OSIRIS® Network
User's Guide

206-002-07

POSITRON
Networks

Seventh Edition: October 2005

A publication of:
Positron Networks Inc.
5101 Buchan
Montreal, Quebec
Canada, H4P 2R9
service@positronnetworks.com

Printed in Canada

Trademarks

This *Network User's Guide* was written for OSIRIS-VUE 14.01, DS1 PM+ 1.1.15, 1.1.16, EC1 TSA 1.1.12, and PacketPath 1.2.9. NE Software supported appears below. Use these versions when performing the procedures appearing in this guide.

NE Software Supported

	MCU	NMCU	NMCU 32 MB
SONET	N/A	21.14.xx/23.14.xx/25.14.xx	21.14.xx/23.14.xx/25.14.xx
			31.14xx/33.14xx/35.14xx
SONET—OSI	N/A	N/A	31.14.xx/33.14.xx/35.14.xx
SDH	4.09.xx/4.99.xx	6.09.xx/6.99.xx	6.09.xx/6.99.xx

Table of Contents

Introduction

Positron OSIRIS® optical multiplexers are designed for the rapidly expanding broadband access market and provide third generation SONET/SDH Add/Drop multiplexer capabilities in modular, flexible, and upgradable packages.

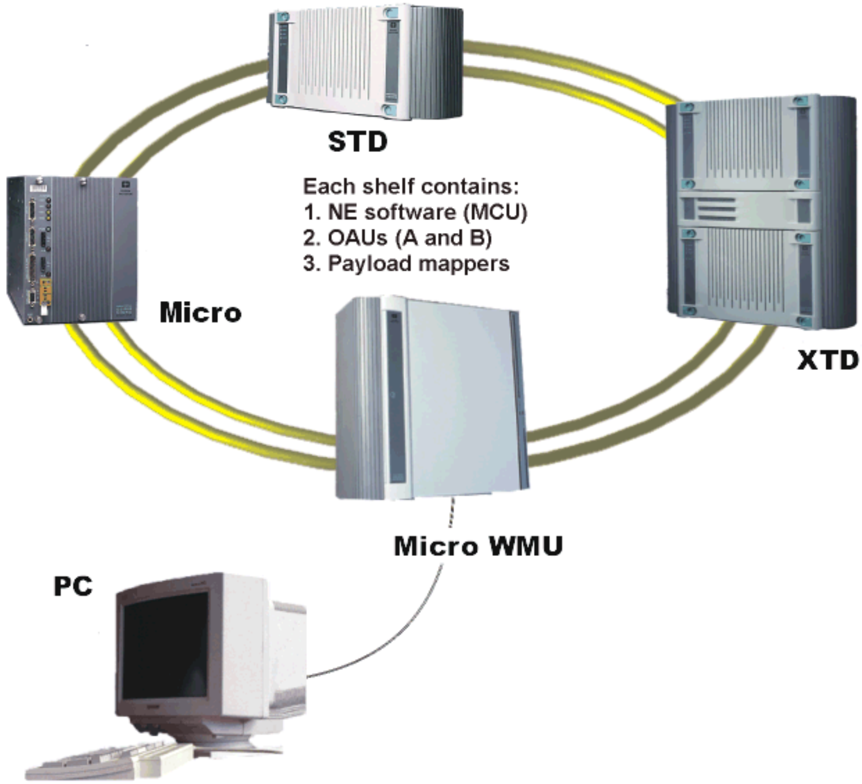
This network user's guide contains an overview of OSIRIS networking components, networking applications, general network element and Ring Start-up procedures, and NE software management.

System Overview

An OSIRIS network consists of:

- Network Elements (OSIRIS STD shelf, OSIRIS XTD shelf, OSIRIS XTS shelf, OSIRIS Micro shelf, and OSIRIS Micro WMU).
- NE software—operating system software that runs on each shelf and controls provisioning and management procedures.
- OSIRIS-VUE™/OSIRIS-VUE PLUS™ network element management software—runs on a PC and communicates with NE software to allow configuration and provisioning.

The NE software operates on the MCU or NMCU of each OSIRIS shelf. This software interprets management and provisioning instructions received from the PC operating OSIRIS-VUE software or issuing TL1 commands. OSIRIS-VUE software provides a graphical user interface (GUI). Instructions from the OSIRIS-VUE software are received by the NE software which then provisions shelves accordingly. Shelves are provisioned in various configurations, and multiplex/demultiplex traffic according to settings received from OSIRIS-VUE software or TL1 commands.



NE System Software

NE software communicates between the local node and the OSIRIS-VUE software. All OSIRIS optical multiplexers operate using NE software which runs on the Monitor and Control Unit (MCU) or Network MCU (NMCU). The NMCU has a powerful microprocessor, supports larger memory capacities, and provides a 10BaseT Ethernet interface. NE software controls monitoring and alarm reporting, systems logs, test and diagnostics, protection switching and security services.

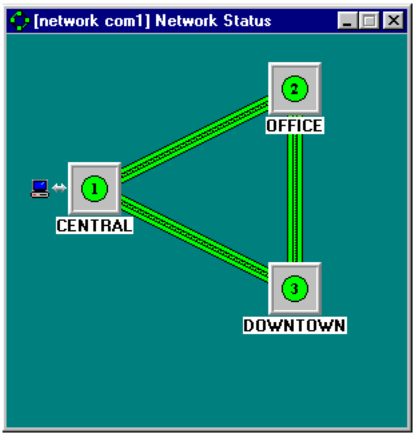
The OSIRIS-VUE software can access all network shelves, from a connection to a single shelf. Provisioning information is passed through this shelf as TL1 commands and sent to the rest of the network via the Data Communication Channel (DCC).

By broadcasting autonomous TL1 messages, the network automatically informs OSIRIS-VUE software about the following activities via the NE software:

- Security-related activities
- Alarm status changes
- Provisioning information

OSIRIS-VUE Software

The OSIRIS-VUE network management and provisioning system gives you a flexible, easy-to-use working environment in which to provision, test, and maintain fiber-optic networks and network elements.



An OSIRIS network configuration can be saved using an OSIRIS-VUE software file to back up and restore all the provisioning data.

For more information, refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001).*

OSIRIS Shelves

All OSIRIS SONET shelves have the same basic functionality, however, each has a different terminating capacity.

Two independent power feeds supply redundant power to the OSIRIS shelf. Due to this power architecture, a failure to one power input does not compromise power to any part of the OSIRIS shelf.

OSIRIS STD Shelf

- **SONET**—The OSIRIS STD shelf has a maximum terminating capacity of 28 DS1s, 3 DS3s/EC-1s, one OC-3c, or a mix of DS1, DS3, EC-1, Ethernet, Fast Ethernet, Multi-Service Ethernet and PacketPath mappers, up to a maximum of OC-3 bandwidth.
- **SDH**—The OSIRIS STD shelf has a maximum capacity of 28 E1/DS1s or 3 E3/DS3s, one STM-1, or a mix of DS1, E1, E3, Ethernet, Fast Ethernet, V.35, and PacketPath mappers.

OSIRIS Micro shelf and OSIRIS Micro WMU

- **SONET—**The OSIRIS Micro shelf DS1/E1 shelf has a terminating capacity of up to 8 (protected) or up to 16 (unprotected) DS1s. The DS1/E1 OSIRIS Micro shelf can also accommodate Ethernet, Fast Ethernet, OC-3c or a mix of these signals. The OSIRIS Micro shelf DS3/E3 has a terminating capacity of one DS3 or one EC-1 (protected or unprotected). The OSIRIS Micro shelf DS3/E3 can also accommodate Ethernet, Fast Ethernet, Multi-Service Ethernet, OC-3c, or a mix of these signals.
- **SDH**—The OSIRIS Micro shelf DS1/E1 shelf has a terminating capacity of 4 DS1 or E1 protected or up to 8 DS1 or E1 unprotected. The OSIRIS Micro shelf DS3/E3 has a termination capacity of one DS3 or one E3 (protected or unprotected). The OSIRIS Micro shelf DS3/E3 can also accommodate Ethernet, Fast Ethernet, V.35, STM-1 or a mix of these signals.

The OSIRIS Micro WMU (DS1/E1 or DS3/E3) is an OSIRIS Micro shelf equipped with an AC/DC rectifier, battery backup, integrated alarm management, patch panel, and stand-alone cabinet enclosure.

Note: The 16 DS1 unprotected configuration is not possible on the OSIRIS Micro WMU DS1/E1.

OSIRIS XTD shelf

- **SONET**—The OSIRIS XTD shelf, when using OC-3 OAUs, can support up to 84 DS1s, or three DS3s/EC-1s or a combination of DS1, DS3, EC-1, Ethernet, Fast Ethernet, PacketPath, and OC-3c mappers.

  The OSIRIS XTD shelf, when using OC-12 or OC-48 OAUs, has access to 12 STS-1s. The shelf can support up to 12 DS4s/EC-1s or a combination of DS1, DS3, EC-1, Ethernet, Fast Ethernet, Multi-Service Ethernet, PacketPath and OC-3c mappers.

- **SDH**—the OSIRIS XTD shelf, when using STM-1 OAUs, can support up to 84 E1s, or three DS3s/E3s or a combination or DS1, E1, E3, DS3, Ethernet, Fast Ethernet, PacketPath, V.35 and STM-1 mappers.

  The OSIRIS XTD shelf, when using STM-1 OAUs, can support up to 12 DS3s/E3s or a combination or DS1, E1, E3, DS3, Ethernet, Fast Ethernet, PacketPath, V.35 and STM-1 mappers.

OSIRIS XTS shelf

- **SONET**—The OSIRIS XTS shelf, when using OC-3 OAUs, can support up to three DS3s/E3s or a combination of DS1, DS3, EC-1, Ethernet, Fast Ethernet, Multi-Service Ethernet, PacketPath, and OC-3c mappers.

  The OSIRIS XTS shelf, when using OC-12 or OC-48 OAUs, has access to 12 STS-1s. The shelf can support a combination of DS1, DS3, EC-1, Ethernet, Fast Ethernet, PacketPath, and OC-3c mappers.

- **SDH**—The OSIRIS XTS shelf, when using STM-1 OAUs, can support up to three DS3s/E3s or a combination of DS1, E1, E3, DS3, Ethernet, Fast Ethernet, PacketPath, V.35, and STM-1 mappers.

  The OSIRIS XTS shelf, when using STM-4 OAUs, can support a combination of DS1, E1, E3, DS3, Ethernet, Fast Ethernet, PacketPach, V.35, and STM-1 mappers.

  Note: All shelves are upgradeable from OC-3/STM1 to OC-12/STM4 to OC-48.

Common Shelf Components

This section describes equipment appearing in all OSIRIS optical multiplexers.

Optical Access Units (OAU)

OAUs collect traffic from the backplane (received from the mappers), and add the SONET/SDH framing and overhead to build the standard OC-3/STM-1, OC-12/STM-4, OC-48 signals. The OAU performs all necessary synchronization, pointer processing, overhead processing, and multiplexing functions. Signals enter the optical fiber and are transmitted to other network nodes.

OAUs also demultiplex incoming signals, dropping traffic to the backplane of a shelf.

Two OAUs are installed in each OSIRIS shelf to provide path redundancy (OAU-A and OAU-B).

Redundant optical paths enable OSIRIS networks to offer path protection switching (PPS). PPS uses two optical fibers, a working and a protection fiber. Optical signals are transmitted on both fibers simultaneously. Should a failure occur on one fiber, the receiving node automatically switches to the other fiber.

The Set up configurations, including time-slot assignments, are stored in non-volatile memory, and in multiple locations in a shelf, including the OAUs. This prevents unit removal and power failures from affecting basic service and traffic. The amount of time required to recover from a system failure is also greatly reduced.

Each OAU has its own timing circuitry. The following timing sources are available:

- External clock—derived from an external DS1/E1, EC-1, or OC3c/STM-1 channel.
- Internal clock—derived from an internal oscillator.
- Line Clock—The clock derived from the received optical signal.

MCU and Network MCU

The Monitor and Control Unit (MCU) resides in all OSIRIS optical multiplexers. The MCU initializes all cards in the OSIRIS system and houses the NE software. The Network Monitor and Control Unit (NMCU) has the same functionality as an MCU but has a powerful microprocessor, supports larger memory capacities, and provides a 10BaseT Ethernet interface. An Ethernet connection lets you provision a shelf via a LAN connection.

All management, provisioning and gathering of alarm information is performed via the NMCU. All communication between shelves is performed via the DCC.

Performance Monitoring (PM) statistics are received by the NMCU on each shelf. PM lets you monitor transmission quality of network traffic. PM provides automatic error statistics for items such as the section and line layers of the SONET/SDH signal, as well as others. PM lets providers detect maintenance problems before they affect service.

Mappers

Mappers are installed in each OSIRIS shelf. Mappers accept the tributary signal and generate SONET/SDH framed payload data which is synchronized and output to two backplane ADD busses, one for the working fiber ring and one for a protection, or backup, fiber ring. Each mapper plug-in unit can add or extract, data from any of the SONET/SDH frame time slots that you define using OSIRIS-VUE software or TL1 commands.

OSIRIS optical multiplexers offer equipment protection switching (EPS) for DS1/E1, DS3/E3, and EC-1 mappers. In the event of a mapper failure, traffic switches to a backup mapper card.

DS1

The DS1 card is a four channel mapper (seven channels for the OSIRIS Micro shelf) and connects a DS1 signal to a SONET network.

DS1-SDH

The DS1-SDH card is a four channel mapper and carries DS1 traffic over an OSIRIS SDH network.

DS1PM+

The DS1PM+ mapper supplies the electrical interface to the OSIRIS line of Add/Drop Multiplexers, allowing the synchronous transport of asynchronous signals. The DS1PM+ mapper supports the following frame formats which transport signals into the Payload Capacity of a VT1.5 SPE:

- Unframed (Clear-channel)
- SuperFrame (SF)
- Extended SuperFrame (ESF)

The DS1PM+ mapper is available in the following configurations:

- 4-channel (800334)
- 8-channel (800337)

E1

The E1 is a four channel mapper and connects an E1 signal to an SDH network.

DS3

The DS3 card connects one DS3 signal to a SONET network.

DS3-SDH

The DS3-SDH card connects a DS3 signal to an SDH network.

E3

The E3 card connects an E3 signal to an SDH network.

OC-3c

The OC-3c mapper lets you carry OC-3c ATM traffic over a SONET backbone. the OC-3c mapper may operate in both OC-3 and OC-12 systems and operates concurrently with any other mapper type.

STM-1

The STM-1 mapper extracts the VC4 signal from the incoming STM-1 tributary signal and places it on the ADD bus of an OSIRIS shelf. In the other direction, the STM-1 mapper takes the VC4 signal from the DROP bus to form the outgoing STM-1 tributary signal.

The STM-1 signal can be used to transport high bandwidth capacity traffic such as video, ATM (Asynchronous Transfer Mode), or synchronous STM-1 payload.

OC-3 TRIB

Positron OSIRIS OC-3 Tributary cards are used to interconnect OSIRIS access rings to external equipment while supporting STS1 and VT1.5 level path protection as well as unidirectional linear APS (1+1) for OC-3 tributary lines.

The OC-3 Tributary card also supports the following standard OSIRIS features:

- Timing reference: The OC-3 card can act as the primary or secondary external timing reference.
- Performance monitoring (PM): Near-end line and SEF-S parameter are monitored on OC-3 line.
- Alarm provisioning: The OC-3 Tributary card supports full OSIRIS-VUE alarm provisioning. The OSIRIS-VUE software lets you customize alarm definitions. For intance, you can redefine levels of alarms or restore removed alarms.

STM-1 TU12

The STM-1 TU12 card can be used in the following sample applications:

- Ring Interconnection at the TU12/TU3 level: This application connects two OSIRIS access rings across a higher order backbone while maintaining TU12 and TU3 granularity for each access ring.
- STM-1 TU12 tributary cards also used to interconnect OSIRIS rings to external equipment while supporting TU3 and TU12 level path protection as well as unidirectional linear APS (1+1) or STM-1 tributary lines.

  The STM-1 TU12 card also supports the following standard OSIRIS features:

  - Timing reference: The STM-1 TU12 card can act as the primary or secondary external timing reference.
  - Performance monitoring (PM): Near-end line and SEF-S parameter are monitored on STM-1 line.
  - Alarm provisioning: The STM-1 TU12 card supports full OSIRIS-VUE alarm provisioning. The OSIRIS-VUE lets you customize alarm definintions.

EC-1

The EC-1 mapper lets you interconnect OSIRIS UPSRs at an EC-1 synchronous level to SONET STS-1 digital cross-connects and/or other SONET NEs. This mapper provides an EC-1 electrical interface which has the bandwidth of a SONET STS-1 payload.

There are three EC-1 mappers: a bulk mapper, a VT mapper and a TSA mapper.

- EC-1 BULK—does not terminate the STS-1 Path Overhead but transparently passes the complete STS-1 path. This mapper lets you configure point-to-point connections between networks. This EC-1 mapper allows the OSIRIS system to map an incoming EC-1 signal onto the OC-3/OC-12 payload at the STS-1 level.
- EC-1-VT—is deployed in a head-end application. This application consists of an OC-3/OC-12 UPSR that homes all VT signals to one location called the head end. This mapper allows up to 28 VTs as part of the EC-1 structure prior to hand-off to a digital cross-connect or other SONET NEs.
- EC-1-TSA—allows synchronous connections between OSIRIS and/or other vendors equipment. The EC-1 TSA Mapper allows up to twenty-eight (28) VT 1.5 Path Level Protection Switching from any three STS1. The EC-1 TSA Mapper is deployed in all remote sites that require a certain number of VT 1.5 and assigns them onto a single EC-1. The EC-1 TSA has the flexibility to terminate any VT 1.5 within the total bandwidth (OC-3/OC-12) from any three STS1s.

Ethernet

The Ethernet mapper provides point to point Ethernet service connection over a SONET or SDH backbone. The Ethernet interface operates at a line rate of 10 Mbps.

Fast Ethernet

The Fast Ethernet Mapper provides a connection between two Ethernet LANs via a SONET or SDH backbone. The Fast Ethernet interface operates at a line rate of 100 Mbps.

Multi-Service Ethernet

The Multi-Service Ethernet (MSE) Mapper provides a connection between two Ethernet LANs via a SONET backbone. The Multi-Service Ethernet has a 4-Port interface which operate at a line rate of 10/100 Mbps each.

V.35

The V.35 mapper provides access to two V.35 channels. There are two V.35 PCS Honda 20-pin cable connectors on the front of the V.35 mapper, one connector for each channel.

PSCU

The Protection Switch Control Unit (PSCU) is required when DS1 services are terminated at the local shelf and DS1 equipment switching is required. This card provides switching between a failed DS1 working mapper and a Protection Mapper Unit. One PSCU provides protection for 28 DS1 channels.

AUX2 Card

The Auxiliary card (AUX2) relays alarm conditions from a terminal block to the OSIRIS shelf to which it is connected, and then to OSIRIS-VUE. The AUX2 can handle eleven alarm inputs and four alarm outputs or directly to the AUX2.

The AUX2 generates an alarm as a response to an incoming user-programmed alarm from a terminal block. The OSIRIS PWR shelf can route its alarms to a terminal block, and then to the AUX2 or directly to the AUX2.

PacketPath Mappers

Positron's OSIRIS with PacketPath is a powerful bandwidth-on-demand solution that dynamically assigns unused bandwidth to current data traffic. Optimized for the broadband access market, the PacketPath product line consists of two mapper cards that provide data over SONET and SDH optical networks. The PacketPath cards are known as follows:

- PacketPath Fractional Ethernet Access Card (PEC4)
- PacketPath ATM Concentrator Card (PAC155)

These two (2) mappers provide routed IP and bridged multi-protocol support in SONET and SDH optical rings. PEC4 (800344) cards are placed at the customer-premise inside a SONET or SDH optical ring to offer, both routed and bridged, packet connectivity to a head-end switch or router. PAC155 (800349) cards are also part of the optical ring, but instead act as a gateway to the head-end switch or router.

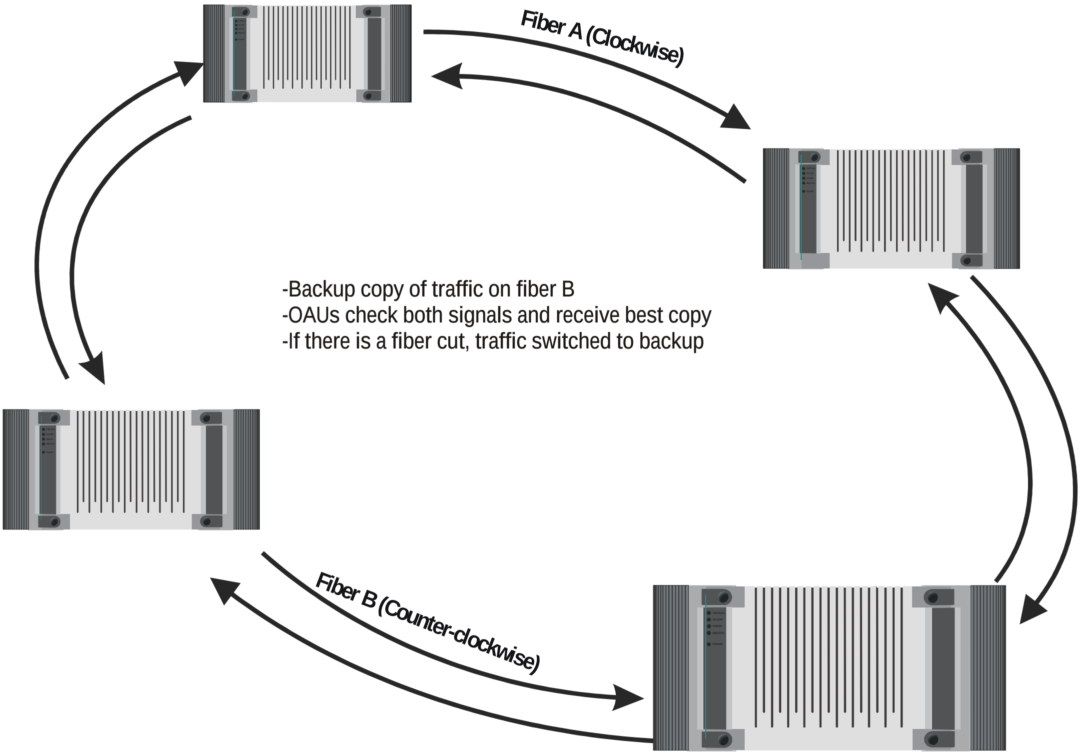
PacketPath mappers let you share Positron OSIRIS STS-1/TUG3 or STS3c/VC4 bandwidth between separate customers. Each of these interfaces is assigned a different Virtual Circuit (VC). VCs are independent of each other and completely secure. As an example, five VCs may represent five separate customers, each with a separate service level agreement (SLA).

UPSR Network Overview

The OSIRIS system is designed as a UPSR (Unidirectional Path Switched Ring) network. This ring topology protects network traffic using a path switching scheme.

When the network is set up, information transferred between the two end points in a circuit is duplicated. One copy of all information (voice/data/image) travels on the primary path (usually fiber A) in the clockwise direction, and another copy travels counter-clockwise on the secondary fiber (usually fiber B).

Mapper cards in the OSIRIS shelf continuously read both copies of the signal received and chooses the highest quality signal.



In a normal UPSR ring application, the bandwidth used for a specific Point to Point cross-connection cannot be reused elsewhere for another cross-connection. The alternate path around the ring is used for protection against fiber cuts.

If fiber path protection is not required, or if protection is assured by other means than the UPSR ring, you may choose to reuse the same bandwidth on different segments around the ring. Refer to "Bandwidth Reuse Application" on page 46.

Network Installation and Start-up Checklist

The logical order of setting up an OSIRIS network consists of the following:

1. Determine what network application or topology you want to implement. Refer to “Network Applications” on page 21.
2. Determine what signal type you need to carry into the OSIRIS shelf.
3. Install the hardware. Refer to the appropriate installation document in “Related Documents” on page 77.
4. Install the NE software. Refer to “Managing NE Upgrades” on page 1.
5. Perform Ring Start-up procedures. Refer to “Ring Start-up” on page 49.
6. Provision network traffic using OSIRIS-VUE software. Refer to *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User’s Guide (206-001).*

Contacting Customer Service

Should a problem arise, please contact us:

Toll Free: 1-866-331-3003 (North America only)
International Line: +1-514-345-2202
Fax: +1-514-345-2304
E-mail: service@positronnetworks.com

Returned Material Department

If equipment needs to be repaired or exchanged, please contact us. A representative will give you a Return Material Authorization (**RMA**) number. You must have an **RMA** number before you ship equipment to Positron for repair.

RMA Toll Free: 1-866-331-3003 (North America only)
RMA International Line: +1-514-345-2202
Fax: +1-514-345-2304
E-mail: service@positronnetworks.com

Pack all equipment in antistatic material with sufficient protection against shipping damage and ship the equipment back to Positron. It is highly recommended that you insure your package.

Make sure that the RMA number is clearly marked on the packaging.

For USA customers, send equipment to:

Positron Inc.
c/o Freeport Forwarding
1320 Route 9
Champlain, NY
12919

For non-USA customers, send equipment to:

Positron Technologies Inc., Networks Division
18107 Trans-Canada Highway
Kirkland, Quebec
Canada H9J 3K1

Order Entry Department

If you wish to place an order for new equipment or to inquire about the status of an already placed order, please call the Order Entry department at 1-866-331-3003 or +1-514 345-2296.

Chapter 1

Network Applications

This chapter describes the specific management and traffic applications available for telecom networks using OSIRIS optical multiplexers.

The following applications are available:

- Point-to-Point
- Broadcast
- Logical Ring
- Matched Nodes
- Path Protected Interconnected Ring
- Subtended Rings
- Dual Homing
- Bandwidth Reuse

This chapter also describes how to perform network management via a LAN connection.

For information on configuring these network applications or provisioning mappers using OSIRIS-VUE™ software, see the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)*.

Point-to-Point Application

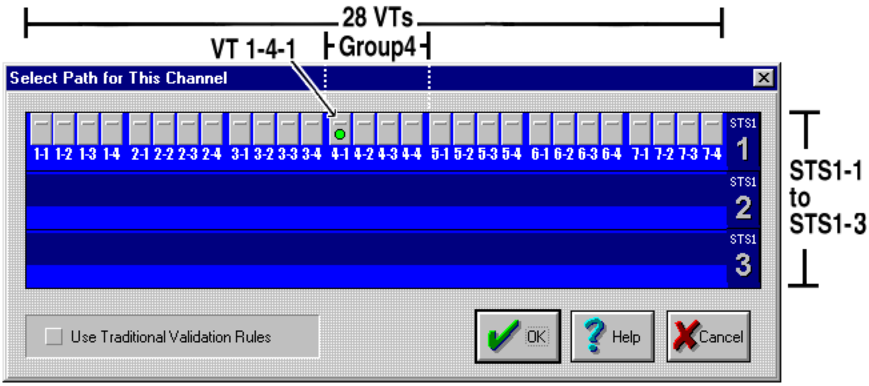
The Point-to-Point application is the most basic form of cross-connection type. This represents an Add/Drop cross-connection which lets traffic enter and drop from a specific timeslot.

Add/Drop cross-connections consist of the following:

Add Component	Drop Component
Add A **and** Add B	Drop A **or** Drop B

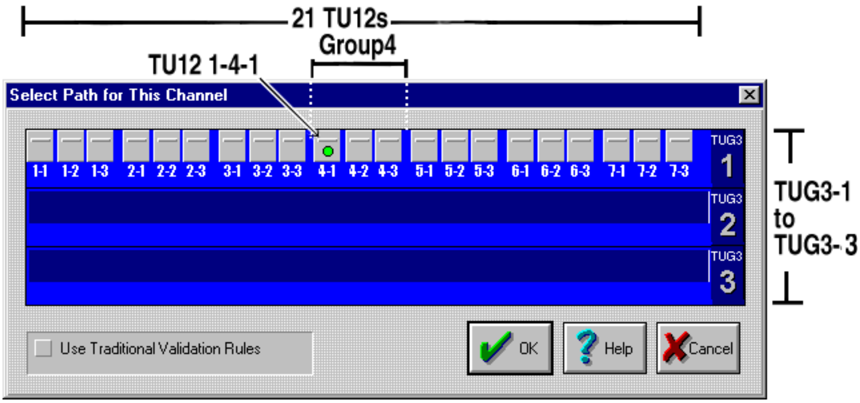
In the SONET standard, OC bandwidth is divided into STS-1s. For example, an OC-12 system defines its bandwidth as 12 STS-1s. Each STS-1 can contain an equivalent capacity of a DS3 signal. Each STS-1 can be divided into 28 Virtual Tributaries (VT1.5s) (7 groups of 4 VT1.5s). Each VT1.5 has an equivalent capacity to a DS1 signal.

Examples in this chapter use the 1-4-1 bandwidth timeslot. This refers to the first VT of the fourth group on the first STS-1. The following displays this timeslot reserved in OSIRIS-VUE software.



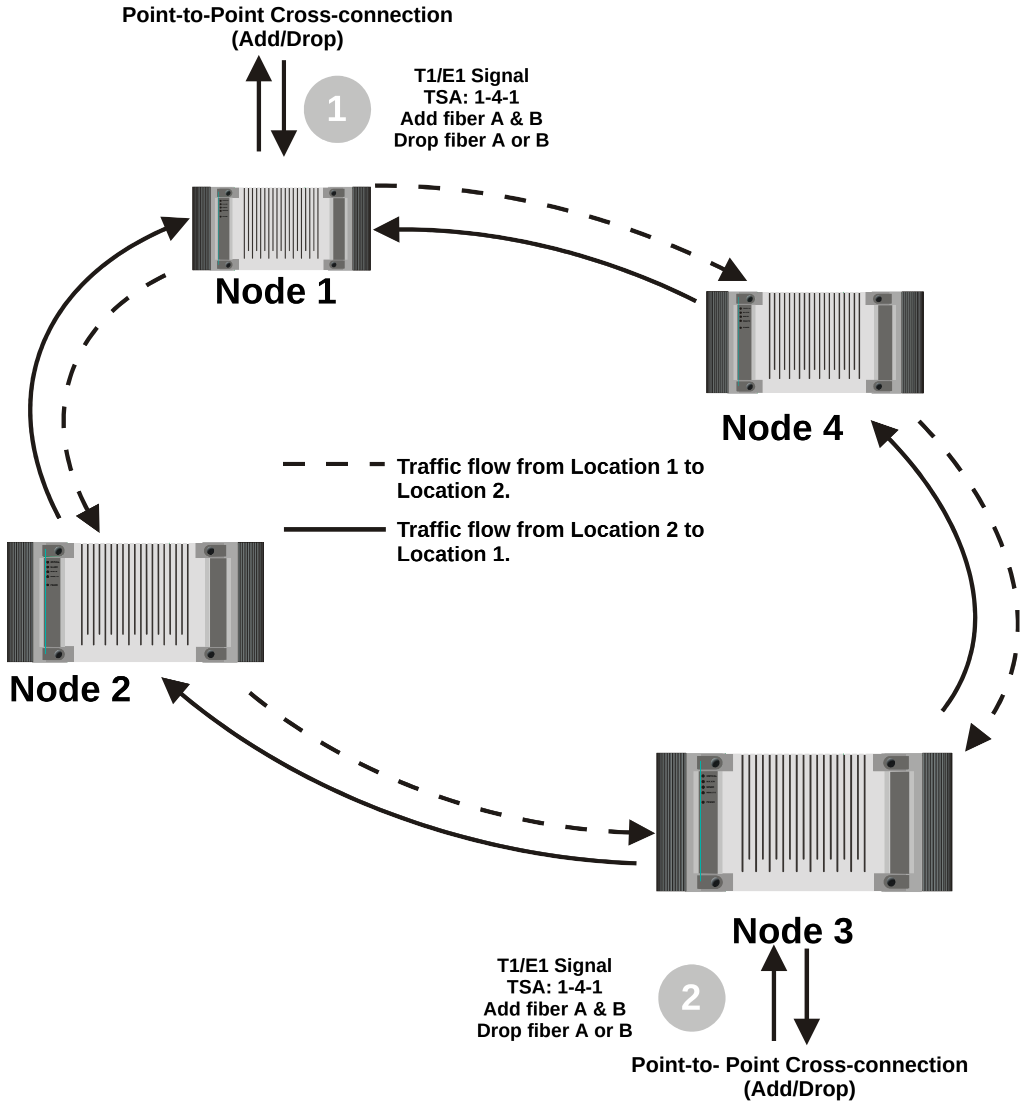
In the SDH standard, network bandwidth is divided into STM-1. For example, a STM-4 system defines its bandwidth as STM-1s. An STM-1 can be divided into 3 TUG3s. A TUG3 can carry an equivalent capacity of an E3 signal. Each TUG3 can be divided into 21 subsections (TU12s) (7 groups of 3 TU12s). Each TU12 has an equivalent capacity to an E1 signal.

Examples in this chapter use the 1-4-1 bandwidth timeslot. This refers to the first TU12 of the fourth group on the first TUG3. The following displays this timeslot reserved in OSIRIS-VUE software.



Topology

The following diagram depicts a **Point-to-Point** network topology.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 2. In particular:

1. A Point-to-Point cross-connection is provisioned at Location 1 in timeslot 1-4-1 of the bandwidth. Traffic is added onto the same portion of bandwidth on **both** fiber A and fiber B. Traffic travels clockwise on fiber A and counter-clockwise on fiber B.

   Point-to-Point cross-connections carry bi-directional network traffic. An example of bi-directional traffic is a telephone connection, in which a user can both speak and listen at the same time.

   Therefore, the Point-to-Point cross-connection provisioned at Location 1 also receives traffic travelling from Location 2. This traffic is dropped from the OSIRIS network to an external device.

   A circuit path carrying bi-directional traffic has been created in the 1-4-1 timeslot of the bandwidth between Location 1 and Location 2.

2. A Point-to-Point cross-connection is provisioned at Location 2 in timeslot 1-4-1 of the network bandwidth. Point-to-Point cross-connections add to the same portion of bandwidth on **both** fiber A and fiber B.

   Traffic being received from Location 1 through this virtual path drops from the OSIRIS network through timeslot 1-4-1 to an external device.

   Note: In order to create a bi-directional path, you must provision **two** cross-connections.

Broadcast Application

Broadcast traffic enters a network from a single location, but exits at many locations.

Broadcast can be either a single ring application or a multiple-ring application, employing a Matched Nodes or Logical Ring configuration. For more information on multiple-ring applications, refer to "Logical Ring Application" on page 28 or "Matched Nodes Application" on page 34.

Application

The Broadcast application may be defined as follows.

Option	Cross-connection
Source with feedback	Add/Drop
Source, no feedback	Add
Drop Site	Drop

Source With Feedback

Network traffic enters and exits the traffic stream at the location provisioned as **Source with feedback**. This cross-connection is the only place where network traffic enters an OSIRIS network for this portion of bandwidth.

Only one point can be provisioned as the broadcast source. All other cross-connections provisioned on the same timeslot must be specified as Drop.

This cross-connection type also receives the signal which it transmits. This can be used to verify the quality of the signal sent.

