# Technical Description

## MINI-LINK 6600 R1

DESCRIPTION

**Copyright**

**Disclaimer**

# Contents

# 1 Introduction

MINI-LINK 6600 consists of small flexible nodes for high capacity, with advanced Ethernet functionality and designed for an efficient migration path for customers going to an all-IP network.

The MINI-LINK 6600 product family:

- MINI-LINK 6651 (Compact Node)
- MINI-LINK 6654 with PNM 1001 or PNM 1002
- MINI-LINK 6655 with PNM 1002
- MINI-LINK 6691 with NPU 1002, NPU 1003, or NPU 1005
- MINI-LINK 6692 with NPU 1002 or NPU 1005
- MINI-LINK 6693 with NPU 1002, NPU 1003, or NPU 1005
- MINI-LINK 6694 with NPU 1002, NPU 1003, or NPU 1005

MINI-LINK 6600 provides a switch capacity of up to 88 Gbps and can connect up to 16 split mounted radio links with a maximum of 15 radio directions due to being equipped with dual carrier modems. 1 Gbps, 2.5 Gbps, and 10 Gbps interfaces, fiber rings and E-band links can also be connected to the node. The node supports radio links with high modulation of 4096 QAM.

MINI-LINK 6600 offers both compact nodes and nodes using plug-in units, which make it easy to customize configurations and make future upgrades. The full range of MINI-LINK outdoor units can easily be combined in many different ways: traditional frequencies (6–42 GHz), V-band 60 GHz, E-band 70/80 GHz, single and dual carrier, Coax and Ethernet interface.

Different packet migration strategies are supported by MINI-LINK 6600. For cost efficient migration MINI-LINK 6600 are hop compatible with MINI-LINK TN R6 equipped with MMU4 A. Upgrading a site to MINI-LINK 6600, the radio unit, antenna and outdoor cabling can be reused.

# 2 System Overview

From a functional and configuration perspective, a Network Element (NE) based on MINI-LINK 6600 can be divided into the following parts:

| | |
|---|---|
| **Basic Node** | The Basic Node holds the system platform providing traffic and system control.<br>Specific plug-in units provide Ethernet and TDM traffic interfaces for connection to other network equipment, for example radio base stations.<br>It also includes indoor mechanical housing, power distribution, and cooling. |
| **Radio Terminals** | A Radio Terminal provides microwave transmission and consists of an outdoor radio connected to an indoor modem carrier, that is, a split mount solution.<br>MINI-LINK 6600 provides single or dual carrier modem, and can be connected to two outdoor radios to create two separate Radio Terminals.<br>For more information, see Section 3 on page 11. |

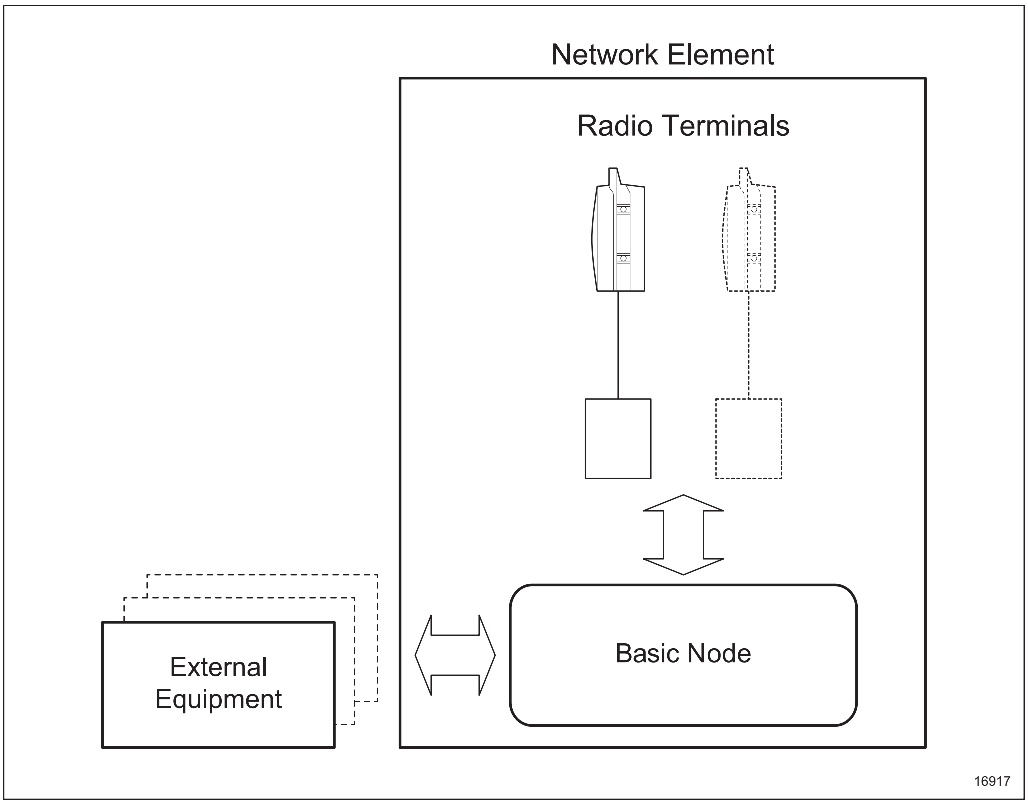


Figure 1 Basic Node and Radio Terminals

## 2.1 Indoor Part

All MINI-LINK 6600 products fit into standard 19" or metric racks.

Table 1 MINI-LINK 6600 Comparison

| | **MINI-LINK 6651/1 Compact Node** | **MINI-LINK 6651/2 Compact Node** | **MINI-LINK 6651/3 Compact Node** | **MINI-LINK 6651/4 Compact Node** | **MINI-LINK 6654** | **MINI-LINK 6655** | **MINI-LINK 6691** | **MINI-LINK 6692** | **MINI-LINK 6693** | **MINI-LINK 6694** |
|---|---|---|---|---|---|---|---|---|---|---|
| Height | 1U | 1U | 1U | 1U | 1U | 1.5U | 1U | 3U | 1.5U | 2U |
| Traffic interfaces | 2×FE/1G RJ45<br>4×1G/2.5G SFP+<br>8×E1 | 2×FE/1G RJ45<br>3×1G/2.5G SFP+<br>8×E1 | 2×FE/1G RJ45<br>4×1G/2.5G SFP+<br>8×E1 | 2×1G RJ45<br>4×1G/10G SFP+<br>8×E1 | 2xFE/1G RJ45<br>2x1G SFP<br>2x1G/10G SFP+<br>4xE1/DS1 | 2xFE/1G RJ45<br>2x1G SFP<br>2x1G/10G SFP+<br>4xE1/DS1 | 2×FE/1G RJ45<br>1×FE/1G SFP<br>2×1G/10G SFP+ | 2×FE/1G RJ45<br>1×FE/1G SFP<br>2×1G/10G SFP+ | 2×FE/1G RJ45<br>1×FE/1G SFP<br>2×1G/10G SFP+ | 2×FE/1G RJ45<br>1×FE/1G SFP<br>2×1G/10G SFP+ |

Table 1 MINI-LINK 6600 Comparison

| | **MINI-LINK 6651/1 Compact Node** | **MINI-LINK 6651/2 Compact Node** | **MINI-LINK 6651/3 Compact Node** | **MINI-LINK 6651/4 Compact Node** | **MINI-LINK 6654** | **MINI-LINK 6655** | **MINI-LINK 6691** | **MINI-LINK 6692** | **MINI-LINK 6693** | **MINI-LINK 6694** |
|---|---|---|---|---|---|---|---|---|---|---|
| Switch capacity | 14.5 Gbps | 14.5 Gbps | 14.5 Gbps | 47 Gbps | 36.5 Gbps (PNM 1001)<br>44 Gbps (PNM 1002) | 44 Gbps | 38 Gbps (NPU 1002 or NPU 1003)<br>43 Gbps (NPU 1005) | 88 Gbps(1) (NPU 1002)<br>65.5 Gbps (NPU 1005) | 46.5 Gbps (NPU 1002)<br>45.5 Gbps (NPU 1003)<br>55.5 Gbps (NPU 1005) | 59.5 Gbps (NPU 1002)<br>45.5 Gbps (NPU 1003)<br>55.5 Gbps (NPU 1005) |
| Combo solution (PFU, NPU, and MMU) | – | – | – | – | PNM 1001 or PNM 1002 | PNM 1002 | – | – | – | – |
| Node Processor Unit (NPU) | – | – | – | – | – | – | NPU 1002, NPU 1003 or NPU 1005 | NPU 1002 or NPU 1005(2) | NPU 1002, NPU 1003 or NPU 1005 | NPU 1002, NPU 1003 or NPU 1005(2) |
| Dual Carrier Modem Unit (MMU) | – | – | – | – | MMU 1002 or MMU 1004 | MMU 1002 or MMU 1004 | MMU 1002 or MMU 1004 | MMU 1002 or MMU 1004 | MMU 1002 or MMU 1004 | MMU 1002 or MMU 1004 |
| Single Carrier Modem Unit (MMU) | – | – | – | – | MMU 1001 | MMU 1001 | MMU 1001 | MMU 1001 | MMU 1001 | MMU 1001 |
| Line Termination Unit (LTU) for E1/DS1 | – | – | – | – | LTU 1001 | LTU 1001 | LTU 1001 | LTU 1001 | LTU 1001 | LTU 1001 |
| Line Termination Unit (LTU) for E1/DS1 and STM-1 | – | – | – | – | LTU 1002 | LTU 1002 | LTU 1002 | LTU 1002 | LTU 1002 | LTU 1002 |
| Ethernet Termination Unit (ETU) | – | – | – | – | ETU 1001 | ETU 1001 | ETU 1001 | ETU 1001 | ETU 1001 | ETU 1001 |
| Ethernet Termination Unit (ETU) | – | – | – | – | ETU 1002 | ETU 1002 | ETU 1002 | ETU 1002 | ETU 1002 | ETU 1002 |

(1) 7.5 Gbps is reserved for future use.

(2) NPU protection can be used with two NPU 1002 or two NPU 1005.

The indoor part also includes cables and installation accessories.

The interconnection between the outdoor part (radios and antennas) and the indoor part is one coaxial cable per carrier interface. This cable carries full duplex traffic, DC supply voltage, and management data.

### 2.1.1 MINI-LINK 6651 Indoor Parts

MINI-LINK 6651 is a compact node suitable for tail sites.

It has a replaceable Fan Unit that provides cooling for the indoor part.

There are four variants, MINI-LINK 6651/1 (Figure 2), MINI-LINK 6651/2 (Figure 3), MINI-LINK 6651/3 (Figure 4), and MINI-LINK 6651/4 (Figure 5).

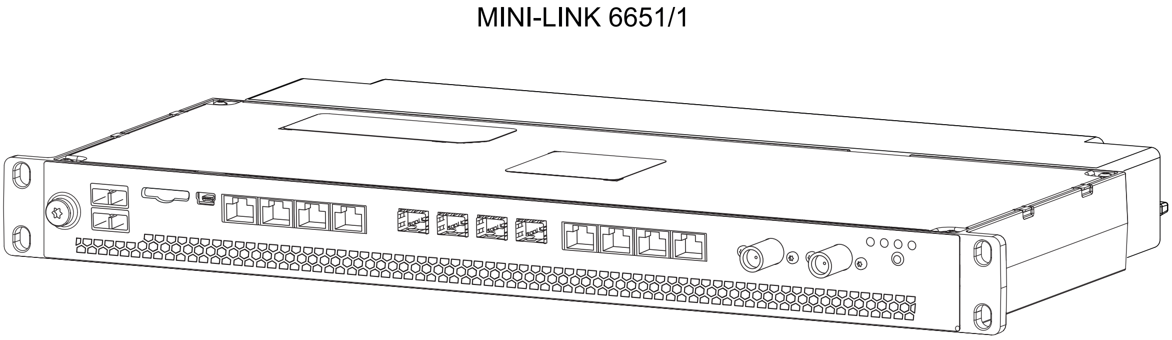


Figure 2 MINI-LINK 6651/1

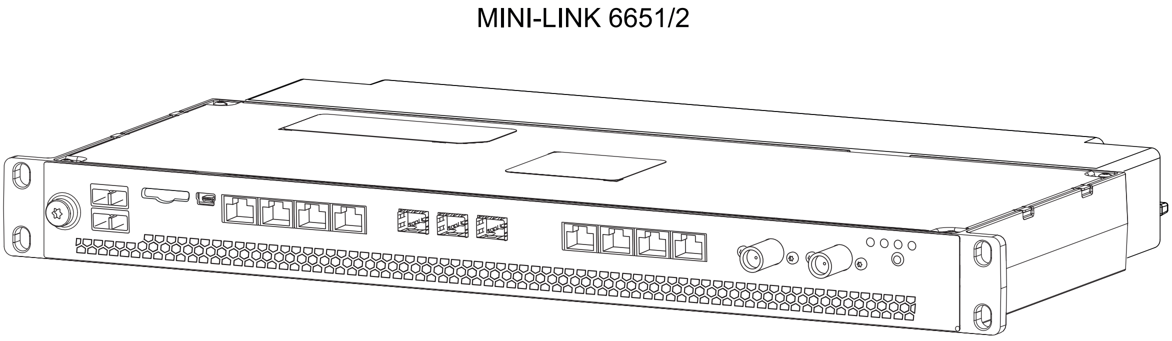


Figure 3 MINI-LINK 6651/2

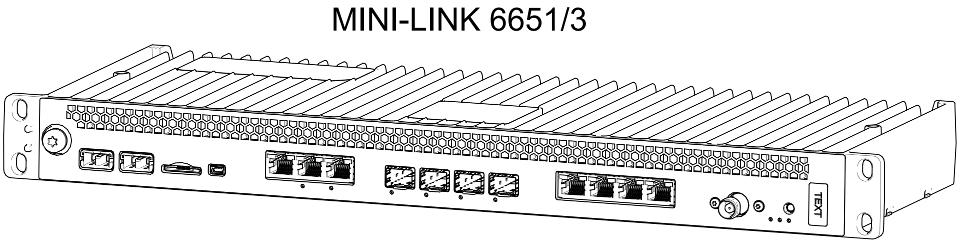


Figure 4 MINI-LINK 6651/3

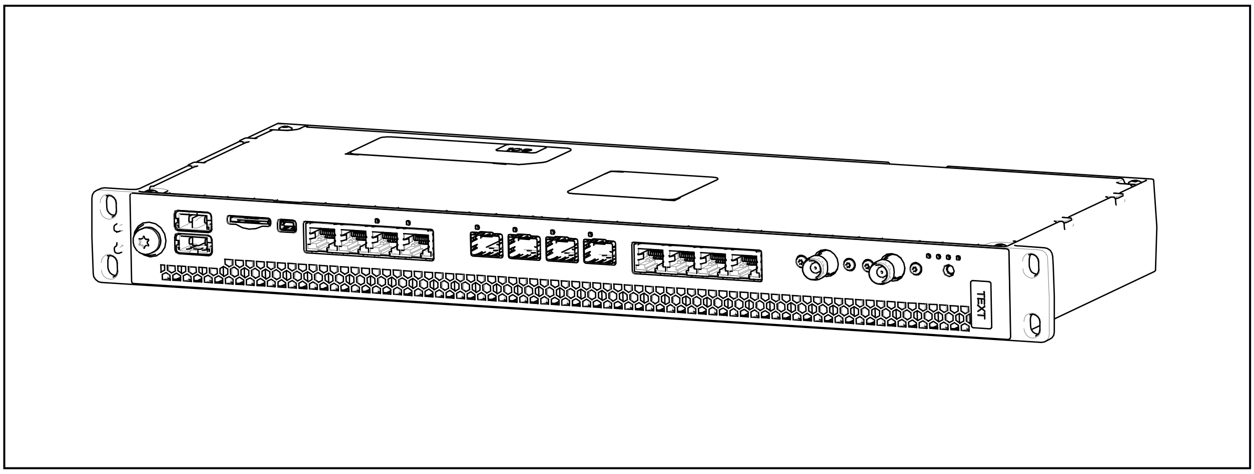


Figure 5 MINI-LINK 6651/4

### 2.1.2 MINI-LINK 6654 and MINI-LINK 6655 Indoor Parts

The indoor part consists of an Enclosure with plug-in units interconnected through a backplane. One plug-in unit occupies one slot in the Enclosure.

| | |
|---|---|
| **Enclosure** | The Enclosure houses the plug-in units and provides backplane interconnection of traffic, power, and control signals. It fits into standard 19" or metric racks. |
| **PFU, NPU, and MMU (PNM) Unit** | The PNM handles the control functions of the system. It also provides traffic and management interfaces. |
| **Modem Unit (MMU)** | The MMU constitutes the indoor part of a Radio Terminal. It determines the traffic capacity and modulation scheme. |
| **Fan Unit (FAU)** | The FAU provides cooling for the indoor part. |
| **Line Termination Unit (LTU)** | The LTU provides E1/DS1 interfaces. LTU 1002 also provides an STM-1 interface. |
| **Ethernet Termination Unit (ETU)** | The ETU provides Ethernet interfaces. |

### 2.1.3 MINI-LINK 6691, MINI-LINK 6692, and MINI-LINK 6693 Indoor Parts

The indoor part consists of an Enclosure with plug-in units interconnected through a backplane. One plug-in unit occupies one slot in the Enclosure.

| | |
|---|---|
| **Enclosure** | The Enclosure houses the plug-in units and provides backplane interconnection of traffic, power, and control signals. It fits into standard 19" or metric racks. |
| **Node Processor Unit (NPU)** | The NPU handles the control functions of the system. It also provides traffic and management interfaces. |
| **Modem Unit (MMU)** | The MMU constitutes the indoor part of a Radio Terminal. It determines the traffic capacity and modulation scheme. |
| **Power Filter Unit (PFU)** | The PFU filters the external power and distributes the internal power to the plug-in units through the backplane. |
| **Fan Unit (FAU)** | The FAU provides cooling for the indoor part. |
| **Line Termination Unit (LTU)** | The LTU provides E1/DS1 interfaces. LTU 1002 also provides an STM-1 interface. |
| **Ethernet Termination Unit (ETU)** | The ETU provides Ethernet interfaces. |

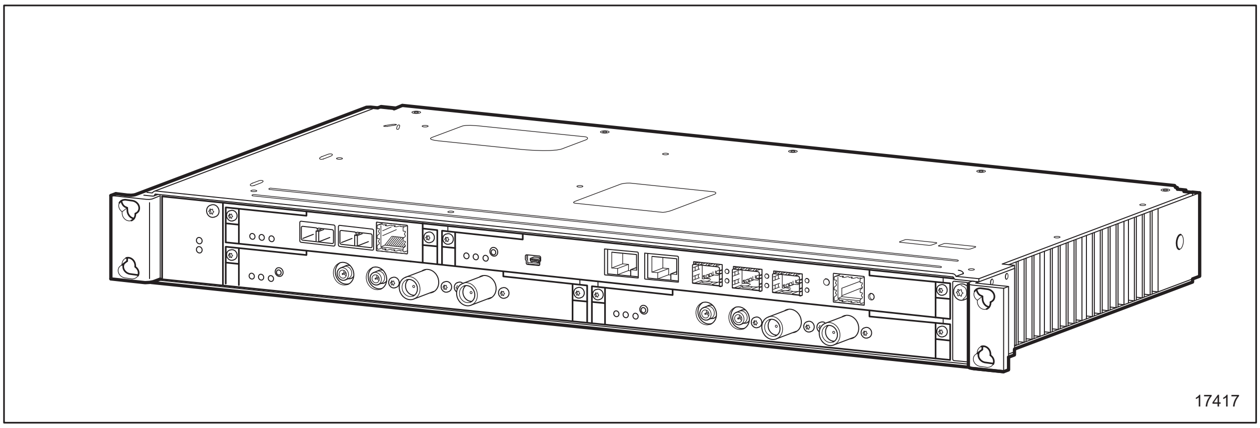


Figure 6 MINI-LINK 6691

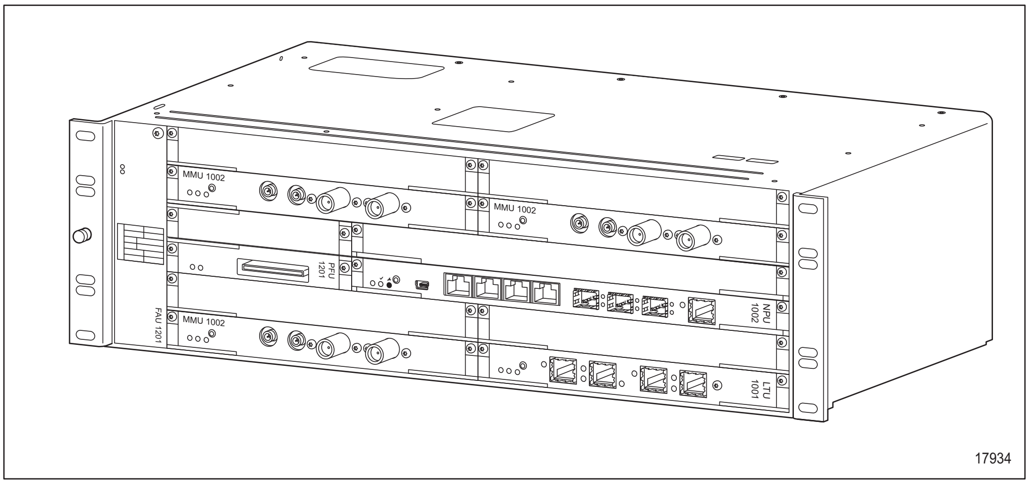


Figure 7 MINI-LINK 6692

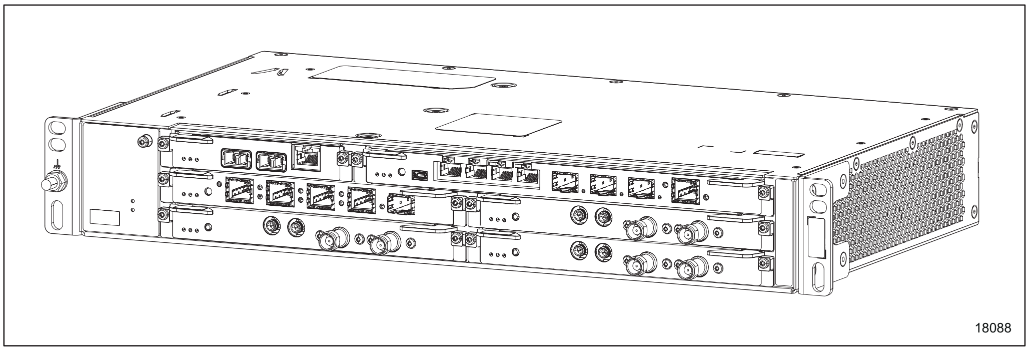


Figure 8 MINI-LINK 6693

## 2.2 Outdoor Part

The outdoor part is supplied for various frequency bands, including the E-band (80 GHz). It consists of an antenna, a radio, and associated installation hardware. The MINI-LINK 6363, MINI-LINK 6363/2, MINI-LINK 6365, and RAU2 X radios can be connected to a MINI-LINK 6600 modem.

The radio and the antenna are easily installed on a wide range of support structures. The radio is fitted directly to the antenna as standard, integrated installation. The radio and the antenna can also be fitted separately and connected by a flexible waveguide. In all cases, the antenna is easily aligned and the radio can be disconnected and replaced without affecting the antenna alignment.

The MINI-LINK 6363, MINI-LINK 6363/2, MINI-LINK 6365, and RAU2 X radios are described in more detail in Section 15.18 on page 204.

The antennas are described in more detail in Section 15.19 on page 211.

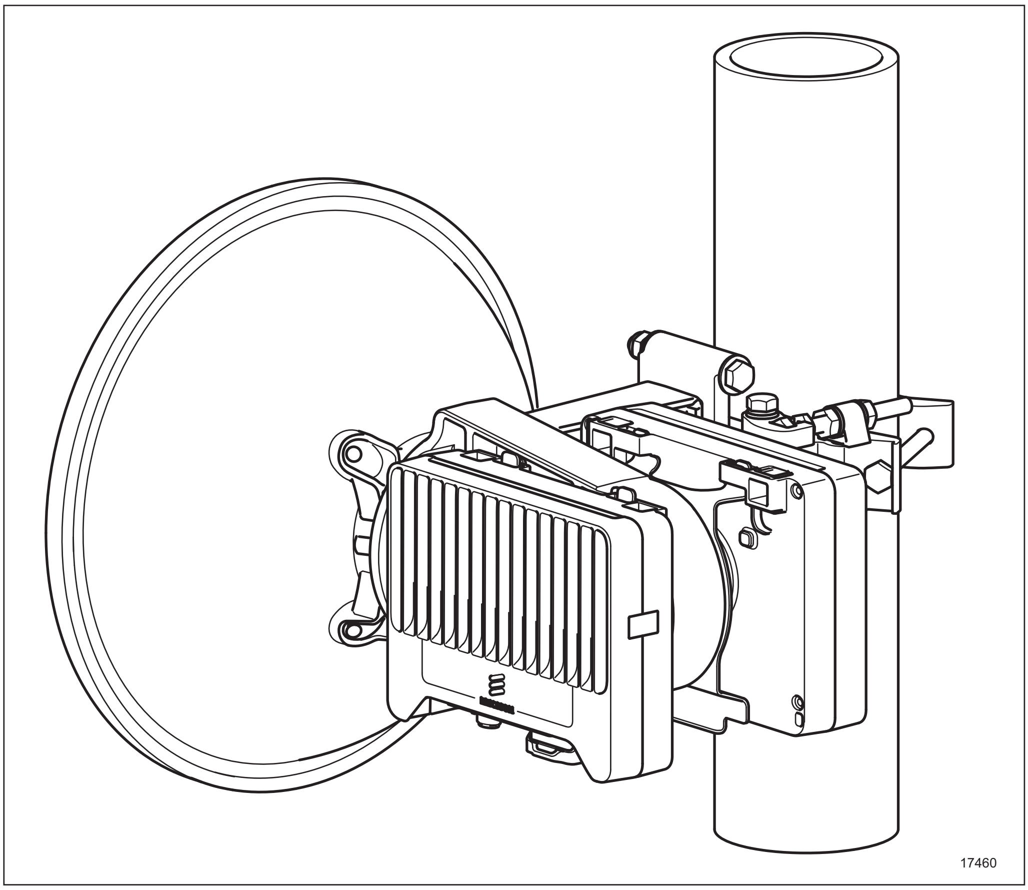


Figure 9 MINI-LINK 6363 or MINI-LINK 6365 and Antenna

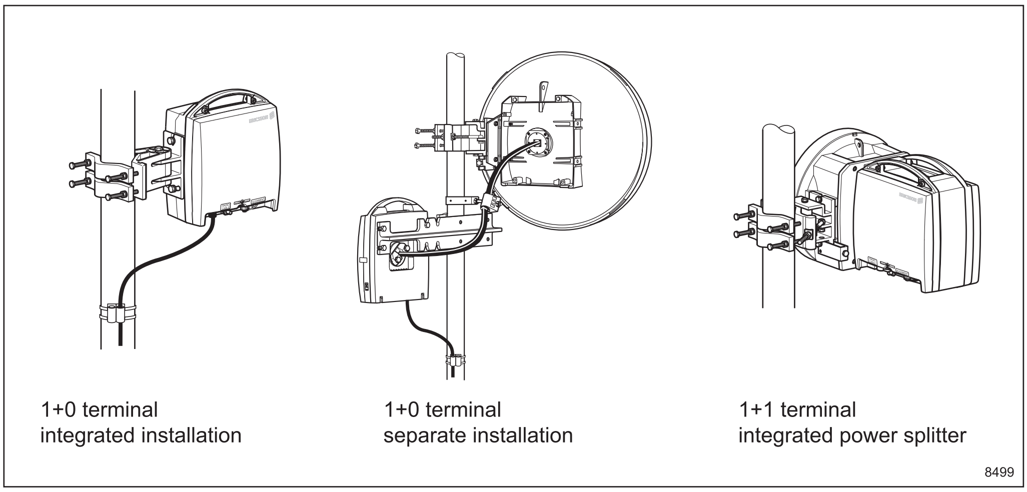


Figure 10 RAU2 X and Antennas in Different Installation Alternatives

# 3 Radio Link

MINI-LINK 6600 provides radio links for microwave transmission up to 1067 Mbps, operating within the 5 to 80 GHz frequency bands, using 4–4096 QAM modulation schemes.

MINI-LINK 6600 supports Ethernet (packet link), PDH, and a mix thereof in a Hybrid Radio Link sending Ethernet and PDH traffic simultaneously.

MINI-LINK 6600 can be configured as unprotected (1+0), 1+1 Radio Link Protection, or 2+0 Radio Link Bonding, and supports Cross Polarization Interference Canceller (XPIC), Adaptive Coding and Modulation (ACM). MINI-LINK 6600, except from MINI-LINK 6651, also supports Multiple Input Multiple Output (MIMO). Dual 1+0 is available in MINI-LINK 6600, except with MINI-LINK 6651/1 or MINI-LINK 6651/3.

## 3.1 Hybrid Radio Link

A Hybrid Radio Link is a Radio Link optimized for maximum throughput of Ethernet and PDH traffic.

**Note:** MINI-LINK 6651 can only send PDH traffic with E1s, that is, only for ETSI.

Ethernet and PDH traffic are sent simultaneously over the Hybrid Radio Link, see Figure 11.

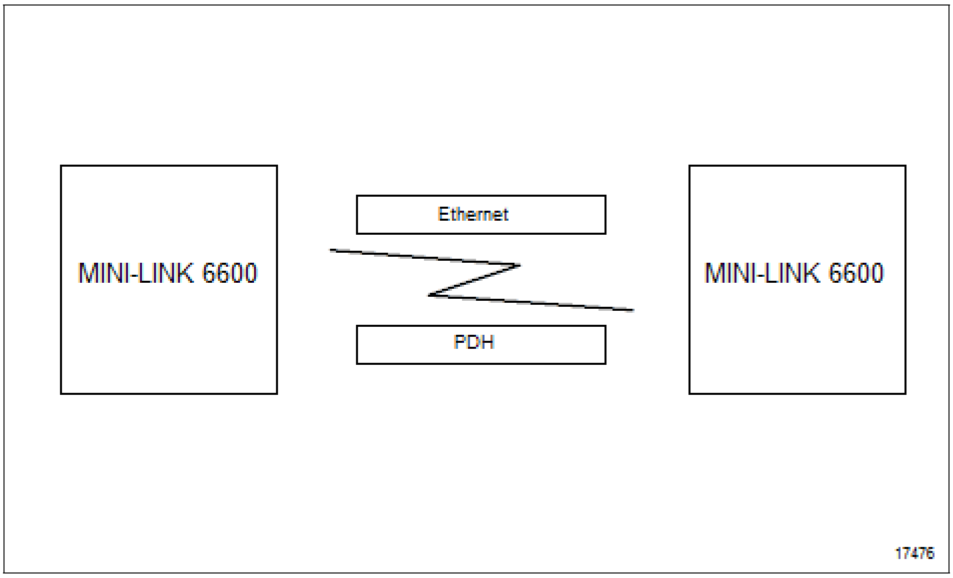


Figure 11 Traffic over a Hybrid Radio Link

The Ethernet traffic is sent over a dedicated physical link. When Ethernet is sent over a Hybrid Radio Link, the capacity range is from 0 Mbps to total link capacity depending on the amount of configured PDH Traffic.

A Hybrid Radio Link supports flat multiplexing of PDH traffic, which enables control of the number of E1s/DS1s to be transported. PDH traffic is normally transported in sets of 4×E1/DS1 and 16×E1/DS1. With flat multiplexing it is possible to set an exact number of E1s/DS1s to be transported, for example, 7×E1/DS1 or 23×E1/DS1. This allows optimized usage of bandwidth since all E1s/DS1s fitting in the bandwidth also can be transported. Due to the use of one mux layer for all E1s/DS1s, instead of one mux layer for each set of 4×E1/DS1 and 16×E1/DS1, the PDH overhead is decreased. A minimum of the total link capacity is used for overhead and PDH traffic and all remaining capacity can be used for Ethernet.

The ratio between Ethernet and PDH traffic is configurable and is set with E1/DS1 granularity, see Figure 12.

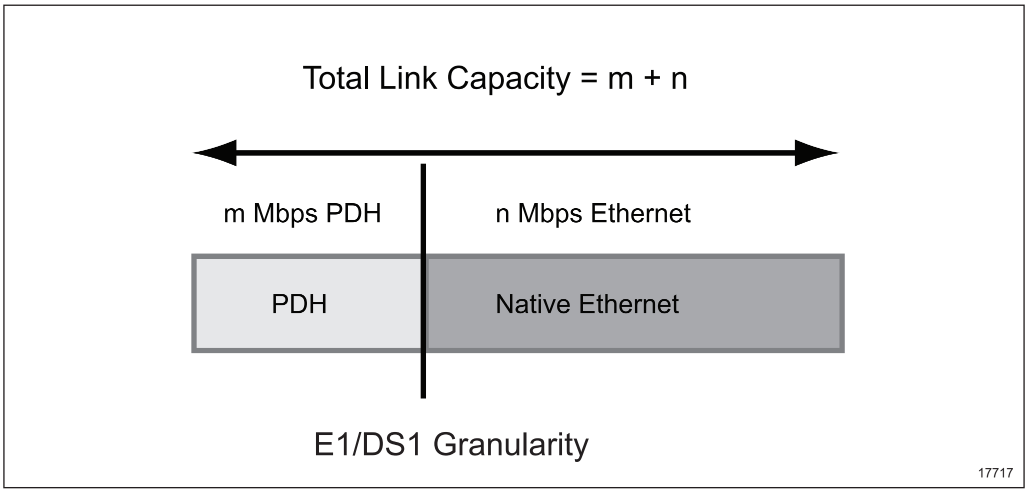


Figure 12 Packet Sent over a Hybrid Radio Link

**Example (ETSI)**

- Total link capacity: 154 Mbps
- PDH traffic capacity: 22×E1 (45 Mbps)
- Ethernet capacity: 154 Mbps – 45 Mbps = 109 Mbps

**Example (ANSI)**

- Total link capacity: 158 Mbps
- PDH traffic capacity: 22×DS1 (34 Mbps)
- Ethernet capacity: 158 Mbps – 34 Mbps = 124 Mbps

In Hybrid Radio Links, Ethernet capacity range from 0 to maximum link capacity, while PDH capacity range from 0 to 80×E1/DS1. The PDH capacity is limited by the backplane capacity of the modem.

MMU 1002/1004 and MINI-LINK 6651 are hop compatible with MMU4 A in MINI-LINK TN R6. See MINI-LINK 6600 R1 Compatibility, Reference [1], for details regarding hop compatibility.

## 3.2 Hitless Adaptive Coding and Modulation

Hitless Adaptive Coding and Modulation (ACM) enables automatic switching between different physical modes, depending on radio channel conditions. Hitless ACM makes it possible to increase the available capacity over the same frequency channel during periods of normal propagation conditions.

Code rate and modulation, and thereby capacity, are high during normal radio channel conditions and lower during less favorable channel conditions, for example, when affected by rain or snow. Physical mode switches are hitless, that is, error free. In situations where traffic interruption normally would occur, it is possible to maintain parts of the traffic by switching to a lower physical mode, using Hitless ACM.

Figure 13 shows how the capacity changes when the received input signal crosses the receiver threshold for each physical mode order.

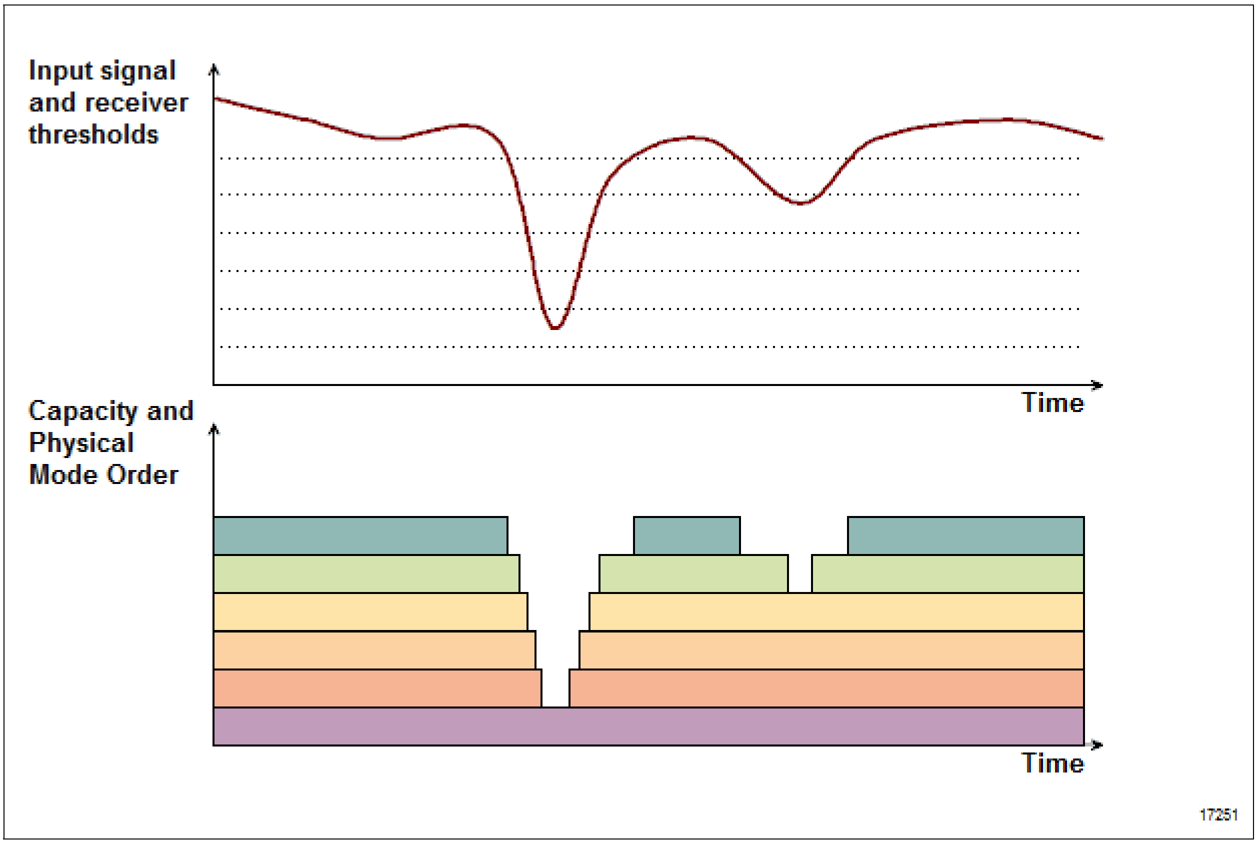

Input signal and receiver thresholds
Time
Capacity and Physical Mode Order
Time
17251

Figure 13 Principles of Hitless ACM

When using only Adaptive Modulation, the steps in Figure 13 only differ in terms of modulation. When using ACM, the steps can differ in both coding and modulation, which increases the number of possible steps.

In order to handle channel variations, the channel conditions are continuously monitored on the Rx side by measurement of Signal to Noise and Interference Ratio (SNIR). When the receiver, based on this data, detects that channel conditions imply a change to the next higher or lower physical mode, a message is sent to the transmitter on the other side requesting a higher or lower physical mode. Upon receipt of such request the transmitter starts transmitting with the new physical mode. Each direction is independent. At demodulation the receiver follows the physical mode as a slave.

The physical mode can also be configured with the maximum physical mode equal to the minimum physical mode, and thereby achieving a mode comparable to static mode, where the physical mode remains unchanged.

Hitless ACM is compatible with Automatic Transmit Power Control (ATPC), which works in a closed loop in any configured physical mode. If the modulation goes down, for example, due to interference, then the output power does not go to the maximum level.

### Buffering

ACM can influence the design of the buffer dimensioning. In case packet aging is not used, the maximum delay variation time will increase due to that the buffer is configured in bytes and that data will travel at a slower speed during lower physical mode steps. When packet aging is enabled, the maximum delay variation time will be kept regardless of physical mode level. This will also ensure that there is no old data in lower priority queues when physical mode is increased after a fading situation.

ACM can influence the position of the narrowest congestion point in the network, with too small buffers this can have a strong negative impact on utilization and end user TCP performance. To ensure high link utilization and high TCP performance, buffers for TCP traffic should be dimensioned in the area above average Round Trip Time (RTT), which is typically in the area of 100–200 ms.

### RSEC (ETSI only)

Reference Spectrum Efficiency Class (RSEC) defines the spectral mask, that is, which SEC that is used as a reference. The maximum output power is dependent on the RSEC used. The configurable RSEC depends on the configured minimum physical mode, which is illustrated in Table 2.

Table 2 RSEC (ETSI)

| Configured Minimum Physical Mode | Configurable RSEC |
|---|---|
| 4 QAM | 2, 4L, 4H, 5LB, 5HB, 6LB, 6HB, 7 |
| 16 QAM | 4L, 4H, 5LB, 5HB, 6LB, 6HB, 7 |
| 32 QAM | 4H, 5LB, 5HB, 6LB, 6HB, 7 |
| 64 QAM | 5LB, 5HB, 6LB, 6HB, 7 |
| 128 QAM | 5HB, 6LB, 6HB, 7 |
| 256 QAM | 6LB, 6HB, 7 |
| 512 QAM | 6HB, 7 |
| 1024 QAM | 7 |
| 2048 QAM | 7 |
| 4096 QAM | 7 |

When installing a new link or when upgrading an existing link to ACM, it is important to consider spectrum license requirements. The link configuration must be set with respect to the RSEC (referred to as Reference Mode in ETSI EN 302 217-1 and ETSI EN 302 217-2-2) and output power as specified in the spectrum license. Consult the relevant authority for information on the national radio transmission specifications and spectrum license conditions.

## 3.3 Transmit Power Control

The radio transmit power can be controlled in Remote Transmit Power Control (RTPC) mode, selectable from the management system, including setting of associated parameters. In Automatic Transmit Power Control (ATPC) mode, the transmit power can be increased rapidly during fading conditions, which allows the transmitter to operate at less than the maximum power during normal path conditions. The normally low transmit power allows more efficient use of the available spectrum, while the high transmit power can be used as input to path reliability calculations, such as fading margin and carrier-to-interference ratio.

Traditionally, the radio unit consumes the same amount of power independent of the output power used in the air interface. By using MINI-LINK ECO Mode, the radio units adjust the power requirements according to the used output power in the radio interface, which varies according to the actual link conditions and output margin design.

The transmitter can be turned on or off from the management system.

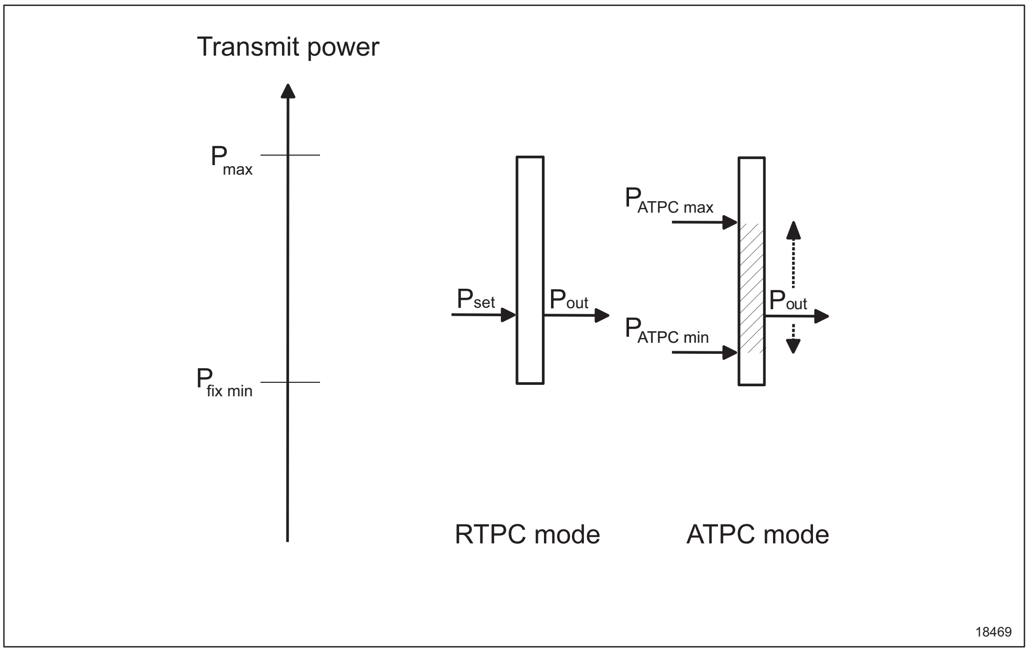


Figure 14 Transmit Power Control

### 3.3.1 RTPC Mode

In RTPC mode, the transmit power ($P_{out}$) ranges from a minimum level ($P_{fix\ min}$) to a maximum level ($P_{max}$). The desired value ($P_{set}$) can be set in 1 dBm increments.

### 3.3.2 ATPC Mode

ATPC is used to automatically adjust the transmit power ($P_{out}$) in order to maintain the received input level at the far-end terminal at a target value. The received input level is compared with the target value, and then a deviation is calculated and sent to the near-end terminal to be used as input for possible adjustment of the transmit power. ATPC varies the transmit power between a selected maximum level ($P_{ATPC\ max}$) and a selected minimum level ($P_{ATPC\ min}$).

The highest possible value for $P_{ATPC\ max}$ is $P_{max}$. The lowest possible value for $P_{ATPC\ min}$ is $P_{fix\ min}$. Therefore, the maximum adjustment range varies between these two values.

#### 3.3.2.1 Traffic Aware Power Save (TAPS)

TAPS (Traffic Aware Power Save) is a power saving functionality available for all MINI-LINK 6600 products, when used with MINI-LINK 6363 or MINI-LINK 6365 radio units. It is aimed at keeping the system power use as low as possible while still handling the actual traffic rate.

When TAPS is enabled, power consumption is automatically adapted based on actual capacity need by minimizing the transmitted power. Every 6 milliseconds, link utilization is measured by comparing the actual traffic rate with the possible traffic rate. If the system is working at the maximum possible rate configured, ATPC is enabled and no output power regulation is done by TAPS. On the other hand, if the system is not working at the maximum possible rate configured, TAPS is enabled and the output power is regulated to minimize the transmit power in relation to the actual traffic rate. If the system is running at the lowest configured rate, the power is slowly increased to avoid link loss. Based on the increases and decreases in near-end transmit power, higher or lower profile is requested by the far-end NE, which results in a higher or lower traffic rate, respectively.

**Note:** TAPS is a licensed feature.

ATPC has to be configured in order to enable TAPS.

## 3.4 Dual Carrier Modem

With the modem MMU 1002/1004 in MINI-LINK 6600, and the compact nodes MINI-LINK 6651/1, MINI-LINK 6651/2, and MINI-LINK 6651/4, dual carrier modems are introduced.

A dual carrier modem can be configured in different ways:

- Dual Directions

  When configured as a 1+0 dual directions link, each carrier has its own connection to a switchport and both carriers can optionally be configured as a Hybrid radio link, that is combining TDM and Ethernet traffic on the same radio path. In MINI-LINK 6651/1 dual directions is not available.

- Bonded Single Direction

  When configured as a 2+0 Radio Link Bonding (RLB) single direction link, the capacity of the two carriers are combined and only one switchport is used. In this configuration the combined capacity of the two can optionally be configured as a Hybrid Radio Link.

  When this is configured with one MMU 1002/1004 or one MINI-LINK 6651, RAU and antenna protection is achieved.

  When this is configured with two MMU 1002/1004s, MMU, RAU, and antenna protection is achieved, that is, Equipment Protection (EQP).

- Protected Single Direction

  When configured as a 1+1 Radio Link Protection (RLP) single direction link, both carriers are used for Radio Link path protection, and a single switchport is used.

  When this is configured with one MMU 1002/1004 or one MINI-LINK 6651, RAU and antenna protection is achieved.

  When this is configured with two MMU 1002/1004, MMU, RAU, and antenna protection is achieved, that is, EQP.

**Note:** EQP is not applicable for MINI-LINK 6651.

MMU 1002/1004 is described in detail in Section 15.12 on page 188.

**Note:** When having two MMU 1002/1004, 2+2 and 4+0 modes are also available, see Section 3.8.2 on page 25.

## 3.5 Radio Link Bonding

Radio Link Bonding (RLB) requires a license.

RLB uses multiple radio paths in a single direction to increase capacity. With RLB, a single port on the Ethernet switch is connected to an MMU/modem. The MMU/modem has an internal function to distribute the incoming Ethernet and PDH traffic between the available packet links.

The PDH traffic is prioritized and the remaining capacity is used for the packet links.

**Note:** MINI-LINK 6651 can only send PDH traffic with E1s, that is, only for ETSI.

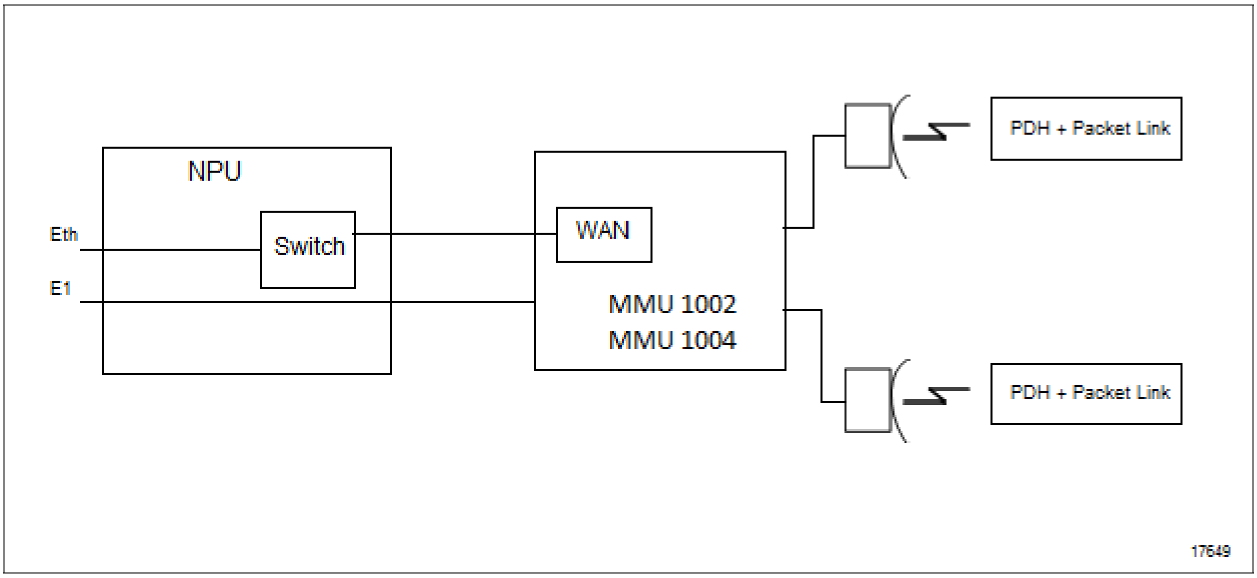


Figure 15 MINI-LINK 6691, 6692, 6693, and 6694, Hybrid Radio Link with RLB, Frequency Diversity

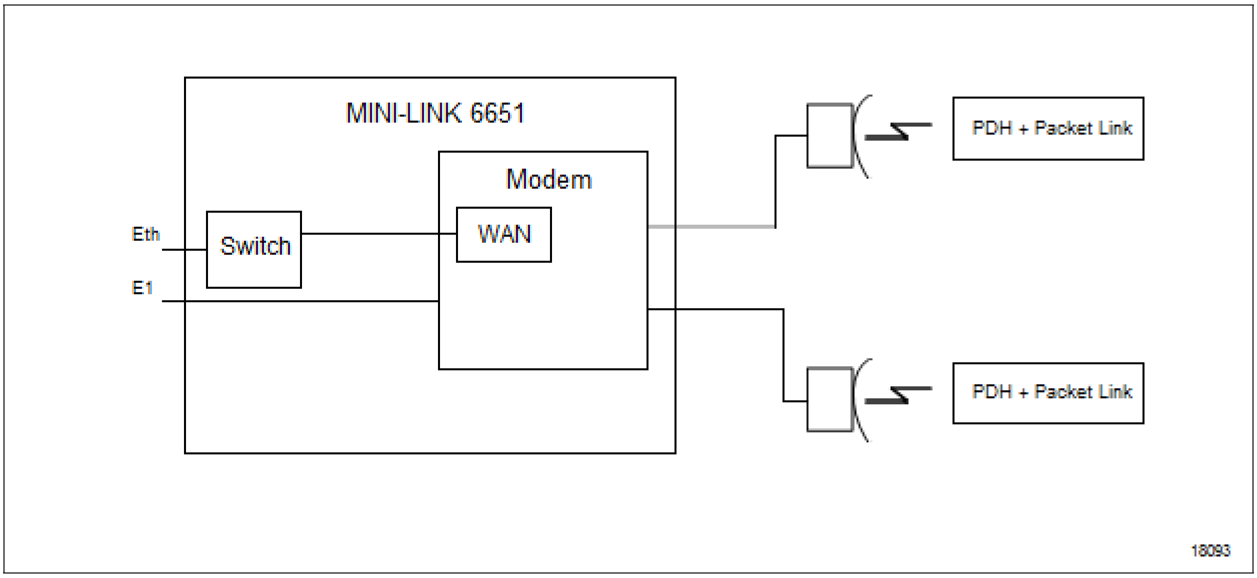


Figure 16 MINI-LINK 6651/1, 6651/2, and 6651/4 Hybrid Radio Link with RLB, Frequency Diversity

## 3.6 Hierarchical Radio Link Bonding

Hierarchical Radio Link Bonding (RLB) requires a license.

Hierarchical Radio Link Bonding (hRLB) is a Layer 1 technology which is used for bonding separately configured RLBs into one hRLB interface to achieve a higher radio link capacity. It can also be used for bonding an E-Band radio link with a traditional RLB.

hRLB requires a dedicated resource. MINI-LINK 6651/4 supports hRLB as it is a stand-alone product. In case of NPU1005, RLBs are configured separately on the MMU and the hRLB interface is configured on the NPU.

Different configurations are available for the MINI-LINK 6600 family. For details on supported configurations, see MINI-LINK 6600 R1 Compatibility.

Bonding an E-Band radio link with a traditional RLB creates a Multi-Band Booster scenario and requires a MINI-LINK 6352. The MINI-LINK 6352 can connect to the NPU 1005 directly using a LAN interface or through an ETU 1002. For details on Multi-Band Booster supported hRLB configurations, see MINI-LINK 6600 R1 Compatibility.

## 3.7 Multi-Band Booster

Multi-Band Booster increases the performance of microwave backhaul, and is a tool that can increase network capacity up to tenfold. It supports flexible bonding of different carriers and frequency band combinations. Multi-Band Booster provides more efficient use of diverse backhaul spectrum assets, using higher frequencies over much wider geographical areas.

The main principle for Multi-Band Booster is to use two radio links in different frequency regions, one low frequency region and one high frequency region. Usually, the low frequency region carries also the TDM traffic and the high frequency region carries only Ethernet.

Figure 17 gives examples of multi-band possibilities.

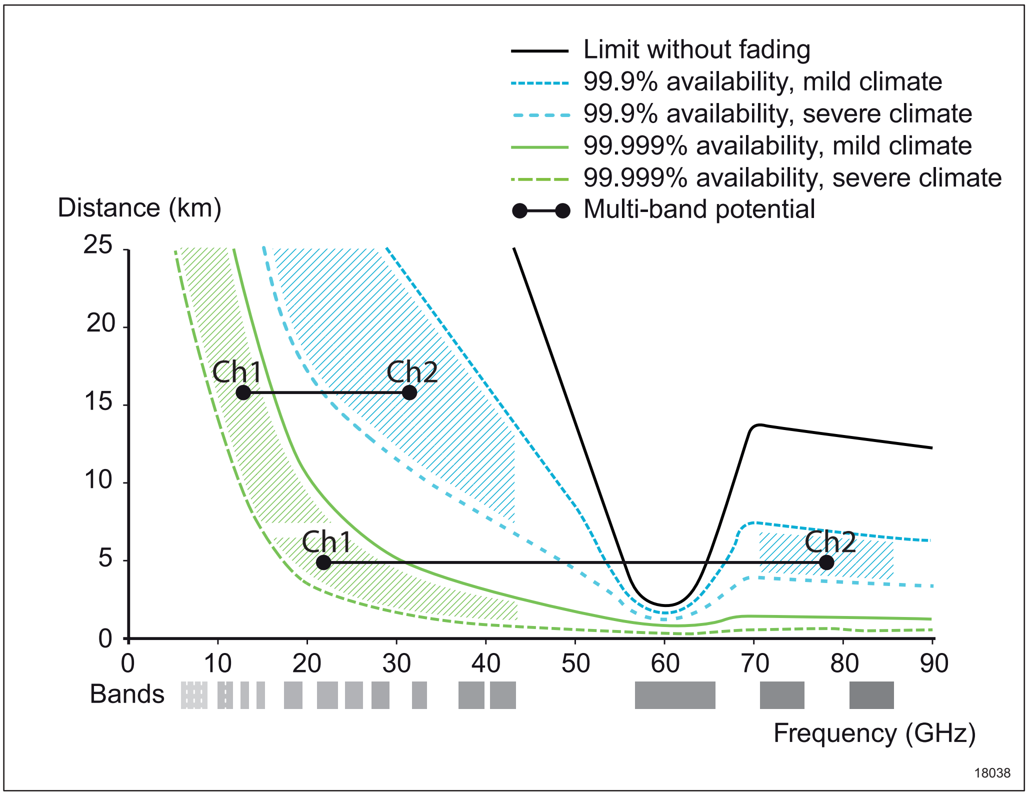


Figure 17 Relevant Distances and Frequency Bands for Multi-Band Booster

The low frequency band is named Ch1, and the high frequency band is named Ch2.

Ch1 – normally the link already in operation – has basic capacity and availability in the range of [99.99 ; 99.999]%. Since Ch1 gives high availability, TDM is transported on Ch1.

Ch2 – the added boosting link – adds high capacity in the range of [99.5 ; 99.95]% availability. This availability target is applicable for the capacity boost needed in non-fading conditions. Since Ch2 gives high capacity, Ethernet is transported on Ch2.

### 3.7.1 Multi-Band Booster with Policy-Based Forwarding

Policy-Based Forwarding is an enhancement to Multi-Band Booster by L1 packet bonding, which enables scheduling of the traffic with priority fields. This enables the user to select higher-priority traffic to be forwarded on trusted, high-availability links with a lower bandwidth and to forward the remaining traffic on higher-bandwidth links with lower availability. Available priority decisions are VLAN PCP, IP DSCP, and MPLS Traffic Class priority values. Forwarding decision can also be made using VLAN IDs in protected and unprotected mode. Protected mode is when the configured link fails, the VLAN is forwarded on the remaining link. In unprotected mode it is not moved to the remaining link. By default PCP values 5 through 7 are mapped to the master interface and 0 through 4 are mapped to the member interface.

Based on the actual usage of a local WAN interface, VLANs can be dynamically allocated to increase local link utilization.

#### Dynamic VLAN Mapping

VLANs forwarded using Policy-Based Forwarding can be measured using automatic VLAN allocation in the L1 bonding configuration page. This enables collection of bandwidth utilization data of the VLANs configured and also the current utilization of the master interface. If the utilization of the master interface is below 60% then whole VLANs are mapped using best fit algorithm to reach 60% utilization. If the link utilization goes above 80% then some of the dynamically mapped traffic is removed from the master interface to go below the 80% threshold. After a VLAN has been moved back then the PBF rules are used to make forwarding decisions.

#### Dynamic PCP Mapping

When using Dynamic Priority Code Point (PCP) Mapping, the bandwidth utilization of the traditional link is measured automatically and traffic is moved to protect high priority traffic and enhance bandwidth utilization. If enabled, bandwidth utilization is measured and PCP mappings are assigned automatically, overriding the manual configuration. Bandwidth measurements are done on the PCP-level and the existing priority values (by default, PCP 5–7 for high-priority traffic and PCP 0–4 for low-priority traffic) are used.

Dynamic allocation can be either PCP-based or VLAN-based. So when Dynamic PCP is used, the dynamic VLAN must be disabled beforehand.

If Dynamic PCP Mapping is enabled, after a 30 seconds measurement period, a mapping action is done based on the gathered utilization data. If the measured utilization of the traditional link is below 60%, traffic with the highest PCP values is moved from the E-Band link to the traditional link until 80% of utilization is achieved. If the measured utilization of the traditional link exceeds 80%, traffic with the lowest PCP values is moved from the traditional link to the E-Band link until the utilization of the traditional link drops to 80%. When the utilization of the traditional link exceeds 80% or if more than 30 seconds have passed since the last mapping action, the 30 seconds measurement period is not needed.

### 3.7.2 Multi-Band Booster with Hierarchical Radio Link Bonding

Bonding an E-Band radio link with a traditional RLB creates a Multi-Band Booster scenario and requires a MINI-LINK 6352 or a MINI-LINK 6651/4. The MINI-LINK 6352 can connect to the NPU 1005 directly using a LAN interface or through an ETU 1002. The MINI-LINK 6651/4 is a non-modular product, that supports two external hRLB groups, bonding the traffic of two MINI-LINK 6352s. The Multi-Band Booster related configurations are described in the Configuring Multi-Band Booster with Hierarchical Radio Link Bonding (hRLB) document in the **Operation and Maintenance** folder.

**Note:** A separate cable is required for DCN connection towards MINI-LINK 6352.

## 3.8 Radio Link Equipment and Propagation Protection

For Ethernet traffic, Ericsson recommend 2+0 Radio Link Bonding (RLB) with graceful degradation meaning that all available bandwidth is used and if one link experience traffic disturbance the capacity goes down to what the corresponding 1+0 configuration can handle. By using 2+0 RLB configurations, all hardware and spectrum is utilized to its maximum in normal case. It is important to note that it requires some configuration on QoS to decide which traffic gets priority in case of link failure.

For TDM traffic (E1/DS1 or STM-1) that needs high availability (that is, high capacity links or critical links for other parts of the network), 1+1 Radio Link Protection (RLP) configurations are recommended when using a limited spectrum, and 2+0 RLB configurations are recommended when fully utilizing spectrum.

The drawback with 1+1 RLP configurations is that they always have a higher cost than 1+0, by using redundant hardware or diversity installation.

The drawback with 2+0 RLB configurations is that they always consume more bandwidth than 1+0, since the basic idea is to transport traffic over more than one path.

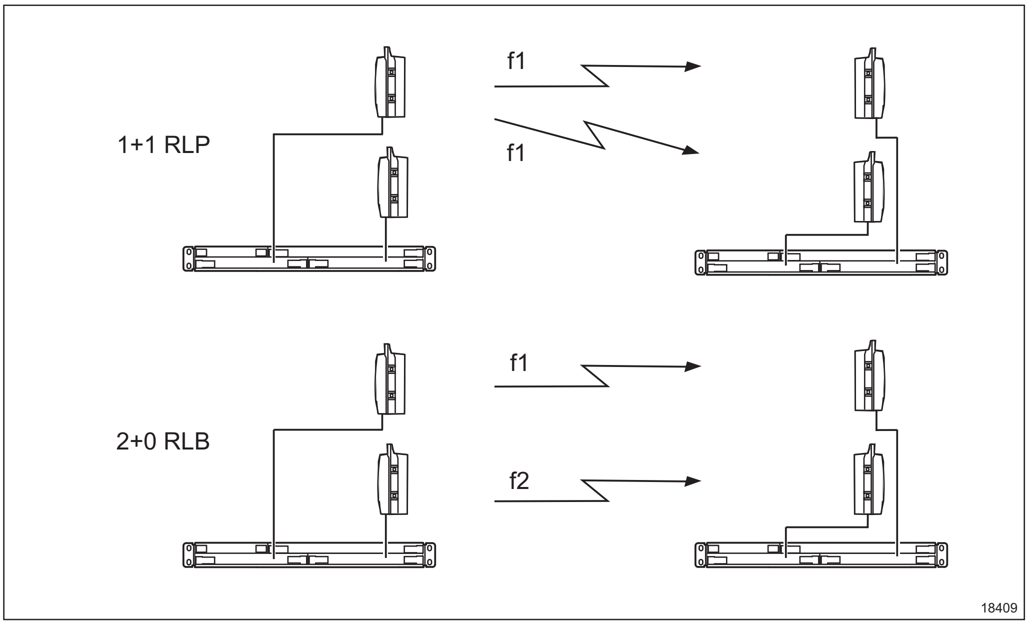


Figure 18 Radio Link Protection Modes

How to choose the optimal configuration is dependent of availability requirements, performance needed by the specific hop situation (hop length, rain zones, fading situation, installation cost, site rent) as well as obtaining a cost-efficient solution.

When planning and configuring this, it is important to consider all means of link utilization and protection, for example RLB (see Section 3.5 on page 18) and Cross Polarization Interference Canceller (XPIC) (see Section 3.9 on page 28).

There are three major protection methods:

- Equipment Protection
  - Tx Equipment Protection
  - Rx Equipment Protection
- Radio Path Protection with Space Diversity
- Radio Path Protection with Frequency Diversity

Equipment Protection may be used on radio links where requirements on availability are high or repair time is assumed to affect the continuation of service.

Radio Path (propagation) Protection may be used on radio links where fading due to meteorological or ground conditions makes it difficult to meet the required transmission quality.

### 3.8.1 One Dual Carrier Modem Configurations

A Radio Terminal with one dual carrier modem (MINI-LINK 6691/6692/6693/6694/6654/6655 with one MMU 1002/1004, MINI-LINK 6651/1, MINI-LINK 6651/2, or MINI-LINK 6651/4) can be configured for the following:

- 1+1 Radio Link Protection (RLP)
- 2+0 Radio Link Bonding (RLB)

#### 3.8.1.1 1+1 Radio Link Protection

1+1 RLP gives the RAU and the antenna equipment protection.

1+1 RLP can be with or without space diversity. When using two antennas, they can be placed for space diversity with a mutual distance where the impact of selective fading (multipath) is reduced. With one (or two co-located) antenna, space diversity cannot be achieved.

**Note:** Space diversity is a counter measure against multipath, and is most efficient for frequencies up to 15 GHz.

1+1 RLP uses hot standby. One transmitter is working while the other one, tuned to the same frequency, is in standby. It is not transmitting but ready to transmit if the active transmitter malfunctions. Both RAUs receive signals.

**Radio Path Protection**

This protection case involves a Diversity selection in each MMU, providing hitless and error free traffic selection in case of radio channel degradation.

The Diversity selection works autonomously and is controlled by the protection logic in the active MMU Rx.

The Diversity selection reacts on quality measures from the two traffic streams. The selection is performed hitless.

### 3.8.1.2 2+0 Radio Link Bonding

2+0 RLB gives the RAU and the antenna graceful degradation.

2+0 RLB can use one or two frequencies. When using two different frequency channels (ACCP) the impact of selective fading (multipath) is reduced. When using one frequency channel (CCDP) XPIC must be used to achieve full performance.

**Note:** Frequency diversity is a counter measure against multipath, and is most efficient for frequencies up to 15 GHz.

2+0 RLB is most spectrum efficient when used together with XPIC (see Section 3.5 on page 18).

## 3.8.2 Two Single or Dual Carrier Modems Configurations

A Radio Terminal with two dual carrier modems (MINI-LINK 6691/6692/6693/6694/6654/6655 with two MMU 1002/1004) can be configured for the following:

- 1+1 Radio Link Protection (RLP) with Equipment Protection (EQP)
- 2+0 Radio Link Bonding (RLB) with EQP
- 4+0 RLB with EQP
- 2+2 RLP with EQP

A Radio Terminal with two single carrier modems (MINI-LINK 6691/6692/6693/6694/6654/6655 with two MMU 1001) can be configured for the following:

- 1+1 Radio Link Protection (RLP) with Equipment Protection (EQP)
- 2+0 Radio Link Bonding (RLB) with EQP

To achieve EQP, the two modems must be positioned in adjacent slots with 2-BPI connection as specified in the installation documents.

**MMU Equipment Protection**

This protection case involves the Ethernet or TDM traffic switching in the backplane. Tx and Rx traffic is switched from active MMU to standby MMU in case of radio link malfunction.

The NPU monitors the alarms generated in the RAU and MMU, and also controls the switches appropriately.

### 3.8.2.1 1+1 RLP with EQP

1+1 RLP with EQP gives the MMU, RAU, and antenna equipment protection.

1+1 RLP with EQP can be with or without space diversity. When using two antennas, they can be placed for space diversity with a mutual distance where the impact of selective fading (multipath) is reduced. With one (or two co-located) antenna, space diversity cannot be achieved.

**Note:** Space diversity is a counter measure against multipath, and is most efficient for frequencies up to 15 GHz.

1+1 RLP with EQP uses hot standby. One transmitter is working while the other one, tuned to the same frequency, is in standby. It is not transmitting but ready to transmit if the active transmitter malfunctions. Both RAUs receive signals.

#### Radio Path Protection

This protection case involves a Diversity selection in each MMU, providing hitless and error free traffic selection in case of radio channel degradation.

The Diversity selection works autonomously and is controlled by the protection logic in the active MMU Rx.

The Diversity selection reacts on quality measures from the two traffic streams. The selection is performed hitless.

### 3.8.2.2 2+0 RLB with EQP

2+0 RLB with EQP gives the MMU equipment protection and the RAU and the antenna graceful degradation.

2+0 RLB with EQP can use one or two frequencies. When using two different frequency channels (ACCP) the impact of selective fading (multipath) is reduced. When using one frequency channel (CCDP), XPIC must be used to achieve full performance.

**Note:** Frequency diversity is a counter measure against multipath, and is most efficient for frequencies up to 15 GHz.

2+0 RLB with EQP is most spectrum efficient when used together with XPIC (see Section 3.5 on page 18).

It is possible to set up a second 2+0 RLB with EQP configuration. Using two dual carrier MMUs, dual Radio Link Bonding can be achieved.

### 3.8.2.3 4+0 RLB with EQP

4+0 RLB with EQP gives the MMU equipment protection and the RAU and the antenna graceful degradation.

4+0 RLB with EQP with 2×MMU 1002/1004s is an efficient way to achieve high capacity with graceful degradation as well as EQP.

4+0 RLB EQP can use one, two, or four frequencies. When using four different frequency channels (ACCP) the impact of selective fading (multipath) is reduced. When using two frequency channel (CCDP), XPIC must be used to achieve full performance. When using one frequency channel (spatial CCDP), Multiple-Input Multiple-Output (MIMO) must be used to achieve full performance.

**Note:** Frequency diversity is a counter measure against multipath, and is most efficient for frequencies up to 15 GHz.

4+0 RLB with EQP is more spectrum-efficient when used together with XPIC (see Section 3.5 on page 18).

4+0 RLB with EQP is the most spectrum-efficient when used together with MIMO (see Section 3.10 on page 32).

4+0 RLB EQP with MIMO uses the corresponding XPIC licenses.

### 3.8.2.4 2+2 RLP with EQP

2+2 RLP with EQP gives the MMU, RAU, and antenna equipment protection.

2+2 RLP with EQP can use one or two frequencies. When using two different frequency channels (ACCP) the impact of selective fading (multipath) is reduced. When using one frequency channel (CCDP), XPIC must be used to achieve full performance.

2+2 RLP with EQP can be with or without space diversity. When using two antennas, they can be placed for space diversity with a mutual distance where the impact of selective fading (multipath) is reduced. With one (or two co-located) antenna, space diversity cannot be achieved.

**Note:** Space diversity is a counter measure against multipath, and is most efficient for frequencies up to 15 GHz.

2+2 RLP with EQP is most spectrum efficient when used together with XPIC (see Section 3.5 on page 18).

## 3.8.3 1+1 RLP with Asymmetrical Power Splitters

In a 1+1 protection hop with asymmetrical radio paths, revertive switching assures that a switch is made from a path with higher attenuation back to the path with lower attenuation when the path with lower attenuation has been restored. A switch in a 1+1 protection hop could be triggered by, for example, a system restart.

Revertive switching is applicable for 1+1 RLP with asymmetrical power splitters.

**Revertive Switching**

When asymmetrical power splitters (−1 dB and −7 dB) are used in master/slave 1+1 RLP configurations, the active radio normally uses the −1 dB path of the splitter. The active radio remains in this path until a fault on the radio occurs or a manual switch of active radio is done.

If system service is performed, it is possible that the active radio is via the −7 dB path after a manual functional test of the system has been performed. In this scenario the system gain is decreased by 12 dB (6 dB on each side of the hop).

