



Protection Schemes and Network Topologies

This chapter describes how protection is implemented on the Cisco ONS 15540 ESPx. It also describes the supported network topologies and how protection works in these topologies. This chapter contains the following major sections:

- [About Protection Against Fiber and System Failures, page 2-1](#)
- [Splitter Based Facility Protection, page 2-1](#)
- [Y-Cable Based Line Card Protection, page 2-3](#)
- [Client Based Line Card Protection, page 2-4](#)
- [Trunk Fiber Based Protection, page 2-5](#)
- [Supported Topologies, page 2-6](#)

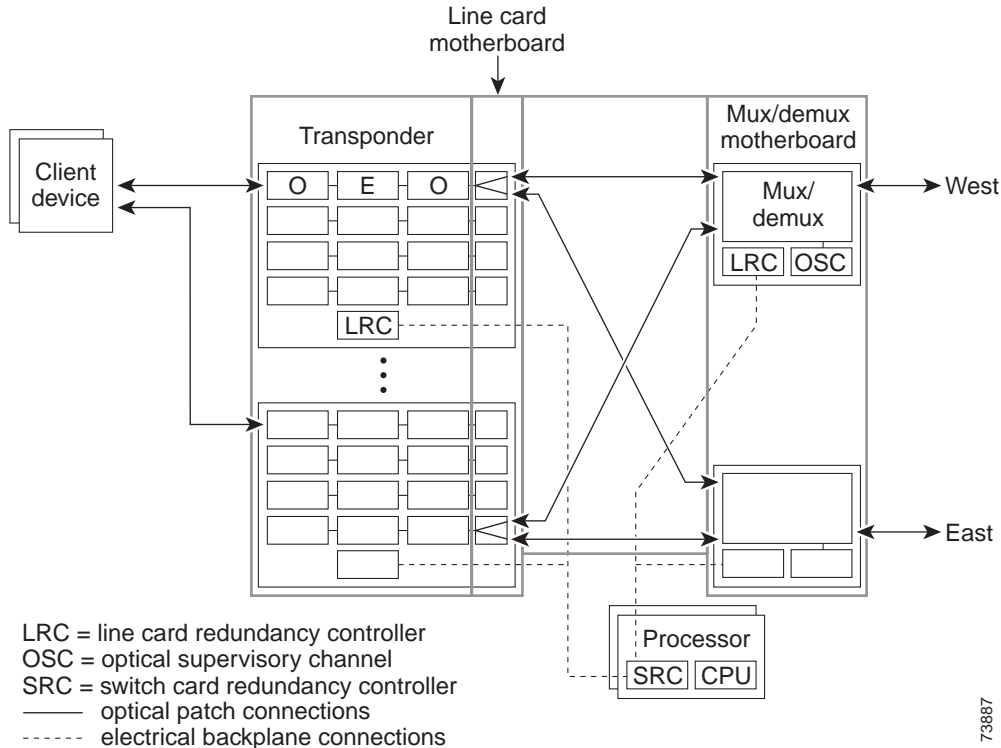
About Protection Against Fiber and System Failures

The design of the Cisco ONS 15540 ESPx provides for two levels of network protection, facility protection and line card protection. Facility protection provides protection against failures due to fiber cuts or unacceptable signal degradation on the trunk side. Line card protection provides protection against failures both on the fiber and in the transponders, which contain the light emitting and light detecting devices as well as the 3R (reshape, retime, retransmit) electronics. Line card protection can also be implemented using redundant client signals. This provides protection against the failure of the client, the transponder, or the fiber.

Splitter Based Facility Protection

To survive a fiber failure, fiber optic networks are designed with both active and standby fibers. In the event of a fiber cut or other facility failure, working traffic is switched to the protection fiber. The Cisco ONS 15540 ESPx supports such facility protection using a *splitter* scheme (see [Figure 2-1](#)) to send the output of the DWDM transmitter on two trunk side interfaces.

Figure 2-1 Splitter Protection Scheme



With splitter protection, a splitter module on the line card motherboard duplicates the DWDM signal from each transponder module. The front panel of the splitter line card motherboard has two MTP connectors for cross connections to the mux/demux modules. The transponder modules signals are transmitted out of both MTP connectors, but in the receive direction, an optical switch selects one signal per transponder module to be the active one. If a failure is detected on an active signal, a switch to the standby signal is made under control of the LRC (line card redundancy controller). Assuming, for example, that the active signal in [Figure 2-1](#) is on the east interface, a failure of the signal on that fiber would result in a switchover, and the signal on the west interface would be selected for the receive signal. APS switchovers are triggered in hardware by loss of light on the receive signal.

