

Troubleshooting Microsoft Network Neighborhood After Establishing a VPN Tunnel With the Cisco VPN Client

Document ID: 43066

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Browsing Problems

- Cannot Ping Network Resources and Computers by IP Address, NetBIOS Name, or FQDN

- Cannot Map a Network Drive or Browse Network Neighborhood

- Cannot Log on to the Domain

 - Windows 95/98

 - Windows NT, 2000, and XP

 - Windows ME

Additional Troubleshooting Information

Related Information

Introduction

This document shows how to troubleshoot some common issues while you browse the Network Neighborhood when the Cisco VPN Client runs on Microsoft Windows/NT platforms.

Note: When IP connectivity is present from the remote VPN Client to internal network devices, the issues discussed here need to be resolved by Microsoft. Browsing the Network Neighborhood is a function of Microsoft's browsing service, not the Cisco VPN Client. Network Neighborhood is not supported officially. However, it works if it is configured correctly. Problems occur if the PC or master browsers do not function properly.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN Client
- Microsoft Windows Operating Systems XP, 2000, NT, 95, 98

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Browsing Problems

When the VPN tunnel is established, you cannot browse the Network Neighborhood. This issue can be caused by several common Microsoft networking issues that occur with VPN products issues. The issues are:

- Cannot ping network resources and computers by IP address, NetBIOS name, or FQDN.
- Cannot map a network drive or browse Network Neighborhood.
- Cannot log on to the domain.

The solutions to these specific problems are explained in the various sections of this document . If you still have issues after you check the appropriate solution(s), call Microsoft for detailed debugging support.

Cannot Ping Network Resources and Computers by IP Address, NetBIOS Name, or FQDN

In some cases, you are not be able to ping the remote computer, Windows Internet Naming Service (WINS) server, domain controller, file server by IP address and NetBIOS name and fully qualified domain name (FQDN, such as myserver.mydomain.com). If you *can* ping by IP address, then IP connectivity is present. The problem is most likely related to name resolution issue on your Windows network.

Note: Because IPSec does not allow multicast or broadcast down the tunnel, NETBIOS is not supported over VPN tunnel as it sends broadcasts/multicasts to the network in order to perform the name resolution.

Try these suggestions to resolve your problem.

- If you are able to ping network resources, see the section on Cannot map a network drive or browse Network Neighborhood.
- If you are unable to ping, check routing devices and Network Address Translation (NAT) devices for possible configuration issues.
- For further assistance, refer to the Microsoft web site for information on TCP/IP and name resolution.
 - ◆ Managing TCP/IP Networking
 - ◆ Client Receives Error When Resolving FQDN
 - ◆ Microsoft TCP/IP Host Name Resolution Order
 - ◆ NetBIOS over TCP/IP Name Resolution and WINS
 - ◆ Troubleshooting Browsing with Client for Microsoft Networks
 - ◆ Default Node Type for Microsoft Clients

Cannot Map a Network Drive or Browse Network Neighborhood

IPsec does not encapsulate NetBIOS broadcast traffic. A WINS server is required to map a drive on the Microsoft network.

Consider these suggestions when you try to determine the root of the problem.

- Issue the **net use** CLI command for the shared drive that you try to access.

- Select **Start > Run** and type **Find Computer** to try to locate the network resource.
- Double-click on the Network Neighborhood icon. Check that some or all network resources and PCs are shown.
- Verify that the PC that runs the VPN Client gets the correct WINS and Domain Name System (DNS) information.
 - ◆ Select **Start > Run** and type **winiipcfg** (on Windows 9x machines) or **ipconfig /all** (on Windows NT, 2000, and XP machines) to see this information.
 - ◆ Check event logs and debugs to see the WINS and DNS information that is passed down from the headend device to the remote VPN Client.
- If you use an LMHOSTS file, try to use NetBIOS names by issuing the **nbtstat -c** command. After an LMHOST file is loaded, the lifetime reads -1.
- For Windows 9x and ME clients, verify that the network client is loaded. (This is not supported on XP Home.)

Cannot Log on to the Domain

These are some general items to check if you experience problems.

- Do you use the Cisco VPN Client Start Before Login utility?
- Do you use the client for Microsoft networking on 9x clients?
- Do you see any log in failure event messages on your domain controller when you turn on audit trails?

Detailed troubleshooting information is shown here for specific operating platforms.

Windows 95/98

Verify that the Network Client is loaded.

