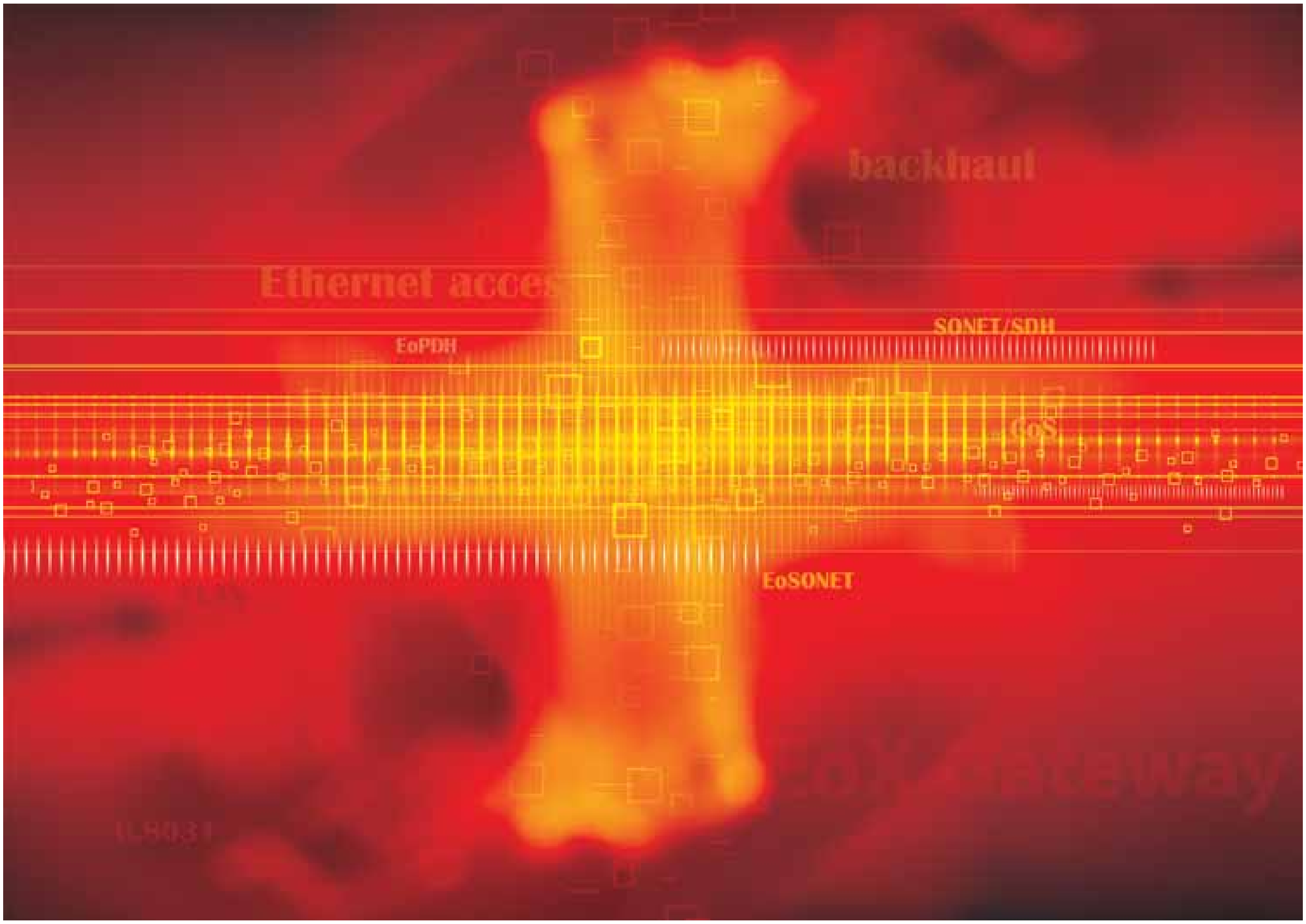
FUJITSU

Unlocking Ethernet Access and Backhaul with the EoX Gateway



Ethernet has become the most popular interface to attach end users and access devices to the range of Ethernet and IP network services. This simple, low-cost, familiar technology is easy for end users to own and operate. A single Ethernet jack can support multiple connections and a wide range of access bandwidths, thus enabling end users to grow connectivity and bandwidth easily as needed. Ethernet services are often priced more inexpensively per unit bandwidth than legacy TDM-based services. With the emergence of COE, Ethernet now promises the same reliability, performance, and security of SONET/SDH, but with the low network cost and bandwidth flexibility inherent to Ethernet.

Connection-Oriented Ethernet (COE) using Ethernet Tag Switching brings advanced traffic engineering capabilities to Carrier Ethernet. Connection-Oriented Ethernet accomplishes for Ethernet what SONET technology accomplished for DS1s and DS3s by enabling network providers—for the first time—to deploy a single, long-lasting Ethernet infrastructure for all Ethernet private line and access/backhaul applications. By invoking per-flow traffic engineering, resource reservation and connection admission control along with the latest Ethernet OAM and protection standards, COE delivers the performance, reliability and security of SONET/SDH networking, while retaining the networking efficiency of native Ethernet networking. To read more about COE, please see the Fujitsu white papers, "Connection-Oriented Ethernet – Completing the Ethernet Revolution", and "Connection-Oriented Ethernet – Operational and Deployment Considerations"

The Challenges

Providers face complex economic and networking challenges as they work to offer Ethernet-attached services to their customers. These challenges are inherent to access and backhaul networks, and they restrict the scale, cost-effectiveness and velocity at which Ethernet-attached services can be deployed.

Diverse Access Networks

For access and backhaul networks, the technology choice is often driven by the cost of the specific deployment, which can drive network providers to rely on a complex mix of technologies such as optical Ethernet, EoS, EoPDH, or Ethernet over OTN. This access environment may be owned or leased by the provider. Each of these networks may employ different transport layer functions, including encapsulations, OAM methods, and protection protocols.

Complex Service and Transit Network Handoffs

The overall solution for delivering Ethernet-attached services often involves multiple networks owned by one or more providers. The access and backhaul provider is then responsible for terminating the various access networks and delivering a standard handoff to a network or transit network, each of which may use a different technology, have its own set of handoff requirements and may be operated by a different business entity.

The combined challenges of diverse access networks and complex service and transport handoffs, together with the presence of multiple business entities, creates an expensive and complex networking problem at hub offices where these environments collide. This problem is typically addressed in a brute-force manner by deploying multiple types of elements including MSPPs, EoPDH termination boxes, Ethernet switches and DCS platforms that perform the various required Layer 1 and Ethernet layer termination and encapsulation functions. This approach results in much additional cost.

