

User Manual



IPS Fast Ethernet Switch

Contents

IPS Ethernet Switch Introduction	1
General	1
Switching Methods	1
Installation	2
Quick Instructions	2
IPS Front Panel	3
IPS Switch Mechanical Connections	3
IPS Switch Models	3
IPE Encoder / IPD Decoder with IPS Switch Mechanical Connections	4
IPE Encoder / IPD Decoder with IPS Switch Models	4
Connections	5
Local Port Connections	5
Up-Link Port Connections	5
Management Connection	6
VLAN Connections	6
Fibre Connection	6
Redundant Ring	7
Introduction	7
Ring Wiring	7
Spanning Tree Protocol (STP)	8
Rapid Spanning Tree Protocol (RSTP)	8
Fast Re-configuration of Network Topology (FRNTv0)	8
Virtual LANs (VLAN)	9
General	9
Operation	9-10
IP Config Tool	11
Introduction	11
System Requirements	11
How to Get the IP Config Tool	11
How to Install the IP Config Tool	11
Operating	11
Device List Page	12
How to Configure the Switch	12
Selected Device Page	13
Port Configuration Page	14
VLAN Configuration Page	15
How to Configure VLAN	15-16
How to Create the STP/RSTP Ring	17
Creating FRNT v0 Ring	18
Notes on the IP Configuration Tool	19
Trouble Shooting	19
Firmware Upgrade via IP Config Tool	19
IP Config Tool and Firmware Versions	19
Glossary	20-22
Technical Specifications	23
Copyright Acknowledgements	25

IPS Fast Ethernet Switch Introduction

Stand-alone 8 port Fast Ethernet switch with 6 x 10/100Base-TX local ports and 2 x 100Base-FX up-link ports, in-band management

Welcome, and thank you for purchasing Teleste's EASI™ Products.

General

EASI™ **IPS** is a fully managed field hardened stand-alone **Ethernet Switch** for video networking applications. The **IPS** is available as an Ethernet Switch only device or alternatively as an integral part of EASI™ **IPE** Encoder or **IPD** Decoder. The **IPS** supports SNMP management, QoS (layer 2 and 3), network redundancy (FRNT 0 protocol), port configuration, port alarms, IGMP snooping and VLAN.

Switching Methods

The **IPS** stores incoming packets and then checks the packet for check sum errors, if an error is found the packet is discarded. Other reasons for discarding packets are undersized (less than 64 bytes) or oversized packets (larger than 1522 bytes). Once the Switch verifies the packets are correct they are then forwarded onto the port(s) of the Switch and then to the corresponding network device. The Switching decision is made based on the MAC tables (Layer 2 Switching). All MAC tables are created and maintained automatically. When the **IPS** receives a packet on a port it stores the source MAC address in the MAC table that corresponds to that port. If a node is silent for a long time the MAC address will "age out" and be removed from the table.

If the **IPS** does not have the MAC address in the table it will send the packet to all ports (flooding). This is also the case for broadcast packets and multicast packets. The MAC table can hold up to 8000 address entries.

The packet memory in the **IPS** is one megabyte, this is normally enough to store thousands of packets (depending on size). The **IPS** does not use flow control (IEEE 803.3x) to throttle end nodes to avoid dropping packets during network congestion. Instead of flow control it uses HOL (head of line blocking prevention). HOL guarantees that high priority packets can be forwarded to ports congested by low priority data. It is also possible to separate some ports for VLAN usage.

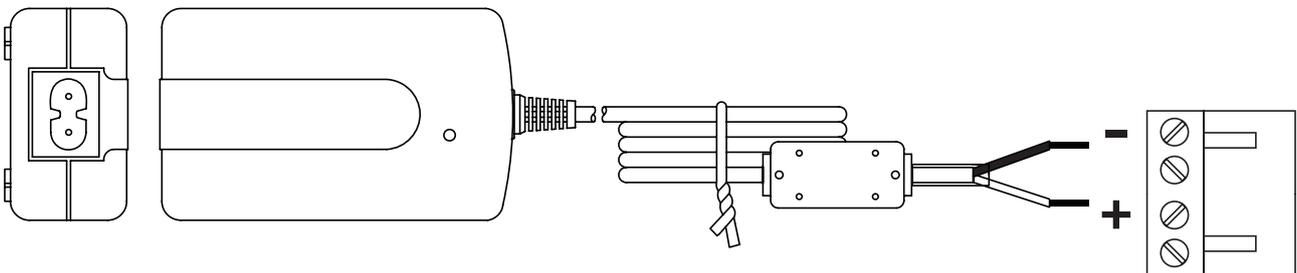
Installation

Quick instructions

- 1 Install the field hardened **IPS** Ethernet Switch (1U high, 19" wide) to the installation cabinet. A 12 V supply voltage is provided by a **CPS24x** mains adapter.
- 2 Switch on the power and see that all indicator LEDs on the front panel are going thru a routine checking cycle.
- 3 Connect all necessary 10/100Base-TX Ethernet cables.
- 4 Open **IP Config tool** on the computer connected to the Switch and configure all necessary settings.

- Make sure that the port indicator led on the front panel is lit green on the ports where cables are connected. If the indicator led is dark, the Ethernet connection does not operate at that port.
- 5

- Default network addresses for the devices are are the following:
- 6 **10.9.96.30 (IP)**
255.255.255.0 (Netmask)
10.9.96.1 (Gateway)



Picture 1. CPS24x series power supply with connector.

IPS Front Panel

IPS Switch Mechanical Connections

1. Power led indicator.
2. 2 x Up-link ports, depending on model, **dual MT-RJ** (when optical multimode) or **dual-LC** (when optical singlemode).
3. 6 x Local Ethernet 10/100Base-TX ports, (RJ-45 female).

Note! Management connection to the device can be created via any of local port.

4. Led indicators for local and up-link ports.

Models (stand-alone devices) / Up-link medias

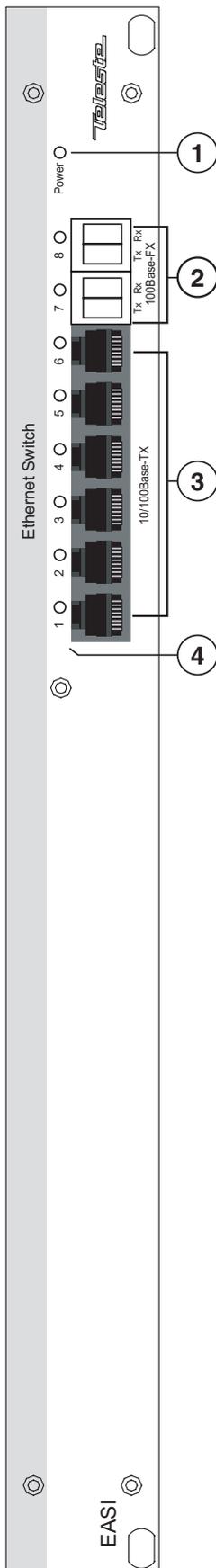
IPS Switch only:

IPS3XX00XA CAT5 (100 m)

