

Troubleshooting IPv6

Joseph Davies

Introduction

This article describes the techniques and tools that you can use to help identify a problem at successive layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack that is using an Internet Protocol version 6 (IPv6) Internet layer in Microsoft® Windows® XP with Service Pack 1 (SP1), Windows XP with Service Pack 2 (SP2), or Windows Server 2003. Depending on the type of problem, you might do one of the following:

- Start at the bottom of the stack and move up.
- Start at the top of the stack and move down.

The following sections are organized from the top of the stack and describe how to:

- Verify IPv6 connectivity
- Verify Domain Name System (DNS) name resolution for IPv6 addresses
- Verify IPv6-based TCP connections

Although not specified in the following sections, you can also use Network Monitor to capture IPv6 traffic to troubleshoot many problems with IPv6-based communications. Network Monitor is provided with Microsoft Systems Management Server® and as an optional network component with Windows Server 2003. However, to correctly interpret the display of IPv6 packets in Network Monitor, you must have detailed knowledge of the protocols included in each packet. For in-depth information about IPv6 protocols and processes, see the Understanding IPv6 Microsoft Press book.

This article describes the tasks and tools to gather information and test networking components when troubleshooting an arbitrary problem with IPv6 in Windows. For information about solutions to common IPv6 problems, see Troubleshooting.

Verifying IPv6 Connectivity

You can use the following tasks to troubleshoot problems with IPv6 connectivity:

- Verify configuration
- Manage configuration
- Verify reachability
- View and manage the IPv6 routing table
- Verify router reliability
- Verify Configuration

To check the current IPv6 settings for the correct address configuration (when manually configured) or an appropriate address configuration (when automatically configured), you can use the following:

```
ipconfig /all
```

The display of the ipconfig /all command includes IPv6 addresses, default routers, and DNS servers for all interfaces. The Ipconfig tool only works on the local computer.

```
netsh interface ipv6 show address
```

This command only displays the IPv6 addresses assigned to each interface. Netsh can also be used to show the configuration of a remote computer by using the r RemoteComputerName command line option. For example, to display the configuration of the remote computer named FILESRV1, use the netsh r filesrv1 interface ipv6 show address command.

Troubleshooting IPv6

Joseph Davies

Manage Configuration

To manually configure IPv6 addresses, use the netsh interface ipv6 set address command. In most cases, you do not need to manually configure IPv6 addresses because they are automatically assigned for hosts through IPv6 address autoconfiguration.

To make changes to the configuration of IPv6 interfaces, use the netsh interface ipv6 set interface command. To add the IPv6 addresses of DNS servers, use the netsh interface ipv6 add dns command.

Verify Reachability

To verify reachability with a local or remote destination, try the following:

- **Check and flush the neighbor cache**

Similar to the Address Resolution Protocol (ARP) cache, the neighbor cache stores recently resolved link-layer addresses. To display the current contents of the neighbor cache, use the netsh interface ipv6 show neighbors command. To flush the neighbor cache, use the netsh interface ipv6 delete neighbors command.

- **Check and flush the destination cache**

The destination cache stores next-hop IPv6 addresses for destinations. To display the current contents of the destination cache, use the netsh interface ipv6 show destinationcache command. To flush the destination cache, use the netsh interface ipv6 delete destinationcache command.

- **Ping the default router**

Use the Ping tool to ping your default router by its IPv6 address. You can obtain the link-local IPv6 address of your default router from the display of the ipconfig, netsh interface ipv6 show routes, route print, or nbtstat -r commands. Pinging the default router tests whether you can reach local nodes and whether you can reach the default router, which forwards IPv6 packets to remote nodes.

When you ping the default router, you must specify the zone identifier (ID) for the interface on which you want the ICMPv6 Echo Request messages to be sent. The zone ID is the interface index of the default route (::/0) with the lowest metric, from the display of the netsh interface ipv6 show routes or route print commands.

