V4.0

U/R/T200 series Operator Manual

1 Introduction

This Operator Manual describes the properties of the T200, R200 and U200 series.

1.1 T200

The T200 is the time synchronization switch series of Westermo OnTime. The T200 series has also full management support including QoS, network redundancy either based on FRNT or RSTP/STP, SNMP, IGMP snooping, VLAN and MAC security. The switches are approved for industrial use.

All chapters in this document are relevant for the T200 series.

1.2 R200

The R200 series contains the same features as the R200 series except for time synchronization.

All chapters in this document except chapter 13 are relevant for the R200 series.

1.3 U200

The U200 series is an unmanaged switch implementation with QoS support (layer 2 and 3). The U200 switch series has the same approvals for industrial use as the R200 and T200 series.

All chapters in this document except chapters 7-13 are relevant for the U200 series.

2 About Westermo OnTime

2.1 Company History

Westermo OnTime is dedicated to the implementation of industrial and deterministic Ethernet infrastructure. Westermo OnTime is a privately held company based in Norway and Sweden. We work closely with a number of large automation companies; enhancing older proprietary networks and working in partnership developing new network technology.

2.2 Mission Statement

Westermo OnTime's mission is to provide an extension of Ethernet to the factory floor, outdoor installation and real time application by offering high end Ethernet products that fulfilling industrial and real time requirements.

2.3 Core Technology

Westermo OnTime's Ethernet switches are based on a robust and reliable industrial design for maximum life cycle and minimum life time costs. Real time properties are implemented in order to achieve determinism for real time critical applications.

3 Ethernet – Industrial Ethernet

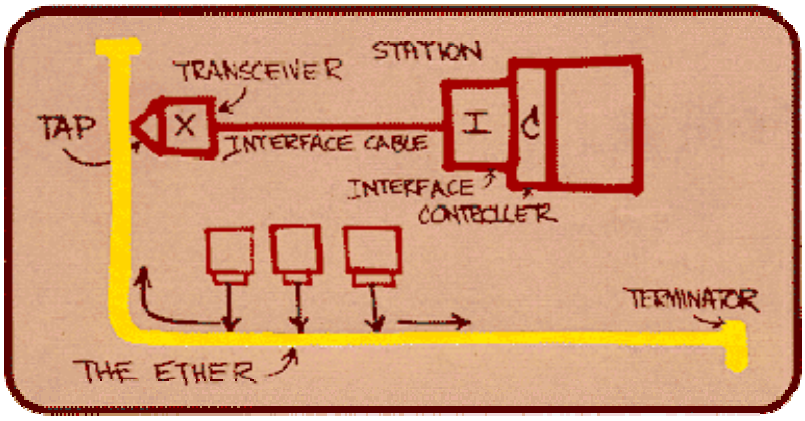
3.1 History of Ethernet

In late 1972, Metcalfe and his Xerox PARC colleagues developed the first experimental Ethernet system to interconnect the Xerox Alto, a personal workstation with a graphical user interface. The experimental Ethernet network was used to link Altos to each other, and to servers and laser printers.

The signal clock for the experimental Ethernet interface was derived from the Alto's system clock, which resulted in a data transmission rate on the experimental Ethernet of 2.94 Mbps.

Robert Metcalfe's first experimental network was called the Alto Aloha Network.

In 1973, Robert Metcalfe changed the name to "Ethernet," to make it clear that the system could support any type of computer; not just the Xerox Altos and to point out that his new network mechanisms had evolved well beyond the Aloha system. He chose to base the name on the word "ether" as a way of describing an essential feature of the system: the physical medium (i.e., a cable) carries bits to all stations, much the same way that the old "luminiferous ether" was once thought to propagate electromagnetic waves through space. Thus, Ethernet was born."



``*The diagram ... was drawn by Dr. Robert M. Metcalfe in 1976 to present Ethernet ... to the National Computer Conference in June of that year. On the drawing are the original terms for describing Ethernet. Since then other terms have come into usage among Ethernet enthusiasts."*

Figure 1

3.2 Industrial Ethernet – What Are The Differences?

Ethernet is moving into the Automation Industry. Manufacturers are exporting their legacy protocols onto Ethernet, designing new IP based communication protocols and providing

embedded Web-Pages within PLCs to provide real-time information using simple tools like Internet Explorer and Netscape.

However, the domain of Ethernet has always been controlled by the IT department who configured office networks normally with an iron fist and dictated to the company how the network would be designed with complex recovery protocols like spanning tree and SNMP to help with fault finding and system analysis. If a network failure occurred the IT department would casually look at repairing the equipment - there was no real rush as it was an office network. However, with Industrial Ethernet you need very fast repair time, and, with an IT department not present on the factory floor the maintenance personnel need to be made aware of the fault, find the error and repair it - quickly.

Industrial rated Switches are intended to be installed in harsh conditions and electrical environments with the added benefit of fast recovery of a network failure. The Westermo OnTime switches are an excellent example of how such Switches should be designed – very high operating temperatures, fast repair of redundant ring, layer 2 and layer 3 priority switching, time synchronization capability, etc. Without doubt, Westermo OnTime switches are technically superior to many similar models available on the market.

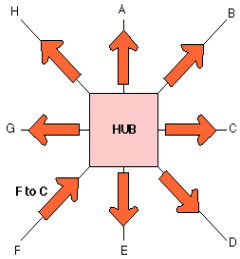
3.3 Switches vs. Hubs

A hub consists of a number of ports normally with either RJ-45 (copper) sockets and / or fiber optic ports that have a number of different styles of fiber optic sockets. Usually a 'patch cable' is connected to the hub; the other end is normally connected to a device (PC, Printer etc).

A hub has no intelligence and therefore is unable to identify addresses or any information contained within the Header frame of an Ethernet packet. This means that it is not capable of determining which port to send the frame to. Therefore, every frame is sent to every port.

A network of repeaters and hubs is called a 'Shared Ethernet' or 'Collision Domain'. Various systems will all compete with each other using 'Carrier Sense Multiple Access / Collision Detect' (CSMA/CD) protocol. ***This means that only one system is allowed to proceed with a transmission of a frame within a Collision Domain at any one time.*** This is a major disadvantage when using Hubs and Repeaters within a network.

If a hub sees a collision on a cable segment, it is detected and a 'jam' signal is generated. The 'jam' signal is sent to *all* connected devices. This ensures that every device is aware of the collision and they do not attempt to transmit during the collision.



All Ports Receive the Same Ethernet Frame

Figure 2, hub

To summarise, hubs operate with the following limitations:

- Only a single speed of operation – no ability to automatically change between 10M or 100M.
- Only one system is allowed to proceed with a transmission of a frame within a Collision Domain at any one time.
- Hubs require special ‘crossed’ cables to enables links from Hub to Hub (If no up-link port with twisted wiring is present).

4 Switch Operation

4.1 Introduction

A switch has to forward and receive packets from one LAN or device to another. The switch could forward all packets, but if this was the case it would have similar behavior to a hub.

It would be more intelligent if the switch only forwarded packets which need to travel from one LAN or device to another. To do this, the switch must learn which devices or LANs are connected to each port. In simplistic terms; it needs to learn the destination and source ports of each and every packet received on each individual Switch port. Once learnt, any identically addressed packet will be automatically be forwarded.

4.2 Error Detection

The switch stores every incoming packet and scans this for errors, usually by checking the frame CRC (cyclic redundancy check sum). If any errors are found or detected the packet is discarded. In addition each frame is checked for size. Undersized packets (less than 64 Bytes) and oversized packets (more than 1518 bytes (*)) are also discarded.
Once these basic checks have been carried out the switch can then start learning packet source and destination information.
(*) When implementing Ethernet MAC tagging maximum Ethernet packet length is increased to 1522 bytes.

4.3 Flooding

The switch needs to make a decision regarding which port(s) the packet is to be forwarded to. This decision is based upon the MAC tables that are maintained and updated automatically by the Switch. The process is known as Layer 2 Switching.
When first powered on the MAC tables within the Switch are empty. When a packet is received on a port the Switch does not know where the destination MAC address is located. The Switch learns the address by ‘flooding’ the packet out to all ports. Eventually, the destination node responds, the address is located and the Switch remembers the destination port. In simplistic terms; when a Switch receives a packet on a port it stores the source MAC address in the MAC table that corresponds to that Port. The flooding technique is always used with Broadcast and Multicast packets. If the switch is equipped with multicast management then multicast packets will not be flooded.

4.4 MAC Table and Packet Memory

.
The MAC table can hold up to 8 K entries with a MAC aging interval of five minutes. MAC aging means that a MAC address learned on a given port will be removed from the MAC table if no packets with this MAC address as the source MAC address are received on the port for five minutes.

The total packet memory is 1Mbyte. This means that 657 (maximum packet length - 1522 bytes) to 15625 (minimum packet length - 64 bytes) packets. The packet memory is used to handle short high load/overload situations. Exceeding the packet memory means that the switch engine will drop packets. Packet re-transmission is then required and must be handled by the end nodes (e.g. TCP).

A MAC table of 8 K entries and a packet memory of 1Mbyte is adequate for large networks.

4.5 Full Wire Speed

The Switch supports full wire speed. This equates to 100Mbit/s full duplex on every port. 100Mbit/s in each direction on all ports equals 200Mbit/s per port.

4.6 Twisted Pair Port Specification

4.6.1 Introduction

The T/R/U200 series is available with up to eight copper ports. The copper ports support the long cable specification that enables standard CAT5e copper cables to run up to 150 Meters when used with devices that also support this specification. This highlights the enhanced design specification the switch employs when used in noisy electrical environments. In industrial networks long cables should be avoided but equipment specified according to long cable specification gives more margins for disturbances.

Port configuration is available via the IP configuration tool or the push buttons on the front panel of the Switch. See the Installation Guide for details.

4.6.2 MDX/MDI-X

There are two types of copper Ethernet ports available; MDI (Medium Dependant Interface) and MDI-X (Medium Dependant Interface Crossover). The MDI port types are associated with copper interfaces available on NICs (Network Interface Cards), PLCs, VSDs and DCSs etc. The latter type of interface (MDI-X) is found on Hubs or Switches.
In addition there are two types of Ethernet cable available. These are referred to as a ‘straight through cable’ or ‘crossed cable’.

4.6.3 Straight Connection –Switch-PLC, Hub-PLC, Switch-NIC etc.

	Connector A				Connector B		
Pair 1		pin	4	<------->	Pin	4	
		pin	5	<------->	Pin	5	
Pair 2	RD +	pin	3	<------->	Pin	3	RD +
	RD -	pin	6	<------->	Pin	6	RD -
Pair 3	TD +	pin	1	<------->	Pin	1	TD +
	TD -	pin	2	<------->	Pin	2	TD -
Pair 4		pin	7	<------->	Pin	7	
		pin	8	<------->	Pin	8	

4.6.4 Crossed Connection – Switch-Switch, Hub-Hub, Switch-Hub

	Connector A				Connector B		
Pair 1		pin	4	<------->	Pin	7	
		pin	5	<------->	Pin	8	
Pair 2	RD +	pin	3	<------->	Pin	1	TD +
	RD -	pin	6	<------->	Pin	2	TD -
Pair 3	TD +	pin	1	<------->	Pin	3	RD +
	TD -	pin	2	<------->	Pin	6	RD -
Pair 4		pin	7	<------->	Pin	4	
		pin	8	<------->	Pin	5	

4.6.5 Auto MDX/MDI-X

The complete range of Westermo OnTime Switches automatically detects the transmit and receive copper pairs used in a patch cable. This eliminates the need to source the two types of patch cable (crossed and straight through) highlighted above and therefore reduces the cost of carrying two types of spares.

4.6.6 Electrical Isolation

The copper (TX) ports incorporate high electrical isolation between the signal lines and the internal electronics. In addition, the switch can also withstand over 500 Amps through the shield for short periods of time (20-30mS) without effecting the operation and communication of the Switch. However, this is not advisable. Fiber optical cables should be used in such environments. Each TX port is isolated to chassis and other ports. Isolation is rated 1500Vrms (1 minute).

4.6.7 Auto-Negotiation

Auto-Negotiation is a protocol that controls the speed and duplex of a copper cable when a connection is established between two Ethernet devices. Auto-Negotiation detects the various modes that exist in the device on the other end of the cable and highlights its own abilities to automatically configure itself. Therefore, it will automatically operate at the highest performance in relation to speed and duplex. This allows simple and automatic connection of devices that support a variety of modes from a variety of manufacturers. The auto-negotiation protocol only functions on copper ports.

As standard the range of Westermo OnTime Switches are shipped with the Auto-Negotiation feature enabled.

4.7 Fiber Optic Port Specification

4.7.1 Fiber Optic Communications

The fiber optic (FX) ports are available with either multi-mode or single mode fiber transceivers. Multi-mode transceivers are available with MTRJ, SC or ST style connectors. Single mode transceivers are only available with LC or SC style connectors.

