IPv6 configurations

The IPv6/IPv4 nodes with a dual stack or dual IP architecture, DNS infrastructure, and IPv6 over IPv4 tunneling are used to coexist with an IPv4 infrastructure and to provide eventual migration to anIPv6-only infrastructure. The chapter presents the IPv6 address configuration and verification commands. It also lists and describe the different types of IPv4 and IPv6 nodes, mechanisms for IPv4 to IPv6 transition, types of tunneling configurations.

Address Auto configuration

A highly useful aspect of IPv6 is its ability to automatically configure itself without the use of a stateful configuration protocol, such as Dynamic Host Configuration Protocol for IPv6 (DHCPv6). By default, an IPv6 host can configure a link-local address for each interface. By using router discovery, a host can also determine the addresses of routers, additional addresses, and other configuration parameters. The Router Advertisement message indicates whether a stateful address configuration protocol should be used. Address autoconfiguration can be performed only on multicast-capable interfaces.

Autoconfigured Address States

Autoconfigured addresses are in one or more of the following states:

Tentative The address is in the process of being verified as unique. Verification occurs through duplicate address detection.

Preferred An address for which uniqueness has been verified. A node can send and receive unicast traffic to and from a preferred address. Router Advertisement messages include the period of time that an address can remain in the tentative and preferred states.

Deprecated An address that is still valid but whose use is discouraged for new communication. Existing communication sessions can continue to use a deprecated address. Nodes can send and receive unicast traffic to and from deprecated addresses.

Valid An address from which unicast traffic can be sent and received. The valid state covers both the preferred and deprecated states. Router Advertisement messages include the amount of time that an address remains in the valid state. The valid lifetime must be longer than or equal to the preferred lifetime.

Invalid An address for which a node can no longer send or receive unicast traffic. An address enters the invalid state after the valid lifetime expires.

The following figure shows the relationship between the states of an autoconfigured address and the preferred and valid lifetimes. With the exception of link-local addresses, address autoconfiguration is specified only for hosts. Routers must obtain address and configuration parameters through another means (for example, manual configuration).

Types of Autoconfiguration

Autoconfiguration falls into three types:

1. Stateless Configuration is based on Router Advertisement messages. These messages include stateless address prefixes and require that hosts not use a stateful address configuration protocol.

2. Stateful Configuration is based on a stateful address configuration protocol, such as DHCPv6, to obtain addresses and other configuration options. Hosts use stateful address configuration when they receive Router Advertisement messages that do not include address prefixes and that require the hosts to use a stateful address configuration protocol. A host will also use a

172

stateful address configuration protocol when no routers are present on the local link.

3. Both Configuration is based on Router Advertisement messages. These messages include stateless address prefixes but require hosts to use a stateful address configuration protocol.

For all autoconfiguration types, a link-local address is always configured.

Autoconfiguration Process

Address autoconfiguration for an IPv6 node occurs as follows:

1. A tentative link-local address is derived, based on the link-local prefix of FE80::/64 and the 64-bit interface identifier.

2. Duplicate address detection is performed to verify the uniqueness of the tentative link-local address. If the address is already in use, the node must be configured manually.

3. If the address is not already in use, the tentative link-local address is assumed to be unique and valid. The link-local address is initialized for the interface. The corresponding solicited-node multicast link-layer address is registered with the network adapter.

4. The host sends a Router Solicitation message.

5. If the host receives no Router Advertisement messages, then it uses a stateful address configuration protocol to obtain addresses and other configuration parameters.

Windows Server 2003 does not support the use of a stateful address configuration protocol for IPv6.

6. If the host receives a Router Advertisement message, the host is configured based on the information in the message

7. For each stateless address prefix that the message includes: A tentative address is derived from the address prefix and the appropriate 64-bit interface identifier.
173

8. The uniqueness of the tentative address is verified. If the tentative address is in use, the address is not initialized for the interface.

