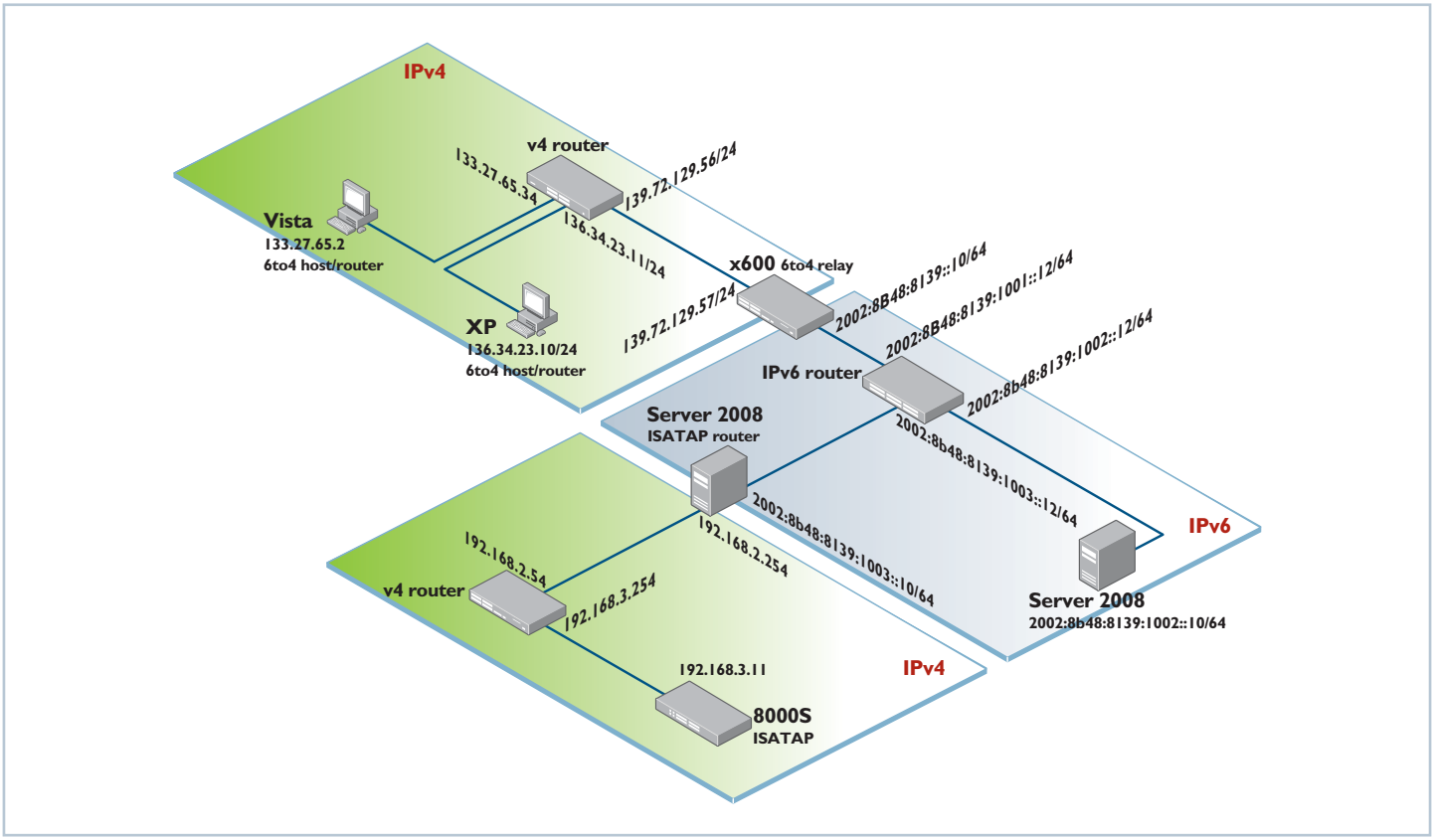
Tested Solution: IPv6 Transition Technologies

Moving a network from IPv4 addressing to IPv6 addressing cannot be performed in a single step. The transition necessarily proceeds in stages, with islands of IPv6 developing within the IPv4 network, and gradually growing until they cover the whole network.
During this transition process, the islands of IPv6 need to be able to communicate with each other across the IPv4 network. Additionally, it is desirable to be able to transition some network functions across to IPv6 while the majority of the network is still using IPv4.
Allied Telesis provides robust solutions for IPv4-to-IPv6 network transitioning, using IPv6 tunneling and dual IPv4/IPv6 network management.
The Allied Telesis IPv6 transition technologies integrate seamlessly with the complementary facilities provided within Microsoft server and workstation operating systems.

The Allied Telesis IPv6 transition solution will be presented here by a detailed description of an example IPv4/IPv6 hybrid network, consisting of Allied Telesis switches and servers and workstations running various versions of Microsoft Windows

Network topology

The example network used in this example consists of two sections of IPv4 network, and a section of pure IPv6 network.



The workstations in the upper IPv4 network are able to communicate using both IPv4 and IPv6. Similarly, the 8000S switch in the lower IPv4 network is able to be managed by both IPv4 and IPv6.

Tunneling techniques

Two different IPv6-over-IPv4 tunneling methods are in use in this network:

- 6to4 tunneling is used to enable the workstations in the upper IPv4 network to tunnel their IPv6 traffic across the IPv4 network to reach the IPv6 network.
- ISATAP tunneling is used by the 8000S switch to tunnel its IPv6 traffic through to the IPv6 network.

These two tunneling methods have different characteristics, and require different configurations on the switches and hosts. Let us examine the characteristics and implementation of these two types of tunneling.

6to4 tunneling

This technique enables IPv6 networks to communicate with each other across an IPv4 network.

Although this method is called **6to4 tunneling**, it does not involve discrete point-to-point tunnels. The **tunneling** in 6to4 tunneling refers to the fact that the IPv6 packets are **encapsulated** in IPv4 packets to be tunneled across the IPv4 domain. Hence, 6to4 tunneling is primarily a scheme for encapsulating IPv6 packets inside IPv4 headers.

Using 6to4 tunneling, you are **not** required to specify tunnel destination addresses. The IPv4 address that represents the point at which any given IPv6 packet will eventually exit the IPv4 domain is derived from the IPv6 packet itself. This is because 6to4 tunneling is designed to use IPv6 addresses which have an IPv4 address embedded within them. This embedded IPv4 address becomes the destination address of the IPv4 header that encapsulates the IPv6 packet during its travel across the IPv4 network.

