Clavister ATCA SG6010 Getting Started Guide

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com

Published 2010-03-18

Clavister ATCA SG6010
Getting Started Guide

Published 2010-03-18

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. Clavister makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Clavister reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

List of Figures

Preface

Target Audience

The target audience for this guide is the user who has taken delivery of a packaged SG6010 Security Gateway Blade. The guide takes the user from unpacking and installation of the device through to power-up and initial network connection.

Notes to the Main Text

Special sections of text which the reader should pay special attention to are indicated by icons on the left hand side of the page followed by a short paragraph in italicized text. There are the following types of such sections:

Note

This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasised or something that is not obvious or explicitly stated in the preceding text.

Tip

This indicates a piece of non-critical information that is useful to know in certain situations but is not essential reading.

Caution

This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.

Important

This is an essential point that the reader should read and understand.

Warning

This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

Trademarks

Certain names in this publication are the trademarks of their respective owners.

CorePlus is the trademark of Clavister AB.

Windows, *Windows XP*, *Windows Vista* and *Windows 7* are either registered trademarks or

trademarks of Microsoft Corporation in the United States and/or other countries.

Apple and *Mac* are trademarks of Apple Inc. registered in the United States and/or other countries.

Chapter 1: Overview

The *SG6010 Security Gateway Blade* (SGB) is a high performing, blade based computing platform designed to run the Clavister CorePlus network security operating system in performance critical environments such as the telecoms industry, service providers, the financial sector and data centers. It is designed for insertion only into a Clavister ATCA chassis. Detailed chassis descriptions can be found in separate product manuals.

Figure 1.1. The SG6010 Security Gateway Blade

Follow Electrostatic Discharge (ESD) Precautions

Components can be damaged by electrostatic discharge (ESD). When an installation step instructs you to protect any replaceable component from ESD, follow the precautions described below:

- The product contains static-sensitive components and should be handled with care. Failure to employ adequate anti-static measures can cause irreparable damage to components.
- Handle the product only when wearing a grounded wrist strap at a grounded work area.
- Do not remove blades from the chassis or from their electrostatic discharge (ESD) shielding bags until a step instructs you to do so. Failure to follow ESD precautions may cause hardware damage.

Delivered and Optional Components

Included in the delivered package will be the SG6010 Security Gateway Blade itself. Optional components are:

- A Rear Transition Module (RTM).
- 1 or 2 advanced mezzanine cards (AMCs).

Not Included Components

The following components are not included with the packaged blade:

- A USB cable.
- A console serial cable (RJ-45 to DE9-S). The same cable is included with the Clavister SF6090 Switch Fabric Blade.

Chapter 2: Blade Installation

Optionally Install AMCs into the SG6010

If Advanced Mezzanine Cards (AMCs) are to be added to the blade, follow the AMC installation steps described in Chapter 3, *Optional AMC Installation*.

Optionally Install the RTM into the Chassis

The optional RTM is not normally required but can be added to provide extra ports for debugging purposes. The RTM is hot-swappable and can be installed before or after the SG6010 blade is installed and while power is applied to the chassis. This procedure explains where and how to install the RTM.

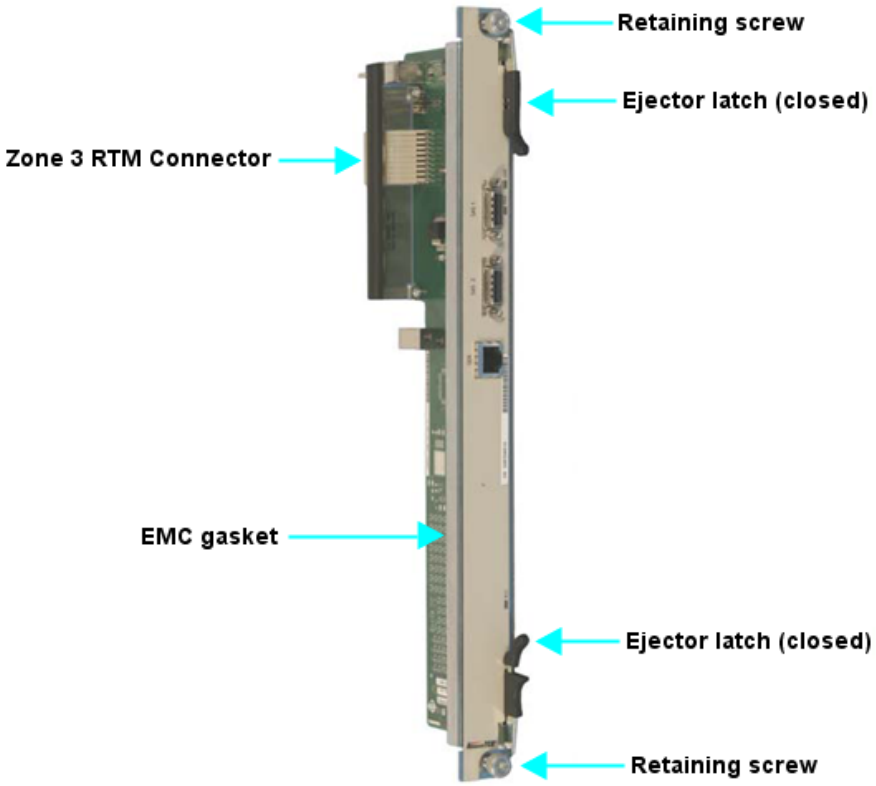


Figure 2.1. The Optional Rear Transition Module (RTM)

1. Identify placement in the back of the chassis. For example, if the CPM is installed in slot 1 in the front, the RTM will connect to the back of the chassis in slot 1.

2. Remove the airflow management panel, if present, from the back of the chassis where the RTM is to be installed.

3. Remove the RTM from its ESD shielding bag.

4. Inspect the EMC gasket to make sure it is free of debris. Lift the RTM ejector latches to the open position, and insert the RTM into the back panel slot. Use firm pressure to fully seat the RTM in the backplane connector. Make sure the EMC gasket seals the surfaces it touches.

5. Once the RTM is seated, simultaneously close both ejector latches.

6. Tighten the retaining screws in the top and bottom of the RTM panel.

Install the blade into the Chassis

The blade is hot-swappable and can be installed while power is applied to the chassis. This procedure assumes the power is already applied to the chassis.

1. Determine the node slot where the SG6010 is to be installed. Avoid the slots reserved for the hub modules. In the SC6500 chassis, the hub slots are 7 and 8; in the SC6300 chassis, the hub slots are 1 and 2.

2. Remove the blade from its ESD shielding bag.

3. Lift the ejector latches to the open position. Before inserting the SG6010, inspect the EMC gasket to make sure it is free of debris.

4. Holding the ejector latches in the open position, slide the blade all the way into the shelf.

5. When the ejector latches reach the latch rail on the shelf, close both ejector latches, but open the bottom or right latch again right away (so only the top or left ejector latch remains closed). This will prevent the SG6010 from starting up. Later, you will be instructed to close the other ejector latch to start the bootup.

6. Make sure that the front panel EMC gasket seals all the surfaces it touches.

Connect a Console to the Serial Port

A console can be connected to display and interact with CorePlus as shown in the illustration below. This console can be used to enter CLI commands and will be necessary later to determine the MAC address of any of the physical interfaces.

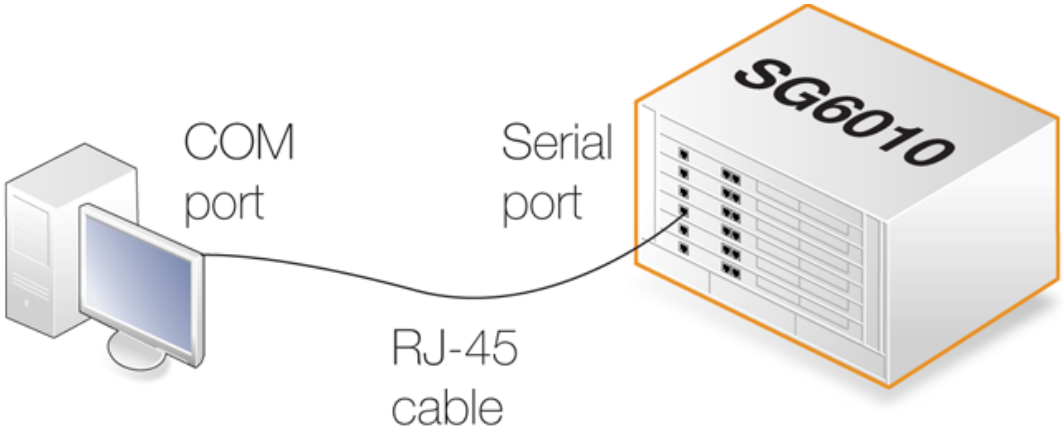


Figure 2.2. Serial Port Connection

The setup steps are as follows:

1. Connect a serial cable to the serial port of the CPM.
2. Connect the other end of the cable to the COM port of the console. This will probably be a computer running a treminal emulator.
3. Configure the terminal emulator to match the default settings for the blade. The setting are:
   a. 115200 bps.
   b. No parity.
   c. 8 data bits.
   d. 1 stop bit.
   e. No flow control.
   f. For best display results, the terminal should be set to at least 80 columns by at least 25 lines.

Note

If distorted characters are displayed, double-check that the same communication parameters are set for both the serial port and the COM port.

Chapter 3: Optional AMC Installation

Clavister *Advanced Mezzanine Cards* (AMCs) are standard form-factor components defined by PCI Industrial Computer Manufacturers Group and can be installed in any compatible ATCA carrier module such as a SG6010 blade.

Note
This guide assumes the SG6010 is already installed in a chassis with the power applied.

Unpacking

AMCs should be unpacked with the same precautions as the SG6010 which are described in Chapter 1, *Overview*.

Warning
Do not remove an AMC before its hot-swap LED turns solid blue. Removing it prematurely can cause unpredictable results in other parts of the system.

Remove an Existing AMC or Filler Module

To remove an installed AMC or airflow management filler module from a carrier module bay:

1. Gently pull the AMC module handle (see Figure 1). If removing a filler module, proceed to the step 4.
2. Wait for the AMC's hot-swap LED to turn solid blue.
3. If possible, wait 3 to 5 minutes to let the airflow of the system cool the AMC.

Warning
Be careful when removing the AMC. Do not touch the AMC's heat sink. It may be hot to the touch.

4. Pull the module handle firmly and slide the module out of the bay.

Install an AMC or filler module into each unpopulated bay to continue operating within EMC and

thermal specifications.

Installation

To install the AMC into the SG6010 the steps are:

1. Remove the new AMC from its ESD shielding bag.
2. Ensure that the EMC gaskets on the AMC are free from debris.
3. Insert the AMC into the bay opening.
4. Slide the AMC along the guide rails, and firmly seat it into the carrier module's connector. Make sure the AMC's EMC gaskets seal the surfaces they touch.
5. Press the module handle firmly into the AMC until it stops. This starts the AMC power cycle.

   If the carrier module is installed in a shelf with power applied, the blue hot-swap LED flashes until the module is active, then turns off.

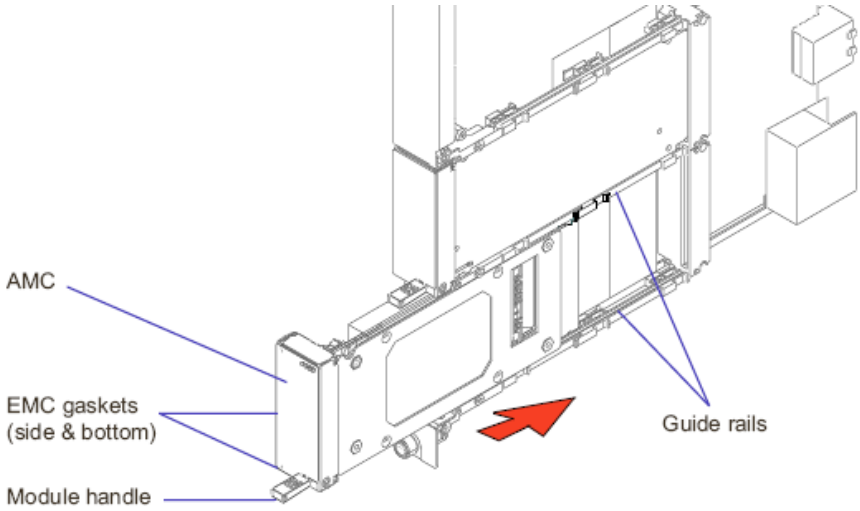


Figure 3.1. AMC Insertion

Verifying Installation

After a hot swap is complete, wait one additional minute, then confirm the following from the LEDs:

1. The red or amber out-of-service LED is off.
2. The green power LED is on.
3. The blue hot-swap LED is off.

If the LEDs are not in the states listed above, verify that the ejector latches on the carrier module are completely closed, and that the AMC module handle is pushed in firmly. See the AMC's reference manual for additional troubleshooting tips. All LED colors are shown below.

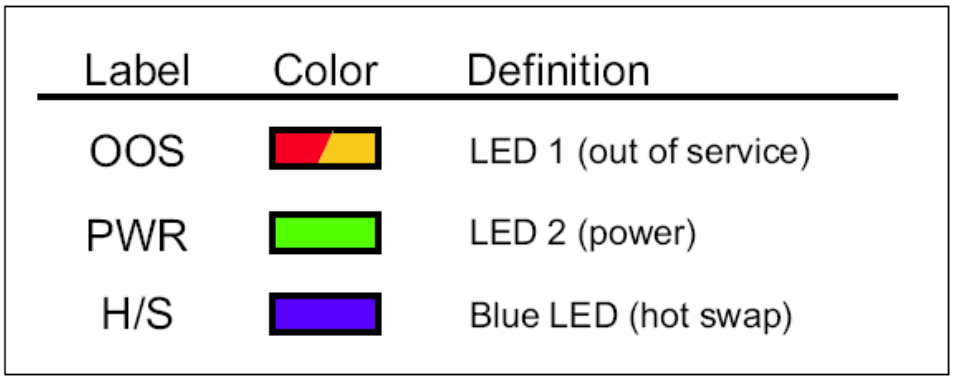


Figure 3.2. LED States

Chapter 4: CorePlus Configuration

4.1. Management Workstation Connection

CorePlus is Pre-installed on Clavister Hardware

It is assumed you have now unpacked, installed and powered up the SG6010 blade unit. If not, you should refer to the earlier chapters in this manual before continuing. CorePlus is already installed on the SG6010 blade in the factory and will automatically boot up after switching on power.

The Default Management Interface

After first time startup, CorePlus scans the available Ethernet interfaces and makes management access available on the first interface found and assigns the internal IP address *192.168.1.1* to it.

For the SG6010 blade, this is the **ge1** interface.

Alternative CorePlus Setup Methods

Initial CorePlus software configuration can be done in one of the following ways:

- **Through a web browser.**

  A standard web browser running on a standalone computer (also referred to as the *management workstation*) can be used to access the CorePlus *Web Interface*. This provides an intuitive graphical interface for CorePlus management. When this interface is accessed for the first time, a *setup wizard* runs automatically to guide a new user through key setup steps. The

wizard can be closed if the administrator wishes to go directly to the Web Interface to perform setup manually.

