Configuration Manual

XG6846

Revision E

Table of Contents

Overview XG6846

Hardware

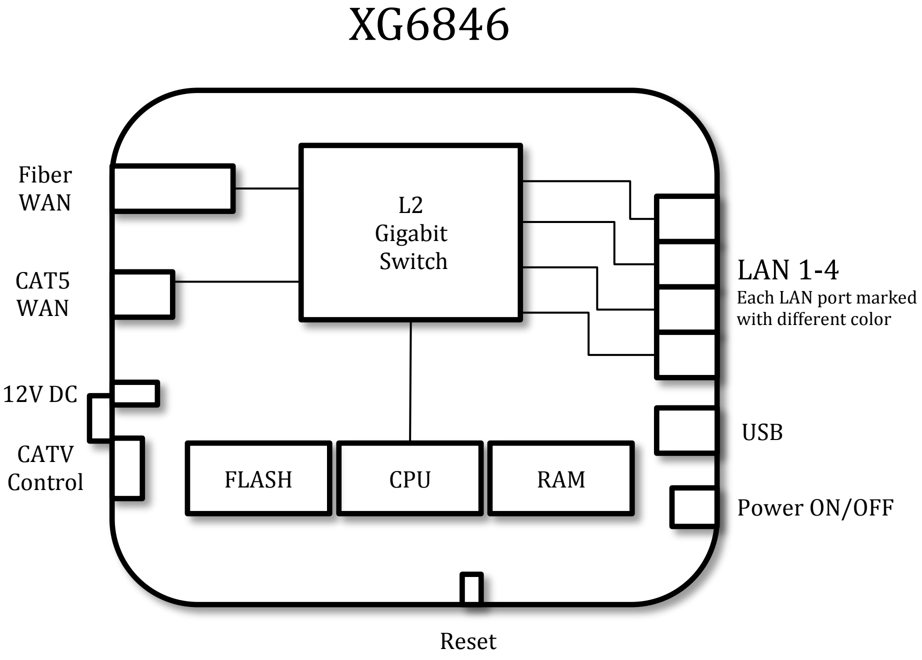


Figure 1

The XG6846 is a manageable non-blocking Gigabit Ethernet Layer 2 CPE with one CAT5 WAN (EXT1) , one SFP fiber WAN port and 4 Gigabit LAN ports.
The 4 LAN ports are color marked to simplify end user support.
IGMP Snooping for IPTV is supported for all LAN ports and is enabled by default.

Dual WAN
SFP is inserted in the SFP tray => CAT5 WAN (EXT1) is used as LAN port 5.
No SFP is inserted CAT5 WAN => (EXT1) is used as WAN port.

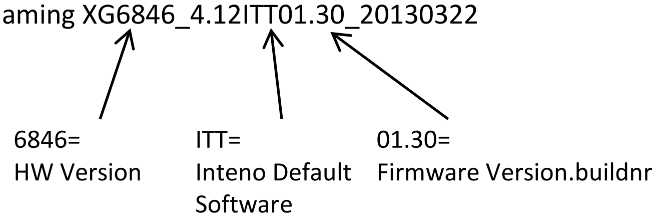
XG6846 have a CPU which is used for IP management and for controlling the L2 switch.
The CPU is connected to the L2 switch on a separate Ethernet port.

The 6846 have a static memory (FLASH) for storage of configuration and firmware.

A USB 2.0 port is located beside the LAN ports.

Firmware Naming

Firmware Image Naming XG6846_4.12ITT01.30_20130322



6846=
HW Version

ITT=
Inteno Default
Software

01.30=
Firmware Version.buildnr

Management Overview

The XG684x products support a variety of configuration methods, WEGBUI, XML, TR069, SNMP and basic CLI.
Main configuration interface is the WEBGUI combined with XML configuration through configuration file download.
Inteno Universal Provisioning, IUP, is using DHCP options to redirect a non-configured XG to the management server of choice. Please contact your Inteno support contact or Inteno sales representative for more details on IUP documentation.

IP Communication

XG684x run a DHCP Client internally and will after power on send a DHCP discover on the WAN port in order to get a dynamic IP address from IP network.

If no DHCP server is used in the access network it is possible to configure XG684x from all LAN ports in a static IP address:

192.168.168.1 /255.255.255.0

Configuration Parameter Storage

All configuration parameters in the XG are stored as XML parameters which contains a value.
The parameter value is changeable by all management methods.
No internal classification or priority is used in the configuration.

Last change will be used by XG.

I.e., configuration using SNMP can be combined with WEBGUI configuration.

XG684x will store the configuration in static memory until reset to software factory default settings.

FLASH Memory /Dual bank

The XG have dual image banks for firmware file in the FLASH memory.
The firmware file is loaded into each bank and if one bank fails the other one will be used.

Factory Default / Restore Default

To restore the CPE to default settings in firmware file :

> *Press Reset button and hold for more than 10 sec then release Reset button*
> or
> *Use restore default function in WEBGUI/CLI.*

When the above is done then XG684x will reboot, clear the config and start using firmware default values from last loaded firmware file.

WEB GUI

XG684x have an internal WEBGUI which can be reached on:

> HTTP TCP port 80
> Username= admin
> Password= admin

Both WEBGUI access and password can be changed in configuration if needed.

Three users exists

> admin/admin
> support/support
> user/user

WEBGUI is described more in detail in Appendix1 WEBGUI.

XML Configuration

XG684x can be configured to download a XML based configuration file from a TFTP or HTTP server. The XG684x then at defined interval download the file from the TFTP/HTTP server.

Requirements

- DHCP Server
  - Must supporting standard DHCP Options and DHCP Option43,66,67,128,132
  - DHCP server must be IP reachable from XG684x IP network.
- HTTP Server using port TCP Port 80
- XML Configuration files in HTTP or TFTP server

Description of XML provisioning process

Upon delivery, or restore default, the XG684x use no VLANs and use DHCP for IP allocation.
If the XG6846x receive a DHCP Offer with Option containing IUP configuration data the XG6846 will follow IUP rule set.

By using Inteno Universal Provisioning, IUP, a true plug-and-play auto configuration is possible.
For more details on IUP please check separate Appendix 4.

The XML configuration has some predefined parameters to handle filenames in an efficient way.
One example is the mac parameter what tells the XG6846 to replace the mac with its own MAC address. Another example is ser which means serial nr.

Example
XG684x with MAC 11:22:33:44:55:66 will try to download file “11223445566.conf” if download file is specified as MAC.conf.
This means that each CPE can have its own mac.conf file in TFTP/HTTP server.
If a one-file-to-many type of setup is need the operator can specify one file that should be loaded to all XG6846 in the DHCP options.

The configuration file is a XML file containing parameters and values.

Note:
The XG684x have limited security mechanism for detecting error on the XML configuration so take great care when editing and creating these files.
Best way to create a valid file is to build the configuration in the WEBGUI and then after verification extract the file and then do possible modification.

Important XML Parameters

XmlprovProfileInterval

```
<X_XAVI_COM
_XmlprovProfileInterval>300</X_XAVI_COM_XmlprovProfileInterval>
```

This parameter, value 300 seconds, specify at what interval the XG684x should download the file from TFTP/HTTP server.
(Default value is 300.)

XmlprovVersion

```
<X_XAVI_COM_XmlprovVersion>0.0.1</X_XAVI_COM_XmlprovVersion>
```

This parameter, value 0.0.1, is used by XG684x to know if the configuration is synchronized or not.

If the XG684x download the file and get different XmlprovVersion value than used in running configuration the XG684x will reboot and activate all settings in downloaded file.

If the XmlprovVersion in new file is same as running value nothing happens and CPE consider itself synchronized.

To activate a change in XG684x configuration the version number must be changed in the file and a reboot need to happen to activate new settings.

XML Config File Creation

A good way to create a XML configuration file from start is to use the XG684x built in web interface, configure the settings needed and then extract the configuration to a file.

Work flow to make the XML file

- Login to the web interface and go through all tabs to see what can be configured. (Different software versions might have different configuration options.)
- Change all settings that are required for the setup and save configuration.
- Extract backup file with all settings using Backup function.

Note:
If CPE Management VLAN is changed, the XG684x will reboot on save to activate new VLAN.
All other parameters/settings in the CPE are used directly on save. No reboot is needed.

Firmware Upgrade

XG684x can be upgraded through the XML configuration.
If X_XAVI_COM_XmlprovFWUrlparameter exists in the XML the XG6846 will download the firmware from HTTP server if the running firmware version is different.
The firmware download will start randomly between 5-120 sec after XML file have been loaded and parameter been received.
Only HTTP protocol is supported for firmware upgrade.

X_XAVI_COM_XmlprovFWUrl
<X_XAVI_COM_XmlprovFWUrl>**192.168.10.201, XG6846_4.12ITT01.30_20130322**
</X_XAVI_COM_XmlprovFWUrl>

In this example

Firmware	XG6846_4.12ITT01.30_20130322
HTTP server	192.168.10.201

Note that , is used in this parameter and not /.

3DES Encryption

The XML configuration file can be encrypted using 3DES if higher security is required.
All XG6846 PCB boards have an preconfigured unique 3DES keys installed at production.
3DES keys can be retrieved from your Inteno logistics or from your Inteno sales contact.

The encryption is 3DES using no salt and no IV.
The 3DES key must be converted to hex format.

Examples of how-to create 3DES encryption of config file in Linux server:

Example of a bash script called encrypt on Linux

```
-----encrypt----------
#!/bin/bash
KEY=`echo $1 |xxd–p’;
opensslenc-e -des-ede -nosalt -K $KEY -iv "0000000000000000" -in $2 -out $3;
--------------------------
```

Run the script with argument

```
./encrypt <3DES key> <txt based XML file> <output file, 3des encrypted> <enter>
```

TR-069

XG6846 support management using Broadband forum TR-069.
For more info on TR069 configuration please check TR069 part in Appendix 1 WEBGUI.

Simple Network Management Protocol, SNMP

SNMP Version 1, 2 can be used to read/write configuration in XG6846 MIB file.
Standard MIB2 is supported which can be used for WAN/LAN port statistics.
Most configuration options are available through 684x MIB file including FW upgrade.
If SNMP MIB is needed for configuration please contact you sales representative.

Command Line Interface, CLI

XG6846 have a CLI which be accessed through TELNET or SSH.
The CLI interface use same username/passwords as WEBGUI.

Usable commands:

?	Display command list
swversion show	Display running sw version
ifconfig	Show Interface information
restoredefault	Complete reset to factory default settings

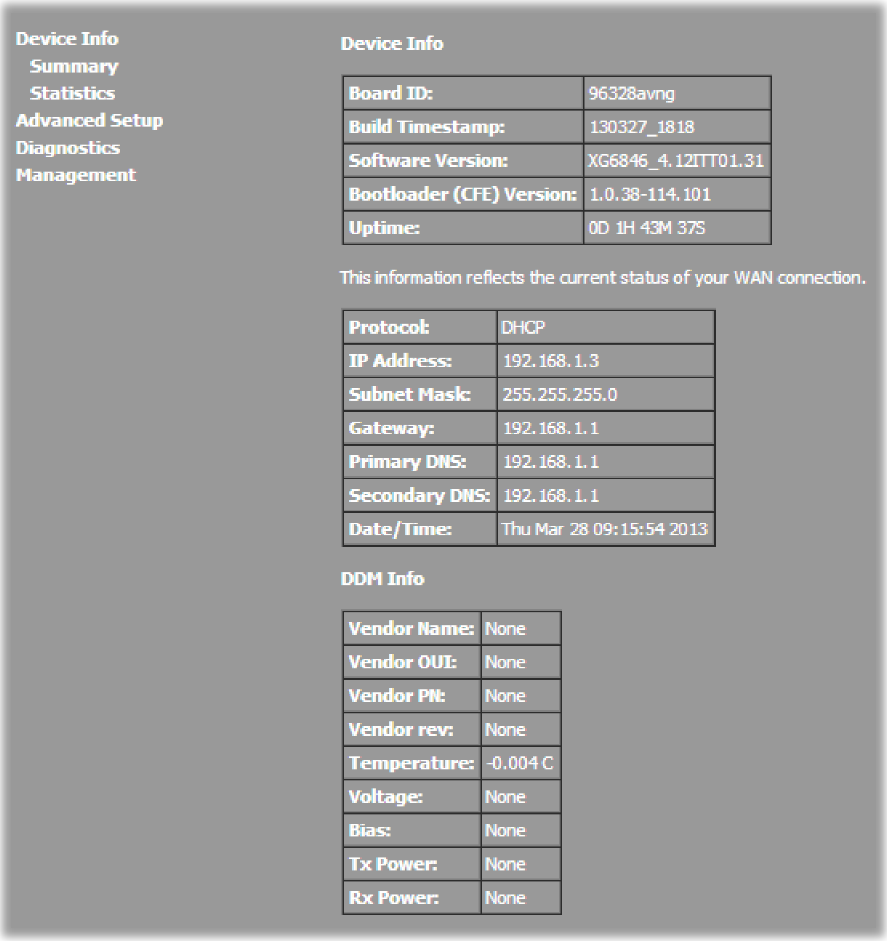
Firmware Upgrade

```
>sh<enter>
# tftpbcm -g -t i -f <Firmware file><TFTP server IP>
```

Note:
The CLI is not intended to be used for management purpose and should only be used by advanced users.

Appendix 1
WEBGUI

Device Info



Device Info

Board ID:	96328avng
Build Timestamp:	130327_1818
Software Version:	XG6846_4.12ITT01.31
Bootloader (CFE) Version:	1.0.38-114.101
Uptime:	0D 1H 43M 37S

This information reflects the current status of your WAN connection.