The IPv6 addresses used in 6to4 tunneling are of the form:

2002: <valid-IPv4-unicast-address> : XX:XX:XX:XX:XX

This makes use of the fact that for every valid IPv4 unicast address A.B.C.D, there is always a corresponding valid IPv6 subnet 2002:<A.B.C.D>::/48. For every global IPv4 address that has been allocated to an organization, there is immediately a global IPv6 subnet 2002:<ipv4-address>::/48 available to that organization.

In this solution, an x600 switch is configured as a 6to4 tunneling router. Hosts in the IPv4 network are configured with IPv6 and IPv4 addresses. Their IPv6 addresses are of the 6to4-compatible form 2002: <IPv4-address> : XX:XX:XX:XX:XX. To communicate with the IPv6 network, their IPv6 packets are encapsulated in IPv4, and use the x600 switch as a relay to give them access to the IPv6 network.

The 6to4-capable hosts are effectively small islands of IPv6, and 6to4 tunneling is used to connect those islands to the main IPv6 network.

Configuration of the Allied Telesis 6to4 tunneling switch

The interface connecting to the IPv4 network is configured with an IPv4 address

```
interface vlan1
 ip address 139.72.129.57/24
```

Create routes to the IPv4 subnets beyond the IPv4 router that is connected to VLAN1

```
ip route 133.27.65.0/24 139.72.129.56
ip route 136.34.23.0/24 139.72.129.56
```

The interface connecting to the IPv6 network is configured with an IPv6 address of the form 2002:<address on IPv4 interface>: XX:XX:XX:XX:XX

```
vlan database
 vlan 2 name v6

interface vlan2
 ipv6 address 2002:8b48:8139:1001::10/64
```

A tunnel interface is created. The source IP address configured on the tunnel is the address that will be the source IP on the IPv4 headers that encapsulate the tunneled IPv6 packets. Configuring this address on the tunnel also identifies the interface via which the tunneled packets will egress the switch

```
interface tunnel100
 tunnel source 139.72.129.57
 tunnel mode ipv6ip 6to4
```

IPv6 forwarding must be enabled

```
ipv6 forwarding
```

The bulk of the IPv6 2002::/16 range are accessed via the IPv4 network

```
ipv6 route 2002::/16 tunnel100
```

Some 2002:: subnets are reached via the IPv6 network

```
ipv6 route 2002:8b48:8139::/48 2002:8b48:8139:1001::12
ipv6 route 2002:8b48:8139:1002::/64 2002:8b48:8139:1001::12
ipv6 route 2002:8b48:8139:1003::/64 2002:8b48:8139:1001::12
ipv6 route 2002:c0a8:500:1001::/64 2002:8b48:8139:1001::12
```

Enable SNMP

```
snmp-server
snmp-server community public
```

Configure a port into VLAN 2

```
interface port3.0.2
switchport access vlan 2
```

Configuring the 6to4 hosts

On both Microsoft Windows XP and Vista, the configuration of 6to4 tunneling is performed from the text command line, rather than by graphical means.

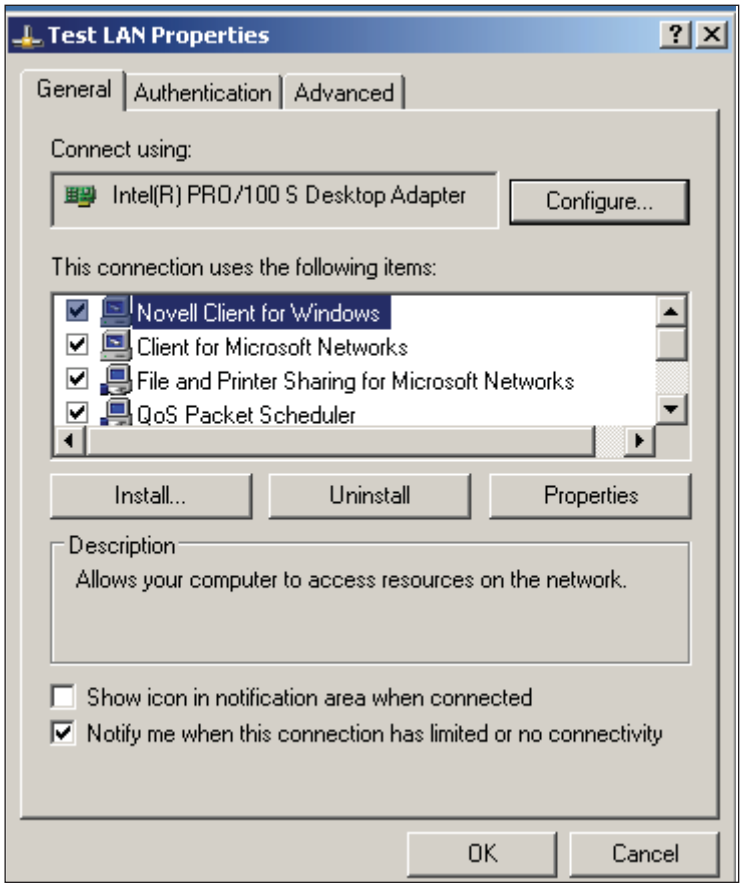
The initial installation and enabling of the IPv6 protocol can be performed graphically, but thereafter the configuration is performed textually.

- Under Windows Vista, the IPv6 protocol is installed by default.
- Under Windows XP, it must be installed.

To install the IPv6 protocol in Windows XP

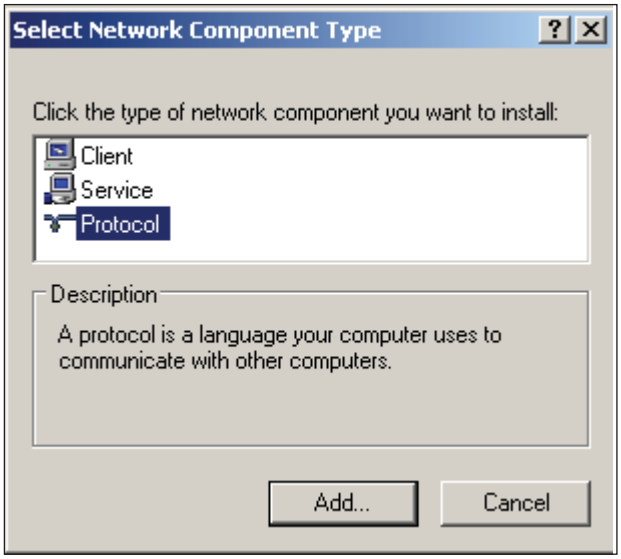
Open the **Network Connections** window, from the Control Panel.

