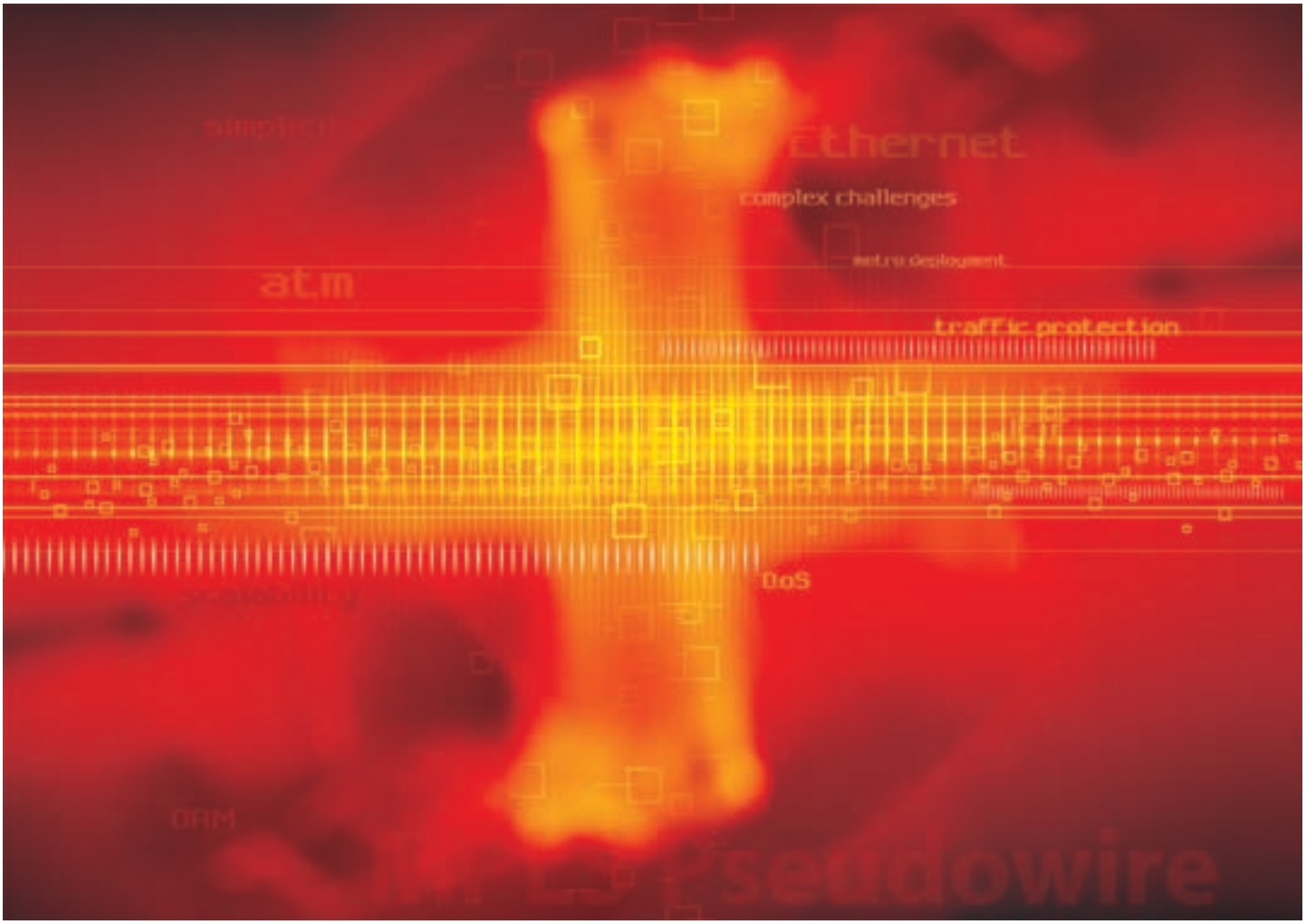
THE POSSIBILITIES ARE INFINITE FUJITSU

MPLS Pseudowire Innovations: The Next Phase Technology for Today's Service Providers



Introduction

MPLS technology enables a smooth evolution of core networks within today's service provider infrastructures. In particular, MPLS allows service providers to cost-effectively support triple-play services and the diverse traffic types generated by enterprises and residential customers. However, this new capability introduces additional challenges within the metro network. The role of data aggregation at the edge of the metro network becomes increasingly critical for economic and operational reasons, and continues to evolve as a broader array of services is envisioned.

Faced with the need to manage diverse traffic types, service providers continually seek the best alternatives for aggregating user "flows" into the MPLS core as shown in Figure 1. User traffic largely arrives over:

- Private leased lines (T1/E1, T3/E3) carrying ATM or Frame Relay traffic. Over time, Ethernet will replace these leased lines.
- Consumer access lines are typically delivered to the network from DSLAMs, which carry broadband traffic over either ATM or Ethernet links. Over time, these links will migrate to IP over Ethernet, and some portion of these links will become PON connections, which are high-bandwidth optical links.