Available fiber connector types are shown below:

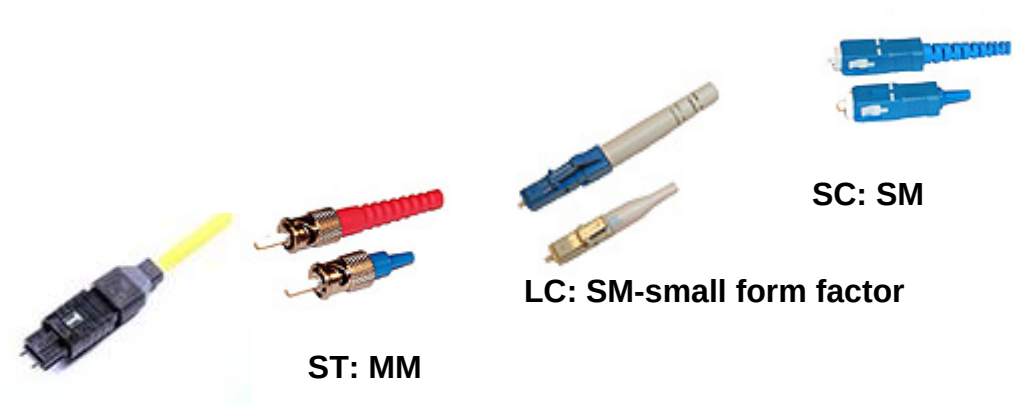


Figure 3, FX connector types

4.7.2 Fiber Optic Parameters

Parameters that have relevance for fiber power budget calculations for relevant fiber transceivers are given below:

Link type	Link dist-ance [km]	Con-nector	Zero cable len.	Output power min.	Output power typical	Rec-eiver sensi-tivity min. [dBm]	Rec-eiver sensi-tivity max. [dBm]	Rec-eiver satura-tion power [dBm]	Link budget min. [dBm]	Center Wave-length [nm]	Aging during lifetime
Multi mode	2	MTRJ	Yes	-19dBm (62,5/ 125µm MMF)	-15,7dBm (62,5/ 125µm MMF)	-31	-34,5	-14 (min)	11	1270-1380	1dBm included in budget
Multi mode	2	MTRJ	Yes	-22,5dBm (50/ 125µm MMF)	-20,3dBm (50/ 125µm MMF)	-31	-34,5	-14 (min)	7,5	1270-1380	1dBm included in budget
Single mode	15	LC	Yes	-15dBm (9µm SMF)	-8dBm (9µm SMF)	-31	-38	-8 (min)	16	1261-1360	included in budget
Single mode	40	LC	No	-5dBm (9µm SMF)	-0dBm (9µm SMF)	-34	-38	-8 (min)	29	1280-1335	included in budget
Single mode	85	LC	No	-5dBm (9µm SMF)	-0dBm (9µm SMF)	-34	TBD	-10 (min)	29	1480-1580	included in budget
Multi mode	2	SC	Yes	-20dBm (62,5/125 µm MMF)	TBD	-31	-35,2	-14 (min)	11	1270-1380	1dBm included in budget
Multi mode	2	ST	Yes	-20dBm (62,5/125 µm MMF)	TBD	-31	-35,2	-14 (min)	11	1270-1380	1dBm included in budget
Single mode	15	MTRJ	Yes	-20dBm (9µm SMF)	TBD	-31	TBD	-8 (min)	11	1261-1360	included in budget

Note: Fiber Ports are always configured for 100 Mbit/s and full duplex.

5 Power Supply Connector

5.1 Redundant power inputs

The switch is designed to operate permanently over a very wide range of power (19 V DC to 60 VDC). Two redundant inputs are provided to provide enhanced redundancy if either supply fails.
The power supply draws power from the input that has the highest potential difference when compared to the alternate supply.

This enables use of e.g. a 48V source as primary supply with a 24VDC battery as back up.

Power supply inputs have reverse polarity protection.

Large transient protection devices are present on both power inputs. During transients, transient currents of up to more than thousand Ampere may pass thru cabling infrastructure.

The switch is delivered with a power connector (Wieland 25.621.3553.0) that is suitable for wires between AWG 20 and AWG 22 (0,34-0,5 mm^2).

Figure 4, Power contact

5.2 Fault Contact

The switch is incorporated with a user configurable fault contact (STAT pin) that enables network and switch faults to be highlighted, see the Installation Guide.

The user configurable fault contact is a solid state component and therefore requires power to control the device. The fault relay is equipped with transient protection.

As standard the fault contact will always highlight the following:

- Internal switch watchdog failure.
- Link / Port 7 Failure (if FRNT 0 is activated)
- Link / Port 8 Failure (if FRNT 0 is activated)
- Power Supply Failure
- Focal Point / Redundancy Mode activated.

Using the Switch configuration software (relevant for switches in the R200 and T200 series), the fault contact can highlight the following addition failures:

- Link / Port 1 to Port 8 Failure; relevant for the R/T200 series.
- A minute pulse that is used for time synchronization can be enabled for switches in the T200 series. This is a special function that disables all other fault indication.

5.3 Power Supply & Fault Contact Connection Diagram

Power supply connection terminals +VinA and +VinB are not interconnected internally within the Switch. -COM terminals on the other hand are internally connected to each other. –COM, +Vin and STAT terminals have an isolation barrier to internal logic and chassis ground that withstand 1500Vrms.

In some cases polarity needs to be reversed or current increased on the fault contact, in such cases an external relay may be used. Dual relays may be used if monitoring of individual power supplies is required. Two example circuit diagrams are presented as a guideline, see Figure 5 and Figure 6.

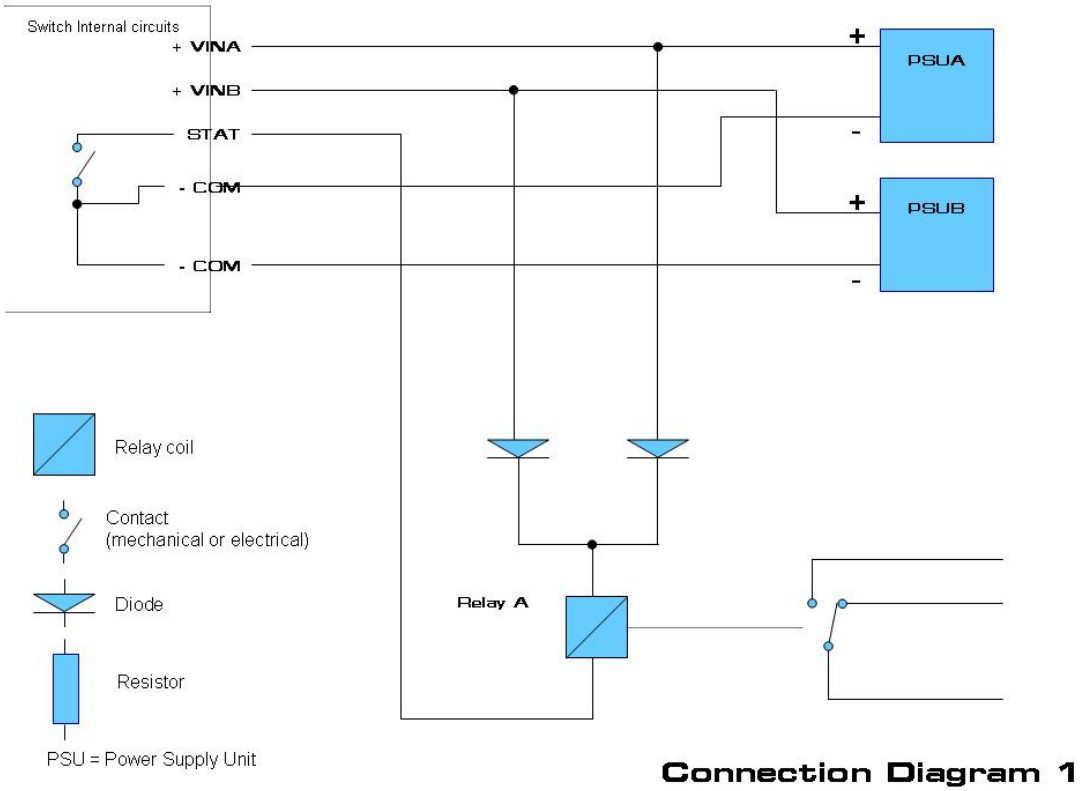


Figure 5, Power and fault contact – connection diagram 1

The diodes can be omitted if only one power supply is used. The diode can be any general purpose diode capable of carrying the current through the relay winding. The function of the circuit is that the current through the relay winding goes from the positive terminal of the power supply via diodes and into the STAT connection. The STAT pin is normally connected to the –COM terminal during normal operation resulting in a magnetised relay in normal mode. The STAT pin will float when an error occurs and the relay will be de-energised.

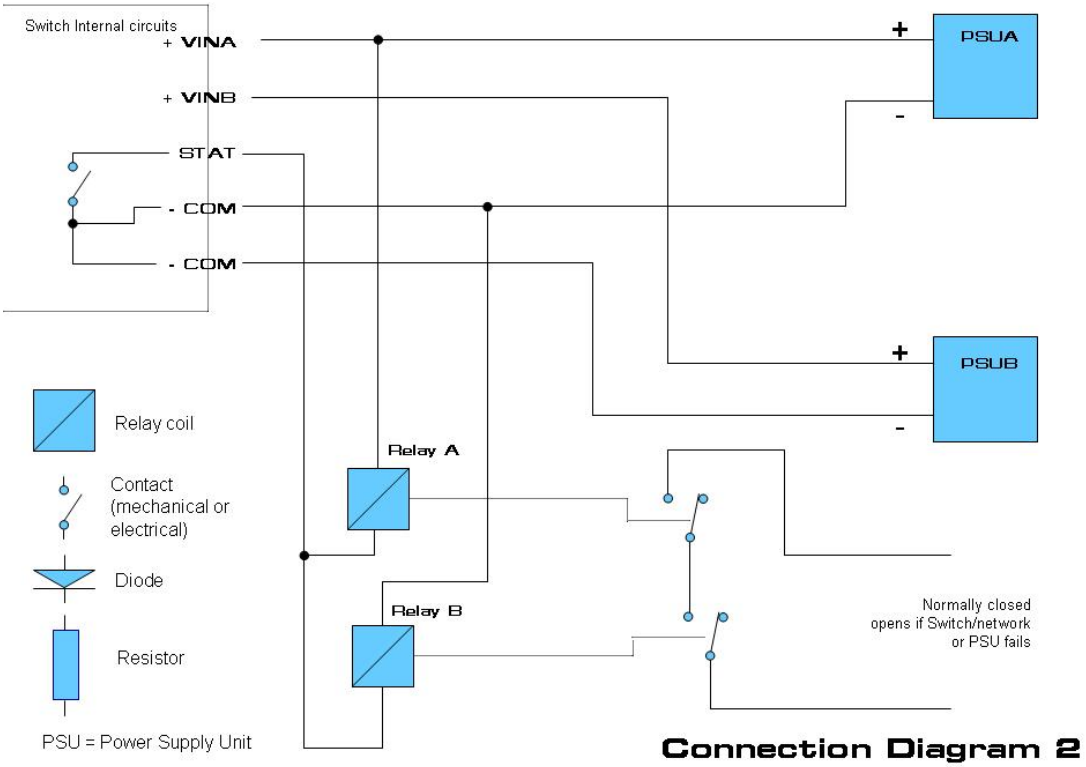


Figure 6, Power and fault contact – connection diagram 2

Example circuit 1, see Figure 5, will not indicate if one of the external power supplies fails, while example circuit 2 will if this is required, see Figure 6. The only difference between the two examples (except that two relays are used) is that each relay is powered from only one of the power supplies. The result of this is that if a power supply is failing the corresponding relay will be de-energised.

Example circuit 3, see Figure 7 shows how to connect the fault contact (status connection) to a PLC. The reason for connecting the fault contact to a local PLC can be that the PLC needs to know the status of the network in order to decide operational mode or to summarize alarms if SNMP and SNMP traps are not used, see chapter 9. Connection of status output of the two PSUs can be done in the same way. The fault contact in the switch is an electronic relay with an internal resistance of approx. 8Ω. When calculating the pullup resistor R the threshold voltage of the digital input on the PLC needs to be taken into account. Also the maximum power dissipated in the resistor R as well as the maximum current thru the fault contact. If +24V supply is used to pullup the resistor (+5V may also be used) as in connection diagram 3, a suitable resistor is 2,2kΩ 0,5W.