Then, within this window, double-click the NIC via which you wish the PC to perform 6to4 tunneling. In the resulting **Properties** window, click **Install...**

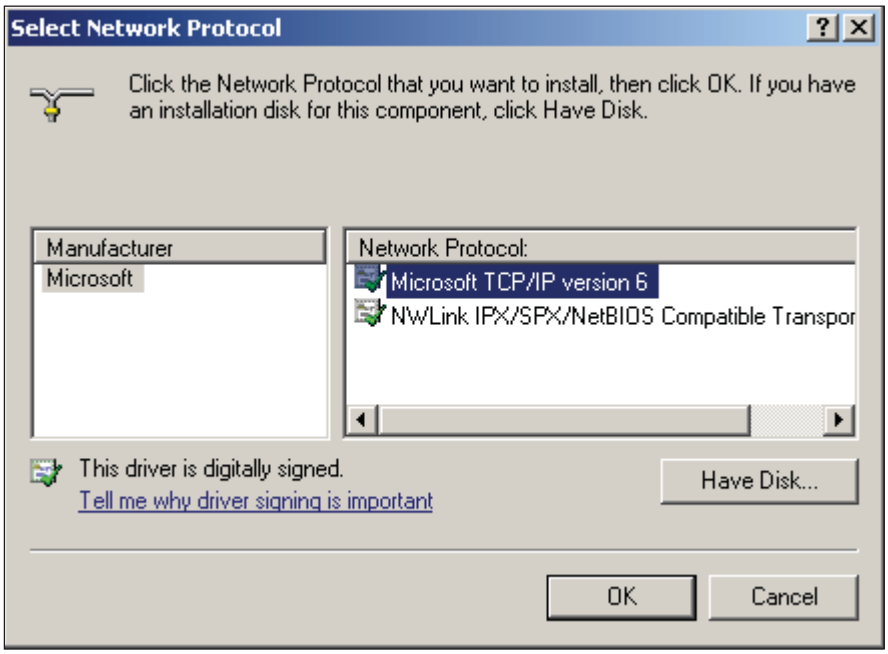


You will then be presented with the **Select Network Component Type** window from which to choose the type of network component you wish to install.

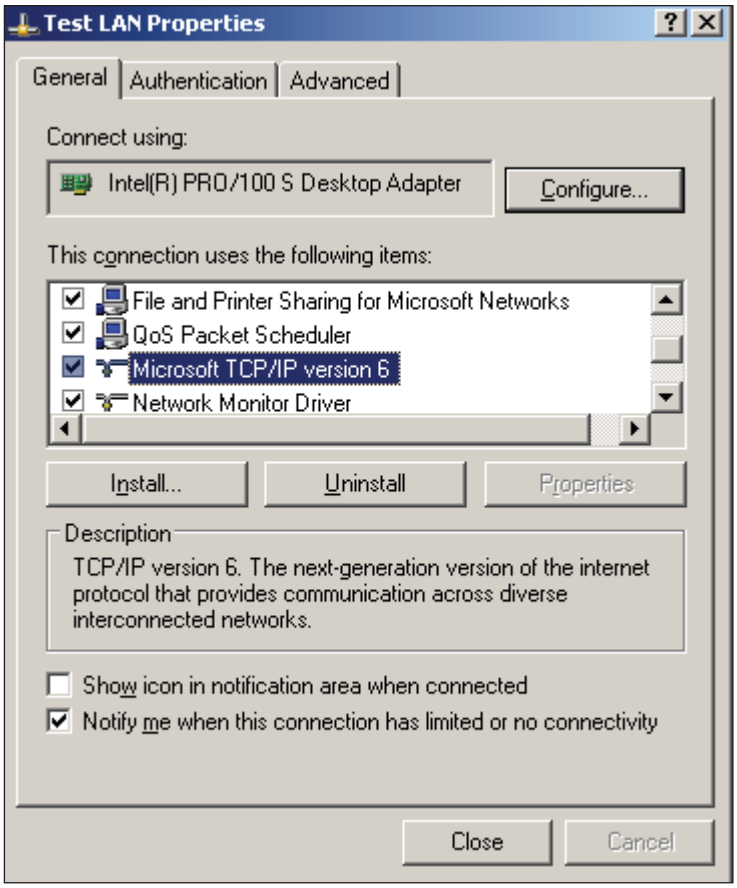
Choose **Protocol**, and click **Add....**



From the resulting **Select Network Protocol** window, choose **Microsoft TCP/IP version 6**, and click **OK**.



Click **OK** in the previous window, to drop back to the NIC properties window. Ensure that the check box beside **Microsoft TCP/IP version 6** is ticked.



IPv6 is now installed, and enabled.

Close the NIC properties window.

To configure the 6to4 tunnel

Open a **Command Line** window.

The 6to4 tunnel is configured via a set of **netsh** commands.

With IPv6 having been enabled, a set of IPv6 tunnel interfaces are automatically created, including a 6to4 tunnel interface.

```
C:\>netsh interface ipv6 show interface

Querying active state...

Idx  Met    MTU    State         Name

---  ----   -----  ------------  -----
  6  0      1500   Disconnected  Main LAN
  5  0      1500   Disconnected  Test LAN
  4  2      1280   Disconnected  Teredo Tunneling Pseudo-Interface
  3  1      1280   Disconnected  6to4 Pseudo-Interface
  2  1      1280   Disconnected  Automatic Tunneling Pseudo-Interface
  1  0      1500   Connected     oopback Pseudo-Interface
```

Configure the x600's IPv4 address as the relay to which the PC will tunnel its IPv6 data into, in order to communicate with the IPv6 network.

```
C:\>netsh interface ipv6 6to4 set relay 139.72.129.57 enable
Ok.
```

