Reduction/Done (MLD)	132
Router Solicitation (ND)	133
Router Advertisement (ND)	134
Neighbor Solicitation (ND)	135
Neighbor Advertisement (ND)	136
Redirect (ND)	137

Table 2-15 Multicast Listener Discovery and Neighbor Discovery message types

IPv6 Addressing

An IPv6 address is 128 bits long, which would mean a very long number if you used the same decimal numbering scheme as in IPv4—not to mention using binary and writing out 128 ones and zeros. To make IPv6 addresses manageable, the hexadecimal numbering format known as base 16 is used. (The hexadecimal format is often called hex.) An IPv6 address consists of eight hex groups separated by colons. Each hex group contains a 16-bit value, and each digit represents a 4-bit value. The following examples show what an IPv6 address looks like:

4EDC:0000:7654:3210:F3DC:BA98:7654:AB1F

1080:0:0:0:8:800:200C:417A

Including leading zeros in a group is not necessary, and hex letters are not case sensitive. You can also replace consecutive zeros with a double colon, as shown in this modification:

1080::8:800:200C:417A

This “compression” of leading zeros comes in handy when typing long strings, but remember that the double colon can be used only once in an address. In a mixed environment of IPv6 and IPv4, you can use the colon hexadecimal notation of IPv6 addresses and the 32-bit dotted decimal notation of IPv4 addresses, as shown in the following examples:

0:0:0:0:0:0:22.1.68.45

0:0:0:0:0:FFFF:131.123.2.8

Using the double colon, you can condense these addresses to the following:

::22.1.68.45

::FFFF:131.123.2.8

You might wonder what address is used for the loopback. It looks like 0:0:0:0:0:0:0:1, which can be compressed to ::1.

Unicast, Multicast, and Anycast Addressing

IPv6 uses three types of addresses: unicast, multicast, and anycast. Notice that IPv6 does not use broadcast addresses.

Unicast is used for one-to-one communication, such as that between two single hosts. Another example is communication between two routers. A unicast address is configured for each interface connected to the network. IPv6 has several forms, or scopes, of unicast addresses:

- *Global unicast addresses*—Equivalent to public addresses in IPv4, these addresses are routable on the Internet.
- *Site-local unicast addresses*—Similar to private addresses in IPv4, this type of address is being phased out and is not permitted in new IPv6 implementations.
- *Unique local IPv6 unicast addresses*—These addresses are replacing the sometimes ambiguous site-local unicast addresses. Unique local IPv6 unicast addresses are private to an organization but are still unique throughout the organization.
- *Link-local unicast addresses*—These addresses are used by hosts when they communicate with other hosts on their same network segment. These addresses are equivalent to the APIPA (Automatic Private IP Addressing) used in IPv4. Link-local unicast addresses always begin with FE80 in the first 16-bit section.

Multicast is used for one-to-many communication, in which a single host can send packets to a group of recipients. Multicast addresses also use scopes: site-local, link-local, and interface-local. Multicast addresses always begin with FF in the first byte.

Anycast addresses are used for one-to-one or one-to-many communication. Anycast addresses are not assigned a specific range; instead, they are created automatically when a unicast address is assigned to more than one interface. This means that anycast addresses are assigned from unicast address ranges and have the same scopes as unicast addresses. The idea behind anycast is to offer flexibility in providing services. For example, a group of servers might provide a service. Using anycast, the service can be provided by any one of the servers—usually the one that is closest. Anycast addresses are currently used only by routers, but their use will expand as the technology becomes widespread.

IPv6 Configuration

Microsoft operating systems since Windows XP SP 1 have built-in IPv6 support. These platforms support stateless autoconfiguration and do not usually need manual configuration. By default, a link-local address is assigned to every Ethernet interface during startup. IPv6 addresses, such as global addresses, are assigned automatically based on the receipt of IPv6 Router Advertisement messages. You must have a correctly configured IPv6-capable router on your network segment to receive additional addresses through IPv6 Router Advertisement messages. Note that a single host often has more than one IPv6 address. For example, a host with a global address will also have a linklocal address.

Some manual configuration is required for more advanced features and setups of IPv6. You can find procedures for your equipment with an Internet search or by contacting the vendor for instructions.

