221 02-ZAP 701 25/1 Rev C 2006-08-04

Marconi OMS 1200
Optical MultiService Metro-Edge

Technical Product Description

Release 3.4

ERICSSON

Since January 2006, Marconi is a member of the Ericsson group.

Copyright

Disclaimer

Trademarks

Table of Contents

List of Figures

List of Tables

Chapter 1:
About This Document

1.1 Introduction

This topic provides the technical description for the OMS 1200 equipment.

Chapter 2: Product Description

Provides an outline level description of the OMS 1200 equipment. It includes configuration options and a brief explanation of compatibility issues.

Chapter 3: Functional Overview
Provides an explanation of the functions of the system and individual cards. Functionality includes network management and access via the LCT and LCTs. It also covers protection principals applied by the LCT and LCTs. Further details are provided in the “LCT/LCTS Operating Procedures” handbook .

Chapter 4: Typical Applications

Discusses a range of scenario applications, together with operator configurable options.

Chapter 5: Power Consumption

Provides power consumption details. The “Safety Guide” handbook provides other safety related information.

Chapter 6: Synchronisation

Discusses timing synchronisation, operator configurations and card configuration in relation to regular operation of the OMS 1200 equipment.

Chapter 7: Protection Schemes

Discusses a more detailed description of the functioning protection systems as background information to the instructions supplied in the “LCT/LCTS Operating Procedures” handbook. Card and traffic protection are discussed in line with common maintenance scenarios, fault and failure alarm conditions. Further maintenance information is provided in the “Maintenance and Fault Procedures” handbook.

Reference drawings and details of individual units in the OMS 1200 are provided to enable easy identification of cards, fascias and LEDs used in the alarm and fault diagnosis procedures. Detailed pin outs are given where appropriate for reference by installation and commissioning engineers. Further information on fault diagnosis and maintenance is provided in the “Maintenance and Fault Procedures” handbook, and installation and commissioning information in the “Subrack Installation Guide”.

Blank Page

Chapter 2:
Product Description

2.1 Equipment Overview

The OMS 1200 is a range of SDH (Synchronous Digital Hierarchy) Add Drop Multiplexers, optimised for ring and terminal applications.

The family comprises two members at Release 3.4:

- **OMS 1240**: Compact sub-rack with:
  - STM-1/4 Core/CCU Card and 5Gbit switch (see Section 2.1.4) or
  - STM-4/16 Core/CCU Card and 10Gbit switch (see Section 2.1.6)
- **OMS 1260**: Full size sub-rack with:
  - STM-1/4 Core/CCU Card and 5Gbit switch (see Section 2.1.5) or
  - STM-4/16 Core/CCU Card and 10Gbit switch (see Section 2.1.6).

2.1.1 Common Family Features

The OMS 1200 range is an evolutionary development of the SMA and MSH product ranges, which are deployed extensively in SDH access networks (in street cabinets, local exchanges and directly in customer premises), and complements these products.

The OMS 1200 is managed by Ericsson's ServiceOn Optical Element Manager or by a local terminal.

All members of the OMS 1200 offer:

- Up to two Core cards, each providing a fully non-blocking switch matrix supporting cross-connections of all container sizes defined by ETSI EN 300 147 and able to operate as a protected pair. Two Core card types are available, offering either two STM-1/4 ports or a single STM4/16 port with front-panel access via SFP modules.
- Provision of a number of dedicated backplane slots for 2Mb/s PDH Tributary cards plus associated LTUs, including a Tributary Card protection scheme.
- Provision of a number of "Generic Tributary" backplane slots, capable of accepting legacy SMA Tributary cards plus new compatible Tributary cards.
- A Comms/Auxiliary/Ancillary card providing network timing, network management and alarm scheme connections.

- An SDH Multi-rate tributary card providing both capital and operational expenditure savings. A single SDH tributary card provides four front access STM-1 interfaces or a single STM-4 interface, thereby offering on a single card the same level of connectivity provided by up to four legacy tributaries and saving up to three generic tributary card slots.

- Range of “Data” cards providing 10/100 and Gigabit Ethernet connectivity.

2.1.2 Deployment

The OMS 1200 can be deployed in networks with existing Marconi SDH products, and in mobile radio networks for the collection and consolidation of traffic from radio base stations. The OMS 1200 can be used in mixed rings with and subtended from the existing ADMs.

The OMS 1200 equipment may be adapted for specific customer requirements, but typical uses may include the following locations:

- Telecom centres:
  - Equipment buildings designated with restricted access controls
  - Environment as designated for telecom centres where the equipment requirement for operational performance is EN 300 019-1-3 Class 3.2.
- Locations assumed to have the status of equipment rooms or cabinets in end-customer premises:
  - Rooms and cabinets providing for restricted access controls
  - Environments similar to public telecomm equipment buildings where the equipment requirement for operational performance is EN 300 019-1-3 Class 3.2.
- Street/roadside locations (enclosed cabinets) - see notes below:
  - Cabinets providing for restricted access controls.
- Rail trackside locations (enclosed cabinets) - see notes below:
  - Cabinets providing for restricted access controls
  - Cabinets providing for installation not being installed within the 3 metre zone of the nearest ‘running rail’.
- Mobile radio base stations locations (enclosed cabinets) see notes below:
  - Cabinets providing for restricted access controls.
- Underground locations (enclosed cabinets) see notes below.
  - Cabinets providing for restricted access controls.

Note: In the worst scenarios these environments can be assumed to be outdoor stations which could be located in the proximity of rail tracks and/or earthquake zones.

Note: Locations where the environmental conditions exceed the limits of EN 300 019-1-3 Class 3.2, and where a protective enclosed cabinet is used to provide a managed micro-climate for the OMS 1200 equipment, compliant with EN 300 019-1-3 Class 3.2.

2.1.3 Data Transport

Comprehensive functionality of data transport is provided by use of data tributary cards and mapping of data client signal into a single virtual concatenation group through Generic Frame Procedure (GFP) encapsulation. Bandwidth configuration of the SDH virtual containers can be flexibly allocated to efficiently carry data client traffic. Additionally, LCAS bandwidth management protocol can be applied.

Depending on the client signal bandwidth, the GFP encapsulated signals can be transported in the following SDH containers: VC-12, VC-12-nv, VC-3, VC-3-nv, VC-4 and VC-4-nv. The generic SDH multirate card enables multiple STM-1 or a single STM-4 configuration on a single card. The OMS 1260 equipment offers seven generic tributary card slots, with five being available when using an STM-1/4 core card, and all seven being available when using an STM-4/16 core card.

2.1.4 OMS 1240 with STM-1/4 Core Card - Summary

OMS 1240 with STM-1/4 Core Card is intended for applications requiring high volume of 2Mbit/s transport at STM-1 and for light traffic STM-4 applications that require the flexibility and protection options provided by a slide-in unit subrack format. The equipment is also targeted for use in enclosed cabinets. It offers a flexible range of service deliveries including Ethernet. It is also ideal for multi-tenanted buildings as it has the capacity to serve multiple businesses whilst minimising space requirements.

This unit provides STM-1/4 SDH functionality to the customer together with protected SDH ring and terminal applications through four line interfaces.

This equipment has an extremely small footprint and flexible mounting options, vertical or horizontal, enabling effective use of space. Two adjacent vertically mounted units can be mounted in a standard ETSI or 19” rack.

Features List

- Compatible with Ericsson’s range of new generation-SDH multiplexers
- Two line interfaces for each STM-1/4 core card supporting both ring and terminal applications
- Two core card slots, providing a protected switch matrix plus physical duplication of line interfaces.
- Supports SNCP or 1+1 MSP traffic protection, plus core and tributary card protection
- Supports I.421 for primary rate ISDN

- STM-1 (155 Mbit/s) and STM-4 (622 Mbit/s) aggregate line rate options
- Full, non-blocking, VC-12 cross connect capability
- Tributary traffic ports
  - 2Mbit/s, 34Mbit/s, 45Mbit/s, 140Mbit/s and STM-1 electrical
  - STM-1 and STM-4 optical
  - Ethernet 10 baseT, 100 baseT and Gigabit Ethernet
  - Tandem Connection Monitoring (TCM) for termination of inter-operator path.
- Comprehensive configuration, fault and performance management features
- Compact design, suitable for customer premises
- Hot pluggable SFP modules, including optical STM-1, STM-4 and electrical STM-1 modules.
- Power/LCT LTU providing duplicated DC power inputs, plus LCT interface connection.

2.1.5 OMS 1260 with STM-1/4 Core Card - Summary

The OMS 1260 with STM-1/4 core card is intended for applications requiring a higher capacity subrack than that afforded by the OMS 1240 with a STM-1/4 core card, and is installed in a standard ETSI or 19” rack.

The OMS 1260 with STM-1/4 core card offers a full capacity STM-4 network node.

Features List

The OMS 1260 with STM-1/4 core card has the features of the OMS 1240 with STM-1/4 core card listed in 2.1.4 plus the additional features shown below.

- Up to four 63x2Mbit/s tributary cards, plus one 63x2Mbit/s protection tributary card

- Maximum capacity of 252 x 2Mbit/s balanced tributary access within the subrack
- Maximum capacity of 126 x 2Mbit/s unbalanced tributary access within the subrack
- Maximum capacity of 252 x 2Mbit/s unbalanced tributary access using high-profile LTUs that extend the vertical space occupancy of the subrack
- 1:n 2Mbit/s protection ($n \leq 4$), independent of core card protection
- Seven physical generic tributary slots. Backplane connections between tributary slots and each core card slot provide the following:
  - Slots 1 to 3 have 2xSTM-1 bandwidth each
  - Slots 4 and 5 have 4xSTM-1 bandwidth each
  - Slots 6 and 7 have no connection to the STM-1/4 core card and therefore cannot be used in the OMS 1260 with STM-1/4 core card product
- Duplicated single-input Power/LCT LTU.

2.1.6 OMS 1200 with STM-4/16 Core Card - Summary

The STM-4/16 core card replaces the STM-1/4 core card in both OMS 1240 and OMS 1260 subracks to provide an upgrade to the STM-16 aggregate line rate. The STM-4/16 core card can, as its name implies, also operate at STM-4.

CAUTION!

The STM1/4 core cards are not compatible with the STM 4/16 core cards.

When upgrading a network element from STM1/4 to STM4/16, both existing STM1/4 core cards must be removed before any new core cards are fitted. Failure to do so will permanently damage the units. This caution applies to both OMS 1240 and OMS 1260 shelves.

The OMS 1240 and OMS 1260 with a STM-4/16 are identical to the OMS 1240 and OMS 1260 with an STM-1/4 core card with the following exceptions.

- The STM-4/16 core card has only one bi-directional line interface, therefore a maximum of two line interfaces are supported. 1+1 MSP protection of line interfaces is therefore not possible except in terminal applications.
- Two-fibre MS-SPRING protection of line interfaces is supported (SNCP also remains available as an alternative protection option).
- On the OMS 1260 only, the Generic Tributary Slots 6 and 7 are available, each having four x STM-1 bandwidth to each STM-4/16 core card.

2.2 OMS 1240 Product Structure

2.2.1 Subrack for OMS 1240

The OMS 1240 equipment subrack is designed for installation:

- As a single unit, vertical alignment in a telecom equipment rack with dimensions, height 2200mm, width 600mm, and depth 300mm, conforming to ETSI standard document EN 300 119-3.
- As two vertically aligned OMS 1240 modules mounted side by side across the rack width. In this case, the overall subrack width is <452mm, excluding rack side mounting assemblies.
- As a single unit, horizontally aligned, in a standard 19” rack using the appropriate horizontal subrack-mounting kit. In this case, the overall subrack vertical space occupancy is 227mm allowing it to fit easily within the 264mm of a 6-VU rack height envelope.
- As a single OMS 1240 unit, vertically aligned and mounted side-by-side with and powered from an AC Power / Battery Backup Unit type 03HAN00007AAH.

In all cases, the subrack mechanical design and realisation conforms to the standard equipment practices covered by EN 300 119-4.

Vertical and horizontal mounting options of OMS 1240 are shown in Figure 2-1.

Figure 2-1: Basic OMS 1240 Subrack Structure

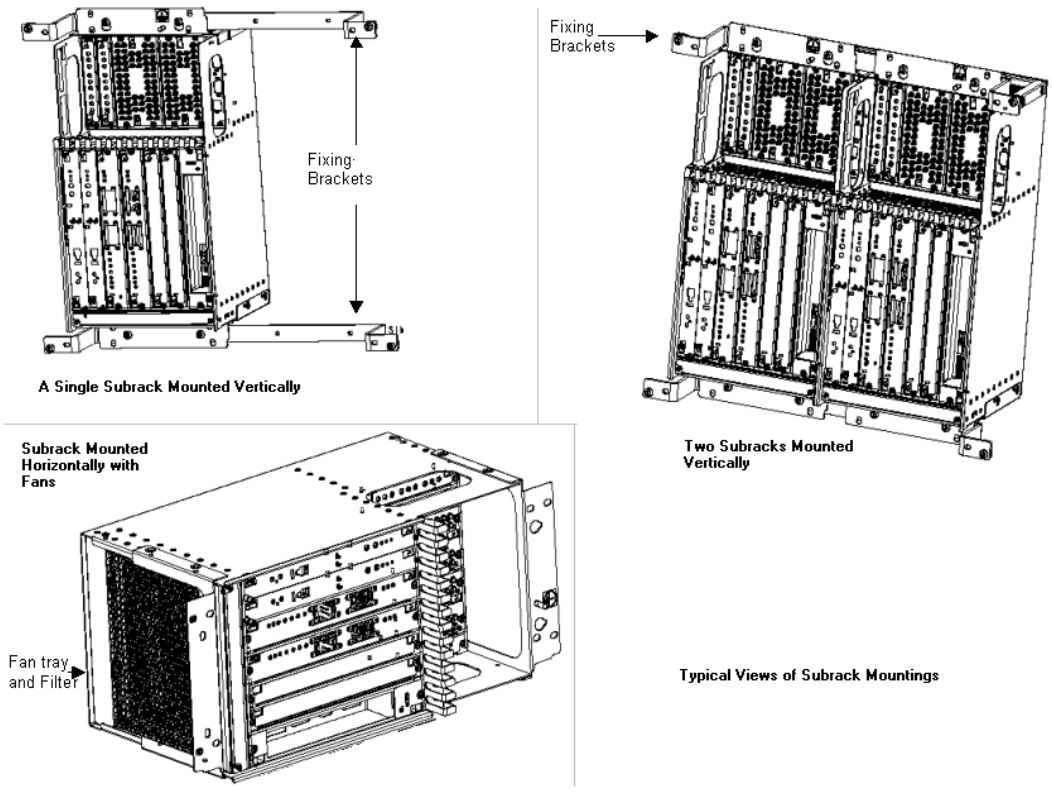
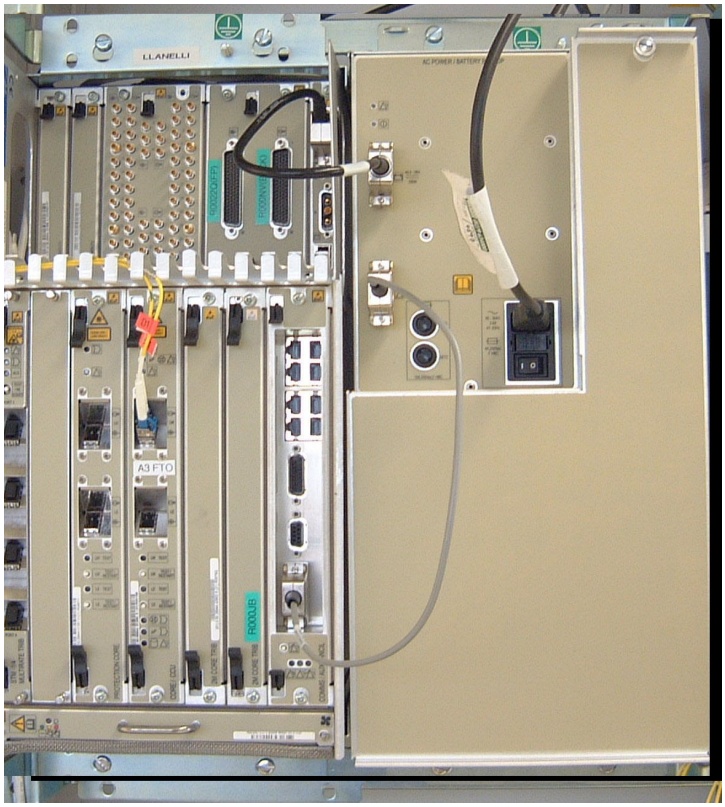


Figure 2-2: OMS1240 with Battery Box

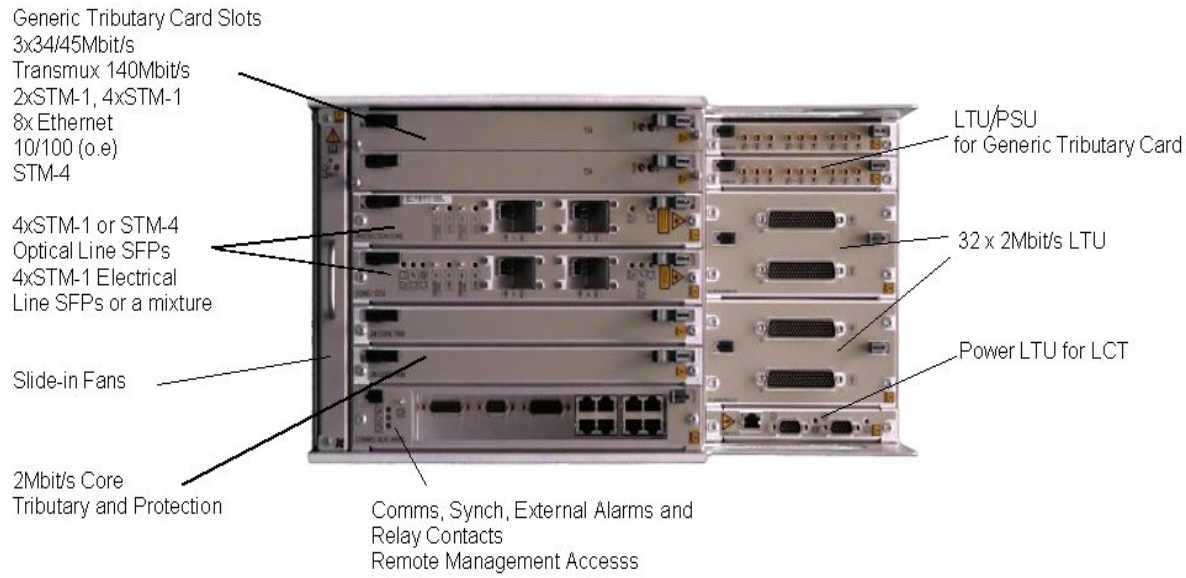


For further information on the use of the Battery Box unit, see 03PHB00002AAR AC Power & Battery Back-up Unit.

2.2.2 OMS 1240 Shelf and Cards

The basic subrack structure is illustrated in Figure 2-3.

Figure 2-3: Basic OMS 1240 Subrack



2.2.3 Cooling the OMS 1240 Subrack

The OMS 1240 subrack design incorporates a forced-air cooling fan enclosure, allowing in-service replaceable fan installations as an equipment installation option. Fan installation is mandatory in horizontally mounted subracks, where natural convection-current airflow is negligible. For vertical subrack mounting, fan installation is required only for certain specific configurations or if high inlet air temperatures are expected.

2.3 OMS 1260 Product Structure

2.3.1 Subrack for OMS 1260

The OMS 1260 subrack is designed for installation in a standard vertical-airflow alignment in an ETSI (metric or 19”) or DIN 19” equipment rack. The subrack mechanical design and realisation conforms to the standard equipment practices covered by ETSI EN 300 119-4.

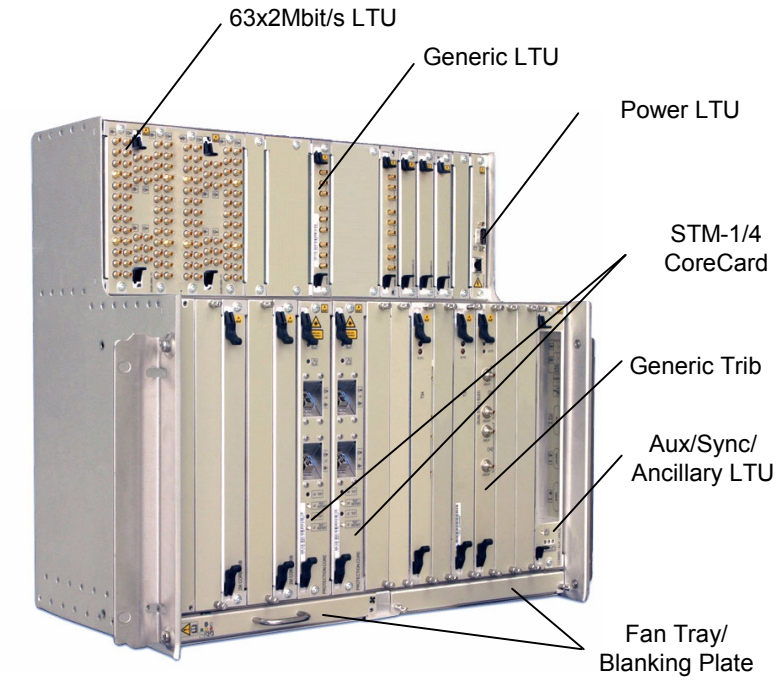
The OMS 1260 is shown in Figure 2-4.

Figure 2-4: Basic OMS 1260 Subrack Structure

2.3.2 OMS 1260 Shelf and Cards

The basic subrack structure is illustrated in Figure 2-5.

Figure 2-5: Example of a Basic OMS 1260 Subrack



2.3.3 Cooling the OMS 1260 Subrack

The OMS 1260 subrack design incorporates two forced-air cooling fan enclosures in which two, one or no fans may be fitted according to local configuration options and operating conditions. Any unused fan slots must be covered with EMC blanking plates supplied in the core SE.

2.4 Power Supply Architecture

The OMS 1200 equipment requires telecommunications industry standard DC power supplies as defined in EN 300 132-2 and described in the “Safety Guide” handbook. A variation is applied in that the rated voltage range of the OMS 1200 equipment is extended to -38.4Vdc at the low end, and to -75Vdc at the high end.

Two power input ports are provided, giving 1+1 protection of the power feeds.

Each power feed is connected to a power LTU, which then supplies the power to the backplane. Both power feeds are distributed through the backplane to the plug-in card slots that require them. The power is then combined by diodes on each card and fed to a DC-DC converter that produces the low-voltage rails required by the card. All card types other than generic tributary cards and 2Mb/s LTU cards use this power architecture.

Generic Tributary cards are powered from stabilised low-voltage supplies, delivered through the backplane. To provide the necessary low voltage supplies, each generic tributary card has an associated PSU/LTU card equipped with DC-DC converters that convert the station battery voltage to generate the low-voltage supplies. Each generic tributary card installed must therefore have an appropriate PSU/LTU fitted in the associated PSU/LTU slot.

2.4.1 Power/LCT LTU Cards

2.4.1.1 OMS 1240 Power/LCT LTU

The OMS 1240 subrack has a single slot for a Power/LCT LTU. The Power/LCT LTU has two D-type connectors, each providing a single DC power input to the subrack thereby providing protection for the external power supplies. Either power port can be used in a non-protected configuration.

The LTU also contains the interface transceivers and connector for the LCT serial port, and carries the subrack inventory PROM containing the subrack serial number and accessed via a backplane connection to the system inventory bus – these features are not protected.

The LCT serial port connector is a single RJ-45 socket. The LCT interface connects via the backplane to the Core/CCU Card, and via the LCT serial port connector and a cable directly to a PC serial port to provide local subrack management.

The OMS 1240 Power/LCT LTU is available in two versions differing only in the type of power input connector: one is equipped with 9-pin D-Type connectors; the other is equipped with 3-pin “Power D-Type” connectors.

- OMS 1240 LTU with 9-Pin D-Type 1HAM 61217 AAK
- OMS 1240 LTU with 3-Pin Power D-Type 1HAM 61217 ABC

The Power/LCT LTU must be ordered separately from the core product. If the OMS 1240 is to be powered from an AC Power / Battery Backup unit (03HAN00007AAH) then the 3-pin option must be selected.

2.4.1.2 OMS 1260 Power/LCT LTU

The OMS 1260 subrack has two Power/LCT LTU slots each accommodating an identical Power/LCT LTU card, thus both the power supply and the Power/LCT LTU can be protected. Each Power/LCT LTU has a single 3-pin power D-type connector providing a single power input port.

The LTU also contains the interface transceivers and connector for the LCT serial port, and carries the subrack inventory PROM (containing the subrack serial number) that is accessed via a backplane connection to the system inventory bus. The backplane connections that enable these features are present only at Slot S3-21; therefore these features are not protected even when two Power/LCT LTUs are installed.

The LCT serial port connector is a single RJ-45 socket. The LCT interface connects via the backplane to the Core/CCU Card, and via the LCT serial port connector and a cable directly to a PC serial port to provide local subrack management.

The OMS 1260 product core SE includes a single Power/LCT LTU fitted in slot S3_21. A second Power/LCT LTU can be ordered as an option: this is installed in Slot S3_20 to provide a protected power supply configuration. Slot S3_21 must always be equipped in every OMS 1260 subrack.

The card in slot S3_21 can be replaced without power loss to the system if a protection Power/LCT LTU is fitted in Slot S3_20 and has power connected, and vice versa. When the card in slot S3_21 is replaced the CCU will adopt the new system serial number contained on the replacement card.

2.4.2 *Generic Tributary PSU/LTU Cards*

As described in Section 2.4 above, the Generic Tributary Power LTU for OMS 1200 takes power from the station battery supplies distributed via the backplane, and employs DC-DC converters to produce low voltage power (+5V, -5V, +12V) which is then distributed via the backplane to its associated generic tributary slot. This card type is used with Generic Tributary cards that have front-panel access to interface cables.

There are two versions of this card:

- Generic Tributary Power LTU Version 1 - 1HAM61218AAM. This card is now obsolete, but may be found in early installed OMS 1200 subracks.
- Generic Tributary Power LTU Version 2 - 1HAM61232AAE. This is an enhanced card having higher maximum load capability. It is used with all new installations of front-access Generic Tributary cards, and is the only card capable of providing sufficient power for the ETO-100 and Layer 2 Data cards.

Other variants of this type of card are available that provide, in addition to low-voltage power, LTU traffic port access for 3x34M, 3x45M and 1x140M PDH or 2xSTM-1e Generic Tributary cards.

2.5 Line and Tributary Traffic and Comms Units

Note: The OMS 1260 version of the sub-rack will only support the following STM-1/4 tributary cards.

- Four port STM-1/4 multirate card (with SFP modules).
- Two port fixed STM-1 electrical interface (required for STM-1 operation with card protection).
- STM-4 VC-4 C/V contiguous to virtual concatenation conversion tributary.

2.5.1 STM-1/4 Core Switch/Line/CCU Card

Two versions of this unit are available: the STM-1/4 Core/CCU and the STM-1/4 Protection Core cards. They are identical except that the Protection Core card does not have the CCU function. Each card provides a fully transparent non-blocking switch plus two SDH line interface ports.

A full connectivity switch is provided, allowing cross-connections to be made between any combination of line and tributary ports, including tributary-to-tributary switching. All container sizes and mixes thereof, as defined by ETSI EN 300 147, can be cross-connected.

The line interface feature concentrates traffic signals from the switch into a 155Mbit/s stream (STM-1) or a 622Mbit/s stream (STM-4) for transmission over the East or West optical or electrical bearers. Small Form-Factor Pluggable (SFP) STM-1/4 optical or STM-1 electrical modules are used to provide the Line-East and Line-West connections to the cards. The optical SFP modules are available in a range of options providing choice of line rate, wavelength and distance.

The Communication Controller Unit (CCU) function is integrated into the design of the core/CCU card and provides the message routing for the internal control interfaces between the multiplexer controller, the network management ports and the other SMA modules. It provides the Qx and embedded communications channel Q_{ecc} within the SDH frame for central network-management control.

Application software is stored in non-volatile system memory, with an optional backup to return to a previous version of software. System configuration and status data is stored in non-volatile configuration database memory.

Software download is available to all cards, including the tributary modules, either from the element manager or via the LCT.

The subrack provides two slots for core switch/line units. Equipping the Core Switch/Line Unit A slot with a core/CCU card creates an unprotected system. The addition of a protection core card in the Core Switch/Line Unit B slot provides 1:1 equipment level protection for the core switch and timing/synchronisation functions plus four STM-1/4 line interface ports. This also allows the configuration option to deliver 1+1 Linear MSP Protection for two network line interfaces. Alternatively, the ports can be configured to provide single Line-East and Line-West interfaces, with the remaining two ports functioning as additional tributary interfaces.

2.5.2 STM-4/16 Core Unit

Two versions of this unit are available: the STM-4/16 Core/CCU and the STM-4/16 Core Cards. They are identical except that the STM-4/16 core card does not have the CCU function. Each card provides a fully transparent non-blocking switch plus one SDH line interface port.

A full connectivity switch is provided, allowing cross-connections to be made between any combination of line and tributary ports, including tributary-to-tributary switching. All container sizes and mixes thereof, as defined by ETSI EN 300 147, can be cross-connected.

The line interface feature concentrates traffic signals from the switch into a 622Mbit/s stream (STM-4) or a 2488Mbit/s stream (STM-16) for transmission over optical bearers. Small Form-Factor Pluggable (SFP) STM-4 or STM-16 optical modules are used to provide the optical connections to the cards. The optical SFP modules are available in a range of options providing choice of line rate, wavelength and distance.

The Communication Controller Unit (CCU) function is integrated into the design of the core/CCU card and provides the message routing for the internal control interfaces between the multiplexer controller, the network management ports and the other SMA modules. It provides the Qx and embedded communications channel Qecc within the SDH frame for central network-management control.

Application software is stored in non-volatile system memory, with an optional backup to return to a previous version of software. System configuration and status data is stored in non-volatile configuration database memory.

Software download is available to all cards, including the tributary modules, either from the element manager or via the LCT.

The subrack provides two slots for core switch/line units. Equipping the Core Switch/Line Unit A slot with an STM-4/16 core/CCU card provides a single line interface for terminal applications only.

The addition of an STM-4/16 core card in the Core Switch/Line Unit B slot provides 1:1 equipment level protection for the core switch and timing/synchronisation functions plus a second STM-4/16 line interface. This can be configured to provide one of the following options:

- 1+1 linear MSP protection for a single network line interface in a terminal application
- Single Line-East and Line-West interfaces for ring applications with the options of SNCP and 2-fibre MSSPRING protection schemes.

2.5.3 OMS 1240 64x2Mbit/s Core Tributary Card and LTUs

The OMS 1240 employs a single dedicated Core Tributary card to provide up to 64 channels of 2Mbit/s PDH traffic, with interface cable connection ports provided exclusively by LTUs. The Core Tributary card provides the HDB3 line drivers and receivers, permitting the LTUs to be simple cards providing only interface cable connectors plus passive line termination.

Two Core Tributary slots are provided to enable the option of 1:1 Core Tributary card protection. Both slots drive and receive the same set of HDB3 interface connections to the LTUs.

The Core Tributary card has no on-board intelligence and is thus functionally dependent upon the presence of a host Core card: Core A is the host for Core TRIB A and Core B is the host for Core TRIB B. The minimum configuration for 2M PDH operation with no protection requires the equipping of slots Core A and Core TRIB A only. The “B” cards are only installed if protection of the Core and/or the Core Tributary card is required, or if additional STM-1/4/16 ports are required.

