

ApplianX DPNSS-to-Q.SIG Gateway



1 GETTING STARTED	4
1.1 How to use this guide	4
1.2 Prerequisites	4
1.3 L.E.Ds.....	4
1.4 Logging in to the web interface.....	4
1.5 First time use.....	5
1.6 The Setup Wizard	6
1.7 The Main Menu	7
1.8 The Overview Page	8
1.9 System Time	9
1.10 Software Updates	9
1.11 Networking.....	11
1.12 Network settings via the web interface.....	11
1.13 Network settings via USB Flash Memory	12
2 CONFIGURING THE GATEWAY	13
2.1 Gateway Configuration	13
2.2 Gateway Configuration Page Descriptions	13
2.3 General Configuration Information	13
2.4 Editing Trunks	14
2.5 Editing a Trunk	14
2.6 Editing a Trunk Protocol.....	15
2.6.1 Clocking	17
2.6.2 Backing up and Restoring Configurations.....	18
3 DIAGNOSTICS	21
3.1 Remote Logging	21
3.2 Diagnostic Log	21
4 TROUBLESHOOTING	23

4.1 Logging into the remote interface	23
4.1.1 I can't get access to the gateway Web Interface.....	23
4.1.2 I log on but the overview screen has errors at the top	23
4.1.3 I get a warning saying that the gateway has not connected to the hardware.	23
4.2 Making calls through the gateway	23
4.2.1 I can't make a call through the gateway.....	23
4.3 Configuring the gateway	25
4.3.1 I have made changes to the configuration but they don't seem to have had any effect.	25
4.3.2 I used the Setup Wizard to create an initial configuration but I have an error saying that there is no active configuration.....	25
5 GLOSSARY	26

1 Getting Started

1.1 How to use this guide

The ApplianX DPNSS-to-Q.SIG Gateway management interface has been designed to be intuitive. However we still recommend that new users read chapters 1 and 2 of this guide before trying to set up a gateway for the first time. Chapters 3 and 4, Diagnostics and Troubleshooting, should only be needed if problems have been encountered.

1.2 Prerequisites

The gateway is configured via a Web Interface. Therefore a device with a web browser that supports TCP/IP will be needed to connect to the gateway. Also any networking cables and switches needed to allow this connection will be needed.

1.3 L.E.Ds

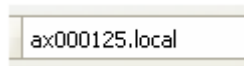
There are a number of LED's on the front of the gateway which can help during the installation and running of the gateway.

- Halted – This red LED indicates a serious error. If this has occurred in any circumstance other than restarting or shutting down the gateway then a serious error has occurred and a restart of the unit will be required.
- Error – This red LED indicates that the gateway has an error condition that may be resolved. Log into the gateway via the web interface to identify the nature of the problem
- Activity – This blue LED will flash when the gateway is starting up and also when the gateway is processing calls.
- Ready – This Green LED is lit when the gateway engine is running.
- Startup – This Yellow LED indicates that the gateway is starting. Note that user interaction may be needed via the web interface to complete start up.

1.4 Logging in to the web interface

The gateway should be powered up with a LAN cable connecting the administration port to the network. The gateway will take approximately one minute and twenty seconds to bring up the web interface.

Connect a PC to the same network that the administration port is connected to in order to allow access to the gateway's web interface. Type `axnnnnnn.local` into the browser's address window, where `nnnnnn` is the 6 digit serial number for the gateway.



The serial number can be found on a label on the rear of the unit and also on a label on the front left if you are facing it.

The resolution of the ApplianX name to an IP address utilises Zero Configuration Networking (Zeroconf) protocols. Some older web browsers may not support these protocols. An alternative method of discovering the IP address assigned to the gateway is to use a Windows software application called *ApplianX Search Tool* (available from www.applianx.com/tools.aspx). Once installed, start *ApplianX Search Tool* from the *start* menu and press the *Start* button. *ApplianX Search Tool* will

search the local network for ApplianX gateway's and report the IP address of any gateway's it finds (see Figure 1-1 below).

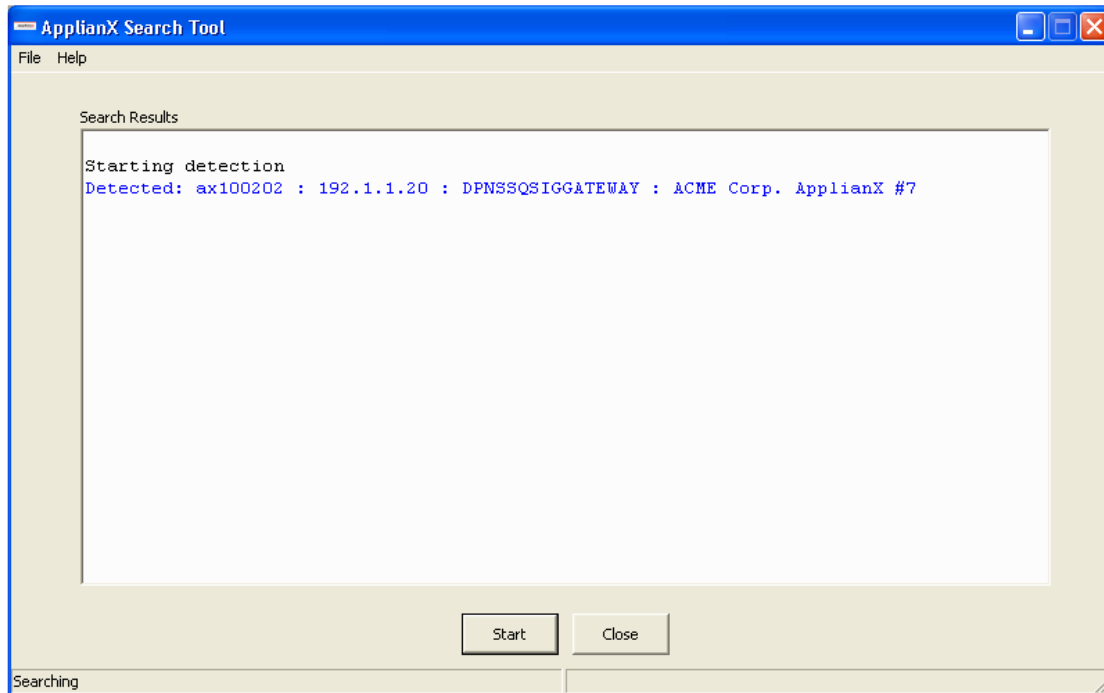


Figure 1-1 ApplianX Search Tool

Once you have discovered the IP address of your gateway, you can enter it into your browser's address window in order to access the gateway's web interface. Please see the troubleshooting section if you cannot gain access to any gateway web pages.

1.5 First time use

On first use the gateway Management Interface will display the page as in Figure 1-2. The user is required to provide a user name and password for an administrative user for the gateway.