- **Ping a remote destination by its IPv6 address**

If you are able to ping your default router, ping a remote destination by its IPv6 address.

- **Trace the route to the remote destination**

If you are unable to ping a remote destination by its IPv6 address, there might be a routing problem between your node and the destination node. Use the tracert d IPv6Address command to trace the routing path to the remote destination. The d command line option prevents the Tracert tool from performing a DNS reverse query on every near-side router interface in the routing path, which speeds up the display of the routing path.

Troubleshooting IPv6

Joseph Davies

Check Packet Filtering

The problem with reaching a destination node might be due to the configuration of Internet Protocol security (IPsec) or packet filtering on the source node, intermediate routers, or destination node that is preventing packets from being sent, forwarded, or received.

On the source node, check for IPsec for IPv6 policies that have been configured with the Ipsec6 tool. For information about the Ipsec6 tool, see IPv6 utilities.

On intermediate IPv6 routers that are running Windows XP or Windows Server 2003, check for the following:

- **IPsec for IPv6 policies that have been configured with the Ipsec6 tool**
- **The simple IPv6 firewall**
IPv6 for Windows Server 2003 includes support for a simple firewall on an interface. When enabled, IPv6 drops incoming TCP Synchronize (SYN) segments and drops all unsolicited incoming UDP messages. You can configure the simple firewall with the netsh interface ipv6 set interface interface=NameOrIndex firewall=enabled disabled command.
- **Internet Connection Firewall for IPv6**
The Internet Connection Firewall for IPv6 is included with the Advanced Networking Pack for Windows XP, a free download for Windows XP with SP1. For more information, see Internet Protocol version 6 (IPv6) Internet Connection Firewall.
- **Windows Firewall**
The Windows Firewall is included with Windows XP Service Pack 2 and later and Windows Server 2003 Service Pack 1 and later. For more information, see Manually Configuring Windows Firewall in Windows XP Service Pack 2, the May 2004 The Cable Guy article.

On third-party intermediate IPv6 routers or firewalls, check for the configuration of IPv6-based packet filters and IPsec policies.

On the destination node, check for the following:

- IPsec for IPv6 policies that have been configured with the Ipsec6 tool
- The simple IPv6 firewall
- Internet Connection Firewall for IPv6
- Windows Firewall

View and Manage the IPv6 Routing Table

The inability to reach a local or remote destination might be due to incorrect or missing routes in the local IPv6 routing table. To view the local IPv6 routing table, use the route print, netstat r, or netsh interface ipv6 show routes commands. Verify that you have a route corresponding to your local subnet and, if automatically configured with a default router, a default route. If you have multiple default routes with the same lowest metric, you might need to modify your IPv6 router configurations so that the default route with the lowest metric uses the interface that connects to the network with the largest number of subnets.

To add a route to the IPv6 routing table, use the netsh interface ipv6 add route command. To modify an existing route, use the netsh interface ipv6 set route command. To remove an existing route, use the netsh interface ipv6 delete route command.

Troubleshooting IPv6

Joseph Davies

Verify Router Reliability

If you suspect a problem with router performance, use the `pathping d IPv6Address` command to trace the path to a destination and display information on packet losses for each router in the path. The `d` command line option prevents the Pathping tool from performing a DNS reverse query on every near-side router interface in the routing path, which speeds up the display of the routing path.

Verifying DNS Name Resolution for IPv6 Addresses

If reachability using IPv6 addresses works but reachability using host names does not, you might have a problem with host name resolution, which is typically a problem with the DNS configuration of the DNS client or problems with DNS registration.

