>BUSINESS MADE **SIMPLE**

NORTEL

Nortel BCM50e
Nortel BSR222
Engineering

> BCM50e-BSR222 Secure Voice & Data for Small Businesses Teleworking Solution Technical Configuration Guide

Enterprise Solutions Engineering
Document Date: July, 2007
Document Number : NN48500-508
Document Version: 1.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. Nortel Networks, the Nortel Networks logo and the Globemark are trademarks of Nortel Networks.

Abstract

This document is a Technical Configuration Guide for “BCM50e-BSR222 Secure Voice and Data and Teleworking Solution for Small Businesses”. It describes the solution, the benefits, the major components, the Internet access requirement, and the network reference model. It also provides a lab-proven example with step-by-step configurations for a multi-sites deployment. The information provided can be used as technical reference by engineers.

Table of Contents

List of Figures

1. Introduction

This document is a Technical Configuration Guide for “BCM50e-BSR222 Secure Voice & Data and Teleworking Solution for Small Businesses. It describes the solution, the benefits, the major components, the Internet access requirement, and the network reference model. It also provides a lab-proven example with step-by-step configurations for a multi-sites deployment. The information provided can be used as technical reference by engineers.

2. BCM50-BSR222 Secure Voice & Data Solution for Small Businesses

2.1 Business Drivers

According to a recent market survey to more than 1,000 small and medium businesses, the top three technologies that SMBs surveyed find most important are network security, data networking and voice/telephony systems. The key reasons SMBs purchase business communication solutions are to increase/improve communication and performance. Many SMBs purchase technologies to primarily improve their customer service and enhance their employee productivity. Other benefits SMBs expect include becoming more cost-effective, being able to act and react quickly and being able to be connected from anywhere.

2.2 Solution Reference Model

The reference topology is validated and its configuration steps are documented in this guide. Sales can flexibly tailor or expand the solution for their SMB customers.

This solution targets small businesses with:

- 3-30 employees
- in single or multi-sites, typically local or regional
- small budget, but want to look big
- no IT personnel
- require secure connections between branch offices, business partners and remote users for protecting the integrity and security of business information
- Teleworking and mobile employees

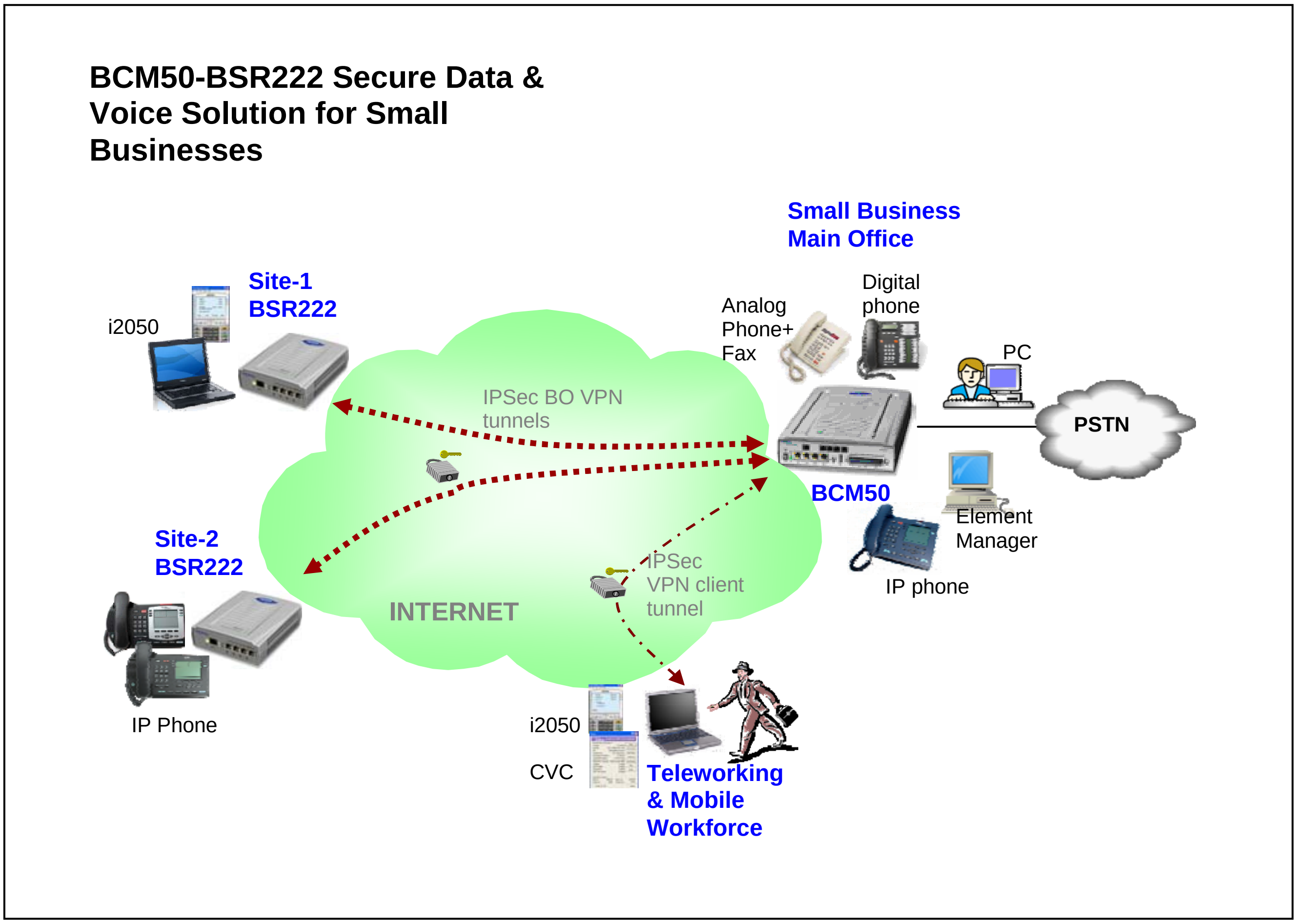


Figure 1 Solution Reference Model

2.3 Solution Reference Model Description

In this solution model, the small business has one Main-office and several temporary or permanent remote sites, and several mobile or teleworkers. A virtual private network between sites is built over the open public internet. Voice and data are securely transferred and protected by the VPN.

One Main-office:

- In the main-office, one BCM50 Platform is deployed to provide centralized converged voice and data services at the infrastructure, management and application levels.
- Up to 4 analog trunks are connected to PSTN for external PSTN calls.
- A mix of several IP phones, digital phones, and traditional analog phones/fax are used for voice communication.
- One PC is configured with BCM Element Manager for managing, monitoring and configuring the small network.
- Several PCs are used for the daily needs of employees, such as internet access, emails, file sharing, etc.

- A private virtual Intranet across the open public Internet is established for inter-office voice, data, emails, file sharing among locations via the secured full mesh of VPN tunnels.
- The BCM50 is configured to terminate IPSec VPN client tunnels for mobile teleworkers.

Several remote sites:

- Each remote site has one Business Secure Router BSR222 configured to create IPSec VPN branch tunnels for inter-office secure connection among locations. This could actually be a BSR222 deployed to provide secure access for a full-time work-at-home employee.
- VPN tunnels are terminated on the BCM50 to build a private intranet over the public Internet for employees to share information, file transfer, voice services, etc.
- One or more IP phones or IP Softphone 2050 installed on PCs are used for inter-office voice services.
- One or more PCs used for the daily needs of the employees.

Several mobile Teleworkers:

- Each mobile teleworker has one laptop configured with Nortel VPN Client software for IPSec VPN client connection terminated on the BCM50 in the Main-office.
- One IP Softphone 2050 installed on the laptop is used for inter-office voice services.
- The same laptop is used for the daily needs of the employee.

Solution Capacity:

With The BCM50e, the solution basic model supports:

• Target Number of Users	3-30
• Number of digital stations	44
• Number of IP stations	32
• Number of voice mail ports	10
• Support IP/digital mobility	Yes
• Support Cordless mobility	Yes
• Support Intelligent Contact Center	Yes
• Support IP music on hold	Yes
• VPN tunnels (BO + Client)	Up to 10
• Ad Hoc Conferencing	Up to 18 participants, in one or more conferences
• Analog trunk	up to 4 or more with Media Bay Modules (MBMs)
• Analog phone	up to 4 or more with MBMs
• Secure Voice between sites	
• Secure Data between sites	
• Secure voice/data between mobile worker and Main-office	

2.4 Solution Benefits

This solution of “BCM50e-BSR222 Secure Data, Voice & Teleworking for Small Businesses” increases a small business’s profitability and productivity in many ways:

- **Reduce costs:**

  High toll charges for inter-office calls among locations for voice and fax calls can be reduced or eliminated, and traditional telephone PSTN lines can be relegated to back-up status.

- **Streamline the network architecture:**

  Deliver advanced voice and data over an easy-to-manage IP network, and converge disparate voice and data networks into a single infrastructure that can carry both types of traffic and save as much as 50 percent in capital and operating costs.

- **Make services portable and flexible:**

  Moves, adds and changes become almost seamless, and services can easily be extended to remote sites, home offices and mobile employees over cost-effective Internet.

- **Bring new value to voice applications:**

  The convergence of voice and data enables powerful new capabilities such as unified messaging, Web enabled multimedia call centers and PC-based call management.

- **To securely connect multiple sites over the Internet:**

  Nortel BCM50 and BSR222 create virtual private networks that travel across the open Internet yet preserve the integrity and confidentiality of communications. Small business can set up an intranet so employees can share information, an extranet to share information with partners and suppliers, and Web access to interact with customers.

- **Protect the confidentiality of data in transit:**

  Through encryption, authentication, confidentiality, data integrity, anti-replay protection and protection against traffic flow analysis.

- **Extend secure access to mobile users and telecommuters:**

  With a security “client” on their laptops, remote mobile users can securely connect to the company Main-office from anywhere for voice and data applications.

2.5 Internet Access

- Internet access with high speed
- ISPs of Cable modem, DSL, Fiber Optic (Note: Satellite services are not currently recommended as they do not offer the quality required by VOIP services).
- Modems are provided by ISPs
- One static IP address from ISP is required for the WAN interface of the BCM50e located in the central Main-office
- One dynamic IP address from ISP is required for the WAN interface of the BSR222 located in any site
- One dynamic IP address from ISP is required for the laptop of the road warrior in anywhere

2.6 Bandwidth Management

The BSR222 and the BCM50 support Bandwidth Management (BWM). With BWM, you can allocate an interface's outgoing capacity to specific types of traffic, and you can also forwards certain types of traffic with minimum delay.

Bandwidth management allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024kbps if the broadband device connected to the WAN port has an upstream speed of 1024kbps.

You can also use BWM to classify applications and to allocate specific amounts of bandwidth capacity to each class or sub-class. The actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth from ISP.

For more information about bandwidth management, refer to the NTP of "BSR222 configuration basic".

3. Configuration Example

This example describes LAB configuration steps of the “BCM50e-BSR222 Secure Voice, Data & Teleworking Solution” for a small business with one Main-office and two remote sites and a mobile employee. The configuration was successfully tested in lab environment.

3.1 Lab Topology

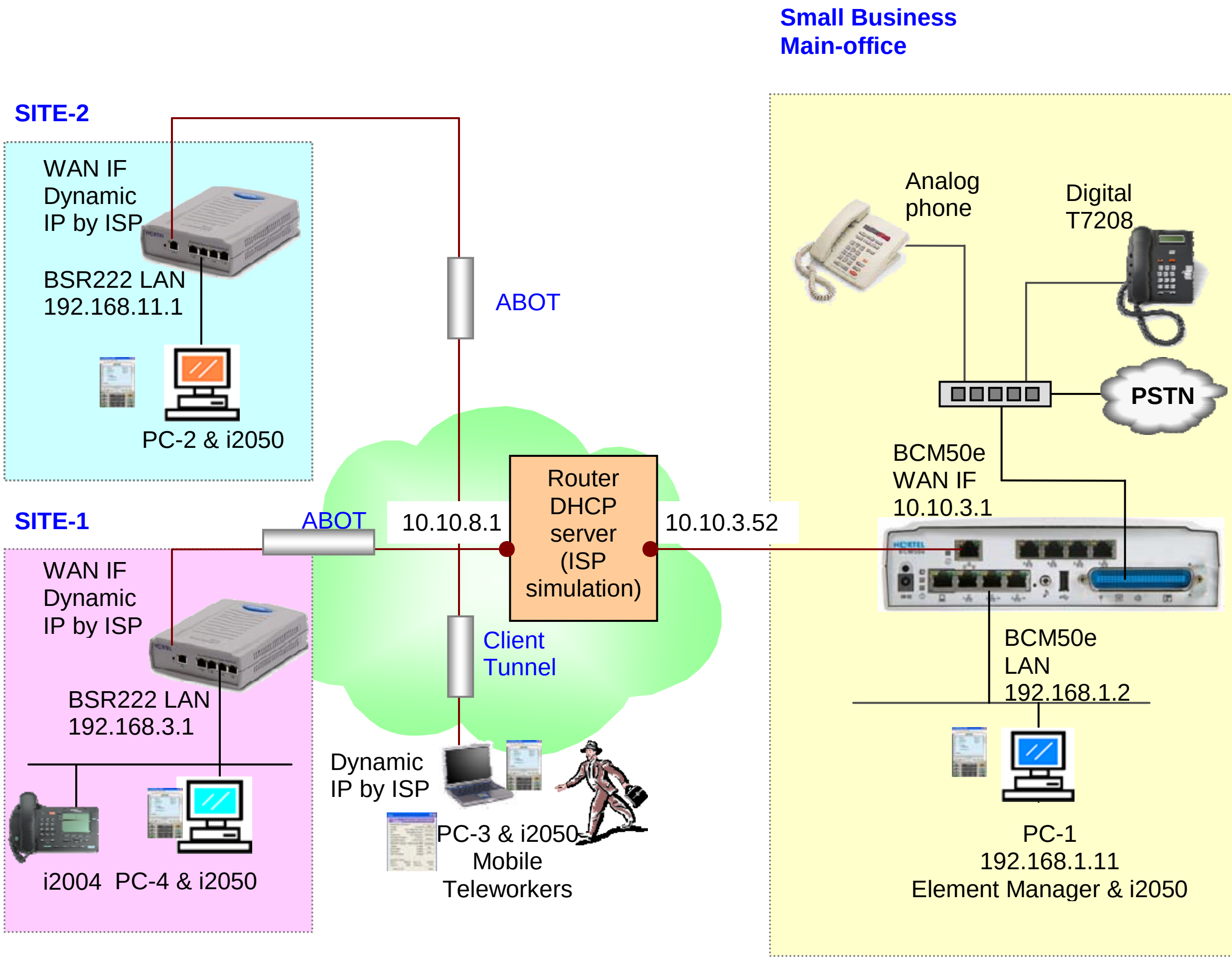


Figure 2 Diagram of LAB Topology

3.1.1 VPN Requirement

This solution uses a hub-spike topology to establish VPN tunnels between sites and the Main-office (HUB) as show on above diagram:

- An Asymmetrical Branch Office Tunnel (ABOT) between the Main-office and Site-1
- An ABOT between the Main-office and Site-2
- An IPSec VPN Client tunnel between the Main-office and the laptop of a teleworker.

3.1.2 Hardware and Software Used

Internet ISP simulation

- A router with the capability of DHCP server is used to simulate an Internet ISP. Two networks are configured on the router: 10.10.3.0/24 and 10.10.8.0/24. The DHCP server is configured with an IP address pool of 10.10.8.0.

Main-office

- One BCM50e R2 hardware with rls2 software
- The BCM50e integrated router is installed with VBCM222_2.6.0.0.005
- One PC (PC-1) loaded with OS of WinXP SP-1, IE6.0 and BCM Element Manager
- One IP Softphone 2050 is installed on the same PC
- The PC is connected to one of the BCM50e LAN ports
- The BCM50e WAN interface configured with a static IP address (10.10.3.1) is connected to the router on the network of 10.10.3.0/24
- One analog phones (any type)
- One digital phone of T7208

Site-1

- One BSR222 loaded with VBSR222_2.6.0.0.003
- One PC (PC-4) connecting to any of the 4 LAN ports on BSR222
- The PC is installed with WinXP, and IP Softphone 2050 V2
- The BSR222 WAN interface configured with a dynamic IP address is connected to the router on the network of 10.10.8.0/24. The WAN IP address is dynamically assigned by the ISP DHCP server
- One IP Phone 2004 connected to any of the 4 LAN ports on BSR222

Site-2

- One BSR222 loaded with VBSR222_2.6.0.0.003
- One PC (PC-4) connecting to any of the 4 LAN ports on BSR222
- The PC is installed with WinXP, and IP Softphone 2050 V2
- The BSR222 WAN interface configured with a dynamic IP address is connected to the router on the network of 10.10.8.0/24. The WAN IP address is dynamically assigned by the ISP DHCP server.

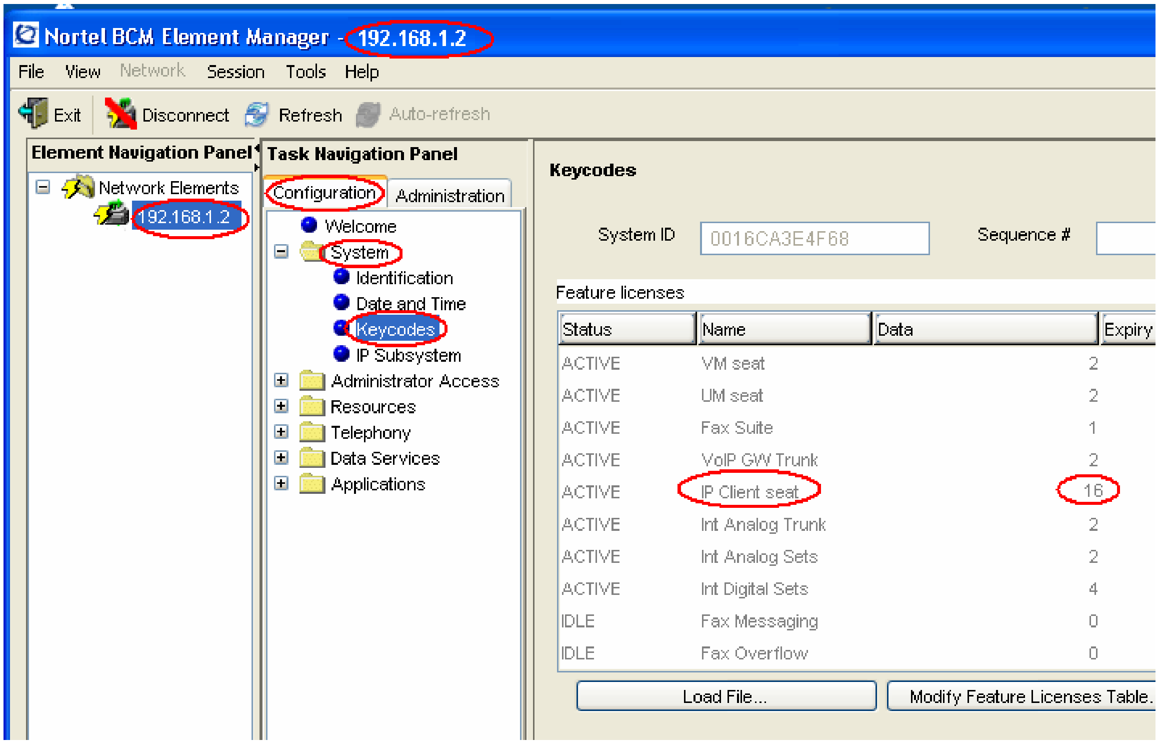
Mobile Teleworker

- One PC NIC interface with dynamic IP address is connected to the router on the network of 10.10.8.0/24. Its IP address is dynamically assigned by the ISP DHCP server.
- The laptop (PC-3) is configured with a dynamic IP address and connected to the router on the network of 10.10.8.0/24. Its IP address is dynamically assigned by the ISP DHCP server.
- The laptop (PC-3) is installed with WinXP, and IP Softphone 2050 V2
- A Mobile USB Headset Adapter (optional) is used for IP Softphones
- The PC is installed with Nortel VPN Client software (V06)

3.2 Main-Office BCM50e Configuration

3.2.1 Keycode Installation

- This lab test requires a keycode of “P Clients” with minimum of 5 seats.
- Assuming you have purchased and retrieved your keycode file from the Keycode Retrieval System (KRS) at: http://www.nortel.com/servsup/krs.
- To load the keycode file, use the BCM Element Manager
- Log on to the BCM Element Manager and select the BCM50 of “192.168.1.2”. (Note: the IP address of “192.168.1.2” is the default IP address of BCM50 Call Server, and it has the default ID of “nnadmin” and default Password of “PlsChgMe!”).
- On the Task Navigation Panel, select the Configuration tab and the configuration folders appear.
- Select the System folder and click the Keycodes task, and the Keycodes panel appears.
- Click Load File, and the Open file dialog box appears.
- Browse to the keycodes file downloaded from KRS, then click Open.
- The file uploads and the feature appears in the Keycodes list as shown in the following screen shot.
- For more information about keycode installation, please refer to the NTP of “BCM Keycode Installation Guide”, Version 02.01, and Part Code N0060604



Keycodes

System ID 0016CA3E4F68 Sequence #

Feature licenses

Status	Name	Data	Expiry
ACTIVE	VM seat	2	
ACTIVE	UM seat	2	
ACTIVE	Fax Suite	1	
ACTIVE	VoIP GW Trunk	2	
ACTIVE	IP Client seat	16	
ACTIVE	Int Analog Trunk	2	
ACTIVE	Int Analog Sets	2	
ACTIVE	Int Digital Sets	4	
IDLE	Fax Messaging	0	
IDLE	Fax Overflow	0	

3.2.2 Configure BCM50e IP Phone Registration

3.2.2.1 Determining IP Phone Registration Process

The Nortel IP telephones must register with the BCM50 system to be able to use the call features and system features. The IP phone registration process is set up using the BCM Element Manager.

Ensure that you have loaded the appropriate keycodes to activate the Nortel IP telephones on your BCM50 system before this process.