Source With No Feedback

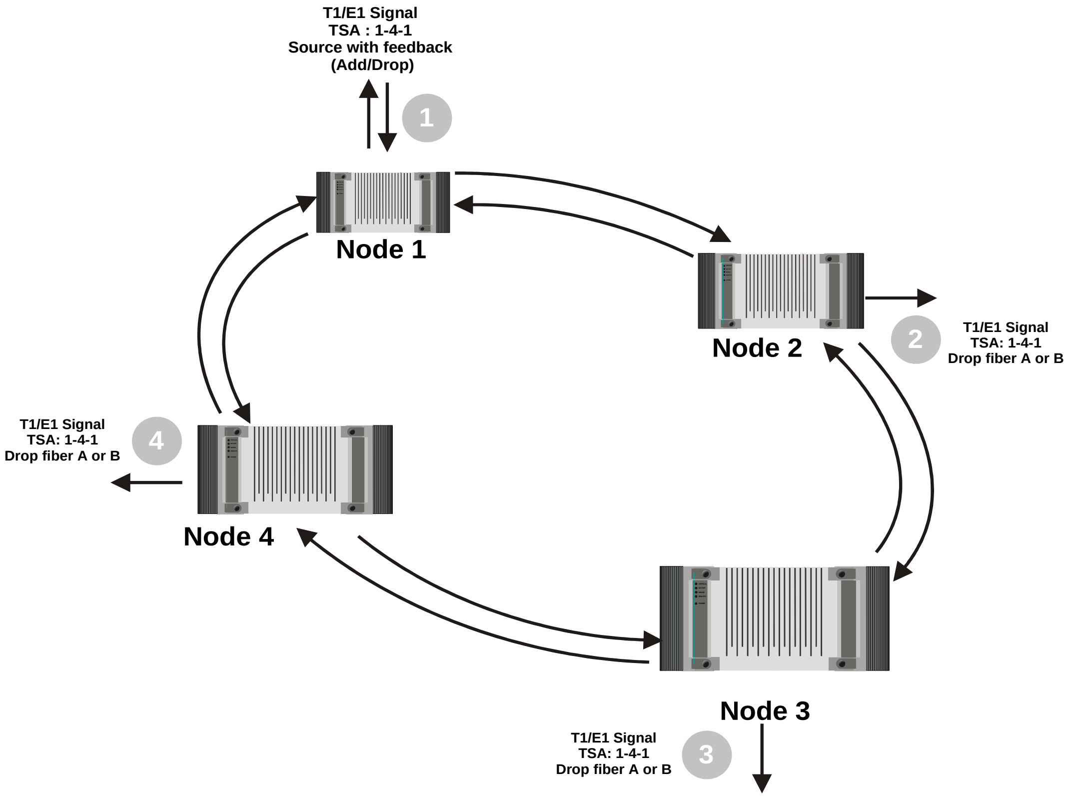
Source with no feedback represents the unidirectional entry point of a signal into the network.

Drop Site

Because the Broadcast application sends network traffic from one-to-many locations, many cross-connections may be provisioned as **Drop Site** for the same portion of bandwidth. Locations provisioned as Drop Site provide the receiving location for uni-directional traffic.

Topology

The following diagram depicts the Broadcast application network topology.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Locations 2, 3, and 4. In particular:

1. In the illustration, a T1/E1 Add/Drop cross-connection is provisioned at Node 1 in timeslot 1-4-1 of the bandwidth. This cross-connection is set to Source with feedback, indicating that the signal is both added to and dropped from this timeslot. Feedback lets you verify whether the signal has been sent properly. Broadcast traffic is added to both fiber A and fiber B. It drops from the fiber that provides the best quality signal.
2. At locations 2, 3, and 4, traffic drops from timeslot 1-4-1 of the bandwidth off the fiber that provides the best quality signal. Cross-connections are provisioned as Drop Site on each Node at the 1-4-1 timeslot, indicating that broadcast traffic is received at each location.

Logical Ring Application

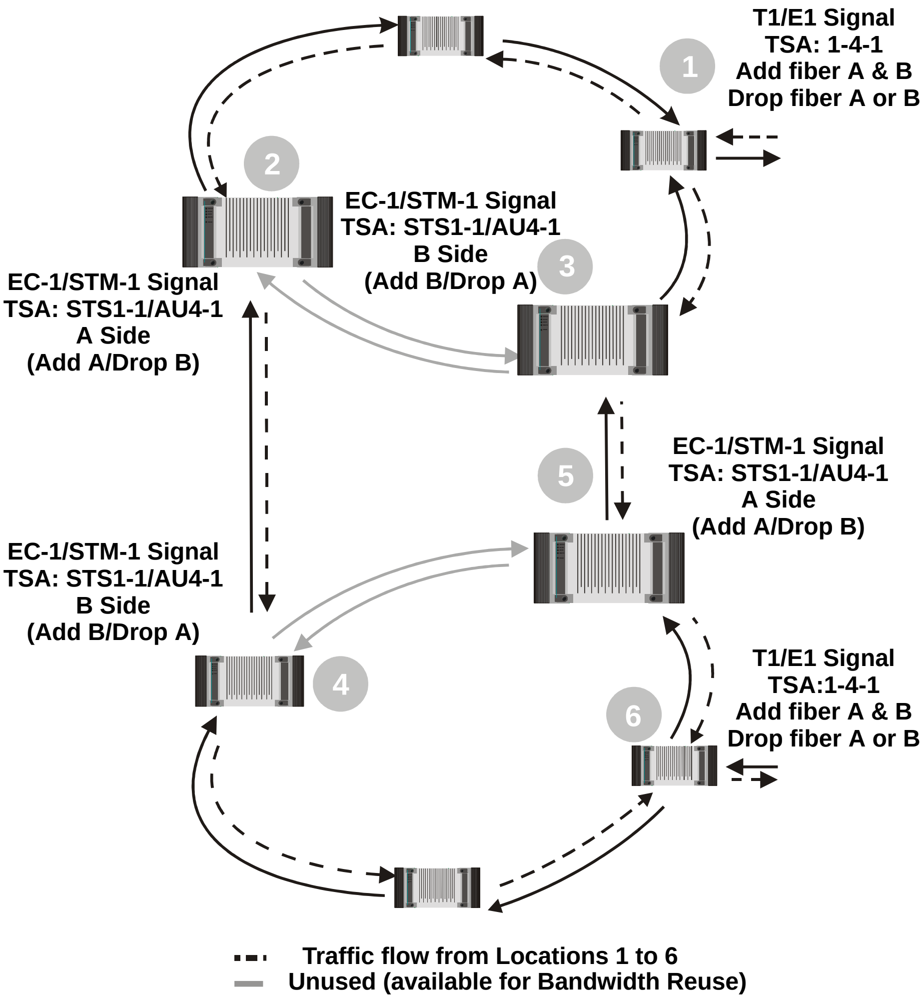
The Logical Ring application is designed for ring interconnection scenarios.

During normal operation, an OSIRIS network operates as a Unidirectional Path Switching Ring (UPSR). Traffic travelling on each virtual path has a backup copy. If a path fails, traffic switches to the backup copy.

The Logical Ring configuration creates a virtual UPSR from two interconnected rings. This lets traffic provisioned on each virtual path flow from one ring to another as if it were travelling on only one ring.

Topology

The following diagram depicts the Logical Ring Application.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 6. It may be described in detail in the following way.

1. In this example, the Logical Ring application aims to provision a virtual path between Location 1 and Location 6 using a Point-to-Point cross-connection. Logical Ring is the ring interconnection method used to make this cross-connection a simple Point-to-Point between rings.

At Location 1, traffic enters the first ring through a Point-to-Point cross-connection provisioned on timeslot 1-4-1 of the bandwidth. Traffic is added to both fiber A and fiber B and travels toward Locations 2 and 3. Traffic flows clockwise on fiber A and counter-clockwise on fiber B.

For more information on provisioning a Point-to-Point cross-connection, refer to the "Point-to-Point Application" section earlier in this chapter.

Note: This explanation tracks traffic in one direction only. However, at the same time that network traffic leaves Location 1, traffic is also received from Location 6 through this same Point-to-Point cross-connection. The Point-to-Point cross-connections between Location 1 and 6 carry bi-directional network traffic.

2. Locations 2, 3, 4, and 5 are the serving nodes which establish EC-1/STM-1 links between rings. The cross-connections on these nodes are provisioned as **Logical Ring** in the Cross-connect tab.

   Cross-connections at these locations must be provisioned as follows.

Location 2	Location 3	Location 4	Location 5
A Side (Add A/Drop B)	B Side (Add B/Drop A)	B Side (Add B/Drop A)	A Side (Add A/Drop B)

These cross-connections result in a pair of interconnected rings which acts as a logical UPSR.

At Location 2, traffic exits the first OSIRIS ring through an EC-1/STM-1 channel provisioned as A Side (Add A/Drop B), indicating that traffic exits the ring from fiber B. The signal travels across this bi-directional link between rings towards Location 4.

Note: The Logical Ring application provisions cross-connections as drop-only, not drop-and-continue. In this example, traffic exits the first ring at Location 2. Traffic *drops* at this location; it does not continue along fiber B to Location 3. This means that traffic may not survive a fiber cut in each ring. A similar application can survive a fiber cut in each ring; refer to "Matched Nodes Application" on page 34.

At Location 4, traffic enters the second network through an EC-1/STM-1 channel provisioned as B Side (Add B/Drop A).

Location 3 is provisioned as B Side (Add B/Drop A).

Location 5 is provisioned as A Side (Add A/Drop B).

Note: This example of a Logical Ring Application depicts two pairs of serving nodes which provide a connection between rings. One pair of serving nodes may also be used. Bandwidth may be reused between the serving nodes with the Logical Ring application. Since traffic drops from the ring through these locations and does not continue, other traffic may be inserted into this portion of the bandwidth for Point-to-Point communication between serving nodes on the same ring.

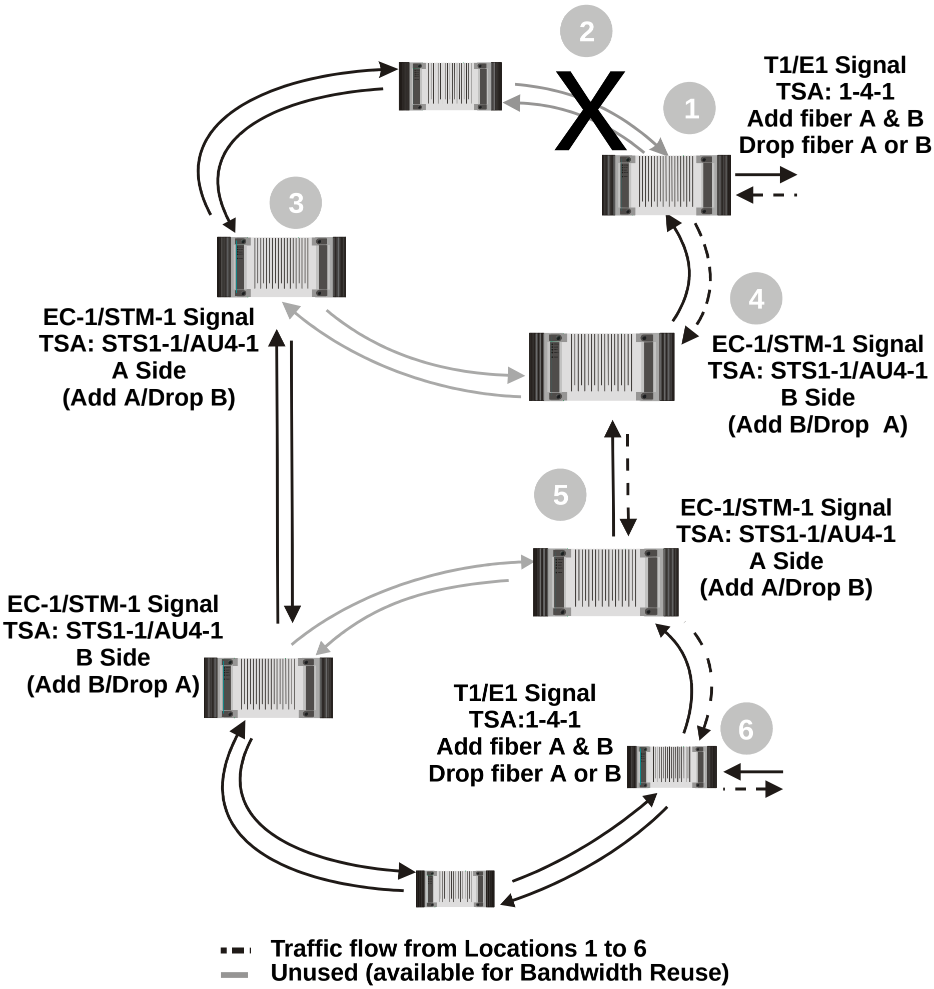
3. Traffic must be provisioned from Location 1 to Location 6 through a Point-to-Point cross-connection. A Logical Ring is the configuration used to enable the interconnection of rings. For more information on provisioning a Point-to-Point cross-connection, refer to the “Point-to-Point Application” on page 22.

Path Switching (Single Fiber Cut)

Paths are protected with the Logical Ring Application. A Point-to-Point (Add/Drop) cross-connection provisioned between locations on two interconnected rings **will** withstand a fiber cut in either ring.

Note: The Logical Ring application does not always withstand two fiber cuts (i.e., one in each ring). This level of protection is a feature available with the Matched Nodes application.

The following graphic shows a fiber cut.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 6 with **one** fiber cut occurring on the interconnected network. In particular:

1. A Point-to-Point (Add/Drop) cross-connection is provisioned between Locations 1 and 6. The network traffic flows clockwise on fiber A and counter-clockwise on fiber B leaving from Location 1.
2. A fiber cut occurs at Location 2, and network traffic is not received from Location 1 at Location 3 on fiber B. Traffic reaches the second ring from fiber A only.
3. The serving node at Location 3 no longer receives network traffic on fiber A due to the fiber cut. This serving node cannot pass traffic on to the second network.

   Note: Traffic does not flow between Location 3 and Location 4 in either direction in the Logical Ring application. The EC-1/STM-1 cross-connections are provisioned to **drop** traffic only. Traffic exits the ring at this location and is sent to the second ring. Another cross-connection type known as drop-and-continue would drop the signal through the EC-1/STM-1 cross-connection and forward it on to the next node on the same ring. The Drop only characteristic allows the Logical Ring to survive only one fibercut, **not** two.

4. Because a fiber cut occurred at Location 2, network traffic is received by the serving node at Location 4 on fiber A only. Traffic is passed on to the second ring through an EC-1/STM-1 channel.
5. Traffic then enters the second ring through Location 5, which is transmitted from Location 4. Traffic is injected onto the traffic stream on fiber A at Location 5, and is transmitted in a clockwise direction toward Location 6.
6. Traffic carried on the Point-to-Point cross-connection from Location 1 arrives at Location 6 on fiber A.

Matched Nodes Application

The OSIRIS Matched Nodes application adds reliability to the Logical Ring application by adding a second level of redundancy for ring interconnection. The Matched Nodes application is similar to the Logical Ring Application, except that it provides a more robust protection level which can withstand one fiber cut in each interconnected ring. Logical Ring can withstand only one fiber cut in either ring.

Typical applications for the OSIRIS Matched Nodes configuration include the following:

- Hospital Communication Links
- Military Networks
- 911 lines
- Emergency Services
- Police Communications
- Power Utility Networks
- Other Mission Critical Applications

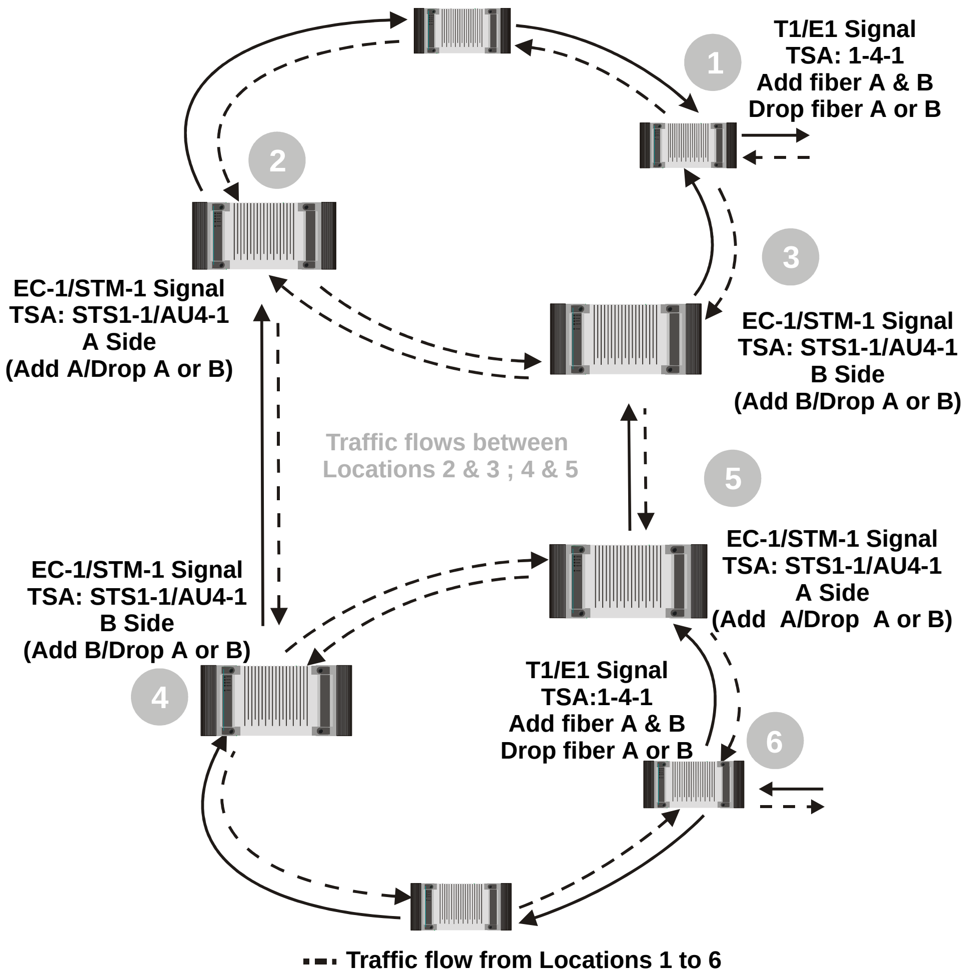
Topology

The Matched Nodes Configuration consists of two rings interconnected by two redundant EC-1/STM-1 bridges. Both EC-1/STM-1 bridges carry the same traffic.

The EC-1/STM-1 bridges are terminated on four Network Elements known as the Matched Nodes.

Once the EC-1/STM-1 bridges have been properly established, it is possible to span services from one ring to another. These services can include DS1/E1, DS3/E3, and Ethernet end-to-end connectivity.

The following graphic depicts a Matched Nodes application.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 6 with no fiber cuts occurring on the interconnected network. In particular:

1. Traffic originates from the first interconnected ring at Location 1. Provisioned as Add/Drop, network traffic is injected onto both fiber A and fiber B at the 1-4-1 timeslot. This application carries bi-directional traffic between rings using a Point-to-Point cross-connection.

2. Traffic arrives at Location 2 and 3 from Location 1 on fiber A and B. Locations 2, 3, 4, and 5 are the serving nodes which establish EC-1/STM-1 links between rings. The cross-connections on these nodes are provisioned as **Matched Nodes** in the Cross-connect tab.

   Cross-connections at these locations must be provisioned as follows.

Location 2	Location 3	Location 4	Location 5
A Side (Add A/Drop)	B Side (Add B/Drop)	B Side (Add B/Drop)	A Side (Add A/Drop)

   Note: The difference between Logical Ring and Matched Nodes is that cross-connections at the matched nodes are provisioned as drop-and-continue, **not** as drop only. In this example, network traffic is sent between Locations 2 and 4, however, traffic also continues along the fiber from Location 2 to Location 3. This is the crucial point which allows Matched Nodes to withstand one fiber cut in each ring.

   You cannot reuse bandwidth between Locations 2 and 3 due to this drop-and-continue feature.

   At Location 4, traffic enters the second network through an EC-1/STM-1 channel provisioned as B Side (Add B/Drop).

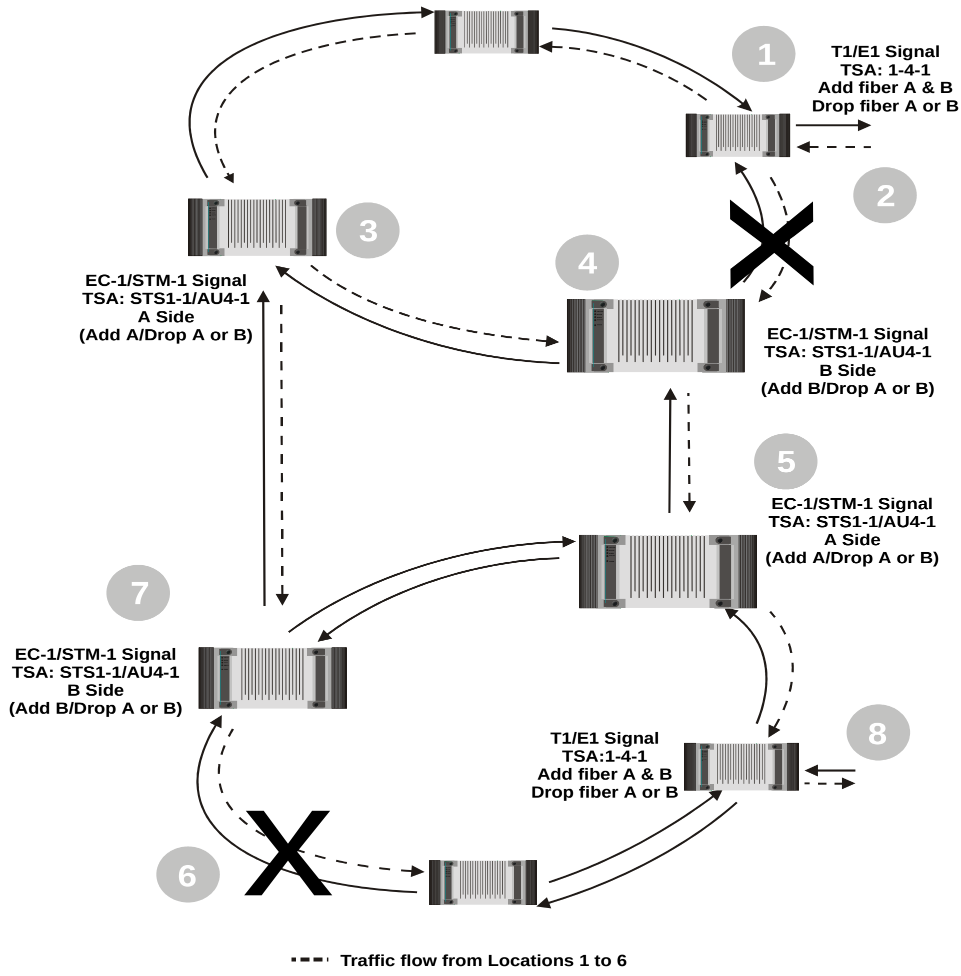
3. Locations 4 and 5 receive the EC-1/STM-1 signal from the first ring and injects it into the fiber of the second ring.

4. Location 6 is also provisioned as an Add/Drop cross-connection. The aim of the Matched Nodes application is to allow traffic to travel between interconnected rings. In the previous example, traffic flows between Location 1 and Location 6 in timeslot 1-4-1 of the bandwidth through a Point-to-Point cross-connection.

Path Switching (Two Fiber Cuts)

The strength of the Matched Nodes application is that it can withstand **two** fiber cuts, one in each ring, whereas Logical Ring can withstand only one fiber cut in either of the interconnected rings.

The following graphic shows a Matched Nodes application with two fiber cuts.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 8 with **two** fiber cuts occurring on the interconnected network. In particular:

1. A Point-to-Point (Add/Drop) cross-connection is provisioned between Locations 1 and 8. The network traffic flows clockwise on fiber A and counter-clockwise on fiber B from Location 1.
2. A fiber cut occurs at Location 2.
3. No traffic is received from Location 1 at Location 4 on fiber A due to the fiber cut which has occurred at Location 2. However traffic is received from Location 1 at Location 3 on fiber B. At this location, traffic is forwarded to Location 4 as well as passing to the second ring.
4. Because Matched Nodes cross-connections are provisioned as drop-and-continue, traffic travels between Location 3 and Location 4. In this example, traffic continues from Location 3 to Location 4 on fiber B.

   Because of a second fiber cut at location 6 (described later), the signal cannot be routed to the intended destination through the EC-1/STM-1 bridge at Location 3. This is true, because traffic is added to fiber B on the second ring. When traffic enters the second ring it travels along fiber B toward the fiber cut at Location 6. Traffic cannot reach Location 8 via this path.

   Because the Matched Nodes application lets traffic pass between Location 3 and Location 4, traffic enters the second ring at Location 5 from Location 4.
5. Traffic from the first ring enters the second ring at this location. The signal is injected onto fiber A and travels in a clockwise path toward its destination at Location 8.
6. A second fiber cut has occurred at Location 6.
7. Traffic is received at Location 7 from Location 3. Traffic is added to fiber B of the second ring and travels counter-clockwise towards Location 8. However, traffic drops because of the fibercut at Location 6.
8. Traffic from the first ring is received from the first ring on fiber A only.

   The Matched Nodes application has protected a Point-to-Point cross-connection from two fiber cuts.

Path Protected Interconnected Ring

Before you provision a Matched Nodes cross-connection, consider the following:

- Mapper card types
- Card provisioning
- Timeslot Assignment
- Equipment Protection

Mapper Card Types

This application channels network signals and sends them into an STS-1/OC3c/VC4 (STM-1) bridge, which is connected to another ring. The bridge connection is redundant. Two EC-1/OC3c/STM-1 bridges are required.

The EC1-TSA - SONET

The EC-1 TSA (800507) Mapper provides the electrical SONET interface to OSIRIS networks, allowing synchronous connections between OSIRIS and/or other vendors equipment.

The EC-1 TSA Mapper allows path level protection switching for up to 28 VT 1.5 signals, from any three STS-1s. The EC-1 TSA Mapper is deployed in all remote sites that require a certain number of VT 1.5s, and assigns them onto a single EC-1.

The EC-1 TSA mapper requires one of the following OAU: 800310/3, 800311/3, 800318/2 or higher.

The EC1-VT Mapper - SONET

This EC1-VT mapper interconnects OSIRIS UPSRs at an EC-1 synchronous level (or STS-1).

The EC1-VT (800502) is deployed in a head-end application. This application consists of an OC-3 UPSR that homes all channel signals to one location called the head-end. This mapper allows up to 28 VTs path level switching as part of the EC-1 structure prior to hand-off to a digital cross-connect or other NEs.

Four working EC1-VT mapper cards must be installed for the Matched Nodes Application (one in each of the Matched Nodes).

The EC1-BULK Mapper - SONET

The EC1-BULK mapper card (800501) cannot be used for the DS1 Matched Nodes application if the DS1 are gathered from multiple sites. If the application consists of incoming DS1 located at a single site or if the application consists of a DS3 Point-to-Point, then the EC1-BULK mapper can be used.

Four working EC1-BULK mapper cards must be installed for the Matched Nodes Application (one in each of the Matched Nodes).

OC3c Tributary Card - SONET

The OC3c mapper card (800504, 800505) can be used to transport high bandwidth capacity traffic such as video, and ATM (Asynchronous Transfer Mode) or any synchronous OC3c payload. This mapper can only be used for bulk OC3c applications.

Four working OC3c mappers must be installed for this application to work.

STM-1 Tributary Card - SDH

The STM-1 mapper extracts the VC4 signal from the incoming STM-1 tributary signal and places it on the ADD bus of an OSIRIS optical multiplexer. In the other direction, the STM-1 mapper takes the VC4 signal from the DROP bus to form the outgoing STM-1 tributary signal.

The STM-1 signal can be used to transport high bandwidth capacity traffic such as video, and ATM (Asynchronous Transfer Mode) or synchronous STM-1 payload, as well as E1, E3, Ethernet, and Fast Ethernet traffic. This mapper can only be used for bulk STM-1 applications.

Four working STM-1 mappers must be installed for this application to work.

STM-1 TU12 - SDH

The STM-1 TU12 mapper card (800410, 800420, 800430) is deployed in a head-end application. This application consists of an STM-1 or STM-4 ring that homes TU12 signals to one location called the head-end. This mapper allows up to 63 TU12s path level switching as part of the STM-1 structure prior to hand-off to a digital cross-connect or other NEs.

SS Bits

SS bits represent two bits in the H1 byte, which allow a user to transport a SONET OC3c signal over an SDH ring, or an SDH STM-1 signal over a SONET ring. SS Bit provisioning is supported on the MCU (800302) and the Network MCU (800307).

For more information, see the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001).*

Card Provisioning

It is recommended that EC-1/OC3c/STM-1 cards on both rings be cross-connected to the same STS-1/STS3c/VC4 (STM-1) number for easier management.

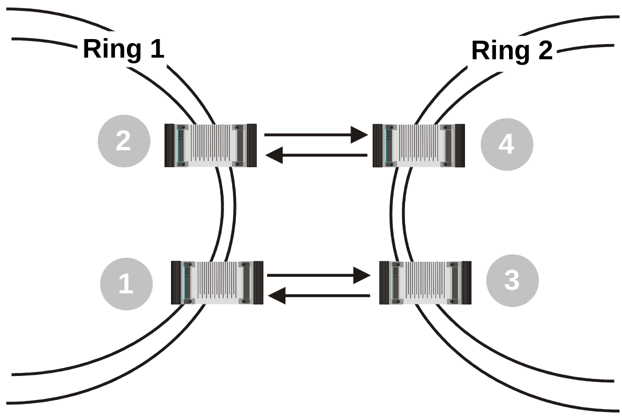
The cross-connection provisioned as Add must be configured to transmit traffic only on one fiber; either the A or B.

The cross-connection provisioned as Drop must remain in normal Path Switching mode to allow proper fault recovery. The Drop selector will still be able to toggle between fiber A and B.

For matched node EC-1/OC3c/STM-1 configuration, refer to the following table.

Matched Node 1	Matched Node 2	Matched Node 3	Matched Node 4
A Side	B Side	B Side	A Side

Matched Nodes appear in the following locations.



Time Slot Assignment

Once the framework for this application has been set up, the last step is to establish end-to-end circuits (e.g., DS1/E1) across two matched nodes.

The section explains how to establish a DS1/E1 circuit. On each of the interconnected rings, a specific time slot must be reserved for this traffic.

The channel group and number must be identical in both interconnected rings. The following table displays possible timeslot assignments.

Circuit Identifier	Timeslot on Ring 1	Timeslot on Ring 2
Circuit 1	2-**7**-**4**	2-**7**-**4**
Circuit 2	1-**2**-**1**	3-**2**-**1**
Circuit 3	3-**1**-**2**	3-**1**-**2**
Circuit 4	2-**5**-**3**	11-**5**-**3**

Equipment Protection

To maximize the robustness of this application, we recommend you use OSIRIS equipment protection wherever possible. This ensures mapper failure protection and EC-1 mapper failure protection.

Note: EC1-VT and EC1-TSA mappers (Product Numbers: 800502, and 800507 respectively) can be protected only by cards of the same type. The EC1-VT and EC1-TSA mapper cards cannot be protected by the EC1-BULK card (800501).

Dual Homing Application

Dual Homing provides extended path protection for traffic entering an OSIRIS network through two T1/E1 lines. The T1/E1 lines connect a customer site to two separate OSIRIS optical multiplexers to provide path redundancy. If one T1/E1 connection fails, a separate T1/E1 connection is available as backup. Dual Homing is a bi-directional application.

The Dual Homing application provides path protection beyond the limits of a OSIRIS network. The paths travelling on T1/E1 lines are also protected.

Dual Homing applications may be provisioned for DS1/E1 traffic only, and representing Add A/Drop B, Add B/Drop A, and Add/Drop cross-connections.

The Homing Site is where DS1/E1 traffic exits the OSIRIS network through a T1/E1 line destined for another location.

Application

Dual Homing cross-connections may be provisioned with one of the following three options:

- Side A
- Side B
- Homing Site

Side A

A cross-connection provisioned as **Side A** adds the traffic received from the T1 line to fiber A. The same portion of bandwidth is also provisioned as Drop B.

Side B

A cross-connection provisioned as **Side B**, adds the traffic received from the T1 line to fiber B. The same portion of bandwidth is also provisioned as Drop A.

Homing Site

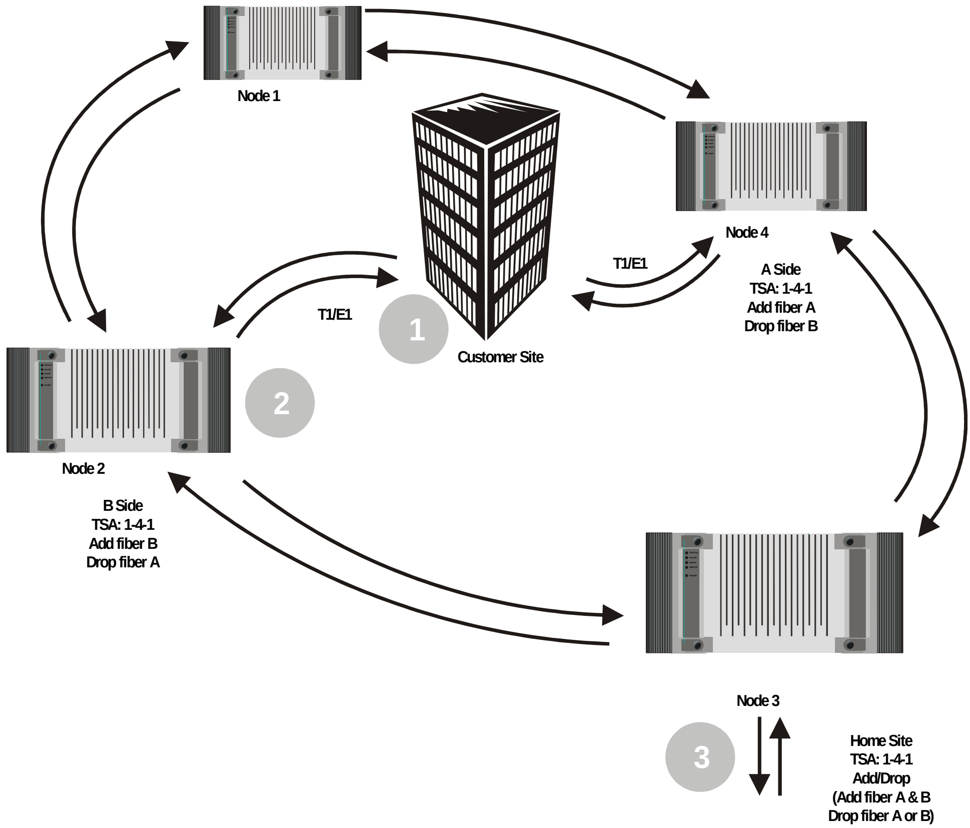
A cross-connection provisioned as **Homing Site** transfers traffic from this portion of the bandwidth to a T1 line. This cross-connection type performs switching. A Homing Site cross-connection is provisioned as Add A and B, Drop A or B.

Time Slot Assignment

All three “ends” within a Dual Homing application must be provisioned in the same timeslot. For example, all three cross-connections can use the timeslot 1-4-1.

Topology

The following diagram depicts a Dual Homing network topology.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 3. In particular:

1. Traffic leaves a customer site at location 1. Note that Dual Homing is a bi-directional application. Bi-directional traffic flows to both Node 2 and Node 4.
2. Traffic enters an OSIRIS network through Node 2. The DS1/E1 cross-connection on this network element is provisioned as B Side (Add B/Drop A).

Assume that traffic enters the OSIRIS network through a B Side cross-connection provisioned in timeslot **1-4-1**. The traffic is injected on to fiber B's 1-4-1 timeslot. The traffic travelling in the opposite direction (back to the customer site) exits the OSIRIS network through the same timeslot, but from fiber A. The traffic exits through fiber A's 1-4-1 timeslot.

Traffic flows along fiber B toward Location 3, which is also known as the **Homing Site**.

Traffic also enters an OSIRIS network through Node 4. The DS1/E1 cross-connection on this network element is provisioned as A Side (Add A/Drop B).

3. The Homing Site is the cross-connection through which traffic exits an OSIRIS network. Homing Site cross-connections are Add/Drop cross-connection.

Fiber or Cable Cut Scenario

The Dual Homing application supports protection beyond the limits of an OSIRIS network. In the previous example, paths were protected at any point on the fiber-optic cable between network elements. If a fiber cut occurs, a backup copy of traffic is available from the alternate path because two T1 lines lead to the customer location, protection is extended beyond the boundaries of an OSIRIS network. In the previous example, if a T1 line cut had occurred between Locations 1 and 2, traffic would still have reached the OSIRIS network on the redundant T1 line.

Bandwidth Reuse Application

In a normal UPSR ring application, the bandwidth used for a specific Point-to-Point cross-connection cannot be reused elsewhere for another cross-connection. An alternate path around the ring is reserved for protection against fiber cuts.

If fiber path protection is not required, or if protection is assured by other means than the UPSR ring, you can reuse the same bandwidth on different segments around the ring.

Bandwidth Reuse mode can be used on the whole bandwidth of the ring or on specific bandwidth sections. Normal protected UPSR traffic and Bandwidth Reuse traffic can co-exist on the same ring, each using different time slots.

Application

Bandwidth reuse cross-connections may be provisioned as Side A or Side B.

