

Tellabs® 8600 Managed Edge System — Reliability, Protection and QoS in Mesh IP/MPLS Networks

Introduction

The Tellabs® 8600 Managed Edge System is a carrier-class, highly scalable Multiprotocol Label Switching (MPLS)-based platform that helps to enable a robust packet-based mesh backhaul solution. With support for Time Division Multiplexing (TDM) and Ethernet-based pseudowires, the Tellabs 8600 system has the ability to transport 1x Radio Transmission Technology (1xRTT) and 1x Evolution Data Optimized (1xEV-DO)-based traffic types. Rapid route recovery and low latency transport maximize network performance and reliability, and Quality of Service (QoS) mechanisms help ensure proper treatment of the backhaul traffic.

As shown in Figure 1, mesh/ring architectures support redundant paths and provide the foundation for a fully protected architecture, from the core to the hub elements. Future growth to ring or mesh base station elements is also possible, pushing the protection further to the edge.

MPLS Overview

MPLS is a versatile, low-overhead architecture initially developed to address the challenges presented by modern networks that has now emerged as an elegant solution to meet the bandwidth management and service requirements for next-generation backhaul networks as well. MPLS addresses the speed, scalability, routing (based on QoS and service quality metrics) and traffic engineering issues common in today's packet-based networks and can exist over virtually any Layer 2 network. Tellabs understands the attributes of MPLS-based technology and how to leverage its traffic engineering capabilities to achieve hard Service Level Agreement (SLA) requirements.

Fundamentally, MPLS employs an encapsulation technique providing internetworking between different technologies, coupled with the necessary signaling protocols to discover, configure and manage connectivity. In addition to signaling protocols, MPLS uses resiliency protocols like Fast Re-route and Bi-directional Fault Detection (BFD) to determine failures and switch to standby links. MPLS-based backhaul using TDM pseudowires enables the use of more cost-effective, scalable Ethernet transport that can migrate easily to IP for 4G.

MPLS Pseudowires

MPLS Pseudowire Emulation Edge to Edge (PWE3) is a mechanism that emulates the essential attributes of a service (such as a T-1 leased line or Frame Relay) over a Packet Switch Network (PSN). PWE3 is intended to provide only the minimum necessary functionality to emulate the wire with the required degree of faithfulness for the given service definition.

Pseudowires can encapsulate service-specific bitstreams, cells or Protocol Data Units (PDU) arriving at an ingress port and carry them across an IP path or MPLS tunnel. In some cases, it may be necessary for pseudowires to perform other operations, including timing and order management, to emulate the behavior and characteristics of the service to the required degree of faithfulness.

The Tellabs® 8600 system packet switching technology with multiservice features enables IP, MPLS, Ethernet, Asynchronous Transfer Mode (ATM), Frame Relay, Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) and Time Division Multiplexing

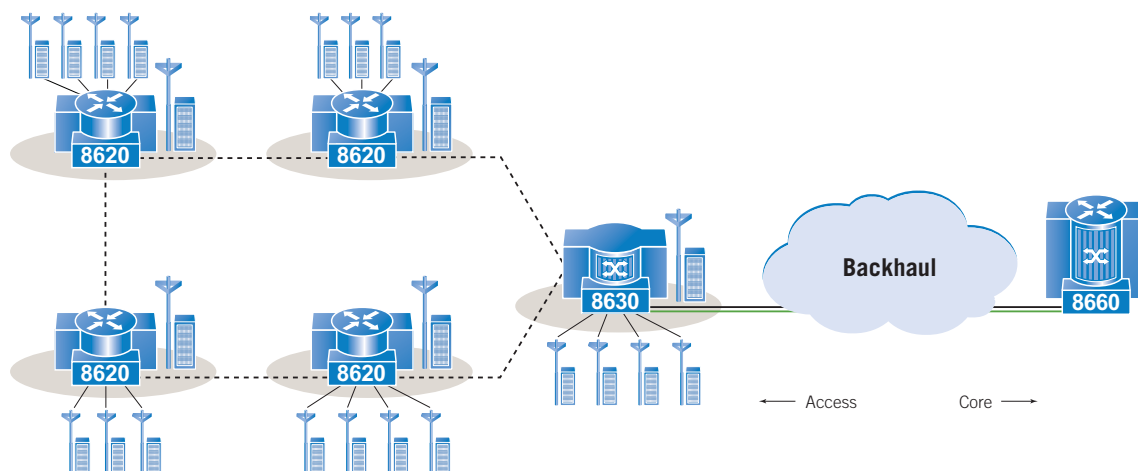


Figure 1. Network architecture

(TDM) services and existing 2G, 3G and 4G services into a single converged network. MPLS-based switching technology provides independence from the underlying transmission technology and MPLS pseudowires extend the portions of the network in which new service or technologies can be effectively employed.