Splitter Protection Considerations

The following considerations apply when using splitter protection:

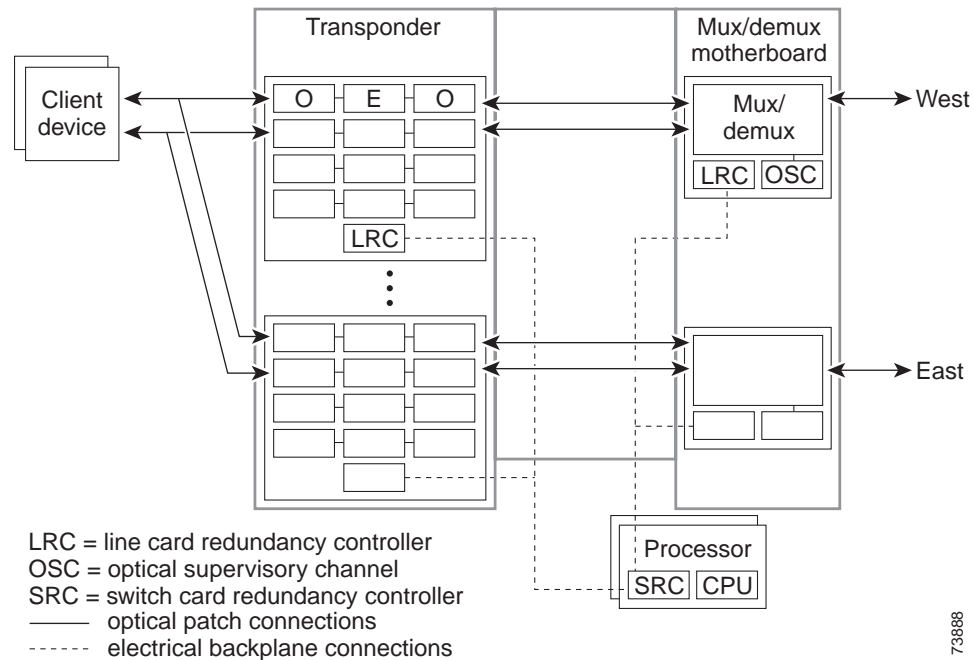
- The splitter protected line card motherboard supports splitter protection. Because the signal splitter introduces 4.6 dB of loss in the transmit direction, we recommend using the unprotected line card motherboards for configurations where splitter protection is not required.
- Switchover after a failure under splitter protection is nonrevertive. After a switchover, manual intervention is required to revert to using the previously failed fiber for the working traffic once the fault has been remedied.

For rules on how to configure the shelf for splitter protection, see [Chapter 3, “Shelf Configuration Rules.”](#) For instructions on configuring the software for splitter protection, refer to the [Cisco ONS 15540 ESPx Configuration Guide](#).

Y-Cable Based Line Card Protection

The Cisco ONS 15540 ESPx supports line card protection using a *y-cable* scheme. Y-cable protection protects against both facility failures and failure of the transponder module. Using an external 2:1 combiner cable (the y-cable) between the client equipment and the transponder interfaces, the client signal is duplicated and sent to two transponder interfaces. [Figure 2-2](#) illustrates this arrangement.

Figure 2-2 Y-Cable Protection Scheme



In y-cable protected configurations, one of the transponder modules functions as the active and the other as the standby. On the active transponder, all the lasers and receivers are sending and receiving the client signal. On the standby transponder, however, the client side laser is turned off to avoid corrupting the signal transmitted back to the client equipment. The performance monitor on the active transponder module optically monitors the signal received from the trunk side. If loss of light, signal failure, or signal degrade is detected, and an acceptable standby signal is available, the system switches over to the standby signal. The precise conditions that trigger a switchover based on signal failure or signal degrade are configurable in the alarm threshold software.

Y-Cable Protection Considerations

The following considerations apply when using y-cable protection:

- Y-cable protection does not protect against failures of the client equipment. To protect against client failures, protection should be implemented on the client equipment itself in addition to the line card protection configuration on the Cisco ONS 15540 ESPx shelf.
- Due to their lower optical power loss, we recommend using the unprotected line card motherboards for configurations with y-cable protection.

