

2018-06-27, JÅ



GT11

The GT11 is WISI's integrated gigabit Ethernet switch in the GT01W and GN50 base units. The GT11 adds network switch capability, redundancy and power supply and fan bay status to the base units.

For more information on the GT01W and GN50 base units, please consult their separate documentation. This document describes the GT11 software.

Service and support

For support information and help, please contact our support organisation. The support organisation is manned by support staff from both Sweden and Germany.

For support, please create a ticket at <https://wisiconnect.tv>.

At the wisiconnect.tv portal, you will find the Manual, Release Notes, Known Issues, Software Compatibility and the software binary for each software release.

Apart from this general information, there is also a Knowledge Base. Our Knowledge Base will give answers to frequently asked questions, and more information will continuously be added.



This manual is also available
at the wisiconnect.tv portal.

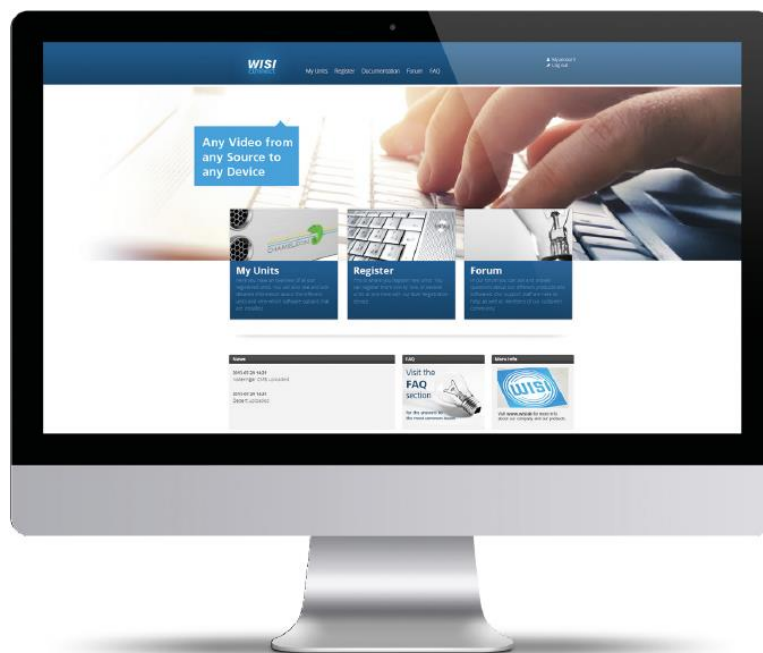


Table of content

1 Getting started	6
1.1 Registration	6
1.2 Assembling in base unit	6
1.3 Connecting	6
1.4 Changing the IP address.....	6
1.5 Configuring the GT11	6
2 Software options.....	7
3 The wisiconnect.tv portal.....	8
3.1 Registering user.....	8
3.2 Registering the GT11.....	9
3.3 Downloading software and software options.....	9
4 Uploading software and software options	10
4.1 Uploading via WISI IP Supporter	10
4.2 Uploading via the GT11's web UI	10
5 Security.....	11
6 Switch overview	12
6.1 Networking performance.....	12
7 Front panel LED	13
8 The GT11 web user interface	14
8.1 Accessing the web UI	14
8.2 The web UI structure	14
8.3 Using the web UI.....	15
8.4 Ethernet switch	16
8.4.1 VLAN.....	16
8.4.2 IGMP.....	17
8.4.3 Multicast flooding	18
8.4.4 Port monitoring.....	18
8.4.5 Forwarding database	18
8.5 Modules	20
8.5.1 Status	20
8.5.2 Redundancy.....	20
8.5.3 Automatic configuration	21
8.5.4 Manual change of module state	22
8.6 Power supply and fan monitoring.....	22
8.7 Headend System	23
8.7.1 Headend System management.....	23

8.8 System UI	24
8.8.1 System mode.....	24
8.9 Networking.....	25
8.9.1 Adding and configuring Management interface	25
8.9.2 SNMP.....	26
8.10 Date and time.....	28
8.11 User management.....	29
8.12 Maintenance	30
8.12.1 Reboot.....	30
8.12.2 Backup and restore	30
8.12.3 Diagnostic file.....	30
8.13 Log.....	31
8.13.1 Web UI	31
8.13.2 Syslog	31
8.14 Transport stream monitor	32
8.14.1 Syslog	32
8.15 Status	33

1 Getting started

This chapter briefly describes how to get the GT11 up and running. A more detailed description is available in other sections of this manual.

1.1 Registration

Before anything can be done with a new GT11, it must be registered at <https://wisiconnect.tv>, see section 3.2.

After registration, the entitlement file must be uploaded to the GT11. See sections 3.3 and 4 on how to do this.



1.2 Assembling in base unit

The GT11 must be fitted in one of the base units that WISI provides. Available base units can be found at <https://www.wisi.se> and <http://www.wisi.de>.

1.3 Connecting

The GT11 is powered using the power supply that is delivered with the base unit.

The GT11 is controlled via Ethernet, so the GT11 must be connected to a computer/network using an Ethernet cable.

The GT11's default IP address on the Management interface is 192.168.0.11. Before connecting to the GT11, the computer (or network) must be configured to allow access to this IP range.

The connection to the GT11 is tested by entering <http://192.168.0.11> in the address field of a web browser.

1.4 Changing the IP address

When using multiple GT11s, it is recommended to change the default Management interface IP address to a system unique IP address. See section 8.9.1 on how to do this.

An alternative is to change the GT11's IP address using the stand-alone program WISI IP Supporter, available at <https://wisiconnect.tv>.

1.5 Configuring the GT11

Configure the GT11 to do its desired task. See sections 8 and onward in this document for more information.

2 Software options

The GT11 comes fully functional, but some of its functionality is not available immediately. The first step is to purchase the needed functionality. WISI calls this functionality "software options". The software options are transferred to the GT11 via an Entitlement file, which has the name <serial number>.ent.

WISI uses the SUA (Software Update Agreement) to give customers access to bug fixes and feature enhancements via new software. Each new GT11 comes with the GNM1/GTM1 SUA, whose start date is the date of registration at wisiconnect.tv. A new SUA uses the end date of the previous Maintenance software option as start date. WISI offers two different SUAs, GNM1/GTM1 and GNM3/GTM3. GNM1/GTM1 is for one year, while GNM3/GTM1 is for three years.

There are two ways to see which software options a GT11 has:

- wisiconnect.tv. Go to **My Units** and click on the GT11's serial number.
- GT11 web UI. Look under **CONFIGURATION** in the **Status** view.