Enter a user name, password and confirm the password. The user name and password cannot be left blank. Click **Submit** to create the account and login.

IMPORTANT: Until the gateway has been configured, this user name and password will be the only means of accessing the gateway. Pressing the reset button on the front panel will delete any users and reset the gateway back to its factory default settings. If the user names and passwords are forgotten then this is the only way to gain access to the gateway via the web interface.

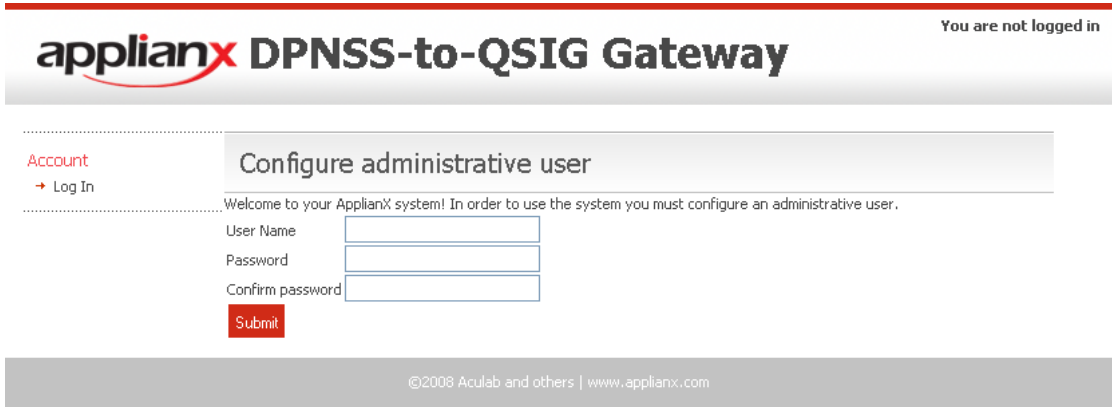


Figure 1-2 Configuring initial administrative user

1.6 The Setup Wizard

There are a number of steps that need to be carried out before the gateway can be used to service calls. The **Setup Wizard** is designed to create a default configuration. The Setup Wizard is accessed from the gateway menu. It is also automatically invoked the first time the gateway is used. The Setup Wizard allows the creation of a basic configuration, prompting for the most commonly required and important configuration details. Default values or reasonable values are used wherever possible.

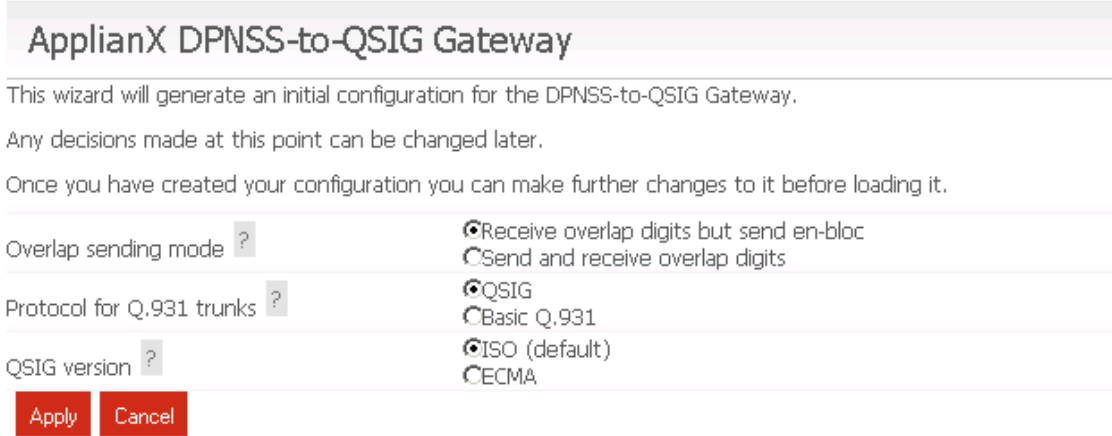


Figure 1-3 Setup Wizard

Cancel can be selected to return to the main gateway “Overview” page. No configuration is stored until the user selects **Apply**.

A Wizard-created new configuration will have:

- At least one DPNSS trunk
- At least one Q.SIG trunk
- TDM clocking configured to use any good available TDM trunk or otherwise to fall back to local clocking

Calls are routed between trunks 1 and 2 and between trunks 3 and 4. If there are more than four trunks present, this paired-routing pattern is continued.

Once completed, the Setup Wizard will redirect your web browser to the “Edit Configurations” page. Here you have a list of all configurations that have been set up on the gateway. Note that if this is the first time a configuration has been created then the new configuration will be listed in the “Available configurations” list. The configuration must be activated to bring it into use. This is done by selecting **Use** for the required configuration.

1.7 The Main Menu

On the left of the screen at all times, apart from when the Setup Wizard is running, you will be able to access all the configuration and status pages.

- **Status**
 - **Overview** – A page with some basic gateway call counts and a list of actions required of the gateway administrator.
 - **Alarms** – This page will display any Layer 1 or Layer 2 alarms on the TDM trunks. It will also allow the masking of these alarms.
 - **Calls** – A graphical display of all the call activity on the gateway.
 - **Call Log** – A recent history of calls that the gateway has attempted to route. This page can be very useful for diagnosing issues during the set up phase for the gateway.
 - **Trunk Status** – This has detailed information on the TDM trunks

- **System Configuration**
 - **Global Configuration** – This allows the gateway to be named.
 - **System Time** – This allows the setting of the clock to local time.
 - **Software Update** – From this page a check can be made for software updates.
 - **System Users** – This allows the addition of new administrators to the gateway and the setting of their privileges.
 - **Backup and Restore** – This allows configurations to be saved and restored to the gateway.
 - **Networking** – This allows the user to choose between either setting a static IP address or using DHCP. Also, the addresses of Domain Name System (DNS) servers to be used by the gateway can be set here.
 - **SNMP** – This allows the configuration of the SNMP settings. From here you can enable SNMP and enter the IP addresses of hosts you wish to send traps to.
 - **Setup Wizard** – This allows the Setup Wizard to be run to create a basic configuration.

- **Gateway Configuration**
 - **Edit Configurations** – This takes you to the main configuration overview where different gateway configurations can be selected and edited.

- **Diagnostics**
 - **Remote Logging** – This allows the administrator to point the syslog output from the gateway to an external syslog client. This is for advanced users and support teams.
 - **Watchdog Status** – This reveals the status of the “watchdogs” running on the gateway. They are here to look for any elements that have failed or are reporting problems. This is for advanced users and support teams.
 - **Restart** – This is used to “reboot” the gateway. Note that rebooting will cause all contact to be lost with the gateway through the user interface.
 - **Diagnostic Log** – This provides a high level overview of gateway processes and can be used for debugging purposes.
 - **About** – This displays build information about the gateway.
 - **Hardware** – This displays the version and status of the hardware used in the gateway.

