This paper introduces different technologies used to provide EoSDH, and the associated benefits for the operator and their customers.

Executive Summary

Public network access for business customers has, traditionally been based on a PDH or an SDH network.

Over the years PDH and SDH technologies have developed into high-quality networks for TDM applications like voice and leased lines. However, traditional SDH is not optimised to meet today’s needs for huge data traffic growth and the demand for new and differentiated data services.

Next-generation SDH incorporating Ethernet-over-SDH (EoSDH) capabilities makes SDH an ideal platform for data requirements, as it combines efficient data transport with the carrier-class protection inherent in SDH and the stability of a proven, widely deployed technology.

The Tellabs 6300 range of EoSDH solutions utilises into four key technologies:  
- EoSDH Mapping (incorporating virtual concatenation and LCAS).  
- EoSDH MPLS transport.  
- EoSDH MAC switching.  
- EoSDH IEEE 802.1q tagging.
**EoSDH Mapping**

This is a technology that efficiently map Ethernet frames into SDH Virtual Containers (VCs), which in turn are transported through the EoSDH network and delivered as Ethernet frames from the EoSDH network.

The benefits of this technology include:
- An Ethernet service interface which is lower cost than the traditional E-1, E-3 or STM-1, thus lowering an operator’s capital expenditure (CapEx).
- An interface type that can span a broad range of access speeds, removing the need for site visits to provide service upgrades and thus lowering an operator’s operational expenses (OpEx).
- Flexible bandwidth allocation to the customer down to steps of 2 Mbit/s, as opposed to the usual step in PDH/SDH: E-1 to E-3 to STM-1 to STM-4. This not only uses the network more efficiently but also allows the operator to expand the service offering and improve competitiveness.
- A new protection capability through a feature called Link Capacity Adjustment Scheme (LCAS) that can effectively double network capacity when compared to traditional SDH protection.
- More efficient utilisation of the network and more network flexibility through Virtual Concatenation when compared to traditional Contiguous Concatenation.

**EoSDH MPLS Transport**

This is a technology that encapsulates Ethernet frames within Multi-Protocol Label Switching (MPLS) and transports them through the MPLS enabled SDH network and again delivers them as Ethernet frames.

The benefits of this approach include:
- Over-subscription in the SDH network, allowing up to 100 times improvement in network utilisation.
- The ability to offer differentiated services e.g. leased line, burst or best-effort services, similar to ATM and Frame Relay services. In contrast an EoSDH mapping solution or the traditional SDH solution can only offer a leased line service.
- Controlled over-subscription in the network — due to differentiated services.
• Security levels on a par with a traditional leased service, Frame Relay/X.25 service or ATM/MPLS VPN service.

**EoSDH MAC Switching**

With EoSDH MAC switching an Ethernet switch is installed in some of the EoSDH enabled SDH network elements. The VCs or MPLS LSPs terminate at these Ethernet switches, turning the EoSDH network into a full blown Ethernet Private Network (EPN) similar to Frame Relay and ATM, but now based on standard Ethernet technology.

The benefits include:
• Using the SDH network to create a wide area Ethernet private network.
• Re-use of the same technology used in the Local Area Network LAN as in the wide area for the first time in the industry.
• Using the SDH network to create multiple private Ethernet networks so that each customer receives their own wide area Ethernet i.e. basically turning the SDH network into a Virtual Private Network (VPN).

**EoSDH 802.1q Tagging**

With EoSDH — 802.1q tagging, the operator can offer several service classes to the customer, e.g. at one single interface.

The benefits include:
• At the customer or the operators access router differentiated services can be offered on the same Ethernet interface, e.g. a customer can request and receive a leased line for voice traffic, burst for business oriented data traffic and best effort for non-business oriented traffic, all offered on one Ethernet interface.
• At the operator’s access router multiple customers can be attached to the same Ethernet interface and still keep complete privacy. This could be an IP access router or an MPLS Provider Edge router, meaning huge savings in interface cost, footprint, equipment etc.

**Introduction**

Network operators are facing an increasing demand for Ethernet based services, both as a low-cost and flexible data interconnection service, and as an interconnection method for
next-generation Digital Subscriber Line (DSL) — i.e. to support a migration from ATM to Ethernet based DSLAM-BAS interconnection.

At the same time operators and service providers are facing competition that challenges them to utilise their network and staff in a more efficient manner, and offer more flexible and customer tailored solutions.

Ethernet-over-SDH is an effective response to these challenges. By integrating Ethernet based services and SDH transport, much greater utilisation of an existing SDH network can be achieved. By leveraging existing SDH personnel and processes, EoSDH also offers a very operationally efficient way to introduce Ethernet services, minimising operational expenses.

This white paper provides the following:
• A review of the limitations within a conventional SDH network for data transport.
• An overview of the different technologies utilised in providing EoSDH.
• A description of the different technologies utilised in providing EoSDH.

This paper does not cover the application of the technologies described. For this, please refer to Tellabs EoSDH application notes.

Background and Scope

In today’s Wide Area Network (WAN) environment, the customer is connected to the operator’s data network via a range of different access technologies, including:
• SDSL
• HDSL
• G.SHDSL
• VDSL
• Radio links running 2 Mbit/s
• Radio links running 34 Mbit/s
• E-1
• E-3
• STM-1
• STM-4
• Etc.

