converged access

CAP - Converged Access Point™

User Guide

Version 2.0
August 1, 2005

Part # 721-001020-00 Rev. B

Converged Access Inc.
31 Dunham Road • Billerica, MA 01821
http://www.convergedaccess.com
Tel. +1.978.436.9111
Fax +1.978.436.9922

Converged Access Point User Guide

Version 2.0

The information in the manual is provided without warranty of any kind and is subject to change without notice. Converged Access Inc. assumes no responsibility, and shall have no liability of any kind, arising from supply or use of this publication or any material contained herein.

Regulatory Compliance

Converged Access Point (CAP) devices meet the EMC requirements of:

FCC Part 15 Class A

EN55022:1998
EN55024-1:1997

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This model has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio and television communications.
Operation of this equipment in a residence area is likely to cause interference in which cause the user will be required to correct the interference at his or her own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the □
user's authority to operate this equipment.□
IMPORTANT NOTE:□
FCC Radiation Exposure Statement:□
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment □
should be installed and operated with minimum distance 20cm between the radiator & your body.□
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.□
Converged Access Inc. declares that CAP-1000-E-4A-W (FCC ID: TDW-WVRTD-100G-W) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in Unit.

Canadian Department of Communications (DOC) Notices

This digital apparatus does not exceed the **Class A** limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n' emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Safety Warnings

- **Electric Shock Hazard** — To prevent electric shock, do not remove the cover. This unit contains hazardous voltages and should only be opened by a trained and qualified technician. Disconnect electric power to the product before connecting or disconnecting Ethernet cables to the LAN and WAN ports.
- **Lightning Danger** — Do not work on equipment or cables during periods of lightning activity.
- **Grounding** — This equipment must be grounded. The power plug must be connected to a properly wired earth-ground socket outlet. An improperly wired socket outlet could place hazardous voltages on accessible metal parts.
- **Power Cord** — The power cord supplied with the system must only be plugged into a 110-volt outlet.
- **Mounting** — Mount equipment such that a hazardous condition is not created due to uneven loading.

The CAP meets the safety requirements of:

- UL 1950
- CSA C22.2 NO 950-93-CAN/CSA
- EN60950 (IEC 950:1991, Modified)

Caution

Air vents must not be blocked and must have free access to the room ambient air for cooling.

Do not attempt to repair or modify this equipment. Any repairs to the unit must be performed by Converged Access or a Converged Access authorized representative.

Table of Contents

1.0 INTRODUCTION TO THE CONVERGED ACCESS POINT 1

1.1 WHAT IS THE CONVERGED ACCESS POINT? 1
1.2 FEATURES 2
1.2.1 Network Interfaces 2
1.2.3 Network Security 2
1.2.4 Virtual Private Networks 2
1.2.5 Simplicity 3
1.2.6 Control & Provisioning 3
1.2.7 "Future-Proof" 3

2.0 GETTING STARTED 4

2.1 CONNECTING A COMPUTER TO THE CAP 5
2.1.1 Step 1 - PC Network Configuration 5
2.1.2 Step 2 - LAN Physical Connection 7
2.1.3 Step 3 - Internet Physical Connection 7
2.1.4 Step 4 - Web Based Management 8
2.2 QUICK SETUP 9
2.2.1 Router Mode or Bridge Mode Selection 9
2.2.2 Configuring Your Internet/WAN Connection 10
2.3 CONFIGURING YOUR LAN ETHERNET INTERFACE 12
2.3.1 Accessing the 'LAN Bridge' to Configure Your LAN Connection 13

3.0 NAVIGATING THE WEB-BASED MANAGEMENT INTERFACE 17

3.1 ACCESSING THE WEB-BASED MANAGEMENT 18
3.2 THE CAP'S NETWORK MAP 18
3.3 LEFT SIDEBAR 20
3.4 MANAGING LISTS 21

4.0 CREATING VPN CONNECTIONS 22

4.1 OVERVIEW 22
4.2 CONFIGURING THE CAP AS A PPTP SERVER 23
4.2.1 Email Notification on the PPTP client 25
4.3 IPSEC VPN CONNECTIONS 26
4.3.1 Technical Specifications 26
4.3.2 Basic IPSec Settings 27
4.3.3 Key Management 28
4.3.4 Log Settings 29
4.3.5 Configuring an IPSec VPN 30
4.3.6 IPSec Advanced Configuration Parameters Definitions 36
4.3.6 Example IPSec VPNC Scenario 38

5.0 SECURITY 44

5.1 FIREWALL SECURITY OVERVIEW 45
5.1.1 Configuring the Firewall Security Level 47
5.2 ADDING ACCESS CONTROLS 47
5.3 USER-DEFINED SERVICES 49
5.4 LOCAL SERVERS (PORT FORWARDING) 51

5.5 Designating a Demilitarized (DMZ) Host 53
5.6 Port Triggering 54
5.6.1 Defining Port Triggering 54
5.7 Remote Management of the CAP 56
5.8 IP-Hostname Filtering 57
5.9 Security Log 60
5.10 Advanced Filtering 63
5.10.1 Adding an Advanced Filtering Rule 66
5.11 Applying Corporate Security 72

6.0 QOS TRAFFIC MANAGEMENT CAPABILITIES 74

6.1 Configuring QoS in the CAP 74

7.0 ADVANCED 88

7.1 System Settings 89
7.1.1 Management Console Settings 89
7.1.2 Management Application Ports Settings 89
7.1.3 System Logging Settings 90
7.1.4 Security Logging Settings 90
7.1.5 Outgoing Mail Server Settings 90
7.2 Managing the DNS Server 91
7.2.1 Viewing and Modifying the DNS Table 91
7.3 Dynamic DNS 93
7.3.1 Using Dynamic DNS 94
7.4 DHCP - Managing IP Address Distribution 94
7.4.1 DHCP Server Summary 95
7.4.2 Editing DHCP Server Settings 97
7.4.3 DHCP Connections 97
7.5 Network Objects 99
7.6 Routing 101
7.6.1 Managing Routing Table Rules 101
7.6.2 Multicasting 102
7.7 Managing & Defining Users 103
7.7.1 Email Notification 104
7.8 RADIUS 104
7.9 Date & Time 105
7.10 Scheduler Rules 106
7.11 Point-to-Point Tunneling Protocol (PPTP) 109
7.11.1 Managing Remote Users 109
7.11.2 Email Notification 110
7.11.3 Advanced PPTP Server Settings 112
7.11.4 Advanced PPTP Client Settings 113
7.15 Simple Network Management Protocol (SNMP) 116
7.15.1 Configuring the CAP's SNMP Agent 116
7.16 MAC Cloning 117
7.17 Diagnostics 118
7.17.1 Diagnosing Network Connectivity 118
7.18 Remote Administration 118
7.18.1 Configuring Remote Administration Services 119
7.20 Restart 120
7.21 Saving, Restoring & Resetting the CAP Configuration 121
7.22 Tunneling IP V6 Inside of IP V4 124

8.0 SYSTEM MONITORING 125

8.1 Monitoring Connections 126
8.2 Traffic Statistics 127

8.3 QoS TRAFFIC 128
8.4 SYSTEM LOG 129
8.5 SYSTEM UP TIME 130

9.0 FIRMWARE UPGRADE 131

9.1 UPGRADING FROM THE INTERNET 131
9.2 UPGRADING FROM A LOCAL COMPUTER 132

10.0 ANALOG VOICE GATEWAY CONFIGURATION 134

10.1 CONfiGURING VOIP – ATA 135
10.1.1 The “IP Telephony” Tab 135
10.1.2 The “Phone Settings” tab 138
10.1.3 Creating and editing Speed Dial and the Address Book 139
10.1.4 Telephony Features 140

11.0 GLOSSARY 142

List of Acronyms

ALG	Application-Level Gateway
API	Application Programming Interface
CAP	Converged Access Point
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
OAM	Operations and Maintenance
PDA	Personal Digital Assistant
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

Contacting Converged Access Inc.

Corporate Headquarters

Converged Access, Inc. • 31 Dunham Road • Billerica, MA 01821-5729
http://www.convergedaccess.com

Technical Support

If you require technical assistance, contact the company through whom you acquired the CAP device and the Service Contract. To expedite assistance, have the following information available:

- Your service contract number.
- Your name, company name, and phone number.
- Product Model Number
- Product Serial Number
- A brief description of the problem.

Then forward your problem, together with the above information, to your Technical Support Provider.

1

1.0 Introduction to the Converged Access Point

1.1 What is the Converged Access Point?

The Converged Access Point is a customer premise platform that by operating at layer seven, enables enterprises to converge voice, video and data applications across a single wide area network while guaranteeing toll quality voice and data application performance. The CAP allows the simultaneous usage of a wide range of compelling broadband-based applications, while allowing you to secure your network and prioritize business critical applications towards and from your WAN link. The CAP delivers a set of highly integrated solutions required for the small enterprise market, including:

- **Integral Ethernet switching**
- **Advanced QoS Traffic management**
- **Integral VoIP gateway**
- **Network security (Stateful Packet Inspection)**
- **Virtual Private Networking (VPN)**
- **Remote management (web and SNMP based)**
- **Remote update capabilities**

1.2 Features

1.2.1 Network Interfaces

The CAP can be used with a variety of wide area networking services including DSL, T1 and broadband cable. These wide area network services are connected to the CAP via 10/100 Ethernet WAN port.

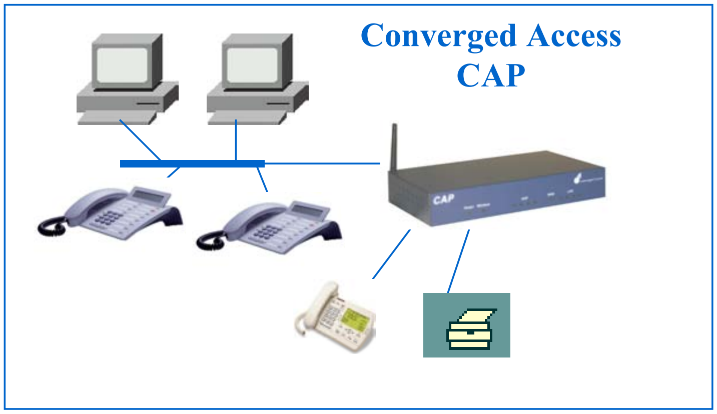
There are also four 10/100 Mbps, auto-sensing switched Ethernet LAN interfaces to connect local LAN traffic to the CAP. Each port supports half-or full-duplex operation, although it is recommended that for full, bi-directional QoS, you should either connect PC's and IP-phones etc. directly to the CAP, or connect them to the CAP via a 'Switch', which supports full-duplex operation.

1.2.3 Network Security

The CAP maintains network security using an ICSA 4.0 certifiable Stateful Packet Inspection (SPI) firewall, and a wide variety of advanced filtering options to properly secure your network entities as well as your data and VoIP traffic.

1.2.4 Virtual Private Networks

The CAP has an integrated VPNC certifiable VPN hardware accelerator, ensuring a secure communications path over the Internet to access remote computers or sites. By implementing industry standard encryption, authentication and key management schemes, the CAP's VPN capability is interoperable with leading VPN technologies such as IPSec and PPTP.



1.2.5 Simplicity

The CAP has been designed to provide seamless connectivity with minimal user configuration. Auto-learning DNS enables communication between LAN computers using host names instead of IP addresses, and the DHCP client/server completely automates the network connection process. Advanced security and prioritization is easily configured via a ‘point and click’ Web management interface.

1.2.6 Control & Provisioning

An intuitive web-based management interface offers comprehensive control over the CAP. If allowed, the CAP can allow remote management access by service providers using the web-based management, SNMP or telnet protocols. By default, remote administrative access via the WAN interface is completely disabled.

1.2.7 “Future-Proof”

The CAP’s simple, on-line firmware upgrade capabilities, allows you to quickly and easily upgrade the firmware to enable the latest features and functionality. Information on the latest releases and features is available on the ‘http://www.convergedaccess.com’ website, to allow you to quickly determine if a new version would be applicable to your business needs.

2

2.0 Getting Started

Connecting both your LAN and WAN network devices to the CAP is a simple procedure.

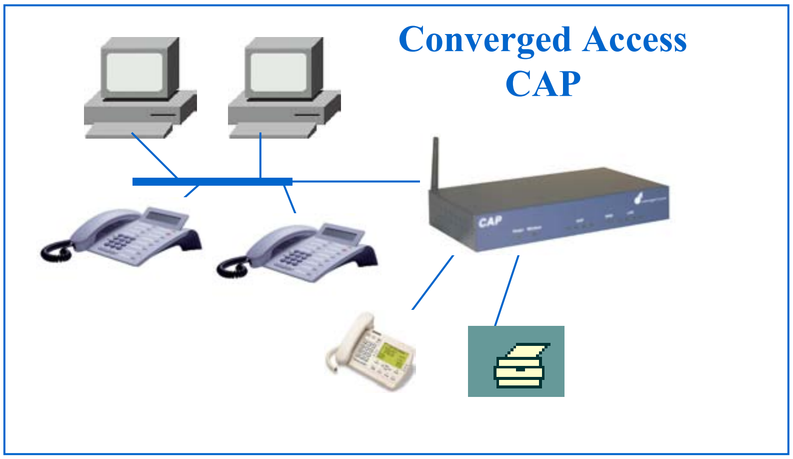
The setup is designed to seamlessly integrate CAP with your existing network. The ‘Windows default network settings’ dictate that in most cases the setup procedure described below will be unnecessary. For example, the default DHCP setting in Windows 2000 is ’client’, requiring no further modification.

However, it is advised to follow the setup procedure described below to verify that all communication parameters are valid and that the physical cable connections are correct.

2.1 Connecting a Computer to the CAP

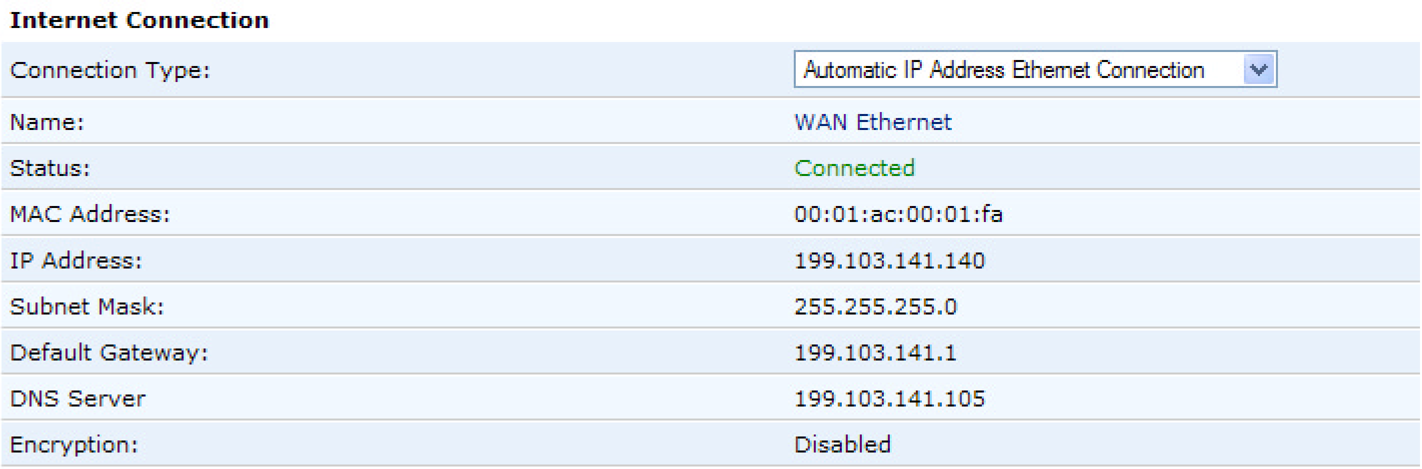
The basic setup procedure consists of four configuration steps:

1. PC network configuration.
2. Connecting a computer to the CAP (LAN connection).
3. Connecting the CAP to the outside world (WAN/Internet connection).
4. Definition of your traffic and bandwidth management objectives via the Web-based management interface.



2.1.1 Step 1 - PC Network Configuration

The CAP is designed to run as a DHCP client, initiating the DHCP protocol with a network DHCP server in order to dynamically obtain an IP address on the CAP's WAN interface.

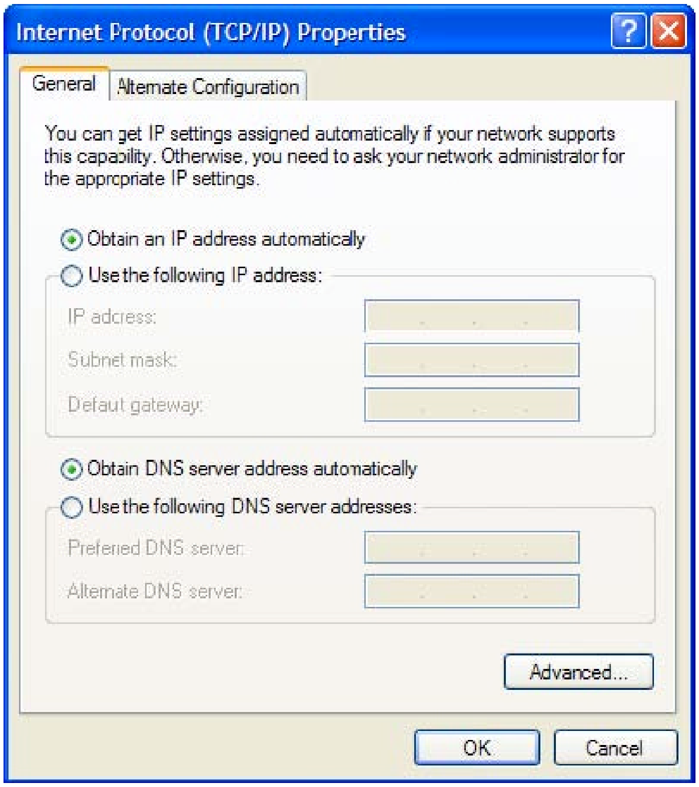


Internet Connection

Connection Type:	Automatic IP Address Ethernet Connection
Name:	WAN Ethernet
Status:	Connected
MAC Address:	00:01:ac:00:01:fa
IP Address:	199.103.141.140
Subnet Mask:	255.255.255.0
Default Gateway:	199.103.141.1
DNS Server	199.103.141.105
Encryption:	Disabled

Similarly, the computer's operating system regards the CAP as a DHCP server, thus the computers connected to the LAN ports of the CAP can be configured as DHCP clients.

The following diagrams show the steps necessary to configure your PC to be a DHCP client of the CAP, if automatic client configuration via DHCP is preferred. This configuration principle is identical in each operating system, but the steps to be performed are different on each operating system.