The table below shows the software options that can be purchased for the GT11. A detailed description on what the software options do can be found in the separate software option documentation on wisiconnect.tv, or by contacting a WISI sales representative.

Software Option	Description
REDUNDANCY	
GNNRED	N+1 module redundancy in the GN50 base unit
GTNRED	N+1 module redundancy in the GT01W base unit

3 The wisiconnect.tv portal

The wisiconnect.tv portal is the place where

- The GT11 is registered.
- The GT11 is handled.
- Support is given.
- Documents, software and software options are downloaded.

The wisiconnect portal is located at <https://wisiconnect.tv>.

3.1 Registering user

Before using the wisiconnect.tv portal for the first time, an account must be created. Register by clicking on **Register account** at <https://wisiconnect.tv>. Only a valid email address and a password are required.

If the password has been forgotten, click the **Lost your password?** link, and an email containing further information will be sent to the entered email address.



The screenshot shows a web browser window with the address bar displaying <https://wisiconnect.tv>. The page has a navigation bar with links for 'WISI CONFIGURATOR', 'WISI CATALOG', and 'WISI.DE'. The main content area features the WISI logo at the top. Below it, a 'WISI Connect Account' section contains two input fields: 'Enter your e-mail here' and 'Enter your password here'. A yellow 'Sign In' button is positioned below these fields. At the bottom of the registration section, there are two links: 'Register account' and 'Lost your password?'. The footer of the page includes social media icons for Facebook, LinkedIn, X, Google+, Twitter, and Email, along with the copyright notice '© The WISI Group 2015'.

3.2 Registering the GT11

Before anything can be done with a new GT11 it must be registered at the wisiconnect.tv portal.

Done this by logging in to the wisiconnect.tv portal and there click the **Register Unit** tab. In the **Register Unit** tab, enter the serial number of the GT11, and select the distributor who sold the GT11 in the drop-down list.

Optionally, also enter **Module Name**, **Installation Site**, and **Description**. These fields are intended for personal use, so that you can track and maintain all your GT11s.

Click the **Register** button to complete the registration.

Several units can be registered at once using the Bulk Registrator. Clicking the **Bulk Registrator** will present a text box in which any number of GT11 serial numbers can be entered.

The screenshot shows the 'Register Unit' page on the wisiconnect.tv portal. The page has a blue header with the WISI logo and navigation links: My Units, Register Unit (highlighted), Knowledge Base, Forum, Downloads, and Submit Ticket. The main content area is titled 'Register Unit' and contains the following fields:

- Serial Nr * (text input)
- Module Name (text input)
- Installation Site (text input)
- Distributor (dropdown menu, currently showing 'Not specified')
- Description (large text area)

A blue 'Register' button is located at the bottom right of the form. Below the form, there is a section titled 'Need to register units in bulk?' with a link 'Try the Bulk Registrator' and a blue 'Bulk Registrator' button. The footer of the page reads '© The WISI Group 2015'.

3.3 Downloading software and software options

To download software from wisiconnect.tv, first log in to the wisiconnect.tv portal and click the **Downloads** tab. Then navigate to the software that is to be downloaded and save the file to the computer.

To download the entitlement file from wisiconnect.tv, first log in to the wisiconnect.tv portal and click the **My Units** tab. Then click on the  icon for the unit and save the file to the computer.

4 Uploading software and software options

Software and software options can be uploaded to the GT11 via the stand-alone WISI IP Supporter software, or via the GT11's web UI.

GT11 software previous to 2.2 cannot be directly upgraded to a newer software version. Instructions on how this is handled can be found in earlier software manuals.

In the GN50 base unit, the software version for the Chameleons has to be compatible with the software version for the GT11. Compatibility between software versions is described in the separate `chameleon_platform_software_compatibility` document, available at <https://wisiconnect.tv>.

In the GT01W base unit, the software versions for the Tangram modules also have to be compatible. For GT11 software version 3.2.4, make sure that all Tangram modules in the GN50 base unit are running software version 2.3 or later. When using the System UI, the Tangram module software should preferably be 3.1 or newer.

4.1 Uploading via WISI IP Supporter

The external WISI IP Supporter program is available at the wisiconnect.tv portal, and can be used to upload files to the GT11. Entitlement files can be updated without downloading them first.

To upload a file from a computer, start WISI IP Supporter and then select to which GT11 to upload the file. Select the **Entitlement upgrade** tab to upload entitlement or **Software upgrade** to upload software. Then use the  button to select which file to upload, and click the **Upload** button. For entitlement files, deselect the **Entitlement from WISI server** tick-box.

To upload an entitlement file directly from the wisiconnect.tv portal to your GT11, start WISI IP Supporter and then select to which GT11 to upload the entitlement. Then check the **Entitlement from WISI server** tick-box and click the **Upload** button. Note that this requires that the computer is connected to both the Internet and the GT11.

4.2 Uploading via the GT11's web UI

All file uploads are handled the same way in the GT11's web UI, whether it is a software file or an entitlement file. Upload is done via the **SOFTWARE AND ENTITLEMENT UPGRADE** section in the **Settings** view.

1. Click on the **UPLOAD** button to browse for the file to be uploaded from your computer.
2. Click on the **BROWSE** button and then locate the file (`.bin` for firmware, `<serial number>.ent` for entitlement) on your computer.
3. Click **Open** in the browsing window to select the file.
4. Click the **UPLOAD** button.
5. Wait for the feedback that the upload was successful.
6. Click the **REBOOT** button to reboot the module.

5 Security

The GT11 is not designed to provide Internet security. This means that the GT11 is immediately vulnerable if it is connected to an Ethernet network.

It is therefore advised that the GT11 is connected to a secured network (not the Internet). If the GT11 is connected to the Internet, it should be placed behind a firewall. A VPN can then be used to access the GT11 through the firewall.