The reason for all these different technologies is as extensive as the technologies themselves, e.g.:
• The lowest cost or most efficient type at the time of deployment.
• The only option at the time of deployment. (due to standardisation etc.)
• The only option due to the customer’s location. (POP versus radio links)
• The only option due to technology development. (for instance PDH/SDH access)

However drawbacks exist in one form or another with all of these access approaches.

**Inflexible Granularity in Bandwidth Offerings to the Customer**

From a more technical point of view, the drawback with almost all access technologies (except for some of the DSL technologies) is that the granularity in bandwidth is very limited.

Typically the following capacities and interfaces will be delivered to the customer:
• 2 Mbit/s via E-1
• 34 Mbit/s via E-3
• 155 Mbit/s via STM-1
• 622 Mbit/s via STM-4

The consequence of this limited granularity and inflexibility in service offering includes:
• Inflexible service offerings to the customer which means an upgrade from for instance 8 Mbit/s (realised via 4 E-1’s) to 12 Mbit/s (typically is realised via E-3) (E-1 pricing inhibits the use of 6 x E-1s).
• Wasted capacity in the access network, leading to the necessity for earlier network upgrades. Depending upon when the network hits a grooming point (for instance access router or MPLS PE) this waste in bandwidth can continue for miles and miles.
• Loss of competitiveness compared to new operators who can offer a finer granularity, perhaps down to the VC-12 level or even lower.

**Inflexible and Expensive Interfaces**

The “traditional” access methodologies (E-1, E-3 etc.) have different physical interfaces. This means that when a customer requests a capacity upgrade (from, for instance, 6 Mbit/s to 8 Mbit/s = 3*E-1 to 4*E-1) an E-1 interface needs to be installed at the customer premise and
assigned at the operator’s network: Interface changes increase capital investment in equipment and if the customer is providing the CPE, this expense is highly visible.

Changes of interfaces are also a heavy burden on OpEx as a field engineer has to be dispatched.

Many Expensive and Inflexible Interfaces at PoP and Operator Access Sites

The “traditional access technologies” are based on traditional PDH or SDH, meaning point-to-point connections, which in turn lead to multiple physical interfaces on IP access equipment. The consequence of this is:

- Expensive access routers for Internet or VPN services.
- Increased space and power requirements due to bigger access routers, SDH equipment and cabling.
- High OpEx, due to recabling, multiple interfaces, spare parts etc.

Traditional TDM Multiplexing is Not Optimal for Bursty Data Applications

Traditional access services were
developed for voice and real time applications, making use of time division multiplexing (TDM). A major part of the today’s bandwidth is used for data that do not require a strict TDM service on the contrary, they are bursty by nature meaning they expect multiples of bandwidth in bursts. On the other hand they do not utilise bandwidth the majority of the time.

Adding statistical multiplexing will create huge benefits by adding packet multiplexing into the access network, thereby enabling over-subscription in the access as an alternative to doing the oversubscription in the IP access equipment which will:

• Meet the customer’s requirement for burst requirements.
• Make much more efficient use of the existing SDH access network, and there by postponing the need for capacity upgrades and capital expenditure.
• Due to over-subscription and packet multiplexing, it is possible to resell the capacity several times, giving benefits of scale that enhance the operator’s competitiveness.

**Ethernet-over-SDH Technologies**

Ethernet-over-SDH is a very promising solution to the above-mentioned challenges.

Specifically with EoSDH the operator will benefit from the following:

• One single low-cost interface type — Ethernet. As opposed to the traditional PDH/SDH E-1, E-3, STM-1 etc.
• Flexible granularity in bandwidth — the customer can order and receive bandwidth down to a granularity of 2 Mbit/s or sometimes as low as 100 kbit/s, as opposed to the traditional steps in E-1, E-3, STM-1 etc.
• Service bandwidth upgrades/downgrades from the network management system, as opposed to today’s solutions, where a field engineer visit to the customer and PoP/central office is necessary.
• Ethernet packet multiplexing in SDH, which allows for over-subscription in the SDH access layer. This gives greater access network efficiency as opposed to transporting the data all the way to an IP access router before doing the grooming and over-subscription.
• Ability to support differentiated services and Quality-of-Service (QoS) in the SDH access network, as opposed to the traditional leased line service; hence now burst or best-effort services can be offered.

• One single interface, to the operator’s data access equipment (traditional DAS or IP MPLS PEs), as opposed to the many expensive traditional E-1, E-3, STM-1 etc reducing equipment and the associated cost in terms of additional footprint, recabling etc.

All the above can be offered via EoSDH. However EoSDH is more than one technology: it is in fact four technologies of which each offer a subset of the above mentioned benefits, and which can be combined in order to offer the customer the best solution for the customer’s demand.

The four technologies are:

• EoSDH mapping
• EoSDH MPLS transport
• EoSDH MAC switching
• EoSDH 802.1q VLAN tagging

A technical description of each of the four technologies now follows.
EoSDH Mapping

In this solution a SDH access Add/Drop Multiplexer (ADM) or Terminal Multiplexer (TM) is equipped with an Ethernet interface as an alternative to a traditional PDH or SDH interface. The Ethernet traffic received on the interface is mapped into a number of VCs and transported in these VCs (i.e. all SDH nodes these VCs are passing through need no knowledge about Ethernet) to the destination, where the data is unmapped and forwarded out on the specified Ethernet interface.

Thus EoSDH mapping provides point-to-point connections where the traditional interfaces (for instance E-1) are replaced with Ethernet interfaces.