1. Right-click on Network Neighborhood. Select **Properties**. Verify that Client for Microsoft Networks and File and Printer Sharing are present. Install these features if they are not already installed. Restart the computer if you are prompted to do so.
2. On the VPN Client, click **Options > Properties > Connections** and check **Connect to the Internet via dial-up**.
3. On the VPN Client, click **Options > Windows Logon Properties** and check **Enable start before logon**.

Windows NT, 2000, and XP

Windows NT, 2000 and XP machines behave differently than the Windows 95/98 machines. The VPN Client does not have the option to log on to the Microsoft network. It prompts you to log on to the domain when you boot up your machine.

If you try to establish a connection from a remote site without access to the domain (in other words, you are not on the internal network), you get an error message which indicates that "No Domain Controller could be found."

When you try to establish a VPN tunnel with the VPN Concentrator by dialing up through an ISP or using a DSL service, the connection does not prompt you to log on to a domain. Instead, you are able to continue with a secure link.

Map a drive (if you have not done so) to log on to the domain. Double-click on the mapped drive to get the password prompt so that you can log on to the network.

Check the networking properties on the machine to ensure that the PC has been configured with the correct domain name, and so on.

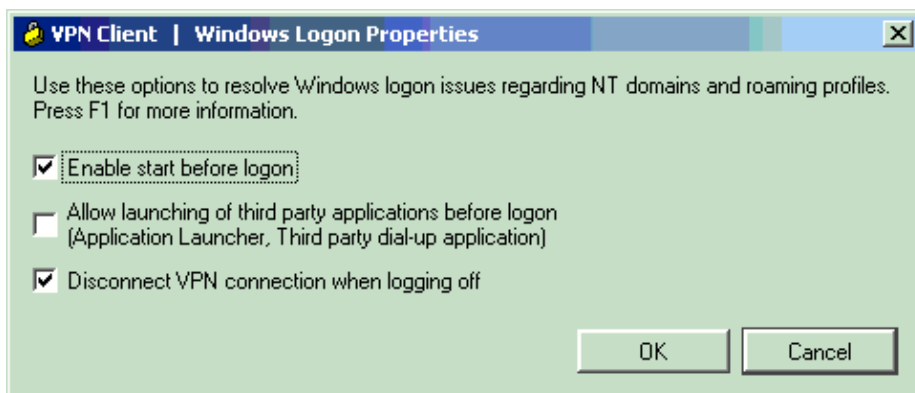
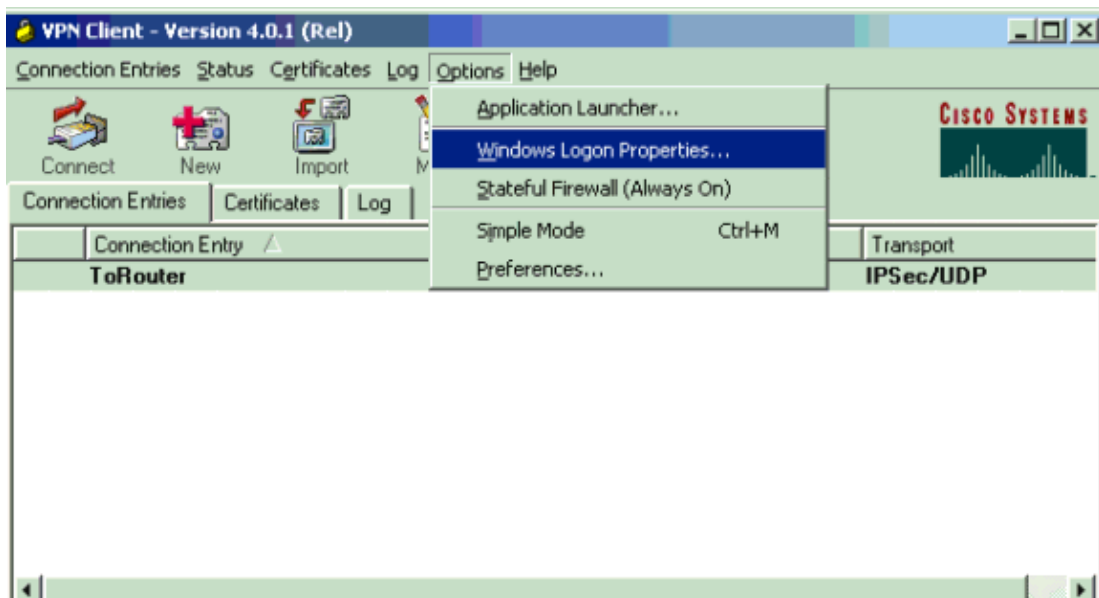
Note: The key is to log on to the NT domain successfully.