The following features are key attributes to the convergence of the network:

- Structure Agnostic TDM over Packet (SAToP): The nature of a structure-agnostic TDM pseudowire is defined in RFC 4553
- Circuit Emulation Service over Packet Switched Network (CESoPSN): Structure-aware TDM pseudowires are defined in CESoPSN, currently a draft standard in the IETF
- Adaptive Timing: Adaptive timing can be used to synchronize the TDM endpoints (Figure 2).

Network Resiliency

Bidirectional Forwarding Detection (BFD)

BFD provides a fault detection mechanism that enables fast traffic protection. It also works as a trigger for rerouting or for protection switchover at the MPLS layer. When BFD is used in conjunction with Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS) or Resource Reservation Protocol - Traffic Engineering (RSVP-TE), it can provide a fast and scalable solution for detecting faults in the Ethernet network between IP/MPLS routers. Current Hello mechanisms in OSPF or IS-IS cannot provide sub-second fault detection times, but BFD is designed to enable it.

In Figure 3, the Virtual Local Area Networks (VLAN) within the Ethernet network are set up so that the router to the right can see two routes to the router farthest to the left. When BFD is run through both routes, it is possible to quickly detect the fault within the Ethernet network and perform required switchover/rerouting.

MPLS Layer Path Protections with RSVP-TE

MPLS layer path protection provides fast protection switching using a predefined secondary RSVP-TE tunnel path. This technique is interoperable with third-party equipment and uses Explicit Route Object (ERO), along with PATH and RESV messages, to verify and build primary and redundant paths. Sub-200ms switching times can be achieved when RSVP-TE is utilized.

Figure 4 depicts a simple example in which primary and secondary Label Switch Paths (LSP) are set up over different physical paths by establishing RSVP-TE ERO LSPs. In primary path failure, RSVP switches to the protecting LSP, based on RSVP Path Tear message or BFD Control Message timeout.