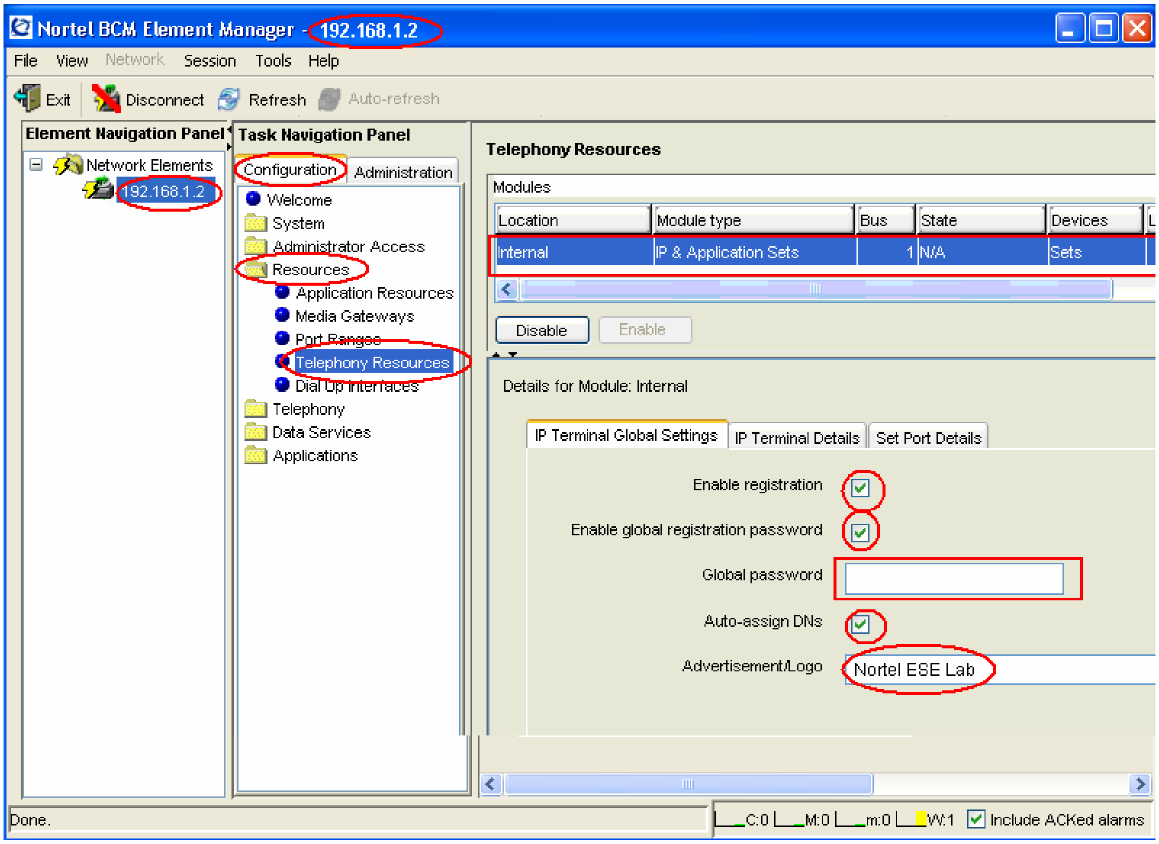
Go to the BCM Element Manager, under Resources > Telephony Resources > IP Terminal Global Settings tab, and on the Global Settings panel:

- Select the Enable registration check box.
- If you want the installers to use a single password to configure and register the telephone, select the Enable global registration password check box, and then enter a numeric password in the Global password field.
- If you want the system to automatically assign DN records to the telephones, select the Auto-assign DNs check box.

3.2.2.2 Configure IP Phone for Automatically Assigned DN

For simplification, in this lab example, we chose to use the procedure of “automatically configure IP Phones with DNs assigned”. This procedure can be found in Nortel NTP of “Telephony Device Installation Guide”, Chapter 7. Document Number: NN40020-309

- In the page of Configuration ->Resources->Telephone Resources
- Select the Enable registration check box
- Select the Enable global registration password check box
- Leave Global password field blank
- Select the Auto-assign DNs check box



Telephony Resources

Modules

Location	Module type	Bus	State	Devices
Internal	IP & Application Sets	1	N/A	Sets

Details for Module: Internal

Enable registration ☑

Enable global registration password ☑

Global password

Auto-assign DNs ☑

Advertisement/Logo Nortel ESE Lab

3.2.2.3 Security Warning

In the real world deployment, Nortel recommends you turn “Enable registration” and “Auto-assign DNs” off when the telephones are registered. Nortel cautions that leaving your IP registration open and unprotected by a password can pose a security risk.

3.2.3 Configure BCM50e WAN and LAN

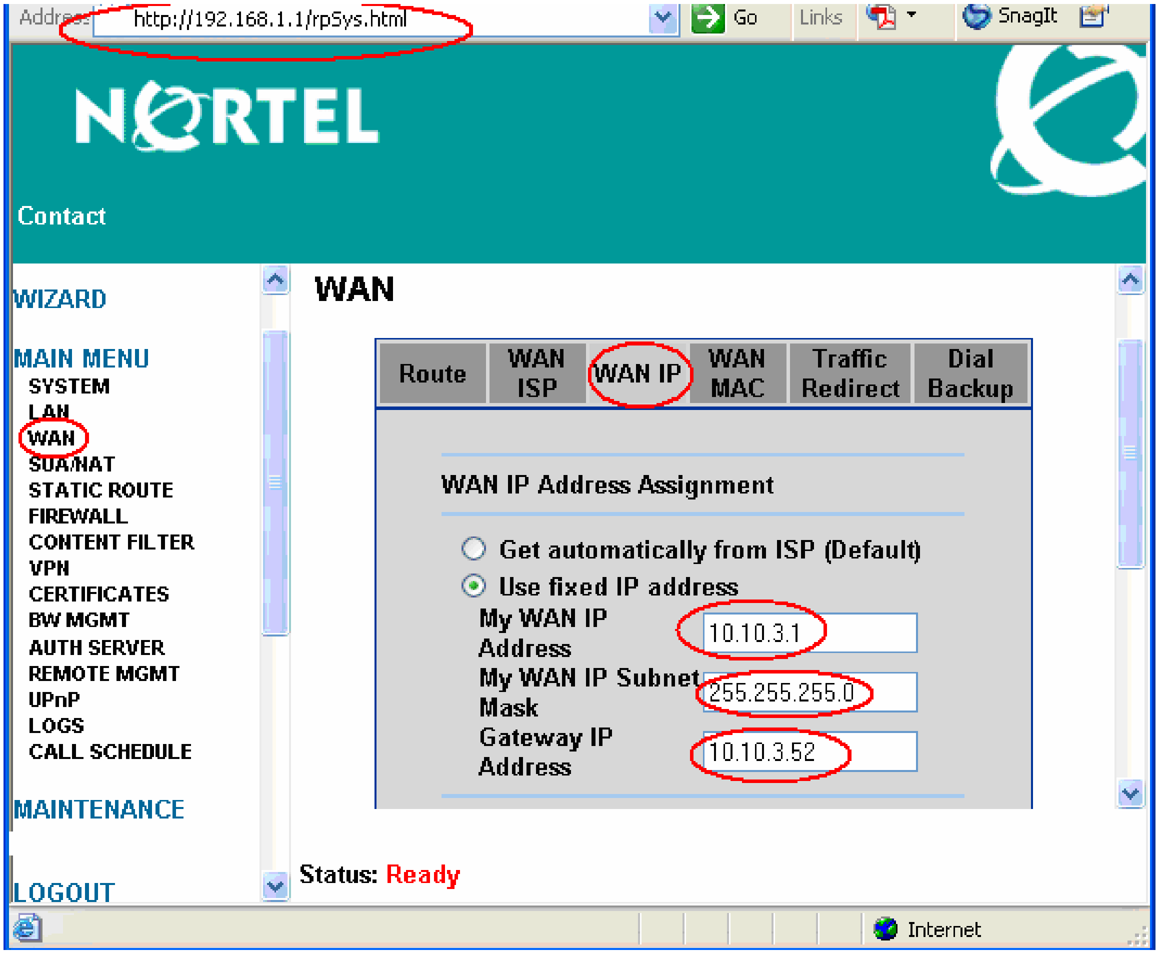
In this section, we will configure WAN IP and LAN IP on the BCM50e Integrated Router.

3.2.3.1 Configure Fixed WAN IP Address

The static WAN IP address should be obtained from your ISP in real life. In this lab example, the static IP of “10.10.3.1/24” is used for the WAN interface on the BCM50e Integrated Router.

Launch a web browser and type "http://192.168.1.1" to open the BCM50 router’s GUI interface. Click WAN ISP tab under WAN menu. Fill in the IP addresses as show in the following window.

Note: The “Gateway IP Address” 10.10.3.52/24 is the IP address of ISP router. (See the “Diagram of Lab Topology”).



WAN IP Address Assignment

○ Get automatically from ISP (Default)

● Use fixed IP address

My WAN IP Address: 10.10.3.1

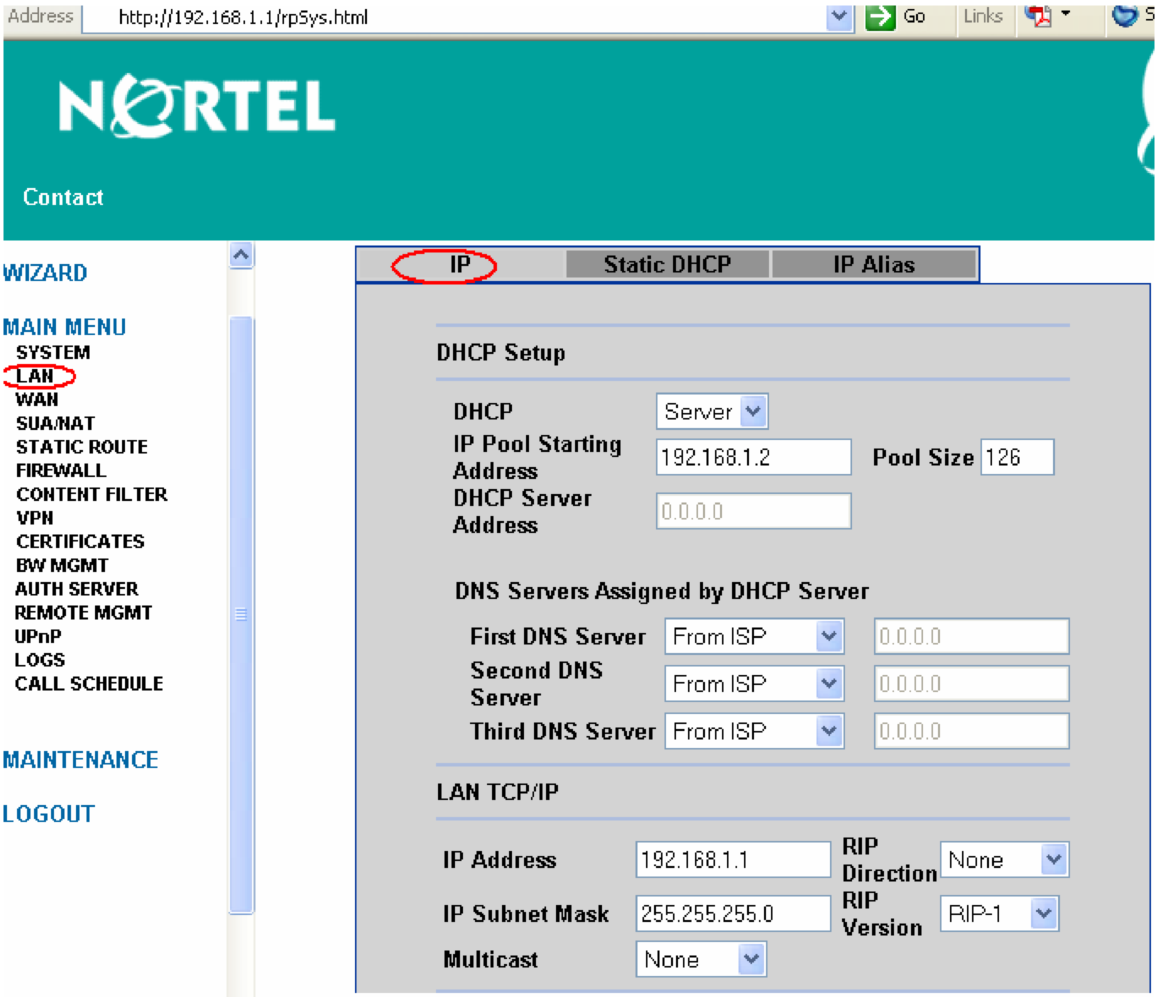
My WAN IP Subnet Mask: 255.255.255.0

Gateway IP Address: 10.10.3.52

Status: Ready

3.2.3.2 Configure LAN

By default, the BCM50e LAN is configured with an IP address of 192.168.1.1/24, and a DHCP server with an IP Pool starting from 192.168.1.2 (Note: the IP address of “192.168.1.2” is automatically assigned to the BCM50 Call Server interface). You can make changes to suit the needs of your network. In this lab example, we keep the factory default settings for the BCM50 LAN and DHCP IP Pool. See the following window.



http://192.168.1.1/rpSys.html

DHCP Setup

DHCP: Server
IP Pool Starting Address: 192.168.1.2 Pool Size: 126
DHCP Server Address: 0.0.0.0

DNS Servers Assigned by DHCP Server

First DNS Server: From ISP 0.0.0.0
Second DNS Server: From ISP 0.0.0.0
Third DNS Server: From ISP 0.0.0.0

LAN TCP/IP

IP Address: 192.168.1.1 RIP Direction: None
IP Subnet Mask: 255.255.255.0 RIP Version: RIP-1
Multicast: None

3.2.4 Configure BCM50e ABOT

In this section, we will configure the BCM50e Integrated Router to support:

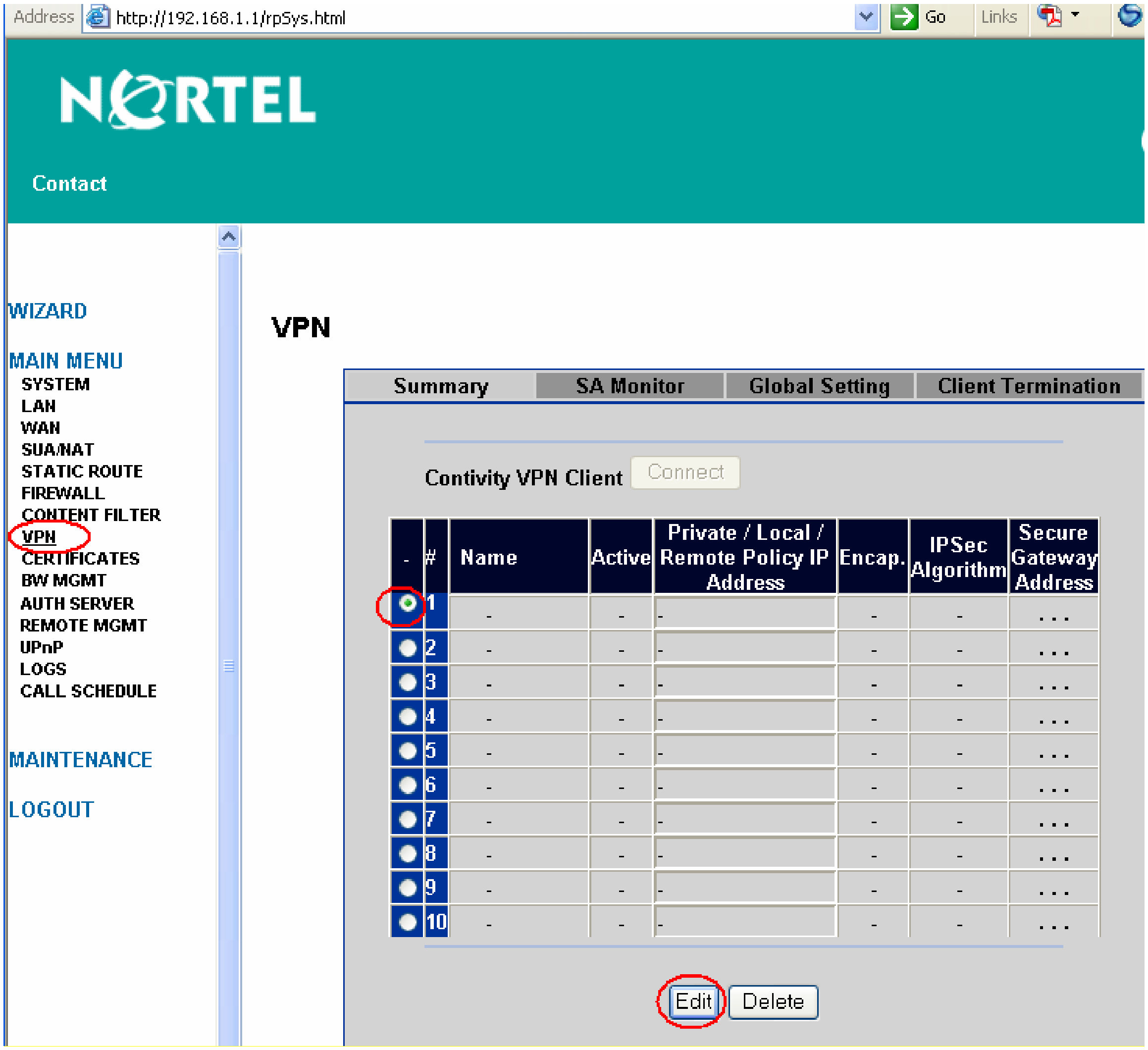
- ABOT termination from various remote sites
- Nortel VPN Client Termination from road warriors

If you need more information about configuring BCM50e integrated router, please refer to Nortel NTP of “BCM50e Integrated Router Configuration”, Document Number: N0115788.

3.2.4.1 Create a New Rule

Click VPN to open the Summary screen. This is a read-only menu of the IPSec rules (tunnels). Create an IPSec rule by selecting an index number and then clicking Edit to configure the associated submenus.

- In VPN -> Summary window, select #1 (unused) rule.
- Click “Edit” button.



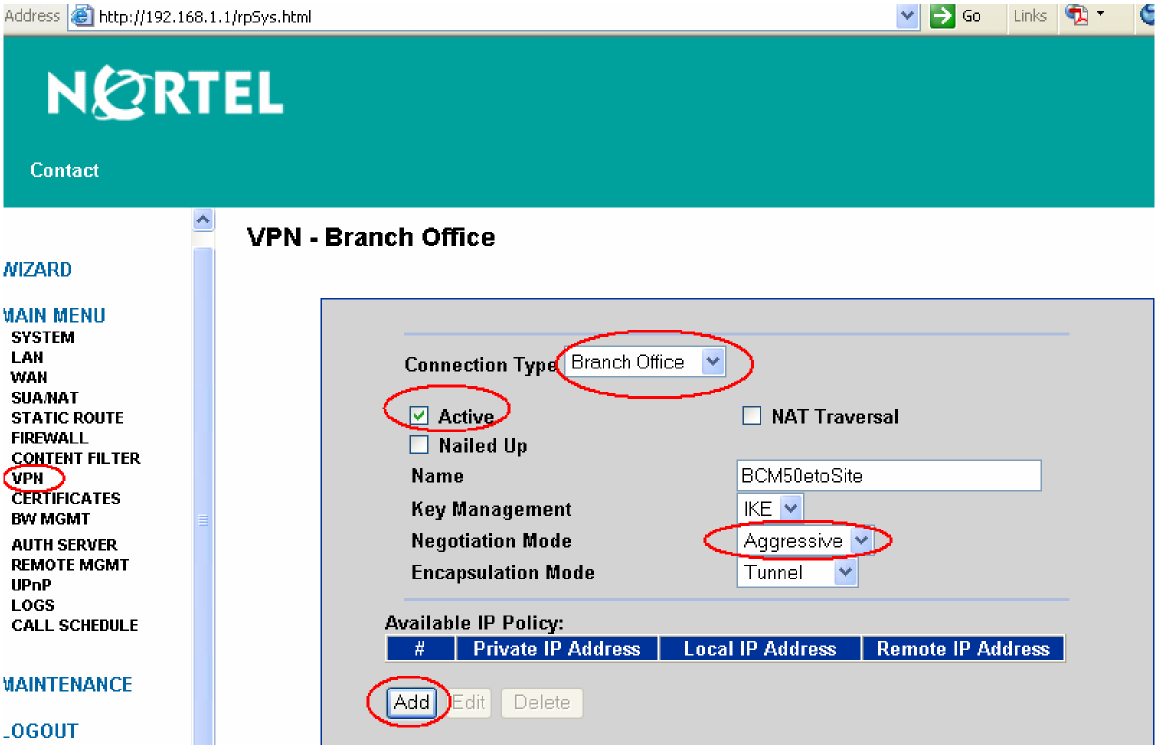
Contivity VPN Client

-	#	Name	Active	Private / Local / Remote Policy IP Address	Encap.	IPSec Algorithm	Secure Gateway Address
◉	1	-	-	-	-	-	...
○	2	-	-	-	-	-	...
○	3	-	-	-	-	-	...
○	4	-	-	-	-	-	...
○	5	-	-	-	-	-	...
○	6	-	-	-	-	-	...
○	7	-	-	-	-	-	...
○	8	-	-	-	-	-	...
○	9	-	-	-	-	-	...
○	10	-	-	-	-	-	...

3.2.4.2 Configure ABOT VPN Tunnel

The "VPN Branch Office" window is opened:

- Check "Active", and select "Branch Office" tunnel
- Name it as "BCM50etoSite"
- Select negotiation mode as "Aggressive"
- See the following screenshot
- Click "Add" button for the next step



VPN - Branch Office

Connection Type: Branch Office

☑ Active

□ NAT Traversal

□ Nailed Up

Name	BCM50etoSite
Key Management	IKE
Negotiation Mode	Aggressive
Encapsulation Mode	Tunnel

Available IP Policy:

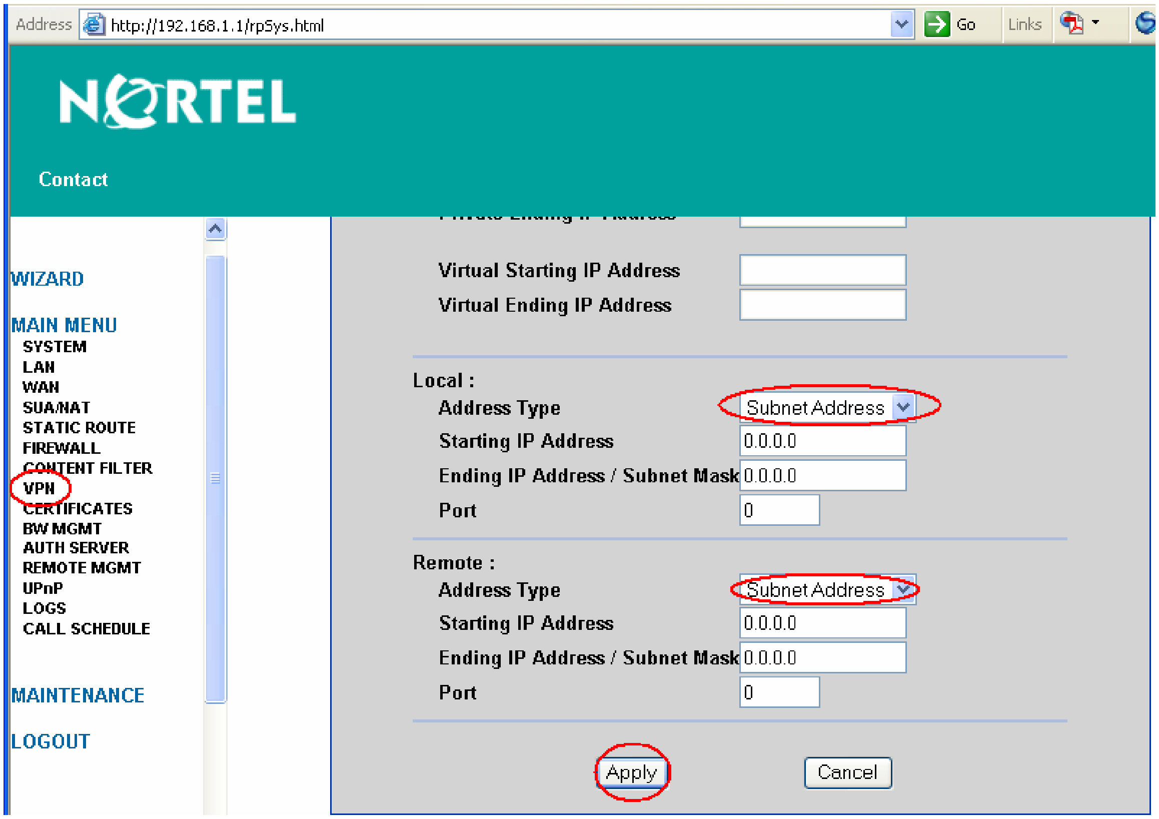
#	Private IP Address	Local IP Address	Remote IP Address

3.2.5 VPN - Branch Office - IP Policy

After click “Add” button, the window of “IP Policy” is opened as shown in the following screen.