The wizard is recommended for its simplification of initial setup and is described in detail in *Section 4.2, "Web Interface and Wizard Setup"*.

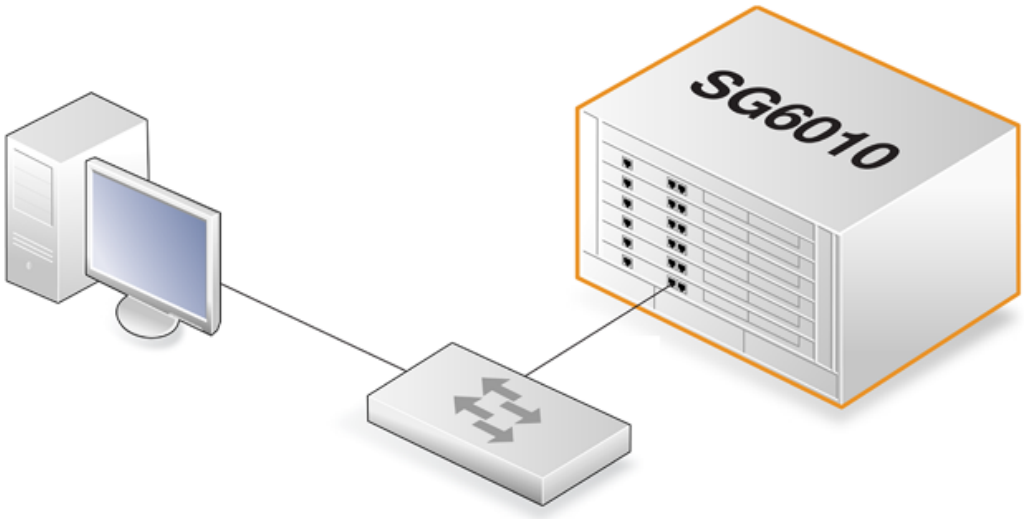
- **Through a terminal console using CLI commands.**

  The setup process can alternatively be performed using console CLI commands and this is described in *Section 4.4, "CLI Setup"*. The CLI allows step by step control of setup and should be used by administrators who fully understand both the CLI and setup process.

  CLI access can be remote, across a network to a physical interface using a similar connection to that used with the Web Interface. Alternatively, CLI access can be through a console connected directly to the local RS-232 port on the SG6010 blade hardware. Direct console connection is described in *Chapter 2, Blade Installation*.

Network Connection Setup

For setup using the Web Interface or the remote CLI, we must first connect a workstation to the SG6010 blade across a network. Workstation connection is illustrated below.



The designated management interface for the SG6010 blade is **ge1** and this should be connected to the same network as the management workstation (or a network accessible from the workstation via one or more switches). Typically the connection is made via a switch or hub in the network using a regular straight-through Ethernet cable. For connection to the public Internet, another interface should be connected to your ISP and this is referred to below and in the setup wizard as the *WAN* interface.

For the SG6010 blade, the *WAN* interface could be chosen from any of the physical interfaces other than the **ge1** interface.

Using Crossover Cables

Connection to the management interface by the workstation can be done directly without a switch or hub. This is done by using a crossover cable.

Workstation Interface Setup

Traffic will be able to flow between the designated workstation interface and the Clavister Security Gateway interface because they are on the same IP network. This means the workstation interface must be first assigned the following static IP addresses:

- **IP address:** *192.168.1.30*
- **Subnet mask:** *255.255.255.0*
- **Default gateway:** *192.168.1.1*

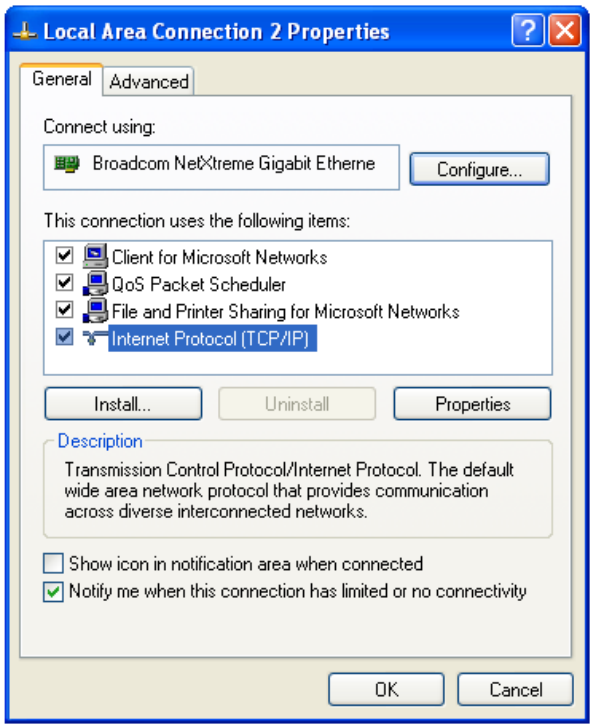
Tip: Using another interface IP address

*The assigned IP address **192.168.1.30** could be another address from the 192.168.1.0/24 network as long as it is different from **192.168.1.1** which is the address used by CorePlus on its default management interface.*

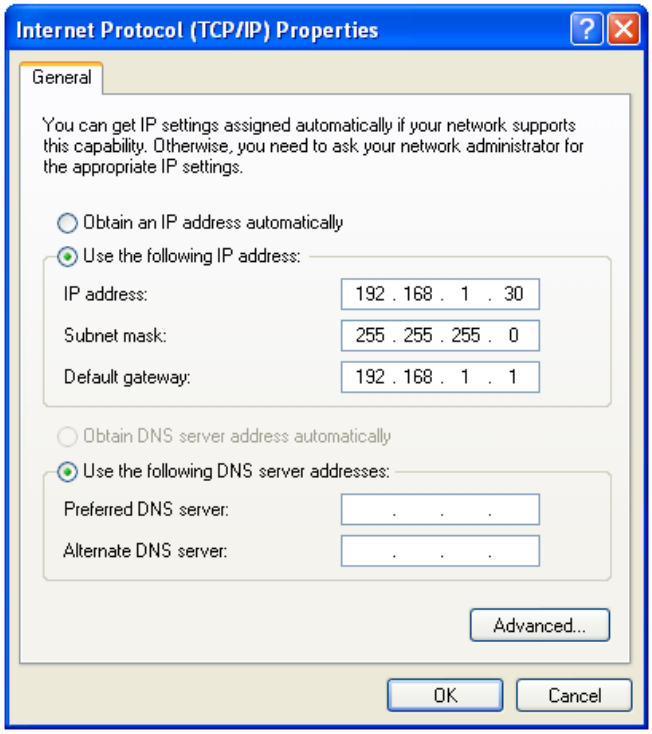
To enter these settings on a PC running Windows XP, the following steps are needed:

- Click the **Start** button.
- Right click on **My Network Places** and select **Properties**.

- Right click the chosen Ethernet interface and select **Properties**.
- Select **Internet Protocol (TCP/IP)** and click **Properties**.



- Enter the IP addresses given above and click **OK**.



Note: DNS addresses can be entered later

To browse the Internet from the management workstation via the security gateway then it is possible to go back to the last step's properties dialog later and enter DNS server IP addresses. For now, they are not required.

IP Setup on Other Platforms

The following appendicies describe management workstation IP setup for other platforms:

- ***Appendix B, Vista IP Setup***.
- ***Appendix C, Windows 7 IP Setup***.
- ***Appendix D, Apple Mac IP Setup***.

4.2. Web Interface and Wizard Setup

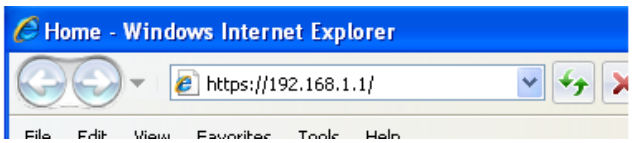
This chapter describes the setup when accessing the CorePlus for the first time through a web browser. The user interface accessed in this way is called the *Web Interface*.

Note

Many of the screenshots in this chapter have had whitespace removed from the original image to improve the readability. However, all of the informational content in the images has been preserved.

Connect By Surfing to *https://192.168.1.1*

Using a web browser (Internet Explorer or Firefox is recommended) enter the address *https://192.168.1.1* into the navigation window as shown below.



Check for a proxy server and turn off popup blocking.

Make sure the web browser does not have a proxy server configured.

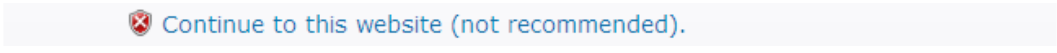
Any popup blocking in the browser should also be temporarily turned off to allow the setup wizard to run.

If there is no response from CorePlus and the reason is not clear, refer to the help checklist in *Section 4.5, "Troubleshooting Setup"*.

The CorePlus Self-signed Certificate

When responding to an *https://* request, CorePlus sends a self-signed certificate which will not be initially recognised so it will be necessary to tell the browser to accept the certificate for this and future sessions. Different browsers handle this in slightly different ways. In Microsoft Internet Explorer the following error message will be displayed in the browser window.

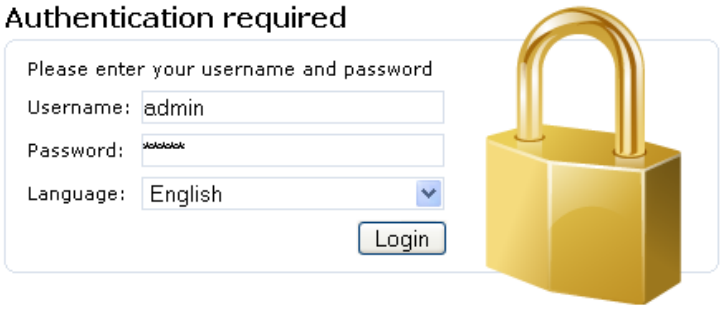
To continue, tell IE to accept the certificate by clicking the following link which appears near the bottom of the browser window.



In FireFox this procedure is called *Add a security exception*.

The Login Dialog

CorePlus will next respond like a web server with the initial login dialog page as shown below.



The available Web Interface language options are selectable at the bottom of this dialog. This defaults to the language set for the browser if CorePlus supports that language.

Logging In and the Setup Wizard

Now login with the username *admin* and the password *admin*. The Web Interface will appear and the CorePlus setup wizard should begin automatically. The first wizard dialog is the wizard welcome screen which should appear as shown below.

Cancelling the Wizard

The setup wizard can be cancelled at any point before the final *Activate* screen and run again by choosing the *Setup Wizard* option from the Web Interface toolbar. Once any configuration changes have been made and activated, either through the wizard, Web Interface or CLI, then the wizard cannot be run since the wizard requires that CorePlus has the factory defaults.

The Wizard Assumes Internet Access will be Configured

The wizard assumes that Internet access will be configured. If this is not the case, for example if the Clavister Security Gateway is being used in *Transparent Mode* between two internal networks, then the configuration setup is best done with individual Web Interface steps or through the CLI instead of through the wizard.

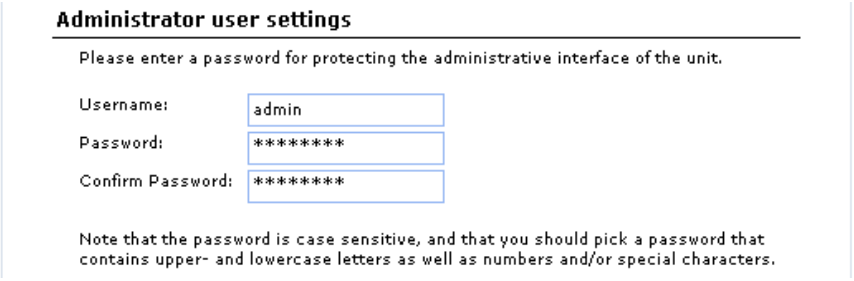
Advantages of the Wizard

The wizard makes setup easier because it automates what would otherwise be a more complex set of individual setup steps. It also reminds you to perform important tasks such as setting the date and time and configuring a log server.

The steps that the wizard goes through after the welcome screen are listed next.

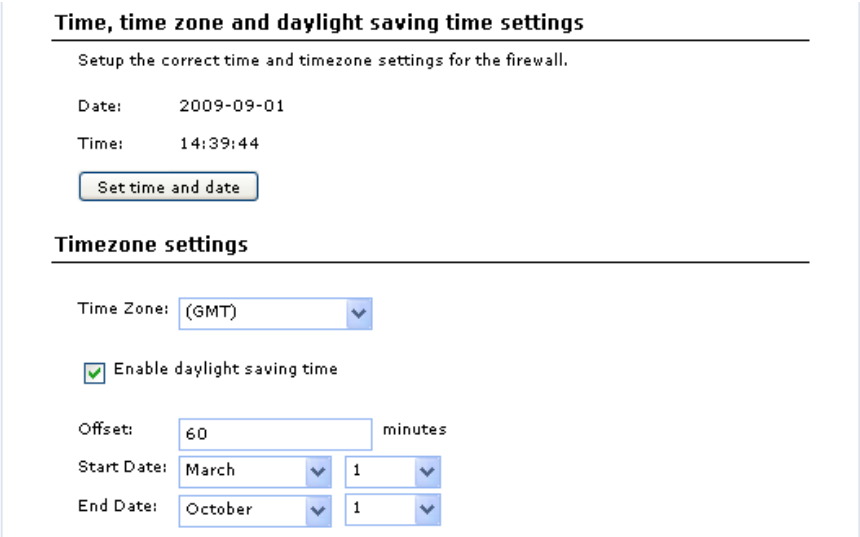
Wizard step 1: Enter a new username and password

You will be prompted to enter a new administration username and password as shown below. It is recommended that this is always done and the new username/password is remembered (if these are forgotten, restoring to factory defaults will restore the original *admin*/*admin* combination). The password should be composed in a way which makes it difficult to guess.



Wizard step 2: Set the date and time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly in the fields shown below.

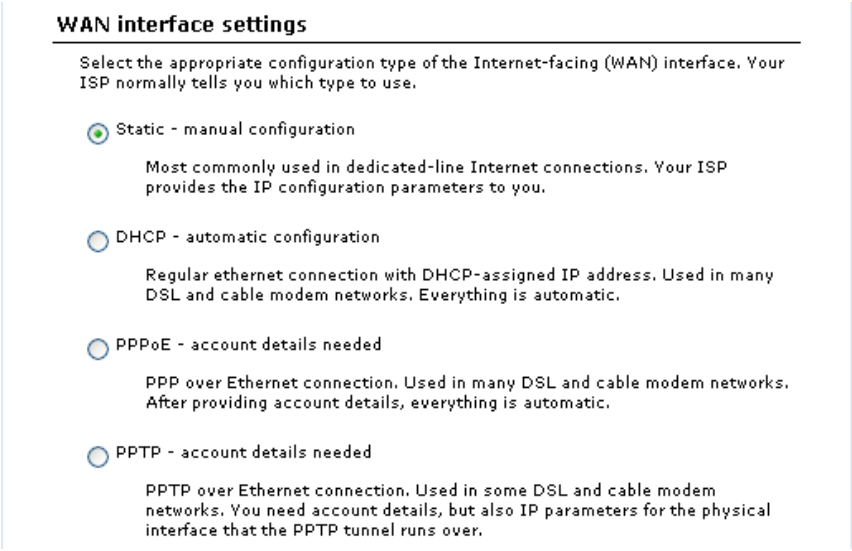


Wizard step 3: Select the *WAN* interface

Next, you will be asked for the *WAN* interface that will be used to connect to your ISP for Internet access.