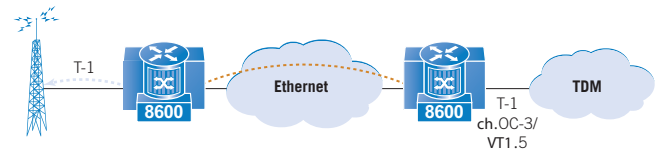


Figure 2. Adaptive timing for TDM endpoints

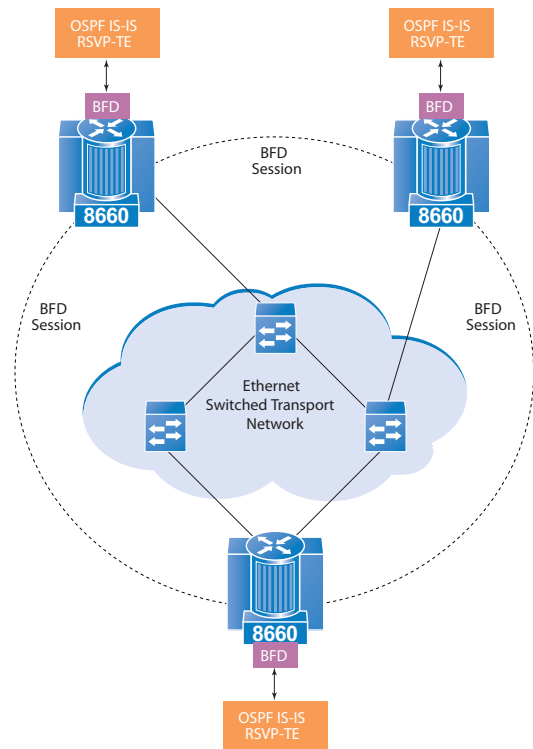


Figure 3. BFD session

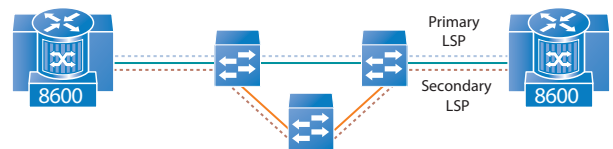


Figure 4. Path protection with RSVP-TE

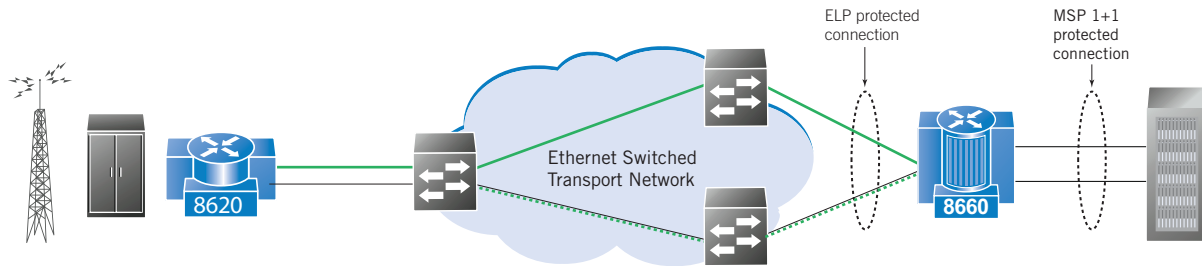


Figure 5. ELP for Ethernet transport network interface protection

Ethernet Link Protection (ELP)

ELP is used to protect the network from Ethernet link failures in various network topologies and applications. For example, it may be used to create a resilient connection between a Tellabs 8600 system IP/MPLS network element and an Ethernet transport network, as illustrated in Figure 5.

In addition to protecting connections between Tellabs 8600 system network elements, ELP may be used in cases where a Tellabs 8600 system network element is directly connected to a third-party network element that supports Ethernet link aggregation (IEEE 802.3ad). From the third-party network element point of view, the Tellabs 8600 system network element looks like a device that also supports link aggregation, but has only one physical link-up at a time.

When the currently active link is detected to be down, the Tellabs® 8660 Edge Switch moves the logical interface (including IP and MAC addresses) from the currently active physical interface to the protecting physical interface. Since IP and MAC addresses remain the same, switchover is transparent to IP and MPLS layers and traffic starts to flow immediately after the Ethernet transport network has adapted to the changed topology. To accelerate Ethernet transport network adaptation, the Tellabs® 8660 switch sends learning frames — gratuitous Address Resolution Protocol (ARP) by using the MAC address of the ELP group as the source address — to drive the Ethernet switches to quickly update switching tables.

Quality of Service

The major benefit of an IP/MPLS infrastructure is that it can simultaneously deliver services with strict quality of service, class of service and Best Effort (BE) delivery. The Tellabs 8600 system uses Strict Priority (SP) and Weighted Fair Queuing (WFQ) scheduling algorithms. The actual WFQ algorithm is based on Start-time Fair Queuing (SFQ). Real-time/ Expedited Forwarding (EF) traffic class and network control traffic (CS7) use SP scheduling, while Assured Forwarding (AF) and BE traffic classes use WFQ. The priority between the AF and BE classes is selected by setting a weight for each class, making it freely configurable by the user. This scheduling architecture supports minimum delay for real-time Figure 5. ELP for Ethernet transport network interface protection Ethernet Switched Transport Network 8620 ELP protected connection

MSP 1+1 protected connection 8660 services, while helping to ensure fair treatment of AF and BE traffic classes. If a higher priority service is not using the bandwidth, all the bandwidth is available to lower priority traffic classes. In the case of congestion (assuming there are no packets in SP queues), WFQ weights guarantee a minimum bandwidth for each traffic class based on its weight.

