Knowledge Base

HOW TO: Install and Configure a Virtual Private Network Server in Windows 2000

PSS ID Number: 308208

Article Last Modified on 3/10/2004

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional

This article was previously published under Q308208
For a Microsoft Windows XP version of this article, see 314076.
For a Microsoft Small Business Server 2000 version of this article, see 320697.

IN THIS TASK

SUMMARY

A virtual private network (VPN), allows you to connect components to a network, via another network, such as the Internet. You can make your Windows 2000 Server-based computer a remote-access server so that other users can connect to it by using VPN, and then access shared files on your local drives or on your network. Virtual private networks accomplish this by "tunneling" through the Internet or another public network in a manner that provides the same security and features as a private network. With a VPN, connections across the public network can transfer data using the routing infrastructure of the Internet, but to the user it appears as though the data were being sent over a dedicated private link.

This article describes how to install virtual private networking (VPN) and how to create a new VPN connection in Windows 2000.

back to the top

Overview of VPN

A virtual private network (VPN) is a means of connecting to a private network (such as your office network) by way of a public network, such as the Internet. This combines the virtues of a dial-up connection to a dial-up server with the ease and flexibility of an Internet connection. By using an Internet connection, you can travel worldwide and still, in most places, connect to your office with a local call to the nearest Internet access phone number. If you have a high-speed Internet connection (such as cable or DSL) at your computer (and at your office), you can communicate with your office at full Internet speed, which is much faster than any dial-up connection using an analog modem.

VPNs use authenticated links to ensure that only authorized users can connect to your network, and they use encryption to ensure that data that travels over the Internet can't be intercepted and used by others. Windows achieves this security using Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP).

VPN technology also allows a corporation to connect to its branch offices or to other companies over a public network (such as the Internet) while maintaining secure communications. The VPN connection across the Internet logically operates as a dedicated wide area network (WAN) link.

back to the top

Components of a VPN

A VPN in Windows 2000 consists of a VPN server, a VPN client, a VPN connection (the portion of the connection in which the data is encrypted), and the tunnel (the portion of the connection in which the data is encapsulated). The tunneling is done through one of the tunneling protocols included with Windows 2000, both of which are installed with Routing and Remote Access. The two tunneling protocols included with Windows 2000 are:

- **Point-to-Point Tunneling Protocol (PPTP)**: Provides data encryption using Microsoft Point-to-Point Encryption.
- **Layer Two Tunneling Protocol (L2TP)**: Provides data encryption, authentication, and integrity using IPSec.

Your connection to the Internet should use a dedicated line such as T1, Fractional T1, or Frame Relay. The WAN adapter must be configured with the IP address and subnet mask assigned for your domain or supplied by an Internet service provider (ISP), as well as the default gateway of the ISP router.

NOTE: To enable VPN, you must be logged on using an account that has administrative rights.

back to the top

How to Install and Enable VPN

To install and enable a VPN server, follow these steps:

1. On the Microsoft Windows 2000 VPN computer, confirm that both the connection to the Internet and the connection to your local area network (LAN) are correctly configured.
2. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
3. Click the server name in the tree, and click **Configure and Enable Routing and Remote Access** on the **Action** menu, and then click **Next**.
4. In the **Common Configurations** dialog box, click **Virtual private network (VPN server)**, and then click **Next**.
5. In the **Remote Client Protocols** dialog box, confirm that TCP/IP is included in the list, click **Yes, all of the available protocols are on this list**, and then click **Next**.
6. In the **Internet Connection** dialog box, select the Internet connection that will connect to the Internet, and then click **Next**.
7. In the **IP Address Assignment** dialog box, select **Automatically** in order to use the DHCP server on your subnet to assign IP addresses to dialup clients and to the server.
8. In the **Managing Multiple Remote Access Servers** dialog box, confirm that the **No, I don't want to set up this server to use RADIUS now** checkbox is selected.
9. Click **Next**, and then click **Finish**.
10. Right click the **Ports** node, and then click **Properties**.
11. In the **Ports Properties** dialog box, click the WAN Miniport (PPTP) device, and then click **Configure**.
12. In the **Configure Device - WAN Miniport (PPTP)** dialog box, do one of the following:
    - If you do not want to support direct user dialup VPN to modems installed on the server, click to clear the **Demand-Dial Routing Connections (Inbound and Outbound)** check box.
    - If you do want to support direct user dialup VPN to modems installed on the server, click to select the **Demand-Dial Routing Connections (Inbound and Outbound)** check box.
13. Type the maximum number of simultaneous PPTP connections that you want to allow in the **Maximum Ports** text box. (This may depend on the number of available IP addresses.
14. Repeat steps 11 through 13 for the L2TP device, and then click **OK**.

back to the top

How to Configure the VPN Server

To further configure the VPN server as required, follow these steps.