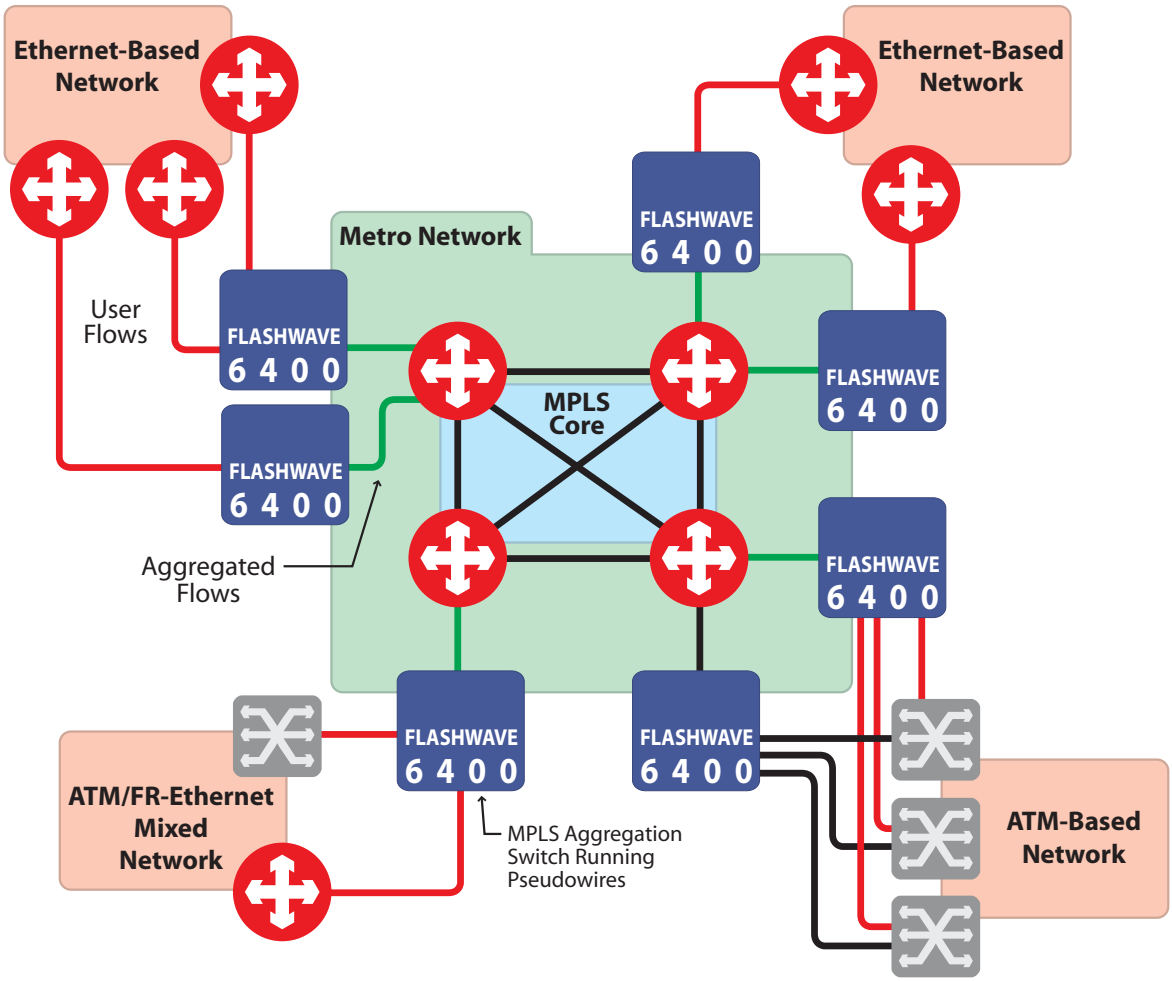


Figure 1: Network Evolution and the Importance of Data Aggregation

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

For your convenience, a list of acronyms can be found at the end of this document.

The Challenges: Complexity and Cost

To handle user traffic, service providers are faced with supporting multiple Layer 2 technologies (e.g., ATM, Frame Relay, and Ethernet) simultaneously. Given the need for more bandwidth on access lines, Ethernet will gradually replace most of the existing ATM and Frame Relay infrastructure. Within this complex and dynamic environment, the effectiveness of per-data-flow management and service interworking become vital. Cost management will also remain critical such that the service providers need an aggregation solution that is engineered to provide only the required functionalities. Over-engineered solutions (i.e., those that can route IP packets at the data forwarding layer with extensive IP routing protocol capabilities) have become less attractive and quite costly for broad deployment at the metro edge.

The Solution: MPLS Pseudowire Technology

Service providers have migrated to a converged IP/MPLS core that is capable of supporting all traffic types, but also want a way to converge traffic at the metro edge. MPLS pseudowires have emerged as the preferred technology to create a uniform interface that can serve this role. Purpose-built MPLS pseudowire switches, with a subset of router features geared for metro aggregation, provide a cost-effective solution for all interface types (e.g., channelized interfaces, PoS, EoS, and Ethernet).

MPLS pseudowire technology was originally designed to encapsulate Layer 2 packets into the MPLS packet format for transport over an MPLS-enabled router core network. The LDP allows MPLS pseudowires to be set up over packet networks [1]. Since the MPLS pseudowire encapsulation method retains the characteristics of original Layer 2 circuits, service providers retain the powerful capability to provision, monitor and control user traffic on a per-flow basis at the network edge.

Realizing these important implications and their potential, Fujitsu has been working with service providers to establish MPLS pseudowire technology as a common network service layer. To be adopted as a viable service, the original MPLS pseudowire technology needed to be enhanced in the following key areas:

- Service interworking
- QoS
- OAM
- Traffic protection and redundancy
- Inter-service provider-network data transport
- Scalability

The combination of the MPLS pseudowire encapsulation and the above enhancements enable service providers to manage and control any type of Layer 2 circuits from the network edge, and are therefore categorized as a "Layer 2.5" technology. Today, several service providers have started the process of deploying MPLS pseudowire technology as the means for service convergence. Service providers and vendors alike have been working closely in various standards bodies (in particular, the IETF and MFA Forum) to advocate and define the appropriate Layer 2.5 techniques.

Access Options

MPLS pseudowire termination devices, or MPLS pseudowire packet switches, have the potential to cost-effectively aggregate the three predominant types of traffic coming into a metro network as shown in Figure 2:

- **ATM:** Many access networks, and in particular wireless backhaul networks, are still deployed using ATM. The MPLS pseudowire switches at the metro edge can map ATM VPIs or VCIs onto MPLS pseudowires, and thereby support traffic moving over the metro network towards the core. In most service provider networks, ATM traffic has been managed in the form of SPVCs using the ATM PNNI protocol. There are a number of methods to carry ATM traffic over an MPLS pseudowire-based network, and the most efficient technique available is defined in a specification included in the MPLS/Frame Relay Alliance Technical Committee draft [2]. This technique requires a gateway to process both PNNI and MPLS pseudowire signaling protocols and map each SPVC into a single MPLS pseudowire. Draft-Swallow allows the service providers to migrate ATM circuits into other forms of circuits (such as Ethernet) transparently.