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:

The figure above displays the 'TCP/IP Properties' dialog box as it appears in Windows 2000. The following are TCP/IP DHCP client configuration instructions for all supported operating systems. If you already have DHCP enabled, and want to release your current IP address and obtain a new one from the CAP, you can open a command prompt window on your PC and enter "ipconfig /release", followed by "ipconfig /renew" to obtain your IP address information directly from the CAP.

2.1.1.1 Windows XP

1. Access 'Network Connections' from the Control Panel.
2. Right-click on the Ethernet connection's icon, and select 'Properties' to display the connection's properties.
3. From the 'General' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
4. The 'Internet Protocol (TCP/IP)' properties will be displayed.
   (a) Select the 'Obtain an IP address automatically' radio button.
   (b) Select the 'Obtain DNS server address automatically' radio button.
5. Continue to section 2.2.

2.1.1.2 Windows 2000/98/Me

1. Access ’Network and Dialing Connections’ from the Control Panel.
2. Right-click on the Ethernet connection’s icon, and select ’Properties’ to display the connection’s properties.
3. Select the ’Internet Protocol (TCP/IP)’ component, and press the ’Properties’ button.
4. The ’Internet Protocol (TCP/IP)’ properties will be displayed.
   (a) Select the ’Obtain an IP address automatically’ radio button.
   (b) Select the ’Obtain DNS server address automatically’ radio button.
5. Continue to section 2.2.

2.1.1.3 Windows NT

1. Access ’Network’ from the Control Panel to display the network control panel.
2. From the ’Protocol’ tab, select the ’Internet Protocol (TCP/IP)’ component, and press the ’Properties’ button.
3. From the ’IP Address’ tab select the ’Obtain an IP address automatically’ radio button.
4. From the ’DNS’ tab, verify that no DNS server is defined in the ’DNS Service Search Order’ box and no suffix is defined in the ’Domain Suffix Search Order’ box.
5. Reboot.
6. Continue to section 2.2.

2.1.1.4 Linux

1. Login into the system as a super-user, by entering ‘su’ at the prompt.
2. Type ’ifconfig’ to display the network devices and allocated IP’s.
3. Type ’pump -i dev’, where dev is the network device name.
4. Type ’ifconfig’ again to view the new allocated IP address.
5. Continue to section 2.2.

2.1.2 Step 2 - LAN Physical Connection

Plug your computer into a LAN ethernet port on the CAP via a category 3/5 ethernet cable. At this point, your PC will have obtained an IP address automatically from the CAP. On Windows systems, you can open a “command prompt” on your PC, and type ‘ipconfig’ to see the IP address automatically provided to your PC by the CAP.

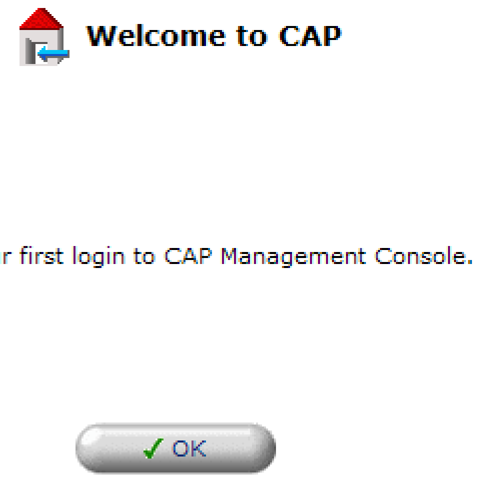
2.1.3 Step 3 - Internet Physical Connection

Connect the CAP’s WAN interface to your DSL or cable modem, or to a bridge/router with an integral CSU/DSU. Consult your external device’s documentation regarding specific cables necessary for connection.

2.1.4 Step 4 - Web Based Management

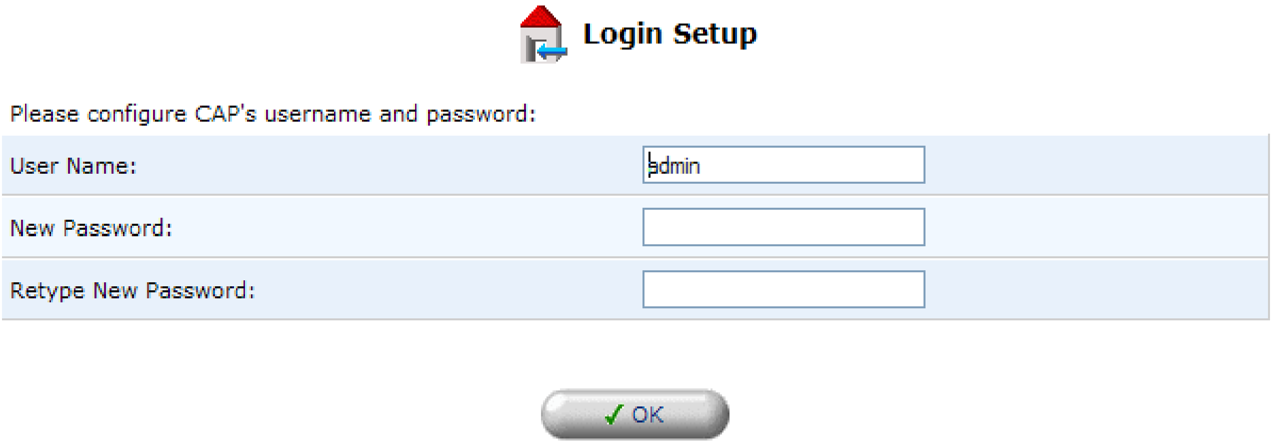
The CAP’s web-based management interface allows you to configure and monitor various system parameters. The interface is accessed through a web browser as follows:

1. Launch a web browser on your PC
2. Enter the URL address http://192.168.1.1 to display the web-base management interface. When first logging on to the web-based management, the “Welcome Screen" will appear, enabling you to place a shortcut to this screen in your ’Favorites’ folder. Press ’OK’ to continue’, the ’Login Setup’ screen will appear .
3. To configure your login settings, enter a user name and password. To verify correctness, retype the password, and press ’OK’ to login to the management console. The default user name is ’admin’, and there is no password by default. You should enter a new password to provide system security.



Welcome to CAP

This is your first login to CAP Management Console.



Login Setup

Please configure CAP's username and password:

User Name:	admin
New Password:	
Retype New Password:	

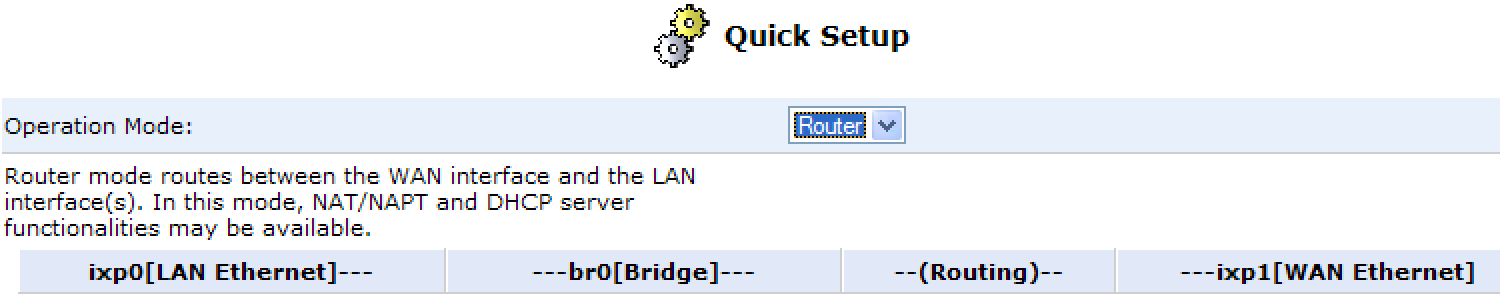
2.2 Quick Setup

The ‘Quick Setup’ utility is designed to help you quickly and easily set up your CAP’s ‘Internet’ WAN connection.

2.2.1 Router Mode or Bridge Mode Selection

The first and most important configuration option on the CAP is whether to set it up in Bridge mode, or Router mode. As you’ll note from the following screen shots, many of the benefits of the CAP cannot be enabled if the CAP is configured to be a Bridge, such as NAT/NAPT, IP-Sec VPNs, and the DHCP server.

Unless the CAP is set up behind an Internet/WAN router already, you should configure the CAP in Router mode to have access to the entire suite of benefits the CAP provides.

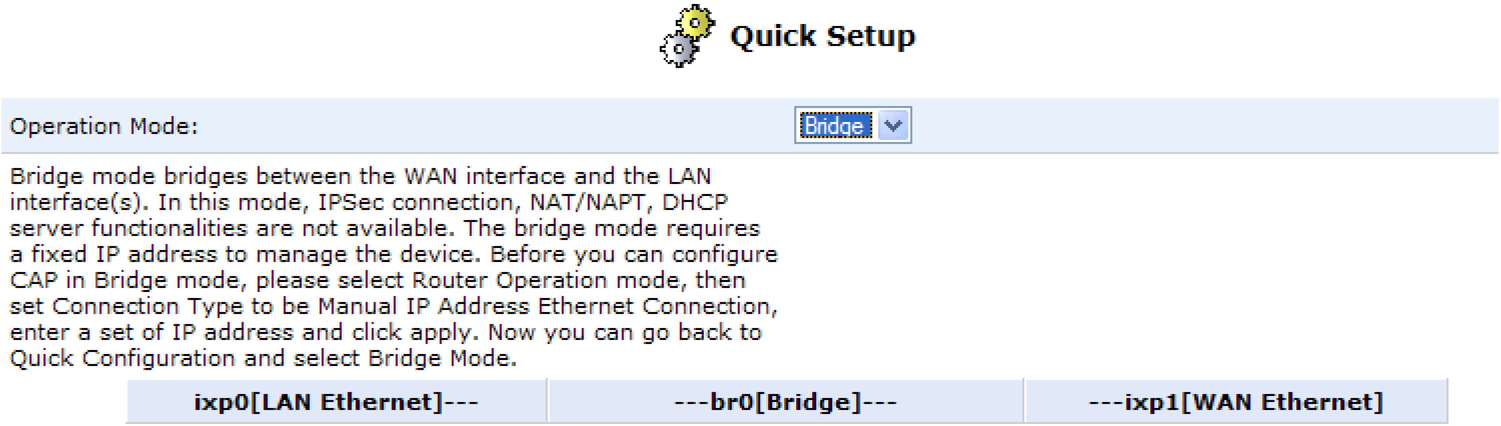


Quick Setup

Operation Mode: Router

Router mode routes between the WAN interface and the LAN interface(s). In this mode, NAT/NAPT and DHCP server functionalities may be available.

ixp0[LAN Ethernet]---	**---br0[Bridge]---**	**--(Routing)--**	**---ixp1[WAN Ethernet]**



Quick Setup

Operation Mode: Bridge

Bridge mode bridges between the WAN interface and the LAN interface(s). In this mode, IPSec connection, NAT/NAPT, DHCP server functionalities are not available. The bridge mode requires a fixed IP address to manage the device. Before you can configure CAP in Bridge mode, please select Router Operation mode, then set Connection Type to be Manual IP Address Ethernet Connection, enter a set of IP address and click apply. Now you can go back to Quick Configuration and select Bridge Mode.

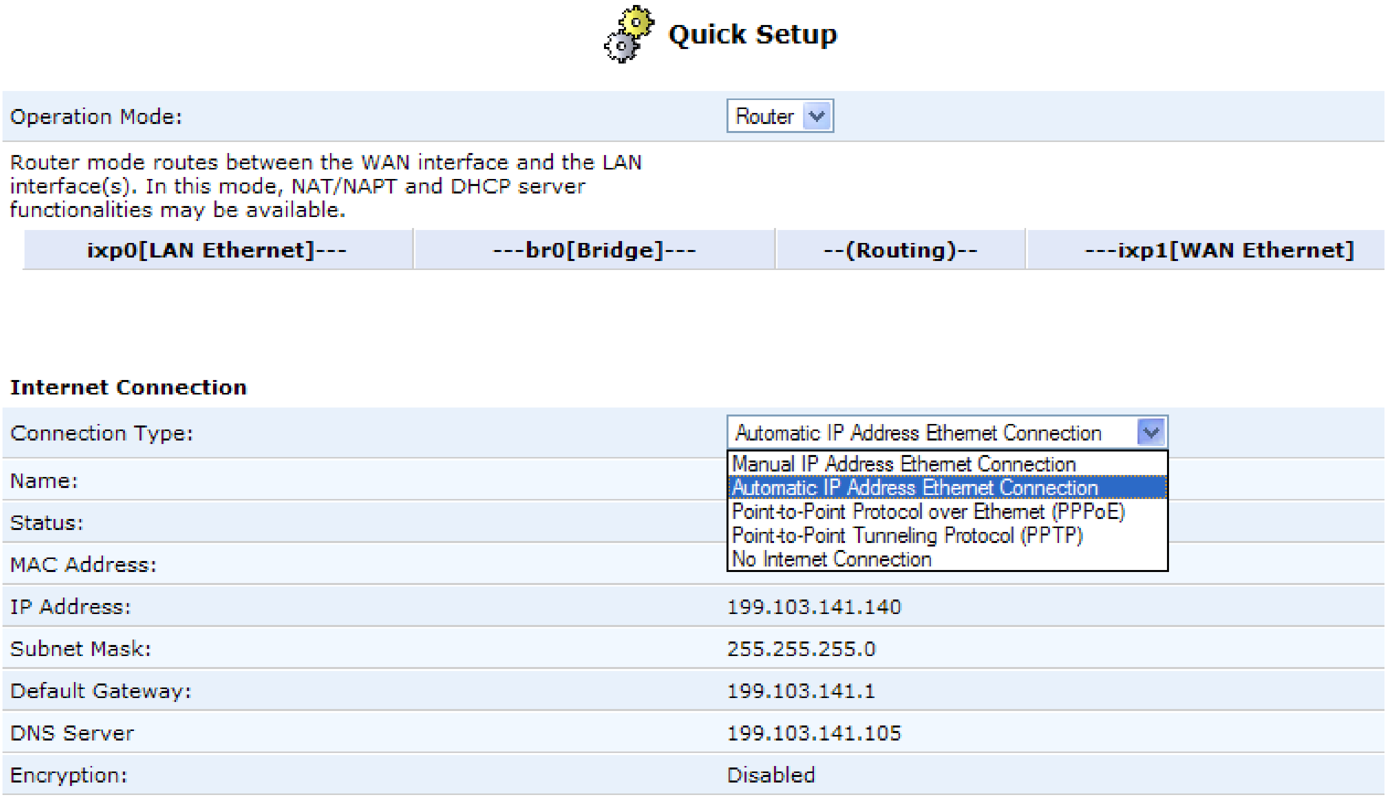
ixp0[LAN Ethernet]---	**---br0[Bridge]---**	**---ixp1[WAN Ethernet]**

2.2.2 Configuring Your Internet/WAN Connection

When subscribing to a broadband service, you should be well aware of the method by which you are connecting to the Internet. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you connect to the Internet using a static or dynamic IP address, or what protocols, such as PPTP or PPPoE, you will be using to communicate over the Internet. The “Quick Setup” page is launched automatically when you log on to the CAP for the first time.

Your WAN connection can be configured using one of the following methods:

- Manual IP Address Ethernet Connection
- Automatic IP Address Ethernet Connection
- Point-to-point protocol over Ethernet (PPPoE)
- Point-to-Point Tunneling Protocol (PPTP)



Quick Setup

Operation Mode:	Router

Router mode routes between the WAN interface and the LAN interface(s). In this mode, NAT/NAPT and DHCP server functionalities may be available.

ixp0[LAN Ethernet]---	---br0[Bridge]---	--(Routing)--	---ixp1[WAN Ethernet]

Internet Connection

Connection Type:	Automatic IP Address Ethernet Connection
Name:	
Status:	
MAC Address:	
IP Address:	199.103.141.140
Subnet Mask:	255.255.255.0
Default Gateway:	199.103.141.1
DNS Server	199.103.141.105
Encryption:	Disabled

Manual IP Address Ethernet Connection
Automatic IP Address Ethernet Connection
Point-to-Point Protocol over Ethernet (PPPoE)
Point-to-Point Tunneling Protocol (PPTP)
No Internet Connection

2.2.2.1 Manual IP Address WAN Ethernet Connection

1. Select ’Manual IP Address Ethernet Connection’ from the ’Connection Type’ combo-.box
2. According to your service provider’s instructions, specify the following parameters:
    - IP address
    - Subnet mask
    - Default gateway
    - Primary DNS server
    - Secondary DNS server
3. Specify the gateway’s host name in the ’CAP’s Hostname’ field. This address is used to access the gateway’s web-based management, assuming you have an entry established for this name already defined in your company DNS server.
4. Specify the administrator’s email in the ’email’ field. System alerts and notifications are sent to this email address.
5. Clicking on the ’Apply’ button.
6. Clicking the ‘OK’ button will exit you from your current location within the Web management interface, and place your view at the next level higher up in the management interface.
7. Continue to section 3.0.

2.2.2.2 Automatic IP Address WAN Ethernet Connection

1. Select ’Automatic IP Address Ethernet Connection’ from the ’Connection Type’ combo-box.
2. Specify the gateway’s host name in the ’CAP’s Hostname’ field. This address is used to access the gateway’s web-based management, assuming you have an entry established for this name already defined in your company DNS server.
3. Specify the administrator’s email in the ’email’ field. System alerts and notifications are sent to this address.
4. Click on the ’Apply’ button.
5. Clicking the ‘OK’ button will exit you from your current location within the Web management interface, and place your view at the next level higher up in the management interface.
6. Continue to section 3.0.

2.2.2.3 Point-to-Point Protocol over Ethernet (PPPoE)

1. Select ’Point-to-Point Protocol over Ethernet (PPPoE)’ from the ’Connection Type’ combo-box.
2. Your Internet Service Provider (ISP) should provide you with the following information:
    - Login user name
    - Login password
3. Specify the gateway’s host name in the ’CAP’s Hostname’ field. This address is used to access the gateway’s web-based management, assuming you have an entry established for this name already defined in your company DNS server.
4. Specify the administrator’s email in the ’email’ field. System alerts and notifications are sent to this address.
5. Click on the ’Apply’ button.
6. Clicking the ‘OK’ button will exit you from your current location within the Web management interface, and place your view at the next level higher up in the management interface.
7. Continue to section 3.0.

2.2.2.4 Configuring the CAP as a PPTP Client

1. Select ‘Point-to-Point Tunneling Protocol (PPTP) from the ‘Connection Type’ combo box.
2. Your Internet Service Provider (ISP) should provide you with the following information:
   • Login user name
   • Login password
3. Specify the gateway’s host name in the ’CAP’s Hostname’ field. This address is used to access the gateway’s web-based management, assuming you have an entry established for this name already defined in your company DNS server.
4. Specify the administrator’s email in the ’email’ field. System alerts and notifications are sent to this address.
5. Click on the ’Apply’ button.
6. Clicking the ‘OK’ button will exit you from your current location within the Web management interface, and place your view at the next level higher up in the management interface.
7. Continue to section 3.0.

