Transformation of mission-critical communications networks

Migrating from SDH/SONET networks to IP/MPLS networks

White paper

Momentous changes are occurring in mission-critical communications networks. The current SDH/SONET networks, which are TDM-based, have proven to be resilient, reliable and secure in delivering voice, video and data traffic 24x7. However, there are a number of challenges driving many operators of mission-critical communications networks to consider migrating to IP/MPLS networks: the imminent obsolescence of SDH/SONET network equipment, the approaching end of their TDM leased line contracts with service providers, the adoption of new bandwidth-intensive applications and the pressing need to consolidate multiple dedicated networks into one converged network to optimize costs. This paper discusses the key considerations for network migration planning and provides an SDH/SONET-to-IP/MPLS migration blueprint.

Contents

Challenges for mission-critical networks

Industry and the public sector – from power utilities and oil & gas to public transportation, public safety and defense – rely on SDH/SONET network technology to build resilient and secure mission-critical communications networks. The SDH/SONET networks offer reliable circuit-based connectivity for TDM-based user equipment to run a wide variety of mission-critical applications, including voice, SCADA, private mobile radio/land mobile radio (PMR/LMR) and teleprotection. To avoid disruption in operations, it is imperative that these applications continuously run smoothly.

To exchange more data, these applications have now evolved from being TDM-based to being Ethernet- and/or IP-based. This is true for even widely-deployed applications such as SCADA, emergency communications, train signaling and teleprotection.

At the same time, new applications such as geographic information systems, high resolution video protection, LTE/5G connectivity and machine-to-machine communications are starting to be widely adopted to provide more operations intelligence, automation and control. They are also IP/Ethernet-based and consume much more bandwidth than current SDH/SONET networks can possibly provide. Moreover, deployed SDH/SONET network equipment is nearing end-of-life due to electronic component obsolescence and decreased demand as a result of the telecommunications industry's shift to IP. This situation is driving many service providers to retire their TDM leased line services that operators often use to complement their own networks.

The end result is that operators of mission-critical networks are struggling not just to maintain the current networks with necessary spare parts and support but also to evolve the networks for the future. A new network that can bridge the past to the present and scale for the future needs to be built. A foremost consideration is how to migrate legacy applications (see Table 1) to this new network.

An IP/MPLS network can rise to this challenge and provide the same network performance, quality of service (QoS), reliability and security as today's SDH/SONET network plus many new capabilities for future evolution.

Table 1. Common TDM applications

	Utilities	Urban and mainline rail	Oil and gas	Defense	Public safety	Airport traffic control
Analog voice	X	X	X	X	X	X
PMR/LMR/GSM-R/AGA	X	X	X	X	X	X
SCADA/telemetry	X	X	X	X		X
CCTV	X	X	X	X	X	
Radar				X		X
Signaling		X				
Teleprotection and differential protection	X					

This paper discusses the key considerations required during network migration planning. It explains how IP/MPLS can support the essential SDH/SONET network attributes while also providing other functionality, and how IP/MPLS carries TDM traffic. Then, an SDH/SONET-to-IP/MPLS migration blueprint is presented.

Key considerations during migration to IP/MPLS

- The key considerations during migration to IP/MPLS are:
- Network migration without compromise
- Migrating to a service provider's next-generation service
- Support for a diversity of applications

Each of these considerations is discussed in detail in the following sections.

Network migration without compromise

SDH/SONET networks have provided very robust, reliable and secure connectivity to operators of mission-critical communications networks. Therefore, when migrating to a converged IP/MPLS network, the new network must continue to meet all key mission-critical network requirements:

- Guaranteed QoS
- High availability and resiliency
- Traffic engineering
- Precise synchronization
- Strong security
- Effective and efficient network management

Guaranteed QoS

Legacy applications are TDM-based. TDM transport requires guaranteed network QoS to ensure that all bits and bytes arrive on time at the receiving end. Furthermore, some legacy applications such as voice, train signaling and teleprotection, are very delay sensitive while others, such as SCADA, are not. The new network must be capable of meeting the QoS requirements of the different classes of legacy applications without performance degradation.

High availability and resiliency

Any disruption in providing connectivity to mission-critical applications could cause significant harm to society, incur huge economic losses and even jeopardize human lives. For example, interruption of PMR/LMR (including TETRA/TETRAPOL, P25 and GSM-R traffic backhaul) could put the lives of field crews and public safety personnel in danger or paralyze rail transportation. If real-time telemetry data is not available, oil and gas production might need to stop. If teleprotection is disrupted, expensive power grid assets such as high-voltage transformers become vulnerable to damage, disrupting the essential electricity supply. To avoid these situations, the new network must have the same high availability and resiliency as the legacy SDH/SONET network.

Traffic engineering

SDH/SONET networks allow operators to select the appropriate physical route for path layers across the network for mission-critical and real-time applications. The new network needs to provide the same functionality.

Precise synchronization

TDM applications require precise frequency synchronization distributed across the network. Otherwise, TDM circuit errors such as frame slips as well as buffer overruns or underruns can occur. The new network needs to provide the same synchronization accuracy.

Strong security

An SDH/SONET network is usually very secure because it is usually isolated from an organization's IT network and the internet. In contrast, an IP/MPLS-based network is typically connected to the internet to support IT applications and remote device access; as a result, it is essential that the network be built to mitigate the effects of both internal and external threats.

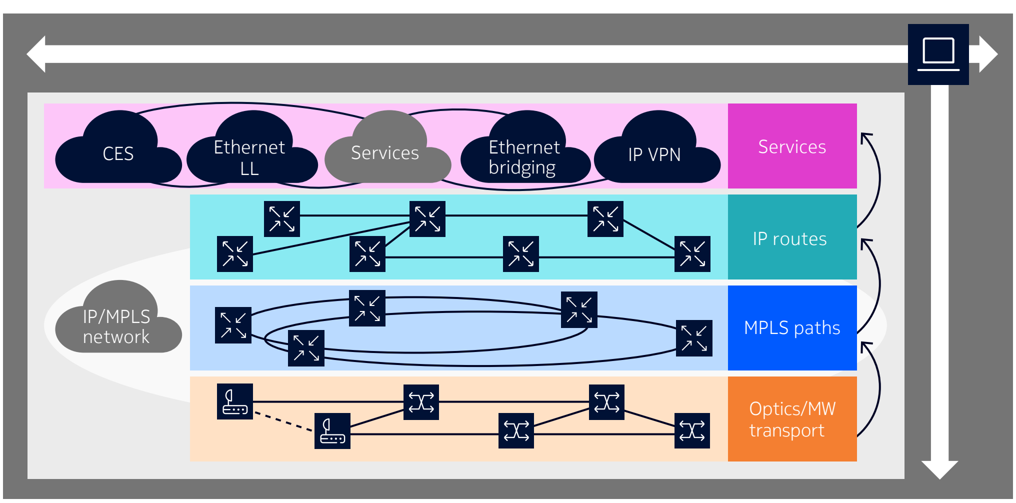
An IP/MPLS network is also inherently secure. Because transport of traffic is over a label switched path (LSP) tunnel, traffic sent by an attacker is not injected into the tunnel. MPLS-based VPN also makes extensive use of segregated routing, switching and cross-connect tables. Therefore, even if one MPLS VPN is compromised, the attacker cannot reach out to other VPN domains. The use of an access control list, a stateful firewall, Network Address Translation (NAT) and MPLS encryption also further fortify the network.

Effective and efficient network management

Operations and maintenance tools need to simplify the deployment and day-to-day operation of a communications network. Operations tools such as service and interface tests should allow for rapid troubleshooting, enabling proactive awareness of the state of traffic flows to help minimize service down time. The tools should also offer proactive surveillance, configuration, validation and diagnosis to simplify problem resolution, reduce configuration errors and reduce troubleshooting time.