Two versions of the Core Tributary card exist. In a system having a protected Core, one can tolerate temporary removal of its host Core card without traffic loss, the other cannot. This has implications where it is desired to protect the Core cards but not the Core Tributary cards - see Section 7.2.1.1 for details.

Two slots are provided for OMS 1240 2M LTUs, each slot carrying 32 channels of 2M traffic. Balanced and unbalanced LTU options are available, each type being a composite module consisting of one SIU card plus a front panel providing either 2 x 78-pin high-density D-Type connectors (balanced) or 64 x 1.0/2.3 coaxial connectors (unbalanced).

2.5.4 OMS 1260 63 x 2Mbit/s Tributary Card and LTUs

Unlike the OMS 1240 Core Tributary card, the OMS 1260 2Mbit/s Tributary card provides 63 x 2Mb/s PDH channels, has on-board intelligence and is not dependent upon a host Core card. The OMS 1260 subrack provides five slots for 2M Tributary cards, one of which (in slot position S1_05) is dedicated as a protection card. Tributary card protection is therefore via a 1:n scheme where $n \leq 4$, and is independent of core card protection. Protection traffic routing is handled by the LTUs, and controlled by the core cards.

The OMS 1260 2M tributary cards are connected to cable ports via OMS 1260 2M LTUs, again these differ from the OMS 1240 2M LTUs.

Three LTU slots are provided for each 2M Tributary card, each slot carrying 21 channels of 2M traffic. Balanced and unbalanced LTU options are available as follows:

OMS 1260 63x2Mbit/s Balanced LTU

The Balanced LTU option consists of a single-card 21-port LTU having a front panel with two high-density D-Type connectors (input and output). Up to three of these can be installed per 2M tributary card and up to twelve can be installed per subrack, thus providing a maximum of 252x2Mbit/s balanced ports.

OMS 1260 63x2Mbit/s Unbalanced LTU (SP60EA)

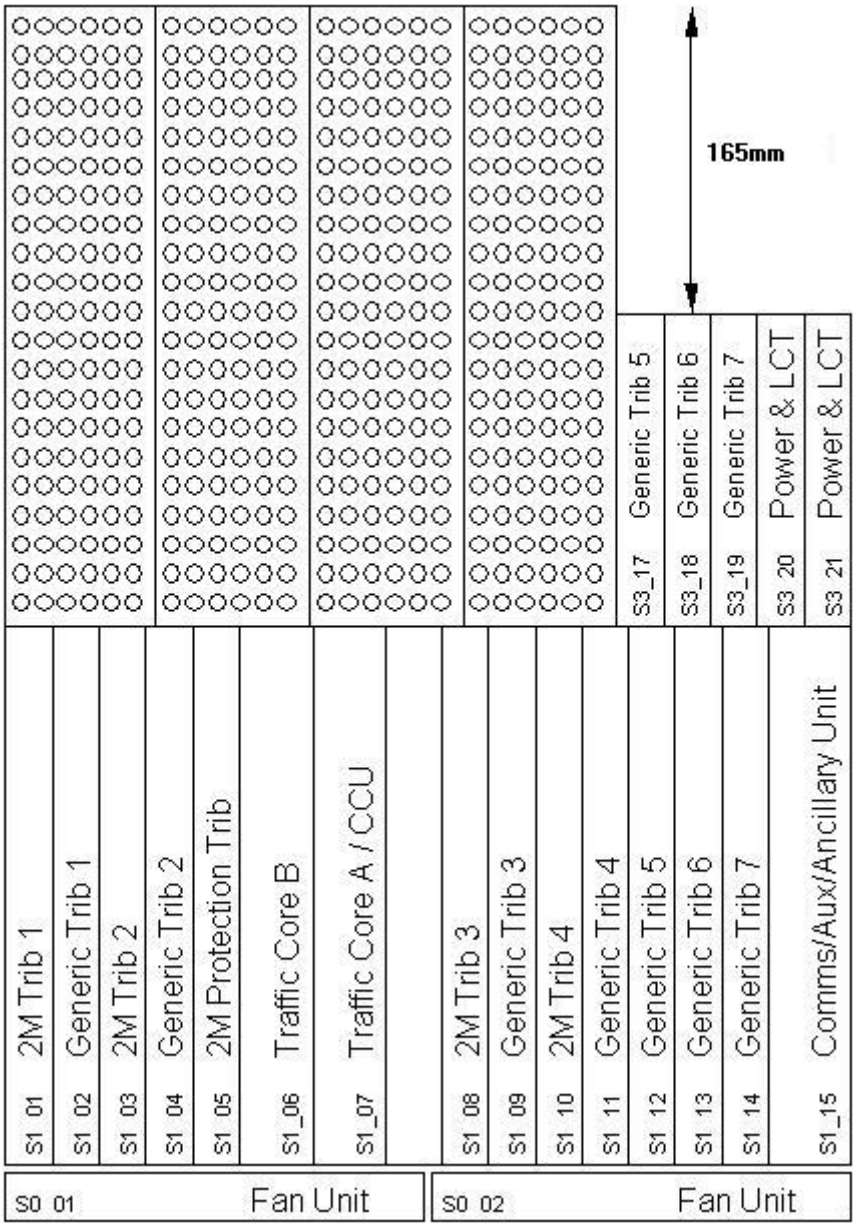
The standard Unbalanced LTU option consists of a single 63 port LTU, this being a composite module consisting of three SIU cards plus a front panel providing 126 1.0/2.3 coaxial connectors. The installation of any such LTU occupies the LTU front panel space that serves both its own tributary card and that of its neighbour to the right. Therefore, a limit of two standard unbalanced LTUs can be installed per sub-rack, providing a maximum of 126x2Mbit/s unbalanced ports and supported by two 2M Tributary cards.

OMS 1260 Vertically Extended 63x2Mbit/s Unbalanced LTU (SP60EZ)

An optional high-profile 63-port Unbalanced LTU provides the same functionality as the standard version but has narrow width and extends 165mm above the top of the subrack thus increasing the profile height of the subrack. This LTU allows installation of up to four LTUs per subrack, providing a maximum of 252x2Mbit/s unbalanced ports.

Use this LTU when more than 126 x 2Mbit/s ports are required to be connected to a single OMS 1260 subrack, or if any future expansion of the NE will increase the number of 2M ports beyond 126. When planning the installation, bear in mind that this LTU will extend 165mm beyond the top of the subrack.

Figure 2-6: Vertically Extended 63x2Mbit/s LTU



2.5.5 Generic Tributary Units

Two generic tributary slots are provided in the OMS 1240 subrack, each one having associated with it a generic tributary PSU/LTU slot.

Seven generic tributary slots are provided in the OMS 1260 subrack, each one having associated with it a generic tributary PSU/LTU slot. Only Slots 1-5 are available for use with an STM-1/4 core card. The STM-4/16 core card has access to all seven slots.

The generic tributary slots are capable of supporting a range of generic SMA tributary cards including PDH, SDH and Data cards. See Table 2-1 for a full list of Generic Tributary cards and their compatibility with OMS 1240 and OMS 1260.

For generic tributary cards that do not use front-access traffic ports, the associated generic tributary PSU/LTU card also provides the traffic port physical interfaces.

Note: Where two or more identical generic tributary cards are installed, and those cards use LTU-based traffic port access (PDH, STM-1 electrical), 1:n tributary card level protection is supported by LTU-based protection-switching functions. The tributary cards in each 1:n protection group must be in contiguously-numbered slots: note that in OMS 1240 the value of “n” is restricted to “1” since there are only two Generic TRIB slots.

Table 2-1: OMS 1200 Generic Tributary Card Compatibility

Serial	Type	Card Name	Card Code	OMS 1240	OMS 1260
1	PDH	3 x 34Mbit/s Asynchronous	1HAT60622BAA	✓	✓
2	PDH	3 x 45Mbit/s Asynchronous	1HAT60623BAQ	✓	✓
3	PDH	1 x 140Mbit/s Asynchronous	1HAT60624BFE	✓	✓
4	PDH	34 Transmux Async/Byte/Bit floating	1HAT60979AAC	✓	✓
5	SDH	STM-1 G703 Electrical	1HAT60803ABT	✓	
6	SDH	STM-1 G957 L-1.1	1HAT60791ABU/AFP	✓	
8	SDH	STM-1 G957 L-1.2	1HAT60791~~A~~CM/AGG	✓	
9	SDH	Dual STM-1 card G703 Electrical	1HAT61004ABP	✓	✓
10	SDH	Flexible dual STM-1	1HAT60878AAT	✓	
11	SDH	Quad STM-1 G703 Electrical	1HAT61059AAJ	✓	
12	SDH	Quad STM-1 G957 L-1.1	1HAT61055ABS/ACK	✓	
13	SDH	Quad STM-1 G957 S-1.1	1HAT61057ABW/ACP	✓	
14	SDH	Quad STM-1 G957 L-1.2	1HAT61056ABU/ACM	✓	
15	SDH	Quad STM-1 G957 I-1.1 Multimode	1HAT61063ABD/ACV	✓	
16	SDH	STM-4 G957 L-4.1+	1HAT61008AEA/AQY	✓	
17	SDH	STM-4 G957 S-4.1	1HAT61008ABX/AMW	✓	
18	SDH	STM-4 G957 L-4.2 and L-4.3	1HAT61008ADH/APG	✓	
19	SDH	STM-4 G957 L-4.2+	1HAT61008AFS/ARR	✓	
20	SDH	STM-4 G957 L-4.1	1HAT61008ACQ/ANP	✓	
21	SDH	STM-4 C to V Optimux	1HAT61009ABA/ACS	✓	✓
22	Data	ETA-100	03HAT00010AAS	✓	✓
23	Data	ETO-100	03HAT00017AAH	✓	✓
24	Data	ELS-1000S (Layer 2 Card)	05HAT00021AAM	✓	✓
25	SDH	SDH Multirate (replacing many of the OMS 1240 only cards)	03HAT00043AAU	✓	✓

Note: Grey-shaded rows in the table above represent cards in the process of being phased out.

2.5.6 OMS 1260 Tributary Groups

Due to the large number of backplane tributary-to-LTU interface connections required, it is not possible to combine the 63 x 2Mbit/s and generic tributary functions into a single slot. OMS 1260 therefore uses dedicated 2M tributary card slots each of which is associated with an adjacent generic tributary card slot. This pair of slots is known as a 'Tributary Group'.

The two tributary slots in each tributary group share common interface connections to the switch units as shown in Figure 2-7 and are therefore mutually exclusive. For each tributary group, a slide mechanism at the front of the OMS 1260 subrack prevents incorrect card installation by physically preventing insertion of more than one card into that tributary group.

Note: Generic Tributary Card Slots 5, 6 and 7 are not associated with 2M tributary cards, i.e. they do not belong to any tributary group.

As shown in Figure 2-7 and Figure 2-8, Tributary Groups 1 to 3 plus the 2Mbit/s slot of Tributary Group 4 each have a bandwidth equivalent to 2 x STM-1: The generic tributary slot of Tributary Group 4 and Generic Tributary Slots 5 to 7 each have a bandwidth equivalent to 4 x STM-1. Generic Tributary Slots 6 and 7 have no connection to the switch when an STM-1/4 core is fitted.

Figure 2-7: OMS 1260 (with STM-1/4 Core) Tributary Groups Showing Bandwidth Available

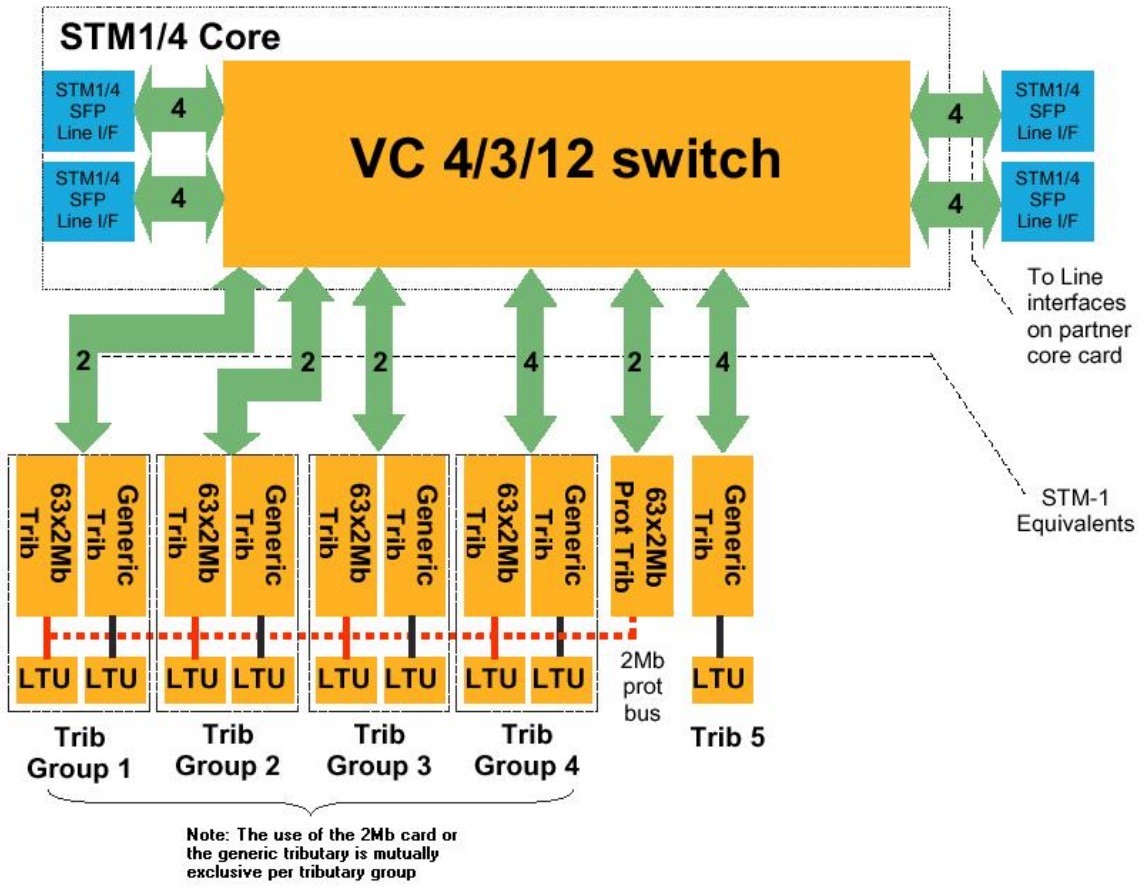
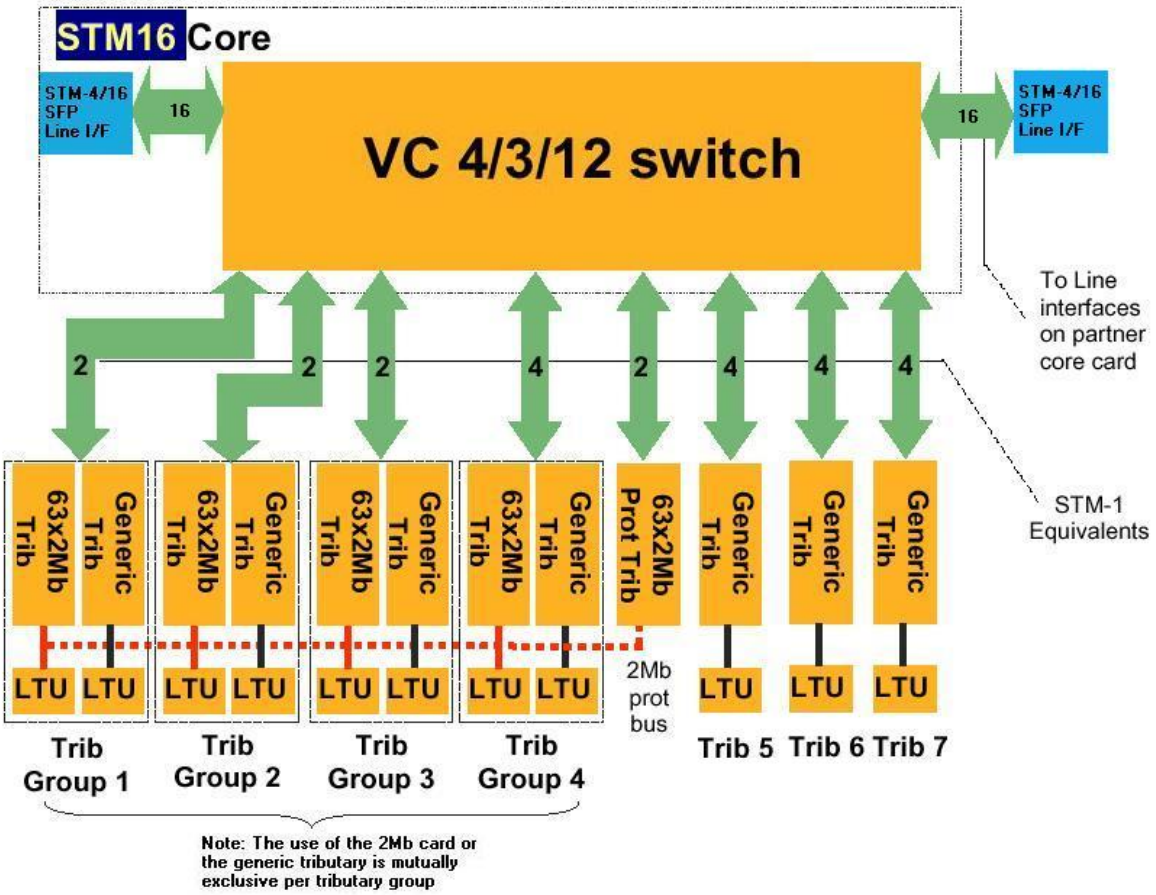


Figure 2-8: OMS 1260 (with STM-4/16 Core) Tributary Groups Showing Bandwidth Available



Note: The 2M tributary slot of Tributary Group 4 only receives 2 x STM-1, and all 2M tributaries use only 1 x STM-1 out of the two available.

2.5.7 *Comms/Auxiliary/Ancillary Unit*

Access to selected section overhead (SOH) bytes is provided by the auxiliary interface, enabling, for example, low rate external telemetry signals to be carried within the SDH SOH. EOW functionality is provided by an external stand-alone unit, which plugs into the comms/aux/ancillary card.

For details of other comms/auxiliary/ancillary features, refer to the “Subrack Installation Guide”.

2.5.8 SFP Tributary and Line Interfaces

For the OMS 1240 and OMS 1260 products, most of the SDH interfaces are realised in the form of a Small Form-Factor Pluggable (SFP) module. The following table shows the SFP interface types that are available and which cards they are compatible with. The number represents the maximum number of SFPs that can be fitted.

Table 2-2: SFP Interface Types

SE Code	I/F Type	Connector Type	STM-1/4 Core ([1])	STM-4/16 Core ([2])	SDH Multirate ([3])
SU65AA	STM-1 Elec.	1.0/2.3 Coax	2	-	4
SU66AA	STM-1 S1.1	LC	2	-	4
SU66AB	STM-1 L1.1	LC	2	-	4
SU66AC	STM-1 L1.2	LC	2	-	4
SU67AA	STM-4 S4.1	LC	2	1	1
SU67AB	STM-4 L4.1	LC	2	1	1
SU67AC	STM-4 L4.2	LC	2	1	1
SU67AD	STM-4 L4.1+	LC	2	1	1
SU67AE	STM-4 L4.2+	LC	2	1	1
SU68AB	STM-16 S16.1	LC	-	1	-
SU68AC	STM-16 L16.1	LC	-	1	-
SU68AD	STM-16 L16.2	LC	-	1	-

([1]) STM-1/4 Core: 1HAT61105AAF – STM-1/4 Core/CCU

1HAT61114AAT – STM-1/4 Protection Core

([2]) STM-4/16 Core: 03HAT00041AAQ – STM-16 Core/CCU (Core A)

03HAT00041ABH – STM-16 Core (Core B)

([3]) SDH Multirate: 03HAT00043AAU – Quad Flexible STM-1/STM-4 SFP Tributary

The STM-16 ports on STM-4/16 Core cards can also be equipped to interface to a CWDM passive optical multiplexer/de-multiplexer. Table 2-3 and

Table 2-4 list the eight short-haul and eight long-haul SFP modules available, each having a different optical wavelength and each capable of operation at data rates of STM-16.

Table 2-3: Short-Haul SFP Modules for CWDM

SE Code	Function	Bail Colour	Wavelength (Nominal, nm)	STM-4/16 Core (^{2})
SU68CA	λ Channel 1	Grey	1471	1
SU68CB	λ Channel 2	Violet	1491	1
SU68CC	λ Channel 3	Blue	1511	1
SU68CD	λ Channel 4	Green	1531	1
SU68CE	λ Channel 5	Yellow	1551	1
SU68CF	λ Channel 6	Orange	1571	1
SU68CG	λ Channel 7	Red	1591	1
SU68CH	λ Channel 8	Brown	1611	1

Table 2-4: Long-Haul SFP Modules for CWDM

SE Code	Function	Bail Colour	Wavelength (Nominal, nm)	STM-4/16 Core (^{2})
SU68CN	λ Channel 1	Grey	1471	1
SU68CO	λ Channel 2	Violet	1491	1
SU68CP	λ Channel 3	Blue	1511	1
SU68CQ	λ Channel 4	Green	1531	1
SU68CR	λ Channel 5	Yellow	1551	1
SU68CS	λ Channel 6	Orange	1571	1
SU68CT	λ Channel 7	Red	1591	1
SU68CU	λ Channel 8	Brown	1611	1

Chapter 3:
Functional Overview

3.1 Network Management

ServiceOn Optical Element Managers achieve integrated network management control via a Q interface. This allows the OMS 1200 to be managed alongside existing Ericsson products. ServiceOn Access for fixed access radio networks also manages the OMS 1240.

The network management information is carried over a DCC channel contained in the SDH Section Overhead (SOH). The SOH also provides an auxiliary channel for the transport of NM information for crossing Other Licensed Operator (OLO) networks. NM information for third party IP-managed equipment can also be carried across the SDH network by the *IP Tunnelling* feature.

The equipment management operations systems use Ericsson standard workstation terminals for providing management and control of the element.

Software download is achieved from the LCT, or from the ServiceOn Optical Element Managers.

3.2 Synchronisation

The following features are supported:

- The OMS 1200 offers two modes of operation for synchronisation:
  - Single SETG clock
  - Equipment freerun.
- SSMB enable/disable
- Revertive/non–revertive selection
- SSM quality assignment
- SSMB overwrite on STM–n inputs/outputs
- External output squelch on quality threshold
- System clock and external output priority tables
- External output type configuration (2Mbit/s with/without SSM, 2MHz, 1.5MHz)
- STM–n line traffic.

For further details on synchronisation, refer to Chapter 6:.

3.3 Protection

3.3.1 MSP Protection

The MSP function provides protection for the STM-n (n = 1, 4, 16) signal against channel-associated failures within a multiplex section. All possible options specified for the Multiplex Section Protection (MSP) protocol (bytes K1 and K2), as defined in ITU-T/G.841, are used.

The following criteria may be used at the receive end for switching to the protection path:

- Signal Fail (SF) (LOS, LOF or MS-AIS) at section level
- Signal Degrade (SD)
  - USE (Default)
  - CDEG
  - BER (DEG - that is, bit error rate exceeds a pre-set threshold in the range of 10-5 to 10-9).
- Command from the LCT or from the network management system.

3.3.2 Sub-Network Connection Protection

The Sub-Network Connection Protection is defined in ITU-T Rec. G.841.

When OMS 1200 products are connected in a sub network (e.g. a ring topology), the relevant VC to be protected may be protected by transmitting it from the tributary to both STM-n line interfaces. At the receive side; the best quality signal is selected.

The switching between the two directions is based on the following criteria:

- AU/TU AIS and AU/TU LOP alarms (inherent monitoring)
- Error performances (BIP information), payload and routing correctness (Unequipped Signal and Trace Identifier) at the VC level (non intrusive monitoring)
- Command from the LCT or from the network management system.

In this way, the channel is protected against any single failure in the sub network.

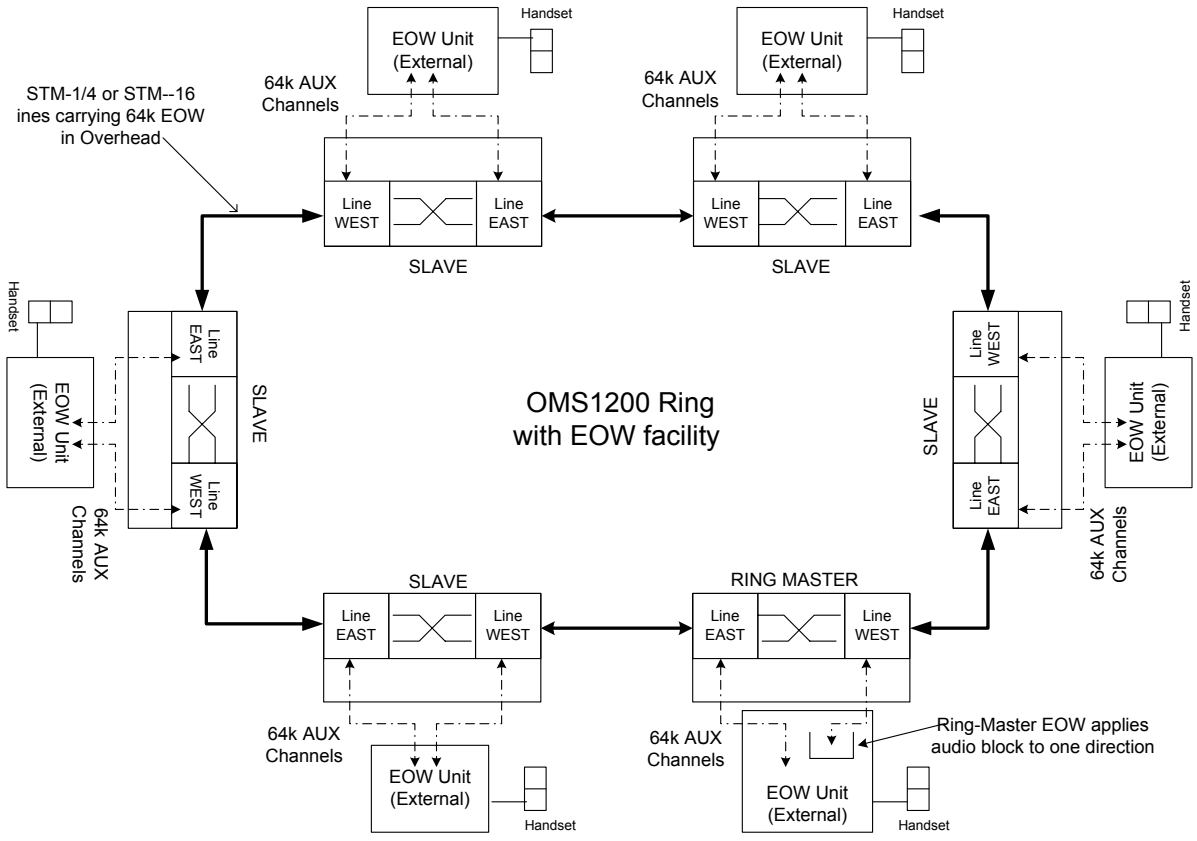
3.4 Cross Connections

Cross-connections can be made for VC-12s, VC-2s, VC-3s and VC-4s. Any allowed mix of VCs can be multiplexed into the STM-1 signal and these VCs can be cross-connected from one timeslot in an incoming STM-1 signal to another timeslot in the outgoing STM-n signal.

3.5 Engineer's Order Wire (EOW)

To provide an EOW facility, an external EOW unit is required. The external EOW unit interfaces to the two 64K Aux channels on the Aux/Ancillary Card. The Aux channel can be selected from one of the configurable section overhead bytes. These overhead bytes can be sourced from either Line or Trib SDH interfaces

Figure 3-1: Engineers Order Wire



3.6 Other Licensed Operator's Networks

Alternative OSI comms channel transport occurs when NEs are sited at remote locations away from an operator's main network. Traffic transmission and management communication with these remote nodes is over another licensed operator's network (OLO network), and the standard SDH OH DCC transport channels cannot be used to carry management information to the remote nodes.

The alternative communications physical channels supported are:

- For STM-n SDH trail interfaces, two Embedded Communications Channels (ECCs) are supported:
  - ECC-F2 at 64kbit/s (G.707, VC-4 POH, F2).
- For VC-12 SDH trail interfaces a single ECC is supported:
  - ECC-TS 9 at 576kbit/s (G.704, PDH 2048kbit/s, TS 1 – TS 9).

The SOH also provides an auxiliary channel for the transport of network management information for crossing OLO networks.

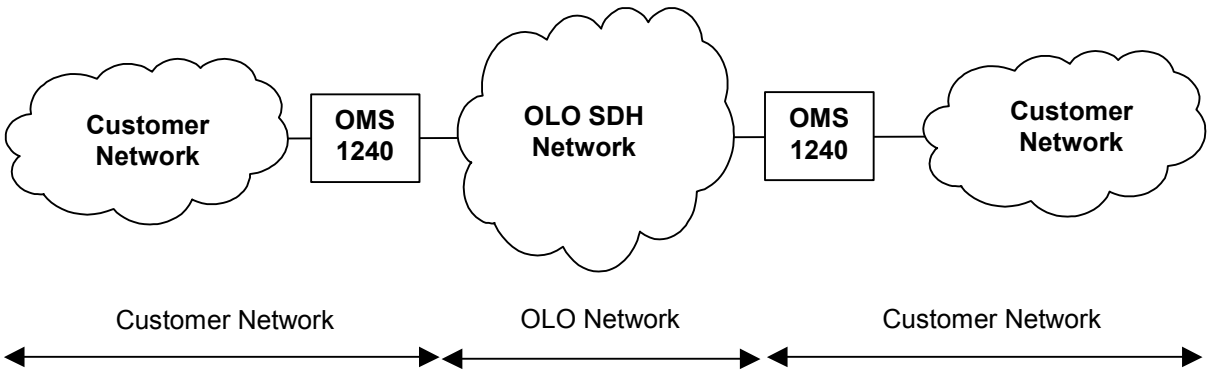
Note: For the OMS 1260 equipment only, Comms/OH access is only available on Port #1 of the Dual STM-1e Trib.

When the OMS 1240 is used in the customer premises connected via leased line from another operator or connecting via SDH equipment where the normal DCC cannot be used, the F2 byte in the path overhead is used to carry the management communications traffic. It is a configurable option; if selected it enables the selection an AUX channel (F2 byte associated with a VC-4) and then uses this for the transport of management comms (which is normally carried over a DCC link).

For the above application, the solution is being used for user communications purposes between path elements (the operator is a user in this context who is a client of the OLO providing a VC-4 link).

It is assumed the leased line is carried over the OLO's SDH network; the OLO does not have access to data channels in STM-n overheads to carry management traffic.