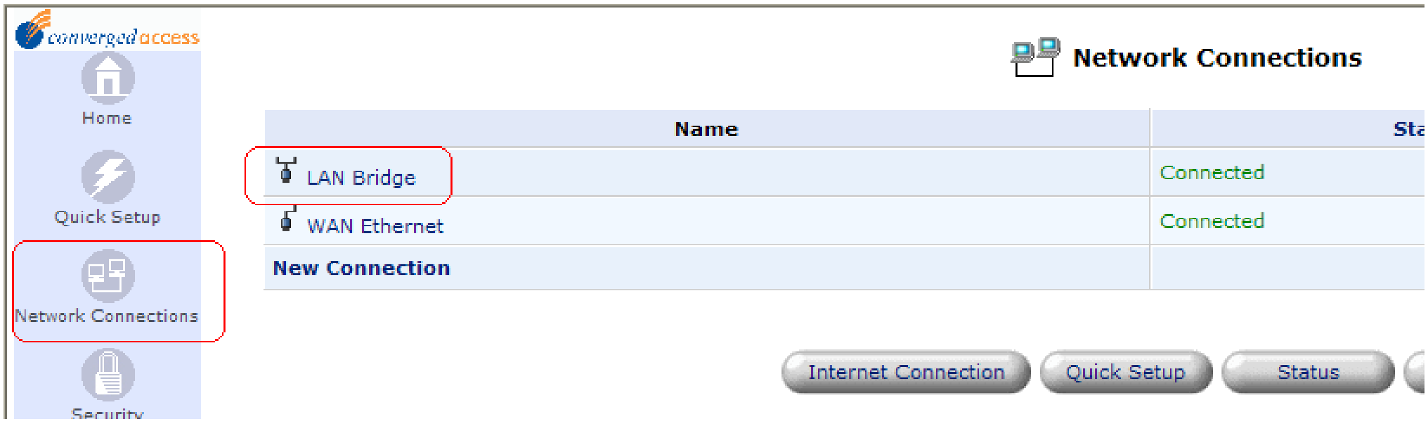
2.3 Configuring your LAN Ethernet Interface

Your LAN Ethernet(s) ship pre-configured with an IP address of 192.168.1.1, as well as are pre-configured to provide DHCP services to clients requesting DHCP services through the LAN interfaces. The default IP pool is from 192.168.1.1 through 192.168.1.244.

You can change this LAN information, along with a number of other LAN features via the ‘Network Connections’ section of the web interface.

2.3.1 Accessing the ‘LAN Bridge’ to Configure Your LAN Connection

Click on ‘Network Connections’ to open up the network connection list



Network Connections

Name	Sta
LAN Bridge	Connected
WAN Ethernet	Connected
New Connection	

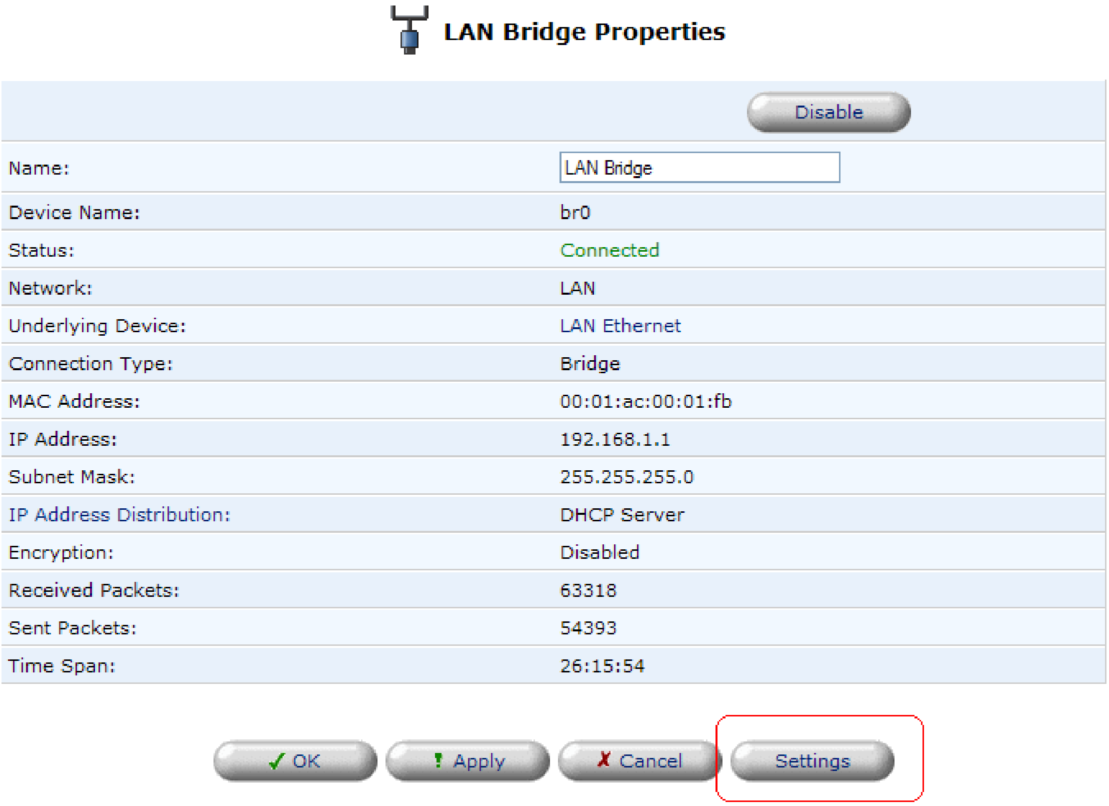
NOTE:

The ‘WAN Ethernet’ shown is your Internet/WAN link. You can click on ‘WAN Ethernet’, then ‘Settings’, to review it’s full configuration.

The “LAN Bridge’ shown above, is actually a reference point to an internal LAN Bridge within the CAP. If you have enabled Routing on your Internet/WAN interface**, configuring the LAN Bridge, does not disable your Routing features in any way.** This again, is simply a reference point within the CAP, is where you should currently configure your LAN interface options, and will be the logical connection point between the ‘Wired LAN’ ports and the ‘Wireless LAN’ ports when 802.11b/g wireless becomes available in the CAP.

Click on ‘LAN Bridge’ to open up the pre-configured Ethernet. At this point, if you’d prefer, you could simply change the ‘Name:’ of the LAN Bridge to another name of your choice such as ‘Ethernet’ at this location, but it is actually a reference point to an internal device at this point in the product.

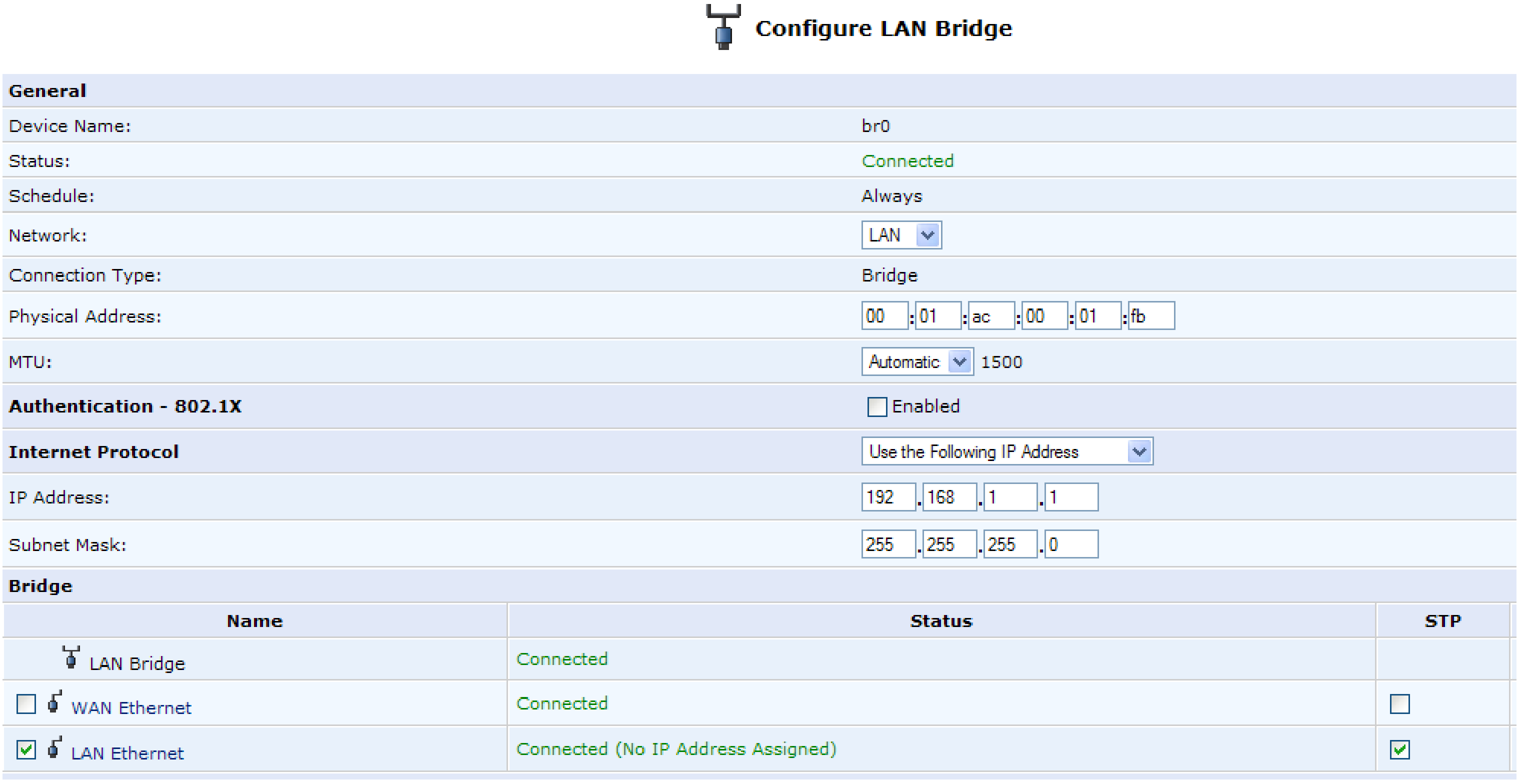
Then click on ‘Settings’ to open up the full LAN Bridge (Ethernet LAN) configuration window.



LAN Bridge Properties

Name:	LAN Bridge
Device Name:	br0
Status:	Connected
Network:	LAN
Underlying Device:	LAN Ethernet
Connection Type:	Bridge
MAC Address:	00:01:ac:00:01:fb
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Encryption:	Disabled
Received Packets:	63318
Sent Packets:	54393
Time Span:	26:15:54

This screen shows the configuration options available to customize your Ethernet LAN configuration to your needs. Click on 'Apply' to activate and save your changes, and click on 'OK' to exit this area of the web configuration.



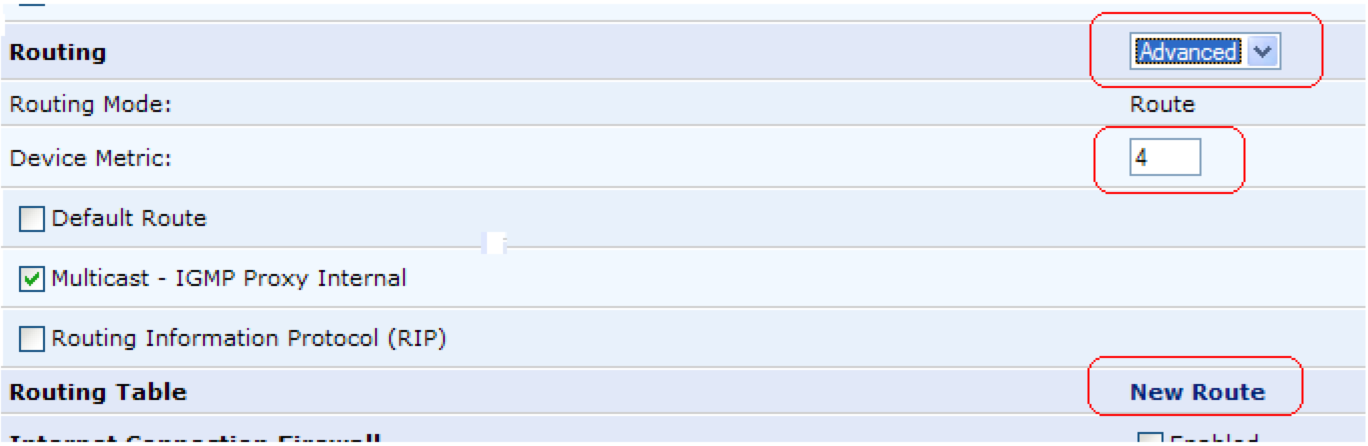
Configure LAN Bridge

General	
Device Name:	br0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Bridge
Physical Address:	00 : 01 : ac : 00 : 01 : fb
MTU:	Automatic 1500
Authentication - 802.1X	□ Enabled
Internet Protocol	Use the Following IP Address
IP Address:	192 . 168 . 1 . 1
Subnet Mask:	255 . 255 . 255 . 0

Bridge

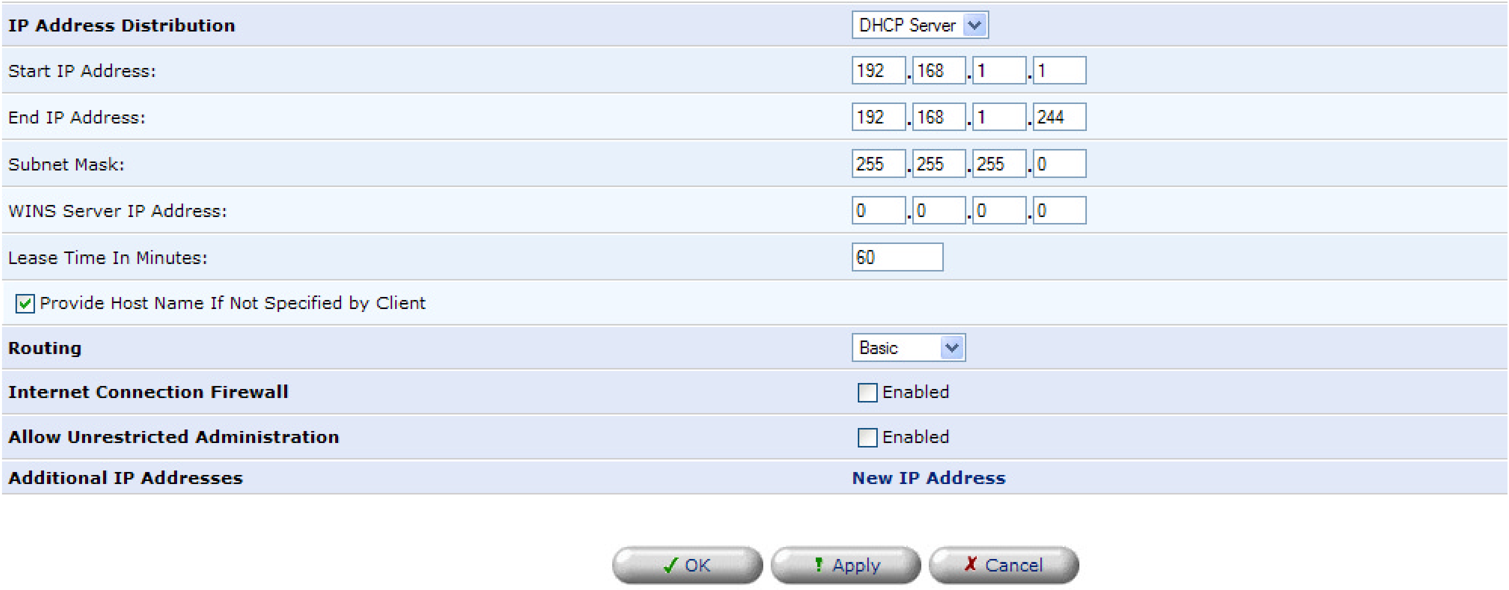
Name	Status	STP
LAN Bridge	Connected	
□ WAN Ethernet	Connected	□
☑ LAN Ethernet	Connected (No IP Address Assigned)	☑

You can enable Dynamic Routing updates on the Ethernet interface, and/or add static routes by clicking on the down-arrow in the 'Routing' section (defaults to 'Basic'), and changing it to 'Advanced'. This will then allow you to enable RIP, create a metric for the CAP to advertise about its route(s), and establish static routes.



Routing	Advanced
Routing Mode:	Route
Device Metric:	4
□ Default Route	
☑ Multicast - IGMP Proxy Internal	
□ Routing Information Protocol (RIP)	
Routing Table	**New Route**

By clicking on 'New Route', a window opens up for you to enter new static routes on the CAP.



IP Address Distribution	DHCP Server
Start IP Address:	192 . 168 . 1 . 1
End IP Address:	192 . 168 . 1 . 244
Subnet Mask:	255 . 255 . 255 . 0
WINS Server IP Address:	0 . 0 . 0 . 0
Lease Time In Minutes:	60
☑ Provide Host Name If Not Specified by Client	
Routing	Basic
Internet Connection Firewall	□ Enabled
Allow Unrestricted Administration	□ Enabled
Additional IP Addresses	**New IP Address**

NOTE: Static Routes can also be entered in the 'Advanced' section of the management interface. This will be reiterated later in the 'Advanced' section of the manual.

3

3.0 Navigating the Web-based Management Interface

The CAP does not require any further basic configuration in order to start working as an Internet/WAN firewall and 4 port ethernet bridge.

After the setup described in section 2, has been completed, you can immediately start using your Convergence Access Point to:

- Share a broadband Internet/WAN connection among multiple LAN devices and the WAN (if enabled) for applications such as HTTP, FTP, Telnet, NetMeeting, etc.
- Via the default firewall security level implemented (aka - ‘Typical Security’), outbound connections can be established, and the stateful inspection firewall will subsequently allow the inbound traffic associated with those sessions, but inbound initiated sessions will be rejected.
- Build a complete business network by connecting additional PCs and/or switches/hubs to the CAP.
- Share resources (files, printers, etc.) between computers in the business network using their names.
    - Auto-learning DNS enables CAP to automatically detect the network identification names of the LAN PCs, enabling mutual communication using names, not IP addresses.
- Control network parameters, including DHCP, DNS and WAN settings.
- View network status, traffic statistics, system logs, etc.

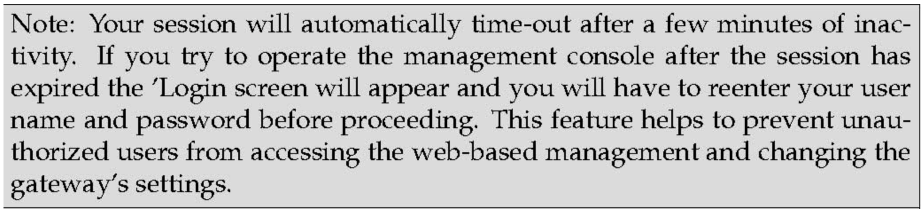
At this point, the system administrator can then begin to implement the advanced features of the CAP to:

- Allow access from the Internet to services on your CAP’s LAN network (ie. Web Server, IP-PBX, FTP server, etc.).
- Block network access to specific Internet web sites or to all WAN services.
- Fully configure and control all bandwidth management and QoS prioritization functionality
- Increase or decrease the security level on the system for traffic and management.