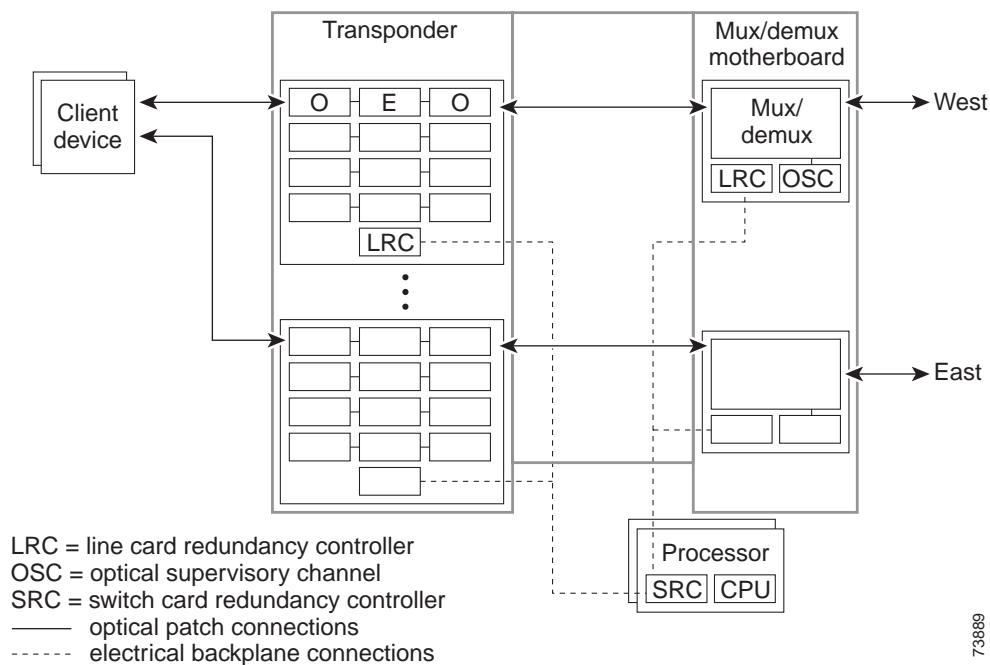
- The APS software that supports y-cable protection can be configured as revertive or nonrevertive. After a switchover, the working traffic can be put back on the previously failed fiber, once the fault has been remedied, either automatically (revertive) or through manual intervention (nonrevertive).
- Y-cable protected configurations allow monitoring of the protection fiber without the OSC.

For rules on how to configure the shelf for y-cable protection, see [Chapter 3, “Shelf Configuration Rules.”](#) For instructions on configuring the software for y-cable protection, refer to the [Cisco ONS 15540 ESPx Configuration Guide](#).

Client Based Line Card Protection

While y-cable protection protects against failures in the transponders or on the fiber, the client still remains vulnerable. For some applications additional protection of the client equipment may be desirable. As [Figure 2-3](#) shows, the same architecture that supports y-cable protection also supports client protection. Rather than using a y-cable to split a single client signal, the client equipment transmits and receives two separate signals. Operationally, client protection is also different in that signal monitoring and switchover are under control of the client rather than the protection mechanisms on the Cisco ONS 15540 ESPx.

Figure 2-3 Client Based Line Card Protection Scheme



Client Protection Considerations

The following considerations apply when using client protection:

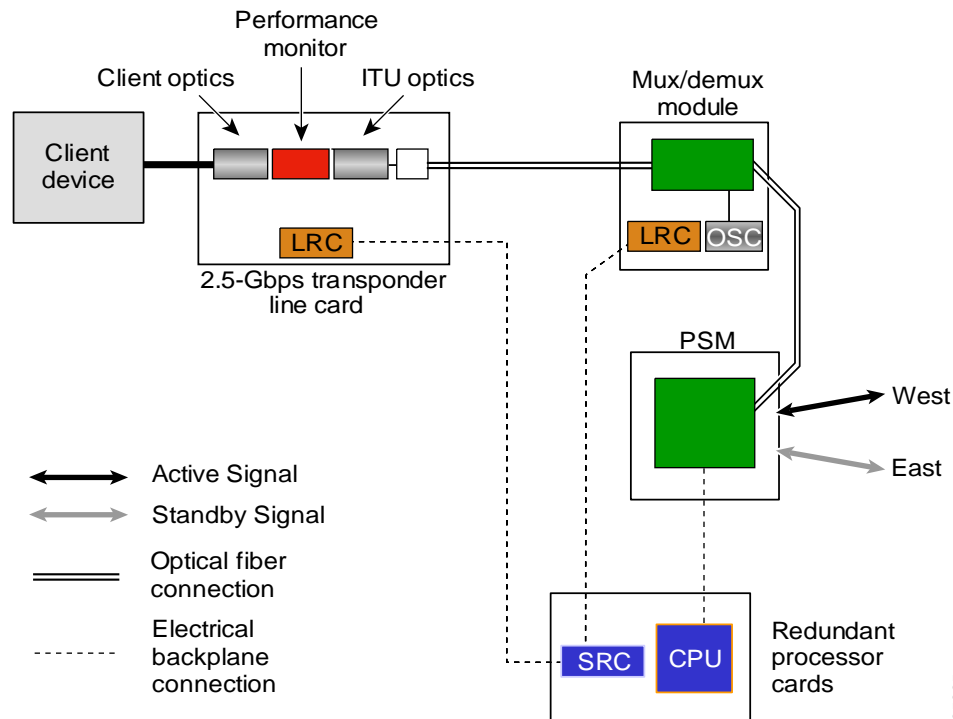
- Client protection uses the same shelf configuration as y-cable based line card protection.
- Due to their lower optical loss, we recommend using the unprotected line card motherboards for configurations with client protection.
- Client protected configurations allow monitoring of the protection fiber without the OSC.

