Avaya VPN Router Troubleshooting – Client

Avaya VPN Router
Release 8.01

Document Status: **Standard**

Document Number: **NN46110-700**

Document Version: **02.02**

Date: **May 2011**

AVAYA

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Preface

This guide provides information about how to manage and troubleshoot the Avaya VPN Client.

Before you begin

This guide is intended for network managers who monitor and maintain the Avaya VPN Router. This guide is based on the assumption that you have experience with system administration and that you are familiar with network management.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. Example: If the command syntax is **ping** <*ip_address*>, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names, options, or text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.

braces ({})	Indicates required elements in syntax descriptions where more than one option exists. You must choose only one option. Do not type the braces when you enter the command. Example: If the command syntax is **ldap-server source {external | internal}**, you must enter either **ldap-server source external** or **ldap-server source internal**, but not both.
brackets ([ ])	Indicates optional elements in syntax descriptions. Do not type the brackets when you enter the command. Example: If the command syntax is **show ntp [associations]**, you can enter either **show ntp** or **show ntp associations**. Example: If the command syntax is **default rsvp** [**token-bucket** {**depth** | **rate**}], you can enter **default rsvp**, **default rsvp token-bucket depth**, or **default rsvp token-bucket rate**.
ellipsis (. . .)	Indicates that you repeat the last element of the command as needed. Example: If the command syntax is **more disk***n***:***<directory>***/...***<file_name>***, you enter **more** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, an underscore connects the words. Example: If the command syntax is **ping** *<ip_address>*, *ip_address* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`

comma (,)	Shows menu paths. Example: Choose **Status**, **Health Check**.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. Example: If the command syntax is **`terminal paging {off | on}`**, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both.

Related publications

For more information about the Avaya VPN Router, see the following publications:

- Release notes provide the most recent information, including brief descriptions of new features, problems fixed in this release, and known problems and workarounds.
- *Avaya VPN Router Configuration—Client* (NN46110-306) provides information to install and configure client software for the VPN Router.
- *Avaya VPN Router Configuration—TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Avaya VPN Router Upgrades—Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Avaya VPN Router Installation and Upgrade—Client Software Release 8.01* (NN46110-409) provides information to upgrade the Avaya VPN Client to the most recent release.
- *Avaya VPN Router Configuration—Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Avaya VPN Router Configuration—SSL VPN Services* (NN46110-501) provides instructions to configure services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Avaya VPN Router Configuration—Advanced Features* (NN46110-502) provides configuration information for advanced features, such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *Avaya VPN Router Configuration—Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Avaya VPN Router Configuration—Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), Multirouting policy services, and client address redistribution (CAR).
- *Avaya VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).

- *Avaya VPN Router Configuration—Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and VPN Router interface and tunnel filters.
- *Avaya VPN Router Security—Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Avaya VPN Router Troubleshooting—Server* (NN46110-602) provides information about system administrator tasks, such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Avaya VPN Router Administration* (NN46110-603) provides information about system administrator tasks, such as backups, file management, serial connections, initial passwords, and general network management functions.

New in this release

The following sections detail what's new in *Avaya VPN Router Troubleshooting—Client* (NN46110-700) for Release 8.01:

Features

See the following section for information about feature changes:

Two factor authentication

Release 8.01 supports two factor authentication. For more information about troubleshooting, see "Diagnosing client connectivity problems" on page 29.

Other changes

See the following section for information about changes that are not feature-related:

Moved content

The following topics are moved from *Avaya VPN Router Troubleshooting—Server* (NN46110-602):

Troubleshooting fundamentals

As a network administrator, your primary concern is to maintain connectivity within the network. For extranet access, you must maintain secure connections between remote users and the private intranet that the Avaya VPN Router services. Performance is another area of concern. You must also monitor performance to address issues before they become problems.

This chapter provides basic information to assist in troubleshooting. This chapter includes the following topics:

Connectivity problems

Connectivity problems occur when the remote user cannot establish a connection to areas of the private corporate network. Several points of failure when you diagnose connectivity problems. Problems can arise from simple connectivity issues on the remote user local network, Internet routing problems, or the VPN Router configuration.

