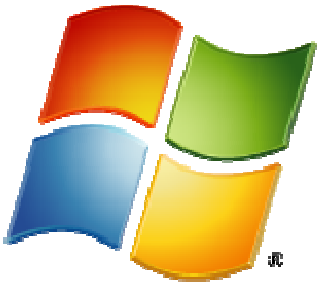

Windows Server 2008

Intra-site Automatic Tunnel Addressing Protocol (ISATAP) Guide

Microsoft Corporation

Abstract

The Intra-site Automatic Tunnel Addressing Protocol (ISATAP) in the Microsoft® Windows Server® 2008 R2, Windows Server 2008, Windows 7,and Windows Vista™ operating systems provides an Internet Protocol version 6 (IPv6) connectivity option for test labs and fortemporary connectivityon an existing Internet Protocol version 4 (IPv4)-only network. This white paper describes how to use ISATAP with Windows-based ISATAP hosts and routers and assumes that the reader has a basic understanding of networking, IPv6, and IPv6 transition technologies.

Microsoft

Contents

Introduction

IPv6 is the next generation Internet protocol. Although IPv6 has been standardized for over a decade, recent attention has increased because of a decrease in unallocated public IPv4 addresses, a quickly expanding Internet, and a demand for ubiquitous connectivity. The next generation Internet that uses IPv6 promises to enable a new breed of applications.

This white paper describes the Intra-site Automatic Tunnel Addressing Protocol (ISATAP) IPv6 transition technology defined in RFC 4214. ISATAP allows the deployment of IPv6 on an existing IPv4-only networking environment without an upgrade to any routers or other support infrastructure. With ISATAP, IPv4-dependent applications can continue to utilize IPv4 while newer applications can be deployed utilizing IPv6. Both types of traffic share a single common IPv4 infrastructure.

The benefit of ISATAP is that an existing IPv4-only infrastructure can provide IPv6 connectivity immediately with no requirements for router software or hardware upgrades.

Appropriate Uses for ISATAP on Intranets

ISATAP in Windows is not designed for production networks.On a production network, ISATAP should be used in a limited capacity for testing while you deploy native IPv6 capabilities. Microsoft does not recommend the use of ISATAP across entire production networks. Instead, you should deploy native IPv6 routing capability.

This document describes how ISATAP works and how to configure Windows-based ISATAP hosts and routers for test labs and for IPv6 connectivity testing on production network deployments.

ISATAP in Windows XP and Windows Server 2003

Although Windows XP and Windows Server 2003 support ISATAP host and router functionality, most of the built-in applications and system services of these operating systems do not support IPv6. Therefore, Microsoft does not recommend the use of ISATAP for IPv6 connectivity to computers running Windows XP or Windows Server 2003.

ISATAP Overview

ISATAP uses a tunneling approach to transport IPv6 traffic across an existing IPv4 infrastructure. ISATAP utilizes an innovative principle in which the whole IPv4 network emulates a single IPv6 logical link or subnet to a set of ISATAP hosts. This principle allows all ISATAP nodes, no matter where they are located on the IPv4 network, to automatically create IPv6 tunnels without having to traverse any IPv6-capable routers.

Figure 1 shows a logical ISATAP subnet.