3.1 Accessing the Web-based Management

To access the management console:

1. Launch a Web-browser on a PC in the LAN.
2. Type the gateway’s IP address or name as provided with your gateway in the address bar (Internet Explorer) or location bar (Netscape Navigator). The default IP address is 192.168.1.1, and default name is ’CAP’.
3. Enter your username and password to log on to the web-based management. The default user name is ’admin’, and there is no password by default. **Note:** for security reasons, you should change these settings after the initial login. See section 5 for details.
4. The web interface is configured to time out in 900 seconds to protect the CAP from un-authorized access. You can change this under the System Settings (see section 7 for details).



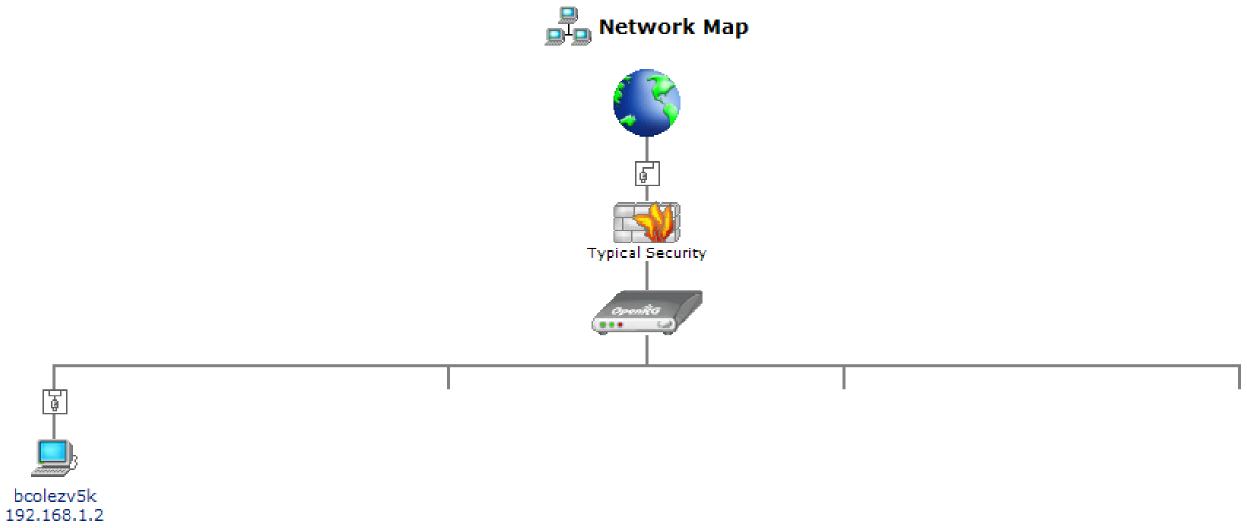
Note: Your session will automatically time-out after a few minutes of inactivity. If you try to operate the management console after the session has expired the ’Login screen will appear and you will have to reenter your user name and password before proceeding. This feature helps to prevent unauthorized users from accessing the web-based management and changing the gateway’s settings.

3.2 The CAP’s Network Map

When you log into the management console you will see the ‘Home’ **Network Map**.

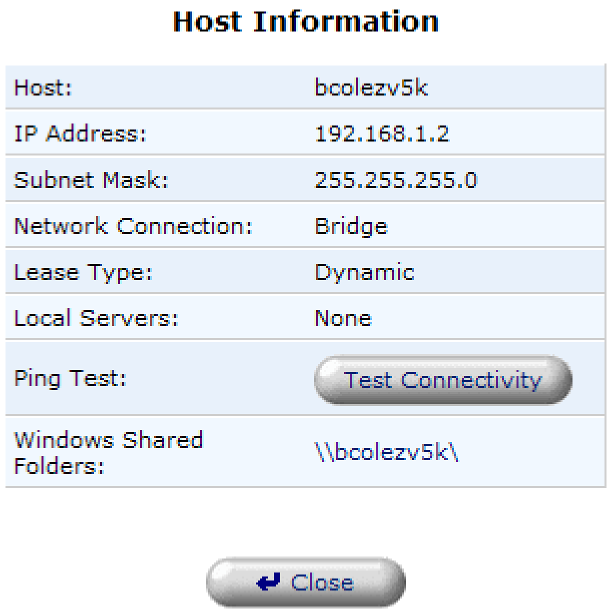
The network map simply depicts the various network elements associated with the CAP, including:

- Local network computers that have learned their addresses from the CAP via DHCP
- Firewall
- Converged Access Point
- External Internet/WAN network interface
- Internal network interface (Ethernet)



Since the CAP is equipped with multiple LAN interfaces, the local network is shown sub-divided into sub-networks (or subnets) and you can see which computers are part of each sub-network.

You can click on each computer shown to see it's IP configuration and test access to that station.

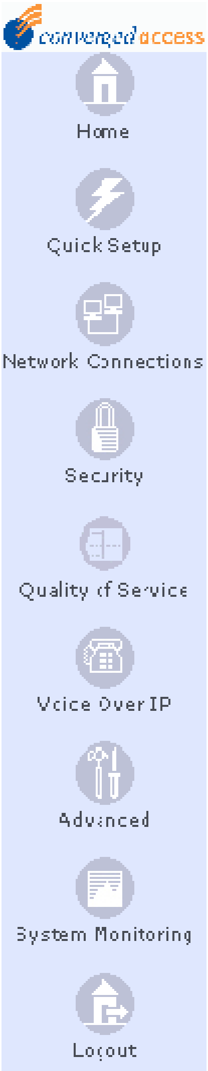


Host Information

Host:	bcolezv5k
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Network Connection:	Bridge
Lease Type:	Dynamic
Local Servers:	None
Ping Test:	Test Connectivity
Windows Shared Folders:	\\bcolezv5k\

3.3 Left Sidebar

The web-based management screens have been grouped into several subject areas and may be accessed by clicking on the appropriate icon in the left sidebar. The subject areas are:



Home: Display the CAP's network map

Quick Setup: Quickly configure your Internet/WAN connection (see section 2 for details)

Network Connections: More detailed configuration of the network interfaces, and also the location to create and configure VPN's (see section 4 for details).

Security: Configure the Firewall and regulate communications between the Internet and the enterprise network (see section 5 for details).

Quality of Service: Bandwidth management and traffic prioritization configuration (see section 6 for details).

Voice Over IP: Analog voice gateway configuration, phone and address book settings (see section 10 for details).

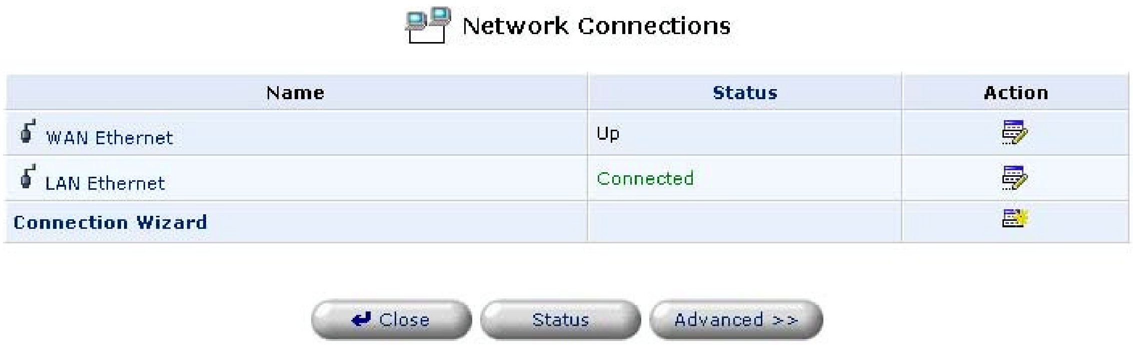
Advanced: System upgrade, static routes, SNMP, system setting, Dynamic DNS, Radius, Date/Time, Users, etc. (see section 7 for details)

System Monitoring: View network status, traffic statistics and the system log (see section 8 for details)

Logout: Log out from the CAP

3.4 Managing Lists

Lists are structures used throughout the web-based management. Lists handle user-defined entries relating to elements such as network connections, local servers, restrictions and configurable parameters. The principles outlined in this section apply to all list structures in the web-based management.



Network Connections

Name	Status	Action
WAN Ethernet	Up	✎
LAN Ethernet	Connected	✎
Connection Wizard		✚

This figure illustrates a typical list structure. Each row defines an entry in the list.

The following buttons located in the ’Action’ column enable **adding, editing** and **deleting** list entries:

Use the **Add** button to add an item to the list

Use the **Edit** button to edit an item from the list.

Use the **Delete** button to delete an item from the list.

4

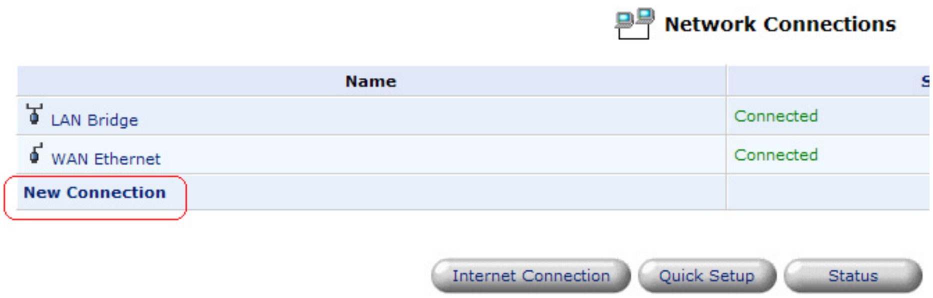
4.0 Creating VPN Connections

When you initially configured your CAP’s Internet/WAN connection under the ‘Quick Setup’, depending on your link, you may have configured the CAP as a PPTP VPN client. This section details how to configure the CAP for additional VPN terminations beyond the PPTP client setup.

4.1 Overview

The ‘New Connection’ button is where you start to create a new virtual connection such as a IPSec or L2TP VPN, or to establish the CAP as a PPTP server for remote clients. The management interface guides you through a series of selection choices, collecting all the necessary information for the new connection, and checks the status of the connection once you complete it. In some cases, you will be required to specify networking parameters that must be provided by your Internet Service Provider (ISP).

To create a new connection, click on the ’Network Connection’ icon on the side bar. The ’Network Connections’ screen will appear, listing all current connections. To create a new connection, click on either the ‘New Connection’ text, or the ‘Edit’ icon provided at the end of its row.



Network Connections

Name	S
LAN Bridge	Connected
WAN Ethernet	Connected
New Connection	

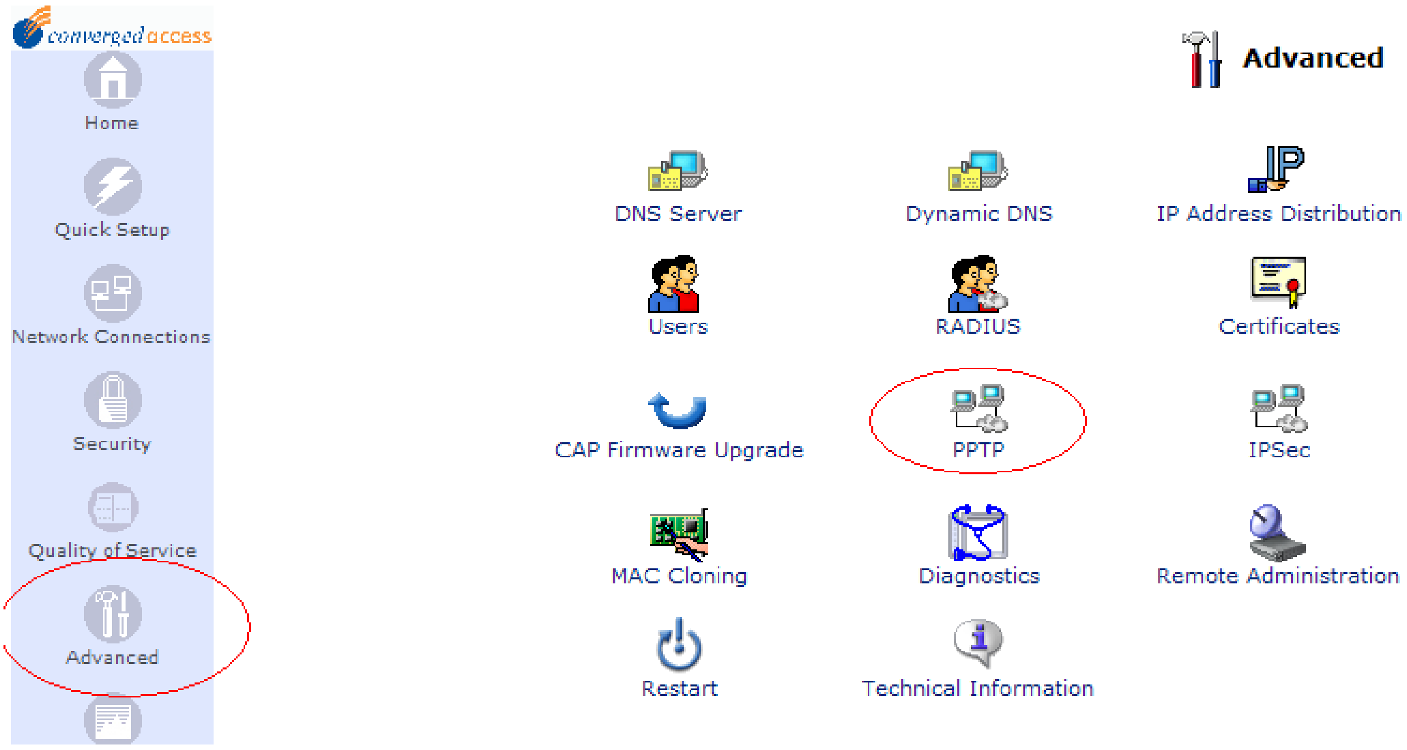
NOTE: As you click through the configuration screens, you will find the following buttons at the bottom of many of them: 'Back', 'Next' and 'Cancel'. Use the 'Back' button to go back and change selections and parameters, or the 'Next' button to confirm your selection choices and advance. The 'Cancel' button will exit the setup and return you to the 'Network Connections' screen.

4.2 Configuring the CAP as a PPTP Server

Point-to-Point Tunneling Protocol (PPTP) is an extension of the Internet's Point-to-Point Protocol (PPP) that allows two systems to establish a Virtual Private Network (VPN) over the Internet by creating a virtual serial link. PPP encapsulates data from the Network layer (e.g.: IP, IPX) into the HDLC format, this data is encapsulated into the GRE protocol format and is sent over the public network.

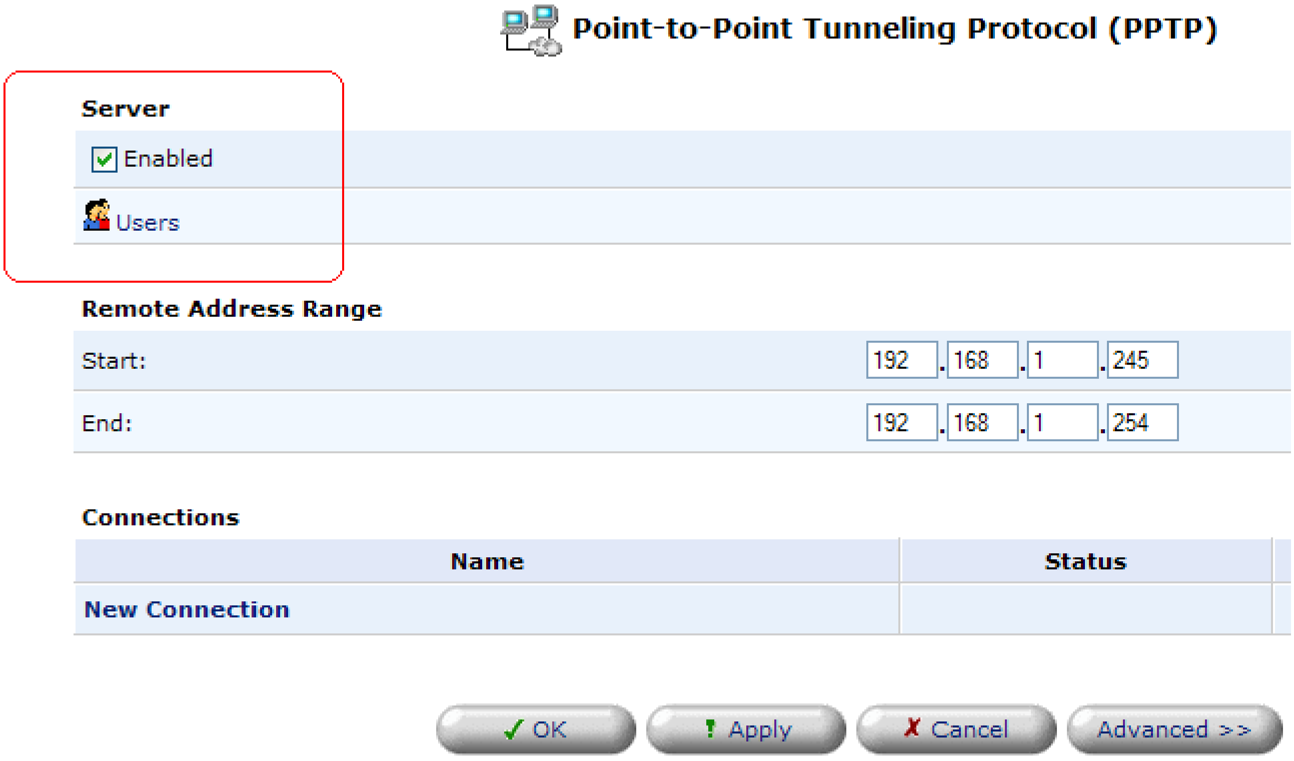
The CAP can terminate up to 25 total VPN tunnels, including IPSec, L2TP, and/or PPTP tunnels. To enable and configure the CAP as a PPTP server in order to terminate PPTP clients onto the CAP, perform the following steps:

1. Click on Advanced, then click on PPTP



2. Under this configuration window, you can configure the CAP as both a PPTP client, and as a PPTP Server. You may already have configured the CAP as a client under the 'Quick Setup' section, but if you need to terminate PPTP clients on the CAP, this is the proper location to activate the PPTP server and define your clients list. As stated previously, the CAP can terminate up to 25 simultaneous VPN tunnels.

Check the Server 'Enabled" box, then click on 'Users' to configure your list of PPTP clients that may connect to the CAP.



