Com.X Router/Firewall Module

Use Cases

White Paper

Version 1.0, 21 May 2014

Document History

Version	Date	Description of Changes
1.0	2014/05/21	Preliminary

Table of Contents

1 Introduction

This document aims to highlight the usefulness of the router and firewall module included on 1.3 Com.X PBX and gateway devices. A few scenarios are described, with a detailed explanation of configurations that cover common usage patterns.

2 Networking Ports

Each Com.X device contains a variety of virtual and physical network ports. Configuration of all ethernet LAN, WAN, X.21 and PPP ports is possible through the Network tab of the Comma GUI. This module allows further control of router and firewall settings, including configurations of zones on a port-by-port basis, general firewall policies, and individual rules, providing exceptions to the configured policies.

Any port that is connected to the internet and thereby has a public IP address, is termed a WAN port. When any network port of the Com.X is connected in this way, it must be configured as a WAN port with firewall enabled to protect the Com.X and the local network from external attacks.Usually, the WAN connection will be a PPP connection.

2.1 Configuring PPP0 for ADSL

PPP connections from the Com.X are available through a variety of interfaces. Some Com.X models are equipped with an internal DSL router, and all Com.X units can connect to a LAN based DSL router in bridge mode to obtain PPP connections to a service provider.

Regardless of the physical port used to make a connection to your provider, configuration of the authentication credentials to authenticate with your internet service provider, is controlled through port PPP0 on the Com.X.

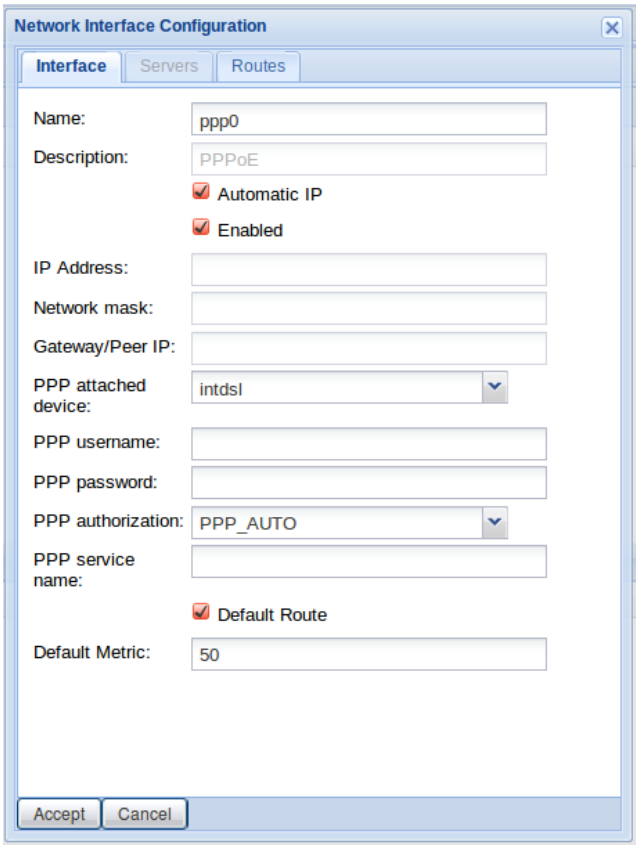

Figure 1: Configuring ISP authentication credentials on port PPP0.

Field	Description
Name	Select a suitable name for the PPP port.
Automatic IP	If enabled, the interface will attempt to dynamically receive an IP address via IPCP. If left unchecked, a static IP address can be configured.
Enabled	Enabled by default. Disabling will prevent any transmission or reception of traffic over this interface.
IP Address	If Automatic IP is disabled, a static IP address can be configured in this field. If Automatic IP is enabled then this field can not be edited from the Gui.
Network Mask	The network mask to use on the network. Auto-assigned if DHCP Client is enabled.
Gateway/Peer IP	The IP address of the bridge mode router handling PPPoE traffic. This could be an internal router (on select Com.X units) or another router on the local network.
PPP attached device	The port through which the router can be reached. This could be a LAN port on the Com.X or the internal DSL router on select Com.X units.
PPP username	The username of with which to authenticate with your service provider.
PPP password	The password associated with your username, used to authenticate with your service provider.
PPP authorization	The authorization method used to authenticate your account with your service provider.
PPP Service name	This field should be left blank, unless your service provider has requested that your configure your service with a specific name.
Default Route	If enabled, the PPPoE interface will be configured as the default route for any IP traffic to an address matching no other configured route.
Default Metric	The metric of a network route is a property used by a routing protocol to determine whether one particular route should be chosen over another. In conflicting cases, traffic will be directed towards the gateway containing the lowest value metric.

Table 1: PPP0 port configuration options.

