

Contivity 221 ABOT
Technical Configuration Guide
for Deployments using Web GUI

Abstract

This document details a methodology for effectively configuring a large deployment of Contivity 221 ABOT configurations to Central Office locations using the Web GUI.

Revision Control

No	Date	Version	Revised by	Remarks
1	12/8/2003	1.0	Shangli Lu	Initial Draft- presentation
2	1/22/04	1.1	B. Coughlin	Update and conversion to TCG format

Copyright © 2004 Nortel Networks

All rights reserved. January 2004

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Contivity are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporate.

All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

1. INTRODUCTION 3

1.1 TARGET AUDIENCES 3
1.2 REQUIREMENTS: 4

2. CONTIVITY 221 CLIENT EMULATION 4

3. DEPLOYMENT METHODOLOGY 4

3.1 PLANNING VPN NETWORK 4
3.1.1 C221 Default Factory 5
3.1.2 Selecting BO type - ABOT 5
3.1.3 C221 Initiator ID and pre-shared key 5
3.2 PRE-BUILDING C221 CONFIGURATION FILES IN CO LAB 7
3.3 PROVIDE END-USERS WITH INSTRUCTIONS 7
3.4 DOWNLOADING CONFIGURATION FILES FROM CO LAB TO REMOTE C221 7

4. CONTIVITY C221 DEPLOYMENT EXAMPLE 8

4.1 ABC VPN DEPLOYMENT TASKS 8
4.2 NETWORK PLANNING 8
4.3 CONFIGURE CONTIVITY GATEWAY 1100 IN CO LOCATION 9
4.4 PRE-BUILD C221 CONFIG FILES FOR FIVE SITES 18
4.5 DOWNLOAD FILES FROM CO TO REMOTE BRANCH OFFICES 25

5. REFERENCE DOCUMENTATION: 32

6. APPENDIX A: TERMINOLOGY 33

1. Introduction

This document proposes a methodology for effectively configuring a large deployment of Contivity 221 ABOT configurations to Central Office locations using the Web GUI. The Contivity 221 has a unique feature called "Client Emulation" which creates a user tunnel connection to a CO. Configuring "Client Emulation" is simple and can be done by non-technical resources.

The Contivity 221 ABOT configuration requires a more complicated configuration which requires more experienced technical resources. The method covered in this document allows the configuration work to be performed in a centralized location such as a CO.

The areas covered in this document are as follows:

- Preparing the ABOT configuration files for all sites in a simulated lab environment. This requires technical resources.
- End-users configuring Client Emulation and starting the client connection to the CO. End users can perform this task.
- Downloading prepared ABOT configuration files to the Branch Office or end user location over this client tunnel. (The Contivity 221 will auto-reboot after download and activate the ABOT configuration. Then, C221 ABOT configuration is completed and established.)
- Testing the ABOT connection using PING.

1.1 Target Audiences

Enterprises and Carrier Customers, both large and small, who plan to use the Web GUI to deploy ABOT connections between Contivity 221 units and Contivity Gateways over an Internet Connection.

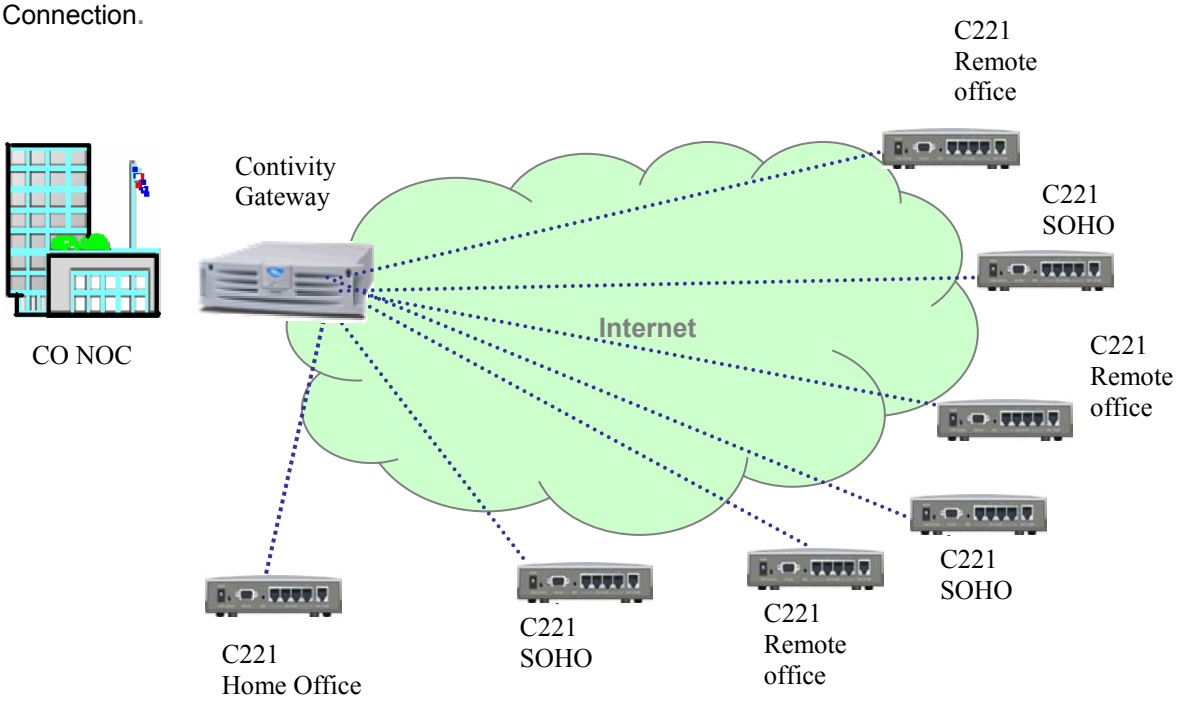


Figure 1: Deployment Scenario

1.2 Requirements:

- Microsoft PC with Internet Explorer
- The Contivity 221 must be able to access to the Internet using it's Ethernet connection.
- Static IP address for the Contivity Gateway in the Central Office location.
- Management tools are not required (e.g. CCM).

2. Contivity 221 Client Emulation

The Contivity 221 has a unique feature called “Client Emulation”. This feature allows a connection to a remote Contivity Gateway as a user (hard client). An IPSec user tunnel will be established between the Contivity 221 and the Contivity Gateway when the connection is initiated from C221. “Client Emulation” is also called “Contivity hard client emulation” or “Contivity VPN Client”. “Client Emulation” uses the IPSec protocol only.

In the “Client Emulation” configuration, there is a many-to-one NAT filter from the C221 private addresses and the C221 public address. Therefore, traffic sent from the Contivity Gateway private network to the C221 private network does not make it further than the C221 assigned public address. In this way the central site is not required to learn or manage the remote sites’ private networks. To set the Contivity Client rule to active, all other VPN rules must be set to inactive**.**

Configuring “Client emulation” is very simple. End-users need to know only 3 parameters: User-name, Password, and gateway address.

3. Deployment Methodology

This next section will cover the following six steps in detail:

1. Planning the VPN network before deployment
2. Pre-building the C221 ABOT configuration files (rom-0) for all sites
3. Providing remote end-users with simple instructions to setup & start C221 Client tunnel.
4. Downloading or FTPing pre-built configuration file from CO to remote C221 over client tunnel (The C221 unit will auto-reboot to activate the new configuration).
5. Testing the ABOT tunnel using PING.

3.1 Planning VPN Network

This step includes various items such as determining Network topology, size, location, device model, bandwidth, and number of users. Specific tasks are:

-Obtain the static IP and gateway address for Contivity gateway in CO from the ISP

-Determine the private IP network addresses for each site. Private IP addresses can be selected from:10.x.x.x,172.16.x.x-172-31.x.x, 192.168.x.x. Ensure each site is assigned a unique IP address.

-Reserve 192.168.1.0/24 for using only by C221 factory-default configuration to avoid potential address conflicts.

-Define subnet size for each site. A class C address using 8 bits is commonly used since it is easy to manage. A Class mask of 255.255.255.0 allows up to 254 hosts.

-Plan unique “Initiator ID” for each site. Make the ID meaningful for future troubleshooting, and event logging. For example circuit or site identifiers, or phone numbers can be used

3.1.1 C221 Default Factory

The Contivity 221 is shipped with a default factory configuration. With this default configuration the DHCP server on its private interface is enabled with the address range from 192.168.1.3 to 192.168.1.254/24. PCs connecting to the C221 private interface will be assigned an IP address in the same subnet if they have dynamic addressing set.

The C221 has a default management interface address of 192.168.1.1/24 with a default password of “setup”. The factory default configuration has the DHCP client enabled on the public interface. When connecting to an ISP, a dynamic public IP address will be assigned. This default configuration allows end users to access to the Internet in a plug and play fashion.
The C221 hard client is designed as a 3DES client, and uses 3DES/SHA to connect to the CO Contivity user group. This method is the most secure algorithm of SA offered in this release.

3.1.2 Selecting BO type - ABOT

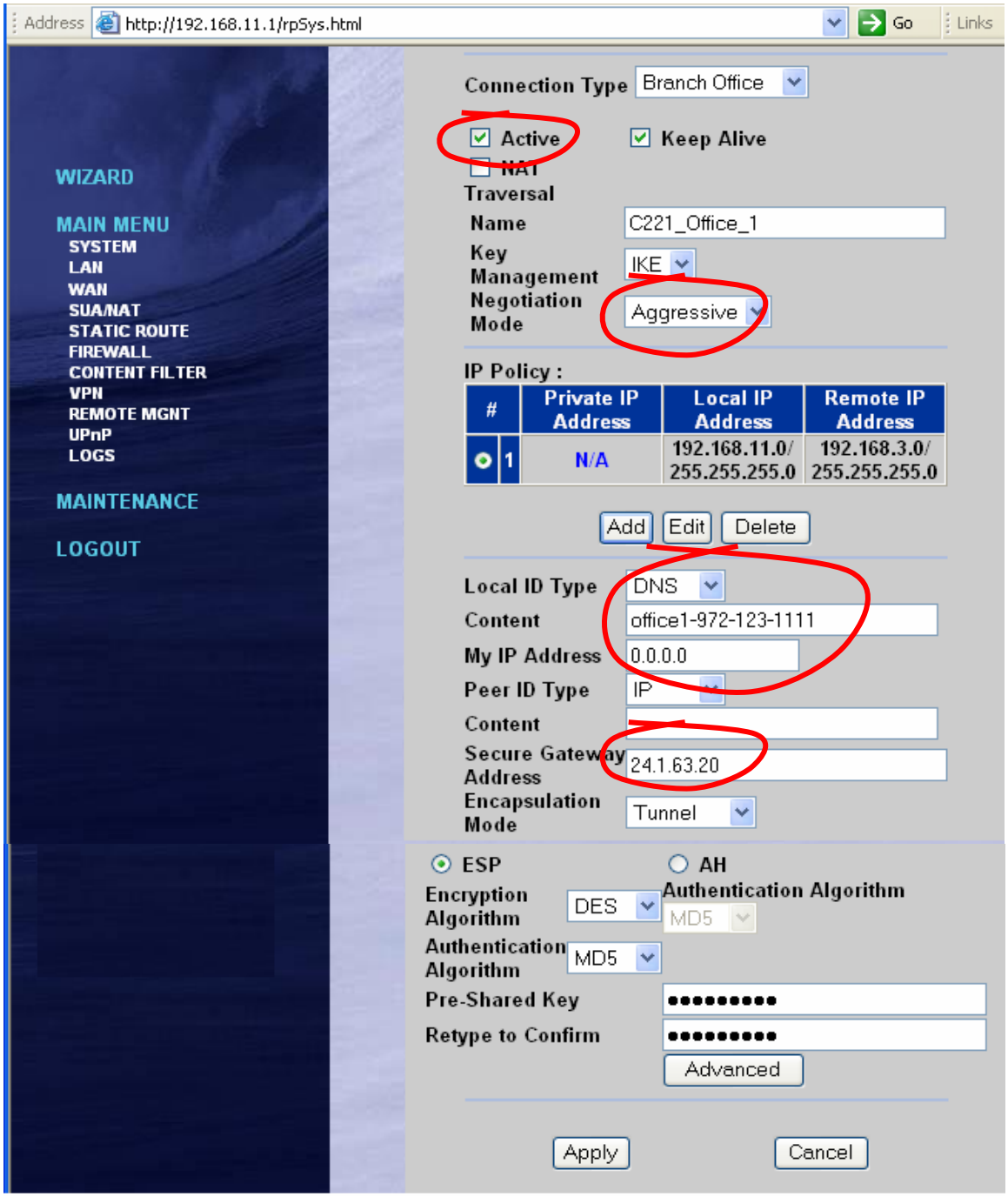
ABOT should be selected since the C221 public interface is using a dynamic IP address from the ISP. (Peer-to-peer branch tunnels are not applicable since these use main mode for the IKE Phase 1 exchange. Main mode can only be used if both VPN Gateways have fixed IP addresses.)