The 6to4 tunnel interface is automatically configured with an IPv6 address that is derived from its IPv4 address. Confirm that bytes 3 through 6 of the address are 8822:170a, which are a hex representation of the IPv4 address 136.34.23.10

```
C:\>netsh interface ipv6 show interface 3
Querying active state...

-----------------------------------------------------------------------

Interface 3: 6to4 Tunneling Pseudo-Interface

Addr Type  DAD State   Valid Life   Pref. Life   Address
---------  ----------- ------------ ------------ ----------------------------
Other      Preferred   infinite     infinite     2002:8822:170a::8822:170a

Connection Name             : 6to4 Tunneling Pseudo-Interface
GUID                        : {A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
State                       : Connected
Metric                      : 1
Link MTU                    : 1280 bytes
True Link MTU               : 65515 bytes
Current Hop Limit           : 128
Reachable Time              : 38s
Base Reachable Time         : 30s
Retransmission Interval     : 1s
DAD Transmits               : 0
DNS Suffix                  :
Firewall                    : disabled
Site Prefix Length          : 48 bits
Zone ID for Link            : 3
Zone ID for Site            : 1
Uses Neighbor Discovery     : No
Sends Router Advertisements : No
Forwards Packets            : No
```

Add a route to the 2002::/16 IPv6 address range via the tunnel.

```
C:\>ipv6 rtu 2002::/16 3 pub
```

```
C:\>netsh interface ipv6 show routes
Querying active state...

Publish  Type      Met   Prefix                    Idx  Gateway/Interface Name
-------  --------  ----  ------------------------  ---  --------------------
yes      Manual    1001  2002::/16                 3    6to4 Tunneling Pseudo-Interface
```