Protocol:	DHCP
IP Address:	192.168.1.3
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
Primary DNS:	192.168.1.1
Secondary DNS:	192.168.1.1
Date/Time:	Thu Mar 28 09:15:54 2013

DDM Info

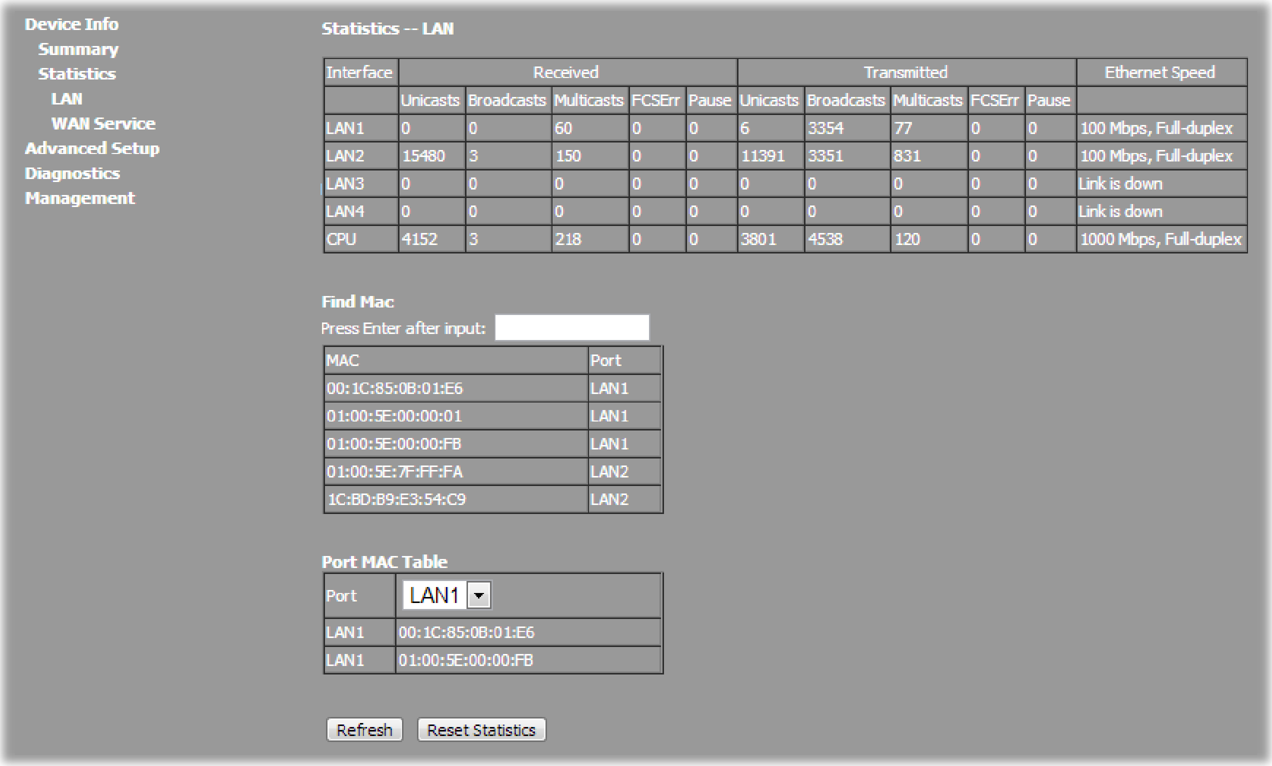
Vendor Name:	None
Vendor OUI:	None
Vendor PN:	None
Vendor rev:	None
Temperature:	-0.004 C
Voltage:	None
Bias:	None
Tx Power:	None
Rx Power:	None

Figure 1

Board ID	HW Board ID
Build Timestamp	Firmware build information
Software Version	Software/firmware version number
Bootloader (CFE) Version	Startup program version
Uptime	Time since last reboot in days, hours and minutes
Protocol	DHCP or Static IP address
IP Address	IP address used for management
Subnet mask	Subnet mask
Gateway	IP Gateway received through DHCP or statically configured
Primary DNS	DNS Server
Secondary DNS	Backup DNS server
Date/Time	If NTP server is used real time will be display.
DDM Info	Digital Diagnostics Monitoring (Values taken from SFP)

Vendor Name	Vendor Name
Vendor OUI	Vendor OUI Number
Vendor PN	Vendor Product Number
Vendor rev	Vendor Revision
Temperature	Temperature inside SFP
Voltage	Voltage level
Bias	Bias Value
TX Power	Transmit power in dbm
RX Power	Receive power in dbm

Port Statistics LAN



Statistics -- LAN

Interface	Received					Transmitted					Ethernet Speed
	Unicasts	Broadcasts	Multicasts	FCSErr	Pause	Unicasts	Broadcasts	Multicasts	FCSErr	Pause	
LAN1	0	0	60	0	0	6	3354	77	0	0	100 Mbps, Full-duplex
LAN2	15480	3	150	0	0	11391	3351	831	0	0	100 Mbps, Full-duplex
LAN3	0	0	0	0	0	0	0	0	0	0	Link is down
LAN4	0	0	0	0	0	0	0	0	0	0	Link is down
CPU	4152	3	218	0	0	3801	4538	120	0	0	1000 Mbps, Full-duplex

Find Mac

Press Enter after input:

MAC	Port
00:1C:85:0B:01:E6	LAN1
01:00:5E:00:00:01	LAN1
01:00:5E:00:00:FB	LAN1
01:00:5E:7F:FF:FA	LAN2
1C:BD:B9:E3:54:C9	LAN2

Port MAC Table

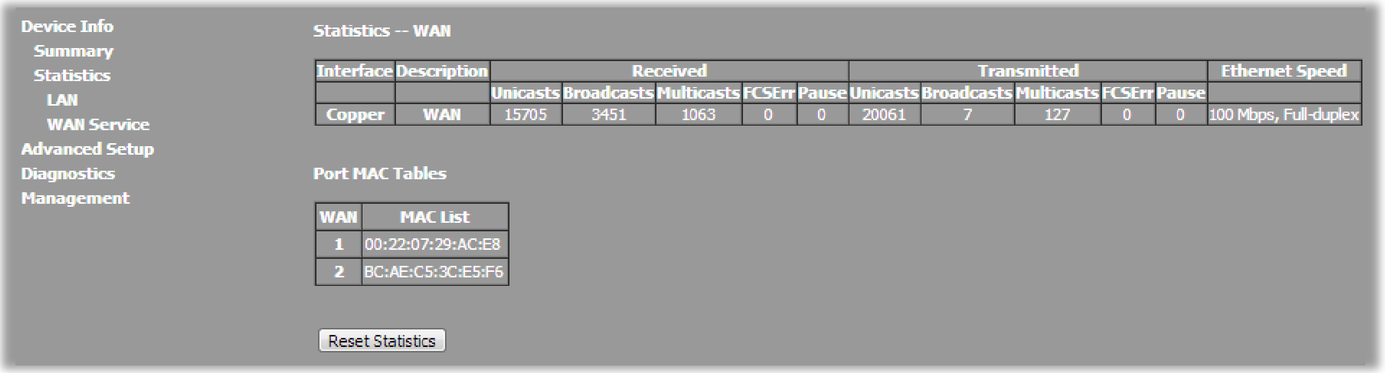
Port	LAN1
LAN1	00:1C:85:0B:01:E6
LAN1	01:00:5E:00:00:FB

Figure 2

The statistics view shows all LAN interfaces link status and counters per RX/TX.
XG6846 can display known MAC addresses per LAN port and also find/return port for specific MAC address.

Unicast	Unicast packet
Broadcast	Broadcast packet
Multicast	Multicast packet
FCSErr	Error frames
Pause	802.1 Pause frames
Ethernet Speed	Negotiated Ethernet Duplex/Speed
CPU	Ethernet Port towards CPU
LAN1-5	LAN1-4 and LAN5=EXT1

Port Statistics WAN



Statistics -- WAN

Interface	Description	Received					Transmitted					Ethernet Speed
		Unicasts	Broadcasts	Multicasts	FCSErr	Pause	Unicasts	Broadcasts	Multicasts	FCSErr	Pause	
Copper	WAN	15705	3451	1063	0	0	20061	7	127	0	0	100 Mbps, Full-duplex

Port MAC Tables

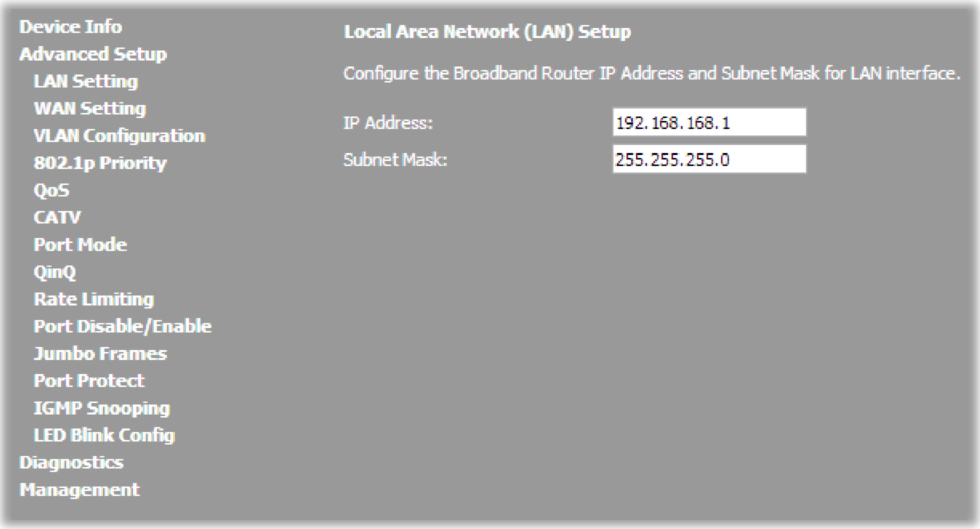
WAN	MAC List
1	00:22:07:29:AC:E8
2	BC:AE:C5:3C:E5:F6

Figure 4

The statistics view shows all WAN interfaces link status and counters per RX/TX.
XG6846 can display known MAC addresses on WAN port and also find/return port for specific MAC address.

Table format is same as for LAN port above.

Advanced Setup->LAN Setting



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface.

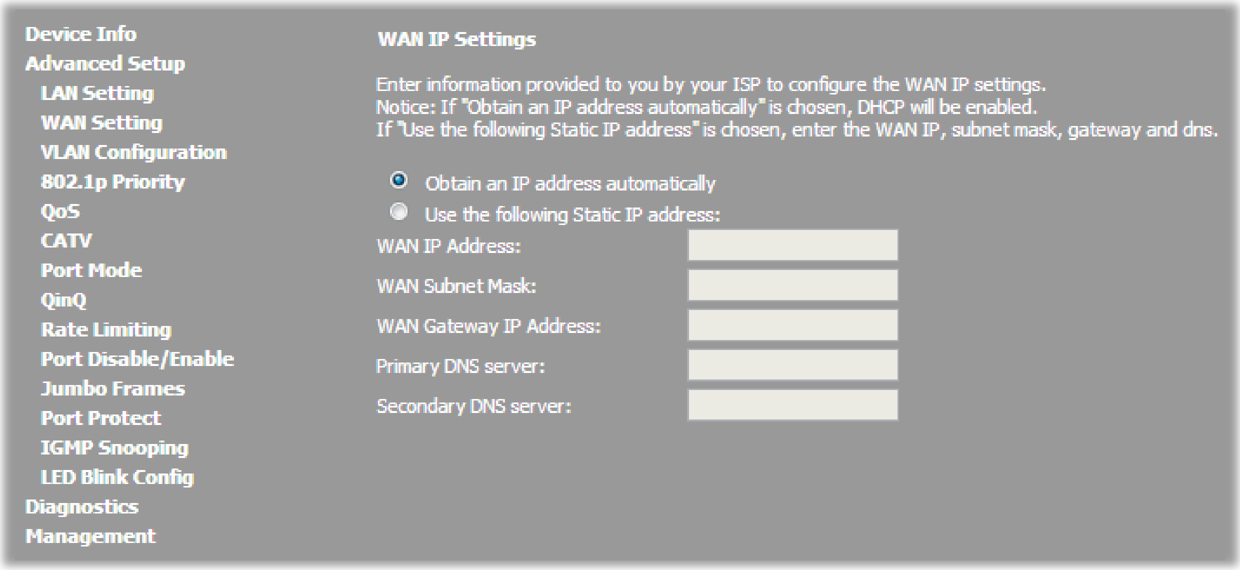
IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

Figure 5

IP Address	Static IP address in XG
Subnet Mask	Subnet mask

Advanced Setup->WAN Settings



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled.
If "Use the following Static IP address" is chosen, enter the WAN IP, subnet mask, gateway and dns.

● Obtain an IP address automatically
○ Use the following Static IP address:

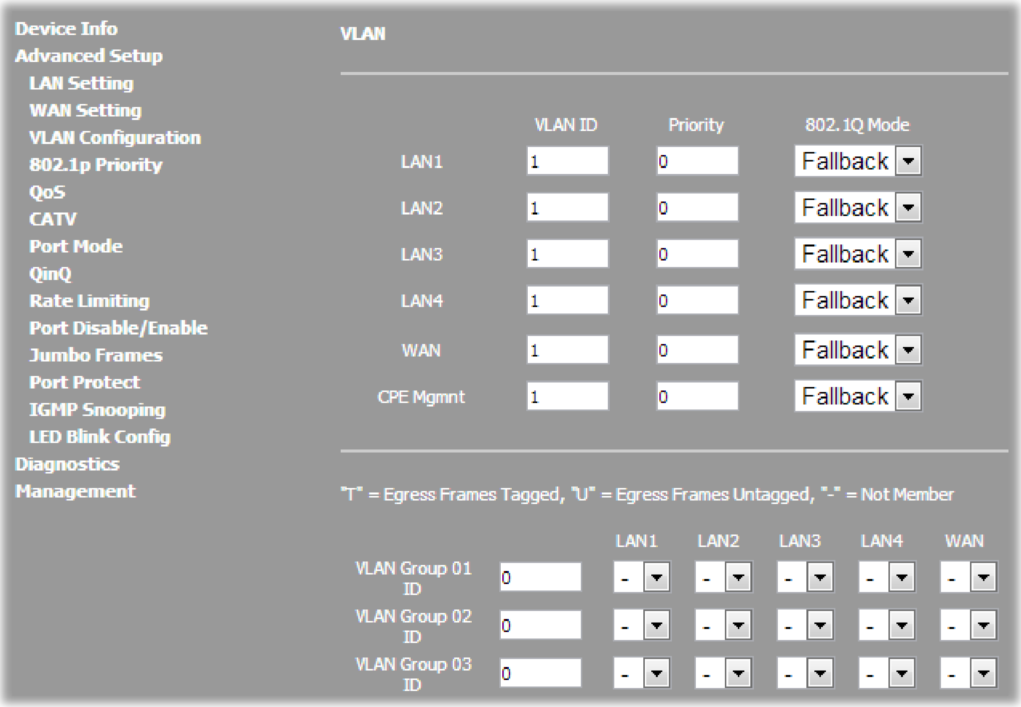
WAN IP Address:
WAN Subnet Mask:
WAN Gateway IP Address:
Primary DNS server:
Secondary DNS server:

Figure 6

This setting configure how the XG Management IP should be configured.
DHCP or statically assigned IP.

