Module 8

Implementing IPv6

Module Overview

IPv6 is a technology that helps the Internet support a growing user base and an increasingly large number of IP-enabled devices. IPv4 has been the underlying Internet protocol for almost thirty years. Its robustness, scalability, and limited feature set is now challenged by the growing need for new IP addresses. This is due in large part to the rapid growth of new network-aware devices.

This module discusses the features and benefits of IPv6, how IPv6 affects IPv4 networks, and how to integrate IPv6 into IPv4 networks by using various transition technologies.

Overview of IPv6

IPv6 has been included with Windows® client operating systems and servers beginning with Windows Server® 2008. The use of IPv6 is becoming more common on corporate networks and on the Internet.

It is important for you to understand how this technology affects current networks, and how to integrate IPv6 into those networks. This lesson discusses the benefits of IPv6, and how it differs from IPv4.

Benefits of IPv6

IPv6 support is included in Windows Server 2012 and Windows 8. The following list of benefits describes why IPv6 is being implemented.

Benefits of IPv6 include:
- Larger address space
- Hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Required support for Internet Protocol security (IPsec)
- End-to-end communication
- Required support for Quality of Service (QoS)
- Improved support for single-subnet environments
- Extensibility

Larger Address Space

The IPv6 address space is 128-bit, which is much larger than the 32-bit address space in IPv4. A 32-bit address space has 2^{32} or 4,294,967,296 possible addresses; a 128-bit address space has 2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 (or 3.4×10^{38} or 340 undecillion) possible addresses. As the Internet continues to grow, IPv6 provides for the required larger address space.

Differences Between IPv4 and IPv6

When the IPv4 address space was designed, it was unimaginable that it could ever be exhausted. However, because of changes in technology and an allocation practice that did not anticipate the growth of number of Internet hosts, it was clear by 1992 that a replacement would be necessary.

When the IPv6 address space was designed, the addresses were made 128 bits long so that the address space could be subdivided into hierarchical routing domains that reflect modern-day Internet topology. With 128 bits, there are enough bits to create multiple levels of hierarchy, and there is flexibility for designing hierarchical addressing and routing. These features are currently lacking on the IPv4-based Internet.

Feature	IPv4	IPv6
Fragmentation	Performed by routers and sending host	Performed only by sending host
Address Resolution	Broadcast ARP Request frames	Multicast Neighbor Solicitation messages
Manage multicast group membership	IGMP	Multicast listener discovery
Router Discovery	ICMP Router Discovery (optional)	ICMPv6 Router Solicitation and Router Advertisement (required)
DNS host records	A records	AAAA records
DNS reverse lookup zones	IN-ADDR.ARPA	IP6.ARPA
Minimum packet size	576 bytes	1280 bytes

IPv6 Address Format

The most distinguishing feature of IPv6 is its use of much larger addresses. IPv4 addresses are expressed in 4 groups of decimal numbers, such as 192.168.1.1. Each grouping of numbers represents a binary octet. In binary, 192.168.1.1 is as follows:

11000000.10101000.00000001.00000001
(4 octets = 32 Bits)

However, an IPv6 address is 4 times larger than an IPv4 address. Because of this, IPv6 addresses are expressed in hexadecimal (hex). For example:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

- 128-bit address in binary:
  001000000000000010000110110111000000000000000000
  000000101111001110110000001010101010000000000000
  1111111111111111000101000100111000101 1010
- 128-bit address divided into 16-bit blocks:
  0010000000000001 0000110110111000
  0000000000000000 0010111100111011
  0000001010101010 0000000011111111
  1111111000101000 1001110001011010
- Each 16-bit block converted to HEX (base 16):
  2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
- Further simplify by removing leading zeros:
  2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

This might seem complex for end users, but the assumption is that users will rely on DNS names to resolve hosts and will rarely type IPv6 addresses manually. The IPv6 address in hexadecimal is also easier to convert between binary and hexadecimal than it is to convert between binary and decimal. This simplifies working with subnets, and calculating hosts and networks.

Converting from Binary to Hexadecimal

The following table describes converting 8 bits of binary into hexadecimal for the binary number [0010][1111]:

Binary	0010	1111
Values of each binary position	8421	8421
Adding values where the bit is 1	0+0+2+0=2	8+4+2+1=15 or hexadecimal F

Each 16-bit block is expressed as 4 hexadecimal characters, and is then delimited with colons. The result is as follows:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

You can simplify IPv6 representation further by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address representation becomes the following:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

IPv6 Address Structure

Each IPv6 address is 128 bits long. The prefix is the part of the address that indicates the bits that have fixed values, or that are the subnet prefix's bits. This is equivalent to the network ID for IPv4 addresses.

