

Setting Up an IPv6 Test Lab

This appendix provides information about how you can use five computers to create a test lab to configure and test the IPv6 protocol for Windows. These instructions take you through setting up a test lab based on the Base Configuration test lab and deploying IPv6 using four server computers and one client computer. The resulting IPv6 test lab demonstrates default and configured IPv6 connectivity across an intranet and a simulated IPv4-only Internet.

Beyond the set of tasks described in this appendix, these instructions allow you to create a functioning IPv6-capable network. You can use this network to:

- Learn about and experiment with IPv6 features and functionality
- Explore network protocol and process specifics by capturing network traffic with a packet analyzer such as Network Monitor 3.4
- Aid in developing applications for IPv6 or modifying existing applications to work over both IPv4 and IPv6.



Important The following instructions are for configuring an IPv6 test lab using the minimum number of computers. Individual computers are needed to separate the services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network. Attempting to adapt this IPv6 test lab configuration to a pilot or production deployment can result in configuration or functionality issues.

IPv6 Test Lab Setup

In this test lab, IPv6 connectivity is deployed with:

- One computer running Windows Server 2012 (when using the Windows Server 2012-based Base Configuration test lab) or Windows Server 2008 R2 Enterprise Edition (when using the Windows Server 2008 R2-based Base Configuration test lab) named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, Dynamic Host Configuration Protocol (DHCP) server, and an IPv6 router.

- One intranet member server running Windows Server 2012 (when using the Windows Server 2012-based Base Configuration test lab) or Windows Server 2008 R2 Enterprise Edition (when using the Windows Server 2008 R2-based Base Configuration test lab) named EDGE1 that is configured as a 6to4 relay.
- One intranet member server running Windows Server 2012 (when using the Windows Server 2012-based Base Configuration test lab) or Windows Server 2008 R2 Enterprise Edition (when using the Windows Server 2008 R2-based Base Configuration test lab) named APP1 that is configured as a general application server.
- One stand-alone server running Windows Server 2012 (when using the Windows Server 2012-based Base Configuration test lab) or Windows Server 2008 R2 Enterprise Edition (when using the Windows Server 2008 R2-based Base Configuration test lab) named INET1 that is configured as an Internet DHCP server, DNS server, and web server.
- One roaming member client computer running Windows 8 (when using the Windows Server 2012-based Base Configuration test lab) or Windows 7 Enterprise or Ultimate (when using the Windows Server 2008 R2-based Base Configuration test lab) named CLIENT1.

The IPv6 test lab consists of three subnets isolated from your organization intranet that simulate the following:

- The Internet (131.107.0.0/24). Note that this subnet is not connected to the actual Internet.
- An intranet subnet named Corpnet (10.0.0.0/24), separated from the Internet by EDGE1.
- An additional intranet subnet named Corpnet2 (10.0.1.0/24), separated from the Corpnet subnet by DC1.

Computers on each subnet connect using a hub or switch. See Figure C-1 for the configuration of subnets and computers.

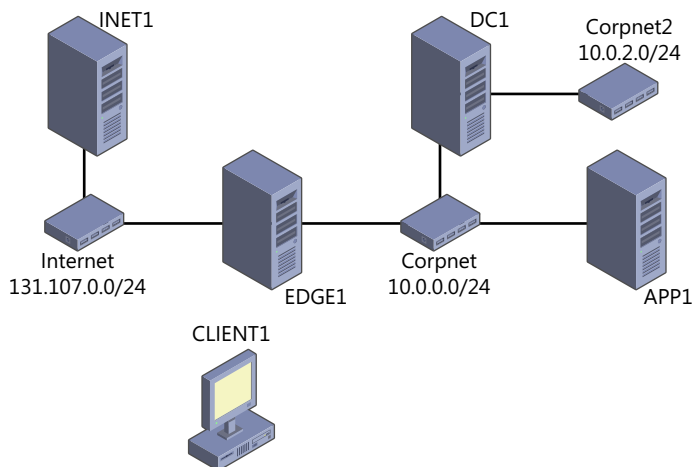


FIGURE C-1 The IPv6 test lab.

This appendix demonstrates the following:

- The default behavior of IPv6 and connectivity on an IPv4-only intranet
- IPv6-based intranet connectivity using the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- IPv6-based intranet connectivity using native IPv6 addressing
- IPv6 connectivity across a simulated IPv4-only Internet using 6to4

Optional exercises include setting up a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, demonstrating a DNS zone transfer over IPv6, and configuring the Corpnet and Corpnet2 subnets for IPv6-only operation.

Hardware and Software Requirements

The following are required components of the test lab:

- The product disc or files for Windows Server 2012 or Windows Server 2008 R2.
- The product disc or files for Windows 8 or Windows 7.
- Four computers that meet the minimum hardware requirements for Windows Server 2012 or Windows Server 2008 R2 Enterprise Edition. Two of these computers have two network adapters installed.
- One computer that meets the minimum hardware requirements for Windows 8 or Windows 7 Enterprise or Ultimate.

Steps for Configuring the IPv6 Test Lab

There are six steps to follow when setting up the IPv6 test lab.

1. Set up the Base Configuration test lab.

The IPv6 test lab requires either the Windows Server 2012 Base Configuration test lab or the Windows Server 2008 R2 Base Configuration test lab as its starting point.

You can get the Base Configuration Test Lab Guide for Windows Server 2012 and Windows 8 from <http://go.microsoft.com/fwlink/p/?Linkid=236358>.

You can get the Base Configuration Test Lab Guide for Windows Server 2008 R2 and Windows 7 from <http://go.microsoft.com/fwlink/p/?Linkid=198140>.

2. Configure the test lab for the Corpnet2 subnet.

Add the Corpnet2 subnet, and configure routing and DHCP so that all IPv4 locations on the Corpnet and Corpnet2 subnets are reachable.

3. Demonstrate default IPv6 connectivity.

Show the automatic configuration but limited connectivity of link-local IPv6 addresses.

4. Demonstrate ISATAP-based IPv6 connectivity.

Configure EDGE1 as an advertising ISATAP router, and show how ISATAP provides IPv6 connectivity across both subnets of the IPv4-only Contoso intranet.

5. Demonstrate native IPv6 connectivity.

Configure DC1 as an advertising and forwarding IPv6 router, and show the resulting native IPv6 connectivity across the Contoso intranet.

6. Demonstrate 6to4-based connectivity.

Configure EDGE1 as a 6to4 relay, and show the IPv6 connectivity between CLIENT1 on the Internet subnet and the Contoso intranet.



Note You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this appendix. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

This appendix provides steps for configuring the computers of the IPv6 test lab and demonstrating various types of IPv6 connectivity. The following sections provide details about how to perform these steps.

Step 1: Set Up the Base Configuration Test Lab

Set up the Base Configuration test lab for both the Corpnet and Internet subnets by using the procedures in the “Steps for Configuring the Corpnet Subnet” and “Steps for Configuring the Internet Subnet” sections of the Test Lab Guide: Base Configuration for Windows Server 2012 (<http://go.microsoft.com/fwlink/p/?LinkId=236358>) or the Test Lab Guide: Base Configuration (<http://go.microsoft.com/fwlink/p/?LinkId=198140>) (for Windows Server 2008 R2 and Windows 7).