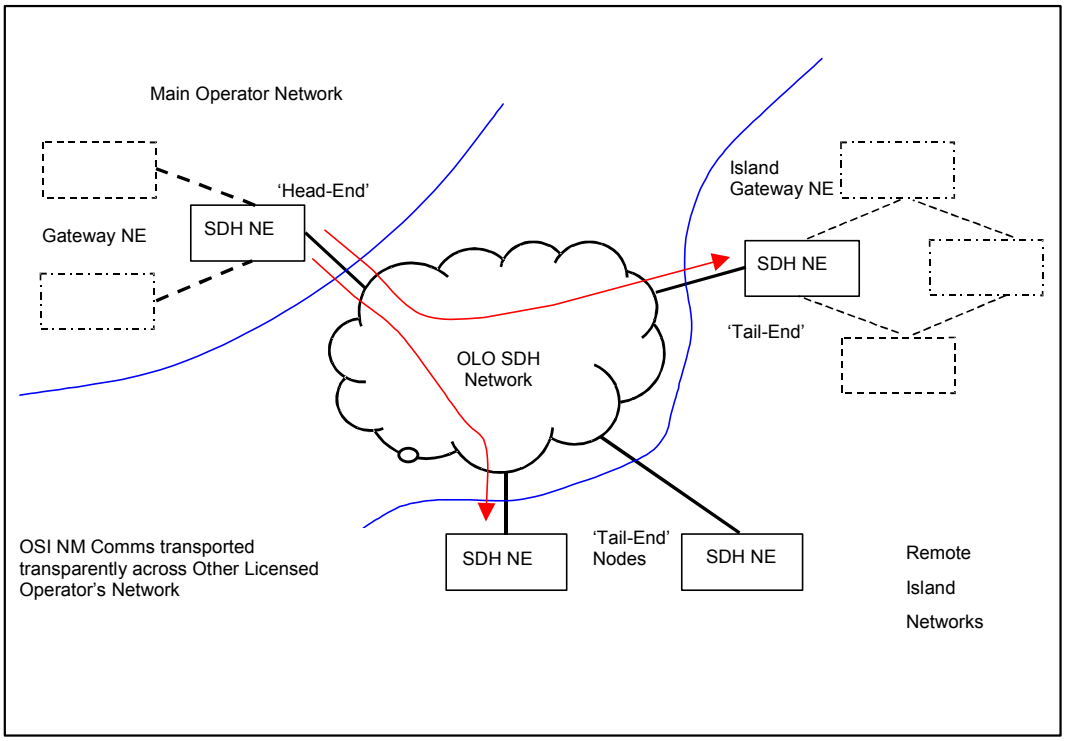
Figure 3-2: Off-Net Customer Network Configuration



3.6.1 Remote Management via VC-12 n x 64kbit/s Comms Channels

In equipment release 3.4, the OMS 1200 provides for alternative OSI Comms Channel Transport over Other Licensed Operators (OLO) Networks using a VC-12 traffic path.

Figure 3-3: Example of Remote Management over OLO Network



Referring to Figure 3-3, if the Gateway NE and Tail End NE have VC-12 trail termination traffic interfaces, a selected VC-12 trail could be used to carry management comms data. Leasing the VC-12 will give transparent transport across the OLO network.

This may be desirable if an operator does not wish to pay the premium of leasing a full VC-4, however this will be at the cost of losing a VC-12, which could otherwise be carrying revenue-earning traffic.

Similarly, if the main network 'Gateway NE' and the 'Island Gateway NE' each have VC-12 trail termination traffic interfaces, then again a selected VC-12 trail could be used to carry management comms data between them across the OLO network.

In these scenario the three Comms NE types are as follows:

- A main network 'Gateway NE' type which will operate as a 'head-end' distribution node for VC-12 n x 64kbit/s comms routing to a number of remote nodes across the OLO network
- An isolated 'Tail-end NE' type which solely operates as a 'tail-end' node for VC-12 n x 64kbit/s comms.
- An 'Island Gateway NE' type which operates as a 'tail-end' node for VC-12 n x 64kbit/s comms, with conversion back to SDH DCC comms for onwards routing within the island network.

The OMS 1200 supports the 'Tail-end NE' type and the 'Island Gateway NE' type in these applications. A single 2Mbit/s PDH traffic signal carrying management comms data is extracted by the Core Trib card port-32 OMS 1240 equipment) or a selected Trib Card port-32 OMS 1260 equipment), and is selectively configured for switching onto the Aux / Ancillary Unit (not the associated traffic LTU). A traffic processing function of the Aux/Ancillary Unit recovers the nx64kbit/s comms data (where n = 9 providing a 576kb/s comms channel) and feeds this to/from the CCU cards communications processor.

Different NE products, such as Ericsson's OMS1664 range of equipment, would usually support the main network 'Gateway NE' type application. However, for a single Node-point-to-Node-point comms routing scenario, the OMS 1200 family could operate as head-end in the operator's main network, and tail-end in a remote' island' of that network.

3.7 IP Management of Third Party Co-Located Equipment

The management of SDH equipment is usually achieved using OSI protocols.

The situation can arise in networks where third party equipment uses IP protocols for its management. This situation is very often resolved by creating a completely separate Data Communications Network (DCN) for this IP-managed equipment.

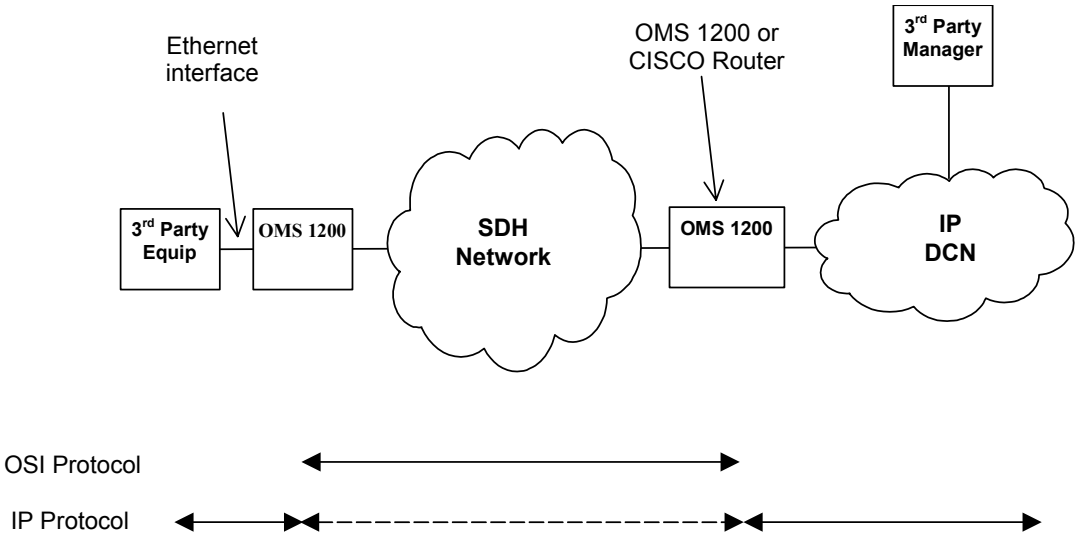
The feature of IP tunnelling allows this IP management traffic to be carried over the existing OSI SDH DCN.

The IP tunnelling feature is required at either side of the SDH network, firstly co-located with the third party equipment where the connection is through the Ethernet 'Q' interface of the SDH element.

The second location is at the site of the IP manager of the third party equipment (or through an IP path to that manager). The equipment at the second location can be either another OMS 1240, OMS 1260 or a CISCO™ router.

The OMS 1240 or OMS 1260 can terminate up to 10 tunnels.

Figure 3-4: IP Management of Third Party Co-Located Equipment



3.8 Tandem Connection Monitoring (TCM)

All SDH cards support TCM sub-layer performance monitoring (full TCM).

Blank Page

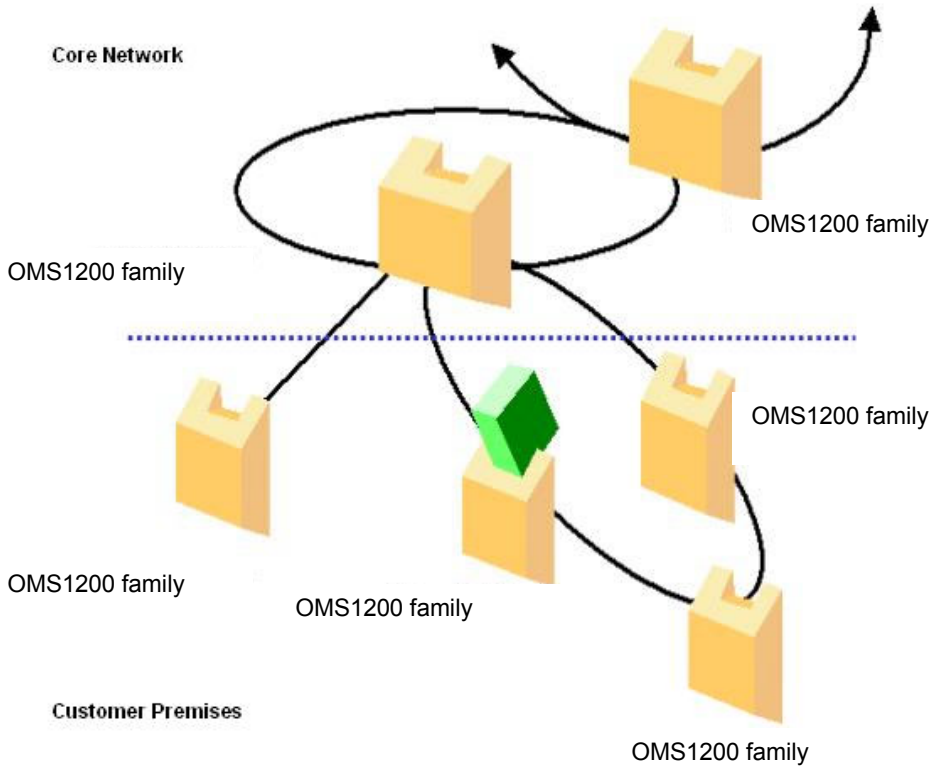
Chapter 4:
Typical Applications

4.1 Network Applications

4.1.1 General

The OMS 1200 can be deployed, as Network Termination Equipment (NTE), on customer premises. Applications include campus rings and multi-tenanted buildings. It is deployed either as a terminal, in hubbing architectures, or as a ring based ADM. Traffic protection may be employed for both these applications, 1+1 Multiplex Section Protection (MSP), Sub Network Connection Protection (SNCP) or Multiplex Section Shared Protection (MS-SPRING).

Figure 4-1: Network Configurations



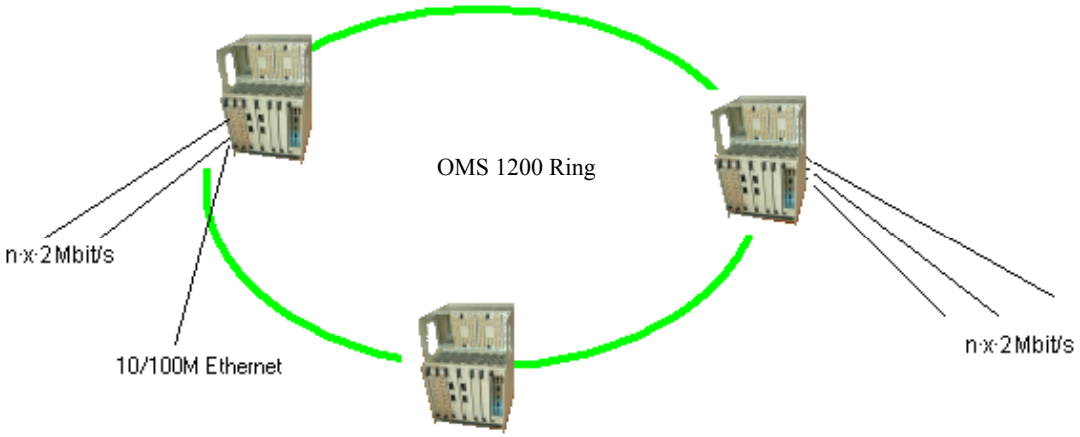
The OMS 1200 can also be deployed in mobile radio networks for the collection and consolidation of traffic from radio base stations. Other applications are deployment within the access network, particularly in enclosed cabinets.

Example applications include telephony where the product is deployed alongside primary multiplexers, delivering narrow-band services to residential customers.

4.1.2 Ring Application

OMS 1200 equipment provides a number of Trib options, VC-12, VC-3 and VC-4. This single box solution reduces network complexity, saves costs, space and operation effort.

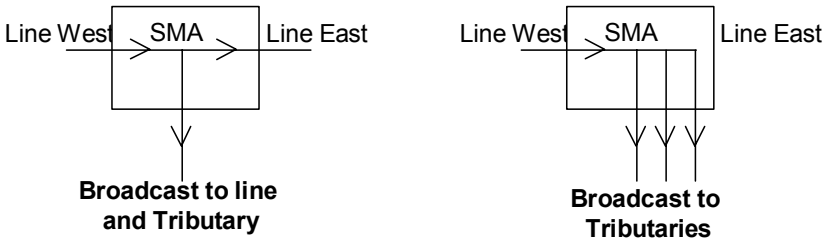
Figure 4-2: Ring Applications



4.1.3 Broadcast

Broadcast supports point to multi-point, unidirectional, transmission of circuits. One of the main applications is in the delivery of video and television signals. There are two basic configurations for broadcast. Firstly, where a signal is received and passed through to a line port whilst being switched to a tributary port. Secondly, where the signal is received at a line port and is switched to several tributary ports.

Figure 4-3: Broadcast



4.2 Point to Point

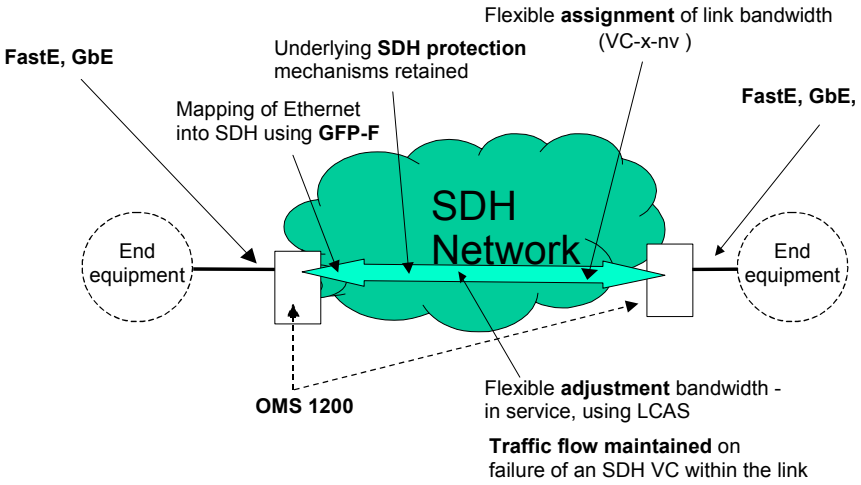
Although intended as a solution for integration within an SDH network, the OMS 1240 can also be used for point-to-point systems. This configuration can be used to support PDH/SDH rates such as 2Mbit/s leased lines, direct connection to PBXs and data.

4.3 Data Applications

4.3.1 Ethernet Private Line

Ethernet Private Line (EPL) is also known as Transparent LAN service. This application is supported for 10/100M Ethernet signals. Based on multi-port Ethernet interfaces more than one connection can be established from one end to the other. Each packet arriving from end user LAN is mapped via GFP or Link Access Procedure – SDH (LAPS) into SDH-leased line. The transfer capacity may be a fixed or flexible leased line, resized via Link Capacity Adjustment Scheme (LCAS). For each connection, one VC-group is used.

Figure 4-4: Ethernet Private Line



4.4 Network Management Channel Communications Configuration

In general, across the product family all currently available SDH line and tributary port interfaces support embedded communications channels (DDCm/DCCr).

See 4.4.1 and 4.4.2 for more detailed information on which communications channels are supported by the various SDH Tributary cards available in the OMS 1200.

4.4.1 OMS 1240 Product

Legacy Quad STM-1 Optical/Electrical Card

- Does not support F2 OLO comms over any of its STM-1 bearers
- Can support comms over the conventional DCCr/DCCm channels (DCCr on Ports 1 and 2, DCCm on Ports 3 and 4).

STM-1/4 Multirate Tributary

When configured as Quad STM-1, the STM-1/4 Multirate Tributary supports:

- DCCr on Ports 1 and 2, or F2 on Ports 1 and 2
- Only DCCm on Ports 3 and 4.

Note: When configured as Dual STM-1 or STM-4, all DCC/F2 comms channels are available.

4.4.2 OMS 1260 Product

For the STM-1/4 core cards, the OMS 1260 is only designed to support Comms/Aux transport via tributary cards in Slots 4 and 5 (only these have internal system OH-busses). There is no comms support via Slots 1, 2 or 3.

The STM-4/16 core cards have overhead bus connections to all seven generic tributary slots.

Legacy Dual STM-1 Electrical Tributaries:

These cards only support comms on Port #1. No comms channels are available on Port #2.

STM-1/4 Multirate Tributary

When configured as Quad STM-1, the STM-1/4 Multirate Tributary supports:

- DCCr on Ports 1 and 2, or F2 on Ports 1 and 2
- Only DCCm on Ports 3 and 4.

Note: When configured as Dual STM-1 or STM-4, all DCC/F2 comms channels are available.

Chapter 5:
Power Consumption

5.1 OMS 1240 Power Consumption

The maximum power consumption of the OMS 1240 is 180.5W. This value is attained with the configuration shown in Table 5-1, with a power supply voltage of 55Vdc and high inlet air temperature causing the fans to run at full speed.

For information on the Battery Box Unit see 03PHB00002AAR AC Power & Battery Back-up Unit.

5.2 OMS 1260 Power Consumption

The maximum power consumption of the OMS 1260 is 348.5W. This value is attained with the configuration shown in Table 5-1, with a power supply voltage of 55Vdc and high inlet air temperature causing the fans to run at full speed.

Table 5-1: OMS 1200 Power Consumption

Cards/Unit configuration	OMS 1240	OMS 1260
STM-4/16 Core/CCU	25W	25W
STM-4/16 Core	22W	22W
Power LTU	0.5W	0.5W
Generic power LTU (1)	7.2W	5.3W
Generic power LTU (2)	7.2W	5.3W
Generic power LTU (3)	-	5.3W
Generic power LTU (4)	-	7.2W
Generic power LTU (5)	-	7.2W
Generic power LTU (6)	-	7.2W
Generic power LTU (7)	-	7.2W
2M core tributary (worker)	18W	-
2M core tributary (protection)	4W	-
Comms/aux/ancillary	12W	12W
Trib Card - (1)	34W	25W
Trib Card - (2)	34W	25W
Trib Card - (3)	-	25W
Trib Card (4) - Layer 2 card (1)	-	34W
Trib Card (5) - Layer 2 card (2)	-	34W
Trib Card (6) - Layer 2 card (3)	-	34W
Trib Card (7) - Layer 2 card (4)	-	34W
Fan Tray - (1)	16.5W	16.5W
Fan Tray - (2)	-	16.5W
Totals	180.5W	348.5W

Blank Page

Chapter 6: Synchronisation

6.1 Timing Sources

Timing signals can be derived from the following sources:

- **External sources** – from PDH or SDH Tributary Cards, or via the dedicated External 1 or 2 clock inputs on the Comms/Aux/Ancillary Card.
- **Line interfaces**
- **Internal oscillator -** Freerun mode (default condition at commissioning).

A source may be nominated by including it in a timing sink priority table.

6.2 Synchronisation Modes

The system can be configured to operate in Freerun or Single SETG Timing Modes.

Note: The defaults stated in each subsequent section exist if the NE is declared operative without configuring synchronisation.

6.2.1 Freerun

In Freerun mode, the system clock, external outputs and all SDH line/tributary outputs are synchronised to the highly stable internal oscillator on the Core Card. Only configuration options described in Sections 6.3, 6.10 and 6.12 have any effect in Freerun mode.

Note: Default: Freerun.

6.2.2 SETG Timing

In SETG Mode the NE is capable of deriving timing, from a choice of inputs:

- Incoming STM–N line interfaces.
- Tributary ports: either STM–N, 140 Mbit/s, 34/45 Mbit/s or 2 Mbit/s.
- Two external input timing signal ports.

The selection of timing sources is performed by using a priority table.

Single SETG clock mode is provided in accordance with ITU and ETSI specifications where a single clock is selected to time the SETS clock within the SDH equipment. All STM-n line and tributary outputs are then timed from this clock.

6.2.3 Holdover

This is a standby mode that comes into operation automatically if all input timing sources fail, it is not operator initiated. The output frequency is held within close limits to that set by the last used timing source.

6.3 Timing Marker Operation

The quality level of a timing source is normally determined from the received SSMB timing markers or by Operator configuration. An operator can choose to ignore the received timing markers on a ‘global’ basis, and select timing sources by priority only if timing marker operation is disabled. When disabled the "Default SSMB" code shall be transmitted on all outputs supporting SSMB.

Timing marker operation is used to eliminate problems associated with synchronisation timing loops. The configurable destination ID description for interconnecting STM-n interfaces are compared, and a ‘do not use’ SSMB marker is set to downstream NEs if they are found to be the same.

Note: Default: - Timing Marker Enabled.

6.3.1 Destination ID

The destination ID for each STM-n can be configured. This is a text string of up to 52 characters. The SSMB associated with the interface can also be overwritten.

Note: Default: - card and port ID (e.g. Line East A).

6.4 Revertive/Non-revertive Operation

The equipment may be configured for revertive or non-revertive operation.

Note: Default: - Revertive.

6.5 Wait to Restore Period

A wait-to-restore period is entered following restoration of a failed source, before the quality level is returned to the original value or becomes available. When timing marker operation is enabled, a change in SSMB value does not initiate a wait-to-restore period. The wait-to-restore period can be set from zero to 30 minutes (in 30-second increments).

Note: Default: - 1 minute.

6.6 Priority Table Options

In SETG mode, you can configure two priority tables, one for equipment clock sink and one for external output sink.

Assigning a clock source to a priority table defines it as a nominated source. The entries may be chosen from any of the sources listed in Table 6-1, Table 6-2, Table 6-3 & Table 6-4.

Table 6-1: OMS1240–4 Sync Priority Options

Source	Equipment Clock	External Output
Core 1-9:1 SDH line recovered clock - West A	Yes	Yes
Core 1-9:2 SDH line recovered clock - East A	Yes	Yes
Core 1-8:1 SDH line recovered clock - West B	Yes	Yes
Core 1-8:2 SDH line recovered clock - East B	Yes	Yes
Ext/Trib clock	Yes	-
System clock	-	Yes
SASE Equipment clock	-	Yes

Table 6-2: OMS1240–16 Sync Priority Options

Source	Equipment Clock	External Output
Core 1-9:1 SDH line recovered clock	Yes	Yes
Core 1-8:1 SDH line recovered clock	Yes	Yes
Ext/Trib clock	Yes	-
System clock	-	Yes
SASE Equipment clock	-	Yes

Table 6-3: OMS1260-4 Sync Priority Options

Source	Equipment Clock	External Output
Core 1-26:1 SDH line recovered clock - West A	Yes	Yes
Core 1-26:2 SDH line recovered clock - East A	Yes	Yes
Core 1-25:1 SDH line recovered clock - West B	Yes	Yes
Core 1-25:2 SDH line recovered clock - East B	Yes	Yes
Ext/Trib clock	Yes	-
System clock	-	Yes
SASE Equipment clock	-	Yes

Table 6-4: OMS1260-16 Sync Priority Options

Source	Equipment Clock	External Output
Core 1-26:1 SDH line recovered clock	Yes	Yes
Core 1-25:1 SDH line recovered clock	Yes	Yes
Ext/Trib clock	Yes	-
System clock	-	Yes
SASE Equipment clock	-	Yes

Only configured cards may be selected as timing sources in the priority tables.

Table 6-5:Defaults:

External Output Sink Priority Table:	System Equipment clock = 1
	All other sources = none
Equipment Clock Sink Priority Table:	All sources = none

6.7 Ext/Tributary Clock Selection

Two external timing sources and a third tributary card timing source can be selected in the External/Trib timing clock priority tables in Section 6.6. The tributary card timing sources can use either a generic SDH tributary card or a generic PDH tributary card.

Note: Default: None selected.

6.7.1 OMS1240 Tributary Selection

One of the ports from the two generic tributary slots, or two core tributary slots may be chosen as the tributary synchronisation input.

Only configured cards may be selected as timing sources in the priority tables.

Note: Default: None selected.

6.7.2 OMS1260 Tributary Selection

One of the ports from the five generic tributary slots in OMS1260-4, or one of the ports from the seven generic tributary slots in OMS1260-16 may be chosen as the tributary synchronisation input.

Only configured cards may be selected as timing sources in the priority tables.

Note: Note: Default: None selected.

6.8 SDH Timing Sources

The SDH timing source quality level is normally determined from the received SSMB timing markers. It is also possible to choose to ignore the received timing markers and assign a fixed SSMB value to be used instead.

Note: Default: Use received SSMB to determine quality level.

6.9 PDH Timing Sources

The SSMB code (and associated implied quality level) for PDH tributary clocks must be assigned, if timing marker operation is enabled.

Note: Default: Tributary Clock Quality Levels: 16 (Undefined, SSMB=0000).

6.10 External Timing Input

The input clock frequency and type are configurable from the following options:

- 1.5MHz Clock
- 1.5Mbit/s G.703, unframed
- 2MHz Clock
- 2Mbit/s G.703, unframed
- 2Mbit/s G.703, framed with SSMB
- 2Mbit/s G.703, framed

Note: Default: 2Mbit/s G.703, unframed

6.10.1 External Timing Quality levels

If timing marker operation is enabled the quality levels for external clocks and data signals not supporting SSMB must be assigned, as described in Section 6.12.

Note: Default:

Ext 1 Clock Quality Level: 1 (PRC, SSMB=0010)

Ext 2 Clock Quality Level: 1 (PRC, SSMB=0010).

6.10.2 External Input SSMB position

The SSMB position can to be specified in positions 4, 5, 6, 7 or 8 in external 2Mbit/s framed SSMB mode. The quality level is determined from the received SSMB. The operator can also configure a fixed SSMB value and the received SSMB value is ignored.

Note: Default: bit position is 8.

Note: Default: Use received SSMB to determine quality level.

6.11 External Timing Output

The output clock frequency and type are configurable from the following options:

- 2Mbit/s G.703, framed with SSMB operation
- 2Mbit/s G.703, framed without SSMB operation
- 1.5MHz Clock
- 2MHz Clock

Note: Default: - 2MHz G.703.

6.11.1 External Output SSMB position

The SSMB position can to be specified in positions 4, 5, 6, 7 or 8 in external 2Mbit/s framed SSMB mode.

Note: Default: bit position 8.

6.11.2 External Output off State

The external timing output will switch off when the source quality level falls below a certain threshold or all sources are unavailable. There are three types of off state, which can be configured:

- High impedance
- 0V
- DC offset.

Note: Default: 0V

6.12 Default SSMB

The transmitted SSMB timing marker value can be configured for all output ports when in equipment Freerun mode, or when timing marker operation is disabled, as described in Section 6.3. Any of the SSMB codes in Table 6-6 may be configured.

Table 6-6: SSMB Timing Marker from MSOH S1 Byte (Defaults)

Serial	SSMB code bits: 5 6 7 8	Quality	Description
1	0 0 0 0	16	Quality unknown (treated as Undefined)
2	0 0 0 1	16	Undefined
3	0 0 1 0	1	Traceable to G.811
4	0 0 1 1	16	Undefined
5	0 1 0 0	2	Traceable to G.812 transit clock
6	0 1 0 1	16	Undefined
7	0 1 1 0	16	Undefined
8	0 1 1 1	16	Undefined
9	1 0 0 0	3	Traceable to G.812 local clock
10	1 0 0 1	16	Undefined
11	1 0 1 0	16	Undefined
12	1 0 1 1	4	Traceable to G.813 clock
13	1 1 0 0	16	Undefined
14	1 1 0 1	16	Undefined
15	1 1 1 0	16	Undefined
16	1 1 1 1	16	Not to be used for synchronisation

Note: Default: - 1011 (G.813).

6.13 SSMB Code to Quality Level Assignment

Quality levels between 1 and 16 may be configured against each SSMB code. One (1) is the highest quality level. Only the codes assigned by the operator may be used when performing the configuration described in Sections 6.9, 6.11.1.

Note: Defaults: - as Table 6-6.

6.14 SASE Mode

The equipment can be configured in Stand Alone Synchronisation Equipment mode (SASE) or one of the Enhanced SASE Modes (ESM). An external SASE regenerator is used to clean the timing signal on the T4 output before it is fed back into the T3 input.

- Options:

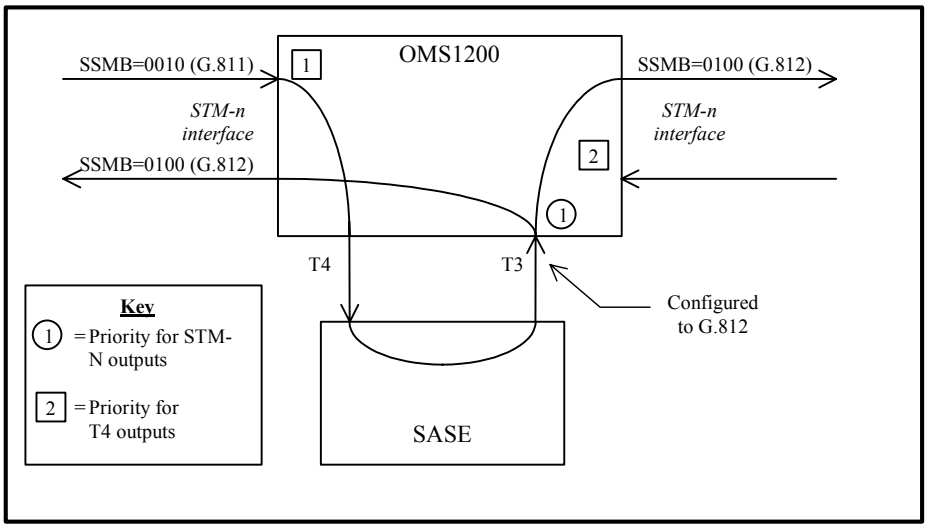
- SASE Mode
- ESM Input 1
- ESM Input 2
- ESM Inputs 1 and 2
- Disabled.

Note: Default: SASE Mode Disabled.

6.14.1 SASE Mode disabled

The OMS 1200 uses the T3 timing source to time the SDH interfaces. The S1 byte of the SDH interfaces indicates the operator assigned SSMB quality of the T3 input signal.

Figure 6-1: SASE Mode Disabled

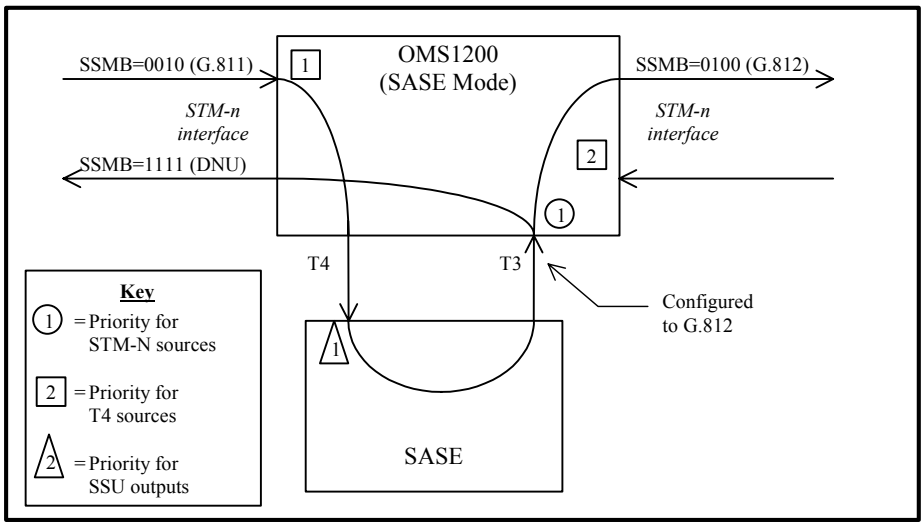


The SASE does not forward the correct SSMB value from SDH input interface to SDH output interface. It also fails to indicate that the synchronisation source has been looped back. This could, in certain situations, lead to the creation of a timing loop in the network. These problems lead to the introduction of the 'SASE' Mode operation.