Note: If you want to run logon scripts through the NT machine, enable the Enable start before logon feature in the client.

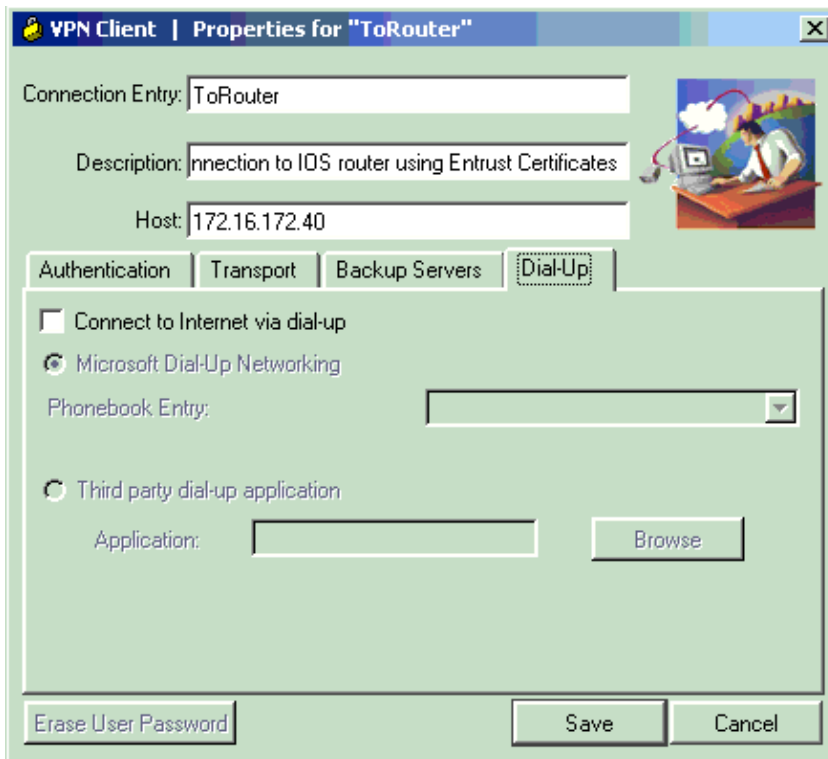
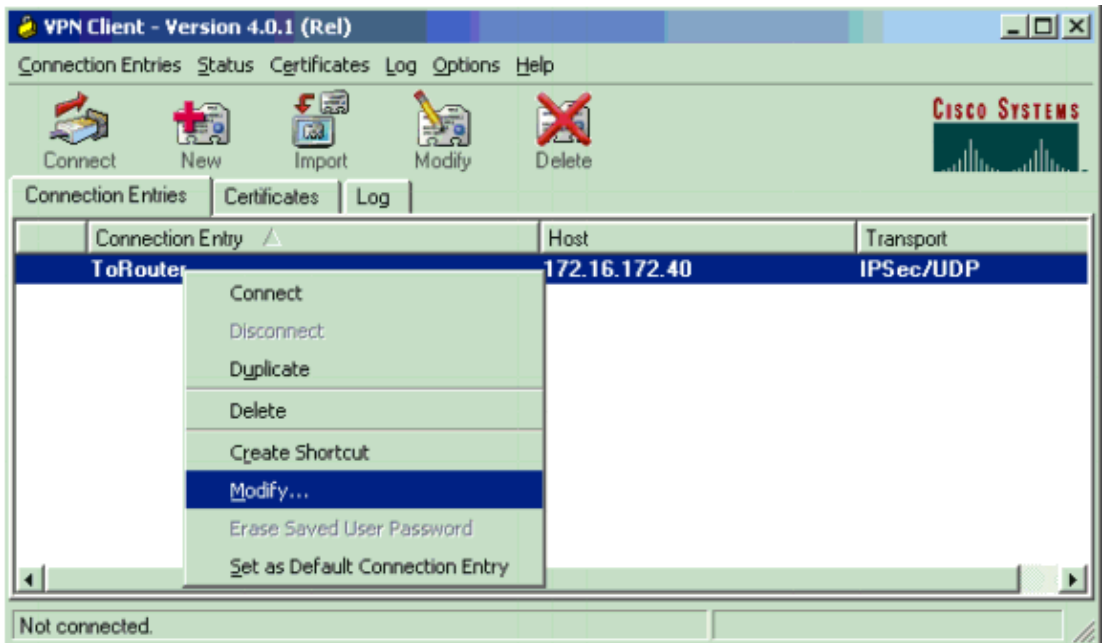
Using a Dial-Up Connection

Complete these steps to connect using a dial-up modem.