Step 2: Configure the Test Lab for the Corpnet2 Subnet

To demonstrate the default IPv6 behavior and IPv6 connectivity between the subnets of an intranet, you must add another subnet, Corpnet2, to the Contoso intranet. Use the following procedures:

- Configure DC1.
- Configure EDGE1.

- Configure APP1.
- Verify IPv4 connectivity to the Corpnet2 subnet.

Configure DC1

In this procedure, we configure DC1 with an additional network adapter, with a DHCP scope for the new Corpnet2 subnet, and as an IPv4 router between the subnets.

1. Add another network adapter to DC1, and connect it to the Corpnet2 subnet.
2. From DC1:
 - a. For Windows Server 2008 R2: Click Start, right-click Network, and then click Properties.
 - b. For Windows Server 2012: Right-click the network icon in the notification area, and then click Open Network and Sharing Center.
3. In the Network and Sharing Center, click Change Adapter Settings.
4. In Network Connections, right-click the network connection that is connected to the Corpnet subnet, and then click Rename.
5. Type **Corpnet**, and then press Enter.
6. Right-click the network connection that is connected to the Corpnet2 subnet, and then click Rename.
7. Type **Corpnet2**, and then press Enter.
8. Right-click Corpnet2, and then click Properties.
9. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties.
10. Select Use The Following IP Address. In IP Address, type **10.0.2.1**. In Subnet Mask, type **255.255.255.0**.
11. Click Advanced, and then click the DNS tab.
12. In DNS Suffix For This Connection, type **corp.contoso.com**, click OK three times, and then click Close.
13. Close the Network Connections window.
14. To open the DHCP snap-in:
 - a. For Windows Server 2008 R2: click Start, point to Administrative Tools, and then click DHCP.
 - b. For Windows Server 2012: from the Start screen, click DHCP.
15. In the console tree, open dc1.corp.contoso.com/IPv4/Scope [10.0.0.0] Corpnet, right-click Scope Options, and then click Configure Options.

16. In the Available Options list, select 121 Classless Static Routes, and then click Add Route.
17. In the Add a Static Route dialog box, type **10.0.2.0** in Destination, type **255.255.255.0** in Network Mask, type **10.0.0.1** in Router, and then click OK twice.
18. In the console tree, right click IPv4, click New Scope, and then click Next.
19. On the Scope Name page, type **Corpnet2** in Name, and then click Next.
20. On the IP Address Range page, type **10.0.2.100** in Start IP Address, type **10.0.2.150** in End IP Address, type **24** in Length, and then click Next.
21. On the Add Exclusions And Delay page, click Next.
22. On the Lease Duration page, click Next.
23. On the Configure DHCP Options page, click Next.
24. On the Router (Default Gateway) page, type **10.0.2.1** in IP Address, click Add, and then click Next.
25. On the Domain Name And DNS Servers page, click 127.0.0.1, and then click Remove.
26. Type **10.0.0.1** in IP Address, click Add, and then click Next.
27. On the WINS Servers page, click Next.
28. On the Activate Scope page, click Next.
29. On the Completing The New Scope Wizard page, click Finish.
30. Close the DHCP snap-in.
31. To open a command prompt or Windows PowerShell:
 - a. For Windows Server 2008 R2: click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run As administrator.
 - b. For Windows Server 2012: on the taskbar, right-click Windows PowerShell, and then click Run As Administrator.
32. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv4 set interface Corpnet forwarding=enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv4 -Forwarding Enabled* Windows PowerShell command.
33. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv4 set interface Corpnet2 forwarding=enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias Corpnet2 -AddressFamily IPv4 -Forwarding Enabled* Windows PowerShell command.
34. Leave the Command Prompt or Windows PowerShell window open.

Configure EDGE1

In this procedure, we configure EDGE1 with a static route so that IPv4 locations on the new Corpnet2 subnet are reachable and enable file sharing, which allows incoming traffic for the Ping.exe tool.

1. On EDGE1, to open a command prompt or Windows PowerShell:
 - a. For Windows Server 2008 R2: click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run As administrator.
 - b. For Windows Server 2012: on the taskbar, right-click Windows PowerShell, and then click Run As Administrator.
2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv4 add route 10.0.2.0/24 interface=Corpnet nexthop=10.0.0.1**, and then press Enter. For Windows Server 2012, you can also use the *Add-NetRoute -DestinationPrefix 10.0.2.0/24 -InterfaceAlias Corpnet -NextHop 10.0.0.1 -AddressFamily IPv4* Windows PowerShell command.
3. In the Command Prompt or Windows PowerShell window, type **ping 10.0.2.1**, and then press Enter. There should be four successful replies.
4. Leave the Command Prompt or Windows PowerShell window open.
5. Right-click the network icon in the notification area, and then click Open Network And Sharing Center.
6. In the Network And Sharing Center window, click Change Advanced Sharing Settings.
7. Open Domain, click Turn On File And Printer Sharing, and then click Save Changes.
8. Close the Network And Sharing Center window.

Configure APP1

In this procedure, we configure APP1 with a static route so that IPv4 locations on the Corpnet2 subnet are reachable.

1. On APP1, to open a command prompt or Windows PowerShell:
 - a. For Windows Server 2008 R2: click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run As administrator.
 - b. For Windows Server 2012: on the taskbar, right-click Windows PowerShell, and then click Run As Administrator.
2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv4 add route 10.0.2.0/24 interface="Wired Ethernet Connection" nexthop=10.0.0.1** (for Windows Server 2012) or **netsh interface ipv4 add route 10.0.2.0/24 interface="Local Area Connection" nexthop=10.0.0.1** (for Windows Server 2008 R2) and then press Enter. For Windows Server 2012, you can also use the *Add-NetRoute -DestinationPrefix 10.0.2.0/24*

-InterfaceAlias "Wired Ethernet Connection" -NextHop 10.0.0.1 -AddressFamily IPv4 Windows PowerShell command.

3. In the Command Prompt or Windows PowerShell window, type **ping 10.0.2.1**, and then press Enter. There should be four successful replies.
4. Leave the Command Prompt or Windows PowerShell window open.

Verify IPv4 Connectivity to the Corpn2 Subnet

In this procedure, we verify that CLIENT1 can communicate with IPv4 locations on the Corpn2 subnet and, while on the Corpn2 subnet, can resolve names and communicate with locations on the Corpn subnet.