Delay and Jitter

Delay and jitter must be closely managed when delay-sensitive traffic is transported. There are six delay components that need to be considered:

- Packetization delay
- Signal propagation delay
- Forwarding delay
- Queuing delay
- Serialization delay
- Jitter buffer delay

Packetization delay is dependent on the emulated service bandwidth and the packet size. The delay with SAToP pseudowires is lower than with CESoPSN pseudowires because of the faster service. Packetization delay with the default SAToP payload size (192 bytes) is 1ms. The packetization delay for SAToP pseudowires can be calculated by the formula: $\text{Delay (ms)} = L/S$, where L = payload size (bits) and S = speed of the emulated service (kbps). CESoPSN pseudowire delay performance depends heavily on the number of TDM frames carried within a single packet.

CESoPSN packetization delay can be derived from the following formula, which is derived from the fact that frequency of TDM frames is 8000 per second:

$\text{Delay (ms)} = M/8$, where M = number of TDM frames in the single packet

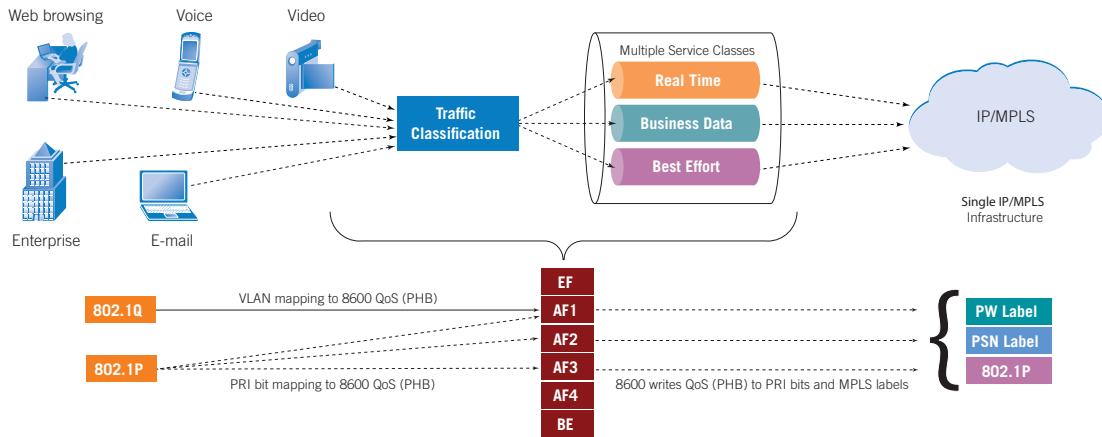


Figure 6. QoS and priority mapping

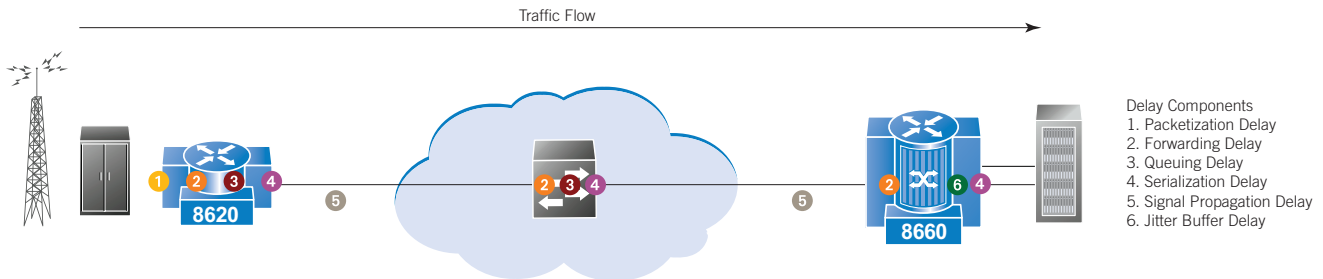


Figure 7. Delay components

Signal propagation delay is the speed of signal in the physical medium, e.g., the speed of light in a fiber is 5 ms/1000 km. Forwarding delay is an internal delay by a packet node making a forwarding decision for a packet. This delay is typically <50 microseconds in modern packet switches.