Side A

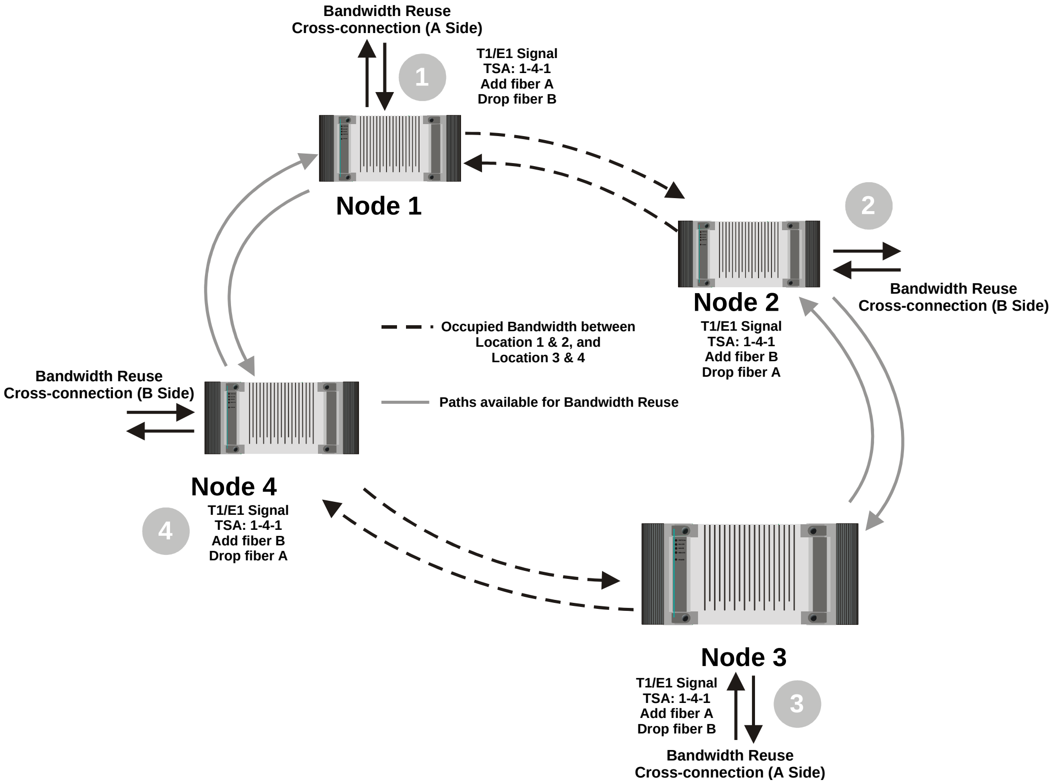
This option provisions an Add A/Drop B cross-connection. Traffic is added to fiber A, and the second portion of bi-directional traffic drops through this timeslot from fiber B.

Side B

This option provisions an Add B/Drop A cross-connection. Traffic is added to fiber B, and the second portion of bi-directional traffic drops through this timeslot from fiber A.

Topology

The following diagram depicts a Bandwidth Reuse network topology.



Traffic Flow

This figure illustrates the flow of traffic between Location 1 and Location 2. In particular:

1. A Bandwidth Reuse cross-connection is provisioned as **A Side** (Add A/Drop B) at Location 1 in the 1-4-1 location of the bandwidth. Traffic is added to fiber A and travels clockwise toward Location 2.
2. A Bandwidth Reuse cross-connection is provisioned as **B Side** (Add B/Drop A) at Location 2 in the 1-4-1 portion of the bandwidth. Traffic travelling from Location 1 drops from fiber A. Traffic is added at Location 2 on timeslot 1-4-1 of fiber B. Traffic travels counter-clockwise on fiber B towards Location 1.
3. Bandwidth may be reused on timeslot 1-4-1 around the ring. For example, the identical timeslot used between Locations 1 and 2 is reused between Locations 3 and 4.

Timeslot 1-4-1 is provisioned as **A Side** (Add A/Drop B) at Location 3. Traffic is added to fiber A and travels clockwise toward Location 4.

4. A Bandwidth Reuse cross-connection is provisioned as **B Side** (Add B/Drop A) at Location 4 in the 1-4-1 portion of the bandwidth. Traffic travelling from Location 3 drops from fiber A. Traffic is added at Location 4 on timeslot 1-4-1 of fiber B. Traffic travels counter-clockwise on fiber B toward Location 3.

   Note: Once a specific timeslot is provisioned for bandwidth reuse, all other cross-connections provisioned in the same timeslot anywhere on the ring must also be provisioned for bandwidth reuse.

Chapter 2
Ring Start-up

Once you have installed your OSIRIS optical multiplexers, you must connect optical fiber to each shelf to form a working network.

Ring start-up provisioning includes the following procedures:

- Looping back OAUs
- Identifying nodes
- Connecting fiber to the nodes
- Provisioning Network clock information

Looping Back OAUs

An OAU loop procedure prevents alarms from occurring during network setup. Alarms are a crucial part of troubleshooting OSIRIS networks, however, during start-up, no network traffic is being carried on the optical fiber. Once ring start-up is complete, all alarms disappear.

Note: This procedure is performed for every shelf in the OSIRIS network.

Follow these steps to loopback OAUs.

1. Unseat the Optical Access Unit (OAU) located in the slot labelled OAU-A.

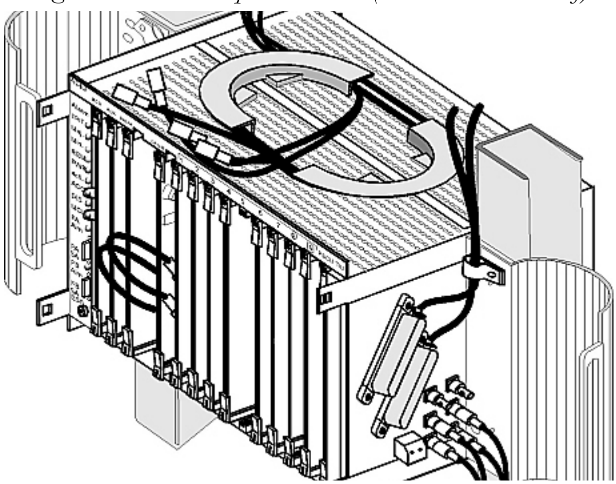
CAUTION

Do not remove fiber cables from the OAU before you unseat the OAU. Invisible laser radiation may be present in an operational OAU, which may cause blindness.

2. Remove protection caps from fiber patch cord connectors.
3. Connect one end of a fiber patch cord to the OAU card transmitter labelled OUT, and connect the other end of the fiber patch cord to the OAU card receiver labelled IN. Refer to Figure 1.

   Note: Attenuate long reach optics by 10 db.
4. Insert the OAU. If a second OAU is installed, repeat Steps 1 to 3.

Figure 1 OAU Loop Connection (OSIRIS STD Shelf)



Identifying Nodes

Each shelf in an OSIRIS network must be assigned a name (TID) and ID so that it is recognized by other NEs in the network. A copy of the network setup, known as the TIDMAP, must also be downloaded so that any NE can recognize all other network NEs.

Follow the three procedures in this section to identify all nodes on the network.

Assigning a Name (TID) and ID

Before you provision a node, you must assign the node a name (TID) and ID.

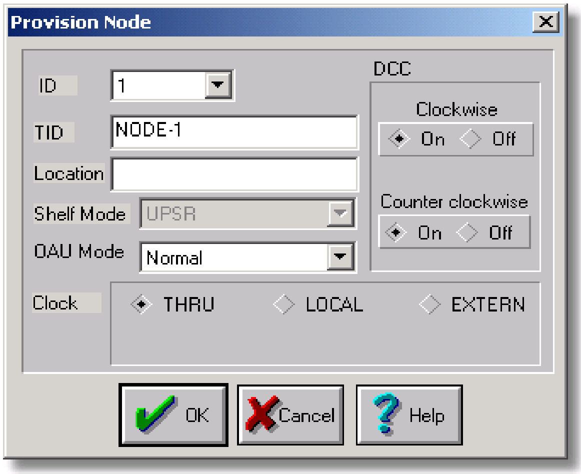
Follow these steps to assign a TID and ID Number to a new node:

1. Write down the names (TIDs) of NEs for the network as well as the Node ID. Also include TIDs of neighboring nodes. An example of this information appears as follows:

Location of Node	Node ID	TID	Clockwise (TID)	Counter-clockwise (TID)
City	1	Node1	Node2	Node3
Town	2	Node2	Node3	Node1
Office tower	3	Node3	Node1	Node2

2. Establish a direct connection to the OSIRIS optical multiplexer. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for details. The **Network Status** dialog box appears.

3. Double click the unprovisioned node. The **Provision Node** dialog box appears.



4. Select an **ID** number. Refer to the notes you made in Step 1.

   Note: Each node must be assigned a unique ID and TID.

5. Enter a **TID**. Refer to the notes you made in Step 1.

   Note: Each node must be assigned a unique TID.

6. Select an **OAU Mode**. You can set this parameter to **Locked** or **Normal**. OAU Mode must be **Locked** if transmitting EC1-VT or OC-3 Trib VT traffic.

7. Set **Clock** to **LOCAL**.

WARNING

Do not modify the DCC settings. If DCC settings are changed, communication between nodes may be interrupted once you add the new node to the existing network.

Note: These settings instruct the NE to generate its own timing information. At this stage of ring start-up NEs are not yet connected as a network.

When provisioning Network clock settings, note the following:

- nodes are set as **THRU** when timing information is generated remotely.
- nodes are set as **LOCAL** when timing information originates from that node.
- nodes are set as **EXTERN** when timing information originates from an external timing source.

For more information on Network clock settings, refer to “Provisioning Network Clock Information” on page 57.

8. Click **OK**. The **Node Identity Manager** appears.

   When you change an ID number or TID using OverView software, the static node map must be updated on the new node.

9. Click **Copy On-Line**. The new node ID number and TID appear in the **Static Node Map** column.

10. Click **Download**. The Network Status dialog box reappears. The ID number and TID have been provisioned for this node.

11. Repeat this procedure for all nodes.

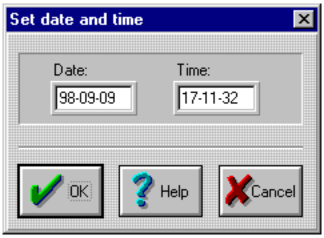
Setting the Date and Time

The system date and time are set to a default when you power up the new OSIRIS optical multiplexer.

Note: This procedure must be repeated on each node within an OSI ring.

To provision the current date and time, perform the following steps:

1. Right-click the node icon and click **Download Real Time Clock**. The **Set Date and Time** dialog box appears.



2. Enter the current date (yy-mm-dd).
3. Enter the current time (hh-mm-ss).
4. Click **OK**. The Network Status dialog box reappears. The date and time have been provisioned for the new node.

Downloading the Network TIDMAP

The map of the OSIRIS network must be downloaded to each new node. This lets each node recognize and communicate with other nodes in the network.

Note: This procedure is not necessary when using OSI.

To enter and download the network TIDMAP for a node, perform the following steps.

1. From the **Network** menu click **Node Identity Manager**. The **Node Identity Manager** appears.
2. Click **NEW**. The **New TIDMAP** Entry dialog box appears.

   Note: This procedure informs the new node that other nodes will eventually be added to the OSIRIS network. Adding a new node through the New TIDMAP Entry dialog box **does not** provision this node. You must still physically connect to other nodes and provision them using OverView software.

3. Select the **ID**. The ID and TID must be those of the node being added.
4. Click **OK**. The new node appears in the **Static Node Map** column.
5. Click **Download**. The static node map is transferred to the node.

6. Enable Switching Reported. Right-click the node and click **Maintenance Path Switching** then **Switching Reported**. This instructs the system to inform you of path switching events during regular operation of an OSIRIS network.

7. Log off and disconnect from the OSIRIS optical multiplexer. Refer to *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)*.

8. Repeat the sections "Assigning a Name (TID) and ID" to "Downloading the Network TIDMAP" for each new node added to the network.

Connecting Fiber to the Nodes

Once nodes are physically installed in their permanent locations you must connect them to the optical fiber. Make sure that you have physically installed the shelf before connecting it to the optical fiber.

Follow the procedure below to connect fiber patch cords to the OAUs.

WARNING

Do not remove the protective caps from the OAU before you unseat the OAU. Invisible laser radiation may be present in an operational OAU, which may cause blindness.

1. If the Optical Access Unit (OAU), located in the slot labelled OAU-A, is completely inserted, unseat it. **This is a CRITICAL step.**
2. Remove the protective caps from the OAU and fiber patch cord A.
3. Clean the fiber with alcohol and a piece of lint-free tissue.
4. Connect the transmit patch cord from fiber A (default path) to the OUT connector on the OAU in the slot labelled OAU-A.
5. Connect the receive patch cord from fiber A to the IN connector on the same OAU.
6. Insert the OAU.
7. If the OAU, located in the slot labelled OAU-B, is completely inserted, unseat it. **This is a CRITICAL step.**
8. Remove the protective caps from the OAU and fiber patch cord B.
9. Clean the fiber with alcohol and a piece of lint-free tissue.
10. Connect the transmit patch cord from fiber B (alternate path) to the OUT connector on the OAU in the slot labelled OAU-B.
11. Connect the receive patch cord from fiber B to the IN connector on the same OAU.
12. Insert the OAU.
13. Repeat Steps 1 to 12 for each node in the network.

Provisioning Network Clock Information

Provision the network clock after you have:

- Provisioned and downloaded the network TIDMAP to all nodes.
- Connected all nodes to the optical fiber.

Network clock information was originally set to LOCAL and REGEN because each node was isolated. Once all nodes are connected to the fiber, one element must control timing for the network.

Two types of Network clock may be provisioned:

- Internal Network clock
- External Network clock

Internal Network Clock

If you want the internal clock of a particular node to generate timing for a network, you must set the clock to LOCAL.

Note: Do not confuse the local node with the node generating Network clock information (LOCAL). The local node is the one connected directly to the PC operating OverView software. The node known as LOCAL provides Network clock information for the OSIRIS network and is not required to be connected to the PC operating OSIRIS-VUE software.

All other nodes must have the clock set to THRU.

External Network Clock

If you want an external timing device to supply timing to the network, you must set the clock to EXTERN. The node connected to the External clock must have a mapper channel reserved and provisioned for timing information.

All other nodes must have the clock set to THRU.

One node on the network must initiate synchronization of all nodes. This node is provisioned as REGEN.

Provisioning an Internal Network Clock

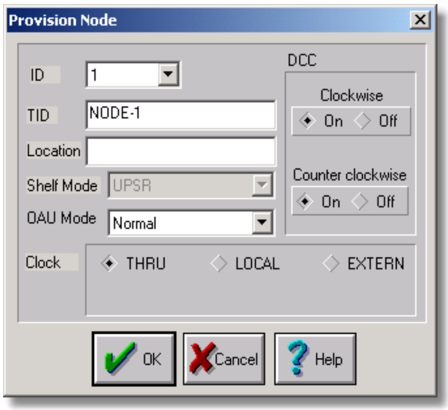
To provision network timing information, do the following steps:

1. Record the Network Clock settings for each node in the network.

   The following is an example of this information.

Node ID	TID	Clock	
1	Node1	LOCAL	
2	Node2	THRU	
3	Node3	THRU	

2. Right-click the node you want to provision as LOCAL and select **Set Shelf Info**. The **Provision Node** dialog box appears.



3. Set clock to **LOCAL**.

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

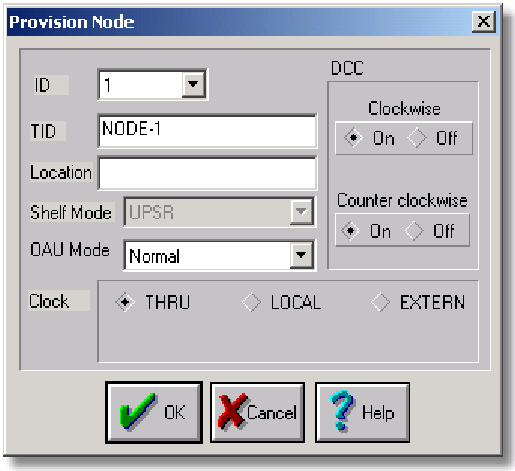
4. Click **OK**. The Network Status dialog box reappears.
5. Verify that all other nodes have Clock set to THRU.

Provisioning an External Network Clock

An externally generated Network clock originates from outside an OSIRIS network. Network clock timing information must enter the network through channel(s) on one node provisioned as EXTERN. This node synchronizes the network timing information for all other nodes. All other nodes must be set to THRU.

To provision network timing information, follow these steps:

1. Right-click the node that you want to provision as the External clock and click **Set Shelf Info**. The **Provision Node** dialog box appears.



2. Set Clock to **EXTERN**.

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

3. Click OK. The Network Status dialog box reappears. A Clock Missing alarm may appear in the Active Alarms report. This alarm occurs because no Network clock channel has been provisioned yet.
4. Verify that all other nodes have Clock set to THRU.

Provisioning an External Network Clock Channel

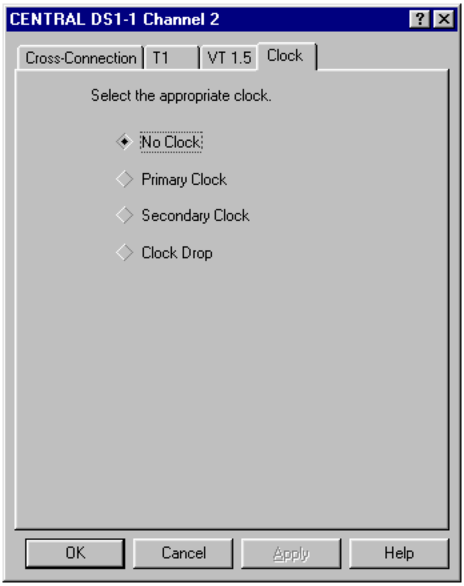
The Network clock provides timing information through a provisioned mapper channel on the node defined as EXTERN.

Note: All mappers are capable of providing Primary and Secondary external timing. This section describes timing source provisioning for DS1/E1 mappers. This procedure is similar for other mappers, such as EC-1 or OC3c/STM-1.

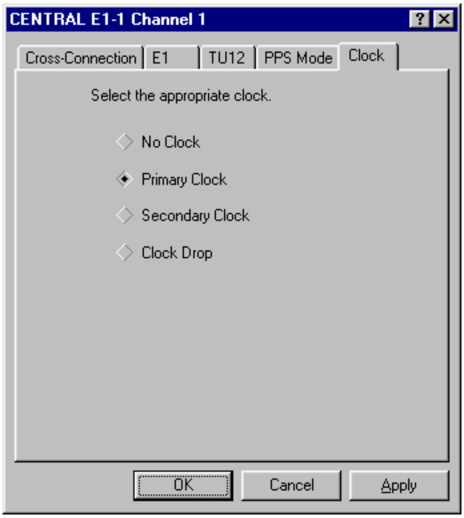
To provision a channel or channels reserved for this information, do the following steps:

1. In the **Network Status** dialog box, double-click the node provisioned as EXTERN. The **Shelf-level** dialog box appears.
2. Right-click a slot that contains a DS1/E1 mapper.
3. Click **Provision As**, then click **DS1/E1**.
4. Double-click the DS1/E1 mapper card. The **Mapper-level** dialog box appears.
5. Double-click the first channel. The **Channel-level** dialog box appears.
6. Click the **Clock** tab.

SONET



SDH



7. Click **Primary Clock**.
8. Click **OK**. The **Confirm Operation** dialog box appears.
9. Click **Yes**.

Verifying Network Status

To verify the status of all nodes, perform the following steps:

1. Verify that all nodes are displayed in the **Network Status** dialog box.
2. Verify that all nodes display proper ID names and numbers.
3. Verify that no alarms appear in the network.

   If any of these conditions cannot be verified, refer to the *OSIRIS® Troubleshooting Guide (203-008)*, or "Contacting Customer Service" on page 19.

Chapter 3

Point to Point Start-up Using one Fiber Pair

Under normal operation an OSIRIS network contains two OAUs per shelf. Each OAU is attached to two optical-fibers. However, a Point to Point network can be installed at a reduced cost with only one OAU per shelf and one optical-fiber pair.

Note: An OSIRIS network is a Unidirectional Path Switching Ring (UPSR) which offers path redundancy with a backup fiber. A single fiber ring application does **not** offer path protection.

In a single fiber point-to-point connection, you can use either one or two OAU cards per node. Ring start-up procedures for both one and two OAU cards are described in this chapter.

How to Start-up with One OAU

If you are using only one OAU per node, you can place both OAUs in the A slots, or you can place both OAUs in the B slots. The start-up procedure is different depending on which slot the OAU cards are installed in. The OAUs must be installed before you start this procedure.

OAUs Residing in Slot A

The procedure is divided into three sections:

- Defining the Local node
- Defining the Remote node
- Removing outstanding alarms

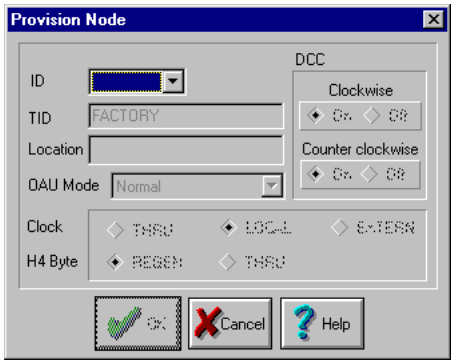
Defining the Local Node

1. Connect the fibers as shown below (Tx to Rx and Rx to Tx).

Figure 2 Start-up with one fiber pair and one OAU per NE

2. Connect your PC to one of the network elements. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for instructions on how to connect.
3. Log on to the network element OSIRIS-VUE software. The default name and password are **ROOT** and **FACTORY1%**. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for instructions on how to log on.

4. In the **Network Status** window, double-click the node icon. The **Provision Node** dialog box appears.



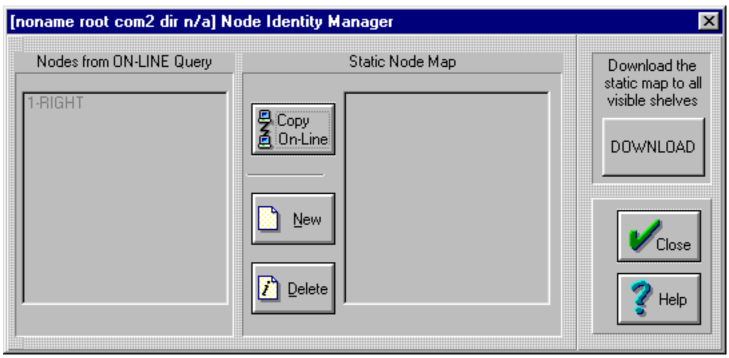
5. Set the **ID**, **TID** and **Clock**.

   Note: Set Clock to **LOCAL**.

WARNING

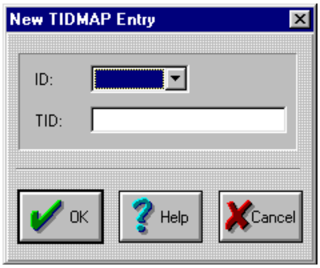
Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

6. Click **OK**. The **Node Identity Manager** dialog box appears.



7. Click the **Copy On-line** button. The Local node name appears in the **Static Node Map** column.

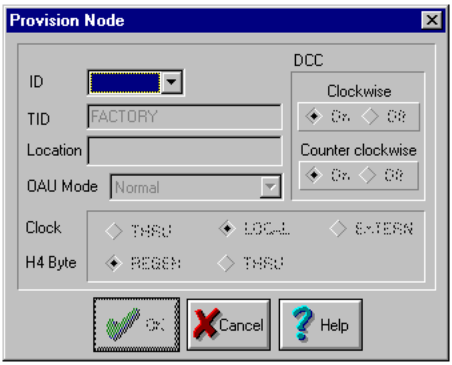
8. Click the **New** button. The **New TIDMAP** Entry dialog box appears.



9. Enter the **ID** and **TID** of the Remote node that will be part of the network, then click **OK**. The Node Identity Manager dialog box reappears.
10. Click the **Download** button.
11. Log off the OSIRIS optical multiplexer.

Defining the Remote Node

1. Physically re-locate to the site of the second network element.
2. Log on to the network element through OSIRIS-VUE software. The default name and password are **ROOT** and **FACTORY1%**. Refer to *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for log on instructions
3. In the **Network Status** window, double-click the node icon. The **Provision Node** dialog box appears.



4. Set the **ID** and **TID** for this node.

5. Set **Clock** to **THRU** and **H4 Byte** to **THRU**, then click **OK**.

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

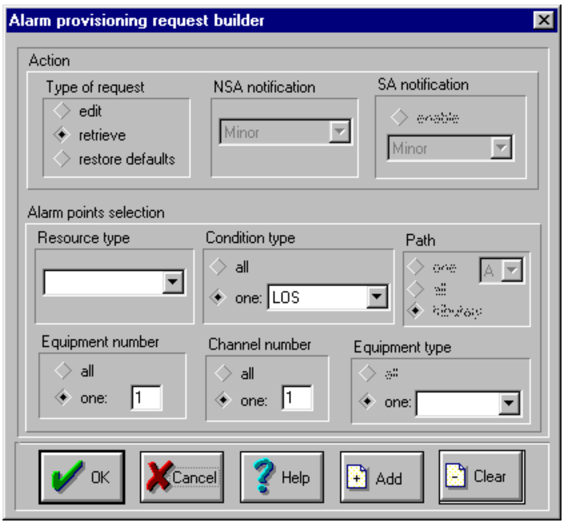
The **Node Identity Manager** dialog box appears.

6. Click the **Copy On-line** button. The Local node name appears in the **Static Node Map** column.
7. Click the **New** button. The **New TIDMAP** Entry dialog box appears.
8. Enter the ID and TID of the first node that you configured, then click **OK**. The Node Identity Manager dialog box reappears.
9. Click **Download**. Both nodes appear in the **Network Status** dialog box. Wait for the status to be updated.

   DCC and OAU-B card removal alarms appear on both shelves. Go to the next section to remove outstanding alarms.

Removing Outstanding Alarms

1. To remove outstanding alarms on a shelf, right-click a node, then click **Full Alarm Provisioning**. The **Alarm Provisioning Request Builder** dialog box appears.



2. Set **Type of request** to **edit**.

3. Set **NSA notification** to **Not Reported**.
4. Enable **SA notification** and set it to **Not Reported**.
5. Set **Resource type** to **EQPT**.
6. Set **Condition type** to **one** and select **CRDRMVD**.
7. Set **Equipment type** to **one** and select **OAU card**.
8. Set **Path** to **one** and select **B**.
9. Click **Add**.
10. Set **Resource type** to **OAU facility**.
11. Set **Condition type** to **DCC**.
12. Click **Add**.
13. Click **OK**.
14. Repeat Steps 1 to 13 for the second node.
15. In the **Network Status** window, right-click each node and then select **Update Shelf**.

OAUs Residing in Slot B

The start-up procedure for OAUs in slot B brings up the network faster than the previous procedure. The limitation of this procedure is that several error messages appear. Click **Cancel** whenever an error message appears in OSIRIS-VUE.

The procedure is divided into three sections:

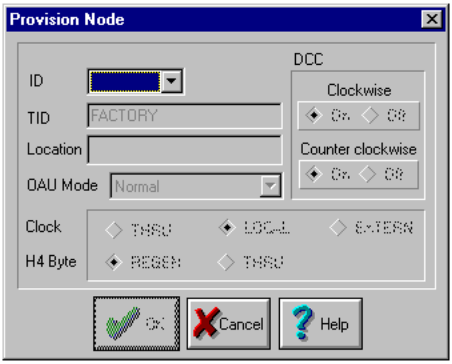
- Defining the Local node
- Defining the Remote node
- Removing outstanding alarms

Defining the Local Node

1. Connect the fibers as shown below (Tx to Rx and Rx to Tx).

Figure 3 Start-up with one fiber pair and one OAU per NE

2. Connect your PC to one of the network elements. Refer to *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001).*
3. Log on to the network element through OverView software. The default name and password are **ROOT** and **FACTORY1%**. Refer to *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for log on instructions.
4. In the **Network Status** dialog box, double-click the node. The **Provision Node** dialog box appears.



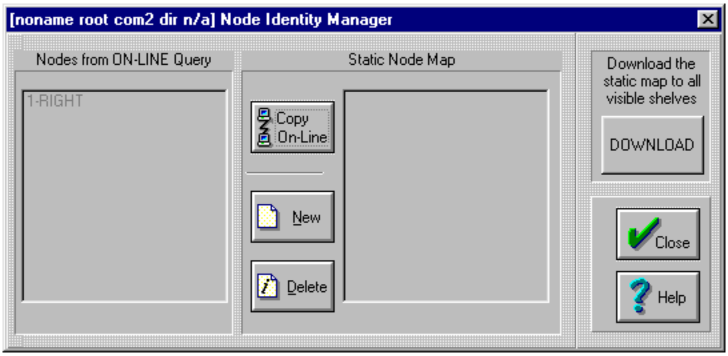
5. Set the **ID**, **TID** and **Clock.**

Note: Set Clock to **LOCAL**.

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

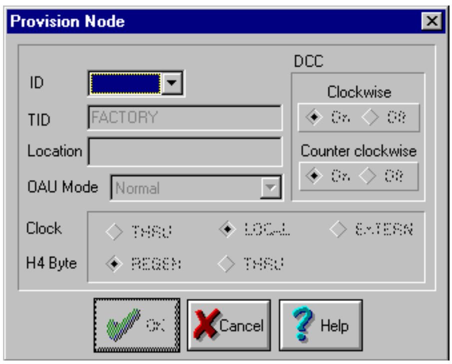
6. Click **OK**. The **Node Identity Manager** dialog box appears.



7. Click **Copy On-line**, then click **Download**.
8. Wait for the second node to appear in the **Network Status** window.

Defining the Remote Node

1. In the **Network Status** dialog box, double-click the second node. The **Provision Node** dialog box appears.



2. Set the **ID**, **TID** and **Clock**, then click **OK**.

Note: Set Clock to **THRU**.

WARNING

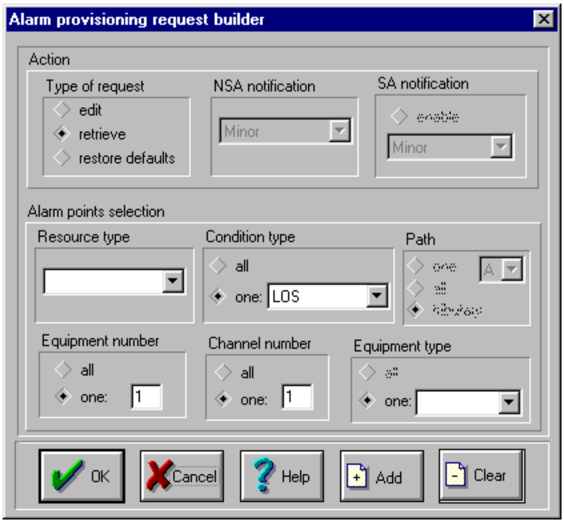
Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

An **Update Failed** error message appears.

3. Click **Cancel** to exit the error message. The **Node Identity Manager** dialog box appears. Both nodes appear in the dialog box.
4. Click **Copy On-line**, then click **Download**. A **TIDMAP Not Downloaded** error message appears.
5. Click **Cancel** to exit the error message. A **Clock Source Not Changed** error message appears.
6. Click **Cancel** to exit the message. The Network Status dialog displays three nodes.
7. Log out of the session and then log in again. Two nodes appear in the Network Status dialog with DCC and OAU-A card removal alarms. If the second node is crossed out, on the **Network** menu, click **Node Identity Manager**. Click **Copy Online**, then click **Download**.
8. Go to the next section to remove outstanding alarms.

Removing Outstanding Alarms

1. To remove outstanding alarms, right-click a node, then click **Full Alarm Provisioning**. The **Alarm Provisioning Request Builder** dialog box appears.



2. Set **Type of request** to **edit**.
3. Set **NSA notification** to **Not Reported**.
4. Set **SA notification** to **enable** and **Not Reported**.
5. Set **Resource type** to **EQPT**.
6. Set **Condition type** to **one** and select **CRDRMVD**.
7. Set **Equipment type** to **one** and select **OAU card**.
8. Set **Path** to **one** and select **A**.
9. Click **Add**.
10. Set **Resource type** to **OAU facility**.
11. Set **Condition type** to **DCC**.
12. Click **Add**.
13. Click **OK**.
14. Repeat Steps 1 to 13 for the second node.
15. In the Network Status window, right-click each node and then select **Update Shelf**.

How to Start-up with Two OAUs

Follow this procedure if you are using two OAU cards per node. This procedure is a temporary installation used only if you do not have adequate optical-fiber.

The OAUs must be installed before you start this procedure. The procedure is divided into three sections:

- Defining the Local node
- Defining the Remote node
- Removing outstanding alarms

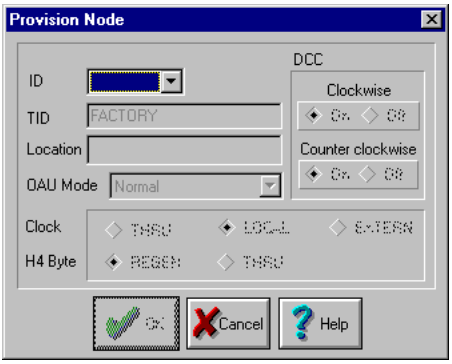
Defining the Local Node

1. Connect the local shelf's OAU-A Tx to the remote shelf's OAU-A Rx.
2. Do not remove dust caps from the unused OAU connectors.
3. Connect the remote shelf's OAU-B Tx to the local shelf's OAU-B Rx.

Figure 4 Start-up with one fiber pair and two OAUs per NE

4. Connect the Local network element to your PC. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for connection instructions.
5. Log on to the Local network element through OverView software. The default name and password are **ROOT** and **FACTORY1%**. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for log on instructions.

6. In the Network Status dialog box, double-click the Local node. The **Provision Node** dialog box appears.

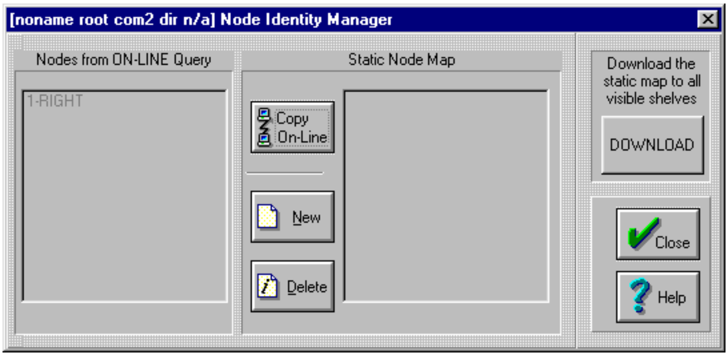


7. Set the **ID**, **TID** and **Clock**, then click **OK**.
8. Set **Clock** to **LOCAL**.

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

The **Node Identity Manager** dialog box appears.



9. Click **Copy On-line**, then click **Download**.
10. Wait for the remote end node to appear. This may take up to 40 seconds.

Defining the Remote Node

1. In the Network Status dialog box, double-click the remote node.
2. Set the **ID**, **TID** and **Clock**, then click **OK**.
3. Set **Clock** to **THRU**.

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between nodes may be interrupted.

The **Node Identity Manager** dialog box appears.

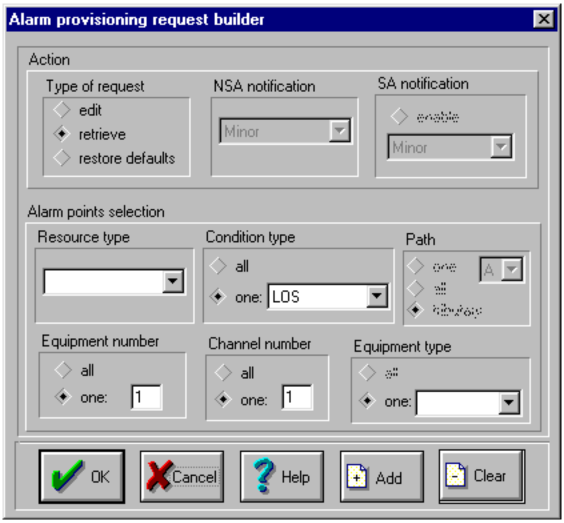
4. Click **Copy On-line**, then click **Download**.

   Major alarms appear on both network elements. The Local node displays a loss of signal (LOS) on OAU-A, and the far-end node displays an LOS on OAU-B. Proceed to the next section to remove these alarms.

Removing Outstanding Alarms

1. To remove outstanding alarms, right-click the Local node, then click **Full Alarm Provisioning**.

   The **Alarm Provisioning Request Builder** dialog box appears.



2. Set **Type of request** to **edit**.
3. Set **NSA notification** to **Not Reported**.
4. Set **SA notification** to **enable** and **Not Reported**.

