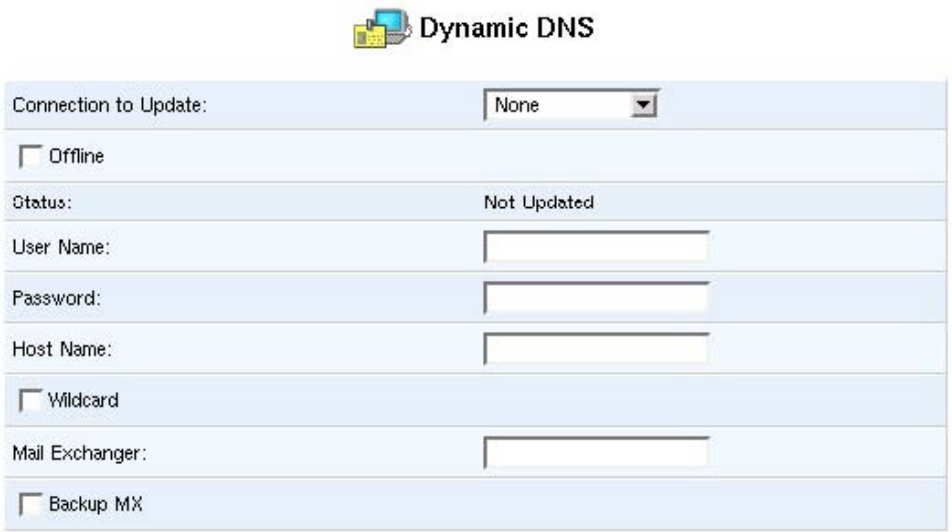
7.3 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessible from various locations on the Internet.

Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name.

Each time the IP address provided by your ISP changes, the DNS database will change 'dynamically' to reflect the change in IP address. In this way, even though a domain name's IP address will change often, your domain name will still be accessible to other hosts.

To be able to use the Dynamic DNS feature you must open a DDNS account, free of charge, at http://www.dyndns.org/account/create.html. When applying for an account, you will need to specify a user name and password. Please have them readily available when customizing the CAP's DDNS support. For more information regarding Dynamic DNS, please refer to http://www.dyndns.org.



7.3.1 Using Dynamic DNS

- 1. Click the 'DDNS' icon in the 'Advanced' screen of the Management Con sole. The DDNS table will appear.
- 2. Specify the Dynamic DNS parameters:

Connection to Update:	Select the connection to which you would like to couple the Dynamic DNS service.
Offilne	Select the 'Offline' checkbox if the host is not currently online, and you need to let people know who try to use the host.
User Name	Enter your Dyndns user name.
Host Name	Enter a subdomain name, and select a suffix from the do-main combo-box to define your host name.
Wildcard	Select the 'Wildcard' checkbox if you want anything-here.yourhost.dyndns.org to work (ie. to make things like www.yourhost.dyndns.org work).
Mail Exchanger	Enter your mail exchange server address, to redirect all e-mails arriving at your Dyndns address to your mail server.
Backup MX	Select this check box to designate the mail exchange server to be a backup server.

7.4 DHCP - Managing IP Address Distribution

Your gateway's DHCP server makes it possible to easily add computers that are configured as DHCP clients to the enterprise network. It provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to them.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as 'taken'. At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease. This allows it to update its network configuration to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.

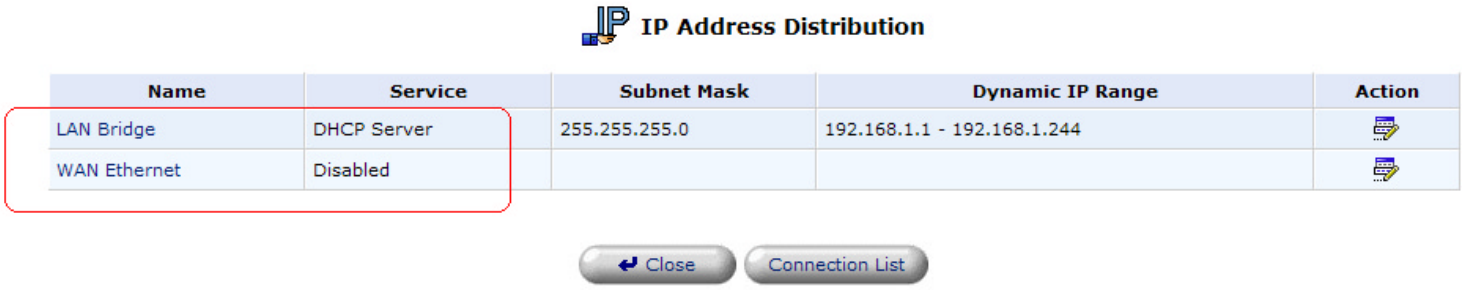
The CAP's DHCP server:

- Displays a list of all DHCP hosts devices connected to The CAP
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/disabled separately for each LAN device
- Can assign a static lease to a LAN PC so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each PC that is connected to the LAN

7.4.1 DHCP Server Summary

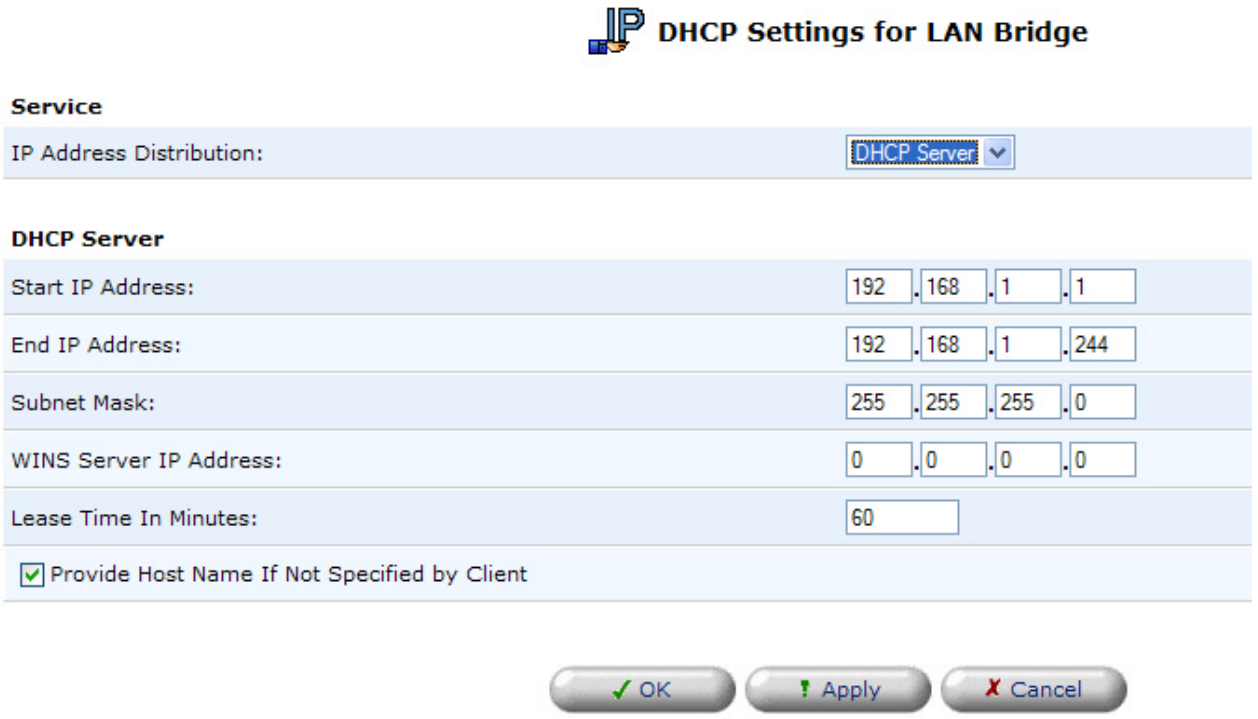
To view a summary of the services currently being provided by the DHCP server, click the 'IP Address Distribution' icon in the 'Advanced' screen of the Management Console. The 'IP Address Distribution' screen will appear.

You can view the status of your DHCP Server here for all available interfaces on the CAP.

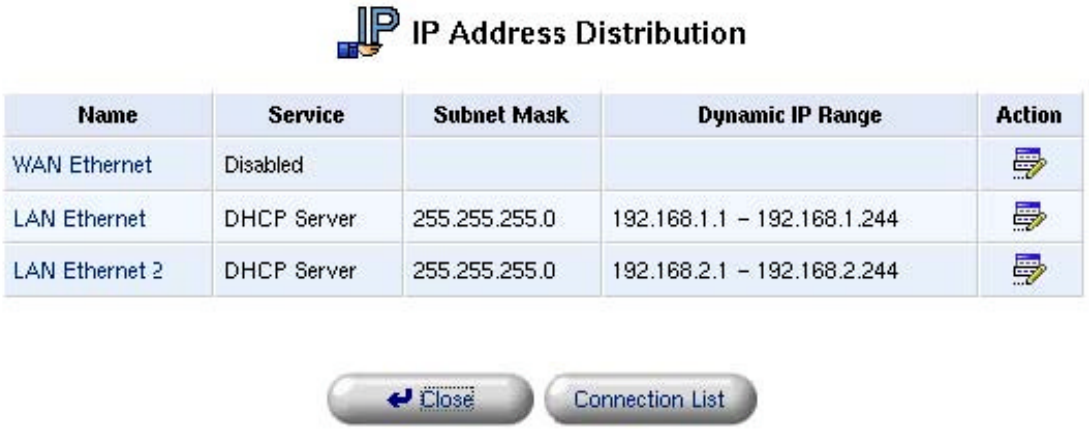


Select/ the connection 'Name' check-box to view the status of DHCP services on this interface (ie. 'LAN Bridge')

Enable/disable the DHCP server for a device.



Note that if a device is listed as 'Disabled' in the Status column then DHCP services are not being provided to hosts connected to the network through that device. This means that the gateway will not assign IP addresses to these computers—useful if you wish to work with static IP addresses only.



7.4.2 Editing DHCP Server Settings

To edit the DHCP server settings for a device:

1. Click the 'Edit' button in the Action column. The DHCP Settings for this device will appear.

2. Choose whether to enable or disable the DHCP server for this device. This can also be done on the 'DHCP Server Summary' screen.

3. Complete the following fields:

- **IP Address Range (Start and End):** Determines the number of hosts that may be connected to the network in this subnet. 'Start' specifies the first IP address that may be assigned in this subnet and 'End' specifies the last IP address in the range.
- **Subnet Mask:** A mask used to determine what subnet an IP address belongs to. An example of a subnet mask value is 255.255.0.0.
- **Lease Time:** Each device will be assigned an IP address by the DHCP server for a limited time ('Lease Time') when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, then the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.
- **WINS Server IP Address:** You can define a relay server / WINS Server, allowing LAN clients to access Windows services over the WAN.
- **Provide host name if not specified by client:** If the DHCP client does not have a host name, the gateway will assign the client a default name.

Click the 'OK' button to save your changes.

7.4.3 DHCP Connections

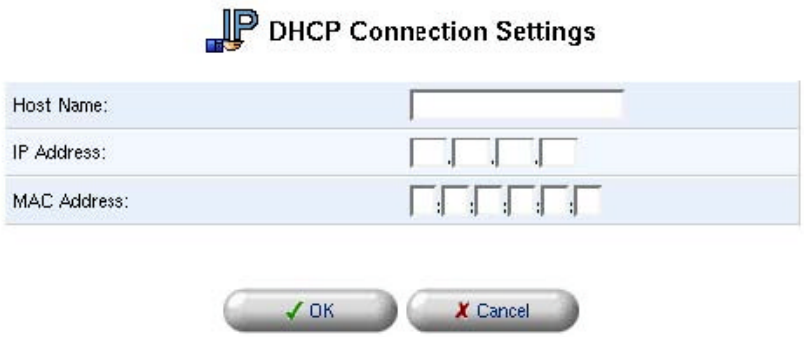
To view a list of computers currently recognized by the DHCP server click the 'Connection List' button that appears at the bottom of the 'DHCP Server Summary' screen. The 'DHCP Connections' screen will be displayed.

To edit the properties for a static connection:

- Click the 'Edit' button that appears in the Action column. The 'DHCP Connection Settings' screen will appear.

To define a new connection with a fixed IP address:

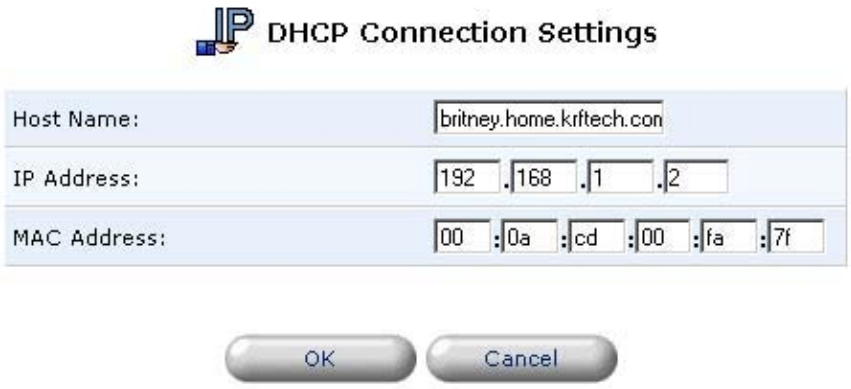
1. Click the 'New Static Connection' button that appears on top of the 'DHCP Connections' screen. The 'DHCP Connection Settings' screen will appear.



2. Enter a host name for this connection.

3. Enter the fixed IP address that you would like to have assigned to the computer.

4. Enter the MAC address of the computer's network card.



5. Click the 'OK' button to save your changes.

Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

To remove a host from the table:

- Click the 'Delete' button that appears in the Action column.

7.5 Network Objects

Network Objects is a method of abstractly defining a set of LAN hosts. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring the CAP´s security filtering settings such as IP address filtering, host name filtering or MAC address filtering.

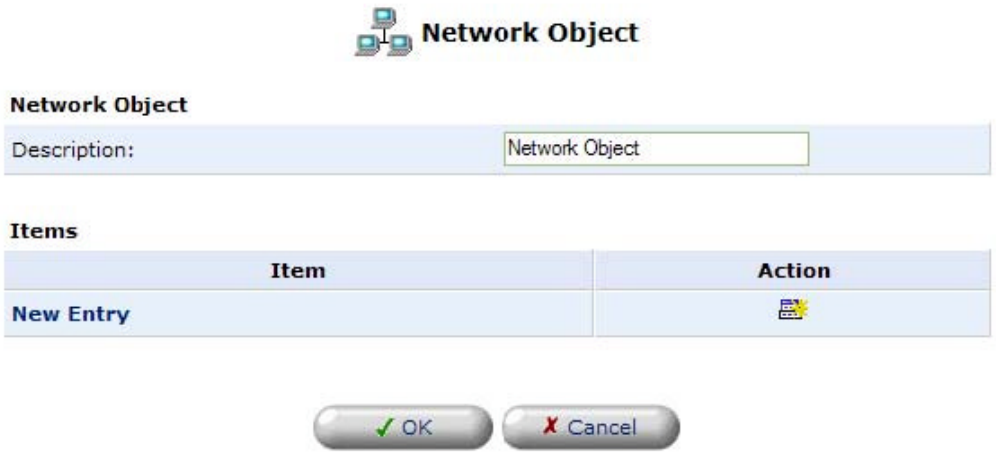
You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. Moreover, it is possible to define network objects according to MAC addresses, making rule application even more low-level.