WAN IP Address	Static WAN IP address in XG used for management
Subnet Mask	Subnet mask
WAN Gateway IP Address	Gateway
Primary DNS Server	Primary DNS Server
Secondary DNS Server	Secondary DNS Server

Advanced Setup->VLAN Configuration



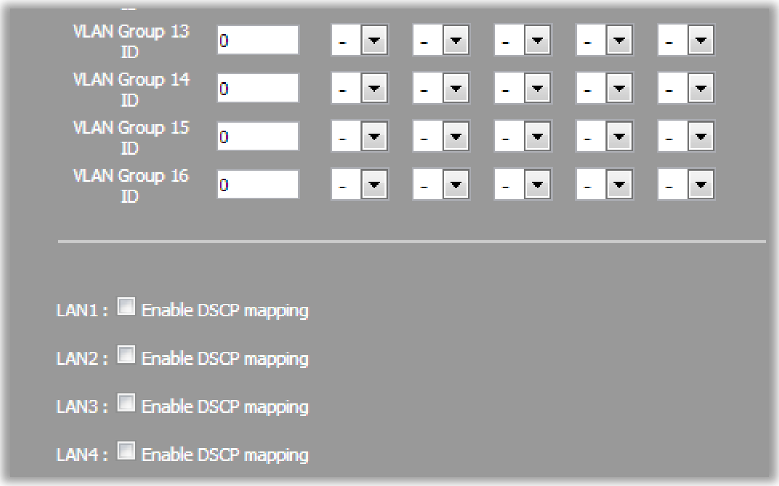
VLAN

	VLAN ID	Priority	802.1Q Mode
LAN1	1	0	Fallback
LAN2	1	0	Fallback
LAN3	1	0	Fallback
LAN4	1	0	Fallback
WAN	1	0	Fallback
CPE Mgmnt	1	0	Fallback

"T" = Egress Frames Tagged, "U" = Egress Frames Untagged, "-" = Not Member

		LAN1	LAN2	LAN3	LAN4	WAN
VLAN Group 01 ID	0	-	-	-	-	-
VLAN Group 02 ID	0	-	-	-	-	-
VLAN Group 03 ID	0	-	-	-	-	-

Figure 7



VLAN Group 13 ID	0	-	-	-	-	-
VLAN Group 14 ID	0	-	-	-	-	-
VLAN Group 15 ID	0	-	-	-	-	-
VLAN Group 16 ID	0	-	-	-	-	-

LAN1 : □ Enable DSCP mapping

LAN2 : □ Enable DSCP mapping

LAN3 : □ Enable DSCP mapping

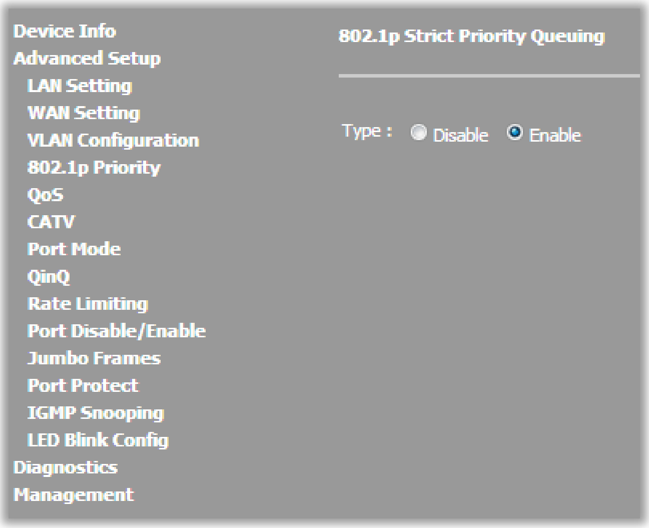
LAN4 : □ Enable DSCP mapping

Figure 8

The VLAN configuration can be split into three parts as can be seen in above figures.
First part of the configuration defines VLAN ID and priority for Ingress untagged frames per port.
The second part, VLAN Group, define VLAN ID and how the VLAN should exist logically per port. (T=tagged, U=Untagged, -=not member)
The third part defines if DSCP QoS mapping should be use on the LAN port.
A complete VLAN configuration example can be found in Appendix 2 VLAN Configuration Example

VLAN ID	Port PVID. Ingress untagged frames will be tagged with this VLAN before entering switch fabric
Priority	VLAN Priority added to ingress ingress traffic on the port.
802.1Q Mode	Configure how L2 switch should handle unknown ingress VLAN frames. When using service VLANs Secure Mode is recommended. For more details check Appendix 3.
CPE Mgmnt	CPE Management VLAN
VLAN Group X ID	Configuration for the VLAN group. Configure on what ports the VLAN should exists, tagged ,untagged or non member. (U,T,-)
LAN X Enable DSCP Mapping	Enable QoS per port using DiffServ Code Point

Advanced Setup->Strict Priority Queuing



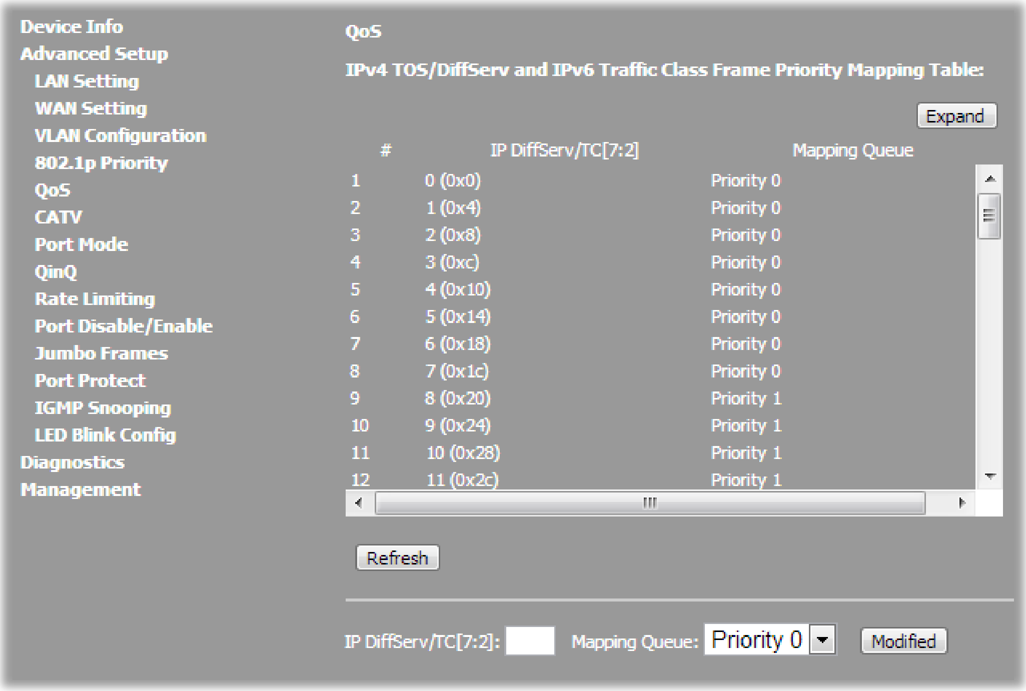
802.1p Strict Priority Queuing

Type : ○ Disable ● Enable

Figure 9

The XG is default using strict priority queuing for the 4 HW queues.
The setting can be enabled or disabled.
If disabled QoS priority mapping will revert to WFQ type.

Advanced Setup->QoS



QoS

IPv4 TOS/DiffServ and IPv6 Traffic Class Frame Priority Mapping Table:

#	IP DiffServ/TC[7:2]	Mapping Queue
1	0 (0x0)	Priority 0
2	1 (0x4)	Priority 0
3	2 (0x8)	Priority 0
4	3 (0xc)	Priority 0
5	4 (0x10)	Priority 0
6	5 (0x14)	Priority 0
7	6 (0x18)	Priority 0
8	7 (0x1c)	Priority 0
9	8 (0x20)	Priority 1
10	9 (0x24)	Priority 1
11	10 (0x28)	Priority 1
12	11 (0x2c)	Priority 1

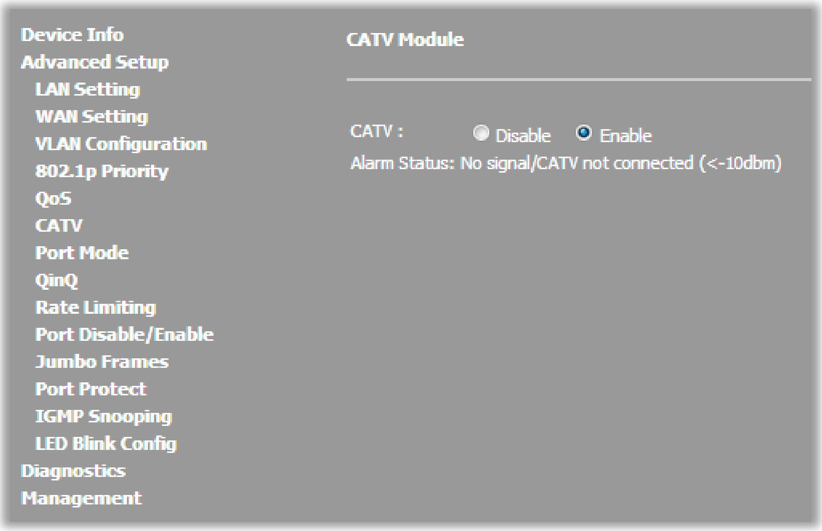
IP DiffServ/TC[7:2]: Mapping Queue: Priority 0

Figure 10

Only used if Enable DSCP Mapping is activated on port in VLAN Configuration tab.

# 1-64	Configure DSCP for QoS
IP DiffServ/ToS [7:2]	Predefined DSCP/TOS values
Mapping Queue	DSCP/TOS mapping towards Queue’s
IP DiffServ TC /Priority 0-3	Configuration/Modification of predefined QoS DSCP

Advanced Setup->CATV Module



CATV Module

CATV : ○ Disable ● Enable

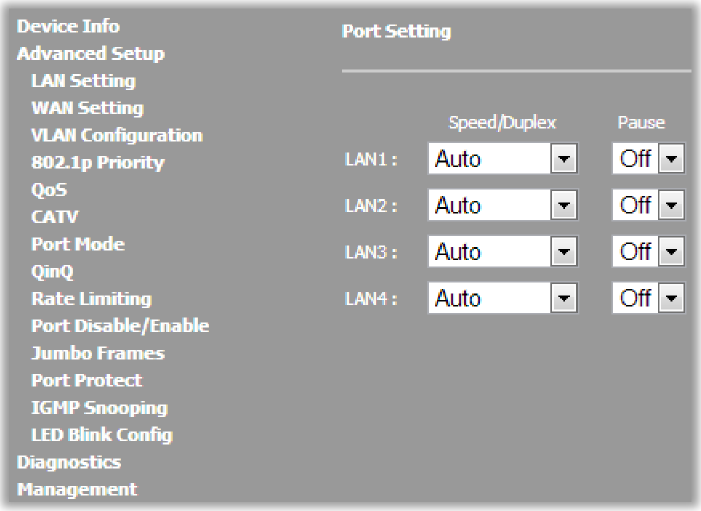
Alarm Status: No signal/CATV not connected (<-10dbm)

Figure 11

The XG6846 can remotely enable/disable the CATV Module through configuration and also send SYSLOG messages if CATV Input power goes from High to Low.

CAT Module Disable/Enable	Enable/Disable CATV Module in Fiber Tray
Alarm Status	Alarm threshold is -10dbm in CATV input

Advanced Setup->Port Mode



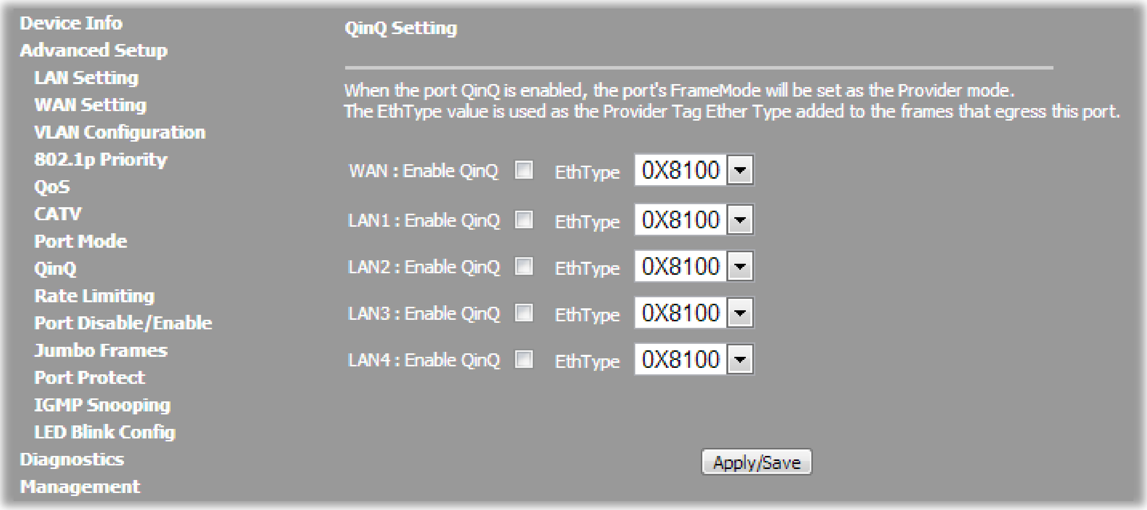
Port Setting

	Speed/Duplex	Pause
LAN1 :	Auto	Off
LAN2 :	Auto	Off
LAN3 :	Auto	Off
LAN4 :	Auto	Off

Figure 12

Port Setting LANx Speed/Duplex	Auto – Auto negotiation of Ethernet Link speed/Duplex 10HD Fixed 10 Mbit/s Half Duplex 10FD Fixed 10 Mbit/s Full Duplex 100HD Fixed 100 Mbit/s Half Duplex 100FD Fixed 100 Mbit/s Full Duplex
Pause	802.1 PAUSE Frames/Flow Control ON/OFF

Advanced Setup->QinQ Mode



QinQ Setting

When the port QinQ is enabled, the port's FrameMode will be set as the Provider mode.
The EthType value is used as the Provider Tag Ether Type added to the frames that egress this port.