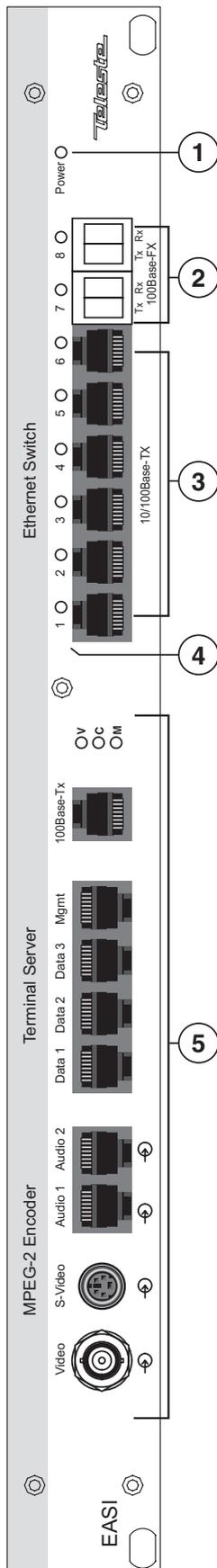
IPS3XX20XA Multimode (2 km)

IPS3XX30XA Singlemode Short Haul (15 km)

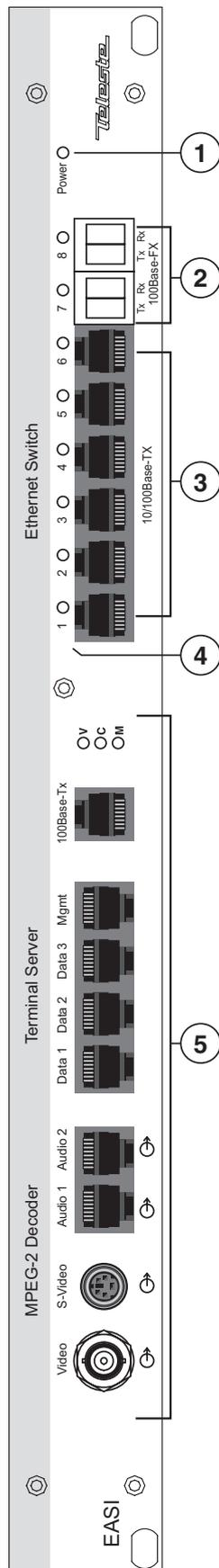
IPS3XX40XA Singlemode Medium Haul (40 km)



Picture 2.
IPS3XX***A Ethernet
Switch / connections.



Picture 3.
IPE3****A MPEG-2 Encoder / connections.



Picture 4.
IPD3****A MPEG-2 Decoder / connections.

IPE Encoder & IPD Decoder with IPS Switch Mechanical Connections

1. Power indicator led.
2. 2 x Up-link ports, depending on model, either **dual MT-RJ** (when optical multimode) or **dual-LC** (when optical singlemode).
3. 6 x Local Ethernet 10/100Base-TX ports, (RJ-45 female).

Note! Management connection to the device can be created via any of local port.

4. Led indicators for local and up-link ports.
5. IPE MPEG-2 Encoder / IPD MPEG-2 Decoder device.

*Note! Refer to the **IPE/IPD** user manual for detailed description.*

Models (stand-alone devices) / Up-link medias

IPE MPEG-2 Encoder + IPS Switch:

- IPE30000XA** CAT5 (100 m)
- IPE30020XA** Multimode (2 km)
- IPE30030XA** Singlemode Short Haul (15 km)
- IPE30040XA** Singlemode Medium Haul (40 km)

IPE MPEG-2 Encoder + Terminal Server + IPS Switch:

- IPE30100XA** CAT5 (100 m)
- IPE30120XA** Multimode (2 km)
- IPE30130XA** Singlemode Short Haul (15 km)
- IPE30140XA** Singlemode Medium Haul (40 km)

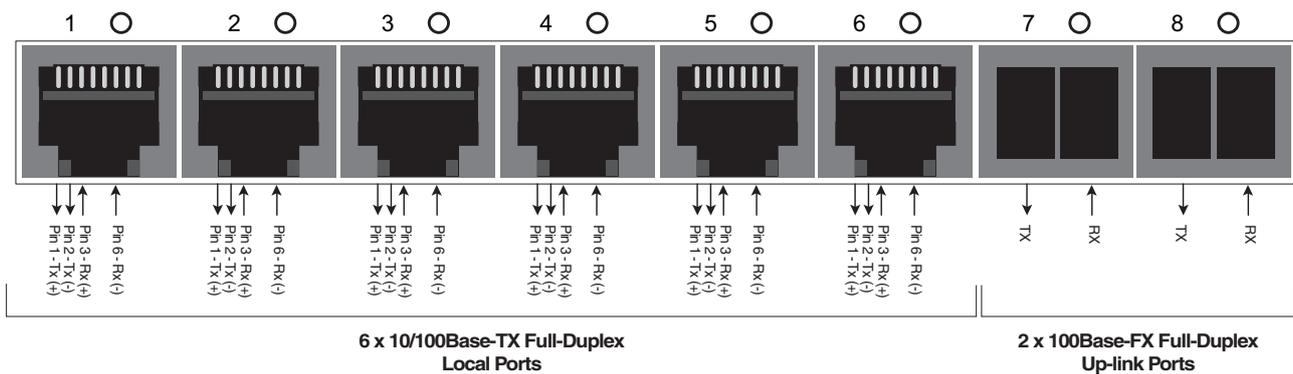
IPD MPEG-2 Decoder + IPS Switch:

- IPD30000XA** CAT5 (100 m)
- IPD30020XA** Multimode (2 km)
- IPD30030XA** Singlemode Short Haul (15 km)
- IPD30040XA** Singlemode Medium Haul (40 km)

IPD MPEG-2 Decoder + Terminal Server + IPS Switch:

- IPD30100XA** CAT5 (100 m)
- IPD30120XA** Multimode (2 km)
- IPD30130XA** Singlemode Short Haul (15 km)
- IPD30140XA** Singlemode Medium Haul (40 km)

Connections



Picture 5. 10/100Base-Tx Local and Up-link port connections.

Local Port Connections (6 pcs)

A standard **IPS** Switch comes with six (6) – 10/100Base-TX local ports (CAT5). All local port connectors are type RJ-45 female (see picture 5).

When a connection to local port is established the indicator led on top of port is lit as solid green. This led also indicates the status of in/outgoing data stream by blinking in sync with the data traffic. In a case that the Ethernet signal is missing or the signal level is too low, the indicator led is dark.

All local ports support extended 185 m distances when using high quality CAT5 or better cables. Further all 10/100Base-TX UTP ports support **MDI/MDIX** by automatically accepting both straight and crossover Ethernet UTP cables. The Switch also automatically corrects polarity errors. Furthermore the 10/100Base-TX UTP ports have isolation barriers between the signal lines and the internal electronics withstanding 1500 Vrms.

Up-Link Port Connections (2 pcs)

For Up-link network connections the Switch has two (2) **100Base-FX** Ethernet interfaces. The Ethernet 100Base connector in use is a dual **MT-RJ** (when optical multimode) or **dual-LC** (when optical singlemode). When Ethernet connection to the Up-link port is established the indicator led on top of port is lit as solid green. This led also indicates the status of in/outgoing data stream by blinking in sync with the data traffic. In a case that the Ethernet signal is missing or the signal level is too low, the indicator led is dark.

Management Connection

The **IPS** Switch can be configured locally and/or remotely via any of the Ethernet ports. However, **port 1** is recommended for management connection. The **IPS** switches are configured with **IP Config Tool** (see page 11).

