User Manual

NUSA1, NUSA1-F
nusa1_r3b

STM-16, STM-4, STM-1, EoS, TDM services

XMC20

Document PEC

EN/LZTBU 372 142/2 RB

Document release

XMC20 R6B | 10 December 2015

Published by

http://www.keymile.com

Content

Figures

1 Preface

1.1 Precautions and Safety

Before you handle any equipment you must comply with the safety advices.

Adherence to the safety instructions ensures compliance with the safety requirements as defined in EN 60950 (Safety of Information Technology Equipment).

Please refer to the following document:

[202] Safety Instructions “Precautions and safety”.

1.2 Symbols and Notations

This User Manual uses the following symbols:

CAUTION

Non-observance could result in minor or moderate injury.

Failing to comply with this may result in the injury of the user or in physical damage.

→ Possible actions are given.

Risk of operating trouble!

Indicates that an action may lead to operating trouble or loss of data.

→ Possible actions are given.

Please note:

Shows significant information.

→ Possible actions are given.

1.3 Interfaces and Circuit Categories

Table 1: Electrical interfaces and circuit categories

NUSA1 interface	Circuit category according to EN 60950-1	Max. rating	
		Voltage	Current
Local power supply	TNV2	< 72 V_{DC}	< 1.6 A
Electrical Gigabit or Fast Ethernet	SELV	< 3 V	< 10 mA
Electrical STM-1	SELV	< 1V	< 10 mA

Table 2: Optical interfaces

NUSA1 interface	Parameter	Max. rating	Remarks
Optical STM-1, STM-4 and STM-16	Laser class (according to EN 60950-1)	1 [a]	
	Optical transmitted power [b]	5 dBm	
	Transmitted wavelength	1310 nm, 1550 nm, 1470 nm … 1610 nm	non-visible radiation
	Time until automatic safety power reduction operates	0.85 s	
	Time until automatic restart takes place	110 s	

a. As the laser protection class 1 is complied, dangerous radiation cannot be emitted. Thus, special precautions for failures or laser warnings are not necessary.
b. Optical transmitted power, modulation and wavelengths are typical values for SFP modules, however these values may vary depending on SFP types and manufacturers.
Please refer to SFP manufacturers data sheets for more details.

1.4 Document History

Table 3: Document history

KEYMILE PEC		Date	XMC20 release	Changes since previous version
EN/LZTBU 372 142/2	RB	November 2015	R6B	Unit not usable in slot-13 of the XMC20 subrack. RSTP and MSTP no longer supported. Support of rate limiters on Ethernet and EoS ports.
EN/LZTBU 372 142/2	RA	March 2015	R6A	Support of MPLS-TP.
EN/LZTBU 372 142/1	RA	March 2015	R4C	Ethernet transmit timing is always free running. The EoS differential delay is configurable.
EN/LZTBU 372 142	RD	February 2015	R4C	First revision for the XMC20 system release R4C.

1.5 Definition of Terms

Table 4: Specific terms

Term	Explanation
NUSA1	Designates the one slot wide functional unit NUSA1 nusa1_r3b, SDH transport unit for TDM and Ethernet traffic of the XMC20. It must be operated in an actively cooled XMC20 subrack with a fan unit. In this user guide, the term NUSA1 is used to name the NUSA1 and NUSA1-F. Where certain features or characteristics apply to the NUSA1-F only, the NUSA1-F is named explicitly.
NUSA1-F	Designates the two slot wide functional unit NUSA1 nusa1_r3b, SDH transport unit for TDM and Ethernet traffic of the XMC20. NUSA1-F is functionally identical to the NUSA1 unit, but can be operated in XMC20 subracks with passive cooling, i.e. fanless operation.

2 Introduction

This section provides a general introduction to the NUSA1 unit. Further on it presents a unit view in section 2.2 Unit View (on page 14) and a block diagram in section 2.3 Block Diagram (on page 15).

2.1 General

This document describes the architecture and functions of the NUSA1 and NUSA1-F units and shows, how the units are commissioned and operated as part of the XMC20.

The NUSA1 is a 1 slot wide functional unit of XMC20 that must be operated in actively cooled subracks. The NUSA1-F is a 2 slot wide functional equivalent to the NUSA1 unit that can be operated in passively cooled subracks.

The NUSA1 and NUSA1-F units are SDH units, providing four SDH front interfaces, four Ethernet front interfaces, PBUS access (XMC20 internal TDM bus) and also connect to the Gb-Ethernet star (XMC20 internal Ethernet connection to the core unit).

The NUSA1 and NUSA1-F units can be configured as an SDH access system with termination and add/drop functionality from STM-16, STM-4 and STM-1 trunks. Typical applications are the termination of STM-16, STM-4 or STM-1 traffic from an STM-16, STM-4 or STM-1 trunk in linear networks (terminal multiplexer TM) and add/drop of VC-n traffic in linear or ring networks (add/drop multiplexer ADM).

The following SDH interfaces are supported:

- two interfaces STM-16 or STM-4:
  - STM-16 optical or
  - STM-4 optical,
- two interfaces STM-4 or STM-1:
  - STM-4 optical or
  - STM-1 electrical or optical,

The interfaces can be used as aggregate interfaces for the transmission of STM-16, STM-4 or STM-1 traffic into the transport network, or as tributary interfaces for the access of subtended network elements. The aggregate or tributary usage of an interface is independent of the NUSA1 or NUSA1-F configuration.

The interfaces are implemented on NUSA1 and NUSA1-F with four SFP cages, allowing to plug in any compatible SFP module according to the network application.

The NUSA1 and NUSA1-F units implement also the synchronous equipment timing source (SETS) for the unit.

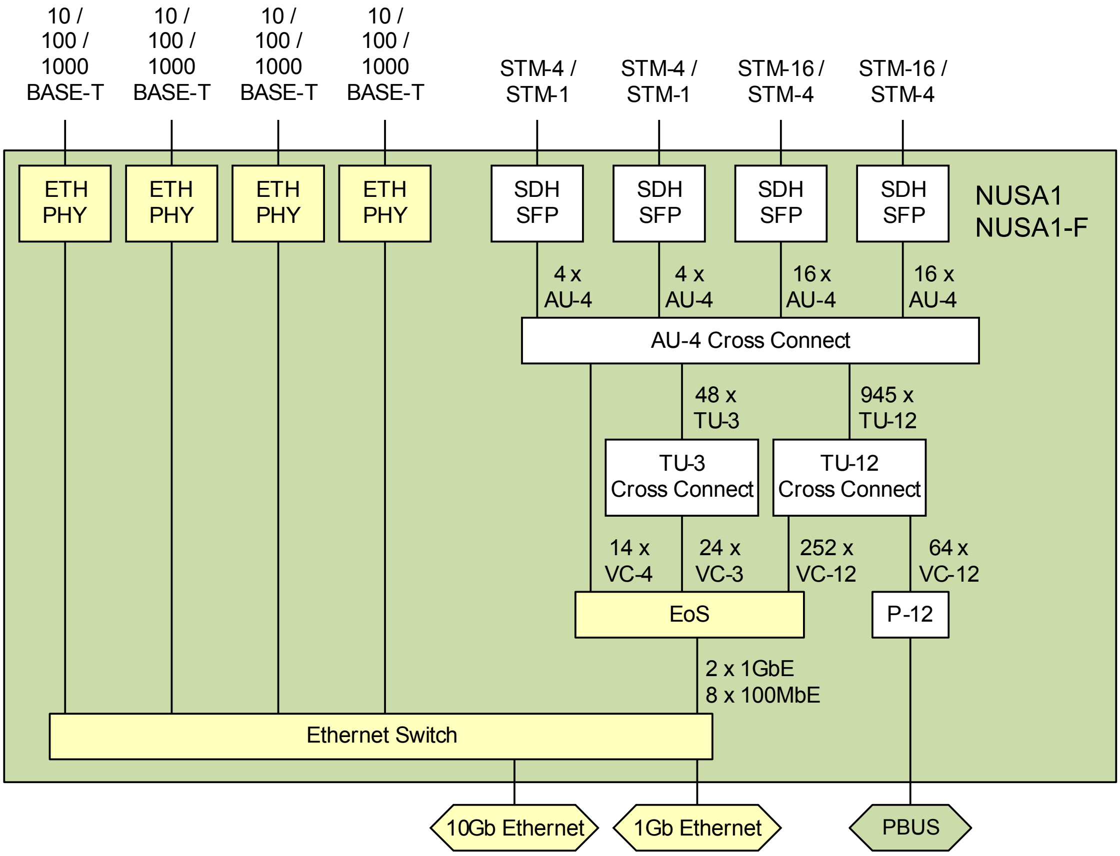


Figure 1: NUSA1 and NUSA1-F overview

The NUSA1 and NUSA1-F units access Ethernet services via the units four electrical 10/100/1000BASE-T front interfaces and the Gb-Ethernet star from the COGE5 core unit(s). The Gb-Ethernet star connects the NUSA1 or NUSA1-F unit to the working and protecting COGE5 core units. The Ethernet switch device on the NUSA1 and NUSA1-F unit participates in the XMC20 Switch.

Please note:

The access to the 10Gb-Ethernet star will be available in a future release.

Ethernet over SDH (EoS) traffic can be transported in two modes:

- Unswitched mode:
  The Ethernet traffic from an Ethernet front port is bypassing the Ethernet switch device and is mapped to a EoS group. There is one dedicated EoS group per front port in the unswitched mode.
  Ethernet traffic from any other XMC20 Switch port can be transported over SDH. With the four Ethernet front ports using the unswitched mode, 28 EoS groups remain available for the XMC20 Switch ports. The total EoS transport capacity is limited to 2 Gbit/s.
- Switched mode:
  A NUSA1 or NUSA1-F Ethernet front port in the switched mode accesses the switch device and participates in the XMC20 Switch. Ethernet traffic from the Ethernet front ports and any other XMC20 Switch port can be transported over SDH. There are 32 EoS groups in maximum. The total EoS transport capacity is limited to 2 Gbit/s.

Please note:

Using the MPLS-TP Transport function with the VPWS service, the number of EoS groups is limited:

→ Maximum 8 EoS groups in the unswitched mode.

→ Maximum 12 EoS groups in the unswitched mode.

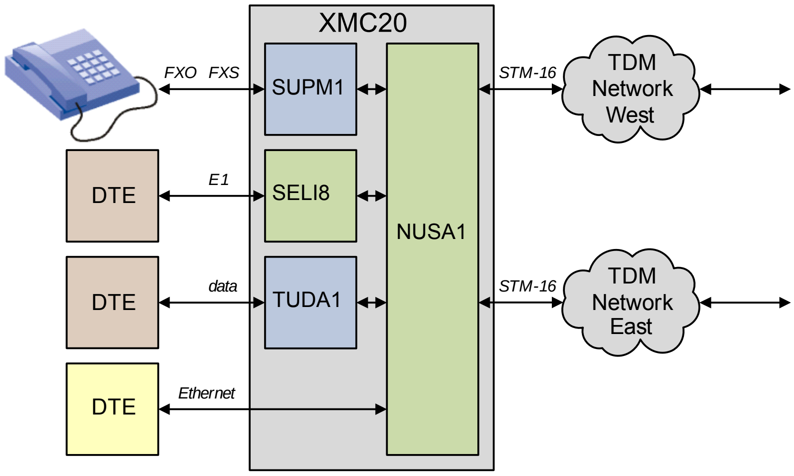


Figure 2: NUSA1 unit in an add/drop multiplexer application

The NUSA1 and NUSA1-F units access TDM services via PBUS. Up to 64 P12 tributary signals can directly be accessed.

2.2 Unit View

Figure 3: NUSA1 (left) and NUSA1-F (right) unit view

Figure 3 "NUSA1 (left) and NUSA1-F (right) unit view" shows the NUSA1 and NUSA1-F unit hardware. On the front plate are two LEDs for unit- and traffic failure indication.

CAUTION

Non-observance could result in minor or moderate injury.

The front of the NUSA1-F can become hot.

→ Do not touch the front cover.

2.3 Block Diagram

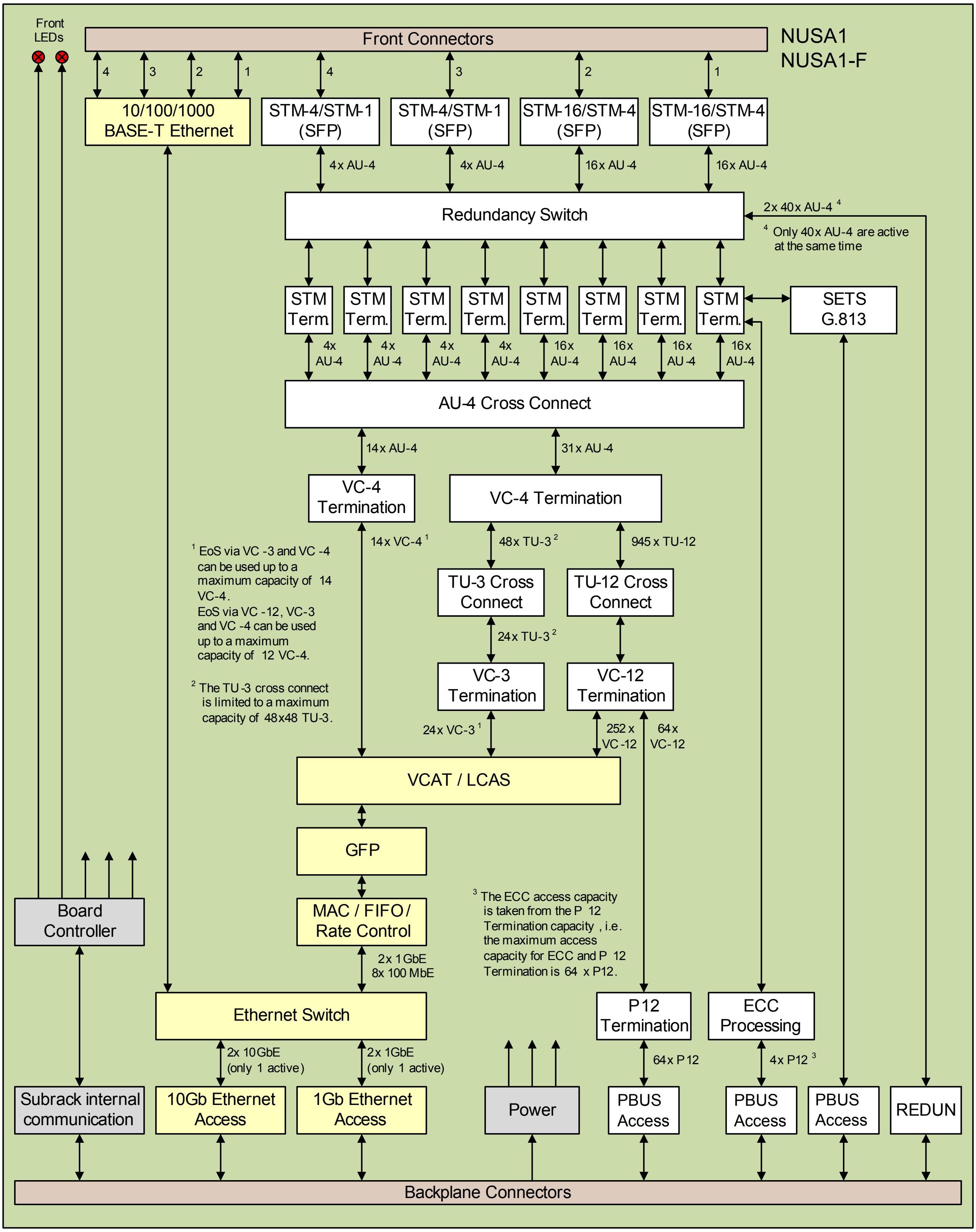


Figure 4: NUSA1 block diagram

Figure 4 "NUSA1 block diagram" shows the block diagram of the NUSA1 unit. The main functions of the NUSA1 unit can be divided into the following eight parts:

- SDH terminal multiplexer or add/drop multiplexer with four SDH interfaces: 2 x STM-16/STM-4 and 2 x STM-4/STM-1.
- SDH cross connect system for 125 x 125 AU-4.
- SDH cross connect system for 48 x 48 TU-3
- SDH cross connect system for 1261 x 1261 TU-12
- Termination to the PBUS of 64 x P12.
- Ethernet over SDH for up to 32 EoS groups with a maximum capacity of 2 Gbit/s.
- Redundancy switch
  The redundancy switch is used for the 1+1 equipment protection application with two NUSA1 units. It connects the protecting NUSA1 unit via the backplane with a capacity of 2 x 40 x AU-4.

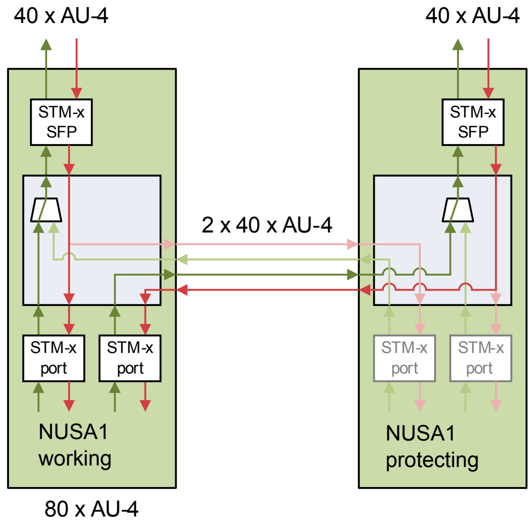


Figure 5: Redundancy switch, working unit is active

  The redundancy switch makes the four SDH ports on the working unit and the four SDH ports on the protecting unit available on the working unit, i.e. doubles the terminated SDH traffic from 40 x AU-4 to 80 x AU-4.
- Ethernet switch
  The Ethernet switch device on the NUSA1 unit participates in the XMC20 Switch. XMC20 Switch ports are all external Ethernet ports on units participating in the XMC20 Switch, the NUSA1 EoS ports and, depending of the switch mode, the NUSA1 external Ethernet ports:
  - Unswitched mode:
    A NUSA1 external Ethernet port is not part of the XMC20 Switch. The Ethernet traffic from the Ethernet front ports is bypassing the Ethernet switch device and is mapped to a dedicated EoS port with a point-to-point connection.
    With the VLAN Bridge function all EoS ports can be used as customer VLAN ports (CVP).
    With the MPLS-TP Transport function up to 8 EoS ports can be used as Pseudo Wire Attachment Circuits (PWAC) in a VPWS or up to 28 EoS ports can be used as Customer VLAN Ports (CVP) in a VPLS.
  - Switched mode:
    A NUSA1 external Ethernet port is part of the XMC20 Switch.

With the VLAN Bridge function all external Ethernet ports and EoS ports can be used a customer VLAN ports (CVP).

With the MPLS-TP Transport function the external Ethernet ports and up to 12 EoS ports can be used as Pseudo Wire Attachment Circuits (PWAC) in a VPWS or up to 32 EoS ports can be used as Customer VLAN Ports (CVP) in a VPLS.

3 Functions and Specifications

The NUSA1 unit uses the following feature licences, provides the functions listed below and conforms to the corresponding standards and recommendations (conformance to applicable parts of the standards).

3.1 Feature Licences

This unit is subject to one or several feature licences. The following licences are available for this unit.

Table 5: Feature licences relevant for this unit

Licence ID	Short Description	Description
FL_STM16	Lic NUSA STM16	Feature Licence for STM-16 operation of NUSAx and NUSAx-F - right to use per card.

Please note:

Two NUSA1 units operating as equipment protected pair and both using STM-16 ports need two feature licences.

For more information on features licences please refer to [012] Release Note “XMC20 System Release R6B” and to [915] Technical Bulletin “Feature Licences for XMC20”.

3.2 Summary of Standards

Table 6: Standards

Feature	Standard	Release
SDH transport, ETSI	- EN 300 147 (09/2001) Synchronous digital hierarchy multiplexing structure - EN 300 417-1-1 (10/2001) Generic processes and performance - EN 300 417-2-1 (10/2001) SDH and PDH physical section layer functions - EN 300 417-3-1 (10/2001) STM-N regenerator and multiplex section layer functions - EN 300 417-4-1 (10/2001) SDH path layer functions	r1a
SDH transport, ITU-T	- ITU-T G.707 (01/2007) Network node interface for the synchronous digital hierarchy - ITU-T G.783 (03/2006) Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks - ITU-T G.803 (03/2000) Architecture of transport networks based on the synchronous digital hierarchy (SDH) - ITU-T G.805 (03/2000) Generic functional architecture of transport networks - ITU-T G.806 (01/2009) Characteristics of transport equipment – Description methodology and generic functionality - ITU-T G.841 (10/98) Types and characteristics of SDH network protection architectures - ITU-T G.808.1 (02/2010) Generic protection switching – Linear trail and subnetwork protection - ITU-T G.957 (03/2006) Optical interfaces for equipments and systems relating to the synchronous digital hierarchy	r1a
Optical interfaces	SFF committee - INF-8074i Rev. 1.0 (05/2001) SFP (Small Formfactor Pluggable) Transceiver - SFF-8472 Rev. 9.5 (06/2004) Diagnostic Monitoring Interface for Optical Xcvrs ITU-T - G.694.2 (12/2003) Spectral grids for WDM applications: CWDM wavelength grid IEC - 60825-1 (08/2001) Safety of laser products – Part 1: Equipment classification, requirements and user's guide	r1a

Table 6: Standards (continued)

Feature	Standard	Release
Synchronization and timing	ETSI - EN 300 417-6-1 (05/99) Synchronization layer functions - EN 300 462-1-1 (05/1998) Definitions and terminology for synchronization networks - EN 300 462-4-1 (05/1998) Timing characteristics of slave clocks suitable for synchronization supply to Synchronous Digital Hierarchy (SDH) and Plesiochronous Digital Hierarchy (PDH) equipment - EN 300 462-5-1 (05/1998) Timing characteristics of slave clocks suitable for operation in Synchronous Digital Hierarchy (SDH) equipment ITU-T - ITU-T G.813 (03/2003) Timing characteristics of synchronous digital hierarchy (SDH) equipment slave clocks (SEC) - ITU-T G.825 (03/2000) The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)	r1a
PDH transport	ETSI - EN 300 417-5-1 (10/2001) PDH path layer functions ITU-T - ITU-T G.704 (10/1998) Synchronous frame structures used at 1544, 6312, 2048, 8488 and 44736 kbit/s hierarchy levels - ITU-T G.775 (10/98) Loss of Signal (LOS), Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) defect detection and clearance criteria for PDH signals - ITU-T G.805 (03/2000) Generic functional architecture of transport networks	r1a
Access digital section for ISDN primary rate	ETSI - ETS 300 233 (05/1994) Integrated Services Digital Network (ISDN); Access digital section for ISDN primary rate	r1a
Ethernet transport	IEEE - IEEE 802.3-2008 CSMA/CD access method and physical specifications. - IEEE 802.1D-2004 Media Access Control bridges.	r1a
Ethernet over SDH transport	ITU-T - ITU-T G.7041(04/2011) Generic Frame Procedure - ITU-T G.7042 (03/2006) Link Capacity Adjustment Scheme (LCAS) for virtually concatenated signals.	r1a

Table 6: Standards (continued)

Feature	Standard	Release
Performance parameters and limits	ITU-T - ITU-T G.826 (12/2002) End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections - ITU-T M.2101.1 (04/97) Performance limits for bringing into service and maintenance of international SDH paths and multiplex section	r1a
Ethernet management	IETF - RFC 1213 (03/1991) Management Information Base for Network Management of TCP/IP-based internets: MIB-II - RFC 2819 (05/2000) Remote Network Monitoring Management Information Base	r1a
Character set	ITU-T - ITU-T T.50 (09/92) International Reference Alphabet (IRA) - Information technology - 7 bit coded character set for information interchange	r1a

3.3 Specifications

Risk of operating trouble!

The usage of specific VLAN IDs in the XMC20 Switch is prohibited when a NUSA1 unit is plugged in a XMC20 subrack.

→ Never use the VLAN IDs 4059 to 4062.

Please note:

For the specifications exclusively applicable for the NUSA1-F unit please refer to section 3.4 NUSA1-F Function Overview (on page 28).

Table 7: Functions and specifications - SDH parameters

Feature	Rating or standard	Release
SDH ports		r1a
- Number of STM-16/STM-4 ports	2 STM-16: optical STM-4: optical	
- Number of STM-4/STM-1 ports	2 STM-4: optical STM-1: optical or electrical	
- Optical STM-16 interface	SFP module with optical STM-16 interface according to ITU-T G.957 with different transmission ranges	
- Optical STM-4 interface	SFP module with optical STM-4 interface according to ITU-T G.957 with different transmission ranges	
- Optical STM-1 interface	SFP module with optical STM-1 interface according to ITU-T G.957 with different transmission ranges	
- Optical connection	Fibres according to ITU-T G.957 Connector duplex LC-type	
- SFP features	- Manual laser activation / deactivation - Automatic laser shutdown (ALS) - Automatic laser restart (ALR)	
- Parameters of the optical interfaces (SFP modules)	According to the manufacturer's data sheets	
- Electrical STM-1 interface	SFP module with electrical STM-1 interface according to ITU-T G.703	
- Electrical connection	Coaxial, 75 Ω Connector DIN 1.0/2.3 (push-pull self latching/coupling)	
SDH traffic layers		r1a
- Number of VC-4 resources	80	
- AU-4 cross connect	125 x 125, unrestricted	
- Number of VC-3 resources	48	
- TU-3 cross connect	48 x 48, unrestricted	
- Number of VC-12 resources	945	
- TU-12 cross connect	1261 x 1261, unrestricted	

Table 7: Functions and specifications - SDH parameters (continued)

Feature	Rating or standard	Release
Synchronization		r1a
- SETS on unit	1	
- Number of selectable SDH clock sources	- 4, derived from working unit STM-16/STM-4/STM-1 signals - 4, derived from protecting unit STM-16/STM-4/STM-1 signals - 4, derived from SDH signals from other units (shared with terminated PDH signals)	
- Number of selectable PDH clock sources	4, derived from terminated PDH signals (shared with SDH signals from other units)	
- External synchronization input	2, derived from the external synchronization signal on the working and protecting COGE5	r1a
- Local oscillator	Reference clock with an accuracy of ± 4.6 ppm according to ITU-T G.813 (clause 5, option 1).	r1a
- External synchronization output	1, external clock output on the working and protecting COGE5	r1a

Table 8: Functions and specifications - PDH parameters

Feature	Rating or standard	Release
Number of P12 resources	64	r1d
P12 traffic signal handling, 64 P12 signals	- terminated G.704 with CAS, with CRC4 - terminated G.704 with CAS, without CRC4 - terminated G.704 without CAS, with CRC4 - terminated G.704 without CAS, without CRC4 - V5 uplink, with CRC4 - V5 uplink, without CRC4 - transparent - clock master	r1d
ECC layer	via SDH RS DCC (D1 … D3 bytes, 192 kbit/s), and/or via SDH MS DCC (D4 … D12 bytes, 576 kbit/s)	r1a

Table 9: Functions and specifications - Ethernet parameters

Feature	Rating or standard	Release
Ethernet ports		r1a
- Number of Ethernet ports	4 electrical	
- Interface type	10/100/1000BASE-T	
- Interface mode	Auto - MDI/MDI-X	
- Electrical connection	Connector RJ-45 Impedance 100 ± 15 Ω for the frequency band from 1 to 100 MHz	
Ethernet traffic layers		r1a
- Ethernet modes	- 10BASE-T half duplex - 10BASE-T full duplex - 100BASE-TX half duplex - 100BASE-TX full duplex - 1000BASE-T full duplex - Autonegotiation	

Table 9: Functions and specifications - Ethernet parameters (continued)

Feature	Rating or standard	Release
- Ethernet features	- Flow control IEEE 802.3	r1a
	- Link pass through	r2a
- VLAN Bridging [a]	- between the Ethernet front interfaces and the VC group, transport capacity limited to 100 Mbit/s per VC group (unswitched mode) - between the Ethernet front interfaces and any other XMC20 Switch port, including up to 32 VC groups, transport capacity limited to 2 Gbit/s for all VC groups (switched mode)	r1a
- MPLS-TP Transport with VPWS [b]	- between the (switched) Ethernet front interfaces (PWAC) and an MPLS-TP port on the core unit. - between the EoS groups 1 to 12 (PWAC) and an MPLS-TP port on the core unit.	r3a
- MPLS-TP Transport with VPLS [b]	- between the (switched) Ethernet front interfaces (CVP) and an MPLS-TP port on the core unit. - between the EoS groups 1 to 32 (CVP) and an MPLS-TP port on the core unit.	r3b
- Frame size	up to 9’194 bytes	r1a
EoS layer		r1a
- Number of virtual concatenation groups	- 4 switched or unswitched (point-to-point, EPL) - 28 switched	
- Framing procedure	GFP according to ITU-T G.7041	
- VC concatenation	virtual concatenation according to ITU-T G.783	
- VC capacity adjustment	link capacity adjustment scheme according to ITU-T G.7042	
- Number of VC-4 resources	up to 14 [c]	
- Number of VC-3 resources	up to 24	
- Number of VC-12 resources	up to 252	
Ingress buffer, switched or unswitched	guaranteed per Ethernet port or EoS group: - 10’240 bytes, - 1 frame	r1e
Egress buffer, switched or unswitched	guaranteed per Ethernet port or EoS group: - 3’584 bytes per queue [d], - 19 frames per queue. limit per Ethernet port or EoS group: - 3’584 bytes per queue, plus up to 128 kB from a pool of 512 kB [d], - 19 frames per queue, plus up to 128 frames from a pool of 2048 frames.	

a. The switch device will drop any incoming Ethernet packet with an incorrect length field.
b. An Ethernet front interface in the unswitched mode connects directly to the corresponding EoS group. This EoS group is no longer available for the MPLS-TP Transport function.
c. This value is valid if only VC-4 and VC-3 EoS group members are used.
If also VC-12 EoS group members are used the maximum number of VC-4 equivalents is reduced to 12:
- up to 8 VC-4 equivalents for VC-4 and VC-3 members,
- up to 4 VC-4 equivalents for VC-12 members.
d. Buffers are consumed by the frames in steps of 256 bytes, e.g. a frame with a size of 300 bytes occupies a buffer size of 512 bytes.

Table 10: Functions and specifications - maintenance features

Feature	Rating or standard	Release
Error detection	MS layer VC-4 layer VC-3 layer VC-12 layer	r1a
Trail trace identifier (TTI)	RS layer VC-4 layer VC-4, VC-3 and VC-12 layer per VCG VC-12 layer	r1a
Signal label	VC-4 layer VC-3 layer VC-12 layer	r1a
Remote defect indication	VC-4 layer VC-3 layer VC-12 layer	r1a
Loops	P12 front to front P0 front to front	r1a

Table 11: Functions and specifications - protection and alarming

Feature	Rating or standard	Release
Protection		
- 1:1 equipment protection	Two NUSA1 units, - PDH traffic to PBUS - EoS traffic to Ethernet interfaces - SETS	r1a
- Multiplex section protection (MSP)	SDH ports on the same NUSA1 unit (unidirectional and bidirectional) SDH ports on two NUSA1 units plugged in mating subrack slots (unidirectional and bidirectional)	r1a
- SNCP/I	up to 255 protected connections between any 2 not terminated VC-n, on the same NUSA1 unit	r1a
- SNCP/I protection modes	- 1+1 unidirectional, revertive - 1+1 unidirectional, non-revertive	
- SNCP/N	up to 255 protected connections between any 2 terminated VC-n, on the same NUSA1 unit	r1a
- SNCP/N protection modes	- 1+1 unidirectional, revertive - 1+1 unidirectional, non-revertive - 1+1 bidirectional, revertive, for VC-12 terminated to PBUS - 1+1 bidirectional, non-revertive, for VC-12 terminated to PBUS	
- SNCP	between any 2 P12 or P0-nc signals from the PBUS	r1a
- SNCP protection modes	- 1+1 unidirectional, revertive - 1+1 unidirectional, non revertive (for P0-1c only)	
Alarm reporting	ITU-T X.733 (1992) Information technology – open systems interconnection – systems management: Alarm reporting function	r1a

Table 12: Functions and specifications - performance monitoring

Feature	Rating or standard	Release
ITU-T G.826	MS layer VC-4 layer VC-3 layer VC-12 layer P12 layer	r1a
Layer specific events	PS layer: - Out of frame MS layer: - Protection switchover VC-4 layer: - Protection switchover VC-3 layer: - Protection switchover VC-12 layer: - Protection switchover P12 layer: - Positive slips - Negative slips	r1a
MIB-2 statistics	Ethernet layer: - In octets - In unicast packets - In discarded packets - In errors - In flow control packets - Out octets - Out packets - Out flow control packets	r1a
GFP encapsulation	GFP layer: - Transmitted GFP frames - Received GFP frames - Discarded GFP frames - Errored GFP frames	r1a

Table 13: Functions and specifications - mechanical and environmental parameters

Feature	Rating or standard	Release
Power supply		
- Power supply range V_{BAT}	refer to [201] System Description “XMC20 R6B”	
- Maximum current consumption, I_{VBAT} V_{BAT} = -48 V	0.8 A	
- Maximum total power requirement from battery, P_{TOT} V_{BAT} = nominal voltage	39 W The above rating includes the power consumption of four typical S.4-1 SFPs (4 x 1 W). Depending on the actually plugged SFP modules, the power consumption may be higher.	

Table 13: Functions and specifications - mechanical and environmental parameters (continued)

Feature	Rating or standard	Release
Mechanical parameters		
- Construction practice	19 inch	
- Height of unit (1 HU = 44.45 mm)	6 HU	
- Width of unit (1 TE = 5.08 mm)	4 TE (1 slot)	
- Size of the PCB (H x D)	233 mm x 220 mm	
- Weight	510 g	
- RoHS	Directive 2002/95/EC of the European Parliament and of the Council of 27.1.2003 on the Restriction of the use of certain hazardous substances in electrical and electronic equipment	
- WEEE	Directive 2002/96/EC of the European Parliament and of the Council of 27.1.2003 on waste electrical and electronic equipment	
Reliability		
- Calculated MTTF at 35 °C (MIL-HDBK-217F)	47 years	
Emission	refer to [201] System Description “XMC20 R6B”	
Immunity	refer to [201] System Description “XMC20 R6B”	
Safety	refer to [201] System Description “XMC20 R6B” SFP modules: according to the manufacturer’s data sheets (typically IEC 60825-1 Class 1 laser product)	
Ambient conditions	refer to [201] System Description “XMC20 R6B”. Error free operation up to 60°C ambient temperature is only guaranteed with SFP/SFP+ modules specified for the industrial temperature range (up to 85°C).	

3.4 NUSA1-F Function Overview

The NUSA1-F unit provides the same functions and supports the same standards as the NUSA1 unit, with the following exceptions:

Table 14: NUSA1-F function overview - equipment features

Function or Feature	Specification or Standard	Release
Mechanical parameters - Width of the unit (1 TE = 5.08mm) - Weight of the NUSA1-F unit	 8 TE (2 slots) 1’700 g	
Unit cooling	Operation without fan unit (passive ventilation). Vertical mounting of the units is mandatory.	
Reliability - Calculated MTTF at 35 °C (MIL-HDBK-217F)	 20 years	

Table 15: NUSA1-F function overview - other standards

Function or Feature	Specification or Standard	Release
Ambient conditions - Storage, Transport and Operation with active cooling	 refer to [201] System Description “XMC20 R6B”	
- Operation with passive cooling	-25°C … +55°C [a] Error free operation up to 55°C ambient temperature is only guaranteed with SFP/SFP+ modules specified for the industrial temperature range (up to 85°C).	

a. The NUSA1-F hardware revisions R1A and R1B support only a reduced maximum ambient temperature of 50°C instead of 55°C.

3.5 SFP Modules

The SDH interfaces of the NUSA1 unit are implemented with SFP cages where different SFP pluggable modules can be inserted providing STM-16, STM-4 and/or STM-1 front interfaces.

The SFP modules are standardised modules following the SFP – MSA (Multi-Source Agreement) and are implemented according to INF-8074.

For more information please refer to section 4.3 SFP Modules (on page 33).

3.6 Restrictions and Limitations of Implementation

3.6.1 Implementation Restrictions

The table below shows the implementation restrictions that are specific for the NUSA1 unit.

Table 16: Implementation restrictions

Keyword	Description
Threshold for degraded defect dDEG	In NUSA1 the threshold for the degraded defect dDEG is configured on the unit level per VC type, not individually per VC.
Wait to restore time, guard time and hold off time for SNCP	In NUSA1 the wait to restore time, guard time and hold off time for SNCP are configured on the unit level per VC type, not individually per VC.
Trail trace identifier TTI	NUSA1 supports the 16 byte TTI only. The one byte TTI is not supported.
E1 and E2 bytes	The E1 and E2 bytes of the RS and MS overhead provide a local order wire channel for voice communication between regenerators and multiplexers. NUSA1 provides no access to the E1 and E2 bytes.
F1 byte	The F1 byte provides a channel for user purposes. NUSA1 provides no access to the F1 byte.

3.6.2 Implementation Limitations

For limitations that apply to the NUSA1 implementation, please refer to [012] Release Note “XMC20 System Release R6B”.

4 Installation

4.1 Prerequisites

Before installing a NUSA1 unit take care to follow the safety advice as listed in [202] Safety Instructions “Precautions and safety”.

Valid combinations of hardware (HW) and embedded software (ESW) versions are given in [012] Release Note “XMC20 System Release R6B”.

For the installation of XMC20 HW
refer to [301] User Guide “XMC25 Installation”, or
refer to [310] User Guide “XMC23 Installation”, or
refer to [322] User Guide “XMC22 Installation”.

Risk of operating trouble!

Disconnect fibres before removing or installing SFP modules. Otherwise, there is a potential risk of damaging the optical interfaces and fibres.

4.2 Slots for the NUSA1 Unit

The NUSA1 unit uses one slot in the XMC20 subrack. The NUSA1-F unit uses two slots in the XMC20 subrack.

In a XMC25, the NUSA1 unit can be operated in any of the following slots:

NUSA1: 1 … 10, 12, 14 … 21.

NUSA1-F: 1 … 9, 12, 14 … 20.

In a XMC23, the NUSA1 unit can be operated in any of the following slots:

NUSA1: 7 … 10, 12, 14.

NUSA1-F: 7 … 9, 12.

In a XMC22, the NUSA1 unit can be operated in any of the following slots:

NUSA1: 9 … 10, 12.

NUSA1-F: 9.

Slot 11 is reserved for the working COGE5 unit.

When using NUSA1 equipment protection specific slot pairs in the XMC25 and XMC23 must be used:

XMC25:

- Slot 4 and slot 6
- Slot 18 and slot 20

XMC23:

- Slot 7 and slot 9

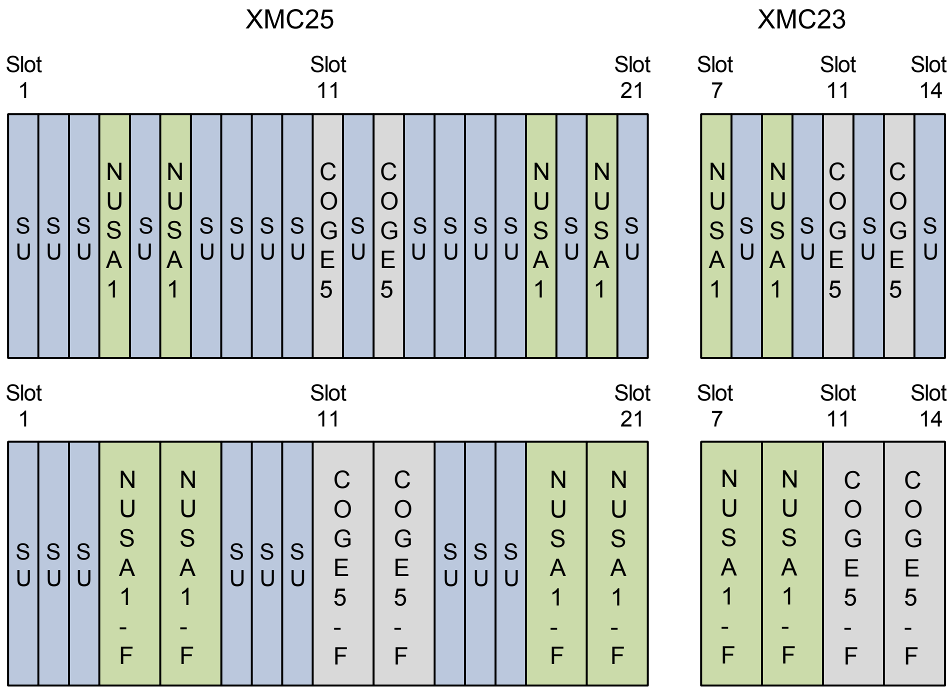


Figure 6: XMC25 and XMC23 subracks with NUSA1 and COGE5 equipment protection using dedicated slot pairs

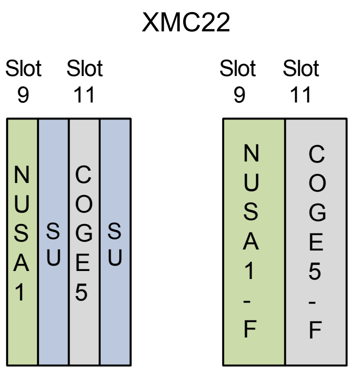


Figure 7: XMC22 subrack with NUSA1 and COGE5

4.3 SFP Modules

4.3.1 SFP Interface Types

NUSA1 has four SFP cages where different SFP modules for the SDH interfaces can be inserted. All recommended SFP modules are designed in conformance with the SFP Multi-Source Agreement (SFF document INF-8074i) and are hot pluggable, i.e. they can be installed and removed from an operational NUSA1 unit.

The supported SFP modules can provide the following interfaces:

- Optical STM-16 interface SFP modules
  - I-16.1 optical port (1310 nm, intra-office short haul)
  - S-16.1 optical port (1310 nm, short haul)
  - S-16.2 optical port (1550 nm, short haul)
  - L-16.1 optical port (1310 nm, long haul)
  - L-16.2 optical port (1550 nm, long haul)
- Optical STM-4 interface SFP modules
  - S-4.1 optical port (1310 nm, short haul)
  - L-4.1 optical port (1310 nm, long haul)
  - L-4.2 optical port (1550 nm, long haul)
  - X-4.2 optical port (1550 nm, enhanced long haul)
  - Bidirectional optical port (1310/1550 nm, short haul)
- Optical STM-1 interface SFP modules
  - S-1.1 optical port (1310 nm, short haul)
  - L-1.1 optical port (1310 nm, long haul)
  - L-1.2 optical port (1550 nm, long haul)
  - X-1.2 optical port (1550 nm, enhanced long haul)
  - Bidirectional optical port (1310/1550 nm, short haul)
  - CWDM optical port (1470 … 1610 nm, long haul)
  - CWDM optical port (1470 … 1610 nm, enhanced long haul)
- Electrical STM-1 interface SFP modules
  - Electrical STM-1 interface according to ITU-T G.703

The selection of the transceiver and the media type will determine the maximum distance.

For details on connectors and pins for these interfaces please refer to INF-8074i.

Please note:

The SFP transceiver modules must be mounted by the customer.

Please note:

Refer to http://www.keymile.com to get the latest list of recommended SFP modules:
Extranet / Documentation & Software / XMC20 / Techn. Documentation / Bulletins / Technical Bulletins)

→ Only SFP modules recommended by KEYMILE can guarantee the specified functionality of the NUSA1 unit.

4.3.2 SFP Module Mounting

A plugged SFP module is secured in the SFP cage by a locking mechanism. To remove the SFP module from the SFP cage this locking must be released. There are different, non standardised, methods to release this locking mechanism:

- with a bail (generally used on optical SFP modules), or
- with a unlocking actuator (generally used on electrical SFP modules).

No tool or equipment is required to install or remove an SFP module.

4.3.2.1 SFP module with bail actuator

To insert SFP modules, the bail latch should be in the locked position. The module is oriented so that the bail is on the right side of the SFP. The module is pushed into the SFP cage carefully until a clicking sound indicates that the module is locked.

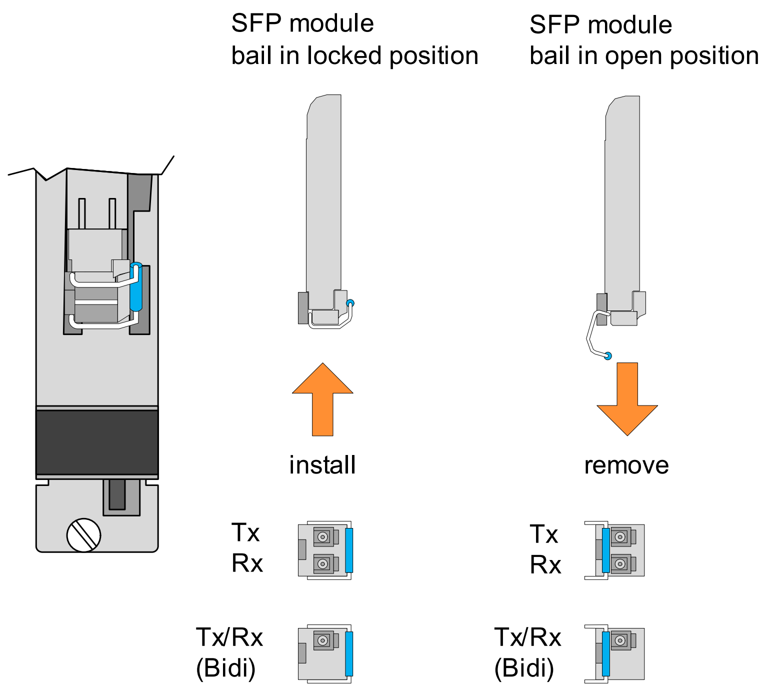


Figure 8: SFP module handling

After disconnection of the optical cable, SFP modules can be removed from the SFP cage by using the metal bail latch located on the right side of the SFP module. Pull on the bail to unlock and remove the SFP module.

Please note:

To protect optics, dust covers should always be installed when cables are not connected.

Please note:

Unplugged SFP modules should be stored in an ESD safe environment.

4.3.2.2 SFP module with unlocking actuator

To insert SFP modules, the module is oriented so that the unlocking actuator is on the left side of the SFP. The module is pushed into the SFP cage carefully until a clicking sound indicates that the module is locked.

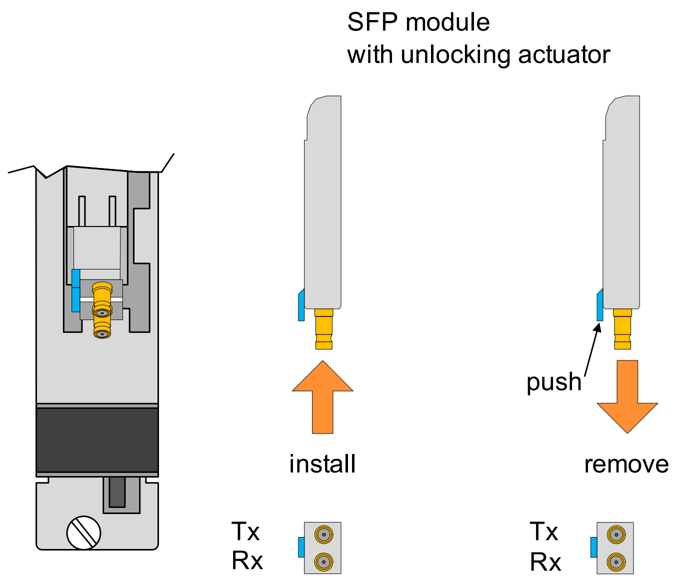


Figure 9: SFP module handling

The SFP modules can be removed from the SFP cage by pushing the unlocking actuator and then pulling on the module itself or the electrical cables to remove the SFP module.

Please note:

Unplugged SFP modules should be stored in an ESD safe environment.

4.4 Compatibility

4.4.1 XMC20 Units

NUSA1 is compatible with any other XMC20 service unit with an ESW release of the current XMC20 system release. Please refer to [012] Release Note “XMC20 System Release R6B”.

4.4.2 Previous ESW Revisions

The NUSA1 unit with the ESW release nusa1_r3b is compatible to the previous ESW release available for the XMC20 system release R6A.

When upgrading to the ESW release nusa1_r3b all configuration parameters are inherited from an existing configuration. New parameters get their default values.

4.5 Connections and Cables

4.5.1 Front Connectors of the NUSA1 Unit

The NUSA1 has four SDH interfaces on the unit front, designated from bottom up with port-1 to port-4. The optical or electrical interface connectors are provided by the pluggable SFP modules.

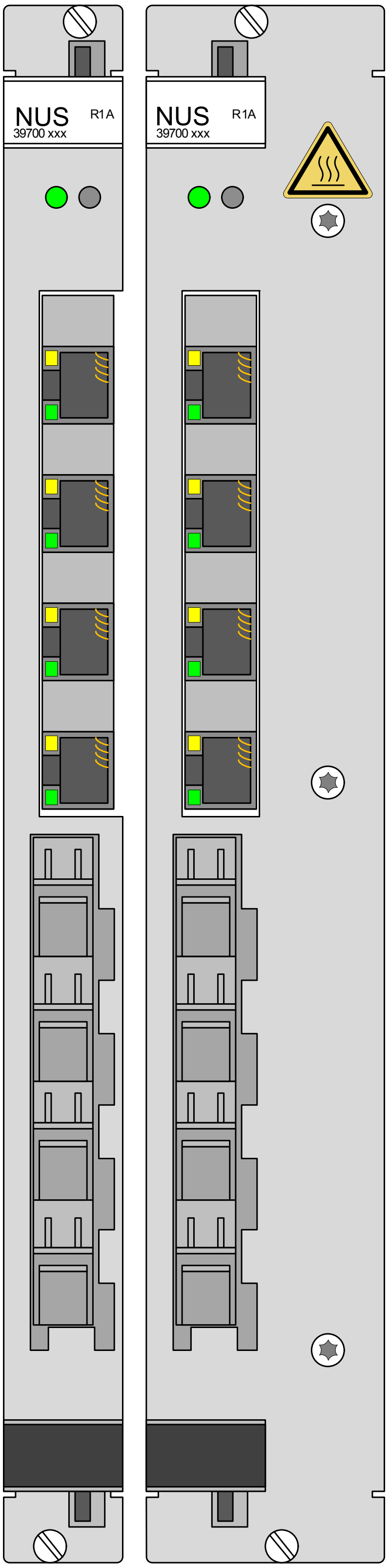
The optical SDH interfaces are equipped with industry standard duplex LC connectors. The bidirectional (bidi) SFP modules have a simplex LC connector.

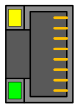
The electrical SDH interfaces are equipped with industry standard DIN 1.0/ 2.3 (push-pull self latching/coupling) connectors for coaxial cables.

The four Ethernet interfaces are designated from bottom up with port-5 to port-8.

The Ethernet interfaces are equipped with RJ-45 connectors. The interface layout is per default according to the MDI-X layout, but implements automatic crossover functionality (MDI/MDI-X).

The pin and port assignment of the eight front panel connectors is shown in the figure below.





Pin	10BASE-T		100BASE-TX		1000BASE-T	
	MDI	MDI-X	MDI	MDI-X	MDI	MDI-X
1	TD+	RD+	Transmit +	Receive +	BI_DA+	BI_DB+
2	TD-	RD-	Transmit -	Receive -	BI_DA-	BI_DB-
3	RD+	TD+	Receive +	Transmit +	BI_DB+	BI_DA+
4					BI_DC+	BI_DD+
5					BI_DC-	BI_DD-
6	RD-	TD-	Receive -	Transmit -	BI_DB-	BI_DA-
7					BI_DD+	BI_DC+
8					BI_DD-	BI_DC-

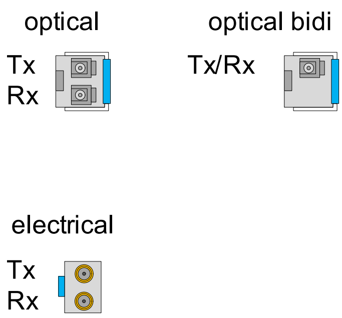


Figure 10: NUSA1 (left) and NUSA1-F (right) front panel and interface connectors

The ⚠ symbol indicates the risk of the hot NUSA1-F front cover.

Each Ethernet interface provides two LEDs indicating the link activity state and the link state:

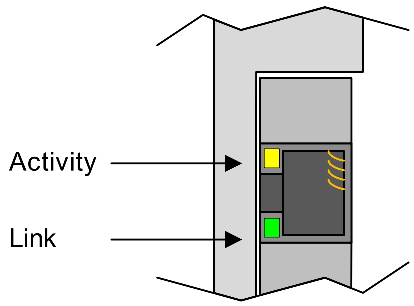


Figure 11: Ethernet link LEDs on the NUSA1 unit

The activity LED has the following states:

- Yellow blinking: Traffic activity.
- Dark: No traffic.

The link LED has the following states:

- Green: 10/100/1000 Mbit/s link up.
- Dark: Link down.

4.5.2 Optical SDH Interface Cables

The optical SDH interfaces (SFP modules) are equipped with industry standard duplex LC connectors (bidi SFP modules: simplex LC connector). Connection to other types of connectors as e.g. LC, SC or FC-PC is possible with converter cables (optical jumpers) or via an optical distribution frame.

The NUSA1 unit performs as specified with optical single mode fibres that conform to the ITU-T G.652 recommendation (Characteristics of a single mode optical fibre and cable).

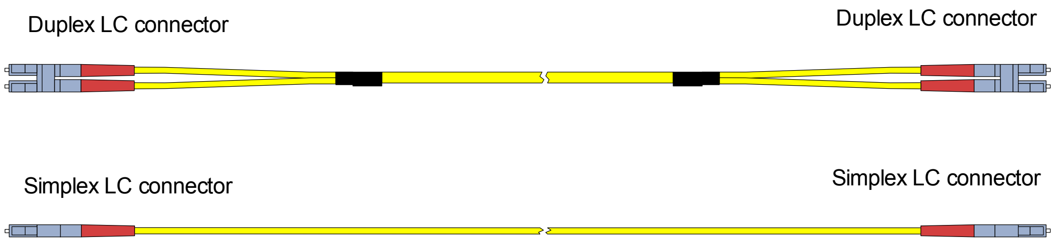


Figure 12: NUSA1 duplex and simplex LC to LC cable

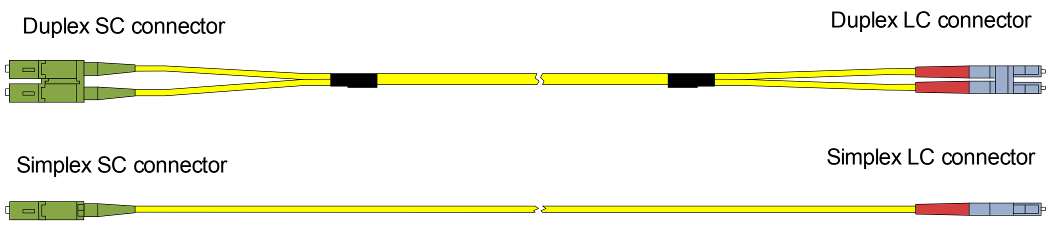


Figure 13: NUSA1 duplex and simplex LC to SC adapter cable

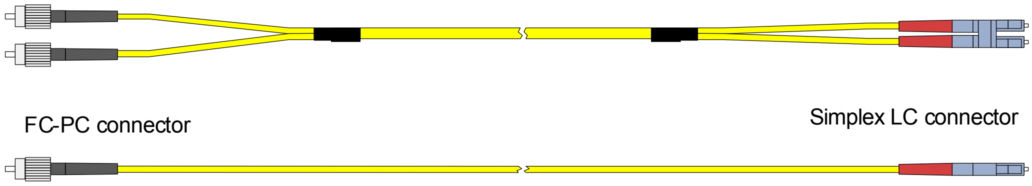


Figure 14: NUSA1 duplex and simplex LC to FC-PC adapter cable

Please note:

The above cables can be ordered directly from KEYMILE.

For details on available optical cables, please refer to [506] User Manual "XMC20 cables".

4.5.3 Electrical SDH Interface Cable, DIN to open End

The electrical SDH interfaces (SFP modules) are equipped with industry standard DIN 1.0/2.3 (push-pull self latching/coupling) connectors for 75 Ω coaxial cables.

This cable provides input and outputs to/ from the NUSA1 unit with SFP modules for STM-1 G.703 / 75 Ω circuits. The other end of this cable is not terminated.

Please note:

The electrical interface requires two cables.

Please note:

The above cable can be ordered directly from KEYMILE.

For details on available coaxial cables, please refer to [506] User Manual "XMC20 cables".

4.5.4 Electrical SDH Interface Cable, DIN to BNC

The electrical SDH interfaces (SFP modules) are equipped with industry standard DIN 1.0/2.3 (push-pull self latching/coupling) connectors for 75 Ω coaxial cables.

This cable provides input and outputs to/ from the NUSA1 unit with SFP modules for STM-1 G.703 / 75 Ω circuits. The other end of this cable is terminated with a male BNC connector.

Please note:

The electrical interface requires two cables.

Please note:

The above cable can be ordered directly from KEYMILE.

For details on available coaxial cables, please refer to [506] User Manual "XMC20 cables".

4.5.5 Ethernet Interface Cables

The Ethernet interfaces are equipped with RJ-45 connectors. The interface layout is per default according to the MDI-X layout, but implements automatic crossover functionality (MDI/MDI-X), i.e. it can adapt itself automatically to work with a host or a switch. The interface therefore works with crossover and straight cables.

The following media types are supported:

Table 17: Ethernet media types

IEEE Standard	Distance	Media Type
10BASE-T	100m	Category 3 UTP or better
100BASE-TX	100m	Category 5 UTP or better
1000BASE-T	100m	Category 5e UTP or better

Please note:

The latching clips of the connectors must be positioned to the left to insert the connector correctly.

Please note:

The Ethernet cables can be ordered directly from KEYMILE.

For details on available Ethernet cables, please refer to [506] User Manual “XMC20 cables”.

4.5.6 Fixing the Cables to the Cable Tray

The optical or electrical cables must be attached to the cable tray of the XMC25 or the corresponding device of the XMC23.

The open cable shields (electrical cables only) must be in contact with the XMC20 grounding bar.

The figure below shows the cable/cable tray assembly of the XMC25. For additional information refer to [301] User Guide “XMC25 Installation”.

With the XMC23 the cable tray functionality is implemented differently and depends on the type of installation (rack-, wall-mounted). For more information on fixing the cables with the XMC23 refer to [310] User Guide “XMC23 Installation”.

The 19-inch adapter of the XMC22 provides no cable tray. For more information on fixing the cables with the XMC22 refer to [322] User Guide “XMC22 Installation”.

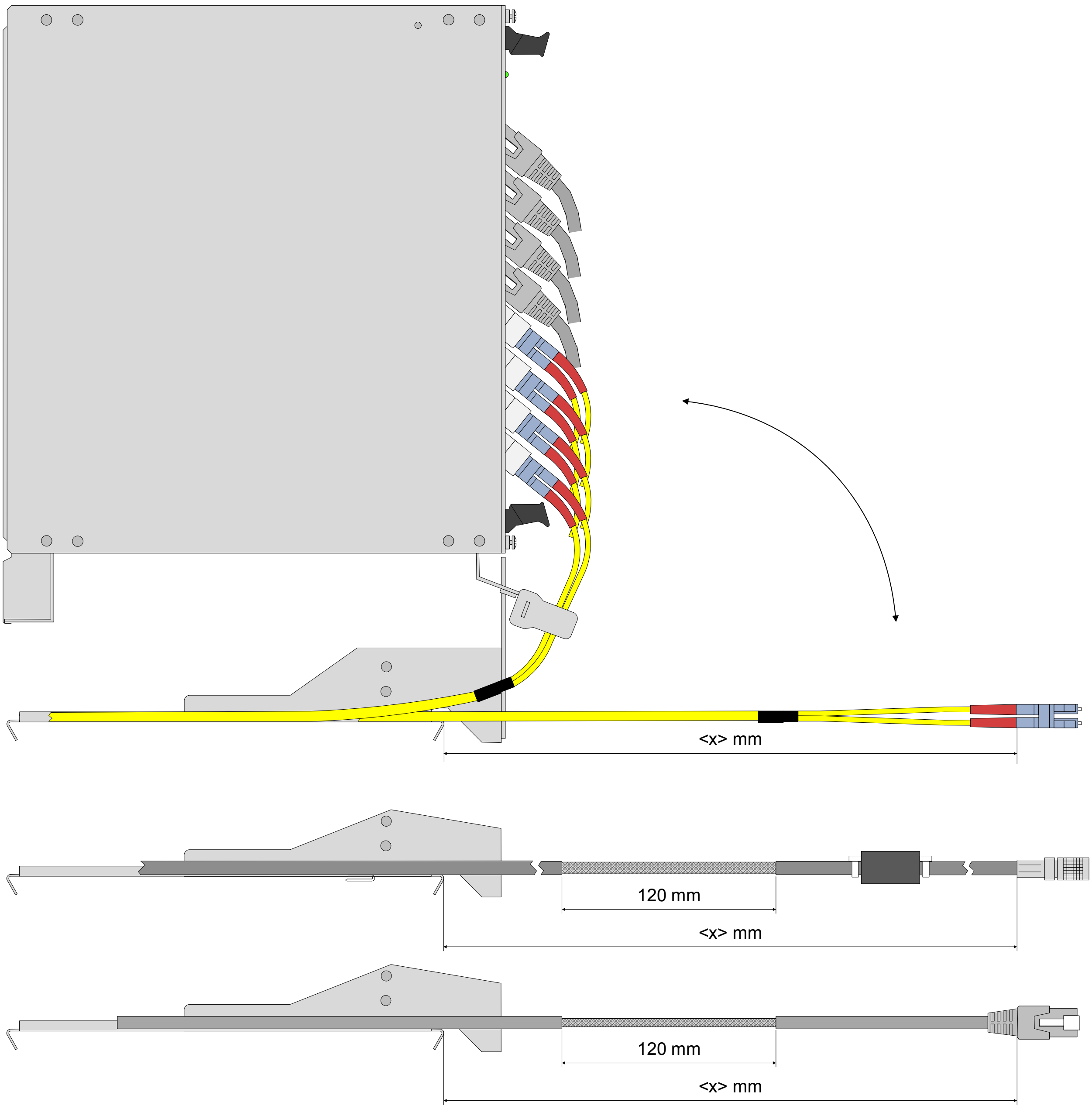


Figure 15: Side view of the XMC25 cable tray and cables

The open cable length <x> between the cable fixing point on the cable tray and the connector depends on the connected interface.

Please note:

The cable route on the cable tray should follow approximately the projection of the unit slot on the cable tray.

Please note:

Do not exceed the specified bending radius or squeeze the optical fibres when fixing the fibres to the cable tray.
Stressing the fibres in excess to the specified parameters or squeezing the fibres can permanently degrade the performance of the optical fibres.

5 Functional Description

This section gives the detailed functional description of the NUSA1 unit as an SDH terminal multiplexer and add/drop multiplexer in the XMC20 subrack.

5.1 Applications

The main applications with the NUSA1 unit are
- NUSA1 as SDH terminal multiplexer with SDH, PDH and Ethernet tributaries.
- NUSA1 as SDH add/drop multiplexer with SDH, PDH and Ethernet tributaries.

This section presents some application examples implemented with the NUSA1 unit.

5.1.1 SDH Terminal Multiplexer unprotected

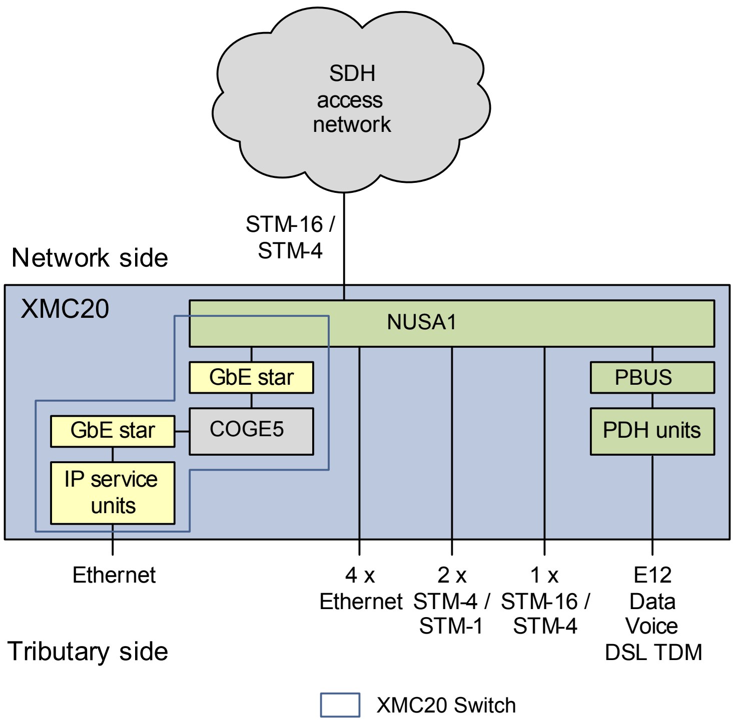


Figure 16: SDH terminal multiplexer, unprotected

An SDH terminal multiplexer with an unprotected STM-16 or STM-4 uplink can be implemented with one NUSA1 unit.

The NUSA1 unit offers three SDH tributary ports, one STM-16 or STM-4 and two STM-4 or STM-1.

The Ethernet traffic is connected to the NUSA1 unit via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.4 Ethernet over an SDH Terminal Multiplexer (on page 46).

5.1.2 SDH Terminal Multiplexer with MSP Protection

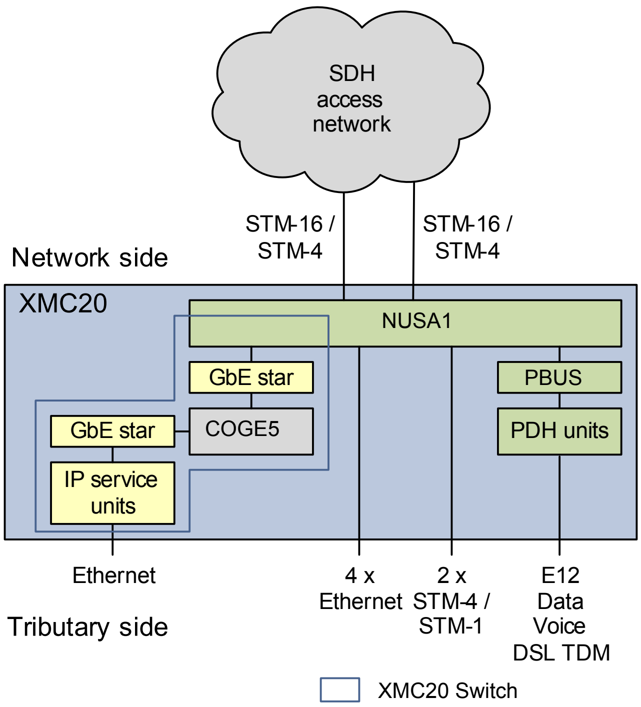


Figure 17: SDH terminal multiplexer, MSP protected

An SDH terminal multiplexer with MSP protected STM-16 or STM-4 uplinks can be implemented with one NUSA1 unit.

The NUSA1 unit offers two STM-4 or STM-1 tributary ports. These ports can be handled

- as two independent tributary ports or
- as subtending ring ports or
- as one MSP protected STM-4 or STM-1 tributary.

The Ethernet traffic is connected to the NUSA1 unit via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.4 Ethernet over an SDH Terminal Multiplexer (on page 46).

5.1.3 SDH Terminal Multiplexer with MSP and Equipment Protection

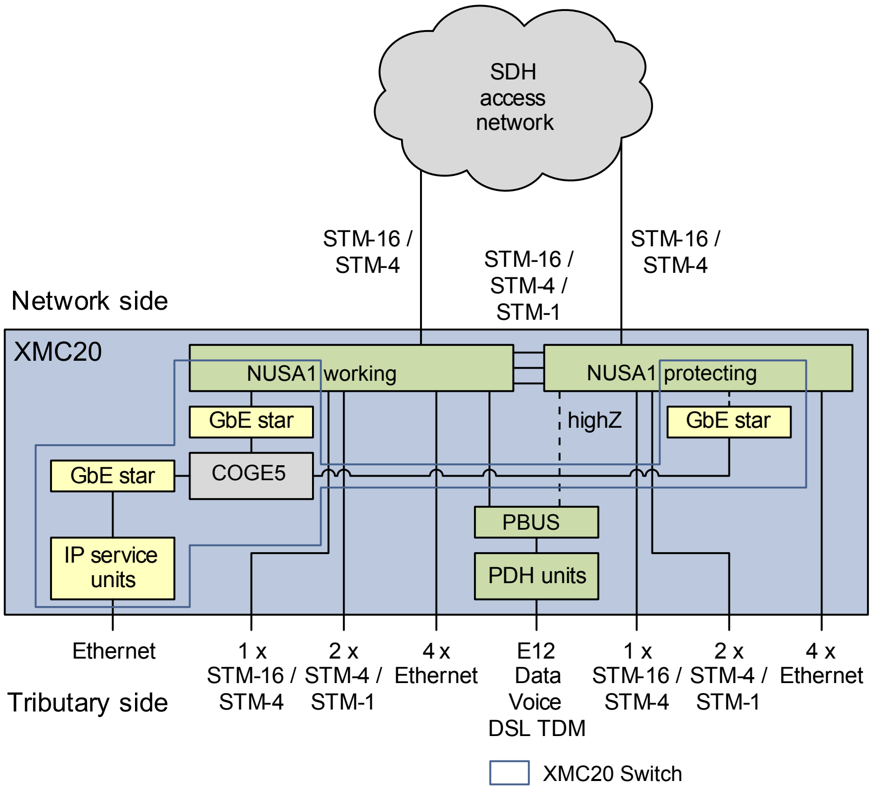


Figure 18: SDH terminal multiplexer, MSP protected

An SDH terminal multiplexer with MSP protected STM-16 or STM-4 uplinks can be implemented with two NUSA1 units, operating as equipment protection pair. Both NUSA1 units have one SDH port active towards the network side. The traffic processing, i.e. SDH termination, access to the PBUS and the access to the Ethernet front interfaces takes place on the working NUSA1 unit.

Please note:

MSP over two NUSA1 units not operating as equipment protection pair is not supported.

The other SDH ports on both NUSA1 units remain operational, i.e. two STM-16 or STM-4 ports and four STM-4 or STM-1 ports. These ports can be handled

- as six independent tributary ports or
- as subtending ring ports or
- as MSP protected STM-16 or STM-4 or STM-1 tributaries.

The Ethernet traffic is connected to the working and protecting NUSA1 units via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.4 Ethernet over an SDH Terminal Multiplexer (on page 46).

5.1.4 Ethernet over an SDH Terminal Multiplexer

5.1.4.1 Ethernet over SDH, unswitched transport mode

In the unswitched transport mode the Ethernet traffic from an Ethernet port on the NUSA1 unit is transported in SDH networks using the EoS (Ethernet over SDH) approach providing point to point Ethernet connections. Ethernet traffic is transported in virtually concatenated VC-4, VC-3 or VC-12.

The Ethernet traffic from an Ethernet device is connected to the NUSA1 unit via cables connecting the Ethernet front interfaces using the unswitched mode.

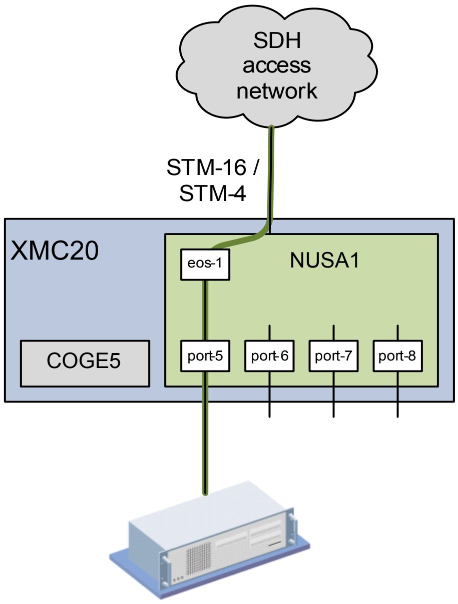


Figure 19: EoS without NUSA1 EQP, unswitched mode

When using NUSA1 equipment protection, the Ethernet traffic from an Ethernet device is connected to both NUSA1 units via cables. This requires two Ethernet ports on the Ethernet device. Alternatively an Ethernet switch can be used to connect both NUSA1 ports to one Ethernet front port on the Ethernet device.

The Ethernet device Ethernet ports may have RSTP disabled since the EoS transport on a standby NUSA1 unit is not active.

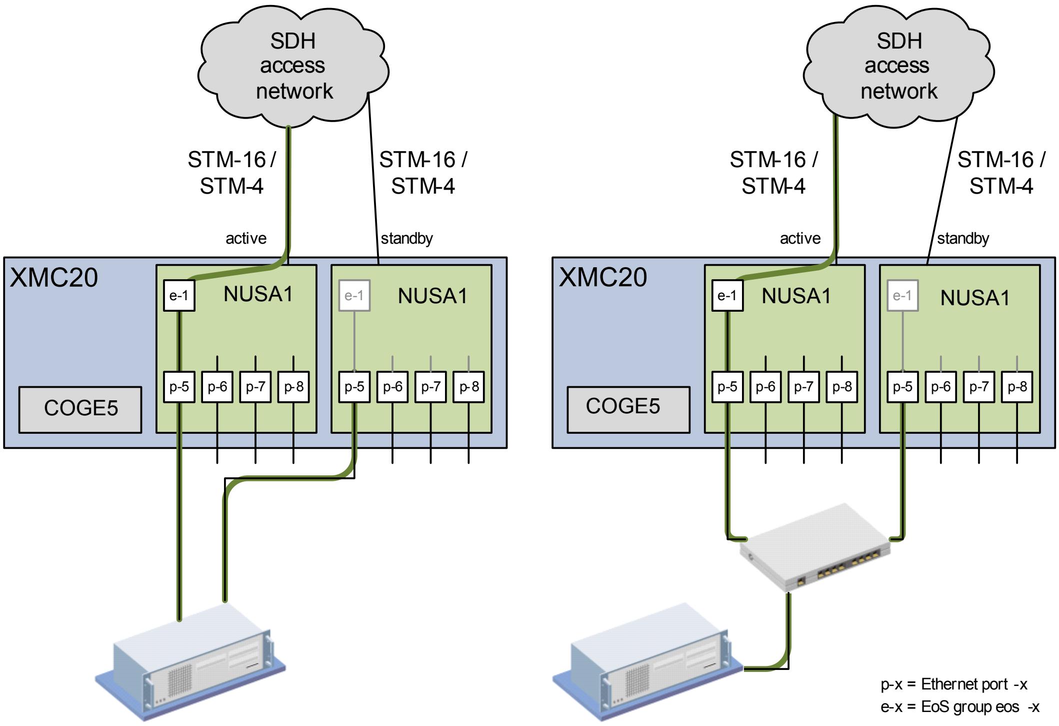


Figure 20: EoS with NUSA1 EQP, unswitched mode

5.1.4.2 Ethernet over SDH, switched transport mode

The Ethernet over SDH, switched transport mode, makes use of the VLAN Bridge function of the XMC20.

In the switched transport mode there are no dedicated EoS ports reserved for the NUSA1 front ports. All EoS ports are used as external ports of the XMC20 Switch, i.e. the Ethernet switch device on the NUSA1 unit participates in the XMC20 Switch.

The Ethernet traffic from any XMC20 Ethernet port participating in the XMC20 Switch is connected to the NUSA1 unit via the GbE star.

When using COGE5 equipment protection, also the Ethernet switch device on the redundant COGE5 is part of the XMC20 Switch. The COGE5 redundancy is handled by the network element control processes. The EoS application requires no redundancy specific configuration.

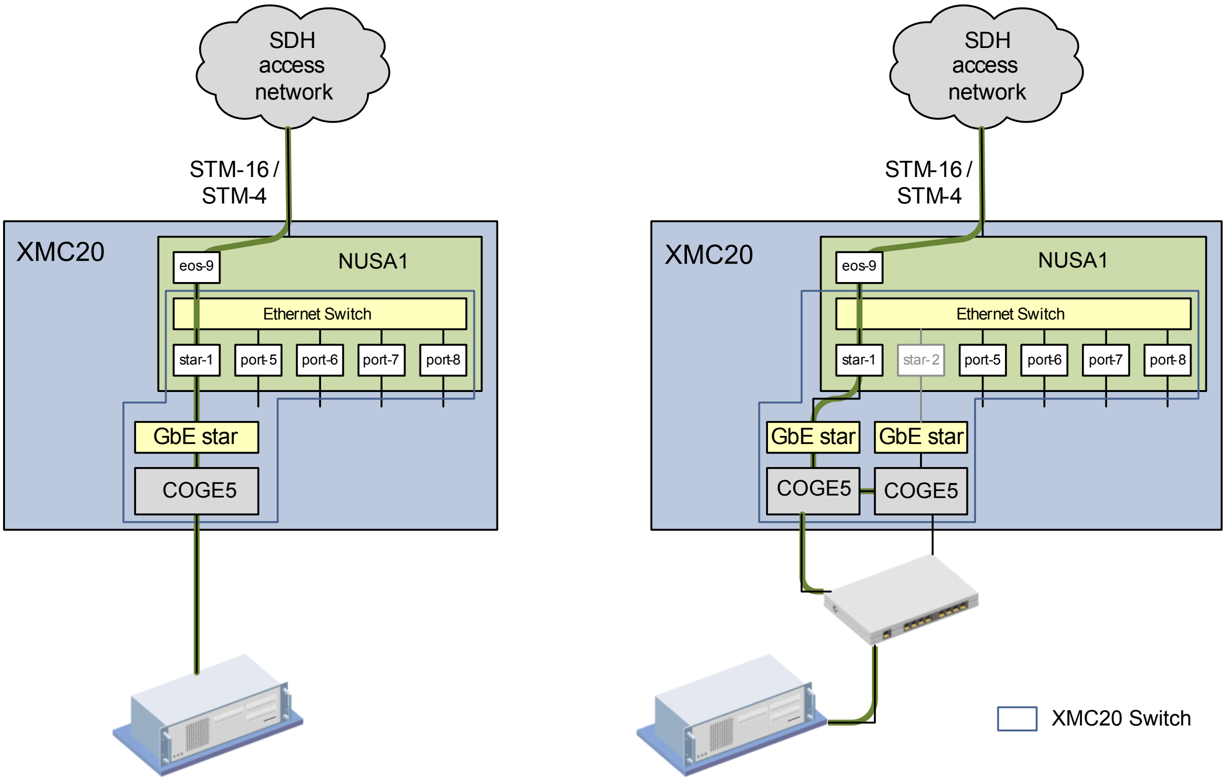


Figure 21: EoS, switched mode

When using NUSA1 equipment protection, also the redundant NUSA1 is part of the XMC20 Switch, the Ethernet front ports on the active and on the standby NUSA1 unit are active. The EoS transport is only operational on the active NUSA1 unit and disabled on the standby NUSA1 unit.