For ABOT, only IPSEC tunnel type is supported. The IPSEC tunnel will be established using pre-shared secret key and initiator ID. The ABOT tunnel uses static routing, since dynamic routing over an IPSec tunnel is not available in the C221 current release.

With ABOT, one side must be configured as the initiator and the other as the responder. The C221 should be configured as “initiator” with the Contivity Gateway in CO as the “responder”. Only the Initiator (C221) can bring up the tunnel.

3.1.3 C221 Initiator ID and pre-shared key

With aggressive negotiation mode, the C221 uses “Initiator ID” to establish ABOT. The “Initiator ID” on the C221 is configured in the “content” field as a DNS domain name. The DNS domain name in the “Initial ID” field is used for identification purposes only and does not need to be a real domain name. The C221 DNS domain name may have up to 31 characters. When using special characters, make sure they are accepted by both CO and BO. Leave “My IP address” set to 0.0.0.0.



The “Initiator ID” configured on the C221 must be identical to the ID configured on the CO Contivity Gateway. The Pre-shared key that is configured on the C221 must be identical on both sides (BO and CO).

3.2 Pre-building C221 Configuration Files in CO Lab

This step should be performed in the CO by technical resources who are trained and familiar with the Nortel Contivity product suite.

1) Set up the lab environment to simulate the real network. (using the same IP address for remote Contivity Gateway and a similar network topology).

2) Configure the Contivity Gateway (adding BO groups/connections, User-groups and IP-pool).

3) Configure the C221 LAN with planned IP address and subnet.

4) Configure the C221 with:
- one client tunnel (inactive).
- one BO tunnel (active).
- static routing.

5) Test the configuration in the lab environment ensuring the remote connection to the CO Contivity Gateway can be established and there are no errors. Validate download and activation of C221 configuration file, then start and test ABOT tunnel.

6) Save the configuration file to local computer disk and rename it.

7) Repeat the above procedures for each CO and remote site. Validate each configuration

3.3 Provide End-Users with Instructions

Provide the remote end-users with very simple instructions for establishing the initial connection. It is best to distribute the instructions by FAX, phone, or mail. The instructions for setting up the C221 Client tunnel should contain the following information at a minimum:

– Username (configured in gateway user-group)
– Password (pre-shared key)
– CO gateway address for PING validation test.
-- Press “Connect” button to start connection

Add additional scheduling or contact information as required.

3.4 Downloading Configuration Files from CO lab to remote C221

When the C221 hard client connection has been established, CO Technicians will then download the pre-built configuration file to the remote C221 using the GUI “maintenance->Restore” tool or the FTP command line.

When the download is completed, the remote C221 will reboot automatically to activate the new configuration file. Following the reboot, a ping from the C221 to the Contivity gateway will bring up the ABOT tunnel. Repeat the same procedure for each site. Refer to the following Section 4 for detailed configuration examples.

4. Contivity C221 Deployment Example

Company ABC has one small corporate center with five remote branch offices. They plan to build a VPN (ABC VPN) using ISP Internet services and Nortel Contivity Gateways. The remote offices have access to the Internet. The remote offices need access to private servers in the CO Headquarters location via VPN.

ABC purchased 6 Contivity 221 units and one Contivity 1100 Gateway from Nortel. The Contivity units shipped directly to the remote locations with default factory configurations.

4.1 ABC VPN Deployment Tasks

Similar to the steps in Section 3.0, the following steps are completed:

1. **Network planning**
2. **Configure Contivity gateway C1100**
3. **Pre-build five BO-config-files in CO**
4. **Download config file from CO to BO**
5. **Repeat the procedure for all sites**

4.2 Network planning

- Network topology: hub-spoke, 1x C1100 gateway, 5xC221 BOs
- Connectivity: one ABOT tunnel and one Client tunnel per C221 BO
- BO IP address: 192.168.x.0/24, 192.168.x.1 for management
- Initiator ID structure: office#-areacode-phone#
- Obtained IP from ISP: 24.1.63.20, gateway: 24.1.48.1
- IP-pool for user group: 172.16.10.1-172.16.10.5
- Software level C1100 V04_80.124, and C221 VE221_2.0.0.0.013

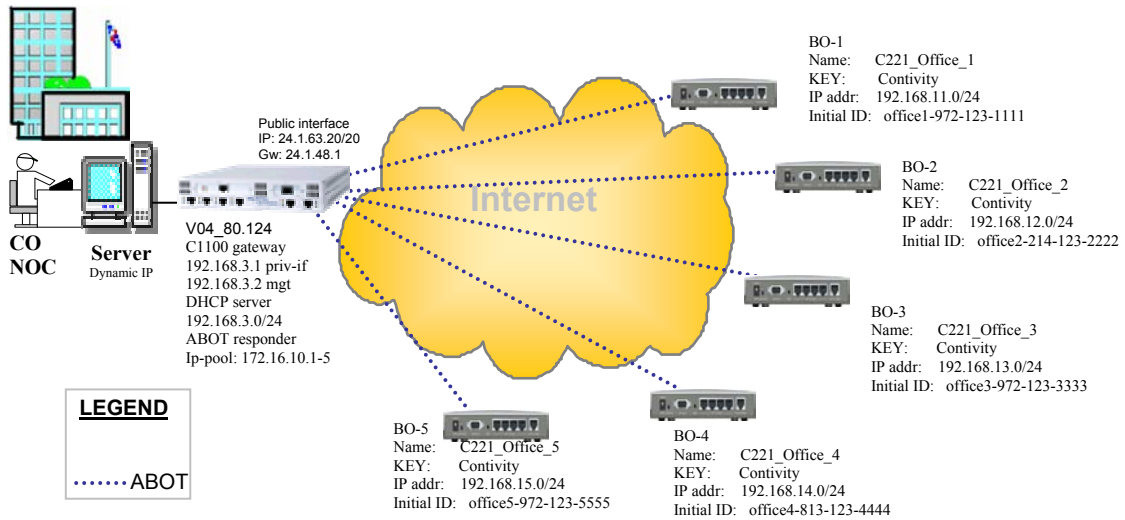
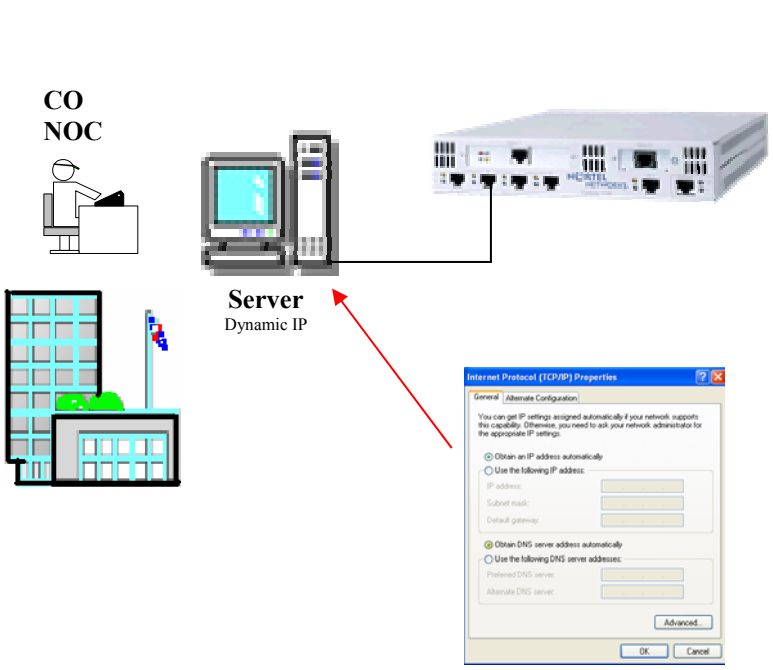


Figure 2: Sample ABC Network

4.3 Configure Contivity Gateway 1100 in CO Location



V04_80.124
C1100 gateway
192.168.3.1 priv-if
192.168.3.2 mgt
DHCP server
192.168.3.0/24
ABOT responder
Ip-pool: 172.16.10.1-5

Figure 3: Reset of Factory Defaults

Configure IP address & DHCP for C1100:

STEP-1: Reset C1100 to Factory Default (V04_80.124), open web GUI.

STEP-2: configure IP addresses for management and private interface (address and mask are determined during the phase of Network planning)

Slot 0, Port 1, Private LAN
Management IP Address = 192.168.3.2, (Subnet Mask = 255.255.255.0)
Interface IP Address = 192.168.3.1
Subnet Mask = 255.255.255.0

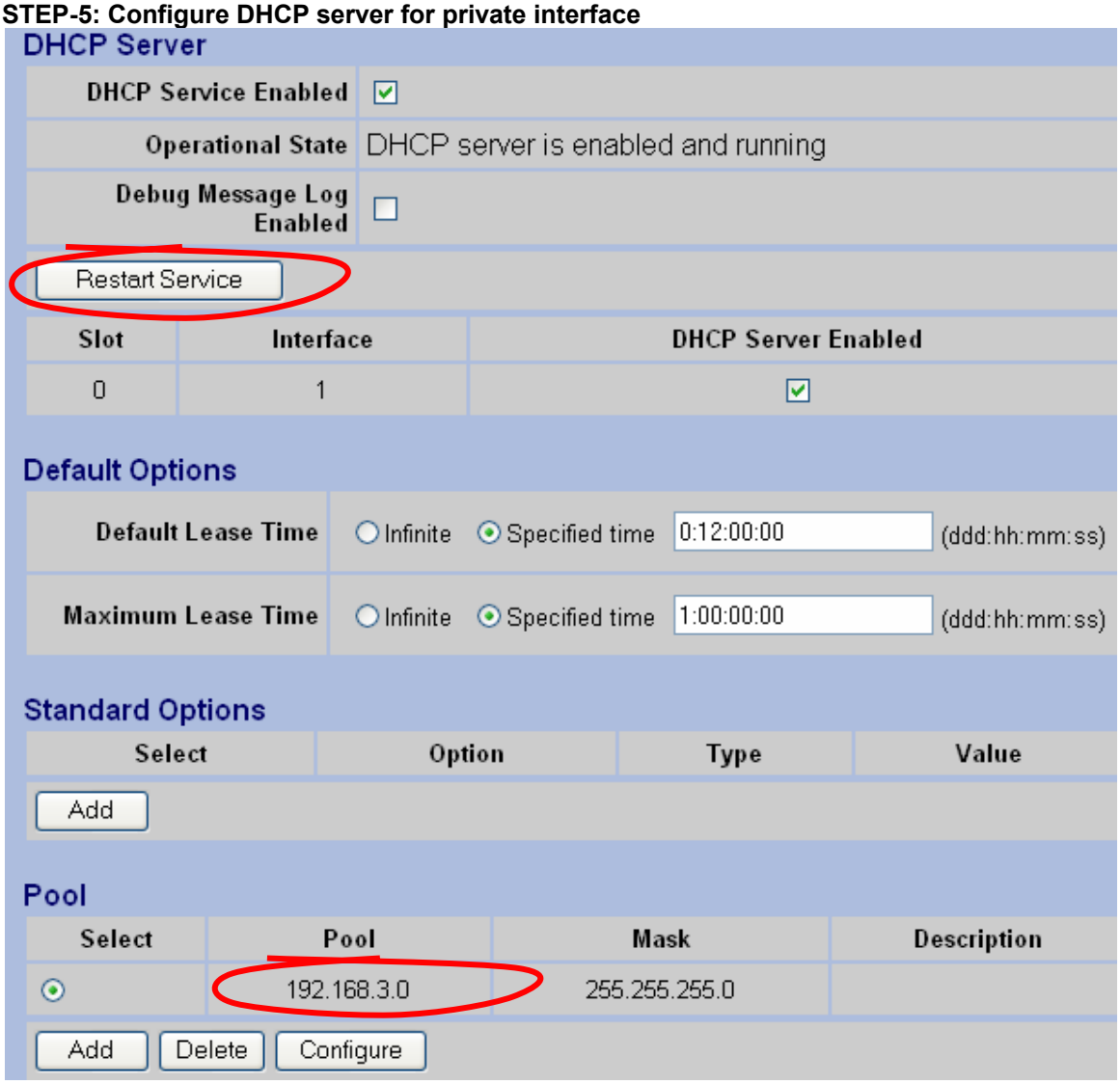
STEP-3: Configure public interface (must obtain IP address and mask from ISP)

