CHAPTER 6

Next Generation Optical Networks

6.1 INTRODUCTION

A mesh optical network consists of several cross-connecting nodes (Figure 6.1). Some nodes are O-E-O and some all optical. Large nodes are capable of carrying aggregate traffic at extremely high capacities, and also to add–drop and groom traffic. Each interconnecting link consists of many dual fibers (one fiber per direction), and they include signal conditioners (equalization and regeneration) when the optical signal is transported over distances of hundreds of kilometers. The mesh network has excellent protection strategies, as nodes may be reprovisioned to reroute traffic away from the failure condition (fiber cut or failed node). Faults are detected with power detectors and performance parameter thresholds. Reconfiguration may be made autonomous by switching to protection to SONET/SDH standards (switch to protection takes less than 50 ms). Reconfiguration may also be accomplished via network management procedures. More sophisticated management protocols perform reconfiguration to provide traffic balancing and traffic grooming.

The Unidirectional Path Switched Ring (UPSR) is a popular and well-studied network topology (Figure 6.2). It is most applicable to small and medium-size LANs and metropolitan ring networks (metros). It consists of a dual-fiber counterrotating ring. Each ring passes the same traffic but in opposite directions (one ring is for service and the other for protection).

1. When a link fault occurs on the service ring, the UPSR is able to detect it (with power detectors and performance parameter thresholds) and reconfigure itself by switching to protection ring. Switch to protection typically complies with SONET standards (<50 ms).
2. When a single fiber link is at fault, then the ring without faults is used.
3. When both fibers on a span are at fault, then traffic is passed from one ring onto the other by looping back at the nodes adjacent to the fault. This is also known as span protection and the action is known as self-healing. The typical bandwidth on the ring is OC-48. In DWM rings, coarse wavelengths (20 with 400 Ghz separation) are used.

Next Generation SONET/SDH, by Stamatios V. Kartalopoulos
ISBN 0-471-61530-7

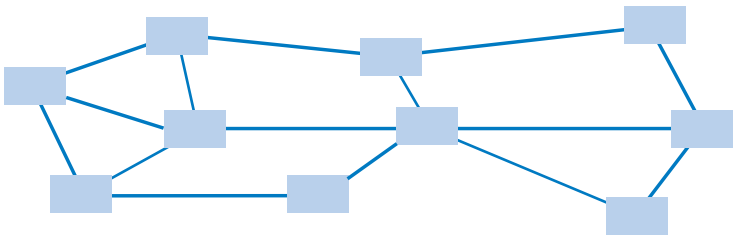

Figure 6.1 A mesh optical network consists of cross-connecting nodes, O-E-O or all optical.

The Two-Fiber Bidirectional Line Switched Ring (2f-BLSR) is also a popular and well-studied network topology (Figure 6.3). It is most applicable to small and medium-size LANs and Metropolitan ring networks (metros). It consists of a dual fiber counterrotating ring. In this scheme, half of the bandwidth on the ring is allocated to protection. Thus, if each ring uses an OC-48, STS-1 #1 to #24 are used for traffic and STS-1s #95 to #48 are allocated for protection. When a single fiber cut occurs, the traffic is routed over the healthy ring and it uses the allocated available bandwidth, in which case all STS-1s are used #1 to #48. In DWM rings, coarse wavelengths (up to 20 with 400 Ghz separation) are used. Switch to protection complies with SONET standards (<50 ms).

The Four-Fiber Bidirectional Line Switched Ring (4f-BLSR) is a popular and well-studied network topology (Figure 6.4). It is most applicable to medium and large-size LANs and Metropolitan ring networks (metros). It consists of two dual-fibers with counterrotating rings. In this scheme, the 4f-BLSR combines both ring and span protection. Ring protection transfers traffic onto the healthy dual ring and span protection wraps around (or loops back) traffic from one ring onto the other to

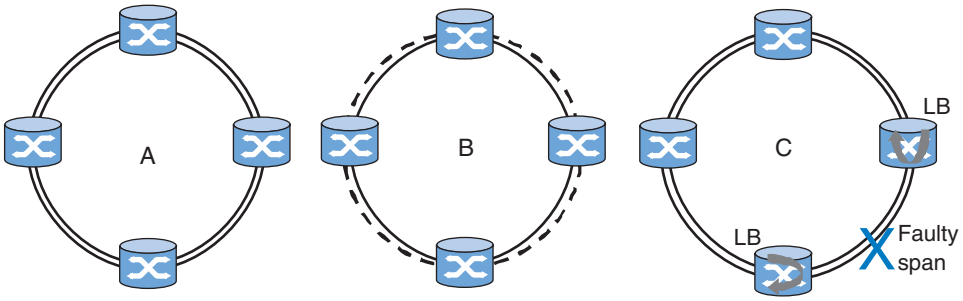

Figure 6.2 The Unidirectional Path Switched Ring consists of a dual-fiber counterrotating ring. Each ring passes the same traffic but in opposite directions (A). When a link fault occurs on the service ring, the UPSR detects it and reconfigures itself by switching to protection ring. When a single fiber link is at fault, then the ring without faults is used (B). When both fibers are at fault, then traffic is passed from one ring onto the other by looping back at the nodes adjacent to the fault (C).