- **Account**
 - **Log Out** – This allows the current user to log out of the gateway administration screens.
 - **Change Password** – This allows the current user to change their password.

1.8 The Overview Page

The Overview page gives some basic statistics for the gateway such as total incoming and outgoing call counts. At the bottom of this page will be a list of actions that the gateway is flagging for the administrator.

Overview	
Status	Running
Incoming Calls	77
Outgoing Calls	77
Unroutable Calls	0
Clock source	Local

Required Actions	
Error	Trunk: (Trunk 1) - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)
Error	Trunk: (Trunk 2) - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)
Error	Trunk: (Trunk 4) - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)
Error	Trunk: (Trunk 3) - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)

Figure 1-4 The Overview page

As you can see in the above example the gateway is telling us that we have Layer 1 errors on all trunks. In this case it is because we have not connected any TDM trunks to the gateway yet.

1.9 System Time

The System Time page can be accessed by selecting **Global Configuration** which then expands the menu, followed by selecting **System Time**. A page similar to the one shown below in Figure 1-5 will be displayed.

System Time	
Local settings	
Time	<input type="text" value="Dec 04 2008 15:52"/>
Time zone	<input type="text" value="Europe/London"/>
NTP daemon settings	
Time server 1 ?	<input type="text" value="192.1.1.30"/>
Time server 2	<input type="text" value="192.1.1.31"/>
Time server 3	<input type="text"/>
Time server 4	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Figure 1-5 System time page

This page allows the gateway clock to be set. The clock is used for time-stamping events in the gateway diagnostic logs. Not all variants of the gateway are equipped with a battery-backup for the clock in the event that mains power is lost. For this reason it is recommended that the gateway be configured to synchronise its clock with a Network Time Protocol (NTP) server. The IP address or FQDN of up to four NTP servers can be entered here. Ensure that each server address is visible from the gateway. If your NTP servers are beyond a firewall, ensure that the NTP port (port 123) is open on the firewall.

1.10 Software Updates

The Software Updates page can be accessed by selecting **Global Configuration**, which then expands the menu, followed by selecting **Software Updates**. A page similar to the one shown below in Figure 1-6 will be displayed.

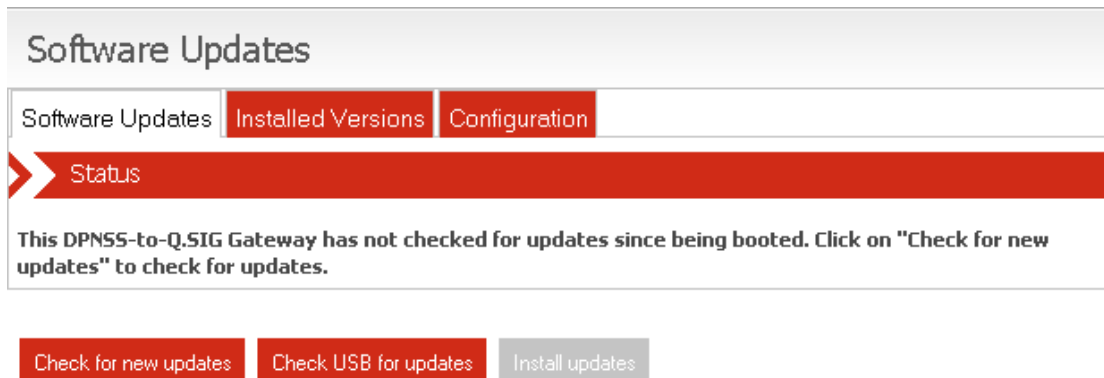


Figure 1-6 Software updates page

If the gateway has access to the internet, select **Check for new updates** to get the latest update information from the ApplianX server. Once the updates have been identified select **Install updates**.

If your gateway is not connected to the internet, new updates can be installed via USB device. In order to install updates from a USB device, the latest updates first need to be downloaded from the ApplianX server and copied onto the USB device. To achieve this, install and use the Windows software application called *ApplianX USB Update Tool* (available from www.applianx.com/tools.aspx) on a Windows PC which is attached to the internet. Once you have a USB device which holds the latest updates, attach it to your gateway and select **Check USB for updates**. Once the updates have been identified select **Install updates**.

Note that when the software updates are applied, the gateway will download the updated software packages and will install them. At the end of the update the user will be asked to reboot the gateway so that the updates can take full effect.

Selecting the **Installed Versions** tab will give a list of all the software packages that make up the gateway and their version number. This may help advanced user to diagnose issues.

The **Configuration** tab takes you to the page shown below in Figure 1-7. Here you can set up any local HTTP proxy information that is needed to give the gateway access to the ApplianX update archive.



Figure 1-7 Software updates page - Configuration tab

1.11 Networking

The gateway requires a single IP address. By default this is set to be acquired via DHCP. Note that if DHCP is selected and there is no DHCP server on the network the gateway will use Zeroconf technologies to get an address and to provide access to the unit. Network settings can be configured by using the web interface or by using a USB flash memory device.

1.12 Network settings via the web interface

Adjust network settings by selecting **Networking** from the menu on the left. Here entries can be made for the IP address of the gateway and for any DNS servers that the gateway should use for name resolution.

The screenshot shows a web interface for configuring network settings. At the top, there is a header labeled "Networking". Below this, a red bar with a white arrow points to the right, labeled "Administration interface". The main configuration area is divided into two sections. The first section, "Administration interface", contains a checkbox for "DHCP" which is unchecked. Below this are four input fields: "IP address" with the value "192.168.0.99", "Netmask" with "255.255.255.0", and "Gateway" with "192.168.0.1". The second section, "Name resolution settings", contains three input fields: "Name server" with "192.168.0.5", another "Name server" with "192.168.0.6", and "Search domains" with "acme.com". At the bottom of the interface, there are two buttons: "Save Configuration" and "Cancel Changes".

Figure 1-8 Networking

Note that changing the IP address of the gateway will cause the browser to lose contact with the gateway. The browser should be manually redirected to the new IP address.

1.13 Network settings via USB Flash Memory

The gateway will check for the presence of a USB device when it is booting up. If it finds one then it will look on this device for User Defined IP settings and will configure the unit to come into service with those settings. Note that using this method it takes a few minutes longer for the unit to come up and switch to using the new IP address.

On the USB flash device create a directory called *applianx_net* in the root directory. Place a single file in this directory called *admin*. Note that this filename has no extension so be careful with the editor you are using in case it adds an extension for you.