EoSDH mapping as such is a point-to-point solution and offers the following benefits:
• One low-cost interface type, Ethernet, as alternative to E-1, E-3 etc.
• Flexible bandwidth allocation, for some vendors down to 100 kbit/s, as an alternative to n*E-1, E-3, STM-1 etc.
• Additionally EoSDH mapping gives more benefits with respect to bandwidth and network utilisation in the sense of: Virtual concatenation, as opposed to
contiguous concatenation, which gives a huge benefit in utilisation and flexibility of the SDH network.

• LCAS, as a new protection method as opposed to traditional SDH protection, which effectively doubles the capacity while providing the same bandwidth to the customer.

Virtual Concatenation

Virtual concatenation is standardised in accordance with ITU-T G.707 and ANSI T1.105.02

Virtual concatenation addresses the flexibility and scalability problem in traditional SDH networks. The flexibility problem comes into play in the fact that until now capacity, through the SDH network has been assigned in steps from VC-12 to VC-3 to VC-4. This is not a very flexible bandwidth assignment as it both wastes capacity and is not satisfying for customers.

When the interface is changed from G.703 etc. to Ethernet a more flexible approach like assigning capacity at the lower VC level, as opposed to the traditional step levels, is beneficial.

**Figure 4 — Problems With Contiguous Concatenation**

- 10 Mbit/s — VC-3
- 100 Mbit/s — VC-4
- 1 Gbit/s — VC-4-16C
However the bandwidth restrictions from the “traditional” SDH world are still causing problems:

- A 10 Mbit/s Ethernet connection needs to be carried in a VC-3 (45 Mbit/s). This is only 20% utilisation.
- A 100 Mbit/s Ethernet connection needs to be carried in a VC-4 (140 Mbit/s). This is only 66% utilisation.
- A 1 Gbit/s Ethernet connection needs to be carried in a VC-16C (2.5 Gbit/s). This is only 41% utilisation.

A more flexible approach would be if a number of low-order VCs could be concatenated to carry a 10 Mbit/s Ethernet connection. This could be offered via 5 concatenated VC-12s (as opposed to before where a VC-3 was needed).

An even more flexible solution would be if the customer’s bandwidth demand could be specified at low-order VCs for instance, a 24 Mbit/s connection could be delivered via Fast Ethernet and 12 *VC-12s. If the customer wishes to upgrade from, for instance, the 24 Mbit/s to 36 Mbit/s, this would simply be realised by adding a number of VC-12s to the connection.

The solution is virtual concatenation, where VCs are combined to form a Virtual Concatenation Group (VCG). The virtual concatenation is defined at the entry and exit point of the network (Ethernet interfaces), thus the SDH nodes within the network need not to have any knowledge of the virtual concatenation.

Another advantage is that the VCs in a VCG don’t have to traverse the same trail, giving a more flexible approach to VC assignment and a better utilisation of the network. Due to this the different VCs might take different tours through the network, and end up arriving with different delays. In an EoSDH solution, the traffic transported in a VCG is delivered as Ethernet frames, meaning that this differential delay have to be compensated for. This delay compensation is made in the exit node, before the data is passed to the Ethernet interface.

Virtual concatenation also opens up a “new” protection method. As the VCs are not traversing the same trail, then if any
one particular trail fails only a part of the connection is affected. It is this phenomenon that LCAS exploits.

If you would like more information about virtual concatenation, please refer to the ITU/ANSI specifications.

**Link Capacity Adjustment Scheme**

Link Capacity Adjustment Scheme (LCAS) is standardised according to ITU-T G.7042.

LCAS is another fairly new standard that offers large potential benefits for data service deployment.

In traditional SDH, protection has typically been based on two complete separate trails established through the network from entry to exit point. One trail is selected as the primary, and all traffic is passed on that trail. The other trails acts as back-up, ready to take over the traffic in case of a failure in the primary trail. The secondary trail is unused until a failure occurs.

In a traditional TDM world, where the trail is serving voice, video, SNA or other time delay sensitive applications, this approach makes sense. However in a bursty data world this complete 1:1 protection may not be necessary and is a potential waste of bandwidth.

LCAS offers a solution that combines the best of the SDH world with the actual requirements of the data world.

*Figure 5 — LCAS as a New Protection Method*
Typically a data service will be offered with no protection. However due to the fact that more and more mission critical services use data applications, a demand for protection is arising. But even though data services will require more and more protection, it not very likely that 1:1 protection would be preferred, an alternative could be to offer “half” protection using LCAS:

- A protected trail is established between the two end points.
- Instead of one trail being completely empty, traffic is transported on both trails, so as opposed to SDH protection, the “back-up trail” is used in this case.

If one trail fails, LCAS ensures the connection remains but with degraded capacity (for instance from 26 Mbit/s to 12 Mbit/s), as opposed to traditional protection where the capacity remains the same. In a TDM world for voice or video applications, this would be intolerable. However for a data service the consequence will be a matter of slower download of files, and slower transactions, which would be acceptable for a smaller period of time, particularly if accompanied by a lower price when compared to a fully protected service.

If you would like more information about LCAS, you are referred to the ITU/ANSI specifications.

The bottom line is that LCAS gives the ability to effectively double the available network capacity compared to a traditional SDH full protection scheme, and enables an operator to offer a new way of service protection.

Another benefit of LCAS is that the technology can offer hitless change of bandwidth, meaning a VCG can be up or downgraded without any loss of data. However from a data application point of view — and thereby from a typical EoS/DH subscriber point of view — this function might be less important as data applications are used to packet loss.