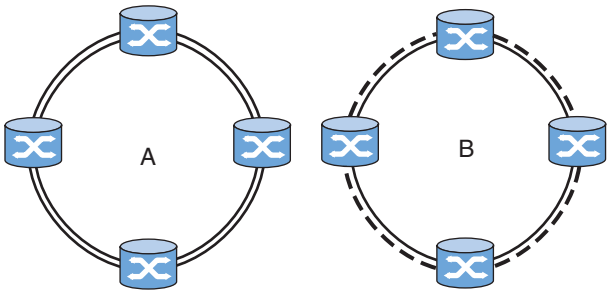

Figure 6.3 The Two-Fiber Bidirectional Line Switched Ring consists of a dual-fiber counterrotating ring (A) but only half of the bandwidth is allocated to the protection ring. When a single-fiber cut occurs, the traffic is routed over the healthy ring and it uses the allocated available bandwidth (B).

avoid the faulty link or span. In WDM 4f-BLSR rings, coarse (20 with 400 Ghz separation) or dense wavelengths (40 with 100 Ghz separation) are used. The typical rate per wavelength is in the range OC-48 to OC-192. Switch to protection complies with SONET standards (<50 ms).

6.2 NEXT GENERATION OPTICAL RINGS

The Next Generation Optical Ring (NG-OR), depending on application, will be UPSR, 2f-BLSR, or 4f-BLSR. However, each fiber carries many wavelengths, from

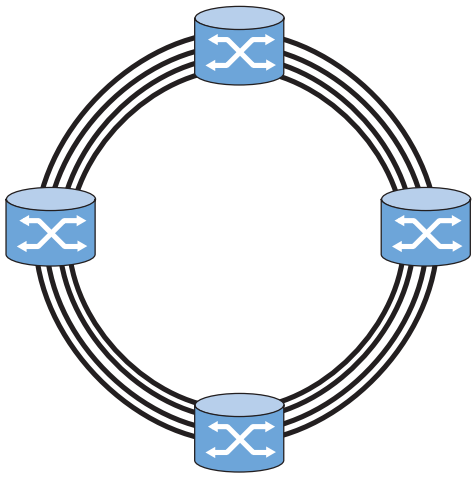

Figure 6.4 The Four-Fiber Bidirectional Line Switched Ring consists of two dual fibers with counterrotating rings. It combines both ring and span protection.

coarse (20 wavelengths + 1 or 2 for supervision) to dense (up to 80 per band with 2 or 4 for supervision). In addition, each wavelength will be modulated at different bit rates, spanning from OC-48 to OC-192, and, in certain cases, OC-768. Some wavelengths may also carry raw 1 GbE or 10 GbE. The ring nodes will consist of two functions: a purely optical add–drop multiplexer (OADM) that drops and adds one or more specific wavelengths from–to the ring (known as the optical regime), and a network element that disaggregates/aggregates traffic (in the electronic regime). As a consequence, the network element function receives a diverse client payload of synchronous and asynchronous data and is able to encapsulate in GFP and map in NG-S frames.

One of the key issues that is currently under intense study is the wavelength assignment (WA) on a static and dynamic capacity. These studies also include protection strategies on the fiber and on the wavelength level. The key objective is to protect traffic and preserve traffic integrity, which must be maintained when a wavelength degrades beyond the acceptable threshold or when a fault occurs. Clearly, a fiber cut or a faulty laser do not invoke the same protection mechanisms.

Thus, the NG-OR must exhibit advanced fault detection strategies and advanced signaling protocols. In addition, other design issues need to be resolved, such as amplification, equalization, wavelength conversion, and management.

Taskforces, such as the IETF, aim to address and resolve the above issues with the generalized multiprotocol label or lambda switching (GMPLS), an evolution of the multiprotocol label switching (MPLS) standard.

Thus, the network elements in the NG-OR support a variety of interfaces to provide aggregation, grooming, and switching capabilities. They respond to alarm and