To define a network object:

1. Click the 'Advanced' icon on the side-bar.
2. Click the 'Network Objects' icon — the 'Network Objects' screen will appear.

3. Click the 'New Entry' link — the 'Network Object' screen will appear.

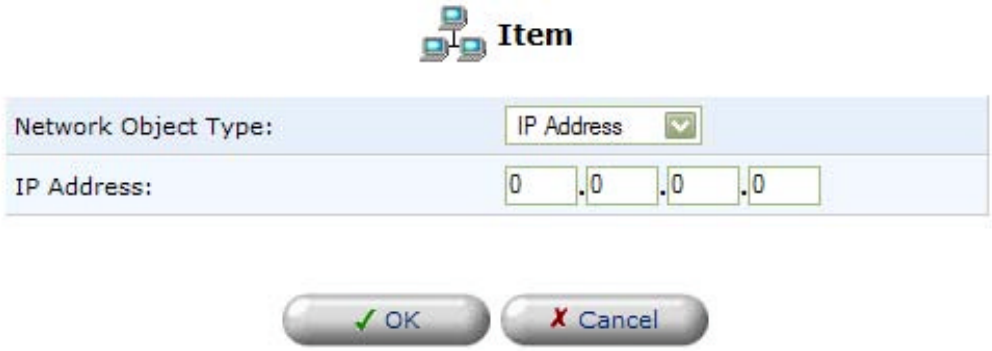
4. Specify a name for the network object in the ’Description’ field.



5. Click the ’New Entry’ link — the ’Item’ screen will appear.

6. Select the type of network object type from the ’Network Object Type’ combo-box:

   - IP Address
   - MAC Address
   - Host Name



7. Specify the appropriate description for the network object type.

8. Press the ’OK’ button.

7.6 Routing

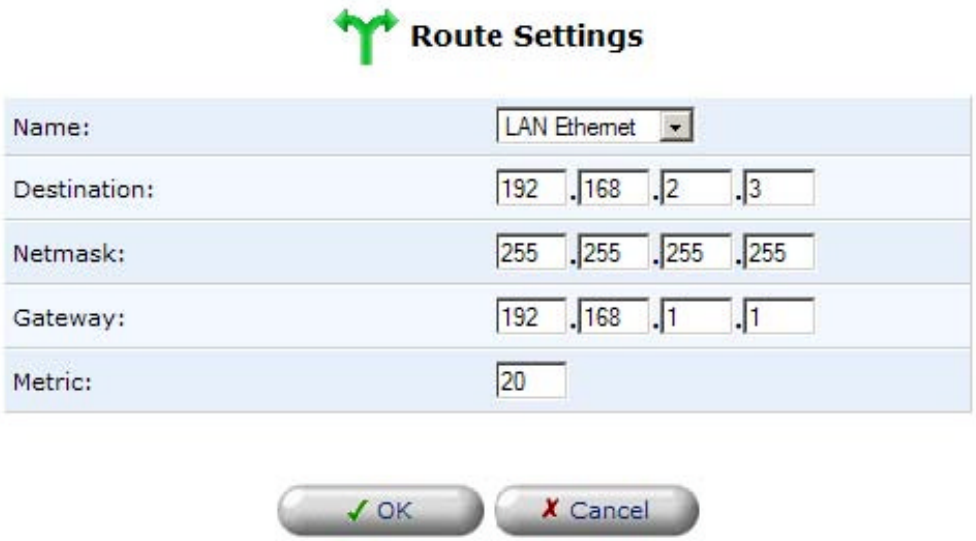
The Routing control available under the ‘Advanced’ section of the management interface allows you to add, edit and delete routing rules from the Routing Table.

7.6.1 Managing Routing Table Rules

You can access the routing table rules by clicking the ’Routing’ icon from the ’Advanced’ screen. The ’Routing’ screen will appear.

When adding a routing rule, you need to specify:

- **Device:** Select the network device.
- **Destination:** The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
- **Netmask:** The network mask is used in conjunction with the destination to determine when a route is used.
- **Gateway:** Enter the gateway’s IP address.
- **Metric:** A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.



7.6.2 Multicasting

The CAP provides support for IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a pre-defined group of recipients. When you join a multicast group you will receive all messages addressed to the group, much like what happens when an e-mail message is sent to a mailing list.

IGMP multicasting enables UPnP capabilities over wireless networks and may also be useful when connected to the Internet through a router. When an application running on a computer in the enterprise network sends out a request to join a multicast group, the CAP intercepts and processes the request.

If The CAP is set to 'Minimum Security' no further action is required.

However, if The CAP is set to 'Typical Security' or 'Maximum Security' you must add the group's IP address to the CAP's 'Multicast Groups' screen. This will allow incoming messages addressed to the group to pass through the Firewall and on to the correct LAN computer.

1. Click the 'Routing' icon in the 'Advanced' screen.
2. Select the 'Multicast Groups Management' check-box.
3. Press the 'OK' button.

7.7 Managing & Defining Users

You can add, edit and delete users on the CAP. These users could be **system administrators** capable of accessing the CAP's management interface, or they could be **PPTP clients** with their login credentials stored on the CAP. When adding a user, you need to specify the following parameters:

- **Full Name:** The remote user's full name.
- **User Name:** The name a remote user will use to access your enterprise network.
- **New Password:** Type a new password for the remote user. If you do not want to change the remote user's password leave this field empty.
- **Retype New Password:** If a new password was assigned, type it again to verify correctness.
- **Permissions:** Select the remote user's privileges on your enterprise network.
  - **Remote Access by PPTP** Grants access with no system modification privileges.
  - **Administrator Privileges** Grants remote system setting modification via web-based management or telnet.

Note: Changing any of the user parameters will prompt the connection associated with the user to terminate. For changes to take effect you should activate the connection manually after modifying user parameters.

7.7.1 Email Notification

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.

7.8 RADIUS

For 802.1x client authentication to work over the LAN, either the CAP must have static entries for every LAN client to be authenticated through its LAN, or it must consult a RADIUS (Remote Authentication Dial-in User Service) server for authenticating users.

The RADIUS server verifies the client's credentials to determine whether the device is authorized to connect to the LAN. If the RADIUS server accepts the client, the server responds by exchanging data with the CAP, including security keys for subsequent encrypted sessions.

To configure the RADIUS authentication mechanism, perform the following:

1. Click the 'RADIUS' icon in the 'Advanced' screen of the Management Console. The RADIUS screen will appear.

Specify the following parameters: **RADIUS Client** Select this check-box to enable RADIUS client authentication.

- **Server IP** Type in the RADIUS server's IP address.
- **Server Port** Type in the RADIUS server's port.
- **Shared Secret** Type in your shared secret.

7.9 Date & Time

To configure date, time and daylight savings time settings perform the following:

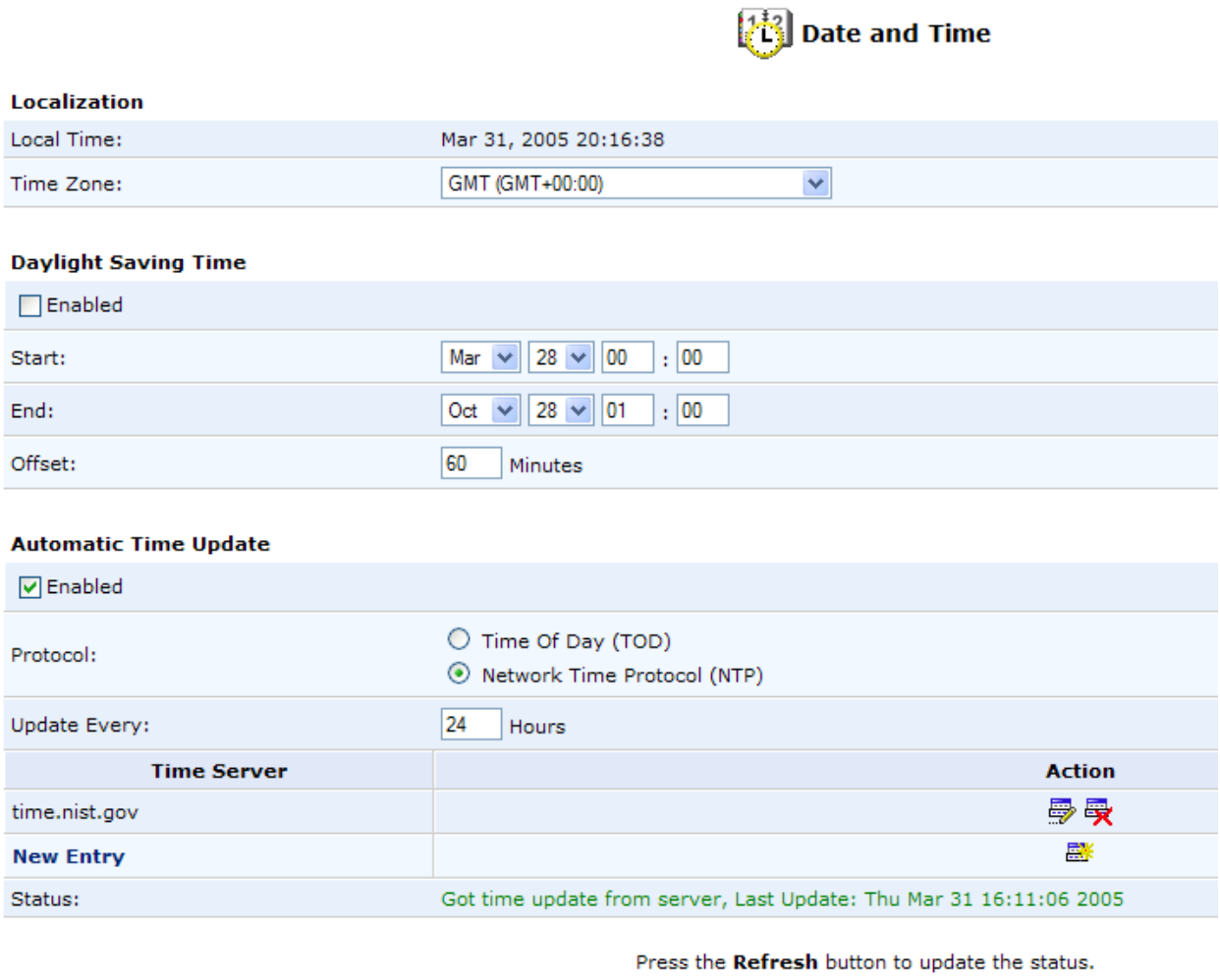
1. Click the 'Date and Time' icon in the 'Advanced' screen of the Management Console. The 'Date & Time' settings screen will be displayed.

2. Select the local time zone from the pull-down menu. The CAP can automatically detect daylight saving setting for selected time zones. If the daylight saving settings for your time zone are not automatically detected, the following fields will be displayed:

- **Enabled** Select this check box to enable daylight saving time.
- **Start** Date and time when daylight saving starts.
- **End** Date and time when daylight saving ends.
- **Offset** Daylight saving time offset.

3. If you want the gateway to perform an automatic time update, perform the following:

- Select the 'Enabled' checkbox under the 'Automatic Time Update' section.
- Select the protocol to be used to perform the time update by selecting wither the 'Time of Day' or 'Network Time Protocol' radio button.
- Specify how often to perform the update in the 'Update Every' field.
- You can define time server addresses by pressing the 'New Entry' link on the bottom of the 'Automatic Time Update' section.



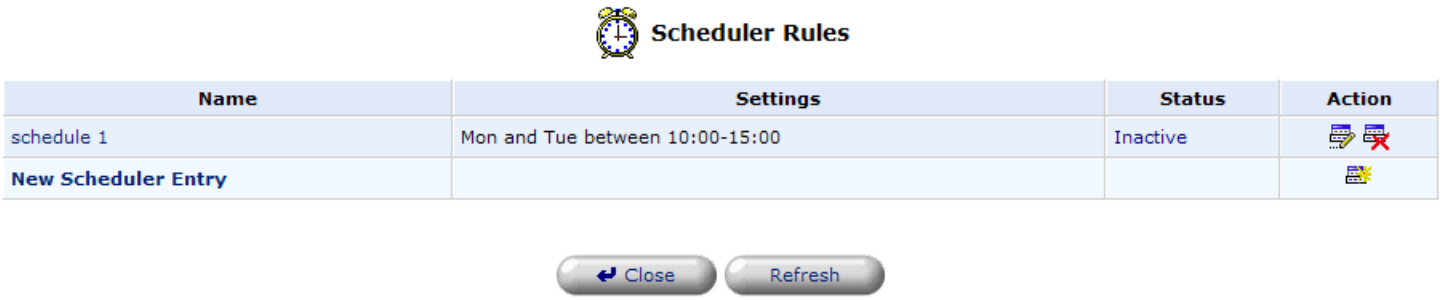
7.10 Scheduler Rules

Scheduler rules are used for limiting the application of Firewall rules to specific time periods, specified in days and hours.

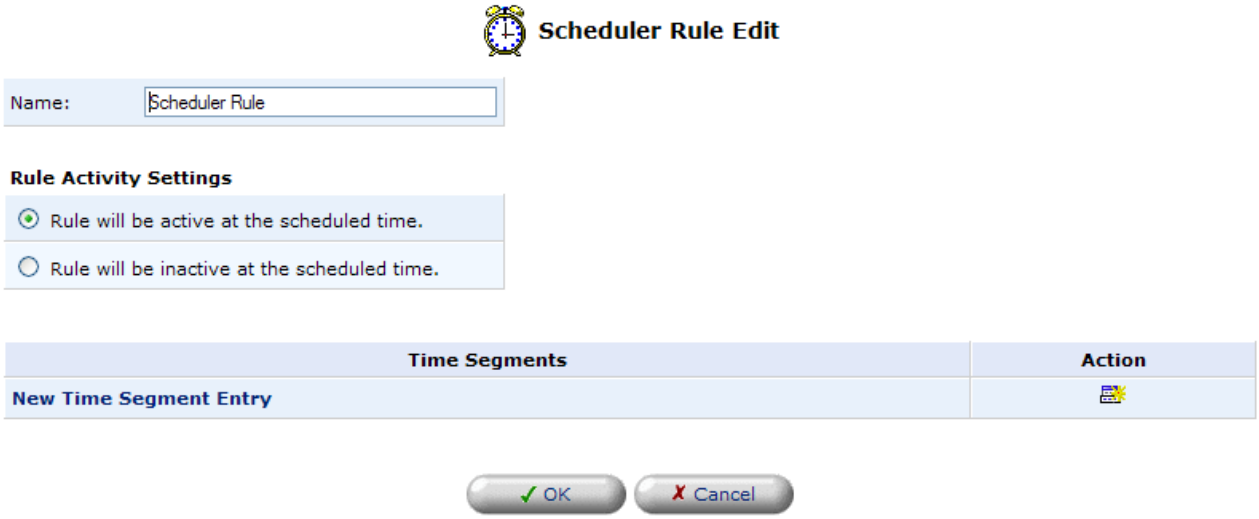
To define a Rule:

1. Click the 'Advanced' icon on the side-bar.

2. Click the 'Scheduler Rules' icon — the 'Scheduler Rules' screen will appear.



3. Click the 'New Scheduler Entry' link — the 'Scheduler Rule Edit' screen will appear.

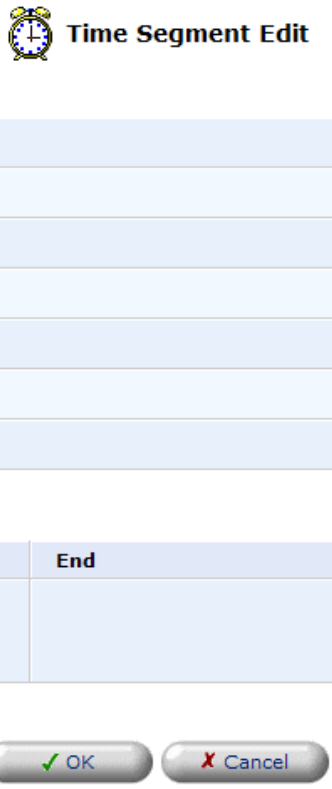


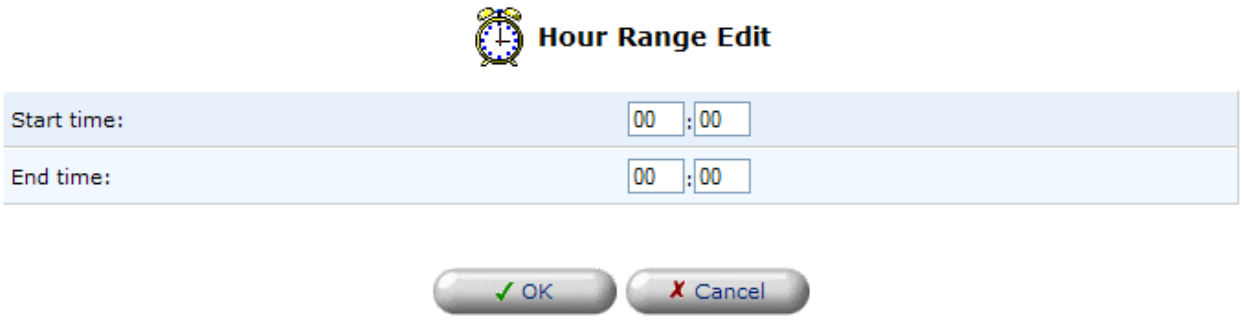
4. Specify a name for the rule in the 'Name' field.

5. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate 'Rule Activity Settings' check-box.

6. Click the 'New Time Segment Entry' link to define the time segment to which the rule will apply

- Select active/inactive days of the week.
- Click the 'New Time Segment Entry' to define an active/inactive hourly range.





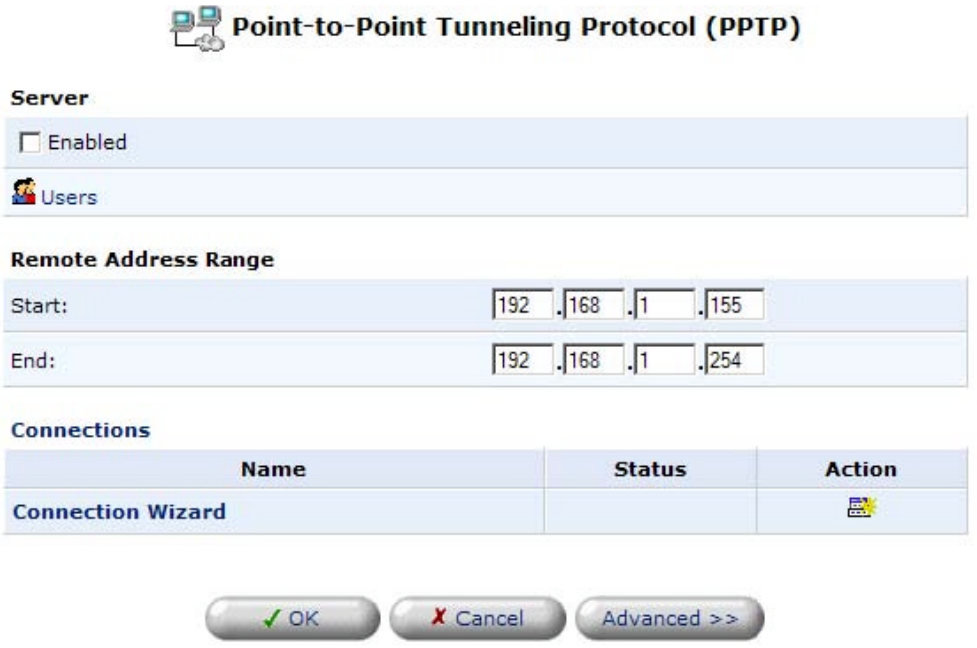
7. Press the 'OK' button.

7.11 Point-to-Point Tunneling Protocol (PPTP)

To access the PPTP settings click the PPTP icon from the 'Advanced' screen. The 'Advanced PPTP Settings' screen will appear.

This screen enables you to configure:

- The remote users that will be granted access to your enterprise network.
- The IP address range an authorized remote user can use when accessing your enterprise network.
- Advanced PPTP client/server connection settings.

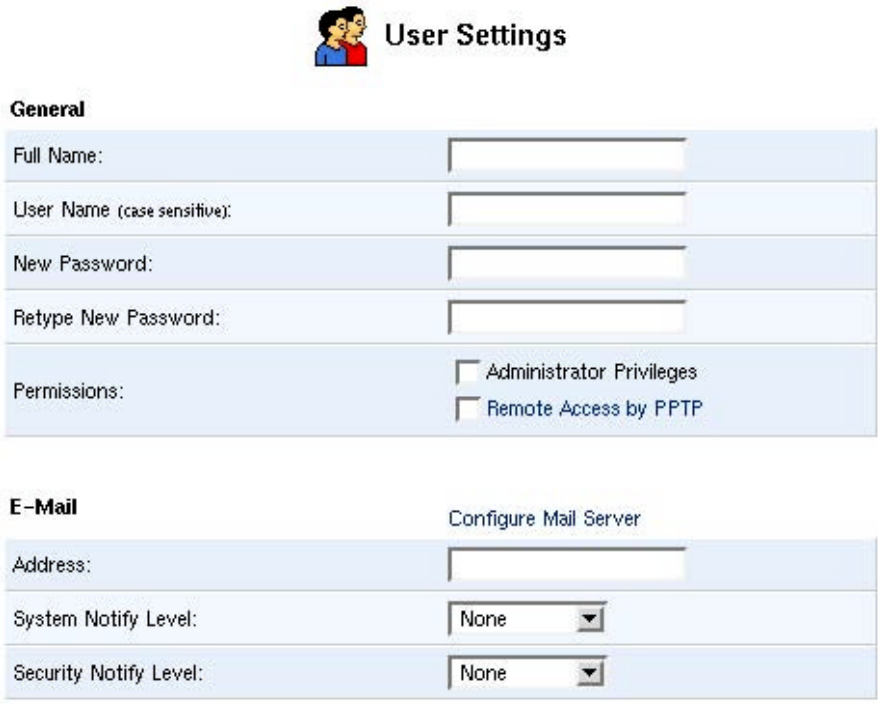


7.11.1 Managing Remote Users

Select the 'Users' link to define and manage remote users. You can add, edit and delete users. When adding a user, you need to specify the following parameters:

- **Full Name:** The remote user's full name.
- **User Name:** The name a remote user will use to access your enterprise net work.

- **New Password:** Type a new password for the remote user. If you do not want to change the remote user's password, leave this field empty.
- **Retype New Password:** If a new password was assigned, type it again to verify correctness.
- **Permissions:** Select the remote user's privileges on your enterprise network.
  - **Remote Access by PPTP:** Grants access with no system modification privileges.
  - **Administrator Privileges:** Grants remote system setting modification via web-based management or telnet.

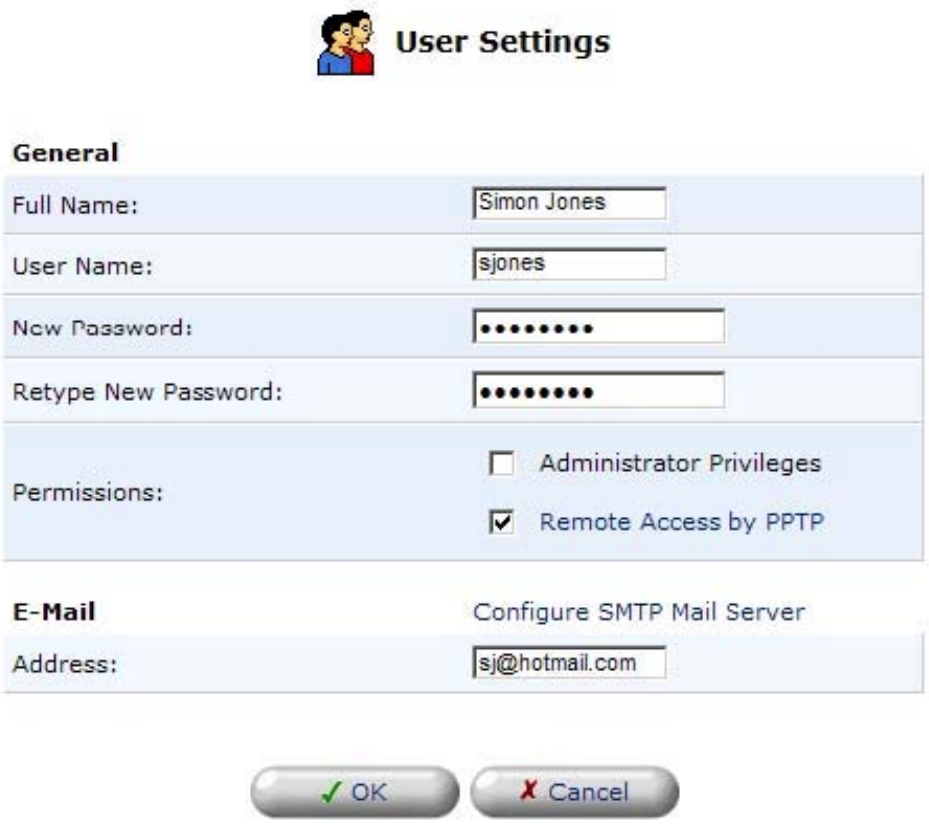


7.11.2 Email Notification

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.

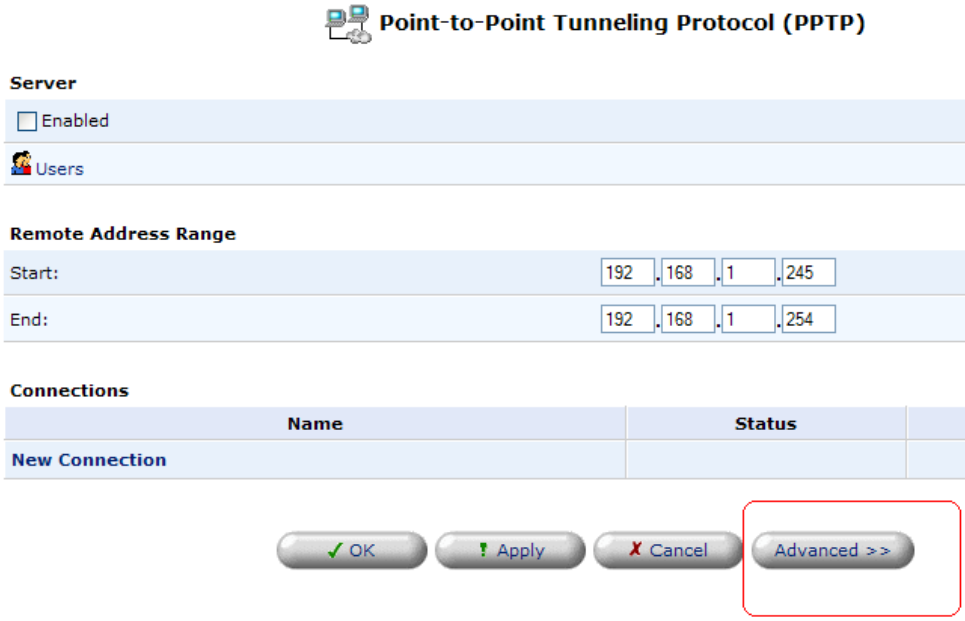
To configure email notification for a specific user:

- 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.



7.11.3 Advanced PPTP Server Settings

To configure advanced PPTP server settings press the 'Advanced' button on the PPTP screen. The 'Advanced PPTP Settings' screen will appear.



This screen enables you to configure the following:

- **Enabled:** Enable or disable the PPTP server.

- **Maximum Idle Time to Disconnect:** Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects a PPTP connection.

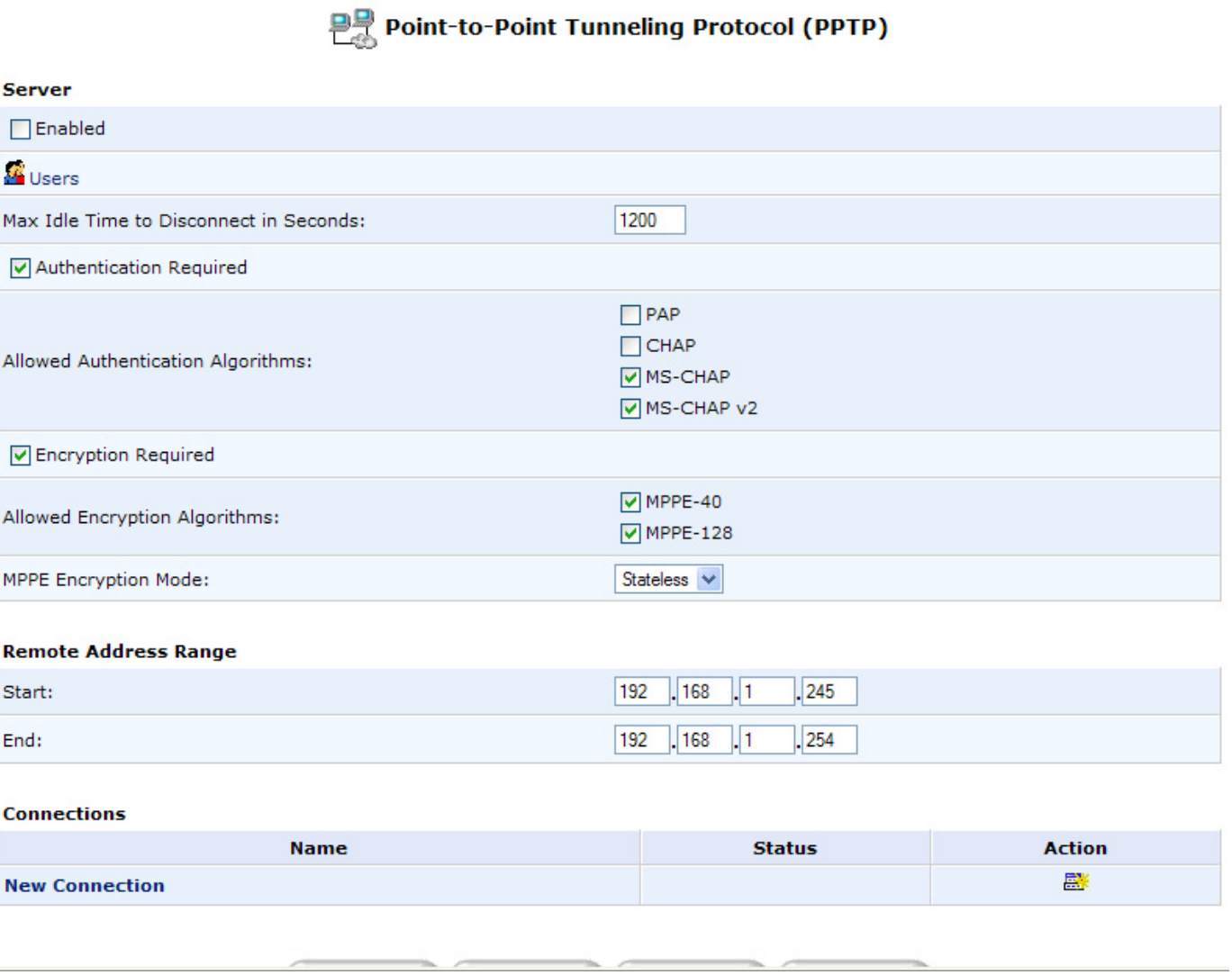
- **Force User Security:** Select whether PPTP will use authentication, encryption, or both.