In order to allow the BCM50e router to act as a VPN hub and to terminate ABOT tunnels from any branches, a dynamic policy is created.

The dynamic policy use “0.0.0.0” as starting address for both local and remote, see the following screen:



http://192.168.1.1/rpSys.html

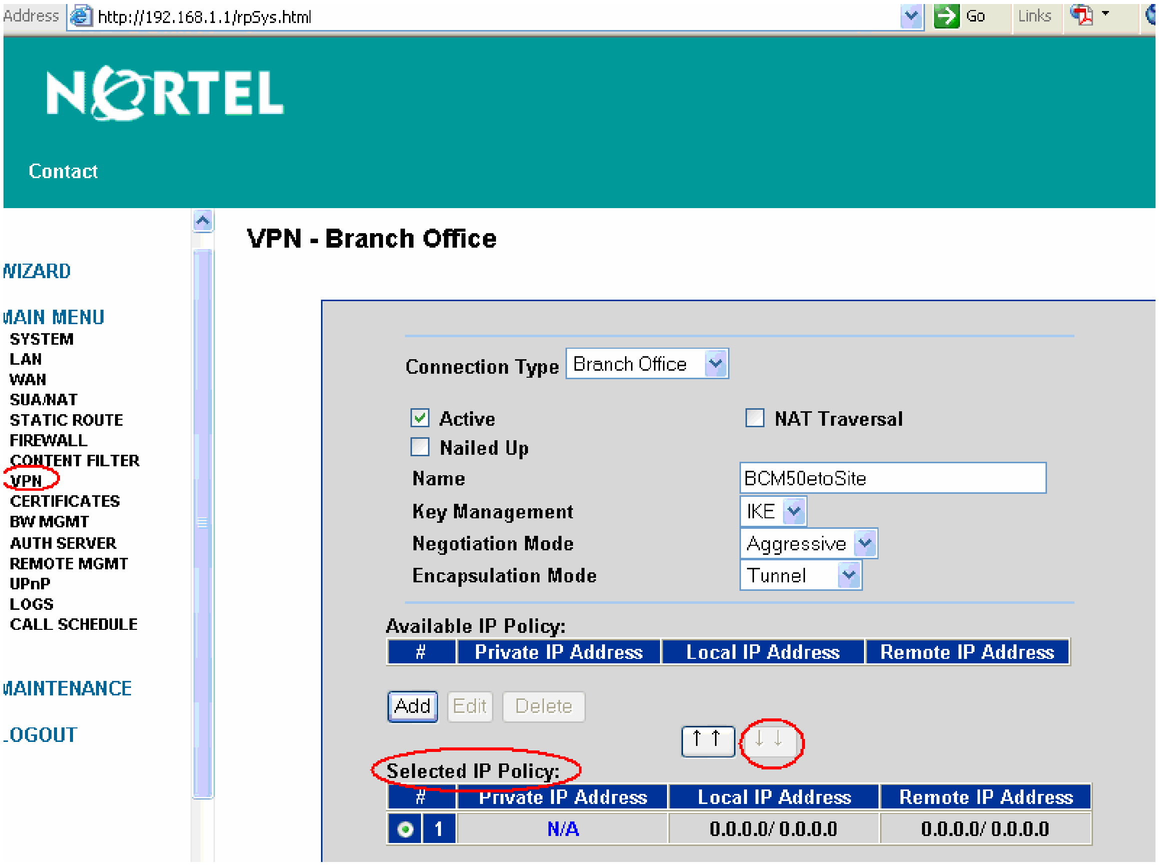
Virtual Starting IP Address
Virtual Ending IP Address

Local :
Address Type: Subnet Address
Starting IP Address: 0.0.0.0
Ending IP Address / Subnet Mask: 0.0.0.0
Port: 0

Remote :
Address Type: Subnet Address
Starting IP Address: 0.0.0.0
Ending IP Address / Subnet Mask: 0.0.0.0
Port: 0

3.2.5.1 Selected IP Policy

The newly created dynamic policy is not applied until it is selected. Use double-arrow button to select the newly created IP policy. See the following screen of "Selected IP Policy".



VPN - Branch Office

Connection Type: Branch Office

☑ Active

□ NAT Traversal

□ Nailed Up

Name: BCM50etoSite

Key Management: IKE

Negotiation Mode: Aggressive

Encapsulation Mode: Tunnel

Available IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address

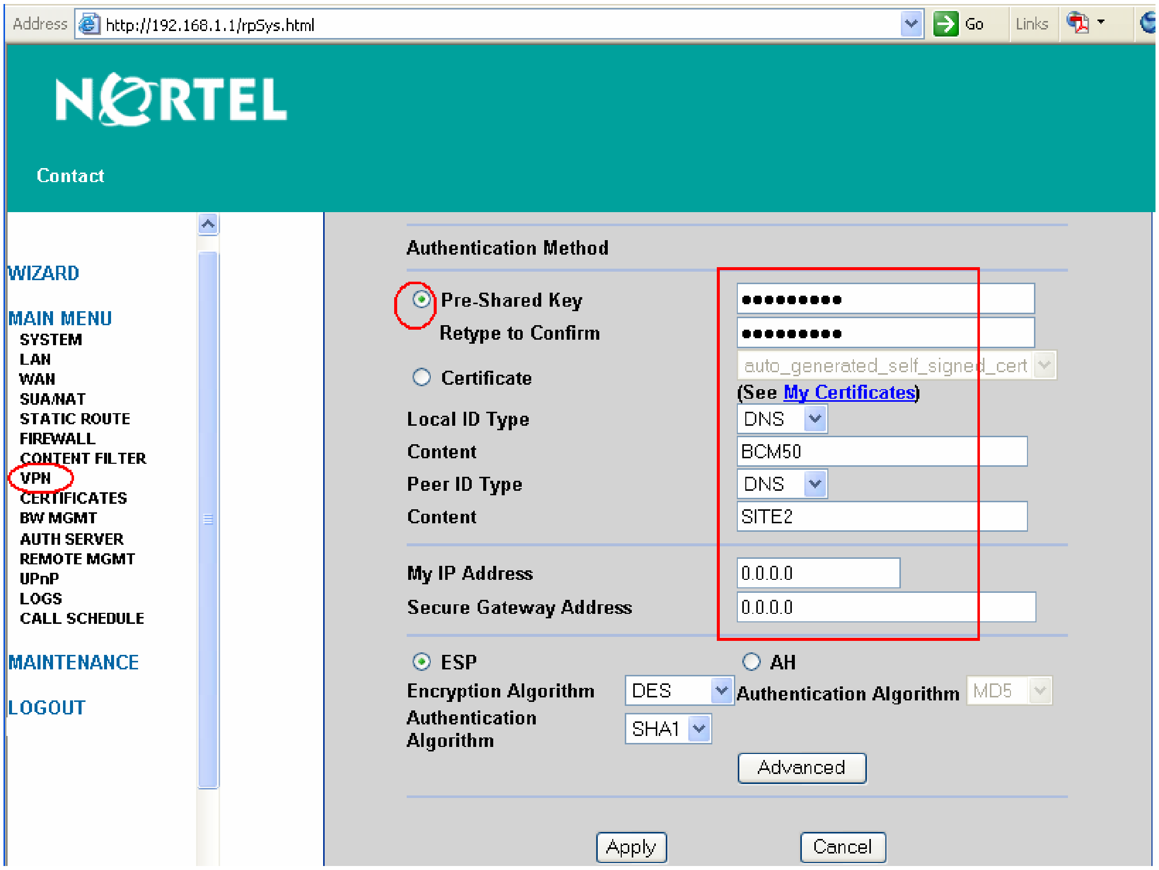
Selected IP Policy:

	#	Private IP Address	Local IP Address	Remote IP Address
●	1	N/A	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0

3.2.5.2 ABOT IP Address and Authentication

We continue to configure the “BCM50etoSite” with the following steps:

- Enter the authentication information with a pre-shared key of “contivity” (for use in our example).
- Select “DNS” as “Local ID Type” and enter “BCM50” (or as desired) as “Content”. Note: The domain name (up to 31 characters) in the Content field is used for identification purposes only and does not need to be a real domain name, and what is assigned here must also be used in the ABOT authentications in Sections of 3.3.2.4 and 3.4.2.4.
- Select “DNS” as “Remote ID Type” and enter “SITE” (or as desired) as “Content” (Note: what is assigned here must also be used in the ABOT authentications in Sections of 3.3.2.4 and 3.4.2.4.)
- Enter “0.0.0.0” in the field of “My IP Address” and this will cause the BCM50 router to use WAN IP address 10.10.3.1 as “My IP address”.
- Enter “0.0.0.0” as the Secure Gateway Address”, since the remote VPN router has a dynamic WAN IP address in ABOT architecture, and the SA is initiated by a remote VPN switch or teleworker.
- Select the default encryption and authentication algorithms.
- Click “Apply” to save and apply the ABOT configuration.
- See the following screen.



http://192.168.1.1/rpSys.html

Authentication Method

● Pre-Shared Key: ●●●●●●●●●
Retype to Confirm: ●●●●●●●●●

○ Certificate: auto_generated_self_signed_cert
(See My Certificates)

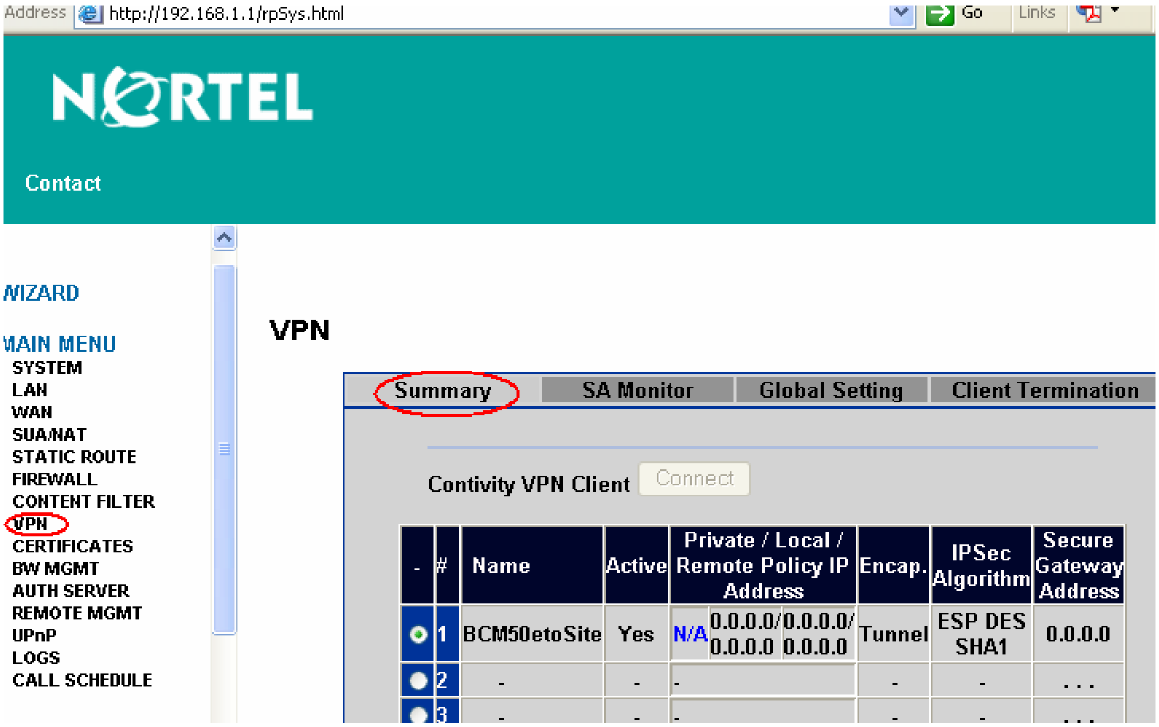
Local ID Type: DNS
Content: BCM50
Peer ID Type: DNS
Content: SITE2

My IP Address: 0.0.0.0
Secure Gateway Address: 0.0.0.0

● ESP ○ AH
Encryption Algorithm: DES
Authentication Algorithm: SHA1
Authentication Algorithm: MD5

3.2.5.3 VPN Summary

After “Apply”, the VPN should have a summary as shown in the following screen:



VPN

Contivity VPN Client

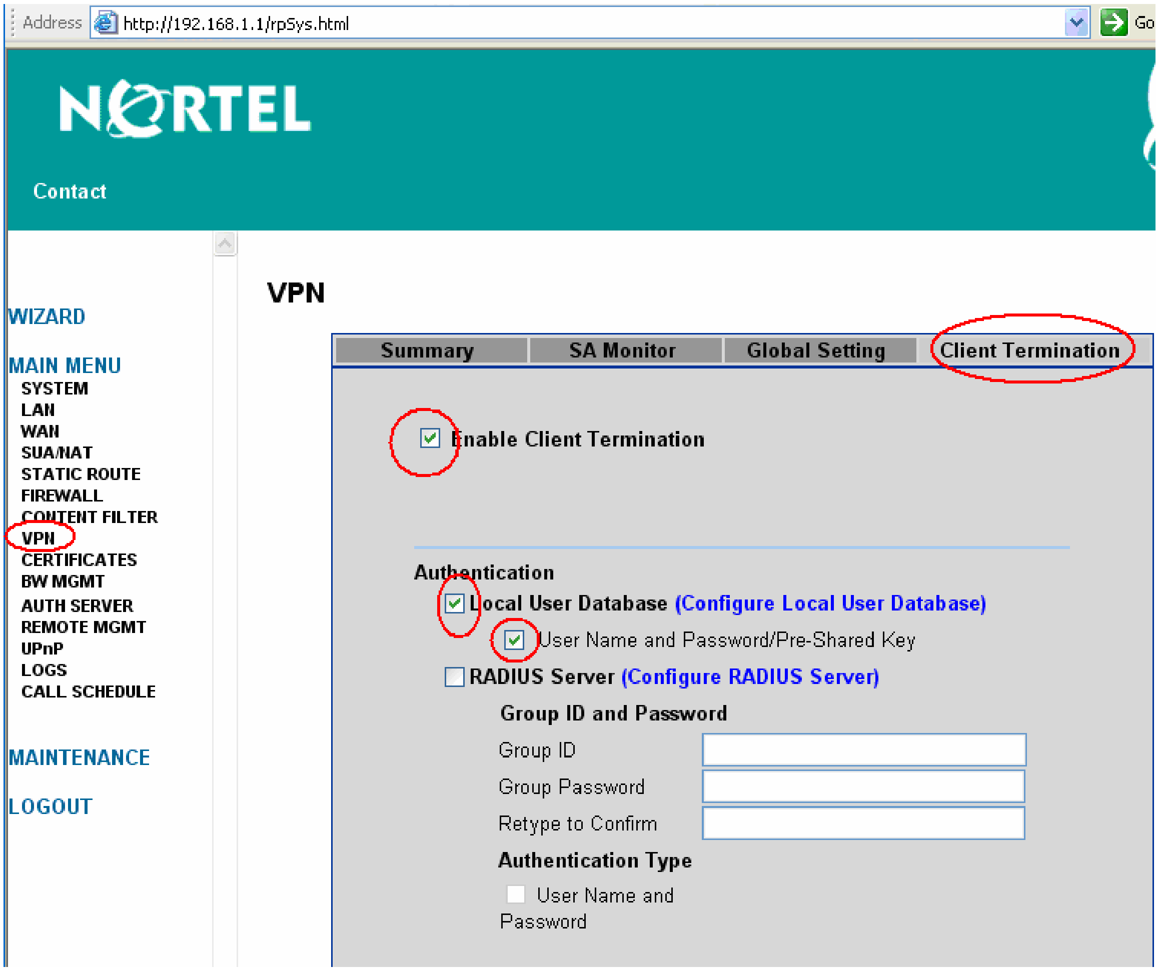
-	#	Name	Active	Private / Local / Remote Policy IP Address			Encap.	IPSec Algorithm	Secure Gateway Address
●	1	BCM50etoSite	Yes	N/A	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0
○	2	-	-	-			-	-	. . .
○	3	-	-	-			-	-	. . .

3.2.6 Configure BCM50e VPN Client Termination

The BCM50e R2 supports both Branch Office termination and VPN Client termination. In this section, we will configure the BCM50e to terminate Nortel VPN Clients from the road warriors' laptops.

3.2.6.1 Enable Client Termination

- Go to VPN, check "Client Termination" button to enable Client Termination.
- In this example, we check/use "local User Database", and "user and password" for authentication.



VPN

☑ Enable Client Termination

Authentication

☑ Local User Database (Configure Local User Database)

☑ User Name and Password/Pre-Shared Key

□ RADIUS Server (Configure RADIUS Server)

Group ID and Password

Group ID

Group Password

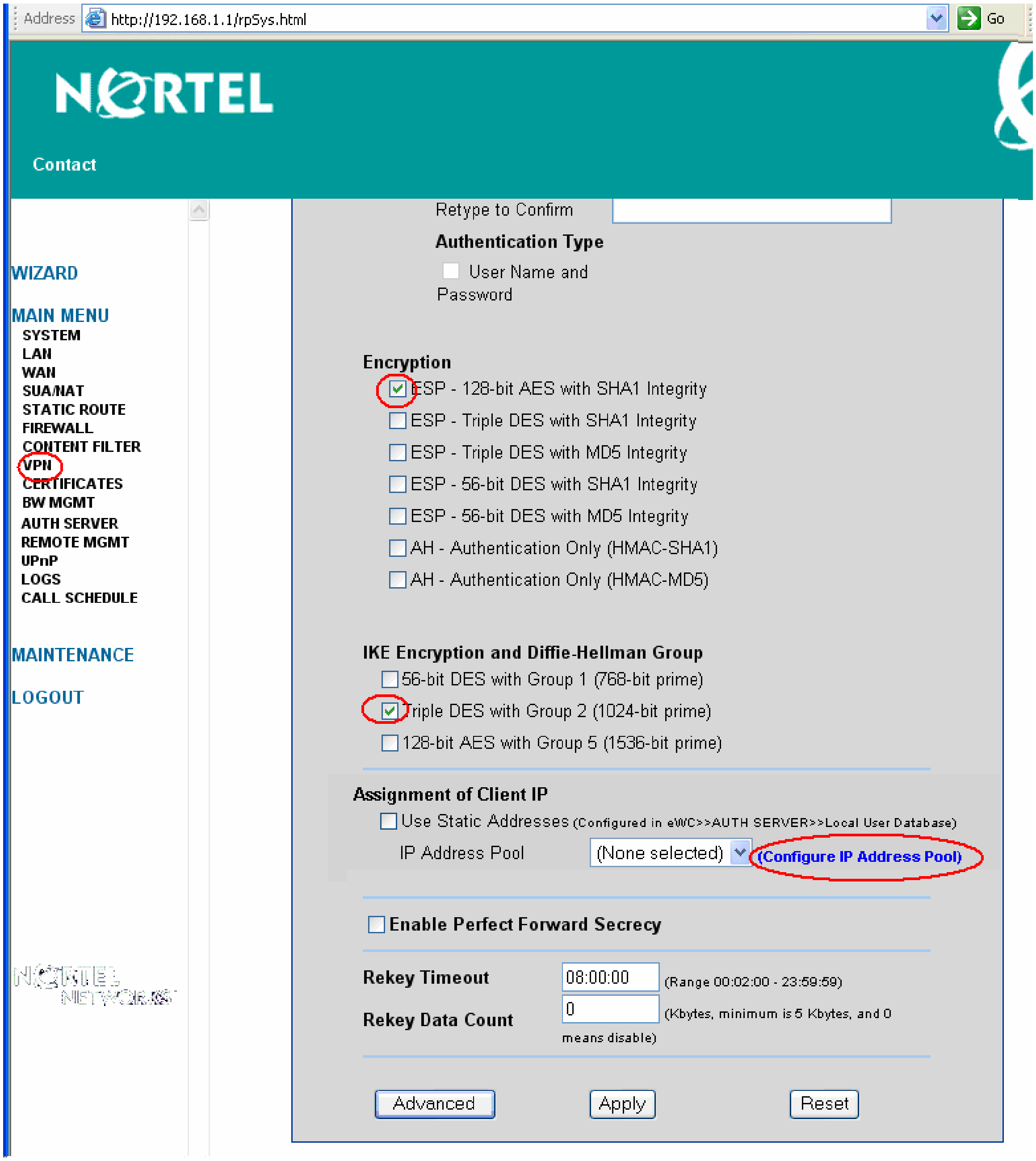
Retype to Confirm

Authentication Type

□ User Name and Password

3.2.6.2 Configure Client Termination Encryption

- For terminating Nortel VPN Client, select Encryption type of “128-bit AES with SHA1 integrity” (or as desired)
- Select IKE Encryption type of “Triple DES with group 2” as shown in the following screen
- Apply the configuration
- Click “Configure IP Address Pool” for further configuration in next step



Retype to Confirm

Authentication Type

□ User Name and Password

Encryption

☑ ESP - 128-bit AES with SHA1 Integrity
□ ESP - Triple DES with SHA1 Integrity
□ ESP - Triple DES with MD5 Integrity
□ ESP - 56-bit DES with SHA1 Integrity
□ ESP - 56-bit DES with MD5 Integrity
□ AH - Authentication Only (HMAC-SHA1)
□ AH - Authentication Only (HMAC-MD5)

IKE Encryption and Diffie-Hellman Group

□ 56-bit DES with Group 1 (768-bit prime)
☑ Triple DES with Group 2 (1024-bit prime)
□ 128-bit AES with Group 5 (1536-bit prime)

Assignment of Client IP

□ Use Static Addresses (Configured in eWC>>AUTH SERVER>>Local User Database)
IP Address Pool (None selected) (Configure IP Address Pool)