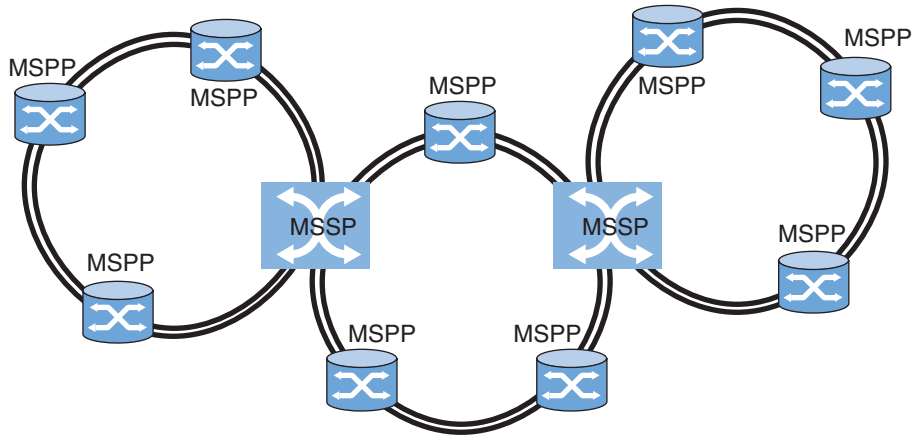

Figure 6.5 The NG-OR supports the multiservice provisioning platform (MSPP). NG-OR network elements are able to connect two or more NG-Ors, and they support the multiservice switching platform (MSSP).

error SONET/SDH conditions and, thus, they support the multiservice provisioning platform (MSPP).

Some network elements provide bandwidth and wavelength management via large, nonblocking switching fabrics (cross-connects) on the NG-OR. They are able to connect two or more NG-Ors and they support the multiservice switching platform (MSSP) (Figure 6.5).

6.3 SHARED RINGS

The Path Protected Mesh Network (PPMN) may be viewed as consisting of many NG-ORs interconnected with large MSSPs that are capable of carrying aggregate traffic at extremely high capacities (Figure 6.6). The network elements of the PPMN are MSPPs capable of aggregating a variety of client data, including voice/video, and of adding–dropping and grooming traffic. Each interconnecting link consists of few or many dual fibers (fiber per direction), and signal transport may depend on signal conditioners (equalization and regeneration) to be able to transport the optical signal over distances of hundreds of kilometers.

6.4 PROTECTION

The PPMN network has a protection strategy that combines the best of both ring and mesh protection (Figure 6.7). Nodes may be provisioned to reroute traffic away from a failure condition (fiber cut, failed node, or failed wavelength). Faults are detected with power detectors and performance parameter thresholds. Reconfiguration may be autonomous by switching to protection (ring or wavelength) according

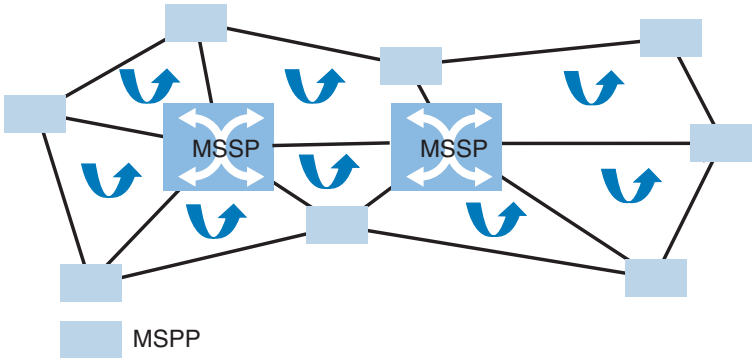

Figure 6.6 The Path-Protected Mesh Network (PPMN) may be viewed as consisting of many NG-ORs interconnected with large MSSPs. The network elements of the PPMN are MSPPs capable of aggregating a variety of client data, including voice/video, and able to add–drop and groom traffic.

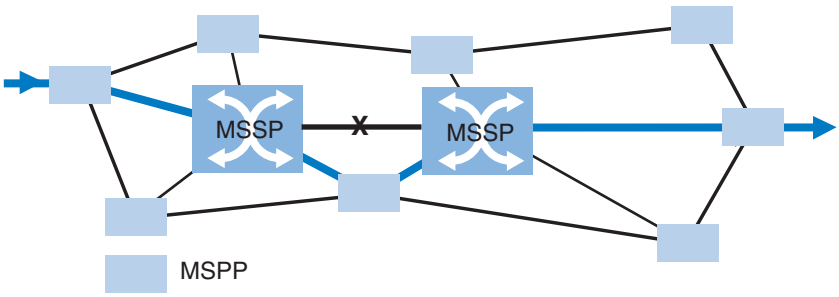

Figure 6.7 The PPMN network has a protection strategy that combines the best of both ring and mesh protection. PPMN can also resolve multiple failure conditions.

to SONET/SDH standards (switch to protection takes less than 50 ms) and according to new wavelength management strategies. Reconfiguration may also be via sophisticated management protocols that perform traffic balancing and traffic grooming. PPMN can resolve multiple failure conditions on the network as well as on the channel (wavelength) level. However, rerouting a channel needs to address the end-to-end wavelength assignments over the path with nodes that support or may not support wavelength conversion; this may slow down and complicate the protection process.

Two key strategies for switching to protection are possible (Figure 6.8). One strategy is based on predetermined redundant paths. For every possible path, another path has been identified as the best alternate. Thus, when a fault occurs on the working path, a quick switch is performed by looking up the table that contains the alternate path. This is the fastest "switch to protection" strategy, although the protection path may not be the best possible path at the time of failure, as congestion conditions may occur unpredictably.