The same scenario occurs at a DC power off/on if the −7 dB path is chosen for the radio connected to the MMU in the lowest slot, since this MMU is always active at startup. If this setup is done at both near and far end, the total system gain loss is 12 dB (6 dB on each side of the hop).

Revertive Tx Switching makes it possible to manually set the preferred txRadio (txRadio1 or txRadio 2) and thereby avoid a decrease in system gain.

## 3.9 Cross Polarization Interference Canceller (XPIC)

XPIC is used to transmit two radio carriers across the same frequency, increasing the link utilization. XPIC is not a form of protection.

In an XPIC-configuration there is a risk that both receivers lock to the same transmitter. To prevent this, the Carrier-ID is used to uniquely identify each carrier in an XPIC configuration. A Far-end receiver can only lock to a Near-end transmitter with the same Carrier-ID.

Therefore, the Carrier-ID must be set to different values for the horizontal and the vertical polarization, and have identical setting for the same polarization on both sides of the hop according to Figure 19.

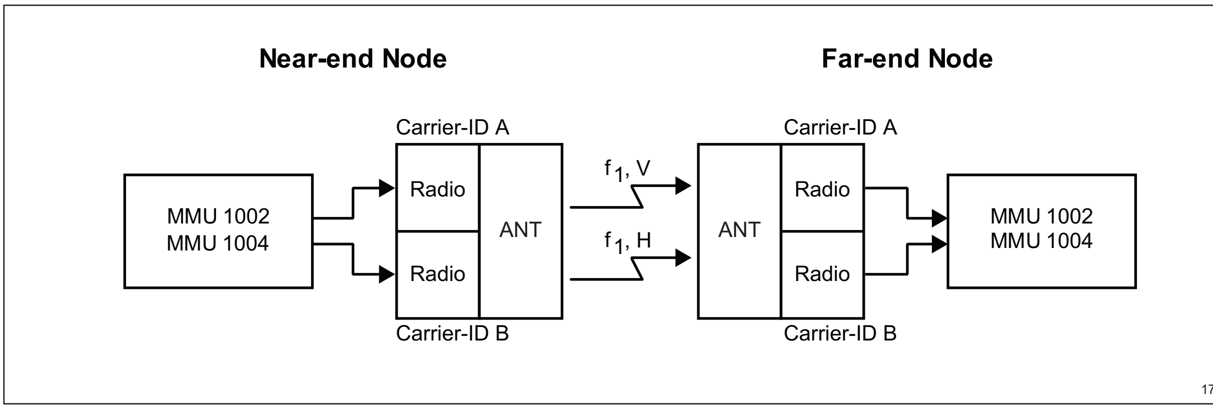


Figure 19 Carrier-ID for XPIC

It is recommended to use one dual-polarized antenna instead of two single-polarized antennas.

### 3.9.1 XPIC Recovery and Restore

When a fault at the receiver of one Carrier Termination (CT), for example H-pol, prevents the received signal to be sent to the other polarization, V-pol, then XPIC of the V-pol CT cannot recover the V-pol original signal. This means that both H and V links are unavailable in the direction toward the faulty receiver, even if only the H-pol receiver is faulty.

XPIC Recovery is the corrective procedure to recover the data traffic on the faultless channel, and must be enabled by the user.

XPIC Recovery is triggered either by user actions or by faults, and consists of the following:

- Switching off the two transmitters of the faulty CT.
- Disabling the four XPIC cancellers, both near-end and far-end.

XPIC Restore is the procedure to re-configure XPIC on both channels.

Considering the example above, once the recovery procedure is triggered no cross-polar interference from H-pol to V-pol link is generated and the traffic over the faultless radio channel (V-pol link) is error free. After the fault has been repaired, the restore is triggered, either manually or automatically.

XPIC Restore consists of re-enabling all XPIC cancellers and turning all transmitters on. Both cross-polar links (H- and V-pol) are fully recovered and traffic is error free.

### 3.9.2 2+0 RLB with XPIC Configuration

The 2+0 RLB with XPIC Radio Link configuration consists of the following equipment on one side of the hop:

- One 1002/1004 (MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655)

  or

  One MINI-LINK 6651/1, one MINI-LINK 6651/2, or MINI-LINK 6651/4
- Two radios
- One integrated dual-polarized antenna

It is possible to use Adaptive Modulation in this configuration.

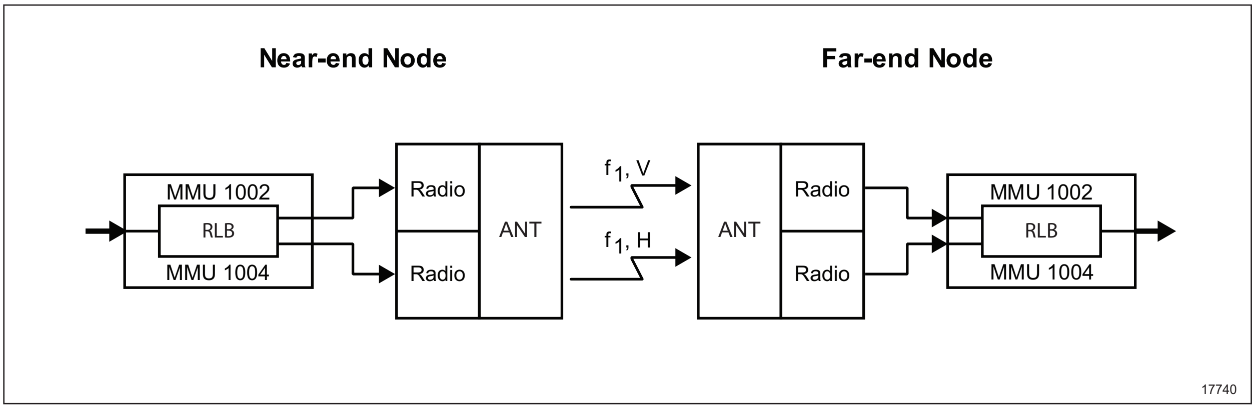


Figure 20

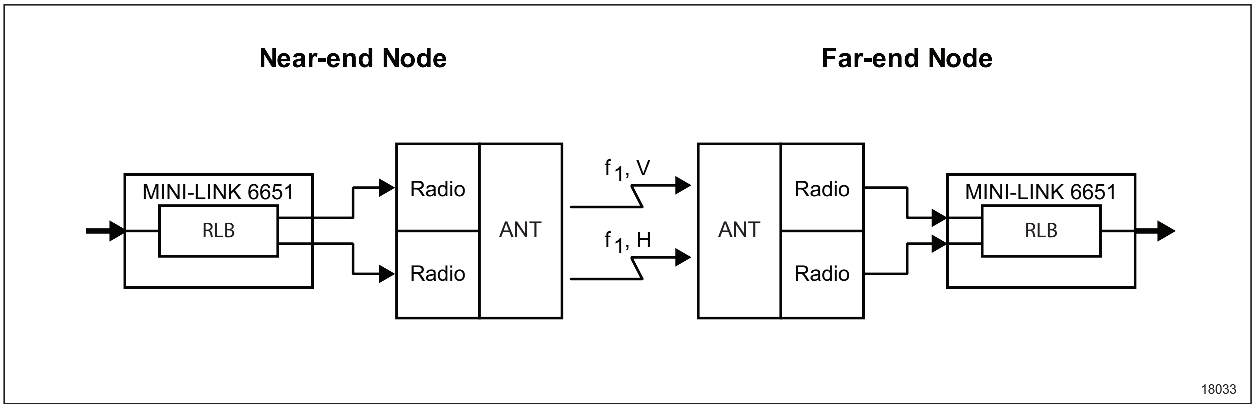


Figure 21 2+0 RLB with XPIC Configuration with MINI-LINK 6651/1, MINI-LINK 6651/2, or MINI-LINK 6651/4

Figure 20 and Figure 21 show only one direction of transmission (from left to right), but the transmission is symmetrical in both directions.

No XPIC cross-cable is needed, since the connection is done internally.

### 3.9.3 Dual (1+0) with XPIC Configuration

The dual (1+0) with XPIC Radio Link configuration consists of the following equipment on one side of the hop:

— One MMU 1002/1004 (MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655)

  or

  One MINI-LINK 6651/2 or one MINI-LINK 6651/4

— Two radios

— One integrated dual-polarized antenna

It is possible to use Adaptive Modulation in this configuration.

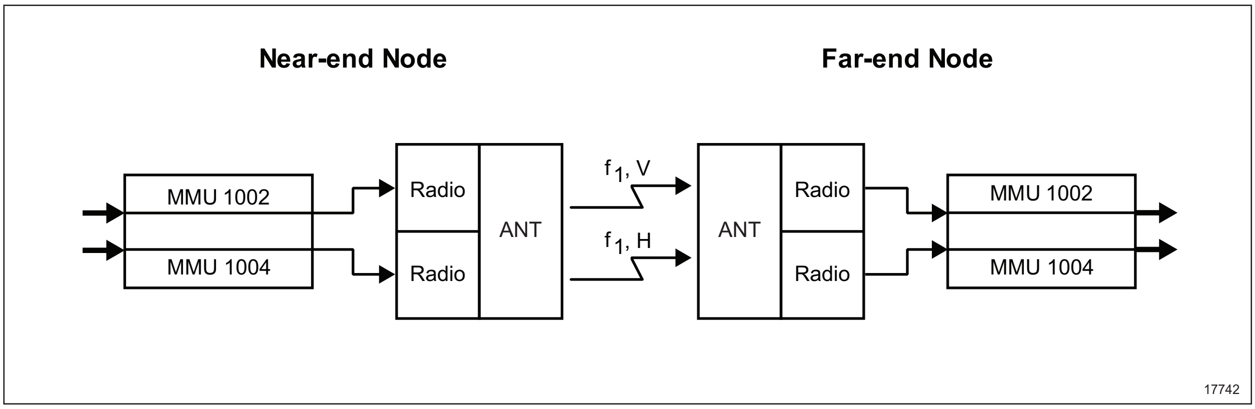


Figure 22 Dual (1+0) with XPIC Configuration with MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655

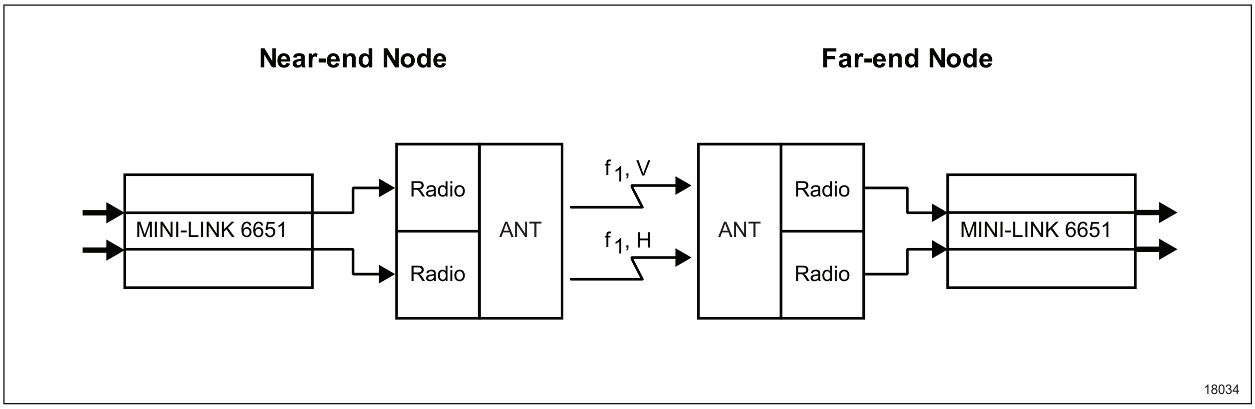


Figure 23 Dual (1+0) with XPIC Configuration with MINI-LINK 6651/2 or MINI-LINK 6651/4

Figure 22 and Figure 23 show only one direction of transmission (from left to right), but the transmission is symmetrical in both directions.

No XPIC cross-cable is needed, since the connection is done internally.

### 3.9.4 2+0 RLB EQP with XPIC Configuration

The 2+0 RLB EQP with XPIC Radio Link configuration consists of the following equipment on one side of the hop:

- Two MMU 1002/1004s (MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655)

  or

  Two MMU 1001s (MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655)
- Two radios

- One integrated dual-polarized antenna
- XPIC cable

It is possible to use Adaptive Modulation in this configuration.

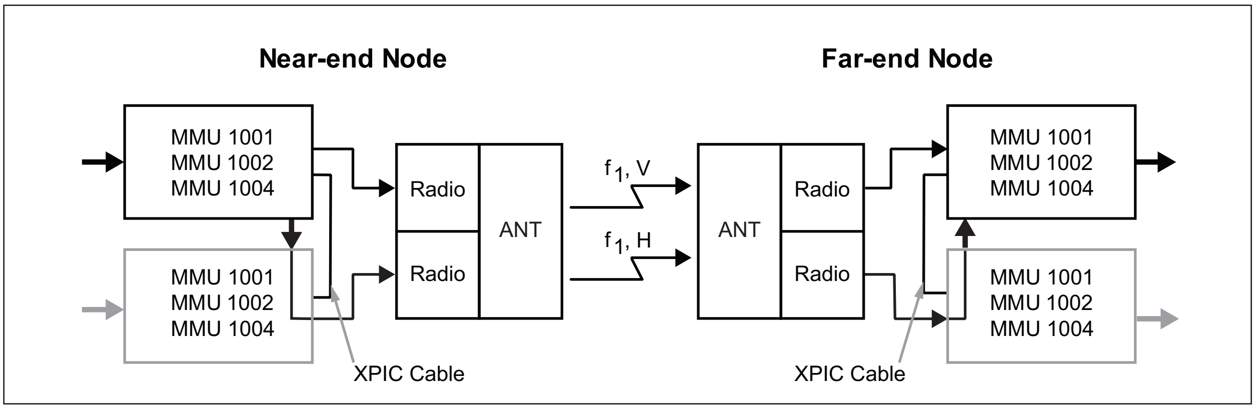


Figure 24 2+0 RLB EQP with XPIC Configuration with MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655

Figure 24 shows only one direction of transmission (from left to right), but the transmission is symmetrical in both directions.

It is possible to set up a second 2+0 RLB EQP with XPIC configuration. Using two MMU 1002/1004s, dual Radio Link Bonding with Equipment Protection and XPIC can be achieved. When configuring two 2+0 RLB EQP links using two adjacent MMU boards, XPIC can be configured on both RLT1 and RLT 2.

## 3.10 Multiple-Input Multiple-Output (MIMO)

Multiple-Input Multiple-Output (MIMO) is a method for increasing the capacity of a radio link using multiple transmission and receiving antennas, to exploit multiple propagation.

In MINI-LINK 6600 products, the support of MIMO increases the spectral efficiency by utilizing the available spectrum with multiple carriers in the same frequency channel.

4x4 MIMO provides up to four times more capacity and uses the combination of the following modes:

- 2x2 spatial MIMO with antenna separation
- 2x2 polarization MIMO with Cross Polarization Interference Canceller (XPIC)

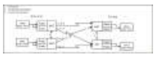


Figure 25 4x4 MIMO

2x2 MIMO provides up to two times more capacity and uses the following mode:

- 2x2 spatial MIMO with antenna separation

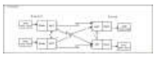


Figure 26 2x2 MIMO

The basis of a fully functional MIMO system is to exchange received baseband information between all involved carriers, for cancellation of the internal co-channel interference. All MMUs must be active in receiving direction, Rx, in order to achieve transmission over the hop. This will limit the EQP function.

When using EQP in a MIMO configuration, switching due to faults in TX direction will lead to graceful degradation and switching due to faults in RX direction may lead to traffic loss.

## 3.11 Multi-Layer Header Compression (MLHC)

Multi-Layer Header Compression (MLHC) improves the efficiency of transportation of Ethernet traffic over Radio Links by compressing Ethernet/MPLS (Layer 2), IP (Layer 3), and UDP (Layer 4) headers. MLHC increases the maximum throughput at WAN interface by reducing the size of the Ethernet frames as they are transmitted over the Radio Link. The size is not configurable as it only depends on the type of header of the Ethernet frame. See Figure 27.

Supported headers:

- Ethernet
    - Untagged frames
    - Customer Bridge
    - Provider Bridge
- MPLS
    - Up to three labels per frame
- IP
    - IPv4
    - IPv6
- UDP

MLHC compresses frames with combinations of the above listed headers. Also, compression of L2VPN and L3VPN are supported.

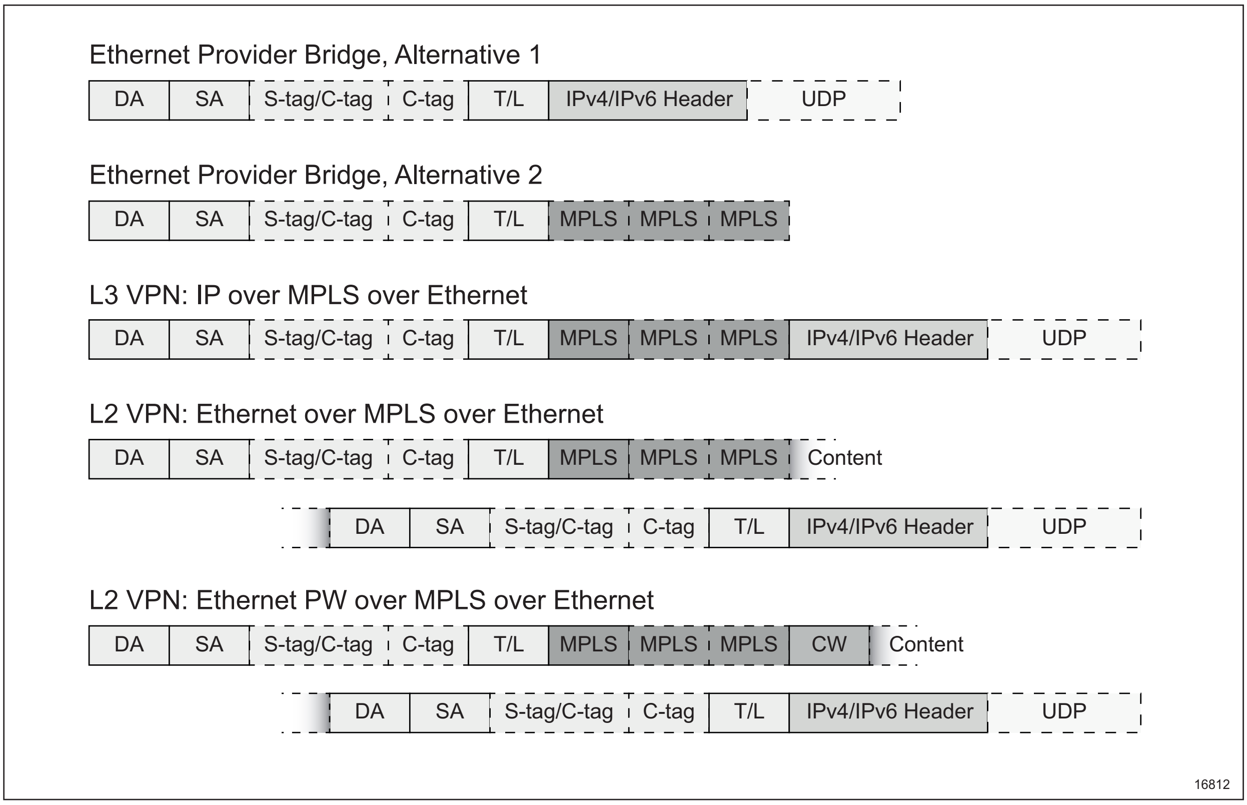

Ethernet Provider Bridge, Alternative 1
DA
SA
S-tag/C-tag
C-tag
T/L
IPv4/IPv6 Header
UDP
Ethernet Provider Bridge, Alternative 2
MPLS
L3 VPN: IP over MPLS over Ethernet
L2 VPN: Ethernet over MPLS over Ethernet
Content
L2 VPN: Ethernet PW over MPLS over Ethernet
CW
16812

Figure 27 Compression of Headers in Different Layers

**Note:** 1588 frames are not compressed.

At each side of the Radio Link there is an MLHC compression pair (one compressor and one decompressor), implementing the header compression functionality. The compressor at one side of the Packet Radio Link sends compressed traffic frames to the corresponding decompressor at the other side of the hop. See Figure 28.

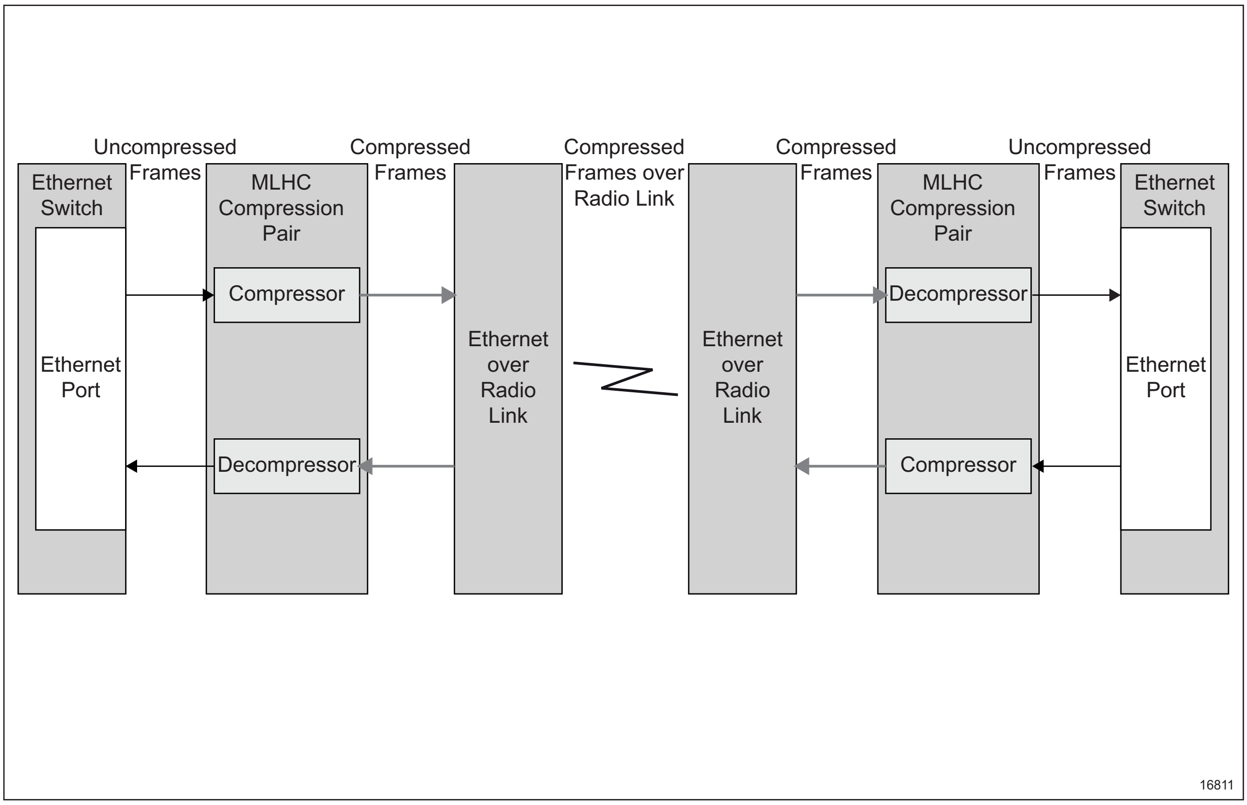


Figure 28 Compression and Decompression Functionality

## 3.12 AES Encryption Over-the-Hop (OTH)

AES encryption over-the-hop (OTH) is a radio link integrity feature. The encryption is to disguise if a radio link is used or not. The encryption is compliant to AES-256-CTR.

**Note:** Encryption is only possible on MMU 1002/1004 configured as 1+0 or 2+0 (on one modem).

Every carrier termination (CT) has two separate session keys for communication over the radio link:

- one for Near End ⇒ Far End
- one for Far End ⇒ Near End

Every CT can therefore be encrypted independently of each other. The Tx and Rx are also encrypted independently of each other.

AES Encryption over-the-hop is controlled by license. The feature is disabled and hidden until the proper licenses are installed on the node.

# 4 Ethernet Overview

MINI-LINK 6600 is targeting multiple applications and network environments with the embedded Ethernet capabilities. MINI-LINK 6600 therefore provides flexibility and supports a large number of Ethernet services and features.

For details on the required HW for specific functions, see MINI-LINK 6600 R1 Compatibility, Reference [1].

## 4.1 Ethernet Services

Ethernet services according to MEF (Metro Ethernet Forum) specifications are supported. The following MEF standards are supported: MEF 2, MEF 9, MEF 10, and MEF 14.

Figure 29 shows a basic model for Ethernet services. The Ethernet service is provided by Metro Ethernet Network (MEN) provider. The Customer Edge (CE) and MEN exchange service frames across the User Network Interface (UNI).

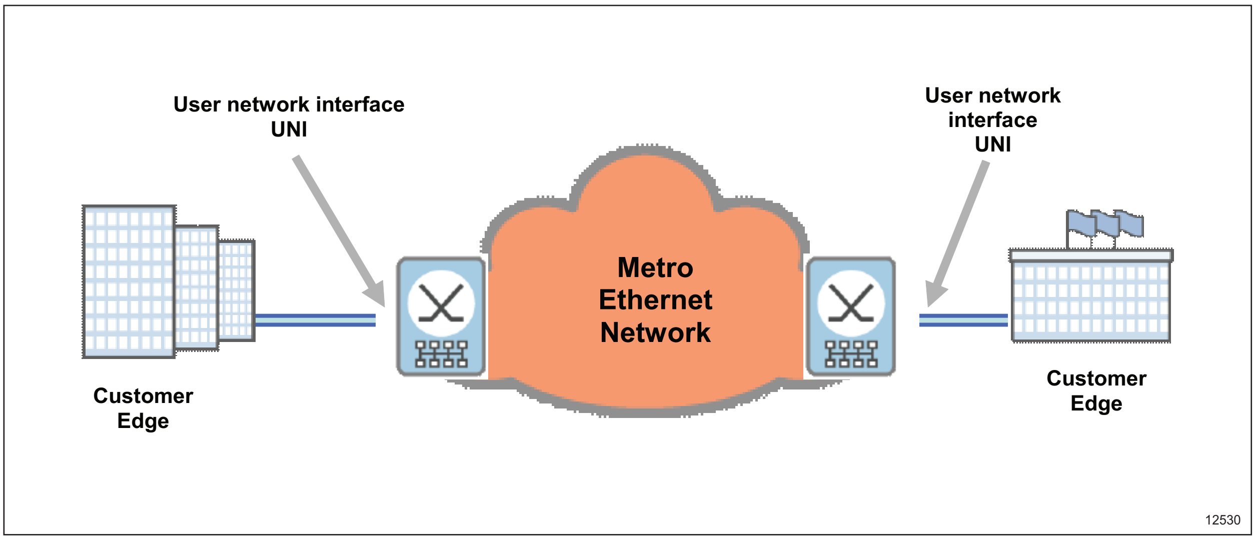


Figure 29 Ethernet Service Model

Based on Ethernet Virtual Connections (EVCs), the following service types are supported:

- Point-to-Point EVC:
  - Ethernet Private Line (EPL) service
  - Ethernet Virtual Private Line (EVPL) service
- Multipoint-to-Multipoint EVC:

- Ethernet Private LAN (EPLAN) service
- Ethernet Virtual Private LAN (EVPLAN) service

# 5 Ethernet Bridging/Switching

MINI-LINK 6600 has an embedded Ethernet bridge that can be configured for customer mode (IEEE802.1Q-2005) or provider mode (IEEE802.1ad-2005). MINI-LINK 6600 also supports a MAC bridge/switch according to IEEE802.1D-2004.

The following features are supported:

- Store and forward switching
- VLAN ID (VID) and priority tagging
- Port-based VLAN (up to 1,000 VLANs in the range of 1–4094)
- MAC address table (32,000 entries)
- Self learning with aging of MAC addresses
- Static L2 Unicast routes
- Static L2 Multicast routes
- Head of line blocking prevention (HOLB)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- Link Aggregation Group (LAG)
- Link Aggregation Control Protocol (LACP)
- SNMP-based management interface, for example, DCN over VLAN
- QinQ
- Many-to-one/All-to-one Mapping for Provider Mode and for QinQ
- Internet Group Management Protocol (IGMP) snooping
- Multicast Listener Discovery (MLD) snooping
- Multiple VLAN configuration

## 5.1 L2 Connectivity Provisioning for Customers over a Provider Network

The provider network functionality enables transport of customer Ethernet traffic over an L2 network. Upon entrance to a service provider network, a Service VLAN tag (S-tag) is added to the Ethernet frame. The S-tag contains the information required to provide a virtual separation of traffic from different customer domains. Once the frame has been transported through the service provider network, the S-tag is removed from the Ethernet frame at the service provider network egress point. In the service provider network it is treated as an ordinary VLAN Ethernet frame.

MINI-LINK 6600 supports the following two types of L2 connectivity provisioning:

- QinQ
- IEEE 802.1ad

For QinQ, the S-tag is similar to the Customer VLAN tag (C-tag) and includes the following:

- Tag Protocol Identifier (0×8100)
- Priority bits (for priority handling in the provider network)
- Drop Eligible Indicator (DEI) bit (for support of color marking).
- S-VLAN ID

QinQ enhances scalability by removing the 1000 VLANs limitation from Customer Mode (IEEE 802.1Q). In this case, the spanning tree of the customer network is proposed to be split into several spanning tree domains. The interconnection between the customer and provider allowed to be a single L2 link and special care of the loop-free L2 topology has to be taken.

For IEEE 802.1ad, the S-tag is similar to the C-tag and includes the following:

- Tag Protocol Identifier (0×88a8)
- Priority bits (for priority handling in the provider network)
- Drop Eligible Indicator (DEI) bit (for support of color marking).
- S-VLAN ID

Provider Bridge enhances scalability by removing the 1000 VLANs limitation from Customer Mode (IEEE 802.1Q) as well as the size limitation of the spanning tree since the number of hops in the service provider network is not a part of the calculation by the customer spanning tree.

MINI-LINK 6600 implements a Provider Edge Bridge which comprises a single S-VLAN component and one or more C-VLAN components.

- Customer Edge Port (CEP): A C-VLAN component Port on a Provider Edge Bridge that is connected to customer owned equipment and receives and transmits frames for a single customer

CEP is an external physical interface. It is a UNI interface and is named CE-UNI in MINI-LINK 6600.

- Customer Network Port (CNP): An S-VLAN component within a Provider Edge Bridge that receives and transmits frame for a single customer.

  A CNP can be an external physical interface, or a virtual internal interface when connected to a Provider Edge Port (PEP). The CNP is a UNI interface, named CN-UNI in MINI-LINK 6600.

- Provider Network Port (PNP): An S-VLAN component Port on a Provider Bridge that transmits and receives frames for multiple customers.

  A PNP is an external physical interface. It is an NNI interface, named I-NNI (PN) in MINI-LINK 6600.

- Provider Edge Port (PEP): A C-VLAN component Port within a Provider Edge Bridge that connects to a Customer Network Port and receives and transmits frames for a single customer.

  The PEP is a virtual internal interface and the port parameters are set to fixed values and can be read from the management system.

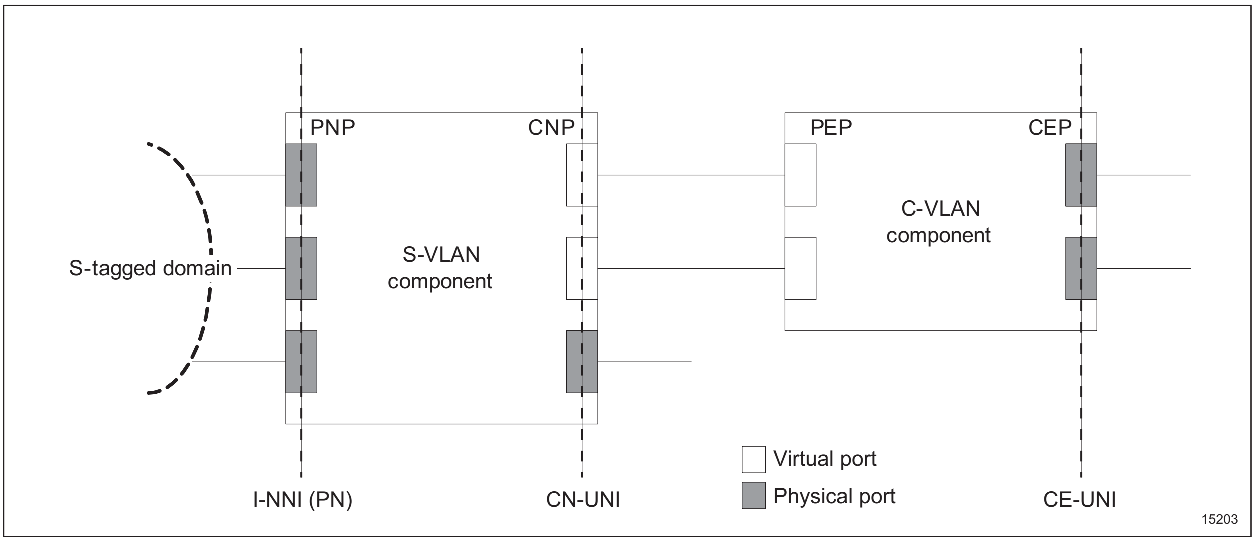


Figure 30 Provider Bridge

## 5.2 Port Roles

Depending on bridge configuration (customer mode or provider mode) different switch port roles are available in MINI-LINK 6600.

UNI and I-NNI port roles are available in customer mode, while Customer Edge UNI (CE-UNI), Customer Network UNI (CN-UNI) and Provider Network NNI (I-NNI (PN)) are available in provider mode.

The UNI ports in customer mode and the CE-UNI and CN-UNI ports in provider mode are the interface between the customer and operator network.

The I-NNI and I-NNI (PN) ports are interfaces used within a transport network. The I-NNI ports in customer mode accept only C-tagged frames while the I-NNI (PN) ports in provider mode only accept S-tagged frames.

For I-NNI ports the TPID can be changed from the default value to the C-VLAN TPID `0x8100`.

## 5.3 Supported Frame Sizes

Ethernet frames of different sizes are common in real networks and the frame size is often related to the application. A real-time application, for example, voice and video, that requires minimum latency typically uses small Ethernet frames, while a data application with non real-time characteristics uses the maximum frame size. MINI-LINK 6600 handles both small and large Ethernet frames as well as a mix.

All ports support 64 to 9,216 byte frame size.

## 5.4 Header Decoding

MINI-LINK 6600 supports header decoding for C-VLANs in customer mode and S-VLANs in provider mode. The EtherType value, also referred to as Tag Protocol Identifier (TPID), for C-VLANs is `0×8100`. For S-VLANs the EtherType value is `0×88a8`.

The EtherType value is unique for the entire network in customer and provider mode, respectively.

## 5.5 Multiple VLAN Configuration

VLAN operations on a range of VLANs are possible, as batch operations are supported.

# 6 Ethernet Security and Admission Control

MINI-LINK 6600 supports multiple security and admission control mechanisms to enable the operator to control the traffic flow into the network individually per port.

The security and admission control features are only available on a port configured as an L2 connection.

## 6.1 Frame Admittance

At the network edge it is possible, with the frame admittance feature, to select which frame types to admit and block. The following frame type options are available:

- Admit Only VLAN Tagged Frames
- Admit Only Untagged and Priority Tagged Frames
- Admit All Frames

The frame admittance settings for bridge ports are specified below.

Customer Mode

- UNI ports: configurable frame types with default value Admit All Frames
- I-NNI ports: non-configurable frame types set to Admit Only VLAN Tagged Frames

Provider Mode

- CE-UNI ports: non-configurable frame types set to Admit All Frames

  **Note:** Tagged frames with EtherType other than `0×8100` are discarded.

- CN-UNI ports: configurable frame types with default value Admit All Frames
- I-NNI (PN) ports: non-configurable frame types set to Admit Only VLAN Tagged Frames

## 6.2 L2CP Frames Processing

MINI-LINK 6600 supports the following filtering behavior of Layer 2 control protocols:

- Discard (IEEE 802.1ad/MEF 10.1)

- Peer (MEF 10.1)
- Forward Unchanged
- Tunneling

The options above are configurable on UNI, CE-UNI, and CN-UNI ports. On I-NNI and I-NNI (PN) ports, the behavior depends on the protocol running in the node.

For all L2CP listed in the tables below, the default behavior on all port types is discard. This is in accordance with IEEE 802.1ad. The alternative behavior for the protocols supported in MINI-LINK 6600 is presented in the tables below.

Table 3 Filtering Behavior of L2CP Protocols on UNI

| **MAC Address** | **Application** | **Tunnelable** | **Optional Configurable Behavior** |
|---|---|---|---|
| 01-80-C2-00-00-00 | Customer Bridge Protocol Data Units (BPDUs) | Yes | Peer if enabled |
| 01-80-C2-00-00-01 | MAC Pause | No | None |
| 01-80-C2-00-00-02 subtype 0x01 | Link Aggregation Control Protocol (LACP) | Yes | Peer if enabled, Forward |
| 01-80-C2-00-00-02 subtype 0x02 | Link Aggregation Marker Protocol (LAMP) | Yes | Peer if enabled, Forward |
| 01-80-C2-00-00-02 subtype 0x03 | Link OAM | Yes | Peer if enabled, Forward |
| 01-80-C2-00-00-02 subtype 0x04–0x09 | Future slow protocols | Yes | None |
| 01-80-C2-00-00-02 subtype 0x0A | Ethernet Synchronization Messaging Channel (ESMC) | No | Peer if enabled(1) |
| 01-80-C2-00-00-03 | 802.1X authentication | Yes | None |
| 01-80-C2-00-00-0D | Provider GVRP | Yes | None |
| 01-80-C2-00-00-0E | Link Layer Discovery Protocol (LLDP) | Yes | Peer if enabled(2) |
| 01-80-C2-00-00-04 | Future standard bridge -04 | Yes | None |
| 01-80-C2-00-00-05 | Future standard bridge -05 | Yes | None |
| 01-80-C2-00-00-06 | Future standard bridge -06 | Yes | None |
| 01-80-C2-00-00-07 | Metro Ethernet Forum ELMI | Yes | None |
| 01-80-C2-00-00-09 | Future standard bridge -09 | Yes | None |
| 01-80-C2-00-00-0A | Future standard bridge -0A | Yes | None |
| 01-80-C2-00-00-0B | Future standard bridge -0B | Yes | None |
| 01-80-C2-00-00-0C | Future standard bridge -0C | Yes | None |

| MAC Address | Application | Tunnelable | Optional Configurable Behavior |
|---|---|---|---|
| `01-80-C2-00-00-10` | All Bridges Protocol | Yes | None |
| `01-80-C2-00-00-20` | GARP Multicast Registration Protocol (GMRP) | Yes | None, Forward |
| `01-80-C2-00-00-21` | GARP VLAN Registration Protocol (GVRP) | Yes | None, Forward |
| `01-80-C2-00-00-2x` (x=2..F) | Generic Attribute Registration Protocol (GARP) | Yes | None, Forward |
| `01-80-C2-00-00-08` | Provider Bridge Protocol Data Units (BPDUs) | Yes | None |
| `01-80-C2-00-00-0F` | Future standard bridge -0F | Yes | None |

(1) Not supported if the interface is an hRLB group interface.

(2) : When LLDP is enabled on a port it is peered regardless of the configured L2CP behavior. The configured L2CP behavior is applied when LLDP is disabled.

Table 4 Filtering Behavior of L2CP Protocols on I-NNI

| MAC Address | Application | Alternative Behavior(1) |
|---|---|---|
| `01-80-C2-00-00-00` | Bridge Group Address (BPDUs) | Peer if enabled |
| `01-80-C2-00-00-02` subtype `0x01` | Link Aggregation Control Protocol (LACP) | Peer if enabled |
| `01-80-C2-00-00-02` subtype `0x02` | Link Aggregation Marker Protocol (LAMP) | Forward unchanged |
| `01-80-C2-00-00-02` subtype `0x03` | Link OAM | Peer if enabled |
| `01-80-C2-00-00-02` subtype `0x0A` | Ethernet Synchronization Messaging Channel (ESMC) | Peer if enabled |
| `01-80-C2-00-00-0E` | Link Layer Discovery Protocol (LLDP) | Peer if enabled |
| `01-80-C2-00-00-0x` (x=1,3..F) | All other C-VLAN component reserved group addresses | None |

(1) Not configurable

Table 5 Filtering Behavior of L2CP Protocols on CE-UNI

| MAC Address | Application | Tunnelable | Optional Configurable Behavior |
|---|---|---|---|
| `01-80-C2-00-00-00` | Customer Bridge Protocol Data Units (BPDUs) | Yes | Forward |
| `01-80-C2-00-00-01` | MAC Pause | No | None |
| `01-80-C2-00-00-02` subtype `0x01` | Link Aggregation Control Protocol (LACP) | Yes | Peer if enabled, Forward |
| `01-80-C2-00-00-02` subtype `0x02` | Link Aggregation Marker Protocol (LAMP) | Yes | Peer if enabled, Forward |
| `01-80-C2-00-00-02` subtype `0x03` | Link OAM | Yes | Peer if enabled, Forward |

| MAC Address | Application | Tunnelable | Optional Configurable Behavior |
|---|---|---|---|
| 01-80-C2-00-00-02 subtype 0x04–0x09 | Future slow protocols | Yes | None |
| 01-80-C2-00-00-02 subtype 0x0A | Ethernet Synchronization Messaging Channel (ESMC) | No | Peer if enabled(1) |
| 01-80-C2-00-00-03 | 802.1X authentication | Yes | None |
| 01-80-C2-00-00-0D | Provider GVRP | Yes | None |
| 01-80-C2-00-00-0E | Link Layer Discovery Protocol (LLDP) | Yes | Peer if enabled(2) |
| 01-80-C2-00-00-04 | Future standard bridge -04 | Yes | None |
| 01-80-C2-00-00-05 | Future standard bridge -05 | Yes | None |
| 01-80-C2-00-00-06 | Future standard bridge -06 | Yes | None |
| 01-80-C2-00-00-07 | Metro Ethernet Forum ELMI | Yes | None |
| 01-80-C2-00-00-09 | Future standard bridge -09 | Yes | None |
| 01-80-C2-00-00-0A | Future standard bridge -0A | Yes | None |
| 01-80-C2-00-00-0B | Future standard bridge -0B | Yes | None |
| 01-80-C2-00-00-0C | Future standard bridge -0C | Yes | None |
| 01-80-C2-00-00-10 | All Bridges Protocol | Yes | None |
| 01-80-C2-00-00-20 | GARP Multicast Registration Protocol (GMRP) | Yes | None, Forward |
| 01-80-C2-00-00-21 | GARP VLAN Registration Protocol (GVRP) | Yes | None, Forward |
| 01-80-C2-00-00-2x (x=2..F) | Generic Attribute Registration Protocol (GARP) | Yes | None, Forward |
| 01-80-C2-00-00-08 | Provider Bridge Protocol Data Units (BPDUs) | Yes | None |
| 01-80-C2-00-00-0F | Future standard bridge -0F | Yes | None |

(1) Not supported if the interface is an hRLB group interface.

(2) : When LLDP is enabled on a port it is peered regardless of the configured L2CP behavior. The configured L2CP behavior is applied when LLDP is disabled.

Table 6 Filtering Behavior of L2CP Protocols on CN-UNI

| MAC Address | Application | Tunnelable | Optional Configurable Behavior |
|---|---|---|---|
| 01-80-C2-00-00-00 | Customer Bridge Protocol Data Units (BPDUs) | Yes | Forward |

| MAC Address | Application | Tunnelable | Optional Configurable Behavior |
|---|---|---|---|
| `01-80-C2-00-00-01` | MAC Pause | No | None |
| `01-80-C2-00-00-02` subtype `0x01` | Link Aggregation Control Protocol (LACP) | Yes | Peer if enabled, Forward |
| `01-80-C2-00-00-02` subtype `0x02` | Link Aggregation Marker Protocol (LAMP) | Yes | Peer if enabled, Forward |
| `01-80-C2-00-00-02` subtype `0x03` | Link OAM | Yes | Peer if enabled, Forward |
| `01-80-C2-00-00-02` subtype `0x04–0x09` | Future slow protocols | Yes | None |
| `01-80-C2-00-00-02` subtype `0x0A` | Ethernet Synchronization Messaging Channel (ESMC) | No | Peer if enabled(1) |
| `01-80-C2-00-00-03` | 802.1X authentication | Yes | None |
| `01-80-C2-00-00-0D` | Provider GVRP | Yes | None |
| `01-80-C2-00-00-0E` | Link Layer Discovery Protocol (LLDP) | Yes | Peer if enabled(2) |
| `01-80-C2-00-00-04` | Future standard bridge -04 | Yes | None |
| `01-80-C2-00-00-05` | Future standard bridge -05 | Yes | None |
| `01-80-C2-00-00-06` | Future standard bridge -06 | Yes | None |
| `01-80-C2-00-00-07` | Metro Ethernet Forum ELMI | Yes | Nonev |
| `01-80-C2-00-00-09` | Future standard bridge -09 | Yes | None |
| `01-80-C2-00-00-0A` | Future standard bridge -0A | Yes | None |
| `01-80-C2-00-00-0B` | Future standard bridge -0B | Yes | None |
| `01-80-C2-00-00-0C` | Future standard bridge -0C | Yes | None |
| `01-80-C2-00-00-10` | All Bridges Protocol | Yes | None |
| `01-80-C2-00-00-20` | GARP Multicast Registration Protocol (GMRP) | Yes | None, Forward |
| `01-80-C2-00-00-21` | GARP VLAN Registration Protocol (GVRP) | Yes | None, Forward |
| `01-80-C2-00-00-2x` (x=2..F) | Generic Attribute Registration Protocol (GARP) | Yes | None, Forward |

| MAC Address | Application | Tunnelable | Optional Configurable Behavior |
|---|---|---|---|
| 01-80-C2-00-00-08 | Provider Bridge Protocol Data Units (BPDUs) | Yes | Peer if enabled |
| 01-80-C2-00-00-0F | Future standard bridge -0F | Yes | None |

(1) Not supported if the interface is an hRLB group interface.

(2) : When LLDP is enabled on a port it is peered regardless of the configured L2CP behavior. The configured L2CP behavior is applied when LLDP is disabled.

Table 7 Filtering Behavior of L2CP Protocols on I-NNI (PN)

| MAC Address | Application | Alternative Behavior(1) |
|---|---|---|
| 01-80-C2-00-00-02 subtype 0x01 | Link Aggregation Control Protocol (LACP) | Peer if enabled |
| 01-80-C2-00-00-02 subtype 0x02 | Link Aggregation Marker Protocol (LAMP) | Forward unchanged |
| 01-80-C2-00-00-02 subtype 0x03 | Link OAM | Peer if enabled |
| 01-80-C2-00-00-02 subtype 0x0A | Ethernet Synchronization Messaging Channel (ESMC) | Peer if enabled |
| 01-80-C2-00-00-08 | Provider Bridge Group Address | Peer if enabled |
| 01-80-C2-00-00-0E | Link Layer Discovery Protocol (LLDP) | Peer if enabled |
| 01-80-C2-00-00-0x (1,3..7,9..A) | All other S-VLAN component reserved group addresses | None |

(1) Not configurable

### 6.2.1 L2CP Frames Processing on a Layer 1 Ethernet Service

On an L1 Ethernet Service, MINI-LINK 6600 supports the following filtering behavior of L2 control protocols:

- Discard (IEEE 802.1Q/IEEE 802.3/MEF 6.1)
- Peer (MEF 6.1)
- Forward Unchanged

The default and alternative behavior for the protocols supported in MINI-LINK 6600 are presented in Table 8.

Table 8 Filtering Behavior of Reserved Group MAC Addresses.

| MAC Address | Application | Default Behavior | Optional Configurable Behavior |
|---|---|---|---|
| 01-80-C2-00-00-00 | Bridge Group Address (BPDUs) | Forward unchanged | None |
| 01-80-C2-00-00-01 | MAC Pause | Discard | None |
| 01-80-C2-00-00-02 subtype 0x01 | Link Aggregation Control Protocol (LACP) | Discard | Forward unchanged |

| MAC Address | Application | Default Behavior | Optional Configurable Behavior | |
|---|---|---|---|---|
| 01-80-C2-00-00-02 subtype 0x02 | Link Aggregation Marker Protocol (LAMP) | Discard | Forward unchanged | |
| 01-80-C2-00-00-02 subtype 0x03 | Link OAM | Discard | Peer if enabled | Forward unchanged |
| 01-80-C2-00-00-02 subtype 0x04–0x09 | All other slow Protocols multicast address | Forward unchanged | None | |
| 01-80-C2-00-00-02 subtype 0x0A | Ethernet Synchronization Messaging Channel (ESMC) | Discard | Peer if enabled(1) | |
| 01-80-C2-00-00-0E | Link Layer Discovery Protocol (LLDP) | Forward unchanged | Peer if enabled(2) | Discard |
| 01-80-C2-00-00-0x (x=3...F) | All other reserved group addresses | Forward unchanged | None | |

(1) Not supported if the interface is an hRLB group interface.

(2) When LLDP is enabled on a port it is peered regardless of the configured L2CP behavior. The configured L2CP behavior is applied when LLDP is disabled.

## 6.3 White Lists

Individual white lists can be created per port to specify which source MAC addresses MINI-LINK 6600 can accept on a port. Frames with a source MAC address not on the list will be discarded.

## 6.4 Ethernet Loop Detection

Ethernet loop detection is used to detect Layer 2 Ethernet loops in the network by configuring Ethernet loop alarms.

There are two use cases for Ethernet loops:

- Ethernet loop

  The NE itself is part of an Ethernet loop.

- Ethernet external loop

  The NE itself is not part of an Ethernet loop, but is connected to a Layer 2 domain where an Ethernet loop occurs.

There are also two use cases regarding provider and customer relations:

- Provider-only loops

  Can be detected when NNI ports are used.

- Provider-customer loops

The customer has redundant interconnection towards the provider network. Can be detected when both NNI and UNI ports are used.

In case a provider has redundant interconnection towards the customer, it is important to detect loops that can occur over the redundant connection. In such a case, configure also the UNI (CE-UNI or CN-UNI) ports for Ethernet loop detection. When Ethernet loop detection is configured on UNI (CE-UNI or CN-UNI) ports, the customer network receives traffic from outside of the customer network. To receive traffic from outside of the customer network, an agreement is needed between the network provider and the customer.

**Note:** Loop detection can be restricted to search for loops in one or a few VLANs. In this case, only these VLANs will be tested for loops.

It is recommended to use Ethernet loop detection together with storm protection to avoid flooding of the test frames, see Section 6.5 on page 50.

## 6.5 Storm Protection

Broadcast storm protection is a protection mechanism, which prevents that other parts or areas of the network are affected by traffic flooding from unicast, broadcast, or multicast traffic at a very high data rate.

Filters can be activated per port to prevent flooding of unwanted and hostile traffic. Individual filters are used for broadcast, multicast and destination lookup failure traffic. The filters are specified as frames per second. When the limit is reached, additional frames will be discarded until the frame rate is below the specified threshold.

Storm protection can be configured on all Ethernet bridge ports in provider bridge mode and customer bridge mode.

## 6.6 Port Blocking

The port blocking feature prevents forwarding of frames from a given ingress port to one or more egress ports.

## 6.7 MAC Address Learning

If MAC address learning is activated on the node it is possible, from one interface, to flood the learning table. A flooded learning table prevents learning on all other ports. By limiting the MAC addresses per port it is possible to prevent MAC address flooding.

MAC address learning can be disabled on a per port basis or on a per VLAN basis.

# 7 Quality of Service

Quality of Service (QoS) of a network deals with the ability of the network to provide transport services suitable for the applications using the network itself. The Quality of Service support in MINI-LINK 6600 is ensured by classifying packets and handling their transmission through the network according to the classification results of each packet.

The following three main parameters affect the quality of the transmission:

- Packet loss: packets lost in the network.
- Delay: the time it takes for a packet to traverse through the network from sender to receiver.
- Jitter: variation in the delay within the same traffic flow.

The different service types (video, voice, data) have different QoS requirements.

In order to meet the different QoS requirements, QoS implementation is based on priority assignment. This supports a number of different priorities in accordance with the Ethernet or IP priority scheme. Ethernet priority scheme conforms to the IEEE 802.1Q specification and supports up to 8 priority levels usually served in Strict Priority. IP priority scheme relies on a higher number of priority levels served according to their per-hop-behavior defined for DiffServ.

Both priority schemes have traffic classification where each packet is associated to a traffic class (in a small or large set), instead of an individual flow. There is not a single flow, but a set of indistinct flows with the same characteristics. Each system in the network can be configured to differentiate traffic based on the traffic class. Each traffic class can be managed differently to separate the high priority traffic from the low priority traffic.

Different features contribute to provide QoS and allow the system to resolve bottlenecks and to guarantee higher priority traffic with respect to lower. The features are listed below.

- Policing: the policer manages traffic matching a certain level of service (usually a bandwidth value). The feature is applied to make sure a subscriber is using the allowed amount of resources in a network. A policer usually performs a configurable action on non-compliant traffic, for example, discard or de-prioritize.
- Queue Management: queue management operates at queue level. It drops or marks frames entering the queue before the queue is full. Typically, queue management operates with a probabilistic approach, dropping or marking frames depending on the queue usage (or its evaluation) and a drop-probability.

- Traffic Scheduler: the traffic scheduler typically operates at port level on the queues associated to that port. It manages the forwarding of different packets, based on their service class, using queue management and various scheduling algorithms. The scheduler ensures that frame delivery corresponds to the QoS parameters for each flow.

An overview of the execution order for different QoS functions is illustrated in Figure 31.

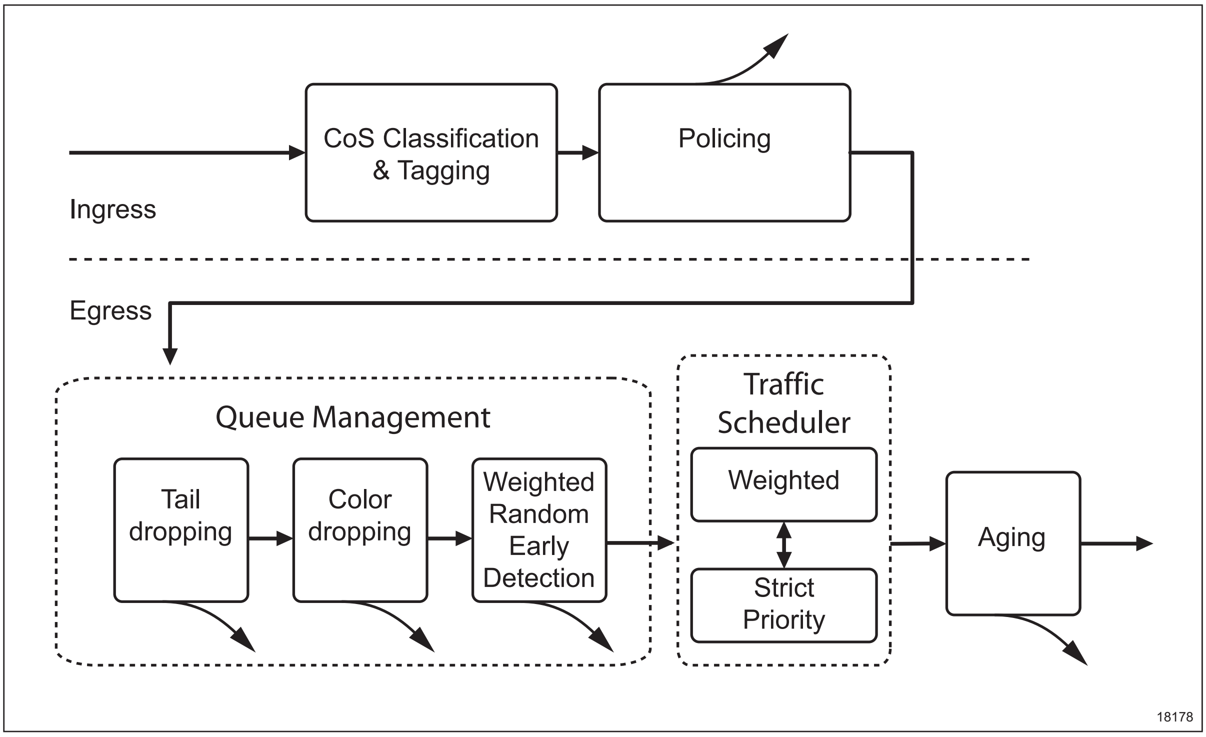


Figure 31 QoS Execution Order

Frames can be dropped at the ingress or egress side by the different QoS functions described in this section.

**Note:** IEEE 802.3x-based congestion handling mechanism does not take into account the usage of different priority levels. The reception of a PAUSE message triggers a network element to halt all Ethernet frames. This means that IEEE 802.3x-based congestion handling is not suitable for networks configured for different priority levels and transmission of real-time traffic.

## 7.1 Classification/Tagging (Ingress)

### 7.1.1 VID Handling

Frames entering UNIs, CN-UNIs, and CE-UNIs are discarded or accepted depending on the information in the frame header and on the parameters set on the port. Before entering the bridge, the frame header can be modified by adding or changing the VLAN tag. The VID is often added to the VLAN tag together with a priority.

VLAN modifications are done if the frame complies with the following conditions:

- The source MAC address of the incoming frame does not belong to the reserved group MAC address
- The format of the incoming frame is supported by the acceptable frame type configured on the port
- The port receiving the frame belongs to the member set of the VLAN carried by the frame (when applicable)

If these conditions are met, the VLAN modifications below are performed.

**Customer Mode**

A UNI is a C-tag aware interface. Incoming C-tagged frames are accepted. Untagged and priority tagged frames are assigned the Port VID (PVID). The PVID is added as a C-tag.

An I-NNI is C-tag aware interface. C-tagged frames are accepted. Non C-tagged frames are always discarded.

**Provider Mode**

A CE-UNI is a C-tag aware interface. Incoming C-tagged frames having the C-VID registered in the C-VID registration table are tagged with the corresponding S-VID.

Incoming C-tag frames not registered in the C-VID registration table are discarded. Untagged and priority tagged frames are assigned the S-VLAN corresponding to the PVID in the C-VID registration table. Any tagged frame with EtherType different than `0×8100` is discarded.

As an external physical interface, a CN-UNI is S-tag aware and C-tag unaware. S-tagged frames are accepted. Incoming C-tagged frames are handled as untagged frames and are assigned the Port VID (PVID). The PVID is added as an S-tag. Untagged and priority tagged frames are assigned the Port VID (PVID).

An I-NNI (PN) is an S-tag aware interface. S-tagged frames are accepted. Non S-tagged frames are always discarded.

### 7.1.2 C-VID Registration Table

CE-UNI ports have a mapping table for C-VLAN and S-VLAN, which is an explicit C-VID registration table that provides mapping between C-VIDs and S-VIDs. The table has an entry for each of the allowed C-VLANs on the CE-UNI port.

When a frame enters a CE-UNI port and carries one of the allowed C-VLANs for the port, the S-VLAN that corresponds to the frame C-VLAN in the table is added to the frame.

In Provider Mode, it is possible to configure a CE-UNI port with characteristics comparable to a CN-UNI port. By configuring a default mapping rule into the C-VID registration table of a port, all C-VLANs can be mapped to an S-VLAN similar to how a CN-UNI port operates. If needed, it is possible to define exceptions from the all-to-one mapping by adding non-default entries to the C-VID registration table.

When untagged or priority-tagged frames enter the CE-UNI port, the entry corresponding to the port default parameter PVID is used to determine which S-VLAN should be added to the frame. If the PVID parameter is set to `0`, incoming untagged and priority tagged frames are dropped (this is the default behavior).

**Note:** The default mapping rule does not apply to untagged and priority tagged frames.

In order to achieve the “default” tagging behavior for untagged and priority tagged frames, a non-default entry has to be created in the C-VID registration table, between any arbitrary C-VLAN ID and the S-VLAN ID also used for the default mapping rule, and the PVID of the port has to be set to this arbitrary C-VLAN ID.

**Example configuration**

PVID=999

| C-VLAN ID | S-VLAN ID | Effect |
|---|---|---|
| 1 | 1 | S-VLAN ID 1 is added to incoming frames with C-VLAN 1 |
| 2 | 1 | S-VLAN ID 1 is added to incoming frames with C-VLAN 2 |
| 3 | 1 | S-VLAN ID 1 is added to incoming frames with C-VLAN 3 |
| 0 | 2 | Default mapping rule: S-VLAN ID 2 is added to incoming frames with any C-VLAN ID except 1, 2, 3 and 999 |
| 999 | 2 | S-VLAN ID 2 is added to incoming frames with C-VLAN ID 999<br>S-VLAN ID 2 is added to incoming untagged and priority tagged frames |

### 7.1.3 QinQ

When operating in customer mode, it is possible to encapsulate IEEE 802.1Q VLANs in other IEEE 802.1Q VLANs (both having TPID `0x8100`), thus enabling the construction of Provider Ethernet networks without equipment supporting IEEE 802.1ad.

The configuration is possible on UNI ports, using the QinQ Termination Table. This table defines a mapping between Customer Edge VLAN IDs (Ce VLAN ID) and Provider Edge VLAN IDs (Pe VLAN ID).

When a frame enters a UNI port with QinQ Termination configured, and carries a VLAN ID defined as Ce VLAN ID in the QinQ Termination Table of the port, an outer IEEE 802.1Q VLAN tag is added to it with the corresponding Pe VLAN ID (this is called selective, or one-to-one mapping).

It is also possible to define a ‘‘default’’ (many-to-one/all-to-one) mapping in the QinQ Termination Table, by creating a mapping entry with Ce VLAN ID 0. If a many-to-one entry is configured in the QinQ Termination Table of the port, an outer IEEE 802.1Q VLAN tag is attached to ingressing frames which carry a VLAN ID not defined as a Ce VLAN ID in the QinQ Termination Table.

If QinQ Termination is configured on a UNI port, the outer VLAN tag is removed (stripped) from outgoing frames if the carried VLAN ID is registered as Pe VLAN ID in the QinQ Termination Table of the port (either for one-to-one or many-to-one mapping).

Ingressing frames with certain C-VLAN IDs can be admitted ‘‘transparently’’, without the addition of a second VLAN tag, even if ‘‘default’’ (many-to-one) mapping is configured in the QinQ Termination Table. This is done by configuring the port as member of these VLANs but not using these VLAN IDs either as Ce VLAN IDs or Pe VLAN IDs when configuring QinQ Termination. Egressing frames carrying these VLAN IDs will be transmitted without removing the (outer) VLAN tag.

**Note:** If a certain VLAN ID is configured as a Pe VLAN ID on a port (either with a one-to-one or many-to-one QinQ Termination mapping), it is not possible to ‘‘transparently’’ admit frames with that VLAN ID. If neither ‘‘default’’ (many-to-one) QinQ Termination mapping, nor a one-to-one QinQ Termination mapping with the certain VLAN ID as Ce VLAN ID is configured, incoming frames with the certain VLAN ID are dropped.

### 7.1.4 Priority Handling (Ingress)

The main objective of the priority classification/tagging process is to establish a frames relative priority to offer appropriate propagation in the network and internally in MINI-LINK 6600.

**Definitions**

Trusted Port

In MINI-LINK 6600 there are different criteria that come into play when a frame is priority tagged. First of all the operator must decide whether the connected user domain is trusted or not. For a trusted domain the operator can reuse the priority information in the frame, set by the client. For an untrusted port the default network priority value is used.

User/Customer and Network Domains

The actual priority of a frame in an end to end Ethernet connection can be different based on where in the network it is. A network can be logically split up in a network domain and one or more user/customer domains. All nodes in an area have a similar congestion behavior. In the user/customer domain, the priority settings of an Ethernet frame are based on the individual user/customer definitions and referred to as user/customer priority. In the network domain the network priority settings, defined by the operator, are used.

User/Customer Priority

The priority setting used in the user/customer domain and set by the user/customer. The user/customer priority information can be retrieved from the user domain frames in one of the following ways:

1. From the PCP bits in the C-VLAN Ethernet header (valid for UNI in customer mode; CE-UNI in provider mode; CN-UNI in provider mode, only if the acceptable frame type of the CN-UNI port is set to Admit Only Untagged and Priority Tagged Frames).

2. From the PCP bits in the S-VLAN Ethernet header (valid for CN-UNI in provider mode).

3. From the IPv4 DSCP bits in the IP header.

4. From the IPv6 DSCP bits in the IP header.

5. In Layer 2 mode, the option DSCP IPv4 and IPv6 makes it possible to use trusting on IPv4 and IPv6 DSCP at the same time.

6. From the EXP bits in the MPLS tag.

7. From both the EXP bits in the MPLS tag and the DSCP bits in the IP header. Primarily the classification in this case is based on MPLS EXP, but in case of non-MPLS traffic, the IP DSCP value is used for prioritization.

Network Priority

The network priority is the Ethernet frame’s priority setting used in the operator/network domain. The different network priority values are defined by the operator.

The network priority of an Ethernet frame is typically a representation of the traffic type and the application generating the Ethernet flow, for example, voice call.

The traffic types and associated priority values are standardized in IEEE 802.1Q and IEEE 802.1D. Each traffic type is associated with a priority value to indicate the relative importance of that traffic type. Highest number equals highest priority.

In a network, it is important that only one set of priority definitions is used, for example, IEEE 802.1D. Otherwise, the handling of Ethernet frames and the mapping to egress queues can differ between network elements. The outcome of this scenario is a non predictable behavior for the different traffic types, for example, voice.

Priority Code Point (PCP)

The Priority Code Point is the three bits in the Ethernet header that is used to carry the priority value and coloring information for the Ethernet frame. The priority information is mandatory while coloring information is only applied when the Ethernet flow is policed.

### Priority Tagging

When a frame enters the network domain (UNI), the user/customer priority settings are either mapped to the operator network priority definitions (trusted interface) or to the default priority setting (untrusted interface). The main purpose of the priority tagging process is to mark a frame with appropriate priority to be used in the network domain, that is, network priority. Priority tagging is only available on a port configured as a Layer 2 connection.

Figure 32 illustrates how the user/customer priority is mapped to the appropriate network priority at the ingress side of MINI-LINK 6600 as a part of the frame tagging process. The network priority value is stored in the PCP bits in the Ethernet header (the possible user/customer priority alternatives are specified earlier in this chapter). For untagged frames and untrusted interfaces the default network priority is used. The network priority value is used as the frame's priority in the CoS/congestion handling mechanisms internally in MINI-LINK 6600. On the egress side of MINI-LINK 6600 the PCP value is encoded from the network priority value and stored in the Ethernet frame's PCP bits. The Ethernet frame is mapped to the appropriate priority/TC buffer.

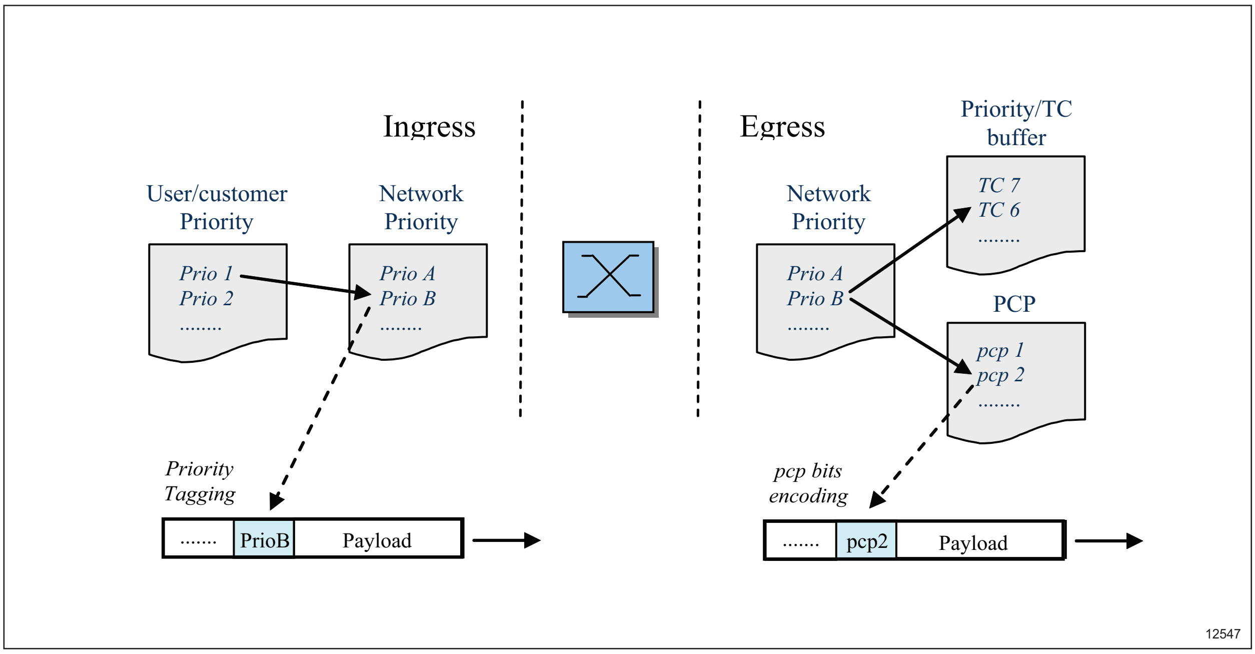


Figure 32 Priority Tagging at Network Edge for Trusted Interface

**Note:** The network priority and PCP value is a 1:1 mapping unless the PCP bits are used to carry coloring information. See Section 7.2 on page 60, for more information.

The flowchart in Figure 33 is used in the tagging process to establish network priority at the network edge.

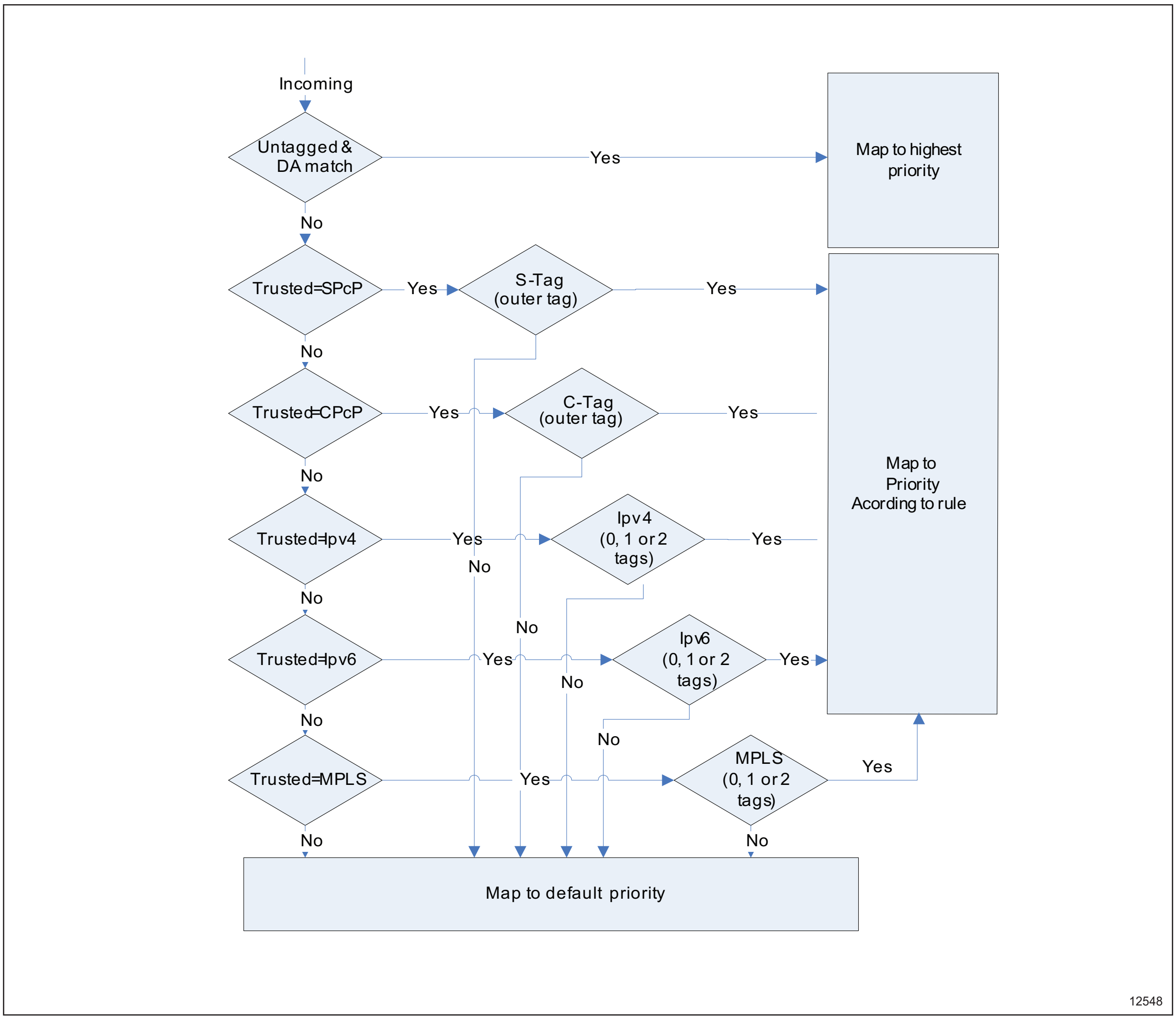


Figure 33 Priority Tagging Flowchart

**Untagged & DA match** test if the frame is untagged and have a destination MAC address belonging to the reserved group MAC addresses. BPDU, Link OAM, MAC Pause all belong to this category.

