



Configuration – Remote Worker

Avaya Business Communications Manager Release 6.0

Document Status: **Standard**

Document Number: **NN40171-505**

Document Version: **01.04**

Date: **October 2010**

© 2010 Avaya Inc.
All Rights Reserved.

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/](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

Contents	3
Customer Service	5
Navigation	5
Getting technical documentation	5
Getting product training	5
Getting help from a distributor or reseller	5
Getting technical support from the Avaya Web site	5
Getting started with remote worker support	7
About remote worker support	7
Audience	7
Acronyms	8
Symbols and text conventions	8
Related publications	9
Virtual private network configuration overview	11
Navigation	11
Network configuration	11
VPN configurations support	14
Remote worker configuration when branch tunnels are used	15
Security credentials	16
VPN Security banner	17
Licensing	17
Node-locked licensing	18
Using the BCM as an HTTP server for downloading license and configuration files	18
Prerequisites	19
Procedure steps	19
SRS-type license file tokens	19
Licensing user interface	19
Known issues	21
Invalid PSK userID	21
Procedure steps	21
Speech path interruption during re-key	21
Provisioning the VPN	23
Configuration parameters	23
Pre-provisioning VPN within the corporate network (before deployment)	24
Manual configuration using the Network Configuration menu	25
Remote provisioning using the remote PC application	25
Configuring the IP phone using the Remote PC Application	26

Remote worker configuration overview	29
Router configuration requirements	31
Configuring the remote worker feature	33
Enabling the remote worker keycode	33
Configuring the public IP address	34
Enabling the remote worker feature	34
Sample lab set up for remote worker configuration	37
Equipment requirements	38
VoIP signaling and media information	39
Router configuration for BCM50E #1	40
Firewall configuration	40
Static NAT and static PAT configuration:	42
Dynamic NAT and dynamic PAT configuration	43
Branch office tunnel configuration	44
VPN client termination configuration	45
Router configuration for BCM50E 2	47
Static NAT and static PAT configuration	47
Dynamic NAT and dynamic PAT configuration:	48
Branch office tunnel configuration	49
Router configuration for Secure Router 100x 1	50
Firewall configuration	50
Static NAT and static PAT configuration	51
Dynamic NAT and dynamic PAT configuration:	51
Router configuration snapshot	51
Router configuration for Secure Router 100x 2	52

Customer Service

This section explains how to get help for Avaya products and services. Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to <http://www.avaya.com> or go to one of the pages listed in the following sections.

Navigation

- “Getting technical documentation” on page 5
- “Getting product training” on page 5
- “Getting help from a distributor or reseller” on page 5
- “Getting technical support from the Avaya Web site” on page 5

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>.

Chapter 1

Getting started with remote worker support

This section contains information on the following topics:

- [“About remote worker support” on page 7](#)
- [“Audience” on page 7](#)
- [“Acronyms” on page 8](#)
- [“Symbols and text conventions” on page 8](#)
- [“Related publications” on page 9](#)

About remote worker support

Avaya Business Communications Manager 6.0 (BCM 6.0) includes new options for remote worker support. You can connect your Avaya 1100 Series IP Deskphone to the Avaya BCM through a secure VPN tunnel, or by using the new remote worker feature. Using the remote worker feature, you can use the BCM system as an HTTP server, allowing you to distribute configuration files, license files, and firmware to IP clients.

This guide includes an appendix, which provides details on a sample network setup that supports remote workers.

Audience

This guide is intended for administrators who want to configure the BCM for remote worker support.

Acronyms

This guide uses the following acronyms:

BOT	branch office tunnel
HTTP	hypertext transfer protocol
IP	internet protocol
LAN	local area network
NAT	network address translation
PAT	port address translation
PSK	pre-shared key
RTCP	realtime control protocol
RTP	realtime transfer protocol
UDP	user data protocol
VPN	virtual private network
WAN	wide area network

Symbols and text conventions

These symbols are used to highlight critical information for the [Product Name (short)] system:



Caution: Alerts you to conditions where you can damage the equipment.



Danger: Alerts you to conditions where you can get an electrical shock.



Warning: Alerts you to conditions where you can cause the system to fail or work improperly.



Note: A Note alerts you to important information.



Tip: Alerts you to additional information that can help you perform a task.



Security note: Indicates a point of system security where a default should be changed, or where the administrator needs to make a decision about the level of security required for the system.



Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.



Warning: Alerts you to remove the [Product Name (short)] main unit and expansion unit power cords from the ac outlet before performing any maintenance procedure.

These text conventions are used in this guide to indicate the information described:

Convention	Description
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the info command. Example: Enter show ip {alerts routes} .
<i>italic text</i>	Indicates book titles
plain Courier text	Indicates command syntax and system output (for example, prompts and system messages). Example: Set Trap Monitor Filters
FEATURE HOLD RELEASE	Indicates that you press the button with the coordinating icon on whichever set you are using.
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.

Related publications

Related publications are listed below. For more information about the Avaya Business Communications Manager 6.0 documentation suite, see *Documentation Roadmap* (NN40170-119).

Avaya Business Communications Manager 6.0 Configuration — Telephony (NN40170-502)

Chapter 2

Virtual private network configuration overview

The virtual private network (VPN) feature provides VPN client capability to the following IP sets:

- Avaya 1120E IP Deskphone
- Avaya 1140E IP Deskphone
- Avaya 1150E IP Deskphone

For more information about configuring your IP set for VPN, see the Avaya IP Deskphone configuration guide for your model of IP set.

Navigation

- ["Network configuration" \(page 11\)](#)
- ["VPN configurations support" \(page 14\)](#)
- ["Remote worker configuration when branch tunnels are used" \(page 15\)](#)
- ["Security credentials" \(page 16\)](#)
- ["VPN Security banner" \(page 17\)](#)
- ["Licensing" \(page 17\)](#)
- ["Using the BCM as an HTTP server for downloading license and configuration files" \(page 18\)](#)
- ["Known issues" \(page 21\)](#)

Network configuration

The following table shows supported VPN routers.

Table 1 VPN routers

Router	Model	Release
VPN router	1750, 2700, 5000	Release 3.2
VPN gateway	3050, 3070	Release 7.0
Avaya Business Communications Manager 50 (BCM50) integrated router	Avaya BCM50a/ba, BCM50e/be, CSC versions other than 1*	Release 6.0
Note: Your CSC version can be found in Business Element Manager at Administration > Hardware Inventory > Additional Information > CSC Hardware version		

The VPN feature enables the set to establish an encrypted VPN tunnel from the set to a Avaya BCM 6.0 system. When the tunnel is established, the following IP set-related traffic traverses the tunnel:

- UNISTim signaling
- media
- TFTP provisioning
- HTTP provisioning

All set-related traffic must travel through a single tunnel. For example, it is not possible for some traffic to travel inside the tunnel and some traffic to travel outside the tunnel. Traffic on the PC port of the set is always excluded from the VPN tunnel.

If you have a BCM50 system with an integrated router (BCM50a, BCM50ba, BCM50e, or BCM50be models) the VPN tunnel terminates on the BCM50 integrated router. If you use pre-shared key (PSK) authentication, user credentials are validated on the BCM50 integrated router. If you use XAUTH authentication, user credentials are validated on the BCM50 integrated router and on the Radius server, which resides on the customer LAN.