FUJITSU

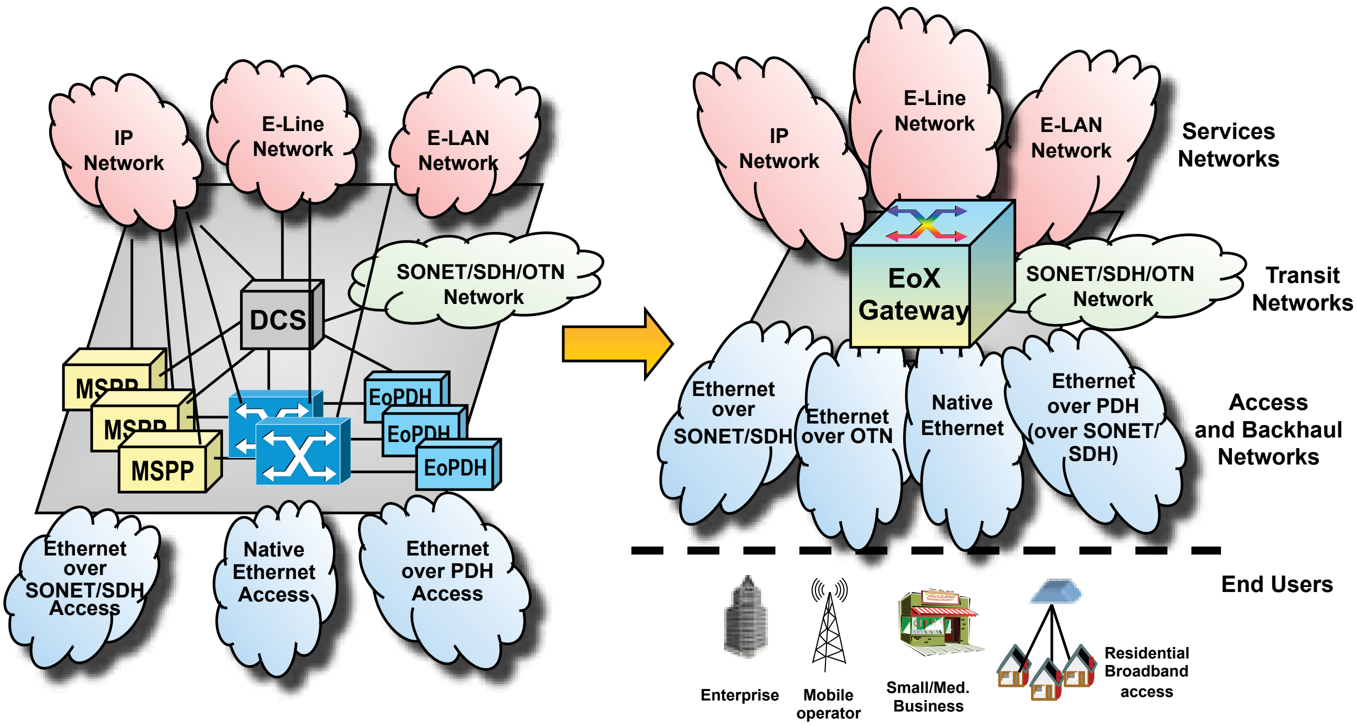
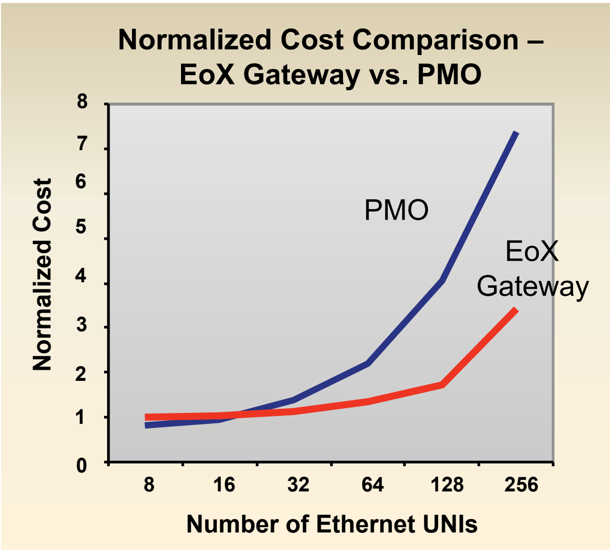


Figure 1: EoX Gateway Simplifies Hub Offices by Interconnecting Access and Backhaul Networks to Service and Transit Networks

As shown in Figure 1, the EoX Gateway eliminates multiple elements by terminating the diversity of access networks and presenting a flexible variety of handoffs to the full range of service and transit networks. By converging multiple access networks, EoPDH, EoSONET, and native Ethernet onto a single EoX Gateway element, substantial network cost savings and network element reduction can be achieved, as shown in Figure 2.



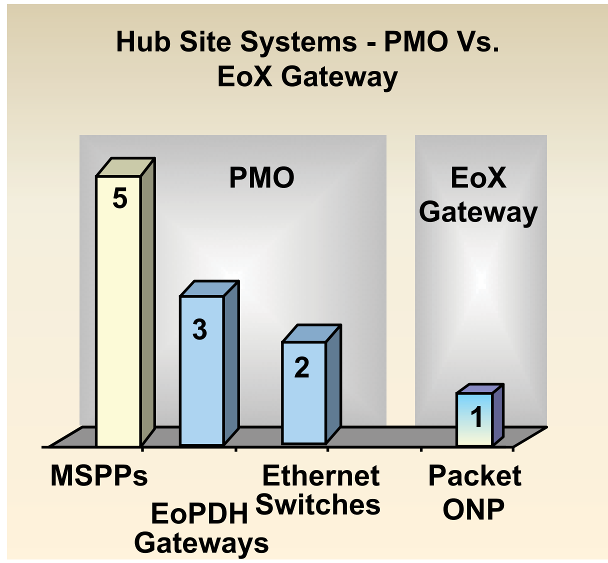


Figure 2: Example Cost savings and Element Reduction of EoX Gateway Versus Present Mode of Operation (PMO)

The EoX Gateway serves many important applications, including wholesale Ethernet access service, retail Ethernet and IP services access, mobile backhaul, and DSLAM backhaul. This paper describes the EoX Gateway functions that leverage the integration of Layer 1 networking and COE that define Packet ONPs, facilitating cost-effective and scalable access and backhaul of Ethernet-attached services.

Packet Optical Networking Platforms (Packet ONPs) integrate traditional layer 1 optical networking such as SONET/SDH and photonic networking with Connection-Oriented Ethernet. An "open platform" Packet ONP implementation enables network providers to create a universal aggregation, transport, and private line services infrastructure that equally serves Ethernet and traditional TDM networking needs. To read more about Packet Optical Networking, please see the Fujitsu white paper, "Packet Optical Networking Platforms - Delivering the Connected Experience"

The EoX Gateway

A Packet ONP configured as an EoX Gateway sits among the access, transit, and service networks. The EoX Gateway provides a range of both optical transport layer and Ethernet service layer functions, as shown in Figure 3.