Please note:

The two EoS ports on the working and the protecting NUSA1 units are both attached to the XMC20 Switch. One EoS port is active, the other is standby, but both EoS ports are available as bridge ports in the ECST “Switching” view.

→ The bridge port configuration (port mode, PVID, VLANs, …) must be configured identically for both ports.

Please note:

When connecting an Ethernet device via two XMC20 Switch ports as shown in Figure 21 "EoS, switched mode" and Figure 22 "EoS with NUSA1 EQP, switched mode" on the right side, “meshed” VPLS pseudo wires must be configured to avoid a packet loop.

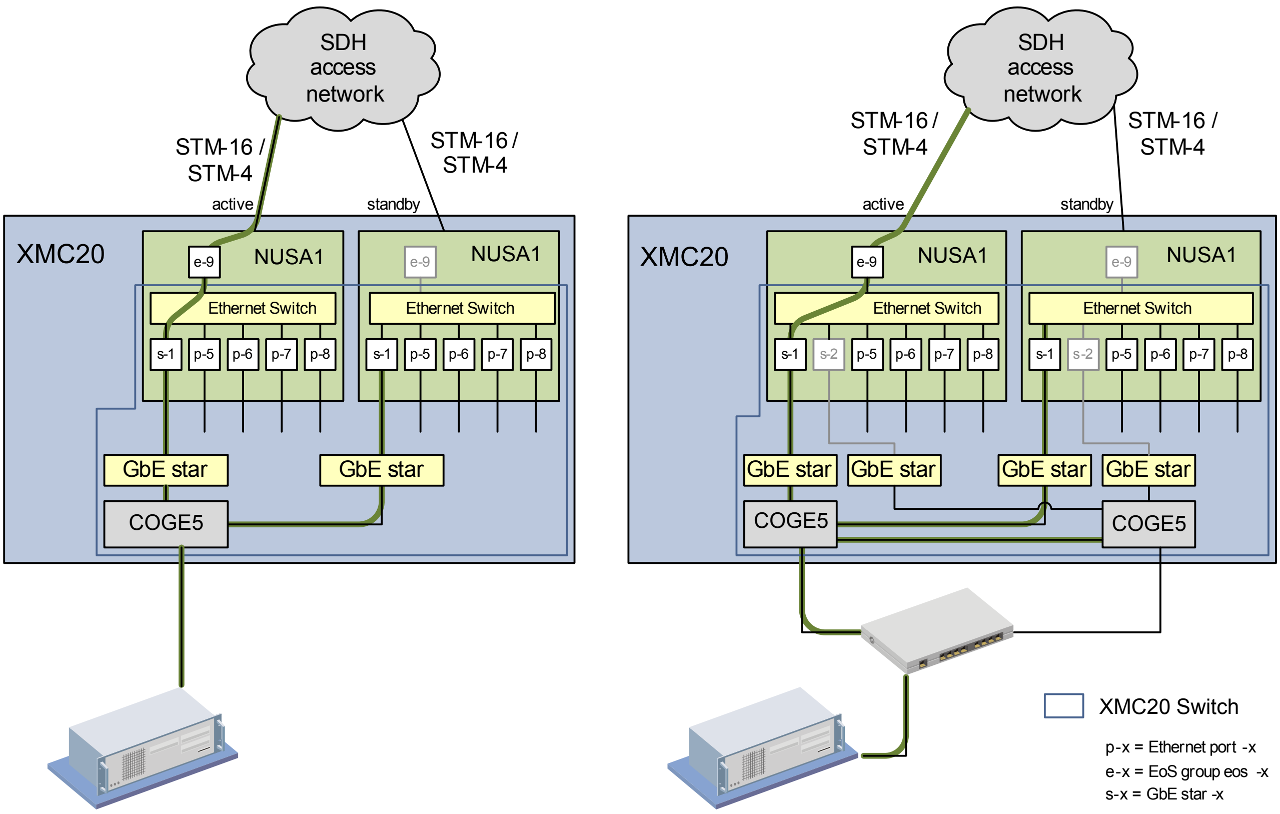


Figure 22: EoS with NUSA1 EQP, switched mode

5.1.5 SDH add/drop Multiplexer

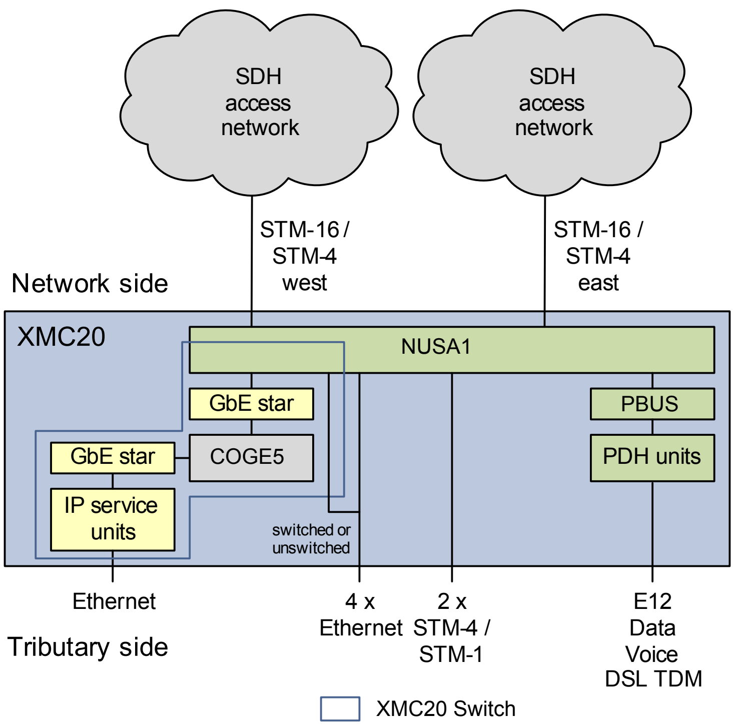


Figure 23: SDH add/drop multiplexer, unprotected

An SDH add/drop multiplexer with unprotected STM-16 or STM-4 uplinks can be implemented with one NUSA1 unit.

The NUSA1 unit offers two STM-4 or STM-1 tributary ports. These ports can be handled

- as two independent tributary ports or
- as subtending ring ports or
- as one MSP protected STM-4 or STM-1 tributary.

This application offers subnetwork connection protection (SNCP) on the VC-4, VC-3 and VC-12 layers.

This application offers also subnetwork connection protection (SNCP) with bidirectional switching type for the VC-12 signals terminated to the PBUS.

The Ethernet traffic is connected to the NUSA1 unit via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.9 Ethernet over an SDH add/drop Multiplexer (on page 53).

5.1.6 SDH add/drop Multiplexer with MSP Protection

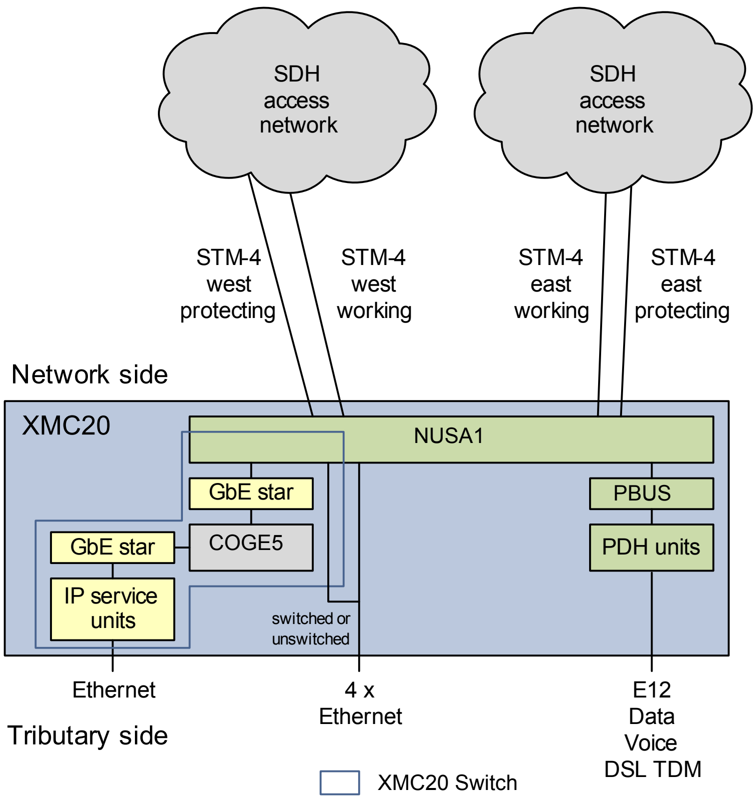


Figure 24: SDH add/drop multiplexer, MSP protected

An SDH add/drop multiplexer with MSP protected STM-4 uplinks can be implemented with one NUSA1 unit. STM-16 and STM-1 interfaces cannot be supported in this scenario.

The NUSA1 unit supports no SDH tributary ports.

This application offers subnetwork connection protection (SNCP) on the VC-4, VC-3 and VC-12 layers.

This application offers also subnetwork connection protection (SNCP) with bidirectional switching type for the VC-12 signals terminated to the PBUS.

The Ethernet traffic is connected to the NUSA1 unit via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.9 Ethernet over an SDH add/drop Multiplexer (on page 53).

5.1.7 SDH add/drop Multiplexer with Equipment Protection

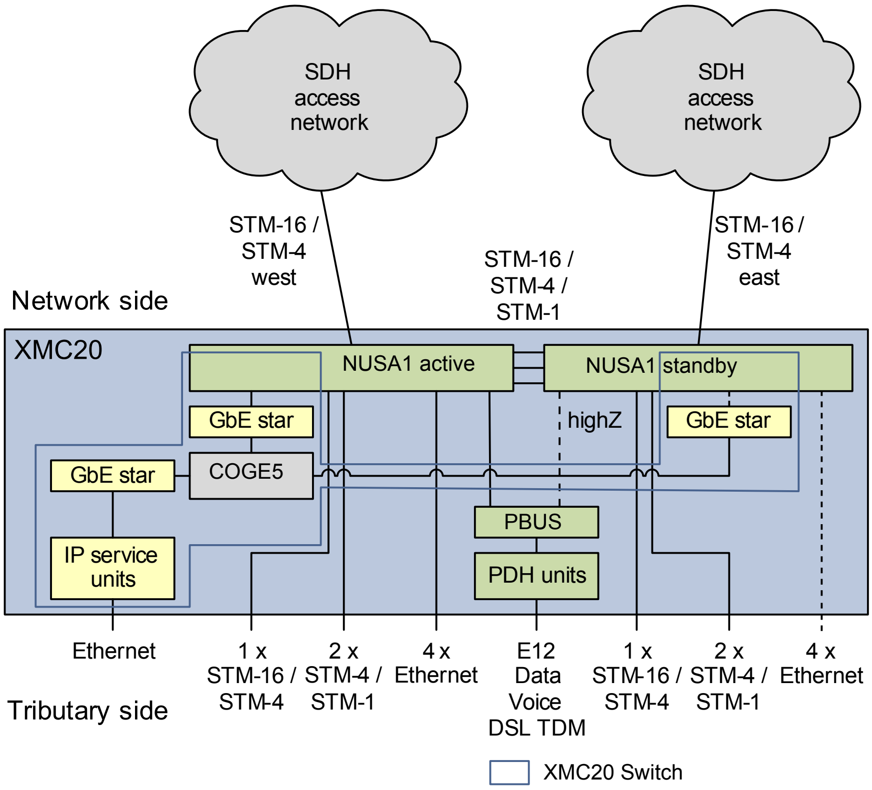


Figure 25: SDH add/drop multiplexer, EQP protected

An SDH add/drop multiplexer with equipment protection (EQP) and unprotected STM-16 or STM-4 uplinks can be implemented with two NUSA1 units, operating as equipment protection pair. Both NUSA1 units have one SDH port active towards the network side. The traffic processing, i.e. SDH termination, access to the PBUS and the access to the Ethernet front interfaces takes place on the working NUSA1 unit.

The other SDH ports on both NUSA1 units remain operational, i.e. two STM-16 or STM-4 ports and four STM-4 or STM-1 ports. These ports can be handled

- as six independent tributary ports or
- as subtending ring ports or
- as MSP protected STM-16 or STM-4 or STM-1 tributaries.

Please note:

MSP over two NUSA1 units not operating as equipment protection pair is not supported.

The Ethernet traffic is connected to the working and protecting NUSA1 units via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.9 Ethernet over an SDH add/drop Multiplexer (on page 53).

5.1.8 SDH add/drop Multiplexer with MSP and Equipment Protection

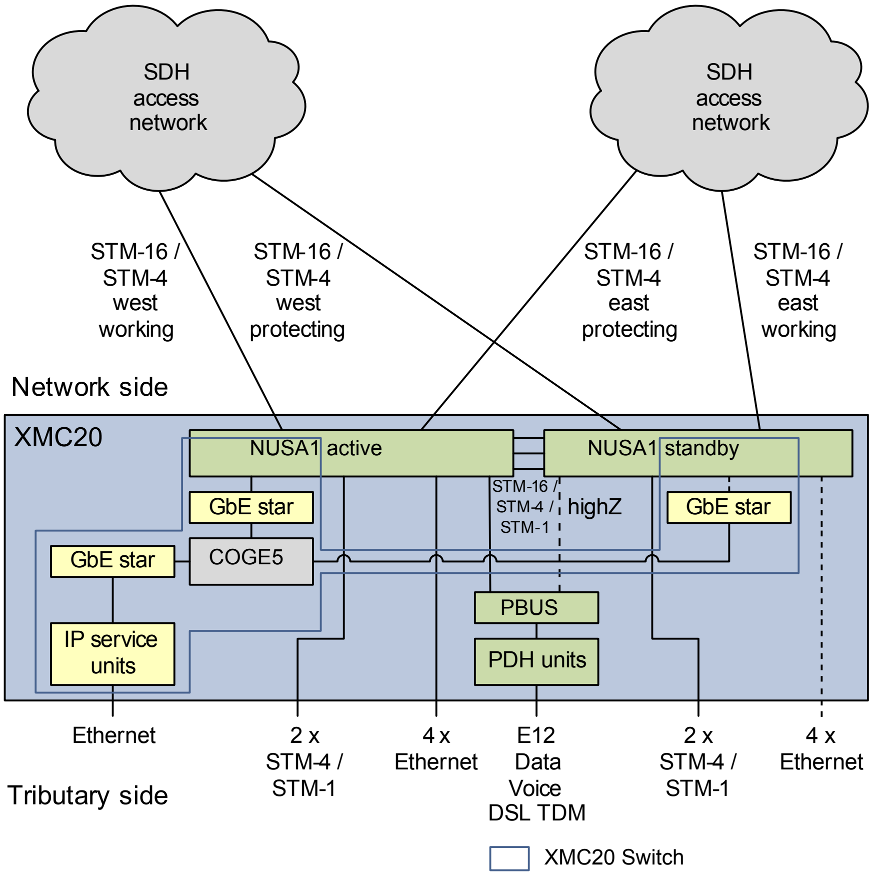


Figure 26: SDH add/drop multiplexer, EQP protected

An SDH add/drop multiplexer with equipment protection (EQP) and multiplex section protected STM-16 or STM-4 uplinks can be implemented with two NUSA1 units, operating as equipment protection pair. Both NUSA1 units have two SDH ports active towards the network side. The traffic processing, i.e. SDH termination, access to the PBUS and the access to the Ethernet front interfaces takes place on the working NUSA1 unit.

The other SDH ports on both NUSA1 units remain operational, i.e. four STM-4 or STM-1 ports. These ports can be handled

- as four independent tributary ports or
- as subtending ring ports or
- as MSP protected STM-4 or STM-1 tributaries.

Please note:

MSP over two NUSA1 units not operating as equipment protection pair is not supported.

The Ethernet traffic is connected to the working and protecting NUSA1 units via cables connecting the front interfaces, or via the GbE star as part of the XMC20 Switch. Refer also to section 5.1.9 Ethernet over an SDH add/drop Multiplexer (on page 53).

5.1.9 Ethernet over an SDH add/drop Multiplexer

5.1.9.1 Ethernet over SDH, unswitched transport mode

In the unswitched transport mode the Ethernet ports on the NUSA1 unit provide point to point Ethernet connections.

The Ethernet traffic from any Ethernet device uses two EoS ports, one for the west and one for the east direction. The Ethernet traffic is connected to the NUSA1 unit via cables connecting the Ethernet front interfaces using the unswitched mode.

The Ethernet device Ethernet ports must have RSTP enabled to avoid a packet loop.

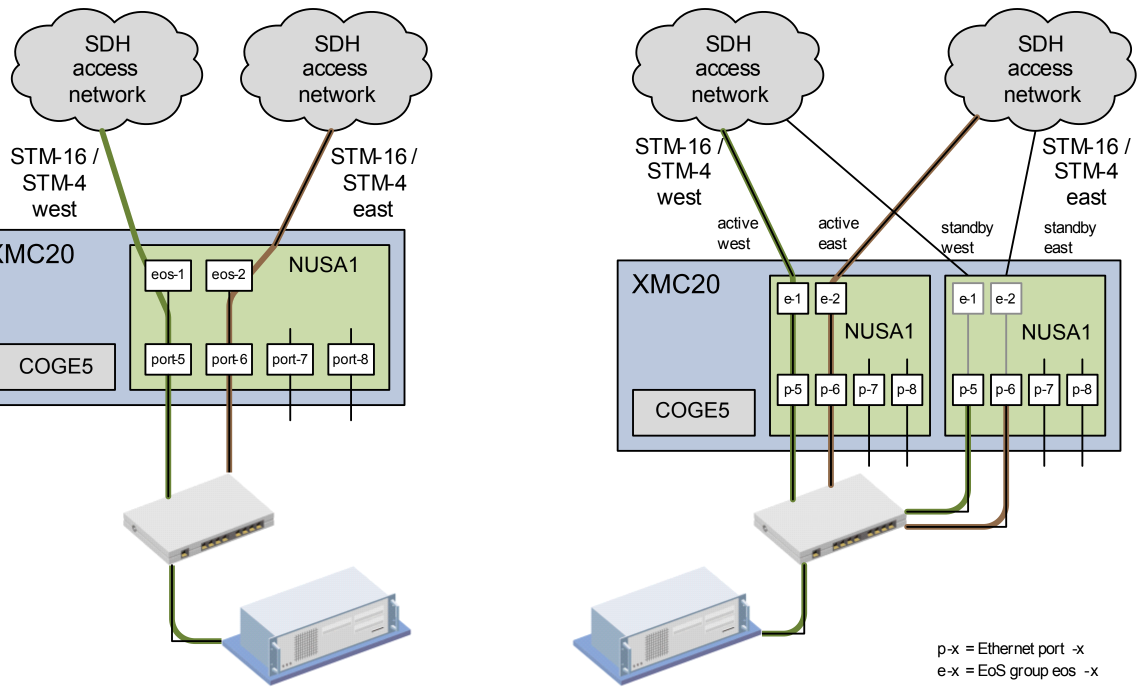


Figure 27: EoS with and without NUSA1 EQP, unswitched mode

5.1.10 MPLS-TP Transport with VPWS

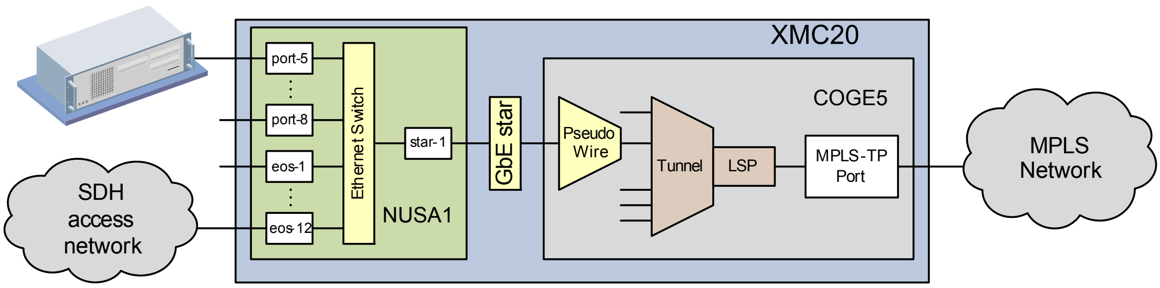


Figure 28: MPLS-TP Transport function with NUSA1 and COGE5

With the MPLS-TP Transport function of the XMC20 the NUSA1 Ethernet front ports and the EoS ports can be used as PWAC ports of a Virtual Private Wire Service (VPWS).

In the switched mode of the Ethernet front ports the EoS ports eos-1 to eos-12 are available.

In the unswitched mode of the Ethernet front ports the EoS ports eos-5 to eos-12 are available.

EoS traffic can be SNC protected on the VC-4, VC-3 and VC-12 layers.

Please note:

A NUSA1 Ethernet front port or EoS port used for the MPLS-TP VPWS Transport function is no longer available for the VLAN Bridge function.

For detailed information about the MPLS-TP application with XMC20 please refer to [358] User Manual “MPLS-TP”.

5.1.11 MPLS-TP Transport with VPLS

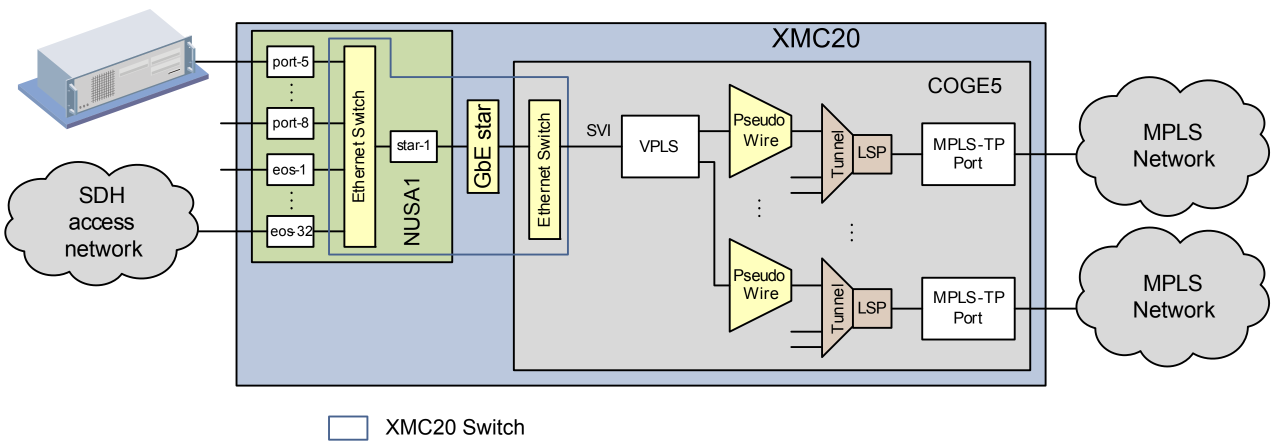


Figure 29: MPLS-TP VPLS Transport function with NUSA1 and COGE5

With the MPLS-TP Transport function of the XMC20 the NUSA1 Ethernet front ports and the EoS ports can be used as CVP ports of a Virtual Private LAN Service (VPLS). The CVP ports of the NUSA1 unit and the SVI (Switch Virtual Interface) of the VPLS are attached to the XMC20 Switch, using the VLAN Bridge application.

In the switched mode of the Ethernet front ports the EoS ports eos-1 to eos-32 are available.

In the unswitched mode of the Ethernet front ports the EoS ports eos-5 to eos-32 are available.

EoS traffic can be SNC protected on the VC-4, VC-3 and VC-12 layers.

For detailed information about the MPLS-TP application with XMC20 please refer to [358] User Manual “MPLS-TP”.

5.2 SDH Multiplexing

5.2.1 SDH Multiplexing in ITU-T and ETSI Standards

The figure below shows the STM-16, STM-4 and STM-1 multiplexing structure according to the ITU G.707 recommendation and the ETSI EN 300 147 standard.

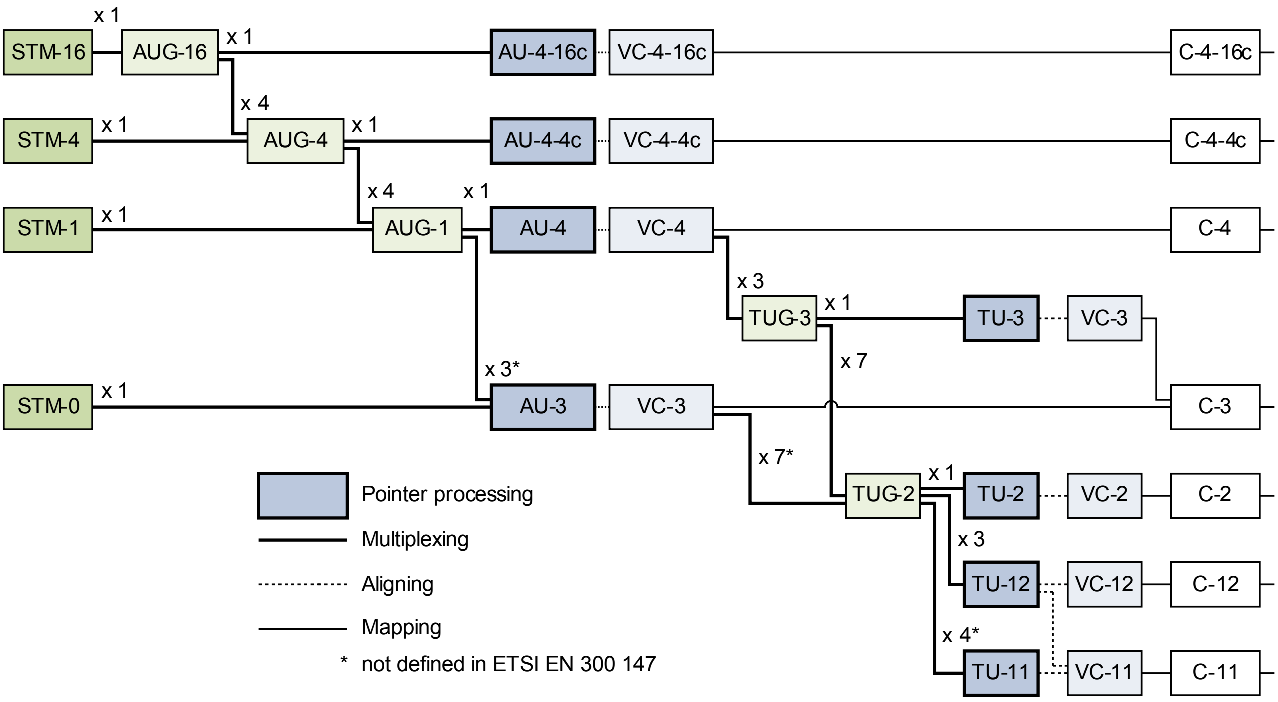


Figure 30: Multiplexing structure according to ITU-T G.707 and ETSI EN 300 147

For the definition of terms, refer to ITU-T G.707.

5.2.2 SDH Multiplexing in XMC20

The multiplexing structure implemented in NUSA1 and supported in XMC20 is a subset of the complete multiplexing structure defined in ITU-T G.707.

NUSA1 provides the multiplexing functions for VC-12, VC-3 and VC-4 as depicted in the figure below.

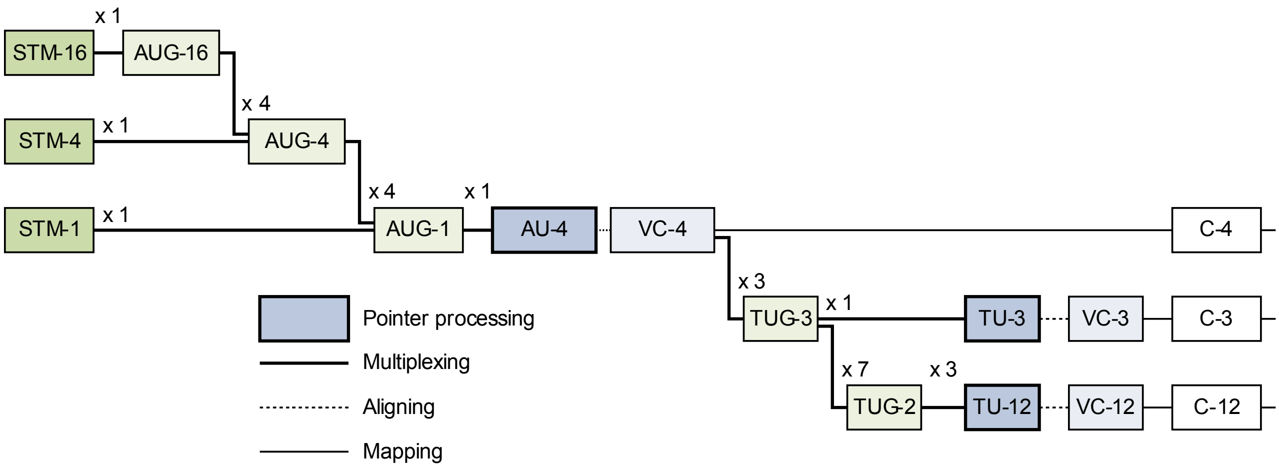


Figure 31: Multiplexing structure supported in NUSA1

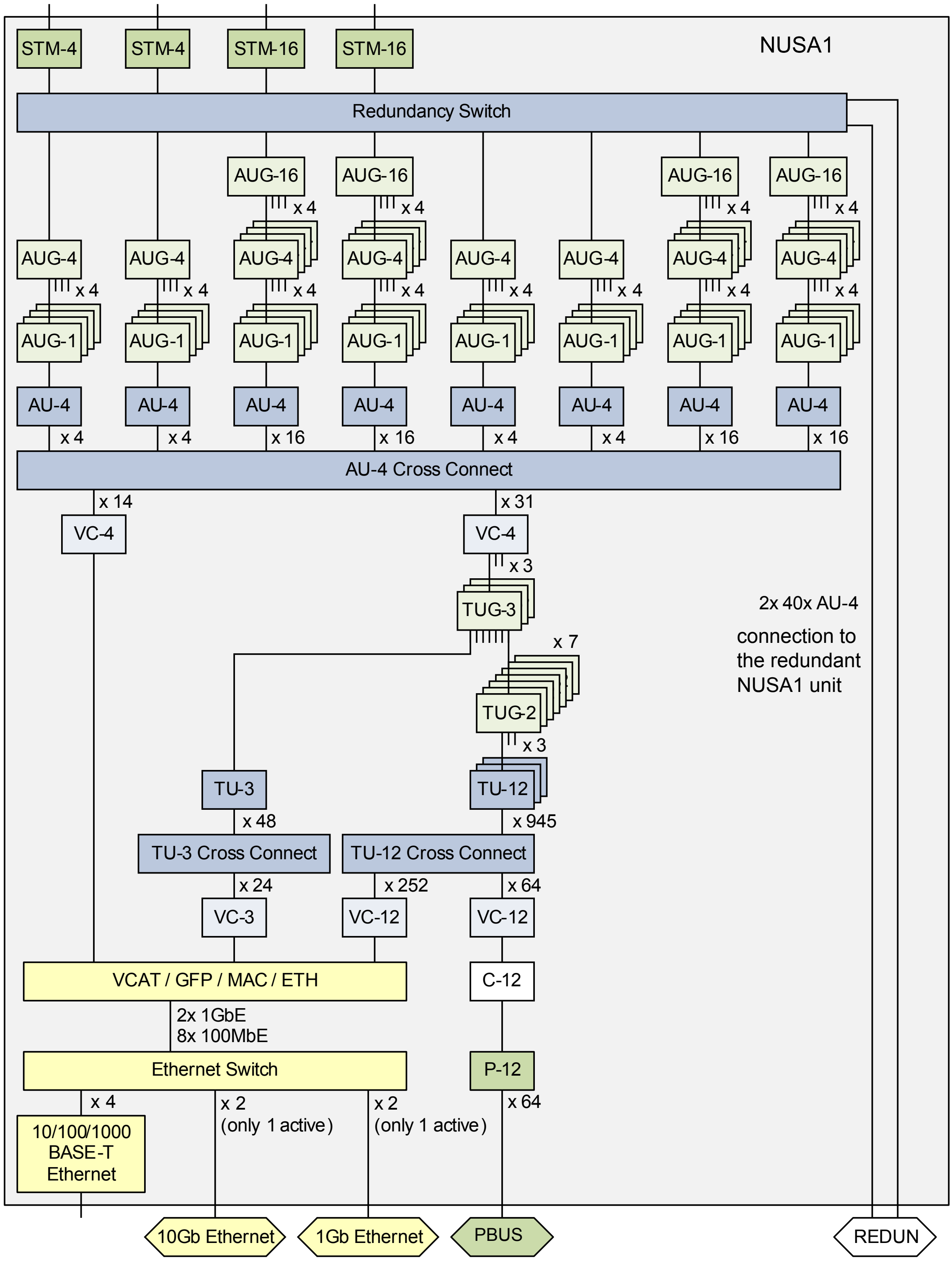


Figure 32: SDH multiplexing with NUSA1

The functional blocks implemented in the NUSA1 unit are shown in the Figure 32 "SDH multiplexing with NUSA1". The figure shows also the numbers of available functional blocks, e.g. the number of TU-12 processing blocks is 15 (VC-4) x 3 (TUG-3) x 7 (TUG-2) x 3 (TU-12) = 945.

The two 40x AU-4 signals at the redundancy switch connect two NUSA1 units, operating as equipment protection pair.

The STM-16, STM-4 and STM-1 output signals are frequency locked to the SETS (Synchronous Equipment Timing Source) timing.

5.3 SDH Layers and Functions

5.3.1 PS Layer

The optical section (OS) layer or electrical section (ES) layer of the NUSA1 unit are handled in a common layer called physical section (PS). The physical section provides the following functions:

- Termination of the optical or electrical section. The optical section can be STM-16, STM-4 or STM-1. The electrical section is STM-1.
  - Optical/electrical converter
  - Receive signal regeneration
  - Clock and data recovery
  - STM-16, STM-4 or STM-1 frame alignment
- Control of laser shutdown and restart (OS only)
  - Automatic laser shutdown (ALS) automatically switches off the optical transmitter if there is a broken or missing cable in the section.
  - The automatic laser restart (ALR) function automatically restarts the laser after an automatic shutdown. After ALS the interface monitors the input for an appropriate laser signal and restarts its laser if the received signal remains stable for a defined period of time. In addition the interface periodically restarts its laser and monitors the input for an appropriate laser signal.

  ALS and ALR are implemented according to ITU-T G.664.

5.3.2 RS Layer

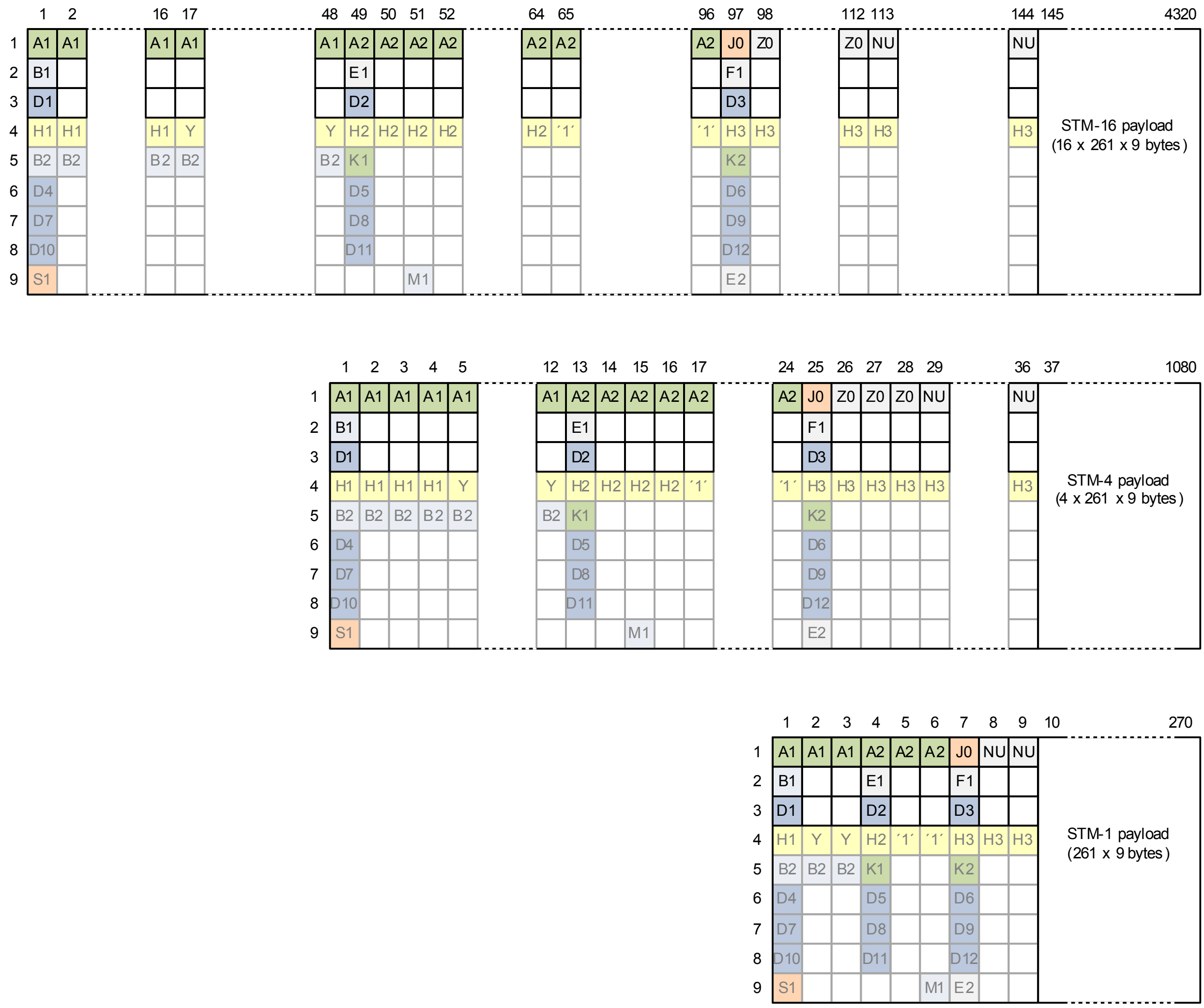


Figure 33: STM-16, STM-4 and STM-1 regenerator section overhead, row 1 to 3

The regenerator section (RS) layer of the NUSA1 unit provides the following functions:

- Termination of the STM-16, STM-4 or STM-1 regenerator section
  - Scrambling/descrambling
  - Check of the B1 byte (BIP-8)
    The bit interleaved parity (BIP) code BIP-8 determines if a transmission error has occurred over a path. Its value is calculated over all bits of the previous scrambled STM-16, STM-4 or STM-1 and placed in the current frame.
    The evaluation of the B1 byte is used for the performance monitoring function.
  - Control of the RS trail trace identifier (TTI) in the J0 byte.
    The RS TTI function allows the XMC20 to control the proper connection of the traffic signal path in a regenerator section via the 16 byte TTI (15 characters).

- Access to the RS data communication channel (DCC) in the D1 to D3 overhead bytes (192 kbit/s). The DCC is used in XMC20 for the embedded communication channel (ECC) connected to COGE5.

Please note:

The access to the RS DCC requires PBUS resources.

→ As soon as one of the RS DCC is configured the vc12-61 to vc12-64 resources are no longer available.

Please note:

The access to the RS orderwire byte (E1) and user channel byte (F1) is not supported.

5.3.3 MS layer

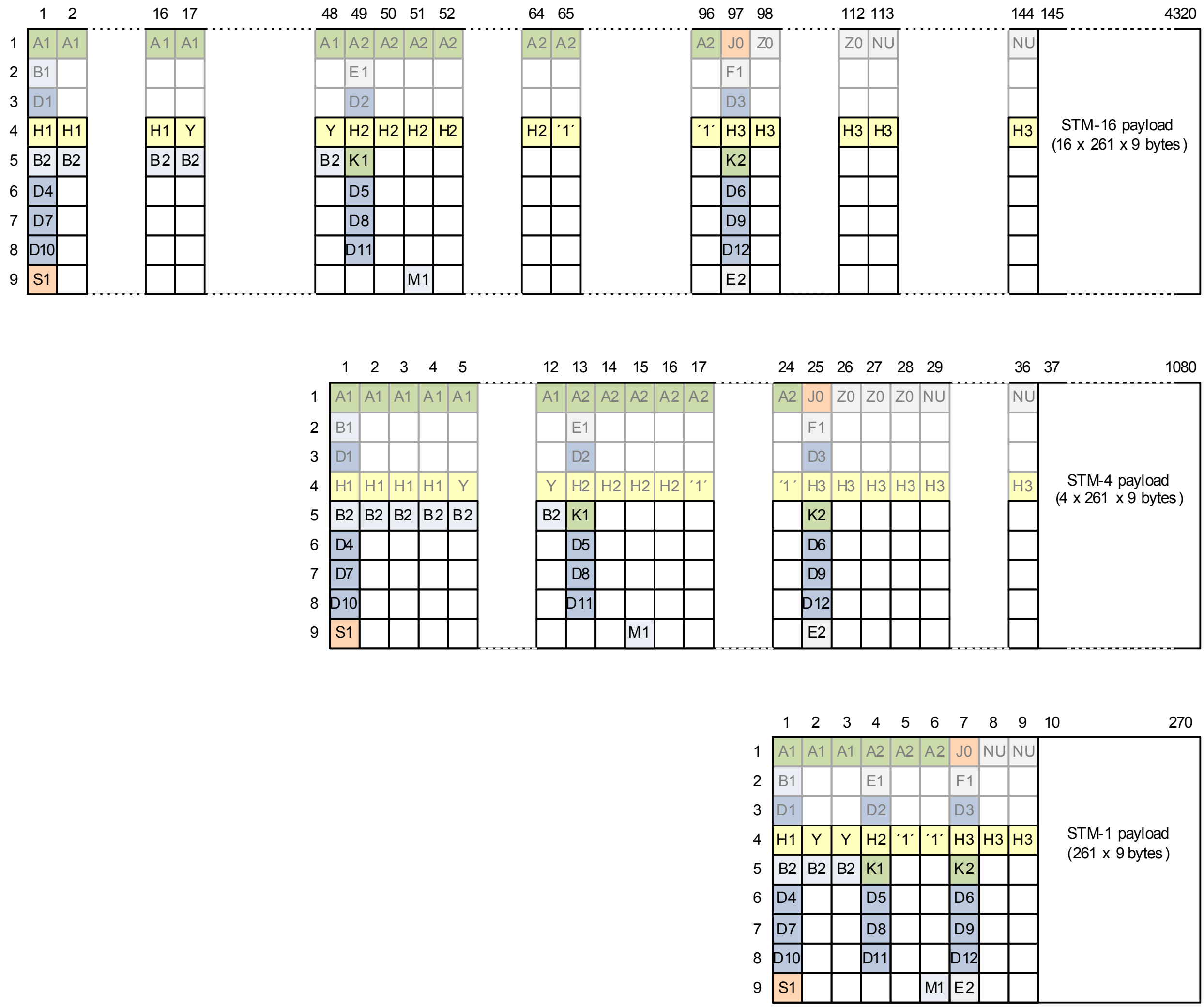


Figure 34: STM-16, STM-4 and STM-1 multiplex section overhead, row 4 to 9

The multiplex section (MS) layer of the NUSA1 unit provides the termination of the STM-16, STM-4 or STM-1 multiplex section with the following functions:

- Access to the M1 byte for the remote error indication or AIS indication.
  The M1 byte indicates the number of remote BIP-384, BIP-96 or BIP-24 errors as described in ITU-T G.707.
- Access to the K2[6-8] byte for the remote defect indication.
- Access to the B2 bytes (BIP-384, BIP-96 or BIP-24).
  The bit interleaved parity (BIP) code BIP-384 (for STM-16), BIP-96 (for STM-4) or BIP-24 (for STM-1) determines if a transmission error has occurred over a path. Its value is calculated over all bits of the previous frame except the regenerator section overhead and placed in the current frame.
  The evaluation of the bit error ratio of the MS traffic assumes a poisson error distribution. The threshold level to set a degraded signal defect can be configured: Degraded BER threshold: 10E-5 … 10E-8.
- Access to the synchronization status message (SSM) byte S1.
  The SSM mode allows the XMC20 to transmit and receive synchronization status messages with the traffic signal. The XMC20 internally processes this information for the selection of the SETS timing source.
  The SSM processing at the port level provides
  - an input mapping table which maps the quality level (QL) received with the traffic signal to some other value.
  - an output mapping table which maps the intrinsic QL for the transmission with the traffic signal to some other QL.
  - a routing table which allows the NUSA1 to mark the transmitted traffic signals depending on the selected traffic source as “can be used” or “do not use” for synchronization purposes.
- Access to the automatic protection switching (APS) channel in the K1 and K2[1-5] bytes. Please refer to section 5.8.1 Multiplex Section Protection (MSP) (on page 86).
- Access to the MS data communication channel (DCC) in the D4 to D12 overhead bytes (576 kbit/s). The DCC is used in XMC20 for the embedded communication channel (ECC) connected to COGE5.
- Multiplexing and demultiplexing of the
  - 16 AU-4 to/from the STM-16, or
  - 4 AU-4 to/from the STM-4, or
  - 1 AU-4 to/from the STM-1.
- Pointer generation and interpretation for all AU-4.
- Frequency adaptation to the SETS clock.

Please note:

The access to the MS DCC requires PBUS resources.

→ As soon as one of the MS DCC is configured the vc12-61 to vc12-64 resources are no longer available.

Please note:

The access to the MS orderwire byte (E2) is not supported.

5.3.4 AU-4 cross Connect

Between the MS layer and the VC-4 layer the NUSA1 unit provides an AU-4 cross connect for 80 front interface AU-4 and 45 tributary AU-4. The cross connect is non blocking, i.e. arbitrary cross connections between all inputs and outputs are allowed.

Please note:

The 45 tributary AU-4 limit the amount of traffic that can be brought to the SDH front interfaces from the Ethernet interfaces, the GbE star and the PBUS.

5.3.5 VC-4 Layer

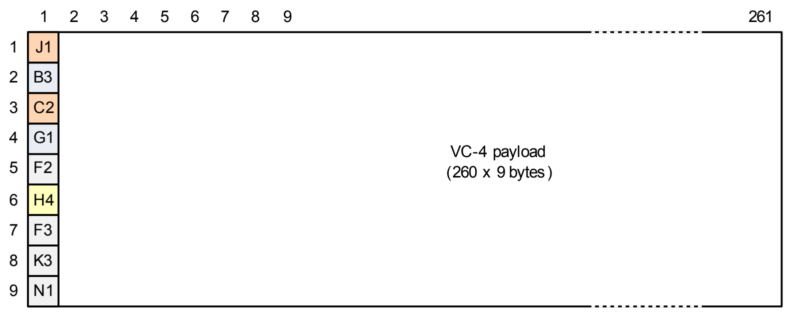


Figure 35: VC-4 path overhead

The VC-4 layer of the NUSA1 unit is used in the EoS (VC-4) application and as an intermediate layer towards the lower order (LO) layers (VC-3, VC-12). It provides the termination of the VC-4 path overhead with the following functions:

- Control of the VC-4 trail trace identifier (TTI) in the J1 byte.
  The VC-4 TTI function allows the XMC20 to control the proper connection of the traffic signal path in an SDH network via the 16 byte TTI (15 characters).
  Note that there is one transmitted TTI per virtual concatenation group (VCG), used in every group member. The received TTI is available for every group member.
- Access to the B3 byte (BIP-8).
  The bit interleaved parity (BIP) code BIP-8 determines if a transmission error has occurred over a path. Its value is calculated over all bits of the preceding VC-4.
  The evaluation of the bit error ratio of the VC-4 assumes a poisson error distribution. The threshold level to set a degraded signal defect can be configured common for all VC-4 on the NUSA1 unit: Degraded BER threshold: 10E-5 … 10E-8
- Access to the C2 byte for the signal label insertion and extraction. The received signal label is displayed in the ECST, together with a consistency indication.
- Access to the G1[1-4] byte for the remote error indication.
  The G1[1-4] byte indicates the number of remote BIP-8 errors as described in ITU-T G.806.
- Access to the G1[5] byte for the remote defect indication.
  The G1[5] byte remote defect indication can be displayed in ECST.

Please note:

The access to the VC-4 user channel bytes (F2, F3), to the automatic protection switching channel byte (K3) and to the tandem connection monitoring byte (N1) is not supported.

5.3.6 TU-3 Cross Connect

Below the VC-4 layer the NUSA1 unit provides a TU-3 cross connect for 48 front interface TU-3.

The cross connect is non blocking, i.e. arbitrary cross connections between all inputs and outputs are allowed.

Please note:

The VC-3 EoS application uses the TU-3 cross connect. Each EoS VC-3 requires therefore two TU-3 resources in the cross connect, one for the connection towards the front interface and one for the connection towards the EoS application.

→ This limits the VC-3 EoS capacity to 24 x VC-3.

→ The TU-3 cross connect capacity must be shared between the EoS application and the cross connected VC-3 in an add/drop multiplexer application.

5.3.7 VC-3 Layer

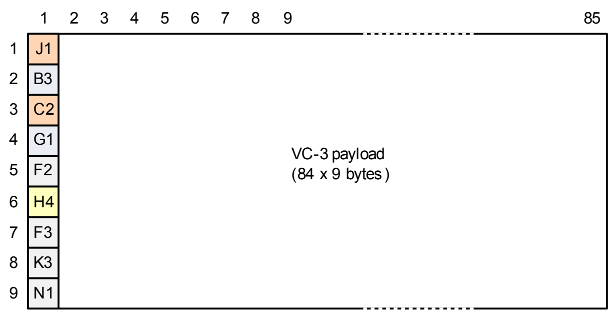


Figure 36: VC-3 path overhead

The VC-3 layer of the NUSA1 unit is used in the EoS application. It provides the termination of the VC-3 path overhead with the following functions:

- Control of the VC-3 trail trace identifier (TTI) in the J1 byte.
  The VC-3 TTI function allows the XMC20 to control the proper connection of the traffic signal path in an SDH network via the 16 byte TTI (15 characters).
  Note that there is one transmitted TTI per virtual concatenation group (VCG), used in every group member. The received TTI is available for every group member.
- Access to the VC-3 path overhead B3 byte (BIP-8).
  The bit interleaved parity (BIP) code BIP-8 determines if a transmission error has occurred over a path. Its value is calculated over all bits of the preceding VC-3.

The evaluation of the bit error ratio of the VC-3 assumes a poisson error distribution. The threshold level to set a degraded signal defect can be configured common for all VC-3 on the NUSA1 unit: Degraded BER threshold: 10E-5 … 10E-8.

- Access to the signal label in the C2 byte for the signal label insertion and extraction.
- Access to the G1[1-4] byte for the remote error indication.
- Access to the G1[5] byte for the remote defect indication.

Please note:

The access to the VC-3 user channel bytes (F2, F3), to the automatic protection switching channel byte (K3) and to the tandem connection monitoring byte (N1) is not supported.

5.3.8 TU-12 Cross Connect

Between the VC-4 layer and the VC-12 layer the NUSA1 unit provides a TU-12 cross connect for 945 front interface TU-12, 252 tributary EoS TU-12, and 64 tributary PBUS TU-12.

The cross connect is non blocking, i.e. arbitrary cross connections between all inputs and outputs are allowed.

5.3.9 VC-12 Layer

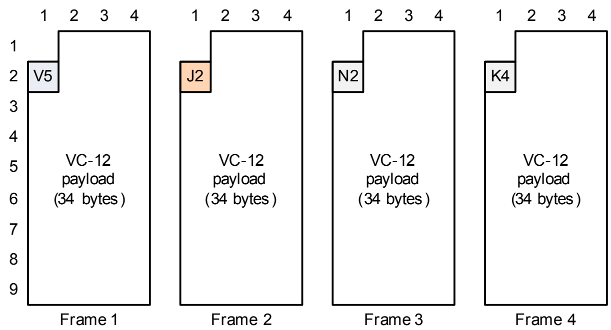


Figure 37: VC-12 path overhead

The VC-12 layer of the NUSA1 unit is used for the EoS application and for the PBUS access application. It provides the termination of the VC-12 path overhead with the following functions:

- Control of the VC-12 trail trace identifier (TTI) in the J2 byte.
  The VC-12 TTI function allows the XMC20 to control the proper connection of the traffic signal path in an SDH network via the 16 byte TTI (15 characters).
  Note that there is one transmitted TTI per virtual concatenation group (VCG), used in every group member. The received TTI is available for every group member.
- Access to the VC-12 path overhead V5[1-2] byte (BIP-2).
  The bit interleaved parity (BIP) code BIP-2 determines if a transmission error has occurred over a path. Its value is calculated over all bits of the preceding VC-12.

The evaluation of the bit error ratio of the VC-12 assumes a poisson error distribution. Two threshold levels can be set to evaluate an excessive and a degraded signal defect. The configuration is valid for all VC-12 on the NUSA1 unit:
Excessive BER threshold: 10E-3 … 10E-5.
Degraded BER threshold: 10E-5 … 10E-8.

- Access to the RFI bit in the V5[4] byte in the PBUS access application. This bit is used to indicate to the remote VC-12 termination function the state of the SNCP selector:
  - Working path selected: RFI = 0,
  - Protecting path selected: RFI = 1.

  This procedure is KEYMILE proprietary.
- Access to the signal label in the V5[5-7] byte for the signal label insertion and extraction.
- Access to the V5[3] byte for the remote error indication.
- Access to the V5[8] byte for the remote defect indication.

Please note:

The access to the VC-12 automatic protection switching channel byte (K4) and to the tandem connection monitoring byte (N2) is not supported.

The VC-12 layer makes also use of the multiframe synchronization contained in the H4 byte of the VC-4 path overhead.

5.4 PDH Layers and Functions

5.4.1 P12 Layer

The P12 layer of the NUSA1 unit is used for the PBUS access of up to 64 P12 signals. NUSA1 supports the asynchronous mapping of the P12 to the VC-12.

The P12 mode controls the P12 signal structure, the mapping on the XMC20 internal TDM bus (PBUS), the synchronization and the handling of the time slot 0 Sa-bits:

- Terminated (P12 mode: PCM30, PCM30C, PCM31, PCM31C, V5 Uplink, V5 Uplink NCI)
  The time slot 0 of the P12 signal is analysed in the receive direction (from the network interface) and regenerated in the transmit direction.
  Cross connection and protection switching (P0-nc SNCP) is established on the P0-nc (n x 64 kbit/s) traffic signal level.
  For terminated signals the following functions are available:
  - CAS (PCM30, PCM30C)
    Support of channel associated signalling in time slot 16.
  - CRC4 (PCM30C, PCM31C)
    Generation and evaluation of the CRC4 code in time slot 0.
- Transparent P12 mode:
  The P12 signal has an unknown structure.
  Cross connection and protection switching is established on the P12 (2 Mbit/s) traffic signal level.

Please note:

The transparent mode features clock transparent cross connections. That means that the signal is in a plesiochronous phase relationship with the NE timing source.

- Clock master
  Unlike the transparent mode, a clock master traffic signal is only cross connected transparently in terms of its structure. The P12 output signal is always resynchronized by the NE timing source. The input signal must be synchronous to the output signal in order to avoid bit slips.
  For details of the clock master mode, please refer to [314] User Guide "TDM Services and Cross Connections in XMC20".
- V5.x applications (P12 mode: V5 Uplink, V5 Uplink NCI)
  The V5.x applications will be available in a future release.

The NUSA1 unit offers maintenance loops at the P12 and P0-nc layer.

5.5 Ethernet Layers and Functions

5.5.1 Ethernet Front Interfaces

NUSA1 offers four electrical 10/100/1000BASE-T Ethernet interfaces.

5.5.1.1 LAN mode

The LAN mode can be configured to a fixed link speed or to autonegotiation. Full duplex mode is supported with 10, 100 and 1000BASE-T, half duplex mode is supported with 10 and 100BASE-T.

The Ethernet ports support auto-negotiation with parallel detection. Auto-negotiation provides the automatic selection of the highest performance mode on a given link.

Risk of operating trouble!

Be aware that when connecting Ethernet ports configured in manual mode (no auto-negotiation) to Ethernet ports in auto-negotiation mode, the following situation may occur:
The link will be up but the duplex settings may be inconsistent and this can result on poor throughput performance on the link.

The previous note applies to any Ethernet device and is a consequence of the behaviour of auto-negotiation and parallel detection. When a port supporting auto-negotiation is connected to a port not supporting auto-negotiation, the port supporting auto-negotiation will revert to parallel detection. This can detect the link type (e.g. 10BASE-T or 100BASE-TX) but will assume half-duplex operation (reference IEEE 802.3 clause 28.2.3.1 note 2). If the far side port is manually configured in full-duplex mode then there is an inconsistent configuration and the side operating in half-duplex may experience collisions while transmitting data.

5.5.1.2 IEEE 802.3 flow control

The Ethernet functional layer allows using IEEE 802.3x flow control.

Flow control is a mechanism which allows inhibiting transmission of data frames for a specified period of time. This is normally used when the receive data buffer is almost full. This state is indicated to the transmitter to stop the transmission of frames for the specified period of time.

In half-duplex mode NUSA1 supports collision-based congestion control. This operates independently of the setting of the 802.3 flow control configuration parameter in the ECST.

Please note:

The flow control feature is only available for the EoS ports in the EPL (unswitched) mode.

5.5.1.3 Link pass through

NUSA1 also provides the “link pass through” feature. This feature can bring the local link state (up or down) to the remote Ethernet interface. If the local link state is down NUSA1 will generate GFP client signal fail management frames going to the remote site. A failure in the SDH path will interrupt the GFP connection.

If the GFP receiver on the remote site will receive GFP client signal fail management frames or no GFP frames at all, it will set the Ethernet interface to the down state accordingly.

With this feature the Ethernet transport is transparent also for link states.

Please note:

The link pass through feature must be enabled on the Ethernet interfaces at both sides of the SDH path to become operational.

Please note:

The link pass through feature is only available for the EoS ports in the EPL (unswitched) mode.

5.5.2 Ethernet Internal Interfaces

NUSA1 has a connection via the Gb Ethernet star in the XMC20 backplane to the active and to the redundant COGE5 units. These connections are internal connections of the XMC20 Switch.

Please note:

Only the connection to the active COGE5 unit is used.

→ The connection to the standby COGE5 unit is deactivated.

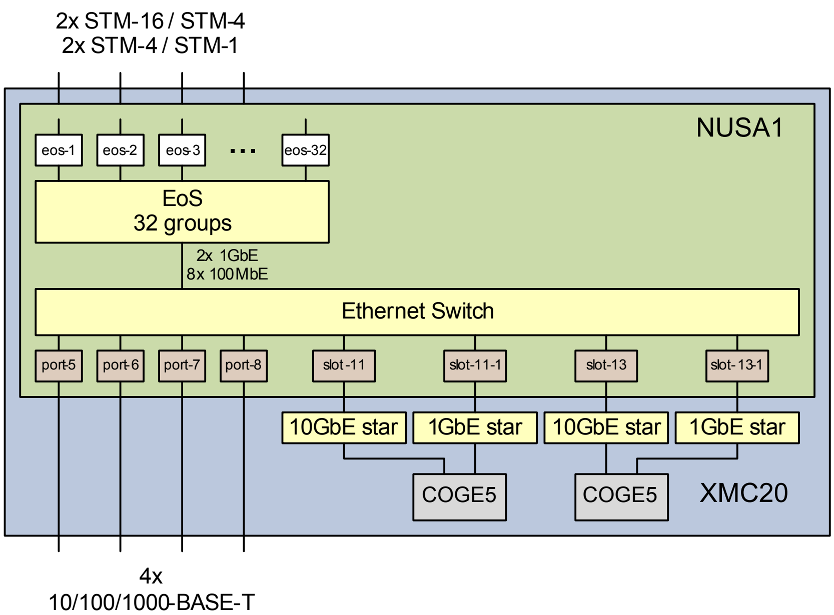


Figure 38: Ethernet internal interfaces

Please note:

Figure 38 "Ethernet internal interfaces" shows the switched port mode for the EoS ports.

→ Refer to section 5.5.3.2 Switched port mode (on page 73).

Please note:

The access to the 10Gb-Ethernet star will be available in a future release.

5.5.3 Ethernet Switch

The Ethernet switch device on the NUSA1 unit participates in the XMC20 Switch. The Ethernet front ports can be configured to bypass the VLAN bridge.

With the VLAN Bridge function the Ethernet front ports and the EoS ports support up to three operation modes:

- Unswitched mode (see section 5.5.3.1):
  In the unswitched mode the Ethernet traffic from an Ethernet front port is directly connected to an EoS port. The Ethernet front port and the EoS port are not part of the XMC20 Switch.
- Switched mode (see section 5.5.3.2):
  In the switched mode the Ethernet traffic from an Ethernet front port and from an EoS port accesses the XMC20 Switch. The Ethernet front port and the EoS port are handled as any other port of the XMC20 Switch.
- Expansion mode (see section 5.5.3.3):
  An EoS port eos-9 to eos-12 in the expansion mode provides five additional EoS ports to be used as XMC20 Switch ports. The feature set of an EoS expansion port is reduced compared with a normal EoS switched port.

The availability of the different port modes for the Ethernet front ports and the EoS ports is as follows:

Table 18: Available port modes

Port	Mode		
	Unswitched	Switched	Expansion
port-5: Ethernet	yes	yes	no
port-6: Ethernet	yes	yes	no
port-7: Ethernet	yes	yes	no
port-8: Ethernet	yes	yes	no
eos-1	yes	yes	no
eos-2	yes	yes	no
eos-3	yes	yes	no
eos-4	yes	yes	no
eos-5	no	yes	no
eos-6	no	yes	no
eos-7	no	yes	no
eos-8	no	yes	no
eos-9	yes	yes	yes
eos-10	yes	yes	yes

Table 18: Available port modes (continued)

Port	Mode		
	Unswitched	Switched	Expansion
eos-11	no	yes	yes
eos-12	no	yes	yes
eos-13 to eos-32	no	no	yes

Please note:

Without using expansion ports the number of usable EoS ports is limited to 12.

→ Refer to section 5.5.3.3 Expansion port mode (on page 74).

Please note:

The switched, unswitched or expansion port mode is configurable individually per Ethernet port and EoS port, respecting the port mode availability listed in Table 18.

5.5.3.1 Unswitched port mode

The unswitched mode connects an Ethernet front port directly to the corresponding EoS port, bypassing the VLAN bridge. This corresponds to the EPL (Ethernet Private Line) application.

The following point-to-point connections are available:

Table 19: Unswitched port mode

Ports connected		EoS Bandwidth	QoS	Restrictions
Ethernet	Eos			
port-5	eos-1	100 Mbit/s	Flow control, Scheduling	none
port-5	eos-9	1000 Mbit/s	Flow control, Scheduling	If eos-9 is used in the unswitched port mode the following EoS ports are not usable, i.e. are not available for user traffic: eos-11, eos-13 to eos-17, eos-23 to eos-27.
port-6	eos-2	100 Mbit/s	Flow control, Scheduling	none
port-6	eos-10	1000 Mbit/s	Flow control, Scheduling	If eos-10 is used in the unswitched port mode the following EoS ports are not usable, i.e. are not available for user traffic: eos-12, eos-18 to eos-22, eos-28 to eos-32.
port-7	eos-3	100 Mbit/s	Flow control, Scheduling	none
port-8	eos-4	100 Mbit/s	Flow control, Scheduling	none

Please note:

In the ECST “Switching” tab the Ethernet front port and the corresponding EoS port must be configured to the “unswitched” port mode ***before*** *the EPL mode can be enabled for the ports.*

→ When using the EoS port eos-9 in the “unswitched” port mode also the EoS port eos-11 must be configured to the “unswitched” port mode **before** the EPL mode can be enabled.

→ When using the EoS port eos-10 in the “unswitched” port mode also the EoS port eos-12 must be configured to the “unswitched” port mode **before** the EPL mode can be enabled.

All Ethernet ports and EoS ports not configured for the unswitched port mode operate in the switched or expansion port mode, accessing the VLAN bridge. Refer to section 5.5.3.2 Switched port mode (on page 73) and section 5.5.3.3 Expansion port mode (on page 74).

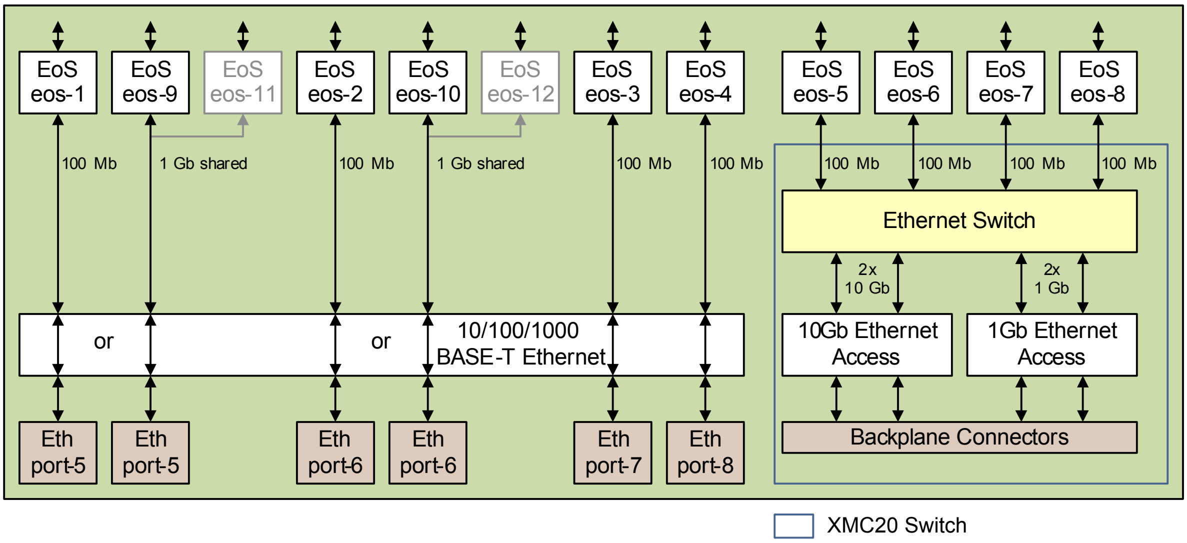


Figure 39: EoS and Ethernet switching in unswitched mode

Please note:

In Figure 39 "EoS and Ethernet switching in unswitched mode" the not usable expansion EoS ports eos-13 to eos-32 are not shown.

5.5.3.2 Switched port mode

The switched mode connects an Ethernet front port or an EoS port directly to the XMC20 Switch.

The port can be used as VLAN bridge port (in the VLAN Bridge application) or as PWAC port (for the MPLS-TP VPWS Transport application.

Table 20: Switched port mode

Port	Bandwidth	QoS	Restrictions
port-5	10/100/1000 Mbit/s	standard XMC20 Switch port	none
port-6	10/100/1000 Mbit/s	standard XMC20 Switch port	none
port-7	10/100/1000 Mbit/s	standard XMC20 Switch port	none
port-8	10/100/1000 Mbit/s	standard XMC20 Switch port	none
eos-1	100 Mbit/s	standard XMC20 Switch port	none
eos-2	100 Mbit/s	standard XMC20 Switch port	none
eos-3	100 Mbit/s	standard XMC20 Switch port	none
eos-4	100 Mbit/s	standard XMC20 Switch port	none
eos-5	100 Mbit/s	standard XMC20 Switch port	none
eos-6	100 Mbit/s	standard XMC20 Switch port	none
eos-7	100 Mbit/s	standard XMC20 Switch port	none
eos-8	100 Mbit/s	standard XMC20 Switch port	none
eos-9	1000 Mbit/s	standard XMC20 Switch port	Bandwidth shared with eos-11
eos-10	1000 Mbit/s	standard XMC20 Switch port	Bandwidth shared with eos-12

Table 20: Switched port mode (continued)

Port	Bandwidth	QoS	Restrictions
eos-11	1000 Mbit/s	standard XMC20 Switch port	Bandwidth shared with eos-9
eos-12	1000 Mbit/s	standard XMC20 Switch port	Bandwidth shared with eos-10

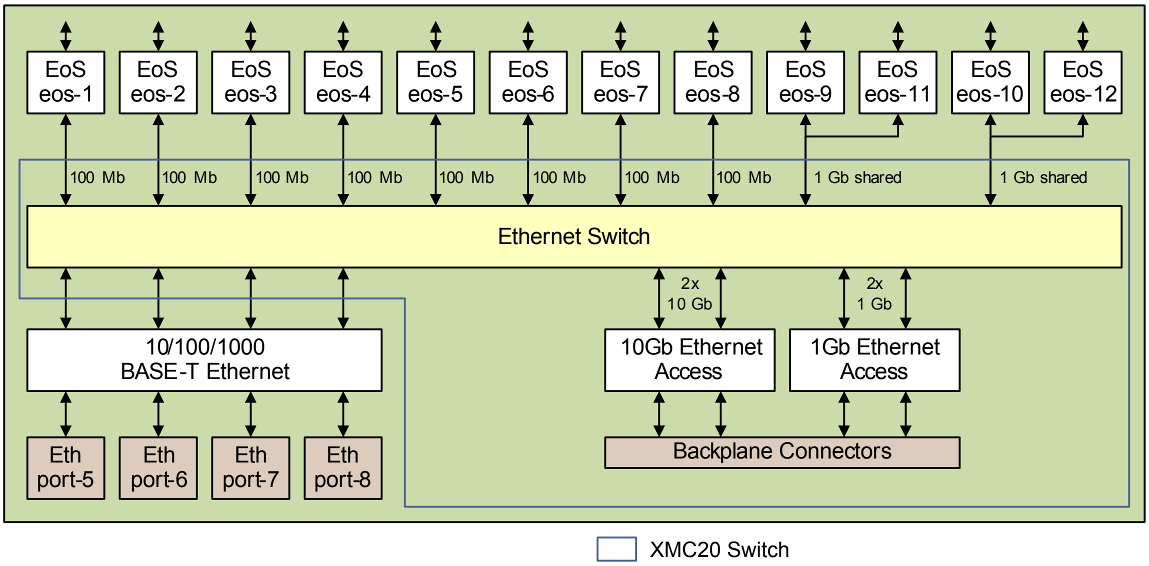


Figure 40: EoS and Ethernet switching in switched mode

Please note:

In Figure 40 "EoS and Ethernet switching in switched mode" the EoS ports eos-9 to eos-12 are all configured to the switched port mode.

→ The expansion EoS ports eos-13 to eos-32 are not usable and are not shown.

5.5.3.3 Expansion port mode

When one of the EoS ports eos-9 to eos-12 is configured to the expansion port mode it is called “master expansion port”. Each master expansion port makes five additional EoS ports usable as VLAN bridge ports. The master expansion port and the five additional EoS ports belong to one expansion group, designated X1 to X4.

Even though all EoS ports of an expansion group access the VLAN bridge, only the master expansion port is visible in the ECST “Switching” tab. In the “Switching” tab this master expansion port has to be configured

- to the “trunk” port mode, or
- to the “general” port mode with “tagged” acceptable frame types and “tagged” egress frames. All used VLAN IDs must be added to the VLAN membership table.
- The QoS configuration of the master expansion port is applied to all EoS ports of the expansion group.

Risk of operating trouble!

When using an additional expansion port, the master expansion port of this expansion group must have an EoS group configured and must be in the administrative state “Up”.

→ Otherwise the expansion ports of this expansion group will not be operational.

The VLAN configuration of all expansion group members is done on the NUSA1 unit at the AP: /unit-x/eos/eos-y - Configuration - Port Mode:

- Expansion mode frame type:
  - Tagged:
    Ingress frames must be tagged.
    Egress frames are sent out tagged.
    The usable VLAN IDs must be configured in the VLAN table.
    The Port VLAN ID is not used.
  - Untagged.
    Ingress frames must be untagged and are tagged with the Port VLAN ID inside the XMC20 Switch.
    Egress frames are sent out untagged, or with the outer VLAN tag removed.
    The Port VLAN ID must be configured in the VLAN table.
- Port VLAN ID:
  Only used for the untagged frame type.
- VLAN table:
  - List of VLAN IDs for tagged and untagged traffic

Risk of operating trouble!

The VLAN table of an expansion port can contain multiple VLAN IDs, but a VLAN ID cannot be member of more than one EoS port of the same expansion group.

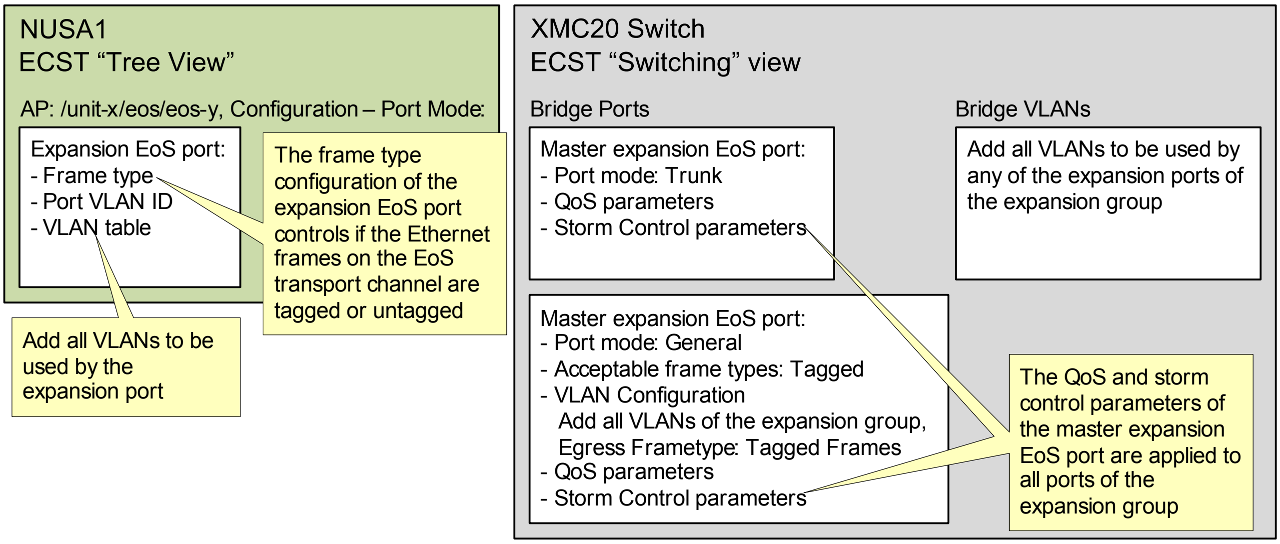


Figure 41: Configuration parameters of an expansion EoS port

Table 21: Expansion port mode

Master expansion port	Expansion group	Expansion ports	Bandwidth	QoS
eos-9	X1	eos-9 eos-13 eos-14 eos-15 eos-16 eos-17	1000 Mbit/s, shared between eos9, eos-13 to eos-17, and eos-11, and eos-23 to eos-27 if expansion mode is used for eos-11.	standard VLAN bridge port configuration of eos-9 is applied to eos-9 and eos-13 to eos-17
eos-10	X2	eos-10 eos-18 eos-19 eos-20 eos-21 eos-22	1000 Mbit/s, shared between eos10, eos-18 to eos-22, and eos-12, and eos-28 to eos-32 if expansion mode is used for eos-12.	standard VLAN bridge port configuration of eos-10 is applied to eos-10 and eos-18 to eos-22
eos-11	X3	eos-11 eos-23 eos-24 eos-25 eos-26 eos-27	1000 Mbit/s, shared between eos11, eos-23 to eos-27, and eos-9, and eos-13 to eos-17 if expansion mode is used for eos-9.	standard VLAN bridge port configuration of eos-11 is applied to eos-11 and eos-23 to eos-27
eos-12	X4	eos-12 eos-28 eos-29 eos-30 eos-31 eos-32	1000 Mbit/s, shared between eos12, eos-28 to eos-32, and eos-10, and eos-18 to eos-22 if expansion mode is used for eos-10.	standard VLAN bridge port configuration of eos-12 is applied to eos-12 and eos-28 to eos-32

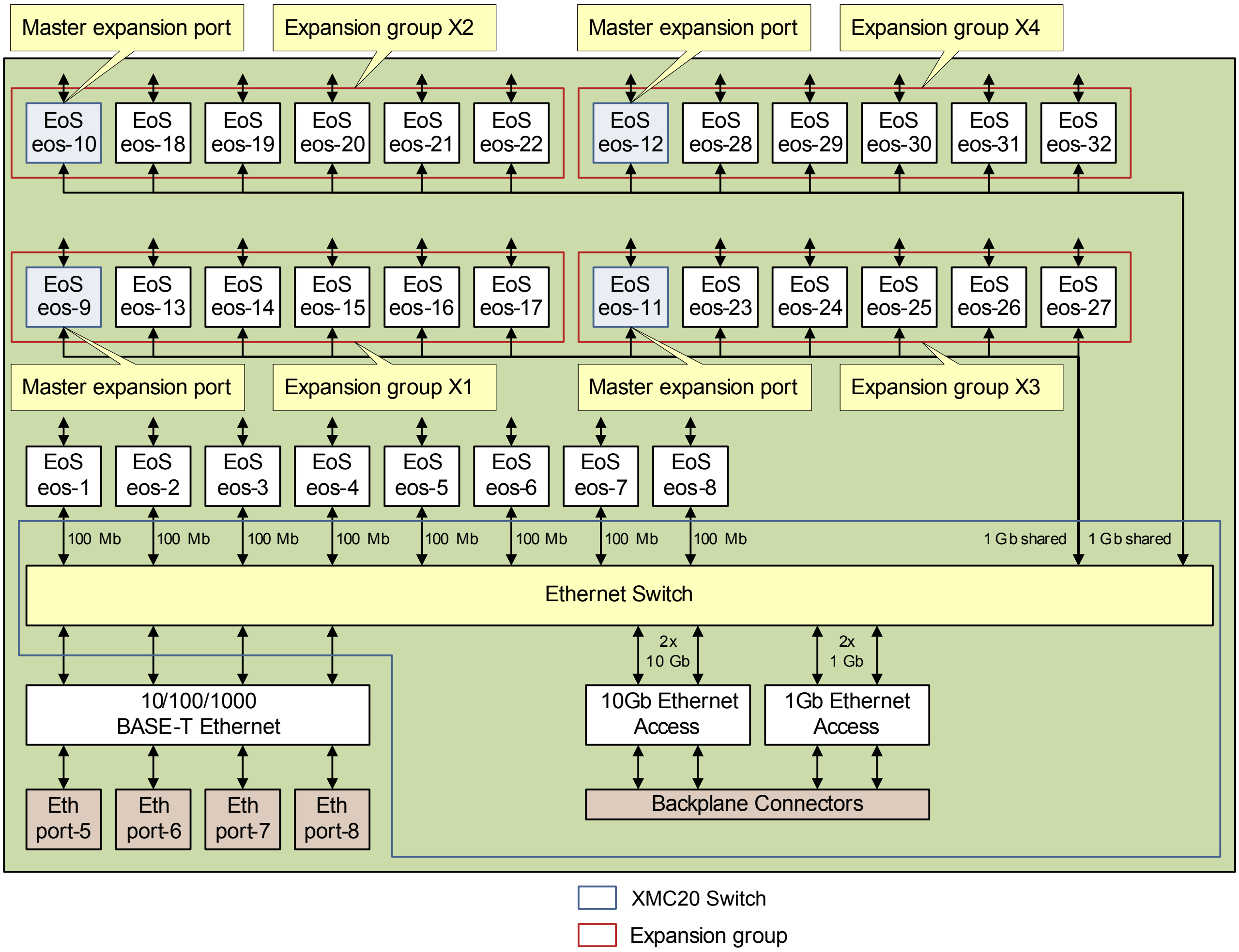


Figure 42: EoS and Ethernet switching in expansion mode

5.5.4 Ethernet over SDH (EoS)

NUSA1 enables the interconnection of dispersed LANs through SDH networks by creating point to point connections with “Ethernet over SDH” (EoS). NUSA1 supports up to 32 EoS ports. EoS ports accessing the VLAN bridge are handled as external ports of the VLAN bridge. Refer also to section 5.5.3 Ethernet Switch (on page 71).