### Bandwidth Adjustment — Sizing to the Pipe

Clearly when transporting bursty data applications that arrive at a Fast Ethernet speed of 100 Mbit/s over, for instance, a 4 Mbit/s pipe (2 x VC-12’s) some kind
right sizing or traffic shaping is needed. This traffic shaping is typically done via a leaky bucket algorithm that resides at the Ethernet interface.

The leaky bucket algorithm is simple:
• Traffic arrives at the Ethernet interface at wire speed.
• Every Ethernet interface has an associated bucket, although in some instances there could be several buckets, where each bucket is associated with a different class/type of service e.g. one bucket for best-effort service or one bucket for leased line service etc.

• In the bucket is a hole that corresponds to the capacity that is allocated through the network, for instance 4 Mbit/s.
• The depth of the bucket is equal to a burst size. This is the number of Ethernet frames that can wait for transmission.
• As long as the transmitter sends traffic below the 4 Mbit/s threshold all frames are transmitted.
• If the transmitter starts to send at a rate exceeding 4 Mbit/s the bucket will start to fill.
• If the transmitter continually transmits more than 4 Mbit/s the bucket will become full, and frames will be dropped.
• This drop of frames will continue until the transmitter slows down and allows the bucket to empty.

This drop of frames can, from a traditional transmission point of view, seem very drastic, but by adjusting their speed accordingly and retransmitting frames that have been dropped almost all data applications are designed to cope with this. So from a data point of view this is a common concept.

**EoSDH Mapping — a Summary of the Benefits**

The use of EoSDH mapping technology provides a number of advantages when compared to the use of traditional SDH access for delivering data services:

• One low-cost interface type — Ethernet.
• Flexible bandwidth allocation, via virtual concatenation, this flexibility is typically down to the VC level, and for some vendors down to even lower values which enables the SDH network to be utilised in a highly flexible manner.
• A new protection method, via LCAS, which can effectively double the capacity required compared to traditional protection schemes and enables the operator to offer “a third protection option” to its customers.

**Figure 7 — Benefits With Ethernet-over-SDH**
EoSDH MPLS Transport

EoSDH mapping as described in the previous section also has some limitations that could be better addressed. These are:

• Static mapping of Ethernet frames into VCs does not fit well with the bursty nature of data traffic. Some statistical or packet multiplexing is required in order to support bursts and over-subscription.

• EoSDH mapping alone provides a basic Ethernet-over-SDH solution suited for leased line replacement. It provides no means to create multiple service classes to suite the varying needs of data applications e.g. best-effort service for Internet access, burst services for Intranet applications and guaranteed service for mission critical applications.

These drawbacks are addressed using MPLS transport, an approach Tellabs uses in its Tellabs 6300 range of EoSDH solutions.

MPLS Types

MPLS generically is “only” an encapsulation protocol, meaning that:

• Traffic that enters into the MPLS network is encapsulated within a MPLS label.

• Traffic is forwarded through the MPLS network via these labels i.e. the IP or Ethernet addresses in the packets are not used.

• When the traffic reaches the destination, it is delivered as received (IP, Ethernet, etc.) i.e. the customer has no visibility of the MPLS function.

In this respect MPLS is very similar to other encapsulation protocols such as Frame Relay, X.25 or ATM.

In the past MPLS has been marketed to deliver IP MPLS VPNs as a new type of public data service, meaning IP aware equipment has been necessary.

However MPLS can also be implemented via the Martini draft specification. The Martini draft specification specifies how MPLS can be used to offer Layer 2 VPN services with QoS as opposed to the traditional IP MPLS that requires IP functionality.
The following describes the difference between IP MPLS and the Martini draft specification.

**IP MPLS Theory**

An IP MPLS network consists of three components:

- **Customer Premises Equipment (CPE).**
- **Provider Edge (PE) router; this is also called the edge Label Switch Router (LSR).**
- **Provider (P) router also called the LSR.**

The CPE router interfaces to the network via standard interfaces (E-1, E-3, Ethernet etc.) and standard routing protocols (static routes, RIP, OSPF, BGP).

The **Provider Edge router:**

- Receives and forwards traffic to and from the CPE.
- Assigns MPLS labels and encapsulates the traffic going into the MPLS network in MPLS labels.
- Remove the labels from traffic going out of the MPLS network.
- Send the traffic out of the correct interface with the correct Layer 2 framing (for instance Ethernet).

The **provider router:**

- Transports the MPLS packets through the network.
- Changes the label on the MPLS packet. As an MPLS label only has point-to-point significance, the label is changed by every provider node it passes along the way to the destination.

---

**Figure 8 — IP MPLS Theory**

![Figure 8 — IP MPLS Theory](image-url)
The new label is determined via a label table that resides within the provider router.

- The label table specifies what new label should be assigned, and from what interface the MPLS packet should be forwarded.
- When the new label has been assigned the packet is forwarded out on the correct interface.
- In total the path in the MPLS network is called the Label Switched Path (LSP).

The PE routers use the physical interface and IP address in order to decide what MPLS label should be assigned to traffic coming from the CPEs. This means that the PE needs to understand IP and IP routing protocols (OSPF, BGP etc.).

The provider routers however only use the MPLS labels for the switching decisions. This means that provider routers don’t need IP knowledge.

However, in practice the provider routers need to understand IP and IP routing protocols, due to the methodology used in MPLS label assignment and traffic engineering etc. (a description of this is outside the scope of this document).