Another strategy is based on algorithms (e.g, the shortest path, constraint-based, such as the least congested path or most available path, and others well-known from

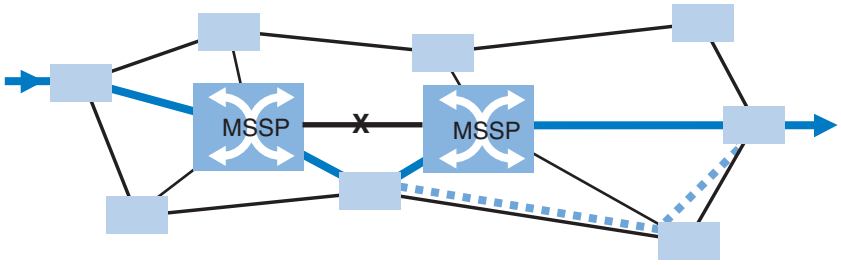

Figure 6.8 The PPMN switch to protection path is either based on predetermined redundant paths or on algorithms (the shortest path, constraint-based). It may also combine quick algorithms based on network metrics

the Generalized Multiprotocol Label Switching (GMPLS) to identify the best possible path available. Such algorithms require knowledge of the status of nodes on the network, and, therefore, they require extensive signaling and complex protocols. Such algorithms are slow in finding the protected path but they do find the best available at the time.

Yet another strategy may combine quick algorithms that, based on network metrics, identify the best available protection path from a set of predetermined redundant paths.

6.5 NETWORK MANAGEMENT

The Telecommunications Management Network (TMN) is a hierarchical network that enables telecommunication service providers to communicate across operating systems and telecommunications networks and to achieve interconnectivity and control of network resources. The existing TMN communicates between the operations support system (OSS) and network elements (NEs) using standardized protocols. NEs are distribution systems, switching systems, access systems, and so on. The TMN consists of five layers (Figure 6.9).

A network consists of interconnected NEs (Figure 6.10). This is known as the network element management layer (NEL). Each network that consists of NEs is complex and has its own element management system (EMS). This is known as the element management layer (EML). EMSs abstract (or filter) relevant aspects from NEs and communicate them via a northbound interface to NML. In a multivendor network, the communication protocol between a NE and its corresponding EMS may be proprietary or standard, such as Transport Language 1 (TL1), Simple Net-

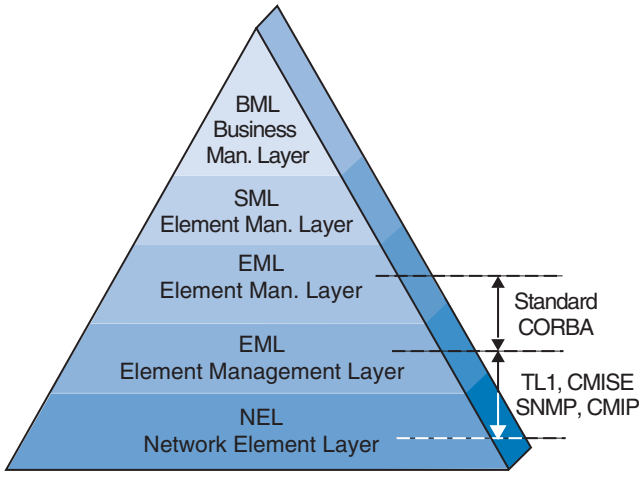

Figure 6.9 TMN consists of five layers.

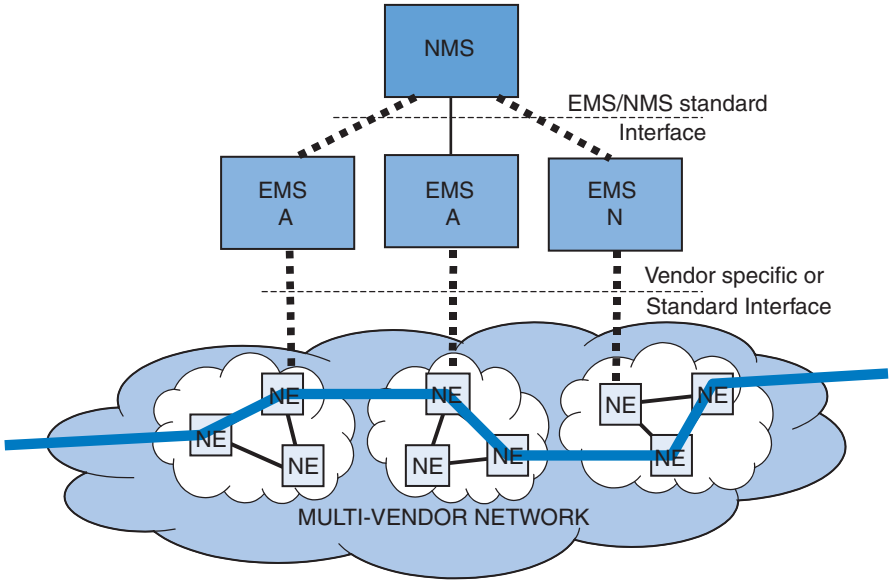

Figure 6.10 A multivendor network consists of interconnected NEs. NEs are connected with the NMS via EMSs.