1. Connect CLIENT1 to the Corpn subnet.
2. To open a command prompt or Windows PowerShell:
 - a. For Windows Server 2008 R2: click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run As administrator.
 - b. For Windows Server 2012: on the taskbar, right-click Windows PowerShell, and then click Run As Administrator.
3. In the Command Prompt or Windows PowerShell window, type **ping 10.0.2.1**, and then press Enter. There should be four successful replies.
4. Connect CLIENT1 to the Corpn2 subnet.
5. In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. CLIENT1 should have an IPv4 address in the range 10.0.2.100 to 10.0.2.150, with a default gateway of 10.0.2.1 and the DNS Server address of 10.0.0.1.
6. In the Command Prompt or Windows PowerShell window, type **ping 10.0.0.2**, and then press Enter. There should be four successful replies.
7. In the Command Prompt or Windows PowerShell window, type **ping 10.0.0.3**, and then press Enter. There should be four successful replies.
8. In the Command Prompt or Windows PowerShell window, type **ping edge1**, and then press Enter. There should be a successful name resolution to the IPv4 address 10.0.0.2 and four successful replies.
9. In the Command Prompt or Windows PowerShell window, type **ping app1**, and then press Enter. There should be a successful name resolution to the IPv4 address 10.0.0.3 and four successful replies.

Step 3: Demonstrate Default IPv6 Connectivity

In the absence of advertising IPv6 routers, the Windows-based computers on the Corpnet and Corpnet2 subnets automatically configure link-local IPv6 addresses (beginning with "fe80"). However, these addresses have limited scope and function for connectivity and are not registered in DNS.

Use the following procedures to show the default IPv6 connectivity:

- Demonstrate default IPv6 configuration and link-local connectivity on the same subnet.
- Demonstrate link-local connectivity between subnets.

Demonstrate Default IPv6 Configuration and Link-local Connectivity on the Same Subnet

In this procedure, we demonstrate the default IPv6 configuration and link-local connectivity on the Corpnet subnet.

1. Connect CLIENT1 to the Corpnet subnet.
2. On DC1, to open the DNS snap-in:
 - a. For Windows Server 2008 R2: click Start, point to Administrative Tools, and then click DNS.
 - b. For Windows Server 2012: from the Start screen, click DNS.
3. In the console tree, open DNS\DC1\Forward Lookup Zones, and then click corp.contoso.com. Notice that there are no AAAA records corresponding to registered IPv6 addresses for DC1, CLIENT1, or APP1 listed in the contents pane.
4. Leave the DNS snap-in open.
5. On APP1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the IPv6 address assigned to the Wired Ethernet Connection or Local Area Connection interface that starts with "fe80". This is the automatically-assigned link-local address. Write the address here: _____
6. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the IPv6 address assigned to the Wired Ethernet Connection or Local Area Connection interface that starts with "fe80". Write the address here: _____
7. In the Command Prompt or Windows PowerShell window, type **ping APP1's link-local address** (from step 5), and then press Enter. You should see four successful replies.

Demonstrate Link-local Connectivity Between Subnets

In this procedure, we demonstrate the scope of functionality for link-local addresses.

1. Connect CLIENT1 to the Corpnet2 subnet.

2. In the Command Prompt or Windows PowerShell window, type **ping APP1's link-local address** (from step 5 of the previous procedure), and then press Enter. You should see four Destination host unreachable messages.
3. On APP1, in the Command Prompt or Windows PowerShell window, type **ping CLIENT1's link-local address** (from step 6 of the previous procedure), and then press Enter. You should see four Destination host unreachable messages.
4. On DC1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press ENTER. Notice the link-local IPv6 address assigned to the Corpnet2 interface. Write the address here: _____
5. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ping DC1's link-local address** (from step 4), and then press Enter. You should see four successful replies.

In their default configuration on the Contoso intranet, the computers running Windows automatically configure link-local IPv6 addresses that provide connectivity only to other IPv6 hosts on the same subnet. These link-local addresses are not registered in DNS.

Step 4: Demonstrate ISATAP-Based IPv6 Connectivity

ISATAP provides IPv6 connectivity across an IPv4-only intranet without having to configure native IPv6 addressing and routing. This step demonstrates configuring ISATAP for the Contoso intranet.

Use the following procedures to show ISATAP-based connectivity on the Contoso intranet:

- Configure ISATAP for the Contoso intranet.
- Demonstrate ISATAP connectivity on the Contoso intranet.

Configure ISATAP for the Contoso Intranet

In this procedure, we configure EDGE1 as an advertising ISATAP router.

1. On EDGE1, in the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 set interface isatap.corp.contoso.com advertise=enable**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias isatap.corp.contoso.com -AddressFamily IPv6 -Forwarding Enabled -Advertising Enabled* Windows PowerShell command.
2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 add route 2001:db8:0:abcd::/64 interface=isatap.corp.contoso.com publish=yes**, and then press Enter. For Windows Server 2012, you can also use the *Add-NetRoute -DestinationPrefix 2001:db8:0:abcd::/64 -InterfaceAlias isatap.corp.contoso.com -AddressFamily IPv6 -Publish Yes* Windows PowerShell command.
3. On DC1, in the Command Prompt or Windows PowerShell window, type **dnscmd /config /globalqueryblocklist wpad**, and then press Enter. This step removes the name "ISATAP" from the default global query block list.

4. In the console tree of the DNS snap-in, right-click DNS, point to All Tasks, and then click Restart.
5. In the console tree of the DNS snap-in, open DNS\DC1\Forward Lookup Zones, right-click corp.contoso.com, and then click New Host (A Or AAAA).
6. In the New Host dialog box, type **isatap** in Name, type **10.0.0.2** in IP Address, click Add Host, click OK, and then click Done.

Demonstrate ISATAP Connectivity on the Contoso Intranet

In this procedure, we demonstrate the configuration of ISATAP addresses on Contoso computers, DNS registration of ISATAP addresses, and ISATAP-based connectivity across the Corpnet and Corpnet2 subnets.

1. Connect CLIENT1 to the Corpnet subnet.
2. In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the new IPv6 address beginning with "2001" that is assigned to the interface named isatap.corp.contoso.com. This address is based on the 2001:db8:0:abcd::/64 prefix that EDGE1 is advertising as an ISATAP router.
3. On APP1, in the Command Prompt or Windows PowerShell window, type **net stop iphlpsvc**, press Enter, type **net start iphlpsvc**, and then press Enter.
4. In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the IPv6 address 2001:db8:0:abcd:0:5efe:10.0.0.3 that is assigned to the isatap.corp.contoso.com interface.
5. On DC1, in the Command Prompt or Windows PowerShell window, type **net stop iphlpsvc**, press Enter, type **net start iphlpsvc**, and then press Enter.
6. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ping 2001:db8:0:abcd:0:5efe:10.0.0.2**, and then press Enter. You should see four successful replies.
7. In the Command Prompt or Windows PowerShell window, type **ping 2001:db8:0:abcd:0:5efe:10.0.0.3**, and then press Enter. You should see four successful replies.
8. In the Command Prompt or Windows PowerShell window, type **ipconfig /flushdns**, and then press Enter.
9. In the Command Prompt or Windows PowerShell window, type **ping app1**, and then press Enter. You should see four successful replies. Notice that CLIENT1 is now using 2001:db8:0:abcd:0:5efe:10.0.0.3, the ISATAP-based IPv6 address of APP1, rather than the IPv4 address 10.0.0.3.
10. In the Command Prompt or Windows PowerShell window, type **ping edge1**, and then press Enter. You should see four successful replies. Notice that CLIENT1 is now using 2001:db8:0:abcd:0:5efe:10.0.0.2, the ISATAP-based IPv6 address, rather than the IPv4 address 10.0.0.2.