3 Firewall module

As of release 1.3 Far South Networks Com.X and gateway devices ship with a fully-featured, sip-aware, NAT capable, firewall module, which can be used to secure a system with an internet-facing WAN interface (say a dedicated voice network connection) or even to act as the main firewall for an entire network, with the Com.X acting as firewall and router.

If the onboard firewall option oin your Com.X is enabled, then the Com.X device can manage firewall services on your network.

The firewall module is fully NAT capible, so it is seamlessly able to represent several devices behind a single public IP address and distribute returning network traffic to the correct device.

SIP-awareness means that no special firewall configuration is required to allow SIP connections. The firewall is able to detect source and destination details from outgoing SIP connections and keep open a pinhole for return communications, with no threat of refused packets or one way audio.

A complete set of default firewall policies is available on each Com.X which, upon restoration, will prevent any inbound access at all on internet facing ports, but allow for outbound traffic, including SIP.

3.1 Firewall zones

For ease of configuration and management, networking ports on Com.X devices are arranged into groupings or zones, each of which is authorised to access different portions on the network.

Zone	Access
Com.X	The Com.X zone represents the Com.X PBX itself, including SIP, ssh, http and other services. By default, the Com.X zone is accessible from the LAN and DMZ, but not from the Internet.
LAN	Interfaces placed in the LAN zone are protected from any inbound access from the internet, unless specific rules override this behaviour.
DMZ	The De-Militarized Zone has access both to the internet and a limited partition of the internal network. Interfaces in this zone are typically used to connect to servers or gateways that require both internet and LAN connectivity.
Internet	The Internet zone represents interfaces that are exposed to the internet. It is accessible from all other zones for outbound connections, but has no access to LAN or Com.X zones for inbound.

Table 2: Firewall zones and typical access permissions.

The zone association of any interface can be altered, through the Network page of the Com.X GUI. Typically, one interface will be in the Internet zone, and the others in the LAN zone.

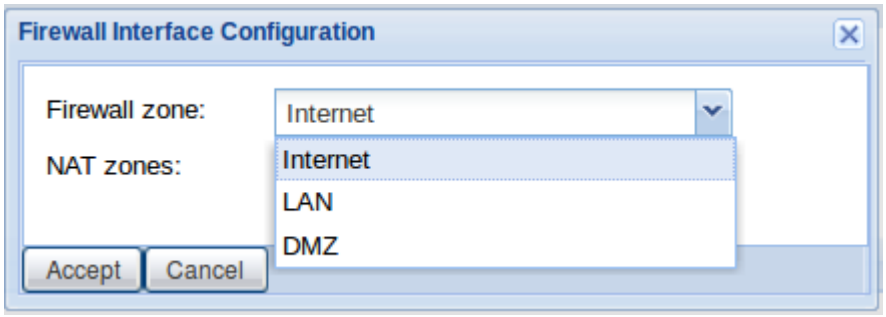

Figure 2: the firewall zone association of each interface is easily editted.

3.2 Firewall Policies

Firewall policies are used to manage the access allowed to devices in each firewall zone. Policies are explicitly defined to provide a standard method of dealing with network traffic moving from one zone to another.

A policy can be configured to respond to traffic in the three ways described in Table 3.

Policy	Action
Accept	Allow traffic between the two zones.
Drop	Ignore any packets travelling from the source zone to the destination zone.
Reject	Reject any packets sent from the source zone to the destination zone with a rejection message.

Table 3: Firewall Policy response options for handling traffic.

3.2.1 Default policies

A comprehensive set of default firewall policies is included on the Com.X.

The default policies provide a secure conifiguration to which rules can be added to accomodate special cases.

To enable the firewall default policies, navigate to the firewall section of the Network section of the GUI and select Options, Load Defaults.

Under normal circumstances, these policies should be left at defaults.

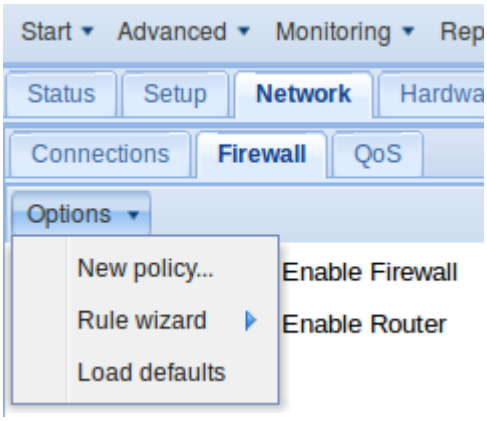

Figure 3: Accessing the default firewall policies.

Default Policies are shown in Table 4 below

Source Zone	Destination Zone	Action
Com.X	Internet	Accept
Com.X	LAN	Accept
Com.X	DMZ	Accept
LAN	Com.X	Accept
LAN	Internet	Accept
LAN	DMZ	Accept
DMZ	Com.X	Accept
DMZ	Internet	Accept
DMZ	LAN	Drop
Internet	All Zones	Drop
All Zones	All Zones	Reject

Table 4: Com.X Firewall default policies.