WAN : Enable QinQ □ EthType 0X8100

LAN1 : Enable QinQ □ EthType 0X8100

LAN2 : Enable QinQ □ EthType 0X8100

LAN3 : Enable QinQ □ EthType 0X8100

LAN4 : Enable QinQ □ EthType 0X8100

Figure 13

WAN/LAN Enable QinQ	Enable/Disable QinQ per port
EthType	QinQ Outer Ethernet Type tag 0x8100 – (Default value) 0x9100

Example Configuration for QinQ setup

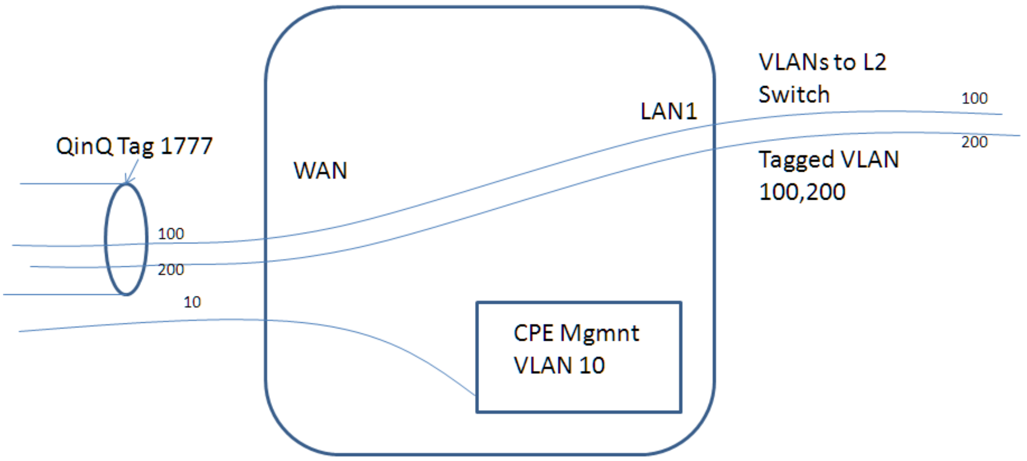
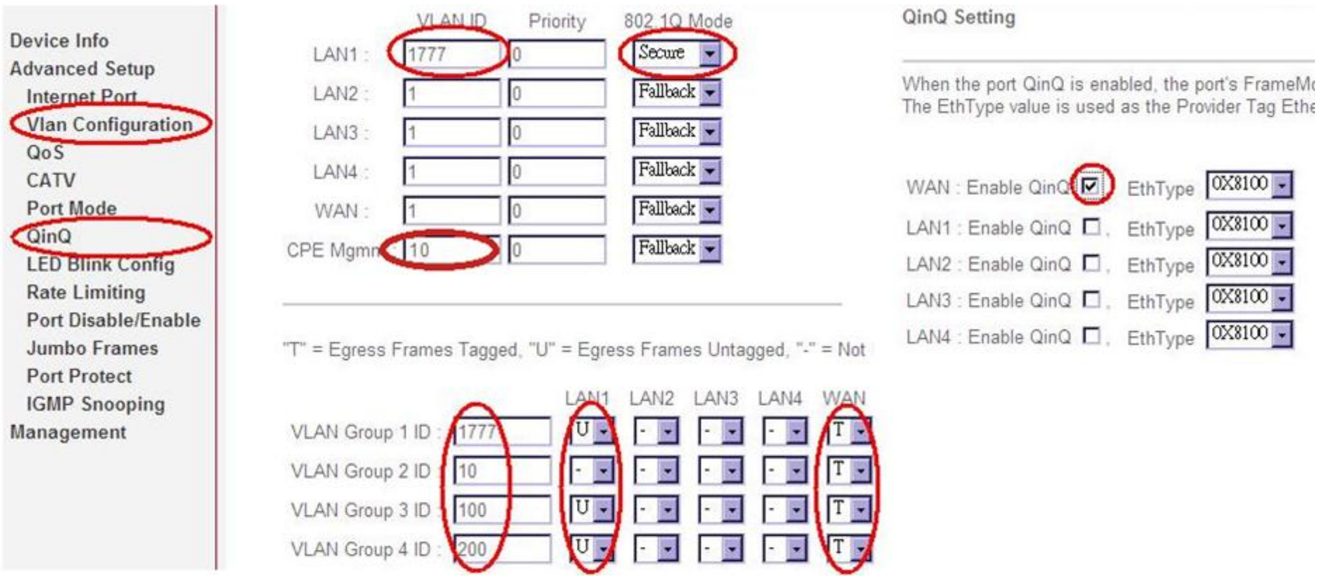


Figure 14



	VLAN ID	Priority	802.1Q Mode
LAN1 :	1777	0	Secure
LAN2 :	1	0	Fallback
LAN3 :	1	0	Fallback
LAN4 :	1	0	Fallback
WAN :	1	0	Fallback
CPE Mgmn	10	0	Fallback

"T" = Egress Frames Tagged, "U" = Egress Frames Untagged, "-" = Not

		LAN1	LAN2	LAN3	LAN4	WAN
VLAN Group 1 ID :	1777	U	-	-	-	T
VLAN Group 2 ID :	10	-	-	-	-	T
VLAN Group 3 ID :	100	U	-	-	-	T
VLAN Group 4 ID :	200	U	-	-	-	T

QinQ Setting

When the port QinQ is enabled, the port's FrameMo
The EthType value is used as the Provider Tag Ethe

WAN : Enable QinQ ☑ EthType 0X8100
LAN1 : Enable QinQ □ , EthType 0X8100
LAN2 : Enable QinQ □ , EthType 0X8100
LAN3 : Enable QinQ □ , EthType 0X8100
LAN4 : Enable QinQ □ , EthType 0X8100

Figure 15 (Picture from XG6746)

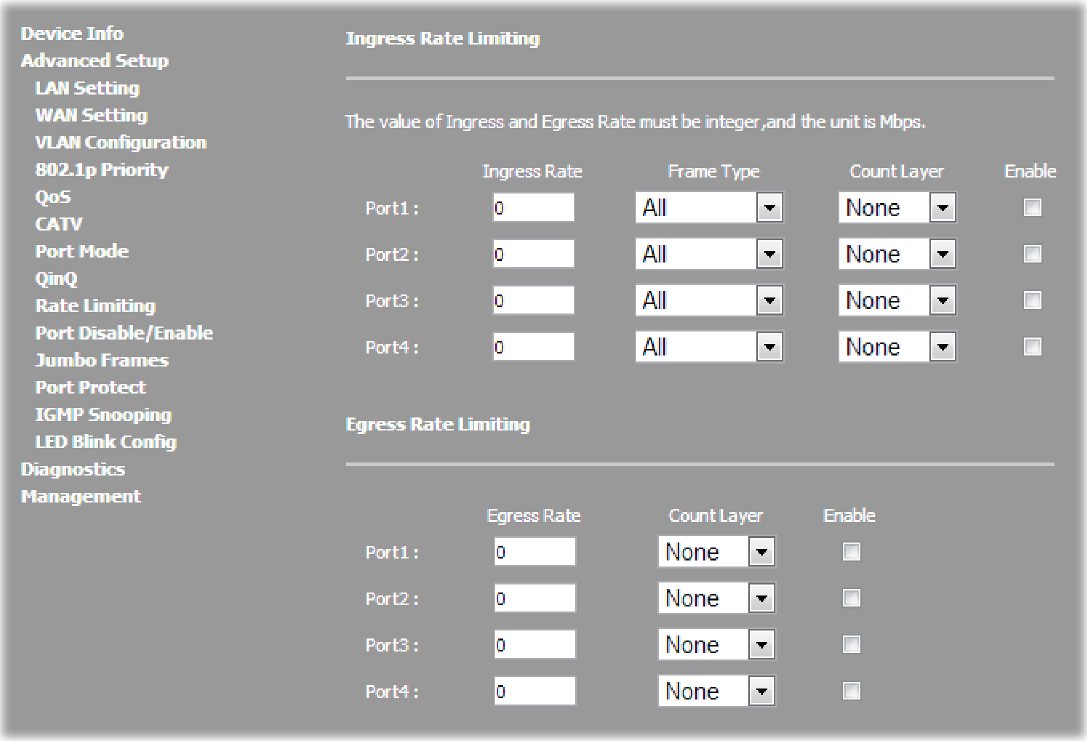
802.1Q Mode Secure

VLANs defined in VLAN Group is only allowed to traverse inside the QinQ tunnel. All other VLANs will be dropped.

802.1Q Mode Disabled

All VLAN can traverse inside the QinQ tunnel.

Advanced Setup->Rate Limiting



Ingress Rate Limiting

The value of Ingress and Egress Rate must be integer ,and the unit is Mbps.

	Ingress Rate	Frame Type	Count Layer	Enable
Port1 :	0	All	None	□
Port2 :	0	All	None	□
Port3 :	0	All	None	□
Port4 :	0	All	None	□

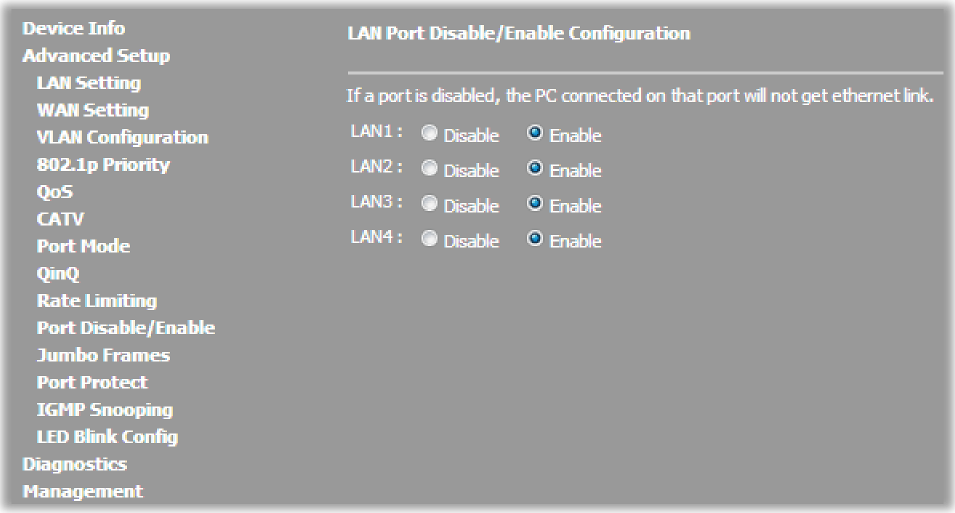
Egress Rate Limiting

	Egress Rate	Count Layer	Enable
Port1 :	0	None	□
Port2 :	0	None	□
Port3 :	0	None	□
Port4 :	0	None	□

Figure 16

Ingress Rate Port x	Bandwidth allowed to ingress (received) the port per sec in steps of Mbit/s. Ex 1 => 1 Mbit/s is allowed to ingress LAN port / sec. 0.1 or 25.5 is not allowed.
Ingress Frame Type Port x	Frame type to apply rate limiting on. All- Use RL on all traffic on the port Unicast- Use RL only for Unicast packets Multicast- Use RL only for Multicast traffic Broadcast- Use RL only for Broadcast.
Ingress Count Layer x	Calculate RL bandwidth per OSI Layer payload
Ingress Enable Port x	Enable/Disable RL per port
Egress Rate Port x	Bandwidth allowed to egress (output) the port per sec in steps of Mbit/s.
Egress Count Layer x	Calculate RL bandwidth based on OSI Layer payload
Egress Enable Port x	Enable/Disable RL per port

Advanced Setup->Port Enable/Disable



LAN Port Disable/Enable Configuration

If a port is disabled, the PC connected on that port will not get ethernet link.

LAN1 : ○ Disable ● Enable

LAN2 : ○ Disable ● Enable

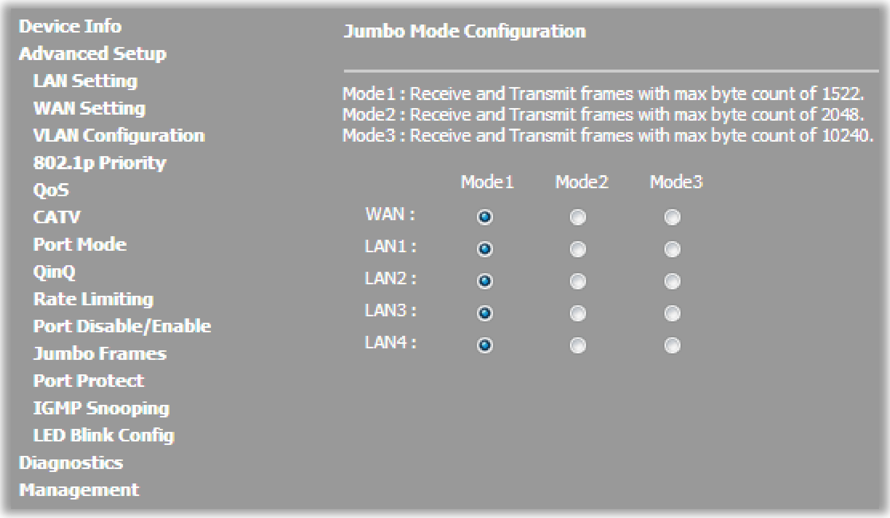
LAN3 : ○ Disable ● Enable

LAN4 : ○ Disable ● Enable

Figure 17

LAN X Port Disable/Enable	Disabled- Devices connected on LAN port will not get Ethernet link. Enable- Device connected will get Ethernet link

Advanced Setup->Jumbo Frames



Jumbo Mode Configuration

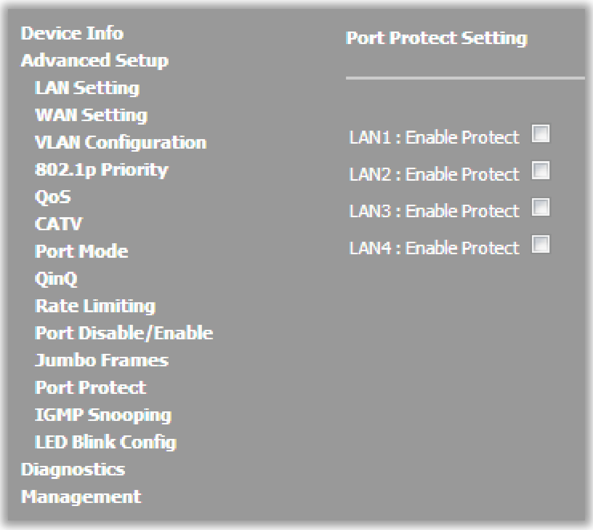
Mode1 : Receive and Transmit frames with max byte count of 1522.
Mode2 : Receive and Transmit frames with max byte count of 2048.
Mode3 : Receive and Transmit frames with max byte count of 10240.