work Management Protocol (SNMP), and so on. Above the EMS is the network management layer (NML). In this layer, the network management system (NMS) manages the network and systems for capacity, congestion, and diversity. The NE-specific EMSs communicate with the NMS via an open, standard, northbound interface. Above the NML is the service management layer (SML), which is responsible for service quality and cost. The highest layer is the business management layer (BML), which is responsible for market share, and so on.

The EMS plays a key role in maintaining both NEs and transmission facilities. It is the primary repository of detailed history of NE-specific faults, QoS, events, technicians' actions, and performance data. The EMS model includes service provisioning, service assurance, EMS and NE operations support, and automation enabling. Some of the EMS tasks are:

- Install the NE (load parameters, autodiscover the NE equipment, establish and verify connectivity).
- Collect data used to determine whether the service provided matches subscribers' usage characteristics and to forecast demand.
- Provision and plan for capacity (autodiscover NE components, provide inventory information and information on available capacity).
- Upgrade the NE (autodiscover new equipment, download software upgrades, maintain concurrency between EMS and NE software and hardware releases).

- Protect NEs and EMS database integrity (back up and restore databases, monitor loss of NE–EMS connectivity, resynchronize database when connectivity is lost).
- Ensure that the purchased service is provisioned as agreed upon and delivered. This includes network maintenance and restoration and network monitoring and control.
- Periodically collect quality metrics to characterize the performance of network resources and discover degradation trends.
- Support fault management to ensure that the provided service remains available and at the agreed upon QoS. This involves the proactive monitoring of network resources to detect degradations and faults, performance, and utilization parameters.
- Ensure that the quality metrics (QoS) characterizing the network performance remain within the agreed upon limits.
- Measure subscriber usage of the resources for billing. This applies only to those NEs that provide a chargeable function, such as connection and call setup.

The NML has three primary functions:

- Fault management and root-cause analysis
- Integrated end-to-end service provisioning of multivendor and multitechnology networks. Service provisioning encompasses tasks such as equipment installation, capacity planning, capacity provisioning, and NE database integrity upgrading and protecting
- Integration between the EML and SML

NML, SML, and BML perform high-level management processes, such as network inventory, development and planning, network configuration, and network provisioning.

- Inventory management keeps a detailed record of all NE resources in the subnetwork: locations, types of equipment, model numbers, serial numbers, versions, installation dates, and more.
- Configuration management performs gross control of subnetwork resources, topologies, and redundancies. It includes the installation and turn-on of new equipment resources, the assignment of resources to trunk routes or service areas, and network protection switching. It may also include the partitioning of resources into virtual private networks (VPN).
- Provisioning involves the creation of specific connections or the enabling of specific subnetwork features, including QoS, which are assigned to a specific subscriber for an agreed upon period.

Thus, the existing TMN is a system that consolidates functionality related to network resource management, monitoring, and controlling and assures the consistent performance of the network and services. This model allows for backward compatibility with existing operating systems (OSs), different databases (DBs), and different programming languages (PLs).

ITU-T has partitioned the general management functionality offered by systems into five key functional areas: **F**ault, **C**onfiguration, **A**ccounting, **P**erformance, and **S**ecurity, known as FCAPS. FCAPS is not the responsibility of a specific layer of the TMN architecture but portions of FCAPS functionality are performed at different layers. For example, as part of fault management, the EML logs in detail each discrete alarm or event. It then abstracts (filters) this information and forwards it to an NMS (at the NML layer) that performs alarm correlation across multiple nodes and technologies and root-cause analysis.

The Next Generation Optical Network will capitalize on this architecture but it will have a much simplified management protocol suite to manage network elements at the access, medium and large metro, backbone, and linear point-to-point with add–drops. Many management functions currently residing in the three lower layers (NML, SML, and BML), such as partial fault management, may be pushed down to the NEs, and new functions may be included to address specific multiwavelength DWDM issues such as wavelength assignment and reassignment, wavelength assignment verifications, bandwidth balancing, autonomous protection, and so on.

