

Operational Efficiency in Evolving Mobile Networks

Manage all required technologies and services in your mobile network with the Tellabs® 8000 Intelligent Network Manager.

Executive Summary

As the next generation 3G mobile networks evolve, they will contain thousands of Node Bs, hundreds of regional hub locations and numerous Radio Network Controller (RNC) sites. The associated Network Management Systems (NMS) should be able to manage these transmission networks with predictable performance even when several people are operating the network simultaneously. The management system needs to be easy to use and provide a Graphical User Interface (GUI) to perform all configurations. It should provide tools for optimizing workflows across all phases from network and service planning, configuration, connection and service provisioning right through to service maintenance. The management system can further increase operational efficiency by automating many of these steps during service operation. A key requirement for every management system is to provide reliable northbound interfaces to the umbrella Operational Support Systems (OSS). The ability to provide high-level interfaces and provide refined high-level data to the OSS helps minimize the overall system integration costs. The Tellabs® 8000 Intelligent Network Manager is designed in collaboration with our customers to address the operational needs of all TDM, FR, SDH, ATM and IP/MPLS-based mobile transmission networks.

Introduction

The majority of today's mobile transmission networks were built to serve the needs of 2G traffic. The deployment of 3G network services is focusing the attention of mobile operators on the evolution from TDM-based 2G transport networks to ATM- and IP/MPLS-based 3G transport networks. The use of High-Speed Downlink Packet Access (HSDPA) for the delivery of content-rich data raises even more issues for service differentiation and QoS handling in mobile transport networks. As 3G networks increase their coverage, the existence of multiple technologies and service classes will cause operators to pay more attention to the operational costs of the networks. Transport optimization and leased line cost management will continue to play a major role in operating expenditure costs. But at the same time, everyday operations and management costs could escalate unless operators implement carrier-class management solutions to handle the next-generation mobile transport networks.

This technical solution description discusses the service provider requirements for an operationally efficient management system of a wireless transport network. It addresses the need to manage all the technologies and services required in 2G and 3G R99, R4 and R5 networks. It describes how the Tellabs 8000 Intelligent Network Manager addresses and solves these challenges.

Issues for Managing 2G and 3G Transport Networks

A network management system must be scalable and reliable in order to manage a large number of network elements and connections. It must be able to support several users simultaneously without degrading system performance or generating network inconsistencies. As the network grows, service providers need easy-to-use tools to perform day-to-day operations so that the number of operational tasks is kept under control.

Today's IP network management systems have a reputation for being difficult to use. Often their GUI-based tools only cover part of the network and service related operations; the rest must be controlled using the more basic Command Line Interface (CLI). Ideally, the network operational staff who performs the daily provisioning tasks should not need to be IP experts; they should not need to understand and specify all the protocol and signaling configurations throughout the network. Instead, they should be able to perform all mobile transport configurations with a minimum of effort across all platforms regardless of the transport technology used for a particular network connection.

Most service providers deploy umbrella management systems to support their business processes. These umbrella management systems in turn connect to various sub-management systems provided by different vendors. If the sub-management system is able to provide high-level data to the umbrella management system, the integration and operational costs can be significantly reduced. In this case, a smaller investment is required to make all the processes work reliably and run smoothly. This places high demands on the capabilities of the sub-management systems. The bottom line is that each sub-management system should be capable of performing the correct network tasks and providing reliable data about the network and the services upwards to the umbrella management system.

Some operators have addressed this problem from a different angle. They have divided their transport network into separate regions and each region will often have a solution from a single infrastructure vendor. In these cases, the capabilities of the vendor's management system will have a significant role in everyday operations. The vendor-specific NMS must be more than just an element manager; it is required to support service and connectivity level tasks and optimize the time and money spent on network level operations like provisioning, online documentation and network modifications.