5. Set **Resource type** to **OAU facility**.
6. Set **Condition type** to **one** and select **LOS**.
7. Set **Equipment type** to **one** and select **OAU card**.
8. Set **Path** to **one** and select **A**.
9. Click the **Add** button, then click **OK**.
10. Repeat Steps 1 to 9 for the Remote node, but set **Path** to **B**.
11. In the **Network Status** window, right-click each node and then select **Update Shelf**.

Chapter 4

Adding and Removing Network Nodes

This chapter describes how to add or remove network nodes to/from OSIRIS networks.

Adding a Node to an Existing Network

The procedure consists of the following tasks:

- Switching traffic to fiber A
- Connecting fiber B to the new NE
- Provisioning the new NE
- Switching traffic to fiber B
- Connecting fiber A to the new NE
- Removing traffic force from fiber B

Switch Traffic to Fiber A

You must force all traffic to fiber A before you add the new node to fiber B.

To force all traffic to fiber A, perform the following steps:

1. Log on the network using OSIRIS-VUE software. The **Network Status** dialog box appears.
2. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
3. Right click any node icon and click **Maintenance Path Switching** then click **Force All On A**. A confirmation dialog box appears.
4. Click **Yes**.
5. Repeat Steps 2 and 3 for each node icon.

   A Forced Switch Request (FRCDSWREQ) message appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.

   Note: A forced switch causes a traffic hit that meets Telcordia requirements per cross-connected path.

Connecting Fiber B to the New NE

Once all network traffic is switched to fiber A, the new node may be inserted on to fiber B without affecting network traffic.

For this procedure, existing nodes are referred to as **Node 1** and **Node 2**. The new node is referred to as **Node 3**.

Note: Any fiber connections to or from an NE should be performed through a demarcation point, such as a fiber patch panel, and not directly to the OAUs.

1. Disconnect the OAU-B TX of Node 1. Refer to Figure 5.

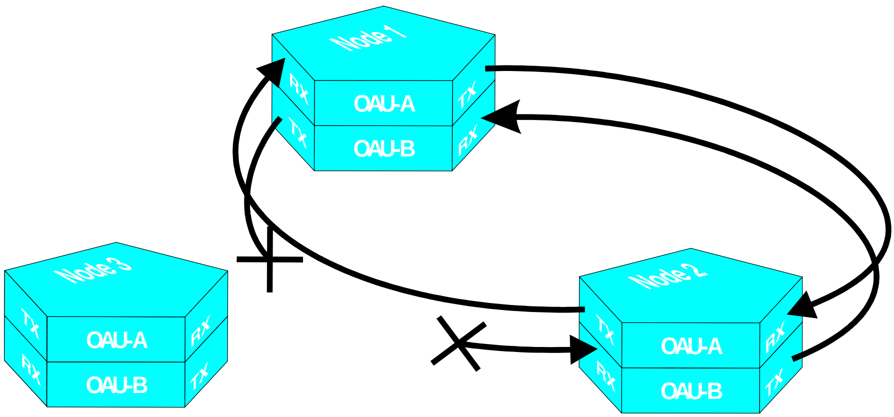
CAUTION

Take special care in handling any fiber cables on the B ring. Invisible laser radiation may be present in an operational fiber ring, which may cause blindness.

2. Disconnect OAU-B RX of Node 2.

   Note: Disconnecting the OAU-Bs does not interrupt network traffic because traffic has been forced to fiber A. In this example, a DCC-X alarm appears for OAU-B of Node 2 and a DCC-Y alarm appears for OAU-B of Node 1. These DCC alarms are minor and are not service-affecting.

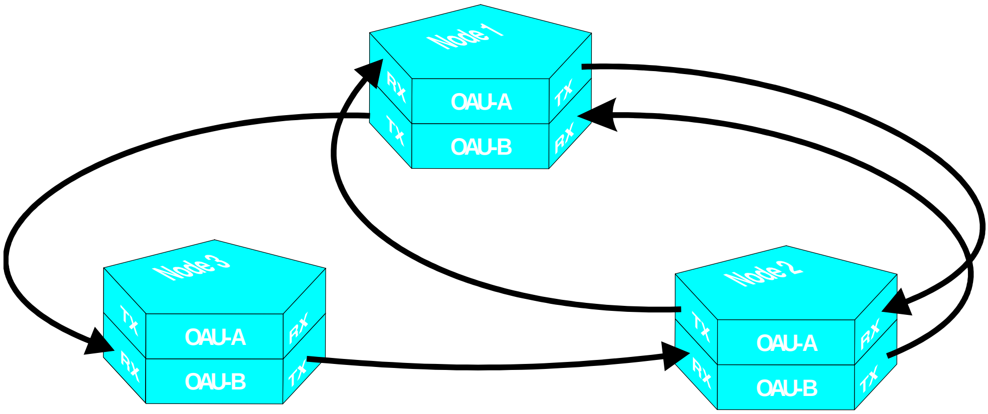
Figure 5 Disconnecting OAU-B TX of Node 1 and OAU-B RX of Node 2



3. Connect OAU-B TX of Node 1 to OAU-B RX of Node 3. Refer to Figure 6.

4. Connect OAU-B TX of Node 3 to OAU-B RX of Node 2.

Figure 6 Inserting OAU-B of Node 3 into the Existing Network

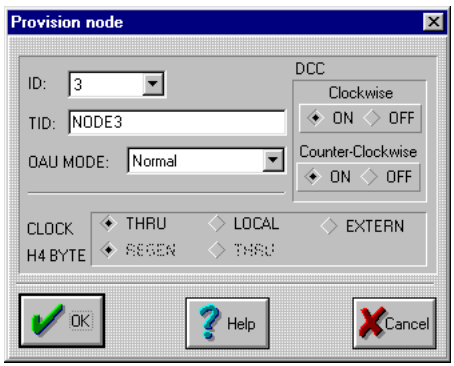


Provisioning the New NE

This section applies only when using proprietary DCC. When using OSI/DCC, the new NE must be locally configured or pre-configured.

Node 3 appears in the Network Status dialog box as follows:

1. Double-click this node. The **Provision Node** dialog box appears.



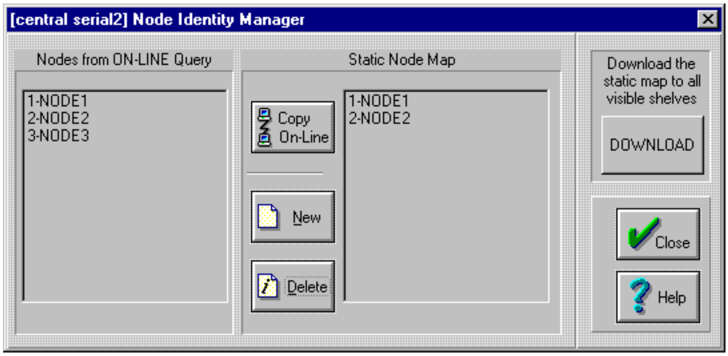
2. Select an **ID** number.
3. Enter a name in the **TID** text box.

4. Set **Clock** and **H4 Byte** to **THRU.**

WARNING

Do not modify the DCC settings. If the DCC settings are changed, communication between NEs may be interrupted once you add the new NE to the existing network.

5. Click **OK**. The **Node Identity Manager** appears.



6. Click **Copy On-Line**. The new node ID number and TID appear in the **Static Node Map** column.
7. Click **Download**. The Network Status dialog box reappears. The ID number and TID have been provisioned for this node. The Network Status dialog box reappears.

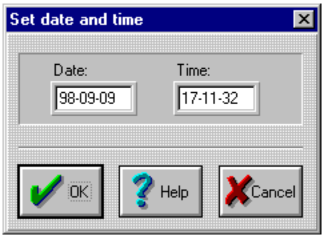
   The following alarms remain outstanding:

Alarm	Node	Severity	Reason
Card Removed (CRDRMVD) OAU-A	Node3 (new node)	Major	OAU-A has not yet been inserted to close the network on both fibers paths. This alarm is not service-affecting because traffic does not flow through the A side on this node.
DCC-X	Node2	Minor	DCC alarms appear until both fibers of the new node are connected to the network.
DCC-Y	Node1	Minor	DCC alarms appear until both fibers of the new node are connected to the network.

   The fiber lines between the nodes in the Network Status dialog box do not appear green because the DCC is not continuous.

8. Verify that all other alarms have been cleared. Refer to the *OSIRIS® Troubleshooting Guide (203-008)*.

9. To provision a date and time, right-click the node icon and click **Download Real Time Clock**. The **Set Date and Time** dialog box appears.



Note: When using OSI/DCC, download RTC must be done in each NE.

10. Enter the current date (yy-mm-dd).
11. Enter the current time (hh-mm-ss).
12. Click **OK**. The Network Status dialog box reappears.
13. To set the bandwidth for the new node, click **Bandwidth Provisioning** from the **Network** menu. The **Bandwidth Provisioning** dialog box appears.
14. The new NE bandwidth must be the same as nodes already contained in the network.
    1. Click a node previously existing in the network from **Network Element or Ring**. Record the bandwidth for each STS-1/TUG3 (e.g., ASYNC, VTFLOAT).
    2. Click the new node from **Network Element or Ring**.
    3. Right-click the STS-1/TUG3 and change bandwidth to the same as all other nodes in the network (e.g., **Change STS-1 to VTFLOAT**).
    4. Repeat Step 2 and 3 for each STS-1/TUG3.
15. Click **OK**. Bandwidth has been set for the new network element.

Switch Traffic to Fiber B

Switching network traffic to fiber B includes the following procedures:

- Provision a test cross-connection (optional)
- Switch test traffic to fiber B
- Force network traffic to fiber B

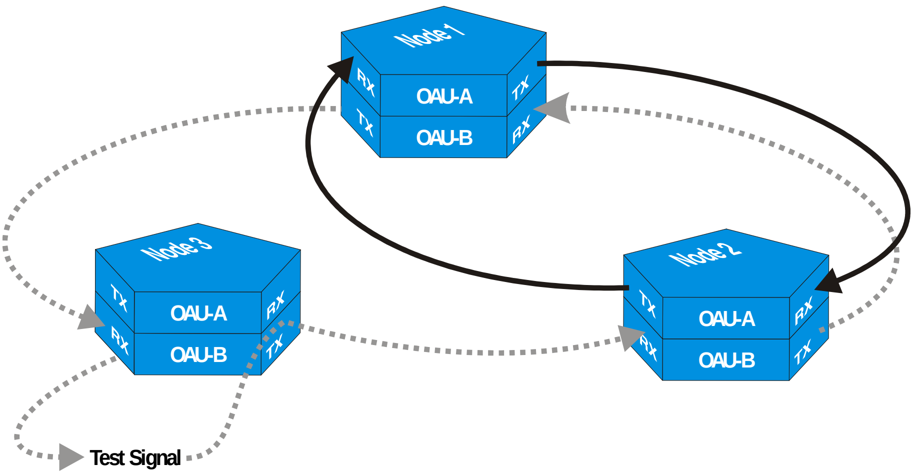
Provision a Test Cross-connection (Optional)

You can now test the continuity of the optical signal on fiber B.

1. Provision a cross-connection (e.g., a DS1/E1) on the local node in the OSIRIS network. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for provisioning instructions.

   Continuity testing is performed without dropping the signal at the far end of the network. Instead, the signal circulates back to the original location on this time slot of the bandwidth. The signal should return with no bit errors.

Figure 7 Sending a Test Signal Through the "B" Fiber



Switch Test Traffic to Fiber B

Since the default path is fiber A, you must switch test traffic to fiber B.

1. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
2. In the **Shelf-level** dialog box, double-click the mapper carrying the test signal. The **Mapper-level** dialog box appears.
3. Double-click the cross-connected channel. The **Channel-level** dialog box appears.
4. Click the **PPS** tab.
5. Force traffic on fiber B. A confirmation dialog box appears.
6. Click **Yes**.

   A Forced Switch Request (FRCDSWREQ) alarm appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.
7. Verify that no bit errors appear in your test traffic.

Once you have verified that test traffic flows error-free on fiber B, you can switch all network traffic to fiber B.

8. Deprovision the test cross-connection.

Force Traffic to Fiber B

To switch network traffic to fiber B, perform the following steps:

1. Right-click a node icon and click **Maintenance Path Switching**, then click **Remove all Lock/Force**.
2. Repeat Step 1 for each node **except the new node**.
3. Right-click every node (except the new one) and click **Maintenance Path Switching**, then click **Force All on B**.

   A Forced Switch Request (FRCDSWREQ) alarm appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.

   Note: A forced switch causes a traffic hit that meets Telcordia requirements per cross-connected path.

Connecting Fiber A to the New NE

Now that traffic is carried on fiber B, you can connect fiber A to the new node. To do this, perform the following steps:

Note: Any fiber connections to or from an NE should be performed through a demarcation point, such as a fiber patch panel, and not directly to the OAUs.

1. Disconnect OAU-A RX of Node 1. Refer to Figure 8.

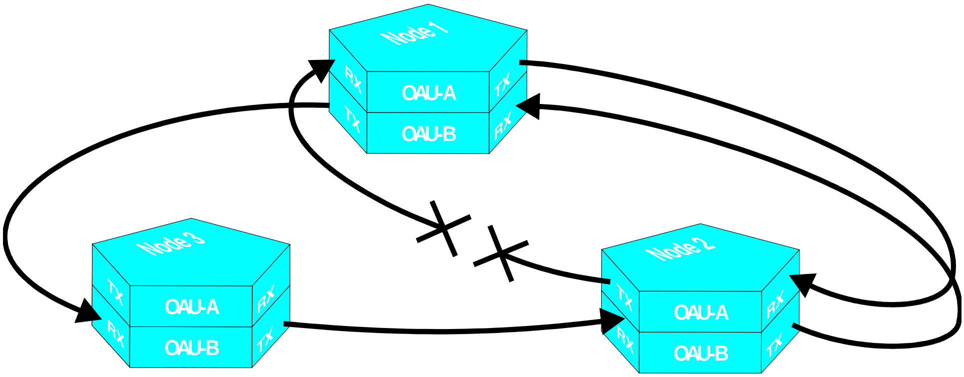
WARNING

Take special care in handling any fiber cables on the B ring. Invisible laser radiation may be present in an operational fiber ring, which may cause blindness.

2. Disconnect OAU-A TX of Node 2.

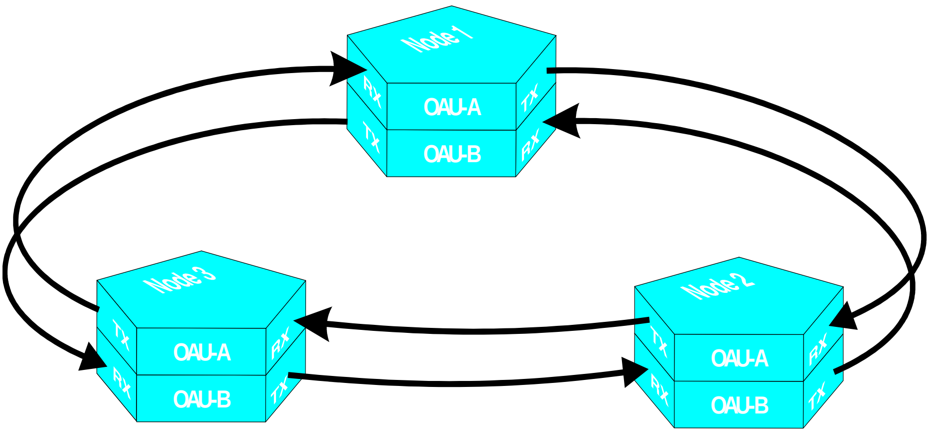
Note: Disconnecting the OAU-As does not interrupt network traffic because traffic is forced to the B path.

Figure 8 Disconnecting OAU-A RX of Node 1 and OAU-A TX of Node 2



3. Connect OAU-A TX of Node 2 to OAU-A RX of Node 3. Refer to Figure 9.
4. Connect OAU-A TX of Node 3 to OAU-A RX of Node 1.

Figure 9 Inserting OAU-A of Node 3



Fibers appear between all three nodes in the Network Status dialog box.

Removing Force From Fiber B

Removing traffic force from fiber B includes the following procedures:

- Provision a test cross-connection (optional)
- Lock test traffic to fiber A
- Remove traffic force from fiber B

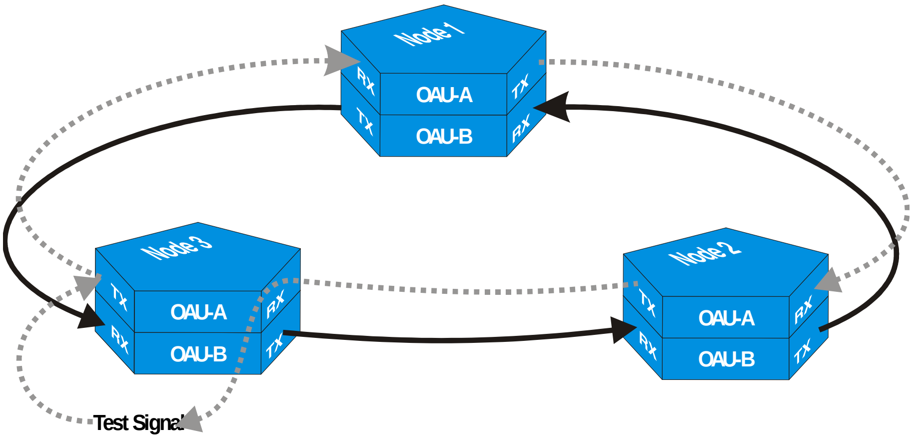
Provision a Test Cross-connection (Optional)

You can now test the continuity of the optical signal on fiber A.

1. Provision a cross-connection (e.g., DS1/E1) on the local node in the OSIRIS network.

   Continuity testing is performed without dropping the signal at the far end of the network. Instead, the signal circulates back to the original location on this time slot of the bandwidth. The signal should return with no bit errors.

Figure 10 Sending a Test Signal Through the "A" Fiber



Switch Test Traffic on Fiber A

1. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
2. In the **Shelf-level** dialog box, double-click the mapper carrying the test signal. The **Mapper-level** dialog box appears.
3. Double-click the cross-connected channel. The **Channel-level** dialog box appears.
4. Click the **PPS** tab.
5. Force traffic on fiber A. A confirmation dialog box appears.
6. Click **Yes**.

   A Forced Switch Request (FRCDSWREQ) alarm appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.
7. Verify that no bit errors appear in your test data.

Once you have verified that test traffic flows error free on fiber A, you can remove the forced switch.

8. Deprovision the test cross-connection.

Remove Traffic Force from Fiber B

To remove network traffic force from fiber B, perform the following steps:

1. Right click a node and click **Maintenance Path Switching**, then click **Remove all Lock/Force**.
2. Repeat Step 1 for each node **except the new node**.

   Note: Traffic remains on the B path unless fiber B fails. If path A is preferred as default, use a Manual Switch to switch traffic to fiber A.

Removing an NE from an Existing Network

This chapter describes how to remove a network element from an existing network. The procedure consists of the following tasks:

- Switching traffic to fiber A
- Removing fiber B from extra NE
- Switching traffic to fiber B
- Removing fiber A from extra NE
- Removing traffic force from fiber B

Note: Before starting this procedure, verify that no cross-connections are provisioned on the node you want to remove.

Switch Traffic to Fiber A

You must force all traffic to fiber A before removing the extra node from fiber B.

To force all traffic to fiber A, perform the following steps:

1. Log on the network using OSIRIS-VUE software. The **Network Status** dialog box appears.
2. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
3. Right click any node icon and click **Maintenance Path Switching** then click **Force All On A**. A confirmation dialog box appears.
4. Click **Yes**.
5. Repeat Steps 3 and 4 for each node icon.

   A Forced Switch Request (FRCDSWREQ) message appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.

   Note: A forced switch causes a traffic hit that meets Telcordia requirements per cross-connected path.

Removing Fiber B from the Extra NE

Once all network traffic is switched to fiber A, the new node may be removed from fiber B without affecting network traffic.

For this procedure, existing nodes are referred to as **Node 1** and **Node 2**. The extra node is referred to as **Node 3**.

Note: Any fiber connections to or from an NE should be performed through a demarcation point, such as a fiber patch panel, and not directly to the OAUs.

1. Remove OAU-B from the extra node and disconnect the OAU-B TX and RX.

CAUTION

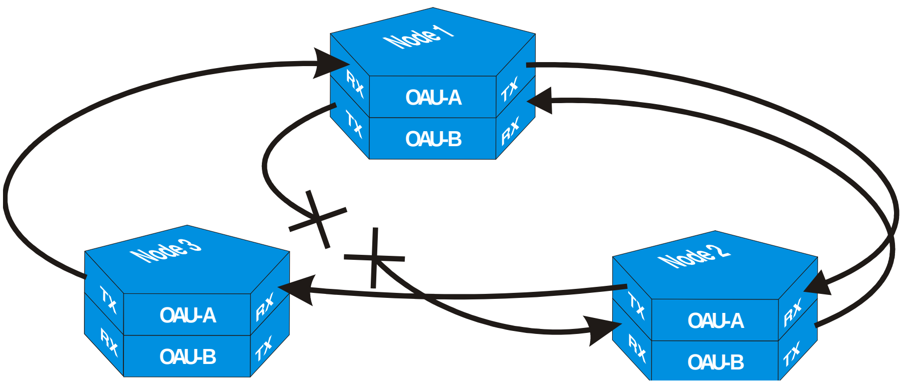
Take special care in handling any fiber cables on the B ring. Invisible laser radiation may be present in an operational fiber ring, which may cause blindness.

2. Disconnect OAU-B TX of Node 1. Refer to Figure 11.

   Note: Disconnecting the OAU-Bs does not interrupt network traffic because traffic has been forced to fiber A. In this example, a DCC-X alarm appears for OAU-B of Node 2 and a DCC-Y alarm appears for OAU-B of Node 1. These DCC alarms are minor and are not service-affecting.

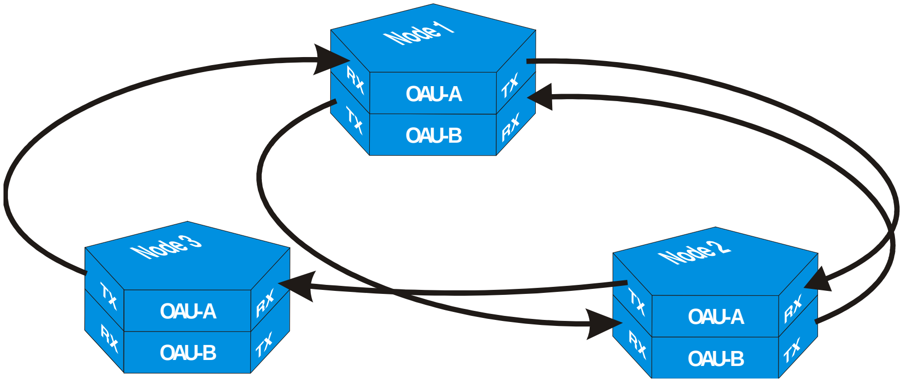
3. Disconnect OAU-B RX of Node 2.

Figure 11 Disconnecting OAU-B TX of Node 1 and OAU-B RX of Node 2



4. Connect OAU-B TX of Node 1 to OAU-B RX of Node 2.

Figure 12 Connecting OAU-B TX of Node 1 to OAU-B RX of Node 2



Switch Traffic to Fiber B

Switching network traffic to fiber B includes the following procedures:

- Provision a test cross-connection (optional)
- Switch test traffic to fiber B
- Force network traffic to fiber B

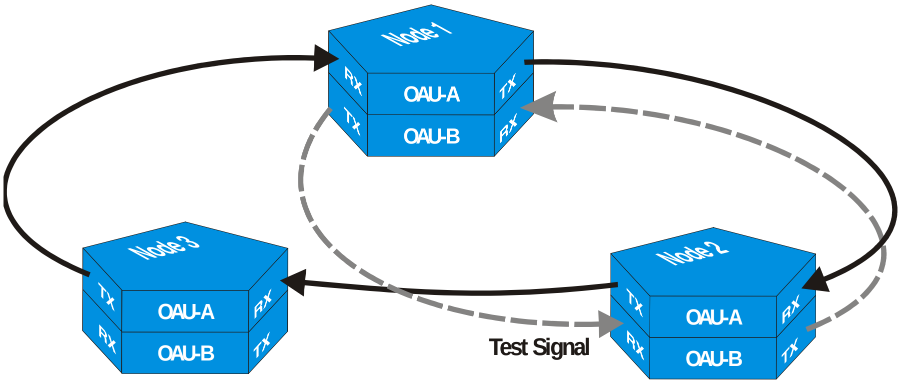
Provision a Test Cross-connection (Optional)

You can now test the continuity of the optical signal on fiber B.

1. Provision a cross-connection (e.g., a DS1/E1) on Node 1 or Node 2. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for provisioning instructions.

Continuity testing is performed without dropping the signal at the far end of the network. Instead, the signal circulates back to the original location on this time slot of the bandwidth. The signal should return with no bit errors.

Figure 13 Sending a Test Signal Through the "B" Fiber



Switch Test Traffic to Fiber B

Since the default path is fiber A, you must switch test traffic to fiber B.

1. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
2. In the **Shelf-level** dialog box, double-click the mapper carrying the test signal. The **Mapper-level** dialog box appears.
3. Double-click the cross-connected channel. The **Channel-level** dialog box appears.
4. Click the **PPS** tab.
5. Force traffic on fiber B. A confirmation dialog box appears.
6. Click **Yes**.

   A Forced Switch Request (FRCDSWREQ) alarm appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.
7. Verify that no bit errors appear in your test traffic.

   Once you have verified that test traffic flows error-free on fiber B, you can switch all network traffic to fiber B.
8. Deprovision the test cross-connection.

Force Traffic to Fiber B

To switch network traffic to fiber B, perform the following steps:

1. Right-click Node 1 or Node 2 and click **Maintenance Path Switching**, then click **Remove all Lock/Force**. Repeat this step for all nodes except the extra one (Node 3).
2. Right-click Node 1 or Node 2 and click **Maintenance Path Switching**, then click **Force All on B**. Repeat this step for all nodes except the extra one (Node 3).

   A Forced Switch Request (FRCDSWREQ) alarm appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.

   Note: A forced switch causes a traffic hit that meets Telcordia requirements per cross-connected path.

Removing Fiber A from the Extra NE

Now that traffic is carried on fiber B, you can remove fiber A from the extra node. To do this, perform the following steps:

Note: Any fiber connections to or from an NE should be performed through a demarcation point, such as a fiber patch panel, and not directly to the OAUs.

1. Remove OAU-A of the extra node and disconnect the RX and TX.

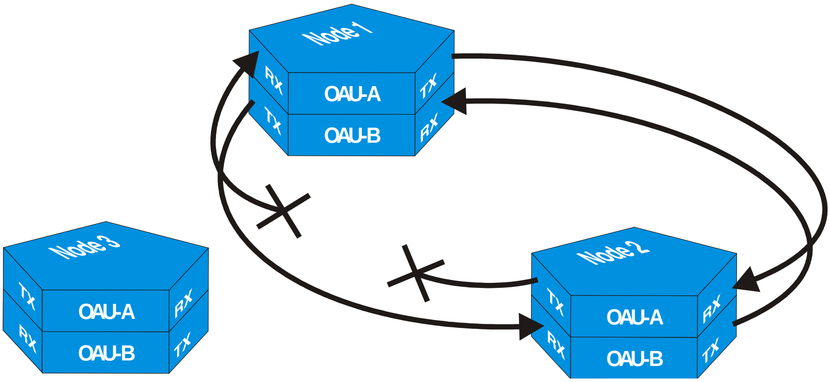
WARNING

Take special care in handling any fiber cables on the B ring. Invisible laser radiation may be present in an operational fiber ring, which may cause blindness.

2. Disconnect OAU-A TX of Node 2.

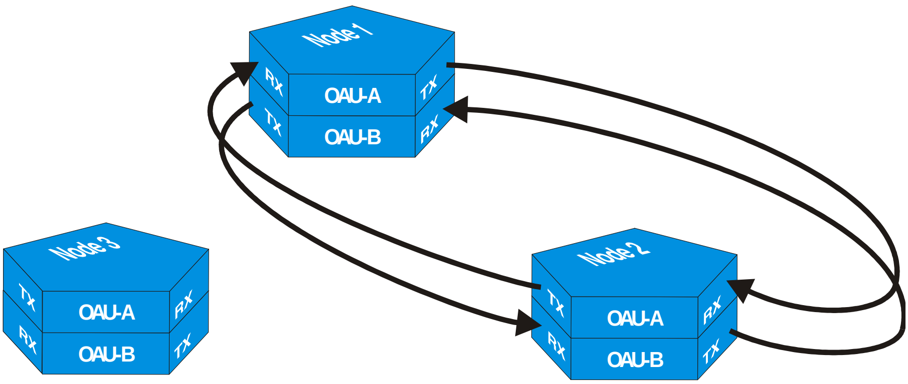
Note: Disconnecting the OAU-As does not interrupt network traffic because traffic is forced to the B path.

Figure 14 Disconnecting OAU-A RX of Node 1 and OAU-A TX of Node 2



3. Disconnect the OAU-A RX of Node 1.
4. Connect OAU-A TX of Node 2 to the OAU-A RX of Node 1.

Figure 15 Inserting OAU-A of Node 3



Fibers appear between Node 1 and Node 2 in the Network Status dialog box.

Removing Traffic Force From Fiber B

Removing traffic force from fiber B includes the following procedures:

- Provision a test cross-connection (optional)
- Lock test traffic to fiber A
- Remove traffic force from fiber B

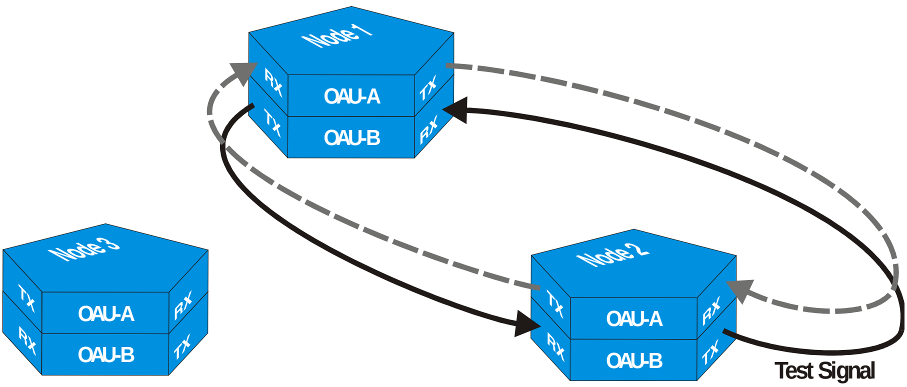
Provision a Test Cross-connection (Optional)

You can now test the continuity of the optical signal on fiber A.

1. Provision a cross-connection (e.g., DS1/E1) on Node1 or Node 2. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for provisioning instructions.

   Continuity testing is performed without dropping the signal at the far end of the network. Instead, the signal circulates back to the original location on this time slot of the bandwidth. The signal should return with no bit errors.

Figure 16 Sending a Test Signal Through the "A" Fiber



Switch Test Traffic on Fiber A

1. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
2. In the **Shelf-level** dialog box, double-click the mapper carrying the test signal. The **Mapper-level** dialog box appears.
3. Double-click the cross-connected channel. The **Channel-level** dialog box appears.
4. Click the **PPS** tab.
5. Force traffic on fiber A. A confirmation dialog box appears.

6. Click **Yes**.

   A Forced Switch Request (FRCDSWREQ) alarm appears in the Active Alarms report for each node. Forced Switch Requests are minor alarms and are not service-affecting.

7. Verify that no bit errors appear in your test data.

   Once you have verified that test traffic flows error free on fiber A, you can remove the forced switch.

8. Deprovision the test cross-connection.

Remove Traffic Force from Fiber B

To remove network traffic force from fiber B, perform the following steps:

1. Right click a node and click **Maintenance Path Switching**, then click **Remove all Lock/Force**.

2. Repeat Step 1 for each node

   Note: At this point all drop traffic remains on the B path unless fiber B fails. If path A is preferred as default, use a Manual Switch to switch traffic to fiber A.

Managing NE Upgrades

NE software is installed on the NMCU of all OSIRIS optical multiplexers. However, you may want to upgrade this software as new features become available.

Upgrading NE software may require upgrading the OAUs in your OSIRIS shelf. You can upgrade from one software version to the next, or you can upgrade from one software version to a higher capacity software. If you are upgrading the NE software to a higher capacity software, you will need to upgrade the OAUs for each node that this applies to.

This document consists of the following sections:

- NE software upgrade procedure
- OAU upgrade procedure
- Mixed NE software in OSIRIS optical multiplexer rings
- Network MCU

NE Software Upgrade Procedure

This procedure upgrades software to a new version of the same capacity, e.g., upgrading OC-3 to a more recent version of OC-3 software.

Upgrading the OC-3/STM-1, OC-12/STM-4 or OC-48 system software for a network element is done in five phases.

- Verifying the existing software
- Downloading the software
- Switching the software
- Verifying Multi-Service Ethernet & PacketPath compatibility

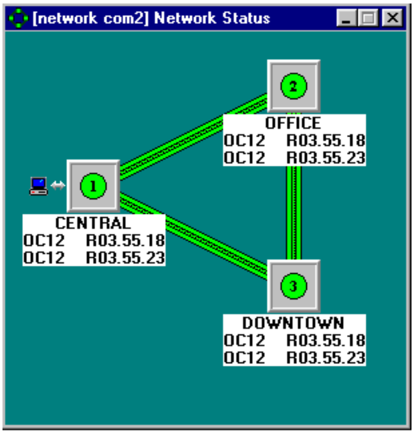
Verifying the Existing Software

Determine which version of software is currently running on the system.

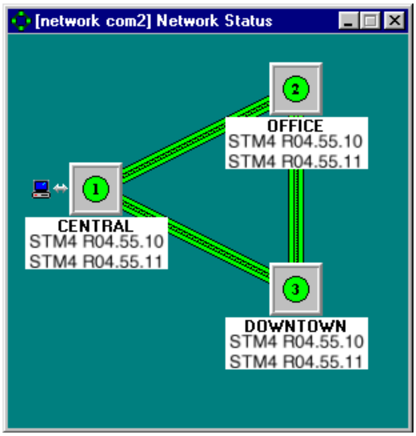
1. Log on to the OSIRIS optical multiplexer using OSIRIS-VUE software. The **Network Status** dialog box appears.
2. From the **Connect** menu, click **Preferences** and click **Network Status Display**. The **Network Status Display Control** dialog box appears.
3. Enable **Software Revision** and **Software Backup**.
4. Click **OK**. The Network Status dialog box reappears and displays the current and backup software versions

   The following are examples of typical screens:.

SONET



SDH



5. Verify that both the working and backup software are present.

   If the correct backup software version is present, proceed to "Switching the Software".

Downloading Software

If you wish to download software by connecting directly to the local node with a serial cable, follow the procedure indicated below.

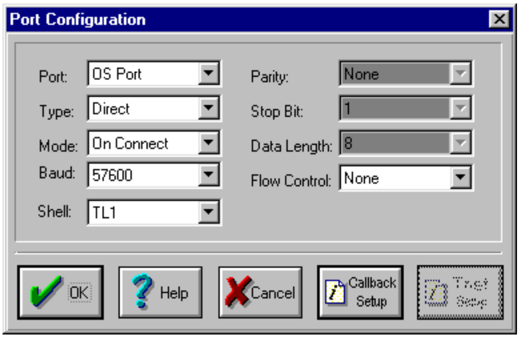
If you wish to download software using a remote connection with TFTP, proceed to "Remote Software Download".

Local Software Download

Setting Port Speed for File Download

Set the port speed to make download time as quick as possible.

1. From the Network Status dialog box, right-click the Local icon and click **Set Ports**. The **Port Configuration** dialog box appears.



2. Set **Port**, **OS Port**, or **Craft** depending on which port you are connected to.
3. Select a baud rate. A baud rate of 57600 bps is recommended.
4. Click **OK**. The Network Status dialog reappears.

   The serial port baud rate does not change while you are logged on. Perform Step 5 or 6 to reset the current port speed.

5. If you are connected to the OSIRIS shelf through the OS or Craft port, reset the currently active NE software by following the steps below.
   1. From the Network Status dialog box, double-click the Local node icon. The **Shelf-level** dialog box appears.
   2. Click **RST**. If backup NE software is present on the shelf, the **Select Software to Reset** dialog box appears; click **Current Software**.
   3. The **Please Confirm** dialog box appears.
   4. Click **This Node**. NE software reset takes 3-5 minutes.
   5. Exit OSIRIS-VUE software.