11. Connect CLIENT1 to the CorpNet2 subnet.
12. In the Command Prompt or Windows PowerShell window, type **ping 2001:db8:0:abcd:0:5efe:10.0.0.3**, and then press Enter. You should see four successful replies.
13. On EDGE1, in the Command Prompt or Windows PowerShell window, type **ping client1**, and then press Enter. You should see four successful replies.

You can use ISATAP for IPv6 addressing and connectivity across an IPv4-only intranet that is not possible with link-local addresses. However, ISATAP should be used in a limited capacity for testing while you deploy native IPv6 capabilities.

Step 5: Demonstrate Native IPv6 Connectivity

Use the following procedures to show native IPv6 connectivity across the Contoso intranet:

- Remove ISATAP connectivity
- Configure native IPv6 connectivity
- Demonstrate native IPv6 connectivity

Remove ISATAP Connectivity

In this procedure, we remove the ISATAP configuration, returning the Contoso intranet to link-local IPv6 connectivity.

1. On EDGE1, in the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 set interface isatap.corp.contoso.com advertise=disabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias isatap.corp.contoso.com -AddressFamily IPv6 -Forwarding Enabled -Advertising Disabled* Windows PowerShell command.
2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 delete route 2001:db8:0:abcd::/64 interface=isatap.corp.contoso.com**, and then press Enter. For Windows Server 2012, you can also use the *Remove-NetRoute -DestinationPrefix 2001:db8:0:abcd::/64 -InterfaceAlias isatap.corp.contoso.com -AddressFamily IPv6* Windows PowerShell command.
3. On DC1, in the console tree of the DNS snap-in, open DNS\DC1\Forward Lookup Zones\corp.contoso.com.
4. In the details pane, right-click the isatap A record, click Delete, and then click Yes.
5. In the Command Prompt or Windows PowerShell window, type **net stop iphlpsvc**, press Enter, type **net start iphlpsvc**, press Enter, type **ipconfig /registerdns**, and then press Enter.
6. On EDGE1, in the Command Prompt or Windows PowerShell window, type **net stop iphlpsvc**, press Enter, type **net start iphlpsvc**, press Enter, type **ipconfig /registerdns**, and then press Enter.

7. In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the link-local IPv6 address that is assigned to the Corpnet interface. Write the address here: _____
8. On APP1, in the Command Prompt or Windows PowerShell window, type **net stop iphlpsvc**, press Enter, type **net start iphlpsvc**, press Enter, type **ipconfig /registerdns**, and then press Enter.
9. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **net stop iphlpsvc**, press Enter, type **net start iphlpsvc**, press Enter, type **ipconfig /registerdns**, and then press Enter.
10. On DC1, refresh the details pane of the DNS snap-in and verify that there are no IPv6 addresses (AAAA records) registered for CLIENT1, DC1, and APP1.

Configure Native IPv6 Connectivity

In this procedure, we configure DC1 as an advertising and forwarding IPv6 router that advertises native IPv6 prefixes to the Corpnet and Corpnet2 subnets. For this procedure, you will need the link-local address of EDGE1's Corpnet interface, as recorded in step 7 of the previous procedure.

1. On DC1, in the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 set interface Corpnet forwarding=enabled advertise=enabled advertisedefaultroute=enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -Forwarding Enabled -Advertising Enabled -AdvertiseDefaultRoute Enabled* Windows PowerShell command.
2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 set interface Corpnet2 forwarding=enabled advertise=enabled advertisedefaultroute=enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias Corpnet2 -AddressFamily IPv6 -Forwarding Enabled -Advertising Enabled -AdvertiseDefaultRoute Enabled* Windows PowerShell command.
3. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 add route 2001:db8::/64 interface=Corpnet publish=yes**, and then press Enter. For Windows Server 2012, you can also use the *Add-NetRoute -DestinationPrefix 2001:db8::/64 -InterfaceAlias Corpnet -AddressFamily IPv6 -Publish Yes* Windows PowerShell command.
4. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 add route 2001:db8:0:2::/64 interface=Corpnet2 publish=yes**, and then press Enter. For Windows Server 2012, you can also use the *Add-NetRoute -DestinationPrefix 2001:db8:0:2::/64 -InterfaceAlias Corpnet2 -AddressFamily IPv6 -Publish Yes* Windows PowerShell command.
5. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 add route ::/0 interface=Corpnet nexthop=link-local address of EDGE1's Corpnet interface publish=yes** (from step 7 of the previous procedure), and then press Enter. For Windows Server 2012, you can also use the *Add-NetRoute -DestinationPrefix ::/0 -InterfaceAlias Corpnet*

-*NextHop* link-local address of EDGE1's Corpnet interface -*AddressFamily IPv6* -*Publish Yes*
Windows PowerShell command.

6. In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the new IPv6 address starting with "2001:db8::" assigned to the Corpnet interface and the address starting with "2001:db8:0:2" assigned to the Corpnet2 interface. Notice the link-local address of the Corpnet interface. Write the address here:

7. On APP1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the new IPv6 address starting with "2001:db8::" and the default gateway of DC1's link-local address, as recorded in step 6.
8. Connect CLIENT1 to the Corpnet subnet.
9. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the new IPv6 address starting with "2001:db8::" and the default gateway of DC1's link-local address, as recorded in step 6.
10. On DC1, refresh the details pane of the DNS snap-in and verify there are new AAAA records registered for CLIENT1, EDGE1, APP1, and DC1.

Demonstrate Native IPv6 Connectivity

In this procedure, we demonstrate native IPv6 connectivity on both the Corpnet and Corpnet2 subnets.

1. Connect CLIENT1 to the Corpnet2 subnet.
2. On APP1, in the Command Prompt or Windows PowerShell window, type **ipconfig /flushdns**, and then press Enter.
3. In the Command Prompt or Windows PowerShell window, type **ping client1**, and then press Enter. You should see a successful name resolution to CLIENT1's IPv6 address on the Corpnet2 subnet (starting with "2001:db8:0:2") and four successful replies.
4. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ipconfig /flushdns**, and then press Enter.
5. In the Command Prompt or Windows PowerShell window, type **ping edge1**, and then press Enter. You should see a successful name resolution to EDGE1's IPv6 address on the Corpnet subnet (starting with "2001:db8::") and four successful replies.
6. In the Command Prompt or Windows PowerShell window, type **ping app1.corp.contoso.com**, and then press Enter. You should see four successful replies. Notice that CLIENT1 is using APP1's IPv6 address starting with "2001:db8::", rather than the IPv4 address 10.0.0.3.
7. From the taskbar, click the Internet Explorer icon.