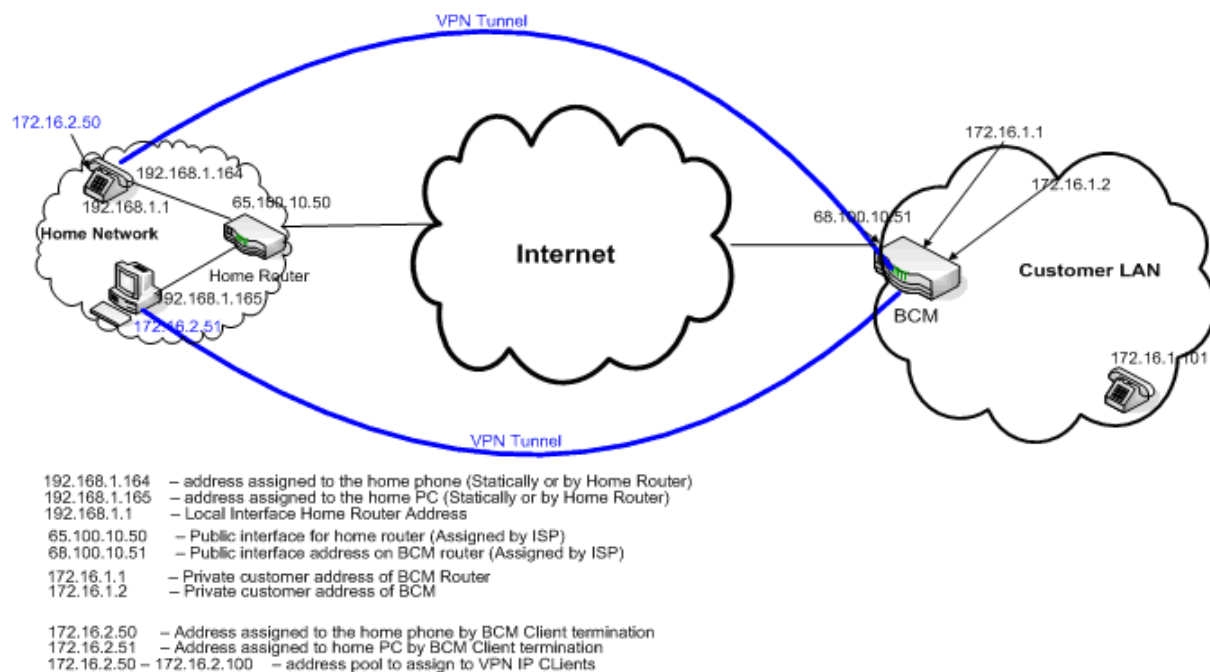
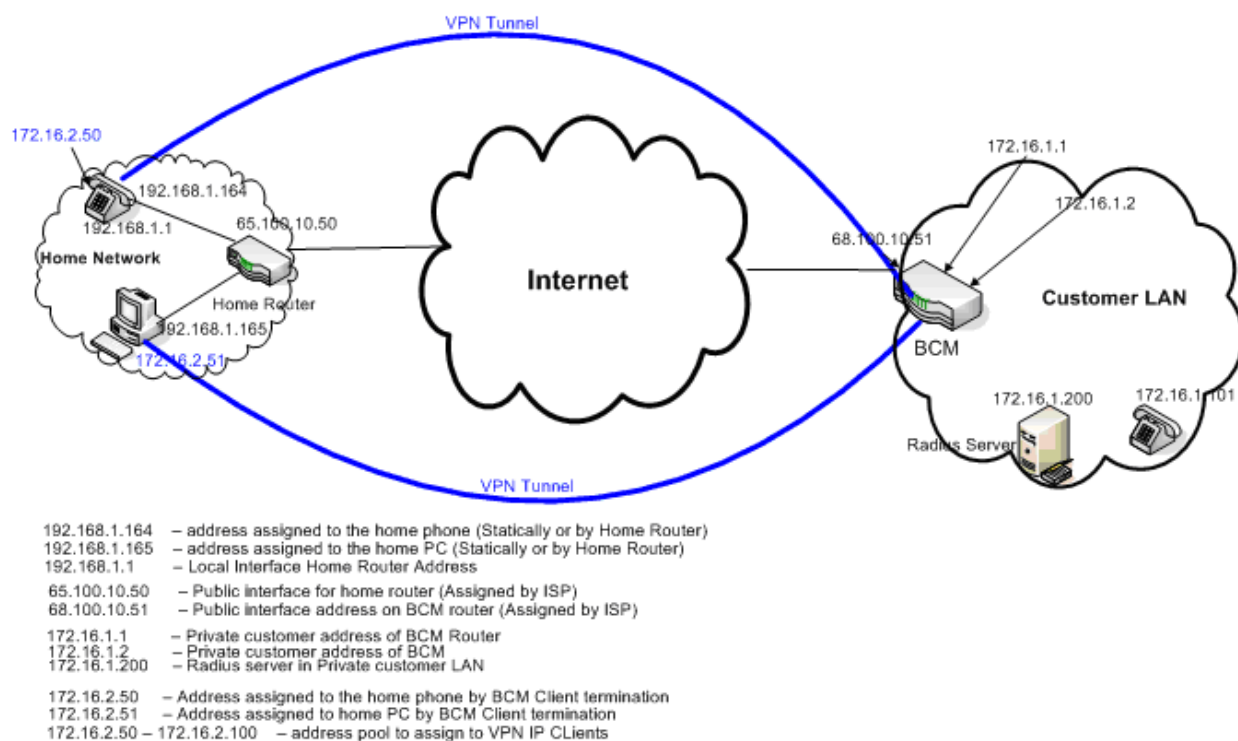
You must install the VPN client for your version of Windows on your PC or laptop in order to utilize the VPN feature. For more information about configuring VPN client termination on a BCM50 integrated router, see the BCM50 Integrated Router Configuration Guide for your BCM50 model. For information about configuring VPN client termination on a VPN router or VPN gateway, see the configuration guide for your model of VPN router or VPN gateway.

VPN access to the BCM Customer LAN consists of 3 separate networks:

- Home network - The VPN user's home network, located behind a router and connected through an Internet Service Provider (ISP) to the Internet.
- Public Internet - Access to this network is provided by the ISP.
- BCM LAN - The office LAN with the BCM providing telephony services.

The BCM LAN and the Home LAN network cannot be on the same LAN. Most commercially available home routers and BCM systems share the same default subnet of 192.168.1.x, Avaya recommends that the subnet on the BCM system be changed.

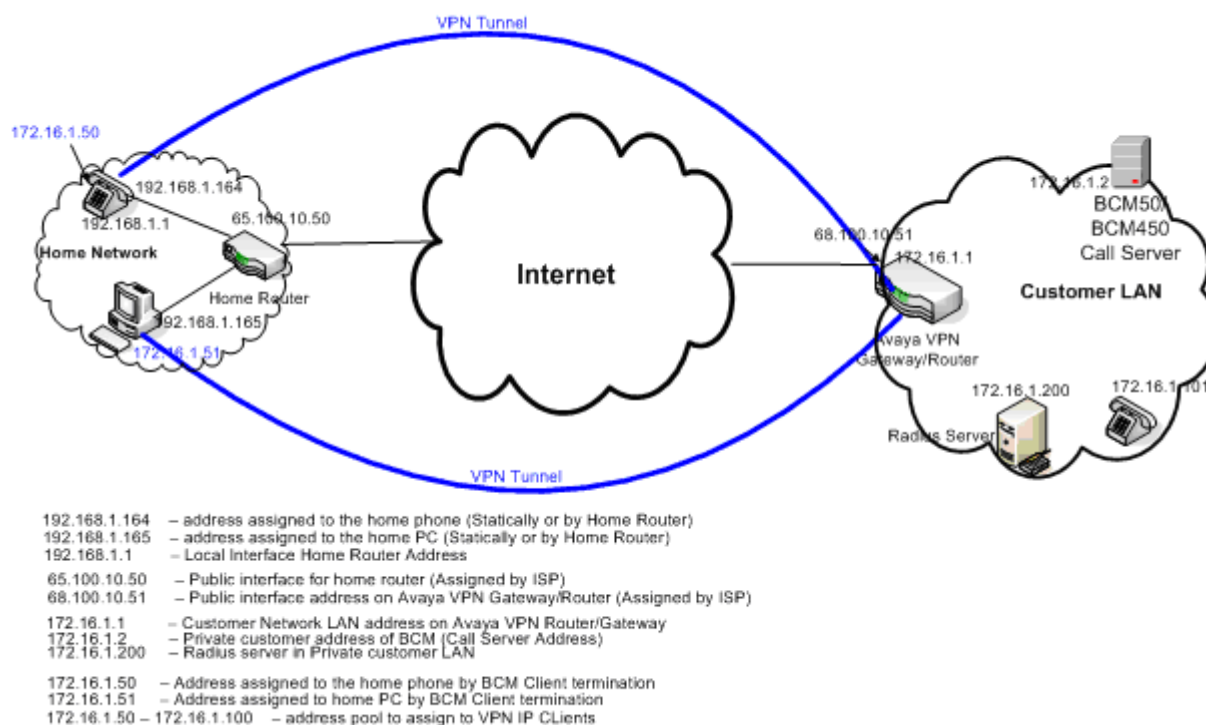
[Figure 1 "PSK authentication network diagram" \(page 13\)](#) shows the VPN deployment model with a BCM50 system with an integrated router using PSK authentication. [Figure 2 "XAUTH authentication network diagram" \(page 13\)](#) shows the VPN deployment model with a BCM50 system with an integrated router using XAUTH authentication.

Figure 1 PSK authentication network diagram**Figure 2** XAUTH authentication network diagram

If you have a BCM450 system, or a BCM50 system that does not include an integrated router, you can use a VPN router or VPN gateway. In this case, place the VPN router or gateway on the edge of your network. The VPN tunnel from the set terminates on the VPN router or gateway and the set registers to the call server on the BCM50 or BCM450 system. This configuration is used when you have a large number of VPN users (set or CVC).

Figure 3 "VPN router/gateway and BCM call server network diagram" (page 14) shows a configuration of a network using a VPN router or gateway and a BCM call server.

Figure 3 VPN router/gateway and BCM call server network diagram



VPN configurations support

The following table shows valid VPN configuration parameters for IP sets. BCM supports Aggressive mode when you use a VPN router or VPN gateway.

Table 2 Supported configurations

VPN parameter	Aggressive mode PSK with no XAUTH	Aggressive mode PSK with XAUTH	Main mode X.509 with no XAUTH
Protocol	VPN router/gateway	VPN router/gateway	VPN router/gateway
Mode	Aggressive	Aggressive	Main*
Authentication	PSK	PSK	X.509
PSK-UserID	<user_ID>	<user_ID>	N/A

Table 2 Supported configurations

VPN parameter	Aggressive mode PSK with no XAUTH	Aggressive mode PSK with XAUTH	Main mode X.509 with no XAUTH
PSK-Password	<user_password>	<user_password>	N/A
XAUTH	dis	ena	dis
XAUTH-UserID	N/A	<user_password>	N/A
XAUTH-Password	N/A	<user_password>	N/A
Primaryserver	<FQDN>	<FQDN>	<FQDN>
Secondaryserver	<FQDN>	<FQDN>	<FQDN>
Root Cert	N/A	N/A	<required>
Device Cert	N/A	N/A	<required>
*Note: Main mode is not supported if client termination resides on the BCM system.			

Remote worker configuration when branch tunnels are used

You can deploy VPN Client tunnels the Avaya BCM50a/e when VPN branch tunnels are used. When you deploy VPN Client tunnels in this manner, the number of active tunnels you can have is limited on the BCM50a/e.

Complete the following procedure to establish a VPN between two sites using a VPN branch tunnel. The recommended method to do this is through a branch-to-branch IPSec tunnel. For more information, see *BCM50e Integrated Router Configuration — Basics* (N0115788).