Wizard step 4: Select the *WAN* interface settings

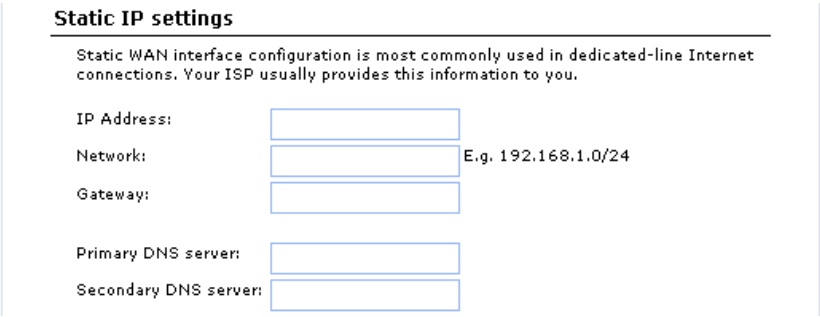
This step selects how the WAN connection to the Internet will function. It can be one of *Manual configuration*, *DHCP*, *PPPoE* or *PPTP* as shown below.



These four different connection options are discussed next in the following subsections **4A** to **4D**.

- **4A. Static - manual configuration**

  Information supplied by the ISP should be entered in the next wizard screen. All fields need to be entered except for the *Secondary DNS server* field.

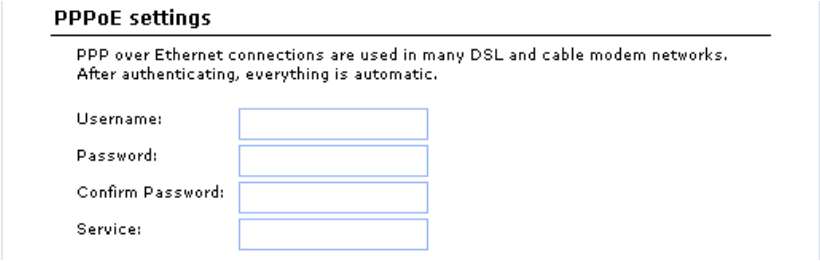


- **4B. DHCP - automatic configuration**

  All required IP addresses will automatically be retrieved from the ISP's DHCP server with this option. No further configuration is required for this so it does not have its own wizard screen.

- **4C. PPPoE settings**

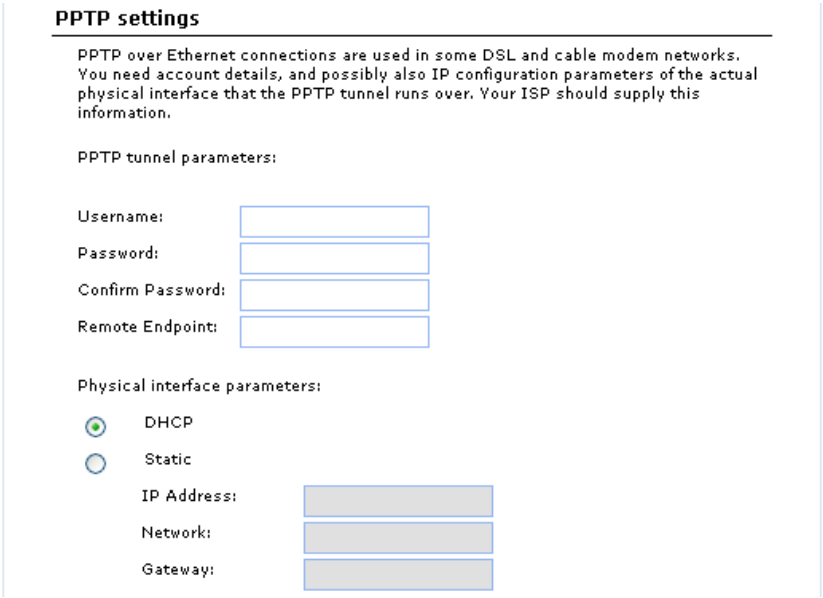
  The username and password supplied by your ISP for PPPoE connection should be entered. The *Service* field should be left blank unless the ISP supplies a value for it.



DNS servers are set automatically after connection with PPPoE.

- **4D. PPTP settings**

  The username and password supplied by your ISP for PPTP connection should be entered. If DHCP is to be used with the ISP then this should be selected, otherwise *Static* should be selected followed by entering the static IP address supplied by the ISP.

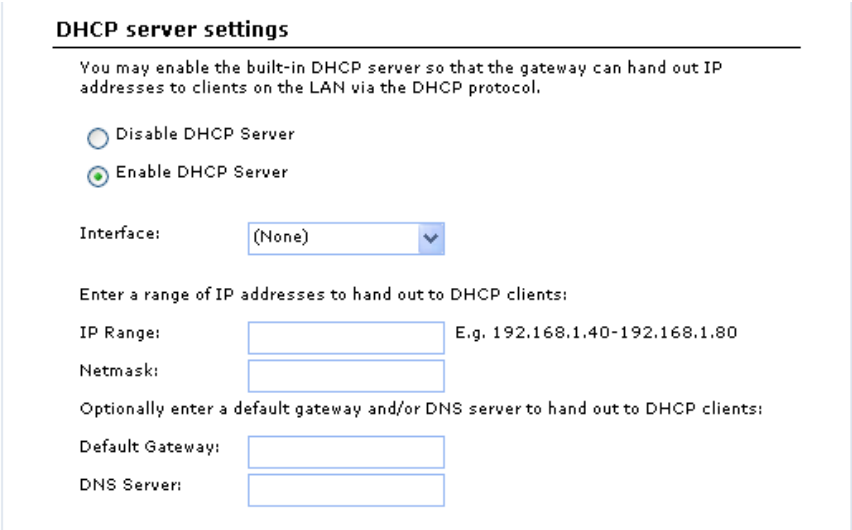


DNS servers are set automatically after connection with PPTP.

Wizard step 5: DHCP server settings

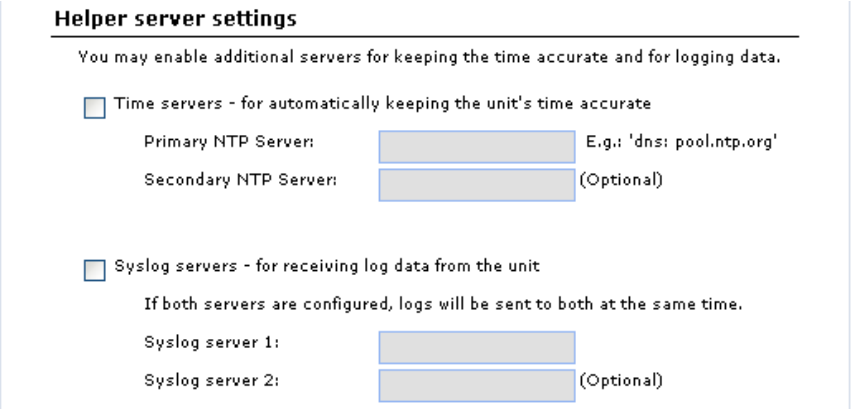
If the Clavister Security Gateway is to function as a DHCP server, it can be enabled here in the wizard on a particular interface or configured later.

The range of IP addresses that can be handed out must be specified in the form *nn.nn.nn.nn - nn.nn.nn.nn*. For instance, the internal IP address range *192.168.1.50 - 192.168.1.150* might be specified.



Wizard step 6: Helper server settings

Optional NTP and Syslog servers can be enabled here in the wizard or configured later. *Network Time Protocol* servers keep the system date and time accurate. Syslog servers can be used to receive and store log messages sent by CorePlus.

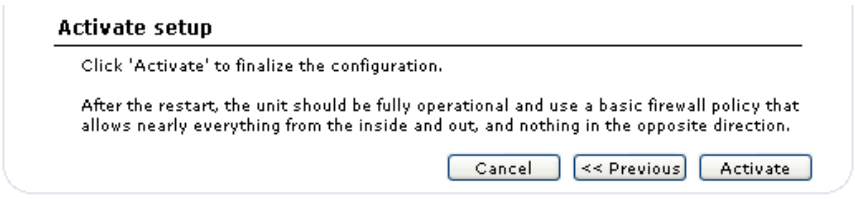


For the default gateway, it is recommended to specify the IP address *192.168.1.1* and the DNS server specified should be the DNS supplied by your ISP.

When specifying a hostname as a server instead of an IP address, the hostname should be prefixed with the string *dns:*. For example, the hostname *host1.company.com* should be entered as *dns:host1.company.com*.

Wizard step 7: Activate setup

The final step is to activate the setup by pressing the *Activate* button. After this step the Web Interface returns to its normal appearance and the administrator can continue to configure the system.



Running the Wizard Again

Once the wizard has been successfully finished and activated, it cannot be run again. The exception to this is if the Clavister Security Gateway has its factory defaults restored in which case the unit will behave as though it were being started for the first time.

Uploading a License

If the wizard has been run or not, the Web Interface can now be used to upload a valid license to the Clavister Security Gateway. Without a license, CorePlus will run in *demonstration mode* which means that it will cease to function after two hours of operation (restarting the system will re-enable CorePlus for another two hours). The steps for license upload are:

- Using a web browser, surf to the Clavister *Customer Web* (this can be found at *https://clientweb.clavister.com*) and register for the first time. You will require your Clavister *registration key* to do this. If you are already registered as a customer then you need to directly login to the Customer Web.
- The Customer Web system will ask for a *MAC address* to associate with the Clavister license. This is the hardware Ethernet address associated with one of the Ethernet interfaces on the unit.

  An interface MAC address can be read from the output of the *ifstat* CLI command and this command can be entered via the serial console. The *ifstat* on its own will give a list of detected interfaces with their names. Typing the same command followed by the interface name will provide the MAC address for that interface. For example, with the interface *ge1* the command is:

```
Device:/> ifstat ge1
```

- Now download a valid *.lic* license file from the Customer Web to the hard disk of the workstation.
- In the Web Interface menu bar, go to **Maintenance > Upgrade** and use the **Browse** button to select the license file, then upload it. As soon as the license is uploaded, demonstration mode will end and CorePlus will be restricted only by the limitations of the license.

4.3. Manual Web Interface Setup

This section describes initial CorePlus configuration performed directly through the Web Interface, without using the setup wizard. Configuration is done as a series of individual steps, giving the administrator more direct control over the process. Even if the wizard is used, this section can also be read as a good introduction to using the Web Interface for configuring key aspects of CorePlus.

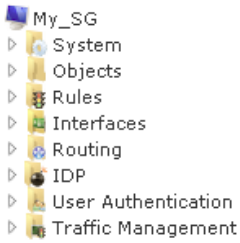
Ethernet Interfaces

The physical connection of external networks to the Clavister Security Gateway is through the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, CorePlus scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All CorePlus interfaces are logically equal for CorePlus and although their physical capabilities may be different, any interface can perform any logical function. With the SG6010 blade, the *ge1* interface is the default management interface. The other interfaces can be used as required. For this section, we will assume that the *ge2* interface will be used for connection to the public Internet and the *sfp1* interface will be used for connection to a protected, local network.

The Navigation Tree

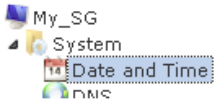
The Web Interface presents the various components of CorePlus in a tree structure in the left-hand pane of the browser window.



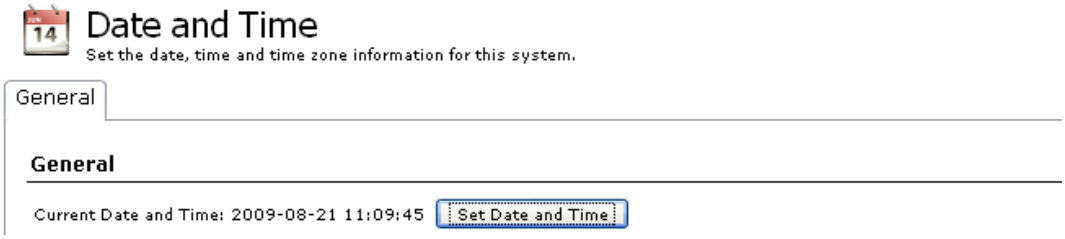
By clicking on the navigation tree we can expand its nodes to examine and change the properties of the various *settings*, *objects* and *rules* that make up a CorePlus configuration. A simple example of changing a configuration is discussed next.

Setting the Date and Time

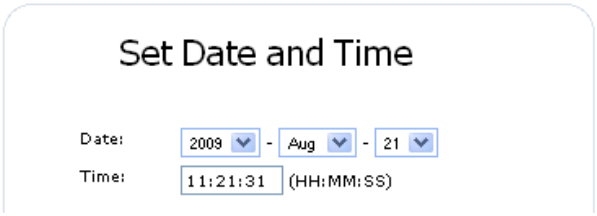
Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly. To do this, open the *System* node in the navigation tree.



If we now click on the *Date and Time* node in the tree, the properties of the current date and time settings will appear in the central panel of the Web Interface.



By pressing the **Set Date and Time** button, a dialog appears that allows the exact time to be set.



A **Network Time Protocol** (NTP) servers can optionally be configured to maintain the accuracy of the system date and time and this will require public Internet access. Enabling this option is strongly recommended since it ensures the accuracy of the date and time. A typical NTP setup is shown below.

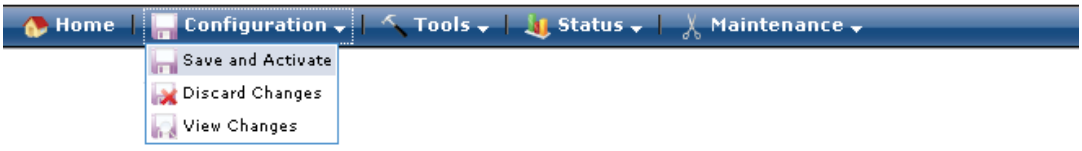
Note: The time server URL requires the "dns:" prefix

*When specifying a URL in CorePlus for the time server, the URL must have the prefix "**dns:**".*

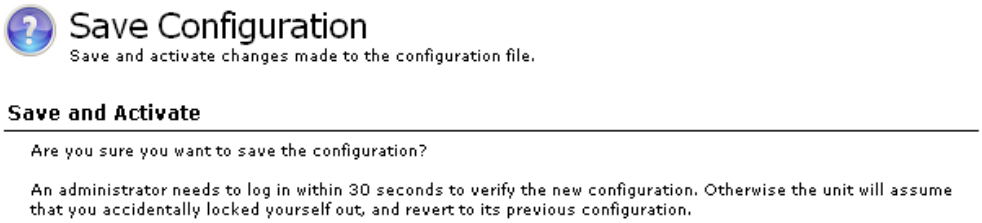
Once the values are set correctly, we can press the **OK** button to save the values while we move on to more steps in CorePlus configuration. Although changed values like this are saved by CorePlus, they do not become active until the entire saved configuration becomes the current and active configuration. We will look at how to do this next.