Within this file you need to put the information to set the static IP address:

```
[Config]
ip = 192.168.0.99
netmask = 255.255.255.0
gateway = 192.168.0.1
```

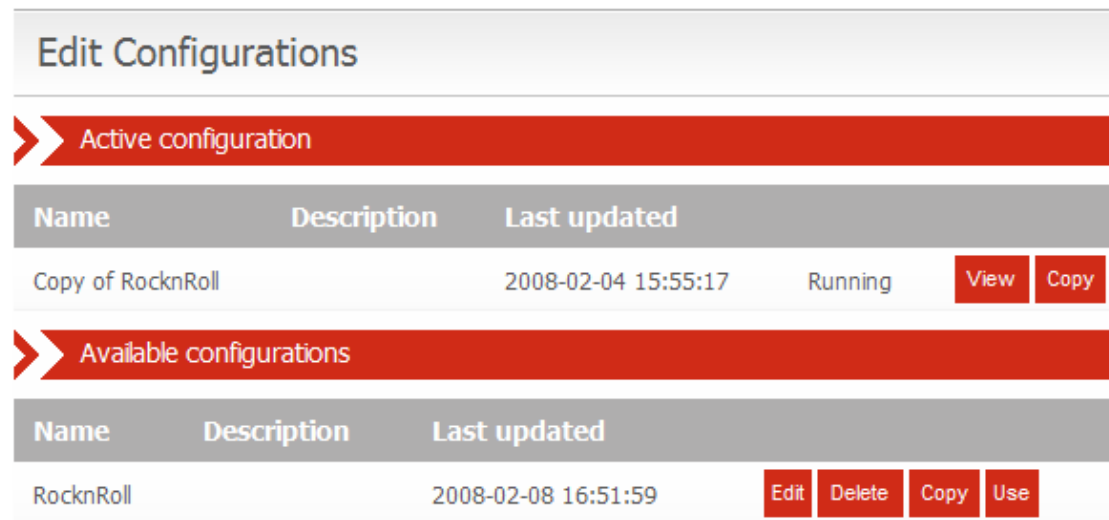
or to set an interface to DHCP use:

```
[Config]
dhcp = 1
```

2 Configuring the Gateway

2.1 Gateway Configuration

All gateway configurations are managed from the “Edit Configurations” page (see Figure 2-1 below). The currently active configuration is listed first. This may not be directly edited, but may be examined by selecting **View**. To modify the active configuration, it is first necessary to click **Copy** next to the active configuration entry. When you are happy with edits made to a new or copied configuration you can select this to be the active configuration by selecting the **Use** button on the right of the configuration.



The screenshot shows the 'Edit Configurations' page. It has a title bar 'Edit Configurations'. Below it is a red bar with a white arrow pointing right and the text 'Active configuration'. Underneath is a table with columns 'Name', 'Description', and 'Last updated'. The first row shows 'Copy of RocknRoll' with a 'Last updated' of '2008-02-04 15:55:17' and a status of 'Running'. To the right of this row are two buttons: 'View' and 'Copy'. Below this is another red bar with a white arrow pointing right and the text 'Available configurations'. Underneath is another table with columns 'Name', 'Description', and 'Last updated'. The first row shows 'RocknRoll' with a 'Last updated' of '2008-02-08 16:51:59'. To the right of this row are four buttons: 'Edit', 'Delete', 'Copy', and 'Use'.

Name	Description	Last updated		
Copy of RocknRoll		2008-02-04 15:55:17	Running	View Copy

Name	Description	Last updated				
RocknRoll		2008-02-08 16:51:59	Edit	Delete	Copy	Use

Figure 2-1 Edit Configurations page

2.2 Gateway Configuration Page Descriptions

Configuration information is presented as a set of inter-related tabbed pages, some of which lead to further more detailed pages. At any time, selecting **Cancel Changes** will cause all changes to be discarded. Selecting **Save Configuration** will save the changes made. In either case, the main Edit Configurations page is redisplayed.

2.3 General Configuration Information

This page, shown in Figure 2-2, enables the setting of a configuration name and description. A configuration may be renamed by changing the **Configuration name**. The **Configuration description** allows any notes or important information to be stored along with a configuration.

Editing: New configuration

General **Trunks** Clocking

General Configuration Information

Configuration name

Configuration description

Save Configuration Cancel Changes

Figure 2-2 General

2.4 Editing Trunks

All available trunks are listed on the “Trunks” page as in Figure 2-3. Settings for an individual trunk can be changed by selecting **Edit** next to the trunk.

Editing: New configuration

General Trunks **Clocking**

TDM trunks

Name	Description	Type	Group	
Trunk 1		TDM	DPNSS Group 1	Edit
Trunk 2		TDM	Q.931 Group 1	Edit
Trunk 3		TDM	DPNSS Group 2	Edit
Trunk 4		TDM	Q.931 Group 2	Edit

Save Configuration Cancel Changes

Figure 2-3 Trunks page

2.5 Editing a Trunk

Each Trunk requires a name distinct from all other Trunks. Changing the name of a Trunk causes all references to the Trunk to also change. The time at which the speech path is opened for calls on this trunk can be selected to be prior to the call being connected. This is useful for the passing of in-band information related to the call. It is possible to block a trunk from participating in call activity. The strategy for allocating outgoing timeslots can be selected from a list of options. The inter-digit

timeout in milliseconds can be specified. This is the time that the gateway waits for another digit before deciding it has got them all. The currently configured protocol is displayed. This can be configured by selecting **Edit** (see section 2.2.9). Finally the SNMP trap can be enabled for this trunk.

Editing: New configuration

Apply
Cancel

>> General settings

Trunk name	<input style="width: 90%;" type="text" value="Trunk 1"/>
Trunk description	<input style="width: 90%;" type="text"/>
Open inward speech path before answer <small>?</small>	<input checked="" type="checkbox"/>
Block trunk from call activity <small>?</small>	No <small>▼</small>
Outgoing timeslot allocation strategy <small>?</small>	Highest available <small>▼</small>
Minimum digit count <small>?</small>	<input style="width: 90%;" type="text" value="0"/>
Interdigit timeout (milliseconds) <small>?</small>	<input style="width: 90%;" type="text" value="0"/>
Interdigit timeout for virtual calls (milliseconds) <small>?</small>	<input style="width: 90%;" type="text" value="1000"/>
Send sending complete on outgoing calls <small>?</small>	<input checked="" type="checkbox"/>
Send overlap digits on outgoing calls <small>?</small>	<input type="checkbox"/>

>> SNMP configuration

Enable SNMP traps	<input checked="" type="checkbox"/>
-------------------	-------------------------------------

>> Protocol configuration

Protocol	DPNSS	Edit
----------	-------	--

Figure 2-4 Edit Trunk page

2.6 Editing a Trunk Protocol

Each TDM Trunk also requires a trunk protocol. DPNSS trunks are pre-configured with the DPNSS protocol and cannot be assigned an alternative protocol. Q.931 trunks can be assigned either the Q.SIG or ETS 300 protocols. The selected protocol must be chosen to be compatible with the remote equipment connected to the trunk. The current protocol can be set or modified by selecting **Change**. Protocol configuration options can be reached by selecting **Edit**. A page similar to the one in Figure 2-5 will be displayed. All settings and options for the trunk protocol are specific to the user's installation. You should seek the advice of your service provider or switch maintenance team for advice on the protocol selection and settings used.