EoS transport is possible using the generic framing procedure (GFP) and virtual concatenation (VCAT). The link capacity adjustment scheme (LCAS) allows an EoS group to remain operational also when one of the links fails. LCAS also provides the capability to manually add or delete links to or from an EoS group.

The following sections present the main functions, features and protocols used by EoS.

5.5.4.1 Generic framing procedure (GFP)

The NUSA1 unit implements GFP according to ITU-T G.7041. This recommendation defines the required procedures for transporting variable length frames over SDH transport paths.

GFP provides a unified way to encapsulate and transport client signals instead of application specific mapping protocols.

G.7041 defines two GFP modes of operation:

- Frame mapped GFP
  A single client frame is mapped into a single GFP frame.
- Transparent GFP
  A number of client data characters are mapped into efficient block codes for transport within a GFP frame.

NUSA1 supports frame mapped GFP.

GFP supports two types of frames:

- Client frames
  Client frames transport client data (client data frame) or management information (client management frame).
- Control frames
  Control frames are used as idle frames, i.e. when no client data has to be transported.

The basic signal structure of a GFP client frame is shown in the figure below. GFP frames are octet aligned and consist of a GFP core header and a GFP payload area, i.e. a payload header and a payload information field.

A GFP control frame consists of a core header only.

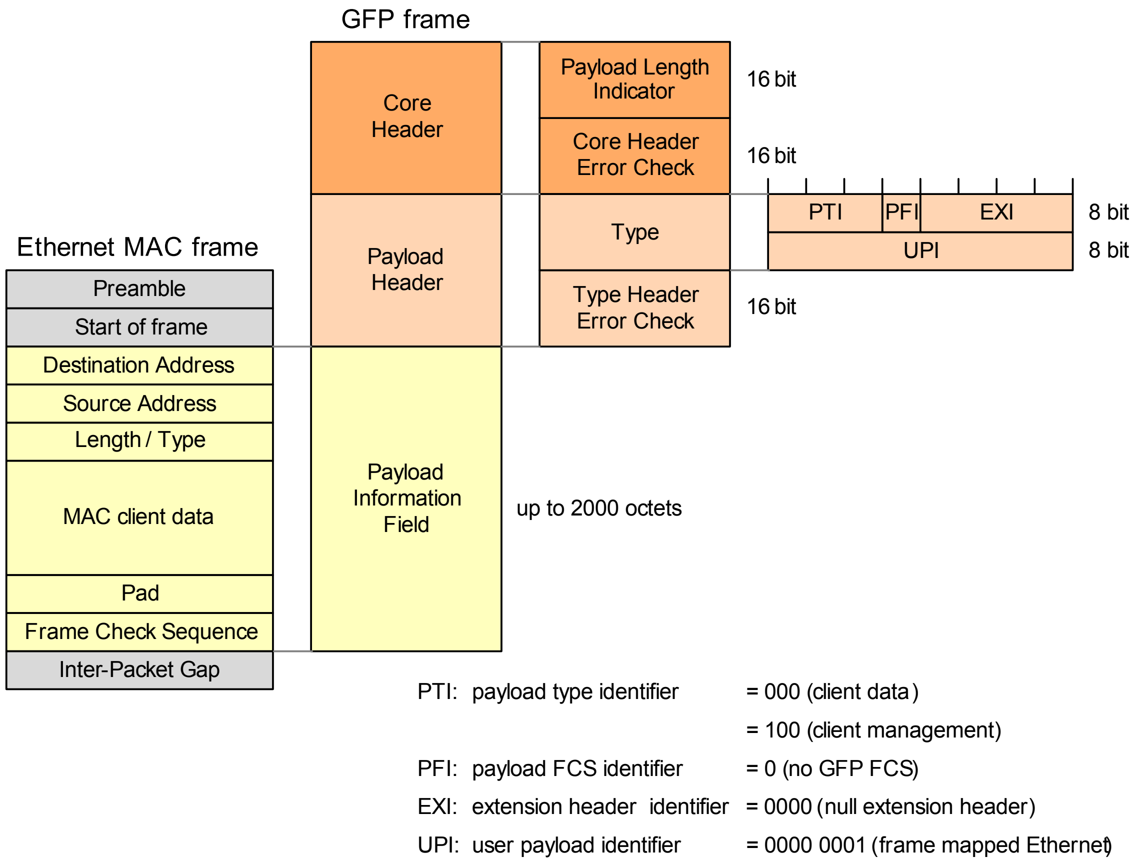


Figure 43: Frame mapped GFP

NUSA1 implements the following payload header type fields for **client data**:

Table 22: Payload header type fields

Field	Value	Description
PTI	000	Client data
PFI	0	No GFP frame check sequence (FCS)
EXI	0000	Null header extension
UPI	0000 0001	Frame mapped Ethernet

The payload information field contains the framed PDU. The client PDU is always transferred into the GFP payload information field as an octet aligned packet stream.

The GFP payload contains the Ethernet MAC frame excluding the Ethernet “preamble” and “start of frame” bytes but including the Ethernet FCS.

NUSA1 implements the following payload header type fields for **client management**:

Table 23: Payload header type fields

Field	Value	Description
PTI	100	Client management
PFI	0	No GFP frame check sequence (FCS)
EXI	0000	Null header extension
UPI	0000 0001	Loss of client signal
	0000 0010	Loss of client character synchronization

Client management frames are used to propagate a client signal fail (CSF) indication to the far end. In case of a Link Down, the NUSA1 generates client management GFP frames once every 100 – 150 ms. The GFP CSF condition will be cleared after 3 s, if no GFP CSF frames are received, or upon receiving a valid GFP client data frame.

The GFP frame stream is mapped into a container-n or virtually concatenated container-n-Xv (n = 12, 3, 4) with its byte boundaries aligned with the byte boundaries of the container. The container is then mapped into the VC-n, or VC-n-Xv respectively, together with the associated path overhead.

The GFP frame boundaries are thus aligned with the VC-n byte boundaries. Since the container-n capacity is not an integer multiple of the variable length GFP frame, a GFP frame may cross a container-n frame boundary.

GFP frames arrive as a continuous byte stream with a capacity that is identical to the VC payload, due to the insertion of GFP idle frames at the GFP adaptation stage.

5.5.4.2 Virtual concatenation (VCAT)

NUSA1 provides 32 EoS groups (virtual concatenation groups, VCG groups) that can be used for the transport of Ethernet traffic over SDH.

Each EoS group consists of a number of virtual channels, the members of this group. All members of a group must be of the same VC type. The following group member types are supported:

Table 24: EoS group members

Member type	Max. number of members per group	Max. number of members per unit
VC-12	63	252
VC-3	24	24
VC-4	14	14

The maximum available EoS capacity depends on the usage of VC-12 EoS members:

- No VC-12 EoS members used:
  The VC-4 and VC-3 EoS members share a total capacity of 14 VC-4 equivalents.
- VC-12 EoS members used:
  The VC-4, VC-3 and VC-12 EoS members share a total capacity of 12 VC-4 equivalents:
  - Up to 8 VC-4 equivalents for VC-4 and VC-3 members,
  - Up to 4 VC-4 equivalents for VC-12 members.

Please note:

The 48 x 48 TU-3 cross connect capacity of NUSA1 must be shared for EoS VC-3 group members and through connected VC-3.

→ (Number of EoS VC-3) + (Number of through connected VC-3) ≤ 24

The members of an EoS group are virtually concatenated. Virtual concatenation allows transporting more efficiently low capacity payloads which are unable to fill complete VC-3 or VC-4 signals. This is achieved by the concatenation of smaller signal containers (e.g. VC-12) with a common destination. The aggregation of signal containers (members) is called a virtual concatenation group (VCG).

A GFP frame is split over all members of the virtual concatenation group. Each member of a VCG can take a different path through the network. The VCG will be reassembled at the destination point. The reassembly buffer supports with an adaptive buffer a differential delay of up to 64 ms between virtual concatenated VCs.

The following figure shows how frames are split over different VC belonging to the same VCG. The VC is labelled with the frame counter and a sequence indicator which makes it possible to reassemble the frames at the remote end.

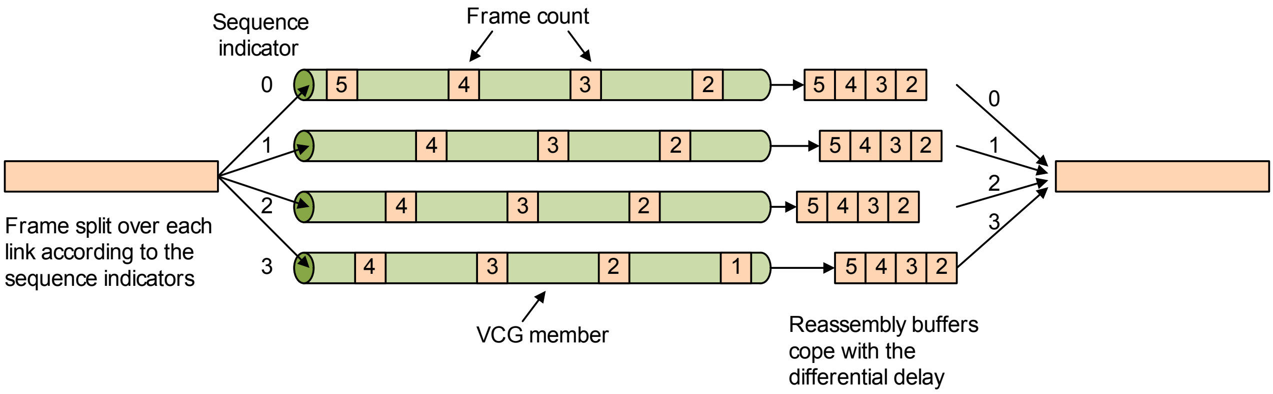


Figure 44: Virtual concatenation

The sequence indicator and the frame count are transported in the VC path overhead of every virtual container.

Table 25: VCG frame counter and sequence indicator

VC	Frame count	Sequence indicator	Transport
VC-4 VC-3	0 … 4095	0 … 255	H4 byte
VC-12	0 … 31	0 … 63	K4[2] byte

With VC-12 virtual concatenation the usable capacity is a multiple of 2’176 kbit/s, up to a maximum of 63 x 2’176 = 137’088 kbit/s.

With VC-3 virtual concatenation the usable capacity is a multiple of 48’384 kbit/s, up to a maximum of 24 x 48’384 = 1’161’216 kbit/s.

With VC-4 virtual concatenation the usable capacity is a multiple of 149’760 kbit/s, up to a maximum of 14 x 149’760 = 2’096’640 kbit/s.

Table 26: Ethernet to VCG traffic allocation examples

Ethernet bandwidth	Container types	Number of containers	VCG capacity	VCG utiliza-tion [a]
10 Mbit/s	C-12 (2’176 kbit/s)	5	10.880 Mbit/s	92%
	C-3 (48.384 kbit/s)	1	48.384 Mbit/s	20%
100 Mbit/s	C-12 (2’176 kbit/s)	46	100.096 Mbit/s	100%
	C-3 (48.384 kbit/s)	3	145.152 Mbit/s	69%
	C-4 (149’760 kbit/s)	1	149.760 Mbit/s	67%
1000 Mbit/s	C-4 (149’760 kbit/s)	7	1’048.320 Mbit/s	95%

a. Calculated for the Ethernet bandwidth

Please note:

The VCG groups are attached to EoS ports of the VLAN bridge or to a NUSA1 Ethernet front port, limiting the available bandwidth per EoS port to 100 Mbit/s for eos-1 to eos-8 and 1000 Mbit/s for eos-9 plus eos-11 and eos-10 plus eos-12.

→ Please refer to section 5.5.3 Ethernet Switch (on page 71).

5.5.4.3 Link capacity adjustment scheme (LCAS)

The link capacity adjustment scheme (LCAS) protocol is an addition to the virtual concatenation process which allows you to use a variable number of virtual concatenated containers. This means that the number of members in the VCG can be changed on demand of the user. The LCAS protocol provides a synchronization and a handshake mechanism between the concatenation source and sink functions to allow a change in the group size without transmission hits. LCAS uses control packets that are transmitted over the links in advance of a configuration change so that the receiver can switch hitless to a new configuration. The different states of a link can be seen in the VC status section.

Another function of the LCAS protocol is to autonomously remove members that experience transmission failures or degraded transmission performance. This feature can be used to implement resilience by routing link members over different network routes.

Note further that there is no need to have an identical number of members in the two directions of a bi-directional link, however there should be at least one member active in both directions.

The operation of LCAS is unidirectional which means that in order to add or remove members of a VCG the operation has to be done at both ends. These actions are independent from each other, do not require to be synchronized and have to be performed by the management system (ECST or UNEM).

It is possible to enable or disable LCAS in ECST.

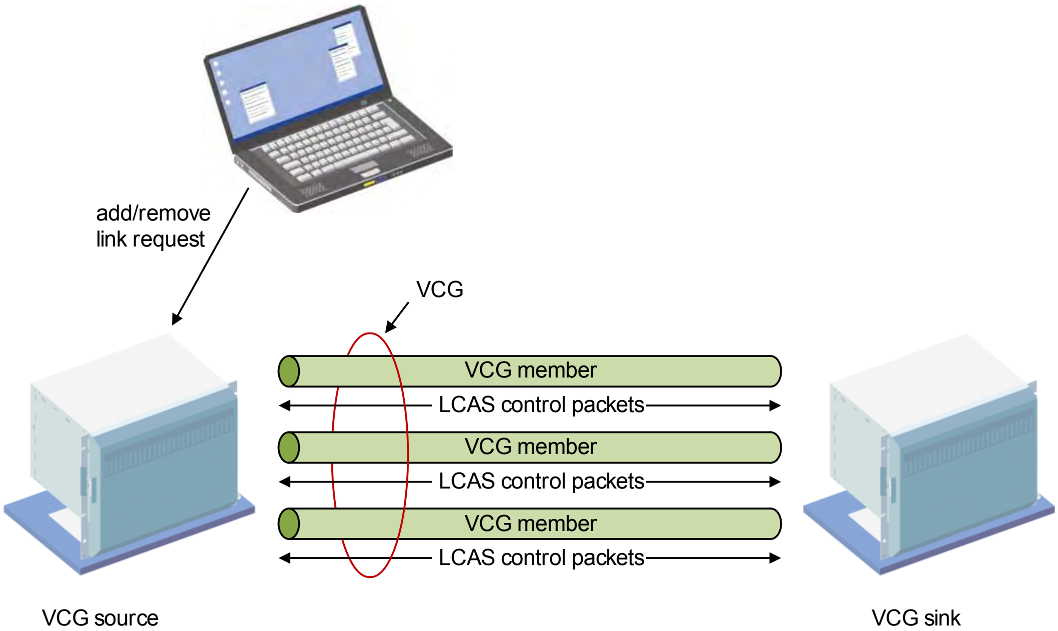


Figure 45: LCAS operation

5.6 Embedded Communication Channel (ECC)

The embedded communication channel (ECC) of XMC20 provides an integrated communication structure for the management communication. The element manager accesses the ECC normally via a management interface of the COGE5 unit. The ECC is transported via aggregate signals connecting the NEs.

NUSA1 provides the DCC in the regenerator section overhead (3 x 64 kbit/s) and the multiplex section overhead (9 x 64 kbit/s) for the ECC transport. The ECC is transported either via the RSOH DCC or the MSOH DCC or via both DCC channels.

The ECC is connected via the PBUS to the COGE5 unit which provides the routing function. When using the RSOH DCC and MSOH DCC of eight SDH ports the required bandwidth is 8 x (3 + 9) = 96 time slots, occupying 4 P12 signals on the PBUS.

Please note:

The access to the RS and/or MS DCC requires PBUS resources.

→ As soon as one of the RS or MS DCC is configured the vc12-61 to vc12-64 resources are no longer available.

The DCC status function provides information about the HDLC link status towards the SDH port and towards the PBUS access.

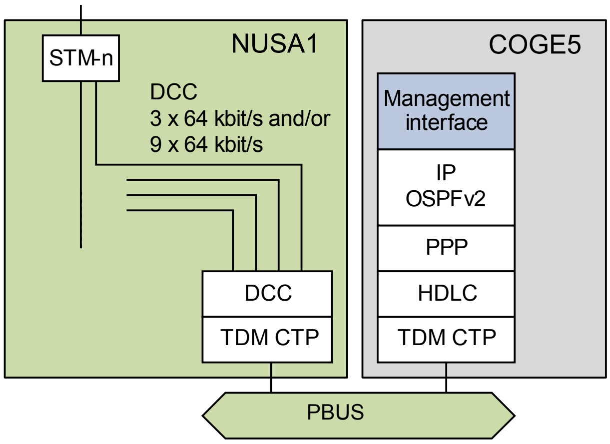


Figure 46: NE management over DCC operation

It is also possible to use a partially or completely filled P12 for the ECC transport. The P12 is transported in a VC-12.

The COGE5 unit is used the same way as with the ECC over DCC transport.

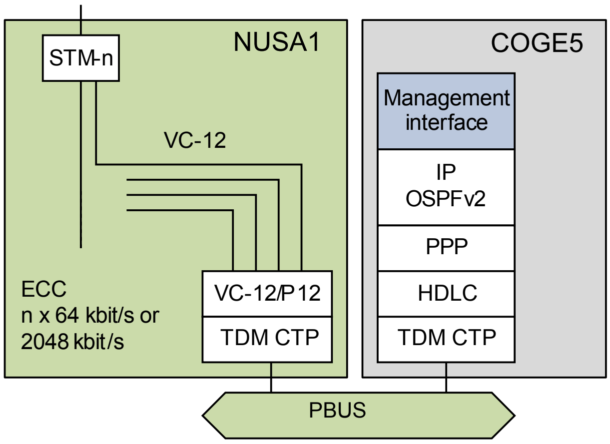


Figure 47: ECC over P12 operation

5.7 Synchronization and Timing Functions

For a description of the NUSA1 and XMC20 synchronization and timing functions please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.

5.8 Traffic Protection

5.8.1 Multiplex Section Protection (MSP)

NUSA1 supports multiplex section protection (MSP) on a single unit. MSP can be enabled on the STM-16, STM-4 and/or STM-1 port pairs, i.e. MSP is supported between the logical SDH ports

- sdh-1 and sdh-2, and
- sdh-3 and sdh-4.

In addition the NUSA1 unit supports MSP on two units, operating as equipment protection pair. MSP can be enabled on the STM-16, STM-4 and/or STM-1 port pairs. With MSP configured to “intracard”, MSP is supported between the logical SDH ports

- sdh-1 and sdh-2, and
- sdh-3 and sdh-4, and
- sdh-5 and sdh-6, and
- sdh-7 and sdh-8.

With MSP configured to “intercard”, MSP is supported between the logical SDH ports

- sdh-1 and sdh-5, and
- sdh-2 and sdh-6, and
- sdh-3 and sdh-7, and
- sdh-4 and sdh-8.

The MSP mode “intracard” or “intercard” is individually configurable per logical SDH port.

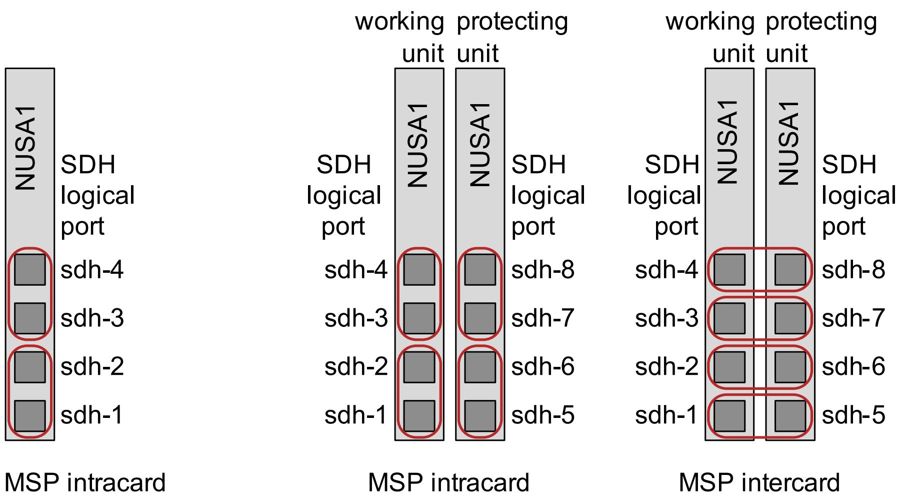


Figure 48: MSP on a single unit (left) and on two units (right)

MSP protects against failures in the physical section (optical or electrical), the regenerator section and the multiplex section. Using the “intercard” MSP mode, MSP protects also against NUSA1 equipment failures. MSP provides the following functions:

- 1+1 unidirectional protection mode according to ITU-T G.841, § 7.1.4.4.
  The NUSA1 unit selects the received signal from one of the two STM-16, STM-4 or STM-1 interfaces and switches to the other interface if this signal fails.
  1+1 unidirectional protection switching uses no protocol.
- 1+1 bidirectional protection mode
  A dedicated protocol, transported in the K1 and K2 bytes of the MS overhead, synchronizes the local and remote STM-16, STM-4 or STM-1 interfaces of the multiplex section to select the received signal from the same STM-16, STM-4 or STM-1 interface.
  Bidirectional protection switching uses a fixed bridge (without extra traffic), compatible with 1:n bidirectional switching according to ITU-T G.841, § 7.1.4.5.1.

The operation type is non-revertive, i.e. the system does not switch back to the working channel if the working channel becomes available again after a switch-over to the protecting channel.

If after a protection switchover the working channel is available again while the protecting channel fails, the system switches back to the working channel. However, the protection protocol of the bidirectional protection is not switched to the working channel.

The working channel provides the active STM-16, STM-4 or STM-1 signal under normal operating conditions. The standards refer to the working channel as channel 1. The protecting channel protects the working channel. The standards refer to the protecting channel as channel 0.

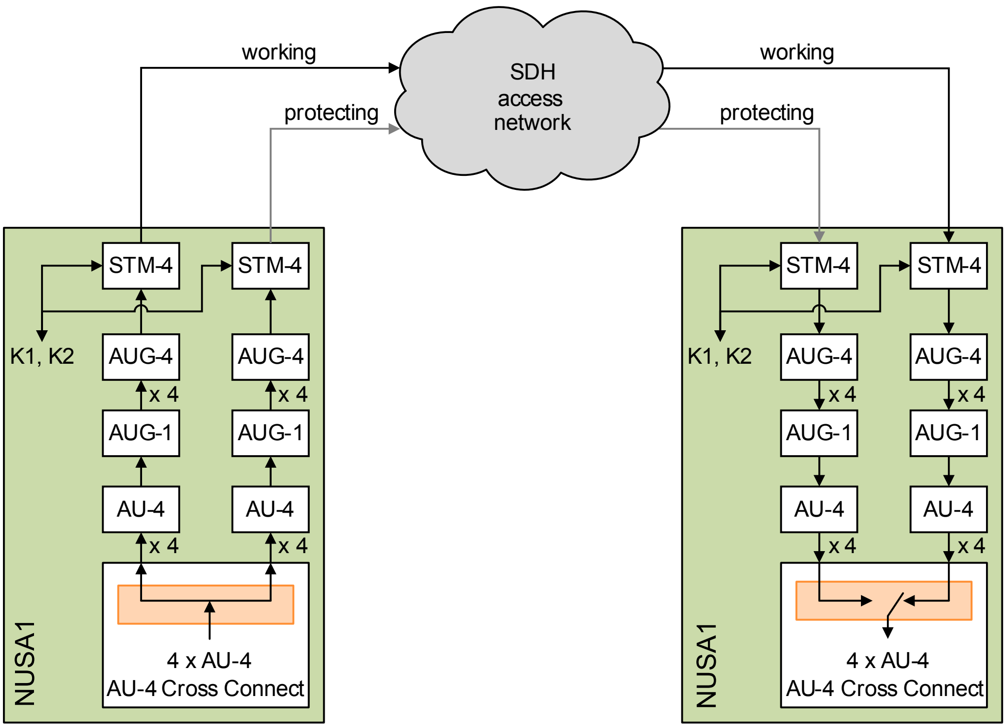


Figure 49: 1+1 MSP (only one direction of the MS trail is shown)

The figure above shows an example with STM-4.

Protection switching takes place in the higher order cross connect (AU-4 cross connect). 16 (STM-16 interface), 4 (STM-4 interface) or 1 (STM-1 interface) AU-4 signals are switched simultaneously.

Protection switching action can be driven by two different request types:

Traffic signal requests:

- Signal fail (SF)
  The SF state is activated if the analysis of the STM-16, STM-4 or STM-1 traffic signal reports a signal failure in the PS, MS or RS:
  - Loss of optical or electrical signal,
  - Loss of frame alignment,
  - TTI mismatch,
  - AIS.
- Signal degraded (SD)
  The SD state is activated if the analysis of the STM-16, STM-4 or STM-1 traffic signal shows a degraded traffic signal. Please refer to section 5.3.3 MS layer (on page 62).

External command requests:

External commands are the switching requests applied by the user via the management system. The list below shows the external commands for MSP in the descending order of priority. Please note the restrictions on effectiveness for some of the commands:

- Clear
  Clears all switching requests listed below.
- Lockout of protection (Protecting channel only).
  This command blocks all switching requests to switch the active channel from the working to the protecting channel.
- Forced switch
  Switches the active channel to the port where the command has been applied to, unless an equal or higher priority switch command is in effect.
  Since a forced switch has higher priority than SF or SD on the working channel, this command will be carried out regardless of the condition of the working channel.
  Note that an SF condition on the protecting channel has higher priority than a forced switch. Therefore it is not possible to switch from the working channel to the protecting channel if this channel has SF.
- Manual switch
  Switches the active channel to the port where the command has been applied to, unless an equal or higher priority switch command is in effect or an SF condition exists on this channel.
  Since manual switch has lower priority than SF or SD on a working or protecting channel, this command will be carried out only if the channel is not in SF or SD condition.
- Exercise
  Effective for the bidirectional MSP mode and working channel only.
  This command checks the responses of automatic protection switching (APS) bytes to a switch request, unless the protecting channel is in use. The switch is not actually completed for the traffic signal.
  The remote request will display a “Reverse request”.

Each request (signal, external) has a fixed priority. These priorities allow the MSP to select the request with the highest priority if there is more than one request pending. The table below lists the requests with the corresponding priorities according to ITU-T G.841.

Table 27: Types of request (Table 7-1/G.841)

Bits 1234	Condition, state or external request	Order [a]
1111	Lockout of protection [b]	Highest
1110	Forced switch	|
1101	Signal fail high priority	|
1100	Signal fail low priority	|
1011	Signal degrade high priority	|
1010	Signal degrade low priority	|
1001	Unused [c]	|
1000	Manual switch	|
0111	Unused [c]	|
0110	Wait to restore	|
0101	Unused [c]	|
0100	Exercise	|
0011	Unused [c]	|
0010	Reverse request	|
0001	Do not revert	|
0000	No request	Lowest

a. An SF condition on the protection section is higher priority than any of the requests that would cause a working channel to be selected from the protection section.
b. Only the null signal (0), i.e. the protecting channel, is allowed with a lockout of protection request.
c. Some network operators may use these codes for network specific purposes. The receiver is capable of ignoring these codes.

In the bidirectional MSP mode it is possible to indicate locally the requests issued by the remote interface. This information is transmitted via the K1/K2 bytes in the SOH.

Beside the signal requests and external requests there is a protocol failure which can actuate a protection switching. FOP (failure of protocol) is available only for the bidirectional MSP mode. The FOP switchover has a higher priority than all the other requests above.

Failure of protocol:

- Failure of protocol (FOP) driven switchover
  If the protocol in the protecting channel fails, the system generates a FOP failure and switches the traffic signal to the working channel.
  For example, the FOP failure (alarm) is generated if a switch command issued from an interface in bidirectional MSP mode receives no answer from the remote interface that operates in unidirectional MSP mode.

Please note:

The protocol for the bidirectional protection mode is always running on the protecting channel (channel 0).

Please note:

When using the DCC in the regenerator and/or multiplex section overhead for ECC, please note that

→ MSP affects payload traffic only. The channels in the SOH are not protected with the configuration of MSP.

→ Accordingly, the MSP maintenance functions do not affect the channels in the SOH.

→ the ECC, transported in the DCC bytes, is taken from the unprotected side, i.e. protection of the ECC is done in the management communication network. Note that this doubles the required capacity on the PBUS.

5.8.2 Subnetwork Connection Protection SNCP/N

NUSA1 supports non-intrusively monitored subnetwork connection protection (SNCP/N) for trails terminated on the unit. SNCP/N protects against server failures, disconnected matrix connections (via unequipped signal detection) and mis-connections (via TTI mismatch supervision).

The EoS application terminates the VC-4, VC-3 and VC-12.

The PBUS application (P12) terminates the VC-4 and VC-12.

SNCP/N is supported for VC-4, VC-3 and VC-12. SNCP/N can be enabled on any VC pairs.

Please note:

The number of SNCP protected VC-n connections is limited to 255.

SNCP/N provides the following functions:

- 1+1 unidirectional protection mode according to ITU-T G.841, § 8.
  - The NUSA1 unit selects the received signal from one of the two VCs and switches to the other VC if this signal fails.
  - 1+1 unidirectional protection switching uses no protocol.
  - The operation type can be configured to non-revertive or revertive.
  - The working channel provides the active VC under normal operating conditions. The protecting channel protects the working channel.
  - There is no restriction about the selection of working and protecting VC.

In addition NUSA1 supports SNCP/N with bidirectional switching type and revertive or non-revertive operation type for the **PBUS application**, i.e. for VC-12 trails terminated on the unit.

This type of protection provides the following functions:

- 1+1 bidirectional protection mode.
  - The NUSA1 unit selects the received signal from one of the two VCs and switches to the other VC if this signal fails. The selector state is signalled to the remote termination function which switches its selector accordingly.
  - 1+1 bidirectional protection switching uses a proprietary protocol transported in the RFI bit of the V5[4] byte.
  - The operation type can be configured to revertive or non-revertive.
  - The working channel provides the active VC under normal operating conditions. The protecting channel protects the working channel.

- There is no restriction about the selection of working and protecting VC.

The protection parameters SNCP “wait to restore time”, “hold off time” and “guard time” are configurable per VC type on the unit configuration layer. Please refer to section 8.2.3.1 AP: / unit-x, Configuration - General - SNCP Times (on page 166).

When cross connections in NUSA1 have been protected with SNCP it is possible to check and control the status of the SNCP/N protection switch (working, protecting circuit) via the CTP status function.

In case of revertive operation type the active trail status displays if the path selector is in the WTR (wait to restore) state.

In case of bidirectional protection switching the general status dialogue displays also the path selector state from the remote end:

- Working: The remote path selector has selected the working path,
- Protecting: The remote path selector has selected the protecting path.

The APS Protocol Failure is activated when the received APS protocol state mismatches the local path selector state.

For more information on the principles of protection please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.

5.8.2.1 SNCP/N for VC-4

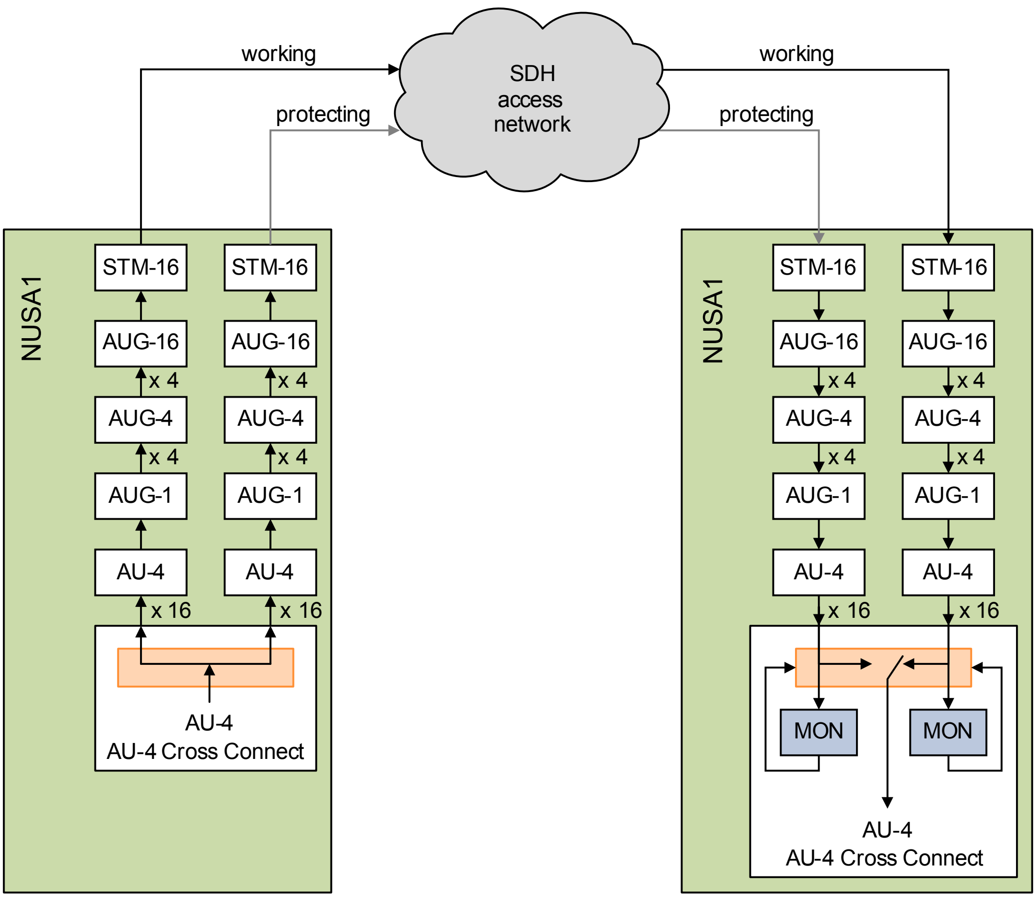


Figure 50: VC-4 SNCP/N

VC-4 protection switching takes place in the higher order cross connect (AU-4 cross connect).

Protection switching action can be driven by two different request types:

- Traffic signal requests:
  - Signal fail (SF)
    The SF state is activated if the analysis of the VC-4 traffic signal reports a signal failure:
    - AU-4 AIS,
    - AU-4 loss of pointer,
    - VC-4 unequipped,
    - TTI mismatch.
  - Signal degraded (SD)
    The SD state is activated if the analysis of the VC-4 traffic signal shows a degraded traffic signal.
- External command requests
  - Forced switch to working
  - Forced switch to protecting
  - Manual switch to working
  - Manual switch to protecting

Note that a forced switch is executed even when there is a failure on the target signal. The command is a maintenance function, i.e. it is not stored in the unit's database.

Note that a manual switch is executed only when there is no failure on the target signal. The command is a maintenance function, i.e. it is not stored in the units database.

5.8.2.2 SNCP/N for VC-3 and VC-12

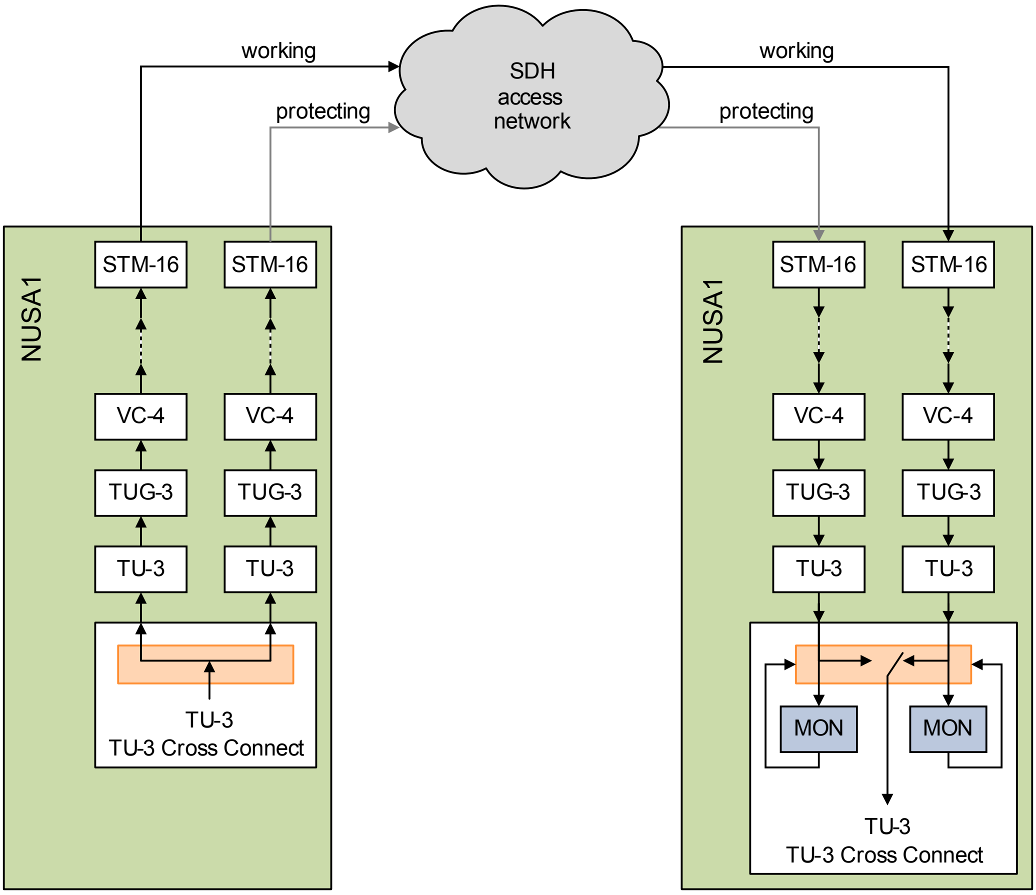


Figure 51: VC-3 SNCP/N

VC-3 and VC-12 protection switching takes place in the lower order cross connects (TU-3 cross connect and TU-12 cross connect).

Protection switching action can be driven by two different request types:

- Traffic signal requests:
  - Signal fail (SF)
    The SF state is activated if the analysis of the VC-3 or VC-12 traffic signal reports a signal failure:
    - TU-3 or TU-12 AIS,
    - TU-3 or TU-12 loss of pointer,
    - VC-3 or VC-12 unequipped,
    - TTI mismatch.
  - Signal degraded (SD)
    The SD state is activated if the analysis of the VC-3 or VC-12 traffic signal shows a degraded traffic signal.
- External command requests
  - Forced switch to working
  - Forced switch to protecting
  - Manual switch to working
  - Manual switch to protecting

Note that a forced switch is executed even when there is a failure on the target signal. The command is a maintenance function, i.e. it is not stored in the unit's database.

Note that a manual switch is executed only when there is no failure on the target signal. The command is a maintenance function, i.e. it is not stored in the units database.

5.8.3 Subnetwork Connection Protection SNCP/I

NUSA1 supports inherently monitored subnetwork connection protection (SNCP/I) for trails not terminated on the unit. SNCP/I protects against server failures.

Through connected VC-4, VC-3 and VC-12 are not terminated.

SNCP/I is supported for VC-4, VC-3 and VC-12. SNCP/I can be enabled on any VC pairs.

Please note:

The number of SNCP protected VC-n connections is limited to 255.

SNCP/I provides the following functions:

- 1+1 unidirectional protection mode according to ITU-T G.841, § 8.
  - The NUSA1 unit selects the received signal from one of the two VCs and switches to the other VC if this signal fails.
  - 1+1 unidirectional protection switching uses no protocol.
  - The operation type can be configured to non-revertive or revertive.
  - The working channel provides the active VC under normal operating conditions. The protecting channel protects the working channel.
  - There is no restriction about the selection of working and protecting VC.

The protection parameters SNCP “wait to restore time”, “hold off time” and “guard time” are configurable per VC type on the unit configuration layer. The same configuration as for SNCP/N applies.

5.8.3.1 SNCP/I for VC-4

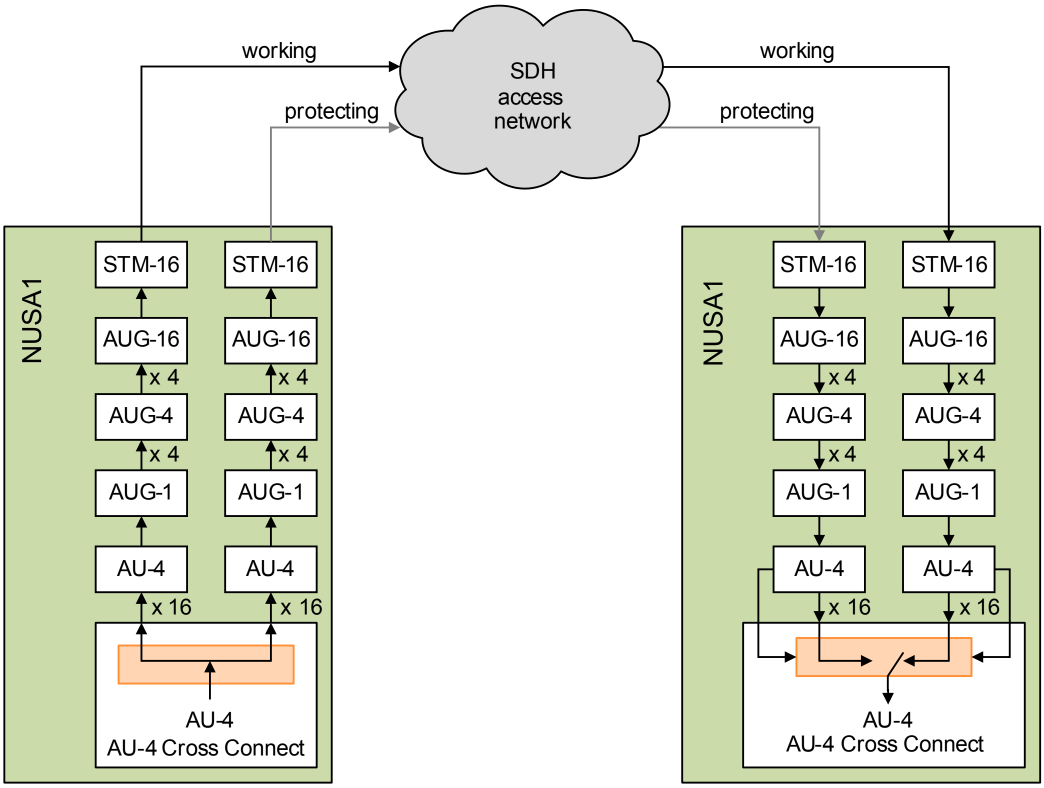


Figure 52: VC-4 SNCP/I

VC-4 protection switching takes place in the higher order cross connect (AU-4 cross connect).

Protection switching action can be driven by two different request types:

- Traffic signal request:
  - Signal fail (SF)
    The SF state is activated if the analysis of the VC-4 traffic signal reports a signal failure:
    - AU-4 AIS,
    - AU-4 loss of pointer.
- External command requests
  - Forced switch to working
  - Forced switch to protecting
  - Manual switch to working
  - Manual switch to protecting

Note that a forced switch is executed even when there is a failure on the target signal. The command is a maintenance function, i.e. it is not stored in the unit's database.

Note that a manual switch is executed only when there is no failure on the target signal. The command is a maintenance function, i.e. it is not stored in the units database.

5.8.3.2 SNCP/I for VC-3 and VC-12

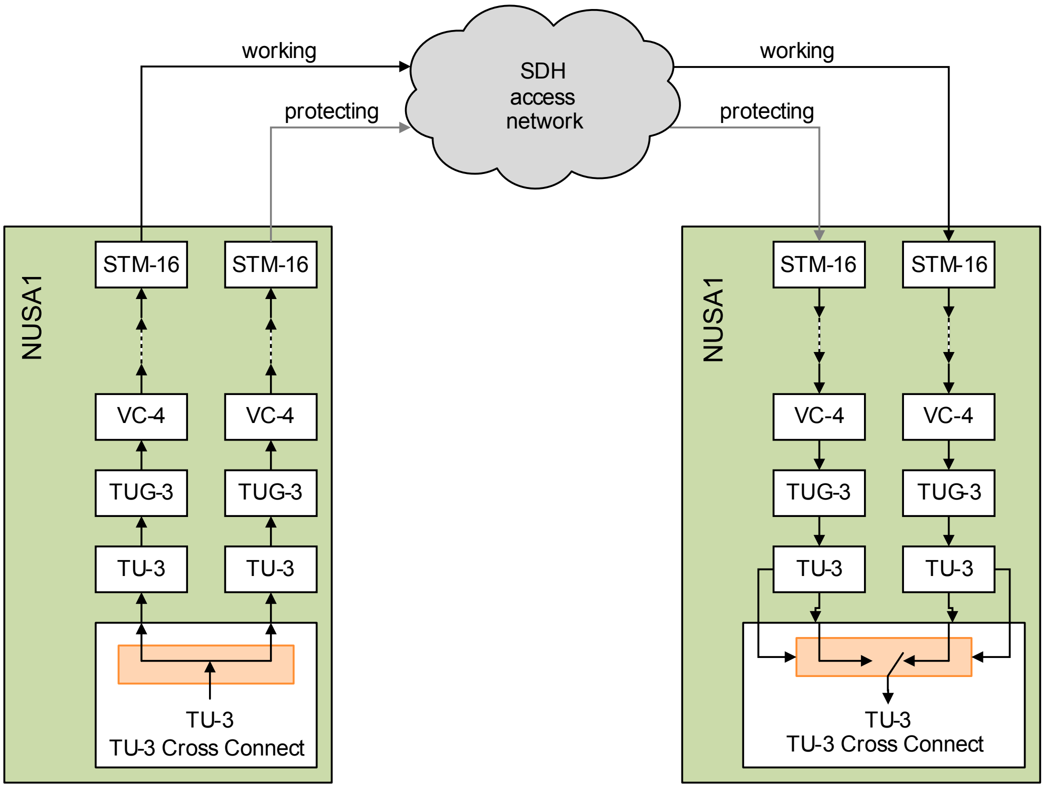


Figure 53: VC-3 SNCP/I example

VC-3 and VC-12 protection switching takes place in the lower order cross connects (TU-3 cross connect and TU-12 cross connect).

Protection switching action can be driven by two different request types:

- Traffic signal request:
  - Signal fail (SF)
    The SF state is activated if the analysis of the VC-3 or VC-12 traffic signal reports a signal failure:
    - TU-3 or TU-12 AIS,
    - TU-3 or TU-12 loss of pointer.
- External command requests
  - Forced switch to working
  - Forced switch to protecting
  - Manual switch to working
  - Manual switch to protecting

Note that a forced switch is executed even when there is a failure on the target signal. The command is a maintenance function, i.e. it is not stored in the unit's database.

Note that a manual switch is executed only when there is no failure on the target signal. The command is a maintenance function, i.e. it is not stored in the units database.

5.8.4 P12 and P0-nc Subnetwork Connection Protection SNCP

NUSA1 supports inherently monitored subnetwork connection protection (SNCP/I) for P12 and P0-nc signals.

The protection can be configured to protect P12 and P0-nc signals from the aggregate side (network side) or from the tributary side (PBUS side).

5.8.4.1 Protection from tributary side

P12 and P0-nc signals connected to one or two tributary units, e.g. SELI8, are terminated or through connected transparently. The signal state of the working and protecting signal is brought via the PBUS to the NUSA1 unit where the protection switching takes place.

SNCP/I provides the following functions:

- 1+1 unidirectional protection mode according to ITU-T G.808.1, § 11.2.
  - The NUSA1 unit selects the received signal from one of the two P12 or P0-nc signals and switches to the other P12 or P0-nc if this signal fails.
  - 1+1 unidirectional protection switching uses no protocol.
  - The operation type is revertive or non-revertive (for P0-1c only).
  - There is no restriction about the selection of working and protecting P12 or P0-nc.

In addition NUSA1 supports bidirectional switching type for terminated P12 signals.

This type of protection provides the following functions:

- 1+1 bidirectional protection mode.
  - The NUSA1 unit selects the received signal from one of the two P12 signals and switches to the other P12 signal if this signal fails. The failure state is signalled to the remote termination function with the RDI which switches its selector accordingly.
  - 1+1 bidirectional protection switching uses RDI as protection switching criterion. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20” for further information.
  - The operation type can be configured to revertive or non-revertive (non-revertive for P0-1 only).
  - The working channel provides the active P12 signal under normal operating conditions. The protecting channel protects the working channel.
  - There is no restriction about the selection of working and protecting P12 signal.

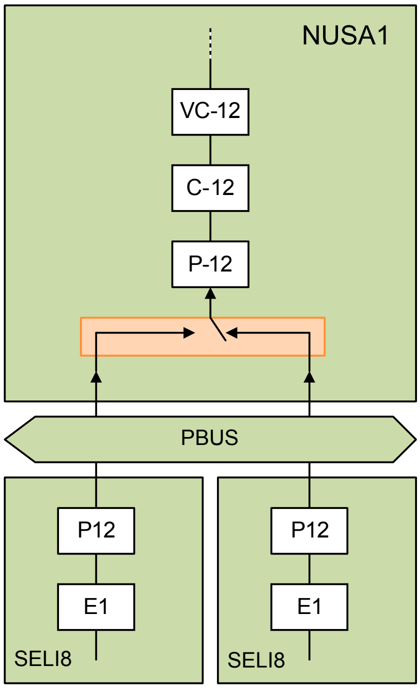


Figure 54: P12 SNCP/I from the tributary side

P12 and P0-nc protection switching takes place in the P12/P0-nc cross connect function of the PBUS access circuit.

Protection switching action can be driven by two different request types:

- Traffic signal request:
  - Signal fail (SF)
    The SF state is activated if the analysis of the P12 or P0-nc traffic signal reports a signal failure:
    - E12 loss of signal,
    - P12 AIS,
    - P12 loss of frame alignment (terminated P12 mode only),
    - P12 loss of multiframe alignment (terminated P12 mode only),
    - P12 TTI mismatch (terminated P12 mode only, future release),
    - P12 bit error ratio > 10E-3 (terminated P12 mode only).
  - Signal degraded (SD)
    The SD state is activated if the analysis of the P12 traffic signal shows a degraded traffic signal (terminated P12 mode only).
- External command requests
  - Forced switch to working
  - Forced switch to protecting
  - Manual switch to working
  - Manual switch to protecting

Note that a forced switch is executed even when there is a failure on the target signal. The command is a maintenance function, i.e. it is not stored in the unit's database.

Note that a manual switch is executed only when there is no failure on the target signal. The command is a maintenance function, i.e. it is not stored in the units database.

5.8.4.2 Protection from network side

P12 and P0-nc protection switching for signals from the network or aggregate side takes place on a tributary unit, e.g. SELI8. A P12 or P0-nc signal transported over the network is received on one or two NUSA1 units as a working and a protecting signal. The tributary unit performs the selection according to the signal states of the two signals.

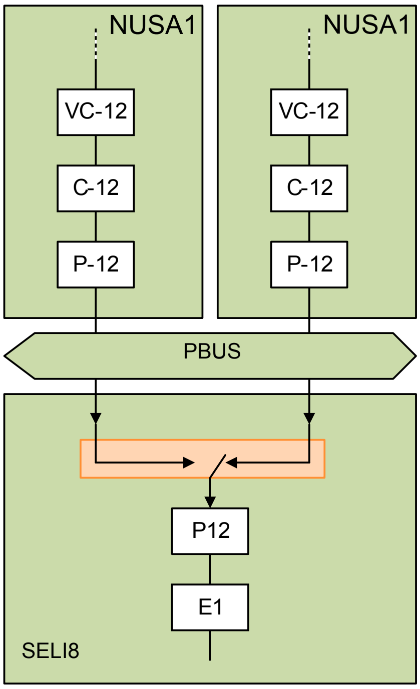


Figure 55: P12 SNCP/I from the network side with two NUSA1 units

Please note:

The protection parameters wait-to-restore time, holdoff time and guard time are not available for P12 and P0-nc SNCP.

5.8.5 Ethernet Protection

NUSA1 provides no dedicated facilities for Ethernet protection. Ethernet protection shall be done on an external Ethernet layer 2 device using an appropriate protocol (e.g. STP, RSTP).

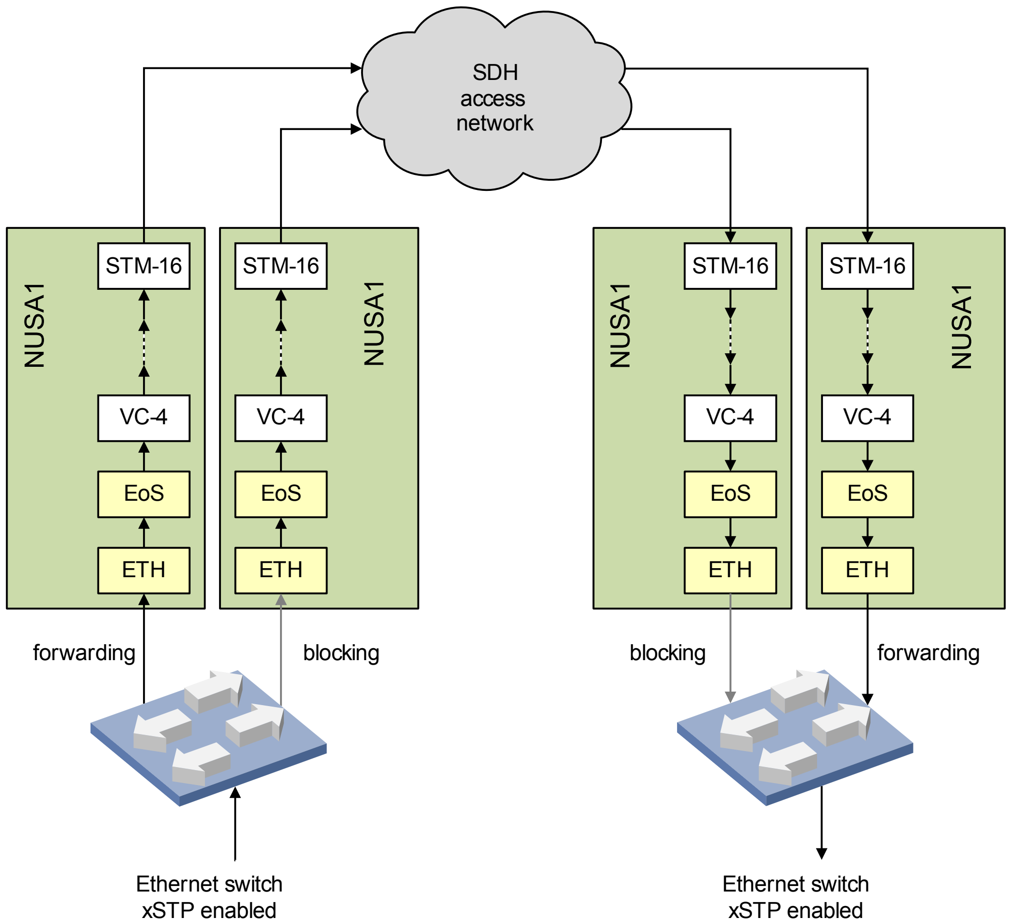


Figure 56: Ethernet protection using an Ethernet switch

Please note:

The two NUSA1 units in Figure 56 "Ethernet protection using an Ethernet switch" are **no** *equipment protected pair of units.*

5.9 Equipment Protection (EQP)

Equipment protection of the NUSA1 unit within XMC20 is only available if the working and the protecting NUSA1 units are plugged as pairs in dedicated subrack slots:

Table 28: XMC20 slot pairs for NUSA1 EQP

Network element	Working unit	Protecting unit
XMC25	slot-4	slot-6
XMC25	slot-18	slot-20
XMC23	slot-7	slot-9

Please note:

The roles of working and protecting unit is fixed within a slot pair.

Please note:

The XMC22 provides no dedicated slot pair for NUSA1 equipment protection.

After startup the working unit is the active unit and the protecting unit is the standby unit.

5.9.1 Redundancy Switch

The redundancy switch on the NUSA1 unit is placed between the SDH SFPs and the STM-1/4/16 termination circuits. It makes a connection between the SDH SFPs of the working and protecting units and the STM-1/4/16 termination circuits on the working and protecting unit via the backplane of the XMC20. There are in total four STM-16 and four STM-4 bidirectional connections.

Without EQP the connections between the working and the protecting NUSA1 units are not used.

Please note:

The Figure 57 "Redundancy switch connections, working unit is active" and the Figure 58 "Redundancy switch connections, protecting unit is active" show STM-16 and STM-4 SFP modules as an example.

→ STM-16 SFP modules can be replaced with STM-4 SFP modules.

→ STM-4 SFP modules can be replaced with STM-1 SFP modules.

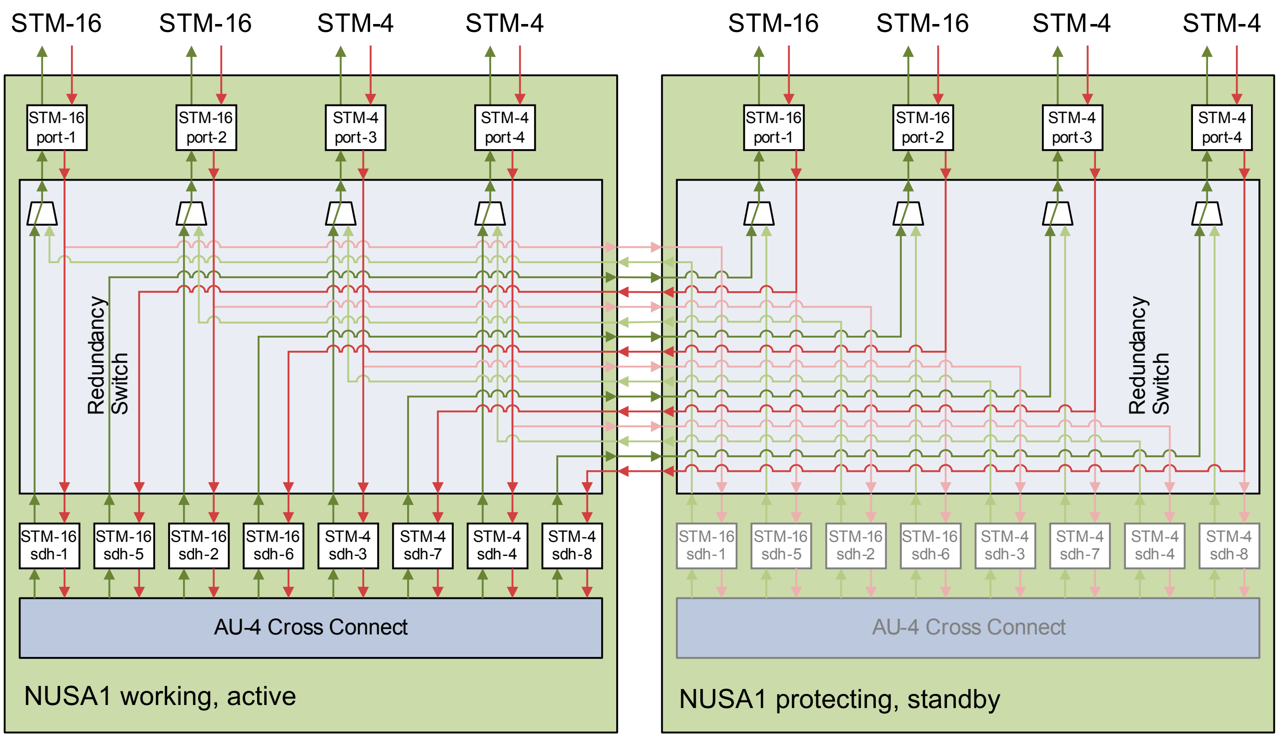


Figure 57: Redundancy switch connections, working unit is active

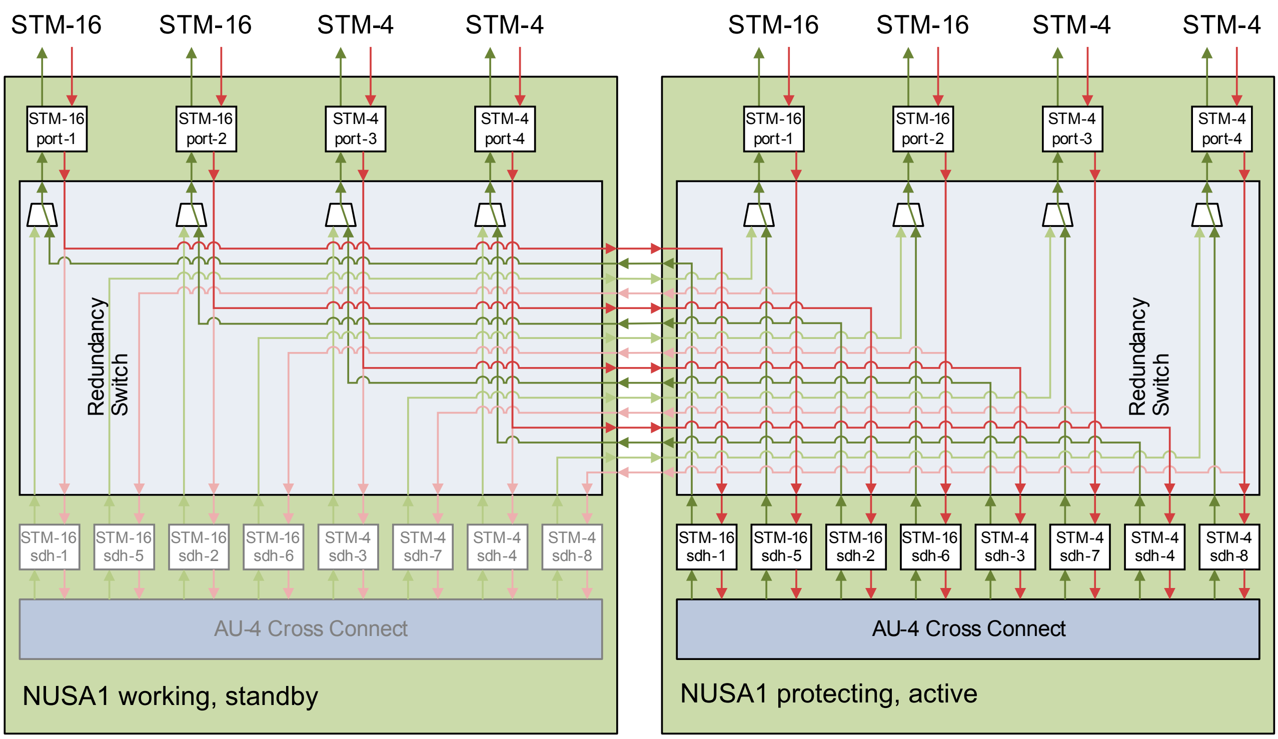


Figure 58: Redundancy switch connections, protecting unit is active

The redundancy switch on the working unit connects the physical SDH ports (SFPs) port-1 to port-4 on the working unit to the logical SDH ports sdh-1 to sdh-4 on the working and protecting unit.

The redundancy switch on the protecting unit connects the physical SDH ports (SFPs) port-1 to port-4 on the protecting unit to the logical SDH ports sdh-5 to sdh-8 on the working and protecting unit.

On the standby unit, working or protecting, the SFPs and the redundancy switch are active. The Ethernet switch as part of the XMC20 Switch and the Ethernet front ports are also active. The access circuits to the PBUS, the EoS ports and the SDH circuits are disabled.

5.9.2 EQP with SETS Protection

On an equipment protected pair of NUSA1 units the SETS function is equipment protected. This means:

- Only the SETS on the active NUSA1 unit provides the SDH timing signals.
- Only the working NUSA1 unit is available as PDH clock source in the PETS configuration on the NE level.
- Only the working NUSA1 unit is available as SDH clock source in the ESO-2 configuration on the NE level.

After a protection switch-over the SETS function on the protecting NUSA1 unit will provide the SDH timing signals, will be used as PDH clock source and will be used as source for ESO-2.

Please note:

During a protection switch-over the ESO-2 synchronization output on the COGE5 is squelched for several seconds.

5.9.3 EQP with Traffic Protection

NUSA1 equipment protection can be used together with traffic protection, i.e. path protection (MSP) or subnetwork connection protection.

Traffic protection together with equipment protection protects also against failures in the network and a failure of the SFP or redundancy switch.

5.9.3.1 PDH traffic protection

The PDH traffic accessing the PBUS is protected as follows: During normal operation, the VC-12 traffic from the west and east direction is terminated on the working unit (active), using the redundancy switch. The TU-12 cross connect selects the working or the protecting VC-12 signal from the west or east direction. The selected signal accesses the PBUS. The PBUS access on the protecting unit (standby) is disabled.

In case of a failure of the working unit, the working unit becomes the standby unit and the protecting unit becomes the active unit. The VC-12 traffic from the west and east direction is terminated on the protecting unit (active), using the redundancy switch. The TU-12 cross connect selects the working or the protecting VC-12 signal from the west or east direction. The selected signal accesses the PBUS. The PBUS access on the working unit (standby) is disabled.

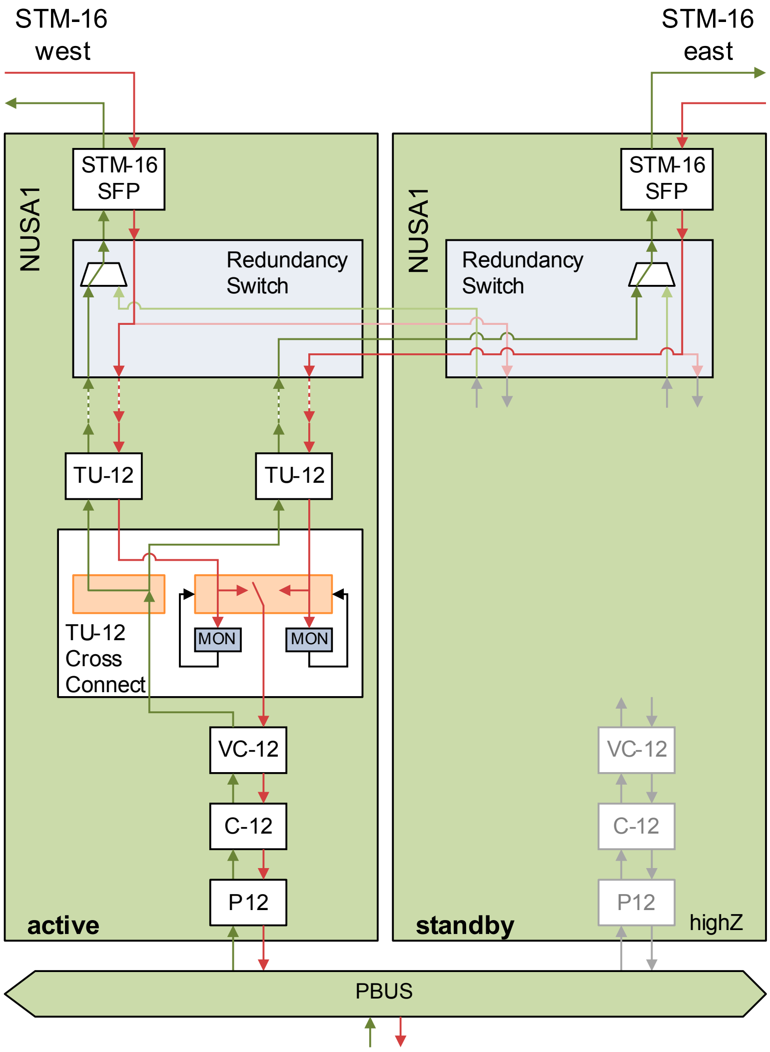


Figure 59: Equipment protection for PDH traffic

5.9.3.2 Ethernet traffic protection over EPL ports

The Ethernet traffic accessing the Ethernet front ports in the unswitched port handling mode is protected as follows: During normal operation, the EoS VC-4, VC-3, and VC-12 traffic from the west and east direction is terminated on the working unit (active), using the redundancy switch. The terminated signal is forwarded to the Ethernet port. The Ethernet ports on the protecting unit (standby) remain active, but the forwarding of packets is disabled.

In case of a failure of the working unit, the working unit becomes the standby unit and the protecting unit becomes the active unit. The EoS VC-4, VC-3, and VC-12 traffic from the west and east direction is terminated on the protecting unit (active), using the redundancy switch. The terminated signal is forwarded to the Ethernet port. The Ethernet ports on the working unit (standby) remain active, but the forwarding of packets is disabled.

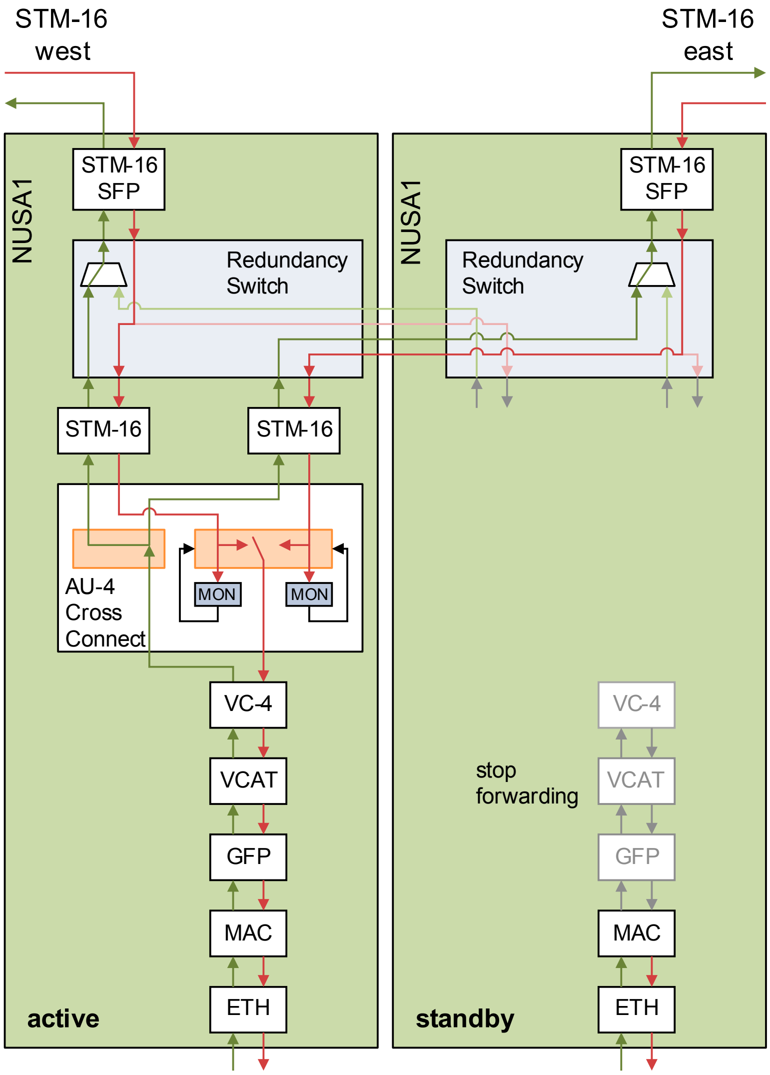


Figure 60: Equipment protection for unswitched Ethernet traffic (VC-4 EoS)

Please note:

The Ethernet ports used on the working and the protecting NUSA1 units must be both set to the administrative state “up”.

Please note:

The EPL handling on the working and the protecting NUSA1 units must be configured identically.

Please note:

The EoS ports used for the EPL application on the working and the protecting NUSA1 units must be configured identically (port mode = unswitched) in the bridge port configuration in the ECST “Switching” view.

Please note:

Both Ethernet front ports of the working and the protecting unit can be connected to the same Ethernet switch.

→ xSTP is not required since the Ethernet front port on the standby unit is not in the forwarding state.

Please note:

During a protection switching event the user traffic is interrupted for up to 8 s.

5.9.3.3 Ethernet traffic protection over switched ports

The Ethernet traffic accessing the Ethernet front ports in the switched port handling mode is protected as follows: During normal operation, the EoS VC-4, VC-3, and VC-12 traffic from the west and east direction is terminated on the working unit (active), using the redundancy switch. The terminated signal is forwarded to the XMC20 Switch and can be accessed at any Ethernet front port which is attached to XMC20 Switch. The example in Figure 61 "Equipment protection for switched Ethernet traffic (VC-4 EoS)" shows the external Ethernet front port located on the working NUSA1 unit. The Ethernet front ports on the standby unit are not used.

In case of a failure of the working unit, the working unit becomes the standby unit and the protecting unit becomes the active unit. The EoS VC-4, VC-3, and VC-12 traffic from the west and east direction is terminated on the protecting unit (active), using the redundancy switch. The terminated signal is forwarded to the XMC20 Switch and can still be accessed at the Ethernet front port on the working unit (standby). This scenario requires no external Ethernet switch, but relies on an operational switch circuit and Ethernet port on the standby NUSA1 unit.

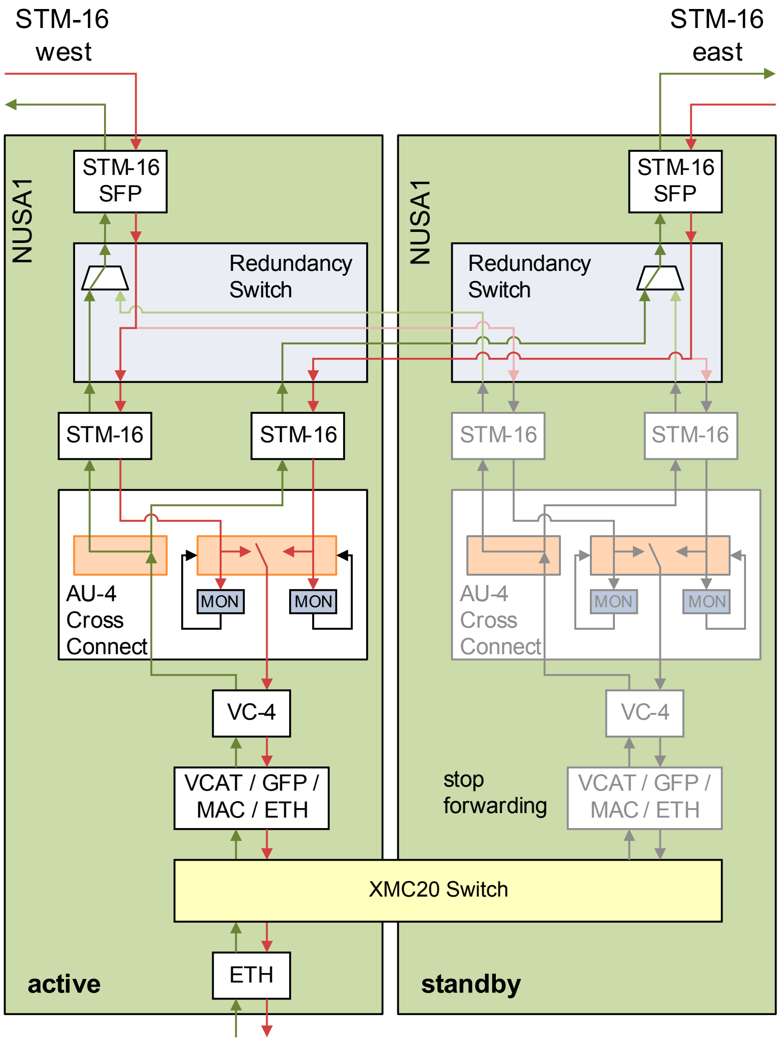


Figure 61: Equipment protection for switched Ethernet traffic (VC-4 EoS)

Please note:

The two EoS ports on the working and the protecting NUSA1 units are both attached to the XMC20 Switch. One EoS port is active, the other is standby, but both EoS ports are available as bridge ports in the ECST “Switching” view.