Because the network buildout can ride over optical fiber or microwave transport, the new network manager (see Figure 1), which can manage end-to-end across layers – from services to IP/MPLS to transport – can greatly reduce operation cost and complexity. Its capability to correlate events in a cross-layer manner also streamlines fault diagnosis procedures.

Figure 1. Cross-layer end-to-end network management



Migrating to a service provider's next-generation service

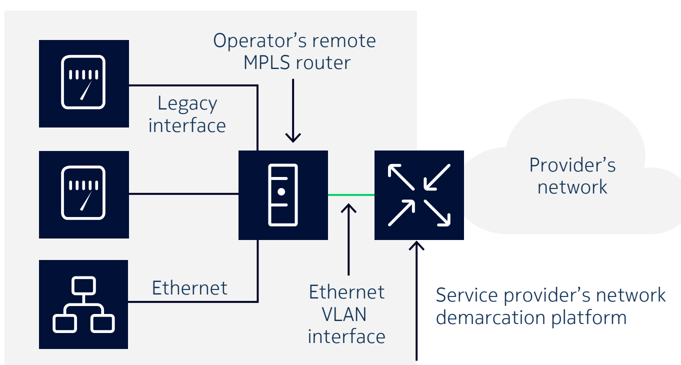
Many network operators have been using a service provider's TDM leased line service to complement their private networks or to act as a fallback path to increase reliability. The service is usually in the form of a DS1/T1 at 1.544 Mb/s, E1 at 2 Mb/s, and n x 64 kb/s for both.

As service providers have begun the transition to an all-IP network, these services are becoming unavailable and are replaced by Ethernet-access-based, next-generation service. Operators of mission-critical networks need to weigh two options: migrate to the service provider's new service or expand their private network.

With the first option, instead of a TDM interface, service providers now provide a VLAN interface inside an Ethernet port (see Figure 2). Operators need to be able to transport data of legacy TDM circuits with the new services by using circuit emulation capability such as TDM pseudowire and MEF 8. They also need to be able to aggregate IP and Ethernet traffic from future applications onto the same Ethernet VLAN interface before handing off to the service provider. In essence, they still deploy IP/MPLS that will run on top of the provider's network end-to-end. Furthermore, it is also important to understand the QoS requirements of all the applications.

Network operators also need to work closely with service providers to determine the required service parameters (for example, bandwidth, delay and jitter) and service availability to define a suitable Service Level Agreement.

Figure 2. Connecting to a service provider's next-generation network



If network operators decide to instead expand their private network, they need to provision new connectivity to the locations using optical fiber, microwave or cellular broadband.

Operators need to understand the technical and economic aspects of the two options when making the decision to use one or the other, or both.

Support for a diversity of applications

A key characteristic of mission-critical networks is that there are a broad variety of applications with widely different communications requirements. One way to categorize these services is by application type:

- Voice applications (for example, telephony, teleconferences): Require constant but moderate bandwidth (kb/s) with very short transmission delay (100 ms) and limited jitter.
- Video applications (for example, CCTV, live video from car-mounted or body-worn cameras, videoconferencing): Require variable and significantly higher bandwidth (Mb/s) with short transmission delay and limited jitter.

- Data-based applications (for example, file transfer and control data from remote devices): Require bandwidths ranging from very moderate (tens of kb/s) to high (Mb/s).

Data-based applications can further be divided into two sub-categories:

- TDM-based data: While the applications encapsulate data in a protocol data unit (PDU), the network transparently transports the data. Even when PDU transmission is intermittent, all data bits (PDU and idling data) are transported. This is typically found in legacy applications such as SCADA, LMR/GSM-R and teleprotection. Traffic, whether it is data or voice, is carried as transparent data bits. Delay tolerance depends on the nature of the applications.
- Packet-based data: The data is typically encapsulated in an Ethernet frame or an IP packet within an Ethernet frame. The traffic is usually bursty, with short periods of high activity followed by long idle periods. Applications such as voice, signaling and teleprotection are still delay sensitive, like their TDM counterparts, while others, such as environmental sensor data, are less so.
- Depending on the sub-category, the data can be transparently transported as TDM bits or forwarded by Ethernet or IP capability found in IP/MPLS network equipment. Delay tolerance depends on the nature of the applications.

Another way to classify applications is topological:

- Point-to-point applications such as LMR as well as legacy PBX and voice
- Point-to-multipoint applications such as in SCADA and CCTV
- Multipoint applications such as conferencing

To ensure smooth migrations of all applications, it is important that both TDM point-to-point and point-to-multipoint (also known as multi-drop data bridge) as well as pulse-code-modulation (PCM) bridging capabilities are supported in the new network.

Comparing SDH/SONET and IP/MPLS

MPLS provides the capability to establish connection-oriented paths or tunnels, called label switched paths (LSPs), over a connectionless IP network. It enables intelligent and precise traffic engineering and optimal use of network resources. It allows next-generation Ethernet- and/or IP-based applications to run over all types of transport: optics, microwave and copper. MPLS was also specifically designed to support Layer 1 and Layer 2 services simultaneously.

Although it might sound as though there is a great leap when migrating from SDH/SONET to IP/MPLS, both technologies were designed from inception to be robust, reliable and flexible. As a result, many common underlying network concepts are used by both technologies.

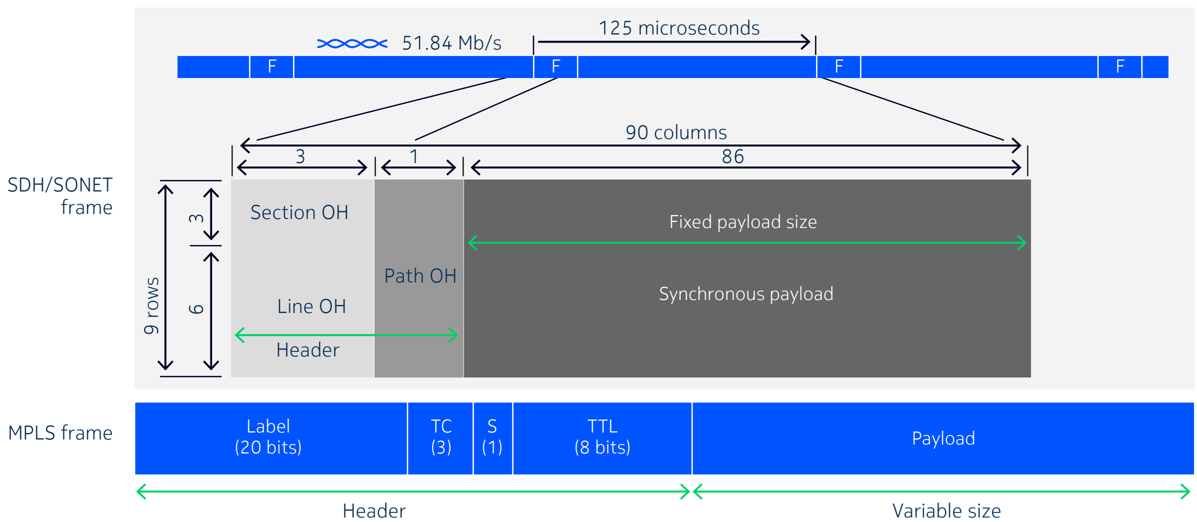
The following sections explain similarities that provide network operators further benefits after an SDH/SONET-to-IP/MPLS migration.