	Mode1	Mode2	Mode3
WAN :	●	○	○
LAN1 :	●	○	○
LAN2 :	●	○	○
LAN3 :	●	○	○
LAN4 :	●	○	○

Figure 18

Jumbo Mode Configuration WAN/LANx	Configure what Jumbo frame size should be allowed per port Mode1 – Max Frame Size 1522 (Default Value) Mode2 – Mac Frame Size 2048 Mode3 - Mac Frame Size 10240

Advanced Setup->Port Protect



Port Protect Setting

LAN1 : Enable Protect □

LAN2 : Enable Protect □

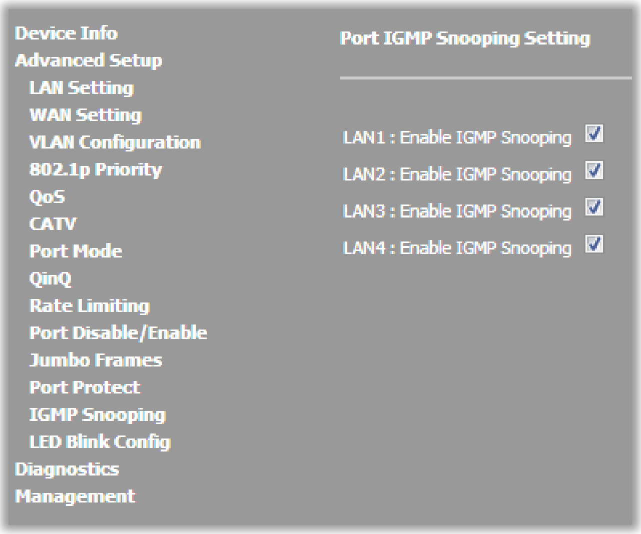
LAN3 : Enable Protect □

LAN4 : Enable Protect □

Figure 19

Port Protect Setting LAN1	If Port Protect is enabled on a LAN port then LAN port hosts will not be able to communicate to other LAN port. If enabled traffic is only allowed between WAN and LAN port.

Advanced Setup->IGMP Snooping



Port IGMP Snooping Setting

LAN1 : Enable IGMP Snooping ☑

LAN2 : Enable IGMP Snooping ☑

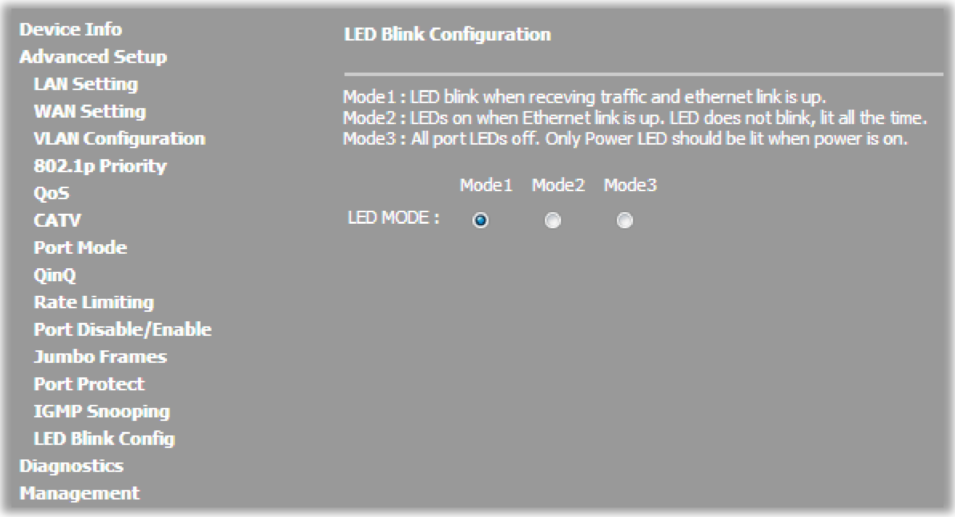
LAN3 : Enable IGMP Snooping ☑

LAN4 : Enable IGMP Snooping ☑

Figure 20

Port IGMP Snooping Settings LAN c	Enables IGMP Snooping per port. Default enabled on all LAN ports. Enable if more than multicast 2 STB is used within one VLAN.

Advanced Setup->LED Blink Configuration



LED Blink Configuration

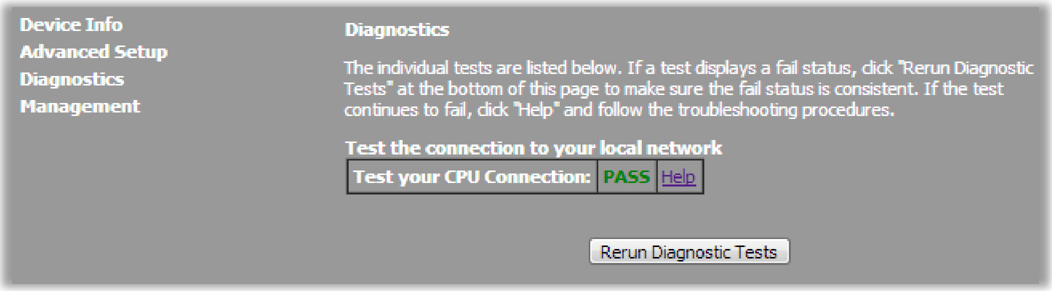
Mode1 : LED blink when receving traffic and ethernet link is up.
Mode2 : LEDs on when Ethernet link is up. LED does not blink, lit all the time.
Mode3 : All port LEDs off. Only Power LED should be lit when power is on.

LED MODE : ● Mode1 ○ Mode2 ○ Mode3

Figure 21

LED MODE	LED Blink Mode Mode1- LED Blink when receiving traffic on port and Ethernet link is up on the port. (Default value) Mode2-No LED Blink. LED lit all the time if Ethernet link is up. Mode3- LED disabled. Only PWR LED is lit, all LAN LEDS disabled.

Diagnostics



Diagnostics

The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

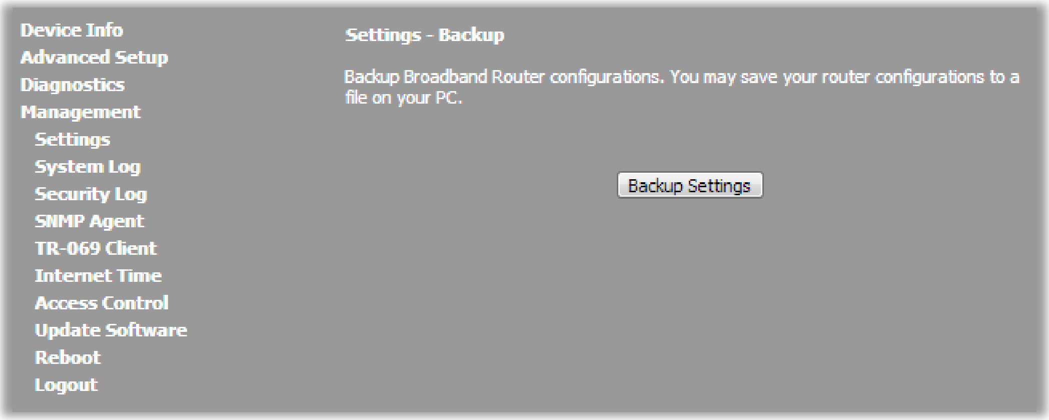
Test your CPU Connection:	PASS	Help

Figure 22

Under diagnostics tools be bee added which helps troubleshooting.
Note: When this manual was made the features was not yet developed.

TBD	TBD

Management->Settings->Backup



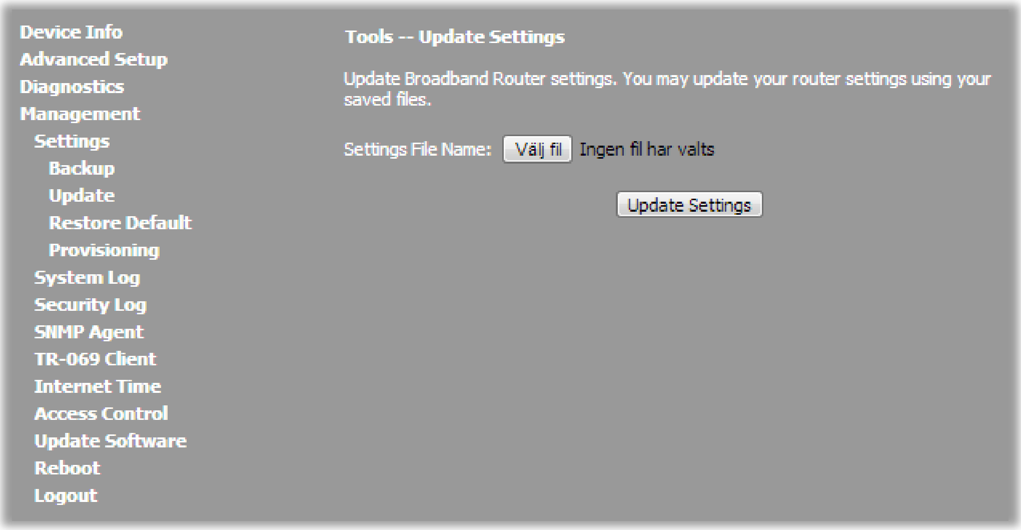
Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Figure 23

Backup	Extract running configuration in XML format.

Management->Settings->Update



Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

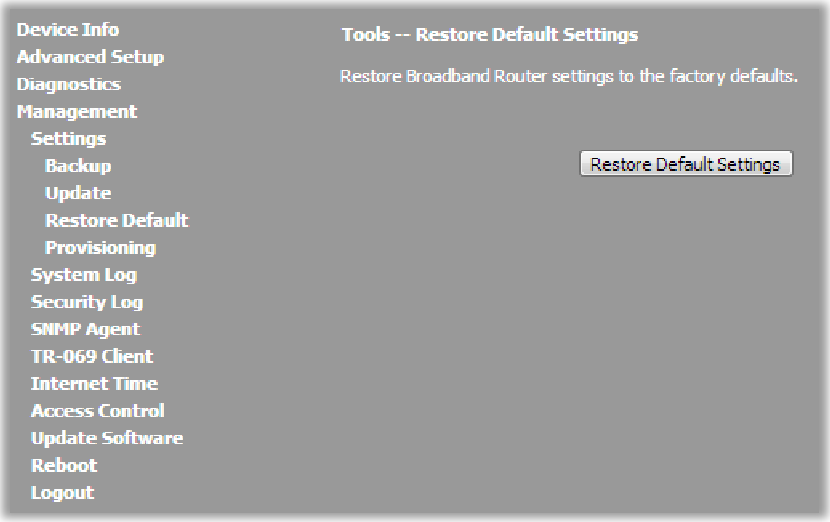
Settings File Name: Välj fil Ingen fil har valts

Update Settings

Figure 24

Settings File name	Select the XML file and press Update Settings buton to load the configuration file to the XG6846. The XG6846 will reboot and use new settings in uploaded file.

Management->Settings->Restore Default



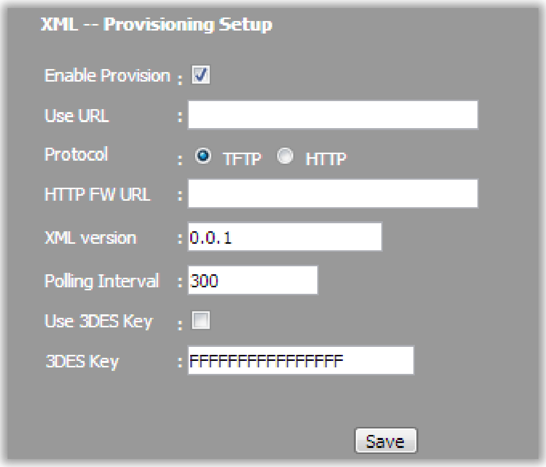
Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Figure 25

Restore Default Settings	Pressing the button will cause the XG6846 to clear all configuration settings , reboot and read all the settings from the loaded firmware file.

Management->Settings-> Provisioning



XML -- Provisioning Setup

Enable Provision : ☑

Use URL :

Protocol : ● TFTP ○ HTTP

HTTP FW URL :

XML version : 0.0.1

Polling Interval : 300

Use 3DES Key : □

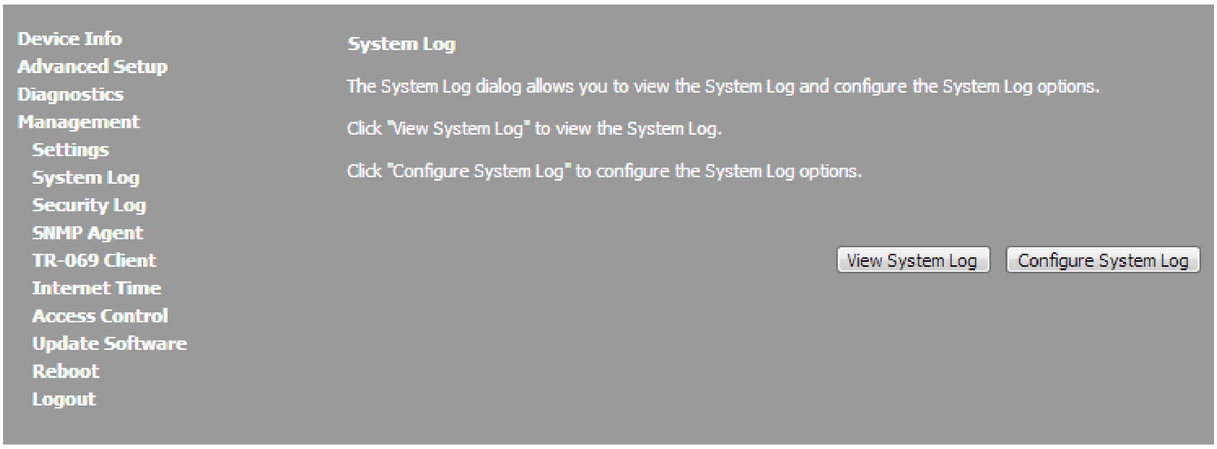
3DES Key : FFFFFFFFFFFFFFFF

Figure 26

This tab configures how the CPE should use XML configuration file based provisioning.