6.14.2 SASE Mode

In SASE Mode the OMS 1200 overwrites the outgoing STM-n SSMB in the direction that provided the T4 source with a Do-Not-Use (DNU) SSMB. However, if the quality of the received timing source decreases, the transmitted timing source will still continue to carry the configured SSMB.

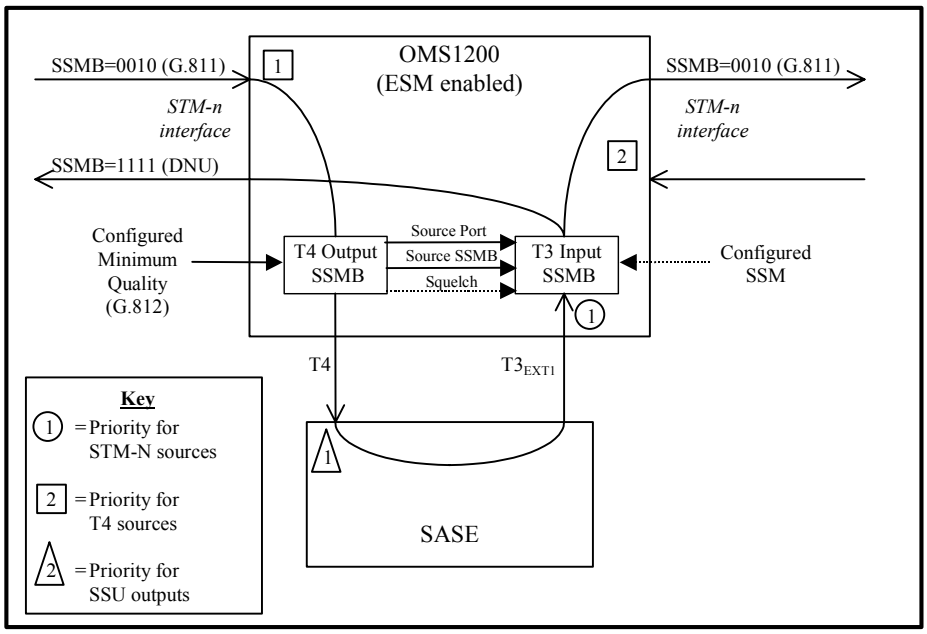
Figure 6-2: SASE Mode



6.14.3 Enhanced SASE Mode

In Enhanced SASE Mode (ESM) the T3 input SSMB is dynamically set according to the received SSMB on the selected T4 source. The “Source Port” and “Source SSMB” information is passed directly to the T3 input. This information is then used to generate the SSMBs for the SDH STM-n interface outputs synchronised to the T3 input.

Figure 6-3: Enhanced SASE Mode



In ESM, if all the configured T4 sources fall below the minimum quality threshold (e.g. G.812) the T4 output will be squelched and this is signalled internally to the T3 input using the “Squelch” control line. This causes the T3 input to ignore the source information received from T4 and instead it uses the operator configured SSMB value for transmission on STM-n interfaces.

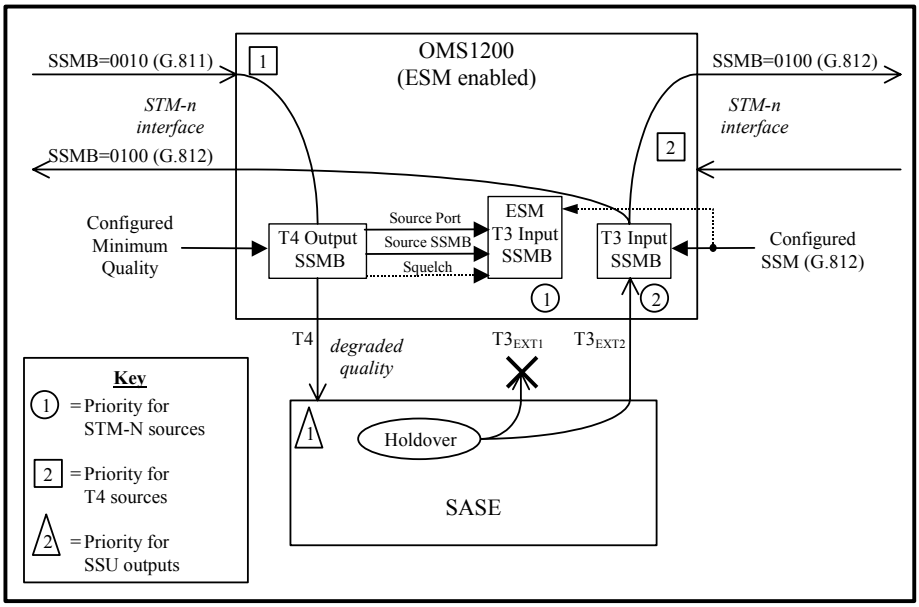
6.14.4 Enhanced SASE Mode on External 1/2

The SASE will enter holdover mode (G.812) if it rejects the timing source from the T4 output because of poor phase/frequency performance. However, no indication will be passed back to the T3 input of the OMS 1200.

ESM can be configured on only one of the T3 inputs to overcome this problem. The other T3 input operates as a normal timing source. In this mode the SASE needs to be able to control its outputs independently.

In the diagram below the SASE rejects the quality of the T4 clock from the OMS 1200 and in response it squelches one of its outputs. The squelched output would normally feed the T3 external input 1 and in its absence the OMS 1200 selects the second priority source (external input 2). The configured value for T3 SSM decides the SSMB that is transmitted on STM-n interface outputs locked to the external 2 input.

Figure 6-4: Enhanced SASE Mode on External 1/2



6.15 2Mbit/s De-Synchroniser Bandwidth

The jitter bandwidth for the 2Mbit/s through data is determined by the bit justification bandwidth of the de-synchroniser. Either normal or narrow bandwidth can be configured on an equipment basis.

Note: Default: Normal.

6.16 SDH Port SSMB Override

The SSMB value for each SDH port has the option to set on a per port basis.

Any of the 16 permitted SSMB values may be configured.

Note: Default: Not configured.

6.17 Card Configuration

The OMS 1200 cards require configuration data to enable the timing/synchronisation scheme to operate. The configuration data required by each card is detailed below.

6.17.1 Core Card Configuration

The micro-controller sets up selectors as instructed by the CCU. These selections are held until a new configuration is written. The external input and output conditions are set up as selected in Sections 6.10 and 6.11.

6.17.2 Controller/Comms Configuration

Controller and comms functions are on the Core/CCU Card. Operator configuration is as defined in Section 6.2. Non-volatile storage of the current configuration, including priority tables, on the Core Card allow operations to continue following shelf power down without the need for reconfiguration.

6.17.3 PDH Tributary Card

PDH tributary cards are configured as part of the selection mechanism for the equipment.

6.17.4 Synchronisation Configuration on Reset

The following default configuration occurs for each card on power-up of the shelf, or on insertion of a card into a powered shelf.

The controller function restores the configuration contained in non-volatile memory on the SMC. Until the configuration is restored or before the equipment is declared operative, the controller function takes no action and individual card power up states persist.

During power up of the Core Card(s), the micro-controller disables all clock sink outputs and the equipment clock selects Freerun. The external timing outputs are disabled in tri-state mode. The card then awaits configuration by the controller function.

All SDH tributary cards power up in on-card Freerun mode. Timing bus outputs are also disabled and the ‘Do Not Use for Synchronisation’ SSMB timing marker code is transmitted. The card then awaits configuration by the controller function.

The PDH line and tributary cards power up with timing bus outputs disabled. The card then awaits configuration by the controller function.

Chapter 7: Protection Schemes

7.1 Introduction to Protection

Equipment protection and network protection is used to prevent traffic errors due to single points of failure.

This chapter describes the behaviour of the protection schemes implemented in the OMS 1200 equipment.

The protection schemes supported by the OMS 1240 and the OMS 1260 are shown in Table 7-1:

Table 7-1: Protection Mechanisms

Protection scheme	OMS 1240	OMS 1260
1 + 1 MSP	✓	✓
SNCP.	✓	✓
MS-SPRING*	✓	✓
Switch Protection	✓	✓
1:N Card Protection (PDH & STM-1 Elec.).	✓	✓
PDH Port Protection.	✓	✓

* MS-SPRING only available with STM4/16 Core cards

7.2 General Protection Information and Architecture Rules

The same protection schemes apply in OMS 1200 family equipment, but because of the increased size of the OMS 1260 rack and available bandwidth slots, the position of the protection cards must be located as described.

7.2.1 OMS 1240 Protection Rules

7.2.1.1 Core and Core Tributary Protection

The OMS 1240 provides two slots for Core cards, designated A and B, and two slots for 2Mb/s Core Tributary cards, also designated A and B. Unprotected systems use the “A” slots only - the “B” slots are used for protection.

Core cards are fitted in slots S1_03 (Protection Traffic Core B) and S1_04 (Traffic Core A/CCU).

The 2M core tributary associated with Core A/CCU is fitted to Slot S1_06 (Core Tributary A). The 2M core tributary associated with Traffic Core B is fitted to Slot S1_05 (Core Tributary B).

The equipping rules for these four slots are inter-dependent, and are defined in Table 7-2.

There are two variants of Core Tributary card:

- 1HAT61107AAK – Original 2Mb/s Core TRIB
- 1HAT61107ABC – Enhanced 2Mb/s Core TRIB

Note: These cards differ only in their slot equipping rules for Core Protection as defined in Table 7-2.. With the 1HAT61107ABC variant, Core Trib B does not need to be fitted if 2Mbit/s protection is not required.

The AAK variant is now obsolescent, the ABC variant is preferred.

Table 7-2: OMS 1240 Protection Configuration Options

Protection Options	Config				
		Core A	Core B	Core TRIB A	Core TRIB B
Unprotected Core Unprotected 2M Core Trib	A	✓		AAK or ABC	
Protected Core Unprotected 2M Core Trib	B	✓	✓	ABC	
Protected Core Protected 2M Core Trib[123]	C	✓	✓	AAK or ABC	AAK or ABC

Notes:

1 When protecting the Core, if Core TRIB A is an AAK variant then Core TRIB B must be installed and can be either variant.

2 A Core TRIB card cannot function without its associated Core card, thus Core B must be installed to support Core TRIB B.

3 If Core TRIB A is an AAK variant then it is not possible to upgrade from Config. “D” or “E” to Config. “B” without some level of 2M traffic loss. The sequence necessary to minimise traffic hits is:

- Force switch 2M traffic to B (short burst of traffic hits)
- Replace Core TRIB A with an ABC variant
- Force switch 2M traffic to A (short burst of traffic hits)

- Remove Core TRIB B

7.2.1.2 Generic Tributary Protection

The Generic Tributary card in slot S1_02 can either operate independently or be used to protect an identical Tributary card in slot S1_01. In either case, both Generic Tributary cards must be supported by the appropriate Generic Tributary LTU card.

To operate as a protected pair the Generic Tributary cards must use connections to the network via the Generic Tributary LTU in slot S3_01. The LTU in slot S3_02 then provides only power to the protection Tributary in Slot S1_02 plus protection traffic routing from S1_02 to S3_01.

Generic Tributary protection is totally independent of Core and Core Tributary protection.

7.2.2 OMS 1260 Protection Rules

7.2.2.1 Core Cards

The core card in slot S1_07 may have a protection card in slot S1_06. Trib card protection and Core card protection are independent: it is therefore possible to have protected core and unprotected TRIBs and vice-versa.

Table 7-3: Slot Position Rules for OMS 1260 Core Card and Protection Options

Slot S1_ …														
01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**
Core card protection rules. See notes below.														
						UP								
					P	CW								
	UG				P	CW								
	G		GP		P	CW								

Note: 1: CW=Core Worker card, P=Protection card, UP=Unprotected core card, G=Generic tributary card, GP=Generic tributary protection card, UG=Unprotected generic tributary card.

Note: 2: See also Table 7-4 for generic tributary card protection and 2M card protection options respectively.

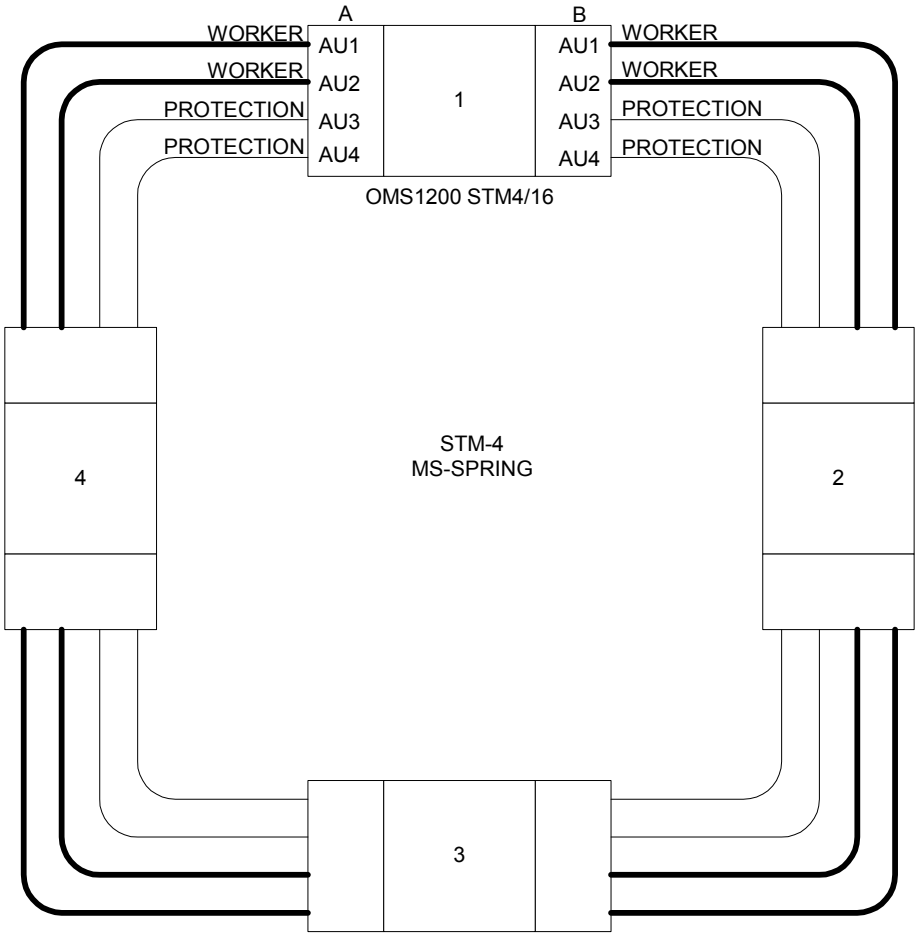
Protection Rules

- Core A must be fitted
- Core B provides switch protection and additional Line interface(s), which may be used to protect Core A Line(s)
- Core Protection is independent of Trib protection

Possible Types of Protection

- 4/16-Core Ring (MS-SPRING line protection)

Figure 7-1: 4/16-Core Ring (MS-SPRING Protection)

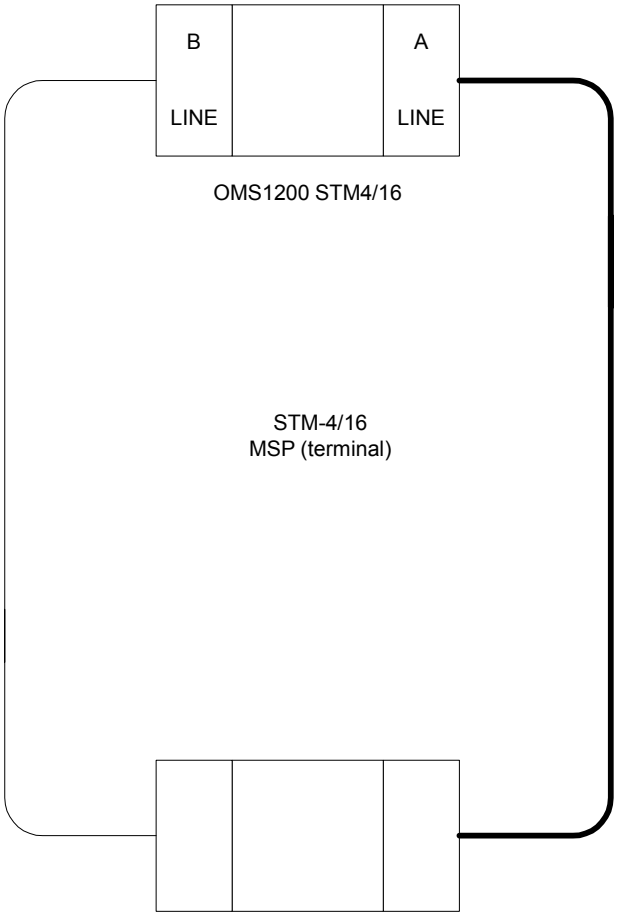


In this example shown in Figure 7-1 the ring is protected using MS-Spring. In this case Core A Line and Core B line provide both worker traffic and protection traffic.

Note: This configuration can only be achieved with the STM 4/16 core card)

- 1/4 –Core Ring (MSP line protection).

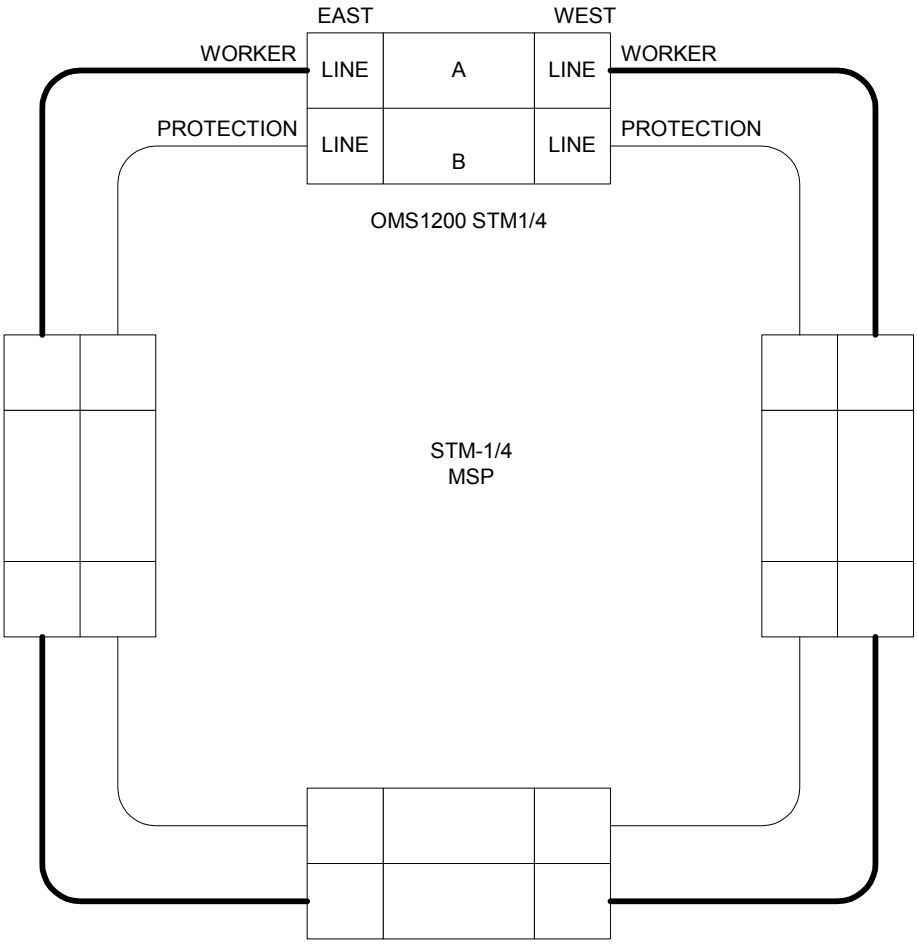
Figure 7-2: 4/16-Core Ring (MSP Line Protection)



In this example shown in Figure 7-2 MSP is configured for the line interfaces. Core B then acts as a protection card and does not carry normal worker traffic. MSP can only be used for Terminal applications.

- 1/4-Core Ring (MSP line protection)

Figure 7-3: 1/4 Core Ring (MSP line protection



In this example shown in Figure 7-3 MSP is configured on the STM-1/4 core card. The Core B card acts as a Protection card and does not carry normal worker traffic.

7.2.2.2 Tributary Cards

In addition to the rules in Section 7.2.2.1, the following slot positions must apply where generic tributary cards are used.

Generic tributary cards are located in numerically adjacent slots, with the protection card in the next available slot to the right, jumping the core and protection cards and the blank slot. Generic tributary cards can be arranged in groups, with each group having its own generic tributary card protection. See Table 7-4.

Rules

- Unprotected generic Trib cards can be fitted in any generic Trib slot.
- For 1+1 protection groups the protection trib must be fitted in the next generic trib slot to the right of the worker

- For 1:N protection groups the protection trib must be fitted in the next generic trib slot to the right of the worker group. Workers must be fitted in adjacent generic trib slots.
- It is possible to have multiple 1:N protection groups. Each group has a dedicated protection trib.

Possible Types of Protection

- Unprotected Tribs (all different types)
- 1+1
- 1:N (1:6- i.e max)
- Multiple 1:N (protection other side of Core Cards)
- Multiple protection groups including 1:1 and 1:N

Single and Multiple Group Generic Tributary Card Protection Rules

OMS 1260 generic tributary cards can be organised in groups, where each group has a protection card. See Table 7-4.

Table 7-4: Slot Position Rules for OMS 1260 Generic Tributary Cards and Protection Options

	Slot S1_ …														
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**
	Single group generic tributary card protection examples. See notes below.														
1		U		U					U		U	U	U	U	
2		W		P					N		N	N	N	N	
3		W		W					W		W	W	W	P	
4		W		W					P		W	W	W	P	
5		W		P					W		P	W	W	P	

Note: 1: Key: W=Worker card, P=Protection card, U=Unprotected card, N=Not fitted

Note: 2: The protection card must be fitted to the right of the card or group of cards which it is protecting.

Table 7-5: Slot Position Rules for Generic Tributary LTUs and 2M Balanced LTUs

Trib Description		**Trib Slot Number**	**LTU Description**	**LTU Slot Number**
Tributary Group 1	2M Trib 1 (ports 1-21)	S1_01	2M LTU 1A	S3_01
	2M Trib 1 (ports 22-42)	S1_01	2M LTU 1B	S3_02
	2M Trib 1 (ports 43-63)	S1_01	2M LTU 1C	S3_03

	Generic Trib 1	S1_02	Generic Trib 1 PSU/LTU	S3_04
Tributary Group 2	2M Trib 2 (ports 1-21)	S1_03	2M LTU 2A	S3_05
	2M Trib 2 (ports 22-42)	S1_03	2M LTU 2B	S3_06
	2M Trib 2 (ports 43-63)	S1_03	2M LTU 2C	S3_07
	Generic Trib 2	S1_04	Generic Trib 2 PSU/LTU	S3_08
2M Protection Trib		S1_05	---	---
Tributary Group 3	2M Trib 3 (ports 1-21)	S1_08	2M LTU 3A	S3_09
	2M Trib 3 (ports 22-42)	S1_08	2M LTU 3B	S3_10
	2M Trib 3 (ports 43-63)	S1_08	2M LTU 3C	S3_11
	Generic Trib 3	S1_09	Generic Trib 3 PSU/LTU	S3_12
Tributary Group 4	2M Trib 4 (ports 1-21)	S1_10	2M LTU 4A	S3_13
	2M Trib 4 (ports 22-42)	S1_10	2M LTU 4B	S3_14
	2M Trib 4 (ports 43-63)	S1_10	2M LTU 4C	S3_15
	Generic Trib 4	S1_11	Generic Trib 4 PSU/LTU	S3_16
Generic Trib 5		S1_12	Generic Trib 5 PSU/LTU	S3_17
Generic Trib 6		S1_13	Generic Trib 6 PSU/LTU	S3_18
Generic Trib 7		S1_14	Generic Trib 7 PSU/LTU	S3_19

Note: In each tributary group it is not possible to fit the 2M tributary card and the generic tributary card at the same time. This is indicated by the dotted line.

Table 7-6: Slot Equipping rules for 63x2M Unbalanced LTU - 02HAM 00003 AAL

2M LTU 1			2M LTU 2			2M LTU 3			2M LTU 4		
S3_01	S3_02	S3_03	S3_05	S3_06	S3_07	S3_09	S3_10	S3_11	S3_13	S3_14	S3_15
OMS 1260 63x2M LTU – 2M Trib 1											
						OMS 1260 63x2M LTU – 2M Trib 3					
			OMS 1260 63x2M LTU – 2M Trib 2								
OMS 1260 63x2M LTU – 2M Trib 1						OMS 1260 63x2M LTU – 2M Trib 3					

Note: This LTU is a multi-card assembly with a large front-plate to give enough physical space for the 126 1.0/2.3 coax connectors. When this LTU is fitted, it covers a total of seven slots (6x2M LTU + 1xgeneric LTU). This makes the adjacent 2M tributary LTU area unusable. Table 7-6 shows which combination of slots this LTU can be fitted into.

Note: As Table 7-6 shows, fitting 2M Tributary 2 with an unbalanced LTU will not allow future expansion of 2M unbalanced interfaces.

Table 7-7: Slot Equipping rules for Vertically Extended 63x2M Unbalanced LTU - 03HAM 00009 AAL

2M LTU 1			2M LTU 2			2M LTU 3			2M LTU 4		
S3_01	S3_02	S3_03	S3_05	S3_06	S3_07	S3_09	S3_10	S3_11	S3_13	S3_14	S3_15
OMS 1260 63x2M LTU – 2M Tributary 1			OMS 1260 63x2M LTU – 2M Tributary 2			OMS 1260 63x2M LTU – 2M Tributary 3			OMS 1260 63x2M LTU – 2M Tributary 4		

Note: The Vertically Extended LTU increases the subrack height by 180mm.

Protection Scheme Summary

In summary, the OMS 1200 includes the following protection schemes in line with generic SMA products:

- Network Level Protection Schemes:
  - SDH Trail - Linear Multiplex Section Protection (Linear MSP)
  - VC-trail - Sub-Network Connection Protection (SNCP)
  - PDH Trail - PDH Tributary Port Protection.
  - Two Fibre MS-SPRING is available for OME1240 and OMS 1260 fitted with STM-4/16 Core cards.
- SMA Equipment Level Protection Schemes:
  - SDH/PDH/ETA Tributary Interface Card Protection
  - Core Card Protection.

Network level protection schemes protect against failure of equipment and line plant external to the SMA (for example SNC protection). These schemes are intended to provide enhanced availability for complete end-to-end traffic trails, or segments of them, in a network. Given worker and protection channel traffic from the network, the SMA uses SDH section and path layer monitoring to determine which is the most viable transport channel and switches accordingly.

Equipment level protection schemes increase the availability of traffic paths within the SMA equipment by providing fast, autonomous recovery from card/unit failures. The peripheral traffic interface cards internally monitor the quality of signals received from each core unit. On detection of faults, they switch accordingly.

7.3 Intra/Inter Card MSP and SNCP Protection

The terms intra-card and inter-card MSP and SNCP protection are used to describe different traffic protection behaviour when worker and protection paths are set up on the same core card (refer to Figure 7-4) or on different core cards (refer to Figure 7-6), respectively.

Figure 7-4: Intra Card Protection

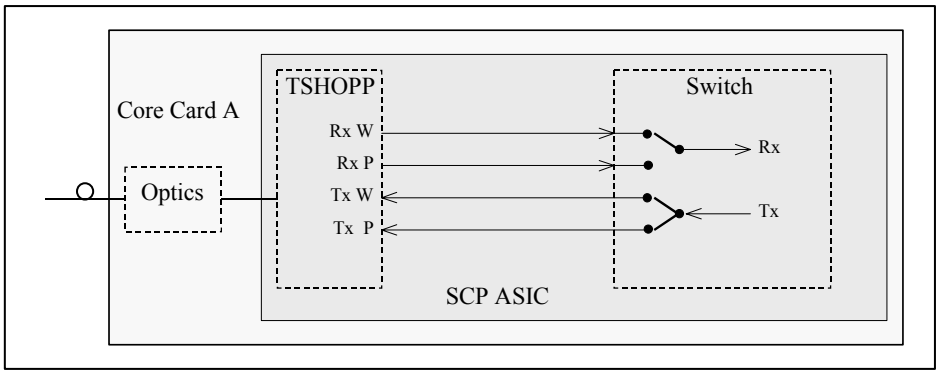
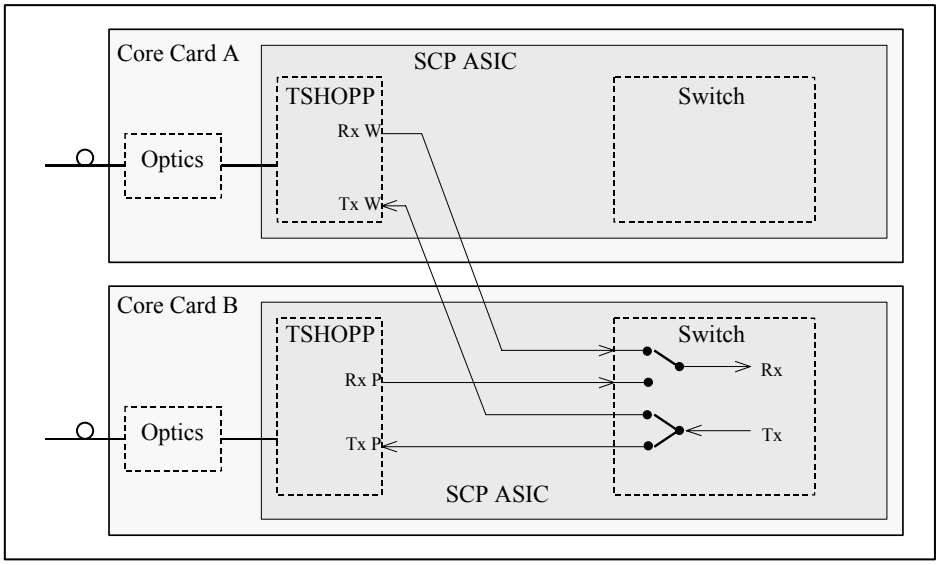


Figure 7-5: Inter Card Protection



7.4 SDH Trail Linear Multiplex Section Protection (MSP)

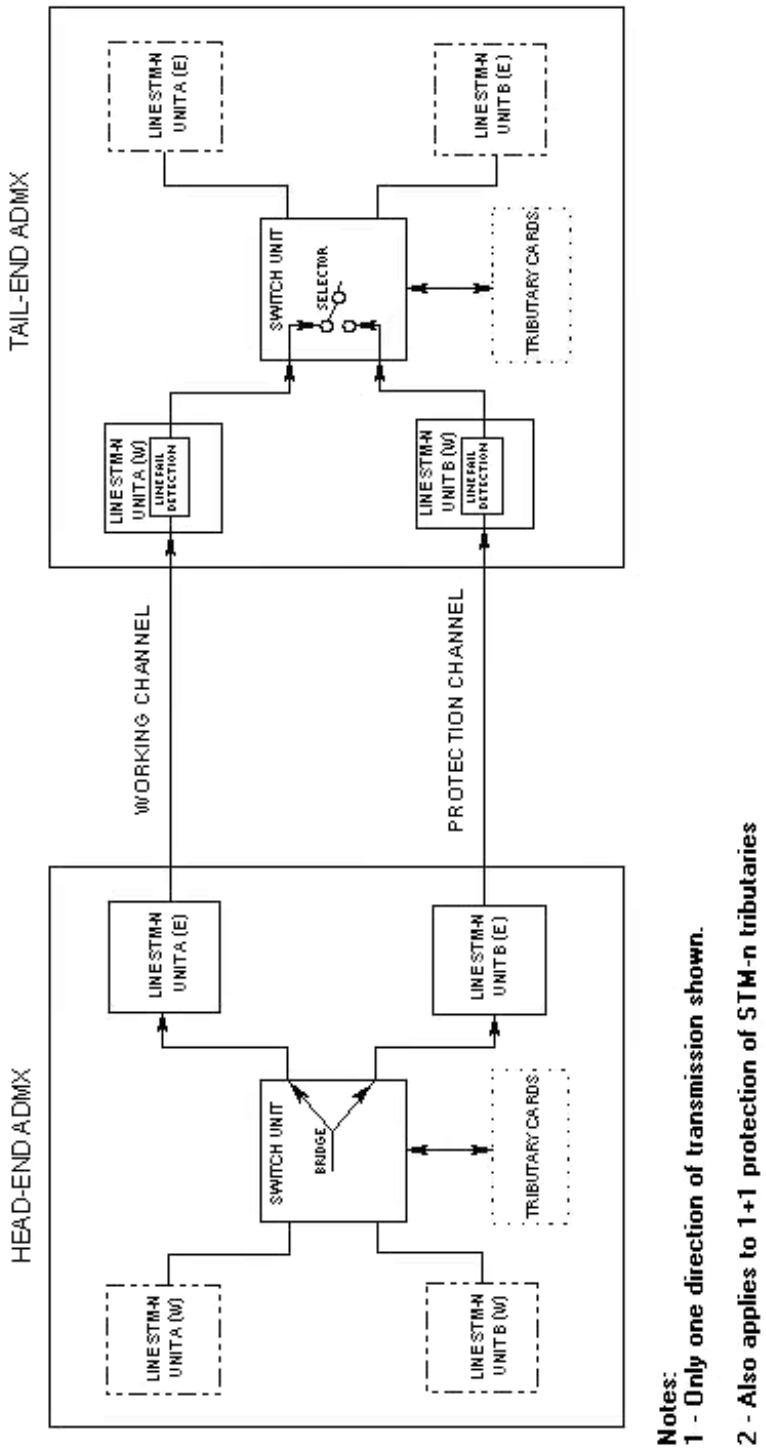
MSP is used in the SMA- equipment to protect against external failures of equipment and/or SDH line plant (e.g. fibres, regenerators) connected to the STM-n line and tributary interface units. Although MSP is principally an external protection mechanism, it also inherently provides a method of protecting against failure of the SDH line interface functions within the equipment.