On a trusted port, the EXP/DSCP priority information in the MPLS/IP header or PCP bits in the Ethernet header is used to establish the network priority. The translation is done according to a mapping table customized by the operator.

**Priority Classification**

Priority classification is done internally in the network domain to decode the network priority value from the PCP bits. The network priority value is used as the priority of the frame in the CoS/congestion handling mechanisms internally in MINI-LINK 6600. On the egress side of MINI-LINK 6600 the PCP value is encoded from the network priority value and stored in the PCP bits in the Ethernet frame. The Ethernet frame is put in the appropriate priority/TC buffer, see Figure 34.

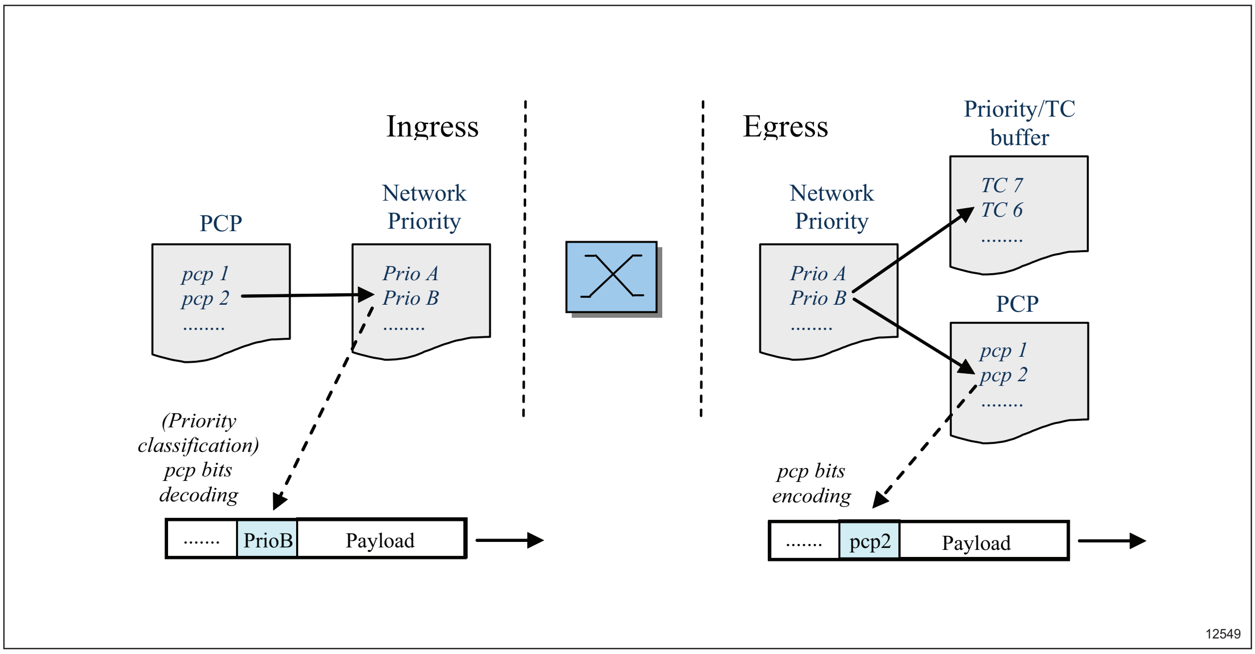


Figure 34 Priority Classification on Internal Network Interfaces

**Note:** The network priority and PCP value is a 1:1 mapping unless the PCP bits are used to carry coloring information. See Section 7.2 on page 60, for more information.

### 7.1.5 Priority Handling Layer 1

The contents and concepts described in Section 7.1.4 on page 55 also apply to L1 Ethernet Services.

In the case of a trusted Layer 1 port, the user/customer priority information can be retrieved from the user domain frames in one of the following ways:

1. From the PCP bits in the C-VLAN Ethernet header.
2. From the PCP bits in the S-VLAN Ethernet header.
3. From the IPv4 DSCP bits in the IP header.
4. From the IPv6 DSCP bits in the IP header.

5. With the option DSCP IPv4 and IPv6 it is possible to use trusting on IPv4 and IPv6 DSCP at the same time.

6. From the EXP bits in the MPLS tag.

7. From both the EXP bits in the MPLS tag and the DSCP bits in the IP header. Primarily the classification in this case is based on MPLS EXP, but in case of non-MPLS traffic, the IP DSCP value is used for prioritization.

**Header Decoding**

L1 Ethernet Service is transparent to all kinds of traffic: untagged traffic; any kind of tagged traffic, including tagged traffic with VLAN ID compliant to IEEE 802.1Q or IEEE 802.1ad.

## 7.2 Policing/Color Marking (Ingress)

At the network edge the policing rate enforcement feature controls the flow into the network. The policing feature can be used to make sure the traffic from an external customer does not violate the specified input rate and burst size. The policing feature in MINI-LINK 6600 is compliant to the ingress Bandwidth Profile functionality specified in MEF 10.1.

In MINI-LINK 6600, policing can be activated either per port or per port per user/customer priority or per port per VLAN. This means that policing rate enforcement can be activated for the consolidated input flow, independent of the traffic types , or individually for each traffic type in the input flow based on either priority or VLAN. The policing feature is only available on a port configured as a Layer 2 connection.

As described later in this chapter, the user/customer priority can be obtained in different ways, for example, DSCP. To select the appropriate Bandwidth Profile (policer) for a flow, the corresponding user/customer priority value is mapped to a user priority group. The user priority group is pointing to the appropriate Bandwidth Profile, see Figure 35.

In case of VLAN based policing, the Bandwidth Profile assignment can be done in a similar way. VLAN IDs can be mapped to a VLAN group, and the Bandwidth Profile can be assigned to the VLAN group.

For policing per port, the port number is directly associated with the Bandwidth Profile.

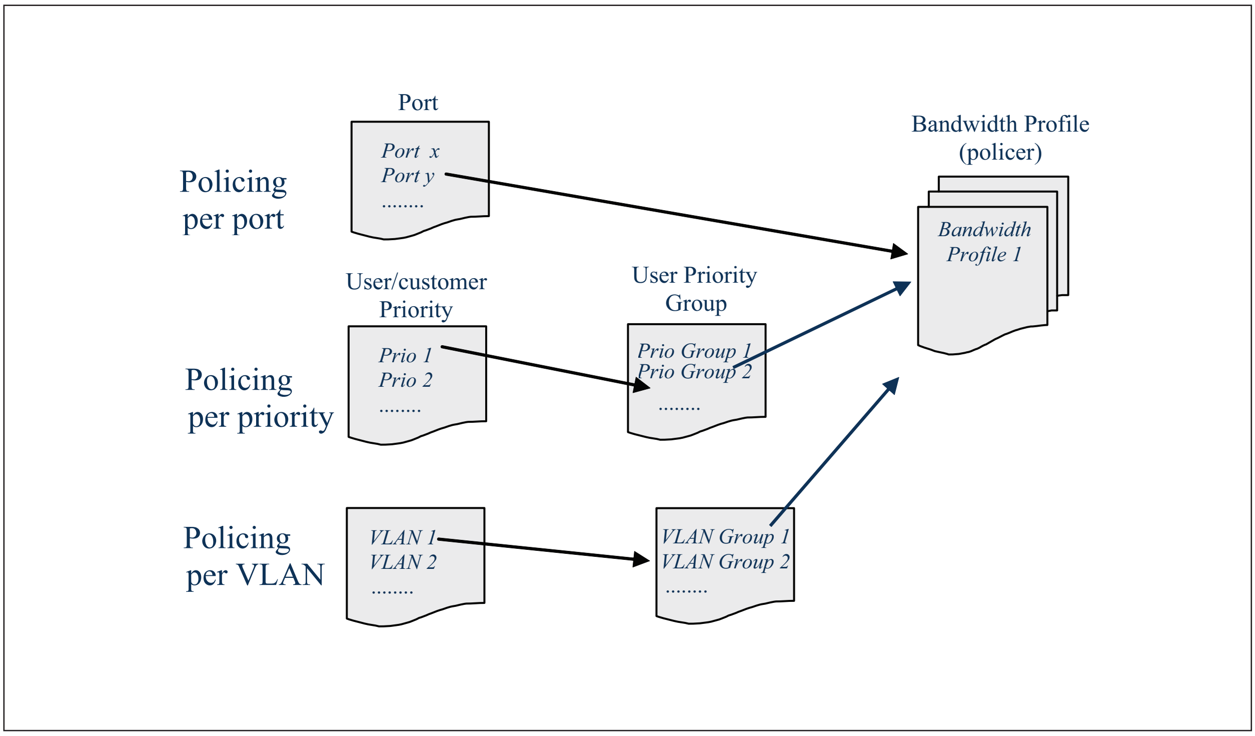


Figure 35 Policing Data Model

The output of the policing function in MINI-LINK 6600 is typically a colored or dropped frame, see Figure 36. The criteria for the deciding whether the frame is colored (green or yellow) or dropped (red) are based on the compliance with the parameters specified below.

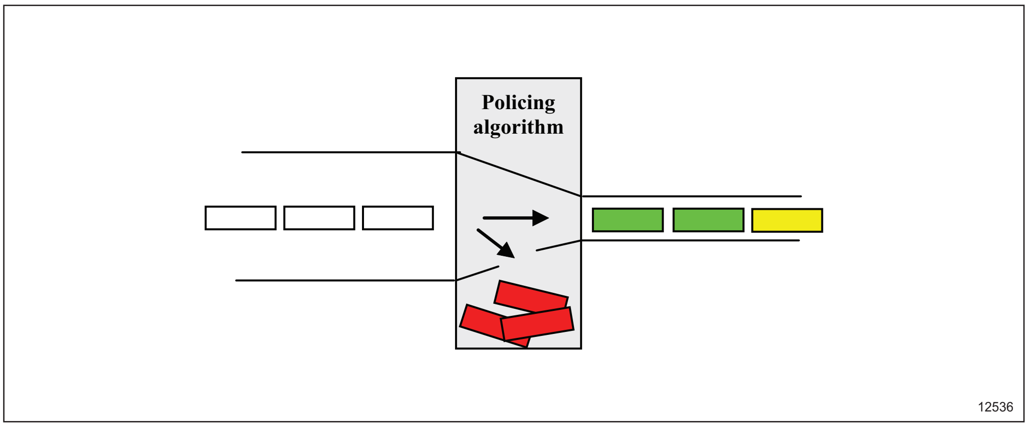


Figure 36 Policing Function in MINI-LINK

By using the policing feature the input flow can be controlled with the following parameters:

— Committed Information Rate (CIR): The CIR value is typically a guaranteed end to end throughput rate, that is, all frames within the CIR value from the external client are propagated transparently with no frame loss. CIR is specified as bps.

- Committed Burst Size (CBS): The CBS value indicates the guaranteed burst length, that is, all frames within the CBS burst length from the external client are propagated transparently with no frame loss. CBS is specified in number of bytes
- Excess Information Rate (EIR): The EIR value is a throughput rate above the CIR committed input rate. Frame rates above the CIR but below EIR are accepted in to the network but with no guarantees. EIR is specified as bps.
- Excess Burst Size (EBS): The EBS value indicates the excess burst length. Burst lengths above the CBS but below the EBS size are accepted in to the network but with no guarantees. EBS is specified in number of bytes.
- Coupling Flag (CF): The CF value controls the volume of the frames that are colored yellow. In MINI-LINK 6600 the CF flag is set to 0, that is, the long term average bit rate of frames declared yellow is bounded by EIR.
- Color mode (CM): The CM value decides whether existing color information in a frame should be used in the policing algorithm or not. In MINI-LINK 6600 the CM is set to Color Blind, that is, existing color information is disregarded in the policing algorithm.

The coloring process uses the above parameters in the following manner to identify the appropriate color for a frame:

- Green frames: Input Rate<CIR and Burst Size<CBS
- Yellow frames: CIR<Input Rate<EIR+CIR and CBS<Burst Size<EBS
- Red frames: Input Rate>EIR or Burst Size>EBS

A graphical presentation of the coloring criteria is illustrated in Figure 37.

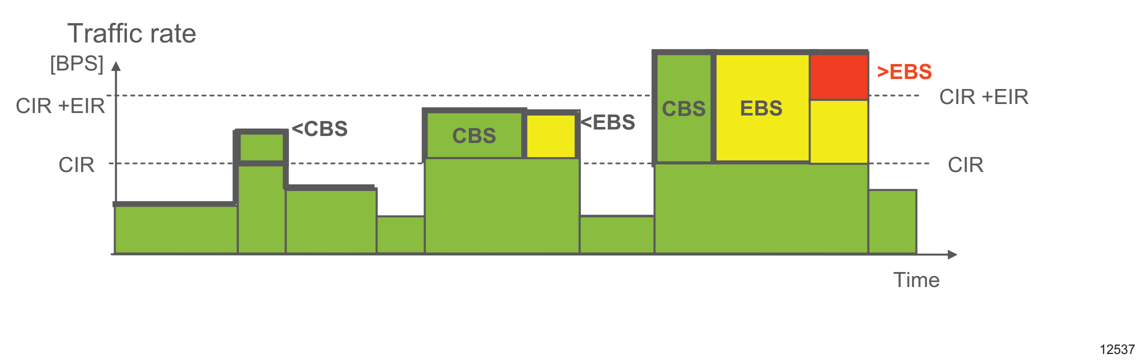


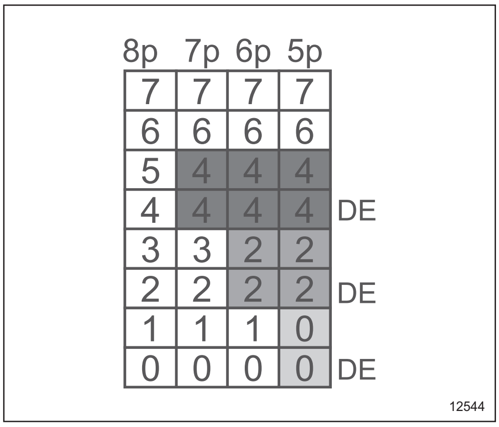
Figure 37 Coloring of Frames in the Policing Function

The color information in a Customer bridge network is transported in the PCP bits in the Q-tag. If policing/coloring is used for a port, the number of priority/TC queues for that port is reduced, that is, some PCP bit values are used for coloring information. For each priority level set up with policing the number of priority/TC queues is reduced by one.

The color information or drop eligibility in a provider network can be either explicitly or implicitly encoded in the S-VLAN tag. Drop eligibility can be encoded with the priority in the PCP field of the S-tag as specified for the C-tag, or it can be encoded explicitly by using the Drop Eligible Indicator (DEI) bit in the S-tag.

The IEEE802.1ad standard defines that PCP allows encoding of five, six, seven, or eight distinct priorities, with a drop eligibility on three, two, one, or zero of those priorities respectively, see Figure 38.

**Note:** Color dropping is not applicable for the two highest priorities, 6 and 7.



| 8p | 7p | 6p | 5p | |
|---|---|---|---|---|
| 7 | 7 | 7 | 7 | |
| 6 | 6 | 6 | 6 | |
| 5 | 4 | 4 | 4 | |
| 4 | 4 | 4 | 4 | DE |
| 3 | 3 | 2 | 2 | |
| 2 | 2 | 2 | 2 | DE |
| 1 | 1 | 1 | 0 | |
| 0 | 0 | 0 | 0 | DE |

Figure 38 PCP Encoding

| | |
|---|---|
| **8p0d** | 8 priorities, 0 priorities with color dropping |
| **7p1d** | 7 priorities, 1 priority with color dropping |
| **6p2d** | 6 priorities, 2 priorities with color dropping |
| **5p3d** | 5 priorities, 3 priorities with color dropping |
| **8p8d** | Only available in Provider mode. Eight priorities, the DEI bit in the S-VLAN tag is used to retrieve or indicate the drop eligibility of frames. |

In Customer mode, coloring is performed at I-NNIs, while the UNIs always operate in 8p0d PCP selection as long as the PCP bits in the C-VLAN tag are trusted.

In Provider mode, coloring is performed at I-NNI (PN)s and CN-UNIs. On I-NNI (PN)s it obeys the selection. CN-UNIs have the following behavior:

- If the PCP value of the incoming frame differs from 8p8d and the PCP bits in the S-VLAN tag are trusted, the PCP value is set to 8p0d.

- If the PCP value of the incoming frame is 8p8d and the PCP bits in the S-VLAN tag are trusted, the PCP value is set to 8p8d.

The CE-UNI always operates in 8p0d PCP selection, if the PCP bits in the C-VLAN tag are trusted.

Coloring can be configured for maximum three priority levels, that is, 5p3d. This means that three out of five priority levels can be color marked. It is possible however to activate policing for the priority levels with no coloring support. These frames will be policed according to CIR/CBS and either dropped or passed through but with no color information applied to the frame.

For a customer interface protected with LAG, policing cannot be activated.

## 7.3 Queue Management

In a multi service network there is a need to differentiate the processing of the different flows in the congestion points. Typically a voice flow would require low latency/jitter and thus higher priority than a best effort data flow with no latency requirements.

Differentiation of flows is done based on the network priority value in the header part of each Ethernet frame. The network priority value to be used in the network domain is typically set as a part of the tagging process at the network edge.

The priority value of a frame is used to provide different Classes of Service (CoS) and is a representation of the end user application, for example, voice, best effort data, and so on. The priority value of an Ethernet frame indicates what type of behavior it expects from the network and how it shall be prioritized with respect to the other Ethernet frames in an interim network element.

An alternative to the mechanisms described in this chapter is to overprovision the network, that is, the capacity is sufficient to guarantee a congestion free network.

### Traffic Class (TC) Mapping

MINI-LINK 6600 supports eight TCs or priority queues for each egress Ethernet port.

The Ethernet frames are mapped to the different TCs based on the network priority value in the PCP bits in the Ethernet header (see Figure 32). The mapping can be done according to IEEE 802.1D, see Figure 39, IEEE 802.1Q, see Figure 40, or it can be customized.

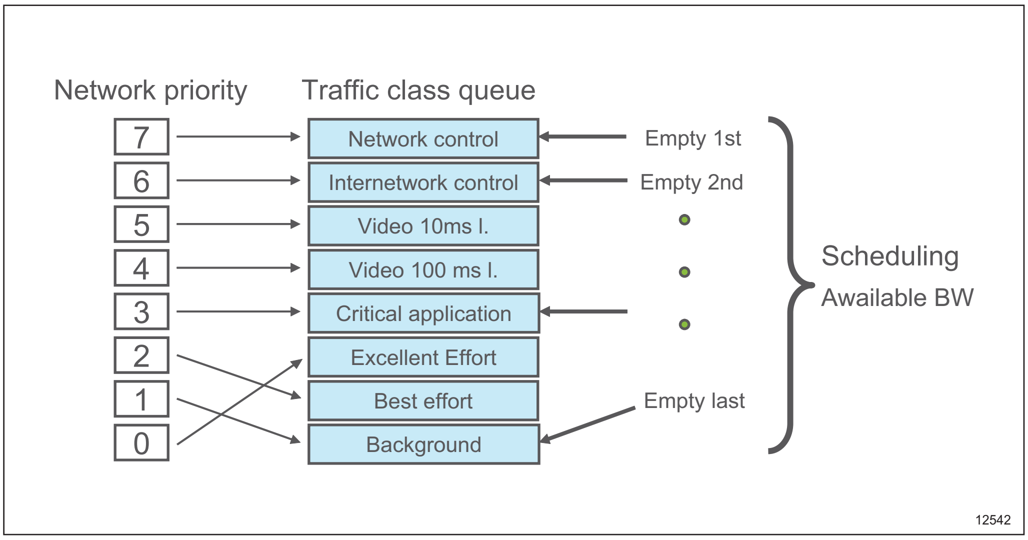


Figure 39 IEEE 802.1D Mapping

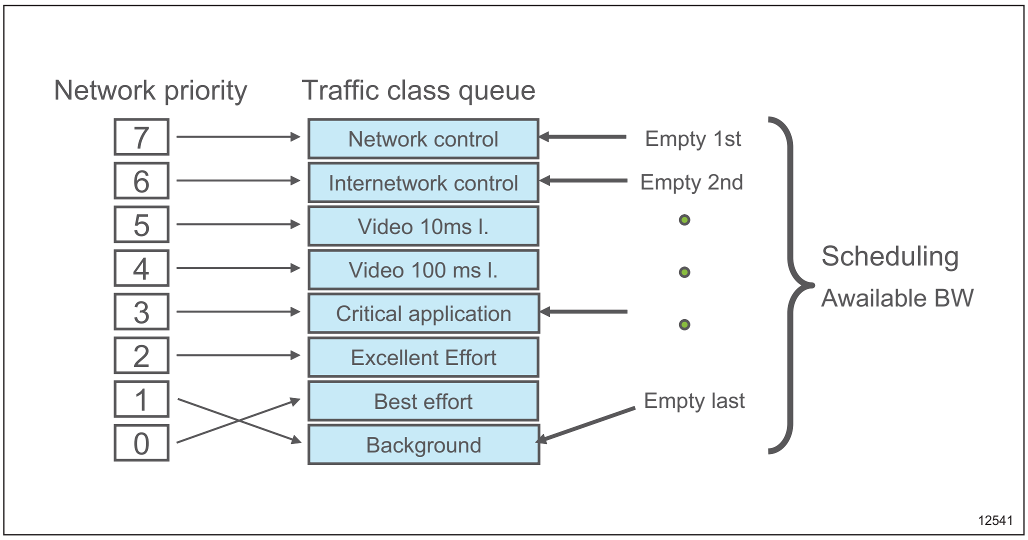


Figure 40 IEEE 802.1Q Mapping

### Shared Packet Buffering

Ethernet interfaces share the available memory, so multiple queues compete for the same buffering resource. A buffer management algorithm is used to efficiently manage the existing buffer resources in fair manner.

A discard threshold for the queues is dynamically calculated based on the size of the remaining buffer space. In a non-congested or relatively uncongested state the remaining buffer space is large, so the queue discard thresholds are set to a higher value which allows better burst absorption. On the other hand, if the remaining buffer space is very small, then the switch is facing severe congestion, therefore queue discard threshold is lower.

A frame is enqueued in the corresponding queue, if the queue length is smaller than the calculated discard threshold. Otherwise the frame is dropped. In congested state the frames attempting to enter the longer queues are more likely to be dropped than frames entering shorter queues since the queue length of the longer queues would be higher than the threshold. Consequently this fair buffer management algorithm aggressively drops frames belonging to longer queues, thereby freeing up resources for queues that are relatively uncongested, see Figure 41.

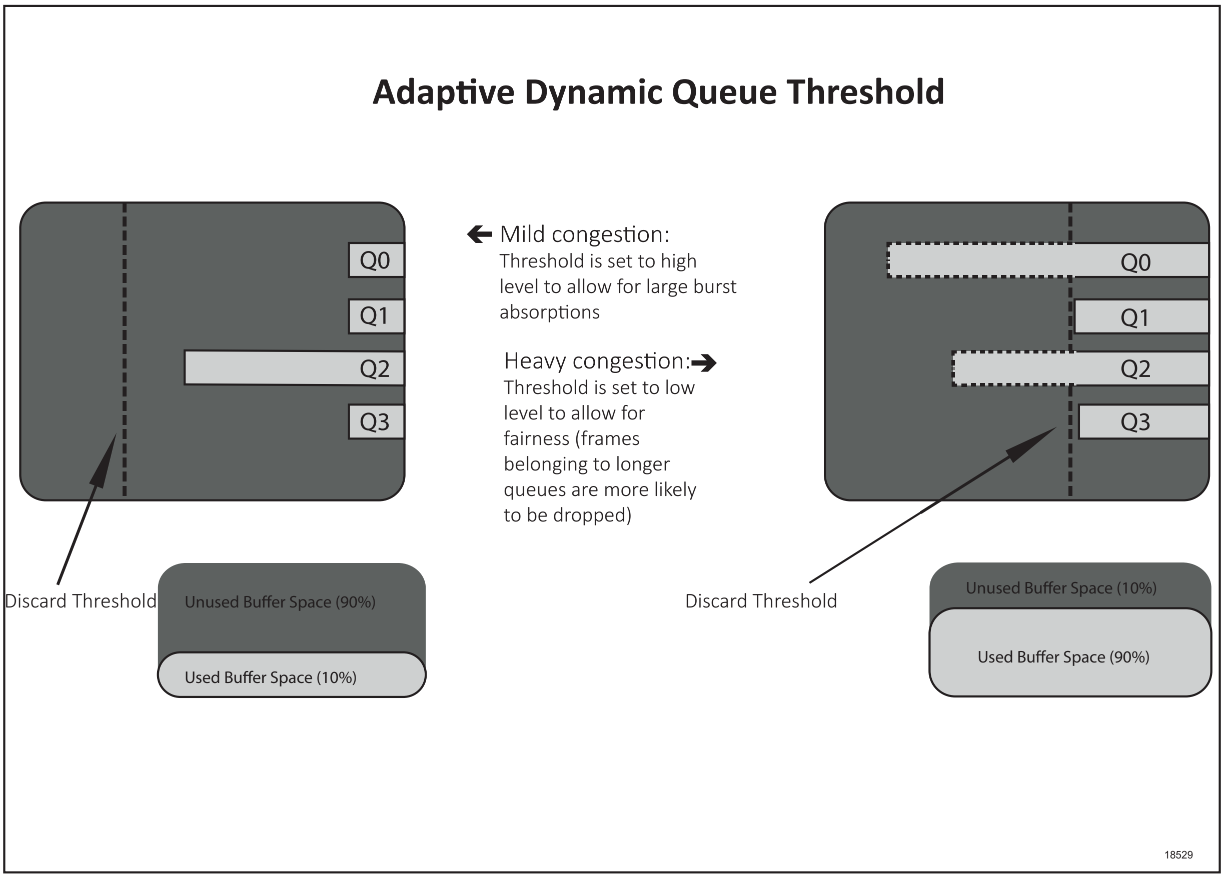

Adaptive Dynamic Queue Threshold
Q0
Q1
Q2
Q3
Mild congestion:
Threshold is set to high level to allow for large burst absorptions
Heavy congestion:
Threshold is set to low level to allow for fairness (frames belonging to longer queues are more likely to be dropped)
Q0
Q1
Q2
Q3
Discard Threshold
Unused Buffer Space (90%)
Used Buffer Space (10%)
Discard Threshold
Unused Buffer Space (10%)
Used Buffer Space (90%)
18529

Figure 41 Adaptive Dynamic Queue Threshold

The recommended way of limiting queue size is either by configuring a user-defined queue size limit for tail-drop or by using WRED.

### Time Stamp-Based Dropping/Aging

A timestamp is applied to the frame when it enters the TC queue buffer. Before exiting the TC buffer (that is, served by the scheduler) the timestamp is checked towards the aging timer. If the timestamp value exceeds limit for aging time from when the frame was stored in the queue, the frame is discarded. The aging time can be adjusted from the management interface based on the PCP priority value of the incoming frame.

**Note:** Aged frames consume egress bandwidth and can cause the transmitted traffic rate to drop below line rate.

### WRED

To give a better understanding of WRED, some basics of the TCP protocol is described first.

The nature of a TCP connection is an increasing bandwidth until frames are lost. When the TCP protocol recognizes frame loss, the throughput is reduced by 50%. TCP then repeats the process by increasing the throughput until frames are lost. The throughput pattern is often referred to as saw tooth shape, see Figure 42.

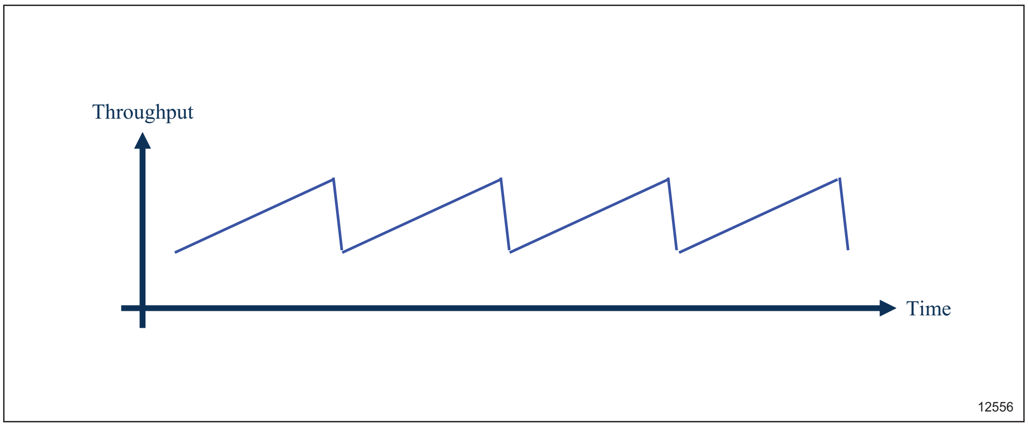


Figure 42 Saw Tooth Shaped TCP Throughput

When multiple TCP flows experience congestion in the same port, all TCP flows loose packets at the same time (tail drop). This means that all TCP flows simultaneously reduce throughput by 50%. The result is a link with low average throughput. With WRED activated, frames are randomly discarded at a configurable buffer filling threshold. This means that tail drop can be avoided and only a limited number of the TCP flows will experience frame loss and reduce the throughput. Thus, WRED can increase the average throughput by minimizing the throughput variations, see Figure 43.

WRED starts discarding frames when the buffer filling has reached a certain configurable threshold. If the buffer filling continues to increase the drop probability increases, see Figure 43. The buffer filling is calculated as an average value, estimated over a certain period of time. This is a more accurate way of measuring buffer than for instance instant measurements.

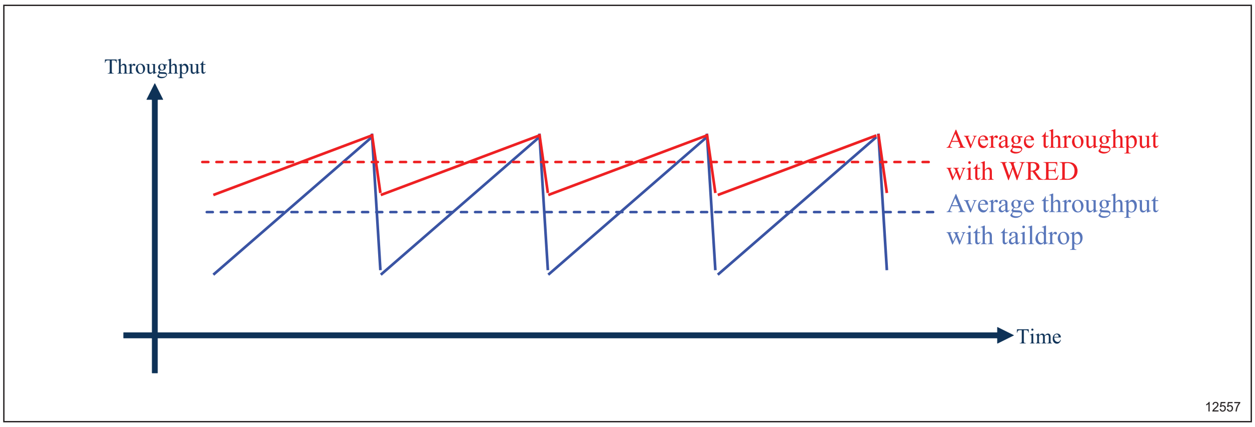


Figure 43 WRED Thresholds

WRED can be enabled on ports with deep buffer.

If Color-aware WRED is used to regulate a queue, then different WRED profiles can be applied for green and yellow traffic.

**Note:** WRED requires buffering, therefore it can only be set on interfaces with enabled deep-buffering.

### Tail Drop

The tail drop discard mechanism is used when a TC buffer reaches the dynamically calculated discard threshold. In this case, the tail drop feature ensures that new frames are dropped at the entry point of the TC queue.

Tail drop is used to handle discarding of frames during long bursts that would completely fill up the available buffer space.

Tail drop queue user-defined size limitation is only effective when deep buffering enabled on the port.

### Frame Discard Summary

Figure 44 illustrates how the different discard mechanisms are organized in MINI-LINK 6600.

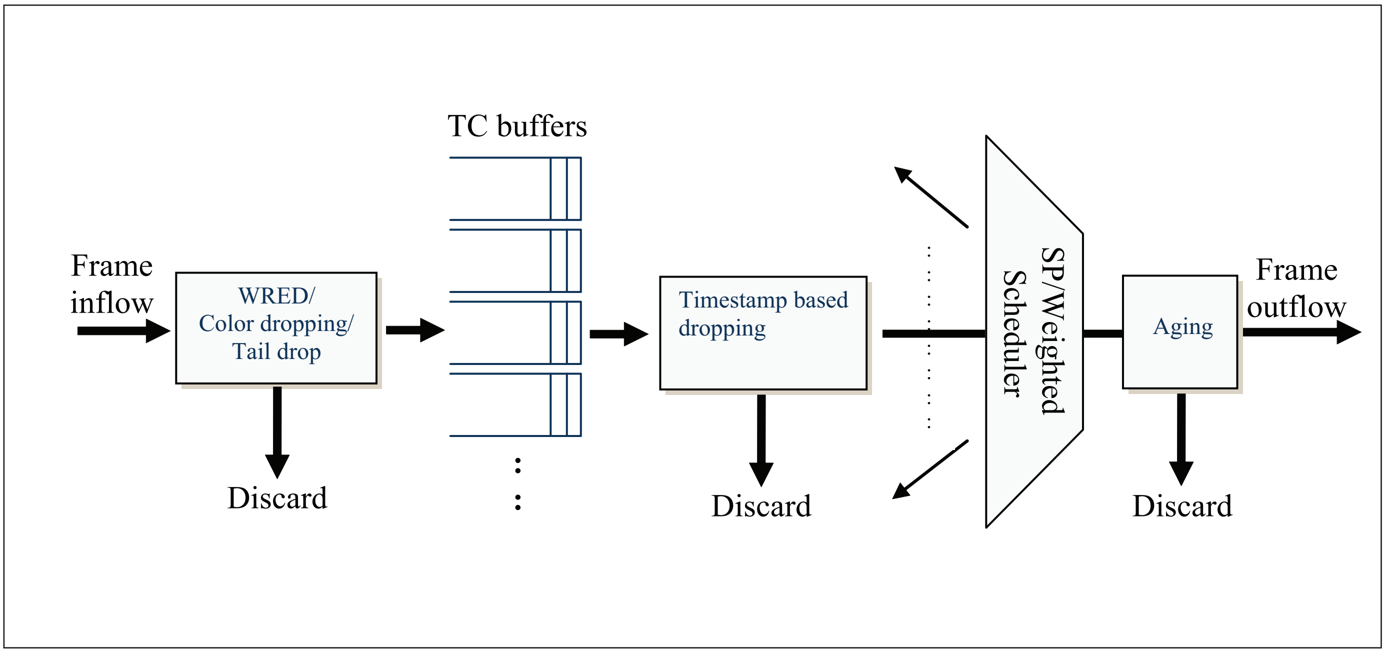


Figure 44 Discard Mechanisms in MINI-LINK

## 7.4 Scheduling (I-NNI and I-NNI (PN))

When an Ethernet port is congested the egress priority/TC buffers are filled up with Ethernet frames. To empty the buffers a scheduler must serve the buffers according to a predefined algorithm. MINI-LINK 6600 supports both Strict Priority (SP) and weighted scheduling algorithms (for example Deficit Weighted Round Robin (DWRR)) to empty the egress priority/TC buffers.

The SP algorithm is typically used for delay sensitive traffic like voice, video and sync packets. With SP, Ethernet frames in the buffer with the highest priority are always scheduled first, for example, all Ethernet frames with priority level 7 are scheduled before Ethernet frames with priority level 6.

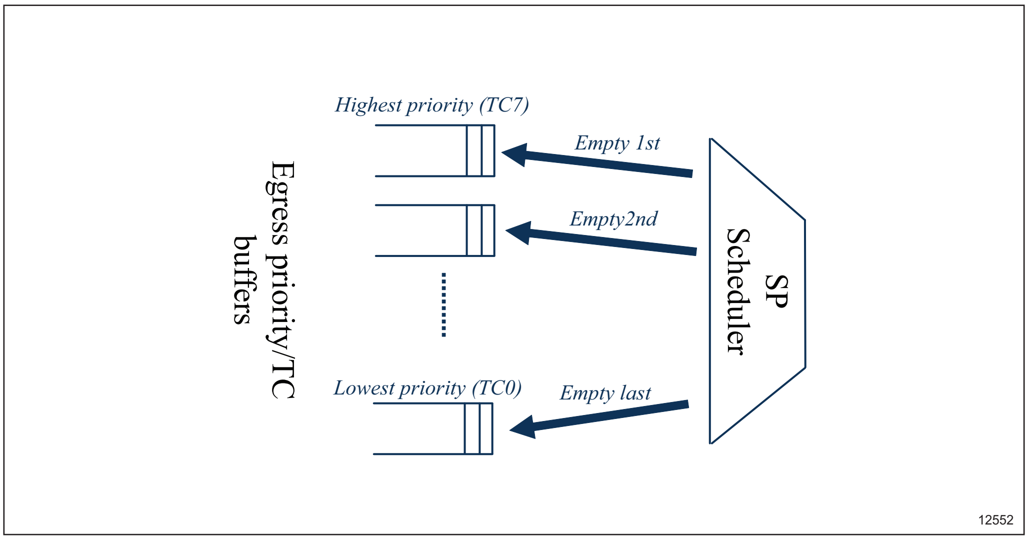


Figure 45 Strict Priority-Based Scheduling

The weighted scheduling algorithm is used when low latency is not crucial, but it is important to prevent starvation of buffers. With SP, buffers with lower priority will never get served if high priority queues are constantly being filled up. Weighted scheduler, however, will make sure that all queues are served according to the predefined weight ratio. The accuracy of the allocation is roughly 1%, where constant bit rate traffic is more accurate than burst traffic. Weighted scheduler is typically used for buffers with non delay sensitive data traffic.

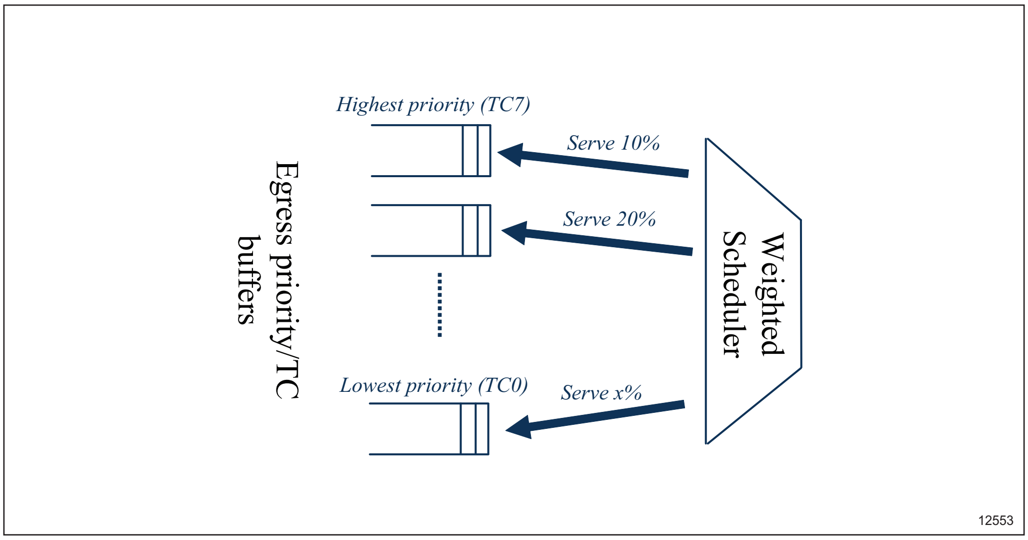


Figure 46 Weighted Scheduling

In a live network the SP and weighted scheduling algorithms are typically combined. In MINI-LINK 6600 the SP and weighted algorithms can be applied to different buffers as described in the example below. The size of the SP and weighted areas (x and y values) can differ but the SP/Weighted organization is fixed. The scheduler will serve the high priority SP area first and empty the buffers according to the SP algorithm. When the high priority SP area is empty the scheduler starts serving the weighted buffers according to individual weight.

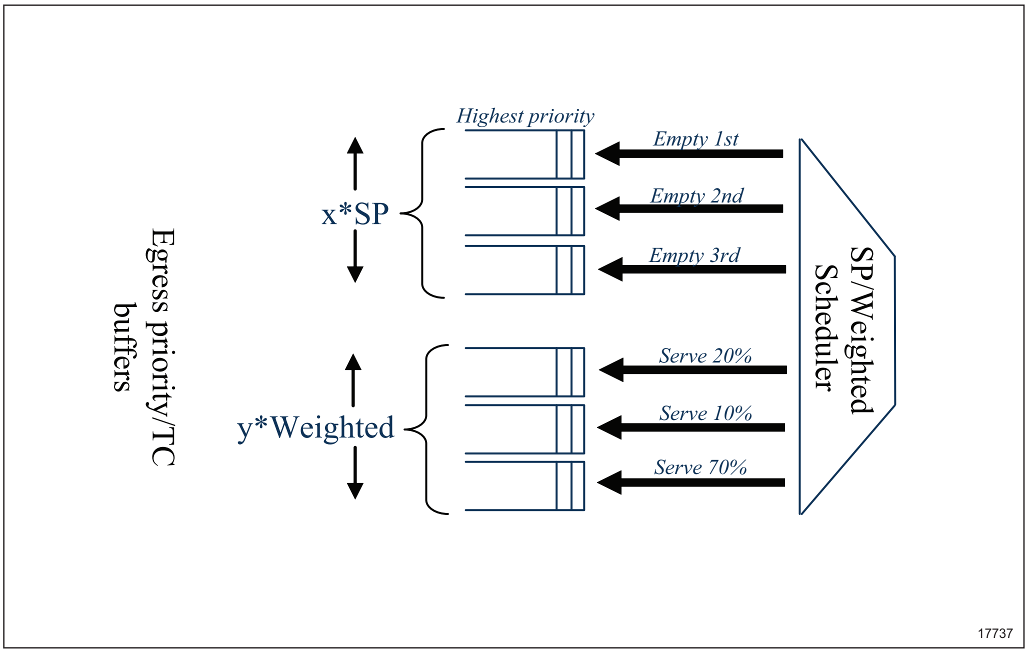
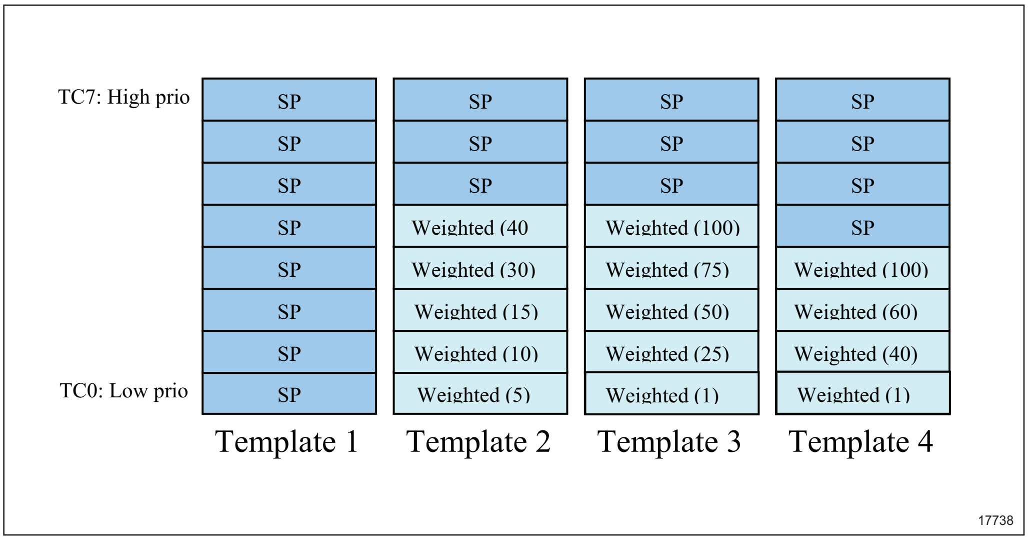


Figure 47 SP and Weighted Scheduling Combined in the Same Port

The SP and weighted schedulers can be configured individually per port from CLI and SNMP (not MINI-LINK Node GUI). However, to simplify the configuration effort the following predefined templates are supported. These templates can be selected individually from CLI, SNMP and MINI-LINK Node GUI,.



| | Template 1 | Template 2 | Template 3 | Template 4 |
|---|---|---|---|---|
| TC7: High prio | SP | SP | SP | SP |
| | SP | SP | SP | SP |
| | SP | SP | SP | SP |
| | SP | Weighted (40 | Weighted (100) | SP |
| | SP | Weighted (30) | Weighted (75) | Weighted (100) |
| | SP | Weighted (15) | Weighted (50) | Weighted (60) |
| | SP | Weighted (10) | Weighted (25) | Weighted (40) |
| TC0: Low prio | SP | Weighted (5) | Weighted (1) | Weighted (1) |

Figure 48 Scheduling Templates

## 7.5 Congestion Handling Summary

Congestion Handling in MINI-LINK can be summarized as follows:

- For trusted user domains, priority information is mapped from user/customer domain to network domain at the UNI.
- For untrusted user domains, default priority value is used as network priority in the network domain.
- Internally in the network domain the network priority settings are stored in the L2 PCP bits in the L2 header.
- Ethernet frames are mapped to egress TC buffer according to IEEE802.1D/Q or custom.
- In the egress TC buffer, frames are serviced according to a SP scheduler or weighted scheduler (DWRR), or both.
- Frames are dropped in the egress TC buffer due to tail dropping, color dropping, or WRED.
- WRED and color dropping are implemented for interfaces with deep buffer.

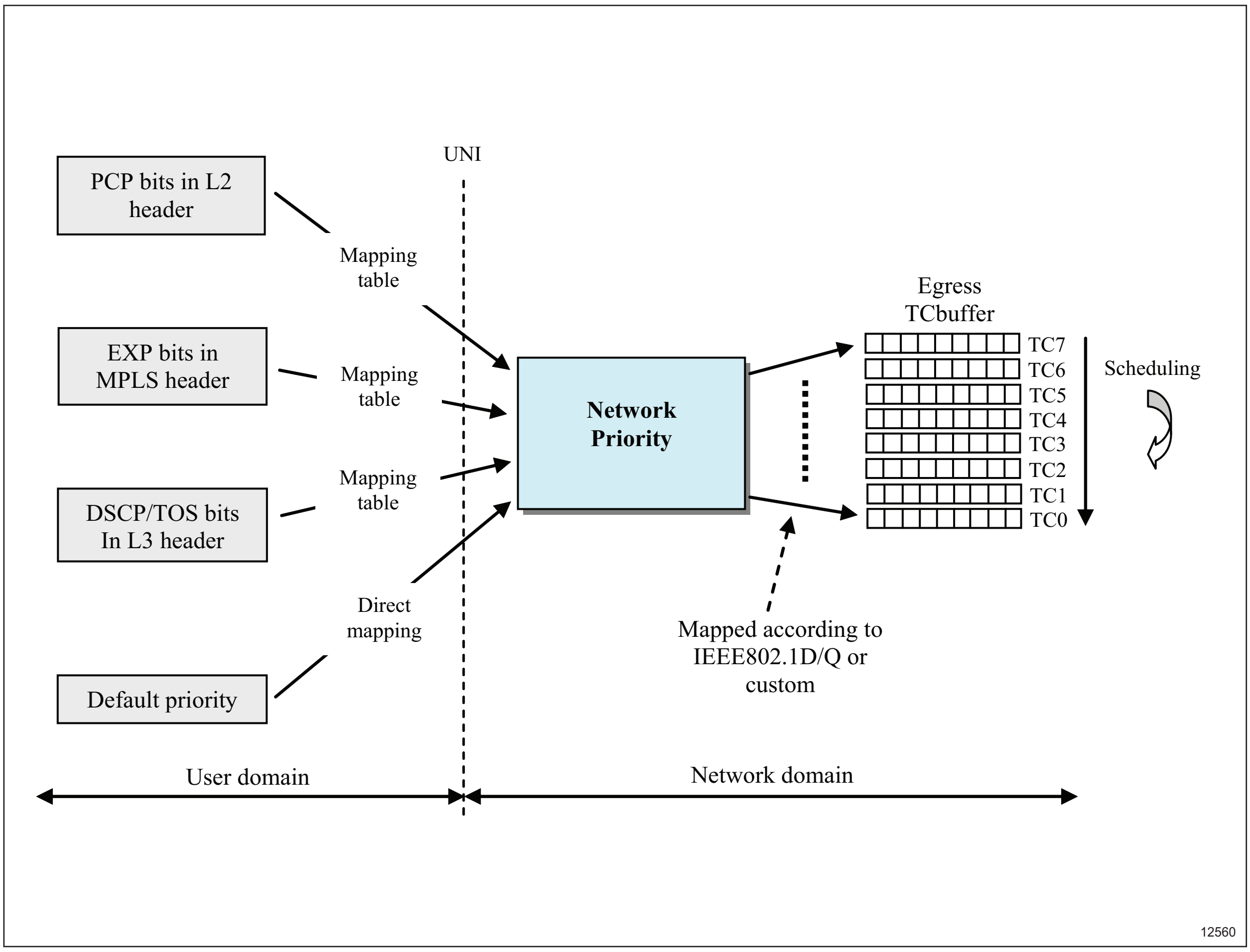


Figure 49 Congestion Handling in MINI-LINK

# 8 Hierarchical Quality of Service

Hierarchical QoS (HQoS) provides an additional level of traffic differentiation based on VLANs, therefore it enables that service quality can be ensured in a shared network scenario when multiple service providers share the same network, and also it helps to manage multiple RAN technologies separated by VLANs.

The traditional 2-level queue-port hierarchy can be extended to up to 4-level hierarchy, that is queue–node–node–port. The nodes can be configured to form the hierarchy according to the required use-case.

QoS features for HQoS are:

- VLAN based shaping: A maximum bandwidth can be set for a VLAN or a group of VLANs, that is, for an operator or an RBS.
- VLAN based scheduling: Both strict priority and deficit weighted round-robin are supported.

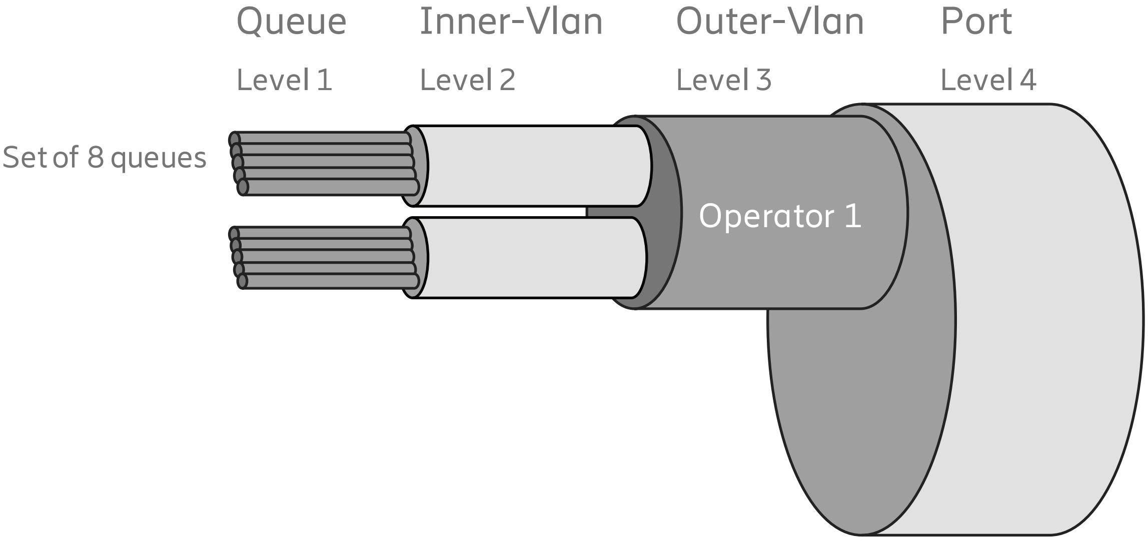


Figure 50 Principles of Hierarchical Quality of Service

# 9 Forwarding

## 9.1 Unicast Forwarding

MINI-LINK 6600 supports up to 1000 VLANs and storage and learning of 16K MAC addresses. It also supports an aging function, which discards MAC addresses that have been unused for a given time.

Each VLAN has individual learning, which in customer mode is performed on C-VLAN (EtherType 0×8100) and in provider mode performed on S-VLAN (EtherType 0×88a8). Each VLAN has a Filtering Database with dynamic and static entries.

Dynamic entries are automatically added and updated by the MAC learning process. Static entries are added manually and prevent flooding in case frames arrive for a destination address from which no Ethernet frames have arrived yet.

## 9.2 Multicast Forwarding

MINI-LINK 6600 supports a Layer 2 (MAC level) and a Layer 3 (IP level) multicast forwarding table.

- The L2 multicast table contains static entries. Each entry associates a (MAC address, VLAN) pair with a set of egress ports on that VLAN.
- The L3 multicast table is maintained dynamically by Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping. Each entry associates an IP multicast group (*, G, VLAN) or channel (S, G, VLAN) with a set of egress ports on that VLAN.

**Note:** The table lookup is based on the outer VLAN tag of the frame, that is, the C-VLAN in customer mode and the S-VLAN in provider mode.

IPv4 and IPv6 multicast packets are first looked up in the L3 multicast forwarding table by their source, destination (group) IP address, and VLAN ID. If a matching entry is found, the packet is forwarded to the ports in the entry, otherwise the packet is looked up in the L2 multicast forwarding table by its destination MAC address and VLAN Id. If no matching entry is found, the packet is classified as an Unregistered Multicast frame.

Non-IP Ethernet multicast frames are looked up by their destination MAC address and VLAN Id in the L2 multicast forwarding table. If a matching entry is found the frame is forwarded to the ports in the entry, otherwise it is classified as Unregistered Multicast.

Unregistered Multicast frames are either flooded to the VLAN or discarded. The handling is configurable per VLAN.

## 9.3 IGMP Snooping (IPv4) and MLD Snooping (IPv6)

IGMP for IPv4 and MLD for IPv6 are the protocols used by IPv4 and IPv6 hosts to report their IP multicast group memberships to neighboring multicast routers.

By default, a Layer 2 switch will flood multicast traffic to all ports in the VLAN (broadcast). The broadcast traffic can cause unnecessary bandwidth consumption in the network and extra processing load on host devices.

IGMP&MLD snooping uses the mechanism by which a Layer 2 device actively listens to Layer 3 IGMP&MLD messages between multicast hosts and routers. By parsing the messages passing through the switch, the Layer 2 switch learns the member status of multicast groups, and then builds a multicast table with this learned knowledge.

IGMP&MLD snooping switches will only forward multicast traffic to the ports where interested hosts are attached, thereby using link capacities in an efficient way.

MINI-LINK 6600 supports IGMP and MLD snooping for IGMPv2/v3 and MLDv1/v2 messages. Both Source-Specific Multicast (SSM) and Any-Source Multicast (ASM) service models are supported.

In MINI-LINK 6600, IGMP and MLD snooping is configured independently per VLAN instance. IGMP and MLD snooping can be simultaneously enabled on a VLAN. In customer mode, IGMP and MLD snooping can be activated on single C-tagged VLANs, while in provider mode both single S-tagged or S+C double-tagged VLANs are supported. IGMP and MLD snooping is disabled on all VLANs by default.

**Note:** In provider mode only the SVID is used in forwarding lookup, thus all CVIDs in an SVID share a common forwarding state. It is recommended to use only one CVID per SVID for multicast to avoid unwanted multicast traffic flooded to CEs.

The switch detects multicast router ports automatically based on the reception of IGMP and MLD general query and PIMv2 Hello messages.

When MINI-LINK 6600 detects an STP topology change and is the root bridge on the affected VLAN, a Query solicitation message is broadcasted to the Querier router to facilitate fast convergence of multicast forwarding state.

By default MINI-LINK 6600 operates in transparent snooping mode. In this mode the switch forwards all IGMP and MLD messages between hosts and routers transparently, and processes them to maintain the L3 multicast forwarding table.

The following is valid for IGMP and MLD snooping:

- Proxy Reporting

Proxy reporting extends the basic snooping functionality aiming to minimize the IGMP and MLD protocol processing load on upstream multicast routers and IGMP and MLD snooping switches.

When Proxy reporting is enabled, IGMP and MLD join reports for existing IGMP and MLD states are suppressed. Only the first IGMP and MLD join message is propagated towards routers. In addition, IGMP and MLD leave messages are forwarded from the hosts to the IGMP and MLD routers only when the last member leaves a group.

- Immediate-leave

  MINI-LINK 6600 supports Immediate-leave on individual VLAN ports. Upon receiving an IGMP and MLD leave message, IGMP and MLD snooping immediately removes the port from the forwarding table entry for that multicast group without sending out an IGMP and MLD group-specific query and waiting for its timeout.

  **Note:** Immediate-leave should only be enabled on VLAN ports to which a single host is attached. Otherwise, some hosts can be inadvertently dropped.

- Ethernet Switch Limits

  The L3 multicast forwarding table can accommodate up to 1000 multicast groups.

# 10 Ethernet Protection

MINI-LINK 6600 offers multiple redundancy features that fulfill different needs and operate both on plug-in unit and connection level.

## 10.1 RSTP/MSTP

Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) help build logical loop-free topology for Ethernet networks. The basic function is to prevent bridge loops and the broadcast radiation that results from them.

**RSTP**

The RSTP offers redundancy and rerouting of traffic if a node is out of service. The Ethernet transport network is typically divided in multiple RSTP domains. Within one RSTP domain a reconfiguration of the active Ethernet connections typically takes 50–100 ms without service impact.

**MSTP**

MSTP supports multiple concurrent topologies and spanning trees mapping VLANs into spanning trees. It uses basic RSTP mechanisms for topology calculation and rapid port state transitions.

MSTP configures a separate Spanning Tree for each VLAN group and blocks the links that are redundant within each Spanning Tree. This enables load balancing of network traffic across redundant links.

MSTP is backward compatible with RSTP and STP and the same performance requirements are applicable for MSTP as for RSTP.

## 10.2 Ethernet Ring Protection (ERP)

Ethernet Ring Protection (ERP) switching and Ethernet Linear Protection Switching (LPS) are supported according to ITU-T standards G.8031, G.8032v1, and G.8032v2.

### 10.2.1 ERP Single Ring

A single Ethernet ring consists of at least two NEs that are connected to each other in a ring configuration. One of the links is designated as the Ring Protection Link (RPL) which protects the entire ring.

To avoid loops, the RPL is inactive during normal operation. See Figure 51.

If one of the other links in the ring fails, the RPL is activated and the traffic is rerouted to avoid disturbances. See Figure 52.

When the failed link is restored, the RPL becomes inactive again.

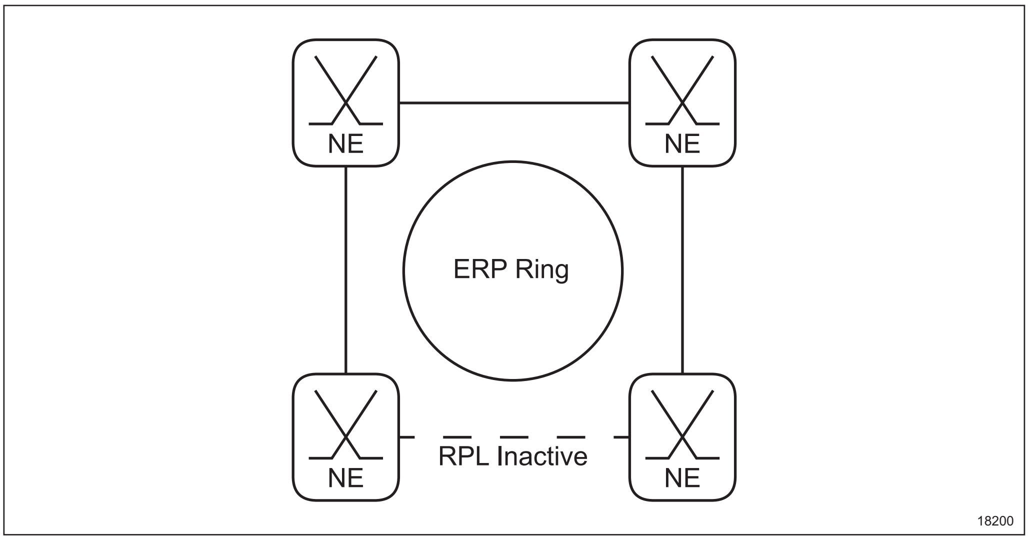


Figure 51 Single Ring, Normal Operation

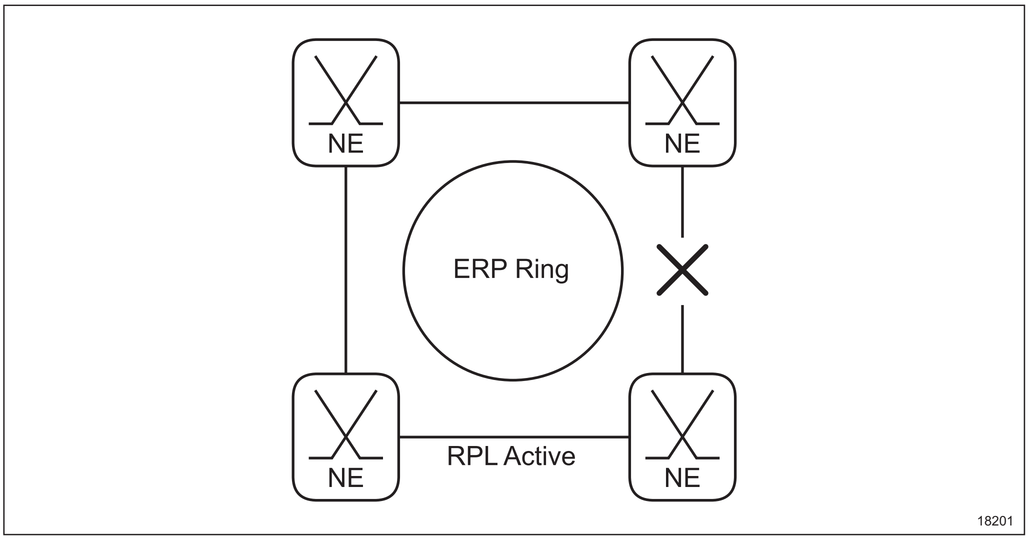


Figure 52 Single Ring, Link Failure

### 10.2.2 ERP Multiple Rings

Multiple Ethernet rings consist of NEs that are connected to each other in a configuration with two or more rings, one main ring and one or more sub-rings. In each ring, one of the links is designated as the Ring Protection Link (RPL) which protects that ring.

To avoid loops, the RPL is inactive during normal operation. See Figure 53.

If one of the other links in the ring fails, the corresponding RPL is activated and the traffic is rerouted to avoid disturbances. See Figure 54.

When the failed link is restored, the RPL becomes inactive again.

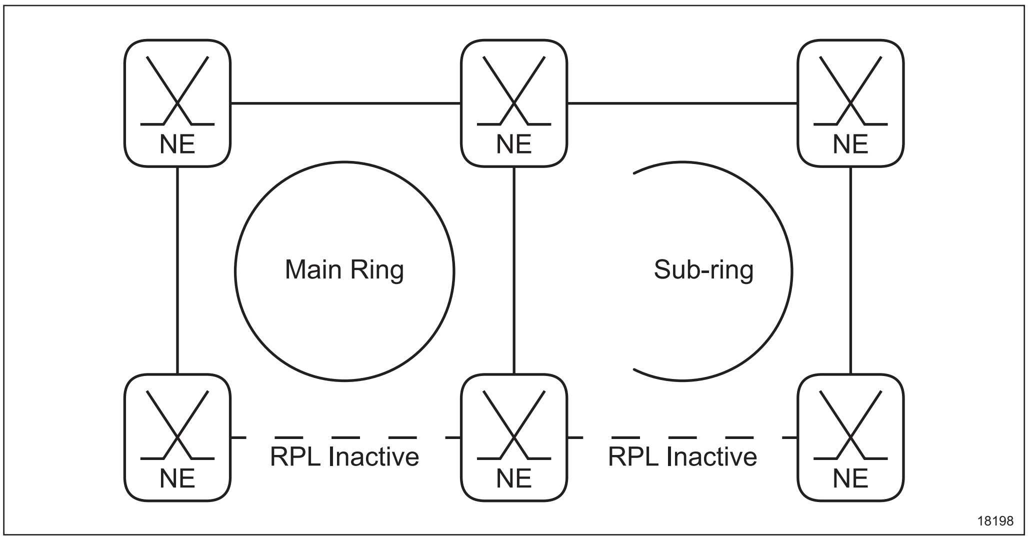


Figure 53 Multiple Rings, Normal Operation

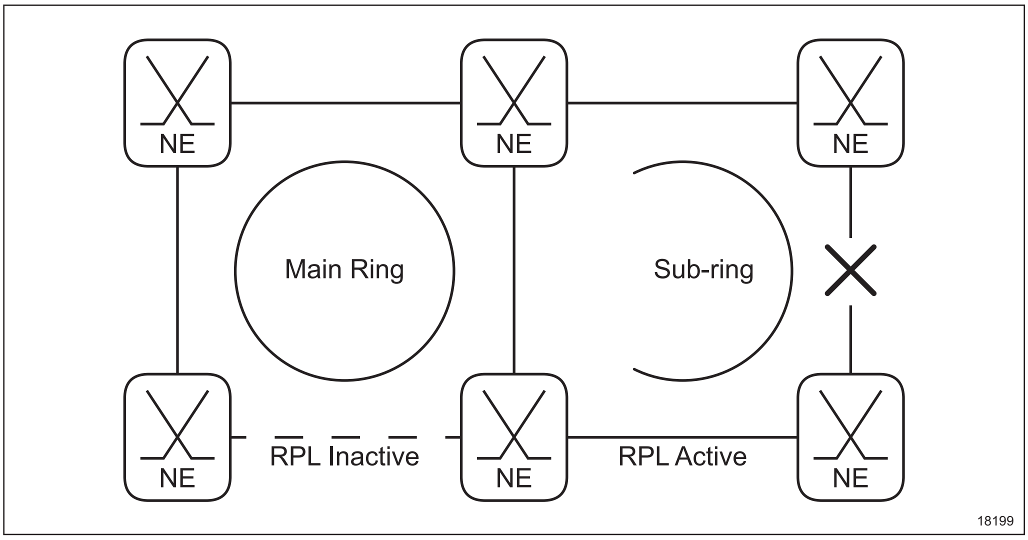


Figure 54 Multiple Rings, Link Failure

## 10.3 Link Aggregation Group (LAG) with LACP

This section presents the protection mechanisms available on Layer 2 connections.

**Link Aggregation Group**

MINI-LINK 6600 supports Link Aggregation Group (LAG) with Link Aggregation Control Protocol (LACP), which aggregates several external Ethernet links into one logical link and provides line protection.

A LAG supports a maximum of four links, but in case of NPU 1002 or NPU 1005 the number of links increase so that a LAG supports a maximum of eight links.

LACP has three operational modes:

- Static

  No LACP PDU communication. LAG hashing is governed by the port operational and administrative states or optionally by LinkOAM.

- Active

  LAG hashing is governed by the LACP state machine using the information inferred from LACP PDU communication.

- 1+1

  Al LAG-LACP operation applicable for 2-port LAGs, when LACP allows only one active port out of the 2 LAG member ports.

When a new LAG is created, the default LACP operation mode is Static.

Link Aggregation Control configures and controls the Link Aggregation sublayer using static or dynamic information, exchanged between the connected NEs by means of LACP. LACP enables dynamic configuration of LAG.

LACP is used by the nodes on either end of a LAG to automatically monitor and maintain adjoining LAG links between them.

On a regular basis, L2 Link Aggregation devices with running LACP advertise their capabilities and status on potential aggregation. The peering devices compare their own configuration and the configuration of their partner and states with each other, associated with each link of the LAG. Each peer can then decide what action to take in terms of setting a link traffic carrying status. Once in a steady state, LAGs are maintained by regular exchange of information between peers.

If a link in a LAG fails, traffic is redirected from the faulty link to the remaining links in the LAG using graceful degradation. The switch from active to passive path takes less than 50 ms for a bidirectional link failure and does not impact the traffic. A faulty link affects the total link capacity and traffic with low priority may be discarded to ensure that traffic with high priority is sent.

When a 2-port LAG is configured in LACP 1+1 mode, the LAG member ports form an active/standby pair. Generic Ethernet traffic is transmitted and received through the active port. LACP PDUs are exchanged through both ports.

Whenever there is a connectivity fault in the link connected to the former active port, then the former standby port is activated and Ethernet traffic is redirected to this port. When the link of the higher priority link is recovered, it regains the active role if revertive switching is enabled.

Whenever there is a connectivity fault in the link connected to the standby port, the Ethernet traffic through the active port remains undisturbed.

In MINI-LINK 6600, the LAG master port is assigned with the highest LACP port priority.

Which of the 2 LAG member ports becomes active is determined by negotiating the LACP port priorities between the two LACP hosts.

**Note:** The near end LACP host is configured with LACP 1+1, while the far-end host is configured with LACP Active, then the LAG will operated in active/standby manner and the active port will be arbitrated between the two LACP hosts according to the LACP standard.

Network rerouting according to Ethernet Ring Protection (ERP) and Rapid/Multiple Spanning Tree Protocol (RSTP/MSTP) is not triggered unless all physical links in an LAG fails.

ERP and RSTP/MSTP activates a redundant link in case of link failure and protects the network from infinite loops.

To improve the switch-over time for unidirectional faults, LAG should be combined with Link OAM. Link OAM will take down the link if a unidirectional fault is detected.

A Hashing Algorithm is used to identify the different traffic flows and assign them to the different ports, belonging to the same LAG.

Hashing algorithm is configurable and is based on different L2 or L3/L4 traffic parameters, according to Table 9.

Table 9 Hashing Algorithms

| MINI-LINK Node GUI Parameter | CLI Parameter | Hashing Algorithm |
|---|---|---|
| srcMac | mac-sa | Source MAC address, VLAN ID, Ethertype, and source bridge port ID. |
| dstMac | mac-da | Destination MAC address, VLAN ID, Ethertype, and source bridge port ID. |
| srcDstMac | mac-sa-da | Source MAC address, destination MAC address, VLAN ID, Ethertype, and source bridge port ID. |

| MINI-LINK Node GUI Parameter | CLI Parameter | Hashing Algorithm |
|---|---|---|
| srcIp | ip-src | Source IP address and source TCP/UDP port. |
| dstIp | ip-dst | Destination IP address and destination TCP/UDP port. |
| srcDstIp | ip-src-dst | Source IP address, destination IP address, source TCP/UDP port, and destination TCP/UDP port. |

The hashing algorithm selection allows an effective traffic load balancing between the different links belonging to an LAG.

### 10.3.1 LAG/LACP 1+1 Protection of MINI-LINK 6352

LAG/LACP 1+1 protection can be used in combination with a redundant E-Band link pair of two MINI-LINK 6352 according to Figure 55, so that the connectivity is protected against both E-band link faults and MINI-LINK 6352 equipment.