Activating Configuration Changes

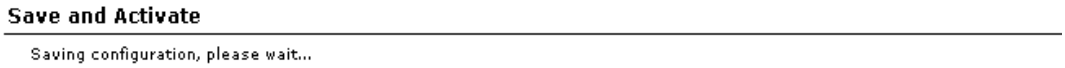
To activate any CorePlus configuration changes made so far, we need to select the **Save and Activate** option from the **Configuration** menu (this process is also sometimes referred to as *deploying* a configuration).



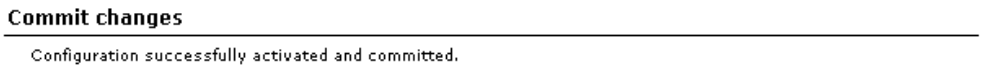
A dialog is then presented to confirm that the new configuration is to become the running configuration.



After clicking **OK**, CorePlus *reconfiguration* will take place and, after a short delay, the Web Interface will try and connect again to the security gateway.



If no reconnection is detected by CorePlus within 30 seconds (this length of time is a setting that can be changed) then CorePlus will revert back to the original configuration. This is to ensure that the new configuration does not accidentally lock out the administrator. After reconfiguration and successful reconnection, a success message is displayed indicating successful reconfiguration.



Reconfiguration is a process that the CorePlus administrator may initiate often. Normally, reconfiguration takes a brief amount of time and causes only a slight delay in traffic throughput. Active user connections through the Clavister Security Gateway should rarely be lost.

Tip: How frequently to commit changes

It is up to the administrator to decide how many changes to make before activating a new configuration. Sometimes, activating configuration changes in small batches can be appropriate in order to check that a small set of changes work as planned. It is, however, not advisable to leave changes uncommited for long periods of time, such as overnight, since any system outage will result in these edits being lost.

Automatic Logout

If there is no activity through the Web Interface for a period of time (the default is 15 minutes), CorePlus will automatically log the user out. If they log back in through the same web browser session then they will return to the point they were at before the logout occurred and no saved (but not yet activated) changes are lost.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access. The setup wizard described in the previous chapter, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The individual manual steps to configure these connection alternatives with the Web Interface are discussed next.

A. Static - manual configuration

Manual configuration means that there will be a direct connection to the ISP and all the relevant IP addresses for the connecting interface are fixed values provided by the ISP which are entered into CorePlus manually.

Note: The interface DHCP option should be disabled

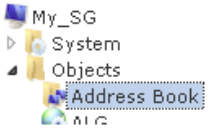
For static configuration of the Internet connection, the DHCP option must be disabled (the default) in the properties of the interface that will connect to the ISP.

The initial step is to set up a number of IP address objects in the CorePlus *Address Book*. Let us assume for this section that the physical interface used for Internet connection is *ge2*, the static IP address for this interface is to be *10.5.4.35*, the ISP's gateway IP address is *10.5.4.1*, and the network to which they both belong is *10.5.4.0/24*.

Note: Private IP addresses are used for example only

Each installation's IP addresses will be different from these IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IP addresses and in reality an ISP would use public IP addresses instead.

Let's now add the gateway *IP4 Address* object which we will call *wan_gw* and assign it the IP address *10.5.4.1*. The ISP's gateway is the first router hop towards the public Internet from the Clavister Security Gateway. Go to **System > Objects > Address Book** in the Web Interface navigation tree.



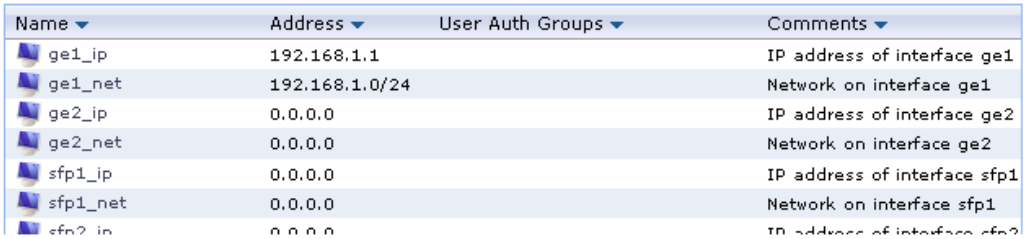
The current contents of the address book will be listed and will contain a number of predefined objects created by CorePlus after it scans the interfaces for the first time. The screenshot below shows the initial address book for the SG6010 blade.

Name	Address	User Auth Groups	Comments
all-nets	0.0.0.0/0		All possible networks
InterfaceAddresses			
localhost	127.0.0.1 (127.0.0.2)		Localhost, for non-management High Availability cluster interfaces

Note: The all-nets address

*The IP address object **all-nets** is a wildcard address that should never be changed and can be used in many types of CorePlus rules to refer to any IP address or network range.*

All the interface related address objects are gathered together in an *address book folder* called *InterfaceAddresses*. By clicking on this folder, we open it and can view the addresses it contains. The first few default addresses in the folder are shown below.

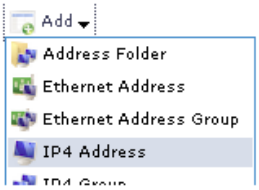


By default on initial startup, two IP address objects are create automatically for each interface detected by CorePlus. One IP address object is named by combining the physical interface name with the suffix *_ip* and this is used for the IP address assigned to that interface. The other address object is named by combining the interface name with the suffix *_net* and this is the network to which the interface belongs.

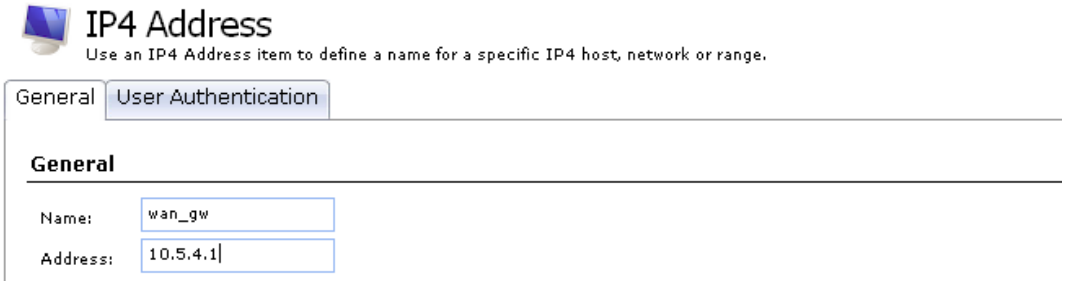
Tip: Creating address book folders

New folders can be created when needed and provide a convenient way to group together related IP address objects. The folder name can be chosen to indicate the folder's contents.

Now click the **Add** button at the top left of the list and choose the *IP4 Address* option to add a new address to the folder.



Enter the details of the object into the properties fields for the IP4 Address. Below, we have entered the IP address *10.5.4.1* for the address object called *wan_gw*. This is the IP of the ISP's router which acts as the gateway to the Internet.

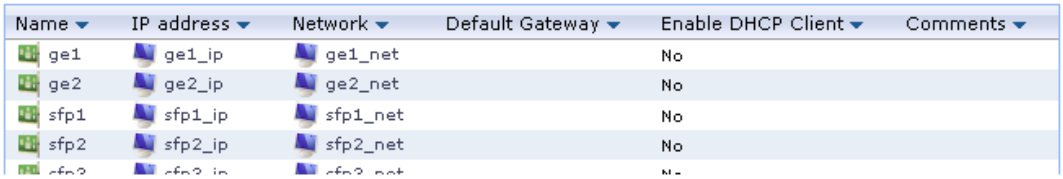


Click the **OK** button to save the values entered.

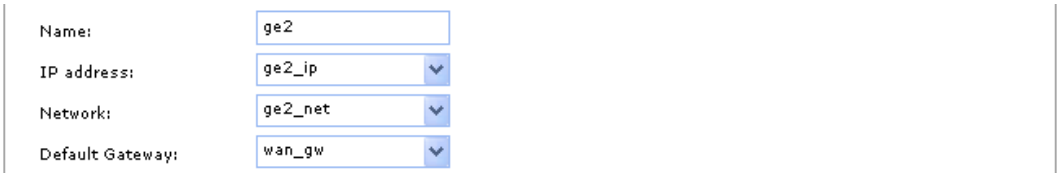
Then set up *ge2_ip* to be *10.5.4.35*. This is the IP address of the *ge2* interface which will connect to the ISP's gateway.

Lastly, set the IP4 Address object *ge2_net* to be *10.5.4.0/24*. Both *ge2_ip* and *wan_gw* must belong to this network in order for the interface to communicate with the ISP.

Together, these 3 IP address objects will be used to configure the interface connected to the Internet which in this example is *ge2*. Select **Interfaces > Ethernet** in the navigation tree to display a list of the physical interfaces. The first few lines of the interface list for the SG6010 blade are shown below.



Click on the interface in the list which is to be connected to the Internet. The properties for this interface will now appear and the relevant settings can be entered or changed.



Press **OK** to save the changes. Although changes are remembered by CorePlus, the changed configuration is not yet activated and won't be activated until CorePlus is told to activate the changed configuration.

Remember that DHCP should **not** be enabled when using static IP addresses and also that the IP address of the *Default Gateway* (which is the ISP's router) **must** be specified. As explained in more detail later, specifying the *Default Gateway* also has the additional effect of automatically adding a route for the gateway in the CorePlus routing table.

At this point, the connection to the Internet is configured but no traffic can flow to or from the Internet since all traffic needs a minimum of the following two CorePlus configuration objects to exist before it can flow through the Clavister Security Gateway:

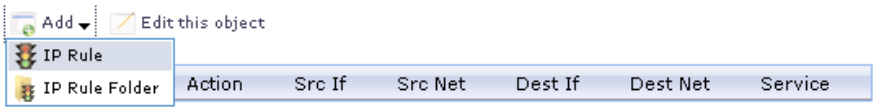
- An *IP rule* defined in a CorePlus *IP rule set* that explicitly allows traffic to flow from a given source network and source interface to a given destination network and destination interface.
- A *route* defined in a CorePlus routing table which specifies on which interface CorePlus can find the traffic's destination IP address.

  If multiple matching routes are found, CorePlus uses the route that has the smallest (in other words, the narrowest) IP range.

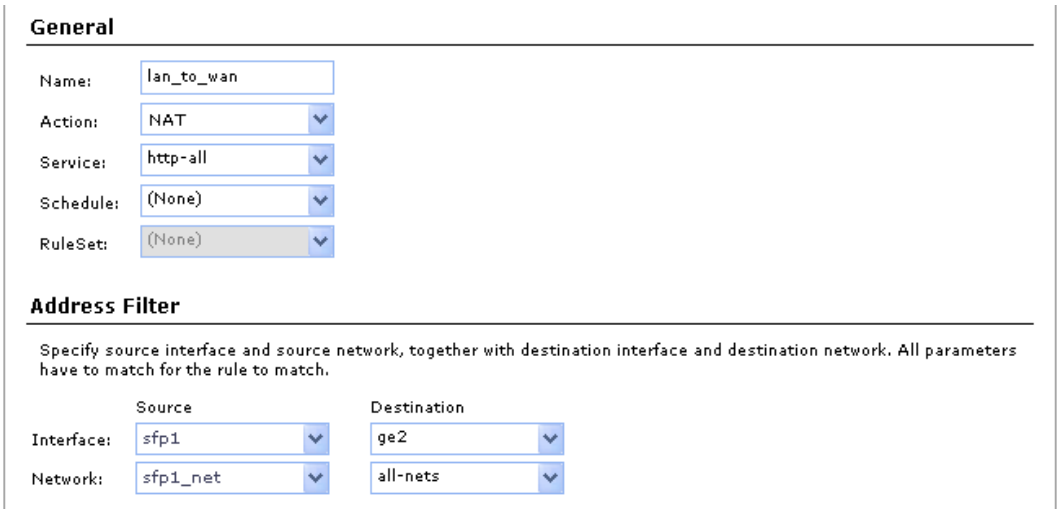
We must therefore first define an IP rule that will allow traffic from a designated source interface and source network. In this case let us assume we want to allow web surfers on the internal network *sfp1_net* connected to the interface *sfp1* to be able to access the public Internet.

To do this, we first go to **Rules > IP Rule Sets > main** in the navigation tree.

The empty *main* IP rule set will now appear. Press the **Add** button at the top left and select **IP Rule** from the menu.



The properties for the new IP rule will appear. In this example, we will call the rule *lan_to_wan*. The rule *Action* is set to *NAT* (this is explained further below) and the *Service* is set to *http-all* which is suitable for most web surfing (it allows both HTTP and HTTPS connections). The interface and network for the source and destinations are defined in the *Address Filter* section of the rule.



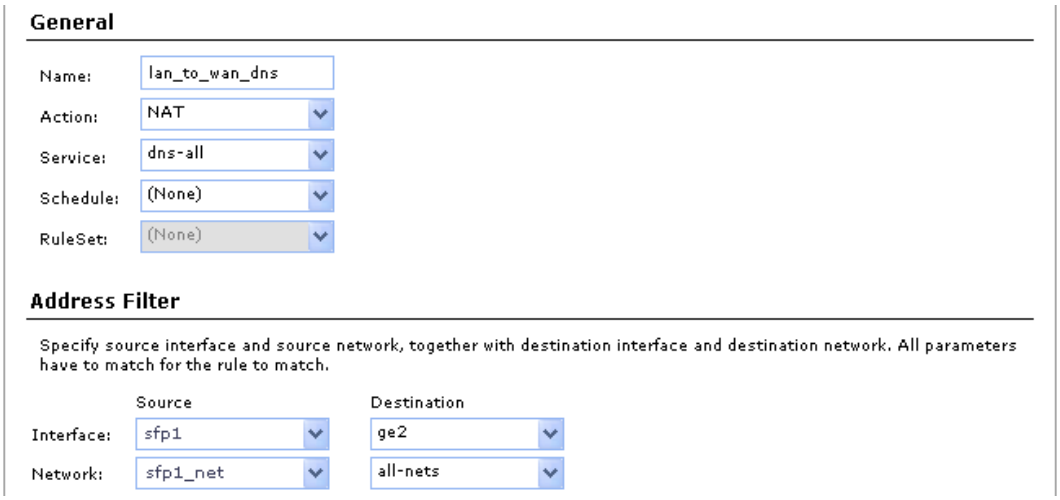
The destination network in the IP rule is specified as the predefined IP4 Address object *all-nets*. This is used since we don't know to which IP address the web surfing will be done and this allows surfing to any IP address. IP rules are processed in a top down fashion, with the first matching rule being obeyed. An *all-nets* rule like this should be placed towards the bottom of the rule set since other rules with narrower destination addreses should trigger before it does.

Only one rule is needed since any traffic controlled by a *NAT* rule will be controlled by the CorePlus *state engine*. This means that the rule will allow *connections* that originate from the source network/destination and also implicitly allow any returning traffic that results from those connections.

In the above, we selected the service called *http_all* which is already defined in CorePlus. It is advisable to make the service in an IP rule as restrictive as possible to provide the best security possible. Custom service objects can be created and new service objects can be created which are combinations of existing services.