**Martini Draft Specification**

The Martini draft specification is an MPLS implementation that does not require IP or routing capabilities. The Martini draft can be described as follows:

- In the Martini draft only the physical port is used as discriminator for label assignment, as opposed to IP MPLS,
where both the physical port and the IP address is used in label assignment.

- MPLS packets are forwarded in the same manner as in IP MPLS, i.e. the label is checked and changed by every MPLS enabled SDH node that the MPLS packet meets as it moves through the MPLS network.
- At the edge of the network the label is removed (POPed) and the packet is handed to the CPE in the same manner as within IP MPLS.

The major difference between IP MPLS and Martini MPLS is that IP is used as the distinguisher in IP MPLS, but Martini MPLS uses only the physical port (or 802.1q tagging).

### EoSDH MPLS Transport

Tellabs has based its EoSDH solutions on MPLS transport and the Martini specification. This means:

- Traffic that enters the MPLS domain on an Ethernet port or in a VCG is assigned a label.
- The traffic is encapsulated in MPLS with the assigned label and transmitted out on a specified VCG.

- The traffic is standard SDH switched through the network until it reaches an MPLS enabled PDH/SDH node.
- The MPLS enabled PDH/SDSDH node checks the label, assigns the new label and transmits it out on a specified VCG.
- At the edge of the network, the label is POP’ed and delivered as a native Ethernet frame.

Since the MPLS frames are transported in VCGs, the traffic can be transported through non-MPLS aware SDH node, this means the number of MPLS nodes can be limited according to the customer traffic flows.

### Packet Multiplexing, Over-Subscription and Data Privacy

MPLS is a packet oriented protocol, meaning that the Ethernet frames are encapsulated in MPLS and label switched through the MPLS network based on these labels. The positive consequences of this are:

- Support of the bursty behavior from the data applications, using a packet oriented protocol in the LAN as well as in the Wide Area Network (WAN).
• Support of bursty data applications to meet the customers demand for bursty WAN services.

• Support of packet multiplexing to give the possibility to oversubscribe the SDH network, i.e. more efficient utilisation when having bursty customers.

• Encapsulation of the Ethernet frames into MPLS to assure customer privacy at the same level as ATM or Frame Relay network, even though the traffic is transported over the same VCGs.

**Differentiated QoS and Controlled Over-Subscription**

Over-subscription in itself only gives the possibility to utilise the network much more efficiently. It can only offer a best-effort service to customers, i.e. a service similar to Internet access with no bandwidth guarantee.

However with a Tellabs EoSDH-MPLS based solution it is possible to offer differentiated service classes. These could for instance be:

• **Best-effort service** — no guarantee or promises, just a huge pipe into the network. Could be used for standard Internet access.

• **Burst service** — a guaranteed minimum bandwidth with peak possibilities. Could be used for standard LAN-LAN interconnection.
• Differentiated real-time service — a minimum bandwidth with peak possibilities with lower and constant delay. Could be used for compressed voice and video.

• Leased line service — a constant bandwidth, low delay, could be used for voice, video and other real-time applications.

The differentiated service classes are implemented in the EoSDH-MPLS transport solution via the network management system (NMS) in the following way:

• The NMS knows all the available VCGs in the network.

• The NMS knows all LSPs that are all ready configured throughout the network and used for customer traffic.

• The NMS knows the traffic profile of each LSP, i.e. guaranteed bandwidth, peak bandwidth and maximum delay.

• When a new connection i.e. a new site needs to be established, the end points (physical Ethernet ports) are identified to the NMS, and at the same time the traffic profile for this new connection is specified.

• Based upon the NMS system’s knowledge about the available VCGs (and thereby the available network resources) and the LSPs that are already
provisioned, (and thereby the utilisation of the VCGs), the connection can be granted/not granted.
• Based upon the above, the NMS also finds the best path through the network.
• The NMS is also responsible for assigning labels and downloading these labels to the MPLS enabled SDH nodes, so these can make the actual label swapping.
• The NMS is also responsible for downloading the traffic profile to the MPLS SDH nodes switches.
• This traffic profile download is used in the QoS process and is explained in the following section.
• After the LSP’s have been provisioned the customer traffic can start to flow.

Now that the LSPs and the traffic profile have been defined and downloaded, it is time to look into how QoS is realised. The process is as follows.

When the Ethernet frame arrives at the first MPLS enabled SDH node the packet is labeled (as described earlier).

Then the first MPLS enabled SDH node marks the packet according to whether it corresponds to the traffic profile:
• If it is a burst service (with a minimum bandwidth and with the right to burst up to a peak limit), and the traffic is within the guaranteed bandwidth limit, the packet is forwarded to the output queue.
• If it is a burst service, and the traffic is between the guaranteed bandwidth and peak bandwidth, the packet is marked (via the MPLS Exp bit).
• If there is enough capacity on the VCG at this very instance (i.e. the output queue is not too full) the packet is placed in the output queue and will be transmitted.
• If there is NOT enough capacity on the VCG at this very instance (i.e. the output queue is filled up to a certain level) the packet is dropped.

The above description is related to the first MPLS enabled SDH node the customer traffic meets.