The transport functions encompass more than just physical layer termination. They can include complete transport network termination: physical layer termination, protection switching and protocol termination, Ethernet encapsulation, and OAM. Since these transport functions are isolated on each side of the Gateway, the EoX Gateway will often provide many instances of transport network termination for many different technologies.

The Ethernet service functions flow across both sides of the Gateway and are the same regardless of the underlying transport network. The EoX Gateway is responsible to assure the integrity of the Ethernet service, especially CoS marking, QoS management, and OAM, across disparate transport networks and business entities.

Figure 3 depicts the network-to-network interface (NNI)—the demarcation and handoff point between commercial entities on the "service/transit network" side of the EoX Gateway. In this case, the access provider is responsible for access network termination and creating the acceptable handoff to the service network.

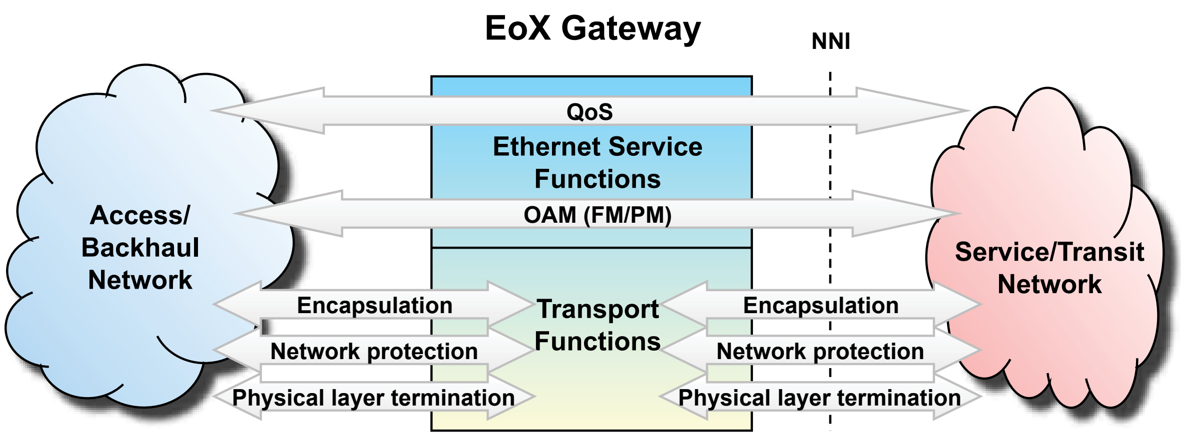


Figure 3: EoX Gateway

EoX Gateway Transport Functions

The EoX gateway is responsible for terminating a wide variety of transport network technologies, including Ethernet over SONET/SDH, Ethernet over PDH over SONET/SDH, and native Ethernet.

For Ethernet-attached services, both non-routed optical Ethernet and SONET/SDH access technologies will remain in use for the next several years for simple economic reasons. Tens of thousands of SONET/SDH systems are deployed at customer premises locations and are being leveraged for transporting Ethernet. This is because the cost of deploying an Ethernet port on those systems is far less than capitalizing and managing an additional access element and an additional fiber pair.

SONET/SDH systems remain in use for Ethernet access where the end-user attaches to the access network with an Ethernet over PDH system to the fiber access point and a SONET/SDH network transports the PDH circuits to the service edge. This results in the requirement for a multilayer Ethernet over PDH over SONET/SDH network termination at the EoX Gateway.

Increasingly, native Ethernet access networks are being deployed with different physical layers, protection schemes, and tagging options.

The EoX Gateway is deployed at homing points for the access and backhaul networks, where it provides the termination of the physical layer, its associated framing and physical layer OAM. The EoX Gateway also performs the more complex functions of:

- Operating the protection switching protocol toward the access network
- De-encapsulating Ethernet traffic from its physical layer transport

TDM Protection

For access networks that use Ethernet over SONET/SDH and Ethernet over PDH (over SONET/SDH), the protection protocol exists at the SONET/SDH layer and is well understood. In the typical homed backhaul ring environments, UPSR/SNCP higher order and lower order protection is the prevalent architecture, along with some deployment of 1+1 line layer/multiplex section layer protection for point-to-point access.

Ethernet Protection

Several existing or emerging Ethernet protection technologies are better suited to access networks than legacy IEEE 802.1 spanning tree-based approaches. These technologies include ITU-T G.8031 Ethernet Linear Protection Switching, and IEEE 802.1AX link aggregation protocols.

While link aggregation is standardized over point-to-point configurations only, G.8031 protection achieves 50 ms protection switching speed over any physical topology, including the homed-ring topologies that are prevalent in access environments. G.8031 provides a dedicated protection path with identical resources to the working path. In the event of node, link, or connection failures, a simple APS protocol provides 50 ms switching to the protection resources, as illustrated in Figure 4.

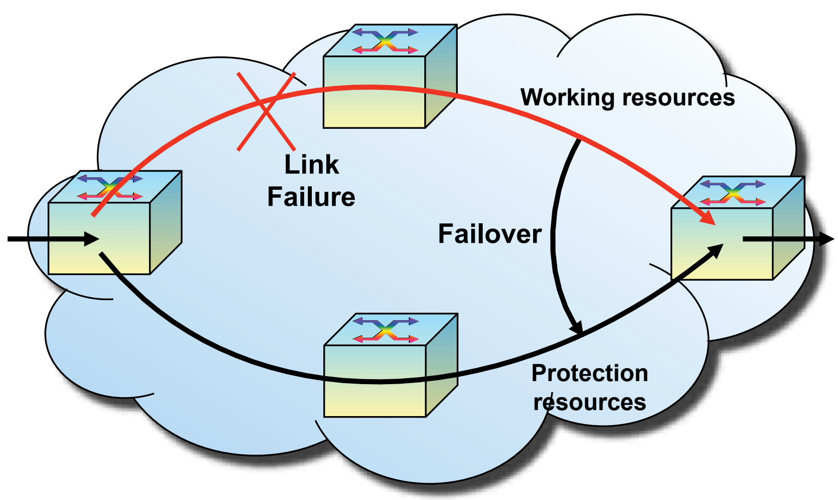


Figure 4: G.8031 End-to-End Protection Illustration

G.8031 offers several advantages. It provides both end-to-end and segment protection (Figure 5), so that the backhaul network can be protected independently from an attached service or transit network. It also protects multiple connection tunnels simultaneously and provides protection regardless of how the Ethernet frames are tagged.