→ The bridge port configuration (port mode, PVID, VLANs, …) must be configured identically for both ports.

Please note:

During a protection switching event the user traffic is interrupted for up to 8 s.

5.9.4 EQP Prerequisites

To enable equipment protection for the NUSA1 unit some prerequisites must be met:

- The protecting NUSA1 unit must be plugged in one of the dedicated protecting unit slots of the XMC20 subrack.
- The protecting NUSA1 unit must be in the unassigned state. Otherwise the unit will not be selectable in the EQP configuration in AP: /unit-x, Configuration - EQP: Create Group…, EQP Group Creation, Protecting Unit.
- The protecting unit must be hardware compatible with the working unit. Check the hardware compatibility status after the EQP group configuration in the AP: /unit-x, Status - EQP: Units Status, HW Compatible.
  The following requirements must be fulfilled that the two units are stated as hardware compatible:
  - Identical unit function. The unit function is composed of the 5 first characters of the unit name, e.g. NUSA1. The unit name is available at the AP:/ Main - Equipment, Unit.
  - Identical board identification, e.g. 383. The board identification is available at the AP:/ Main - Inventory, Board ID.
  - Identical hardware variant. The hardware variant is the truncation of the hardware key divided by 256, e.g. 1/256 = 0. The hardware key is available at the AP:/ Main - Inventory, Hardware Key.
- The protecting unit must be software compatible with the working unit. Check the software compatibility status after the EQP group configuration in the AP: /unit-x, Status - EQP: Units Status, SW Compatible.
  The following requirements must be fulfilled that the two units are stated as software compatible:
  - Identical unit function. The unit function is composed of the 5 first characters of the software name, e.g. nusa1. The unit name is available at the AP:/ Main - Equipment, Software.

  In order to guarantee the full compatibility of all features it is strongly recommended to use the same software on the working and on the protecting unit.
  The compatible software must be installed on the NUSA1 unit before the EQP group creation.
- The unit configuration of an equipment protection group is mainly done on the active unit.
- The standby unit requires the configuration of the following items:
  - Physical SDH front ports:
    All SFP related parameters must be configured.
    The ports must be in the administrative state “up”.
  - Physical Ethernet front ports:
    All PHY parameters must be configured.
    The ports must be in the administrative state “up”.
  - Bridge ports of the XMC20 Switch (VLAN Bridge function):
    The EoS ports and, if used, the Ethernet front ports attached to the XMC20 Switch must be configured in the “Tree View” and “Switching” view of the ECST.
  - PWAC ports of the XMC20 Switch (MPLS-TP VPWS Transport function):
    The EoS ports and, if used, the Ethernet front ports attached to the XMC20 Switch must be configured in the “Tree View” view of the ECST.
  - SETS:
    No SETS parameters must be configured. The SETS parameters of the working unit are applied to the protecting unit after a switch-over.

In the PETS and ESO configuration on the NE only the working NUSA1 unit is available as PDH clock source.
All other items on the standby unit are not configurable.

Risk of operating trouble!

The configuration of an equipment protection group must be saved (ECST NE menu or ECST tool bar: Save to NE).

→ Otherwise, in case of a protection switch event, the NE will load an outdated configuration from the internal configuration database and the NE configuration will be corrupted.

5.9.5 EQP Configuration

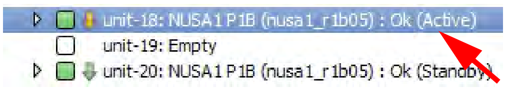
The working NUSA1 unit of an EQP group is assigned and configured the same way as a stand alone NUSA1 unit.

The protecting NUSA1 unit is running with the same ESW as the working unit and must be in the unassigned state.

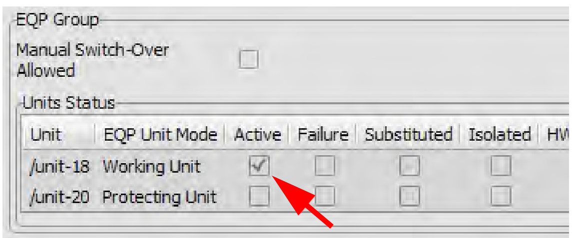
The 1:1 equipment protection group is configured on the working unit:

- AP: /unit-x, Configuration - EQP.
  - Execute the command “Create EQP Group…”.
  - Select the Protecting unit, e.g. /unit-6.
  - Execute “OK”.
- Configure the protecting unit according to the list given in section EQP Prerequisites:
  - Physical SDH ports.
  - Physical Ethernet ports.
  - XMC20 Switch ports and VLANs.
  - SETS.
- Configure all required TDM cross connections with the involved CTPs on the working unit which must also be the active unit.
- Save the NE configuration.

Further on any changes on the NUSA1 configuration, except ports and cross connections, must be done on the active unit. To find out which unit is the active unit check the AP tree



or the unit status of the working or protecting NUSA1 unit.



Please note:

The TDM cross connections on the NUSA1 unit must be created on the working unit. The working unit must also be the active unit.

Please note:

The TDM cross connections on the NUSA1 unit always use the MO addresses of the working unit.

5.9.6 EQP Status

The unit status of the working and protecting units shows the actual status of the units belonging to the equipment protection group. The unit status offers also the commands for the EQP manipulation:

- Manual switch-over
  The currently standby unit is set as active unit and the currently active unit is set as standby unit. This requires that the currently standby unit is in operational state, i.e.
  - has no failure,
  - is not isolated.

  A manual switch is possible if it is indicated with the “Manual Switch-Over Allowed” parameter.
  Note that this command can only be activated on the working unit status dialogue.
- Forced switch-over
  The currently standby unit is set as active unit, independent of the operational state of the currently standby unit.
  Note that there is a risk that the user traffic will be permanently interrupted if the currently standby unit is not operational.
  The currently active unit is set as standby unit.
  Note that this command can only be activated on the working unit status dialogue.
- Isolate unit
  To be able to perform a maintenance action, e.g. update of the embedded software, on an active unit without activating a protection switchover, the working unit can be isolated. This means that the protection switching state machine is frozen and no protection switch will be done until the isolation of the unit is removed.
  Note that the isolate unit command can only be applied to the working unit.
- Join unit
  Remove the isolation of a previously isolated unit.
  Note that the join unit command can only be applied to the working unit.

The table in the EQP status dialogue displays the following items. Please refer also to section 8.2.6.5 AP: / unit-x, Status - EQP (on page 188):

- Unit
  MO address of the unit belonging to the EQP group.
- EQP unit mode
  The working unit is the unit where the protection group has been configured.
  The protecting unit is the unit that has been set to the unassigned state before configuring the protection group.
- Active
  Active true means the unit is the active unit, i.e. it is the operational unit.
  Active false means the unit is the standby unit, i.e. it is not the operational unit.

The active state can be changed with the “Manual Switch” and “Forced Switch” commands.

- Failure
  Failure true means the unit is in a failure state.
  Failure false means the unit is not in a failure state.
  The failure state can not be changed manually.
- Substituted
  Substituted true on the working unit means the unit has been substituted by the protecting unit. A substituted unit is also in the “active false” state.
  Substituted false on the working unit means the unit has not been substituted, i.e. it is the active unit or it has been isolated.
  The substituted state of the protecting unit is always false.
- Isolated
  Isolated true means the unit has been isolated with the “Isolate Unit” command.
  Isolated false means the unit is not isolated.
  The isolation state can be changed with the “Isolate Unit” and “Join Unit” commands.
  The isolated state of the protecting unit is always false.
- HW Compatible
  HW compatible true means the working HW unit is compatible with the protecting HW unit.
  HW compatible false means the working HW unit is not compatible with the protecting HW unit. Equipment protection is not possible.
- SW Compatible
  SW compatible true means the working unit embedded software (ESW) is compatible with the protecting unit ESW.
  SW compatible false means the working unit ESW is not compatible with the protecting unit ESW. Equipment protection is not possible.
- DB Saved
  DB saved true means the current configuration of the working and protecting unit has been saved to the XMC20 internal database.
  DB saved false means the current configuration of the working or protecting unit has not been saved to the XMC20 internal database. A protection switching event will load an outdated configuration and traffic will be disturbed.

6 Commissioning

This section describes the management of the basic system functions of the NUSA1 unit and the configuration of the PDH and EoS transport.

Please refer to [355] User Manual “ECST” for details on the general GUI aspects, and refer to [302] User Guide “XMC25/XMC23/XMC22” for specific characteristics of the XMC20.

6.1 Cross Connections

The NUSA1 unit implements three cross connect functions, an AU-4 cross connect, a TU-3 cross connect and a TU-12 cross connect. All signals that are cross connected through the NUSA1 unit must pass either the AU-4 cross connect or the AU-4 and TU-3 or TU-12 cross connects.

Accordingly only traffic signal cross connections on the VC-4 layer can be configured in a single step. Traffic signal cross connections on the VC-3 and VC-12 layers are configured in two steps, cross connections on the P12 and P0-nc layers must be configured in three steps.

An exception is the DCC which can be cross connected in one step to a channel on the COGE5 unit.

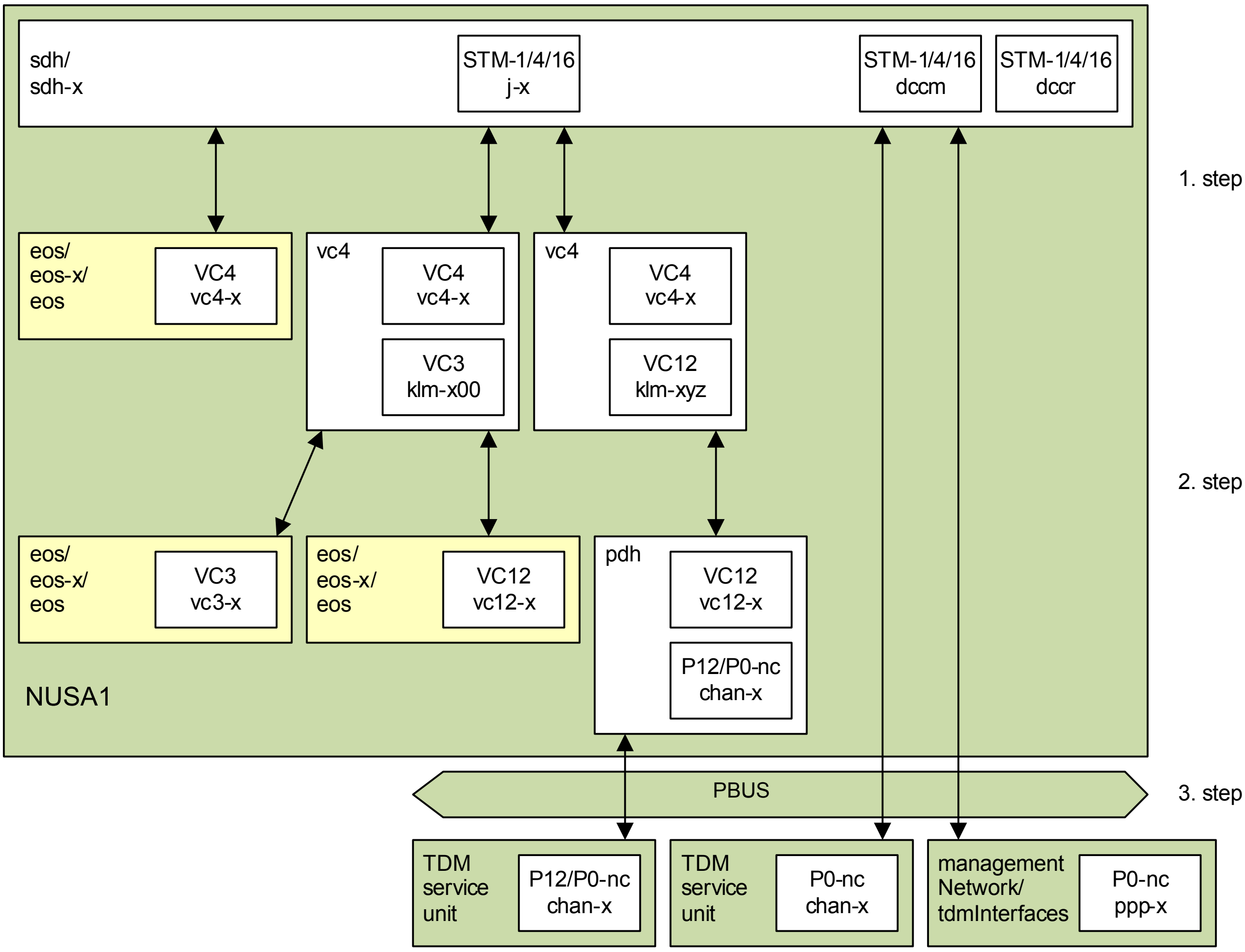


Figure 62: Cross connection overview

The figure below shows all cross connections on the NUSA1 unit. These cross connections are described in detail in the following sections.

Please note:

In the figure below all items “Ethernet switch/port” stand for a NUSA1 Ethernet front port or for a VLAN bridge Ethernet port.

Please note:

In all figures and all tables of this section the numbering of the ports, SDH, PDH and Ethernet signals uses the same characters on both sides of a connection.
Despite of this the numbering needs not to be identical, e.g. a VC-12 signal designated “vc4/vc4-1/klm-121” can be cross connected to another VC-12 signal designated “vc4/vc4-5/klm-372”.

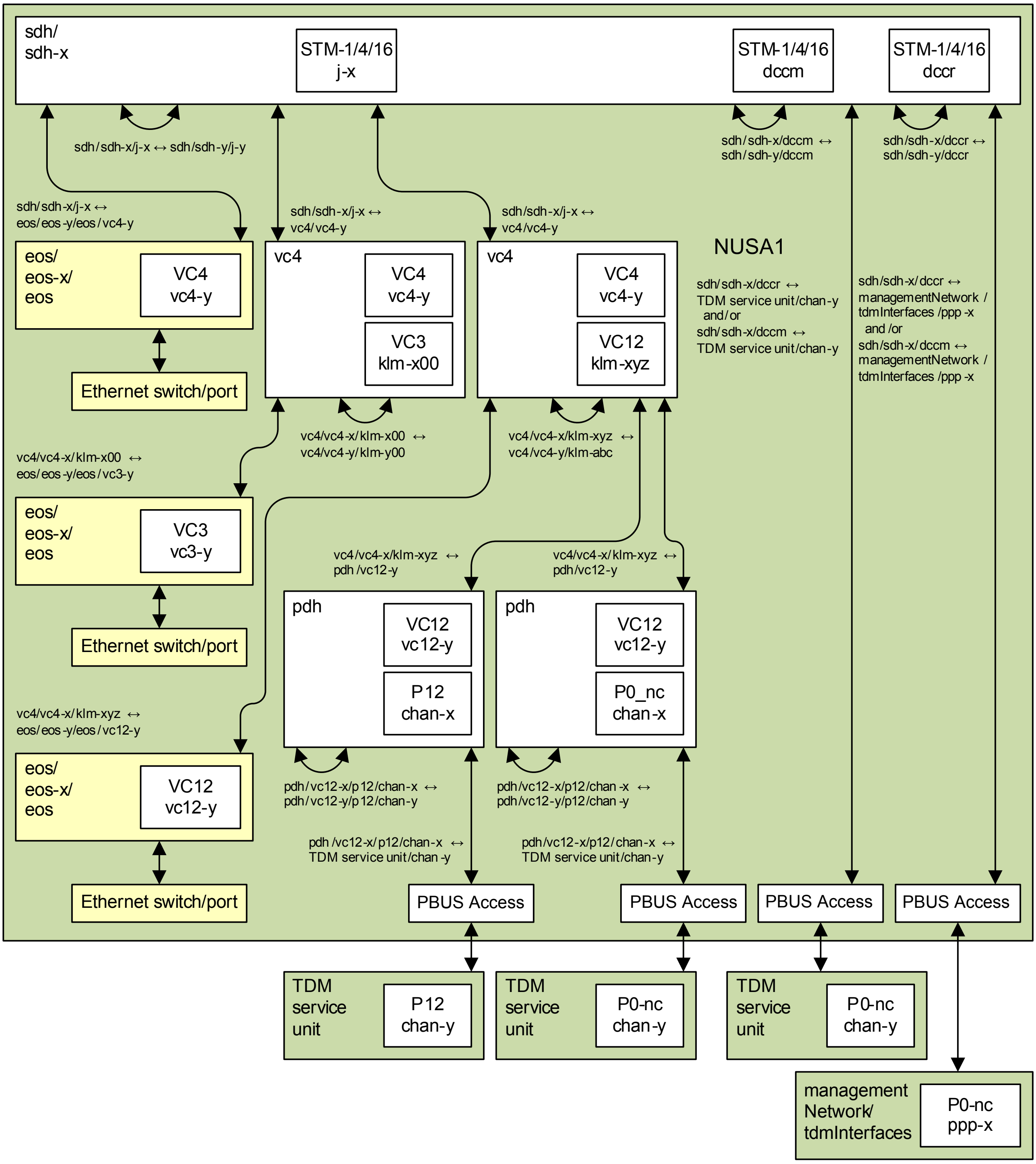


Figure 63: Cross connection detail view

6.1.1 VC-4 Cross Connections

VC-4 cross connections can only be done on a single NUSA1 unit. There is no way to access a VC-4 signal on another SDH unit.

Please note:

Cross connections related to the physical SDH ports located on a protecting NUSA1 unit are handled as if these ports were located on the working NUSA1 unit, i.e. the logical SDH ports managed objects are available on the working NUSA1 unit.

VC-4 resources on the NUSA1 unit are available as follows:

- STM-16, STM-4 or STM-1 port resources are available in the “/unit-x/sdh/sdh-x” access points.
- VC-4 resources used for the lower layers (VC-3, VC-12, P12, P0-nc) must be created in the “/unit-x/vc4” configuration.
- EoS resources (VCG members) must be created in the “/unit-x/eos/eos-x/eos” configuration.

On the VC-4 layer in NUSA1 the following signal types are available:

- /unit-x/sdh/sdh-y/j-z, e.g. /unit-4/sdh/sdh-1/j-1:
  y = 1 to 4 (physical SDH port number 1 to 4 on the working NUSA1 unit)
  y = 5 to 8 (physical SDH port number 1 to 4 on the protecting NUSA1 unit)
  z = 1 (AU-4 number of STM-1), or
  z = 1 to 4 (AU-4 number of STM-4), or
  z = 1 to 16 (AU-4 number of STM-16)
  The maximum number of available AU-4 in NUSA1 is 80, when using NUSA1 equipment protection with two STM-4 ports and two STM-16 ports on both units.
- /unit-x/vc4/vc4-y, e.g. /unit-4/vc4/vc4-1:
  y = 1 to 31 (VC-4 number)
  vc4-y are internal resources of the NUSA1 unit. The maximum number of available VC-4 with a TUG-3 structure in NUSA1 is 31.
  The maximum number of available VC-3 in a terminated VC-4 is 48.
  The maximum number of available VC-12 in a terminated VC-4 is 945.
  There is no restriction for the TUG-3 structure, i.e. any mixture of VC-3 and VC-12 is configurable.
- /unit-x/eos/eos-y/eos/vc4-z, e.g. /unit-4/eos/eos-1/eos/vc4-1:
  y = 1 to 32 (EoS port number)
  z = 1 to 14 (VCG member number)
  The maximum number of available EoS VC-4 members on the NUSA1 unit and in a virtual concatenation group is 14.

Please note:

The EoS capacity of 14 VC-4 must be shared between the EoS VC-4 members and the EoS VC-3 members.

Please note:

The total EoS capacity of is reduced to 12 VC-4 if also EoS VC-12 members are configured:

→ Up to 8 VC-4 equivalents for VC-4 and VC-3 members,
→ Up to 4 VC-4 equivalents for VC-12 members.

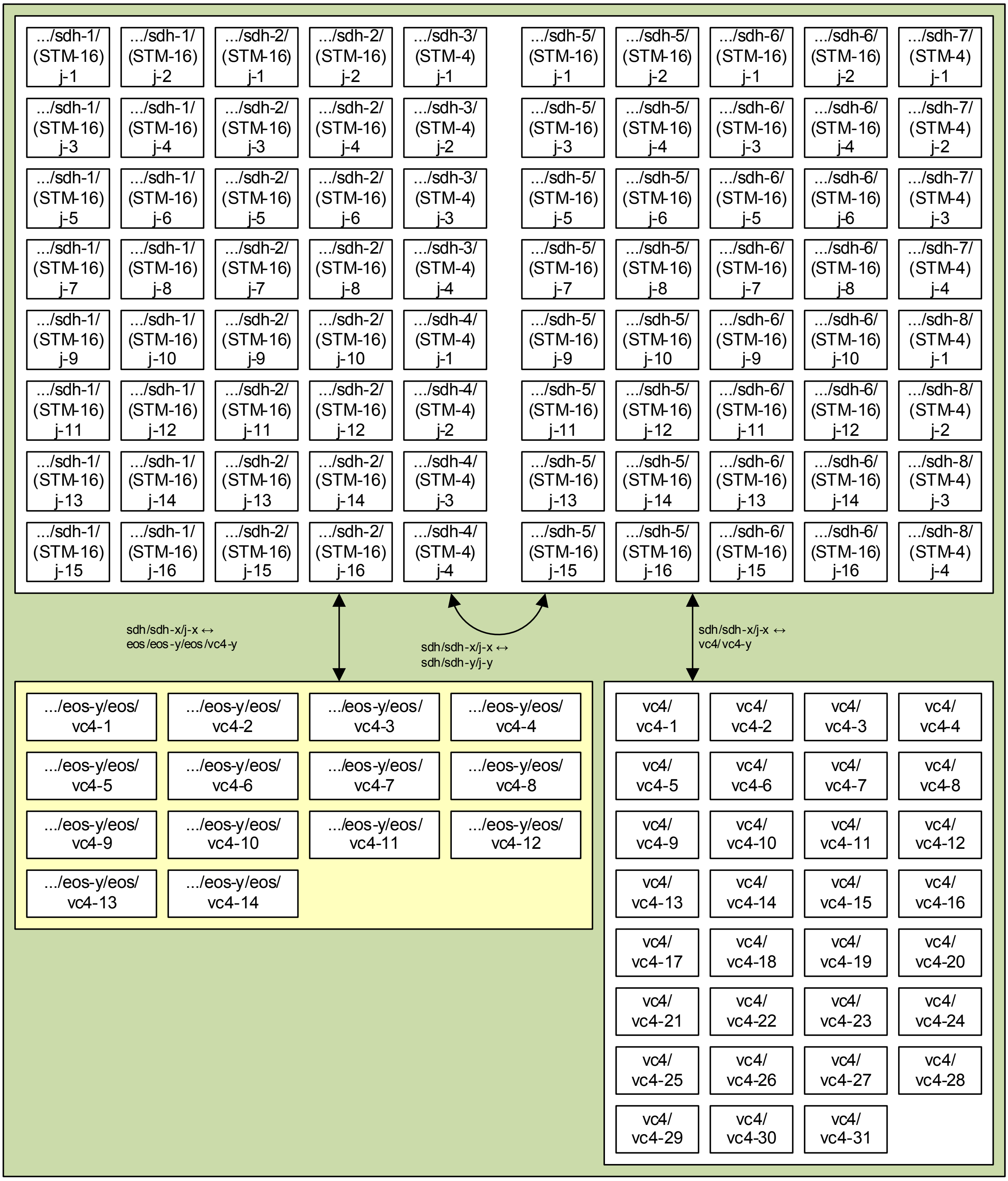


Figure 64: Cross connections in the VC-4 layer

Please note:

The logical SDH ports sdh-5 to sdh-8 are only available with equipment protection of the NUSA1 unit, i.e. using a working and a protecting NUSA1 unit.

The following unidirectional and bidirectional cross connections are configurable:

Table 29: VC-4 layer cross connections

a-End	z-End	Cross connection
/sdh/sdh-x/j-x	/sdh/sdh-y/j-y	Connects a VC-4 signal from an SDH port to itself or to another VC-4 signal on an SDH port. This cross connection is used for through connected VC-4 signals or can be used for maintenance purposes. i.e. to loop a VC-4 back towards the SDH port using a unidirectional cross connection. There is no restriction in the number of through connected VC-4.
/sdh/sdh-x/j-x	/vc4/vc4-y	Connects a VC-4 signal from an SDH port to an internal VC-4. This cross connection is used for terminating signals below the VC-4 layer, i.e. signals of the VC-3 or VC-12 layer. The maximum number of terminated VC-4 is 31.
/vc4/vc4-x	/sdh/sdh-y/j-y	Connects a VC-4 signal from an internal VC-4 to an SDH port. This cross connection is used for terminating signals below the VC-4 layer, i.e. signals of the VC-3 or VC-12 layer. The maximum number of terminated VC-4 is 31.
/sdh/sdh-x/j-x	/eos/eos-y/eos/vc4-y	Connects a VC-4 signal from an SDH port to an EoS VC-4 member. This cross connection is used for Ethernet transport over virtually concatenated or non concatenated VC-4. The maximum number of terminated VC-4 is 14, including the number of VC-4 used for the EoS VC-3 members. The maximum number of terminated VC-4 is 12, including the number of VC-4 used for the EoS VC-3 and 252 VC-12 members.
/eos/eos-x/eos/vc4-x	/sdh/sdh-y/j-y	Connects a VC-4 signal from an EoS VC-4 member to an SDH port. This cross connection is used for Ethernet transport over virtually concatenated or non concatenated VC-4. The maximum number of terminated VC-4 is 14, including the number of VC-4 used for the EoS VC-3 members. The maximum number of terminated VC-4 is 12, including the number of VC-4 used for the EoS VC-3 and 252 VC-12 members.

In the VC-4 layer the following SNC protections can be configured:

Table 30: VC-4 layer protection cross connections

a-End working	a-End protecting	z-End	Protection
/sdh/sdh-x/j-x	/sdh/sdh-y/j-y	/sdh/sdh-z/j-z	Protects an outgoing VC-4 signal by two incoming VC-4 signals from one or two SDH ports. This cross connection is used for protected VC-4 through traffic.
/sdh/sdh-x/j-x	/sdh/sdh-y/j-y	/vc4/vc4-z	Protects an internal VC-4 by two incoming VC-4 signals from one or two SDH ports. This cross connection is used for protected terminating signals below the VC-4 layer, i.e. signals of the VC-3 or VC-12 layer.
/sdh/sdh-x/j-x	/sdh/sdh-y/j-y	/eos/eos-z/eos/vc4-z	Protects an EoS VC-4 member by two incoming VC-4 signals from one or two SDH ports. This cross connection is used for protected Ethernet transport over virtually concatenated or non concatenated VC-4.

6.1.2 VC-3 Cross Connections

VC-3 cross connections on NUSA1 are used for Ethernet access and for through connected VC-3 traffic.

VC-3 cross connections can only be done on a single NUSA1 unit. There is no way to access a VC-3 signal on another SDH unit.

VC-3 resources on the NUSA1 unit are available as follows:

- VC-3 resources belonging to an internal VC-4 must be created in the "/unit-x/vc4/vc4-y" configuration.
- EoS resources (VCG members) must be created in the "/unit-x/eos/eos-y/eos" configuration.

On the VC-3 layer in NUSA1 the following signal types are available:

- /unit-x/vc4/vc4-y/klm-z00, e.g. /unit-4/vc4/vc4-1/klm-100:
  y = 1 to 31 (VC-4 number)
  z = 1 to 3 (TU-3 number)
  vc4-y/klm-z00 are all VC-3 signals handled in the TU-3 cross connect of the NUSA1 unit. The maximum number of available VC-3 in NUSA1 is 48.

Please note:

All VC-3 signals used for through connected VC-3 traffic or used for EoS transport must pass the TU-3 cross connect of the NUSA1 unit.

→ When using 24 VC-3 for EoS traffic no capacity is left for through connected traffic.

- /unit-x/eos/eos-y/eos/vc3-z, e.g. /unit-4/eos/eos-5/eos/vc3-1:
  y = 1 to 32 (EoS port number)
  z = 1 to 24 (VCG member number)
  The maximum number of available EoS VC-3 members on the NUSA1 unit and in a virtual concatenation group is 24.

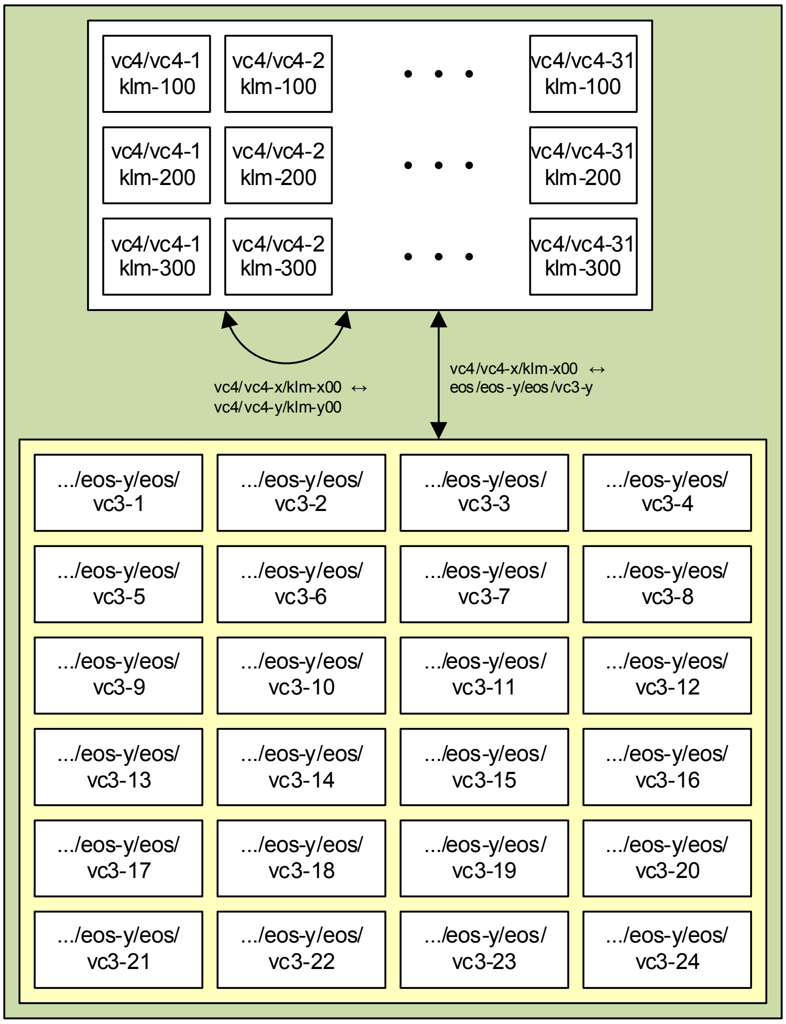


Figure 65: Cross connections in the VC-3 layer

Please note:

The EoS capacity of 14 VC-4 must be shared between the EoS VC-4 members and the EoS VC-3 members.

Please note:

The total EoS capacity of is reduced to 12 VC-4 if also EoS VC-12 members are configured:

→ Up to 8 VC-4 equivalents for VC-4 and VC-3 members,

→ Up to 4 VC-4 equivalents for VC-12 members.

The following unidirectional and bidirectional cross connections are configurable:

Table 31: VC-3 layer cross connections

a-End	z-End	Cross connection
/vc4/vc4-x/klm-x00	/vc4/vc4-y/klm-y00	Connects a VC-3 to itself or to another VC-3 signal. This cross connection is used for through connected VC-3 signals or can be used for maintenance purposes. i.e. to loop a VC-3 back towards the internal VC-4 using a unidirectional cross connection.

Table 31: VC-3 layer cross connections (continued)

a-End	z-End	Cross connection
/vc4/vc4-x/klm-x00	/eos/eos-y/eos/vc3-y	Connects a VC-3 signal from an internal VC-4 to an EoS VC-3 member. This cross connection is used for Ethernet transport over virtually concatenated or non concatenated VC-3. The maximum number of terminated VC-3 is 24.
/eos/eos-x/eos/vc3-x	/vc4/vc4-y/klm-y00	Connects a VC-3 signal from an EoS VC-3 member to an internal VC-4. This cross connection is used for Ethernet transport over virtually concatenated or non concatenated VC-3. The maximum number of terminated VC-3 is 24.

In the VC-3 layer the following SNC protections can be configured:

Please note:

The working and the protecting path of an SNC protected connection must be located on the same NUSA1 unit or on an equipment protected pair of NUSA1 units.

Table 32: VC-3 layer protection cross connections

a-End working	a-End protecting	z-End	Protection
/vc4/vc4-x/klm-x00	/vc4/vc4-y/klm-y00	/vc4/vc4-z/klm-z00	Protects an outgoing VC-3 by two incoming VC-3 signals from one or two internal VC-4. This cross connection is used for protected through connected VC-3 signals.
/vc4/vc4-x/klm-x00	/vc4/vc4-y/klm-y00	/eos/eos-z/eos/vc3-z	Protects an EoS VC-3 member by two incoming VC-3 signals from one or two internal VC-4. This cross connection is used for protected Ethernet transport over virtually concatenated or non concatenated VC-3.

6.1.3 VC-12 Cross Connections

VC-12 cross connections on NUSA1 can be used for Ethernet access, for PBUS access and for through connected VC-12 traffic.

VC-12 cross connections can only be done on a single NUSA1 unit. There is no way to access a VC-12 signal on another SDH unit.

VC-12 resources on the NUSA1 unit are available as follows:

- VC-12 resources belonging to an internal VC-4 must be created in the "/unit-x/vc4/vc4-y" configuration.
- EoS resources (VCG members) must be created in the "/unit-x/eos/eos-y/eos" configuration.
- VC-12 resources for the PBUS access are all available in the "/unit-x/pdh" access point.

On the VC-12 layer in NUSA1 the following signal types are available:

- /unit-a/vc4/vc4-b/klm-xyz, e.g. /unit-4/vc4/vc4-1/klm-121:
  b = 1 to 31 (VC-4 number)
  x = 1 to 3 (TUG-3 number)
  y = 1 to 7 (TUG-2 number)
  z = 1 to 3 (TU-12 number)

vc4-y/klm-xyz are all VC-12 signals terminated or through connected on the NUSA1 unit. The maximum number of available VC-12 in NUSA1 is 945.

- /unit-x/eos/eos-y/eos/vc12-z, e.g. /unit-4/eos/eos-5/eos/vc12-1:
  y = 1 to 32 (EoS port number)
  z = 1 to 63 (VCG member number)
  The maximum number of available VC-12 members on the NUSA1 unit is 252. The maximum number of available VC-12 members in a virtual concatenation group is 63.
- /unit-x/pdh/vc12-z, e.g. /unit-4/pdh/vc12-1:
  z = 1 to 64 (VC-12 number)
  pdh/vc12-z are the VC-12 signals whose contained P12 signals can access the PBUS. The number of available VC-12 members in the pdh access point is fixed to 64.

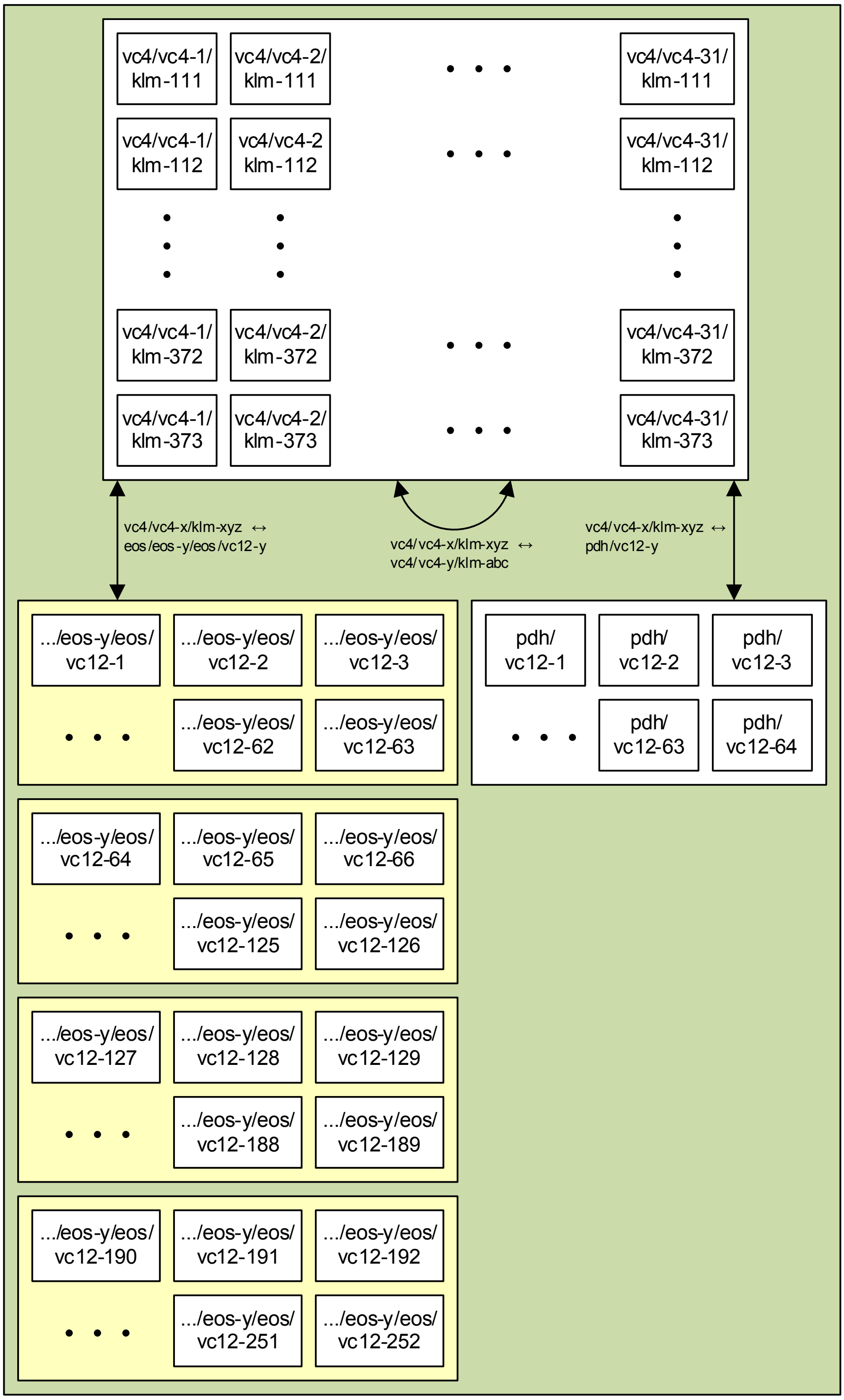


Figure 66: Cross connections in the VC-12 layer

The following unidirectional and bidirectional cross connections are configurable:

Table 33: VC-12 layer cross connections

a-End	z-End	Cross connection
/vc4/vc4-x/klm-xyz	/vc4/vc4-a/klm-abc	Connects a VC-12 to itself or to another VC-12 signal. This cross connection is used for through connected VC-12 signals or can be used for maintenance purposes. i.e. to loop a VC-12 back towards the internal VC-4 using a unidirectional cross connection.
/vc4/vc4-x/klm-xyz	/eos/eos-y/eos/vc12-y	Connects a VC-12 signal from an internal VC-4 to an EoS VC-12 member. This cross connection is used for Ethernet transport over virtually concatenated or non concatenated VC-12. The maximum number of terminated VC-12 is 252 per NUSA1 unit. The maximum number of terminated VC-12 is 63 per virtual concatenation group.
/eos/eos-x/eos/vc12-x	/vc4/vc4-a/klm-abc	Connects a VC-12 signal from an EoS VC-12 member to an internal VC-4. This cross connection is used for Ethernet transport over virtually concatenated or non concatenated VC-12. The maximum number of terminated VC-12 is 252 per NUSA1 unit. The maximum number of terminated VC-12 is 63 per virtual concatenation group.
/vc4/vc4-x/klm-xyz	/pdh/vc12-y	Connects a VC-12 signal from an internal VC-4 to a VC-12 accessing the PBUS. This cross connection is used for PBUS access with structured and unstructured P12 signals. The maximum number of VC-12 with PBUS access is 64.
/pdh/vc12-x	/vc4/vc4-a/klm-abc	Connects a VC-12 signal accessing the PBUS to a VC-12 going to an internal VC-4. This cross connection is used for PBUS access with structured and unstructured P12 signals. The maximum number of VC-12 with PBUS access is 64.

Risk of operating trouble!

It is possible to create a connection between a VC-12 EoS member and a PDH VC-12.

→ Since the EoS mapping and the VC-12 with PDH mapping are not compatible this cross connection makes no sense.

The following SNC protections can be configured in the VC-12 layer:

Please note:

The working and the protecting path of an SNC protected connection must be located on the same NUSA1 unit or on an equipment protected pair of NUSA1 units.

Table 34: VC-12 layer protection cross connections

a-End working	a-End protecting	z-End	Protection
/vc4/vc4-x/klm-xyz	/vc4/vc4-a/klm-abc	/vc4/vc4-d/klm-def	Protects an outgoing VC-12 by two incoming VC-12 signals from one or two internal VC-4. This cross connection is used for protected through connected VC-12 signals.
/vc4/vc4-x/klm-xyz	/vc4/vc4-a/klm-abc	/eos/eos-z/eos/vc12-z	Protects an EoS VC-12 member by two incoming VC-12 signals from one or two internal VC-4. This cross connection is used for protected Ethernet transport over virtually concatenated or non concatenated VC-12.

Table 34: VC-12 layer protection cross connections (continued)

a-End working	a-End protecting	z-End	Protection
/vc4/vc4-x/klm-xyz	/vc4/vc4-a/klm-abc	/pdh/vc12-z	Protects a VC-12 signal with PBUS access by two incoming VC-12 signals from one or two internal VC-4. This cross connection is used for protected P12 PBUS access. The switching type of this SNC protection can be configured to be unidirectional or bidirectional.

6.1.4 P12 Cross Connections

P12 cross connections on NUSA1 are used for PBUS access.

P12 resources on NUSA1 are enabled by the P12 configuration of the PDH VC-12 signals to one of the following P12 modes:

- Transparent,
- Clock master.

The following signal types are available on the P12 layer:

- /unit-x/pdh/vc12-y/p12/chan-z, e.g. unit-4/pdh/vc12-1/p12/chan-1:
  y = 1 to 64 (VC-12 number)
  z = 1 (channel index)
  vc12-y/p12/chan-z are all unterminated P12 signals demapped from a VC-12 of the NUSA1 unit. The maximum number of available P12 channels in NUSA1 is 64.

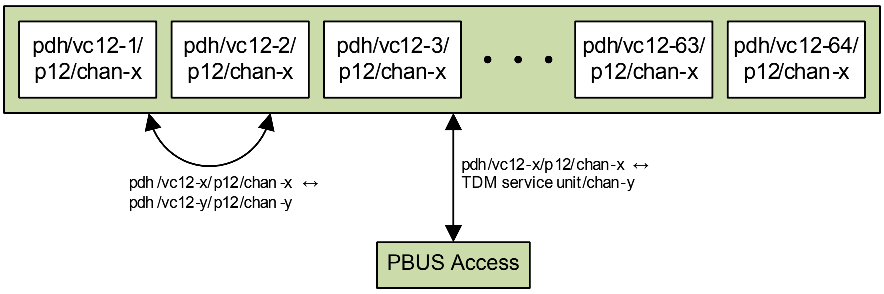


Figure 67: Cross connections in the P12 layer

The following unidirectional and bidirectional cross connections are configurable:

Table 35: P12 layer cross connections

a-End	z-End	Cross connection
/pdh/vc12-x/p12/chan-x	<TDM service unit>/chan-y	Cross connection between the NUSA1 unit and another PBUS unit: Connects an unterminated P12 signal from a VC-12 to the PBUS. This cross connection is used for unterminated P12 signals using the PBUS. The maximum number of P12 signals accessing the PBUS is 64.
<TDM service unit>/chan-y	/pdh/vc12-x/p12/chan-x	Cross connection between another PBUS unit and the NUSA1 unit. Connects an unterminated P12 signal from a VC-12 to the PBUS. This cross connection is used for unterminated P12 signals using the PBUS. The maximum number of P12 signals accessing the PBUS is 64.
/pdh/vc12-x/p12/chan-x	/pdh/vc12-y/p12/chan-y	Cross connection on the same NUSA1 unit: Connects an unterminated P12 to itself or to another P12 signal. This cross connection is mainly used for maintenance purposes. i.e. to loop a P12 back towards the VC-12 using a unidirectional cross connection.

The following SNC protections can be configured in the P12 layer:

Table 36: P12 layer protection cross connections

a-End working	a-End protecting	z-End	Protection
/pdh/vc12-x/p12/ chan-x	/pdh/vc12-y/p12/ chan-y	<TDM service unit>/ chan-z	Cross connection between the NUSA1 unit and another PBUS unit: Protects a P12 signal on another PBUS unit by two P12 signals from the same or different NUSA1 units. This cross connection is used for protected unterminated P12 signals using the PBUS. Please refer to Figure 55: "P12 SNCP/I from the network side with two NUSA1 units" (on page 99).
<TDM service unit>/ chan-x	<TDM service unit>/ chan-y	/pdh/vc12-z/p12/ chan-z	Cross connection between the NUSA1 unit and another PBUS unit: Protects a P12 signal on the NUSA1 unit by two P12 signals coming from other PBUS units. This cross connection is used for protected unterminated P12 signals using the PBUS. Please refer to Figure 54: "P12 SNCP/I from the tributary side" (on page 98).
/pdh/vc12-x/p12/ chan-x	/pdh/vc12-y/p12/ chan-y	/pdh/vc12-z/p12/ chan-z	Cross connection on the same or different NUSA1 units: Protects an outgoing P12 signal by two incoming P12 signals. This cross connection is used for protected through connected P12 signals. Note that this type of protection requires three (P12) PBUS access resources.

For more information about the P12 connection termination points and the P12 cross connection configuration refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.

6.1.5 P0-nc Cross Connections

P0-nc cross connections on NUSA1 are used for PBUS access.

P0-nc resources on NUSA1 are enabled by the P12 configuration of the PDH VC-12 signals to one of the following P12 modes:

- PCM30,
- PCM30C,
- PCM31,
- PCM31C,
- V5 uplink,
- V5 uplink NCI.

Other P0-nc resources are the DCC of the RS (dccr) and MS (dccm) layer of the SDH ports. The DCC must be enabled by the ECST configuration.

The following signal types are available on the P0-nc layer:

- /unit-x/pdh/vc12-y/p12/chan-z, e.g. unit-4/pdh/vc12-1/p12/chan-1:
  y = 1 to 64 (VC-12 number)
  z = 1 to 32 (channel index)
  vc12-y/p12/chan-z are all single or concatenated timeslots of a terminated P12 signal, mapped/demapped to/from a VC-12 of the NUSA1 unit. Time slot 0 is not accessible, time slot 16 is only accessible if CAS is dis-

abled. The maximum number of available P0-nc channels in NUSA1 is 64 x 31 = 1984.

- /unit-x/sdh/sdh-y/dccr, e.g. unit-4/sdh/sdh-1/dccr:
  y = 1 to 8 (logical SDH port number)
  dccr are all concatenated timeslots with n=3 (RS DCC).
- /unit-x/sdh/sdh-y/dccm, e.g. unit-4/sdh/sdh-1/dccm:
  y = 1 to 8 (logical SDH port number)
  dccm are all concatenated timeslots with n=9 (MS DCC).

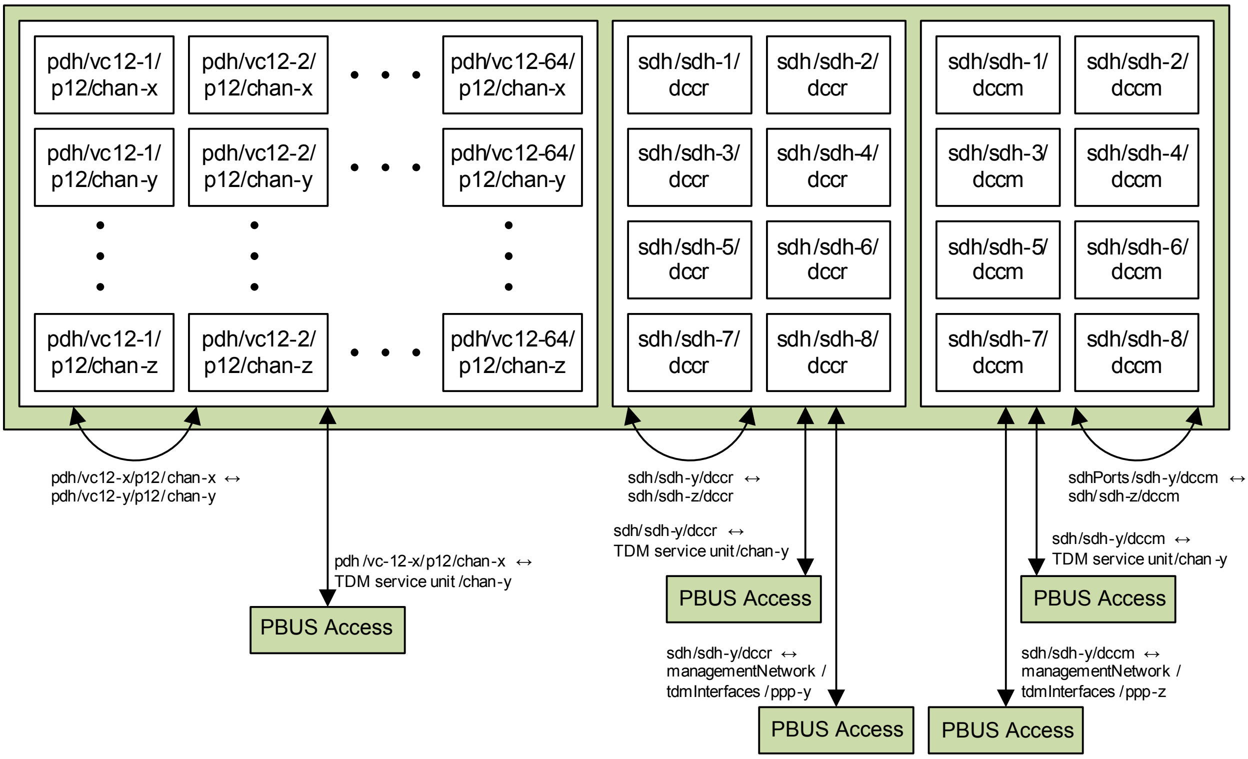


Figure 68: Cross connections in the P0-nc layer

Please note:

The access to the RS and/or MS DCC requires PBUS resources.

→ As soon as one of the RS or MS DCC is configured the vc12-61 to vc12-64 resources are no longer available.

The following unidirectional and bidirectional cross connections are configurable:

Table 37: P0-nc layer cross connections

a-End	z-End	Cross connection
/pdh/vc12-x/p12/chan-x	<TDM service unit>/chan-y	Cross connection between the NUSA1 unit and another PBUS unit: Connects a P0-nc channel from a VC-12 to the PBUS. This cross connection is used for terminated P12 signals using the PBUS. The maximum number of P0-nc signals accessing the PBUS is 1984.
<TDM service unit>/chan-y	/pdh/vc12-x/p12/chan-x	Cross connection between another PBUS unit and the NUSA1 unit: Connects a P0-nc channel from a VC-12 to the PBUS. This cross connection is used for terminated P12 signals using the PBUS. The maximum number of P0-nc signals accessing the PBUS is 1984.

Table 37: P0-nc layer cross connections (continued)

a-End	z-End	Cross connection
/pdh/vc12-x/p12/chan-x	/pdh/vc12-y/p12/chan-y	Cross connection on the same NUSA1 unit: Connects a P0-nc channel from a VC-12 to itself or to another P0-nc channel. This cross connection is mainly used for maintenance purposes. i.e. to loop a P0-nc channel back towards the VC-12 using a unidirectional cross connection.
/sdh/sdh-x/dccr	/managementNetwork/tdmInterfaces/ppp-y	Cross connection between the NUSA1 unit and the XMC20 management router: Connects a RS DCC to a PPP signal of the XMC20 management router. The maximum number of RS DCC accessing the PBUS is 8.
/sdh/sdh-x/dccr	/sdh/sdh-y/dccr	Cross connection on the same or another NUSA1 unit: Connects a P0-nc channel from a RS DCC to itself or to another RS DCC.
/sdh/sdh-x/dccr	<TDM service unit>/chan-y	Cross connection between the RS DCC and the same or another PBUS unit: Connects a P0-nc channel from a RS DCC to a P0-nc channel with 3 time slots in a P12.
/sdh/sdh-x/dccm	/managementNetwork/tdmInterfaces/ppp-y	Cross connection between the NUSA1 unit and the XMC20 management router: Connects a MS DCC to a PPP signal of the XMC20 management router. The maximum number of MS DCC accessing the PBUS is 8.
/sdh/sdh-x/dccm	/sdh/sdh-y/dccm	Cross connection on the same or another NUSA1 unit: Connects a P0-nc channel from a MS DCC to itself or to another MS DCC.
/sdh/sdh-x/dccm	<TDM service unit>/chan-y	Cross connection between the MS DCC and the same or another PBUS unit: Connects a P0-nc channel from a MS DCC to a P0-nc channel with 9 time slots in a P12.

The following SNC protections can be configured in the P0-nc layer:

Table 38: P0-nc layer protection cross connections

a-End working	a-End protecting	z-End	Protection
/pdh/vc12-x/p12/chan-x	/pdh/vc12-y/p12/chan-y	<TDM service unit>/chan-z	Cross connection between the NUSA1 unit and another PBUS unit: Protects a P0-nc signal on another PBUS unit by two P0-nc signals from the same or different NUSA1 units. This cross connection is used for protected terminated P12 signals using the PBUS.
<TDM service unit>/chan-x	<TDM service unit>/chan-y	/pdh/vc12-z/p12/chan-z	Cross connection between the NUSA1 unit and other PBUS units: Protects a P0-nc signal on the NUSA1 unit by two P0-nc signals coming from other PBUS units. This cross connection is used for protected terminated P12 signals using the PBUS.
/pdh/vc12-x/p12/chan-x	/pdh/vc12-y/p12/chan-y	/pdh/vc12-z/p12/chan-z	Cross connection on the same or different NUSA1 units: Protects an outgoing P0-nc signal by two incoming P0-nc signals. This cross connection is used for protected through connected P0-nc signals.
/sdh/sdh-x/dccr	/sdh/sdh-y/dccr	/managementNetwork/tdmInterfaces/ppp-z	Cross connection between one or two NUSA1 units and the XMC20 management router: Protects a PPP signal on the management router by two RS DCC signals from the same or different NUSA1 units.

Table 38: P0-nc layer protection cross connections (continued)

a-End working	a-End protecting	z-End	Protection
/sdh/sdh-x/dccr	/sdh/sdh-y/dccr	<TDM service unit>/ chan-y	Cross connection between one or two NUSA1 units and another PBUS unit. Protects a P0-nc signal on another PBUS unit by two RS DCC signals from the same or different NUSA1 units.
<TDM service unit>/ chan-x	<TDM service unit>/ chan-y	/sdh/sdh-z/dccr	Cross connection between the NUSA1 unit and other PBUS units: Protects a RS DCC on the NUSA1 unit by two P0-nc channels with 3 time slots coming from other PBUS units.
/sdh/sdh-x/dccr	/sdh/sdh-y/dccr	/sdh/sdh-z/dccr	Cross connection on the same or different NUSA1 units: Protects an outgoing RS DCC by two incoming RS DCC.
/sdh/sdh-x/dccm	/sdh/sdh-y/dccm	/managementNet-work/tdmInterfaces/ ppp-z	Cross connection between one or two NUSA1 units and the XMC20 management router: Protects a PPP signal on the management router by two MS DCC signals from the same or different NUSA1 units.
/sdh/sdh-x/dccm	/sdh/sdh-x/dccm	<TDM service unit>/ chan-y	Cross connection between one or two NUSA1 units and another PBUS unit. Protects a P0-nc signal on another PBUS unit by two MS DCC signals from the same or different NUSA1 units.
<TDM service unit>/ chan-x	<TDM service unit>/ chan-y	/sdh/sdh-z/dccm	Cross connection between the NUSA1 unit and other PBUS units: Protects a MS DCC on the NUSA1 unit by two P0-nc channels with 9 time slots coming from other PBUS units.
/sdh/sdh-x/dccm	/sdh/sdh-y/dccm	/sdh/sdh-z/dccm	Cross connection on the same or different NUSA1 units: Protects an outgoing MS DCC by two incoming MS DCC.

For more information about the P0-nc connection termination points and the P0-nc cross connection configuration refer to [314] User Guide "TDM Services and Cross Connections in XMC20".

6.1.6 Cross Connection Examples

In the following the cross connection configuration steps are given for some application examples. Note that all connection termination points (CTP) are on the NUSA1 unit except where indicated otherwise (e.g. SELI8).

Table 39: EoS with 4 VC-4

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1 /unit-4/sdh/sdh-1/j-2 /unit-4/sdh/sdh-1/j-3 /unit-4/sdh/sdh-1/j-4	/unit-4/eos/eos-1/eos/vc4-1 /unit-4/eos/eos-1/eos/vc4-2 /unit-4/eos/eos-1/eos/vc4-3 /unit-4/eos/eos-1/eos/vc4-4	VC4

Table 40: EoS with 4 VC-3

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1 /unit-4/sdh/sdh-1/j-2	/unit-4/vc4/vc4-1 /unit-4/vc4/vc4-2	VC4
/unit-4/vc4/vc4-1/klm-100 /unit-4/vc4/vc4-1/klm-200 /unit-4/vc4/vc4-1/klm-300 /unit-4/vc4/vc4-2/klm-100	/unit-4/eos/eos-1/eos/vc3-1 /unit-4/eos/eos-1/eos/vc3-2 /unit-4/eos/eos-1/eos/vc3-3 /unit-4/eos/eos-1/eos/vc3-4	VC3

Table 41: EoS with 3 VC-12

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1	/unit-4/vc4/vc4-1	VC4
/unit-4/vc4/vc4-1/klm-111 /unit-4/vc4/vc4-1/klm-112 /unit-4/vc4/vc4-1/klm-113	/unit-4/eos/eos-1/eos/vc12-1 /unit-4/eos/eos-1/eos/vc12-2 /unit-4/eos/eos-1/eos/vc12-3	VC12

Table 42: Through connection with 3 VC-4

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1 /unit-4/sdh/sdh-1/j-2 /unit-4/sdh/sdh-1/j-3	/unit-4/sdh/sdh-2/j-1 /unit-4/sdh/sdh-2/j-2 /unit-4/sdh/sdh-2/j-3	VC4

Table 43: Through connection with 3 VC-3

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1 /unit-4/sdh/sdh-2/j-1	/unit-4/vc4/vc4-1 /unit-4/vc4/vc4-2	VC4
/unit-4/vc4/vc4-1/klm-100 /unit-4/vc4/vc4-1/klm-200 /unit-4/vc4/vc4-1/klm-300	/unit-4/vc4/vc4-2/klm-100 /unit-4/vc4/vc4-2/klm-200 /unit-4/vc4/vc4-2/klm-300	VC3

Table 44: PBUS access with 2 P12

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1	/unit-4/vc4/vc4-1	VC4
/unit-4/vc4/vc4-1/klm-111 /unit-4/vc4/vc4-1/klm-112	/unit-4/pdh/vc12-1 /unit-4/pdh/vc12-2	VC12
/unit-4/pdh/vc12-1/p12/chan-1 /unit-4/pdh/vc12-2/p12/chan-1	SELI8/port-1/chan-1 [a] SELI8/port-2/chan-1 [b]	P12

a. SELI8 port-1 is configured to an unterminated P12 mode.
b. SELI8 port-2 is configured to an unterminated P12 mode.

Table 45: PBUS access with 2 P0-nc

CTP a-End	CTP z-End	Layer
/unit-4/sdh/sdh-1/j-1	/unit-4/vc4/vc4-1	VC4
/unit-4/vc4/vc4-1/klm-111	/unit-4/pdh/vc12-1	VC12
/unit-4/pdh/vc12-1/p12/chan-1 [a] /unit-4/pdh/vc12-1/p12/chan-2 [b]	SELI8/port-1/chan-1 [c] SELI8/port-1/chan-2 [d]	P0-nc

a. chan-1 comprises n time slots.

b. chan-2 comprises m time slots.
c. SELI8 port-1 is configured to a terminated P12 mode. chan-1 comprises n time slots.
d. SELI8 port-2 is configured to a terminated P12 mode. chan-2 comprises m time slots.

6.2 SNCP Configuration

6.2.1 SNCP Timer Configuration

In the revertive mode of SNC protection the path selector switches back to the working path as soon as the configured “wait to restore” (WTR) timer elapses. The WTR timer is reset when the working path is in a failure state and starts when the working path becomes fault free.

The “holdoff” time is the time interval to define how long the switching criteria have to be active before the protection switching is activated.

The “guard time” is the time interval after an automatic protection switchover when no additional switchover is allowed. During the guard time the path selector does not switch back to the working path even if the protecting path becomes faulty.

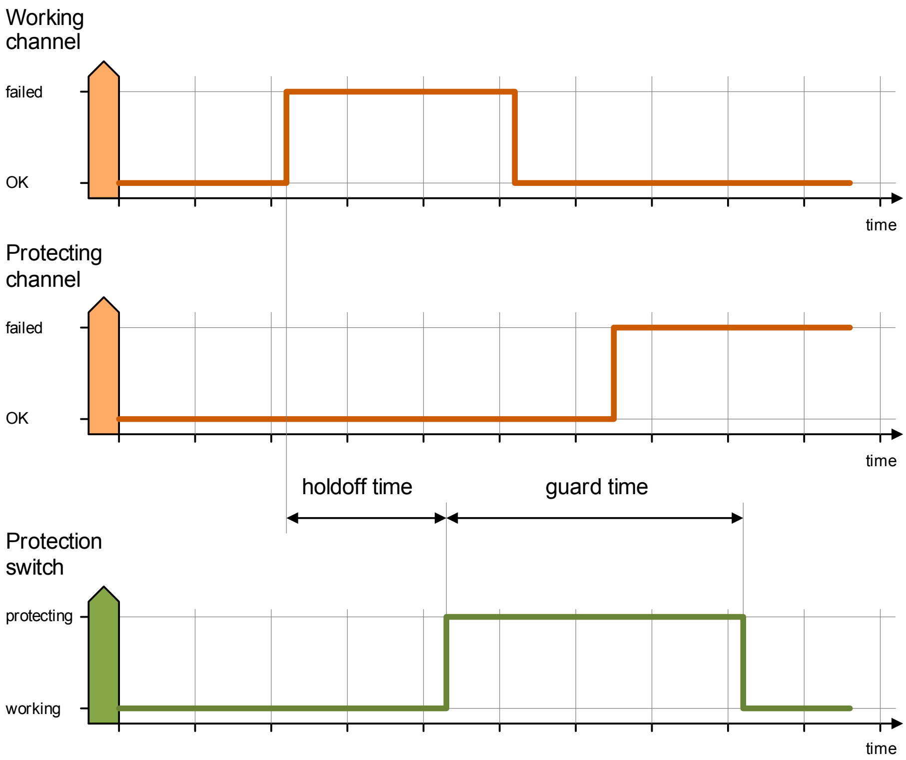


Figure 69: Holdoff and guard times

The SNCP “wait to restore”, “holdoff” and “guard time” timers are configured per VC type for the whole unit.

6.2.2 SNCP degraded Signal Configuration

The threshold level to set a degraded signal defect can be configured per VC type for the whole NUSA1 unit.

Please refer to section 7.3 Detection of Signal Defects (on page 153) for a description of the degraded signal defect evaluation.

6.3 Automatic Laser Shutdown and Restart

Please note:

The NUSA1 supports the same parameters for SFP modules with optical and electrical STM-1 interfaces. Accordingly the electrical STM-1 interface supports also management functions that are normally only applicable for the optical interface, such as laser shutdown and laser restart.

6.3.1 Automatic Laser Shutdown

Automatic laser shutdown (ALS) is a technique to automatically shutdown the output power of laser transmitters to avoid exposure to hazardous levels.

With this option enabled, the laser transmitter automatically shuts down when the received optical signal is lost (LOS) for more than 500 ms. The shutdown is activated within 850 ms after the “loss of light” at the receiver input.

As soon as a valid optical signal is received, the laser is restarted.

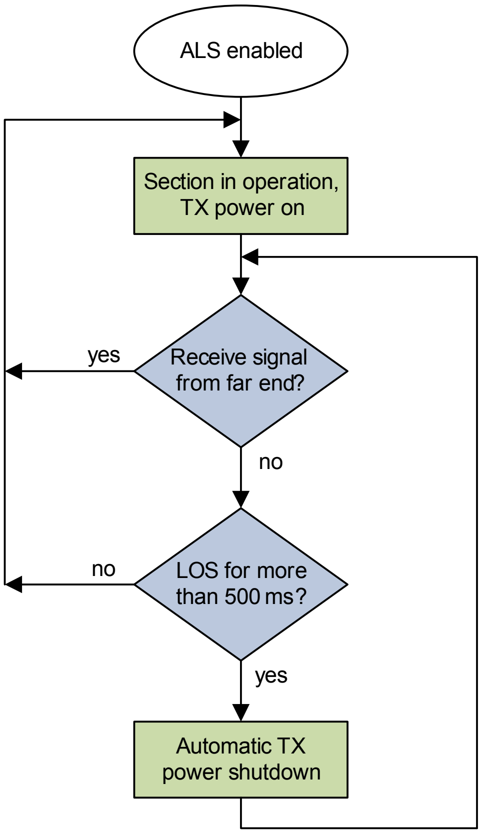


Figure 70: Automatic laser shutdown (ALS)

6.3.2 Automatic Laser Restart

After an automatic laser shutdown, the laser can be restarted in several ways to get the section operational again:

- Automatic laser restart
  With the automatic laser restart enabled, the laser automatically restarts periodically for 2 ± 0.25 s at an interval of 110 s.
- Manual laser restart (maintenance function)
  The manual laser restart activates the laser for 2 ± 0.25 s.
- Manual laser restart for test (maintenance function)
  The manual laser restart for test activates the laser for 90 ± 10 s.

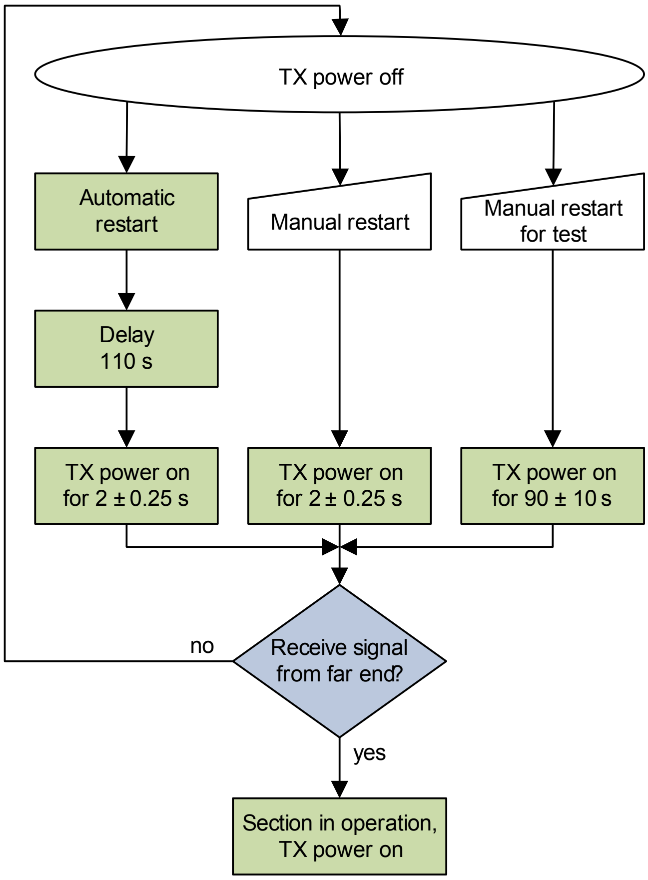


Figure 71: Automatic laser restart (ALR)

6.4 Commissioning Example of PDH and EoS Transport

6.4.1 Prerequisites

Before starting the commissioning of an SDH multiplexer for PDH and EoS transport on the NUSA1 unit, the following prerequisites need to be fulfilled.

6.4.1.1 COGE5 unit

In a XMC20, a COGE5 needs to be in operation in slot 11 of the XMC20 subrack.

6.4.1.2 NUSA1 unit

The NUSA1 service unit is inserted into a slot of the XMC20 subrack. Available slots are listed in section 4.2 Slots for the NUSA1 Unit (on page 31).

A valid ESW is installed on the NUSA1 unit. For the management of ESW, refer to [355] User Manual “ECST”. For details about compatible ESW versions, refer to [012] Release Note “XMC20 System Release R6B”.

6.4.1.3 ECST

ECST needs to be installed on a PC, and a management connection from the ECST to the XMC20 needs to be up and running. For details about the installation and operation of the ECST, please refer to [355] User Manual “ECST” and [354] Quick Guide “ECST”.

The amount and accessibility of operations depend on the user profile with which you are logged in. For more information, please refer to [323] User Guide “Management Communication”.

6.4.2 Configuration of the SDH Multiplexer

SDH multiplexer configuration

This action list shows step by step how to configure the SDH multiplexer for PDH and EoS transport. The multiplexer transports
- Ethernet traffic of Ethernet port 5 in a single VC-4, using the unswitched Ethernet transport mode with EoS port 1,
- Ethernet traffic of Ethernet port 6 in two concatenated VC-3, using the switched Ethernet transport mode with EoS port 2,
- The Ethernet port 6 and the EoS port 2 are access ports of the VLAN bridge, using the port VLAN ID 1,
- four P12 signals in transparent mode from the SELI8 ports 1 to 4.
- The Ethernet traffic is transported via j-1 (AU4-1) and j-2 (AU4-2) of the SDH port 1,
- the PDH traffic is transported in protected mode via j-2 (AU4-2) of the SDH port 1 and via j-1 (AU4-1) of the SDH port 2.

For the configuration of the SDH multiplexer for PDH and EoS transport, the following steps have to be performed. The main steps are:

- Configure the Ethernet transport mode
- Configure the physical SDH ports
- Configure the logical SDH ports
- Configure the physical Ethernet ports
- Configure the EoS ports
- Create and configure the VC-4 resources with TUG-3 structure
- Configure the VC-12 and P12 signals used for the PDH traffic
- Create the channels on the P12 signals
- Configure the E1 interface unit
- Create the cross connections to the EoS group members
- Create the cross connections to the E1 ports
- Configure the SETS
- Activate the SDH and Ethernet ports
- Activate the VC-ts4 and VC-12 resources
- Activate the E1 port

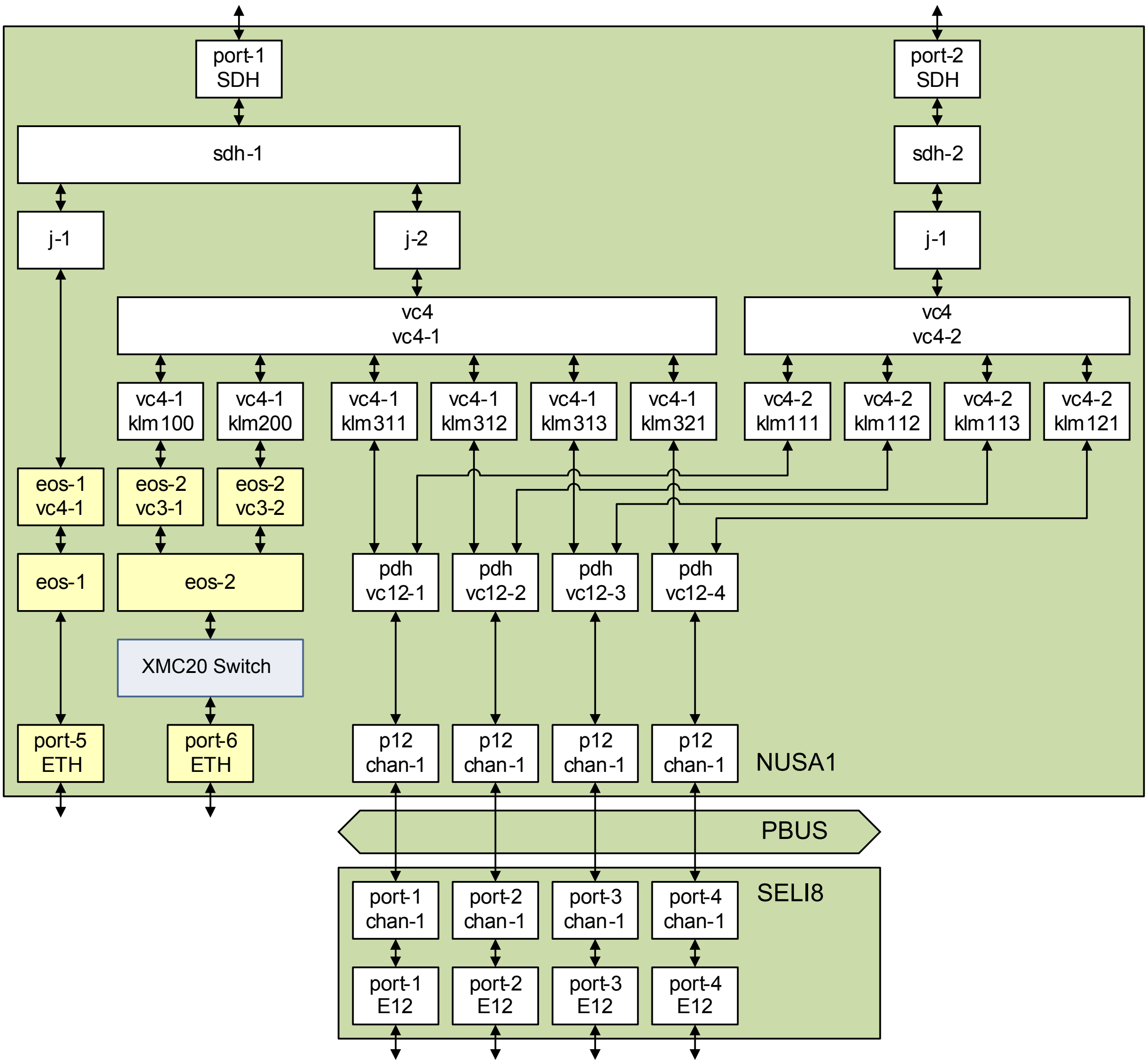


Figure 72: NUSA1 configuration example

The following assumptions and identifiers are used:
- The NUSA1 unit is assumed to be plugged in slot 4 of the XMC25.
- The NUSA1 unit is assigned.
- Port 1 and port 2 of the NUSA1 unit are equipped with SFP modules supporting STM-4, e.g. S-4.1.
- The E1 transport unit SELI8 running with a proper ESW is plugged in slot 20 of the XMC25. The port-1 to port-4 are used for the PDH traffic.

Configure the VLAN bridge ports

Proceed as follows:

1. Navigate to the unit VLAN bridge port configuration:
   - ECST “Switching” tab
   - AP: /Switching/Bridges/bridge-1, Ports.
2. Configure the unswitched Ethernet ports:
   - /unit-4/port-5, Mode = Unswitched.
   - /unit-4/eos/eos-1, Mode = Unswitched.
3. Configure the switched Ethernet ports:
   - /unit-4/port-6, Mode = Access, PVID = 1.
   - /unit-4/eos/eos-2, Mode = Access, PVID = 1.
4. Execute “Apply”.

Result: The VLAN bridge ports are configured.

Configure the Ethernet transport mode

Proceed as follows:

1. Navigate to the unit EPL configuration dialogue:
   - AP: /unit-4, Configuration - EPL.
2. Configure the EPL handling:
   - port-5 = eos-1.
   - port-6 = no EPL.
3. Execute “Apply”.

Result: The Ethernet transport mode is configured.

Configure the physical SDH port-1

Proceed as follows:

1. Navigate to the port-1 physical section configuration dialogue:
   - AP: /unit-4/port-1, Configuration - PS.
2. Set the SFP port mode:
   - SFP Port Mode = STM-4.
3. Enable the automatic laser shutdown:
   - Automatic Laser Shutdown = true.
4. Enable the automatic laser restart:
   - Automatic Laser Restart = true.
5. Execute “Apply”.

Result: The physical SDH port 1 is fully configured.

Configure the physical SDH port-2

Proceed as follows:

1. Navigate to the port-2 physical section configuration dialogue:
   - AP: /unit-4/port-2, Configuration - PS.
2. Set the SFP port mode:
   - SFP Port Mode = STM-4.

3. Enable the automatic laser shutdown:
   - Automatic Laser Shutdown = true.
4. Enable the automatic laser restart:
   - Automatic Laser Restart = true.
5. Execute “Apply”.

Result: The physical SDH port 2 is fully configured.

Configure the logical SDH port-1

Proceed as follows:

1. Navigate to the logical SDH port-1 regenerator section configuration dialogue:
   - AP: /unit-4/sdh/sdh-1, Configuration - RS.
2. Set the port mode:
   - Port Mode = STM-4.
3. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
4. Navigate to the port-1 multiplex section configuration dialogue:
   - AP: /unit-4/sdh/sdh-1, Configuration - MS.
5. Enable the synchronization status message:
   - SSM = true.
6. Select the excessive signal threshold:
   - Excessive Defect Threshold = 10E-3.
7. Select the degraded signal threshold:
   - Degraded Defect Threshold = 10E-6.
8. Keep the default setting of the input mapping table for the quality levels:
   - The adapted QL equals the received QL.
9. Keep the default setting of the output mapping table for the quality levels:
   - The adapted QL equals the transmitted QL.
10. Keep the default setting of the synchronization usability of all clock sources:
    - sdh-1 = “Do Not Use”.
    - All other ports = “Can Be Used”.
11. Navigate to the port-1 multiplex section protection configuration dialogue:
    - AP: /unit-4/sdh/sdh-1, Configuration - MSP.
12. Disable the multiplex section protection:
    - Protection = None.
13. Navigate to the port-1 DCC configuration dialogue:
    - AP: /unit-4/sdh/sdh-1, Configuration - DCC.
14. Disable the DCC usage:
    - DCC Type = None.
15. Execute “Apply”.

Result: The logical SDH port 1 is fully configured.