- 1 In VPN / Summary, add a new tunnel by editing an unused rule.
- 2 Create an Active Branch Office tunnel.
- 3 Select **Nailed Up**, if the tunnel should not be closed while not in use.
- 4 Select **Main** for Negotiation Mode.
- 5 Enter the authentication information, with either a pre-shared key or an imported certificate.
- 6 Enter the IP Address assigned to the router WAN port. This should be a static address, or a dynamic DNS name, and the IP address of the remote router.
- 7 Select the encryption and authentication algorithms.
- 8 Add an IP policy, by specifying the IP address ranges of the local and remote hosts that use the tunnel.
- 9 Repeat these steps 1 through 7 at the other end of the branch.



Note: If a VPN Client Termination is used on these sites, you must include the client termination address range in the tunnel policies in order for the VPN clients to see the other site.

Security credentials

The VPN feature requires different types of security credentials depending on the mode of authentication selected. Security credentials are configured on the VPN router or VPN gateway by the administrator. For more information about configuring security credentials, see the configuration guide for your VPN router or VPN gateway.

The following table shows which credentials are required for each mode.

Table 3 Security credentials required for each authentication mode

Mode	Credentials
Aggressive Mode with Authentication PSK, XAUTH disabled	PSK (user ID and password)
Aggressive Mode with Authentications PSK and XAUTH enabled	PSK (user ID and Password), XAUTH user ID, and XAUTH password
Main Mode X.509 certificates, no XAUTH*	Root certificate, device certificate
*Not applicable if the BCM is used to terminate the tunnel.	

The following list provides a description of the credentials.

- PSK (user ID and password)

The IP set uses PSK to authenticate itself to the VPN router (also known as Group ID and Group Password). You can provision PSK in the configuration menu or through a configuration file. The PSK user ID and password is a maximum of 20 alphanumeric characters.

You can configure the user ID manually or you can pre-configure the user ID using the configuration file. If you save the PSK user ID, you do not have to reenter it when you want to use it.

You can configure the password manually or pre-configure the password using the configuration file. Optionally, you can leave the password blank. If you configure the password, you do not have to reenter it when you use it. If you do not configure the password, you are prompted to enter it each time it is required. You can configure the VPN server to provide a policy message to instruct the set not to save the password locally. The server policy takes precedence over the password saved in the IP set.



Note: The XAUTH password is saved locally to the IP set until the IP set successfully connects to the VPN server for the first time. The VPN server policy then takes precedence.

- XAUTH (user ID and password)

The user ID and password is the end user password used with XAUTH protocol, which authenticates the user to the VPN router. The User ID and Password can be provisioned in the configuration menu or through a configuration file. You can configure the VPN server to provide a configuration message to instruct the set not to save the password locally. The server configuration takes precedence over a provisioned password.

The XAUTH User ID and Password is remembered temporarily to allow graceful to the VPN server due to temporary network interruptions. These re-connections to the VPN server do not prompt the end user to enter the credentials. However, if the IP set powers down and powers up, then the user is prompted for credentials when the call server policy dictates the password is not allowed to be saved locally.



Note: X.509 certificate credentials are always handled by the VPN router. The user is not prompted to enter a user ID or password.

- Main Mode X.509 (root certificate, device certificate)

Root certificate is the customers root certificate and is installed as part of the configuration file or as part of the SCEP process. Device certificate is assigned specifically to the set. It is installed using the SCEP process when the set is configured prior to the installation process. If the set is configured using the peer-to-Peer configuration process the device certificate is installed directly from the associated PC.

VPN Security banner

The VPN Security Banner presents security information provided by the VPN gateway on the set display.

The banner displays when the set establishes a VPN tunnel to the VPN gateway for the first time, after which the set accepts the banner without user intervention. If you change the VPN primary gateway VPN Server 1 parameter, the new security banner is displayed.

You must accept the Security Banner to establish a tunnel and allow data traffic. If you select Cancel you are prompted to accept the security Banner again.

Licensing

The VPN feature requires a license for each set you want to connect remotely. When you first power on the set or when the set establishes the tunnel, the VPN feature queries the license client to determine if the set has sufficient licensing tokens. If system denies the license request, telephony services are restricted. Local menus, such as Diagnostics, Provisioning, and Configuration menus can still be activated. The VPN Tunnel will still activate which allows you obtain valid license file, and provisioning information.

The IP set downloads the license files automatically from the BCM when it establishes a connection to the BCM call server. For more information about using the BCM system as an HTTP server for downloading license and configuration files, see ["Using the BCM as an HTTP server for downloading license and configuration files"](#) (page 18).

Node-locked licensing

Node-locked licensing is intended primarily for small phone installations where you do not want to manage a license server. In this case, the token license file created by KRS is keyed to a specific phone by using the MAC address of that phone. The token license file is then loaded to the phone. The license client does not attempt to access any license server and instead grants token requests to the phone application, as long as the request does not exceed the number of tokens provided in the license file.

Downloading the licence file

Complete this procedure to download a token license file for VPN access on IP phones.

- 1 Configure the IP phone with a provisioning IP address so it can access a provisioning server.
- 1 Enter the license file of the phone in the server.

The file format of the license file is <ipctokenMAC.cfg>, where MAC is the 12-character MAC address of the IP phone.

- 2 Add a [LICENSING] section to the phone configuration file, for example, 1110.cfg, 1120e.cfg, 1140e.cfg, 1150e.cfg.

```
[LICENSING]
```

```
VERSION version
```

```
FILENAME X*.Y
```

- 3 Start the provisioning server so the phone can retrieve the .cfg files when it boots.

When the phone retrieves the setting during boot up, it downloads the licensing file, renames the file as ipclient.lic, and then saves the file in the phone flash.

Using the BCM as an HTTP server for downloading license and configuration files

You can use a BCM as an HTTP server to download the license and configuration files for an Avaya 1100 Series IP Deskphone. Additionally, Avaya 1120e IP Deskphones and Avaya 1140e IP Deskphones can establish an encrypted VPN tunnel to a VPN server. The VPN tunnel carries all set-related traffic, enabling you to use your set remotely.

In order to enable the VPN feature, an administrator must first prepare the configuration files and obtain the license files for the IP sets and upload it to the BCM system. The administrator specifies the BCM as an HTTP server in the configuration files. After the VPN feature is enabled on the set and establishes a VPN tunnel the model configuration file (for example, 1140e.cfg) and license file are downloaded from the BCM giving the user full use of the VPN connection. This feature is compatible with PSK and dual-factor authentication methods.

Every time the set reboots, it connects with the BCM to read the configuration files and download the firmware or license file if necessary.

The configuration files stored on the BCM are backed up with the data from IP Telephony. The Delete All button in the Business Element Manager removes all IP set configuration files uploaded if the administrator wants to remove this functionality from the BCM.

The initial configuration files for the Avaya 1100 Series IP Deskphones can be downloaded from <http://www.avaya.com/support>.

For information about setting up a BCM system as an HTTP server, see *Avaya Business Communications Manager 6.0 Configuration — System* (NN40170-501). For more information about configuring VPN on the BCM50 integrated router, see the BCM50 Integrated Router configuration guide for your system. For more information about configuring your VPN router or VPN gateway, see the configuration guide for your router or gateway.

Prerequisites

- Ensure that you have an available IP client license for each IP set you want to use.

Procedure steps

- 1 Upload the configuration files to the BCM. For information about managing configuration files, see *Avaya Business Communications Manager 6.0 Configuration — System* (NN40170-501).
- 2 On the user's PC, run the IP VPN configuration tool to enable and setup the VPN connection on the IP set. Once the VPN connection is established the configuration files, license files, and any firmware updates are automatically downloaded.

SRS-type license file tokens

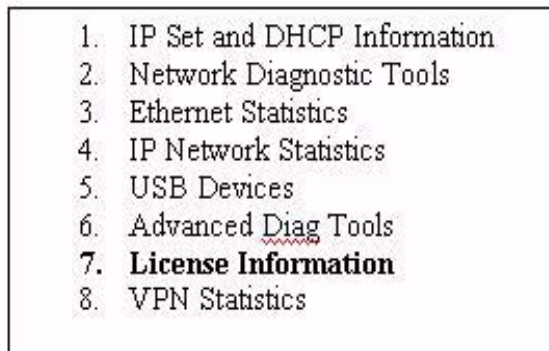
SRS-type license file tokens are service contract tokens that are verified based on the firmware build and warranty date of the client. For IP clients, there are two types of keycodes for this type of license file token: an SRS-based keycode and an expiry-based keycode (expires based on an expiry date associated with the keycode). The licensing file generated by KRS can contain an SRS keycode, which has contract expiry date.

The SRS-type license file token is valid when either the client firmware build date or the warranty date within the contract date is specified in the token. The token is verified against the firmware build date first. If verification of the contract date fails, the licensing client requests an expiry-type keycode from the server to fulfill the initial request. The licensing client always requests an SRS-type keycode first and an expiry-based keycode only if verification of the former fails.

Licensing user interface

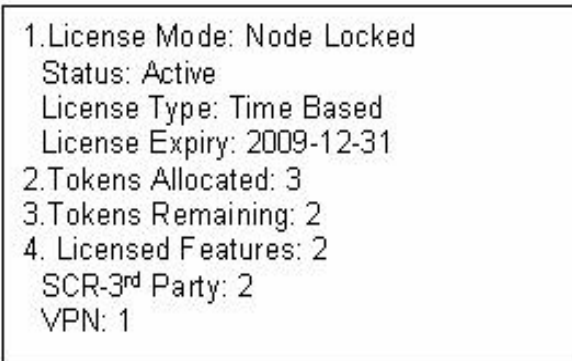
The licensing feature introduces a new submenu to the existing Local diagnostics menu in the IP phone interface. In the IP phone licensing submenu, select 7 to see your current licensing information.