1. Create a Microsoft Dial-Up Networking (DUN) connection to your ISP.
2. Enable Client for Microsoft Networks and File and Print Sharing on your dial-up adapter. By default, these features are not enabled. However, they are required to run Microsoft services.
3. Select **Start > Programs > Cisco Systems VPN Client**. Select the **Options** menu. Select **Windows Logon Properties**, and ensure that **Enable start before logon** is selected. Click **OK**.



4. Right-click on the connection entry (or create one, if needed) and select **Modify**. Go to the Dial-up tab and select **Connect to the Internet via Dial-up**. Choose the DUN connection that you created in step 1 and click **Save**.



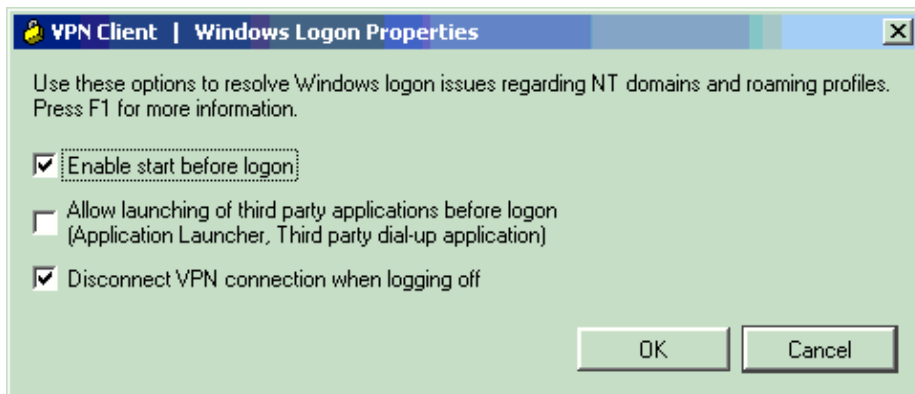
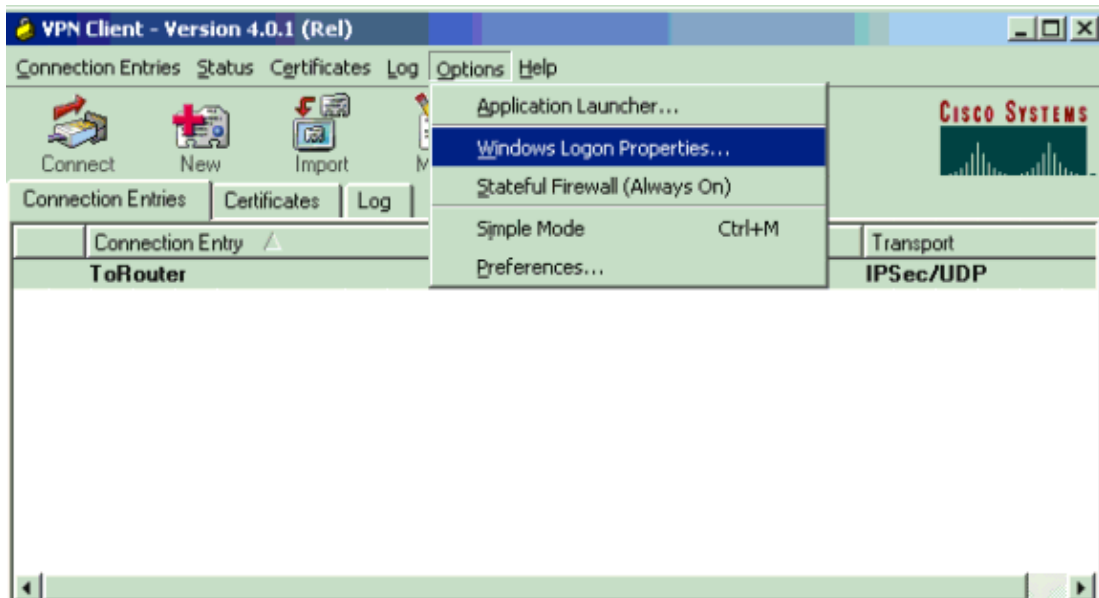
5. Log off the computer. It is not necessary to reboot.
6. Press **Ctrl–Alt–Delete**. Enter your DUN username and password to connect to the Internet and launch the VPN Client.
7. Click **Connect** to establish a connection with the VPN Client.
8. When prompted, enter your Microsoft username and password to log on to the domain.