8. In the Address bar, type **http://app1.corp.contoso.com/**, and then press Enter. You should see the default IIS 7 webpage for APP1.
9. For the Windows Server 2008 R2-based test lab, in the Address bar, type **https://app1.corp.contoso.com/**, and then press Enter. You should see the default IIS 7 webpage for APP1.
10. To view the \\app1\\Files shared folder:
 - a. For Windows Server 2008 R2: click Start, type **\\app1\\Files**, and then press Enter.
 - b. For Windows Server 2012: from Internet Explorer, in the Address bar, type **\\app1\\Files**, and then press Enter.
11. You should see the contents of the Files shared folder.
12. Double-click the Example.txt file. You should see the contents of the Example.txt file.
13. Close the Example.txt file and the Files shared folder window.

Step 6: Demonstrate 6to4-Based Connectivity

Computers running Windows use the 6to4 transition technology for IPv6 connectivity across the IPv4-only Internet. In this step, you configure EDGE1 as a 6to4 relay and demonstrate how CLIENT1 uses it to reach IPv6 locations on the Contoso intranet.



Important This step is not a recommended practice for real-world deployments because it creates a direct channel of communication between Internet and intranet hosts. A variation of this configuration is used by DirectAccess in Windows Server 2012, Windows Server 2008 R2, Windows 8, and Windows 7. However, the incoming traffic to the DirectAccess server destined for the intranet is authenticated and protected with Internet Protocol security (IPsec).

Use the following procedures to show 6to4-based connectivity across the Internet subnet:

- Configure 6to4-based connectivity
- Demonstrate 6to4-based connectivity

Configure 6to4-Based Connectivity

In this procedure, we configure EDGE1 as a 6to4 relay.

1. On EDGE1, in the Command Prompt or Windows PowerShell window, type **netsh interface 6to4 set state enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-Net6to4Configuration -State Enabled* Windows PowerShell command.

2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 set interface "6TO4 Adapter" forwarding=enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias "6TO4 Adapter" -AddressFamily IPv6 -Forwarding Enabled* Windows PowerShell command.
3. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 set interface Corpnet forwarding=enabled**, and then press Enter. For Windows Server 2012, you can also use the *Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -Forwarding Enabled* Windows PowerShell command.
4. On INET, to open the DNS snap-in:
 - a. For Windows Server 2008 R2: click Start, point to Administrative Tools, and then click DNS.
 - b. For Windows Server 2012: from the Start screen, click DNS.
5. In the console tree, open DNS\INET1.
6. Right-click Forward Lookup Zones, click New Zone, and then click Next.
7. On the Zone Type page, click Next.
8. On the Zone Name page, type **ipv6.microsoft.com** in Zone Name, and then click Next.
9. On the Dynamic Update page, click Do Not Allow Dynamic Updates, click Next, and then click Finish.
10. In the console tree, right-click the ipv6.microsoft.com zone, and then click New Host (A or AAAA).
11. In the New Host dialog box, type **6to4** in Name, type **131.107.0.2** in IP Address, click Add Host, click OK, and then click Done.

Demonstrate 6to4-Based Connectivity

In this procedure, we demonstrate 6to4-based IPv6 connectivity between CLIENT1 on the Internet subnet and computers on the Contoso intranet.

1. On EDGE1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press ENTER. Notice the 2002:836b:2::836b:2 and 2002:836b:3::836b:3 IPv6 addresses assigned to the 6TO4 Adapter. These are 6to4 addresses that EDGE1 automatically assigns based on the public IPv4 addresses 131.107.0.2 and 131.107.0.3, which are assigned to the Internet interface.
2. Connect CLIENT1 to the Internet subnet.
3. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press ENTER. Notice the address starting with "2002:836b:" assigned to the 6TO4 Adapter. This is a 6to4 address corresponding to its public IPv4 address. Also notice that the default gateway for the 6TO4 Adapter is set to 2002:836b:2::836b:2, a 6to4 address assigned to EDGE1.

4. On APP1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the address starting with "2001:db8::" assigned to the Wired Ethernet Connection or Local Area Connection interface. Write the address here: _____
5. On DC1, in the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice the address starting with "2001:db8:0:2:" assigned to the Corpnet2 interface. Write the address here: _____
6. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ping APP1's IPv6 address** (from step 4), and then press Enter. You should see four successful replies.
7. In the Command Prompt or Windows PowerShell window, type **ping DC1's IPv6 address on the Corpnet 2 interface** (from step 5), and then press Enter. You should see four successful replies.

The 6to4 transition technology and EDGE1 acting as a 6to4 relay allows CLIENT1 to reach locations on the IPv6-capable Contoso intranet over the IPv4-only Internet subnet.

Snapshot the Configuration

To save this configuration of the IPv6 test lab so that you can quickly return to a working IPv6 configuration for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots IPv6. If your lab uses physical computers, create disk images to save the IPv6 test lab configuration.

Additional IPv6 Test Lab Exercises

The following sections describe additional exercises that you can do with the IPv6 test lab.

Demonstrate DHCPv6

This section describes how to configure DHCPv6 for the Contoso intranet. You configure DC1 as a DHCPv6 server and modify its role as an advertising router for the Corpnet and Corpnet2 subnets.

Configure DC1 as the DHCPv6 Server

1. On DC1, to open a command prompt or Windows PowerShell:
 - a. For Windows Server 2008 R2: click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run As Administrator.

- b. For Windows Server 2012: on the taskbar, right-click Windows PowerShell, and then click Run As Administrator.
2. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 add address Corpnet 2001:db8::1111**, and then press Enter. For Windows Server 2012, you can also use the *New-NetIPAddress -InterfaceAlias Corpnet -IPAddress 2001:db8::1111* Windows PowerShell command.
3. In the Command Prompt or Windows PowerShell window, type **netsh interface ipv6 add address Corpnet2 2001:db8:0:2::2222**, and then press Enter. For Windows Server 2012, you can also use the *New-NetIPAddress -InterfaceAlias Corpnet2 -IPAddress 2001:db8:0:2::2222* Windows PowerShell command. The DHCP Server service needs static IPv6 addresses on its interfaces to service DHCPv6 requests from IPv6 hosts.
4. On DC1, to open the DHCP snap-in:
 - a. For Windows Server 2008 R2: click Start, point to Administrative Tools, and then click DHCP.
 - b. For Windows Server 2012: from the Start screen, click DHCP.
5. In the console tree of the DHCP snap-in, open dc1.corp.contoso.com, right-click IPv6, and then click New Scope.
6. On the Welcome page, click Next.
7. On the Scope Name page, type **Corpnet** in Name, and then click Next.
8. On the Scope Prefix page, type **2001:db8::** in Prefix, and then click Next.
9. On the Add Exclusions page, click Next.
10. On the Scope Lease page, click Next.
11. On the Completing page, click No in Activate Scope Now, and then click Finish.
12. In the console tree of the DHCP snap-in, right-click IPv6, and then click New Scope.
13. On the Welcome page, click Next.
14. On the Scope Name page, type **Corpnet2** in Name, and then click Next.
15. On the Scope Prefix page, type **2001:db8:0:2::** in Prefix, and then click Next.
16. On the Add Exclusions page, click Next.
17. On the Scope Lease page, click Next.
18. On the Completing page, click No in Activate Scope Now, and then click Finish.
19. In the Command Prompt or Windows PowerShell window, run the following commands:

```
netsh interface ipv6 set interface Corpnet managedaddress=enable  
otherstateful=enable
```

```
netsh interface ipv6 set interface Corpnet2 managedaddress=enable  
otherstateful=enable
```