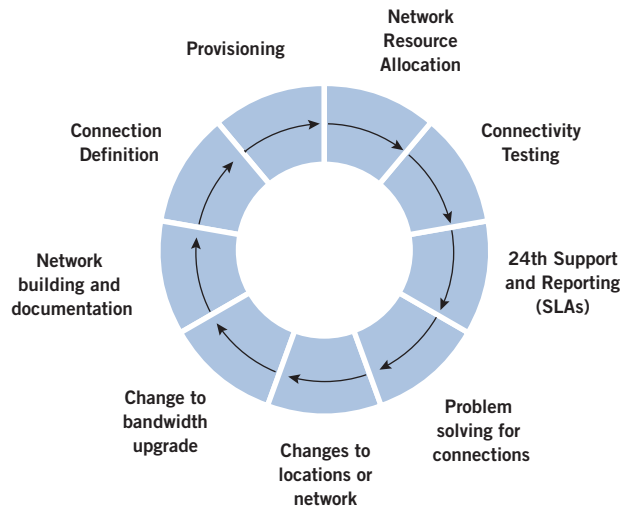


Figure 1: Operational processes during the connectivity life cycle

Service Life Cycle and Operational Processes

As we discussed in the previous section, service providers require easy-to-use tools to manage their evolving networks; especially with the increasing number of E-1 connections from 2G Base Transceiver Stations (BTS) and 3G Node B systems. Let us take as an example the simple E-1 connectivity provisioning from a Node B to an RNC. The complete business process from capacity allocation to end point moves to maintenance must be handled with minimum operational time and effort. Before provisioning the connection, the network needs to be configured properly and the information about the configured network needs to be accurate and up to date before it is presented to the service provisioning application. Connectivity provisioning itself must be straightforward and follow the “right the first time” principle. Getting it right the first time avoids the need for extensive troubleshooting during provisioning. The service availability must be monitored continuously and the error detection tools must be comprehensive and sophisticated.

After it has been provisioned for the first time, the connectivity configuration will almost certainly need to be changed in the future. As more RNCs are added to a given area, reassignment of the connection end point will become a very common task both now and in the future. Also, the need to change the traffic profile and classification policies for a connection will increase significantly. As new mobile applications based on the delivery of data are deployed, data traffic priorities will need to be changed frequently. Traffic classification changes have to be performed without the need for an army of skilled people and the changed configuration needs to be fully documented in the system.

The connection life cycle shown in Figure 1 describes all the phases that a connection experiences as it exists in one network: from allocation and configuration through to maintenance and decommissioning. Regardless of the multiple technologies used in the transport network, all connections must be easily manageable throughout the whole network life cycle. In optimal mobile networks, this means that the same tools and processes are used regardless of the underlying technologies.

NMS Capabilities that help Service Providers to Manage Complexity in Wireless Networks

Nowadays, most connectivity services are delivered using mature technologies such as SDH, PDH, ATM and FR. The platforms that use these technologies have been developed and deployed for over a decade. Similarly, many management systems supporting these platforms have been developed over the years in collaboration with service providers to meet and fulfill their requirements. Service providers have also invested in system integration projects to ensure that their business process platforms are interoperable with all their other systems. The deployment of IP-aware platforms for R5 RAN is currently under evaluation amongst most major service providers. There is little actual experience in how the associated IP management systems will perform in the context of service providers' large scale networks. In these environments, operations are repeated many times a day and fast reaction and response times are expected. The following sections describe some of the essential capabilities required from an advanced and robust network management system operating in such a highly demanding environment.

GUI with Parameterization Templates

As the number of services or connections provisioned per day increase significantly, the management system should have an easy-to-use GUI. In addition, all complicated processes should be automated whenever possible. The information describing the interface, link and circuit or tunnel settings should be defined in windows where the data is logically organized and can be easily entered. This will allow it to be easily checked and reconfigured later on. Different type of views, such as tree and list views, network maps and comprehensive search functions provide the basis for smooth operations. They also provide a visual representation of the network architecture whenever needed. Generally, GUI configuration tools make it much easier to learn to use the system when compared to traditional CLI or ATM management tools. Also, the training period required to teach the network operators is significantly reduced.

As mobile networks become more data-centric, the use of parameterization templates becomes essential. This is especially the case where QoS and traffic engineering configurations require an extensive understanding of the underlying IP technology. By allowing the technical experts to define the parameterization templates to be used, the operational personnel can then focus on the basic operations. Templates also help hide the technical details of TDM, SDH, FR, ATM and IP/MPLS; by hiding the complexity of the network, they greatly reduce the chance of user-induced errors.