Figure 4 Licensing interface, main menu

- 
1. IP Set and DHCP Information
 2. Network Diagnostic Tools
 3. Ethernet Statistics
 4. IP Network Statistics
 5. USB Devices
 6. Advanced Diag Tools
 - 7. License Information**
 8. VPN Statistics

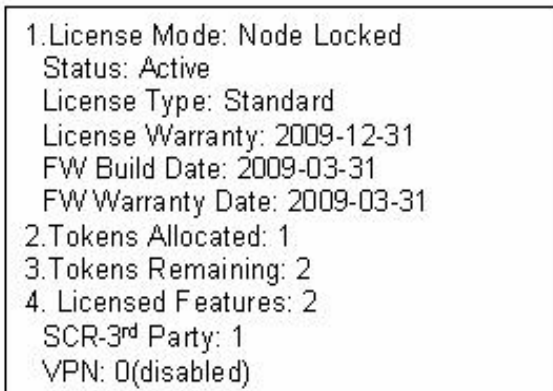
If the type of active license on the phone is node-locked and time-based, the License Type field indicates this, and shows the expiry date of the license token.

Figure 5 Node-locked mode licensing, time-based license token

- 
1. License Mode: Node Locked
Status: Active
License Type: Time Based
License Expiry: 2009-12-31
 2. Tokens Allocated: 3
 3. Tokens Remaining: 2
 4. Licensed Features: 2
SCR-3rd Party: 2
VPN: 1

If the type of active license on the phone is node-locked and SRS-based, the License Type field indicates this, and shows the warranty date of the license token, the firmware build and the warranty date of the firmware build.

Figure 6 Node-locked mode licensing, SRS-based license token

- 
1. License Mode: Node Locked
Status: Active
License Type: Standard
License Warranty: 2009-12-31
FW Build Date: 2009-03-31
FW Warranty Date: 2009-03-31
 2. Tokens Allocated: 1
 3. Tokens Remaining: 2
 4. Licensed Features: 2
SCR-3rd Party: 1
VPN: 0(disabled)

The licence information screen also provides information on the number of tokens allocated and remaining to be used, as well as the number of licensed features available.

Known issues

This section describes known issues and possible solutions for the VPN feature.

Invalid PSK userID

If the VPN tunnel terminates on a BCM50 integrated router and the PSK userID is incorrect, the tunnel does not establish and the system does not prompt to re-enter your credentials.

In this case, the PSK userID must be corrected manually. This limitation applies to PSK and XAUTH authentication methods. Use the following procedure to manually re-enter your PSK credentials.

Procedure steps

- 1 On the IP set, press **Services** twice.
- 2 Select option 3.
- 3 Press the right arrow key to scroll through the options and select **PSK UserID**.
- 4 Press **Enter** to edit the field.
- 5 Re-enter your PSK userID, followed by **Enter**.
- 6 Press the **Apply** softkey. The IP set reboots and attempts to re-establish the VPN tunnel. If the VPN tunnel is not established, contact your system administrator to verify that the PSK userID is correct.

Speech path interruption during re-key

During the VPN tunnel re-key there can be a small (1 second) speech path interruption on active calls or at the dial tone. This is caused by a delay in the VPN gateway response to the re-key sequence. After the initial interruption the set operates normally.

The re-key timer is configurable on the VPN router or VPN gateway with a default of 8 hours. Setting this timer to a larger value reduces the occurrence of this issue. For more information about setting the re-key timer, see the configuration guide for your VPN router or VPN gateway.

Chapter 3

Provisioning the VPN

There are three options for configuring a phone for virtual private network (VPN). The method you choose can depend on whether or not the phone must be provisioned before deployment to the home user.

- "Pre-provisioning VPN within the corporate network (before deployment)"
- "Manual configuration using the Network Configuration menu"
- "Remote provisioning using the remote PC application"

For procedures on how to configure the VPN and the IP phone before deployment to the remote worker, see *Business Communications Manager 6.0 Administration — Remote Worker* (NN40171-600).

Configuration parameters

You can manually configure VPN using the Network Configuration screen on the IP phone. If Auto-Provisioning is enabled for VPN (default), you can install the full VPN configuration on the phone using configuration and provisioning files without manually entering the parameters.

The following tables show the mapping between the Network Configuration screen parameters and the Auto-Provisioning parameters, including the allowed values and defaults.

Table 1 Network Configuration screen and with Auto-Provisioning configuration parameters

Configuration parameter	Default value	Provisioning parameter	Provisioning values
VPN Enable	Disabled	vpn	y = Enabled n = Disabled
VPN Router Type	Avaya VPN	vpntype	1 = Avaya VPN
Mode	Aggressive	vpnmode	aggressive main
Authentication	PSK	vpnauth	psk certificate
XAuth	None	vpnauth	0 = None 1 = Password
PSK User ID	<Empty>	vpnpskuser	<string>
PSK Password	<Empty>	vpnpskuser	<string>
XAuth User ID	<Empty>	vpnauthuser	<string>
XAuth Password	<Empty>	vpnauthpwd	<string>
VPN Server 1	<Empty>	vpns1	<string> (IP address or FQDN), see Note)

Table 1 Network Configuration screen and with Auto-Provisioning configuration parameters

Configuration parameter	Default value	Provisioning parameter	Provisioning values
VPN Server 2	<Empty>	vpns2	<string> (IP address or FQDN, see Note)
VPN DSCP	False (0)	vpndiffcny	y = Copy DSCP from original packet n= Use vpndiff value
	0	vpndiff	0 - 255
MOTD Timer	30 (seconds)	vpnmotd	0 - 999
Local DNS	<Empty>	N/A	N/A
Note: You can specify the configured VPN routers as either an FQDN or as an IP Address. Any combination of FQDN or IP Address between VPN Server 1 and VPN Server 2 is permitted. If you choose to enter an FQDN, the user's local network must have access to DNS to resolve the entered name. Typically in a home office environment, this is the DNS server associated with the user's Internet connection.			

Pre-provisioning VPN within the corporate network (before deployment)

In the corporate network, you can use an existing provisioning server to configure a phone for VPN before deploying the phone to the remote worker.

The following describe the high-level steps of pre-provisioning VPN on an IP phone when you are working within the corporate network.

- 1 If a zone has been defined on the phone, you must add the following line to the system.prv file. This forces the phone to download a zone provisioning file.

```
file=z;
```



Note: If no zone has been defined on the phone, adding this line has no effect.

- 2 In the Network Configuration menu of the phone, enter the name of a new zone (for example, vpn).
- 3 Create a zone provisioning file (for example, vpn.prv) that contains the unique configuration attributes required for VPN.
- 4 Reboot the phone.

The zone provisioning file downloads and the VPN configuration is installed. After provisioning is complete, the phone automatically reboots with VPN activated.

Manual configuration using the Network Configuration menu

You can manually configure the IP phone for VPN anywhere, except when X.509 authentication is used. You must be familiar with the configuration interface of the phone before you try attempt manual configuration.

Use the Network Configuration screen on the phone to configure all VPN parameters. By default, VPN is set to be Auto-provisioned. To deselect auto-provisioning, press the Auto softkey. Deselect the box beside VPN. Press the Config softkey to return to the Network Configuration screen.

VPN parameters are located at the top of the Network Configuration screen and are now be enabled. You can now enter all non-certificate configuration parameters.

Remote provisioning using the remote PC application

End users who use the VPN remote worker solution to connect to their corporate phone network can configure their IP phone for VPN in the home office environment using the VPN Remote PC Application. Users can use this application to upgrade their Unistim to version 4, which is required to support the VPN remote worker feature.

The VPN Remote PC Application is a wizard-style, stand-alone Java application that runs on Windows XP, Windows Vista, and Mac platforms. The application supports 25 languages.

The VPN Remote PC Application is supported on the following IP deskphones:

- 1120E
- 1140E

The VPN Remote PC Application simplifies VPN setup on the phone by

- supporting configuration files packed in a zip file
- using built-in TFTP/HTTP servers that allow the application to act as a provisioning server to update the phone software and to provision VPN parameters
- using a discovery service that detects phones automatically
- eliminating the need for the user to manually configure the phone

Without the VPN Remote PC Application, the end user must set up the phone manually. To setup VPN on the phone manually, the end user must have:

- network-specific knowledge:
- phone installation in the network
- phone-specific knowledge
- interaction with HTTP/TFTP/FTP server
- HTTP, TFTP or FTP server
- zip application

Before the end user can configure their IP phone using the application, their system administrator must provide them with the required configuration/provisioning files and the VPN Remote PC Application. The system administrator can email the zipped files and the application to the end user for installation on their home PC.

For phones with UNISTim 4 software pre-installed, the user completes the following set up steps.

- 1 Launch the VPN Remote PC Application.
- 2 Select the zip file sent to them by their system administrator.
- 3 Press a short key sequence on the phone.
- 4 Click a button in the VPN Remote PC Application to start configuration.

Configuring the IP phone using the Remote PC Application

- 1 Launch the Remote PC Application.
- 2 In the Welcome and Language Selection screen, select your language preference from the drop-down list.
- 3 Click **Next**.
- 4 In the Equipment Setup and VPN screen, mouse over the network diagrams to ensure your cable connections are correct between your home router, PC, and IP phone.
- 5 Click **More** for additional information about VPN before disconnecting.
- 6 Click **OK**.
- 7 Click **Next**.
- 8 In the Select Data Files screen, click **Browse** to navigate to the folder where your configuration files are stored.
- 9 Click **Next**.
- 10 In the Prepare Phone for Configuration screen, press the key sequence indicated in the Wizard screen to put the phone into Listening Mode.
- 11 Click **Yes** to confirm the phone is in Listening Mode. Click **No** if the phone is not in Listening Mode.