Point-to-Point Tunneling Protocol (PPTP)

Server

☑ Enabled

Users

Remote Address Range

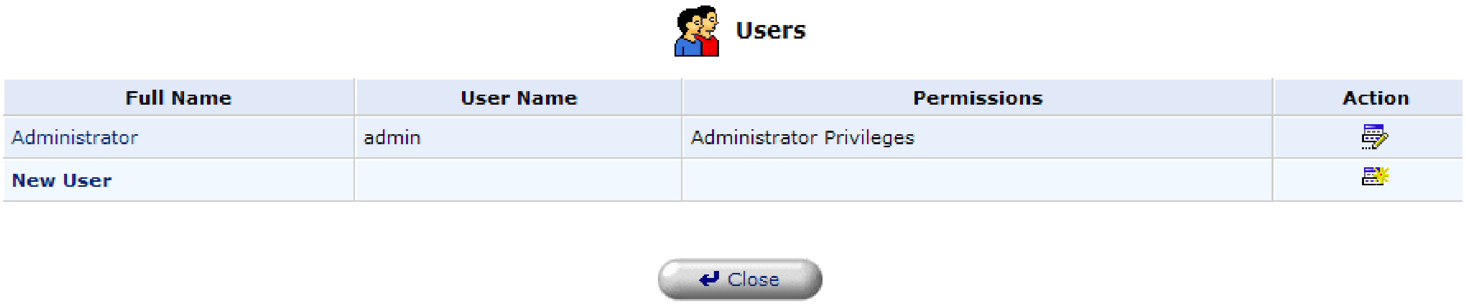
Start: 192 . 168 . 1 . 245

End: 192 . 168 . 1 . 254

Connections

Name	Status
New Connection	

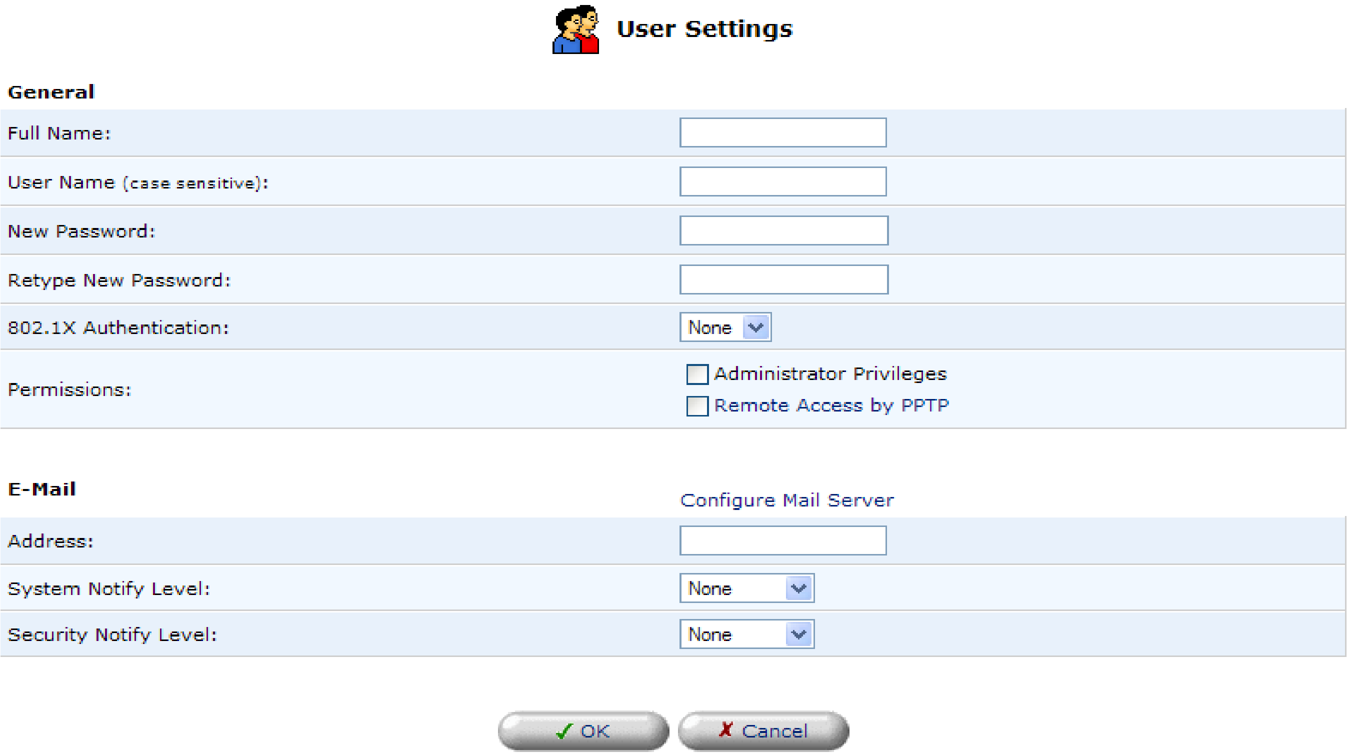
3. Configure your user PPTP 'User List' by clicking on 'New User'



Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Privileges	
New User			

4. Enter the new user's information and hit the 'OK' button to save it. Repeat process for each PPTP client of the CAP.



User Settings

General

Full Name:	
User Name (case sensitive):	
New Password:	
Retype New Password:	
802.1X Authentication:	None
Permissions:	□ Administrator Privileges □ Remote Access by PPTP

E-Mail Configure Mail Server

Address:	
System Notify Level:	None
Security Notify Level:	None

5. After configuring your PPTP clients, note that changing any of the user parameters will prompt the connection associated with the user to terminate. You should manually re-activate the connection to re-establish the tunnel.

4.2.1 Email Notification on the PPTP client

You can use email notification to receive indications of system events for a pre-defined severity classification. The available types of events are 'System' or 'Security' events. The available severity of events are 'Error', 'Warning' and 'Information'. If the 'Information' level is selected, the user will receive notification of 'Information', 'Warning' and 'Error' events. If the 'Warning' level is selected the user will receive notification of 'Warning' and 'Error' events etc.

To configure email notification for a specific user:

- First make sure you have configured an outgoing mail server in 'System Settings'. A click on the 'Configure Mail Server' link will display the 'System Settings' page were you can configure the outgoing mail server.

- Enter the user's email address in the 'Address' field in the 'Email' section.

- Select the 'System' and 'Security' notification levels in the 'System Notify Level' and 'Security Notify Level' combo boxes respectively.

4.3 IPSec VPN Connections

IPSec is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPSec protocols include:

- AH (Authentication Header) provides packet-level authentication.
- ESP (Encapsulating Security Payload) provides encryption and authentication.
- IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two services.

IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to inter-operate.

4.3.1 Technical Specifications

- Security architecture for the Internet Protocol
- Connection type: Tunnel, Transport
- Key management: Manual, Automatic, Internet Key Exchange
- Gateway authentication: X.509, RSA signatures, pre-shared secret key, ISAKMP (manual and aggressive modes)
- IP protocols: ESP, AH
- Encryption: AES, 3DES, DES, HW encryption integration
- Authentication: MD5, SHA-1
- IP Payload compression
- Interoperability: Windows 2000, FreeS/WAN, OpenBSD, FreeBSD, Cisco Routers, Nortel, Windows NT, Checkpoint Firewall-1, F-Secure VPN for Windows, Xedia Access Point/QVPN, PGP 6.5 Mac and Windows IPSec Client, PGPnet, IRE Safenet/Intel LANrover, Sun Solaris, NetScreen

NOTE: The CAP supports the creation of up a total of to 25 VPN tunnels, including IPSec, PPTP, and L2TP tunnels.

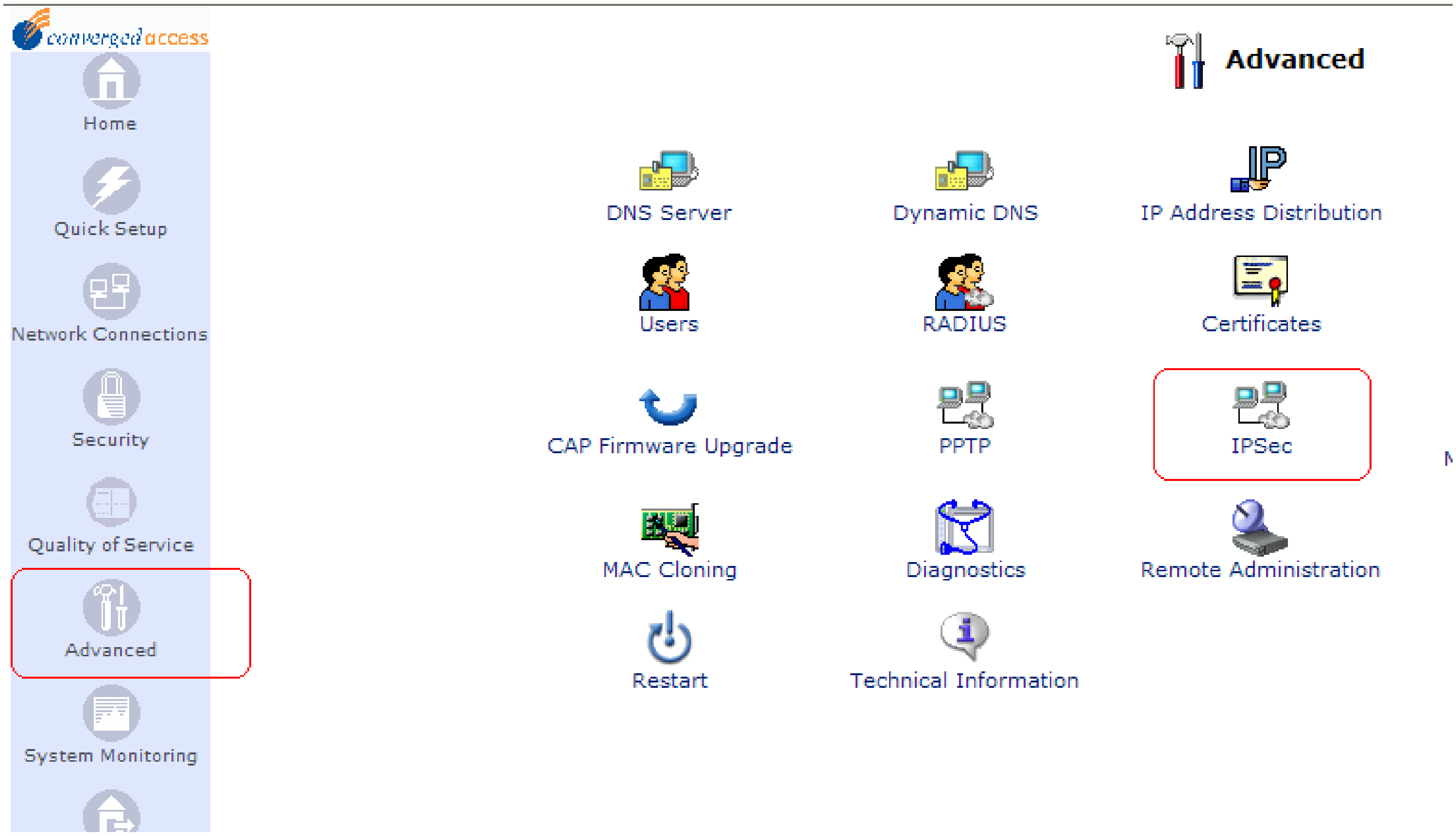
The CAP's IPSec configuration supports two IPSec modes: 'Network-to-Network' and 'Network-to-Host' IPSec.

With 'Network-to-Network', *all* traffic to and from a remote NETWORK is tunneled within IPSec between the CAP and a remote IPSec capable device, such as a VPN Router.

With 'Network-to-Host', *all* traffic to and from a remote HOST is tunneled within IPSec between the CAP and a IPSec capable hosts, such as Windows 2000 VPN clients.

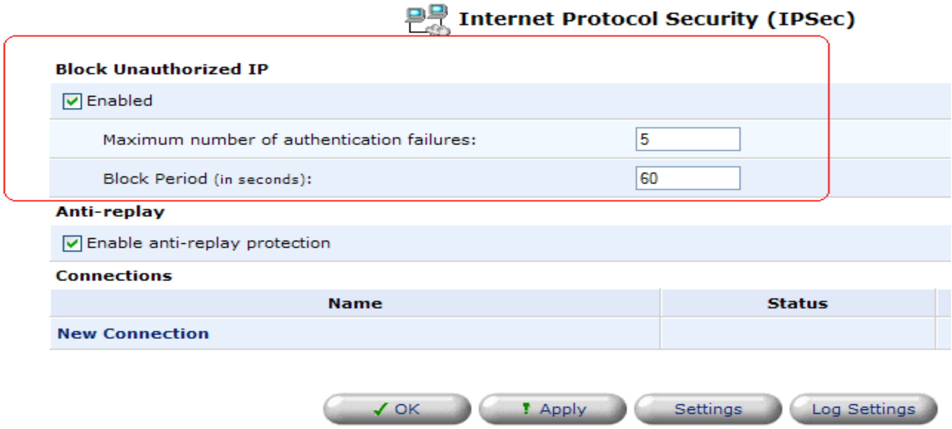
4.3.2 Basic IPSec Settings

1. Press the ’Advanced’ icon, then the ‘IPSec’ icon.



2. Select the ’Enabled’ checkbox to block unauthorized IPSec network connection to the CAP. To define what an unauthorized IPSec connection means and how long to block it, specify the following:

- Maximum number of authentication failures
- Block period (in seconds)



Internet Protocol Security (IPSec)

Block Unauthorized IP

☑ Enabled

Maximum number of authentication failures:	5
Block Period (in seconds):	60

Anti-replay

☑ Enable anti-replay protection

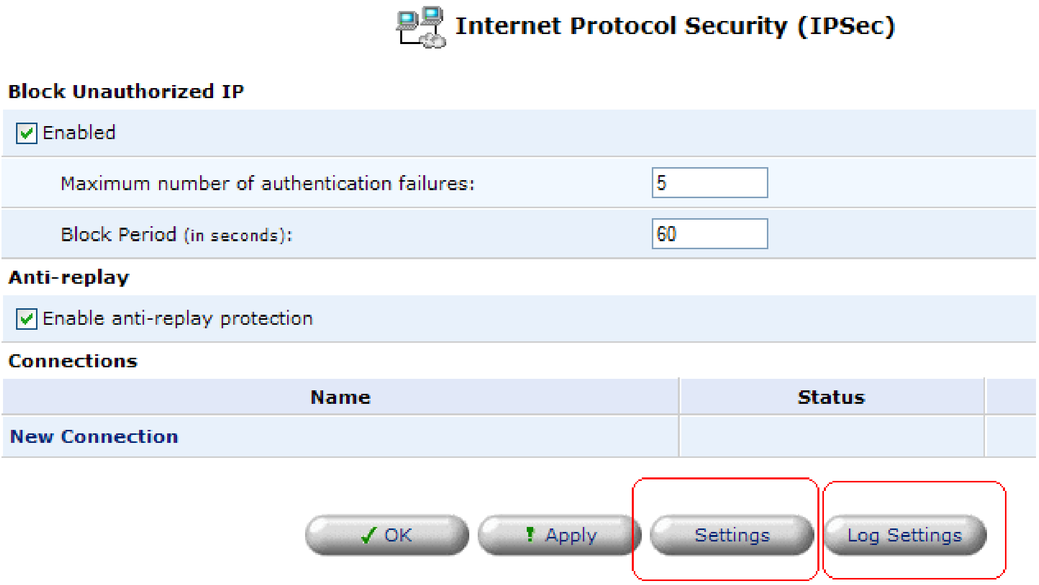
Connections

Name	Status
New Connection	

4.3.3 Key Management

1. Press the 'Settings' button view the CAP's public key. If necessary, you can copy the public key from this screen.

2. Press the 'Recreate Key' button to recreate the pubic key, or the 'Refresh' button to refresh the key displayed in this screen.



Internet Protocol Security (IPSec)

Block Unauthorized IP

☑ Enabled

Maximum number of authentication failures: 5

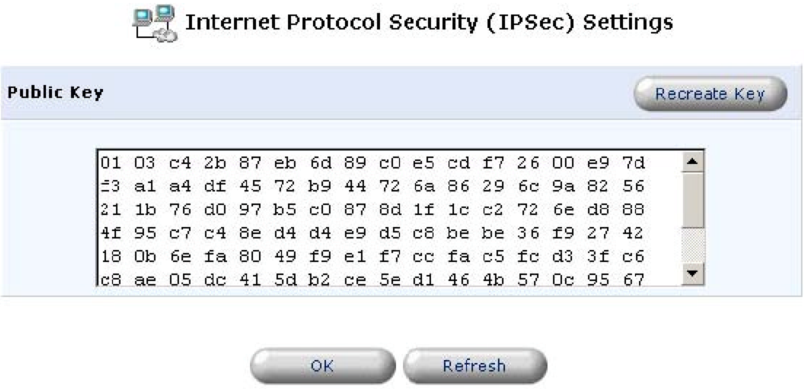
Block Period (in seconds): 60

Anti-replay

☑ Enable anti-replay protection

Connections

Name	Status
New Connection	



Internet Protocol Security (IPSec) Settings

Public Key

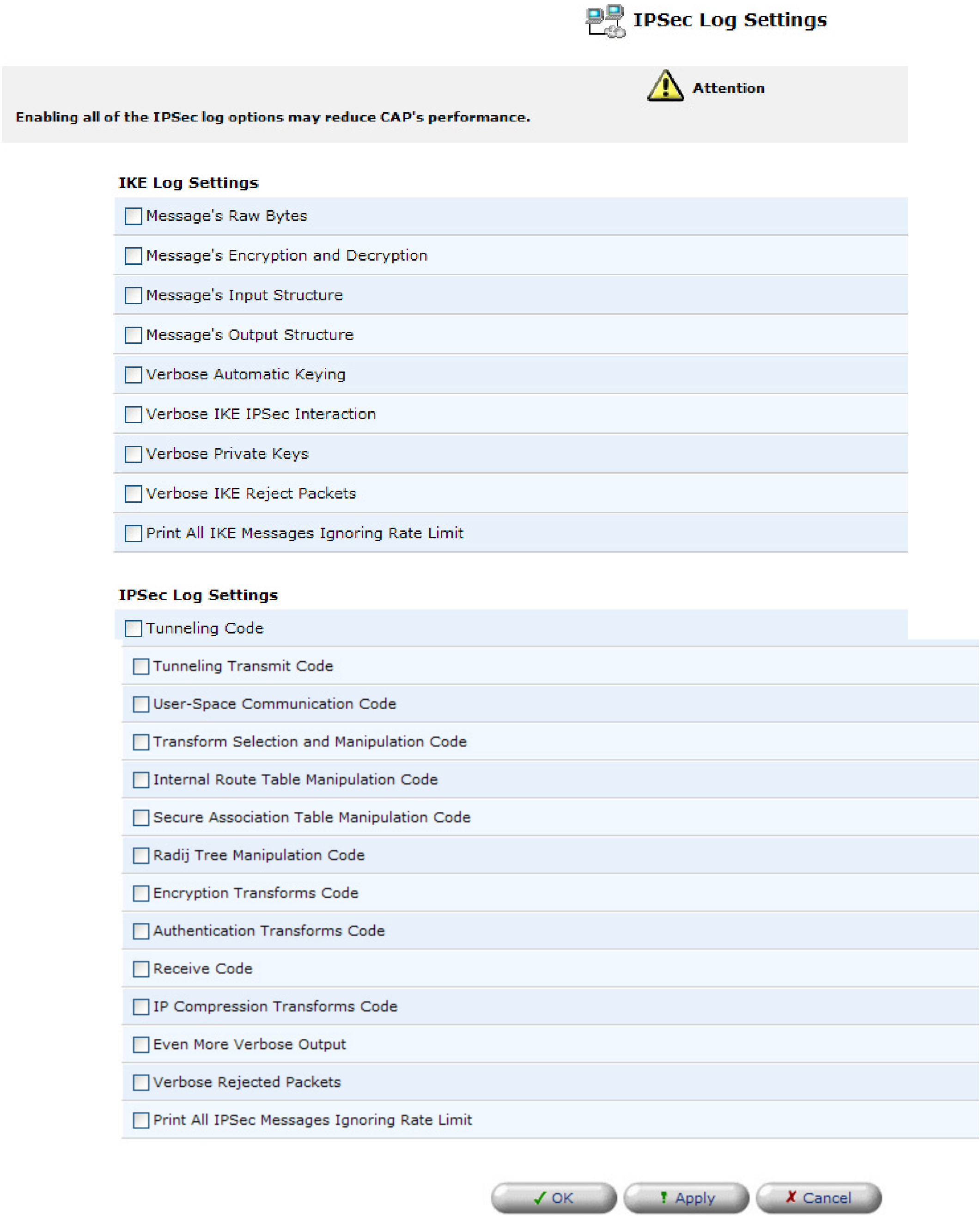
```
01 03 c4 2b 87 eb 6d 89 c0 e5 cd f7 26 00 e9 7d
e3 a1 a4 df 45 72 b9 44 72 6a 86 29 6c 9a 82 56
21 1b 76 d0 97 b5 c0 87 8d 1f 1c c2 72 6e d8 88
4f 95 c7 c4 8e d4 d4 e9 d5 c8 be be 36 f9 27 42
18 0b 6e fa 80 49 f9 e1 f7 cc fa c5 fc d3 3f c6
c8 ae 05 dc 41 5d b2 ce 5e d1 46 4b 57 0c 95 67
```