□ **Enable Perfect Forward Secrecy**

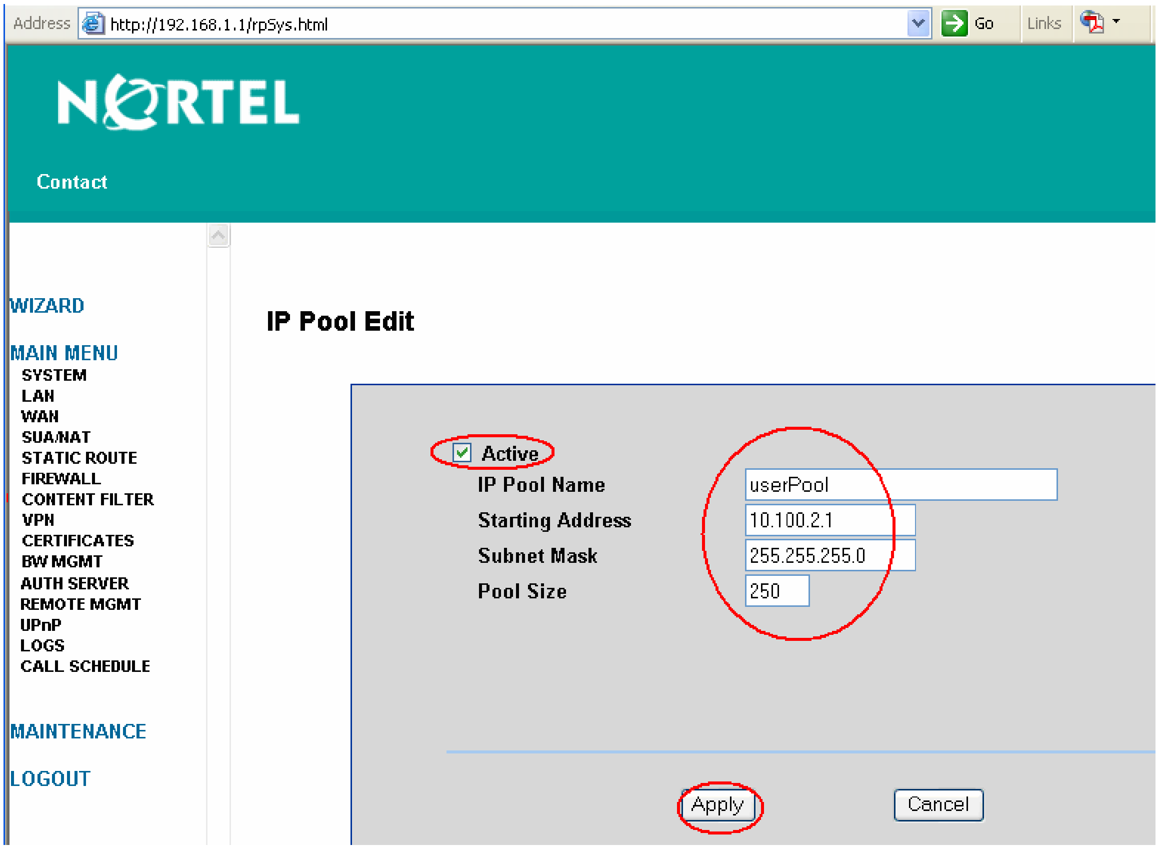
Rekey Timeout 08:00:00 (Range 00:02:00 - 23:59:59)

Rekey Data Count 0 (Kbytes, minimum is 5 Kbytes, and 0 means disable)

3.2.6.3 Configure IP Address Pool

In the lab example, we use IP Pool to dynamically assign IP address to remote road warriors. To create the IP Address Pool, use the following steps:

- Check “Active” for enabling the IP Pool
- Name: “userPool” (for use in our example)
- Starting address: 10.100.2.1 (or as desired)
- Mask: 255.255.255.0 (or as desired)
- Size: 250 (or as desired)
- Click “Apply”



IP Pool Edit

☑ Active

IP Pool Name: userPool

Starting Address: 10.100.2.1

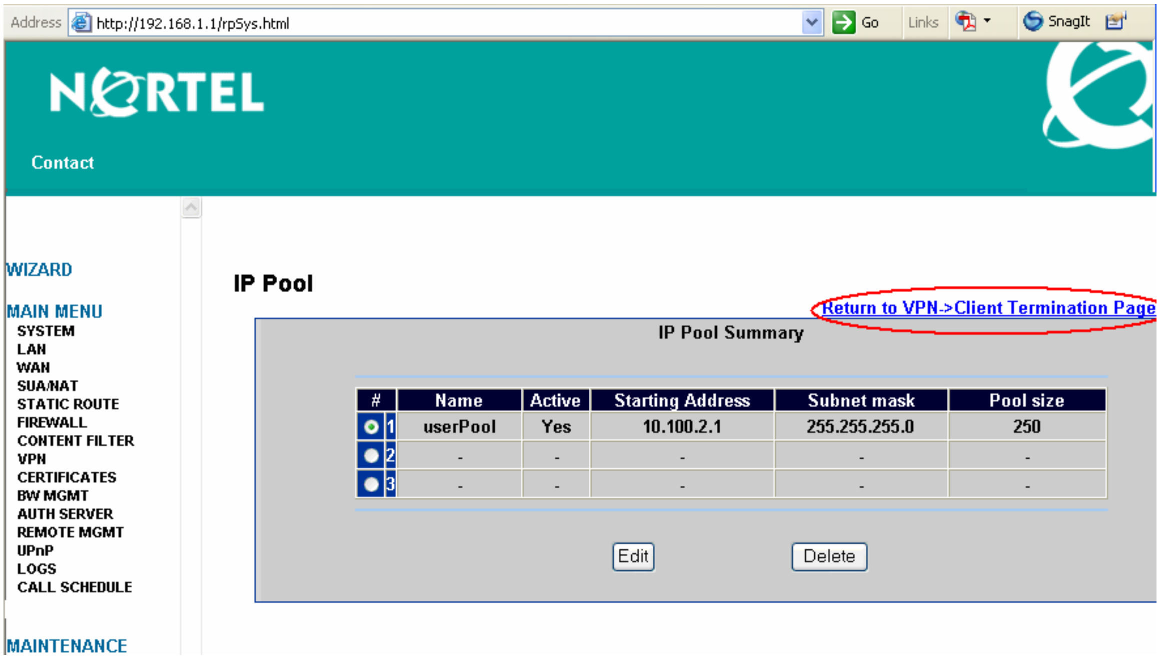
Subnet Mask: 255.255.255.0

Pool Size: 250

3.2.6.4 IP Pool Summary

The IP Pool of “userPool” is shown in the summary window.

To complete the configuration of Client Termination, click the link of “Return to VPN->Client Termination Page.



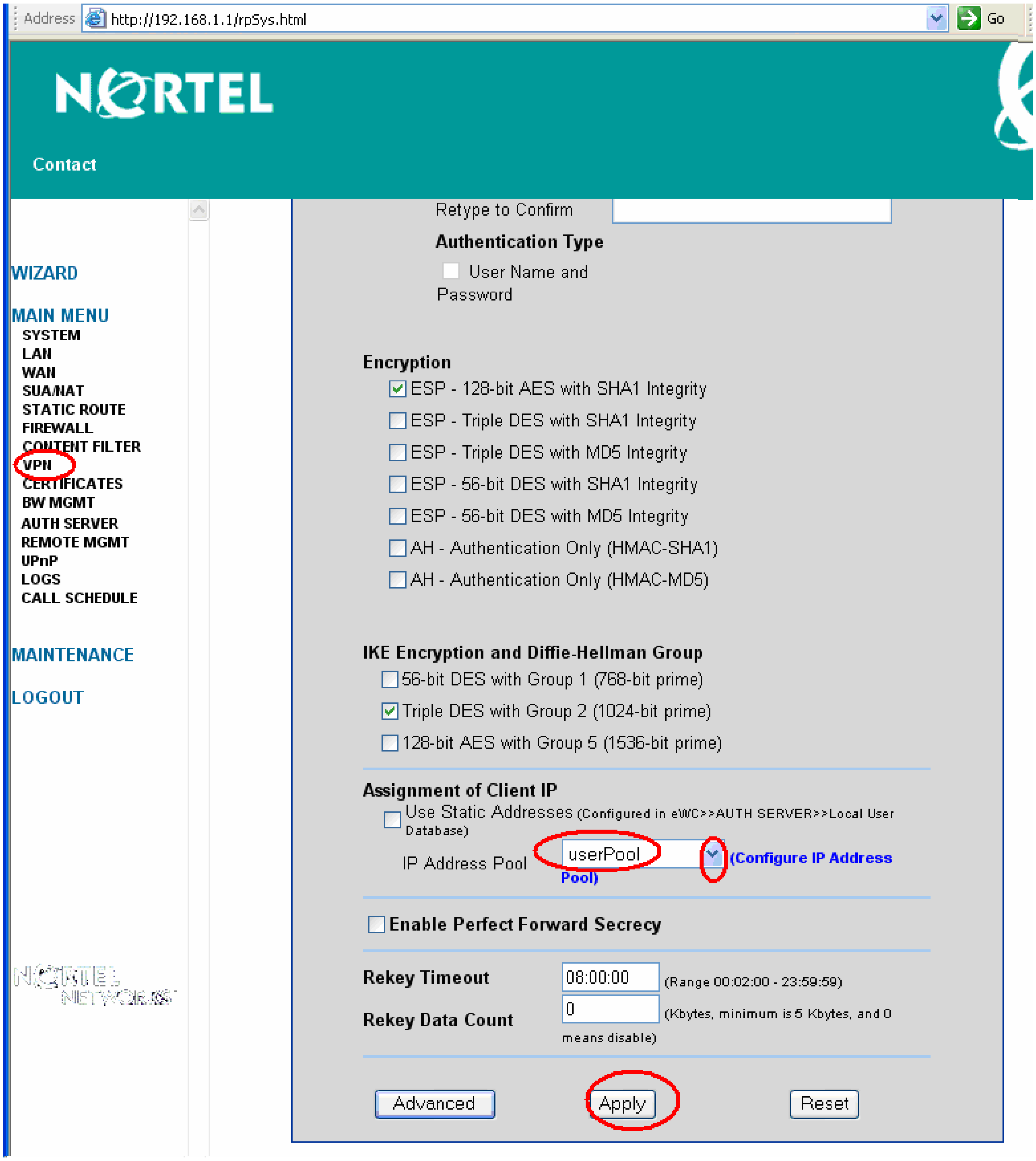
IP Pool

IP Pool Summary

#	Name	Active	Starting Address	Subnet mask	Pool size
● 1	userPool	Yes	10.100.2.1	255.255.255.0	250
○ 2	-	-	-	-	-
○ 3	-	-	-	-	-

3.2.6.5 Select IP Pool

After return to the page of “Client Termination”, select the newly created “userPool” as the IP address pool, then click “Apply”.



Retype to Confirm

Authentication Type

□ User Name and Password

Encryption

☑ ESP - 128-bit AES with SHA1 Integrity
□ ESP - Triple DES with SHA1 Integrity
□ ESP - Triple DES with MD5 Integrity
□ ESP - 56-bit DES with SHA1 Integrity
□ ESP - 56-bit DES with MD5 Integrity
□ AH - Authentication Only (HMAC-SHA1)
□ AH - Authentication Only (HMAC-MD5)

IKE Encryption and Diffie-Hellman Group

□ 56-bit DES with Group 1 (768-bit prime)
☑ Triple DES with Group 2 (1024-bit prime)
□ 128-bit AES with Group 5 (1536-bit prime)

Assignment of Client IP

□ Use Static Addresses (Configured in eWC>>AUTH SERVER>>Local User Database)

IP Address Pool: userPool

□ **Enable Perfect Forward Secrecy**

Rekey Timeout 08:00:00 (Range 00:02:00 - 23:59:59)

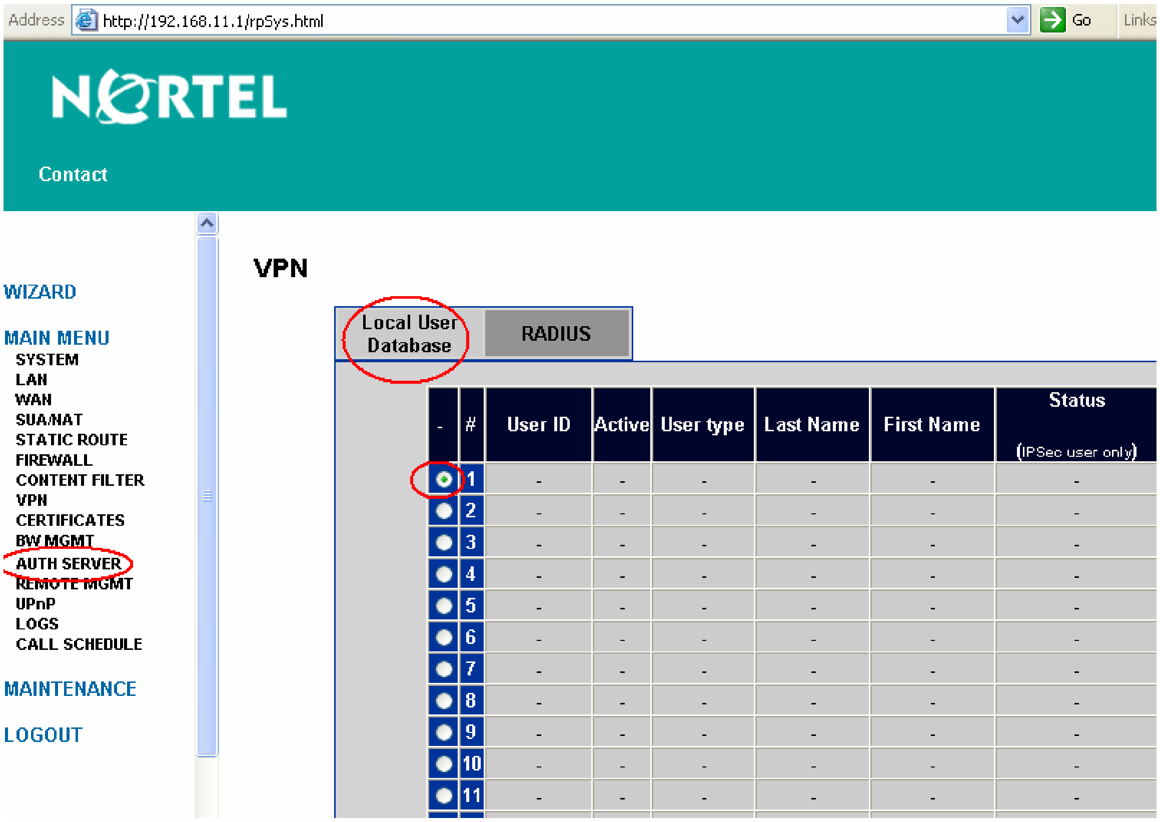
Rekey Data Count 0 (Kbytes, minimum is 5 Kbytes, and 0 means disable)

3.2.7 Configure BCM50e Local User Database

In the lab example, a Local User Database is used for authenticating teleworkers. To build the user database, add user name and password to the local user database as an IPSec user, and activate it. Total of 32 users can be added in the local user database.

Under Main Menu, click “AUTH SERVER”, and you will see an empty list in the summary of the “Local User Database” as shown in the following window.

- To add the first user, select #1 and click “Edit”
- Go to next step for editing user

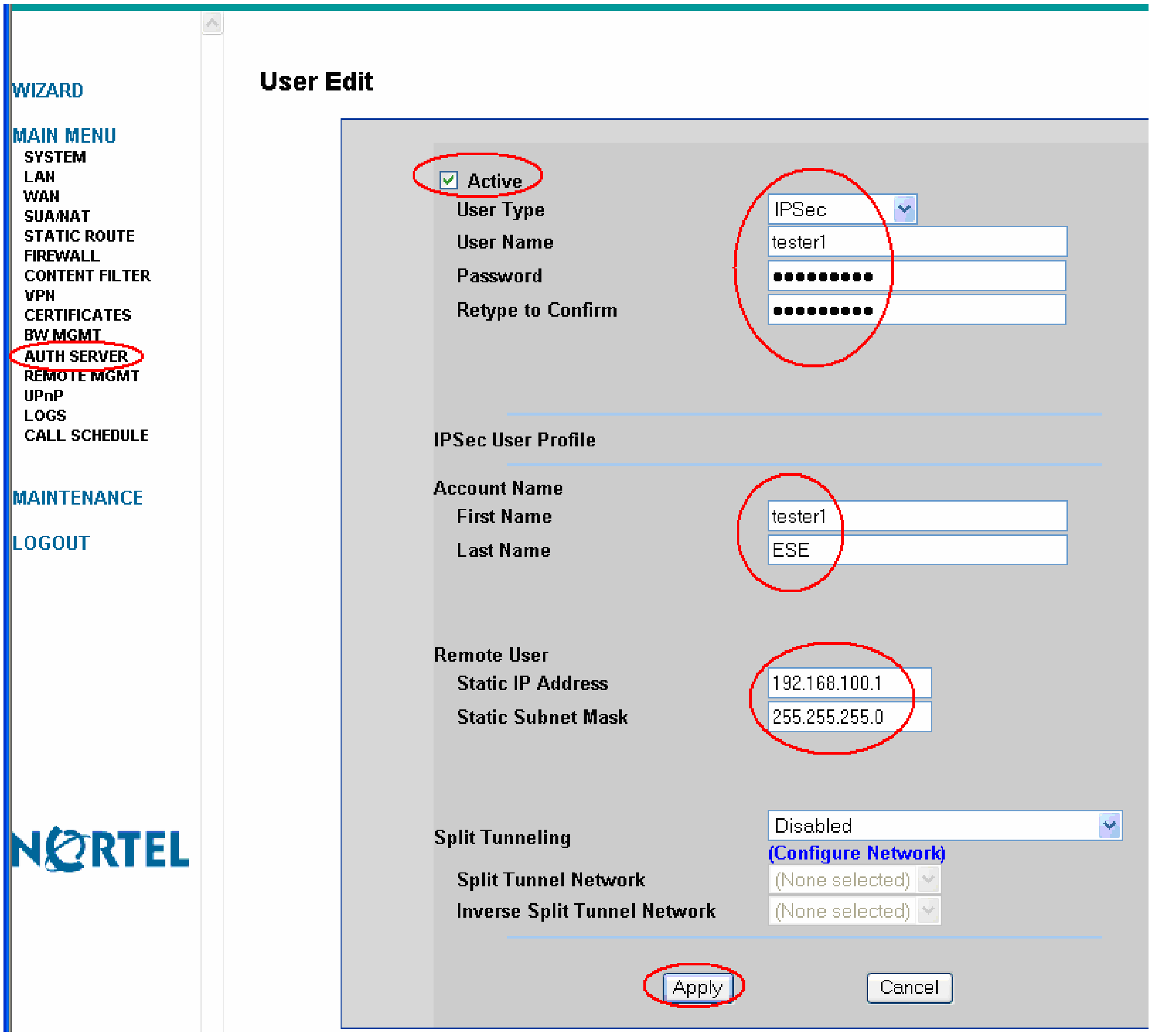


-	#	User ID	Active	User type	Last Name	First Name	Status (IPSec user only)
●	1	-	-	-	-	-	-
○	2	-	-	-	-	-	-
○	3	-	-	-	-	-	-
○	4	-	-	-	-	-	-
○	5	-	-	-	-	-	-
○	6	-	-	-	-	-	-
○	7	-	-	-	-	-	-
○	8	-	-	-	-	-	-
○	9	-	-	-	-	-	-
○	10	-	-	-	-	-	-
○	11	-	-	-	-	-	-

3.2.7.1 Edit Users

Edit the first user by:

- Select “Active”
- Username: tester1, last name “ESE” (or as desired)
- Password: telework1 (for use in our example) (note: what is assigned here must also be used in the client configuration in Section 3.5.2.3).
- Remote User Static IP address: If the road warrior is assigned a static IP address, enter the address that will be assigned to the user. In the lab example, we use IP Pool to dynamically assign IP address to remote road warriors, and the Static IP address is not used. You must not leave the field empty. In order to avoid error message, you must enter an IP address, such as 192.168.100.1/24.
- Apply the change

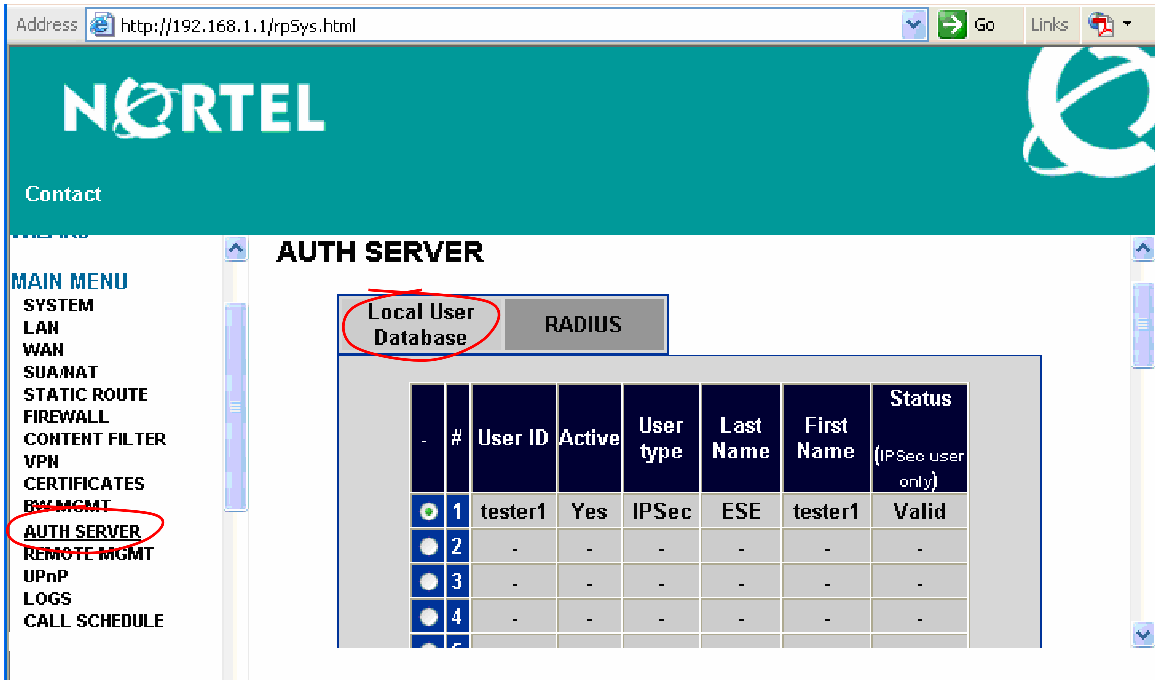


User Edit

☑ Active	
User Type	IPSec
User Name	tester1
Password	●●●●●●●●●
Retype to Confirm	●●●●●●●●●
IPSec User Profile	
Account Name	
First Name	tester1
Last Name	ESE
Remote User	
Static IP Address	192.168.100.1
Static Subnet Mask	255.255.255.0
Split Tunneling	Disabled
	(Configure Network)
Split Tunnel Network	(None selected)
Inverse Split Tunnel Network	(None selected)

3.2.7.2 Summary of Local User Database

The user “tester1” is added to the local user database.