Enable Provisioning	Enable XML configuration file type of provisioning
Use URL	URL to TFTP server or HTTP server where the XML configuration file can be downloaded by CPE. Format is <FQDN/IP>,<file.conf> Example 1.2.3.4,112233445566.conf
Protocol	TFTP CPE will download XML file using TFTP HTTP CPE will download XML file using HTTP
HTTP FW URL	Firmware Download URL Firmware upgrade is only supported using HTTP protocol HTTP format is <URL>,<Filename>
XML Version	XML Synchronization flag If different from downloaded XML file CPE consider last downloaded file to have new configuration. CPE will reboot and then use setting in downloaded XML file
Polling Interval	Time in sec between download of configuration file Default 300 sec
Use 3DES Key	If enabled the XML config file must be encrypted with same 3DES key as being in use by CPE.
3DESKey	fffffffff => Use the 3DES key on PCB It is possible to use a static 3DESkey for all CPEs by configuring the key in this field. Important : Use 16 characters in the 3DESKEY

Management->System Log



System Log

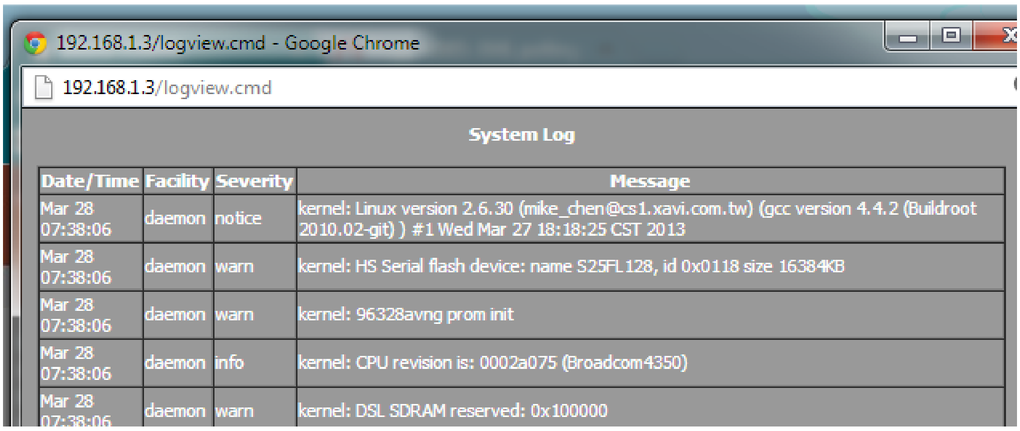
The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

Figure 27

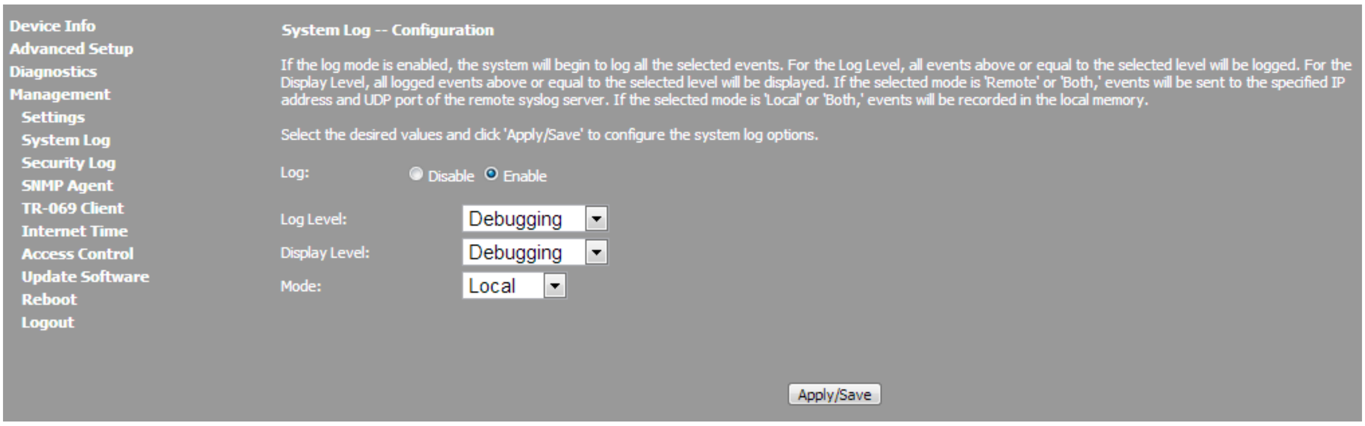
XG6846 have internal logging possibility and also SYSLOG reporting to IP destination. Internal log is stored in RAM and reboot/power off clear the log.



System Log

Date/Time	Facility	Severity	Message
Mar 28 07:38:06	daemon	notice	kernel: Linux version 2.6.30 (mike_chen@cs1.xavi.com.tw) (gcc version 4.4.2 (Buildroot 2010.02-git)) #1 Wed Mar 27 18:18:25 CST 2013
Mar 28 07:38:06	daemon	warn	kernel: HS Serial flash device: name S25FL128, id 0x0118 size 16384KB
Mar 28 07:38:06	daemon	warn	kernel: 96328avng prom init
Mar 28 07:38:06	daemon	info	kernel: CPU revision is: 0002a075 (Broadcom4350)
Mar 28 07:38:06	daemon	warn	kernel: DSL SDRAM reserved: 0x100000

Figure 28 View System log



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ○ Disable ● Enable

Log Level: Debugging

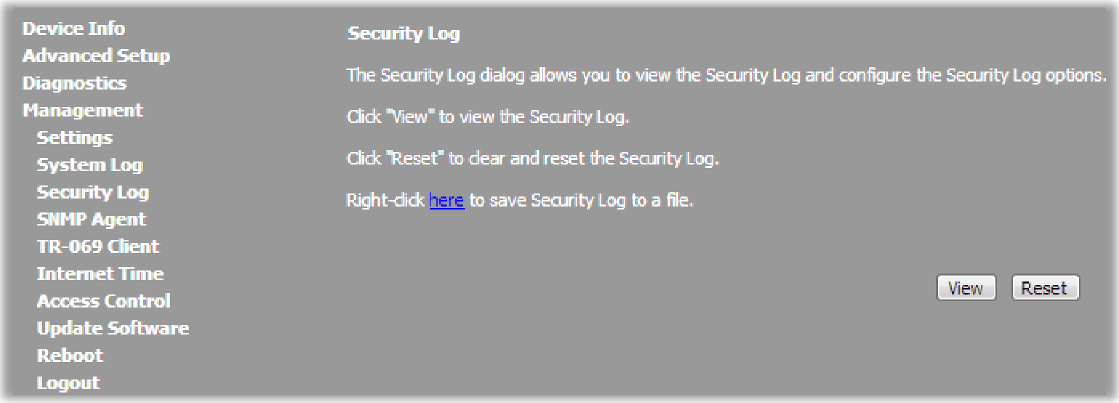
Display Level: Debugging

Mode: Local

Figure 29 Configuration System Log

Log	Enable or Disable logging (Default OFF)
Log Level	SYSLOG Log Level. Select debug for maximum log level
Mode	Local Log stored only in XG Remote Log send to SYSLOG server Both Log stored locally and sent to SYSLOG server
Server IP Address	SYSLOG server IP
Server UDP Port	SYSLOG Server UDP port (default port 514)

Management->Security Log



Security Log

The Security Log dialog allows you to view the Security Log and configure the Security Log options.

Click "View" to view the Security Log.

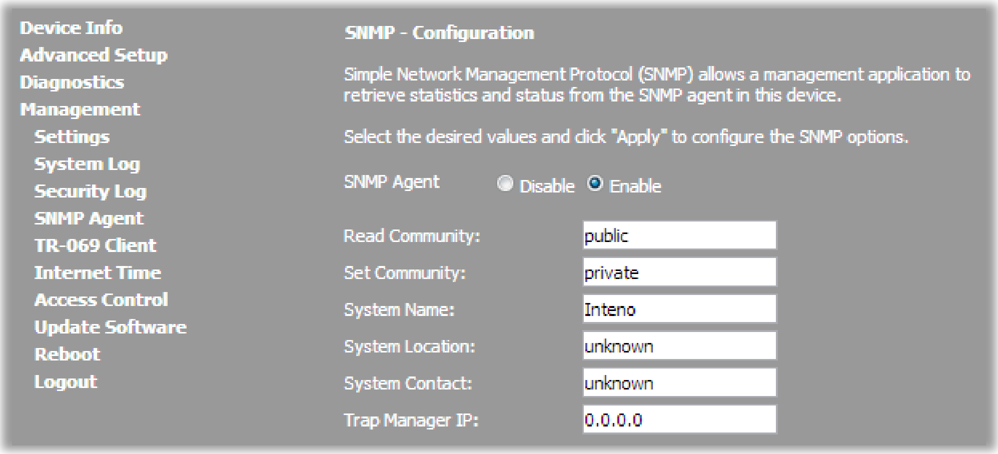
Click "Reset" to clear and reset the Security Log.

Right-click here to save Security Log to a file.

Figure 30

Reserved for future use.

Management->SNMP Agent



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ○ Disable ● Enable

Read Community: public

Set Community: private

System Name: Inteno

System Location: unknown

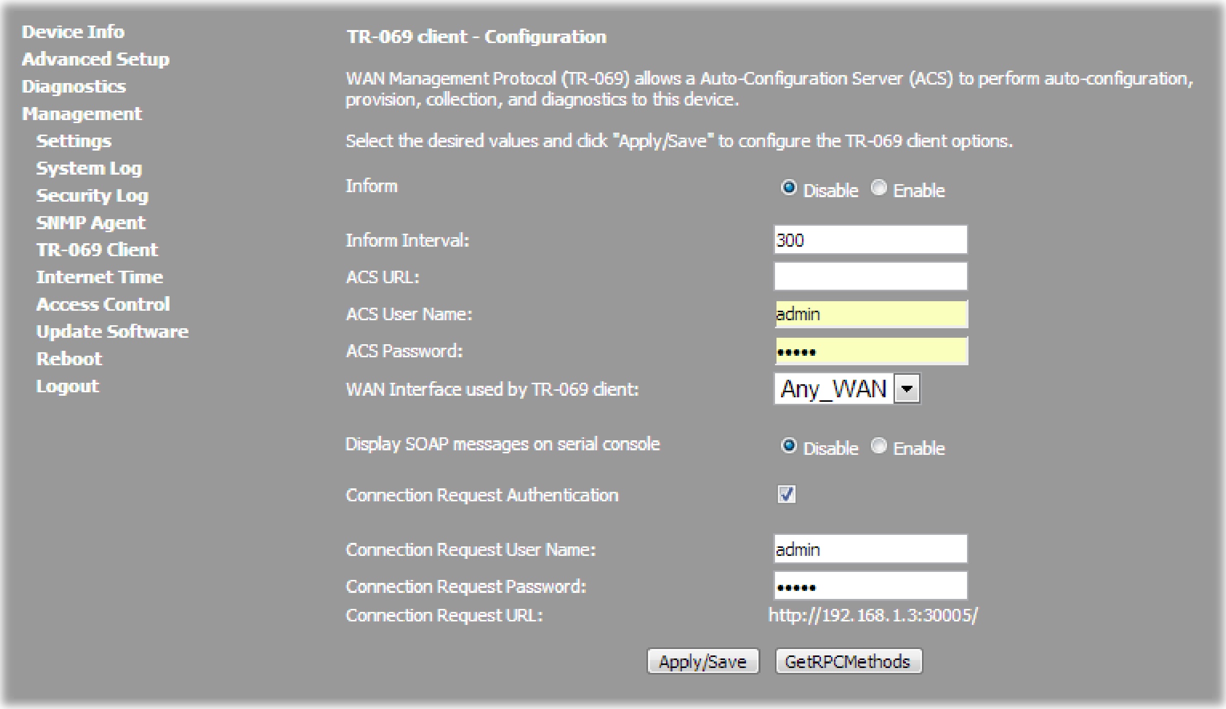
System Contact: unknown

Trap Manager IP: 0.0.0.0

Figure 31

SNMP Agent Enable/Disable	Enable/Disable SNMP in CPE Default SNMP is enabled
SNMP Read Community	SNMP Read Community Default = “public” Used for SNMP GET Command.
SNMP Write Community	SNMP Write Community Default = “private” Used for SNMP SET command.
System Name	SNMP System Name. sysName
System Location	SNMP Location. sysLocation
System Contact	SNMP Contact. SysContact
Trap Manager IP	SNMP Trap Destination IP

Management->TR-069 Client



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

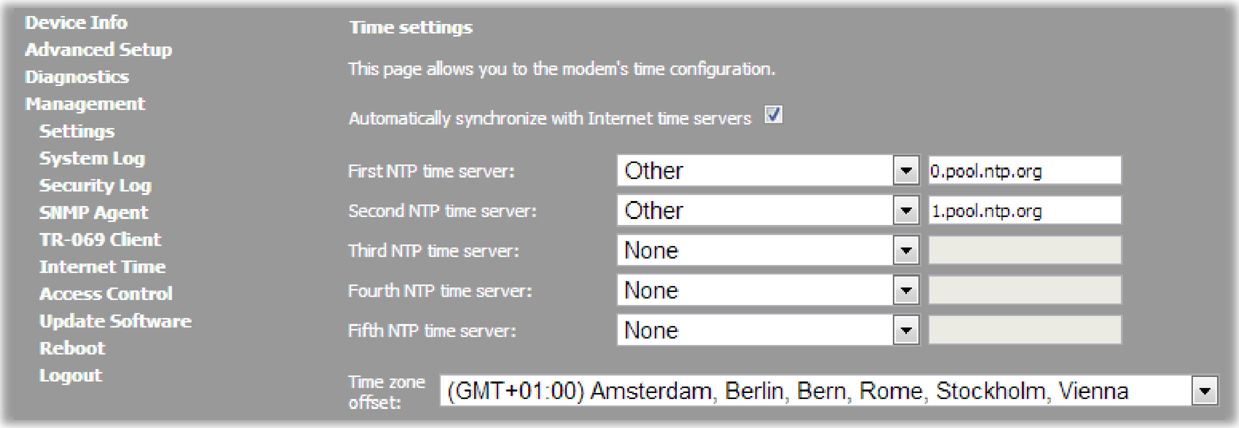
Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	● Disable ○ Enable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••
WAN Interface used by TR-069 client:	Any_WAN
Display SOAP messages on serial console	● Disable ○ Enable
Connection Request Authentication	☑
Connection Request User Name:	admin
Connection Request Password:	•••••
Connection Request URL:	http://192.168.1.3:30005/

Figure 32

Inform	Enable or Disable TR-069 Provisioning
Inform Interval	Time in seconds between TR-069 Inform messages sent from CPE to ACS server. Default value is 300 sec
ACS URL	ACS Server Full URL
ACS User Name	ACS Username Default in XG is "admin"
ACS Password	ACS Password Default value is “12345”
Display SOAP Messages on serial Console	Echo TR069 messages on serial console interface. Used only for troubleshooting when having console/serial cable available.
Connect Request Authentication parameters	Settings for TR069 Authentification

Management->Internet Time



Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers ☑

First NTP time server: Other 0.pool.ntp.org

Second NTP time server: Other 1.pool.ntp.org

Third NTP time server: None

Fourth NTP time server: None

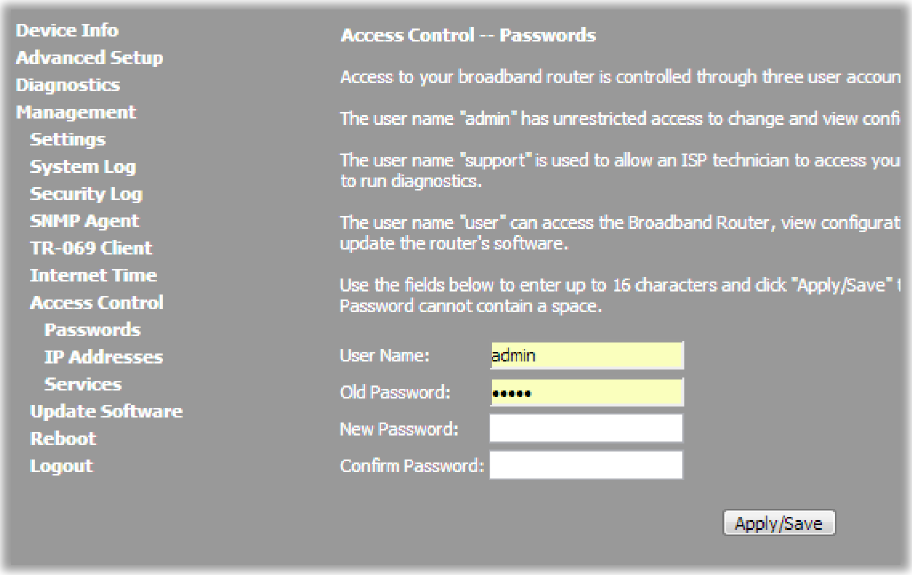
Fifth NTP time server: None

Time zone offset: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Figure 33

Automatic synchronize with internet time server	Enable/Disable NTP in CPE
List of 1-5 SNTP servers	CPE will start using first SNTP server and use next in list if it does not get response from SNTP server.
Time Zone Offset	Time zone +- from GMT

Management->Access Control->Password



Access Control -- Passwords

Access to your broadband router is controlled through three user accoun

The user name "admin" has unrestricted access to change and view confi

The user name "support" is used to allow an ISP technician to access you
to run diagnostics.