4.3.4 Log Settings

The IPSec Log can be used to identify and analyze the history of the IPSec package commands, attempts to create connections, etc. IPSec activity, as well as that of other CAP modules, is displayed together in this view.

1. Press the ''Log Settings' button.

2. Select the check-boxes relevant to the information you would like the IPSec log to record.



IPSec Log Settings

Attention

Enabling all of the IPSec log options may reduce CAP's performance.

IKE Log Settings

- □ Message's Raw Bytes
- □ Message's Encryption and Decryption
- □ Message's Input Structure
- □ Message's Output Structure
- □ Verbose Automatic Keying
- □ Verbose IKE IPSec Interaction
- □ Verbose Private Keys
- □ Verbose IKE Reject Packets
- □ Print All IKE Messages Ignoring Rate Limit

IPSec Log Settings

- □ Tunneling Code
- □ Tunneling Transmit Code
- □ User-Space Communication Code
- □ Transform Selection and Manipulation Code
- □ Internal Route Table Manipulation Code
- □ Secure Association Table Manipulation Code
- □ Radij Tree Manipulation Code
- □ Encryption Transforms Code
- □ Authentication Transforms Code
- □ Receive Code
- □ IP Compression Transforms Code
- □ Even More Verbose Output
- □ Verbose Rejected Packets
- □ Print All IPSec Messages Ignoring Rate Limit

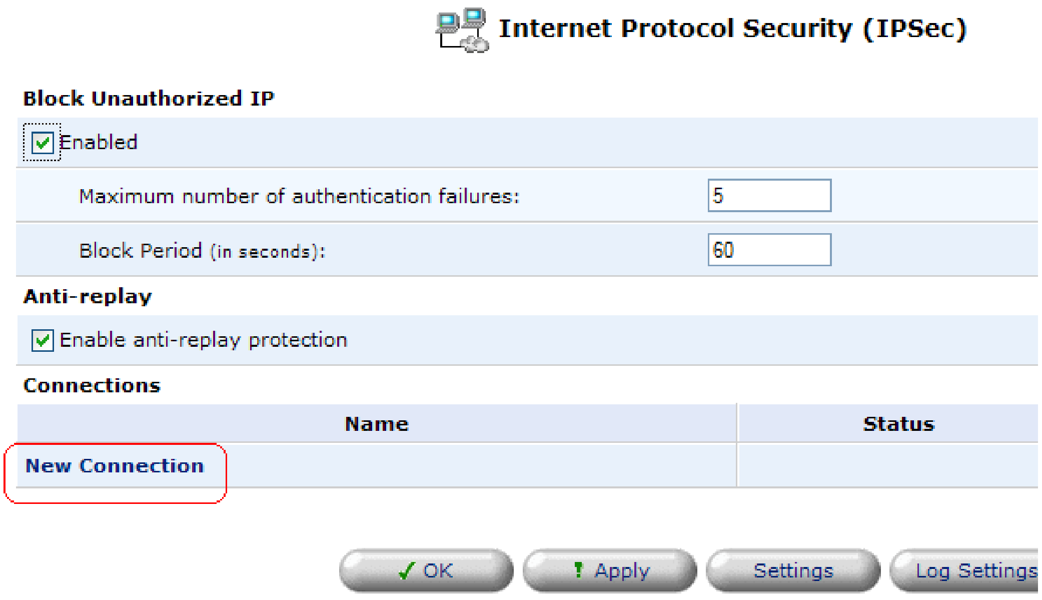
4.3.5 Configuring an IPSec VPN

4.3.5.1 Network-to-Network IPSec VPN Configuration

With ‘Network-to-Network’, *all* traffic to and from a remote NETWORK is tunneled within IPSec between the CAP and a remote IPSec capable device, such as a VPN Router.

To configure a Network-to-Network IPSec VPN, perform the following steps:

1. Under ‘Advanced’, ‘IPSec’, click on ‘New Connection”



Internet Protocol Security (IPSec)

Block Unauthorized IP

☑ Enabled

Maximum number of authentication failures:	5
Block Period (in seconds):	60

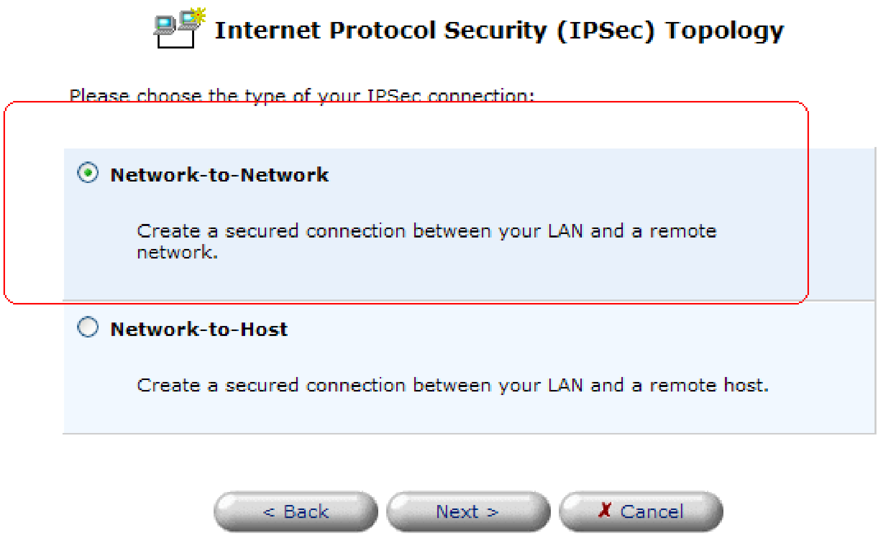
Anti-replay

☑ Enable anti-replay protection

Connections

Name	Status
New Connection	

2. Make sure the radio button for Network-to-Network is selected, then hit ‘Next’



Internet Protocol Security (IPSec) Topology

Please choose the type of your IPSec connection:

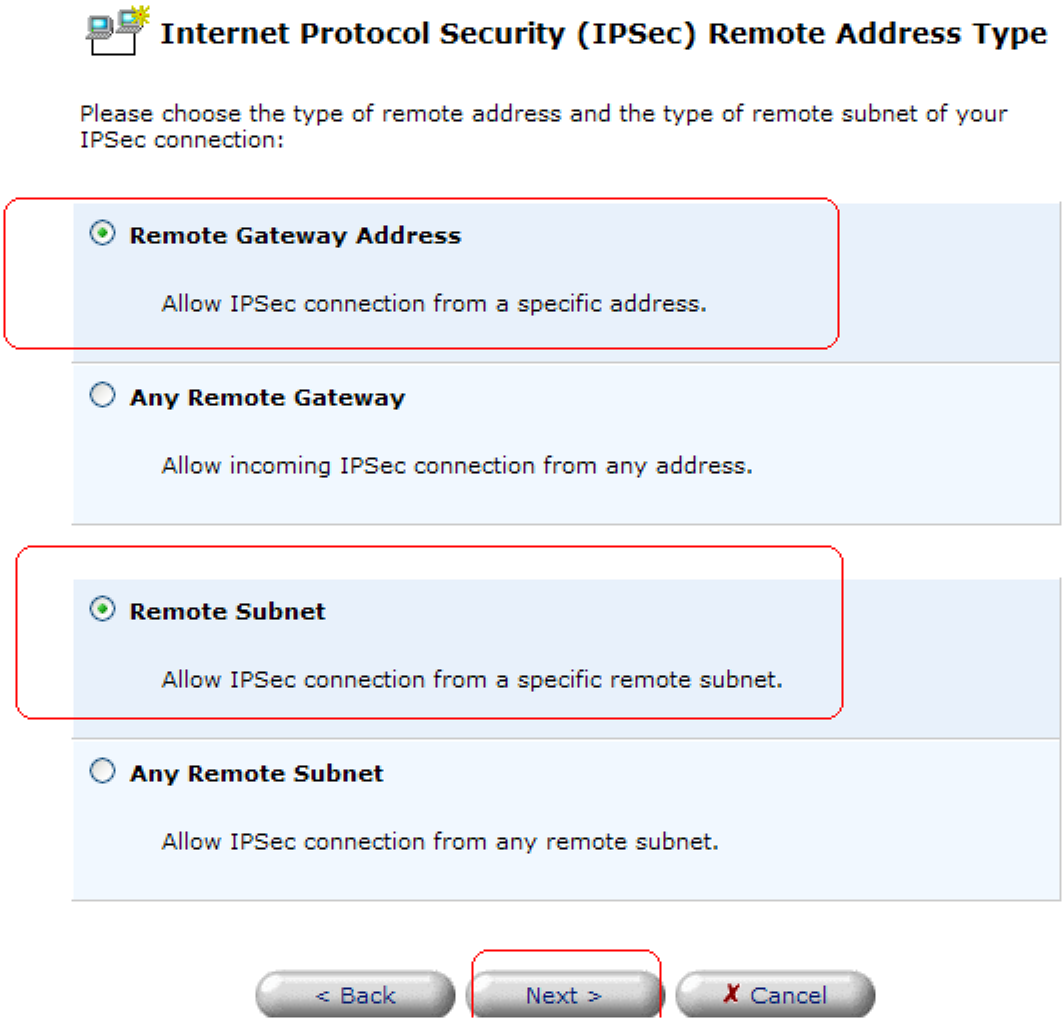
● **Network-to-Network**

Create a secured connection between your LAN and a remote network.

○ **Network-to-Host**

Create a secured connection between your LAN and a remote host.

3. You need to specify if you want ‘Any Remote Gateway’ to be allowed into this IPSec connection, or if you need to have a single ‘Remote Gateway Address’ defined. Also, you need to define if the source addresses allowed through this VPN will be allowed from a ‘Any Remote Subnet’, or from a single ‘Remote Subnet’. Make your selection and click ‘Next’. We’ll assume you are defining the IP address of the IPSec tunnel endpoint, as well as specifying the subnet address allowed through the connection.



Internet Protocol Security (IPSec) Remote Address Type

Please choose the type of remote address and the type of remote subnet of your IPSec connection:

● **Remote Gateway Address**

Allow IPSec connection from a specific address.

○ **Any Remote Gateway**

Allow incoming IPSec connection from any address.

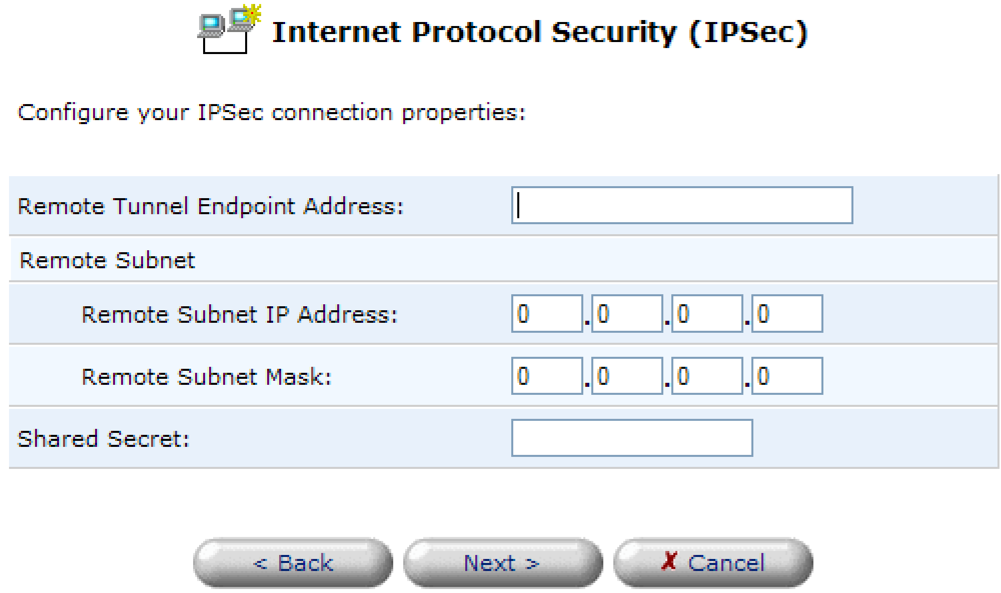
● **Remote Subnet**

Allow IPSec connection from a specific remote subnet.

○ **Any Remote Subnet**

Allow IPSec connection from any remote subnet.

4. Enter the IP address of your IPSec VPN gateway at the far end of this connection, as well as define the subnet allowed thru the link.

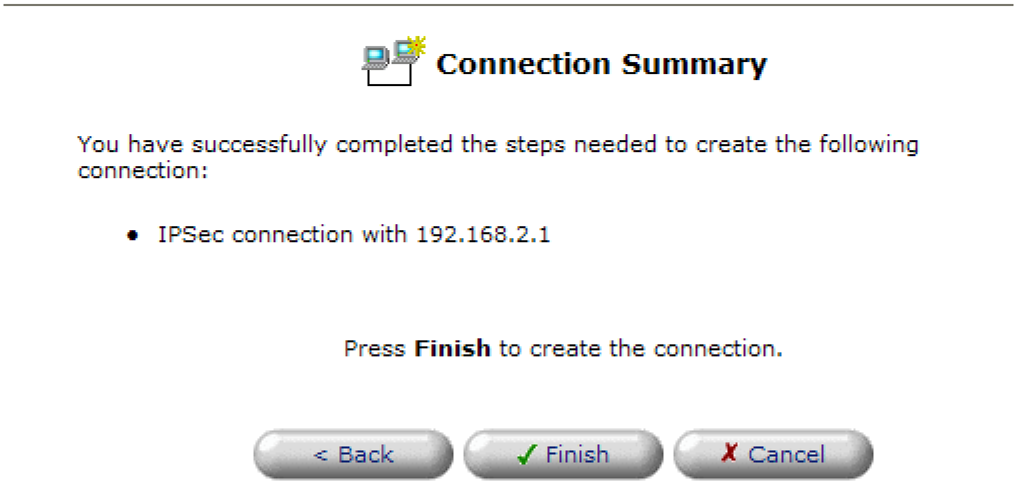


Internet Protocol Security (IPSec)

Configure your IPSec connection properties:

Remote Tunnel Endpoint Address:	
Remote Subnet	
Remote Subnet IP Address:	0 . 0 . 0 . 0
Remote Subnet Mask:	0 . 0 . 0 . 0
Shared Secret:	

5. Click ‘Finish’ to save your IPSec Network-to-Network VPN connection



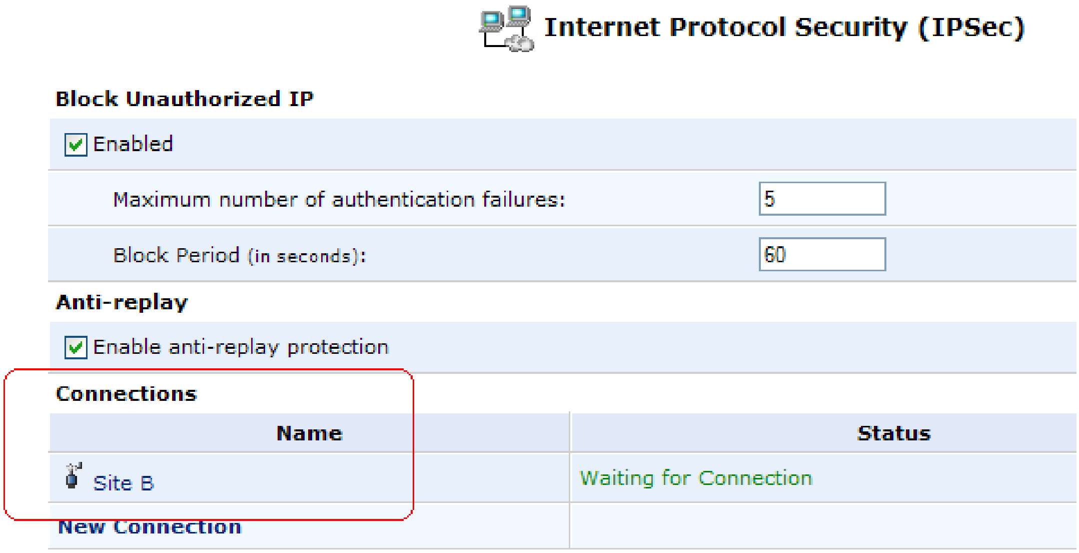
Connection Summary

You have successfully completed the steps needed to create the following connection:

- IPSec connection with 192.168.2.1

Press **Finish** to create the connection.