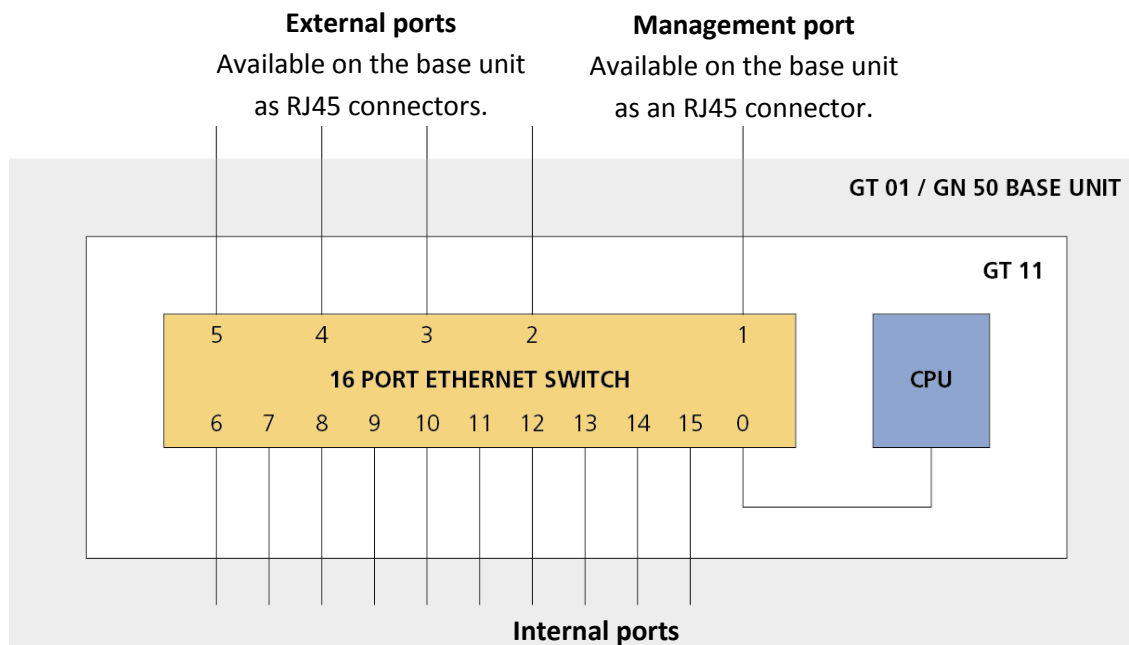
Obvious weak points are:

- Weakness against (D)DOS attacks.
- Lack of secure authentication.

6 Switch overview

The GT11 behaves in many aspects as a generic, managed Ethernet switch. By understanding the internal connections, it is easier to understand how it is configured and how traffic is forwarded. The term "module" is used in this manual to refer to a Tangram or Chameleon product that is inserted into the GT01W/GN50 base unit.

GT11's 16 Gigabit Ethernet ports are connected as shown in the picture below:



Connected to modules internally in the base unit. In the GT01W base unit, ports 12-15 are treated as External ports as they can be connected to the GT12 Switch Extender.

Port 1 above, is in this manual referred to as the "Management port". Ports 2, 3, 4 and 5 above, are in this manual referred to as "External ports". Ports 6-15 above, are in this manual referred to as "Internal ports". In GT01W, ports 12-15 can be exposed externally via the GT12 module.

Port 0 above, is in this manual referred to as the "Management CPU port". It is a completely internal port but it is always connected to port 1, the "Management port". This means that management of the GT11 always can be done via port 1. When configuring Networking (chapter 8.9), what is actually configured is the "CPU" interface on port 0.

All 15 ports (1-15) can be used for management and streaming.

The GT11 segments the internal physical network into VLANs (virtual local area networks). VLANs are used internally in the GT11 to maximise its performance and to make it more versatile. Simplified, this means that the GT11's network is configured on a VLAN basis, rather than on a port basis.

IGMP is a protocol used by network devices to indicate that they are interested in receiving traffic for a multicast group. Without IGMP, multicast traffic would be forwarded to all ports on the GT11. The multicast traffic can then reach the bit rate limit of the GT11, which will result in packet loss. The GT11 supports IGMP, and it is configured per VLAN.

6.1 Networking performance

When Ethernet frames are forwarded in the GT11, they are queued on the ports transmit queue. The average bit rate of the traffic forwarded to one port may not be greater than the capacity of that port. If it is, the

transmit queue will eventually overflow. When an overflow occurs on a port, a counter is incremented. The status of this counter can be read via the UI.

In the case of streaming, Ethernet frames from one or more ports are constantly added to a port transmit queue. The probability for a transmit queue overflow will increase with the number of ports which forward frames to the transmit queue. This probability will increase if the average bit rate is high, as there is less margin to handle traffic peaks.

If the streams are bursty, the probability increases that they cause a traffic peak. If the peak is large enough, it will in turn cause a transmit buffer overflow. Regarding transport streams, constant bit rate transport streams are in nature less bursty than a variable bit rate transport stream. A constant bit rate transport stream is less bursty than a variable bit rate transport stream, also when transporting them over IP.

7 Front panel LED

The LED in the front panel indicates the operational state of the GT11:

- Constant blue indicates normal operating state.
- Blinking blue indicates that power up is in progress.
- Blinking orange indicates that software is being uploaded.

8 The GT11 web user interface

The GT11 is managed mainly via the web UI (web user interface), but it also supports a sub-set of all configuration via SNMP. However, only the web UI will be explained here. The web UI will work with most browsers, except for Microsoft Internet Explorer versions prior to 11.

8.1 Accessing the web UI

The default IP address for a GT11's management interface is 192.168.0.11. To use the web UI, simply connect the GT11's management interface port to a computer, either directly or via a network. If the GT11 is connected directly to a computer, the computer's TCP/IP settings must match the GT11's. A safe way is to set the computer's IP address to 192.168.0.10 and its netmask to 255.255.255.0.

Use the computer's web browser to connect by typing the IP address of the GT11 in the address field of the browser.

8.2 The web UI structure

The web UI is designed to be easy to use, while at the same time allow access to all the advanced statuses/settings.

Close to the top there are four headings; **Status**, **Switch**, **Modules** and **Settings**. In the remainder of this manual, these are referred to as "views":

- **Status** shows some basic information about the GT11 and the power supply and fans in the GT01W/GN50 base unit.
- **Switch** is for configuring the network switch functionality in the GT11.
- **Modules** is for controlling the modules in the GT01W/GN50 base unit.
- **Settings** are for managing all the remaining things:
 - Networking (including SNMP).
 - Web server security.
 - Software and software options upload.
 - Logging.
 - Reboot, backup, diagnosis.
 - Date and time.
 - User management.

8.3 Using the web UI

The web UI aims to be self-explanatory, but it is a good idea to understand the concept. Below is a screenshot with some explanations. All settings are grouped together and the information in each group can be expanded/contracted.

The screenshot displays the web UI for configuring outputs. It features two main sections: 'My ASI output' and 'My DVB-C output'. The 'My DVB-C output' section is expanded, showing a table of settings and values. Red arrows and boxes highlight various UI elements:

- Info icon:** The info-icon gives additional information.
- Arrows:** The arrows show how items in the UI expand/contract.
- Exclamation mark icon:** The exclamation mark indicates potential problems.
- Menu icon:** The menu icon gives access to context related settings.
- Settings table:** The notifications pop-up gives more detailed information about problems.
- Notifications pop-up:** The notifications pop-up gives more detailed information about problems.
- Settings table:** The name of the setting is shown to the left and the actual setting is shown to the right.