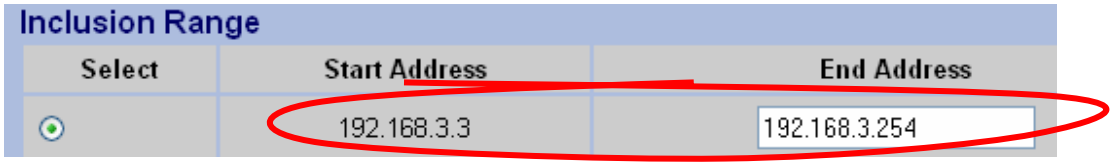
Slot 1, Port 1, Public LAN
IP Address = 24.1.63.20
Subnet Mask = 255.255.240.0
Speed/Duplex = AutoNegotiate

STEP-4: Configure public default gateway (must obtain gateway address from ISP)

Default Public Route Menu
0) Gateway IP Address = 24.1.48.1
Cost = 10
A) Add New Gateway
R) Return to the Main Menu

STEP-5: Configure DHCP server for private interface





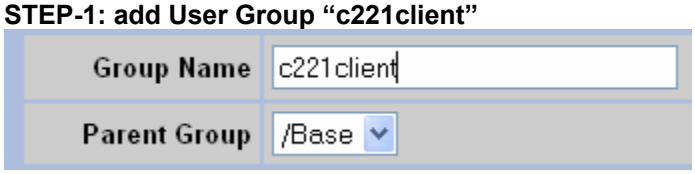
STEP-6: Renew PC ip address

When the DHCP server is configured, press “restart service” button. On the PC, to renew the IP address, issue the following commands:

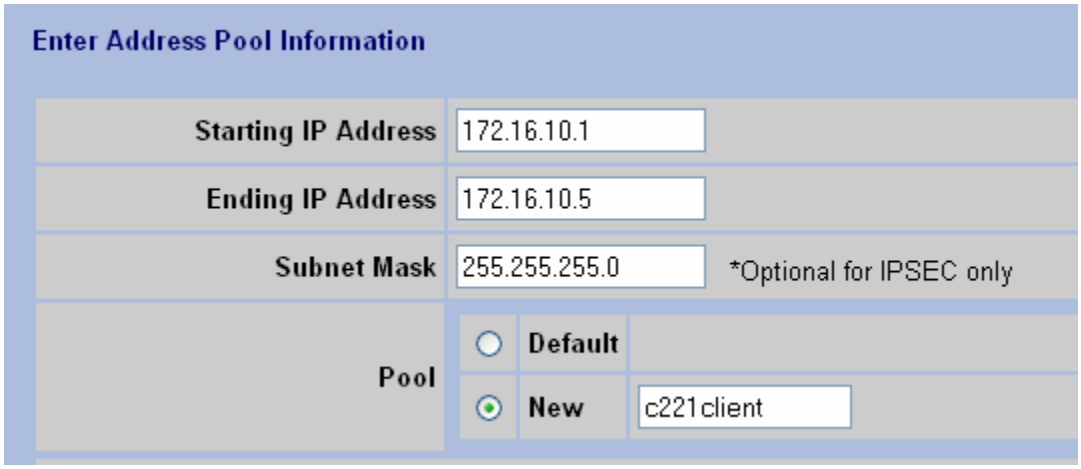
Ipconfig /release
Ipconfig /renew

Configure User Group for C1100

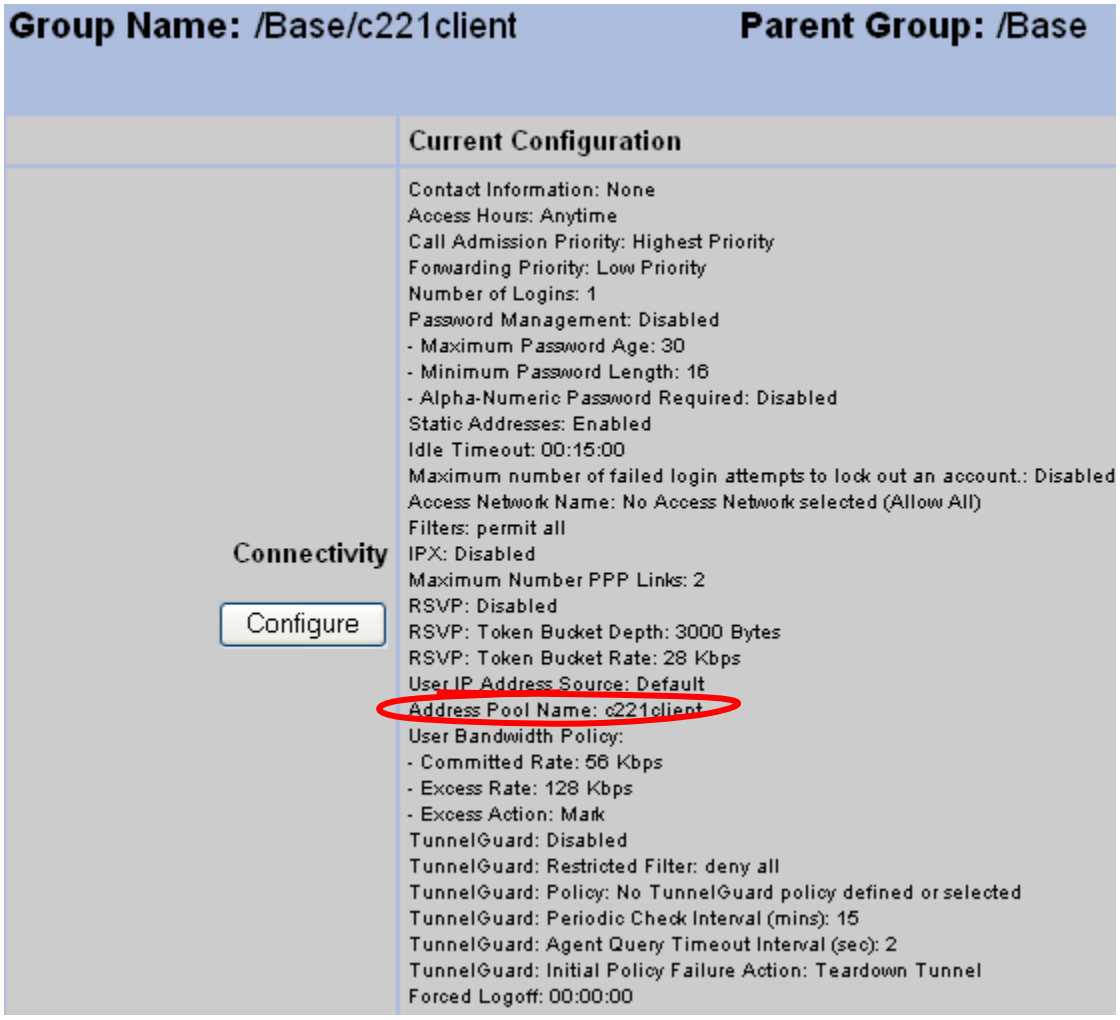
STEP-1: add User Group “c221client”



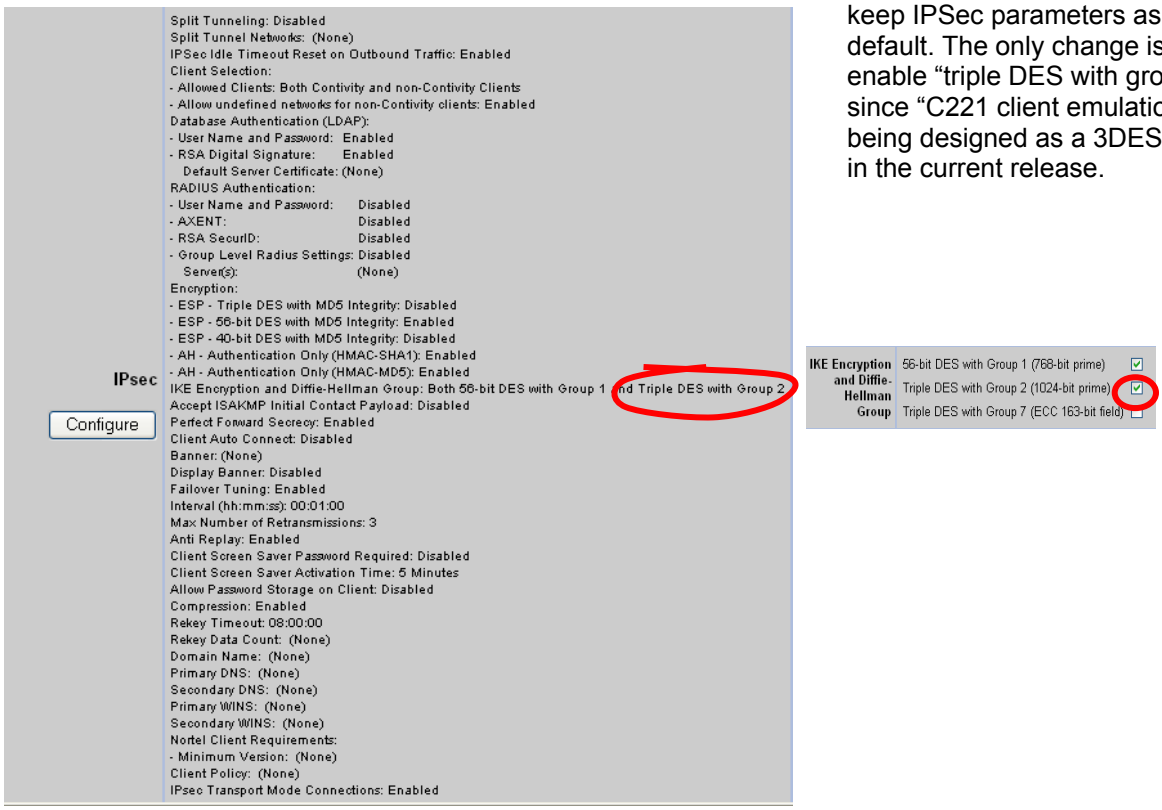
STEP-2: add IP-Pool “c221client”



STEP-3: set IPSec connectivity with ip-pool "c221client" , keep the rest as default