Both transmit in frames

SDH/SONET encapsulates data in fixed-size frames (see Figure 3) and transmits at a fixed rate dependent on the interface speed. By contrast, MPLS encapsulates in variable-sized frames transmitting at a variable rate as applications send out information.

For TDM applications, MPLS still transmits frames at a fixed rate. For IP- and/or Ethernet-based applications, MPLS transmits only when the applications send information. Flexible frame size and variable rate enable MPLS to efficiently carry short frames at a constant rate (in the order of tens of bytes) as well as jumbo frames at a bursty rate.

Figure 3. SDH/SONET and MPLS framing



Both use on circuit-based transport

Operators provision an end-to-end circuit, or path, for transport in SDH/SONET and MPLS networks. In SDH/SONET, there is a channel bank in front of the SDH/SONET add-drop multiplexer (ADM). Legacy interfaces such as G.703, E&M, FSX/FSO and serial interfaces are multiplexed onto various timeslots in an E1 or DS1 carrier.

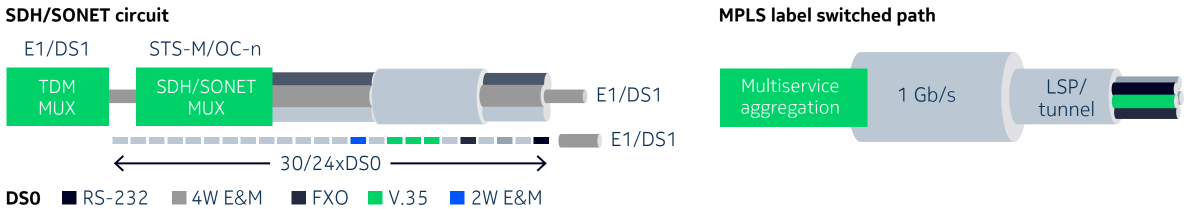
There are also DS1 or E1 interfaces directly from other customer equipment such as a legacy PBX. An interface enters the ADM and is mapped into a Synchronous Transport Signal (STS) container as a virtual container or tributary (VC-12 for SDH and VT-1.5 for SONET). It is then cross-connected across the SDH/SONET network.

To support flexible bandwidth capacity, enhancements such as link capacity adjustment scheme and generic framing procedures have been standardized to support virtual concatenation to create a larger capacity payload container, in a multiple of 2 Mb/s (for SDH) and 1.544 Mb/s (for SONET).

Similarly, the legacy interfaces and DS1/E1 interfaces are transported by the MPLS platform as a pseudowire circuit, which is carried inside an LSP across the IP/MPLS network (see Figure 4).

In an IP/MPLS network, the bandwidth reserved for the LSP can be any number within the line speed instead of the rigid 2 Mb/s or 1.544 Mb/s multiples. This allows more flexible network capacity planning and more efficient bandwidth resource utilization.

Figure 4. Circuit in SDH/SONET and IP/MPLS



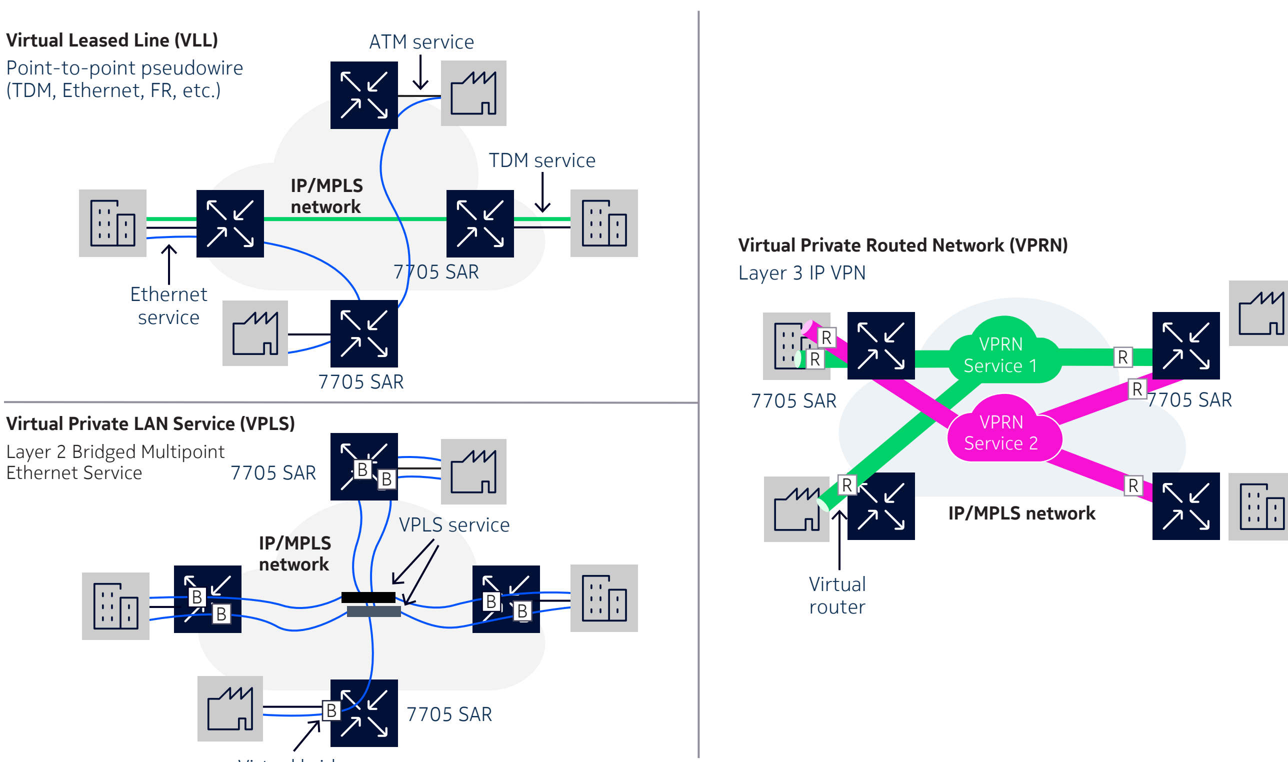
When provisioning an end-to-end SDH/SONET path, the physical route can be selected according to administration policy. Similarly, the physical route of an LSP can also be explicitly specified or computed according to policy or constraints such as bandwidth, number of hops and link type.

Both support multiprotocol transport

Both SDH/SONET and MPLS networks can carry multiprotocol data in their respective frames. Whether it is TDM and frame relay data in E1/E3/DS1/DS3, Ethernet or IP, the multiprotocol data can be carried over SDH/SONET and MPLS. It is notable that MPLS frames can also be carried over SDH/SONET using Packet over SDH/SONET (POS) framing format as defined in IETF RFC 2615.

While an SDH/SONET network can carry Ethernet and IP traffic, it mainly provides only transport[1]. An MPLS network supports bridging and routing in the forms of Layer 2 Ethernet and Layer 3 IP VPN (see Figure 5). This new capability allows the network to perform Layer 2 and Layer 3 aggregation and to support different VPN types.

Figure 5. MPLS-based VPN



1 An exception is next-generation SDH/SONET, which can be equipped with an Ethernet card to perform basic Ethernet bridging.

This wide range of VPN support provides high flexibility for operators to optimally transport traffic from new Ethernet- and/or IP-based applications.