- **Ethernet:** Ethernet is rapidly becoming the predominant access media for end users. Service providers use Ethernet VLANs to separate different types of user traffic. MPLS pseudowire switches can map each Ethernet VLAN to an individual MPLS pseudowire. Because Ethernet VLAN flows and MPLS pseudowires operate on different network layers, OAM represents the major challenge in this area. OAM mapping enables the operators to monitor and diagnosis edge-to-edge user flows for Ethernet.

- **MPLS Pseudowires:** A number of service providers bring end-user traffic into the metro network over MPLS pseudowires. For this configuration, the MPLS pseudowire switch must first terminate the incoming MPLS pseudowires and switch the data packets onto another MPLS pseudowire to traverse the metro network (see Figure 2). Since MPLS pseudowires can be established using various conventions—static, PWid (also known as FEC 128), or Generic FEC [1], the MPLS pseudowire switch functions as a proxy to switch MPLS pseudowires directly. This proxy role is known as MPLS pseudowire "stitching" or "switching."

All three types of applications involve diverse traffic, and individual data flows will have different priorities and QoS parameters. To ensure that these priorities and QoS requirements are met, MPLS pseudowire switches must be able to protect user flows on a per-MPLS pseudowire basis.

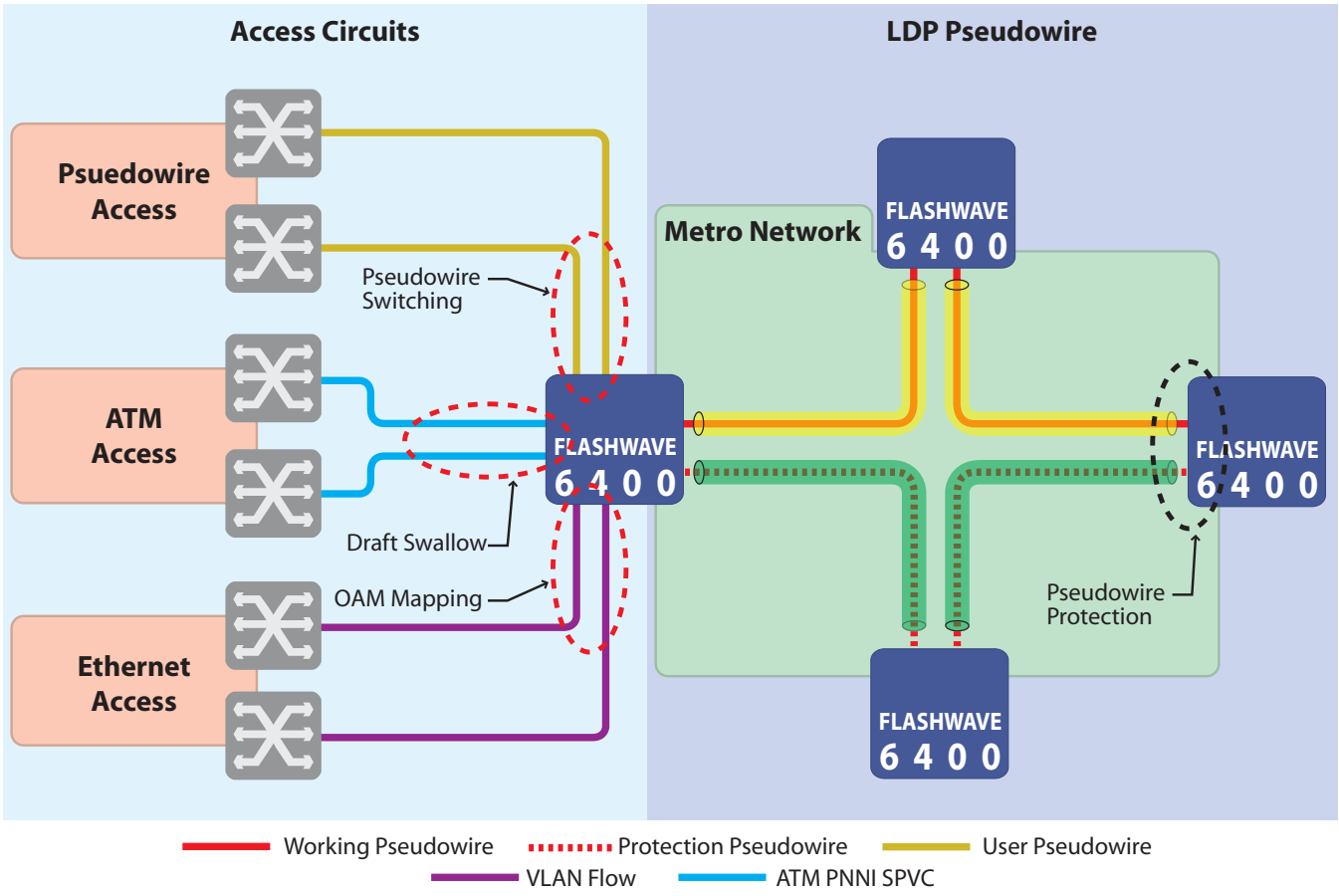


Figure 2: MPLS Pseudowire Termination and Switching Devices

Metro Deployment: MPLS LSR

Within the metro network, MPLS pseudowire switches provide a cost-effective alternative to full-function routers. As shown in Figure 3, affordable MPLS pseudowire switches can function as typical MPLS LSRs if designed with the following built-in capabilities:

- Discover topology by using an IGP such as OSPF or IS-IS
- Set up LSPs using RSVP-TE or LDP
- Apply RSVP Fast Reroute [4] and other path protection techniques to ensure that service level requirements are met for each traffic flow

Service providers have applied traditional MPLS-enabled routers for both the LER and LSR roles, but the requirements for these two functions are very different. The LERs must extensively interface with IP routing protocols (such as routing filtering, import and export) to route each individual data packet onto the corresponding LSPs. As a result, these routers are quite complex to operate and expensive to build.