If your phone is not in Listening Mode, you must manually prepare the phone to be configured. Follow the instructions provided in the Wizard to reboot the phone, navigate to the provisioning screen, and manually provision your IP address.

When you have manually configured the phone, return to the Prepare Phone for Configuration screen, and click **Yes** to confirm that the phone is now in Listening Mode.

- 12 With the phone in Listening Mode, in the Autodiscover Phone screen, allow the Wizard to detect your phone.
- 13 If more than one IP phone is discovered, verify the MAC address on the label on the back of your phone. Select the correct MAC address from the drop-down list in the Wizard screen.

- 14 When the phone is discovered, record the details indicated in the Confirmation and Finish Screen.
- 15 Click **Finish**.

Chapter 4

Remote worker configuration overview

Avaya Business Communications Manager 6.0 (BCM 6.0) introduces the UNISTim remote worker feature. The remote worker feature is an alternative to configuring a virtual private network (VPN) for IP sets to connect to the BCM.

You can configure the remote worker feature to support the registration of UNISTim terminals located on a public network as UNISTim remote users with an Avaya BCM located on the corporate network. The public network where the UNISTim terminals reside can be located on the public network or on private networks behind home routers. A home router can also mean a branch router, such as a router located at a business headquarters interacting with its remote branches. The BCM is located behind a corporate router. The BCM can be accessed from the public network using its public IP address and dedicated UNISTim signaling ports. UNISTim signaling ports are 7000 to 7002. These ports are fixed on the BCM. Open these ports at the corporate secure router. After successful registration, remote UNISTim users can access services in the same way as locally registered UNISTim users. When you enable the remote worker keycode, its scope is global. As many remote worker IP sets can register as there are IP client seats available.

All media that involves remote UNISTim terminals is anchored at the BCM and relayed by BCM RTP relay sessions. You can configure the BCM user data protocol (UDP) port range 30000 to 30xxx through the Business Element Manager for BCM RTP relay sessions for the remote worker media path. On the corporate router, open the UDP port ranges for UNISTim signaling and media and redirect this traffic through either static network address translation (NAT) or static port address translation (PAT).



Note: The media between two remote UNISTim terminals that are collocated behind the same home router and that do not have call recording turned on for calls, are directly connected to each other and are not relayed through the BCM. This is also true for IP sets collocated behind the same private corporate network where the BCM resides, or two IP sets collocated on the public network, that do not have call recording turned on for calls.



Note: When VPN is configured, signaling and media traffic of remote workers is encrypted. Unlike over a VPN, when the remote worker feature is enable, signaling and media traffic is not encrypted.

The following figure illustrates a sample network setup between a public network, or private network behind home routers, and the private corporate network where the BCM resides behind the corporate secure router. Behind the corporate secure router, the BCM is configured with the remote worker feature to allow a connection with the IP set to be established. All IP sets on the public side and on the remote private side register with the BCM using the public IP address of the router. UNISTim signaling is always exchanged through the BCM.

For the media path there are five scenarios for intercom calls (that is, IP sets registered on the same BCM and calling each other). The media path behavior falls in two categories:

- 1 the media path is optimized so that IP sets send RTP/RTCP (real time control protocol) streams directly to one another
- 2 the media path is anchored on the BCM so that it is relayed by the BCM itself using its public IP address in the configured range of 30000-30xxx

Scenario 1: Two private IP sets reside on the same private LAN where the BCM is located. The media path is optimized in such a way that the two IP sets send RTP/RTCP streams directly to one another.

Scenario 2: Two private IP sets reside behind the same home router and remotely register with the same BCM. The media path is optimized in such a way that the two IP sets send RTP/RTCP streams directly to one another.

Scenario 3: A private IP set resides on the private LAN where the BCM is located. The first IP set calls another IP set that is on the public side or behind a remote home router. The media path is anchored on the BCM in such a way that the media path is relayed by the BCM itself.

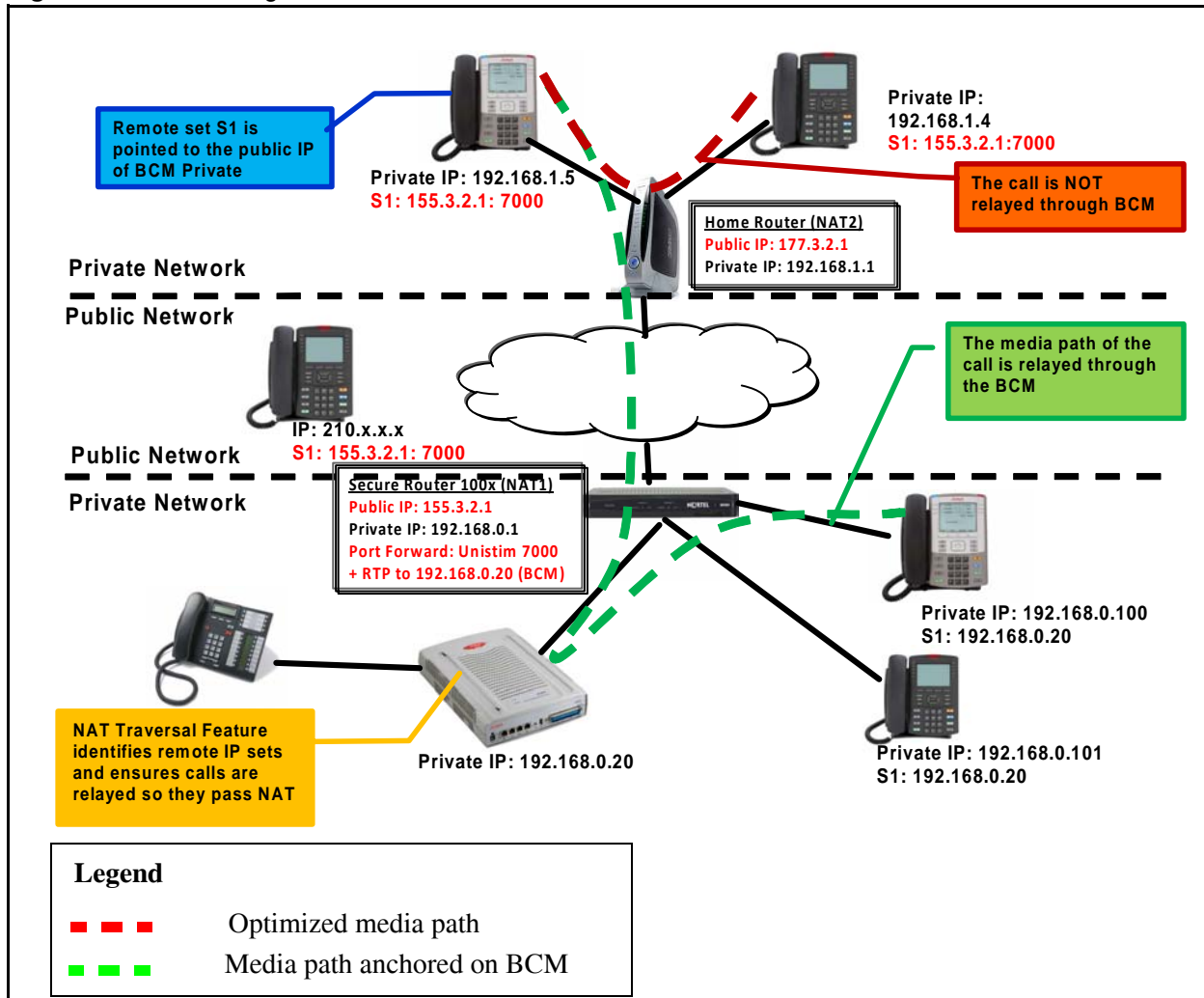
Scenario 4: A public IP set calls another IP set that is on the public side. The media path is optimized for a public-to-public path.

Scenario 5: A public IP set calls another IP set that is behind a remote home router. The media path is anchored on the BCM in such a way that the media path is relayed by the BCM.

Scenario 6: Two IP sets each that reside behind separate home routers call one another. The media path is anchored on the BCM in such a way that the media path is relayed by the BCM itself.



Warning: You must ensure that the remote terminal is not configured with both the BCM public IP address and the published IP address (for example, S1=BCM public IP address while S2=BCM published IP address).

Figure 7 Network diagram of remote worker feature

Router configuration requirements

At a minimum, you must configure the secure router to do static network address translation (NAT) of all the public traffic to the BCM on the LAN side and the other way around. In the example shown in Figure 1, traffic from the public network destined to IP address 155.3.2.1 on the router is translated through NAT to the destination IP address 192.168.0.1 on the private network so that it can reach the BCM. The reverse mapping is also done when the BCM sends traffic from the private network to the public network through the secure router.

Alternatively, you can configure the secure router for static port address translation (PAT). This is also known as port forwarding. When you configure the secure router for PAT, only specific traffic is redirected to and from the BCM. The minimum static PAT configuration consists of translating the IP address of UDP traffic within the range of 7000 to 7002 to and from the public IP address (155.3.2.1) of the router and the private address (192.168.0.2) of the BCM. The private address (192.168.0.2) of the BCM allows VoIP signaling from a remote IP set on the public network to reach the IP server on the BCM. In addition, for VoIP media to pass between the BCM and the remote IP set, you must configure static PAT to translate the range of realtime transfer protocol (RTP) and RTCP ports configured in the Business Element Manager for remote worker. The default range for UDP ports is 30000 to 30099 for BCM50 and 30000 to 30999 for BCM450.

When a firewall is required on the router, the firewall must at least permit the signaling traffic for IP sets and the associated media traffic for the remote worker IP set range to flow between the public network and the BCM on the private network.