In packet-switched networks, packets arrive asynchronously into the egress buffers and may need to wait in the buffer before they are scheduled to the physical line. Queuing delay increases if the egress port is congested. Even if the packet is real-time packet, which has high priority, it will experience some amount of queuing delay due to two factors:

- Multiple real-time packets may try to get to the line simultaneously
- Switches typically transmit the entire packet, even if it is low priority, before starting to send a new packet; thus, if a low-priority packet transmission has already started, a high-priority packet must wait until it can enter the line

Serialization delay is dependent on egress port bandwidth and packet size. The calculation formula is:

$$Delay = \text{packet-size (bits)} / \text{port-bandwidth (bits/second)}$$

Since the links in the packet-switched network are typically a much higher speed (e.g. 1 Gbps) than emulated service, serialization delay is typically a lot smaller than packetization delay.

The jitter buffer at egress Label Edge Router (LER) is configured to absorb the packet delay variation caused by the packet network. The jitter buffer target depth defines the operation point (or buffer fill level), which should be valid if there is little or no delay variation in the packet network traffic received by the jitter buffer. However, delay variations inherent in packet networks may cause the jitter buffer to fill over or below the target depth. For example, if packets accumulate into some packet network buffers resulting in a burst, the jitter buffer fill level may go beyond the target depth (depending on burst size and configured target depth).

The delay caused by jitter buffer can be calculated as follows:

$$Delay (ms) = L/S, \text{ where } L = \text{length of jitter buffer (bits)} \text{ and } S = \text{speed of the emulated service (kbps)}$$

Figure 7 details the delay components of the TDM pseudowire.

Tellabs 8600 System Network Elements

The Tellabs 8600 system is a next-generation platform for building advanced telecommunications networks and services. It has been designed to meet the requirements of service providers who need to extend packet switching technologies deeper and deeper into their access networks. While doing so, it provides the reassurance of a true carrier-class platform on which to build and deploy new services.

The Tellabs 8600 system is based on a distributed switching, meaning there is no dedicated switch card. Switching is handled by each of the line cards, which are connected in a full mesh. A switchless architecture results in lower initial costs as the service provider does not have to invest in dedicated switch cards. Instead, the switching capacity increases as the number of interfaces is incremented.

Tellabs 8600 system applications range from the cell site to the mobile core. The platform consists of five products:

- Tellabs® 8660 Edge Switch for large hub sites
- Tellabs® 8630 Access Switch for small and medium aggregation sites
- Tellabs® 8620 Access Switch for small aggregation sites and cell sites
- Tellabs® 8605 Access Switch and Tellabs® 8607 Access Switch for cell sites

Table 1 illustrates the various nodes and key features of each platform.

Tellabs 8600 System Element Redundancy

Power and control functions reside on the Control and DC power Card (CDC) on the end slots of the Tellabs® 8660 switch and Tellabs® 8630 switch nodes for a fully redundant configuration. In between, slots are available for line cards that can be provisioned in protection and non-protection modes.

Control and DC Power Card (CDC)

The CDC is responsible for the following basic functionalities:

- Control plane
- DC power feed for the element
- Synchronization

Due to its fundamental role, the CDC can be redundant to reduce the risk of network outages. Tellabs has taken a long-term approach in the development of Tellabs 8600 system — the platform control plane implements the latest network protocols and the layered and modular architecture allows for flexible upgrades.

Feature	Tellabs 8660	Tellabs 8630	Tellabs 8620	Tellabs 8605 Tellabs 8607
Forwarding Cap. (Gbps)	42	14	3.5	.300
CDC (Control Card)	2	2	N/A	N/A
IFC (Line Card)	12	4	N/A	N/A
IFM (Modules)	24	8	2	N/A
IP routing, MPLS signaling	Yes	Yes	Yes	Yes
IP VPN	Yes	Yes	Yes	No
MPLS pseudowires	Yes	Yes	Yes	Yes
Element height	14U	5U	2U	1U
19" rack-mountable	Yes	Yes	Yes	Yes
1+1 48V DC power	Yes	Yes	Yes	Yes
1+1 Control Card	Yes	Yes	No	No
Switch (forwarding) protection	Yes	Yes	No	No

Table 1. Tellabs 8600 system network elements



Tellabs® 8605 Access Switch / Tellabs® 8607 Access Switch



Tellabs® 8620 Access Switch



Tellabs® 8630 Access Switch



Tellabs® 8660 Edge Switch

Table 2 summarizes the redundancy scheme for the Tellabs 8600 system:

Protections Enabled with 2 CDC Cards	Tellabs 8660 Tellabs 8630
Duplicated data, control timing and power buses	X
Duplicated timing module	X
Duplicated management Ethernet interface	X
Redundant control plane (IP routing and MPLS protocols)	X
Protected configuration backups of line cards	X
Non-service-affecting switchover of CDC (graceful restart)	X
Non-service-affecting software upgrades of CDC	X
Tellabs 8600 system management channel (BMP) protection	X
Duplicated data, control, timing and power buses	X
Separate control and forwarding planes	X
Distributed switching architecture	X
Redundant and temperature-controlled fans	X
Hot-swappable architecture for control cards, line cards and SFPs	X

Table 2. Tellabs 8600 system network element-level equipment redundancy

Network Management System

Network and connection management have become more and more important in today’s networking world. The ability to manage a complex and large network with a limited amount of non-specialized resources is essential for service providers. An efficiently designed management system can help to streamline processes and considerably shorten service delivery and repair times.

The Tellabs network management system’s northbound interfaces are available for different functional requirements. This enables the service provider to implement automated processes over a multi-vendor network. The high-level interface hides the complexity related to internal architecture, simplifying the operation and management of the network (Figure 8).

Tellabs has many years of experience integrating with a number of third-party Operations Support Systems (OSS), including IBM® Tivoli® Netcool® (formerly Micromuse® Netcool), Cramer, HP OpenView® TeMIP, NetCracker®, Elitecore and Servion OSS. In addition, some customers have successfully integrated the platform with other vendors’ solutions, such as Orchestream® and Concord OSS (Figure 9).

The primary advantages of the Tellabs® 8000 Intelligent Network Manager (INM) are:

- End-to-end service and connectivity provisioning results in faster time-to-revenue. Remote configurations, automated processes and service templates help reduce site visits and the time to deliver services.