Configuring the Remote Access Server as a Router

For the remote access server to forward traffic properly inside your network, you must configure it as a router with either static routes or routing protocols, so that all of the locations in the intranet are reachable from the remote access server.

To configure the server as a router:

1. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click the server name, and then click **Properties**.
3. On the **General** tab, click to select **Enable This Computer As A Router**.
4. Select either **Local area network (LAN) routing only** or **LAN and demand-dial routing**, and then click **OK** to close the **Properties** dialog box.

back to the top

How to Configure PPTP Ports

Confirm the number of PPTP ports that you need. To verify the number of ports or to add ports, follow these steps:

1. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, expand **Routing and Remote Access**, expand the server name, and then click **Ports**.
3. Right-click **Ports**, and then click **Properties**.
4. In the **Ports Properties** dialog box, click **WAN Miniport (PPTP)**, and then click **Configure**.
5. In the **Configure Device** dialog box, select the maximum number of ports for the device, and then select the options to specify whether the device accepts incoming connections only, or both incoming and outgoing connections.

back to the top

How to Manage Addresses and Name Servers

The VPN server must have IP addresses available in order to assign them to the VPN server's virtual interface and to VPN clients during the IP Control Protocol (IPCP) negotiation phase of the connection process. The IP address assigned to the VPN client is assigned to the virtual interface of the VPN client.

For Windows 2000-based VPN servers, the IP addresses assigned to VPN clients are obtained through DHCP by default. You can also configure a static IP address pool. The VPN server must also be configured with name resolution servers, typically DNS and WINS server addresses, to assign to the VPN client during IPCP negotiation.

back to the top

How to Manage Access

Configure the dial-in properties on user accounts and remote access policies to manage access for dial-up networking and VPN connections.

NOTE: By default, users are denied access to dial-up.

back to the top

Access by User Account

If you are managing remote access on a user basis, click **Allow Access** on the **Dial-In** tab of the user's **Properties** dialog box for those user accounts that are allowed to create VPN connections. If the VPN server is allowing only VPN connections, delete the default remote access policy called "Allow Access If Dial-In Permission Is Enabled." Then create a new remote access policy with a descriptive name, such as VPN Access If Allowed By User Account. For more information, see Windows 2000 Help.

CAUTION: After you delete the default policy, a dial-up client that does not match at least one of the policy configurations you create will be denied access.

If the VPN server is also allowing dial-up remote access services, do not delete the default policy, but move it so that it is the last policy to be evaluated.

back to the top

Access by Group Membership

If you are managing remote access on a group basis, click the **Control access through remote access policy** radio button on all user accounts by using the Active Directory Users and Computers Console in Administrator Tools or MMC snap-in. Create a Windows 2000 group with members who are allowed to create VPN connections. If the VPN server allows only VPN connections, delete the default remote access policy called Allow Access If Dial-In Permission Is Enabled. Next, create a new remote access policy with a descriptive name such as VPN Access If Member Of VPN-Allowed Group, and then assign the Windows 2000 group to the policy.

If the VPN server also allows dial-up networking remote access services, do not delete the default policy; instead move it so that it is the last policy to be evaluated.

back to the top

How to Configure a VPN Connection from a Client Computer

To set up a connection to a VPN:

1. On the client computer, confirm that the connection to the Internet is correctly configured.
2. Click **Start**, point to **Settings**, and then click **Network And Dial-Up Connections**.
3. Double-click **Make New Connection**.
4. Click **Next**, and then click **Connect To A Private Network Through The Internet**, and then click **Next**.
5. Do one of the following:
   - If you use a dial-up connection to connect to the Internet, click **Automatically Dial This Initial Connection** and then select your dial-up Internet connection from the list.
   - If you use a full-time connection (such as a cable modem), click **Do Not Dial The Initial Connection**.
6. Click **Next**.
7. Type the host name (for example, Microsoft.com) or the IP address (for example, 123.123.123.123) of the computer to which you want to connect, and then click **Next**.
8. Click to select **For All Users** if you want the connection to be available to anyone who logs on to the computer, or click to select **Only For Myself** to make it available only when you log onto the computer, and then click **Next**.
9. Type a descriptive name for the connection, and then click **Finish**.