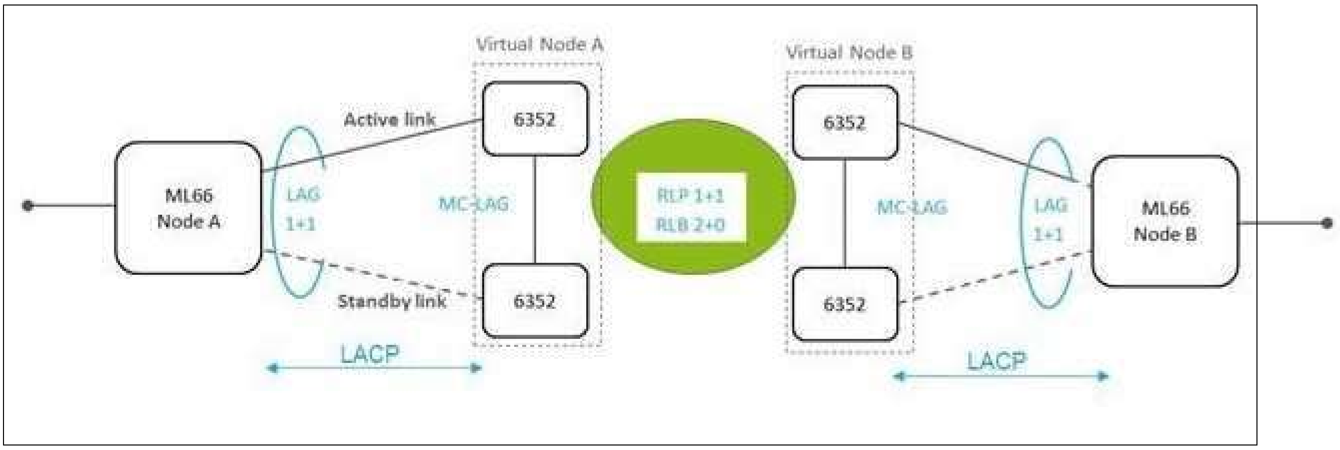


Figure 55 LAG/LACP 1+1 Protection of MINI-LINK 6352

For the details of the protection mechanism, please refer to the CPI library of MINI-LINK 6352.

## 10.4 Ethernet Layer 1 Protection Mechanisms

The Link Loss Forwarding (LLF) feature improves the protection switching time for Layer 1 connections by propagating connectivity loss information to both connection end points. LLF is not supported with ETU interfaces.

LLF can be split in two scenarios, broken WAN links or broken LAN links.

### WAN Link Broken

When the terminating end points of the point to point connection detects that the WAN connection is lost, the Ethernet ports on both sides will be taken down (that is, disable line carrier).

### LAN Link Broken

When a terminating end point of the point to point connection detects that the LAN connection is lost, the corresponding WAN port will be taken down. On the remote end, the disconnected WAN link is detected and the corresponding LAN port will be taken down.

# 11 Ethernet Operation & Maintenance

MINI-LINK 6600 have support for a number of Ethernet application related O&M functionalities.

## 11.1 Ethernet Performance Counters

For information on the performance counters supported for LAN/WAN Ethernet ports in MINI-LINK 6600, see Section 16.9.2 on page 233.

## 11.2 Ethernet Link OAM

MINI-LINK 6600 supports Ethernet in the First Mile (EFM) or Link OAM according to IEEE802.3ah for all LAN ports. Link OAM is a diagnostic tool that can be used in both online and offline configurations.

**Note:** Ethernet Link OAM is only supported for LAN interfaces (Layer 1 Connection and Layer 2).

The three main Ethernet Link OAM services are as follows:

- **Failure Notification**

  Notification of an Ethernet link failure to or from far end for an NE in operation.

  The following three types of failures are supervised:

  - Link fault (RDI)

    The **Link fault (RDI)** alarm is generated when a failure in a physical layer has occurred in the receiving direction.

  - Dying gasp

    The **Dying gasp** alarm is generated when a plug-in unit is about to restart or is going to operational state **Down**. This occurs when an unrecoverable failure has occurred.

    **Note:** Only supported in receiving direction (an event is raised).

  - Critical event

    The **Critical event** is generated when an unspecified critical event has occurred.

    **Note:** Only supported in receiving direction (an event is raised).

- **Link Monitoring**

Link monitoring is used for event notification on errored frames at both near and far end and is used on NEs in operation. The notifications are based on a threshold crossing within a specific time window.

The following events are reported:

- Errored Symbol Period Event

  Generated when the number of symbol errors exceeds a threshold in a given time window, which is defined by a number of symbols.

- Errored Frame Event

  Generated when the number of errored frames exceeds a threshold in a given window, which is defined by a period of time.

- Errored Period Event

  Generated when the number of errored frames exceeds a threshold in a given window, which is defined by a number of frames.

- Errored Frame Seconds Summary Event

  Generated when the number of errored frame seconds exceeds a threshold in a given time period. An errored frame second is defined as a 1 second interval with one or more frame errors.

— **Remote Loopback**

Link OAM remote loopback can be used for fault localization and link performance testing on LAN interfaces. Statistics from both near end and far end NE can be requested and compared at any time while the far end NE is in O&M remote loopback mode. The requests can be sent before, during, or after loopback frames have been sent to the far end NE. The loopback frames in the O&M sublayer can be analyzed to determine which frames are being dropped due to link errors.

In the offline set up all traffic is halted for the affected ports. A loop is configured manually and a traffic generator sends test frames as indicated in Figure 56. PM measurements in the receiving end are compared with the submitted traffic from the test generator to detect errors. The manually configured loop can be set on either side of the connection.

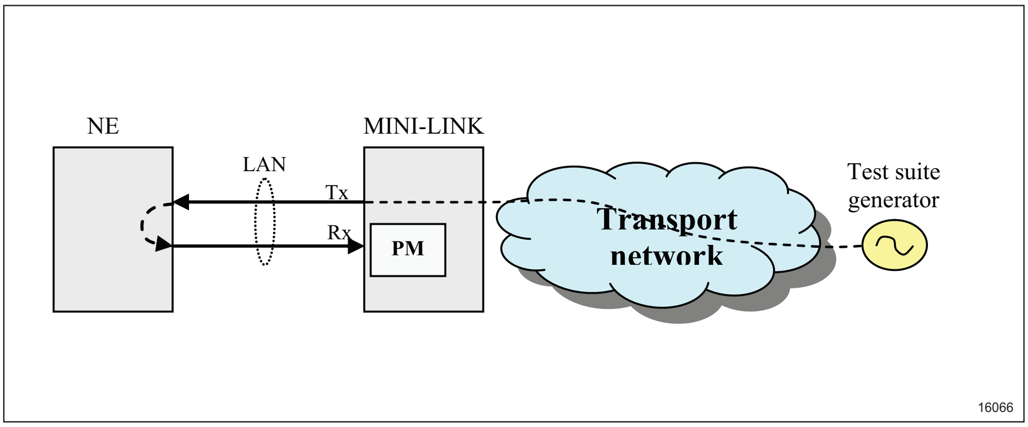


Figure 56 Link OAM Offline Configuration

As an online diagnostic tool, Link OAM is constantly monitoring the link status and detects unidirectional and bidirectional faults, see Figure 57. When a link fault is detected, for example, LOC, RDI is transmitted in the Tx direction. On the receiving side an alarm is triggered.

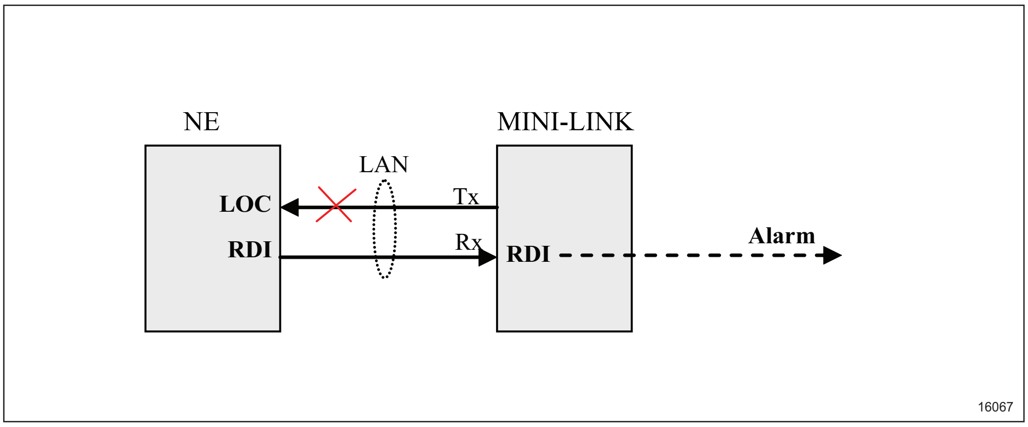


Figure 57 Link OAM Online Configuration

## 11.3 Ethernet Service OAM

Ethernet Service OAM is used to manage networks comprising of multiple LANs. It provides performance monitoring, according to ITU-T Y.1731 and Y.1730, and supports fault management on Ethernet links, according to IEEE 802.1ag.

Ethernet Service OAM can be used in both Customer mode and Provider mode, if Ethernet Service OAM PDUs are C- or S-VLAN tagged, and can be used in LAG and RSTP/MSTP scenarios.

The four main Ethernet Service OAM functions are as follows:

- **Continuity Check Monitoring**

Continuity Check Monitoring detects service interruption between MEPs. Continuity Check Messages (CCMs) are sent from one MEP to another, enabling MEPs to locate other MEPs. CCM confirmation can also be requested by an MEP from a linked MEP, to ensure that the CCMs are sent and received without fault.

The CCM intervals can be set at 3.3 ms, 10 ms, 100 ms, 1 s, 10 s, 1 min, or 10 min.

- **Remote Defect Indication**

  An MEP uses Remote Defect Indication (RDI) to communicate with linked MEPs that a fault has occurred, usually that CCM confirmation were not received. The RDI is an indication that a fault has occurred either at the far-end MEP or between the two MEPs.

- **Loopback**

  Loopback is a troubleshooting tool that verifies the connectivity of a MEP with linked MEPs and linked Maintenance Intermediate Points (MIPs).

- **Linktrace**

  Linktrace is a bidirectional continuity check used for fault localization. When a Linktrace Message (LTM) is sent to a destination MEP or MIP, a Linktrace Reply (LTR) is expected from all the intermediate MIPs along the path to the destination and from the destination MEP or MIP itself. Missing or misordered LTRs point out the location of a fault in an efficient way.

Ethernet Service OAM supports the following PM functions:

- Frame Delay
- Frame Delay Variation Measurement
- Frame Loss Measurement (ETH-LM)
- Ethernet Bandwidth Notification (ETH-BN)

A Maintenance Domain (MD) is defined as a network or sub-network, at the Ethernet level, within which OAM frames are exchanged. An MD determines the span of an OAM flow, across network administrative boundaries.

There are the following three types of MDs:

- Network Operator MD
- Service Provider MD
- Customer MD

MDs are hierarchal and as such, MDs of the same type do not overlap each other, for example, two MDs of the same level do not overlap each other. However, different MD types from different levels may overlap, for example, a Customer MD may overlap multiple Service Provider MDs, but the Customer MD cannot overlap another Customer MD.

An MD consists of the following components:

- Maintenance Entity (ME) – An OAM entity that requires management.
- Maintenance Association (MA) – A group of MEs that belong to the same service inside a common MD. An IEEE concept.
- MD Level – A way of distinguishing which MEs belong to the same MD. All MEs belonging to the same MD share the same MD Level. An IEEE concept.
- ME Group (MEG) – A group of MEs that belong to the same service inside a common MD. An ITU-T concept.
- MEG Level (MEL) – A way of distinguishing which MEs belong to the same MD. All MEs belonging to the same MD share the same MEG Level. An ITU-T concept.
- Maintenance End Point (MEP) – An OAM reference point that can initiate and terminate OAM frames, and that reacts to diagnostic OAM frames.
- Maintenance Intermediate Point (MIP) – An OAM reference point that reacts to diagnostic OAM frames initiated by MEPs.

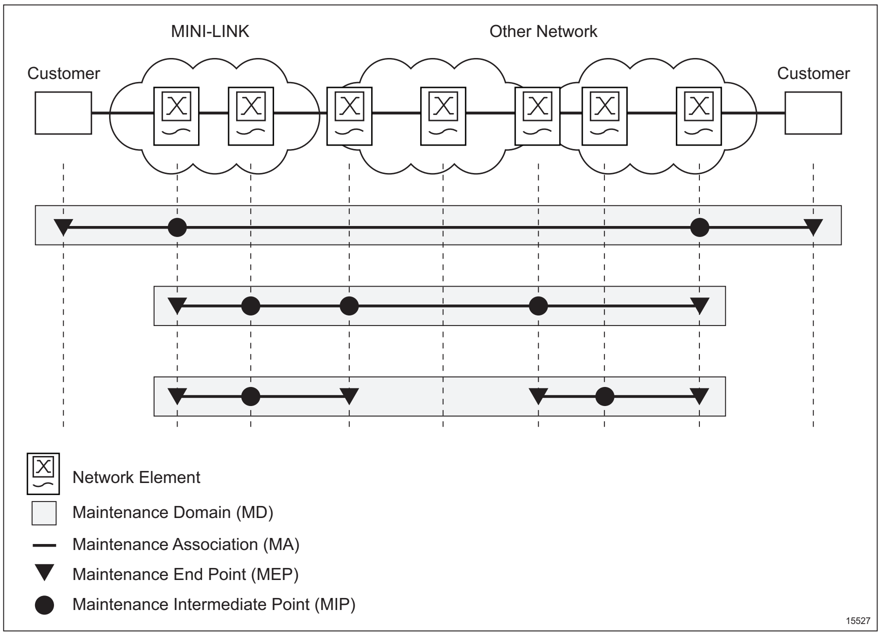

MINI-LINK
Other Network
Customer
Customer
Network Element
Maintenance Domain (MD)
Maintenance Association (MA)
Maintenance End Point (MEP)
Maintenance Intermediate Point (MIP)
15527

Figure 58 Ethernet Service OAM Network Overview

ETH-BN is supported according to ITU-T G.8013/Y.1731 and Y.1730.

ETH-BN reports bandwidth changes of a monitored WAN interface with Bandwidth Notification Message (BNM) frames. When a bandwidth change is detected, ETH-BN reports it after a configured hold time. BNM frames contain the nominal (licensed) bandwidth and the actual bandwidth of the link.

MINI-LINK implementation of ETH-BN relies on a MEP to be configured on the node. It is used to determine on which interfaces the BNM frames should be sent. The MEP could be on a different interface, together with the up/down status these are used to determine the outgoing interfaces. Up and down MEPs are defined in IEEE 802.1ag.

A down MEP sends BNM frames out on only one interface. See Figure 59.

An up MEP sends BNM frames towards the switch rather than the egress direction of the interface. In this way the VLAN switching can send the BNM frames towards multiple outgoing interfaces. See Figure 60.

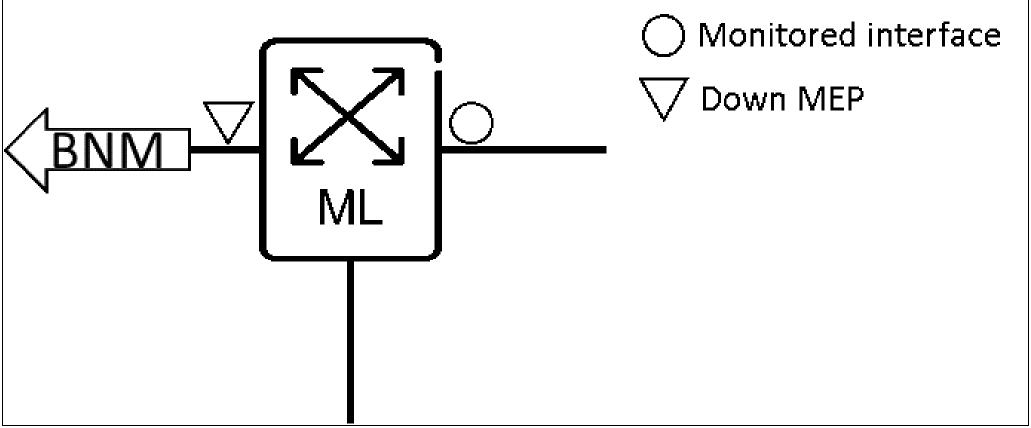


Figure 59 ETH-BN with Down MEP

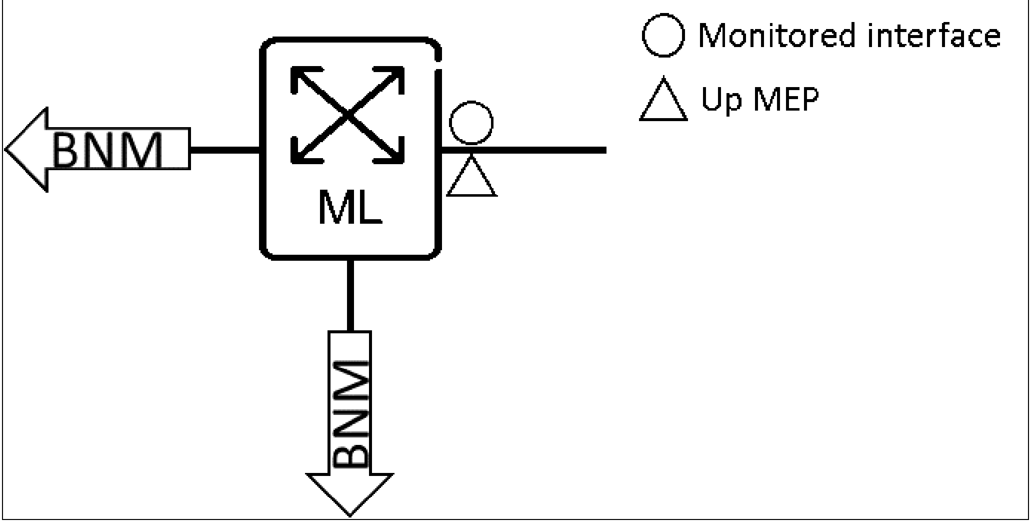


Figure 60 ETH-BN with Up MEP

By default, BNM frames are always sent, even when the link is at full speed or drops to zero. This behavior can be changed to sending only one BNM frame or no

BNM frames when the link is restored to full speed, and the same configuration is possible for link failure.

**Note:** It is not recommended to turn off sending BNM frames for both full link speed and link failure.

In this case, once the ETH-BN stops sending BNM frames, the receiving router cannot determine whether the link is restored to full speed, or it failed.

## 11.4 Port Mirroring

Port mirroring can be used for packet traffic crossing in MINI-LINK 6600. The port mirroring feature sends a copy of all packets seen on one LAN/WAN switch port to a LAN test port, see Figure 61. The test port is named Mirror to Port (MTP).

**Note:** Deep buffering must be disabled for the MTP ports.

This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion detection system and troubleshooting.

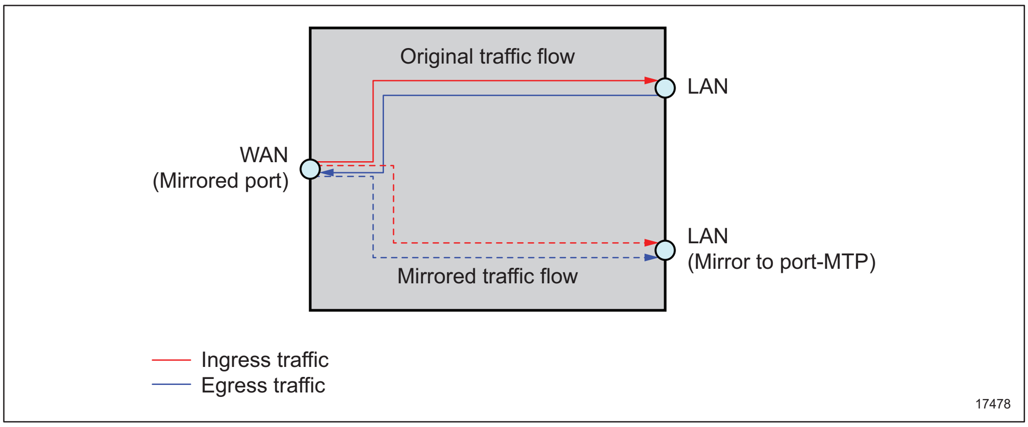


Figure 61 Port Mirroring – Mirroring a WAN Interface to a LAN Port

It is possible to enable ingress and egress port mirroring separately.

If the MTP VLAN tag is configured, both ingress and egress mirrored traffic is always tagged at the MTP with the MTP VLAN tag as outer tag.

# 12 L3 Services

The NE provides Layer 3 Virtual Private Network (L3VPN) services and IPv4 routing and transport services.

Table 10 lists the features that are possible to configure for Layer 3 solutions.

Table 10 Configurable Features for Layer 3 Solutions

| Business Application | | Routing Options | Services |
|---|---|---|---|
| L3VPN | BGP/MPLS<br>Layer 3 VPN (L3 PE router)<br>P router | CE-PE routing options:<br>OSPFv2<br>Static<br>eBGP<br>Core routing options:<br>iBGP<br>MPLS<br>LSP: LDP, RSVP-TE<br>IGP: OSPFv2, IS-IS | QoS<br>Route filters<br>LAG or ECMP<br>BFD<br>MPLS OAM |
| Layer 3 IP Router | | Core routing options:<br>BGP<br>IGP: OSPFv2, IS-IS | QoS<br>Route filters<br>LAG or ECMP<br>BFD |

## 12.1 L3 IP Router

The NE supports standard IP routing that forwards packets to their final destination using intermediate nodes. Each node looks up the destination IP address and forwards the packet toward the destination through routes collected in a routing table.

On the NE, route information is collected from the different routing protocols in the RIB on the controller card, which calculates the best routes and downloads them to the FIB stored on the NE. The RIB process collects routes to directly attached devices, configured static IP routes, and routes learned dynamically from OSPF and BGP.

When a network event causes routes to go down or become unavailable, routers distribute routing update messages that are propagated across networks, causing a recalculation of optimal routes. Routing algorithms that converge slowly can cause routing loops or network outages.

## 12.2 L3VPNs

The NE provides the following Layer 3 services and solutions:

- End-to-end Layer 3 connection over an IP/Multiprotocol Label Switching (MPLS) core network
- Business Virtual Private Networks (VPNs), such as Border Gateway Protocol (BGP)/MPLS L3VPNs.
- Core routing solutions, such as P router, in an IP/MPLS core network
- Multiple virtual routing instances via Virtual Routing Forwarding (VRF)
- The NE can provide Layer 2 Ethernet transport services and Layer 3 unicast routing on the same NE without separate Layer 2 and Layer 3 devices.

Figure 62 illustrates MINI-LINK 6600 in a Layer 3 network with VPNs.

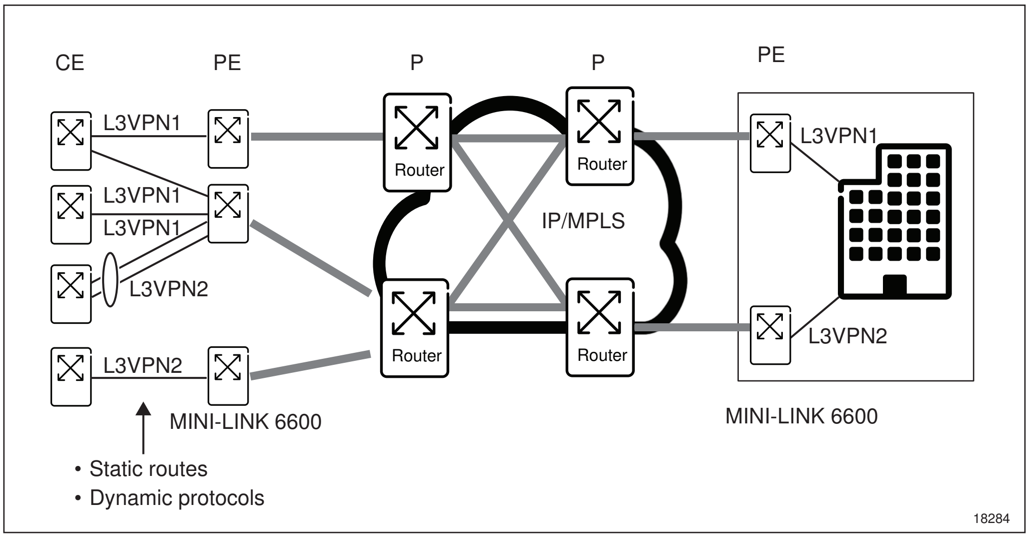


Figure 62 L3VPNs

## 12.3 Supported Routing Protocols

The NE supports the following routing protocols:

- **Static Routing**
- **OSPF**

  OSPF is an Interior Gateway Protocol (IGP) that uses Link-State Advertisements (LSAs) to inform other routers of the state of the sender links. In a link-state routing protocol, each NE distributes information about its interfaces and neighbor relationships. The collection of the link states forms a database that describes the Autonomous System (AS) topology. As OSPF routers accumulate link-state information, they use the Shortest Path First (SPF) algorithm to calculate the shortest path to each node, which forms the basis for developing routing information for that AS.

  The following summarizes the OSPF features:

  - An NE can be a part of a non-stub area, stub area or totally stub area.
  - An NE can act as an Internal Router (IR), as an Area Border Router (ABR), or as an Autonomous System Border Router (ASBR).
  - Virtual links are supported, which is useful when an area needs to be split in two parts.
  - Link summarization is supported, which is used in the ABR to minimize the routing information distributed to the backbone and/or other areas.
- **IS-IS**

  Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. It accomplishes this by determining the best route for data through a packet-switched network.

  IS-IS enables the separation of an IS-IS domain into separate areas, improving the scalability of the IS-IS network. IS-IS level 2 and level 1-2 node functionality is required on the borders of the areas.

  A multi-area IS-IS network can be used for MPLS transport with inter-area LSPs either by using LDP or by using RSVP-TE with strict hops along the path.
- **BGP**

  BGP, an EGP based on distance-vector algorithms, uses TCP as its transport protocol. BGP operates between two BGP nodes, called BGP speakers. After a TCP connection is established, the two BGP speakers exchange dynamic routing information over the connection. The exchange of messages is a BGP session between BGP peers.

  - Multiprotocol internal BGP (MP-iBGP) is used to exchange routing information and service label allocations between VPN endpoints in PE nodes in a L3VPN network.

  - External BGP (eBGP) is run by routers that belong to different autonomous systems and exchange BGP updates. It can for example be used to exchange routing information between PE and CE nodes.

- **Routing Policies**

  Routing policies allow network administrators to enforce various routing policy decisions on incoming, outgoing, and redistributed routes. The tools used to configure routing policies include BGP AS path lists, BGP community lists, IP-prefix lists, and route maps with match and set conditions.

## 12.4 MPLS Networking

The NE supports MPLS to forward packets through a network efficiently.

In a conventional IP Network, routers forward packets through the network from one NE to the next, with each NE making an independent forwarding decision by analyzing the packet header. Packet processing often causes considerable forwarding delay. With MPLS, the complete analysis of the packet header is performed only once when it enters an MPLS-enabled network.

### 12.4.1 MPLS-Based Solutions

The NE supports L3VPN solutions using MPLS networks in which customer connectivity among multiple remote sites is deployed across a shared central infrastructure and still provides the same access or security as a private network.

- **BGP/MPLS VPNs**

  Layer 3 BGP/MPLS VPNs are a collection of policies that control connectivity among a set of sites. A customer site is connected to the service provider network, often called a backbone, by one or more ports. The service provider associates each port with a VPN context.

  A BGP/MPLS VPN allows you to implement a wide range of policies. For example, within a VPN, you can allow every site to have a direct route to every other site (full mesh), or you can restrict certain pairs of sites from having direct routes to each other (partial mesh).

### 12.4.2 Label Distribution

To communicate labels and their meanings among LSRs, MPLS uses a label distribution protocol (LDP or RSVP-TE), which enable dynamic label allocation and distribution in an MPLS network.

- **LDP:** An LSR enabled with LDP can establish LSPs to other LSRs in the network. LDP creates label bindings by assigning labels to connected routes and advertising the bindings to neighbors. LDP also assigns labels to label bindings learned from neighbors and readvertises the binding to other neighbors. When an LSR advertises a label binding for a route, the LSR is advertising the availability of an LSP to the destination of that route. LDP can learn several LSPs from different neighbors for the same route. LDP must be configured with an IGP, such as OSPF. LDP assigns a label only to routes selected by the underlying IGP.

— **RSVP-TE:** The LSRs can establish LSPs to other LSRs using RSVP-TE. The RSVP-TE allows the establishment of MPLS label switched paths (LSPs), considering the network constraint parameters, such as link coloring or available bandwidth. Unlike LDP, where LSP paths always follow the IGP topology, the RSVP-TE allows the definition of explicit paths defined by the user.

### 12.4.3 RSVP-TE Fast Reroute

RSVP-TE based MPLS networks can offer restoration times in the range of several seconds using reconvergence of the protocols in case of a link or node failure. To improve resiliency times to 50 ms or below, the Fast Reroute solution can be applied.

Fast Reroute (FRR) provides local protection, that is, FRR is used to protect local link or node failures. To protect a link failure, any router - except for the egress node - can set up a backup (bypass/ detour) LSP avoiding the protected link to its next-hop router. On the other hand, to protect a node failure, a router has to set up a backup LSP to its next-next-hop router.

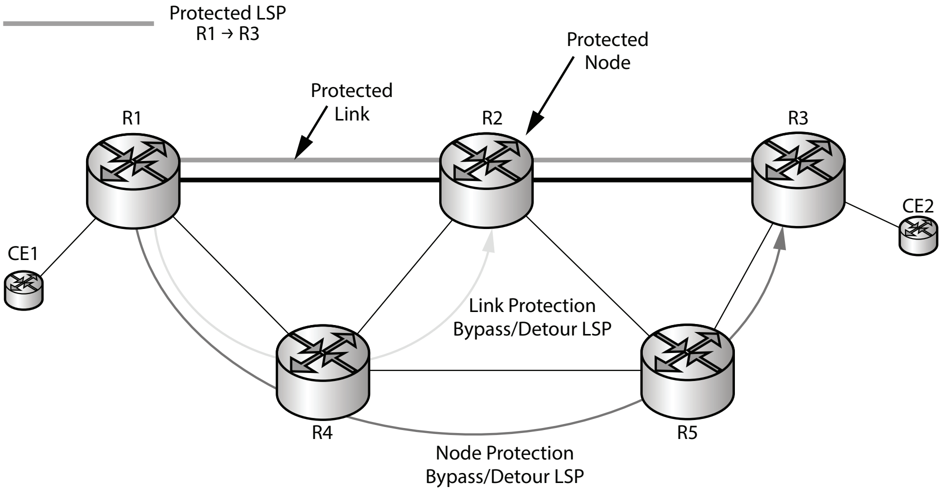


Figure 63 RSVP-TE Fast Reroute

The routers monitor the next hops by using Bidirectional Forwarding Detection (BFD), and immediately reroute to the backup LSP in case the BFD session is broken. Using BFD timers of 10 ms will result in detection times of 30 ms and rerouting times below 50 ms.

There are two schemes in RSVP-TE FRR, namely one-to-one backup and facility backup:

- In one-to-one backup, one backup LSP has to be established for every protected LSP. Specifically, if there are N protected LSPs, N backup LSPs are needed.
- In facility backup, one backup LSP can be used to protect all LSPs using the same outgoing interface/link; this requires pushing another (third) label to the packets.

Apparently, facility backup scales better than one-to-one backup, but the implementation is more complex due to the use of the extra label. In ML66, the one-to-one backup is supported.

**Note:** In ML66, the 50ms switchover time criterion is not guaranteed on managed node restart.

The backup LSP takes the traffic until the routing protocols reconverge and set up a new primary LSP (also with new backup LSPs). From that point, the new LSP takes over the traffic, while the old LSP and its backup LSPs are torn down.

### 12.4.4 RSVP-TE Path Protection

RSVP-TE Path Protection enables establishing primary and backup Label-Switched Paths (LSPs). In case of a failure along the primary LSP, the head-end will switch over to the backup LSP with a switchover time less than a second.

The primary and backup LSPs are manually established end-to-end between the head-end and tail-end nodes, using TE techniques such as explicit hops or administrative groups. One LSP is configured as primary and the other as secondary. In case of the failure of the primary LSP, the secondary LSP takes over the traffic, shown in Figure 64.

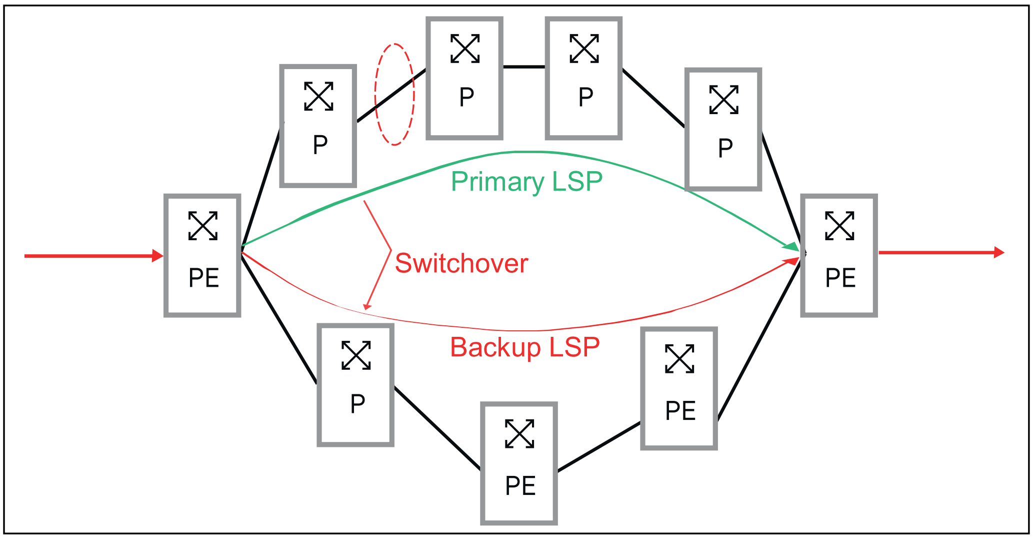


Figure 64 LSP Switchover

BFD over LSP (RFC5884) can be used for end-to-end connectivity monitoring of the primary LSP, enabling a switchover below 50ms.

This feature does not require any specific licenses.

### 12.4.5 BGP Alternate Path Routing

BGP Alternate Path Routing (APR) enables dual-homing of a Cell Site Provider Edge (CS-PE) node to two Switch Site Provider Edge (SS-PE) nodes, see Figure 65. The CS-PE has two routes to a destination and computes a primary and an alternate route to the two SS-PEs. The CS-PE downloads both the primary and alternate routes to the MPLS FTN Table. The alternate BGP remote nexthop is used only if the primary BGP remote nexthop is not reachable. By running multi-hop BFD to monitor the states of the BGP neighbors, the cell site PE can react very quickly to the failure of the primary SS-PE node and switch over to the alternate SS-PE node. Depending on the BFD timer settings, recovery time can be as low as a few 100 milliseconds.

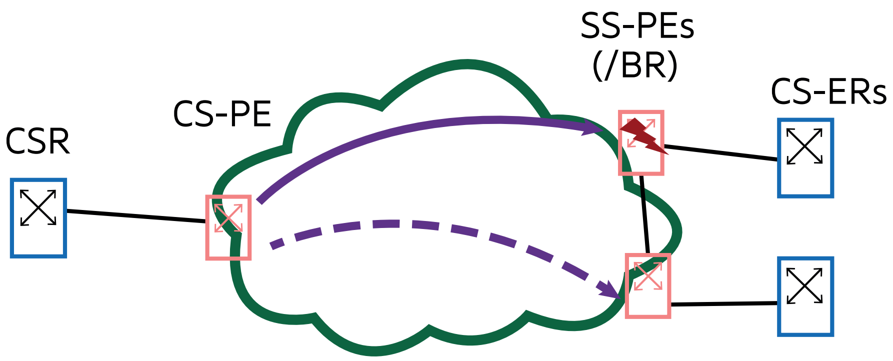


Figure 65 BGP Alternate Path Routing

### 12.4.6 Seamless MPLS

Seamless MPLS offers a solution for extending MPLS across Autonomous Systems. An additional label is added to the MPLS header that is used for label-switching the traffic at AS Border Routers. BGP Labeled Unicast (BGP-LU) is used to distribute label allocations from the AS borders towards the routers in the connected ASs.

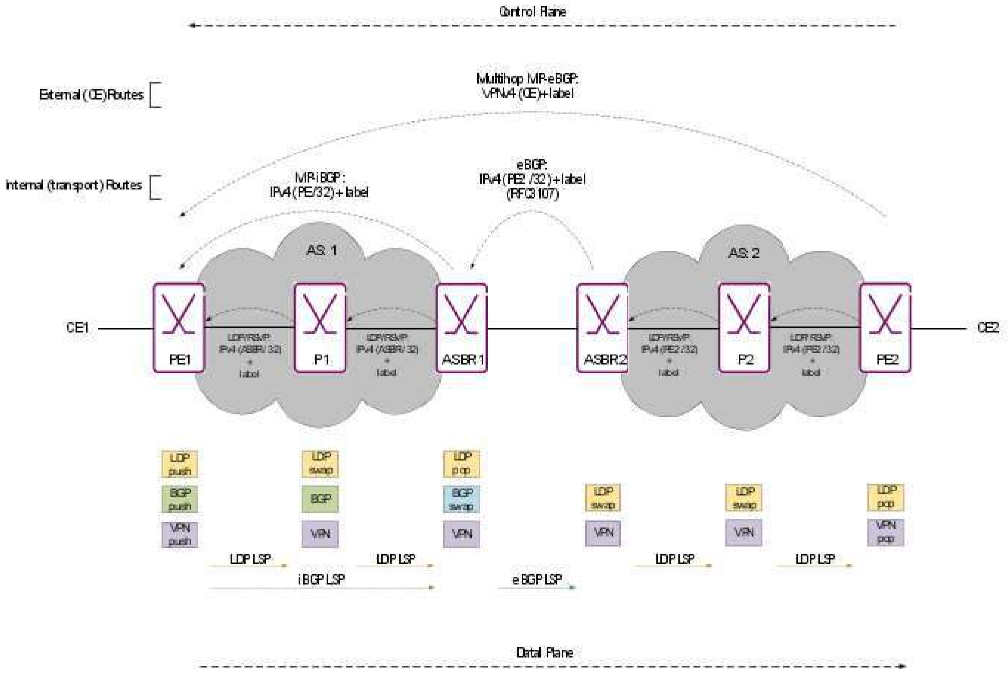


Figure 66 Seamless MPLS

## 12.5 Supported IP Protocols

The NE supports the following IP service protocols:

- **ARP**

  The ARP implementation is consistent with RFC 826, An Ethernet Address Resolution Protocol, also called Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. In addition, the NE provides a configurable ARP entry-age timer and the option to delete expired dynamic ARP entries automatically.

- **BFD**

  The NE supports RFC 5880, BFD. BFD is a simple Hello protocol that is similar to the detection components of some routing protocols. A pair of routers periodically transmits BFD packets over each path between the two routers. If a system stops receiving BFD packets after a predefined time interval, a component in the bidirectional path to the neighboring NE is assumed to have failed. A path is declared to be operational only when two-way communication has been established between the systems. To establish BFD sessions, configure one or more BFD clients on the same interface as BFD. BFD clients are routing protocols, which use BFD events to detect link failures; for example, BFD clients can be BGP, OSPF, and other applications.

- **NTP**

  The NE supports versions 1, 2, and 3 of the Network Time Protocol (NTP). On the NE, NTP operates only in client mode. A remote NTP server can synchronize the NE, but the NE cannot synchronize remote clients.

  **Note:** Before using NTP, the NE must be configured with the IP address of one or multiple NTP servers.

- **DHCP**

  DHCP dynamically leases IP address information to host clients. The NE provides the following DHCP support.

  - DHCPv4 relay server

    The NE acts as an intermediary between an external DHCPv4 server and the client. The NE forwards requests from the client to the DHCPv4 server and relays the responses from the server back to the client.

  - DHCPv6 relay server (only for DCN)

    The NE relays or passes client requests for IPv6 addresses and prefixes to an external server (third-party equipment). The external server then provides the IPv6 addresses or prefixes to the client.

# 13 TDM

MINI-LINK 6600 provides an E1/DS1 traffic routing function that facilitates the handling of PDH traffic aggregation. This function enables interconnection of E1/DS1 traffic connections going through the NE.

Plug-in units connect n×E1/DS1 to the backplane, where the traffic is cross-connected to another plug-in unit. The E1s/DS1s are unstructured with independent timing.

The traffic routing function is configured from MINI-LINK Node GUI, locally or remotely.

**Note:** For MINI-LINK 6651, only E1s for ETSI are supported. No support is available for DS1s (ANSI) or SDH/SONET in MINI-LINK 6651.

MINI-LINK 6600 provides STM-1 interfaces via LTU 1002 for SDH.

## 13.1 TDM Protection Mechanisms

This section describes the protection mechanisms provided by the Basic Node. Protection of the radio link is described in Radio Link.

### 13.1.1 Overview

To ensure high availability, MINI-LINK 6600 provides protection mechanisms on various layers in the transmission network as illustrated in Figure 67.

- Network layer protection using the 1+1 SNCP mechanism provides protection for the sub-network connection **a-b** in Figure 67. Network layer protection uses only signal failure as switching criterion.
- Physical link layer protection using MSP 1+1 indicated by the link **c** between two adjacent NEs **1** and **2** in Figure 67. Physical link layer protection uses both signal failure and signal degradation as switching criteria.
- By routing the protected traffic in parallel through different physical units, equipment protection can also be achieved. An example using two plug-in units is shown for the NEs **1** and **2** in Figure 67.

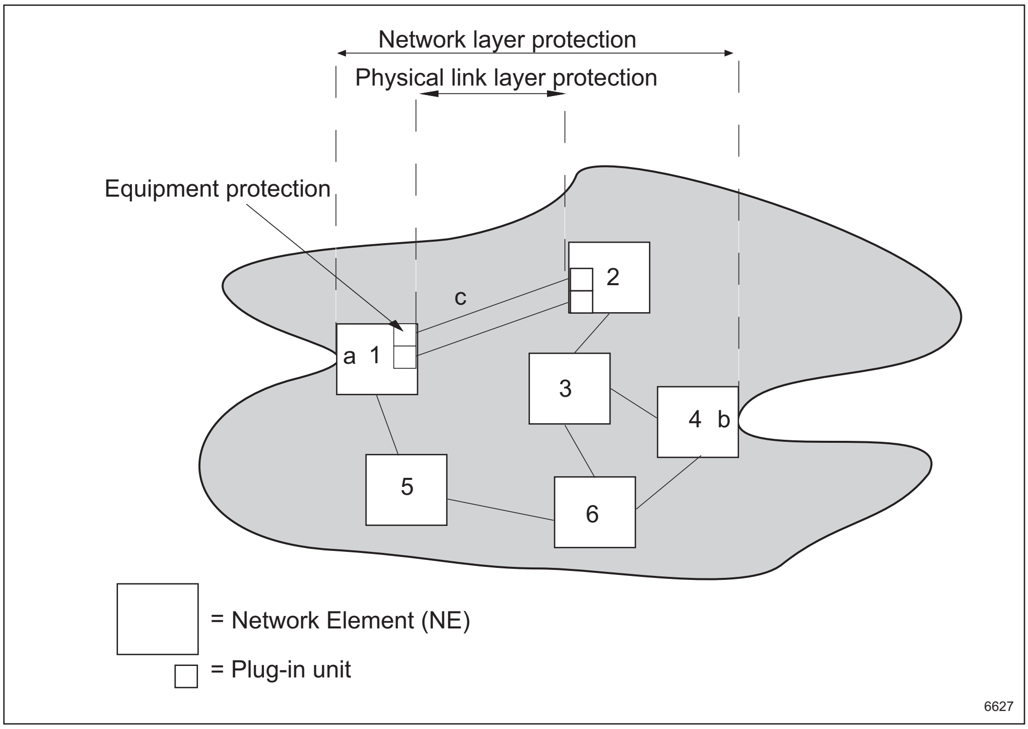


Figure 67 The NE Provides High Availability Through Various Protection Mechanisms

Network layer and physical link layer protection share the following characteristics:

| | |
|---|---|
| **Permanently Bridged** | Identical traffic is transmitted on the active and the passive physical link/connection. |
| **Uni-directional** | Only the affected direction is switched to protection. The equipment terminating the physical link/connection in either end will select which line to be active independently. |
| **Non-revertive** | No switch back to the original link/connection is performed after recovery from failure. The original active link/connection is used as passive link/connection after the protection is reestablished. |
| **1+1** | One active link/connection and one passive (standby) link/connection. |
| **Automatic/Manual switching mode** | In automatic mode, the switching is done based on signal failure or signal degradation. Switching can also be initiated from the management system provided that the passive link/connection is free from alarms.<br>In manual mode, the switching is only initiated from the management system, regardless of the state of the links/connections. |

### 13.1.2 Network Layer Protection

#### 13.1.2.1 1+1 E1/DS1 SNCP

1+1 E1/DS1 Sub-Network Connection Protection (1+1 E1/DS1 SNCP) is a protection mechanism used for network protection on E1/DS1 level, between two NEs. It is based on the simple principle that one E1/DS1 is transmitted on two separate E1/DS1 connections.

The switching is performed at the receiving end where the two connections are terminated. It switches automatically between the two incoming E1s/DS1s in order to use the better of the two. The decision to switch is based on signal failure of the signal received (LOS or AIS).

At each end of the protected E1/DS1 connection, two E1/DS1 connections must be configured to form a 1+1 E1/DS1 SNCP group.

An operator may also control the switch manually.

The connections may pass through other equipment in between, provided that AIS is propagated end-to-end.

The 1+1 E1/DS1 SNCP function is independent of the 1+1 radio protection and the MSP 1+1.

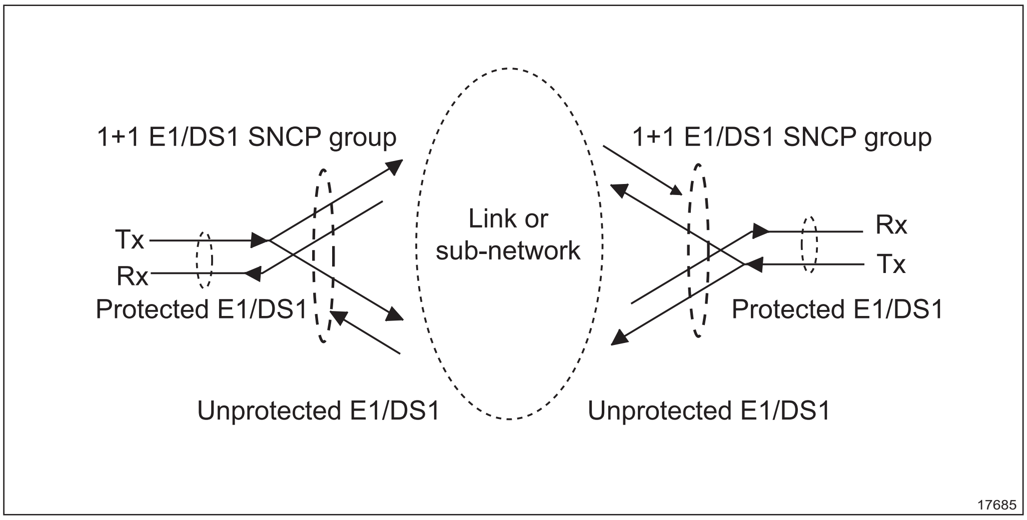


Figure 68 1+1 E1/DS1 SNCP Principle

Performance data is collected and fault management is provided for unprotected as well as protected VC/VT interfaces (that is the 1+1 E1/DS1 SNCP group). This gives accurate information on the availability of network connections.

### 13.1.2.2 Ring Protection for PDH and SDH

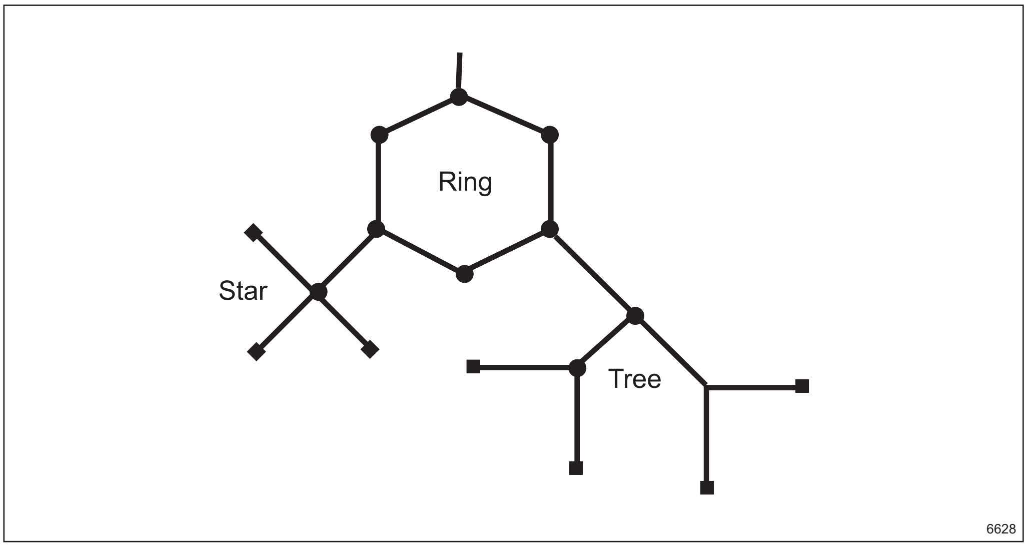


Figure 69 Network Topologies

The 1+1 SNCP mechanism described in the previous section can be used to create protected ring structures in the microwave network. In a ring topology, all nodes are connected so that two nodes always have two paths between them.

A connection entering a ring at one point and exiting at another point can therefore be protected with a 1+1 SNCP group configured at each end of the connection. The traffic is transmitted in both directions of the ring and the traffic is received from two directions at the termination point.

In this solution, the ring network can tolerate one failure without losing transmission. When the failure reoccurs, the affected connections are switched in the other direction.

In a MINI-LINK network, these ring structures can be built using PDH Radio Terminals with capacities of up to 80×2 Mbps, and using SDH Radio Terminals with LTU 1002 with capacities up to 63×2 Mbps.

Capacity is distributed from a common feeder node to the ring nodes where it is dropped off to star or tree structures as shown in Figure 70.

As an example, consider the nodes **A** and **E** in Figure 70. To protect the connection from **A** to **E** the two alternative connections from **A** to **E** must be defined as a 1+1 SNCP group at **A** and as a 1+1 SNCP group at **E**.

Similarly, to protect the connection from **A** to **C**, the two alternative connections between **A** and **C** must also be configured as two 1+1 SNCP groups at **A** and **C**.

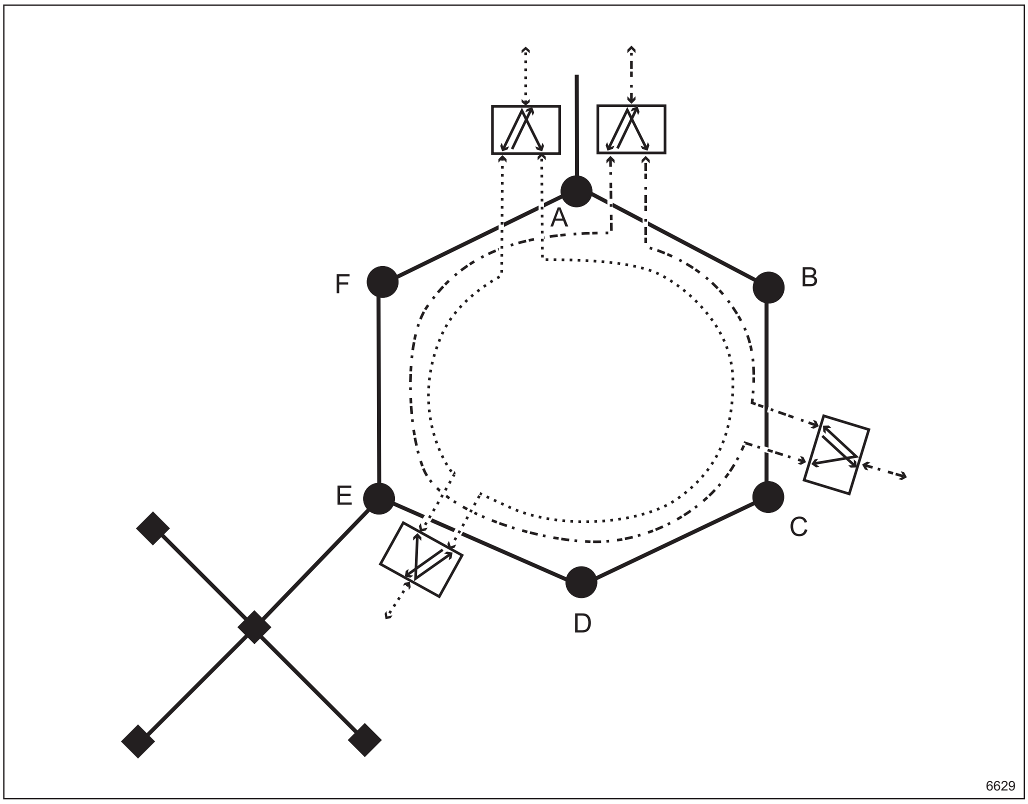


Figure 70 Example of Ring Protection with 1+1 SNCP

The 1+1 SNCP function can be used to build protection in more complex topologies than rings, using the same principle.

### 13.1.3 MSP 1+1 for SDH

**Note:** SDH is only available for ETSI, and not for ANSI (SONET).

The LTU 1002 STM-1 interface supports Multiplexer Section Protection (MSP) 1+1. This SDH protection mechanism provides both link protection and equipment protection. Its main purpose is to provide maximum protection at the interface between the microwave network and the optical network.

MSP 1+1 requires two LTU 1002 plug-in units configured to work in an MSP 1+1 pair, delivering only one set of 63×E1 to the backplane at a time as illustrated in Figure 71. The unit intercommunication is done over the BPI bus.

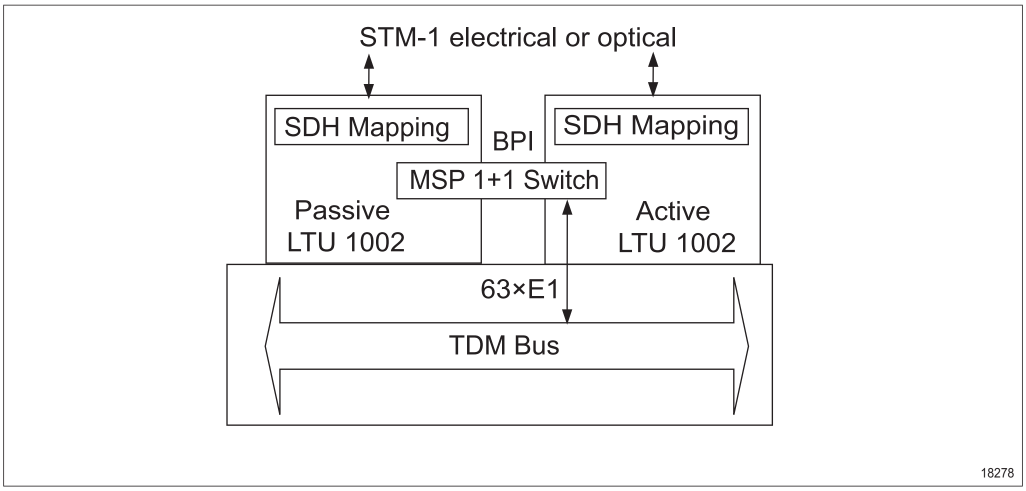


Figure 71 Two LTU 1002 Plug-In Units in an MSP 1+1 Configuration

The switching is done automatically if the following is detected:

- Signal Failure (SF): LOS, LOF, MS-AIS, or RS-TIM
- Signal Degradation (SD) based on MS-BIP Errors (BIP-24)
- Local equipment failure

The operator can also initiate the switching manually.

The switch logic for MSP 1+1 is handled by the Device Processor of the unit.

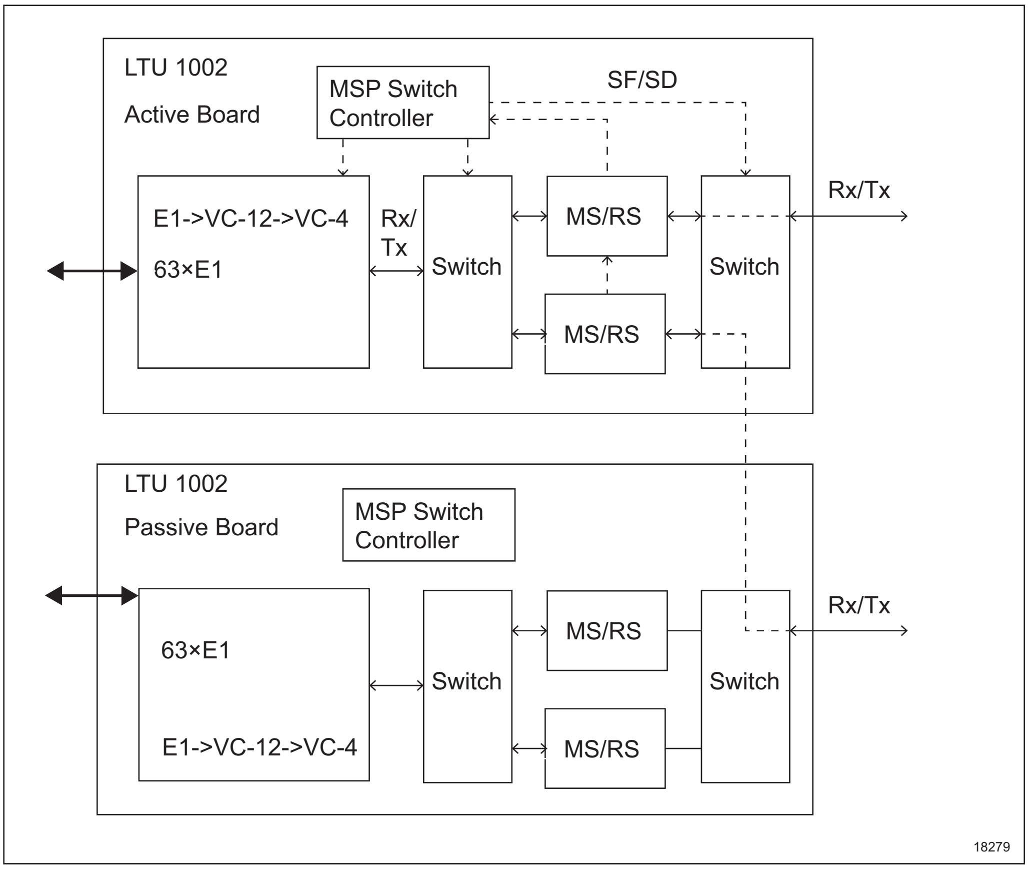


Figure 72 MSP 1+1 Principle for LTU 1002

## 13.2 TDM over Packet using CES

TDM traffic can be transported over Ethernet by using the Circuit Emulation Service (CES).

**Note:** CES is configurable in a MINI-LINK 6600 node that has an LTU 1002 installed or in a MINI-LINK 6651/4 node.

MINI-LINK supports both TDM and packet data transportation, with TDM being more traditional and packet-only networks slowly replacing old TDM or hybrid networks. CES enables a packet-only network to support TDM data transportation, meaning a hybrid network is not required. CES converts traditional TDM traffic at a node to Ethernet traffic and the traffic can then be sent over a packet network.

The MINI-LINK 6600, equipped with an LTU 1002, or the MINI-LINK 6651/4 converts the TDM traffic into a packet format and then it is sent over a Native Ethernet network.

CES adds an additional overhead to all data, due to the specific requirements of packet data.

The following TDM encapsulation mode is provided:

- **Structure Agnostic Model** — The complete E1/DS1 is encapsulated into a pseudowire.

Each TDM interface is transferred in a separate pseudowire. The pseudowires can be transported directly over Ethernet using MEF8 protocol headers. The underlying Ethernet network can operate in Customer Mode or Provider Mode. The customer VLAN tags are set per pseudowire.

LTU 1002 provides CES services with different options depending on the selected LTU 1002 profile. For details on the available board profiles, see Section 15.15 on page 201.

### 13.2.1 Synchronization of TDM Interface

One of the basic tasks of the CES function is to reconstruct the timing on the transported TDM service.

MINI-LINK 6600 supports the following methods to synchronize the TDM transmit clock at one end of the packet network, to the TDM receive clock at the other end of the packet network:

- **Loop Timing Method** — The TDM transmit clock is derived from the received TDM signal. It is required that the TDM network on both sides have access to the same network clock.
- **Adaptive Method** — TDM transmit clock is derived based on the packet arrival rate from the packet network.
- **Network Synchronization Method** — TDM transmit clock is derived from the SEC in network frequency synchronization mode.

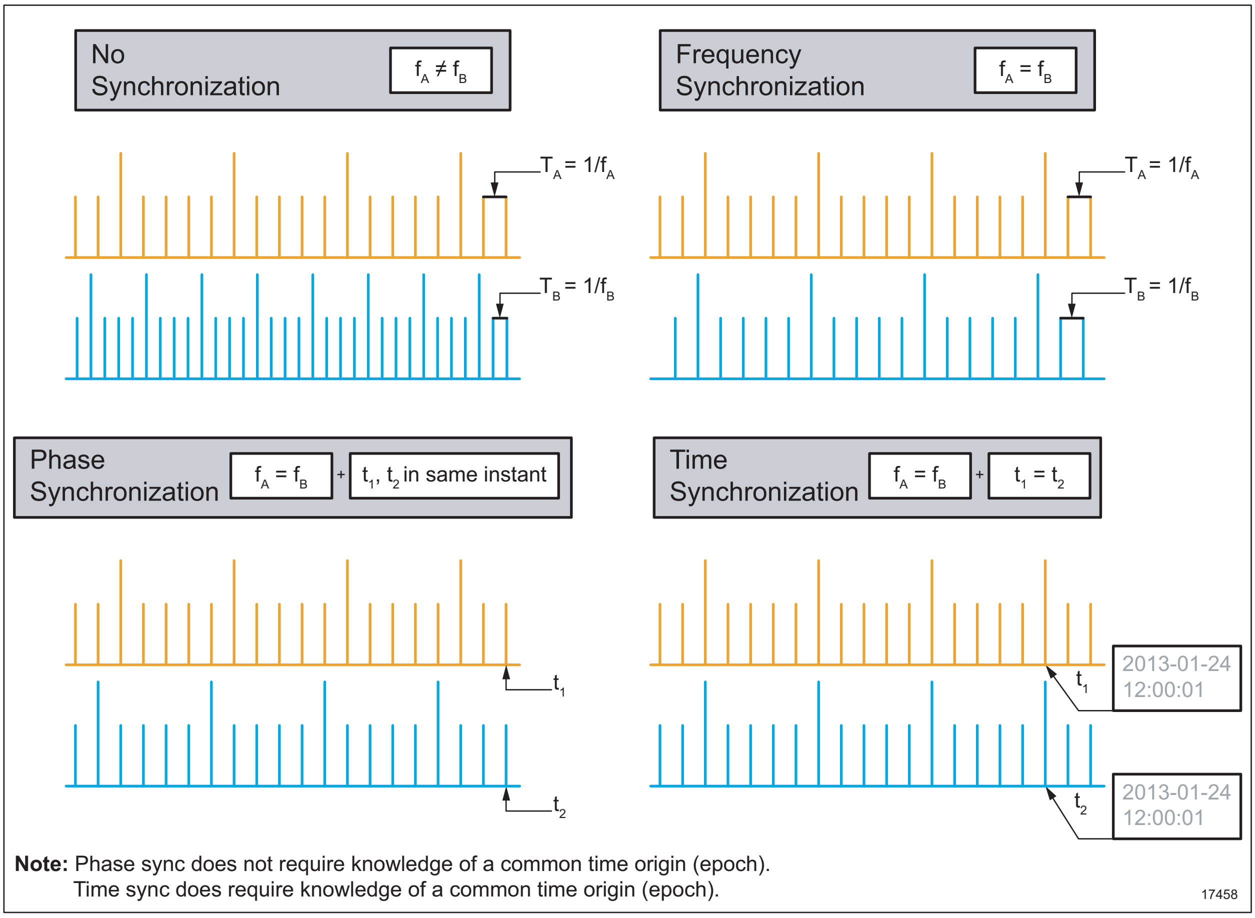
The loop timing and adaptive methods are useful in scenarios when the TDM service has independent timing.

# 14 Synchronization

## 14.1 General Overview

Network synchronization is an important supporting function in telecommunication networks, since proper operation of different transport and radio technologies requires certain type and level of synchronization of the network equipment.

Different synchronization types are described in Figure 73.



**Note:** Phase sync does not require knowledge of a common time origin (epoch).
Time sync does require knowledge of a common time origin (epoch).

Figure 73 Different Synchronization Types

If there is no alignment between the time instances of two system clocks, then the two clocks are not synchronized (Figure 73, top left). If the periodicity (or rate of change) of the clock instances in two systems are equal, then the two clocks are frequency synchronized (Figure 73, top right). Phase synchronization means that time instances of the two remote system clocks occur at exactly the same time, but absolute time is not known by the systems, so their significant instances may be unaligned (Figure 73, bottom left). In case absolute time information is assigned to each time instance of the clocks and they are aligned, then the two clocks are time synchronized (Figure 73, bottom right).

Though phase and time synchronization do not exactly mean the same, they are usually used interchangeably in synchronization terminology and it always means time synchronization in telecommunication networks.

Frequency synchronization is required by TDM-based transport networks and FDD-based radio technologies (GSM, WCDMA, LTE-FDD, and so on), while time synchronization is required by some advanced radio technologies (LTE-TDD, eMBMS, and so on).

In MINI-LINK, frequency synchronization is handled by the Netsync function, that contains a Synchronous Equipment Timing Generator (SETG). The SETG can be frequency synchronized to any physical interface that can carry synchronization. The recovered clock is handed over to the Frequency synchronization function as frequency reference interface. Out of all potential synchronization reference interfaces, four interfaces can be selected to be connected to the synchronization source selection logic.

Time synchronization is provided by the PTP described in the IEEE1588-2008 standard. It can be used in G.8275.1 profile mode, and it synchronizes the Real Time Clock (RTC) of the node to an external time reference through exchange of PTP packets supported by HW timestamping. Time synchronization function relies on stable clock frequency that is provided using the Netsync function based on physical layer frequency synchronization signals. Therefore it is also prerequisite to enable and lock the Netsync function to a Primary Reference Clock (PRC)/Primary Reference Source (PRS) traceable synchronization signal before time synchronization is activated.

Since the PTP function communicates over standard traffic interfaces it is a prerequisite to create the traffic configuration of the interfaces that are intended for PTP usage.

Figure 74 shows the node operation when PTP is configured in G.8275.1 profile and time recovery is supported by the frequency synchronization function.

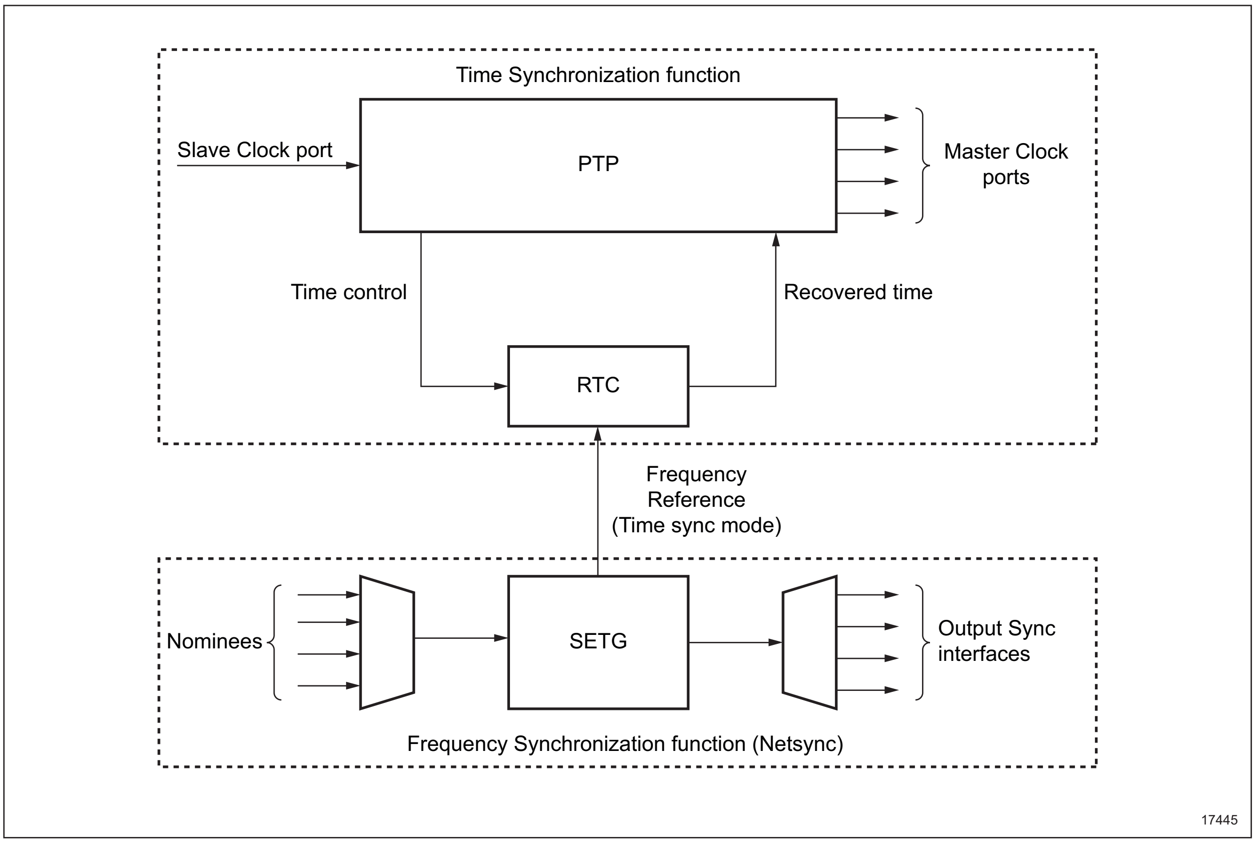

Time Synchronization function
Slave Clock port
PTP
Master Clock ports
Time control
Recovered time
RTC
Frequency Reference (Time sync mode)
Nominees
SETG
Output Sync interfaces
Frequency Synchronization function (Netsync)
17445

Figure 74 G.8275.1 Node Time Synchronization

## 14.2 Frequency Synchronization Technologies

MINI-LINK 6600 supports the following frequency synchronization functions:

- Sync over Radio Link
- Synchronous Ethernet
- Sync over SDH (only for ETSI)
- Sync over PDH
- Sync over 2 MHz/2048 kbps
- Sync over PTP (G.8265.1 Mode)

### 14.2.1 Sync over Radio Link

Quality Level (QL) is communicated over radio link side channel in order to support QL based reference selection.

### 14.2.2 Synchronous Ethernet

Synchronous Ethernet is supported on the various interfaces as shown in Table 11.

Table 11 SyncE Support on Ethernet Interfaces

| | **Interface** | | | | | |
|---|---|---|---|---|---|---|
| **Unit** | **LAN RJ45 100 Mbps** | **LAN RJ45 1 Gbps** | **LAN SFPo 1 Gbps** | **LAN SFPo 2.5 Gbps** | **LAN SFPo 10 Gbps** | **LAN SFPe** |
| NPU 1002 | Yes | Yes | Yes | No | Yes | No |
| NPU 1003 | Yes | Yes | Yes | No | Yes | No |
| NPU 1005 | Yes | Yes | Yes | No | Yes | No |
| PNM 1001 | Yes | Yes | Yes | No | Yes | No |
| PNM 1002 | Yes | Yes | Yes | No | Yes | No |
| ETU 1001 | Yes | Yes | – | – | – | – |
| ETU 1002 | – | – | Yes | – | Yes | – |
| MINI-LINK 6651/1, 6651/2, or 6651/3 | Yes | Yes | Yes | Yes | – | No |
| MINI-LINK 6651/4 | Yes | Yes | Yes | – | Yes | No |

Synchronous Ethernet enables propagation of frequency synchronization clock over Ethernet interfaces. It also supports QL communication using Ethernet Synchronization Status Message (ESMC) messages according to ITU-T G.8264. The ESMC handling can be disabled for interfaces in order to provide interoperability to other equipment that do not support the ESMC protocol.