- **Allowed Authentication Algorithms:** Select the algorithms the server may use when authenticating its clients.

- **Allowed Encryption Algorithms:** Select the algorithms the server may use when encrypting data.

- **Remote Address Range:** Specify the range of IP addresses remote users can use to access your enterprise network.

Note: Please note that the client settings must be in tune with the server settings.

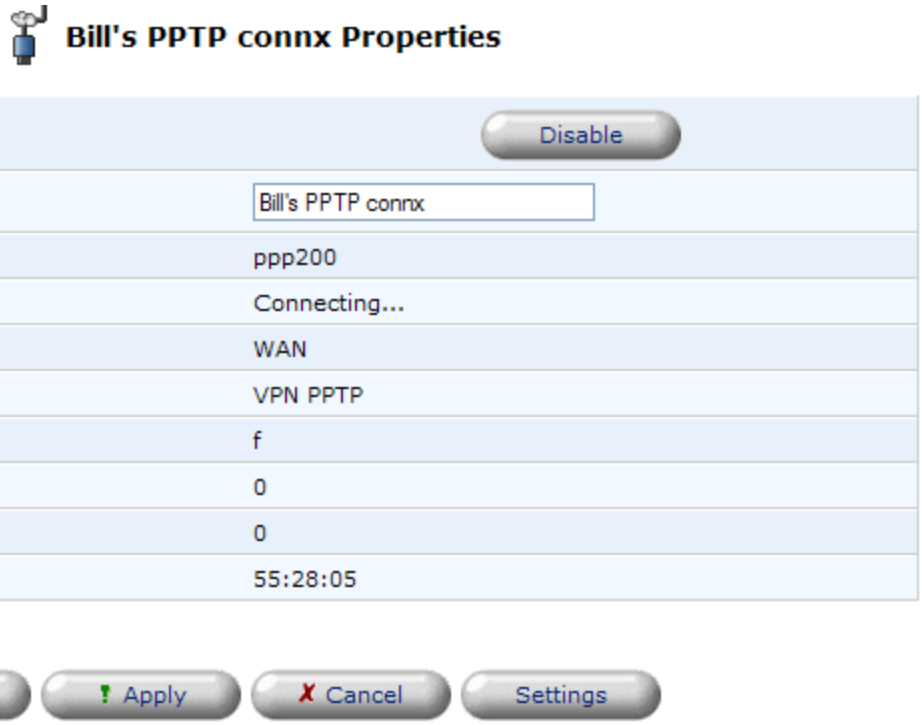


7.11.4 Advanced PPTP Client Settings

The PPTP connections are displayed in the 'Advanced PPTP Settings' screen.

To configure advanced PPTP client and server settings perform the following steps:

1. Press a specific connection's 'Edit' button. The 'Connection Summary' screen will appear.

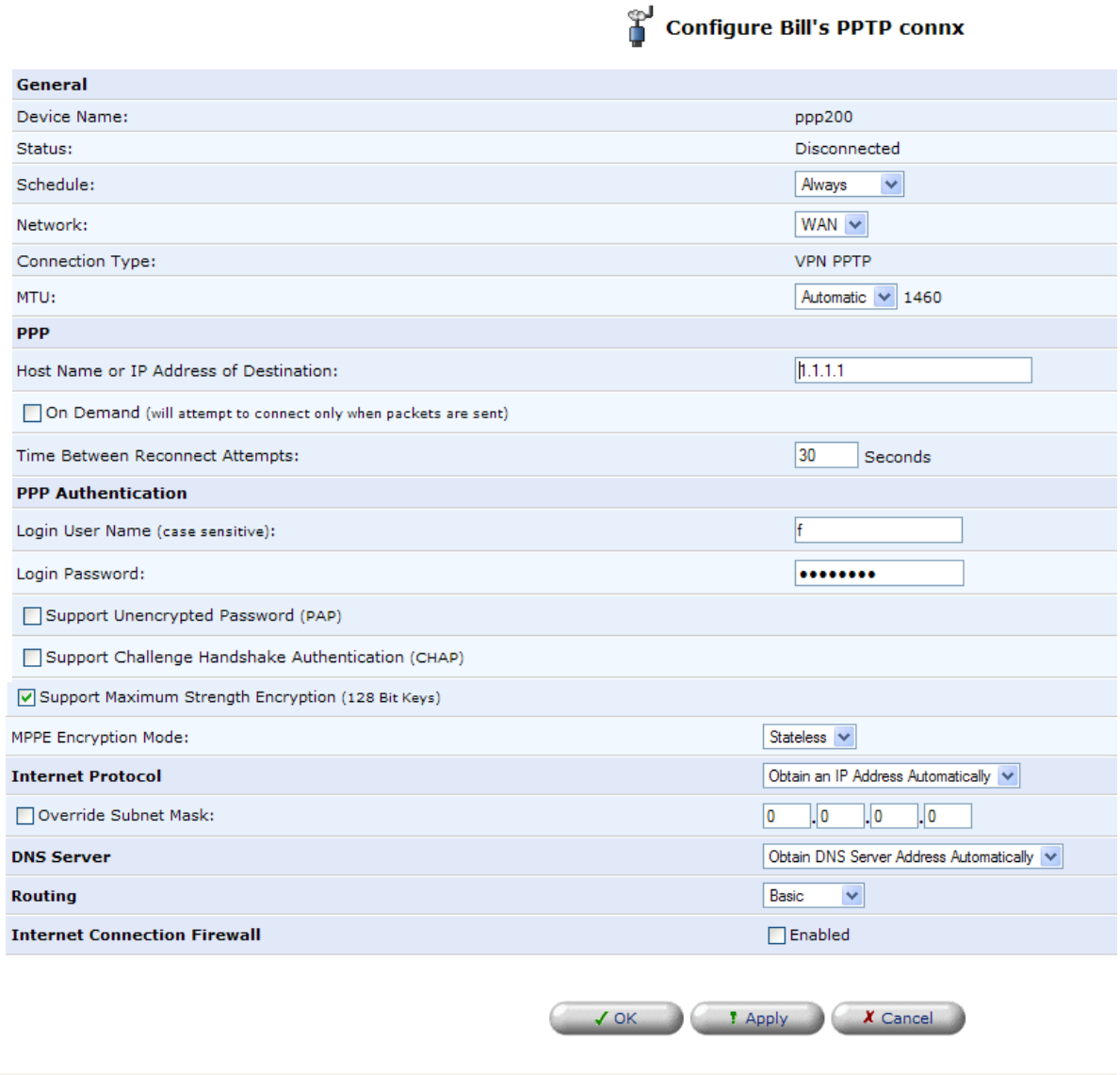


2. Press the 'Settings' button. The 'Advanced PPTP Client Settings' screen will appear, enabling you to configure the following advanced PPTP client settings:

- **PPP Settings**
  - **Host Name:** The host name of your PPTP server.
  - **Login User Name:** Your user name.
  - **Login Password:** Your password.
  - **Idle Time Before Hanging Up:** The period of idle time (during which no data is sent or received) that should elapse before the gateway disconnects the PPTP client connection.
- **PPP Authentication:** Select the authentication algorithms your gate way may use when negotiating with a PPTP server. Select all the check-boxes if no information is available about the server's authentication methods.
- **PPP Encryption:** Select the encryption algorithms your gateway may use when negotiating with a PPTP server. Select all the check boxes if no information is available about the server's encryption methods.
- **Routing:** Define the connection's routing rules.

- **DNS Server:** Select whether the PPTP client 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 PPTP client connection as a network interface monitored by the CAP's Firewall.



7.15 Simple Network Management Protocol (SNMP)

SNMP enables network management systems to remotely configure and monitor the CAP. Your Internet service provider (ISP) may use SNMP in order to identify and resolve technical problems.

7.15.1 Configuring the CAP's SNMP Agent

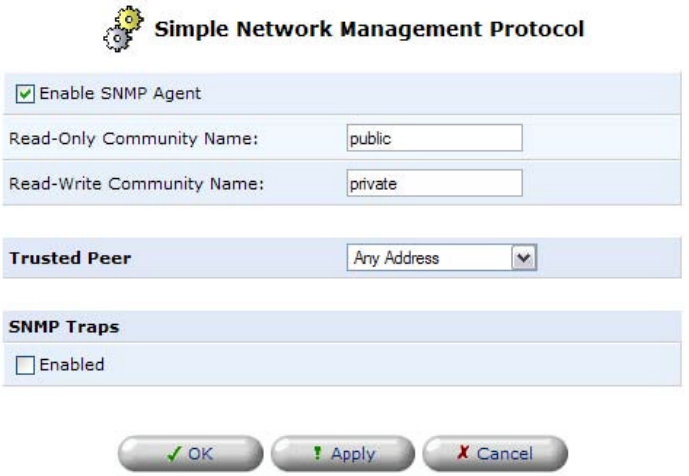
Technical information regarding the properties of the CAP's SNMP manager and agent should be provided by your system administrator or Managed Service Provider.

To configure the CAP's SNMP agent perform the following:

1. Click the 'SNMP' icon in the 'Advanced' screen of the Management Console. The SNMP screen will appear.

2. Specify the following SNMP parameters, as provided by your Internet service provider:

- **SNMP Trusted Peer:** The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on the CAP.
- **Read-only/Write Community Names:** SNMP community strings are passwords used in SNMP messages between the management system and the CAP. A read-only community allows the manager to monitor the CAP. A read-write community allows the manager to both monitor and configure the CAP.
- **SNMP Traps:** Messages sent by the CAP to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. The CAP supports both SNMP version 1 and SNMP version 2c traps.



7.16 MAC Cloning

A MAC address is the numeric code that identifies a device on a network, such as your external cable/DSL modem or a PC network card. Your service provider may ask you to supply the MAC address of your PC, external modem, or both.

When replacing an external modem with the CAP (a future capability), you can simplify the installation process by copying the MAC address of your existing PC to the CAP. In such a case, you do not need to delay the setup process by informing your service provider of newly installed equipment.

Configuring MAC Cloning:

1. Click the 'MAC Cloning' icon in the 'Advanced' screen of the Management Console. The MAC Cloning screen will appear.

2. Enter the physical MAC address to be cloned.

3. Press 'OK'.

Note: If you want the CAP to clone your PC's MAC address, press the 'Clone My MAC Address' button, then press 'OK"

7.17 Diagnostics

The Diagnostics screen can assist you in testing network connectivity. This feature will enable you to ping (ICMP echo) an IP address and view statistics such as the number of packets transmitted and received, round trip time and success status.

7.17.1 Diagnosing Network Connectivity

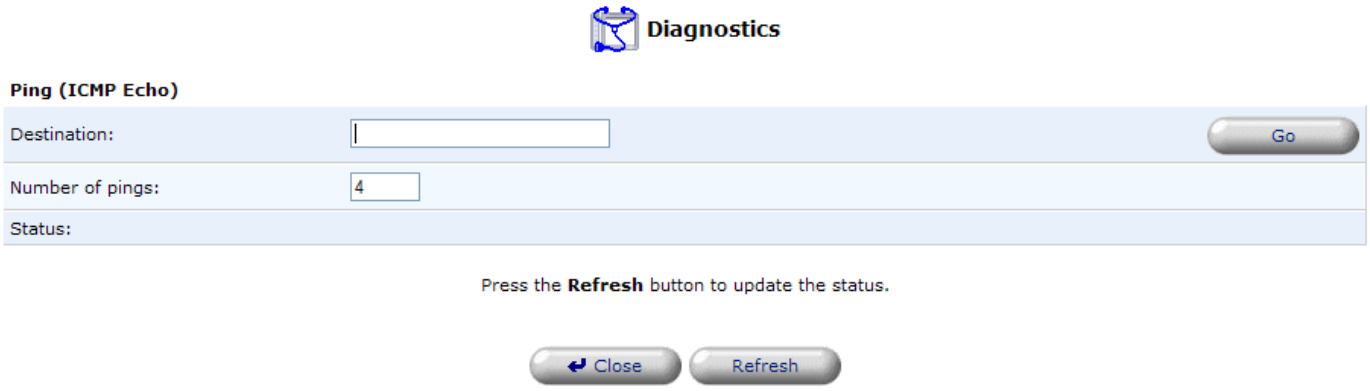
To diagnose network connectivity perform the following steps:

1. Click the 'Diagnostics' icon from the 'Advanced' screen in the management console. The 'Diagnostics' screen will appear.

2. Enter the IP address to be tested in the 'Destination' field.

3. Press the 'Go' button under the 'Ping' section.

4. In a few seconds, diagnostics statistics will be displayed. If no new information is displayed, press the 'Refresh' button.



7.18 Remote Administration

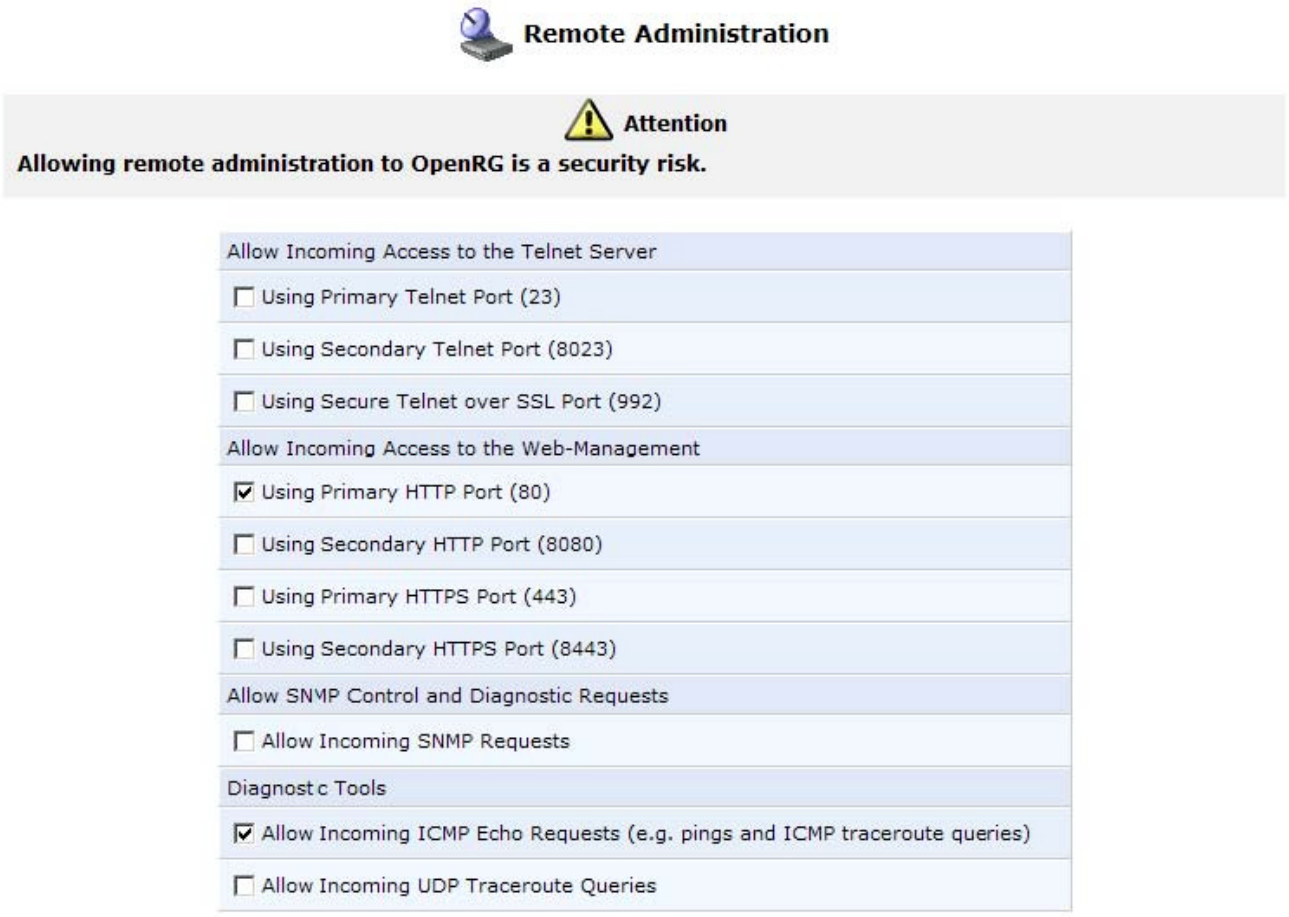
In its default state, the CAP blocks all external (WAN side) users from connecting to or communicating with it. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may wish to enable certain services that grant remote users administrative privileges in your network.