VLAN (up to 7 pcs)

A VLAN is a group of end stations with a common set of requirements, independent of physical location. A VLAN has the same attributes as a physical LAN but allows you to group end stations even if the VLANs are not located physically on the same LAN segment. VLANs allow you to group ports on a Switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out other ports belonging to that VLAN.

Fibre Connection

The 1310 nm optical wavelength is used for both multimode and singlemode fibers. The optical mean launch powers are as follows:

- Multimode fiber: -19...-14 dBm
- Single mode fiber (15km, short haul) : -15...-8 dBm
- Single mode fiber (40km, medium haul): -5...0 dBm

When installing the fiber optic cable, do not exceed the minimum bending radius when connecting cable to the system.

Note! For correct optical operation ensure that all optical connectors are cleaned immediately before mating. Connectors should always be cleaned using high purity alcohol (e.g. methyl or isopropyl alcohol). Dry the surfaces using clean compressed air or other equivalent pressurized gas. The optical connectors on the equipment should always be protected with dustcaps when there is no fiber inserted.

Optical Ethernet connection meets Class 1 laser safety requirements of IEC 825-2: 1993 and US department of health services 21 CFR 1040.10 and 1040.11 (1990) when operated within the specified temperature, power supply and duty cycle ranges.

Redundant Ring

Introduction

The redundant ring technology eliminates network failure caused by fiber or copper failures. The **EASI™ IPS** Switches supports standard Spanning Tree Protocol (**STP**), Rapid Spanning Tree Protocol (**RSTP**) and Fast Reconfiguration Network Topology (**FRNT**). The latter protocol is alternative ring protocol optimized for rings containing many Switches and requiring very low re-configuration times.

Two possible configurations for Switch redundancy are available. One is Based on two Switches at each connection point in the ring, and the other is Based on dual ring configuration. Redundant ring topology is an excellent choice when high availability is required.

The re-configuration time is a critical factor for several applications. Therefore Switches from the **IPS** series re-configure the network in only 20 ms in case of ring failure (when using **FRNT**). Together with a reliable hardware design and optional redundant power supplies systems with maximum availability can be achieved. Switches are configured via Ethernet connection using PC with MS Windows 2000 operating system and **IP Config Tool** . This means that all equipment can be installed prior to the configuration. The same IP Config Tool can also be used for remote configuration and management.

Note! No routers and other equipment filtering broadcast traffic can be placed between the management PC and the ring Switches.

Ring Wiring

Connect port **8** to port **7** on the next Switch in the ring.

Note! RSTP/STP and FRNT can not be combined.

Spanning Tree Protocol (STP)

The **EASI™ IPS** switches support the Spanning Tree Protocol. The Spanning Tree Protocol, which is also referred to as **STP**, is defined in the IEEE Standard **802.1d**.

The STP provides a loop-free network. When a switch supporting STP recognizes a loop in the network topology, it blocks one or more redundant ports. Spanning Tree Protocol continually explores the network, so when the network topology changes, STP automatically reconfigures switch ports to avoid the failure by blocking certain ports. It allows the device to interact with other STP compliant devices in your network to ensure that only one path exists between any two stations on the network.

Rapid Spanning Tree Protocol (RSTP)

The **EASI™ IPS** switches support the Rapid Spanning Tree Protocol. The Rapid Spanning Tree Protocol, which is also referred to as **RSTP**, is defined in the IEEE Standard **802.1w**.

RSTP is an evolution of the STP, and provides faster spanning tree convergence after a topology change. The 802.1d terminology remains primarily the same, and most parameters have been left unchanged so users familiar with 802.1d can rapidly configure the new protocol comfortably.

Fast Re-configuration of Network Topology (FRNTv0)

The **EASI™ IPS** switches support the Fast Re-configuration Topology Protocol version 0, which is also referred to as FRNTv0. The FRNTv0 protocol is similar to the IEEE Spanning Tree Protocol (STP) except for the following:

The **FRNT** keeps network load generated by ring packets at very low level, thus the reaction times are faster. Each switch in a ring topology has knowledge of the network topology, not only of its neighboring switches as is the case for **STP**. A **FRNT** topology change event packet will be sent directly to the focal point switch in case of a topology change (e.g. a link loss or a link establishment), while a **STP** implementation will only send **STP** control packets one network hop.

The ring is managed by one Switch selected as Focal Point in **FRNT**. The other Switches in the ring are called member Switches. The **FRNT** ring solution can recover from a failure in only 20 ms if such a failure does occur.

*Note: When using **FRNT** protocol all Switches have to be **EASI™ IPS** series Switches.*

Virtual LANs (VLAN)

General

A virtual LAN, commonly known as a **vLAN** or as a **VLAN**, is a logically-independent network. Several VLANs can co-exist on a single physical switch. A VLAN consists of a network of computers that behave as if connected to the same wire - even though they may actually physically connect to different segments of a LAN. Network administrators configure VLANs through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs emerges when physically moving a computer to another location: it can stay on the same VLAN without the need for any hardware reconfiguration. The **IEEE 802.1Q** tagging protocol dominates the VLAN world.

A physical Ethernet network can be divided into several overlapping Virtual LANs (VLAN) without having IEEE802.1Q tagging or GVRP (Generic VLAN Registration Protocol) support on the Ethernet end nodes. All Ethernet trunk ports are member of all of the seven legal VLANs. A trunk port means a switch port connected to another switch; where a network redundancy protocol is running (e.g. FRNT or RSTP). This means that the VLAN tables on each switch are dynamically updated during a network topology change. Thus, no VLAN user configuration is required on the trunk ports.

See page 15 how to configure the VLAN settings.

Operation

The VLAN implementation is meant for both Ethernet end nodes that support tagging and for those that do not. An Ethernet end node that is not able to send tagged packets can, however, only participate in one VLAN, i.e. the default VLAN id for the port is used as the VLAN for such an end node. A default VLAN id for a given port will be associated to each untagged packet received on the switch (or tagged packet with VLAN id equal to 0). This VLAN id will be added to packet as an IEEE802.1Q tag. This tag can be removed at the output port(s) if the port(s) is configured for tag removal.

Seven different VLANs are available:

- White, VLAN id = 1, priority = 7 [high]
- Red, default VLAN id = 2, default priority = 0 [low]
- Blue, default VLAN id = 3, default priority = 0 [low]
- Green, default VLAN id = 4, default priority = 0 [low]
- Yellow, default VLAN id = 5, default priority = 0 [low]
- Brown, default VLAN id = 6, default priority = 0 [low]
- Pink, default VLAN id = 7, default priority = 0 [low]

The VLAN that is selected as the default VLAN for a given port will appear as an unchangeable VLAN, while other VLAN's selected for the same port has only relevance in case the end node connected to the same port is able to send and receive packets with these VLAN ids. All ports on a switch are members of the white VLAN, and this is cannot be changed. However, an end node can not send "white" packets unless the end node sends packets with the white VLAN id unless the default VLAN for the port is the white VLAN.

Port 1 has the white VLAN id as the default VLAN is, and this cannot be changed. An end node that is used for network management (SNMP or IP configuration) must always use the white VLAN in order to communicate with the switch's CPU. Thus, the switch CPU can always be accessed via port 1 with untagged packets, since port 1 has the white VLAN as the default VLAN.

Note! this means that red, blue, green, yellow, brown and pink packets never will be sent to the switch CPU. This is important in order to avoid that the port between the switch fabric and the CPU becomes a bottleneck, where important packets might be lost (e.g. FRNT control packets).