If the tentative address is not in use, the address is initialized. Initialization includes setting the valid and preferred lifetimes based on information in the Router Advertisement message. Initialization also includes registering the corresponding solicited-node multicast link-layer address with the network adapter.

9. If specified in the Router Advertisement message, the host uses a stateful address configuration protocol to obtain additional addresses or configuration parameters.

IPv6 Transition Technologies

1. Node Types
2. Address Compatibility

Protocol transitions are not easy, and the transition from IPv4 to IPv6 is no exception. Protocol transitions are typically deployed by installing and configuring the new protocol on all nodes within the network and verifying that all node and router operations work. Although this might be possible in a small- or medium-sized organization, the challenge of making a rapid protocol transition in a large organization is very difficult. Additionally, given the scope of the Internet, rapid protocol transition becomes an impossible task. The transition from IPv4 to IPv6 will take years, and organizations or hosts within organizations might continue to use IPv4 indefinitely. Therefore, although migration is the long-term goal, equal consideration must be given to the interim coexistence of IPv4 and IPv6 nodes. It defines the following transition criteria:

1. Existing IPv4 hosts can be upgraded at any time, independent of the upgrade of other hosts or routers.

2. Hosts that use only IPv6 can be added at any time, without dependencies on other hosts or routing infrastructure.

3. IPv4 hosts on which IPv6 is installed can continue to use their IPv4 addresses and do not need additional addresses.

4. Little preparation is required to either upgrade IPv4 nodes to IPv6 or deploy new IPv6 nodes.
174

The inherent lack of dependencies between IPv4 and IPv6 hosts, IPv4 routing infrastructure, and IPv6 routing infrastructure requires several mechanisms that allow seamless coexistence.

1. Node Types

Defines the following node types:

IPv4-only Node

A node that implements only IPv4 (and has only IPv4 addresses). This node does not support IPv6. Most hosts and routers installed today are IPv4-only nodes.

IPv6-only Node

A node that implements only IPv6 (and has only IPv6 addresses). This node is able to communicate only with IPv6 nodes and applications. This type of node is not common today, but it might become more prevalent as smaller devices such as cellular phones and handheld computing devices include the IPv6 protocol.

IPv6/IPv4 Node

A node that implements both IPv4 and IPv6. This node is IPv6-enabled if it has an IPv6 interface configured. For coexistence to occur, the largest number of nodes (IPv4 or IPv6 nodes) can communicate using an IPv4 infrastructure, an IPv6 infrastructure, or an infrastructure that is a combination of IPv4 and IPv6. True migration is achieved when all IPv4 nodes are converted to IPv6-only nodes. However, for the foreseeable future, practical migration is achieved when as many IPv4-only nodes as possible are converted to IPv6/IPv4 nodes. IPv4-only nodes can communicate with IPv6-only nodes only through an IPv4-to-IPv6 proxy or translation gateway.

2. Address Compatibility

The following addresses are defined to help IPv4 and IPv6 nodes coexist:

IPv4-compatible Addresses

IPv6/IPv4 nodes that are communicating with IPv6 over an IPv4 infrastructure use IPv4-compatible addresses, 0:0:0:0:0:0:w.x.y.z or ::w.x.y.z (where w.x.y.z is the dotted decimal representation of a public IPv4 address). When an IPv4-compatible address is used as an IPv6 destination, IPv6 traffic is automatically encapsulated with IPv4 headers and sent to their destinations using the IPv4 infrastructure.

175

IPv4-mapped Addresses

The IPv4-mapped address, 0:0:0:0:0:FFFF:w.x.y.z or ::FFFF:w.x.y.z, is used to represent an IPv4-only node to an IPv6 node. It is used only for internal representation. The IPv4-mapped address is never used as a source or destination address of an IPv6 packet. The IPv6 protocol for Windows Server 2003 does not support IPv4-mapped addresses. Some IPv6 implementations use IPv4-mapped addresses when translating traffic between IPv4-only and IPv6-only nodes.