Trunk Fiber Based Protection

The PSM (protection switch module) provides trunk fiber based protection for Cisco ONS 15540 ESPx systems configured in point-to-point topologies. This type of protection only guards against trunk fiber cuts, not specific channel failure as provided by splitter and line card based schemes. However, this protection scheme allows for much simpler shelf configurations in topologies where per-channel protection is not required.

Figure 2-4 shows trunk fiber based protection configured with a transponder line card.

Figure 2-4 Trunk Fiber Based Protection Scheme



Trunk Fiber Based Protection Considerations

The following considerations apply when using trunk fiber based protection:

- Trunk fiber based protection does not protect against failures on the shelf itself or the client equipment. To protect against these failures, line card protection should be implemented on the client equipment itself.
- The APS software that supports trunk fiber based protection can be configured as revertive or nonrevertive. After a switchover, the active traffic can be put back on the previously failed working fiber, once the fault has been remedied, either automatically (revertive) or through manual intervention (nonrevertive).
- Use PSMs only in point-to-point topologies.
- In a dual shelf node, install the PSM on the shelf connected to the trunk fiber.

- The point-to-point topology can have no more than two EDFAs. The cumulative noise of three or more EDFAs interferes with detecting the data channel loss on the PSM.
- When EDFAs are present in the topology, the power of the data channels at the PSM receiver must be greater than the cumulative noise of the EDFAs.

Supported Topologies

The Cisco ONS 15540 ESPx can be used in linear and ring topologies with Cisco ONS 15540 ESP, Cisco ONS 15530, and Cisco ONS 15540 ESPx systems. Linear topologies include protected and unprotected point-to-point and bus. Ring topologies support add/drop nodes and can be hubbed or meshed. The following sections give a brief overview of these topologies.

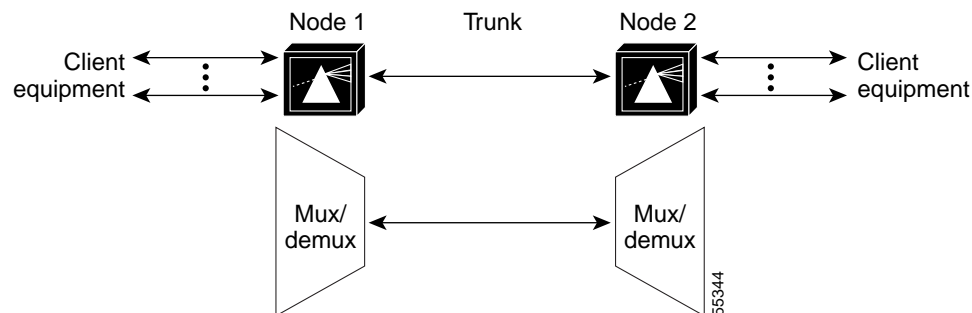
Linear Topologies

In a pure point-to-point topology all channels terminate on the nodes at each end of the trunk. Point-to-point topologies have many common applications, including extending the reach of GE or SONET, and can be configured for unprotected or for protected operation.

Unprotected Point-to-Point Topology

Figure 2-5 shows a point-to-point topology without protection. In this configuration only one optical mux/demux slot is used in each of the nodes. The west or east trunk side interface (mux/demux slot 0 or 1) of node 1 connects to the corresponding interface on node 2.

Figure 2-5 Unprotected Point-to-Point Topology



For an example configuration of an unprotected point-to-point topology, see the “[Unprotected 32-Channel Point-to-Point Configuration](#)” section on page 5-13.