**Note:** Disabling ESMC handling is not recommended and such usage is under the responsibility of the operator.

The terms “ESMC” and “Synchronization Status Message (SSM)” are used interchangeably in the Synchronous Ethernet context in MINI-LINK documentation.

### 14.2.3 Sync over SDH

**Note:** Sync over SDH is not available for MINI-LINK 6651.

**Note:** LTU 1002 is required for MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, or MINI-LINK 6694 with NPU 1002, NPU 1003, or NPU 1005.

Frequency synchronization over SDH requires termination of the STM-1 in an LTU 1002.

Quality Level (QL) is communicated over SDH interfaces using Synchronization Status Message (SSM) in order to support QL based reference selection.

It is not supported to use a PDH carried inside an STM-1 as a sync source. The recommendation is to use the STM-1 as sync source instead.

### 14.2.4 Sync over PDH

**Note:** LTU 1001 or LTU 1002 is required for MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, or MINI-LINK 6694 with NPU 1002 or NPU 1005.

**Note:** Sync over PDH is not available for MINI-LINK 6651.

Any E1/DS1 interface can be used as frequency reference source.

E1s/DS1s are cross-connected transparently, that is the clock frequency on the outgoing E1/DS1 interface will always follow the clock frequency of its relevant E1/DS1 input.

QL forwarding on PDH interfaces is not supported. It is configurable to Squelch (AIS) outgoing PDH interfaces when frequency synchronization fails.

It is not supported to use a PDH carried in an STM-1 as a sync source. The recommendation is to use the STM-1 as sync source instead.

### 14.2.5 Sync over 2 MHz/2048 kbps

Sync over 2 MHz/2048 kbps is supported on the various interfaces as shown in Table 12.

Table 12 Sync over 2 MHz/2048 kbps Support

| Unit | 2 MHz/2048 kbps |
|---|---|
| NPU 1002 | Yes |
| NPU 1003 | Yes |
| NPU 1005 | Yes |
| PNM 1001 | Yes |
| PNM 1002 | Yes |
| MINI-LINK 6651 | No |

The synchronization clock signal can be connected to external units by connecting the external units directly to an arbitrary 2 MHz/2048 kbps port. This can be used in the peripheral parts of the network where an RBS is connected to a MINI-LINK 6600.

QL forwarding on 2 MHz/2048 kbps interface is not supported. It is configurable to Squelch (AIS) outgoing signal when frequency synchronization fails.

### 14.2.6 Sync over PTP (G.8265.1 Mode)

On NPU 1002, NPU 1003, NPU 1005, PNM 1001, PNM 1002, and MINI-LINK 6651, the PTP protocol can be used to provide frequency synchronization of multiple slaves to a grandmaster according to the ITU-T G.8265.1 profile using UDP/IPv4 unicast transport. This profile does not require any PTP support from the network between the master and the slave. This means that transport nodes along the PTP packet path do not need to be aware of or to support the PTP protocol. However, when setting up a network for packet-based frequency synchronization following the G.8265.1 profile, the 1588 packets must be given the highest prioritization in the QoS hierarchy to minimize the packet delay variation of the PTP packets.

If the NE is configured as a frequency grandmaster, the frequency of the SETG clock is distributed.

If the NE is configured as a packet slave, the PTP recovered frequency is a candidate for the frequency synchronization source selection. In this profile, the delay request-response mechanism in two-way message exchange is supported. Peer-to-Peer operation is not supported.

The NE sends PTP event messages in one-step mode, while both one-step and two-step messages are accepted and processed properly. The only allowed encapsulation in this profile is IP unicast.

IP host functionality of the PTP entity is handled by the port-based L3 subinterfaces in the NE. The exact routing of the G.8265.1 PTP messages is determined by the L3 routing stack. The VLAN encapsulation is also determined by the L3 subinterface configuration.

**Note:** Only IPv4 is supported.

Only clock type Ordinary Clock (OC) is supported. Slave mode consists of a Single Slave-only OC (SOOC) instance.

To maximize the performance of the frequency synchronization, it is beneficial to forward the frequency by microwave link function, SyncE, PDH/SDH, or 2MHz inside the transport domain and hand the frequency over by G.8265.1 profile only at the edges of the transport domain, as it is shown in Figure 75. For this reason, G.8265.1 OC is supported only through LAN ports. On microwave links, the standard Netsync frequency forwarding is supported.

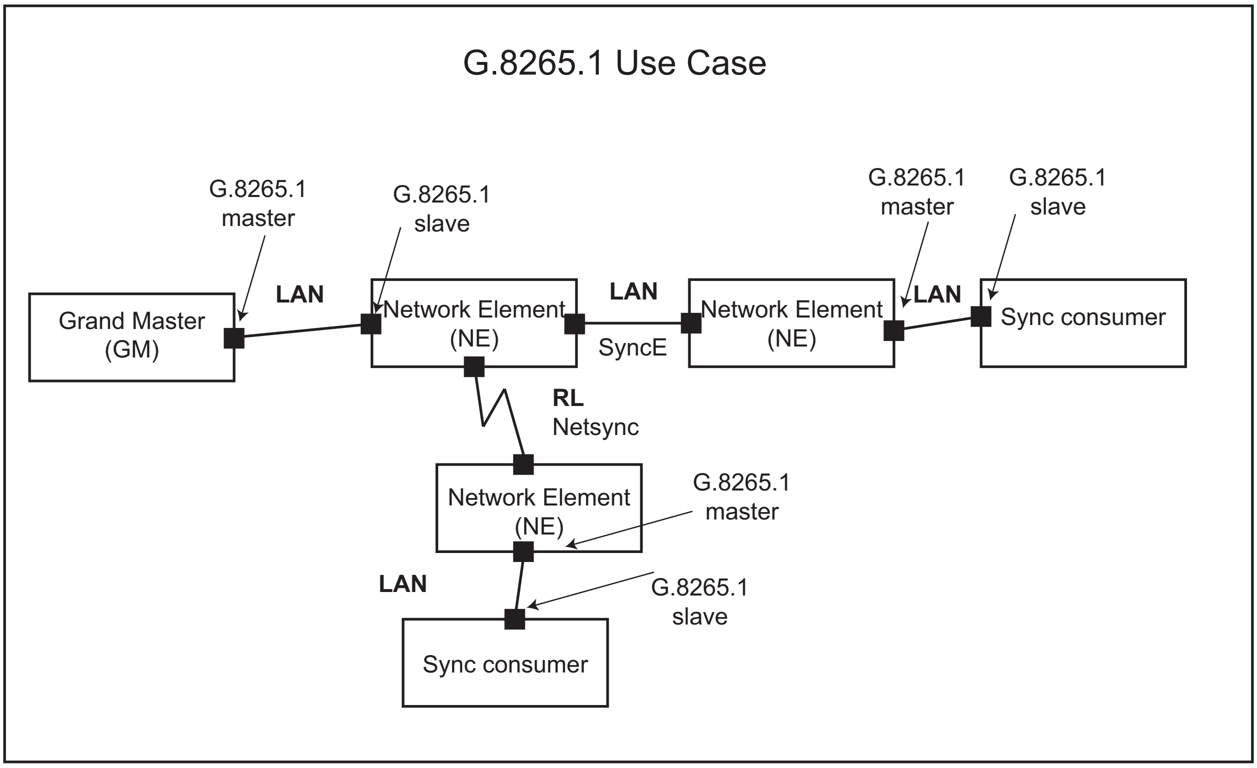


Figure 75 G.8265.1 Use Case

## 14.3 Time Synchronization Technologies

The time synchronization device is the Precision Time Protocol (PTP) entity that can receive packet based synchronization signal from any PTP capable interface, and can distribute the time synchronization information over any PTP capable interface or 1PPS/ToD output.

**Note:** The 1PPS/ToD interface is available on NPU 1002, NPU 1003, NPU 1005, PNM 1001, and PNM 1002.

To synchronize time via PTP, MINI-LINK 6600 requires a PRC/PRS-traceable frequency from the Frequency Synchronization function that is recovered from an L1 (non-PTP) source, for example Synchronous Ethernet or Sync over Radio Link, as described in the previous chapter.

When setting up a network for time synchronization, it is essential to configure PTP support throughout the synchronization path. In addition the PTP packets shall be given the highest prioritization in the QoS hierarchy in order to avoid PTP packet loss on congested links.

IEEE1588-2008 standard provides the general framework for packet-based time synchronization, including Boundary Clock (BC), Ordinary Clock (OC), and Transparent Clock (TC). However, in order to meet the functional and performance requirements of a certain application, further requirements defined in a so called “profile” need to be supported as well. Applicable performance requirements are defined in ITU-T G.8273.2 for telecom devices, and in G.8271.1 for end-to-end network limits.

### 14.3.1 Default PTP Profile

PTP can be used to provide time synchronization according to the IEEE1588-2008 Annex J using Ethernet multicast transport. This profile assumes full network timing support from the network. This means that all transport nodes along the time synchronization chain from the grandmaster to the end application must support PTP.

In this profile, MINI-LINK 6600 supports the delay request-response mechanism in two-way message exchange. Peer-to-Peer operation is not supported.

MINI-LINK 6600 sends PTP event messages in one-step mode, while both one-step two-step messages are accepted and processed properly.

Default encapsulation for MINI-LINK 6600 is Ethernet multicast. MINI-LINK 6600 always sends packets with the forwardable multicast address, while both the forwardable (01-1B-19-00-00-00) and the non-forwardable (01-80-C2-00-00-0E) multicast addresses are accepted. Ethernet unicast can also be configured.

MINI-LINK 6600 supports PTP packet exchange in Customer and Provider Bridge modes.

The following VLAN tagging options are supported for the default PTP profile:

- No VLAN tag
- Single VLAN tag (Customer mode, or Provider mode with S-tag only)
- Double VLAN tags (Provider mode with both S-tag and C-tag)

The following clock types are supported for the default PTP profile:

- Boundary Clock (BC)
- Ordinary Clock (OC)
- Transparent Clock (TC)

A PRC/PRS-traceable frequency from the Frequency Synchronization function that is recovered from an L1 (non-PTP) source is required in all operation modes.

In TC mode the node does not terminate the PTP protocol, just compensates for the residence time within the node of each PTP packet. The node clock is not synchronized in time, but is required to be synchronized in frequency via a physical layer technology.

### 14.3.2 ITU-T G.8275.1 Profile

PTP can be used to provide time synchronization according to the ITU-T G.8275.1 profile. This profile assumes full network timing support from the network. This means that all transport nodes along the time synchronization chain from the grandmaster to the end application must support PTP in G.8275.1 profile.

In this profile, MINI-LINK 6600 supports the delay request-response mechanism in two-way message exchange. Peer-to-Peer operation is not allowed in this profile.

MINI-LINK 6600 sends PTP event messages in one-step mode, while both one-step and two-step messages are accepted and processed properly.

The only allowed encapsulation in this profile is Ethernet multicast. MINI-LINK 6600 sends by default packets with the forwardable address, and non-forwardable packet sending can also be configured. Both the forwardable (`01-1B-19-00-00-00`) and the non-forwardable (`01-80-C2-00-00-0E`) multicast addresses are accepted.

MINI-LINK 6600 supports PTP packet exchange in Customer and Provider Bridge modes.

The following VLAN tagging options are supported for the ITU-T G.8275.1 profile:

- No VLAN tag
- Single VLAN tag (Customer mode, or Provider mode with S-tag only)
- Double VLAN tags (Provider mode with both S-tag and C-tag)

The following clock types are supported for the ITU-T G.8275.1 profile:

- Telecom Boundary Clock (T-BC)
- Telecom Time Slave Clock (T-TSC)
- Telecom Transparent Clock (T-TC)

A PRC/PRS-traceable frequency from the Frequency Synchronization function that is recovered from an L1 (non-PTP) source is required in all operation modes.

### 14.3.3 Time Error Generation

Timing characteristics requirements for Telecom Boundary Clocks and Telecom Slave Clocks are defined in G.8273.2 standard for networks with full timing support. The standard defines limits for maximum absolute time error (max|TE|), permissible range of constant time error (cTE), and dynamic time error (dTE).

Table 13 Performance Categories of the Recovered Clock

| [ns] | T-BC Class B (G.8273.2)(1) | 1G LAN(2)(3)(4) | 10G LAN(2)(3)(4) | Radio Link(5) |
|---|---|---|---|---|
| max\|TE\| | 70 | 70 | 70 | 70 |
| Range of cTE | ±20 | ±20 | ±20 | ±20 |
| dTE | 40 | 40 | 40 | 40 |

(1) ITU-T G.8273.2 is supported, except for clause 7.2.

(2) Timestamping in FE is not supported.

(3) SFP interfaces are validated only with officially supported SFP types. Performance is not guaranteed with 3rd party SFP types that is not on the official Ericsson list.

(4) While 1588 timestamping is supported on any type of SFPs, Synchronous Ethernet – which is prerequisite for phase synchronization – is not supported on electrical SFPs. However, 1588 phase synchronization in general can work, in case network synchronization is provided to the node over any other interface.

(5) For supported HW, see the compatibility document in the Planning folder

## 14.4 Precision Time Protocol

This chapter summarizes the general aspects of packet based synchronization based on the IEEE1588-2008 protocol.

IEEE Std 1588™-2008 is a standard for packet-based network synchronization that is suitable both for frequency and time synchronization. It describes hierarchical master-slave architecture for clock distribution. The title of the standard is Precision Time Protocol (PTP), and so the terms IEEE1588 and PTP are used interchangeably to refer to the standard and the protocol.

The standard defines different clock types, that are embedded into network elements and provides synchronization function to the devices. These devices maintain various data sets that describe clock device and clock signal properties. The clock devices exchange these data sets information that allows each device to identify peer clocks and autonomously decide master-slave hierarchy. When master-slave relationships are established, clocks start to periodically exchange timing messages that are used to maintain synchronization of the device clocks.

The protocol has the following operational phases in the normal execution of the protocol:

- Network configuration

  Transport network and IEEE1588 clocks need to be configured according to required application in order to provide connectivity between clock devices.

- Establishing master-slave hierarchy

  Clocks start to exchange clock quality information, run the reference selection algorithm locally and automatically decide on synchronization topology

- Synchronizing the clocks

  Clocks start to exchange time event messages and perform clock synchronization.

If there is a change in the network topology, clock states, or performance, the master-slave hierarchy is automatically re-established, which may lead to re-synchronization of clocks.

IEEE1588 standard defines the framework for packet-based network synchronization in general and does not restrict the usage for any application, as well as does not define any performance requirements that would be needed for certain applications. Instead it defines the concept of Profile, which – within the framework of the standard – allows organizations to specify certain parameter subsets and operational requirements that are needed to achieve proper performance of certain applications. A PTP profile is a set of required options, prohibited options, and the ranges and defaults of configurable attributes.

ITU-T defined several standards that provide detailed requirements for packet-based network synchronization for telecommunication networks including definition of terminology, network-level requirements, clock definitions with performance levels, and profiles.

In order to support IEEE1588-2008 packet-based synchronization in any supported profile, MINI-LINK 6600 requires at least an NPU (acting as clock device) and time stamping capable interfaces such as LAN and WAN ports.

If time recovery is active, MINI-LINK 6600 can jump to phase/time holdover state in order to maintain the accurate time information. The prerequisite of phase holdover is that MINI-LINK 6600 previously was in phase locked state and the underlying frequency synchronization is stable. The period of holdover time is configurable from 0 to infinite.

In MINI-LINK 6600 all Ethernet interfaces support time stamping except LAN RJ45 ports running at 10 Mbps or 100 Mbps.

Table 14 summarizes the 1PPS/ToD interface availability.

Table 14 1PPS/ToD Support

| | **1PPS/ToD input** | **1PPS/ToD output** |
|---|---|---|
| NPU 1002 | HW prepared | Yes |
| NPU 1003 | HW prepared | Yes |
| NPU 1005 | HW prepared | Yes |
| PNM 1001 | HW prepared | Yes |
| PNM 1002 | HW prepared | Yes |
| MINI-LINK 6651 | HW prepared | HW prepared |

# 15 Hardware

## 15.1 MINI-LINK 6651

MINI-LINK 6651 is a compact node with a dual carrier modem, suitable for tail sites.

It has a replaceable Fan Unit (FAU) that provides cooling for the indoor part.

There are four variants, MINI-LINK 6651/1 (Figure 76), MINI-LINK 6651/2 (Figure 77), MINI-LINK 6651/3 (Figure 78), and MINI-LINK 6651/4 (Figure 79).

MINI-LINK 6651/2 and MINI-LINK 6651/4 supports the dual directions configuration option.

MINI-LINK 6651/3 is single carrier (only `1+0` is possible) and has no fan unit.

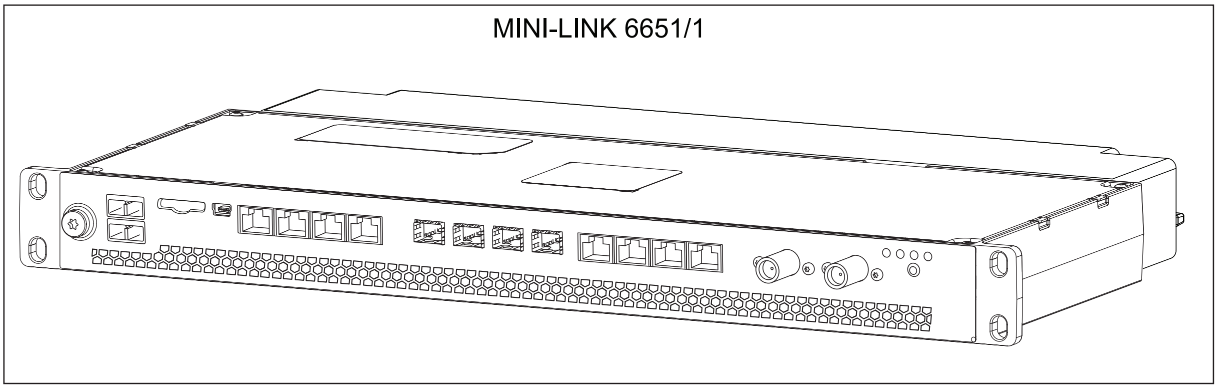


Figure 76 MINI-LINK 6651/1

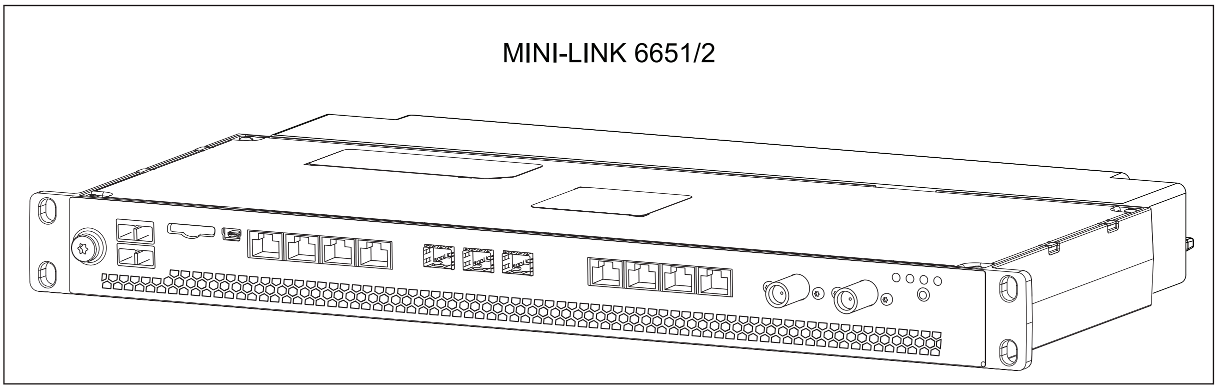


Figure 77 MINI-LINK 6651/2

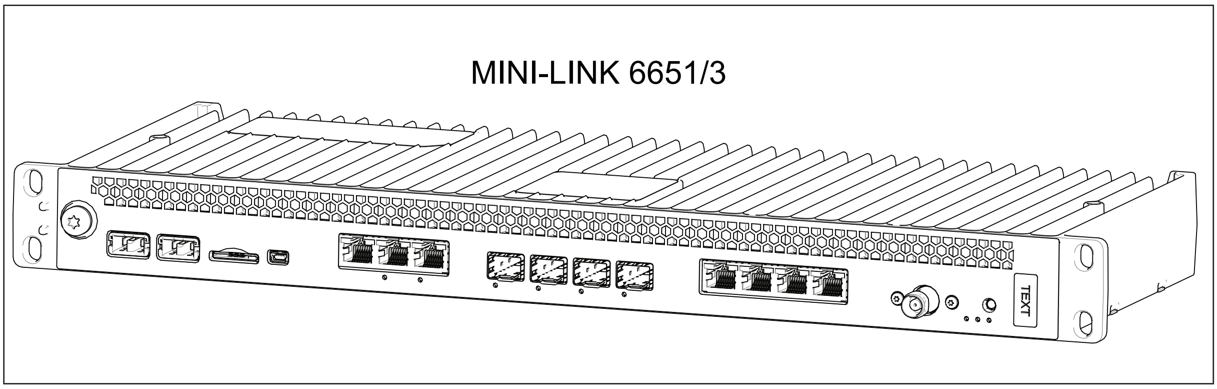


Figure 78 MINI-LINK 6651/3

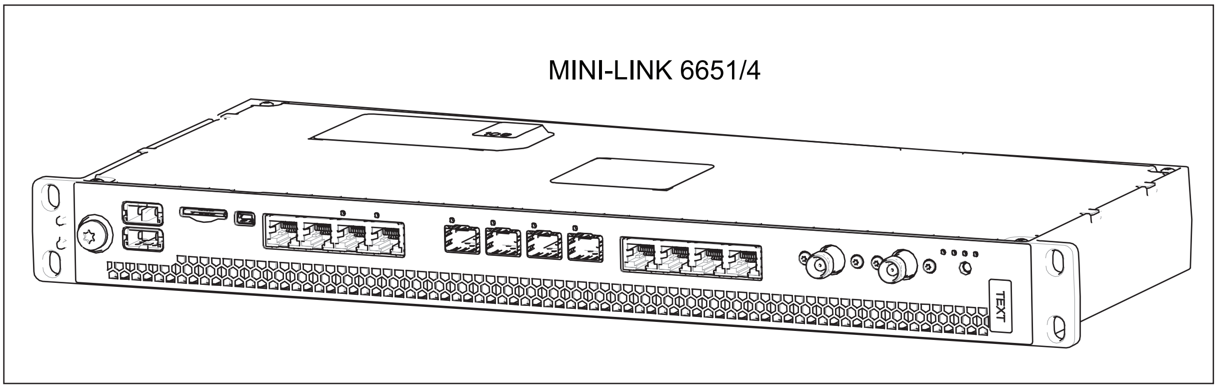


Figure 79 MINI-LINK 6651/4

MINI-LINK 6651 can be fitted in a standard 19" or metric rack. The height of a MINI-LINK 6651 is 1U.

MINI-LINK 6651 has a dual carrier modem supporting Single WAN `1+0`, `2+0`, or `1+1`. MINI-LINK 6651/2 and MINI-LINK 6651/4 also supports Dual WAN `2x(1+0)`.

1+1 Radio Link Protection (RLP) is supported.

The dual carrier in MINI-LINK 6651 can be configured in different ways:

- Single Direction `1+0`

  Supported by MINI-LINK 6651/1, MINI-LINK 6651/2, MINI-LINK 6651/3, and MINI-LINK 6651/4.

- Dual Directions

  When configured as a `1+0` dual directions link, each carrier has its own connection to a switchport and both carriers can optionally be configured as a Hybrid radio link, that is combining TDM and Ethernet traffic on the same radio path.

  Supported by MINI-LINK 6651/2 and MINI-LINK 6651/4.

- Bonded Single Direction

  When configured as a bonded single direction link, the capacity of the two carriers are combined and only one switchport is used.

  Supported by MINI-LINK 6651/1, MINI-LINK 6651/2, and MINI-LINK 6651/4.

- Protected Single Direction

  When configured as 1+1 Radio Link Protection, both carriers are used for Radio Link path protection, and a single switchport is used.

  Supported by MINI-LINK 6651/1, MINI-LINK 6651/2, and MINI-LINK 6651/4.

MINI-LINK 6651 has a high-capacity PDH/Ethernet modem with support for XPIC (including XPIC Recovery and Restore), see Section 3.9 on page 28, Adaptive Coding and Modulation (ACM), see Section 3.2 on page 13, and modulation schemes up to 4096 QAM.

MINI-LINK 6651 supports Radio Link Bonding (RLB), see Section 3.5 on page 18.

MINI-LINK 6651 provides physical layer Sync over Radio Link.

MINI-LINK 6651 enables Ethernet transport over a radio hop, that is, a Packet Link. MINI-LINK 6651 uses the high speed connections to communicate with the Ethernet switch on the NPU boards.

MINI-LINK 6651 carries PDH traffic and have an interface to the TDM bus. The capacity split between packet and circuit transport is configured individually per MINI-LINK 6651.

MINI-LINK 6651 supports control of the ratio between Ethernet and PDH traffic sent over Hybrid Radio Links. The Ethernet part of the aggregated capacity is set with E1 granularity.

MINI-LINK 6651/4 supports CES, enabling E1s being transported over packet. The following board profiles can be set for MINI-LINK 6651/4:

| | |
|---|---|
| **PDH only** | Provides 8×E1s through the front LAN port and 16×E1s over the radio. |
| **CES only** | Provides 8×CES E1s transported over packet. |

MINI-LINK 6651 supports the following Ethernet-related features:

- Store and forward MAC (IEEE802.1D-2004) and VLAN-based switching (IEEE802.1Q-2005 and IEEE802.1ad-2005).
- Port-based VLAN (up to 1,000 VLANs in the range of 1–4094).
- MAC address table (32,000 entries) with learning and aging.

- IPv4 and IPv6
- Static unicast/multicast routes.
- Jumbo frames for LAN and Packet Link WAN ports.
- Multiple internal Layer 1 and Layer 2 Ethernet connections.
- MSTP/RSTP/LAG protection mechanism.
- Link Aggregation Control Protocol (LACP).
- Link Loss Forwarding for internal Layer 1 connections.
- Policing/color marking per ingress port with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress port per QoS priority with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress port per VLAN with CIR/EIR and CBS/EBS.
- Traffic shaping per egress port with CIR and CBS.
- Ethernet loop detection.
- Broadcast/multicast/destination lookup failure storm protection.
- Frame admission control.
- Classification/tagging of priority and VLAN ID.
- Congestion handling with eight priority queues (TC) per port.
  - Frame discard: WRED, color dropping, aging and tail drop.
  - TC scheduling: SP, WDRR.
- In-band management transport in Ethernet flow (DCN over VLAN).
- Management/diagnostics.
  - PM counters.
  - Link OAM.
  - Ethernet Service OAM.
  - Port mirroring.

MINI-LINK 6651/1 provides the interfaces presented in Figure 80.

MINI-LINK 6651/2 provides the interfaces presented in Figure 81.

MINI-LINK 6651/3 provides the interfaces presented in Figure 82.

MINI-LINK 6651/4 provides the interfaces presented in Page 131.

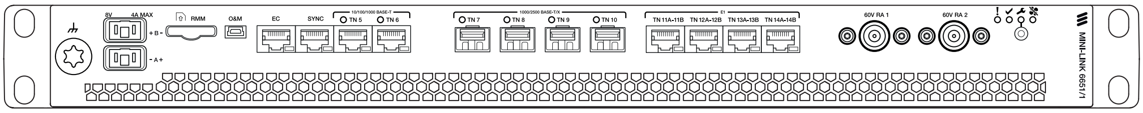


Figure 80 MINI-LINK 6651/1 Front Interfaces

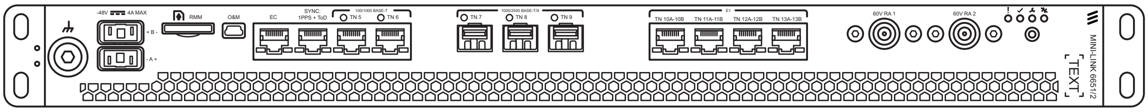


Figure 81 MINI-LINK 6651/2 Front Interfaces

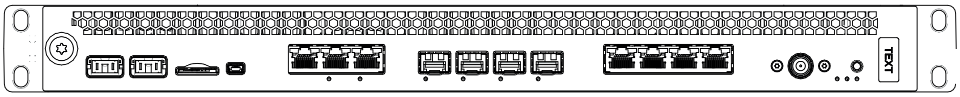


Figure 82 MINI-LINK 6651/3 Front Interfaces

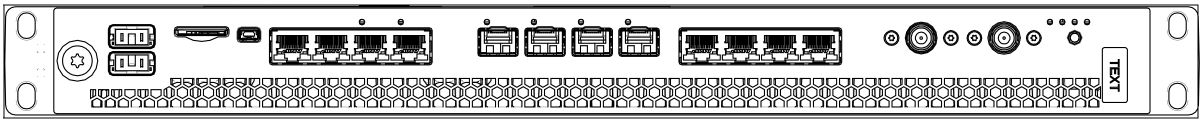


Figure 83 MINI-LINK 6651/4 Front Interfaces

### PDH Traffic Interfaces

The front panel provides 8×E1 interfaces (4×(2×E1)) configured to 120 Ohm.

**Note:** Only E1s for ETSI are supported. No support is available for DS1s (ANSI) in MINI-LINK 6651.

### Ethernet Traffic Interfaces

The front panel at MINI-LINK 6651/1 and MINI-LINK 6651/3 provides two fixed electrical 10/100/1000 BASE-T Ethernet interfaces and four 1000/2500BASE-T/X SFP+ interfaces. One of the fixed Ethernet ports can be configured as a site LAN port.

The front panel at MINI-LINK 6651/2 provides two fixed electrical 10/100/1000 BASE-T Ethernet interfaces and three 1000/2500BASE-T/X SFP+ interfaces. One of the fixed Ethernet ports can be configured as a site LAN port.

The front panel at MINI-LINK 6651/4 provides two fixed electrical 10/100/1000 BASE-T Ethernet interfaces and four 1000/10GBASE SFP/SFP+ interfaces.

All 1000/2500BASE-T/X SFP+ interfaces are both electrical and optical.

The SFP/SFP+ cages can be equipped with Ericsson approved SFP/SFP+ modules, see MINI-LINK 6600 R1 Compatibility, Reference [1].

For the basic offering for MINI-LINK 6651, two Ethernet ports are enabled at the front. To get access to more ports, licenses are needed.

The high speed connections and the LAN ports enable MINI-LINK 6651 to aggregate traffic from multiple directions as well as dropping Ethernet traffic locally at the site.

MINI-LINK 6651 supports Packet Link WAN connections.

### User Input/Output

Table 15 MINI-LINK 6651/4 User Input and Output Ports

| Compact Node | Number of Input Signals | Number of Output Signals | Connector Type |
|---|---|---|---|
| MINI-LINK 6651/4 | Two | One | RJ-45 connector |

### O&M Interface

A USB interface for an alternative MINI-LINK Node GUI connection is available.

### RMM Interface

A SIM card slot is available for a Removable Memory Module (RMM).

### Radio Interface

The front panel on MINI-LINK 6651/1, 6651/2, and 6651/4 provides two 60 V RAU connectors.

The front panel on MINI-LINK 6651/3 provides one 60 V RAU connector.

**Note:** The coaxial interface on modems and radios is equipped with built-in gas discharge tubes for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

### Power

MINI-LINK 6651 provides two −48V DC connectors for power redundancy. Power redundancy is possible by using two external power sources, each of them connected to one of the two DC connectors on the MINI-LINK 6651 unit, through a dedicated power cable.

### Radio Cables

The radio cables connecting the Radio with MINI-LINK 6651 are available in the following three diameters:

- Ø 7,6 mm, with lengths up to 100 m.

This cable can be directly connected to the MINI-LINK 6651.

- Ø 10 mm, with lengths between 100 and 200 m.
- Ø 16 mm, with lengths between 200 and 400 m.

### 15.1.1 DC Supply Voltage

**Normal service voltage range**

The system is able to run at full operation in this range.

**Abnormal service voltage range**

No function is guaranteed, but no permanent damage will occur when operated in this range.

The system is restored to full operation when returning to normal service voltage range.

Table 16 DC Supply Voltage Ranges

| Nominal voltage | −48 VDC |
|---|---|
| Normal service voltage range | −58.8 V to −40 V |
| Abnormal service voltage range | −60 V to −58.8 V<br>−40 V to 0 V |
| Typical startup voltage | −44 V to −46 V |
| Typical shut-down voltage | −37.5 V to −39.5 V |

### 15.1.2 Fan Unit

**Note:** MINI-LINK 6651/3 has no fan unit.

Air-cooling is provided by the Fan Unit, see Figure 84.

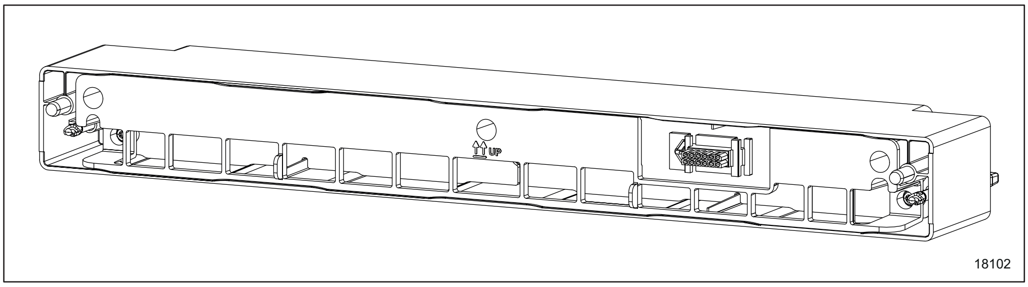


Figure 84 Fan Unit

The Fan Unit has an automatic fan speed control and houses four internal fans.

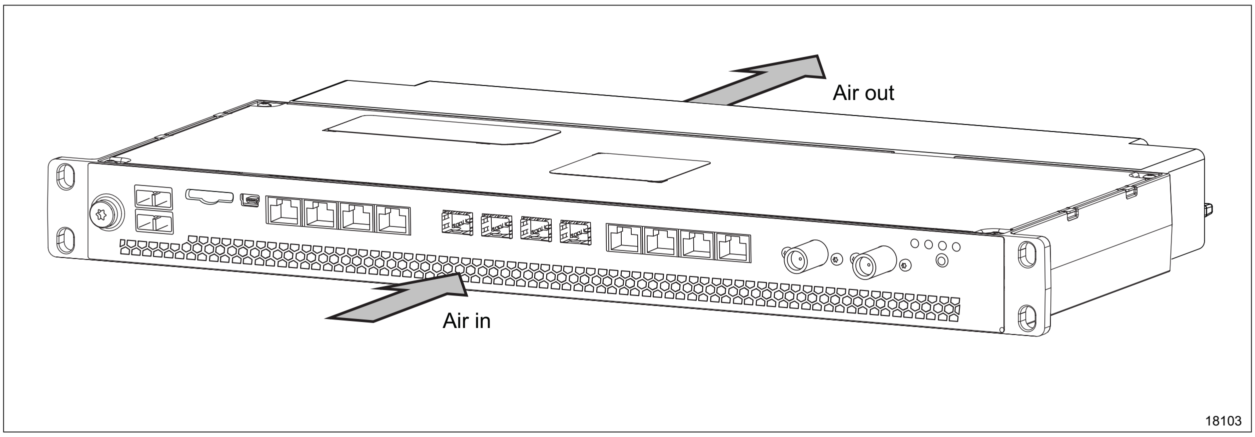


Figure 85 Cooling Airflow in MINI-LINK 6651

The air enters at the front of the MINI-LINK 6651 and exits at the back.

### 15.1.3 Traffic Capacities for MINI-LINK 6651

MINI-LINK 6651 is used for the traffic capacities specified in Table 17 and Table 18 (ETSI), or in Table 19 (ANSI).

Table 17 Ethernet Capacity for MINI-LINK 6651 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | **7 MHz** | **14 MHz** | **28 MHz** | **40 MHz** | **56 MHz** | **80 MHz** | **112 MHz** |
| 4 QAM STRONG | 8 | 18 | 37 | 53 | 75 | 108 | 150 |
| 4 QAM | 10 | 21 | 43 | 62 | 87 | 126 | 175 |
| 16 QAM STRONG | 17 | 37 | 74 | 106 | 150 | 216 | 301 |
| 16 QAM | 20 | 43 | 87 | 124 | 175 | 252 | 351 |
| 32 QAM | 26 | 54 | 109 | 156 | 220 | 317 | 441 |
| 64 QAM | 32 | 68 | 136 | 195 | 276 | 397 | 553 |
| 128 QAM | 38 | 80 | 161 | 231 | 326 | 469 | 653 |
| 256 QAM | 44 | 92 | 186 | 266 | 377 | 541 | 754 |
| 512 QAM | 47 | 99 | 198 | 284 | 402 | 577 | 804 |
| 512 QAM LIGHT | 50 | 105 | 211 | 302 | 427 | 614 | 854 |
| 1024 QAM | 53(1) | 110 | 221 | 316 | 447 | 643 | 895 |
| 1024 QAM LIGHT | 56(1) | 116 | 233 | 334 | 472 | 679 | 945 |
| 2048 QAM | – | 121(1) | 243 | 347 | 491 | 706 | 983 |

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 2048 QAM LIGHT | – | 127(1) | 256 | 365 | 516 | 742 | 1033 |
| 4096 QAM | – | – | 264 | 377 | 533 | 767(1) | 1067(1) |
| 4096 QAM LIGHT | – | – | 276 | 395 | 558 | – | – |

(1) XPIC not supported.

Table 18 Maximum PDH Capacities for MINI-LINK 6651 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in E1s(1)(2) | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 4 QAM STRONG | 2×E1 | 6×E1 | 15×E1 | 23×E1 | 34×E1 | 47×E1 | 70×E1 |
| 4 QAM | 3×E1 | 8×E1 | 18×E1 | 28×E1 | 40×E1 | 56×E1 | 80×E1 |
| 16 QAM STRONG | 6×E1 | 15×E1 | 34×E1 | 49×E1 | 70×E1 | 80×E1 | 80×E1 |
| 16 QAM | 7×E1 | 18×E1 | 39×E1 | 57×E1 | 71×E1 | 80×E1 | 80×E1 |
| 32 QAM | 10×E1 | 24×E1 | 50×E1 | 73×E1 | 80×E1 | 80×E1 | 80×E1 |
| 64 QAM | 13×E1 | 30×E1 | 63×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 128 QAM | 16×E1 | 36×E1 | 75×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 256 QAM | 19×E1 | 42×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 512 QAM | 21×E1 | 45×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 512 QAM LIGHT | 22×E1 | 48×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 1024 QAM | 23×E1(3) | 51×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 1024 QAM LIGHT | 25×E1(3) | 54×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 2048 QAM | – | 56×E1(3) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 2048 QAM LIGHT | – | 59×E1(3) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 4096 QAM | – | – | 80×E1 | 80×E1 | 80×E1 | 80×E1(3) | 80×E1(3) |
| 4096 QAM LIGHT | – | – | 80×E1 | 80×E1 | 80×E1 | – | – |

(1) The ML6651/1 and ML6651/3 capacity are limited to 8×E1.

(2) The ML6651/4 capacity is limited to 16xE1.

(3) XPIC not supported.

Table 19 Ethernet Capacity for MINI-LINK 6651 Adaptive Physical Modes (ANSI)

| **Modulation** | **Capacity in Mbps** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Channel Bandwidth** | | | | | | |
| | **10 MHz** | **20 MHz** | **30 MHz** | **40 MHz** | **50 MHz** | **60 MHz** | **80 MHz** |
| 4 QAM STRONG | 12 | 26 | 39 | 53 | 67 | 81 | 108 |
| 4 QAM | 14 | 30 | 46 | 62 | 78 | 94 | 126 |
| 16 QAM STRONG | 25 | 52 | 79 | 107 | 135 | 162 | 216 |
| 16 QAM | 29 | 61 | 93 | 125 | 157 | 189 | 252 |
| 32 QAM | 36 | 77 | 116 | 157 | 197 | 237 | 317 |
| 64 QAM | 46 | 96 | 146 | 197 | 247 | 297 | 397 |
| 128 QAM | 54 | 114 | 173 | 233 | 292 | 351 | 469 |
| 256 QAM | 63 | 131 | 199 | 268 | 337 | 405 | 541 |
| 512 QAM | 67 | 140 | 213 | 286 | 360 | 432 | 577 |
| 512 QAM LIGHT | 71 | 149 | 226 | 304 | 382 | 459 | 614 |
| 1024 QAM | 74(1) | 156 | 237 | 319 | 400 | 481 | 643 |
| 1024 QAM LIGHT | 79(1) | 165 | 250 | 337 | 423 | 508 | 679 |
| 2048 QAM | – | 171 | 260 | 350 | 440 | 528 | 706 |
| 2048 QAM LIGHT | – | 180 | 273 | 368 | 462 | 555 | 742 |
| 4096 QAM | – | – | 282 | 380 | 477 | 574 | 767(1) |
| 4096 QAM LIGHT | – | – | 296 | 398 | 500 | 601 | – |

(1) XPIC not supported.

### 15.1.4 Hardware Handling

The system offers several functions for easy operation and maintenance.

- The configuration file is stored non-volatile on the RMM, and can also be backed up and restored using a local or central FTP server. The RMM storage thus enables replacement without using an FTP server.
- When a radio is replaced, no new setup has to be performed.
- Various restarts can be ordered from the management system. A cold restart can be initiated for an NE, and this type of restart disturbs the traffic. A warm restart restarts the control system and does not affect the traffic, which is possible due to the separated control and traffic system.
- MINI-LINK 6651 is equipped with temperature sensors. Overheated parts that exceed limit thresholds, are put in out of service by the control

system. This is to avoid hardware failures in case of over-temperature, for example, due to a fan failure or an ambient temperature that is too high. The MINI-LINK 6651 is automatically returned to normal operation when the temperature is below the high threshold level.

There are two thresholds:

- The high temperature threshold:

  The MINI-LINK 6651 raises a temperature alarm (critical). The MINI-LINK 6651 is still in full operation.

- The excessive temperature threshold:

  The MINI-LINK 6651 shuts down (out of service).

— Access to inventory data like software and hardware product number, serial number, and version. User defined asset identification is supported, enabling tracking of hardware.

### 15.1.5 Ethernet Switch

The Ethernet switch functionality is shown in Table 20.

Table 20 Ethernet Switch Functionality

| Modes | Port roles | Comment |
|---|---|---|
| Provider Bridge mode | CE-UNI | CEP, including default mapping rule |
| | CN-UNI | CNP |
| | I-NNI | – |
| Customer Bridge mode | UNI | Including QinQ termination, default mapping rule |
| | NNI | – |

The switch is a managed VLAN switch (IEEE 802.1Q and IEEE 802.1D) and supports Provider mode (IEEE 802.1ad) and Customer mode (IEEE 802.1Q) switching.

The switch supports Jumbo frames. The Ethernet site LAN ports on MINI-LINK 6651 have interfaces that support auto-negotiation 10/100/1000/2500 Mbps and 10Gbps speed. The interfaces are physical RJ-45 or SFP connectors.

### 15.1.6 Ethernet LAN Ports

The Ethernet LAN ports are described in Table 21.

Table 21 Ethernet LAN Ports

| Functionality | Description |
|---|---|
| Interface types | 10/100/1000/2500 Mbps<br>2.5/10 Gbps<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Duplex mode | Full duplex.<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Connectors/cables | RJ-45 with MDI/MDIX support for all electrical i/f.<br>Single/multi-mode fiber with LC connector for the optical i/f. |
| SFP modules | SFP/SFP+ plug-in modules are supported with 1 Gbps, 2.5 Gbps, and 10 Gbps optical and 100/1000 Mbps electrical interfaces.<br>For more information regarding SFP/SFP+, see MINI-LINK 6600 R1 Compatibility, Reference [1]. |
| LED indicators | Each Ethernet interface has one green LED for network link indication. |
| Standard frame sizes | Up to 2000 bytes when used as an external interface (IEEE802.3as-2006).<br>Up to 2048 bytes when used as an internal interface. |
| Jumbo frames | 9,216 byte frame size for data applications. |
| Buffer capacity | Ethernet ports share a 180 MB buffering capacity. The buffer capacity sharing among the traffic queues is based on a fair adaptive dynamic algorithm. |
| Flow control | MINI-LINK 6651 supports the IEEE 802.3x standard to handle temporary congestion on ports configured as Layer 2 connections (connected to the switch). MINI-LINK 6651 only supports asymmetrical flow control. When a congestion threshold is reached in an NE downstream, the NE generates a PAUSE signal and MINI-LINK 6651 temporarily halts the transmission of Ethernet frames, but MINI-LINK 6651 cannot generate PAUSE signals to control the transmission process on connected equipment. |

## 15.2 MINI-LINK 6654

MINI-LINK 6654 supports Ethernet (packet link), PDH, and a mix thereof in a Hybrid Radio Link sending Ethernet and PDH traffic simultaneously.

It consists of a rack, Enclosure 1401, that must be equipped with a fan, FAU 1401, and a PNM board, either PNM 1001 or PNM 1002.

MINI-LINK 6654 can also be equipped with up to two MMU 1001/1002, two LTU 1001/1002, two ETU 1001/1002, or a combination thereof, see Figure 86.

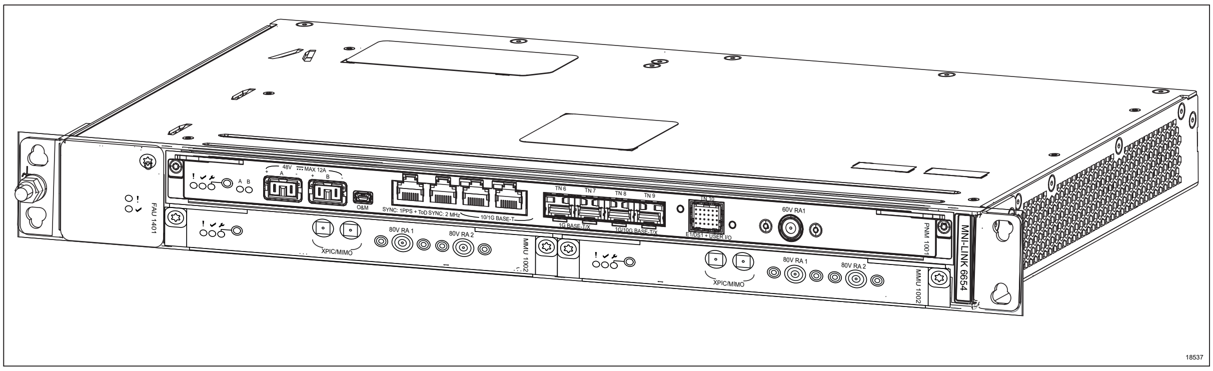


Figure 86 MINI-LINK 6654

Unused slots in MINI-LINK 6654 must be equipped with Dummy Units, as this is essential to maintain the cooling within the magazines and to meet EMC requirements.

MINI-LINK 6654 can be fitted in a standard 19" or metric rack or on a wall using a dedicated mounting set. The height of a MINI-LINK 6654 is 1U, see Figure 87.

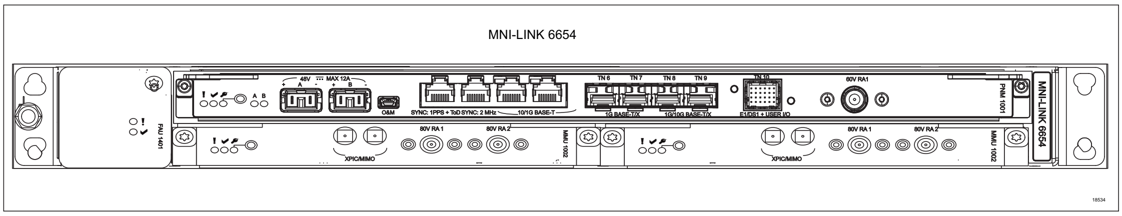


Figure 87 Front interfaces on the MINI-LINK 6654

The following slots are paired in MINI-LINK 6654:

- Slot 1 and Slot 3

Figure 88 shows the paired slots in MINI-LINK 6654.

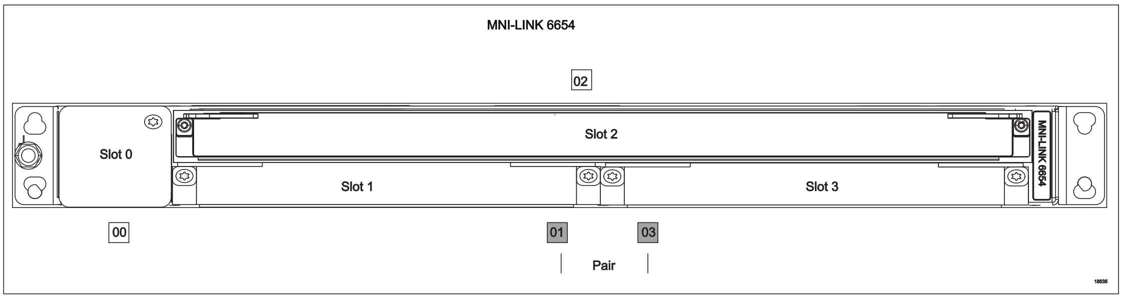


Figure 88 Interconnected slots in MINI-LINK 6654

### 15.2.1 PNM 1001

PNM 1001 is a board that is combo solution for PFU (Power-Filtering-Unit), NPU (Node-Processor-Unit) and MMU (Modem Unit), see Figure 89.

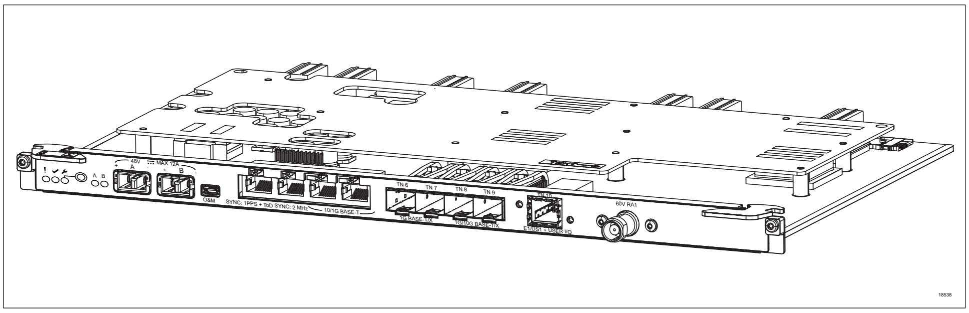


Figure 89 PNM 1001

The Modem part of PNM 1001 is a single carrier modem supporting single WAN (1+0). For modem capability please refer to MMU 1001 performance in 1+0.

**PDH Traffic Interfaces**

4×E1/DS1

User I/O (two users in, one user out)

**Ethernet Traffic Interfaces**

2×Electrical (10M/100M/1G)

2×SFP (1G)

2×SFP+ (1G/10G)

**Sync Interfaces**

1×2 MHz

1×1PPS+ToD

**O&M Interface**

1×USB interface for an alternative MINI-LINK Node GUI connection is available.

**Radio Interface**

1×60 V RAU connector.

**Note:** The coaxial interface on modems and radios is equipped with built-in gas discharge tubes for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

**Power**

2×−48V DC connectors for power redundancy.

Figure 90 shows the interfaces on the PNM 1001.

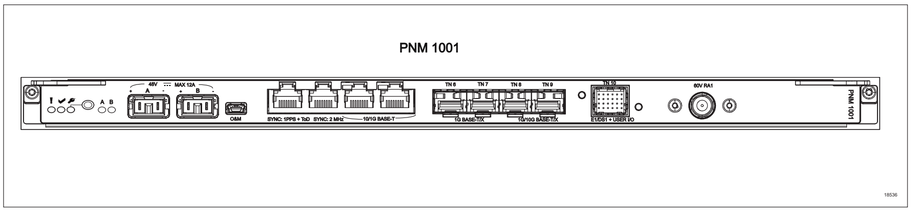


Figure 90 Front Interfaces on the PNM 1001

### 15.2.1.1 User Input/Output

The User Input ports can be used to connect user alarms to MINI-LINK Node GUI. Applications like fire alarms, burglar alarms, and low power indicators are easily implemented using these input ports. The User Input ports can be configured to be normally opened or closed.

The User Output ports can be used to export summary alarms of the accumulated severity in the NE to the supervision system of other equipment. The User Output ports can be controlled by the operator or triggered by one or several alarm severities.

Table 22 PNM 1001 User Input and Output Ports

| Plug-In Unit | Number of Input Signals | Number of Output Signals | Connector Type |
|---|---|---|---|
| PNM 1001 | Two | One | Male 24 pin SOFIX connector |

## 15.2.2 PNM 1002

PNM 1002 is a board that is combo solution for PFU (Power-Filtering-Unit), NPU (Node-Processor-Unit) and MMU (Modem Unit), see Figure 91.

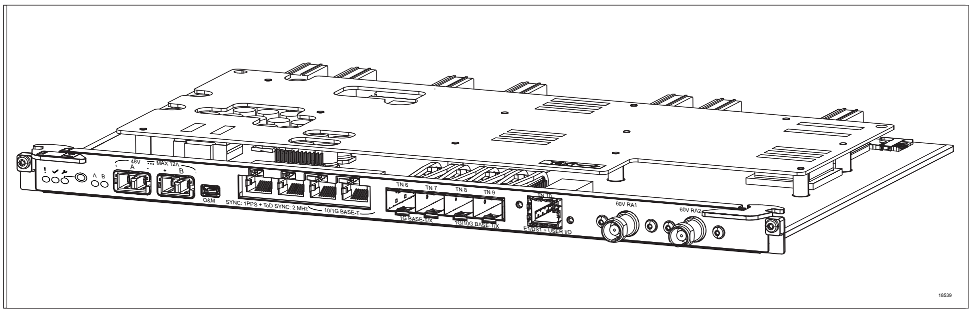


Figure 91 PNM 1002

The Modem part of PNM 1002 is a Dual carrier modem supporting dual WAN 1+0/2+0/1+1 and Dual WAN 2×(1+0). For modem capability please refer to MMU 1002 performance on a single modem.

### PDH Traffic Interfaces

4×E1/DS1

User I/O (two users in, one user out)

### Ethernet Traffic Interfaces

2×10M/100M/1G (Electrical)

2×1G SFP

2×1G/10GSFP+

### Sync Interfaces

1×2 MHz

1×1PPS+ToD

### O&M Interface

1×USB interface for an alternative MINI-LINK Node GUI connection is available.

### Radio Interfaces

2×60 V RAU connector.

**Note:** The coaxial interface on modems and radios is equipped with built-in gas discharge tubes for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

**Power**

2×−48V DC connectors for power redundancy.

Figure 92 shows the interfaces on the PNM 1002.

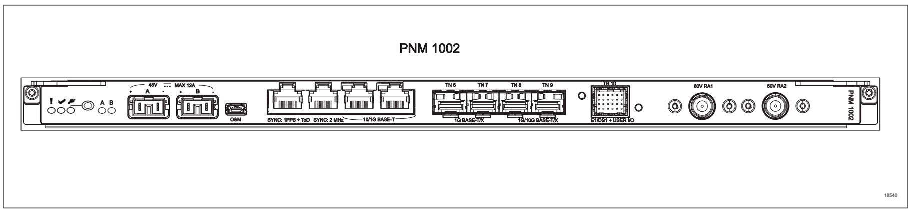


Figure 92 Front Interfaces of PNM 1002

### 15.2.2.1 User Input/Output

The User Input ports can be used to connect user alarms to MINI-LINK Node GUI. Applications like fire alarms, burglar alarms, and low power indicators are easily implemented using these input ports. The User Input ports can be configured to be normally opened or closed.

The User Output ports can be used to export summary alarms of the accumulated severity in the NE to the supervision system of other equipment. The User Output ports can be controlled by the operator or triggered by one or several alarm severities.

Table 23 PNM 1002 User Input and Output Ports

| Plug-In Unit | Number of Input Signals | Number of Output Signals | Connector Type |
|---|---|---|---|
| PNM 1002 | Two | One | Male 24 pin SOFIX connector |

## 15.2.3 Enclosure 1401

Enclosure 1401 supports both Ethernet and PDH traffic simultaneously.

The Ethernet capacity is 2×2.5G for each APU slot.

## 15.2.4 Input Voltage Behavior

Figure 93 shows the input voltage behavior for MINI-LINK 6654. The different units turn on and off at different voltages.

To prevent the units from turning on and off repeatedly around a threshold (so called power flapping), there is a hysteresis for all units.

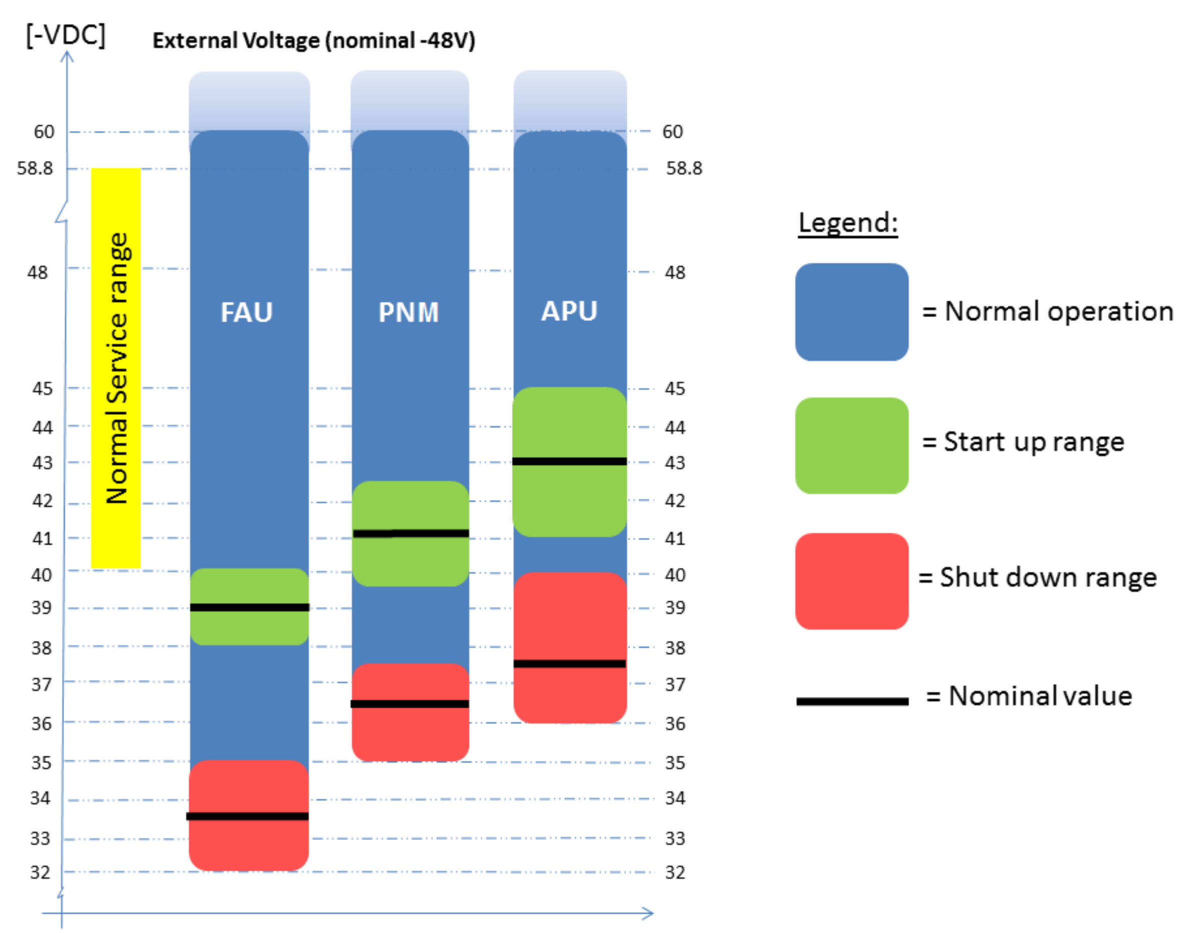


Figure 93 Start and Stop Voltages

## 15.3 MINI-LINK 6655

MINI-LINK 6655 supports Ethernet (packet link), PDH, and a mix thereof in a Hybrid Radio Link sending Ethernet and PDH traffic simultaneously.

It consists of a rack, Enclosure 1501, that must be equipped with a fan, FAU 1501, and a PNM board, PNM 1002. For the description of PNM 1002, see Section 15.2.2 on page 141.

MINI-LINK 6655 can also be equipped with up to four MMU 1001/1002, four LTU 1001/1002, four ETU 1001/1002, or a combination thereof.

Unused slots in MINI-LINK 6655 must be equipped with Dummy Units, as this is essential to maintain the cooling within the magazines and to meet EMC requirements.

MINI-LINK 6655 can be fitted in a standard 19" or metric rack. The height of a MINI-LINK 6655 is 1.5U, see Figure 94.

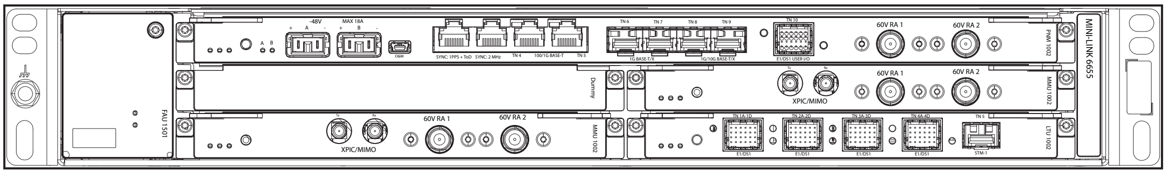


Figure 94 Front interfaces on the MINI-LINK 6655

The following slots are paired in MINI-LINK 6655:

- Slot 1 and Slot 2
- Slot 4 and Slot 5

### 15.3.1 Enclosure 1501

Enclosure 1501 supports both Ethernet and PDH traffic simultaneously.

The MMUs, LTUs and ETUs are placed in the Application Plug-in Unit (APU) slots, that is, slots 1–2 and 4–5. The available traffic capacity is dependent on the board types and their position in the enclosure. Traffic capacities are shown in Table 24.

Table 24 Enclosure 1501 Ethernet Capacities

| Slot | Ethernet Capacity with PNM 1002 [Gbps] |
|---|---|
| 5 | 1×2.5 |
| 4 | 1×2.5 |
| 2 | 2×2.5 |
| 1 | 2×2.5 |

### 15.3.2 Input Voltage Behavior

Figure 95 shows the input voltage behavior for MINI-LINK 6655. The different units turn on and off at different voltages.

To prevent the units from turning on and off repeatedly around a threshold (so called power flapping), there is a hysteresis for all units.

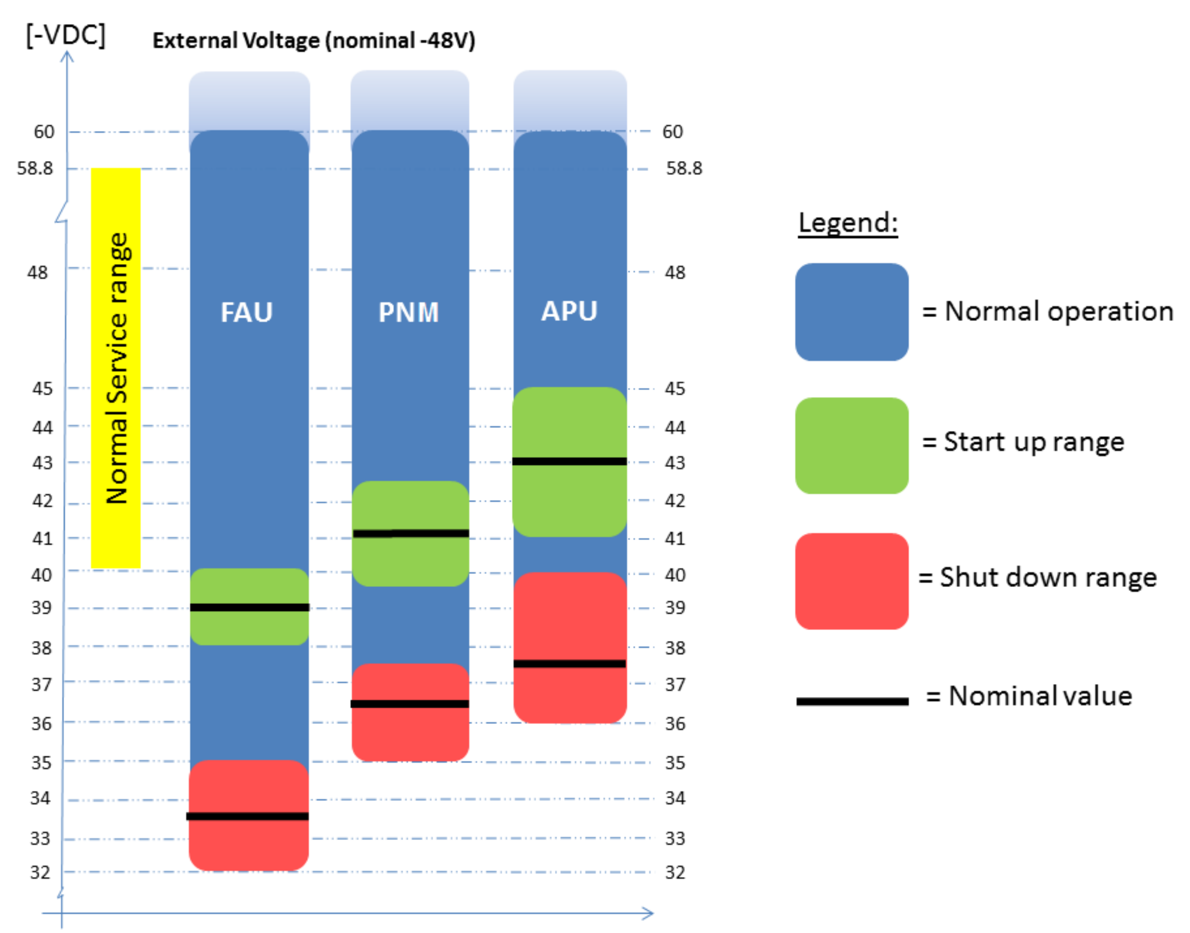


Figure 95 Start and Stop Voltages

## 15.4 MINI-LINK 6691

MINI-LINK 6691 is suitable for end site and repeater site applications as well as medium-sized hub sites or prioritized small-sites.

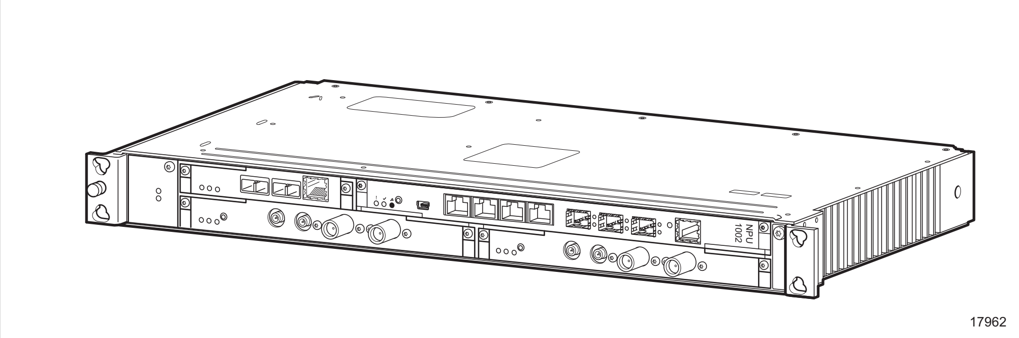


Figure 96 MINI-LINK 6691

MINI-LINK 6691 consists of a rack, Enclosure 1101, that must be equipped with a fan, FAU 1101, and power supply, PFU 1101.

MINI-LINK 6691 can also be equipped with one NPU 1002/1003/1005 and two MMU 1001/1002, or with one NPU 1002/1003/1005, one MMU 1001/1002, and one LTU 1001/1002. LTU 1001 provides E1/DS1 interfaces for PDH and LTU 1002 provides E1/DS1 and STM-1 interfaces for PDH and SDH. MINI-LINK 6691 can also be equipped with ETU 1001/1002, which provides additional Ethernet interfaces.

Unused slots in MINI-LINK 6691 must be equipped with Dummy Units, as this is essential to maintain the cooling within the magazines and to meet EMC requirements.

MINI-LINK 6691 can be fitted in a standard 19" or metric rack or on a wall using a dedicated mounting set. The height of a MINI-LINK 6691 is 1U.

### 15.4.1 PFU 1101

Power handling and filtering is performed by the Power Filter Unit (PFU) 1101, see Figure 97.

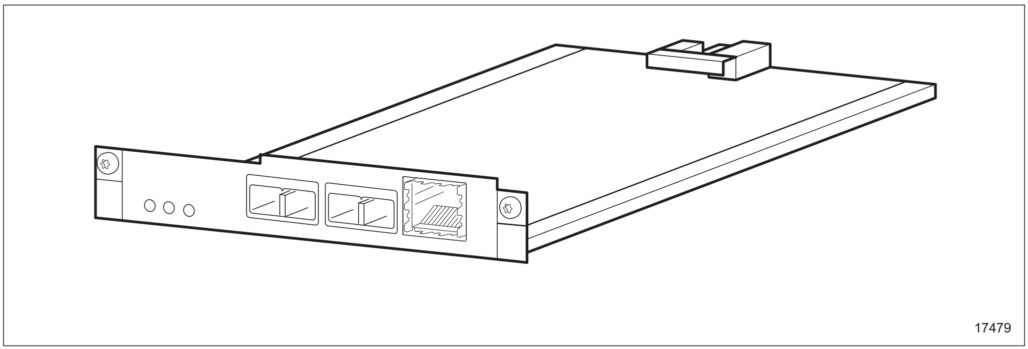


Figure 97 PFU 1101

To achieve redundant power, two power sources must be connected.

#### 15.4.1.1 System Monitoring

The PFU supports the monitoring of the node power consumption by measuring the input current and voltage on the incoming −48V.

The following data can be read:

- The current values of input voltage and the power consumption of the node.
- The accumulated and persistently stored energy consumption of the node.

### 15.4.2 FAU 1101

Air-cooling is provided by the FAU 1101, see Figure 98.

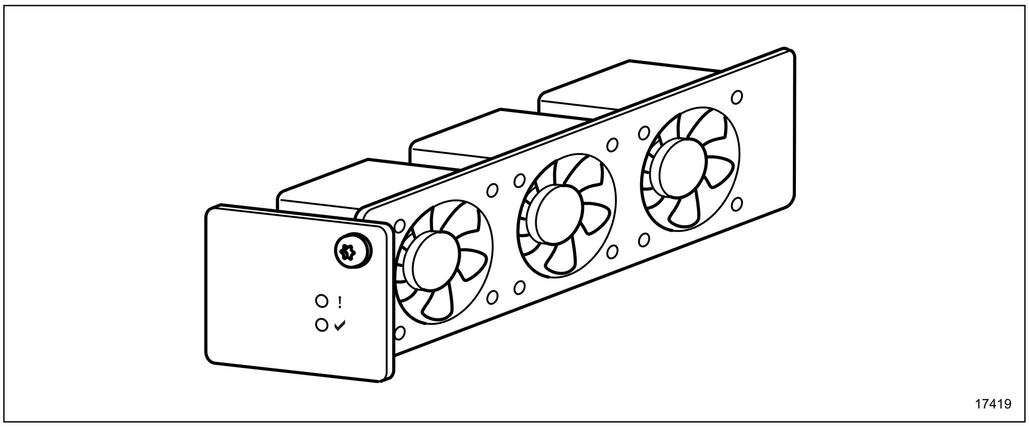


Figure 98 FAU 1101

FAU 1101 has an automatic fan speed control and houses three internal fans.

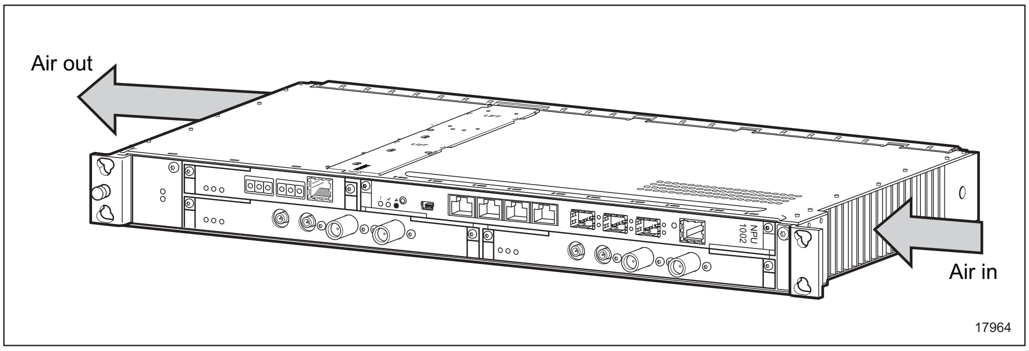


Figure 99 Cooling Airflow in MINI-LINK 6691

The air enters at the right side of the enclosure and exits at the left side of the enclosure.