It is now possible to ping to the server in the IPv6 network

```
C:\>ping 2002:8b48:8139:1002::10

Pinging 2002:8b48:8139:1002::10 with 32 bytes of data:

Reply from 2002:8b48:8139:1002::10: time<1ms
Reply from 2002:8b48:8139:1002::10: time<1ms
Reply from 2002:8b48:8139:1002::10: time<1ms
Reply from 2002:8b48:8139:1002::10: time<1ms

Ping statistics for 2002:8b48:8139:1002::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To install IPv6 protocol in Windows Vista

Configuring Windows Vista uses the same commands as are used on Windows XP. The only difference is that the IPv6 protocol does not have to be installed at the start of the process, as it is installed by default.

ISATAP tunneling

6to4 tunneling is effective for connecting IPv6 networks to each other over an IPv4 network, or for connecting IPv6 hosts to an IPv6 network. However, it does not enable IPv6 hosts connected to an IPv4 network to communicate directly to each other.

An alternative tunneling technique is **ISATAP tunneling**, which enables direct IPv6 host-to-host communication across an IPv4 network, and host communication to an IPv6 network across an IPv4 network. Unlike 6to4 tunneling, it does not enable whole IPv6 networks to communicate with each other across an IPv4 network.

In this solution example, we will look at configuring an Allied Telesis 8000-series switch to use ISATAP to enable it to be managed by IPv6 even though it is attached to an IPv4 network.

Configuring the ISATAP router

Before considering the configuration of the 8000-series switch, we need to look at the setting up of an ISATAP router.

Any IPv4 network that uses ISATAP needs an ISATAP router connected to some point on the IPv4 network. The router **advertises** to the ISATAP host the IPv6 subnet address that is being used on the network. The ISATAP hosts **learn** this subnet address from the router, and derive their own host addresses by appending their IPv4 address to the end of the IPv6 subnet address.

The format of the ISATAP host IPv6 addresses is:

2002:XX:XX:XX:XX::5efe:<ipv4 address>

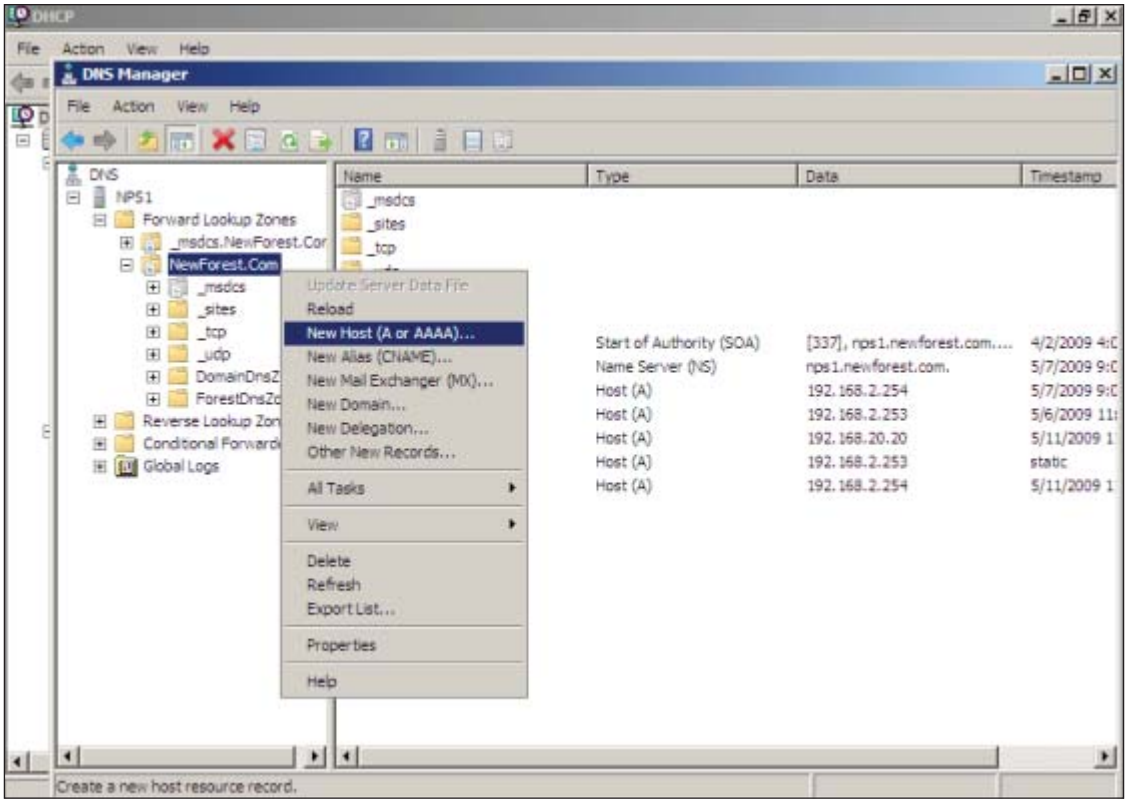
e.g. 2002:c0a8:500:1001::5efe:192.168.3.11