Chapter 5

Configuring the remote worker feature

Complete the following procedures to configure the remote worker feature on the Avaya Business Communications Manager (BCM) to allow IP sets on the public network, or on a private network behind a home router, to access the secure router and connect with the BCM.

You must purchase and install a remote worker keycode to enable this feature. For more information about obtaining and installing keycodes, see *Keycode Installation Guide* (NN40010-301).

Before you configure the remote worker feature on the BCM, you must configure the RTP over UDP port ranges on the secure router to allow the IP set signals and media to flow to the BCM and from the BCM to the remote IP sets.

Enabling the remote worker keycode

Complete this procedure to enable the remote worker keycode and therefore to configure the remote worker feature.

- 1 Purchase and install the remote worker keycode.

For more information about obtaining and installing keycodes, see *Keycode Installation Guide* (NN40010-301).

- 2 In the Task Navigation Panel of the Business Element Manager, go to **Configuration > System > Keycodes**.
- 3 In the Feature Licenses table, click the remote worker keycode.
- 4 Click **Load Keycode File**.

Configuring the public IP address

You must configure the public IP address of the BCM on the secure router before you can enable the remote worker feature. For more information about how to configure the public IP address of the BCM, see *Avaya Business Communications Manager 6.0 Configuration — Telephony* (NN40010-502).



Note: If you do not properly configure the public IP address of the BCM when the remote worker feature check box is enabled, the remote worker IP sets cannot register with the BCM and show the error message SERVER: NO PORTS LEFT.

- 1 In the Task Navigation panel of the Business Element Manager, go to **Configuration > System > IP Subsystem > General Settings**.
- 2 In the Public Network area of the **General Settings** tab, click **Modify**.
The Modify Public Network IP dialog appears.
- 3 In the **Modify Public Network IP** dialog, type the appropriate values in the **Provisioned Public Address** field. Optionally, you can also configure the following fields:
 - Discovered Public Address
 - Provisioned Public Port
- 4 Click **OK**.

Enabling the remote worker feature

You must configure the public IP address of the BCM on the secure router before you can enable the remote worker feature. Complete this procedure to enable the remote worker feature.



Security note: When you enable the Support Remote Worker features, any IP set can potentially register with your system. To prevent unauthorized IP sets from registering with your BCM system, change the default IP set registration password and the default Telset administration password before you enable the feature. When no new IP sets must be registered, it is recommended that you deselect the Enable Registration option.

- 1 In the Task Navigation Panel of the Business Element Manager, go to **Configuration > Resources > Telephony Resources**.
- 2 In the **Telephony Resources** table, in the Configured Device column, click **IP Sets**.
The Details for Module pane appears below the Telephony Resources table.

- 3 In the IP Terminal Global Settings tab, select the **Support Remote Worker** checkbox.



Security note: When you select the Support Remote Worker checkbox and enable the feature, the following warning dialog appears:

WARNING

By enabling Support Remote Worker, IP set registration is accessible from the Internet and therefore it is important to take actions to prevent unauthorized registration of IP sets.

Prior to enabling, please ensure the following passwords are changed from system defaults to non-trivial passwords:

IP set registration (Global password)

Telset based administration (Telset account password)

Best practice – leave the Enable Registration option disabled when no new set registration is required.

You must accept the warning message to ensure that the default telset and global IP set registration passwords are updated and to avoid unauthorized IP set registrations from the public network.



Note: The Support Remote Worker checkbox is greyed out if you have not enabled the remote worker keycode.

- 4 If any IP sets show the error message SERVER: NO PORTS LEFT, you must power cycle the affected IP sets to force them to register with the BCM.

The remote worker feature is enabled.

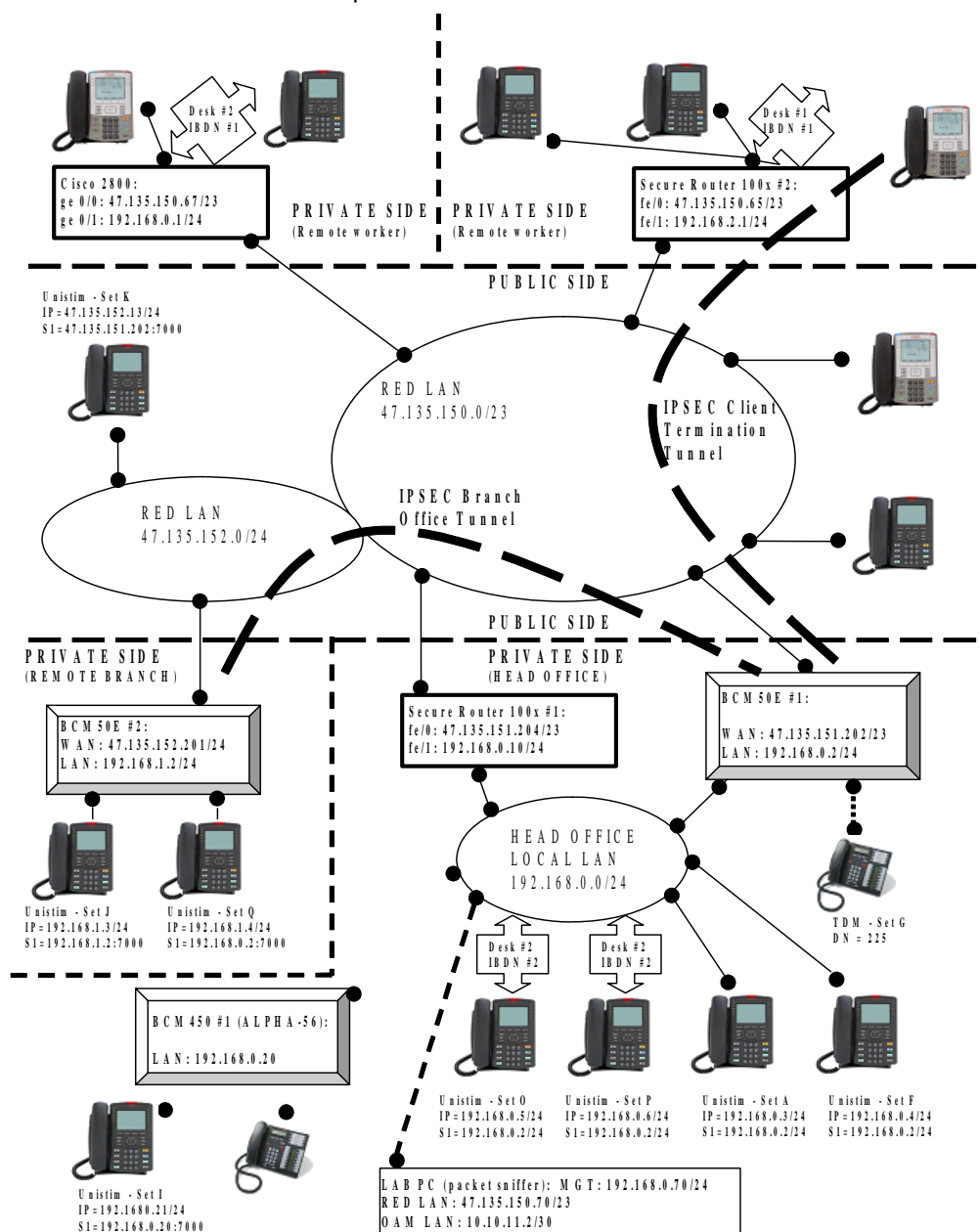
Appendix A

Sample lab set up for remote worker configuration

This appendix provides details on lab requirements for creating a network that uses and supports remote worker configuration.

Figure 8 shows the sample lab setup.

Figure 8 Remote worker network setup



Equipment requirements

The following table lists the equipment required for the network setup illustrated in [Figure 8](#).

Table 4 Remote worker network setup equipment requirements

Name	Model	Description
BCM50E #1		
BCM450 #1	Avaya BCM450	Main head office BCM450 system under test where few local and remote IP sets register.
BCM50E #2	Avaya BCM50E	Remote branch office BCM50E. The integrated router is configured to support IPSec BOT, NAT, and PAT.
Secure Router #1	Avaya SR1001	This router is configured to support NAT, PAT and firewall. This router sends public IP telephony traffic to BCM450 #1 on the private side.
Secure Router #2	Avaya SR1002	This router is configured to support PAT. The router can represent a remote branch without Avaya Business Communications Manager (BCM) or a home office.
Cisco 2800	Cisco 2800	This router is configured to support PAT. The router can represent a remote branch without BCM or a home office.
IP Set A	Avaya 1230	UNISTim IP set which registers locally with head office.
IP Set B	Avaya 1230	UNISTim IP set located behind a router which registers remotely with head office.
IP Set C	Avaya 1230	UNISTim IP set located behind a router which registers remotely with head office.
IP Set D	Avaya 1140E	UNISTim IP set located behind a router which registers remotely with head office.
IP Set E	Avaya 1230	UNISTim IP set located directly on the public network which registers remotely with head office.
IP Set F	Avaya 1230	UNISTim IP set which registers locally with head office.
TDM Set G	Avaya 7316E	TDM set directly connected to head office.
TDM Set H	Avaya 7316E	TDM set directly connected to head office.
IP Set I	Avaya 1230	UNISTim IP set which registers locally with head office.
IP Set J	Avaya 1230	UNISTim IP set which registers locally with branch office.
IP Set K	Avaya 1230	UNISTim IP set located directly on the public network which registers remotely with head office.
IP Set L	Avaya 1230	UNISTim IP set located behind a router which registers remotely with head office.
IP Set M	Avaya 1140E	UNISTim v4 IP set located behind a router which registers remotely with head office over a VPN client termination connection.
IP Set N	Avaya 1140E	UNISTim IP set located directly on the public network which registers remotely with head office.
IP Set O	Avaya 1230	UNISTim IP set which registers locally with branch office.
IP Set P	Avaya 1230	UNISTim IP set which registers locally with branch office.