When the MPLS packet is received by MPLS enabled SDH nodes within the network, the process is as follows:
• A look-up in the label table is made in order to find the new label and to define the physical interface (or VCG) that the MPLS packet will be sent out on.
• If the MPLS label is not marked, i.e. the packet is within the traffic contract, the packet is placed in the output queue and will be transmitted.
• If the MPLS label is marked i.e. the packet is outside the guaranteed bandwidth and if there is enough capacity on the VCG at this very instance (i.e. the output queue is not too full) the packet is placed in the output queue and will be transmitted.
• If the MPLS label is marked and if there is not enough capacity on the VCG at this very instance, the packet is dropped.

So guaranteed traffic will always get through the network while non guaranteed traffic will only get through when there is no congestion.

Fine Granularity

MPLS offers one more advantage, namely that it can provide an even finer granularity in bandwidth assignment, than down to the VC level.

In MPLS the bandwidth is specified at LSP set-up, and this specification can be done below the VC-12 level, for instance at steps in 100 kbit/s.

The positive consequence is of course a more flexible bandwidth offering to the customer.

EoSDH MPLS — a Summary of the Benefits

To sum up, the additional advantages in EoSDH MPLS transport compared to EoSDH mapping are:
• Creates ability for statistical multiplexing, thereby utilising capacity more effectively given the bursty nature of data traffic.
• Provides QoS and differentiated service classes.
• Provides controlled over-subscription via QoS, as opposed to EoSDH mapping where there is no over-subscription.
• Ensure complete customer privacy, even when customers are sharing the same VCG’s the MPLS encapsulation ensures complete privacy and at the same time support for differentiated services and QoS. It is in this aspect the EoSDH MPLS solution is so unique.
The EoSDH MPLS transport explained in the previous section has one drawback that, for some customers, could be better addressed which is that it is still a point-to-point solution. The consequence of this point to point solution can be:

- No “real” data network, there is no switching or redirection of traffic, so this redirection has to be done by other equipment. For a customer with a headquarter and a number of branch sites where the communication also goes from branch site to branch site, a redirection in the network would in many cases be beneficial for the customer.

- This earlier redirection would also be beneficial for the operator, as traffic would not have to travel back and forth.

- Because it is point-to-point connections, the headquarter will receive multiple connections from the remote sites, and so will also need multiple service interfaces.

The solution to this scenario is EoSDH MAC switching.

MAC Switching Theory

What needs to be emphasized, is that up until now, the EoSDH system only had knowledge of Ethernet at OSI Layer 1 i.e. the 0s and 1s in the data stream were either mapped into VCG or encapsulated into MPLS.
With EoSDH MAC switching the equipment becomes Ethernet OSI Layer 2 aware i.e. it carry out switching of Ethernet traffic based upon Ethernet addresses.

The following is a very short summary of Ethernet as a technology.

All Ethernet equipment has an address called the MAC address (Media Access Control). This address is unique on a worldwide basis and is typically hard burned on the Ethernet adapter by the adapter manufacture.

An Ethernet frame is built up as follows:
- A destination MAC address — that is, the address of the receiver, called DA.
- A Source MAC address — that is, the address of the transmitter, called SA.
- The actual data — could be IP, LLC, IPX etc.
- FCS (Frame Check Sequence) — used by the receiver to verify the integrity of the Ethernet packet.

The MAC switch is a device that understands the Ethernet frame structure and MAC addresses.

So when a MAC switch receives an Ethernet frame on one of its ports it will run through the following sequence:
• The switch has a table called a MAC table that correlates a MAC address to a physical port on the switch.
• The table is a learning table i.e. whenever a station transmits a packet, the packet enters the MAC switch, and so the switch sees which ports particular source MAC addresses enter on and updates its table accordingly.
• When the switch receives an Ethernet frame (notice we are now talking Ethernet frames, not bits), it make an FCS check. If the packet is corrupted, it will be dropped.
• If the packet is OK the switch checks the DA in the learning table.

• If the switch knows which port to forward the packet to it will forward the packet.
• If the switch doesn’t know where to forward the packet it broadcasts the packet on all its ports.

**EoSDH MAC Switching**

When it comes to EoSDH MAC switching theory, it is very similar to the above theory with some small exceptions:

• The MAC switch is now installed in an SDH node.
• The MAC switch can receive Ethernet packets on a port, which can be either a local Ethernet interface, a VCG or

![Figure 15 — EoSDH MAC Switching](image-url)

- = Ethernet Customer A
- = Ethernet Customer B
- = Ethernet Customer B in MPLS
- = Ethernet Customer C
- = Ethernet Customer C in MPLS
a MPLS LSP, i.e. not just on an Ethernet interface.

- The MAC switch will depending upon the destination MAC address, forward the Ethernet packet to another port, which can be a VCG, an Ethernet interface or an MPLS LSP.

EoSDH MAC switching enables for point-to-multipoint solutions, meaning the number of interfaces at a central customer site can be reduced from n (the number of branches) to one single interface.

MAC switching on traffic received in VCGs does not support QoS or differentiated service classes. If differentiated services are needed, MPLS LSPs must be used to transport the traffic to the MAC switch.

- A customer with two branch offices and one headquarters connected via Ethernet to the SDH network.
- An Ethernet MAC switch is configured in the SDH network.
- At the MAC switch the customer’s connections are terminated.
- Two of the connections is a VCG.
- The other are a MPLS LSP (this is just to emphasize that this can be mixed).
- The MAC switch performs MAC switching of the Ethernet frames received on the three connections, thereby creating the capability to provide a Layer 2 VPN grooming service.