7.18.1 Configuring Remote Administration Services

1. Click the 'Remote Administration' icon in the 'Advanced' screen of the Management Console. The Remote Administration screen will appear.

2. Select the check-boxes next to the service names that you wish to enable.

3. Press the 'OK' button.



7.19 Restoring Default Settings

You may sometimes wish to restore the CAP's factory default settings. This may happen, for example, when you wish to build a new network from the beginning, or when you cannot recall changes made to the network and wish to go back to the default configuration.

To restore default settings:

1. Click the 'Restore Defaults' icon in the 'Advanced' screen of the Management Console. The 'Restore Defaults' screen will be displayed.

2. Click the 'OK' button to restore the CAP's factory default settings.

Note: *All Web-based management settings and parameters,* not only those in the Advanced section, will be restored to their default values. This includes the administrator password; a user-specified password will no longer be valid.

7.20 Restart

To restart the CAP:

1. Click the 'Restart' icon in the 'Advanced' screen of the Management Console. The 'Restart' screen will be displayed.

2. Click the 'OK' button to restart the CAP. This may take up to one minute.

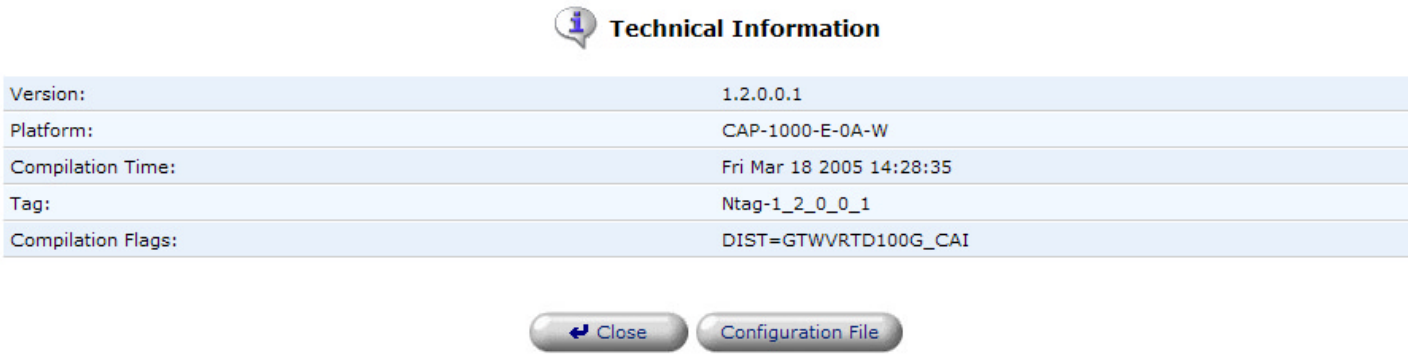
To reenter the Management Console after restarting the gateway click the browser's 'Refresh' button.

7.21 Saving, Restoring & Resetting the CAP Configuration

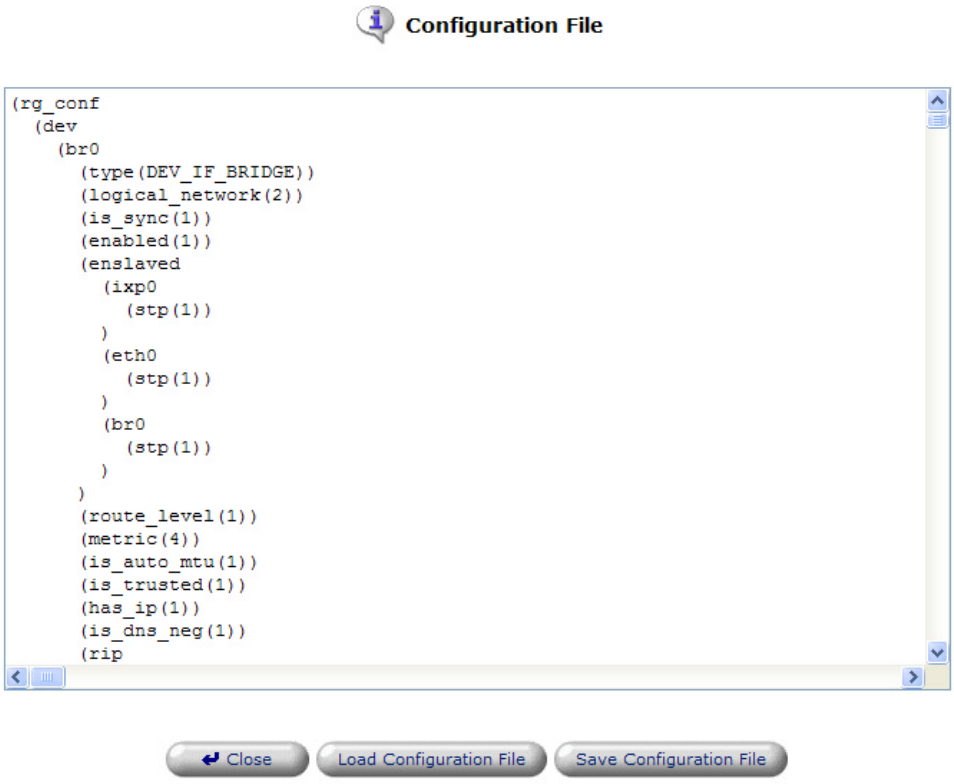
You can review technical system information regarding the CAP, such as the firmware version, when it was created, and the CAP's current configuration file.

To view technical information regarding the CAP:

4. Click the 'Technical Info' icon in the 'Advanced' screen of the Management Console. The 'Technical Information' screen will appear.

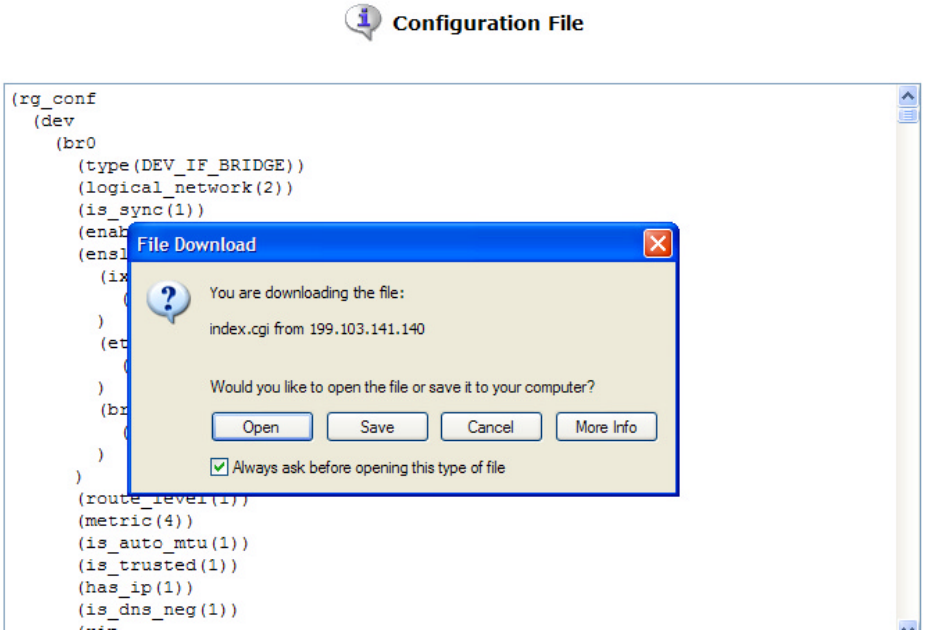


2. Click the 'Configuration File' button to view the complete contents of the CAP's configuration file.

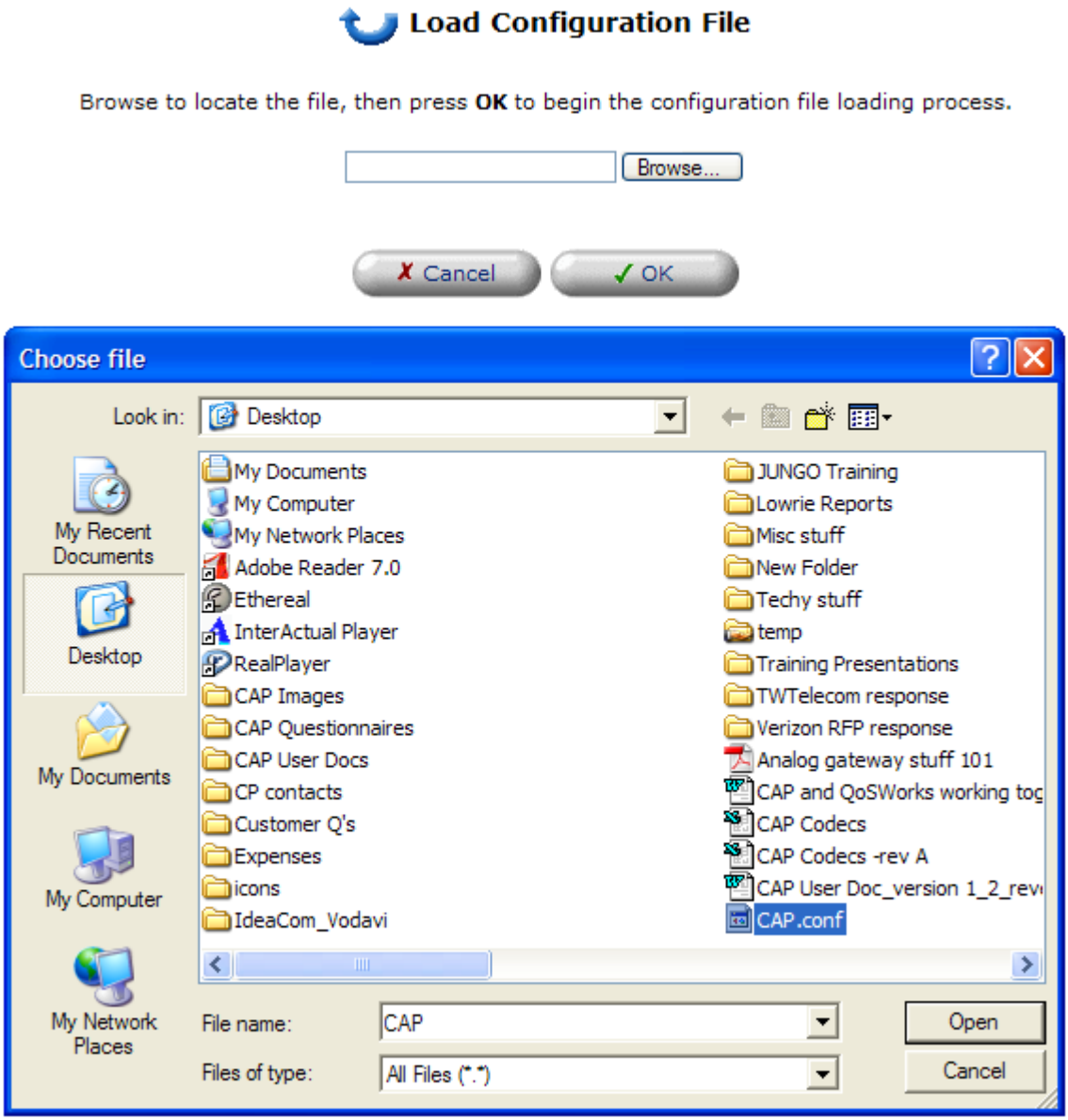


---

5. Click the 'Save Configuration File' to save a copy of the configuration file to your PC.



6. Click the ‘Load Configuration File’ to load a configuration file and restart the CAP. Hit the ‘Browse’ button to select a configuration file from your PC.

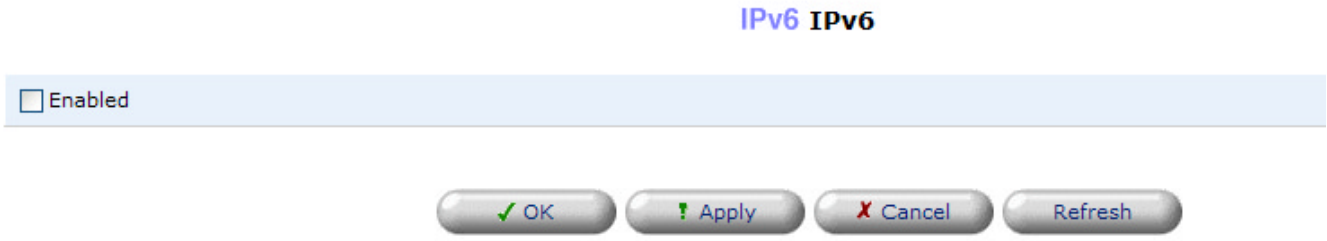


7.22 Tunneling IP V6 Inside of IP V4

You can configure the CAP to tunnel IP version 6 traffic inside of an IP version 4 packet.