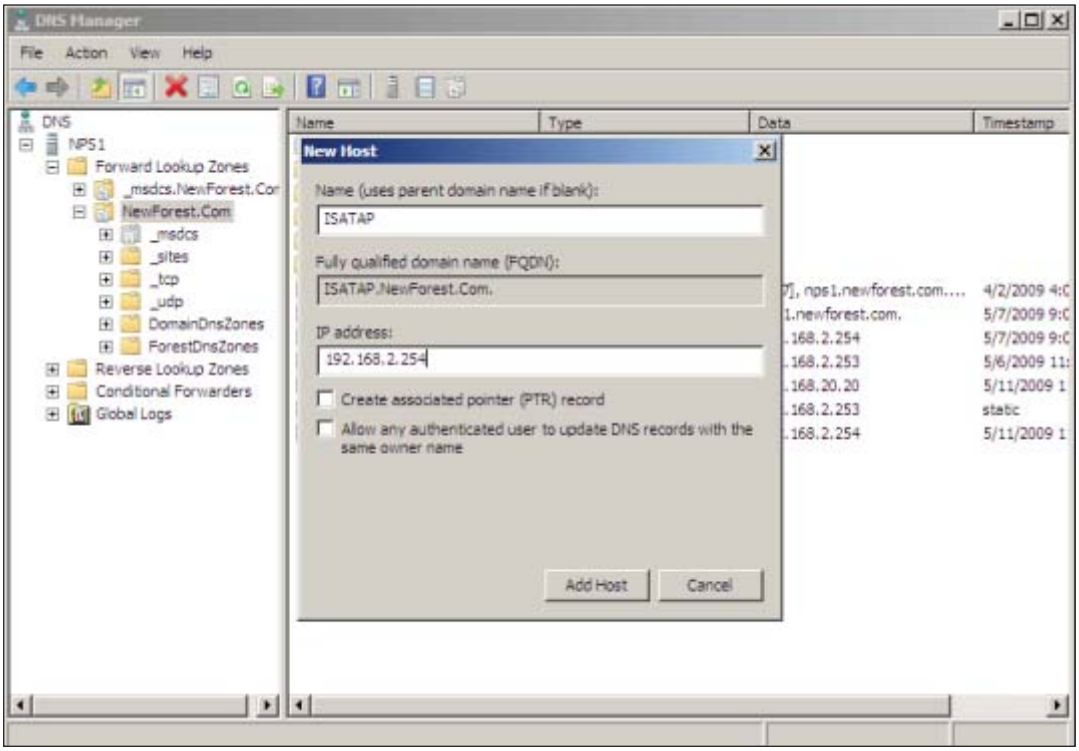
Where 2002:XX:XX:XX:XX is the subnet address advertised from the ISATAP router. The ISATAP router can also be used to enable the ISATAP hosts to communicate with an IPv6 network.

In this solution, we will use a Microsoft Windows 2008 server as the ISATAP router.

To set up an ISATAP router

First, it is necessary to add a record to the network's DNS server. Most ISATAP host implementations find the identity of the ISATAP router by performing a DNS lookup for the name ISATAP.<domain name>. So, add a record for the name ISATAP to the network's DNS server.

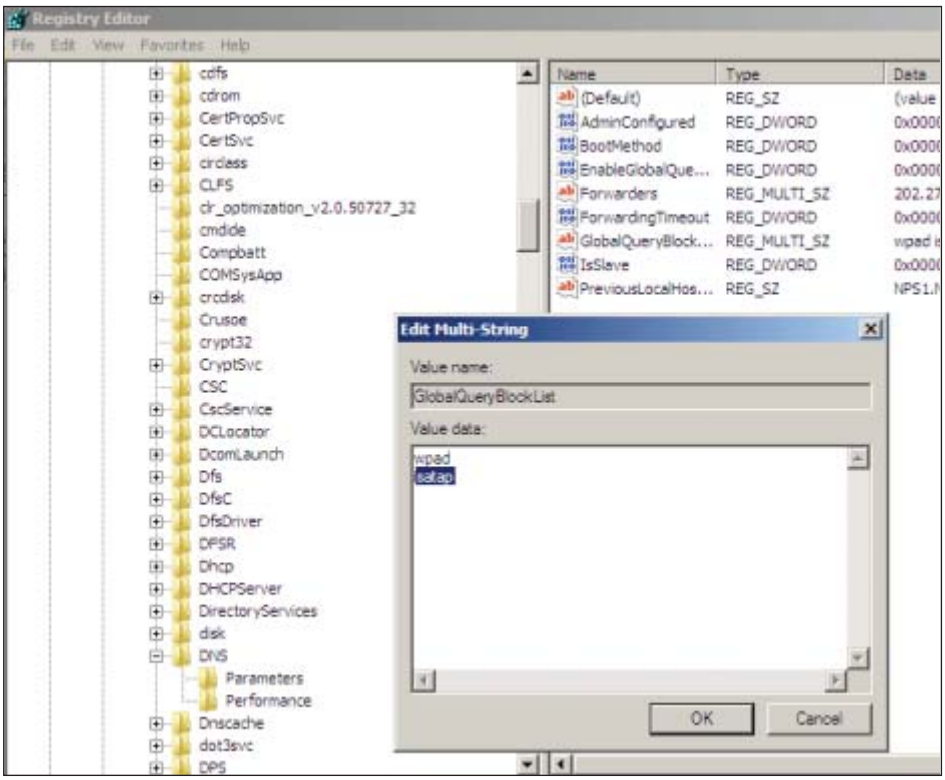


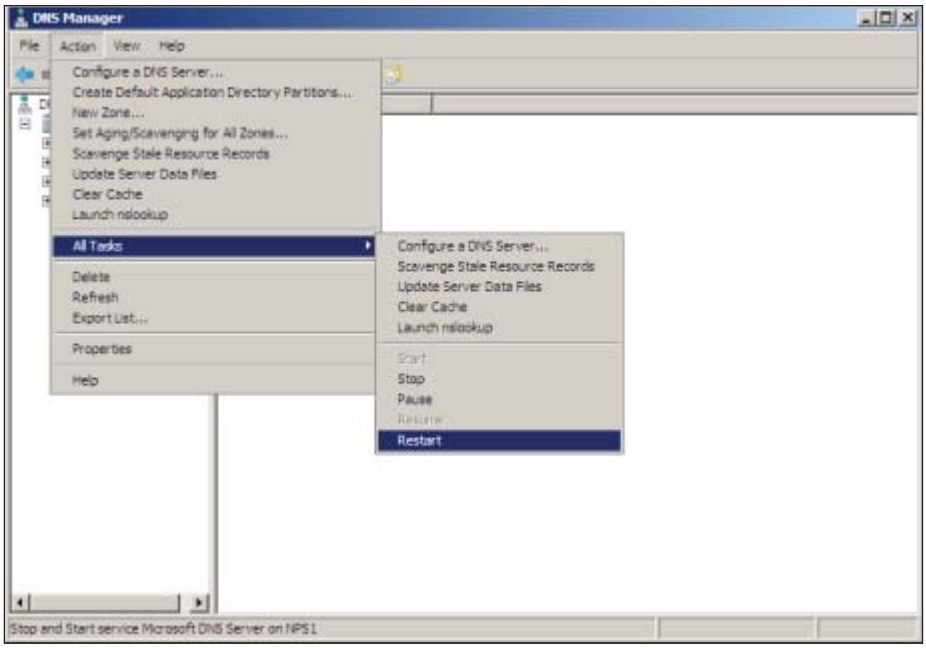


By default, the Microsoft Windows DNS server will block DNS requests for the name **isatap**. To re-configure to server to accept these requests, you need to edit the registry.

Run **Regedit**, and navigate to the Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters.

Within this key, double-click on the parameter **GlobalQueryBlockList**. This will list the names that server is currently blocking requests for. Delete the name **isatap** from this list.



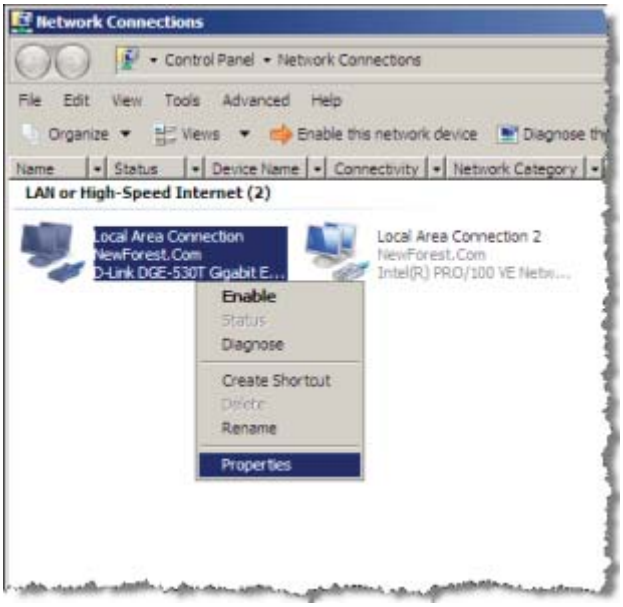


To configure the Microsoft Windows Server 2008 as an ISATAP router:

Begin by configuring an IPv6 address on the interface that attaches to the IPv6 network.

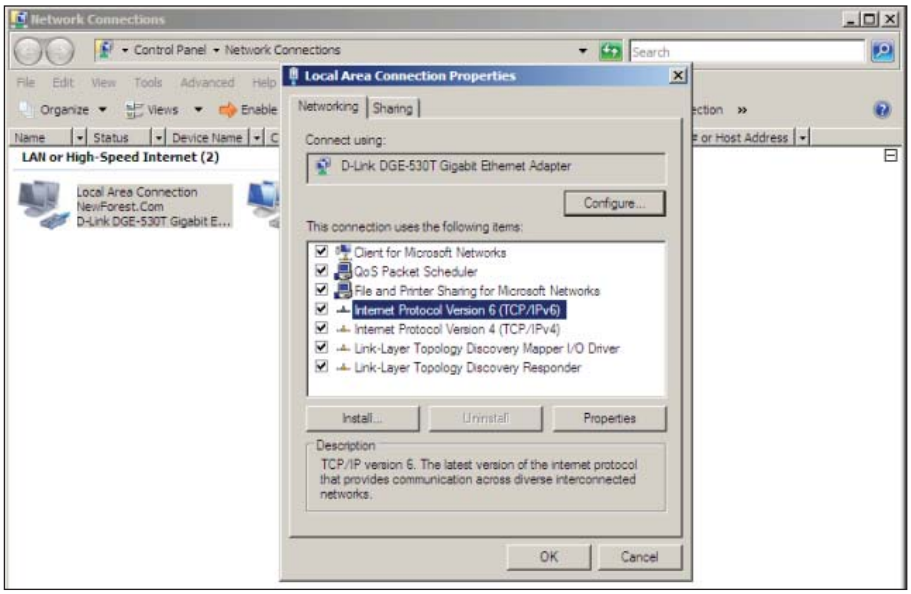
For this change to take effect, it is necessary to **restart** the DNS server.

In **Control Panel** > **Network Connections**, right-click on the NIC that connects to the IPv6 network, and choose **Properties** from the resulting pop-up menu.

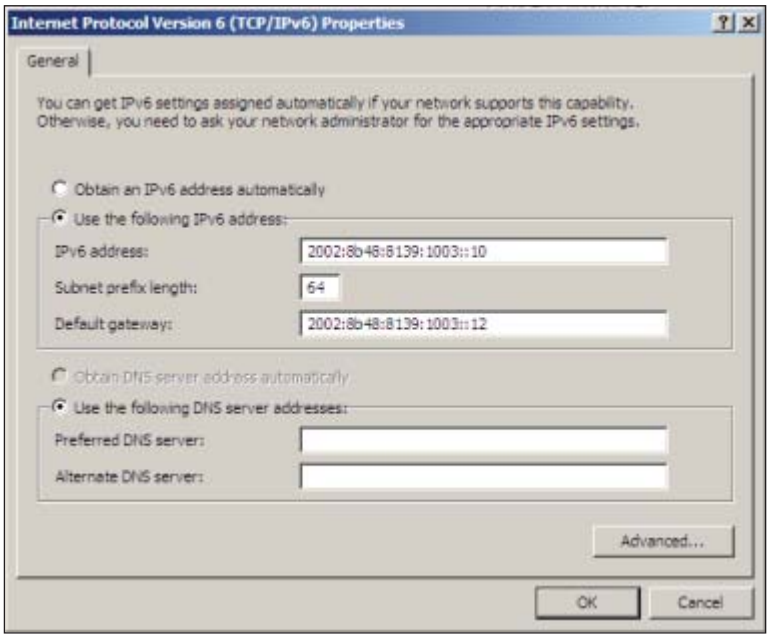


This will open the **NIC properties** window.

In this window, choose **Internet Protocol Version 6(TCP/IPv6)**, then click **Properties**.



This will open the **IPv6 Properties** window. In this window specify an **IPv6 address** and **Default gateway**.



The configuring of the ISATAP interface on the Server is carried out on the command line.

At the command line:

Set the ISATAP router address to be the IP address on the server's own IPv4 interface