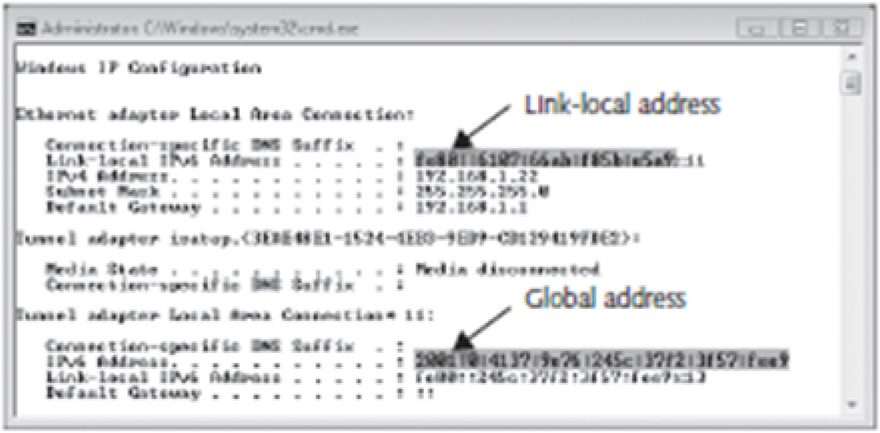
IPv6 Utilities

IPv6 includes several integrated utilities for configuration, troubleshooting, and other administrative tasks. Some utilities are familiar because they are used in IPv4 and have not changed much. In the following sections, you examine some major Windows IPv6 utilities.

IPv6 supports many different tools, and an Internet search for IPv6 tools yields many sites that offer handy utilities, including www.ipv6tools.org, www.ultratools.com/ipv6Tools, and http://dns.antd.nist.gov/ipv6/.

IPconfig

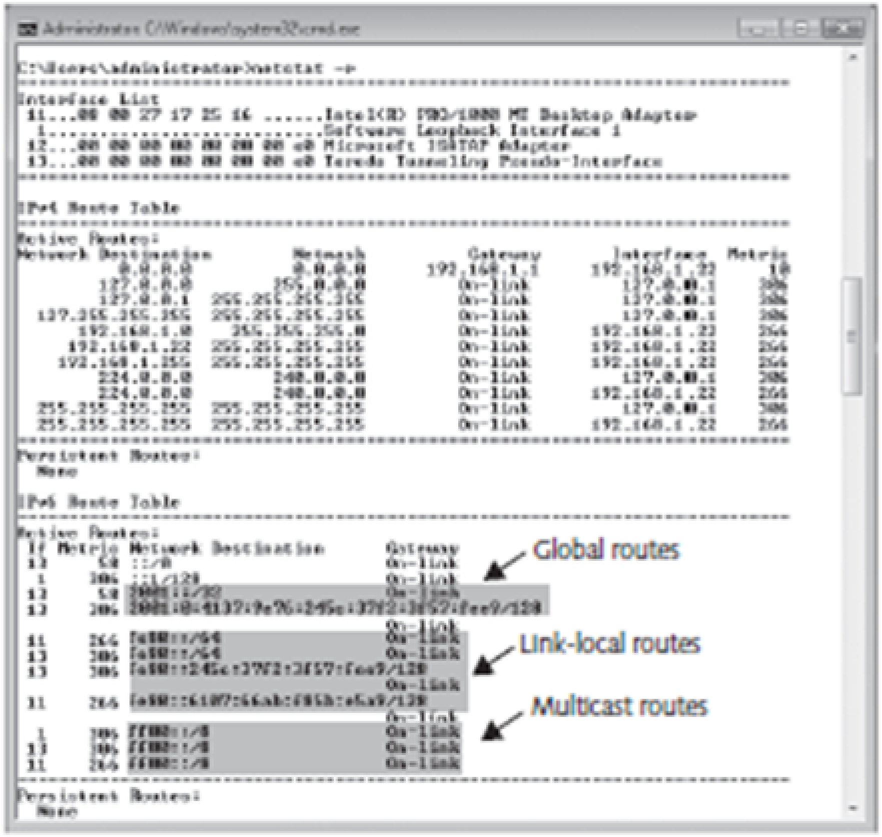
The ipconfig command shows IPv6 configuration details when IPv6 is installed on a Windows operating system. You can also use the command with IPv4. Figure 2-10 shows the result of using the ipconfig command on a system running a dual stack (both IPv4 and IPv6). Note that the host has both a link-local address and a global IPv6 address on the tunnel adapter and a different link-local address on the Ethernet interface, demonstrating that hosts in IPv6 can have multiple IPv6 addresses.



```
Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6107:66ab:f85b:a5a9%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{[illegible]}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e76:245c:37f2:3f57:fea9
   Link-local IPv6 Address . . . . . : fe80::245c:37f2:3f57:fea9%13
   Default Gateway . . . . . . . . . : ::
```