6.6 BANDWIDTH MANAGEMENT

Consider a network of resistors and a voltage across it. Current flows through it continuously in the most efficient manner according to network parameters (the resistance, in this case) (Figure 6.11). Each resistor represents the link load of the net-

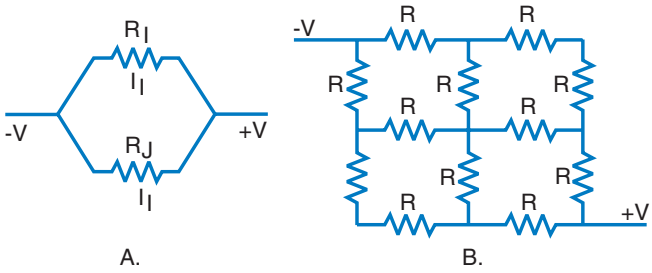

Figure 6.11 An analog paradigm. A resistor network automatically adjusts the current flow according to the resistance (load) of each branch without additional intelligence. (A) As the load R_I or R_J varies, the current flow is automatically adjusted accordingly. (B) A similar action takes place in a more complex network. The Next Generation Optical Network, although not analog, will also automatically adjust the traffic flow according to traffic load.

work. As the value of one of the resistors changes, an automatic balancing action takes place without external protocols and controllers (Figure 6.11A). Such balancing action also takes place in complex networks (Figure 6.11B). The Next Generation Optical Network consists of network elements and fiber links. Each fiber link has a maximum traffic capacity that is calculated from the product of (number of wavelength) × (bit rate per wavelength). However, the effective traffic per wavelength is less than the bit rate, as many packets are idle or non-customer-related. Thus, assuming that all network elements can handle the same amount of traffic, bandwidth management addresses the issue of balancing the effective traffic per link as the resistors network does—fast, efficiently, without excessive complexity, and cost-efficiently on both the fiber level (aggregate) and on the wavelength level.

The Next Generation Optical Network, although in principle not analog, will automatically adjust traffic in a similar manner by monitoring the traffic density at every node. Unfortunately, the Next Generation Optical Network is challenged to manage an unprecedented variety of traffic types. The difficulty with traffic management in this case lies in the large variety of different types, such as:

- Real-time voice (bidirectional) transported by circuit-switched TDM networks
- Real-time compressed voice (bidirectional) transported by circuit-switched TDM networks
- Non-real-time voice (unidirectional) for "store and forward" applications (such as voice messaging)
- Real-time video (unidirectional) adapted in DS-n or packetized
- Real-time video interactive (bidirectional)
- Non-real-time video for "store and forward" applications (real-time only in the access network)
- Packetized data: small packets for fast transactions such as authorization, ID verification, reservations, and cash transactions (ATM, cash registers, etc.)
- File transfers: large packets and bursty, mostly unidirectional transmission, for fast, slow, or best-effort transport
- Data (mostly unidirectional, and in some applications interactive) for home security, surveillance, and emergency use. In specific applications, data is real-time and almost continuous, such as in air-traffic control.
- Data or packets for new applications with parameters to be defined

Clearly, such a variety of traffic types impacts the design complexity of the network element, protection strategy, network architecture, network fault management, and bandwidth management.

6.7 WAVELENGTH MANAGEMENT

In current DWDM systems, each wavelength is used as a separate channel and, thus, the wavelength assignment may be fixed over the complete path (end-to-end)

in the network, even if the path is through several subnetworks managed by different network (domain) operators (Figure 6.12).

When the best path is found, a wavelength assignment over the path is made. This path may consist of the same wavelength, end-to-end, or it may consist of a specific concatenation of wavelengths over the end-to-end path (Figure 6.13).

The first method presents its limitations as protection may not be supported. However, this wavelength assignment is simple since the end-to-end protocol is either simple, or it is not required if the wavelength value is in the packet label. The second method requires wavelength conversion and, thus, the wavelength assignment is more complex as input–output tables at each node need to be constructed. In this case and during protection or traffic congestion, dynamic wavelength reassignment is required. Dynamic wavelength assignment and reassignment that meets fast switching objectives requires fast and intelligent algorithms as well as sophisticated monitors. Wavelength conversion adds to cost, but as technology advances, cost is expected to decrease.

However, it is important to identify certain issues pertaining to the two methods (single-wavelength assignment and concatenated-wavelength assignment). In the case of the same-wavelength assignment over the complete optical path (Figure 6.12), each node on the path has been provisioned with the input–output–wavelength association. That is, each node "knows" where a wavelength comes from (input) and where it goes to (output). However, in the case of wavelength conversion, how does the next node on the path "know" where the converted wavelength is and where it is destined to? Figure 6.13 illustrates *N* signals converted from one wavelength to another as they travel through and are switched by six nodes.

Thus, in the Next Generation Optical (DWDM) Network the issue of wavelength management is new since it did not exist in legacy single-wavelength optical (such as SONET) or nonoptical systems and networks. In fact, in dynamically wavelength-configurable DWDM networks, wavelength blocking may occur as wavelengths are switched from one fiber to another.