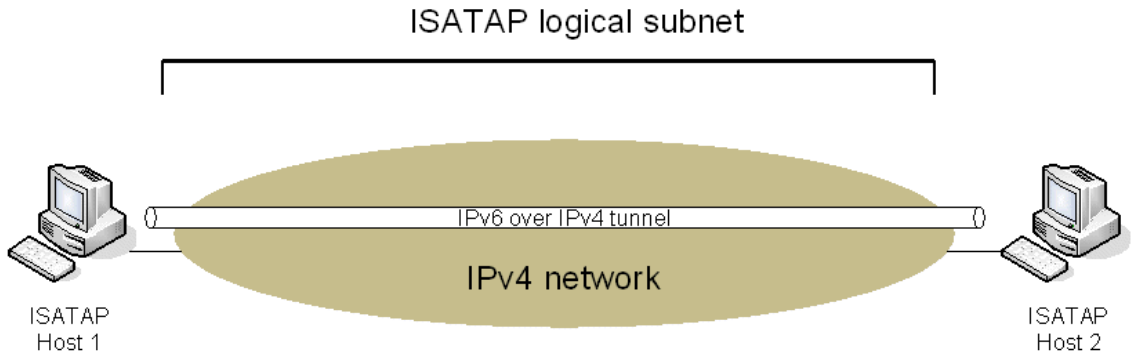

Figure 1: A logical ISATAP subnet

ISATAP Addressing

In ISATAP, the IPv4 address of an ISATAP host is also stored as part of the IPv6 address so that any ISATAP host can determine the IPv4 address of the IPv6-over-IPv4 tunnel endpoint without having to utilize some other protocol. The ISATAP address format is one of the following:

64-bit_Unicast_Prefix:0:5efe:*w.x.y.z*

64-bit_Unicast_Prefix:200:5efe:*w.x.y.z*

- *64-bit_Unicast_Prefix* can be a global, link-local, or unique local unicast address prefix. ISATAP was designed for use within an intranet or autonomy, in which ISATAP logical subnets are IPv6 subnets.
- For the interface ID ::0:5efe:*w.x.y.z*, *w.x.y.z* is a private IPv4 address that is assigned to an interface of an ISATAP node. For the interface ID ::200:5efe:*w.x.y.z*, *w.x.y.z* is a public IPv4 address that is assigned to an interface of an ISATAP node.

Examples of ISATAP address are 2001:db8::5efe:10.98.47.117 and 2001:db8::200:5efe:131.107.98.204.

ISATAP hosts communicate by tunneling IPv6 packets as the payload of IPv4 packets. There are no pre-established tunnels that are needed. The sending ISATAP host automatically performs the tunneling for each packet as it is sent. The sending ISATAP host determines the IPv4 tunnel endpoint—the destination address in the IPv4 header of the tunneled packet—from the last 32 bits of the next-hop address corresponding to the IPv6 destination address. For example, for traffic to ISATAP hosts on the same logical ISATAP subnet, the IPv4 tunnel endpoint is the last 32 bits (*w.x.y.z*) of the destination IPv6 address. For traffic to ISATAP or IPv6 hosts that are not

on the same logical ISATAP subnet, the IPv4 tunnel endpoint is the last 32 bits of the next-hop ISATAP address of an ISATAP router.

Once the IPv4 tunnel endpoint is determined, a sending ISATAP host dynamically creates the IPv4 encapsulation for each packet sent to the destination. ISATAP encapsulates IPv6 packets within an IPv4 header. The Protocol field in the IPv4 header is set to 41, indicating an IPv6 packet as the payload. This means that the transport (TCP or UDP) is not directly accessible without first removing both the IPv4 and IPv6 headers.

Figure 2 shows the protocol layering and the fields needed to deliver ISATAP-encapsulated application data.