Configure the logical SDH port-2

Proceed as follows:

1. Navigate to the logical SDH port-2 regenerator section configuration dialogue:
   - AP: /unit-4/sdh/sdh-2, Configuration - RS.
2. Set the port mode:
   - Port Mode = STM-4.

3. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
4. Navigate to the port-2 multiplex section configuration dialogue:
   - AP: /unit-4/sdh/sdh-2, Configuration - MS.
5. Enable the synchronization status message:
   - SSM = true.
6. Select the excessive signal threshold:
   - Excessive Defect Threshold = 10E-3.
7. Select the degraded signal threshold:
   - Degraded Defect Threshold = 10E-6.
8. Keep the default setting of the input mapping table for the quality levels:
   - The adapted QL equals the received QL.
9. Keep the default setting of the output mapping table for the quality levels:
   - The adapted QL equals the transmitted QL.
10. Keep the default setting of the synchronization usability of all clock sources:
    - sdh-2 = “Do Not Use”.
    - All other ports = “Can Be Used”.
11. Navigate to the port-2 multiplex section protection configuration dialogue:
    - AP: /unit-4/sdh/sdh-2, Configuration - MSP.
12. Disable the multiplex section protection:
    - Protection = None.
13. Navigate to the port-2 DCC configuration dialogue:
    - AP: /unit-4/sdh/sdh-2, Configuration - DCC.
14. Disable the DCC usage:
    - DCC Type = None.
15. Execute “Apply”.

Result: The logical SDH port 2 is fully configured.

Configure the physical Ethernet port-5

Proceed as follows:

1. Navigate to the port-5 PHY configuration dialogue:
   - AP: /unit-4/port-5, Main - Physical.
2. Configure the Ethernet ports MTU size:
   - MTU = 1578 Octets.
3. Configure the Ethernet interface speed and duplex mode:
   - Admin = Auto.
4. Disable the Ethernet interface flow control:
   - Admin = false.
5. Execute “Apply”.

Result: The physical Ethernet port 5 is fully configured.

Configure the physical Ethernet port-6

Proceed as follows:

1. Navigate to the port-6 PHY configuration dialogue:
   - AP: /unit-4/port-6, Main - Physical.
2. Configure the Ethernet ports MTU size:
   - MTU = 1578 Octets.

3. Configure the Ethernet interface speed and duplex mode:
   - Admin = Auto.
4. Disable the Ethernet interface flow control:
   - Admin = false.
5. Execute “Apply”.

Result: The physical Ethernet port 6 is fully configured.

Configure the EoS port 1

Proceed as follows:

1. Navigate to the EoS port eos-1 configuration dialogue:
   - AP: /unit-4/eos/eos-1, Configuration - EoS.
   - Execute “Create EoS Group…”.
2. Set the layer rate:
   - Layer Rate = VC4.
3. Enable LCAS:
   - LCAS = true.
4. Set the number of EoS group members:
   - Number Of Members = 1.
5. Execute “OK”.

Result: The EoS port eos-1 is fully configured. The EoS group has one member vc4-1. It transports the Ethernet traffic from the Ethernet port 5.

Configure the EoS port 2

Proceed as follows:

1. Navigate to the EoS port eos-2 configuration dialogue:
   - AP: /unit-4/eos/eos-2/eos, Configuration - EoS.
   - Execute “Create EoS Group…”.
2. Set the layer rate:
   - Layer Rate = VC3.
3. Enable LCAS:
   - LCAS = true.
4. Set the number of EoS group members:
   - Number Of Members = 2.
5. Execute “OK”.

Result: The EoS port eos-2 is fully configured. The EoS group has two members vc3-1 and vc3-2. It transports the (untagged) Ethernet traffic from the VLAN bridge with the switch internal VLAN ID 1.

Create the VC-4 resource with TUG-3 structure for EoS and PDH traffic

Proceed as follows:

1. Navigate to the VC-4 configuration dialogue:
   - AP: /unit-4/vc4, Configuration - General.
   - Execute the command “Create VC4”.
2. Configure the VC-4 index:
   - Index = 0 (automatically select the next free index).
3. Select the structure of the three TUG-3:
   - k-1 = VC3.
   - k-2 = VC3.
   - k-3 = VC12.

4. Select the number of repetitions:
   - Repetitions = 1.
5. Execute “OK”.

Result: The VC-4 called vc4-1 with the TUG-3 structure is created.

Create the VC-4 resource with TUG-3 structure for protected PDH traffic

Proceed as follows:

1. Navigate to the VC-4 configuration dialogue:
   - AP: /unit-4/vc4, Configuration - General.
   - Execute the command “Create VC4”.
2. Configure the VC-4 index:
   - Index = 0 (automatically select the next free index).
3. Select the structure of the three TUG-3:
   - k-1 = VC12.
   - k-2 = VC3.
   - k-3 = VC3.
4. Select the number of repetitions:
   - Repetitions = 1.
5. Execute “OK”.

Result: The VC-4 called vc4-2 with the TUG-3 structure is created.

Configure the VC-4 resources with TUG-3 structure

Proceed as follows:

1. Navigate to the VC-4-1 configuration dialogue:
   - AP: /unit-4/vc4/vc4-1, Configuration - General.
2. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
3. Execute “Apply”.
4. Navigate to the VC-4-2 configuration dialogue:
   - AP: /unit-4/vc4/vc4-2, Configuration - General.
5. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
6. Execute “Apply”.

Result: The VC-4-1 and VC-4-2 are configured.

Configure the VC-12 resources for PDH traffic

Proceed as follows:

1. Navigate to the VC-12-1 configuration dialogue:
   - AP: /unit-4/pdh/vc12-1, Configuration - General.
2. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
3. Execute “Apply”.
4. Navigate to the VC-12-2 configuration dialogue:
   - AP: /unit-4/pdh/vc12-2, Configuration - General.
5. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
6. Execute “Apply”.
7. Navigate to the VC-12-3 configuration dialogue:
   - AP: /unit-4/pdh/vc12-3, Configuration - General.

8. Disable the trail trace identifier supervision:
   - TTI Supervision = false.
9. Execute “Apply”.
10. Navigate to the VC-12-4 configuration dialogue:
    - AP: /unit-4/pdh/vc12-4, Configuration - General.
11. Disable the trail trace identifier supervision:
    - TTI Supervision = false.
12. Execute “Apply”.

Result: The VC-12 resources are configured.

Configure the P12 resources

1. Navigate to the P12 configuration dialogue:
   - AP: /unit-4/pdh/vc12-1/p12, Configuration - General.
2. Configure the P12 termination mode:
   - Mode = Transparent.
3. Execute “Apply”.
4. Navigate to the P12 configuration dialogue:
   - AP: /unit-4/pdh/vc12-2/p12, Configuration - General.
5. Configure the P12 termination mode:
   - Mode = Transparent.
6. Execute “Apply”.
7. Navigate to the P12 configuration dialogue:
   - AP: /unit-4/pdh/vc12-3/p12, Configuration - General.
8. Configure the P12 termination mode:
   - Mode = Transparent.
9. Execute “Apply”.
10. Navigate to the P12 configuration dialogue:
    - AP: /unit-4/pdh/vc12-4/p12, Configuration - General.
11. Configure the P12 termination mode:
    - Mode = Transparent.
12. Execute “Apply”.

Result: The four P12 signals are configured.

Create the P12 channels

1. Navigate to the P12 configuration dialogue:
   - AP: /unit-4/pdh/vc12-1/p12, Configuration - Channels.
   - Execute the command “Create Channel”.
2. Configure the P12 channel index:
   - Index = 0 (automatically select the next free index).
3. Execute “OK”.
4. Navigate to the P12 configuration dialogue:
   - AP: /unit-4/pdh/vc12-2/p12, Configuration - Channels.
   - Execute “Create Channel…”.
5. Configure the P12 channel index:
   - Index = 0 (automatically select the next free index).

6. Execute “OK”.
7. Navigate to the P12 configuration dialogue:
   - AP: /unit-4/pdh/vc12-3/p12, Configuration - Channels.
   - Execute “Create Channel…”.
8. Configure the P12 channel index:
   - Index = 0 (automatically select the next free index).
9. Execute “OK”.
10. Navigate to the P12 configuration dialogue:
    - AP: /unit-4/pdh/vc12-4/p12, Configuration - Channels.
    - Execute “Create Channel…”.
11. Configure the P12 channel index:
    - Index = 0 (automatically select the next free index).
12. Execute “OK”.

Result: The four channels chan-1 on the four P12 signals are created.

Configure the E1 interface unit

Proceed as follows:

1. On the E1 interface unit SELI8, 4 ports (port-1 to port-4) have to be configured to the “Transparent” termination mode. Please refer to [410] User Manual “SELI8 seli8_r5” for the detail configuration.

Result: The E1 interface unit is configured.

Create the cross connection to the EoS group member of eos-1

Proceed as follows:

1. Select the “Cross connections” view of the ECST.
   - Click on the “Connection Wizard” button:

   - The “Create TDM Connection” dialogue opens.
2. Set the connection parameters:
   - Layer Rate = VC4.
   - Directionality = Bidirectional.
   - Protected = No.
   - Number = 1.
   - Label 1 = <anyName>.
   - Label 2 = <anyName>.
3. Execute “Next ->”.
4. Select the Z-End CTP:
   - Select the NUSA1 unit, eos, eos-1, eos, vc4-1.
5. Execute “Next ->”.
6. Select the A-End CTP:
   - Select the NUSA1 unit, sdh, sdh-1, j-1.
7. Execute “Create”.

Result: The connection from the VC-4 EoS group to the SDH port-1 is created.

Create the cross connections to the EoS group members of eos-2

Proceed as follows:

1. Select the “Cross connections” view of the ECST.
   - Click on the “Connection Wizard” button:

   - The “Create TDM Connection” dialogue opens.
2. Set the connection parameters:
   - Layer Rate = VC4.
   - Directionality = Bidirectional.
   - Protected = No.
   - Number = 1.
   - Label 1 = <anyName>.
   - Label 2 = <anyName>.
3. Execute “Next ->”.
4. Select the Z-End CTP:
   - Select the NUSA1 unit, vc4, vc4-1.
5. Execute “Next ->”.
6. Select the A-End CTP:
   - Select the NUSA1 unit, sdh, sdh-1, j-2.
7. Execute “Create”.

Result: The connection from the internal VC-4 with TUG-3 structure to the SDH port-1 is created.

8. Select the “Cross connections” view of the ECST.
   - Click on the “Connection Wizard” button:

   - The “Create TDM Connection” dialogue opens.
9. Set the connection parameters:
   - Layer Rate = VC3.
   - Directionality = Bidirectional.
   - Protected = No.
   - Number = 2.
   - Label 1 = <anyName>.
   - Label 2 = <anyName>.
10. Execute “Next ->”.
11. Select the Z-End CTPs:
    - Select the NUSA1 unit, eos, eos-2, eos, vc3-1.
    - Select the NUSA1 unit, eos, eos-2, eos, vc3-2.
12. Execute “Next ->”.
13. Select the A-End CTPs:
    - Select the NUSA1 unit, vc4, vc4-1, klm-100.
    - Select the NUSA1 unit, vc4, vc4-1, klm-200.

14. Execute “Create”.

Result: The two connections from the EoS group members vc3-1 and vc3-2 to the VC-3 of the internal VC-4 with TUG-3 structure are created.

Create the cross connections to the protected VC-12 signals

Proceed as follows:

1. Select the “Cross connections” view of the ECST.
   - Click on the “Connection Wizard” button:

   - The “Create TDM Connection” dialogue opens.
2. Set the connection parameters:
   - Layer Rate = VC4.
   - Directionality = Bidirectional.
   - Protected = No.
   - Number = 1.
   - Label 1 = <anyName>.
   - Label 2 = <anyName>.
3. Execute “Next ->”.
4. Select the Z-End CTP:
   - Select the NUSA1 unit, vc4, vc4-2.
5. Execute “Next ->”.
6. Select the A-End CTP:
   - Select the NUSA1 unit, sdh, sdh-2, j-1.
7. Execute “Create”.

Result: The connection from the second internal VC-4 with TUG-3 structure to the SDH port-2 is created.

8. Select the “Cross connections” view of the ECST.
   - Click on the “Connection Wizard” button:

   - The “Create TDM Connection” dialogue opens.
9. Set the connection parameters:
   - Layer Rate = VC12.
   - Directionality = Bidirectional.
   - Protected = Yes.
   - Number = 4.
   - Label 1 = <anyName>.
   - Label 2 = <anyName>.

10. Execute “Next ->”.
11. Select the Z-End CTPs:
    - Select the NUSA1 unit, pdh, vc12-1.
    - Select the NUSA1 unit, pdh, vc12-2.
    - Select the NUSA1 unit, pdh, vc12-3.
    - Select the NUSA1 unit, pdh, vc12-4.
12. Execute “Next ->”.
13. Select the A-End CTPs:
    - Select the NUSA1 unit, vc4, vc4-1, klm-311.
    - Select the NUSA1 unit, vc4, vc4-1, klm-312.
    - Select the NUSA1 unit, vc4, vc4-1, klm-313.
    - Select the NUSA1 unit, vc4, vc4-1, klm-321.
14. Execute “Next ->”.
15. Select the A-End Protecting CTPs:
    - Select the NUSA1 unit, vc4, vc4-2, klm-111.
    - Select the NUSA1 unit, vc4, vc4-2, klm-112.
    - Select the NUSA1 unit, vc4, vc4-2, klm-113.
    - Select the NUSA1 unit, vc4, vc4-2, klm-121.
16. Execute “Create”.

Result: The four protected connections from the two internal VC-4 vc4-1 and vc4-2 to the four VC-12 are created.

Create the cross connections to the E1 ports on the SELI8 unit

Proceed as follows:

1. Select the “Cross connections” view of the ECST.
    - Click on the “Connection Wizard” button:

    - The “Create TDM Connection” dialogue opens.
2. Set the connection parameters:
    - Layer Rate = P12.
    - Directionality = Bidirectional.
    - Protected = No.
    - Number = 4.
    - Label 1 = <anyName>.
    - Label 2 = <anyName>.
3. Execute “Next ->”.
4. Select the Z-End CTPs:
    - Select the NUSA1 unit, pdh, vc12-1, p12, chan-1.
    - Select the NUSA1 unit, pdh, vc12-2, p12, chan-1.
    - Select the NUSA1 unit, pdh, vc12-3, p12, chan-1.
    - Select the NUSA1 unit, pdh, vc12-4, p12, chan-1.
5. Execute “Next ->”.
6. Select the A-End CTPs:
    - Select the SELI8 unit, port-1, chan-1.
    - Select the SELI8 unit, port-2, chan-1.
    - Select the SELI8 unit, port-3, chan-1.
    - Select the SELI8 unit, port-4, chan-1.

7. Execute “Create”.

Result: The connections from the four VC-12 to the SELI8 E1 port-1 to port-4 are created.

Configure the SETS

Proceed as follows:

1. Navigate to the configuration dialogue:
   - AP: /unit-4, Configuration - SETS.
2. In the SETS Clock Selection table select the “sdh-1” row.
3. Configure the clock source parameters:
   - Priority = 1.
   - QL = Received.
   - Holdoff Time = 0.
   - Wait-To-Restore Time = 0.
4. In the SETS Clock Selection table select the “sdh-2” row.
5. Configure the clock source parameters:
   - Priority = 2.
   - QL = Received.
   - Holdoff Time = 0.
   - Wait-To-Restore Time = 0.
6. Select the clock selection algorithm:
   - Selection Algorithm = Priority.
7. Execute “Apply”.

Result: The SETS is fully configured.

Activate the SDH and Ethernet ports

Proceed as follows:

1. AP: /unit-4/port-1, Main - Admin And Oper Status:
   - Set the administrative status of the physical SDH port-1 to up:
   - State = Up.
2. Execute “Apply”.
3. AP: /unit-4/port-2, Main - Admin And Oper Status:
   - Set the administrative status of the physical SDH port-2 to up:
   - State = Up.
4. Execute “Apply”.
5. AP: /unit-4/sdh/sdh-1, Main - Admin And Oper Status:
   - Set the administrative status of the logical SDH port-1 to up:
   - State = Up.
6. Execute “Apply”.
7. AP: /unit-4/sdh/sdh-2, Main - Admin And Oper Status:
   - Set the administrative status of the logical SDH port-2 to up:
   - State = Up.
8. Execute “Apply”.
9. AP: /unit-4/port-5, Main - General:
   - Set the administrative status of the physical Ethernet port-5 to up:
   - Admin Status = Up.
10. Execute “Apply”.
11. AP: /unit-4/port-6, Main - General:
    - Set the administrative status of the physical Ethernet port-6 to up:
    - Admin Status = Up.

12. Execute “Apply”.
13. AP: /unit-4/eos/eos-1, Main - Admin And Oper Status:
    - Set the administrative status of the EoS port eos-1 to up:
    - State = Up.
14. Execute “Apply”.
15. AP: /unit-4/eos/eos-2, Main - Admin And Oper Status:
    - Set the administrative status of the EoS port eos-2 to up:
    - State = Up.
16. Execute “Apply”.

Result: All physical and logical SDH and Ethernet ports on the NUSA1 unit have been activated.

Activate the VC-4 and VC-12 resources

Proceed as follows:

1. AP: /unit-4/vc4/vc4-1, Main - Admin And Oper Status:
    - Make sure the administrative status of the vc4-1 is up:
    - State = Up.
2. Execute “Apply”.
3. AP: /unit-4/vc4/vc4-2, Main - Admin And Oper Status:
    - Make sure the administrative status of the vc4-2 is up:
    - State = Up.
4. Execute “Apply”.
5. AP: /unit-4/pdh/vc12-1, Main - Admin And Oper Status:
    - Set the administrative status of the vc12-1 to up:
    - State = Up.
6. Execute “Apply”.
7. AP: /unit-4/pdh/vc12-2, Main - Admin And Oper Status:
    - Set the administrative status of the vc12-2 to up:
    - State = Up.
8. Execute “Apply”.
9. AP: /unit-4/pdh/vc12-3, Main - Admin And Oper Status:
    - Set the administrative status of the vc12-3 to up:
    - State = Up.
10. Execute “Apply”.
11. AP: /unit-4/pdh/vc12-4, Main - Admin And Oper Status:
    - Set the administrative status of the vc12-4 to up:
    - State = Up.
12. Execute “Apply”.

Result: All VC-4 and VC-12 resources on the NUSA1 unit have been activated.

Activate the E1 ports on the SELI8 unit

Proceed as follows:

1. AP: /unit-20/port-1, Main - Admin And Oper Status:
    - Set the administrative status of the E1 port-1 to up:
    - State = Up.
2. Execute “Apply”.
3. AP: /unit-20/port-2, Main - Admin And Oper Status:
    - Set the administrative status of the E1 port-2 to up:
    - State = Up.

4. Execute “Apply”.
5. AP: /unit-20/port-3, Main - Admin And Oper Status:
   - Set the administrative status of the E1 port-3 to up:
   - State = Up.
6. Execute “Apply”.
7. AP: /unit-20/port-4, Main - Admin And Oper Status:
   - Set the administrative status of the E1 port-4 to up:
   - State = Up.
8. Execute “Apply”.

Result: All E1 ports on the SELI8 unit have been activated.

End of instruction

7 Operation

This section describes the operation functions of the NUSA1 unit.

Please note:

The operation functions described in this section assume a correctly configured and operational NUSA1 unit.

7.1 Unit optical Indicators

LEDs on the front of the NUSA1 unit are used to indicate to the operator the alarm status summary of the unit and of the network traffic signals.

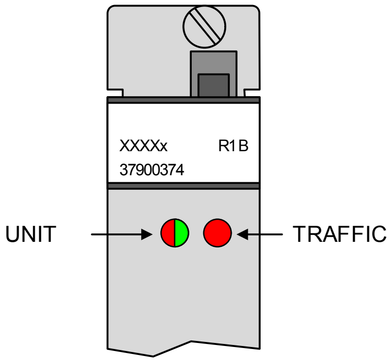


Figure 73: Fault indication LEDs on the NUSA1 unit

Table 46: LED signalling on NUSA1

LED name	Colour	State	Meaning
UNIT	Red	Failure	Unit is not in service. The unit is not able to provide the requested function due to - equipment failure (total breakdown), - mismatch of HW and SW. Recovery from this error situation is done usually by replacement of unit HW or ESW.
	Green / Red (blinking 1 Hz)	Booting or waiting	Unit has not been taken in service yet or the unit has not been provisioned. Recovery from this situation is done by taking this unit into service with ECST.
	Green	Running	Unit is up and running, it is ready to provide the required service.
	Off	Failure	System is not powered or outage of power supply on unit or outage of LED.
TRAFFIC	Red	Failure	One or more active failures on the unit, independent of the severity. More detailed information is provided by ECST.
	Off	Normal	Normal (error free) operation.

7.2 Loops

7.2.1 VC Loops

There are no dedicated maintenance functions available for the application of VC-4, VC-3 or VC-12 loops on NUSA1.

To apply a loop on a VC, a unidirectional cross connection must be configured on the desired path itself.

Please note:

Only the unidirectional cross connections for the front to front loops are applicable.

Please note:

Loops activated with a unidirectional cross connection generate no “maintenance function active” alarm as regular test loops would do.

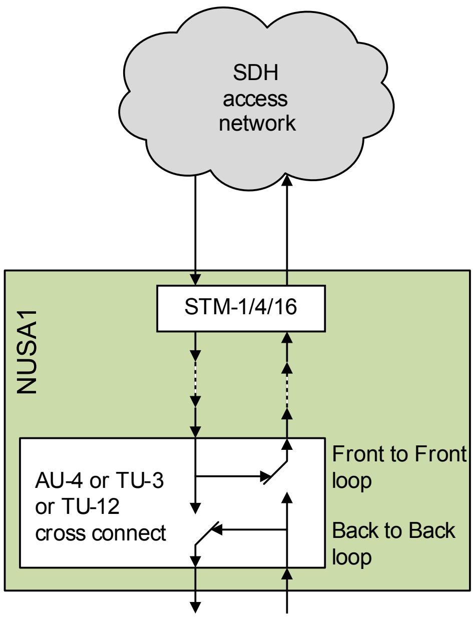


Figure 74: Loops with unidirectional cross connections

Table 47: Loops with unidirectional cross connections

Loop	Signal type	Signal name
Front to front	VC-4	/unit-x/sdh/sdh-y/j-z
Back to back	VC-4	not applicable
Front to front	VC-3	/unit-x/vc4/vc4-y/klm-x00 [a]
Back to back	VC-3	not applicable
Front to front	VC-12	/unit-x/vc4/vc4-y/klm-xyz [a]
Back to back	VC-12	not applicable

a. This loop requires the corresponding cross connections on the VC-4 layer.

7.2.2 P12 and P0-nc Loops

Please note:
Activated loops generate the “maintenance function active (MFA)” alarm.

Please note:
When applying a loop the operational state of the access point changes to “Testing”.

Please note:
P12 and P0-nc loops are not treated as configuration parameters and are not stored in the configuration. They are permanent until they are deactivated manually or by a unit restart or by a power reset.

The following diagnostic loops can be individually set for each of the 64 P12 signals in the /unit-x/pdh/vc12-y/p12 Status - Maintenance dialogue or for all P12 and P0-nc channels in the /unit-x/pdh/vc12-y/p12/chan-z Status - Maintenance dialogue:

- P12 front to front loop:
  Loops the received P12 signal back towards the SDH interface. The loop is transparent, i.e. no AIS is transmitted in direction to the PBUS.

Please note:
The P12 “back to back” loop will be available in a future release.

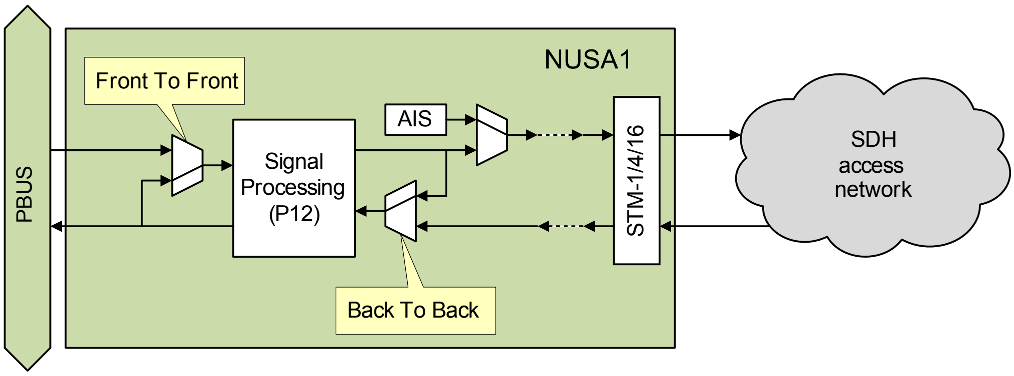


Figure 75: Loops on the P12 access point

- Channel (P12 and P0-nc) front to front loop:
  Loops the received P12 or P0-nc channel signal back towards the SDH interface. The loop is transparent, i.e. no AIS is transmitted in direction to the PBUS.

Please note:
To be able to activate a diagnostic loop the channel CTP must be the source (a-End) of a configured connection.

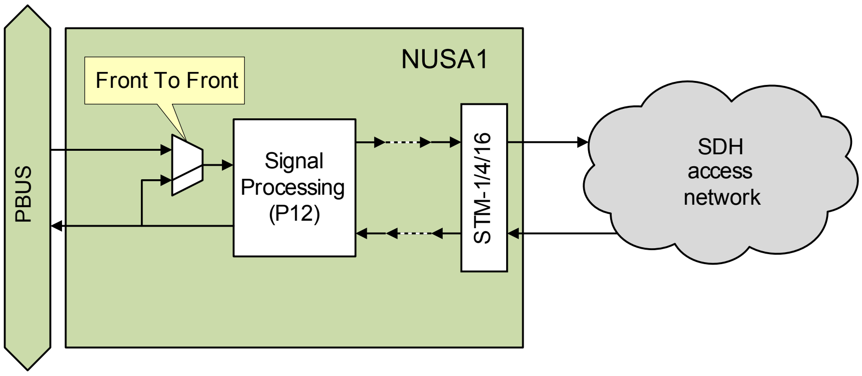


Figure 76: Loop on the channel access point

It is also possible to apply P12 and P0-nc loops with unidirectional cross connections.

Please note:
Only the unidirectional cross connections for the front to front loops are applicable.

Table 48: Loops with unidirectional cross connections

Loop	Signal type	Signal name
Front to front	P12	/unit-a/pdh/vc12-x/p12/chan-y [a]
Front to front	P0-nc	/unit-a/pdh/vc12-x/p12/chan-y [a]
Back to back	P0-nc	not applicable

a. This loop requires the corresponding cross connections on the VC-4 and VC-12 layers.

7.3 Detection of Signal Defects

Bit or block errors in a signal are detectable by checking the signal's associated error detection code (EDC). An example of the EDC is the SDH BIP-N (bit interleaved parity of level N).

The procedure to set and clear an excessive or degraded signal defect is as follows, assuming a poisson error distribution. Refer to ITU-T G.806, clause 6.2.3.1.1:

- The signal defect is set if the equivalent bit error ratio (BER) exceeds a preset threshold.
- The signal defect is cleared if the equivalent BER is better than the preset threshold divided by 10.

NUSA1 offers the evaluation of the excessive and degraded signal defects on the following layers:

- MS16
- MS4
- MS1
- VC-4
- VC-3
- VC-12

The thresholds to set a signal defect are configurable in the ECST. The configuration is done individually for the MS16, MS4 and MS1, and per unit for the VC-4, VC-3 and VC-12:

Table 49: Signal defect parameters

Layer	EDC	Blocks/s	Excessive signal defect		Degraded signal defect	
			Threshold range	Threshold default	Threshold range	Threshold default
MS16	BIP-1	3’072’000	10E-3 … 10E-5	10E-3	10E-5 … 10E-8	10E-6
MS4	BIP-1	768’000	10E-3 … 10E-5	10E-3	10E-5 … 10E-8	10E-6
MS1	BIP-1	192’000	10E-3 … 10E-5	10E-3	10E-5 … 10E-8	10E-6
VC-4	BIP-8	8’000	10E-3 … 10E-5	10E-3	10E-5 … 10E-8	10E-6
VC-3	BIP-8	8’000	10E-3 … 10E-5	10E-3	10E-5 … 10E-8	10E-6
VC-12	BIP-2	2’000	10E-3 … 10E-5	10E-3	10E-5 … 10E-8	10E-6

7.4 Trail Trace Identifier (TTI)

The trail trace identifier (TTI) is a means to identify each direction of a bidirectional path. A wrong cross connection of the path within the network is detected and generates an alarm.

- At the transmit side, the configured “Transmitted TTI” string is inserted into the TTI byte.
- At the receive side, the received TTI is extracted from the TTI byte. The received TTI is then compared with the configured “Expected TTI” for that signal.
- If the received TTI and the configured “Expected TTI” are not the same, the trace identifier mismatch (TIM) alarm indicates a wrong connection somewhere in the network.

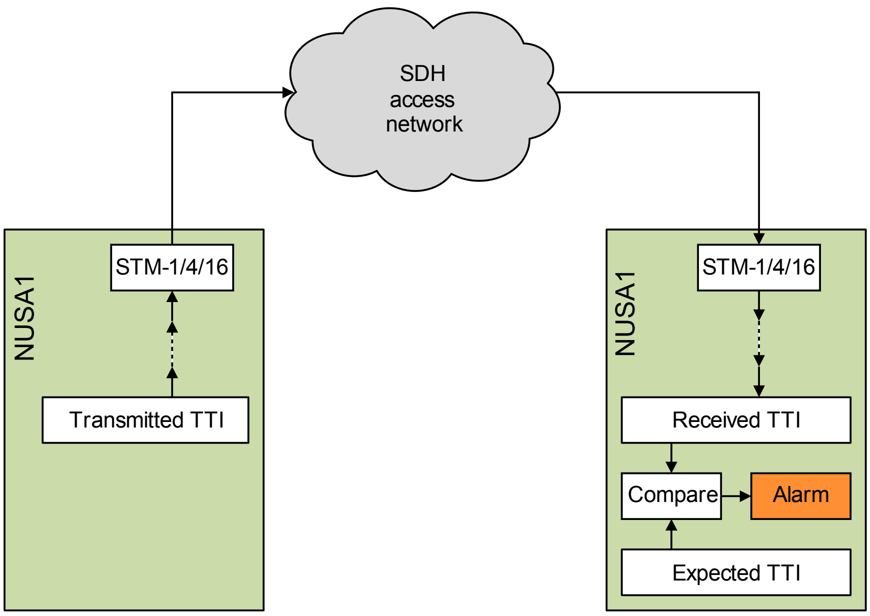


Figure 77: TTI application

The TTI is implemented in accordance with ITU-T G.806. It uses the 16 bytes / 15 characters format for all layers.

TTI on NUSA1 is supported for the following layers:

- RS,
- VC-4 terminated,
- VC-12 terminated,
- EoS VC-4, one transmitted TTI per EoS group, display of the received TTI for every group member,
- EoS VC-3, one transmitted TTI per EoS group, display of the received TTI for every group member,
- EoS VC-12, one transmitted TTI per EoS group, display of the received TTI for every group member,
- P12 (proprietary TTI, future release).

Please note:

In accordance to the ITU-T recommendation, the TTI always requires all the 15 characters. If a TTI is not completely defined, the NUSA1 will supplement “SPACE” characters up to a total of 15 characters.

Risk of operating trouble!

The UMUX service unit SYN4E uses the “NUL” character to fill up a not completely defined TTI.

→ To be interoperable with the NUSA1 unit you have to fill up the transmitted and expected TTI values in the SYN4E unit with “SPACE” characters.

7.5 Maintenance

7.5.1 Inventory Data

It is possible to read inventory data from the NUSA1 unit via the ECST with the following access point:

AP: /unit-x, Main - Inventory.

7.5.2 Unit ESW Download

It is possible to update the embedded software (ESW) of the NUSA1 unit via software download.

Please refer to [355] User Manual “ECST” for the description of the ESW download.

Risk of operating trouble!

The assignment of new embedded software restarts the NUSA1 unit.

Thus, the installation of new ESW on the unit affects all traffic functions of the NUSA1 unit.

7.5.3 ESW Upgrade with EQP

When upgrading the ESW on 1:1 equipment protected NUSA1 units, care must be taken concerning the traffic interruptions and which unit will finally be the active unit. At the end of the upgrade procedure the working unit shall be the active unit.

It is assumed that the working unit is plugged in slot 4 and the protecting unit is plugged in slot 6 of the XMC25 subrack.

ESW upgrade procedure 1

The following procedure provides the upgrade process with one traffic interruption of up to four minutes.

Please note:

A typical ESW upgrade will interrupt the traffic for a duration as indicated above.

→ The ESW upgrade procedure 2 provides two shorter interruptions.

Isolate the working unit

Proceed as follows:

1. Isolate the working NUSA1 unit:
   - AP: /unit-4, Status – EQP.
   - Execute the “Isolate Unit” command.

Result: The working NUSA1 unit is isolated, i.e. it will not perform a protection switchover.

ESW download and start

Proceed as follows:

1. Open the “Software Download” dialogue:
   - Menu NE - Software Download….
2. Configure the ESW download for the working NUSA1 unit:
   - Click on the table row with ID “/unit-4”.
   - In the “Software to install” column select the new ESW to be installed.
   - In the “Delete unused Software” column tick the selection box.
3. Configure the ESW download for the protecting NUSA1 unit:
   - Click on the table row with ID “/unit-6”.
   - In the “Software to install” column select the new ESW to be installed.
   - In the “Delete unused Software” column tick the selection box.
4. Execute the “Download and Start…” command.
   - The “Parameters for command Download and Start” opens.
5. Select the download algorithm:
   - Algorithm = Upgrade Units Only.
6. Execute “OK”.
   - The new ESW is downloaded and becomes active on the working and the protecting units.
   - Traffic will be interrupted for up to four minutes (but see note above!).

Result: The new ESW is active on the working and the protecting NUSA1 units. The working NUSA1 unit in slot 4 remains the active unit.

Join the working unit

Proceed as follows:

1. Join the working NUSA1 unit:
   - AP: /unit-4, Status – EQP.
   - Execute the “Join Unit” command.

Result: The working NUSA1 unit is able again to perform a protection switchover.

End of instruction

ESW upgrade procedure 2

An alternative procedure requires two shorter interruptions of up to 8 s instead of one long interruption. Please refer to the note above.

ESW download

Proceed as follows:

1. Open the “Software Download” dialogue:
   - Menu NE - Software Download….
2. Configure the ESW download for the working NUSA1 unit:
   - Click on the table row with ID “/unit-4”.
   - In the “Software to install” column select the new ESW to be installed.
   - In the “Delete unused Software” column tick the selection box.
3. Configure the ESW download for the protecting NUSA1 unit:
   - Click on the table row with ID “/unit-6”.
   - In the “Software to install” column select the new ESW to be installed.
   - In the “Delete unused Software” column tick the selection box.

4. Execute the “Download” command.
   - The new ESW is downloaded to the working and the protecting NUSA1 units

Result: The ESW download is complete.

ESW upgrade on the protecting unit

Proceed as follows:

1. Navigate to the software configuration dialogue:
   - AP: /unit-6, Main - Software.
2. Set the parameters in the “Configuration” frame:
   - Software = Select the downloaded software.
   - Software Installation = Manual Start
   - Execute the “Apply” command.
3. Save the configuration:
   - Click on the “Save to NE” button.
4. Start the new ESW on the protecting NUSA1 unit:
   - Execute the “Start Software” command.
   - The new ESW becomes active on the protecting unit. This takes up to four minutes.

Result: The ESW upgrade on the protecting unit is complete.

Manual switch to protecting unit

1. Navigate to the EQP status dialogue on the working unit:
   - AP: /unit-4, Status - EQP.
2. Perform a manual switch-over from the working to the protecting NUSA1 unit:
   - Execute the “Manual Switch-Over” command.
   - Traffic will be switched to the protecting unit.
   - Traffic will be interrupted for up to 8 s.

Result: The protecting NUSA1 unit is active.

ESW upgrade on the working unit

1. Navigate to the software configuration dialogue:
   - AP: /unit-4, Main - Software.
2. Set the parameters in the “Configuration” frame:
   - Software = Select the downloaded software.
   - Software Installation = Manual Start
   - Execute the “Apply” command.
3. Save the configuration:
   - Click on the “Save to NE” button.
4. Start the new ESW on the working NUSA1 unit:
   - Execute the “Start Software” command.
   - The new ESW becomes active on the protecting unit. This takes up to four minutes.
   - Wait until the working unit has rebooted.

Result: The ESW upgrade on the working unit is complete.

Manual switch to working unit

1. Navigate to the EQP status dialogue on the working unit:
   - AP: /unit-4, Status - EQP.

2. Perform a manual switch-over from the protecting to the working NUSA1 unit:
   - Execute the “Manual Switch-Over” command.
   - Traffic will be switched to the working unit.
   - Traffic will be interrupted for up to 8 s.

Result: The ESW upgrade is complete and the working NUSA1 unit is active.

End of instruction

8 User Interface Reference

This section gives a complete reference of the managed objects, properties, and commands of the NUSA1 service unit as far as these are not covered in the generic descriptions in [302] User Guide “XMC25/XMC23/XMC22”.

For a description on how to configure and bring into operation the NUSA1 unit and its main functions, please refer to section 6 Commissioning (on page 112).

8.1 Introduction

Below, you will find a detailed description of all the configuration parameters and operations belonging to the managed objects model (MOM) for the NUSA1 functional unit.

Figure 78 "MOM (managed object model) of the NUSA1 unit" shows the access point (AP) tree for an active NUSA1 unit with its managed objects.

Figure 79 "MOM (managed object model) of the standby NUSA1 unit" shows the access point (AP) tree for a standby NUSA1 unit with its managed objects.

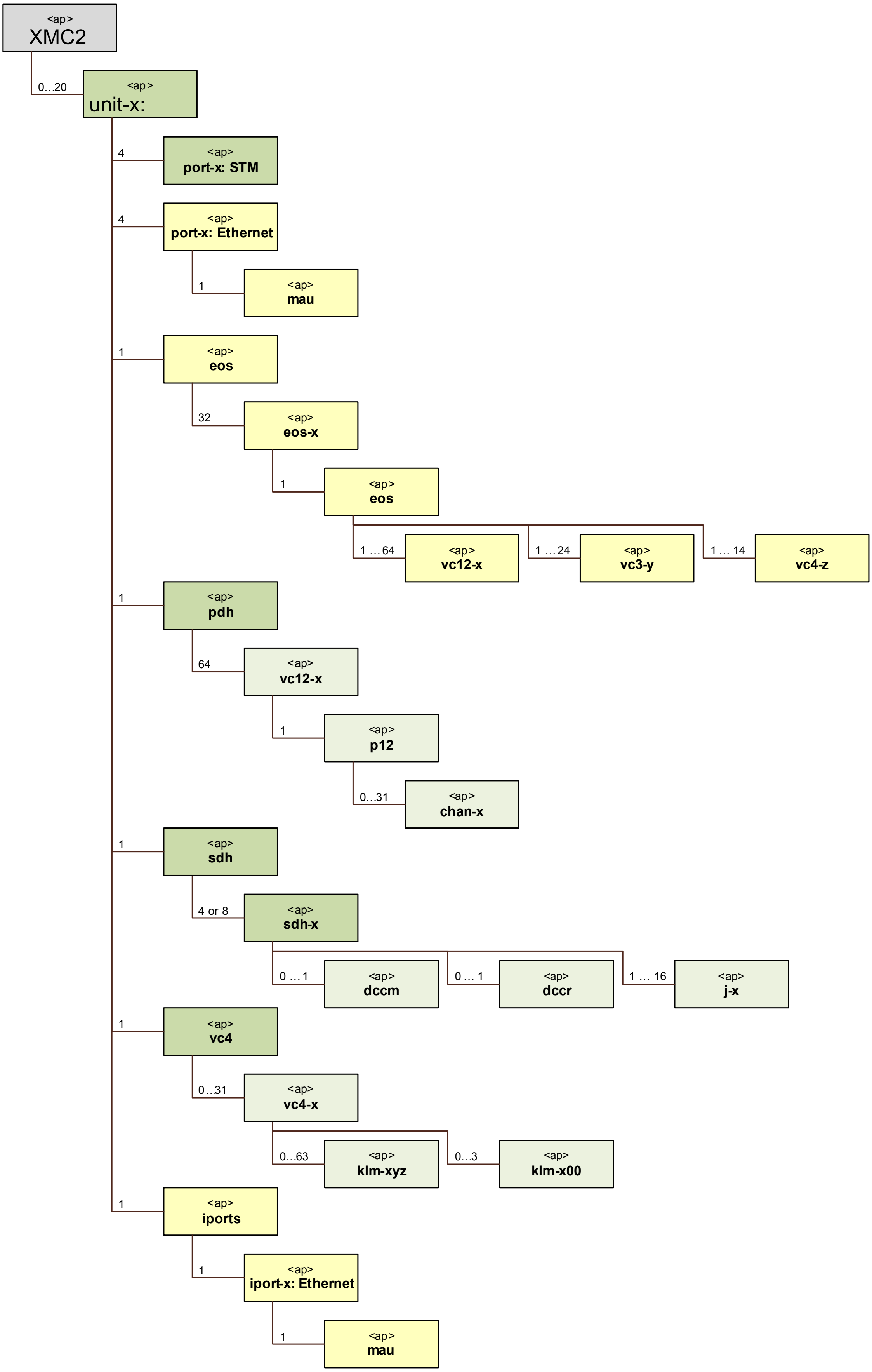


Figure 78: MOM (managed object model) of the NUSA1 unit

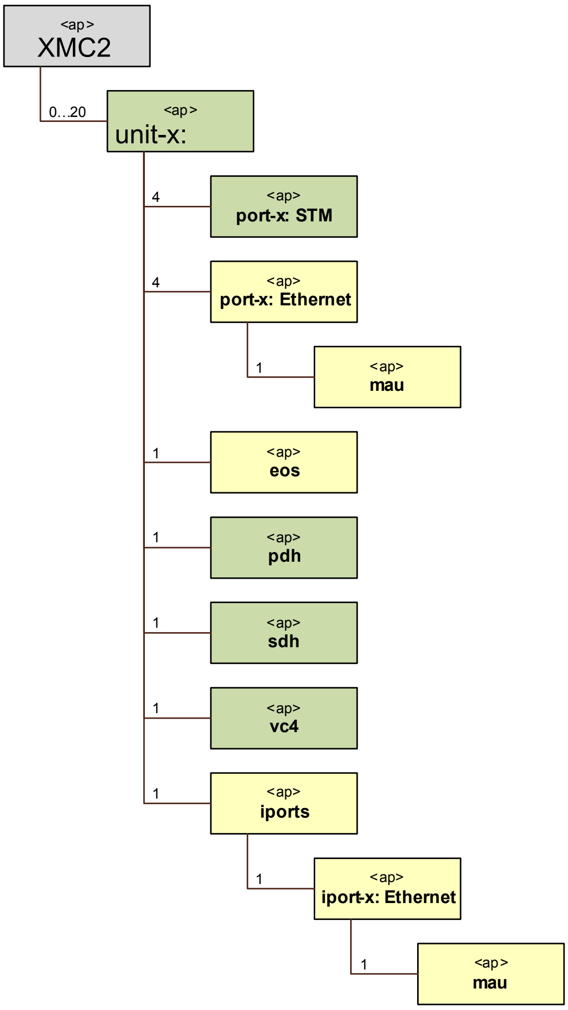


Figure 79: MOM (managed object model) of the standby NUSA1 unit

With these managed objects (MOs) the following functions are covered:

Table 50: Managed objects (MOs) for NUSA1

MO	Description of the management functions
unit-x: NUSA1 Rxx (nusa1_r3b)	Restart of the unit, management of the unit ESW, labelling, indication of the equipment status, display of inventory data, presentation of logbooks. General parameters for VC SNC protection and degraded signal evaluation. SETS and ESO clock selection and priority configuration. SETS and ESO status display. EQP group creation and deletion. EQP status display.
eos	The eos MO contains per default 32 EoS ports.
eos-x	Configure the EoS ports in the switched, unswitched or expansion transport mode. Create and delete an EoS group.
eos	Configure the EoS group. Add and delete EoS group members. Fault management, performance management and status indication of the EoS group.

Table 50: Managed objects (MOs) for NUSA1 (continued)

MO	Description of the management functions
vc12-x vc3-y vc4-z	EoS group members. Fault and performance management. Status indication of the VC and the CTP.
pdh	The pdh MO contains the VC-12/P12 resources accessing the PBUS.
vc12-x	TTI and CTP configuration of the VC-12. Bidirectional protection switching. Fault and performance management. Status indication of the VC and the CTP.
p12	P12 mode and channel configuration. Fault and performance management. Maintenance functions for the P12 signal.
chan-x	Display of the configured channel parameters.
port-x, x = 1 … 4	Configuration of the SDH ports physical section. Fault management and status indication.
port-x, x = 5 … 8	Configuration of the Ethernet front ports speed and duplex, flow control. Fault management and statistics. Port status display.
mau	The mau is the access point for the physical media attachment unit. It provides no fault management functions.
sdh	The sdh MO contains the 4 logical SDH ports of an unprotected NUSA1 unit or the 8 logical SDH ports of an equipment protected NUSA1 unit.
sdh-x	Configuration of the SDH regenerator section, multiplex section and DCC usage. Fault and performance management. MSP configuration and status indication.
dccm	CTP configuration and status of the SDH MS DCC signals.
dccr	CTP configuration and status of the SDH RS DCC signals.
j-x	CTP configuration and status of the SDH ports VC-4 signals.
vc4	Create and delete a VC-4 with a TUG-3 structure.
vc4-x	TUG-3 structure, TTI and CTP configuration of the VC-4. Fault and performance management. Status indication of the VC and the CTP.
klm-xyz	VC-12 CTP configuration and status indication.
klm-x00	VC-3 CTP configuration and status indication.
iports	The iports MO contains the internal Ethernet port.
iport-x, x = 1	Management of the Ethernet internal port. The internal Ethernet port connects the NUSA1 unit via the GbE star with the core unit.
mau	The mau is the access point for the physical media attachment unit. It provides no fault management functions.

For each of the managed objects, properties and commands, the GUI “Tree Views” are given.

This reference section comprises the management functions:

- Overview,
- Main,
- Statistics,
- Configuration,
- Fault Management,
- Performance Management, and
- Status.

Most of the APs only offer a part of the management functions listed above.

The order of appearance of the management function descriptions is in accordance with the APs in the ECST AP tree and the availability of the management functions of each AP.

In the tables of the sections below, the parameter default values for properties are underlined.

Please note:

For better legibility of numbers in this user guide, inverted commas are used when the number's size exceeds three digits (e.g. 40'000). In parameter entry fields of the ECST, these inverted commas must not be entered. Instead, the numbers are entered without these inverted commas (e.g. 40000).

Please note:

Screenshots presented in this reference are examples and show configurations or data that may not correspond to the view you see when managing your XMC20 equipment.

8.2 AP: / unit-x: NUSA1

8.2.1 AP: / unit-x, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”,
- “Overview - Mirroring”,
- “Overview - Port Type”,
- “Overview - STM Allocation”,
- “Overview - VC4 TUG Allocation”,
- “Overview - Timeslot Allocation”,
- “Overview - Unused Channels”, and
- “Overview - Statistics”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.2.2 AP: / unit-x, Main

For a description of the
- “Main - General”,
- “Main - Equipment”,
- “Main - Inventory”,
- “Main - Logbooks”, and
- “Main - Software”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.2.3 AP: / unit-x, Configuration

8.2.3.1 AP: / unit-x, Configuration - General - SNCP Times

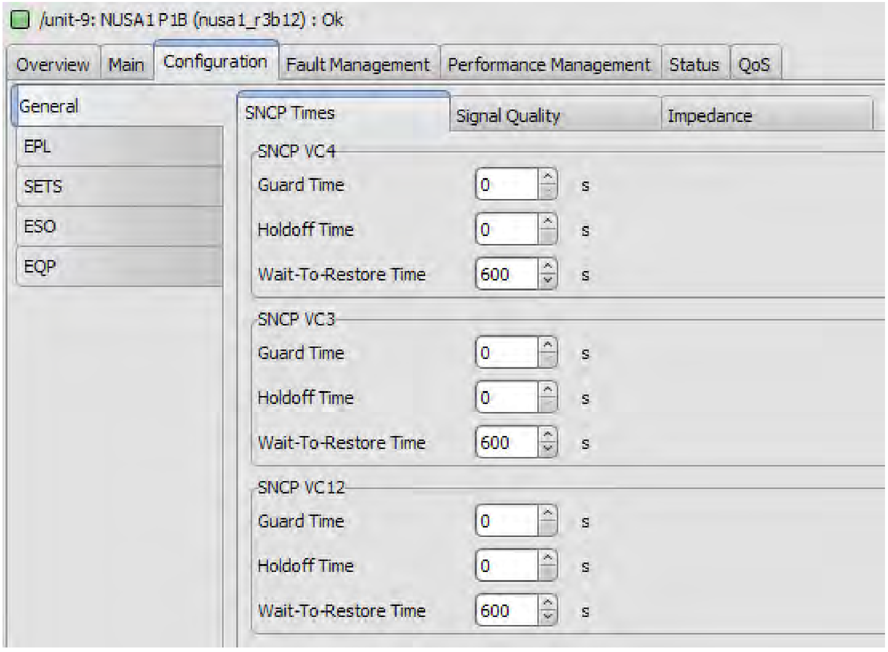


Table 51: AP: / unit-x, Configuration - General - SNCP Times

Operation Name	Parameter Name	Range	Description / Details
SNCP VC4	Guard Time	0 … 60 s	The holdoff and guard times are configured per VC type for the whole unit. The guard time is the time interval after an automatic protection switchover when no additional switchover is allowed. The holdoff time is the time interval to define how long the switching criteria have to be active before the protection switchover is activated. For further information please refer to section 6.2 SNCP Configuration (on page 131). The revertive operation type of the SNC protected VC signal provides the configuration of the wait to restore (WTR) timer. The WTR timer is configured per VC type for the whole unit. A path selector which selects the protecting path switches back to the working path as soon as the configured WTR timer elapses. The WTR timer is reset when the working path is in a failure state and starts when the working path becomes fault free.
	Holdoff Time	0 … 20 s	
	Wait-To-Restore Time	0 … 600 … 1800 s	
SNCP VC3	Guard Time	0 … 60 s	
	Holdoff Time	0 … 20 s	
	Wait-To-Restore Time	0 … 600 … 1800 s	
SNCP VC12	Guard Time	0 … 60 s	
	Holdoff Time	0 … 20 s	
	Wait-To-Restore Time	0 … 600 … 1800 s	

8.2.3.2 AP: / unit-x, Configuration - General - Signal Quality

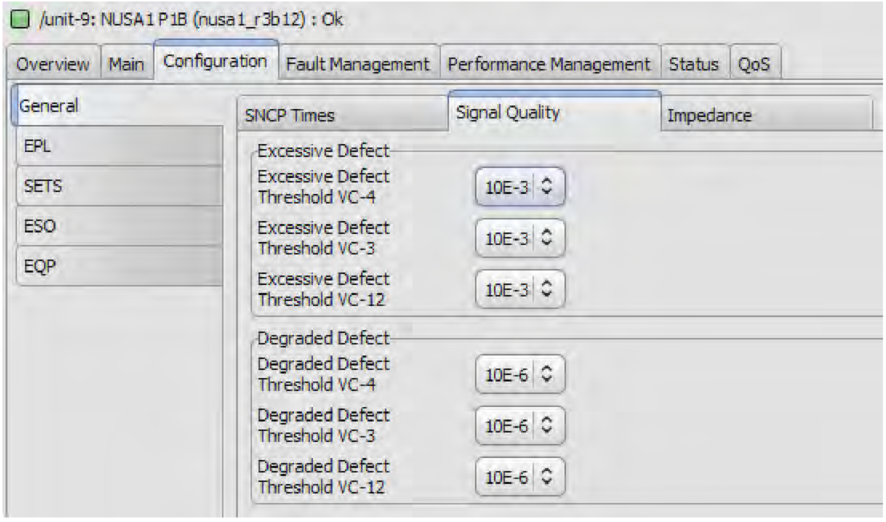


Table 52: AP: / unit-x, Configuration - General - Signal Quality

Operation Name	Parameter Name	Range	Description / Details
Excessive Defect	Excessive Defect Threshold VC-4	10E-3 … 10E-5	The bit error ratio for the excessive signal defect are configured per VC type for the whole unit. Please refer to section 7.3 Detection of Signal Defects (on page 153) for a description of the excessive signal defect evaluation. Please note that the error distribution for the excessive signal is assumed to be poisson.
Excessive Defect	Excessive Defect Threshold VC-3	10E-3 … 10E-5	
Excessive Defect	Excessive Defect Threshold VC-12	10E-3 … 10E-5	
Degraded Defect	Degraded Defect Threshold VC-4	10E-5 … 10E-6 … 10E-8	The bit error ratio for the degraded signal defect are configured per VC type for the whole unit. Please refer to section 7.3 Detection of Signal Defects (on page 153) for a description of the degraded signal defect evaluation. Please note that the error distribution for the degraded signal is assumed to be poisson.
Degraded Defect	Degraded Defect Threshold VC-3	10E-5 … 10E-6 … 10E-8	
Degraded Defect	Degraded Defect Threshold VC-12	10E-5 … 10E-6 … 10E-8	

8.2.3.3 AP: / unit-x, Configuration - General - Impedance

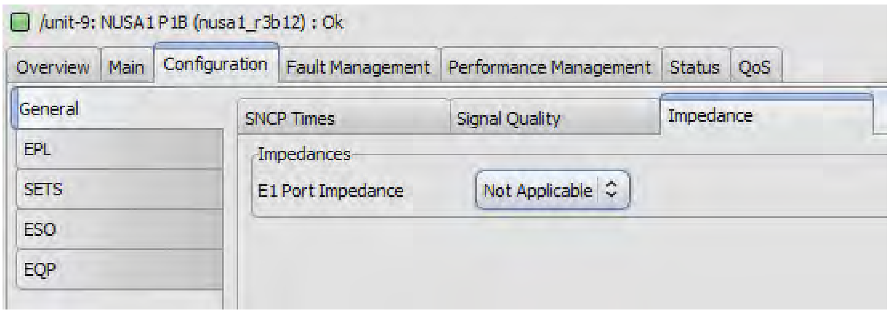


Table 53: AP: / unit-x, Configuration - General - Impedance

Operation Name	Parameter Name	Range	Description / Details
Impedance	E1 Port Impedance	Not Applicable	The NUSA1 has no E12 front ports. This parameter is not applicable.

8.2.3.4 AP: / unit-x, Configuration - EPL

Please note:

An Ethernet port used in an Ethernet Private Line (EPL) must be configured to the port mode “unswitched” in the ECST “Switching” tab ***before*** *assigning it to an EPL EoS port.*

Please note:

An EoS port used in an Ethernet Private Line (EPL) must be configured to the port mode “unswitched” in the ECST “Switching” tab ***before*** *assigning it to an EPL Ethernet port.*

Please note:

Refer to section 5.5.3 Ethernet Switch (on page 71) for further information.

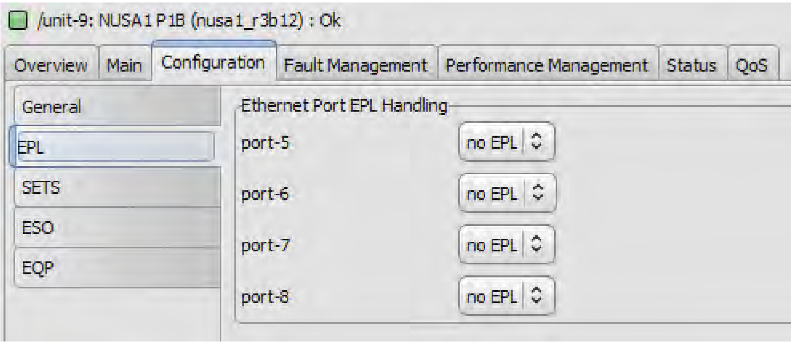


Table 54: AP: / unit-x, Configuration - EPL

Operation Name	Parameter Name	Range	Description / Details
Ethernet Port EPL Handling	port-5	no EPL	The Ethernet port participates in the VLAN bridge.
		eos-1	The Ethernet port and the EoS port eos-1 (100 Mbit/s) or eos-9 (1 Gbit/s) are interconnected with a point-to-point connection, bypassing the VLAN bridge.
		eos-9	
	port-6	no EPL	The Ethernet port participates in the VLAN bridge.
		eos-2	The Ethernet port and the EoS port eos-2 (100 Mbit/s) or eos-10 (1 Gbit/s) are interconnected with a point-to-point connection, bypassing the VLAN bridge.
		eos-10	
	port-7	no EPL	The Ethernet port participates in the VLAN bridge.
		eos-3	The Ethernet port and the EoS port eos-3 (100 Mbit/s) are interconnected with a point-to-point connection, bypassing the VLAN bridge.
	port-8	no EPL	The Ethernet port participates in the VLAN bridge.
		eos-4	The Ethernet port and the EoS port eos-4 (100 Mbit/s) are interconnected with a point-to-point connection, bypassing the VLAN bridge.

Risk of operating trouble!

The EoS ports eos-9 and eos-11, and if applicable the EoS ports eos-13 to eos-17 and/or eos-23 to eos-27, share one unit internal physical 1 Gb Ethernet link.

→ When using the EoS port eos-9 in an Ethernet Private Line, the EoS ports eos-11, eos-13 to eos-17 and eos-23 to eos-27 are no longer available.

Please note:

When using the EoS port eos-9 in an Ethernet Private Line, also the EoS port eos-11 must be configured to the port mode “unswitched” in the ECST “Switching” tab ***before*** *assigning the EoS port eos-9 to an EPL Ethernet port.*

Risk of operating trouble!

The EoS ports eos-10 and eos-12, and if applicable the EoS ports eos-18 to eos-22 and/or eos-28 to eos-32, share one unit internal physical 1 Gb Ethernet link.

→ When using the EoS port eos-10 in an Ethernet Private Line, the EoS ports eos-12, eos-18 to eos-22 and eos-28 to eos-32 are no longer available.

Please note:

When using the EoS port eos-10 in an Ethernet Private Line, also the EoS port eos-12 must be configured to the port mode “unswitched” in the ECST “Switching” tab ***before*** *assigning the EoS port eos-10 to an EPL Ethernet port.*

8.2.3.5 AP: / unit-x, Configuration - SETS

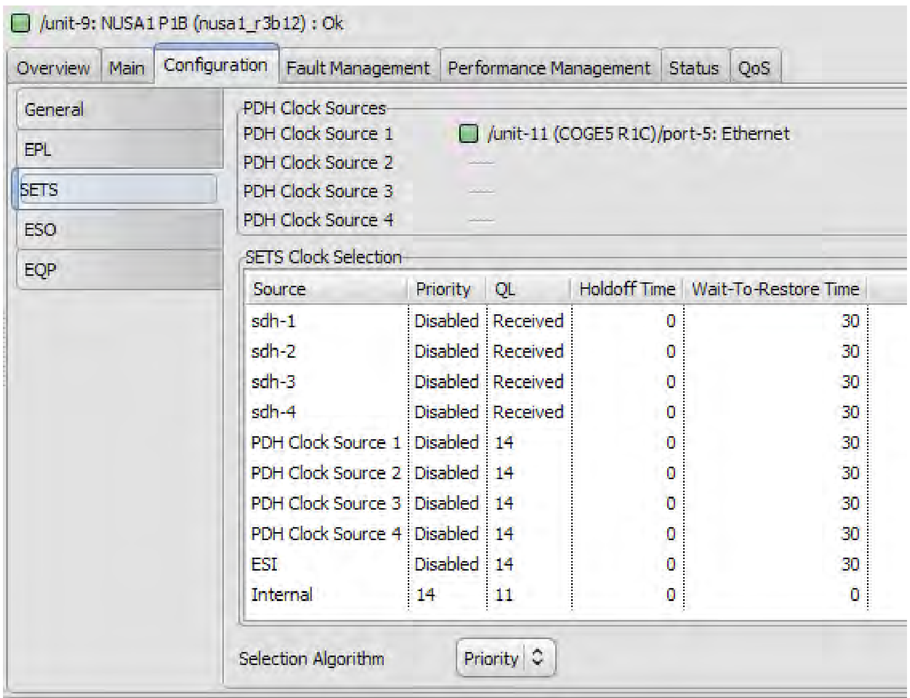


Table 55: AP: / unit-x, Configuration - SETS

Operation Name	Parameter Name	Range	Description / Details
PDH Clock Sources	PDH Clock Source 1	<MO address>	The managed object address of the four PDH clock sources. These parameters are read-only.
	PDH Clock Source 2	<MO address>	
	PDH Clock Source 3	<MO address>	
	PDH Clock Source 4	<MO address>	
SETS Clock Selection	Source	sdh-1	Available timing sources for the SETS synchronization. Note that the sdh-5 to sdh-8 sources can only be used if a protecting NUSA1 unit is available. These values are read-only. For more information regarding quality level handling please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	
		Internal	
	Priority	1 … 14	The priority of a timing source is used as a selection criterion if the selection algorithm is configured to “priority based” (see below). 1 is the highest priority, 14 is the lowest priority. It is possible to assign the same priority to more than one source.
		<u>Disabled</u>	A disabled timing source is not used for the SETS synchronization. The internal timing source cannot be disabled.

Table 55: AP: / unit-x, Configuration - SETS (continued)

Operation Name	Parameter Name	Range	Description / Details
	QL	1 … 14	The quality level QL of a timing source is used as a selection criterion if the selection algorithm is configured to “QL based” (see below). 1 is the highest QL, 14 is the lowest QL. Assign a QL for timing sources that provide no QL or if you want to fix the QL for a timing source. Note that the use of some of the QL values is standardized. The default QL of the PDH Clock Sources is “14”. The internal timing source has a default quality level of 11. For more information regarding quality level handling please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.
		Received	Use the QL as received with the timing source. The QL is transported within the SSM (synchronization status message). The default QL of the sdh-x clock sources is “Received”. Timing sources not providing the SSM only have an assigned quality level.
	Holdoff Time	0 … 60 s step 0.1 s	During the holdoff time the timing source selection process performs no switchover to a lower priority or lower quality level timing source. The holdoff timer starts when the timing source enters a failure state.
	Wait-To-Restore Time	0 … 30 … 720 s step 1 s	During the wait to restore (WTR) time the timing source selection process performs no switchover from a lower priority or lower quality level timing source. The WTR timer is reset when the timing source is in a failure state and starts when the timing source becomes fault free.
Selection Algorithm	Selection Algorithm	Priority	Select the timing sources according to the assigned priorities. This selection algorithm disregards the quality levels (QL).
		QL	Select the timing sources according to the received or assigned quality levels (QL). The selection algorithm first considers the QL and then the priority.

8.2.3.6 AP: / unit-x, Configuration - ESO

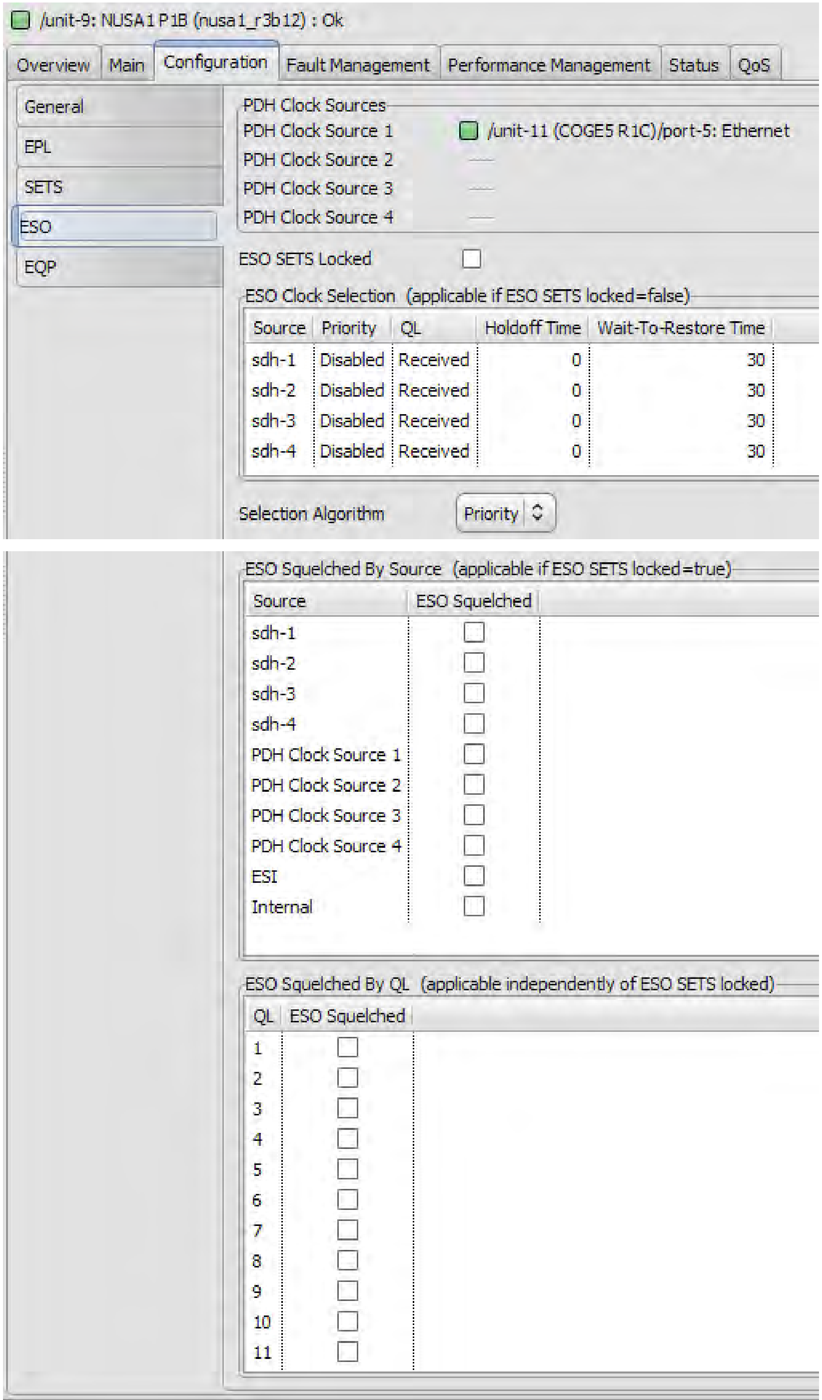


Table 56: AP: / unit-x, Configuration - ESO

Operation Name	Parameter Name	Range	Description / Details
PDH Clock Sources	PDH Clock Source 1	<MO address>	The managed object address of the four PDH clock sources. These parameters are read-only.
	PDH Clock Source 2	<MO address>	
	PDH Clock Source 3	<MO address>	
	PDH Clock Source 4	<MO address>	

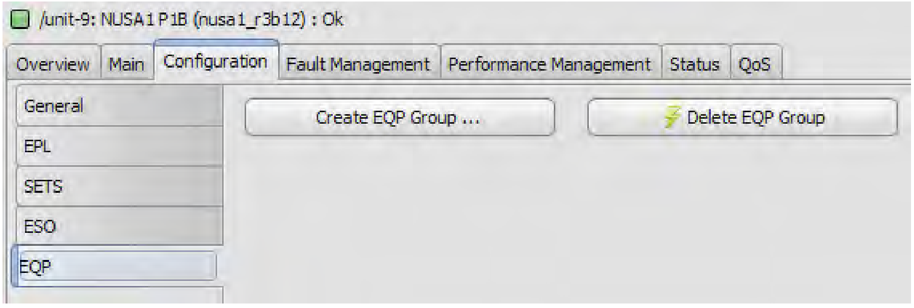
Table 56: AP: / unit-x, Configuration - ESO (continued)

Operation Name	Parameter Name	Range	Description / Details
ESO SETS Locked	ESO SETS Locked	☑	The external synchronization output on the COGE5 unit is synchronized to the SETS function. For more information regarding ESO please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.
		☐	The external synchronization output on the COGE5 unit is synchronized to the selected ESO clock source.
ESO Clock Selection	Source	sdh-1 sdh-2 sdh-3 sdh-4 sdh-5 sdh-6 sdh-7 sdh-8	Note that the ESO Clock Selection parameters are only applicable for the **non SETS locked** mode, i.e. “ESO SETS locked” = false. Refer to the parameter above. Available timing sources for the ESO synchronization. Note that the sdh-5 to sdh-8 sources can only be used if a protecting NUSA1 unit is available. The source parameter values are read-only. For more information regarding quality level handling please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.
	Priority	1 … 14	The priority of a timing source is used as a selection criterion if the selection algorithm is configured to “priority based” (see below). 1 is the highest priority, 14 is the lowest priority. It is possible to assign the same priority to more than one source.
		Disabled	A disabled timing source is not used for the SETS synchronization.
	QL	1 … 14	The quality level QL of a timing source is used as a selection criterion if the selection algorithm is configured to “QL based” (see below). 1 is the highest QL, 14 is the lowest QL. Assign a QL for timing sources that provide no QL or if you want to fix the QL for a timing source. Note that the use of some of the QL values is standardised. For more information regarding quality level handling please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.
		Received	Use the QL as received with the timing source. The QL is transported within the SSM (synchronization status message). Timing sources not providing the SSM only have an assigned quality level
	Holdoff Time	0 … 60 s step 0.1 s	During the holdoff time the timing source selection process performs no switchover to a lower priority or lower quality level timing source. The holdoff timer starts when the timing source enters a failure state.

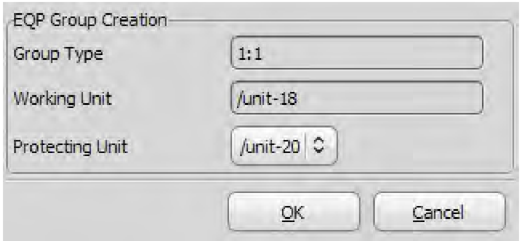
Table 56: AP: / unit-x, Configuration - ESO (continued)

Operation Name	Parameter Name	Range	Description / Details
	Wait-To-Restore Time	0 … 30 … 720 s	During the wait to restore (WTR) time the timing source selection process performs no switchover from a lower priority or lower quality level timing source. The WTR timer is reset when the timing source is in a failure state and starts when the timing source becomes fault free.
Selection Algorithm	Selection Algorithm	Priority	Select the timing sources in the non SETS locked mode according to the assigned priorities. This selection algorithm disregards the quality levels (QL).
		QL	Select the timing sources in the non SETS locked mode according to the received or assigned quality levels (QL). The selection algorithm first considers the QL and then the priority.
ESO Squelched By Source	Source	sdh-1 sdh-2 sdh-3 sdh-4 sdh-5 sdh-6 sdh-7 sdh-8 PDH Clock Source 1 PDH Clock Source 2 PDH Clock Source 3 PDH Clock Source 4 ESI Internal	Note that the ESO Squelched By Source parameters are only applicable for the **SETS locked** mode, i.e. “ESO SETS locked” = true. Refer to the parameter above. Available timing sources for the ESO synchronization. Note that the sdh-5 to sdh-8 sources can only be used if a protecting NUSA1 unit is available. These values are read-only.
	ESO Squelched	☑	The ESO output on the COGE5 unit is squelched, i.e. disabled, if the corresponding source is selected.
		☐	The ESO output on the COGE5 unit is active, i.e. enabled, if the corresponding source is selected.
ESO Squelched By QL	QL	1 … 15	Note that the ESO Squelched By QL parameters are applicable for the **SETS locked** and the **non SETS locked** modes, i.e. “ESO SETS locked” = true or false. Quality levels of the timing sources for the ESO synchronization. These values are read-only.
	ESO Squelched	☑	The ESO output on the COGE5 unit is squelched for the selected QL.
		☐	The ESO output on the COGE5 unit is active for the selected QL.

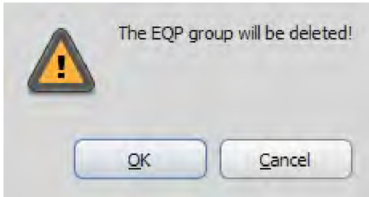
8.2.3.7 AP: / unit-x, Configuration - EQP



"Create EQP Group" dialogue



"Delete EQP Group" dialogue



Please note:

The roles of working and protecting unit is fixed within a slot pair.

→ Please refer to Table 28: "XMC20 slot pairs for NUSA1 EQP" (on page 101).

Table 57: AP: / unit-x, Configuration - EQP

Operation Name	Parameter Name	Range	Description / Details
Create EQP Group …			Open the dialogue for the creation of an equipment protection (EQP) group.
EQP Group Creation	Group Type	1:1	Type of the EQP group.
	Working Unit	<MO address>	MO address of the working unit, e.g. /unit-18. In the ECST the working unit MO address is read-only.
	Protecting Unit	<MO address> -	List of the MO addresses of all HW and SW compatible units which are not assigned, e.g. /unit-20. Default is no unit selected.
Delete EQP Group			Delete an existing protection group. Traffic on the protecting unit will be interrupted and services will be re-established on the working unit. The protecting unit will become unassigned.

Please note:

The creation and deletion of an EQP group must be done on the working unit.

8.2.4 AP: / unit-x, Fault Management

For the a description of the general aspects of the

- "Fault Management - Status", and
- "Fault Management - Configuration"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22". The following table lists the fault causes of the current AP.

Table 58: AP: / unit-x, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
SWM	Software Mismatch	Equipment Alarm	☐	Minor	The running ESW does not match the assigned ESW.
SSWNA	Scheduled Software Not Available	Equipment Alarm	☐	Minor	The ESW that is scheduled for installation is not available on the unit. Make sure that the ESW is downloaded to the unit.
SWIN	Software Incompatible With Network Element	Equipment Alarm	☑	Major	The running ESW is not compatible with the version required by the NE type or version.
CCE	Configuration or Customization Error	Processing Error Alarm	☑	Major	An invalid configuration has been accepted by the unit by mistake. To get rid of the alarm redo the complete configuration or reboot the unit. If the alarm persists please contact KEYMILE.
PRC	PBUS Resource Conflict	Processing Error Alarm	☑	Major	The PBUS access circuit of another TDM unit in the subrack is defective. Remove or unassign the other TDM units in the subrack one by one until the alarm is cleared. Replace the defective unit.
LOSESI	Loss Of Signal On External Synchronisation Input	Communication Alarm	☐	Warning	Loss of timing source ESI.
LOSP1	Loss Of Signal On PDH Clock Source 1	Communication Alarm	☐	Warning	Loss of timing source on PDH clock source 1.
LOSP2	Loss Of Signal On PDH Clock Source 2	Communication Alarm	☐	Warning	Loss of timing source on PDH clock source 2.
LOSP3	Loss Of Signal On PDH Clock Source 3	Communication Alarm	☐	Warning	Loss of timing source on PDH clock source 3.
LOSP4	Loss Of Signal On PDH Clock Source 4	Communication Alarm	☐	Warning	Loss of timing source on PDH clock source 4.
LOSS1	Loss Of Signal On SDH Clock Source 1	Communication Alarm	☐	Warning	Loss of timing source on SDH port-1, STM-16 or STM-4.
LOSS2	Loss Of Signal On SDH Clock Source 2	Communication Alarm	☐	Warning	Loss of timing source on SDH port-2, STM-16 or STM-4.
LOSS3	Loss Of Signal On SDH Clock Source 3	Communication Alarm	☐	Warning	Loss of timing source on SDH port-3, STM-4 or STM-1.
LOSS4	Loss Of Signal On SDH Clock Source 4	Communication Alarm	☐	Warning	Loss of timing source on SDH port-4, STM-4 or STM-1.
LOSS5	Loss Of Signal On SDH Clock Source 5	Communication Alarm	☐	Warning	Loss of timing source on SDH port-1 of the protecting NUSA1 unit, STM-16 or STM-4.
LOSS6	Loss Of Signal On SDH Clock Source 6	Communication Alarm	☐	Warning	Loss of timing source on SDH port-2 of the protecting NUSA1 unit, STM-16 or STM-4.

Table 58: AP: / unit-x, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
LOSS7	Loss Of Signal On SDH Clock Source 7	Communication Alarm	☐	Warning	Loss of timing source on SDH port-3 of the protecting NUSA1 unit, STM-4 or STM-1.
LOSS8	Loss Of Signal On SDH Clock Source 8	Communication Alarm	☐	Warning	Loss of timing source on SDH port-4 of the protecting NUSA1 unit, STM-4 or STM-1.
SCSL	All Selected Clock Sources Lost	Communication Alarm	☐	Minor	Loss of all SDH Equipment Clock (SEC) timing sources.
SETSSNP	SETS Clock Source Not Primary	Communication Alarm	☐	Warning	The currently active SETS clock source is not the source with the highest priority, on condition that QL-mode is disabled.
SETSHO	SETS Holdover	Communication Alarm	☐	Minor	The SETS is in the holdover state, i.e. all external synchronization sources are lost or the selected source has a frequency offset of more than ±15 ppm. The SETS maintains operation within specifications.
SETSOOL	SETS Out Of Limits	Communication Alarm	☑	Minor	The measured SETS frequency exceeds the limit of ± 15 ppm.
SETSPLL	SETS PLL Out Of Lock	Communication Alarm	☑	Minor	Marks the start-up phase during which the PLL is probably unlocked.
ECSL	All Selected ESO Clock Sources Lost	Communication Alarm	☐	Minor	All configured timing sources for the ESO clock output on the COGE5 unit are lost. The clock output is squelched.
ESOSNP	ESO Clock Source Not Primary	Communication Alarm	☐	Warning	The selected timing source for the ESO clock output on the COGE5 unit is not the one with the highest priority, on condition that QL-mode is disabled.
EQM	Equipment Malfunction	Equipment Alarm	☐	Critical	The NUSA1 controller detects any anomalies on the unit, e.g. a voltage is missing, a chip does not respond, etc.
HWIC	Hardware Incompatible With Configuration	Equipment Alarm	☑	Major	The plugged HW is not compatible with the unit configuration HW stored in the database. You may need to change the HW or re-create the configuration for the unit.
SWIC	Software Incompatible With Configuration	Equipment Alarm	☑	Major	The ESW running on the unit is not compatible with the unit configuration stored in the database. You may need to upgrade, or downgrade the ESW, or re-create the configuration with the currently running ESW.
GSW	General Software Alarm	Equipment Alarm	☐	Major	An ESW internal error has been detected that might inhibit the ESW from running correctly.
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	A maintenance function has been activated by the operator. E.g. the synchronization condition has been manually changed in the timing sources status.