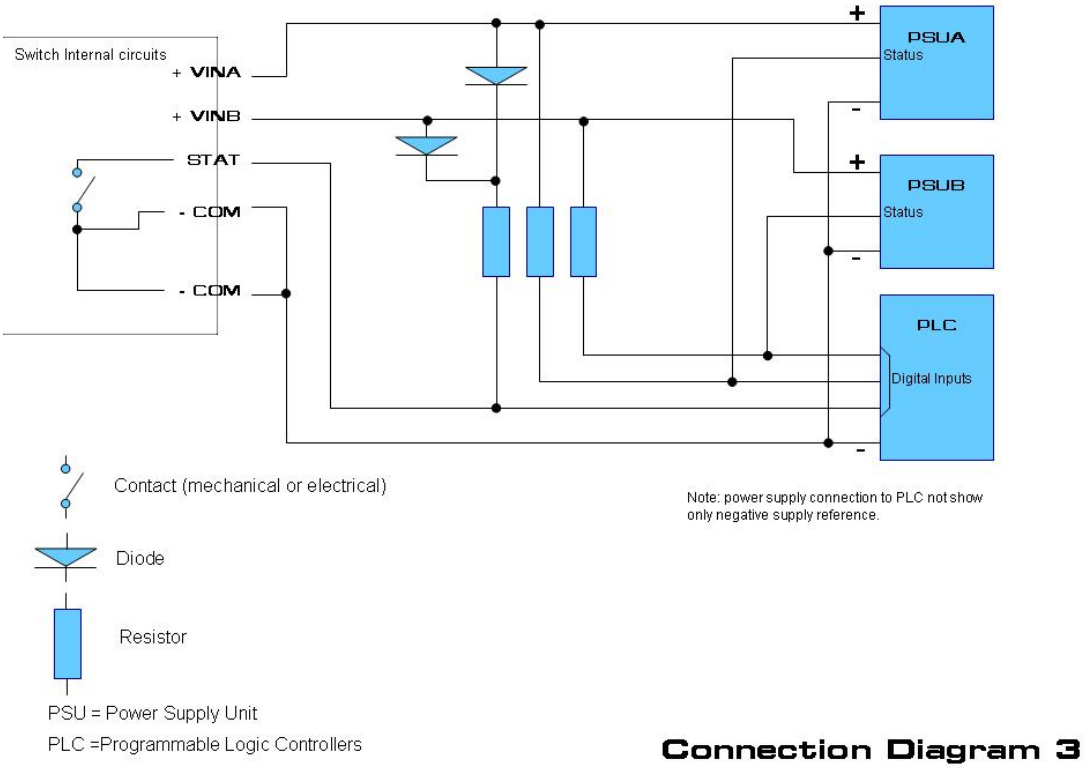


Figure 7, Power and fault contact – connection diagram 3

6 Deterministic Ethernet - QoS

6.1 Principles of Deterministic Ethernet

Westermo OnTime switches can operate in full duplex mode. This ensures that an Ethernet controller will never see any collisions occurring when operated in such a manner. The core section of the Network; the redundant ring topology always runs full duplex and at 100Mbit/s; this cannot be altered.
In addition a very fast switching core is provided to ensure that the switch can handle full wire speed on each port. Finally, a large buffer is available to store packets destined for a busy port. However, it is very unlikely that the buffers are used during normal network operation.
It should be noted that if buffers are used in such a network then it is not viable to state that a network is Deterministic. In practice, the only time such buffers maybe used is in 10M / 100M, half duplex devices. Where such devices are in use, a feature called Head of Line Blocking Prevention is automatically implemented to ensure critical data is received at the destination node, see 6.5 for details.

The switch contains two priority queues. A packet that is identified as a high priority packet is put in the high priority queue. The switch alternates between the two queues by using strict priority. I.e. packets from the low priority queue are only sent if the high priority queue is empty. A packet is identified as a high priority packet based on priority tagging according to IEEE 802.1p (layer 2 priority) or IP Type of Service (ToS -layer 3 priority).

6.2 Layer 2 priority

The IEEE 802.1p and IEEE802.1q standards specify an extra field for the Ethernet MAC header. This field is called Tag Control Info (TCI) field, and is inserted between the source MAC address and the MAC Type/Length field of an Ethernet packet, see figure below.

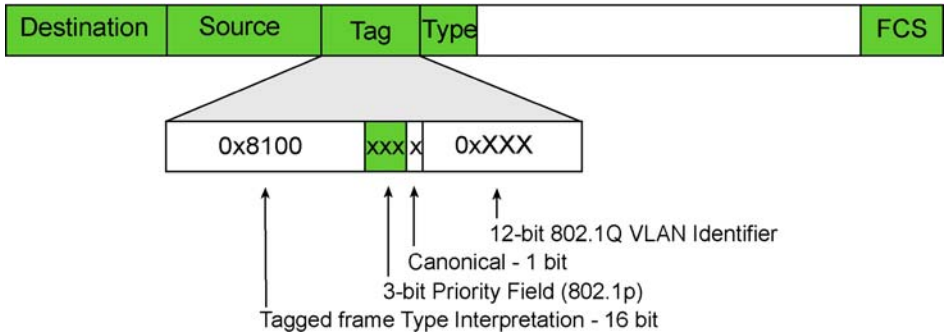


Figure 8, MAC header with tag

This field contains a 3 bit priority field that is used for priority handling. The switch will put a tagged packet with the priority field set to four or higher in the high priority queue, while all other packets will be put in the low priority queue.

6.3 Layer 3 priority

Each IPv4 header contains a ToS field, see figure below. The switch is configured to put IP packets with the following ToS values in the high priority queue:

- 0x04 (IPTOS_RELIABILITY)
- 0x08 (IPTOS_THROUGHPUT)
- 0x10 (IPTOS_LOWDELAY)
- 0xF8
- 0xFC

High priority setting of the IP ToS field of real time critical packets must be set in the IP protocol of the sending station. This can be done on TCP/UDP socket level by a setsockopt( ) command both on the client and server socket side in most Operating Systems (OS). E.g.:

```
tos = 0xFC;
setsockopt( .., IP_TOS, &tos,...)
```

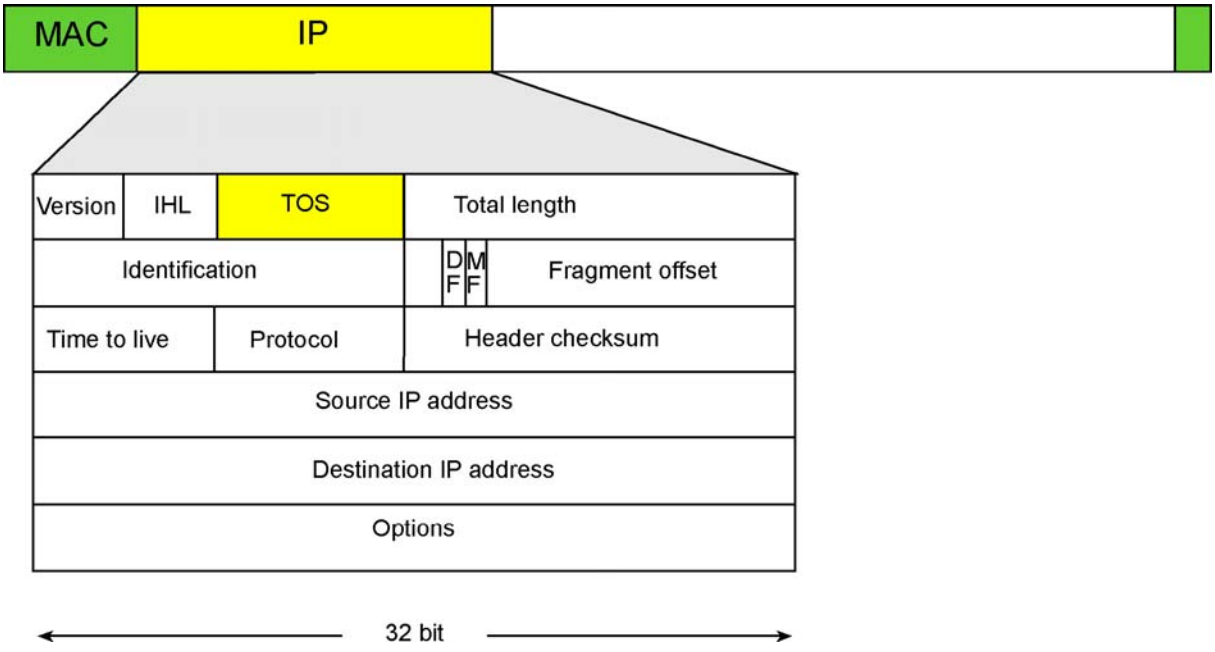


Figure 9, IP header

6.4 Flow control

By default the switch is disabled for flow control (IEEE 803.3x), since flow control is a not a good real time property.

6.5 Head of Line Blocking Prevention

The switch supports head of line blocking prevention for low priority packets only. This means that low priority packets received on any port will not be forwarded to ports that are congested. This will reduce the amount of packets in the output buffer. This function is particular useful when high amounts of multicast, unknown unicast and broadcast traffic are available in large networks where both 10BASE and 100BASE ports are available. High priority packets will always be forwarded.

7 Fast Re-configuration of Network Topology (FRNT)

7.1 Introduction

The Westermo OnTime 200 series is available with redundant ring technology. This eliminates network failure caused by fiber or copper failures on the trunk ports (ring ports). The speed of ring recovery is an essential part of designing your network. The Westermo OnTime ring solution can recover from a failure in only 30mS if such a failure does occur. When used in conjunction with redundant power supplies a very reliable system can be designed.

Standard Ethernet networks would collapse and fail if normal office based Ethernet Switches were formed into a complete ring. This failure is commonly referred to as a 'broadcast storm' as Ethernet Packets have multiple routes on a network to communicate to devices. Usually, an incorrect type of packet broadcasts (or floods) over a network and causes hosts to respond all at once, typically with wrong responses. This starts the process over and over again; hence your network crashes.

7.2 FRNT version 0

7.2.1 FRNT version 0 principles

The FRNT version 0 protocol is similar to the IEEE Spanning Tree Protocol (STP) except for the following:

Each switch in a ring topology has knowledge of the network topology, see figure below. I.e. not only 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 focal point switch will, based on the received topology change event packet, generate a topology change command. This packet is sent to each member switch in the ring. The time it takes from the occurrence of a topology change until the corresponding topology change event packet is received on the focal point is typical a fraction of millisecond (ms) or a few milliseconds (ms) at the most, even though there is 50 switches on the path between the topology change detecting switch and the focal point and the network load on the links are high (e.g. 50 % of full wire speed). Thus, the switch latency in the no load scenario is 15 microseconds (µs), while a conservative estimate in case of 50 % load is 70 microseconds (µs). The most time consuming part in case of a topology change is MAC table update procedure. The MAC tables on each switch must be updated in case of a topology change. This operation takes approx. 20 milliseconds (ms) and is **independent** on the number of switches in the ring.

Note:
Similar proprietary network redundant protocols are often based on polling instead of event controlled handling of a topology change. This will introduce a slower establishment of a new topology. Another aspect is link re-training. A proprietary network redundant protocols that are based on link re-training will suffer from a delay of 300 milliseconds (mS) or more.

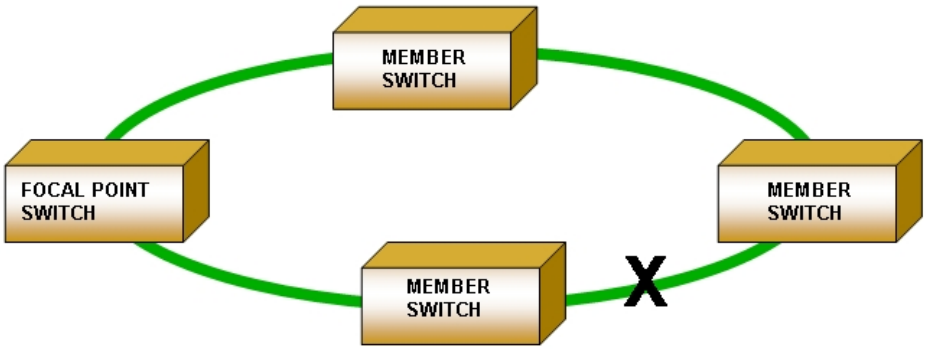


Figure 10, FRNT version 0, single ring topology

7.2.2 FRNT version 0, configuration rules

The 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)

7.3 FRNT version 1

7.3.1 FRNT version 1 principles

The Fast Re-configuration of Network Topology (FRNT) protocol version 1 is used together with FRNT version 0 rings, when redundancy between FRNT version 0 rings also is required, see figure below.

Two FRNT version 0 rings are linked together via a primary and a backup link, where these two links are originating from two different switches in the same FRNT version 0 ring. These two switches are both enabled for FRNT version 1 operation. The two links are connected to two different switches in the second FRNT version 0 ring. These two switches in the second ring are NOT enabled for FRNT version 1 operation.

Link health packets are sent on both primary and the backup link in order to verify that the links are ok or not. The primary link is default in packet forwarding state and the backup link is default in packet blocking state (only link health packets get through). The backup link will be put in packet forwarding state if the backup link is ok and the:

- primary link is not ok, or
- there is no communication between the primary switch and backup switch

The communication media between the two FRNT version 0 rings may not be under direct control of the switches at either end. Thus any type of commutation technologies can be used on the primary and a backup links.

Failure of the either the primary or the backup links will cause the primary or backup switch to raise an alarm via SNMP, activate the fault contact and start switch LED blinking.

A FRNT version 1 topology change (link loss or link establishment on the primary and a backup link) will also trig a MAC table on some or all switches in the FRNT 0 rings. The re-configuration time in case of is FRNT version 1 topology change is comparable to the FRNT version 0 re-configuration time.