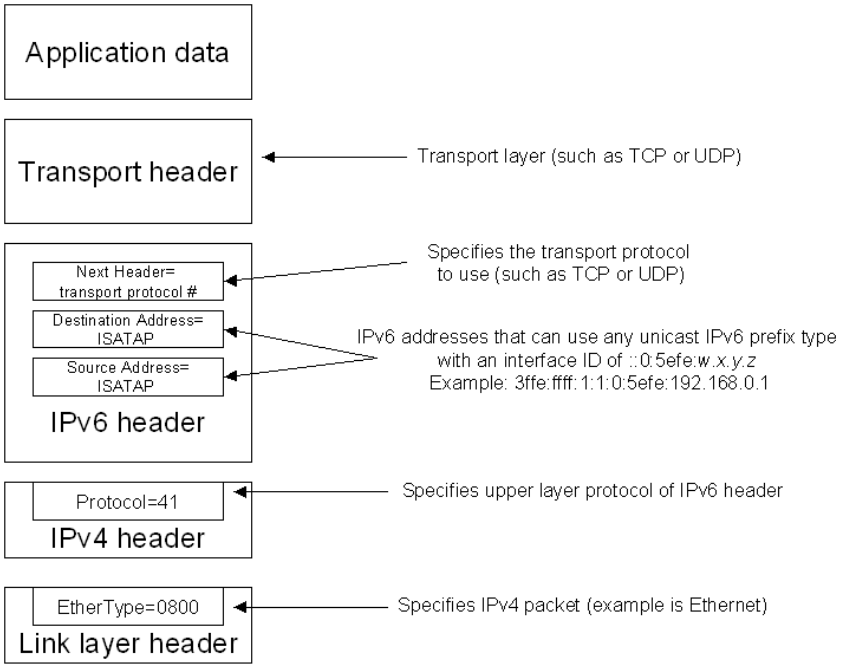

Figure 2: Protocol layering and the fields needed to deliver ISATAP-encapsulated application data

Name Resolution for ISATAP Addresses

ISATAP addresses are just like any other IPv6 unicast addresses and resolving names to ISATAP addresses uses the same methods, such as the Domain Name System (DNS) and Hosts file entries.

For DNS servers running Windows Server 2008 and later, the DNS server must be configured to allow the querying of the ISATAP name using the following steps:

1. Open the Registry Editor (Regedit.exe).

   Caution: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

2. In Registry Editor, navigate to the following registry location:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

3. Double-click the**GlobalQueryBlockList** value.
4. Select the **ISATAP** name, press **DELETE**, and then click **OK**.
5. Restart the DNS Server service.

AWindows-based ISATAP host that is starting up automatically registers the appropriate ISATAP unicast addresses using DNS dynamic update. By default, computers running Windows 7, Windows Vista,Windows Server 2008 R2, or Windows Server 2008 use DNS traffic over IPv4 for DNS registration and name resolution. When a host obtains ISATAP addresses in the DNS Name Query Response message, it uses them for IPv6 connectivity just like any other IPv6 destination address.

ISATAP Router

Although ISATAP hosts do not need any IPv6-capable routers or IPv6 routing infrastructure, Microsoft recommends that you use at least one ISATAP router. Without an ISATAP router, an ISATAP host will only use link-local ISATAP addresses, which are not registered using DNS dynamic update. Because most hosts depend on DNS for name resolution, you should operate an ISATAP environment with an ISATAP router.

An ISATAP router does the following:

- Provides prefix information to ISATAP hosts to configure additional ISATAP addresses for the logical ISATAP subnet.
- Optionally advertises itself as a default router so that ISATAP hosts can exchange traffic with hosts that are not located on the logical ISATAP subnet. The next-hop address for the default route is the link-local ISATAP address of the ISATAP router.

ISATAP Router Discovery Process

A computer running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008 by default attempts to automatically discover the IPv4 address of the ISATAP router by attempting to resolve the single-label, unqualifiedname "ISATAP" using the following name resolution techniques:

1. Check the local host name.
2. Check the DNS client resolver cache, which includes the entries in the Hosts file in the %*SystemRoot%*\system32\drivers\etc folder.
3. If the physical interface has a connection-specific suffix, append that suffix and query for the FQDN. For example, if the computer running Windows 7 is using wcoast.contoso.com domain as its primary DNS suffix (and there are no other domain names in the search list), the computer by default sends DNS queries to resolve the names isatap.wcoast.contoso.com and isatap.contoso.com.
4. Attempt to resolve the “ISATAP” name using Link-Local Multicast Name Resolution (LLMNR).
5. If NetBIOS over TCP/IP is enabled, convert the ISATAP name into the NetBIOS name "`ISATAP <00>`" and do the following:
    - Check the NetBIOS name cache.

- Send a NetBIOS name query to a configured Windows Internet Name Service (WINS) server.
- Send NetBIOS broadcasts.
- Check the Lmhosts file in the %*SystemRoot%*\system32\drivers\etc folder.

If the name resolution is successful, the ISATAP host sends an IPv4-encapsulated Router Solicitation message to the ISATAP router. The ISATAP router then responds with an IPv4-encapsulated unicast Router Advertisement message that contains prefixes to use for the autoconfiguration of ISATAP-based addresses and, optionally, advertises itself as a default router.