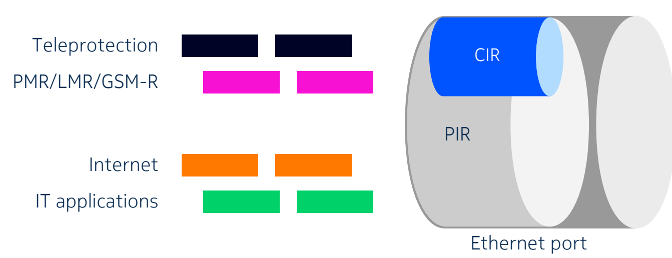
Both guarantee QoS

Because TDM-based applications are extremely sensitive to delay and jitter, their traffic needs to be treated with higher priority than other applications. When traffic arrives at a router, it needs to be classified based on header marking (EXP field for MPLS frames) and be placed in different queues. TDM traffic such as teleprotection must be placed in the high-priority queue and be exhaustively[2] serviced continuously to achieve minimal delay and jitter (see Figure 6).

SDH/SONET has been well recognized for delivering guaranteed QoS. Its framing hierarchy and TDM-based transport allow SDH/SONET to guarantee QoS for transported data. MPLS was also designed to support guaranteed QoS with greater flexibility.

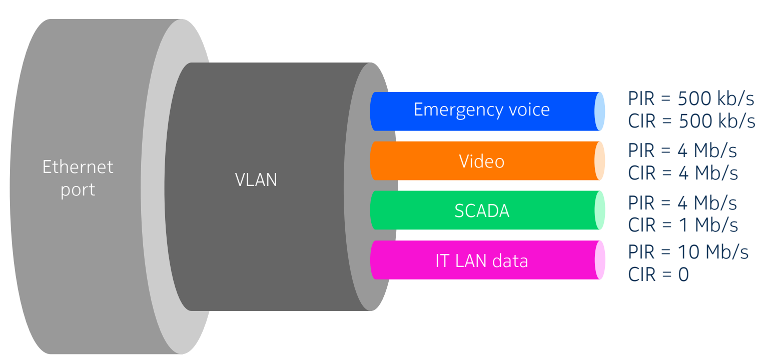
SDH/SONET, being TDM-based, treats all applications, from real-time delay/jitter-sensitive to best-effort ones, with the same priority. While this guarantees QoS, there is inefficiency in bandwidth utilization because traffic of best-effort applications such as internet access is bursty. With IP/MPLS, traffic from each individual application is first classified and rate-limited before entering the network. (See Figure 6 for an example.)

Figure 6. Traffic classification and rate-limiting



After being classified and rate-limited, the traffic is encapsulated in an MPLS frame that has a shim header with a 3-bit traffic (TC) field, previously commonly known as experimental (EXP) bits. The field indicates the QoS level assigned for the MPLS traffic. It also incorporates a flexible traffic management scheme that allows a committed information rate (CIR) and peak information rate (PIR) to be set (see Figure 7).

Figure 7. CIR and PIR bandwidth resource partition



2 Exhaustive queuing is a traffic management technique that continues to transmit a packet in the queue until it is empty.

This process provides a flexible way to manage the bandwidth and delivery performance of different applications. Legacy traffic can be classified and assigned to the highest QoS level by the TC field so that the traffic will always fall into the CIR bandwidth region whose delivery will be assured[3].

Some applications, such as e-mail and internet browsing, can be classified as best-effort traffic with minimum or even no CIR bandwidth. If there is no traffic from other competing applications, a best-effort application can use all the available bandwidth until competing, higher priority traffic is received. Because not every non-critical application will transmit at the same time, operators can take advantage of statistical multiplexing to optimize the use of network bandwidth.

Applying a hierarchical QoS model can also ensure that a common group of services can be allocated a fixed amount of bandwidth, ensuring fairness among different groups.

Both have strong resiliency

Current SDH/SONET-based networks have automatic protection switching (1+1 APS) for link protection as well as unidirectional path-switched ring (UPSR) and bidirectional line-switched ring (BLSR) for link and nodal protection in a ring. These resiliency mechanisms have proven to be extremely reliable, providing rapid recovery in 50 ms after a network fault is detected.

IP/MPLS supports fast re-route (FRR) technology that can re-route traffic around the link or nodal failure to a pre-established LSP FRR tunnel, also in 50 ms after detection. In the case of SDH/SONET, because the bandwidth of the protecting link or path is locked up for protection, half of the link or ring bandwidth cannot be used. For MPLS, the FRR tunnel is established without locking up any bandwidth; therefore, all bandwidth in the link and ring are put to use.

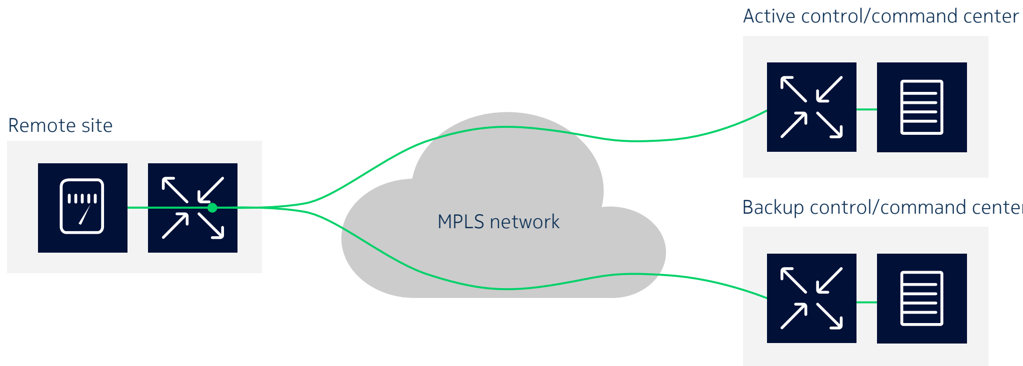
Furthermore, mission-critical networks often call for even higher availability beyond that required by a typical commercial service provider. The network topology often evolves from a simple ring to a multi-ring or meshed topology to provide richer path diversity in order to recover from a multi-fault scenario, which is common during natural disasters or deliberate sabotage.

As long as physical connectivity is available, IP/MPLS's intelligence path compute capability allows connectivity to be re-established, thereby providing maximum network availability even in a multi-fault scenario. Furthermore, because IP/MPLS rides on top of various physical and link layer technologies, operators can optionally take advantage of each technology's protection mechanism (SDH/SONET's APS, UPSR and BLSR; microwave's 1+1; and Ethernet's LAG) in conjunction with IP/MPLS resiliency mechanisms.

IP/MPLS can further provide geo-diversity protection, which is not possible on SDH/SONET networks, particularly to a control/command center. For mission-critical operations that need to continue to operate even in the face of a serious disaster or accident, this capability allows all traffic to switch a backup control/command center if the primary control/command center fails (see Figure 8).

3 To achieve guaranteed QoS, it is important to engineer so that the total CIR does not exceed the interface speed.

Figure 8. Geo-diversity redundancy with MPLS network



Complementing these network recovery mechanisms is the hitless switching of the control and routing module in an IP/MPLS platform. This unique redundancy mechanism elevates IP/MPLS network reliability to the same level as an SDH/SONET network.

Both have extensive OAM capability

SDH/SONET's operations/administration and maintenance (OAM) capability, from alarm propagation to remote defect indication to loss of signal detection, is vital to a network operator's day-to-day operation.

IP/MPLS has its own end-to-end tools for OAM capability, such as LSP ping/traceroute, virtual circuit connectivity verification and bidirectional forwarding detection. These tools are complemented by the OAM capability of the underlying link layer, which can be Ethernet, microwave or SDH/SONET.

Both support precise frequency synchronization

In an SDH/SONET network, frequency synchronization, which is vital to TDM transport, is achieved with line timing recovered from the SDH/SONET interface. An IP/MPLS network can do the same thing by recovering from an SDH/SONET interface, a synchronous Ethernet link and a packet microwave link with equal precision.