Protected Point-to-Point Topology

Figure 2-6 shows a protected point-to-point topology configured for splitter or line card per-channel protection. In either case, there are two trunk side interfaces, west and east, connected by two fiber pairs.

Figure 2-6 Splitter and Line Card Protected Point-to-Point Topology

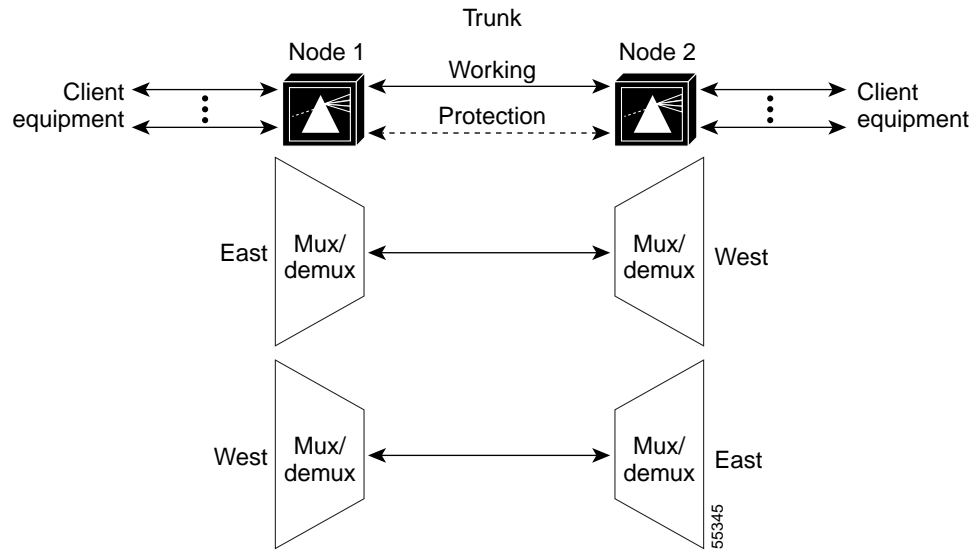
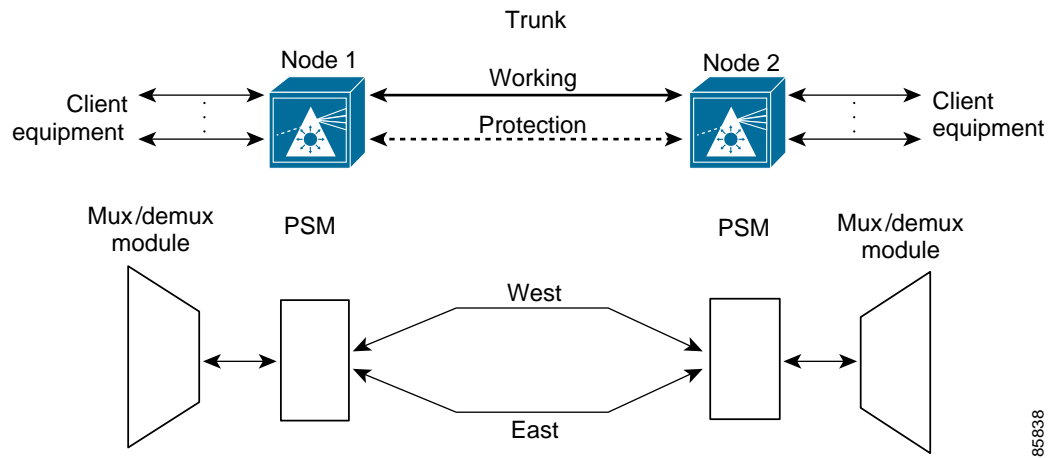


Figure 2-7 shows a protected point-to-point topology configured for trunk fiber protection. There are two trunk side interfaces, west and east, connected by two fiber pairs.