Group operations can also help users with tasks that need to be performed several times. An example of a group operation is: end point move. Let us assume that a new RNC is added to the network and several E-1 connections from the Node Bs connected to other RNCs must be moved to the new RNC. With an NMS, which does not support group operations, this task must be performed separately for each and every E-1. Whereas with an NMS, which supports group operations, all the connections can be grouped together, deactivated, reassigned to the new RNC and reactivated. The result is quicker and easier maintenance that causes only the minimum downtime for end-users.

Main Network Management Tools Integrated into One System

In most cases, it is beneficial to have a single management system for all the operations that manage network elements from a particular product family or vendor. Examples of these types of operations are: element installation and set-ups, link configuration, service provisioning service updates (e.g., adding a new end point) and root cause analysis for alarms. The tools which perform these operations exchange large amounts of information related to the network and the services. Therefore it is an essential requirement that this information is entered into the NMS only once, at which point all the tools can share it. When the management tools are integrated into one system, they can utilize the same information base. The information is either entered by the operator or generated by one of the tools as shown in Figure 2. For example, when a connection has been provisioned, other modules such as fault management and testing tools should be able to monitor the same connection and its layout, route and connection details based on the service ID, connection ID or name. The concept of integrated tools guarantees that service providers do not need to perform any special

customization to make the tools work together seamlessly. An additional benefit for operators is that with integrated management tools, the vendor is able to provide useful proprietary capabilities. For example, one tool can execute another tool directly without the operator needing to run it manually. For instance, the provisioning tool can command the network building tool directly to create TE-tunnels in the IP/MPLS part of network.

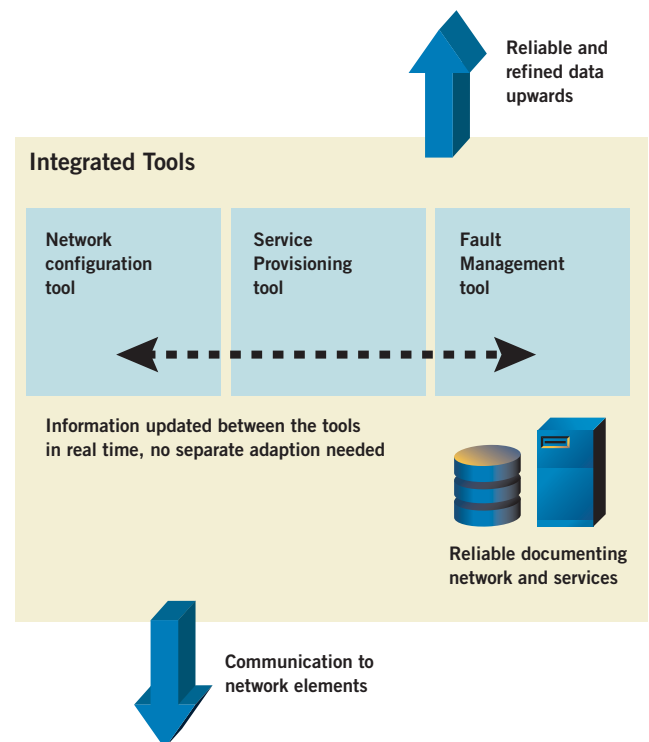


Figure 2: Integrated network management tools streamline operational processes and decrease integration costs for service providers

Reliable Documentation of Network and Services

Network inventory systems provide service providers with up-to-date information about the network and connections at any time of the day or night. An NMS should be able to document the inventory information by itself without the need for a separate inventory tool; service providers want to avoid using any extra tools or adapting new systems to use these tools due to the high costs of building and maintaining adaptation interfaces. Naturally, the inventory data stored by the network management system itself should be available for the umbrella management systems to read.

Everyday operations can be performed much faster if the database contained not only the inventory data, but also the detailed information such as interface settings and connectivity information for every network element. Naturally, database information should be updated automatically every time a change takes place. Once the system has documented all of these details about the network, many operations can be automated. For example, when considering service provisioning and capacity reservation, the system should be able to analyze the available link capacities and utilize only those link capacities available for a certain traffic class.