### 15.4.3 Backplane Architecture

MINI-LINK 6691 with NPU 1002/1003/1005 provides high-speed connections of up to 10 Gbps between the NPUs, MMUs, ETUs and LTUs. The available traffic capacity is dependent on the board types and their position in the enclosure.

| Slot | Ethernet capacity with NPU 1002 [Gbps] |
|---|---|
| 3 | 1×10 or 4×2.5 |
| 1 | 2×2.5 |

| Slot | Ethernet capacity with and NPU 1003 [Gbps] |
|---|---|
| 3 | 1×10 or 4×2.5 |
| 1 | 2×2.5 |

| Slot | Ethernet Capacity with NPU 1005 [Gbps] |
|---|---|
| 3 | 1x10 or 4x2.5 |
| 1 | 1x10 or 4x2.5 |

The following pair of slots are interconnected (2-BPI) in the MINI-LINK 6691 backplane, and can be used for Modem Equipment Protection (EQP):

- Slots 1 and 3

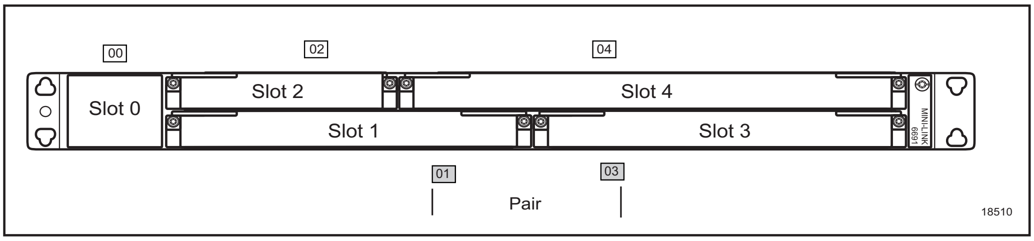


Figure 100 Interconnected Slots in MINI-LINK 6691

### 15.4.4 Hardware Handling

The system offers several functions for easy operation and maintenance.

- Plug-in units can be inserted while the NE is in operation. This enables adding of new Radio Terminals or other plug-in units without disturbing existing traffic.
- Plug-in units other than the NPU can be removed while the NE is in operation.
- When replacing a faulty plug-in unit, the new plug-in unit automatically inherits the configuration of the old plug-in unit.
- The configuration file is stored non-volatile both on the RMM and in a flash memory on the NPU, and can also be backed up and restored using a local or central FTP server. The RMM storage thus enables NPU replacement without using an FTP server.
- The backplane in all subracks has a digital serial number which is also stored on the RMM of the NPU. When inserting an NPU, for example, as a replacement, the serial numbers are compared on power up.
- Various restarts can be ordered from the management system. A cold restart can be initiated for an NE or single plug-in unit, and this type of restart disturbs the traffic. A warm restart is only available for the whole NE, and this

restarts the control system and does not affect the traffic, which is possible due to the separated control and traffic system.

- All plug-in units are equipped with temperature sensors. Overheated boards that exceed limit thresholds, are put in out of service by the control system. This is to avoid hardware failures in case of over-temperature, for example, due to a fan failure or an ambient temperature that is too high. The plug-in unit is automatically returned to normal operation when the temperature is below the high threshold level.

  There are two thresholds:

  - The high temperature threshold:

    The NPU raises a temperature alarm (critical). The NPU is still in full operation.

    All plug-in units except NPUs raise a temperature alarm (minor). The plug-in unit is still in full operation.

  - The excessive temperature threshold:

    The NPU shuts down the entire NPU (out of service).

    All plug-in-units except NPUs raise a temperature alarm (critical) and shut down the entire plug-in unit (out of service).

- Access to inventory data like software and hardware product number, serial number, and version. User defined asset identification is supported, enabling tracking of hardware.

- Slot availability and capacity can be monitored by using MINI-LINK Node GUI, or CLI. In this way, choosing a slot for additional plug-in units is easier.

### 15.4.5 Input Voltage Behavior

Figure 101 shows the input voltage behavior for MINI-LINK 6691. The different units turn on and off at different voltages.

To prevent the units from turning on and off repeatedly around a threshold (so called power flapping), there is a hysteresis for all units.

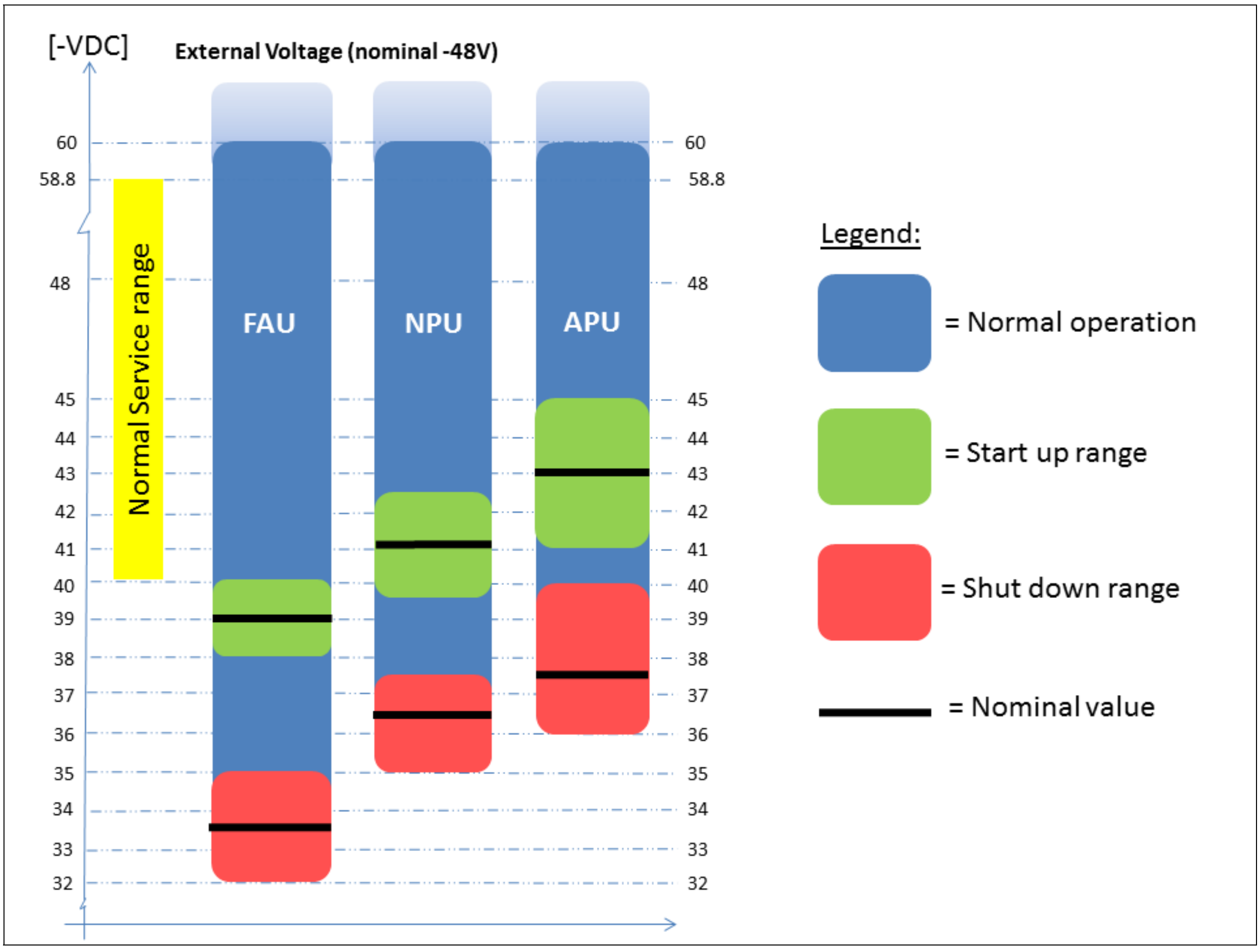


Figure 101 Start and Stop Voltages

## 15.5 MINI-LINK 6692

MINI-LINK 6692 is suitable for end site and repeater site applications as well as medium-sized hub sites or prioritized small-sites.

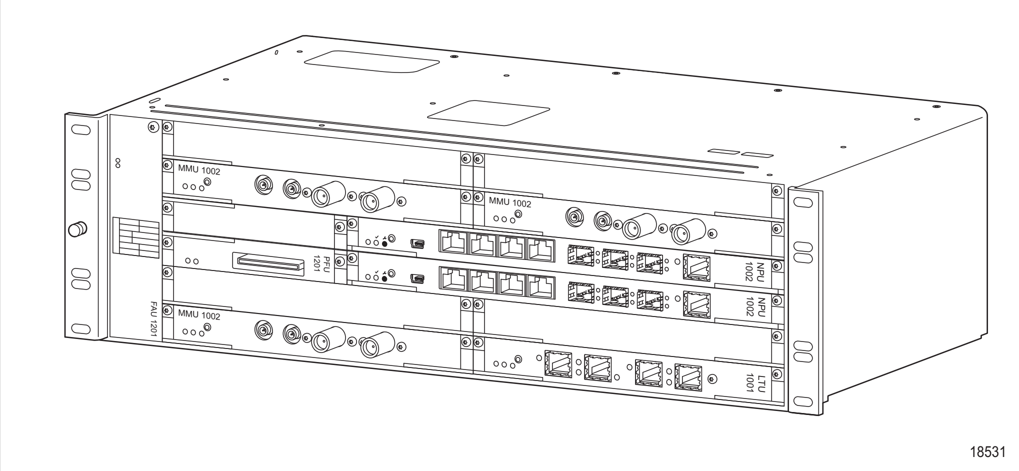


Figure 102 MINI-LINK 6692

MINI-LINK 6692 consists of a rack, Enclosure 1201, that must be equipped with a fan, FAU 1201, and power supply, PFU 1201.

MINI-LINK 6692 can also be equipped with one or two NPU 1002/NPU 1005, and up to eight MMU 1001/1002, LTU 1001/1002, or a combination thereof. It is not possible to combine NPU 1002 and NPU 1005 in the same magazine. LTU 1001 provides E1/DS1 interfaces for PDH and LTU 1002 provides E1 and STM-1 interfaces for PDH and SDH. MINI-LINK 6692 can also be equipped with ETU 1001/1002, which provides additional Ethernet interfaces.

To achieve NPU protection, two NPU 1002 or two NPU 1005 must be used. See Section 15.5.5 on page 157.

Unused slots in MINI-LINK 6692 must be equipped with Dummy Units, as this is essential to maintain the cooling within the magazines and to meet EMC requirements.

MINI-LINK 6692 can be fitted in a standard 19" or metric rack or on a wall using a dedicated mounting set. The height of a MINI-LINK 6692 is 3U.

### 15.5.1 PFU 1201

Power handling and filtering is performed by the Power Filter Unit (PFU) 1201, see Figure 97.

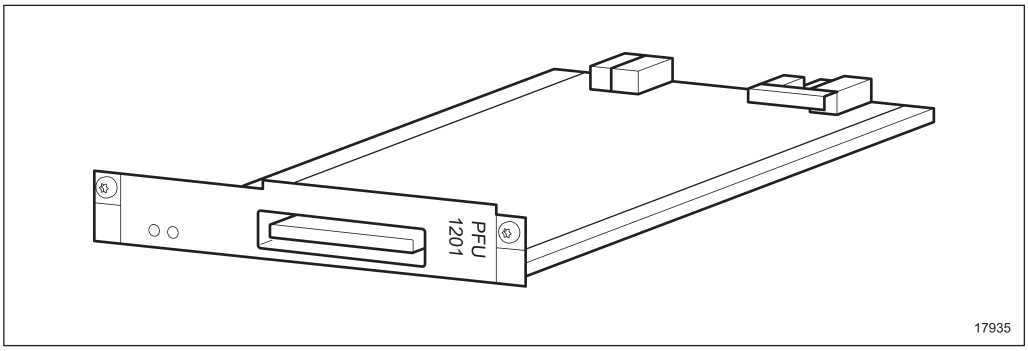


Figure 103 PFU 1201

To achieve redundant power, two PFU 1201 are needed, and two power sources, one connected to each PFU 1201.

#### 15.5.1.1 System Monitoring

The PFU supports the monitoring of the node power consumption by measuring the input current and voltage on the incoming −48V.

The following data can be read:

- The current values of input voltage and the power consumption of the node.
- The accumulated and persistently stored energy consumption of the node.

### 15.5.2 FAU 1201

Air-cooling is provided by the FAU 1201, see Figure 104.

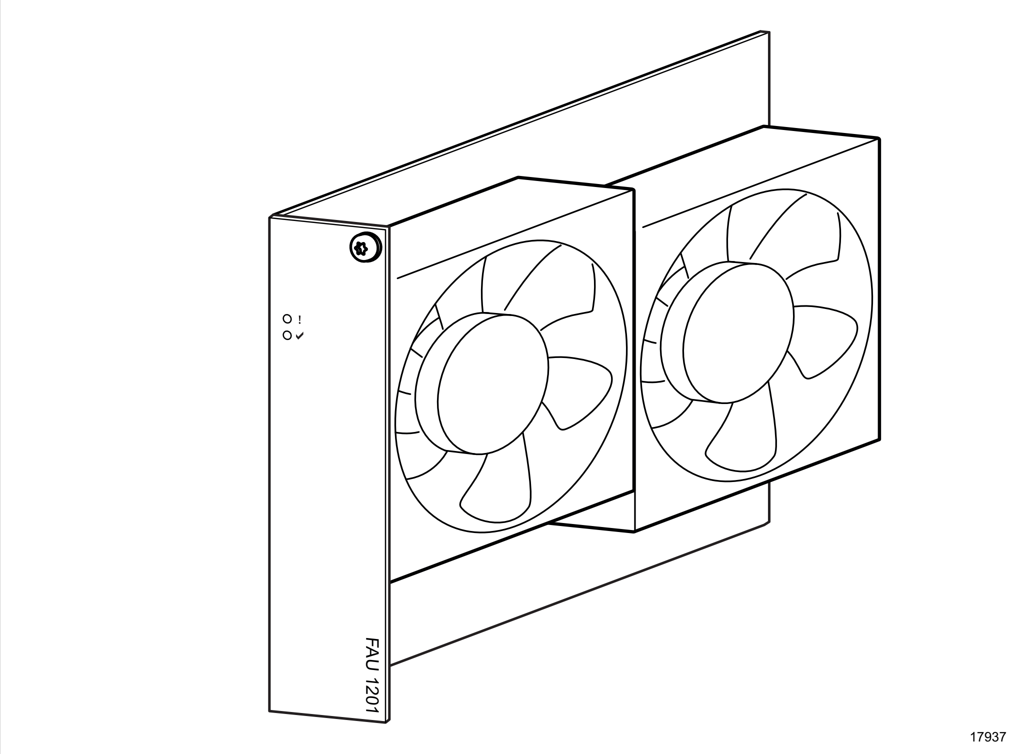


Figure 104 FAU 1201

FAU 1201 has an automatic fan speed control and houses three internal fans.

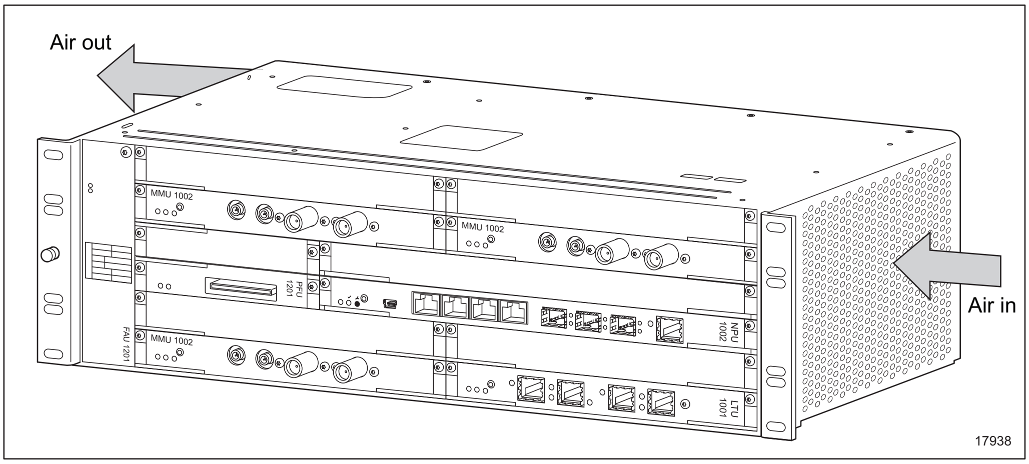


Figure 105 Cooling Airflow in MINI-LINK 6692

The air enters at the right side of the enclosure and exits at the left side of the enclosure.

### 15.5.3 Backplane Architecture

MINI-LINK 6692 provides high-speed connections of up to 10 Gbps between the NPUs, MMUs, ETUs and LTUs. The available traffic capacity is dependent on the board types and their position in the enclosure.

The MMUs, LTUs, and ETUs are placed in the Application Plug-in Unit (APU) slots, that is, slots 1–2, 5–8, and 11–12.

| Slot | Ethernet capacity with NPU 1002 [Gbps] | Slot | Ethernet capacity with NPU 1002 [Gbps] |
|---|---|---|---|
| 6 | 1×2.5 + 1×1 | 12 | 1×2.5 + 1×1 |
| 5 | 2×2.5 | 11 | 2×2.5 |
| 2 | 1×10G (4 lanes) or 4×2.5 | 8 | 1×10G (4 lanes) or 4×2.5 |
| 1 | 2×2.5 | 7 | 1×2.5 |

| Slot | Ethernet capacity with NPU 1005 [Gbps] | Slot | Ethernet capacity with NPU 1005 [Gbps] |
|---|---|---|---|
| 6 | 1×2.5 | 12 | 1×2.5 |
| 5 | 1×10G (4 lanes) or 4×2.5 | 11 | 1×2.5 |
| 2 | 1×10G (4 lanes) or 4×2.5 | 8 | 1×2.5 |
| 1 | 1×10G (4 lanes) or 4×2.5 | 7 | 1×2.5 |

The following pairs of slots are interconnected (2-BPI) in the MINI-LINK 6692 backplane, and can be used for Modem Equipment Protection (EQP):

- Slots 1 and 2
- Slots 5 and 6
- Slots 7 and 8
- Slots 11 and 12

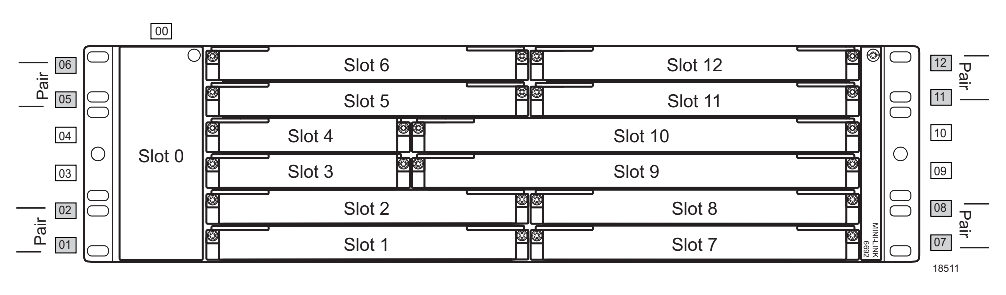


Figure 106 Interconnected Slots in MINI-LINK 6692

### 15.5.4 Hardware Handling

The system offers several functions for easy operation and maintenance.

- Plug-in units can be inserted while the NE is in operation. This enables adding of new Radio Terminals or other plug-in units without disturbing existing traffic.

- Plug-in units other than the NPU can be removed while the NE is in operation.

- When replacing a faulty plug-in unit, the new plug-in unit automatically inherits the configuration of the old plug-in unit.

- The configuration file is stored non-volatile both on the RMM and in a flash memory on the NPU, and can also be backed up and restored using a local or central FTP server. The RMM storage thus enables NPU replacement without using an FTP server.

- The backplane in all subracks has a digital serial number which is also stored on the RMM of the NPU. When inserting an NPU, for example, as a replacement, the serial numbers are compared on power up.

- Various restarts can be ordered from the management system. A cold restart can be initiated for an NE or single plug-in unit, and this type of restart disturbs the traffic. A warm restart is only available for the whole NE, and this restarts the control system and does not affect the traffic, which is possible due to the separated control and traffic system.

- All plug-in units are equipped with temperature sensors. Overheated boards that exceed limit thresholds are put in out of service by the control system. This is to avoid hardware failures in case of over-temperature, for example, due to a fan failure or an ambient temperature that is too high. The plug-in unit is automatically returned to normal operation when the temperature is below the high threshold level.

  There are two thresholds:

  - The high temperature threshold:

    The NPU raises a temperature alarm (critical). The NPU is still in full operation.

    All plug-in units except NPUs raise a temperature alarm (minor). The plug-in unit is still in full operation.

  - The excessive temperature threshold:

    The NPU shuts down the entire NPU (out of service).

    All plug-in-units except NPUs raise a temperature alarm (critical) and shut down the entire plug-in unit (out of service).

- Access to inventory data like software and hardware product number, serial number, and version. User defined asset identification is supported, enabling tracking of hardware.

- Slot availability and capacity can be monitored by using MINI-LINK Node GUI, or CLI. In this way, choosing the correct slot when adding additional plug-in units is made easier.

### 15.5.5 NPU Protection

When two NPU 1002/NPU 1005 are inserted into MINI-LINK 6692, NPU Protection can provide board, port, and full functional redundancy for the NPU, if configured and licensed properly. It is not possible to combine NPU 1002 and NPU 1005 in the same magazine.

In case of a hardware or software fault in the master NPU, an automatic failover takes place, and the slave NPU becomes the master by inheriting all configuration. All user traffic and DCN access recovers after the failover.

When having two NPU 1002, the front LAN ports of the slave NPU can be extended and configured to be used for user traffic. This way the extended ports could have different configuration than the corresponding port of the master NPU and used in different setup. After fail or switchover the configuration remains on each port, but the ports of the new slave NPU will be handled as extended.

**Note:** The front LAN ports on the slave NPU cannot be extended on NPU 1005.

### 15.5.6 Input Voltage Behavior

Figure 107 shows the input voltage behavior for MINI-LINK 6692. The different units turn on and off at different voltages.

To prevent the units from turning on and off repeatedly around a threshold (so called power flapping), there is a hysteresis for all units.

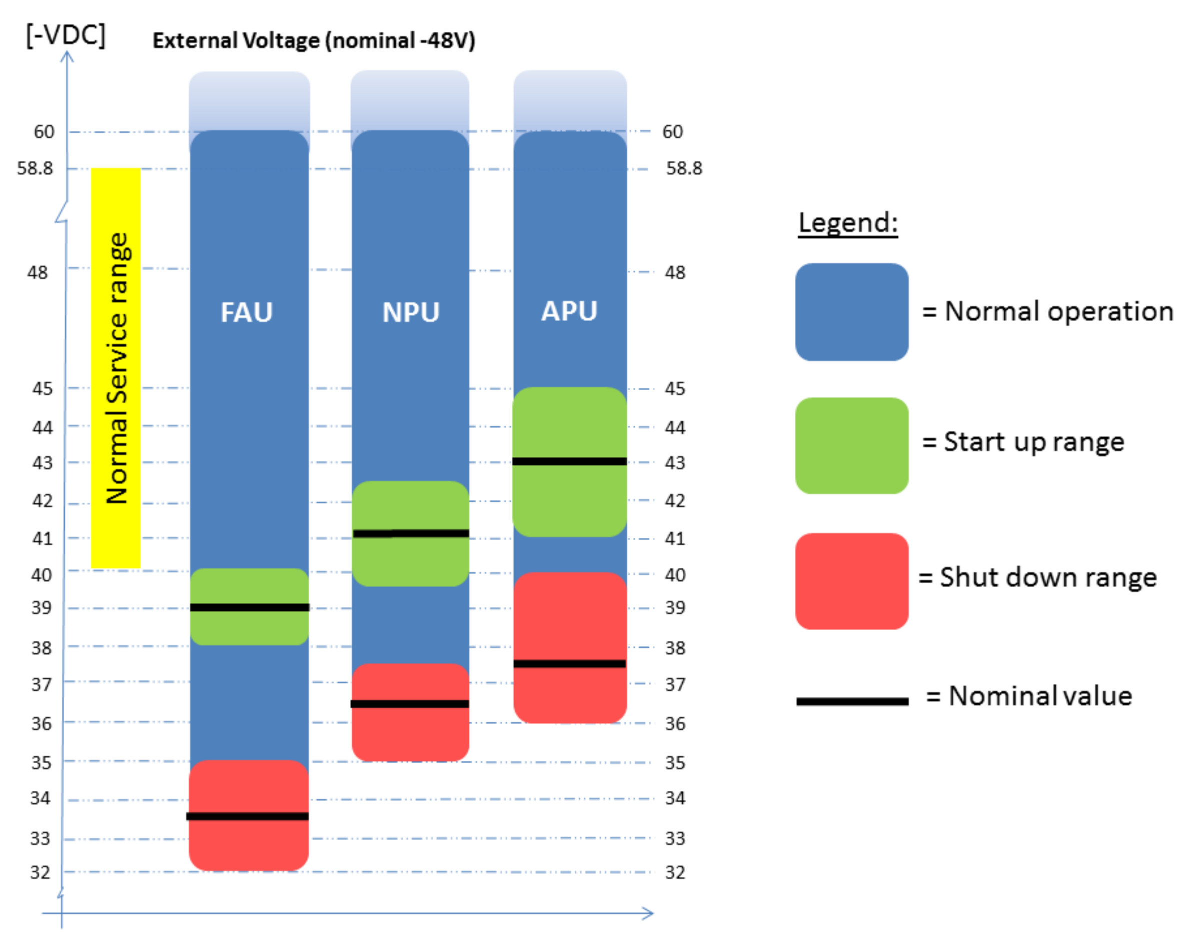


Figure 107 Start and Stop Voltages

## 15.6 MINI-LINK 6693

MINI-LINK 6693 is suitable for end site and repeater site applications as well as medium-sized hub sites or prioritized small-sites.

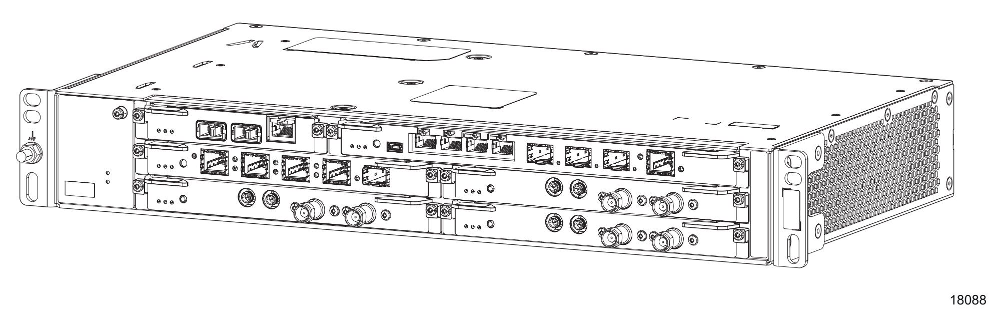


Figure 108 MINI-LINK 6693

MINI-LINK 6693 consists of a rack, Enclosure 1301, that must be equipped with a fan, FAU 1301, and power supply, PFU 1301.

MINI-LINK 6693 can also be equipped with one NPU 1002/1003/1005, and up to four MMU 1001/1002, LTU 1001/1002, or a combination thereof. LTU 1001 provides E1/DS1 interfaces for PDH and LTU 1002 provides E1/DS1 and STM-1 interfaces for PDH and SDH. MINI-LINK 6693 can also be equipped with ETU 1001/1002, which provides additional Ethernet interfaces.

Unused slots in MINI-LINK 6693 must be equipped with Dummy Units, as this is essential to maintain the cooling within the magazines and to meet EMC requirements.

MINI-LINK 6693 can be fitted in a standard 19" or metric rack or on a wall using a dedicated mounting set. The height of a MINI-LINK 6693 is 1.5U.

## 15.6.1 PFU 1301

Power handling and filtering is performed by the Power Filter Unit (PFU) 1301, see Figure 97.

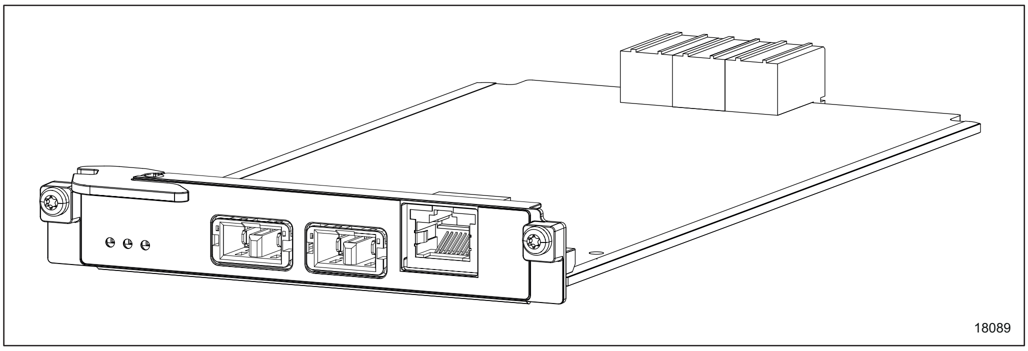


Figure 109 PFU 1301

To achieve redundant power, two power sources must be connected.

### 15.6.1.1 System Monitoring

The PFU supports the monitoring of the node power consumption by measuring the input current and voltage on the incoming −48V.

The following data can be read:

- The current values of input voltage and the power consumption of the node.
- The accumulated and persistently stored energy consumption of the node.

## 15.6.2 FAU 1301

Air-cooling is provided by the FAU 1301, see Figure 104.

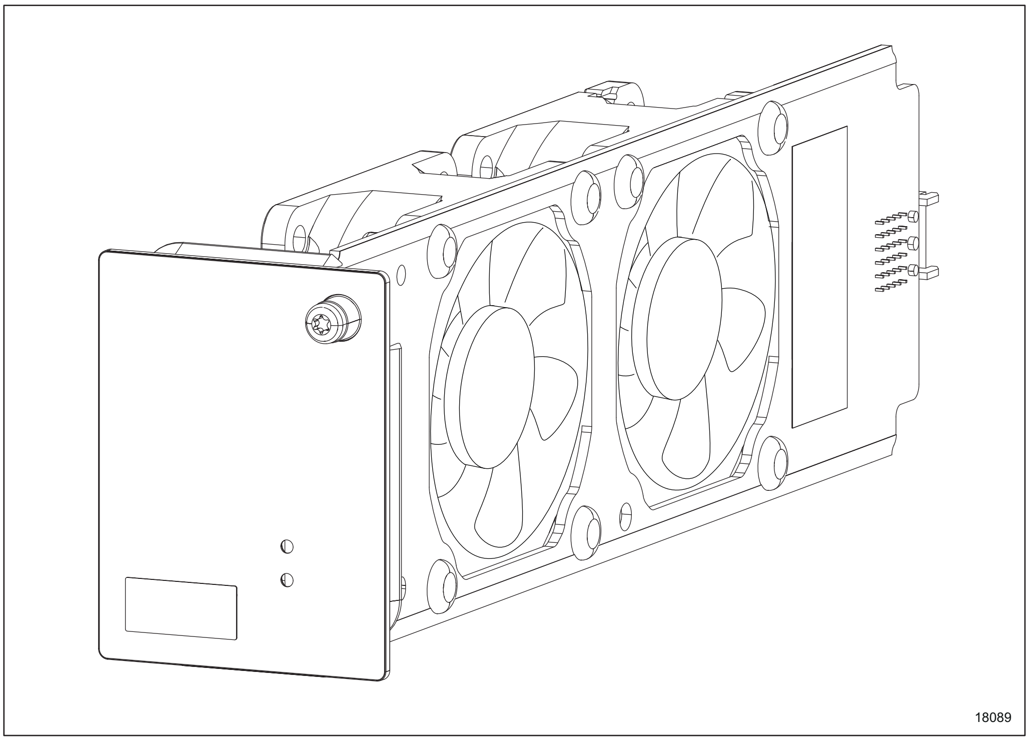


Figure 110 FAU 1301

FAU 1301 has an automatic fan speed control and houses two internal fans.

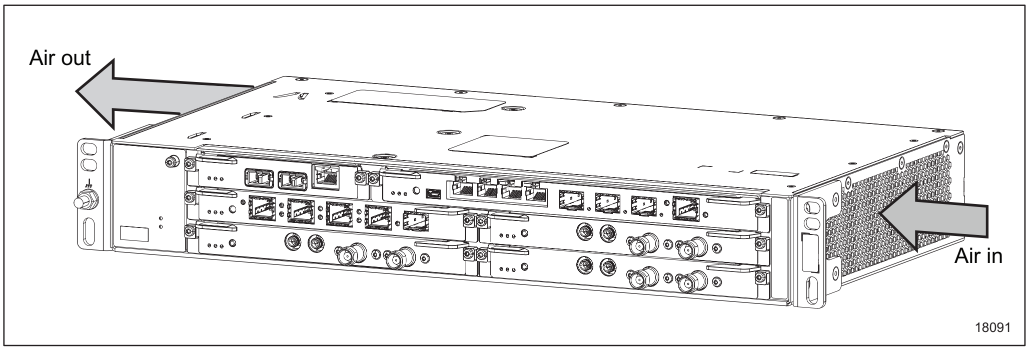


Figure 111 Cooling Airflow in MINI-LINK 6693

The air enters at the right side of the enclosure and exits at the left side of the enclosure.

### 15.6.3 Backplane Architecture

MINI-LINK 6693 provides high-speed connections of up to 10 Gbps between the NPUs, MMUs, ETUs and LTUs. The available traffic capacity is dependent on the board types and their position in the enclosure.

The MMUs, LTUs, and ETUs are placed in the Application Plug-in Unit (APU) slots, that is, slots 1–2 and 4–5.

| Slot | Ethernet capacity with NPU 1002 [Gbps] |
|---|---|
| 5 | 1×2.5 + 1×1 |
| 4 | 2×2.5 |
| 2 | 1×10 or 4×2.5 |
| 1 | 2×2.5 |

| Slot | Ethernet capacity with NPU 1003 [Gbps] |
|---|---|
| 5 | 2×2.5 |
| 4 | 1×2.5 |
| 2 | 1×10 or 4×2.5 |
| 1 | 2×2.5 |

| Slot | Ethernet capacity with NPU 1005 [Gbps] |
|---|---|
| 5 | 1×2.5 |
| 4 | 1×10 or 4×2.5 |
| 2 | 1×10 or 4×2.5 |
| 1 | 1×10 or 4×2.5 |

The following pairs of slots are interconnected (2-BPI) in the MINI-LINK 6693 backplane, and can be used for Modem Equipment Protection (EQP):

- Slots 1 and 2
- Slots 4 and 5

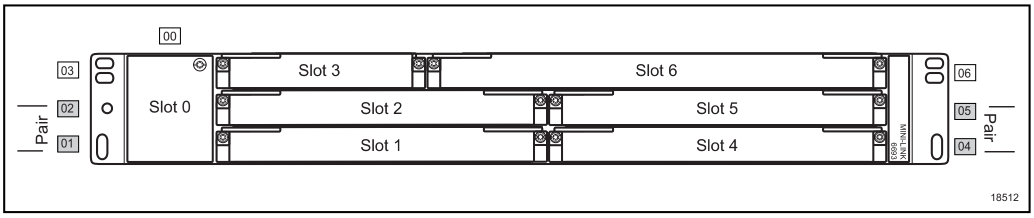


Figure 112 Interconnected Slots in MINI-LINK 6693

### 15.6.4 Hardware Handling

The system offers several functions for easy operation and maintenance.

- Plug-in units can be inserted while the NE is in operation. This enables adding of new Radio Terminals or other plug-in units without disturbing existing traffic.

- Plug-in units other than the NPU can be removed while the NE is in operation.
- When replacing a faulty plug-in unit, the new plug-in unit automatically inherits the configuration of the old plug-in unit.
- The configuration file is stored non-volatile both on the RMM and in a flash memory on the NPU, and can also be backed up and restored using a local or central FTP server. The RMM storage thus enables NPU replacement without using an FTP server.
- The backplane in all subracks has a digital serial number which is also stored on the RMM of the NPU. When inserting an NPU, for example, as a replacement, the serial numbers are compared on power up.
- Various restarts can be ordered from the management system. A cold restart can be initiated for an NE or single plug-in unit, and this type of restart disturbs the traffic. A warm restart is only available for the whole NE, and this restarts the control system and does not affect the traffic, which is possible due to the separated control and traffic system.
- All plug-in units are equipped with temperature sensors. Overheated boards that exceed limit thresholds are put in out of service by the control system. This is to avoid hardware failures in case of over-temperature, for example, due to a fan failure or an ambient temperature that is too high. The plug-in unit is automatically returned to normal operation when the temperature is below the high threshold level.

  There are two thresholds:

  - The high temperature threshold:

    The NPU raises a temperature alarm (critical). The NPU is still in full operation.

    All plug-in units except NPUs raise a temperature alarm (minor). The plug-in unit is still in full operation.

  - The excessive temperature threshold:

    The NPU shuts down the entire NPU (out of service).

    All plug-in-units except NPUs raise a temperature alarm (critical) and shut down the entire plug-in unit (out of service).

- Access to inventory data like software and hardware product number, serial number, and version. User defined asset identification is supported, enabling tracking of hardware.
- Slot availability and capacity can be monitored by using MINI-LINK Node GUI, or CLI. In this way, choosing the correct slot when adding additional plug-in units is made easier.

### 15.6.5 Input Voltage Behavior

Figure 113 shows the input voltage behavior for MINI-LINK 6693. The different units turn on and off at different voltages.

To prevent the units from turning on and off repeatedly around a threshold (so called power flapping), there is a hysteresis for all units.

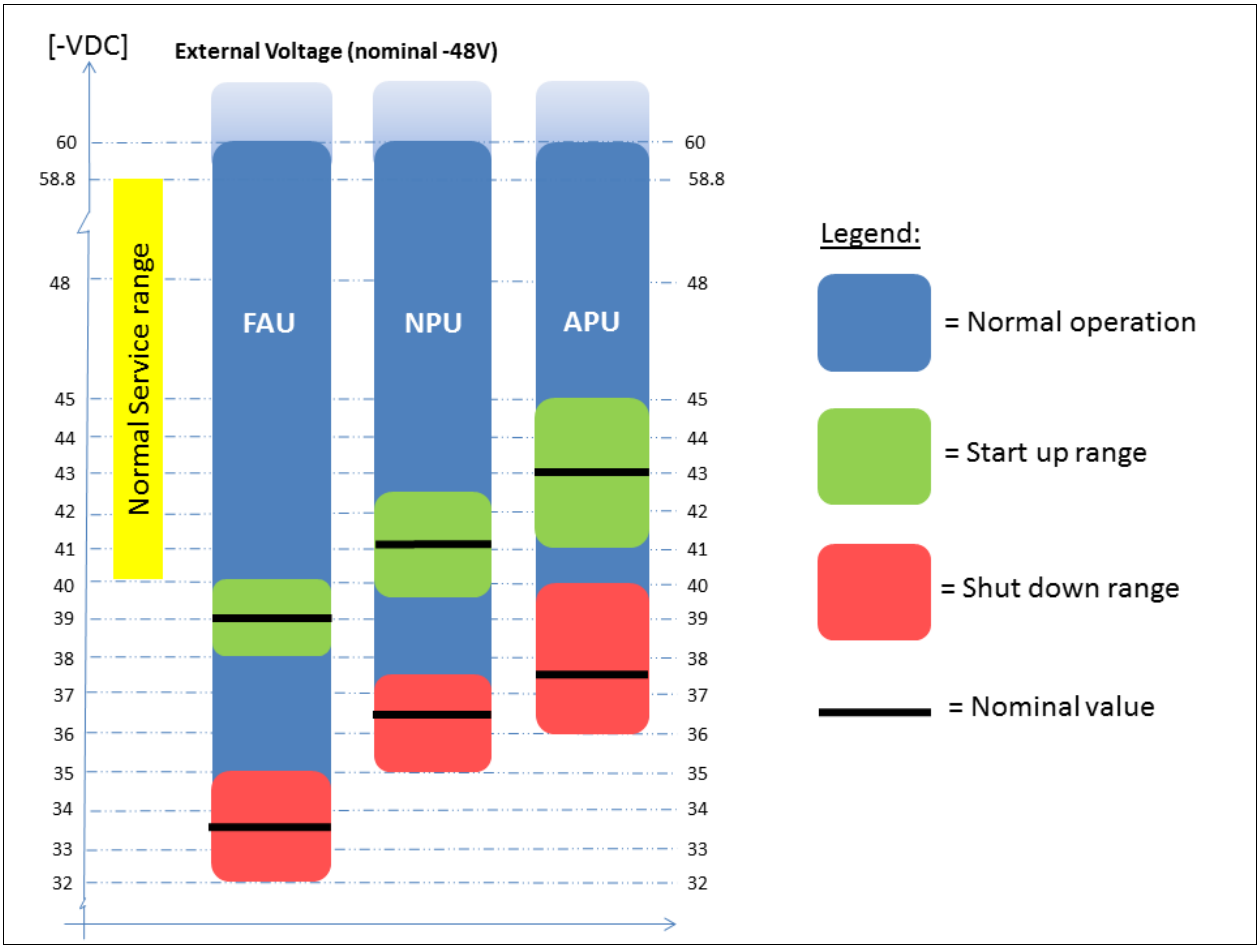


Figure 113 Start and Stop Voltages

## 15.7 MINI-LINK 6694

MINI-LINK 6694 is suitable for end site and repeater site applications as well as medium-sized hub sites or prioritized small-sites.

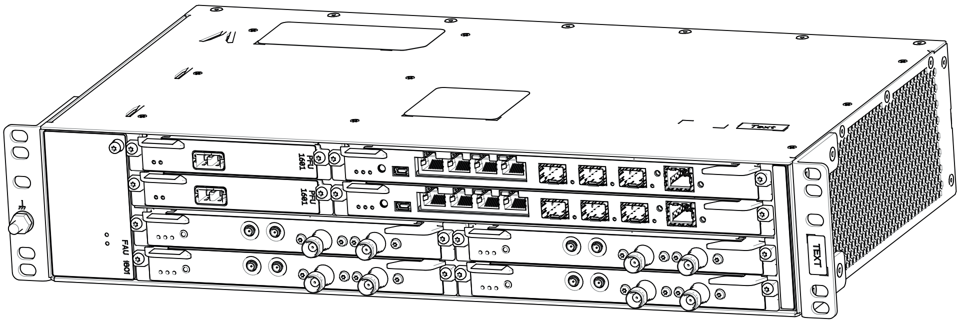


Figure 114 MINI-LINK 6694

MINI-LINK 6694 consists of a rack, Enclosure 1601, that must be equipped with a fan, FAU 1601, and power supply, PFU 1601.

MINI-LINK 6694 can also be equipped with one or two NPU 1002/NPU 1005 or one NPU1003 and up to four MMU 1001/1002, LTU 1001/1002, or a combination thereof. It is not possible to combine NPU 1002 and NPU 1005 in the same magazine. LTU 1001 provides E1/DS1 interfaces for PDH, and LTU 1002 provides E1/DS1 and STM-1 interfaces for PDH and SDH. MINI-LINK 6694 can also be equipped with ETU 1001/1002, which provides additional Ethernet interfaces.

To achieve NPU protection, two NPU 1002 or two NPU 1005 must be used. See Section 15.7.4 on page 167.

Unused slots in MINI-LINK 6694 must be equipped with Dummy Units, as this is essential to maintain the cooling within the magazines and to meet EMC requirements.

MINI-LINK 6694 can be fitted in a standard 19" or metric rack or on a wall using a dedicated mounting set. The height of MINI-LINK 6694 is 2U.

### 15.7.1 PFU 1601

Power handling and filtering is performed by the Power Filter Unit (PFU) 1601, see Figure 115.

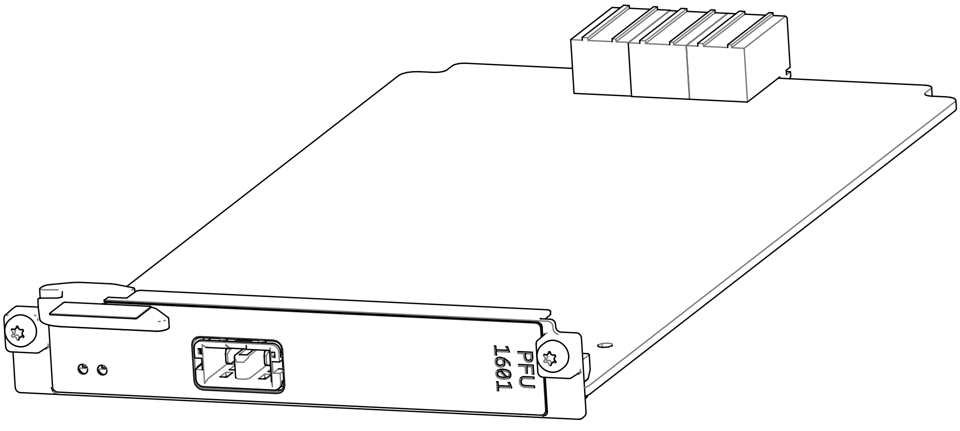


Figure 115 PFU 1601

To achieve redundant power, two power sources must be connected.

### 15.7.1.1 System Monitoring

The PFU supports the monitoring of the node power consumption by measuring the input current and voltage on the incoming −48V.

The following data can be read:

- The current values of input voltage and the power consumption of the node.
- The accumulated and persistently stored energy consumption of the node.

## 15.7.2 FAU 1601

Air-cooling is provided by FAU 1601, see Figure 116.

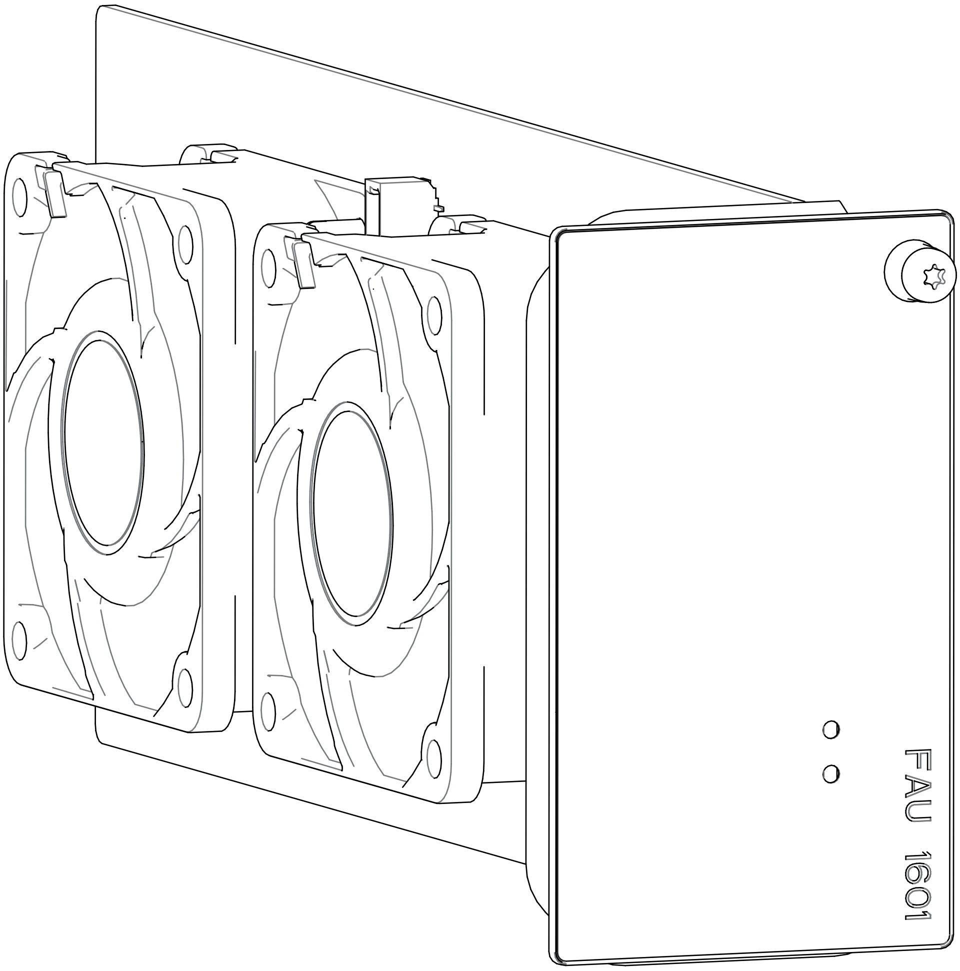


Figure 116 FAU 1601

FAU 1601 has an automatic fan speed control and houses two internal fans.

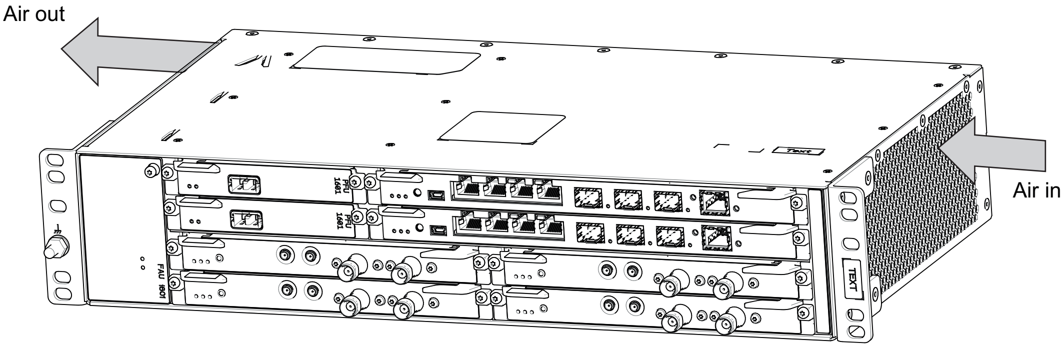


Figure 117 Cooling Airflow in MINI-LINK 6694

The air enters at the right side of the enclosure and exits at the left side of the enclosure.

### 15.7.3 Backplane Architecture

MINI-LINK 6694 provides high-speed connections of up to 10 Gbps between the NPUs, MMUs, ETUs and LTUs. The available traffic capacity depends on the board types and their positions in the enclosure.

The MMUs, ETUs, and LTUs are placed in the Application Plug-in Unit (APU) slots, that is, slots 1–2 and 5–6.

| Slot | Ethernet Capacity with NPU 1002 [Gbps] |
|---|---|
| 6 | 1×2.5 + 1×1 |
| 5 | 2×2.5 |
| 2 | 1×10 or 4×2.5 |
| 1 | 2×2.5 |

| Slot | Ethernet Capacity with NPU 1003 [Gbps] |
|---|---|
| 6 | 2×2.5 |
| 5 | 1×2.5 |
| 2 | 1×10 or 4×2.5 |
| 1 | 2×2.5 |

| Slot | Ethernet Capacity with NPU 1005 [Gbps] |
|---|---|
| 6 | 1×2.5 |
| 5 | 1×10 or 4×2.5 |
| 2 | 1×10 or 4×2.5 |
| 1 | 1×10 or 4×2.5 |

The following pairs of slots are interconnected (2-BPI) in the MINI-LINK 6694 backplane and can be used for Modem Equipment Protection (EQP):

- Slots 1 and 2
- Slots 5 and 6

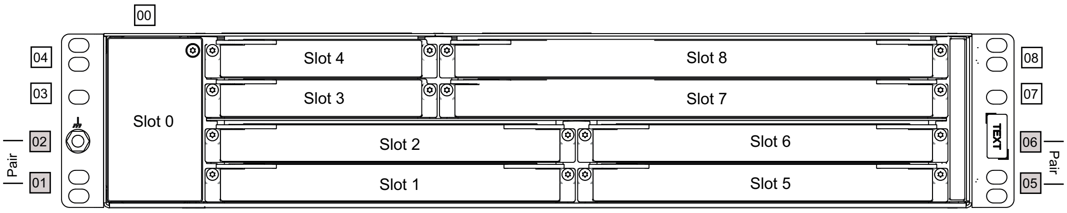


Figure 118 Interconnected Slots in MINI-LINK 6694

## 15.7.4 NPU Protection

When two NPU 1002/NPU 1005 are inserted into MINI-LINK 6694, NPU Protection can provide board, port, and full functional redundancy for the NPU, if configured and licensed properly. It is not possible to combine NPU 1002 and NPU 1005 in the same magazine.

In case of a hardware or software fault in the Master NPU, an automatic failover takes place, and the Slave NPU becomes the Master by inheriting all configurations. All user traffic and DCN access recovers after the failover.

When having two NPU 1002, the front LAN ports of the Slave NPU can be extended and configured to be used for user traffic. This way, the extended ports can have different configurations than the corresponding port of the Master NPU and can be used in different setups. After fail- or switchover, the configuration remains on each port, but the ports of the new Slave NPU are handled as extended.

**Note:** The front LAN ports on the slave NPU cannot be extended on NPU 1005.

## 15.7.5 Hardware Handling

The system offers several functions for easy operation and maintenance.

- Plug-in units can be inserted while the NE is in operation. This allows for adding new Radio Terminals or other plug-in units without disturbing the existing traffic.
- Plug-in units other than the NPU can be removed while the NE is in operation.
- When replacing a faulty plug-in unit, the new plug-in unit automatically inherits the configuration of the old plug-in unit.
- The configuration file is stored non-volatile both on the RMM and in a flash memory on the NPU and can also be backed up and restored using a local or central FTP server. The RMM storage thus enables NPU replacement without using an FTP server.

- The backplane in all subracks has a digital serial number which is also stored on the RMM of the NPU. When inserting an NPU, for example, as a replacement, the serial numbers are compared on power-up.

- Various restarts can be ordered from the management system. A cold restart can be initiated for an NE or a single plug-in unit, and it disturbs the traffic. A warm restart is only available for the whole NE, and it restarts the control system and does not affect the traffic due to the separated control and traffic systems.

- All plug-in units are equipped with temperature sensors. Overheated boards that exceed threshold limits are put in out-of-service by the control system. This is to avoid hardware failures in case of over-heating, for example, due to a fan failure or an ambient temperature that is too high. The plug-in unit is automatically returned to normal operation when the temperature is below the high threshold limit.

  There are two thresholds:

  - The high temperature threshold:

    The NPU raises a temperature alarm (critical). The NPU is still in full operation.

    All plug-in units except NPUs raise a temperature alarm (minor). The plug-in unit is still in full operation.

  - The excessive temperature threshold:

    The NPU shuts down the entire NPU (out of service).

    All plug-in-units except NPUs raise a temperature alarm (critical) and shut down the entire plug-in unit (out of service).

- Access to inventory data like software and hardware product numbers, serial number, and version. User-defined asset identification is supported, enabling hardware tracking.

- Slot availability and capacity can be monitored by using MINI-LINK Node GUI or the CLI. In this way, choosing the correct slot when adding additional plug-in units is made easier.

### 15.7.6 Input Voltage Behavior

Figure 119 shows the input voltage behavior for MINI-LINK 6694. The different units turn on and off at different voltages.

To prevent the units from turning on and off repeatedly around a threshold (so called power flapping), there is a hysteresis for all units.

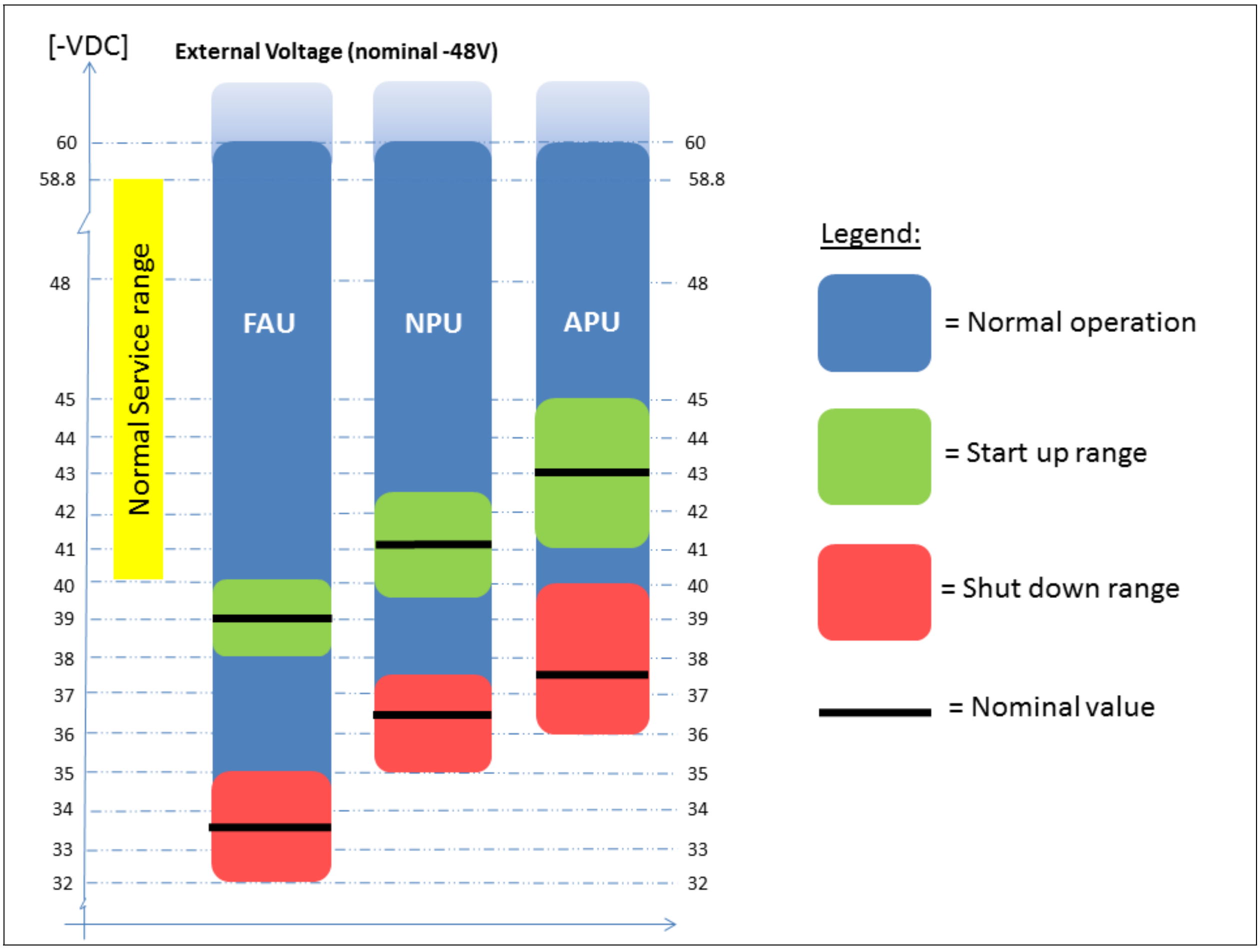


Figure 119 Start and Stop Voltages

## 15.8 NPU 1002

NPU 1002 is a full size processor board that fits in MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, and MINI-LINK 6694.

NPU 1002 contains an embedded Ethernet switch which makes it an ideal component at a medium or small Ethernet aggregation site. It also supports Synchronous Ethernet.

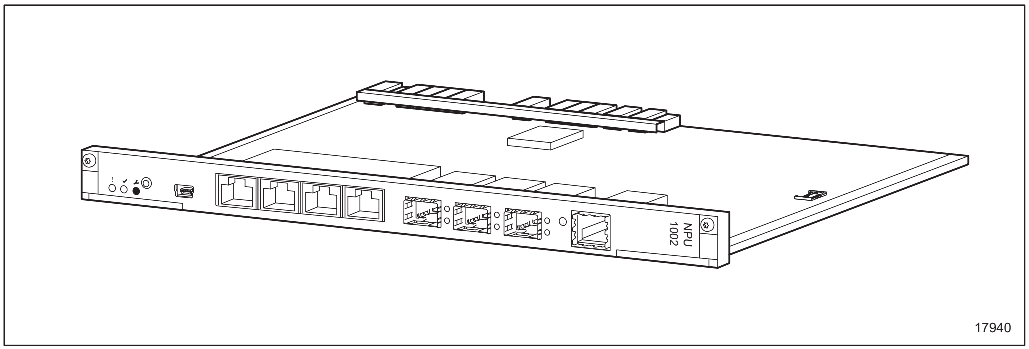


Figure 120 NPU 1002

The NPU 1002 supports the following Ethernet-related features:

- Store and forward MAC (IEEE802.1D-2004) and VLAN-based switching (IEEE802.1Q-2005 and IEEE802.1ad-2005).
- Port-based VLAN (up to 1,000 VLANs in the range of 1–4094).
- MAC address table (32,000 entries) with learning and aging.
- IPv4 and IPv6
- Static unicast/multicast routes.
- Jumbo frames for LAN and Packet Link WAN ports.
- Multiple internal Layer 1 and Layer 2 Ethernet connections.
- MSTP/RSTP/LAG protection mechanism.
- Link Aggregation Control Protocol (LACP).
- Link Loss Forwarding for internal Layer 1 connections.
- Policing/color marking per ingress port with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress port per QoS priority with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress port per VLAN with CIR/EIR and CBS/EBS.
- Traffic shaping per egress port with CIR and CBS.
- 2 MHz sync input/output.
- Ethernet loop detection.
- Broadcast/multicast/destination lookup failure storm protection.
- Frame admission control.
- Classification/tagging of priority and VLAN ID.

- Congestion handling with eight priority queues (TC) per port.
  - Frame discard: WRED, color dropping, aging and tail drop.
  - TC scheduling: SP, WDRR.
- In-band management transport in Ethernet flow (DCN over VLAN).
- Management/diagnostics.
  - PM counters.
  - Link OAM.
  - Ethernet Service OAM.
  - Port mirroring.

### 15.8.1 NPU 1002 Front Interfaces

- **O&M** – Mini USB port for Local Management.
- **SYNC: 1PPS + ToD** – HW prepared.
- **SYNC: 2 MHz** – 2 MHz/2048 Kbps sync input/output.
- **TN 4** & **TN 5** – 2 x RJ 45 10Mbps/100Mbps/1Gbps Ethernet ports. All LAN ports are SyncE capable.
- **TN 6** – 1 x SFP 1Gbps Ethernet port. SyncE capable except with SFPe.
- **TN 7** & **TN 8** – 2 x SFP/SFP+ 1Gbps or 10Gbps Ethernet ports. All LAN ports are SyncE capable except with SFPe.
- **USER I/O** – 6 user in, 3 user out.

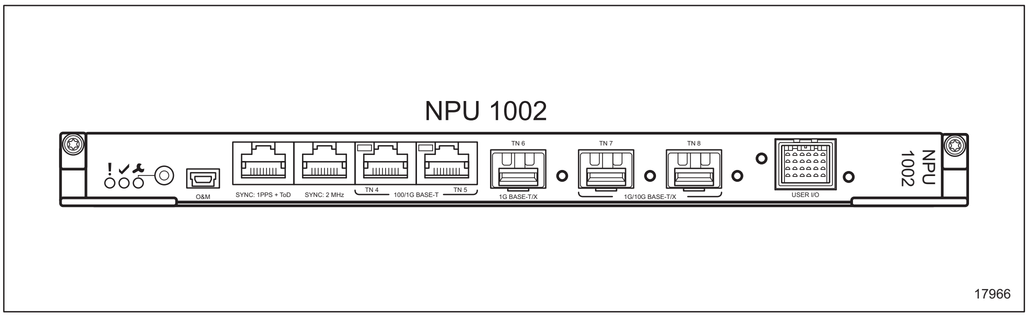


Figure 121 Front Interfaces on the NPU 1002

NPU 1002 has two fixed electrical LAN 10/100/1000BASE-T Ethernet interfaces, one SFP cage supporting 1 Gbps, and two SFP+ cages supporting up to 10 Gbps on the front. One of the fixed Ethernet ports can be configured as a site LAN port.

The SFP/SFP+ cages can be equipped with Ericsson approved SFP/SFP+ modules, see MINI-LINK 6600 R1 Compatibility, Reference [1].

The User I/O interface provides six User Input ports and three User Output ports.

For the basic offering for NPU 1002, two Ethernet ports are enabled at the front. To get access to more ports, licenses are needed. Licenses are also needed for the 10G ports.

NPU 1002 supports Packet Link WAN connections.

The high speed connections and the LAN ports enable NPU 1002 to aggregate traffic from multiple directions as well as dropping Ethernet traffic locally at the site.

#### 15.8.1.1 User Input/Output

The User Input ports can be used to connect user alarms to MINI-LINK Node GUI. Applications like fire alarms, burglar alarms, and low power indicators are easily implemented using these input ports. The User Input ports can be configured to be normally opened or closed.

The User Output ports can be used to export summary alarms of the accumulated severity in the NE to the supervision system of other equipment. The User Output ports can be controlled by the operator or triggered by one or several alarm severities.

Table 25 NPU 1002 User Input and Output Ports

| Plug-In Unit | Number of Input Signals | Number of Output Signals | Connector Type |
|---|---|---|---|
| NPU 1002 | Six | Three | Male 24 pin SOFIX connector |

### 15.8.2 Ethernet Switch

The Ethernet switch functionality is shown in Table 26.

Table 26 Ethernet Switch Functionality

| Modes | Port roles | Comment |
|---|---|---|
| Provider Bridge mode | CE-UNI | CEP, including default mapping rule |
| | CN-UNI | CNP |
| | I-NNI | – |

| Modes | Port roles | Comment |
|---|---|---|
| Customer Bridge mode | UNI | Including QinQ termination, default mapping rule |
| | NNI | – |

The switch is a managed VLAN switch (IEEE 802.1Q and IEEE 802.1D) and supports Provider mode (IEEE 802.1ad) and Customer mode (IEEE 802.1Q) switching.

The switch supports Jumbo frames. The Ethernet site LAN ports on NPU 1002 have interfaces that support auto-negotiation 10/100/1000 Mbps speed. The interfaces are physical RJ-45 connectors.

### 15.8.3 Ethernet LAN Ports

The Ethernet LAN ports are described in Table 27.

Table 27 Ethernet LAN Ports

| Functionality | Description |
|---|---|
| Interface types | 10/100/1000 Mbps<br>10 Gbps<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Duplex mode | Full duplex.<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Connectors/cables | RJ-45 with MDI/MDIX support for all electrical i/f.<br>Single/multi-mode fiber with LC connector for the optical i/f. |
| SFP modules | SFP/SFP+ plug-in modules are supported with 1 Gbps and 10 Gbps optical and 100/1000 Mbps electrical interfaces.<br>For more information regarding SFP/SFP+, see MINI-LINK 6600 R1 Compatibility, Reference [1]. |
| LED indicators | Each Ethernet interface has one green LED for network link indication. |
| Standard frame sizes | Up to 2000 bytes when used as an external interface (IEEE802.3as-2006).<br>Up to 2048 bytes when used as an internal interface. |
| Jumbo frames | 9,216 byte frame size for data applications. |

Table 27 Ethernet LAN Ports

| Functionality | Description |
|---|---|
| Buffer capacity | Ethernet ports share a 720 MB buffering capacity. The buffer capacity sharing among the traffic queues is based on a fair adaptive dynamic algorithm. |
| Flow control | NPU 1002 supports the IEEE 802.3x standard to handle temporary congestion on ports configured as Layer 2 connections (connected to the switch). NPU 1002 only supports asymmetrical flow control. When a congestion threshold is reached in an NE downstream, the NE generates a PAUSE signal and NPU 1002 temporarily halts the transmission of Ethernet frames, but NPU 1002 cannot generate PAUSE signals to control the transmission process on connected equipment. |

## 15.9 NPU 1003

NPU 1003 is a processor board that fits in MINI-LINK 6691 MINI-LINK 6693, and MINI-LINK 6694.

NPU 1003 contains an embedded Ethernet switch which makes it an ideal component at a medium or small Ethernet aggregation site. It also supports Synchronous Ethernet.

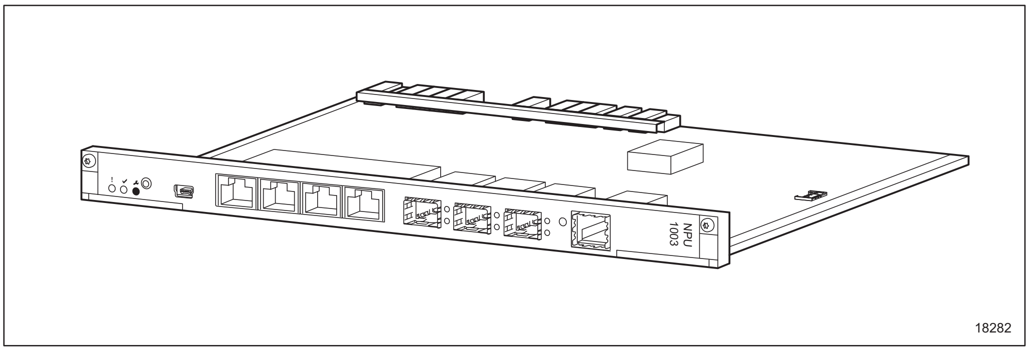


Figure 122 NPU 1003

The NPU 1003 supports the following Ethernet-related features:

- Store and forward MAC (IEEE802.1D-2004) and VLAN-based switching (IEEE802.1Q-2005 and IEEE802.1ad-2005).
- Port-based VLAN (up to 1,000 VLANs in the range of 1–4094).
- MAC address table (32,000 entries) with learning and aging.
- IPv4 and IPv6
- Static unicast/multicast routes.

- Jumbo frames for LAN and Packet Link WAN ports.
- Multiple internal Layer 1 and Layer 2 Ethernet connections.
- MSTP/RSTP/LAG protection mechanism.
- Link Aggregation Control Protocol (LACP).
- Link Loss Forwarding for internal Layer 1 connections.
- Policing/color marking per ingress port with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress port per QoS priority with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress port per VLAN with CIR/EIR and CBS/EBS.
- Traffic shaping per egress port with CIR and CBS.
- 2 MHz/2048 Kbps sync input/output.
- Ethernet loop detection.
- Broadcast/multicast/destination lookup failure storm protection.
- Frame admission control.
- Classification/tagging of priority and VLAN ID.
- Congestion handling with eight priority queues (TC) per port.
  - Frame discard: WRED, color dropping, aging and tail drop.
  - TC scheduling: SP, WDRR.
- In-band management transport in Ethernet flow (DCN over VLAN).
- Management/diagnostics.
  - PM counters.
  - Link OAM.
  - Ethernet Service OAM.
  - Port mirroring.

### 15.9.1 NPU 1003 Front Interfaces

- **O&M** – Mini USB port for Local Management.
- **SYNC: 1PPS + ToD** – HW prepared.
- **SYNC: 2 MHz** – 2 MHz/2048 Kbps sync input/output.

- **TN 4** & **TN 5** – 2 x RJ 45 10Mbps/100Mbps/1Gbps Ethernet ports. All LAN ports are SyncE capable.
- **TN 6** – 1 x SFP 1Gbps Ethernet port. SyncE capable except with SFPe.
- **TN 7** & **TN 8** – 2 x SFP/SFP+ 1Gbps or 10Gbps Ethernet ports. All LAN ports are SyncE capable except with SFPe.
- **TN 9** – 4 E1/DS1 and User I/O (2 user in, 1 user out). The E1 interface can be used as sync source.

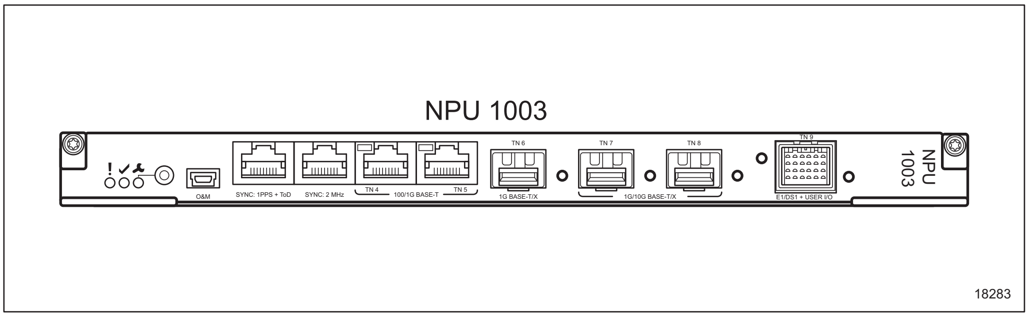


Figure 123 Front Interfaces on the NPU 1003

NPU 1003 has two fixed electrical LAN 10/100/1000BASE-T Ethernet interfaces, one SFP cage supporting 1Gbps, and two SFP+ cages supporting up to 10 Gbps on the front. One of the fixed Ethernet ports can be configured as a site LAN port. The NPU 1003 also has shared E1/DS1 and User I/O port.