Prefixes for IPv6 subnets, routes, and address ranges are expressed in the same way as IPv4 Classless Interdomain Routing (CIDR) notations. An IPv6 prefix is written in address/prefix-length notation. For example, 2001:DB8::/48 and 2001:DB8:0:2F3B::/64 are IPv6 address prefixes.

- The number of network bits is defined by the prefix
- Each host has 64-bits allocated to the interface identifier

Type of address	IPv4 address	IPv6 address
Unspecified	0.0.0.0	::
Loopback	127.0.0.1	::1
Autoconfigured	169.254.0.0/16	FE80::/64
Broadcast	255.255.255.255	Uses multicasts instead
Multicast	224.0.0.0/4	FF00::/8

Note: IPv6 uses prefixes instead of a subnet mask.

When a unicast IPv6 address is assigned to a host, the prefix is 64 bits long. The remaining 64 bits are allocated to the interface identifier, which uniquely identifies the host on that network. The interface identifier can be either randomly generated, assigned by DHCPv6, or based on the media access control (MAC) address of the network. By default, the host bits are generated randomly unless assigned by DHCPv6.

Note: The routes on an IPv6 router have varying prefix sizes that are determined by the size of the network.

IPv6 Equivalents to IPv4 Special Addresses

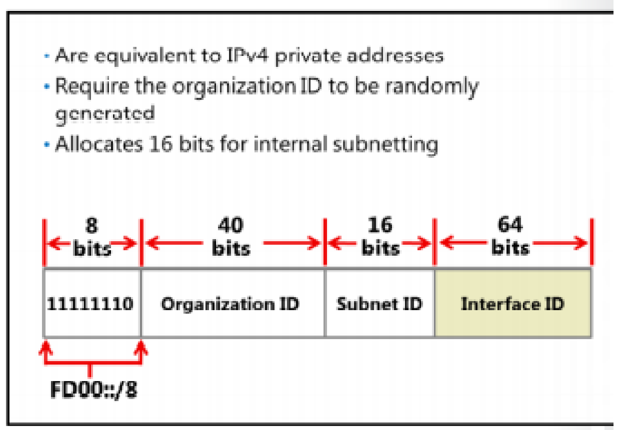
The following table shows IPv6 equivalents to some common IPv4 addresses.

	IPv4 Address	IPv6 Address
Unspecified address	0.0.0.0	::
Loopback address	127.0.0.1	::1
Autoconfigured addresses	169.254.0.0/16	FE80::/64
Broadcast address	255.255.255.255	Uses multicasts instead
Multicast addresses	224.0.0.0/4	FF00::/8

Unique Local Unicast Addresses

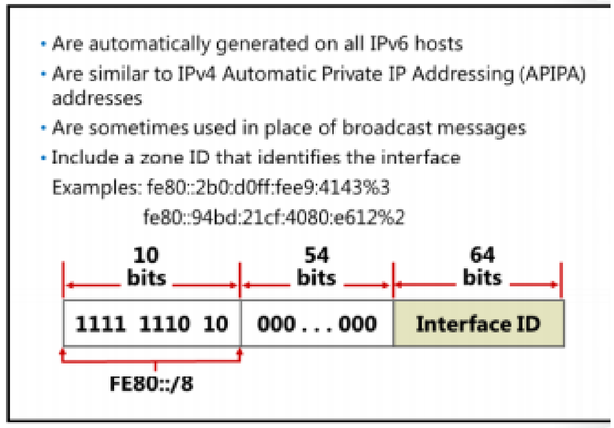
Unique local unicasts addresses are the IPv6 equivalent of IPv4 private addresses. These addresses are routable within an organization, but not on the Internet.

IPv4 private IP addresses were a relatively small part of the overall IPv4 address space, and many companies used the same address space. This caused problems when separate organizations tried to communicate directly. It also caused problems when merging the networks of two organizations—possibly following a merger or a buyout.



Link-Local Unicast Addresses

All IPv6 hosts have a link-local address that is used for communication only on the local subnet. The link-local address is generated automatically, and is non-routable. In this way, link-local addresses are similar to IPv4 APIPA addresses. However, a link-local address is an essential part of IPv6 communication.



Link-local addresses are used for communication in many scenarios where IPv4 would have used broadcasts. For example, link-local addresses are used when communicating with a DHCPv6 server. Link-local addresses are also used for neighbor discovery, which is the IPv6 equivalent of ARP in IPv4.