SETTING	VALUE
Output enabled	On
Name	My DVB-C output
Frequency table	CCIR
Frequency (MHz)	1 (Manual)
Constellation	64QAM
QAM spectrum	Normal
Symbol rate (kBaud)	6800
Carrier level (dBpV)	78

Some settings take effect immediately, while other settings require that the is clicked. Before clicking the , the settings that have been modified will be shown on a yellow background. This way, it is easy to see what the changes are, and it shows which changes will be applied by clicking the .

Most often the first step is to configure the VLAN for the GT11's Internal ports and for the modules in the GT01W/GN50 base unit. In many cases, the GT11's default VLAN configuration is sufficient.

8.4 Ethernet switch

8.4.1 VLAN

The GT11 segments the internal physical network into VLANs, in the same manner that you would expect from any managed switch.

Communication between the GT11 and a module in the GT01W/GN50 base unit requires them to be members of the same VLAN. For the module in the base unit, the VLAN must be configured on a network interface.

VLAN 16 is reserved traffic between modules inside the GT01W/GN50 base unit.

The VLANs can be freely configured, with the exception of VLAN 1 and 16.

8.4.1.1 Default VLAN configuration

The GT11 has a default VLAN configuration, which will work in most network setups. Note that this default VLAN configuration only will be active after it has been manually reset, see section 8.4.1.3. The default VLAN configuration is configured as:

The External ports and the Management port are configured for the same VLAN ID as the port number. I.e., the Management port is configured for VLAN ID 1 and the External ports 2-5 are configured for VLAN ID 2, 3, 4 and 5. In the GT01W base unit, Internal ports 12-15 (connectable to the GT12) are considered as External ports and are therefore configured to use VLAN ID 6, 7, 8 and 9.

Additionally, VLAN 10 is used for streaming traffic between modules inside the GT01W/GN50 base unit.

Each Internal port is a member of VLAN 1-5, VLAN 10 and VLAN 16. This enables IP traffic on all External ports and the Management port to reach all Internal ports. However, the External ports and the Management port will not share traffic. This way, 4 Gbit/s of data on the GT11's External ports can be forwarded to any of the Internal ports.

Data to and from the GT11 is expected to be untagged for the Management port and the External ports. For the Internal ports, data is expected to be tagged.

8.4.1.2 VLAN membership

For a port to be reachable in the GT11, it must be a member of at least 1 VLAN.

A port is configured to transmit traffic tagged or untagged, and this is set for each VLAN of which the port is a member. VLAN tagging will not be explained in this manual as it is an integral part of the VLAN concept.

The GT11's Management CPU port and Management port are always fixed to VLAN1. VLAN1 is therefore called the management VLAN.

Untagged incoming traffic is assigned to the GT11 port's default VLAN. The default VLAN ID is set to the VLAN ID on which the port is an untagged member.

8.4.1.3 Reset VLAN configuration

To get the default VLAN configuration as described in 8.4.1.1, click the **Reset** button in the **Switch** menu's **VLAN**. This will also reset the IGMP configuration for all VLANs.

8.4.1.4 Configure module VLAN

When using the default VLAN configuration for the GT11, configure the Tangram or Chameleon modules streaming interface with a corresponding VLAN ID. Since all the GT11's Internal ports are members of all VLANs, it does not matter where in the GT01W/GN50 base unit the module is placed.

Configuration of the Tangram and Chameleon network interfaces can be done using the module's context menu in the GT11. The module's context menu is located in the **Switch** view, under the VLAN's **Interfaces**.

8.4.1.5 Cascading management between multiple GT11s

To connect to several GT11s without using an external switch, the switch settings can be reconfigured to use one of the External ports for management traffic. This can be done in 2 steps (assuming the default VLAN configuration is currently used):

1. Connect an Ethernet cable between anyone of the GT11s External ports.
2. Remove the VLAN for the External port that is to be used for management.
3. Add the External port, that is to be used for management, to the Management VLAN as Untagged.

8.4.1.6 Creating a VLAN for tagged external traffic

Receiving VLAN tagged external traffic can be done in 2 steps (assuming the default VLAN configuration is currently used):

1. Create a new VLAN.
2. Add the External ports, that are to use the tagged external traffic, as Tagged members on the newly created VLAN.

8.4.2 IGMP

IGMP is a protocol for managing multicast group memberships. The protocol is used between a host that wishes to receive traffic from a particular multicast group, and a multicast router on the local network. Multicast routers listen to membership requests, and periodically send queries to maintain a correct membership list. A host requests to become a member of a multicast group and replies to queries.

Switches in the local network can use a feature called IGMP Snooping. IGMP Snooping gathers information from the IGMP messages that are sent between the multicast group members and the multicast router. With this information, the snooping switches can maintain their local multicast group membership state.

In GT11, IGMP Snooping is enabled and configured per VLAN. When enabled, the GT11 will only forward multicast traffic to the hosts that requested to be members of that multicast group. The GT11 support IGMP version 1 and version 2. The default configuration enables IGMP Snooping for all VLANs, except for the Management VLAN.

The GT11 can act as an IGMP Querier with the querying feature of a multicast router in order for IGMP to work even when there is no multicast router in the local network. A valid and unique source IP address on the local network has to be configured when enabling the IGMP Querier. Parameters such as the query interval used by the IGMP Querier are configured globally, but enable and the source IP address are configured per VLAN. The default configuration disables IGMP Querier for all VLANs, except for VLAN 10 (streaming between modules inside the GT01W/GN50 base unit). VLAN 10 has by default an IGMP Querier, to make sure that multicast is not forwarded to all modules in the base unit. To get the default configuration, click the **Reset** button in the **Switch** view's **VLAN** tab. This will also reset the VLAN configuration. The GT11 IGMP Querier can be configured in 3 ways:

- **Off.** The GT11 will not act as an IGMP Querier on the specific VLAN.
- **Forced.** The GT11 will act as an IGMP Querier as long as no other IGMP Querier with a lower IP address exists on the VLAN.

- **Auto.** The GT11 will act as an IGMP Querier as long as no other IGMP Querier exists on the VLAN.

An internal IGMP Querier always exists on VLAN 16. It uses the global IGMP Querier settings, see below. Since no external port may become a member of VLAN 16 and it uses IGMP Snooping, it also has IGMP Querier enabled.