   NOTE: This option is available only if you are logged on as a member of the Administrators group.
10. Click **Start**, point to **Settings**, and then click **Network And Dial-Up Connections**.
11. Double-click the new connection.
12. Click **Properties** to further configure options for the connection:
    - If you are connecting to a domain, click the **Options** tab, and then click to select the **Include Windows logon domain** check box to specify whether to request Windows 2000 logon domain information before attempting to connect.
    - If you want the connection to be redialed if the line is dropped, click the **Options** tab, and then click to select the **Redial if line is dropped** check box.

To use the connection:

1. Click **Start**, point to **Settings**, and then click **Network And Dial-Up Connections**.
2. Double-click the new connection.
3. If you do not currently have a connection to the Internet, Windows offers to connect to the Internet.
4. Once the connection to the Internet is made, the VPN server prompts you for your user name and password. Enter your user name and password, click **Connect**, and your network resources should be available to you in the same way they are when you connect directly to the network.**NOTE**: To disconnect from the VPN, right-click the connection's icon, and then click **Disconnect**.

back to the top

Troubleshooting

Troubleshooting Remote Access VPNs

Unable to Establish a Remote Access VPN Connection

- **Cause**: The machine name of the client computer is the same as the machine name of another computer on the network.

  Solution: Verify that the machine names of all computers on the network and connecting to the network are using unique machine names.
- **Cause**: The Routing and Remote Access service is not started on the VPN server.

  Solution: Verify the state of the Routing and Remote Access service on the VPN server.

See Windows 2000 online Help for more information about how to monitor the Routing and Remote Access service, and how to start and stop the Routing and Remote Access service.

- **Cause**: Remote access is not enabled on the VPN server.

  Solution: Enable remote access on the VPN server.

  See Windows 2000 online Help for more information about how to enable the remote access server.

- **Cause**: PPTP or L2TP ports are not enabled for inbound remote access requests.

  Solution: Enable PPTP or L2TP ports, or both, for inbound remote access requests.

  See Windows 2000 online Help for more information about how to configure ports for remote access.

- **Cause**: The LAN protocols used by the VPN clients are not enabled for remote access on the VPN server.

  Solution: Enable the LAN protocols used by the VPN clients for remote access on the VPN server.

  See Windows 2000 online Help for more information about how to view properties of the remote access server.

- **Cause**: All of the PPTP or L2TP ports on the VPN server are already being used by currently connected remote access clients or demand-dial routers.

  Solution: Verify that all of the PPTP or L2TP ports on the VPN server are not already being used by clicking **Ports** in Routing and Remote Access. If necessary, change the number of PPTP or L2TP ports to allow more concurrent connections.

  See Windows 2000 online Help for more information about how to add PPTP or L2TP ports.

- **Cause**: the VPN server does not support The tunneling protocol of the VPN client.

  By default, Windows 2000 remote access VPN clients use the **Automatic** server type option, which means that they try to establish an L2TP over IPSec-based VPN connection first, and then they try a PPTP-based VPN connection. If VPN clients use either the **Point-to-Point Tunneling Protocol (PPTP)** or **Layer-2 Tunneling Protocol (L2TP)** server type option, verify that the selected tunneling protocol is supported by the VPN server.

  By default, a computer running Windows 2000 Server and the Routing and Remote Access service is a PPTP and L2TP server with five L2TP ports and five PPTP ports. To create a PPTP-only server, set the number of L2TP ports to zero. To create an L2TP-only server, set the number of PPTP ports to zero.

  Solution: Verify that the appropriate number of PPTP or L2TP ports is configured.

  See Windows 2000 online Help for more information about how to add PPTP or L2TP ports.

- **Cause**: The VPN client and the VPN server in conjunction with a remote access policy are not configured to use at least one common authentication method.

  Solution: Configure the VPN client and the VPN server in conjunction with a remote access policy to use at least one common authentication method.

  See Windows 2000 online Help for more information about how to configure authentication.

- **Cause**: The VPN client and the VPN server in conjunction with a remote access policy are not configured to use at least one common encryption method.

  Solution: Configure the VPN client and the VPN server in conjunction with a remote access policy to use at least one common encryption method.