We could have specified the rule *Action* to be *Allow*, but only if all the hosts on the protected local network have public IP addresses. By using *NAT*, CorePlus will use the destination interface's IP address as the source IP. This means that external hosts will send their responses back to the interface IP and CorePlus will automatically direct the traffic back to the originating local host. Only the outgoing interface therefore needs to have a public IP address and the internal network topology is hidden.

To allow web surfing, DNS lookup also needs to be allowed in order to resolve URLs into IP addresses. The service *http_all* does not include the *DNS* protocol so we need a similar IP rule that allows this. This could be done with one IP rule that uses a custom service which combines the *HTTP* and *DNS* protocols but the recommended method is to create an entirely new IP rule that mirrors the above rule but specifies the service as *dns-all*. This method provides the most clarity when the configuration is examined for any problems. The screenshot below shows a new rule called *lan_to_wan_dns* being created to allow DNS.



This IP rule also specifies that the action for DNS requests is *NAT* so all DNS request traffic is sent out by CorePlus with the outgoing interface's IP address as the source IP.

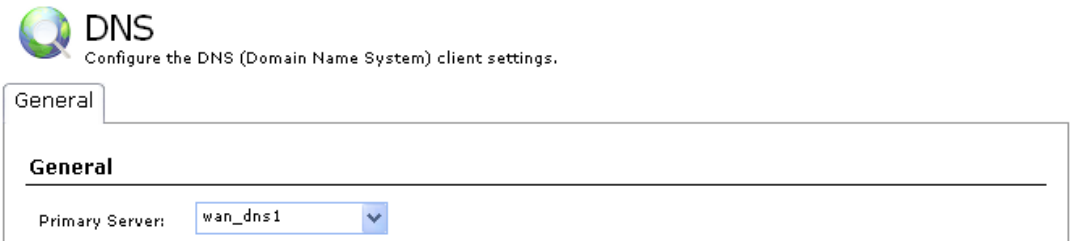
For the Internet connection to work, we also need a *route*defined so that CorePlus knows on which interface the web surfing traffic should leave the Clavister Security Gateway. This route will define the interface where the network *all-nets* will be found. If we open the default *main* routing table by going to **Routing > Routing Tables > Main** in the navigation tree, the route needed should appear as below.

This required *all-nets* route is, in fact, added automatically after specifing the *Default Gateway* for a particular Ethernet interface which we did earlier after setting up the required IP4 Address objects.

Note: Disabling automatic route generation

*Automatic route generation is enabled and disabled with the setting "**Automatically add a default route for this interface using the given default gateway**" which can be found in the properties of the interface.*

As part of the setup, it is also recommended that at least one DNS server is also defined in CorePlus. This DSN server or servers (a maximum of three can be configured) will be used when CorePlus itself needs to resolve URLs which is the case when a URL is specified in a configuration instead of an IP address. Let's assume an IP address object called *wan_dns1* has already been defined in the address book which is the IP address for the first DNS server. By choosing **System > DNS** in the navigation tree, the DNS server dialog will open and this object from the address book can be assigned as the first server.



B. DHCP - automatic configuration

All the required IP addresses for Internet connection can, alternatively, be automatically retrieved from an ISP's DHCP server by enabling the **DHCP Client** option for the interface connected to the ISP. We enable this option by first selecting **Ethernet > Interfaces** in the navigation tree to display a list of all the interfaces.

Click the *ge2* interface in the list to display its properties.

In the above screenshot, DHCP is enabled for this interface and this is the required setting if IP addresses are to be retrieved automatically. Usually, a DHCP *Host Name* does not need to be specified but can sometimes be used by an ISP to uniquely identify this Clavister Security Gateway as a particular DHCP client to the ISP's DHCP server.

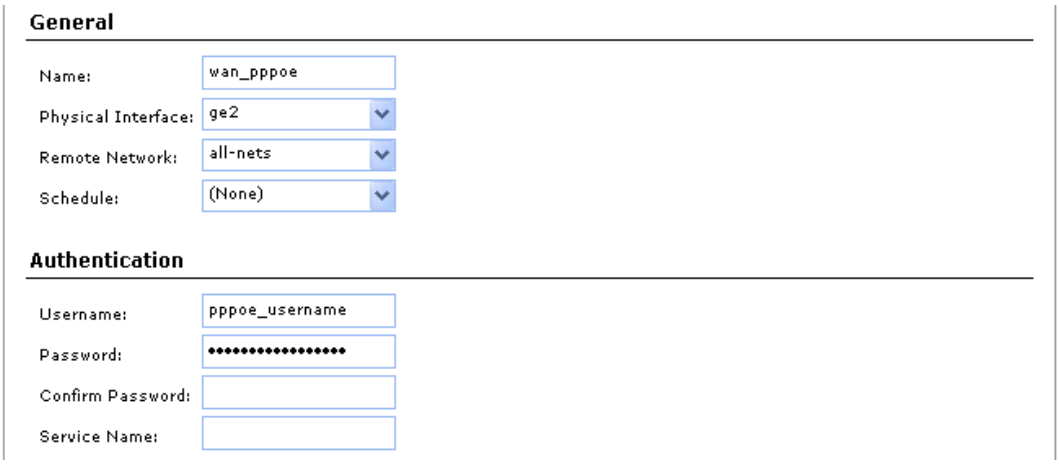
On connection to the ISP, all required IP addresses are retrieved automatically from the ISP via DHCP and CorePlus automatically sets the relevant address objects in the address book with this information.

For CorePlus to know on which interface to find the public Internet, a *route* has to be added to the *main* CorePlus routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by CorePlus during the DHCP address retrieval process.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *sfp1_net* and interface *sfp1*) to flow to the destination network *all-nets* and the destination interface *ge2*.

C. PPPoE setup

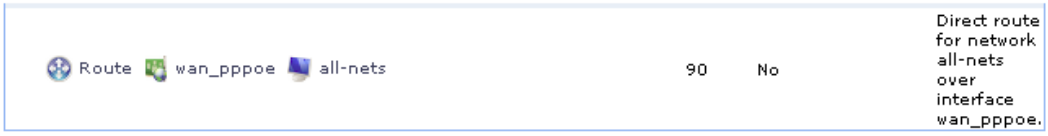
For PPPoE connection, we must create a PPPoE tunnel interface associated with the physical Ethernet interface. Assume that the physical interface is *ge2* and the PPPoE tunnel object created is called *wan_pppoe*. Go to **Interfaces > PPPoE** in the navigation tree and select **Add > PPPoE Tunnel**. These values can now be entered into the PPPoE Tunnel properties dialog.



Your ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. If we go to **Routing > Routing Tables > Main** in the navigation tree we can see this route.



If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *sfp1_net* and interface *sfp1*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel we have defined.

D. PPTP setup

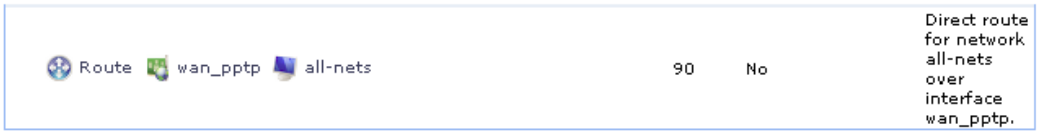
For PPTP connections, a PPTP client tunnel interface object needs to be created. Let us assume that the PPTP tunnel will be called *wan_pptp* with a a remote endpoint *10.5.4.1* which has been defined as the IP4 Address object *pptp_endpoint*. Go to **Interfaces > PPTP/L2TP Clients** in the navigation tree and select **Add > PPTP/L2TP Client**. The values can now be entered into the properties dialog and the *PPTP* option should be selected.

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by CorePlus looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

If we go to **Routing > Routing Tables > Main** in the navigation tree we can see this route.



If the PPTP tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source network and source interface (in this example, the network *sfp1_net* and interface *sfp1*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that we have defined.

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

First create an IP4 Address object which defines the address range to be handed out. Here, we will assume this is called *dhcp_range*. We will also assume that an IP4 Address object *dhcp_netmask* has been created which specifies the netmask.

We now create a DHCP server object called *dhcp_lan* which will only be available only on the interface. To do this, go to **System > DHCP > DHCP Servers** and select **Add > DHCP Server**. We can now specify the server properties.

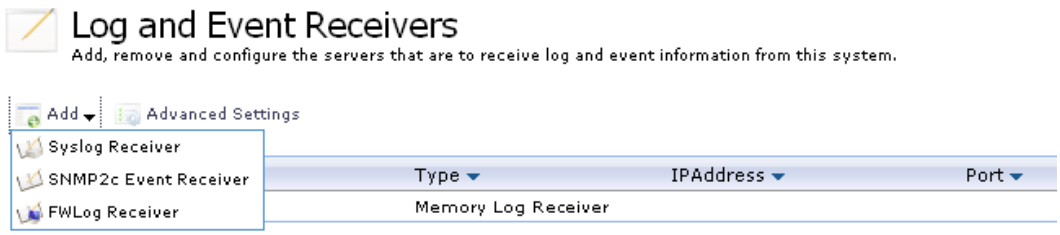
In addition it is important to specify the *Default gateway* for the server. This will be handed out to DHCP clients on the internal networks so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *sfp1_ip*

Also in the **Options** tab, we should specify the DNS address which is handed out with DHCP leases. This could be set, for example, to be the IP address object *dns1_address*.

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless at least one log server is set up to receive them and this is configured in CorePlus. *Syslog* is one of the most common server types.

First we create an IP4 Address object called, for example, *syslog_ip* which is set to the IP address of the server. We then configure the sending of log messages to a Syslog server from CorePlus by selecting **System > Log and Event Receivers** from the navigation tree and then choosing **Add > Syslog Receiver**.



The syslog server properties dialog will now appear. We give the server a name, for example *my_syslog*, and specify its IP address as the *syslog_ip* object.

Tip: Address book object naming

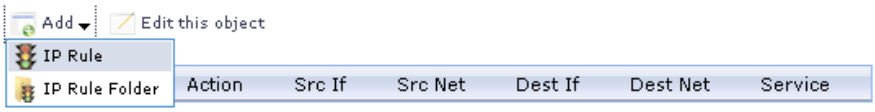
The CorePlus address book is organized alphabetically so when choosing names for IP address objects it is best to have the descriptive part of the name first. In this case, use ***syslog_ip*** *as the name and not* ***ip_syslog****.*

Allowing ICMP *Ping* Requests

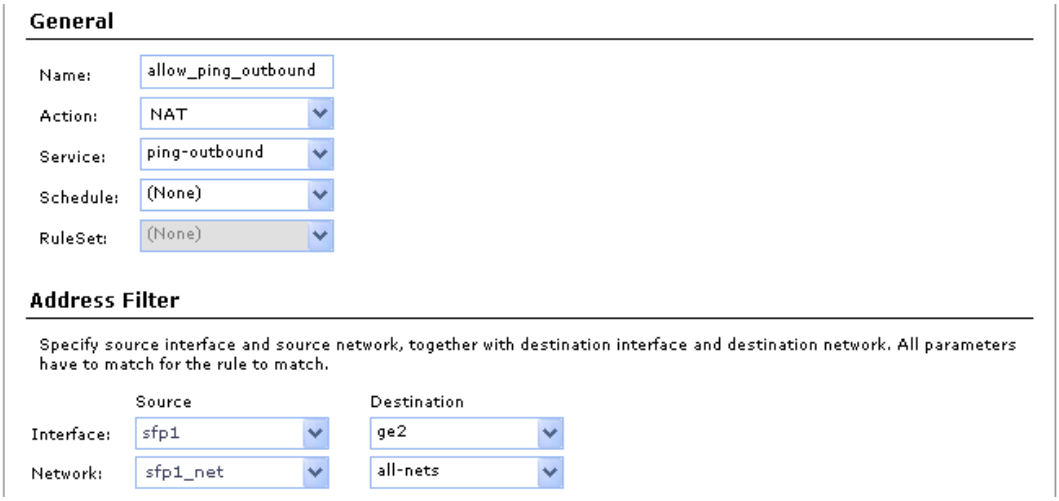
As a further example of setting up IP rules, it can be very useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the CorePlus will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *sfp1_net* network.

There can be several rule sets defined in CorePlus but there is only one rule set defined by default and this is called *main*. To add a rule to it, first select **Rules > IP Rule Sets > main** from the navigation tree.

The *main* rule set list contents are now displayed. Press the **Add** button and select **IP Rule**.



The properties for a new IP rule will appear and we can add a rule, in this case called *allow_ping_outbound*.



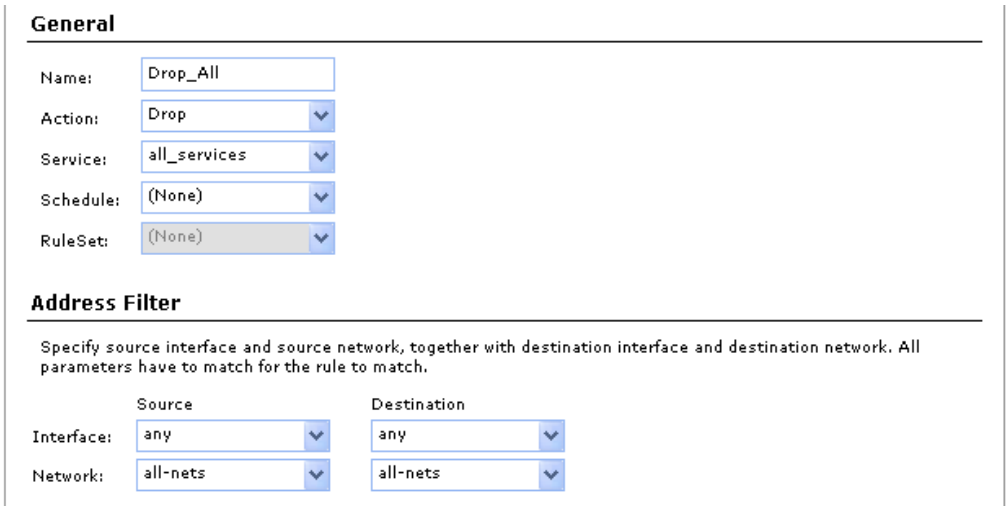
The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP repsonses to this single IP and CorePlus will then forward the response to the correct private IP address.

Adding a Drop All Rule

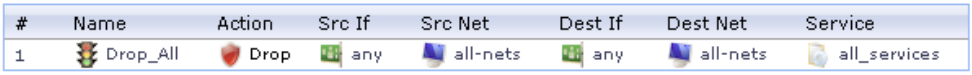
The top-down nature of the IP rule set scanning has already been discussed earlier. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

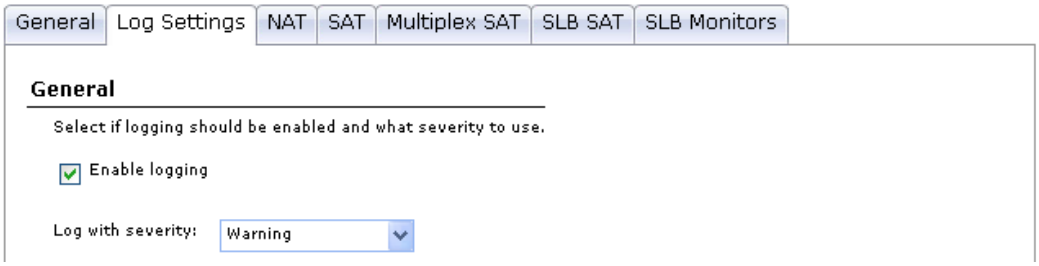
The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic.



