5.6.4 IPv4 to IPv6 Migration

The worldwide transition from IPv4 to IPv6 will be a long process. Although IPv6 is not yet widely adopted, you can implement it if your systems support it. As the implementation of IPv6 proceeds, there will be times when compatibility with IPv4 will be necessary.

IPv6 Deployment Strategies

The following table lists various strategies for deploying IPv6.

Method	Description
Dual Stack	A *dual stack* configuration enables a host to communicate with IPv4 and IPv6 hosts; the IPv4 and IPv6 protocol stacks run concurrently on a host. IPv4 is used to communicate with IPv4 hosts, and IPv6 is used to communicate with IPv6 hosts. When dual stack is implemented on hosts, intermediate routers and switches must also run both protocol stacks.
Tunneling	*Tunneling* allows IPv6 hosts or sites to communicate over the existing IPv4 infrastructure. A device encapsulates IPv6 packets within IPv4 packets for transmission across an IPv4 network, and then the IPv6 packets are de-encapsulated by another device at the other end. Tunneling solutions include the following:
Manually Configured tunnel	In this configuration, tunnel endpoints are configured as point-to-point connections between devices. Because of the time and effort required for configuration, use manually configured tunnels only when you have a small number of sites that need to connect through the IPv4 internet or when you want to configure secure site-to-site associations. Manual tunneling: • Is configured between routers at different sites. • Requires dual stack routers as the tunnel endpoints, but is compatible with IPv6-only hosts. • Works through NAT. • Uses a static association of an IPv6 address to the IPv4 address of the destination tunnel endpoint.
6-to-4 Tunneling	With 6-to-4 tunneling, tunneling endpoints are configured automatically between devices. Use 6-to-4 tunneling to dynamically connect multiple sites through the IPv4 internet. Because of its dynamic configuration, 6-to-4 tunneling is easier to administer than manual tunneling. 6-to-4 tunneling: • Is configured between routers at different sites. • Requires dual stack routers as the tunnel endpoints, but can work with IPv6-only hosts. • Works through NAT. • Uses a dynamic association of an IPv6 site prefix to the IPv4 address of the destination tunnel endpoint. • Automatically generates an IPv6 address for the site using the 2002::/16 prefix followed by the public IPv4 address of the tunnel endpoint router. For example, a router with an IPv4 address of 207.142.131.202 would serve the site with the following prefix: 2002:CF8E:83CA::/48 (CF8E:83CA is the hexadecimal equivalent of 207.142.131.202).
4-to-6 Tunneling	4-to-6 tunneling works in a manner similar to 6-to-4 tunneling. However, instead of tunneling IPv6 traffic through an IPv4 network, 4-to-6 tunnels IPv4 traffic through an IPv6 network by encapsulating IPv4 packets within IPv6 packets.

Intra-site Automatic Tunnel Addressing Protocol (ISATAP)	The intra-site automatic tunnel addressing protocol is a tunneling method that provides IPv6 communication over a private IPv4 network. ISATAP tunneling:
	
	• Is configured between individual hosts and an ISATAP router.
	• Requires a special dual stack ISATAP router to perform tunneling and dual stack or IPv6-only clients. Dual stack routers and hosts perform tunneling when communicating on the IPv4 network.
	• Does not work through NAT.
	• Automatically generates link-local addresses that includes the IPv4 address of each host.
	    • The prefix is the well-known link-local prefix: FE80::/16.
	    • The remaining prefix values are set to 0.
	    • The first two quartets of the interface ID are set to 0000:5EFE.
	    • The remaining two quartets use the IPv4 address written in either dotted decimal or hexadecimal notation.
	
	For example, a host with the IPv4 address 192.168.12.155 would have the following IPv6 address when using ISATAP: FE80::5EFE:C0A8:0C9B (also designated as FE80::5EFE:192.168.12.155).

| | | Use ISATAP to begin a transition to IPv6 within a site. You can start by adding a single ISATAP router and configuring each host as an ISATAP client. |
| | Teredo Tunneling | Teredo tunneling establishes a tunnel between individual hosts so they can communicate through a private or public IPv4 network. Teredo tunneling: Is configured between individual hosts. Uses dual stack hosts and performs IPv6 tunneling to send on the IPv4 network. Works through NAT. In Windows 7, the Teredo component is enabled but inactive by default. In Windows 8, Teredo is enabled by default on work and home network profiles. On Linux, the Miredo client software is used to implement Teredo tunneling. |