Avaya VPN Client – Troubleshooting

VPN Client Software
Release 10.05

Document Status: **Standard**

Document Number: **NN46110-701**

Document Version: **02.03**

Date: **May 2011**

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

Copyright

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

Preface

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

Before you begin

This guide is for network managers who monitor and maintain the Avaya VPN Router. This guide assumes 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 (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is
ping *<ip_address>*, you enter
ping 192.32.10.12

bold Courier text

Indicates command names and options and text that you need to enter.

Example: Use the **show health** command.

Example: Enter **terminal paging** {**off** | **on**}.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering 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 ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering 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 points (. . .)

Indicate 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, the words are connected by an underscore.

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.`

separator (,)

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 entering 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 Nortel VPN Router, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Avaya VPN Client — Configuration* (NN46110-509) provides information to install and configure client software for the VPN Router.
- *Nortel VPN Router Configuration — TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Avaya VPN Router Upgrades — Server Software Release 8.01* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Avaya VPN Client — Installation and Upgrades* (NN46110-412) provides information to install and upgrade the Avaya VPN Client to the most recent release.
- *Nortel VPN Router Configuration — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration .
- *Nortel 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.
- *Nortel 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) .
- *Nortel VPN Router Configuration — Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shorest Path First (OSPF), Virtual Router Redunancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).

- *Nortel 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).
- *Nortel VPN Router Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and VPN Router interface and tunnel filters.
- *Nortel VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Nortel 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.

Printed technical manuals

To print selected technical manuals and release notes for free, directly from the Internet, go to www.avaya.com/support, find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. For more information about a free copy of the Adobe Reader, go to the Adobe Systems Web site at www.adobe.com .

Customer service

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

Navigation

- “Getting technical documentation” on page 10

- “Getting product training” on page 10
- “Getting help from a distributor or reseller” on page 10
- “Getting technical support from the Avaya Web site” on page 10

Getting technical documentation

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

New in this release

The following sections detail what’s new in *Avaya VPN Router Troubleshooting — Client* (NN46110-701) for Release 10.05:

- “Client for Windows Vista” on page 11
- “Other changes” on page 11

Features

Client for Windows Vista

The Avaya VPN Client for release 10.05 is a completely new Avaya VPN Client for the Microsoft Windows Vista operating system. Release 10.05 runs only on the Windows Vista operating system.

“Client logging configuration” on page 17

Other changes

Moved content

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

- “Diagnosing client connectivity problems” on page 27
- “Common client connectivity problems” on page 28

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 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" on page 13
- "Performance problems" on page 14
- "Client logging" on page 14

Connectivity problems

Connectivity problems occur when the remote user cannot establish a connection to areas of the private corporate network. There are several points of failure to consider when you diagnose connectivity problems. Problems can range from asimple modem configuration error on the client workstation to a complex High-Level Data Link Control (HDLC) protocol error on the T1 Wide Area Network (WAN) interface.

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 you follow the Open Systems Interconnect (OSI) network architecture layers. Therefore, 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 27.

Performance problems

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

Client logging

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 the AVC 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.

The log file does not include passwords, certificates and other security-sensitive information.

Client logging does not save to files on the hard drive automatically, but you can manually export the logs.

Troubleshooting tools

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

Avaya VPN Client Status monitor

The Avaya VPN Client Status monitor provides network statistics on device, connection, and network errors that help monitor traffic flow and assess IPsec and SSL connection performance. Statistic counters are updated once a second. For more information on the Avaya VPN Client Status 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 on 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 (AVC) logging. Use this information to configure logging on the AVC.

This chapter includes the following topics:

Enabling logging on the AVC

To enable logging, perform the following steps:

1. Choose **Start, All programs, Avaya, Avaya VPN Client, Avaya VPN Client**. The Avaya VPN Client window appears.
2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3. From the left pane, click **Manage Options.** The Manage Options window appears. Click **Logging Level**, and then choose a level to view when using the **Log Viewer.** The logging level is grayed out when the AVC is not running in administration context.

Use the information in Table 1 “Logging levels” on page 18 when choosing a logging level .

Table 1 Logging levels

Logging level	Description
Debug	Shows detailed information to help you to debug a problem. Also logs positive events that mark successful milestones.
Information	Shows general type (high level) of information. Logs important and successful milestones of application execution, regardless of whether the application is working properly or not.
Warning	Shows a possible problem has occurred or can occur, but the application still functions correctly. However, it cannot continue to work properly.
Error	Shows that unexpected processing has happened. The application cannot perform a task as expected. However, the application is still up and running.
Fatal	Shows unhandled exceptions where the application has stopped working.
Disabled	The logging level is disabled. No logs are generated.

4 Click **Apply** to save the option.

Disabling logging on the AVC

To disable the logging, perform the following steps:

1 Choose **Start, All programs, Avaya, Avaya VPN Client, Avaya VPN Client**. The Avaya VPN Client window appears.

2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

3 From the left pane, click **Manage Options.** The Manage Options window appears. Deselect **Logging Level.**

4 Click **Apply** to save the option.

Creating an IPSec profile using Manage Profiles

Whenever you need a standard VPN tunnel, use the IPSec tunnel type. You must be in administrator mode to enable Global Profile.