A single centralized database that stores all the network and service data, guarantees that the information is consistent and up to date. If several network and element level tools have separate databases, there is a high risk that the data will not be properly synchronized between the databases. As a consequence, an operation such as ATM pseudowire provisioning can be highly time-consuming if extra troubleshooting is needed to solve any inconsistencies. With an inconsistent database, the operation could also introduce further problems into the network. For these reasons, both documentation and a centralized database are essential requirements to guarantee that the operator receives reliable and consistent information about the network and services.

Improved Efficiency with Pre-planning

Operators should be able to perform network operations using the network management system whenever it is most suitable from the overall workflow point of view. They should also be able to avoid unnecessary waiting times. For instance, in many cases element installation would be more efficient if the configurations could be designed in the database before being applied to the actual hardware. When the hardware is shipped and installed, the new configurations can be downloaded to the hardware by executing a single command. This pre-planning capability should allow any type of drafting in the network database before activating the hardware. For example, when creating services and connections, all the end-point, link and traffic classification configuration information should be able to be drafted in the database. When the hardware is ready to be activated, the configurations can be updated as fast as NMS performance allows. Obviously, a prerequisite for pre-planning is that all the network and service details are up to date in the database. The pre-planning functionality means that overnight work can be minimized and errors resulting from anti-social working times can be decreased. Additionally, the immediate database reports can identify any potential faulty configurations and restrict the actions to those that are compatible with the actual hardware configuration.

Interoperability with Service Provider OSS

As discussed previously, any newly introduced management system must be interoperable with the other management systems in a service provider's network. It follows that every management system, even if used only for a certain area, should be easily integrated under the service provider's OSS. A network management system — even when integrated under an umbrella system — must support the service provider's specific operational processes, make all the relevant information available for other systems and implement a specialized set of capabilities rather than support isolated point products. An easily integrated network management system provides reliable and refined, high-level data upwards (or northbound) as shown in Figure 3. Typically, this data is related to service or network level objects and the northbound interface itself is based on the Common Object Request Broker Architecture (CORBA).

The main reason that service providers require an open sub-management system with a high-level northbound interface is to minimize the expensive integration and maintenance costs for adapting their OSS. The high-level data should be as refined and processed as possible so that the sub-management system hides the complexity and details of the network and services from the OSS. When the northbound interface model is simple and the sub-management system provides high-level processed data, there is no need to specify and build custom OSS adapters for each vendor. Let us take connectivity provisioning as an example. The umbrella management system should only need to feed the key parameters which define the connection. Using this information the sub-management system executes multiple tasks to create the objects, reserve network capacity and provision an end-to-end connection across the network elements. In this case, the sub-management system processes most of the operations.

The OSS interface will be more stable when the sub-management only provides generic objects upwards. For instance, if a new element is already supported by the sub-management system, the OSS adapter does not need to be updated to support it. A high-level northbound interface therefore results in less version dependencies between the OSS and the sub-management systems. However, in some specific cases service providers will also need an EMS-level northbound interface or even an element CLI interface. In these cases, the interface and interface updates must be well documented to make the OSS adapter coding as easy as possible.

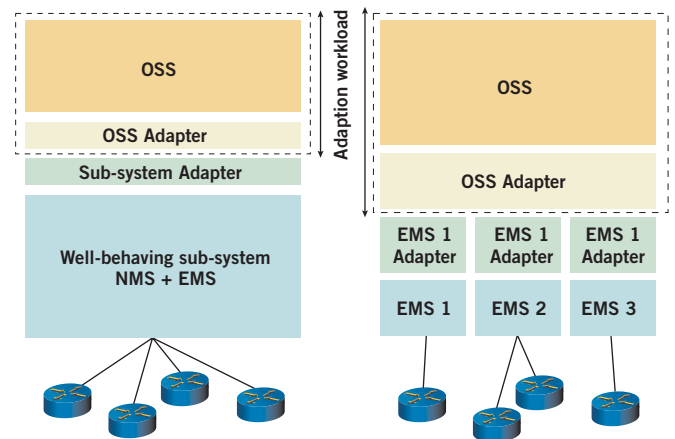


Figure 3: The integration investment decreases with the use of open and easily integrated management systems