DPNSS

>> General settings

Impedence	120 Ohms (default) ▾
CRC4 enabled	<input type="checkbox"/>
Master/Slave configuration	AX ▾

>> Basic features

Display direction [?]	Send and receive ▾
Allow incoming data calls [?]	<input checked="" type="checkbox"/>
Loop avoidance mapping [?]	<input type="radio"/> Disabled <input checked="" type="radio"/> Transparent <input type="radio"/> Transit
Global transit limit [?]	25
Insert loop avoidance in outgoing calls [?]	<input type="checkbox"/>
Do-not-disturb mapping [?]	<input checked="" type="checkbox"/>
Method for generating outgoing CLC [?]	<input type="radio"/> Use a fixed value <input checked="" type="radio"/> Map from the incoming leg (default) <input type="radio"/> Map from the calling name
Insert Bearer Service Selection (BSS) [?]	<input checked="" type="radio"/> Disabled <input type="radio"/> Preferred <input type="radio"/> Mandatory
Call Offer Enabled [?]	<input checked="" type="checkbox"/>
Call Transfer Enabled [?]	<input checked="" type="checkbox"/>

>> Call Diversion Supplementary Service Support

Call Diversion Enabled [?]	<input checked="" type="checkbox"/>
Automatic Diversion Validation [?]	<input type="checkbox"/>
Call Redirection Enabled [?]	<input checked="" type="checkbox"/>

>> CBWF/CBWNU (CC) Supplementary Service Support

CBWF/CBWNU (CC) Enabled [?]	<input checked="" type="checkbox"/>
--------------------------------------	-------------------------------------

>> Message Waiting Supplementary Service Support

Message Waiting Method [?]	Call-Back Messaging (default) ▾
Message Waiting On NSI string [?]	B*AN*1
Message Waiting Off NSI string [?]	B*AN*0

>> Route Optimisation

Route Optimisation Enabled [?]	<input checked="" type="checkbox"/>
Pad digit for DPNSS call references [?]	9

>> Raw configuration options

Options [?]	
----------------------	--

Apply
Cancel

Figure 2-5 Editing a TDM Trunk Protocol

2.6.1 Clocking

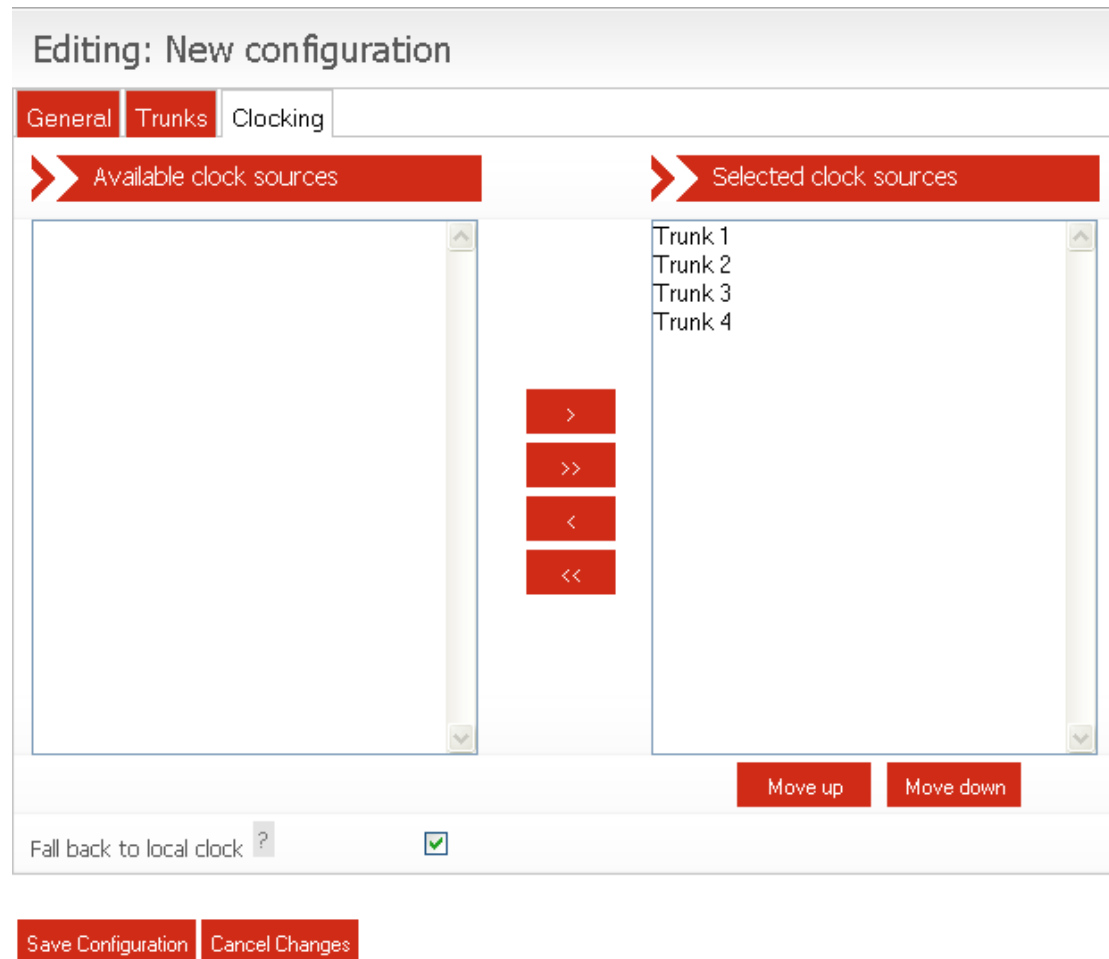


Figure 2-6 Clocking control page

This page controls the source of the gateway's telephony clock. A correctly configured clock is essential for proper operation of the gateway.

The page displays two columns. The left-hand column shows the Available Clock Sources. These are all the trunks not currently selected as a possible clock source. The right-hand column shows Selected Clock Sources. These trunks are currently selected as possible clock sources.