Table 58: AP: / unit-x, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
UNAV	Unit Not Available	Equipment Alarm	☑	Critical	The unit that is configured is either not plugged or not recognized due to a failure.
NSW	No Application Software	Equipment Alarm	☑	Major	There is no application ESW installed on the unit, or the application ESW has not yet finished its boot process.
UNAS	Unit Not Assigned	Equipment Alarm	☐	Warning	The unit is not assigned and cannot be configured. To assign the unit, execute the “Assign” command in the “Main” function of the unit.
UIC	Unit Incompatible	Equipment Alarm	☑	Major	The inserted unit is not compatible with the assigned unit.
PWRSVE	Battery Power Saving	Equipment Alarm	☑	Critical	Power saving is active on the unit, i.e. it is kept in the “reset” state during battery power backup.
EQPUNV	EQP Unit Not Available	Equipment Alarm	☑	Major	The standby unit is not available, i.e. not plugged in or has an equipment failure. This alarm is available on the working and the protecting unit of an EQP group.
EQPHWI	EQP Hardware Incompatible With Configuration	Equipment Alarm	☑	Major	The actual hardware is not compatible with the hardware of the protecting unit. This alarm is available on the working unit of an EQP group only.
EQPSWI	EQP Software Incompatible With Configuration	Equipment Alarm	☑	Major	The running software (ESW) is not compatible with the software on the protecting unit. This alarm is available on the working unit of an EQP group only.
EQPNPR	EQP Group Not Protected	Equipment Alarm	☐	Major	The working or the protecting unit is not available, i.e. not plugged in or has an equipment failure. This alarm is available on the working unit of an EQP group only.
EQPWUI	EQP Working Unit Isolated	Equipment Alarm	☐	Major	The working unit has been isolated with the “Isolate Unit” status command. No protection is available in this state. This alarm is available on the working unit of an EQP group only.
EQPUNA	EQP Working Unit Not Active	Equipment Alarm	☐	Major	An automatic protection switch or a “manual switch” or a “forced switch” to the protecting unit has been done. This alarm is available on the working unit of an EQP group only.

Please note:

Automatic, manual and forced protection switching is available from the working to the protecting unit and vice versa.

→ Please refer to section 5.9 Equipment Protection (EQP) (on page 101).

8.2.5 AP: / unit-x, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

The PM parameters are presented in different groups. The following counter group is available for the NUSA1 unit:

- “Unfiltered Events” group, see section 8.2.5.1 AP: / unit-x, Performance Management - Unfiltered Events (on page 179).

The following counter intervals are available:

Table 59: PM counter interval availability

Counter interval	Unfiltered Events
User Counter	yes
History 15min	yes
History 24h	yes
Alarm 15min	no
Alarm 24h	no

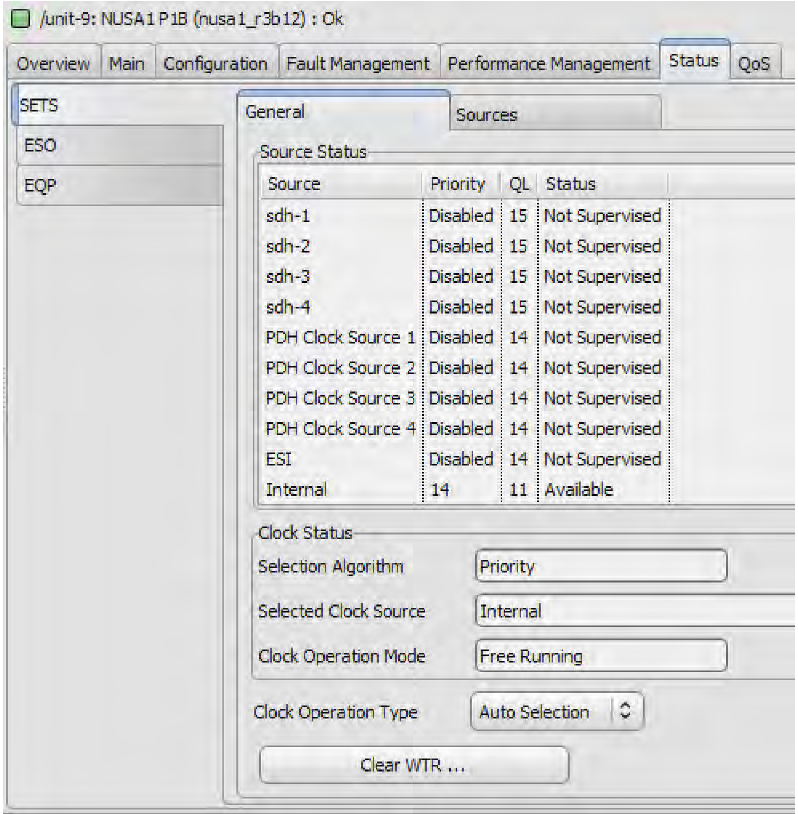
8.2.5.1 AP: / unit-x, Performance Management - Unfiltered Events

Table 60: PM group: Unfiltered Events

PM parameter	Description
SETS Source Switch	The timing source of the SETS function has changed.
ESO Source Switch	The timing source of the ESO clock has changed.

8.2.6 AP: / unit-x, Status

8.2.6.1 AP: / unit-x, Status - SETS - General



“Clear WTR” dialogue:

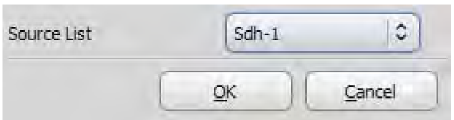


Table 61: AP: / unit-x, Status - SETS - General

Operation Name	Parameter Name	Range	Description / Details
Source Status	Source	sdh-1	List of all timing sources.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	
		Internal	
	Priority	1 … 14	Configured priority value of the timing source.
		<u>Disabled</u>	
	QL	1 … 15	Adjusted or received quality level of the timing source, as it is used by the selection algorithm in the SETS selectors A and B.
	Status	Not Supervised	Disposability of the timing source.
		Available	
		Holdoff	
		Failed	
		Wait To Restore	
Clock Status	Selection Algorithm	Priority	Display of the configured selection algorithm for the timing sources: - Priority Table based - Quality Level based
		QL	
	Selected Clock Source	<Timing Source>	Display of the selected timing source.
	Clock Operation Mode	Free Running	Display of the current operation mode of the SETS system: - Locked: Locked to a traffic signal. - Free-running: SETS synchronized to the internal oscillator. - Holdover: SETS keeps the acquired frequency from a traffic signal which has been lost. The acquired frequency is calculated during 1 minute as the average frequency. The maximum allowed offset for the holdover frequency is ±10 ppm.
		Locked	
		Holdover	

Table 61: AP: / unit-x, Status - SETS - General (continued)

Operation Name	Parameter Name	Range	Description / Details
Clock Operation Type	Clock Operation Type	Auto Selection	With the clock operation type it is possible to force the SETS to change its state for maintenance purposes. These manual commands override the automatic selection. Forced states are not configuration data and thus not stored in the MIB database. A forced clock operation state activates the maintenance function active (MFA) alarm.
		Forced Free Run	
		Forced Holdover	
Clear WTR …			Open the ECST dialogue to select a timing source.
Clear WTR	Source List	sdh-1	The WTR timer can be cleared to immediately switch back from the lower priority or lower quality level timing source.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	

8.2.6.2 AP: / unit-x, Status - SETS - Sources

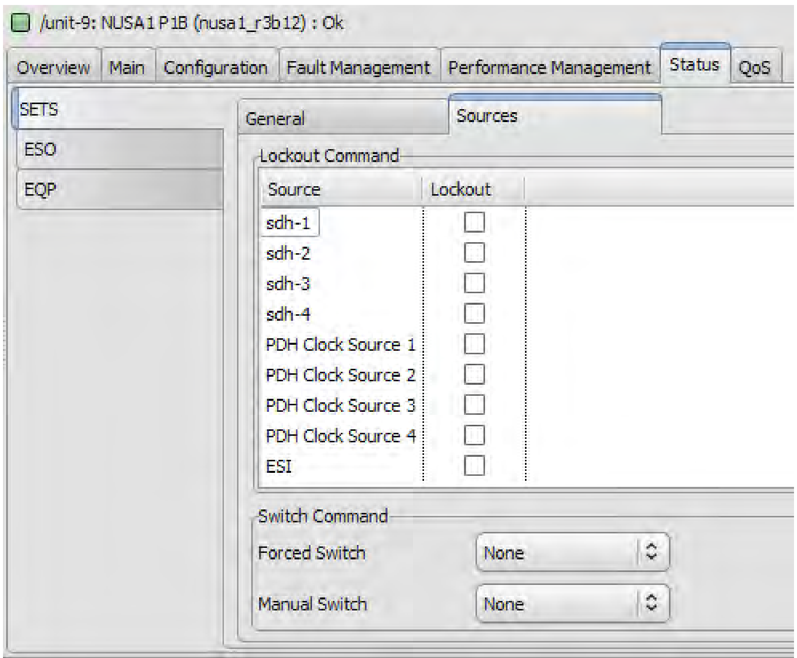


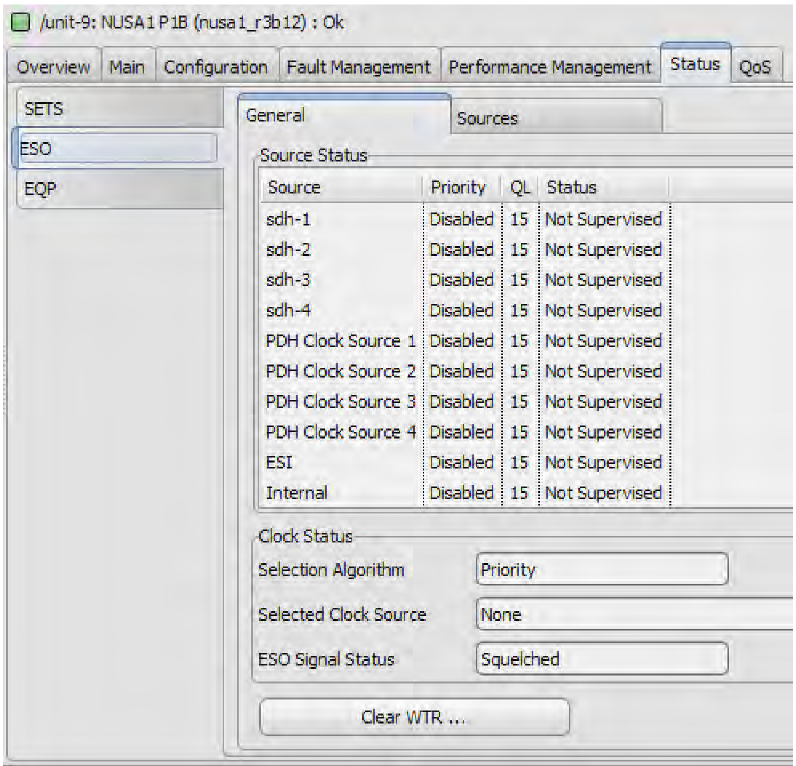
Table 62: AP: / unit-x, Status - SETS - Sources

Operation Name	Parameter Name	Range	Description / Details
Lockout Command	Source	sdh-1	The lockout of a port prevents the selection as a SETS timing source. It is not possible to override the lockout of a source with a forced or manual switch command.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	
	Lockout	☑	locked out
		☐	not locked out
Switch Command	Forced Switch	None	Perform a forced switch to a specific timing source for the SETS. The switch command is only accepted if the source is enabled, i.e. has a priority configured. If the source is not available, i.e. failed or in WTR state, “Internal” is selected.
		sdh-1	
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	

Table 62: AP: / unit-x, Status - SETS - Sources (continued)

Operation Name	Parameter Name	Range	Description / Details
	Manual Switch	<u>None</u>	Perform a manual switch to a specific timing source for the SETS. The switch command is only accepted if no forced switch is active and the source is available. The source is not available if - disabled, or - failed, or - in WTR state.
		sdh-1	
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	

8.2.6.3 AP: / unit-x, Status - ESO - General



“Clear WTR” dialogue:

Table 63: AP: / unit-x, Status - ESO - General

Operation Name	Parameter Name	Range	Description / Details
Source Status	Source	sdh-1	List of all timing sources.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	
		Internal	
	Priority	1 … 14	Configured priority value of the timing source.
		Disabled	
	QL	1 … 15	Adjusted or received quality level of the timing source, as it is used by the selection algorithm in the SETS selectors A and B.
	Status	Not Supervised	Disposability of the timing source.
		Available	
		Holdoff	
		Failed	
		Wait To Restore	
Clock Status	Selection Algorithm	Priority	Display of the configured selection algorithm for the timing sources: - Priority Table based - Quality Level based
		QL	
	Selected Clock Source	<Timing Source>	Display of the selected timing source.
	ESO Signal Status	Active	Display of the current operation mode of the ESO clock output: - Active: The ESO clock signal is active - Squelched: The ESO clock signal is squelched due to the selected timing source or due to the QL of the selected timing source.
		Squelched	
Clear WTR…			Open the ECST dialogue to select a timing source.

Table 63: AP: / unit-x, Status - ESO - General (continued)

Operation Name	Parameter Name	Range	Description / Details
Clear WTR	Source List	sdh-1	The WTR timer can be cleared to immediately switch back from the lower priority or lower quality level timing source.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	

8.2.6.4 AP: / unit-x, Status - ESO - Sources

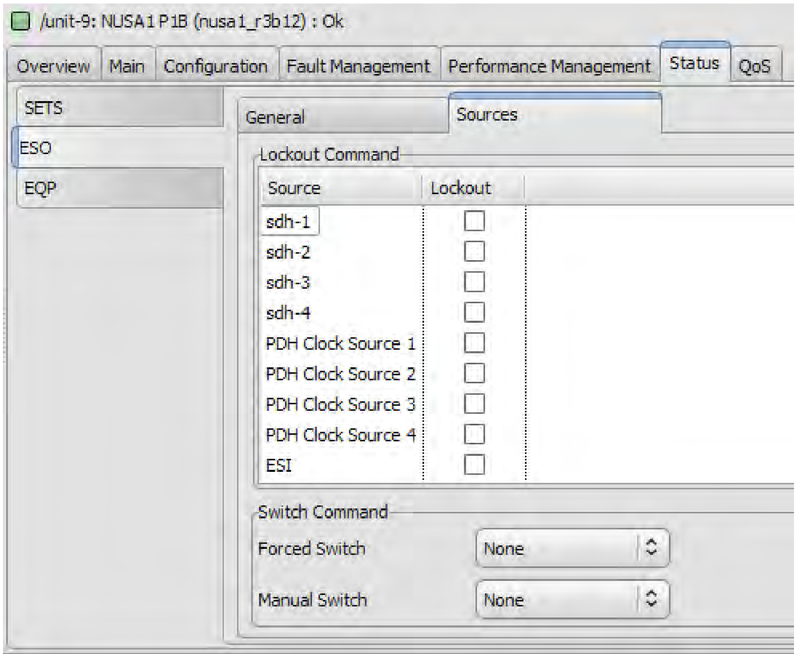


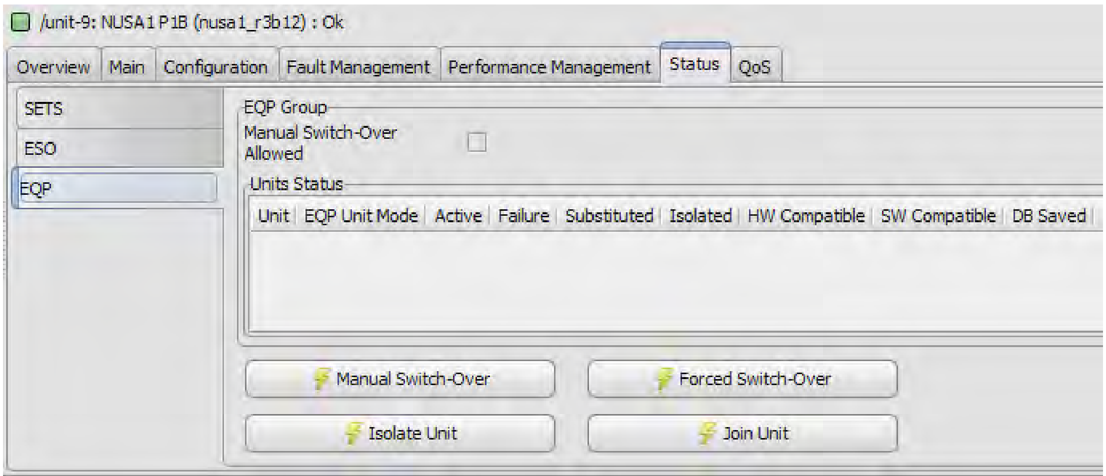
Table 64: AP: / unit-x, Status - ESO - Sources

Operation Name	Parameter Name	Range	Description / Details
Lockout Command	Source	sdh-1	The lockout of a port prevents the selection as an ESO timing source. It is not possible to override the lockout of a source with a forced or manual switch command.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	
	Lockout	☑	locked out
		☐	not locked out
Switch Command	Forced Switch	None	Perform a forced switch to a specific timing source for the ESO clock output. The switch command is only accepted if the source is enabled, i.e. has a priority configured. If the source is not available, i.e. failed or in WTR state, “Internal” is selected.
		sdh-1	
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	

Table 64: AP: / unit-x, Status - ESO - Sources (continued)

Operation Name	Parameter Name	Range	Description / Details
	Manual Switch	None	Perform a manual switch to a specific timing source for the ESO clock output. The switch command is only accepted if no forced switch is active and the source is available. The source is not available if - disabled, or - failed, or - in WTR state.
		sdh-1	
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	

8.2.6.5 AP: / unit-x, Status - EQP



Please note:

The roles of working and protecting unit is fixed within a slot pair.

→ Please refer to Table 28: "XMC20 slot pairs for NUSA1 EQP" (on page 101).

Table 65: AP: / unit-x, Status - EQP

Operation Name	Parameter Name	Range	Description / Details
EQP Group	Manual Switch-Over Allowed	☑	Indication that the standby unit, i.e. the working or the protecting unit is operational and can take over the service.
		☐	Indication that the standby unit, i.e. the working or the protecting unit is not operational due to a failure or to isolation. A manual protection switching is not possible.

Table 65: AP: / unit-x, Status - EQP (continued)

Operation Name	Parameter Name	Range	Description / Details
EQP Group - Units Status	Unit	<MO address>	MO address of the unit belonging to the EQP group.
	EQP Unit Mode	Undefined Mode	Mode of a unit in the EQP group.
		Working Unit	
		Protecting Unit	
	Active	☑	The unit is active (operational).
		☐	The unit is standby (not operational).
	Failure	☑	The unit has detected failure(s).
		☐	
	Substituted	☑	The working unit has been taken over by the protecting unit.
		☐	
	Isolated	☑	The working unit has been isolated with the “Isolate Unit” command.
		☐	
	HW Compatible	☑	The working unit is hardware compatible with the protecting unit in the EQP group. Please refer to section 5.9.4 EQP Prerequisites (on page 107).
		☐	
	SW Compatible	☑	The working unit is embedded software compatible with the protecting unit in the EQP group. Please refer to section 5.9.4 EQP Prerequisites (on page 107).
		☐	
	DB Saved	☑	The configuration of the unit has been saved.
		☐	
Manual Switch-Over			Manual switch (active to standby) of the unit in the EQP group. A switch-over is performed only when the other unit is error free and is not isolated. Refer to the “Manual Switch-Over Allowed” property above. Note: The traffic will be interrupted for up to 8 s.
Forced Switch-Over			Forced switch (active to standby) of the unit in the EQP group. A switch-over is performed independent of the error state of the other unit. Note: Traffic will be interrupted for up to 8 s. Note: Traffic will remain interrupted if the active unit is not operational.
Isolate Unit			Isolate the working unit from the EQP group. An isolated working unit will not perform any protection switch action. The protection switching state of the unit is frozen.
Join Unit			Join the isolated working unit to the EQP group, i.e. remove the isolation.

8.2.7 AP: / unit-x, QoS

8.2.7.1 AP: / unit-x, QoS – Rate Limiting

For a description of the
- "QoS - Rate Limiting"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.3 AP: / unit-x / port-y, y = 1 … 4 (SDH)

8.3.1 AP: / unit-x / port-y, Overview

For a description of the
- “Overview - Alarms”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.3.2 AP: / unit-x / port-y, Main

8.3.2.1 AP: / unit-x / port-y, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.3.2.2 AP: / unit-x / port-y, Main - SFP

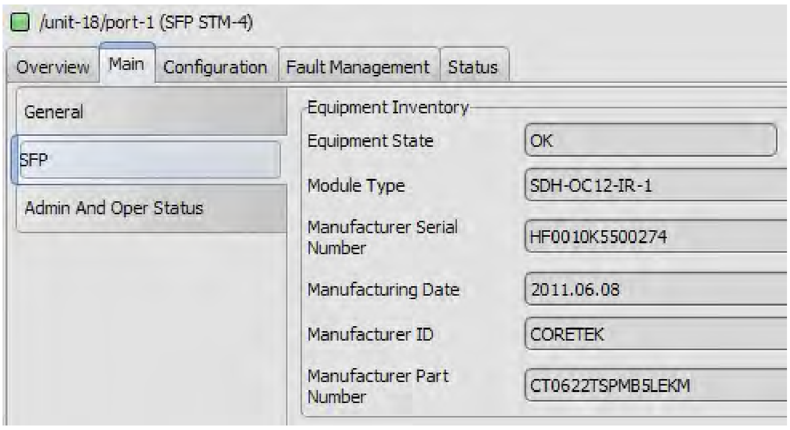


Table 66: AP: / unit-x / port-y, Main - SFP

Operation Name	Parameter Name	Range	Description / Details
Equipment Inventory	Equipment State	OK	Equipment state of the plugged SFP module.
		Unknown	
		Empty	
		Plugged	
		Mismatch	
		Failed	

Table 66: AP: / unit-x / port-y, Main - SFP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Module Type	0 … 16 characters	In the SFP module type the following abbreviations are used: - SDH: SDH module - OC3: STM-1 module - OC12: STM-4 module - OC48: STM-16 module - SM: Single mode fibre - SR: Short reach - IR: Intermediate reach - LR: Long reach - XR: Enhanced long reach Note that with electrical modules this field is normally not specified (SFP module “unrecognized”). However, some manufacturers may show proprietary information such as “OC3-MMODE SR, OC-3 Multi-Mode Short Reach” which is not directly applicable to electrical interfaces.
	Manufacturer Serial Number	0 … 16 characters	These description fields provide information about the vendor, part number, revision and production date.
	Manufacturing Date	0 … 10 characters	
	Manufacturer ID	0 … 16 characters	
	Manufacturer Part Number	0 … 16 characters	

8.3.2.3 AP: / unit-x / port-y, Main - Admin And Oper Status

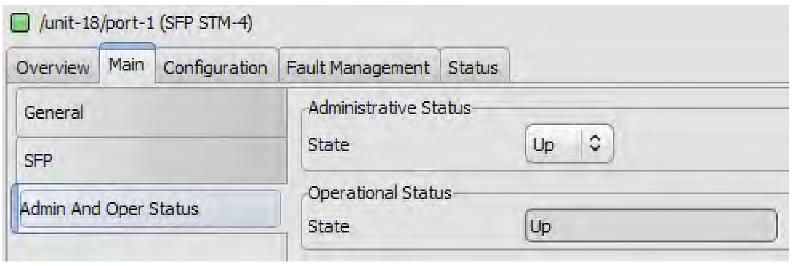


Table 67: AP: / unit-x / port-y, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Administrative Status	State	Up <u>Down</u>	Set the IETF administrative status of the physical SDH port. Unused ports (without fibres or electrical cables connected to them) should be set to the down state, so that they do not generate alarms (i.e. loss of signal).

Table 67: AP: / unit-x / port-y, Main - Admin And Oper Status (continued)

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the physical SDH port.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.3.3 AP: / unit-x / port-y, Configuration

8.3.3.1 AP: / unit-x / port-y, Configuration - PS

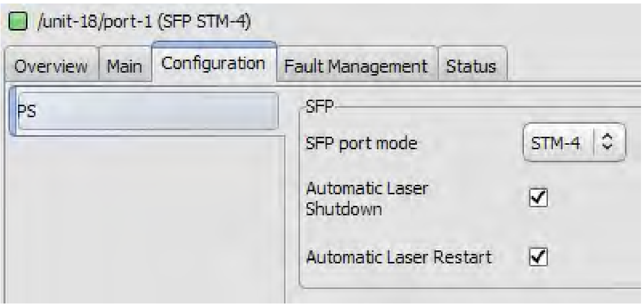


Table 68: AP: / unit-x / port-y, Configuration - PS

Operation Name	Parameter Name	Range	Description / Details
SFP	SFP Port Mode	STM-1	The port-1 and port-2 support STM-16 and STM-4. Default is STM-4 The port-3 and port-4 support STM-4 and STM-1. Default is STM-1
		STM-4	
		STM16	
	Automatic Laser Shutdown	☑	With automatic laser shutdown (ALS) enabled, the laser transmitter automatically shuts down when the received optical signal is lost. For further information please refer to section 6.3 Automatic Laser Shutdown and Restart (on page 132)
		☐	
	Automatic Laser Restart	☑	After an automatic laser shutdown, the laser can be restarted automatically. For further information please refer to section 6.3 Automatic Laser Shutdown and Restart (on page 132)
		☐	

8.3.4 AP: / unit-x / port-y, Fault Management

For the a description of the general aspects of the
- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, refer to [302] User Guide “XMC25/XMC23/XMC22”.

The following table lists the fault causes of the current AP.

Table 69: AP: / unit-x / port-y, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
LOS	Loss Of Signal	Communication Alarm	☑	Major	Loss of the optical or electrical input signal (STM-LOS).
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done.
TRF [a]	Transmitter Failure	Equipment Alarm	☑	Major	No optical output power.
TRDEG [a]	Transmitter Degraded	Communication Alarm	☐	Minor	The SFP module reports that the optical output power has fallen below the lower power threshold (SFP specific, typically 2 dB below the normal module operating range).
TRPE [a]	Transmitter Power Exceeded	Communication Alarm	☐	Minor	The SFP module reports that the optical output power has exceeded the upper power threshold (SFP specific, typically 2 dB above the normal module operating range).
ALS	Automatic Laser Shutdown	Communication Alarm	☑	Major	The laser is inactive for safety reasons.
ENA	Equipment Not Available	Equipment Alarm	☑	Major	No SFP module is present.
HWIC	Hardware Incompatible With Configuration	Equipment Alarm	☑	Major	The plugged SFP module is not compatible with the application.

a. The support of this alarm is only possible for SFP modules with diagnostics function. SFP modules with electrical interfaces do not support this alarm (no diagnostics function available).

8.3.5 AP: / unit-x / port-y, Status

8.3.5.1 AP: / unit-x / port-y, Status - DDM

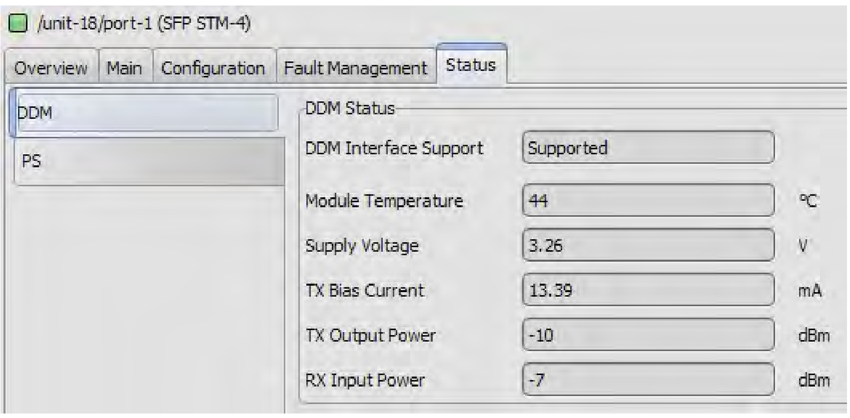


Table 70: AP: / unit-x / port-y, Status - DDM

Operation Name	Parameter Name	Range	Description / Details
DDM Status	DDM Interface Support	Supported Not Supported Unknown	If diagnostic is supported, some physical parameters are displayed. Note that all KEYMILE recommended SFP modules with optical interfaces support SFP diagnostic.
	Module Temperature	°C	SFP module temperature, displayed in °C.
	Supply Voltage	V	SFP supply voltage, displayed in V.
	TX Bias Current	mA	SFP bias current, displayed in mA.
	TX Output Power	dBm	Optical power at the transmit interface, displayed in dBm.
	RX Input Power	dBm	Optical power at the receive interface, displayed in dBm.

Please note:

NUSA1 supports diagnostics for SFP modules. Support of diagnostics is not mandatory for SFP modules with optical interfaces. However KEYMILE recommends only optical SFP modules that support diagnostics.
SFP modules with the electrical STM-1 interface do not support diagnostics.

8.3.5.2 AP: / unit-x / port-y, Status - PS - ALS

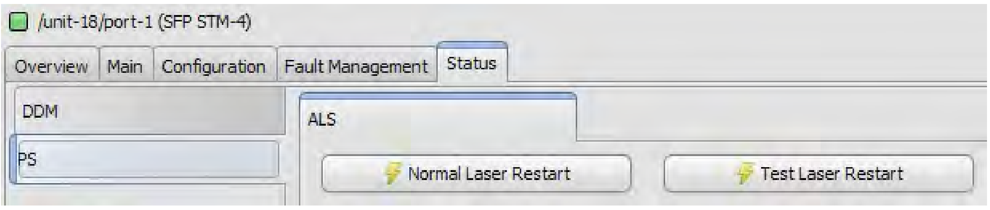


Table 71: AP: / unit-x / port-y, Status - PS - ALS

Operation Name	Parameter Name	Range	Description / Details
Normal Laser Restart			The laser restart can be delayed up to 110 s. The “normal laser restart” option can force the start up procedure. Normal restart will activate the laser transmitter for t = 2 ± 0.25 s.
Test Laser Restart			Test laser restart will activate the laser transmitter for t = 90 ± 10 s. For further information please refer to section 6.3 Automatic Laser Shutdown and Restart (on page 132)

Please note:

NUSA1 supports laser restart for SFP modules with optical and electrical interfaces.

→ The laser restart function is also applied to the electrical interface.

8.4 AP: / unit-x / port-y, y = 5 … 8 (Ethernet)

8.4.1 AP: / unit-x / port-y, Overview

For a description of the
- "Overview - Alarms",
- "Overview - Mirroring", and
- "Overview - Port Type"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.4.2 AP: / unit-x / port-y, Main

8.4.2.1 AP: / unit-x / port-y, Main – General

For a description of the "Labels" and "Alarm Status" parameters in the
- "Main - General"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

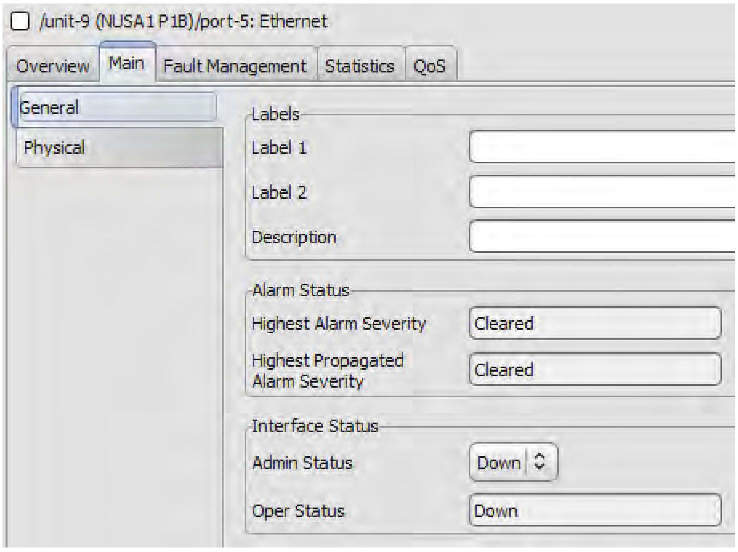


Table 72: AP: / unit-x / port-y, Main – General

Operation Name	Parameter Name	Range	Descriptions / Details
Interface Status	Admin Status	Up	Select "Up" to bring the port into service
		<u>Down</u>	Select "Down" to take the port out of service.
	Oper Status	Up	Shows the operational state is up. The state can only be up if the administrative state is up and there are currently no failures.
		Down	Shows the operational state is down.
		Testing	Shows the port is in a testing state.

8.4.2.2 AP: / unit-x / port-y, Main – Physical

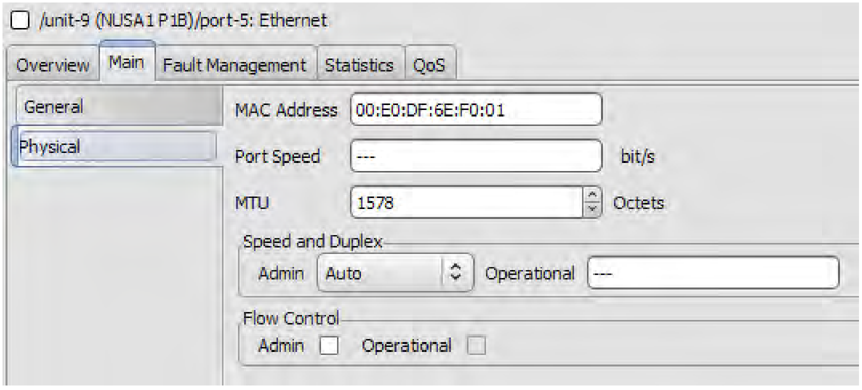


Table 73: AP: / unit-x / port-y, Main – Physical

Operation Name	Parameter Name	Range	Descriptions / Details
	MAC Address	00:00:00:00:00:00 … ff:ff:ff:ff:ff:ff	Shows the physical (MAC) address of this port. This parameter is read-only.
	Port Speed	10 Mbit/s	Shows the port speed. This parameter is read-only.
		100 Mbit/s	
		1000 Mbit/s	
	MTU	42 … 1'578 … 9'194 Octets, step 2 Octets	Maximum Transmission Unit, i.e. maximum IP packet size. The MTU size is calculated including the IP headers.
Speed And Duplex	Admin	Auto	Autonegotiation
		10BaseT HD	10 Mbit/s, half duplex
		10BaseT FD	10 Mbit/s, full duplex
		100BaseTX HD	100 Mbit/s, half duplex
		100BaseTX FD	100 Mbit/s, full duplex
		1000BaseT FD	1'000 Mbit/s, full duplex
	Operational	10BaseT HD	10 Mbit/s, half duplex
		10BaseT FD	10 Mbit/s, full duplex
		100BaseTX HD	100 Mbit/s, half duplex
		100BaseTX FD	100 Mbit/s, full duplex
		1000BaseT FD	1'000 Mbit/s, full duplex
Flow Control	Admin	☑	Port Ethernet flow control according to IEEE 802.3x. Flow control is a mechanism which allows the receiving party of a connection to control the rate of the sending party.
		☐	
	Operational	☑	
		☐	

Please note:

For an overview on the specific characteristics of XMC20 Switch ports, please refer to [201] System Description "XMC20 R6B".

Risk of operating trouble!

Be aware when connecting Ethernet ports configured in manual mode on NUSA1 (no autonegotiation) to Ethernet ports in autonegotiation mode, the following situation may occur:
The link will be up but the duplex settings may be inconsistent and this can result in poor throughput performance on the link.

8.4.3 AP: / unit-x / port-y, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 74: AP: / unit-x / port-y, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
LOS	Loss Of Signal	Communication Alarm	☑	Major	Ethernet link not established.

8.4.4 AP: / unit-x / port-y, Statistics

8.4.4.1 AP: / unit-x / port-y, Statistics – General

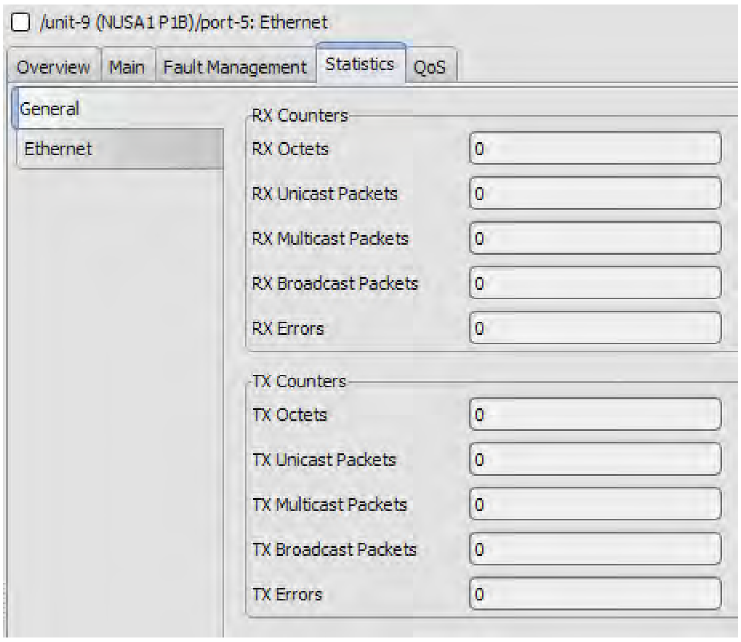


Table 75: AP: / unit-x / port-y, Statistics – General

Operation Name	Parameter Name	Range	Descriptions / Details
RX Counters	RX Octets	0 … 2^{64} -1	Number of ingress octets
	RX Unicast Packets	0 … 2^{64} -1	Number of ingress unicast packets
	RX Multicast Packets	0 … 2^{64} -1	Number of ingress multicast packets
	RX Broadcast Packets	0 … 2^{64} -1	Number of ingress broadcast packets
	RX Errors	0 … 2^{32} -1	Number of ingress errored packets
TX Counters	TX Octets	0 … 2^{64} -1	Number of egress octets
	TX Unicast Packets	0 … 2^{64} -1	Number of egress unicast packets
	TX Multicast Packets	0 … 2^{64} -1	Number of egress multicast packets
	TX Broadcast Packets	0 … 2^{64} -1	Number of egress broadcast packets
	TX Errors	0 … 2^{32} -1	Number of egress errored packets

Please note:
The statistics counters restart with 0 when they reach their upper range limit.

8.4.4.2 AP: / unit-x / port-y, Statistics – Ethernet

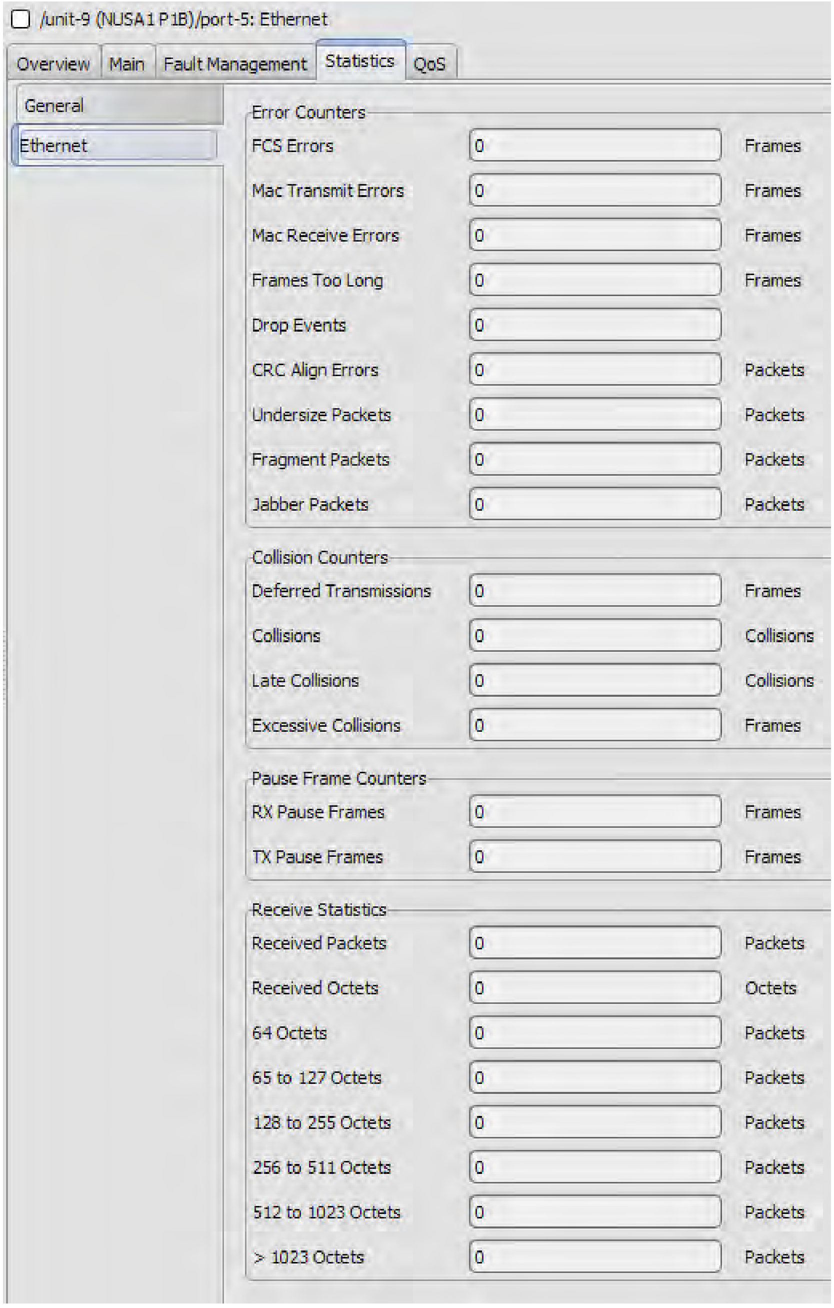


Table 76: AP: / unit-x / port-y, Statistics – Ethernet

Operation Name	Parameter Name	Range	Descriptions / Details
Error Counters	FCS Errors	0 … 2^{64} -1	Number of ingress frames with FCS errors
	Mac Transmit Errors	0 … 2^{64} -1	Number of egress frames with a MAC sublayer transmit error
	Mac Receive Errors	0 … 2^{64} -1	Number of ingress frames with a MAC sublayer receive error
	Frames Too Long	0 … 2^{64} -1	Number of ingress frames that exceed the maximum permitted frame size.
	Drop Events	0 … 2^{32} -1	Number of ingress drop events
	CRC Align Errors	0 … 2^{32} -1	Number of ingress packets with CRC alignment errors
	Undersize Packets	0 … 2^{32} -1	Number of ingress undersized packets (< 64 bytes)
	Fragment Packets	0 … 2^{32} -1	Number of ingress fragment packets
	Jabber Packets	0 … 2^{32} -1	Number of ingress jabber packets
Collision Counters	Deferred Transmissions	0 … 2^{32} -1	Number of egress frames for which the first transmission attempt is delayed because the medium is busy
	Collisions	0 … 2^{32} -1	Number of estimated collisions
	Late Collisions	0 … 2^{32} -1	Number of times that a collision is detected later than one slot time into the transmission of a packet.
	Excessive Collisions	0 … 2^{32} -1	Number of frames for which transmission fails due to excessive collisions
Pause Frame Counters	RX Pause Frames	0 … 2^{64} -1	Number of ingress pause MAC control frames
	TX Pause Frames	0 … 2^{64} -1	Number of egress pause MAC control frames
Receive Statistics	Received Packets	0 … 2^{64} -1	Number of ingress packets
	Received Octets	0 … 2^{64} -1	Number of ingress octets
	64 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 64 octets
	65 to 127 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 65 to 127 octets
	128 to 255 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 128 to 255 octets
	256 to 511 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 256 to 511 octets
	512 to 1023 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 512 to 1023 octets
	> 1023 Octets	0 … 2^{64} -1	Number of ingress packets with a size of more than 1023 octets

Please note:

The statistics counters restart with 0 when they reach their upper range limit.

8.4.5 AP: / unit-x / port-y, QoS

8.4.5.1 AP: / unit-x / port-y, QoS – QoS Scheduling

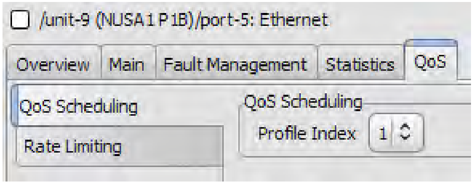


Table 77: AP: / unit-x / port-y, Main – Physical

Operation Name	Parameter Name	Range	Descriptions / Details
QoS Scheduling	Profile	1 … 5	Select the QoS scheduling profile number. QoS scheduling profiles are configured with ECST in the “Switching” view at Switching/ Bridges, bridge-1/QoS, Scheduling Profiles.

8.4.5.2 AP: / unit-x / port-a, QoS – Rate Limiting

Please note:

The Rate Limiting tab is only available if the port type of the Ethernet port is configured to PWAC or to CVP.

→ First configure the port type to PWAC or to CVP.

For a description of the

- “QoS - Rate Limiting”

management function, please refer to [302] User Guide “XMC25/XMC23/ XMC22”.

8.5 AP: / unit-x / port-y / mau, y = 5 … 8

8.5.1 AP: / unit-x / port-y / mau, Overview

For a description of the
- “Overview - Alarms”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.5.2 AP: / unit-x / port-y / mau, Main

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.6 AP: / unit-x / eos

8.6.1 AP: / unit-x / eos, Overview

For a description of the
- "Overview - Alarms",
- "Overview - Cross Connections",
- "Overview - Mirroring",
- "Overview - Port Type", and
- "Overview - Statistics",

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.6.2 AP: / unit-x / eos, Main

For a description of the
- "Main - General"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.6.3 AP: / unit-x / eos, QoS

For a description of the
- "QoS - Rate Limiting"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.7 AP: / unit-x / eos / eos-y

8.7.1 AP: / unit-x / eos / eos-y, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”,
- “Overview - Mirroring”, and
- “Overview - Port Type”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.7.2 AP: / unit-x / eos / eos-y, Main

8.7.2.1 AP: / unit-x / eos / eos-y, Main - General

For a description of the “Labels” and “Alarm Status” parameters in the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

The “Interface Status” parameters in the
- “Main - General”

management function are only available for the EoS ports eos-1 to eos-12.

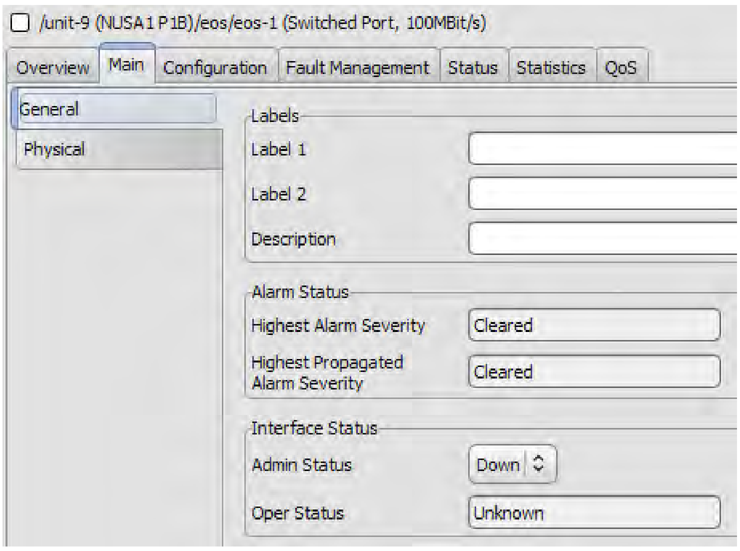


Table 78: AP: / unit-x / eos / eos-y, Main - General

Operation Name	Parameter Name	Range	Descriptions / Details
Interface Status	Admin Status	Up	Select “Up” to bring the port into service
		Down	Select “Down” to take the port out of service.
	Oper Status	Up	Shows the operational state is up. The state can only be up if the administrative state is up and there are currently no failures.
		Down	Shows the operational state is down.
		Testing	Shows the port is in a testing state.

8.7.2.2 AP: / unit-x / eos / eos-y, Main - Physical

The “Main - Physical” management function is only available for the EoS ports eos-1 to eos-12.

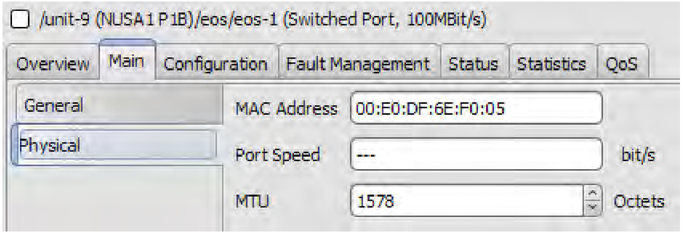


Table 79: AP: / unit-x / eos / eos-y, Main - Physical

Operation Name	Parameter Name	Range	Description / Details
	MAC Address	00:00:00:00:00:00 … ff:ff:ff:ff:ff:ff	Shows the physical (MAC) address of this port. This parameter is read-only.
	Port Speed	100 Mbit/s	Shows the port speed. This parameter is read-only.
		1000 Mbit/s	
	MTU	42 … 1’578 … 9’194 Octets, step 2 Octets	Maximum Transmission Unit, i.e. maximum IP packet size. The MTU size is calculated including the IP headers.

8.7.2.3 AP: / unit-x / eos / eos-y, Main - Admin And Oper Status

The “Main - Admin And Oper Status” management function is only available for the EoS ports eos-13 to eos-32.

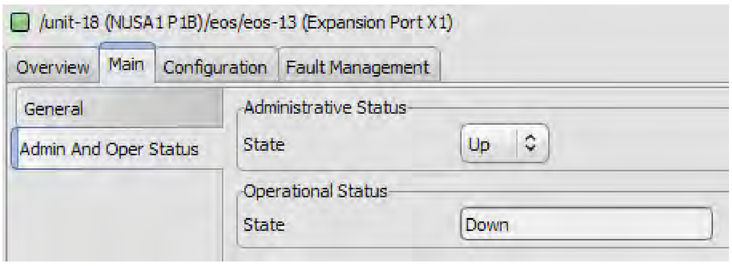


Table 80: AP: / unit-x / eos / eos-y, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Administrative Status	State	Up	Set the IETF administrative status of the EoS port.
		Down	
Operational Status	State	Up	Display of the IETF operational status of the EoS port.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

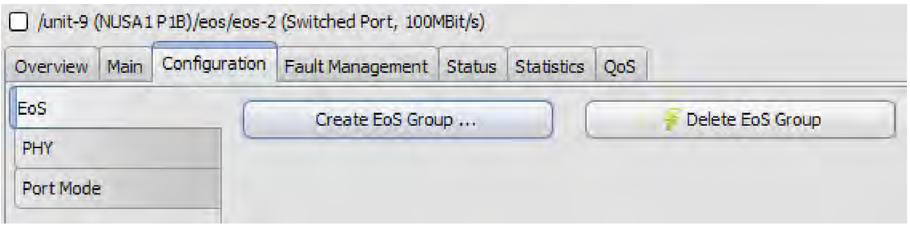
8.7.3 AP: / unit-x / eos / eos-y, Configuration

8.7.3.1 AP: / unit-x / eos / eos-y, Configuration - EoS

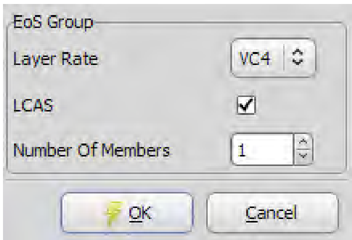
Please note:

An EoS port can be operated in switched, unswitched or expansion mode.

→ Please refer to section 5.5.3 Ethernet Switch (on page 71) for further information.



“Create EoS Group …” dialogue:



“Delete EoS Group” dialogue:

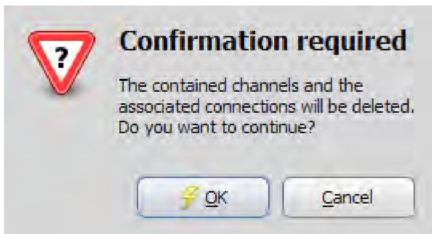


Table 81: AP: / unit-x / eos / eos-y, Configuration - EoS

Operation Name	Parameter Name	Range	Description / Details
Create EoS Group …			Open the ECST dialogue to create an EoS group. Only one EoS group can be created per EoS port.
Delete EoS Group			Delete the EoS group of this EoS port. The confirmation is only required if a cross connection has been created for a member of this EoS group.

Table 81: AP: / unit-x / eos / eos-y, Configuration - EoS (continued)

Operation Name	Parameter Name	Range	Description / Details
EoS Group	Layer Rate	VC4 VC3 VC12	VC type carrying the Ethernet payload. Note that all members of a EoS group are of the same VC type.
	LCAS	☑ ☐	Enable or disable LCAS for the EoS group. For further information refer to section 5.5.4.3 Link capacity adjustment scheme (LCAS) (on page 81). When LCAS is not enabled it is not assured that member 1 connects to member 1 on the other side, member 2 to member 2, etc.
	Number Of Members	0 … 1 … n	Number of VCs constituting the virtual concatenation group (VCG). The total available tributary VC capacity per NUSA1 unit for VC-4 and VC-3 group members only is 14 VC-4 equivalents. The total available tributary VC capacity per NUSA1 unit for VC-4, VC-3 and VC-12 group members is 12 VC-4 equivalents: - Up to 8 VC-4 equivalents for VC-4 and VC-3 members, - Up to 4 VC-4 equivalents for VC-12 members. The maximum number n of VC-4 is 14 per VCG and 14 per unit. The maximum number n of VC-3 is 24 per VCG and 24 per unit. The maximum number n of VC-12 is 63 per VCG and 252 per unit. Please refer to section 5.5.4 Ethernet over SDH (EoS) (on page 77) for further information.

8.7.3.2 AP: / unit-x / eos / eos-y, Configuration - PHY

The “Configuration - PHY” management function is only available for the EoS ports eos-1 to eos-12.

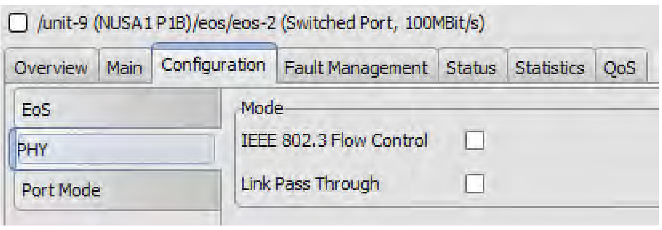


Table 82: AP: / unit-x / eos / eos-y, Configuration - PHY

Operation Name	Parameter Name	Range	Description / Details
Mode	IEEE 802.3 Flow Control	☑ ☐	Enable or disable flow control. For further information please refer to section 5.5.1.2 IEEE 802.3 flow control (on page 69).

Table 82: AP: / unit-x / eos / eos-y, Configuration - PHY (continued)

Operation Name	Parameter Name	Range	Description / Details
	Link Pass Through	☑ ☐	The link pass through feature can bring the local link state (up or down) to the remote Ethernet interface. With this feature the Ethernet transport is transparent also for link states. For further information please refer to section 5.5.1.3 Link pass through (on page 70).

Please note:

The link pass through feature must be enabled on the Ethernet interfaces at both sides of the SDH path to become operational.

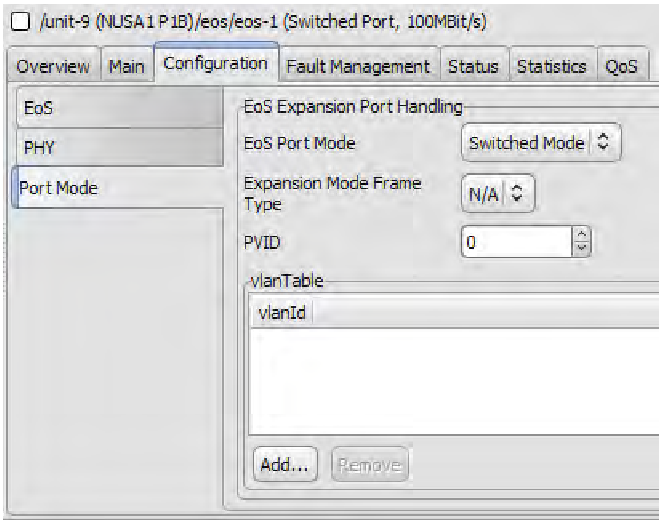
Please note:

The link pass through feature is only available for the EoS ports in the EPL (unswitched) mode.

Please note:

The flow control feature is only available for the EoS ports in the EPL (unswitched) mode.

8.7.3.3 AP: / unit-x / eos / eos-y, Configuration - Port Mode



Add a VLAN to the VLAN table:

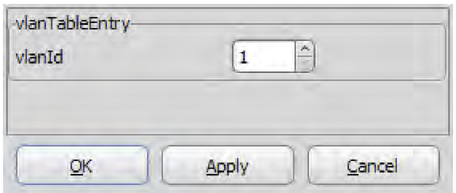


Table 83: AP: / unit-x / eos / eos-y, Configuration - Port Mode

Operation Name	Parameter Name	Range	Description / Details
EoS Expansion Port Handling	EoS Port Mode	EPL Mode	An EoS port in the EPL Mode accesses an Ethernet front port of the NUSA1 unit, bypassing the VLAN bridge. Please refer to section 5.5.3 Ethernet Switch (on page 71). This mode is displayed and cannot be modified if an EoS port has been configured to the EPL mode in the AP: /unit-x, Configuration - EPL management function of the NUSA1 unit. Applicable for the EoS ports eos-1 to eos-4, eos-9 and eos-10.
		Switched Mode	An EoS port in the Switched Mode accesses the VLAN bridge. Please refer to section 5.5.3 Ethernet Switch (on page 71). This mode is displayed if an EoS port has **not** been configured to the EPL mode in the AP: / unit-x, Configuration - EPL management function of the NUSA1 unit. Applicable for the EoS ports eos-1 to eos-12.
		Expansion Mode	An EoS port in the Expansion Mode accesses the VLAN bridge. Please refer to section 5.5.3 Ethernet Switch (on page 71). This mode is configurable on the EoS ports eos-9 to eos-12. This mode cannot be modified on the EoS ports eos-13 to eos-32. Applicable for the EoS ports eos-9 to eos-32.
	Expansion Mode Frame Type	<u>Tagged</u>	The ingress frames must be tagged. Egress frames are sent out tagged. This parameter is only applicable for the expansion port mode.
		Untagged	The ingress frames must be untagged and are tagged with the Port VLAN ID inside the VLAN bridge Egress frames are sent out untagged, or with the outer VLAN tag removed. This parameter is only applicable for the expansion port mode.
	PVID	<u>1</u> … 4094	Port VLAN ID for untagged frames. This parameter is only applicable for the expansion port mode using the untagged frame type.
	vlanTable, vlanId	1 … 4094	List of all VLAN IDs that are transported over the EoS port. If the EoS port uses the untagged frame type also the Port VLAN ID must be configured in the VLAN table. This list is only applicable for the expansion port mode.
	vlanTable, Add…		Open the ECST dialogue to add a new VLAN ID to the VLAN table.
	vlanTableEntry, vlanId	<u>1</u> … 4094	Enter the VLAN ID
	vlanTable, Remove		Remove the selected VLAN ID from the VLAN table.

Risk of operating trouble!

The VLAN table of an expansion port can contain multiple VLAN IDs, but a VLAN ID cannot be member of more than one EoS port of the same expansion group.

Risk of operating trouble!

Expansion ports of the same expansion group have all the same QoS parameters, as they are configured for the master expansion port.

8.7.4 AP: / unit-x / eos / eos-y, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 84: AP: / unit-x / eos / eos-y, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
OPSDWN	Operational State Down	Communication Alarm	☑	Major	The EoS group is not operational. This can be due to a loss of the total capacity of the virtual concatenation group.

8.7.5 AP: / unit-x / eos / eos-y, Status

8.7.5.1 AP: / unit-x / eos / eos-y, Status - PHY

The “Status - PHY” management function is only available for the EoS ports eos-1 to eos-12.

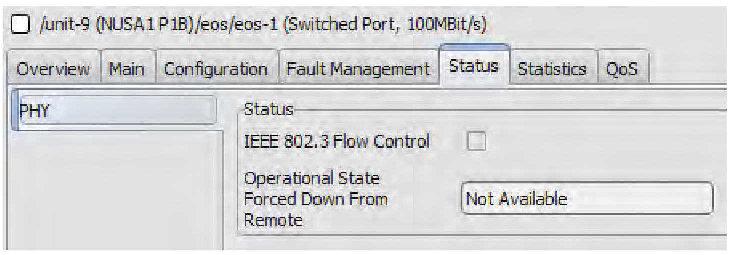


Table 85: AP: / unit-x / eos / eos-y, Status - PHY

Operation Name	Parameter Name	Range	Description / Details
Status	IEEE 802.3 Flow Control	☑	Flow control is enabled on this port.
		☐	Flow control is disabled on this port.

Table 85: AP: / unit-x / eos / eos-y, Status - PHY (continued)

Operation Name	Parameter Name	Range	Description / Details
	Operational State Forced Down From Remote	Not Available	The link pass through feature is disabled on this port.
		True	The link pass through feature is enabled and the Ethernet port is disabled due to a link down state of the Ethernet port at the remote end of the SDH path.
		False	The link pass through feature is enabled and the Ethernet port is enabled.

8.7.6 AP: / unit-x / eos / eos-y, Statistics

8.7.6.1 AP: / unit-x / eos / eos-y, Statistics – General

The “Statistics - General” management function is only available for the EoS ports eos-1 to eos-12.

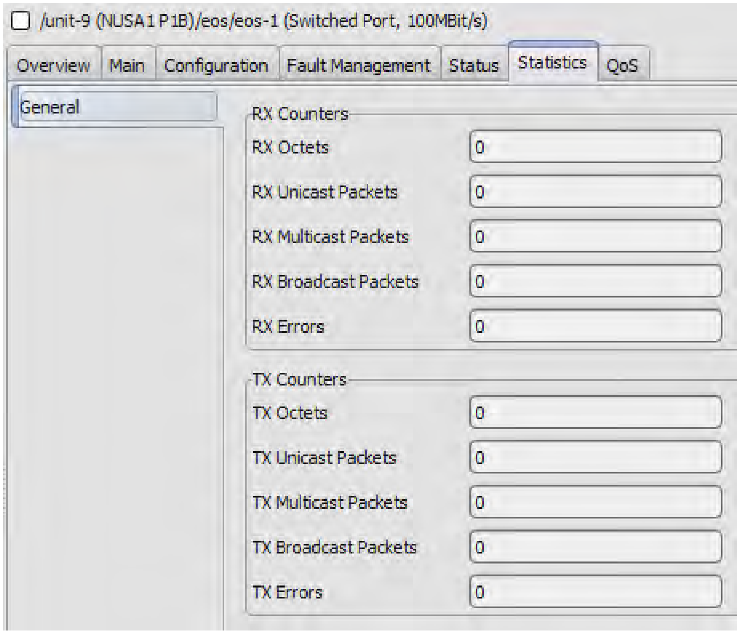


Table 86: AP: / unit-x / eos / eos-y, Statistics – General

Operation Name	Parameter Name	Range	Descriptions / Details
RX Counters	RX Octets	0 … 2^{64} -1	Number of ingress octets
	RX Unicast Packets	0 … 2^{64} -1	Number of ingress unicast packets
	RX Multicast Packets	0 … 2^{64} -1	Number of ingress multicast packets
	RX Broadcast Packets	0 … 2^{64} -1	Number of ingress broadcast packets
	RX Errors	0 … 2^{32} -1	Number of ingress errored packets
TX Counters	TX Octets	0 … 2^{64} -1	Number of egress octets
	TX Unicast Packets	0 … 2^{64} -1	Number of egress unicast packets
	TX Multicast Packets	0 … 2^{64} -1	Number of egress multicast packets
	TX Broadcast Packets	0 … 2^{64} -1	Number of egress broadcast packets
	TX Errors	0 … 2^{32} -1	Number of egress errored packets

Please note:
The statistics counters restart with 0 when they reach their upper range limit.

8.7.7 AP: / unit-x / eos / eos-y, QoS

8.7.7.1 AP: / unit-x / eos / eos-y, QoS – QoS Scheduling

The “QoS - QoS Scheduling” management function is only available for the EoS ports eos-1 to eos-12.

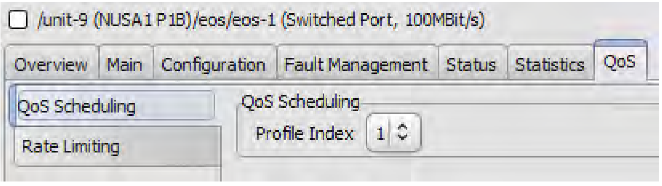


Table 87: AP: / unit-x / eos / eos-y, Main – Physical

Operation Name	Parameter Name	Range	Descriptions / Details
QoS Scheduling	Profile	1 … 5	Select the QoS scheduling profile number. QoS scheduling profiles are configured with ECST in the “Switching” view at Switching/ Bridges, bridge-1/QoS, Scheduling Profiles.

8.7.7.2 AP: / unit-x / eos / eos-y, QoS – Rate Limiting

The “QoS - Rate Limiting” management function is only available for the EoS ports eos-1 to eos-12.

For a description of the

- “QoS - Rate Limiting”

management function, please refer to [302] User Guide “XMC25/XMC23/ XMC22”.

8.8 AP: / unit-x / eos / eos-y / eos

8.8.1 AP: / unit-x / eos / eos-y / eos, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - EoS Group Overview”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.8.2 AP: / unit-x / eos / eos-y / eos, Main

8.8.2.1 AP: / unit-x / eos / eos-y / eos, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.8.2.2 AP: / unit-x / eos / eos-y / eos, Main - Admin And Oper Status

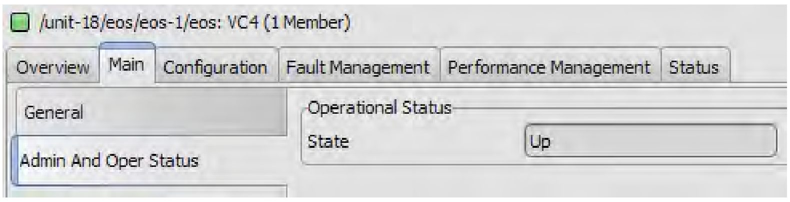
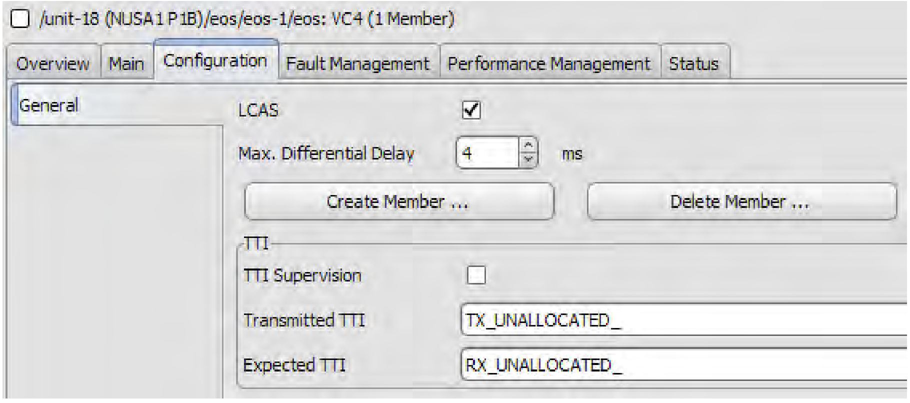


Table 88: AP: / unit-x / eos / eos-y / eos, Main - Admin And Oper Status

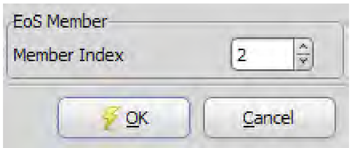
Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the eos group. The operational state is up when the port administrative state is up and no GFPLOF or VCGLOTC defect is active.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.8.3 AP: / unit-x / eos / eos-y / eos, Configuration

8.8.3.1 AP: / unit-x / eos / eos-y / eos, Configuration - General



“Create Member” dialogue:



“Delete Member” dialogue:

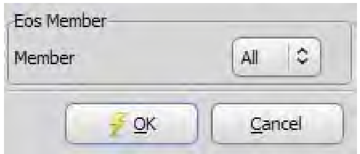


Table 89: AP: / unit-x / eos / eos-y / eos, Configuration - General

Operation Name	Parameter Name	Range	Description / Details
LCAS	LCAS	☑ ☐	Enable or disable LCAS for the EoS group. For further information refer to section 5.5.4.3 Link capacity adjustment scheme (LCAS) (on page 81). When LCAS is not enabled it is not assured that member 1 connects to member 1 on the other side, member 2 to member 2, etc.
Max. Differential Delay		1 … 4 … 64 ms	Set the expected maximum differential delay for the EoS group members. The measured differential delay is available in the EoS group status. See section 8.8.6.1 AP: / unit-x / eos / eos-y / eos, Status - General (on page 219). Note that the differential delay causes also a traffic delay of the same amount.
Create Member …			Open the ECST dialogue to create an additional member to an existing EoS group.
EoS Member	Member Index	0 … 63	Enter the index number of the new member to be created. 0 is a reserved value used for the auto-assignment of a EoS member index: The auto-assigned index is the highest existing index number + 1. In the ECST the default value is the autoassigned index number.
Delete Member …			Open the ECST dialogue to delete a member from an existing EoS group.

Table 89: AP: / unit-x / eos / eos-y / eos, Configuration - General (continued)

Operation Name	Parameter Name	Range	Description / Details
EoS Member	Member	vc12-1 … vc12-63, vc3-1 … vc3-24, vc4-1 … vc4-14	Select the EoS group member name to be deleted.
		All	
TTI	TTI Supervision	☑	The trail trace identifier (TTI) supervision can be enabled or disabled. In the disabled mode no check is done on the received TTI of all EoS group members and no alarm is generated. For further information please refer to section 7.4 Trail Trace Identifier (TTI) (on page 154)
		☐	
	Transmitted TTI	15 characters	TTI transmitted in the VC path overhead (J1 byte for VC-4 and VC-3, J2 byte for VC-12). The default string is TX_UNALLOCATED_. In the disabled mode the transmit TTI string is TX_UNALLOCATED_ or any other configured TTI. Note that the same TTI is transmitted in every member of an EoS group. A TTI shorter than 15 characters is automatically completed with SPACE characters.
	Expected TTI	15 characters	TTI expected in the VC path overhead. The default string is RX_UNALLOCATED_. In the disabled mode the expected TTI string is RX_UNALLOCATED_ or any other configured TTI. Note that the same TTI is expected in every member of an EoS group. A TTI shorter than 15 characters is automatically completed with SPACE characters.

8.8.4 AP: / unit-x / eos / eos-y / eos, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 90: AP: / unit-x / eos / eos-y / eos, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
GFPLOF	GFP Loss Of Frame	Communication Alarm	☑	Major	Multiple bit errors detected on the GFP core header or GFP type header by the HEC (header error check).
VCGLOA	VCG Loss Of Alignment	Communication Alarm	☑	Major	The differential delay in the virtual concatenation group exceeds the size of the alignment buffer.

Table 90: AP: / unit-x / eos / eos-y / eos, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
VCGLOTC	VCG Loss Of Total Capacity	Communication Alarm	☑	Major	The virtual concatenation group is not available due to the fact that - in non LCAS mode at least one member of a group suffers from payload mismatch, loss of multiframe or a failure in the server layer, or - in LCAS mode all members of a group suffer from payload mismatch, loss of multiframe or a failure in the server layer
VCGLOPC	VCG Loss Of Partial Capacity	Communication Alarm	☑	Minor	One or more members of a group suffer from payload mismatch, loss of multiframe or a failure in the server layer, but the group is still available. LCAS mode only.
LOP	VC Loss Of Pointer	Communication Alarm	☑	Major	Eight consecutive invalid AU-4, TU-3 or TU-12 pointer values have been received in one or more of the VCG members. A persistent mismatch between provisioned and received AU or TU types will also result in a LOP failure.
AIS	VC AIS Received	Communication Alarm	☑	Minor	Failure in the received optical or electrical signal, in the RS or MS layer (AU-4-AIS), or in the EoS VC-4 layer (TU-3-AIS, TU-12-AIS) of one or more of the VCG members.
PLM	VC Payload Mismatch	Communication Alarm	☑	Major	The received and accepted trail signal label does not indicate the expected “GFP” in the VC-4, VC-3 or VC-12 (VC-n-PLM) in one or more of the VCG members.
UNEQ	VC Unequipped	Communication Alarm	☑	Major	The received and accepted trail signal label indicates “Unequipped” (VC-n-UNEQ) in one or more of the VCG members.
TIM	VC Trace Identifier Mismatch	Communication Alarm	☑	Major	The received and accepted TTI does not match the expected TTI (VC-n-TIM) in one or more of the VCG members.
RDI	VC Remote Defect Indication	Communication Alarm	☑	Minor	The far end equipment has one or more of the following defects in one or more of the VCG members: AU-4-LOP, AU-4-AIS, VC-4-UNEQ, VC-4-TIM, (VC-4), or VC-4-PLM, TU-3-LOP, TU-3-AIS, VC-3-UNEQ, VC-3-TIM (VC-3), or VC-4-LOM, VC-4-PLM, TU-12-LOP, TU-12-AIS, VC-12-UNEQ, VC-12-TIM (VC-12).
VCATSNM	VCAT Sequence Number Mismatch	Communication Alarm	☑	Major	The received VCAT sequence number does not match with the expected one.

Table 90: AP: / unit-x / eos / eos-y / eos, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
VCATLOMF	VCAT Loss Of Multi-frame	Communica-tion Alarm	☑	Major	Loss of the VCAT multiframe alignment in the H4 byte (VC-4, VC-3) or in the K4 bit 2.

8.8.5 AP: / unit-x / eos / eos-y / eos, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

The PM parameters are presented in different groups. The following counter group is available for the NUSA1 EoS groups:

- "EoS GFP Encapsulation" group, see section 8.8.5.1 AP: / unit-x / eos / eos-y / eos, Performance Management - EoS GFP Encapsulation (on page 218).

The following counter intervals are available:

Table 91: PM counter interval availability

Counter interval	EoS GFP Encapsulation
User Counter	yes
History 15min	yes
History 24h	yes
Alarm 15min	no
Alarm 24h	no

8.8.5.1 AP: / unit-x / eos / eos-y / eos, Performance Management - EoS GFP Encapsulation

Table 92: PM group: EoS GFP Encapsulation

PM parameter	Description
Transmitted GFP Frames	Number of egress GFP frames.
Received GFP Frames	Number of ingress GFP frames.
Discarded GFP Frames	Number of ingress discarded GFP frames.
Errored GFP Frames	Number of ingress errored GFP frames.

8.8.6 AP: / unit-x / eos / eos-y / eos, Status

8.8.6.1 AP: / unit-x / eos / eos-y / eos, Status - General

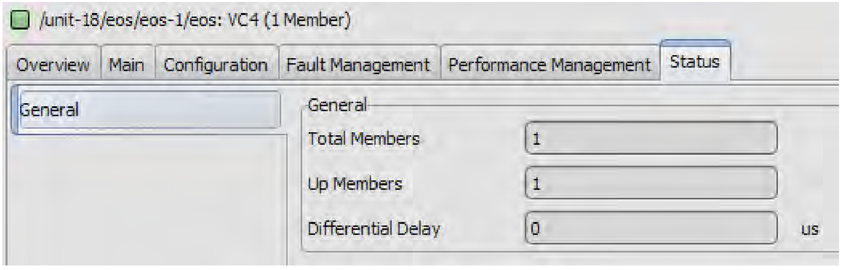


Table 93: AP: / unit-x / eos / eos-y / eos, Status - General

Operation Name	Parameter Name	Range	Description / Details
General	Total Members	0 … 63	Display of the total number of EoS group members.
	Up Members	0 … 63	Display of the number of operational EoS group members.
	Differential Delay	0 … 64’000 µs	Display of the maximum transfer time difference between all members of the EoS group (VCG) in microseconds. This value can be different from 0 when the transmission path is not the same for all members of a group.

8.9 AP: / unit-x / eos / eos-y / eos / vcz-a

z = 4 (vc4), 3 (vc3) or 12 (vc12).