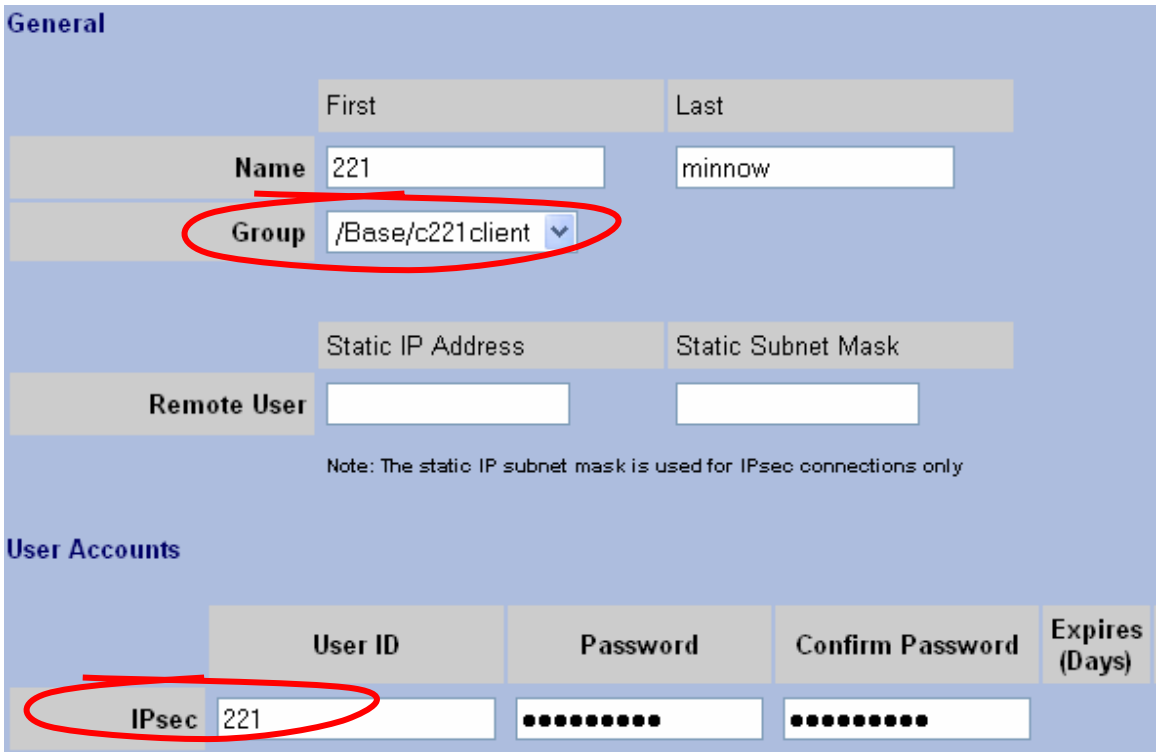


STEP-4: set IPSec parameter for interworking with C221 Client Emulation



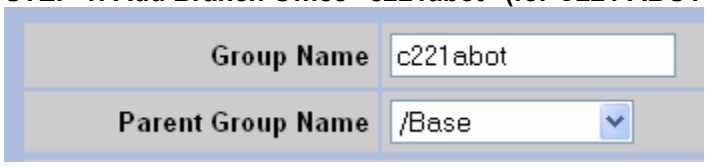
To interwork with the C221 client, keep IPSec parameters as factory default. The only change is to enable “triple DES with group 2”, since “C221 client emulation is being designed as a 3DES client in the current release.

STEP-5: Add a user to group "c221client", the password is "Contivity", userID is "221" (this group is for VPN connection by C221 hardware clients)

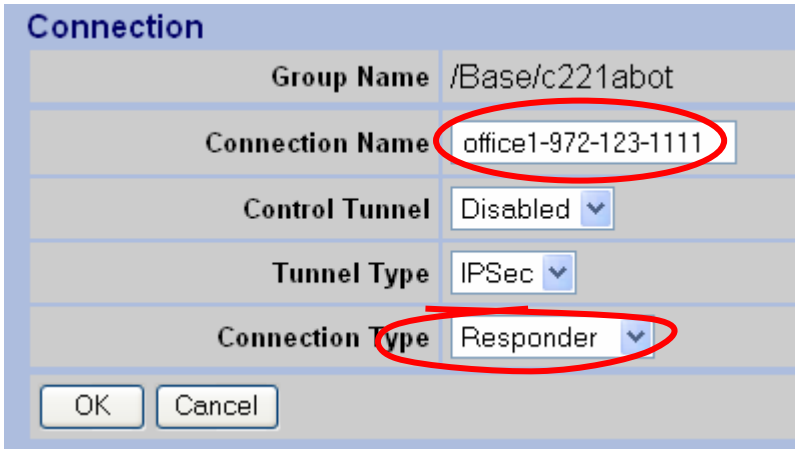


Configure BO group for Contivity 1100

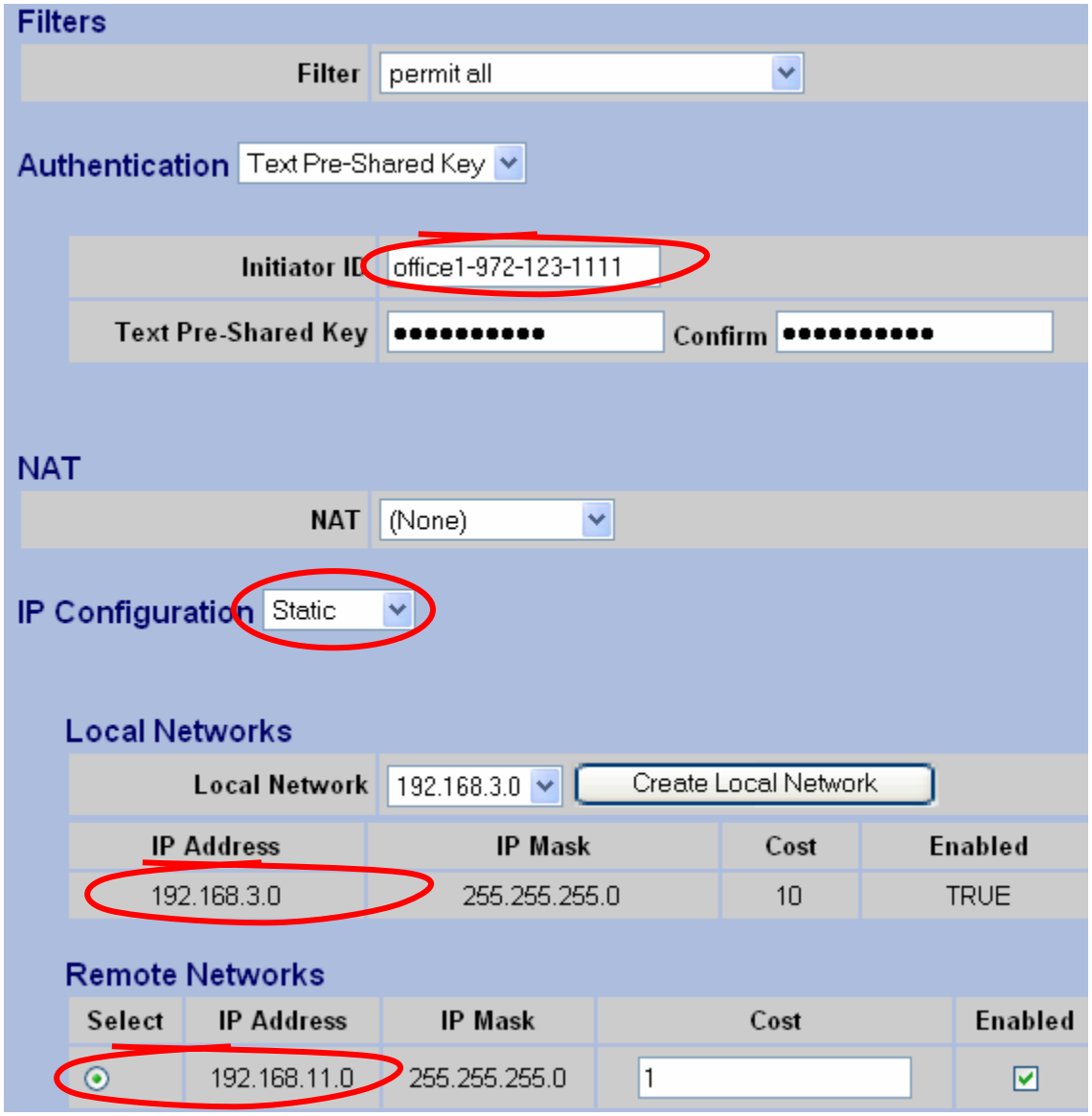
STEP-1: Add Branch Office "c221abot" (for C221 ABOT connections)



STEP-2: add connection "office1-972-123-1111" under group "c221abot" define connection type as "responder", and add each connection per site.



STEP-3: Configure "Initiator ID", pre-shared Key "Contivity", local and remote network



STEP-4: Configure ABOT group parameters
To interwork with the C221 ABOT, keep all the parameters in IPSec and Connectivity as factory default (V04_80.124).

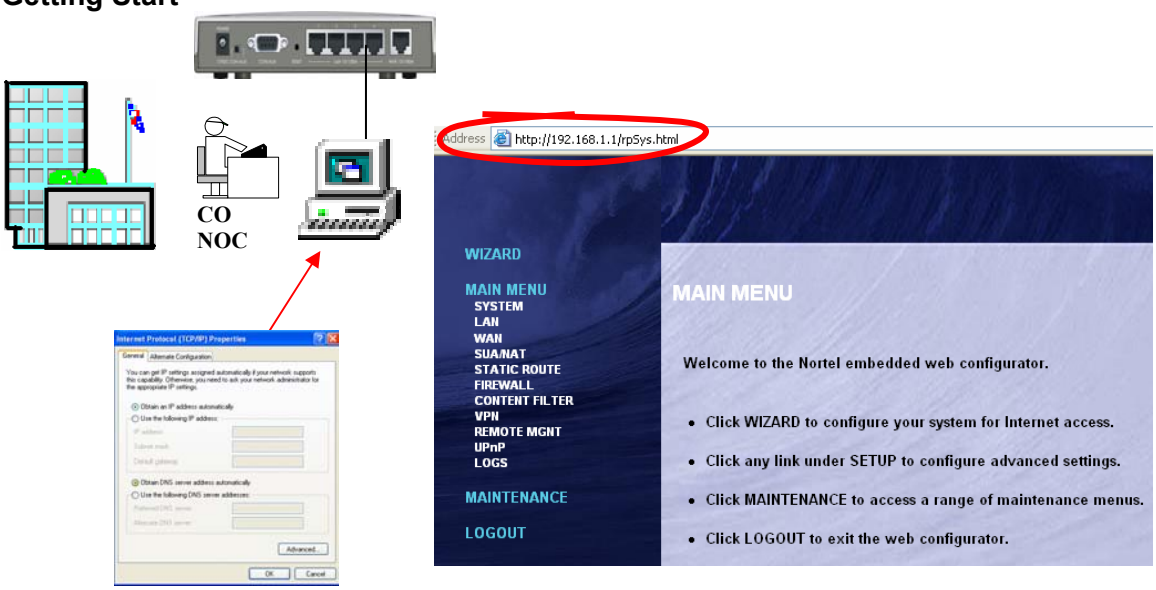
Group Name: /Base/c221abot **Parent Group: /Base**

	Current Configuration
Connectivity Configure	Nailed Up: Enabled Access Hours: Anytime Call Admission Priority: Highest Priority Forwarding Priority: Low Priority Idle Timeout: 00:15:00 Forced Logoff: 00:00:00 RSVP: Disabled RSVP: Token Bucket Depth: 3000 Bytes RSVP: Token Bucket Rate: 28 Kbps Branch Office Bandwidth Policy: - Committed Rate: 56 Kbps - Excess Rate: 128 Kbps - Excess Action: Mark
IPsec Configure	Encryption: - ESP - Triple DES with MD5 Integrity: Disabled - ESP - 56-bit DES with MD5 Integrity: Enabled - ESP - 40-bit DES with MD5 Integrity: Disabled - AH - Authentication Only (HMAC-SHA1): Enabled - AH - Authentication Only (HMAC-MD5): Enabled IKE Encryption and Diffie-Hellman Group: 56-bit DES with Group 1 (768-bit prime) Vendor ID: Enabled Aggressive Mode ISAKMP Initial Contact Payload: Disabled Perfect Forward Secrecy: Enabled Compression: Enabled Rekey Timeout: 08:00:00 Rekey Data Count: (None) ISAKMP Retransmission Interval: 16 ISAKMP Retransmission Max Attempts: 4 Keepalive interval: 00:01:00 Keepalive (On-Demand connections): DISABLED Anti Replay: ENABLED

4.4 Pre-build C221 config files for five sites

• Start from Branch-Office-1
• Change LAN IP
• Build Client tunnel
• Build ABOT tunnel
• LAB verification
• Save and rename configuration file
• Repeat the above procedure for each office

Getting Start



Make sure the C221 is set to factory defaults (VE221_2.0.0.0.013). Connect PC to the Contivity 221 private interface. Make sure the PC is configured with dynamic IP and the C221 default IP address is 192.168.1.1, the default DHCP ip range is 192.168.1.0/24, and the default Password is: "setup".