To enable IP V6 tunneling:

- Click on ‘Advanced’, then click on IPV6 icon
- Check the ‘Enabled’ box and then click ‘OK’



8

8.0 System Monitoring

The System Monitoring screen displays important system information, including:

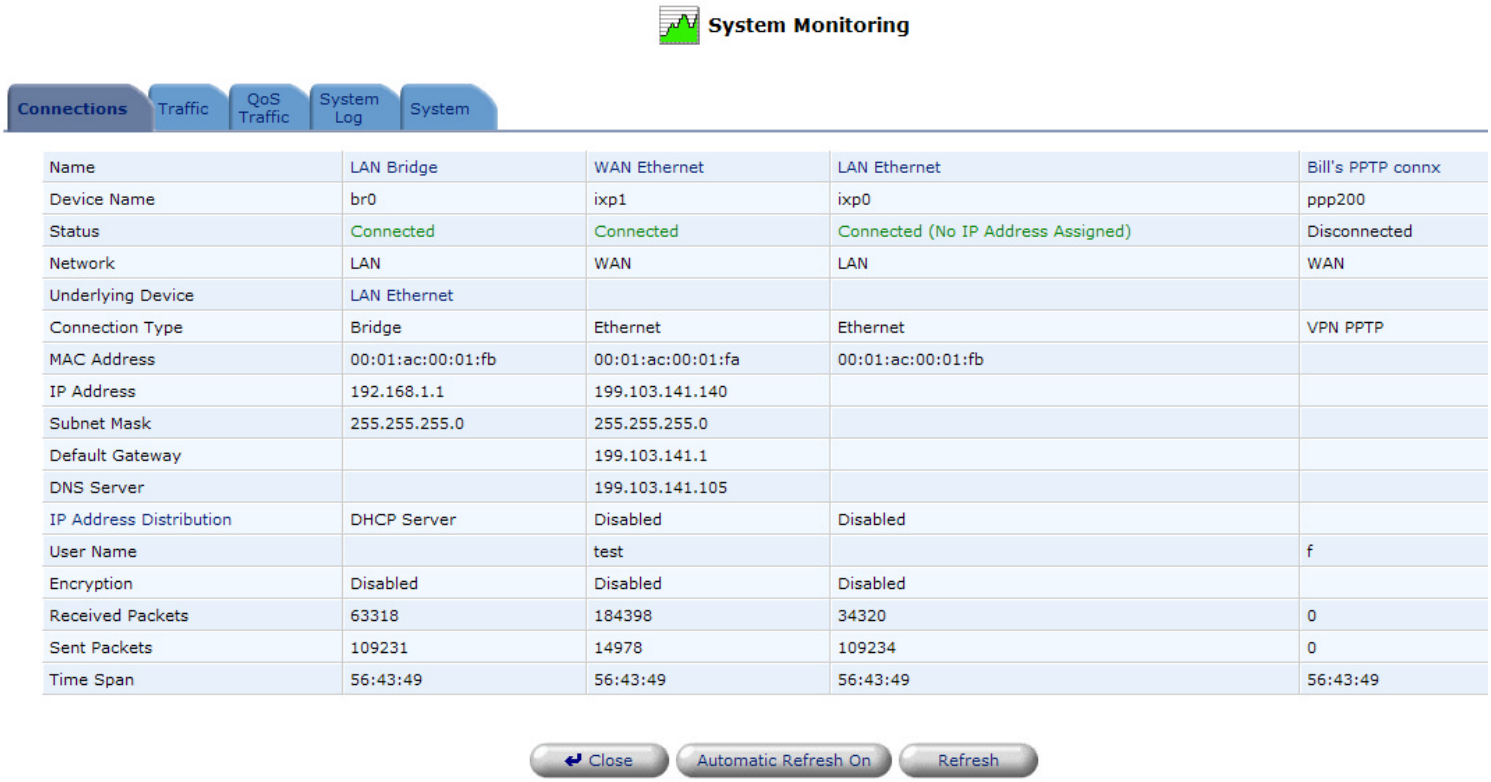
- Key network device parameters
- Network traffic statistics
- QoS statistics
- The system log
- The amount of time that has passed since the CAP was last started

Click on 'System Monitoring' to access the monitoring screens

8.1 Monitoring Connections

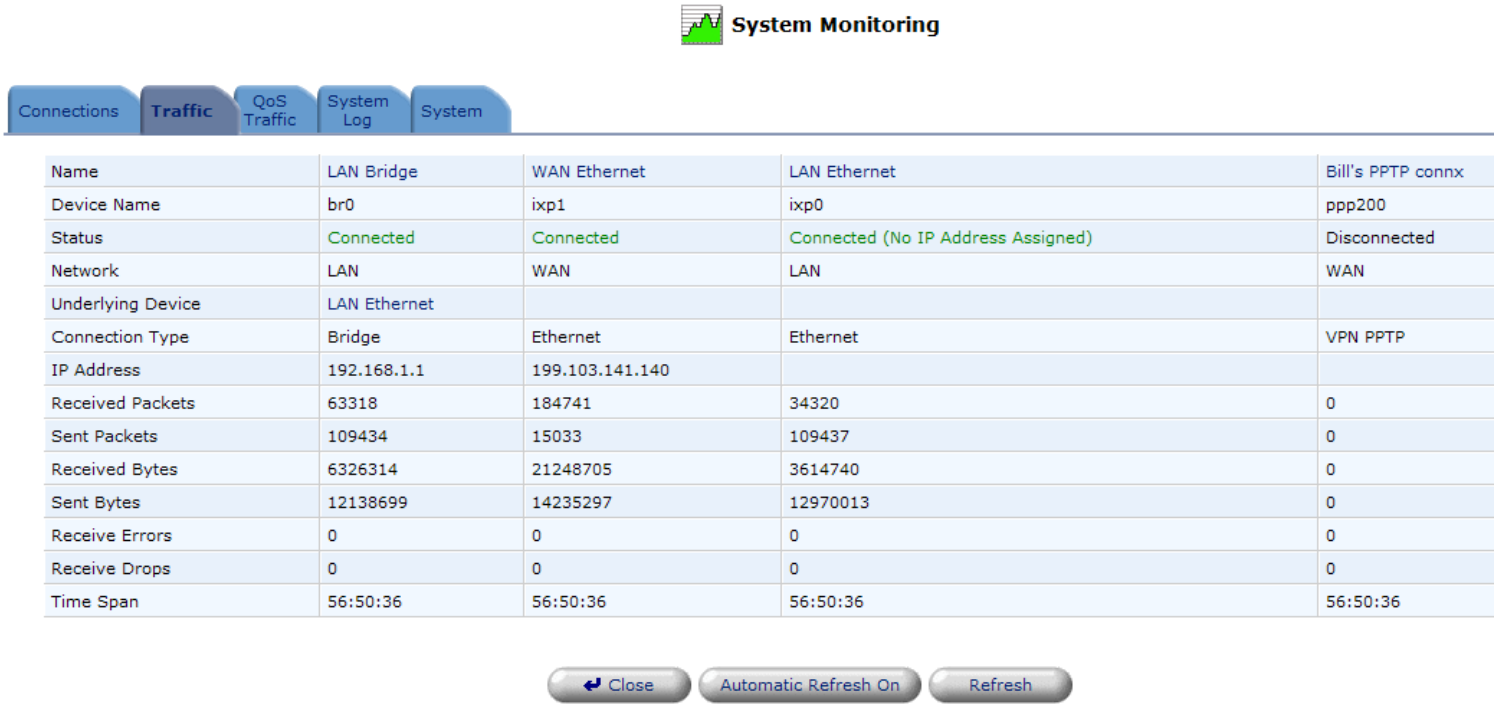
1. Click the 'System Monitoring' icon in the left sidebar to display a table summarizing the monitored connection data.

2. Click the 'Refresh' button to update the display, or press the 'Automatic Refresh' button to constantly update the displayed parameters.



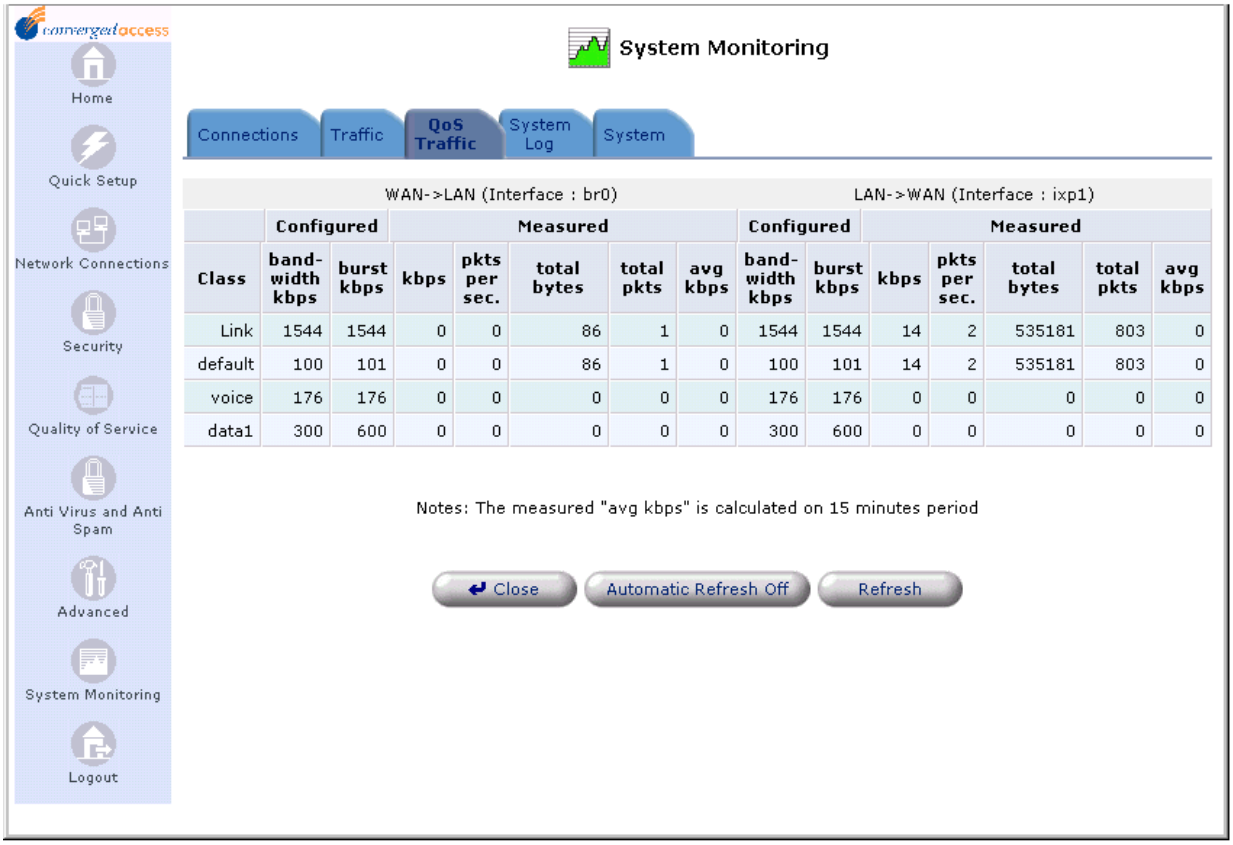
8.2 Traffic Statistics

The CAP is constantly monitoring traffic within the local network and between the local network and the Internet. You can view up-to-the-second statistical information about data received from and transmitted to the Internet (WAN) and about data received from and transmitted to computers in the local network (LAN).



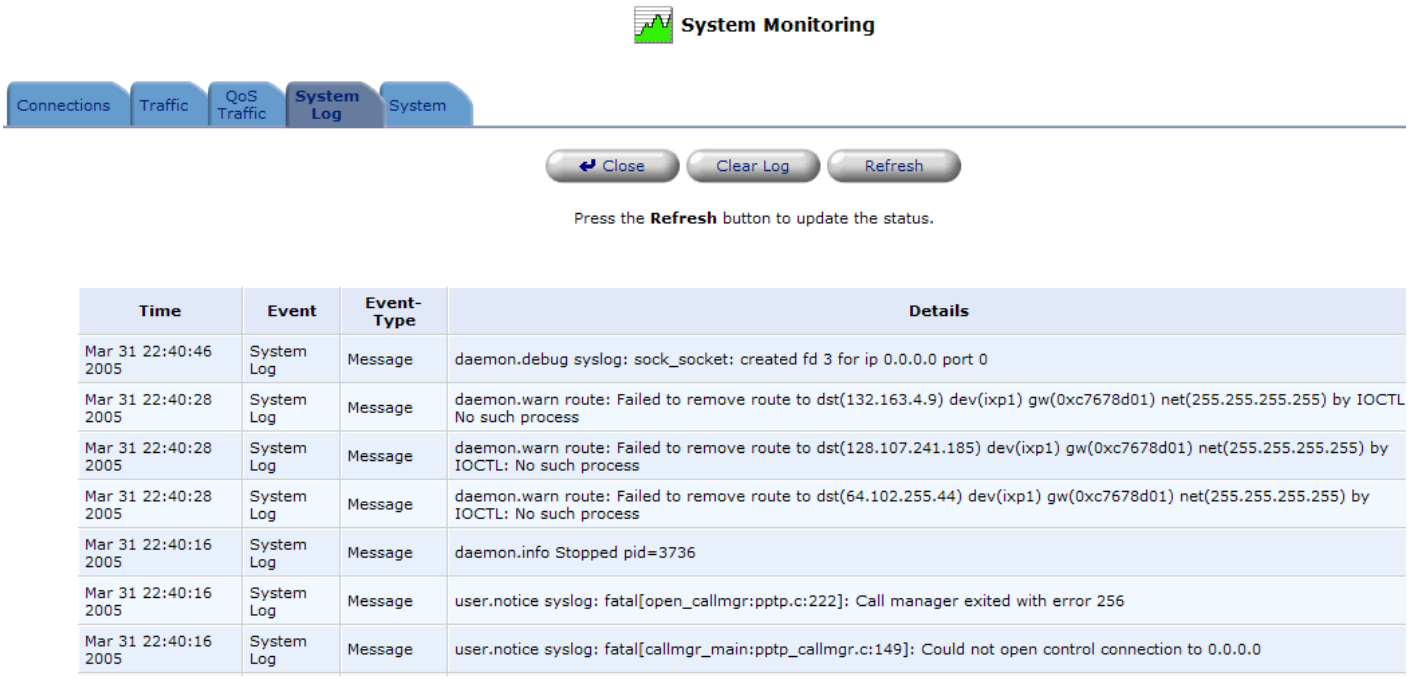
8.3 QoS Traffic

The QoS Traffic report displays statistics specific to Links and configured Classes on the CAP.



8.4 System Log

Press the 'System' button to display the amount of time that has passed since the system was last started.



Time	Event	Event-Type	Details
Mar 31 22:40:46 2005	System Log	Message	daemon.debug syslog: sock_socket: created fd 3 for ip 0.0.0.0 port 0
Mar 31 22:40:28 2005	System Log	Message	daemon.warn route: Failed to remove route to dst(132.163.4.9) dev(ixp1) gw(0xc7678d01) net(255.255.255.255) by IOCTL No such process
Mar 31 22:40:28 2005	System Log	Message	daemon.warn route: Failed to remove route to dst(128.107.241.185) dev(ixp1) gw(0xc7678d01) net(255.255.255.255) by IOCTL: No such process
Mar 31 22:40:28 2005	System Log	Message	daemon.warn route: Failed to remove route to dst(64.102.255.44) dev(ixp1) gw(0xc7678d01) net(255.255.255.255) by IOCTL: No such process
Mar 31 22:40:16 2005	System Log	Message	daemon.info Stopped pid=3736
Mar 31 22:40:16 2005	System Log	Message	user.notice syslog: fatal[open_callmgr:pptp.c:222]: Call manager exited with error 256
Mar 31 22:40:16 2005	System Log	Message	user.notice syslog: fatal[callmgr_main:pptp_callmgr.c:149]: Could not open control connection to 0.0.0.0

8.5 System Up Time

Press the 'System' button to display the amount of time that has passed since the system was last started.

9

9.0 Firmware Upgrade

There are two ways to upgrade the system software:

1. Upgrading from the Internet – automatically retrieve an updated system software file.

2. Upgrading from a local computer – use an update system software file located on a local disc drive.

The following are instructions for each of these methods.

9.1 Upgrading From the Internet

The Remote Update mechanism makes it easy to perform a software upgrade. Each day, the system automatically checks to see if there is a newer software version available.[1]

If an upgrade is available, the 'Upgrade' screen will be displayed upon logging into the Management Console. If no upgrade is available the Network Map will appear, as usual.

To learn if an upgrade is available, click the 'CAP Firmware Upgrade' button from the 'Advanced' screen. You will be informed whether an upgrade is available, and if not, be opted to choose an image file from which to upgrade The CAP.

If an upgrade is available:

- To upgrade click the 'Yes' button.