  See Windows 2000 online Help for more information about how to configure encryption.

- **Cause**: The VPN connection does not have the appropriate permissions through dial-in properties of the user account and remote access policies.

  Solution: Verify that the VPN connection has the appropriate permissions through dial-in properties of the user account and remote access policies. In order for the connection to be established, the settings of the connection attempt must:

  - Match all of the conditions of at least one remote access policy.
  - Be granted remote access permission through the user account (set to **Allow access**) or through the user account (set to **Control access through Remote Access Policy**) and the remote access permission of the matching remote access policy (set to **Grant remote access permission**).
  - Match all the settings of the profile.
  - Match all the settings of the dial-in properties of the user account.

  See Windows 2000 online Help for an introduction to remote access policies, and for more information about how to accept a connection attempt.

- **Cause**: The settings of the remote access policy profile are in conflict with properties of the VPN server.

  The properties of the remote access policy profile and the properties of the VPN server both contain settings for:

  - Multilink
  - Bandwidth allocation protocol
  - Authentication protocols

  If the settings of the profile of the matching remote access policy are in conflict with the settings of the VPN server, the connection attempt is rejected. For example, if the matching remote access policy profile specifies that the EAP-TLS authentication protocol must be used and EAP is not enabled on the VPN server, the connection attempt is rejected.

  Solution: Verify that the settings of the remote access policy profile are not in conflict with properties of the VPN server.

  See Windows 2000 online Help for more information about how to enable authentication protocols, and how to configure authentication.

- **Cause**: The answering router is unable to validate the credentials of the calling router (user name, password, and domain name).

  Solution: Verify that the credentials of the VPN client (user name, password, and domain name) are correct and can be validated by the VPN server.
- **Cause**: There are not enough addresses in the static IP address pool.

  Solution: If the VPN server is configured with a static IP address pool, verify that there are enough addresses in the pool. If all of the addresses in the static pool have been allocated to connected VPN clients, the VPN server is unable to allocate an IP address, and the connection attempt is rejected. Modify the static IP address pool if needed. See Windows 2000 online Help for more information about TCP/IP and remote access, and how to create a static IP address pool.
- **Cause**: The VPN client is configured to request its own IPX node number and the VPN server is not configured to allow IPX clients to request their own IPX node number.

  Solution: Configure the VPN server to allow IPX clients to request their own IPX node number.

  See Windows 2000 online Help for more information about IPX and remote access.
- **Cause**: The VPN server is configured with a range of IPX network numbers that are being used elsewhere on your IPX network.

  Solution: Configure the VPN server with a range of IPX network numbers that is unique to your IPX network.

  See Windows 2000 online Help for more information about IPX and remote access.
- **Cause**: The authentication provider of the VPN server is improperly configured.

  Solution: Verify the configuration of the authentication provider. You can configure the VPN server to use either Windows 2000 or RADIUS to authenticate the credentials of the VPN client.

  See Windows 2000 online Help for more information about authentication and accounting providers, and how to use RADIUS authentication.
- **Cause**: The VPN server cannot access Active Directory.

  Solution: For a VPN server that is a member server in a mixed-mode or native-mode Windows 2000 domain that is configured for Windows 2000 authentication, verify the following:

  - The **RAS and IAS Servers** security group exists. If not, create the group and set the group type to Security and the group scope to Domain local.
  - The **RAS and IAS Servers** security group has Read permission to the **RAS and IAS Servers Access Check** object.
  - The computer account of the VPN server computer is a member of the **RAS and IAS Servers** security group. You can use the **netsh ras show registeredserver** command to view the current registration. You can use the "netsh ras add registeredserver" command to register the server in a specified domain.

    If you add (or remove) the VPN server computer to the **RAS and IAS Servers** security group, the change does not take effect immediately (due to the way that Windows 2000 caches Active Directory information). To immediately effect this change, you need to restart the VPN server computer.
  - For a native-mode domain, the VPN server has joined the domain.

  See Windows 2000 online Help for more information about how to add a group, how to verify permissions for the RAS and IAS security group, and about NetShell commands for remote access.
- **Cause**: A Windows NT 4.0 VPN server cannot validate connection requests.