```
C:\Users\Administrator>netsh interface isatap set router 192.168.2.254
Ok.
```

The server will possess a set of IPv6 interfaces. It is not immediately obvious which one is the ISATAP interface.

```
C:\Users\Administrator>netsh interface ipv6 show interface

Idx  Met  MTU    State        Name

---  ---  -----  -----------  -------------------
  1   50 4294967295  connected  Loopback Pseudo-Interface 1
 19   25   1280   connected    Local Area Connection* 8
 11   10   1280   disconnected Local Area Connection* 9
 13   25   1280   connected    Local Area Connection* 11
 10   20   1500   connected    Local Area Connection
 12   20   1500   connected    Local Area Connection 2
```

In this case, the ISATAP interface is interface **13**. This is seen from the fact that the link-local IPv6 address on this interface is of the form **fe80::5efe:<IPv4 address>**, which is the form of the link-local address for an ISATAP interface.

```
C:\Users\Administrator>netsh interface ipv6 show addresses 13

Address fe80::5efe:192.168.2.254%13 Parameters

----------------------------------------------------------
Interface Luid       : Local Area Connection* 11
Scope Id             : 0.13
Valid Lifetime       : infinite
Preferred Lifetime   : infinite
DAD State            : Preferred
Address Type         : Other
```

Configure this interface as a routing interface, which sends out router advertisements.

```
C:\Users\Administrator>netsh interface ipv6 set interface 13 forwarding=enable
Ok.

C:\Users\Administrator>netsh interface ipv6 set interface 13 advertise=enabled
Ok.
```

Configure a subnet address that the router will advertise to the ISATAP hosts attached to the IPv4 network.

```
C:\Users\Administrator>netsh interface ipv6 add route 2002:c0a8:0500:1001::/64
13 publish=yes
Ok.
```

Configure the interface connected to the IPv6 network as a routing interface, which sends out router advertisements.

```
C:\Users\Administrator>netsh interface ipv6 set interface 10 advertise=enabled
Ok.

C:\Users\Administrator>netsh interface ipv6 set interface 10 forwarding=enabled
Ok.
```

Add a default route that is directed towards the IPv6 network. This route must be set with **Publish=yes**. This will ensure that the router advertisements sent from the ISATAP interface will advertise the router as a default router. If the 8000-series switch (and other ISATAP hosts) receives router advertisements that do not identify the router as a default router, then it will not create an IPv6 default route, and will not be able to communicate outside its local IPv6 subnet.

```
C:\Users\Administrator>netsh interface ipv6 add route::/0 interface=10
next=2002:8b48:8139:1003::12 publish=yes
Ok.
```

The Microsoft Windows 2008 server is now set up as an **ISATAP router.**

Configuring the 8000-series switch as an ISATAP host

An IPv4 IP address and default gateway needs to be configured on the switch

```
interface vlan 1
ip address 192.168.3.11 255.255.255.0
ip default-gateway 192.168.3.254
```

Create the ISATAP tunnel interface

```
interface tunnel 1
tunnel mode ipv6ip isatap
tunnel source auto
```

A DNS server and domain name need to be configured, so that the switch can perform the DNS lookup to identify the ISATAP router

```
ip domain-name newforest.com
ip name-server  192.168.2.254
```

Configure the switch for management by SNMPv6

```
snmp-server community public rw
 2002:c0a8:500:1001::5efe:192.168.2.254
```

The switch will discover the IPv4 address of the ISATAP router

```
sh ipv6 tunnel

Router DNS name : isatap
Router IPv4 address : 192.168.2.254
DNS Query interval    : 10 seconds
Min DNS Query interval     : 0 seconds
Router Solicitation interval      : 10 seconds
Min Router Solicitation interval : 0 seconds
Robustness : 20
```

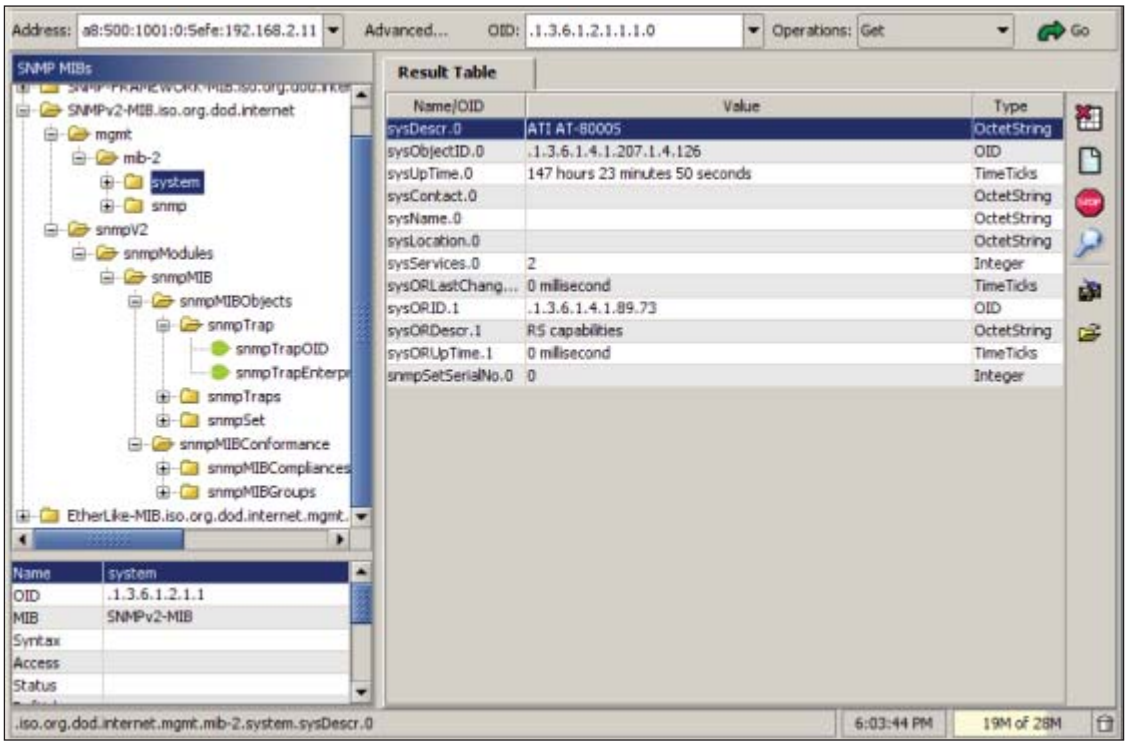
The switch will automatically generate its ISATAP IPv6 address by appending its IPv4 address to the IPv6 subnet address advertised by the ISATAP router. It will also have the link-local IPv6 address of the ISATAP router as its IPv6 default gateway.