For applications that require phase and time-of-day (ToD) synchronization, the remote site resorts to installing an external Global Positioning System (GPS) receiver because SDH/SONET has no inherent mechanism to transport phase or ToD information. This sole synchronization source is a single point of failure. If the GPS signal reception quality degrades or hardware failure occurs at the GPS receiver, the site loses synchronization and application devices need to switch back to holdover mode. In this mode, the accuracy of the clock in devices running the applications quickly degrades.

IP/MPLS network pairing with Precision Timing Protocol as defined in IEEE1588v2 allows a protecting synchronization source for phase and ToD to be transported. MPLS platforms are now typically designed with IEEE1588 hardware assist capability to allow for precise synchronization transport over a large number of spans in the network.

Additional benefits of IP/MPLS

The IP/MPLS network technology provides numerous additional benefits that SDH/SONET cannot provide:

- Topology and transmission medium agnostic
- Multitenant/shared infrastructure enablement
- Future communications readiness

Topology and transmission medium agnostic

IP/MPLS can run over any network topology, including ring, multi-ring, necklace and meshed. It is crucial that mission-critical networks maintain connectivity during multi-fault failure scenarios, which are not uncommon during a natural disaster. An IP/MPLS platform can intelligently compute path as long as there is physical connectivity.

IP/MPLS can also be deployed over any transmission medium, providing operators with the flexibility to add new links as required to boost resiliency. For example, a microwave link can be strategically deployed overlaying a fiber ring to attain high network availability.

Multitenant/shared infrastructure enablement

To streamline network operations and strive for greater economic efficiency, operators of mission-critical networks want to consolidate multiple networks into one converged network that can serve multiple needs. With proper design and engineering, the service-oriented nature of IP/MPLS network management enables operators to serve individual needs without compromise.

Future communications readiness

IP/MPLS-based VPN services natively support Ethernet and IP, including IP multicast and IPv6, to support future applications. The services also facilitate the future adoption of software defined network and network functions virtualization.

Migration of legacy TDM applications

Migrating legacy mission-critical applications requires an adequate technical understanding of how TDM circuits are transported over IP/MPLS to render the same level of performance as before. The following sections explain how TDM traffic is transported over an IP/MPLS network using Circuit Emulation Service over Packet Switched Network (CESoPSN), discuss end-to-end delay considerations, and explain TDM circuit synchronization.

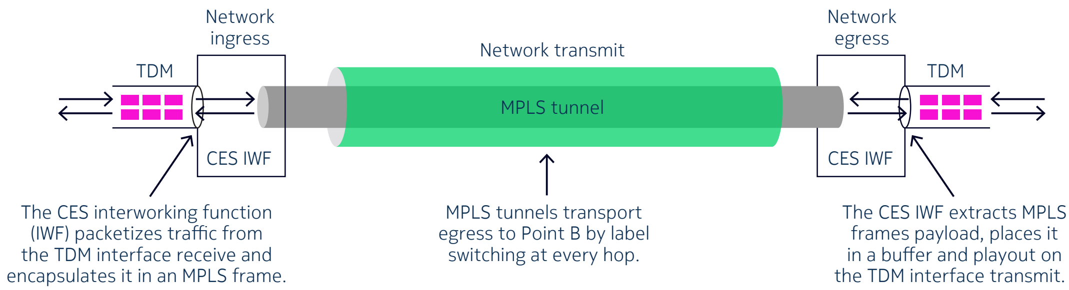
Circuit Emulation Service

An IP/MPLS network uses a Circuit Emulation Service (CES) to carry data of legacy applications. The key engineering considerations to provision a CES are latency, jitter and synchronization. Different TDM applications have different requirements. Latency and jitter will be considered first.

The latency for TDM traffic consists of packetization delay at network ingress, network transit delay, and jitter buffer/playout delay at network egress. To address these issues effectively and provide the most optimized delivery performance, IP/MPLS routers need to allow network operators to fine-tune packetization delay and jitter buffer/playout delay based on the network topology.

Operating with legacy TDM networks and services is straightforward when using MPLS CES functionality. CES delivers the same quality of experience as the existing TDM network infrastructure with the same level of predictability. The MPLS network has a CES interworking function that ensures all information required by a TDM circuit is maintained across the packet network (see Figure 9). This functionality provides a full transition to the packet network while providing TDM service continuity.

Figure 9. Circuit Emulation Service



The major delay contributors for TDM CES are:

- TDM packetization at service ingress
- MPLS during network transit (at every hop)
- TDM playout delay at service egress

TDM packetization

The packetization process is shown in Figure 10. The ingress MPLS router receives frames of digital information at a fixed interval (for example, 1 byte every 125 microseconds for a DS0 circuit). The router encapsulates the digital information in an MPLS frame that has two labels: a tunnel label that specifies an LSP and a service label that specifies a pseudowire circuit associated with the particular CES service.

As explained earlier, it is also important that the TC field, a 3-bit field, is marked appropriately, reflecting an expedited class of QoS. The actual TC value depends on the network QoS policy set by the network operator.

The operator has two choices: to package this byte in an MPLS frame and transmit it across the network immediately with practically no packetization delay (other than that incurred by hardware processing) or to wait until a pre-configured number of bytes arrive before transmitting them all together in one MPLS frame, thereby incurring more packetization delay.

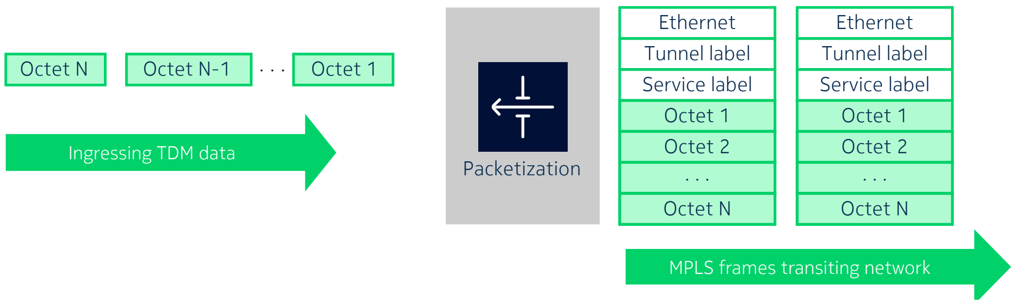
The packet payload size is configurable by the network operator.

Smaller payload sizes lead to a higher number of MPLS frames per second, resulting in higher bandwidth but lower packetization delay and, ultimately, lower end-to-end delay. By contrast, larger payload sizes with a lower number of frames per second result in lower bandwidth but higher packetization delay and higher end-to-end delay.

Depending on the network design and delay budget of the TDM applications, network operators can optimize the setting to achieve engineered targets. If delay tolerance of the application is stringent, operators should consider using a smaller payload size that consumes a larger bandwidth in the network[4].

4 It has been tested that with small payload and jitter buffer size (2 bytes and 1 ms) in a three-hop network, the end-to-end delay can be as low as in the 2 ms range.

Figure 10. Packetization process at ingress

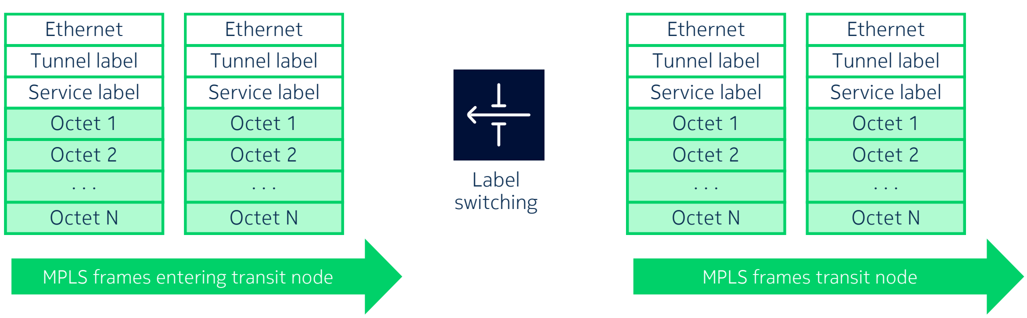


For an analog interface such as E&M, the router needs to digitize the analog signal with PCM before packetization. The PCM algorithms commonly used are μ-law in North America and Japan and A-law internationally.