You can find your new IPSec connection under the ‘IPSec’ ‘Connections’ display



Internet Protocol Security (IPSec)

Block Unauthorized IP

☑ Enabled

Maximum number of authentication failures:	5
Block Period (in seconds):	60

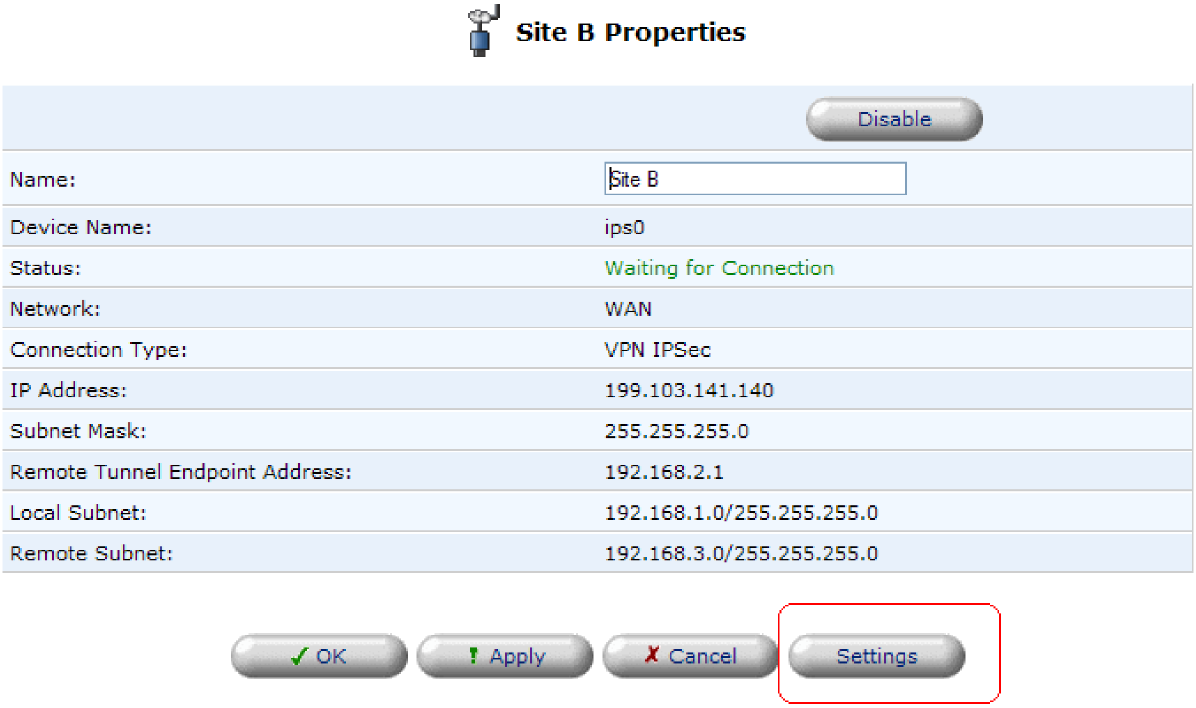
Anti-replay

☑ Enable anti-replay protection

Connections

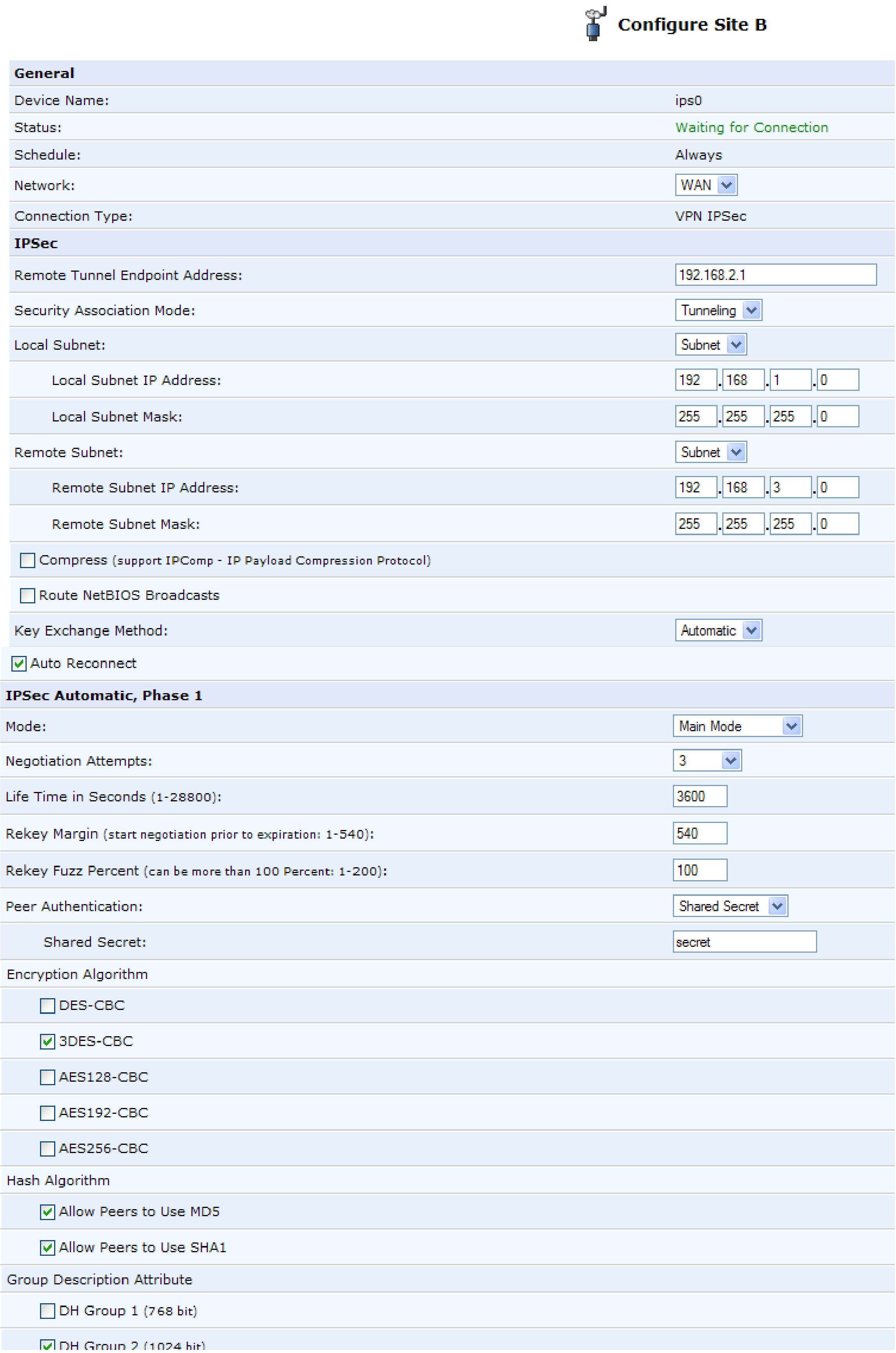
Name	Status
Site B	Waiting for Connection
New Connection	

Click on the Connection Name (ie. Site B above) to see a summary of the VPN. Then, click on ‘Settings’ to enable further options on the IPSec VPN connection.



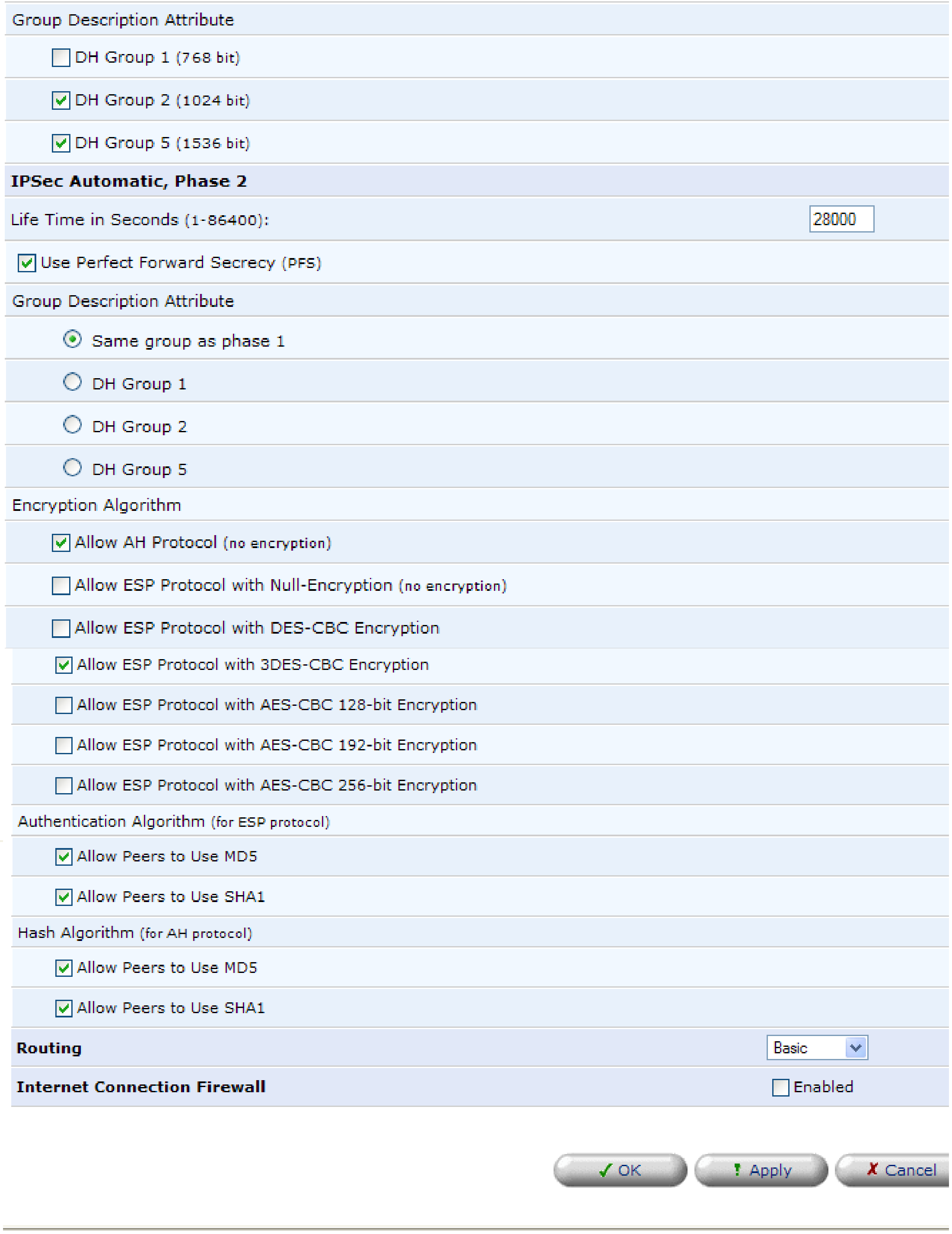
Site B Properties

Name:	Site B
Device Name:	ips0
Status:	Waiting for Connection
Network:	WAN
Connection Type:	VPN IPSec
IP Address:	199.103.141.140
Subnet Mask:	255.255.255.0
Remote Tunnel Endpoint Address:	192.168.2.1
Local Subnet:	192.168.1.0/255.255.255.0
Remote Subnet:	192.168.3.0/255.255.255.0



Configure Site B

General	
Device Name:	ips0
Status:	Waiting for Connection
Schedule:	Always
Network:	WAN
Connection Type:	VPN IPSec
IPSec	
Remote Tunnel Endpoint Address:	192.168.2.1
Security Association Mode:	Tunneling
Local Subnet:	Subnet
Local Subnet IP Address:	192 . 168 . 1 . 0
Local Subnet Mask:	255 . 255 . 255 . 0
Remote Subnet:	Subnet
Remote Subnet IP Address:	192 . 168 . 3 . 0
Remote Subnet Mask:	255 . 255 . 255 . 0
☐ Compress (support IPComp - IP Payload Compression Protocol)	
☐ Route NetBIOS Broadcasts	
Key Exchange Method:	Automatic
☑ Auto Reconnect	
IPSec Automatic, Phase 1	
Mode:	Main Mode
Negotiation Attempts:	3
Life Time in Seconds (1-28800):	3600
Rekey Margin (start negotiation prior to expiration: 1-540):	540
Rekey Fuzz Percent (can be more than 100 Percent: 1-200):	100
Peer Authentication:	Shared Secret
Shared Secret:	secret
Encryption Algorithm	
☐ DES-CBC	
☑ 3DES-CBC	
☐ AES128-CBC	
☐ AES192-CBC	
☐ AES256-CBC	
Hash Algorithm	
☑ Allow Peers to Use MD5	
☑ Allow Peers to Use SHA1	
Group Description Attribute	
☐ DH Group 1 (768 bit)	
☑ DH Group 2 (1024 bit)	



Group Description Attribute

☐ DH Group 1 (768 bit)

☑ DH Group 2 (1024 bit)

☑ DH Group 5 (1536 bit)

IPSec Automatic, Phase 2

Life Time in Seconds (1-86400): 28000

☑ Use Perfect Forward Secrecy (PFS)

Group Description Attribute

● Same group as phase 1

○ DH Group 1

○ DH Group 2

○ DH Group 5

Encryption Algorithm

☑ Allow AH Protocol (no encryption)

☐ Allow ESP Protocol with Null-Encryption (no encryption)

☐ Allow ESP Protocol with DES-CBC Encryption

☑ Allow ESP Protocol with 3DES-CBC Encryption

☐ Allow ESP Protocol with AES-CBC 128-bit Encryption

☐ Allow ESP Protocol with AES-CBC 192-bit Encryption

☐ Allow ESP Protocol with AES-CBC 256-bit Encryption

Authentication Algorithm (for ESP protocol)

☑ Allow Peers to Use MD5

☑ Allow Peers to Use SHA1

Hash Algorithm (for AH protocol)

☑ Allow Peers to Use MD5

☑ Allow Peers to Use SHA1

Routing Basic

Internet Connection Firewall ☐ Enabled

4.3.6 IPSec Advanced Configuration Parameters Definitions

As you can see, there are an extensive variety of options you can configure on IPSec VPN connections. The following information provides summary details on what those options represent to your IPSec VPN connection.

Enable those options that your connection requires, and hit ‘Apply’ to activate them.

MTU Mode:

Maximum Transmission Unit (MTU) is the largest physical packet size, measured in bytes, that will be transmitted through the IPSec connection. Packets larger than the MTU are divided into smaller packets before being sent. You can set the MTU size manually, or select an automatic MTU mode.

Host Name or IP Address of Remote Tunnel Endpoint:

The IP address of your IPSec peer.

Transport Type:

Transport type can be ’Tunneling’ or ’Transport’. ’Transport’ needs no explicit configuration. ’Transport’ type requires that you configure the following parameters:

- Local Subnet
- Local Subnet Mask
- Remote Subnet
- Remote Subnet Mask

Compress (Support IPCOMP protocol):

Select this check-box to use the IPComp protocol.

Key Exchange Method:

The key exchange method can be ’Manual or ’Automatic’.

The following are the parameters that are required to configure an ’Automatic’ key exchange:

Negotiation attempts:

Select the number of negotiation attempts to be performed in Phase 1 of the automatic key exchange method.

Life Time in Seconds:

The length of time before a security association automatically performs a re-negotiation. A short Life Time increases security by forcing the VPN hosts to update the encryption and authentication keys. However, every time the VPN Tunnel renegotiates, users accessing remote resources are disconnected. Therefore, the default Life Time is recommended.

Rekey Margin:

Specifies how long before connection expiry should attempts to negotiate a replacement begin. It is similar to that of the Key Life Time and is given as an integer denoting seconds.

Rekey Fuzz Percent:

Specifies the maximum percentage by which Rekey Margin should be randomly increased to randomize rekeying intervals.

Phase 1 Peer Authentication:

Select the method by which the CAP will authenticate you IPSec peer:

- Shared secret
- RSA Signature
- Certificate

Phase 1 Encryption Algorithm:

Select the encryption algorithms that the CAP will attempt to use when negotiating with the IPSec peer.

Hash Algorithm:

Select the hash algorithms that the CAP will attempt to use when negotiating with the IPSec peer.

Use Perfect Forward Secrecy (PFS):

Select whether Perfect Forward Secrecy of keys is desired on the connection's keying channel (with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier).

ESP:

Select the encryption and authentication algorithms the CAP will use during Phase 2 of the automatic key exchange method. You can choose 3DES-CBC, DES-CBC or NULL encryption algorithms; MD5 or SHA1 authentication algorithms.

AH:

Select the hash algorithms the CAP will use during Phase 2 of the automatic key exchange method. You can choose MD5 or SHA1 authentication header algorithms.

The following are the parameters that are required to configure a 'Manual' key exchange:

Security Parameter Index – SPI:

A 32 bit value which together with IP address and security protocol uniquely identifies a particular security association. This value must be the same for both Local and Remote Tunnel.

IPSec Protocol:

Select the encryption and authentication algorithms. All algorithms values should be entered in HEX format.

Routing:

Define the connection's routing rules.

DNS Server:

Select whether the connection should obtain a DNS server address automatically. If not, configure the DNS server's IP address.

Internet Connection Firewall:

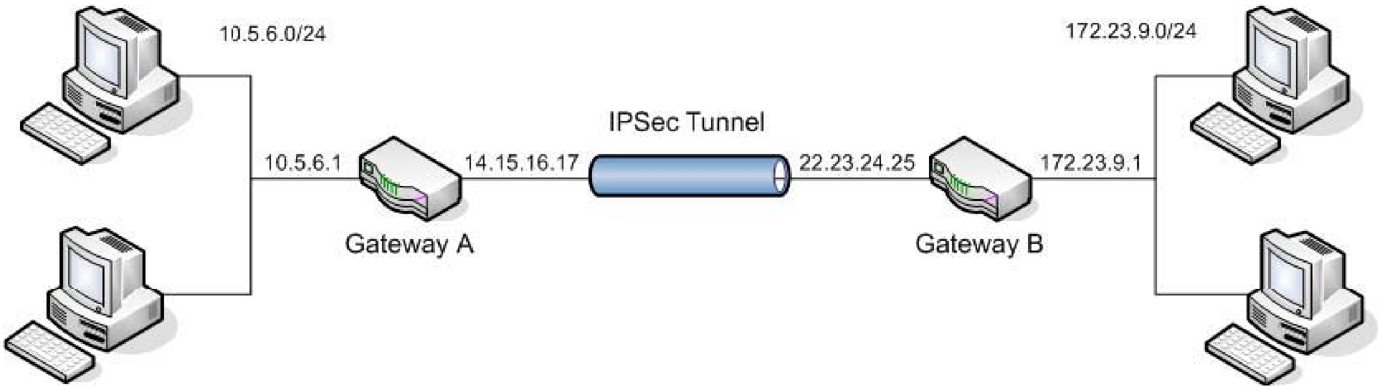
Select this check-box to include the IPSec connection as a network interface monitored by the gateway's Firewall.