For Windows Server 2012, you can also use the following Windows PowerShell commands:

```
Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -ManagedAddressConfiguration  
Enabled -OtherStatefulConfiguration Enabled
```

```
Set-NetIPInterface -InterfaceAlias Corpnet2 -AddressFamily IPv6 -ManagedAddress  
Configuration Enabled -OtherStatefulConfiguration Enabled
```

- 20.** Connect CLIENT1 to the Corpnet subnet.
- 21.** In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice that there is an address starting with "2001:db8::" assigned to the Wired Ethernet Connection or Local Area Connection adapter. DC1 is still advertising stateless address prefixes on the Corpnet and Corpnet2 subnets.
- 22.** On DC1, in the console tree of the DHCP snap-in, right-click Scope [2001:db8::] Corpnet, and then click Activate.
- 23.** In the console tree of the DHCP snap-in, right-click Scope [2001:db8:0:2::] Corpnet2, and then click Activate.

Demonstrate the Use of DHCPv6 by CLIENT1

- 1.** Connect CLIENT1 to the Corpnet2 subnet.
- 2.** In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter.
- 3.** Notice that there are two IPv6 addresses beginning with "2001:db8:0:2" assigned to the Wired Ethernet Connection or Local Area Connection adapter.
- 4.** In the Command Prompt or Windows PowerShell window, type **ipconfig /all**, and then press Enter.
- 5.** Notice that one of the IPv6 addresses beginning with "2001:db8:0:2" has Lease Obtained and Lease Expires fields after the address. This indicates that this address was assigned by a DHCPv6 server.
- 6.** In the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.
- 7.** In the Command Prompt or Windows PowerShell window, type **ipconfig /all**, and then press Enter.

8. Notice that the Lease Obtained and Lease Expires fields for the DHCPv6-assigned address have changed to new times (from step 5).
9. Notice that 10.0.0.1 is the only DNS server assigned to the Wired Ethernet Connection or Local Area Connection adapter.
10. On DC1, in the DHCP snap-in, right-click Server Options, and then click Configure Options.
11. On the General tab, select 0023 DNS Recursive Name Server IPv6 Addresses, type **2001:db8::1111** in New IPv6 Address, click Add, and then click OK.
12. On CLIENT1, in the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.
13. In the Command Prompt or Windows PowerShell window, type **ipconfig /all**, and then press Enter. Notice that the DNS servers assigned to the Wired Ethernet Connection or Local Area Connection adapter now include 2001:db8::1111.

With this new configuration, CLIENT1 can obtain native IPv6 addresses on the Contoso intranet from a DHCPv6 server in addition to the router advertisements sent by the native IPv6 router for the Corpnet and Corpnet2 subnets (DC1). CLIENT1 can also obtain the IPv6 address of its DNS server (DC1). Notice that CLIENT1 is still configuring its default router from the router advertisements sent by the native IPv6 router (DC1). There is no DHCPv6 option to configure the default gateway.

Hosts on the Corpnet and Corpnet2 configure two IPv6 addresses: one that is stateless from DC1 as an advertising router and one that is stateful from DC1 as the DHCPv6 server. Because there is no way to clear the Autonomous flag in an advertised route for a Windows-based advertising router, in the IPv6 test lab we can configure one of the following configurations:

- Allow DC1 to advertise the 2001:db8::/64 and 2001:db8:0:2::/64 routes, resulting in two IPv6 addresses, but hosts will have local-subnet routes of 2001:db8::/64 when attached to the Corpnet subnet and 2001:db8:0:2::/64 when connected to the Corpnet2 subnet.
- Prevent DC1 from advertising the 2001:db8::/64 and 2001:db8:0:2::/64 routes, resulting in a single IPv6 address (stateful from DHCPv6), but hosts will not have local-subnet routes of 2001:db8::/64 when attached to the Corpnet subnet and 2001:db8:0:2::/64 when connected to the Corpnet2 subnet. Without a local subnet route, hosts must rely on a Redirect message from the subnet router (DC1) to communicate with hosts on the same subnet. This is the least desirable configuration.

Restore the IPv6 Test Lab

If you are running the IPv6 test lab in a virtual environment, you can discard the changes made by these procedures by restoring the previously made snapshots of the VMs for all of the computers in the test lab. Alternatively, if you would like return to this working configuration using DHCPv6, you can create a new set of snapshots before restoring the previously made snapshots.

To manually restore the configuration of the IPv6 test lab, perform the following procedure.

1. On DC1, in the Command Prompt or Windows PowerShell window, run the following commands:

```
netsh interface ipv6 del address Corpnet 2001:db8::1111
```

```
netsh interface ipv6 del address Corpnet2 2001:db8:0:2::2222
```

```
netsh interface ipv6 set interface Corpnet managedaddress=disable  
otherstateful=disable
```

```
netsh interface ipv6 set interface Corpnet2 managedaddress=disable  
otherstateful=disable
```

For Windows Server 2012, you can also use the following Windows PowerShell commands:

```
Remove-NetIPAddress -InterfaceAlias Corpnet -IPAddress 2001:db8::1111
```

```
Remove-NetIPAddress -InterfaceAlias Corpnet2 -IPAddress 2001:db8:0:2::2222
```

```
Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -ManagedAddressConfiguration  
Disabled -OtherStatefulConfiguration Disabled
```

```
Set-NetIPInterface -InterfaceAlias Corpnet2 -AddressFamily IPv6 -ManagedAddress  
Configuration Disabled -OtherStatefulConfiguration Disabled
```

2. In the DHCP console tree, click Server Options.
3. In the details pane, right-click 00023 DNS Recursive Name, click Delete, and then click OK.
4. In the DHCP console tree, right-click Scope [2001:db8:] Corpnet, click Delete, and then click Yes twice.
5. In the DHCP console tree, right-click Scope [2001:db8:0:2:] Corpnet2, click Delete, and then click Yes twice.

Demonstrate DNS Zone Transfers over IPv6

This section describes how to configure and demonstrate DNS zone transfers over IPv6. You configure APP1 as a DNS server, configure APP1 as a secondary DNS server for the corp.contoso.com domain (using the IPv6 address of DC1), and then demonstrate the zone transfer over the IPv6 address.

Configure APP1 as a DNS Server

To configure DC1 to allow zone transfers to APP1's IPv6 address:

1. On DC1, to open the DNS snap-in:
 - a. For Windows Server 2008 R2: click Start, point to Administrative Tools, and then click DNS.
 - b. For Windows Server 2012: from the Start screen, click DNS.