Remote access problems typically originate at the client end when the remote user cannot establish a connection, loses a connection, or has difficulty browsing the network. When connectivity problems occur and the source of the problem is unknown, Avaya recommends that you follow the Open Systems Interconnect (OSI) network architecture layers. Diagnose the physical layers, such as the modem and the cables, before you move up to the network and application layers. To diagnose the network and application layers, you can ping a host and verify that the remote user can browse the Web.

For more information about troubleshooting connectivity issues, see "Diagnosing client connectivity problems" on page 29.

Performance problems

As with connectivity, there are many places in the VPN network where network performance is affected. To avoid problems and enhance the productivity of the extranet, you can regularly check network statistics, logs, and health check information, and inform users of good network practices.

Client logging

Prior to the introduction of logging on the Avaya VPN Client, Avaya VPN Router supported only the Contivity Secure IP Services Gateway logging functionality to debug user tunnels. Now you can use both client and server logs to locate and solve connectivity problems. You can enable the logging feature specifically on the client to log all information. The logging feature generates log files for you to use when you need to recover a failed tunnel connection.

When you enable Avaya VPN Client logging or if the connection establishment fails, log entries populate the log file. The parameters needed to make a connection are also logged in the log file.

Note: The log file does not include passwords, certificates, or other security-sensitive information.

The in-memory buffer keeps logging information until the software requests to flush the information into the file on a disk. This saves the performance on the remote workstation.

The log entries appear in the following format:

```
[Date:Time]: Facility: Severity: Message
```

The log entry parameters are as follows:

- Date and Time derive from the current client system time.
- Facility indicates from what area of code the message generates. For example, ISAKMP.
- Severity is defined by the following code:
  - F—Fatal: Critical error, execution halted
  - E—Error: Minor error, execution continues but some functionality may be crippled
  - W—Warning: Outcome of operation may cause problems
  - I—Informational: Messages to show progress, and status
  - S—Success: Operation completed successfully
- Message shows a user-friendly message to help you debug.

After the system generates the log file, it saves the log file in the C:\Program Files\Avaya\log folder or C:\Program Files\Avaya\log.

The log file has the following naming convention:

```
<Profile name>.log
```

Each time a new log generates, the old log is renamed using the following naming convention:

```
<Profile name>_xxx.log
```

where xxx is the number of the log. For example: ces_4.log or office_5.log. Only five old logs are kept at a time; the older logs are removed to manage the remote workstation disk space.

Troubleshooting tools

This chapter contains information about the following Avaya VPN Client-specific troubleshooting tools:

IPsec VPN Client Monitor

IP security (IPsec) VPN Client Monitor provides network statistics on device, connection, and network errors to help monitor traffic flow and assess IPsec connection performance. Statistic counters update once every second. For more information about the IPsec VPN Client Monitor, see the Avaya VPN Client online Help.

Microsoft PPTP Dial-Up Networking Monitor

Microsoft Point-to-Point Tunneling Protocol (PPTP) Dial-Up Networking Monitor provides network statistics on device, connection, and network protocols that help monitor traffic flow and assess PPTP connection performance. For more information about the PPTP Dial-Up Networking Monitor, see the PPTP help or your Microsoft PPTP client documentation.

Client logging configuration

This chapter contains procedures about Avaya VPN Client logging. Use this information to configure logging on the Avaya VPN client.

This chapter includes the following topics:

Enabling logging on the Avaya VPN Client

To enable logging, perform the following steps:

1. Launch the Contivity VPN Client.
2. Select the **Options** tab in the top menu bar.

   The menu appears.
3. Select **Log Session to File**.

   A check mark appears next to Log Session to File to indicate that logging is enabled.

Disabling logging on the Avaya VPN Client

To disable logging, perform the following steps:

1. Launch the Contivity VPN Client.
2. Select the **Options** tab in the top menu bar.

   The menu appears.
3. Clear the **Log Session to File** check box.