If the this rule us the only one defined, displaying the *main* IP rule set will be as shown below.



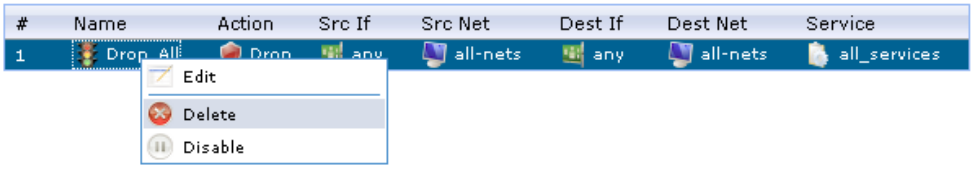
Logging can now be enabled on this rule with the desired severity. Click the **Log Settings** tab, and click the **Enable logging** box. All log messages generated by this rule will be given the selected severity and which will appear in the text of the log messages. It is up to the administrator to choose the severity and depends on how they would like to classify the messages.



Deleting Configuration Objects

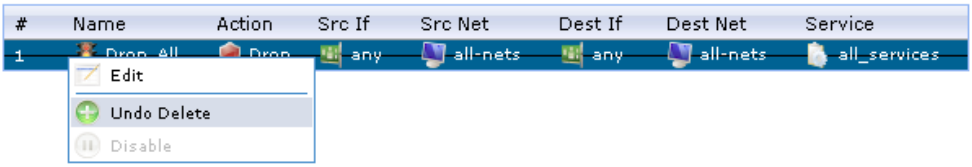
If information is deleted from a configuration during editing then these deletes are indicated by a line scored through the list entry while the configuration is still not yet activated. The deleted entry only disappears completely when the changes are activated.

For example, we can delete the drop all IP rule created in the previous paragraph by right clicking the rule and selecting *Delete* in the context menu.



The rule now appears with a line scored through it.

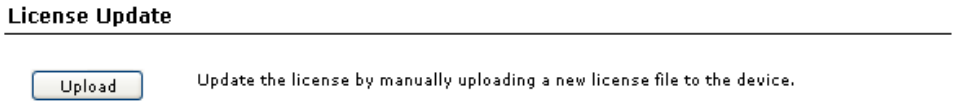
We can reverse the delete by right clicking the rule again and choosing *Undo Delete*.



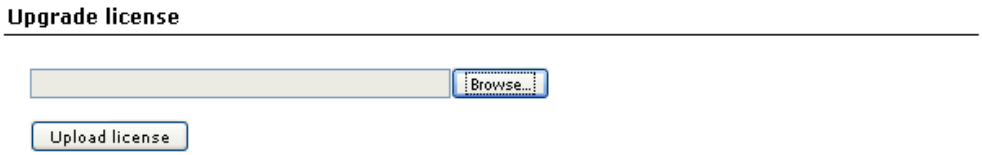
Uploading a License

Without a valid license loaded, CorePlus operates in *demonstration mode* which means it will cease operations after 2 hours from startup. To remove this restriction, a valid license must be uploaded to the Clavister Security Gateway.

To do this, download a license as described in the last part of *Section 4.2, "Web Interface and Wizard Setup"*. This license can then be uploaded directly to CorePlus by selecting the **License** option from the **Maintenance** menu and then pressing the **Upload** button.



Now press the **Browse** button to select the file from the load file system and then the **Upload License** button to send it to CorePlus.



As soon as upload of the license is complete, the 2 hour restriction will be removed and CorePlus will be restricted only by the restrictions of the license.

4.4. CLI Setup

This chapter describes the setup steps using CLI commands instead of the setup wizard.

The CLI is accessible in two ways:

- Across the local network at default IP address *192.168.1.1* using an SSH (Secure Shell) client. The network connection setup is the same as that described in *Section 4.2, "Web Interface and Wizard Setup"* as is the way the workstation interface's static IP address must be set up so it is on the same network as the Clavister Security Gateway's interface.

  If there is a problem with workstation connection, a help checklist can be found in *Section 4.5, "Troubleshooting Setup"*.

- Using a terminal or computer running a console emulator connected directly to the local RS-232 console port on the Clavister Security Gateway. Performing console port connection is described in the hardware installation manual for each Clavister hardware model.

The CLI commands listed below are grouped so that they mirror the options available in the setup wizard.

Confirming the Connection

Once connection is made to the CLI, pressing the **Enter** key will cause CorePlus to respond. The response will be a normal CLI prompt if connecting locally through the RS-232 console port and a username/password combination will not be required (a password for this console can be set later).

```
Device:/>
```

If connecting remotely through an SSH (Secure Shell) client, an administration username/password must first be entered and the initial default values for these are username *admin* and password *admin*. When these are accepted by CorePlus, a normal CLI prompt will appear and CLI commands can be entered.

Changing the Password

To change the administration username or password, use the *set* command to change the current CLI object category (sometimes refered to as the *object context*) to be the *LocalUserDatabase* called *AdminUsers*.

```
Device:/> cc LocalUserDatabase AdminUsers
Device:/AdminUsers>
```

Tip: Using tab completion with the CLI

The tab key can be pressed at any time so that CorePlus gives a list of possible options in a command.

Now set the username/password, which are case sensitive, to be the new chosen values for the user called *admin*. In the example below, we change to the username *new_name* and password *new_pass*.

```
Device:/AdminUsers> set User Admin Name=new_name Password=new_pass
```

The new username/password combination should be remembered and the password should be composed in a way which makes it difficult to guess. The next step is to return the CLI to the default top level of object categories.

```
Device:/AdminUsers> cc
Device:/>
```

Setting the Date and Time

Many CorePlus functions rely on an accurate date and time, so it is important that this is set correctly using the *time* command. A typical usage might be:

```
Device:/> time -set 2008-06-24 14:43:00
```

Notice that the date is entered in *yyyy-mm-dd* format and the time is stated in 24 hour *hh:mm:ss* format.

Ethernet Interfaces

The connection of external networks to the Clavister Security Gateway is via the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, CorePlus scans for these interfaces and determines which are available and allocates their names. The first interface detected in the scan always becomes the initial default management interface and this cannot be changed beforehand.

All CorePlus interfaces are logically equal for CorePlus and although their physical capabilities may be different, any interface can perform any logical function. With the SG6010 blade, the *ge1* interface is the default management interface. The other interfaces can be used as desired. For the sake of example, we will assume that the *ge2* interface will be used for connection to the public Internet and the *sfp1* interface will be used for connection to a protected, local network.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access with the CLI. The setup wizard described previously, provides the following four options:

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The individual manual steps to configure these connection alternatives with the CLI are discussed next.

A. Static - manual configuration

We first must set or create a number of IP address objects. It's assumed here that the interface used for Internet connection is *ge2*, the ISP gateway IP address is *10.5.4.1*, the IP address for the connecting interface will be *10.5.4.35* and the network to which they belong is *10.5.4.0/24*.

Note: Private IP addresses are used for example only

Each installation's IP addresses will be different from these IP addresses but they are used here only to illustrate how setup is done. Also, these addresses are private IP addresses and in reality an ISP would use public IP addresses instead.

We first add the gateway IP address object which we will call *wan_gw*:

```
Device:/> add Address IP4Address wan_gw Address=10.5.4.1
```

This is the address of the ISP's gateway which is the first router hop towards the public Internet. If this IP object already exists, it can be given the IP address with the command:

```
Device:/> set Address IP4Address wan_gw Address=10.5.4.1
```

Now use this object to set the gateway on the *ge2* interface which is connected to the ISP:

```
Device:/> set Interface Ethernet ge2 DefaultGateway=wan_gw
```

Next, set the IP object *ge2_ip* which will be the IP address of the interface connected to the ISP:

```
Device:/> set IP4Address InterfaceAddresses/ge2_ip
              Address=10.5.4.35
```

Note: Qualifiying the names of IP objects in folders

*On initial startup of the SG6010 blade, CorePlus automatically creates and fills the **InterfaceAddresses** folder in the CorePlus address book with the interface related IP address objects.*

*When we specify an IP address object which is located in a folder, we must qualify the object's name with the name of the folder. When we specify, for example, the address **ge2_ip** we must qualify it with the folder name **InterfaceAddresses** so the qualified name becomes **InterfaceAddresses/ge2_ip**.*

If an object is not contained in a folder and is at the top level of the address book then no qualifying folder name is needed.

Now set the IP object *ge2_net* which will be the IP network of the connecting interface:

```
Device:/> set IP4Address InterfaceAddresses/ge2_net
              Address=10.5.4.0/24
```

It is recommended to verify the properties of the *ge2* interface with the command:

```
Device:/> show Interface Ethernet ge2
```

The typical output from this will be similar to the following:

```
                  Property  Value
 -------------------------  -------------------------
                      Name:  ge2
                        IP:  InterfaceAddresses/ge2_ip
                   Network:  InterfaceAddresses/ge2_net
            DefaultGateway:  wan_gw
                 Broadcast:  10.5.4.255
                 PrivateIP:  <empty>
                     NOCHB:  <empty>
                       MTU:  1500
                    Metric:  100
               DHCPEnabled:  No
```

```
           EthernetDevice:  0:ge2  1:<empty>
         AutoSwitchRoute:  No
AutoInterfaceNetworkRoute:  Yes
  AutoDefaultGatewayRoute:  Yes
  ReceiveMulticastTraffic:  Auto
     MemberOfRoutingTable:  All
                 Comments:  <empty>
```

Setting the default gateway on the interface has the additional effect that CorePlus automatically creates a route in the default *main* routing table that has the network *all-nets* routed on the interface. This means that we do not need to explicitly create this route.

Even though an *all-nets* route is automatically added, no traffic can flow without the addition of an *IP rule* which explicitly allows traffic to flow. Let us assume we want to allow web surfing from the protected network *sfp1_net* on the interface *sfp1*. A simple rule to do this would have an *Action* of *Allow* and would be defined with the following commands.

Firstly, we must change the current CLI context to be the default *IPRuleSet* called *main* using the command:

```
Device:/> cc IPRuleSet main
```

Additional IP rulesets can be defined which is why we do this, with the rule set *main* existing by default. Notice that the CLI prompt changes to reflect the current context:

```
Device:/main>
```

Now add an IP rule called *lan_to_wan* to allows the traffic through to the public Internet:

```
Device:/main> add IPRule name=lan_to_wan
                Action=Allow SourceInterface=sfp1
                SourceNetwork=InterfaceAddresses/sfp1_net
                DestinationInterface=ge2
                DestinationNetwork=all-nets
                Service=http-all
```

This IP rule would be correct if the internal network hosts have public IP addresses but in most scenarios this will not be true and internal hosts will have private IP addresses. In that case, we must use NAT to send out traffic so that the apparent source IP address is the IP of the interface connected to the ISP. To do this we simply change the *Action* of the above command from *Allow* to *NAT*:

```
Device:/main> add IPRule name=lan_to_wan
                Action=NAT SourceInterface=sfp1
                SourceNetwork=InterfaceAddresses/sfp1_net
                DestinationInterface=ge2
                DestinationNetwork=all-nets
                Service=http-all
```

The service used in the IP rule is *http-all* which will allow most web surfing but does not include the DNS protocol to resolve URLs into IP addresses. To solve this problem, a custom service could be used in the above rule which combines *http-all* with the *dns-all* service. However, the recommended method which provides the most clarity to a configuration is to create a separate IP rule for DNS:

```
Device:/main> add IPRule name=lan_to_wan_dns
                Action=NAT SourceInterface=sfp1
                SourceNetwork=InterfaceAddresses/sfp1_net
                DestinationInterface=ge2
                DestinationNetwork=all-nets
                Service=dns-all
```

It is recommended that at least one DNS server is also defined in CorePlus. This DSN server or servers (a maximum of three can be configured) will be used when CorePlus itself needs to resolve URLs which is the case when a URL is specified in a configuration instead of an IP address. If we assume an IP address object called *dns1_address* has already been defined for the first DNS server, the command to specify the first DNS server is:

```
Device:/> set DNS DNSServer1=dns1_address
```

Assuming a second IP object called *dns2_address* has been defined, the second DNS server is specified with:

```
Device:/> set DNS DNSServer2=dns2_address
```

B. DHCP - automatic configuration

All required IP addresses can alternatively be automatically retrieved from the ISP's DHCP server by enabling DHCP on the interface connected to the ISP. If the interface on which DHCP is to be enabled is *ge2*, then the command is:

```
Device:/> set Interface Ethernet ge2 DHCPEnabled=Yes
```

Once the required IP addresses are retrieved with DHCP, CorePlus automatically sets the relevant address objects in the address book with this information.

For CorePlus to know on which interface to find the public Internet, a *route* has to be added to the *main* CorePlus routing table which specifies that the network *all-nets* can be found on the interface connected to the ISP and this route must also have the correct *Default Gateway* IP address specified. This *all-nets* route is added automatically by CorePlus during the DHCP address retrieval process. Automatic route generation is a setting for each interface that can be manually enabled and disabled.

After all IP addresses are set via DHCP and an *all-nets* route is added, the connection to the Internet is configured but no traffic can flow to or from the Internet since there is no IP rule defined that allows it. As was done in the previous option (**A**) above, we must therefore manually define an IP rule that will allow traffic from a designated source interface and source network. (in this example, the network *sfp1_net* and interface *sfp1*) to flow to the destination network *all-nets* and the destination interface *ge2*.

C. PPPoE setup

For PPPoE connection, create the PPPoE tunnel interface on the interface connected to the ISP. The interface *ge2*, is assumed to be connected to the ISP in the command shown below which creates a PPPoE tunnel object called *wan_ppoe*:

```
Device:/> add Interface PPPoETunnel wan_ppoe
                EthernetInterface=ge2 username=pppoe_username
                Password=pppoe_password Network=all-nets
```

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password*.

Your ISP will supply the correct values for *pppoe_username* and *pppoe_password* in the dialog above.

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be a route associated with the PPPoE tunnel to allow traffic to flow through it,

and this is automatically created in the *main* routing table when the tunnel is defined. If the PPPoE tunnel object is deleted, this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *sfp1_net* and interface *sfp1*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel that we have defined.

D. PPTP setup

For PPTP connection, first create the PPTP tunnel interface. It is assumed below that we will create a PPTP tunnel object called *wan_pptp* with the remote endpoint *10.5.4.1*:

```
Device:/> add Interface L2TPClient wan_pptp Network=all-nets
              username=pptp_username Password=pptp_password
              RemoteEndpoint=10.5.4.1 TunnelProtocol=PPTP
```

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint.

Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by CorePlus looking up the *Remote Endpoint* IP address in its routing tables.

The PPTP client tunnel interface can now be treated exactly like a physical interface by the policies defined in CorePlus rule sets.