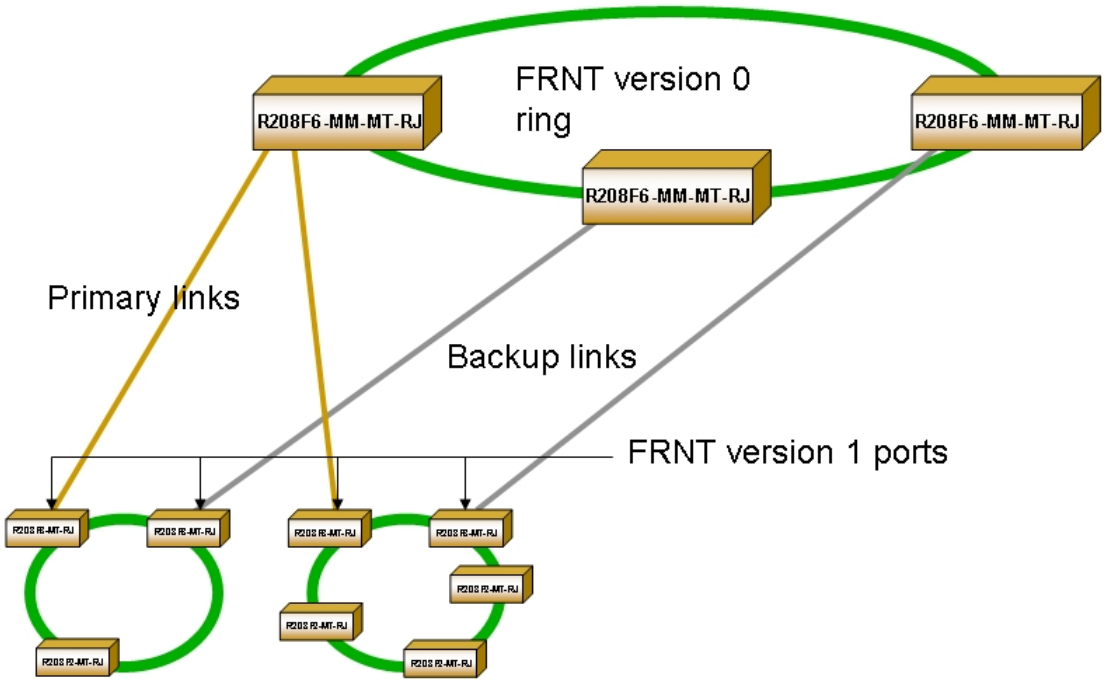


Figure 11, FRNT version 1, multiple ring topology

7.3.2 FRNT version 1, configuration rules

The rules are as follows:

- Only two switches in a FRNT version 0 ring can be configured for FRNT version 1, one as primary
- Only one port can be enabled for FRNT version 1

7.3.3 FRNT trouble shooting

Check cabling, port 8 must be connected to port 7 on the next switch.
Only one FRNT v0 focal point switch is allowed in a ring.
Setting FRNT parameters require restart of the switch.

8 Rapid Spanning Tree Protocol (RSTP)

The R/T200 switch series supports the Rapid Spanning Tree Protocol (RSTP) according to IEEE802.1w with fall-back to the Spanning Tree Protocol (STP - IEEE802.1D). The STP fallback feature means that the R/T200 switches can be used together with switches that only have support for STP.

RSTP/STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages with broadcast storm and an unstable network as result.
The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root (focal point) of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root - a forwarding port elected for the spanning-tree topology
- Designated - a forwarding port elected for every switched LAN segment
- Alternate - a blocked port providing an alternate path to the root port in the spanning tree

Switches that have ports with these assigned roles are called root or designated switches.
Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames, but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment. When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings determine which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

The stable, active spanning-tree topology of a switched network is determined by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch
- The spanning-tree path cost to the root switch
- The port identifier (port priority and MAC address) associated with each port

When the switches in a network are powered up, each switch functions as if is the root switch. Each switch sends a configuration BPDU through all of its ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age

- The identifier of the sending port
- Values for the hello, forward-delay, and max-age protocol timers

When a switch receives a configuration BPDU that contains *superior* information (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the switch, the switch also forwards it with an updated message to all attached LANs for which it is the designated switch.
If a switch receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.
A BPDU exchange results in these actions:

- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network).
- For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (0x8000), the switch with the lowest MAC address in the VLAN becomes the root switch.
- A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch.
- The shortest distance to the root switch is calculated for each switch based on the path cost.
- A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.
- Ports included in the spanning-tree instance are selected. Root ports and designated ports are put in the forwarding state.
- All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode.

The user can easily set the root of the network by configuring one of the switches in the network as the RSTP focal point (see Installation manual). This will result in a lower priority value for this switch than for the other switches in the network.

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a port transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.
Each port on a switch using spanning tree exists in one of these states:

- Blocking - the port does not participate in frame forwarding.
- Listening - the first transitional state after the blocking state when the spanning tree determines that the port should participate in frame forwarding.
- Learning - the port prepares to participate in frame forwarding.
- Forwarding – the port forwards frames.
- Disabled – the port is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

A port moves through these states:

- From initialization to blocking

- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

The typical time it takes to enter forwarding state from blocking state or vica versa (i.e. the network re-configuration time) in case of a RSTP enabled network is approx. XXX seconds, while the re-configuration time in case of a STP based network network is approx. 40 seconds.

9 Simple Network Management Protocol (SNMP)

The Westermo OnTime R/T200 switch supports Simple Network Management Protocol version 2c (SNMPv2c).

SNMP is an Internet standard protocol (IP) developed to manage IP nodes (servers, workstations, routers, switches and hubs etc.) on an Ethernet network. SNMP enables network administrators and controls engineers to manage network performance, find and solve network problems, and plan for network growth.

Devices or Ethernet Switches that support SNMP are usually referred to as Managed Switches. There are currently three different versions of SNMP available; SNMPv1, SNMPv2 and SNMPv3. Any node on a network that must is managed incorporates an agent module that is responsible for the following:

- Collecting and maintaining information about the local environment and network.
- Providing that information to a SNMP Master, either responding to a request or in an unsolicited fashion, or, when an event the managed device has been configured to monitor occurs.
- Responding to manager commands to alter the local configuration or operating parameters.

Each agent on the network maintains a unique Management Information Base (MIB) that is specific to the SNMP agent. This is the case with the Westermo OnTime Switches. SNMP is based on a standard that covers all type of devices. Some of the information is common regardless of Switch manufacturer (Port Health , Port Status etc) while other information is specific to the Switch Manufacturer (Switch temperature, No. of Satellites available etc).

The R/T200 MIB is divided into groups allowing the SNMP manager to poll the SNMP agents for information. The following MIB groups are implemented and can be found on www.ontimenet.com/upgrade.htm

- MIB-2 System Group, RFC1213-MIB, OID: 1.3.6.1.2.1.1. Contains generic configuration information such as system description (switch type, software version), location, hostname, etc on the switch CPU.
- MIB-2 Interface Group, RFC1213-MIB, OID: 1.3.6.1.2.1.2. Contains generic information on the entities at the interface layer. This means port speed, switch MAC address, and packets statistics (number of packets sent and received, number of unicast and multicast, packet sizes, over- and undersized packets, CRC errors, collisions, etc) per port on the switch.
- MIB-2 Internet Protocol Group (IP), RFC1213-MIB, OID: 1.3.6.1.2.1.4. Contains information used to keep track of the IP layer on the switch CPU.
- MIB-2 Internet Control Message Protocol Group (ICMP), RFC1213-MIB, OID: 1.3.6.1.2.1.5. Contains 26 counters, counting how many times this message type was generated by the local IP entity and how many times this message type was received

by the local IP entity. It also counts the total number of ICMP messages received, sent, received in error, or not sent due to error on the switch CPU.

- MIB-2 Transmission Control Protocol Group (TCP) , RFC1213-MIB, OID: 1.3.6.1.2.1.6. Contains information used to keep track of the application entities using TCP on the switch CPU.

- MIB-2 User Datagram Protocol Group (UDP), RFC1213-MIB, OID: 1.3.6.1.2.1.7. Contains information used to keep track of the application entities using UDP on the switch CPU.

- MIB-2 SNMP Group, RFC1213-MIB, OID: 1.3.6.1.2.1.11. Contains information used to keep track of SNMP application entities. It provides statistical information about the SNMP protocol entity and tracks the amount of management traffic that the switch CPU responds to.

- BRIDGE-MIB dot1dBridge dot1dStp Group, RFC1493, OID: 1.3.6.1.2.1.17.2. This MIB holds Spanning Tree Protocol information on per port basis.

- ifMIB ifMIBObjects ifxTable Group, RFC2863, OID: 1.3.6.1.2.1.31.1.1. Contains network load on per port basis and represents an extension to the MIB2-Interface group.

- ifMIB ifRcvAddressTable Group, RFC2863, OID: 1.3.6.1.2.1.31.1.4. Contains network MAC table on the switch CPU.

Originally, SNMP was designed for networks designed using Hubs. Network bandwidth allocated for SNMP had to be kept to a minimum and hence the Simple Network Management Protocol was designed to be simple. Therefore, an SNMP manager can carry out the following simple commands:

- Query SNMP agents

- Get responses from agents

- Set variables in agents

- Acknowledge asynchronous events from agents

-

9.1 Westermo OnTime private MIB Information

The Westermo OnTime Management Information Base (MIB) is a collection of variables or data that determines the properties of the managed device. The MIB is unique to the Westermo OnTime device and has therefore been compiled to take this into account.

There are various tools available that enable the MIB data to be displayed in a software package or via OPC so that the MIB information can be displayed onto a SCADA.

The Westermo OnTime MIB is available on the documentation / software CD that is included with every Westermo OnTime Switch
The Westermo OnTime private MIB contains the following:

- General
- FRNT 0 status
- Status information
- Time synchronization configuration parameters and status information
- Multicast configuration
- Temperature alarm configuration
- SNMP host addresses

The Westermo OnTime private MIB is available for download from OnTime web page: http://www.ontimenet.com/upgrade.htm

9.2 SNMP Traps

One feature of SNMP is that the SNMP agent (in this case an Westermo OnTime switch) can send SNMP traps to one or more SNMP Hosts. SNMP traps means system alarms such as a port link loss or a port enabled for port alarms or the switch temperature exceeding a predefined threshold.

10 IGMP snooping

10.1 IP Multicast filtering

Several applications are based on multicast communication. Data is only sent once even though the data is meant for more than one receiver. However, the multicast packets will be sent on every drop link in the network unless the Ethernet switches support multicast filtering. The R/T200 series support IP multicast filtering. This means that IP multicast "join" and "leave" requests will be trapped by the switches, and the multicast filters will be set based on which drop links where these requests are received.

10.2 Routerless operation

IGMP "Join" and "leave" request are forwarded to one or more IGMP servers (routers) present in the network. This is one of the main properties of IGMP. The Westermo OnTime IGMP snooping implementation does not depend on the availability of an IGMP Querier (IGMP server) in the network. This is important from robustness or a performance point of view. Thus, the multicast filtering feature will work even though the network connection to a standalone IGMP Querier is lost or not, and the drop link to such standalone IGMP Querier will not become a bandwidth bottleneck in the network, because the switch can also act as an IGMP Querier. The IGMP Querier operation of the switch is controlled by the “Auto mode” and “Querier” parameters. The following combinations of these two parameters are possible:

- “Auto mode” enabled + Querier enabled: the switch is able to act as an IGMP Querier (IGMP server) and the IGMP Querier in the network is selected automatically. The switch (with Querier support) in the network with the lowest IP address will be chosen as the network Querier (i.e. IGMP focal point). Only one Querier will exist in the network if all IGMP enabled switches and routers in the network have this configuration. This is the default IGMP settings.
- “Auto mode” enabled + Querier disabled: same operation as above, but the switch cannot act as an IGMP Querier.
- “Auto mode” disabled + Querier enabled: the switch will always act as an IGMP Querier. Each switch/router will act as IGMP Querier if this configuration is used on each switch/router in the network.

A switch with “Auto mode” enabled, which is not acting as the IGMP Querier, will forward IGMP Queries received from the IGMP Querier on all ports except the port where the IGMP Queries are received. The port where IGMP Queries are received is referred to as the “Router port”. This port is part of every active multicast filter. The use of “Router port” is not relevant in case “Auto mode” is disabled since the switch in this mode always is acting as a Querier (IGMP focal point). A switch in this mode will not forward IGMP queries received. IGMP Measurement reports for each active multicast filter on the switch will be sent back for each IGMP Query received. This is valid for both “Auto mode” being enabled and disabled.
The interval between two IGMP query packets can also be set in the IP configuration tool. Four intervals are possible: [12, 30, 70, 150] seconds.
The IGMP snooping implementation will also forward IGMP information (join, leave, measurements reports) on the switch trunk ports. A trunk ports is automatically detected in case a network redundancy protocol such as if FRNT or STP are running, but the user may also configure manually ports as trunk ports. Manually trunk port configuration might be

relevant in case no network redundancy protocol is running on a port connected to another IGMP snooping enabled switch. This feature is required in case the multicast producers (i.e. Ethernet end nodes sending IP multicast packets) make no IGMP join or IGMP measurements reports according to IGMP v2. IP multicast producers are not required to make an IGMP join during start up or answer with IGMP measurement reports on received IGMP query packets (ref. RFC 2236).

10.3 Stop filter option

A stop filter will be set if a multicast packet is received prior to a "join" to an IP multicast group where the received multicast address belong if the "Multicast stop filter" option is enabled. This means that IP multicasting based on IGMP is required in order to get multicast through the network. Multicast filters will be properly set only for IP multicast packets if this option is disabled. That means that multicast packets not based on IP will be forwarded in the same way as broadcast packets. This is acceptable if the non IP based multicast network load is reasonable low.

10.4 FRNT integration

The IP multicast filter implementation is integrated with the Fast Re-configuration of Network Topology (FRNT) protocol. This means that the multicast filters will be updated as fast the FRNT implementation handles a topology change, i.e. approx. 30 ms.

11 VLAN

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). 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.

Figure 12 shows the VLAN dialog setup of the IP configuration tool.