Example: A non white broadcast load close to full wire speed is not a problem for correct switch CPU operation.

The tag is not removed on packets sent on a trunk port, and each trunk port is member of all seven VLANs. This means that the user does not need to set any VLAN parameters on the trunk ports, and that any network topology change will be handled automatically.

The layer 2 priority of a given VLAN can also be set. I.e.:

- Priority 0, 1: QoS level 1
- Priority 2, 3: QoS level 2
- Priority 4, 5: QoS level 3
- Priority 6, 7: QoS level 4

This priority will be added to the tag. The legal VLAN id range is 1...4096. A few VLAN ids in this range are reserved for other use. These ids can not be set in the IP Config Tool . The network should only be based on switches enabled for VLAN or not. A mix of switches with and without VLAN support will not provide the user with the capability of tag removal on all parts of the network.

IP Config Tool

Introduction

This chapter introduces how the **IP Config Tool** is used to configure and manage the **IPS** switches. The IP Config Tool is used to configure the network settings such as IP address, subnet mask and default gateway of the **IPS** switches. This Tool is also used to configure the redundant ring and time server parameters.

Port 1 is always advised to be used as a local management port. In case a device is connected to the Port 1, only remote management is available.

System Requirements

- The IPS Fast Ethernet switch (SW Ver 3.14 or newer)
- The X86 based PC computer running Windows 2000 or XP
- Ethernet network card
- Administrative rights are required during installation
- The IP Config Tool (**TelestIPConfig.exe**, ver **9.6.1** or newer).
- The interconnection Ethernet cable

How to Get the IP Config Tool

You can download the latest version of IP Config Tool from Teleste's web site at: www.teleste.com.

How to Install the IP Config Tool

Unzip the file **IP_Config_Tool.zip** by using e.g. WinZip and extract all the files to the folder you want. Ensure that all files reside in the same folder and that you can find the folder after you extract them there. Start the program by running **TelestIPConfigxxx.exe**.

Operating

The IP Config Tool consists principally of several windows. On the Selected Device page you can configure the chosen device.

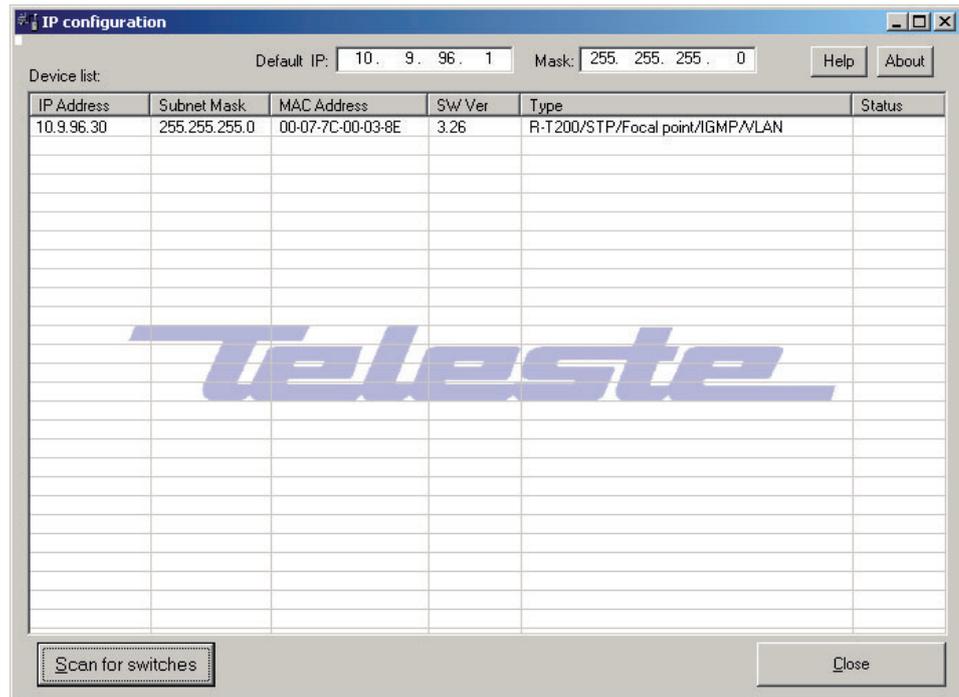
The IP Config Tool has the following configuration display pages that are introduced in this document:

- **IP Configuration / Device list**
- **Selected Device**
- **Port configuration**
- **VLAN configuration**

The information on configuration sheets is shown in data fields or boxes. You can change settings in data fields or boxes whose background is white. Place your cursor in the desired data field or box and enter the new setting. Some settings are entered by ticking a checkbox or clicking on a radio button, by selecting from a pull-down list or by scrolling digits with the help of spin buttons.

Information without datafield or box is read only parameter and can not be change.

Device List Page

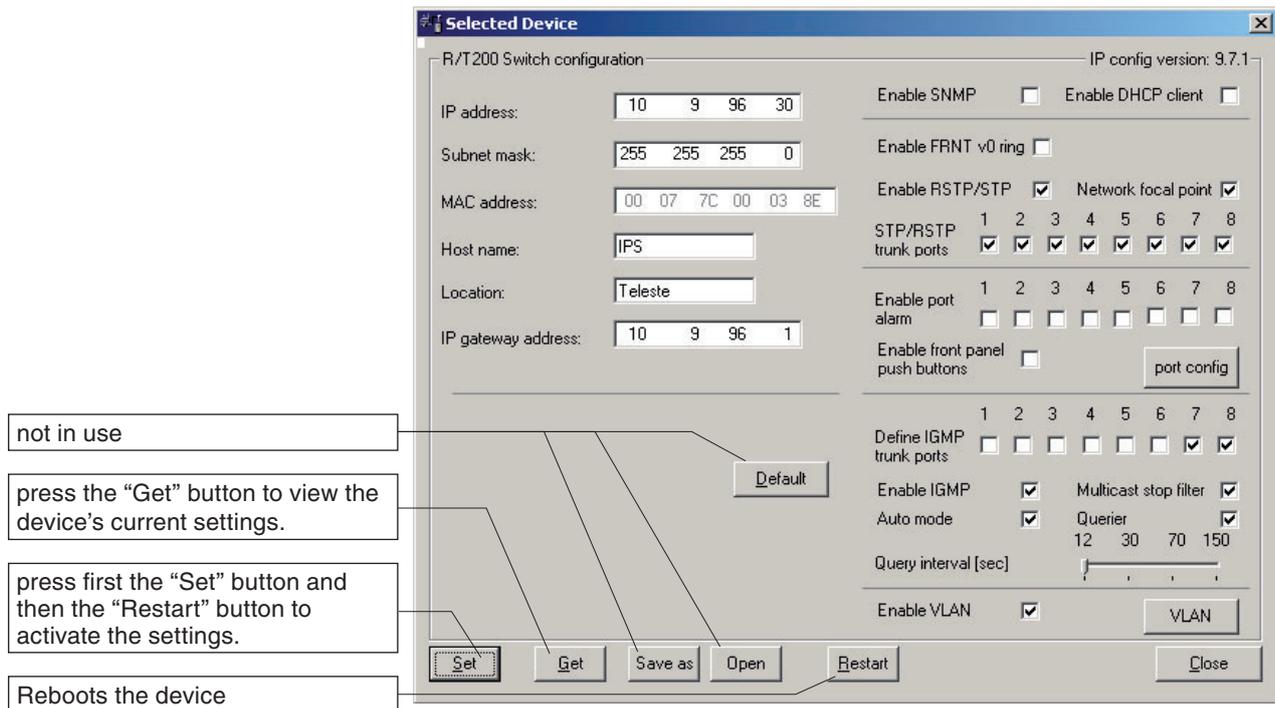


Picture 6. Device list page view (with one Switch).