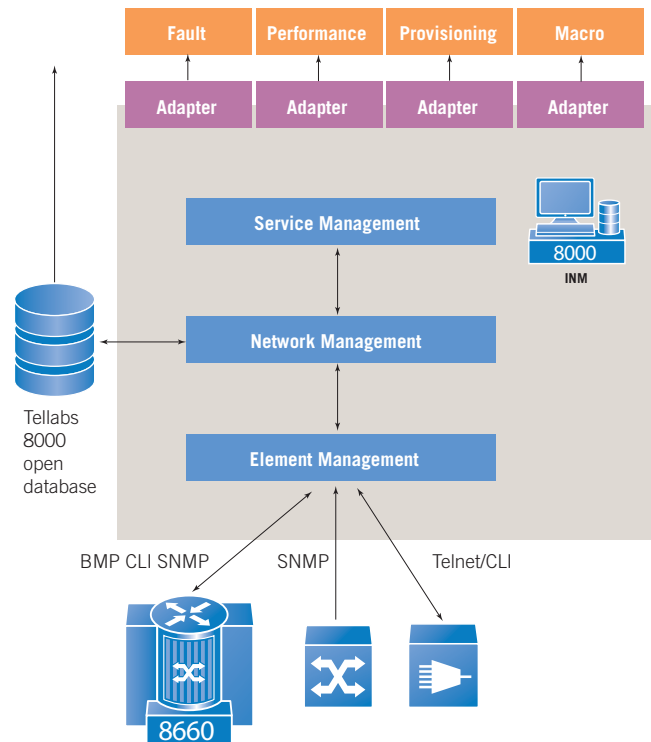


Figure 8. High-level northbound interfaces

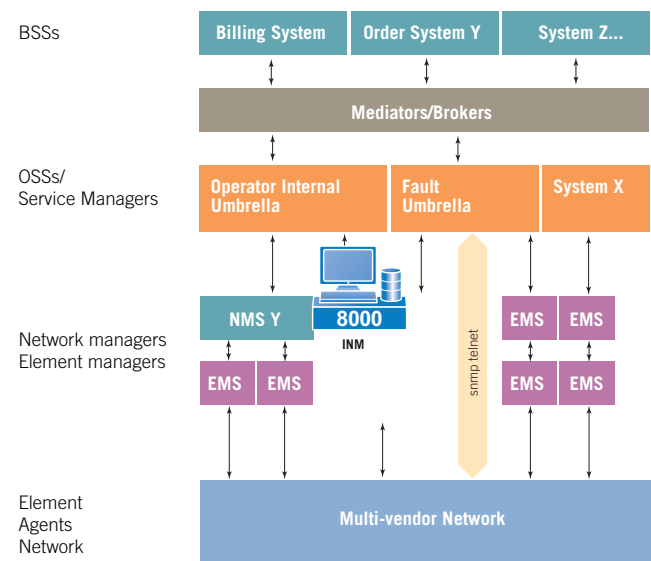


Figure 9. Example service provider OSS environment



- Advanced testing tools for connectivity, QoS and throughput help ensure that high-quality service is maintained for customers, as well as accurate service-level and connection-level data for SLA reporting.
- Fast trouble shooting with proactive and accurate fault identification maximizes network availability.
- A single management solution with support for TDM, ATM, Frame Relay, IP and Ethernet technologies provides an easy upgrade path from TDM to IP.
- No special in-depth technology knowledge is needed, so provisioning can be handled by fewer operators. The advanced Graphical User Interface (GUI) is easy to learn and helps enable fast operations. The system includes comprehensive online help to support users.
- A significant amount of time is saved when compared to the command line approach, especially for large networks.
- Errors can be significantly reduced by using automated tasks and service templates.
- The system maintains a centralized database updated in real-time with modifications made using different tools by multiple users. A consistency check is made between the different network elements and the database notifies the user of any mistakes to prevent entry of faulty configurations.
- Service definitions need only be specified at the top level. The system automatically handles all complex element configurations. Templates make it easier to learn and use these processes.
- Network virtualization supports more effective traffic engineering. Network elements, links and even services can be simulated in the database without updating the physical hardware. This allows different network planning options to be analyzed. For example, the effect on network congestion of a new service can be modeled without changing the physical network in any way.
- Fault and performance data are collected from network elements and correlated to individual services and connections. The overall state of a connection can be checked at a glance. Fault management monitoring covers network elements, links between the elements, and network-wide parameters, as well as the network management system itself.
- The entire Tellabs 8600 system network — devices, configurations, services — is automatically documented in the Tellabs® 8000 Intelligent Network Manager database. For example, service configuration data is stored in the database when a service or connection is provisioned and is kept constantly up-to-date with any changes made to the configuration.
- The distributed architecture helps ensure that there is no single point of failure and maintains consistency between the physical network and its management. The Tellabs® 8000 Intelligent Network Manager is designed to be scalable, quick to integrate and easy to use in order to deliver a reliably running network with simple service provisioning and monitoring.

North America

Tellabs
1415 West Diehl Road
Naperville, IL 60563
U.S.A.
+1 630 798 8800
Fax: +1 630 798 2000

Asia Pacific

Tellabs
3 Anson Road
#14-01 Springleaf Tower
Singapore 079909
Republic of Singapore
+65 6215 6411
Fax: +65 6215 6422

Europe, Middle East & Africa

Tellabs
Abbey Place
24-28 Easton Street
High Wycombe, Bucks
HP11 1NT
United Kingdom
+44 871 574 7000
Fax: +44 871 574 7151

Latin America & Caribbean

Tellabs
Rua James Joule No. 92
EDIFÍCIO PLAZA I
São Paulo – SP
04576-080
Brasil
+55 11 3572 6200
Fax: +55 11 3572 6225

The following trademarks and service marks are owned by Tellabs Operations, Inc., or its affiliates in the United States and/or in other countries: TELLABS®, TELLABS and T symbol®, T symbol®, and SMARTCORE®. Statements herein may contain projections or other forward-looking statements regarding future events, products, features, technology and resulting commercial or technological benefits and advantages. These statements are for discussion purposes only, are subject to change and are not to be construed as instructions, product specifications, guarantees or warranties. Actual results may differ materially. The information contained herein is not a commitment, promise or legal obligation to deliver any material, code, feature or functionality. It is intended to outline Tellabs' general product direction. The development, release and timing of any material, code, feature or functionality described herein remains at Tellabs' sole discretion.