Downloading Software

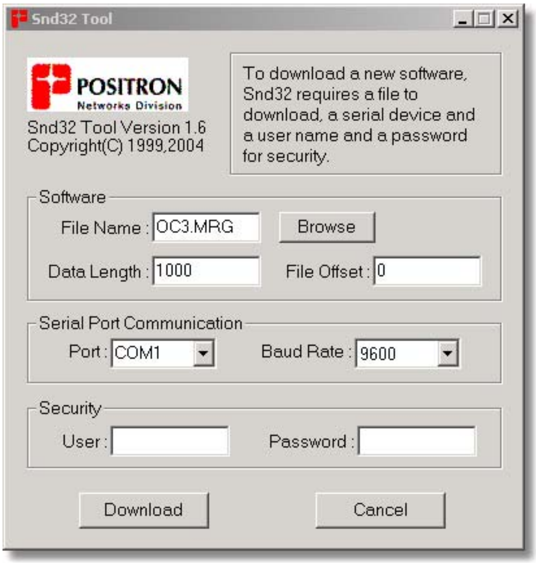
Before you download the software:

- Unzip the NE software.
- Make sure that SND32 is installed on your PC. Refer to "Possible Error Messages".
- Connect your PC to the shelf with a serial cable.

1. Start SND32. The **SND32 Tool** dialog box appears.

   Note: Make sure that any other applications using the same COM port as your PC are closed before you launch SND32.

The following is an example of a typical screen:



2. Click **Browse** to specify the file location of the NE software. The **File Open** dialog box appears.
   1. Browse for the file to be downloaded.
   2. Select the file and click **OK**. The SND32 Tool dialog box reappears.
   3. The file name appears in the **File Name** text box.

Note: The OSIRIS NE software uses the file extension *.MRG. For a OSIRIS optical multiplexer OC-3 system, NE software files for older MCU's are named OC3.MRG and for OC-12 they are OC12.MRG. For NMCU's, the files are named OC3p.MRG, OC12p.MRG and OC48p.MRG. NE software files named OC3o.MRG, OC12o.MRG and OC48o.MRG are the OSI version softwares and are only compatible with NMCU's. Make sure not to confuse *.MRG files from different versions of the NE software. Frequent upgrades may leave several versions of each *.MRG file on the hard drive of your PC.

For NE softwares version 10 and below.

If upgrading the Network from OC-3 to OC-12, the OC12.MRG and/or OC12p.MRG file must be renamed to the same as the Current OC-3 NE software presently running on the Network.

Ex: If OC-3 Network is running version 5.07.24 and will be upgraded to an OC-12 version 5.77.24, the OC12p.MRG file must be renamed to OC3p.MRG to successfully download using SND32.

The following table displays NE software filenames available for download:

MCU/ NMCU	SONET Software	Filename	SDH Software	Filename
MCU	OC-3	oc3.mrg	STM-1	stm1.mrg
NMCU	OC-3	oc3p.mrg	STM-1	stm1p.mrg
MCU	OC-12	oc12.mrg	STM-4	stm4.mrg
NMCU	OC-12	oc12p.mrg	STM-4	stm4p.mrg
NMCU	OC-48	oc48p.mrg		
NMCU	OC-3—OSI	oc3o.mrg		
NMCU	OC-12—OSI	oc12o.mrg		
NMCU	OC-48—OSI	oc48o.mrg		

3. Enter a user name and password. User name and password parameters are the same as those used to log on to the OSIRIS optical multiplexer.
4. Set **Port** to the COM port connected to the OSIRIS optical multiplexer.
5. Set the **Baud Rate**. This baud rate should be the same as that specified in the "Local Software Download". Select **Current** if you do not know the baud rate. The Current setting matches the baud rate to whatever rate was used last time you logged on to the OSIRIS optical multiplexer with OSIRIS-VUE software.
6. Enter a file offset and data length (if desired).
7. Click **Download**. The **Start Download** dialog box appears displaying estimated download time.
8. Click **Yes**. All OSIRIS optical multiplexer MCU LEDs begin to flash green. The **Download Progress** dialog box appears.

   At the end of the software download procedure, a confirmation dialog box appears.

   Refer to "Possible Error Messages" if SND32 software displays any error messages during the download procedure.
9. Click **OK**.

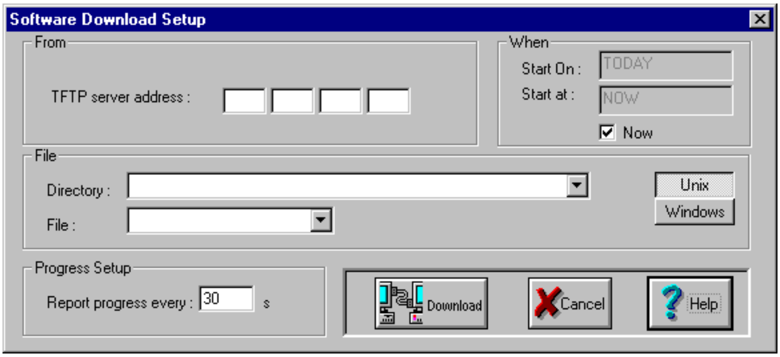
   SND32 Tool dialog box reappears. The OSIRIS optical multiplexer MCU LEDs stop flashing and remain green.
10. Click **Cancel** to close the SND32 Tool dialog box.

Remote Software Download

To upgrade all the NEs within the ring, a new software load must be transferred to one of the NEs on the ring. OSIRIS-VUE TFTP, used in both SONET and SDH configurations, allows for remote software downloads to network elements on a ring.

Follow the procedure below to download files with the **TFTP** option.

1. In the **Network Status** window right-click the local node to access the **Software Download Menu**. Alternatively, you may access the **Software Download Menu** by right-clicking on the background of the **Shelf-level** window.
2. Choose **Software Download**. The **Software Download Setup** dialog box appears.



3. Set the **TFTP server address** to the IP address of the terminal which has the software to be downloaded.
4. Ensure that the appropriate computer configuration is set: Unix or Windows.

   Note: The **Directory** is to be left blank.

   The *.MRG file must be contained within the directory that the user can access on the TFTP server.
5. Set **File** to the name of the software to download: i.e., OC-3/STM-1, OC-12/STM-4 or OC-48.

   Note: The OSIRIS optical multiplexer NE software uses the file extension *.MRG. Be sure not to confuse *.MRG files from different versions of the NE software. Frequent upgrades may leave several versions of each *.MRG file on the hard drive of your PC.

The following table displays NE software filenames available for download:

MCU/ NMCU	SONET Software	Filename	SDH Software	Filename
MCU	OC-3	oc3.mrg	STM-1	stm1.mrg
NMCU	OC-3	oc3p.mrg	STM-1	stm1p.mrg
MCU	OC-12	oc12.mrg	STM-4	stm4.mrg
NMCU	OC-12	oc12p.mrg	STM-4	stm4p.mrg
NMCU	OC-48	oc48p.mrg		
NMCU	OC-3—OSI	oc3o.mrg		
NMCU	OC-12—OSI	oc12o.mrg		
NMCU	OC-48—OSI	oc48o.mrg		

6. Set **Start on** to the date of the download in the form of YY-MM-DD.

   Set **Start at** to the time of the download in the form of 99:99.

   Check off the **Now** box if you would for the download to start immediately.

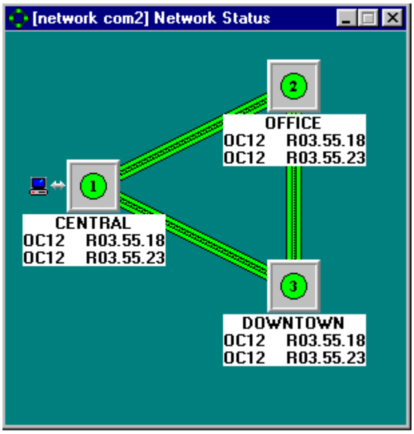
7. Click the **Download** button to start downloading the software.

Switching the Software

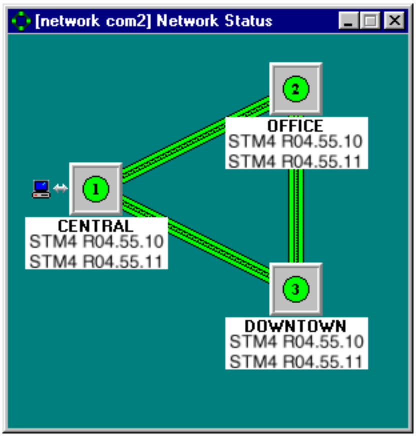
1. Start OSIRIS-VUE software and log on to the Local node.
2. Verify that the correct software version has been downloaded to the OSIRIS optical multiplexers.

   The following are examples of typical screens:

   SONET

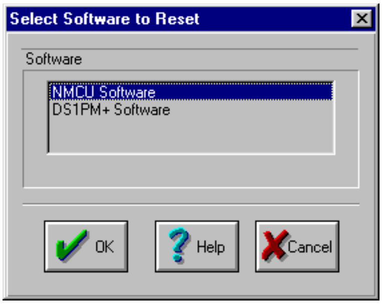


   SDH



3. Double-click the **Local** node. The **Shelf-level** dialog box appears.

4. Click **RST**. The **Select Software to Reset** dialog box appears.



5. Select **MCU Software**.
6. Click **OK**. The **Software Reset** dialog box appears.
7. Select a node.
8. Click **Alternate Software**. The **Software Change** dialog box appears.
9. Click **OK**.

   The MCU LEDs on each OSIRIS optical multiplexer turn red. These LEDs remain red for 3-5 minutes during the switch.

   Watch the LED on the MCU as the software switch is in progress. The LED changes color as the switch progresses.

Color of LED	Action
Red	Switch in progress
Green	Switch has been completed
Yellow	Verifying shelf configuration to the memory
Green	Download has been completed

   Note: At this point, you may have to wait up to 2 to 3 minutes for the software to switch. You **cannot** log on to the OSIRIS optical multiplexer before this period has expired.

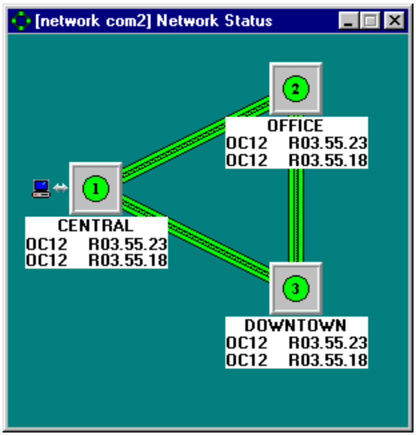
   After 3-5 minutes, the Network Status dialog box re-connects automatically.

10. Verify that the NE software has been switched.

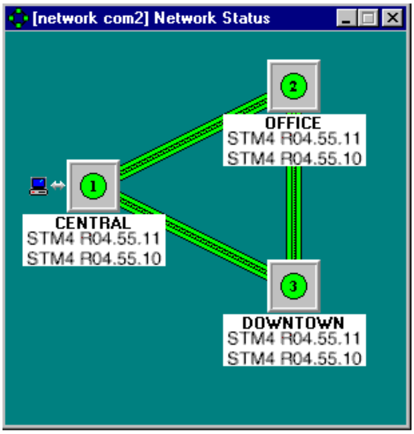
   Note: If software has not been switched on all nodes, repeat the switching procedure

The following are examples of typical screens:.

SONET



SDH



Verifying Mapper Software Compatibility

If your OSIRIS shelf contains Multi-Service Ethernet, PacketPath, EC1 TSA, or DS1PM+ mappers, you must verify that the software running on them is compatible with the newly upgraded NE software.

The following table displays the compatibility between Multi-Service Ethernet or PacketPath and NE software:

NE Software	MSE-4	PAC155	PEC4
x.x7.xx	n/a	n/a	n/a
x.x8.xx	n/a	1.1.58/1.1.48	1.1.58/ 1.1.48
x.x9.xx	n/a	1.1.69	1.1.69
x.x10.xx	n/a	1.2.9	1.2.9

NE Software	MSE-4	PAC155	PEC4
x.11.xx	n/a	1.2.9	1.2.9
x.12.xx	1.1.8	1.2.9	1.2.9
x.14.xx	1.3.1	1.2.9	1.2.9

To verify or upgrade the software, see the following release notes:

- *PacketPath Fractional Ethernet Access Card (202-037)*
- *PacketPath ATM Access Card (202-040)*

OSIRIS release 10 is compatible with EC1 TSA software version 1.1.12 and DS1PM+ version 1.1.16.

OAU Upgrade Procedures

To increase your network capacity, you may upgrade your OSIRIS network from:

- OC-3/STM-1 to OC-12/STM-4
- OC-3 to OC-48
- OC-12 to OC-48

Note: Please keep in mind that upgrades from **OC-3/OC-12 to OC-48** can only be performed for **SONET networks**.

For these procedures, you must upgrade all OAUs as well as the NE software on each network element. For upgrade to OC-48 OAUs, you must also be running NMCU version 800307/2 (SONET) or 800309/2 (SDH).

The OAU upgrade procedure applies to upgrades from OC-3 to OC-12, OC-12 to OC-48, and from OC-3 to OC-48.

- Before you begin
- Downloading the software
- Switching the software
- Upgrading OAU-Bs
- Testing traffic on fiber B
- Upgrading OAU-As
- Testing traffic on Fiber A
- Verifying software switch

Note: This procedure is non-service affecting.

Before You Begin

Forced switches during OAU replacement are **not** supported for EC-1 VT mappers. For part of this procedure, traffic switching must be performed by removing an OAU from all shelves containing the EC-1 VT mapper simultaneously. Removing an OAU causes traffic to switch to the opposite fiber (automatic protection switching). For more information, see "Switching to Fiber B".

CAUTION

Failure to remove the OAU in the shelf containing the EC-1 VT mapper may be service affecting if a forced switch is attempted.

Downloading The Software

Downloading new NE software consists of the following procedures:

- Verifying existing software
- Downloading new software

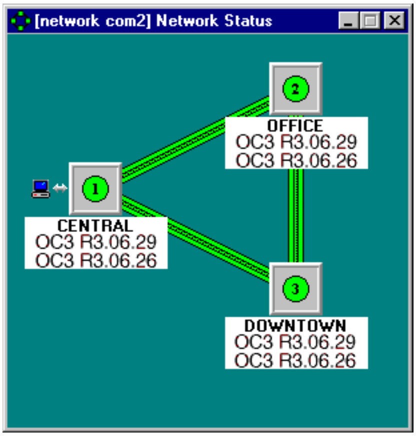
Verifying Existing Software

To determine the software version that is currently running, perform the following steps:

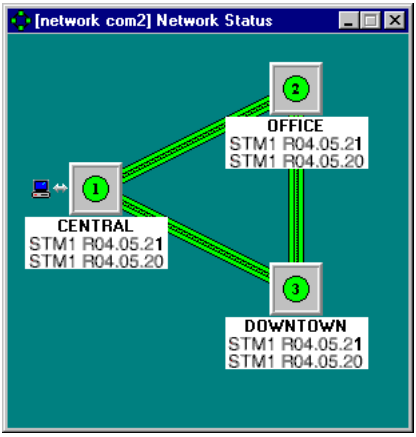
1. Log on to the OSIRIS optical multiplexer using OSIRIS-VUE software. The **Network Status** dialog box appears.
2. From the **Connect** menu, click **Preferences** and click **Network Status Display**. The **Network Status Display Control** dialog box appears.
3. Enable **Software Revision** and **Software Backup**.
4. Click **OK**. The Network Status dialog box reappears and displays the current and backup software versions

The following are examples of typical screens:.

SONET



SDH



5. Verify that both the working and backup software are present.

   If the correct backup software version is present, proceed to the next section on Switching the Software.

Downloading New Software

For instructions detailing the downloading procedure, please refer to "Remote Software Download".

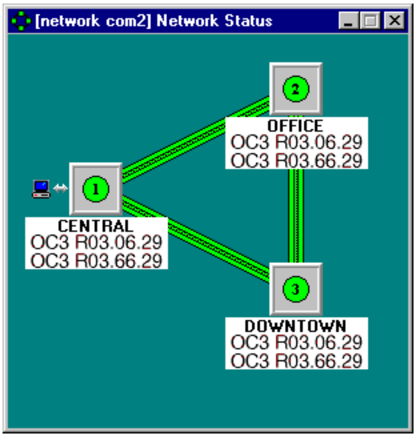
Switching The Software

To switch the software, perform the following steps:

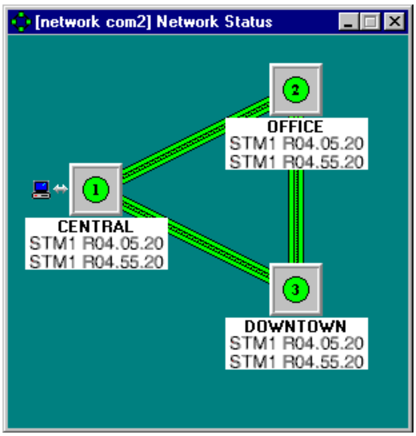
1. Start OSIRIS-VUE software and log onto the Local node. Remember to set the port speed to the same speed set in "Downloading The Software".
2. Update the network to ensure the latest software versions appear. Right-click the Network Status dialog box and click **Update Network**.
3. Verify that the correct software version has been downloaded to the OSIRIS optical multiplexers

   The following are examples of typical screens for OC-3 and OC-12 upgrades:

SONET

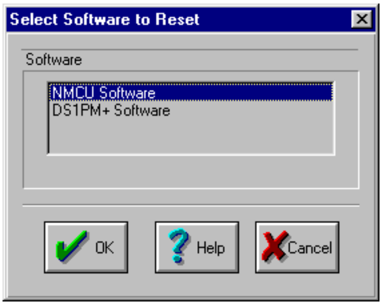


SDH



Note: The new software appears, although the revision number is correct. At this point, the OC-3/STM-1 ring does not recognize the new software. When software is switched, it appears as the higher capacity OC-12/STM-4.

4. Double-click the Local node. The **Shelf-level** dialog box appears.
5. Click **RST**. The **Select Software to Reset** dialog box appears.



6. Select **MCU Software**.
7. Click **OK**. The **Software Reset** dialog box appears.

   Note: This procedure assumes that software was downloaded correctly to all shelves in the ring. In this case, **all** shelves contain the same backup software version.

8. Click **Alternate Software**. The **Software Change** dialog box appears.
9. Click **OK**.

CAUTION

DCC traffic will be disrupted for several minutes while the initialization process is in effect. Rebooting the system will not affect customer traffic on the network.

The MCU LEDs on each OSIRIS optical multiplexer turn red. These LEDs remain red for several minutes during the switch.

Watch the LED on the MCU as the software switch is in progress. The LED changes color as the switch progresses.

Color of LED	Action
Red	Switch in progress
Green	Switch has been completed
Yellow	Verifying shelf configuration to the memory
Green	Download has been completed

Note: At this point, you may have to wait up to 2 to 3 minutes for the software to switch. You **cannot** log on to the OSIRIS optical multiplexer before this period has expired.

10. After 2 to 3 minutes, you are logged off the OSIRIS network and will be re-connected automatically.

When the Network Status dialog box re-connects, Card Mismatch alarms (CRDMISMAT) appear for all OAUs. Minor DCC-X and DCC-Y alarms still appear. These card mismatch alarms do not affect service.

At this point, if an OAU is removed and re-inserted or there is a power loss, the OAUs are not reprogrammed and lose ability to carry traffic.

Upgrading OAU-Bs

To upgrade OAU-B, perform the appropriate following procedure:

- Upgrading OAUs in a shelf without BIUs
- Upgrading OAUs in a shelf containing BIUs

Upgrading OAUs in a Shelf Without BIUs

1. To avoid electrostatic discharge that may damage a plug-in unit or the shelf, ensure that you are properly grounded to the shelf using an ESD device.
2. Remove the OAU from the OAU-B slot and disconnect optical fibers.

WARNING

Do not remove the optical caps from the OAUs. Invisible laser radiation may be present in operational OAUs, which may cause blindness.

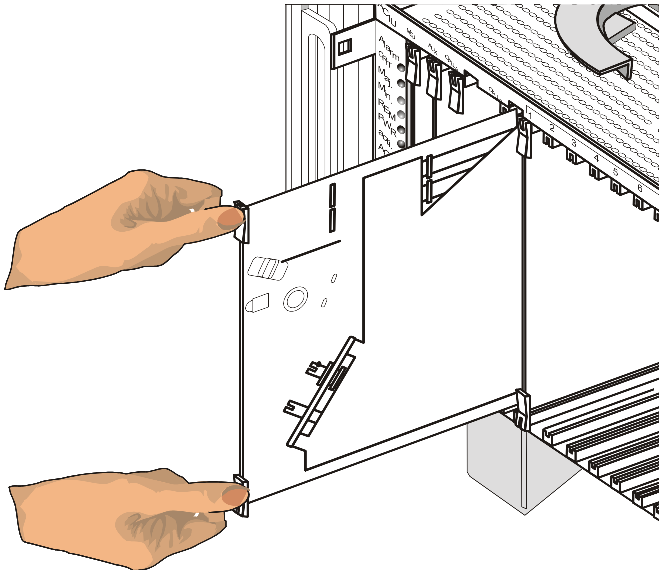
Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

ALL Network traffic will be switched automatically to Fiber path A and a card removed (CRDRMVD) alarm appears for the OAU.

3. Remove the new OAU from its antistatic bag.
4. Grip the new OAU by its two extractor levers, hold it vertically so that the components face to the right, and slide it into the OAU-B slot, making sure that the OAU edges slide through the tracks in the shelf.
5. Connect optical fibers.
6. When the OAU reaches the back of the shelf, push it into place so that the edge-connectors on the OAU fit firmly into the backplane connector. Refer to Figure 17.

7. Once you have installed the plug-in unit, check to see that the LED illuminates green. The LED illuminates green if the OAU has been installed correctly. The OAU card removed (CRDRMVD) alarm disappears. Minor alarms also disappear for DCC-X and DCC-Y.

Figure 17 Installing an OAU



8. Repeat Steps 1 to 7 for remaining OAU-Bs in the OSIRIS ring.
    - **SONET—**In the new OC-N system, the number of STS paths which were previously available are provisioned the same way. (e.g., STS1-1 to STS1-3 are provisioned the same way as in the OC-3 system) Additional capacity is configured as ASYNC by default.
    - **SDH—**In the new STM-4 system, the number of TUG paths which were previously available are provisioned in the same way. (e.g., TUG3-1 to TUG3-3 are provisioned the same way as in the STM-1 system) Additional capacity is configured as TU12 by default.

Upgrading OAUs in a Shelf Containing BIUs

1. To avoid electrostatic discharge that may damage a plug-in unit or the shelf, ensure that you are properly grounded to the shelf using an ESD device.
2. Remove the BIU (B side only). A card removed (CRDRMVD) alarm appears for the BIU.
3. Remove the OAU from the OAU-B slot and disconnect optical fibers.

WARNING

Do not remove the optical caps from the OAUs. Invisible laser radiation may be present in operational OAUs, which may cause blindness.

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

ALL Network traffic will be switched automatically to Fiber path A and a card removed (CRDRMVD) alarm appears for the OAU.

4. Remove the OAU/BIU from its antistatic bag.

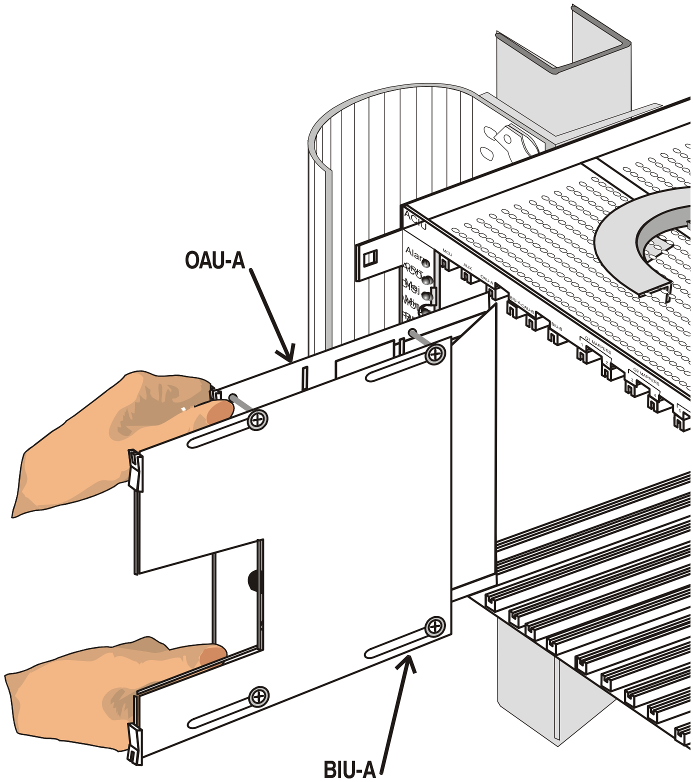
The STM-4/OC-12 and OC-48 systems support an OAU which is mechanically coupled with a BIU, via a slider system, connected directly to the backplane connector.

Refer to Figure 18 as you perform this OAU/BIU installation procedure:

Note: Insert the OAU before inserting the BIU.

5. Grip the OAU/BIU by its extractor levers, hold it vertically so that the components face to the right, and slide the OAU first and then the BIU into their respective slots, making sure that the OAU/BIU edges slide through the tracks in the shelf.

Figure 18 Installing a coupled OAU/BIU



6. Connect optical fibers.
7. Once you have installed the plug-in unit, check to see that the LED illuminates green. The LED illuminates green if the OAU has been installed correctly. OAU and BIU card removed (CRDRMVD) alarms disappear. Minor alarms also disappear for DCC-X and DCC-Y.

8. Repeat Steps 1 to 8 for remaining OAU-Bs in the OSIRIS ring.
   - **SONET**—In the new OC-N system, the number of STS paths which were previously available are provisioned the same way. (e.g., STS1-1 to STS1-3 are provisioned the same way as in the OC-3 system) Additional capacity is configured as ASYNC by default.
   - **SDH**—In the new STM-4 system, the number of TUG paths which were previously available are provisioned in the same way. (e.g., TUG3-1 to TUG3-3 are provisioned the same way as in the STM-1 system) Additional capacity is configured as TU12 by default.

Testing Traffic on Fiber B

You must now test the network traffic on fiber B.

1. Provision a Point-to-Point cross-connection on one node in the OSIRIS network.

   Note: You only have to provision one Point-to-Point cross-connection for this continuity test. Continuity testing is performed without dropping the signal at the far end of the network. Network traffic circulates back to this location.

2. Double-click the shelf icon with the test cross-connection you provisioned. The **Shelf-level** dialog box appears.
3. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
4. Double-click the mapper carrying the test signal. The **Mapper-level** dialog box appears.
5. Double-click the cross-connected channel. The **Channel-level** dialog box appears.
6. Click the **PPS** tab.
7. Force traffic on fiber B.

   A confirmation dialog box appears.

8. Click **Yes**.
9. Verify that no bit errors appear in your test traffic.

   Once you have verified that test traffic flows error-free on fiber B deprovision the test cross-connection.

Upgrading OAU-As

To upgrade OAU-A, perform the appropriate following procedure:

- Upgrading OAUs in a shelf without BIUs
- Upgrading OAUs in a shelf containing BIUs

Upgrading OAUs in a Shelf Without BIUs

1. To avoid electrostatic discharge that may damage a plug-in unit or the shelf, ensure that you are properly grounded to the shelf using an ESD device.
2. Remove the OAU from the OAU-A slot and disconnect optical fibers.

WARNING

Do not remove the optical caps from the OAUs. Invisible laser radiation may be present in operational OAUs, which may cause blindness.

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

A card removed (CRDRMVD) alarm appears for the OAU.

3. Remove the OAU from its antistatic bag.
4. Grip the OAU by its two extractor levers, hold it vertically so that the components face to the right, and slide it into the OAU-A slot, making sure that the OAU edges slide through the tracks in the shelf.
5. Connect optical fibers.
6. When the OAU reaches the back of the shelf, push it into place so that the edge-connectors on the OAU fit firmly into the backplane connector. Refer to Figure 17.
7. Once you have installed the plug-in unit, check to see that the LED illuminates green. The LED illuminates green if the OAU has been installed correctly. The OAU card removed (CRDRMVD) alarm disappears. Minor alarms also appear for DCC-X and DCC-Y.
8. Repeat Steps 1 to 7 for remaining OAU-As in the OSIRIS ring.
   - **SONET—**In the new OC-x system, the number of STS paths which were previously available are provisioned the same way. (e.g., STS1-1 to STS1-3 are provisioned the same way as in the OC-3 system) Additional capacity is configured as ASYNC by default.
   - **SDH—**In the new STM-4 system, the number of TUG paths which were previously available are provisioned in the same way. (e.g., TUG3-1 to TUG3-3 are provisioned the same way as in the STM-1 system) Additional capacity is configured as TU12 by default.

Upgrading OAUs in a Shelf Containing BIUs

1. To avoid electrostatic discharge that may damage a plug-in unit or the shelf, ensure that you are properly grounded to the shelf using an ESD device.
2. Remove the BIU (A side only). A card removed (CRDRMVD) alarm appears for the BIU.
3. Remove the OAU from the OAU-A slot and disconnect optical fibers.

WARNING

Do not remove the optical caps from the OAUs. Invisible laser radiation may be present in operational OAUs, which may cause blindness.

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

A card removed (CRDRMVD) alarm appears for the OAU.

4. Remove the OAU/BIU from its antistatic bag.

   The STM-4/OC-12 and OC-48 systems support an OAU which is mechanically coupled with a BIU, via a slider system, connected directly to the backplane connector.

   Refer to Figure 18 as you perform this OAU/BIU installation procedure:

   Note: Install the OAU before installing the BIU.
5. Grip the OAU/BIU by its extractor levers, hold it vertically so that the components face to the right, and slide the OAU first and then the BIU into their respective slots making sure that the OAU/BIU edges slide through the tracks in the shelf.
6. Connect optical fibers.
7. Once you have installed the plug-in unit, check to see that the LED illuminates green. The LED illuminates green if the OAU has been installed correctly. OAU and BIU card removed (CRDRMVD) alarms disappear. Minor alarms also disappear for DCC-X and DCC-Y.
8. Repeat Steps 1 to 8 for remaining OAU-As in the OSIRIS ring.
   - **SONET**—In the new OC-N system, the number of STS paths which were previously available are provisioned the same way. (e.g., STS1-1 to STS1-3 are provisioned the same way as in the OC-3 system) Additional capacity is configured as ASYNC by default.
   - **SDH**—In the new STM-4 system, the number of TUG paths which were previously available are provisioned in the same way. (e.g., TUG3-1 to TUG3-3 are provisioned the same way as in the STM-1 system) Additional capacity is configured as TU12 by default.

   At this point, the ring should be free of OAU card mismatch (CRDMISMAT), card removed (CRDRMVD), and DCC alarms.

Testing Traffic on Fiber A

You must now test the network traffic on fiber A.

1. Provision a Point-to-Point cross-connection on one node in the OSIRIS network.

   Note: You only have to provision one Point-to-Point cross-connection for this continuity test. Continuity testing is performed without dropping the signal at the far end of the network. Network traffic circulates back to this location.

2. Double-click the shelf icon with the test cross-connection you provisioned. The **Shelf-level** dialog box appears.
3. Right-click a node, then click **Maintenance Path Switching**. Make sure that **Switching Reported** is enabled. Repeat this step for each node in the network.
4. Double-click the mapper carrying the test signal. The **Mapper-level** dialog box appears.
5. Double-click the cross-connected channel. The **Channel-level** dialog box appears.
6. Click the **PPS** tab.
7. Force traffic on fiber A.

   A confirmation dialog box appears.

8. Click **Yes**.
9. Verify that no bit errors appear in your test traffic.

   Once you have verified that test traffic flows error-free on fiber A deprovision the test cross-connection.

   The upgrade procedure is complete.

Mixed NE Software in OSIRIS Rings

Different versions of NE software can be installed on some shelves in an OSIRIS network. This situation may occur if you have different MCU versions in the same network. For example, an older version of an MCU may operate one version of NE software, but one shelf in a ring contains a Network MCU operating the latest software version.

Note: Mixed NE software versions must be of the same protocol. E.g., you cannot mix SONET and SDH software on the same OSIRIS ring.

Adding an NMCU to an Existing Ring

Follow these steps to add a Network MCU to a ring that uses older MCU cards (800300 or 800302 only).

1. If any 800301 MCU cards are used in the ring, you must replace these MCUs with 800300 or 800302 MCUs.
2. Upgrade the software on all 800300 and 800302 MCUs to 3.6.*nn*.
3. Select the network element(s) that will provide a LAN entry point to the ring.
4. Replace the MCU on the selected network element(s) with a Network MCU. The NMCU must be running software version 5.6.*nn*.

Software Download in a Mixed Ring

Use the SND32 utility to download new software to an OSIRIS ring. The two different versions of software (Network MCU and regular MCU) must be downloaded into the ring separately. Each NE in the ring accepts the appropriate software. The download procedure can be initiated from any node.

Possible Error Messages

During the download procedure, the following error messages may appear.

Login Stopped

This message appears when you click the Cancel button during the login sequence.

Login Failed

This message appears when the OSIRIS optical multiplexer does not recognize the password or does not respond after SND32 sends the login parameter. This message most frequently occurs when the baud rate is incorrect.

Activate Software Download Failed

This message appears when SND32 receives a deny or no signal from the MCU software after sending the activate software download command.

Download Stopped

This message appears when you click Cancel.

Fatal Error Transferring Data

This message appears when there is a serial interface error during the software download.

Fail Waiting for Confirmation

This message appears when there is a serial interface error while waiting for software download confirmation.

Error Sending Final ACK

This message appears when there is a serial interface error while waiting for final ACK command to the OSIRIS optical multiplexer.

Result message

This message appears when the software download is complete.

Chapter 5

Data Applications

This chapter contains a general overview of Ethernet applications, followed by instructions on how to provision a transparent LAN, carry ATM traffic and optimize bandwidth usage.

Specifically, how do I:

- Create a transparent LAN using Ethernet and Fast Ethernet products
- Create a transparent LAN over other vendors' equipment
- Carry ATM traffic over OSIRIS networks
- Double bandwidth for datacom (LAN) applications

Ethernet Overview

This Ethernet overview is designed for beginner and intermediate readers. It gives some background on data communications and networking, particularly Ethernet networks.

Basic System Elements

Ethernet systems consist of four basic elements:

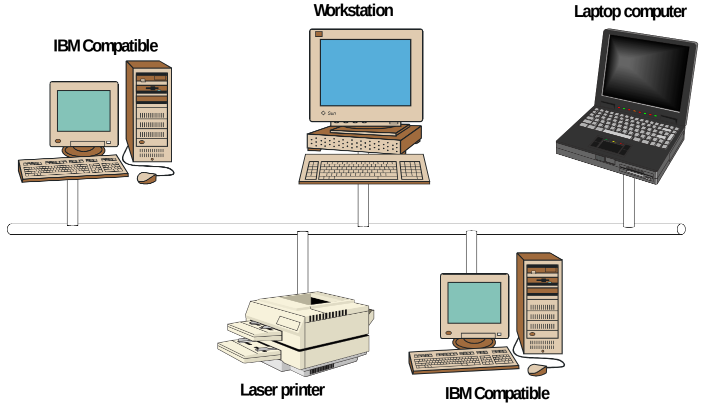
- The physical medium—the physical medium is the carrier that delivers signals between two Ethernet Interfaces (e.g., copper wire or fiber).
- The Medium Access Control (MAC) rules set—rules set that lets multiple Ethernet Interfaces control how Ethernet network bandwidth is shared.
- The Ethernet frame—the Ethernet frame is the actual network message.
- The Ethernet MAC Address—the MAC address is a unique 48 bits identifier administered by the IEEE Organization. Usually for every Ethernet frame, a Destination and Source MAC Address is defined. This address is also known as the physical address or hardware address. Unique MAC Addresses are pre-assigned to each physical network device during manufacturing.