MSP is used on pairs of core card line ports or pairs of tributary ports, but not pairs consisting of both a line and a tributary port. It is possible to configure MSP between STM-1 optical and electrical interface ports, STM-4 optical interface ports, and STM-16 optical interface ports. It is not possible to configure MSP on line ports of tributary cards that are included in a 1:n card protection group. An MSP pair must have the same STM-n rates.

Currently, the OMS 1200 products support SDH line interface function pairs to support a 1+1 linear network section protection architecture where the SDH line signal is permanently bridged onto both worker and protection sections. The APS protocol signalling used in bidirectional operation is the standard protocol compatible with 1:n network protection architectures – ITU-T Rec G.841.

The architecture is as shown in Figure 7-6.

Figure 7-6: 1:1 STM-n Link Protection



Note: References to line cards apply to the TSHOPP and optical line modules of the core cards, and references to the switch cards apply to the switch function of the core cards.

Each STM-1/4 core card provides up to two STM-1/4 line interfaces. These may all operate as unprotected ports on a hubbing NE.

With core cards, addition of a second core card automatically provides equipment – level protection against card failure. Failure/removal of a core card means that its SDH line interface functions are also lost. For full protection, therefore, the SDH line interface functions of a second core provide protection for those equivalent functions of the first core, all configured as inter-core-card MSP protection pairs. However there is no restriction to this allocation, and any pairings are allowed for 1+1 Linear Trail MSP. For example:

- Worker on East: protection on West (and vice-versa)
- Worker on Core Card A: protection on Core Card B (and vice-versa)
- One protection pair/two protection pairs, or none.

STM-16/4 core cards only provide one SDH line interface function, therefore if this needs MSP protection configuration, then two core cards have to be installed with inter-core-card MSP protection pairing.

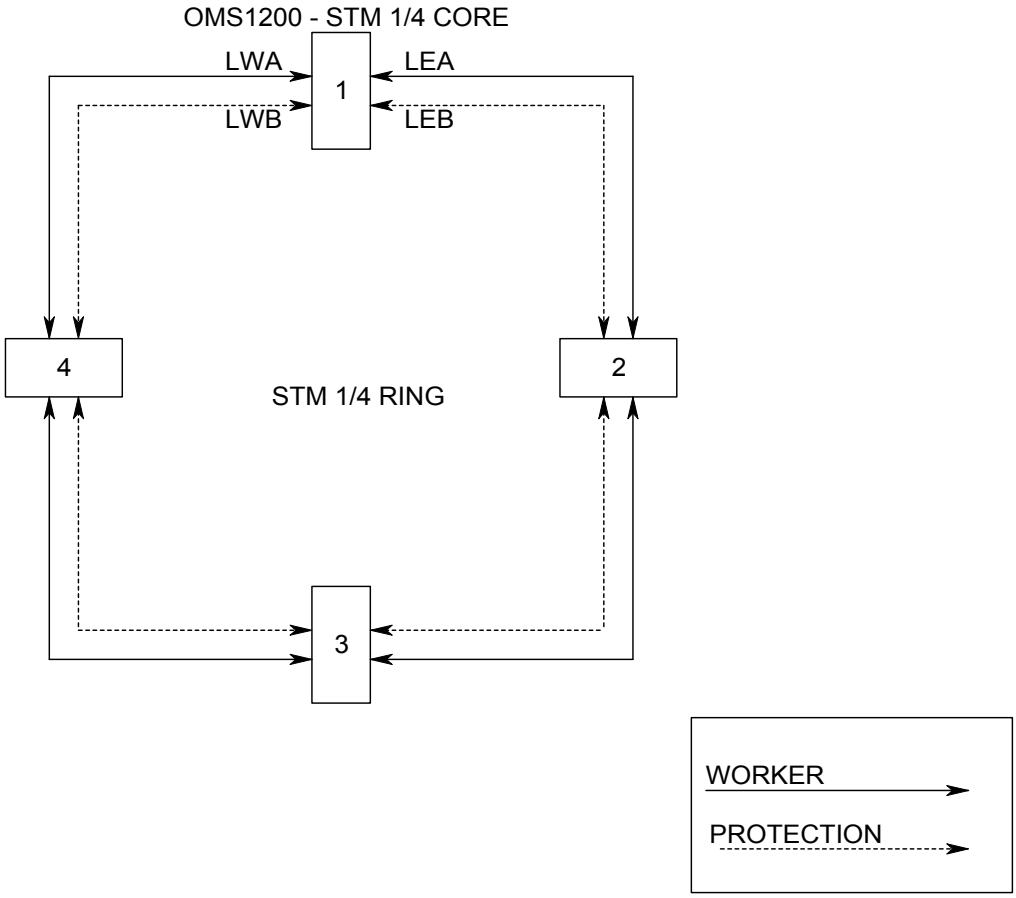
7.4.1 OMS 1200 STM1/4 Core Card

STM-1/4 core cards provide two STM-1/4 line interfaces. These may all be configured to operate as unprotected ports on a hubbing NE.

When two Core Cards are fitted; the second core card automatically provides equipment level protection against card failure. The second core can also be used to provide protection for the SDH line interface functions utilising inter-core-card MSP. There is no restriction to the allocation, any pairings are allowed for 1+1 Linear Trail MSP. For example:

- Worker on East: protection on West (and vice-versa)
- Worker on Core Card A: protection on Core Card B (and vice-versa)
- One protection pair/two protection pairs, or none.

Figure 7-7: MSP Protection with STM-1/4 Core Card



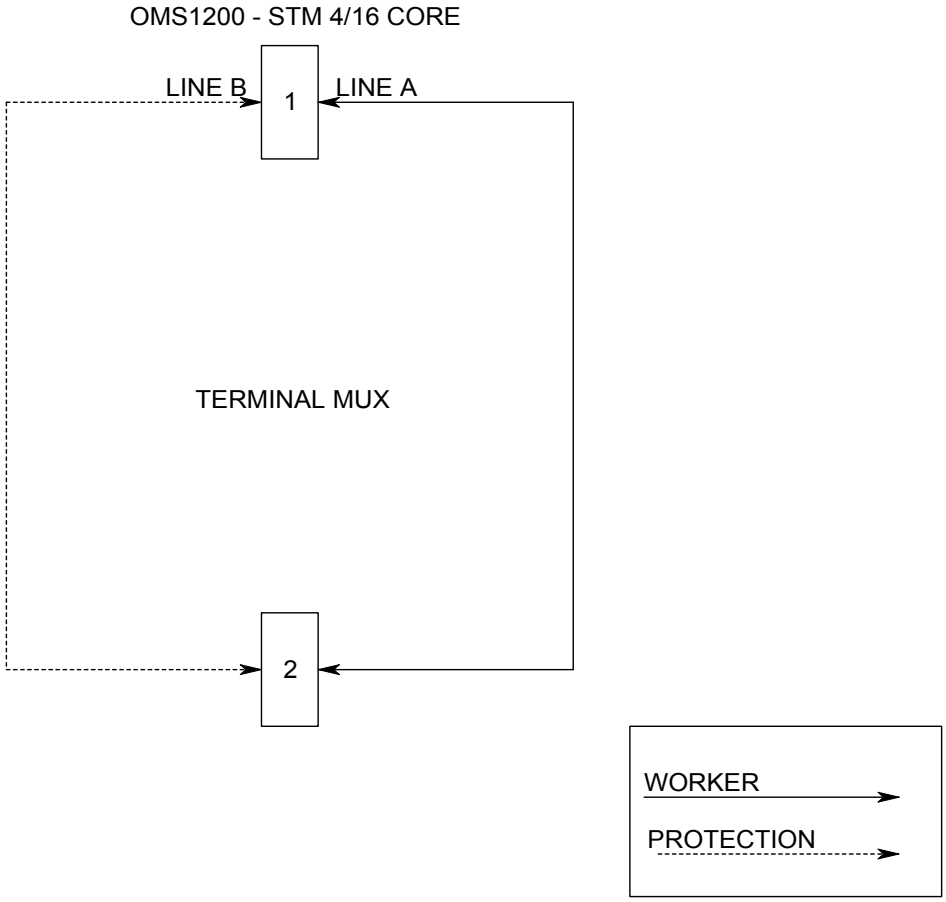
7.4.2 OMS 1200 STM4/16 Core Card

STM-4/16 core cards provide STM-4/16 line interfaces. These can be configured to operate as unprotected ports or as a protected Terminal Mux with MSP.

When two Core Cards are fitted; the second core card automatically provides equipment level protection against card failure. The second core can also be used to provide protection for the SDH line interface functions utilising inter-core-card MSP.

- Worker on Core Card A: protection on Core Card B (and vice-versa)

Figure 7-8: MSP Protection with STM-4/16 Core Card



7.4.3 K1/K2 Protocols

Two different signalling protocols are used to control MSP - the ITU-T/ETSI Protocol (G.783, G.841, ETS 300 417-3-1, ETS 300 746) and the Siemens Proprietary Protocol. Both employ two bytes for signalling located in the SOH - K1 and K2.

The choice of protocol is a configurable option on a per protection section basis at the LCT/LCTS.

7.4.3.1 ITU-T/ETSI Standard K1/K2 Protocols

The K1/K2 protocol described in the standards referred to above is used to send requests for switching. This is used in 1+1 bi-directional and unidirectional modes. The 1+1 K1, K2 protocol mechanism compatible with 1:N network architectures, is used.

The tail end duplicates traffic and sends the K1 and K2 to the far end informing it of the switch to the protection channel. The head end responds by duplicating traffic to the protection card and sends a reverse request with the bridged channel in the K2. The tail end sees that the transmitted K1 and the received K2 match and switches its receive selector. The head end sees that the transmitted K1 and the received K2 match and switches its receive selector as well.

The protection logic of each end determines the highest priority request that is active. This may be a remote request (received via the K1 byte) or a local request (condition, state or switch request of the local MSP function). The protection logic sets the bridge in accordance with the highest priority request. The resultant bridge position is indicated in K2 bits 1-4. For the generation of the sent K1 byte, only the highest priority request is considered.

7.4.3.2 Siemens Accelerated K1/K2 MSP Protocol

The SMA also supports the Siemens Accelerated Protection Switching protocol for 1+1 bi-directional switching for a network using predominantly 1+1 bi-directional switching. The K1, K2 bytes are still used for signalling, however, only a single K1, K2 protocol exchange is required to complete a bi-directional switch. This protocol may only be used for bi-directional switching.

When the protection section is not in use, Null Channel is indicated for the sent K1 bytes on both ends. Bits 1-4 of K2 bytes sent at both ends of the section are set to 0001 to indicate that the selector is released and receiving traffic from the working section.

The protection logic of each end determines the highest priority request that is active. This may be a remote request (received via the K1 byte) or a local request (condition, state or switch request of the local MSP function). The protection logic sets the selector in accordance with the highest priority request. The resultant selector position is indicated in K2 bits 1-4. For the generation of the sent K1 byte, only the highest priority request is considered. Remote requests are not considered, and Reverse Request is never indicated.

7.4.4 Modes of Operation

The MSP architecture is outlined in Table 7-12 (1+1 link protection). Control of the (effective) two-way switches at the receive ends of the links is performed according to the selected mode of operation. There are four modes of operation, which are configurable options at the LCT/LCTS (although the SMA might adopt a different mode according to other factors as described later in this chapter). These modes are:

- Revertive
- Non-revertive
- Uni-directional
- Bi-directional.

Note: The default mode of operation is Bi-directional Non-revertive.

Note: It is not possible to use the Siemens Protocol in Uni-directional mode of operation.

7.4.4.1 Bi-directional Revertive Mode

In this mode, traffic in both directions of transmission is switched automatically to the protection channel in case of failure of the working channel (even if the failure is in only one direction of transmission). To ensure that both multiplexers at each end of the section always switch to the same channel, signalling via the K1, K2 bytes of the SOH is performed.

In Revertive mode, for 1+1 protection, one of the two identical STM-n channels, designated working channel 1 (Worker Channel 1), is the preferred path for the traffic. The other channel is designated protection and is used for traffic only when the working channel fails. Consequently, traffic on the protection channel is automatically switched back (revert) to the working channel upon recovery of the latter.

If a mode mismatch is detected in this mode, the SMA stays in Revertive mode.

7.4.4.2 Bi-directional Non-Revertive Mode

Switching for this mode is in both directions in an identical manner to bi-directional Revertive mode. However, in bi-directional non-revertive mode, traffic on the protection channel is not switched back to the working channel upon recovery of the latter. Instead, traffic remains on the protection channel until the protection channel itself fails (or manual switching is performed). Non-revertive mode of operation is designed to prevent unnecessary disturbances to traffic, which occur when a revertive mechanism switches back.

Note: Although the aim is to make protection switching of channels in an SMA hitless, this may not always be guaranteed.

For 1+1 protection, there is no conceptual distinction between the channels in non-revertive mode and traffic switching between them takes place in an essentially symmetrical manner (i.e. there is no preferred channel). However, the two channels are still termed Working Channel 1 and Protection Channel, including the identification of the channels to an operator via the NMI

7.4.4.3 Unidirectional Revertive Mode

Unidirectional mode means that the transmit and receive directions do not relate to the same worker. The switching decision is based solely on local traffic performance indications received on the incoming STM-n channels (or locally generated manual switch commands). The local receive two-way selector switch therefore operates to select the protection channel when the working channel fails.

Revertive operation means that the switch operates to select the working channel upon its recovery, as for bi-directional Revertive mode, although, in unidirectional mode, the SMA only considers the local working channel recovery conditions.

Signalling between the two SMAs at each end of a multiplexer section is not required in unidirectional mode. However, K1 and K2 bytes are still exchanged to provide indications of local actions to the remote end (rather than requests for action).

It is possible to use Unidirectional Revertive mode on all 1+1 protected SMA equipment using the ITU-T/ETSI standard protocol.

7.4.4.4 Unidirectional Non-Revertive Mode

This mode is similar to Unidirectional Revertive mode, but traffic is not switched from the protection channel to the working channel when the latter recovers. Again, it is only possible to use the ITU-T/ETSI standard protocol. K1 and K2 bytes are generated to indicate the local status.

7.4.4.5 Mode Selection

Although you can configure the preferred operating mode, it is possible for the SMA to automatically select a different mode for operation under certain specific circumstances. There are two reasons for needing this feature.

- Firstly, an SMA may be connected to a remote multiplexer, which has been inadvertently configured into a different operating mode. The SMA is capable of detecting this condition and raising any necessary alarms. It also automatically assumes an appropriate new operating mode to permit continued traffic protection.

  The method of detecting the remote multiplexer operating mode is via the K1, K2 byte protocol. When a mode mismatch alarm is raised, both the alarm and the newly assumed operating mode persist for the duration of the protection switch. If an SMA configured mode is found to be in error, it is possible to change and re-enter it. If Protection Section is failed, Mode Mismatch is disabled.

  Note: It is necessary to check the operating modes of the multiplexers at both ends of the link before re-entering the mode

- The second condition under which the mode can change is in response to a locally detected failure of the protection channel. Since the signalling for bi-directional working is carried over this channel (via the K1, K2 bytes), the signalling mechanism is regarded to have failed when a local Signal Fail (protection) is received. If the SMA is configured for bi-directional working, it automatically adopts unidirectional working during the period that the Signal Fail is active.

  Under these conditions the incoming K1, K2 bytes are not monitored (they are, in any case set to a default value by the STM-n units), although the outgoing K1, K2 byte indications are set as for normal unidirectional mode. The mode mismatch alarm is not set. When the Signal Fail (protection) indication clears, full bi-directional working is automatically restored.

7.4.5 Protection Switching Criteria

MSP switching operates according to events received and detected by the SMA. These events comprise detected STM-n section failures, operator requests for switching and remote requests received from the multiplexer at the end of the protected multiplexer section (via the K1/K2 byte message protocol).

The full list of events, the conditions under which they are considered active/inactive and a brief overview of the system behaviour are described below.

7.4.5.1 Locally Detected Line Failure Events

When a tributary card is removed, the controller function detects a card-out signal and sends a Forced Slot Fail message to the core card switch function stating which psuedo-STM-1 interface is affected. The Forced Slot Fail condition is latched in the core card switch function.

The switch ORs this controller derived interface fail condition with the locally detected interface parity failure. If either failure condition is active, then any SF/SD signalling flags on the affected interface, for protected multiplex sections and HO/LO VC channels, are considered as having failed and are interpreted as SF conditions. An interface failure also causes AIS to be injected toward the router by the tributary-side cross connect in all TU-Ns, resulting in AIS being transmitted on all ports cross-connected to the failed interface.

When a card is replaced into a configured slot, the controller function checks the validity of the card and after downloading the configuration database sends a Clear Slot Fail message to the switch. The controller-derived interface failure is then removed, and provided there is no locally detected interface failure; the SF/SD flags are again monitored.

Detection of locally received failures on an STM-n section is performed by a combination of the receiving STM-n unit and the core unit.

Two criteria are used to indicate the status of each section to the protection switching control mechanism:

- Signal Fail (SF)
- Signal Degrade (SD).

The STM-n unit generates these flags and the core unit receives them and uses them to trigger the next stage of the protection switching sequence.

Each STM-n unit is responsible for monitoring its connected STM-n input. A failure indication is raised if one, or more, of the following criteria is detected:

- STM-n Loss of Signal
- Loss of Frame Alignment
- MS AIS - bits 6, 7 and 8 of K2 received in state 111.

Table 7-8: Failure Types

Serial	Failure Types
1	Excessive Bit Error Ratio (BER) - bit error ratio >1x10-3 (Enable/Disable) - Default: Enabled
2	Section Trace Mismatch - You have the option of either enabling or disabling this criterion - Default: Enabled
3	Signal Degrade - You are able to configure the signal degrade calculation to be based either on equivalent BER or USE or degraded seconds calculations. You also have the option of enabling or disabling signal degrade - Defaults: signal degrade enabled/criteria USE.

Failures of types shown in Table 7-8 cause a Signal Fail (SF) flag or Signal Degrade (SD) flag as applicable to be inserted into the traffic interface to the core unit.

Disabling the above criteria (2) Table 7-8 also disables the associated alarms. The enable/disable functions lie within the section/path maintenance configuration applications of the SMA, not the protection configuration applications.

A failure of type (3) Table 7-8 causes a Signal Degrade (SD) flag to be inserted into the interface to the core unit. Resetting of a condition causes the resetting of the appropriate flag.

Enabling/disabling criteria for setting the SD Flag can either be handled within the protection configuration applications, or within the section/path maintenance configuration applications of the SMA (events and traffic connection management). You are able to configure degraded path performance fault reporting on a per-section basis. The configurations include the following:

- Fault Report Disabled
- Fault Report based on equivalent BER calculations - Path Signal Degrade alarms reported
- Fault Report based on Unacceptable Short-Term Error performance calculations - Path USE alarms reported
- Fault Report based on Degraded Error performance calculations - Path Signal Degrade alarms reported.

The defaults are fault reporting enabled for USE alarm reporting.

Which ever attributes are configured for fault reporting, the same are used as the Enable/Disable configurations for setting the SD signalling flag, and vice-versa.

- The Signal Degrade fault type works on BIP bit equivalent binary error ratio calculations (for example, ratio 10e-6). The USE fault type works on the crossing of a threshold of consecutive severely errored seconds. These are calculated for each multiplex section by the protected pair SDH interface units.
- Degraded path performance can be based on USE or Consecutive Degraded Seconds (CDEGS). Separate configurable thresholds are provided for SES (performance monitoring) and DEGS (events handling).
- You can configure the signal degrade fault type to work on BIP BERs, or CDEGS.

7.4.6 MSP Alarms

There are three possible alarms, which are generated when implementing MSP protection.

1 Tx/Rx K2 (bit 5) mismatch.

Raised if a mismatch between the transmitted and received K2 bit 5 persists for a period of 50ms.

2 Tx K1 (bits 5-8), Rx K2 (bits 1-4) mismatch - ITU-T/ETSI standard protocol.

Raised if a mismatch between the transmitted K1 and received K2 persists for a period of 50ms.

3 Local selected channel, Rx K2 (bits 1-4) mismatch - Siemens protocol.

Raised if a mismatch between the local selector, and the received K2 persists for a period of 1 second (1000ms).

4 Local/Remote operating mode mismatch.

Raised when a mismatch between the local and remote operating modes is detected.

7.4.7 Operator Entered Commands

The MSP switching process also receives operator inputs. You can enter these commands (events) via the local terminal, or from the element manager.

If the command you enter causes a change in switch state, then it is translated into a message, which is compatible with the K1 byte message set (Siemens or ITU-T/ETSI standard) for transmission to the remote multiplexer.

Each of the operator-entered events used for control of switching is described below. The names of the commands are those seen at the LCT. The commands in square brackets are the equivalent commands of the K1 message set.

These states are stored in non-volatile memory and used to restore the equipment to its previous state in the case of a loss of power. Traffic is correctly selected from the appropriate channel upon restoration.

Note: For bi-directional operation, a forced switch is the only way in which the in-traffic LED of either of a pair of single-port STM-n cards may be extinguished. This need for your intervention is to protect against traffic disruption in the event that the local receiving circuits of an STM-n card have failed, but the remote system is currently selecting traffic from the (correctly functioning) transmit circuitry of that card. This does not apply to dual-port STM-1 cards, since the in-traffic LEDs are always lit.

Operator entered commands detailed below are:

- Forced Switch to Worker
  - [Forced Switch (Protection Channel)}.
- Forced Switch to Protection

– [Forced Switch (Worker Channel)].

- Clear.

Remote multiplexer requests detailed below are:

- Wait To Restore
- Exercise
- Reverse Request - ITU-T/ETSI standard protocols ONLY
- Do Not Revert
- No Request.

7.4.8 Forced Switch to Worker

Forced Switch (Protection Channel)

Causes traffic to switch to (or be maintained on) the working channel. This command has a higher priority than received SF or SD conditions on the working channel and therefore traffic remains on the working channel regardless of any failure indications on this channel.

For single-port STM-n cards the in-traffic LED on the protection channel card can be extinguished, but in bi-directional mode only, and only when the remote end has switched.

For dual-port STM-1 cards the in-traffic LEDs are always lit, since each separate port may or may not be in protection, and possibly with different protection card pairings.

7.4.9 Forced Switch to Protection

Forced Switch (worker channel)

Causes traffic to switch to (or be maintained on) the protection channel unless a higher priority switch state is in effect, or an SF condition exists on the protection section.

This command eliminates the possibility of disruption of revenue earning traffic being caused by removal of the working channel card.

For single-port STM-n cards the in-traffic LED on the working channel card can be extinguished, but in bi-directional mode only, and only when the remote end has switched. If a subsequent SF occurs on the protection channel card, the in-traffic LED is lit on the worker and traffic is switched back to the worker; Signal Fail Protection overrides a Force Switch (Worker Channel).

For dual-port STM-1 cards the in-traffic LEDs are always lit, since each separate port may or may not be in protection, and possibly with different protection card pairings.

7.4.10 Clear

This clears any of the above-entered commands and any active WTR states.

The protection state of the currently selected STM-n is displayed.

7.4.11 Remote Multiplexer Requests

The SMA MSP switching mechanism also (in bi-directional mode only) responds to messages received from the multiplexer at the other end of the multiplexer section.

These messages (events) are used to set the switch state for both multiplexers at each end of a bi-directional protected link and are received via the K1 byte in accordance with the protocol detailed in G.783 and the Siemens protocol.

The Multiplexer Controller is capable of interrogating the switch for current settings. This ensures that on controller reset, no states are changed.

The remote events are:

- Forced Switch (Worker Channel).
- Forced Switch (Protection Channel).

The above events are derived from operator requests entered at the remote multiplexer and cause the same actions as the equivalent locally entered commands described in Section 7.4.7 above.

- Signal Fail (Worker Channel).
- Signal Degrade (Worker Channel).
- Signal Fail (Protection Channel).
- Signal Degrade (Protection Channel).

The above events refer to the line conditions being received at the remote multiplexer and have the same meanings as the equivalent locally received line conditions.

7.4.12 Wait to Restore

Used in revertive mode and is received when the remote multiplexer has detected a working channel recovery but is applying a Wait to Restore time-out (persistency check) before allowing traffic to be switched back from the protection channel. See Section 7.4.17.1 for a description of Wait to Restore.

7.4.13 Exercise

This is included for compliance with ITU-T/ETSI standards (there is no equivalent operator-entered exercise condition). The SMA acknowledges an exercise request but performs no other action.

7.4.14 Reverse Request - ITU-T/ETSI Standard Protocols ONLY

Received as an acknowledgement to a request previously transmitted to the remote multiplexer via the K1 byte.

Note: The Siemens protocol does not issue Reverse Requests.

7.4.15 Do Not Revert

Received from a multiplexer configured into the non-revertive mode of operation and instructs the SMA to maintain traffic on the protection channel, even though the working channel has recovered. See Section 7.4.17.2 for a description of Do Not Revert.

7.4.16 No Request

The idle condition received when neither a request nor acknowledgement is being transmitted by the remote multiplexer.

7.4.17 Local WTR and Do Not Revert States

An SMA enters either the Wait to Restore or Do Not Revert state upon recovery of a failed working channel.

7.4.17.1 WTR

The Wait to Restore state is entered automatically when traffic is selected from the protection channel because of a failure of the working channel, and the working channel subsequently recovers.

For an SMA, the state only occurs in Revertive mode of operation although it is possible for an SMA to receive a Wait to Restore request from a remote multiplexer in non-Revertive mode where this is a different vendor's equipment.

Entry to the Wait to Restore state is inhibited if a higher priority condition exists when the working channel recovers.

When the Wait to Restore state is entered, a timer is set and the condition is de-activated upon expiry of the timer period. The condition is de-activated (and the timer reset) if a higher priority condition is received during the timer period.

You can configure the timer from zero to 30 minutes in one-minute (± 5 second) steps. Selection of the zero minute option prevents the SMA ever entering the Wait to Restore condition (that is, it de-selects the Wait to Restore option). You can set the Wait to Restore timer both as a global option and on an individual basis. The default setting is 10 minutes.

Note: You are only able to retrieve WTR values from the NE on an individual channel basis.

7.4.17.2 Do Not Revert

The Do not Revert state is entered under the same circumstances as Wait to Restore. However, there is not a timer associated with the Do not Revert state and it remains active until a higher-level condition is received, at which point Do not Revert is reset. Do not Revert is used in non-Revertive mode of operation only. If it is active, it is reset immediately by re-configuration of the SMA into Revertive mode.

On power-up of an SMA (causing a main reset), the SMA starts up with traffic selected from the working channel, assuming that no failure indications or operator commands require a switch to the protection channel. In particular, the implementation of the protection switching control mechanism does not, on power-up, allow the selection of the protection channel with Wait to Restore or Do not Revert states active.

7.4.18 Protection Switching Control

7.4.18.1 Protection Switching Operation

In a MSP system, the local SMA traffic connections can only be in one of two states according to the position of the selector switch (refer to Table 7-12). These states are, receiving traffic from the working channel and receiving traffic from the protection channel.

The state that the switch is in at any time is governed by the indications, which are active at that time. These indications comprise local line failure flags, operator-entered commands and remote multiplexer requests as described in Section 7.4.5, 7.4.7 and 7.4.11.

The Wait to Restore and Do not Revert conditions affect the state of the selector depending on the protection mode being used.

The switching indications received and the resultant position of the selector switch are shown in Table 7-9. The naming convention used for the indications is such that the channel name given in brackets is the channel for which the indication is active. For example, Forced Switch (protection) is the Forced Switch command for the protection channel and results in traffic being selected from the other (working) channel.

The indications are listed in priority order from Forced Switch (protection), which has the highest priority, to No Request (protection), which has the lowest. The selector is activated according to the highest priority indication active at any time.

A local indication has a higher priority than a remote indication of the same type. If both a local and a remote indication of the same type are received, the local indication becomes the active condition. This is not important for operation of the selector, which assumes the same position irrespective of whether the condition is local or remote. However, it is relevant to the generation of the transmitted K1 byte. In unidirectional operation, remote indications are ignored.

Note: In bi-directional operation, when using the ITU-T/ETSI standard protocol, you can only select the protection channel if, in addition to an appropriate indication being received, the transmitted K1 byte (bits 5-8) and received K2 byte (bits 1-4) are the same.

If a transmitted K1 byte indication and received K2 byte indication do not match, the selector stays released (selecting the working channel) and an alarm is raised. This does not apply in unidirectional mode. Operation of the K1, K2 byte signalling is described in Section 7.4.21.

When using the Siemens protocol, selection of the protection channel is performed automatically. However, if the received K2 byte (bits 1-4) does not match the locally selected channel within 1 second (1000ms), an alarm is raised, and the selector released.