8.9.1 AP: / unit-x / eos / eos-y / eos / vcz-a, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - CTP”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.9.2 AP: / unit-x / eos / eos-y / eos / vcz-a, Main

8.9.2.1 AP: / unit-x / eos / eos-y / eos / vcz-a, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.9.2.2 AP: / unit-x / eos / eos-y / eos / vcz-a, Main - Admin And Oper Status

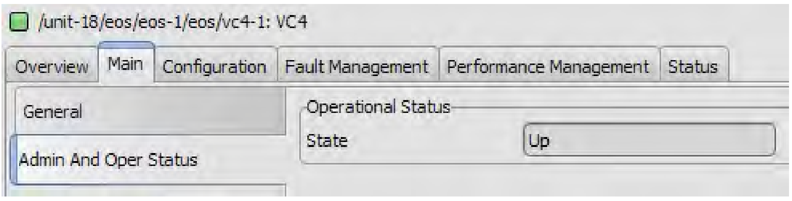


Table 94: AP: / unit-x / eos / eos-y / eos / vcz-a, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the EoS group member. The operational state is up when the EoS port administrative state is up. VC-4 members of an EoS group require in addition a sink connection to another VC-4 resource.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.9.3 AP: / unit-x / eos / eos-y / eos / vcz-a, Configuration

8.9.3.1 AP: / unit-x / eos / eos-y / eos / vcz-a, Configuration - CTP

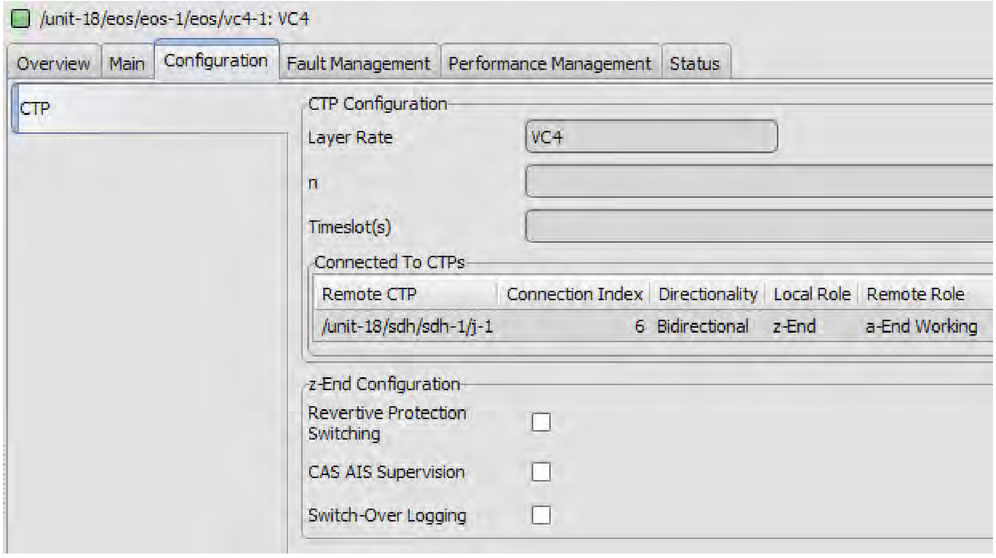


Table 95: AP: / unit-x / eos / eos-y / eos / vcz-a, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	VC4	The layer rate of the connection termination point is fixed according to the EoS group configuration.
		VC3	
		VC12	
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a VC-4, VC-3 or VC-12 is not applicable.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a VC-4, VC-3 or VC-12 is not applicable.
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the VC-4, VC-3 or VC-12. Without a connection the parameter is empty
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The VC-4, VC-3 or VC-12 is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The VC-4, VC-3 or VC-12 is the working starting point of a protected or unprotected connection.
		a-End Protecting	The VC-4, VC-3 or VC-12 is the protecting starting point of a protected connection.

Table 95: AP: / unit-x / eos / eos-y / eos / vcz-a, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is not applicable with VC-4, VC-3 or VC-12.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

Please note:

The z-End of a protected connection shows two entries in the “Connected to CTPs” table, one for the working and one for the protecting path.

8.9.4 AP: / unit-x / eos / eos-y / eos / vc4-a, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 96: AP: / unit-x / eos / eos-y / eos / vc4-a, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
NDPF	Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 2592 or SES ≥ 33 or BBE ≥ 12’960 over a 24 hour interval at the near end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
NUPF	Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 180 or SES ≥ 15 or BBE ≥ 1100 over a 15 min. interval at the near end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 4 and SES = 0 and BBE ≤ 50. The alarm can be cleared by resetting the corresponding PM alarm counter.

Table 96: AP: / unit-x / eos / eos-y / eos / vc4-a, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
FDPF	Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 2592 or SES ≥ 33 or BBE ≥ 12’960 over a 24 hour interval at the far end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
FUPF	Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 180 or SES ≥ 15 or BBE ≥ 1100 over a 15 min. interval at the far end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 4 and SES = 0 and BBE ≤ 50. The alarm can be cleared by resetting the corresponding PM alarm counter.
EXC	Excessive Bit Error Rate	Communication Alarm	☑	Major	The bit error ratio is above the configured “Excessive Defect Threshold” for VC-4.
DEG	Degraded Signal	Communication Alarm	☐	Major	The bit error ratio is above the configured “Degraded Defect Threshold” for VC-4.
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. applying a loop.
TSF	Trail Signal Failure	Communication Alarm	☑	Major	For unprotected connections: Signal failure on the working VC-4 subnetwork connection. For protected connections: Signal failure on the working **and** protecting VC-4 subnetwork connection. Alarm activation criteria: AU-4-LOP, AU-4-AIS, VC-4-UNEQ or VC-4-TIM. Note that this alarm is not monitored by default.
RTSF	Redundant Trail Signal Failure	Communication Alarm	☑	Minor	For unprotected connections: Alarm not available. For protected connections: Signal failure on the working **or** protecting VC-4 subnetwork connection. Alarm activation criteria: AU-4-LOP, AU-4-AIS, VC-4-UNEQ or VC-4-TIM. Note that this alarm is not monitored by default.

Please note:
The monitoring of the TSF and RTSF alarms is disabled by default.

8.9.5 AP: / unit-x / eos / eos-y / eos / vc3-a, Fault Management

For the a description of the general aspects of the
- “Fault Management - Status”, and

– “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 97: AP: / unit-x / eos / eos-y / eos / vc3-a, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
NDPF	Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 2000 or SES ≥ 33 or BBE ≥ 6480 over a 24 hour interval at the near end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
NUPF	Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 150 or SES ≥ 15 or BBE ≥ 1100 over a 15 min. interval at the near end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 3 and SES = 0 and BBE ≤ 50. The alarm can be cleared by resetting the corresponding PM alarm counter.
FDPF	Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 2000 or SES ≥ 33 or BBE ≥ 6480 over a 24 hour interval at the far end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
FUPF	Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 150 or SES ≥ 15 or BBE ≥ 1100 over a 15 min. interval at the far end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 3 and SES = 0 and BBE ≤ 50. The alarm can be cleared by resetting the corresponding PM alarm counter.
EXC	Excessive Bit Error Rate	Communication Alarm	☑	Major	The bit error ratio is above the configured “Excessive Defect Threshold” for VC-3.
DEG	Degraded Signal	Communication Alarm	☐	Major	The bit error ratio is above the configured “Degraded Defect Threshold” for VC-3.
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. applying a loop.
TSF	Trail Signal Failure	Communication Alarm	☑	Major	For unprotected connections: Signal failure on the working VC-3 subnetwork connection. For protected connections: Signal failure on the working **and** protecting VC-3 subnetwork connection. Alarm activation criteria: TU-3-LOP, TU-3-AIS, VC-3-UNEQ or VC-3-TIM. Note that this alarm is not monitored by default.

Table 97: AP: / unit-x / eos / eos-y / eos / vc3-a, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
RTSF	Redundant Trail Signal Failure	Communication Alarm	☑	Minor	For unprotected connections: Alarm not available. For protected connections: Signal failure on the working **or** protecting VC-3 subnetwork connection. Alarm activation criteria: TU-3-LOP, TU-3-AIS, VC-3-UNEQ or VC-3-TIM. Note that this alarm is not monitored by default.

Please note:

The monitoring of the TSF and RTSF alarms is disabled by default.

8.9.6 AP: / unit-x / eos / eos-y / eos / vc12-a, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 98: AP: / unit-x / eos / eos-y / eos / vc12-a, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
NDPF	Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 648 or SES ≥ 33 or BBE ≥ 1620 over a 24 hour interval at the near end. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
NUPF	Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 120 or SES ≥ 15 or BBE ≥ 300 over a 15 min. interval at the near end. The alarm status is reset after a 15 min. interval with ES ≤ 2 and SES = 0 and BBE ≤ 12. The alarm can be cleared by resetting the corresponding PM alarm counter.
FDPF	Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 648 or SES ≥ 33 or BBE ≥ 1620 over a 24 hour interval at the far end. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
FUPF	Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 120 or SES ≥ 15 or BBE ≥ 300 over a 15 min. interval at the far end. The alarm status is reset after a 15 min. interval with ES ≤ 2 and SES = 0 and BBE ≤ 12. The alarm can be cleared by resetting the corresponding PM alarm counter.

Table 98: AP: / unit-x / eos / eos-y / eos / vc12-a, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
EXC	Excessive Bit Error Rate	Communication Alarm	☑	Major	The bit error ratio is above the configured “Excessive Defect Threshold” for VC-12.
DEG	Degraded Signal	Communication Alarm	☐	Major	The bit error ratio is above the configured “Degraded Defect Threshold” for VC-12.
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. applying a loop.
TSF	Trail Signal Failure	Communication Alarm	☑	Major	For unprotected connections: Signal failure on the working VC-12 subnetwork connection. For protected connections: Signal failure on the working **and** protecting VC-12 subnetwork connection. Alarm activation criteria: TU-12-LOP, TU-12-AIS, VC-12-UNEQ or VC-12-TIM. Note that this alarm is not monitored by default.
RTSF	Redundant Trail Signal Failure	Communication Alarm	☑	Minor	For unprotected connections: Alarm not available. For protected connections: Signal failure on the working **or** protecting VC-12 subnetwork connection. Alarm activation criteria: TU-12-LOP, TU-12-AIS, VC-12-UNEQ or VC-12-TIM. Note that this alarm is not monitored by default.

Please note:

The monitoring of the TSF and RTSF alarms is disabled by default.

8.9.7 AP: / unit-x / eos / eos-y / eos / vcz-a, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

The PM parameters are presented in different groups. The following counter groups are available for the NUSA1 EoS members:

- “G.826” group, see section 8.9.7.1 AP: / unit-x / eos / eos-y / eos / vcz-a, Performance Management - G.826 (on page 227).
- “Unfiltered Events” group, see section 8.9.7.2 AP: / unit-x / eos / eos-y / eos / vcz-a, Performance Management - Unfiltered Events (on page 227).

The following counter intervals are available, depending of the counter group:

Table 99: PM counter interval availability

Counter interval	G.826	Unfiltered Events
User Counter	yes	yes
History 15min	yes	yes

Table 99: PM counter interval availability (continued)

Counter interval	G.826	Unfiltered Events
History 24h	yes	yes
Alarm 15min	yes	no
Alarm 24h	yes	no

8.9.7.1 AP: / unit-x / eos / eos-y / eos / vcz-a, Performance Management - G.826

Table 100: PM group: G.826

PM parameter	Description
Near End BBE	VC near end background block errors.
Near End ES	VC near end errored second.
Near End SES	VC near end severely errored second.
Near End UAT	VC near end unavailable time.
Far End BBE	VC far end background block errors.
Far End ES	VC far end errored second.
Far End SES	VC far end severely errored second.
Far End UAT	VC far end unavailable time.
Path UAT	VC path unavailable time.

8.9.7.2 AP: / unit-x / eos / eos-y / eos / vcz-a, Performance Management - Unfiltered Events

Table 101: PM group: Unfiltered Events

PM parameter	Description
Protection Switches	SNC protection switchover event

8.9.8 AP: / unit-x / eos / eos-y / eos / vcz-a, Status

8.9.8.1 AP: / unit-x / eos / eos-y / eos / vcz-a, Status - General

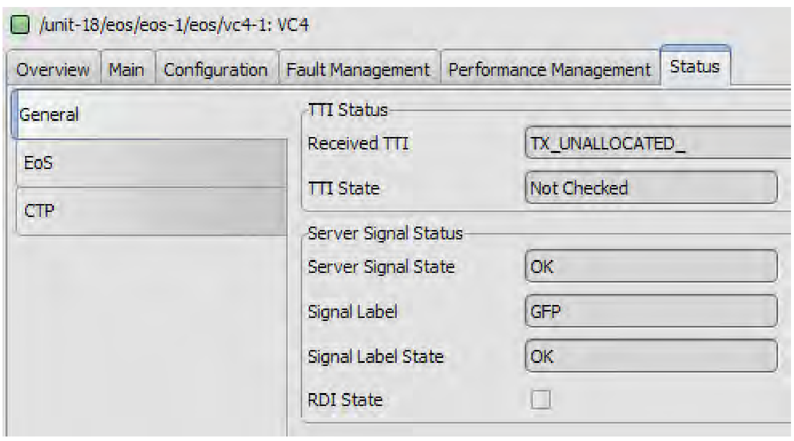


Table 102: AP: / unit-x / eos / eos-y / eos / vcz-a, Status - General

Operation Name	Parameter Name	Range	Description / Details
TTI Status	Received TTI	0 … 15 characters	Display of the received TTI in the J1 byte of the VC-4 or VC-3 path overhead or the J2 byte in the VC-12 path overhead. The received TTI of every group member is displayed.
	TTI State	OK	TTI supervision is enabled and the received TTI equals the expected TTI.
		Mismatch	TTI supervision is enabled and the received TTI is not equal to the expected TTI.
		Not Checked	TTI supervision is not enabled.
Server Signal Status	Server Signal State	OK	Failure indication of the VC-4, VC-3 or VC-12 server signal, i.e. the AU-4, TU-3 or TU-12 signal.
		AU-AIS	
		TU-AIS	
		AU-LOP	
		TU-LOP	
	Signal Label	GFP	The VC-4, VC-3 and VC-12 layers are able to transport a variety of client signals applied to the layer via different adaptation functions. The information about the signal type is carried in the (trail) signal label, transported in the C2 byte of the VC-4 or VC-3 path overhead or the V5 byte of the VC-12 path overhead. NUSA1 inserts the signal label "GFP" for all VC signals used for Ethernet transport.
		Unequipped	
		<Any other signal label>	
	Signal Label State	OK	The received signal label equals the expected signal label, i.e. "GFP".
		Mismatch	The received signal label is not equal to the expected signal label.
		Not Checked	The EoS VC is not cross connected.
	RDI State	☑	The VC-4, VC-3 and VC-12 path remote defect indication (RDI) displays the received RDI state which is sent back from the far end termination function, if either an AU-4, TU-3 or TU-12 server signal failure or a trail signal failure is being detected. RDI is transported in the G1 byte of the VC-4 or VC-3 path overhead or the V5 byte of the VC-12 path overhead. It can be "true" or "false". Note that the VC signal status is not filtered. E.g. a TTI mismatch in the RS layer inserts an AIS as a consequent action. All subsequent failures are also displayed: Signal label mismatch. Note that these states are not visible in the alarm list since the alarms are filtered.
		☐	

8.9.8.2 AP: / unit-x / eos / eos-y / eos / vcz-a, Status - EoS

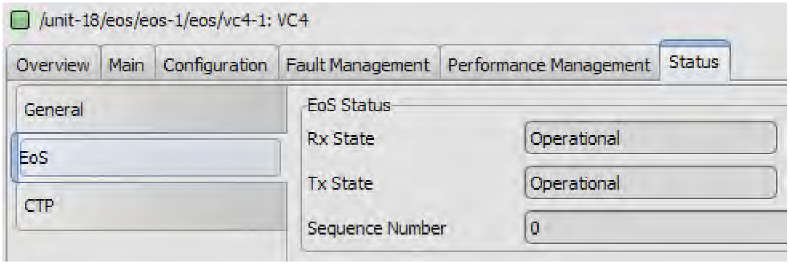


Table 103: AP: / unit-x / eos / eos-y / eos / vcz-a, Status - EoS

Operation Name	Parameter Name	Range	Description / Details
EoS Status	Rx State	Operational	Display of the receiver state of each member (VC-4, VC-3 or VC-12) of an EoS group. The state can be: - Operational, or - Failed, due to a loss of the multiframe alignment or a VC signal failure, or - Idle, the member is not part of the group or about to be removed.
		Failed	
		Idle	
	Tx State	Operational	When LCAS is enabled the transmitter state of each member (VC-4, VC-3 or VC-12) of an EoS group is displayed. Operational indicates normal transmission.
		Added	This member is about to be added to the group.
		Idle	This member is not part of the group or about to be removed.
		Do Not Use	Do not use the payload since the receive side reported a failure
		Fixed Non-LCAS	LCAS is disabled.
	Sequence Number	0 … 63	The sequence number uniquely identifies each received member within an EoS group.
		None	The EoS group member is not operational.

8.9.8.3 AP: / unit-x / eos / eos-y / eos / vcz-a, Status - CTP

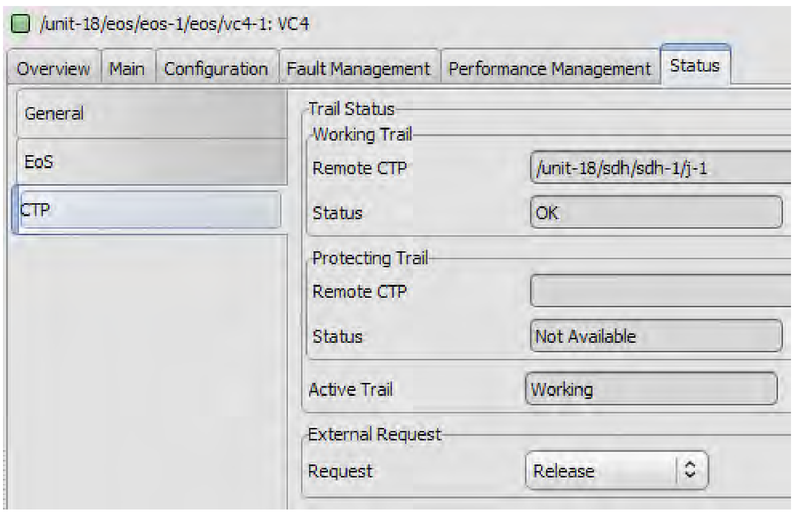


Table 104: AP: / unit-x / eos / eos-y / eos / vcz-a, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-4, VC-3 or VC-12 is connected to, e.g. /unit-20/port-1/j-1.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-4, VC-3 or VC-12 is connected to, e.g. /unit-20/port-2/j-1.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.10 AP: / unit-x / pdh

8.10.1 AP: / unit-x / pdh, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”,
- “Overview - Timeslot Allocation”, and
- “Overview - Unused Channels”

management functions, please refer to [302] User Guide “XMC25/XMC23/ XMC22”.

8.10.2 AP: / unit-x / pdh, Main

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/ XMC22”.

8.11 AP: / unit-x / pdh / vc12-y

8.11.1 AP: / unit-x / pdh / vc12-y, Overview

For a description of the
- "Overview - Alarms",
- "Overview - Cross Connections",
- "Overview - CTP",
- "Overview - Timeslot Allocation", and
- "Overview - Unused Channels"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.11.2 AP: / unit-x / pdh / vc12-y, Main

8.11.2.1 AP: / unit-x / pdh / vc12-y, Main - General

For a description of the
- "Main - General"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.11.2.2 AP: / unit-x / pdh / vc12-y, Main - Admin And Oper Status

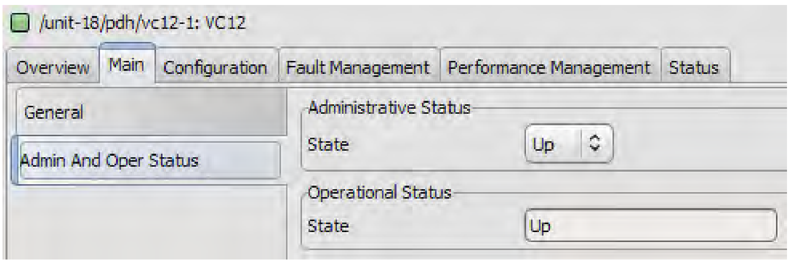


Table 105: AP: / unit-x / pdh / vc12-y, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Administrative Status	State	Up	Set the IETF administrative status of the VC-12 signal.
		Down	
Operational Status	State	Up	Display of the IETF operational status of the VC-12 signal.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.11.3 AP: / unit-x / pdh / vc12-y, Configuration

8.11.3.1 AP: / unit-x / pdh / vc12-y, Configuration - General

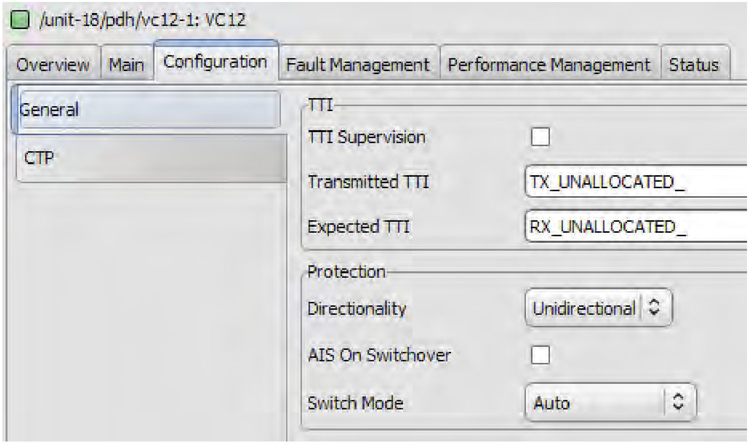


Table 106: AP: / unit-x / pdh / vc12-y, Configuration - General

Operation Name	Parameter Name	Range	Description / Details
TTI	TTI Supervision	☑ ☐	The trail trace identifier (TTI) supervision can be enabled or disabled. In the disabled mode no check is done on the received TTI and no alarm is generated. For further information please refer to section 7.4 Trail Trace Identifier (TTI) (on page 154)
	Transmitted TTI	15 characters	TTI transmitted in the VC-12 path overhead (J2 byte). The default string is TX_UNALLOCATED_. In the disabled mode the transmit TTI string is TX_UNALLOCATED_ or any other configured TTI. A TTI shorter than 15 characters is automatically completed with SPACE characters.
	Expected TTI	15 characters	TTI expected in the VC path overhead. The default string is RX_UNALLOCATED_. In the disabled mode the expected TTI string is RX_UNALLOCATED_ or any other configured TTI. A TTI shorter than 15 characters is automatically completed with SPACE characters.
Protection	Directionality	Unidirectional	In the unidirectional mode the path selector is controlled by the failure state of the working and the protecting paths, and by the WTR timer if the revertive operation type is configured.
		Bidirectional	In the bidirectional mode the path selector is in addition controlled by the remote selector state. In the bidirectional switching mode the local and the remote path selectors are synchronized to select both the same path, i.e. both select the working path or both select the protecting path. The automatic protection switching (APS) protocol used to synchronize the two selectors is transported in bit 4 of the V5 byte.

Table 106: AP: / unit-x / pdh / vc12-y, Configuration - General (continued)

Operation Name	Parameter Name	Range	Description / Details
	AIS On Switchover	☑	AIS on Switch-Over enabled:
		☐	At a switch-over event of the path selector the signal sent towards the PBUS can be replaced by an AIS signal for a duration of 4 s. If there is a mismatch in the local and remote path selector state the AIS insertion is not released until the mismatch state terminates.
	Switch Mode	Auto	For testing or debugging purposes the path selector of the SNC protected VC-12 signal can be forced to the working or the protecting path.
		Force Working	In case the VC-12 is configured to the bidirectional switching type also the remote selector will switch to the configured path.
		Force Protecting	The forced configurations override the external commands available in the CTP status dialogue. Note that no alarm is activated when the path selector is forced to the working or protecting path.

8.11.3.2 AP: / unit-x / pdh / vc12-y, Configuration - CTP

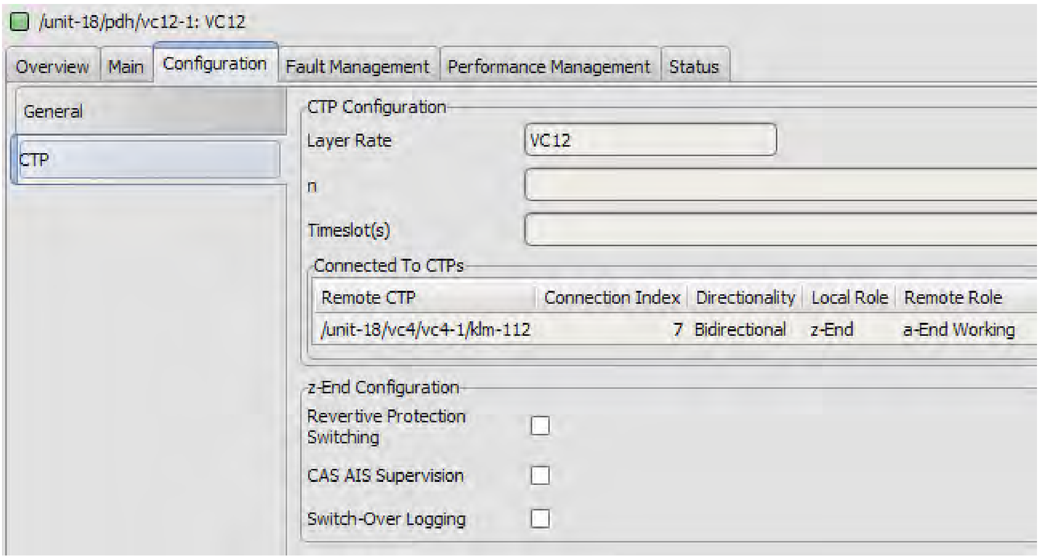


Table 107: AP: / unit-x / pdh / vc12-y, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	VC12	The layer rate of this connection termination point is fixed.
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a VC-12 is not applicable.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a VC-12 is not applicable.

Table 107: AP: / unit-x / pdh / vc12-y, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
Connected To CTPs	Remote CTP	<MO Address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65‘535	Index of a connection assigned to the VC-12. Without a connection the parameter is empty
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The VC-12 is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The VC-12 is the working starting point of a protected or unprotected connection.
		a-End Protecting	The VC-12 is the protecting starting point of a protected connection.
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is only applicable with P0-nc.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

8.11.4 AP: / unit-x / pdh / vc12-y, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 108: AP: / unit-x / pdh / vc12-y, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
AIS	AIS Received	Communication Alarm	☑	Minor	Failure in the received optical or electrical signal, in the RS or MS layer, or in the VC-4 layer or in the P12 VC-12 layer (TU-12-AIS).

Table 108: AP: / unit-x / pdh / vc12-y, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
LOP	Loss Of Pointer	Communication Alarm	☑	Major	Eight consecutive invalid TU-12 pointer values have been received (TU-12-LOP).
PLM	Payload Mismatch	Communication Alarm	☑	Major	The received and accepted trail signal label does not indicate the expected “Asynchronous” in the VC-12 (VC-12-PLM).
RDI	Remote Defect Indication	Communication Alarm	☐	Minor	The far end equipment has one or more of the following defects: VC-4-LOM, VC-4-PLM, TU-12-LOP, TU-12-AIS, VC-12-UNEQ, VC-12-TIM.
TIM	Trace Identifier Mismatch	Communication Alarm	☑	Major	The received and accepted TTI does not match the expected VC-12 TTI.
EXC	Excessive Bit Error Rate	Communication Alarm	☑	Major	The bit error ratio is above the configured “Excessive Defect Threshold” for VC-12.
DEG	Degraded Signal	Communication Alarm	☐	Major	The bit error ratio is above the configured “Degraded Defect Threshold” for VC-12.
UNEQ	Unequipped	Communication Alarm	☑	Major	The received and accepted trail signal label indicates “Unequipped” (VC-12-UNEQ).
NDPF	Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 648 or SES ≥ 33 or BBE ≥ 1620 over a 24 hour interval at the near end. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
NUPF	Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 120 or SES ≥ 15 or BBE ≥ 300 over a 15 min. interval at the near end. The alarm status is reset after a 15 min. interval with ES ≤ 2 and SES = 0 and BBE ≤ 12. The alarm can be cleared by resetting the corresponding PM alarm counter.
FDPF	Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 648 or SES ≥ 33 or BBE ≥ 1620 over a 24 hour interval at the far end. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
FUPF	Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 120 or SES ≥ 15 or BBE ≥ 300 over a 15 min. interval at the far end. The alarm status is reset after a 15 min. interval with ES ≤ 2 and SES = 0 and BBE ≤ 12. The alarm can be cleared by resetting the corresponding PM alarm counter.

Table 108: AP: / unit-x / pdh / vc12-y, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
APSFOP	APS Failure Of Protocol	Communication Alarm	☐	Minor	The remote path selector state received in the V5/4 bit mismatches the local path selector state. Note that there are transient states where the remote path selector indication does not reflect the actual path selector state, e.g. when after a bidirectional interruption of the working path only one direction is brought into service again. In this case the APS Failure Of Protocol alarm is raised even though both selectors still select the protecting path.
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status function has been done. E.g. external switch request.
TSF	Trail Signal Failure	Communication Alarm	☑	Major	For unprotected connections: Signal failure on the working channel subnetwork connection. For protected connections: Signal failure on the working **and** protecting channel subnetwork connection. Alarm activation criteria: Server signal fail or VC-12 signal failure. Note that this alarm is not monitored by default.
RTSF	Redundant Trail Signal Failure	Communication Alarm	☑	Minor	For unprotected connections: Alarm not available. For protected connections: Signal failure on the working **or** protecting channel subnetwork connection. Alarm activation criteria: Server signal fail or VC-12 signal failure. Note that this alarm is not monitored by default.

Please note:

The monitoring of the TSF and RTSF alarms is disabled by default.

8.11.5 AP: / unit-x / pdh / vc12-y, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

The PM parameters are presented in different groups. The following counter groups are available for the NUSA1 VC-12 signals:

- "G.826" group, see section 8.11.5.1 AP: / unit-x / pdh / vc12-y, Performance Management - G.826 (on page 238).
- "Unfiltered Events" group, see section 8.11.5.2 AP: / unit-x / pdh / vc12-y, Performance Management - Unfiltered Events (on page 238).

The following counter intervals are available, depending of the counter group:

Table 109: PM counter interval availability

Counter interval	G.826	Unfiltered Events
User Counter	yes	yes
History 15min	yes	yes
History 24h	yes	yes
Alarm 15min	yes	no
Alarm 24h	yes	no

8.11.5.1 AP: / unit-x / pdh / vc12-y, Performance Management - G.826

Table 110: PM group: G.826 VC-12

PM parameter	Description
Near End BBE	VC near end background block errors.
Near End ES	VC near end errored second.
Near End SES	VC near end severely errored second.
Near End UAT	VC near end unavailable time.
Far End BBE	VC far end background block errors.
Far End ES	VC far end errored second.
Far End SES	VC far end severely errored second.
Far End UAT	VC far end unavailable time.
Path UAT	VC path unavailable time.

8.11.5.2 AP: / unit-x / pdh / vc12-y, Performance Management - Unfiltered Events

Table 111: PM group: Unfiltered Events

PM parameter	Description
Protection Switches	SNC protection switchover event.

8.11.6 AP: / unit-x / pdh / vc12-y, Status

8.11.6.1 AP: / unit-x / pdh / vc12-y, Status - General

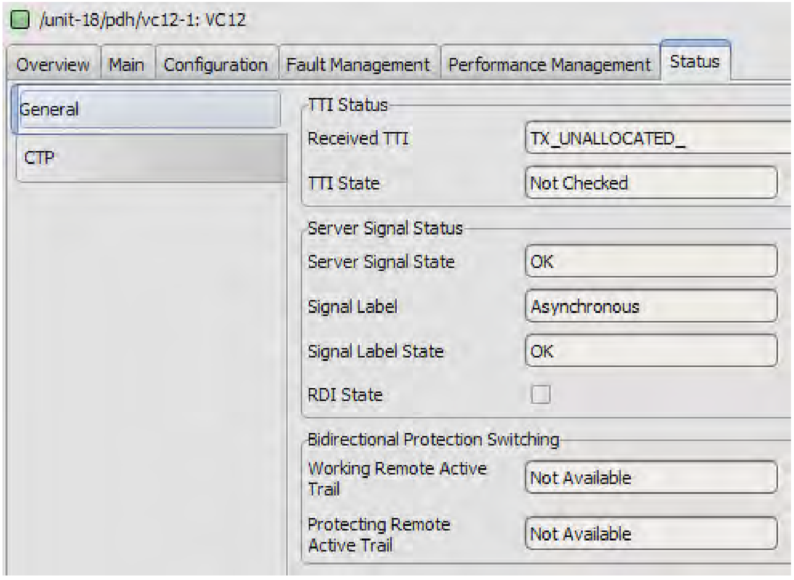


Table 112: AP: / unit-x / pdh / vc12-y, Status - General

Operation Name	Parameter Name	Range	Description / Details
TTI Status	Received TTI	0 … 15 characters	Display of the received TTI in the J2 byte in the VC-12 path overhead.
	TTI State	OK	TTI supervision is enabled and the received TTI equals the expected TTI.
		Mismatch	TTI supervision is enabled and the received TTI is not equal to the expected TTI.
		Not Checked	TTI supervision is not enabled.
Server Signal Status	Server Signal State	OK	Failure indication of the VC-12 server signal, i.e. the TU-12 signal. Signal fail means a SSF in the server signal.
		TU-AIS	
		TU-LOP	
		Signal Fail	
	Signal Label	Asynchronous	The VC-12 layers are able to transport a variety of client signals applied to the layer via different adaptation functions. The information about the signal type is carried in the (trail) signal label, transported in the V5 byte of the VC-12 path overhead. NUSA1 inserts the signal label “Asynchronous” for all VC-12 signals with tributaries from the PBUS. VC-12 signals without cross connection insert the signal label “Unequipped”. VC-12 signals with a server failure show an “Unknown” signal label.
		Unequipped	
		Unknown	
		<Any other signal label>	

Table 112: AP: / unit-x / pdh / vc12-y, Status - General (continued)

Operation Name	Parameter Name	Range	Description / Details
	Signal Label State	OK	The received signal label equals the expected signal label, i.e. “Asynchronous”.
		Mismatch	The received signal label is not equal to the expected signal label.
		Not Checked	The VC-12 is not used for transport, i.e. no cross connections have been configured.
	RDI State	☑	The VC-12 path remote defect indication (RDI) displays the received RDI state of the active trail which is sent back from the far end termination function, if either TU-12 server signal failure or a trail signal failure is being detected. RDI is transported in the V5 byte of the VC-12 path overhead. It can be “true” or “false”. Note that the VC signal status is not filtered. E.g. a server signal AIS has as a consequence also a signal label mismatch. Note that these states are not visible in the alarm list since the alarms are filtered.
		☐	
Bidirectional Protection Switching	Working Remote Active Trail	Working	Display of the remote selector status, transported in the working trail. Not available means that the bidirectional protection switching is not enabled or the trail is faulty. Bit 4 of the V5 VC-12 path overhead is used for the KEYMILE proprietary transport of the automatic protection switching (APS) protocol. The APS Protocol Failure alarm is activated when the received APS protocol state on the active trail mismatches the local path selector state.
		Protecting	
		Not Available	
	Protecting Remote Active Trail	Working	Display of the remote selector status, transported in the protecting trail. Not available means that the bidirectional protection switching is not enabled or the trail is faulty. Bit 4 of the V5 VC-12 path overhead is used for the KEYMILE proprietary transport of the automatic protection switching (APS) protocol.
		Protecting	
		Not Available	

8.11.6.2 AP: / unit-x / pdh / vc12-y, Status - CTP

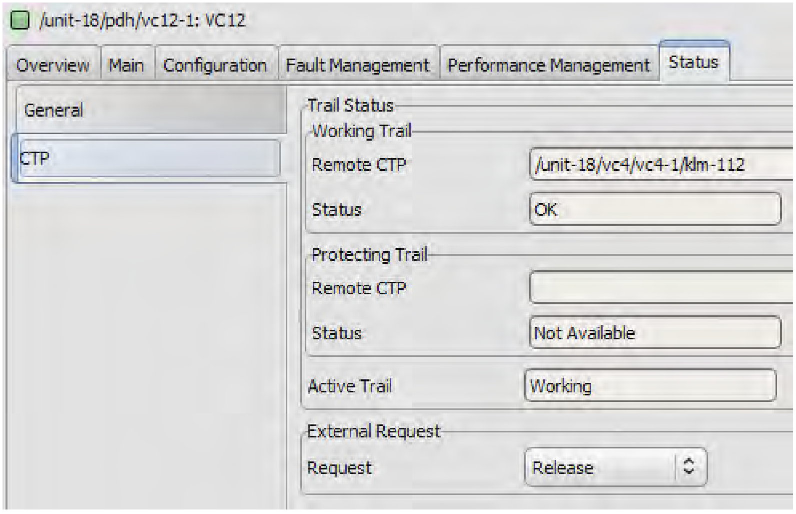


Table 113: AP: / unit-x / pdh / vc12-y, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-12 is connected to, e.g. /unit-18/vc4/vc4-1/klm-112.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-12 is connected to, e.g. /unit-18/vc4/vc4-2/klm-132.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.

Table 113: AP: / unit-x / pdh / vc12-y, Status - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.12 AP: / unit-x / pdh / vc12-y / p12

8.12.1 AP: / unit-x / pdh / vc12-y / p12, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”,
- “Overview - Timeslot Allocation”, and
- “Overview - Unused Channels”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.12.2 AP: / unit-x / pdh / vc12-y / p12, Main

8.12.2.1 AP: / unit-x / pdh / vc12-y / p12, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.12.2.2 AP: / unit-x / pdh / vc12-y / p12, Main - Admin And Oper Status

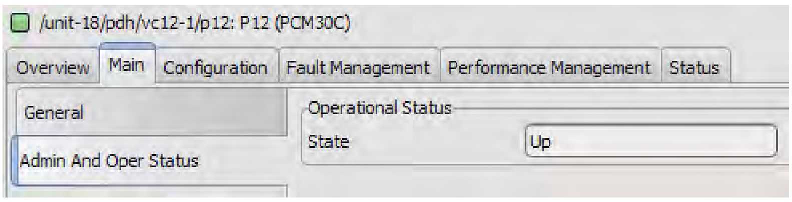


Table 114: AP: / unit-x / pdh / vc12-y / p12, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the P12 signal. The operational status is set to up when the administrative status of the VC-12 is set to up and no major defect is active.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.12.3 AP: / unit-x / pdh / vc12-y / p12, Configuration

Please note that the fields for some of the configuration parameters are context sensitive. Configuration parameters that are not available due to a higher-ranking configuration parameter are indicated as “NA” (not available) or “None”.

The steering parameters for the port configuration are

- Termination Mode
- Synchronization Method

The configuration strategy to be followed is from the uppermost tab (General) to the lowermost tab (Channels), and on the tabs from the top parameter downwards.

After the parameter configuration of a higher-ranking parameter press the “Apply” button to assign the applicable values to the lower-ranking parameters.

8.12.3.1 AP: / unit-x / pdh / vc12-y / p12, Configuration - General

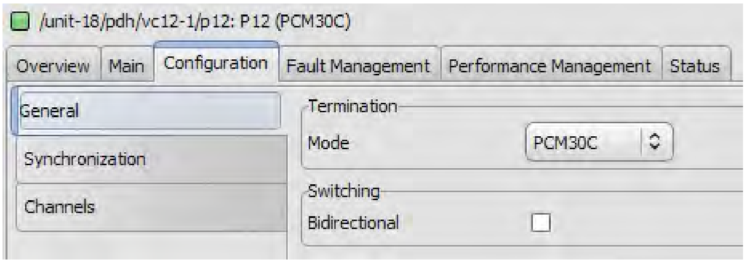


Table 115: AP: / unit-x / pdh / vc12-y / p12, Configuration - General

Operation Name	Parameter Name	Range	Description / Details
Termination	Mode	Transparent	Clock and data transparent. 2048 kbit/s signal with unknown structure.
		Clock Master	Transparent data, clock locked to PETS. 2048 kbit/s signal with unknown structure.
		PCM30	Terminated with CAS, without CRC4. ITU-T G.704 structured 2048 kbit/s signal.
		PCM30C	Terminated with CAS and CRC4. ITU-T G.704 structured 2048 kbit/s signal.
		PCM31	Terminated without CAS or CRC4. ITU-T G.704 structured 2048 kbit/s signal.
		PCM31C	Terminated without CAS, with CRC4. ITU-T G.704 structured 2048 kbit/s signal.
		V5 Uplink	Transport mode for V5 links. The 5 Sa bits (timeslot 0, spare bits Sa4 … Sa8) support V5.x applications. This uplink uses CRC4.
		V5 Uplink NCI	Transport mode for V5 links. The 5 Sa bits (timeslot 0, spare bits Sa4 … Sa8) support V5.x applications. This uplink does not offer CRC4.

Table 115: AP: / unit-x / pdh / vc12-y / p12, Configuration - General (continued)

Operation Name	Parameter Name	Range	Description / Details
Switching	Bidirectional	☑	In the bidirectional mode the path selector is controlled by the failure state of the working and the protecting paths and by the remote selector state. In the bidirectional switching mode the local and the remote path selectors are synchronized to select both the same path, i.e. both select the working path or both select the protecting path. Please refer to [314] User Guide "TDM Services and Cross Connections in XMC20" for a description of the switching criteria.
		☐	In the unidirectional mode the path selector is controlled by the failure state of the working and the protecting paths.

Risk of operating trouble!

Changing the P12 termination mode results in most cases in incompatible layer rates or number of timeslots.

→ The channel with its CTP and the assigned connections are deleted automatically and must be newly created.

→ Please refer to [314] User Guide "TDM Services and Cross Connections in XMC20", section 4.2.2.

8.12.3.2 AP: / unit-x / pdh / vc12-y / p12, Configuration - Synchronization

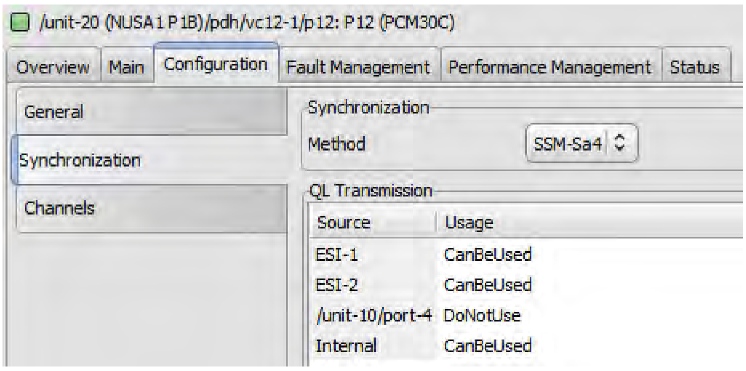


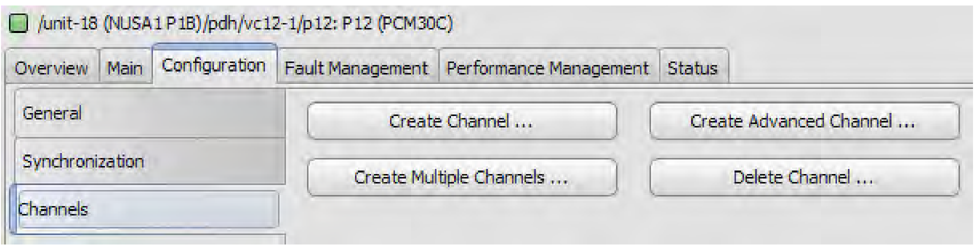
Table 116: AP: / unit-x / pdh / vc12-y / p12, Configuration - Synchronization

Operation Name	Parameter Name	Range	Description / Details
Synchronization	Method	None	Do not use a synchronization method
		SSM-Sa4	Use the selected Sa bit in time slot 0 for the transport of the synchronization status message (SSM). These parameter values are only available with the termination modes “PCM30C” and “PCM31C”.
		SSM-Sa5	
		SSM-Sa6	
		SSM-Sa7	
		SSM-Sa8	
		SSI-Sa5	Use the Sa5 bit in time slot 0 for the transport of the synchronization status indication (SSI). The SSI method is KEYMILE proprietary and is compatible with the UMUX. This parameter value is only available with the termination modes “PCM30”, “PCM30C”, “PCM31” and “PCM31C”.
QL Transmission	Source	ESI-1	Synchronization sources are all the PDH clock sources as they are configured at the AP: /Configuration - PETS
		ESI-2	
		<PDH Clock Source 1>	
		<PDH Clock Source 2>	
		<PDH Clock Source 3>	
		<PDH Clock Source 4>	
		Internal	
	Usage	NA	No synchronization method has been selected.
		CanBeUsed	Transmit the QL value of the selected synchronization source
		DoNotUse	Transmit the QL value 15, i.e. indicating that the traffic signal cannot be used as a synchronization source.

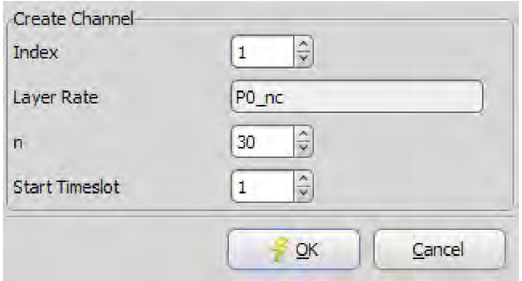
Please note:

For more information regarding quality level handling please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”.

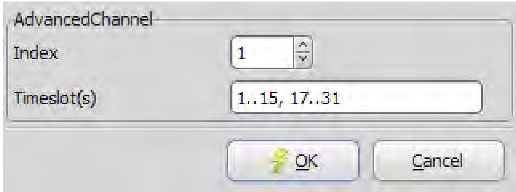
8.12.3.3 AP: / unit-x / pdh / vc12-y / p12, Configuration - Channels

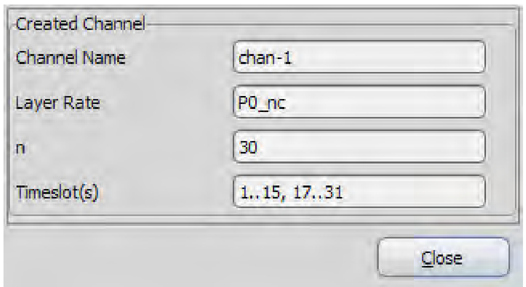


“Create Channel” and “Create Multiple Channels” dialogues:



The “Create Advanced Channel” command displays the created channel:





“Delete Channel” dialogue:

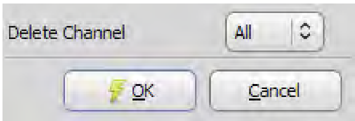


Table 117: AP: / unit-x / pdh / vc12-y / p12, Configuration - Channels

Operation Name	Parameter Name	Range	Description / Details
Create Channel …			Open the ECST dialogue to create one or more channels. A channel is a connection termination point (CTP) used as a starting or ending point of a cross connection.
Create Channel	Index	0 … 32	The channel index is used to identify the channel. 0 is a reserved value used for the auto-assignment of a channel index: The auto-assigned index is the highest existing index number + 1. In the ECST the default value is the autoassigned index number.
	Layer Rate	P12	Unstructured 2048 kbit/s. Automatically selected when the termination mode is configured to “Transparent” or “Clock Master”.
		P0_nc	Structured n x 64 kbit/s. Automatically selected when the termination mode is configured to “PCM30”, “PCM30C”, “PCM31”, “PCM31C”, “V5 Uplink” or V5 Uplink NCI”.
	n	1 … 32	Number of consecutive timeslots (valid for P0_nc only). If the structured P12 signal, the channel is belonging to, uses CAS the timeslot 16 will be skipped automatically, e.g. a channel with n = 19 and start timeslot 1 will occupy timeslots 1 to 15 and 17 to 20 in a PCM30 signal. The default value is the maximum of available timeslots.

Table 117: AP: / unit-x / pdh / vc12-y / p12, Configuration - Channels (continued)

Operation Name	Parameter Name	Range	Description / Details
	Start Timeslot	0 … 31	First timeslot of the first channel in the structured P12 signal (valid for P0_nc only). The minimum valid parameter value is 1. Note that start timeslot 0 is only used for the unstructured P12 mode.
Create Advanced Channel …			Open the ECST dialogue to create one channels with non-consecutive time slots in the structured P12 signal. The termination mode must be configured to “PCM30”, “PCM30C”, “PCM31” or “PCM31C”.
Create Advanced Channel	Index	0 … 32	The channel index is used to identify the channel. 0 is a reserved value used for the auto-assignment of a channel index: The auto-assigned index is the highest existing index number + 1. In the ECST the default value is the autoassigned index number.
	Timeslot(s)	<Timeslot range>	Configure the time slots to be used. A range of consecutive time slots is defined by “..”, e.g. “5..9”. Different ranges are separated by “,”, e.g. “1, 4, 5..9, 31” If the structured P12 signal, the channel is belonging to, uses CAS the timeslot 16 must not be used, i.e. a range must be split so that it does not include the timeslot 16, e.g. “1..15”, “17..31”.
Create Multiple Channels …			Open the ECST dialogue to create one or more channels. The termination mode must be configured to “PCM30”, “PCM30C”, “PCM31” or “PCM31C”.
Create Multiple Channels	Start Index	0 … 32	The start index is the channel index of the first channel. 0 is a reserved value used for the auto-assignment of a channel index: The auto-assigned index is the highest existing index number + 1. In the ECST the default value is the autoassigned index number.
	Number Of Channels	1 … 32	Number of channels to be created. If the configured number of channels to be created is higher than the available number of unused time slots, the ECST creates no channel, and displays a corresponding error message.
	n	1 … 32	Number of consecutive timeslots. If the structured P12 signal, the channel is belonging to, uses CAS the timeslot 16 will be skipped automatically, e.g. a channel with n = 19 and start timeslot 1 will occupy timeslots 1 to 15 and 17 to 20 in a PCM30 signal. The default value is the maximum of available timeslots. The start timeslot of the first channel is the lowest available timeslot number.
Delete Channel …			Open the ECST dialogue to delete one or all channels.

Table 117: AP: / unit-x / pdh / vc12-y / p12, Configuration - Channels (continued)

Operation Name	Parameter Name	Range	Description / Details
Delete Channel	Delete Channel	All	Delete all channels. All connections assigned to the channels will be deleted also.
		chan-1 … chan-31	Delete a channel. All connections assigned to the channel will be deleted also.

8.12.4 AP: / unit-x / pdh / vc12-y / p12, Fault Management

For the a description of the general aspects of the

- "Fault Management - Status", and
- "Fault Management - Configuration"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22". The following table lists the fault causes of the current AP.

Table 118: AP: / unit-x / pdh / vc12-y / p12, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. applying a loop.
AIS	AIS Received	Communication Alarm	☑	Minor	AIS detected on the incoming P12 signal.
LOF	Loss Of Frame	Communication Alarm	☑	Major	Loss of frame alignment on the incoming P12 signal.
LOCM	Loss Of CAS MF	Communication Alarm	☑	Major	Loss of CAS multiframe alignment on the incoming P12 signal.
DEG	Degraded Signal	Communication Alarm	☐	Major	BER > 10^{-3} on the incoming P12 signal from TS0 errors (CRC4 disabled), or BER > 10^{-5} on the incoming P12 signal calculated using CRC4 block errors (CRC4 enabled).
NCI	Non CRC4 Interworking	Communication Alarm	☐	Warning	The CRC4 monitoring function is disabled due to a disabled CRC4 function at the remote equipment.
RDI	Remote Defect Indication	Communication Alarm	☐	Minor	The far end equipment has one or more of the following defects: Hardware fault, AIS received, BER > 10^{-3}, loss of frame, loss of signal.
RLOCM	Remote Loss Of CAS MF	Communication Alarm	☐	Minor	Loss of CAS multiframe alignment on the incoming P12 signal at the remote equipment.
RNCI	Remote Non CRC4 Interworking	Communication Alarm	☐	Minor	"Non CRC4 interworking" alarm at the remote equipment.
NDPF	Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 432 or SES ≥ 22 over a 24 hour interval at the near end. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.

Table 118: AP: / unit-x / pdh / vc12-y / p12, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
NUPF	Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 150 or SES ≥ 15 over a 15 min. interval at the near end. The alarm status is reset after a 15 min. interval with ES ≤ 3 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
FDPF	Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 432 or SES ≥ 22 over a 24 hour interval at the far end. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
FUPF	Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 150 or SES ≥ 15 over a 15 min. interval at the far end. The alarm status is reset after a 15 min. interval with ES ≤ 3 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.

8.12.5 AP: / unit-x / pdh / vc12-y / p12, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

The PM parameters are presented in different groups. The following counter groups are available for the NUSA1 P12 signals:

- “G.826” group, see section 8.12.5.1 AP: / unit-x / pdh / vc12-y / p12, Performance Management - G.826 (on page 250).
- “P12 Events” group, see section 8.12.5.2 AP: / unit-x / pdh / vc12-y / p12, Performance Management - P12 Events (on page 251).

The following counter intervals are available, depending of the counter group:

Table 119: PM counter interval availability

Counter interval	G.826	P12 Events
User Counter	yes	yes
History 15min	yes	yes
History 24h	yes	yes
Alarm 15min	yes	no
Alarm 24h	yes	no

8.12.5.1 AP: / unit-x / pdh / vc12-y / p12, Performance Management - G.826

Table 120: PM group: G.826

PM parameter	Description
Near End BBE	Near end count of Background Block Errors.
Near End ES	Near end count of Errored Seconds.

Table 120: PM group: G.826 (continued)

PM parameter	Description
Near End SES	Near end count of Severely Errored Seconds.
Near End UAT	Near end count of Unavailable Time.
Far End BBE	Far end count of Background Block Errors.
Far End ES	Far end count of Errored Seconds.
Far End SES	Far end count of Severely Errored Seconds.
Far End UAT	Far end count of Unavailable Time.
Path UAT	Path UAT is the UAT of the near end or the far end.

8.12.5.2 AP: / unit-x / pdh / vc12-y / p12, Performance Management - P12 Events

Table 121: PM group: P12 Events

PM parameter	Description
Positive Slips	Near end positive frame slips. The counter for positive frame slips is incremented when the clock of the NE runs faster than the clock provided via the ITU-T G.704 framed 2 Mbit/s traffic signal.
Negative Slips	Near end negative frame slips. The counter for negative frame slips is incremented when the clock of the NE runs slower than the clock provided via the ITU-T G.704 framed 2 Mbit/s traffic signal.

8.12.6 AP: / unit-x / pdh / vc12-y / p12, Status

8.12.6.1 AP: / unit-x / pdh / vc12-y / p12, Status - Maintenance

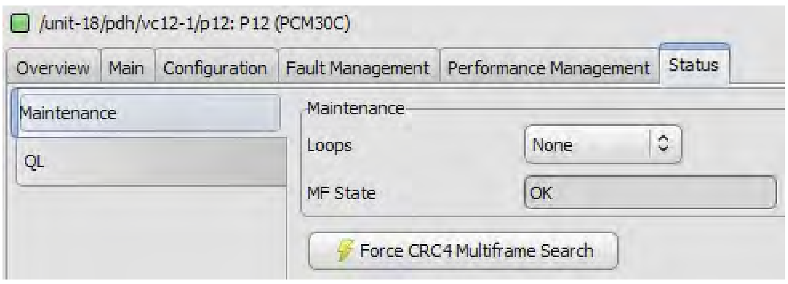


Table 122: AP: / unit-x / pdh / vc12-y / p12, Status - Maintenance

Operation Name	Parameter Name	Range	Description / Details
Maintenance	Loops	None	No loop active. Refer to section 7.2.2 P12 and P0-nc Loops (on page 151)
		Front To Front	The incoming signal from the SDH port is looped back towards the SDH port. The loop is removed when the configuration is restored or the port administrative state is set to down.

Table 122: AP: / unit-x / pdh / vc12-y / p12, Status - Maintenance (continued)

Operation Name	Parameter Name	Range	Description / Details
	MF State	OK	The CRC4 multiframe alignment state is read only. The CRC4 monitoring function is active.
		Non CRC Interworking	The CRC4 monitoring function is disabled due to disabled CRC4 at the remote equipment. If the CRC4 multiframe alignment is in the NCI state no further automatic search is done. A new search for CRC4 multiframe alignment must be initiated manually with the “Force CRC4 Multi-frame Search” command (see below).
		None	The port is configured without CRC4 monitoring.
Force CRC4 Multi-frame Search			Trigger a new attempt for the CRC4 multiframe alignment. To check the result of the new attempt, you have to press the “Refresh” button.

Please note:

During maintenance an NCI Alarm (non-CRC4 interworking) can appear. If this alarm is active, and it is known that the other equipment now sends the CRC4 multiframe, the following procedure can clear the alarm:

→ Perform a “Force new search” in the CRC4 MFA status of the P12 layer, or

→ Disable CRC4 and re-enable the CRC4.

8.12.6.2 AP: / unit-x / pdh / vc12-y / p12, Status - QL

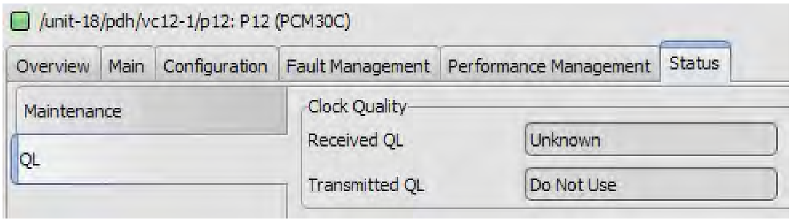


Table 123: AP: / unit-x / pdh / vc12-y / p12, Status - QL

Operation Name	Parameter Name	Range	Description / Details
Clock Quality	Received QL	Unknown	The synchronization method “None” has been configured.
		Do Not Use	Received SSM value = 15. The received SSI value = 0 is interpreted as “Do Not Use” and gets the QL = 15 assigned.
		1 … 14	Display of the received SSM value < 15. The received SSI value = 1 is interpreted as “Can Be Used” and gets the QL = 13 assigned.
	Transmitted QL	Unknown	The synchronization method “None” has been configured.
		Do Not Use	The “Do Not Use” quality level is transmitted as SSM value = 15, or as SSI value = 0.
		1 … 14	Display of the transmitted SSM value < 15. The transmitted SSI value = 1 is displayed as QL = 13.

8.13 AP: / unit-x / pdh / vc12-y / p12 / chan-z

8.13.1 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - CTP”

management functions, please refer to [302] User Guide “XMC25/XMC23/ XMC22”.

8.13.2 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Main

8.13.2.1 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/ XMC22”.

8.13.2.2 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Main - Admin And Oper Status

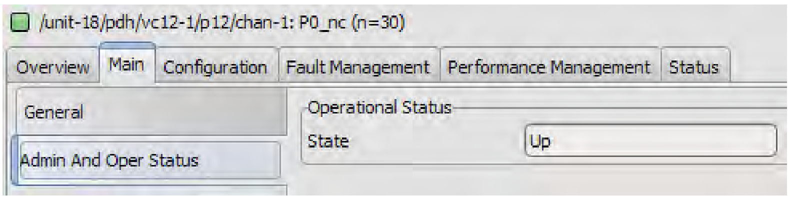
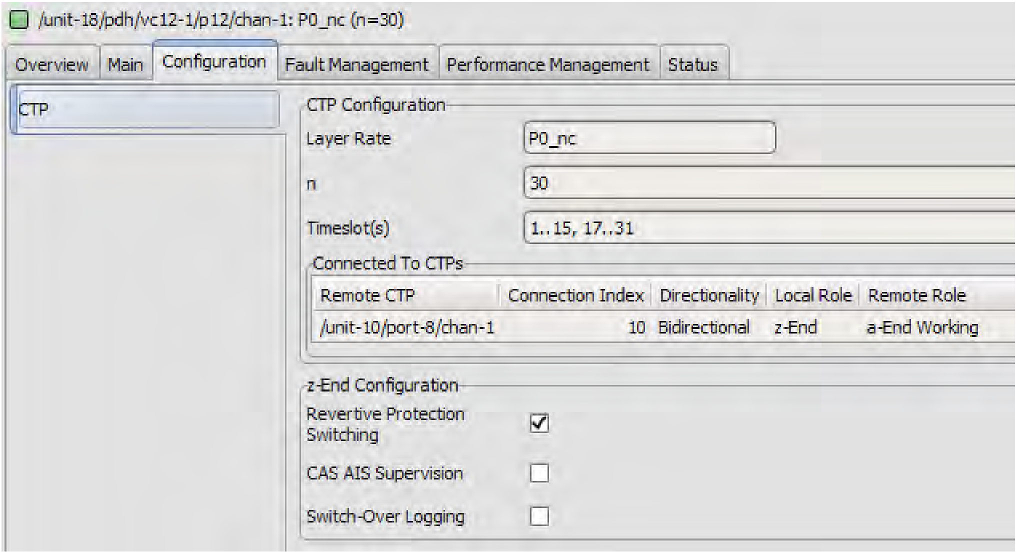


Table 124: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the channel. The operational state is set to up when the channel has a sink connection configured and no defect is active on the received signal from the PBUS.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.13.3 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Configuration

8.13.3.1 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Configuration - CTP



Please note:

All layer rate, number of time slots and time slot allocation parameters are read only.

→ To change a parameter the channel has to be deleted and newly created with the modified parameters.

Table 125: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	P12	Unstructured 2048 kbit/s.
		P0_nc	Structured n x 64 kbit/s.
	n	0 … 2 characters	Number of channel timeslots (valid for P0_nc only).
	Timeslot(s)	0 … 64 characters	Occupied timeslots in the structured P12 signal (valid for P0_nc only).
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the channel. Without a connection the parameter is empty
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The channel is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The channel is the working starting point of a protected or unprotected connection.
		a-End Protecting	The channel is the protecting starting point of a protected connection.

Table 125: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End. Non-revertive protection switching is only available for channels with the number of timeslots n=1. Non-revertive protection switching for n>1 will be available in a future release,
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is only applicable with P0-nc.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

Please note:

The z-End of a protected connection shows two entries in the “Connected to CTPs” table, one for the working and one for the protecting path.

8.13.4 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 126: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. manual switching request.

Table 126: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
TSF	Trail Signal Failure	Communication Alarm	☑	Major	For unprotected connections: Signal failure on the working channel subnetwork connection. For protected connections: Signal failure on the working **and** protecting channel subnetwork connection. Alarm activation criteria: Server signal fail or CAS AIS. Note that this alarm is not monitored by default.
RTSF	Redundant Trail Signal Failure	Communication Alarm	☑	Minor	For unprotected connections: Alarm not available. For protected connections: Signal failure on the working **or** protecting channel subnetwork connection. Alarm activation criteria: Server signal fail or CAS AIS. Note that this alarm is not monitored by default.

Please note:

The monitoring of the TSF and RTSF alarms is disabled by default.

8.13.5 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

The PM parameters are presented in different groups. The following counter group is available for the NUSA1 P12 channels:

- "Protection" group, see section 8.13.5.1 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Performance Management - Protection (on page 256).

The following counter intervals are available:

Table 127: PM counter interval availability

Counter interval	Protection
User Counter	yes
History 15min	yes
History 24h	yes
Alarm 15min	no
Alarm 24h	no

8.13.5.1 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Performance Management - Protection

Table 128: PM group: Protection

PM parameter	Description
Switch-Over	Protection switchover event.

8.13.6 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Status

8.13.6.1 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Status - Maintenance

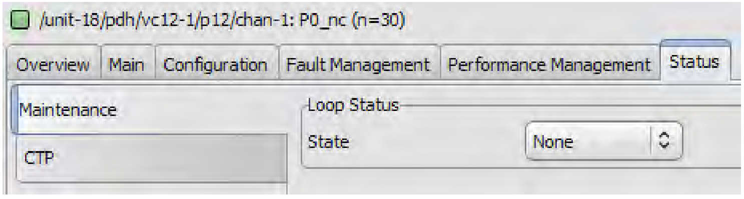


Table 129: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Status - Maintenance

Operation Name	Parameter Name	Range	Description / Details
Loop Status	State	None	Deactivate any loop.
		Front To Front	Activate the Front-to-front loop. For more information refer to section 7.2 Loops (on page 150).

Please note:

The channel CTP must have a cross connection configured, otherwise the loop cannot be activated.

8.13.6.2 AP: / unit-x / pdh / vc12-y / p12 / chan-z, Status - CTP

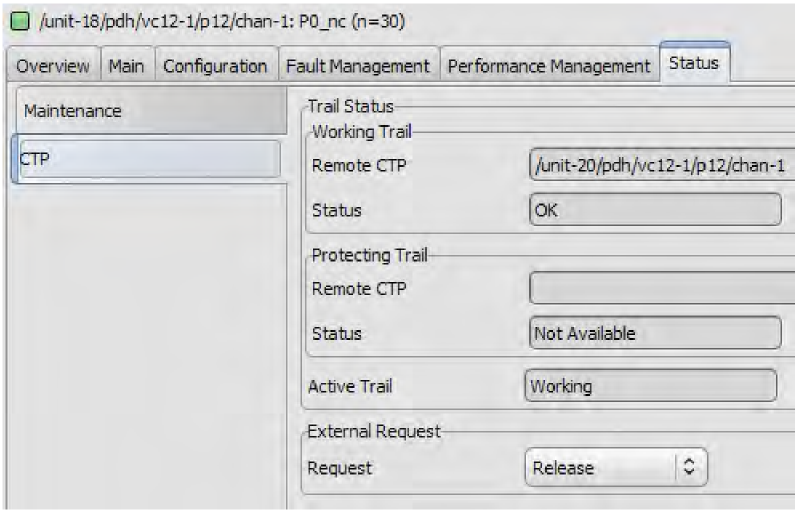


Table 130: AP: / unit-x / pdh / vc12-y / p12 / chan-z, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the P12 or P0-nc signal is connected to, e.g. /unit-21/port-1/chan-1.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		CAS AIS	CAS AIS status in the received signal, i.e. an all ‘1’ signal in time slot 16.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the P12 or P0-nc signal is connected to, e.g. /unit-21/port-2/chan-1.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		CAS AIS	CAS AIS status in the received signal, i.e. an all ‘1’ signal in time slot 16.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.14 AP: / unit-x / sdh

8.14.1 AP: / unit-x / sdh, Overview

For a description of the
- "Overview - Alarms",
- "Overview - Cross Connections", and
- "Overview - STM Allocation"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.14.2 AP: / unit-x / sdh, Main

For a description of the
- "Main - General"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.15 AP: / unit-x / sdh / sdh-y, y = 1 … 8

The sdh-5 to sdh-8 access points are only available within an EQP group.

8.15.1 AP: / unit-x / sdh / sdh-y, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - STM Allocation”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.15.2 AP: / unit-x / sdh / sdh-y, Main

8.15.2.1 AP: / unit-x / sdh / sdh-y, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.15.2.2 AP: / unit-x / sdh / sdh-y, Main - Admin And Oper Status

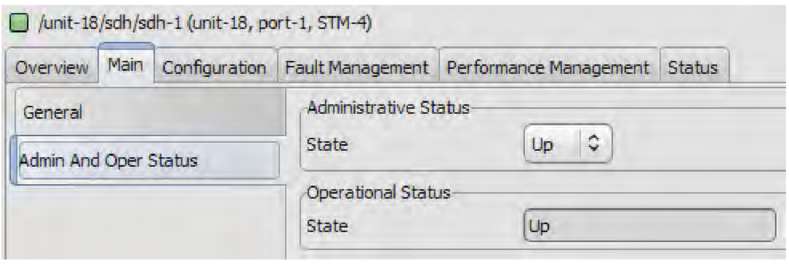


Table 131: AP: / unit-x / sdh / sdh-y, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Administrative Status	State	Up	Set the IETF administrative status of the SDH logical port.
		<u>Down</u>	
Operational Status	State	Up	Display of the IETF operational status of the logical SDH port.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.15.3 AP: / unit-x / sdh / sdh-y, Configuration

8.15.3.1 AP: / unit-x / sdh / sdh-y, Configuration - RS

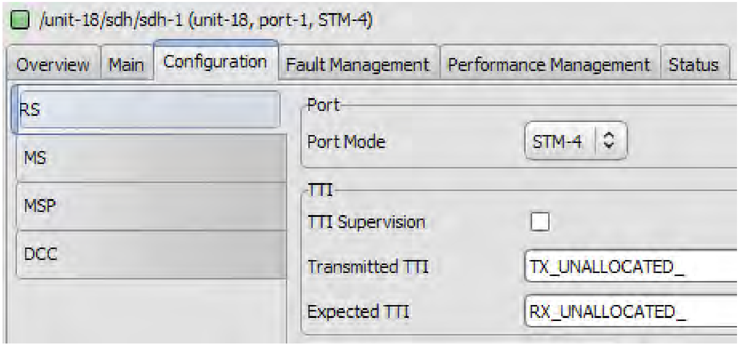


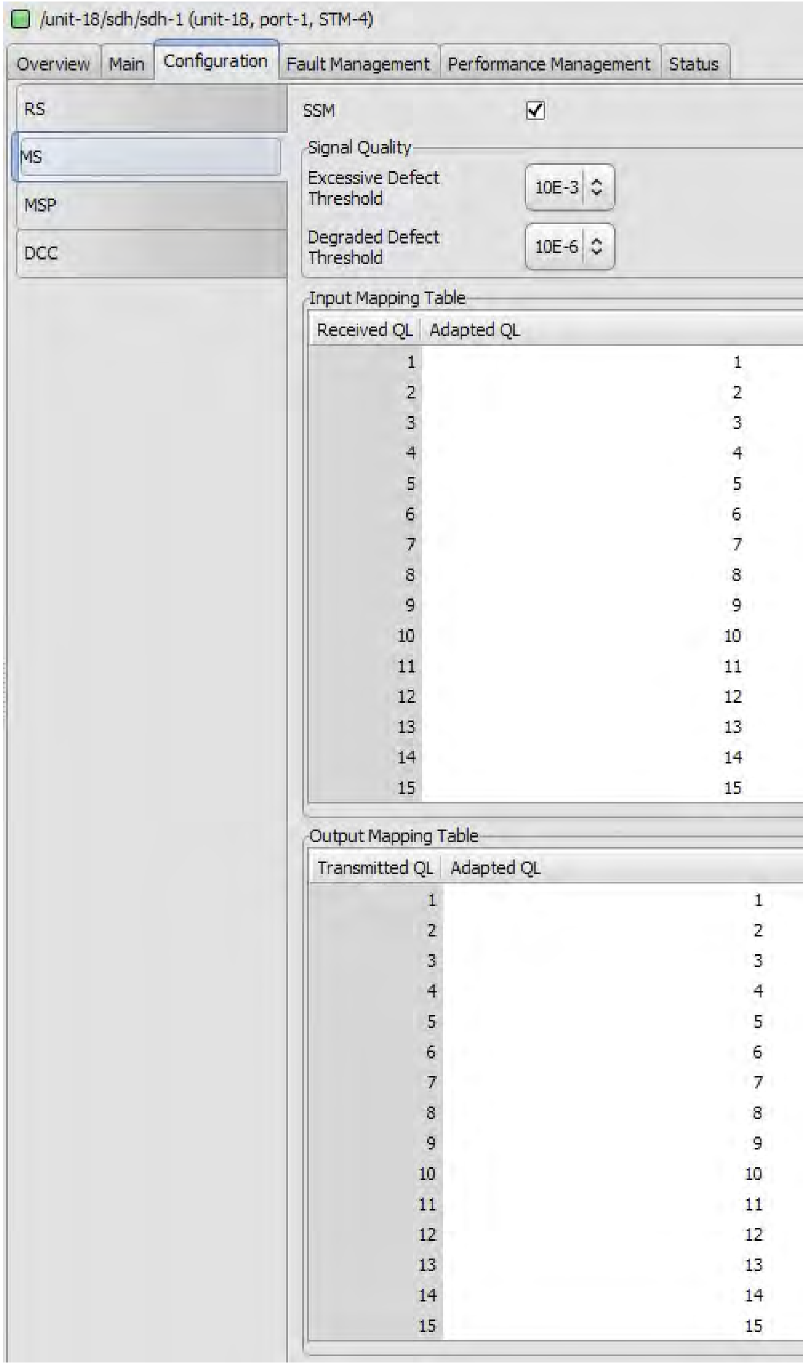
Table 132: AP: / unit-x / sdh / sdh-y, Configuration - RS

Operation Name	Parameter Name	Range	Description / Details
Port	Port Mode	STM-1 STM-4 STM-16	SDH port-1, port-2, port-5 and port-6 can be configured to STM-16 or STM-4. The default value is STM-4. SDH port-3, port-4, port-7 and port-8 can be configured to STM-4 or STM-1. The default value is STM-1. Please note that changing the port mode will remove any existing cross connections of the underlying VC-4 signals. This configuration has to match the configuration of the plugged SFP module. Note that multirate SFP modules are available that can be used for several SDH data rates. A multirate SFP module will be set according to the port type configuration. Note that the optical or electrical type configuration is done automatically by the plugged SFP module. Note that when MSP is enabled the port mode cannot be changed.

Table 132: AP: / unit-x / sdh / sdh-y, Configuration - RS (continued)

Operation Name	Parameter Name	Range	Description / Details
TTI	TTI Supervision	☑ ☐	The trail trace identifier (TTI) supervision can be enabled or disabled. In the disabled mode no check is done on the received TTI and no alarm is generated. For further information please refer to section 7.4 Trail Trace Identifier (TTI) (on page 154)
	Transmitted TTI	15 characters	TTI transmitted in the J0 byte of the RS over-head. The default string is TX_UNALLOCATED_. In the disabled mode the transmit TTI string is TX_UNALLOCATED_ or any other configured TTI. A TTI shorter than 15 characters is automatically completed with SPACE characters.
	Expected TTI	15 characters	TTI expected in the J0 byte of the RS overhead. The default string is RX_UNALLOCATED_. In the disabled mode the expected TTI string is RX_UNALLOCATED_ or any other configured TTI. A TTI shorter than 15 characters is automatically completed with SPACE characters.

8.15.3.2 AP: / unit-x / sdh / sdh-y, Configuration - MS



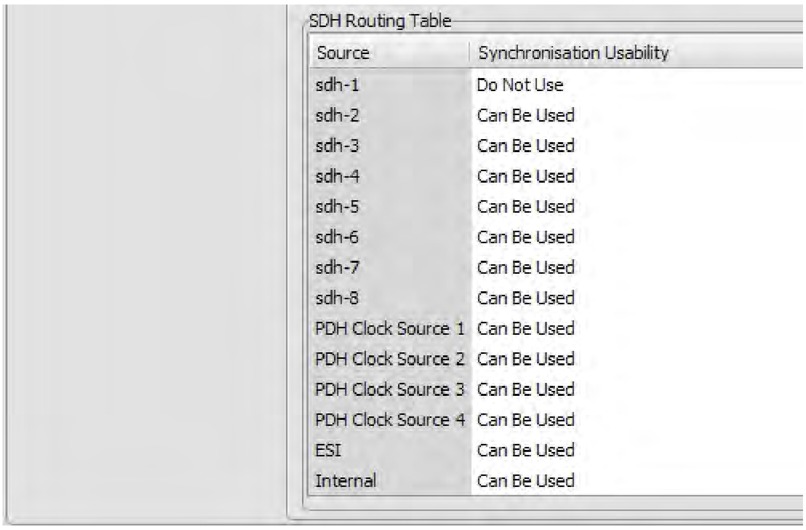


Table 133: AP: / unit-x / sdh / sdh-y, Configuration - MS

Operation Name	Parameter Name	Range	Description / Details
	SSM	<u>☑</u> ☐	Enable or disable the usage of the synchronization status message (SSM). The SSM is carried in the S1 byte of the MS overhead and contains signal quality information (QL 1-15), used for the timing source selection in the SETS. For further information please refer to [314] User Guide "TDM Services and Cross Connections in XMC20".
Signal Quality	Excessive Defect Threshold	<u>10E-3</u> … 10E-5	The bit error ratio threshold for the excessive signal defect is configurable. In the MS layer the error detection code evaluates the BIP-384 (STM-16), the BIP-96 (STM-4) or BIP-24 (STM-1) as a BIP-1. Please refer to section 7.3 Detection of Signal Defects (on page 153) for a description of the excessive signal defect evaluation.
	Degraded Defect Threshold	10E-5 … <u>10E-6</u> … 10E-8	The bit error ratio threshold for the degraded signal defect is configurable. In the MS layer the error detection code evaluates the BIP-384 (STM-16), the BIP-96 (STM-4) or BIP-24 (STM-1) as a BIP-1. Please refer to section 7.3 Detection of Signal Defects (on page 153) for a description of the degraded signal defect evaluation.
Input Mapping Table	Received QL	1 … 15	A received quality level in the range 1 to 15 can be adapted to any other QL which will then be used in the SETS and ESO selection process. Note that a lower QL means a higher clock quality.
	Adapted QL	1 … 15	

Table 133: AP: / unit-x / sdh / sdh-y, Configuration - MS (continued)

Operation Name	Parameter Name	Range	Description / Details
Output Mapping Table	Transmitted QL	1 … 15	A SETS internally used quality level in the range 1 to 15 can be adapted to any other QL which will then be used in the SSM of the corresponding transmit signal. Note that a lower QL means a higher clock quality. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20” for a description of the quality level handling.
	Adapted QL	1 … 15	
SDH Routing Table	Source	sdh-1	SETS timing source signal. These values are read-only.
		sdh-2	
		sdh-3	
		sdh-4	
		sdh-5	
		sdh-6	
		sdh-7	
		sdh-8	
		PDH Clock Source 1	
		PDH Clock Source 2	
		PDH Clock Source 3	
		PDH Clock Source 4	
		ESI	
		Internal	
	Synchronisation Usability	Can Be Used	A STM-16, STM-4 or STM-1 output signal transports the SETS timing. The signal transmitted onwards can be tagged as “Do not use” or “Can be used” in the SSM depending on its own active timing source. The default value for the own source is “Do Not Use”. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20” for a description of the quality level handling.
		Do Not Use	

8.15.3.3 AP: / unit-x / sdh / sdh-y, Configuration - MSP

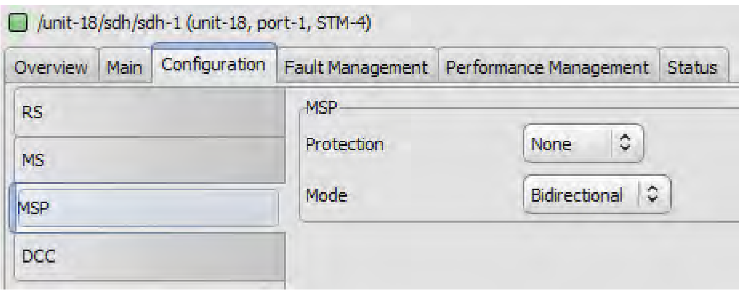


Table 134: AP: / unit-x / sdh / sdh-y, Configuration - MSP

Operation Name	Parameter Name	Range	Description / Details
MSP	Protection	<u>None</u> IntraCard InterCard	Enable or disable multiplex section protection. Note that the two SDH ports constituting an MSP pair must be configured to the same STM type (STM-16, STM-4 or STM-1). For further information please refer to section 5.8.1 Multiplex Section Protection (MSP) (on page 86)
	Mode	Unidirectional	On a failure in one direction of a working multiplex section, only the failed direction is switched to the protecting multiplex section. The protocol in the K1 and K2 bytes is not used.
		<u>Bidirectional</u>	On a failure in one direction of a working multiplex section, both directions are switched to the protecting multiplex section using the protocol in the K1 and K2 bytes of the protecting channel.