How to Configure the Switch

1. Connect the PC into the Ethernet **port 1** of the **IPS** Switch via Ethernet cable and open the IP Config Tool by running the **TelesteIPConfig.exe** program.
The following "IP configuration" window appears on the screen (like picture 6).
2. Assign a free IP address, which is in the same subnet as the PC, to the "Default IP" and click button until the Switch(es) appears on the device list. Now all Switches in the same network will appear on the device list (e.g. one switch in picture 6).
3. Click on the Switch that you want to configure --> "**Selected Device**" window will appear on the screen (picture 7). From this window you can modify the switch settings.

Selected Device Page



Picture 7. Selected Device configuration page view.

Click on the Switch in the IP Configuration page window's device list. "Selected Device" configuration page will appear on the screen (picture 7). On this page you can see/modify the switch's configuration, as following:

IP address: Device IP address

Subnet mask: Mask for subnet definition

MAC address: Device MAC address

Host name: User definable alias name for the device

Location: User definable location name for the device

IP gateway address: Gateway address for router definition

Enable SNMP: Enables Switch to use SNMP

Enable DHCP client: Enables Switch to use DHCP protocol to obtain an IP address. When used with Teleste Libretto product the selection also enables download of config from remote (root Switch)

Enable FRNT v0 ring: Enables FRNT v0 for redundancy Switching

Enable RSTP/STP ring: Enables RSTP/STP for redundancy Switching

Network focal point: The device can be set as focal point in FRNT or RSTP/STP ring (root Switch)

RSTP trunk ports: Enables RSTP signalling on the selected trunk port(s)

Enable port alarm: Enables port alarm for selected port(s)

Port config: Opens port configuration window

Define IGMP trunk ports: Specifies the switch trunk ports. IGMP information is forwarded on the port towards the IGMP Querier and on the switch trunk ports

Enable IGMP: Enables IGMP (RFC 1112)

Multicast stop filter: Enables filtering of all multicast traffic which does not have registered receiver (unknown multicasts)

Auto mode: Ensures that only one Querier is present in the existing network. A device with the lowest IP address will be the Querier

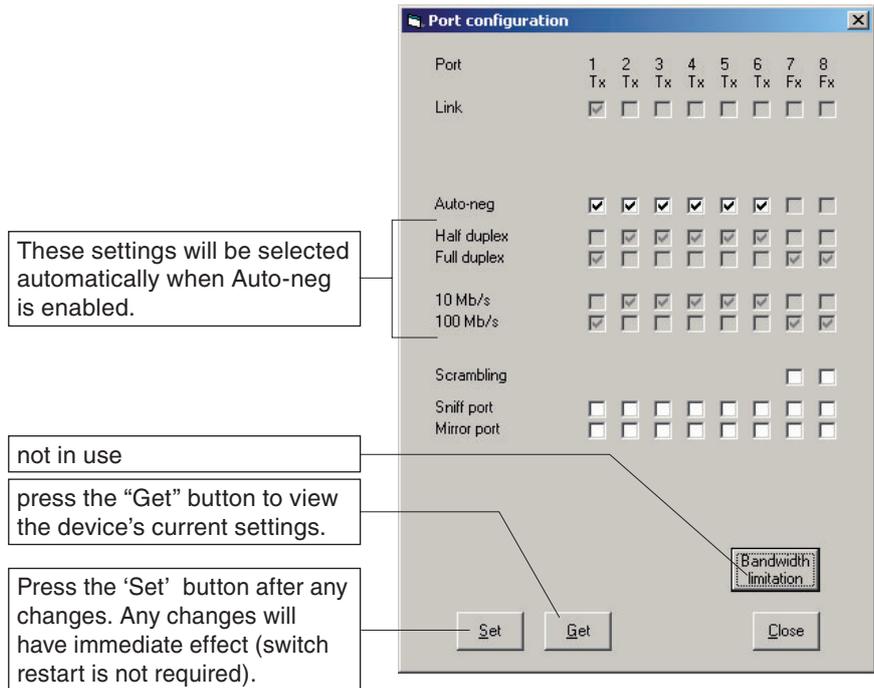
Querier: Enables Switch to act as a Querier (IGMP server)

Query interval (sec): Configurable IGMP query interval in seconds

Enable VLAN: Enables VLAN function

VLAN button: Opens VLAN configuration window

Port Configuration Page



Picture 8. Selected Device configuration page view.

Click on the **port config** button in the selected device window.

"**Port configuration**" window will appear on the screen (picture 8). On this page you can see/modify the port configuration, as following:

Link: Shows whether the link is up or not and link type, either Tx (electrical) or Fx (optical)

Auto-neg: Enables the auto-negotiation feature, which allows the switch to discover and manage the speed and duplex mode settings on a given port. The combination that provides the best performance will be automatically selected

Half duplex & Full duplex: Sets the duplex mode on a given port. If Auto-neg feature is enabled on a given port, this setting can not be modified

10/100 Mb/s: Sets the speed on a given port. If Auto-neg feature is enabled on a given port, this setting can not be modified

Sniff port & Mirror port: This feature allows to sniff the traffic on a given port. The "Sniffed port" should be selected and all the traffic will be redirected to the selected "Mirror port"

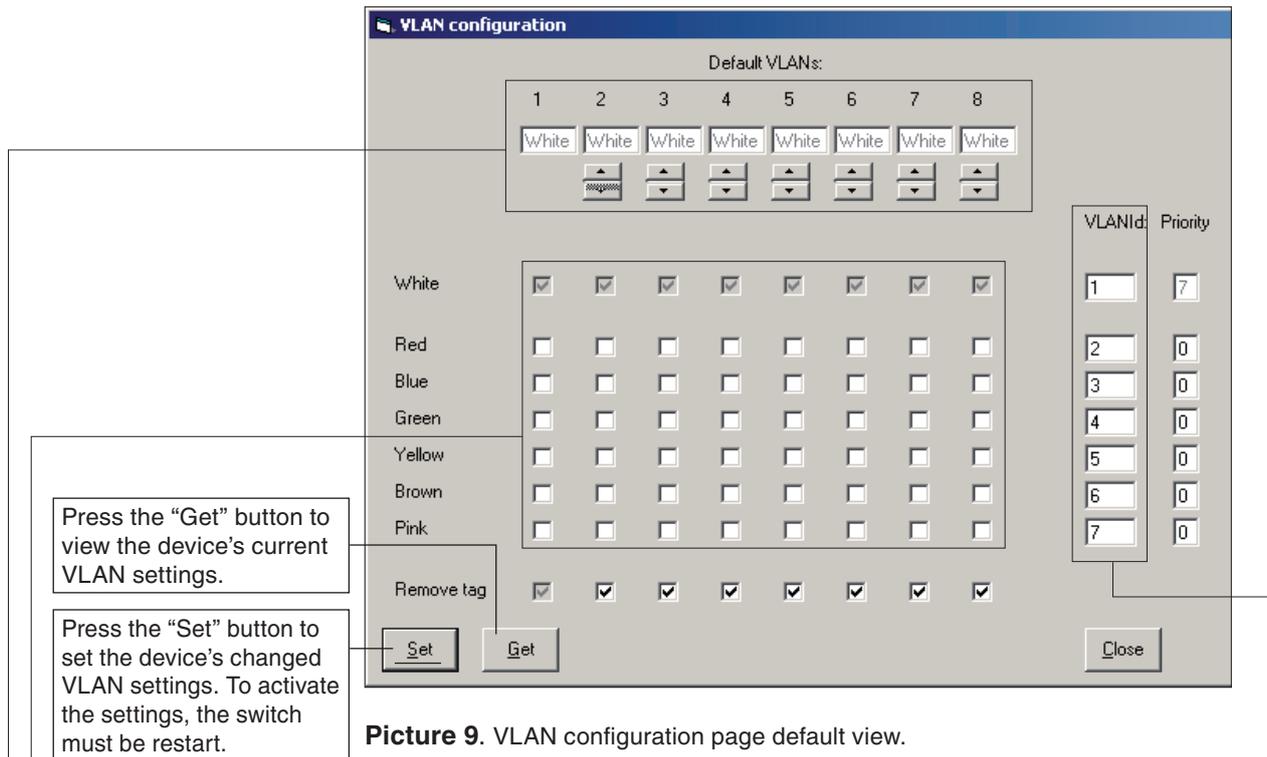
Scrambling: Allows the switch to code the traffic flowing through the selected port. This setting is only available for the trunk ports and must be the same on both sides of the link. This parameter is important for backward compatibility: In older firmware versions scrambling is always enabled (and cannot be changed)