Table 7-9: MSP Switch Indications

Priority	Indication Received (Note 1)	Selected Channel
1	Forced Switch (Protection)	Working
2	Signal Fail (Protection)	Working
3	Forced Switch (Worker Channel)	Protection (Note 3)
4	Signal Fail (Worker Channel)	Protection (Note 3)
5	Signal Degrade (Protection)	Working
6	Signal Degrade (Worker Channel)	Protection (Note 3)
9	Wait to Restore (Worker Channel) (Notes 2,4)	Protection (Note 3)
10	Do not Revert (Worker Channel) (Notes 2,5)	Protection (Note 3)
11	No Request (Protection) (Note 2)	Working (Revertive Mode) or Working Or Protection (Non-Revertive Mode)

Note: **1**: Only local indications apply in unidirectional mode. In bi-directional mode both local and remote indications apply. Remote indications are signalled via the K1 byte. A local indication has a higher priority than a remote indication of the same type. If a local and a remote indication of the same type are received simultaneously the local indication is active.

Note: **2**: Only the protection channel may be specified for a No Request indication. Only the working channel may be specified for Wait to Restore and Do not Revert indications.

Note: **3**: In addition to the active indication, in bi-directional mode, bits 1-4 of the received K2 byte and bits 5-8 of the transmitted K1 byte must be the same for selection of the protection channel.

Note: **4**: Local Wait to Restore applies in revertive mode only.

Note: **5**: Do not Revert applies in non-revertive mode only.

7.4.19 Operator Commands for MSP

7.4.19.1 Configuration

Before the protection switching mechanism can be controlled, you must configure the different parameters related to the type of protection for each protected section.

You can enter these commands via the local terminal or from the EM. See also the “LCT/LCTS Operating Procedures” handbook.

For each STM-n section to be protected consider:

1 STM-n section to be protected and protection section.

- MSP is enabled/disabled by virtue of configuring/deconfiguring the protection and protected section.
- In the case of line section, West/East/A or B line STM-n must be specified.
- In the case of STM-1 tributary, the number of the tributary slot (among the STM-1 slots or STM-4 tributary slots) within the shelf must be specified

  For example: STM-1 in Tributary Slot 1 is protected by an STM-1 in Tributary Slot 2 (1+1).

  Section trace is independently configurable for worker and protection sections.

2 MSP Protocol

- ITU-T/ETSI standard Protocol
- Siemens Protocol.

3 Operating Mode

- Bi-directional revertive
- Bi-directional non-revertive (1+1 only)
- Unidirectional revertive (1+1 only)
- Unidirectional non-revertive (1+1 only).

4 Wait To Restore (if Revertive mode) - Default 10min

The configuration of the Wait To Restore period must be in the range of 0 to 30 minutes (refer to Section 7.4.17.1). WTR is individually configurable for each worker/protection pair or globally for all pairs.

Deconfiguring MSP sets protection switching to the disabled state for the selected port. Disabling protection automatically clears any switch commands you entered and cause traffic to revert to the working channel 1. It also sets the transmitted K1 byte indication to No Request (#0) and transmitted K2 bits 1-4 indicate channel 0.

7.4.20 Multiplexer Controller Restoration

The Multiplexer Controller is capable of interrogating the core or core unit replacement for current settings for protection to ensure that on controller re-set, states are not changed.

7.4.21 Protection Switch Time and K1, K2 Protocol Timing

When using the ITU-T/ETSI standard protocol, the overall protection switch time for a MSP event is less than 50 ms for both unidirectional and bi-directional modes of operation.

When using the Siemens protocol (bi-directional only), bi-directional switching is completed within 1 second (1000ms).

For unidirectional mode, (ITU-T/ETSI standard) this time is defined as the period between an SF or SD flag being set by an STM-n card and completion of the switching action (this includes the operation of the local tail-end selector as well as the transmitted K1, K2 bytes stabilising to a steady state).

In bi-directional operation, when using the ITU-T/ETSI standard protocol, the switching time is as for unidirectional operation except that the time includes multiplexers at both end of the multiplexer section (i.e. the time is for overall switching of the multiplexer section in both directions of transmission).

When using the Siemens protocol, this time includes the time-out period of 1 second (1000ms) in which the received K2 must match the selected channel.

The overall protection switch time for a manually initiated switch is less than 8 seconds. The time is defined as the period from the entry of the protection switch command at the local terminal to the confirmation output from the local-terminal to the operator.

When an SMA is configured to operate in bi-directional mode, the appropriate K2 (bridged channel - ITU-T/ETSI) indication (bits 1-4) is transmitted within 50 ms of a bridging request being received in the K1 byte from the remote multiplexer. A bridging request is any valid K1 byte. Bits 5-8 indicate the channel for which the bridge is requested.

When using the Siemens protocol, the appropriate K2 (selected channel) indication is transmitted within 1 second of a request being received in the K1 byte of the remote multiplexer.

Similarly, in bi-directional mode when using the ITU-T/ETSI standard protocol, when a bridging request is transmitted to the remote multiplexer in byte K1, a 50 ms time-out is applied. If the received K2 byte (bits 1-4) does not indicate the same channel number as that in the transmitted K1 byte (bits 5-8) within this time-out period, the multiplexer reverts to unidirectional operation and raises a Tx K1, Rx K2 mismatch alarm.

Note: This timing is a constraint on the K1,K2 byte protocol only. It is derived from the need for 1:N systems to bridge a channel at the head-end before a tail-end multiplexer switches its selector. Although not strictly required in a 1+1 architecture, the application of this time-out is nevertheless retained in ITU-T/ETSI to maintain compatibility.

Since operation of the MSP mechanism may corrupt switch-unit diagnostic messages (internal to the SMA), the maximum duration of disrupted diagnostic messages received at the destination ports due to operation of this mechanism is 3.0ms for TU-1 or TU-2 traffic, or 0.75ms for TU-3 signals.

7.5 VC-Trail SNCP

7.5.1 Introduction to SNCP

Sub-Network Connection Protection (SNCP) is supported. SNC protection operates on an individual VC- basis at all VC-n path layers (i.e. VC-4, VC-3, VC-2, and VC-12).

In an SDH network, traffic is mapped into a VC- container and is transported across the network on a VC-trail.

A VC-trail exists from the NE at which the VC- termination is sourced, across to the NE at which that VC- termination is sinked. Any VC-trail may only be connected through these two NEs or, more commonly, it may be cross-connected through various NEs on-route between the source and sink NEs. The end-to-end VC-trail is known as a network connection.

Each segment of the VC-trail, as it is transported between one NE and the next, is known as a Sub-Network Connection (SNC).

1+1 SNC protection provides a means of protecting against failure of the components of a SNC in a network, including functions of the involved NEs, optical components, interconnecting fibres and intermediate regenerator equipments.

If we consider a segment (or successive segments) of a VC-trail then this SNC has a source NE and a sink NE, just as the end-to-end VC-trail has. Protection is achieved by setting up a worker SNC through certain NEs in the network, and then a separate protection SNC through a different NE route.

At the source NE, the same VC- has two connections (worker/protection) for broadcast to two separate SDH interface unit ports. In this way, two diverse routes can transport the same VC- traffic across the network.

At the sink NE, those connections are received by two SDH interface units and connected into the core unit as a protection pair.

Protection switch selection is then made between worker and protection connections, based on the detected failure/degrade status of each, or on operator command.

7.5.2 Modes of Operation for SNCP

There are four modes of operation for SNCP, which are operator configurable options via the NMI. The default mode is Unidirectional Non-Revertive.

Bi-directional switching modes of operation only apply to bi-directional traffic SNCs and the Operator is prevented from attempting to configure bi-directional switching modes of operation for unidirectional traffic SNCs.

7.5.2.1 Unidirectional Revertive Mode

In revertive mode, there is a preferred channel for receiving the VC. The preferred channel is denoted the working channel and the channel used for protection purposes is denoted the protection channel.

When there are no failure conditions or active operator entered commands, the receive selector selects traffic from the designated working channel. If there is a failure on the working channel the switching mechanism, under normal circumstances, automatically causes a changeover to select traffic from the protection channel.

Upon recovery of the working channel, the selector is automatically switched to select this channel in preference to the protection channel (after the expiry of any Wait to Restore period). Only the recovery conditions of the local working channel are considered.

7.5.2.2 Unidirectional Non-Revertive Mode

This mode of operation is identical to unidirectional revertive mode except that traffic is not switched back to the working channel from the protection channel when the former recovers from a failure condition. This prevents the disturbance to traffic which otherwise occurs when the selector is operated (switching of VCs is non-hitless).

Automatic protection switching is therefore symmetrical between the two channels in non-revertive mode. However, the two channels are still designated Working and Protection. The SMA selects traffic from the designated working channel as a default when first configured for SNC protection or on power-up of the SMA.

7.5.2.3 Bi-directional Revertive or Non-Revertive Mode

If SNCP is applied across the complete end-to-end VC-trail then the two SMAs involved can operate in bi-directional switching mode. Otherwise, only unidirectional mode is possible.

In this mode, also named dual ended switching, traffic is switched automatically to the same (working or protection) channel at each end of the path. In order to ensure that both multiplexers at each end of the path always switch to the same channel, signalling via nominated VC POH bits is performed.

Revertive operation means that the switch is operated to select the working channel upon its recovery and after expiry of any wait to restore time-out.

Non-revertive operation means that the traffic is not switched to the working channel when the latter recovers.

In bi-directional mode of operation, to avoid multiple switching actions after a WTR timer expires, the SNCP controller in the local node signals a RR use worker channel but does not immediately action a switch back to the worker channel.

The behaviour is such that the remote SNCP controller receives the RR use worker channel and then determines the appropriate switching action according to request priorities. It then sends the appropriate RR back to the local SNCP controller. It is at this stage that the local node switches back to the worker channel, if so instructed by the incoming RR.

Note: With this behaviour there is a short period where the local node indicates No Request - Traffic on Worker state, when in fact it is still switched to protection.

7.5.2.4 SNC Persistency (Protection Switching Hold-Off)

You can configure persistency (or Hold-off) on SNC protection in the range zero - 20s in 100ms (+/-20ms) increments, either on a global or per path basis. The default value is 0ms.

You can only retrieve persistency values from the NE on an individual path basis.

This persistency is required if operating both 1+1 Linear MSP/MS-SPRING protection schemes and SNC protection. It allows the MS layer protection scheme to react and switch, and pre-empt SNCP switching, in the event that a detected fault leading to switching actions is in fact an MS layer fault and not a specific VC-path layer fault.

SNCP switching can be triggered from failures detected at MS and HO path layers (SNC/I monitoring), as well as failures detected at the specific protected VC-path layer (SNC/N monitoring).

The persistency configuration is applied to the protection switch controller on the core unit. It applies a hold-off to autonomous protection switching actions from received SF/SD signalling flag requests.

Protection switching actions are only taken if the SF/SD flag has persisted for a period greater than the configured hold-off time.

7.5.3 Protection Switching Criteria for SNCP

SNC protection switching operates according to events received and detected by the SMA in the network, which is terminating the protected SNC. These events comprise locally detected VC-trail SNC failures, locally applied operator requests for switching received via the NMI, and remotely signalled switching requests received from the SMA at the far end of an end-to-end protected SNC.

Remote requests only apply to bi-directional switching modes and bi-directional switching only operates on end-to-end protected SNCs. Remote requests are signalled across the network via VC- POH bytes of the protected SNC.

7.5.3.1 Locally Detected VC Failure Events

The bearer SDH interface units of the SMA, which is receiving worker and protection SNCs from the network, performs detection of VC-trail failures on a protected SNC.

The bearer SDH interface units are either STM-n interface units or VC-AM sub-STM-1 interface units.

SF And SD Flags

Two criteria are used to indicate the status of the two protected VC- SNCs to the protection switching control mechanism on the core unit; namely the Signal Fail (SF) flag, and Signal Degrade (SD) flag.

The SDH receiving interface units generate these flags and the core unit receives them and uses them to trigger the next stage of the protection switching sequence.

The SF and SD flags that are signalled to the core unit, use allocated signalling bytes within the SOH of the internal traffic signals to the core unit.

The core unit monitors the two flags from each bearer SDH interface unit by internal ASIC (Application Specific Integrated Circuit) polling, every 8ms. The states are returned to the protection switching control function, which takes appropriate action. It ignores further flag state changes until all protection-switching actions are completed for the current flag states.

Signal Fail (SF) Flag

The Signal Fail (SF) flag is declared and signalled if certain failures are detected on the multiplexed layers of the incoming bearer STM-n signal in which the protected VC is contained. These represent (SNC/I), server layer, inherent monitoring.

Additionally, the flag is declared and signalled if failures are detected on the incoming protected VC-path layer. These represent (SNC/N), client layer, non-intrusive monitoring by the VC- POM functions on the bearer SDH interface units. These functions are autonomously enabled when you configure a protected VC- SNC.

The failure types are listed in Table 7-10, which identifies the protection classification for each fault type and any operator configurable enable/disable attributes.

Note: In international standards terminology:

- If all SNC/N class fault types are disabled (including signal degrade fault types), then the SNC protection classification is identified as SNC/I.
- If any SNC/N class fault types are enabled, then the SNC protection classification is identified as SNC/N (this implies SNC/I + SNC/N).

Table 7-10: Fault Criteria for Setting SNCP SF Flags

Serial	Fault Type	Protection Class	Enable/ Disable	Application Notes
1	STM-n Loss of Signal (RS-LOS)	SNC/I		All VC layer SNCPs
2	STM-n Loss of Frame Alignment (RS-LOF)	SNC/I		All VC layer SNCPs
3	Multiplex Section AIS (MS-AIS)	SNC/I		All VC layer SNCPs
4	Multiplex Section Excessive BER (MS-EXC)	SNC/I	YES	All VC layer SNCPs
5	Rx AU Loss of Pointer (HP-LOP)	SNC/I		All VC layer SNCPs

Serial	Fault Type	Protection Class	Enable/ Disable	Application Notes
6	AU- Path AIS (HP-AIS)	SNC/I		All VC layer SNCPs
7	Loss of TU Multiframe (HP-LOM)	SNC/I		only VC-1/2 layer SNCP
8	TU Loss of Pointer (LP-LOP)	SNC/I		only LO VC layer SNCP
9	TU- Path AIS (LP-AIS)	SNC/I		only LO VC layer SNCP
10	HO Path Excessive BER (HP-EXC)	SNC/N	YES	only HO VC-4 layer SNCP
11	HO Path Signal Label Mismatch (HP-PLM)	SNC/N	YES	only HO VC-4 layer SNCP
12	HO Path Signal Label Unequipped (HP-UNEQ)	SNC/N	YES	only HO VC-4 layer SNCP
13	HO Path Trace Mismatch (HP-TIM)	SNC/N	YES	only HO VC-4 layer SNCP
14	LO Path Excessive BER (LP-EXC)	SNC/N	YES	only LO VC layer SNCP
15	LO Path Signal Label Mismatch (LP-PLM)	SNC/N	YES	only LO VC layer SNCP
16	LO Path Signal Label Unequipped (LP-UNEQ)	SNC/N	YES	only LO VC layer SNCP
17	LO Path Trace Mismatch (LP-TIM)	SNC/N	YES	only LO VC layer SNCP

In general, enabling/disabling criteria from the VC- POM functions, which set the SF flag, are not handled within the protection configuration applications.

Enabling/disabling criteria for setting the SF flag are indirectly handled as part of the VC-path maintenance configuration applications of the SMA (events management, and VC connection management). For example, if Path Excessive BER defects are enabled/disabled as alarm reports, the same applies to their contribution to setting the SF flag.

VC-path Signal Labels are autonomously allocated to VC- connections by the Multiplexer Controller connection management applications. At SMAs where the end-to-end VC- trAIL is terminated, specific signal label codes are allocated.

At intermediate node SMAs, where the VC-trail is through-connected, equipped non-specific codes are allocated. With the setting up of VC- connections, the signal label fault type reporting is autonomously enabled.

You can globally disable the individual fault type reporting for PLMs and UNEQs and this disables the fault type contribution to setting the SNCP SF flag, in common.

Within VC-trail connection management applications, you can enable/disable VC-path trail trace processing, on a per-connection basis, at each network SMA that transports a VC-trail across the network. This processing includes the allocation of unique Trail Trace Identifiers for each connection, and autonomously enables/disables TIM fault type reporting. This also enables/disables the TIM fault type contribution to setting the SNCP SF flag.

Signal Degrade (SD) Flag

The Signal Degrade (SD) flag is only declared and signalled if degraded path performance failures are detected on the actual incoming protected VC-path layer. These also represent (SNC/N), client layer, non-intrusive monitoring by the VC- POM functions on the bearer SDH interface units. These functions are autonomously enabled when you configure a protected VC- SNC.

The failure types are listed in Table 7-11, which identifies the protection classification for each fault type and any operator configurable enable/disable attributes.

Table 7-11: Fault Criteria for Setting SNCP SD Flags

Fault Type	Protection Class	Enable/ Disable	Application Notes
HO Path Signal Degrade (HP-DEG)	SNC/N	YES	only HO VC layer SNCP
HO Path Unacceptable Short-term Errors (HP-DEG)	SNC/N	YES	only HO VC layer SNCP
LO Path Signal Degrade (LP-DEG)	SNC/N	YES	only LO VC layer SNCP
LO Path Unacceptable Short-term Errors (LP-DEG)	SNC/N	YES	only LO VC layer SNCP

Enabling/disabling criteria from the VC- POM functions for setting the SD flag can either be handled within the protection configuration applications, or within the VC-path maintenance configuration applications of the SMA (events and traffic connection management). Your can configure degraded path performance fault reporting on a per-path basis. The configurations include the following:

- Fault report disabled
- Fault report based on equivalent BER calculations - Path Signal Degrade alarms reported
- Fault report based on Unacceptable Short-Term Error performance calculations - Path USE alarms reported
- Fault report based on Degraded Error performance calculations - Path Signal Degrade alarms reported.

The defaults are fault reporting enabled for USE alarm reporting.

Whatever attributes are configured for fault reporting, they are used as the Enable/Disable configurations for setting the SNCP SD signalling flag, and vice-versa.

- The Signal Degrade fault type works on BIP bit equivalent binary error ratio calculations (e.g. ratio 10e-6). The USE fault type works on the crossing of a threshold of consecutive severely errored seconds. These are calculated for each VC-path by the VC- bearing SDH interface unit.

- Degraded path performance is based on Consecutive Degraded Seconds (CDEGS). This means that separate configurable thresholds are required for SES (performance monitoring) and DEGS (events handling).

- You can configure the Signal Degrade fault type to work on BIP BERs, or CDEGS.

- SNC protection switching can also be based on long-term error performance monitoring statistics from 15min/24hour performance reporting by the SMAs. This form of switching criteria is determined externally, and input by operator command.

Multiplexer Controller Restoration

If the Multiplexer Controller has been removed, when it is replaced it interrogates the other Core Card in the system for the current settings of protection to ensure the states are not changed

7.5.3.2 Operator Entered Commands

The SNC protection switching mechanism also receives operator inputs. An operator enters these commands via the LCT or NMI.

For each operator-entered event a brief description of the required system behaviour is given below. The names of the commands are those that are specified for use on the Local terminal. In the bi-directional mode of operation, the command is sent to the other end of the path using the POH bytes.

These states are stored and used to restore the equipment to its previous state in the case of loss of power.

The protection state of the selected channel is displayed by the element manager.

Forced Switch to Worker

Causes traffic to switch to, or be maintained on, the designated working channel. This command has a higher priority than locally detected failures on the working channel and therefore traffic remains on the working channel regardless of any failure indications on this channel.

Forced Switch to Protection

Causes traffic to switch to, or be maintained on, the designated protection channel. The command has a higher priority than locally detected failures on the protection channel and therefore traffic remains on the protection channel regardless of any failure indications on this channel.

Manual Switch to Worker

Causes traffic to switch to, or be maintained on, the designated working channel unless a higher priority switch state is in effect. Locally detected conditions on the working channel (SF and SD) have a higher priority than the manual switch command.

Manual Switch to Protection

Causes traffic to switch to, or be maintained on, the protection channel unless a higher priority switch command is in effect. The manual switch command has a lower priority than locally detected conditions on the protection channel.

Clear

Clears any of the above-entered commands and any active WTR states.

7.5.3.3 Remote Multiplexer Requests

1+1 SNC protection switching mechanism is available in bi-directional mode only; to respond to messages received from the multiplexer at the remote end of the VC path.

These events are used to set the switch state for both ends of a bi-directional protected SNC and are received via the V5 or G1 byte of the VC POH.

The remote events are:

- Switch (or maintain) traffic on working channel
- Switch (or maintain) traffic on protection channel.

These are derived from operator requests entered at the remote end or from the local failure conditions detected by the remote end.

7.5.3.4 Wait to Restore and Non-Revertive Mode No Request States

The SMA enters either *Wait to Restore* or *Non-revertive mode No Request* state when the working channel recovers from a failure.

The wait to restore state is entered automatically when traffic is selected from the protection channel (due to a failure of the working channel) and the working channel subsequently recovers. The state occurs only in Revertive mode of operation. Entry to the wait to restore state is inhibited if a higher priority condition exists when the working channel recovers.

When the wait to restore state is entered, a timer is set and the condition is de-activated upon expiry of the timer period. The condition is also de-activated (and the timer reset) if a higher priority condition is received during the timer period.

The timer is an operator configurable option, selectable from zero to 30 minutes in one-minute (+/- 5 second) steps.

Selection of the zero minute option prevents a protected VC from ever entering the wait to restore condition (it de-selects the Wait to Restore option).

The wait to restore timer value can be set both as a global option for all protected VCs in the system, and on an individual basis. The default value is 10 minutes.

Note: You are only be able to retrieve WTR values from the NE on an individual path basis.

In non-revertive mode of operation, a *No Request* state is entered automatically when traffic is selected from the protection channel (due to a failure of the working channel) and the working channel subsequently recovers.

A *No Request - Traffic on Protection* state is reported. This is the equivalent to a *Do not Revert* state as used in Linear MSP schemes, since in non-revertive mode, the switch selector is held on the protection channel, rather than restoring to the worker channel.

The *No Request - Traffic on Protection* is entered under the same circumstances as wait to restore. However, there is no timer associated with this state, and it remains active until a higher-level condition is received. At this point, it is reset and a new state entered.

If *No Request - Traffic on Protection* is active, it is reset immediately by re-configuration of the SMA into Revertive operating mode.

On power up of an SMA (causing a main reset), the SMA ensures that traffic defaults are selected from the working channel, assuming that no failure indications or operator commands require selection from the protection channel.

On power-up, the protection switching control mechanism does not allow the selection of the protection channel with the *Wait to Restore* or *No Request - Traffic on Protection* states active.

7.5.4 Protection Switching Control for SNCP

7.5.4.1 Protection Switching Operation

For a protected SNC the traffic selector can be in only one of two possible states according to the position of the selector switch (see Table 7-12). These states are therefore receiving traffic from the working channel and receiving traffic from the protection channel.

The switch state is governed by the indications that are active at that time. These indications comprise failure flags or path performance, entered-operator commands (via NMI) and remote end requests.

The *Wait To Restore* and *Do not Revert* conditions affect the state of the selector depending on the mode in which the protection mechanism is operating.

The switching indication received and the resultant position of the selector switch are shown in Table 7-12. The conditions are listed in priority order. The position of the selector is determined by the highest priority indication active at any time.

The naming convention used for the indications is that the channel name given in brackets is the channel for which the state is active. For example, Forced Switch (protection) is the Forced Switch command for the protection channel and results in traffic being selected from the working channel.

Table 7-12: SNC Protection Switch Requests and Resultant Position of Receive Selector

Priority	Request Received	Selected Channel
1	Forced Switch (Protection)	Working
2	Forced Switch (Wch)	Protection
3	Signal Fail (Protection)	Working
4	Signal Fail (Wch)	Protection
5	Signal Degrade (Protection)	Working
6	Signal Degrade (Wch)	Protection
7	Manual Switch (Protection)	Working
8	Manual Switch (Wch)	Protection
9	Wait To Restore [Note 2]	Protection
10	Remote Switch (Protection) [Note 1]	Working
11	Remote Switch (Wch) [Note 1]	Protection
12	No Request	

Note: **1**. Remote Switch applies in bi-directional mode only.

Note: **2**. Wait to Restore applies in revertive mode only.

7.5.4.2 Operator Commands for SNC Protection Configuration

Before the protection switching mechanism can be controlled, you must configure the different parameters related to the type of protection for each protected path.

You enter these commands via the local terminal or from the EM.

For each SNC to be protected:

1 Connection to be protected and protection connection.

- It is possible to add protection to any existing VC connection whether it is a normal bidirectional connection or a uni-directional broadcast connection. Applying SNC protection to a unidirectional broadcast connection results in VC-connections being automatically added between the other broadcast destinations in the network, and the protection paths.

- A protection path VC- connection, when configured adopts the same admin. state as its associated worker path connection. Any subsequent change to the admin state of the worker path are automatically adopted by the protection path, and vice-versa.

2 Operating Mode:

- Unidirectional
- Bi-directional
- Revertive
- Non-revertive.

3 Wait to Restore (if Revertive mode) - Global and per path, Default: 10min.

4 Enable/Disable Protection.

5 Swap Worker/Protection connections.

6 Force Switch Traffic to Working channel.

7 Force Switch Traffic to Protection channel.

8 Manual Switch Traffic to Working channel.

9 Manual Switch Traffic to Protection channel.

10 Clear Operator Switch command.

7.5.5 Protection Switching Time

The following are maximum protection switching times for VC channels:

- Unidirectional mode: 50 ms
- Bi-directional mode: 100 ms.

These times are defined from the point at which a local failure is detected or a remote request is received, to the point at which traffic is restored at the appropriate tributary card output port after selection of the other VC channel.

The changeover time of the receive selector is less than 20 micro-seconds. This is the maximum time of disturbance to the VC appearing at the traffic output port of the core unit.

The maximum time to execute an operator entered switch command, via the local terminal, is eight seconds. This time is taken from the entry of a command at the local terminal to the point at which the command is acknowledged.

The full bi-directional switching time, to guarantee full reversion, is 10s.

7.6 1+1 Tandem VC-Trail SNC Protection (TSNCP)

7.6.1 Introduction to TSNCP

Full-TCM monitoring functions add VC-path, client layer, fault types to the list of criteria for setting the internal SF/SD flags of SNC protection schemes, which initiate autonomous protection switching actions. When TCM fault types are included in the protection switching criteria, the operator configured protection scheme is referred to as Tandem Subnetwork Connection Protection (TSNCP).

A tandem connection is a segment of a VC-trail, a SNC, which typically spans across only a single network operator domain, and on which TCM functions have been configured.

If you have not configured TCM on your VC-trail segment, this segment is another normal SNC, and can be protected by 1+1 SNCP.

If you have configured TCM on the VC-trail segment, it is classed as a tandem SNC, and can be protected by 1+1 TSNCP.

TCM functions allow you to monitor the performance of a VC-path across the specific segment, which lies within your administrative domain. This is known as sub-layer monitoring. It does not affect the ability for normal end-to-end VC-path monitoring across the whole network(s).

7.6.2 Modes of Operation for TSNCP

The operator configurable modes of operation, including TSNCP persistency, are as described in Section 7.5.2 above, for VC-trail SNCP.

Similar to SNCP, if TSNCP is applied across the complete end-to-end tandem VC-trail then the two SMAs involved can operate in bi-directional switching mode.

Note: This is only true when the SMAs are handling bidirectional traffic signals on normal bidirectional VC-trail TSNCs.

The default mode is bi-directional and this should always be selected if the following conditions are met:

- The two SMAs are commissioned as full-TCM NE types
- The two SMAs are configured for TCM processing
- Tandem Connection Termination functions (TCTs), and not monitor functions (TCMs), are configured on the worker/protection bearer SDH interface units at each SMA, i.e. the node being configured is actually terminating a tandem VC-trail and not just monitoring at an intermediate node along the trail).

7.6.3 Protection Switching Criteria for TSNCP

In general, the TSNCP switching criteria follows the same principles as defined in Section 7.5.3 above, for VC-trail SNCP. However, additional fault types act as criteria for setting the internal SF/SD signalling flag for autonomous protection switching.

There is also a different bi-directional APS switching protocol, which renders different remote switching requests from the SMA at the far end of a protected tandem VC-trail. The protection switching criteria for TSNCP are set out below.

7.6.3.1 Locally Detected SF/SD Flag Failure Requests

These switching requests arise from local detection of VC-trail fault types which act as criteria for setting the internal SF/SD signalling flags for autonomous protection switching. In the case of TSNCP, new fault types are added to the lists, from monitoring over the tandem sub-layer VC-trails.

The SF flags are generated by outputs from the RST/MST/MSA/HPA/HPT functions, the tandem VC-TCT/TCM functions, and the VC-POM functions. These functions all reside on the bearer SDH interface units. The TCT/TCM functions are autonomously enabled when you configure a protected tandem VC-SNC.

Depending on the network applications of TSNCP, these new fault types can either add to the list of fault types, or provide alternatives to the lists. The complete fault type listings are covered in Table 7-13 and Table 7-14 below.

Table 7-13: Fault Criteria for Setting TSNCP SF Flags

Fault Type	Protection Class	Enable/ Disable	Application Notes
STM-n Loss of Signal (RS-LOS)	SNC/I		All VC layer SNCPs
STM-n Loss of Frame Alignment (RS-LOF)	SNC/I		All VC layer SNCPs
Multiplex Section AIS (MS-AIS)	SNC/I		All VC layer SNCPs
Multiplex Section Excessive BER (MS-EXC)	SNC/I	YES	All VC layer SNCPs
Rx AU Loss of Pointer (HP-LOP)	SNC/I		All VC layer SNCPs
AU- Path AIS (HP-AIS)	SNC/I		All VC layer SNCPs
Loss of TU Multiframe (HP-LOM)	SNC/I		only VC-1/2 layer SNCP
TU Loss of Pointer (LP-LOP)	SNC/I		only LO VC layer SNCP
TU- Path AIS (LP-AIS)	SNC/I		only LO VC layer SNCP
HO Path Excessive BER (HP-EXC)	SNC/N	YES	only HO VC-4 layer SNCP
HO Path Signal Label Mismatch	SNC/N	YES	only HO VC-4 layer SNCP

Fault Type	Protection Class	Enable/ Disable	Application Notes
(HP-PLM)			
HO Path Signal Label Unequipped (HP-UNEQ)	SNC/N	YES	only HO VC-4 layer SNCP
HO Path Trace Mismatch (HP-TIM)	SNC/N	YES	only HO VC-4 layer SNCP
HO Path VC-AIS (HP-VC-AIS)	SNC/N	YES	only HO VC-4 layer SNCP when set up on a tandem VC trail
LO Path Excessive BER (LP-EXC)	SNC/N	YES	only LO VC layer SNCP
LO Path Signal Label Mismatch (LP-PLM)	SNC/N	YES	only LO VC layer SNCP
LO Path Signal Label Unequipped (LP-UNEQ)	SNC/N	YES	only LO VC layer SNCP
LO Path Trace Mismatch (LP-TIM)	SNC/N	YES	only LO VC layer SNCP
LO Path VC-AIS (LP-VC-AIS)	SNC/N	YES	only LO VC- layer SNCP when set up on a tandem VC trail
HO TC Loss of Tandem Connection (HTC-LTC)	SNC/S	YES	only HO tandem VC layer TSNCP
HO TC VC-AIS (HTC-incAIS)	SNC/S	YES	only HO tandem VC layer TSNCP
HO TC Unequipped (HTC-UNEQ)	SNC/S	YES	only HO tandem VC layer TSNCP
HO TC Trace Mismatch (HTC-TIM)	SNC/S	YES	only HO tandem VC layer TSNCP
HO TC Excessive BER (HTC-EXC)	SNC/S	YES	only HO tandem VC layer TSNCP
LO TC Loss of Tandem Connection (LTC-LTC)	SNC/S	YES	only LO tandem VC layer TSNCP
LO TC VC-AIS (LTC-incAIS)	SNC/S	YES	only LO tandem VC layer TSNCP
LO TC Unequipped (LTC-UNEQ)	SNC/S	YES	only LO tandem VC layer TSNCP
LO TC Trace Mismatch (LTC-TIM)	SNC/S	YES	only LO tandem VC layer TSNCP
LO TC Excessive BER (LTC-EXC)	SNC/S	YES	only LO tandem VC layer TSNCP

Table 7-14: Fault Criteria for Setting TSNCP SD Flags

Fault Type	Protection Class	Enable/ Disable	Application Notes
HO Path Signal Degrade (HP-DEG)	SNC/N	YES	only HO VC layer SNCP
HO Path Unacceptable Short-term Errors (HP-DEG)	SNC/N	YES	only HO VC layer SNCP
LO Path Signal Degrade (LP-DEG)	SNC/N	YES	only LO VC layer SNCP
LO Path Unacceptable Short-term Errors (LP-DEG)	SNC/N	YES	only LO VC layer SNCP
HO TC Signal Degrade (HTC-DEG)	SNC/S	YES	only HO Tandem VC layer TSNCP
HO TC Unacceptable Short-term Errors (HTC-DEG)	SNC/S	YES	only HO Tandem VC layer TSNCP
LO TC Signal Degrade (LTC-DEG)	SNC/S	YES	only LO Tandem VC layer TSNCP
LO TC Unacceptable Short-term Errors (LTC-DEG)	SNC/S	YES	only LO Tandem VC layer TSNCP

7.6.3.2 Locally Entered Operator Switching Requests

These Forced Switch, Manual Switch, Clear requests are as described for VC-trail SNCP in Section 7.5.3.2 above.