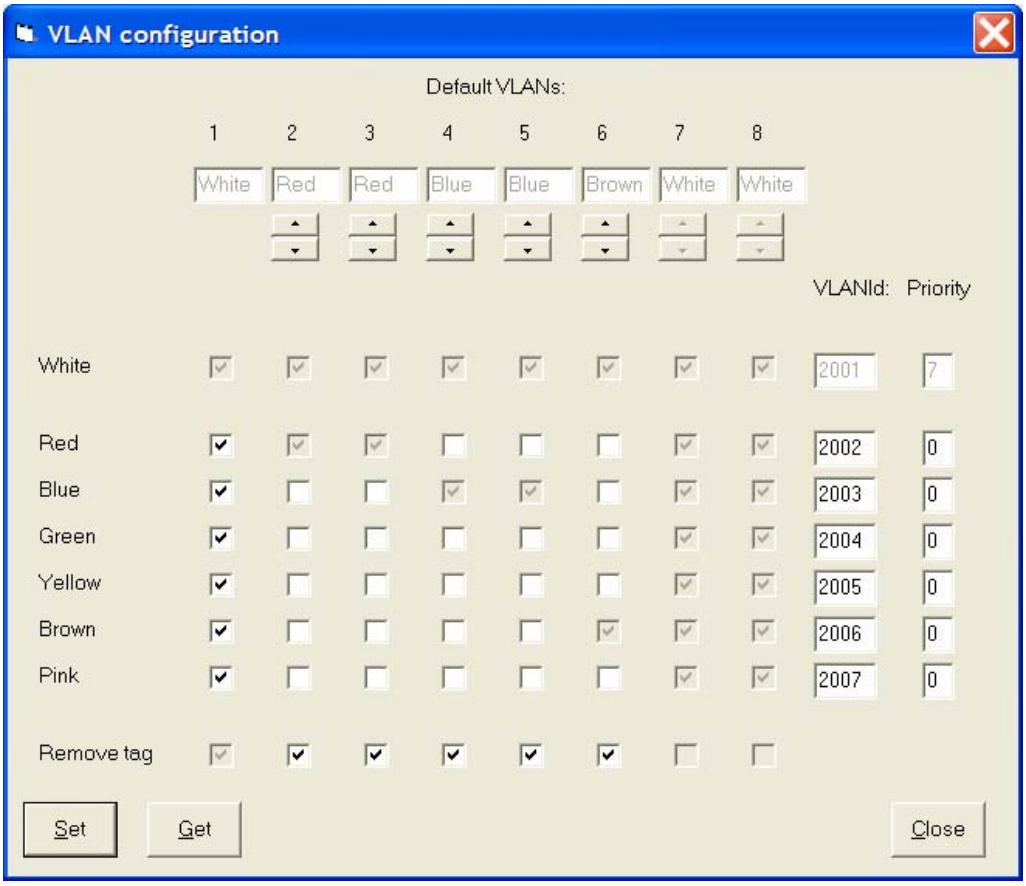


Figure 12, VLAN setup dialog

The VLAN implementation is meant for both Ethernet end nodes that support tagging and for those that do not. An Ethernet end node that are 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 VLANs 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 CPUs. Thus, the switch CPUs 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 CPUs. 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 ..3: low priority
- Priority 4 ..7: high priority

This priority will be added to the tag. See Figure 8 for the MAC header with 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 configuration 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.

The figure below shows an example of a VLAN setup with three VLANs (red, blue and green VLAN) in a network with ring topology.

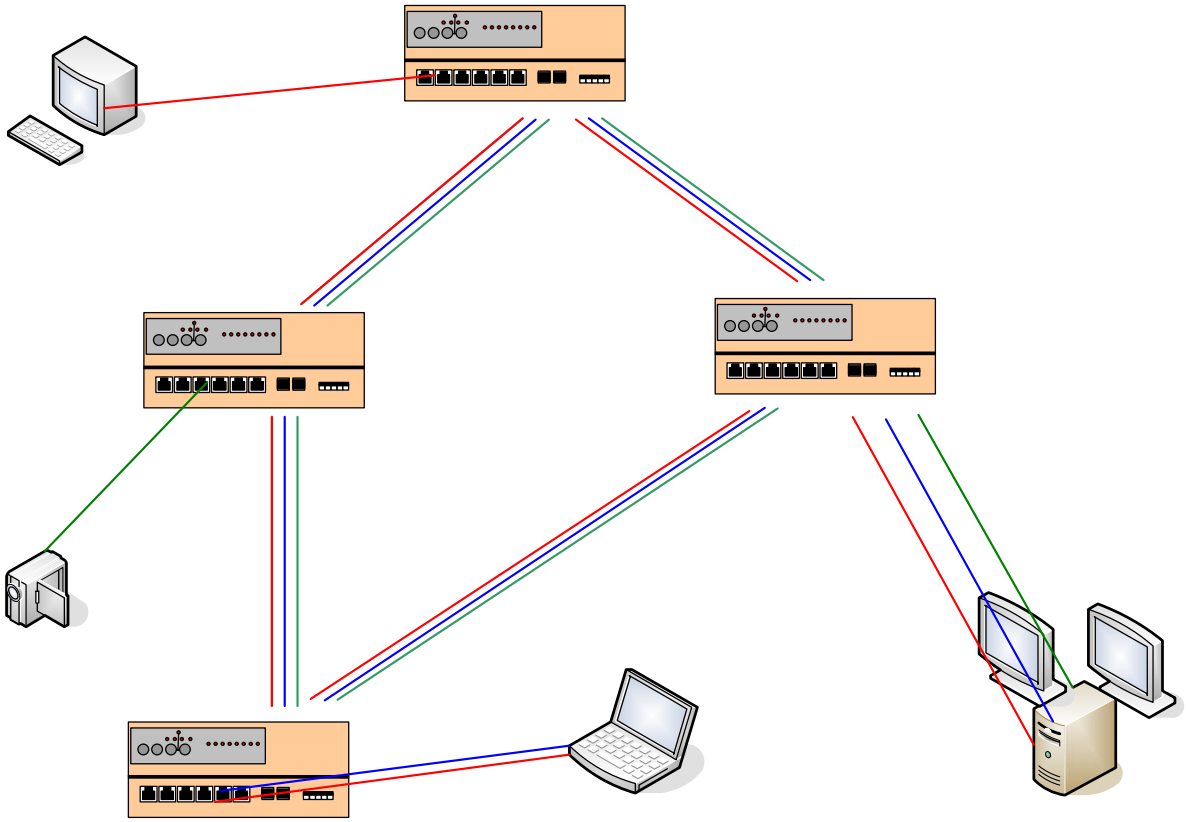


Figure 13, VLAN example

12 Security

12.1 MAC security

12.1.1 MAC learning

CPU based MAC learning is used instead of switch core MAC learning when VLAN is enabled. This means that the CPU will maintain both the MAC and the VLAN tables of the switch. A packet with a new source MAC address and VLAN id combination received on a given port will not be learned and packets with this source MAC address and VLAN id combination will not be forwarded if this combination is illegal. Note: the VLAN id will be equal to the default VLAN for the port where the packets was received if the packet is untagged or the VLAN id of the tag is zero, see chapter 11 for details. This means that FRNT attacks on non-trunk ports is not possible making FRNT immune for any FRNT attacks (i.e. false FRNT packets).

12.1.2 MAC Attack Prevention

The switch will start to flood unicast packets when the number of learned MAC addresses on a switch exceeds the MAC table size of the switch. This unicast flooding can be utilized by a non-authorized user. Programs for frequent generation of new MAC source addresses exist and are used by hackers in order to perform such MAC attacks.

MAC attack prevention is implemented on the R/T200 switches. MAC attack prevention means that new MAC addresses on a given port will not be learned if the number of the MAC addresses learned on the port exceeds a pre-defined threshold. The threshold for a trunk port is much higher than for a non-trunk port. This MAC attack prevention implementation will guarantee that the number of learned MAC addresses never exceeds the MAC table size (8192 entries) of a R/T200 switch.

12.2 Broadcast storm prevention

Avoiding unwanted loops that will introduce broadcast storm is required for ports that are not enabled for FRNT or STP[1]. The R/T200 switches support broadcast storm prevention. Both ports will be put in standby state if this situation occurs.

[1] All ports are enabled for RSTP/STP in case RSTP/STP is enabled on a switch, while FRNT can only be enabled on two ports (FRNT v0) or three ports (FRNT v0 and v1).

13 Time synchronization

Variable latencies through the protocol stacks and the Ethernet switches will degrade the timing accuracy that can be achieved when time synchronization is performed via a switched Ethernet infrastructure. Time stamping of incoming and outgoing time packets shall preferably be done as low as possible in the protocol stack. The Ethernet switch latency depends on the network load and the switch architecture. This problem is solved by integrating state of the art time synchronization properties on the T200 switches from Westermo OnTime. The main building blocks of the Westermo OnTime time server (SNTP/NTP)/Boundary clock (IEEE1588) implementation (T200) is shown below:

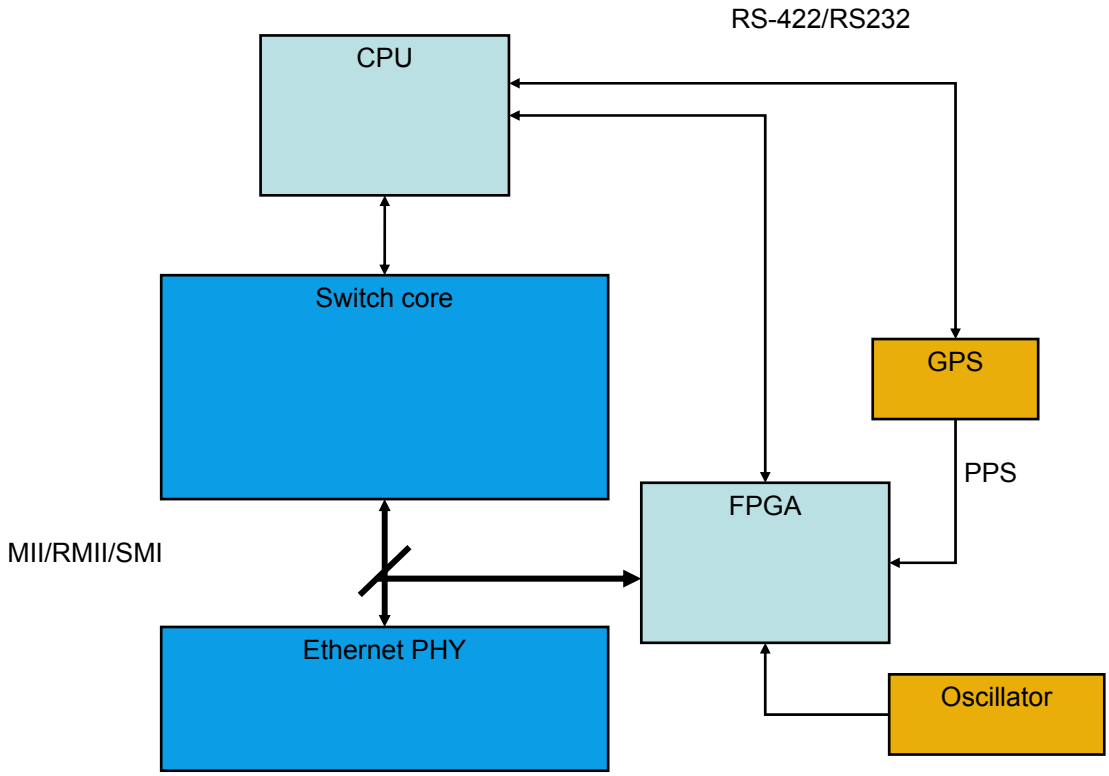


Figure 14, T200 building blocks

Incoming and outgoing time packets are time stamped in hardware at the Media Independent Interface (MII) between the switch core and the Ethernet PHY. An incoming time packet is time stamped before it is forwarded through the Ethernet switch core and an outgoing time packet is time stamped after the packet has been sent through the switch core. This means that variable latency through the switch core has no impact on the time synchronization accuracy. Thus, the T200 is **network load independent**. The time stamping is performed in an FPGA (Field Programmable Gate Array). The FPGA also generates the local clock of the Boundary clock implementation based on either an external Pulse Per Second (PPS) input

from e.g. a GPS receiver, or only based on a local oscillator (e.g. the switch core oscillator). The drift and offset of the local oscillator is adjusted based on the PPS signal in case an external time base is used.
The CPU handles the time sync protocol, T200 configuration via e.g. SNMP, serial interface versus an external clock source (if this available) and the interface versus the FPGA. The NMEA protocol over RS232 or RS-422 versus an external GPS is often relevant in order to have reference to absolute time. RS-422 is the preferred interface for both serial data and the PPS signal in order to meet various installation requirements (distance between GPS receiver and Boundary clock).

NMEA 0183 is an interface protocol created by the National Marine Electronics Association. NMEA is a simple, yet comprehensive ASCII protocol which defines both the communication interface and the data format. For those applications requiring output only from the GPS receiver, NMEA is in most cases the preferred choice. The GGA and ZDA are the two NMEA reports used by the T200. The format of these two reports is as follows:

$GPGGA,<UTC time>,<Latitude>,<N/S>,<Longitude>,<E/W>,<GPS quality>,
<Nr of satellites>,<Horizontal precision>,<Antenna height>,
M,<Geoidal height>,M,<Diff. GPS data age>,<Diff. ref. station ID><CR>,<LF>

UTC time	hhmmss format
Latitude	ddmm.mmmmm format
Latitude N/S	Latitude hemisphere North or South
Longitude	dddmm.mmmmm format
Longitude E/W	Longitude hemisphere East or West
GPS quality	0=fix not available, 1=Non-diff GPS available, 2=diff. GPS fix available
Nr of satellites in use	00 to 12 satellites
Horizontal dilution precision	0.5 to 99.5
Antenna height above/below mean	-9999.9 to 99999.9 meters
Geoidal height	-999.9 to 9999.9 meters
Diff. GPS data age	nr of seconds since last valid RTCM transmission
Diff. ref. station ID	0000 to 1023.