Table 4 Remote worker network setup equipment requirements

Name	Model	Description
IP Set Q	Avaya 1230	UNISTim IP set located behind a BCM50 integrated router which registers remotely with head office over a VPN client branch to branch connection.
LAB PC	Windows XP	Lab PC for miscellaneous use.

VoIP signaling and media information

The following table provides information on NAT traversal and VoIP signaling and media requirements for each of the IP sets used in the sample network setup.

Table 5 IP set network requirements

Phone	NAT traversal feature required?	Encrypted VoIP signaling and media?	Comment
IP Set A	No	No	
IP Set B	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.
IP Set C	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.
IP Set D	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.
IP Set E	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.
IP Set F	No	No	
TDM Set G	No	No	
TDM Set H	No	No	
IP Set I	No	No	
IP Set J	No	No	
IP Set K	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.

Table 5 IP set network requirements

Phone	NAT traversal feature required?	Encrypted VoIP signaling and media?	Comment
IP Set L	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.
IP Set M	No	Yes	IPSec Client Termination to BCM50E #1 is used to encrypt.
IP Set N	Yes	No	BCM 6.0: The IP set indicates NO PORTS LEFT on the display without the NAT traversal feature. BCM 5.0: Set registers with UTPS server but no media path is available without the NAT traversal feature.
IP Set O	No	No	
IP Set P	No	No	
IP Set Q	No	Yes	IPSec BOT between BCM50 #1 and BCM50#2 are used to encrypt.

Router configuration for BCM50E #1

The integrated router on BCM50E #1 is configured with firewall, static network address translation (NAT) and port address translation (PAT), as well as dynamic NAT and PAT. This configuration uses both IPSec branch office tunnel (BOT) and VPN client termination.

Firewall configuration

The integrated router is configured to permit some traffic from the WAN side to the router and to the LAN, but block any other type of traffic coming from the WAN. All traffic flowing from LAN to WAN is permitted.

The remote worker feature requires, at a minimum, the following rules:

- UNISim signaling: UDP ports 7000-7002
- RTP/RTCP media: UDP ports 30000-30099

IPSec BOT and client termination require the following rules:

- IKE: UDP port 500
- IPSec ESP: protocol 51
- IPSec NAT traversal: UDP port 4000

Optional BCM applications and VoIP protocols require the following rules:

- Business Element Manager: TCP port 5989
- SSH: TCP port 22
- SIP: UDP port 5060

- HTTP: TCP port 80
- HTTPS: TCP port 443
- BCM Monitor: TCP port 60001

Optional BOOTP client and ping support require the following rules:

- ICMP (ping): protocol 1
- BOOTP client: UDP port 68

Figure 9 and Figure 10 show the GUI panels where the firewall is configured.

Figure 9 Business Element Manager firewall configuration panel — TCP configuration

The firewall protects against Denial of Service (DoS) attacks when it is enabled.
Note: Browser window will need to be refreshed after enabling the firewall.

☒ **Enable Firewall** ☐ **Bypass Triangle Route**

Firewall Rules Storage Space in Use

0% 100%

Packet Direction: WAN to LAN

Configured rules for this packet direction are displayed in the summary table below.

Action for packets that don't match firewall rules. ☒ Block ☐ Forward

☒ Log packets that don't match these rules.

#	Status	Source Address	Destination Address	Service Type	Action	Log	Alert
1	Active	Any	Any	*BEM(TCP:5989)	Forward	Disabled	No

Insert New Rule Before 1 (Rule Number).

Move Selected Rule (select an Index Number) To 1

Edit Selected Rule

Delete Selected Rule

Apply Reset

*BEM(TCP:5989)
 *RTP(UDP:30000-30099)
 *UTPS(UDP:7000-7002)
 *BCM Monitor(TCP:60001)
 PING(ICMP:0)
 HTTP(TCP:80)
 HTTPS(TCP:443)
 SSH(TCP/UDP:22)
 SIP-V2(UDP:5060)


Figure 10 Business Element Manager firewall configuration panel — IP Sec NAT configuration

Summary Attack Alert

The firewall protects against Denial of Service (DoS) attacks when it is enabled.
 Note: Browser window will need to be refreshed after enabling the firewall.

☒ Enable Firewall ☐ Bypass Triangle Route

Firewall Rules Storage Space in Use

0%  100%

Packet Direction: WAN to WAN / Business Secure Router

Configured rules for this packet direction are displayed in the summary table below.

Action for packets that don't match firewall rules. ☒ Block ☐ Forward

☒ Log packets that don't match these rules.

#	Status	Source Address	Destination Address	Service Type	Action	Log	Alert
1	Active	Any	Any	*IPSEC-NAT(UDP:4000) *IPSEC-NAT(UDP:4000) BOOTP_CLIENT(UDP:68) IKE(UDP:500)	Forward	Disabled	No

Insert New Rule Before 1 (Rule Number).

Move Selected Rule (select an Index Number) To 1 (Rule Number).

Edit Selected Rule

Delete Selected Rule

Apply Reset

Static NAT and static PAT configuration:

Traffic coming from the WAN side that is allowed through the firewall is translated and redirected to the customer LAN IP address of the BCM. This process is called static NAT. You configure static NAT by setting the default SUA/NAT server to the internal customer LAN IP address of the BCM50E. When a more specific SUA/NAT rule is configured, that rule takes priority over static NAT. The process by which more specific rules can redirect traffic to a server IP address on the LAN side, based on a port address or range of ports, is call static PAT.

Figure 11 Business Element Manager —static NAT and static PAT configuration panel

SUA Server Addr Mapping Trigger Port

Default Server 192.168.0.2

#	Active	Name	Start Port	End Port	Server IP Address
1	<input checked="" type="checkbox"/>	ike	500	500	192.168.0.1
2	<input checked="" type="checkbox"/>	ike nat trav	4000	4000	192.168.0.1
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0
+	<input type="checkbox"/>	RR-Reserv	1026	1026	192.168.0.1

Apply Reset

Dynamic NAT and dynamic PAT configuration

Traffic generated on the LAN and destined to the WAN side requires the use of dynamic PAT. This process allows applications on the private side to communicate with the public side, and preserve stateful NAT or PAT sessions so that traffic returning from the public side is sent back to the device that initiated the communication on the private side. To enable dynamic PAT, set the Network Address Translation field to a value other than None.

Figure 12 Business Element Manager — static PAT configuration

Route	WAN ISP	WAN IP	WAN MAC	Traffic Redirect	Dial Backup
WAN IP Address Assignment					
<input type="radio"/> Get automatically from ISP (Default)					
<input checked="" type="radio"/> Use fixed IP address					
My WAN IP Address			47.135.151.202		
My WAN IP Subnet Mask			255.255.254.0		
Gateway IP Address			47.135.150.1		
Network Address Translation					
			Full Feature ▾		
RIP Direction			None ▾		
RIP Version			RIP-1 ▾		
Multicast			None ▾		
Windows Networking (NetBIOS over TCP/IP)					
<input type="checkbox"/> Allow between WAN and LAN					
<input type="checkbox"/> Allow Trigger Dial					
<div>Apply Reset</div>					

Branch office tunnel configuration

A branch office tunnel (BOT) allows two branches to securely communicate over an encrypted IPSec tunnel. In this example, IKE is chosen as the key exchange protocol and the negotiation mode is set to Main.



Note: The selected negotiation mode (Main) must match at both ends of the branch offices otherwise the VPN tunnel cannot be established.

Figure 13 Business Element Manager — branch office tunnel configuration

Connection Type: Branch Office

☒ Active
☒ Nailed Up
 Name: TO_47_135_152_201
 Key Management: IKE
 Negotiation Mode: Main
 Encapsulation Mode: Tunnel

Available IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Selected IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
1	N/A	192.168.0.0/ 255.255.255.0	192.168.1.0/ 255.255.255.0

Authentication Method

☒ Pre-Shared Key
 Retype to Confirm:

☐ Certificate
 Local ID Type: IP
 Content: 0.0.0.0
 Peer ID Type: IP
 Content: 0.0.0.0

My IP Address: 47.135.151.202
 Secure Gateway Address: 47.135.152.201

☒ ESP
 Encryption Algorithm: 3DES
 Authentication Algorithm: SHA1

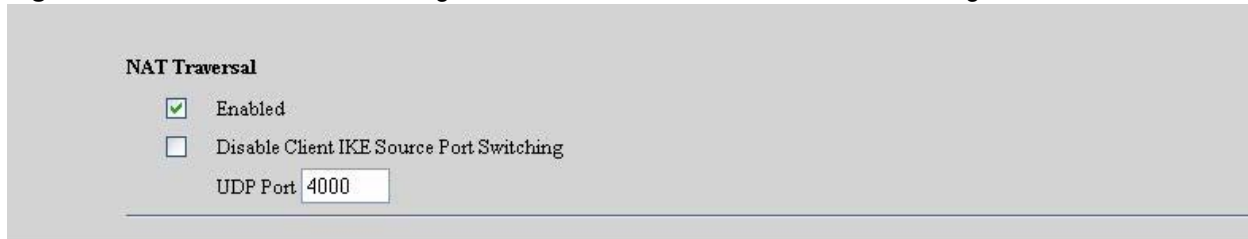
☐ AH
 Authentication Algorithm: MD5

VPN client termination configuration

You can configure the BCM50E to let remote IP devices communicate with the BCM over an encrypted VPN tunnel. In the lab setup, IP set M is configured with VPN parameters so that user1 can be authenticated, followed by the establishment of a VPN tunnel. The profile for user1 is designed to allocate IP address 192.168.3.200 to IP set M. VPN client termination and branch office tunnel can be established independently.