7.6.3.3 Remote Multiplexer Switching Requests (Bi-directional Switching Mode)

The TSNCP protection switch controller responds to remote requests from the SMA at the far end of the protected tandem VC-trail, when operating in bi-directional mode. Each protection switch controller generates these requests from its own locally detected failures, conditions, and operator entered switch requests. It transmits them over the (network) APS channels to the far end. The request types are listed below:

1 Forced Switch (Worker Channel).

2 Forced Switch (Protection Channel).

3 Manual Switch (Worker Channel).

4 Manual Switch (Protection Channel).

The above remote requests are derived from operator entered requests. They carry the same weighting as locally entered operator requests.

5 Signal Fail (Worker Channel).

6 Signal Degrade (Worker Channel).

7 Signal Fail (Protection Channel).

8 Signal Degrade (Protection Channel).

9 The above remote requests (5 to 8) are derived from detected failures on the worker/protection trails. They carry the same weighting as locally detected failure requests.

10 Wait To Restore (Worker Channel).

Wait-to-Restore is used in revertive mode, and is transmitted when a protection switch controller detects a working trail recovery, but is applying a Wait to Restore timeout before allowing the switch selector to switch back from the protection trail.

After time-out expires, if no other higher priority request is active, a No Request (Protection Channel) request is transmitted.

11 No Request (Worker Channel) [Meaning - Do Not Revert].

No Request (Worker Channel) is used in non-revertive mode to mean Do Not Revert. It is issued to instruct the remote protection switch controller to maintain its switch selector on the protection trail, even though a working trail failure has recovered.

12 No Request (Protection Channel).

This is the idle condition signalled when neither a higher priority request, nor acknowledgement is active. However after a switch to protection in Non-revertive mode, when idle conditions subsequently prevail, a No Request (Worker Channel) condition is signalled (meaning Do Not Revert).

7.6.4 APS Protocol Failure - Fault Types

There are three possible failure conditions within the TSNCP APS protocol, which are detected by the protection switch controller, and cause a TSNCP APS Protocol Fail alarm to be raised.

1 Architecture Mismatch.

Raised if the data patterns received from the APS channel indicate a different usage to that expected, and such an anomoly persists for a period of >/= 100ms.

2 Protocol Failure.

Raised if a mismatch between the transmitted and received values of APS channel bit 1(for worker/protection request ID) persists for a period of >/= 500ms.

3 Mode Mismatch.

Raised if a mismatch of the local and remote SMA operating modes is detected as shown in Table 7-18.

Table 7-15: TSNCP Mode Mismatch

Local	Remote
Bidirectional revertive	Bidirectional non-revertive
Bidirectional non-revertive	Bidirectional revertive

The criteria for this failure is based on that specified for STM-n Linear MSP schemes, but with the following exceptions:

- The three failure conditions are logically ORed to provide a single alarm indication, TSNCP APS Protocol Fail. It identifies that either the APS protocol data is corrupted, or bi-directional ganged switching is not occurring at the two SMAs involved, or the TSNCP operating modes are not identically configured at each of the two SMAs.

7.6.5 Protection State Reports

The following lists identify the various states of the TSNCP protection switch controller, and which are reported.

1 TSNCP States - Locally Initiated Only.

- No Request - Traffic on Worker
- No Request - Traffic on Protection
- Remote Request to Worker - Traffic on Worker
- Remote Request to Protection - Traffic on Protection
- Do not Revert - Traffic on Protection
- Wait to Restore - Traffic on Protection
- Manual Switch to Protection - Traffic on Protection
- Manual switch to Worker - Traffic on Worker
- Signal Degrade on Worker - Traffic on Protection
- Signal Degrade on Protection - Traffic on Worker
- Signal Fail on Worker - Traffic on Protection.
- Forced Switch to Protection - Traffic on Protection
- Signal to Worker - Traffic on Worker.

2 TSNCP States - Remotely Initiated Only.

- No Request - Traffic on Worker
- No Request - Traffic on Protection
- WTR/Manual Switch to Protection - Traffic on Protection
- WTR/Manual switch to Worker - Traffic on Worker
- Signal Fail/Signal Degrade on Worker - Traffic on Protection
- Forced Switch to Protection - Traffic on Protection
- Signal Fail/Signal Degrade on Protection - Traffic on Worker
- Forced Switch to Worker - Traffic on Worker.

7.7 Traffic Core Card Protection

7.7.1 Introduction to Traffic Core Card Protection

Core card protection provides equipment level protection for the core switch. The scheme is an equipment level protection scheme, which provides a means of fast, autonomous recovery from card failures.

Given that the core cards support the SDH line interface modules, failure/removal of a core card will also mean that line interfaces become unavailable. Protecting failure/removal of line interfaces can only be achieved by independently setting up linear MSP protection on pairs of line interfaces, across A and B Core Cards. Alternatively (or inclusively), path layer SNCP protection of traffic would be set up using pairs of SDH line interface bearers across A and B Core Cards.

In summary, configuring core card/core tributary protection, linear MSP and/or path layer SNCP may be necessary to achieve full equipment level protection of the multi-function core card, its SDH line interface modules and its dependant core tributary card.

Note: Linear MSP, SNCP, 1:1 generic trib card protection, and PDH trib port protection schemes all operate independently of the core card protection scheme.

Note: MS-SPRING is also available with the STM-4/16 core units to protect the line interfaces.

An SMA may be operated with or without core unit protection.

For unprotected operation, only a single core unit is necessary. The position of the Core card depends on what subrack you are using and what naming convention that you are using:

- In OMS 1240 Core A goes in physical slot S1-04 or logical LCT slot 1-9
- In OMS 1260 Core A goes in physical slot S1-07 or logical LCT slot 1-26

Protected operation is provisioned by duplication of the core unit and appropriate system configuration.

On power-up, in a system equipped with both core units, the destination ports of a peripheral traffic card select traffic from Core A.

Core card protection operates by duplication of the switch core on a protected pair of core cards. Internal pSTM-1 traffic and timing interfaces are duplicated from both core switch functions to all peripheral traffic interface cards and the line and tributary traffic modules of the core cards themselves.

Peripheral traffic cards and modules can autonomously switch between Core Card A and B switch functions, this being determined by monitoring switch status for failure. Failures are determined by monitoring for traffic signal clock failures and errors in Switch Diagnostics Messages (SDMs), which the CCU controller embeds into every VC- traffic connection across the core switch planes.

Traffic cards and modules report switchplane failures to the CCU controller and it initiates master/slave changeover.

Since the CCU function is integrated onto Core Card A, failure of a core card also means failure of the CCU. There is therefore a mechanism to allow a current slave core card to autonomously initiate take-over to become the new master.

Note: Core protection does not cause an associated MSP, SNCP switch. To move working traffic to the master core card, prior to removal of a slave card, you may need to perform manual protection switching actions at a number of network nodes.

To prevent transient alarms and spurious protection switching, the following protection mechanisms and alarms are suspended for the duration of the switch plane changeover:

- Protection Schemes:
  - SNC Protection
  - PDH Port Protection
  - Linear MSP Protection
  - Switch Diagnostic Messaging (for core unit protection).
- Alarm Types:
  - Switch Interface Parity Fail (core card)
  - Switch Interface Parity Fail (Traffic card)
  - Core Card Fail (Traffic card)
  - MSP Architecture Failure (core card)
  - MSP Protocol Failure (core card).

The slave switch, following reconfiguration, signals completion of switch plane changeover and after a delay of 500ms, the MC releases suspension of the protection mechanisms and alarms.

In case of failure of Switch A, while Switch B is operating correctly, the fault is reported to the Multiplexer Controller, this puts Core Unit A out-of-traffic. The Multiplexer Controller then instructs all destination ports to continue to select Switch B even if a fault on that unit is detected.

If both core units fail simultaneously, no switchover occurs and the Multiplexer Controller is informed of the failures.

7.7.2 Modes of Operation

It is possible to commission the system with either one or two core cards. Equipping options of core cards and their SDH line interface modules are shown in Figure 7-9.

Figure 7-9: STM –1/4 Core Card Equipping Options

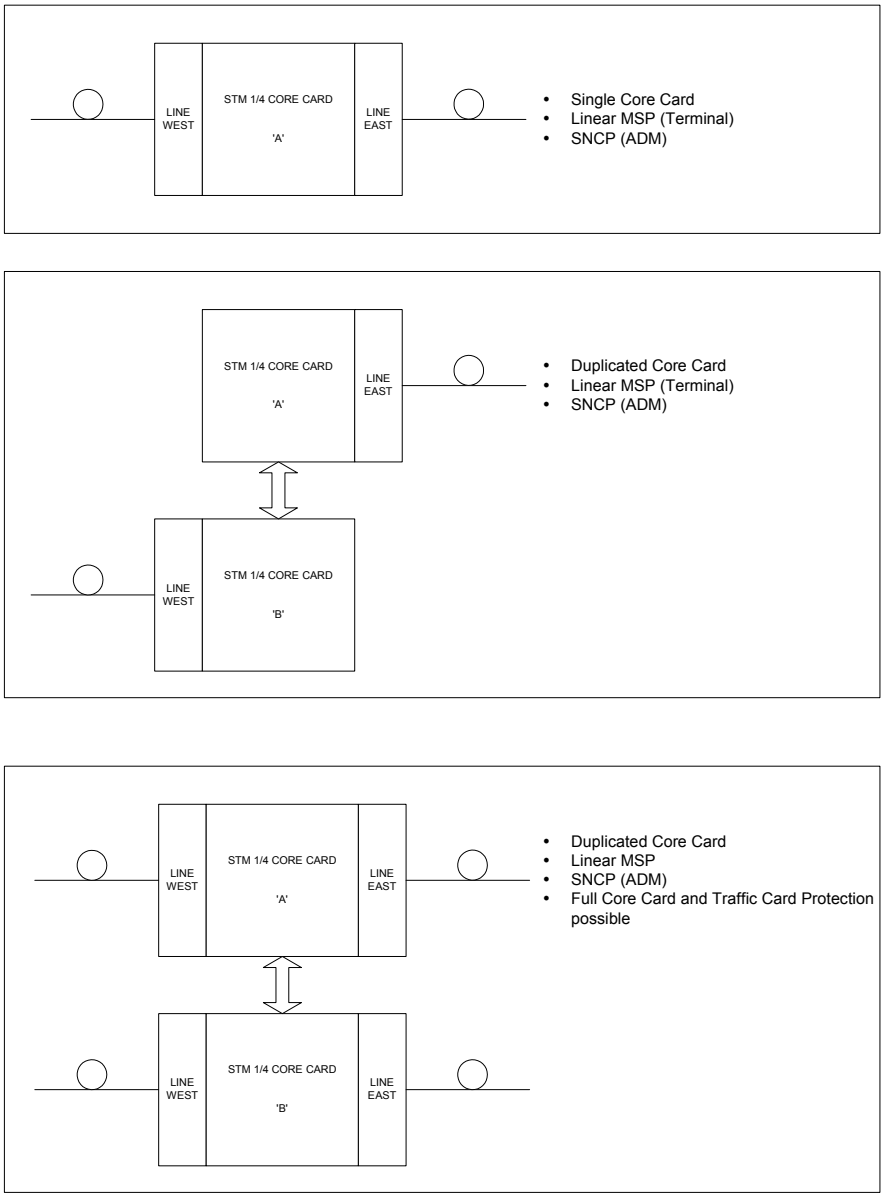
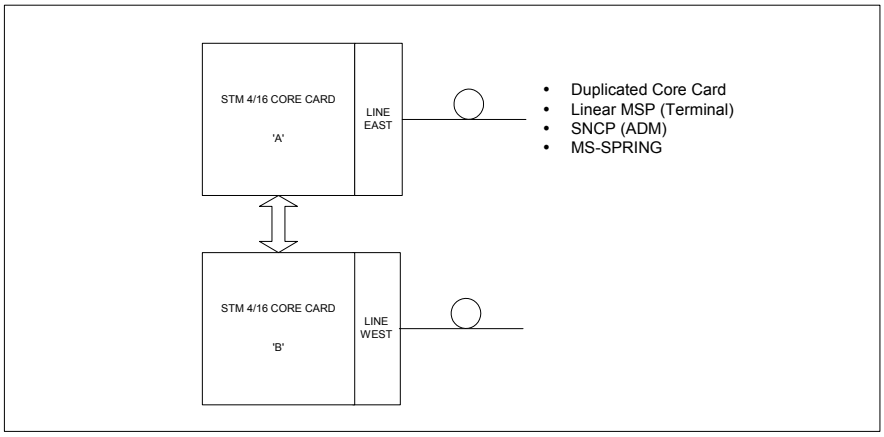


Figure 7-10: STM-4/16 Core Card Equipping Options



For an in-traffic, unprotected system, core card protection is commissioned by the logical addition of a second core card (Traffic Core B).

Note: Core card protection always operates in non-revertive mode; logically adding a second core card to an in-traffic system does not instigate protection switching by peripheral traffic cards and functions (i.e, traffic affecting switching is avoided unless contra-indicating failures are detected).

On power-up, a system in which two switch units are fitted defaults to protected operation and the card-in-traffic indicator is lit on cards of both core units. This indicates that removal of a card of either core unit may disrupt traffic.

Note: Although one core is not carrying traffic, the In-traffic LED is lit.This indicates that both core cards are available to pass traffic and it is unsafe to remove either core card.

7.7.2.1 Reconfiguration for Protected Operation

To add core unit protection to a currently unprotected traffic-carrying system, a second core unit is fitted to the equipment shelf. Once the unit has been logically added to the shelf, the card-in-traffic indicator of the added core unit is lit and the protection mechanism activated. The traffic from the original switch unit remains selected by the destination ports (preventing any unnecessary, traffic-degrading switchovers).

7.7.2.2 Removal of a Core Unit from a Traffic Carrying SMA

During operation, it may become necessary to remove one of the cards from a system that is carrying traffic.

Note: Removing Traffic Core A also removes the NE's CCU function, therefore forced switches must be put in place before removing cards.

Three possible situations arise:

1 Removal of a failed core card.

On detection of a core card failure, the Mux Controller instructs all destination ports to select traffic from the other core unit. The failed core card is then taken out-of-traffic by the Mux Controller. The card-in-traffic indicator of the failed unit is extinguished indicating that card may be removed without degradation of traffic. On replacement of the core card, the system automatically reverts to protected operation.

2 Removal of a working non-selected core card.

The card-in-traffic indicators are illuminated on both cards, indicating that removal of either card may cause errors. In this case, you must switch the unit out-of-traffic via the local terminal by issuing a Forced-Switch to the other core-unit. Removal of this unit may then be carried out without degradation of traffic. [Note 2].

3 Removal of selected core card.

The card-in-traffic indicators are illuminated on both cards. Before the card is removed, the selected traffic must first be manually switched to the other core unit using the Local Terminal by instructing a Forced-Switch to the other core unit. [Note 1 and 2].

Note: **1.** Situation **3** above may cause errors during the switching-over of the selected switch unit and should be avoided if possible.

Note: **2.** To restore core card protection capability, you must issue a Clear Forced Switch command on replacement of the switch unit.

If a core card is removed, on being replaced for the purposes of traffic protection, it is configured according to existing states (i.e. working/protection) as dictated by the other core. This is to prevent the two core units becoming out of phase.

7.7.3 Protection Switching Criteria

Both of the system's peripheral traffic cards detect the same failure criteria for core card protection, and the core card's own traffic modules; namely the SDH line interface modules and the core tributary cards. These line and tributary modules monitor for failures on both their parent core card and the protection core card.

7.7.3.1 Failure Detection

Switch protection operates automatically, according to the conditions detected by the destination ports, or on demand by the Multiplexer Controller.

The conditions, which may initiate switching, are:

- Mismatch on path identification number
- Failure of parity checks
- Failure of alignment (enable/disable)
- Loss-of system-clock transitions.

Failure of Path ID Number

At each destination port, the path identity number of each channel, inserted by the sender port, is compared with the expected address (downloaded from the Multiplexer Controller configuration-data).

The address check is carried out on traffic from both core units simultaneously, to detect failures of either core. This method of failure detection is subject to a persistence check (refer to Persistence Check of Diagnostic Message Failure) and protection switching is in accordance with the priorities in Section 7.5.3.

Failure of Parity Checks

Parity bits are calculated at the sender port and inserted into the diagnostic messages such that even parity is maintained in each channel. At the destination port, the parity of each channel is calculated again and any parity errors generate an alarm. The parity check is carried out on traffic from the working core and the standby core simultaneously. This method of failure detection is subject to a persistence check (see Persistence Check of Diagnostic Message Failure) and protection switching is in accordance with the priorities in Section 7.5.3.

You may enable/disable parity checks on an individual channel or global basis.

Loss of System Clock Transitions

Each peripheral card incorporates transition-loss detectors, which monitor the internal clock signals from each core. Failure of the clock is defined as a loss-of clock transitions for a period exceeding a nominal threshold of 125-500ns. There is no further persistency check on clock failures.

Failure of Alignment

If the alignment bits contained within the diagnostic messages are incorrect, the detecting destination port generates a loss-of-frame alarm. This check is subject to the persistence check (refer to Persistence Check of Diagnostic Message Failure) and protection switching is in accordance with the priorities in Section 7.5.3. You may enable/disable this check.

Demand by the Multiplexer Controller

A request to switch is issued to all destination ports on receipt of a core-failure indication by the Multiplexer Controller. You may issue a request via the NMI. These requests are treated as core-failure conditions. No persistence check is carried out on such conditions.

Persistence Check of Diagnostic Message Failure

In cases of diagnostic message failure, a persistence is performed to prevent spurious switching during transient conditions (e.g. MSP switching). This check takes the form of a threshold on the number of permissible consecutive mismatches of the diagnostic messages. A hardware persistence is applied independently to each VC. You can set this persistence between 1-- 256 successive failures of the check for VC 3/4, and 1 - 7 for VC 1/2. The value is global for all VC 1/2s and VC 3/4.

7.7.4 Further Protection Switching Criteria

In general, the criteria for initiating core card protection switching are the same as for SMA switch card protection. These specify forced switching under operator control and automatic switching actioned by peripheral traffic cards, either by themselves, or on instruction from the CCU controller. The latter is based on the Switch Diagnostics Messaging (SDM) scheme.

The same failure criteria for core card protection is detected by both the system's peripheral traffic cards and the core cards' own traffic modules, namely the SDH line interface modules and the core tributary card modules. These line modules/tributary modules monitor for failures on both their parent core card and the protection partner core card.

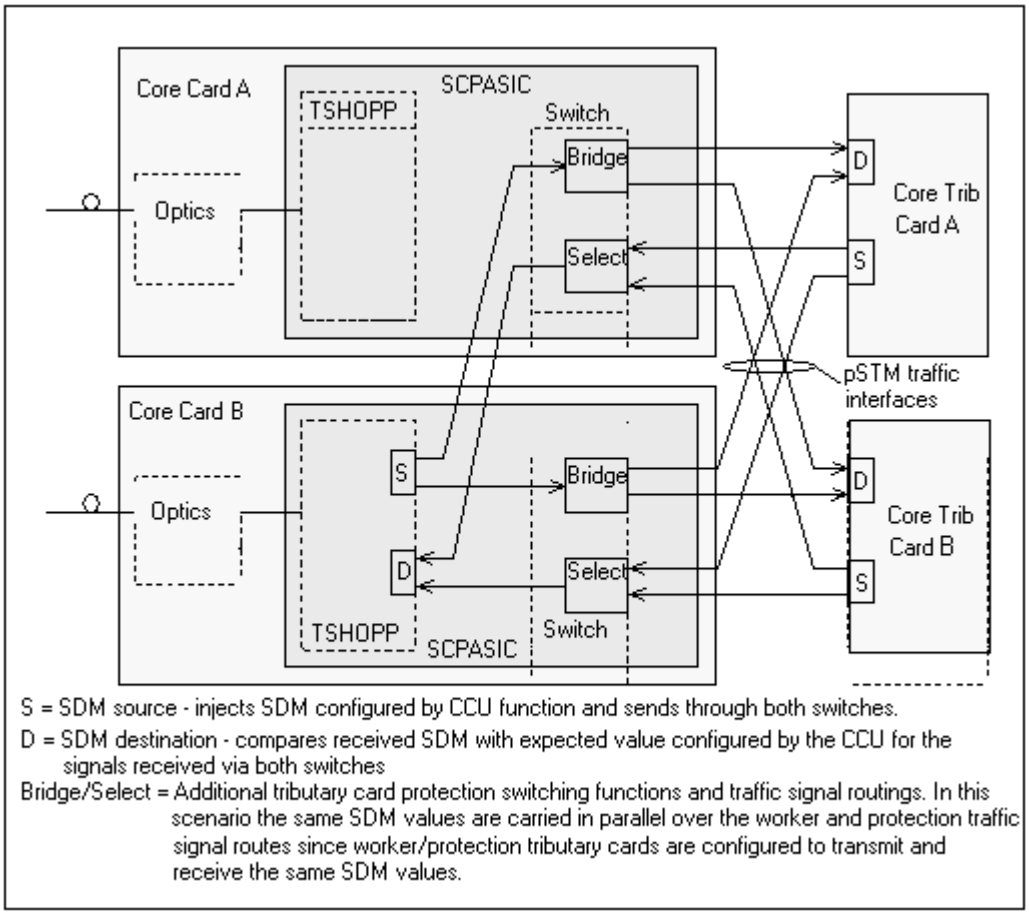
7.7.4.1 Switch Diagnostics Messaging Structure

The SDH line interface functions of the core cards and core tributary functions perform just as ‘peripheral’ traffic cards for the purposes of SDM source and destination handling. Figure 7-11 shows connections between line functions and core tributary functions of OMS 1200 core cards, in a case where core tributary function protection is also configured.

Peripheral traffic cards & modules can autonomously switch between Core Card A & B Switch functions Failures are determined by monitoring for traffic signal clock failures and errors in Switch Diagnostics Messages (SDMs) which the CCU Controller embeds into every VC- traffic connection across the Core Switchplanes.

Configuration of SDM parameters is handled by the CCU's traffic management subsystem. Core switch failures are reported to the CCU by the current master core’s line/tributary functions, and these are independent to the reporting of core switch matrix status.

Figure 7-11: SDM Architecture – Example Connections with the OMS 1240



7.7.4.2 Operator Switching Commands

Operator Forced Switch commands equally apply to core card protection switching. They invoke protection switching by all peripheral traffic interface cards and modules in the system.

For clarification, you should only use Forced Switch (A or B) commands during maintenance activities when there is a need to remove core cards/core tributary cards from an in-service system. Otherwise, protection switching must be allowed to operate autonomously.

It is important that you Clear any Forced Switch commands when the system is restored with two viable core cards.

Forced Switches have non-pre-emptable, highest priority switching control. Once invoked, they can only be revoked by a Clear command (or another Forced Switch).

Forced Switch effectively locks out all protection capability and overrides all autonomous switching opportunities. The Force is always actioned, even if it means switching to a failed or missing core card. Further, if a master core card that has Forced Switch applied to it subsequently fails; no protection switching actions will be invoked.

7.7.4.3 New Switching Criteria

The following criteria relate to legacy SMA products and OMS 1200 products. They take account of the need for peripheral traffic interface cards to protection switch between the pSTM-1 traffic and timing signals from both core cards.

They also account for:

- In the case of OMS 1240 products:
  - The need of core tributary cards to master/slave switch their protection buffers that determine which card handles traffic signals from the core tributary LTUs. These buffers also determine which card drives the 2Mbit/s PDH tributary port test bus.

Tributary to Switch Traffic Interface Parity Failure Reports OMS 1200 Equipment

A switching criterion related to failure detection of the core card's core tributary function applies to the OMS 1240 equipment. In the OMS 1240, the core tributary functions are separate slide-in units.

The core switch function monitors for switch interface parity failures (indicating tributary function failure) on the switch - tributary pSTM-1 traffic interfaces to both A/B core tributary functions. Failure alarms are reported to the CCU controller by the current master core card and the controller initiates full core card protection switching if the alarms are attributed to the current master core tributary function.

Core Card Failure Monitoring by CCU Function and Using Hardware Control Lines

A hardware logic circuit scheme, along with hardwired monitor and control lines allows the CCU controller function to detect catastrophic failure/removal of a core card, and initiate fast master/slave switching between core cards (and their dependant core tributaries in OMS1240 products).

The nature and behaviour of the scheme is covered in the following subsections.

Core Card Switch to Line Span Protection Traffic Interface Clock Failure Monitoring – (STM-1/4 Core Cards)

A further switching criterion applies, related to core cards monitoring each other for failure.

Switch–to-line span protection pSTM-1 traffic interfaces are crossover tracked between core cards and each card receives switch–to-line and line–to-switch crossover (pT0) signal clocks from its partner.

After power-up initialisation and CCU configuration of a core card, partner core clock failures are detected and reported by each core card to its traffic uController, during routine ASIC polling cycles. The uController interprets these as a partner core card failure/removal state and this is a trigger for a core card (and its dependant core tributary in OMS 1240 products) to autonomously take over master status if it is currently in slave status. It effects a master/slave switchover sequence, just as it would if it received a master status interrupt from the CCU controller via the hardware control lines mentioned above.

If a core card is currently in master status, clock failure detection of its slave partner does not invoke any autonomous master/slave switching actions; this to the extent that no spurious switch actions occur upon insertion/extraction/failure of current slave cards.

- Detecting clock failures from a core card implies a catastrophic ASIC/hardware failure. In this case peripheral traffic interface cards and core traffic modules are assumed to also detect core switch failure (via SDMs) and autonomously switch core traffic signals in parallel.
- The design ensures that clock failure monitoring is negated during insertion, power-up and initialisation of a core card.
- A core card does not initiate the master/slave switchover sequence if the CCU controller has previously invoked a master/slave switch due to an operator Forced Switch command. A core card Controller will receive master/slave switching messages over the CCU control busses, either in reaction to autonomous switching actions, or in response to operator Forced Switch commands.
- If a core card is currently responding to master/slave switching instructions from the CCU controller, concurrent detection of clock failures from its partner takes priority and the core card takes over master status.
- In OMS 1240 systems, master status takeover invokes a full core card and core tributary function takeover, though acknowledging the fact that SETG function master/slave switching is prevented.

- In this system failure/removal of Core Card A will most likely mean that the integrated CCU controller function becomes unavailable. This autonomous core card master status takeover scheme is the only means by which core card/core tributary master/slave switchover can be autonomously invoked by Core B.

- There will be cases where Core Card A is current slave (or even cases where 'A' is current master, Core A traffic functions have failed, but the CCU controller has not). Accordingly, a core card may initiate autonomous master status takeover and then receive master/slave switching instructions from the CCU controller. If this occurs then the core card Controller actions one of the following:

  – On detecting failure of the partner core card, set a timer before autonomously initiating master status takeover. This allows the CCU controller to issue instructions if it can.

  – After initiating master status takeover, it repeats the process if the CCU controller subsequently issues the equivalent instructions (assuming this repeat is not hardware or traffic affecting).

  – After initiating master status takeover, it ignores the CCU controller if it subsequently issues the equivalent instructions. It does however make sure that controller instructions resulting from operator Forced Switch commands are not ignored.

7.7.5 Operator Entered Commands

You may make the following requests:

CAUTION!

You should only use Forced Switch (A or B) commands during maintenance activities when there is a need to remove core cards/core tributary cards from an in-service system. Otherwise, protection switching must be allowed to operate autonomously.

Forced Switch effectively locks-out all protection capability and over-rides all autonomous switching opportunities. The Force is always actioned, even if it means switching to a failed or missing core card. If a Forced Master core card subsequently fails, no protection switching actions are invoked

You must clear Forced Switch commands when the system is restored with two viable core cards/core tributaries

1 Forced Switch to A.

Traffic is selected from Core Unit A, and the in-traffic indicator on Core Unit B is extinguished.

2 Forced Switch to B.

Traffic is selected from Core-Unit B, and the in-traffic indicator on Core-Unit A is extinguished.

Note: Forced Switch can only be revoked by a Clear command or another Forced Switch).

Note: A subsequent failure of the selected core-unit does not cause traffic to be selected from the other core-unit.

3 Clear.

Clears all the above forced switch commands.

The protection state of the currently selected core unit is displayed to you.

7.7.6 Protection Switching Control

7.7.6.1 Protection Switching Operation

In a system configured for switch protection, there are two states for the selector at each destination port, receiving traffic from Core A and receiving traffic from Core B. The clock selected is derived from the same core unit as the selected traffic. Except for a transient period between detection of a failure at one destination port and switchover of all other destination port selectors, all selectors in the SMA are in the same state.

The state of each selector on each peripheral tributary card/core line interface module is governed by the state of core failure indications within the SMA and by commands entered by the operator via the LCT (refer to the “LCT/LCTS Operating Procedures” handbook). The state of the selectors is also affected by previous history, in that switching is non-Revertive and the fault that instigated a changeover may no longer be present.

An instruction to select a core unit received from the Multiplexer Controller overrides all locally detected conditions.

In case of two or more detected failures, with (at least) one failure of each core indicated, the selected core is chosen according to the first failure indication received by the core unit. Any subsequent failure detections will not cause the destination ports to switch to the unit that was first detected as having failed until all failures on that unit are cleared.

With core switchplane protection operation, peripheral tributary cards select internal traffic interfaces between Cores A and B. This is also true of the core cards’ own SDH line interface modules. However, as discussed earlier, linear MSP/SNCP protection schemes involving the core line interfaces will operate independently, if (say) a core card fails or is removed.