8.15.3.4 AP: / unit-x / sdh / sdh-y, Configuration - DCC

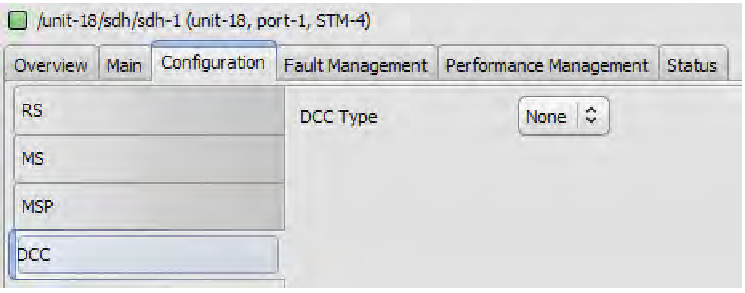


Table 135: AP: / unit-x / sdh / sdh-y, Configuration - DCC

Operation Name	Parameter Name	Range	Description / Details
DCC	DCC Type	None	Disable the usage of the RSOH and MSOH data communication channel (DCC). For further information please refer to section 5.6 Embedded Communication Channel (ECC) (on page 83)
		RSOH	Use the DCC in the regenerator section overhead: Bytes D1 to D3, 192 kbit/s.
		MSOH	Use the DCC in the multiplex section overhead: Bytes D4 to D12, 576 kbit/s.
		Both	Use the DCC in the regenerator and multiplex section overhead.

Please note:

The access to the RS and/or MS DCC requires PBUS resources.

→ As soon as one of the RS or MS DCC is configured the vc12-61 to vc12-64 resources are no longer available.

→ If one of the vc12-61 to vc12-64 resources has already a channel configured, no RS or MS DCC can be configured.

Please note:

In an MSP protected path the DCC is not protected.

→ The DCC configuration and cross connection must be done on the working and on the protecting section. The selection of the active section must be handled by the management communication network.

Please note:

A DCC cannot be used as a-End in a protected connection.

8.15.4 AP: / unit-x / sdh / sdh-y, Fault Management

For the a description of the general aspects of the

- "Fault Management - Status", and
- "Fault Management - Configuration"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22". The following table lists the fault causes of the current AP.

Table 136: AP: / unit-x / sdh / sdh-y, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
LOF	Loss Of Frame	Communication Alarm	☑	Major	Loss of frame of the optical or electrical input signal (STM-LOF).
TIM	Trace Identifier Mismatch	Communication Alarm	☑	Major	The received and accepted TTI does not match the expected RS TTI.
AIS	AIS Received	Communication Alarm	☑	Minor	Multiplex Section AIS received due to a failure in the received optical or electrical signal or in the RS layer.
EXC	Excessive Bit Error Rate	Communication Alarm	☑	Major	The bit error ratio is above the configured "Excessive Defect Threshold" for the logical SDH port.
DEG	Degraded Signal	Communication Alarm	☐	Major	The bit error ratio is above the configured "Degraded Defect Threshold" for the logical SDH port.
RDI	Remote Defect Indication	Communication Alarm	☐	Minor	Multiplex Section RDI received from the far end equipment. RDI is activated by one or more of the following defects: STM-LOS, STM-LOF, RS-TIM, MS-AIS
MSNDPF	MS Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 1728 or SES ≥ 22 or BBE ≥ 62'200 over a 24 hour interval at the near end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
MSNUPF	MS Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 114 or SES ≥ 10 or BBE ≥ 27'000 over a 15 min. interval at the near end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 4 and SES = 0 and BBE ≤ 1100. The alarm can be cleared by resetting the corresponding PM alarm counter.

Table 136: AP: / unit-x / sdh / sdh-y, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MSFDPF	MS Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 1728 or SES ≥ 22 or BBE ≥ 62’200 over a 24 hour interval at the far end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
MSFUPF	MS Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 114 or SES ≥ 10 or BBE ≥ 27’000 over a 15 min. interval at the far end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 4 and SES = 0 and BBE ≤ 1100. The alarm can be cleared by resetting the corresponding PM alarm counter.
MSPFOP	MSP Failure Of Protocol	Communication Alarm	☐	Warning	This alarm appears if the multiplex section protection protocol in the protecting channel fails, e.g. when the remote side is not configured to bidirectional mode.
MSPMFA	MSP Maintenance Function Active	Communication Alarm	☐	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. Manual switching request.

Please note:

The errored signal, degraded signal and performance alarm thresholds are the same for MS16, MS4 and MS1.

8.15.5 AP: / unit-x / sdh / sdh-y, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

The PM parameters are presented in different groups. The following counter groups are available for the NUSA1 logical SDH ports:

- “Unfiltered Events” group, see section 8.15.5.1 AP: / unit-x / sdh / sdh-y, Performance Management - Unfiltered Events (on page 269),
- “G.826” group, see section 8.15.5.2 AP: / unit-x / sdh / sdh-y, Performance Management - G.826 (on page 269).

The following counter intervals are available, depending of the counter group:

Table 137: PM counter interval availability

Counter interval	G.826	Unfiltered Events
User Counter	yes	yes
History 15min	yes	yes
History 24h	yes	yes
Alarm 15min	yes	no
Alarm 24h	yes	no

8.15.5.1 AP: / unit-x / sdh / sdh-y, Performance Management - Unfiltered Events

Table 138: PM group: Unfiltered Events

PM parameter	Description
Out Of Frame	Physical section out of frame event
Protection Switches	Multiplex section protection switchover event

Please note:

The “Out Of Frame” counter will be available in a future release.

8.15.5.2 AP: / unit-x / sdh / sdh-y, Performance Management - G.826

Table 139: PM group: G.826

PM parameter	Description
Near End BBE	Multiplex section near end background block errors.
Near End ES	Multiplex section near end errored second.
Near End SES	Multiplex section near end severely errored second.
Near End UAT	Multiplex section near end unavailable time.
Far End BBE	Multiplex section far end background block errors.
Far End ES	Multiplex section far end errored second.
Far End SES	Multiplex section far end severely errored second.
Far End UAT	Multiplex section far end unavailable time.
Path UAT	Multiplex section path unavailable time.

8.15.6 AP: / unit-x / sdh / sdh-y, Status

8.15.6.1 AP: / unit-x / sdh / sdh-y, Status - RS

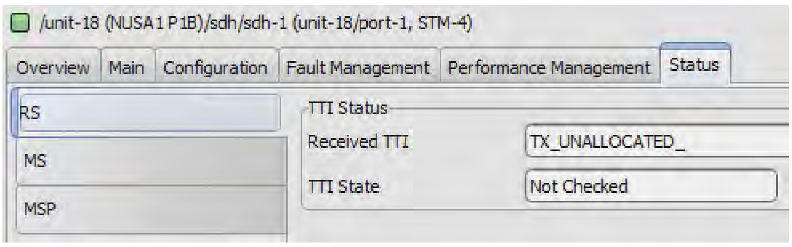


Table 140: AP: / unit-x / sdh / sdh-y, Status - RS

Operation Name	Parameter Name	Range	Description / Details
TTI Status	Received TTI	0 … 15 characters	Display of the received TTI in the J0 byte of the RS overhead.
	TTI State	OK	TTI supervision is enabled and the received TTI equals the expected TTI.
		Mismatch	TTI supervision is enabled and the received TTI is not equal to the expected TTI.
		Not Checked	TTI supervision is not enabled.

8.15.6.2 AP: / unit-x / sdh / sdh-y, Status - MS

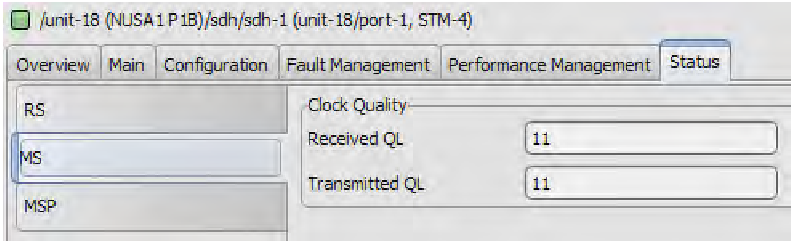
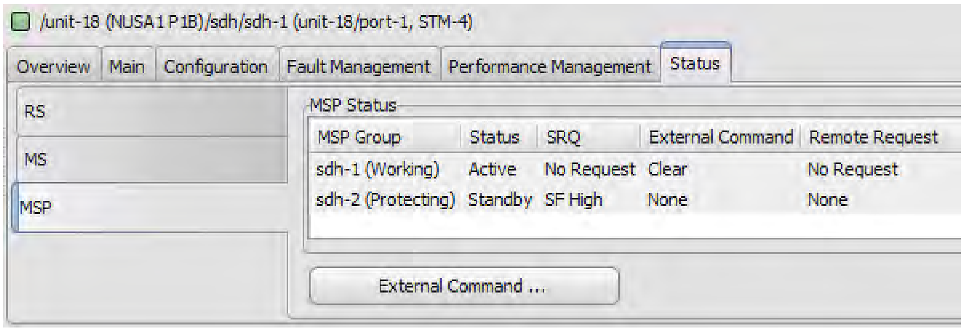


Table 141: AP: / unit-x / sdh / sdh-y, Status - MS

Operation Name	Parameter Name	Range	Description / Details
Clock Quality	Received QL	Unknown	The synchronization method “None” has been configured.
		Do Not Use	Received SSM value = 15.
		1 … 14	Display of the received SSM value < 15.
	Transmitted QL	Unknown	The SSM parameter has been disabled.
		Do Not Use	The “Do Not Use” quality level is transmitted as SSM value = 15.
		1 … 14	Display of the transmitted SSM value < 15.

8.15.6.3 AP: / unit-x / sdh / sdh-y, Status - MSP



“External Command” dialogue:

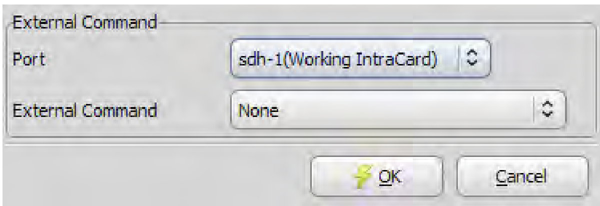


Table 142: AP: / unit-x / sdh / sdh-y, Status - MSP

Operation Name	Parameter Name	Range	Description / Details
MSP Status	MSP Group	0 … 30 characters	Display of the SDH ports belonging to the MSP group. Please refer to section 5.8.1 Multiplex Section Protection (MSP) (on page 86) for further information.
	Status	Active	Indication of the current port usage with respect to the STM-16, STM-4 or STM-1 traffic signal: - Active: The received SDH traffic is processed. - Standby: The received SDH traffic is not processed. The active port can be the working or the protecting channel.
		Standby	
		Not Available	MSP is not enabled.
	SRQ		SRQ are the signal requests. SRQ indicate the result of the receive signal monitoring. The states are:
		No Request	No request: No switching request (due to SF or SD) is pending for the port.
		SF High	A switching request due to SF (signal fail) is pending.
		SD High	A switching request due to SD (signal degraded) is pending.
		Not Available	MSP is not enabled.

Table 142: AP: / unit-x / sdh / sdh-y, Status - MSP (continued)

Operation Name	Parameter Name	Range	Description / Details
	External Command		External commands are the switching requests applied by the user via the ECST. The list below shows the external commands for MSP in the descending order of priority. Please note the restrictions on effectiveness for some of the commands:
		Clear	Clears all switching requests listed below.
		Lockout Of Protection (Protecting Only)	Protecting channel only. This command blocks all switching requests to switch the active channel from the working to the protecting channel.
		Forced Switch	Switches the active channel to the port where the command has been applied to, unless an equal or higher priority switch command is in effect. Since a forced switch has higher priority than SF or SD on the working channel, this command will be carried out regardless of the condition of the working channel. Note that an SF condition on the protecting channel has higher priority than a forced switch. Therefore it is not possible to switch from the working channel to the protecting channel if this channel has SF.
		Manual Switch	Switches the active channel to the port where the command has been applied to, unless an equal or higher priority switch command is in effect or an SF or SD condition exists on this channel. Since manual switch has lower priority than SF or SD on a working or protecting channel, this command will be carried out only if the channel is not in SF or SD condition.
		Exercise (Working Only)	Effective for the bidirectional MSP mode and working channel only. This command checks the responses of automatic protection switching (APS) bytes to a switch request, unless the protecting channel is in use. The switch is not actually completed for the traffic signal. The remote request will display a “Reverse Request”.
		None	No external request is issued. The external command status remains unchanged.

Table 142: AP: / unit-x / sdh / sdh-y, Status - MSP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Remote Request		The remote request indication is for the bidirectional MSP mode available only. In the bidirectional mode it is possible to indicate locally the requests issued by the remote interface. This information is transmitted via the K1/K2 bytes in the SOH.
		Lockout Of Protection	
		Forced Switch	
		Signal Fail High Priority	
		Signal Fail Low Priority	
		Signal Degrade High Priority	
		Signal Degrade Low Priority	
		Manual Switch	
		Wait To Restore	
		Exercise	
		Reverse Request	
		Do Not Revert	
		No Request	
		None	
External Command …			Open the ECST dialogue to apply an external command to a port of the MSP group.
External Command	Port	port-x (Working Intracard) or port-x (Working Intercard)	Select the port where the external command will be applied to.
		port-x (Protecting Intracard) or port-x (Protecting Intercard)	
	External Command	None	For the description refer to the External command status above.
		Clear	
		Forced Switch	
		Manual Switch	
		Exercise (Working Only)	
		Lockout Of Protection (Protecting Only)	

Please note:

The MSP status is available only on the working logical SDH ports.

Please note:

MSP with NUSA1 provides non revertive protection switching, i.e. if after a protection switching to the protecting channel the working channel is operational again, there is no automatic switching back to the working channel.

→ The switching back must be ordered by an external command (manual switch or forced switch).

8.16 AP: / unit-x / sdh / sdh-y / dccm and dccr, y = 1 … 8

The following management functions are related to the access points dccm and dccr, but the screenshots shown are only taken from the dccm access point.

The dccm is the access point for the multiplex section overhead (MSOH) DCC. The dccr is the access point for the regenerator section overhead (RSOH) DCC.

The sdh-5 to sdh-8 access points are only available within an EQP group.

8.16.1 AP: / unit-x / sdh / sdh-y / dccm and dccr, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - CTP”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.16.2 AP: / unit-x / sdh / sdh-y / dccm and dccr, Main

8.16.2.1 AP: / unit-x / sdh / sdh-y / dccm and dccr, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.16.2.2 AP: / unit-x / sdh / sdh-y / dccm and dccr, Main - Admin And Oper Status

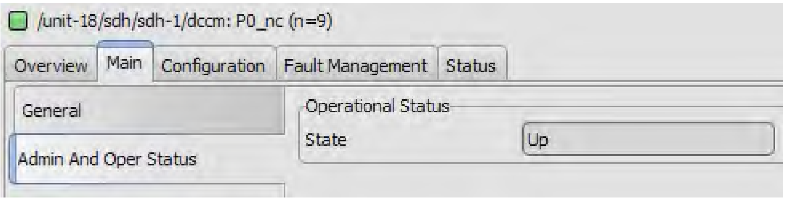


Table 143: AP: / unit-x / sdh / sdh-y / dccm and dccr, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the DCC signal. The operational state is up when the logical SDH port administrative state is up.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.16.3 AP: / unit-x / sdh / sdh-y / dccm and dccr, Configuration

8.16.3.1 AP: / unit-x / sdh / sdh-y / dccm and dccr, Configuration - CTP

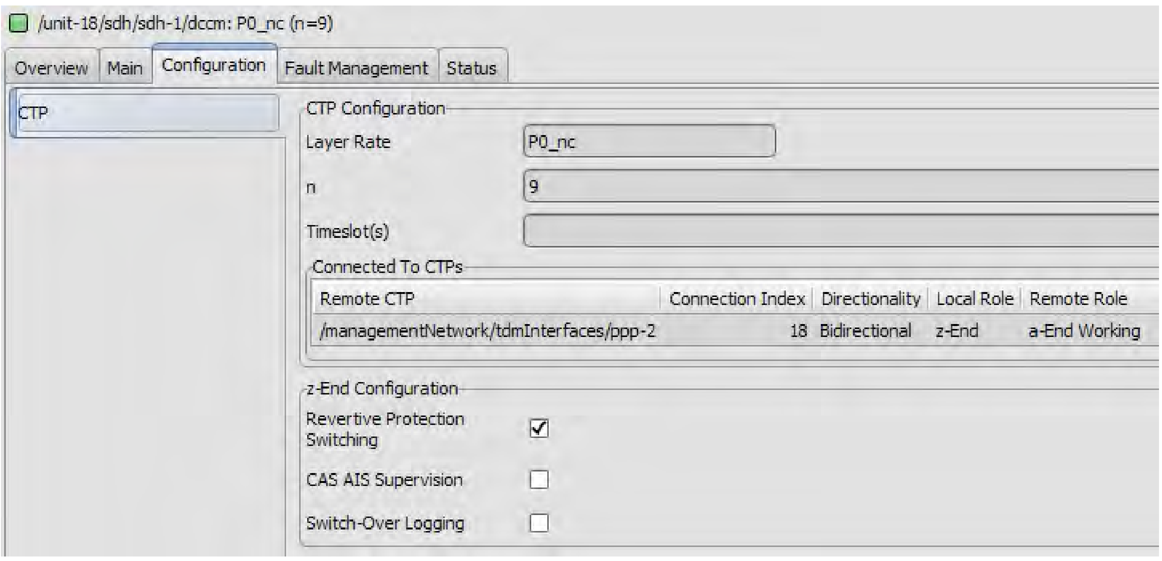


Table 144: AP: / unit-x / sdh / sdh-y / dccm and dccr, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	P0_nc	The layer rate of the connection termination point is P0_nc.
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a RSOH DCC is 3, the number of time slots of a MSOH DCC is 9.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a DCC is not applicable.
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the DCC. Without a connection the parameter is empty

Table 144: AP: / unit-x / sdh / sdh-y / dccm and dccr, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The DCC is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The DCC is the working starting point of a protected or unprotected connection.
		a-End Protecting	The DCC is the protecting starting point of a protected connection.
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End. Non revertive protection switching will be available in a future release.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is not applicable with a DCC.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

8.16.4 AP: / unit-x / sdh / sdh-y / dccm and dccr, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 145: AP: / unit-x / sdh / sdh-y / dccm and dccr, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status function has been done. E.g. external switch request.

8.16.5 AP: / unit-x / sdh / sdh-y / dccm and dccr, Status

8.16.5.1 AP: / unit-x / sdh / sdh-y / dccm and dccr, Status - CTP

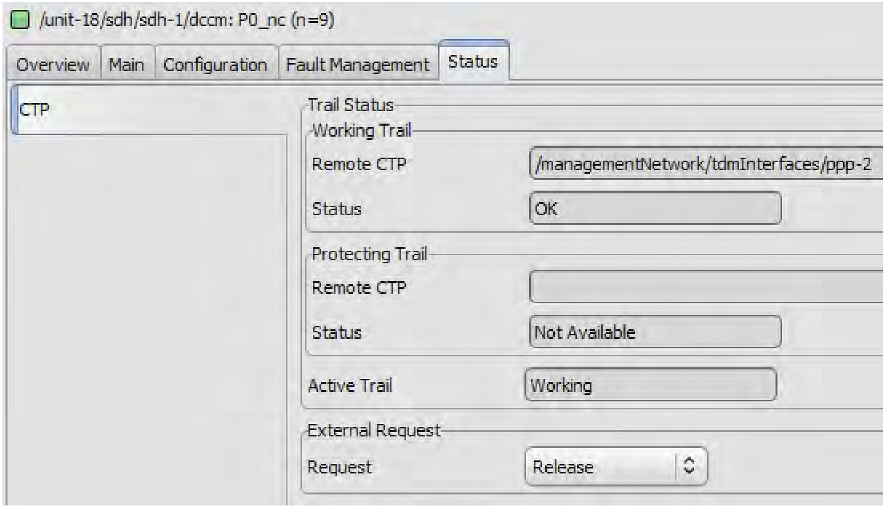


Table 146: AP: / unit-x / sdh / sdh-y / dccm and dccr, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the DCC signal is connected to, e.g. /unit-10/port-3/chan-1.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the DCC signal is connected to, e.g. /unit-10/port-2/chan-1.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.

Table 146: AP: / unit-x / sdh / sdh-y / dccm and dccr, Status - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.17 AP: / unit-x / sdh / sdh-y / j-z, y = 1 … 8

The sdh-5 to sdh-8 access points are only available within an EQP group.

z = 1 … 16 for STM-16 ports.

z = 1 … 4 for STM-4 ports.

z = 1 for STM-1 ports.

8.17.1 AP: / unit-x / sdh / sdh-y / j-z, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - CTP”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.17.2 AP: / unit-x / sdh / sdh-y / j-z, Main

8.17.2.1 AP: / unit-x / sdh / sdh-y / j-z, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.17.2.2 AP: / unit-x / sdh / sdh-y / j-z, Main - Admin And Oper Status

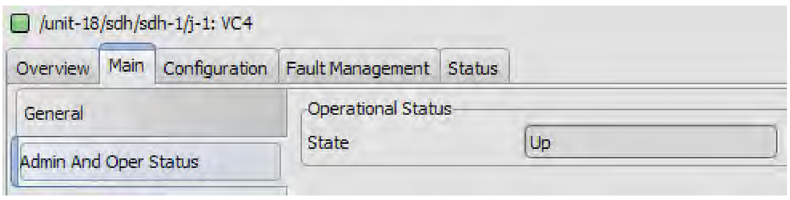


Table 147: AP: / unit-x / sdh / sdh-y / j-z, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the AU-4 signal. The operational state is up when the port administrative state is up and a sink connection to another VC-4 resource is configured and no major defect is active.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.17.3 AP: / unit-x / sdh / sdh-y / j-z, Configuration

8.17.3.1 AP: / unit-x / sdh / sdh-y / j-z, Configuration - CTP

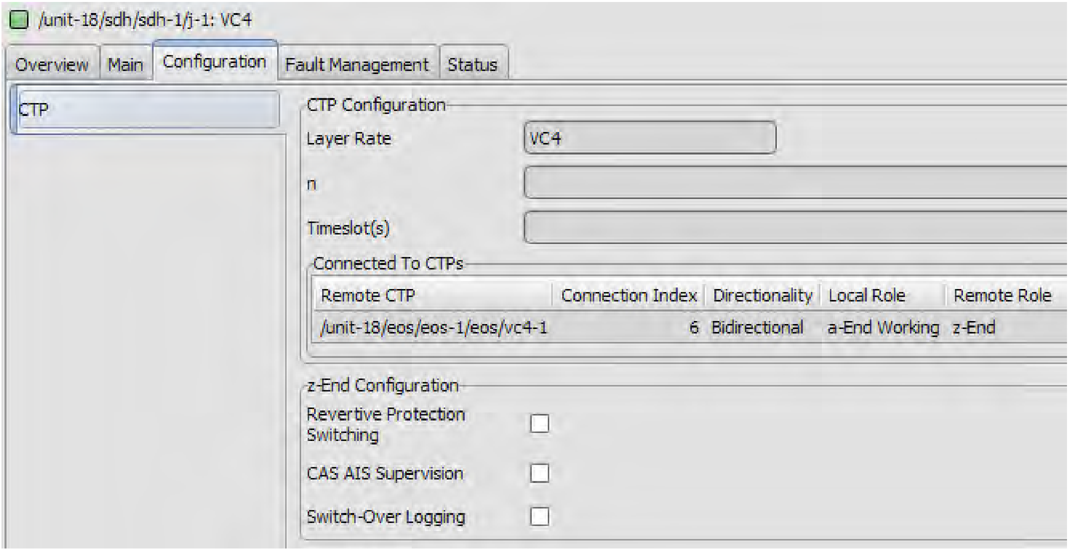


Table 148: AP: / unit-x / sdh / sdh-y / j-z, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	VC4	The layer rate of the connection termination point is VC-4.
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a VC-4 is not applicable.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a VC-4 is not applicable.
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the VC-4. Without a connection the parameter is empty
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The VC-4 is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The VC-4 is the working starting point of a protected or unprotected connection.
		a-End Protecting	The VC-4 is the protecting starting point of a protected connection.

Table 148: AP: / unit-x / sdh / sdh-y / j-z, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide "TDM Services and Cross Connections in XMC20"
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is not applicable with VC-4.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

8.17.4 AP: / unit-x / sdh / sdh-y / j-z, Fault Management

For the a description of the general aspects of the

- "Fault Management - Status", and
- "Fault Management - Configuration"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22". The following table lists the fault causes of the current AP.

Table 149: AP: / unit-x / sdh / sdh-y / j-z, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status function has been done. E.g. external switch request.

8.17.5 AP: / unit-x / sdh / sdh-y / j-z, Status

8.17.5.1 AP: / unit-x / sdh / sdh-y / j-z, Status - CTP

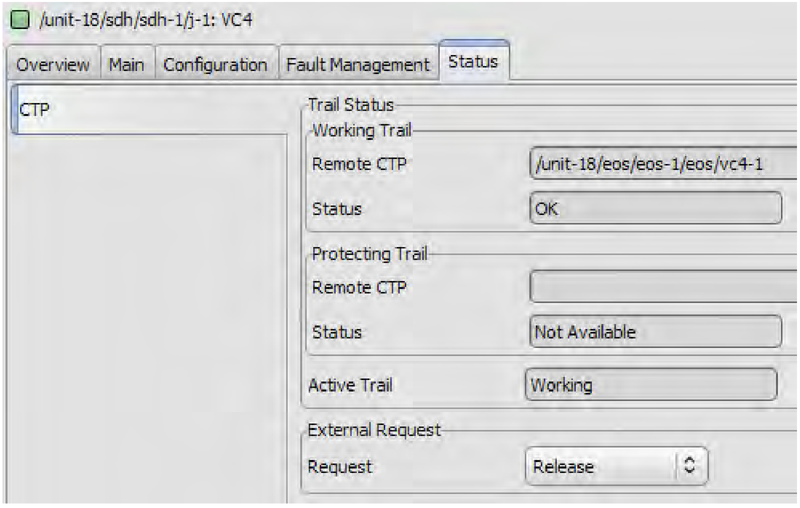


Table 150: AP: / unit-x / sdh / sdh-y / j-z, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-4 signal is connected to, e.g. /unit-18/sdh/sdh-3/j-1.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-4 signal is connected to, e.g. /unit-18/sdh/sdh-2/j-1.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.

Table 150: AP: / unit-x / sdh / sdh-y / j-z, Status - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.18 AP: / unit-x / vc4

8.18.1 AP: / unit-x / vc4, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”,
- “Overview - VC4 Overview”, and
- “Overview - VC4 TUG Allocation”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

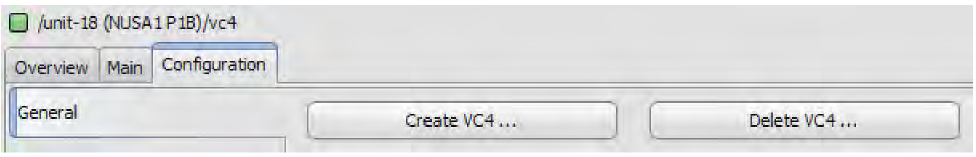
8.18.2 AP: / unit-x / vc4, Main

For a description of the
- “Main - General”

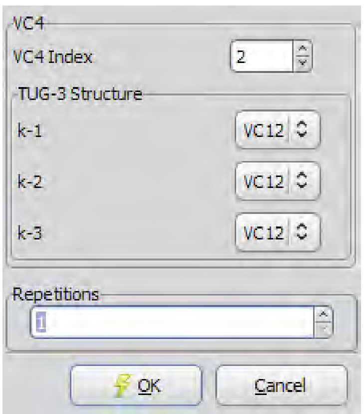
management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.18.3 AP: / unit-x / vc4, Configuration

8.18.3.1 AP: / unit-x / vc4, Configuration - General



“Create VC4” dialogue:



“Delete VC4” dialogue:

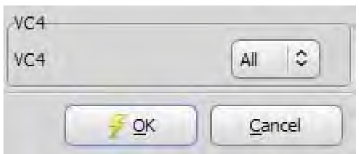


Table 151: AP: / unit-x / vc4, Configuration - General

Operation Name	Parameter Name	Range	Description / Details
Create VC4 …			Open the ECST dialogue to create an additional VC-4 resource with a TUG-3 structure
VC4	VC4 Index	0 … 31	Enter the index number of the new member to be created. 0 is a reserved value used for the auto-assignment of a VC-4 index: The auto-assigned index is the highest existing index number + 1. In the ECST the default value is the autoassigned index number.
	TUG-3 Structure, k-1	VC3	Structure of the first TUG-3.
		VC12	
	TUG-3 Structure, k-2	VC3	Structure of the second TUG-3.
		VC12	
	TUG-3 Structure, k-3	VC3	Structure of the third TUG-3.
		VC12	
Repetitions		1 … 100	Number of VC-4 resources to be created.
Delete VC4 …			Open the ECST dialogue to delete a VC-4 resource.
VC4	VC4	All	Select the VC-4 name to be deleted.
		vc4-1 … vc4-31	

8.19 AP: / unit-x / vc4 / vc4-b

8.19.1 AP: / unit-x / vc4 / vc4-b, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”,
- “Overview - CTP”, and
- “Overview - VC4 TUG Allocation”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.19.2 AP: / unit-x / vc4 / vc4-b, Main

8.19.2.1 AP: / unit-x / vc4 / vc4-b, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.19.2.2 AP: / unit-x / vc4 / vc4-b, Main - Admin And Oper Status

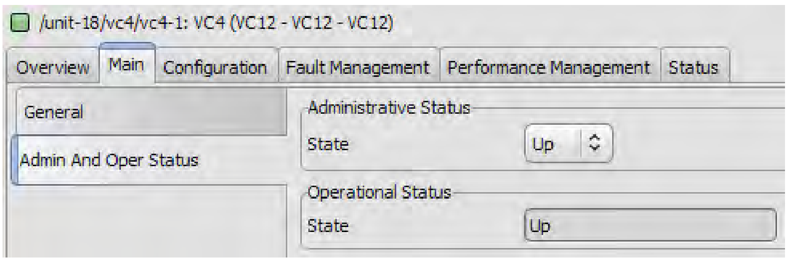


Table 152: AP: / unit-x / port-y, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Administrative Status	State	Up	Set the IETF administrative status of the VC-4. Unused VC-4 (without cross connection) should be set to the down state, so that they do not generate alarms (i.e. unequipped).
		<u>Down</u>	
Operational Status	State	Up	Display of the IETF operational status of the VC-4.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.19.3 AP: / unit-x / vc4 / vc4-b, Configuration

8.19.3.1 AP: / unit-x / vc4 / vc4-b, Configuration - General

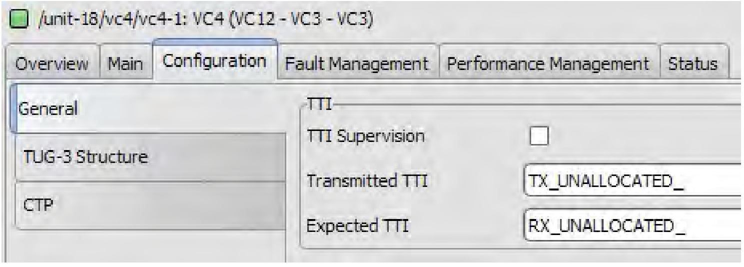


Table 153: AP: / unit-x / vc4 / vc4-b, Configuration - General

Operation Name	Parameter Name	Range	Description / Details
TTI	TTI Supervision	☑ ☐	The trail trace identifier (TTI) supervision can be enabled or disabled. In the disabled mode no check is done on the received TTI and no alarm is generated. For further information please refer to section 7.4 Trail Trace Identifier (TTI) (on page 154)
	Transmitted TTI	15 characters	TTI transmitted in the VC-4 path overhead (J1 byte). The default string is TX_UNALLOCATED_. In the disabled mode the transmit TTI string is TX_UNAL-LOCATED_ or any other configured TTI. A TTI shorter than 15 characters is automatically completed with SPACE characters.
	Expected TTI	15 characters	TTI expected in the VC-4 path overhead. The default string is RX_UNALLOCATED_. In the disabled mode the expected TTI string is RX_UNAL-LOCATED_ or any other configured TTI. A TTI shorter than 15 characters is automatically completed with SPACE characters.

8.19.3.2 AP: / unit-x / vc4 / vc4-b, Configuration - TUG-3 Structure

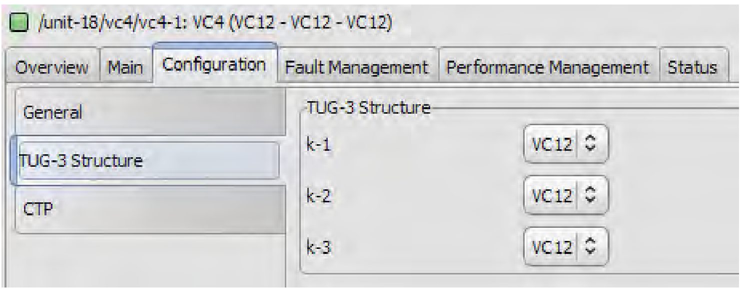


Table 154: AP: / unit-x / vc4 / vc4-b, Configuration - TUG-3 Structure

Operation Name	Parameter Name	Range	Description / Details
TUG-3 Structure	k-1	VC3	Structure of the first TUG-3.
		VC12	
	k-2	VC3	Structure of the second TUG-3.
		VC12	
	k-3	VC3	Structure of the third TUG-3.
		VC12	

Please note:

Changing the structure of a TUG-3 will delete all existing managed objects (MO) of this TUG-3 and create the MOs according to the new TUG-3 structure.

8.19.3.3 AP: / unit-x / vc4 / vc4-b, Configuration - CTP

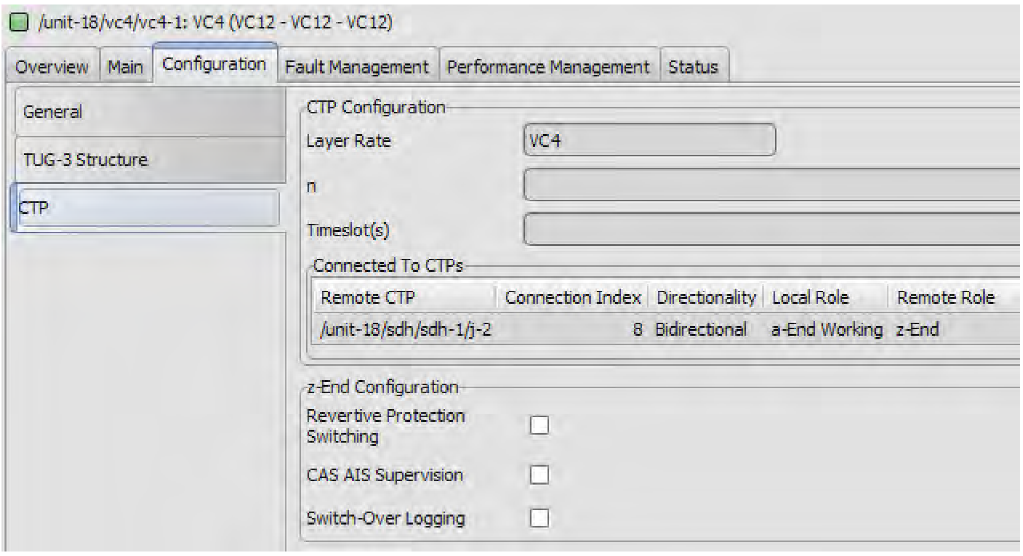


Table 155: AP: / unit-x / vc4 / vc4-b, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	VC4	The layer rate of this connection termination point is fixed.
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a VC-4 is not applicable.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a VC-4 is not applicable.
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the VC-4. Without a connection the parameter is empty

Table 155: AP: / unit-x / vc4 / vc4-b, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The VC-4 is the ending point of a connection. Please refer to [314] User Guide "TDM Services and Cross Connections in XMC20"
		a-End Working	The VC-4 is the working starting point of a protected or unprotected connection.
		a-End Protecting	The VC-4 is the protecting starting point of a protected connection.
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide "TDM Services and Cross Connections in XMC20"
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is not applicable with VC-4.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

Please note:

The z-End of a protected connection shows two entries in the "Connected to CTPs" table, one for the working and one for the protecting path.

8.19.4 AP: / unit-x / vc4 / vc4-b, Fault Management

For the a description of the general aspects of the

- "Fault Management - Status", and
- "Fault Management - Configuration"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22". The following table lists the fault causes of the current AP.

Table 156: AP: / unit-x / vc4 / vc4-b, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
AIS	AIS Received	Communication Alarm	☑	Minor	Failure in the received optical or electrical signal, in the RS or MS layer (AU-4-AIS).

Table 156: AP: / unit-x / vc4 / vc4-b, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
LOM	Loss Of Multiframe	Communication Alarm	☑	Major	Loss of the multi-frame alignment on the incoming VC-4 signal (VC-4-LOM). Applicable only with VC-12 tributary signals.
LOP	Loss Of Pointer	Communication Alarm	☑	Major	Eight consecutive invalid AU-4 pointer values have been received (AU-4-LOP)
PLM	Payload Mismatch	Communication Alarm	☑	Major	The received and accepted trail signal label does not indicate the expected “TUG Structure” in the VC-4 (VC-4-PLM).
RDI	Remote Defect Indication	Communication Alarm	☐	Minor	The far end equipment has one or more of the following defects: AU-4-LOP, AU-4-AIS, VC-4-UNEQ, VC-4-TIM.
TIM	Trace Identifier Mismatch	Communication Alarm	☑	Major	The received and accepted TTI does not match the expected VC-4 TTI (VC-4-TIM).
EXC	Excessive Bit Error Rate	Communication Alarm	☑	Major	The bit error ratio is above the configured “Errored Signal” threshold for the VC-4.
DEG	Degraded Signal	Communication Alarm	☐	Major	The bit error ratio is above the configured “Errored Signal” threshold for the VC-4.
UNEQ	Unequipped	Communication Alarm	☑	Major	The received and accepted trail signal label is the unequipped indication (VC-4-UNEQ).
NDPF	Near End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 2’592 or SES ≥ 33 or BBE ≥ 12’960 over a 24 hour interval at the near end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.
NUPF	Near End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 180 or SES ≥ 15 or BBE ≥ 1100 over a 15 min. interval at the near end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 4 and SES = 0 and BBE ≤ 50. The alarm can be cleared by resetting the corresponding PM alarm counter.
FDPF	Far End Degraded Performance	Communication Alarm	☐	Warning	ES ≥ 2’592 or SES ≥ 33 or BBE ≥ 12’960 over a 24 hour interval at the far end input signal. The alarm status is reset after a 24 hour interval with ES = 0 and SES = 0. The alarm can be cleared by resetting the corresponding PM alarm counter.

Table 156: AP: / unit-x / vc4 / vc4-b, Fault Management (continued)

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
FUPF	Far End Unacceptable Performance	Communication Alarm	☐	Warning	ES ≥ 180 or SES ≥ 15 or BBE ≥ 1100 over a 15 min. interval at the far end input signal. The alarm status is reset after a 15 min. interval with ES ≤ 4 and SES = 0 and BBE ≤ 50. The alarm can be cleared by resetting the corresponding PM alarm counter.
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status/maintenance function has been done. E.g. applying a loop.
TSF	Trail Signal Failure	Communication Alarm	☑	Major	For unprotected connections: Signal failure on the working VC-4 subnetwork connection. For protected connections: Signal failure on the working **and** protecting VC-4 subnetwork connection. Alarm activation criteria: AU-4-LOP, AU-4-AIS, VC-4-UNEQ or VC-4-TIM. Note that this alarm is not monitored by default.
RTSF	Redundant Trail Signal Failure	Communication Alarm	☑	Minor	For unprotected connections: Alarm not available. For protected connections: Signal failure on the working **or** protecting VC-4 subnetwork connection. Alarm activation criteria: AU-4-LOP, AU-4-AIS, VC-4-UNEQ or VC-4-TIM. Note that this alarm is not monitored by default.

Please note:

The monitoring of the TSF and RTSF alarms is disabled by default.

8.19.5 AP: / unit-x / vc4 / vc4-b, Performance Management

For the a description of the general aspects of the performance management (PM) functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

The PM parameters are presented in different groups. The following counter group is available for the NUSA1 VC-4 resources:

- “G.826” group, see section 8.19.5.1 AP: / unit-x / vc4 / vc4-b, Performance Management - G.826 (on page 292).

The following counter intervals are available:

Table 157: PM counter interval availability

Counter interval	G.826
User Counter	yes
History 15min	yes
History 24h	yes

Table 157: PM counter interval availability (continued)

Counter interval	G.826
Alarm 15min	yes
Alarm 24h	yes

8.19.5.1 AP: / unit-x / vc4 / vc4-b, Performance Management - G.826

Table 158: PM group: G.826

PM parameter	Description
Near End BBE	VC near end background block errors.
Near End ES	VC near end errored second.
Near End SES	VC near end severely errored second.
Near End UAT	VC near end unavailable time.
Far End BBE	VC far end background block errors.
Far End ES	VC far end errored second.
Far End SES	VC far end severely errored second.
Far End UAT	VC far end unavailable time.
Path UAT	VC path unavailable time.

8.19.6 AP: / unit-x / vc4 / vc4-b, Status

8.19.6.1 AP: / unit-x / vc4 / vc4-b, Status - General

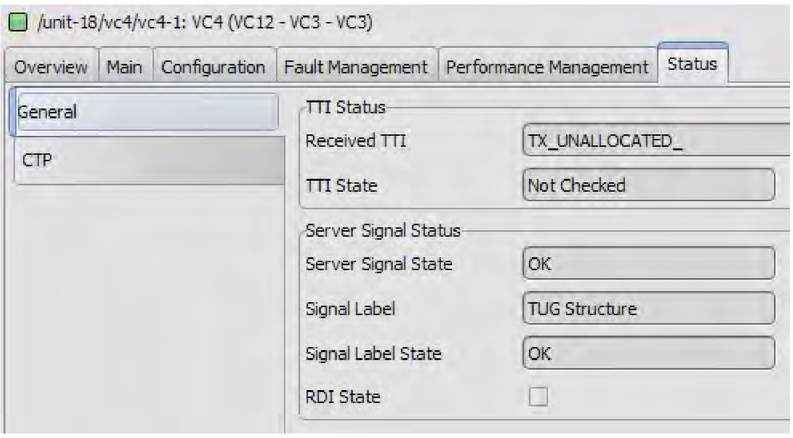


Table 159: AP: / unit-x / vc4 / vc4-b, Status - General

Operation Name	Parameter Name	Range	Description / Details
TTI Status	Received TTI	0 … 15 characters	Display of the received TTI in the J1 byte of the VC-4 path overhead.
	TTI State	OK	TTI supervision is enabled and the received TTI equals the expected TTI.
		Mismatch	TTI supervision is enabled and the received TTI is not equal to the expected TTI.
		Not Checked	TTI supervision is not enabled.

Table 159: AP: / unit-x / vc4 / vc4-b, Status - General (continued)

Operation Name	Parameter Name	Range	Description / Details
Server Signal Status	Server Signal State	OK	Failure indication of the VC-4 server signal, i.e. the AU-4 signal.
		AU-AIS	
		AU-LOP	
	Signal Label	TUG Structure	The VC-4 layer is able to transport a variety of client signals applied to the layer via different adaptation functions. The information about the signal type is carried in the (trail) signal label, transported in the C2 byte of the VC-4 path overhead. NUSA1 inserts the signal label “TUG Structure” for all VC-4 signals with tributaries from the TU-3 / TU-12 cross connect, i.e. VC-3 and VC-12 signals from the PBUS or from the Ethernet ports
		Unequipped	
		<Any other signal label>	
	Signal Label State	OK	The received signal label equals the expected signal label, i.e. “TUG-Structure”.
		Mismatch	The received signal label is not equal to the expected signal label.
		Not Checked	The VC-4 is not used for transport, i.e. no cross connections have been configured.
	RDI State	☑	The VC-4 path remote defect indication (RDI) displays the received RDI state which is sent back from the far end termination function, if either an AU-4 server signal failure or a trail signal failure is being detected. RDI is transported in the G1 byte of the VC-4 path overhead. It can be “true” or “false”. Note that the VC signal status is not filtered. E.g. a TTI mismatch in the RS layer inserts an AIS as a consequent action. All subsequent failures are also displayed: Signal label mismatch. Note that these states are not visible in the alarm list since the alarms are filtered.
		☐	

8.19.6.2 AP: / unit-x / vc4 / vc4-b, Status - CTP

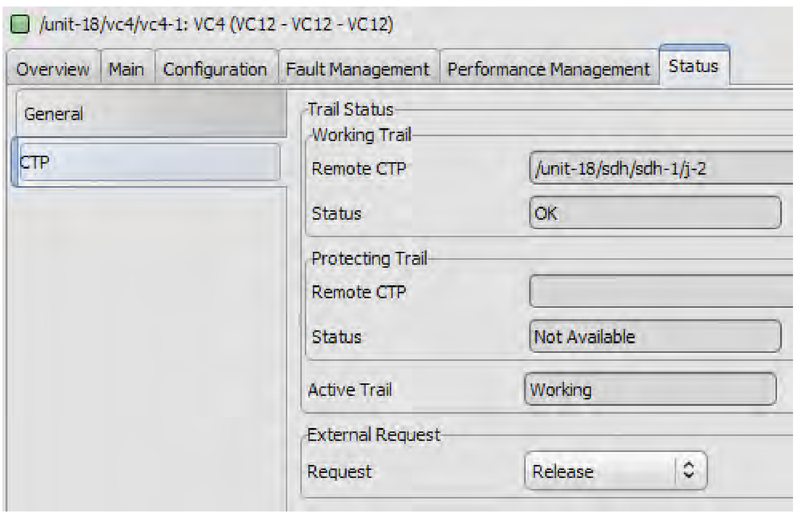


Table 160: AP: / unit-x / vc4 / vc4-b, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-4signal is connected to, e.g. /unit-18/sdh/sdh-1/j-1.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-4 signal is connected to, e.g. /unit-18/sdh/sdh-2/j-1.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.20 AP: / unit-x / vc4 / vc4-b / klm-n00

8.20.1 AP: / unit-x / vc4 / vc4-b / klm-n00, Overview

For a description of the
- "Overview - Alarms",
- "Overview - Cross Connections", and
- "Overview - CTP"

management functions, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.20.2 AP: / unit-x / vc4 / vc4-b / klm-n00, Main

8.20.2.1 AP: / unit-x / vc4 / vc4-b / klm-n00, Main - General

For a description of the
- "Main - General"

management function, please refer to [302] User Guide "XMC25/XMC23/XMC22".

8.20.2.2 AP: / unit-x / vc4 / vc4-b / klm-n00, Main - Admin And Oper Status

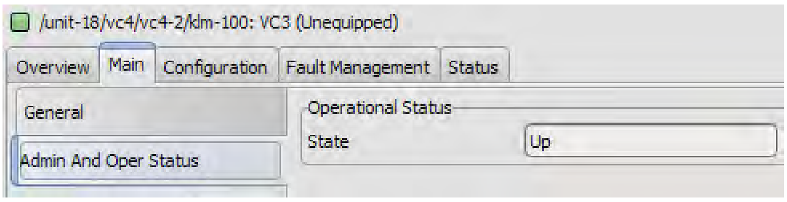


Table 161: AP: / unit-x / vc4 / vc4-b / klm-n00, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the VC-3. The operational state is up when the administrative state of the VC-4 is up and a sink connection to another VC-3 resource is configured.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.20.3 AP: / unit-x / vc4 / vc4-b / klm-n00, Configuration

8.20.3.1 AP: / unit-x / vc4 / vc4-b / klm-n00, Configuration - CTP

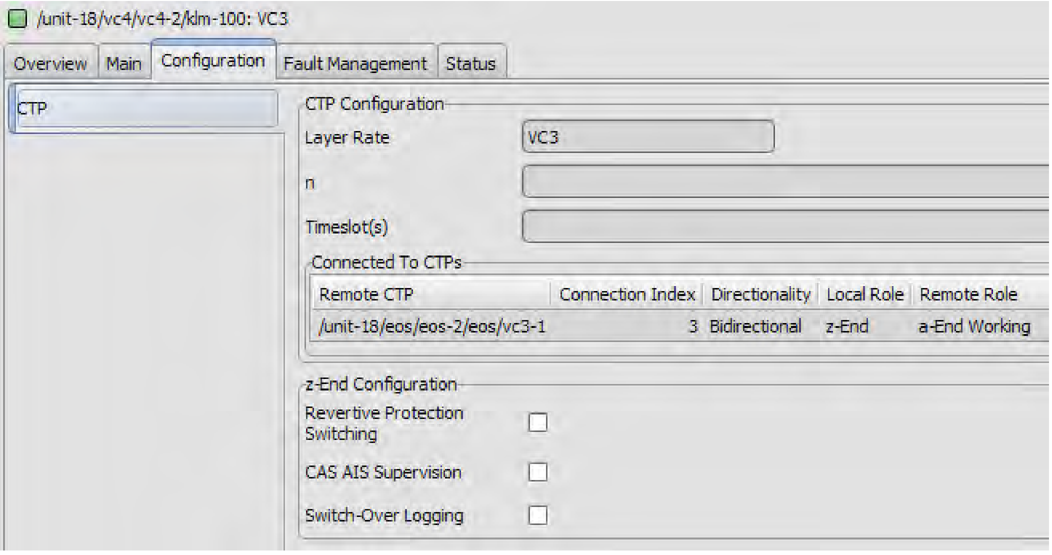


Table 162: AP: / unit-x / vc4 / vc4-b / klm-n00, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	VC3	The layer rate of the connection termination point is fixed according to the TUG-3 structure configuration.
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a VC-3 is not applicable.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a VC-3 is not applicable.
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the VC-3. Without a connection the parameter is empty
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The VC-3 is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The VC-3 is the working starting point of a protected or unprotected connection.
		a-End Protecting	The VC-3 is the protecting starting point of a protected connection.

Table 162: AP: / unit-x / vc4 / vc4-b / klm-n00, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is not applicable with VC-3.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

Please note:

The z-End of a protected connection shows two entries in the “Connected to CTPs” table, one for the working and one for the protecting path.

8.20.4 AP: / unit-x / vc4 / vc4-b / klm-n00, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 163: AP: / unit-x / vc4 / vc4-b / klm-n00, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status function has been done. E.g. external switch request.

8.20.5 AP: / unit-x / vc4 / vc4-b / klm-n00, Status

8.20.5.1 AP: / unit-x / vc4 / vc4-b / klm-n00, Status - CTP

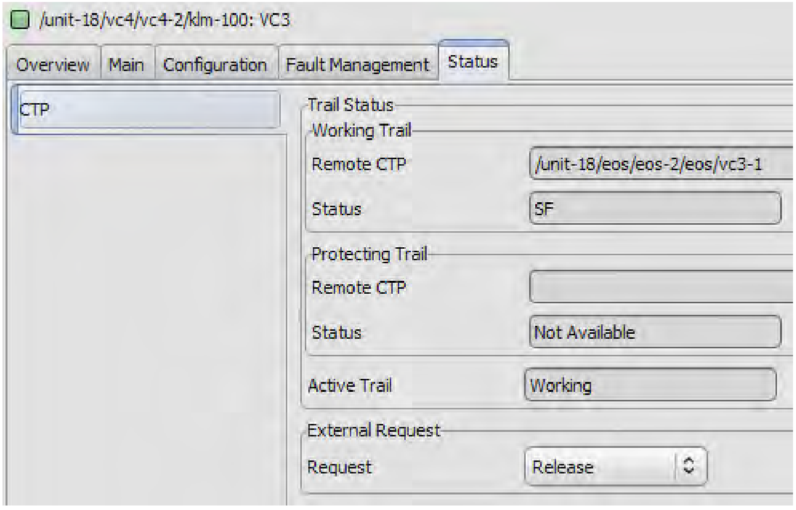


Table 164: AP: / unit-x / vc4 / vc4-b / klm-n00, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-3 is connected to, e.g. /unit-20/vc4/vc4-1/klm-300.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-3 signal is connected to, e.g. /unit-20/vc4/vc4-2/klm-200.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.

Table 164: AP: / unit-x / vc4 / vc4-b / klm-n00, Status - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.21 AP: / unit-x / vc4 / vc4-b / klm-npq

8.21.1 AP: / unit-x / vc4 / vc4-b / klm-npq, Overview

For a description of the
- “Overview - Alarms”,
- “Overview - Cross Connections”, and
- “Overview - CTP”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.21.2 AP: / unit-x / vc4 / vc4-b / klm-npq, Main

8.21.2.1 AP: / unit-x / vc4 / vc4-b / klm-npq, Main - General

For a description of the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.21.2.2 AP: / unit-x / vc4 / vc4-b / klm-npq, Main - Admin And Oper Status

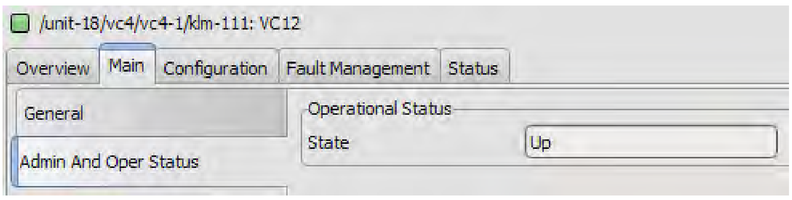


Table 165: AP: / unit-x / vc4 / vc4-b / klm-npq, Main - Admin And Oper Status

Operation Name	Parameter Name	Range	Description / Details
Operational Status	State	Up	Display of the IETF operational status of the VC-12. The operational state is up when the administrative state of the VC-4 is up and a sink connection to another VC-12 resource is configured.
		Down	
		Testing	
		Unknown	
		Dormant	
		Not Present	
		Lower Layer Down	

8.21.3 AP: / unit-x / vc4 / vc4-b / klm-npq, Configuration

8.21.3.1 AP: / unit-x / vc4 / vc4-b / klm-npq, Configuration - CTP

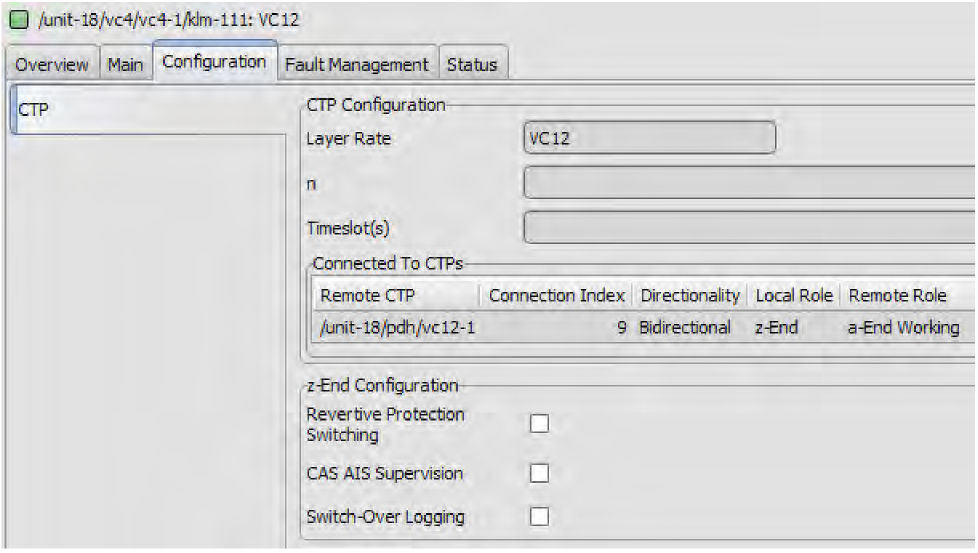


Table 166: AP: / unit-x / vc4 / vc4-b / klm-npq, Configuration - CTP

Operation Name	Parameter Name	Range	Description / Details
CTP Configuration	Layer Rate	VC12	The layer rate of the connection termination point is fixed according to the TUG-3 structure configuration.
	n	0 … 2 characters	Number of timeslots in case of P0_nc. The possible range is from 1 to 32. The number of time slots of a VC-12 is not applicable.
	Timeslot(s)	0 … 64 characters	Used timeslots in a structured P12 signal in case of P0_nc, e.g. 1 … 31. The timeslot(s) property of a VC-12 is not applicable.
Connected to CTPs	Remote CTP	<MO address>	Address string of a connections remote end. Without a connection the parameter is empty
	Connection Index	0 … 65“535	Index of a connection assigned to the VC-12. Without a connection the parameter is empty
	Directionality	Bidirectional	Directionality of the connection.
		Unidirectional	
	Local Role	z-End	The VC-12 is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The VC-12 is the working starting point of a protected or unprotected connection.
		a-End Protecting	The VC-12 is the protecting starting point of a protected connection.

Table 166: AP: / unit-x / vc4 / vc4-b / klm-npq, Configuration - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
	Remote Role	z-End	The CTP at the connections remote end is the ending point of a connection. Please refer to [314] User Guide “TDM Services and Cross Connections in XMC20”
		a-End Working	The CTP at the connections remote end is the working starting point of a protected or unprotected connection.
		a-End Protecting	The CTP at the connections remote end is the protecting starting point of a protected connection.
z-End Configuration	Revertive Protection Switching	☑	Enable revertive protection switching. The z-End will preferably select the working a-End.
		☐	
	CAS AIS Supervision	☑	Use CAS AIS as protection switching criterion. CAS AIS supervision is not applicable with VC-12.
		☐	
	Switch-Over Logging	☑	Enable the logging of the protection switch-over events.
		☐	

Please note:

The z-End of a protected connection shows two entries in the “Connected to CTPs” table, one for the working and one for the protecting path.

8.21.4 AP: / unit-x / vc4 / vc4-b / klm-npq, Fault Management

For the a description of the general aspects of the

- “Fault Management - Status”, and
- “Fault Management - Configuration”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”. The following table lists the fault causes of the current AP.

Table 167: AP: / unit-x / vc4 / vc4-b / klm-npq, Fault Management

ID	Fault Cause	Event Type	Traffic Affecting	Default Severity	Description
MFA	Maintenance Function Active	Communication Alarm	☑	Warning	This alarm appears if a manual change in the status function has been done. E.g. external switch request.

8.21.5 AP: / unit-x / vc4 / vc4-b / klm-npq, Status

8.21.5.1 AP: / unit-x / vc4 / vc4-b / klm-npq, Status - CTP

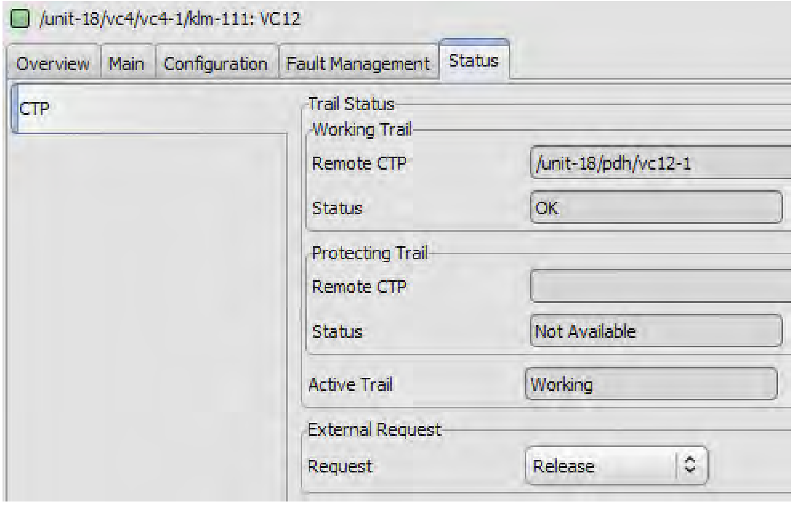


Table 168: AP: / unit-x / vc4 / vc4-b / klm-npq, Status - CTP

Operation Name	Parameter Name	Range	Description / Details
Trail Status	Working Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-12 signal is connected to, e.g. /unit-20/vc4/vc4-1/klm-121.
	Working Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Protecting Trail, Remote CTP	<MO Address>	Managed object address of the CTP (connection termination point) where the VC-12 signal is connected to, e.g. /unit-20/vc4/vc4-2/klm-321.
	Protecting Trail, Status	OK	No failure on the received signal.
		SF	Signal Fail status on the received signal.
		SD	Signal Degraded status on the received signal.
		Not Available	The status of the received signal is not available, e.g. when the CTPs role is a-End in a unidirectional connection.
	Active Trail	Working	The trail from the a-End working remote CTP has been selected.
		Protecting	The trail from the a-End protecting remote CTP has been selected.
		Not Available	There is no active trail.
		Protecting/Wait-To-Restore	In case of revertive protection switching the selector is waiting to switch back to the restored a-End working remote CTP.

Table 168: AP: / unit-x / vc4 / vc4-b / klm-npq, Status - CTP (continued)

Operation Name	Parameter Name	Range	Description / Details
External Request	Request	Release	Automatic trail selection.
		Force Working	Force the selector to use the trail from the a-End working remote CTP.
		Force Protecting	Force the selector to use the trail from the a-End protecting remote CTP.
		Manual Working	Prefer the trail from the a-End working remote CTP. Use this trail only if the fault status is not worse than the fault status of the protecting trail.
		Manual Protecting	Prefer the trail from the a-End protecting remote CTP. Use this trail only if the fault status is not worse than the fault status of the working trail.

8.22 AP: / unit-x / iports

8.22.1 AP: / unit-x / iports, Overview

For a description of the

- “Overview - Alarms”, and
- “Overview - Statistics”

management functions, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.22.2 AP: / unit-x / iports, Main

For a description of the

- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.23 AP: / unit-x / iports / iport-b

The NUSA1 internal backplane Ethernet ports (iport-b) connect the local bridge circuit with the bridge circuits on the working and protecting core units via the GbE star. The backplane port is a 1GbE electrical port. The speed of the port is fixed.

8.23.1 AP: / unit-x / iports / iport-b, Overview

For a description of the
- “Overview - Alarms”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.23.2 AP: / unit-x / iports / iport-b, Main

8.23.2.1 AP: / unit-x / iports / iport-b, Main – General

For a description of the “Labels” and “Alarm Status” parameters in the
- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

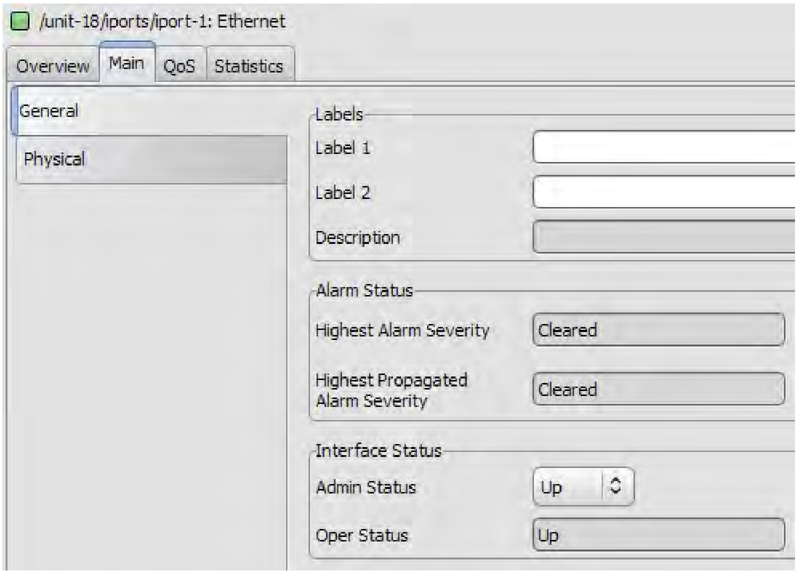


Table 169: AP: / unit-x / iports / iport-b, Main – General

Operation Name	Parameter Name	Range	Descriptions / Details
Interface Status	Admin Status	Up	Select “Up” to bring the internal port into service
		Down	The internal port cannot be set to the Down state.
	Oper Status	Up	Shows the operational state is up. The state can only be up if the administrative state is up and there are currently no failures.
		Down	Shows the operational state is down.
		Testing	Shows the port is in a testing state.

8.23.2.2 AP: / unit-x / iports / iport-b, Main – Physical

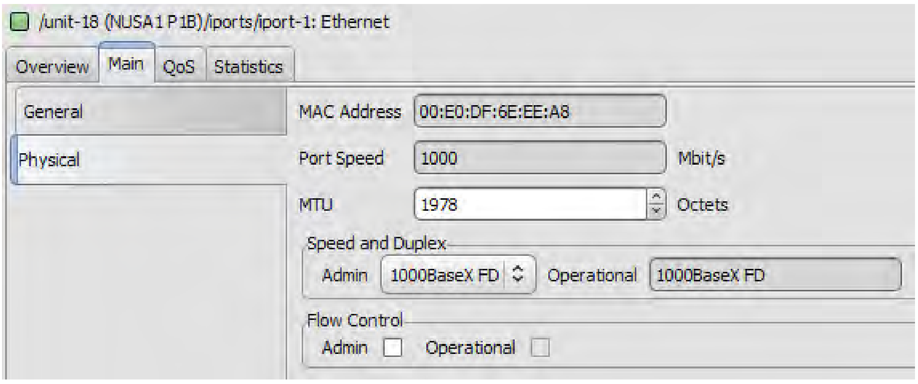


Table 170: AP: / unit-x / iports / iport-b, Main – Physical

Operation Name	Parameter Name	Range	Descriptions / Details
	MAC Address	00:00:00:00:00:00 … ff:ff:ff:ff:ff:ff	Shows the physical (MAC) address of this port. This parameter is read-only.
	Port Speed	1000 Mbit/s	Shows the port speed. This parameter is read-only.
	MTU	1’978 … 9’194 Octets, step 2 Octets	Maximum Transmission Unit, i.e. maximum IP packet size. The MTU size is calculated including the IP headers.
Speed And Duplex	Admin	1000BaseX FD	1’000 Mbit/s, full duplex
		<empty>	
	Operational	1000BaseX FD	1’000 Mbit/s, full duplex
Flow Control	Admin	☑	Port Ethernet flow control according to IEEE 802.3x. Flow control is a mechanism which allows the receiving party of a connection to control the rate of the sending party.
		☐	
	Operational	☑	
		☐	

Please note:

For an overview on the specific characteristics of XMC20 Switch ports, please refer to [201] System Description “XMC20 R6B”.

8.23.3 AP: / unit-x / iports / iport-b, QoS

8.23.3.1 AP: / unit-x / iports / iport-b, QoS – QoS Scheduling

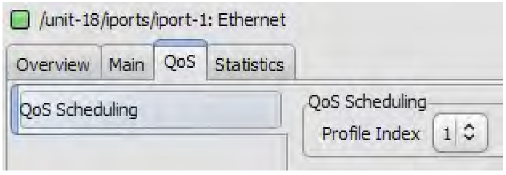


Table 171: AP: / unit-x / iports / iport-b, QoS – QoS Scheduling

Operation Name	Parameter Name	Range	Descriptions / Details
QoS Scheduling	Profile	1 … 5	Select the QoS scheduling profile number. QoS scheduling profiles are configured with ECST in the “Switching” view at Switching/ Bridges, bridge-1/QoS, Scheduling Profiles.

8.23.4 AP: / unit-x / iports / iport-b, Statistics

8.23.4.1 AP: / unit-x / iports / iport-b, Statistics – General

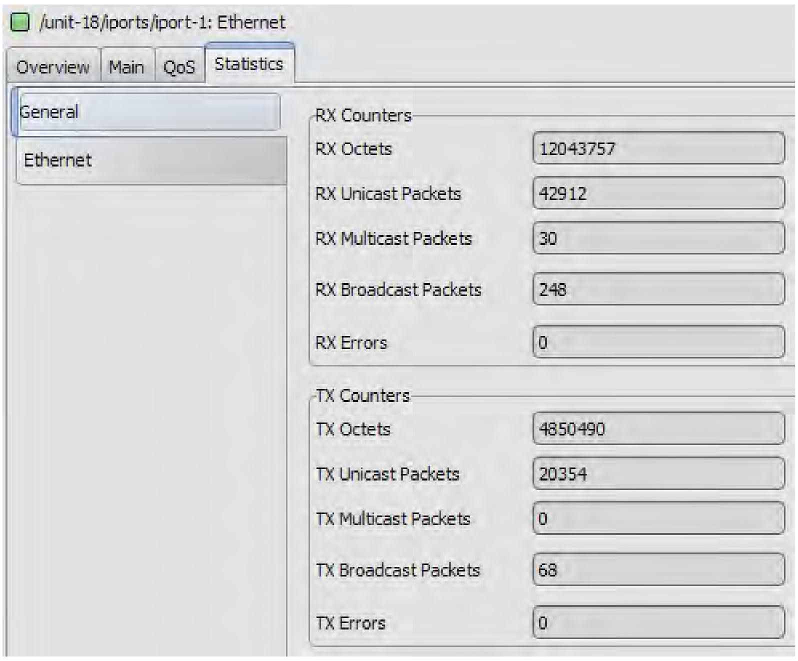


Table 172: AP: / unit-x / iports / iport-b, Statistics – General

Operation Name	Parameter Name	Range	Descriptions / Details
RX Counters	RX Octets	0 … 2^{64} -1	Number of ingress octets
	RX Unicast Packets	0 … 2^{64} -1	Number of ingress unicast packets
	RX Multicast Packets	0 … 2^{64} -1	Number of ingress multicast packets
	RX Broadcast Packets	0 … 2^{64} -1	Number of ingress broadcast packets
	RX Errors	0 … 2^{32} -1	Number of ingress errored packets

Table 172: AP: / unit-x / iports / iport-b, Statistics – General (continued)

Operation Name	Parameter Name	Range	Descriptions / Details
TX Counters	TX Octets	0 … 2^{64} -1	Number of egress octets
	TX Unicast Packets	0 … 2^{64} -1	Number of egress unicast packets
	TX Multicast Packets	0 … 2^{64} -1	Number of egress multicast packets
	TX Broadcast Packets	0 … 2^{64} -1	Number of egress broadcast packets
	TX Errors	0 … 2^{32} -1	Number of egress errored packets

Please note:

The statistics counters restart with 0 when they reach their upper range limit.

8.23.4.2 AP: / unit-x / iports / iport-b, Statistics – Ethernet

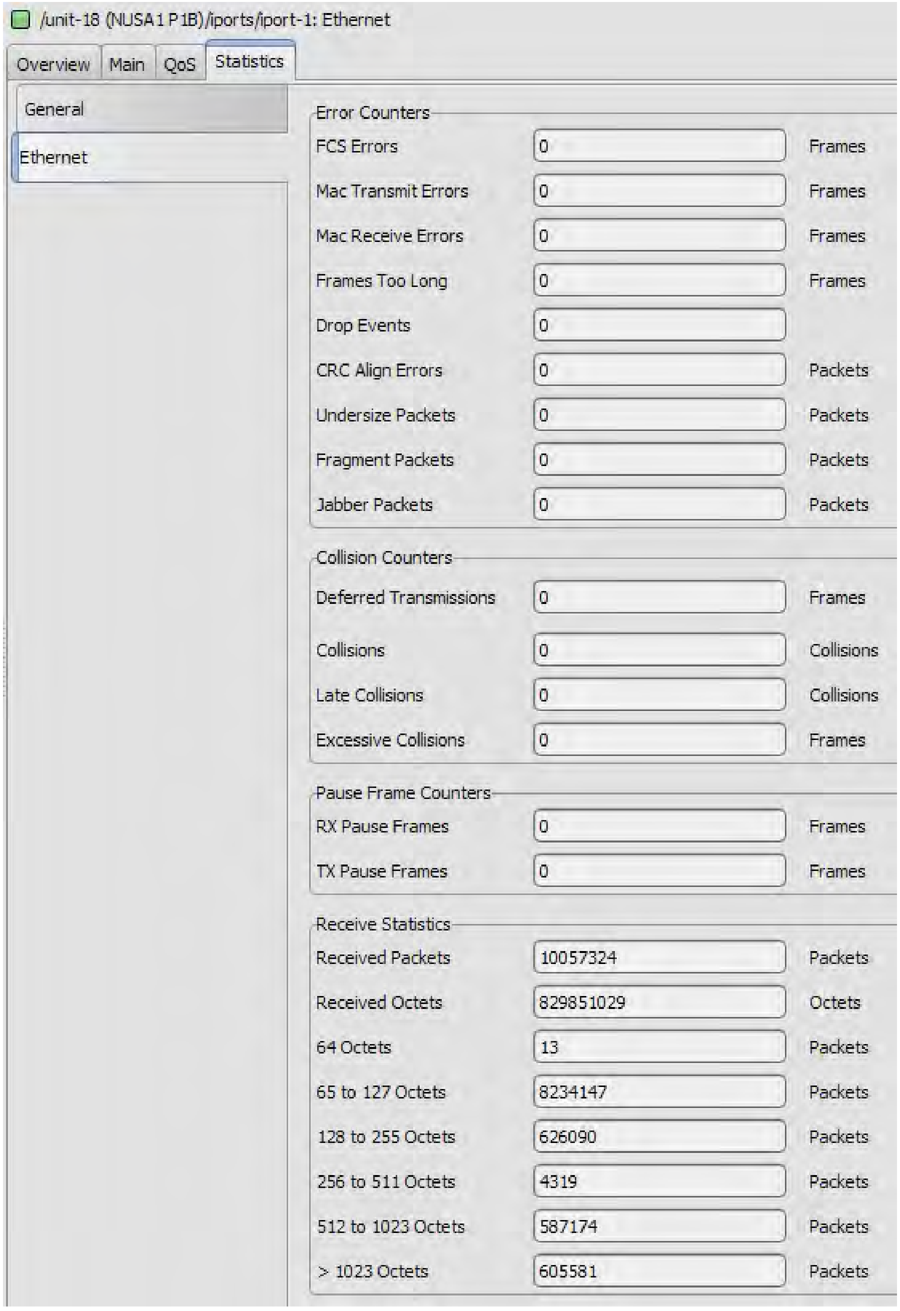


Table 173: AP: / unit-x / iports / iport-b, Statistics – Ethernet

Operation Name	Parameter Name	Range	Descriptions / Details
Error Counters	FCS Errors	0 … 2^{64} -1	Number of ingress frames with FCS errors
	Mac Transmit Errors	0 … 2^{64} -1	Number of egress frames with a MAC sublayer transmit error
	Mac Receive Errors	0 … 2^{64} -1	Number of ingress frames with a MAC sublayer receive error
	Frames Too Long	0 … 2^{64} -1	Number of ingress frames that exceed the maximum permitted frame size.
	Drop Events	0 … 2^{32} -1	Number of ingress drop events
	CRC Align Errors	0 … 2^{32} -1	Number of ingress packets with CRC alignment errors
	Undersize Packets	0 … 2^{32} -1	Number of ingress undersized packets (< 64 bytes)
	Fragment Packets	0 … 2^{32} -1	Number of ingress fragment packets
	Jabber Packets	0 … 2^{32} -1	Number of ingress jabber packets
Collision Counters	Deferred Transmissions	0 … 2^{32} -1	Number of egress frames for which the first transmission attempt is delayed because the medium is busy
	Collisions	0 … 2^{32} -1	Number of estimated collisions
	Late Collisions	0 … 2^{32} -1	Number of times that a collision is detected later than one slot time into the transmission of a packet.
	Excessive Collisions	0 … 2^{32} -1	Number of frames for which transmission fails due to excessive collisions
Pause Frame Counters	RX Pause Frames	0 … 2^{64} -1	Number of ingress pause MAC control frames
	TX Pause Frames	0 … 2^{64} -1	Number of egress pause MAC control frames
Receive Statistics	Received Packets	0 … 2^{64} -1	Number of ingress packets
	Received Octets	0 … 2^{64} -1	Number of ingress octets
	64 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 64 octets
	65 to 127 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 65 to 127 octets
	128 to 255 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 128 to 255 octets
	256 to 511 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 256 to 511 octets
	512 to 1023 Octets	0 … 2^{64} -1	Number of ingress packets with a size of 512 to 1023 octets
	> 1023 Octets	0 … 2^{64} -1	Number of ingress packets with a size of more than 1023 octets

Please note:

The statistics counters restart with 0 when they reach their upper range limit.

8.24 AP: / unit-x / iports / iport-b / mau

8.24.1 AP: / unit-x / iports / iport-b / mau, Overview

For a description of the

- “Overview - Alarms”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

8.24.2 AP: / unit-x / iports / iport-b / mau, Main

For a description of the

- “Main - General”

management function, please refer to [302] User Guide “XMC25/XMC23/XMC22”.

9 Annex

9.1 Associated XMC20 Documents

Any version(s) and/or release(s) indicated with the below listed document titles identify the specific state of the software and/or feature set at the creation time of the present document. If the present document is published as part of a document collection, the hyperlinks might open a document valid for a newer version/release. That updated version is valid in the context of all units and features described in the document collection.

Please note:

For the HTML-based documentation site there are no interdocument hyperlinks realized yet.

→ Please find the required document via the navigation tree on the left.

[012] Release Note “XMC20 System Release R6B”

[201] System Description “XMC20 R6B”

[202] Safety Instructions “Precautions and safety”

[301] User Guide “XMC25 Installation”

[310] User Guide “XMC23 Installation”

[322] User Guide “XMC22 Installation”

[302] User Guide “XMC25/XMC23/XMC22”

[323] User Guide “Management Communication”

[354] Quick Guide “ECST”

[355] User Manual “ECST”

[314] User Guide “TDM Services and Cross Connections in XMC20”

[340] Quick Guide “TDM Services over PDH/SDH”

[341] Quick Guide “Ethernet Switching”

[356] User Manual “Ethernet Switching”

[358] User Manual “MPLS-TP”

[359] Quick Guide “MPLS-TP”

[447] User Manual “COGE5, COGE5-F co5ne_r2, co5un_r2”

[410] User Manual “SELI8 seli8_r5”

[445] User Manual “NUSA1, NUSA1-F nusa1_r3”

[453] User Manual “NUSA2, nusa1_r3”

[506] User Manual “XMC20 cables”

[915] Technical Bulletin “Feature Licences for XMC20”

9.2 Technical Support

Please refer to the KEYMILE Extranet (via http://www.keymile.com) for support contact information.

9.3 Product Training

Training courses are available for a wide range of KEYMILE products and applications.

For contact information, course descriptions, locations and dates, go to the Website: http://www.keymile.com, then search for “product training”.