Tellabs 8000 Intelligent Network Manager — A Manager for Evolving Mobile Networks

The Tellabs 8000 manager is a carrier-class service provisioning, network management and OSS integration platform. It provides element management system for the Tellabs® 8600 Managed Edge System, the Tellabs® 8100 Managed Access System and the Tellabs 6300 Managed Transport System. It provides scalable tools for service, network and element level operations for networks that can consist of hundreds of thousands of connection end points. The Tellabs 8000 manager has been developed in collaboration with our customers to meet all the requirements that have been discussed in the previous sections.

Operational Processes with Tellabs 8000 Intelligent Network Manager

As we discussed previously, all the processes along the service life cycle, from provisioning to maintenance, need to be efficient to minimize the service provider's total cost of ownership for a service. The following sections highlight how some of these important processes are optimized in the Tellabs 8000 manager.

Network building and monitoring:

- A GUI with hierarchical windows and parameterization templates simplifies the network building and configuration process.
- All of the network and service data is documented in a centralized database. The data can be displayed using comprehensive reports and dialogs. The network topology and hierarchy can be logically monitored using tree views and graphical drawings. Full documentation also helps optimize the network capacity, as it keeps track of all the available capacity, even by traffic class.
- The network level settings are kept consistent throughout the network to minimize the need for troubleshooting and to reduce the possibility of configuration errors.

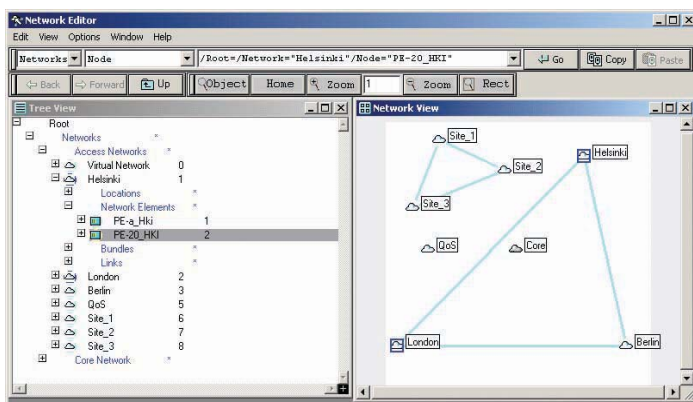


Figure 4: Network configuration tool in the Tellabs® 8000 Intelligent Network Manager

Service provisioning:

- Many operations are automated during service provisioning. For example, when provisioning IP/MPLS connections towards the core network, the operator only needs to define the basic parameters. The service provisioning tool then creates the VRFs and routing instances, allocates and sets route targets, and creates the traffic engineered MPLS LSPs.
- The system minimizes the possibility of incorrect configurations. For instance, the operator is not able to provision new connections to areas where physical link capacity is already being used for other connections.
- All connection related information, such as site location, VRF entries, access lists and tunnels used, is easy to monitor using the provisioning tool.
- For VPN configurations, all of the end points can be set up from a single dialog. If similar settings are needed for other end points, then the copy/paste functionality in the templates tool can be used to save time and reduce the risk of operator errors.
- Traffic classification methods can be created with the help of comprehensive configuration templates.