The SFP/SFP+ cages can be equipped with Ericsson approved SFP/SFP+ modules, see MINI-LINK 6600 R1 Compatibility, Reference [1].

The User I/O interface provides two User Input ports and one User Output port.

For the basic offering for NPU 1003, two Ethernet ports are enabled at the front. To get access to more ports, licenses are needed. Licenses are also needed for the 10G ports.

NPU 1003 supports Packet Link WAN connections.

The high speed connections and the LAN ports enable NPU 1003 to aggregate traffic from multiple directions as well as dropping Ethernet traffic locally at the site.

### 15.9.1.1 User Input/Output

The User Input ports can be used to connect user alarms to MINI-LINK Node GUI. Applications like fire alarms, burglar alarms, and low power indicators are easily implemented using these input ports. The User Input ports can be configured to be normally opened or closed.

The User Output ports can be used to export summary alarms of the accumulated severity in the NE to the supervision system of other equipment. The User Output ports can be controlled by the operator or triggered by one or several alarm severities.

Table 28 NPU 1003 User Input and Output Ports

| Plug-In Unit | Number of Input Signals | Number of Output Signals | Connector Type |
|---|---|---|---|
| NPU 1003 | Two | One | Male 24 pin SOFIX connector |

### 15.9.2 Ethernet Switch

The Ethernet switch functionality is shown in Table 26.

Table 29 Ethernet Switch Functionality

| Modes | Port roles | Comment |
|---|---|---|
| Provider Bridge mode | CE-UNI | CEP, including default mapping rule |
| | CN-UNI | CNP |
| | I-NNI | – |
| Customer Bridge mode | UNI | Including QinQ termination, default mapping rule |
| | NNI | – |

The switch is a managed VLAN switch (IEEE 802.1Q and IEEE 802.1D) and supports Provider mode (IEEE 802.1ad) and Customer mode (IEEE 802.1Q) switching.

The switch supports Jumbo frames. The Ethernet site LAN ports on NPU 1003 have interfaces that support auto-negotiation 10/100/1000 Mbps speed. The interfaces are physical RJ-45 connectors.

### 15.9.3 Ethernet LAN Ports

The Ethernet LAN ports are described in Table 27.

Table 30 Ethernet LAN Ports

| Functionality | Description |
|---|---|
| Interface types | 10/100/1000 Mbps<br>10 Gbps<br>Auto negotiation or manual setting (IEEE802.3-2005). |

Table 30 Ethernet LAN Ports

| Functionality | Description |
|---|---|
| Duplex mode | Full duplex.<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Connectors/cables | RJ-45 with MDI/MDIX support for all electrical i/f.<br>Single/multi-mode fiber with LC connector for the optical i/f. |
| SFP modules | SFP/SFP+ plug-in modules are supported with 1 Gbps and 10 Gbps optical and 100/1000 Mbps electrical interfaces.<br>For more information regarding SFP/SFP+, see MINI-LINK 6600 R1 Compatibility, Reference [1]. |
| LED indicators | Each Ethernet interface has one green LED for network link indication. |
| Standard frame sizes | Up to 2000 bytes when used as an external interface (IEEE802.3as-2006).<br>Up to 2048 bytes when used as an internal interface. |
| Jumbo frames | 9,216 byte frame size for data applications. |
| Buffer capacity | Ethernet ports share a 180 MB buffering capacity. The buffer capacity sharing among the traffic queues is based on a fair adaptive dynamic algorithm. |
| Flow control | NPU 1003 supports the IEEE 802.3x standard to handle temporary congestion on ports configured as Layer 2 connections (connected to the switch). NPU 1003 only supports asymmetrical flow control. When a congestion threshold is reached in an NE downstream, the NE generates a PAUSE signal and NPU 1003 temporarily halts the transmission of Ethernet frames, but NPU 1003 cannot generate PAUSE signals to control the transmission process on connected equipment. |

## 15.10 NPU 1005

NPU 1005 is a full size processor board that fits in MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, and MINI-LINK 6694.

NPU 1005 contains an embedded Ethernet switch which makes it an ideal component at a medium or small Ethernet aggregation site.

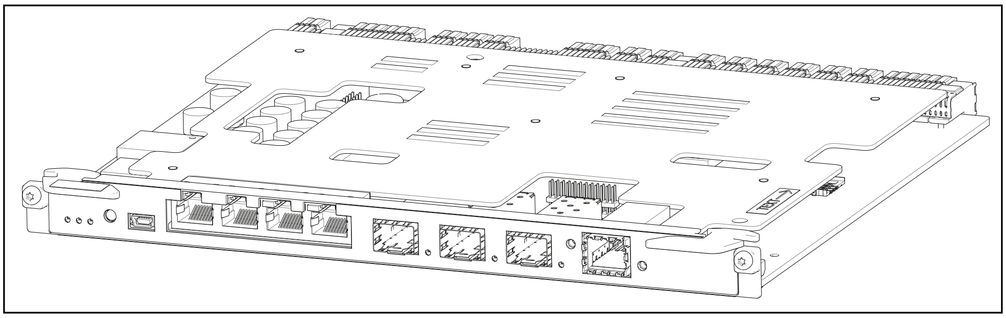


Figure 124 NPU 1005

The NPU 1005 supports the following Ethernet-related features:

- Synchronous Ethernet
- Hierarchical Radio Link Bonding (hRLB)
- Store and forward MAC (IEEE802.1D-2004) and VLAN-based switching (IEEE802.1Q-2005 and IEEE802.1ad-2005).
- Port-based VLAN (up to 1,000 VLANs in the range of 1–4094).
- MAC address table (32,000 entries) with learning and aging.
- IPv4 and IPv6
- Static unicast/multicast routes.
- Jumbo frames for LAN and Packet Link WAN ports.
- Multiple internal Layer 1 and Layer 2 Ethernet connections.
- MSTP/RSTP/LAG protection mechanism.
- Link Aggregation Control Protocol (LACP).
- Link Loss Forwarding for internal Layer 1 connections.
- Policing/color marking per ingress port with CIR/EIR and CBS/EBS.
- Policing/color marking per ingress QoS TC with CIR/EIR and CBS/EBS.
- Traffic shaping per egress port with CIR and CBS.
- 2 MHz sync input/output.
- Ethernet loop detection.
- Broadcast/multicast/destination lookup failure storm protection.
- Frame admission control.
- Classification/tagging of priority and VLAN ID.

- Congestion handling with eight priority queues (TC) per port.
    - Frame discard: WRED, color dropping, aging and tail drop.
    - TC scheduling: SP, WDRR.
- In-band management transport in Ethernet flow (DCN over VLAN).
- Management/diagnostics.
    - PM counters.
    - Link OAM.
    - Ethernet Service OAM.
    - Port mirroring.

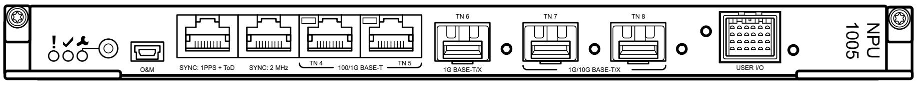


Figure 125 Front Interfaces on the NPU 1005

NPU 1005 has two fixed electrical LAN 10/100/1000BASE-T Ethernet interfaces, one SFP cage, and two SFP+ cages on the front. One of the fixed Ethernet ports can be configured as a site LAN port.

The SFP/SFP+ cages can be equipped with Ericsson approved SFP/SFP+ modules, see MINI-LINK 6600 R1 Compatibility, Reference [1].

The User I/O interface provides six User Input ports and three User Output ports.

For the basic offering for NPU 1005, two Ethernet ports are enabled at the front. To get access to more ports, licenses are needed.

NPU 1005 supports Packet Link WAN connections.

The high speed connections and the LAN ports enable NPU 1005 to aggregate traffic from multiple directions as well as dropping Ethernet traffic locally at the site.

### 15.10.1 Ethernet Switch

The Ethernet switch functionality is shown in Table 26.

Table 31 Ethernet Switch Functionality

| Modes | Port roles | Comment |
|---|---|---|
| Provider Bridge mode | CE-UNI | CEP, including default mapping rule |
| | CN-UNI | CNP |
| | I-NNI | – |
| Customer Bridge mode | UNI | Including QinQ termination, default mapping rule |
| | NNI | – |

The switch is a managed VLAN switch (IEEE 802.1Q and IEEE 802.1D) and supports Provider mode (IEEE 802.1ad) and Customer mode (IEEE 802.1Q) switching.

The switch supports Jumbo frames. The Ethernet site LAN ports on NPU 1005 have interfaces that support auto-negotiation 10/100/1000 Mbps speed. The interfaces are physical RJ-45 connectors.

### 15.10.2 Ethernet LAN Ports

The Ethernet LAN ports are described in Table 27.

Table 32 Ethernet LAN Ports

| Functionality | Description |
|---|---|
| Interface types | 10/100/1000 Mbps<br>10 Gbps<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Duplex mode | Full duplex.<br>Auto negotiation or manual setting (IEEE802.3-2005). |
| Connectors/cables | RJ-45 with MDI/MDIX support for all electrical i/f.<br>Single/multi-mode fiber with LC connector for the optical i/f. |
| SFP modules | SFP/SFP+ plug-in modules are supported with 1 Gbps and 10 Gbps optical and 100/1000 Mbps electrical interfaces.<br>For more information regarding SFP/SFP+, see MINI-LINK 6600 R1 Compatibility, Reference [1]. |
| LED indicators | Each Ethernet interface has one green LED for network link indication. |

Table 32 Ethernet LAN Ports

| **Functionality** | **Description** |
|---|---|
| Standard frame sizes | Up to 2000 bytes when used as an external interface (IEEE802.3as-2006).<br>Up to 2048 bytes when used as an internal interface. |
| Jumbo frames | 9,216 byte frame size for data applications. |
| Buffer capacity | Ethernet ports share a 720 MB buffering capacity. The buffer capacity sharing among the traffic queues is based on a fair adaptive dynamic algorithm. |
| Flow control | NPU 1005 supports the IEEE 802.3x standard to handle temporary congestion on ports configured as Layer 2 connections (connected to the switch). NPU 1005 only supports asymmetrical flow control. When a congestion threshold is reached in an NE downstream, the NE generates a PAUSE signal and NPU 1005 temporarily halts the transmission of Ethernet frames, but NPU 1005 cannot generate PAUSE signals to control the transmission process on connected equipment. |

## 15.11 MMU 1001

MMU 1001 is a single carrier modem.

On one modem, the following is supported:

- Single WAN 1+0

On two modems, the following is supported:

- 2+0 RLB with Equipment Protection (EQP)
- 1+1 RLP with EQP

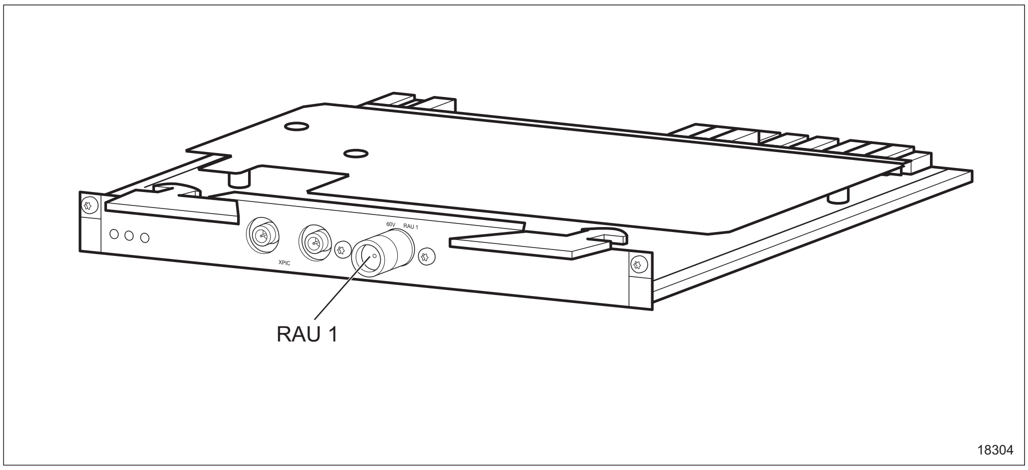


Figure 126 MMU 1001

**Note:** The coaxial interface on modem and radios is equipped with built-in gas discharge tubes for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

Table 38 shows the characteristics of the WAN ports.

Table 33

| Ethernet WAN ports | Description |
|---|---|
| Interface types | 1×Packet Link radio interface. |
| Frame size | An Ethernet over Packet Link WAN port is regarded as an internal MINI-LINK 6600 interface and supports up to 9,216 byte frames (jumbo frames). |
| Throughput | MMU 1001 supports simultaneous PDH and Ethernet transport over the same radio hop. The available bandwidth is split between the PDH and Ethernet traffic.<br>The following maximum bit rate over the radio hop is supported:<br>• ETSI: 1067 Mbps in a 112 MHz channel<br>• ANSI: 767 Mbps in an 80 MHz channel<br>See Table 34 and Table 35 (ETSI), orTable 36 and Table 37 (ANSI) for more information on capacity for MMU 1001. |

| Ethernet WAN ports | Description |
|---|---|
| Latency | The end to end latency for an Ethernet over Packet Link connection will differ based on different parameters, for example, link speed. Typical end to end latency contribution between two Ethernet ports on two nodes connected with Ethernet over packet Link with 558 Mbps link capacity is:<br>• 0.23 ms for 64 byte frame size<br>• 0.29 ms for 1518 byte frame size |
| Buffer capacity | All egress WAN ports are assigned to the centralized deep buffer. The available buffer space is shared between the traffic classes (priority queues) to provide an effective burst absorption capability in a fair manner.<br>The buffer size of traffic class queues can be regulated by configuring a user defined queue-size limit for tail drop or using WRED. |

MMU 1001 is a high-capacity PDH/Ethernet modem with Adaptive Coding and Modulation (ACM), see Section 3.2 on page 13, HW support for XPIC (including XPIC Recovery and Restore), see Section 3.9 on page 28, and modulation schemes up to 4096 QAM.

MMU 1001 has HW support for Radio Link Bonding (RLB). For more information, see Section 3.5 on page 18.

MMU 1001 provides physical layer Sync over Radio Link.

MMU 1001 enables Ethernet transport over a radio hop, that is, a Packet Link. MMU 1001 uses the high speed connections to communicate with the Ethernet switch on the NPU boards.

MMU 1001 carries PDH traffic and have an interface to the TDM bus. The capacity split between packet and circuit transport is configured individually per MMU 1001.

MMU 1001 supports control of the ratio between Ethernet and PDH traffic sent over Hybrid Radio Links. The Ethernet part of the aggregated capacity is set with E1/DS1 granularity.

MMU 1001 has a backplane capacity of up to 2.5 Gbps.

MMU 1001 is used for the traffic capacities specified in Table 34 and Table 35 (ETSI), orTable 36 and Table 37 (ANSI).

Table 34 Aggregated PDH and Ethernet Capacity for MMU 1001 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 4 QAM STRONG | 8 | 18 | 37 | 53 | 75 | 108 | 150 |
| 4 QAM | 10 | 21 | 43 | 62 | 87 | 126 | 175 |
| 16 QAM STRONG | 17 | 37 | 74 | 106 | 150 | 216 | 301 |
| 16 QAM | 20 | 43 | 87 | 124 | 175 | 252 | 351 |
| 32 QAM | 26 | 54 | 109 | 156 | 220 | 317 | 441 |
| 64 QAM | 32 | 68 | 136 | 195 | 276 | 397 | 553 |
| 128 QAM | 38 | 80 | 161 | 231 | 326 | 469 | 653 |
| 256 QAM | 44 | 92 | 186 | 266 | 377 | 541 | 754 |
| 512 QAM | 47 | 99 | 198 | 284 | 402 | 577 | 804 |
| 512 QAM LIGHT | 50 | 105 | 211 | 302 | 427 | 614 | 854 |
| 1024 QAM | 53(1) | 110 | 221 | 316 | 447 | 643 | 895 |
| 1024 QAM LIGHT | 56(1) | 116 | 233 | 334 | 472 | 679 | 945 |
| 2048 QAM | – | 121(1) | 243 | 347 | 491 | 706 | 983 |
| 2048 QAM LIGHT | – | 127(1) | 256 | 365 | 516 | 742 | 1033 |
| 4096 QAM | – | – | 264 | 377 | 533 | 767(1) | 1067(1) |
| 4096 QAM LIGHT | – | – | 276 | 395 | 558 | – | – |

(1) XPIC feature not supported by HW.

Table 35 Maximum PDH Capacities for MMU 1001 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in E1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 4 QAM STRONG | 3×E1 | 7×E1 | 16×E1 | 23×E1 | 34×E1 | 47×E1 | 70×E1 |
| 4 QAM | 3×E1 | 8×E1 | 16×E1 | 27×E1 | 34×E1 | 56×E1 | 80×E1 |
| 16 QAM STRONG | 7×E1 | 16×E1 | 34×E1 | 49×E1 | 71×E1 | 80×E1 | 80×E1 |
| 16 QAM | 7×E1 | 19×E1 | 34×E1 | 57×E1 | 71×E1 | 80×E1 | 80×E1 |
| 32 QAM | 11×E1 | 24×E1 | 51×E1 | 73×E1 | 80×E1 | 80×E1 | 80×E1 |
| 64 QAM | 14×E1 | 31×E1 | 64×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 128 QAM | 17×E1 | 37×E1 | 76×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |

| | Capacity in E1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| **Modulation** | **7 MHz** | **14 MHz** | **28 MHz** | **40 MHz** | **56 MHz** | **80 MHz** | **112 MHz** |
| 256 QAM | 19×E1 | 43×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 512 QAM | 21×E1 | 46×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 512 QAM LIGHT | 21×E1 | 49×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 1024 QAM | 24×E1(1) | 51×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 1024 QAM LIGHT | 24×E1(1) | 54×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 2048 QAM | – | 57×E1(1) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 2048 QAM LIGHT | – | 60×E1(1) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 4096 QAM | – | – | 80×E1 | 80×E1 | 80×E1 | 80×E1(1) | 80×E1(1) |
| 4096 QAM LIGHT | – | – | 80×E1 | 80×E1 | 80×E1 | – | – |

(1) XPIC feature not supported by HW.

Table 36 Aggregated PDH and Ethernet Capacity for MMU 1001 Adaptive Physical Modes (ANSI)

| | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| **Modulation** | **10 MHz** | **20 MHz** | **30 MHz** | **40 MHz** | **50 MHz** | **60 MHz** | **80 MHz** |
| 4 QAM STRONG | 12 | 26 | 39 | 53 | 67 | 81 | 108 |
| 4 QAM | 14 | 30 | 46 | 62 | 78 | 94 | 126 |
| 16 QAM STRONG | 25 | 52 | 79 | 107 | 135 | 162 | 216 |
| 16 QAM | 29 | 61 | 93 | 125 | 157 | 189 | 252 |
| 32 QAM | 36 | 77 | 116 | 157 | 197 | 237 | 317 |
| 64 QAM | 46 | 96 | 146 | 197 | 247 | 297 | 397 |
| 128 QAM | 54 | 114 | 173 | 233 | 292 | 351 | 469 |
| 256 QAM | 63 | 131 | 199 | 268 | 337 | 405 | 541 |
| 512 QAM | 67 | 140 | 213 | 286 | 360 | 432 | 577 |
| 512 QAM LIGHT | 71 | 149 | 226 | 304 | 382 | 459 | 614 |
| 1024 QAM | 74(1) | 156 | 237 | 319 | 400 | 481 | 643 |
| 1024 QAM LIGHT | 79(1) | 165 | 250 | 337 | 423 | 508 | 679 |
| 2048 QAM | – | 171 | 260 | 350 | 440 | 528 | 706 |
| 2048 QAM LIGHT | – | 180 | 273 | 368 | 462 | 555 | 742 |

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | **10 MHz** | **20 MHz** | **30 MHz** | **40 MHz** | **50 MHz** | **60 MHz** | **80 MHz** |
| 4096 QAM | – | – | 282 | 380 | 477 | 574 | 767(1) |
| 4096 QAM LIGHT | – | – | 296 | 398 | 500 | 601 | – |

(1) XPIC feature not supported by HW.

Table 37 Maximum PDH Capacities for MMU 1001 Adaptive Physical Modes (ANSI)

| Modulation | Capacity in DS1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | **10 MHz** | **20 MHz** | **30 MHz** | **40 MHz** | **50 MHz** | **60 MHz** | **80 MHz** |
| 4 QAM STRONG | 5×DS1 | 14×DS1 | 23×DS1 | 32×DS1 | 40×DS1 | 49×DS1 | 66×DS1 |
| 4 QAM | 7×DS1 | 17×DS1 | 27×DS1 | 37×DS1 | 47×DS1 | 58×DS1 | 78×DS1 |
| 16 QAM STRONG | 13×DS1 | 31×DS1 | 48×DS1 | 66×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 16 QAM | 16×DS1 | 36×DS1 | 57×DS1 | 77×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 32 QAM | 21×DS1 | 46×DS1 | 72×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 64 QAM | 27×DS1 | 59×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 128 QAM | 32×DS1 | 70×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 256 QAM | 37×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 512 QAM | 40×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 512 QAM LIGHT | 43×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 1024 QAM | 45×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 1024 QAM LIGHT | 48×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 2048 QAM | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 2048 QAM LIGHT | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 4096 QAM | – | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1(1) |
| 4096 QAM LIGHT | – | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | – |

(1) XPIC feature not supported by HW.

It is possible to configure all Adaptive Coding and Modulation (ACM) physical modes as static physical modes, except for 4096 QAM, by setting **Max Capacity – Modulation** and **Min Capacity – Modulation** to the same value, using MINI-LINK Node GUI. The ACM physical modes configured as static can only be used in hops configured with MMU 1001 on both sides.

### Ethernet WAN Buffers

The WAN port buffers in MINI-LINK 6600 have been designed to handle burst and congestion in order to provide a high link utilization and throughput for high-speed data traffic.

Since extensive buffering has a negative impact on frame delay variation, it is important to have the possibility to regulate buffer/queue size for different traffic classes independently. This can be achieved by using WRED or packet aging.

This means that queues configured to handle delay variation sensitive traffic such as synchronization traffic, shall be regulated accordingly.

In contrast, for traffic queues for less delay variation sensitive traffic the TCP/IP has a congestion avoidance mechanism that is based on buffer utilization. In order to provide a high link utilization and high TCP throughput, queues configured to handle this type of traffic needs to be in the area of hundreds of milliseconds at the smallest congestion point.

## 15.12 MMU 1002

MMU 1002 is a dual carrier modem.

With one modem, the following is supported:

- Single WAN 1+0
- Single WAN 2+0 Radio Link Bonding (RLB)
- Dual WAN 2×(1+0)
- Single WAN 1+1 Radio Link Protection (RLP)

With two modems, the following is supported:

- 1+1 RLP with Equipment Protection (EQP)
- 2+0 RLB with EQP
- 2 x (2+0) RLB with EQP
- 4+0 RLB with EQP
- 2+2 RLP with EQP

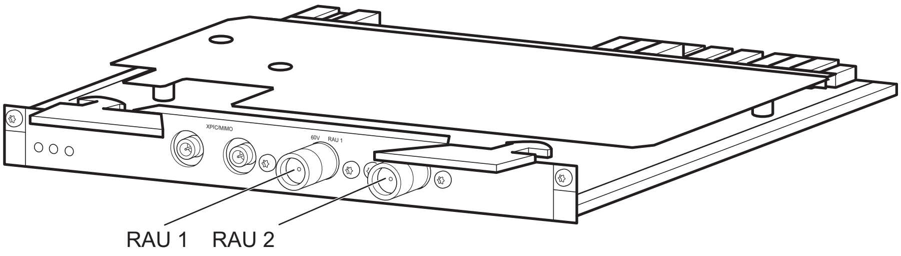


Figure 127 MMU 1002

**Note:** The coaxial interface on modem and radios is equipped with built-in gas discharge tubes for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

Table 38 shows the characteristics of the WAN ports.

Table 38

| Ethernet WAN ports | Description |
|---|---|
| Interface types | 2×Packet Link radio interface. |
| Frame size | An Ethernet over Packet Link WAN port is regarded as an internal MINI-LINK 6600 interface and supports up to 9,216 byte frames (jumbo frames). |
| Throughput | MMU 1002 supports simultaneous PDH and Ethernet transport over the same radio hop. The available bandwidth is split between the PDH and Ethernet traffic.<br>The following maximum bit rate over the radio hop is supported:<br>• ETSI: 1067 Mbps in a 112 MHz channel<br>• ANSI: 767 Mbps in an 80 MHz channel<br>See Table 39 and Table 40 (ETSI), or Table 41 and Table 42 (ANSI) for more information on capacity for MMU 1002. |

| Ethernet WAN ports | Description |
|---|---|
| Latency | The end to end latency for an Ethernet over Packet Link connection will differ based on different parameters, for example, link speed. Typical end to end latency contribution between two Ethernet ports on two nodes connected with Ethernet over packet Link with 558 Mbps link capacity is:<br>• 0.23 ms for 64 byte frame size<br>• 0.29 ms for 1518 byte frame size |
| Buffer capacity | All egress WAN ports are assigned to the centralized deep buffer. The available buffer space is shared between the traffic classes (priority queues) to provide an effective burst absorption capability in a fair manner.<br>The buffer size of traffic class queues can be regulated by configuring a user defined queue-size limit for tail drop or using WRED. |

MMU 1002 is a high-capacity PDH/Ethernet modem with support for XPIC (including XPIC Recovery and Restore), see Section 3.9 on page 28, Adaptive Coding and Modulation (ACM), see Section 3.2 on page 13, and modulation schemes up to 4096 QAM.

MMU 1002 supports Radio Link Bonding (RLB), see Section 3.5 on page 18.

MMU 1002 provides physical layer Sync over Radio Link.

MMU 1002 enables Ethernet transport over a radio hop, that is, a Packet Link. MMU 1002 uses the high speed connections to communicate with the Ethernet switch on the NPU boards.

MMU 1002 carries PDH traffic and have an interface to the TDM bus. The capacity split between packet and circuit transport is configured individually per MMU 1002.

MMU 1002 supports control of the ratio between Ethernet and PDH traffic sent over Hybrid Radio Links. The Ethernet part of the aggregated capacity is set with E1/DS1 granularity.

MMU 1002 has a backplane capacity of up to 2×2.5 Gbps.

MMU 1002 is used for the traffic capacities specified in Table 39 and Table 40 (ETSI), or Table 41 and Table 42 (ANSI).

Using two MMU 1002s, a 4 x 4 MIMO configuration with two separated cross-polarization antennas can provide very high spectral efficiency.

Table 39 Aggregated PDH and Ethernet Capacity for MMU 1002 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | **7 MHz** | **14 MHz** | **28 MHz** | **40 MHz** | **56 MHz** | **80 MHz** | **112 MHz** |
| 4 QAM STRONG | 8 | 18 | 37/36(1) | 53 | 75/73(1) | 108 | 150 |
| 4 QAM | 10 | 21 | 43/42(1) | 62 | 87/86(1) | 126 | 175 |
| 16 QAM STRONG | 17 | 37 | 74/72(1) | 106 | 150/146(1) | 216 | 301 |
| 16 QAM | 20 | 43 | 87/85(1) | 124 | 175/171(1) | 252 | 351 |
| 32 QAM | 26 | 54 | 109/109(1) | 156 | 220/219(1) | 317 | 441 |
| 64 QAM | 32 | 68 | 136/133(1) | 195 | 276/268(1) | 397 | 553 |
| 128 QAM | 38 | 80 | 161/157(1) | 231 | 326/317(1) | 469 | 653 |
| 256 QAM | 44 | 92 | 186/182(1) | 266 | 377/366(1) | 541 | 754 |
| 512 QAM | 47 | 99 | 198/194(1) | 284 | 402/390(1) | 577 | 804 |
| 512 QAM LIGHT | 50 | 105 | 211/206(1) | 302 | 427/415(1) | 614 | 854 |
| 1024 QAM | 53(2) | 110 | 221 | 316 | 447/435(1) | 643 | 895 |
| 1024 QAM LIGHT | 56(2) | 116 | 233 | 334 | 472/459(1) | 679 | 945 |
| 2048 QAM | – | 121(2) | 243 | 347 | 491 | 706 | 983 |
| 2048 QAM LIGHT | – | 127(2) | 256 | 365 | 516 | 742 | 1033 |
| 4096 QAM | – | – | 264 | 377 | 533 | 767(2) | 1067(2) |
| 4096 QAM LIGHT | – | – | 276 | 395 | 558 | – | – |

(1) MIMO supported. Smaller capacity applies for MIMO configuration.

(2) XPIC not supported.

Table 40 Maximum PDH Capacities for MMU 1002 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in E1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | **7 MHz** | **14 MHz** | **28 MHz** | **40 MHz** | **56 MHz** | **80 MHz** | **112 MHz** |
| 4 QAM STRONG | 2×E1 | 6×E1 | 15×E1/15×E1(1) | 23×E1 | 34×E1/33×E1(1) | 47×E1 | 70×E1 |
| 4 QAM | 3×E1 | 8×E1 | 18×E1/18×E1(1) | 28×E1 | 40×E1/39×E1(1) | 56×E1 | 80×E1 |

| Modulation | Capacity in E1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 16 QAM STRONG | 6×E1 | 15×E1 | 34×E1/33×E1(1) | 49×E1 | 70×E1/68×E1(1) | 80×E1 | 80×E1 |
| 16 QAM | 7×E1 | 18×E1 | 39×E1/38×E1(1) | 57×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 32 QAM | 10×E1 | 24×E1 | 50×E1/50×E1(1) | 73×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 64 QAM | 13×E1 | 30×E1 | 63×E1/62×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 128 QAM | 16×E1 | 36×E1 | 75×E1/74×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 256 QAM | 19×E1 | 42×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 512 QAM | 21×E1 | 45×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 512 QAM LIGHT | 22×E1 | 48×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 1024 QAM | 23×E1(2) | 51×E1 | 80×E1 | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 1024 QAM LIGHT | 25×E1(2) | 54×E1 | 80×E1 | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 2048 QAM | – | 56×E1(2) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 2048 QAM LIGHT | – | 59×E1(2) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 4096 QAM | – | – | 80×E1 | 80×E1 | 80×E1 | 80×E1(2) | 80×E1(2) |
| 4096 QAM LIGHT | – | – | 80×E1 | 80×E1 | 80×E1 | – | – |

(1) MIMO supported. Smaller capacity applies for MIMO configuration.

(2) XPIC not supported.

Table 41 Aggregated PDH and Ethernet Capacity for MMU 1002 Adaptive Physical Modes (ANSI)

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz | 80 MHz |
| 4 QAM STRONG | 12 | 26 | 39/39,0(1) | 53/52,4(1) | 67 | 81 | 108 |
| 4 QAM | 14 | 30 | 46/45,8(1) | 62/61,5(1) | 78 | 94 | 126 |
| 16 QAM STRONG | 25 | 52 | 79/78,0(1) | 107/104,7(1) | 135 | 162 | 216 |
| 16 QAM | 29 | 61 | 93/91,0(1) | 125/122,2(1) | 157 | 189 | 252 |
| 32 QAM | 36 | 77 | 116/117,0(1) | 157/157,1(1) | 197 | 237 | 317 |
| 64 QAM | 46 | 96 | 146/143,0(1) | 197/192,0(1) | 247 | 297 | 397 |

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz | 80 MHz |
| 128 QAM | 54 | 114 | 173/169,0(1) | 233/226,9(1) | 292 | 351 | 469 |
| 256 QAM | 63 | 131 | 199/195,0(1) | 268/261,9(1) | 337 | 405 | 541 |
| 512 QAM | 67 | 140 | 213/208,0(1) | 286/279,3(1) | 360 | 432 | 577 |
| 512 QAM LIGHT | 71 | 149 | 226/221,0(1) | 304/296,8(1) | 382 | 459 | 614 |
| 1024 QAM | 74(2) | 156 | 237 | 319 | 400 | 481 | 643 |
| 1024 QAM LIGHT | 79(2) | 165 | 250 | 337 | 423 | 508 | 679 |
| 2048 QAM | – | 171 | 260 | 350 | 440 | 528 | 706 |
| 2048 QAM LIGHT | – | 180 | 273 | 368 | 462 | 555 | 742 |
| 4096 QAM | – | – | 282 | 380 | 477 | 574 | 767(2) |
| 4096 QAM LIGHT | – | – | 296 | 398 | 500 | 601 | – |

(1) MIMO supported. The second capacity applies for MIMO configuration.

(2) XPIC not supported.

Table 42 Maximum PDH Capacities for MMU 1002 Adaptive Physical Modes (ANSI)

| Modulation | Capacity in DS1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz | 80 MHz |
| 4 QAM STRONG | 5×DS1 | 14×DS1 | 23×DS1/22×DS1(1) | 32×DS1/31×DS1(1) | 40×DS1 | 49×DS1 | 66×DS1 |
| 4 QAM | 7×DS1 | 17×DS1 | 27×DS1/26×DS1(1) | 37×DS1/36×DS1(1) | 47×DS1 | 58×DS1 | 78×DS1 |
| 16 QAM STRONG | 13×DS1 | 31×DS1 | 48×DS1/47×DS1(1) | 66×DS1/64×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 16 QAM | 16×DS1 | 36×DS1 | 57×DS1/55×DS1(1) | 77×DS1/75×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 32 QAM | 21×DS1 | 46×DS1 | 72×DS1/72×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 64 QAM | 27×DS1 | 59×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 128 QAM | 32×DS1 | 70×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 256 QAM | 37×DS1 | 80×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 512 QAM | 40×DS1 | 80×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 512 QAM LIGHT | 43×DS1 | 80×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |

| Modulation | Capacity in DS1s |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
|  | Channel Bandwidth |  |  |  |  |  |  |
|  | **10 MHz** | **20 MHz** | **30 MHz** | **40 MHz** | **50 MHz** | **60 MHz** | **80 MHz** |
| 1024 QAM | 45×DS1(2) | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 1024 QAM LIGHT | 48×DS1(2) | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 2048 QAM | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 2048 QAM LIGHT | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 4096 QAM | – | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1(2) |
| 4096 QAM LIGHT | – | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | – |

(1) MIMO supported. Smaller capacity applies for MIMO configuration.

(2) XPIC not supported.

It is possible to configure all Adaptive Coding and Modulation (ACM) physical modes as static physical modes, except for 4096 QAM, by setting **Max Capacity – Modulation** and **Min Capacity – Modulation** to the same value, using MINI-LINK Node GUI. The ACM physical modes configured as static can only be used in hops configured with MMU 1002 on both sides.

### Ethernet WAN Buffers

The WAN port buffers in MINI-LINK 6600 have been designed to handle burst and congestion in order to provide a high link utilization and throughput for high-speed data traffic.

Since extensive buffering has a negative impact on frame delay variation, it is important to have the possibility to regulate buffer/queue size for different traffic classes independently. This can be achieved by using WRED or packet aging.

This means that queues configured to handle delay variation sensitive traffic such as synchronization traffic, shall be regulated accordingly.

In contrast, for traffic queues for less delay variation sensitive traffic the TCP/IP has a congestion avoidance mechanism that is based on buffer utilization. In order to provide a high link utilization and high TCP throughput, queues configured to handle this type of traffic needs to be in the area of hundreds of milliseconds at the smallest congestion point.

## 15.13 MMU 1004

MMU 1004 is a dual carrier modem.

With one modem, the following is supported:

- Single WAN 1+0

- Single WAN 2+0 Radio Link Bonding (RLB)
- Dual WAN 2×(1+0)
- Single WAN 1+1 Radio Link Protection (RLP)

With two modems, the following is supported:

- 1+1 RLP with Equipment Protection (EQP)
- 2+0 RLB with EQP
- 2 x (2+0) RLB with EQP
- 4+0 RLB with EQP
- 2+2 RLP with EQP

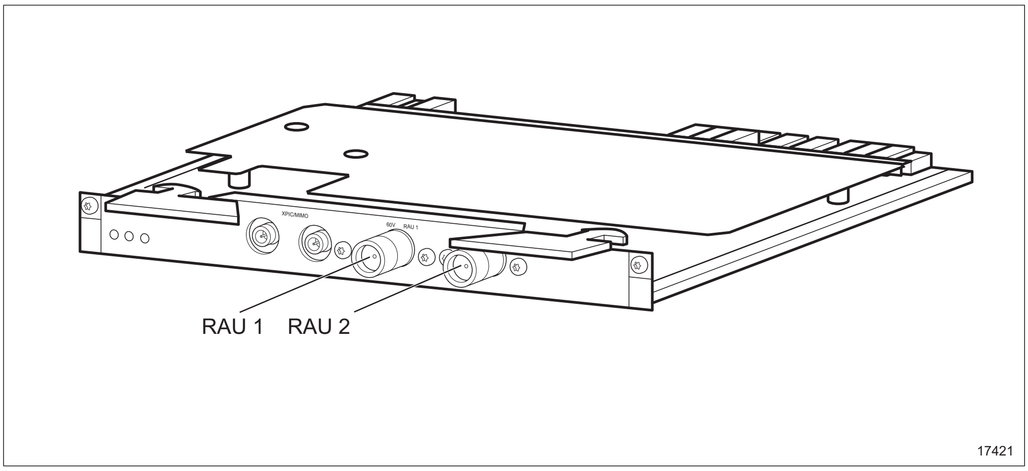


Figure 128 MMU 1004

**Note:** The coaxial interface on modem and radios is equipped with built-in gas discharge tubes for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

Table 43 shows the characteristics of the WAN ports.

Table 43

| Ethernet WAN ports | Description |
|---|---|
| Interface types | 2×Packet Link radio interface. |
| Frame size | An Ethernet over Packet Link WAN port is regarded as an internal MINI-LINK 6600 interface and supports up to 9,216 byte frames (jumbo frames). |

| Ethernet WAN ports | Description |
|---|---|
| Throughput | MMU 1004 supports simultaneous PDH and Ethernet transport over the same radio hop. The available bandwidth is split between the PDH and Ethernet traffic.<br>The following maximum bit rate over the radio hop is supported:<br>• ETSI: 1067 Mbps in a 112 MHz channel<br>• ANSI: 767 Mbps in an 80 MHz channel<br>See Table 39 and Table 40 (ETSI), or Table 41 and Table 42 (ANSI) for more information on capacity for MMU 1004. |
| Latency | The end to end latency for an Ethernet over Packet Link connection will differ based on different parameters, for example, link speed. Typical end to end latency contribution between two Ethernet ports on two nodes connected with Ethernet over packet Link with 558 Mbps link capacity is:<br>• 0.23 ms for 64 byte frame size<br>• 0.29 ms for 1518 byte frame size |
| Buffer capacity | All egress WAN ports are assigned to the centralized deep buffer. The available buffer space is shared between the traffic classes (priority queues) to provide an effective burst absorption capability in a fair manner.<br>The buffer size of traffic class queues can be regulated by configuring a user defined queue-size limit for tail drop or using WRED. |

MMU 1004 is a high-capacity PDH/Ethernet modem with support for XPIC (including XPIC Recovery and Restore), see Section 3.9 on page 28, Adaptive Coding and Modulation (ACM), see Section 3.2 on page 13, and modulation schemes up to 4096 QAM.

MMU 1004 supports Radio Link Bonding (RLB), see Section 3.5 on page 18.

MMU 1004 provides physical layer Sync over Radio Link.

MMU 1004 enables Ethernet transport over a radio hop, that is, a Packet Link. MMU 1004 uses the high speed connections to communicate with the Ethernet switch on the NPU boards.

MMU 1004 carries PDH traffic and have an interface to the TDM bus. The capacity split between packet and circuit transport is configured individually per MMU 1004.

MMU 1004 supports control of the ratio between Ethernet and PDH traffic sent over Hybrid Radio Links. The Ethernet part of the aggregated capacity is set with E1/DS1 granularity.

MMU 1004 has a backplane capacity of up to 2×2.5 Gbps.

MMU 1004 is used for the traffic capacities specified in Table 44 and Table 45 (ETSI), or Table 46 and Table 47 (ANSI).

Using two MMU 1004s, a 4 x 4 MIMO configuration with two separated cross-polarization antennas can provide very high spectral efficiency.

Table 44 Aggregated PDH and Ethernet Capacity for MMU 1004 Adaptive Physical Modes (ETSI)

| **Modulation** | **Capacity in Mbps** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Channel Bandwidth** | | | | | | |
| | **7 MHz** | **14 MHz** | **28 MHz** | **40 MHz** | **56 MHz** | **80 MHz** | **112 MHz** |
| 4 QAM STRONG | 8 | 18 | 37/36(1) | 53 | 75/73(1) | 108 | 150 |
| 4 QAM | 10 | 21 | 43/42(1) | 62 | 87/86(1) | 126 | 175 |
| 16 QAM STRONG | 17 | 37 | 74/72(1) | 106 | 150/146(1) | 216 | 301 |
| 16 QAM | 20 | 43 | 87/85(1) | 124 | 175/171(1) | 252 | 351 |
| 32 QAM | 26 | 54 | 109/109(1) | 156 | 220/219(1) | 317 | 441 |
| 64 QAM | 32 | 68 | 136/133(1) | 195 | 276/268(1) | 397 | 553 |
| 128 QAM | 38 | 80 | 161/157(1) | 231 | 326/317(1) | 469 | 653 |
| 256 QAM | 44 | 92 | 186/182(1) | 266 | 377/366(1) | 541 | 754 |
| 512 QAM | 47 | 99 | 198/194(1) | 284 | 402/390(1) | 577 | 804 |
| 512 QAM LIGHT | 50 | 105 | 211/206(1) | 302 | 427/415(1) | 614 | 854 |
| 1024 QAM | 53(2) | 110 | 221 | 316 | 447/435(1) | 643 | 895 |
| 1024 QAM LIGHT | 56(2) | 116 | 233 | 334 | 472/459(1) | 679 | 945 |
| 2048 QAM | – | 121(2) | 243 | 347 | 491 | 706 | 983 |
| 2048 QAM LIGHT | – | 127(2) | 256 | 365 | 516 | 742 | 1033 |

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 4096 QAM | – | – | 264 | 377 | 533 | 767(2) | 1067(2) |
| 4096 QAM LIGHT | – | – | 276 | 395 | 558 | – | – |

(1) MIMO supported. Smaller capacity applies for MIMO configuration.

(2) XPIC not supported.

Table 45 Maximum PDH Capacities for MMU 1004 Adaptive Physical Modes (ETSI)

| Modulation | Capacity in E1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz | 80 MHz | 112 MHz |
| 4 QAM STRONG | 2×E1 | 6×E1 | 15×E1/15×E1(1) | 23×E1 | 34×E1/33×E1(1) | 47×E1 | 70×E1 |
| 4 QAM | 3×E1 | 8×E1 | 18×E1/18×E1(1) | 28×E1 | 40×E1/39×E1(1) | 56×E1 | 80×E1 |
| 16 QAM STRONG | 6×E1 | 15×E1 | 34×E1/33×E1(1) | 49×E1 | 70×E1/68×E1(1) | 80×E1 | 80×E1 |
| 16 QAM | 7×E1 | 18×E1 | 39×E1/38×E1(1) | 57×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 32 QAM | 10×E1 | 24×E1 | 50×E1/50×E1(1) | 73×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 64 QAM | 13×E1 | 30×E1 | 63×E1/62×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 128 QAM | 16×E1 | 36×E1 | 75×E1/74×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 256 QAM | 19×E1 | 42×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 512 QAM | 21×E1 | 45×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 512 QAM LIGHT | 22×E1 | 48×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 1024 QAM | 23×E1(2) | 51×E1 | 80×E1 | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 1024 QAM LIGHT | 25×E1(2) | 54×E1 | 80×E1 | 80×E1 | 80×E1/80×E1(1) | 80×E1 | 80×E1 |
| 2048 QAM | – | 56×E1(2) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 2048 QAM LIGHT | – | 59×E1(2) | 80×E1 | 80×E1 | 80×E1 | 80×E1 | 80×E1 |
| 4096 QAM | – | – | 80×E1 | 80×E1 | 80×E1 | 80×E1(2) | 80×E1(2) |
| 4096 QAM LIGHT | – | – | 80×E1 | 80×E1 | 80×E1 | – | – |

(1) MIMO supported. Smaller capacity applies for MIMO configuration.

(2) XPIC not supported.

Table 46 Aggregated PDH and Ethernet Capacity for MMU 1004 Adaptive Physical Modes (ANSI)

| Modulation | Capacity in Mbps | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz | 80 MHz |
| 4 QAM STRONG | 12 | 26 | 39/39,0(1) | 53/52,4(1) | 67 | 81 | 108 |
| 4 QAM | 14 | 30 | 46/45,8(1) | 62/61,5(1) | 78 | 94 | 126 |
| 16 QAM STRONG | 25 | 52 | 79/78,0(1) | 107/104,7(1) | 135 | 162 | 216 |
| 16 QAM | 29 | 61 | 93/91,0(1) | 125/122,2(1) | 157 | 189 | 252 |
| 32 QAM | 36 | 77 | 116/117,0(1) | 157/157,1(1) | 197 | 237 | 317 |
| 64 QAM | 46 | 96 | 146/143,0(1) | 197/192,0(1) | 247 | 297 | 397 |
| 128 QAM | 54 | 114 | 173/169,0(1) | 233/226,9(1) | 292 | 351 | 469 |
| 256 QAM | 63 | 131 | 199/195,0(1) | 268/261,9(1) | 337 | 405 | 541 |
| 512 QAM | 67 | 140 | 213/208,0(1) | 286/279,3(1) | 360 | 432 | 577 |
| 512 QAM LIGHT | 71 | 149 | 226/221,0(1) | 304/296,8(1) | 382 | 459 | 614 |
| 1024 QAM | 74(2) | 156 | 237 | 319 | 400 | 481 | 643 |
| 1024 QAM LIGHT | 79(2) | 165 | 250 | 337 | 423 | 508 | 679 |
| 2048 QAM | – | 171 | 260 | 350 | 440 | 528 | 706 |
| 2048 QAM LIGHT | – | 180 | 273 | 368 | 462 | 555 | 742 |
| 4096 QAM | – | – | 282 | 380 | 477 | 574 | 767(2) |
| 4096 QAM LIGHT | – | – | 296 | 398 | 500 | 601 | – |

(1) MIMO supported. The second capacity applies for MIMO configuration.

(2) XPIC not supported.

Table 47 Maximum PDH Capacities for MMU 1004 Adaptive Physical Modes (ANSI)

| Modulation | Capacity in DS1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz | 80 MHz |
| 4 QAM STRONG | 5×DS1 | 14×DS1 | 23×DS1/22×DS1(1) | 32×DS1/31×DS1(1) | 40×DS1 | 49×DS1 | 66×DS1 |
| 4 QAM | 7×DS1 | 17×DS1 | 27×DS1/26×DS1(1) | 37×DS1/36×DS1(1) | 47×DS1 | 58×DS1 | 78×DS1 |
| 16 QAM STRONG | 13×DS1 | 31×DS1 | 48×DS1/47×DS1(1) | 66×DS1/64×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |

| | Capacity in DS1s | | | | | | |
|---|---|---|---|---|---|---|---|
| | Channel Bandwidth | | | | | | |
| **Modulation** | **10 MHz** | **20 MHz** | **30 MHz** | **40 MHz** | **50 MHz** | **60 MHz** | **80 MHz** |
| 16 QAM | 16×DS1 | 36×DS1 | 57×DS1/55×DS1(1) | 77×DS1/75×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 32 QAM | 21×DS1 | 46×DS1 | 72×DS1/72×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 64 QAM | 27×DS1 | 59×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 128 QAM | 32×DS1 | 70×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 256 QAM | 37×DS1 | 80×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 512 QAM | 40×DS1 | 80×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 512 QAM LIGHT | 43×DS1 | 80×DS1 | 80×DS1/80×DS1(1) | 80×DS1/80×DS1(1) | 80×DS1 | 80×DS1 | 80×DS1 |
| 1024 QAM | 45×DS1(2) | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 1024 QAM LIGHT | 48×DS1(2) | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 2048 QAM | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 2048 QAM LIGHT | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 |
| 4096 QAM | – | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1(2) |
| 4096 QAM LIGHT | – | – | 80×DS1 | 80×DS1 | 80×DS1 | 80×DS1 | – |

(1) MIMO supported. Smaller capacity applies for MIMO configuration.

(2) XPIC not supported.

It is possible to configure all Adaptive Coding and Modulation (ACM) physical modes as static physical modes, except for 4096 QAM, by setting **Max Capacity – Modulation** and **Min Capacity – Modulation** to the same value, using MINI-LINK Node GUI. The ACM physical modes configured as static can only be used in hops configured with MMU 1004 on both sides.

### Ethernet WAN Buffers

The WAN port buffers in MINI-LINK 6600 have been designed to handle burst and congestion in order to provide a high link utilization and throughput for high-speed data traffic.

Since extensive buffering has a negative impact on frame delay variation, it is important to have the possibility to regulate buffer/queue size for different traffic classes independently. This can be achieved by using WRED or packet aging.

This means that queues configured to handle delay variation sensitive traffic such as synchronization traffic, shall be regulated accordingly.

In contrast, for traffic queues for less delay variation sensitive traffic the TCP/IP has a congestion avoidance mechanism that is based on buffer utilization. In order to provide a high link utilization and high TCP throughput, queues configured to handle this type of traffic needs to be in the area of hundreds of milliseconds at the smallest congestion point.

## 15.14 LTU 1001

LTU 1001 is a Line Termination Unit (LTU) with 16 E1/DS1 ports for PDH.

LTU 1001 can be used in MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655.

Table 48 LTU 1001 Interfaces

| | |
|---|---|
| Interfaces | 16×E1/DS1<br>• ETSI: 75 Ω or 120 Ω G.703<br>• ANSI: 100 Ω Balanced G.703 |

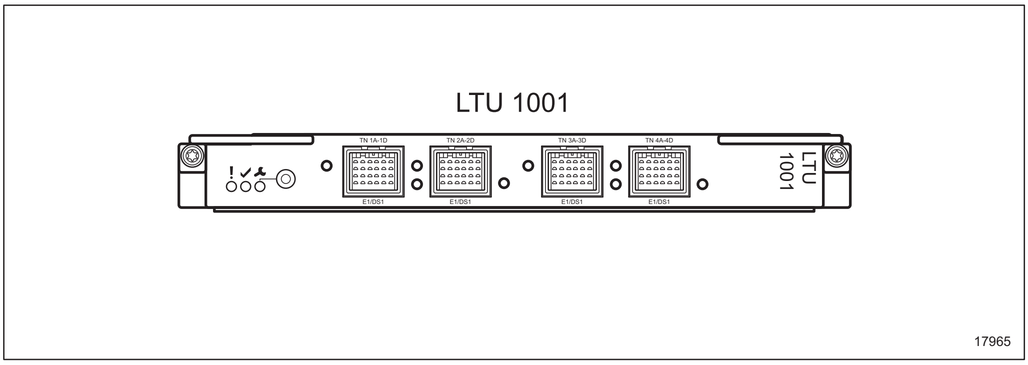


Figure 129 Front Interfaces on the LTU 1001

## 15.15 LTU 1002

LTU 1002 is a Line Termination Unit (LTU) with 16 E1/DS1 ports for PDH and an STM-1 port with up to 63×E1 for SDH. The 16 E1 ports and the STM-1 port with up to 63×E1s can all be used simultaneously. The actual number of supported ports depends on the selected board profile.

**Note:** SDH on LTU 1002 is only available for ETSI, and not for ANSI.

The following board profiles can be set for LTU1002:

| | |
|---|---|
| **PDH and SDH** | Provides 16×E1 front interfaces and one STM-1 front interface for up to 63×E1s. |

| | |
|---|---|
| **PDH and CES** | Provides 16×E1/DS1 front interfaces and 16×CES E1/DS1s through the backplane. |
| **CES only** | Provides 32×CES E1/DS1s through the backplane. |
| **SDH48 and CES32** | Provides one STM-1 front interface for up to 48×E1s, and 32×CES E1s through the backplane. |
| **SDH63 and CES16** | Provides STM-1 termination up to 63xE1s combined with 16xE1s circuit emulation towards the backplane. |
| **PDH and SDH48 and CES16** | Provides a combination of STM-1 (48xE1) and 16x physical E1 termination together with 16xE1s circuit emulation towards the backplane. |

LTU 1002 can be used in MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, MINI-LINK 6694, MINI-LINK 6654, and MINI-LINK 6655.

The SDH functionality consists of front termination, terminal multiplexer, MSP protection and the possibility to send DCN traffic on DCC. The Terminal Multiplexer terminates one STM-1 with 63×E1 mapped asynchronously into 63×VC-12.

At aggregation nodes LTU 1002 acts as an interface between the optical domain and the microwave domain by providing an effective optical northbound interface using one STM-1 connection instead of n×E1 interfaces.

In ring configurations two LTU 1002 can be connected “back-to-back” to allow local add/drop of up to 63×E1. Using two LTU 1002 in a pair provides Multiplexer Section Protection (MSP) 1+1.

LTU 1002 has support for CES, enabling E1/DS1s being transported over packet.

Table 49 LTU 1002 Interfaces

| | |
|---|---|
| Interfaces | 1xSDH SFP (supporting STM-1 for up to 63×E1)<br>16xE1/DS1<br>• ETSI: 75 Ω or 120 Ω G.703<br>• ANSI:100 Ω Balanced G.703 |

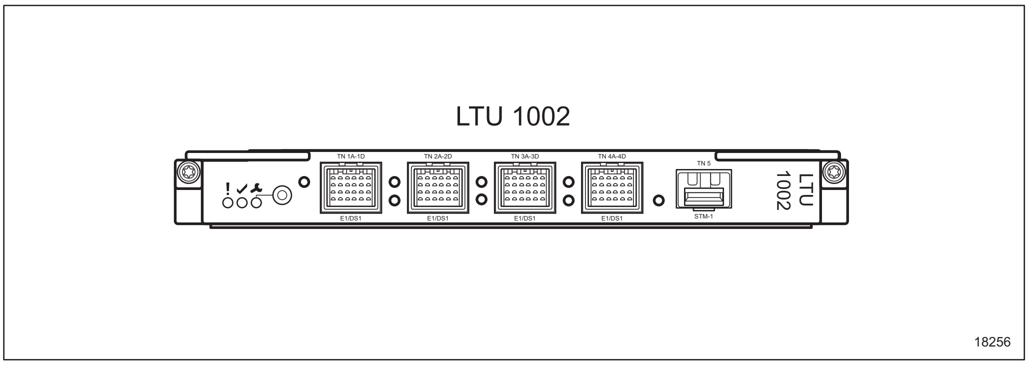


Figure 130 Front Interfaces on the LTU 1002

## 15.16 ETU 1001

ETU 1001 is an Ethernet Termination Unit (ETU) that supports up to four Ethernet ports. The actual number of ports depends upon the NPU type and which APU slot that is used.

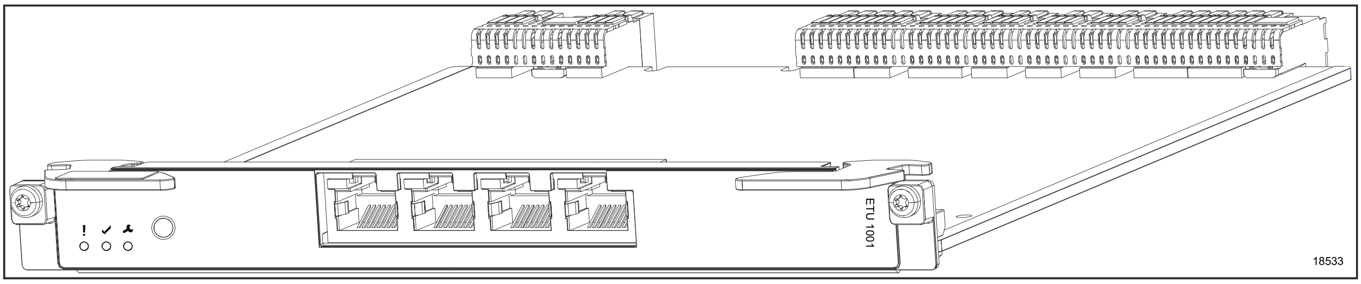


Figure 131 ETU 1001

ETU 1001 can be seen as a port extension to the NPU, where basically the same Ethernet L2 and L3 functionality as on the NPU is supported on the ETU.

ETU 1001 supports SyncE and 1588 Timestamping.

Figure 132 shows the available interfaces of the ETU 1001.

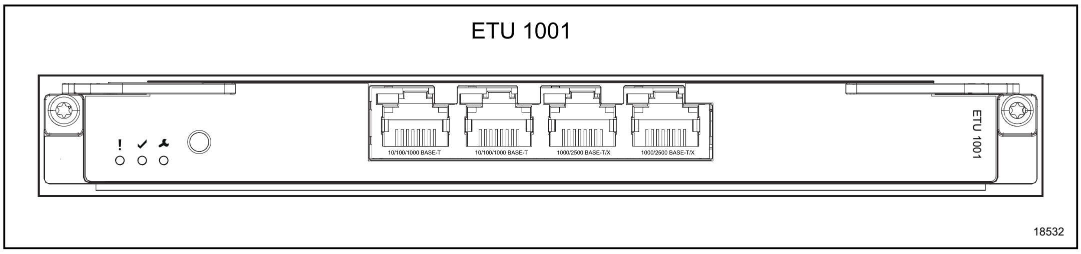


Figure 132 Front interfaces on the ETU 1001

## 15.17 ETU 1002

ETU 1002 is an ETU that supports up to four Ethernet ports. The actual number of supported ports depends upon the NPU type, the selected board profile, and which APU slot is used.

ETU 1002 can be seen as a port extension to the NPU or PNM, where basically the same Ethernet L2 and L3 functionality as on the NPU is supported on the ETU.

ETU 1002 has four SFP cages supporting 4x1G Ethernet, and one SFP+ cage supporting 10G Ethernet, on the front.

1G and 10G ports cannot be used simultaneously.

The following board profiles can be set for ETU 1002:

| | |
|---|---|
| **4X1G** | Provides four 1G front interfaces. |
| **1X10G** | Provides one 10G front interface. |

The 10G port can be used only in MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693, and MINI-LINK 6694.

ETU 1002 supports SyncE and 1588 Timestamping on the 1GE and 10GE interfaces. When using the 10GE interface, ETU 1002 needs to be placed in a 10GE capable slot of the enclosure.

**Note:** SyncE is not supported on the SFPe interface.

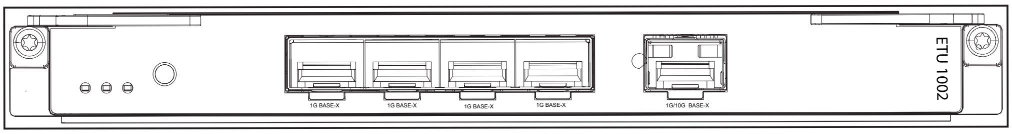


Figure 133 Front Interfaces of ETU 1002

## 15.18 Radio Units

### 15.18.1 Overview

The basic function of the radio is to generate and receive the RF signal and convert it to/from the signal format in the radio cable, connecting the radio and the MMU. It can be combined with a wide range of antennas in integrated or separate installation. The radio connects to the antenna at the waveguide interface. Disconnection and replacement of the radio can be done without affecting the antenna alignment.

There are several types of Radio Units that can be used together with MINI-LINK 6600:

- MINI-LINK 6363 (including support for E-band – 80 GHz), see Figure 134. MINI-LINK 6363 comes in two versions: MINI-LINK 6363, optimized for the highest system gain, and MINI-LINK 6363/2, optimized for the lowest power consumption.

- MINI-LINK 6365, see Figure 134, is optimized for highest system gain and is HW prepared for carrier aggregation 2x28 MHz to 2x112 MHz.

- RAU2 X, see Figure 135.

DC power to the radio is supplied from the MMU through the radio cable.

The radio has a weather proof casing painted white (MINI-LINK 6363 and MINI-LINK 6365) or light gray (RAU2 X), containing for example microwave electronics and a diplexer. It has mechanical features for easy installation on integrated antennas. It also has an optional handle (MINI-LINK 6363 and MINI-LINK 6365) or an integral handle (RAU2 X) for simplified handling during installation.

The radio is independent of traffic capacity. The operating frequency is determined by the radio only and is set in advance at the factory and configured on site using MINI-LINK Node GUI. Frequency channel arrangements are available according to ITU-R and ETSI/FCC recommendations.

**Note:** The coaxial interface on radios and modems is equipped with built in gas discharge tubes, for lightning protection.

Adding components to this interface (for example, extra lightning protection) can impact function and performance and should only be considered after consulting with Ericsson.

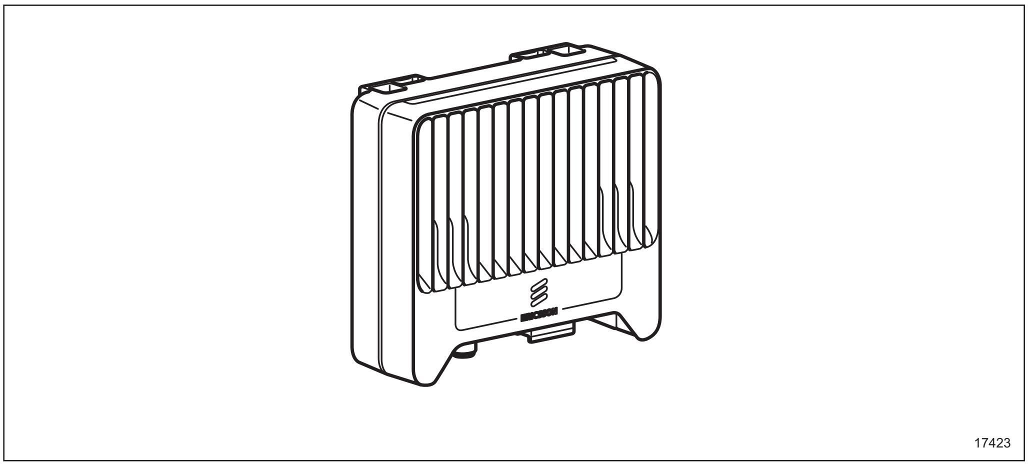


Figure 134 MINI-LINK 6363 or MINI-LINK 6365 Mechanical Design

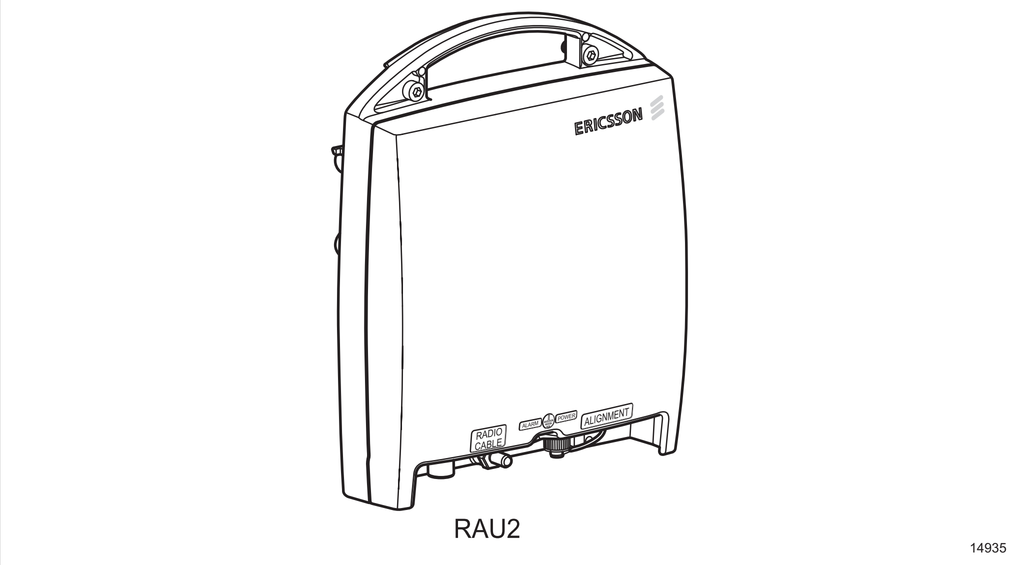


Figure 135 RAU2 X Mechanical Design

## 15.18.2 External Interfaces

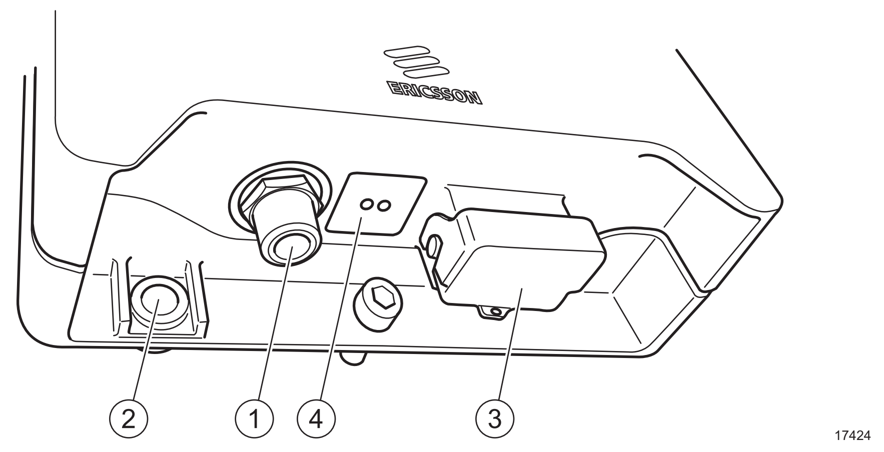


Figure 136 External Interfaces on the MINI-LINK 6363 or MINI-LINK 6365

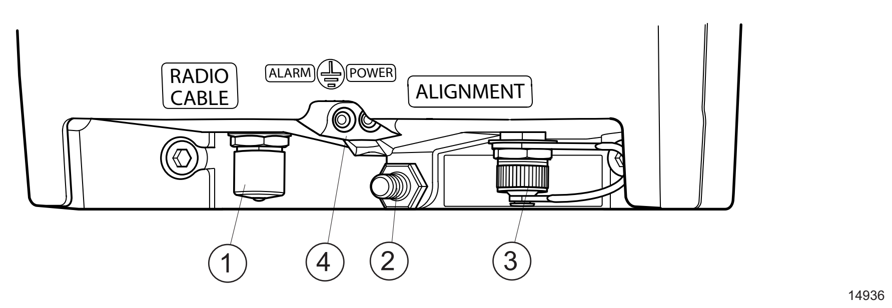


Figure 137 External Interfaces on the RAU2 X

| Item | Description |
|---|---|
| 1 | Radio cable connection to the MMU, 50 Ω N-type connector. The connector is equipped with gas discharge tubes for lightning protection. |
| 2 | Protective ground point for connection to mast ground. |
| 3 | Test port for antenna alignment. |
| 4 | Red LED: Unit alarm. Green LED: Power on. |

## 15.18.3 Radio Modulations

The radio hardware can generate and receive RF signal in single carrier mode.

The tables below show the supported modulations for the radio hardware in single carrier mode and the modulations that also support XPIC and MIMO.

All modulations that support single carrier mode are marked with x. These modulations also support XPIC unless otherwise stated.

### MINI-LINK 6363, MINI-LINK 6363/2, and MINI-LINK 6365 Supported Modulations (ETSI)

Table 50 Supported Modulations for All Frequency Bands (Excluding E-band 80 GHz) with an R-state ≥ R1A

| **Modulation** | **Channel Bandwidth** | | | | | | |
|---|---|---|---|---|---|---|---|
| | 7 MHz | 14/13,75 MHz | 28/27,5 MHz | 40 MHz | 56/55 MHz | 80 MHz | 112/110 MHz |
| 4 QAM | x | x | x(1) | x | x(1) | x | x |
| 8 QAM | x | x | x(1) | x | x(1) | x | x |
| 16 QAM | x | x | x(1) | x | x(1) | x | x |
| 32 QAM | x | x | x(1) | x | x(1) | x | x |
| 64 QAM | x | x | x(1) | x | x(1) | x | x |
| 128 QAM | x | x | x(1) | x | x(1) | x | x |
| 256 QAM | x | x | x(1) | x | x(1) | x | x |
| 512 QAM | x | x | x(1) | x | x(1) | x | x |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1024 QAM | x(2) | x | x | x | x(1) | x | x |
| 2048 QAM | – | x(2) | x | x | x | x | x |
| 4096 QAM | – | – | x | x | x | x(2) | x(2) |

(1) MIMO supported.

(2) XPIC not supported.

Table 51 Supported Modulations for E-band 80 GHz with an R-state ≥ R1A

| | **Channel Bandwidth** | |
|---|---|---|
| **Modulation** | 56/62,5 MHz | 112/125 MHz |
| 4 QAM | x | x |
| 8 QAM | x | x |
| 16 QAM | x | x |
| 32 QAM | x | x |
| 64 QAM | x | x |
| 128 QAM | x | x |
| 256 QAM | x | x |
| 512 QAM | x | x |
| 1024 QAM | x(1) | x(1) |
| 2048 QAM | – | – |
| 4096 QAM | – | – |

(1) XPIC not supported.

### MINI-LINK 6363, MINI-LINK 6363/2 and MINI-LINK 6365 Supported Modulations (ANSI)

Table 52 Supported Modulations for All Frequency Bands (Excluding E-band 80 GHz) with an R-state ≥ R1A

| **Modulation** | **Channel Bandwidth** | | | | | | |
|---|---|---|---|---|---|---|---|
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz | 80 MHz |
| 4 QAM | x | x | x(1) | x(1) | x | x | x |
| 8 QAM | x | x | x(1) | x(1) | x | x | x |
| 16 QAM | x | x | x(1) | x(1) | x | x | x |
| 32 QAM | x | x | x(1) | x(1) | x | x | x |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 64 QAM | x | x | x(1) | x(1) | x | x | x |
| 128 QAM | x | x | x(1) | x(1) | x | x | x |
| 256 QAM | x | x | x(1) | x(1) | x | x | x |
| 512 QAM | x | x | x(1) | x(1) | x | x | x |
| 1024 QAM | x(2) | x | x | x | x | x | x |
| 2048 QAM | – | x(2) | x | x | x | x | x |
| 4096 QAM | – | – | x | x | x | x | x(2) |

(1) MIMO supported.

(2) XPIC not supported.

Table 53 Supported Modulations for E-band 80 GHz with an R-state ≥ R1A

| **Modulation** | **Channel Bandwidth** | |
|---|---|---|
| | 60/62,5 MHz | 80/125 MHz |
| 4 QAM | x | x |
| 8 QAM | x | x |
| 16 QAM | x | x |
| 32 QAM | x | x |
| 64 QAM | x | x |
| 128 QAM | x | x |
| 256 QAM | x | x |
| 512 QAM | x | x |
| 1024 QAM | x(1) | x(1) |
| 2048 QAM | – | – |
| 4096 QAM | – | – |

(1) XPIC not supported.

### RAU2 X Supported Modulations (ETSI)

Table 54 Supported Modulations in Single Carrier Mode for RAU2 X R-state ≥ R6A

| **Modulation** | **Channel Bandwidth** | | | | |
|---|---|---|---|---|---|
| | 7 MHz | 14 MHz | 28 MHz | 40 MHz | 56 MHz |
| 4 QAM | x | x | x | x | x |
| 16 QAM | x | x | x | x | x |
| 32 QAM | x | x | x | x | x |
| 64 QAM | x | x | x | x | x |
| 128 QAM | x | x | x | x | x |
| 256 QAM | x | x | x | x | x |
| 512 QAM | x | x | x | x | x |
| 1024 QAM | x | x | x | x | x |
| 2048 QAM | – | x | x | x | x |
| 4096 QAM | – | – | x | x | x |

### RAU2 X Supported Modulations (ANSI)

Table 55 Supported Modulations in Single Carrier Mode for RAU2 X R-state ≥ R6A

| **Modulation** | **Channel Bandwidth** | | | | | |
|---|---|---|---|---|---|---|
| | 10 MHz | 20 MHz | 30 MHz | 40 MHz | 50 MHz | 60 MHz |
| 4 QAM | x | x | x | x | x | x |
| 16 QAM | x | x | x | x | x | x |
| 32 QAM | x | x | x | x | x | x |
| 64 QAM | x | x | x | x | x | x |
| 128 QAM | x | x | x | x | x | x |
| 256 QAM | x | x | x | x | x | x |
| 512 QAM | x | x | x | x | x | x |
| 1024 QAM | x | x | x | x | x | x |
| 2048 QAM | – | x | x | x | x | x |
| 4096 QAM | – | – | x | x | x | x |

## 15.19 Antennas

All antennas are “compact”, that is the design is compact with a low profile. The antennas are made of aluminum and painted light gray. All antennas have a standardized waveguide interface. The feed can be adjusted for vertical or horizontal polarization.