  Solution: If VPN clients are dialing in to a VPN server running Windows NT 4.0 that is a member of a Windows 2000 mixed-mode domain, verify that the Everyone group is added to the Pre-Windows 2000 Compatible Access group with the following command:

  ```
  "net localgroup "Pre-Windows 2000 Compatible Access""
  ```

  If not, type the following command at a command prompt on a domain controller computer, and then restart the domain controller computer:

  ```
  net localgroup "Pre-Windows 2000 Compatible Access" everyone /add
  ```

  See Windows 2000 online Help for more information about Windows NT 4.0 remote access server in a Windows 2000 domain.
- **Cause**: The VPN server is unable to communicate with the configured RADIUS server.

  Solution: If your RADIUS server is only reachable through your Internet interface, add an input filter and an output filter to the Internet interface for UDP port 1812 (based on RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)"), or UDP port 1645 (for older RADIUS servers) for RADIUS authentication and UDP port 1813 (based on RFC 2139, "RADIUS Accounting"), or UDP port 1646 (for older RADIUS servers) for RADIUS accounting.

  See Windows 2000 online Help for more information about how to add a packet filter.
- **Cause**:Cannot connect to the VPN server over the Internet using the Ping.exe utility.

  Solution: Due to the PPTP and L2TP over IPSec packet filtering that is configured on the Internet interface of the VPN server, Internet Control Message Protocol (ICMP) packets used by the ping command are filtered out. To enable the VPN server to respond to ICMP (ping) packets, you need to add an input filter and an output filter that allow traffic for IP protocol 1 (ICMP traffic).

  See Windows 2000 online Help for more information about how to add a packet filter.

back to the top

Troubleshooting Router-to-Router VPNs

Unable to Establish a Router-to-Router VPN Connection

- **Cause**: The Routing and Remote Access service is not started on the VPN client (the calling router) and the VPN server (the answering router).

  Solution: Verify the state of the Routing and Remote Access service on the VPN client and the VPN server.

See Windows 2000 online Help for more information about how to monitor the Routing and Remote Access service, and how to start and stop the Routing and Remote Access service.

- **Cause**: LAN and WAN routing is not enabled on the calling router and the answering router.

  Solution: Enable **Local and remote routing (LAN and WAN router)** on the calling router and the answering router.

  See Windows 2000 online Help for more information about how to enable LAN and WAN routing.
- **Cause**: PPTP or L2TP ports are not enabled for inbound and outbound demand-dial routing connections.

  Solution: Enable PPTP or L2TP ports, or both, for inbound and outbound demand-dial routing connections.

  See Windows 2000 online Help for more information about how to enable routing on ports.
- **Cause**: All of the PPTP or L2TP ports on the calling or answering router are currently in use by connected remote access clients or demand-dial routers.

  Solution: Verify that all of the PPTP or L2TP ports on the VPN server are not already being used by clicking **Ports** in Routing and Remote Access. If necessary, change the number of PPTP or L2TP ports to allow more concurrent connections.

  See Windows 2000 online Help for more information about how to add PPTP or L2TP ports.
- **Cause**: The answering router does not support the tunneling protocol used by the calling router.

  By default, Windows 2000 demand-dial interfaces use the **Automatic** server type option, which means that they attempt to establish an L2TP over IPSec-based VPN connection first, and then a PPTP-based VPN connection. If calling routers use either the **Point-to-Point Tunneling Protocol (PPTP)** or **Layer-2 Tunneling Protocol (L2TP)** server type option, verify that the selected tunneling protocol is supported by the answering router.

  By default, a computer running Windows 2000 Server and the Routing and Remote Access service is a PPTP and L2TP-capable demand dial router with five L2TP ports and five PPTP ports. To create a PPTP-only router, set the number of L2TP ports to zero. To create an L2TP-only router, set the number of PPTP ports to zero.

  Solution: Verify that the appropriate number of PPTP or L2TP ports is configured on the calling router and the answering router.

  See Windows 2000 online Help for more information about how to add PPTP or L2TP ports.
- **Cause**: The calling router and the answering router in conjunction with a remote access policy are not configured to use at least one common authentication method.

  Solution: Configure the calling router and the answering router in conjunction with a remote access policy to use at least one common authentication method.

  See Windows 2000 online Help for more information about how to configure authentication.
- **Cause**: The calling router and the answering router in conjunction with a remote access policy are not configured to use at least one common encryption method.

  Solution: Configure the calling router and the answering router in conjunction with a remote access policy to use at least one common encryption method.