These settings are user-editable if the auto-neg tick box for the port is not ticked.

Note! The auto-negotiation, duplex connectivity and speed settings for an Fx port are not user-editable.

The fiber configuration is not compatible with older firmware releases of the switch). The latest versions can handle both scrambled and non scrambled fiber communication. This feature is configurable via IPConfig or SNMP.

VLAN Configuration Page



How to Configure VLAN

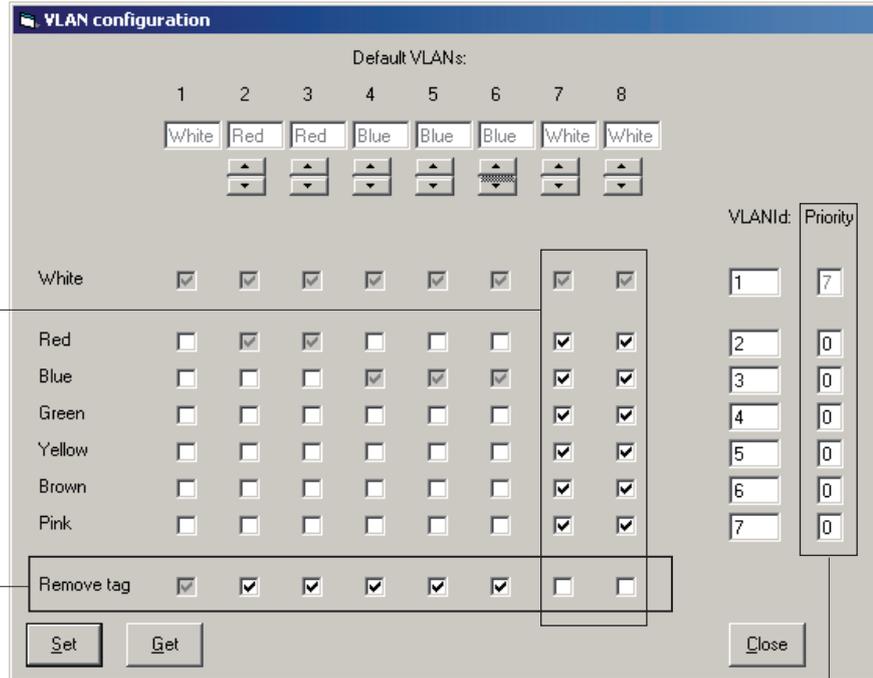
The VLAN tick box must be ticked in order to enable the VLAN button. Click on the VLAN in the Selected Device window. "VLAN configuration" page will appear on the screen (picture 9). On this page you can see/modify the switch's configuration regarding VLANs. The following VLAN parameters can be set:

- **Default VLAN per port**
White, Red, Blue, Green, Yellow, Brown and Pink. The default VLAN for a given port is the only VLAN available for the port if the end node connected to the port is unable to send and receive tagged packets. Selection is done by pushing up/down buttons on the upper side. Default VLAN for port 1 is fixed to White.
- **Additional VLANs per port**
A given port can be member of additional VLANs. This feature is only relevant is the end node is able to send and receive tagged packets with these VLANs' ids. All ports are as well members of the White VLAN and can't be changed.
- **VLAN id's** (The legal range is **1..4095**). The default are the following:
 - o White VLAN id = 1
 - o Red VLAN id = 2
 - o Blue VLAN id = 3
 - o Green VLAN id = 4
 - o Yellow VLAN id = 5
 - o Brown VLAN id = 6
 - o Pink VLAN id = 7

NOTE! VLANs are defined by their VLAN id. The color scale is intended just as a help. When configuring VLANs in different switches, only VLANs with the same id will be part of the same logical group. Therefore, the same VLAN color in all switches must have the same id in order to succeed.

Trunk ports are automatically detected, when at least two switches are connected together. VLAN settings for these ports are automatically set and then can not be changed.

It's recommended that tag removal operation is activated (checkbox is checked) due to the fact that not all NICs (Network Interface Card) are able to understand VLAN tagged frames.



Picture 10. VLAN configuration page example view.

- Priority**
It is the Layer 2 Priority for each VLAN. The legal range is 0...7. The lower the value is, the lower the priority for the given VLAN. For VLAN White priority is fixed to 7.
- Remove tag**
Tag removal on egress. If this option is ticked, VLAN tags will be removed from Ethernet packets on egress: output data will have no VLAN tag. This option is always ticked in port 1 and can't be changed.
Trunk ports must be member of all VLANs and the VLAN tags must not be removed. This settings allow data from all VLANs to be transmitted transparently through the network between different switches.

See picture 10 for a setup example on VLAN configuration:

- Ports 1, 2, 7 and 8 have as default VLAN "White". VLAN id is 1 and its priority is 7.
- Ports 3 and 4 have as default VLAN "Red". VLAN id is 2 and its priority is 0.
- Ports 5 and 6 have as default VLAN "Blue". VLAN id is 3 and its priority is 0.
- VLAN tags are removed on egress on all local ports (ports 1 to 6)
- Trunk ports (7 and 8) are members of all VLANs and VLAN tags are not removed on egress.

After configuring VLANs, save the settings by pressing **Set** button and then end VLAN configuration session by pressing **Close** button. To activate the settings restart the Switch at the Device Configuration Page by pressing **Restart** button.

How to Create the STP/RSTP Ring

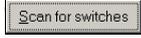
1. Select which Switch will be your Root/Focal Point Switch to manage the ring.
2. Connect your PC with IP Config Tool installed to the Root/Focal Point Switch port 1.
3. Open Teleste IP Config Tool and assign a free IP address, which is in the same subnet as the PC, to the “Default IP” and click button until the Switch(es) appears on the device list. Now all Switches in the same network will appear on the device list.
4. Click on the Switch which is chosen to be Root/Focal Point Switch and tick “**Network focal point**” box.
5. Restart the Switch by clicking button.
6. Set IP address and subnet mask (no restart required).
7. Connect the rest of the Switches (or one at a time) and set IP address and subnet mask.