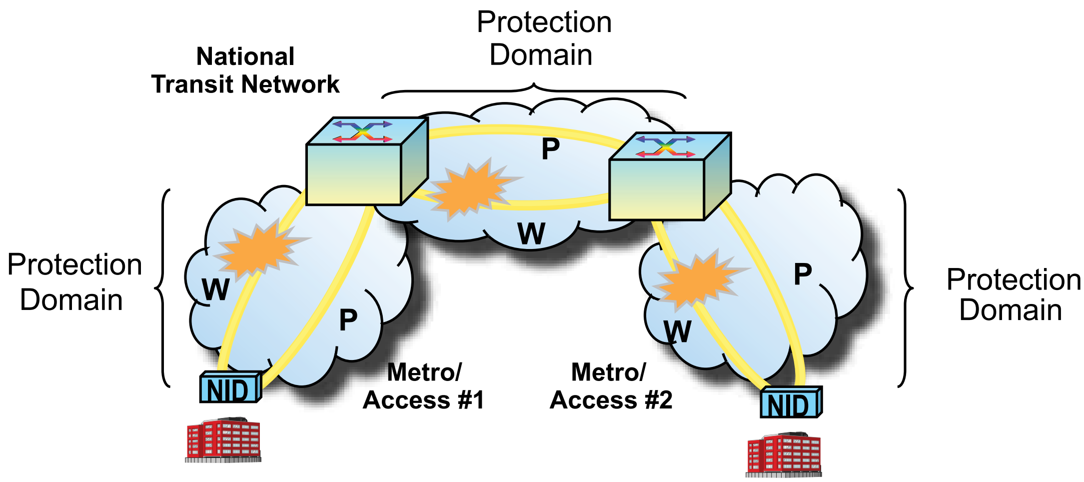


Figure 5: G.8031 Segment Protection Guards Against Multiple Failures

Ethernet over TDM Encapsulations

A variety of Ethernet over PDH and SONET/SDH encapsulations have been employed in conjunction with various virtual concatenation approaches that enable access providers to offer a range of bandwidth over a variety of available physical networks. While the technology for encapsulating Ethernet over a variety of TDM networks is well understood, the sheer breadth of encapsulations in the field represents a significant networking challenge.

Common optical access encapsulation options include:

- Ethernet over X.86 over DS3/E3 over SONET/SDH
- Ethernet over X.86 over STS-1/VC-4
- Ethernet over X.86 over DS1/E1 VCAT group over SONET/SDH
- Ethernet over X.86 over VT1.5/TU11
- Ethernet over GFP over STS/VC-4 VCAT group
- Ethernet over GFP over VT1.5/TU11 VCAT group
- Ethernet over GFP over STS/VC-4 VCAT group
- Ethernet over GFP over DS1/E1 VCAT group over SONET/SDH
- Ethernet over GFP over DS3/E3 VCAT group over SONET/SDH

Ethernet Encapsulation and Tagging Considerations

In addition to the physical layer encapsulation issues that exist with TDM-based access, the EoX Gateway must enable a variety of Ethernet tag encapsulation permutations. These Ethernet tagging considerations apply when Ethernet traffic is being transported not only over an optical Ethernet network, but also over a SONET/SDH or backhaul network to the EoX Gateway. There are several examples of interest as shown in Figure 6.

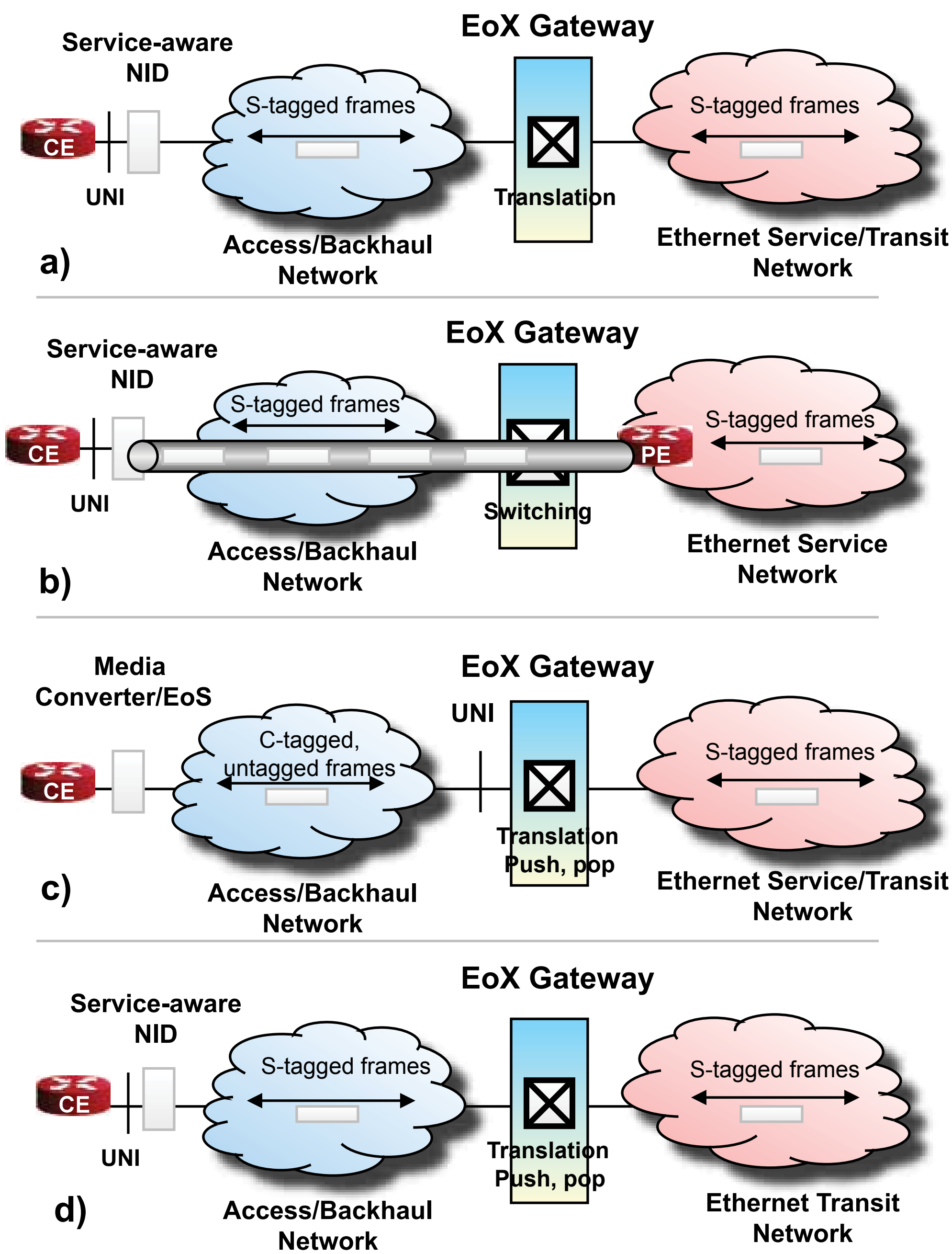


Figure 6: Ethernet VLAN Tagging/Encapsulation Permutations

In many cases (Figure 6a), the Ethernet UNI does not exist on the EoX Gateway, but is provided by a remote service-aware Ethernet NID, close to the end-user location. This remote NID will be responsible for encapsulating the customer Ethernet frames into a service-provider tagged (S-tagged) Ethernet frame. In these cases, the EoX Gateway recognizes and forwards S-tagged frames, potentially performing an S-tag translation depending upon the destination network requirements.