MPLS during network transit

During the label switching (see Figure 11), the priority of the MPLS frames carrying TDM traffic is denoted by the EXP field. With proper marking and network engineering, the frames are placed in the top-priority queue and are serviced without incurring unnecessary queuing delay. As a result, the delay incurred at each label switching hop is negligible. Also, because frames are switched immediately with effectively no queuing delay, minimal jitter is incurred.

Figure 11. Multiprotocol Label Switching



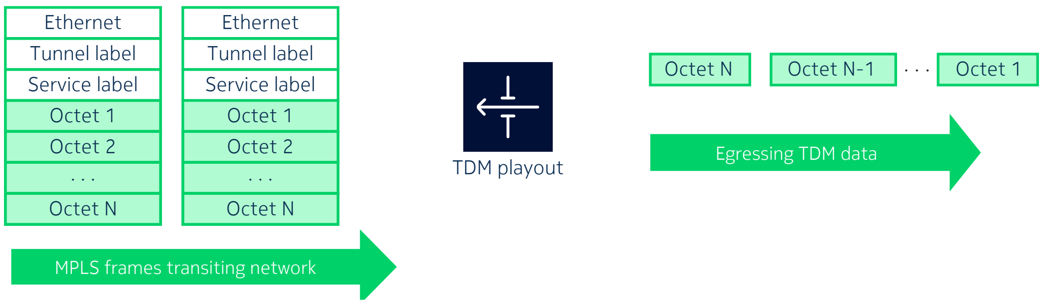
TDM playout delay at service egress

The playout process is shown in Figure 12.

When MPLS frames carrying TDM payload are received, the payload is extracted and placed in the playout buffer. To accommodate jitter incurred on the MPLS frames during transit, the payload gathered in the buffer is not immediately played out, or transmitted, on the TDM transmit circuit. Instead, it waits until half of the configured buffer is full before playout of bits on TDM circuit starts.

The buffer size should be set based on packetization payload size and the estimated network jitter, which is dependent on the number of transit hops and other network engineering factors such as transmission link speed. It is often necessary for operators to measure delay and jitter based on the network design before production deployment.

Figure 12. Playout process



End-to-end delay considerations

With proper engineering design, CES service with stringent QoS requirements can be reliably met.

At ingress, CES starts with packetization, which has deterministic delay that is configurable by operators. The larger the delay, the more TDM data can be carried in a single MPLS frame, resulting in higher bandwidth efficiency.

On egress playout, CES uses a playout buffer, which is essentially a jitter buffer, to ensure that the TDM circuit recovery mechanism can absorb jitter incurred during network transit. This ensures the successful de-packetization of the payload back into the TDM interface connected to the legacy equipment.

This playout buffer delay is also deterministic. The smaller the jitter buffer, the less delay incurred at egress. However, to avoid playout overruns and underruns, the jitter buffer needs to be set at a large enough value to compensate for jitter incurred in the network.

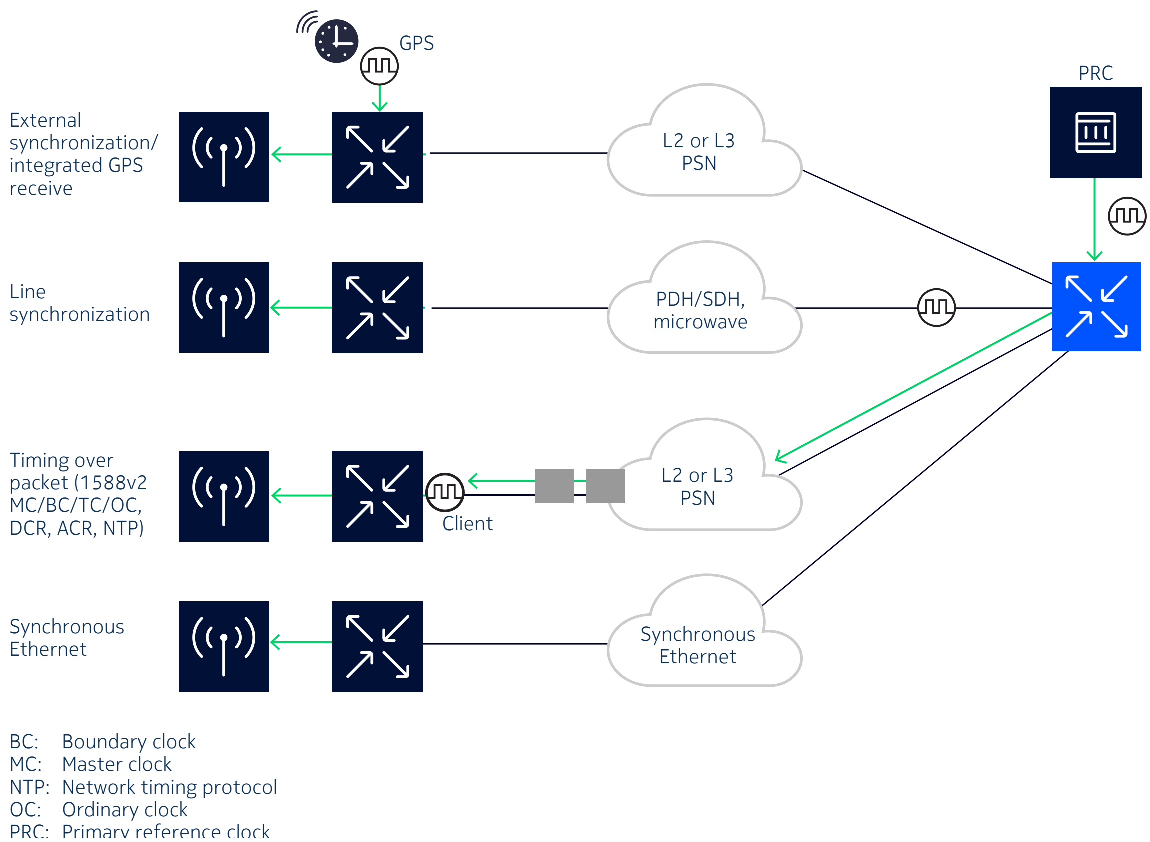
Network operators can customize configurations to set these two delay parameters as well as the network transit delay. Enabled by this flexibility and MPLS's QoS capability, the CES delay is therefore very deterministic.

When ordering a packet service from a third-party network operator, it is important to understand the jitter introduced by their networking equipment as well as the jitter introduced by the CES terminating equipment. Highly unstable jitter can cause problems in TDM circuit recovery at network egress.

TDM circuit synchronization

Synchronization of the TDM circuit end-to-end is another prime consideration for CES. As shown in Figure 13, an MPLS platform can support a full range of synchronization technologies ranging from integrated GPS receiver to line synchronization with Ethernet and SDH/SONET/PDH as well as timing-over-packet technology (including IEEE1588v2, differential clock recovery [DCR] and adaptive clock recovery [ACR]) to adapt to a network operator's synchronization infrastructure.