There also has to be an associated route with the PPTP tunnel to allow traffic to flow through it, and this is automatically created in the *main* routing table when the tunnel is defined. The destination network for this route is the *Remote Network* specified for the tunnel and for the public Internet this should be *all-nets*.

As with all automatically added routes, if the PPTP tunnel object is deleted then this route is also automatically deleted.

At this point, no traffic can flow through the tunnel since there is no IP rule defined that allows it. As was done in option **A** above, we must define an IP rule that will allow traffic from a designated source interface and source network (in this example, the network *sfp1_net* and interface *sfp1* to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that we have defined.

Activating and Committing Changes

After any changes are made to a CorePlus configuration, they will be saved as a new configuration but will not yet be activated. To activate all the configuration changes made since the last activation of a new configuration, the following command must be issued:

```
Device:/> activate
```

Although the new configuration is now activated, it does not become permanently activated until the following command is issued within 30 seconds following the *activate*:

```
Device:/> commit
```

The reason for two commands is to prevent a configuration accidentally locking out the administrator. If a lock-out occurs then the second command will not be received and CorePlus will revert back to the original configuration after the 30 second time period (this time period is a

setting that can be changed).

DHCP Server Setup

If the Clavister Security Gateway is to act as a DHCP server then this can be set up in the following way:

First define an IP address object which has the address range that can be handed out. Here, we will use the IP range *192.168.1.10-192.168.1.20* as an example and this will be available on the *sfp1* interface which is connected to the protected internal network *sfp1_net*.

```
Device:/> add Address IP4Address dhcp_range
              Address=192.168.1.10-192.168.1.20
```

The DHCP server is then configured with this IP address object on the appropriate interface. In this case we will call the created DHCP server object *dhcp_lan* and assume the DHCP server will be available on the *sfp1* interface:

```
Device:/> add DHCPServer dhcp_lan IPAddressPool=dhcp_range
              Interface=sfp1 Netmask=255.255.255.0
              DefaultGateway=InterfaceAddresses/sfp1_ip
              DNS1=dns1_address
```

It is important to specify the *Default gateway* for the DHCP server since this will be handed out to DHCP clients on the internal network so that they know where to find the public Internet. The default gateway is always the IP address of the interface on which the DHCP server is configured. In this case, *sfp1_ip*.

NTP Server Setup

Network Time Protocol (NTP) servers can optionally be configured to maintain the accuracy of the system date and time. The command below sets up synchronization with the two NTP servers at hostname *pool.ntp.org* and IP address *10.5.4.76*:

```
Device:/> set DateTime TimeSyncEnable=Yes
              TimeSyncServer1=dns:pool.ntp.org
              TimeSyncServer2=10.5.4.76
```

The prefix *dns:* is added to the hostname to identify that it must resolved to an IP address by a DNS server (this is a convention used in the CLI with some commands).

Syslog Server Setup

Although logging may be enabled, no log messages are captured unless a server is set up to receive them and *Syslog* is the most common server type. If the Syslog server's address is *195.11.22.55* then the command to create a log receiver object called *my_syslog* which enables logging is:

```
Device:/> add LogReceiverSyslog my_syslog IPAddress=195.11.22.55
```

Allowing ICMP *Ping* Requests

As a further example of setting up IP rules, it can be useful to allow ICMP *Ping* requests to flow through the Clavister Security Gateway. As discussed earlier, the CorePlus will drop any traffic unless an IP rule explicitly allows it. Let us suppose that we wish to allow the pinging of external hosts with the ICMP protocol by computers on the internal *sfp1_net* network. The commands to allow this are as follows.

Firstly, we must change the current CLI context to be the *IPRuleSet* called *main* using the command:

```
Device:/> cc IPRuleSet main
```

Now add an IP rule called *allow_ping_outbound* to allow ICMP pings to pass:

```
Device:/main> add IPRule name=allow_ping_outbound
                Action=NAT SourceInterface=sfp1
                SourceNetwork=InterfaceAddresses/sfp1_net
                DestinationInterface=ge2
                DestinationNetwork=all-nets
                Service=ping-outbound
```

The IP rule again has the *NAT* action and this is necessary if the protected local hosts have private IP addresses. The ICMP requests will be sent out from the Clavister Security Gateway with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP repsonses to this single IP and CorePlus will then forward the response to the correct private IP address.

Adding a Drop All Rule

Scanning of the IP rule set is done in a top-down fashion. If **no** matching IP rule is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed and its action is to drop all such traffic as well as generate a log message for the drop.

In order to gain control over the logging of dropped traffic, it is recommended to create a drop all rule as the last rule in the *main* IP rule set. This rule has an *Action* of *Drop* with the source and destination network set to *all-nets* and the source and destination interface set to *any*.

The service for this rule must also be specified and this should be set to *all_services* in order to capture all types of traffic. The command for creating this rule is:

```
Device:/main> add IPRule name=drop_all
                Action=Drop SourceInterface=any
                SourceNetwork=any
                DestinationInterface=any
                DestinationNetwork=all-nets
                Service=all_services
```

Uploading a License

Without a valid license loaded, CorePlus operates in *demonstration mode* which means it will cease operations after 2 hours from startup. To remove this restriction, a valid license must be uploaded to the Clavister Security Gateway.

To do this, download a license as described in the last part of *Section 4.2, "Web Interface and Wizard Setup"*. This license can then be uploaded directly to CorePlus using a *Secure Copy* (SCP) client (see the CorePlus Administrators Guide for more details of using SCP). As soon as upload of the license is complete, the 2 hour restriction will be removed and CorePlus will be restricted only by the restrictions of the license.

4.5. Troubleshooting Setup

This appendix deals with connection problems that might occur when connecting a management workstation to a Clavister Security Gateway.

If the management interface does not respond after the Clavister Security Gateway has powered up and CorePlus has started, there are a number of simple steps to troubleshoot basic connection problems:

1. Check that the correct interface is being used.

The most obvious problem is that the wrong Clavister Security Gateway interface has been used for the initial connection. Only the first interface found by CorePlus is activated for the initial connection from a browser after CorePlus starts for the first time.

2. Check that interface characteristics match.

If a Clavister Security Gateway's interface characteristics are configured manually then the interface on a switch to which it is connected should be configured with the same characteristics. For instance, the link speeds and half/full duplex settings must match. If they do not, communication will fail. This problem will not occur if the interfaces are set for automatic configuration on both sides and automatic is always the Clavister factory default setting.

3. Check that the workstation IP is configured correctly.

The second most obvious problem is if the IP address of the workstation running the web browser is not configured correctly.

4. Is the management interface properly connected?

Check the link indicator lights on the management interface. If they are dark then there may be a cable problem.

5. Check the cable type connected to the management interface.

Is the management interface connected directly to the management workstation or another router or host? In this case, an Ethernet "cross-over" cable may be needed for the connection, depending on the capabilities of the interface.

6. Using the *ifstat* CLI command.

To investigate a connection problem further, connect a console to the RS-232 port on the Clavister Security Gateway after CorePlus starts. When you press the enter key, CorePlus should respond with the standard CLI prompt. Now enter the following command a number of times:

```
Device:/> ifstat <if-name>
```

Where *<if-name>* is the name of the management interface. This will display a number of counters for that interface. The *ifstat* command on its own can list the names of all the interfaces.

If the *Input* counters in the hardware section of the output are not increasing then the error is likely to be in the cabling. However, it may simply be that the packets are not getting to the Clavister Security Gateway in the first place. This can be confirmed with a packet sniffer if it is available.

If the *Input* counters are increasing, the management interface may not be attached to the correct physical network. There may also be a problem with the routing information in any connected hosts or routers.

7. Using the *arpsnoop* CLI command.

A final diagnostic test is to try using the console command:

```
Device:/> arpsnoop -all
```

This will show the *ARP* packets being received on the different interfaces and confirm that the correct cables are connected to the correct interfaces.

4.6. Going Further with CorePlus

After initial setup is complete, the administrator is ready to go further with configuring CorePlus to suit the requirements of a particular networking scenario. The reference documentation provided for this consists of the following manuals:

- The CorePlus Administrators Guide
- The CorePlus CLI Reference Guide
- The CorePlus Log Reference Guide

The CorePlus Administrators Guide

This guide is a comprehensive description of all CorePlus features and includes a detailed table of contents with a comprehensive index to quickly locate particular topics.

Examples of the setup for various scenarios are included but screenshots are kept to a minimum since the user has a variety of management interfaces to choose from.

Basic CorePlus Objects and Rules

At minimum, the new administrator should first aquaint themselves with the CorePlus *Address Book* for defining IP address objects and with the CorePlus *IP rule set* for defining IP rules which can allow or block traffic types and which are also used to set up NAT address translation.

IP rules also demonstrate the way *Security Policies* are set up in CorePlus by identifying the targeted traffic through combinations of the source/destination interface/network combined with protocol type. By default, no IP rules are defined so all traffic is dropped. At least one IP rule needs to be defined before traffic can traverse the Clavister Security Gateway.

In addition to IP rules, *routes* need to be defined so that traffic can be sent on the correct interface to reach its final destination.

ALGs

Once the address book and IP rules are understood, the various ALGs will probably be of interest for managing higher level protocols such as HTTP. For instance, for management of web surfing, the HTTP ALG provides a number of important features such as content filtering.

VPN Setup

A common requirement is to quickly setup VPN networks based on Clavister Security Gateways. The CorePlus Administrators Guide includes an extensive VPN section and as part of this, a *VPN Quick Start* section which goes through a checklist of setup steps for nearly all types of VPN scenarios.

Included with the quick start section is a checklist for troubleshooting and advice on how best to deal with the networking complications that can arise with certificates.

Log Messages

By default, certain events will generate log messages and at least one log server should be configured in CorePlus to capture these messages although a *memlog* feature is provided which

captures recent log messages in hardware memory. The administrator should review what events are important to them and at what severity. The *CorePlus Log Reference Guide* provides a complete listing of the log messages that CorePlus is capable of generating.

The CLI Reference Guide

The *CLI Reference Guide* provides a complete listing of the available CLI commands with their options. A CLI overview is also provided as part of the *CorePlus Administrators Guide*.

CorePlus Education Courses

For details about classroom and online CorePlus education as well as CorePlus certification, visit the Clavister company website at *http://www.clavister.com* or contact your local sales representative.

Staying Informed

Clavister maintains an RSS feed of announcements that can be subscribed to at *https://forums.clavister.com/rss-feeds/announcements/*. It is recommended to subscribe to this feed so that you receive notifications when new releases of CorePlus versions are available for download and installation. Alternatively, announcements can be read directly from the Clavister forums which can be found at *https://forums.clavister.com/*.

Appendix A: Specifications

General

- **Temperature (ambient)**

State	Value
Operating (with maximum one fan fault)	+5° C to +45° C
Short-term Operating (maximum 96 hours operation)	–5° C to +55° C 30° C/hr rate of change
Storage	–40° C to +70° C

- **Relative humidity**

State	Value
Operating	5% to 85% RH non-condensing
Short-term operating (no fan faults, maximum 96 hours operation)	5% to 90% RH non-condensing at +30° C
Storage	5% to 90% RH non-condensing at +40° C
Short-term storage	5% to 95% RH non-condensing at +40° C

- **Altitude**

  Operating:

  - Up to 5,905 feet (1,800 meters), +55°.
  - > 5,905 feet up to 13,123 feet (4,000 meters), derated linearly to +45° C.

- **Shock (drop)**

State	Value
Unpacked (free fall, corners & edges)	0 to < 10kg = 100 mm drop
Packaged, Unpalletized (free fall, corners & edges)	0 to < 10kg = 750 mm drop

- **Vibration**

  (In each direction for each of three mutually perpendicular axes.)

State	Value
Operating	0.1g, 5 to 100 Hz and back, 0.1 octave/min sine sweep
Transportation (packaged)	0.5g, 5 to 50 Hz and back, 0.1 octave/min sine sweep 3.0g, 50 to 500 Hz and back, 0.25 octave/min sine sweep

- **Seismic**

State	Value
Operating	Per Zone 4 test method, GR-63-CORE

Safety

The safety specifications are measured with ambient temperature approximately 25° C and relative humidity between 30% and 50%. Testing has been performed in partnership with a nationally recognized testing laboratory (NRTL) accredited to provide the required certifications.

Characteristic	Certification	Standard and test criteria
US	Accessory Listing	UL 60950-1 "Safety for Information Technology Equipment"
Canada	Approval	CSA 22.2 #60950-1 "Safety for Information Technology Equipment"
EU	Conformance with the Low Voltage Directive	EN 60950-1 "Safety for Information Technology Equipment"
Other	CB Report	IEC 60950-1 "Safety for Information Technology Equipment"

Dimensions and Weight

Characteristic	Value
Dimensions	322.25 x 280.0 mm +0/–0.3 mm (12.687 x 11.023 in +0.0/–0.012 in)
Board thickness	2.05 mm ±0.2 mm (0.0807 in ±0.008 in)
Board weight (includes 2 DIMMs + AMC)	2.95 kg

NEBS

The SG6010 is designed to meet the following Telcordia NEBS standards.

Standard	Description
GR-63-CORE	NEBS Requirements: Physical Protection
GR-1089-CORE	Electromagnetic Compatibility and Electrical Safety
SR-3580	Network Equipment – Building Systems (NEBS) Criteria Levels Level 3, indoor contaminants levels

Electromagnetic compatibility (EMC)

The ESD, EMC, and Immunity specifications are measured with ambient temperature between 20° C and 30° C and relative humidity between 30% and 50%.

- **Emissions**

Characteristic	State	Standard and criteria
Radiated emissions	Operating	FCC Part 15, Class B EN 300 386, Non-Telecom Centre
Conducted emissions	Operating	FCC Part 15, Class B EN 300 386, Non-Telecom Centre

- **Immunity**

Characteristic	State	Standard and criteria
ESD	Operating	EN 61000-4-2 8KV direct contact, performance criteria A 15KV air discharge, performance criteria A
Radiated	Operating	EN 61000-4-3 10 V/m, 10kHz – 10 GHz, 80% AM Performance Criteria A
Fast transient/Burst	Operating	EN 61000-4-4 0.5kV, 5/50 ns, 5kHz repetition frequency Performance criteria B
Surge voltages	Operating	EN 61000-4-5 Data ports: 1kV, 1.2/50 µs or 8/20 µs DC power port: 0.5kV, 1.2/50 µs or 8/20 µs Performance criteria B
Conducted	Operating	EN 61000-4-6 0.01–80 MHz ***Frequency (MHz) --- Min Calibration Current*** *0.01–0.27 --- 89 dBµA (rms)* *0.27–0.8 --- 77.6 dBµA - 20 log10 f* *0.8–30 --- 79.5 dBµA* *30–80 --- TBD* Performance criteria A
Magnetic field immunity	Operating	EN 61000-4-8 50 Hz / 1 A/m Performance criteria A

Mean Time Between Failures

The calculation results were generated using the references and assumptions listed. This specification and its associated calculations supersede all other released mean time between failures (MTBF) and failure in time (FIT) calculations with earlier dates. The reported failure rates do not represent catastrophic failure.

- Calculation Type: *MTBF/FIT rate*.
- Standard: *Telcordia Standard SR-332 Issue 2*.
- Methods: *Method I, Case I, Quality Level II*.