In order for IGMP to function correctly in the network, some parameters must be known to all snooping switches. All IGMP settings are the IGMP standard settings, so they will not be explained here. The IGMP configuration is located in the **IGMP** tab, in the **Switch** view:

- **Version** selects whether to use IGMP version 1 or IGMP version 2.
- **Robustness** indicates how susceptible the local network is to lost packets. The default value is 2.
- **Query Interval** sets the amount of time between IGMP General Query messages. The default value is 125 seconds.

When using IGMP version 2, additional parameters must also be set:

- **Last Member Query Interval** sets the amount of time between successive Group Specific Query messages. The default value is 0.1 seconds.
- **Last Member Query Count** sets the number of Group Specific Query messages. The default value is 2.

When the GT11 is configured as an IGMP querier, additional parameters must also be:

- **Startup Query Interval** sets the amount of time between successive General Query messages during startup. The default value is 31 seconds.
- **Startup Query Count** sets the number of General Query messages at startup. The default value is 2.
- **Response Time** set the maximum amount of time that the IGMP router waits, to receive a response to a General Query message. The response time must be less than the query interval and its default value is 2 seconds.

8.4.3 Multicast flooding

Enabling **Multicast flooding** will override multicast filtering on the port when IGMP Snooping is enabled. With **Multicast flooding** enabled, all multicast traffic on all VLANs are forwarded to the port. **Multicast flooding** is configured in the **Switch** view's **Ports** tab.

8.4.4 Port monitoring

The GT11 displays the average amount of data, sent and received, for each physical port. Note that this average bit rate, updated every 5 seconds, only can be used as a rough indication of the network traffic. Intermediate peaks in the network traffic that can cause the switch to drop packets, will be averaged out. The direction of the traffic (receiving/transmitting) is as seen by the GT11 switch.

8.4.4.1 Transmit packet loss status

The GT11 counts the number of packets that are dropped in its transmit queues. The number of dropped packets can be viewed in the **Switch** view's **Port monitor** tab. The value can be reset to 0 via its context menu.

8.4.5 Forwarding database

The forwarding database stores information on how traffic should be forwarded in and out of the GT11. Two different algorithms for searching the forwarding database exists; CRC and XOR.

The CRC hash algorithm is best suited for random addresses and VLANs. However, for controlled testing scenarios where sequential addresses (MAC and multicast) and VLANs are often used, the XOR hash algorithm will provide better performance.

The hash chain length can be chosen between 1 and 8. The default chain length, 1, should work in most cases. However, if the number of network addresses are too many to fit in the forwarding database, increasing the hash chain length can be a solution.

8.5 Modules

Some configuration of the modules in the GT01W/GN50 base unit can be managed from the **Modules** view.

Any module in the GT01W/GN50 base unit can be rebooted, powered on and powered off via the GT11. This is done using the module's context menu.

The GT11 can store backup files for the modules in the GT01W/GN50 base unit. The backup file, for a position in the base unit, can then be uploaded to the module. Creating, removing and uploading (restoring) a backup file is done by clicking **Configuration** from the module's context menu. It is also possible to do a factory reset on a module via the module's context menu. The date of the last backup is shown for each module. Creating a new backup will overwrite the current backup.

8.5.1 Status

The GT11 monitors the current state of the modules in the GT01W/GN50 base unit, and this can be seen in the **STATUS** column. The different statuses of a module position in the base unit are:

- Off (module not present). Module is physically not present in the base unit.
- Off (module present). Module is physically present in the base unit but it is not powered on.
- Detected. Module is powered on and has been detected (detekterad hur?).
- Waiting for response. Module is operational and the GT11 attempts to communicate with it.
- Communication Failed. Module is operational but the GT11 fails to communicate with it.
- Module running. Module is operational and the GT11 is successfully communicating with it.

8.5.2 Redundancy

The GT11 adds support for N+1 redundancy in the chassis. To use N+1 redundancy, the software option GTNRED is needed for the GT01W base unit, and GNNRED is needed for the GN50 base unit.

N+1 redundancy means that one or more modules in the GT01W/GN50 base unit shares one backup module. Any module that is not a backup module is called an operational module. A set of operational modules that share one backup module is referred to as an "N+1 redundancy group". A base unit can have multiple N+1 redundancy groups. Each "N+1 redundancy group" is required to have one backup module and at least one operational module.

Create and manage the N+1 redundancy groups by clicking **Redundancy** from the context menu for each module. To create an N+1 redundancy group, simply add modules to the groups by choosing **Set as operational for N+1 Group** or **Set as backup for N+1 Group**. To remove a module from a group, simply choose **Remove from group**.

If an operational module in the N+1 redundancy group fails, it will be powered down and the backup module for that N+1 redundancy group will take over the tasks of the failed module. For this to work, the GT11 needs to have a copy of each module's backup file. If **Automatic configuration** is enabled, the GT11 takes care of the backup files all by itself. See chapter 8.5.3 for information about **Automatic configuration**. However, if **Automatic configuration** is disabled, the backup file for each module must be manually saved. Manual saving of backup files is done from the module's context menu in the **Modules** view.

All modules in the N+1 redundancy group must be of the same product type for N+1 redundancy to work. The backup module should also have the same software options as all of the operational modules.

The backup module should always remain powered on, and it should be configured to keep it in a state where it is ready to take over the tasks of an operational module. For example, if there is a need to keep authorisation of smart cards, the backup module should be configured with inputs that receive the smart

card updates. The backup module can be used just as any other module while it is not taking on the role of a failed operational module.

To enable the N+1 redundancy, set **Automatic failover** to **On**. When **Automatic failover** is disabled, no actions will be done when a module fails. The **Automatic failover** setting will affect all N+1 redundancy groups in the GT11.

When an operational module is deemed to have failed, the GT11 will perform an automatic failover. A module is deemed to have failed if it does not start, starts into Rescue mode or if the module tells the GT11 that it has failed. For information on what can cause the module to tell the GT11 that it has failed, consult the modules documentation. The failover process will power off the faulty module and then load the faulty module's configuration to the backup module.

It is recommended to not change the configuration of a backup module that has taken over the tasks of an operational module, as these changes will be discarded when the operational module is restored. Instead, first restore the failed module and then make any configuration changes to the operational and/or backup module.

A failed module is restored by first powering it on and then restoring its configuration. Powering on and restoring a module is done using the module's context menu in the **Modules** view. The backup module for the restored operational module will then automatically restore its configuration (to what it had before it took over the operational modules tasks).

The **Automatic configuration** setting will affect how the operational module and the backup module behaves after the operational module has been powered on. **Automatic configuration** is further described in chapter 8.5.3.

8.5.3 Automatic configuration

The GT11 can automatically synchronise the configuration of the modules in the GT01W/GN50 base unit. This is enabled and disabled using the **Automatic configuration** setting in the **Modules** view.