Note: The default policies automatically determine which of your interfaces is the default interface facing the internet. If the system has more than one internet-facing networking port, manually allocate it to the internet zone to avoid unwanted connections.

3.2.2 Rules

On the firewall, rules may be created to override the default policies – i.e. rules are specific cases where the policy does not apply. The section below illustrates the use of firewall rules.

3.3 Simple Firewall Use Cases

This section will highlight a few simple scenarios in which the Com.X firewalll can be utilized to simplify management of the unit and examine potentially useful rules and configurations in each case.

3.3.1 Dedicated VOIP Line via 3G, adsl or X21

One typical scenario involves a Com.X device residing on your local network, behind an independent firewall device and DHCP server. The Com.X receives an IP address from the DHCP server on one of it's LAN ports. In this scenario, the Com.X is protected by the external firewall.

For the sake of this scenario, let's assume there is a dedicated ADSL internet connection for SIP trunking. This connection makes use of either an internal or external DSL modem in bridge mode, making use of the Com.X's PPPoE network port, PPP0.

Note: If any interfaces have a direct internet connection, it is very important that the firewall on the Com.X is running, and that, at the very least, the default policies are active. Default policies will protect a Com.X from any inbound connections from interfaces configured to be in the Internet zone.

Now, with a few simple firewall rules, is possible to securely configure a variety of access points to the Com.X and to the network, which could prove extremely useful while managing and maintaining the unit.

3.3.1.1 Com.X GUI access

GUI access is facilitated via HTTP on the default HTTP port, 80. A rule should be configured to allow access at port 80. This can be done using two methods:

3.3.1.1.1 Inbound Access route

An inbound access route allows traffic in at port 80 of your public IP address, which is also port 80 of your Com.X. This means that if your public IP address is accessed from a web browser, the GUI will be available. Of course, it is possible to limit this access to allow only devices within a specific IP address or subnet range access on port 80.

To configure an inbound access route, select Options and then Rule Wizard from the firewall page of the Com.X GUI. Choose an Inbound Access route.

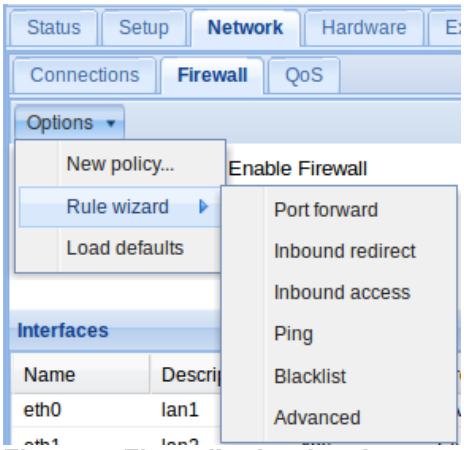

Figure 4: Firewall rule wizard.

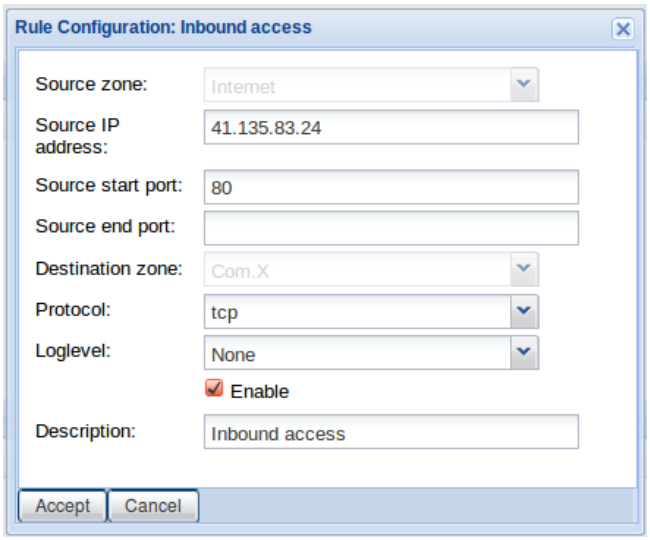

Figure 5: Inbound Access rule configuration.

In Figure 5, only the required fields have been populated. The Source zone for inbound access will always be “Internet” and so this field is populated by default, and read-only.

The rule configured above will allow access on port 80 of the public IP address of the Com.X PPP0 interface (and any interface set to be in the “Internet” zone) to IP address 41.135.83.24.

Field	Contents
Source IP Address	This IP address or range of IP addresses limits which machines on the internet can make use of the rule. In this case, only devices with the public IP of 41.135.83.24 will be permitted access on port 80. If this field is left blank, any device will be granted access on port 80.
Source Start Port	The port to open for inbound access.
Protocol	The transport protocol to be used on this route. (Select between TCP ad UDP)
Log Level	Optional log level in system log for connections
Description	A unique name or description to aid in identifying this route.