6over4 Addresses

Each 6over4 address comprises a valid 64-bit unicast address prefix and the interface identifier ::WWXX:YYZZ (where WWXX:YYZZ is the colon-hexadecimal representation of w.x.y.z, a unicast IPv4 address assigned to an interface). An example of a link-local 6over4 address based on the IPv4 address of 131.107.4.92 is FE80::836B:45C. 6over4 addresses represent a host that use the automatic tunneling mechanism.

6to4 Addresses

6to4 addresses are based on the prefix 2002:WWXX:YYZZ::/48 (where WWXX:YYZZ is the colon-hexadecimal representation of w.x.y.z, a public IPv4 address assigned to an interface). 6to4 addresses represent sites that use the automatic tunneling mechanism

ISATAP Addresses

Each Intra-site Automatic Tunnel Addressing Protocol (ISATAP) addresses comprise a valid 64-bit unicast address prefix and the interface identifier ::0:5EFE:w.x.y.z (where w.x.y.z is a unicast IPv4 address assigned to an interface). An example of a link-local ISATAP address is FE80::5EFE:131.107.4.92. ISATAP addresses represent hosts that use the automatic tunneling mechanism

Teredo Addresses

Teredo addresses use the prefix 3FFE:831F::/32. An example of a Teredo address is 3FFE:831F:CE49:7601:8000:EFFF:62C3:FFFE. Beyond the first 32 bits, Teredo addresses encode the IPv4 address of a Teredo server, flags, and the encoded version of the external address and port of a Teredo client. Teredo addresses represent hosts that use the automatic tunnellingmechanism .

IPv6 - Auto Configuration vs DHCPv6 Introduction

A growing number of IPv6 experts are apprehensive about the adoption of the auto-configuration feature offered by IPv6 in contrast to the services offered by the existing DHCPv6 protocol.

IPv6Auto-Configuration

An important feature of IPv6 is that it allows plug and play option to the network devices by allowing them to configure themselves independently. It is possible to plug a node into an IPv6 network without requiring any human intervention. This feature was critical to allow network connectivity to an increasing number of mobile devices. The proliferation of network enabled mobile devices has introduced the requirements of a mobile device to arbitrarily change locations on an IPv6 network while still maintaining its existing connections. To offer this functionality, a mobile device is assigned a home address where it remains always reachable. When the mobile device is at home, it connects to the home link and makes use of its home address. When the mobile device is away from.

177

IPv6 offers two types of auto-configuration: Stateful auto configuration and stateless auto configuration. **Stateful auto-configuration:** This configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator. **Stateless auto-configuration:** This type of configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements **15.2.6 DHCPv6** The Dynamic Host Configuration Protocol (DHCP) facilitates the addition of new machines in a network. Around October 1993, DHCP began to take shape as a standard network protocol. The protocol allows the network devices to obtain the different parameters that are required by the clients to operate in an Internet Protocol (IP) network. The DHCP protocol significantly reduces the system administration workload as the network devices can be added to the network with little or no change in the device configuration.

DHCP also allows network parameter assignment at a single DHCP server or a group of such server located across the network. The dynamic host configuration is made possible with the automatic assignment of IP addresses, default gateway, subnet masks and other IP parameters. On connecting to a network, a DHCP configured node sends a broadcast query to the DHCP server requesting for necessary information. Upon receipt of a valid request, the DHCP server assigns an IP address from its pool of IP addresses and other TCP/IP configuration parameters such as the default gateway and subnet mask. The broadcast query is initiated just after booting and must be completed before the client initiates IP-based communication with other devices over the network. DHCP allocates IP addresses to the network devices in three different modes: dynamic mode, automatic mode and manual mode. In the dynamic mode, the client is allotted an IP address for a specific period of time ranging from a few hours to a few months. At any time before the expiry of the lease, a DHCP client can request a renewal of the current IP address. Expiry of the lease