Note! In case that more than one switch have been selected to be Root/Focal Point, the one which has smallest IP address will act as network's Root/Focal Point.

8. Close the ring and click button to check the status of all Switches.

Creating FRNT v0 Ring

In a FRNT v0 ring configure only one **IPS** switch must be configured to be the network Focal Point. The Focal Point switch have the role as Redundancy Manager, and thus be responsible for recovery when a connection between the switches is broken. To set up a FRNT v0 configuration the following steps must be followed:

1. Connect the switches in a bus topology (do not close the ring before the switches are all configured for FRNT 0)
2. Define the Switch, that shall be the network Focal Point
3. Power up the switch and connect this to the network
4. Assign an IP address for the configuration software (ensure the address range is within the same Subnet as your assigned IP address for your PC)
5. Press the “Scan for devices” button. The Switches on the network will be listed
6. Click on the focal point switch from list
7. A new configuration Window will open
8. If required; assign a new IP address and Subnet address for this Switch
9. Press the  button to assign this IP address and Subnet settings to the Switch
10. Tick the “Enable FRNT Ring” and “Network focal point” to set the Switch to be the Focal Point and Bus Member to ensure the Switch configured to run within a Redundant Ring
11. Press the  button (all your changes performed will be set)
12. Press the  button to re-configure the Switch. The Switch will run through the start sequence. During this period communication to the Switch will be lost
13. Connect the next Switch into the ring
14. Press the  button. The second Switch will appear on the list
15. Click on the second Switch from list
16. If required; assign a new IP address and Subnet address for this Switch
17. Tick “Enable FRNT ring” to ensure the Switch is configured to run within a Redundant Ring
18. Press the  button.
19. Press the  button to re-configure the Switch. The Switch will run through the start sequence. During this period communication to the Switch will be lost.
20. Continue connecting Switches in this manner until the ring has been completed
21. Close the ring

FRNT version 0, configuration rules are as follows:

- Port 7 and 8 are FRNT version 0 ports
- Always connect port 8 to 7, 8 to 7, .. 8 to 7 through the ring (never 7 to 7 or 8 to 8)
- One switch as the network focal point (root)

Notes on the IP Config Tool

1. IP Config Tool's subnet mask has to be same as PC's.
2. IP Config Tool must have temporary IP address in the same subnet as the PC (for example if PC has **10.9.96.5** the temporary IP can be **10.9.96.1**).

Note! DO NOT USE SPACE BUTTON when typing default IP address for IP Config Tool!

3. If system role (root/or member switch) is changed, IP and subnet mask may not be changed at the same time.
4. If system role is changed a reboot of the device is required.
5. No reboot is required when changing IP and subnet mask settings.
6. When using FRNTv0, only one root switch may be seen by the IP Config Tool during ring configuration, otherwise the member switches configured may belong to the wrong ring (root MAC address can be collected from a root switch that belongs to another ring)
7. No routers or other devices filtering broadcast traffic are allowed to be connected between the ring switches and the configuration PC.
8. If a switch is configured in the wrong way you may have to connect the PC directly into this switch in order to correct the settings.

Trouble Shooting

1. In case Switches are not be found, check that there is no spaces used in IP Config Tool's default IP address field.
2. When using FRNTv0, only one root switch is allowed in a ring.
3. Setting system role (root/member) requires restart of the switch.
4. Disable SNMP before upgrading the switch firmware.

Firmware Upgrade via IP Config Tool

1. Make sure that the PC, the IP Config Tool and the switches that are to be upgraded are in the same IP subnet
2. Unzip the zip file containing the new image to the FTP server directory
3. Select the switch in the IP Config Tool that you want to upgrade
4. Write upgrade in "Host name" field and the name of the unzipped filename (e.g. vx326.bin) in the "Location" field
5. Click "Set" button. A progress bar will appear in the bottom of the dialog box, and the switch will restart

Note! Make sure that you have waited at least 5 minutes after the upgrade procedure is started (pushed the Set button) before you remove power, or you have verified that the switch has restarted. Removing power during the upgrade procedure might damage the file system and the switch will not restart.

IP Config Tool and Firmware Versions

The IP Config Tool version **7.x.x**, or newer, can be used versus any managed switch from Teleste. Switch control options for a given switch will be enabled based on the type of switch and firmware version running on the switch. Old firmware versions of the IP Config Tool can be used with **IPS** switches, but then the user will not be able to configure the new switch features.

Glossary

Auto-Negotiation

A Protocol defined in the Ethernet standard that allows devices at either end of a link segment to advertise and negotiate modes of operation such as the speed of the link, half- or full-duplex operation and full-duplex flow control.

CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

A set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision). The CSMA/CD method is internationally standardized in IEEE 802.3 and ISO 8802.3.

DHCP (Dynamic Host Configuration Protocol)

Internet standard (RFC 1541) protocol for distributing configuration information to network and allows a computer to obtain its own IP address automatically rather than having it entered manually.

Fast Ethernet (100Base-T and 100Base-X)

Uses CSMA/CD access method at 100 Mbps; IEEE 802.3u. Can use full duplex (200 Mbps).

Full Duplex

The ability to transmit and receive signals simultaneously.

Gateway

Gateways are points of entrance to and exit from a communications network. Viewed as a physical entity, a gateway is that node that translates between two otherwise incompatible networks or network segments.

Gigabit Ethernet (1000Base-T and 1000Base-X)

Informal name for standard IEEE 802.3z. CSMA/CD technology designed to provide 1 Gbps network connectivity. Based on existing and evolving 802.3 standards, Gigabit Ethernet is expected to incorporate both half and full-duplex operation, link-level flow control, VLAN support, and systems management. Support for one repeater per collision domain, backward compatibility with 10Base-T and 100Base-Tx.

Half Duplex

The ability to transmit and receive signals in both directions, but only in one direction at a time.

Host

Any device on the network that implements communication above the Data Link Layer.

Hostname

A synonym for IP domain name, which typically takes the form host.

Hub

A physical layer device, generally used to serve at the center of a star-topology network. Hubs accept

host, internetworking, and network management modules; and provide re-timing/repeater, bridging, and/or network management functionality. A hub is an Ethernet multi-port repeater, which sometimes referred to as a concentrator.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet.

IEEE 802.3z

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet.

IEEE 802.1q

VLAN Tagging - Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1d

Spanning Tree Protocol controls redundant links between Layer 2 switches and ensures there's only one active path any two devices and no loops; does not allow for load sharing, only redundancy.

IEEE 802.1p

Provides traffic class expediting and dynamic multicast filtering. Essentially, it provides a mechanism for implementing Quality of Service (QoS) at the MAC level. 802.1p is part of the IEEE 802.1d standard along with IEEE 802.1q.

IEEE 802.1w

Rapid Spanning Tree is an update of the original Spanning Tree Protocol that improves Layer 2 convergence from 30 seconds or more to a few seconds or less.

IEEE 802.3p

Provides QoS. Traffic is classified and prioritized attending to Layer 2 class of service field.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP (Internet Group Multicast Protocol)

The Internet standard (RFC 1112) extensions to IP that support IP datagram multicasting to a "host

group.” Membership in a host group is dynamic and there are no topological restrictions to participating in a host group. Hosts groups may be either permanent or transient. Host groups are identified by Class D IP addresses. There are three levels of conformance: 0: no support; 1: support for sending but not receiving; 2: full support.