Table 5: Inbound access configuration fields.

3.3.1.1.2 Inbound Redirect

As port 80 is the deafult port for Http access, it may be a security concern to leave this port open to the public. A simple way of making use of a non default port would be to configure an Inbound Redirect route.

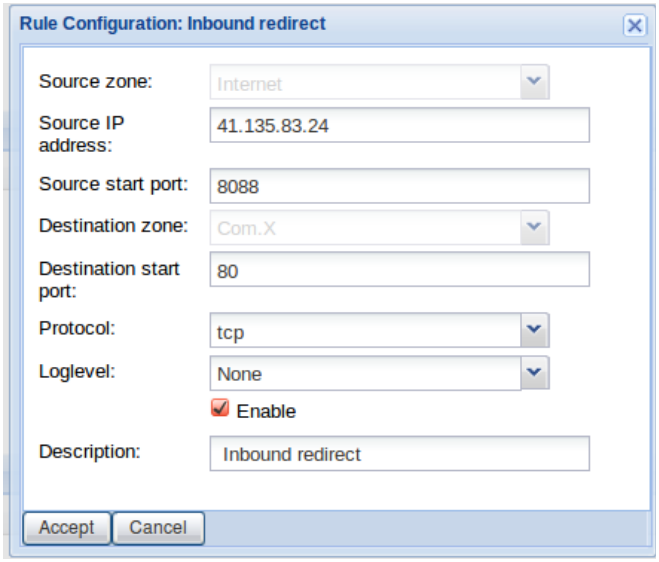

Figure 6: Inbound Redirect Route.

The inbound redirect route configured in Figure 6 is similar to the inbound access route configured above, except that instead of opening port 80 on the public IP of the Com.X, a different port is chosen (in this case 8088) and configured to redirect to port 80.

The configuration above would allow inbound access to port 80 of the Com.X to any device on 41.135.83.24 that tries to access port 8088 of the public IP address of the Com.X.

Note: If a permanent rule exists to allow GUI access, then any other access can be configured only when necessary. A route that is not used frequently can be configured in minutes, used to complete the task at hand, and then deleted or set to the diabled state.

3.3.1.2 Com.X SSH terminal access

Ssh terminal access is provided on port 22 by default. As such, access to port 22 needs to be configured through the firewall.

This too can be done with an inbound access rule or an inbound redirect rule.

3.3.1.2.1 Inbound Access

An inbound access route like that configured in Figure 7 allows any device on the IP 41.135.83.24 to access the Com.X on port 22. Since ssh access defaults to port 22, a user would not need to include a port in the “ssh comma@<com.X-IP>” command.

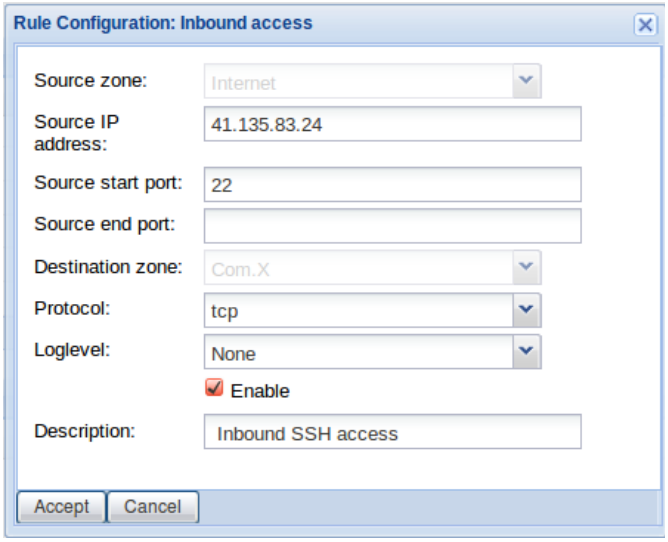

Figure 7: Inbound access for ssh.

3.3.1.2.2 Inbound redirect

An inbound redirect route would be more suitable, as it makes use of a non-default port, which just adds one level of complexity for anyone attempting to gain unauthorized access.