Figure 16 — EoSDH MAC Switching Theory
Please notice that the switching functionality can be placed in any EoSDH enabled SDH switch, this is purely dependent on the operators design. However, the earlier the switching is done, the earlier packet multiplexing and grooming benefits are realised, which in turn leads to better network utilisation.

From figure 16 it appears that every customer must have their own physical MAC switch installed in the SDH node. This is not very scalable nor economical. However allowing several customers to share the same MAC switch is not satisfactory either, since it leads to one broadcast domain and no security. Tellabs solution to this problem is Virtual MAC switching where:

- The MAC switch is logically partitioned into a number of virtual switches, one for every customer that needs a MAC switch at the specific SDH node.
- Each virtual MAC switch is assigned its own ports, either VCGs or MPLS LSPs and/or Ethernet ports.

Consider an example with two customers; Customer A and Customer B, each with several branch offices and a headquarter:

- All sites are connected via Ethernet to the SDH network.
- An Ethernet MAC switch is installed in a SDH node.

**Figure 17 — EoSDH Virtual MAC Switching**
The MAC switch is partitioned into two virtual MAC switches: Customer A’s virtual MAC switch and Customer B’s virtual MAC switch.

Customer A’s VCGs (or LSPs) are terminated in Customer A’s virtual MAC switch.

Customer B’s VCGs (or LSPs) are terminated in Customer B’s virtual MAC switch.

The benefits of this solution are:

• One MAC switch can support multiple customers, due to this logical partitioning.

• In the Tellabs solution each physical MAC switch can be divided into 1024 virtual MAC switches.

• Customer traffic is completely separated, running in different VCGs, LSPs or Ethernets and with different MAC switches, there is no possibility of mixing packet between different customers’ and hence no security risk.

EoSDH MAC Switching — a Summary of the Benefits

The additional advantages in EoSDH MAC switching compared to EoSDH mapping are:

• True Layer 2 VPN services — one single interface at for instance customer headquarter, as opposed to the point-to-point solution with EoSDH mapping or EoSDH MPLS switching solutions.

• Better utilisation of network resources due to earlier traffic redirection and grooming.
• Virtual MAC switching offers a flexible and economic MAC switching solution, whilst retaining full security.

**EoSDH 802.1q Tagging**

Even with a combined MAC switching and MPLS solution, there is still a limitation with separation of traffic beyond separation by physical interface i.e. the lack of ability to create several service flows at the same physical Ethernet interface.

The consequence of this can be explained via the following example. Consider a customer with several sites to be interconnected with the following service requirements:

- “Gold” service for mission critical traffic.
- “Silver” service for normal traffic.
- “Bronze” service for Internet access.

In the technologies explored so far, the MPLS label assignment for an operator using an EoSDH MPLS switched SDH network is done with reference to the physical interface on the MPLS enabled SDH node. This means three physical interfaces are required at the customer sites and at any routers within the network, such as a PE router. Multiple interfaces rapidly increase costs as it means not just more interfaces but more rack space — more footprint, more power etc.

The way to solve this problem is EoS-802.1q tagging.

**IEEE 802.1q Theory**

IEEE 802.1q was originally born out of the Virtual LAN (VLAN) concept. The idea is to separate the switch into a number of completely separated LANs (or broadcast domains). For example:

- One LAN for the sales department.
- One LAN for production.
- One LAN for logistic.
- Etc.

There are many reasons, including:

- Security, as the different LANs are in different broadcast domains i.e. a router or Firewall is needed in order to assure communication.
- It has always been good design to make a hierarchical design as it scales
better, is easier to troubleshoot and maintain etc.

Typically the different VLANs are assigned with reference to the Ethernet interfaces on the switch, for instance:

- Port numbers 1, 5, 34, 56 and 88 belong to the Sales VLAN — all stations on these ports can forward Ethernet frames to one another.
- Port numbers 2, 15, 23, 33, 44 and 89 belong to the Production VLAN — meaning all stations on these ports can forward Ethernet frames to one another.
- Even though the stations are connected to the same switch, stations on the Sales VLAN cannot send Ethernet frames to (and have no knowledge of) the Production VLANs.

With this approach the VLANs are configured on the switch. However what if there are several switches? How can a switch identify a VLAN on a different switch? One way would be to interconnect every VLAN via separate cabling between the switches. As an example let’s consider the scenario from before:

- Switch two is configured with port number 2, 6, 8, 34, 56 and 64 as the Sales VLAN.
- Switch two is configured with port number 3, 7, 19, 45 and 63 as the Production VLAN.

To sum up: the two departments have their own Virtual LAN.
To connect the two VLANs the two switches are interconnected as follows:

- Port 88 on switch one is connected to port number 64 on switch two.
- Port 89 on switch one is connected to port 63 on switch two.

(Note the connection can be made via Fibre, PDS cabling or even a VCG).

Notice from figure 20 how:

- All users connected on ports on the Sales VLAN on the two switches can communicate.
- But the Sales VLAN and the Production VLAN cannot communicate.

However notice how the cabling increases as the number of VLANs increase. A better approach is to add some kind of identification to the frames running on the trunks between the switches, as illustrated in figure 21. This identifier would enable the switches to see which VLAN the frames belonged to and thus enable...
them to forward the frames to the correct VLAN. In this way the number of trunks between switches could be reduced to one single trunk between the switches. This is exactly what IEEE 802.1q tagging does. IEEE 802.1q is a 4-byte extension to the IEEE 802.3 header and resides after the DMAC and SMAC fields. The 4 bytes are divided into four fields:

- 2 bytes are used to identify that the following 2 bytes are 802.1q information and not IEEE 802.3 info.
- 3 bits are used for priority. These are known as the provider bits.
- 1 bit is CFI bit — Canonical Format Identifier and is not to be explained here
- 12 Bits form the VLAN ID number. This is the VLAN identification that the switch will use to define to what VLAN a frame belongs to.