IGMP Querier

The device which manages IGMP service. IGMP Querier asks all the devices in a network for possible multicast groups of interest. In a IGMP enabled network where multicast traffic is being delivered, multicast receivers must join multicast groups, advertise periodically their membership to the groups and finally, leave the groups. There must be only one IGMP Querier in a given network.

IP (Internet Protocol)

The most important protocol of the Internet suite. IP allows information to traverse multiple networks worldwide. The network layer protocol (RFCs 760, 791) for the Internet protocol suite.

Local Area Network (LAN)

A local area network is generally a private network. It is under the control of the owner and used by a set of related individuals and/or workgroups, typically within a single building or over a group of neighboring buildings. LANs are a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

MAC (Media Access Control)

The protocol level that describes network management frames sent on the 802.5 token ring. Most MAC frames are handled transparently by the network adapter.

MAC Address

The unique physical (data link layer) address of an individual network interface. The standard specifies both 16- and 48-bit addresses. The 802.1 standards committee has defined a canonical format for writing and transmitting a MAC address. It is expressed as six octets separated by hyphens, each octet represented as twohexadecimal digits, least-significant bit first (littleendian). (As a matter of custom, non-canonical, most-significant bit first representation is given using colons as the octet separator.) For example, 08-00-20-85-e6-8d is a typical canonical MAC address. Within the MAC address are a number of fields of interest. The most significant (first) bit, known as the I/G bit (for Individual or Group) is 0 if the address represents an

individual station; it is 1 if the address is a multicast (group or broadcast) address. The second bit, known as the U/L (for Universal or Local) bit is 0 if the address is globally administered and registered with the IEEE; it is 1 if it is a locally administered address.

MAC sublayer

Media Access Control sublayer. As defined by the IEEE, the lower portion of the OSI reference model data link layer. The MAC sublayer is concerned with media access issues, such as whether token passing or contention will be used.

Metropolitan Area Network (MAN)

A network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

MIB (Management Information Base)

A collection of objects (database) that can be accessed via a network management protocol. See SNMP and RFC 1066.

MIB-II (Management Information Base, Version 2)

The revised object definitions for Internet standard network management. Objects are defined using a subset of the Abstract Syntax Notation One (ASN.1). See SNMP and RFC 1213.

Multicast

Communication between a single sender and multiple receivers on a network. Streaming content can be sent multicast from one server to many users.

Multicast Address

An address that refers to multiple network devices. Synonymous with group address.

Netmask

A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. This is also sometimes referred to as the address mask or subnet mask.

Network Address

The hostid 0 of an IP address is reserved; an IP address with the hostid zero is used to refer to the network itself.

Network Layer: OSI Layer 3

Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections. Responsible for routing, switching, and subnetwork access across the entire OSI environment.

Ping (Packet InterNet Groper)

Ping is a program that “bounces” a request off of another computer over a network to see if the remote computer is still responding. If the ping comes back, the remote computer is still alive.

QoS (Quality of Service)

Interactive video conferencing requires a high QoS. QoS is important as it determines the quality of your video call. Low quality of service results in latency and a jerky picture with poor and inconsistent audio quality.

Ring

A network topology in which all nodes are connected in a closed loop. Transmission is permitted by passing a token around the ring; a node copies out messages addressed to it and copies in messages addressed to others. Message receipt verification can also be performed with the token.

Router

On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.

Server

A networked computer that contains public resources or services that can be accessed using software applications called “clients.”

SNMP (Simple Network Management Protocol)

A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. **SNMPv2** is a proposed update of version 1, that provides additional administrative structure, authentication, and privacy.

Spanning Tree Protocol (STP)

A standard bridge protocol (IEEE 802.1d). This protocol allows bridges to dynamically discover a subset of the LAN topology that is loop-free and provides connectivity to all LAN segments.

Switch

An internetworking device (multiport bridge) that intelligently segments networks to increase overall bandwidth, isolate traffic and provides an interface to high-speed networks. The switch selects a path or circuit for sending a unit of data to its next destination. A switch may also include some functions of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.

Type of Service (ToS)

A byte in the IPv4 header (RFC 1349). It is represented in an 8-bit (1 byte) field in the header which is used by a variety of QoS methods, including IP Precedence, Differentiated Services Code Point, and ToS field.

Unicast

Communication between a single sender and a single receiver on a network. Compare with Multicast.

VLAN (Virtual LAN)

Network configuration, emulating a broadcast domain, where stations communicate using LAN protocols as if they were on the same LAN, but where they are actually on multiple segments connected through layers 1, 2, and/or 3.

Wide Area Network (WAN)

A geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network connects local area networks to one another, generally using public infrastructure or services. The connections are made using the shared public infrastructure, public infrastructure leased for private use, and sometimes, private infrastructure (e.g., fiber) with public services.

Technical Specifications

Parameter	Specification	Note
Optical		
m/m 1310 nm	2 km	2 fibres
s/m 1310 nm	15 / 40 km	2 fibres
Ethernet		
<u>Local ports</u>		
Number of ports	6	full duplex
Standard	10/100Base-TX	CAT-5 / CAT-5e
<u>Up-link ports</u>		
Number of ports	2	full duplex
Standard	100Base-FX	m/m & s/m fibre
<u>Protocols</u>		
802.3	10Base-T	
802.3u	100Base-TX, -FX	
802.1q	VLAN	
802.1d	STP	
802.1w	RSTP	
802.1p	QoS	layer 2
802.3p	QoS	layer 3 (IP ToS)
802.3x	flow control	
IGMP	version 1, 2 & 3	
FRNT v0	redundant ring	proprietary protocol
SNMP	version 2c	
DHCP		IP address adquisition
Management		
IP config tool	local via ethernet port	
SNMP	remote via network	
General		
Supply voltage	10.5...18 V DC	
Power consumption	11 W	
Dimensions (H x W x D)	1U • 19" • 236 mm	D without connectors
Weight	0.7 kg	
Connectors	RJ-45 MT-RJ LC	CAT-5 (UTP) optical multimode optical singlemode
Operating temperature	-20...+70 °C	field-hardened
Storage temperature	-30...+70 °C	
Humidity	95 %	non condensing
Vibration	EN50130-5	1995
Damp heat	BS2011	p2.1
Emissions	EN50081-1, CE, FCC part 15	
Susceptibility	EN50130-4	

Copyright acknowledgements

Information in this document is subject to change without notice and does not represent a commitment on the part of Teleste Corporation.

Copyright © Teleste Corporation. All Rights Reserved.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any other language without the express permission of Teleste Corporation.

Teleste Corporation
Video Networks
P.O. Box 323
FIN-20101 Turku
FINLAND
www.teleste.com

Trademark acknowledgements

EASI™ is trademark of Teleste Corporation.

WEEE directive

Directive 2002/96/EC of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) obliges that producers appropriately mark electrical and electronic equipment with the symbol indicating separate collection. This obligation applies to the equipment put on the market in EU after 13 August 2005.

Teleste devices which belong to the scope of the directive have been marked with the separate collection symbol shown below. The marking is according to the standard EN 50419. The symbol indicates that the device has to be collected and treated separately from unsorted municipal waste.



User manual revision history note:
The latest version is always available in pdf-format on our web site:
www.teleste.com

Teleste

www.teleste.com