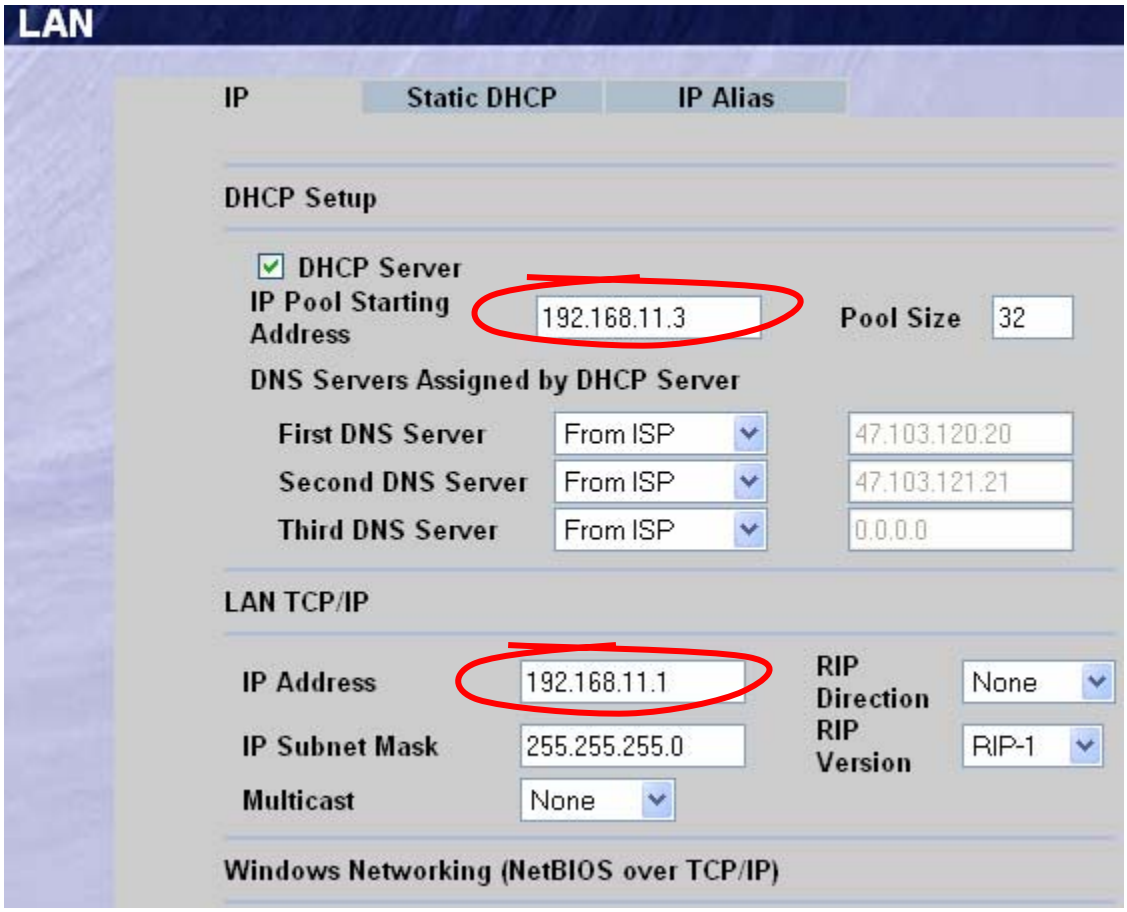
On the PC, open Web GUI to access the C221 with the default address of : http://192.168.1.1

Build two tunnels for each site (starting from Branch-Office-1)

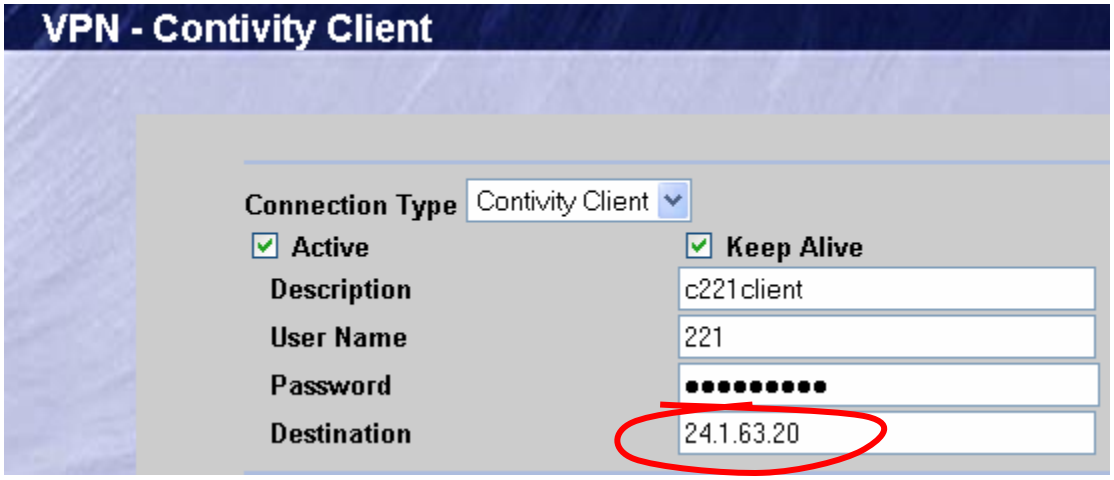
- Client tunnel, make it inactive
- ABOT tunnel, make it active
- Save the configuration file rom-0 to the PC disk and rename the file as “office1-972-123-1111rom-0”.

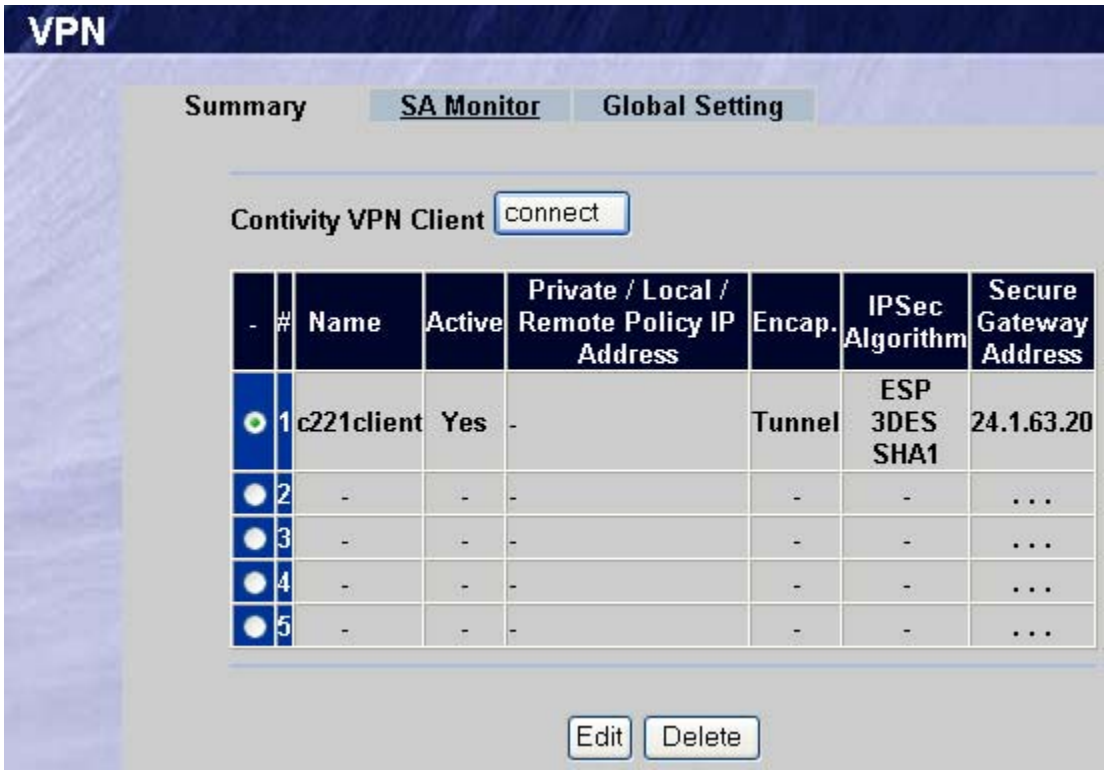
Change LAN IP
BO-1
Name: C221_Office_1
KEY: Contivity
IP addr: 192.168.11.0/24
Initial ID: office1-972-123-1111