Figure 3 shows an example name resolution and initial address configuration.

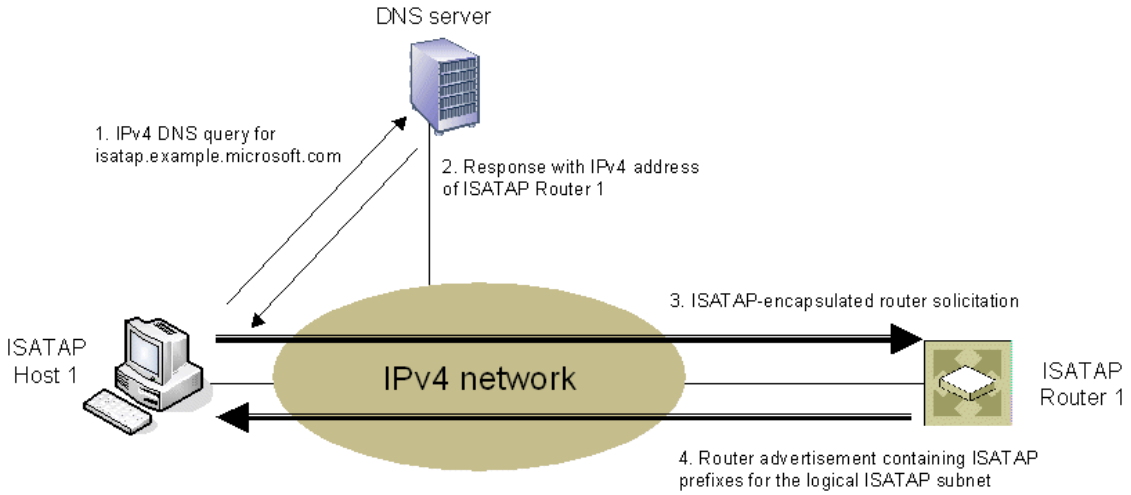

Figure 3: An example name resolution and initial address configuration of an ISATAP host

Intra-ISATAP Subnet Routing

When a set of ISATAP hosts uses a common ISATAP router, they are all configured with the same IPv6 prefixes and are therefore on the same logical ISATAP subnet. ISATAP hosts on the same subnet can communicate directly with each other without going through a router. This allows an IPv6-capable application to leverage the performance and connectivity of an existing IPv4 infrastructure without the necessity of routing traffic through a centralized server or requiring the upgrade of the current IPv4 infrastructure to also support IPv6.

Figure 4 shows the delivery of ISATAP traffic between ISATAP hosts on the same logical ISATAP subnet.

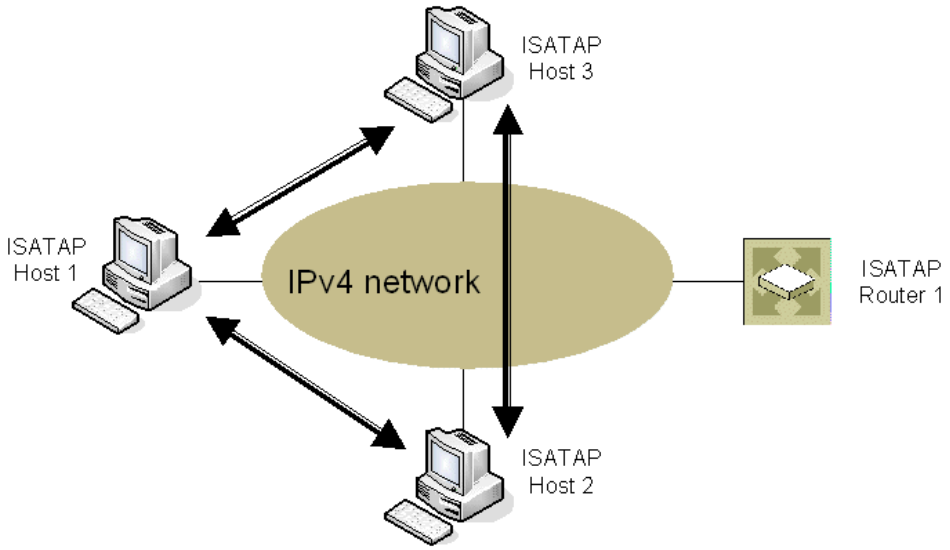

Figure 4: The delivery of ISATAP traffic between ISATAP hosts on the same logical ISATAP subnet