- To move an *Available* trunk to the *Selected* column, highlight it and then click the > button
- To move a *Selected* trunk to the *Available* column, highlight it and click the < button
- To move all *Available* trunks to the *Selected* column, click the >> button
- To move all *Selected* trunks to the *Available* column, click the << button

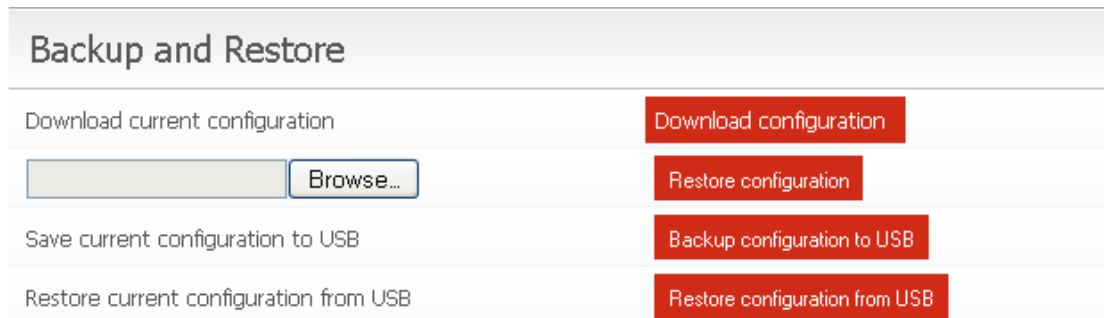
The Selected Clock Sources are listed in the order of application. This order can be changed by highlighting individual trunks and then selecting **Move Up** or **Move Down**.

There is an additional option to fall back to a locally generated clock source when no other clock source is available. By default all trunks are pre-configured with **Fall back to local clock** selected. This can be changed if the local gateway installation requires it.

In operation, the first listed Selected Clock Source that is found to be functional will be used. If, at any time, this should be detected as failed, the gateway will automatically switch to the next listed functional clock source.

2.6.2 Backing up and Restoring Configurations

To save or restore configuration information select **Global Configuration** under the **System Configuration** section in the main menu. This will reveal further options. From here select **Backup and Restore**. This will bring up the Back and Restore page as shown below in Figure 2-7.



The screenshot shows a web interface titled "Backup and Restore". It contains four rows of options, each with a text label on the left and a red button on the right. The first row has the label "Download current configuration" and a button labeled "Download configuration". The second row has a text input field followed by a "Browse..." button, and a button labeled "Restore configuration". The third row has the label "Save current configuration to USB" and a button labeled "Backup configuration to USB". The fourth row has the label "Restore current configuration from USB" and a button labeled "Restore configuration from USB".

Figure 2-7 Backup and Restore

To back up a configuration to the PC that the web browser is on, select the **Download configuration** button on the right. If using Internet Explorer on Windows, this will bring up a window similar to the one below shown in Figure 2-8. Selecting **Save** will bring up the Windows save menu so that you can select where the file is saved and what name is used.

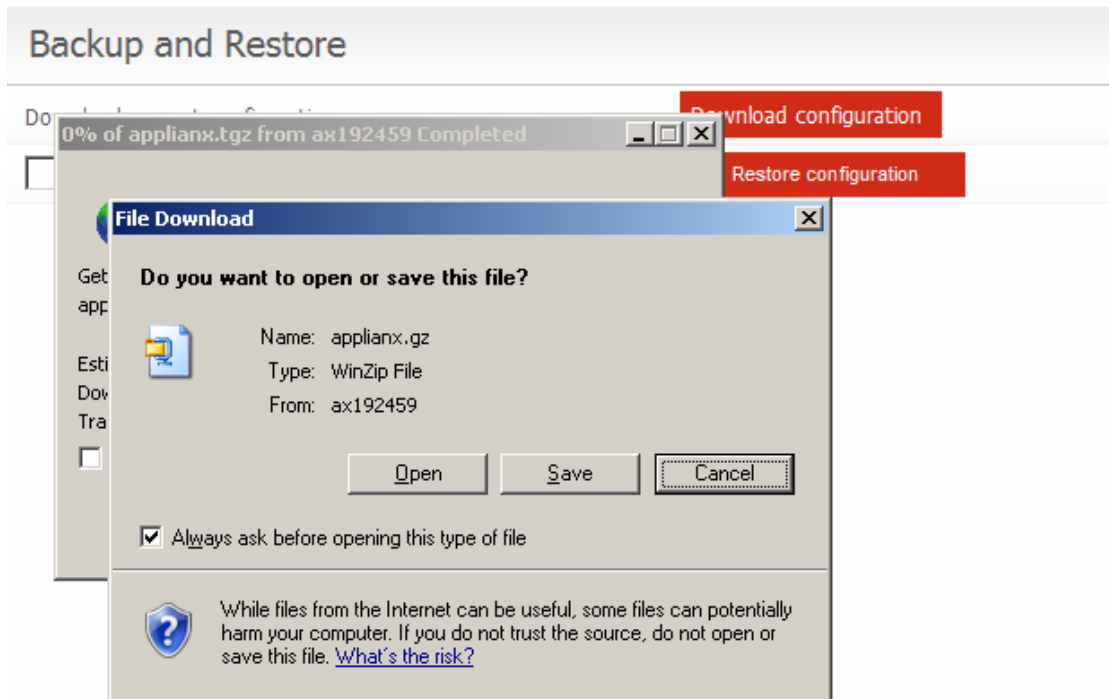


Figure 2-8 Saving the File

To restore a previously saved configuration then either enter the path and filename in the box provided or select browse to locate and select the backup file. Once the required back up has been chosen, select **Restore configuration**.



Figure 2-9 Restore configuration

If this is successful then you will see the message as shown below

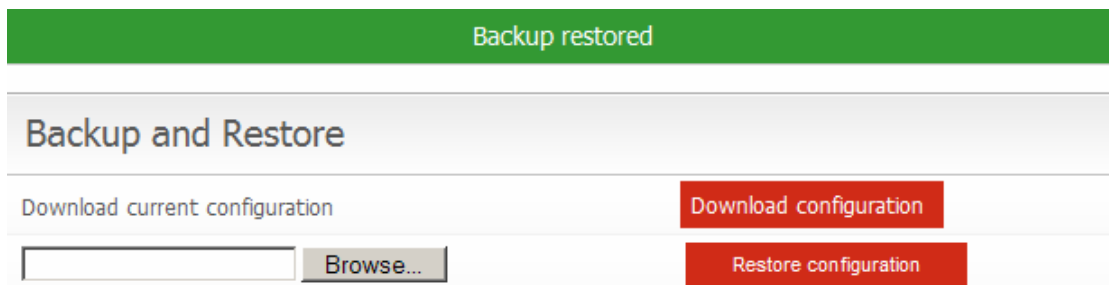


Figure 2-10 Backup restored

In addition, back ups can be saved and retrieved to and from a USB flash memory device that is placed in the USB slot in the front of the gateway. If a non-bootable USB device is placed in the USB slot of the gateway when it is booted and it has a previously saved configuration on it then the gateway will come into service with that configuration.