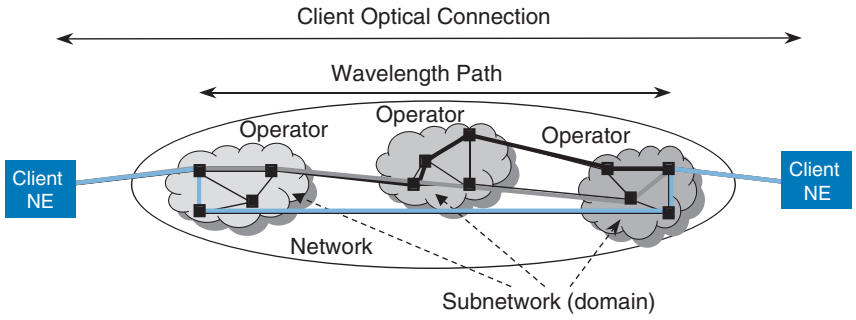

Figure 6.12 A network consists of subnets. Each subnet consists of a few hundred nodes. Each node has fiber connectivity to other nodes with fiber pairs (one fiber per direction). Each subnet may be managed by a different operator.

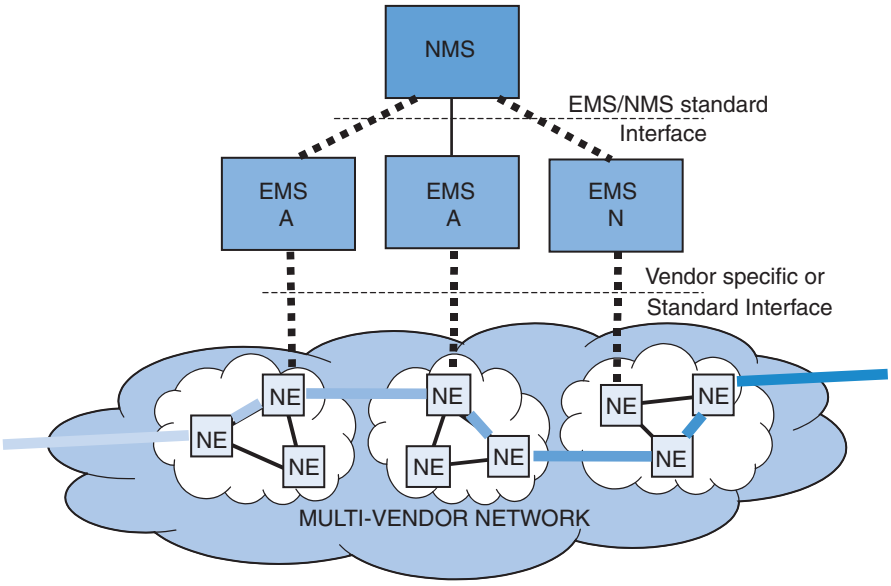

Figure 6.13 Concatenation of wavelengths over the end-to-end path requires wavelength converters and protocols to help construct wavelength conversion tables. In a multivendor network, protocol compatibility and interoperability become equally important.

To study the wavelength assignment and the blocking issue, consider a (DWDM) network element with a switching fabric. To this node, K fibers with N channels each (wavelengths) are in the ingress direction and K fibers in the egress. Thus, there are $N \times K$ wavelengths to be switched. Assuming a 50–50 engineering rule, that is, 50% of the channels pass through as express (or in transit) and 50% are to be switched, the problem reduces to switching $N \times K/2$ or $N^* \times K$, where $N^* = N/2$. If N^* wavelengths from one fiber are to be switched, then $N - N^*$ channels are available from other fibers. However, there are $(K - 1) \times N^*$ potential wavelengths contending for the same wavelength space $(N - N^*)$, where $N - N^*$ is much smaller than $(K - 1) \times N^*$. Clearly, this is a wavelength contention situation where blocking may occur.

Wavelength conversion does not present a technological issue when switches are opaque, as all optical signals (wavelengths) are converted to electrical ones. The system keeps connectivity tables with source and destination identification (ID) codes as well as wavelength values for each incoming signal. In this case, each node on the path "reads" the destination ID and "knows" where to switch to or route the optical signal, assign a wavelength, and multiplex many wavelengths in the fiber. This is predominantly addressed with two different strategies, centralized network wavelength management and distributed wavelength management.

In the centralized case, a network wavelength management function provisions each node with wavelength assignments, establishing semistatic cross-connectivity

over a selected path. Thus, the network wavelength manager "knows" at any time all possible wavelength conversions on a lightpath, whereby each link of the path may have a different wavelength. This case depends on a centralized database and algorithm that finds the optimum shortest and bandwidth-efficient path with the fewest wavelength conversions. Its speed, however, depends on how fast a path can be established; that is, how fast it can communicate with all nodes, and how fast each node can be provisioned without interrupting traffic on another already established connection. This also implies that all communications interfaces with the various domains are compatible; thus, interoperability may be an issue in a multivendor network.