Inter-ISATAP Subnet Routing

If users or applications need to be segmented by some policy, multiple logical ISATAP subnets can be used with each user or application joining the appropriate logical subnet based on a set of administrative constraints and configuration. For example, the hosts on each logical ISATAP subnet would discover a different ISATAP router and receive different subnet prefixes. The ISATAP routers, one for each logical ISATAP subnet, forward traffic to each other through a native IPv6 backbone. A reason to use this configuration is to avoid link-local ISATAP communication across expensive WAN links.

Figure 5 shows the delivery of ISATAP host traffic between hosts on different logical ISATAP subnets. Note that the IPv6 backbone could be an IPv6 tunnel across an IPv4 backbone as well.

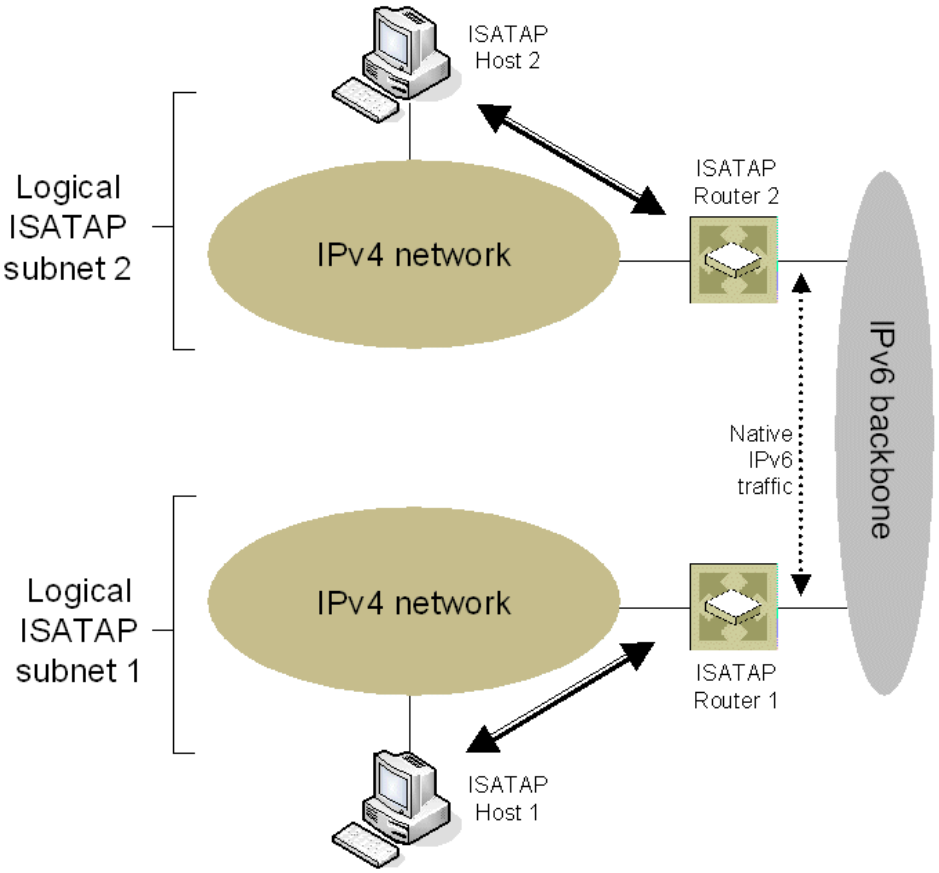

Figure 5: The delivery of ISATAP host traffic between hosts on different logical ISATAP subnets

Routing between ISATAP Hosts and an IPv6-capable Network

An ISATAP router connected to anative IPv6-capable network allows an ISATAP node to have connectivity to other native IPv6 nodes. The ISATAP router de-encapsulates packets sent by ISATAP hosts and encapsulates packets sent to ISATAP hosts. The portion of a network that supports native IPv6 is typically dual-stack and supports both IPv4 and native IPv6 routing.