3 Diagnostics

3.1 Remote Logging

On the main menu on the left of the screen, as seen through the gateway web interface, you will see a **Diagnostics** section. Selecting **Remote Logging** takes you to the following, Figure 3-1.

Remote Logging

Enable remote logging [?]

Host to receive logs [?]

Logging port [?]

Log sources

Log Type	Status	
Switch trace	stopped	<input type="button" value="Start"/>
Trunk 1 protocol trace	stopped	<input type="button" value="Start"/>
Trunk 2 protocol trace	stopped	<input type="button" value="Start"/>
Trunk 3 protocol trace	stopped	<input type="button" value="Start"/>
Trunk 4 protocol trace	stopped	<input type="button" value="Start"/>

Figure 3-1 Remote Logging

There are no facilities for storing Logging information on the gateway. It does, however, support the use of Syslog and can send information using the syslog protocol to a client that can receive syslog messages. The majority of Linux distributions will include a syslog daemon and it will most likely be running by default. For Windows there are freeware implementations available. The trace available through the remote logging is intended for use by your vendor's support staff. Check the ApplianceX web site www.applianceX.com for any self-help tools which may become available to aid understanding of the trace.

3.2 Diagnostic Log

This page gives a high level record of actions carried out by the gateway. It will also show any errors that the gateway encountered while coming into service. This information should be passed to your support contact if you think that there is a problem with the gateway.

Diagnostic Log

```
2008-12-02 11:49:03 Info System booted
2008-12-02 11:49:03 Info Waiting for hardware detection
2008-12-02 11:49:21 Info Loading configuration New configuration
2008-12-02 11:49:21 Info Clock source is now: Local
2008-12-02 11:49:21 Info Starting protocol firmware download
2008-12-02 11:49:22 Info Firmware download to trunk Trunk 1 succeeded (firmware=dpnss.pmx)
2008-12-02 11:49:23 Info Firmware download to trunk Trunk 2 succeeded (firmware=qsig.pmx)
2008-12-02 11:49:25 Info Firmware download to trunk Trunk 3 succeeded (firmware=dpnss.pmx)
2008-12-02 11:49:26 Info Firmware download to trunk Trunk 4 succeeded (firmware=qsig.pmx)
2008-12-02 11:49:26 Info Firmware download complete
2008-12-02 11:49:26 Info Configuration New configuration loaded
2008-12-02 11:49:26 Info System Starting
2008-12-02 11:49:26 Info System Started
2008-12-02 11:49:26 Info Clock source is now: Trunk 1
```

Figure 3-2 Diagnostic Log

In the above example the system boots and then waits for internal hardware detection to complete. Protocol firmware is downloaded to the TDM trunks. Next, the TDM clock source changes to Trunk 1 as Trunk 1 is the first detected usable external clock source. Once firmware download is complete, the currently selected configuration becomes active.

4 Troubleshooting

4.1 Logging into the remote interface

4.1.1 I can't get access to the gateway Web Interface

- Have you tried using the *ApplianX Search Tool* (available from www.applianx.com/tools.aspx)? If not, install this tool on a Windows PC that is attached to the same network as your gateway. Start the tool by clicking the *start* menu and selecting *All Programs* → *ApplianX* → *ApplianX Search Tool*. This tool will enable you to determine the IP address of your gateway if it is correctly attached to your network.
- Try checking the cabling and then try to log in again. The PC and the gateway administration port must be on the same network.
- If you are using an old distribution of Linux then try updating to a current distribution.
- On a Windows XP PC, are you using Microsoft Explorer Version 6 or 7? If not try using one of these browsers. Note that version 7 is preferred.
- Try connecting the network port of your PC directly to the gateway administration port.
- Try accessing the web interface from an up-to-date Linux or MAC OS X PC using *axnnnnnn.local* address if you have one available. Did this work? If so you may have DNS/DHCP network issues. Move to using static IP addresses
- Try setting the IP address of the gateway to a static IP address using a USB flash memory stick as described in 1.13.

4.1.2 I log on but the overview screen has errors at the top

- Wait a couple of minutes and then refresh the screen. The web interface can start before the gateway, which means that until the gateway has started, the web interface will report that it cannot talk to the gateway engine.

4.1.3 I get a warning saying that the gateway has not connected to the hardware.

- This is normal when the unit has started or been rebooted or has had its IP settings changed. The elements that make up the gateway are just starting and establishing their communication paths.

4.2 Making calls through the gateway

4.2.1 I can't make a call through the gateway

- Check the **Call Status** page by selecting **Calls** under the **Status** section on the menu on the left of the web interface. Now make a call in from the one side of the gateway. Looking at the **Call Activity** at the bottom of the screen, check that the call was received by the gateway. In the example given (see Figure 4-1) you can see that the gateway did indeed receive the call but could not route it. Check your configuration to ensure that all settings are correct for each signalling network that the gateway is connected to and ensure that all trunk cables are plugged in correctly.

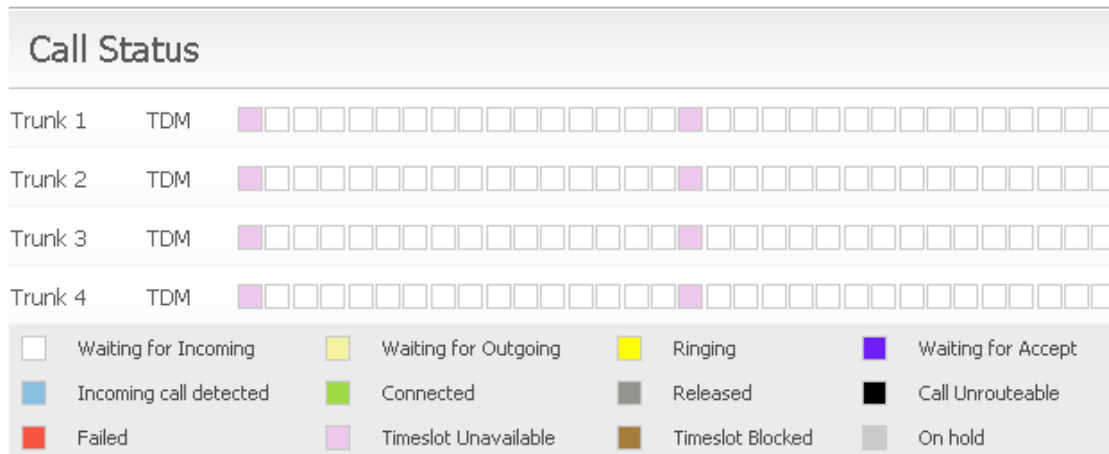


Figure 4-1 The Call Status page

The screenshot shows the 'Call Activity Log' page with a table of call events. The table has four columns: Time, Location, Numbers, and Message.