One important variation (Figure 6b) is where different business entities operate the access network and the Ethernet service network. In this case, the optical access network provides a UTAS between a NID that implements a remote UNI (RUNI) function and the edge device in the Ethernet service network, connected to EoX Gateway that implements a virtual UNI (VUNI) function. The NID encapsulates each of the end user's individual EVCs into a single S-VLAN tag by performing all-to-one bundling, before it forwards those EVCs towards the EoX Gateway. This S-VLAN tag is preserved as it passes through the EoX Gateway and is terminated (popped) on the edge device in the Ethernet service network that implements the VUNI.

Similarly, the edge device encapsulates one of the customer's EVCs into a single S-VLAN tag, before it forwards those EVCs towards the EoX Gateway. The S-VLAN tag is preserved as it passes through the EoX Gateway and is terminated (popped) on the NID. This, in essence, creates a bidirectional "tunnel" between the NID and the edge device in the Ethernet service network. One such tunnel exists for each NID in the optical access network. The EoX Gateway is not service-aware, and is only aware of the S-tagged tunnel. The remaining network elements in the optical access network may also not be service-aware. The benefit of this application is that the Ethernet service provider can create multiple EVCs without repeated interactions with the access provider.

In other cases (Figure 6c), the remote NID device or Ethernet over SONET/SDH access device is not service aware and only provides simple media conversion or Layer 1 encapsulation. In these cases, the EoX Gateway function may be called upon not only to translate S-tag values, but also to push/pop S-tags onto Ethernet frames into and out of the optical access network.

Another permutation (Figure 6d) exists when the EoX Gateway sits at the boundary between an optical access network and a transit network. In this case, the EoX Gateway will often receive an S-tagged Ethernet connection from the access network, but because the transit network forwards traffic based on a second layer of S-tag, the EoX Gateway is required to push a second S-tag in the access to transit direction and pop that second tag in the reverse direction. Optionally, inner or outer S-tag translation may be required.

EoX Gateway Ethernet Service Functions

The EoX Gateway must provide Ethernet service layer functions of CoS marking, QoS management, and Ethernet service OAM. The exact Ethernet service layer functions required vary according to the type of service, access or transit network that is involved and whether or not that network is Ethernet service-aware.

Common combinations of services and network types include:

- E-Line services delivered over either service-aware or service-unaware Ethernet over SONET/SDH or Ethernet over OTN networks
- E-Line services delivered over service-aware native Ethernet or MPLS networks
- E-LAN Ethernet services delivered using IEEE 802.1ah or 802.1ad bridged networks.
- E-LAN Ethernet services delivered using IETF VPLS
- IP services such as internet services or "IP VPN" services delivered over IP/MPLS networks

The MEF ENNI specification is currently scoped to describe the attributes at the physical and Ethernet service layers at an NNI that uses an Ethernet physical layer to connect two Ethernet-aware networks that are providing actual Ethernet services (as opposed to IP services).

Handoffs of Ethernet connections over general NNI interfaces (beyond the scope of the current MEF ENNI specification) are deployed and of interest for EoX Gateway applications. Examples of such handoffs include cases where non-Ethernet physical layers are used and cases where Ethernet connections are handed off to IP services networks or to transit networks that are not Ethernet service-unaware.

CoS Marking

Since the Ethernet service layer is exposed at the EoX Gateway, the Gateway is responsible, as necessary, for properly mapping and interworking CoS marking across the relevant network boundaries. Consider a case where an access network provider may use four classes of service, while the Ethernet service network provider may use only three. The providers must agree how to map one class into another. Accordingly, the PCP marking in the Ethernet service frames may have to be modified or translated by the EoX Gateway.

Figure 7 illustrates the EoX Gateway performing PCP modification in case of a) an ENNI interface, and b) a non-Ethernet NNI interface. For the ENNI interface, as shown in Figure 7a, the EoX Gateway is responsible for PCP translation upon egress from one network to another. Therefore, EoX Gateways on either side of the ENNI perform PCP translation.

In more complicated cases as shown in Figure 6b, a single EoX Gateway on one side of the NNI may have to provide PCP translation in both directions of an EVC. There may be, for example, a non-Ethernet-aware transit network in between an Ethernet-aware access network and an Ethernet-aware service network. It may be of value for an EoX Gateway at one side of the NNI to perform PCP translation in both directions of the EVC. In this way, the access network operator can ensure correct PCP marking in cases that are not currently covered by industry specifications.

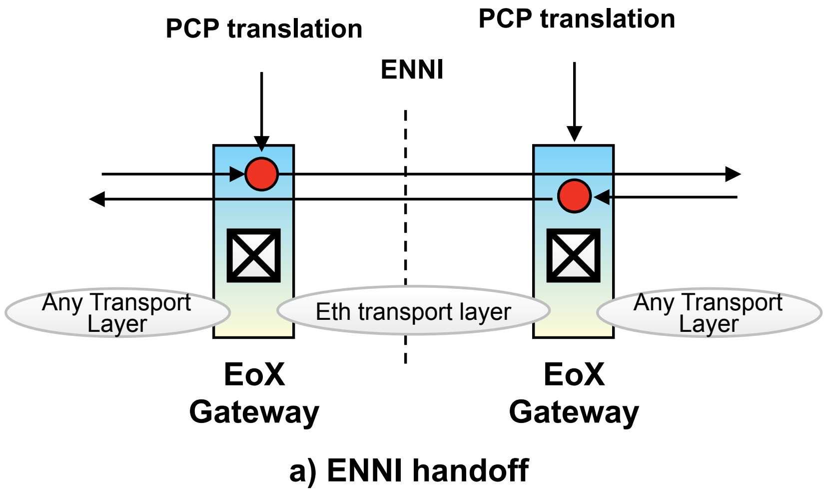


Figure 7: PCP Translation in the EoX Gateway

The MEF 23 specification also describes requirements for maintaining the appropriate color marking for Ethernet service frames that transit an ENNI. Specifically, the ENNI must be color-aware if any of the UNIs in the service are color-aware and the ENNI must be able to appropriately handle inconsistencies between color-aware and color-blind networks. For example, "yellow" frames cannot be inadvertently promoted to "green" frames across the ENNI. One implication of this is when "yellow" frames are exiting a color-aware network to a color-blind network, an EoX Gateway at the color-aware network egress would be required to discard yellow frames rather than passing them to the color-blind network as-is or re-marking the frames as green.

QoS Management

There are several policing and shaping traffic management functions that are invoked for QoS management at the EoX Gateway, depending upon the types of networks that are being joined together.

Policing is invoked at the ingress to a network at a UNI or NNI. Upon egress to another network, policing is invoked at an NNI. Shaping functions are used on egress from a node to ensure QoS as traffic flows into networks that are either not service-aware or for performance reasons do not invoke ingress policing.