Configuring the IPsec user tunnel on Avaya VPN Router

To configure an IPsec user tunnel between the client and the Avaya VPN Client, perform the following steps:

1. Access the Avaya VPN Router.
2. Go to the **Profiles**, **Users**.

   The User Management window appears.
3. From the **Group** list, select the group to which you want to assign the user.
4. Click **Add User**.

   The User Management > Add User window appears.
5. In the **First** box for **Name**, enter the first name of the user.
6. In the **Last** box for **Name**, enter the last name of the user
7. In the **User Id** box for **IPsec**, enter the User ID (IPsec) for the IPsec account.
8. In the **Password** box for **IPsec,** enter a password.
9. In the **Confirm Password** box for **IPsec**, reenter the password.
10. Click **OK**.

    The Remote User Address Pool window appears. You can configure the address pool to issue the address to the client.
11. Go to the **Servers**, **User IP Addr** window.
12. Click **Add** under the **Address Pool** section.

    The Remote User IP Address Pool window appears.
13. In the **Starting IP Address** box, enter the first IP address of the remote user IP address pool.

14 In the **Ending IP Address** box, enter the last IP address in the remote user IP address pool.

15 In the **Subnet Mask** field, enter the subnet mask for the remote user IP address pool.

Note: To save configuration time, leave the Default Pool choice selected as this is the default pool for address assignments. Ensure that you select the Default Pool as the Address Pool Name on the Groups > Edit > Connectivity screen; the Default Pool is selected by default.

16 Click **OK**.

Configuring the Avaya VPN Client for logging

To configure the Avaya VPN Client for logging, perform the following steps:

1 Launch the Avaya VPN Client.

2 From the **Connection** list, select **To CES**.

3 In the **User Name** box, enter **`IPsec`**.

4 In the **Destination** box, enter the IP address of the Avaya VPN Router.

5 Click **Save**.

6 Select **Options, Log Session to File**.

Testing the configuration

To test the configuration, perform the following steps:

1 Launch the Avaya VPN Client.

2 In the **Password** box, enter the password.

3 Click **Connect**.

The Client connects to the Avaya VPN Router and checks for banner text.

4 Open a command prompt window.

5 Enter **ipconfig** to check the routing table.

C:\>**ipconfig**

```
Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :

   IP Address. . . . . . . . . . . . : 192.168.100.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter {6A226141-155B-4306-ADD2-0658D76B57B8}:
Connection-specific DNS Suffix . :

   IP Address. . . . . . . . . . . . : 192.168.10.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.150
```

6 Enter the ping command to ping the Avaya VPN Router to test the connection. For example, enter **ping 192.168.10.1**.

C:\>**ping 192.168.10.1**

```
Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<10ms TTL=64
Reply from 192.168.10.1: bytes=32 time<10ms TTL=64
Reply from 192.168.10.1: bytes=32 time<10ms TTL=64
Reply from 192.168.10.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.10.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7 From the **Start** menu, choose **Disconnect VPN** to disconnect the Avaya VPN Router.

8 Click **Yes** to confirm you want to disconnect the VPN connection.

9 Open the client log file and view the entries.

The log is saved in the installation directory.