Since you are connected remotely, you depend on the WINS or DNS to know where the domain controller is for the domain that you access . If you still have issues, there are problems with your WINS or DNS servers. Create an LMHOSTS file if you get a variation of the error that indicates "No Domain Controller Found."

Use an Ethernet or Broadband Connection

Complete these steps to connect using a high-speed broadband service.

1. Enable Client for Microsoft Networks and File and Print Sharing on your dial-up adapter. By default, these features are not enabled. However, they are required to run Microsoft services.
2. Select **Start > Programs > Cisco Systems VPN Client**. Select the **Options** menu. Select **Windows Logon Properties**, and ensure that **Enable start before logon** is selected. Click **OK**.



3. Log off the computer. It is not necessary to reboot.
4. Press **Ctrl-Alt-Delete** to launch the VPN Client.
5. Click **Connect** to establish a connection with the VPN Client.
6. When prompted, enter your Microsoft username and password to log on to the domain.

Since you are connected remotely, you depend on the WINS or DNS to know where the domain controller is for the domain that you access. If you still have issues, there can be problems with your WINS or DNS servers. Create an LMHOSTS file if you get a variation of the error that indicates "No Domain Controller Found."

Browse the Network Neighborhood

Note: Browsing Network Neighborhood is a function of the Microsoft browsing service, not with the Cisco VPN Client. Any problems are usually because the PC or master browsers do not function properly. Network Neighborhood is officially not supported. However, it works if configured correctly.

Browsing Network Neighborhood works by obtaining the browse list from either a master or backup browser. This list is obtained locally on your LAN by using NetBIOS Broadcasts to find and locate domain browsers.

Broadcasts do not go through an IPsec tunnel. Ensure that the VPN Client PC is set up properly and log on to the domain.

First make sure you have NetBIOS over TCP enabled on the adapter that you use to connect to the domain. Also ensure that the Client for Microsoft Networks is enabled. If you are able to map drives by IP address, then NetBIOS is passing through.

Log on to the domain.

When the computer logs in to the domain, the domain controller (which should be the domain master browser) redirects the browsing service to a master browser. The master browser then redirects to a backup browser. There it obtains the browse list.

If there is a problem with the domain controller initially, such as not being the domain master browser, then it never directs the client to the master browser. Troubleshoot your browsing services on the LAN using BROWSTAT.EXE, which you can obtain off of the NT4 Resource Kit (available from Microsoft).

Windows ME

A PC that runs Windows ME is similar to a machine that runs Windows 98. The PC does not log on to a Windows NT/2000 domain. Configure the workgroup name of your Windows ME PC to be the same as the Windows NT/2000 domain name so that the domain shares the NetBIOS information with the VPN Client.

Additional Troubleshooting Information

If you still have issues, try some of these additional suggestions:

- Lower the maximum transmission unit (MTU) size on the VPN Client.
 1. Select **Start > Programs > Cisco Systems VPN Client > Set MTU**.
 2. Set the MTU to 1400 bytes (or lower). Check that you can use NetBIOS names. This is also used to check for dropped packets.
- Select **Start > Run**. Type **ipconfig /all** to verify that the VPN Client receives the correct WINS and DNS information from the VPN Concentrator. Check the even log for the VPN Client.
- Verify that the PC that runs the VPN Client gets registered with the WINS and or DNS server through Dynamic Host Configuration Protocol (DHCP) correctly.
- Verify that there are no filtering devices between the VPN Client and the resources you try to access. Ensure that the needed ports for Microsoft networking are allowed to pass. By default, the VPN 3000 Concentrator does not block any of these necessary ports. Refer to Windows NT, Terminal Server, and Microsoft Exchange Services Use TCP/IP Ports for more details on Microsoft networking ports.

Related Information

- [Cisco VPN Client Support Page](#)
- [IPsec Support Page](#)
- [Testing the VPN Concentrator](#)
- [Cannot Log in to Windows NT Domain Over Internet Connection](#)
- [Cannot Browse Network Neighborhood or My Network Places Using a Dial-Up Connection](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 21, 2006

Document ID: 43066