Create an IPSec profile, by performing the following procedure:

1 Choose **Start, All programs, Avaya, Avaya VPN Client, Avaya VPN Client**.

The Avaya VPN Clien**t** window appears.

2 From the left pane, click **Edit the Profile**.

The Manage Profiles window appears showing the General tab.

3 Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.

4 From the **General** tab, choose **IPSec Tunnel** as a connection type for this profile from the **Tunnel Type** list.

5 Type in a profile name into the **Profile** box. You can optionally enter a description of the profile.

6 Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.

7 Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.

8 Type an IP address or DNS for the VPN into the **Destination** box.

9 Select one of the following Authentication types:

- **Username and Password**
- **Certificate Authentication**
- **Group Security Authentication**

10 If you choose **Username and Password** perform the following:

a By default **Username and Password** is already selected. Type the username assigned to you by the network administrator into the **Username** box.

b Type the password assigned to you by the network administrator into the **Password** box.

c Click **Save Password** to save the password.

11 If you choose **Certificate Authentication** perform the following:

a Click **Certificate Authentication** to enable the certificate selection.

b Click **Select**. The Select a certificate window appears. Choose either step c or step d.

c If you want to allow the AVC to select a certificate, click **Automatically select a valid certificate**.

d If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.

e Click **OK** to close the window.

f If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.

g Click **Save** to save the new profile.

12 If you choose **Group Security Authentication** perform the following:

a Click **Group Security Authentication** to enable the group security authentication.

b Select a group authentication type from the list.

— **Radius Authentication**

— **Challenge Response Token**

— **Response Only Hardware Token**

— **Response Only Software Token**

The fields in Authentication Information area change according to the type selected. When choosing an authentication type, see Table 2 “IPSec authentication information requirements” on page 21 for the required authentication information.

Table 2 IPSec authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (nonmodifiable)
Radius Authentication	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **Save Password**: click to save the password. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator.
Challenge Response Token	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **Save Password**: click to save the password. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator.

Table 2 IPSec authentication information requirements

Authentication type	**Authentication information**
Response Only Hardware Token	**Username**: type the username supplied by your administrator. **PIN**: type the PIN supplied by your administrator. **Save PIN**: click to save the PIN. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator. **Use Passcode**: click to enable a passcode.
Response Only Software Token	**Username**: type the username supplied by your administrator. **PIN**: type the PIN supplied by your administrator. **Save PIN**: click to save the PIN. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator.

The AVC does not share the group password between local computer accounts. If you log on to the local computer by using a different user account than the one you use to create the AVC profile, you must reenter the group password. For example, you log on to the local computer as the administrator, create the client profile, and log off. If you then log on to the local computer with a different user account, you must reenter the group password in the client profile. You must reenter the password regardless of how you install the Avaya VPN.

13 Click **Save** to save the configuration.

Creating a SSL profile using Manage Profiles

Create a Secure Sockets Layer (SSL) VPN when you are managing the security of message transmissions. The SSL profile also includes the Predefined Login Service that automatically logs on the profile to the server. You must be in administrator mode to enable Global Profile.

Create a SSL profile, by performing the following procedure:

1. Choose **Start, All programs, Avaya, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3. Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.
4. From the **General** tab, choose **SSL Tunnel** from the **Tunnel Type** list as a connection type for this profile.
5. Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.
6. Click the **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.
7. Type an IP address or DNS for the VPN into the **Destination** box.
8. Type in the port number assigned to you by your Administrator into the **Port** box.
9. Click **Certificate Authentication** to enable the certificate selection.
10. Click **Select**. The Select a certificate window appears. Choose either step a or step b.

    a. If you want to allow the AVC to select a certificate, click **Automatically select a valid certificate**.

    b. If you want to manually select a certificate, click **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.

11 Click **OK** to close the window.

12 If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.

13 Click **Predefined Login Service** to enable Predefined Login Service configuration.

14 Choose a name for the service from the **Login Service Name** list. See Table 3 for authentication information.

15 Type the username into the **Username** box.

16 Click **Response Only Software Token** if you want to enable this token. Type the PIN number into the **PIN** box.

17 Click **Save** to save the configuration.

The fields you select in the Predefined Login Service depend upon the type of Login service that you are using. When choosing an authentication type, see Table 3 "SSL authentication information requirements" on page 24 for the required authentication information.

Table 3 SSL authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (nonmodifiable)
Login service (second password is not required)	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **PIN**: if you are using a Response Only Software token, type the PIN supplied by your administrator.
Login service (second password is required)	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **PIN**: if you are using a Response Only Software token, type the PIN supplied by your administrator. **Second Password**: type the password supplied by your administrator.