Figure 2-10 Using the ipconfig command

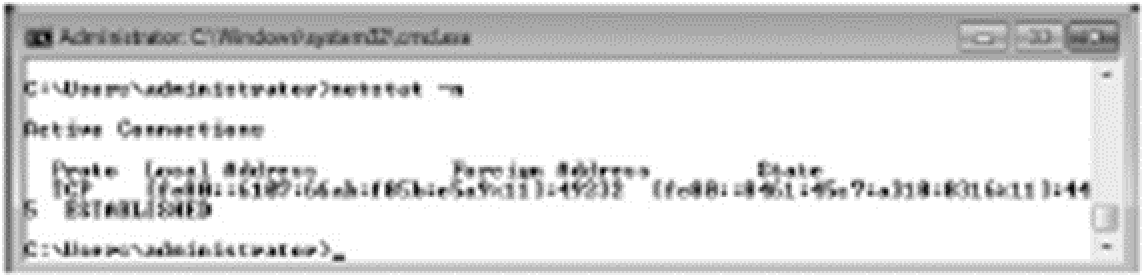
Netstat You can display the system's routing tables by using the netstat -r command, as shown in Figure 2-11. Notice that this example includes routes for three scopes: global, link-local, and multicast.



```
C:\Users\administrator>netstat -r
===========================================================================
Interface List
 11...08 00 27 17 25 16 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.22     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link      192.168.1.22    266
     192.168.1.22  255.255.255.255         On-link      192.168.1.22    266
    192.168.1.255  255.255.255.255         On-link      192.168.1.22    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link      192.168.1.22    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      192.168.1.22    266
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 13     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 13     58 2001::/32                On-link
 13    306 2001:0:4137:9e76:245c:3762:3f57:fee9/128
                                    On-link
 11    266 fe80::/64                On-link
 13    306 fe80::/64                On-link
 13    306 fe80::245c:3762:3f57:fee9/128
                                    On-link
 11    266 fe80::6107:66ab:f85b:e5a9/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    306 ff00::/8                 On-link
 11    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Figure 2-11 Using the netstat –r command

Use the netstat command with the -n option to show current sessions with the associated port numbers. Figure 2-12 shows an IPv6 session between port 49232 on the Windows 7 local machine and its Windows Server 2008 domain controller's port 445.



```
C:\Users\administrator>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    [fe80::6107:66ab:f85b:e5a9%11]:49232  [fe80::8461:45e7:a318:8316%11]:44
5  ESTABLISHED

C:\Users\administrator>_
```

Figure 2-12 Using the netstat command

Use the command netstat -ps IPv6 to display detailed statistics on IPv6 activity since the last bootup. To get even more detailed information, use commands like netstat -ps TCPv6, netstat -ps UDPv6, and netstat -ps ICMPv6.

Netsh

Netsh is a command-line scripting tool on Windows systems that allows troubleshooting and configuration of network interfaces. Netsh works in both noninteractive and interactive modes. In the first of these modes, you can enter commands at the command prompt and receive results. In interactive mode, you can enter the Netsh utility by enteringthe netsh command, and then navigate the different contexts of the netsh tools.

◀ Preliminary Activity for Week 5

Jump to...

Analysis, Application, and Exploration for Week 5 ▶

Navigation

Home

Dashboard

Site pages

My courses

Capstone Project 2

Network Defense and Remote Access Configuration

Participants

General

01 [Enter Module Title Here]

02 [Enter Module Title Here]

03 [Enter Module Title Here]

04 [Enter Module Title Here]

05 [Enter Module Title Here]

Preliminary Activity for Week 5

Lesson Proper for Week 5

Analysis, Application, and Exploration for Week 5

Generalization for Week 5

Evaluation for Week 5

Assignment for Week 5

OJT/Practicum 2

Seminars and Tours

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

- Assignments
- Forums
- Quizzes
- Resources

Bestlink College of the Philippines
College Department

Powered byeLearning Commons