AUTH SERVER

-	#	User ID	Active	User type	Last Name	First Name	Status (IPSec user only)
●	1	tester1	Yes	IPSec	ESE	tester1	Valid
○	2	-	-	-	-	-	-
○	3	-	-	-	-	-	-
○	4	-	-	-	-	-	-

3.3 Site-1 BSR222 Configuration

In this section, we will configure an ABOT tunnel on the site - 1 BSR222 to interworking with the BCM50e in main-office.

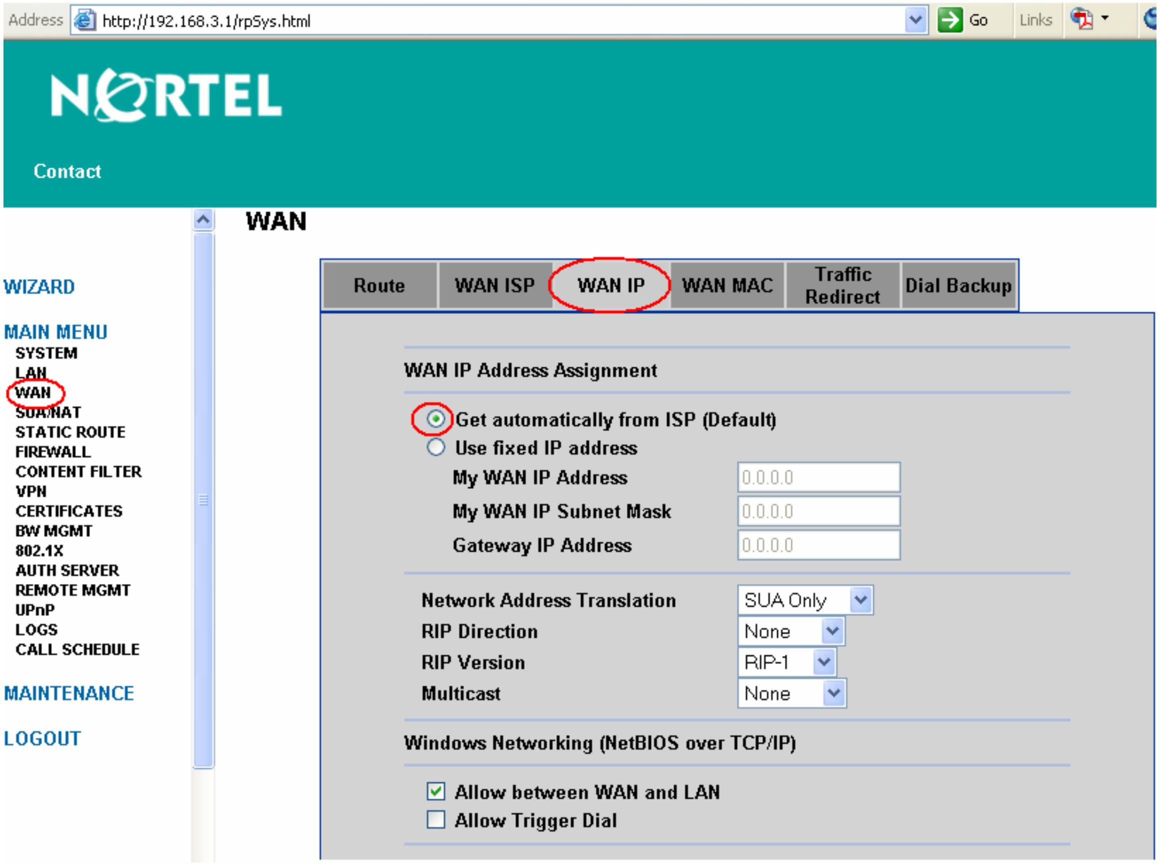
3.3.1 Configure BSR222 WAN and LAN

3.3.1.1 Configure WAN IP

By default, BSR222 WAN IP is configured with a dynamic IP. When the BSR222 is connected to the Internet, an IP address for the WAN IP address is assigned dynamically by your local ISP.

In the BSR222 GUI interface, click WAN ISP tab under WAN menu. Make sure that the field of “Get automatically from ISP” is checked.

See the following screenshot.



WAN

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use fixed IP address

My WAN IP Address	0.0.0.0
My WAN IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0

Network Address Translation	SUA Only
RIP Direction	None
RIP Version	RIP-1
Multicast	None

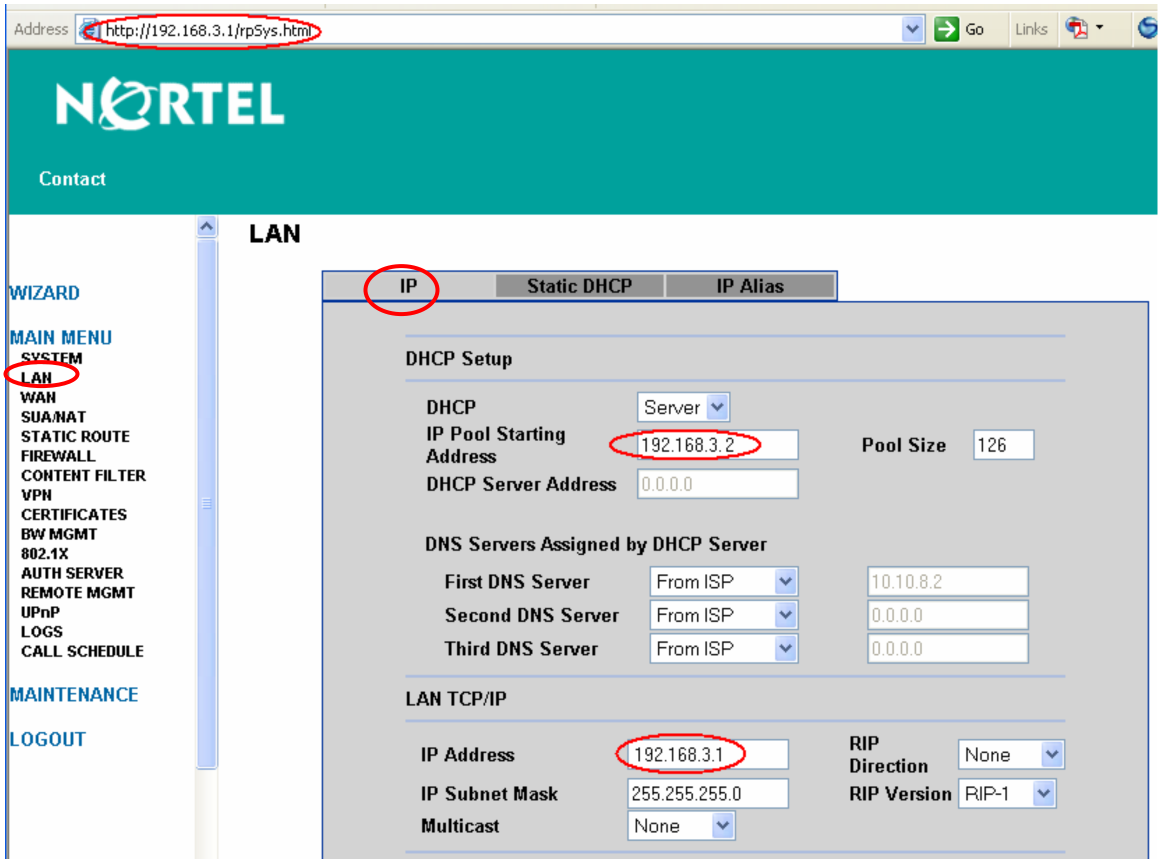
Windows Networking (NetBIOS over TCP/IP)

☑ Allow between WAN and LAN

□ Allow Trigger Dial

3.3.1.2 Configure LAN IP Address

- Change LAN IP address to be 192.168.3.1/24
- Change the IP Pool Starting address to be 192.168.3.2
- Apply the change
- The following page shows the changed IP addresses



Address: http://192.168.3.1/rpSys.html

LAN

DHCP Setup

DHCP	Server		
IP Pool Starting Address	192.168.3.2	Pool Size	126
DHCP Server Address	0.0.0.0		

DNS Servers Assigned by DHCP Server

First DNS Server	From ISP	10.10.8.2
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

LAN TCP/IP

IP Address	192.168.3.1	RIP Direction	None
IP Subnet Mask	255.255.255.0	RIP Version	RIP-1
Multicast	None		

3.3.2 Configure BSR222 ABOT

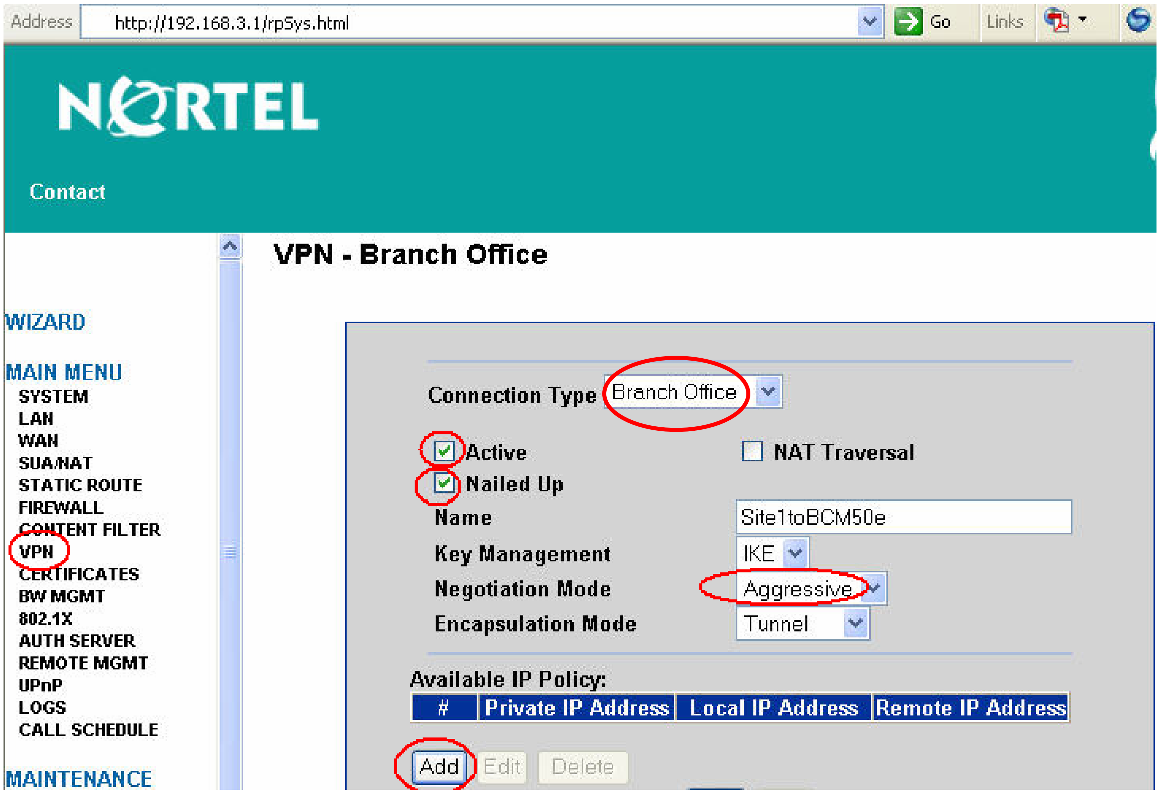
In this section, we will configure the BSR222 to support its ABOT tunnel termination on the BCM50e in the main-office.

If you need more information, please refer to Nortel NTP of “Nortel Business Secure Router 222 Configuration”, Document Number: NN47922-500

3.3.2.1 Configure ABOT VPN Tunnel

Click VPN to open the Summary screen. Selecting an unused index number and then clicking “Edit” to open the following “VPN Branch Office” window.

- Check “Active”, and select “Branch Office” as connection type
- Name it as “Site1toBCM50e” (or as desired)
- Select negotiation mode as “Aggressive”
- Click “Add” button for the next step



VPN - Branch Office

Connection Type: Branch Office

☑ Active □ NAT Traversal

☑ Nailed Up

Name: Site1toBCM50e

Key Management: IKE

Negotiation Mode: Aggressive

Encapsulation Mode: Tunnel

Available IP Policy:

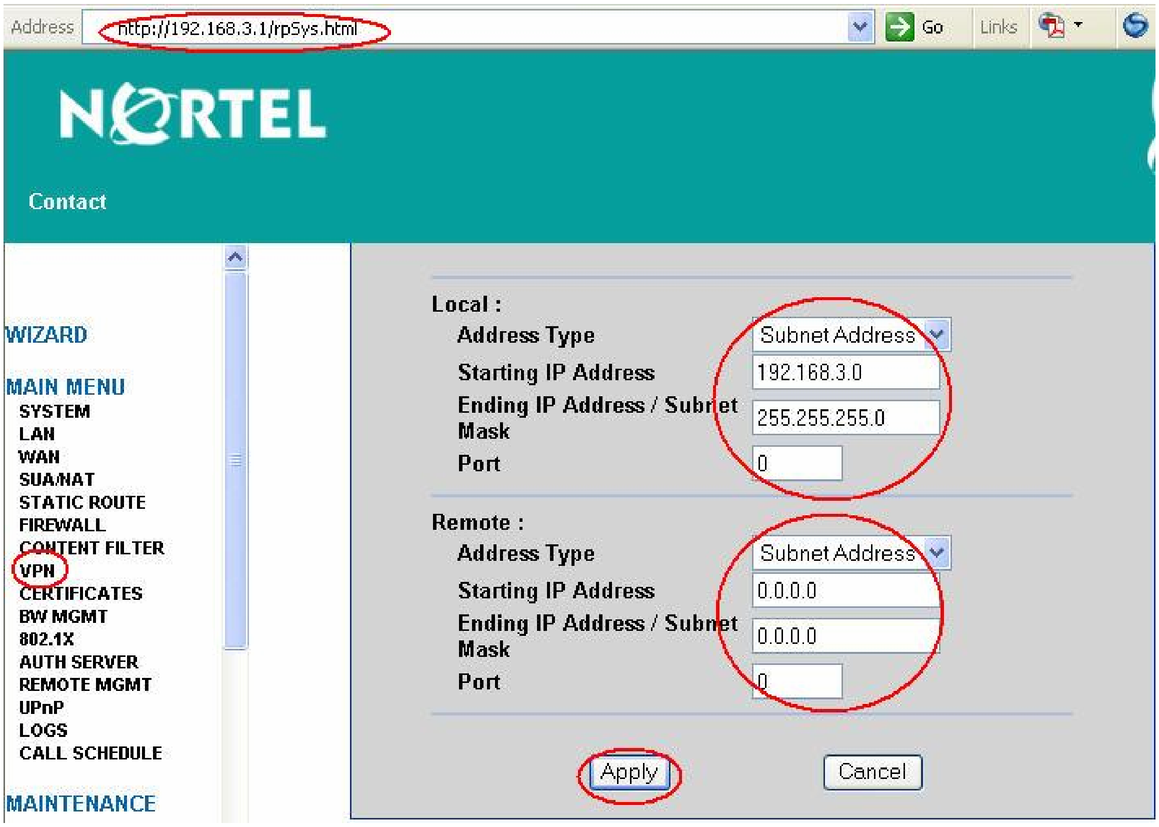
#	Private IP Address	Local IP Address	Remote IP Address

3.3.2.2 VPN - Branch Office - IP Policy

After click “Add” button, the window of “IP Policy” is opened as shown below.

To configure an ABOT tunnel terminate the BCM50e in the main-office and create an IP Policy as shown in the screen shot:

Apply the changes.



Local :

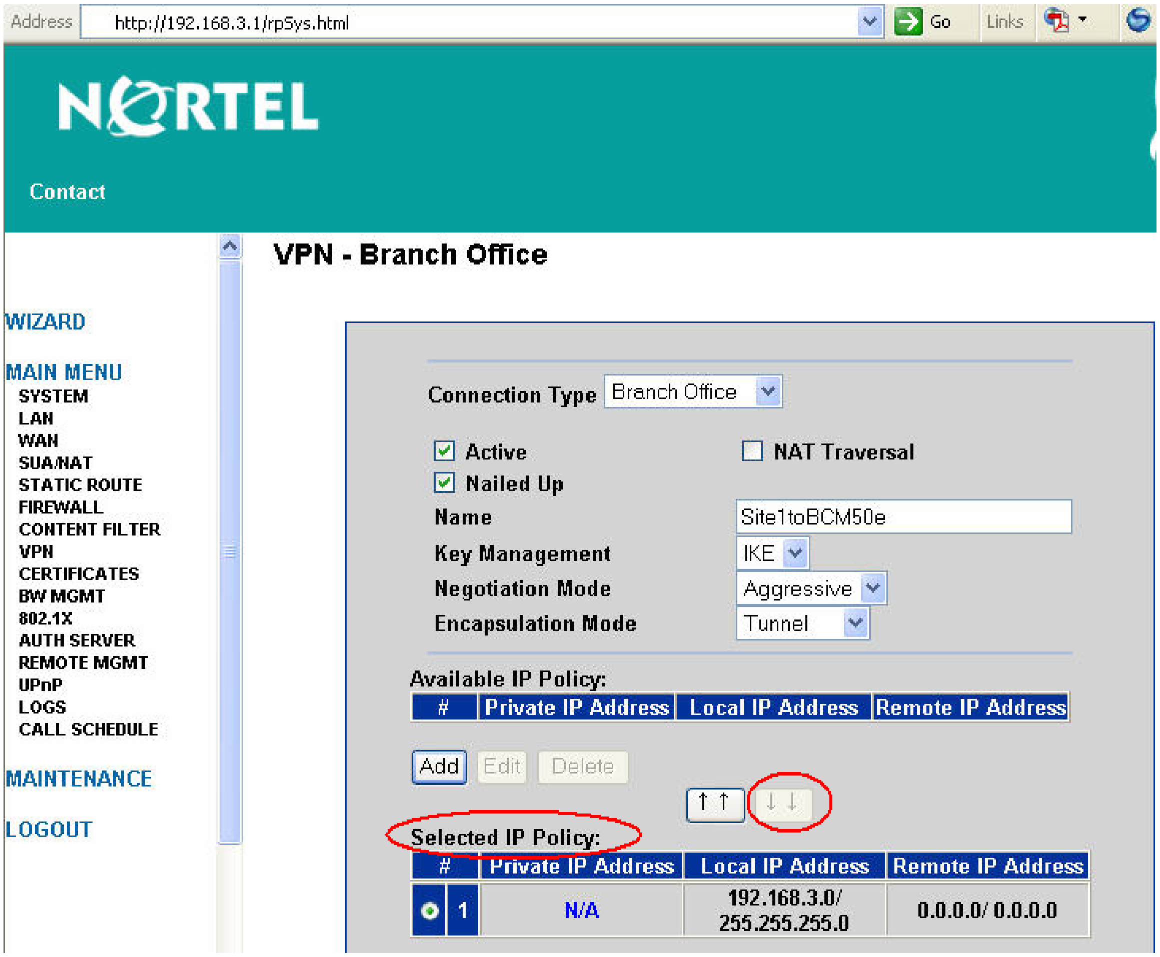
Address Type	Subnet Address
Starting IP Address	192.168.3.0
Ending IP Address / Subnet Mask	255.255.255.0
Port	0

Remote :

Address Type	Subnet Address
Starting IP Address	0.0.0.0
Ending IP Address / Subnet Mask	0.0.0.0
Port	0

3.3.2.3 Selected IP Policy

The newly created dynamic policy is not applied until it is selected. Use double-arrow button to select the newly created IP policy. See the following screen of “Selected IP Policy”.



VPN - Branch Office

Connection Type: Branch Office

☑ Active □ NAT Traversal

☑ Nailed Up

Name: Site1toBCM50e

Key Management: IKE

Negotiation Mode: Aggressive

Encapsulation Mode: Tunnel

Available IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address

Selected IP Policy:

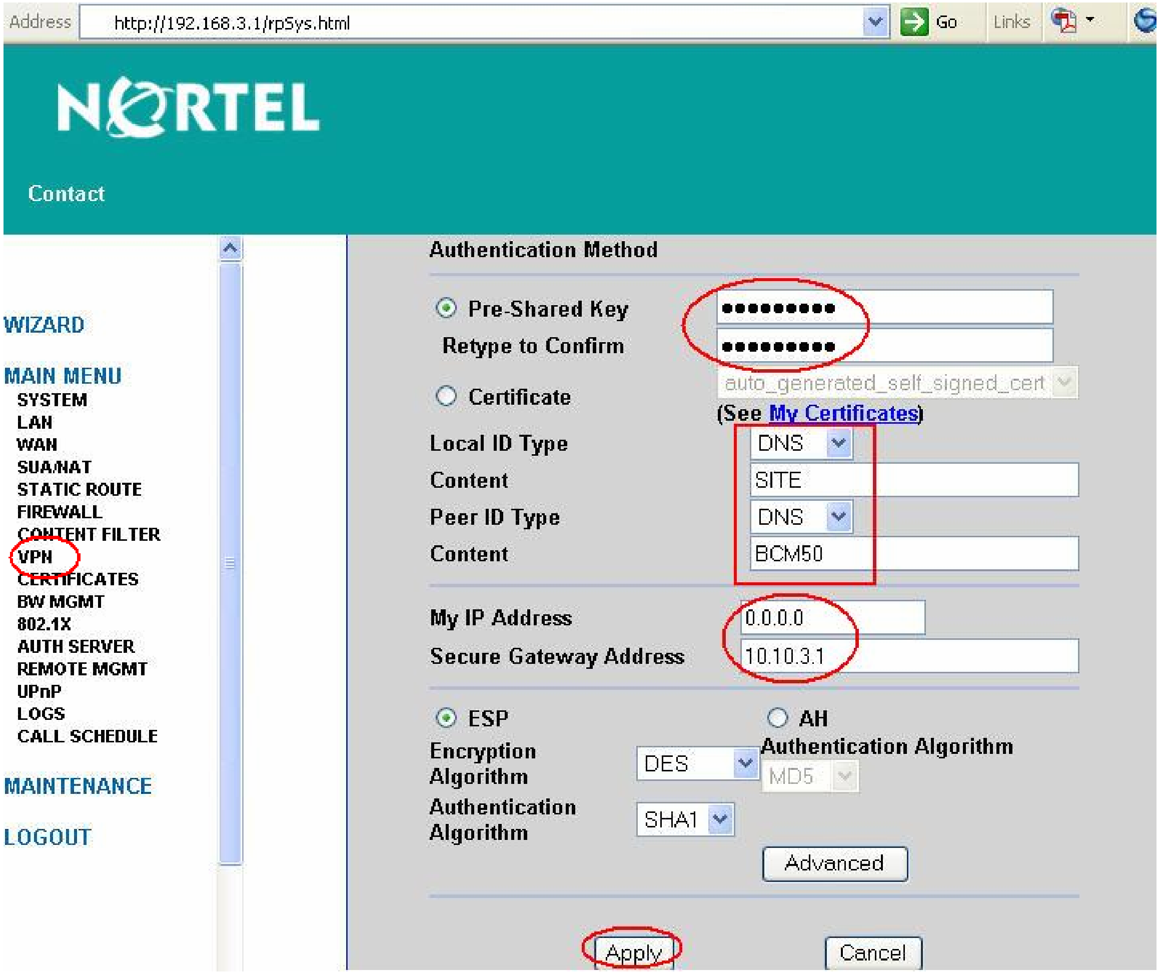
	#	Private IP Address	Local IP Address	Remote IP Address
●	1	N/A	192.168.3.0/ 255.255.255.0	0.0.0.0/ 0.0.0.0

3.3.2.4 ABOT IP Address and Authentication

We continue to configure the ABOT “Site1toBCM50e” with the following steps:

Note: the Authentication of “Pre-shared Key”, “ID Type” and “Content” entered here must match to the authentication configurations of the BCM50e ABOT Authentications in Sections of 3.2.4.5 and with reversed “Remote Content” and “Local Content”.