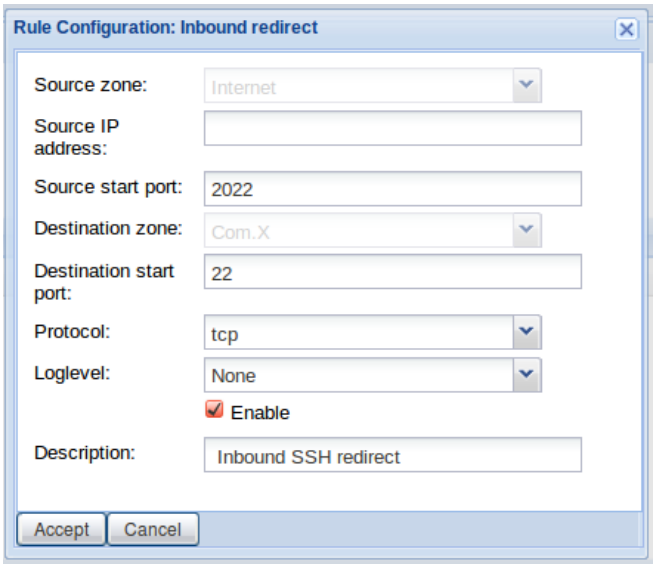

Figure 8: Inbound redirect rule for ssh access.

Figure 8 shows an inbound route that will accept traffic at port 2022 of the Com.X's public IP and redirect that to port 22 or the Com.X.

This means that anyone attempting to access the route will need both the public IP address of the Com.X as well as the port number for ssh access. A command like:

“ssh -p2022 comma@<Com.X-IP>” is required to access the unit. Attempts to access port 22 directly will fail.

3.4 Blacklisting an IP address

It may be necesarry to block all traffic from a particular IP address. To do this, from the Firewall page , select Options, Rule Wizard, Blacklist.

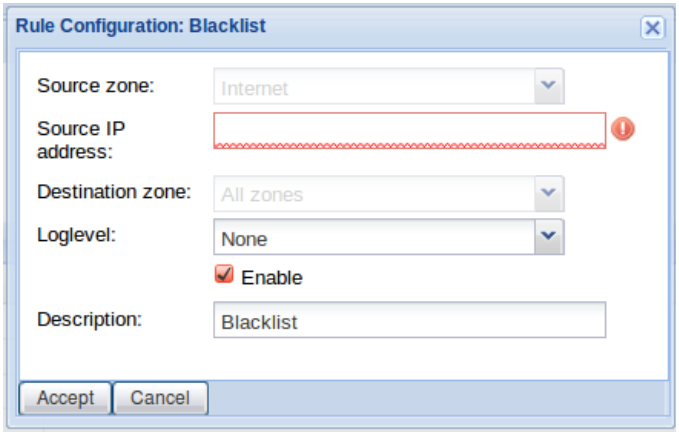

Figure 9: Blacklist Firewall rule configuration

Entering a source IP address will result in all traffic from the IP address being dropped.

3.5 Com.X as an Edge Device

This type of scenario entails the Com.X connecting to the external internet and devices on the local network of the site/company all connect to the internet through the Com.X.

In such a case, SIP trunking and data from the company LAN share the WAN interface of the Com.X.Since other hardware sits behind the Com.X, it will be necessary to create rules to allow traffic to certain ports on certain devices.