All antennas are delivered with a mounting kit.

All high performance antennas have an integrated radome.

There are two sorts of antennas available:

- Modular antennas
- Antennas with fixed radio interface

Modular antennas range from 0.3 m – 1.8 m in diameter. The antenna is divided into two modules: the antenna module and the interface module. The interface module is available as Single polarized or as Dual polarized (OMT), and also with interfaces for ANT0 (separate installation), ANT2 (integrated installation for RAU2 X), and ANT3 (integrated installation for MINI-LINK 6363 and MINI-LINK 6365). This makes it possible to upgrade a modular antenna from single to dual polarization and from one radio type to another, for capacity increase when needed and without having to re-align the antenna.

It is not possible to change the frequency band of the antenna by replacing the interface, since also other parts in the antenna are frequency dependent.

The interface module is included when ordering a modular antenna, and is also possible to order as a separate item.

Antennas with fixed radio interfaces range from 0.3 m – 3.7 m in diameter, in single and dual polarized versions, and are available with ANT0 or ANT2 interface.

### 15.19.1 MINI-LINK 6363 and MINI-LINK 6365 Integrated Installation

For a 2+0 configuration, the MINI-LINK 6363 or MINI-LINK 6365 is fitted directly to the rear of the antenna in an integrated installation. Single polarized antennas up to 1.8 m in diameter are normally fitted integrated with the MINI-LINK 6363 or MINI-LINK 6365.

For a 1+1 configuration the MINI-LINK 6363 or MINI-LINK 6365 can be fitted directly to an Integrated Power Splitter (IPS), see Figure 138.

An asymmetrical power splitter is mainly used for 1+1 hardware protection only. The IPS provides one main channel with low attenuation and one standby channel with higher attenuation.

A symmetrical power splitter is mainly used for 1+1 or 2+0 hardware protection and frequency diversity. The IPS provides equal attenuation in both channels.

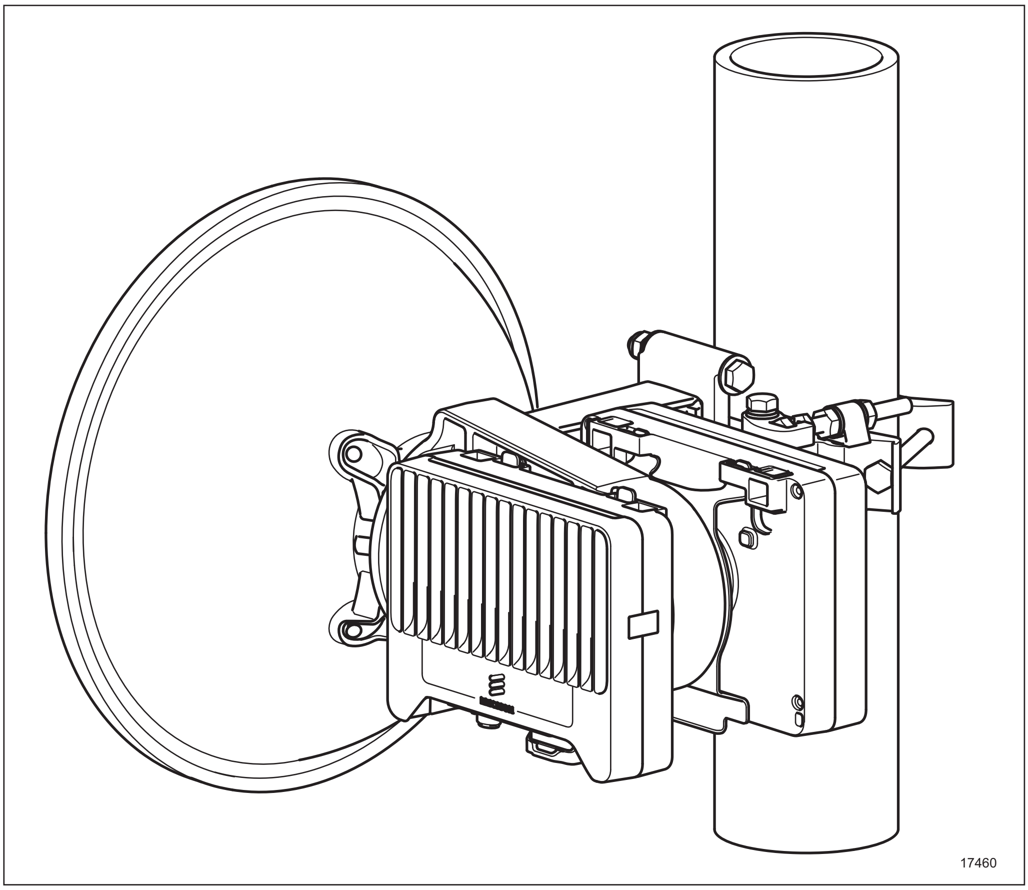


Figure 138 MINI-LINK 6363 or MINI-LINK 6365 Fitted to an Integrated Power Splitter

The 0.3 m and 0.6 m integrated dual polarized antennas are used with two MINI-LINK 6363s or two MINI-LINK 6365s.

In an integrated installation, ANT3 or IPS3 can be used with the MINI-LINK 6363.

Using an antenna adapter plate also enables antennas of type ANT2 or IPS2 to be connected to the MINI-LINK 6363 or MINI-LINK 6365 radio. The antenna adapter plate is illustrated in Figure 139.

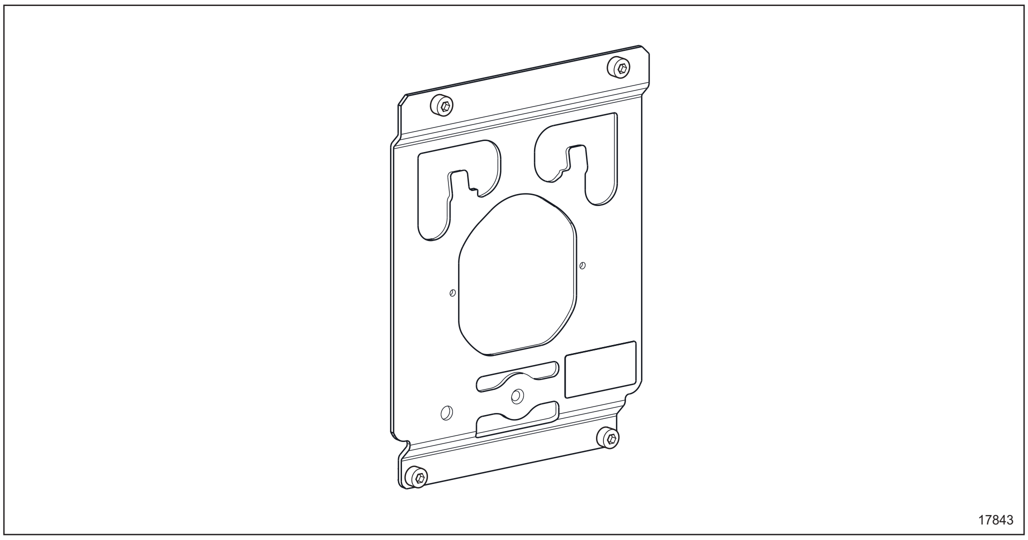


Figure 139 The Antenna Adapter Plate for MINI-LINK 6363 or MINI-LINK 6365

### 15.19.2 RAU2 X Integrated Installation

For a 1+0 configuration, the RAU2 X is fitted directly to the rear of the antenna in integrated installation. Single polarized antennas up to 1.8 m in diameter are normally fitted integrated with the RAU2 X.

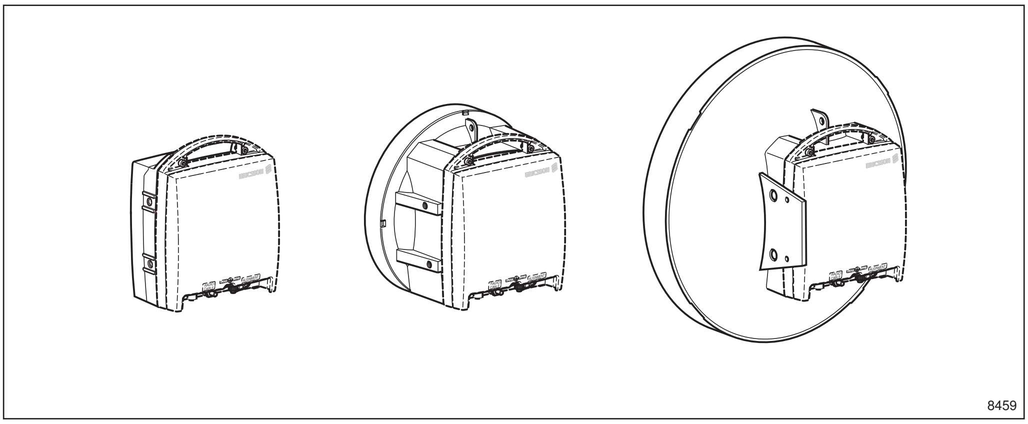


Figure 140 0.2 m, 0.3 m, and 0.6 m Compact Antennas Integrated with RAU2 X

For a 1+1 configuration the RAU2 X can be fitted directly to an Integrated Power Splitter (IPS).

An asymmetrical power splitter is mainly used for 1+1 hot standby configurations, that is, hardware protection only. The IPS provides one main channel with low attenuation and one standby channel with higher attenuation.

A symmetrical power splitter is mainly used for 1+1 working standby or 2+0 configurations, that is, hardware protection and frequency diversity. The IPS provides equal attenuation in both channels.

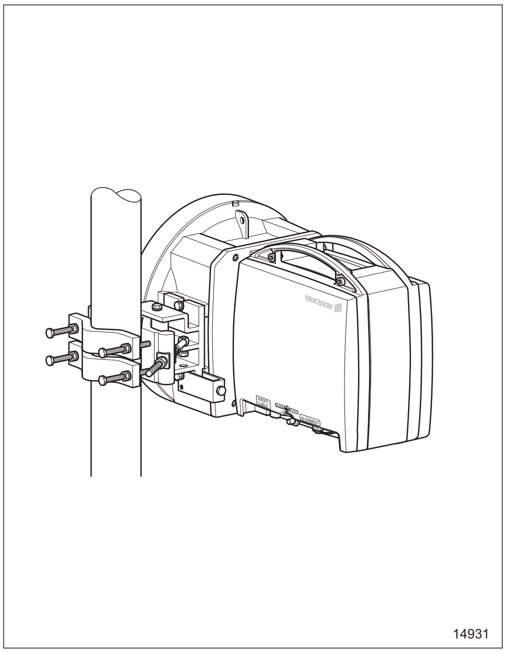


Figure 141 RAU2 X Fitted to an Integrated Power Splitter

The 0.3 m and 0.6 m integrated dual polarized antennas are used with two RAU2s.

In an integrated installation, ANT2 can be used with the RAU2 X, besides the antennas of type ANT2 with fixed radio interface or IPS2.

Using an antenna adapter plate also enables antennas of type ANT1 or IPS1 to be connected to the RAU2 X. The antenna adapter plate is illustrated in Figure 142.

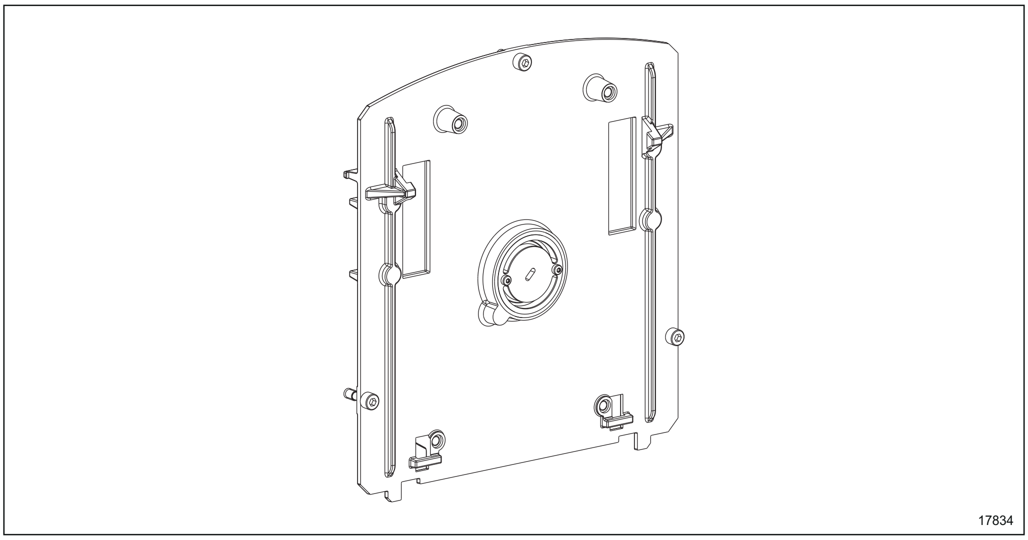


Figure 142 The Antenna Adapter Plate for RAU2 X

### 15.19.3 MINI-LINK 6363, MINI-LINK 6365, and RAU2 X Separate Installation

All antennas have a standardized waveguide interface and can be installed separately, by using a flexible waveguide to connect to the MINI-LINK 6363, MINI-LINK 6365, or RAU2 X. The 2.4–3.7 m dual polarized and single polarized antennas are always installed separately.

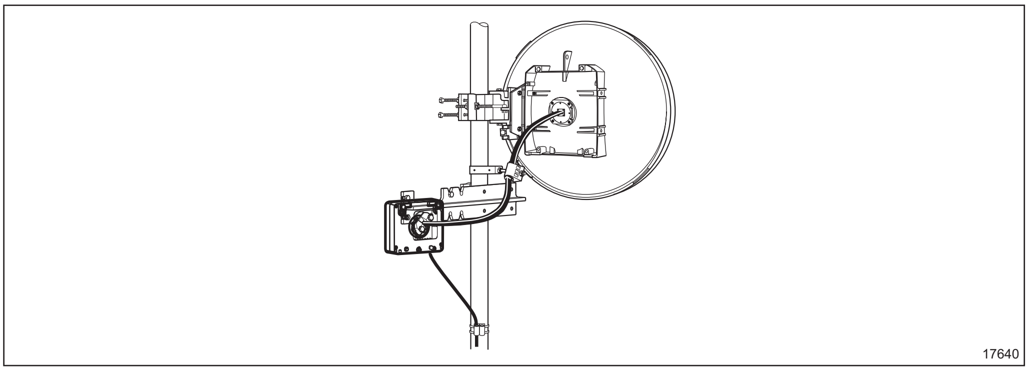


Figure 143 MINI-LINK 6363 or MINI- LINK 6365 Separate Installation in a 1+0 Configuration

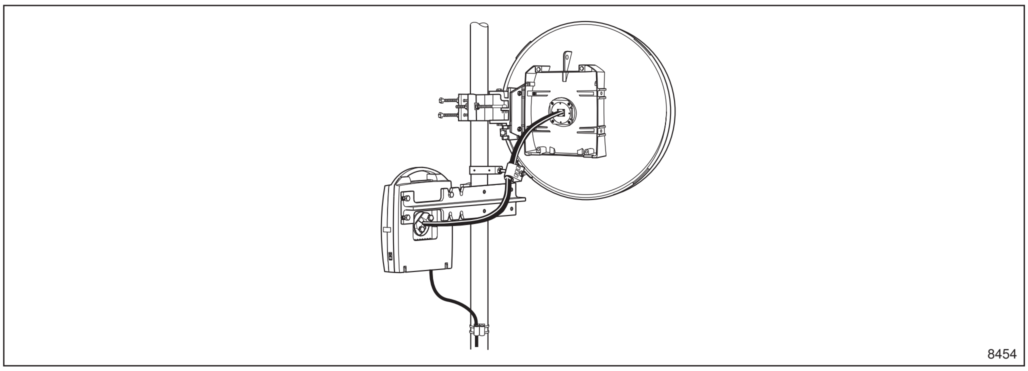


Figure 144 RAU2 X Separate Installation in a 1+0 Configuration

# 16 Management

## 16.1 DCN

This section covers the Data Communication Network (DCN) functions provided by the NE.

Since both IPv4 and IPv6 (only in DCN VLAN mode) are supported, this would imply using two independent DCN networks, one IPv4 and one IPv6, using different addressing and different routing. In one case, though, the two can interfere: when a node via IPv4 asks a DNS server for an IP address, the DNS server might respond with an IPv6 address.

### 16.1.1 IP Services

The following standard external IP network services are supported:

- All clocks, used, for example, for time stamping alarms and events, can be synchronized with a Network Time Protocol (NTP) server. NTP synchronization is supported.
- File Transfer Protocol (FTP) as well as SSH FTP (SFTP) are used as file transfer mechanisms for software upgrade, and for backup and restore of system configuration.
- Domain Name System (DNS) enables the use of host names.
- Dynamic Host Configuration Protocol (DHCP) is used to allocate IP addresses in the DCN. The NE has a DHCP relay agent for serving other equipment on the site LAN.
- Syslog is used to forward log messages in the network and log alarms and events to a central syslog server.

### 16.1.2 DCN Interfaces

MINI-LINK 6600 provides an IP-based DCN for transport of its O&M data. Each NE has an IP router for handling of the DCN traffic. A number of different alternatives to connect and transport DCN traffic are supported. This diversity of DCN interfaces provides the operator with a variety of options when deploying a DCN.

Each physical interface can support two IP hosts, one for IPv4 and one for IPv6.

The following connection options are supported:

- DCN over VLAN

- DCN over VLAN for L1 connections
- Routed DCN in default VRF
- USB
- DCN over PPP
- DCN login to far-end via Radio link

### 16.1.2.1 DCCr/DCCm

**Note:** LTU 1002 is needed to provide STM-1 interfaces for DCCr/DCCm.

The DCCr/DCCm overhead sections in the STM-1 frame can be used to transport DCN traffic. A PPP connection is established over the overhead segments between two end points.

The default bandwidth is automatically established to DCCr=192 kbps and DCCm=192 kbps and DCCm is configurable to 384 kbps and 576 kbps.

For LTU 1002, the bandwidth is fixed to DCCr=192 kbps and DCCm=576 kbps.

The PPP connection in the overhead segments is implemented as PPP over bit synchronous HDLC. Any 3rd party equipment that complies with this and the channel bandwidth segmentation can interoperate with MINI-LINK 6600. DCCm can be used to connect MINI-LINK 6600 to MINI-LINK 6600 over an STM-1 connection. For this connection there can be no multiplexer between the two MINI-LINK 6600 NEs.

**DCN in SDH**

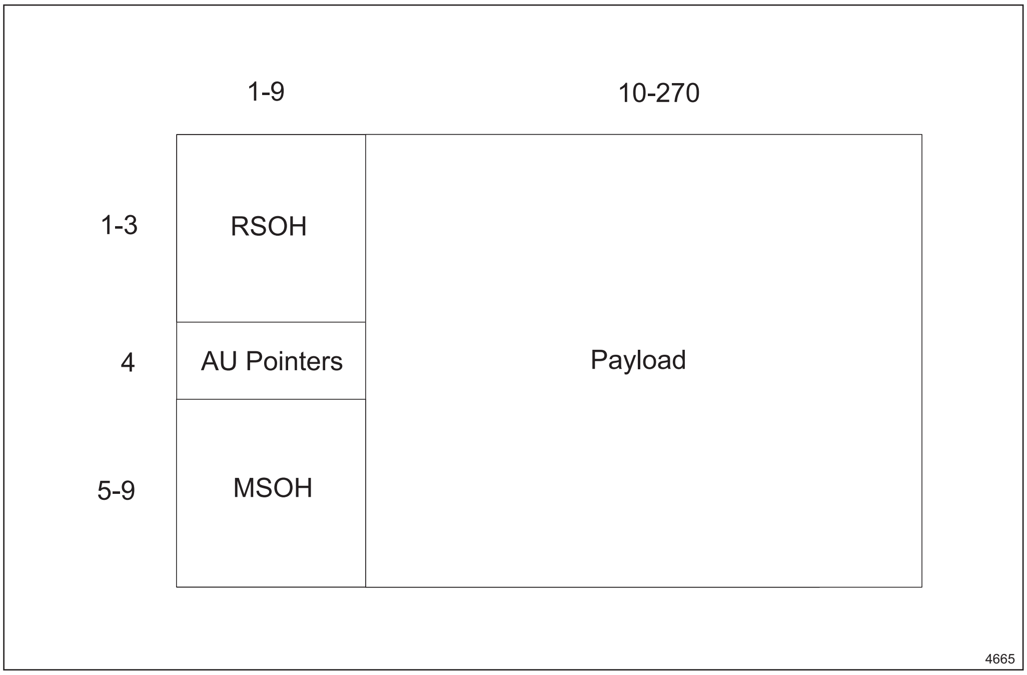


Figure 145 SDH Frame

The following channels can be used for DCN transportation in SDH:

- 128 kbps default proprietary channel available on radio side only.
- 192 kbps channel available on line side and radio side by using EOC or DCC bytes of the Regenerator Section Overhead Frame (RSOH) of the SDH frame.

### 16.1.2.2 10/100BASE-T

Each NE has a 10/100BASE-T Ethernet interface for connection to a site LAN. This interface offers a high speed DCN connection.

### 16.1.2.3 DCN over VLAN

The management traffic can be transported in a logically separated VLAN together with the Ethernet traffic. An internal switch port in MINI-LINK 6600 forwards the management traffic to the IP DCN router.

In Provider Mode, it is possible to separate DCN over VLAN from the rest of the traffic by configuring a default mapping rule into the C-VID registration table of a port.

### 16.1.2.4 DCN over VLAN for L1 Connections

The management traffic can be transported in a VLAN over an L1 connection. In MINI-LINK 6600, ports of L1 connection can be added to one VLAN, thus enabling L2 switching for that VLAN in the L2 connection. By the adding LAN-DCN port to the same VLAN, DCN over VLAN can be used over the L1 connection.

### 16.1.2.5 Routed DCN in Default VRF

High speed routing between multiple DCN VLANs is supported, providing enhanced DCN (compared to DCN over PPP).

The main benefits are:

- Increased bandwidth
- Routing between multiple L3 sub-interfaces
- Better protection of L2 traffic storms.
- Migration can be done remotely without affecting user traffic.

**L3 Interfaces**

The following L3 interfaces are available for Routed DCN:

- L3 VLAN subinterfaces

  L3 VLAN subinterfaces can be defined on Ethernet ports and can use VLAN tagging. L2 switching is not available for L3 VLAN subinterfaces.

- L3 VLAN interfaces - Bridge Virtual Interfaces (BVIs)

  L3 VLAN (BVI) interfaces can be defined on VLANs. L2 switching will operate on the VLAN ports while L3 traffic is handled by the L3 interface. This enables building a L2 DCN with dynamic routing, for example, OSPF.

- PPP interfaces

  PPP interfaces can be used on LTU1002 boards, to create a DCN link over the STM-1 link.

### 16.1.2.6 USB

The USB interface is used for an O&M connection (MINI-LINK Node GUI, CLI session, or CLI Tool) using an IP address, according to the following:

- IPv4

  Local IP address.

- IPv6

Either local (but not link-local) or globally routable IP address.

### 16.1.3 IP Addressing

The DCN of MINI-LINK 6600 supports both IPv4 and IPv6 (in DCN VLAN mode).

#### 16.1.3.1 IPv4

As for generic IP services, DCN for IPv4 supports numbered IP interfaces, used for the Ethernet interface and IP interfaces configured as ABR. All other IP interfaces should be set up with unnumbered IP interfaces.

The use of unnumbered interfaces has several advantages:

- The use of IP addresses is limited. For a large aggregation site, this would imply a lot of addresses.
- The planning of the IP addresses is simplified.
- The amount of configuration is reduced because only one IP address is configured upon installation.

#### 16.1.3.2 IPv6 (in DCN VLAN Mode)

Interfaces support both globally routable IP addresses and link-local addresses on IPv6. With some exceptions, this corresponds to IPv4 according to Table 56.

Table 56 Corresponding IPv4 and IPv6 Addressing

| IPv4 | IPv6 |
|---|---|
| Unnumbered interfaces | Link-local addresses |
| Numbered interfaces | Globally routable addresses |

### 16.1.4 IP Router

The IP router supports the following routing mechanisms:

- Open Short Path First (OSPF), which is normally used for routers within the MINI-LINK domain. OSPFv2 (for IPv4) is supported.
- Static routing

There are two different ways to configure the IP router, Command Line Interface (CLI) (see Section 16.3.3 on page 223) and MINI-LINK Node GUI (see Section 16.3.1 on page 222).

Most configurations are done using CLI, and complex router configuration and troubleshooting can only be performed with CLI.

### 16.1.4.1 OSPF Features

The following summarizes the OSPF features:

- An NE can be a part of a non-stub area, stub area or totally stub area.
- An NE can act as an Internal Router (IR) or an Area Border Router (ABR).
- Virtual links are supported, which is useful when an area needs to be split in two parts.
- Link summarization is supported, which is used in the ABR to minimize the routing information distributed to the backbone and/or other areas.

## 16.2 Link Layer Discovery Protocol (LLDP)

This section gives a brief overview of the LLDP that is used by network elements (NE) for advertising their identity, capabilities, and neighbors.

LLDP is a simplex protocol where each node periodically transmits information about itself. The protocol is stateless, with no confirmation mechanism. LLDP is specified in IEEE 802.1 AB.

Supported TLVs are as follows:

- ChassisID
- PortID
- Time To Live
- System Name
- Management Address

## 16.3 Management Tools and Interfaces

This section gives a brief overview of the management tools and interfaces used for MINI-LINK 6600.

### 16.3.1 MINI-LINK Node GUI

MINI-LINK Node GUI provides tools for on-site installation, configuration management, fault management, performance management and software upgrade. It is also used to configure the traffic routing function, protection and DCN.

MINI-LINK Node GUI is used for local management, that is the NE is accessed locally by connecting a PC to the node with a USB cable.

The NE can also be accessed over the site LAN or remotely over the DCN.

To access an NE remotely through MINI-LINK Node GUI, a MINI-LINK Node GUI license is required on that specific NE to ensure full functionality in MINI-LINK Node GUI.

### 16.3.2 SNMP

Each NE provides an SNMP agent enabling easy integration with any SNMP-based management system. The SNMP agent can be configured to support SNMPv1/v2c/v3 for get and set operations. SNMPv3 is default. The SNMP agent sends SNMPv1, SNMPv2c and SNMPv3 traps.

The system is built on standard MIBs as well as some private MIBs.

### 16.3.3 Command Line Interfaces

A CLI is provided for advanced IP router configuration and troubleshooting. This interface is similar to Cisco's industry standard router configuration and is accessed from a Command Prompt window using Telnet or SSH.

### 16.3.4 Syslog

Logging of alarms and events to syslog servers can be managed through MINI-LINK Node GUI, and CLI.

### 16.3.5 NETCONF/YANG North Bound Interface (NBI)

Read-only access to selected attributes is included in the IETF YANG Data Model for Microwave Radio Link using NETCONF as the NBI.

For details on the IETF-model, refer to https://datatracker.ietf.org/doc/draft-ietf-ccamp-mw-yang/.

## 16.4 Configuration Handling

The configuration can be managed locally and from the O&M center provided that the DCN is set up. The following list gives examples of configuration areas:

- Transmission interface parameters
- Traffic routing
- Radio Link Bonding (RLB)
- DCN parameters, such as host name, IP address

- Security parameters, such as enabling Telnet and SSH, enabling SNMPv3 with encryption, and using RADIUS and TACACS+ for AAA
- Radio Terminal parameters, such as frequency, output power, ATPC, and protection

### 16.4.1 Configuration File

The configuration file is stored non-volatile both on the RMM and in a flash memory on the NPU.

If an NPU needs to be replaced, the RMM from the faulty NPU can be inserted in the new NPU. In this scenario the user copies the configuration file from the RMM to the flash memory of the new NPU.

If an RMM is replaced, for example due to a license upgrade or downgrade, the user copies the configuration file from the flash memory to the new RMM.

### 16.4.2 Aligning the Node with the Network Management System

When the configuration of a node is changed, either through MINI-LINK Node GUI, or CLI, the node sends an event to the Network Management System (NMS).

It is possible to set a timer to decide how long after the configuration change that the event is sent to the NMS. If another configuration change is made before the event has been sent, the timer starts counting from zero again.

If the name of a node is changed, the node immediately sends a separate event to the NMS. Since a name change is also a configuration change, this triggers a configuration change event to be sent as well, but only after the timer value has been reached.

## 16.5 Software Management

The NE system software consists of different software modules for different applications. Software can be upgraded both locally and remotely. Software upgrade uses a local or remote FTP or SFTP server, to distribute the software to the NE. Using SFTP instead of FTP ensures that the entire session, including passwords, is encrypted.

All traffic continues while the software is being loaded. During the execution of the software download a progress indication is provided in the user interface. When the download is completed, the new software and the previous software versions are stored on the unit.

The downloaded software file is automatically checked for corruption with keyed-Hash Message Authentication Code (HMAC) and the Secure Hash Algorithm 1 (SHA-1), both to avoid erroneous transfer and to mitigate malware attacks.

The file integrity check monitors changes to the configuration file, password file, audit log, and Operating System (OS) files. Alarm notifications are generated and information about the captured changes is logged in a report. The operator can then investigate the report and take proper actions. The operator can view the report on the node or upload the report to an external secure server through SFTP.

Performing a restart of the NE activates the new software version. A warm restart only affects the control system. This restart can be performed immediately or scheduled at a later time. The restart, depending on the new functionality, may influence the traffic. When the restart with the new software is completed, the NE will wait for a ‘‘Commit’’ command from the management system. When the ‘‘Commit’’ command is received, the software upgrade process is completed.

The previous software revision remains stored on the unit in case a rollback is required. This may be the case if something goes wrong during the software upgrade or if no ‘‘Commit’’ command is received within 15 minutes after the restart.

If plug-in units with old software versions are inserted into the NE, they can be automatically upgraded.

### 16.5.1 Uploading Local Logs to a Remote FTP Server

The Local Log Upload feature secures the local log files generated on the node by persistently uploading them to a central FTP or SFTP server and making them available for debugging even if the logs on the node are lost due to overwrite, restart, power loss, or any other reasons.

If the feature is enabled, the local log files are automatically uploaded to the server when they are rotated and compressed.

In addition, forced upload can also be initiated manually, where all pending log files are uploaded to the FTP or SFTP server without a delay.

## 16.6 License Handling

The MINI-LINK 6600 features are divided into three types:

- Base Package
- Value Packages
- Capacity Licenses

The Base Package provides a fully functional Network Element (NE) and is a part of the standard product offering. Value Packages and Capacity Licenses, when enabled, enhance the functionality and the capacity of the NE.

The basic features are licensed through the Base Package. The Base Package is mandatory and is valid for the full MINI-LINK 6600 release.

License-controlled features have two licensing modes:

- Locked Mode
- Unlocked Mode

Under certain circumstances, the system or the user is entitled to an unlock period, during which license controlled features can be used without sufficient license.

Alarms are raised if a license-controlled feature is used without sufficient license on the NE.

License handling allows the user to track the license usage on slot/port level, getting detailed information on the state of license controlled features. The user can:

- Identify which port(s)/slot(s) has a missing license when the node license status is degraded.
- Get detailed information about license allocation on slot/port level.

## 16.7 Fault Management

All software and hardware in operation is monitored by the control system. The control system locates and maps faults down to the correct replaceable hardware unit. Faults that cannot be mapped to one replaceable unit result in a fault indication of all suspect units (this may be the whole NE).

Hardware errors are indicated with a red LED found on each plug-in unit and radio.

The control system will generally try to repair software faults by performing warm restarts on a given plug-in unit or on the whole NE.

### 16.7.1 Alarm Handling

The NE uses SNMP traps to report alarms to SNMP-based management system. Alarms can also be sent to a syslog server. To enable a management system to synchronize alarm status, there is a notification log (alarm history log) where all traps are recorded. There is also a list of current active alarms. Both these can be accessed by the management system using SNMP, or MINI-LINK Node GUI. The alarm status of specific managed objects can also be read.

In general, alarms are correlated to prevent alarm flooding. This is especially important for high capacity links, where a defect on the physical layer can result in many alarms at higher layer interface, like E1. Correlation will cause physical defects to suppress alarms, like AIS, at these higher layers.

Alarm notifications can be enabled/disabled for an entire NE, for an individual plug-in unit, and for individual interfaces. Disabling alarm notification means that no new alarms or event notifications are sent to the management systems.

Alarm and event notifications are sent as SNMPv2c/v3 traps with a format according to Ericsson's Alarm IRP SNMP solution set version 1.2. The following fields are included in such a notification:

- Notification identifier: uniquely identifies each notification.
- Alarm identifier: only applicable for alarms, identifies all alarm notifications that relate to the same alarm.
- Managed object class: identifies the type of the source, for example, E1, DS1, and so on.
- Managed object instance: identifies the instance of the source, for example 1/4/6A for an E1 on the NPU.
- Event time: time when alarm/event was generated.
- Event type: X.73x compliant alarm/event type like communications alarm and equipment alarm.
- Probable cause: M.3100 and X.733 compliant probable cause, for example, Loss Of Signal (LOS).
- Perceived severity: X.733 compliant severity, for example, critical or warning.
- Specific problem: free text string detailing the probable cause.

The system can also be configured to send SNMPv1 traps. These traps are translated from the IRP format using co-existence rules for v1 and v2/v3 traps (RFC 2576).

Alarm and event notifications can also be sent to (up to 3) syslog servers in the network. The information content is the same as for the SNMP traps. The messages use a fixed syslog facility of LOG_LOCAL6 and severity mapping and message text is based on RFC 5674 – Alarms in syslog.

### 16.7.2 Ethernet Link OAM

Ethernet Link OAM supports fault management on Ethernet links according to IEEE 802.3ah and provides link monitoring, fault notification, and loopback test.

### 16.7.3 Ethernet Service OAM

Ethernet Service OAM supports fault management on Ethernet links according to IEEE 802.1ag and is used to manage networks comprising of multiple LANs.

### 16.7.4 Loops

Loops can be used to verify that the transmission system is working properly or they can be used to locate a faulty unit or interface.

**Note:** On MINI-LINK 6651/1 and on MINI-LINK 6651/3, only IF and RF loops on the radio is supported.

### 16.7.4.1 Loops for Circuit Switched Traffic

The following loops are available on units with an E1/DS1 line interface.

| | |
|---|---|
| **Connection Loop** | This loop can be initiated for an E1/DS1. The traffic connection is looped in the TDM bus back to its origin, see Figure 146. If an E1/DS1 interface is traffic routed an AIS is sent to the other interface in the traffic routing.<br>A Connection Loop can be used in combination with a BERT in another NE to test a network connection including the termination plug-in unit, in case a Local Loop cannot be used due to the lack of a traffic routing. |
| **Line Loop** | Loops an incoming line signal back to its origin. The loop is done in the plug-in unit, close to the line interface, see Figure 146. An AIS is sent to the TDM bus.<br>A Line Loop in combination with a BERT in an adjacent NE is used to test the transmission link between the two NEs. |
| **Local Loop** | Loops a line signal received from the TDM bus back to its origin, see Figure 146. An AIS is sent to the line interface.<br>A Local Loop in combination with a BERT in another NE can be used to test a connection as far as possible in the looped NE. |

The following loop is only supported on the modem/MMU.

| | |
|---|---|
| **Rx Loop** | This loop is similar to the Connection Loop but the loop is done in the plug-in unit close to the TDM bus, where a group of E1s in the traffic connection is looped back to its origin, Figure 146. Traffic on high-speed bus is not affected.<br>An Rx Loop can be used on the far-end modem/MMU to verify the communication over the radio path, see Figure 147. |

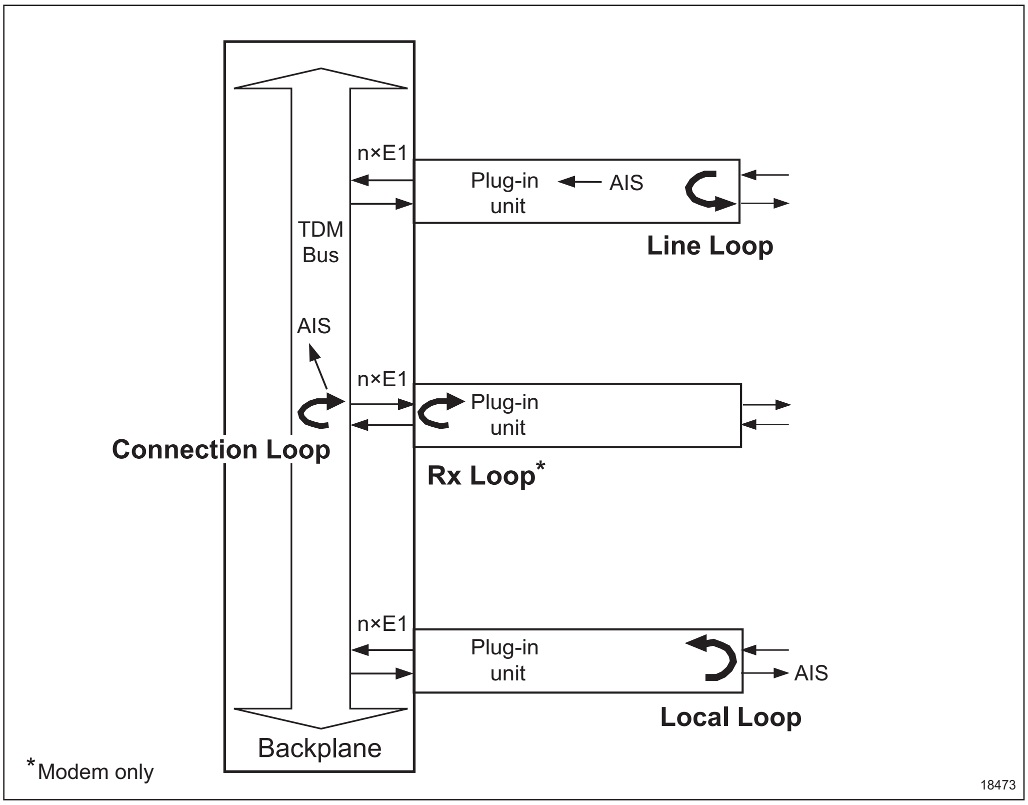


Figure 146 Loops

The following loops on the near-end Radio Terminal are supported in order to find out if the modem/MMU or radio is faulty.

| | |
|---|---|
| **IF Loop** | In the modem/MMU the traffic signal to be transmitted is, after being modulated, mixed with the frequency of a local oscillator and looped back for demodulation (on the receiving side). See Figure 147. |
| **RF Loop** | In the radio, a fraction of the RF signal transmitted is shifted in frequency and looped back to the receiving side. See Figure 147. |

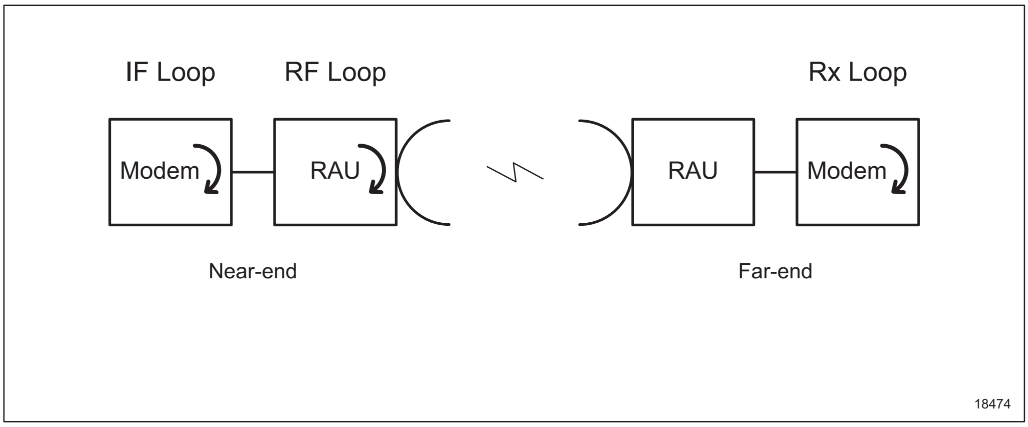


Figure 147 Radio Link Loops

### 16.7.4.2 Loops Impact for Packet Switched Traffic

**Note:** The Ethernet protocol does not have a mechanism that automatically discards frames when a loop occurs. Without a loop prevention mechanism, all traffic is returned back to the port causing problems with MAC address switching tables and possibly affecting the traffic in the entire network.

Loops for Ethernet traffic are considered to be very harmful and should be avoided.

For IF and RF loops, the looped traffic is discarded to prevent Ethernet loops. Thus, IF and RF loops can be set with Ethernet traffic running.

Loops on physical layers are only employed after disconnecting Ethernet services in order to avoid Ethernet loops. During installation and validation of a hop on radio level, it is recommended to perform measurements by installing loops on (temporary) PDH connection and test the point-to-point connection by configuring an Rx loop. After the hop has been installed and validated the (temporary) PDH connection is removed and the Ethernet services reconnected.

Spanning Tree Protocol (STP) or Rapid STP (RSTP) is not able to prevent looped Ethernet traffic flooding into the network for physical loops on the LAN ports or the WAN ports since own BPDU packets are discarded and therefore the looped traffic is passed through.

Test loops installed on physical and logical interfaces could influence Ethernet traffic as follows:

| | |
|---|---|
| **Physical loop** | Traffic can be looped with an external physical Tx-Rx loop. MINI-LINK 6600 does not have any built-in mechanism to prevent loops on LAN ports. All traffic will be returned back to the network. |

The following loop is part of the Ethernet Link OAM functionality:

| | |
|---|---|
| **Remote Loopback** | Loops Ethernet traffic between two adjacent NEs, connected through a LAN interface, and is used for fault localization and link performance testing of Ethernet links. It is available on Ethernet traffic units with support for Ethernet Link OAM.<br>Remote loopback can only be performed on LAN interfaces. |

### 16.7.4.3 MAC Swap Loopback

The source and destination MAC addresses in frames with a specified VLAN ID are swapped at ingress and the frame is looped back. MAC swap loopback can be used for troubleshooting and performance measurement.

The node can be configured to loopback specified L2 frames based on the following configurable parameters:

- Ingress port (LAN/WAN)
- Egress port (LAN/WAN)
- VLAN
- Src MAC address
- Dst MAC address

The src and dst MAC addresses of the specified frames are swapped in linerate (GE/10G).

When Destination MAC address filtering is disabled, the frames with any destination MAC address are looped back and their source MAC address is set to the own MAC address of the local switch.

In case of egress-lookup configuration, the traffic on the ingress port is checked for frames to be egressed on the egress port configured with MAC Swap Loopback. The frames to be egressed are looped back on the ingress port.

Because the loopback always takes place on the ingress port, latency time measurements are the same regradless of whether the latency time is measured for the egress or ingress port.

The following prerequisites must be fulfilled to be able to use the egress-lookup configuration:

- The dst MAC address must already be learnt by the switch to be able to identify the egress port
- The configured egress port **Oper Status** must be **Up**
- The configured egress port must be a member of the configured VLAN

Only one MAC swap loopback session is supported for the node.

Loop is automatically deactivated after the configurable timeout. The default timeout value is `300` seconds.

## 16.8 Spectrum Diagnostics Scan for Potential Interferer

The Spectrum Diagnostics scan used when verifying an installation and can then be activated by a user to automatically scan the frequency range of the configured radio channel or the complete radio sub-band. The test results in Received Signal Strength Indicator (RSSI) values, which are used to verify that there are no interfering signals. If the result indicates the presence of an interferer, further investigation is needed to conclude if this has impact on the radio-link performance or not.

The Spectrum Diagnostics scan can be performed using either CLI commands or MINI-LINK Node GUI.

**Note:** Running a spectrum diagnostics scan on a hop that is already taken into service impacts the traffic and can also lead to lost connection with the node as the transmitters are turned off during the scan.

## 16.9 Performance Measurements

Performance counters are available for 15 minutes and 24 hours intervals. The start time of a 24 hours interval is configurable.

The following counters are stored in the NE:

- Current 15 minutes and the previous 96×15 minutes
- Current 24 hours and the previous 24 hours

Performance data is stored in a volatile memory. Therefore, all gathered data is lost at a restart.

Performance data is available for the following major features:

- Radio link (see Section 16.9.1 on page 232)
- Ethernet traffic (see Section 16.9.2 on page 233)
- PDH (see Section 16.9.3 on page 234)
- Bit Error Testing (see Section 16.9.4 on page 235)
- Ethernet Service OAM (see Section 16.9.5 on page 235)

### 16.9.1 Radio Link Performance Measurements

Radio Link PM makes it possible to compare actual performance with planned performance. The configuration of each microwave link is normally based on radio link planning criteria and RAN requirements (quality, delay, and availability) with the help of planning tools.

**RF Input and Output Power**

RF Input power can be used to identify underperforming radio links in terms of received signal levels, which could indicate a problem caused by, for example, bad RF planning, interference, incorrect configuration, or hardware faults.

RF Output power can be monitored when Automatic Transmit Power Control (ATPC) is activated.

Threshold alarms can be defined for Input and Output Power.

**Radio Link Quality**

G.826 is originally a standard for measurement of the quality of PDH links. In MINI-LINK nodes this measurement is also available on the continuously running serial data stream below any link layer such as Ethernet.

The G.826 PM, such as ES, SES and BBE, give an indication of the quality of the radio link.

The channel conditions are continuously monitored on the Rx side by measurement of Signal to Noise and Interference Ratio (SNIR).

**Adaptive Coding and Modulation**

When Adaptive Coding and Modulation (ACM) is configured counters are available that measure how much time that is spent in each modulation.

See also Section 3.2 on page 13.

#### 16.9.1.1 Radio Cable Monitoring

If the communication between the modem and the radio is disturbed, it can cause intermittent traffic loss and result in the transmitter on the radio getting switched off.

By checking for any alarms on the RAU-MMU communication channel, the connection between the modem and the radio can be monitored and problems with cables between the modem and the radio can be detected.

### 16.9.2 Ethernet PM Counters

The Performance Monitoring function is used by the network operator to analyze the performance and usage of the Ethernet traffic to find unused capacity, congestion points and traffic lost due to congestion or faults. The analysis result is used to re-plan the network for better usage. The Performance Monitoring is also used when troubleshooting and performing functional tests of the equipment.

### Bandwidth Counters

Bandwidth measurements are done on LAN and WAN interfaces in Tx and Rx direction.

WAN interfaces support the measurement on separate TC queues in Tx direction.

Bandwidth measurements (except for TC queue measurements) are also available on a per interface per VLAN basis. Bandwidth measurements for VLANs are disabled by default. For how to enable them, see Configuring an Ethernet Layer 2 Connection.

Average, maximum, and minimum bandwidth, as well as bandwidth histograms are available.

### Traffic Performance Counters

Traffic performance measurements are done on LAN and WAN interfaces in Tx and Rx direction.

Some of the traffic performance counters in Tx direction are also available for separate Traffic Class queues on WAN interfaces.

### Threshold Crossing Alarms for Ethernet PM Counters

It is possible to configure threshold crossing alarms for Ethernet PM counters on used interfaces. The thresholds are configured per interface, where ordinary LAN interfaces have a subset of the thresholds available for a buffered LAN or a WAN interface. The availability of thresholds are based on which counters are provided by the different interfaces.

### XML File

The Ethernet performance data can be transferred to MINI-LINK Node GUI, or an external system, such as ServiceOn or other NMS, in XML files. Upon a file transfer request the NE creates an XML file with the requested data, compresses the file and sends it to the selected FTP or SFTP Server.

The content of the file is based on data available in the NE at the time of the request.

In MINI-LINK Node GUI, it is possible to display historical Ethernet performance data without having an FTP Server installed on the host where MINI-LINK Node GUI is running.

### 16.9.3 PDH

The following performance counters are used for the E1/DS1 line interfaces:

- Errored Seconds (ES)
- Severely Errored Seconds (SES)
- Background Block Error (BBE) (only structured interfaces)
- Unavailable Seconds (UAS)

### 16.9.4 Bit Error Testing

Each NE has a built-in Bit Error Ratio Tester (BERT) in all plug-in units carrying traffic. The BERT is used for measuring performance on E1/DS1 interfaces according to ITU standard O.151. A Pseudo Random Bit Sequence (PRBS) with a test pattern $2^{15}–1$ is sent through the selected interface.

As with loop tests, bit error testing may be used for system verification or for fault location.

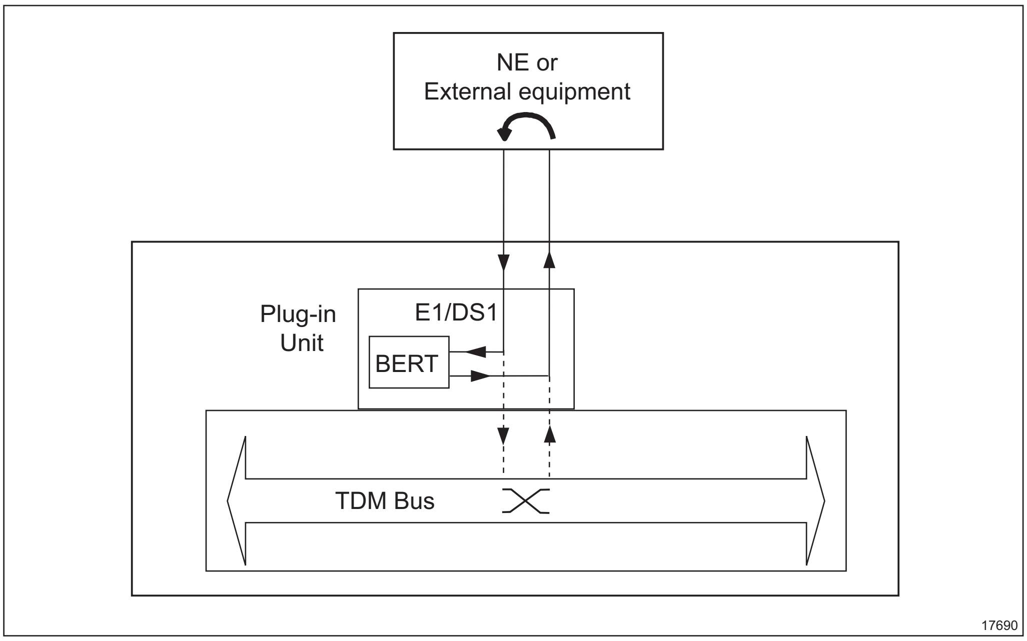


Figure 148 BERT in Combination with an External Loop

The BERT is started and stopped by the operator and the bit error rate as a function of the elapsed time is the test result. The test can be started and stopped locally or remotely using the management system.

Several BERTs can be executed concurrently, but only one BERT per plug-in unit.

### 16.9.5 Ethernet Service OAM

Ethernet Service OAM provides performance monitoring between MEPs, according to ITU-T Y.1731 and Y.1730. Ethernet Service OAM provides delay and delay variation information to the service provider, and ensures that the provided service is in accordance to the SLA.

Ethernet Service OAM supports the following PM functions:

- Frame Delay
- Frame Delay Variation Measurement
- Frame Loss Measurement
- XML File transfer
- Ethernet Bandwidth Notification

### 16.9.6 IP Performance Monitoring with TWAMP Reflector Light

Two-Way Active Measurement Protocol (TWAMP) is a Layer 3 protocol. It provides a flexible method for measuring two-way or round-trip IP performance between two nodes (sender and reflector) in an IP network.

TWAMP is specified in RFC 5357.

TWAMP can be used to measure two-way metrics like inter-packet delay (latency) and delay variation (jitter) between two endpoints, packet loss, far-end delay, far-end jitter, near-end delay, near-end jitter, duplicate packets, and so on, using UDP packets. The supported UDP port range is 863-65535 and the default UDP port number is 862.

TWAMP consists of two major parts; a control plane part and a data plane part. The control part sets up the TWAMP session by using TCP.

The test part is the an UDP based measurement. The sender transmits a test message and that is reflected from the reflector. Both endpoints timestamp the message.

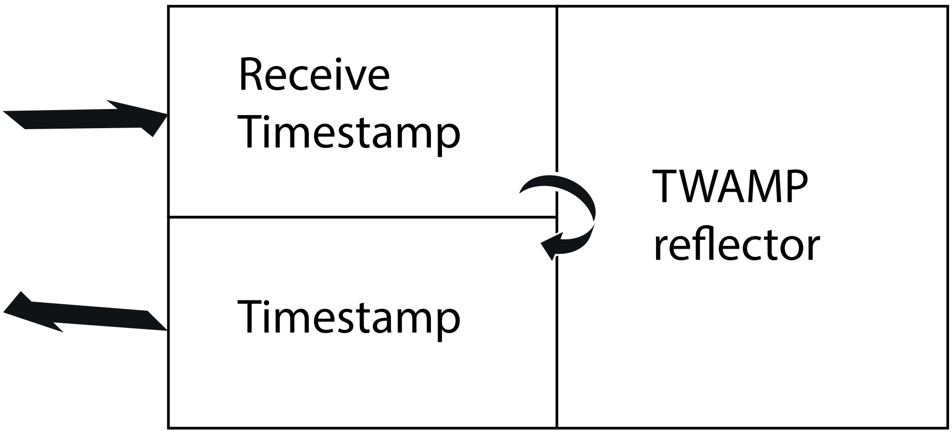


Figure 149 Reflector

The reflector never generates packets by itself, it only sends answers to packets. The reflector has a separate, configurable IP address. There is a special type of implementation for TWAMP with lower complexity that is called TWAMP Light where the control plane is removed and only the test messages are exchanged.

## 16.10 Node Security

All management access to the NE is protected by a user name and a password.

The following user types are defined:

- view_user with read-only access
- oper_user with read and write access
- control_user with read and write access
- admin_user with read and write access

**Note:** Only the admin_user has full read and write access, the oper_user and control_user have full read access, but limited write access.

Only the admin_user can change the system time.

All user types have an associated password. Only the admin_user can change passwords using MINI-LINK Node GUI, CLI, or the SNMPv3 interface.

**Note:** Strong password feature is available and is enabled by default on the MINI-LINK Node GUI and CLI interfaces. Strong passwords require minimum 12 characters in length, and at least three of the following character types: lowercase, uppercase, numeral, non-alphanumeric characters.

The following security mechanisms are used on the various O&M interfaces:

- MINI-LINK Node GUI

Local and remote MINI-LINK Node GUI access requires a user name and password. Default password is not accepted for local USB connection.

It is possible to add a legal notice shown before logging on, to highlight the legal consequences of unauthorized access.

- SNMP

  For SNMPv3 access, the regular user name and password protection is used. In addition to this the User-based Security Model (USM) and View-based Access Model (VACM) are supported. This means that additional users and passwords might be defined by external SNMPv3 managers. The default security level is authentication/no privacy where Message Digest 5 (MD5) is used for authentication. SHA-1 or SHA-2 can also be used for authentication.

  SNMPv3 can be configured to authentication with privacy, using Data Encryption Standard (DES) or Advanced Encryption Standard (AES). This means that the management traffic is secure.

  For SNMPv1/v2c access, the regular user name and password protection does not apply. Instead a community-based access protection is used. As default, a public and a private community are configured. The public community enables default read-access and the private community provides read and write access to MIB-II system information. These privileges can be extended through either MINI-LINK Node GUI, or SNMPv3 interface. The SNMPv1/v2c interface may be disabled.

- CLI

  Access to the Telnet port using CLI commands is protected by the regular user name and password protection. The Telnet port can be disabled from MINI-LINK Node GUI.

  Secure Shell (SSH) protocol can be used for more secure remote access and use of CLI commands. The SSH protocol is enabled as an alternative to the Telnet protocol, using MINI-LINK Node GUI or. When SSH is enabled telnet is automatically disabled and for security reasons can only be re-enabled if SSH is disabled.

  It is possible to regenerate the automatically generated public-private key pairs in case the SSH keys have been compromised.

### 16.10.1 Authentication, Authorization, and Accounting

Authentication, Authorization, and Accounting (AAA) is a security architecture for distributed systems. The Authentication process makes sure that only accepted users can log on to the system, for example, using user names and passwords. The Authorization process gives authenticated users certain permissions, for example, based user roles. The Accounting process records information about access and use of the system.

There are three AAA policies in MINI-LINK: local, RADIUS, and TACACS+. RADIUS and TACACS+ are two types of centralized authentication.

**Note:** If the connection to the remote AAA server is interrupted, the NE falls back to local authentication. When the communication to the AAA server is working again, the centralized authentication (RADIUS or TACACS+) is automatically restored.

MINI-LINK 6600 devices support RADIUS or TACACS+ session accounting for all central and local users. RADIUS or TACACS+ servers for accounting are handled together with the authentication servers. The management sessions are logged by enabling the session accounting feature. When the management session is started, that is, the management user has logged on, the NE sends a RADIUS or TACACS+ accounting start message to the server. When the session is ended, that is, the management user has logged off, the NE sends a RADIUS or TACACS+ accounting stop message to the server. Both the beginning and the end of a session can be recorded. Accounting messages contain the IP address of the client from which the NE is accessed by the user.

### 16.10.1.1 Local Authentication

The local policy supports the following features:

- Authentication

  For local user authentication, it is necessary to supply authentication information in the form of a user name and password. During the authentication process, the NE searches its locally stored configuration for a user with a matching user name. If a matching user name cannot be found, the request is refused. The maximum number of local users supported is four.

- Authorization

  The NE uses local authorization information to distinguish which privileges belong to a role.

  The authorization process is based on the user role (system admin, network admin, operator, or guest).

### 16.10.1.2 Centralized Authentication

The two types of centralized authentication are RADIUS and TACACS+.

The system has two external interfaces, CLI and SNMPv3. Centralized users and authentication are supported for both CLI and SNMPv3. The local admin_user needs to set the AAA policy and configure the TACACS+ or RADIUS servers before attempting a centralized authentication.

SNMPv3 security protocols (authentication and privacy) are configurable by RADIUS/TACACS+ authorization parameters.

If centralized authentication is used, all local users (admin_user, view_user, control_user, and oper_user) are enabled. Passwords for centrally-authenticated user accounts cannot be changed using CLI,MINI-LINK Node GUI.

It is possible to disable local users (admin_user, view_user, control_user, and oper_user) when TACACS+ is configured.

**Note:** Only admin_user can disable local users when centralized authentication is configured.

It is recommended to set SSH as a secure CLI connection, to allow a fully-secure centralized authentication and authorization process.

A session timeout and a user message display, for example, welcome messages, legal banners, and so on, are supported. The timer value and the user messages must be properly configured in the external TACACS+ or RADIUS server. The user message is a text intended to be presented to the user when they connect to the node. The session timeout is the maximum time the user is allowed to stay connected. The audit logging functionality keeps track of the individual user name that has connected to the node.

### RADIUS

The RADIUS protocol, which is based on a client-server model, enables remote access to networks and network services. When configured with the IP or host name of a RADIUS server, the NE can act as a RADIUS client. The format and validation of RADIUS packets is in accordance with the IETF protocol specification RFC 2865.

Both IPv4 and IPv6 are supported.

RADIUS uses UDP, which offers best-effort delivery.

RADIUS only encrypts the password in the Access-Request packet from the client to the server. The rest of the packet (for example, user name, authorized services, and accounting) is not encrypted.

RADIUS supports the following features:

- Authentication

  The NE supports centralized authentication using RADIUS. A user needs to have an account created on the external server before logging on. Once the account is created, the system can be configured to receive centralized authentication using RADIUS. For centralized authentication, all Local Users are enabled.

- Authorization

  The NE supports fetching the user roles through a RADIUS server. The NE uses local authorization information to distinguish which privileges belong to a role.

The authorization process is based on the user role (system admin, network admin, operator, or guest). For authorization using RADIUS, the RADIUS server provides the user role when the user logs on to the NE. The NE can be managed in situations when a RADIUS server is unreachable. Therefore it ensures there is always at least one locally-authenticated system administrator account.

The default is that all Local Users are enabled. The user must manually set them to Disabled, after choosing the centralized mode. If they are disabled, then they will be automatically re-enabled in case all RADIUS servers are down.

— Accounting

The NE supports session accounting using RADIUS or TACACS+. The management sessions can be logged by enabling either the RADIUS or the TACACS+ accounting feature. When the session is started, that is, the management user is logged on, the NE sends an accounting start message to the RADIUS or TACACS+ server. When the session is ended, that is, the management user has logged off, the NE sends an accounting stop message to the RADIUS or TACACS+ server.

— RADIUS Server-Client Feature

The NE supports up to six RADIUS servers. It connects to the servers one-by-one according to their priorities. If no server is reachable, the NE enables local authentication automatically. When the communication to any RADIUS server is working again, the centralized authentication is automatically restored.

The NE supports three RADIUS packet types: Access-Request, Access-Accept, and Access-Reject.

A RADIUS Access-Request message containing the authentication information is sent to a remote server. When the RADIUS server receives the request, it validates the client using a ‘‘shared secret’’. If the client is valid, the RADIUS server consults its user database to validate the access. The server responds to an Access-Request message with either an Access-Reject message or an Access-Accept message. On receipt of an Access-Reject message, the client refuses access to the user. On receipt of an Access-Accept message, the client grants access to the user.

If the NE does not receive a RADIUS response to an Access-Request message within the configured timeout, it keeps retransmitting the request until it receives a response, or until the configured number of maximum transmissions has been reached.

### TACACS+

The TACACS+ protocol enables the building of a system that secures remote access to networks and network services. TACACS+ is based on a client/server architecture. The TACACS+ servers are configured on a per-context basis, with a limit of six servers.

Both IPv4 and IPv6 are supported.

TACACS+ uses the Authentication, Authorization, and Accounting (AAA) architecture. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting.

TACACS+ uses TCP, which offers connection-oriented transport.

TACACS+ encrypts the entire body of the packet.

TACACS+ supports the following features:

- Authentication

  The NE supports centralized authentication using TACACS+. A user needs to have an account created on the external server before logging on. Once the account is created, the system can be configured to receive centralized authentication using TACACS+.

- Authorization

  The NE supports fetching the user roles through a TACACS+ server, and the NE uses local authorization information to distinguish which privileges belong to a role.

  The authorization process is based on the user role (system admin, network admin, operator, or guest). For authorization using TACACS+, the TACACS+ server provides the user role when the user logs on to the NE. The NE can be managed in situations when a TACACS+ server is unreachable. Therefore it ensures there is always at least one locally-authenticated system administrator account. When the communication to any TACACS+ server is working again, the centralized authentication is automatically restored.

  The default is that all Local Users are enabled. The user must manually set them to Disabled, after choosing the centralized mode. If they are disabled, then they will be automatically re-enabled in case all TACACS+ servers are down.

- Accounting

  The NE supports session accounting using RADIUS or TACACS+. The management sessions can be logged by enabling either the RADIUS or the TACACS+ accounting feature. When the session is started, that is, the management user is logged on, the NE sends an accounting start message to the RADIUS or TACACS+ server. When the session is ended, that is, the management user has logged off, the NE sends an accounting stop message to the RADIUS or TACACS+ server.

The NE supports command accounting using TACACS+. User commands can be logged by enabling the TACACS+ command accounting feature. When the session is open, that is, the management user is logged on, the NE sends command accounting messages to the TACACS+ server.

### 16.10.2 NTP Authentication

To prevent manipulation of the time signal, MINI-LINK 6600 authenticates that the system is synchronized with the Network Time Protocol (NTP) server. An event is generated if the connection to the NTP server is lost.

The user is able to do the following:

- Enable/Disable authentication
- Set the external FTP server to download the Key File

  The Key File is a file with a number of cryptographic NTP keys that can be downloaded via SFTP from an external server.
- Download the Key File

### 16.10.3 SFTP

An SFTP server can be used to upgrade NE system software, instead of just using an FTP server. Using SFTP instead of FTP ensures that the entire session, including passwords, is encrypted. When adding a new FTP or SFTP server, it is possible to reserve that server for security tasks, so that only the admin_user is allowed to modify the server. Other users, for example control_user, can add the same server and use it for purposes that are not security related.

For more information about software management, see Section 16.5 on page 224

### 16.10.4 File Integrity Violation

File integrity violation raises an alarm if the internal files of the node are modified. Each node has a file integrity check available, that enhances protection against viruses and Trojan Horses. The file integrity check monitors for changes to files and directories in the system. It uses some cryptographic means that basically protect the configuration files it uses for that scope. When a change is captured, then a report is automatically generated and the user can check the reason for those changes, and then investigate and take proper actions. The user can view the report or upload the report to an external secure server through SFTP. An alarm is raised in case of integrity violations.

### 16.10.5 Security Audit Logging

The NE has an audit log that traces user-initiated events in the node back to the responsible user/operator. The audit log is a text file comprising the following information:

- Sequence number
- Timestamp
- User name
- IP address of the host associated with the event
- Operation including values (when applicable)

The alarm is raised when the audit log transfer to the externally-configured FTP or SFTP server is unsuccessful.

The audit log is not affected if the NE is restarted and it cannot be changed in MINI-LINK Node GUI. The audit log can be transferred to an FTP server on a regular basis.

### 16.10.6 Monitoring Local Users and Active Sessions

It is possible to view and download reports about local users and active sessions from MINI-LINK Node GUI.

**Note:** For viewing and downloading reports, admin_user is required.

About local users generated by the node, information on the previous session (start date and time) can be monitored.

About active sessions, the following parameters can be monitored:

- Information on the user
- IP address
- Session ID
- Interface used (CLI, NETCONF, SNMP, or MINI-LINK Node GUI)
- Start time of the active session

### 16.10.7 Syslog for Security Events

It is possible to send Security events to an external Syslog server in syslog format to trace security events and user actions.

The selected existing security events are sent in Syslog format, independently of the audit log file. "Event" means "setting" in this respect. For example, the protocol setting Telnet/SSH is considered a security event, and the change between Telnet/SSH will be notified to the external Syslog server once it is configured to do so.

### 16.10.8 Disable Local O&M Ports

It is possible to disable local access to an NE by disabling the local ports in terms of the USB port and the LAN port.

If both the USB and LAN port are disabled, it is no longer possible to access the DCN and the NE on-site. It is possible to disable the LAN port and the USB port independently. The only way to access the node is to access the DCN remotely, either from an OMC or from a remote node.

### 16.10.9 Notification on Logon

Through Notification on Logon, the OMC can react on an unexpected logon. Notification on Logon is available for local (USB) connections.

An event is sent to the management systems each time a user logs on to an NE. The notification contains a timestamp, the user name, the IP address, and information on whether a logon is through CLI or SNMP. Upon successful logon, the information associated with the last successful logon is displayed up to 30 days. The Security Issue on Logon alarm, which can be enabled using MINI-LINK Node GUI, is raised in case of three consecutively failed logon attempts. This alerts the management system of a potential security threat.

### 16.10.10 Password Cracking Defense: Setting Brute Force Threshold

Delayed logon is activated to protect against password cracking. When a suspected attack is performed against CLI, MINI-LINK Node GUI, NETCONF or SNMP interface, a delay is inserted in case of an authentication error. The delay is inserted when a certain number of authentication errors is reached during a time window (activation threshold). The normal behavior is restored only when no error is detected during the defense mode for a certain period of time (defense period). The functionality can be managed through the activation threshold setting.

**Note:** When brute force defense mode is activated, the following system response is applicable:

- Users with blacklisted user names or blacklisted IP addresses cannot access the NE.
- Non-blacklisted users can access the NE but can experience system slowdown.

It is possible to set a time limit for how long the brute force protection lockout is to be active after a failed login attempt. It is also possible to monitor and reset the locked sessions. These settings can be configured using either CLI or MINI-LINK Node GUI.

### 16.10.11 Firewall

A firewall is in place for packet filtering on the IP address and the range of the IP address. The packet filter option is protection from external traffic connections through each possible port or service by closing or opening commands. These options are only available to the admin_user.

Both IPv4 and IPv6 are supported.

### 16.10.12 Legal Notice

It is possible to add a legal notice shown before logging on, to highlight the legal consequences of unauthorized access. The legal notice can be customized according to local law.

### 16.10.13 Access Control Lists

IPv4 Access Control Lists (ACLs) can filter incoming or outgoing IPv4 packets on IP interfaces, based on the contents of the IPv4 header. Packets can be permitted or denied at line speed using hardware capabilities.

The supported filtering parameters are the following:

- Source IP address
- Destination IP address
- IP protocol type
- TCP/UDP source port
- TCP/UDP destination port

ACLs can be configured independently on each VLAN interface and VLAN subinterface. The total number of configurable ACLs is limited per node based on the type of the NPU.

Transit and originating or terminating IP packets are filtered by the access lists.

**Note:** ACLs are not supported for PPP and loopback interfaces.

# 17 Accessories

The MINI-LINK 6600 product program contains a comprehensive set of accessories for installation and operation. This section gives additional technical information for Small Form Factor Pluggable (SFP) and Small Form Factor Pluggable Plus (SFP+).

For a full list of approved SFP and SFP+, see MINI-LINK 6600 R1 Compatibility, Reference [1].

## 17.1 SFP

The SFP exists as electrical or optical transmitter/receiver for PDH/Ethernet, see Figure 150.

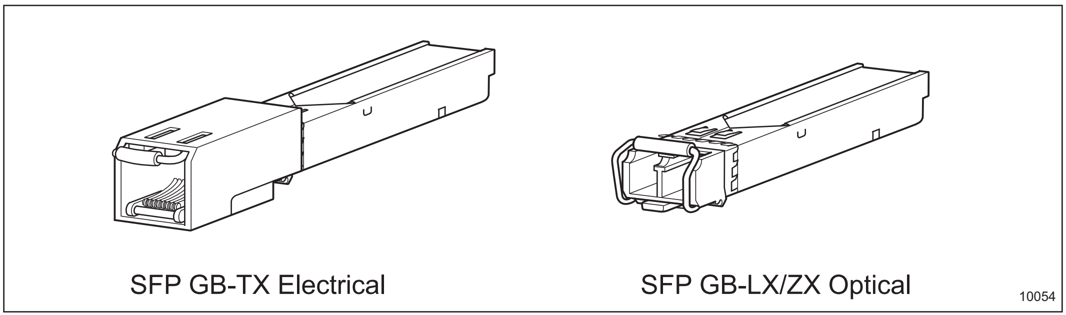


Figure 150 Electrical/Optical SFP

## 17.2 SFP+

The SFP+ exists as optical transmitter/receiver for Ethernet, see Figure 151.

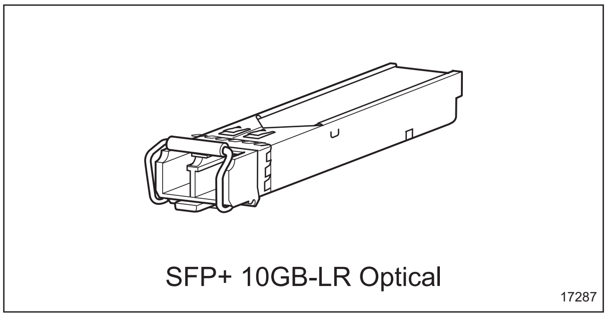


Figure 151 Optical SFP+

## 17.3 Tunable DWDM SFP+

The tunable SFP+ is a Dense Wavelength Division Multiplexing (DWDM) transceiver for Ethernet. Tunable DWDM SFP+ allows adjusting the transmission wavelength within the C-band DWDM International Telecommunication Union (ITU) Grid. The use of tunable DWDM SFP+ is supported in the 10G port of the ETU 1002 plug-in unit.

## 17.4 Direct-Attach Copper Cable

The Direct-Attach Copper Cable (DAC) is an electrical traffic cable that can be used to directly connect MINI-LINK 6600 with another product placed physically close. It is equipped with SFP+ modules at both ends, and it provides a 10 Gbps rate.

# Reference List

[1] MINI-LINK 6600 R1 Compatibility, 1/221 02-HRA 901 20/11

[2] Physical/Electrical Characteristics of Hierarchy Digital Interface, ITU-T G.703 (11/2001)