```
Mon Nov 03 11:01:53 2003 | Isakmpd | I | Connection initiated to
192.168.100.1 [192.168.100.1] using Diffie-Hellman group 1.
Mon Nov 03 11:01:54 2003 | ConfMode | I | IP Address
192.168.10.150.
Mon Nov 03 11:01:54 2003 | ConfMode | I | Keepalive interval set to
60 seconds.
Mon Nov 03 11:01:54 2003 | ConfMode | I | Maximum keepalive
retransmissions set to 3 retries.
Mon Nov 03 11:01:54 2003 | ConfMode | I | Mandatory tunneling
enforced.
Mon Nov 03 11:01:54 2003 | ConfMode | I | Saving Password on client
is turned Off.
Mon Nov 03 11:01:54 2003 | ConfMode | I | Current time on switch is
11/03/03 11:01:21 GMT.
Mon Nov 03 11:01:58 2003 | Failover | W | Failover list set to none.
Mon Nov 03 11:01:59 2003 | DYNDNS | I | Fully qualified domain name
for this host (FQDN): KRISTISE-1.
Mon Nov 03 11:01:59 2003 | DYNDNS | I | Assigned IP address (from
CES) 192.168.10.150
Mon Nov 03 11:01:59 2003 | DYNDNS | I | Reverse lookup IP address is
150.10.168.192.in-addr.arpa
Mon Nov 03 11:01:59 2003 | Isakmpd | I | Dynamic DNS Registration
completed successful
Mon Nov 03 11:08:01 2003 | Isakmpd | I | VPN connection
disconnected by user.
Mon Nov 03 11:08:01 2003 | DYNDNS | I | Fully qualified domain name
for this host (FQDN): KRISTISE-1.
Mon Nov 03 11:08:01 2003 | DYNDNS | I | Assigned IP address (from
CES) 192.168.10.150
```

10 Disconnect the Ethernet cable.

11 Launch the Avaya VPN Client.

12 In the **Password** box, enter the password.

13 Click **Connect**.

The tunnel is not established and the “Login Failure due to: Remote host not responding” error appears.

14 Open the client log file and view the entries.

The old log is renamed To_CES_1.log and the new log entries write into the To_CES.log file.

```
Mon Nov 03 11:22:25 2003 | Isakmp | I | Logging subsystem
initialized.
Mon Nov 03 11:22:29 2003 | Isakmpd | I | Connection initiated to
192.168.100.1 [192.168.100.1] using Diffie-Hellman group 2.
Mon Nov 03 11:23:40 2003 | Isakmpd | F | Login Failure due to:
Remote host not responding
```

15 Reconnect the Ethernet cable.

16 Launch the Avaya VPN Client.

17 In the **Password** box, enter the wrong password (for example, test1 instead of test).

18 Click **Connect**.

Note the Authentication failure error message.

19 Check the new log entries in the To_CES.log file.

```
Mon Nov 03 11:30:16 2003 | Isakmpd | I | Connection initiated to
192.168.100.1 [192.168.100.1] using Diffie-Hellman group 2.
Mon Nov 03 11:30:16 2003 | Isakmpd | E | Unable to complete
encryption handshake with remote side. Encryption Mismatch.
Mon Nov 03 11:30:16 2003 | Isakmpd | I | Connection initiated to
192.168.100.1 [192.168.100.1] using Diffie-Hellman group 1.
Mon Nov 03 11:31:07 2003 | Isakmpd | F | Login Failure due to:
Authentication failure
```

20 To disable logging on the client, from the **Options** menu, choose **Log Session to File**.

21 Enter the wrong password (for example, test1 instead of test) in the **Password** box.

22 Click **Connect**.

23 Check the new log entries in the To_CES.log file.