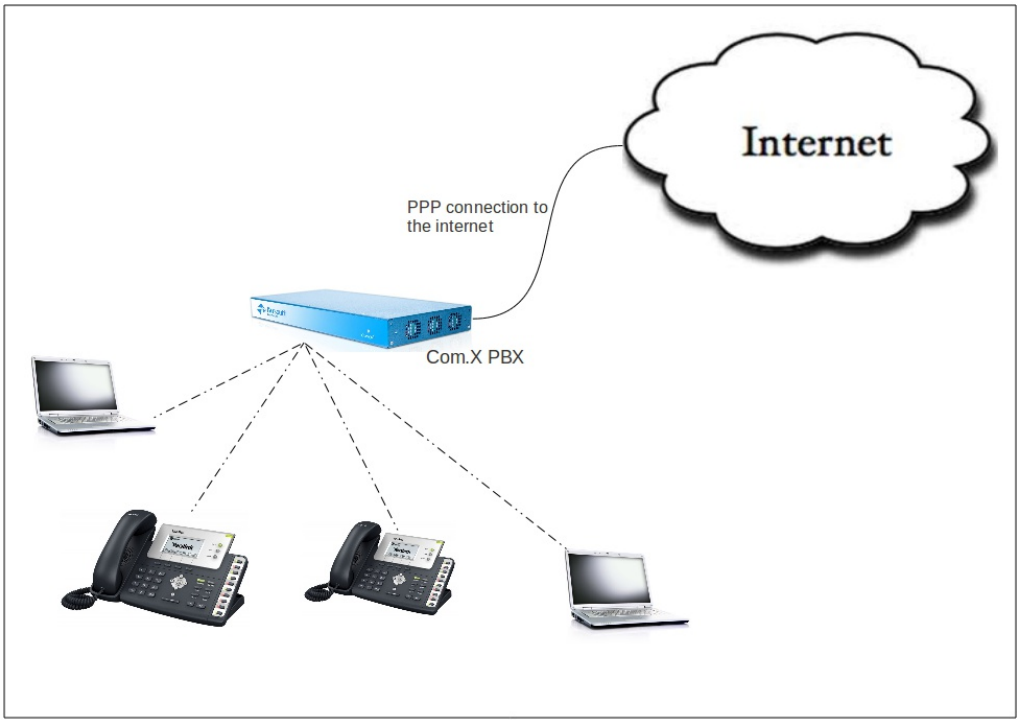

Figure 10: The Com.X acts as an edge router

3.5.1 Hosting generic devices on a static IP address

A Com.X acting an edge router will be providing internet access to a range of devices, on a range of subnetworks. Some of these devices, such as SIP handsets, will likely receive DHCP addresses from an interface on the Com.X, much like in the previous scenario, however, some devices, such as the computers of users, will require static IP addresses, to remove the risk of a device being served a different IP address from time to time, which would result in any firewall rules to the old IP address failing.

First, select a LAN interface on the Com.X, through which you will access devices on the local network. Assigning a static IP address to a hardware device is as simple as accessing the device and manually setting it's IP address to a suitable static IP address, this static IP address should be on the same subnetwork as the selected interface on the Com.X, and the LAN port of the Com.X should be entered as the gateway for this device. This will allow the device to access the external internet through the Com.X.

Note: The Com.X LAN interface that acts as a gateway for the static IP address subnet can also be configured to act as a DHCP server, to serve devices for which IP addresses need not be static. However, the DHCP server range should exclude

the range of IP addresses reserved for static IP addresses.

3.5.1.1 Adding a device as hardware

Adding a device to the hardware list of the Com.X GUI allows http access to the device directly through the Com.X GUI, without the need to create a firewall rule. The Com.X GUI is able to securely forward the GUI port of the device.

To add a device as hardware, navigate to the Hardware panel of the Com.X GUI and select Options, New.

Devices available include Managed SIP Handsets manufactured by Yealink, Snom and Polycom, as well as Far South Networks iTA devices and generic devices.

Managed SIP phones and ITA devices will allow configuration directly from the Com.X GUI, whereas hardware added as a generic device will allow for HTTP proxy connection through the Com.X GUI.

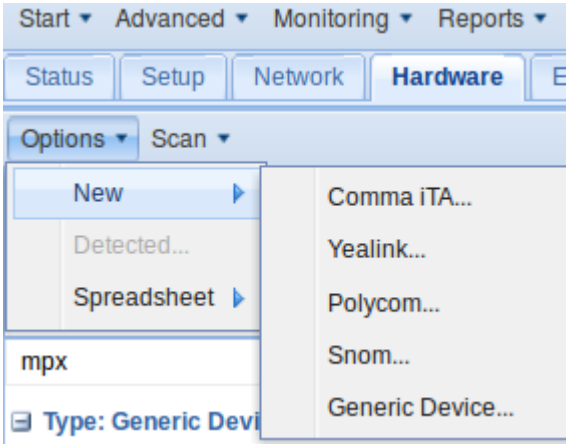

Figure 11: Add a new device as hardware.

To add a generic device with a static IP address, provide a suitable name for the device, uncheck the auto-IP check box, and manually enter the MAC address, configured IP address and the attached network fields.

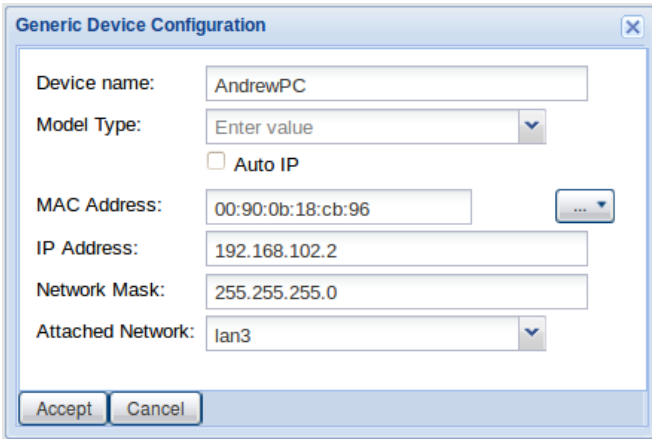

Figure 12: Adding hardware as a generic device. `

Access to the HTTP interface of a generic device is obtained by right-clicking on the desired device, and selecting “Connect” - the Comma GUI will open the device's HTTP portal in a window.

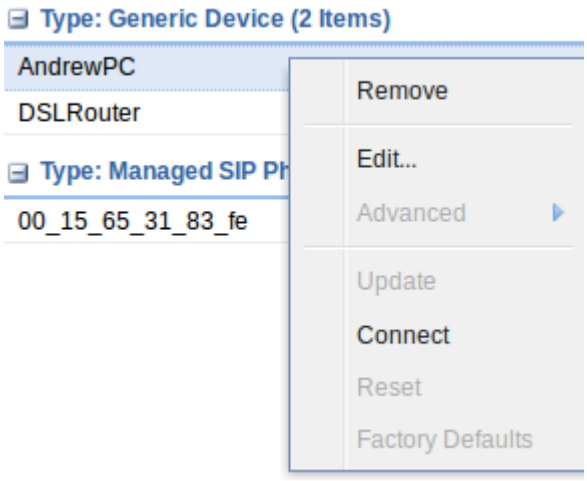

Figure 13: Select "Connect" to access the GUI of this device.