4.3.6 Example IPSec VPNC Scenario

This section provides an example, describing how the VPN Consortium implemented a CAP to configure an IPSec Gateway-to-Gateway connection, with pre-shared secrets.

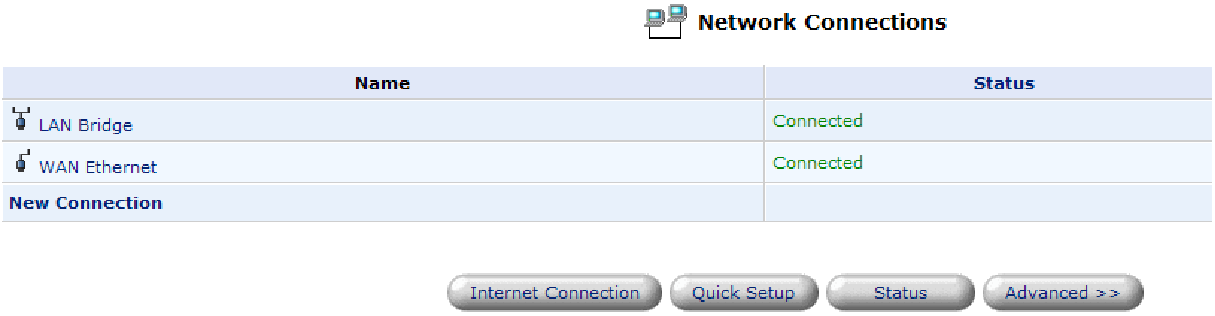
4.3.6.1 IPSec Example Diagram

An IPSec tunnel is established between Gateways A and B, serving as a transparent and secure network for clients from subnets A and B. Because the configuration of the gateways is the same except of their IP addresses this section describes only the configuration of Gateway A. The configuration of gateway B is identical, where A and B are replaced by B and A respectively.



4.3.6.2 LAN Interface Settings

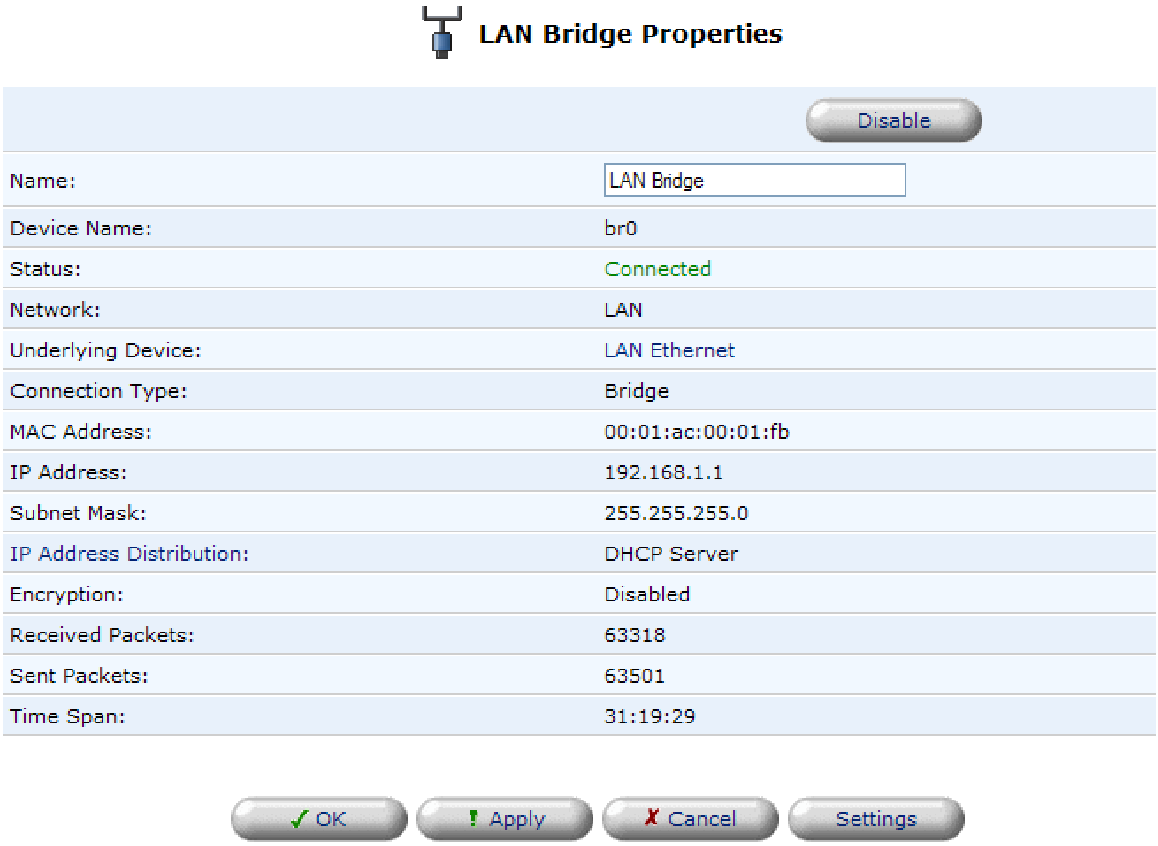
1. Click the 'Network Connections' icon on the side-bar, the 'Network Connections' screen will appear.



Network Connections

Name	Status
LAN Bridge	Connected
WAN Ethernet	Connected
New Connection	

2. Click the 'LAN Bridge' link to access the LAN Bridge's Ethernet properties, the following screen will appear.

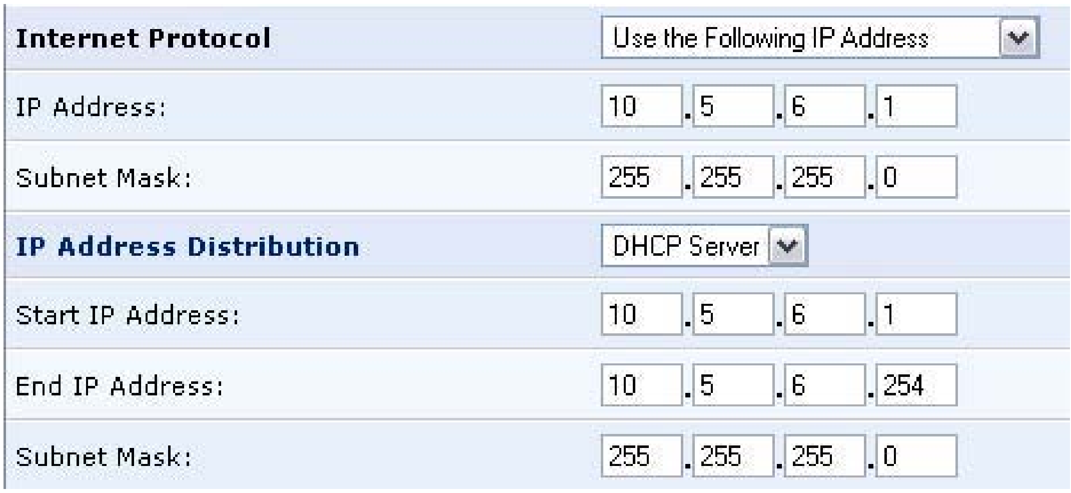


LAN Bridge Properties

	Disable
Name:	LAN Bridge
Device Name:	br0
Status:	Connected
Network:	LAN
Underlying Device:	LAN Ethernet
Connection Type:	Bridge
MAC Address:	00:01:ac:00:01:fb
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Encryption:	Disabled
Received Packets:	63318
Sent Packets:	63501
Time Span:	31:19:29

3. Click the “Settings” button, the LAN settings page will appear. Configure the following parameters.

Internet Protocol:	Select “Use the Following IP Address”.
IP Address:	Specify 10.5.6.1
Subnet Mask:	Specify 255.255.255.0
IP Address Distribution:	Select “DHCP Server”
Start IP Address:	Specify 10.5.6.1
End IP Address:	Specify 10.5.6.254
Subnet Mask:	Specify 255.255.255.0



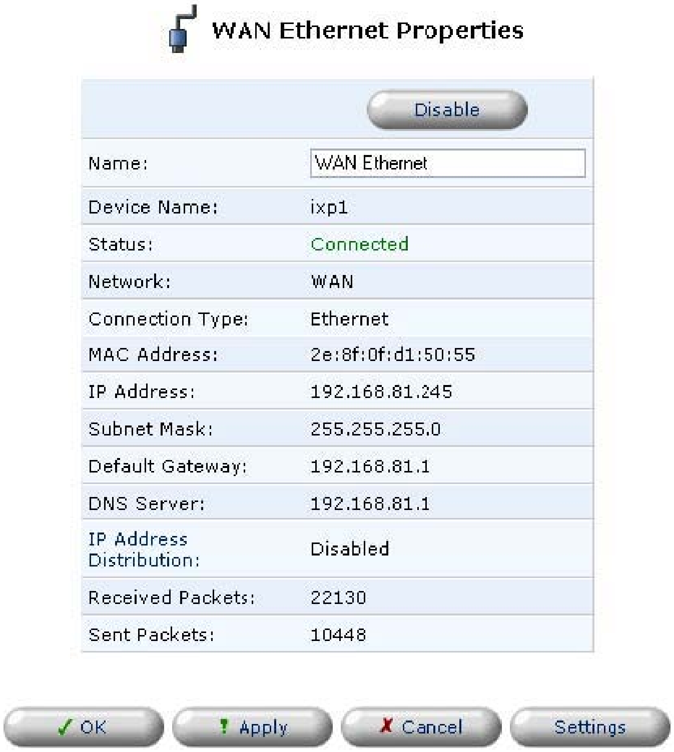
Internet Protocol	Use the Following IP Address
IP Address:	10 . 5 . 6 . 1
Subnet Mask:	255 . 255 . 255 . 0
IP Address Distribution	DHCP Server
Start IP Address:	10 . 5 . 6 . 1
End IP Address:	10 . 5 . 6 . 254
Subnet Mask:	255 . 255 . 255 . 0

4. Press the ‘Apply’ and ‘“OK’ buttons.

4.3.6.2 WAN Interface Settings

1. Click the ’Network Connections’ icon on the side-bar, the ’Network Connections’ screen will appear.

2. Click the ’WAN Ethernet’ link to access the WAN Ethernet properties, the following screen will appear.

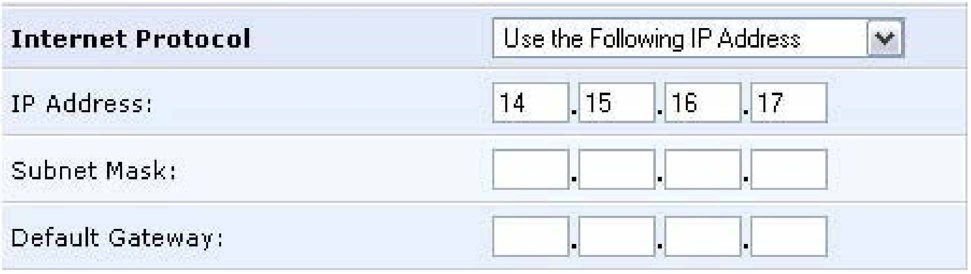


WAN Ethernet Properties

Name:	WAN Ethernet
Device Name:	ixp1
Status:	Connected
Network:	WAN
Connection Type:	Ethernet
MAC Address:	2e:8f:0f:d1:50:55
IP Address:	192.168.81.245
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.81.1
DNS Server:	192.168.81.1
IP Address Distribution:	Disabled
Received Packets:	22130
Sent Packets:	10448

3. Click the “Settings” button, the WAN settings page will appear. Configure the following parameters.

Internet Protocol:	Select “Use the Following IP Address”
IP Address	Specify 14.15.16.17
Subnet Mask	Specify the appropriate subnet mask.
Default Gateway	Specify the appropriate Default Gateway in order to enable IP routing.



Internet Protocol	Use the Following IP Address
IP Address:	14 . 15 . 16 . 17
Subnet Mask:	. . .
Default Gateway:	. . .

4. Press the ‘Apply’ and ‘OK’ buttons.

4.3.6.3 Example: Gateway-to-Gateway with Pre-shared Secrets

The following is a typical gateway-to-gateway VPN that uses a pre-shared secret for authentication. Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17. The diagrams are not provided in this example.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25.

The IKE Phase 1 parameters used are:

- Main mode
- 3DES (Triple DES)
- SHA-1
- MODP group 2 (1024 bits)
- preshared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no Kbytes re-keying The IKE

Phase 2 parameters used are:

- 3DES (Triple DES)
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for re-keying
- SA lifetime of 3600 seconds (one hour) with no Kbytes re-keying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, use the following steps:

1. Click the "Network Connections" icon on the side-bar, the "Network Connections" screen will appear.

2. Click the "New Connection" link.

3. Select "Internet Protocol Security (IPSec)".

4. Press the "Next" button. The "IPSec Topology" screen will appear.

5. Select "Network-to-Network" to create a secure connection between your LAN and a remote network.

6. Press the "Next" button. The "Remote Address Type" screen will appear.

7. Select "Remote Gateway Address" to allow an IPSec connection from a specific address.

8. Select "Remote Subnet" to allow an IPSec connection from a specific remote subnet.

9. Press the "Next" button. The "Connection Parameters" screen will appear.

10. Specify the following parameters: **Remote Tunnel Endpoint Address** Specify

22.23.24.25 **Remote Subnet IP Address** Specify 172.23.9.0 **Remote Subnet Mask** Specify 255.255.255.0 **Shared Secret** Specify “hr5xb84l6aa9r6“

11. Press the “Next” button. The “Connection Summary” screen will appear.

12. Press the “Finish” button. The “Network Connections” screen will now list the newly created IPSec connection.

13. Press the “Edit” action button. The “Connection Properties” screen will appear.

14. Press the “Settings” button. The “IPSec Configuration” screen will appear.

15. De-select the “Compress” checkbox.

16. De-select the “Allow Peers to Use MD5” checkbox (located under “Hash Algorithm”.

17. De-select the “DH Group 5 (1536 bit)” checkbox (located under “Group Description Attribute”.

18. De-select the “Allow AH Protocol (No Encryption)” checkbox (located under “Encryption Algorithm”.

19. Press the “OK” button. The “Connection Properties” screen will appear.

20. Press the “OK” button. The “Network Connections” screen will appear. Note that the IPSec connection’s status has changed to “Connected”.

21. Press the “Enterprise” button on the side-bar to view the Network Map’s depiction of the IPSec connection.

5

5.0 Security

The CAP's security suite includes comprehensive and robust security services: **Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms**. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet.

The Firewall, the cornerstone of your CAP's security suite, has been exclusively tailored to the needs of the enterprise user and has been pre-configured to provide optimum security. In addition, the Firewall has many advanced features that allow you to further customize it to your needs.

Using the management screens in the Security section you can:

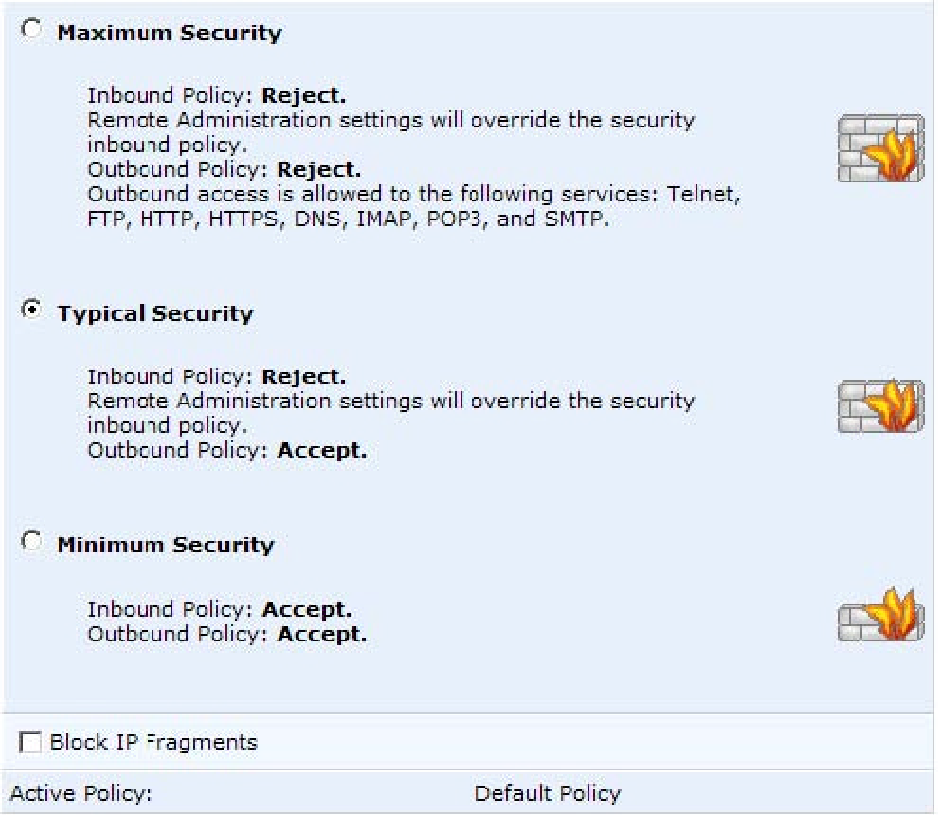
- Choose the **Security Level for the Firewall**
- Configure **'Access Control'** lists to further restrict access from the enterprise network to the Internet .
- The **'Local Servers'** screen can be used to enable access from the Internet to specified services provided by computers in the enterprise network and special Internet applications.
- The **'DMZ Host'** screen allows you to configure a LAN host to receive all traffic arriving to your gateway, which is not belonged to a known session.
- The **'Port Triggering'** screen allows you to define port triggering entries, to dynamically open the Firewall for some protocols or ports.
- The **'Remote Administration'** screen can be used to enable remote configuration of the CAP from any Internet-accessible computer.
- The **'IP/Hostname Filtering'** allows you to block LAN access to a certain host or web site on the Internet.

- **’Advanced Filtering’** allows you to implicitly control the Firewall setting and rules. (see section.

- View and configure the **Firewall Log.**

5.1 Firewall Security Overview

Use the ’Security Settings’ screen to configure the CAP’s basic security settings.



○ **Maximum Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, and SMTP.

● **Typical Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ **Minimum Security**

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

□ Block IP Fragments

Active Policy: Default Policy

The Firewall regulates the flow of data between the enterprise network and the Internet. Both incoming and outgoing data are inspected and then accepted (allowed to pass through the CAP) or rejected (barred from passing through the CAP) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside while allowing enterprise users access to the Internet services that they require.

The Firewall rules specify what types of services available on the Internet may be accessed from the enterprise network and what types of services available in the enterprise network may be accessed from the Internet. Each request for a service that the Firewall receives, whether originating in the Internet or from a computer in the enterprise network, must be checked against