Figure 2-7 Trunk Fiber Protected Point-to-Point Topology

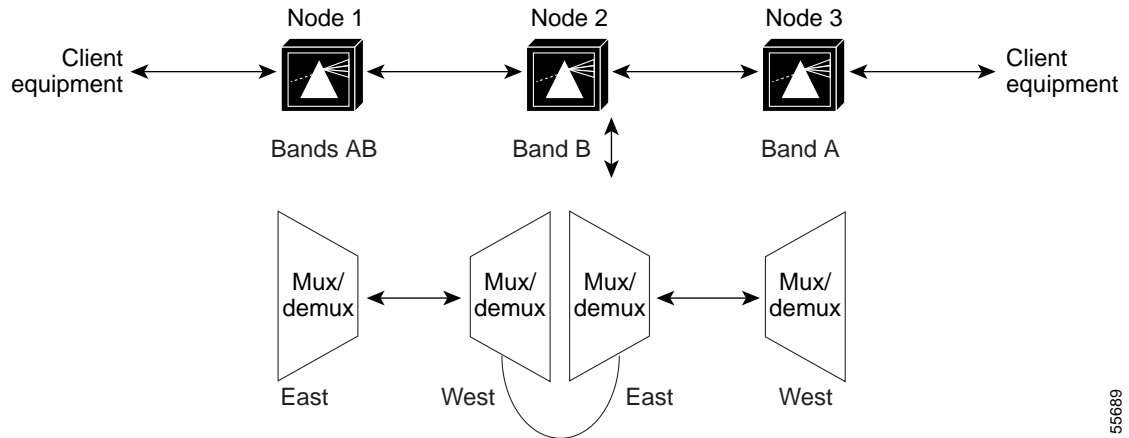


For an example configuration of a protected point-to-point topology, see the “Line Card Protected 16-Channel Point-to-Point Configuration” section on page 5-17.

Bus Topology

In a bus topology, sometimes called *linear add/drop*, there is an intermediate add/drop node between the two terminal nodes. Figure 2-8 shows an example of this type of topology. Bands A and B (channels 1-4 and 5-8) terminate at node 1. Band B is dropped at node 2, which passes band A through. To support this configuration, the add/drop node must have add/drop mux/demux modules in both slots 0 and 1 for west and east directions.

Figure 2-8 Bus Topology Example



55689

This type of topology offers limited protection. In this example a failure on the link between node 2 and node 3 would result in the loss of band A, but band B would remain operational between nodes 1 and 2. A failure on the link between node 1 and node 2 would result in a loss of both bands.

**Note**

If protection for all bands is required in a topology such as this, where there is a single add/drop node between two terminal nodes, a ring can be used.

Ring Topologies

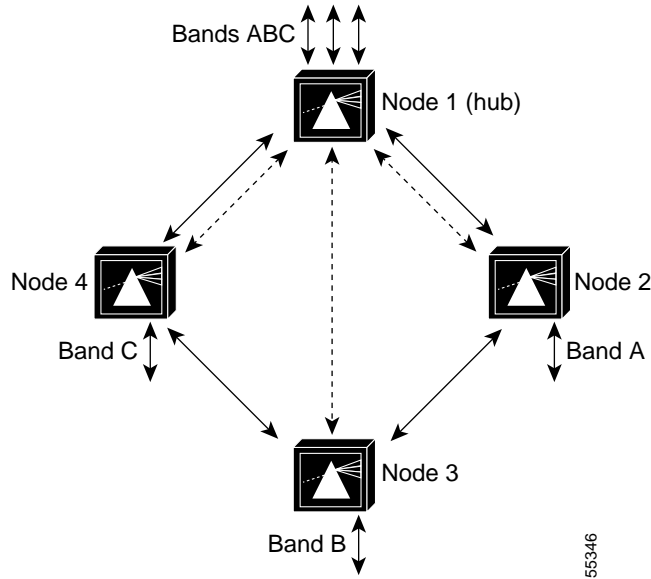
In a ring topology, client equipment is attached to three or more Cisco ONS 15540 ESPx, Cisco ONS 15540 ESP, and Cisco ONS 15530 systems, which are interconnected in a closed loop. Channels can be dropped and added at one or more nodes on a ring. Rings have many common applications, including providing extended access to SANs (storage area networks) and upgrading existing SONET rings. In the cases where SONET rings are at capacity, the SONET equipment can be moved off the ring and connected to the Cisco ONS 15540 ESPx, Cisco ONS 15540 ESP, or Cisco ONS 15530 systems. Then the SONET client signals are multiplexed and transported over the DWDM link, thus increasing the capacity of existing fiber.

Hubbed Ring

A hubbed ring is composed of a hub node and two or more add/drop or satellite nodes. All channels on the ring originate and terminate on the hub node. At the add/drop node, some channels are terminated and regenerated (dropped and added back) while other channels (express channels) are passed through optically, without being electrically regenerated.

Channels are dropped and added in bands. Figure 2-9 shows a four-node hubbed ring in which bands ABC terminate on node 1. Nodes 1 and 2 communicate using band A, nodes 1 and 3 communicate using band B, and nodes 1 and 4 communicate using band C.