3.5.2 Hosting Virtual networks

The networking module supports the creation and configuration of virtual VLAN interfaces. A VLAN interface allows for the same configuration options as the ports eth0 -eth4 on the Com.X, including the ability to act as a DHCP server.

A VLAN port could be utilized to partition an array of devices, that share the network infrastructure with the rest of the network, but reside on a different subnetwork.

3.5.3 Network Address Translation

The Com.X firewall module is capable of Network address translation (NAT) to facilitate the routing of traffic between local network devices and the internet. Typically, a device behind the Com.X will send data through the Com.X router to the internet. As the packets pass through the firewall, they are translated so that the source is a port on the public IP address of the Com.X. The firewall then makes a note of the port and leaves it open for return traffic, closing the port after a particular threshold period of time has past. This enables the Com.X to seamlessly route traffic from local devices in the LAN zone, to the internet, and then distribute the returning traffic to the appropriate device, with no security risk.

3.5.4 Accessing devices behind the Com.X

In many cases, a Com.X is configured to host devices, such as SIP handsets on a DHCP server running on a LAN port. Further devices on static IP addresses may also reside behind the Com.X, and make use of it as an edge router. The Com.X firewall can be configured to allow access to to any port of any device residing behind it.

For the sake of this paper, let's assume that the port Lan3 (or eth2) on the Com.X acts as a DHCP server, serving IP addresses to several SIP handsets.

The port itself has an IP address of 192.168.103.1 and the DHCP server configuration should look something like in Figure 14. Note that the LAN port is acting as the router for all devices receiving DHCP from this server.

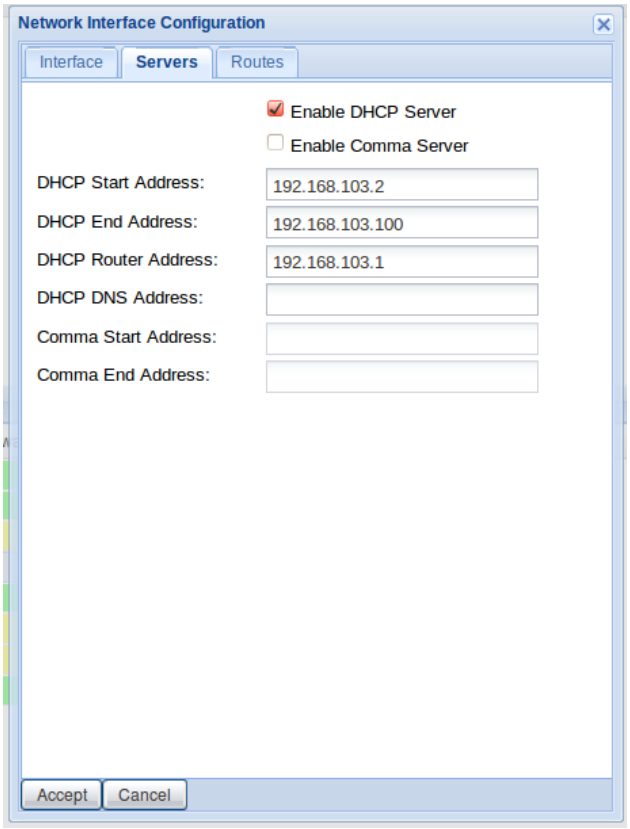

Figure 14: LAN port DHCP server configuration.

Now, for example sake, say there is a SIP handset on this subnet, with the IP address 192.168.103.2. Access to this device can be configured using a port forward rule.