The LSRs, in contrast, are mainly used to switch data paths based on the MPLS labels and are therefore simpler to operate and less expensive to build. Purpose-built MPLS pseudowire switches can perform extremely well—and provide cost savings—when applied as LSRs within the metro network.

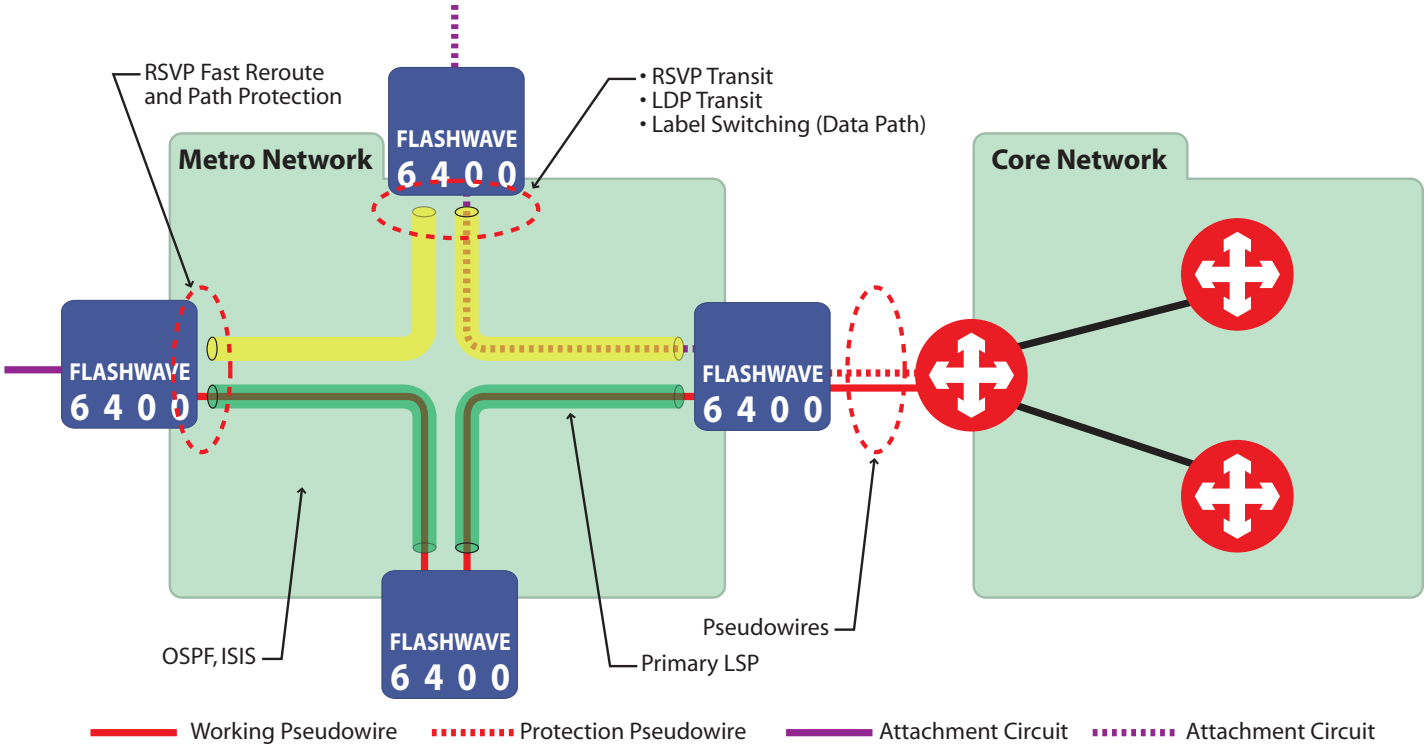


Figure 3: Metro Deployment with MPLS LSRs (MPLS Pseudowire Switches

MPLS Pseudowire Implementation and Innovations

Recognizing the potential benefits and widespread applicability of MPLS pseudowire technology within wireline and wireless service provider networks, Fujitsu became an early innovator using the emerging standard. Today, the Fujitsu FLASHWAVE® 6400 Layer 2.5 aggregation switch offers the most advanced MPLS pseudowire implementation and several advanced features that transform the technology into a robust service platform for today's service provider networks. The FLASHWAVE 6400 platform combines the best of Layer 3 application awareness and the best of Layer 2 economics, operations, and interworking in a single platform.

Metro-Core Interface Alternatives

Two prevalent methods exist for connecting metro networks to a provider's core network. The first conventional approach is the attachment circuit model as shown in Figure 4. This method has the advantage of simplicity because it is easy to implement with existing products. However, this model requires traffic to hop over multiple underlying technologies that may operate on different network management planes, making it very difficult to troubleshoot failures and manage end-to-end per-flow traffic.