Figure 2-9 Hubbed Ring Topology Example



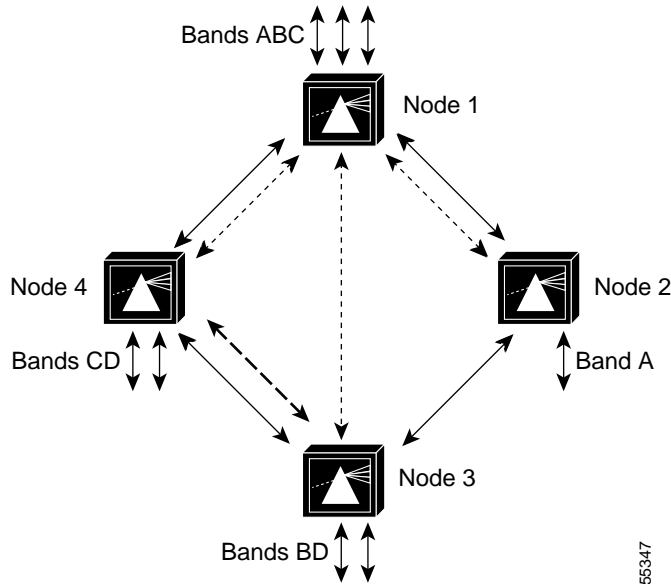
For example configurations of hubbed ring topologies, see the “[Hubbed Ring Topologies](#)” section on [page 5-21](#).

Meshed Ring

A meshed ring is a physical ring that has the logical characteristics of a mesh topology. While traffic travels on a physical ring, the logical connections between individual nodes are meshed. An example of this type of configuration, which is sometimes called a *logical mesh*, is shown in [Figure 2-10](#).

Nodes 1 and 2 communicate using band A, nodes 1 and 3 communicate using band B, and nodes 1 and 4 communicate using band C, as in the previous example ([Figure 2-9](#)). In this example, however, the fact that nodes 3 and 4 communicate independently using band D makes it a meshed ring.

Figure 2-10 Meshed Ring Topology Example



For example configurations of meshed ring topologies, see the [“Meshed Ring Topologies”](#) section on page 5-44.

Protection in Ring Topologies

Protection in the Cisco ONS 15540 ESPx is supported using per-channel unidirectional path switching or bidirectional path switching. Protection mechanisms are implemented in both the hardware and the APS software.

Unidirectional Path Switching

Unidirectional path switching is based on a variant of the SONET UPSR (Unidirectional Path Switched Ring). For each channel on a ring, traffic is transmitted in both directions from each node, using one of the fiber pair for each direction; on each node, traffic is received from one direction. In the event of a failure of the receive signal at a node, the node switches over to receive the signal from the other direction. Switching decisions are made on a node-by-node basis, and some channels can be received from one direction while others are received from the other direction. Protection in rings can be implemented on the Cisco ONS 15540 ESPx using either a splitter or y-cable configuration.

Figure 2-11 shows a three-node hubbed ring. In the example, node 1 is sending traffic from both east and west mux/demux interfaces, but is actively receiving only on the west side.