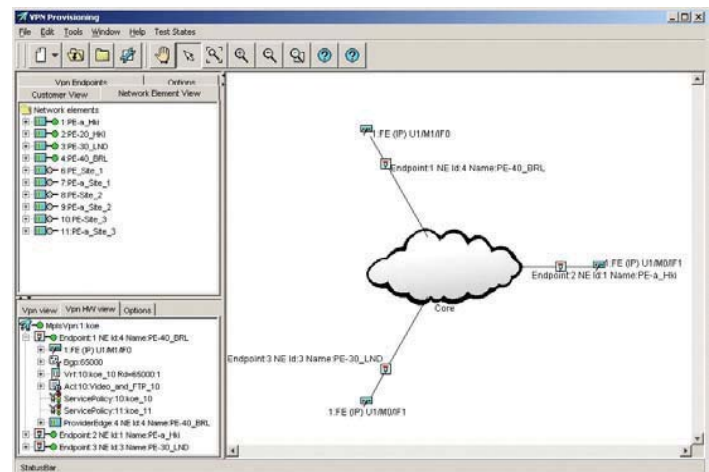
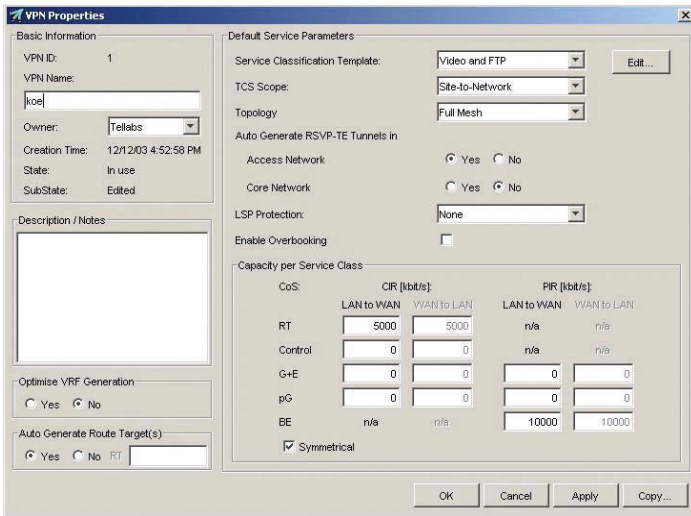


Figure 5: Monitoring a VPN configuration with the VPN provisioning tool

Service testing:

- Tellabs devices include unique capabilities for running automated tests in the network. The results are displayed as reports and graphics that can be saved in the database for later use or can be exported over the northbound interface for third-party systems to analyze.
- Service testing can be performed between two end points or between each set of end points that comprise a connection. The actual tests are run by the built-in test generators and analyzers in the network elements. The NMS functions as a user interface to run the tests and to process and store the test results.



- The following testing modes are available: connection-specific tests including throughput, delay and delay variation tests, traceroute and ping tests; communication to network elements from the communication server; connection and traceroute from network element to network element.
- The testing tools use the same configuration data that has been defined during connection provisioning. This means that the user only needs to type the service ID, customer name or location name to search for the appropriate connection; testing can then start immediately.

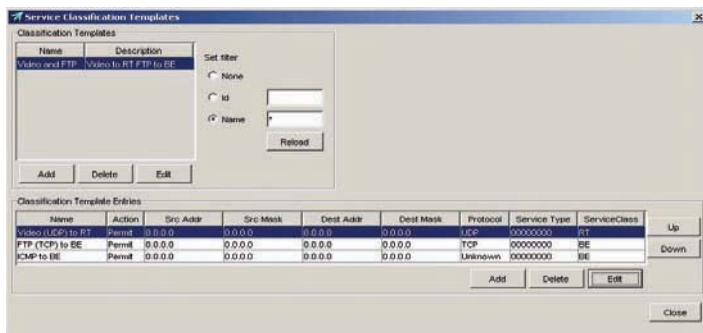


Figure 7: Traffic classification templates allow several entries that define how the packets are classified into different categories

Fault management and performance monitoring:

- The fault management module provides powerful tools to monitor the network status in a way that best suits the operator. Informative fault data and a well-documented network help the operator find the root cause of any faults quickly and perform fault diagnosis easily.
- The fault and performance data collected from the network elements are associated with connections, locations and end-customers. This means that the overall state of a connection can be checked at a glance.

- Fault filtering provides comprehensive methods to filter out non-relevant data from the service provider’s perspective.
- The operator can monitor the network using various types of fault reports and focus on monitoring only certain types of alarms. For example, the operator can choose only to monitor alarms from the MPLS layer.
- All fault and performance data is stored in a single database. The scalable database architecture allows the database to grow safely as the network evolves.