- Enter the authentication information with a pre-shared key of “contivity”.
- Select “DNS” as “Local ID Type” and enter “SITE” as “Content”. Note: The domain name (up to 31 characters) in the Content field is used for identification purposes only and does not need to be a real domain name.
- Select “DNS” as “Remote ID Type” and enter “BCM50” as “Content”.
- Enter “0.0.0.0” in the field of “My IP Address” and this will cause the BSR222 to use dynamically assigned WAN IP address as “My IP address”.
- Enter “10.10.3.1” as the Secure Gateway Address”. Note: this address is the static IP address configured on the BCM50e WAN interface.
- Select the default encryption and authentication algorithms, and click “Apply” to save and apply the ABOT configuration. See the following screen.



Address http://192.168.3.1/rpSys.html

Authentication Method

◉ Pre-Shared Key ●●●●●●●●●●

Retype to Confirm ●●●●●●●●●●

○ Certificate auto_generated_self_signed_cert

(See My Certificates)

Local ID Type DNS

Content SITE

Peer ID Type DNS

Content BCM50

My IP Address 0.0.0.0

Secure Gateway Address 10.10.3.1

◉ ESP ○ AH

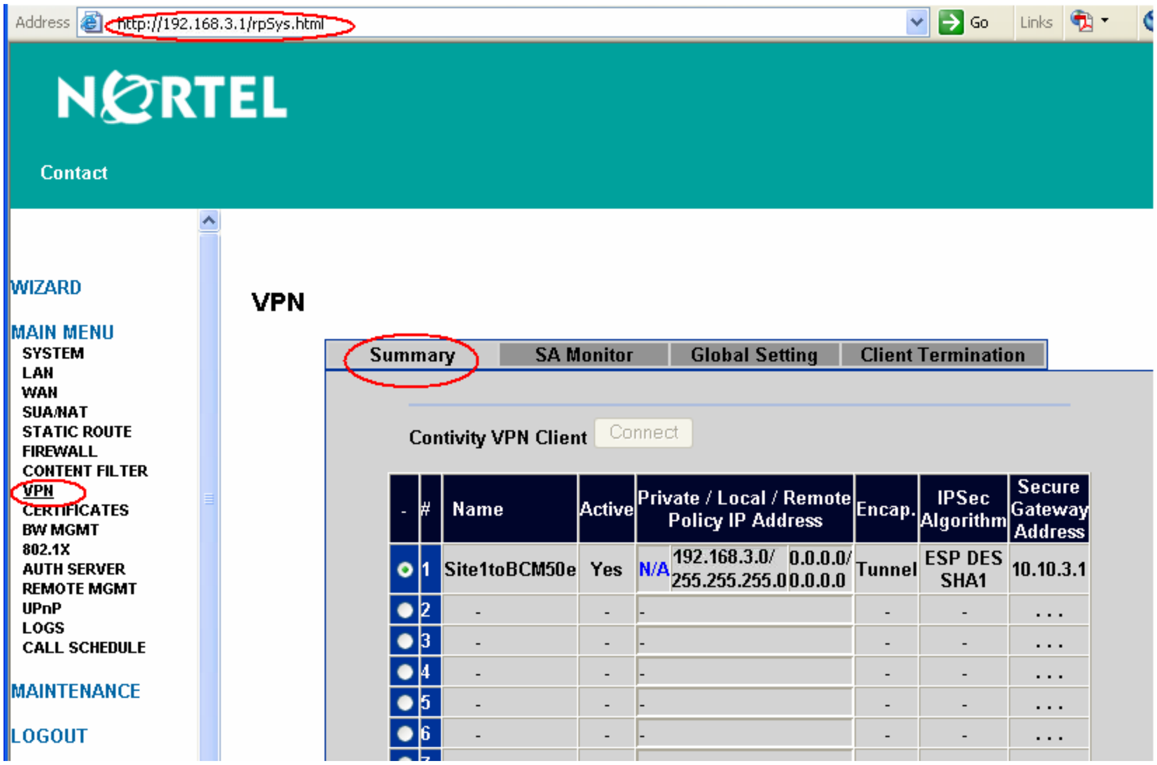
Encryption Algorithm DES

Authentication Algorithm SHA1

Authentication Algorithm MD5

3.3.2.5 VPN Summary

After “Apply”, the VPN should have a summary as shown in the following screen.



Contivity VPN Client

-	#	Name	Active	Private / Local / Remote Policy IP Address			Encap.	IPSec Algorithm	Secure Gateway Address
●	1	Site1toBCM50e	Yes	N/A	192.168.3.0/ 255.255.255.0	0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1	10.10.3.1
○	2	-	-	-			-	-	...
○	3	-	-	-			-	-	...
○	4	-	-	-			-	-	...
○	5	-	-	-			-	-	...
○	6	-	-	-			-	-	...

3.4 Site-2 BSR222 Configuration

In this section, we will configure an ABOT tunnel on the site-2 BSR222 to interworking with the BCM50e in main-office.

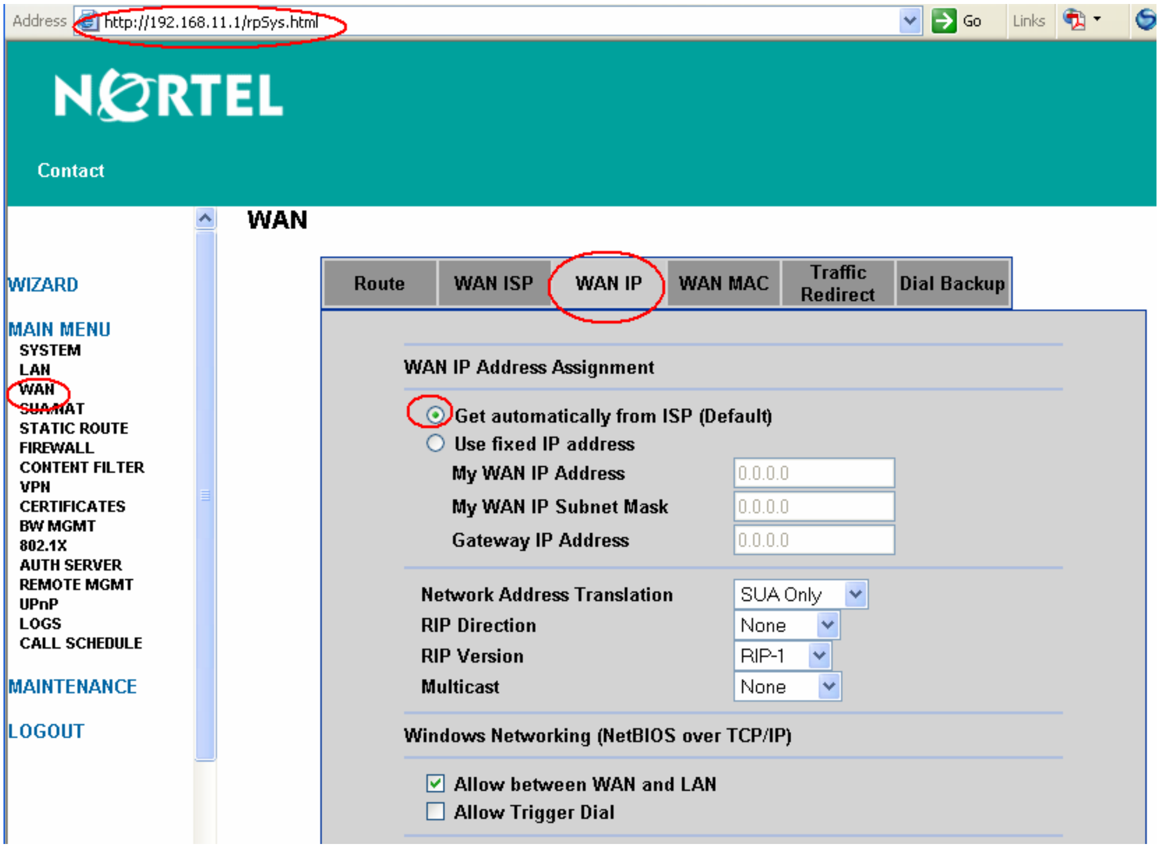
3.4.1 Configure BSR222 WAN and LAN

3.4.1.1 Configure WAN IP

By default, BSR222 WAN IP is configured with a dynamic IP. When the BSR222 is connected to Internet, an IP address for the WAN IP address is assigned dynamically by your local ISP

In the BSR222 GUI interface, click WAN ISP tab under WAN menu. Make sure that the field of “Get automatically from ISP” is checked.

See the following screenshot.



WAN

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use fixed IP address

My WAN IP Address	0.0.0.0
My WAN IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Network Address Translation	SUA Only
RIP Direction	None
RIP Version	RIP-1
Multicast	None

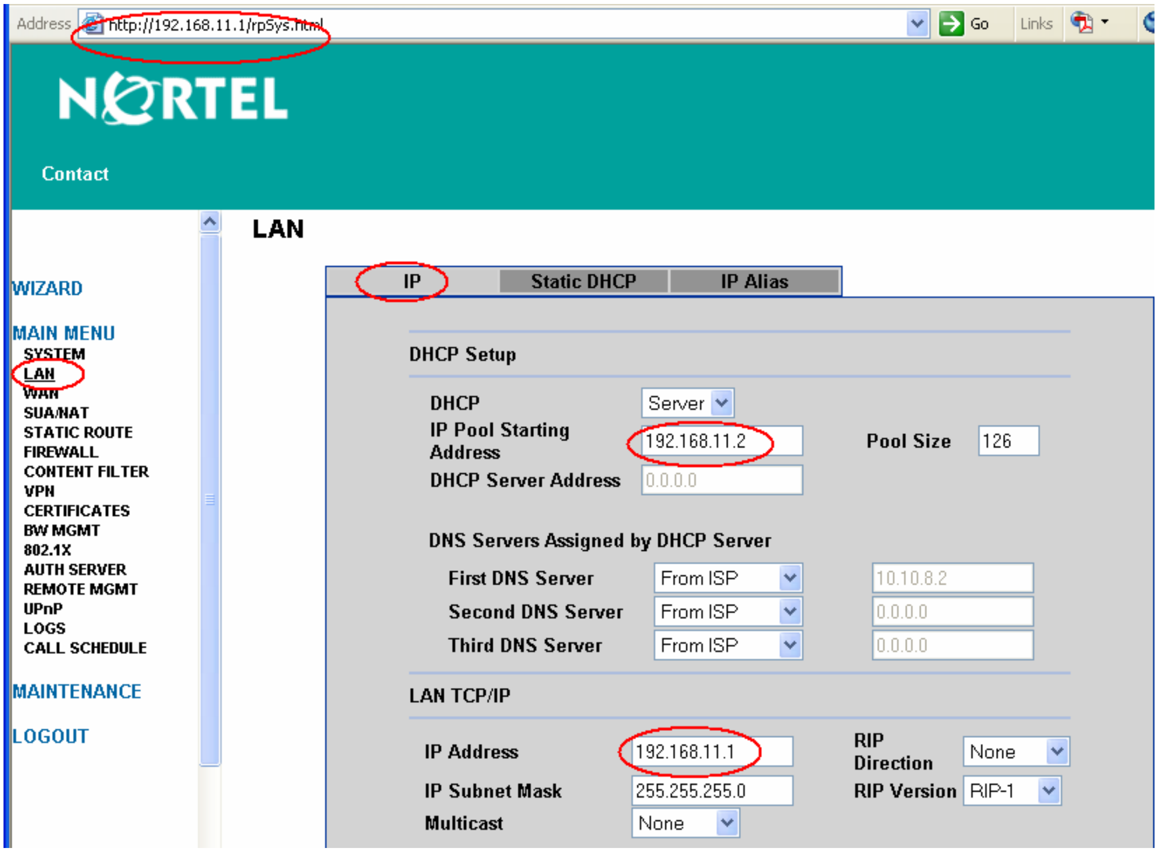
Windows Networking (NetBIOS over TCP/IP)

☑ Allow between WAN and LAN

□ Allow Trigger Dial

3.4.1.2 Configure LAN IP

- Change LAN IP address to be 192.168.11.1/24
- Change the IP Pool Starting address to be 192.168.11.2
- Apply the change
- The following page shows the changed IP addresses



DHCP Setup

DHCP	Server		
IP Pool Starting Address	192.168.11.2	Pool Size	126
DHCP Server Address	0.0.0.0		

DNS Servers Assigned by DHCP Server

First DNS Server	From ISP	10.10.8.2
Second DNS Server	From ISP	0.0.0.0
Third DNS Server	From ISP	0.0.0.0

LAN TCP/IP

IP Address	192.168.11.1	RIP Direction	None
IP Subnet Mask	255.255.255.0	RIP Version	RIP-1
Multicast	None		

3.4.2 Configure BSR222 ABOT

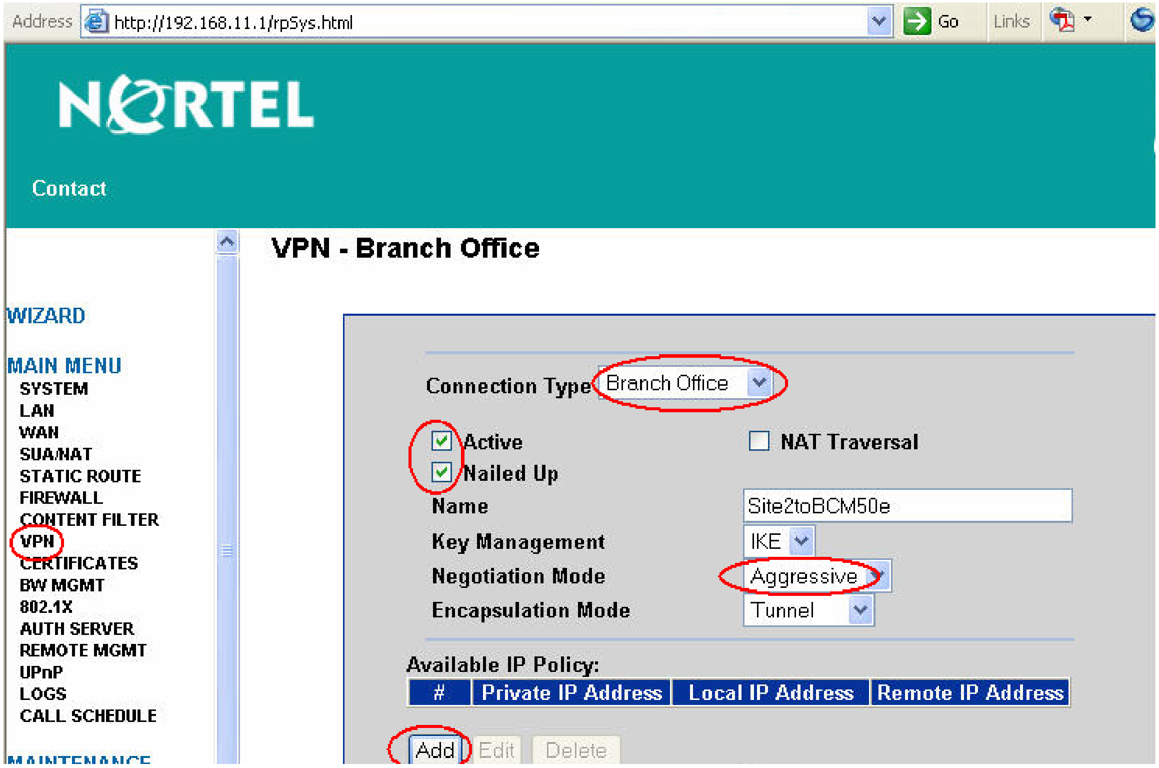
In this section, we will configure the BSR222 to support its ABOT tunnel termination on the BCM50e in the main-office.

If you need more information, please refer to Nortel NTP of “Nortel Business Secure Router 222 Configuration”, Document Number: NN47922-500

3.4.2.1 Configure ABOT VPN Tunnel

Click VPN to open the Summary screen. Selecting an unused index number and then clicking “Edit” to open the following “VPN Branch Office” window.

- Check “Active”, and select “Branch Office” as connection type
- Name it as “Site2toBCM50e” (or as desired)
- Select negotiation mode as “Aggressive”
- Click “Add” button for the next step



VPN - Branch Office

Connection Type: Branch Office

☑ Active ☐ NAT Traversal

☑ Nailed Up

Name	Site2toBCM50e
Key Management	IKE
Negotiation Mode	Aggressive
Encapsulation Mode	Tunnel

Available IP Policy:

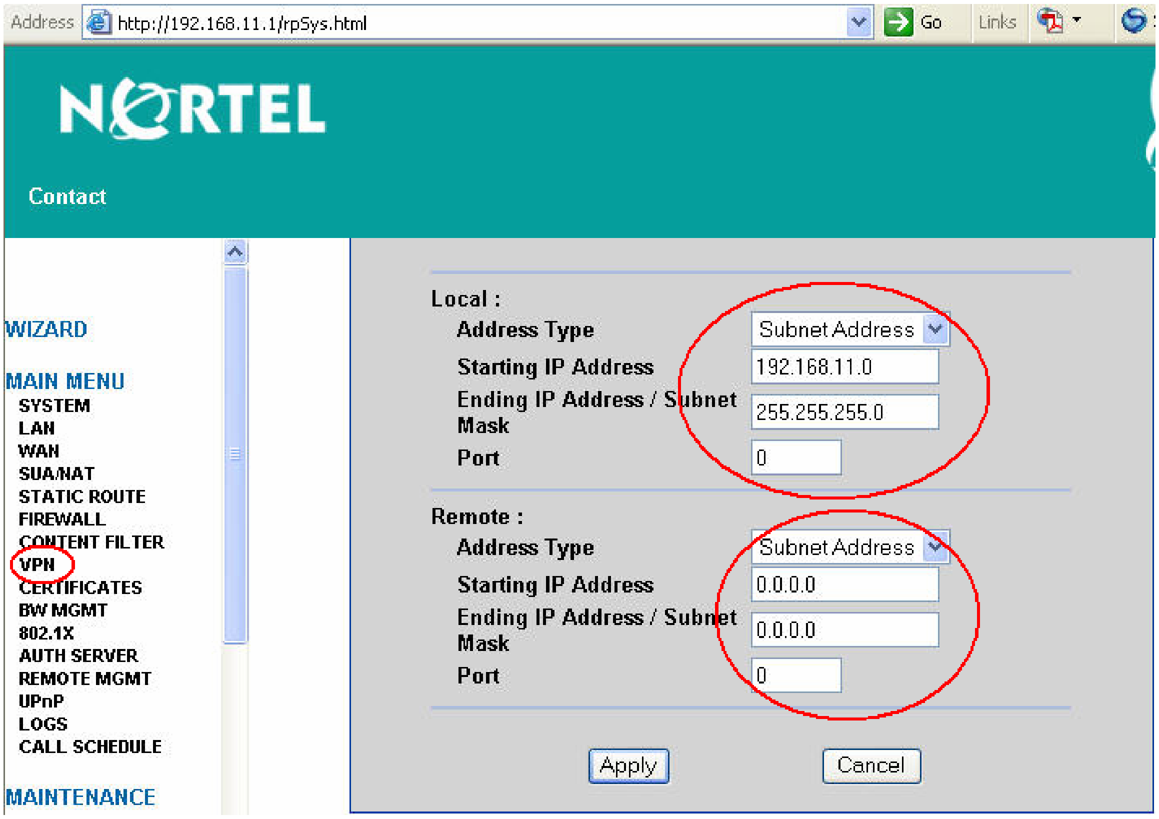
#	Private IP Address	Local IP Address	Remote IP Address

3.4.2.2 VPN - Branch Office - IP Policy

After click “Add” button, the window of “IP Policy” is opened as shown in the following screenshot.