2. In the console tree, double-click DC1, double-click Forward Lookup Zones, right-click corp.contoso.com, and then click Properties.
3. Click the Zone Transfers tab, click Only To The Following Servers, and then click Edit.
4. In Allow Zone Transfers, click <Click Here To Add An IP Address Or DNS Name>, type **APP1**, and then press Tab. The wizard displays both the IPv4 and IPv6 addresses of DC1.
5. Click the 10.0.0.3 address, click Delete, and then click OK twice.

To configure APP1 as a DNS server:

1. On APP1, to open Server Manager:
 - a. For Windows Server 2008 R2: From the task bar, click the Server Manager icon.
 - b. For Windows Server 2012: From the task bar or Start screen, click the Server Manager icon.
2. From the console tree of Server Manager, click Roles.
3. In the details pane, click Add Roles.
4. On the Before You Begin page, click Next.
5. On the Select Server Roles page, click DNS Server, and then click Next.
6. On the DNS Server page, click Next.
7. On the Confirm Installation Selections page, click Install.
8. On the Installation Results page, click Close.

Demonstrating DNS Zone Transfers over IPv6

To create a secondary zone for corp.contoso.com on APP1 and demonstrate the zone transfer from DC1:

1. On APP1, to open the DNS snap-in:
 - a. For Windows Server 2008 R2: click Start, point to Administrative Tools, and then click DNS.
 - b. For Windows Server 2012: from the Start screen, click DNS.
2. In the console tree, open APP1, right-click Forward Lookup Zones, and then click New Zone.
3. On the Welcome to the New Zone Wizard page, click Next.
4. On the Zone Type page, click Secondary zone, and then click Next.
5. On the Zone Name page, type **corp.contoso.com**, and then click Next.
6. On the Master DNS Servers page, type **DC1**, and then press Tab. The wizard displays both the IPv4 and IPv6 addresses of DC1.

7. Click the 10.0.0.1 address, click Delete, and then click Next.
8. On the Completing The New Zone Wizard page, click Finish.
9. In the console tree, click the corp.contoso.com domain. Note that it contains the records of the corp.contoso.com domain. The zone transfer was sent over IPv6 between DC1 and APP1.

Restore the IPv6 Test Lab

You can discard the changes made by these procedures by restoring the previously made snapshots of the VMs for all of the computers in the test lab. To manually restore the configuration of the IPv6 test lab, perform the following procedure.

1. On DC1, from the console tree of the DNS Manager snap-in, double-click DC1, double-click Forward Lookup Zones, right-click corp.contoso.com, and then click Properties.
2. Click the Zone Transfers tab, clear Allow zone transfers, and then click OK.
3. On APP1, from the console tree of Server Manager, click Roles.
4. In the details pane, click Remove Roles.
5. On the Before You Begin page, click Next.
6. On the Remove Server Roles page, clear DNS Server, and then click Next.
7. On the Confirm Removal Selections page, click Remove.
8. On the Installation Results page, click Close, and restart APP1.

Demonstrate an IPv6-Only Environment

This section describes how to configure the Corpnet and Corpnet2 subnets for IPv6-only connectivity. You configure DC1 as a DHCPv6 server and its role as an advertising router for the Corpnet and Corpnet2 subnets, disable IPv4 on all intranet hosts, and then show that all network, Active Directory, and application connectivity works in the IPv6-only environment.

Configure and Demonstrate an IPv6-Only Intranet

To configure DC1 as the DHCPv6 server:

1. On DC1, to open a command prompt or Windows PowerShell:
 - a. For Windows Server 2008 R2: Click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run As Administrator.
 - b. For Windows Server 2012: On the taskbar, right-click Windows PowerShell, and then click Run As Administrator.

2. In the Command Prompt or Windows PowerShell window, type the following commands:

```
netsh interface ipv6 add address Corpnet 2001:db8::1111
```

```
netsh interface ipv6 add address Corpnet2 2001:db8:0:2::2222
```

```
netsh interface ipv6 set interface Corpnet managedaddress=enable  
otherstateful=enable
```

```
netsh interface ipv6 set interface Corpnet2 managedaddress=enable  
otherstateful=enable
```

For Windows Server 2012, you can also use the following Windows PowerShell commands:

```
New-NetIPAddress -InterfaceAlias Corpnet -IPAddress 2001:db8::1111
```

```
New-NetIPAddress -InterfaceAlias Corpnet2 -IPAddress 2001:db8:0:2::2222
```

```
Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -ManagedAddressConfiguration  
Enabled -OtherStatefulConfiguration Enabled
```

```
Set-NetIPInterface -InterfaceAlias Corpnet2 -AddressFamily IPv6 -ManagedAddress  
Configuration Enabled -OtherStatefulConfiguration Enabled
```

3. On DC1, to open the DHCP snap-in:
 - a. For Windows Server 2008 R2: Click Start, point to Administrative Tools, and then click DHCP.
 - b. For Windows Server 2012: From the Start screen, click DHCP.
4. In the console tree of the DHCP snap-in, open dc1.corp.contoso.com, right-click IPv6, and then click New Scope.
5. On the Welcome page, click Next.
6. On the Scope Name page, type **Corpnet** in Name, and then click Next.
7. On the Scope Prefix page, type **2001:db8::** in Prefix, and then click Next.
8. On the Add Exclusions page, click Next.
9. On the Scope Lease page, click Next.
10. On the Completing page, click Finish.
11. In the console tree of the DHCP snap-in, right-click IPv6, and then click New Scope.
12. On the Welcome page, click Next.
13. On the Scope Name page, type **Corpnet2** in Name, and then click Next.
14. On the Scope Prefix page, type **2001:db8:0:2::** in Prefix, and then click Next.

15. On the Add Exclusions page, click Next.
16. On the Scope Lease page, click Next.
17. On the Completing page, click Finish.
18. In the console tree of the DHCP snap-in, right-click Server Options, and then click Configure Options.
19. On the General tab, select 0023 DNS Recursive Name Server IPv6 Addresses, type **2001:db8::1111** in New IPv6 Address, click Add, and then click OK.
20. In the Command Prompt or Windows PowerShell window, run the following command:

netsh interface ipv6 set interface Corpnet advertising=enabled forwarding=enabled otherstateful=enabled advertisedefaultroute=enabled

For Windows Server 2012, you can also use the following Windows PowerShell command:

Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -Advertising Enabled -Forwarding Enabled -OtherStatefulConfiguration Enabled -AdvertiseDefaultRoute Enabled

21. Connect CLIENT1 to the Corpnet subnet.
22. In the Command Prompt or Windows PowerShell window, type **ipconfig /all**, and then press Enter. Notice the IPv6 addresses beginning with "2001:db8::" are assigned to the Wired Ethernet Connection or Local Area Connection adapter and that the DNS servers assigned to the Wired Ethernet Connection or Local Area Connection adapter now include 2001:db8::1111.