Ethernet Topology

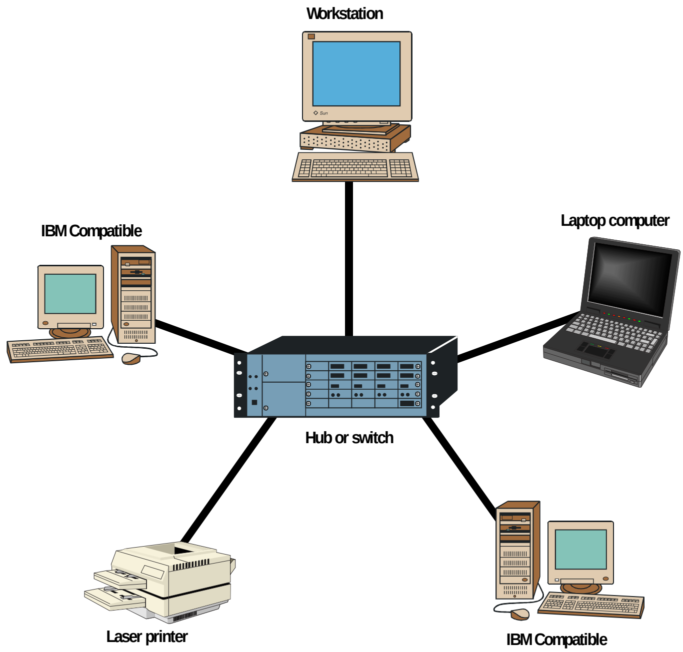
The Ethernet standard offers two different topologies:

- Bus topology
- Star topology

Bus Topology



Star Topology



Bus Topology Networks

The bus network topology was first used because networks were small and network traffic was very low. The positive aspect of this topology was that no external interconnection devices such as hubs or switches were required. As network traffic increased, the bus topology has virtually disappeared.

The bus topology operates over RJ58 Coaxial cables and uses standardized BNC connectors. This configuration also requires terminators (75 ohms resistor) at each end of the bus for line terminations.

Star Topology Networks

With the constant increase in network users and the growing importance of signal quality, the more flexible Star topology has quickly replaced the Bus topology for Ethernet applications.

The star topology requires an External Interconnection Device (EID) such as a Hub or Switch, allowing all connected devices to share the same network.

The star topology applies to 10 Base T, 100 Base TX/FX and the newer Gigabit Ethernet.

A major advantage of the star topology over bus topology is that if any point on the LAN is disconnected, the entire LAN still functions. In a bus topology, disconnecting any point on the LAN without terminating the wire properly causes the LAN to fail.

For more information, refer to "Switches and Hubs" on page 36.

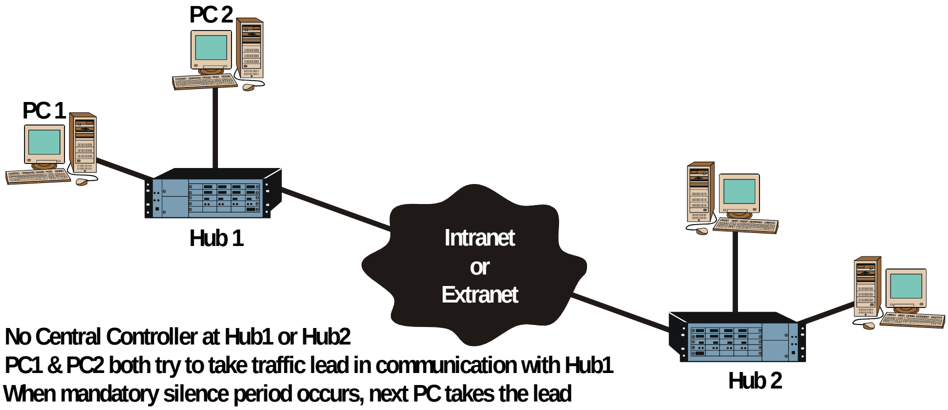
Representing over 80% of all deployed networks world-wide, the star configuration operates over 2 different types of media: copper and optical fiber. Ethernet supports 10BaseT and 100Base TX over twisted pair CAT 5 cable using standardized RJ45 connectors. GigaBit Ethernet is also expected over copper in the near future. However, optical fiber supports 10/100/1000 Base FX/FL physical interfaces.

Shared Signalling

Ethernet equipped devices (e.g., PCs, switches, and routers) are attached to a shared signaling system with no central controller or mediator. Each device operates independently of other network equipment and attempts to transmit traffic when needed.

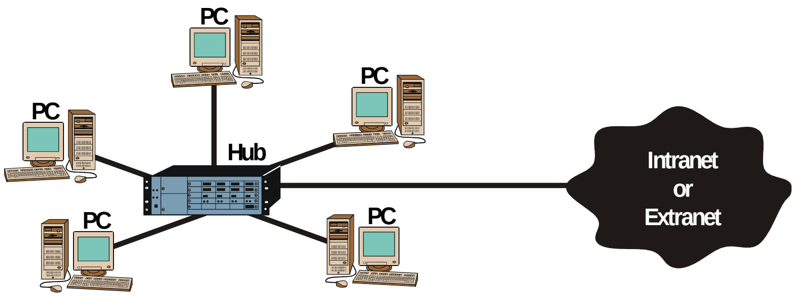
Ethernet frames are transmitted serially to all network equipment. The sending interface transmits data in the form of an Ethernet frame once there is a break in network traffic.

Note: A *Preamble* sequence is transmitted before every Ethernet packet. This sequence is formed with 1,0 (31 times) followed by 1,1 and synchronizes method transmitted frames. Finally, Ethernet packets are followed by a mandatory silence period (960 ns for Fast Ethernet, 9.6 microseconds for Ethernet). This silence period gives a chance for other users to send frames.



- No Central Controller at Hub1 or Hub2
- PC1 & PC2 both try to take traffic lead in communication with Hub1
- When mandatory silence period occurs, next PC takes the lead
- Hub1 & Hub2 also share signalling when communicating with the Intranet

No single station can lock out or overflow other network equipment because of the mandatory silence period. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface on all network equipment. This mechanism is based on a system called CSMA/CD (Carrier Sense Multiple Access with Collision Detection).



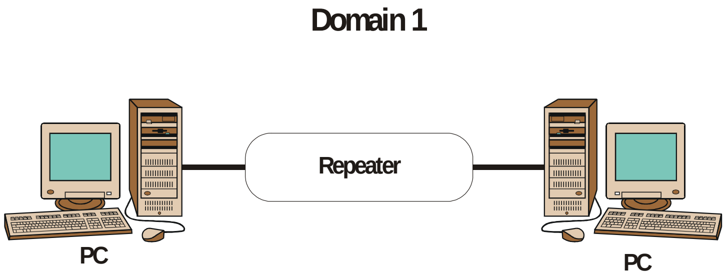
- All devices cannot transmit at once
- Every device must listen for quiet
- When a space occurs, every device has an equal chance to transmit (Multiple Access).
- If two devices start at the same time, they stop (Collision Detection).

Example

CSMA/CD can be compared to the protocol of speaking and listening by 25 people in a conference room. Each person must listen for a period of quiet before speaking (Carrier Sense). Once a space occurs, each person has an equal chance to say something (Multiple Access). If two people start talking at the same time, they detect this and stop speaking (Collision Detection).

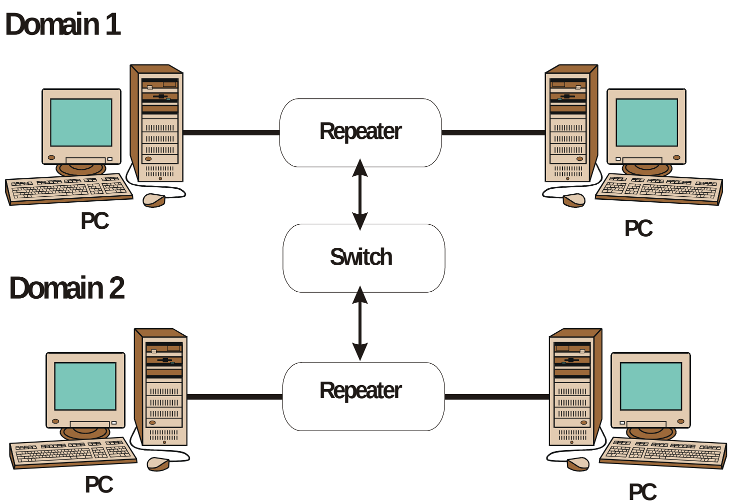
Collision Domains

A collision domain is a group of Ethernet or Fast Ethernet devices that are directly connected by repeaters. Only one device may transmit at any one time inside a collision domain (half-duplex). When a device is transmitting all other devices in the collision domain listen. As the number of network devices in a collision domain increases so does the likelihood of traffic collisions.



- Repeater is a conduit for traffic
- Repeater operates at level lower than MAC address
- Adding more PCs increases likelihood of collision

To improve network efficiency, an Ethernet network may include switches and routers as well as repeaters. Adding a switch or router adds another collision domain. Switches and routers let separate collision domains communicate with each other. Adding collision domains lowers the likelihood of traffic collisions.

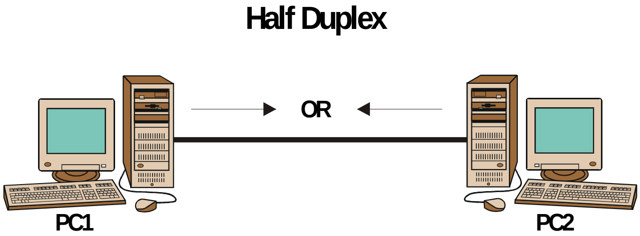


- Adding Switch or Router increases Collision Domains
- More Collision Domains decreases likelihood of traffic collisions

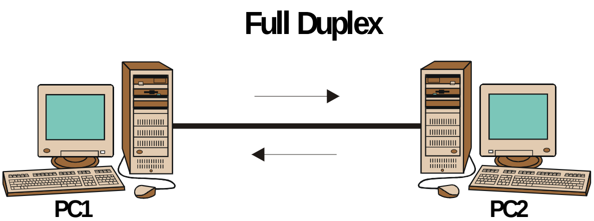
Collision Detection

Traffic collisions occur in the Collision Domain, located between two Half Duplex interfaces. Half Duplex implies that the Ethernet interface can not talk and listen at the same time (i.e., traffic is not bi-directional).

For example, if two Half Duplex Network Interface cards are connected back to back (two computers connected together through their network cards), both PCs can only send a frame or be waiting for one to arrive. In this case, the first PC sends a frame and the second must listen. If both transmit at the same time, traffic collision occurs. In the case of collision, traffic is retransmitted at a later time.



Full Duplex interfaces can send data and be waiting for incoming data. The amount of Full Duplex equipment in the field is increasing rapidly. Virtually all network interface cards and Ethernet switches sold since 1995 support Half or Full Duplex operation. However, Ethernet Hubs support only Half Duplex Ethernet interfaces. Unfortunately this promotes conditions for frequent traffic collisions.



New requirements for voice and data have lead to the terms Quality of Service (QoS) and Class of Service (CoS). Some applications (e.g., voice and video) require a minimum basic quality or class of services. These issues are not currently addressed under a shared environment. Further deployment of Intelligent Switched networks and Full Duplex interfaces may lessen this problem.

Switches and Hubs

This section compares switches and hubs.

Hubs

An Ethernet Hub acts as a concentrator or network repeater. In this application, every network device sends messages to all other devices on the same network. Only the destinations recognizing that the message is intended for them accept this network traffic. In this application, Ethernet hubs act as a network repeater.

For more information, refer to "Shared Signalling" on page 32.

Hub Limitations

An Ethernet hub provides no added value to network services (e.g., no routing, bridging, Virtual LANs, address or protocol). Further hubs only transfer traffic from devices of the same speed: 10 or 100 Mbps (Half Duplex), not both.

Ethernet Switches

Ethernet Switches are more intelligent than hubs. Switches can:

- Store packets
- Verify if packets are valid, saving bandwidth
- Transmit packets only to the correct port
- Bridge Ethernet traffic
- Support virtual LANs
- Support traffic filtering
- Support spanning trees
- Maintain class and quality of service

Switches can simultaneously accept Half and/or Full Duplex interfaces of different speeds (i.e., 10 and/or 100 and/or 1000 Mbps). Some Ethernet switches also support non-native protocols such as ATM, FDDI and offer corresponding Network interfaces (e.g., DS3/E3 and OC3c/STM-1).

Switches isolate all devices from each other and act as a mediator. Switches listen to all incoming Ethernet frames and redirect frames to the defined location.

Switches are able to allocate parallel and independent sub-channels. Traffic collisions are still possible:

- If two devices on the same collision domain send packets at the same time
- If the switch sends a packet at the same time as a station on that collision domain,

however mechanisms exist to handle this situation: CSMA/CD is performed between linked traffic ends.

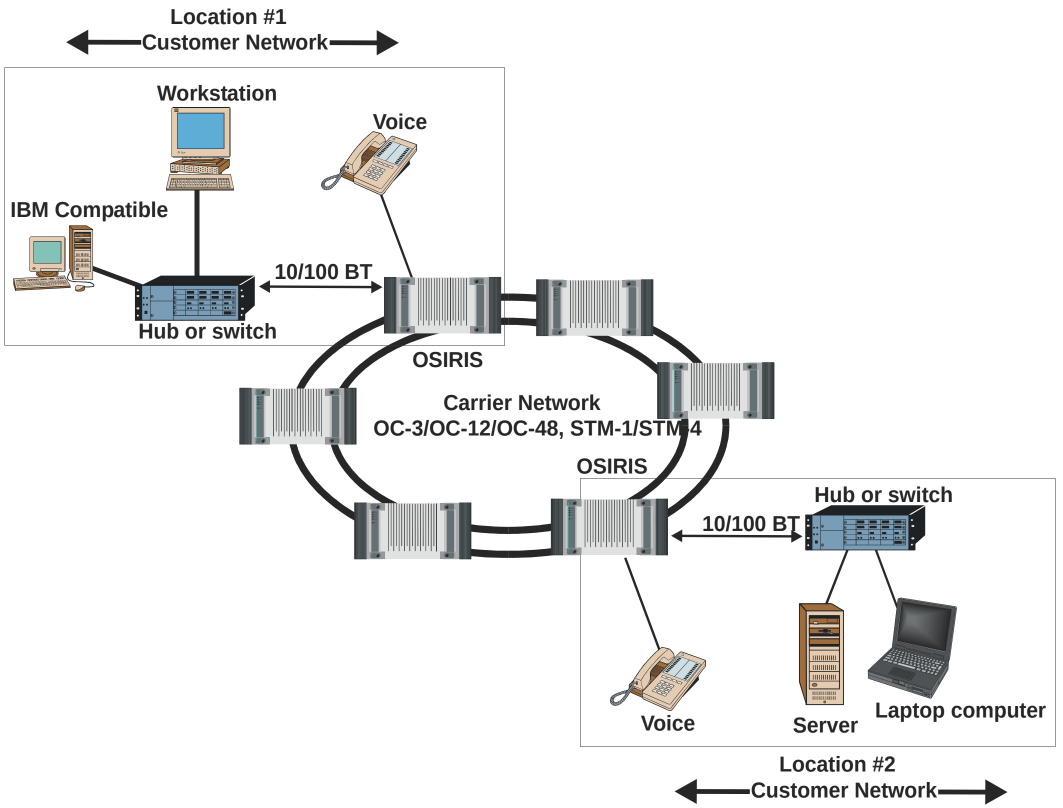
Ethernet switches process all incoming messages with either of these methods:

- **Store and forward**—switches store frames and retransmit them after all frames in the message have been received.
- **Cut-through**—switches start forwarding frames as soon as they arrive.

Transparent LAN using Ethernet and Fast Ethernet Mappers

LAN traffic can be carried transparently over a SONET/SDH backbone consisting of Positron and other vendors' equipment. A virtual-LAN is provisioned on a reserved portion of the fiber-optic bandwidth. Wide Area Networks (WANs) are often provisioned using a transparent LAN topology.

Variable bandwidth is available through Ethernet and Fast Ethernet mappers. These products give you flexible and upgradeable transparent LAN capacity. Refer to "Ethernet 10 Mbps (Half Duplex)" on page 40 and "Fast Ethernet 50/100 Mbps (Full Duplex)" on page 40. Transparent LAN applications may also be performed using the DS3/OC3c, E3/STM-1 mappers.

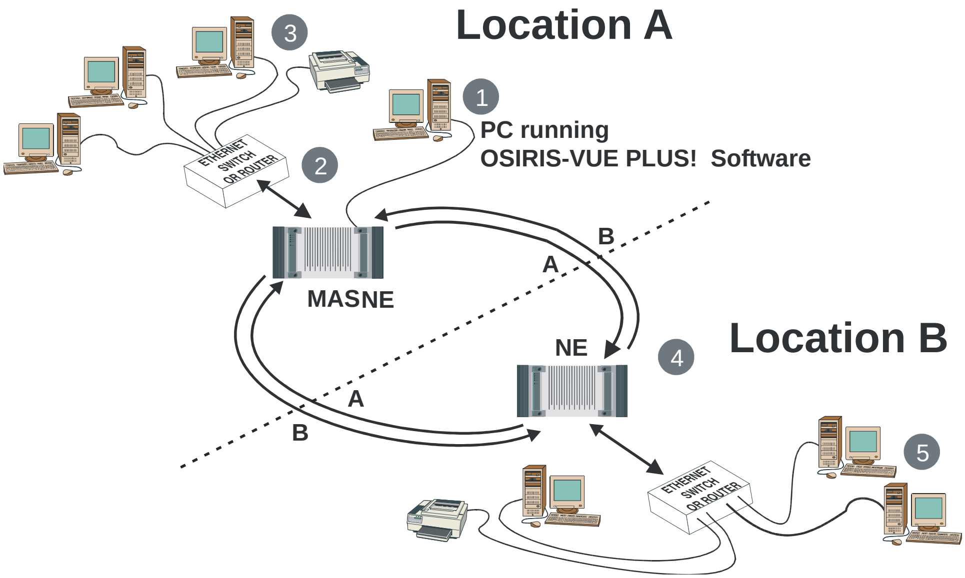


The major benefits of transparent LAN services are as follows:

- Fast point-to-point direct 10/100 BT Ethernet connectivity across UPSR SONET/SDH rings
- No need for 2 different infrastructures: voice and Ethernet data can travel on the same SONET/SDH based infrastructure
- LAN protocol transparency, low latency
- Common provisioning and management systems for LAN and SONET/SDH transport
- No special staff training: Ethernet provisioning is identical to DS1/E1, DS3/E3
- Direct integration with TL1-based embedded OS systems
- All management data is carried in SONET/SDH overhead via the DCC

Application

This figure displays traffic travelling over a transparent LAN via an OSIRIS optical multiplexer backbone.



1. Number 1 represents the PC operating OSIRIS-VUE software. The PC is connected to a shelf via a standard shelf connection and performs all provisioning and management procedures. The user logs on using an OSIRIS **Online** connection. Refer to *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)* for log on instructions.

2. The PC connects to a shelf at Number 2. The PC at Number 1 is used to provision a Point to Point cross-connection on STS1-1/TUG3-1 and STS1-2/TUG3-2 of the network bandwidth. Bi-directional traffic enters the ring and travels clockwise on fiber A and counter-clockwise on fiber B to Location B. Bi-directional traffic drops at Location 2.
3. Bi-directional LAN traffic is sent and received by the LAN Network number 3. This traffic enters and drops from the OSIRIS network at Number 2 through the Ethernet mapper installed in the shelf.
4. Bi-directional traffic drops at Number 4 received from Location A on STS1-1/TUG3-1 and STS1-2/TUG3-2 of the bandwidth.
5. Bi-directional LAN traffic is sent and received by the LAN Network Number 5. This traffic enters and exits the OSIRIS network at Number 4 through the Ethernet mapper installed in the shelf.

Ethernet 10 Mbps (Half Duplex)

The Ethernet mapper provides a physical link between two Ethernet LANs or devices via a SONET/SDH backbone. The Ethernet mapper eliminates other types of equipment that used to be necessary such as CSU/DSUs, inverse multiplexers and other equipment.

The Ethernet mapper is used primarily for the following applications:

- Native LAN service over the same infrastructure, such as voice circuits over SONET networks
- Internet service provisioning

The 10 MB Ethernet mapper integrates voice, video and data services. This mapper fits into all OSIRIS shelves and supports full UPSR path protection architecture.

The 10 MB Ethernet mapper also supports bandwidth reuse for shared bandwidth applications.

Fast Ethernet 50/100 Mbps (Full Duplex)

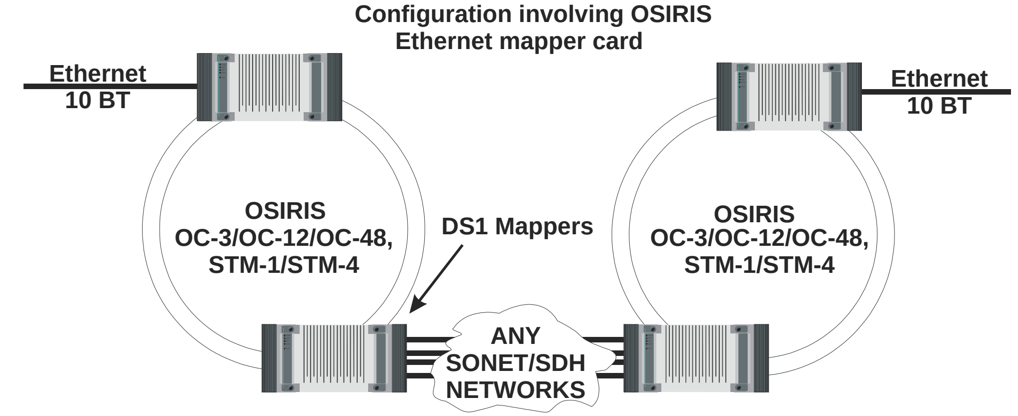
The Fast Ethernet mapper provides a physical link between two Ethernet LANs or devices via a SONET backbone.

The Fast Ethernet mapper is used primarily for the following applications:

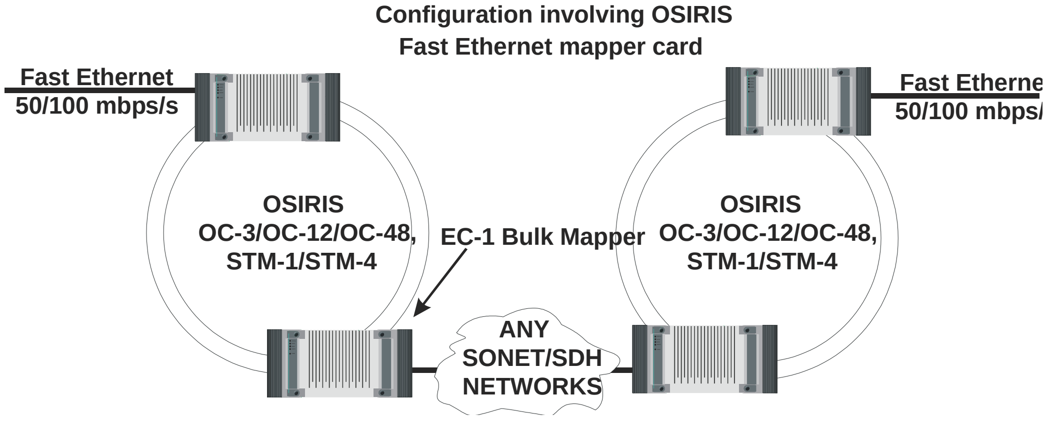
- Native LAN or Internet service
- 50/100 Mbps Ethernet for customers with several locations

Carrying LAN Traffic Over Other Vendors Equipment

This section describes how Ethernet or Fast Ethernet traffic is passed end-to-end through two SONET/SDH backbone networks: an OSIRIS network, and another other vendors network



To join two head end systems across other SONET/SDH networks, a connection of clear channel DS1s (VT1.5), E1 (TU12) or EC-1 BULK/STM-1 mappers can be used. Ethernet traffic is carried transparently over a portion of bandwidth on the SONET/SDH backbone network. These networks are transparent to the end user.



Carrying ATM Traffic Over OSIRIS Networks

OSIRIS optical multiplexer OC3c/STM-1 or DS3/E3 mappers let you provision ATM traffic across SONET/SDH rings. This enables ATM delivery, as well as standard DS1/E1, DS3/E3, Ethernet and Fast Ethernet using the same delivery vehicle.

Benefits of carrying ATM traffic over a SONET/SDH network include:

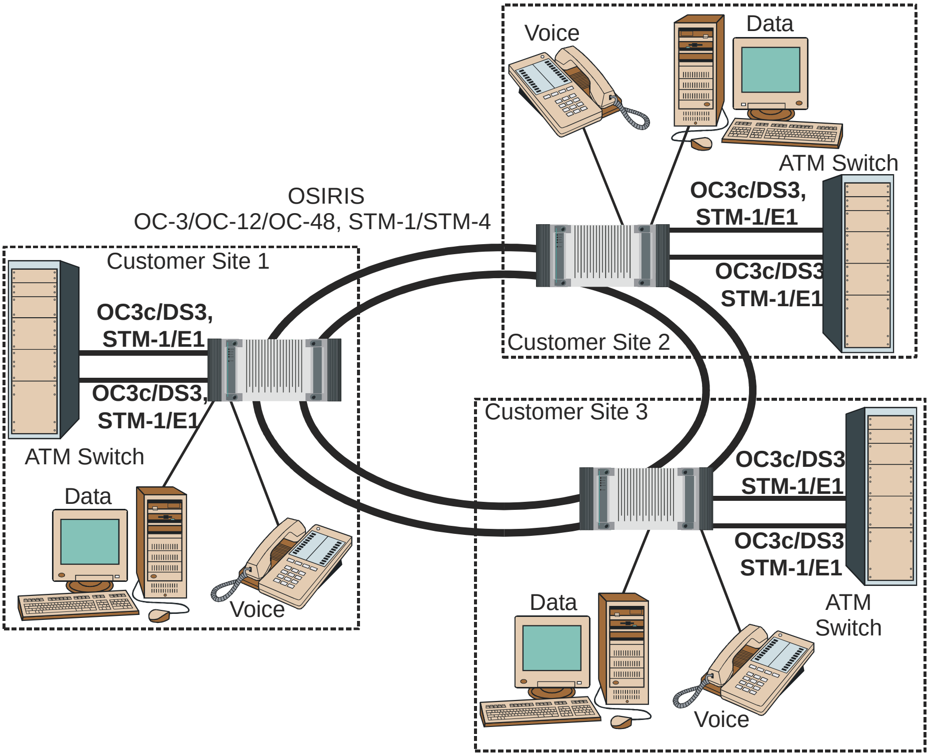
- ATM services on SONET/SDH based access platform - reduces ATM deployment costs.
- Service levels for voice and data applications remain unchanged.
- Provisionable OC3c/STM-1, DS3/E1 service protection—UPSR or Bandwidth Reuse.
- Direct Integration with TL1-based embedded OS systems—reduces service introduction costs.
- Full SONET/SDH *end-to-end* visibility and Performance Monitoring for Voice Applications—fits customer *service guarantee* business model.
- ATM traffic does not affect voice performance or bandwidth requirements.
- Direct SONET/SDH EC-1 connection to backbone transport or digital cross-connection—reduces service access costs while increasing management visibility.

The following application types are possible:

- Native DS3/OC3c ATM Transport
- ATM Campus or MAN Connectivity
- Video Contribution Network

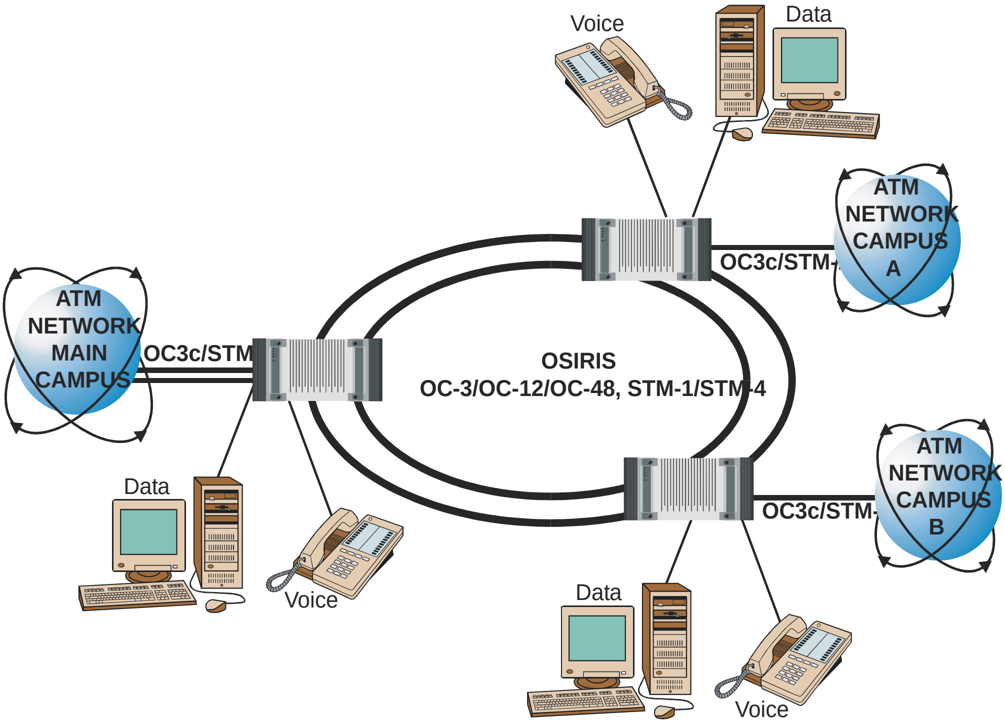
Native ATM Transport

The OSIRIS OC3c/STM-1 or DS3/E3 mappers let you provision Native-mode ATM or video connections on the same SONET/SDH-based infrastructure as existing voice and data applications. Some ATM Switch vendors also offer Ethernet, Fast Ethernet and FDDI Data Services integrated in their switching products.



ATM Campus or MAN Connectivity

In a campus networking environment, OSIRIS rings act as the physical transport for ATM via OC3c/STM-1 or DS3/E3 interfaces while simultaneously providing low cost, high reliability transport of voice and conventional data applications.



In the above figure, the main campus ATM network is interconnected to the ATM networks located at Campus A and Campus B. Each OC3c/STM-1 payload at the Main Campus is provisioned in a Point to Point fashion to Campus A and B.

In this case *bandwidth reuse* coupled with ATM rerouting capabilities let a single STS3c/STM-1 be reused. This offers *shared bandwidth* delivery between multiple locations.

This same application also provides *shared access* ATM service in a Metropolitan Area Network (MAN).

Doubling Bandwidth for LAN Applications

OSIRIS networks are Unidirectional Path Switching Ring (UPSR) providing path protection for all network traffic. The network provides protection with a redundant optical fiber.

However, if intelligent LAN switching or routing equipment is located at each customer site, the inherent re-routing capabilities of LAN switching/routing products provide traffic resiliency.

Bandwidth can be re-used to double datacom carrying capacity. You can reuse bandwidth at the STS-1/TUG3 or VT1.5/TU12 level. The remaining ring capacity can be used in normal UPSR path protected mode. Voice and video circuits are fully protected by SONET UPSR switching while shared bandwidth LAN services rely on the alternate routing capabilities of the attached LAN equipment.

You can double network bandwidth with either of these methods:

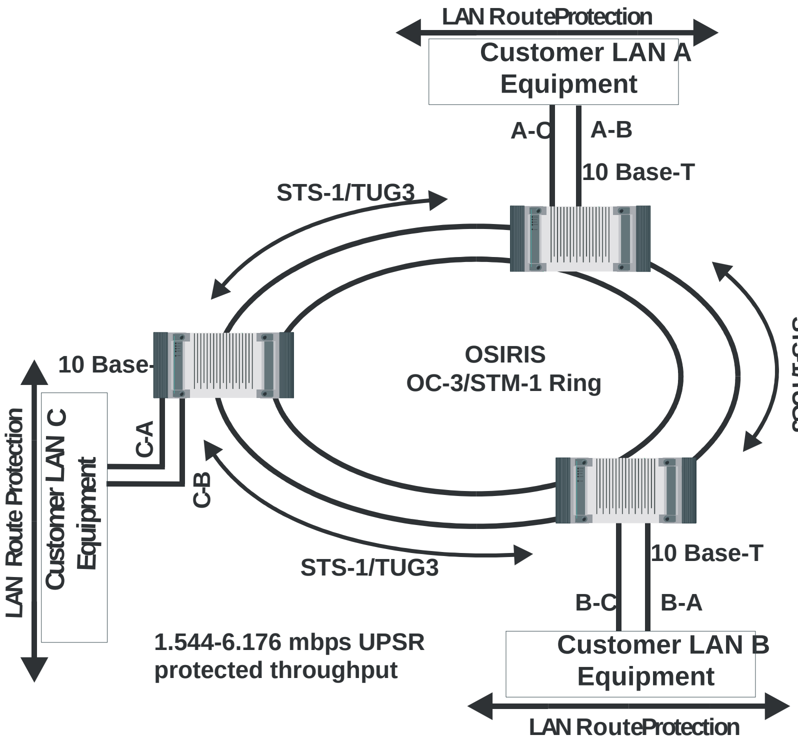
- Bandwidth Reuse mode using the Ethernet or Fast Ethernet mapper
- Single Channel mode using the Fast Ethernet mapper

Bandwidth Reuse Mode

Bandwidth Reuse mode provides a point-to-point connection between 10 Base-T Ethernet, 100BaseTX or 100BaseFX Fast-Ethernet interfaces in adjacent OSIRIS systems. Bandwidth Reuse mode does not protect against fiber cuts in the SONET access ring, and relies on attached LAN devices for path resiliency. The same VT1.5/TU12 channels can be used between multiple adjacent nodes in an OSIRIS ring, enabling overlaid Ethernet rings.

The same STS-1/TUG3 channels can also be used between multiple adjacent nodes in an OSIRIS network using Fast Ethernet mappers.

Using Bandwidth Reuse mode on specific channels does not affect normal UPSR operation on other VT1.5/STS-1, TU12/TUG3 channels.



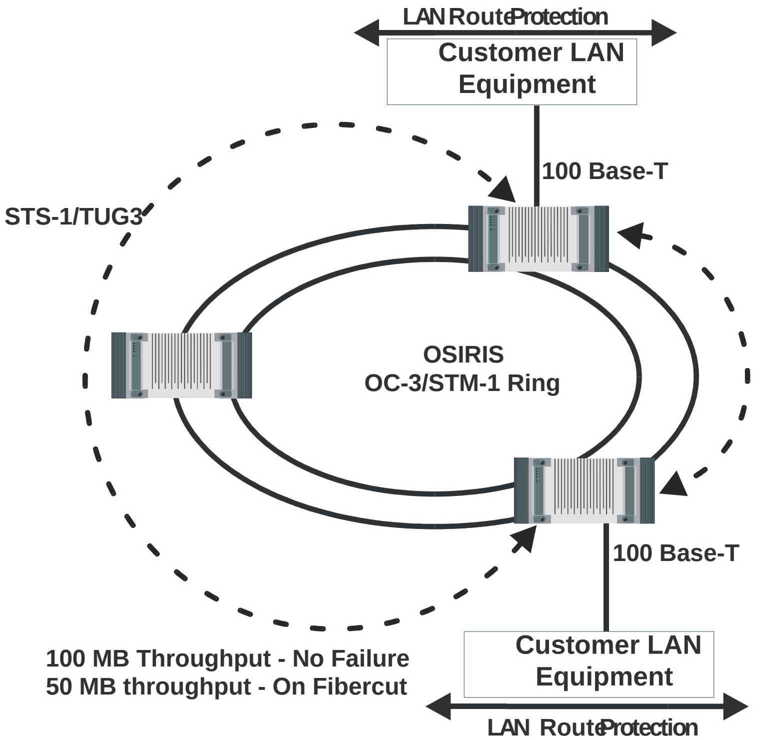
For more information on Bandwidth Reuse, refer to "Bandwidth Reuse Application" on page 46.

Single Channel Mode (Fast Ethernet Mapper)

Single Channel mode provides a Point to Point full 100 Mbps wire-speed connection between two 100Base-TX or 100Base-FX Fast-Ethernet interfaces. Both working and protection fibers carry traffic. This results in 100 Mbps throughput while consuming only one STS-1/TUG3 around the OSIRIS ring.

In the event of a fiber cut, network throughput is reduced automatically to 50 Mbps. Once the fiber cut is repaired, LAN throughput automatically reverts back to a full 100 Mbps wire speed connection.

Single Channel mode offers a full wire-speed and robust solution while consuming only half of the bandwidth that would normally be required in a conventional SONET/SDH UPSR network.