Time	Location	Numbers	Message
2008-12-03 10:31:21.594	Trunk 2 Ts: 1	From: To: 1234567	Idle
2008-12-03 10:31:21.445	Trunk 2 Ts: 1	From: To: 1234567	Matched routing rule ""
2008-12-03 10:31:21.445	Trunk 2 Ts: 1	From: To: 1234567	Call released (No circuit/channel available (34))
2008-12-03 10:31:21.445	Trunk 2 Ts: 1	From: To: 1234567	There are no more outgoing rules matching this call
2008-12-03 10:31:21.445	Trunk 2 Ts: 1	From: To: 1234567	Making an outgoing call on endpoint Trunk 1
2008-12-03 10:31:21.445	Trunk 2 Ts: 1	From: To: 1234567	Call incoming on endpoint Trunk 2
2008-12-03 10:31:21.445	Trunk 2 Ts: 1	From: To: 1234567	Incoming call detected

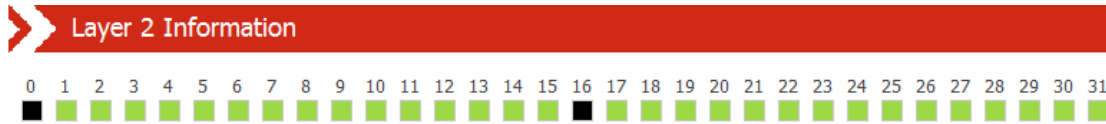
Figure 4-2 Example Call Activity Log showing a failed call

- If there are no calls present then check the status of the trunk. This is done by selecting **Trunk Status** from the **Status** section of the menu. If the trunk is good then the Layer 1 should be showing zero for **Slip errors**, **Bipolar violations** and **Frame Alignment errors**. If there are errors on these then please check the cabling. Ensure that you have configured the correct protocol for the Q.931 trunks. Also check the options that have been chosen for the protocols and ensure that these are correct for the TDM lines that are connected to the gateway.

Layer 1 Information

Slip errors	0
Bipolar violations	0
Frame Alignment errors	0

- If there are no Layer 1 Errors then check the Layer 2. If this isn't showing green for the bearer channels on the trunk then there is a layer 2 problem. Ensure that you have configured the correct protocol for the Q.931 trunks. Check with your service provider or PBX maintenance team for information regarding protocol settings.



4.3 Configuring the gateway

4.3.1 I have made changes to the configuration but they don't seem to have had any effect.

- The gateway does not allow you to edit a configuration that is in use. For this reason you can copy a configuration and edit this. Before these changes can take effect you must select that the gateway use this edited configuration. This is done by selecting the **Use** button by the side of the edited configuration on the **Edit Configurations** page.

4.3.2 I used the Setup Wizard to create an initial configuration but I have an error saying that there is no active configuration.

Required Actions

Error No active configuration (Please apply an available configuration (See 'Edit Configurations' page), or use the 'Setup Wizard' to create a new configuration)

- On completion of the Setup Wizard, a skeleton configuration is created. This configuration is not automatically activated. On completion of the Setup Wizard you will be directed to the **Edit Configurations** screen. Here the configuration created in the Setup Wizard will be shown under the **Available configurations** section. Select **Use** to activate that configuration.

Available configurations			
Name	Description	Last updated	
Copy of My configuration		2007-09-20 14:37:53	<div style="display: flex; gap: 5px;"> Edit Delete Copy Use </div>

5 Glossary

ApplianX – is a product brand of Aculab. It has been developed in order to provide robust and reliable systems for rapid deployment and integration into existing infrastructures.

DNS – Domain Name System. A hierarchical naming system for computers, services, or any resource on an IP network.

E1 – 2.048 Mbit full-duplex communication interface. Used in most countries outside of the United States, Canada and Japan.

FQDN – Fully Qualified Domain Name. A DNS domain name that uniquely identifies the host.

HTTP – Hypertext Transfer Protocol. Used on ApplianX units to send information to and from web browsers

ISDN – Integrated Services Digital Network. Represents the family of protocols that have their origins in the ITU's Q.931 and Q.921 specifications. ETS 300 102 in Europe and National ISDN 2 (NI2) are typical examples of ISDN protocols.

LAYER 1 – Known as the physical layer in the OSI (Open Systems Interconnection) 7 layer model. Responsible for getting raw bits from one node to another. It has some alarm and error transmitting capabilities. Layer 1 services Layer 2 requests.

LAYER 2 – Known as the data link layer in the OSI (Open Systems Interconnection) 7 layer model. This layer is responsible for the transfer of data between two nodes on the same network. It usually has error detection and possibly correction. Within this document and the gateway web interface we refer to Layer 2 for TDM protocols. For ISDN protocols this is based upon the ITU (International Telecommunications Union) Q.921 standard.

LINUX – A Unix-like operating system that is supported and distributed by many organisations. Well known distributions include Red Hat, Fedora, Suse, Debian and Ubuntu to mention just a few.

MAC OS X – The operating system used on Apple (Apple Incorporated formerly Apple Computers Incorporated) PC's.

NTP – Network Time Protocol. A protocol designed to synchronise the clocks of computers over a network.

PBX – Private Branch eXchange. This is a local switch that traditionally terminates POTS (Plain Old TelephoneS) and routes calls between users and into other switches on TDM networks (and more recently IP networks).

SNMP – Simple Network Management Protocol. This can be set up on the gateway so that SNMP software (not supplied) can be used to monitor elements of the gateway status remotely. This requires use of the MIB (Management Information Base) that can be found on the ApplianX web site <http://www.applianx.com>.

T1 – 1.544 Mbit full-duplex communication interface. Used mostly in the United States, Canada and Japan.

TDM – Time Division Multiplexed. Used in this document to refer to the ISDN trunks. Also known as T1 or E1 interfaces on the gateway.

Timeslot – A dedicated slot on the TDM interface used for carrying digitised voice and data information. Typically an E1 interface will have 30 of these and T1 23 or 24.

Trunks – Either an E1 or T1 interface. A wired connection that carries a collection of voice channels and signalling channels.

USB – Universal Serial Bus. Used with the gateway for inserting external memory devices for the configuring of IP settings and saving and restoring of configurations.

Web Interface – This is the user interface on the gateway that has been designed to work with a web browser (not supplied) to allow administrators to configure, monitor and maintain the gateway. Examples of web browsers are Microsoft Internet Explorer (ie6/ie7), Safari, Firefox and Opera.

Windows – Within this document Windows is used as a collective term for a number of operating systems developed by Microsoft Corporation. Namely Windows XP, 2003 Server and Vista. (Previous versions such as 3.1, 95, 2000 and ME have not been tested against the gateway)

ZEROCNF – Zero Configuration Networking. This is a set of techniques that automatically creates a usable network without DHCP and DNS servers or manual configuration. This is used in the gateway when the unit is set to DHCP and no DHCP server can be found on the network.