The user name "user" can access the Broadband Router, view configurat
update the router's software.

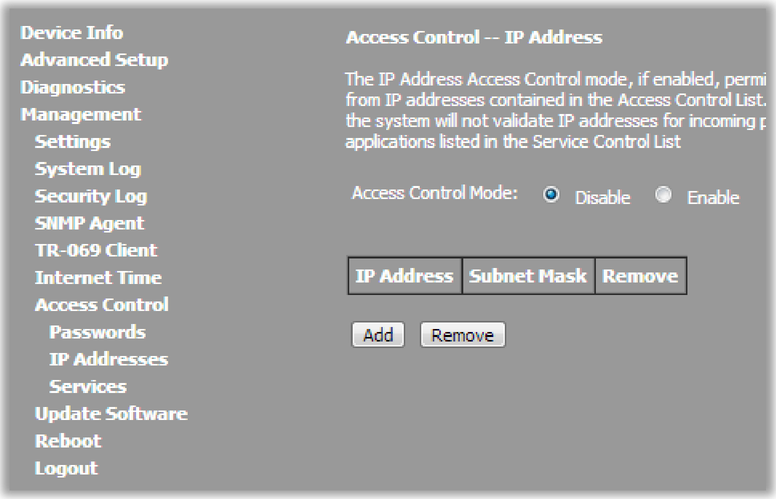
Use the fields below to enter up to 16 characters and click "Apply/Save" t
Password cannot contain a space.

User Name: admin
Old Password: •••••
New Password:
Confirm Password:

Figure 34

Username	Change password for selected users. 3 users exist: admin,support and user username/password admin/admin username/password support/support username/password user/user Important: Change password on all 3 users before deployment in live network.
Password	New password for username
Confirm password	New password for username

Management->Access Control->IP Addresses



Access Control -- IP Address

The IP Address Access Control mode, if enabled, permi
from IP addresses contained in the Access Control List.
the system will not validate IP addresses for incoming p
applications listed in the Service Control List

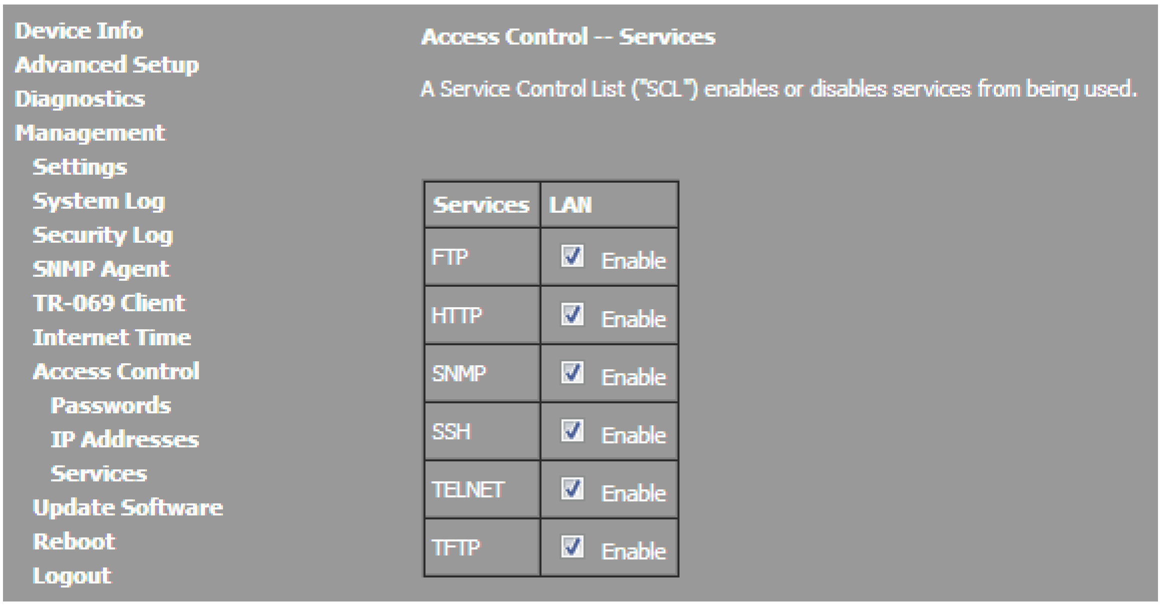
Access Control Mode: ● Disable ○ Enable

IP Address	Subnet Mask	Remove

Figur 35

Access Control Mode	Enable - Only allow defined IP subnets to access CPE services Disable- Do not use Access control **Important:** **The IP subnet configured must be ending with .0** Example Network 192.168.1.0 /24 must be configured as 192.168.1.0 255.255.255.0 If configured as example 192.168.1.1/24 then CPE will ignore the complete subnet.

Management->Access Control->Services



Access Control -- Services

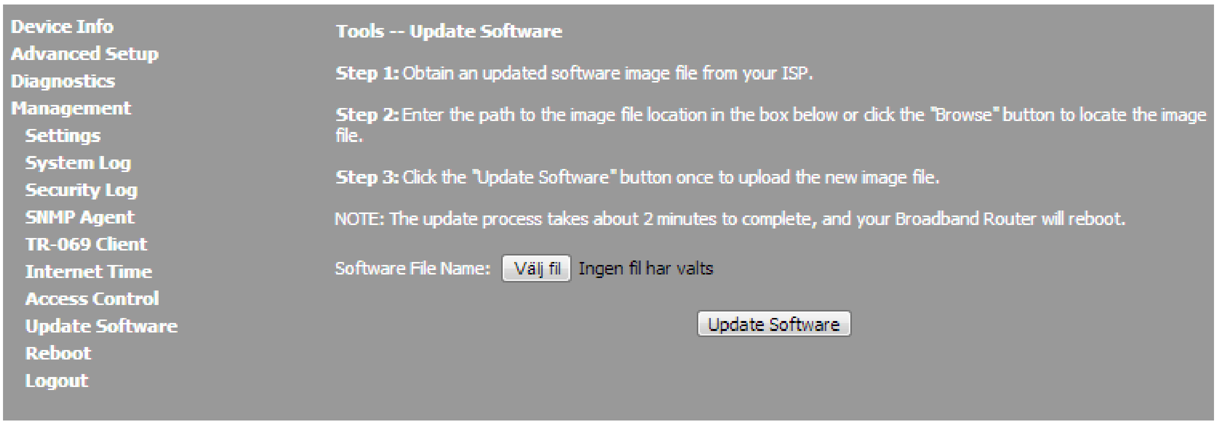
A Service Control List ("SCL") enables or disables services from being used.

Services	LAN
FTP	☑ Enable
HTTP	☑ Enable
SNMP	☑ Enable
SSH	☑ Enable
TELNET	☑ Enable
TFTP	☑ Enable

Figure 36

Services LAN/WAN	Configure if the service is enabled or disabled in CPE (Note: Does not affect outgoing protocols from CPU)
FTP	File Transfer Protocol, FTP
HTTP	HTTP WEB Server
SNMP	SNMP
SSH	SSH CLI
TELNET	TELNET CLI
TFTP	Trivial File Transfer Protocol

Management ->Update Software



Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

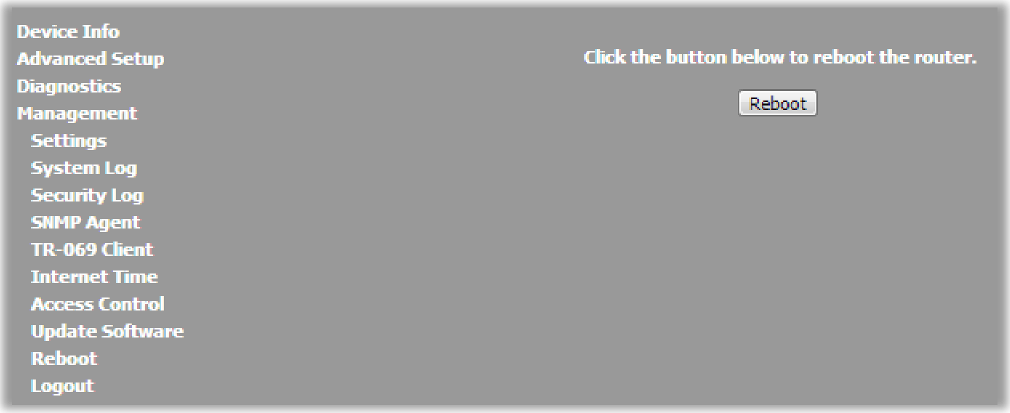
Software File Name: Välj fil Ingen fil har valts

Figure 37

The Upgrade software can be used to upgrade software/Firmware from WEBGUI.
Software is sent from PC to CPE using HTTP.

Software File Name	Use Browse… to find firmware image
Update Software	Push firmware file to CPE. CPE will reboot and start using firmware.

Management ->Reboot



Click the button below to reboot the router.

Figure 38

Reboot	If pressed the CPE do a reboot. No configuration is cleared.

Appendix 2
VLAN Configuration Example

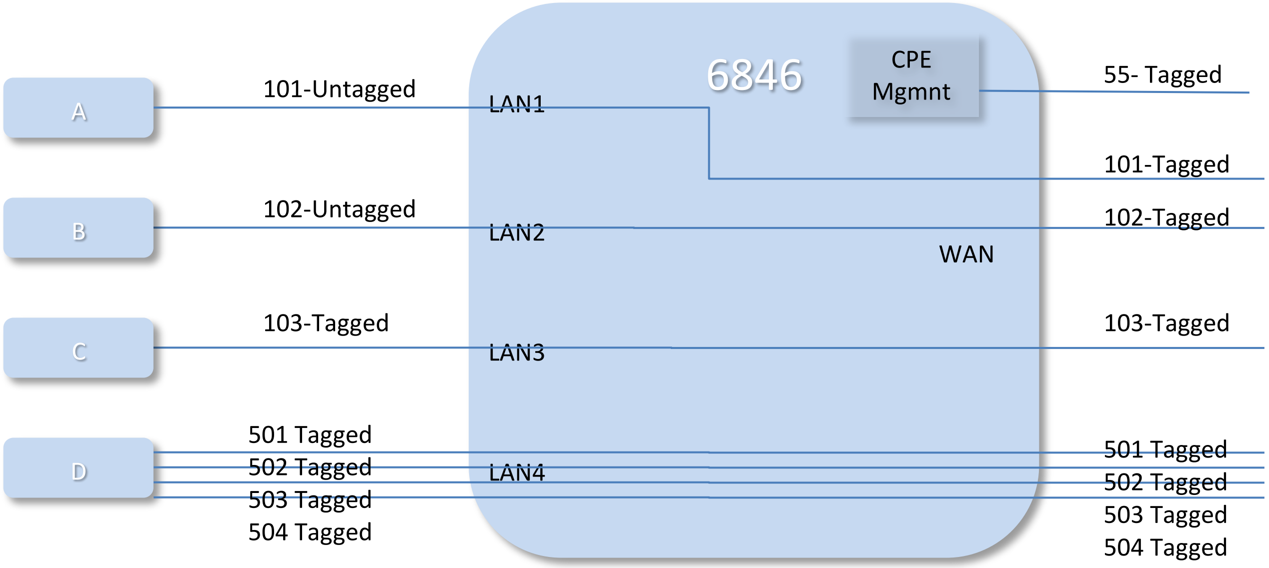
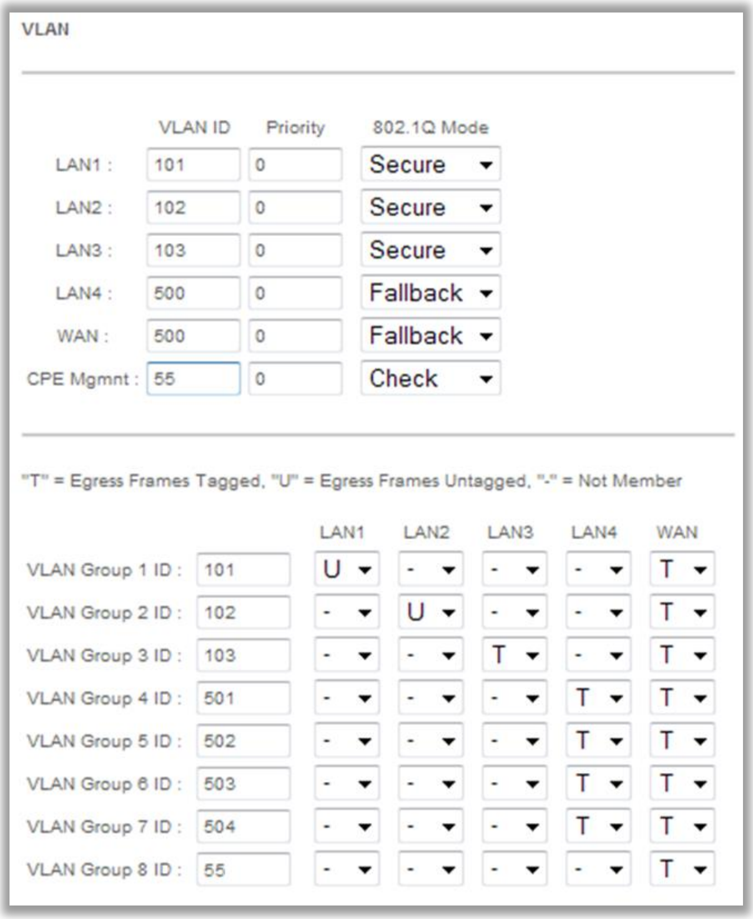


Figure 39



VLAN

	VLAN ID	Priority	802.1Q Mode
LAN1 :	101	0	Secure
LAN2 :	102	0	Secure
LAN3 :	103	0	Secure
LAN4 :	500	0	Fallback
WAN :	500	0	Fallback
CPE Mgmnt :	55	0	Check