Figure 14 Business Element Manager — VPN client termination configuration

Summary	SA Monitor	Global Setting	Client Termination
<input checked="" type="checkbox"/> Enable Client Termination			
<hr/>			
Authentication			
<input checked="" type="checkbox"/> Local User Database (Configure Local User Database)			
<input checked="" type="checkbox"/> User Name and Password/Pre-Shared Key			
<input type="checkbox"/> RADIUS Server (Configure RADIUS Server)			
Group ID and Password			
Group ID		<input type="text"/>	
Group Password		<input type="text"/>	
Retype to Confirm		<input type="text"/>	
Authentication Type			
<input type="checkbox"/> User Name and Password			
<hr/>			
Encryption			
<input checked="" type="checkbox"/> ESP - 128-bit AES with SHA1 Integrity			
<input checked="" type="checkbox"/> ESP - Triple DES with SHA1 Integrity			
<input checked="" type="checkbox"/> ESP - Triple DES with MD5 Integrity			
<input checked="" type="checkbox"/> ESP - 56-bit DES with SHA1 Integrity			
<input checked="" type="checkbox"/> ESP - 56-bit DES with MD5 Integrity			
<input type="checkbox"/> AH - Authentication Only (HMAC-SHA1)			
<input type="checkbox"/> AH - Authentication Only (HMAC-MD5)			
<hr/>			
IKE Encryption and Diffie-Hellman Group			
<input checked="" type="checkbox"/> 56-bit DES with Group 1 (768-bit prime)			
<input checked="" type="checkbox"/> Triple DES with Group 2 (1024-bit prime)			
<input checked="" type="checkbox"/> 128-bit AES with Group 5 (1536-bit prime)			
<hr/>			
Assignment of Client IP			
<input checked="" type="checkbox"/> Use Static Addresses (Configured in «WC»>>AUTH SERVER>>Local User Database)			
IP Address Pool		<input type="button" value="(None selected)"/> (Configure IP Address Pool)	
<hr/>			
<input type="checkbox"/> Enable Perfect Forward Secrecy			
<hr/>			
Rekey Timeout		<input type="text" value="08:00:00"/> (Range 00:02:00 - 23:59:59)	
Rekey Data Count		<input type="text" value="0"/> (Kbytes, minimum is 5 Kbytes, and 0 means disable)	
<hr/>			
<input type="button" value="Advanced"/>		<input type="button" value="Apply"/>	
		<input type="button" value="Reset"/>	

Figure 15 Business Element Manager — VPN client termination advanced configuration

NAT Traversal

☒ Enabled

☐ Disable Client IKE Source Port Switching

UDP Port

Router configuration for BCM50E 2

The integrated router on BCM50E 2 is configured with static NAT and PAT, as well as dynamic NAT and PAT. The firewall is disabled. Only IPSec BOT is used.

Static NAT and static PAT configuration

Traffic coming from the WAN side is translated and redirected to the customer LAN IP address of the BCM. This process is called static NAT, and is configured by setting the default SUA/NAT server the internal customer LAN IP address of the BCM50E. When a more specific SUA/NAT rule is configured, that rule takes priority over static NAT. The process by which more specific rules can redirect traffic to a server IP address on the LAN side, based on a port number or range of port numbers, is call static PAT.

Figure 16 Business Element Manager — static NAT and PAT configuration

SUA Server Addr Mapping Trigger Port

Default Server 192.168.1.2

#	Active	Name	Start Port	End Port	Server IP Address
1	<input checked="" type="checkbox"/>	ike	500	500	192.168.1.1
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0
*	<input type="checkbox"/>	RR-Reserv	1026	1026	192.168.1.1

Apply Reset

Dynamic NAT and dynamic PAT configuration:

Traffic generated on the LAN side and destined to the WAN side requires the use of dynamic PAT. This process allows applications on the private side to communicate with the public side and preserve stateful NAT or PAT sessions such that traffic returning from the public side is sent back to the device that initiated the communication on the private side. To enable dynamic PAT, set the Network Address Translation field to a value other than None.

Figure 17 Business Element Manager — dynamic NAT and PAT configuration

Route	WAN ISP	WAN IP	WAN MAC	Traffic Redirect	Dial Backup
WAN IP Address Assignment					
<input type="radio"/> Get automatically from ISP (Default) <input checked="" type="radio"/> Use fixed IP address					
My WAN IP Address			47.135.152.201		
My WAN IP Subnet Mask			255.255.255.0		
Gateway IP Address			47.135.152.1		
Network Address Translation			Full Feature ▾		
RIP Direction			None ▾		
RIP Version			RIP-1 ▾		
Multicast			None ▾		
Windows Networking (NetBIOS over TCP/IP)					
<input type="checkbox"/> Allow between WAN and LAN <input type="checkbox"/> Allow Trigger Dial					
			<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

Branch office tunnel configuration

A branch office tunnel (BOT) allows two branches to securely communicate over an encrypted IPSec tunnel. In this example, IKE is chosen as the key exchange protocol and the negotiation mode is set to Main.



Note: The selected negotiation mode (Main) must match at both ends of the branch offices otherwise the VPN tunnel cannot be established.

Figure 18 Business Element Manager — branch office tunnel configuration

☒ Active
 ☒ NAT Traversal

☒ Nailed Up

Name: TO_47_135_151_202

Key Management: IKE

Negotiation Mode: Main

Encapsulation Mode: Tunnel

Available IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Selected IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
<input checked="" type="radio"/> 1	N/A	192.168.1.0/ 255.255.255.0	192.168.0.0/ 255.255.255.0

Authentication Method

☒ Pre-Shared Key
 ☐ Certificate

Retype to Confirm:

Local ID Type: IP

 Content: 0.0.0.0

Peer ID Type: IP

 Content: 0.0.0.0

auto_generated_self_signed_cert (See [My Certificates](#))

My IP Address: 47.135.152.201

 Secure Gateway Address: 47.135.151.202

☒ ESP
 ☐ AH

Encryption Algorithm: DES

 Authentication Algorithm: SHA1

Authentication Algorithm: MD5

Router configuration for Secure Router 100x 1

Secure router 1 is configured with a firewall, static NAT and PAT, as well as dynamic NAT and PAT.

Firewall configuration

The secure router is configured to permit some traffic from the WAN side (ethernet 0) to the LAN (ethernet 1) and block any other type of traffic coming from the WAN. All traffic flowing from LAN to WAN is permitted.

The remote worker feature requires at a minimum the following rules:

- UNISim signaling: UDP ports 7000-7002
- RTP/RTCP media: UDP ports 30000-30099

Optional BCM applications and VoIP protocols require the following rules:

- Business Element Manager: TCP port 5989

- SSH: TCP port 22
- SIP: UDP port 5060
- HTTP: TCP port 80
- HTTPS: TCP port 443
- BCM Monitor: TCP port 60001

Optional telnet and ping support require the following rules:

- TELNET: TCP port 23
- ICMP (ping): protocol 1

Static NAT and static PAT configuration

Traffic coming from the WAN side is translated and redirected to the customer LAN IP address of the BCM. This process is called static NAT. When a PAT rule is configured, that rule takes priority over static NAT. PAT rules are used to redirect traffic to a server IP address other than the default NAT IP address on the LAN side based on a port number or range of port numbers.

Dynamic NAT and dynamic PAT configuration:

Traffic generated on the LAN side and destined to the WAN side requires the use of dynamic PAT. This process allows applications on the private side to communicate with the public side, and preserves stateful NAT or PAT sessions so that traffic returning from the public side is sent back to the device that initiated the communication on the private side.

Router configuration snapshot

The following code sample provides a view of the router configuration.

```
conf t
hostname avaya_bcm450
telnet_server
interface ethernet 0
ip address 47.135.151.204 255.255.254.0
nat
enable static
enable dynamic
no reverse
trans_addr 47.135.151.204
trans_mode overflow
address 192.168.0.20 47.135.151.204
port tcp 47.135.151.204 23 47.135.151.204 23
exit 2
interface ethernet 1
ip address 192.168.0.10 255.255.255.0
exit 2
ip route 0.0.0.0 0.0.0.0 47.135.150.1 1
```

```
ip access-list bcm_lan
add permit tcp any 47.135.151.204 dport =23
add permit tcp any 192.168.0.20 dport =22
add permit tcp any 192.168.0.20 dport =5989
add permit tcp any 192.168.0.20 dport =80
add permit tcp any 192.168.0.20 dport =443
add permit tcp any 192.168.0.20 dport =60001
add permit tcp any 192.168.0.20 dport =1222
add permit udp any 192.168.0.20 dport 7000-7002
add permit udp any 192.168.0.20 dport 30000-30099
add permit udp any 192.168.0.20 dport =5060
add permit icmp any 192.168.0.0/24
exit
access-group ethernet0 bcm_lan in
exit 2
```

Router configuration for Secure Router 100x 2

The secure router, in the context of a remote worker, needs to enable dynamic NAT and PAT. The firewall is optional, and is disabled in this setup. No VPN configuration is required to allow VPN client termination. Telnet is enabled for management purposes.

The following code sample provides a view of the router configuration.

```
conf t
hostname avaya_remote
telnet_server
interface ethernet 0
ip address 47.135.150.65 255.255.254.0
nat
enable static
enable dynamic
no reverse
trans_addr 47.135.150.65
trans_mode overflow
exit 2
interface ethernet 1
ip address 192.168.2.1 255.255.255.0
exit 2
ip route 0.0.0.0 0.0.0.0 47.135.150.1 1
exit
```