Testing the configuration

To test the configuration, perform the following steps:

1. Launch the Avaya VPN Client (AVC).
2. Enter the password in the **Password** box.
3. Click **Connect**. The AVC 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.
6. Enter the ping command to ping the Avaya VPN Router to test the connection.
7. Choose **Start**, Disconnect VPN to disconnect the Avaya VPN Router.
8. Click **Yes** to confirm you want to disconnect the VPN connection.
9. Open the AVC log information window and view the entries.
10. Disconnect the Ethernet cable.
11. Launch the AVC.
12. Enter the password in the **Password** box.
13. Click **Connect**.
14. The tunnel is not established and the “Login Failure due to: Remote host not responding” error appears.
15. Open the AVC log information window and view the entries.
16. Reconnect the Ethernet cable.
17. Launch the AVC.
18. Enter the wrong password (for example, test1 instead of test) in the **Password** box.
19. Click **Connect**. Note the Authentication failure error message.
20. Check the new log entries in the **Log Viewer**.
21. From the left pane, click **Manage Options**. The Manage Options window appears. Deselect **Logging Level**.

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

23 Click **Connect**.

24 Check the new log entries in the **Log Viewer**.

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

26 Click **Connect**.

27 Once connected, disconnect the client.
Check the log again. Note that no new entries have been 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 Nortel VPN Router. 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 LAN connection is working properly.

2. Verify that the LAN connection on the local PC is active.

   See "Common client connectivity problems" on page 28 to troubleshoot the connection problem.

3. Check that the ethernet settings are configured properly by performing the following steps:

   a Click **Start**, **Settings**, **Network Connections** to view the properties.

- b Verify that the settings are correct for the ethernet connection.

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 `ipconfig` .
- c View the statistics for the LAN 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 LAN 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.

If the Avaya VPN Client (AVC) is successfully connected to the ISP, but cannot access the intranet over the PPTP, SSL or IPsec AVC connection, ask the remote user to identify the error message to further troubleshoot the connection problem.

Table 4 “Common client connectivity problems” on page 29 shows the associated cause and action statements that the remote client recieves at the IPsec VPN Client user at the remote workstation.

Table 4 Common client connectivity problems

Message	Cause	Action
Remote host not responding	Avaya VPN Router did not respond to the SSL or IPsec connection attempt or that User Datagram Protocol (UDP) port 500 is blocked. The VPN Router allows only a certain number of PING packets from another Internet host before requiring a tunnel connection to be established.	1. Ping the host name or IP address that you filled 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 Avaya VPN Router is accessible but is not responding. If you receive a message that says Request Timed Out from the ping command, the Avaya 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 Avaya 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 you tried to connect outside of the allowed time.	Contact your network administrator the verify the specific hours of access.
Authentication failed	This message indicates that the SSL or 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.

Table 4 Common client connectivity problems

Message	Cause	Action
No proposal chosen	This message indicates that the Avaya 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 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 on the Avaya 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.
The secure extranet connection has been lost	This message indicates that the Avaya 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 was probably lost due to the Idle Timeout configured on the Avaya VPN Router. If no data is transferred through the extranet connection for a long period of time, normally 15 minutes or more, the Avaya VPN Router automatically disconnects the connection.	1. Click **Connect** to reestablish the extranet connection. If you are unable to reestablish the extranet connection, the dial-up connection preventsdata from traveling between the Avaya VPN Client and the Avaya VPN Router. 2. Hang up the dial-up connection and reconnect before you try to reestablish a connection. If you are still unable to connect to the Avaya VPN Router, perform the following steps: 1. Open an MS-DOS Command Prompt. 2. Ping the Avaya VPN Router using the host name or address that you specified in the Destination field. If you receive a Destination Unreachable error message, there is a routing problem at the ISP. If you receive a Request Timed Out error message, the Avaya 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 in Windows 95 only,	Auto Disconnect if you do not use Internet Explorer to access data on the remote network. To do this: 1. Open the **Control Panel**. 2. Choose the **Internet** icon. 3. Select the **Connection** property tab. 4. Clear the **Disconnect if idle for** check box.

Troubleshooting banner message problem

This contains troubleshooting information about the hang at banner text message that might appear when launching the AVC.

In some situations, when you attempt to bring up a user tunnel from the AVC to Avaya VPN Routers, the tunnel establishment might hang at the Checking for banner text message.

Firewall blockage

A common reason for the banner message to hang is a firewall or router, placed somewhere along the path from the remote computer to the gateway, blocks ESP or 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 ISAKMP traffic that negotiates the tunnel establishment, the tunnel establishes, but the ESP- or AH-encapsulted traffic inside the tunnel does not get through. When the banner text is retrieved through the established tunnel, the banner message or any other traffic secured by the ESP or AH never reaches the client and the AVC continues to wait for 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

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 router requirements.

NAT transversal (NAT-T) blockage

The same scenario occurs as in the previous step if NAT-T is configured and the firewall blocks UDP port selected for NAT-T along the path. To resolve this, ensure the port specified in the NAT-T section of the Services IPSec window (shown below) is allowed to pass through the firewalls on a personal, corporate, or ISP level).

1. Access the Avaya VPN Router.
2. Choose **Services**, **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 to go 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 you use the most recent version of the AVC. 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 AVC. If third-party VPN client software runs at the same time as the AVC, it could interfere with AVC operation. In this case, disable or even uninstall third-party VPN clients because they might run in the background preventing successful AVC connections. Open the network interface properties window and uncheck any third-party adapters or drivers.

Index