Chapter 6

The PacketPath Product Line

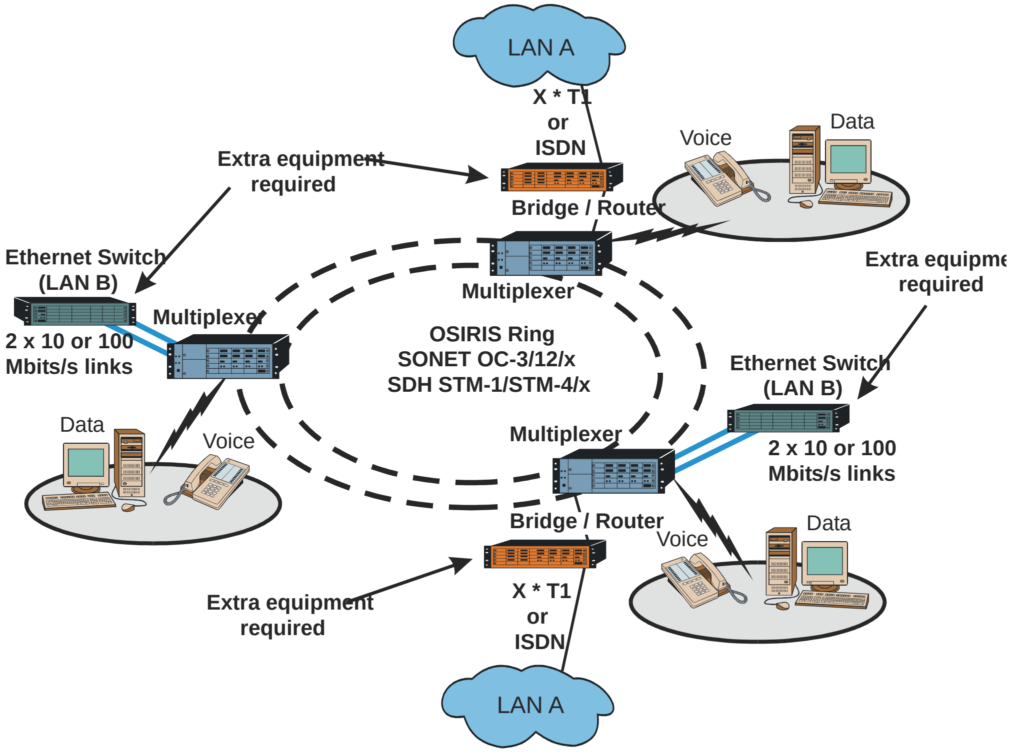
This chapter describes Positron's PacketPath product line and the following applications:

- Transparent LAN Services using the PacketPath Product Line
- IP Services using the PacketPath Product Line
- Mixed TLS and IP Environment
- Extended Optical Virtual Rings

PacketPath Overview

Bandwidth requirements for data networks are soaring, and the popularity of the Internet is pushing current IP networks to the limit. Support for this demand requires multiple technologies for carrying voice, LAN and video services to subscribers. This requires multiple pieces of equipment or independent broadband fiber networks for each traffic type (see Figure 19). This increases costs throughout the network.

Figure 19 Application Without PacketPath



The ultimate solution for carriers is to use one platform that supports Telco grade voice services as well as data services with enough flexibility to support users in large and small companies. Optical networks are a solution to this problem. As one of the first companies to offer native Ethernet and Fast Ethernet services over SONET and SDH optical networks, Positron continues this commitment toward an evolving and unified platform with the PacketPath product line.

PacketPath lets carriers allocate secured data services among multiple subscribers using independent Service Level Agreements (SLA) on shared bandwidth. Network architecture lets you integrate the usual concentration and routing equipment needed for LAN-based solutions for multiple customers.

SONET and SDH optical rings provide the high capacity bandwidth that the datacom world needs, and Positron PacketPath products provide the most efficient and cost-effective means of using this bandwidth.

The PacketPath Solution

Positron's OSIRIS with PacketPath is a powerful bandwidth-on-demand solution that dynamically assigns unused bandwidth to current data traffic. Optimized for the broadband access market, the PacketPath product line consists of three mapper cards that provide data over SONET and SDH optical networks. The PacketPath cards are known as follows:

- PacketPath Fractional Ethernet Access Card (PEC4)
- PacketPath ATM Concentrator Card (PAC155)
- PacketPath ATM Concentrator Card with DS3 interface (PAC45)

These three (3) mappers provide routed IP and bridged multi-protocol support in SONET and SDH optical rings. PEC4 (800344) cards are placed at the customer-premise inside a SONET or SDH optical ring to offer, both routed and bridged, packet connectivity to a head-end switch or router. PAC155 (800349) and PAC45 (800343) cards are also part of the optical ring, but instead act as a gateway to the head-end switch or router.

PacketPath mappers let you share Positron OSIRIS STS-1/TUG3 or STS3c/VC4 bandwidth between separate customers. Each of these interfaces is assigned a different Virtual Circuit (VC). VCs are independent of each other and completely secure. As an example, five VCs may represent five separate customers, each with a separate service level agreement (SLA).

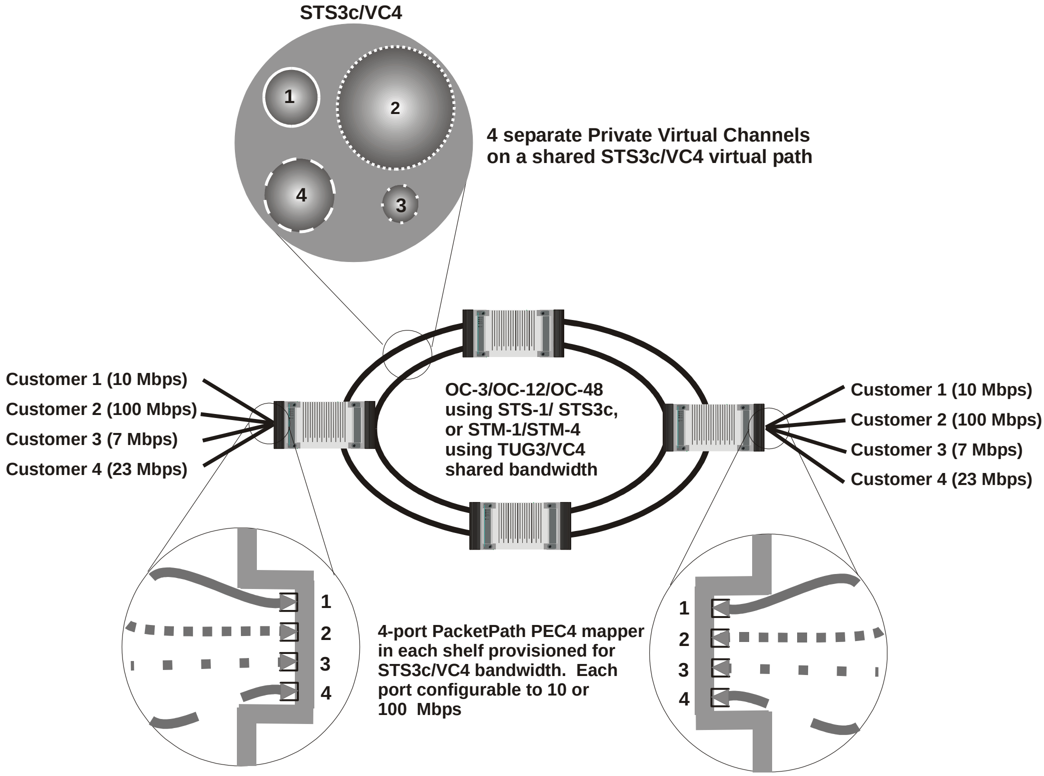
PacketPath Fractional Ethernet Access Card

The PacketPath Fractional Ethernet Access Card (PEC4) terminates four 10/100 BaseT lines in the same location. Each line may be configured as either Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) according to customer needs. The ring owner can thereby serve multiple clients with one mapper, offer committed information rates, and support traffic bursts.

The PEC4 card offers multiple point-to-point connections among multiple subscribers, each with independent parameters and bandwidth.

PEC4 cross-connections may terminate with other PEC4 mappers for applications such as Transparent LAN service. Or PEC4s may terminate with PacketPath ATM Concentrator Cards (PAC155 or PAC45) for IP access or for a bridged Transparent LAN service across two rings.

Figure 20 Ethernet to Ethernet



Detailed features of this mapper are listed below:

- 4 x RJ45 (MDI) standard Interfaces 10/100 BaseT
- Full or Half Duplex provisionable
- Fully compliant with Ethernet Standards (802.3, 802.3u)
- Ethernet Frame Type and sub-protocol independent
- Powerful bandwidth-on-demand solution with rates from 256Kbps to 100Mbps
- Secured Virtual Circuits (VC)/1 per physical Ethernet port.
- Versatile Service Level Agreement & Quality of Service offering
- Transparent LAN Services (TLS) using Bridged Virtual Circuits on a per port basis

- Supports specific protocols: Cisco ISL, VLAN tagging and spanning.
- Connects to the SONET/SDH network at STS-1/TUG3 or STS3c/VC4 level
- Full Path Protection at the VC level under 50 ms.
- IP router Port Extension using IRDP and RIP protocols.
- Works in conjunction with all other PacketPath products
- Provisioned by the same, easy to use, OSIRIS-VUE Network Management platform

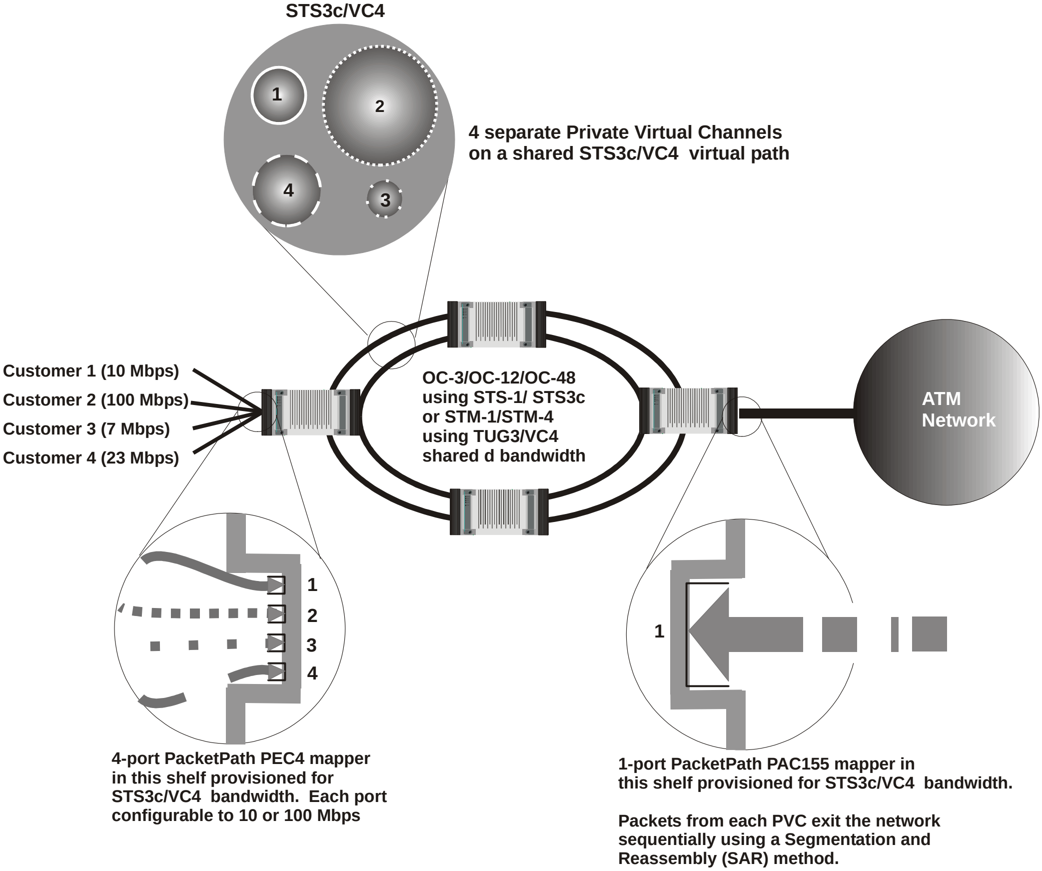
PacketPath ATM Concentrator Cards

The PacketPath ATM Concentrator Cards (PAC155) act as a gateway between the head-end switch and the router. Ethernet packets can be transported to a remote location and packets can be dropped in the desired format, terminating in an ATM OC3c interface (PAC155).

This saves chassis slots, ATM switch ports, and prevents messy wiring.

PacketPath cards also performs SAR (Segmentation and Reassembly), concentration, trunking and support up to 128 virtual circuits.

Figure 21 Ethernet to ATM



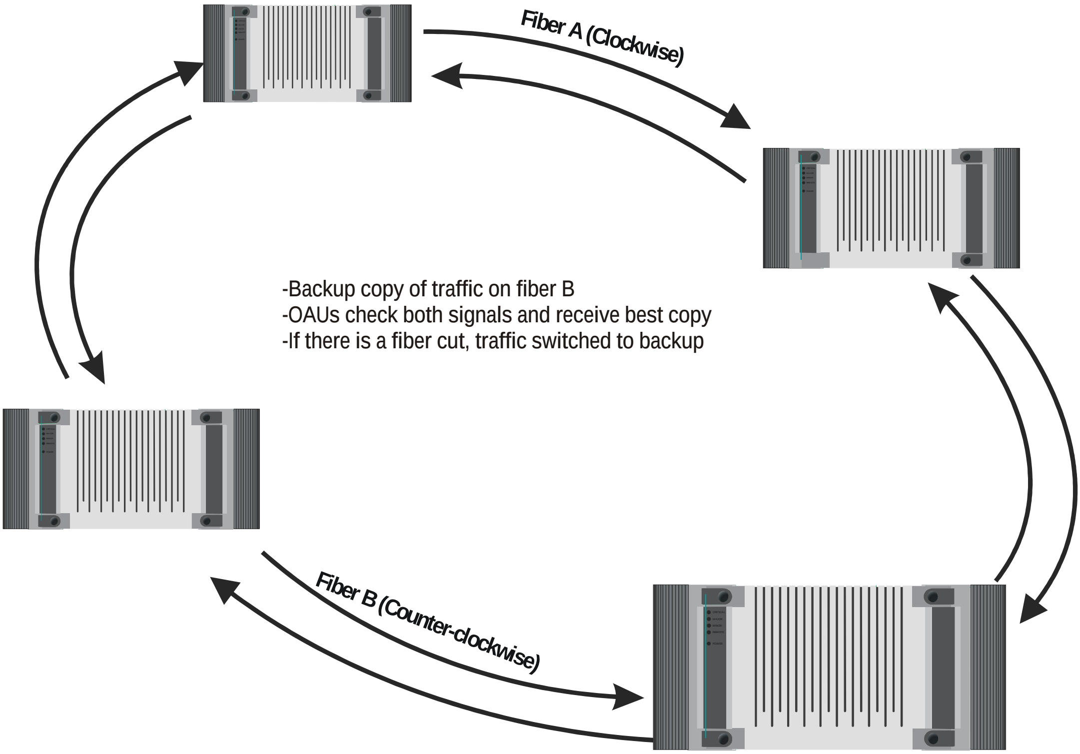
Detailed features of this mapper are listed below:

- ATM OC3c/STM-1 155Mbps optical Interface (SC or ST)
- ATM DS3/E3 75 ohms Coax Interface
- Fully compliant with ATM Forum UNI 3.1 09/94 (PVC)
- Support nrt-VBR and UBR Class of Service
- Compliant with RFC 1483 bridged or IP routed Virtual Circuits
- Supports up to 128 Virtual Circuits
- Bandwidth on Demand (from 256Kbps up to 100 Mbps per virtual circuit)
- Connects to the SONET/SDH network at STS-1/TUG3 or STS3c/VC4 level
- Offers full path protection under 50 ms at the VC level
- Works in conjunction with all other PacketPath products
- Provisioned by the same, easy to use, OSIRIS-VUE Network Management platform

Data Traffic Flow

The PacketPath product line supports data traffic across an OSIRIS UPSR network. Typical UPSR voice traffic is added to both clockwise and counter-clockwise rings (Figure 22). This uses redundant fiber for protection of the voice traffic.

Figure 22 UPSR Configuration

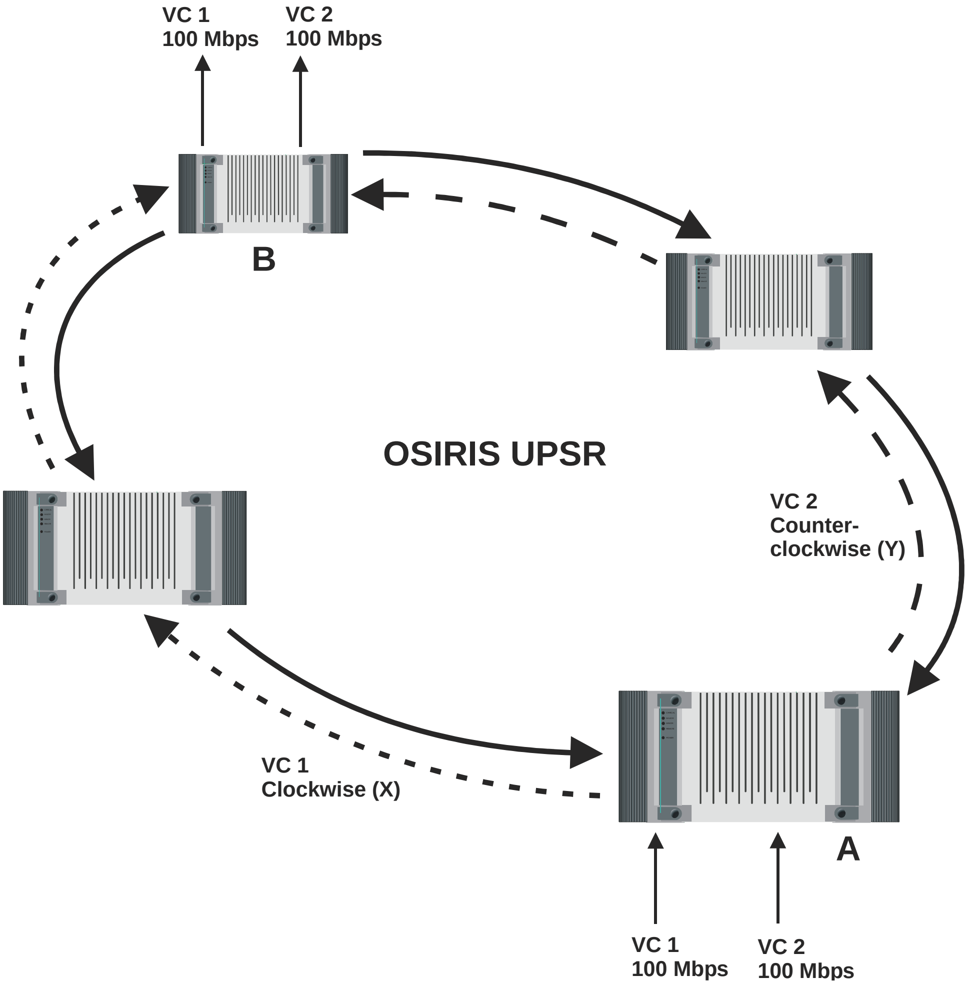


Data traffic is based on the Ethernet or TCP/IP standards, which are packet-based and include built-in error correction. Therefore, separate data traffic can travel on the same timeslot in both directions around the ring.

In the following diagram (Figure 23), VC1 and VC2 (Virtual Channels) carry separate customer traffic and represent two independent Service Level Agreements (SLA). Both SLAs are for 100 Mbps.

Note: Either clockwise or counter-clockwise fiber can be designated as the working path.

Figure 23 PacketPath Data Flow in UPSR



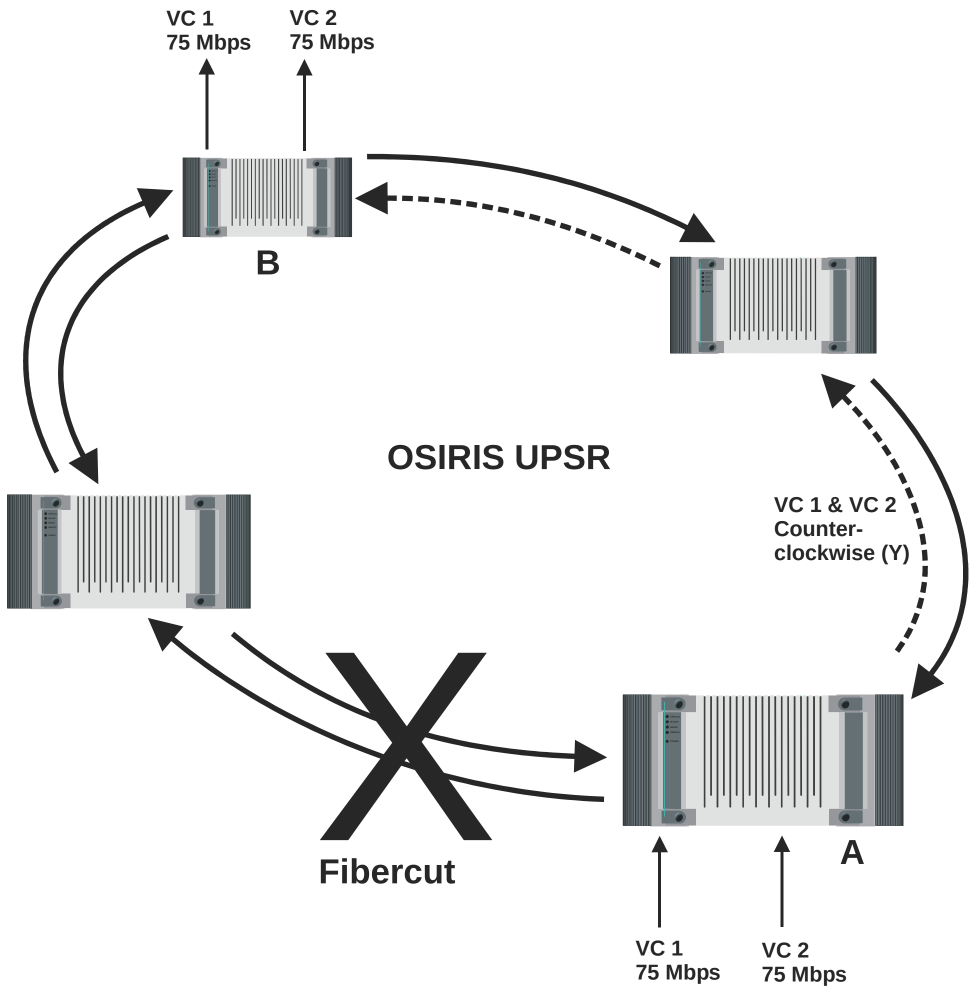
VC1 and VC2 are both provisioned on the same timeslot between nodes. However, VC1 is set to the clockwise fiber and VC2 is set to the counter-clockwise fiber. Because VCs are both adding and dropping at the same nodes, there is no conflict for this timeslot. This method is known as Bandwidth Reuse which doubles ring capacity for certain applications.

Traffic Flow During Fibercut

In the event of a fiber cut or node failure, since both VCs share the same fiber, traffic on VC1 switches to the counter-clockwise fiber. Traffic is re-assembled at the end site and traffic from independent SLAs is never mixed.

Under normal operations throughput is 100 Mbps for both VCs. When protection switching occurs, both VCs share one 100 Mbps bandwidth pipe. Therefore, throughput for each is cut in half, to 50 Mbps.

Figure 24 Data Flow During Fibercut



VCs may be provisioned as revertive or non-revertive. Provisioning as revertive switches the VC back to the original path when a fiber cut is repaired. Non-revertive maintains the VCs on the *switched* fiber. In order to return to a repaired fiber non-revertive VCs must be switched manually.

Bandwidth Flexibility

The PacketPath product line dynamically allocates unused bandwidth to current data traffic. This guarantees a minimum transmission rate as well as the potential for faster line rates. PacketPath's statistical multiplexing lets carriers oversell bandwidth, increasing revenue opportunities.

Committed Information Rate

The Committed Information Rate (CIR) is the guaranteed minimum bit rate the customers subscribed to under a service level agreement. For example, a customer may have signed up for Transparent LAN Services (TLS) at a guaranteed minimum line rate of 78 Mbps (Fast Ethernet).

Because LAN traffic is variable, not all STS-1/TUG3 or STS3c/VC4 bandwidth is always used. PacketPath mappers automatically switch traffic to unused bandwidth, increasing line rate beyond the CIR for this customer.

Burst Information Rate

The Burst Information Rate (BIR) is the maximum rate of customer traffic. For example, a service level agreement for a CIR of 4.5 Mbps (on Ethernet) may have a BIR of 9 Mbps. PacketPath mappers are designed to increase line rate by constantly allocating unused bandwidth. When traffic reaches the BIR, the ring owner must decide whether traffic in excess should be dropped or let through. In most applications, when Ethernet packets are dropped, information is not lost: receiving equipment requests the traffic again and that portion is retransmitted at a speed conforming to the BIR.

Oversubscription

Not all customers subscribing to data services, use the maximum bandwidth available to them at all times. This is due to the variable nature of LAN traffic. This lets the ring owner sell more bandwidth than is actually available. Known as Oversubscription, the PacketPath product line makes this possible by statistical multiplexing on the virtual path.

Differentiated Services

As ring owner, PacketPath offers different methods of slowing traffic from the BIR. Datacom traffic is transmitted in the following way:

- **Weighted fair schedule (WFS)**—PacketPath mappers store traffic in 7 queues while packets are forwarded through the ring. Each queue may represent a separate class of service to which customers may be assigned. The ring owner weighs queues differently for traffic priority level, which has been agreed to in a service level agreement.

  For example, if all queues are full and one queue has a 40% weight (high priority level), then 40% of traffic transmitted comes from that single queue. However, not all data packets are the same size. WFS takes this into account, transmitting the weighted volume of traffic, not simply the number of packets.

- **Weighted random early discard (WRED)**—if a queue becomes full, packets are discarded randomly from the queue. This method affects traffic from all customers on a queue equally. Therefore no specific customer or connection is affected. All traffic is throttled equally within the class of service.

PacketPath Applications

This section describes the following PacketPath applications:

- Transparent LAN Services using the PacketPath Product Line
- IP Services using the PacketPath Product Line
- Mixed TLS and IP Environment
- Extended Optical Virtual Rings

Transparent LAN Service (TLS)

For customers wanting to deploy Wide Area Network (WAN) services, PacketPath offers point-to-point capabilities. It allows for the termination of four Fast Ethernet interfaces in the same location, thereby serving multiple locations on one mapper. PacketPath lets you transport the full Ethernet frame from one point to another. Ethernet packets are transmitted end-to-end in their native format. This assures full transparency so that there are no applications compatibility problems.

When deploying PacketPath for TLS services it is possible to offer services that are more closely matched to the clients bandwidth needs.

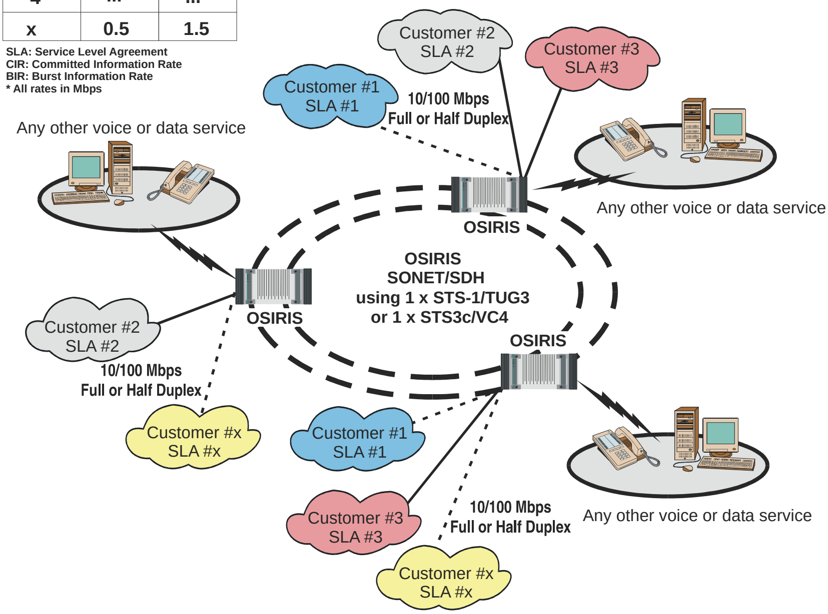
For example: Three customers purchase Service Level Agreements (SLA). Each customer is assigned a VC independent from the others that carries their traffic. These VCs share an STS-1/TUG3. Each VC corresponds to two PEC4 ports, one on each end of the VC. OSIRIS-VUE is used to provision point-to-point cross-connections as follows (also see Figure 25):

Customer	SLA	VC	Bandwidth Timeslot	Cross-connection
1	1	1	STS1-1	Add/Drop on Node 2
		1	STS1-1	Add/Drop on Node 3
2	2	2	STS1-1	Add/Drop on Node 1
		2	STS1-1	Add/Drop on Node 3
3	3	3	STS1-1	Add/Drop on Node 2
		3	STS1-1	Add/Drop on Node 1

Figure 25 Transparent LAN Services

SLA	CIR	BIR
1	10	20
2	3	4.5
3	1.5	10
4	...	...
x	0.5	1.5

SLA: Service Level Agreement
CIR: Committed Information Rate
BIR: Burst Information Rate
* All rates in Mbps



Service Benefits

The following service benefits apply to both subscribers and carriers.

Bandwidth on Demand

Remote network management via OSIRIS-VUE software lets network managers rapidly provision increased customer bandwidth without making site visits.

Secure Traffic

PacketPath mappers transmit all traffic in Virtual Circuits (VCs). Traffic on each VC is totally independent of the other channels.

No Protocol Conversion

Ethernet packets are transmitted end-to-end in their native format. This assures full transparency so that there are no applications compatibility problems.

One Platform Required

Because no external equipment is required for Ethernet conversion, the entire OSIRIS network can be provisioned with user-friendly OSIRIS-VUE software from the network control center.

This requires only one management software at the customer premise location and minimizes the cost of bandwidth management.

Telco Grade Voice Service Supported

OSIRIS networks provide SONET OC-3/OC-12 or SDH STM-1/STM-4 multiplexer capabilities for telecommunications traffic. The PacketPath product line is designed for the rapidly converging telecom and datacom markets.

Statistics Available

The PacketPath product line lets you monitor network usage to enable efficient customer billing.

Required Equipment

This application requires one PacketPath PEC4 card per site where Transparent LAN Services are requested. Because the PacketPath PEC4 has four ports, it is possible to connect up to four individual subscribers and create four different Virtual Circuits (VC) going to any site around a SONET or SDH optical ring.

Transparent LAN service requires one PacketPath PEC4 mapper at each node where services are offered. PEC4 mappers on either end of the transparent LAN connect to only one STS-1/TUG3 or STS3c/VC4.

If there are more than four subscribers per site, a second set of PacketPath PEC4 mappers are required. The second set of mappers carry traffic on a separate STS-1/TUG3 or STS3c/VC4.

For Transparent LAN service bridged across two separate OSIRIS networks, two PacketPath cards are required. These cards are connected together and forward/ receive messages between rings.

IP Services

The growing demand for Internet Access (IP services) and Corporate LAN services have forced the broadband and access infrastructure to adapt to these needs. Networks must support a many-to-many as well as a many-to-one data network.

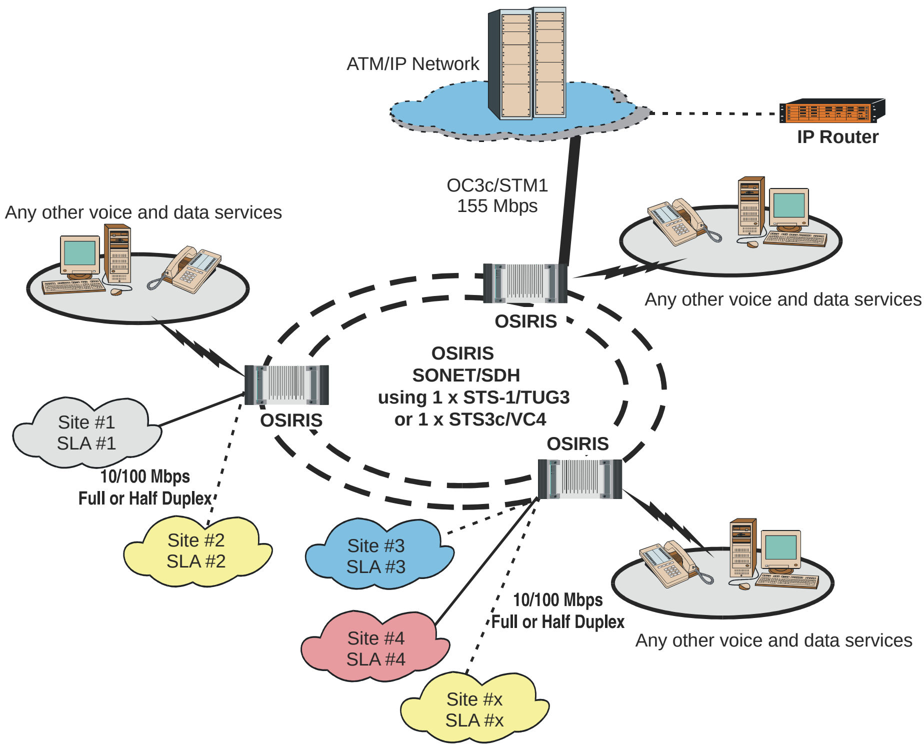
This application is designed to support independent subscribers toward one main head-end for IP Services. The head-end could be an Internet Service Provider or the Corporate Head Office. Each point-to-point link created between the sites toward the head-end could have its own parameters and bandwidth requirements.

In the case of IP service, only the IP packet is sent through and the Ethernet layer is automatically rebuilt on the customer premise's equipment. PacketPath IP service terminates IP tunnels from access or backbone routers at the end-user location. Additional routers and extensive configuration are not necessary.

For example: SLA 1 and 2 may be separate contracts for 10 Mbps service (on Ethernet). LANs from Site 1 and 2 plug into ports 1 and 2 of the same PacketPath PEC4 cards located in an OSIRIS shelf. The OSIRIS-VUE software is used to provision bandwidth between this shelf and the head-end node using a point-to-point configuration (Add/Drop). The head-end node contains a PacketPath PAC155 card and hands off all traffic on the STS3c/VC4 to an ATM/IP network. Refer to Figure 26.

In the sample network layout below, end-users are offered IP services and Internet connectivity according to their needs. As with the Transparent LAN Service, packets are statistically multiplexed on the link to provide improved bandwidth usage and permit bursts and over-subscription.

Figure 26 Using PacketPath in an ATM/IP Network



PacketPath PAC155 and PAC45 mappers provide a router port extension. All IP parameters are acquired automatically when the PacketPath mapper is connected to a properly configured IP router, either directly or through an ATM cloud. As a result, the owner of the ring does not have to set any IP parameters.

Service Benefits

The following service benefits apply to subscribers and carriers.

Easy Traffic Distribution to a Central Point

The PacketPath PAC155 card terminates up to 128 Virtual Circuits from one OC3c or STM-1 optical interface. This eliminates complicated and bulky wiring at the customer location.

Bandwidth on Demand

Remote network management via OSIRIS-VUE software lets network managers provision increased customer bandwidth rapidly without making site visits.

Only One Platform Required

Because no external equipment is required for Ethernet conversion, the entire OSIRIS optical multiplexer network can be provisioned using user-friendly OSIRIS-VUE software from the network control center.

Telco Grade Voice Service Support

The Positron OSIRIS family of optical networks provide SONET OC-3/OC-12, or SDH STM-1/STM-4 multiplexer capabilities for telecommunications traffic. The PacketPath product line is designed for the rapidly converging telecom and datacom markets.

Statistics Available

The PacketPath product line lets you monitor network usage to enable efficient customer billing.

IP Router Port Extension

Automatic IP features extend remote IP router addresses to a PacketPath mapper port. This relieves the provider of configuring any IP information at the customer location. All that is required is a properly configured backbone router. The router port is therefore extended to the customer location.