Whenever a module is started from an "Off" state, the GT11 will restore it using the configuration for that position in the GT01W/GN50 base unit. Restoring means that the backup file for the module to be restored, is uploaded to the module. The GT11 keeps track on which backup file to upload. Note that when the GT11 is started, all modules in the base unit will start from "Off" state. The current configuration on the module that is to be restored will be overwritten.

The behaviour described below is valid when **Automatic configuration** is enabled.

Once a module is synchronized with its backup file, the GT11 monitors for changes to the module's configuration. When a change in configuration is detected, a new backup file is created and the old backup file is deleted.

When the redundancy functionality has powered down a module, and the GT11 later on has detected that a module has been inserted into the same position in the GT01W/GN50 base unit, the Automatic configuration will power up and try to upload the backup file from the earlier failed module. If the upload fails, the GT11 will power down the module.

A backup module that has taken over the role of an operational module will be restored with its backup configuration once the operational module is restored.

A backup module that has taken over the role of an operational module will synchronise its backup file with the operational module.

The Automatic configuration setting will affect all modules attached to the GT11.

8.5.4 Manual change of module state

It is possible to power up, power down, download backup, restore and do a factory reset of modules in the GT01W/GN50 base unit via the GT11. Normally this is not needed, it is taken care of by the Redundancy and the Automatic configuration functionality. See chapters 8.5.2 and 8.5.3 for more information about Redundancy and Automatic configuration.

8.6 Power supply and fan monitoring

The GT11 monitors the power supply units and the fanbay in the GT01W/GN50 base unit. See chapter 8.15 for information about the statuses that are monitored.

8.7 Headend System

Headend System is WISI's name for the system that Tangram and Chameleon modules use to automatically communicate with each other over the local network. Communication is only possible when the modules are on the same local network, since it uses link-local addressing and UDP broadcasting.

The Headend System allows the Tangram and Chameleon modules to:

- Share DVB SI tables. See Chameleon and Tangram module documentation for information on DVB SI sharing.
- Be managed via the System UI. See section 8.8 for information about the System UI.

The Headend System is always activated for a GT11 on VLAN 1.

GT11's in the Headend System can be grouped together by creating Headend System groups, see section 8.7.1. Each GT11 can only be member of one group. The group concept allows GT11's to communicate and exchange data between each other. Communication is required by the System UI, and data exchange is required when sharing PSI/SI information. GT11's in different groups can not communicate or exchange data between each other.

The GT11 is seen as a chassis, with its modules automatically arranged hierarchically. The GT11 will become the "parent" to all modules in the GT01W/GN50 base unit. This hierarchy has nothing to do with Headend System group, but is merely a visualization on how modules are mounted in the base unit.

When connecting several GT01W/GN50 base units, or when connecting Chameleons in other base units (GN01, GN20, GN40), use an external switch. Connect the GT11 Management port and the Chameleons to the external switch.

8.7.1 Headend System management

The Headend System can be managed in the **Headend System Management** section in the **Settings** view. All modules in the GT01W/GN50 base unit that are on the same local network and whose Headend System is enabled will be shown here. This is also the place where the Headend System groups are managed.

Group Name is used to change the name of the Headend System group for the module. Note that **Group Name** is not used to separate groups; it is only a name. Two different Headend System groups can have the same name.

Communication method can be **Broadcast** or **Multicast**. **Broadcast** is simple, as it uses the standard broadcast functionality in TCP/IP. **Multicast** can be used to avoid using Broadcast in the local network.

When changing the Headend System **Group Name** or the **Communication method** for any module in the Headend System, all other modules in the Headend System will be changed as well.

The modules that are mounted in a GT01W/GN50 base unit will have the name of the GT11 shown in the Chassis column.

A Headend System group is created by selecting at least one other module in the **MEMBER** column. Modifying a group is done in the same way, simply by selecting or deselecting modules in the **MEMBER** column. When another module is added to the group, it will automatically have its **Group Name** and **Communication method** changed. To create a new, separate group, connect to one of the modules that will be part of the new group. If a module is removed from its group, it will keep the **Group Name** but it will not be part of the group.

8.8 System UI

The System UI can be regarded as an extra feature in the web UI, as it offers a single UI for management of multiple modules.

All modules mounted in a GT01W/GN50 base unit will automatically be available to the System UI.

The software in the GT11 must be compatible with the software in the Chameleons and Tangrams.

The drop-down list for the System UI is available in all views in the web UI. After selecting a module in the drop-down list, all web UI management is done for that module.

The ✓ icon to the left of the modules in the drop-down list indicates which module is currently being managed. The ➡ icon to the left of the modules in the drop-down list indicates which module the web browser is connected to. For information about the **System mode** choice, see section [8.8.1](#).

The position of the modules in the GT01W/GN50 base unit is also shown.

8.8.1 System mode

System mode is part of the System UI and is accessed by clicking on **System mode** in the drop-down list at the top in the web UI. In System mode the web UI is slightly different, as it displays all modules in the System UI per function (Inputs, Outputs, Services...) instead of per module.

The **Settings** view in the web UI has limited functionality when accessed via System mode. The only things that can be done under the **Settings** view in System mode are to reboot and upload software. This also means that the Headend System management cannot be accessed in System mode.

8.9 Networking

The GT11 has five Gigabit (1000BASE-T) Ethernet ports in the front. One of the ports, the Management port, can always be used to manage the GT11. Configuration of the Management port is done in the **Networking** menu in the **Settings** view. The remaining four ports are considered switch ports and are therefore not configured.



The physical placement of the Management port for the GT01W and the GN50 base unit is shown in the images to the right. In both images, the Management port is the leftmost port.

The GT11's Ethernet ports support 10, 100 and 1000 Mbit/s, half and full duplex, auto-negotiating, auto-MDI-X and IPv4.

The LED indicators on the RJ45 connectors show the status of the link. The leftmost LED indicates link and activity. If the LED is not lit, there is no link at all. If the LED is constantly lit, a link is established but there is no activity. If the LED blinks, a link is established and there is activity. The rightmost LED indicates speed. If the LED is not lit, the link speed is 10 Mbit/s. If the LED is yellow, the link speed is 100 Mbit/s. If the LED is green, the link speed is 1 Gbit/s.

8.9.1 Adding and configuring Management interface

The IP address, Netmask and Gateway must be configured according to the network in which the GT11 is placed. Do not forget to change the IP address in the web browser after changing the GT11's IP address.