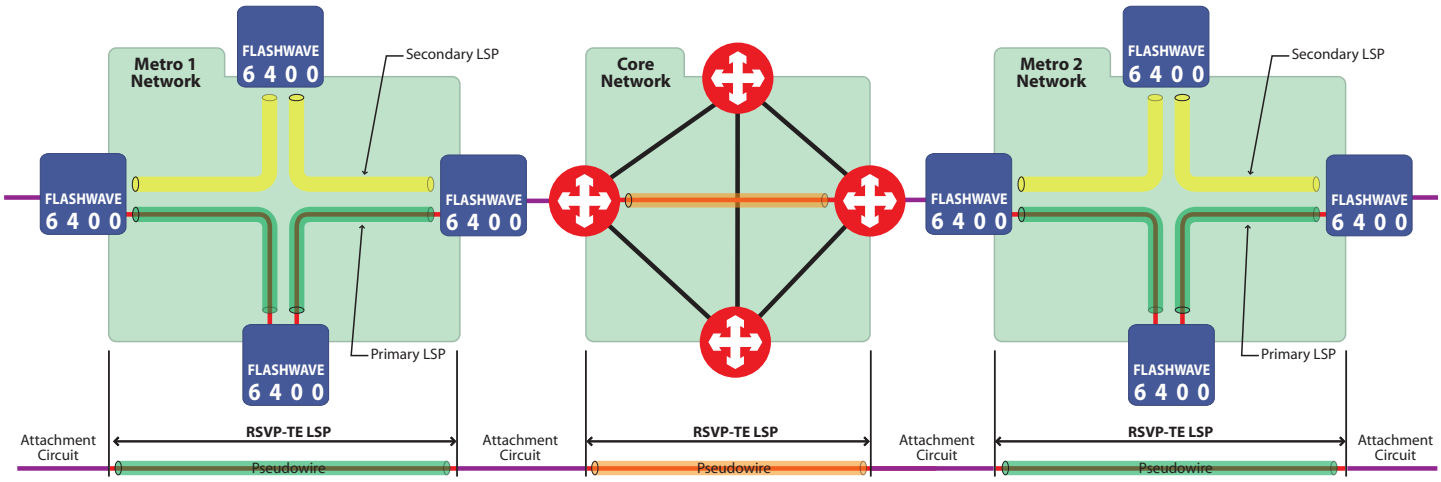


Figure 4: Conventional Model #1—Attachment Circuits for Metro-Core Interfaces

The second conventional alternative is the service provider-over-service provider model as shown in Figure 5. This method is easy to understand since it is based on the well-known BGP 2547 specification. It offers the advantage of end-to-end MPLS functionality. RSVP tunnels are established to create an edge-to-edge MPLS pseudowire connection.

The most serious drawback in this model is the lack of security. To set up inter-domain RSVP tunnels, this model requires that the networks share network resource information, a condition that introduces numerous vulnerabilities between competing service providers.

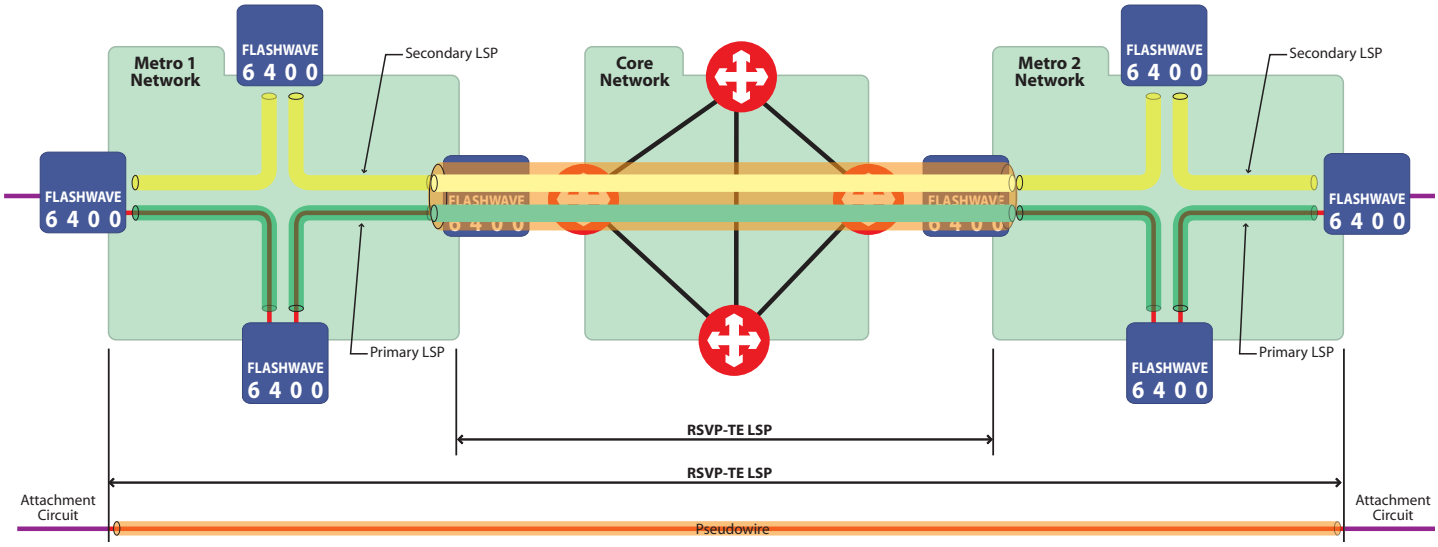


Figure 5: Conventional Model #2—Carrier-over-Carrier

There have been a number of attempts in standards bodies to overcome the "information leaking" problem in RSVP-TE for inter-domain traffic engineering. More time is required to determine if these efforts will be successful.

To connect metro and core networks efficiently, Fujitsu has been working closely with service providers to pioneer an advanced capability known as the MPLS pseudowire multi-hop model as shown in Figure 6. In this model, the networks remain independent. Each user data flow goes through the entire network as a single MPLS pseudowire, and is mapped and aggregated into different RSVP tunnels at the edges of service provider networks. In other words, the MPLS pseudowires traverse multiple hops before reaching their destination.