To configure an ABOT tunnel termination on the BCM50e in the main-office, create an IP Policy as shown in the screen shot:

Apply the changes



Local :

Address Type: Subnet Address

Starting IP Address: 192.168.11.0

Ending IP Address / Subnet Mask: 255.255.255.0

Port: 0

Remote :

Address Type: Subnet Address

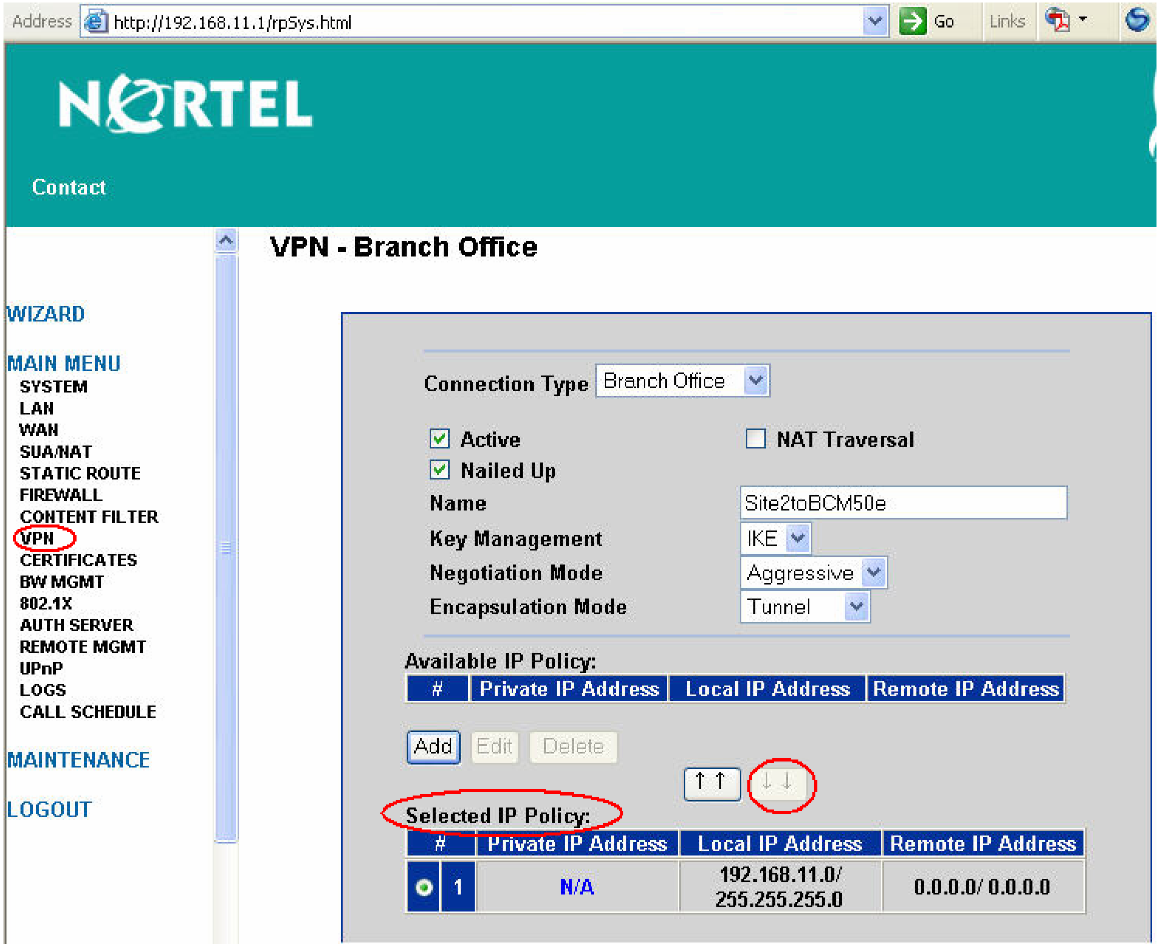
Starting IP Address: 0.0.0.0

Ending IP Address / Subnet Mask: 0.0.0.0

Port: 0

3.4.2.3 Selected IP Policy

The newly created dynamic policy is not applied until it is selected. Use double-arrow button to select the newly created IP policy. See the following screen of “Selected IP Policy”.



http://192.168.11.1/rpSys.html

VPN - Branch Office

Connection Type: Branch Office

☑ Active

☐ NAT Traversal

☑ Nailed Up

Name: Site2toBCM50e

Key Management: IKE

Negotiation Mode: Aggressive

Encapsulation Mode: Tunnel

Available IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address

Selected IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
● 1	N/A	192.168.11.0/ 255.255.255.0	0.0.0.0/ 0.0.0.0

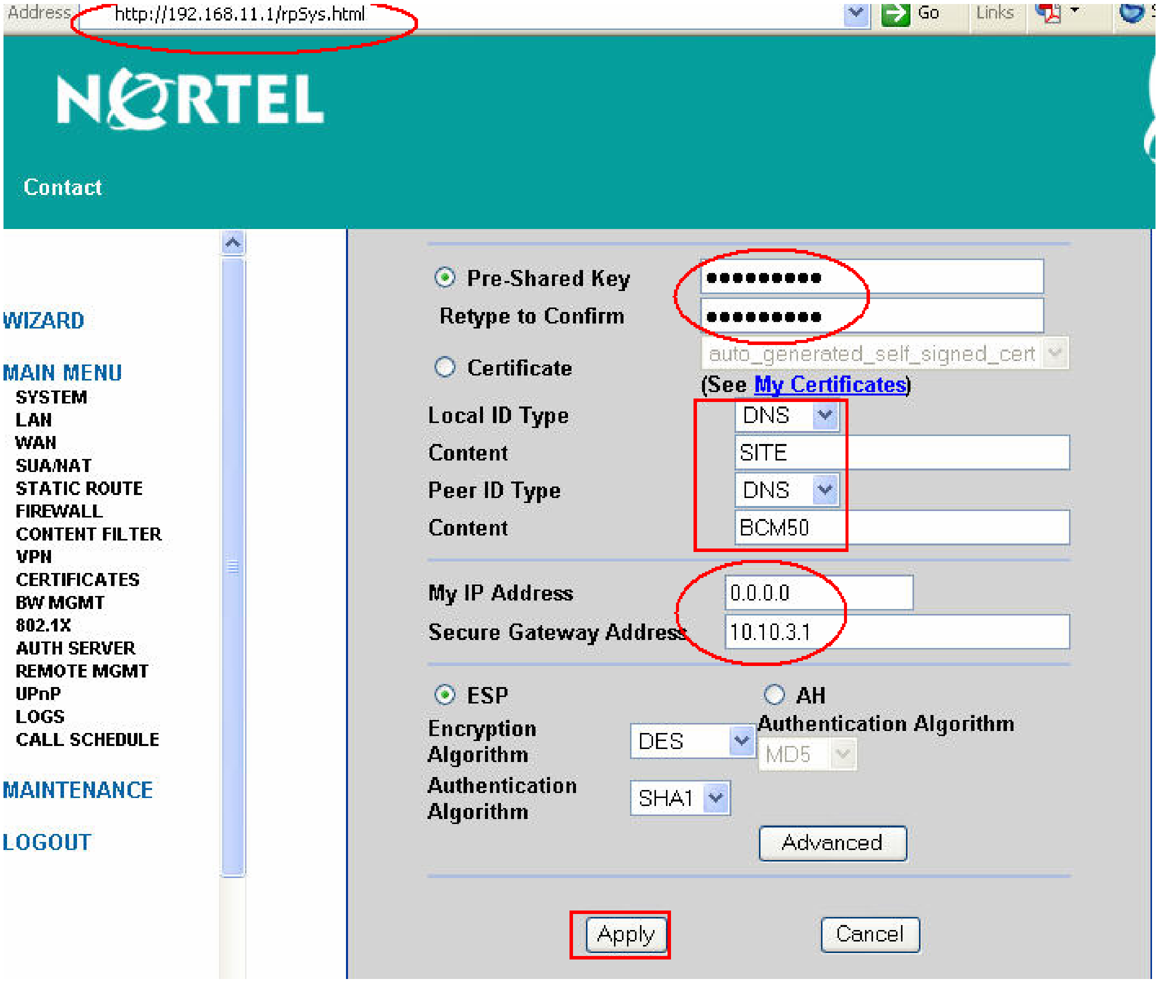
3.4.2.4 ABOT IP Address and Authentication

3.4.2.5 ABOT IP Address and Authentication

We continue to configure the ABOT “Site2toBCM50e” with the following steps:

Note: the Authentication of “Pre-shared Key”, “ID Type” and “Content” entered here must match to the authentication configurations of the BCM50e ABOT Authentications in Sections of 3.2.4.5 and with reversed “Remote Content” and “Local Content”.

- Enter the authentication information with a pre-shared key of “contivity”.
- Select “DNS” as “Local ID Type” and enter “SITE” as “Content”. Note: The domain name (up to 31 characters) in the Content field is used for identification purposes only and does not need to be a real domain name.
- Select “DNS” as “Remote ID Type” and enter “BCM50” as “Content”.
- Enter “0.0.0.0” in the field of “My IP Address” and this will cause the BSR222 to use dynamically assigned WAN IP address as “My IP address”.
- Enter “10.10.3.1” as the Secure Gateway Address”. Note: this address is the static IP address configured on the BCM50e WAN interface.
- Select the default encryption and authentication algorithms, and click “Apply” to save and apply the ABOT configuration. See the following screen.



http://192.168.11.1/rpSys.html

● Pre-Shared Key ●●●●●●●●●●

Retype to Confirm ●●●●●●●●●●

○ Certificate auto_generated_self_signed_cert
(See My Certificates)

Local ID Type DNS

Content SITE

Peer ID Type DNS

Content BCM50

My IP Address 0.0.0.0

Secure Gateway Address 10.10.3.1

● ESP ○ AH

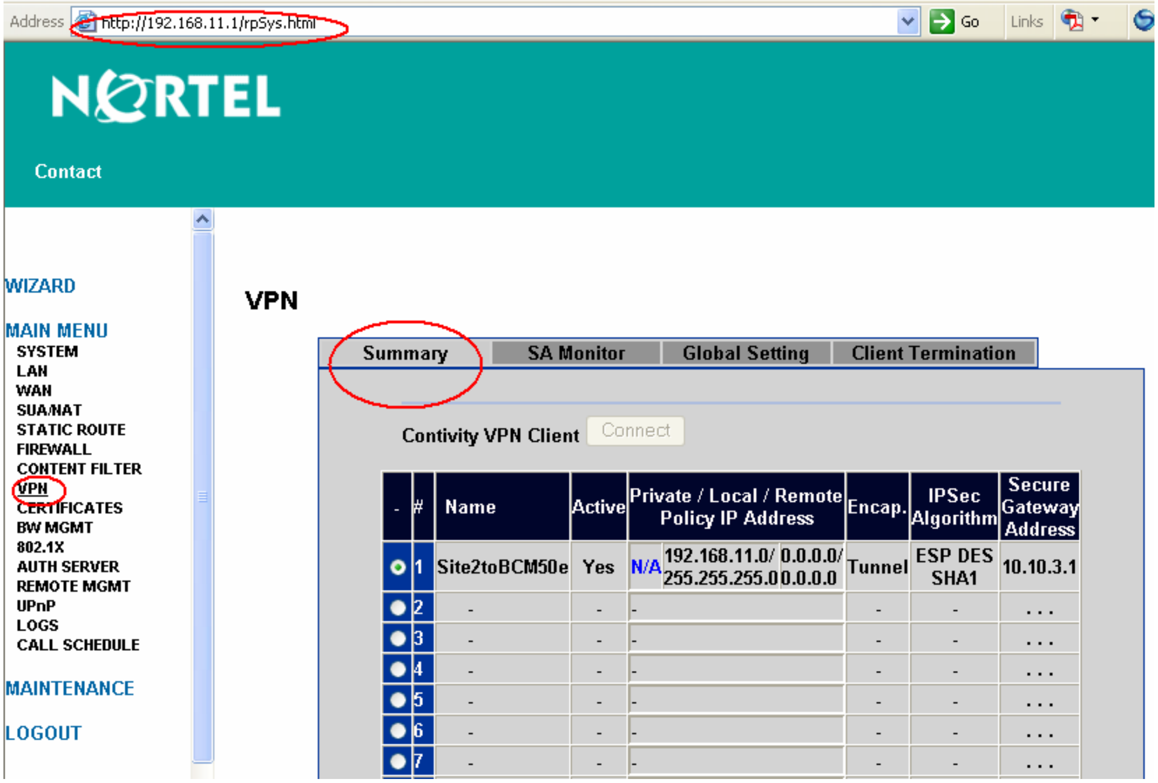
Encryption Algorithm DES

Authentication Algorithm SHA1

Authentication Algorithm MD5

3.4.2.6 VPN Summary

After "Apply", the VPN should have a summary as shown in the following diagram:



http://192.168.11.1/rpSys.html

VPN

Contivity VPN Client

-	#	Name	Active	Private / Local / Remote Policy IP Address	Encap.	IPSec Algorithm	Secure Gateway Address
●	1	Site2toBCM50e	Yes	N/A 192.168.11.0/ 255.255.255.0 0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1	10.10.3.1
○	2	-	-	-	-	-	...
○	3	-	-	-	-	-	...
○	4	-	-	-	-	-	...
○	5	-	-	-	-	-	...
○	6	-	-	-	-	-	...
○	7	-	-	-	-	-	...

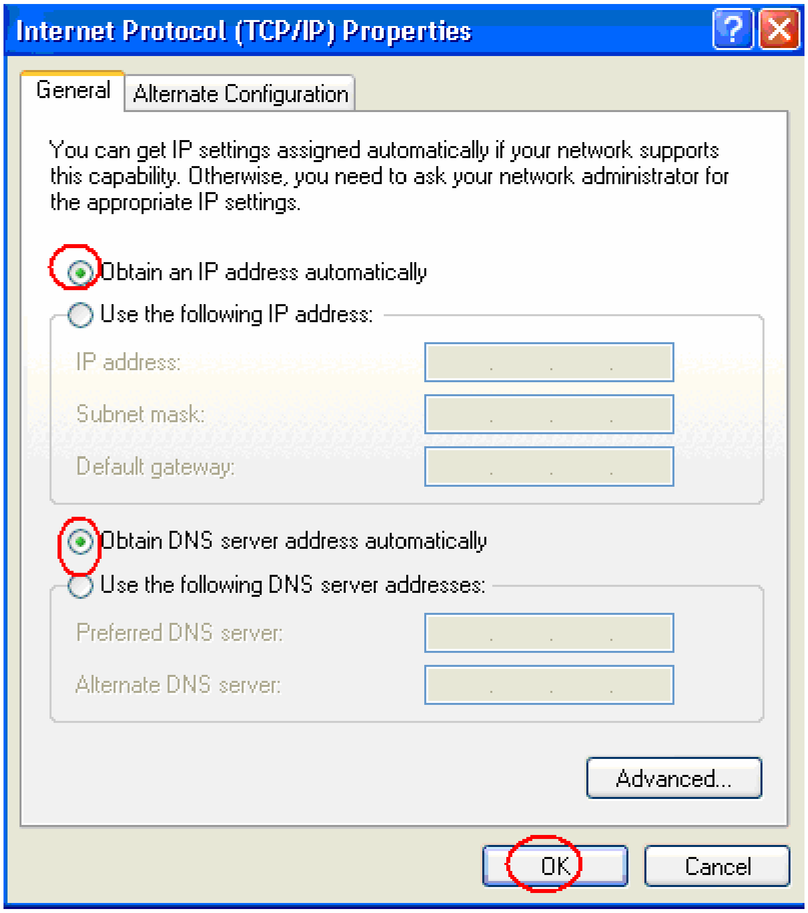
3.5 Mobile Teleworker VPN CLIENT Configuration

3.5.1 Configure IP Address on PC

A dynamic IP address is configured on the mobile worker's laptop (PC-3).

Open the Internet Protocol Properties, and select "Obtain an IP address automatically" and "Obtain DNS server address automatically", click "OK" to apply. See the following window for example.

In the lab example, the PC-3's NIC interface is connected to the DHCP server on the network of 10.10.8.0/24. It will obtain an IP address of 10.10.8.x. See the Lab Topology for reference.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

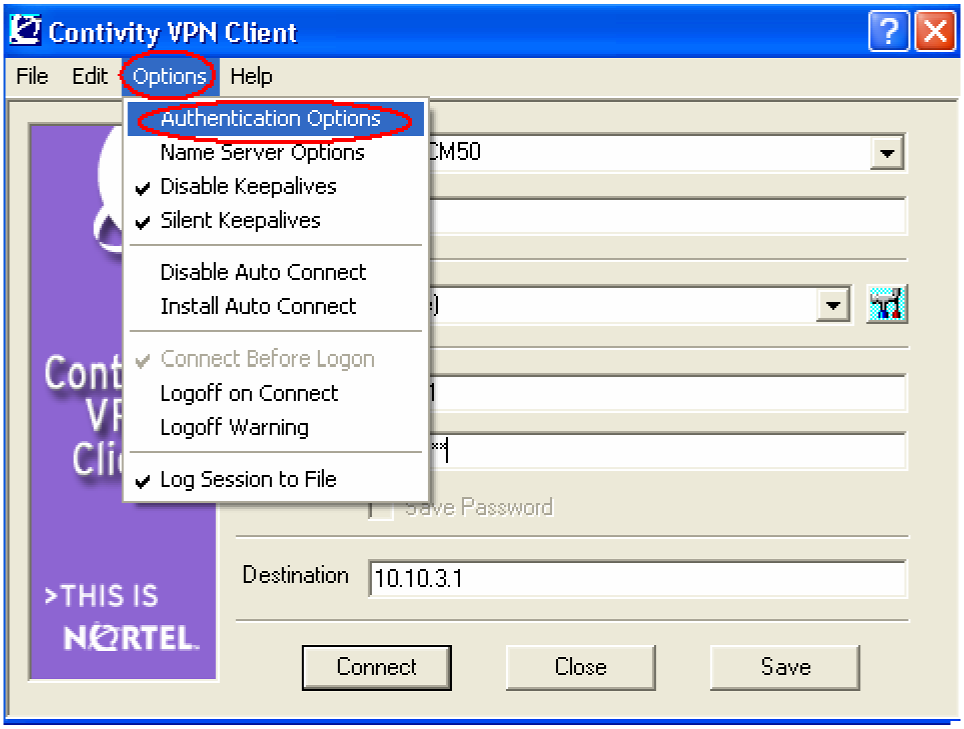
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

3.5.2 VPN Configuration for the Road Warrior

- Obtain Nortel VPN Client software
- Install Nortel VPN Client software on the laptop
- Following the steps below to configure the VPN Client

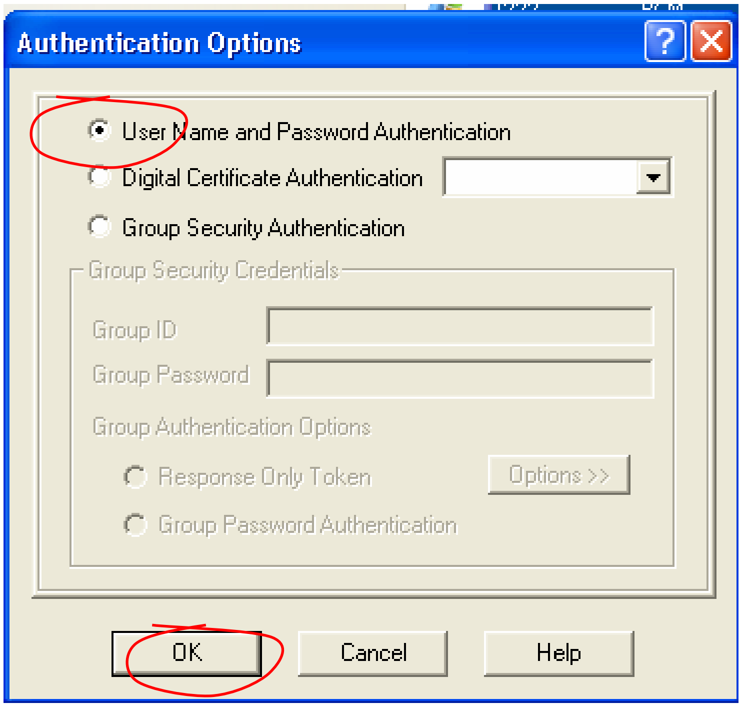
3.5.2.1 Authentication Configuration

- Start the Nortel VPN Client application
- Select "Authentication Options" under the Options pull-down menu as shown below.



3.5.2.2 Select Authentication Option

In the “Authentication Options” window, check “User Name and Password Authentication”, and click “OK”. See below screenshot.

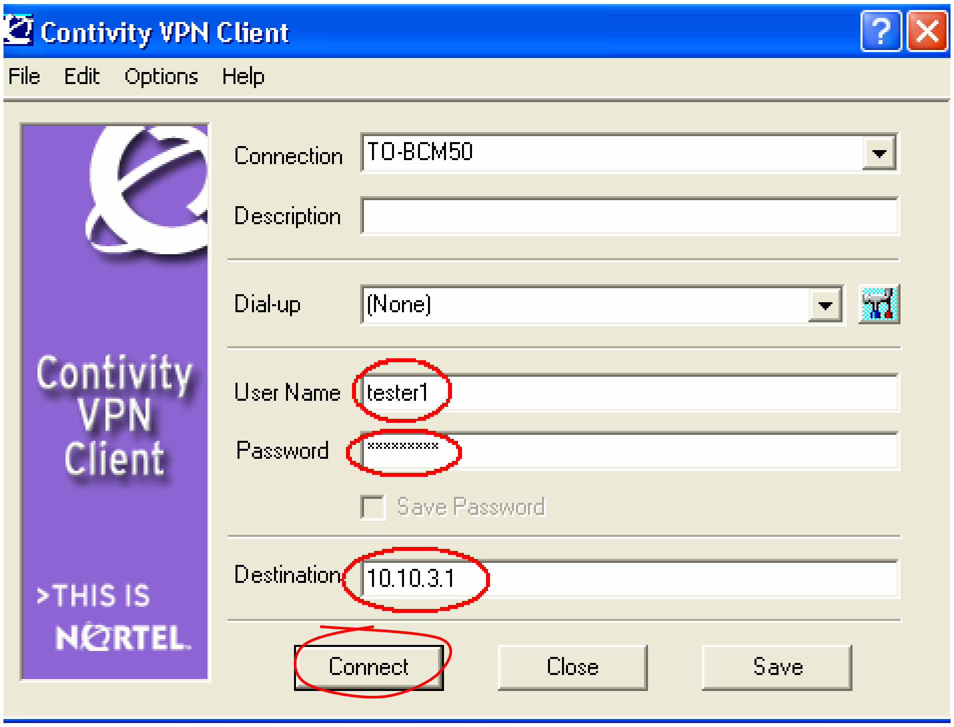


● User Name and Password Authentication
○ Digital Certificate Authentication
○ Group Security Authentication
○ Response Only Token
○ Group Password Authentication

3.5.2.3 Launch VPN Connection

To make the VPN connection to the BCM50e in main-office, enter the following parameters:

- User name: tester1 (Note: the user name here is pre-configured in the User Database in the section of 3.2.6.1).
- Password: telework1 (Note: the password here must be identical to the password assigned to tester1 in section of 3.2.6.1)
- Gateway address: 10.10.3.1 (Note: this is the Static WAN IP on the BCM50e)
- Click “connect” to launch the connection



Connection: TO-BCM50

Description:

Dial-up: (None)

User Name: tester1

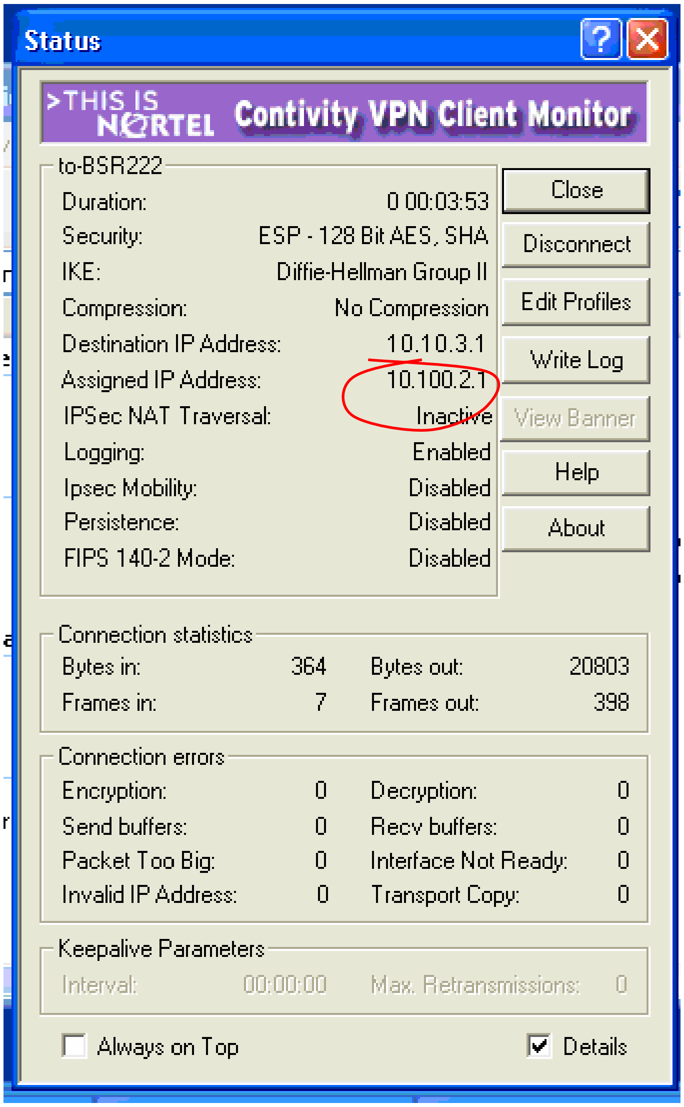
Password: *********

□ Save Password

Destination: 10.10.3.1

3.5.3 Verify and Monitor Connectivity

After the VPN connection is successfully setup, open the status window and you should see the assigned IP address is 10.100.2.1. See the following screenshot.



to-BSR222

Duration: 0 00:03:53
Security: ESP - 128 Bit AES, SHA
IKE: Diffie-Hellman Group II
Compression: No Compression
Destination IP Address: 10.10.3.1
Assigned IP Address: 10.100.2.1
IPSec NAT Traversal: Inactive
Logging: Enabled
Ipsec Mobility: Disabled
Persistence: Disabled
FIPS 140-2 Mode: Disabled

Connection statistics

Bytes in:	364	Bytes out:	20803
Frames in:	7	Frames out:	398

Connection errors

Encryption:	0	Decryption:	0
Send buffers:	0	Recv buffers:	0
Packet Too Big:	0	Interface Not Ready:	0
Invalid IP Address:	0	Transport Copy:	0

Keepalive Parameters

Interval: 00:00:00 Max. Retransmissions: 0

□ Always on Top ☑ Details

3.6 Configure IP Phones

In this section, we will configure Nortel IP Phone 2004 and Nortel IP Softphone 2050. The configuration procedures are identical for any locations (any sites or main-office).