  See Windows 2000 online Help for more information about how to configure encryption.
- **Cause**: The VPN connection does not have the appropriate permissions through dial-in properties of the user account and remote access policies.

  Solution: Verify that the VPN connection has the appropriate permissions through dial-in properties of the user account and remote access policies. In order for the connection to be established, the settings of the connection attempt must:

  - Match all of the conditions of at least one remote access policy.
  - Be granted remote access permission through the user account (set to **Allow access**) or through the user account (set to **Control access through Remote Access Policy**) and the remote access permission of the matching remote access policy (set to **Grant remote access permission**).
  - Match all the settings of the profile.
  - Match all the settings of the dial-in properties of the user account.

  See Windows 2000 online Help for an introduction to remote access policies, and for more information about how to accept a connection attempt.
- **Cause**: The settings of the remote access policy profile are in conflict with properties of the answering router. The properties of the remote access policy profile and the properties of the answering router both contain settings for:

  - Multilink
  - Bandwidth allocation protocol
  - Authentication protocols

  If the settings of the profile of the matching remote access policy are in conflict with the settings of the answering router, the connection attempt is rejected. For example, if the matching remote access policy profile specifies that the EAP-TLS authentication protocol must be used and EAP is not enabled on the answering router, the connection attempt is rejected.

  Solution: Verify that the settings of the remote access policy profile are not in conflict with properties of the remote access router.

  See Windows 2000 online Help for more information about how to enable authentication protocols, and how to configure authentication.
- **Cause**: The credentials of the calling router (user name, password, and domain name) are incorrect and cannot be validated by the answering router.

  Solution: Verify that the credentials of the calling router (user name, password, and domain name) are correct and can be validated by the answering router.
- **Cause**: There are not enough addresses in the static IP address pool.

Solution: If the answering router is configured with a static IP address pool, verify that there are enough addresses in the pool. If all of the addresses in the static pool have been allocated to connected remote access clients or demand-dial routers, the answering router is unable to allocate an IP address, and the connection attempt is rejected. Modify the static IP address pool if needed.

See Windows 2000 online Help for more information about TCP/IP and remote access, and how to create a static IP address pool.

- **Cause**: The answering router is configured with a range of IPX network numbers that are in use elsewhere on your IPX network.

  Solution: Configure the answering router with a range of IPX network numbers that are unique to your IPX network.

  See Windows 2000 online Help for more information about IPX and remote access.

- **Cause**: The authentication provider of the answering router is incorrectly configured.

  Solution: Verify the configuration of the authentication provider. You can configure the answering router to use either Windows 2000 or RADIUS to authenticate the credentials of the VPN client.

  See Windows 2000 online Help for more information about authentication and accounting providers, and how to use RADIUS authentication.

- **Cause**: The answering router cannot access Active Directory.

  Solution: For an answering router that is a member server in mixed-mode or native-mode Windows 2000 domain that is configured for Windows 2000 authentication, verify that:

  - The **RAS and IAS Servers** security group exists. If not, then create the group and set the group type to **Security** and the group scope to **Domain local**.
  - The **RAS and IAS Servers** security group has Read permission to the **RAS and IAS Servers Access Check** object.
  - The computer account of the answering router computer is a member of the **RAS and IAS Servers** security group. You can use the following command to view the current registration:

    ```
    "netsh ras show registeredserver"
    ```

    You can use the following command to register the server in a specified domain:

    ```
    "netsh ras add registeredserver"
    ```

    If you add the answering router computer to, or remove the answering router computer from the **RAS and IAS Servers** security group, the change does not take effect immediately (due to the way that Windows 2000 caches Active Directory information). For the change to take effect immediately, you must restart the answering router computer.
  - For a native-mode domain, the answering router has joined the domain.

  See Windows 2000 online Help for more information about how to add a group, how to verify permissions for the RAS and IAS security group, and about the NetShell commands for remote access.

- **Cause**: An answering router running Windows NT 4.0 with the Routing and Remote Access Service (RRAS) cannot validate connection requests.

  Solution: If calling routers are dialing in to an answering router running Windows NT 4.0 with RRAS that is a member of a Windows 2000 mixed-mode domain, verify that the Everyone group is added to the Pre-Windows 2000 Compatible Access group with the following command:

  ```
  "net localgroup "Pre-Windows 2000 Compatible Access""
  ```

  If not, type the following command at a command prompt on a domain controller computer and then restart the domain controller computer:

  ```
  "net localgroup "Pre-Windows 2000 Compatible Access" everyone /add"
  ```

  See Windows 2000 online Help for more information about Windows NT 4.0 remote access server in a Windows 2000 domain.