Change default LAN IP 192.168.1.0/24 to 192.168.11.0/24 for BO-1



Configure Client

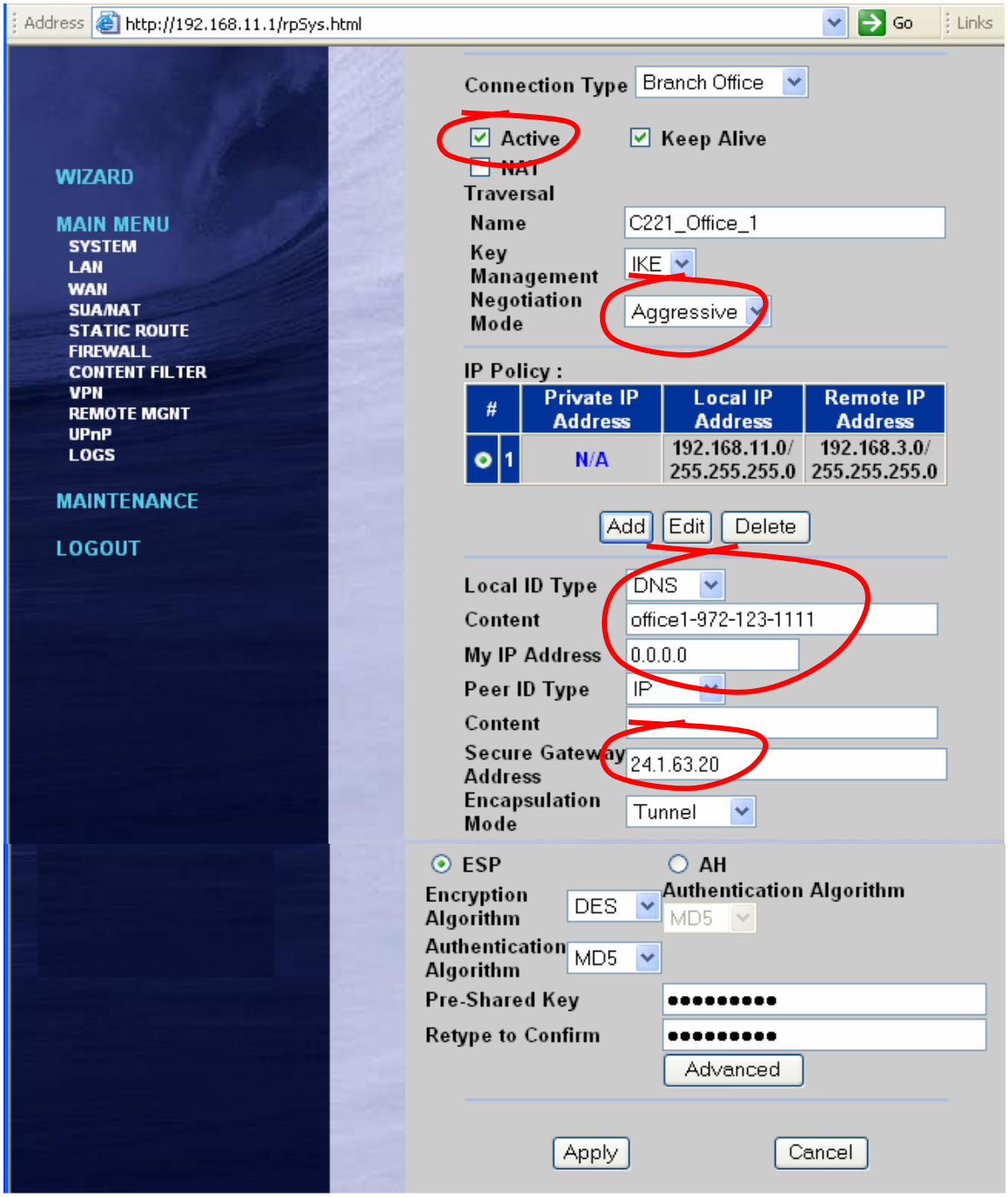




Configure ABOT

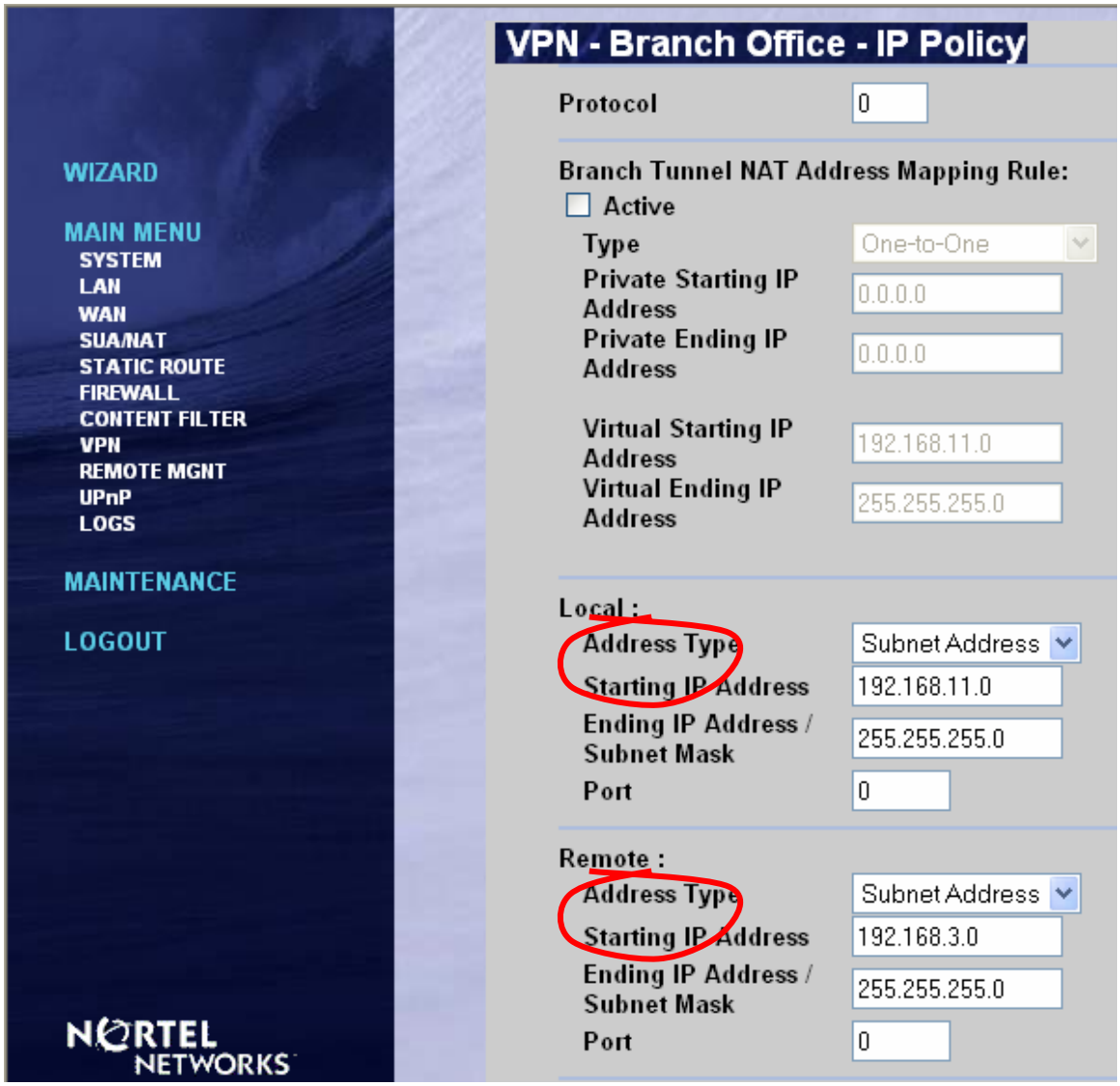
Aggressive mode
DNS = office1-972-123-1111
My IP = 0.0.0.0
Pre-shared key = Contivity
Gateway = 24.1.63.20

Note: The C221 does not allow two active tunnels to the same destination. To activate BO, you must de-activate client emulation first.



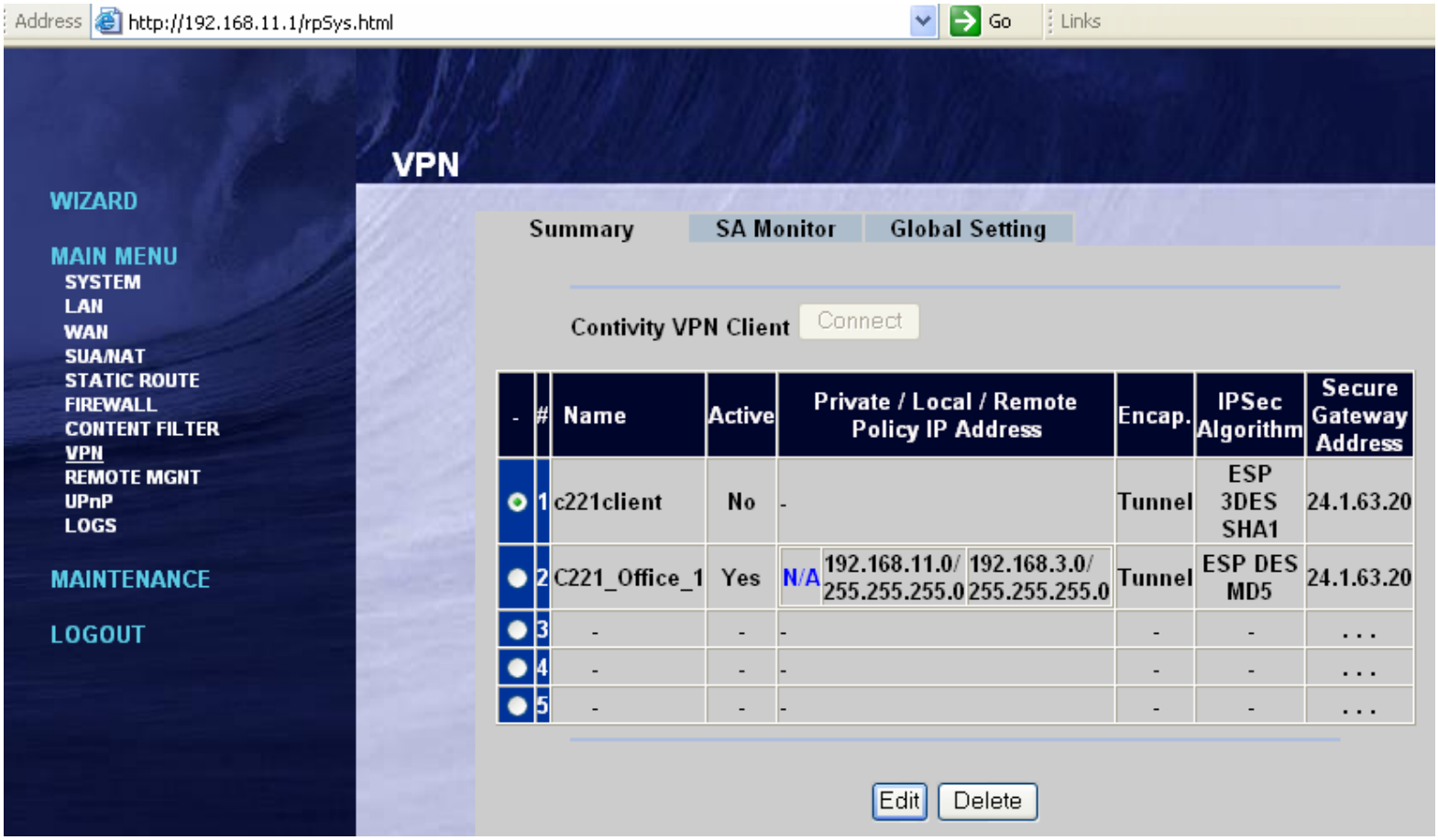
Configure Static routing

Build an ABOT tunnel using static routing.



Two tunnels were built for Branch-office-1.

Note: The C221 does not allow two active tunnels to the same destination. To activate BO, you must de-activate client emulation first.



LAB Verification

1: Set up verification lab as shown below
2: Activate and start Client connection from C221 by clicking “connect”
3: Ping from PC-S3 to PC-S4 (troubleshoot until ping is successful)
4: Activate and start ABOT connection by issuing ping from PC-S3 to PC-S4 (troubleshoot until ping is successful)

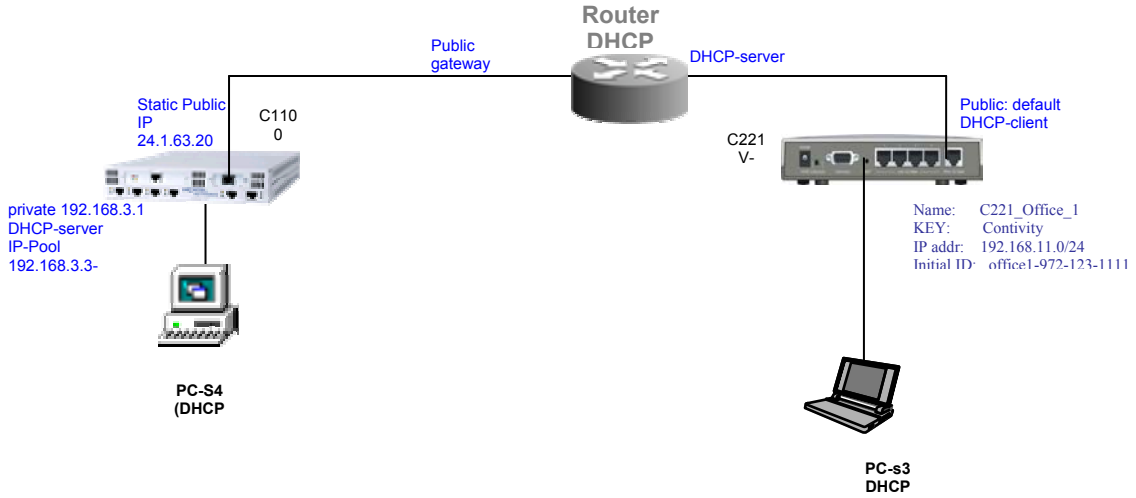
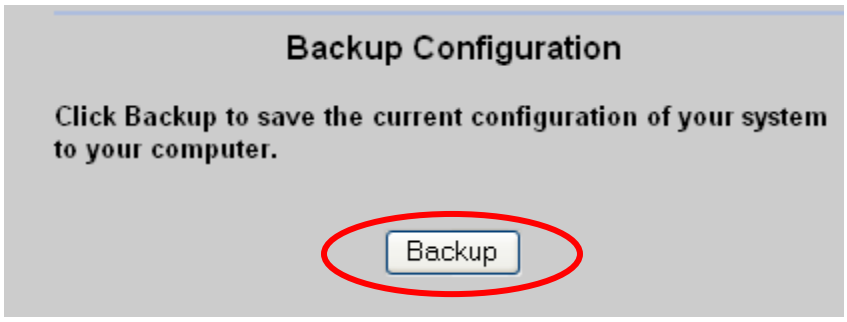


Figure 4: Verification Lab Setup

Save Configuration file:



Once lab verification passes, use “maintenance” to back up the configuration file to the local disk. Before performing backup, make sure that the configuration has ABOT activated and client de-activated. This will help to bring up ABOT tunnel when the file is downloaded to the remote office.

- The file saved is named as: office1-972-123-1111rom-0

Repeat the steps to create configuration files for all remote sites, then rename and store them:

office2-214-123-2222rom-0
office5-972-123-5555rom-0
office4-813-123-4444rom-0
office3-972-123-3333rom-0
office1-972-123-1111rom-0

4.5 Download Files from CO to Remote Branch Offices

- Connect Contivity devices to the Internet
- Branch Office-1 received configuration information
- Set up C221 hard client
- Connect C221 to CO
- C221 ping CO continuously
- Download configuration file from CO to remote BO
- Auto-reboot

Connect to Internet

Note: This deployment procedure was tested in the topology shown below. Other Customer topologies may vary.