GPZDA - Time and Date

$GPZDA,<hhmmss.s>,dd,mm,yyyy,,*hh<CR>,<LF>

UTC	hhmmss.s
Day	dd (01 to 31)
Month	mm (01 to 12)
Year	yyyy
Unused	-
Unused	-

The most relevant time synchronization protocols are based on SNTP/NTP (RFC2030/RFC1305) or P1588 (IEEE Std 1588™-2002). These protocols are all based on UDP/IP.

Timing accuracies in the order of one millisecond (ms) can be achieved on a time client by using the built-in SNTP client software available on newer versions of Windows or other operating systems when time updates are performed versus the T200 time server. 5-25 microseconds (µs) timing accuracies is possible by performing time stamping of incoming an outgoing time packets on the client interrupt service routine. 1 µs accuracy or better can be achieved if time stamping on the client is performed in hardware. Westermo OnTime networks provide intellectual property as part of design in projects together with customers that need highest possible accuracy. Such an implementation is shown below. This is the preferred configuration.

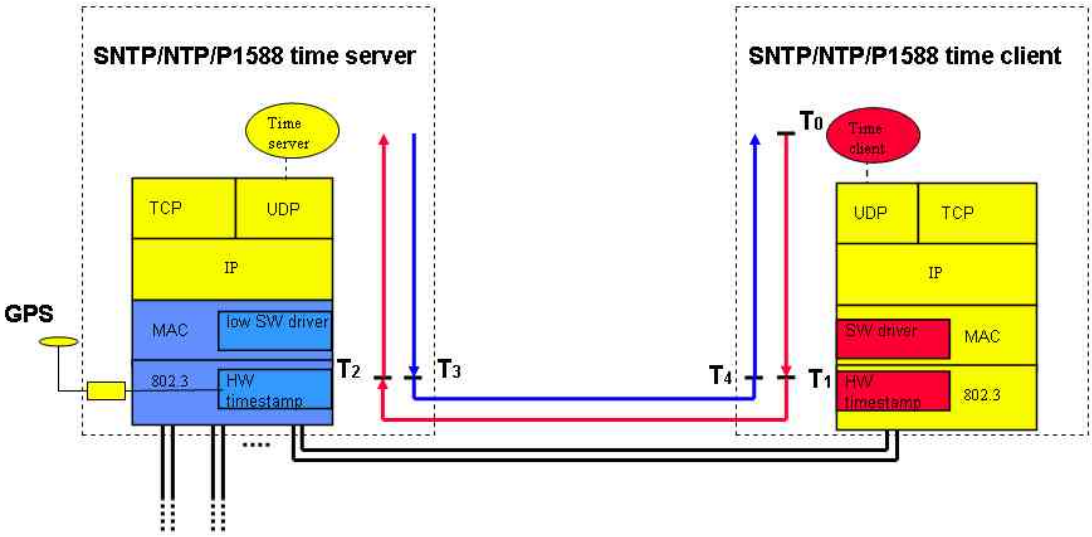


Figure 15, OSI model of time server and time client

13.1 IEEE 1588 Grandmaster

The IEEE 1588 Grandmaster will periodically send SYNC and FOLLOW_UP multicast packets with an interval of two seconds, when the switch is enabled for IEEE 1588 Grandmaster functionality. The SYNC packet contains no accurate time stamp in the fraction part of the SYNC transmit time stamp, *originTimestamp* (nanoseconds), while the corresponding FOLLOW_UP packet contains this time stamp of the SYNC packet in its *preciseOriginTimestamp* (nanoseconds), i.e. the T3 time stamp (see figure above). The sequenceId of the SYNC packet and the *associatedSequenceId* parameter of the FOLLOW_UP packet are used for pairing the SYNC and the corresponding FOLLOW_UP packet at the IEEE 1588 Slave implementation connected to the T200. The IEEE 1588 SYNC and FOLLOW_UP packet contents are shown in the figures below. These figures are taken from the TSCapture tool from Westermo OnTime Networks. The IEEE 1588 Grandmaster will also respond with a DELAY_RESP packet when a DELAY_REQ packet is received from an IEEE 1588 Slave. The *requestingSourceSequenceId* parameter of the DELAY_RESP packet and the *sequenceId* parameter of the DELAY_REQ packet is used for pairing the two packets. The *delayReceiptTimestampSec* and *delayReceiptTimestampFrac* parameters of

the DELAY_RESP packet contains the receive time stamp of the DELAY_REQ packet , i.e. the T2 time stamp (see figure above).

An example of an IEEE1588 SYNC packet is shown in Figure 16. This presentation is taken from the TSCapture network capture tool from Westermo OnTime Networks, contact Westermo OnTime for more details regarding the TSCapture tool.

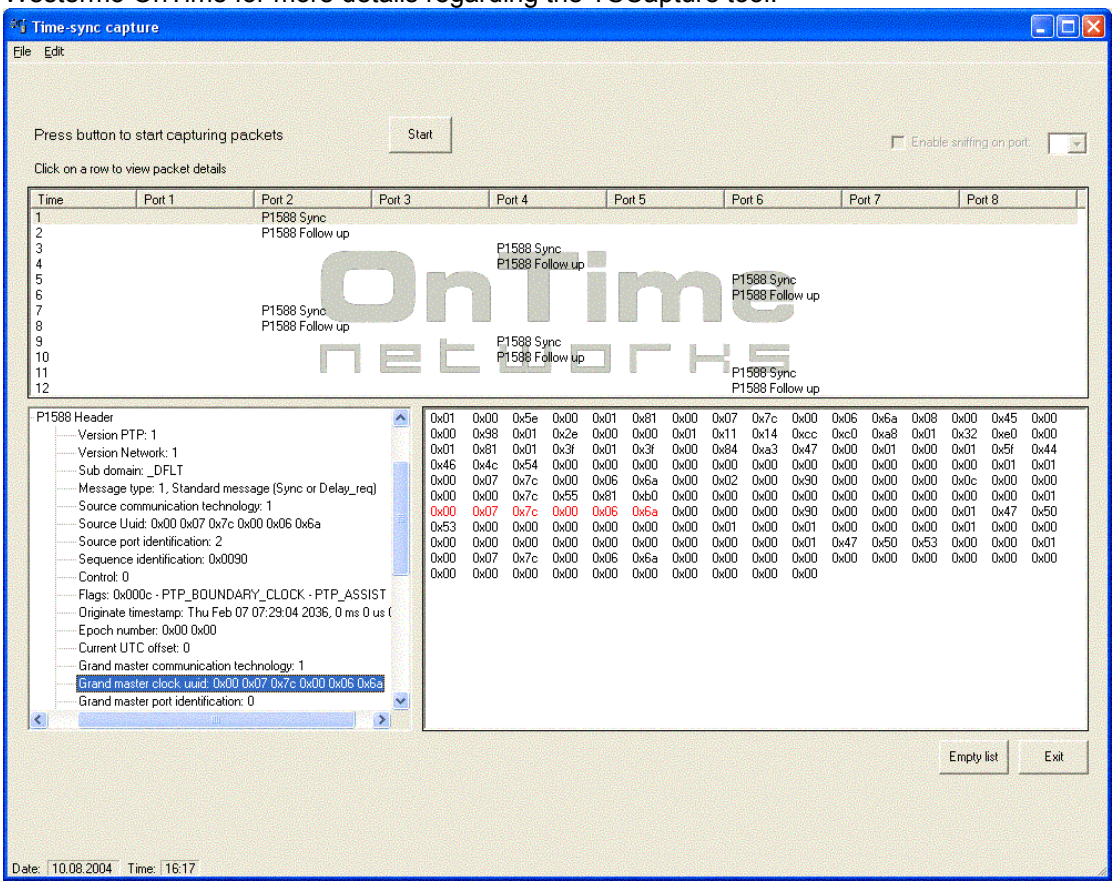


Figure 16, IEEE1588 SYNC packet

13.2 IEEE1588 Transparency

One of the main properties of the IEEE1588 standard is related to the handling of variable network latency between the Grand Master clock and the Slave clocks. Thus, the network load dependable latency through off-the-shelf Ethernet switches without any time sync support will depredate the time sync accuracy that can be achieved on the IEEE1588 Slaves. This degradation is proportional with the number of off-the-shelf switches between the IEEE 1588 Grand Master and the IEEE 1588 Slave.

This problem is solved if T200 switches with IEEE 1588 Transparency are used on all network paths between the Grand Masters and Slaves in the network.

The IEEE 1588 Transparency principles are as follows:

SYNC and FOLLOW_UP packets are sent from the Master to the Slaves. Both packets are sent to the CPU of the Ethernet switch with transparency support before the packets are forwarded on all ports except the port where the two packets were received. A receive time stamp is generated on PHY level when the SYNC packet was received, and transmit time stamps are generated on PHY level for each output port where the SYNC packets are forwarded. The time difference between the transmit time stamps and the receive time stamp, ΔTsync(N-1) (,where N is the number of ports on the Ethernet switch), of the SYNC packet is calculated and stored for each output port. The *sequenceId* of the SYNC packet is also stored and compared with the *assoiciatedSequenceId* of the corresponding FOLLOW_UP packet received on the same input port as the SYNC packet. These two sequence ids must match. The preciseOriginTimestamp of each of the FOLLOW_UP packets that are forwarded on the N-1 output ports are modified with ΔTsync(i) for each output port. The FOLLOW_UP packets are then forwarded on the output ports. See Figure 17 for the handling of the SYNC/FOLLOW_UP packets at the switch with IEEE1588 transparency.

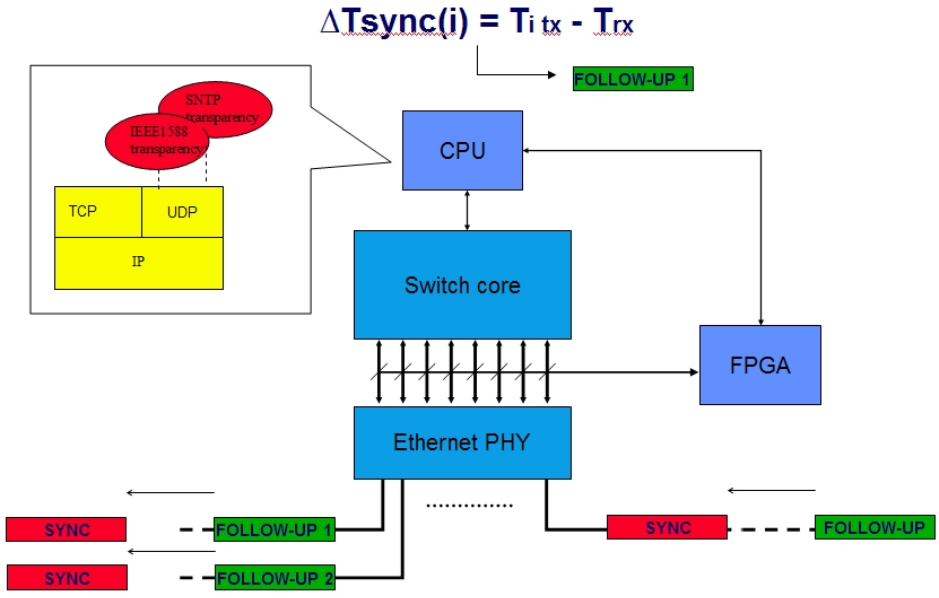


Figure 17, IEEE1588 SYNC/FOLLOW-UP transparency

DEL_REQ packets are sent from the Slave to the Master in order to calculate the propagation delay between Slave and the Master. This means the wire propagation delay in traditional IEEE1588 context. The delay through an Ethernet switch with transparency support will add network load depended switch delay to a DEL_REQ packet (i.e. store-and-forward and queuing delays of the Ethernet switch). This delay must be removed. The delay is measured when the DEL_REQ packet passes the switch and the *delayReceiptTimestamp* parameter of the corresponding DELAY_RESP packet is then modified with this measured delay. The *sequenceId* is used for pairing the DEL_REQ packet the corresponding DEL_RESP packet. See Figure 18 for the handling of the DEL_REQ/DEL_RESP packets at the switch with IEEE1588 transparency.

A switch with IEEE1588 Transparency support maintains a list of ports, where SYNC and FOLLOW-UP packets are received. Any DEL_REQ packets received are only forwarded on these ports.

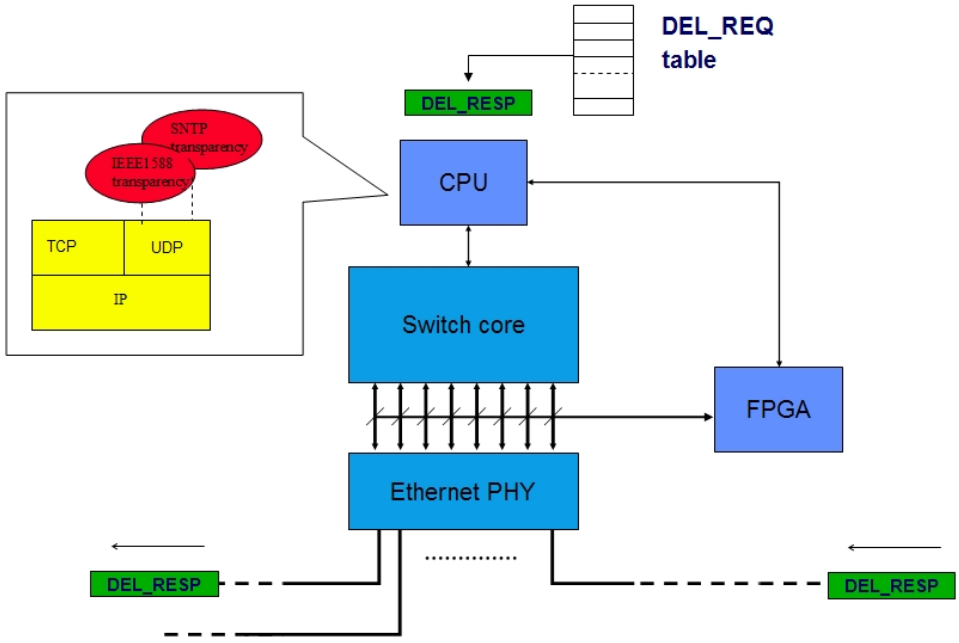


Figure 18, IEEE1588 DEL_REQ/DEL_RESP transparency

A network of switches with IEEE1588 Transparency support can in fact be considered as one big LAN segment as if all the Ethernet switches were Ethernet hubs with the difference that full duplex connectivity and bandwidth scalability of Ethernet switches are maintained.

