Disabling Unused IPv6 Transition Technologies for DirectAccess Clients

From a client perspective, DirectAccess is an **IPv6-only** solution and requires IPv6 connectivity end to end. To enable the solution to work on **IPv4-only** networks, DirectAccess makes use of one of several IPv6 transition technologies – 6to4, Teredo, or IP-HTTPS. By leveraging these IPv6 transition technologies, a DirectAccess client can communicate with the DirectAccess server when they are both connected to the public IPv4 Internet, which is the most common deployment scenario today.

The first two IPv6 transition technologies, 6to4 and Teredo, both require that the DirectAccess server be directly connected to the **public** Internet. Beginning with Windows Server 2012, placing the DirectAccess server behind a border router or edge firewall performing Network Address Translation (NAT) is now supported. However, in this deployment model only the **IP-HTTPS** IPv6 transition protocol can be utilized. In this scenario, it is recommended to **disable** the unused IPv6 transition protocols to prevent potential connectivity issues. You can disable them on a **per-host** basis using PowerShell, which is fine for individual client testing purposes, or **globally** using Active Directory Group Policy Objects (GPOs), which is recommend for enterprise-wide production deployment.

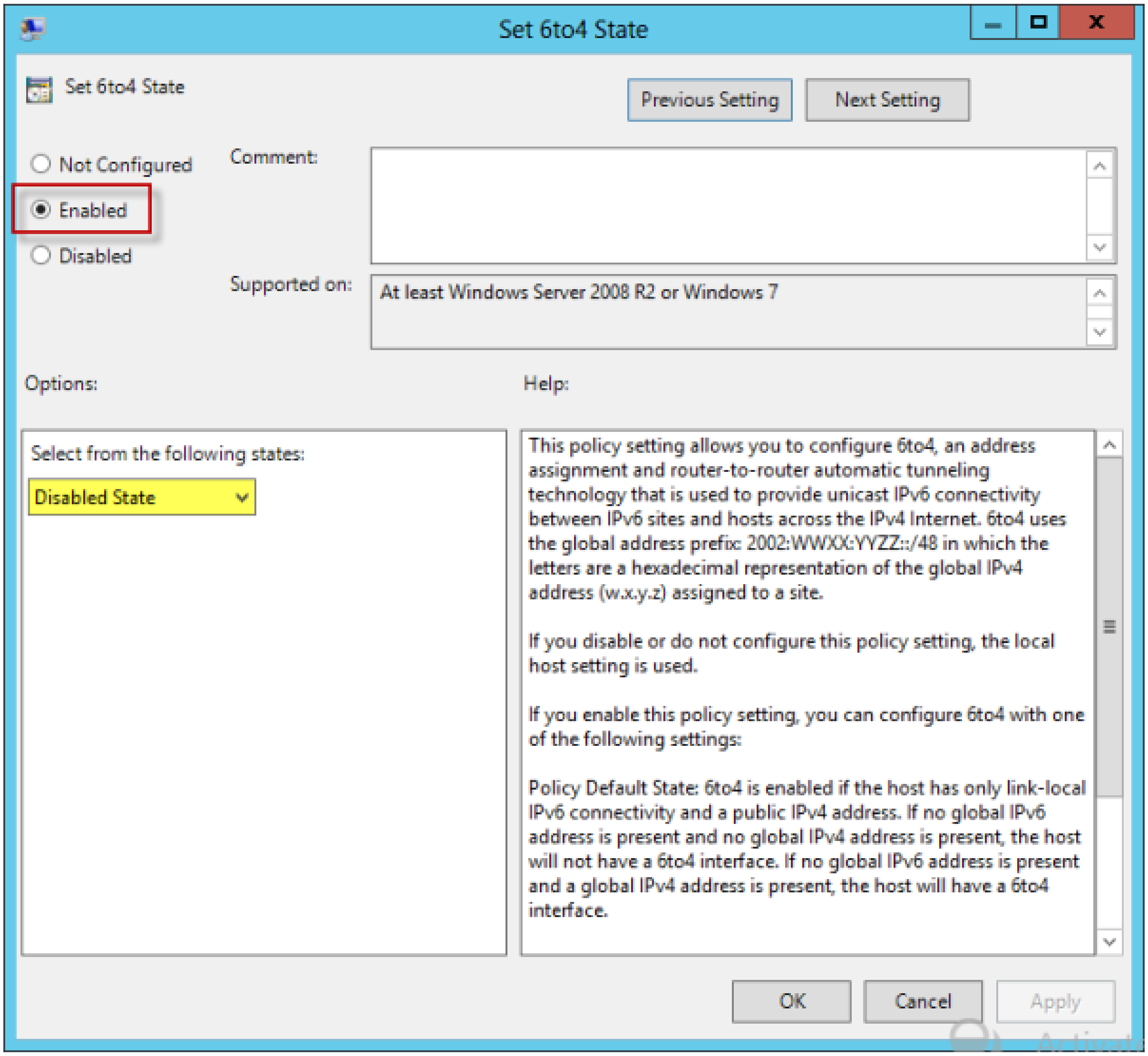
To disable unused IPv6 transition protocols on a per-host basis on **Windows 8** clients using PowerShell, open an elevated PowerShell prompt and execute the following commands:

```
Set-Net6to4Configuration –State disabled
Set-NetTeredoConfiguration –Type disabled
Set-NetIsatapConfiguration –State disabled
```