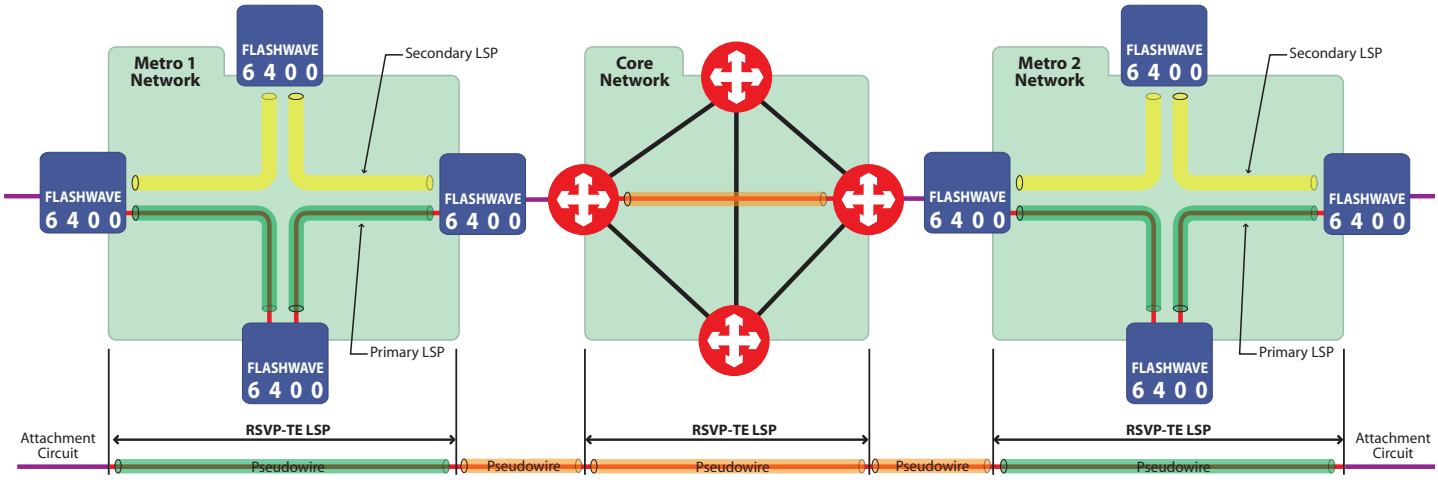


Figure 6: Carrier-preferred Model—MPLS Pseudowire Multi-hop

The MPLS pseudowire multihop capability provides service providers a solution characterized by:

- **Management simplicity:** MPLS pseudowire technology is becoming well understood, and service providers have access to network management tools that support MPLS pseudowires. Instead of working with multiple technologies as required in the attachment circuit model, the multihop model allows operators to monitor and control data traffic at the MPLS pseudowire level across the entire network.
- **Security:** MPLS pseudowires are handled at each service provider's network edge, which means that data forwarding can be controlled based on the service provider's resource and network policy criteria. Consequently, no network information must be exchanged between service provider networks.
- **Scalability:** All MPLS pseudowires are managed via a single control session between any two adjacent edge nodes. The edge nodes will always re-map and aggregate the MPLS pseudowires into different MPLS tunnels. The fact that the MPLS pseudowires are divided into segments enables the control plane to handle a greater number of connections.
- **Standardization:** The MPLS pseudowire multi-hop specification is in the process of being standardized within an IETF committee [3]. The Fujitsu implementation validates this approach and is driving this and future standardization efforts.

ATM SPVC to MPLS Pseudowire Interworking

Many vendors support ATM-MPLS pseudowire network-level interworking as shown in Figure 7. At the network ingress edge, each ATM SPVC is mapped into an MPLS pseudowire and transported over the core. At the egress edge, the MPLS pseudowire is recovered and mapped to an ATM SPVC.

There are a number of disadvantages in this approach, the most serious of which is that the access networks must all be ATM-based. This requirement will handicap a service provider's ability to move away from the existing ATM infrastructure to IP or Ethernet. In addition, this approach does not scale well since each SPVC-MPLS pseudowire mapping pair must be statically configured at the edge nodes.

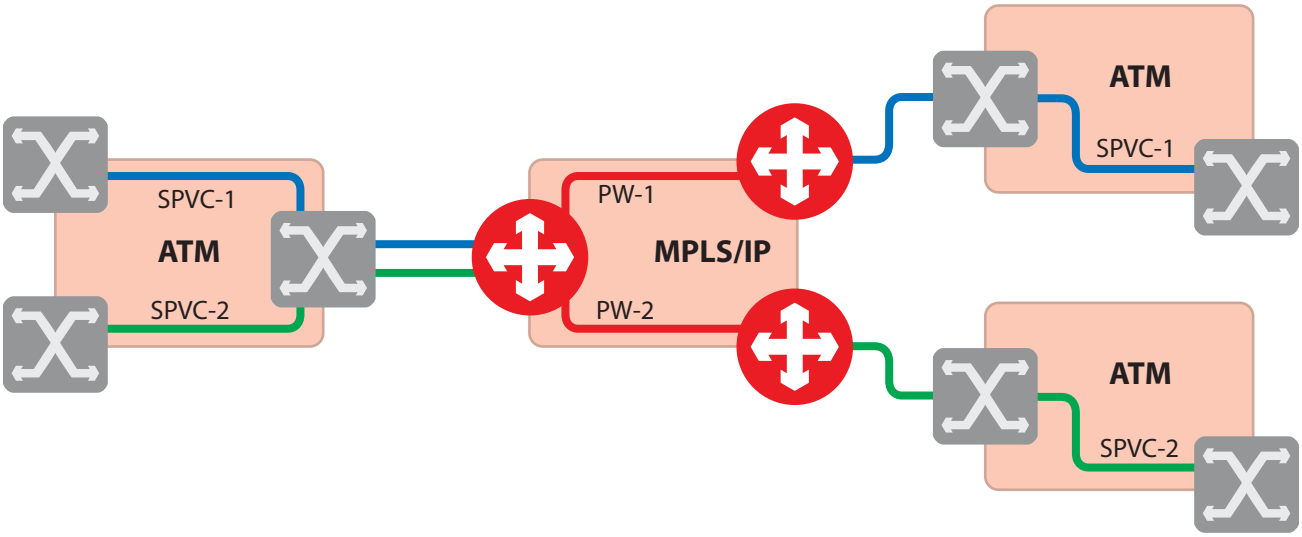


Figure 7: Conventional ATM-MPLS Pseudowire Network Interworking

A more efficient approach, Draft-Swallow, has been undergoing standardization in the MFA Forum. The Fujitsu FLASHWAVE 6400 platform is the first system that supports this functionality in response to significant demand from service providers.

With the Draft-Swallow approach, the MPLS pseudowire switch performs the role of a gateway for connecting the PNNI-based ATM/Frame Relay networks and MPLS/IP networks as shown in Figure 8. This is referred to as service interworking (as opposed to network interworking) since the ingress and egress networks are not the same. As a gateway, the MPLS pseudowire switch will first translate IP edge node addresses into ATM, and then inform the ATM edge nodes about those addresses. Therefore, ATM edge nodes will view the IP edge nodes as "ATM neighbors" connected through the MPLS pseudowire switch. The ATM edge nodes will initiate the SPVCs and transfer data traffic to the MPLS pseudowire switch, which will then map each SPVC to an MPLS pseudowire and forward the traffic to the appropriate IP edge nodes.