- **Cause**: The answering router is unable to communicate with the configured RADIUS server.

  Solution: If your RADIUS server is only reachable through your Internet interface, add an input filter and an output filter to the Internet interface for UDP port 1812 (based on RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)") or to UDP port 1645 (for older RADIUS servers) for RADIUS authentication and UDP port 1813 (based on RFC 2139, "RADIUS Accounting") or to UDP port 1646 (for older RADIUS servers) for RADIUS accounting.

  See Windows 2000 online Help for more information about how to add a packet filter.

- **Cause**: Cannot connect to the answering router from the Internet by using the Ping.exe utility.

  Solution: Due to the PPTP and L2TP over IPSec packet filtering that is configured on the Internet interface of the answering router, Internet Control Message Protocol (ICMP) packets used by the **Ping** command are filtered out. To enable the answering router to respond to ICMP packets, you must add an input filter and an output filter that allow traffic for IP protocol 1 (ICMP traffic).

  See Windows 2000 online Help for more information about how to add a packet filter.

Unable to Send and Receive Data

- **Cause**: The appropriate demand-dial interface has not been added to the protocol being routed.

  Solution: Add the appropriate demand-dial interface to the protocol being routed.

  See Windows 2000 online Help for more information about how to add a routing interface.

- **Cause**: There are no routes on both sides of the router-to-router VPN connection that support the two-way exchange of traffic.

  Solution: Unlike a remote access VPN connection, a router-to-router VPN connection does not automatically create a default route. You need to create routes on both sides of the router-to-router VPN connection so that traffic can be routed to and from the other side of the router-to-router VPN connection.

  You can manually add static routes to the routing table, or you can add static routes through routing protocols. For persistent VPN connections, you can enable Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) across the VPN connection. For on-demand VPN connections, you can automatically update routes through an auto-static RIP update. See Windows 2000 online Help for more information about how to add an IP routing protocol, how to add a static route, and how to perform auto-static

updates

- **Cause**: A two-way initiated, the answering router as a remote access connection is interpreting router-to-router VPN connection.

  Solution: If the user name in the credentials of the calling router appears under **Dial-In Clients** in Routing and Remote Access, the answering router may interpret the calling router as a remote access client. Verify that the user name in the credentials of the calling router matches the name of a demand-dial interface on the answering router. If the incoming caller is a router, the port on which the call was received shows a status of **Active** and the corresponding demand-dial interface is in a **Connected** state.

  See Windows 2000 online Help for more information about how to check the status of the port on the answering router, and how to check the status of the demand-dial interface.

- **Cause**: Packet filters on the demand-dial interfaces of the calling router and answering router are preventing the flow of traffic.

  Solution: Verify that there are no packet filters on the demand-dial interfaces of the calling router and answering router that prevent the sending or receiving of traffic. You can configure each demand-dial interface with IP and IPX input and output filters to control the exact nature of TCP/IP and IPX traffic that is allowed into and out of the demand-dial interface.

  See Windows 2000 online Help for more information about how to manage packet filters.

- **Cause**: Packet filters on the remote access policy profile are preventing the flow of IP traffic.

  Solution: Verify that there are no configured TCP/IP packet filters on the profile properties of the remote access policies on the VPN server (or the RADIUS server if Internet Authentication Service is used) that are preventing the sending or receiving of TCP/IP traffic. You can use remote access policies to configure TCP/IP input and output packet filters that control the exact nature of TCP/IP traffic allowed on the VPN connection. Verify that the profile TCP/IP packet filters are not preventing the flow of needed traffic.

  See Windows 2000 online Help for more information about how to configure IP options.

back to the top

REFERENCES

For additional information about how to create a VPN connection with Windows XP, click the article number below to view the article in the Microsoft Knowledge Base:

305550 HOW TO: Configure a VPN Connection to Your Corporate Network

For additional information, click the following article numbers to view the articles in the Microsoft Knowledge Base:

255784 Increasing security on Windows 2000 VPN Server

254018 How to configure input filters for services that run behind network address translation

260926 Routing and Remote Access Wizard for VPN Server creates non-specific input and output filters

back to the top

Keywords: kbhowto kbHOWTOmaster KB308208
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch

---