Zone ID

Regardless of the number of network interfaces in the host, each IPv6 host has a single link-local address. If the host has multiple network interfaces, the same link-local address is reused on each interface. To make it possible for hosts to identify link-local communication on each unique network interface, a zone ID is added to the link-local address.

A zone ID is used in the following format:

Address%zone_ID

If you cannot ping lon-dc1 from Lon-svr2 first revert and restart svr1 and still fails check if the RTR router running and the network of svr2.

Module 8

Lab: Implementing IPv6

Exercise 1: Configuring an IPv6 Network

▶ Task 1: Verify IPv4 routing

1. On LON-SVR2, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type **ping lon-dc1**, and then press Enter.

   Notice that there are four replies from 172.16.0.10.
3. Type **ipconfig**, and then press Enter.

   Verify that the only IPv6 address listed is a link-local address that cannot be routed.
4. Type **Get-NetIPAddress**, and then press Enter.

   Notice that **Get-NetIPAddress** cmdlet returns a link-local IPv6 address.

▶ Task 2: Disable IPv6 on LON-DC1

1. On LON-DC1, in Server Manager, click **Local Server**.
2. In the Properties window, next to the **Ethernet** section, click **172.16.0.10, IPv6 enabled**.
3. In the Network Connections window, right-click **Ethernet**, and then click **Properties**.
4. In the **Ethernet Properties** dialog box, clear the **Internet Protocol Version 6 (TCP/IPv6)** check box, and then click **OK**.
5. Close the Network Connections window.
6. In Server Manager, verify that **Ethernet** lists only **172.16.0.10**. You may need to refresh the view.

   LON-DC1 is now an IPv4-only host.

▶ Task 3: Disable IPv4 on LON-SVR2

1. On LON-SVR2, in Server Manager, click **Local Server**.
2. In the **Local Server Properties** dialog box, next to Ethernet, click **10.10.0.11, IPv6 enabled**.
3. In the Network Connections window, right-click **Ethernet**, and then click **Properties**.
4. In the **Ethernet Properties** dialog box, clear the **Internet Protocol Version 4 (TCP/IPv4)** check box, and then click **OK**.
5. Close the Network Connections window.
6. In Server Manager, verify that **Ethernet** now lists only **IPv6 enabled**. You may need to refresh the view.

   LON-SVR2 is now an IPv6-only host.

▶ Task 4: Configure an IPv6 network on LON-RTR

1. On LON-RTR, on the taskbar, click the **Windows PowerShell** icon.
2. Configure a network address that will be used on the IPv6 network. At the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

```
New-NetRoute -InterfaceAlias " Ethernet 2" -DestinationPrefix 2001:db8:0:1::/64
-Publish Yes
```

3. Allow clients to obtain the IPv6 network address automatically from LON-RTR. At the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

```
Set-NetIPInterface -InterfaceAlias "Ethernet 2" -AddressFamily IPv6 -Advertising
Enabled
```

4. Type **ipconfig**, and then press Enter.

   Notice that Ethernet 2 now has an IPv6 address on the 2001:db8:0:1::/64 network. This address is used for communication on the IPv6-only network.

▶ Task 5: Verify IPv6 on LON-SVR2

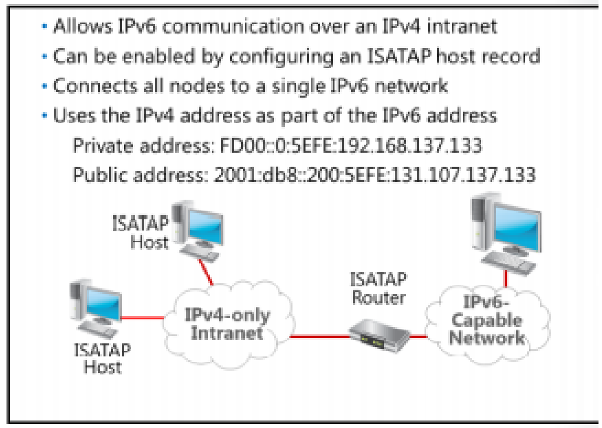
1. On LON-SVR2, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type **ipconfig**, and then press Enter.

   Notice that the Ethernet now has an IPv6 address on the 2001:db8:0:1::/64 network. The network address was obtained from the router through stateless configuration.

Results: After completing the exercise, you will have configured an IPv6–only network.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

What Is ISATAP?