13.3 SNTP/NTP time server

The SNTP/NTP is based on unicast communication. I.e. the NTP/NTP client sends a SNTP/NTP request, and the T200 SNTP/NTP server sends a corresponding SNTP/NTP reply. The SNTP/NTP replay packet contains both the receive time stamp of the SNTP/NTP request packet and the transmit time stamp of the reply packet. I.e. the T2 and T3 time stamps (see figure above).
Note: the SNTP/NTP T3 accuracy is as good as the corresponding T3 time stamp of IEEE 1588 implementation. This is achieved by using the Westermo OnTime patent for deterministic access of an Ethernet packet to an Ethernet drop link.

An example of an SNTP/NTP request packet is shown in Figure 19. This presentation is taken from the TSCapture network capture tool from Westermo OnTime Networks, contact Westermo OnTime for more details regarding the TSCapture tool.

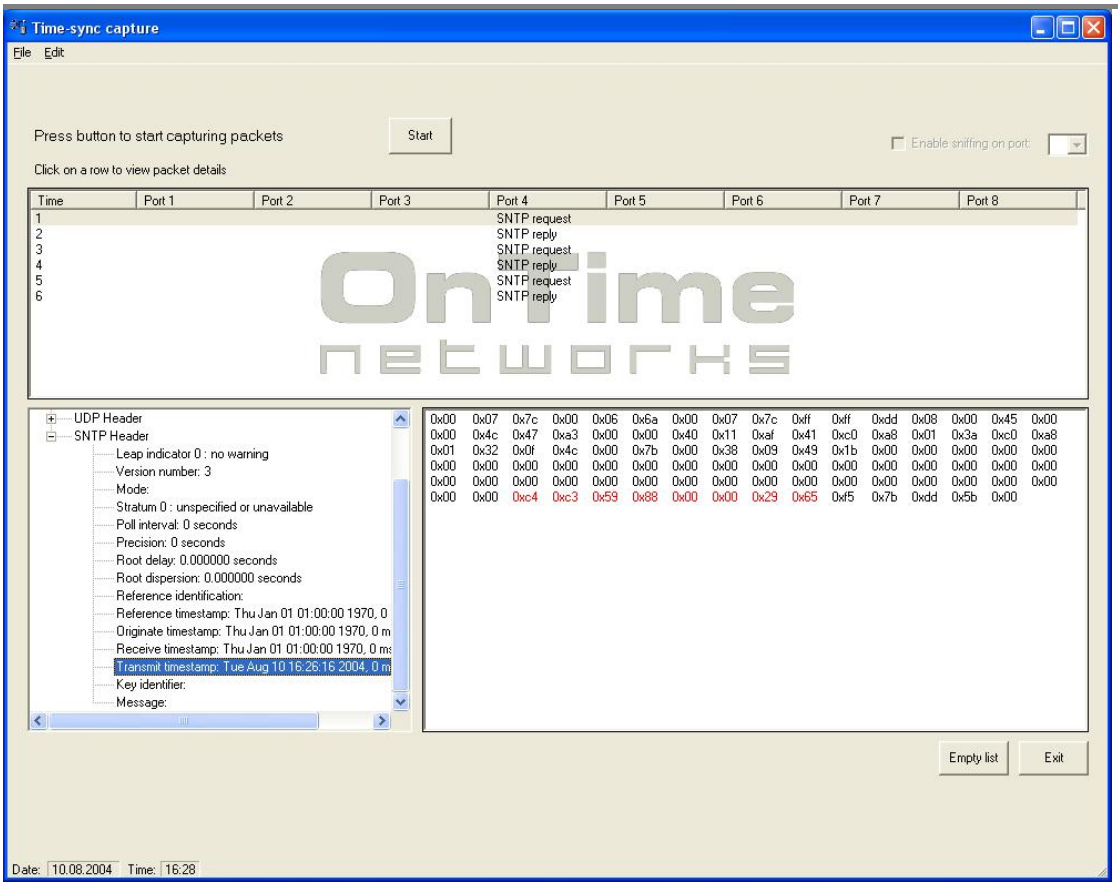


Figure 19, SNTP request packet

13.4 SNTP/NTP time client

The switch can also operate as an SNTP/NTP time client. The switch will then perform time updates versus one or more SNTP/NTP servers in the network in order to update the local clock of the T200 switch. The SNTP/NTP time servers used for time updates are automatically detected. This means that SNTP request packets are sent as local broadcast (anycast in SNTP terminology, see RFC2030 for details) in order to detect available T200 SNTP/NTP servers.

The switch will also act as a time server on the serial interface since this switch is configured as a SNTP client (not SNTP/NTP server with a GPS connected to the serial interface). This means that serial enabled devices can be connected to the T200 serial interface and receive time updates on this interface. Time updates is sent on regular intervals according to the following scheme:

- output UTC
- transmission every second
- transmission with control characters
- transmission with ETX on second increment
- transmission with second forerun

- transmission sequence of control characters CR/LF
- standard string date and time

The characters in each time update are as follows:

0 STX (Start of Text)
1 Status (internal status of the clock), see below
2 day of the week (Monday... Sunday) (hexadecimal coding)
Since 'UTC-time' is used, bit 3 in the "day of the week" is set to 1
3 tens - hours
4 unit - hours
5 tens - minutes
6 unit - minutes
7 tens - seconds
8 unit - seconds
9 tens - day
10 unit - day
11 tens - month
12 unit - month
13 tens - year
14 unit - year
15 LF (Line Feed)
16 CR (Carriage Return)
17 ETX (End of Text)

; where STX = 0x02, ETX = 0x03, LF = 0x0A and CR = 0x0D and status:

The Status byte in the UTC string is described in the table below:

	Hex representation	Nibble representation				Description
Status	0	0	0	x	x	Time/date invalid[2]
	4	0	1	x	x	Crystal operation on SNTP client [3]
	8	1	0	x	x	Local clock operation on T200 SNTP server [4]
	C	1	1	x	x	GPS operation on T200 SNTP server [5]
Days of week	0	0	x	x	x	CEST/CET
	8	1	x	x	x	UTC-time
	9	x	0	0	1	Monday
	A	x	0	1	0	Tuesday
	B	x	0	1	1	Wednesday
	C	x	1	0	0	Thursday
	D	x	1	0	1	Friday
	E	x	1	1	0	Saturday
	F	x	1	1	1	Sunday

[2] SNTP client is not synchronized with a T200 SNTP server.
[3] SNTP client is synchronized with a T200 SNTP server configured without external time base (no reference to absolute time).
[4] SNTP client is synchronized with a T200 SNTP server with external time base (GPS) that has lost GPS coverage (valid reference to absolute time).
[5] SNTP client is synchronized with a T200 SNTP server with external time base (GPS) with GPS coverage (valid reference to absolute time). Best accuracy.

The status byte is output as hexadecimal value. For example: the status character for GPS operation (high accuracy) is output as “C”.

The total time synchronization concept where time synchronization via the Ethernet and the serial interface is shown in Figure 20.

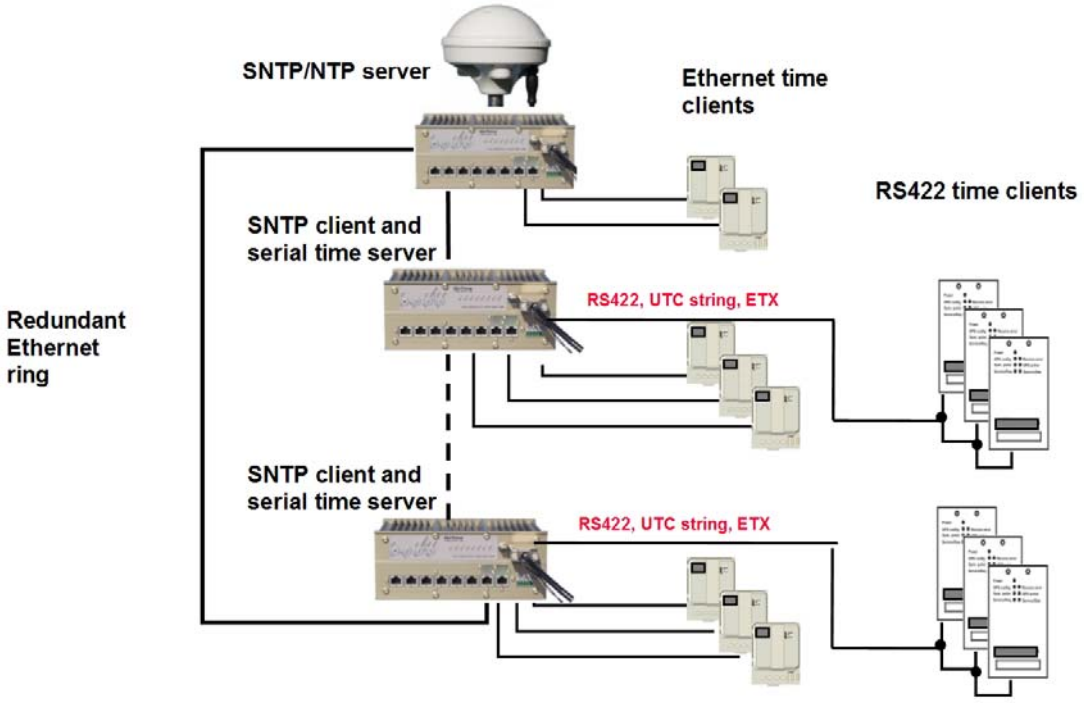


Figure 20, SNTP time client and serial time server

In order to achieve redundancy, the SNTP time client will request for new SNTP servers at regular intervals (1 second). The server selection is done using the scheme shown in Figure 21. The roundtrip delay is defined as d = (T4 – T1) – (T2 – T3) using the time stamp definitions in Figure 15.

Whenever there is a change in the SNTP client going to better accuracy (status change 4 → 8, 8 → 12 or 4 → 12), the status output on the serial time server will be held invalid for a period of TBD seconds. This is to avoid that two or several different serial time clients can have a valid status, but at the same time be out of synchronization. For the same reason, the output status byte will indicate invalid time/date for 60 seconds when the SNTP client switches from one SNTP server to another. An important exception is when the SNTP client stays in the highest accuracy during the transition. This implies that redundancy for single point of failure can be achieved.

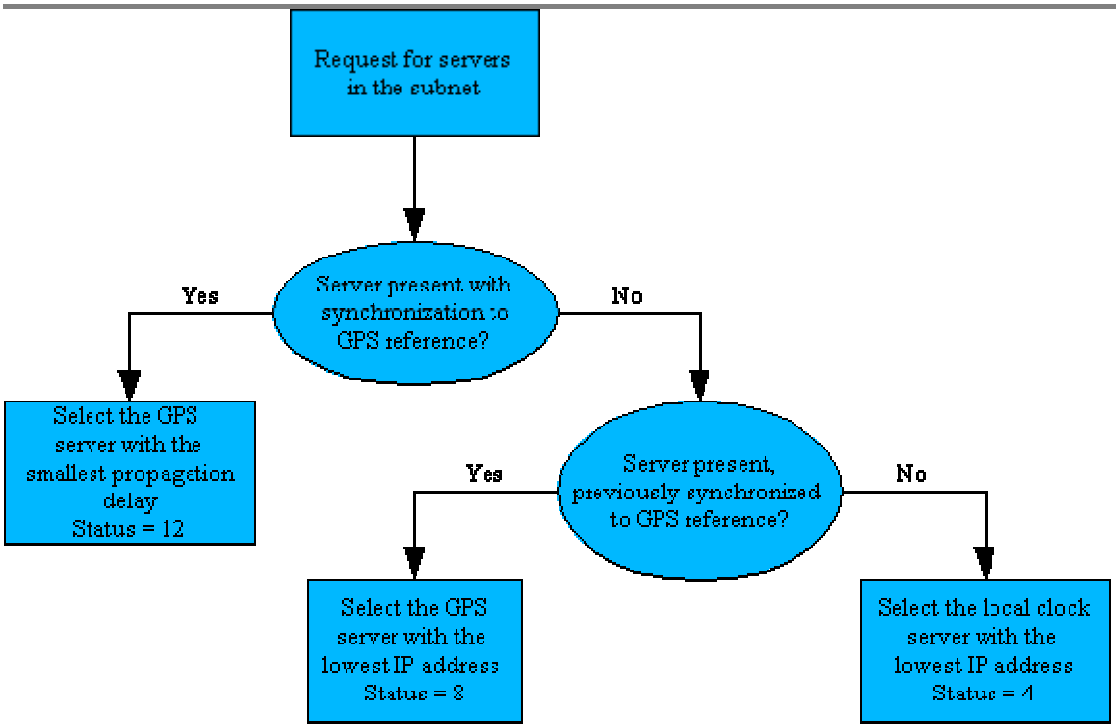


Figure 21, T200 SNTP client: selection of T200 SNTP server

Note: Other Ethernet SNTP/NTP time clients should also select the SNTP/NTP time server with the lowest IP address in case of no GPS coverage on all available SNTP/NTP servers.