In OMS1240, 2Mbit/s traffic is provided by the Core Tributary cards. Each Core Trib Card is a dependant of the Core Card, such that the Core A Card is associated with the Core A Trib and the Core B Card is associated with the Core B Trib. If a Core Card Master/Slave status switch occurs, then Core Tributary worker status will switch in common. This switch (controlled on the tributary cards) determines which Core Trib drives traffic to and from the 2M PDH core tributary traffic LTUs. The result is that 2M PDH traffic is affected when core protection switching occurs.

Version 1 Core Trib cards must be protected if the Core Cards are protected.

Version 2 Core Trib Cards can operate independently of the Master/Slave status when only one Core Trib card is fitted. This allows for Core Trib cards to be unprotected when the system has protected Core Cards.

7.7.6.2 Protection Switching Times

Taking into consideration any VC- traffic cross-connection through the core unit, and the destination port for that connection on any peripheral traffic interface card, autonomous switch unit protection switching by that destination port is effected in </= 10ms. This time is defined as the period between detection of a failure at the destination port, to restoration of error-free traffic for the affected cross-connection.

The failures detected for autonomous protection switching include:

- Switch Diagnostics – Failure of Path ID Number
- Switch Diagnostics – Failure of Parity Checks
- Switch Diagnostics – Failure of Alignment
- Loss of System Clock Transitions.

These failure types are covered in Section 7.7.3.1, above.

Where linear MSP/SNCP protection scheme configurations involve the core line interfaces, these schemes operate independently if (say) a core card fails or is removed. Protection switching times for these schemes are stated earlier in this section.

In the OMS 1240 only, where core cards are configured with core tributary card functions, master/slave protection switching on the tributaries will affect 2M PDH traffic for up to 50ms.

7.8 Tributary Card Protection Schemes

In OMS 1240 and OMS 1260, tributary card protection provides equipment level protection for the PDH and SDH tributary interface cards fitted in the generic tributary card shelf-slots.

7.8.1 General

7.8.1.1 Generic Tributary Card Protection Equipping Rules

34/45/140/155 Mbit/s PDH/SDH Generic Tributary protection

The following rules apply to 34/45M, 34M transmux, 140M, and dual-port STM-1 tributary card protection. This scheme uses the daisy chain protection interfaces.

- 1:n group protection is available for groups of cards fitted in any tributary slot that has an associated LTU position. In the case of the OMS 1240 this is limited to the two generic tributary positions therefore N can only be one.
- The cards in the 1:n group must be fitted in the numerically adjacent slots with the protection card fitted as shown in Table 7-3, Table 7-4 and Table 7-5.
- 1:1 tributary card protection only uses non-revertive mode.

2 Mbit/s PDH/SDH Generic Tributary protection OMS 1260

The four worker 2M tributary cards can be fitted in any number and combination.

Tributary Card Protection General

For all tributary card protection schemes, when a switch to protection card occurs, all tributary input/output signal related alarm reports are suppressed on the affected worker card.

7.8.1.2 Protection LTUs

The OMS 1240 uses a range of LTUs that provide all the required physical interfaces for a particular generic tributary card function. It is necessary to fit both worker and protection tributary LTUs. The LTU performs traffic routing onto the protection bus connections.

Only a single LTU slot is available for each generic tributary card, for example, a PDH 34M tributary card LTU supports all three traffic I/O ports.

Direct driving of the LTU control lines from the traffic processor of the core card is supported in order to achieve fast protection switching (<50ms).

7.8.1.3 Generic Tributary Card Protection Configuration Rules

For tributary card protection to become available, you must configure the appropriate scheme via the local terminal, or from the EM. The following must be configured before tributary card protection is possible:

- The card(s) to be protected must be selected, and the protection card specified.
- The protection tributary slot must be equipped with a tributary card, which has been logically added.
- The appropriate LTUs must be fitted for the nominated protection card (refer to the LTU rules in Section 7.8.1.2 above).
- Automatic protection switching mode is Enabled/Disabled. Enable/Disable of automatic protection is achieved by use of the lockout of protection command.

7.8.2 Operator Entered Switching Control Commands

The tributary card protection schemes all use operator commands to invoke protection switching. In addition, there is an operator configurable option, which enables automatic switching mode. The following operator entered switch commands apply, however Trigger Restoration only applies when automatic switching is invoked:

Lockout of Protection

Traffic is either switched to, or maintained on the worker card(s). Any subsequent failure does not cause traffic to switch to the protection card. The in-traffic indicator on the protection card is extinguished.

Forced Switch to Protection

Traffic from the specified worker card is either switched to, or maintained on the protection card regardless of whether the latter has failed. A subsequent failure of the protection card, or any of the other workers, does not cause traffic to revert. The in-traffic indicator on the worker is extinguished when a forced switch is in effect.

Clear

This clears the Lockout of Protection and Forced Switch to Protection operator commands. It causes traffic (if switched to protection) to be switched back to the worker.

Trigger Restoration

In automatic mode, this command causes traffic to be switched back to the worker if the failed worker has recovered.

Note: This command does not cause traffic to be switched back to the worker if a Forced Switch command is in effect. The only way of clearing a forced switch is with a Clear command.

Note: The protection state of the currently selected card is displayed to you.

7.8.3 2Mbit/s 1:1 Core Tributary Protection (OMS 1240 only)

On the OMS 1240, the 1:1 core tributary protection scheme is available for the core tributary LTU traffic.

Modes of operation, protection switching criteria, protection switching operation and protection switching times, for core tributary protection are defined by the core card protection scheme.

7.8.4 PDH 34/45M/140M and SDH STM-1 Tributary Card Protection

The term Medium Bit-rate (MB) protection refers to 34/45M, transmux card type protection schemes. The term High Bit-rate (HB) protection refers to 140M and STM-1 card type protection schemes.

7.8.4.1 MB/HB Protection Architecture (OMS 1240 Only)

The scheme supports a variety of protected card types in the two tributary slots with LTU access limits as follows:

- 1:1 34/45M card protection for one card (3 ports)
- 1:1 34M transmux protection for one card (1 ports)
- 1:1 140M card protection for one card (1 ports)
- 1:1 STM-1 card protection for one card (1 port)
- 1:1 dual port STM-1 card protection for 1 card (2 ports).

Note: In each of the above card type configurations the worker card is placed in Tributary Slot S1-01 and the protection card in Tributary Slot S1_02.

7.8.4.2 Modes of Operation (OMS 1240 Only)

Tributary cards may operate with or without 1:1 protection. Tributary cards in slot S1_02 only operate as an unprotected card or as a protection card.

Switching traffic from the protected card to the protection card can be automatic under the Multiplexer Controller control, with switching carried out based on fault conditions reported by the protected tributary card. Manual switching, under operator control, is also possible (refer to Section 7.8.2 above).

7.8.4.3 MB/HB Protection Architecture (OMS 1260 only)

The scheme supports a variety of protected card types in the seven tributary slots with LTU access limits as follows:

- 1:n 34/45M card protection for four cards (12 ports)
- 1:n 34M transmux protection for four cards (4 ports)
- 1:n 140M card protection for four cards (4 ports)
- 1:n dual port STM-1 card protection for four cards (8 ports).

Note: In each of the above card type configurations the worker card is placed in slots following the rules explained in Table 7-3, and Table 7-4

7.8.4.4 Modes of Operation (OMS 1260 Only)

Tributary cards operate separately to the core card protection system, with or without 1:n protection.

Switching traffic from the worker card to the protection card can be automatic under the Multiplexer Controller control, with switching carried out based on fault conditions reported by the protected tributary card. Manual switching, under operator control, is also possible (refer to Section 7.8.2).

2Mbit/s tributary cards operate with protection in slot S1_05 only (1-24 on the LCT), regardless of the quantity of Trib cards installed.

7.9 PDH Port Protection

To improve the availability of the PDH traffic signal, input and output ports may be duplicated. The duplicated traffic signal may be on the same tributary card or on different tributary cards.

In the case of protection for 2M signals, the signal may be embedded in a 34M aggregate signal received by a 34M transmux card.

On the OMS 1240, port protection is available between any two 2M ports on the core tributary cards and be set up for 2M ports on 34M transmux.cards which fit in the generic trib slots.

On the OMS 1260, port protection is available between any two 2M tributary cards.

7.9.1 Modes of Operation

7.9.1.1 Mode of Operation (OMS 1240 Only)

The OMS 1240 is able to operate with the following numbers of protected PDH channels shown in Table 7-16.

Table 7-16: Protected PDH Channels

PDH Rate	OMS 1240
2M	32 ports (Core Trib)
34/45M	3 ports
140M	1 port

Note: The above are maximum figures for single bit rates.

7.9.1.2 Mode of Operation OMS 1260 Only

The OMS 1260 is able to operate with the following numbers of protected PDH channels shown in Table 7-17.

Table 7-17: Protected PDH Channels

PDH Rate	OMS 1260
2M	Up to 126 ports
34/45M	10 ports
140M	3 ports

Note: The above are maximum figures for single bit rates.

7.9.1.3 Wait to Restore and Do Not Revert

Either a Wait-to-Restore (WTR) or Do-not Revert state is entered when a working port recovers from a failure.

In revertive mode of operation, the wait-to-restore state is automatically entered when a worker port recovers from a failure. Entry to the wait-to-restore is inhibited if a higher priority condition exists when the working port recovers.

When the wait-to-restore state is entered, a timer is set. The condition is de-activated upon expiry of the timer period. The condition is also de-activated if a higher priority condition is received during the timer period.

You may configure the timer from 0 to 30 minutes in one-minute (+/- 5 second) steps. You can configure the WTR period globally and on an individual port basis for protected ports. The default value is 10 minutes.

Note: You arel only able to retrieve WTR values from the NE on an individual port basis.

The Do-not Revert state is entered under the same circumstances as WTR. However, there is no associated timer. This state remains active until a higher-level condition is received, at which point the Do-not Revert is reset. If it is active, it is immediately reset by a re-configuration into revertive mode.

7.9.2 Protection Switching Criteria

7.9.2.1 Failure Detection

Two criteria are used to indicate the status of the two protected PDH ports to the protection switching control mechanism. The interface cards generate these flags and the switch unit receives them and uses them to trigger the next stage of the protection switching sequence.

A failure indication is raised if one, or more, of the following criteria is detected:

1 Loss of Tributary input.

2 Loss of Frame Alignment.

3 Receipt of AIS.

4 Excessive Bit Error Ratio (EBER).This is defined as a nominal bit error ratio greater than 10^{-3}. (Enable/Disable) - Enabling/Disabling the alarm report also enables/disables this as a criterion for setting the SF flag.

5 Signal Degrade. You may configure to the following:

- Disabled - signal degrade is never raised
- Raised on BER (bit error ratio greater than a single preset threshold in the range of 10^{-9} to 10^{-5} . (default 10e-6)
- Raised on unacceptable short-term error performance (USE)
- Raised on degraded seconds error performance (DEG).

The default config is signal degrade Enabled, using defect criteria USE.

Failures of types 1, 2, 3 and 4 cause a Signal Fail (SF) flag to be inserted into the internal traffic signal frame overhead, from PDH card to switch unit, for the appropriate PDH trib port.

In the case of a 2M signal contained in an aggregate 34M transmux signal, the Signal Fail flag is also inserted if the following failures are detected on the 34M aggregate signal:

- Loss of tributary signal
- EBER; this is calculated only on 34M Frame Alignment Word errors
- AIS.

A failure of Type 5 causes a Signal Degrade (SD) flag to be inserted into the internal traffic signal frame overhead, from PDH card to switch unit, for the appropriate PDH trib port.

In the case of a 2M signal contained in an aggregate 34M transmux signal, the signal degrade flag is also inserted if signal degrade is detected on the 34M aggregate signal (calculated only on 34M Frame Alignment Word errors).

Enabling/disabling criteria for setting the SD flag, can either be handled within the protection configuration applications, or within the section/path maintenance configuration applications of the SMA (events and traffic connection management).

You are able to configure degraded path performance fault reporting on a per-PDH port basis. The configurations include the following:

- Fault Report Disabled
- Fault Report based on equivalent BER calculations - Path Signal Degrade alarms reported
- Fault Report based on Unacceptable Short-Term Error performance calculations - Path USE alarms reported
- Fault Report based on Degraded Error performance calculations - Path Signal Degrade alarms reported.

The defaults are fault reporting enabled for USE alarm reporting.

The attributes that are configured for fault reporting will be applied to the enable/disable states of the SD signalling flag.

Note: The signal degrade fault type works on BIP bit equivalent binary error ratio calculations (e.g ratio 10e-6). The USE fault type works on the crossing of a threshold of consecutive severely errored seconds. These are calculated for each PDH port by the protected port bearing PDH interface units.

Note: Degraded path performance can be based on USE or Consecutive Degraded Seconds (CDEGS). Separate configurable thresholds are provided for SES (performance monitoring) and DEGS (events handling).

Note: You can configure the signal degrade fault type to work on BIP BERs, or CDEGS.

7.9.2.2 Priority of Failure Conditions

The PDH port selected as the source of selected traffic is as shown in Table 7-18.

Table 7-18: PDH Port - Priority of Failure Conditions

Priority	Switch State	Selected Channel
1	Forced Switch (Protection)	Working
2	Forced Switch (Worker Channel)	Protection
3	Signal Fail (Protection)	Working
4	Signal Fail (Worker Channel)	Protection
5	Signal Degrade (Protection)	Working
6	Signal Degrade (Worker Channel)	Protection
7	Manual Switch (Protection)	Working
8	Manual Switch (Worker Channel)	Protection
9	Wait To Restore	Protection
10	Do Not Revert	Protection

The controller-derived switch interface parity failure generates injection of TU-AIS in response to tributary card-out indications and ports to protection switching criteria.

7.9.3 Protection Switching Control

7.9.3.1 Protection Switching Operation

The interface cards process the traffic from duplicated ports completely independently and pass the traffic from each input port, with its SD/SF flags to the switch unit. This unit determines from which port the traffic quality is higher and selects traffic from that channel based on these flags, but taking into account the conditions shown Table 7-18.

On configuration, the identity of duplicate input ports of protected ports is downloaded from the Multiplexer Controller to the switch unit, so that on receipt of a SF/SD failure condition or a request to switch to either input of a particular port, traffic may be selected from the appropriately numbered port.

At the outgoing traffic ports, the switch unit duplicates the output signals to the output ports corresponding to the duplicated protected input ports. Any decision regarding the quality of the traffic at the output ports must be made by equipment external to the OMS 1240.

7.9.3.2 Operator Commands for PDH Port Protection

Before the PDH port protection mechanism can be controlled, you must configure the different related parameters.

You enter these commands via the local terminal or from the Element Manager.

1 For each port to be protected, you must enter the working port and the protection port. Worker and protection port designation cannot be subsequently changed, only removed.

When port protection is configured, the protection port automatically adopts the configuration (mapping, signal structure etc.) of the associated worker port. Any subsequent change to the configuration of the worker port is automatically adopted by the protection port and vice-versa.

2 Operating mode: Revertive/Non-revertive mode of operation.

3 Wait-to-restore period.

To control the protection switching mechanism, you have access to the following facilities explained in Section 7.4.8 onwards:

- Forced Switch to Worker
- Forced Switch to Protection
- Manual Switch to Worker
- Manual Switch to Protection
- Clear.

The protection state of the currently selected port is displayed.

7.9.4 Protection Switching Time

Under automatic control, switching is completed within 50ms of detection of a fault condition at the tributary port when there are <20 connections in broadcast mode. This switching time increases linearly up to a maximum of 500ms for >20 connections.

For manual operation, switching is completed within eight seconds, this time being measured from your entry of the command at the NMI to the confirmation to you.

During the period in which the selected input traffic is switched-over, errors are generated in the V4 byte.

For compatibility with the switch unit protection mechanism or to prevent a switch unit failure indication (in the case of an unprotected switch unit), the maximum duration of any disruption of traffic from the output of the switch unit due to switching between input ports is less than the persistency figures. This avoids exceeding the persistence check period of the V4 byte diagnostic message check.

7.9.5 PDH Port Protection Architecture

The switch function on the core card monitors for fault conditions in the traffic streams from PDH tributary cards and from the P12 function on the core card. The switch function selects incoming traffic from the port with the highest quality and broadcasts outgoing traffic on both ports.

7.10 MULTIPLEX SECTION SHARED PROTECTION (MS–SPRING)

7.10.1 Introduction

MS-Spring schemes provide SDH trail protection by re-routing the AU-4 payloads of aggregate STM-n signals in the event of a failure detected on a particular span, or spans, of the Ring. The schemes provide protection against failure of the components of SDH physical spans including optical fibres, regenerators and the electrical/optical transducers at the multiplexer section termination points. Whilst MS-Spring schemes are principally defined for ‘external’ Network level protection, the implementation also provides protection against ‘internal’ NE equipment failures on the STM-n Interface Units.

In MS-Springs normal traffic is transported on the Worker AU-4 channels of the multiplexed STM-n Line signal. Reserved Protection AU-4 channels are provisioned to transport the protected traffic in the event of failure of the Working sections.

The OMS 1200-16 provides 2-Fibre MS-Spring. In this case there is only one physical ring and the multiplexed STM-n Line signal carries both Worker and reserved Protection AU-4 channels. Accordingly, half the traffic channel capacity on the Ring is logically assigned to Worker channels, and the other half is assigned to reserved Protection channels. Lower Group channels (e.g: 1-8) carry Normal traffic, and Upper Group channels (e.g: 9-16) are reserved for transporting the traffic during a protection event.

7.11 Protection Switching Control

The MS–SPRING protection switching operation can be autonomous, switching over automatically when deterioration in a nominated Worker path is detected, or manually controlled/forced by operator intervention via EM/LCT. Operator control can override demands from the autonomous mode.

7.11.1 External Controls

External operator controls, addressed to a particular Node in the Ring, include: -

Exercise Ring

This command exercises ring protection switching of the requested channel without completing the actual bridge and switch. This is a test feature which allows the operator to check the viability of the protection scheme (in the idle state). The command is issued and the NE superficial actions shall be reported to Element Manager for operator checking. No Bridge and Switch actions are effected and working traffic is not affected.

Exercise Span

This command exercises span protection of the requested channel without completing the actual bridge and switch. This is a test feature, which allows the operator to check the viability of the protection scheme (in the idle state). The command is issued and the NE superficial actions shall be reported to Element Manager for operator checking. No Bridge and Switch actions are effected and working traffic is not affected.

Note: With Exercise test routines the MSSPRING Managers of the two involved adjacent Nodes simulate a Ring or Span switch. Each Manager shall check the responses from the other and the detecting Node(s) shall report an MSSPRING Protocol Fail alarm if the expected responses are not received.

Lockout Working Channels

This command prevents the working channels over the addressed span from accessing the protection channels. If any working traffic is already on protection, the span switch is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span.

The LOW command has higher priority than any other type of Ring-Switch or Span-Switch request for the addressed I/F port, although it doesn't pre-empt switching actions by the opposite Line I/F port.

Lockout Protection Span

This command prevents the usage of the span for any protection activity and prevents using ring switches anywhere in the ring. If any ring switches exist in the ring, this command causes the switches to drop. If there is a span switch for this particular span, it is dropped. Thus, all ring switching is prevented and span switching is prevented only on the locked-out span.

Forced Switch to Protection Ring

This command performs the ring switch from working channels to the protection channels for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This switch occurs regardless of the state of the protection channels, unless the protection channels are satisfying a higher priority bridge request.

Forced Switch to Protection Span

This command switches the traffic from the working channels to the protection channels of that span. This switch occurs regardless of the state of the protection channels, unless the protection channels are satisfying a higher priority bridge request, or a signal failure (or a K-byte failure) exists on the protection channels of the span.

Manual Switch to Protection Ring

This command performs the ring switch from the working channels to the protection channels for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This occurs if the protection channels are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection channels).

Manual Switch to Protection Span

This command switches the traffic from the working channels to the protection channels for the same span over which the command is initiated. This occurs if the protection channels are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection channels).

Clear

This command clears the externally initiated command and WTR at the node to which the command was addressed. The NE-to-NE signalling following removal of the externally initiated commands is performed using the NR code.

7.11.2 Local Autonomous Controls (SF/SD Flags)

Autonomous mode demands for switching are based on locally detected failures by a Node in the Ring and result in the internal setting of Signal Fail (SF) and Signal Degrade (SD) flags. All the involved SDH Line I/F Cards determine SF and SD criteria from monitoring on the Regenerator and Multiplex Section layers (RS/MS layers) for defects and performance degradation.

Signal Fail (SF) is raised if any of the following are detected:

- RS/dLOS
- RS/dLOF
- MS/dAIS

SD is raised from defects such as:

- MS/dDEG (degraded error performance)

SF and SD flags are internally reported to the MS–SPRING Manager on the core Switch Card using dedicated byte locations in the SOH of the internal pseudo–STM–1 traffic signal. This signaling uses internal STM–1 #1 SOH of the STM–n signal from external Line.

SF flags will also be raised and reported to the MS–SPRING Manager should Internal equipment failures of SDH I/F Cards be detected by core Switch Card.

7.11.3 Wait to Restore

Wait–to–Restore (WTR) is also considered an autonomous switching request control since AUTONOMOUS switching always operates in REVERTIVE restoration mode. WTR command is issued by the MS–SPRING controller after clearance of the prevailing SF/SD request criteria.

The wait to restore period can be configured between 0-30 minutes in 1minute intervals.

7.11.4 Remotely Signalled Controls

MS–SPRING switching always involves two adjacent Nodes; either side of the failed Span of the Ring and switching is always bi–directional. A Source node will either detect local failures for autonomous switching or receive external operator commands, and will signal to the destination node, via bi–directional APS signalling, to effect parallel switching actions.

The EM, or an LCT operator, downloads a Ring Map to the NE. Ring Maps are required to provide NE IDs and the orientation of NEs within the Ring, for K1/K2 APS signalling messages.

7.11.5 Bi–directional APS Protocol

MS–SPRING switching always operates in bi–directional mode between a Source node and a Destination node in the Ring.

Typically, a node in the Ring will determine a protection action and will become a Source switching node. It will Bridge Working traffic onto Protection channels and signal a Bridge Request to the adjacent Destination node. The Destination node receives the request, likewise Bridges its outgoing Worker traffic to Protection in the reverse direction, and Switches the incoming protected traffic, from Source node, back onto Worker channels.

The Destination node signals back to Source node, and Source completes its Switch of Protected traffic back onto Worker channels.

The APS signaling between Source and Destination nodes is transported in the MSOH K1/K2 bytes of the aggregate STM–n Line signals.

7.11.6 Multi Ring Switch

This parameter allows the operator to Enable/Disable Multiple Ring Switch handling in the Ring. This permits the MS-Spring managers to either operate on Ring Bridge requests, when multiple Ring Bridge requests become active on the Ring (refer to Figure 7-12) or to clear down multiple requests to No Request conditions. In this latter case, clearing down will leave unprotected failures in the Ring. The MS-Spring Manager will raise the new protection switch status event - 'No Request'. However it shall also raise a 'Multiple Multiplex Section Fail' supervisory alarm.

The default config is 'Multiple Ring Switch Handling - Disabled'.

The configuration must be applied to all NEs in the Ring, in common.

When Multiple Ring Switches are disabled no traffic misconnections can occur in the MS-Spring.

If the operator 'Enables' Multiple Ring Switches, they must be warned that multiple Ring Switch actions can cause traffic misconnections in the MS-Spring (refer to Figure 7-13), unless they set up Trail Trace processing at the VC- layer (and/or Tandem VC-layer) trail termination points across the Network and enable fault actions AIS injection from defect detections.

Where an MS-Spring Manager actions a Ring Switch request, when another Ring Switch is active on the Ring, it shall raise a 'Potential Network Traffic Misconnections' supervisory alarm. In this way, when VC- / Tandem VC- trail trace mismatch alarms are detected in the Network due to actual misconnections, there is an indication of the potential cause from the MS-Spring switching Nodes.

7.11.7 Path of TCM Trail Trace used for Squelch of Mis–Connected Traffic

With multiple Ring Switch handling by NEs in a Ring network, there is the potential for traffic misconnections. That is, where more than one NE bridges worker traffic onto the Ring protection channels, then the different worker signals could each contend for access to the same protection channels in certain spans of the Ring.

To prevent misconnections the Network relies on VC– (and Tandem VC–) Trail Trace processing at the path termination points. Trail Trace Mismatch (dTIM) invokes signal squelching with AIS injection.

7.11.8 Signal Squelching Rules

The following basic rules apply for squelching signal misconnections caused by multiple Ring Switch request handling in MS–SPRINGs.

- If MS–SPRINGs are set up in a single operator Network, VC–1/2/3/4 layer signal squelching will be applied at the Nodes which handle the VC– trail termination points, from VC– Trail Trace Mismatch detection, for all VC–s which traverse an MS–SPRING.

- If MS–SPRINGs are set up in an operator's Domain in a multi–operator Network, and that Domain predominantly uses Nodes with FULL TCM functionality, VC–1/2/3/4 layer signal squelching will be applied as identified above. For any Tandem VC–s which traverse an MS–SPRING, signal squelching will be applied at the Tandem VC– trail termination points, from Tandem VC– Trail Trace Mismatch detection. This may be handled both by TCM Boundary Nodes, and by Tandem trail termination Nodes.

- If MS–SPRINGs are set up in an operator's Domain in a multi–operator Network, and that Domain doesn't generally use Nodes with FULL TCM functionality, VC–1/2/3/4 layer signal squelching will again be applied as identified above.

However for any Tandem VC–s which traverse an MS–SPRING, signal squelching shall be applied at the intermediate Tandem VC– trail points, where those trails enter/exit the MS–SPRING. This shall be achieved by setting up real (but 'dummy') Tandem Connection Termination functions on the MS–SPRING Nodes and squelching from real Tandem VC– Trail Trace Mismatch detection. In parallel, maintenance functions for the end–to–end Tandem VC– trails will be provisioned by setting up PSEUDO Tandem Connection Termination functions on both the TCM Boundary Nodes, and the Tandem trail termination Nodes, as required.

7.12 Network Level Protection Switching Examples

A basic example of 2-Fibre MS–SPRING network level protection switching, is given in Figure 7-12. This example considers a six–node Ring Topology Map and the cases of two isolated Ring traffic connections 'transport circuits X and Y'.

Transport circuit X enters and exits the Ring (added and dropped) bi–directionally at Nodes A and D. Transport circuit Y enters and exits the Ring at Nodes E and F.

7.12.1 Ring Switch

There is only a single physical section around the Ring. Normal traffic connections are set up on the allocated Worker channels (for example. channels #1–8). Protection channels, which are normally idle (i.e. Protection channels #9–16), provide a shared resource for channel protection switching.

Transmission Failure

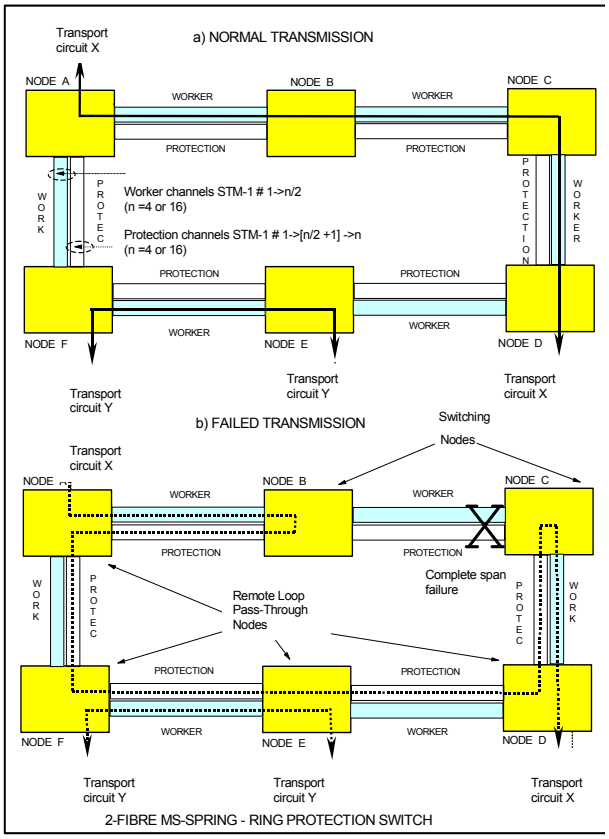
When there is a complete failure of both Worker and Protection sections on the Span between Nodes B and C, then a full Ring switch is required to restore the transport circuit X traffic. Node B senses the failure and Bridges Working channels East-bound onto Protection channels West-bound, away from the failure. Nodes F, E and D provide pass-through connections for the protected traffic to complete a path to Node C. In response to the Bridge at Node B, Node C Switches the protected traffic from East back onto Worker channels East-bound. Node D now receives the working traffic from West, as if no failure had occurred.

In the reverse direction of transmission, with Node C also detecting failure, it would Bridge Working channels West-bound onto Protection channels East-bound, away from the failure and Node B would Switch the protected traffic from West back onto Worker channels West-bound. Node A then, is not aware of failure either.

Note: Transport circuit Y is unaffected by the protection switching. Likewise, circuit connections between, Node B and Node A, or B and F via A, are not affected by the protection switching.

Note: As both Worker and Protection sections are transported on the same physical medium, there are no Span Switch options in 2–Fibre Rings.

Figure 7-12: 2-Fibre MS-SPRING - Ring Protection Switch Concept



7.12.2 Multi-Ring Switch

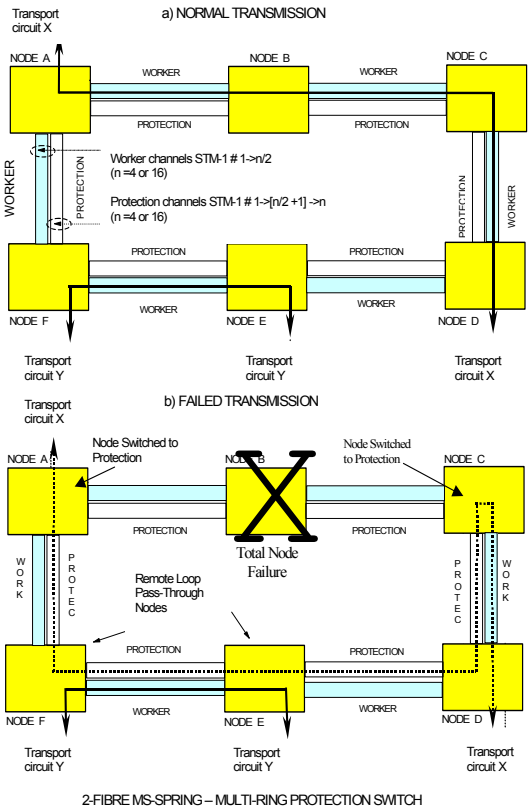
Transmission Failure

When there is a complete failure of a node within the ring, then a Multi-Ring switch is required to restore the transport circuit X traffic. Node A senses the failure and switches the working channels onto protection, away from the failure. Nodes D, E and F provide pass-through connections for the protected traffic to complete the path. Node C switches the anticlockwise protected traffic from the protection channels back onto the worker channels in the clockwise direction. Node D now receives the working traffic from Node C, as if no failure had occurred.

Note: Transport circuit Y is unaffected by the protection switching.

Note: As both Worker and Protection sections are transported on the same physical medium, there are no Span Switch options in 2–Fibre Rings.

Figure 7-13: 2-Fibre MS-SPRING - MultiRing Protection Switch Concept



7.12.3 Multi-Ring Switch – Misconnected Traffic

Transmission Failure

When there is a complete failure of a node within the ring, then a Multi-Ring switch is required to restore the transport circuit X traffic. This illustration demonstrates how it is possible to get misconnected traffic.

Figure 7-14: 2-Fibre MS-SPRING – Misconnected Traffic Concept