Figure 2-11 Per-Channel Unidirectional Path Switching in Normal State

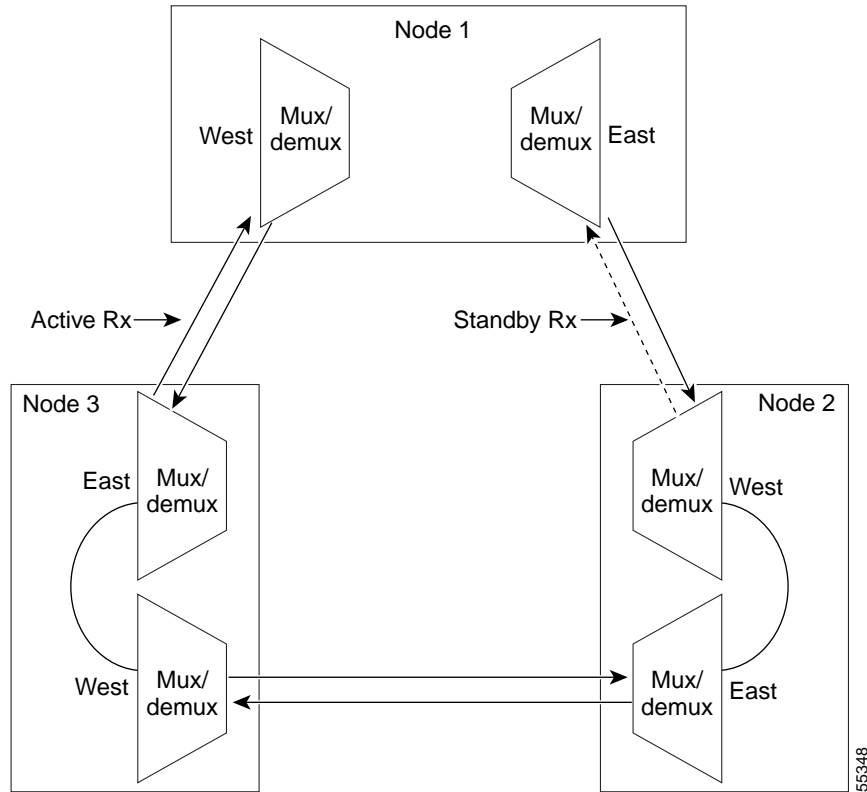
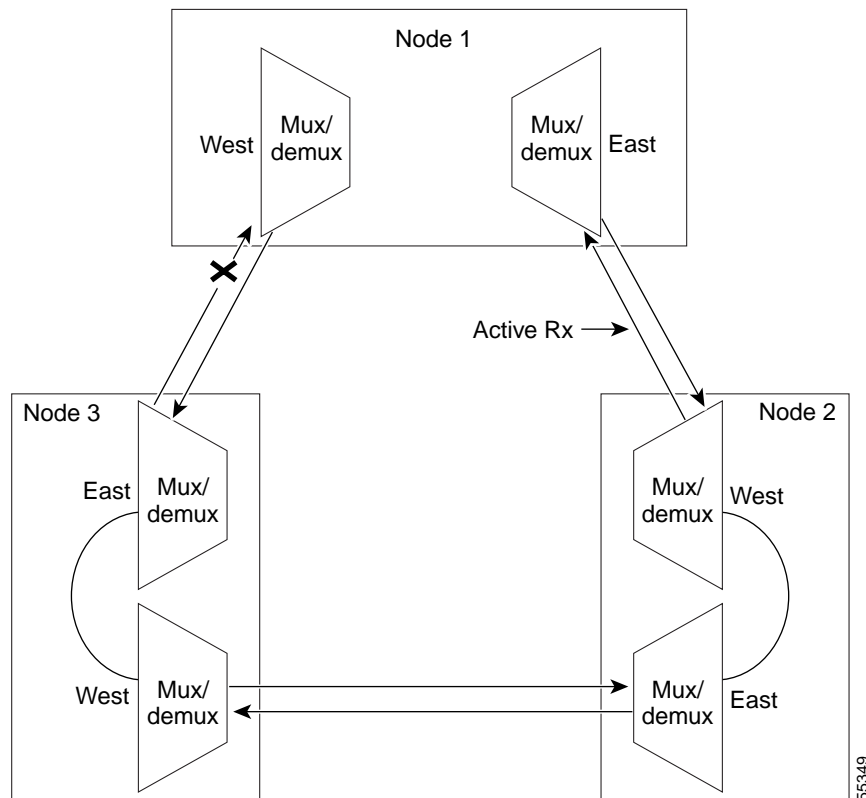


Figure 2-12 shows a channel failure on the receive signal from node 3 to node 1. In this event, node 1 switches to the receive signal on its east mux/demux interface for the failed channel(s). Assuming that the failure is only in one direction between node 1 and node 3, node 3 would not be required to switch receive directions. If, however, both directions were affected (for example, a fiber cut) and node 3 had been receiving on its east side, it would switch to the west side for its active receive signal.

Figure 2-12 Per-Channel Unidirectional Path Switching after Protection Switch



Bidirectional Path Switching

The Cisco ONS 15540 ESPx also supports bidirectional path switching through the APS software. When configured for bidirectional switching, a node that detects a fault sends a signal over the APS message channel to the source node to also switch its receive direction. Assume, for example, that the channels configured between node 1 and node 3 in Figure 2-12 were communicating over the link that fails. When node 1 switches to receive those channels from the east side (over node 2), node 3 would also switch to receive those channels from its west side. This ensures that the distance between the two nodes remains the same for those channels for the active signal. This option is supports protocols that are distance sensitive.

Multiple Trunk Support

The Cisco ONS 15540 ESPx allows two or more trunks to connect to a single shelf. Both point-to-point topologies and ring topologies are allowed in a multiple trunk configuration. All of the trunks can support optical protection but the OSC will only be available as the APS message channel and network management for one trunk. The other trunk must use either the in-band message channel or an IP connection for the APS message channel and network management.