On a sending ISATAP host, destinations on the IPv6 network match the default route in the IPv6 routing table. The next-hop interface is the ISATAP interface and the next-hop address is the link-local ISATAP address of the ISATAP router. The ISATAP interface tunnels the packet to the IPv4 address of the ISATAP router (as specified by the last 32 bits of the link-local ISATAP address of the ISATAP router).

The ISATAP router receives the ISATAP-encapsulated packet, removes the IPv4 header, and uses its IPv6 routing table to determine how to forward the packet. The packet either matches a default route or a more specific route. In either case, the forwarding interface is typically a LAN interface connected to the IPv6 network. The ISATAP router forwards the packet (without an IPv4 header) to either the next IPv6 router in the path to the destination or to the destination.

When the destination sends a response packet back to the ISATAP host, the routers of the IPv6 network forward the packet to the LAN interface of the ISATAP router. The ISATAP router receives the packet and performs the route determination process. The next-hop interface is the ISATAP interface and the next-hop address is the ISATAP host. The ISATAP interface on the

ISATAP router tunnels the packet to the IPv4 address of the ISATAP host (as specified by the last 32-bits of the ISATAP address of the ISATAP host). If the IPv6-capable network is comprised of multiple links, it is highly recommended to statically add the prefix (used by the ISATAP router) into the routing table of the upstream next-hop router. This will allow IPv6 hosts (beyond those that are link-local) to communicate with the hosts connected with ISATAP.

Figure 6 shows the delivery of packets between ISATAP hosts and IPv6 hosts on an IPv6-capable network.

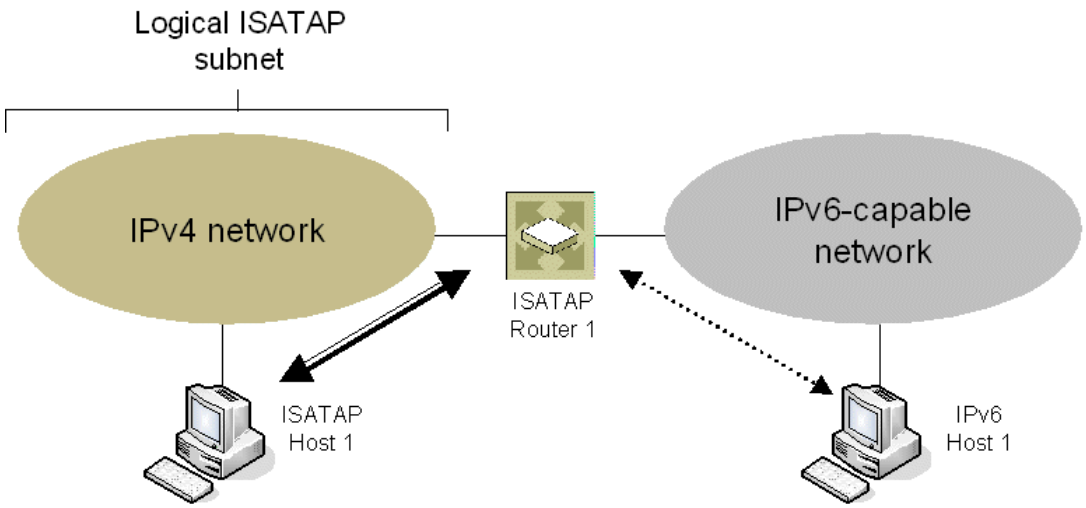

Figure 6: The delivery of packets between ISATAP hosts and hosts on an IPv6-capable network

Configuring ISATAP with Windows-based ISATAP Hosts and Routers

ISATAP can be easily configured in an existing IPv4 environment with computers running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008. The following sections describe how to configure a Windows-based ISATAP host and ISATAP router.