The CAP must be connected to the Internet in order to communicate with the Remote Update server. Those CAP will check each time the system restarts and at 24-hour intervals thereafter.

To wait and upgrade later, do one of the following:

- Click the 'No' button. The system will continue to perform its daily checks for the availability of a software update as scheduled, and will notify you the next time you log into the Management Console.
- Move to another screen by clicking an icon in the left sidebar. Return to the 'Upgrade' screen at a later time by clicking the 'CAP Firmware Upgrade' icon in the 'Advanced' screen.

9.2 Upgrading From a Local Computer

To upgrade The CAP using a file that you have previously downloaded from the Internet or received on CD:

1. When you receive notification that a new software version of is available, retrieve the file as instructed and store it on a computer in the enterprise network.
2. Open the Management Console from this *same computer* and click the 'CAP Firmware Upgrade' icon that appears in the 'Advanced' screen.
3. Click the 'Browse' button. A dialog box will appear. Choose the file to upload to The CAP and click **Open**.
4. Click the 'OK' button that appears at the bottom of the 'Upgrade' screen. The file will be uploaded to The CAP.
5. After the file has been transferred to the CAP its validity will be verified and you will be asked to confirm that you wish to upgrade the CAP with this new file.
6. Click 'Yes' to confirm. The upgrade process will begin and should take no longer than one minute to complete.
7. At the conclusion of the upgrade process, the CAP will automatically reboot. The new software version of will be running, and your custom configurations and settings will be maintained.


CAP Firmware Upgrade
Current Version: 1.2.0.0.1
Upgrade From the Internet:
Automatic Check Disabled
Check at URL
Check Now
Internet Version: No new version available
Force Upgrade
Upgrade From a Computer in the Network:
Select an updated CAP firmware file from a computer's hard drive or CD on the network
Upgrade Now
Press the Refresh button to update the status.
OK
Apply
Cancel
Refresh
Please wait, system is now being upgraded...
Attention
If the page does not refresh automatically in a minute, please press the Login button.
Login

10

10.0 Analog Voice Gateway Configuration

The CAP's Voice over IP (VoIP) support allows you to connect multiple phones over a single broadband connection, providing the benefits and quality of digital voice. Further, the CAP enables you to place and receive calls over the Internet using a standard telephone set connected to CAP. This section describes how to configure the CAP's Analog Voice Gateway functionality.

Voice Gateway / Analog Telephony Adapter (ATA)

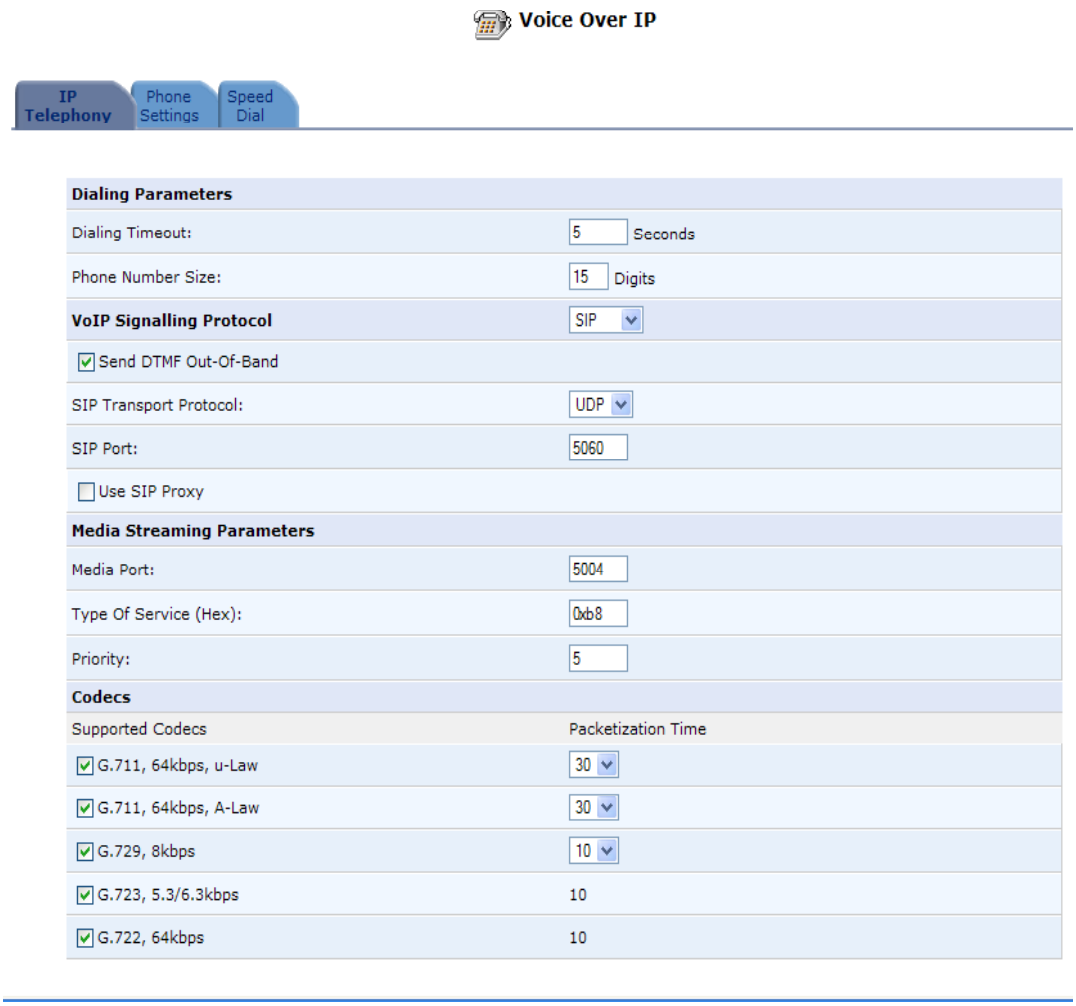
Physical Setup

- Connect a WAN port with the appropriate network cable to your network.
- Connect a POTS telephone to one of the available voice ports.
- Connect CAP to the power supply.

10.1 Configuring VoIP – ATA

Click on “Voice Over IP” on the CAP’s web management GUI, will show you up to 3 configuration tabs, depending on the VoIP protocol that will be implemented to support the analog voice gateway functionality.

10.1.1 The “IP Telephony” Tab



Dialing Parameters

Dialing Timeout - This value defines the maximum allowed time of inactivity between dialed digits, in seconds. If this limit is exceeded, the dialing process will time out and you will hear a warning tone. When you work with a proxy or gatekeeper, the number you have dialed before the dialing process has timed out will be sent to the proxy/gate-keeper as the user ID to be called. This is useful for calling a remote party without creating an entry in the phone book (assuming the remote party is registered with the proxy/gatekeeper).

Phone Number Size - This is the maximum length of shortcut numbers that you can enter and the maximum number of digits that you can dial.

VoIP Gateway Signaling Protocol

You can choose between SIP, H.323 and MGCP. Different subsets of parameters will become visible with each of these choices. NOTE: To make the relevant parameters visible, the screen will be refreshed. However, to apply the change of protocol you must click either 'OK' (this will apply the change and the main CAP screen will be displayed) or 'Apply' (this will apply the changes and the same screen will be displayed).

SIP Parameters:

Media Port - Defines the port to use for voice transport (RTP).

SIP Transport Protocol - The underlying transport protocol to be used for SIP signaling -either TCP or UDP.

SIP Port - The number of port to be used for SIP signaling (TCP)

.

Use SIP Proxy - Register the user with a SIP proxy, thus allowing other parties to call the user through this proxy. When this item is checked, the following fields become visible:

SIP Proxy Address - The IP address of the proxy, in dotted number notation.

SIP Proxy User Name - The login name used for authentication with this proxy.

SIP Proxy Password - The password used for authentication with this proxy.

H.323 Parameters:

Use Fast Start - Use the fast start connect method, which may result in quicker connection establishment, depending on the remote party's settings. NOTE: Microsoft NetMeeting does not support this option, so in order to inter-operate with Microsoft NetMeeting this option must be disabled.

Q.931 Signaling Port - Number of port to use for Q.931 signaling (H.323 call signaling is based upon Q.931)

Register with a Gatekeeper - Register the user with a gatekeeper, thus allowing other parties to call the user through this gatekeeper. When this item is checked, the following fields become visible:

Gatekeeper Address - The IP address of the gatekeeper, in dotted number notation.

Gatekeeper Port - The port on which the gatekeeper is listening for connections.

MGCP Parameters:

Media Gateway Controller Address - The IP address of the MGC (MGCP server), in dotted number notation.

Media Gateway Controller Port - The port on which the MGC is listening for connections.

Media Gateway Port - The port which CAP will use for MGCP connections.

Codecs

The 'IP Telephony' tab contains a list of supported audio codecs, with check boxes next to them. Each codec defines a method of relaying the voice data. Different codecs have different characteristics such as data compression and voice quality. For example, G.723 is a codec which uses compression that is effective where bandwidth is limited, but its voice quality is not as good compared to other codecs such as G.711.

Note that you can have all the codecs checked or just some of them, but at least one of the codecs must be checked, or else you will not be able to make a call. When you start a call to a remote party, your available codecs are compared against the remote party's to determine which codec will be used. If there is no codec that both parties have made available, the call attempt will fail. If more than one codec is common to both parties, you cannot force which of the common codecs that were found will be used by the

remote party's client. If you do wish to force the use of a specific codec, leave only that codec checked.

10.1.2 The "Phone Settings" tab

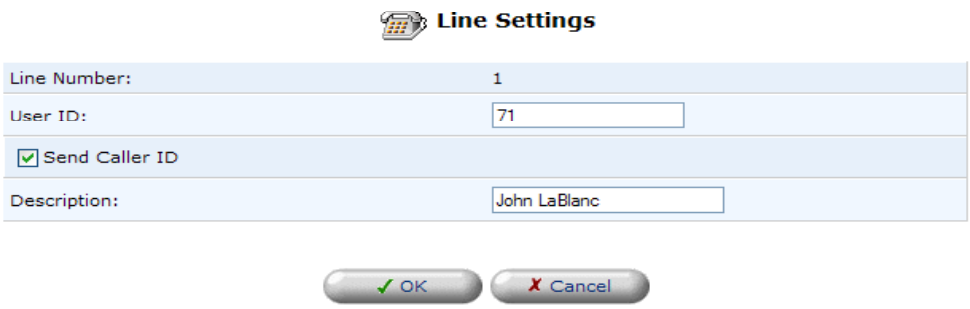
The screen shot above shows the different configuration parameters:

- **Line:** A telephone port in CAP to which you can connect a POTS telephone. You can manage which telephone is operational by marking the check-box next to it.
- **User ID:** This telephone's VoIP user ID, used for identification to initiate and accept calls.
- **Description:** A free text description for you to conveniently identify which telephone is connected to which port.

Before starting to make phone calls, you need to configure each line's parameters. Using "Line 1" as an example:

Click the **"edit"** icon under the **"Action"** column for line 1, the **"Line Settings"** screen will appear.

Specify the **"User ID"** and **"Description"** for this line number and click **"OK".**

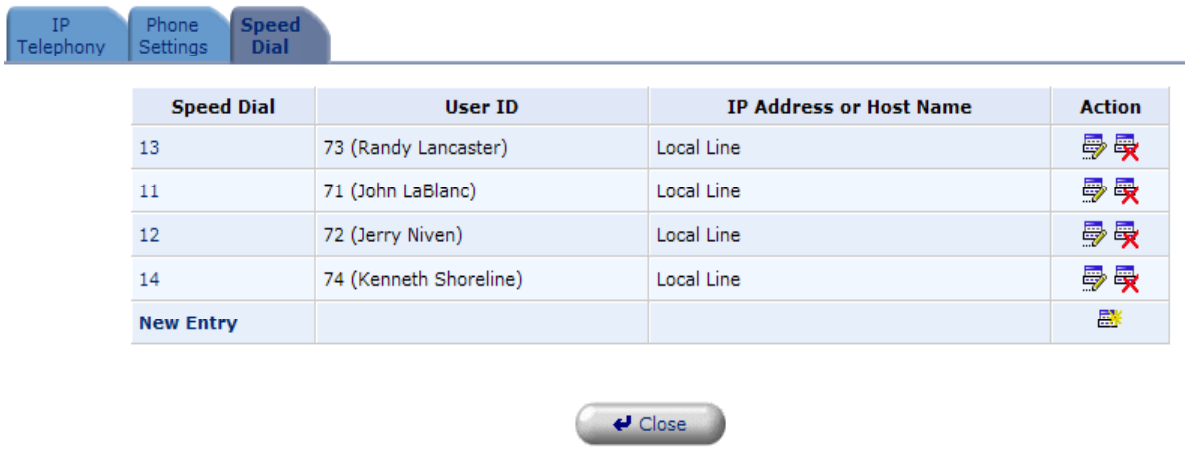


Send Caller ID - This option, which is checked by default, controls whether your user ID is sent when you call a remote party. If it is unchecked, the remote party will not receive your identification.

Configure as many of the line settings as needed. The Description will be useful later on when defining speed dial settings in the address book.

10.1.3 Creating and editing Speed Dial and the Address Book

Click the "Speed Dial" tab. Note: the screen shot below already has speed dial numbers configured. On initial configuration, only the "**New Entry"** choice will be visible.

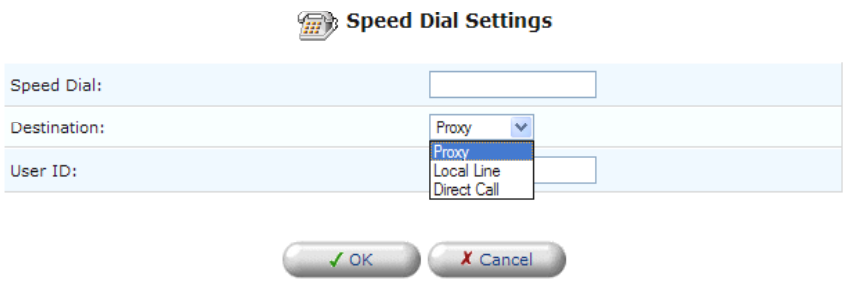


Add a new speed dial phone book entry using the following:

- Select **"New Entry"**

- Assign a Speed Dial number (a shortcut number which you will dial to call this remote party). Example- Speed Dial: 11

- Select what type of call will be made when the speed dial is used.



Proxy – Call destination will be resolved by a defined SIP Proxy

Local Line – Call is local within the defined user IDs in CAP

Direct Call - Call is defined by a remote party's IP address, either as a domain name or in numbers and dots notation. This can be the address of party's gateway or the address of the proxy/gatekeeper at which this party is registered.

The Speed Dial entries will be displayed under the "Speed Dial" tab. This acts as a Speed Dial Address Book and displays the option to create new entries.

To delete an existing Speed Dial entry, click the delete icon on this entry's line in the "Action" column.

To edit an existing phone book entry, click the edit icon on this entry's line in the "Action" column.

10.1.4 Telephony Features

Placing a Call:

1. Pick up the handset on the POTS telephone.
2. Call the remote party by dialing the number you configured in the phone book.

Call Hold:

To place the remote party on hold, do the following:

1. Press “Flash”.
2. Press “1”.
3. The phone will sound a dial-tone. At this point you can initiate a second call by dialing another party’s number. To cancel the hold state and resume the previous phone call, press “Flash”.

Call Transfer With Consultation:

To transfer an existing call (B) to a third party (C):

1. Press “Flash”.
2. Press “2”.
Party B will now be placed on hold, and you will hear a dial tone.

3. Dial party C’s shortcut number (You can engage in conversation).
4. Press “Flash” to complete the transfer -you will hear a warning tone, B and C are now talking to each other.