As mentioned in chapter 6, the configuration of the Management port is actually the configuration of an internal interface. This is essential to understand when configuring a VLAN for the Management port. The GT11's Default Management interface is always connected to VLAN ID 1. When adding a new Management interface, it can be connected to a VLAN. When enabling VLAN, the VLAN ID must be set to a value between 1 and 4095.

8.9.2 SNMP

SNMP can be used to manage the GT11, and all the modules in the GT01W/GN50 base unit. However, it is not as full-fledged as the web UI management. The GT11 acts as an SNMP Agent, receiving read (get) and write (set) requests from a Manager (often called NMS, Network Management Station), and as a Notifier, sending notifications (traps/informs) to the Manager. The Manager must know what requests and notifications the GT11 can handle and this is done using a Management Information Base (MIB).

GT11 has support for SNMPv2c and SNMPv3. The choice of SNMP version affects how the GT11 is configured. For SNMPv3, the agent's EngineID is "0x80001D2903xxxxxxxxxx", where the last numbers are the MAC address of the Management interface.

Please contact support for information about supported requests and notifications. MIB files can be downloaded from <https://wisiconnect.tv>.

SNMP is configured in the **SNMP** menu in the **Settings** view.

8.9.2.1 Requests

SNMP read (get) and write (set) requests are configured under **Agent**, and for the GT11 to receive these, they must be enabled using the **Enable** drop-down box.

The port on which the GT11 should receive the SNMP read (get) and write (set) requests can be changed from the default port 161.

If the Manager (NMS) uses SNMPv1 or SNMPv2c, set **Minimum security level** to **No authentication or encryption**. When using SNMPv2c, **Community read string** and **Community write string** must be set. **Community read string** is used by the GT11 to identify the read requests that come from the Manager. If the string from the Manager does not match the configured string, the GT11 will not process the request. **Community write string** is the same as the read string, except that it is for write requests.

If the Manager (NMS) uses SNMPv3, set **Minimum security level** to match the security setting in the Manager. If authentication is enabled in **Minimum security level**, the GT11 will authenticate against the users that have been configured in the GT11. See section 8.11 for information on user management. If the Manager sends a request with a higher security level than what is set in **Minimum security level**, the GT11 will use the higher level of security.

8.9.2.2 Notifications

SNMP notifications are configured under **Notifications**. Notifications can be of type Trap or Inform. Inform is basically a trap but with acknowledgement, and requires SNMPv2c or SNMPv3.

For GT11 to send SNMP notifications, these must be enabled using the **Enable** drop-down box. The SNMP version to use for the notifications must be configured using **SNMP protocol version**.

If the Manager (NMS) is configured to receive SNMPv1 or SNMPv2c notifications, then the **Community string** that the GT11 generates must be set to match the Managers. **Community string** is used by the Manager to identify the notifications that come from the GT11. If the string from the GT11 does not match the Manager's configured string, the Manager will ignore the notification. If the Manager is configured to receive SNMPv2c notifications, the GT11 can be configured to send them as traps or informs using the **PDU** setting.

If the Manager (NMS) is configured to receive SNMPv3 notifications, then the GT11 must have a user and password configured for authentication (even when **No authentication** is chosen). See section 8.11 for information on user management. The user for SNMP authentication is configured using the user setting.

The level of security to use for the notifications, which must match the Manager's capability, is configured using **Requested security level**. If the Manager is configured to receive SNMPv3 notifications, the GT11 can be configured to send them as traps or informs using the **PDU** setting.

The GT11 can send notifications to up to five destinations and this is configured under **ADD A NEW NOTIFICATION DESTINATION**. **Destination address** can be an IP address or a URL and **Destination port** can be in the range 1 to 65535. All notifications are sent using the same SNMP version and the same security settings.

The GT11 can forward SNMP notifications from the modules in the GT01W/GN50 base unit. This is configured on the modules in the base unit.

8.10 Date and time

The GT11 relies on external time sources for keeping its time. The GT11 accepts two different types of time sources; NTP and User configured.

All time sources supply their time in UTC time, so to get the GT11 to use the local time it must be configured to know the offset between the UTC time and the local time. Normally this is straight forward, just select the time zone that matches the geographic area in which the GT11 is placed. On some occasions the daylight savings time makes it more complicated. If the geographic area uses non-predictive dates for the daylight savings time, this date has to be manually entered. The GT11 has support for this using the POSIX.1 TZ format. This document will not describe the POSIX.1 TZ format, but if the **Time zone** setting is edited, the POSIX.1 TZ format for the selected time zone will be shown. Select time zone **Manual** to use a custom time zone. For daylight savings time to be used by the GT11, **Adjust automatically for daylight saving time** must be enabled.

All available time sources and their time are shown under **Time sources**. The GT11 will only use the time source if it has been enabled, and this is done under **Time sources** in the **Settings** view.

The GT11 can retrieve time from an external NTP server, and supports up to five NTP servers. This requires that at least one of the GT11's network interfaces is connected to the Internet (unless a local NTP server is available). It is recommended to use all five NTP servers, since the GT11 then can determine if one or two of the NTP servers are giving a faulty time.

The GT11's internal clock can be used as a time source. To use it as a time source, the GT11's time must be configured. Please note that the GT11 uses UTC time. The user configured time source will lose its time at a reboot. Therefore at power up, the user configured time will always be January 1st, 2000.

8.11 User management

The GT11 can be access restricted through a username and password. The user name and password are sent unencrypted if HTTPS is disabled. HTTPS is enabled/disabled using **Force HTTPS** under **Services** in the **Settings** view. The GT11 can have hundreds of different users configured.

Users can belong to groups. Groups are only used for User management access restriction. Read further down for information on User management access restriction. A group can have four different access levels:

- **Read write** means that all users in the group can read and write configuration.
- **Read** means that all users in the group can only read configuration.
- **Write** means that all users in the group can only write configuration.
- **None** means that no users in the group can read nor write configuration.

Access can also be restricted depending on the network connection origin (the IP address of the user trying to access the GT11). This is done using **Access list** under **User management** in the **Settings** view. Multiple Access lists can be configured. An origin is defined using CIDR notation. Several origins can be used for each Access list by separating them with a comma. The Access lists are then assigned to users and/or groups by using the user's and group's context menu under **User management** in the **Settings** view.

If the user name or password is forgotten, the access restriction can be removed by contacting WISI support. Before enabling access restriction, a user must be created.

The access restriction is used for three functions in the GT11:

- **Web UI.** The web UI access restriction makes it possible to allow and deny users access to the GT11 web UI. The access restriction only applies for the GT11 when accessing modules in the GT01W/GN50 base unit via the System UI. Web UI access restriction is enabled/disabled using **User interface authentication** under **Services** in the **Settings** view.
- **SNMP.** When using SNMPv3, the access restriction in the GT11 is also used as authentication for SNMP. The password must be at least eight characters long for it to work with SNMP.
- **User management.** The User management restriction makes it possible to allow and deny users access to read and write the configuration for the User management.