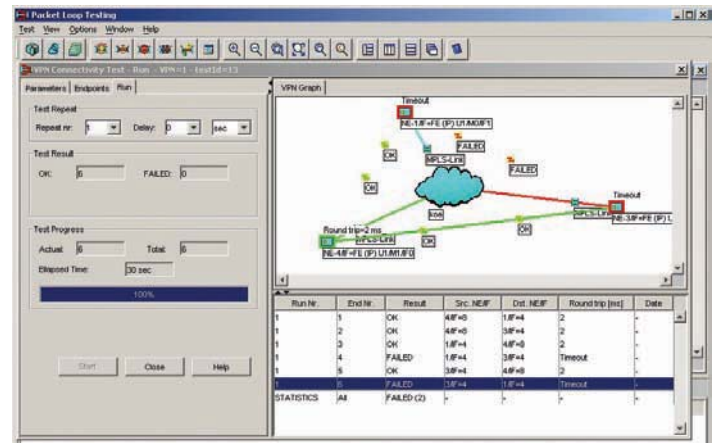


Figure 8: The packet loop testing tool presents the test results in a network diagram and in a test report

The Tellabs 8000 manager also has various wizards and tools to help with many of the typically time-consuming service changes and upgrades. For example, the Tellabs 8000 manager provisioning tool includes the group operation subtool to change settings such as the bandwidth profile for a group of connection end points.

Service Provider Business Benefits with the Tellabs 8000 Intelligent Network Manager

Faster Responsiveness, Lower OpEx

All the aforementioned capabilities in the Tellabs 8000 manager have been developed together with our customers to minimize a service provider’s operational expenses. For instance, it has been calculated that VPN provisioning takes 62% less time when using the Tellabs 8000 manager than when using a system where a CLI is used. One of the major design principles for the NMS is that it should have a fast response time when provisioning, testing, making changes as well as for fault monitoring and isolation. Fast responsiveness correlates directly to better network availability and lower OpEx.

Improved Network Utilization, Lower CapEx

The operationally efficient Tellabs 8000 manager also helps service providers to utilize their network capacity more efficiently. This can save in investments in new equipment and helps reduce CapEx. The Tellabs 8000 manager documents the available and used network capacity and uses this capacity optimally when reserving bandwidth. This helps make traffic engineering management simple and efficient. Additionally, when more network resources are added, a modular and scalable system ensures that the service provider does not keep low revenue-generating resources in the network.

Another aspect of CapEx is the cost of servers and workstations needed to build out the NMS infrastructure. From a single NMS hardware setup, the Tellabs 8000 manager can manage all the TDM, FR, SDH, ATM and IP/MPLS technologies and save in the cost of extra NMS and EMS systems.

Minimum Investment in System Integration, Lower OpEx

The basic management tools for provisioning, fault monitoring and network configurations have already been integrated by Tellabs, saving service providers on integration costs. To adapt to a specific OSS, the Tellabs 8000 manager provides high-level CORBA-based northbound interfaces. These are well documented and fulfill the requirement of OSS subsystems to provide reliable and refined data upwards to the umbrella management system. CORBA-based EMS and NMS interfaces in the Tellabs 8000 manager are also used internally between Tellabs software components. This assures the high quality, stability and high performance of the interfaces. As a result, the Tellabs built-in interoperability concept enables the operator to minimize costs related to in-house adaptation, obviating the need for external consultants for the adaptation and reducing the time required to troubleshoot and fix inconsistencies caused by incorrect integration. In summary, Tellabs solutions are built to optimize the cost of integration, operation and required hardware.

Acronyms

ATM	Asynchronous Transfer Mode
BTS	Base Transceiver Station
CORBA	Common Object Request Broker Architecture
CLI	Command Line Interface
EMS	Element Management System
FR	Frame Relay
GUI	Graphical User Interface
IP	Internet Protocol
LSP	Label Switched Path
MPLS	Multiprotocol Label Switching
NMS	Network Management System
OSS	Operational Support System
QoS	Quality of Service
RAN	Radio Access Network
RNC	Radio Network Controller
SDH	Synchronous Transfer Hierarchy
TDM	Time Division Multiplexing
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

North America

Tellabs
One Tellabs Center
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