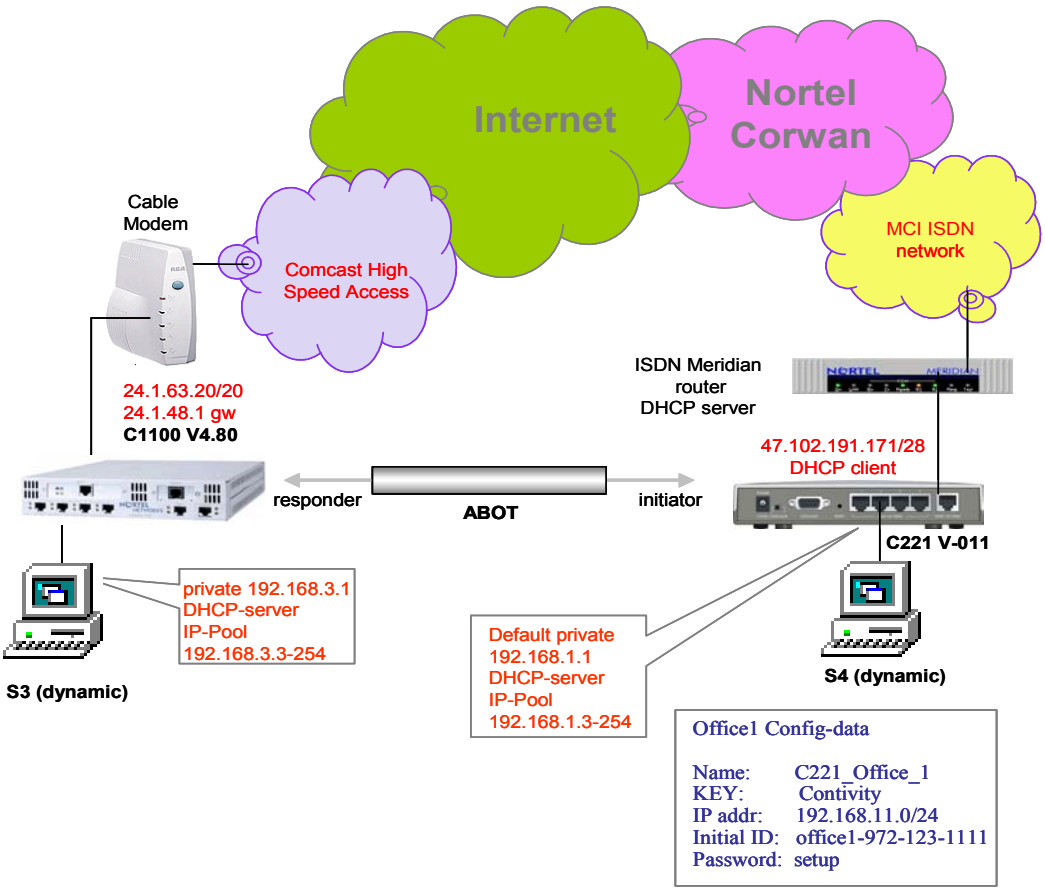


Figure 5: Remote C221 Connection

Preparation:
-Connect devices to network as shown
-Pass Office1 (C221) Config-data as shown
-C221 in Office1 is at factory default settings

Branch Office-1 configuration information

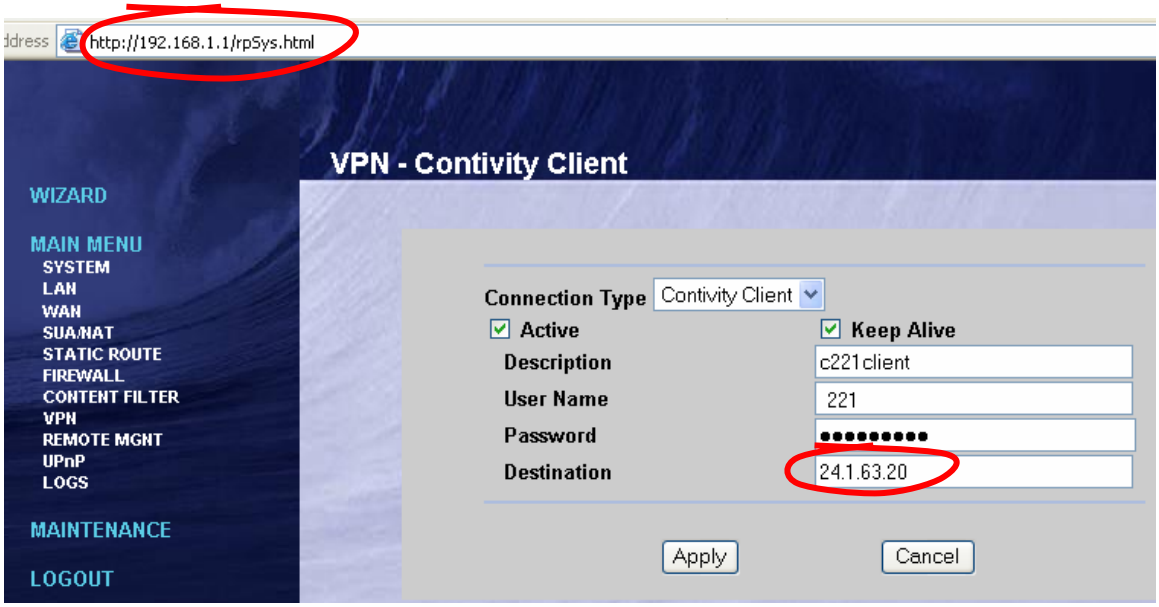
Below is the minimum information required by a branch office:

Branch-office-1

User name:	221
password:	Contivity
gateway	24.1.63.20
CO address:	192.168.3.1

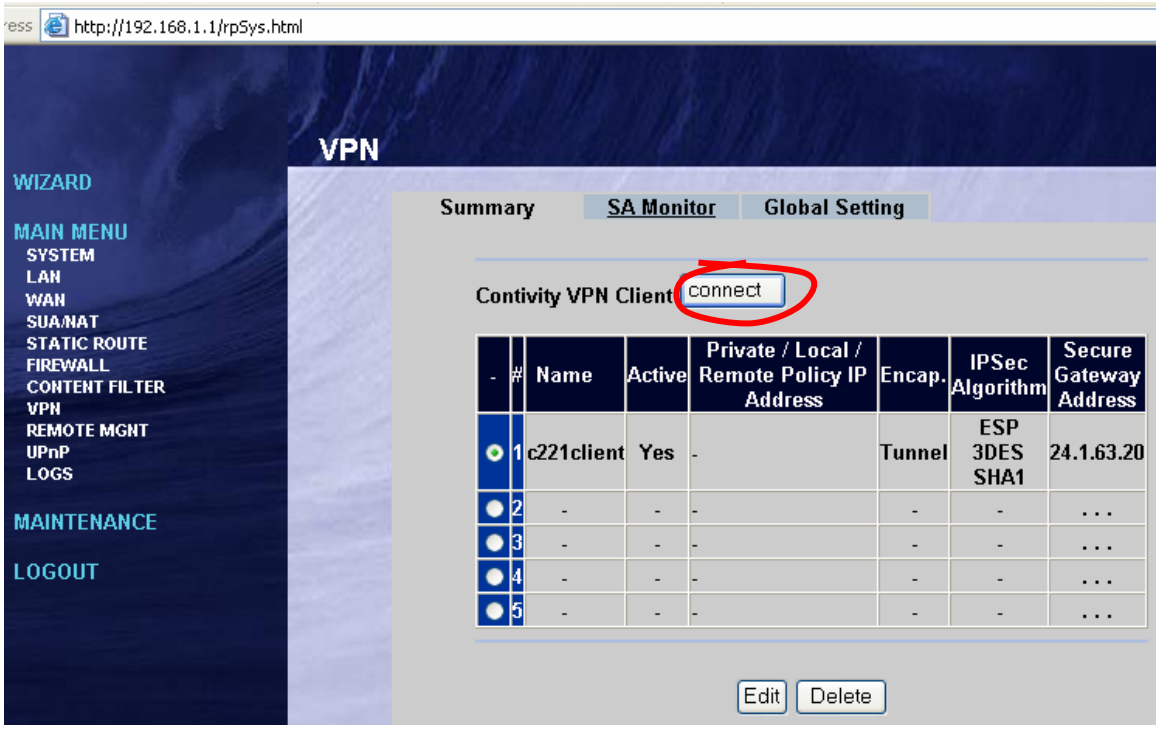
Set up C221 client

- Open a web browser and type default address of: http://192.168.1.1
- Go to “VPN” and edit “item #1”
- Select “connection type” as “Contivity client:”
- User Name: 221
- Password: "Contivity"
- Destination: 21.1.63.20 (C1100 public interface)
- Check “Active”

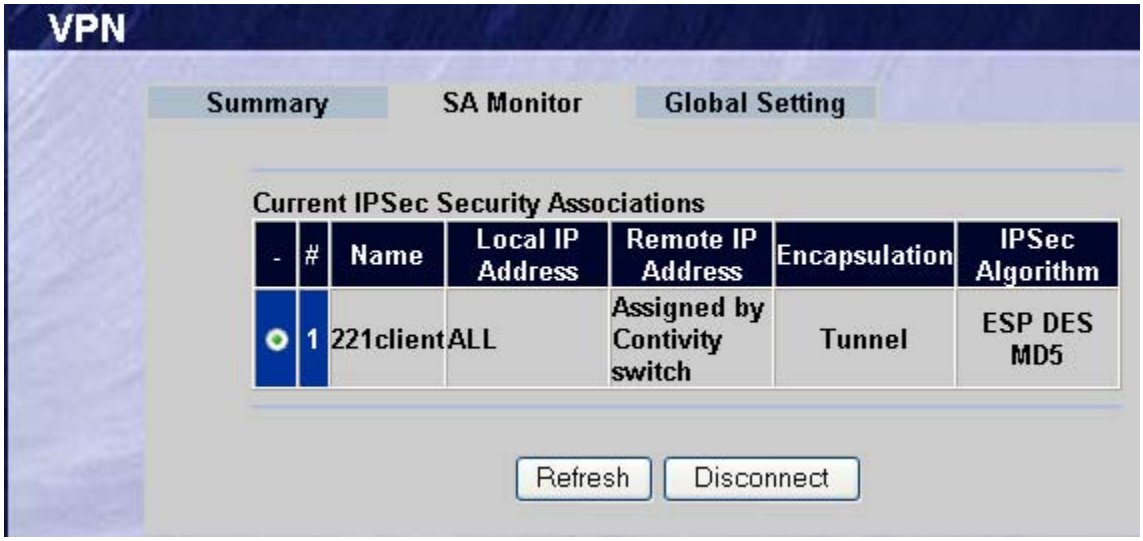


Connect hard-client to CO

Note: Connection can only be initiated by BO



SA is setup



Ping Continuously from BO to CO to keep tunnel up

- Ping CO from BO-1 to initiate the connectivity
- When client connection is up, branch office can reach CO 192.168.3.0/24
- Find out the assigned IP address (172.16.10.5) for remote hard-client (Status->Session)
- Due to NAT, CO cannot see 192.168.11.0/24 other than assigned IP address 172.16.10.5

Example:

```
C:\ ping -t 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=82ms TTL=63
Reply from 192.168.3.1: bytes=32 time=82ms TTL=63
Reply from 192.168.3.1: bytes=32 time=67ms TTL=63
Reply from 192.168.3.1: bytes=32 time=86ms TTL=63
Reply from 192.168.3.1: bytes=32 time=69ms TTL=63
Reply from 192.168.3.1: bytes=32 time=95ms TTL=63
Reply from 192.168.3.1: bytes=32 time=71ms TTL=63
Reply from 192.168.3.1: bytes=32 time=90ms TTL=63
Reply from 192.168.3.1: bytes=32 time=81ms TTL=63
Reply from 192.168.3.1: bytes=32 time=74ms TTL=63
```