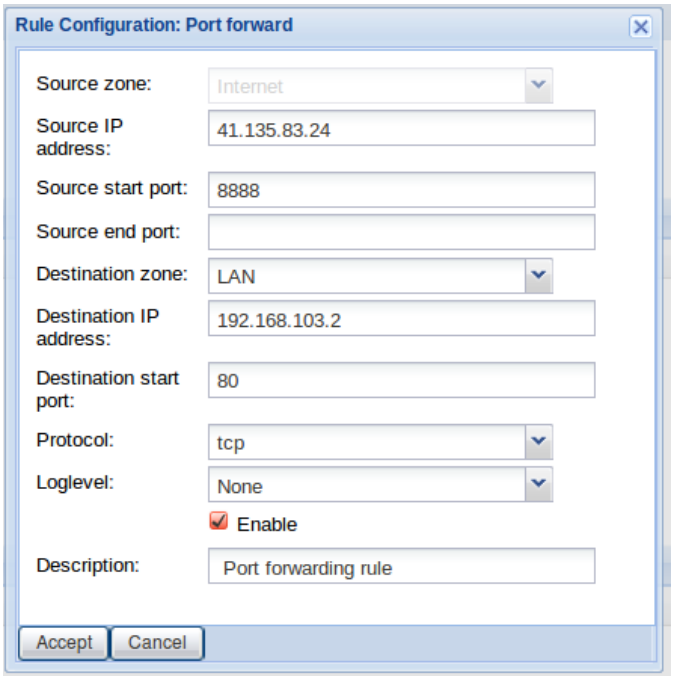

Figure 15: Port forward rule to allow access to another device.

Figure 15 depicts the configuration of a port forward route that will allow traffic on port 8888 of the public IP address of the Com.X, provided the the device requesting access has the IP address 41.135.83.24. Traffic on port 8888 is redirected to port 80 of the device at 192.168.103.2, which in this example, is a SIP handset (with a GUI hosted at port 80).

If the Source IP address field had been left empty, then acess would be allowed to any device that attempts to access port 8888 of the public IP address of the Com.X.

3.5.5 Quality of service features

From the Com.X GUI network tab, it is possible to configure the priorty with which different types of traffic are routed by the Com.X. By default, all SIP related traffic has higher priority than other, ordinary traffic. Highest priority is allocated to voice packets.

To edit these priorities, navingate to the QoS section of the Network page of the Com.X GUI, right click the type of traffic you would like to edit, and select edit.

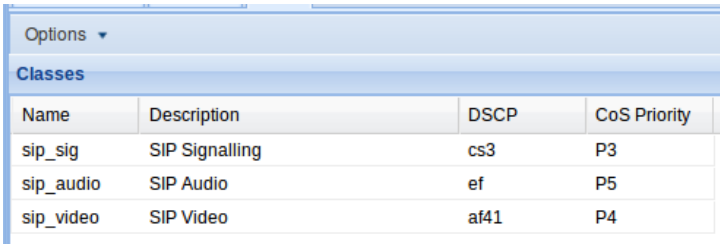

Figure 16: Traffic priority summary

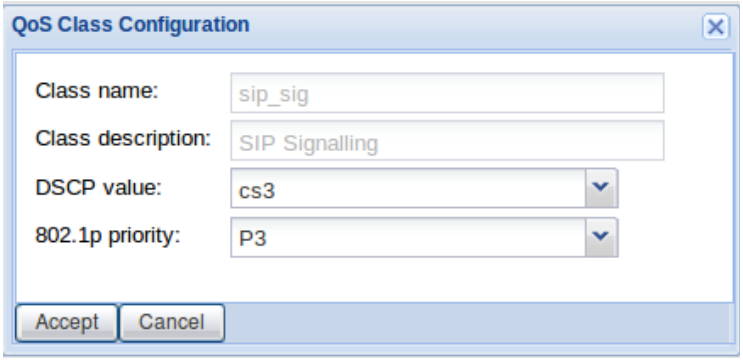

Figure 17: QoS class configuration for sip_sig traffic

Field	Description
Class name	sip_sig, sip_audio or sip_video
Class description	Description of above
DSCP Value	Differentiated Services Code Point as per RFC 5865. Unclassified traffic has DF code point.
802.1p Priority	VLAN priority as per IEEE 802.1Q, also internal network queue priority. P0 is normal priority (unclassified traffic), P7 is highest.

Table 6: QoS configuration options

3.5.5.1 Loading QoS defaults

To load the default QoS priority settings, navigate to the QoS page of the network tab on the Com.X Gui, select options and load defaults.

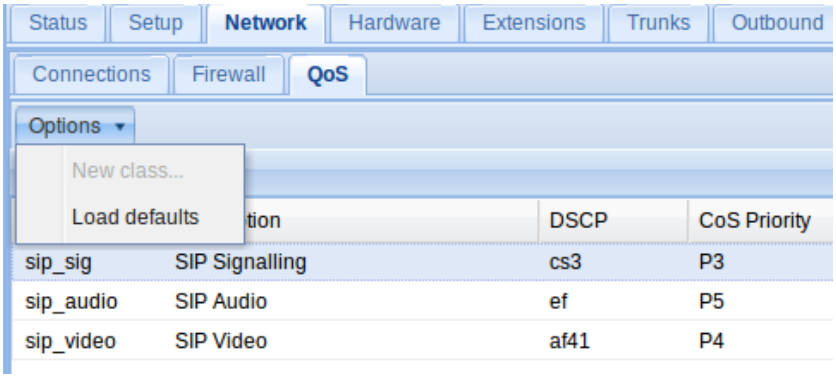

Figure 18: Loading default QoS priorities.