ISATAP Host Configuration

Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008 support ISATAP host functionality that is enabled by default.

To ensure that the Windows-based ISATAP host can automatically discover the ISATAP router by resolving the default name "ISATAP", do one or more of the following as needed:

- If the ISATAP router is a computer running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008, name the computer ISATAP and it will automatically register the appropriate records in DNS and WINS.
- Manually create an ISATAP address (A) record in the appropriate domain in DNS. For example, for the wcoast.contoso.com domain, create an A record for isatap.wcoast.contoso.com.
- Add the following entry to the Hosts file of the computers that need to resolve the name ISATAP:

  IPv4Address ISATAP
- If you are using NetBIOS over TCP/IP on your network, manually create a static WINS record in WINS for the NetBIOS name "`ISATAP  <00>`".
- If you are using NetBIOS over TCP/IP on your network, add the following entry to the Lmhosts file of the computers that need to resolve the name ISATAP:

  IPv4Address ISATAP

If you want to change the default name of ISATAP, you can use the following command on each ISATAP host runningWindows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008:

netsh interface isatap set router *AddressOrName*

AddressOrName is either the IPv4 address of the ISATAP router interface or the name of the router that resolves to the IPv4 address of the ISATAP router.

> **Note:** Do not use FQDNs for the *AddressOrName* field in Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008. Specifying an IPv4 address is the recommended method of configuration.

Configuring ISATAP Host Settings Using Group Policy in Windows Server 2008 R2 and Windows 7

You can centrally configure settings for IPv6 transition technologies, including ISATAP,with Group Policy for computers running Windows 7 or Windows Server 2008 R2. For computers running Windows

Vista or Windows Server 2008, you must configure the equivalent settings through Netsh.exe commands.

You can configure find these settings in the Group Policy Management Editor snap-in at Computer Configuration\Policies\Administrative Templates\Network\TCP/IP Settings\IPv6 Transition Technologies. The following settings configure an ISATAP host:

- ISATAP State

  Allows you to configure the state of the ISATAP host. You can disable ISATAP host functionality by setting ISATAP State to **Disabled**.

- ISATAP Router Name

  Allows you to specify a router name or IPv4 address for an ISATAP router.

ISATAP Router Configuration

Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008 support ISATAP router functionality that is not enabled by default. You can configure an ISATAP router to perform only an advertising function or both advertising and forwarding functions.

To configure a Windows-based advertising ISATAP router, do the following:

- Enable advertising on the ISATAP interface with the following command:

  netsh interface ipv6 set interface *ISATAPInterfaceNameOrIndex* **advertise=enabled**

  You can determine the name of the ISATAP interface from the display of the **ipconfig** command. The ISATAP interface is the interface that has a link-local ISATAP address assigned. You can determine the interface index of the ISATAP interface from the display of the **netsh interface ipv6 show interface** command.

- Add routes for the subnet prefixes of the logical ISATAP subnet to the ISATAP interface and configure them to be published with the following command:

  netsh interface ipv6 add route*IPv6AddressPrefixIPrefixLengthISATAPInterfaceNameOrIndex* **publish=yes**

For example, a computer running Windows Server 2008 R2 has an ISATAP interface with the interface index of 10 that is attached to an IPv4 intranet. The subnet prefix assigned to the logical ISATAP subnet is 2001:db8:0:10::/64. To configure this computer as an advertising ISATAP router, run the following commands:

```
netsh interface ipv6 set interface 10 advertise=enabled
netsh interface ipv6 add route 2001:db8:0:10::/64 10 publish=yes
```

If the router is not named ISATAP or the name "ISATAP" is not resolved to the IPv4 address of the router's intranet interface, you also need to issue the following command on the router:

netsh interface isatap set router *AddressOrName*

Note: Do not use FQDNs for the *AddressOrName* field. Specifying an IPv4 address is the recommended method of configuration.