The MEF 10.1 and ENNI specifications indicate two-rate, three-color policing algorithms to enforce the bandwidth profile attributes of Ethernet connections. These algorithms can be invoked at the port level, EVC level, or CoS instance level (within an EVC), according to the manner in which the bandwidth profile is specified. Similarly, hierarchical egress traffic shaping at the port, EVC, and CoS instance ensures that the latency-sensitive, strictly priority-queued frames are not overscheduled and therefore neither exceed their bandwidth allocation on egress nor starve out lower priority frames.

Several possible scenarios are available for the EoX Gateway to invoke these functions, depending upon whether or not the attached networks are Ethernet service-aware and whether the EoX Gateway is deployed at the boundary between network operators or at a transport network boundary within a single-operator domain.

The simplest case is where an EoX Gateway is deployed at a boundary between two different Ethernet-aware networks in the same provider domain. In this case, ingress policing functions are performed at the UNIs on ingress to each network and the EoX Gateway merely shapes traffic as it passes from one domain to the other.

In many cases, though, the optical access network is SONET/SDH (or PDH over SONET/SDH) and may not be Ethernet service-aware. In these cases, the EoX Gateway is responsible for performing policing on behalf of the non-service-aware network as well as shaping between networks, as shown in Figure 8. An extension of this application is where both networks are not service-aware (for example, one network is SONET/SDH access and the other is an OTN transit network) and the EoX Gateway performs both ingress policing and egress shaping in both directions for all EVCs.

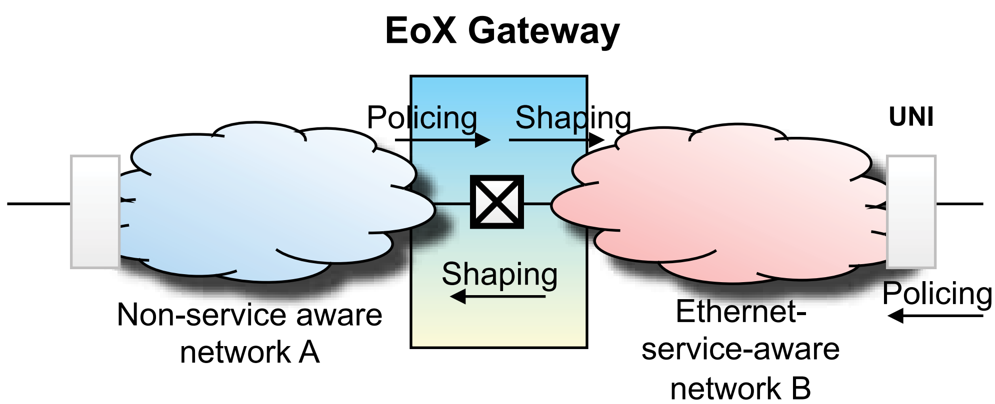


Figure 8: Ingress Policing on Behalf of Non Service-Aware Access Networks

Of further interest are cases covered by the current work of the MEF ENNI specification, as shown in Figure 8. In these cases, the EoX Gateway sits at a boundary between two Ethernet service-aware networks. It is required to invoke both ingress and egress policing functions at the boundary, to enforce the ingress and egress bandwidth profile attributes required by the specification. Although not explicitly required by the specification, shaping in the Gateway is also of value for this application.

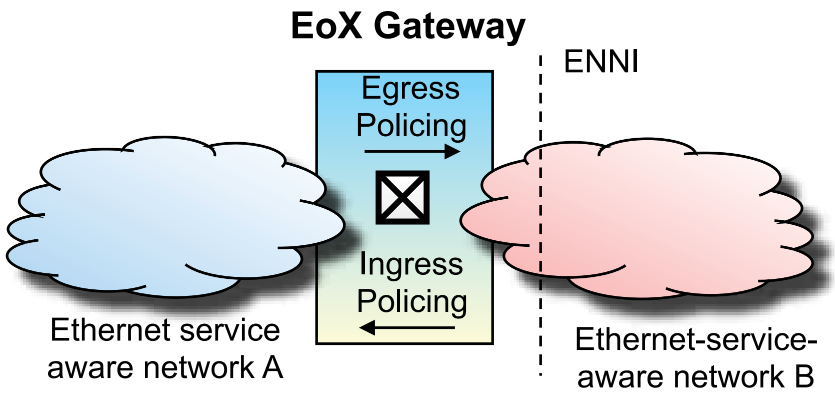


Figure 9: Ingress and Egress Policing at the ENNI

Finally, there are many cases where an optical access network provides Ethernet access for IP VPN services. If the optical access network and the IP service network are operated by the same provider, the service provider can achieve substantial improvement in IP router packet throughput performance. This improvement results from providing egress shaping in the EoX Gateway and not invoking ingress policing in the provider edge router, as shown in Figure 10.

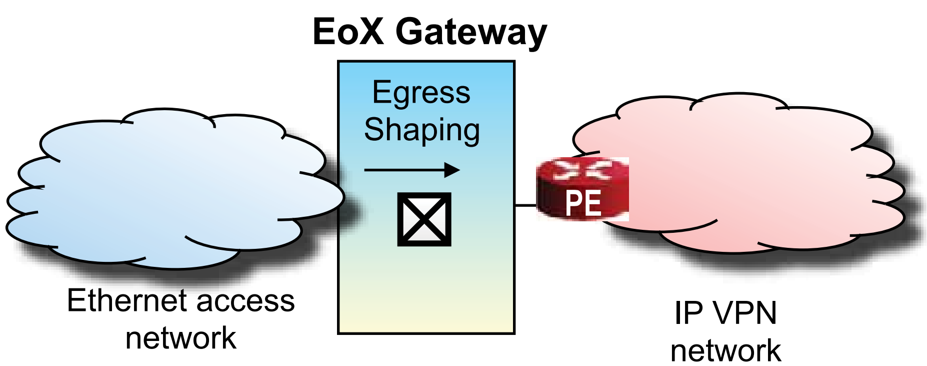


Figure 10: Egress Shaping at the EoX Gateway Improves PE Router Performance for IP Services

Ethernet OAM

In many cases, the interconnection of optical access networks with transit or services networks may occur across business entities. In these cases, the EoX Gateway employs service OAM functionality at the Ethernet service layer to meet the required demarcation functionality.

There are two key OAM standards for Ethernet fault and performance management: ITU-T Y.1731 and IEEE 802.1ag. In addition, MEF ENNI specification describes how to apply these standards in various network scenarios that involve Ethernet-aware networks that deliver Ethernet services.

Y.1731 has defined multiple OAM layers, as well as endpoint and intermediate-point functions known as MEP and MIP functions respectively. An example service OAM architecture applied to an MEF ENNI is shown in Figure 11.