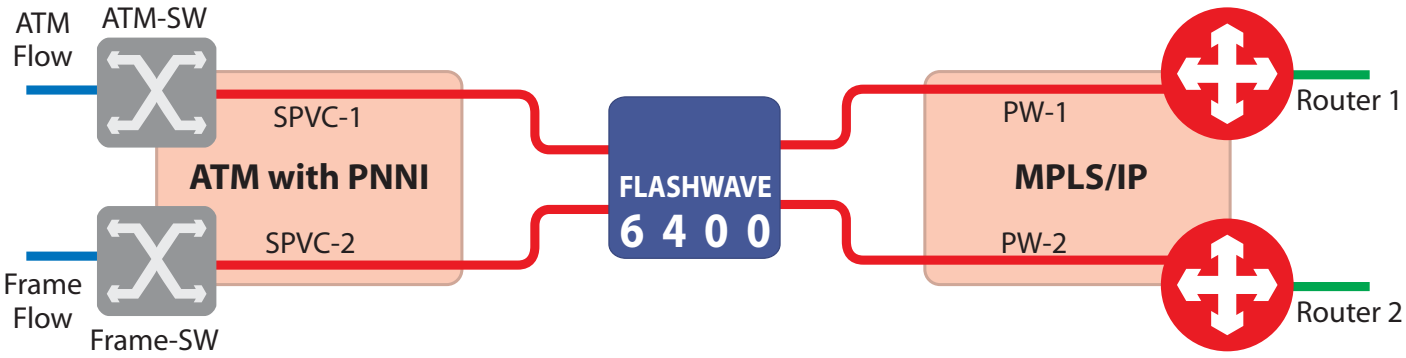


Figure 8: ATM-MPLS Pseudowire Service Interworking (Draft-Swallow)

There are two major differences between the Draft-Swallow approach and the conventional approach:

1. The conventional approach is to "tunnel" one protocol/application across another network. The Draft-Swallow technique "translates" one service to another and provides true service interworking.
2. With the conventional approach, the "network interworking" is to terminate and encapsulate the protocol over point-to-point connections. The Draft-Swallow approach is to translate the control protocol information transparently via an interworking gateway.

The result is that the new approach will allow service providers to seamlessly transfer the existing ATM or Frame Relay services onto IP/MPLS networks. Since the MPLS pseudowire switches interface with both PNNI and MPLS signaling protocols, all the connections can be established automatically.

MPLS Pseudowire Traffic Protection and Restoration

Service providers need to ensure traffic protection on every segment and in every layer of the network. MPLS pseudowire deployments can incorporate adequate protection and redundancy as shown in Figure 9.

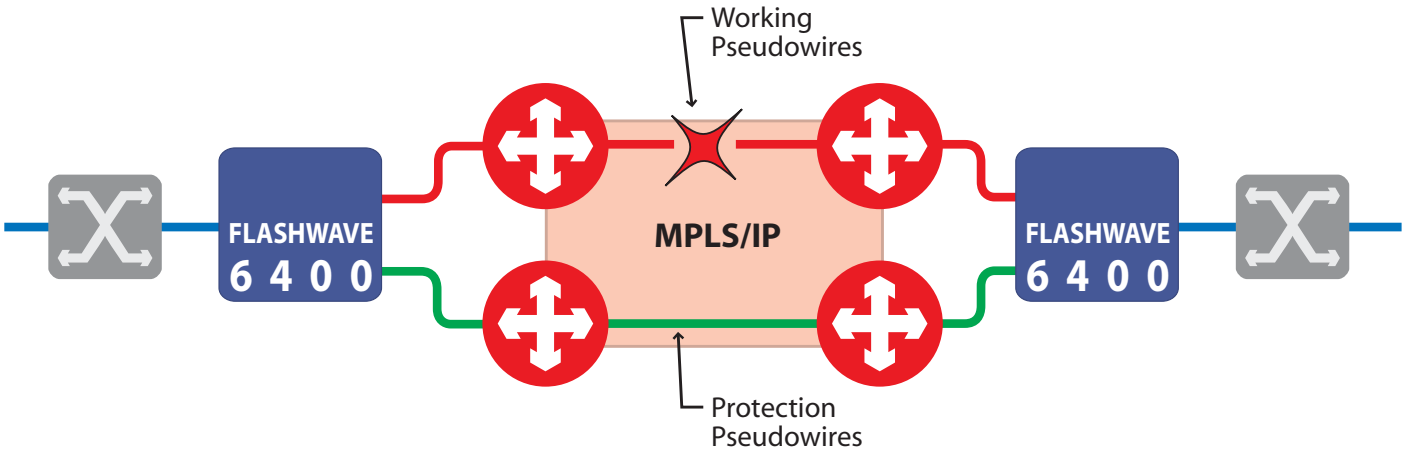


Figure 9: MPLS Pseudowire Protection

For each operational (or working) MPLS pseudowire, the network edge nodes will set up one or multiple back-up (or protecting) MPLS pseudowires. In the event of a network failure, data traffic can continue to be forwarded through the backup MPLS pseudowires.

In today's MPLS networks, service providers have been deploying MPLS Fast Reroute [4] for traffic protection. However, there are a number of limitations that can only be solved with MPLS pseudowire protection:

- **Bandwidth mismatch:** When a lower-speed link is being used as a backup for a higher-speed link, problems can arise during protection and restoration operations. If the higher-speed link fails, all traffic will be switched onto the lower-speed link. However, mission-critical traffic could be dropped as the result of link congestion during the switchover process. This problem is easily resolved by giving each MPLS pseudowire its own priority, which allows the MPLS pseudowires to preempt each other when necessary. Also note that, since the MPLS pseudowires are always bidirectional, the priority assignment must be consistent on both ends of the MPLS pseudowires.
- **Low-cost access devices:** Due to cost and operational reasons, network access devices such as PON ONTs do not have the full functionality of an IP/MPLS router, and use MPLS FRR for traffic protection. However, these access devices can implement MPLS pseudowires and MPLS pseudowire protection for data access and protection. The FLASHWAVE 6400 platform allows the configuration of hot, warm, and cold standby connections. In the case of hot standby situations, the platform delivers a fast switchover of less than 50 ms.
- **Planned traffic shifting:** During times of network maintenance, MPLS pseudowire traffic on one link may be shifted to another link. To support this capability, MPLS pseudowire protection features of the FLASHWAVE 6400 platform give operators the ability to manually trigger traffic shifting when desired.