```
console# sh ipv6 interface

Interface    IP addresses                                          Type
-----------  ------------------------------------------------  ------------
tunnel1      2002:c0a8:500:1001::5efe:192.168.3.11             other
tunnel1      fe80::5efe:192.168.3.11                           linklayer


Default Gateway IP address                 Type       Interface   State
-----------------------------------------  --------   ---------   -----------
fe80::5efe:192.168.2.254                   Dynamic    tunnel1     reachable

console# sh ipv6 route

Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisment
The number in the brackets is the metric.

ND ::/0 via fe80::5efe:192.168.2.254 [32] tunnel1 Lifetime 60462 sec
L  2002:c0a8:500:1001::/64 is directly connected, tunnel1 Lifetime 2145528 sec
```

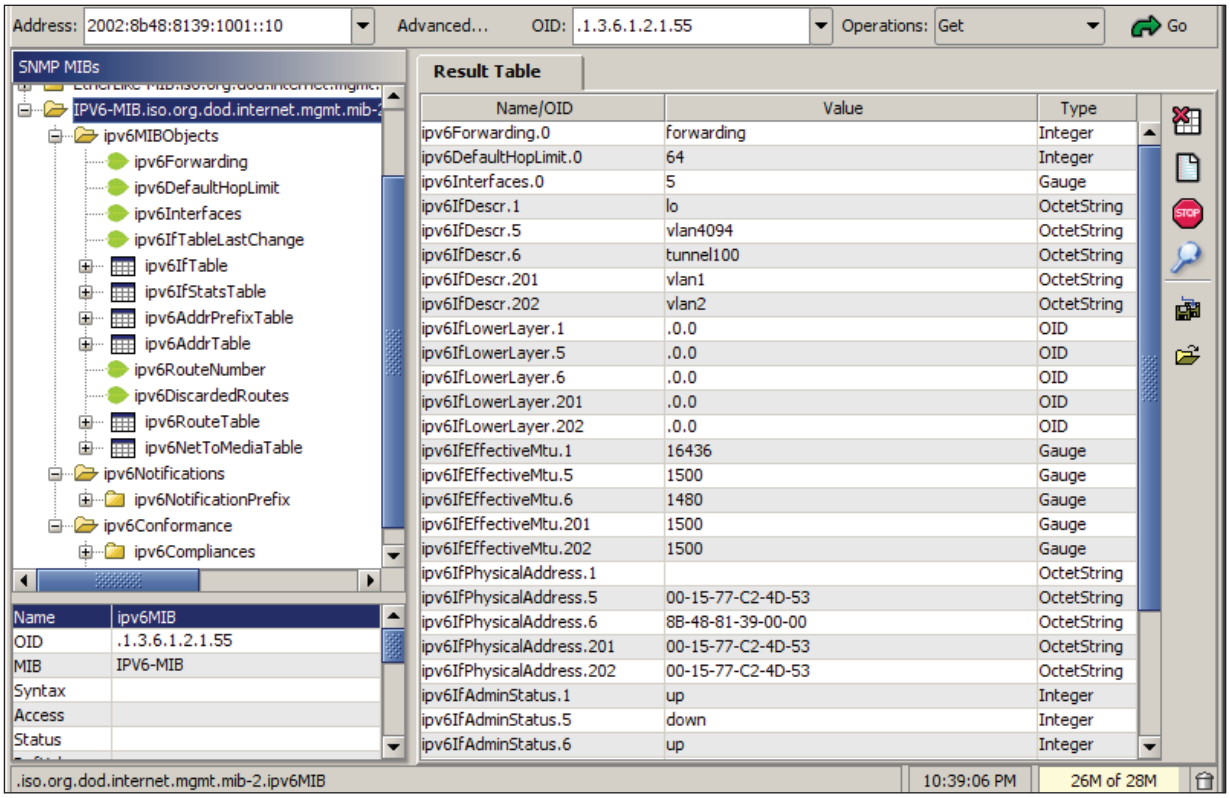
IPv6 network management

The ISATAP configuration on the 8000-series switch means that it can be managed by IPv6 from an IPv6-capable management station.

For example, the switch can be accessed by a MIB browser using SNMPv6.



Similarly, the 6to4 router can be managed by SNMPv6. in fact, the x-series switches support the IPv6 MIB, and so the IPv6 statistics in the switch can be accessed by SNMPv6.



About Allied Telesis Inc.

Allied Telesis is a world class leader in delivering IP/Ethernet network solutions to the global market place. We create innovative, standards-based IP networks that seamlessly connect you with voice, video, and data services.

Enterprise customers can build complete end-to-end networking solutions through a single vendor, with core to edge technologies ranging from powerful 10 Gigabit Layer 3 switches right through to media converters.

Allied Telesis also offer a wide range of access, aggregation, and backbone solutions for Service Providers. Our products range from industry leading media gateways which allow voice, video, and data services to be delivered to the home and business, right through to high-end chassis-based platforms providing significant network infrastructure.

Allied Telesis' flexible service and support programs are tailored to meet a wide range of needs, and are designed to protect your Allied Telesis investment well into the future.

Visit us online at www.alliedtelesis.com

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

www.alliedtelesis.com

 C618-31020-00 Rev. A

Connecting The IP World

Allied Telesis