Reliability Estimate Data

Failure Rate (FIT)	6944 failures in 109 hours
MTBF	144,000 hours

Environmental Assumptions

- Failure rates are based on a 35°C ambient temperature.
- Applied component stress levels are 50% (voltage, current, and/or power).
- Ground, fixed, controlled environment with an environmental adjustment factor equal to 1.0.

General Assumptions

- Component failure rates are constant.
- Board-to-system interconnects are included within estimates.
- Non-electrical components (screws, mechanical latches, labels, covers, etc.) are not included in estimates.

General Notes

- Method I, Case I = Based on parts count. Equipment failure is estimated by totaling device failures rates and quantities used.
- Quality Level II = Devices purchased to specifications, qualified devices, vendor lot-to-lot controls for AQLs and DPMs.

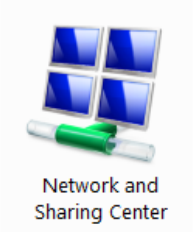
Where available, direct component supplier predictions or actual FIT rates have been used.

Appendix B: Vista IP Setup

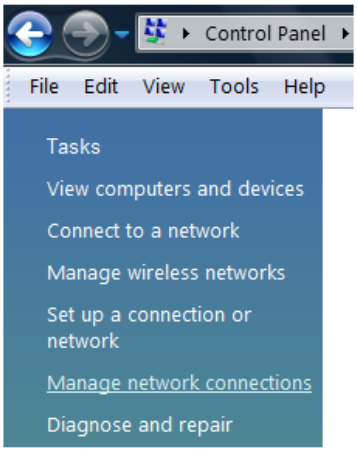
If a PC running Microsoft Vista is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address of *192.168.1.1*.

The IP address *192.168.1.30* will be used for this purpose and the steps to set this up with Vista are as follows:

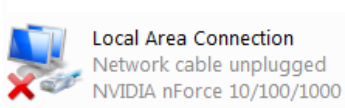
1. Press the Windows **Start** button.
2. Select the **Control Panel** from the start menu.
3. Select **Network & Sharing Center** from the control panel.



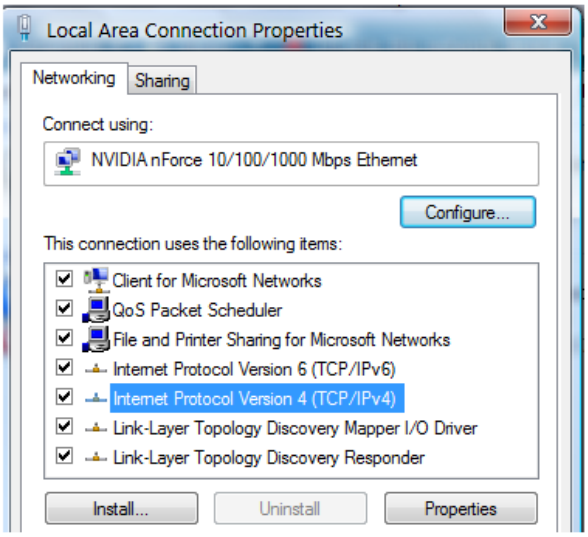
4. Select the **Manage network connections** option.



5. A list of the Ethernet interface connections will appear. Select the interface that will connect to the security gateway.



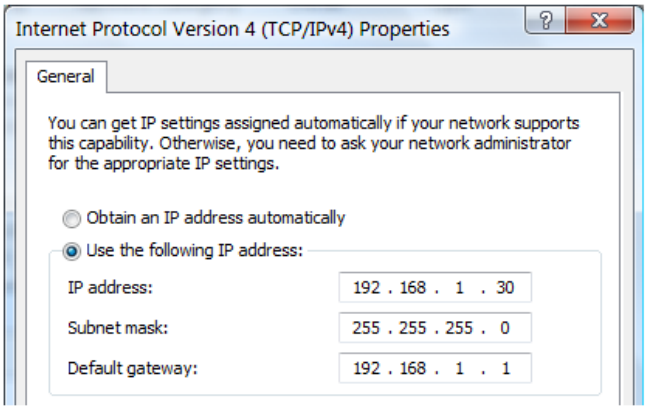
6. The properties for the selected interface will appear.



Select and display the properties for *Internet Protocol Version 4 (TCP/IPv4)*.

7. In the properties dialog, select the option **Use the following IP address** and enter the following values:

   - **IP Address:** *192.168.1.30*
   - **Subnet mask:** *255.255.255.0*
   - **Default gateway:** *192.168.1.1*



DNS addresses can be entered later once Internet access is established.

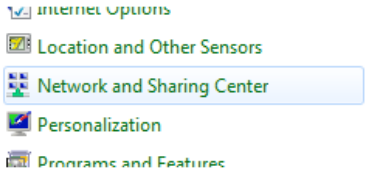
8. Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

Appendix C: Windows 7 IP Setup

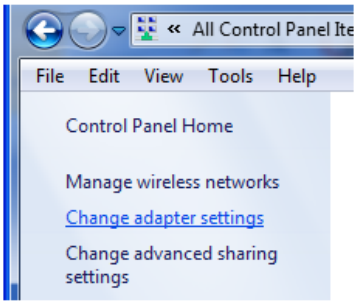
If a PC running Microsoft Windows 7 is being used as the CorePlus management workstation, the computer's Ethernet interface connected to the Clavister Security Gateway must be configured with an IP address which belongs to the network *192.168.1.0/24* and is different from the security gateway's address of *192.168.1.1*.

The IP address *192.168.1.30* will be used for this purpose and the steps to set this up with Windows 7 are as follows:

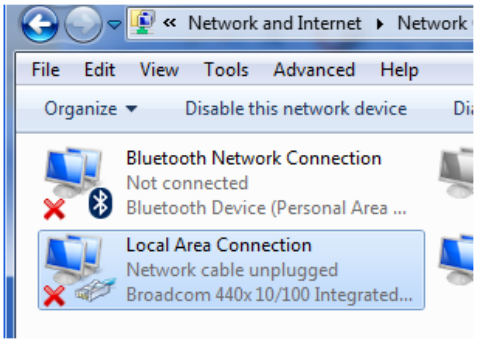
1. Press the Windows **Start** button.
2. Select the **Control Panel** from the start menu.
3. Select **Network & Sharing Center** from the control panel.



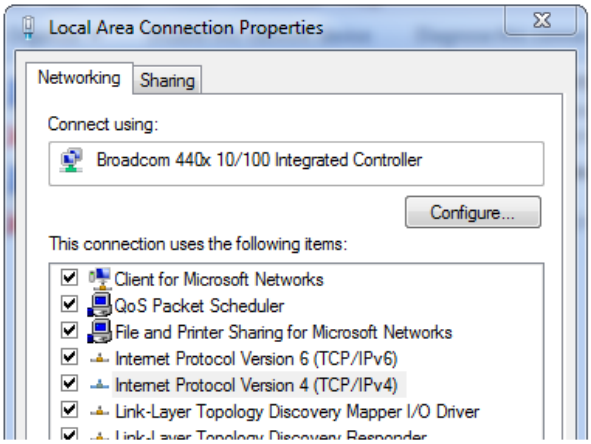
4. Select the **Change adapter settings** option.



5. A list of adapters will appear and will include the Ethernet interfaces. Select the interface that will connect to the security gateway.



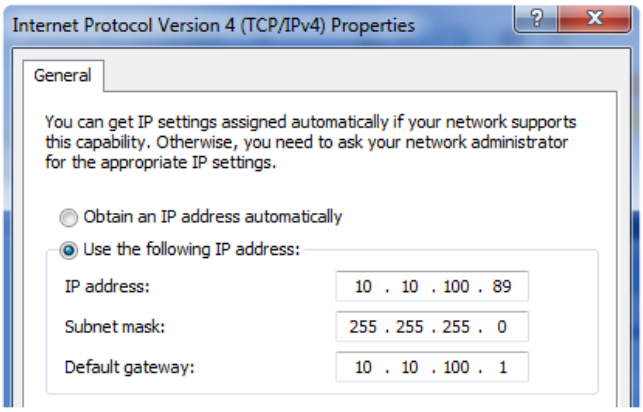
6. The properties for the selected interface will appear.



Select and display the properties for *Internet Protocol Version 4 (TCP/IPv4)*.

7. In the properties dialog, select the option **Use the following IP address** and enter the following values:

   - **IP Address:** *192.168.1.30*
   - **Subnet mask:** *255.255.255.0*
   - **Default gateway:** *192.168.1.1*



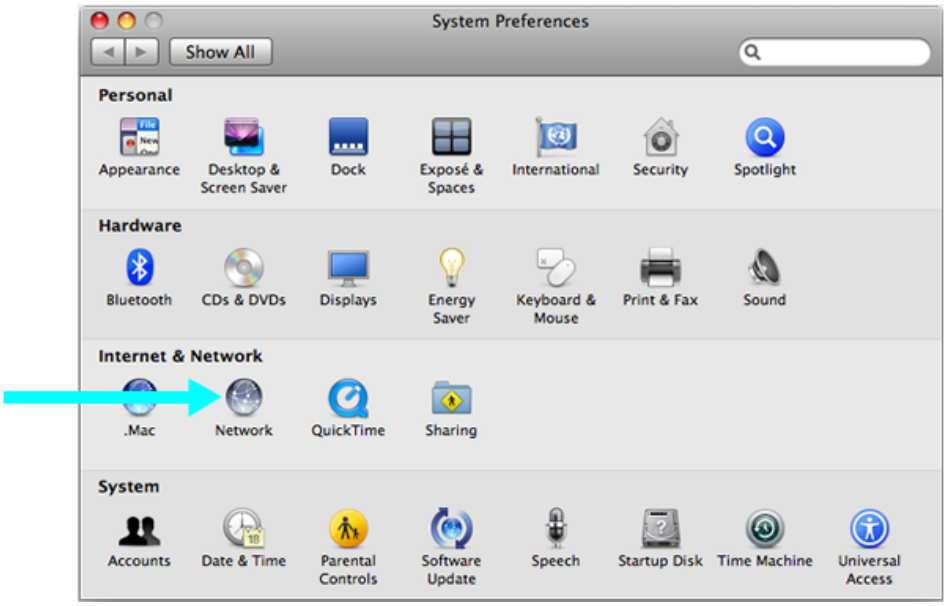
DNS addresses can be entered later once Internet access is established.

8. Click **OK** to close this dialog and close all the other dialogs opened since step **(1)**.

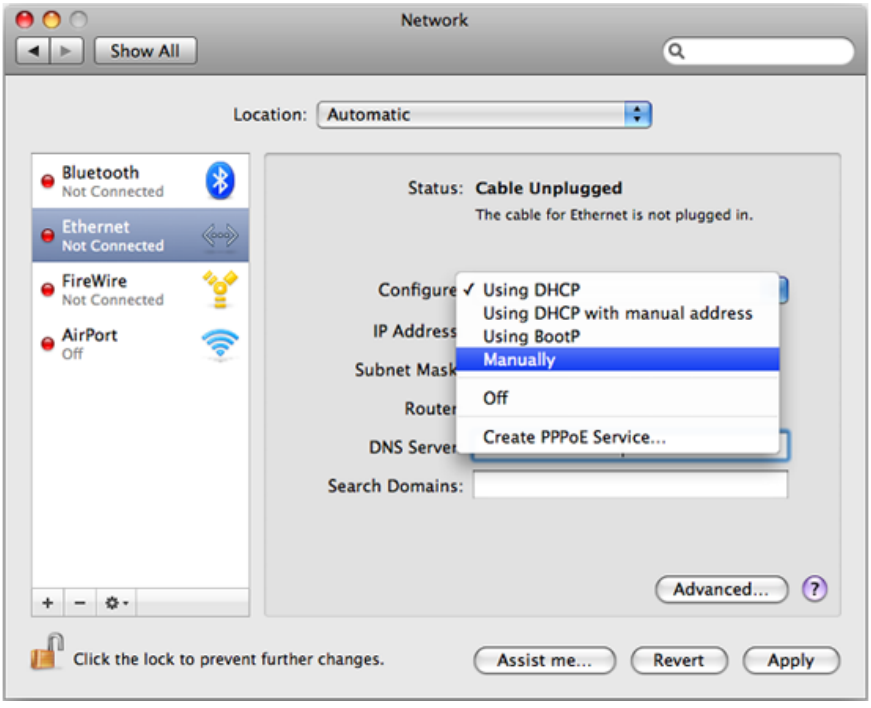
Appendix D: Apple Mac IP Setup

An Apple Mac can be used as the management workstation for initial setup of a Clavister Security Gateway. To do this, a selected Ethernet interface on the Mac must be configured correctly with a static IP. The setup steps for this with Mac OS X are:

1. Go to the **Apple Menu** and select **System Preferences**.
2. Click on **Network**.

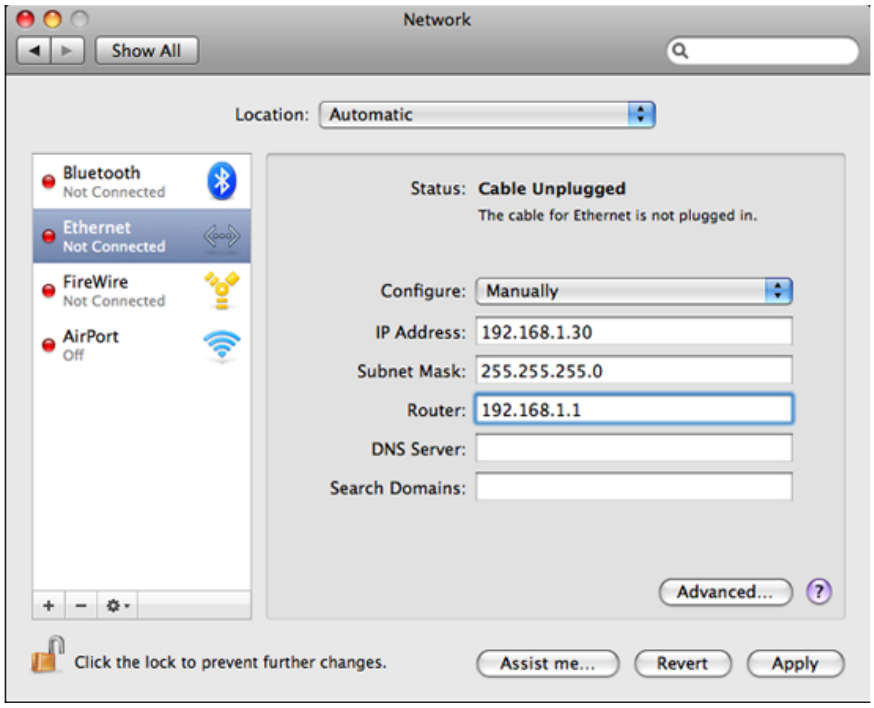


3. Select **Ethernet** from the left sidebar menu.
4. Select **Manually** in the **Configure** pull down menu.



5. Now set the following values:

   - **IP Address:** *192.168.1.30*
   - **Subnet Mask:** *255.255.255.0*
   - **Router:** *192.168.1.1*



6. Click **Apply** to complete the static IP setup.

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com