8.12 Maintenance

8.12.1 Reboot

On some rare occasions, the Chameleon requires a reboot. This can be done by clicking the **Reboot** button under **Maintenance** in the **Settings** view.

8.12.2 Backup and restore

The GT11's entire configuration can be saved and restored by downloading and uploading a backup file from it. This can be useful for copying configurations between different installations, or keeping the possibility to upload the original configuration to a GT11 if a different configuration should be tested. The file is downloaded/uploaded by clicking the **Backup/Restore** button under **Maintenance** in the **Settings** view.

8.12.3 Diagnostic file

The GT11's entire configuration, along with internal debug information, can be saved by downloading a diagnostic file from it. This file is used by the WISI support team to help identify any problems. Attach it to the ticket on wisiconnect.tv when reporting a support issue. The file is downloaded by clicking the **Diagnostic file** button under **Maintenance** in the **Settings** view.

8.13 Log

The GT11 logs internal events with a time stamp, a severity level and a message. It will also log events from the Chameleon/Tangram modules inside the base unit. All these events can be viewed in the web UI or via syslog. Logging via syslog will allow for more extensive logging, since web UI logging is limited in size.

If the GT11 is configured to have a time, as described in 8.10, the log entries will use this time. If the GT11 is not aware of the time, as is the case at boot or when no time source is configured, the log entries will use the time 2000-01-01 00:00:00. Log messages are displayed in the GT11's local time, both for the web UI and for the syslog.

Log messages are displayed with three different priorities. In the web UI these are displayed as **Info**, **Warning** and **Critical**, and these correspond to severities 6, 4 and 2 for syslog.

8.13.1 Web UI

The web UI can display log messages with three different priorities: info, critical and warning. To aid in finding specific log messages, the GT11 can filter log messages based on both the host, priority and the log time. The filtering only affects what is shown in the UI, the logs themselves are not affected. The host filter makes it possible to filter events from Chameleon/Tangram modules inside the base unit.

The host filter has three choices:

- **All** will show all hosts.
- **Is** will show only the selected host.
- **Is not** will show all but the selected host.

The priority filter has five choices:

- **All** will show all priorities.
- **Is** will show only the selected priority.
- **Is not** will show all but the selected priority.
- **From** will show all priorities that are equal to, or higher than, the selected priority.
- **Between** will show priorities in the range of the selected priorities.

The date filter operates on a daily basis, and has five choices:

- **All** will show all dates.
- **Is** will show only the selected date.
- **Is not** will show all but the selected date.
- **From** will show all dates that are equal to, or later than, the selected date.
- **Between** will show dates in the range of the selected dates.

8.13.2 Syslog

To use syslog, a syslog server that can be reached by at least one of the GT11's network interfaces must be installed. The GT11 must also be configured to enable syslog and the syslog's address must be set. The GT11 sends syslog messages using UDP on port 514. The facility code can be configured. The time and date sent in the syslog message is the GT11's local time.

Changing the priorities that the GT11 sends to syslog can only be done using Lua commands. Please contact WISI support for more information.

8.14 Transport stream monitor

The Chameleon/Tangram modules inside the GT11's base unit can generate transport stream monitor events. The GT11 will always show these events in the **TRANSPORT STREAM MONITOR** section in the **Settings** view.

8.14.1 Syslog

All incoming transport stream monitor events can automatically be sent to an external syslog server.

To use syslog, a syslog server that can be reached by at least one of the GT11's network interfaces must be installed. The GT11 must also be configured to enable syslog and the syslog's address must be set. The GT11 sends syslog messages using UDP on port 514. The facility code can be configured. The time and date sent in the syslog message is the GT11's local time.

Active events are sent using severity 3 and inactive events are sent as severity 6.

8.15 Status

The **Status** view gives a general overview of the GT11's status, and also the status for the PSUs and fans.

- The following values are displayed under the **General** tab:
 - **MODULE IDENTIFICATION**
 - **Serial** shows the GT11's unique serial number. Used in contact with support and sales.
 - **Hardware revision** shows the version of the GT11 hardware.
 - **Name** is a text field that has no meaning to the GT11. It is a free text field that can be used by the customer to identify the GT11.
 - **Location** is a text field that has no meaning to the GT11. It is a free text field that can be used by the customer to identify the GT11.
 - **Description** is a text field that has no meaning to the GT11. It is a free text field that can be used by the customer to identify the GT11.
 - **CONFIGURATION**
 - **Software version** shows the version of the software that the GT11 is running.
 - **Software options** shows the purchased software options for the GT11.
 - **STATUS**
 - **Uptime** shows the time since the GT11 was last booted.
 - **Temperature** shows the temperature inside the GT11.
 - **SERVICE UPDATE AGREEMENT (SUA)**
 - **Registered** shows if the GT11 has been registered on wisiconnect.tv. See section 3.2 for more information.
 - **Expires** shows the end date of the Maintenance software option. See section 2 for more information.
- The following values are displayed under the **PSU & Fan monitor** tab:
 - **Left PSU and Right PSU**
 - **Name** shows the product name for the power supply.
 - **Serial** shows the power supply's unique serial number. Used in contact with support and sales.
 - **Hardware revision** shows the version of the power supply hardware.
 - **Software version** shows the version of the software that the power supply is running.
 - **State** shows the operational status of the power supply.
 - **Voltage (V)** shows the output voltage from the power supply.
 - **Current (A)** shows the output current from the power supply.
 - **Temperature** shows the temperature inside the power supply.
 - **Fan bay**
 - **Name** shows the product name for the fan bay.
 - **Serial** shows the fan bay's unique serial number. Used in contact with support and sales.
 - **Operation time** shows the total time that the fan bay has been operating.
 - **Hardware revision** shows the version of the fan bay hardware.
 - **Software version** shows the version of the software that the fan bay is running.
 - The rotational speed for all fans in the GT01W/GN50 base unit are monitored by the fan bay. The rotational speed, in turns per minute, is displayed for each fan.

**Any Video from
any Source to
any Device**

Technical modifications reserved. WISI cannot be held liable for any printing error.



WISI Communications GmbH & Co. KG
Empfangs- und Verteiltechnik
Wilhelm-Sihn-Straße 5–7
75223 Niefern-Oeschelbronn, Germany

Inland: +49 72 33 66 -0, fax -320
Export: +49 72 33 66 -280, fax -350
E-mail: info@wisi.de