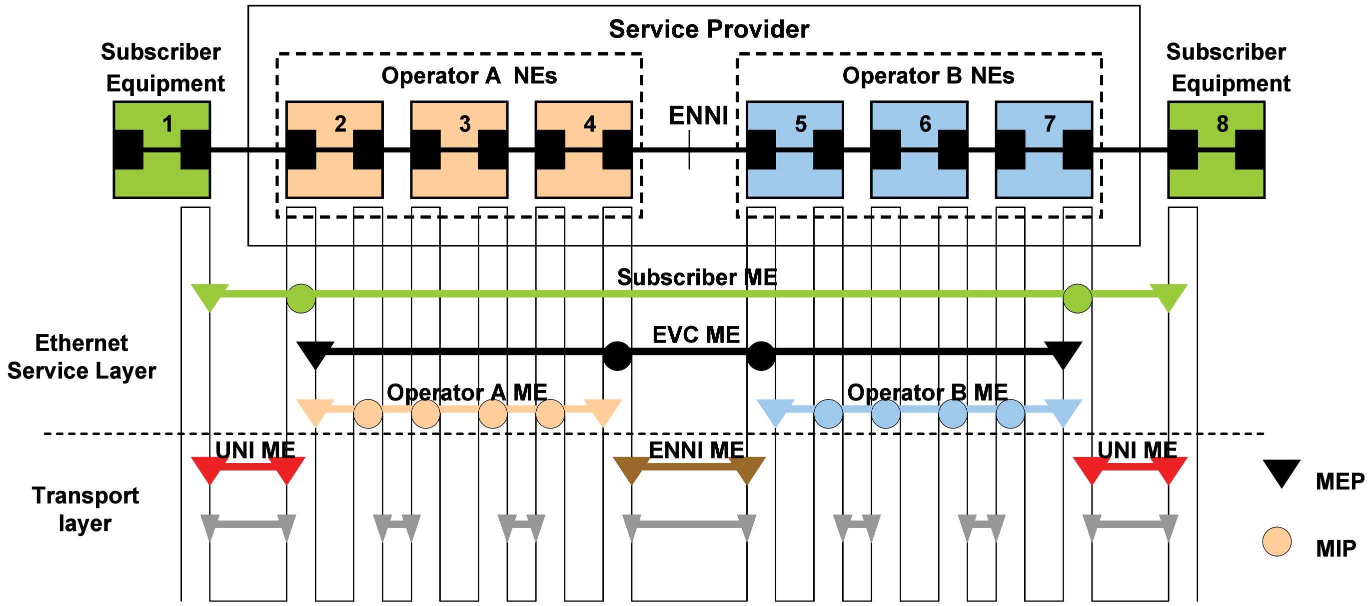


Figure 11: ENNI Service OAM Reference Diagram

The EoX Gateway at elements 4 and 5 will include operator layer MEP functions to provide fault and performance management within each particular operator domain. Additionally, the draft MEF ENNI specification requires EVC layer MIP functions, so that each operator can perform basic fault sectionalization to the other side of the ENNI demarcation. There are also requirements for down MEPs at the ENNI ME layer.

As discussed before, there are many cases where the optical access network will interface to a transit network or a non-Ethernet, service-unaware network. In these cases, since the EoX Gateway is deployed on only one side of the NNI, other permutations of 802.1ag and Y.1731 may be required. Figure 11 shows one example where EoX Gateways connect an access network and a service network, both owned by the same operator, to an intervening transit network owned by a different operator. In this case, the EoX Gateways perform both MEP and MIP functions for fault and performance management. The EoX Gateway may also be responsible to propagate faults, using the AIS function described in Y.1731. This fault propagation can occur either at an individual EVC granularity or at the S-tag tunnel granularity, depending on the network architecture. To read more about Ethernet Service OAM in general, please see the Fujitsu white paper, "Ethernet Service OAM: Overview, Applications, Deployment, and Issues" available from the Fujitsu Website.

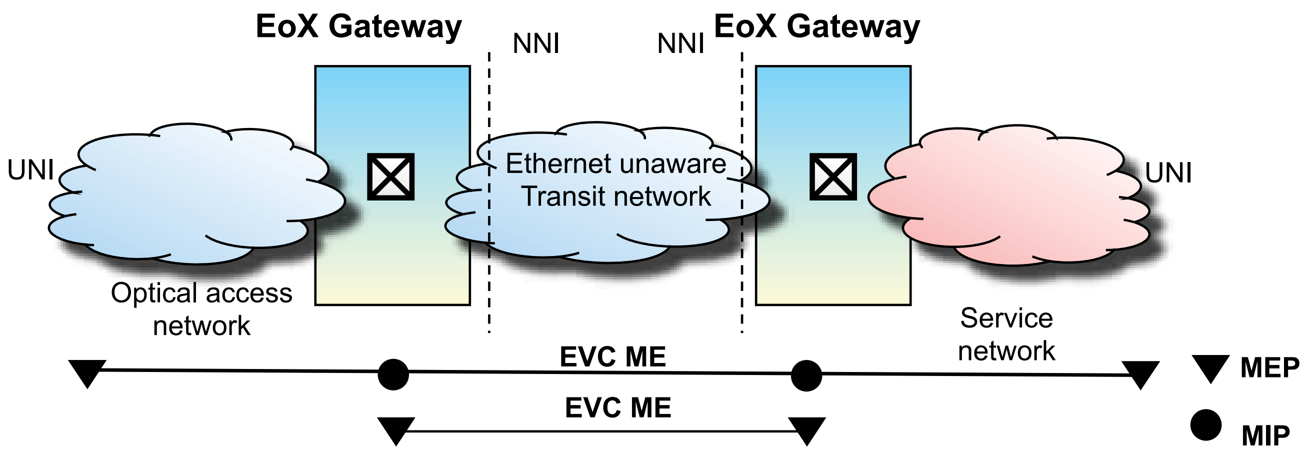


Figure 12: EoX Gateway OAM Functions for a Transit Network Application

EoX Gateway Applications

Important Ethernet applications for the EoX Gateway include wholesale and retail Ethernet access services, mobile backhaul networks, and DSLAM backhaul networks, shown briefly in Figures 13, 14, and 15 respectively.

In each of these applications, there is a need to terminate multiple access and backhaul transport technologies, create handoffs to service and transit networks—often operated by different business entities—and maintain Ethernet service, CoS, QoS, and OAM across these discontinuities.