Figure 13. Synchronization technologies



An SDH/SONET-to-IP/MPLS network migration blueprint

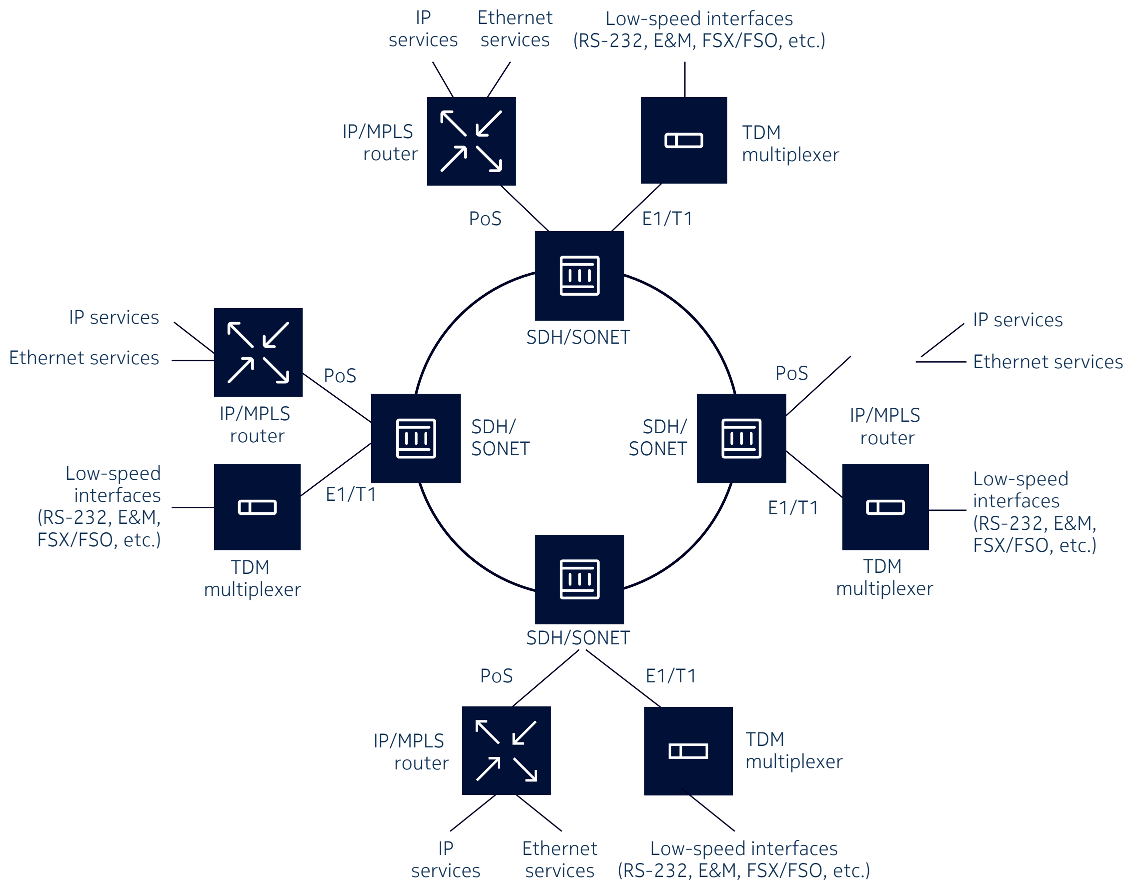
Migration can occur in many different ways, depending on the network resource availability (for example, is there spare fiber or wavelength in the fiber? Are alternate network uplinks available during migration?) and operating constraints such as how much downtime can be allowed. This paper describes a migration scenario that provides a blueprint for operators.

The goal is to keep the disruption of existing applications to a minimum. We recommend that the migration from SDH/SONET to MPLS take place in phases. The following sections describe a three-phase migration.

Phase 1: Adding IP/MPLS routers to the SDH/SONET infrastructure

In Phase 1, IP/MPLS routers are connected to the SDH/SONET infrastructure (see Figure 14). This allows the introduction of new IP services and Ethernet connectivity while continuing to support TDM services on the SDH/SONET infrastructure, for cost savings and reduced disruption. Network operators also have time to become familiar with IP/MPLS capabilities before moving the TDM services. Effective utilization of the existing SDH/SONET infrastructure ensures minimal or no disruption to existing services while new services are added.

Figure 14. Adding IP/MPLS routers for IP and Ethernet services

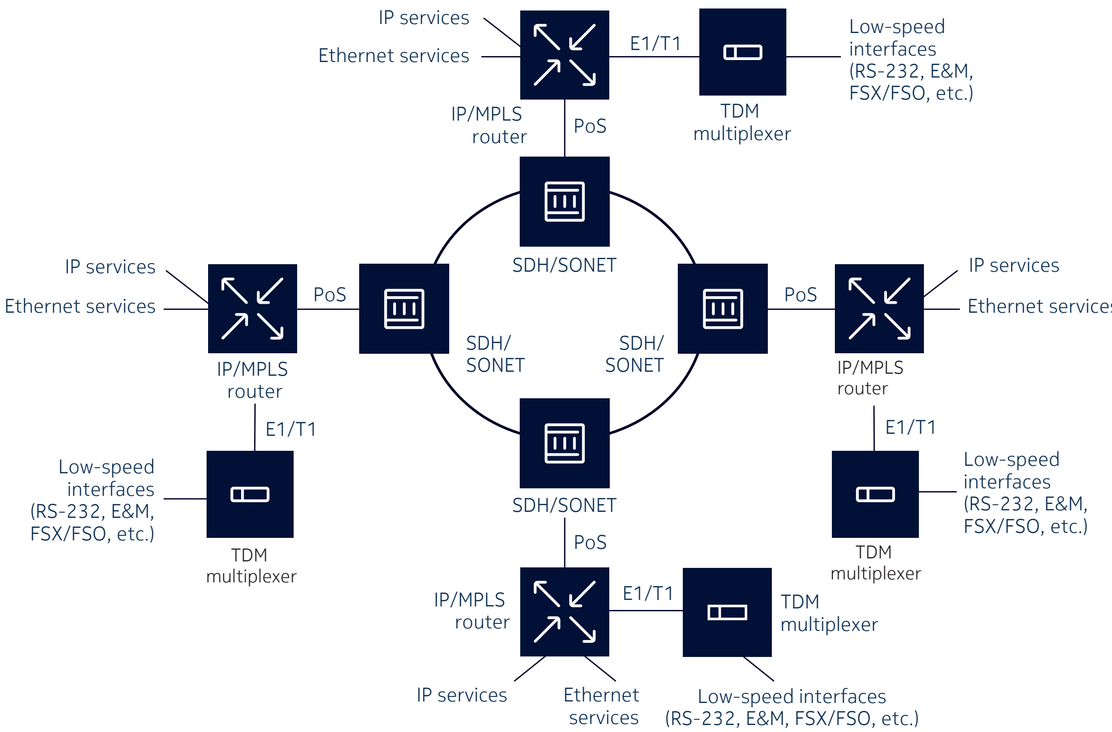


Phase 2: Switching TDM services onto the IP/MPLS infrastructure

In Phase 2, IP/MPLS routers support traditional TDM services – including Synchronous Transport Mode 1/Optical Carrier 3 (STM-1/OC-3), T1/E1, RS-232, V.35, X.21 and E&M – allowing the migration of these services away from the SDH/SONET infrastructure. This migration can be done in stages and with the coexistence of various interface types. Services that have been satisfied with traditional TDM interfaces can also be supported while new Ethernet interfaces for these services are being introduced.

At this point, TDM services will likely be supported on the existing multiplexer TDM equipment or on the IP/MPLS routers while new IP and Ethernet services are supported on IP/MPLS routers (see Figure 15). At the end of this phase, all services should have migrated to the IP/MPLS network.