Required Equipment

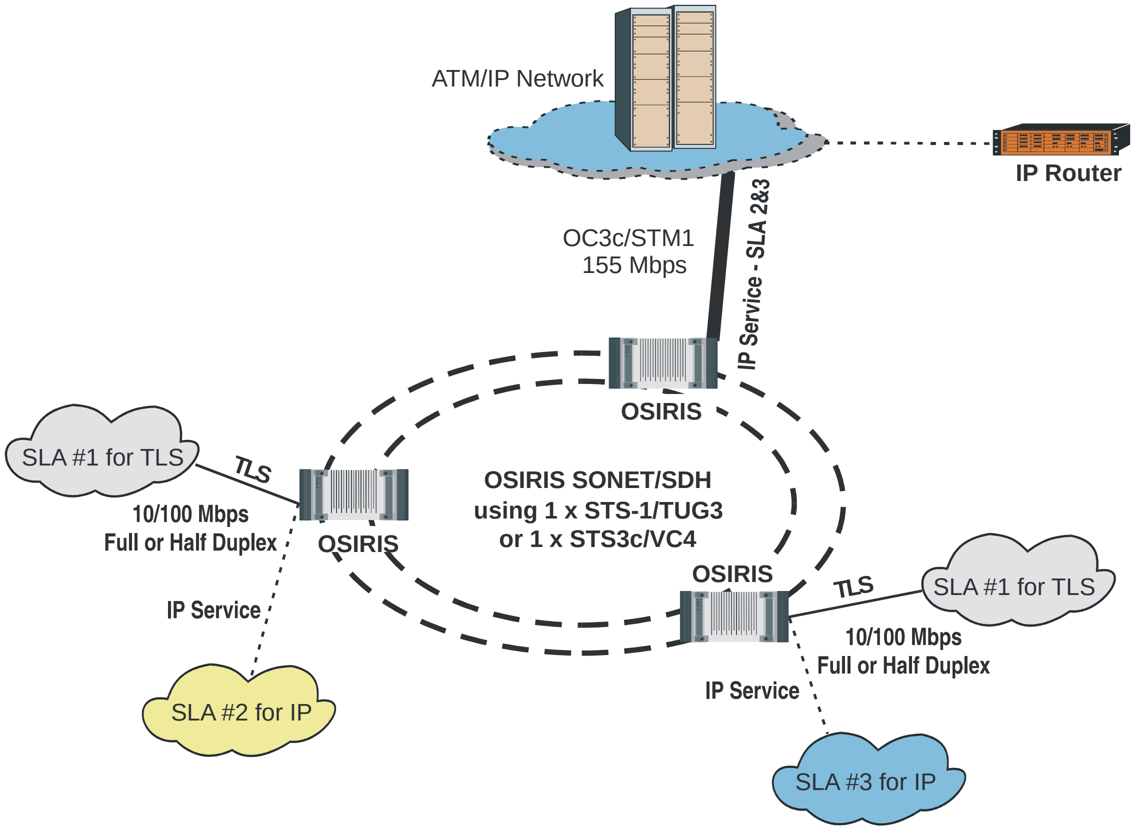
This application requires one PacketPath PEC4 per site where needed and one PacketPath PAC155 or PacketPath PAC45 at the head end. Because the PacketPath PEC4 has four ports, you can connect up to four individual subscribers and create four different Virtual Circuits (VC) going to the head-end or any other site across a SONET or SDH optical ring.

The PacketPath PEC4 connects to only one STS-1/TUG3 or STS3c/VC4 and contains only four Ethernet ports. If there are more than four subscribers per site, a second PacketPath PEC4 would be required. The second mapper would carry traffic on a different STS-1/TUG3 or STS3c/VC4.

Mixed IP and TLS Environment

Because PacketPath is based on Virtual Circuits, the architecture allows simultaneous multiple independent Transparent LAN and IP Services within the same Virtual Ring or even among multiple Virtual Rings. The only limit to traffic combinations is the bandwidth within that same Virtual Ring.

Figure 27 Mixed TLS and IP Services



Extended Optical Virtual Rings

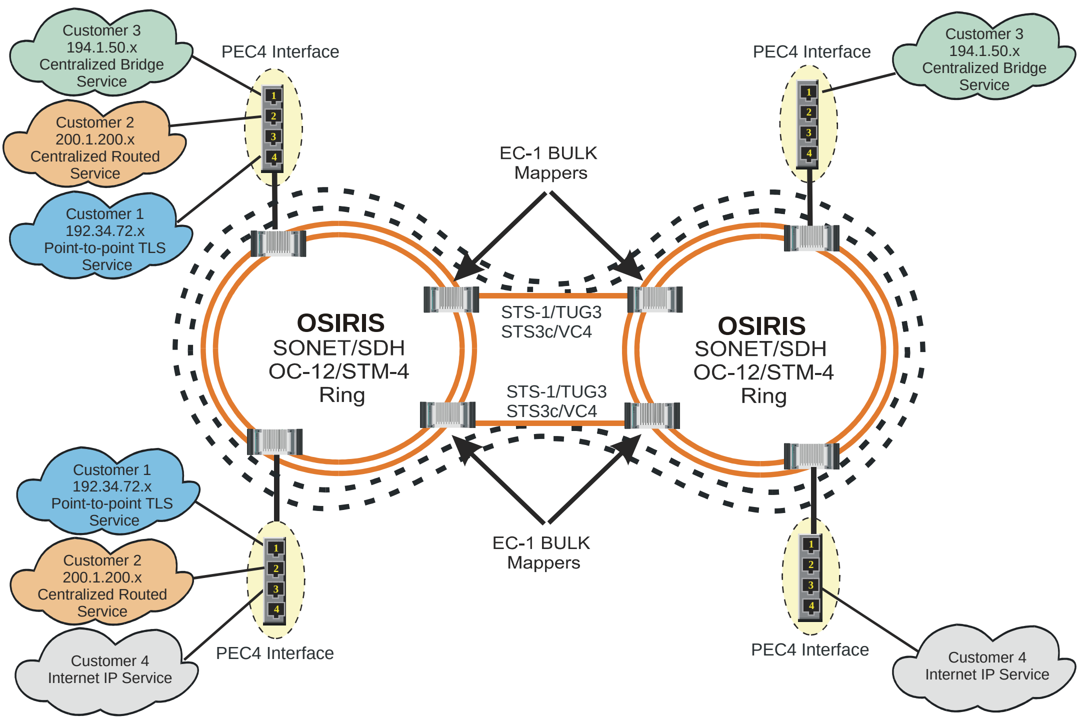
PacketPath enables two types of virtual ring topologies.

SONET and SDH Based Virtual Rings

The OSIRIS platform extends SONET/SDH visibility to more than one interconnected ring. Also known as Virtual Rings, they may be interconnected using EC-1 BULK or OC3c/STM-1 mappers. EC-1 BULK interconnected rings let you carry native Ethernet traffic (e.g., WAN traffic) at STS-1/TUG3 capacity. OC3c/STM-1 interconnected rings let you carry native Ethernet traffic at STS3c/VC4 capacity.

The WAN is built between two PEC4 mappers, one located in each ring.

Figure 28 SONET/SDH Virtual Ring Topology



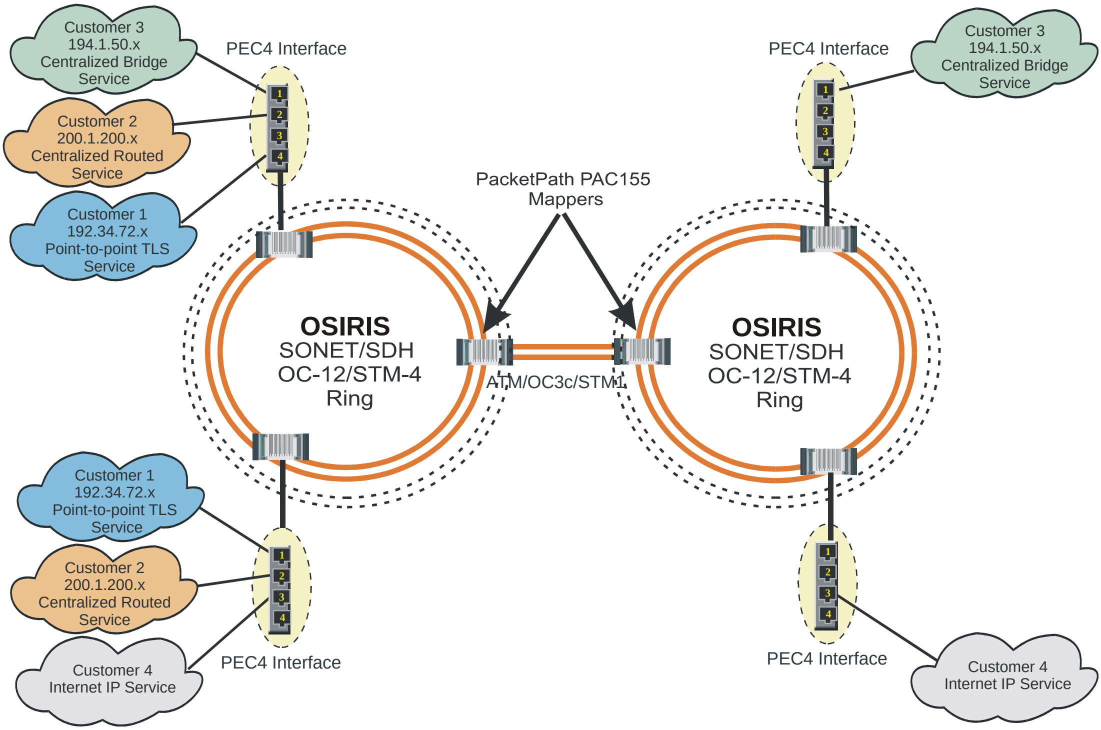
This application has the following characteristics:

- Uses 4 mappers to interconnect two rings
- No statistic visibility at the interconnection
- No traffic engineering & prioritization
- No equipment protection available
- Requires minimal configuration and provisioning

Packet Path Based Extended Virtual Ring

In this application, the PAC155 card acts as the bridge between interconnected rings. This card acts as a concentrator of Ethernet or Fast Ethernet traffic and hands it off at a higher capacity to another SONET/SDH ring.

Figure 29 PacketPath Extended Virtual Ring Topology



This application has the following characteristics:

- Uses four (4) mappers to interconnect two rings
- Statistics available through PAC155
- Traffic engineering & prioritization available
- Equipment protection support (future)
- Requires detailed configuration and provisioning of all VCs across the ring

Chapter 7

Network Management Applications

OSIRIS networks can be managed using any of the following connection types:

- Direct serial connection to the Craft or TL1 port
- Modem connection
- Telnet session via TCP/IP
- Via a Local or Wide Area Network (LAN/WAN) or corporate Intranet
- Via an OSI-based network management system

Any PC with a TCP/IP protocol stack may be used to provision the network.

For information on modem and direct connections between a PC and an OSIRIS network, refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)*.

When installed, the NMCU supports larger memory capacities, and provides a 10BaseT Ethernet interface.

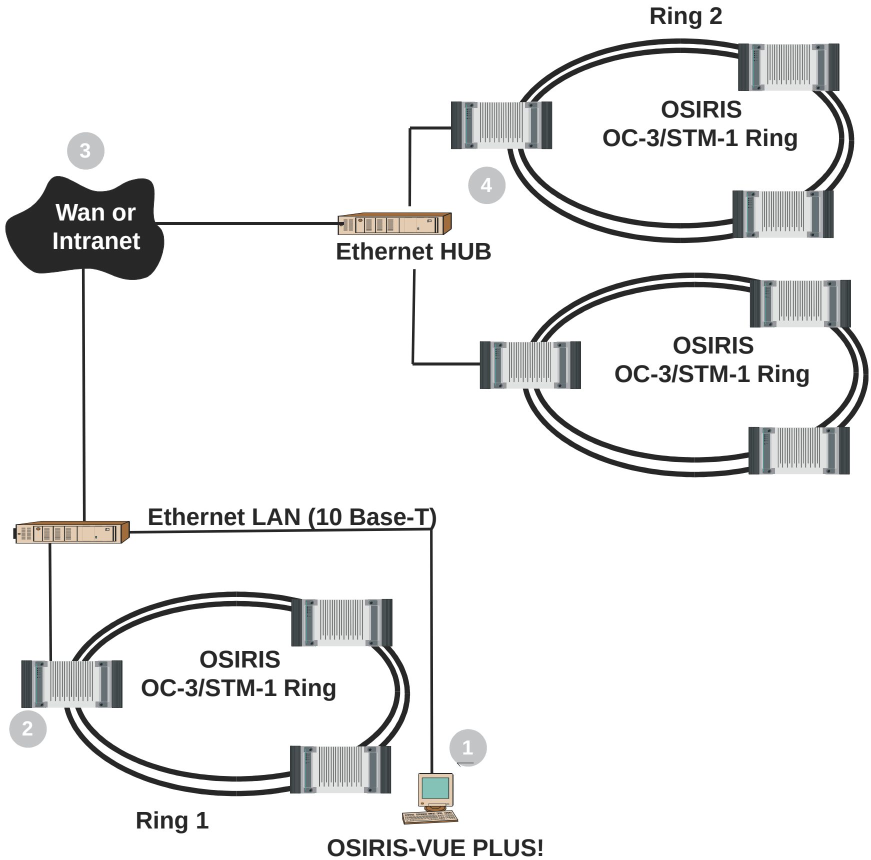
For more information on the NMCU, refer to "Related Documents" on page 77.

Managing a Network Via a LAN

OSIRIS-VUE PLUS! can be used to manage and provision OSIRIS networks remotely using LAN connections. Each shelf connecting with the LAN must be equipped with a Network MCU (NMCU).

The following diagram depicts a typical network management topology on an LAN interconnected network.

Figure 30 LAN Network



1. Location 1 represents a PC operating OSIRIS-VUE software. This PC is connected to the LAN through a typical network connection. Using this PC, you can provision any OSIRIS ring connected to the WAN or Intranet.

To connect using two sessions, you must know the IP address of both OSIRIS rings. Refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)*.

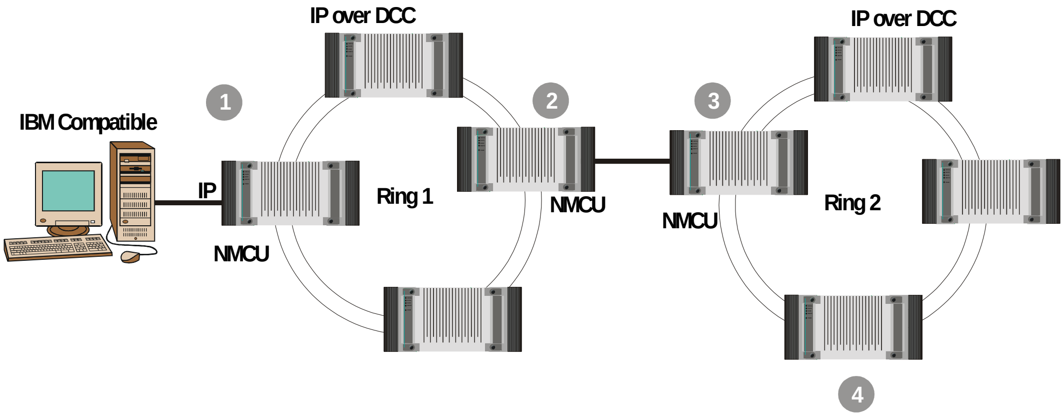
2. At Location 2, the LAN is connected to an OSIRIS optical multiplexer via the NE LAN port of the ACIU. This shelf must contain an NMCU (800307) for the NE LAN port to be active.
3. Location 3 represents the LAN. Multiple OSIRIS rings can be monitored from the same LAN.
4. Location 4 represents a LAN connection to a separate OSIRIS ring. The PC at Location 1 is used to provision this ring via a telnet connection. The LAN is connected to Location 6 via the NE LAN port of the ACIU (OSIRIS STD and OSIRIS XTD only). This shelf must contain an NMCU (800307) for the NE LAN port to be active.

IP Tunneling

IP Tunneling eliminates the need for external routing equipment by making use of the DCC to transport IP management information. Since the DCC is shared with Ring 1 management information, only a portion is available for IP tunneling.

Note: Only NMCUs support IP Tunneling and Ping. Regular MCUs cannot be assigned an IP address.

This figure displays typical traffic flow between several points on a LAN network.



Important Points

The following are important points about the IP tunneling application:

- You must assign IP addresses to several nodes in order to use IP tunneling to manage a remote network. In this case, shelves at Location 1, 2, and 3 are assigned IP addresses.
- Network traffic does not flow between Ring 1 and Ring 2. The connection carries network management information only.
- The connection between Location 2 and 3 is established through the Ethernet ports on the ACIU of both shelves.
- Ring 1 is never visible in OSIRIS-VUE software when you log on to Ring 2 via IP tunnelling. Management information is carried on the DCC of Ring 1 (IP-over-DCC).

For information on IP tunneling, refer to the *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001).*

OSI Network Management

OSI is a management standard that allows interoperability of multivendor equipment.

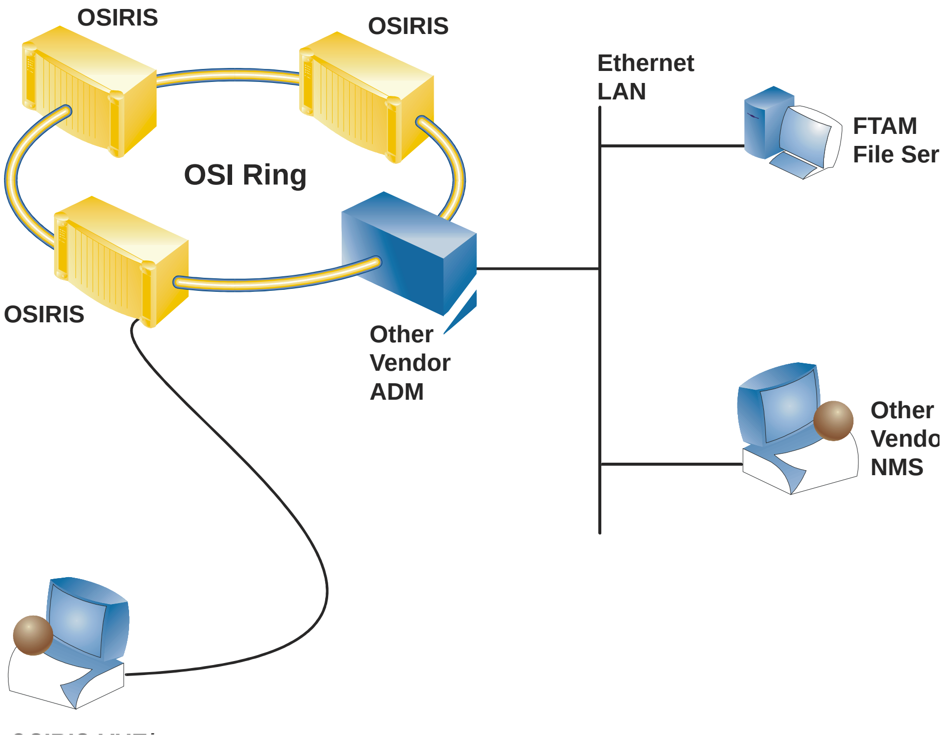
The OSI (Open System Interconnection) specifications were conceived and implemented by the International Organization for Standardization (ISO) and the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T).

The OSI model packages and transports Data Communication Channel (DCC) information from one Network Element to another NE (remote) using a serial port or by establishing a Telnet session. With the OSI option, OSIRIS-VUE/OSIRIS-VUE PLUS! can view and provision the topology of OSIRIS rings from a single DCN (Data Communication Network) connection.

OSI supports the following characteristics depicted in the graphic below:

- **Equipment interworking—**OSIRIS shelves form a closed UPSR with other vendor's equipment which also supports OSI.
- **Compatible provisioning—**both OSIRIS-VUE and other network management systems supporting OSI can be used to provision any OSIRIS shelf in the OSI ring.

- **View beyond the network**—because the other vendor ADM supports OSI, OSIRIS-VUE can see beyond the ring. In this example, OSIRIS-VUE can be used to initiate a file download from an FTAM server to the OSI ring.



Note: For more information on OSI provisioning procedures, see *OSIRIS-VUE™/OSIRIS-VUE PLUS!™ User's Guide (206-001)*.

Appendix A

Related Documents

While reading this guide, you may want to refer to the following documents:

Hardware Installation

- *OSIRIS® Hardware Reference Guide (203-001)*
- *OSIRIS® STD Shelf Installation Guide (203-002)*
- *OSIRIS® XTD Shelf Installation Guide (203-003)*
- *OSIRIS® Micro Shelf Installation Guide (203-004)*
- *OSIRIS® Micro WMU Installation Guide (203-005)*
- *OSIRIS® XTS Shelf Installation Guide (203-022)*

OSIRIS-VUE Software

- *OSIRIS-VUE™/OSIRIS-VUE PLUS™ User's Guide (206-001)*

Testing and Troubleshooting

- *OSIRIS® Shelf Testing Guide (203-007)*
- *OSIRIS® Troubleshooting Guide (203-008)*

Glossary

This glossary includes acronyms and definitions for telecom and datacom applications as well as OSIRIS optical multiplexers.

Acronyms

The following technical acronyms appear in this document.

ACIU	Alarm and Craftperson Interface Unit.
ADM	Add/Drop Multiplexer
AIS	Alarm Indication Signal (Alarm)
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BIU	Buffer Interface Unit
BLSR	Bi-directional Line Switching Ring
BPV	Bipolar Violation
CAP	Competitive Access Provider (telecom)
CO	Central Office
COS	Class of Service
CLEC	Competitive Local Exchange Carrier (telecom)
CRDMISMAT	Card Mismatch (Alarm)
CRDRMVD	Card Removed (Alarm)
CRC	Cyclic Redundancy Code
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSU	Channel Service Unit
DCC	Data Communication Channel

DACS	Digital Access Cross-connect System
DCS	Digital Cross-connect System
DSU	Data Service Unit
DSx	Digital Signal Level x
EIA/TIA	Electronic Industry Association/Telecommunications Industry Association
EID	External Interconnection Device
ES	Errored Second
ESF	Extended Superframe
EPS	Equipment Protection Switching
EXZ	Excessive Zeros
FDDI	Fiber-distributed Data Interface
FEATMSMAT	Feature Mismatch
FE	Far End
FRDCSWREQ	Forced Switch Request
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IR	Intermediate Range
LAN	Local Area Network
LPBK	Loopback
LCRCD	Loop Code Received
LED	Light Emitting Diode
LOS	Loss of Signal
LR	Long Range
MAC	Medium Access Control
MAN	Metropolitan Area Network
Mbps	Megabits per Second
MCU	Monitor and Control Unit
MM	Multimode
NIC	Network Interface Card
NIU	Network Interface Unit
NE	Network Element (Node)
NMCU	Network MCU
NOC	Network Operations Center
NSA	Non-Service Affecting
OAU	Optical Access Unit
OOF	Out of Frame

OS	Operating System
PC	Personal Computer
PBX	Private Branch Exchange
PFEATMS-MAT	Protection Card Feature Mismatch
PM	Performance Monitoring
PPS	Path Protection Switching
RAI	Remote Alarm Indication
RBOC	Regional Bell Operating Company (telecom)
RFI	Remote Failure Indication
RX	Receive (optical signal)
SA	Service-Affecting
SONET	Synchronous Optical Network
SDH	Synchronous Digital Hierarchy
SES	Severely Errored Second
SF	Superframe
STD	OSIRIS STD Shelf
TBOS	Telemetry Byte-oriented Serial cable
TCI/IP	Transmission Control Protocol/Internet Protocol
TIU	Tributary Interface Unit
TL1	Transaction Language 1
TLS	Transparent LAN Services
TOW	Traffic Overwritten
TSA	Timeslot Assignment
TSI	Timeslot Interchange
TX	Transmit (optical signal)
UAS-P	Unavailable Seconds
UPSR	Uni-directional Path Switching Ring
VT	Virtual Tributary
QSSR	Quasi-Random Signal
QoS	Quality of Service
VLAN	Virtual LAN
WAN	Wide Area Network
XTD	OSIRIS XTD Shelf
XTS	OSIRIS XTS Shelf

Glossary

The following technical terms appear in this document.

10Base-2 (Thin net)

An 802.3 standard for LAN supporting 10 Mbps over distances up to 185 meters (607 ft) on thin coaxial cable. This specification allow 30 or fewer MAUs per cable segment spaced at no less than 0.5 meters (1.64 ft.). Both segment ends must be terminated with a 50 ohm terminator. Earth grounding of the segment shield must take place at only one point on the cable.

10Base-T

An Ethernet transmission standard using twisted wire pairs defined at 10Mbps. This standard uses RJ45 or 50-pin AMP connectors when interfacing to a patch panel.

10Base-T (Twisted Pair)

An 802.3 standard for LAN. 10 Mbps over distances up to 100 meters (328 ft.). Cat 3 cable (or better) should be used. RJ-45 connectors are commonly used.

100Base-TX

An alternative contained in the IEEE 802.3 100Base-TX CSMA/CD (Carrier Sense Multiple Access with Collision Detection) proposals for a 100 Mbps Ethernet that specifies two UTP5 pairs.

ADM

Add/Drop multiplexer. See "Multiplexing".

ATM

Asynchronous Transfer Mode (ATM) is a high speed cell-switching technology used to transmit data, voice and video over both LANs and WANs. ATM uses fixed-length cells to transmit data from source to destination. ATM is also known as BISDN and Cell Relay.

Asynchronous refers to the fact that traffic from an individual user is not periodic.

ARP

Address Resolution Protocol (ARP) is the TCP/IP protocol binding a high-level address (e.g., Internet address), to a low-level physical hardware address. ARP operates across a single physical network only.

B8ZS

Binary Eight Zero Suppression (B8ZS) is a data encoding method for T1 transmission facilities.

Backbone

A high capacity network providing an interconnection among other lower capacity networks. Backbone networks typically carry traffic farthest, sometimes continent-wide.

Bandwidth

Bandwidth represents the transmission capacity of a signal, usually measured in thousands of bits per second (kbps). Bandwidth represents the size of the signal payload, not transmission rate.

For example, if a 1-bit signal is transmitted at a certain rate, and a 2-bit signal is transmitted at the same rate, the 2-bit rate carries a larger volume of traffic per unit of time.

A T1 service delivers 1.544 Mbps, whereas ISDN service delivers 128 kbps.

Bit Error Rate Test

A BER test determines the number of error bits received compared to the total number of bits received. BER is usually expressed as a power of 10.

Bit Rate (BR)

The rate of data transmission in bits per second.

BNC connector

A connector type commonly used for coaxial cable connections.

Bridge

A bridge is equipment that connects two similar networks across another type of network. For example, the Ethernet and Fast Ethernet Mapper are considered bridges because they talk Ethernet at the entry level. In this application, Ethernet traffic is converted or mapped over a SONET backbone and is delivered as Ethernet signals at the other end.

Broadband

A method for transmitting data, voice, and video traffic over significant distances. Broadband uses high-frequency transmission over coaxial cable or optical fibers.

Category System (Cat 1, 2, 3, 4 and 5)

An EIA/TIA LAN specification for cables.

CAT	Rated	Specs, etc.
1		CCIT. No performance criteria
2	1 MHz	RS-232. Used for telephone wiring
3	16 MHz	10BASE-T ISDN
4	20 MHz	10BASE-T. Token-Ring
5	100 MHZ	10BASE-T. 100Base-TX

Central Office (CO)

A telephone company location which joins customer lines to switching equipment. Customers can connect to each other through intra- and inter-city trunk lines.

CLEC

Standing for Competitive Local Exchange Carrier, CLECs offer local telephone services.

Collision

An undesired condition where two packets are being transmitted over a medium at the same time, resulting data destruction.

CSMA/CD

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is a refinement of CSMA. In CSMA/CD, a network equipment stops transmission if it detects a collision.

Data Communication Channel (DCC)

The overhead communications channel in the SONET signal. The DCC is used to send provisioning and management instructions throughout the network. The DCC carries alarm, provisioning, and status information between network nodes.

Data Communication Equipment (DCE)

A DCE is any equipment that maintains and terminates transmission on a network.

Data Terminal Equipment (DTE)

A DTE is the end of a network segment (source or destination). For example, a DTE could be a workstation, repeater, or bridge attaching to a network.

Db

A unit measuring signal strength. dBs are measured by comparing an initial and final level.

dBm

dBm (decibels above one milliwatt) is a logarithmic power measurement based upon the power of one milliwatt.

Driver

Software used to communicate between an operating system and a peripheral device.

DS1

Digital Signal Level 1 (1.544 Mbps) is a SONET signal used in North America.

DS3

Digital Signal Level 3 (44.736 Mbps) is a SONET signal used in North America. A DS3 signal may be divided into 28 DS1s.

E1

A Synchronous Digital Hierarchy (SDH) digital transmission capacity of 2.048 Mbit/s. SDH is used outside North America. E1 is equivalent to DS1 in the SONET signal.

E3

A Synchronous Digital Hierarchy (SDH) digital transmission capacity of 34.368 Mbit/s. SDH is used outside North America. E3 is equivalent to DS3 in the SONET signal.

EC-1

EC-1 (Electrical Carrier) has a line rate of 51.840 Mbps. An EC-1 signal can be constructed in two ways: A DS1 can be mapped into a VT1.5 and 28 VT1.5s are multiplexed into one EC-1 signal, or a DS3 can be mapped directly into an EC1.

Fiber Optics

A digital signal transmission technology that sends light through thin strands of glass.

Firewall

A firewall is equipment or a software that protects a LAN from Internet intruders. Some firewalls known as Proxy Server hide the internal corporate IP Addresses from the outside world and act as a middle man for all the Internet requests.

Hub

A hub is an External Interconnection Device (EID). Acting as a repeater, hubs replicate every incoming message on all other attached ports. This function can be thought of as broadcasting. Hubs are rapidly being replaced by switches in the field as switches have become cheaper and are more intelligent devices.

GUI

A graphical user interface (GUI) lets you operate a computer program using graphical items such as a icons, pull-down menus and lets you interact using a mouse. OverView 1500 is an example of a GUI.

IEEE

The IEEE (Institute of Electrical and Electronics Engineers) is a professional organization involved in creating, promoting, and supporting of specifications and standards for communications.

IEEE 802.3

A standard for physical using the CSMA/CD access method on a LAN using bus topology.

This chart displays characteristics of the major standards.

802.3 Standard	Operating Rate	Max. Segment Length	MAUs/ segment	Medium	Topology
10Base-2	10 Mbps	185 m (607 ft.)	30	Coax.	Bus
10Base-5	10 Mbps	500 m (1640 ft.)	100	Coax.	Bus
10Base-FL	10 Mbps	200 m (6560 ft.)	2	Fiber Optic	Star
10Base-T	10 Mbps	100 m (328 ft.)	2	UTP, cat 3	Star
100Base-Tx	10 Mbps	100 m (328 ft.)	2	UTP, cat 5	Star

FDDI

FDDI (Fiber Distributed Data Interface) is a high-speed networking standard for fiber-optical transmission. The FDDI topology is a dual-attached, counter-rotating Token Ring. The FDDI protocol can also operate over traditional copper wires.

Full Duplex

A channel or device which permits transmission in two directions at the same time. Full Duplex supports bi-directional traffic.

Half Duplex

A channel or device capable of transmitting in two directions, but not at the same time. Half Duplex supports uni-directional traffic.

Internetworking

The concept of communication between devices throughout multiple networks.

Interoperability

The ability of separate networks to connect directly, which enables data to flow between networks without conversion or human intervention.

IP (Internet Protocol)

The gateway protocol which connects networks at the OSI network level and above. IP routes messages across networks.

Jitter

The slight fluctuation of data packets in relation to network timing. Jitter is undesirable and should be minimized.

LAN (Local Area Network)

A network system providing high-speed data transmission throughout a relatively small area. LANs typically include PCs, printers, etc. and are linked by coaxial cable or twisted pair wiring.

Latency

The time between initiating data request and the beginning of signal transfer. Network latency refers to the delay when a packet is momentarily stored, analyzed and then forwarded.

The minimum time required to move data from one point to another. Factors influencing latency are as follows:

1. Physical media limitations (e.g., the time for electricity to pass over copper wires; the time for light to pass through optical-fiber; physical interference from other signals).
2. Signal set-up and break-down time required regardless of connection duration.
3. Signal interfaces.

LED (Light Emitting Diode)

A display technology radiating light at a single frequency when charged.

Loopback

A test sending and receiving a signal to/from a particular location on a network. Loopbacks lets you test the integrity of a particular path.

or

A procedure in which the optical transmit and receive paths of a fiber-optic network are connected together, used to block out alarms during general equipment testing.

Local Loopback (Facility)

Local loopback signals are sent between an application and network access equipment. Test signals travel from the application to the network access equipment and back to the application without travelling over the network.

Remote Loopback (Terminal)

Remote loopback signals are sent between an application and remote equipment across a network. Signals are used to test path integrity across the network.

MAC

MAC (Medium Access Control) is the LAN control circuity converting DTE protocols to those required by the LAN. MAC defines the way workstations access transmission media. The MAC layer is the lower sub-layer of the data link layer protocol for IEEE LANs.

MDI

Medium Attachment Interface (MDI) is the mechanical and electrical interface between a cable medium and a 10BASE-T MAU.

MDI-X

Medium Attachment Interface-Cross Over (MDI-X) provides the same interface as MDI but with crossed pairs. MDI-X is used in a 10BASE-T hub when connecting to a 10BASE-T MAU.

Multiplexing

Combining multiple signals into a common bitstream for transmission over a single communication line or channel. The reverse of multiplexing is demultiplexing, or dividing a data stream into multiple channels.

MUX

Another term for Multiplexer - a device that performs multiplexing.

Network Interface Card

A Network Interface Card (NIC) is the physical interface connecting your PC, laptop, terminal or server to a network.

Network Interface Cards are commonly available in 10, 100, or 1000 Mbps capacity.

Network Redundancy

The characteristic of having more than one connection path between all nodes on a network. Redundancy indicates that if one network connection is cut, network traffic is not lost.

NIC

A Network Interface Card (NIC) is a plug-in expansion board enabling PCs to send and receive data through a network.

Node

An element on a network.

OC-3

Optical Carrier Level 3 Signal (155.52 Mbps). OC-3 is part of the SONET standard.

OC-12

Optical Carrier Level 12 Signal (622.04 Mbps). OC-12 is part of the SONET standard.

OSI

OSI (Open System Interconnection) is a seven layer model designed to standardize data transmission functions so equipment. Standardization enables different manufacturers equipment to be interconnected.

Protocol

The set of rules or conventions which govern information exchange between networked nodes.

RBOC

Regional Bell Operating Company.

Repeater

A hardware device regenerating LAN signals to extend the full length of a network. Repeaters may also converts signals between media at the same time as regenerating the signal.

RJ45

A 10BASE-T standard for connecting UTP cabling.

Router

A network device which stores and forwards data traffic packets from one local or wide area network to another. A router communicates with all network stations and becomes the communication link between the Internet and the corporate LAN.

RS-232

(Recommended Standard-232) A TIA/EIA standard for serial transmission between a PC and peripheral devices (e.g., modem, mouse, etc.). It uses a 25-pin DB-25 or 9-pin DB-9 connector. These cables are normally support a length of 50 feet.

Its normal cable limitation of 50 feet can be extended to several hundred feet with high-quality cable.

SNMP (Simple Network Management Protocol)

A popular network monitoring and control protocol in which activity of each network device is directed to the network management workstation.

STM-1

Synchronous Transport Module 1 (STM-1) is the basic transmission rate defined in the Synchronous Digital Hierarchy (155.52 Mbit/s).

STM-4

STM-4 is defined as part of the Synchronous Digital Hierarchy at a transmission rate of 622 Mbit/s.

Switch

An Ethernet Switch is an intelligent EID that acts as a message redirector. A switch analyzes every MAC address it receives and retransmits messages only to the desired attached port. Switches can perform advanced filtering at the Broadcast, Multicast and protocol level.

T1

North American (SONET) standard for a digital transmission link with a 1.544 Mbit/s capacity.

T3

North American (SONET) standard for a digital transmission link with a 45 Mbit/s capacity, or 28 T1s.

TCP/IP

Widely adopted internetworking protocol which lets applications be shared among PCs, hosts, or workstations in a high-speed communications environment.

Telnet

An interactive terminal emulation protocol operating over TCP/IP. TELNET lets you log in and control a remote computer over a network.

TL1

Transaction Language 1 is a Telcordia defined command-line communications language used to provision and manage nodes on a network.

UTP

Unshielded twisted pair. Wires are twisted to minimize interference from other wires. UTP is widely used for telephone wiring. UTP is more popular than shielded twisted pair (STP) because they are pliable and do not take up as much space as STP wires in areas such as ductwork.

V.35

Describes electrical and connector characteristics for a high-speed synchronous interface between a DTE and a DCE.

VT1.5

Virtual Tributary 1.5, a structure for sub-DS3 switching and transport (1.728 Mbps).

Wander

Wander is the maximum positive or negative phase difference between actual and base signal frequency since the beginning of the test. A frequency alternating above and below the base frequency has positive and negative wander.

Index