13.5 IRIG-B

An optical IRIG-B output signal is generated on the ST 850nm fiber transmitter on the T200 front panel if the switch is enabled for SNTP server, SNTP client or IEEE1588 Grand master.

The IRIG-B protocol is a serial protocol that is sent every second with the following packet format:

SS:MM:HH:DD:D0, then status

A position marker, “P” and a “0” is sent between each nibble (e.g. between S and S)

- element 1: SS is seconds, [0..59], note only three bits is used for the second nibble
- element 2: MM is minutes, [0..59]
- element 3: HH is hours, [0..23]
- element 4: DD is days, [0..99]
- element 5: DD is days*100, [0..3]
- element 6: status
- element 7: NA
- element 8: NA
- element 9: NA
- element 10: NA

13.6 Pulse Per X seconds on GPS interface

Two PPX copper output signal can be generated on the GPS interface (15 pin connector) on the front panel of the T200 if the switch is enabled for SNTP server, SNTP client or IEEE1588 Grand master. PPX means that a Pulse Per X seconds is generated. The interval X is 1 by default.

The pulse duration and interval, X, for these two output signals can be configured via SNMP.

Legal interval is:
X = [1, 5, 10, 60, 3600] seconds.
The interval can be different for the two PPX signals.

Legal duration is:
[10us, 20us, 30us, 40us, 50us, 60us, 70us, 80us, 90us, 100us, 1ms, 10ms, 100ms]
The pulse duration is the same for the two PPX signals.

Each of the two output signals is available either as a TTL signal or RS-422.

13.7 Pulse Per Minute on STAT pin

A PPS output signal will be generated on the STAT pin on the power connector.

A Pulse Per Minute (PPM) output signal can be generated on the STAT pin on the power connector if the “Pulse Per Minute” tick box is enabled in the IP configuration tool. The fault contact (STAT pin) will be set for duration of 100ms each minute. All alarms see 5.2, will be disabled if the PPM feature is enabled. The PPM output signal is not an accurate output signal. The accuracy of the PPM signal to UTC is better than 10 ms on the rising pulse (unset to set on the STAT pin).

13.8 External GPS

The T200 GPS interface supports the use of either RS232 or RS-422 interface between the T200 switch and the GPS receiver. The interface that is not used shall be left unconnected, and the T200 will automatically detect the active interface. RS-422 is preferred in all industrial installations due to improved immunity and possibility to use long cables (up to 1km). RS232 and TTL inputs shall only be used when short cables are used and the GPS receiver is installed in the same cabinet as the timeserver. Shielded cables that comply with RS-422 installations and relevant environment shall be used. The GPS interface connector is described in details in the Installation Guide.

An isolation barrier with 3kV (peak to peak) isolation is present between interface signals and internal electronics. Surge clamping devices is present on each input protecting the internal electronics for high energy surges.

The ACUTIME GPS receiver from Trimble Inc, www.trimble.com, is the Westermo OnTime recommended GPS receiver. The GPS receiver and GPS antenna are integrated in the same IP67 housing, and the GPS interface supports RS-422 on both the PPS and the serial interface (where NMEA reports are received). This GPS receiver/antenna is shown below:

Figure 22, Acutime GPS receiver and antenna

13.9 Time Synchronization Redundancy

The figures below show how network and time server redundancy can be achieved.

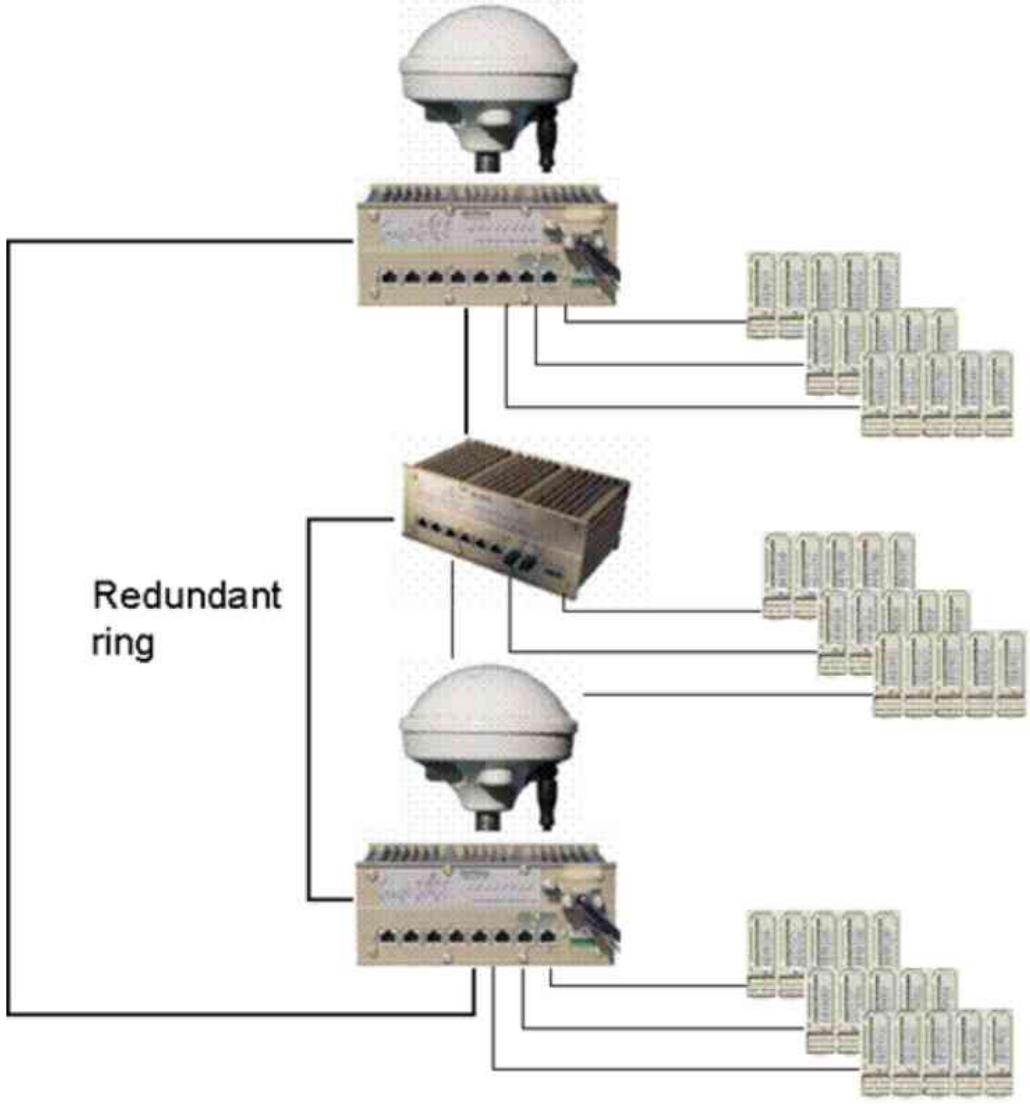


Figure 23, Network and time synchronization redundancy 1

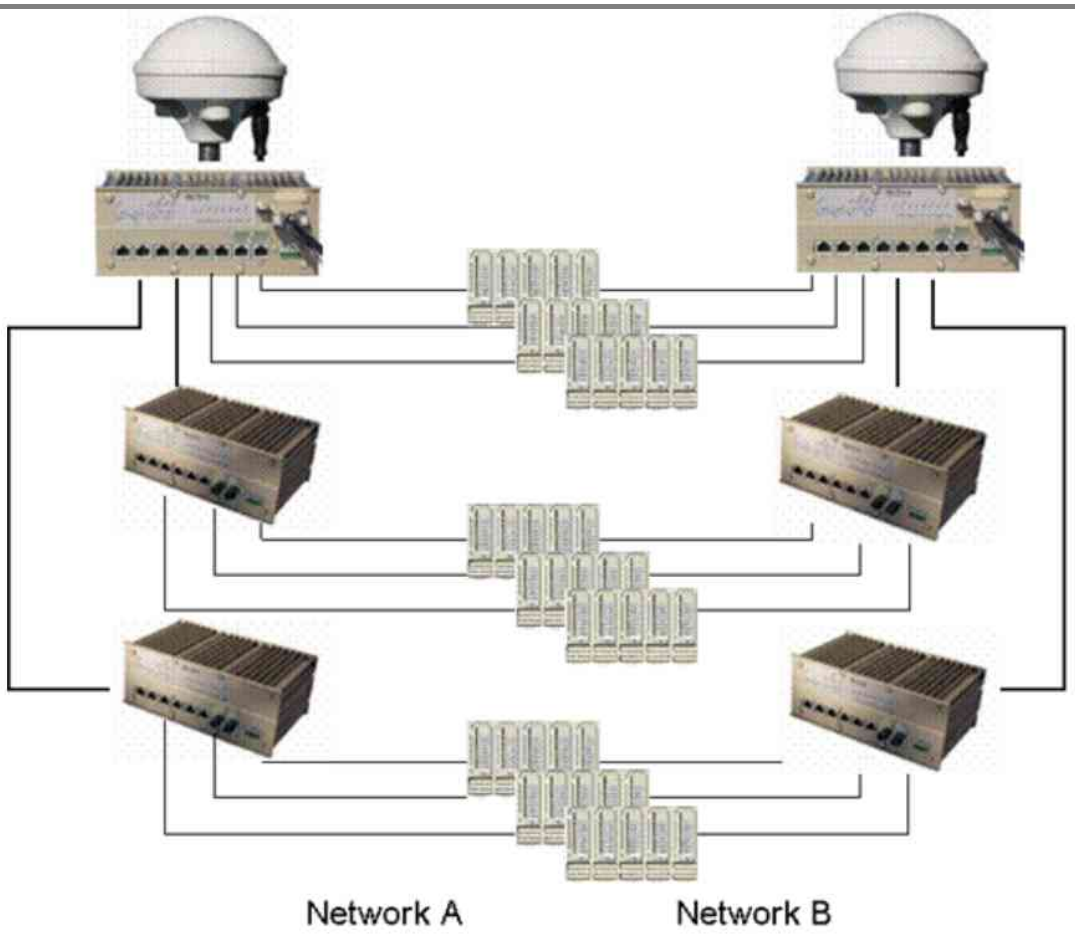


Figure 24, Network and time synchronization redundancy 2

14 Switch Technical Specification

14.1 Interface Specifications

RJ-45 Ports	10/100BASE-TX
	Auto Negotiation Feature Speed Full and Half Duplex mode Auto MDI/MDI-X
	Manual Negotiation Speed Full and Half Duplex mode
Fiber Ports	100BASE-FX Ports
Alarm Contact	Single relay output. Maximum capacity 250 mA

14.2 Fiber Specifications

Distances	Multi mode Single mode	2-3KM 15KM, 40KM or 85KM
Wavelength	See 4.7.2	
Loss Budget Information:	See 4.7.2	
Sensitivity:	See 4.7.2	

14.3 Power Specification

Input Voltage	19VDC..60VDC
Input Current (@24VDC)	Typical 6-17 Watts
Inrush Current	Less than two times nominal current.
Maximum Current	

(All Fiber 85KM Ports)	Maximum 8Watt to 20Watts (Model Dependant)

14.4 Environmental Specification

Indoor use or corresponding environment
Altitude up to 2000M
Operating temperature (-40 .. +65'C) (55deg on F8)
Humidity 5-95'C
Enclosure IP40

14.4.1 Climatic

Cold	IEC 68-2-1 Ad (-40 'C operational 16 Hours)
Storage	IEC 68-2-1 Ad (-40 'C 16 Hours)
Dry Heat	IEC 68-2-2 Bd (+70 'C operational 16 Hours)
Humidity	IEC 68-2-30 Db (25 'C .. 55 'C 95% 6 Cycles 24 Hours)

14.4.2 Mechanical

Oscillation	IEC 255-21-1 Class 1
Shock	IEC 255-21-2 Class 1
Enclosures	IEC 529, IP 40

14.4.3 Electromagnetic Compatibility (EMC)

Industrial Immunity	EN 61000-6-2
Industrial Emission	EN 50081-2
Home / Office Emission	EN 50081-1

14.4.4 Radiated Immunity

ESD	EN 61000-4-2 (4/8 kV)
Magnetic Field	EN 61000-4-8 (300A/m)
RF Field Disturbance	EN 61000-4-3 10 V/m 80% AM 80 .. 1000MHz

14.4.5 Conducted Immunity

Fast Transients	EN 61000-4-4 AC/DC 2kV, Signal 1kV

Surge Immunity	EN 61000-4-5 AC: 2kV/1kV DC: 0.5kV/0.5kV Signal 1kV/-
Voltage Dips Voltage Interruptions	EN 61000-4-11 for AC Supply
Conduced RF Disturbance	EN 61000-4-6 10V, 80% AM, 0, 15-80 MHz

14.4.6 Safety

Low Voltage Directive Standard	EN 60950

Class 1 equipment, in which exposed conductive parts are bonded to a connecting means for a protective conductor.

Eye Safety	IEC 825-1 Class 1