```
Mon Nov 03 11:39:04 2003 | Isakmpd | I | Connection initiated to
192.168.100.1 [192.168.100.1] using Diffie-Hellman group 2.
Mon Nov 03 11:39:04 2003 | Isakmpd | E | Unable to complete
encryption handshake with remote side. Encryption Mismatch.
Mon Nov 03 11:39:04 2003 | Isakmpd | I | Connection initiated to
192.168.100.1 [192.168.100.1] using Diffie-Hellman group 1.
Mon Nov 03 11:39:05 2003 | Isakmpd | F | Login Failure due to:
Authentication failure
```

24 Enter the correct password in the **Password** box.

25 Click **Connect**.

26 After you connect, disconnect the client.

27 Check the log again.

Note that no new entries were added to the log file as the logging was disabled and the tunnel was established successfully.

Troubleshooting

This chapter introduces the concepts and practices of advanced network configuration and troubleshooting for the Avaya VPN Client. Use this chapter when you diagnose client problems. This chapter includes the following topics:

Diagnosing client connectivity problems

A connection can fail at varying points in an extranet. If a remote user cannot access the corporate network and the source of the problem is unknown, Avaya recommends that you guide the remote user through the following steps to determine the source of the problem:

1. Access www.avaya.com —or another site—in the Web browser.

   If you can access the Web site, the PPP dial-up connection is working properly.

2. Verify that there is a Point-to-Point Protocol (PPP) dial-up connection over the internet.

   See "Common client connectivity problems" to troubleshoot the connection problem.

3. Check that the modem type and settings are configured properly by performing the following steps:

   a. Right-click the **Dial-Up Networking** connection icon on the desktop to view the properties.

   b. Verify that the settings are correct for the modem configuration.

4. If you can connect but you cannot access resources or servers, check the system connection information by performing the following steps:
   a. From the **Start** menu, choose **Run**.
   b. In the text box, type **`winipcfg`** (or **`ipconfig`** if you use Windows NT).
   c. View the statistics for the Peer-to-Peer Protocol (PPP) adapter.
   d. Confirm that the entries match the statistics provided by the Internet Service Provider (ISP).
5. If you still cannot view resources or servers over the PPP dial-up connection, contact the ISP to verify if connection attempts were logged from the remote workstation.
   The ISP can provide additional troubleshooting assistance.
6. If you connect to the router using two-factor authentication, ensure that the certificate exists and that you configure the preshared key.

Common client connectivity problems

This section contains information about common client connectivity problems.

Extranet connection problems

If the Avaya VPN Client is successfully connected to the Internet, but cannot access the intranet over the Point-to-Point Tunneling Protocol (PPTP) or IP Security (IPsec) VPN Client connection, ask the remote user to identify the error message to further troubleshoot the connection problem.

The following table provides the messages and the associated cause and action statements that the remote client receives at the IPsec VPN Client user at the remote workstation. This information is also available in the VPN Client online Help.

Table 1 Common client connectivity problems

Message	Cause	Action
Remote host not responding	This message indicates that the Avaya VPN Router did not respond to the IPsec connection attempt or that User Datagram Protocol (UDP) port 500 is blocked. The VPN Router accepts only a certain number of PING packets from another Internet host before requiring a tunnel connection.	1. Ping the host name or IP address that you provided in the Destination field. To ping a host called extranet.corp.com, for example, open an MS-DOS command prompt and type **`ping extranet.corp.com`**. If you receive a reply message, the VPN Router is accessible but not responding. If you receive a "Request Timed Out" message from the ping command, the VPN Router is inaccessible. 2. Use the MS-DOS Trace Route command (tracert.exe) on Windows systems to further diagnose the connection problem.
Maximum number of sessions reached	This message indicates that the maximum number of users for the account has been reached. If you are the only user with access to your account, this error message appears when you restart an IPsec connection immediately after losing the dial-up connection to the ISP. The VPN Router takes up to one minute to determine that a connection is dropped and then logs you off your account.	Wait one minute and retry the connection.
Login not allowed at this time	This message indicates that your account is limited to specific hours of access and that you tried to connect outside of the allowed time.	Contact your network administrator to verify the specific hours of access.

Table 1 Common client connectivity problems

Message	Cause	Action
Authentication failed	This message indicates that the IPsec user name is incorrect or the password is invalid for the user name entered.	1. Verify that the user name you entered is correct. 2. Retype the password before trying the connection again.
No proposal chosen	This message indicates that the VPN Router is not configured to handle the authentication method configured under the current connection profile.	Use the correct IPsec parameters, such as a choice of Encapsulating Security Payload (ESP)-3DES with SHA1. Make sure the parameters match the parameters of the client (for example, an International client).