In the distributed case, there is an additional optical channel that is common to all nodes over which messages are exchanged. These messages contain the input–output–wavelength associations, among other management and information messages. Thus, optimization of wavelength reassignment is left to each node to execute. This is known as the supervisory channel (SUPV), which is terminated and sourced by each node. The SUPV is multiplexed with the client data channels in the same fiber but it has a relatively lower bit rate than the data channels (up to Gbit/s compared with 2.5 or higher Gbit/s), and it may be outside the spectral range of data channels. In addition, it may or may not be protected. For protection, there may be two supervisory channels on the same fiber, or in a different fiber.

The supervisory channel conveys messages from node to node very fast and, thus, it allows for dynamic system reconfigurability. The reconfigurability speed is bounded by the switching speed of the fabric, by the acquisition time of wavelength converters, by other tunable components in the path (such as filters, lasers, etc.), by the time required to communicate the message to the control unit and back (latency), and by the processing time.

Dynamic system reconfigurability is required for system and network upgrades and service restoration. Network upgrades entail downloading new software versions and new system configurations. During network upgrades, service should not be affected.

6.8 SERVICE RESTORATION

Because of component degradation/failure, fiber cuts, excessive additive noise due to nonlinear phenomena and spectral noise, optical power loss, amplification gain drifts and so on, service may be degraded or even lost. Therefore, in order to continue uninterrupted service at the expected QoS, systems and networks are architected and designed for service restoration. Service restoration may be on several levels: on the channel, on the fiber, on the node level, and on the network, each at various degrees of significance.

Service restoration on the channel level implies that a single wavelength has been degraded or lost, affecting all traffic transported by the affected channel. A channel may be affected either by the degradation, by the failure of a single component, by excessive induced noise, or by excessive optical power degradation. Ser-

vice restoration is the action taken to either remove the affecting cause or to move the channel from one wavelength to another. This action may necessitate wavelength conversion.

Service restoration on the fiber level implies that all wavelengths in a fiber are affected, either because a fiber is cut or because a component failed. Service restoration is the taken action taken to move all channels from one fiber to another.

Service restoration on the node level implies that the total aggregate traffic at a node is affected. Service restoration is the action taken to move all traffic to other nodes, bypassing the faulty node.

Service restoration on the network level implies that many nodes in a network have failed; this is also termed disaster failure. Service restoration is the action taken to move all traffic to other parts of the network, bypassing the faulty nodes.

The mechanisms for these four service restoration levels may be summarized as follows:

1. Service restoration on the channel level:
   a. Set BER threshold per channel (according to engineering rules).
   b. Monitor BER of incoming signals.
   c. Correlate excessive BER of channels and determine if they belong to different fibers or to adjacent channels in same fiber.
   d. If in the same fiber, then adjust amplifier/equalizer taps or hop to another wavelength, if supported, by sending supervisory messages backward.
2. Service restoration on the fiber level:
   a. Set power threshold level of each channel to two threshold levels: one minimum, indicating power/no-power; and another to a higher level, indicating good/marginal. If BER is used, the good/marginal level may be eliminated.
   b. Monitor power of incoming signals.
   c. If power is lost on all channels of the same fiber, then there is a fiber cut, or a key component on the link has failed, affecting all channels.
   d. Important question: does this fiber support the supervisory channel? If yes, then switch to protection supervisory channel.
3. Service restoration on the node level:
   a. Monitor power of outgoing signals.
   b. If outgoing signals have failed but the incoming signals have not, then there is a faulty node. The declaration of a faulty node is made if the failure persists after a switch to the protection port has been attempted.
   c. Previous node in the network reroutes traffic such that the faulty node is bypassed. This depends on the survivability strategy supported by the network.
4. Service restoration on the network level:
   a. Similar to the previous case, but now many nodes fail.

b. Nodes in the network synergistically reroute traffic such that the faulty nodes are bypassed. In this case, low-priority traffic may be dropped, and high-priority traffic supported. This depends on the disaster avoidance strategy supported by the network and whether nodes belong to the same domain or not.

One last issue that must be noted is that the optical power budget of an optical path may change as one wavelength changes to another and as new routes are assigned. Thus, amplification, dispersion compensation, and equalization must be provisionable in order to maintain the quality of signal and the quality of service at the agreed upon service level agreement.

REFERENCES

1. S. V. Kartalopoulos, *Understanding SONET/SDH and ATM,* IEEE Press/Wiley, 1999.
2. S. V. Kartalopoulos, *DWDM, Networks, Components and Technology,* IEEE Press/Wiley, 2003.
3. S. V. Kartalopoulos, *Fault Detectability in DWDM,* IEEE Press/Wiley, 2002.
4. S. V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow,* IEEE-Press/Wiley, 2001.
5. F. Bruyere, "Metro WDM," *Alcatel Telecommunications Rev.,* 1st Quarter, 2002, 21–25.
6. J. van Bogaert, "E-MAN: Ethernet-Based Metropolitan Access Networks," *Alcatel Telecommunications Rev.,* 1st Quarter, 2002, 31–34.