You can use the following tasks to troubleshoot problems with DNS name resolution:

- Verify DNS configuration
- Display and flush the DNS client resolver cache
- Test DNS name resolution with the Ping tool
- Use the Nslookup tool to view DNS server responses

Verify DNS Configuration

On the node having DNS name resolution problems, verify the following:

- Host name
- The primary DNS suffix
- DNS suffix search list
- Connection-specific DNS suffixes
- DNS servers

You can obtain this information from the display of the `ipconfig /all` command. To obtain information about which DNS names should be registered in DNS, use the `netsh interface ip show dns` command. By default, IPv6 configures the well-known site-local addresses of DNS servers at `FEC0:0:0:FFFF::1`, `FEC0:0:0:FFFF::2`, and `FEC0:0:0:FFFF::3` on each LAN interface. To add the IPv6 addresses of additional DNS servers, use the `netsh interface ipv6 add dns` command.

To register the appropriate DNS names as IPv6 address resource records (also known as AAAA resource records) with DNS dynamic update, use the `ipconfig /registerdns` command.

Display and Flush the DNS Client Resolver Cache

TCP/IP checks the DNS client resolver cache before sending DNS name queries. If an entry exists for a resolved name, the corresponding IPv6 address is used. If a negative cache entry for the name exists, DNS name queries are not sent.

To display the contents of the DNS client resolver cache, use the `ipconfig /displaydns` command. To flush the contents of the DNS client resolver cache and reload it with the entries in the Hosts file, use the `ipconfig /flushdns` command.

Test DNS Name Resolution with the Ping Tool

To test DNS name resolution, use the Ping tool and ping a destination by its host name or fully qualified domain name (FQDN). The Ping tool display shows the FQDN and its corresponding IPv6 address.

Troubleshooting IPv6

Joseph Davies

Use the Nslookup Tool to View DNS Server Responses

If the Ping tool is using the wrong IPv6 address, flush the DNS client resolver cache and use the Nslookup tool to determine the set of addresses returned in the DNS Name Query Response message. At the Nslookup > prompt, use the set d2 command to display the maximum amount of information about the DNS response messages. Then, use Nslookup to look up the desired FQDN. Look for AAAA records in the detailed display of the DNS response messages.

Verifying IPv6-based TCP Connections

If reachability and name resolution are working but you cannot establish a TCP connection with a destination host, use the following tasks:

- Check for packet filtering
- Verify TCP connection establishment

Check for Packet Filtering

As previously discussed in the "Verifying IPv6 Communications" section of this article, packet filtering by the source node, intermediate routers, and the destination node can prevent TCP connections from being established. Use the information in the "Verifying IPv6 Communications" section of this article to check for packet filtering or IPsec policies at the source node, intermediate routers and firewalls, and the destination node.

In many cases, packet filtering is configured to allow specific types of traffic and discard all others, or to discard specific types of traffic and accept all others. As an example of the former case, a firewall or Web server might be configured to allow only HyperText Transfer Protocol (HTTP) traffic and discard all other traffic destined for the Web server. This means that you will be able to view Web pages on the Web server, but not ping it or access its shared folders and files.

Verify TCP Connection Establishment

To verify that a TCP connection can be established using the known destination TCP port number of the application of the destination, you can use the telnet IPv6Address TCPPort command. For example, to verify whether the Web server service on the computer with the IPv6 address of 3FFE:FFFF::21AD:2AA:FF:FE31:AC89 is accepting TCP connections on TCP port 80, use the telnet 3ffe:fff::21ad:2aa:ff:fe31:ac89 80 command.

If the Telnet tool can successfully create a TCP connection, the command prompt window will clear and, depending on the protocol, display some text. This window allows you to type in commands to the service to which you have connected. Type Control-C to exit the Telnet tool. If the Telnet tool cannot successfully create a TCP connection, it displays the message "Connecting To IPv6Address...Could not open connection to the host, on port TCPPort: Connect failed".

Another tool that you can use to test TCP connection establishment is Test TCP (Ttcp). With Ttcp, you can both initiate TCP connections and listen for TCP connections. You can also use the Ttcp tool for UDP traffic. With Ttcp, you can configure a computer to listen on a specific TCP or UDP port without having to install the application or service on the computer. This allows you to test network connectivity for specific traffic before the services are in place.