From CO to BO

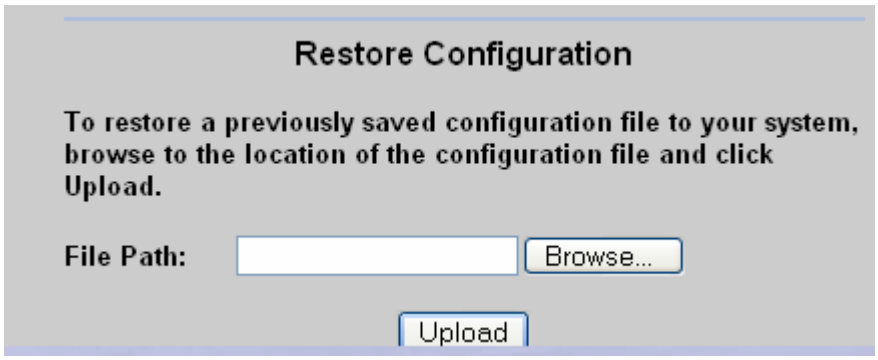
```
C:\>ping 172.16.10.5

Pinging 172.16.10.5 with 32 bytes of data:

Reply from 172.16.10.5: bytes=32 time=73ms TTL=253
Reply from 172.16.10.5: bytes=32 time=70ms TTL=253
Reply from 172.16.10.5: bytes=32 time=65ms TTL=253
Reply from 172.16.10.5: bytes=32 time=76ms TTL=253
Ping statistics for 172.16.10.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 65ms, Maximum = 76ms, Average = 71ms
```

Download Configuration file from CO to branch-office-1

- On PC-S3 in CO NOC, Open GUI interface
  - Type: http://172.16.10.5 to access remote-office-1
  - Go to Maintenance->Restore Configuration
  - Upload pre-built configuration file “office1-972-123-1111rom-0”
  - Remote office C221 will auto reboot when download is done
  - Ping from BO to CO to bring the tunnel up again

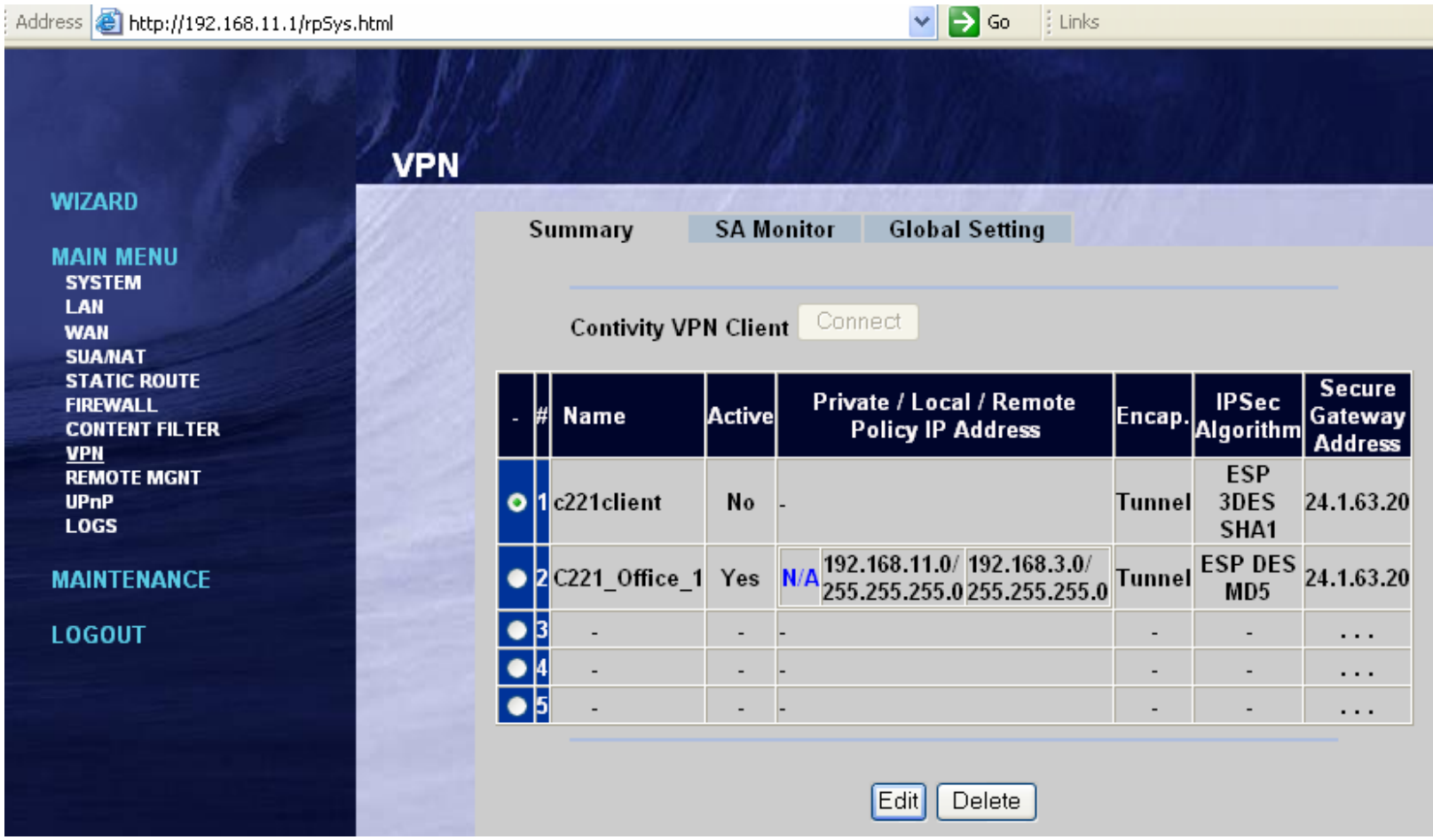


FTP Configuration file to remote office

- Alternatively, using FTP to download config file
- Store config file on C:\ office1-972-123-1111rom-0
- Set to binary, and must use rom-0 as remote file name

```
C:\>ftp 172.16.10.5
Connected to 172.16.10.5.
220 FTP version 1.0 ready at Sat Jan 1 00:14:20 2000
User (172.16.10.5:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put office1-972-123-1111rom-0 rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
ftp: 106496 bytes sent in 16.60Seconds
6.42Kbytes/sec.
ftp> quit
221 Goodbye for writing flash
```

When C221 reboots, deployment for BO-1 is done. Two pre-configured tunnels, and new LAN IP address are restored in BO-1. (see below)



Ping Test

- Ping CO from BO-1 to initiate the connectivity
- When ABOT connection is up, branch office can reach 192.168.3.0/24
- CO can reach 192.168.11.0/24 (unlike hard-client connection)

Ping Continuously from BO to CO to keep tunnel up

```
C:\ ping -t 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=82ms TTL=63
Reply from 192.168.3.1: bytes=32 time=82ms TTL=63
Reply from 192.168.3.1: bytes=32 time=67ms TTL=63
Reply from 192.168.3.1: bytes=32 time=86ms TTL=63
Reply from 192.168.3.1: bytes=32 time=69ms TTL=63
Reply from 192.168.3.1: bytes=32 time=95ms TTL=63
Reply from 192.168.3.1: bytes=32 time=71ms TTL=63
Reply from 192.168.3.1: bytes=32 time=90ms TTL=63
Reply from 192.168.3.1: bytes=32 time=81ms TTL=63
Reply from 192.168.3.1: bytes=32 time=74ms TTL=63
```

From CO to BO

```
C:\>ping 192.168.11.3

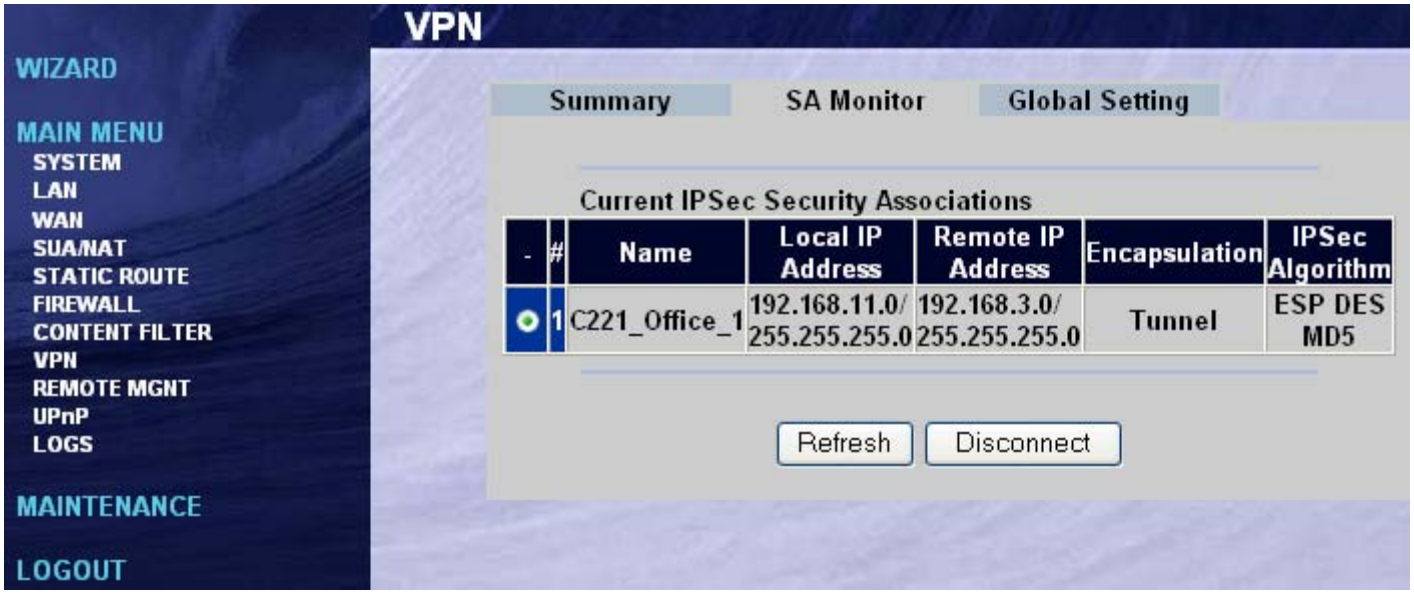
Pinging 192.168.11.3 with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time=73ms TTL=253
Reply from 192.168.11.3: bytes=32 time=70ms TTL=253
Reply from 192.168.11.3: bytes=32 time=65ms TTL=253
Reply from 192.168.11.3: bytes=32 time=76ms TTL=253

Ping statistics for 192.168.11.3:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 65ms, Maximum = 76ms, Average = 71ms
```

SA monitor shows connection:

- **In VPN, select item #2**
- **Select "SA Monitor"**



Repeat the previous steps for remaining sites:

-branch-office-2
-branch-office-3
-branch-office-4
-branch-office-5

5. Reference Documentation:

The following Technical Publications can be found at: http://www.nortelnetworks.com under Technical Documentation/Contivity/Contivity 200 Series/Documentation.

Document Title	Publication Number	Description
Contivity 221 VPN Switch Release Notes	317522-A	Release Notes
Contivity 251 U-R2 ADSL VPN Switch Release Notes	317521-A	Release Notes
Contivity 251 Annex B ADSL VPN Switch Release Notes	317520-A	Release Notes
Contivity 200 Series Interop Guide	n/a	Configuration Guide
Contivity 221 VPN Switch Quick Start Guide	317518-A	Technical Publication
Contivity 221 VPN Switch User's Guide	317517-A	Technical Publication
Contivity 251 VPN Switch User's Guide	317516-A	Technical Publication
Contivity 251 Annex A ADSL VPN Switch Release Notes	317519-A	Release Notes
Contivity 251 VPN Switch Quick Start Guide	317515-A	Technical Publication
Contivity Secure IP Services Gateway Release Notes [Version 4.80]	315000-D	Release Notes

6. Appendix A: Terminology

• ABOT: Asymmetric Branch Office Tunnel
• BO: Branch Office
• BOQS: Branch Office Quick Start
• BOT: Branch Office Tunnel
• C221: Contivity 221
• C1100: Contivity 1100
• Client Emulation: C200 hardware client simulating VPN client sw.
• Contivity Legacy Gateway: Legacy Contivity devices (exclude 100, 200, 400)
• CO: Central Office
• DHCP: Dynamic Host Configuration Protocol
• DNS: Domain Name System
• ISP: Internet Service Provider
• NOC: Network Operation Center
• Private Interface: Intranet connection to a LAN
• Public Interface: Internet connection to the outside world
• SOHO: small office or home office

Contact Us:

For product support and sales information, visit the Nortel Networks website at:

http://www.nortelnetworks.com

In North America, dial toll-free 1-800-4Nortel, outside North America, dial 987-288-3700.

Copyright © 2004 Nortel Networks

All rights reserved. January 2004

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Contivity are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporate.

All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.