"T" = Egress Frames Tagged, "U" = Egress Frames Untagged, "-" = Not Member

		LAN1	LAN2	LAN3	LAN4	WAN
VLAN Group 1 ID :	101	U	-	-	-	T
VLAN Group 2 ID :	102	-	U	-	-	T
VLAN Group 3 ID :	103	-	-	T	-	T
VLAN Group 4 ID :	501	-	-	-	T	T
VLAN Group 5 ID :	502	-	-	-	T	T
VLAN Group 6 ID :	503	-	-	-	T	T
VLAN Group 7 ID :	504	-	-	-	T	T
VLAN Group 8 ID :	55	-	-	-	-	T

Figure 40

Appendix 3
VLAN 802.1Q Mode

The 802.1Q Security features of the device supports the discarding of ingress frames that don't meet the security requirements and ensuring that those frames that do meet the requirements are sent to the allowed ports only.
Three levels of security are supported and they can be set differently on each port.
The security options are processed using the VID assigned to the frame as follows:

Secure
The VID must contained in the VTU and the Ingress port must be a member of the VLAN else the frame is discarded. The frame is allowed to exit only those ports that are both:
– Members of the frame's VLAN
and
– Included in the source port's port-based VLAN

Check
The VID must be contained in the VTU or the frame is discarded (the frame will not be discarded if the Ingress port is not a member of the VLAN). The frame is allowed to exit only those ports that are both:
– Members of the frame's VLAN
and
– Included in the source port's port-based VLAN

Fallback
Frames are not discarded if their VID is not contained in the VTU. If the frame's VID is contained in the VTU, the frame is allowed to exit only those ports that are both:
– Members of the frame's VLAN and
– Included in the source port's port-based VLAN – If the frame's VID is not contained in the VTU, the frame is allowed to exit only those ports that
are:
– Included in the source port's port-based VLAN

Disable
Frames are not discarded if their VID is not contained in the VTU. The frame is allowed to exit only those ports that are:
– Included in the source port's VLAN

Summary

WAN port should normally be set to mode=Fallback
CPU port mode normally use mode=Secure
For normal service VLANs that are <u>untagged</u> on a LAN port <u>use mode=Secure</u> or Check for LAN port.
Ports Mode Fallback will allow all undefined VLAN to traverse the XG6846 switch fabric.

Trunk port should normally be set to Mode=Secure and trunk VLANs should be configured in VLAN group configuration.

Appendix 4
Inteno Universal Provisioning, IUP

The goal of IUP is to direct CPEs to a management server were XML based config files are located
The IUP rule set defines how the Inteno default software should handle and prioritize DHCP Options received during DHCP Process.
IUP function can be used to get newly installed or reset:ed CPEs to automatically provisioning themselves.

Provisioning Flow Schematic

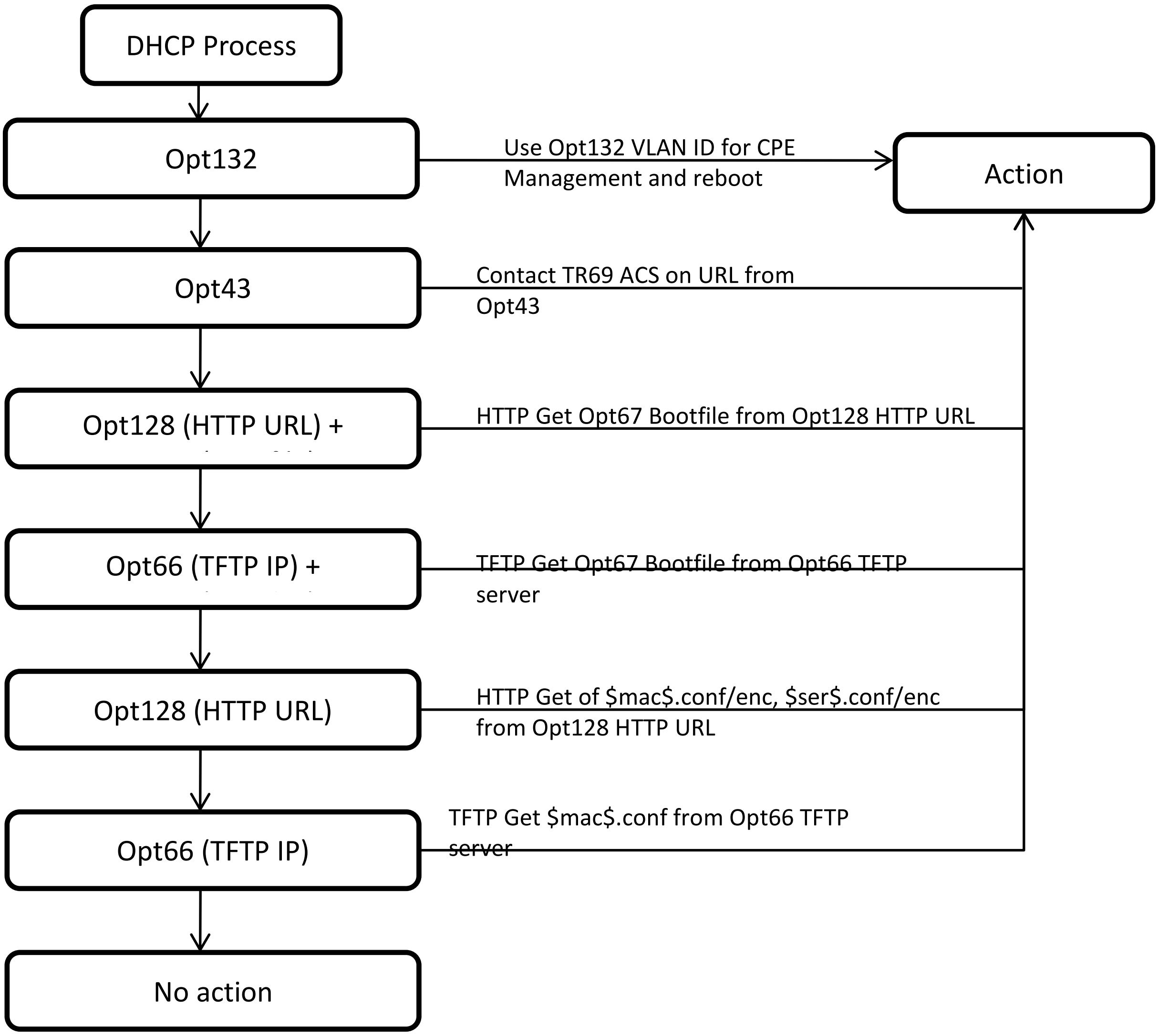

DHCP Process
Opt132
Use Opt132 VLAN ID for CPE Management and reboot
Action
Opt43
Contact TR69 ACS on URL from Opt43
Opt128 (HTTP URL) +
HTTP Get Opt67 Bootfile from Opt128 HTTP URL
Opt66 (TFTP IP) +
TFTP Get Opt67 Bootfile from Opt66 TFTP server
Opt128 (HTTP URL)
HTTP Get of $mac$.conf/enc, $ser$.conf/enc from Opt128 HTTP URL
Opt66 (TFTP IP)
TFTP Get $mac$.conf from Opt66 TFTP server
No action

Figure 41

IUP Rules Summary

Nr	Opt66 TFTP server	Opt67 Bootfile	Opt128 HTTP URL	Opt43 Vendor Specific	Result	Scenario
1	0	0	0	0	No action	No DHCP provisioning in use
2	1	0	0	0	Download mac.conf from 66	TFTP+mac.conf (one file per CPE)
3	0	1	0	0	No action	No DHCP provisioning in use
4	1	1	0	0	Download 67 file from 66 TFTP server	One config file to all CPEs from TFTP server
5	0	0	1	0	Download file from HTTP128 URL	HTTP+MAC/SER (one file per CPE)
6	1	0	1	0	Download file from HTTP128 URL	HTTP+MAC/SER (one file per CPE)
7	0	1	1	0	Download 67 from HTTP128 URL	One config file to all CPEs from HTTP server
8	1	1	1	0	Download 67 from HTTP128 URL	One config file to all CPEs from HTTP server
9	0	0	0	1	Contact ACS	TR69 Management
10	1	0	0	1	Contact ACS	TR69 Management
11	0	1	0	1	Contact ACS	TR69 Management
12	1	1	0	1	Contact ACS	TR69 Management
13	0	0	1	1	Contact ACS	TR69 Management
14	1	0	1	1	Contact ACS	TR69 Management
15	0	1	1	1	Contact ACS	TR69 Management
16	1	1	1	1	Contact ACS	TR69 Management

IUP Rules

1. DHCP Option132 has highest priority of the DHCP options.
   If multiple DHCP Options, together with Opt132, are received by CPE the CPE should only use Opt132 VLANID and reboot.
   CPE should configure the CPE management VLAN VID to the VID inside Opt132 and restart CPE.

2. If CPE Management VLAN is configured from Opt132 and CPE have rebooted, the CPE should accept and use DHCP Options received in Opt132 VLAN DHCP Offer.

3. If both Opt132 VLAN and CPE startup VLAN give DHCP Options to CPE the CPE should use last DHCP Options that was received.
   Example:
   CPE startup and get Opt132=100 and Opt128=”a.b.c.d”
   CPE should then configure CPE management to VLAN 100 and reboot.
   After reboot into the Opt132 VLAN the CPE should accept and use DHCP options if they are sent to CPE.
   If no DHCP Option is sent to CPE in Opt132 VLAN then the previous Opt127=”a.b.c.d” should be used.

4. If CPE management VLAN is already configured in CPE and CPE receives same VLAN ID in Opt132 the CPE should ignore Opt132 VLAN.

5. If CPE management VLAN is already configured in CPE and CPE receives no Option132 the CPE should use running config.

6. If CPE management VLAN is already configured in CPE and CPE receives different VLAN ID in Opt132 the CPE should use new Opt132 VLAN for management and restart to activate changes.

7. If one IUP rule match and CPE successfully get correct provisioning data from DHCP Options, CPE should stop in the IUP provisioning process.
   Example: If CPE received Option43 information it should not also continue with XML file download from HTTP server.

8. If CPE does not get response from provisioning server the CPE should just continue to try to download new file according and should not continue in IUP provisioning process.
   Example: If CPE receives Option 67+Option66 in DHCP Options, the CPE should only use this option until it gets response or is rebooted.

9. Once a XML configuration file or TR-69 synchronization/provisioning have been successful the CPE should ignore the DHCP Options in DHCP messages until reset to restore default.

10. CPEs should only accept the DHCP Option's received in DHCP Discover phase.
    The CPE should ignore DHCP Options in DHCP renewal phase.

11. DHCP Option 128 may contain full URL including file format to download.
    Rules for capital letters
12. MAC and SER must be capital letters.
13. HTTP/http part in URL should be case-insensitive. Ex HTTP or http should be allowed.
14. Opt128 URL should be able to contain capital letters but CPE should only use non-capital letters in HTTP download. (Ex Testserver below)
15.
    If no full URL is configured in DHCP Option128 CPE should use $opt128$/MAC.conf as default when receiving Opt182 URL.

    No 3DES encryption, MAC.conf (MAC address of CPE)
    MAC.conf <-> Option128 Format=" <URL including HTTP/HTTPS>/<directory>/MAC.conf"
    No 3DES encryption, $SER.conf (Serial Number of CPE)
    SER.conf <-> Option128 Format=" <URL including HTTP/HTTPS>/<directory>/SER.conf"
    3DES encryption, MAC.enc (MAC address of CPE)
    MAC.enc <-> Option128 Format="<URL including HTTP/HTTPS>/<directory>/MAC.enc"
    3DES encryption $SER.enc (Serial Number of CPE)
    SER.enc <-> Option128 Format= "<URL including HTTP/HTTPS>/<directory>/SER.enc"

Examples

DHCP Option128 Field Value	Download File	Download URL
HTTP://10.10.1.120	MAC.conf	HTTP://10.10.1.120/MAC.conf
http://download.server.COM/httpserver/onefiletoall.conf	onefiletoall.conf	HTTP://download.server.com/httpserver/onefiletoall.conf
10.10.1.120	MAC.conf	HTTP://10.10.1.120/MAC.conf
HTTP://dl.operatorx.se/www/MAC.conf	MAC.conf	HTTP://dl.operatorx.se/www/MAC.conf
http:// dl.operatorx.se/MAC.enc	MAC.enc	HTTP://download.com/dir/MAC.enc (3DES Encryption)
Testserver.se/SER.enc	SER.enc	HTTP://testserver.se/SER.enc (3DES Encryption)

16. DHCP Option 67 can contain unique file or MAC/SER combination

    No encryption MAC.conf (MAC address of CPE)
    MAC.conf <-> Option67 Format=”MAC.conf”

    No encryption $SER.conf (Serial Number of CPE)
    SER.conf <-> Option67 Format=”SER.conf”

    3DES encryption MAC.enc (MAC address of CPE)
    MAC.enc <-> Option67 Format=”MAC.enc”

    No encryption $SER.enc (Serial Number of CPE)
    SER.enc <-> Option67 Format=”SER.enc”

Appendix 5
DHCP Server Configuration Examples (ISC dhcpd)

The below example shows a dhcpd.conf file that includes of all DHCP options.
TR-069 ACS redirection Option 43 is used in example and give DHCP option43 to clients with Vendor Class Identifier=“XG6846_Inteno”

```
option opt66 code 66 = text;

option opt67 code 67 = text;

option opt128 code 128 = text;

option opt132 code 132 = text;

option space TR069OPT code width 1 length width 1 hash size 2;

option TR069OPT.ManagementServerURL code 1= text;

option TR069OPT.ProvisioningCode code 2 = text;

subnet 192.168.10.0 netmask 255.255.255.0 {

  range 192.168.10.5 192.168.10.200;

  option domain-name-servers 192.168.10.1;

  option domain-name "Testdomain";

  option routers 192.168.10.1;

  option broadcast-address 192.168.10.255;

  #CPE Management VLAN
  option opt132 "101";

   #TFTP Server IP Address
   option opt66 "192.168.10.201";

   #HTTP Server IP Address
   option opt128 "HTTP://192.168.10.201";

  # XML Config File to Download
  option opt67 "XG6846test1.conf";

   default-lease-time 3600;

   max-lease-time 3600;

}
```

```
# Configuration for Opt43 for CPEs with VendorID= “XG6846-INTENO”
class "vendor-classes" {
 match option vendor-class-identifier;
}
subclass "vendor-classes" "XG6846_Inteno" {
 vendor-option-space TR069OPT;
 option TR069OPT.ManagementServerURL "http://10.10.1.137";
 option TR069OPT.ProvisioningCode="1234567890";}
```