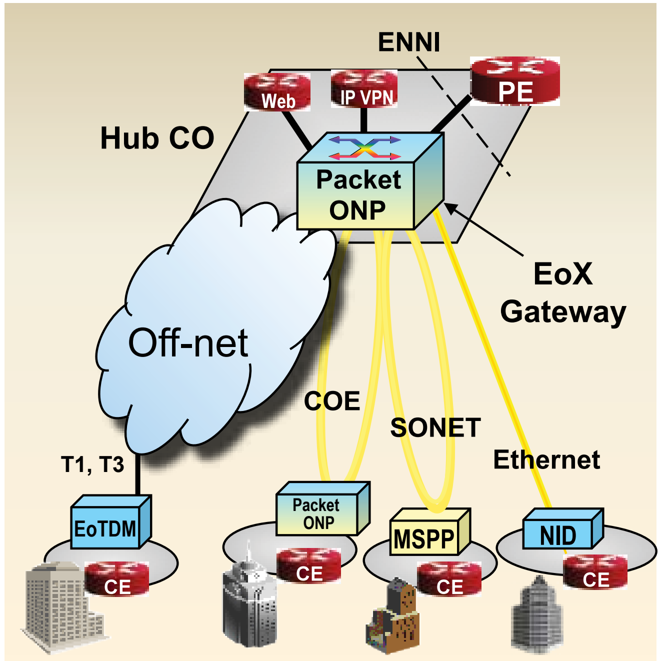


Figure 13: Wholesale and Retail Ethernet Access Service Solution with EoX Gateway at Hub Location

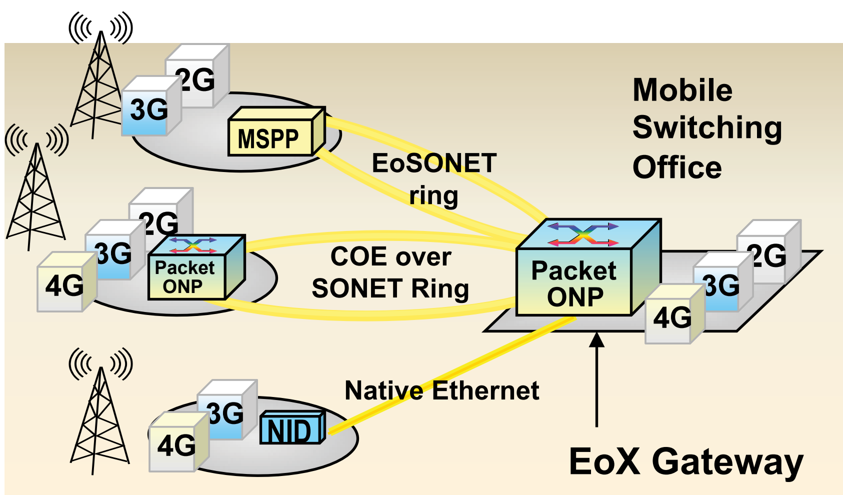


Figure 14: Full-Service Mobile Backhaul with EoX Gateway at Mobile Switching Office

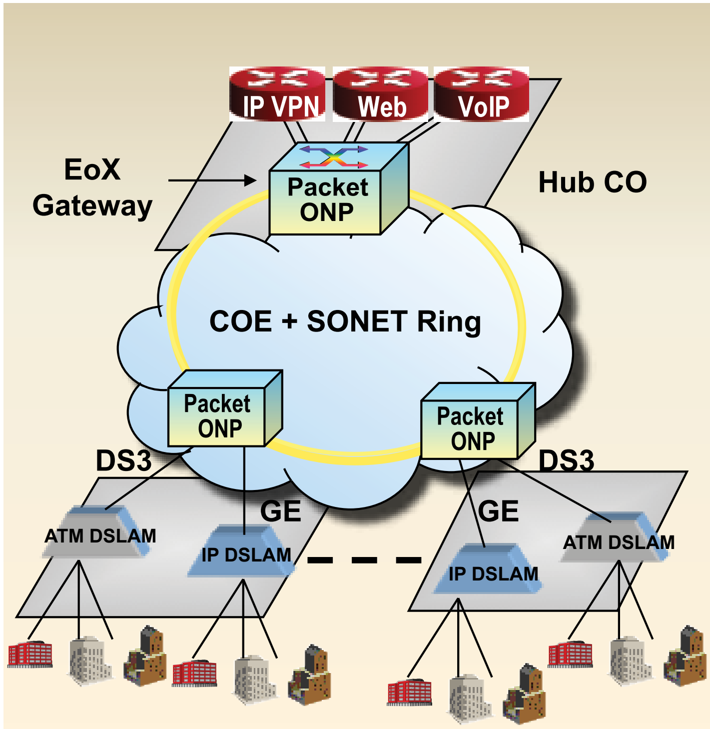


Figure 15: SONET and Connection-Oriented Ethernet DSLAM Backhaul Network with EoX Gateway at Hub Office

Summary

Ethernet has become the most popular interface to attach end users and access devices to the range of Ethernet and IP network services. With the emergence of COE networking, Ethernet now promises to be able to deliver the reliability, performance, and security of SONET/SDH, but with the low cost and bandwidth flexibility inherent to Ethernet.

For many applications, a service provider delivering these Ethernet attached services must deploy multiple access network technologies, and deliver a varied set of handoff interfaces to service and transit networks that may be operated by different business entities.

The combined challenges of access network diversity, service and transport network handoff complexity, and the presence of multiple business entities creates an expensive and complex networking problem at hub offices where these environments collide.

The EoX Gateway solves this problem elegantly. It eliminates additional elements with a combination of rich transport and Ethernet service functions that terminate the diversity of access networks and present a flexible variety of handoffs to the full range of service and transit networks. The EoX Gateway serves many important applications, including wholesale Ethernet access service, retail Ethernet and IP services access, mobile backhaul, and DSLAM backhaul.

Term	Definition
ATM	Asynchronous Transfer Mode
CE	Carrier Ethernet
COE	Connection-Oriented Ethernet
CO	Central Office
CoS	Class of Service
DCS	Digital Cross-Connect System
DSLAM	Digital Subscriber Line Access Multiplexer
DSn	Digital Signal n (1 or 3)
DWDM	Dense Wavelength Division Multiplexing
ENNI	Ethernet Network-Network Interface
EoS	Ethernet over SONET
EoX	Ethernet over any underlying technology
EVC	Ethernet Virtual Circuit
GFP	Generic Framing Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunications Union
MEF	Metro Ethernet Forum
MEG	Maintenance Entity Group
MEP	MEG End Point
MIP	MEG Intermediate Point
MPLS	Multiprotocol Label Switching

Term	Definition
MSPP	Multiservice Provisioning Platform
NID	Network Interface Device
NNI	Network-Network Interface
OAM	Operations, Administration and Management
ONP	Optical Networking Platform
OTN	Optical Transport Network
Packet ONP	Packet Optical Networking Platform
PCP	Priority Code Points
PDH	Plesiochronous Digital Hierarchy
PMO	Present Mode of Operation
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SNCP	Subnetwork Dependent Convergence Protocol.
SONET	Synchronous Optical Networking
STS	Synchronous Transport Signal.
TDM	Time Division Multiplexing
UNI	User-Network Interface
UPSR	Unidirectional Path Switched Ring
UTAS	Universal Tunnel Access Service
VC	Virtual Channel
VCAT	Virtual Concatenation
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

FUJITSU NETWORK COMMUNICATIONS INC.
2801 Telecom Parkway, Richardson, Texas 75082-3515
Telephone: (972) 690-6000
(800) 777-FAST (U.S.)
us.fujitsu.com/telecom