**EoSDH 802.1q Tagging**

EoSDH 802.1q tagging is off-course very closely related to the IEEE 802.1q specification.

The customer can choose to classify the traffic either:

- Via different VLAN identifiers.
- Or via different priorities signaled in the priority field.

The EoSDH network will then map the 802.1q classified frames into the EoSDH network.

The mapping can be either into a MPLS enabled EoSDH network or could be into a EoSDH mapper network.

In the first case (MPLS network) the quality is signaled via VLAN tags or priority field is then mapped into LSP.
with the agreed QoS class. An example could be:

- Best-effort service is signaled via priority field set to 3.
- Burst service is signaled via priority field set to 2.
- Leased line service is signaled via priority field set to 1.

In the latter case, the 802.1q signaling can be used to specify the VCG to be used.

Another example could be multiple customers connected to an IP access router (or MPLS PE). Instead of each customer needing their own Ethernet interface, the customers can share the same interface and be differentiated by the 802.1q tag.

Conclusion — Highly Efficient Ethernet Service Delivery

This paper has described four different technologies for implementing highly efficient Ethernet service delivery via Ethernet-over-SDH as a transport mechanism.

These four technologies combined in an EoSDH implementation will give a network operator the following benefits:

- One single low-cost interface type i.e. Ethernet, as opposed to the traditional PDH/SDH E-1, E-3, and STM-1 etc.
- Flexible granularity in bandwidth so that the customer can order and receive bandwidth down to a granularity of 100 kbit/s, as opposed to the traditional steps in E-1, E-3, and STM-1 etc.
- Bandwidth which can be upgraded or downgraded from the network management System without the need for field engineer visits.
- Ethernet packet multiplexing in the SDH access, which allows for over-subscription in the SDH access layer instead of back-hauling to an IP DAS and the associated back-haul costs.
- Differentiated services and QoS in SDH, so that in contrast to traditional leased line service, burst and/or best-effort” services can be offered.
- One single interface to the operator’s data access equipment (traditional DAS or IP MPLS PE’s) as opposed to the many expensive traditional E-1, E-3, STM-1, reducing equipment cost, rent of footprint, recabling etc.
However what needs to be noticed is that it is not a question of choosing one of these technologies, on the contrary, the technologies can be combined in almost any way and in this respect fulfill multiple different applications. If the reader would like more information regarding applications, please refer to the Tellabs EoSDH application notes, where you will find inspiration and guidelines.
How to reach us:

North America
Tellabs
One Tellabs Center
1415 West Diehl Road
Naperville, IL 60563
U.S.A.
+1.630.378.8800
Fax: +1.630.798.2000

Asia Pacific
Tellabs
9 Temasek Boulevard
#43-02 Suntec Tower Two
Singapore 038989
Republic of Singapore
+65.6336.7611
Fax: +65.6336.7622

Europe, Middle East & Africa
Tellabs
Abbey Place
24-28 Easton Street
High Wycombe, Bucks
United Kingdom
HP11 1NT
+44.870.238.4700
Fax: +44.870.238.4851

Latin America & Caribbean
Tellabs
13800 North West 14th Street
Sunrise, FL 33323
U.S.A.
+1.954.839.2800
Fax: +1.954.839.2828

Glossary
ADM Add/Drop Multiplexer
ATM Asynchronous Transfer Mode
BAS Broadband Access Server
BGP Border Gateway Protocol
CapEx Capital Expenses
CPE Customer Premises Equipment
DAS Direct Access Server
DSL Digital Subscriber Line
DSLAM DSL Access Multiplexer
EOSDH Ethernet-over-SDH
EPN Ethernet Private Network
FCS Frame Check Sequence
GFP Generic Frame Procedure
G.SHDSL Single pair High bit rate Digital Subscriber Line
HDSL High-Data-Rate Digital Subscriber Line
IEEE Institute of Electrical and
Electronics Engineers
IP Internet Protocol
LAN Local Area Network
LAP Link Access Procedure
LCAS Link Capacity Adjustment Scheme
LSP Label Switched Path
MAC Media Access Control
MPLS Multiprotocol Label Switching
NMS Network Management System
OpEx Operational Expenses
OSPF Open Shortest Path First
PDH Plesio synchronous Data Hierarchy
PE Provider Edge
PoP Point-of-Presence
PoS Packet-over Sonet
QoS Quality-of-Service
RIP Routing Information Protocol
SDH Synchronous Data Hierarchy
SDSL Synchronous Digital Subscriber Line
SLA Service Level Agreement
TDM Time Division Multiplexing
TM Terminal Multiplexer
VC Virtual Circuit
VCG Virtual Concatenated Group
VDSL Very high data rate Digital Subscriber Line
VLAN Virtual Local Area Network
VPN Virtual Private Network

The following trademarks and service marks are owned by Tellabs Operations, Inc., or its affiliates in the United States and/or other countries: TELLABS®, TELLABS and T symbol®, and T symbol®.

Any other company or product names may be trademarks of their respective companies.

© 2003 Tellabs. All rights reserved.
74.1391E Rev. A 9/03