3.6.1 Configure IP Phone 2004

Using the following script to configure IP Phone 2004 in Site-1:

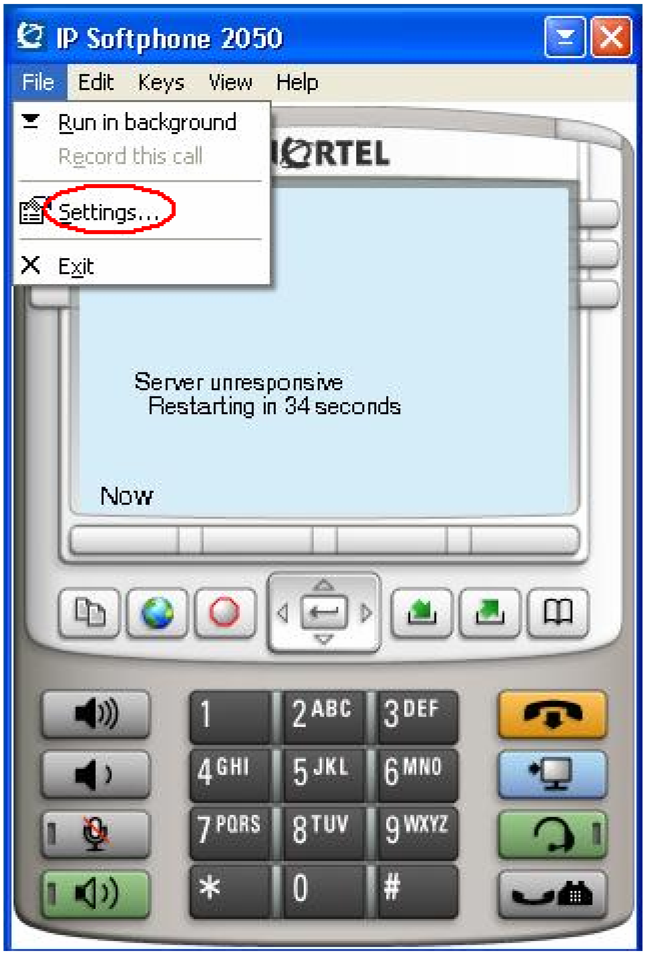
- DHCP: 1(yes)
- partial:1
- S1 IP: 192.168.1.2
- S1 Port: 7000
- S1 Action: 1
- S1 Retry Count: 2

- S2 IP: 192.168.1.2
- S2 Port: 7000
- S2: Action: 1
- S2: Retry Count: 2
- VLAN: 0 (No)
- cfg XAS: 0 (No)
- 100F-DUP: 0 (No)

3.6.2 Configure IP Softphone 2050

3.6.2.1 IP Softphone 2050 Settings

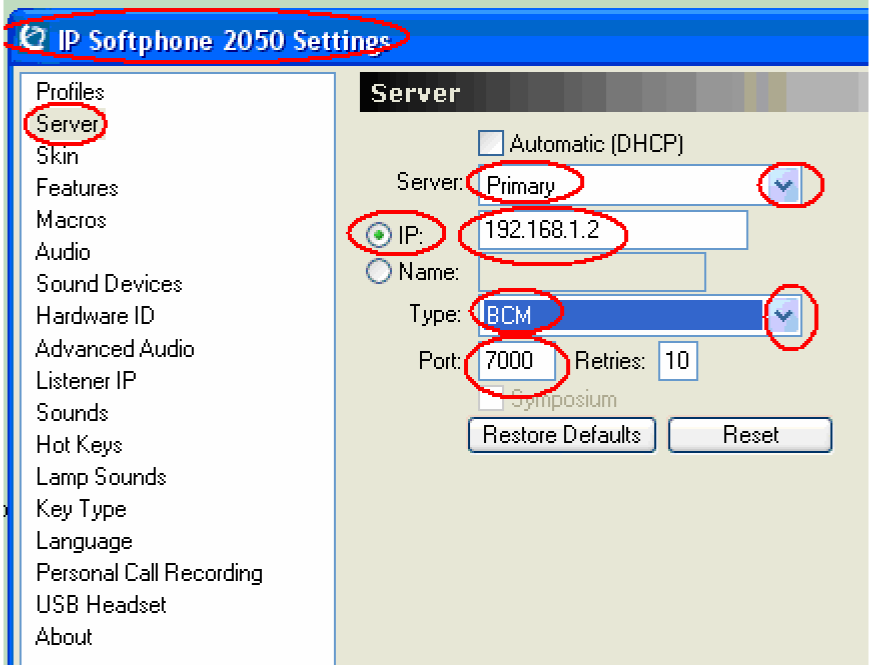
Select “Settings…” in the pull down menu of “File”. See the screenshot below:



Server unresponsive
Restarting in 34 seconds

3.6.2.2 Configure IP Softphone 2050 Settings

In the window of “IP Softphone 2050 Settings”, select “Server”, and enter the BCM50e’s IP “192.168.1.2” as the IP of the primary server. Select “BCM” as the server type, and select port of “7000”, and click “OK”. See below window for details.



IP Softphone 2050 Settings

Server

☐ Automatic (DHCP)

Server: Primary

● IP: 192.168.1.2

○ Name:

Type: BCM

Port: 7000 Retries: 10

☐ Symposium

4. Voice and Data Test

In this section, we will verify the small business VPN network connection, and check the registration status of all phones, and test voice and data over the VPN network.

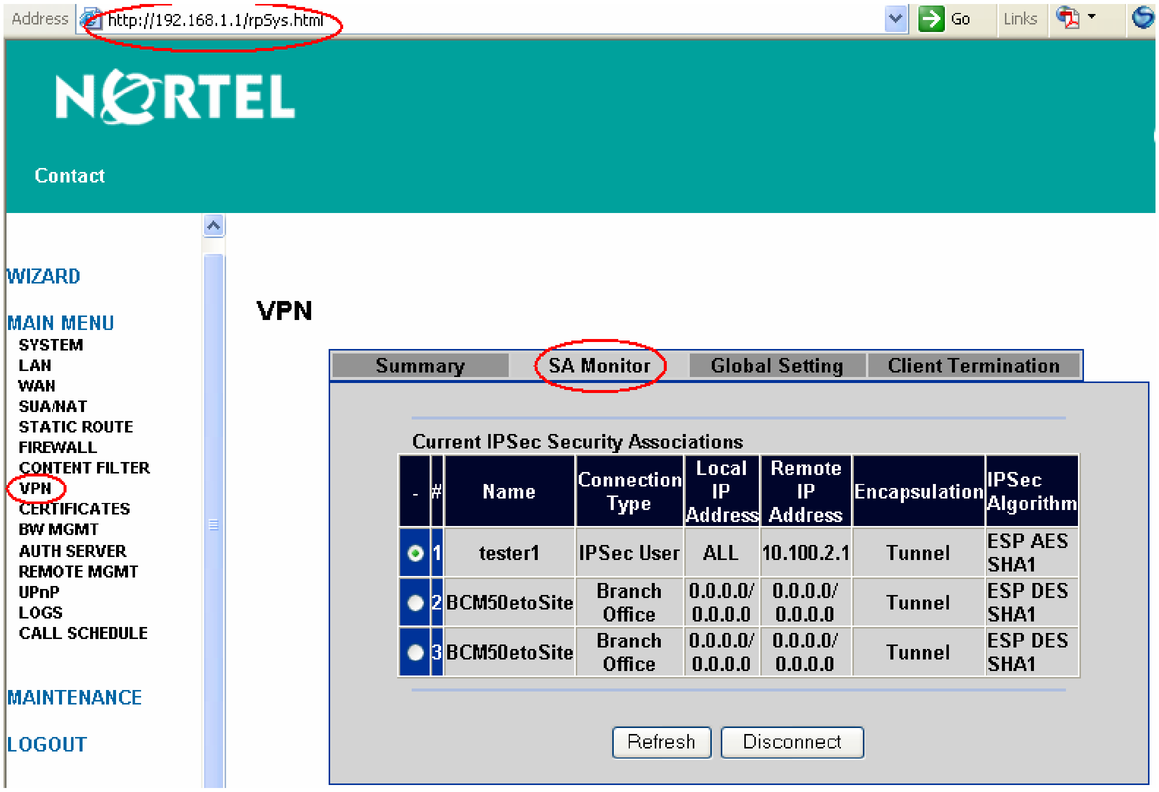
4.1.1 Verify VPN Network Connection

The VPN network connection can be verified by monitoring the VPN status on the BCM50e and SBR222.

4.1.1.1 Monitor VPN Status on BCM50e in Main-Office

Click the "SA Monitor" button in the VPN window of the BCM50e, and the screenshot below shows the VPN network is successfully established.

In this screen, there are total of 3 VPN tunnels established. The first one is the VPN client user tunnel from the road warrior's laptop. The second and third tunnels are dynamic ABOT tunnels from Site-1 and Site-2.

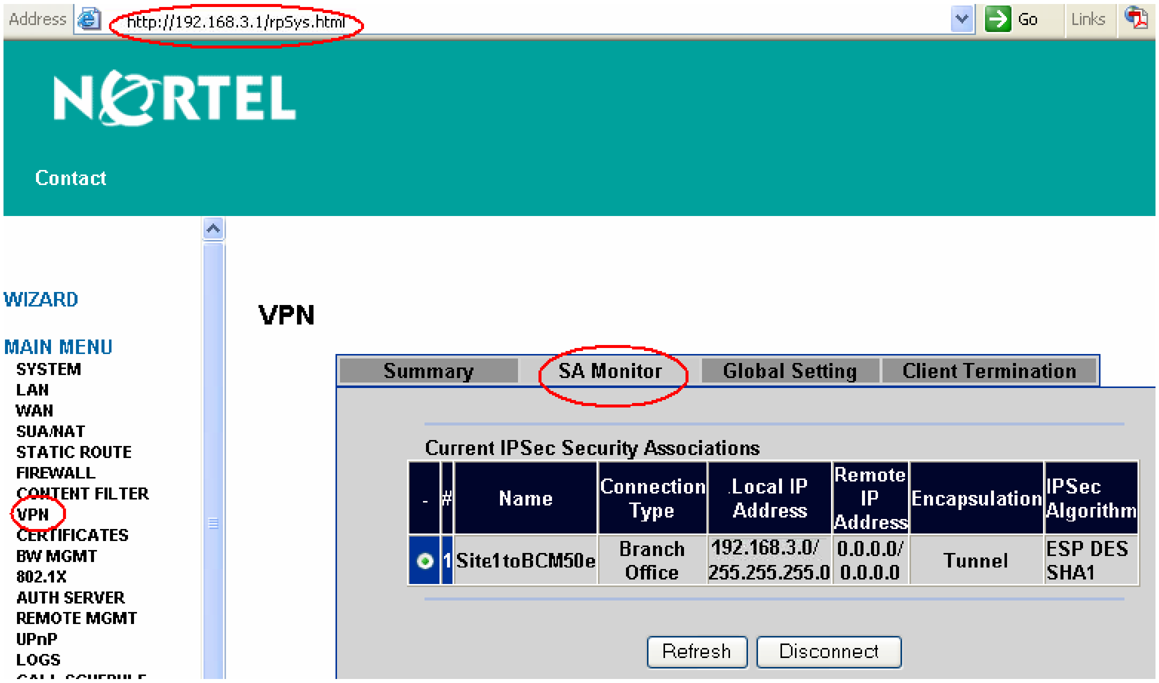


Current IPSec Security Associations

-	#	Name	Connection Type	Local IP Address	Remote IP Address	Encapsulation	IPSec Algorithm
●	1	tester1	IPSec User	ALL	10.100.2.1	Tunnel	ESP AES SHA1
○	2	BCM50etoSite	Branch Office	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1
○	3	BCM50etoSite	Branch Office	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1

4.1.1.2 Monitor VPN Status on Site-1 BSR222

Click the “SA Monitor” button in the VPN window of Site-1 BSR222, and the screenshot below shows that the ABOT VPN tunnel “Site1toBCM50e” is established.

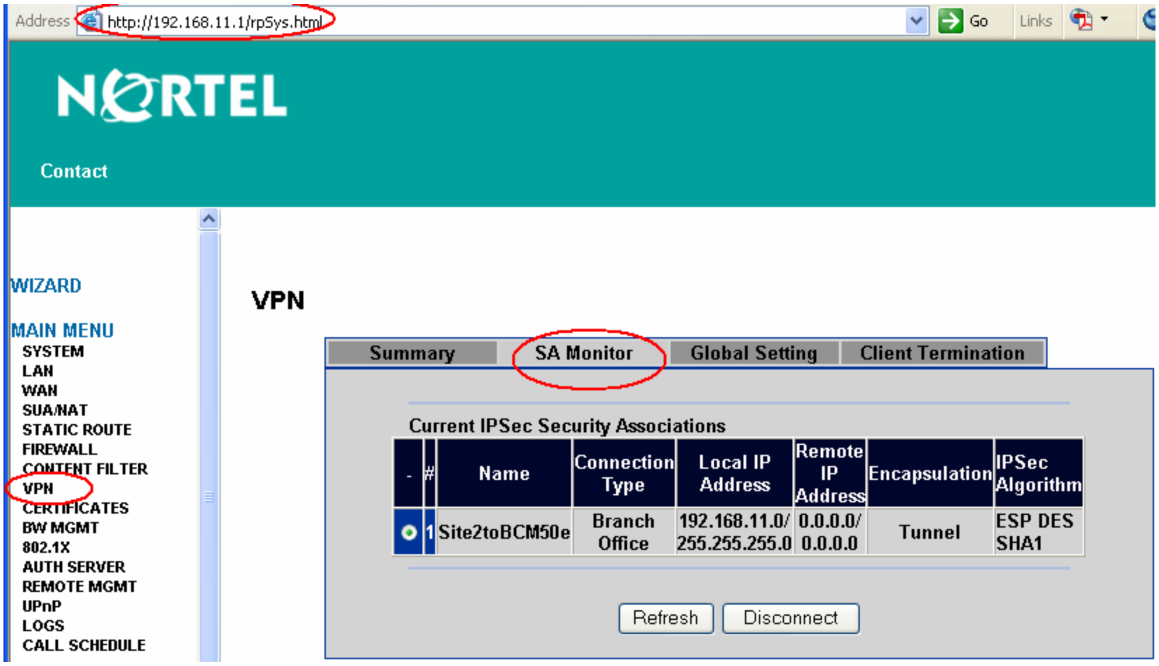


Current IPSec Security Associations

-	#	Name	Connection Type	Local IP Address	Remote IP Address	Encapsulation	IPSec Algorithm
●	1	Site1toBCM50e	Branch Office	192.168.3.0/ 255.255.255.0	0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1

4.1.1.3 Monitor VPN Status on Site-2 BSR222

Click the “SA Monitor” button in the VPN window of Site-1 BSR222, and the screenshot below shows that the ABOT VPN tunnel “Site2toBCM50e” is established.



Current IPSec Security Associations

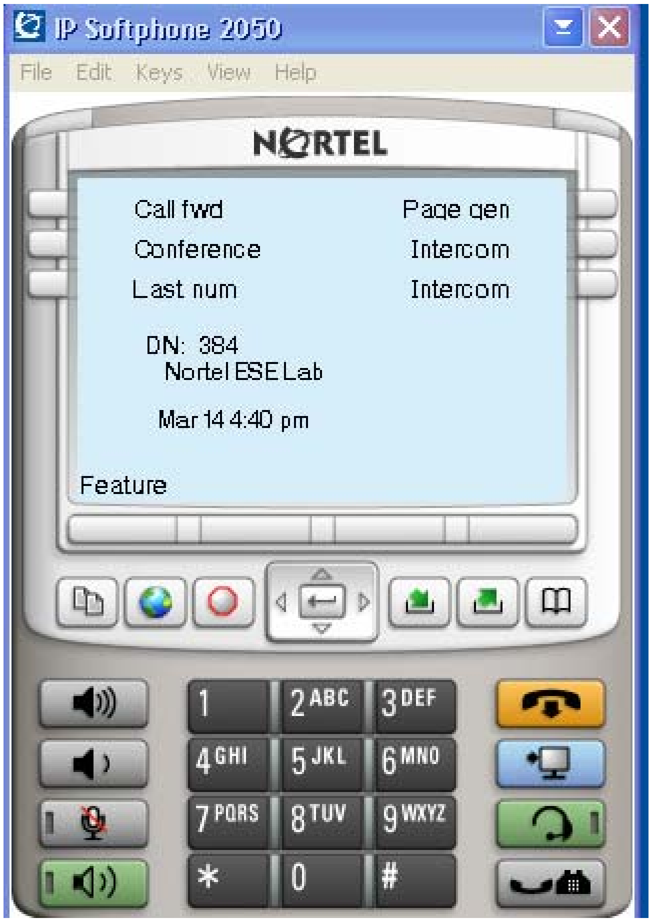
-	#	Name	Connection Type	Local IP Address	Remote IP Address	Encapsulation	IPSec Algorithm
●	1	Site2toBCM50e	Branch Office	192.168.11.0/ 255.255.255.0	0.0.0.0/ 0.0.0.0	Tunnel	ESP DES SHA1

4.1.2 Verify IP Phone Registration Status

When the VPN network connections are all up, the IP Phone 2004 and all IP Softphone 2050 are able to register to the central BCM50e over the secured VPN network.

4.1.2.1 IP Softphone 2050 Registered to BCM50e, and Assigned DN

When an IP Softphone 2050 is registered to the BCM50e, a dynamic DN is assigned by the BCM50e. “Nortel ESE Lab” logo is displayed on its screen. See the following screenshot as an example.



4.1.2.2 IP Phone 2004 Registered to BCM50e, and Assigned DN

When an IP Phone 2004 is registered to the BCM50e, a dynamic DN is assigned by the BCM50e. “Nortel ESE Lab” logo is displayed on its screen. See the following photo as an example.

4.1.3 Voice and Data Tests

Voice and data are ready to be tested after all the above configurations and verifications are successfully passed.

4.1.3.1 Test Objectives

The test objectives are to prove that:

- Secure Voice and Data are supported over VPN BO tunnels between any-any sites (including Main-office)
- Secure Voice and Data are supported over VPN client tunnels between VPN Client and any site (including Main-office)
- Full meshed Voice, phone signaling, FTP, Ping tests should be passed without error or drop.

4.1.3.2 Ping Test Results

Ping test results are shown in the table below:

- Good: ping successful with no error and no loss
- N/A: none applicable

Ping test		**PC**	pc-2	pc-4	pc-1	pc-3
		location	site2	site1	office	mobile
PC	**location**	**VPN**	BO	BO	BO	client
pc-2	site2	BO	N/A	good	good	good
pc-4	site1	BO	good	N/A	good	good
pc-1	office	BO	good	good	N/A	good
pc-3	mobile	Client	good	good	good	N/A

4.1.3.3 FTP Test Results

FTP test results are shown in the table below:

- Good: File transfer successful with no error and no packets loss
- N/A: none applicable

FTP test		**PC**	pc-2	pc-4	pc-1	pc-3
		location	site2	site1	office	mobile
PC	**location**	**VPN**	BO	BO	BO	client
pc-2	site2	BO	N/A	good	good	good
pc-4	site1	BO	good	N/A	good	good
pc-1	office	BO	good	good	N/A	good
pc-3	mobile	Client	good	good	good	N/A

4.1.3.4 Phone Signaling Test Results

Phone signaling test results are shown in the table below:

- Good: signaling is successfully and correctly started and stopped on both sides.
- busy: busy tone

Note: The DN numbers are dynamically assigned by the BCM50 during phone registration. The DN numbers below are recorded on the day when the test was conducted.

Signaling Test			PC	pc-1				pc-4	pc-2	pc-3
			location	office	office	office	site1	site1	site2	mobile
			DN	385	222	234	383	384	382	381
PC	location	DN	phone type	i2050	T7208	analog	i2004	i2050	i2050	i2050
pc-1	office	385	i2050	busy	good	good	good	good	good	good
	office	222	T7208	good	busy	good	good	good	good	good
	office	234	analog	good	good	busy	good	good	good	good
	site1	383	i2004	good	good	good	busy	good	good	good
pc-4	site1	384	i2050	good	good	good	good	busy	good	good
pc-2	site2	382	i2050	good	good	good	good	good	busy	good
pc-3	mobile	381	i2050	good	good	good	good	good	good	busy

4.1.3.5 Phone Speech Test Results

Phone signaling test results are shown in the table below:

- Good: two-way speech established, with clear sound, with good conversation flowing on both ends and with no distortion.
- N/A: none applicable.

Speech Test			PC	pc-1				pc-4	pc-2	pc-3
			location	office	office	office	site1	site1	site2	mobile
			DN	385	222	234	383	384	382	381
PC	location	DN	phone type	i2050	T7208	analog	i2004	i2050	i2050	i2050
pc-1	office	385	i2050	N/A	good	good	good	good	good	good
	office	222	T7208	good	N/A	good	good	good	good	good
	office	234	analog	good	good	N/A	good	good	good	good
	site1	383	i2004	good	good	good	N/A	good	good	good
pc-4	site1	384	i2050	good	good	good	good	N/A	good	good
pc-2	site2	382	i2050	good	good	good	good	good	N/A	good
pc-3	mobile	381	i2050	good	good	good	good	good	good	N/A

5. Reference Documentation:

- Nortel NTP: Nortel BCM50 document suite
- Nortel NTP: Nortel Business Secure Router document suite

Contact us

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

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.