Advertising and Forwarding ISATAP Router

To configure a Windows-based advertising and forwarding ISATAP router, do the following:

- Enable forwarding on the LAN interface attached to the IPv6-capable backbone or IPv6-capable network with the following command:

  netsh interface ipv6 set interface*LANInterfaceNameOrIndex***forwarding=enabled**

- Enable forwarding and advertising on the ISATAP interface with the following command:

  netsh interface ipv6 set interface *ISATAPInterfaceNameOrIndex* **forwarding=enabled advertise=enabled**

- Add routes for the subnet prefixes of the logical ISATAP subnet to the Automatic Tunneling Pseudo-Interface interface and configure them to be published with the following command:

  netsh interface ipv6 add route*IPv6AddressPrefixIPrefixLengthISATAPInterfaceNameOrIndex* **publish=yes**

- Add a default route using the LAN interface attached to the IPv6 backbone or IPv6-capable network and configure it to be published with the following command:

  netsh interface ipv6 add route ::/0*LANInterfaceNameOrIndex***nexthop=***IPv6RouterAddress* **publish=yes**

For example, a computer has an ISATAP interface with the interface index of 10 and a LAN interface named Local Area Connection 2 that is attached to an IPv6-capable network. The address prefix assigned to the logical ISATAP subnet is 2001:db8:0:10::/64. The computer uses a default router on the IPv6-capable network with the next hop address of fe80::2aa:ff:fe98:2ab1. To configure this computer as an ISATAP advertising and forwarding router, run the following commands:

```
netsh interface ipv6 set interface "Local Area Connection 2" forwarding=enabled
netsh interface ipv6 set interface 10 forwarding=enabled advertise=enabled
netsh interface ipv6 add route 2001:db8:0:10::/64 10 publish=yes
netsh interface ipv6 add route ::/0 "Local Area Connection 2"
nexthop=fe80::2aa:ff:fe98:2ab1 publish=yes
```

If the router is not named ISATAP or the name "ISATAP" is not resolved to the IPv4 address of the router's intranet interface, you also need to issue the following command on the router:

netsh interface isatap set router *AddressOrName*

Note: Do not use FQDNs for the *AddressOrName* field. Specifying an IPv4 address is the recommended method of configuration.

Summary

ISATAP is an IPv6 transition technology to test IPv6 in a test lab or in a limited configuration onan IPv4-only network infrastructure. Computers running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008 are ISATAP hosts by default. You can also configure computers running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008 as either advertising or advertising and forwarding ISATAP routers.

Appendix A – ISATAP and Active Directory Sites and Services Configuration

When you are using ISATAP and your Windows-based ISATAP hosts obtain an ISATAP-based IPv6 address, they begin to use ISATAP-encapsulated traffic to communicate if the destination is also an ISATAP host. Because ISATAP uses a single 64-bit subnet for your entire intranet, your communication goes from a segmented, multi-subnet Internet Protocol version 4 (IPv4) communication model to a flat, single-subnet communication model with IPv6. This can affect the behavior of Active Directory Domain Services (AD DS) and other applications that rely on your Active Directory Sites and Services configuration. For example, if you used the Active Directory Sites and Services snap-in to configure sites, IPv4-based subnets, and inter-site transports for forwarding of requests to servers within sites, this configuration is not used by ISATAP hosts.

To configure Active Directory sites and services for forwarding within sites for ISATAP hosts, you have to configure an IPv6 subnet object equivalent to each IPv4 subnet object, in which the IPv6 address prefix for the subnet expresses the same range of ISATAP host addresses as the IPv4 subnet.

For example, for the IPv4 subnet 192.168.99.0/24 and the 64-bit ISATAP address prefix 2002:836b:1:1::/64, the equivalent IPv6 address prefix for the IPv6 subnet object is 2002:836b:1:1:0:5efe:192.168.99.0/120. For an arbitrary IPv4 prefix length (set to 24 in the example), the corresponding IPv6 prefix length is 96 + *IPv4PrefixLength*.

Related Links

See the following resources for additional information:

- Microsoft IPv6 Web page at http://www.microsoft.com/ipv6
- IPv6 Transition Technologies white paper at http://technet.microsoft.com/en-us/library/bb726951.aspx
- Microsoft Windows Server 2008 R2 Home Page at http://www.microsoft.com/windowsserver2008/default.mspx