To configure the Contoso intranet for IPv6-only and demonstrate connectivity:

1. On CLIENT1, right-click the network icon in the notification area, click Network And Sharing Center, click Change Adapter Settings, right-click Wired Ethernet Connection Or Local Area Connection, and then click Properties.
2. In This Connection Uses The Following Items, clear Internet Protocol Version 4 (TCP/IPv4), and then click OK.
3. In the Command Prompt or Windows PowerShell window, type **ipconfig /all**, and then press Enter. Notice that all IPv4 address configuration for the Wired Ethernet Connection Or Local Area Connection interface has been removed.
4. On DC1, right-click the network icon in the notification area, click Network And Sharing Center, click Change Adapter Settings, right-click Corpnet, and then click Properties.
5. In This Connection Uses The Following Items, clear Internet Protocol Version 4 (TCP/IPv4), and then click OK.
6. Right-click Corpnet2, and then click Properties.
7. In This Connection Uses The Following Items, clear Internet Protocol Version 4 (TCP/IPv4), and then click OK.

8. On APP1, right-click the network icon in the notification area, click Network And Sharing Center, click Change Adapter Settings, right-click Wired Ethernet Connection Or Local Area Connection, and then click Properties.
9. In This Connection Uses The Following Items, clear Internet Protocol Version 4 (TCP/IPv4), and then click OK.
10. In the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.
11. In the Command Prompt or Windows PowerShell window, type **ipconfig /all**, and then press ENTER. Verify that APP1 has a DHCPv6-assigned IPv6 address and DNS server (2001:db8::1111).
12. On EDGE1, right-click the network icon in the notification area, click Network And Sharing Center, click Change Adapter Settings, right-click Corpnet, and then click Properties.
13. In This Connection Uses The Following Items, clear Internet Protocol Version 4 (TCP/IPv4), and then click OK.
14. In the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.
15. Connect CLIENT1 to the Corpnet2 subnet.
16. On CLIENT1, log off and then log on using the CORP\User1 account.
17. In the Command Prompt or Windows PowerShell window, type **ipconfig**, and then press Enter. Notice that there is no longer an IPv4 address assigned to the Wired Ethernet Connection or Local Area Connection adapter.
18. In the Command Prompt or Windows PowerShell window, type **nltest /dsgetdc: /force**, and then press Enter. Notice that the domain controller found is DC1 via its IPv6 address.
19. In the Command Prompt or Windows PowerShell window, type **ping edge1**, and then press Enter. You should see a successful name resolution to EDGE1's IPv6 address on the Corpnet subnet (starting with "2001:db8::") and four successful replies.
20. In the Command Prompt or Windows PowerShell window, type **ping app1.corp.contoso.com**, and then press Enter. You should see four successful replies.
21. From the taskbar, click the Internet Explorer icon.
22. In the Address bar, type **http://app1.corp.contoso.com/**, and then press Enter. You should see the default IIS 7 webpage for APP1.
23. For the Windows Server 2008 R2-based test lab, in the Address bar, type **https://app1.corp.contoso.com/**, and then press Enter. You should see the default IIS 7 webpage for APP1.

24. To view the \\app1\\Files shared folder:
 - a. For Windows Server 2008 R2: click Start, type **\\app1\\Files**, and then press Enter.
 - b. For Windows Server 2012: from Internet Explorer, in the Address bar, type **\\app1\\Files**, and then press Enter.
25. You should see the contents of the Files shared folder.
26. Double-click the Example.txt file. You should see the contents of the Example.txt file.
27. Close the example.txt file and the Files shared folder window.

With this new configuration, all network, Active Directory, and application traffic uses only IPv6 and works the same as in the original Base Configuration test lab, which is IPv4-only.

Restore the IPv6 Test Lab

If you are running the IPv6 test lab in a virtual environment, you can discard the changes made by these procedures by restoring the previously made snapshots of the VMs for all of the computers in the test lab. Alternatively, if you would like to return to this working configuration using IPv6-only, you can create a new set of snapshots before restoring the previously made snapshots.

To manually restore the configuration of the IPv6 test lab, perform the following procedure:

1. On DC1, in the Network Connections window, right-click Corpnet, and then click Properties.
2. In This Connection Uses The Following Items, select Internet Protocol Version 4 (TCP/IPv4), and then click OK.
3. Right-click Corpnet2, and then click Properties.
4. In This Connection Uses The Following Items, select Internet Protocol Version 4 (TCP/IPv4), and then click OK.
5. In the Command Prompt or Windows PowerShell window, run the following commands:

```
netsh interface ipv6 del address Corpnet 2001:db8::1111
```

```
netsh interface ipv6 del address Corpnet2 2001:db8:0:2::2222
```

```
netsh interface ipv6 set interface Corpnet managedaddress=disable  
otherstateful=disable
```

```
netsh interface ipv6 set interface Corpnet2 managedaddress=disable  
otherstateful=disable
```

For Windows Server 2012, you can also use the following Windows PowerShell commands:

```
Remove-NetIPAddress -InterfaceAlias Corpnet -IPAddress 2001:db8::1111
```

```
Remove-NetIPAddress -InterfaceAlias Corpnet2 -IPAddress 2001:db8:0:2::2222
```

Set-NetIPInterface -InterfaceAlias Corpnet -AddressFamily IPv6 -ManagedAddressConfiguration Disabled -OtherStatefulConfiguration Disabled

Set-NetIPInterface -InterfaceAlias Corpnet2 -AddressFamily IPv6 -ManagedAddress Configuration Disabled -OtherStatefulConfiguration Disabled

6. In the DHCP console tree, click Server Options.
7. In the details pane, right-click 00023 DNS Recursive Name, click Delete, and then click OK.
8. In the DHCP console tree, right-click Scope [2001:db8::] Corpnet, click Delete, and then click Yes twice.
9. In the DHCP console tree, right-click Scope [2001:db8:0:2::] Corpnet2, click Delete, and then click Yes twice.
10. In the DHCP console tree, right-click dc1.corp.contoso.com, point to All Tasks, and then click Restart.
11. On APP1, in the Network Connections window, right-click Wired Ethernet Connection Or Local Area Connection, and then click Properties.
12. In This Connection Uses The Following Items, select Internet Protocol Version 4 (TCP/IPv4), and then click OK.
13. In the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.
14. On EDGE1, in the Network Connections window, right-click Corpnet, and then click Properties.
15. In This Connection Uses The Following Items, select Internet Protocol Version 4 (TCP/IPv4), and then click OK.
16. In the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.
17. On CLIENT1, in the Network Connections window, right-click Wired Ethernet Connection Or Local Area Connection, and then click Properties.
18. In This Connection Uses The Following Items, select Internet Protocol Version 4 (TCP/IPv4), and then click OK.
19. In the Command Prompt or Windows PowerShell window, type **ipconfig /renew6**, and then press Enter.

For more information about what you can do in the IPv6 test lab, see <http://go.microsoft.com/fwlink/?Linkid=251469>.