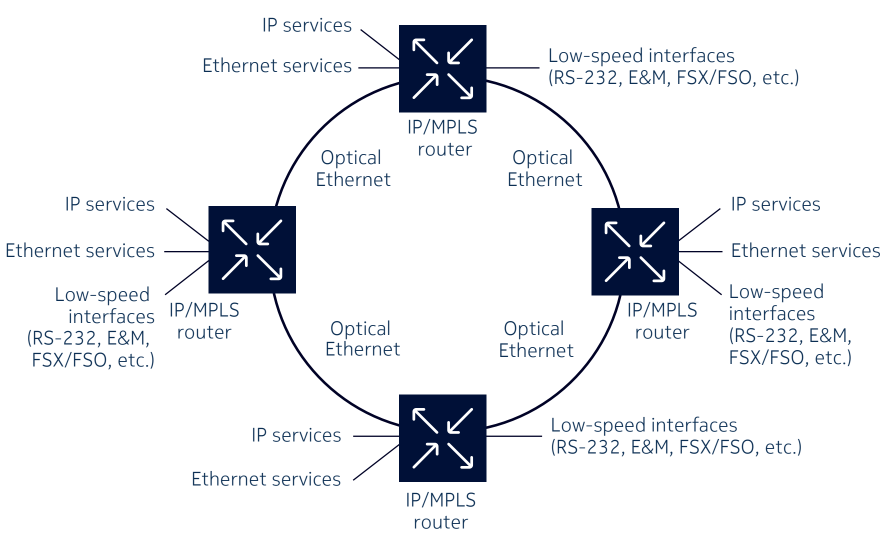
Figure 15. Consolidating TDM services onto and through IP/MPLS routers



Phase 3: Removing the SDH/SONET infrastructure and introducing WDM

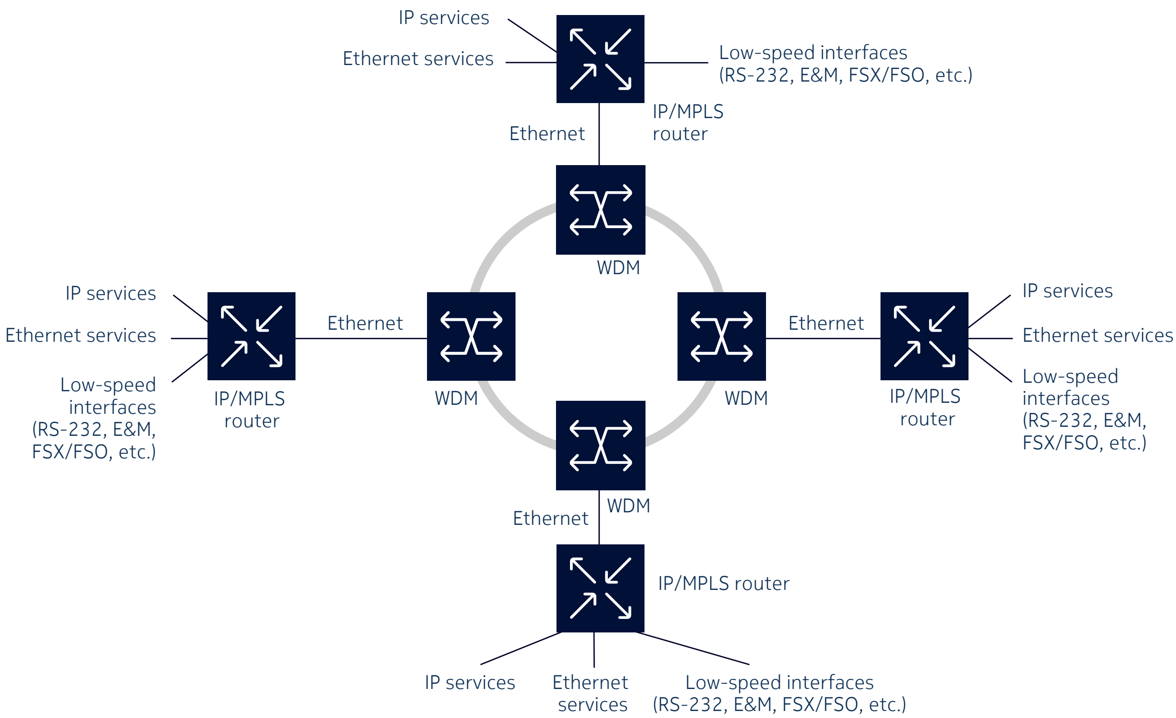
In Phase 3, the SDH/SONET network can be completely removed and the fiber plant can be used to interconnect IP/MPLS routers after all services have migrated onto the routers (see Figure 16). This simplifies network structure and management while providing an infrastructure capable of supporting new services and their bandwidth requirements.

Figure 16. Consolidating access on IP/MPLS and removing SDH/SONET



Furthermore, if huge bandwidth (in the order of tens to hundreds of gigabits per second) is required, wave division multiplexing (WDM) technology can be deployed (see Figure 17). Depending on the projected backbone capacity requirements, operators can consider using coarse WDM (CWDM) or dense WDM (DWDM) for cross-layer management in the IP/MPLS platform.

Figure 17. Deploying WDM to expand bandwidth on fiber



Conclusion

It is imperative that mission-critical networks are built with a network solution that is reliable, resilient and secure. Nokia is a world leader in mission-critical networks. Its unique and comprehensive portfolio of IP/MPLS, microwave, optics and network management communications products have already enabled many operators globally to flexibly build end-to-end managed converged networks. Wide support of legacy interfaces allows customers to migrate deployed legacy applications smoothly. Coupled with advanced MPLS networking and QoS capabilities, all applications can be delivered deterministically, without compromise. The innovative cross-layer network management of the IP/MPLS, microwave, and optics layers further optimizes network provisioning and operations.

More information about Nokia solutions and products for mission-critical networks

Acronyms

5G	Fifth Generation
ACL	Access Control List
AGA	air ground air system
APS	automatic protection switching
BLSR	Bi-directional Line Switched Ring
CCTV	closed circuit television
CES	Circuit Emulation Service
CESoPSN	Circuit Emulation Service over Packet Switched Network
CIR	committed information rate
FXO	Foreign eXchange Office
FXS	Foreign eXchange Service
GPS	Global Positioning System
GSM-R	Global System for Mobile Communications - Railway
IP	Internet Protocol
LAG	Link Aggregation Group
LAN	local area network
LMR	land mobile radio
LSP	label switched path
LTE	long term evolution
MPLS	Multiprotocol Label Switching
MUX	multiplexer
NAT	Network Address Translation
OAM	operations, administration and maintenance
PBX	private branch exchange
PCM	pulse-code modulation
PDH	Plesiochronous Digital Hierarchy
PDU	protocol data unit
PIR	peak information rate
PMR	private mobile radio
POS	Packet over SDH/SONET
QoS	Quality of Service

SCADA	supervisory control and data acquisition
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
STS	Synchronous Transport Signal
TDM	Time Division Multiplexing
TETRA	Terrestrial Trunked Radio
UPSR	Unidirectional Path Switched Ring
VLAN	virtual local area network
VLL	Virtual Leased Line
VPLS	Virtual Private LAN Service
VPN	virtual private network
VPRN	Virtual Private Routed Network
WAN	wide area network
WDM	Wavelength Division Multiplexing

References

1. Nokia 1830 Photonic Service Switch.
2. Nokia 5620 Service Aware Manager.
3. Nokia 7705 Service Aggregation Router.
4. Nokia 9500 Microwave Packet Radio.
5. International Engineering Task Force. RFC 2615: PPP over SONET/SDH. June 1999.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 538650 (April) CID145072