3-Way Conference:

To extend an existing call (B) into a 3-way conference by bringing in an additional party (C):

1. Press “Flash”.
2. Press “33”.
Party B will now be placed on hold and you will hear a dial tone.

3. Dial party C’s shortcut number (You can engage in conversation).
4. Press “Flash” to join both C and B to a single conference.

11

11.0 Glossary

100Base-T	Also known as Fast Ethernet, an Ethernet cable standard with a data transfer rate of up to 100 Mbps.
10Base-T	An older Ethernet cable standard with a data transfer rate of up to 10 Mbps.
802.11, 802.11b	A family of IEEE (Institute of Electrical and Electronics Engineers)-defined specifications for wireless networks. Includes the 802.11b standard, which supports high-speed (up to 11 Mbps) wireless data transmission.
802.3	The IEEE (Institute of Electrical and Electronics Engineers -defined specification that describes the characteristics of Ethernet (wired) connections.
Access point	A device that exchanges data between computers on a network. An access point typically does not have any Firewall or NAT capabilities.
Ad hoc network	A solely wireless computer-to-computer network. Unlike an infrastructure network, an ad hoc network does not include a gateway router.
Adapter	Also known as a network interface card (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.
Administrator	A person responsible for planning, configuring, and managing the day-to-day operation of a computer network. The duties of an administrator include installing new workstations and other devices, adding and removing individuals from the list of authorized users, archiving files, overseeing password protection and other security measures, monitoring usage of shared resources, and handling malfunctioning equipment.
Authentication	The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Bandwidth	The amount of information, or size of file, that can be sent through a

	network connection at one time. A connection with more bandwidth can transfer information more quickly.
Bridge	A device that forwards packets of information from one segment of a network to another. A bridge forwards only those packets necessary for communication between the segments.
Broadband connection	A high-speed connection, typically 256 Kbps or faster. Broadband services include cable modems and DSL.
Broadband modem	A device that enables a broadband connection to access the Internet. The two most common types of broadband modems are cable modems, which rely on cable television infrastructure, and DSL modems, which rely on telephone lines operating at DSL speeds.
Broadcast	Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.
Bus	A set of hardware lines used for data transfer among the components of a computer system. A bus essentially allows different parts of the system to share data. For example, a bus connects the disk-drive controller, memory, and input/output ports to the microprocessor.
Cable modem	A device that enables a broadband connection to access the Internet. Cable modems rely on cable television infrastructure, in other words, the data travels on the same lines as you cable television.
CAT 5 cable	Abbreviation for Category 5 cable. A type of Ethernet cable that has a maximum data rate of 100 Mbps.
Channel	A path or link through which information passes between two devices.
CHAP	Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. The sender and peer must share a pre-defined secret.
Client	Any computer or program that connects to, or requests the services of, another computer or program on a network. For a local area network or the Internet, a client is a computer that uses shared network resources provided by a server.
Client/server network	A network of two or more computers that rely on a central server to mediate the connections or provide additional system resources. This dependence on a server differentiating a client/server network from a peer-to-peer network.
Computer name	A name that uniquely identifies a computer on the network so that all its shared resources can be accessed by other computers on the network. One computer name cannot be the same as any other computer or domain name on the network.
Crossover cable	A type of cable that facilitates network communications. A crossover cable is a cable that is used to interconnect two computers by crossing over (reversing) their respective pin contacts.
DHCP	Acronym for ‘Dynamic Host Configuration Protocol’. A TCP/IP protocol

	that automatically assigns temporary IP addresses to computers on a local area network (LAN). The CAP supports the use of DHCP. You can use DHCP to share one Internet connection with multiple computers on a network.
Dial-up connection	An Internet connection of limited duration that uses a public telephone network rather than a dedicated circuit or some other type of private network.
DMZ	Acronym for 'demilitarized zone'. A collection of devices and subnets placed between a private network and the Internet to help protect the private network from unauthorized Internet users.
DNS	Acronym for 'Domain Name System'. A data query service chiefly used on the Internet for translating host names into Internet addresses. The DNS database maps DNS domain names to IP addresses, so that users can locate computers and services through user-friendly names.
Domain	In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.
Domain name	An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, www.whitehouse.gov identifies the Web server at the White House, which is part of the U.S. government.
Driver	Within a networking context, a device that mediates communication between a computer and a network adapter installed on that computer.
DSL	Acronym for 'Digital Subscriber Line'. A constant, high-speed digital connection to the Internet that uses standard copper telephone wires.
DSL modem	A device that enables a broadband connection to access the Internet. DSL modems rely on telephone lines that operate at DSL speeds.
Duplex	A mode of connection. Full-duplex transmission allows for the simultaneous transfer of information between the sender and the receiver. Half-duplex transmission allows for the transfer of information in only one direction at a time.
Dynamic IP address	The IP address assigned (using the DHCP protocol) to a device that requires it. A dynamic IP address can also be assigned to a gateway or router by an ISP.
Edge computer	The computer on a network that connects the network to the Internet. Other devices on the network connect to this computer. The computer running the most current, reliable operating system is the best choice to designate as the edge computer.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Ethernet	A networking standard that uses cables to provide network access. Ethernet is the most widely-installed technology to connect computers together.
Ethernet cable	A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. there is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second.
Firewall	A security system that helps protect a network from external threats, such as hacker attacks, originating outside the network. A hardware Firewall is a connection routing device that has specific data checking settings and that helps protect all of the devices connected to it.
Firmware	Software information stored in nonvolatile memory on a device.
Flash memory	A type of memory that does not lose data when power is removed from it. Flash memory is commonly used as a supplement to or replacement for hard disks in portable computers. In this context, flash memory either is built in to the unit or, more commonly, is available as a PC Card that can be plugged in to a PCMCIA slot.
FTP	Acronym for 'File Transfer Protocol'. The standard Internet protocol for downloading, or transferring, files from one computer to another.
Gateway	A device that acts as a central point for networked devices, receives transmitted messages, and forwards them. The CAP can link many computers on a single network, and can share an encrypted Internet connection with wired and wireless devices.
Gateway address	The IP address you use when you make a connection outside your immediate network.
Hexadecimal	A numbering system that uses 16 rather than 10 as the base for representing numbers. It is therefore referred to as a base-16 numbering system. The hexadecimal system uses the digits 0 through 9 and the letters A through F (uppercase or lowercase) to represent the decimal numbers 0 through 15. For example, the hexadecimal letter D represents the decimal number 13. One hexadecimal digit is equivalent to 4 bits, and 1 byte can be expressed by two hexadecimal digits.
Host name	The DNS name of a device on a network, used to simplify the process of locating computers on a network.
Hub	A device that has multiple ports and that serves as a central connection point for communication lines from all devices on a network. When data arrives at one port, it is copied to the other ports.
IEEE	Acronym for 'Institute of Electrical and Electronics Engineers'. A society of engineering and electronics professionals that develops standards for the electrical, electronics, computer engineering, and science-related industries. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters I-E-E-E.

Infrastructure network	A network configuration in which wireless devices connect to a wireless access point (such as The CAP) instead of connecting to each other directly.
Internet domain	In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.
Intranet	A network within an organization that uses Internet technologies (such a Web browser for viewing information) and protocols (such as TCP/IP), but is available only to certain people, such as employees of a company. Also called a private network. Some intranets offer access to the Internet, but such connections are directed through a Firewall.
IP	Acronym for 'Internet Protocol'. The protocol within TCP/IP that is used to send data between computers over the Internet. More specifically, this protocol governs the routing of data messages, which are transmitted in smaller components called packets.
IP address	Acronym for 'Internet Protocol' address. IP is the protocol within TCP/IP that is used to send data between computers over the Internet. An IP address is an assigned number used to identify a computer that is connected to a network through TCP/IP. An IP address consists of four numbers (each of which can be no greater than 255) separated by periods, such as 192.168.1.1.
ISO/OSI reference model	Abbreviation for International Organization for Standardization Open Systems Interconnection reference model. An architecture that standardizes levels of service and types of interaction for computers that exchange information through a communications network. The ISO/OSI reference model separates computer-to-computer communications into seven protocol layers, or levels; each builds on and relies on the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the program level. It is a fundamental blueprint designed to help guide the creation of hardware and software for networks.
ISP	Acronym for 'Internet service provider'. A company that provides individuals or companies access to the Internet.
Kbps	Abbreviation of 'kilobits per second'. Data transfer speed, as through a modem or on a network, measured in multiples of 1,000 bits per second.
LAN	Acronym for 'local area network'. A group of computers and other devices dispersed over a relatively limited area (for example, a building) and connected by a communications link that enables any device to interact with any other on the network.
MAC address	Abbreviation for 'media access control' address. The address that is used for communication between network adapters on the same subnet. Each network adapter is manufactured with its own unique MAC address.
MAC layer	Abbreviation for 'media access control' layer. The lower of two sub layers

	that make up the data-link layer in the ISO/OSI reference model. The MAC layer manages access to the physical network, so a protocol like Ethernet works at this layer.
Mapping	A process that allows one computer to communicate with a resource located on another computer on the network. For example, if you want to access a folder that resides on another computer, you map to that folder, as long as the computer that holds the folder has been configured to share it.
Mbps	Abbreviation of 'megabits per second'. A unit of bandwidth measurement that defines the speed at which information can be transferred through a network or Ethernet cable. One megabyte is roughly equivalent to eight megabits.
Modem	A device that transmits and receives information between computers.
MPPE	Microsoft Point to Point Encryption (MPPE) is a means of representing Point to Point Protocol (PPP) packets in an encrypted form.
Multicast	To transmit a single message to a select group of recipients. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks.
NAT	Acronym for 'network address translation'. The process of converting between IP addresses used within a private network and Internet IP addresses. NAT enables all of the computers on a network to share one IP address.
Network	A collection of two or more computers that are connected to each other through wired or wireless means. These computers can share access to the Internet and the use of files, printers, and other equipment.
Network adapter	Also known as a 'network interface card' (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.
Network name	The single name of a grouping of computers that are linked together to form a network.
Network printer	A printer that is not connected directly to a computer, but is instead connected directly to a network through a wired or wireless connection.
Packet	A unit of information transmitted as a whole from one device to another on a network.
PAP	Password Authentication Protocol, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP.
PC Card	A peripheral device that adds memory, mass storage, modem capability, or other networking services to portable computers.
PCI	Acronym for 'Peripheral Component Interconnect'. A specific bus type

	designed to be used with devices that have high bandwidth requirements.
PCI card	A card designed to fit into a PCI expansion slot in a personal computer. PCI cards provide additional functionality; for example, two types of PCI cards are video adapters and network interface cards. See PCI.
PCI expansion slot	A connection socket designed to accommodate PCI cards.
PCMCIA	Acronym for 'Personal Computer Memory Card International Association'. A non-profit organization of manufacturers and vendors formed to promote a common technical standard for PC Card-based peripherals and the slot designed to hold them, primarily on portable computers and intelligent electronic devices.
Peer-to-peer network	A network of two or more computers that communicate without using a central server. This lack of reliance on a server differentiates a peer-to-peer network from a client/server network.
PING	A protocol for testing whether a particular computer is connected to the Internet by sending a packet to the computer's IP address and waiting for a response.
Plug and Play	A set of specifications that allows a computer to automatically detect and configure various peripheral devices, such as monitors, modems, and printers.
Port	A physical connection through which data is transferred between a computer and other devices (such as a monitor, modem, or printer), a network, or another computer. Also, a software channel for network communications.
PPPoE	Acronym for 'Point-to-Point Protocol over Ethernet'. A specification for connecting users on an Ethernet network to the Internet by using a broadband connection (typically through a DSL modem).
PPTP	IP Security, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).
PPTP	Point-to-Point Tunneling Protocol, a technology for creating Virtual Private Networks (VPNs). Because the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.
Profile	A computer-based record that contains an individual network's software settings and identification information.
Protocol	A set of rules that computers use to communicate with each other over a network.
Resource	Any type of hardware (such as a modem or printer) or software (such as an application, file, or game) that users can share on a network.
Restore factory defaults	

	The term used to describe the process of erasing your base station's current settings to restore factory settings. You accomplish this by pressing the Reset button and holding it for five or more seconds. Note that this is different from resetting the base station.
RJ-11 connector	An attachment used to join a telephone line to a device such as a modem or the external telephone lines.
RJ-45 connector	An attachment found on the ends of all Ethernet cables that connects Ethernet (wired) cables to other devices and computers
Server	A computer that provides shared resources, such as storage space or processing power, to network users.
Shared folder	A folder (on a computer) that has been made available for other people to use on a network.
Shared printer	A printer (connected to a computer) that has been made available for other people to use on a network.
Sharing	To make the resources associated with one computer available to users of other computers on a network.
SNTP	Acronym for 'Simple Network Time Protocol'. A protocol that enables client computers to synchronize their clocks with a time server over the Internet.
SSID	Acronym for 'Service Set Identifier', also known as a wireless network name. An SSID value uniquely identifies your network and is case sensitive.
Static IP address	A permanent Internet address of a computer (assigned by an ISP).
Straight-through cable	A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. There is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second. Unlike the Crossover cable, straight-through cable has the same order of pin contacts on each end-plug of the cable.
Subnet	A distinct network that forms part of a larger computer network. Subnets are connected through routers and can use a shared network address to connect to the Internet.
Subnet mask	Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. Similar in form to an IP address and typically provided by an ISP. An example of a subnet mask value is 255.255.0.0.
Switch	A central device that functions similarly to a hub, forwarding packets to specific ports rather than broadcasting every packet to every port. A switch is more efficient when used on a high-volume network.
Switched network	A communications network that uses switching to establish a connection between parties.
Switching	A communications method that uses temporary rather than permanent

	connections to establish a link or to route information between two parties. In computer networks, message switching and packet switching allow any two parties to exchange information. Messages are routed (switched) through intermediary stations that together serve to connect the sender and the receiver.
TCP/IP	Acronym for 'Transmission Control Protocol/Internet Protocol'. A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet communicates by using TCP/IP.
Throughput	The data transfer rate of a network, measured as the number of kilobytes per second transmitted.
USB	Acronym for 'universal serial bus'. USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.
USB adapter	A device that connects to a USB port.
USB connector	The plug end of the USB cable that is connected to a USB port. It is about half an inch wide, rectangular and somewhat flat.
USB port	A rectangular slot in a computer into which a USB connector is inserted.
UTP	Acronym for 'unshielded twisted pair'. A cable that contains one or more twisted pairs of wires without additional shielding. It's more flexible and takes less space than a shielded twisted pair (STP) cable, but has less bandwidth.
Virtual server	One of multiple Web sites running on the same server, each with a unique domain name and IP address.
VPN	A Virtual Private Network (VPN) is a private Network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling Protocol and security procedures.
WAN	Acronym for 'wide area network'. A geographically widespread network that might include many linked local area networks.
Wi-Fi	A term commonly used to mean the wireless 802.11b standard.
Wireless	Refers to technology that connects computers without the use of wires and cables. Wireless devices use radio transmission to connect computers on a network to one another. Radio signals can be transmitted through walls, ceilings, and floors, so you can connect computers that are in different rooms in the house without physically attaching them to one another.
Wireless access point	A device that exchanges data between wireless computers or between wireless computers and wired computers on a network.
Wireless network name	The single name of a grouping of computers that are linked together to form a network.

Wireless security	A wireless network encryption mechanism that helps to protect data transmitted over wireless networks.
WLAN	Acronym for wireless local area network. A network that exclusively relies on wireless technology for device connections.