Other IPsec errors	This message indicates that an error in configuration exists on the VPN Router that only the network administrator can correct.	Contact the Network Administrator with the specific error message.
The physical connection has been lost	This message indicates that the PPP connection to your ISP is disconnected.	1. Reestablish the PPP dial-up connection to the ISP. 2. Reestablish the extranet connection to the remote network.

Table 1 Common client connectivity problems

Message	Cause	Action
The secure extranet connection has been lost	This message indicates that the VPN Router you are connected to has either logged your connection off or is no longer responding. This message applies to IPsec only, The connection is probably lost due to the Idle Timeout configured on the VPN Router. If no data is transferred through the extranet connection for a long period of time, normally 15 minutes or more, the VPN Router automatically disconnects the connection.	1. Click **Connect** to reestablish the extranet connection. If you cannot to reestablish the extranet connection, the dial-up connection prevents data from traveling between the Avaya VPN Client and the VPN Router. 2. Stop the dial-up connection and reconnect before you try to reestablish a connection. If you are still unable to connect to the VPN Router, perform the following steps: 1. Open an MS-DOS Command Prompt. 2. Ping the VPN Router using the host name or address that you specified in the Destination field. If you receive a "Destination Unreachable" error message, a routing problem exists at the ISP. If you receive a "Request Timed Out" error message, the VPN Router is probably not available and you can contact your network administrator.
Auto disconnect closes the dial-up connection during data transfer activity	This message indicates that the Microsoft Auto Disconnect feature does not recognize data activity because it did not pass through Internet Explorer. Microsoft has documented this as a known problem in Windows 95. This error occurs on Windows 95 platforms only.	At the remote workstation, disable Auto Disconnect if you do not use Internet Explorer to access data on the remote network: 1. Open the **Control Panel**. 2. Double-click the **Internet** icon. 3. Click the `Connection property` tab. 4. Clear the **Disconnect if idle for** check box.

Banner message problems

This section contains troubleshooting information about banner text messages that stop responding when you launch the Avaya VPN Client.

In some situations, when you attempt to start a user tunnel from the Avaya VPN Client to Avaya VPN Routers, the tunnel stops responding at the “Checking for banner text” message. To troubleshoot a nonresponsive banner message problem, verify the components identified in the following sections.

Firewall blockage

A common reason for the banner message to stop responding is a firewall or router, placed somewhere along the path from the remote computer to the gateway, which blocks ESP or Authentication Header (AH) traffic. The firewall can be a personal firewall installed on the remote computer, a firewall or router at the Internet Service Provider (ISP), or a corporate firewall. In this situation, IPsec Internet Security and Key Management Protocol (ISAKMP) traffic that negotiates the tunnel establishment goes through the tunnel, but the ESP- or AH-encapsulated traffic inside the tunnel does not get through. When the banner text is retrieved through the established tunnel, the banner message or other traffic secured by the ESP or AH never reaches the client and the Avaya VPN Client continues to wait for a response from the gateway until a timeout period is reached.

To resolve this issue, ensure the following traffic is allowed to pass through the firewalls along the path:

- UDP protocol (17) port 500, both inbound and outbound
- ESP protocol (50), both inbound and outbound
- AH protocol (51), both inbound and outbound

Note: It is not necessary to specify source and destination ports for ESP or AH protocols, but if a particular firewall implementation requires it, use zero or N/A as ports dependent on firewall or other requirements.

Resolving NAT-T blockage

The same scenario occurs as in the previous section if Network Address Translation Transversal (NAT-T) is configured and the firewall blocks the UDP port selected for NAT-T along the path.

To resolve this issue, ensure the port specified in the NAT-T section of the Services IPsec screen can pass through the firewalls on a personal, corporate, or ISP level.

1. Access the Avaya VPN Router.
2. From the **Services** menu, choose **IPsec**.
3. Scroll down the page to the **NAT Transversal** section.
4. Verify that the port specified in the **UDP Port** box can pass through the personal, corporate, or ISP firewalls.

NAT blockage

Verify the NAT configurations at the remote Avaya VPN Client implementation to see if it prevents IPsec traffic from going through. Verify that NAT is configured appropriately and IPsec (ISAKMP, ESP, AH) or UDP (if NAT Traversal is used) traffic can pass through the particular NAT implementation.

Avaya VPN Client version

Ensure the most recent version of the Avaya VPN Client is used. If you have a support contract, you can download the upgrade from the Avaya Technical Support Web site: www.avaya.com/support

Third-party VPN client software

Ensure no third-party VPN client software is running at the same time as the Avaya VPN Client.

If third-party VPN client software runs at the same time as the Avaya VPN Client, it can interfere with Avaya Client operation. In this case, disable or uninstall third-party VPN clients because they can run in the background preventing successful Avaya VPN Client operation. Open the Interface Properties window and clear third-party adapters or drivers.