To disable unused IPv6 transition protocols on a per-host basis on **Windows 7** client using netsh, open an elevated command prompt and execute the following commands:

```
netsh interface 6to4 set state disabled
netsh interface teredo set state disabled
netsh interface isatap set state disabled
```

To disable unused IPv6 transition protocols using Active Directory GPO, open the Group Policy Management Console (GPMC) and create a new GPO. Edit the GPO by navigating to **Computer Configuration / Policies / Administrative Templates / Network / TCP/IP Settings / IPv6 Transition**. Double-click **Set 6to4 State** and enable the policy, then select **Disabled State** from the list of states. Repeat these steps for **Teredo** and **ISATAP**.



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

Select from the following states: Disabled State

Help:

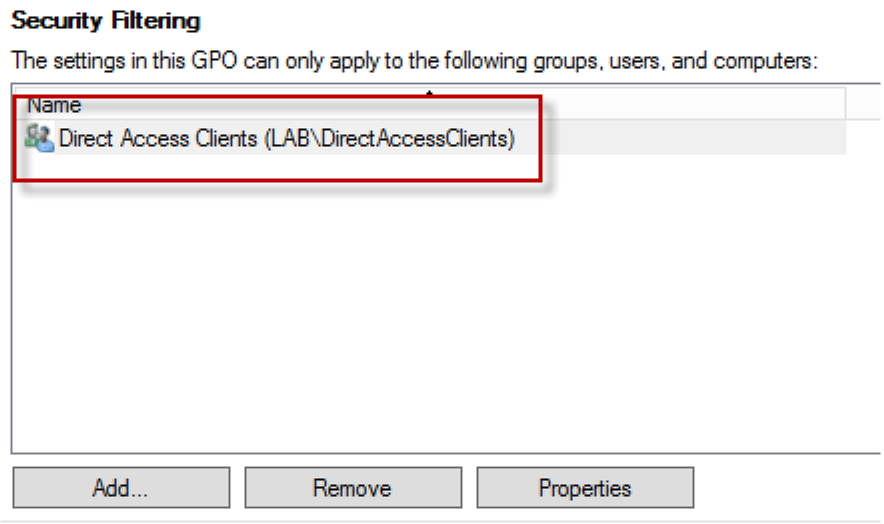
This policy setting allows you to configure 6to4, an address assignment and router-to-router automatic tunneling technology that is used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. 6to4 uses the global address prefix: 2002:WWXX:YYZZ::/48 in which the letters are a hexadecimal representation of the global IPv4 address (w.x.y.z) assigned to a site.

If you disable or do not configure this policy setting, the local host setting is used.

If you enable this policy setting, you can configure 6to4 with one of the following settings:

Policy Default State: 6to4 is enabled if the host has only link-local IPv6 connectivity and a public IPv4 address. If no global IPv6 address is present and no global IPv4 address is present, the host will not have a 6to4 interface. If no global IPv6 address is present and a global IPv4 address is present, the host will have a 6to4 interface.

Change the **security filtering** for the GPO and specify the security group for your DirectAccess clients. Once complete, link the new GPO to the domain.



Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Direct Access Clients (LAB\DirectAccessClients)

As a **reminder**, the steps above are for disabling unused IPv6 transition protocols in a deployment scenario where the DirectAccess server is running **Windows Server 2012/R2** and is deployed **behind a NAT device**. If your DirectAccess server is connected directly to the public Internet, disabling these IPv6 transition protocols is not required.