ISATAP is an address-assignment technology that you can use to provide unicast IPv6 connectivity between IPv6/IPv4 hosts over an IPv4 intranet. IPv6 packets are tunneled in IPv4 packets for transmission over the network. Communication can occur directly between two ISATAP hosts on an IPv4 network, or communication can go through an ISATAP router if one network has only IPv6-only hosts.

ISATAP hosts do not require any manual configuration, and can create ISATAP addresses using standard address autoconfiguration mechanisms. Although the ISATAP component is enabled by default, it only assigns ISATAP-based addresses if it can resolve the ISATAP name on your network.

Exercise 2: Configuring an ISATAP Router

▶ Task 1: Add an ISATAP host record to DNS

1. On LON-DC1, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the New Host window, in the **Name** box, type **ISATAP**.
5. In the **IP address** box, type **172.16.0.1**, and then click **Add Host**. ISATAP clients resolve this host name to find the ISATAP router.
6. Click **OK** to clear the success message.
7. Click **Done** to close the New Host window.
8. Close **DNS Manager**.

▶ Task 2: Enable the ISATAP router on LON-RTR

1. On LON-RTR, configure the IP address of the **Ethernet** adapter as the ISATAP router. At the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

```
Set-NetIsatapConfiguration -Router 172.16.0.1
```

2. Type the following command, and then press Enter:

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address
```

3. Record the InterfaceIndex of the ISATAP interface that has an IPv6 address that includes **172.16.0.1**.

Interface index:	

4. Type the following command, and then press Enter:

```
Get-NetIPInterface -InterfaceIndex IndexYouRecorded -PolicyStore ActiveStore |
Format-List
```

5. Verify that Forwarding is enabled for the interface and that Advertising is disabled.

6. The ISATAP interface for an ISATAP router must have forwarding enabled and advertising enabled. Type the following command, and then press Enter:

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Enabled
```

7. Create a new IPv6 network that will be used for the ISATAP network. Type the following command, and then press Enter:

```
New-NetRoute -InterfaceIndex IndexYouRecorded -DestinationPrefix 2001:db8:0:2::/64
-Publish Yes
```

8. View the IP address configuration for the ISATAP interface. Type the following command, and then press Enter:

```
Get-NetIPAddress -InterfaceIndex IndexYouRecorded
```

9. Verify that an IPv6 address is listed on the 2001:db8:0:2::/64 network.

▶ Task 3: Remove ISATAP from the Global Query Block List

1. On LON-DC1, at the Windows PowerShell prompt, type the following command, and then press Enter.

```
dnscmd /config /globalqueryblocklist wpad
```

2. At the Windows PowerShell prompt, type **Restart-Service DNS -Verbose**, and then press Enter.
3. Type **ping isatap**, and then press Enter.

   The name should resolve and you should receive four replies from 172.16.0.1.

▶ Task 4: Enable LON-DC1 as an ISATAP client

1. On LON-DC1, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Set-NetIsatapConfiguration -State Enabled
```

2. Type **ipconfig**, and then press Enter.
3. Verify that the Tunnel adapter for ISATAP has an IPv6 address on the 2001:db8:0:2/64 network.

   Notice that this address includes the IPv4 address of LON-DC1.

▶ Task 5: Test connectivity

1. On LON-SVR2, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
ping 2001:db8:0:2:0:5efe:172.16.0.10
```

2. In Server Manager, if necessary, click **Local Server**.
3. In the **Local Server Properties** dialog box, next to Ethernet, click **IPv6 enabled**.
4. In the Network Connections window, right-click **Ethernet**, and then click **Properties**.
5. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

6. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following DNS server addresses**.
7. In the **Preferred DNS server** box, type **2001:db8:0:2:0:5efe:172.16.0.10**, and then click **OK**.
8. In the **Ethernet Properties** dialog box, click **Close**.
9. Close the Network Connections window.
10. At the Windows PowerShell prompt, type **ping LON-DC1**, and then press Enter.

    Notice that four replies are received from LON-DC1.

Note: A ping from LON-DC1 to LON-SVR2 does not respond because the firewall configuration on LON-SVR2 blocks ping requests.

Results: After completing this exercise, you will have configured an ISATAP router on LON-RTR to allow communication between an IPv6–only network and an IPv4–only network.

▶ Prepare for the next module

After you finish the lab, revert the virtual machines back to their initial state.

To do this, complete the following steps.

1. On the host computer, start Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20410C-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410C-LON-SVR1, 20410C-LON-RTR** and **20410C-LON-SVR2**.