MPLS pseudowire protection is currently undergoing standardization in the IETF [5].

OAM and OAM Mapping

The OAM function is critical in access networks. In core networks, data traffic can be readily re-routed over an alternative path in the event of a network failure. In access networks, however, data traffic seldom has alternative or backup paths.

Another challenge is imposed by end-to-end OAM support. A variety of OAM techniques are employed for the various network topologies. ATM, Ethernet, and MPLS all have different OAM requirements and mechanisms. However, in most of the service provider networks, an access network is based on either Ethernet or ATM while the core is typically based on MPLS. Therefore, the pseudowire switches must be able to support multiple OAM mechanisms and map the OAM parameters from one network type to another.

Figure 10 illustrates how the Fujitsu FLASHWAVE 6400 platform handles OAM and OAM mapping using VCCV and Ethernet OAM (802.3ah). For example, in the event of an Ethernet failure, the switch will capture the failure alarms and piggyback them onto the VCCV messages. Consequently, remote nodes will receive the failure notification and act appropriately.

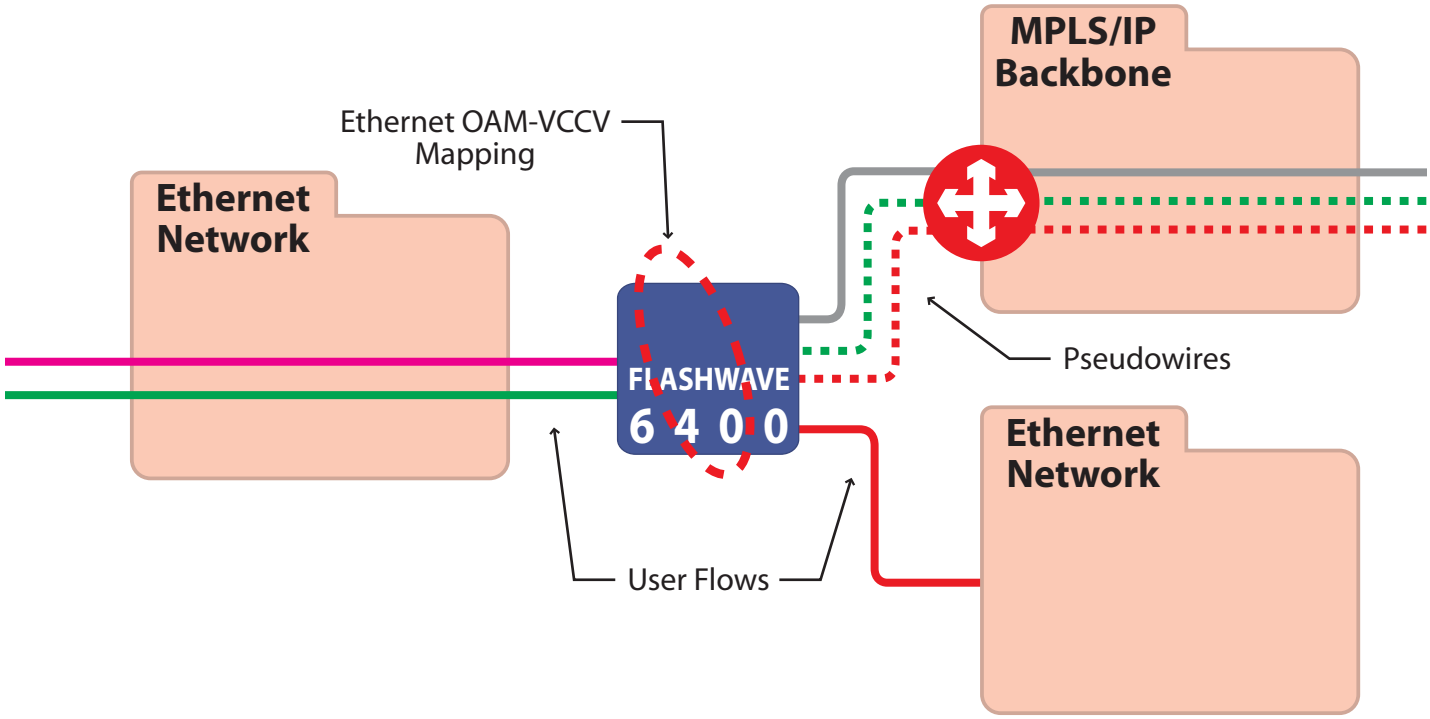


Figure 10: OAM and OAM Mapping

Conclusion

MPLS pseudowire technology presents today's service providers with many opportunities to cost-effectively aggregate diverse traffic onto an IP/MPLS core network while maintaining excellent service to customers with legacy networks. The purpose-built FLASHWAVE 6400 switch allows service providers to reduce costs at the metro edge by deploying a lower-cost alternative to traditional full-function IP/MPLS routers.

Fujitsu provides service providers with the most stable, full-function MPLS pseudowire foundation technologies, and will continue to lead in offering advanced features required for robust, commercial networks. This future direction and commitment are evident in the most recent FLASHWAVE 6400 MPLS pseudowire enhancements, including:

- MPLS pseudowire multihop networking for secure, scalable metro-core interfacing;
- Service interworking functionality for connecting ATM and Frame Relay networks to IP/MPLS networks;
- MPLS pseudowire traffic protection and restoration features for fast switch-overs
- Ethernet-MPLS OAM mapping for end-to-end traffic monitoring and diagnosis.

References

[1] PW-Ctrl "Pseudo-wire Setup and Maintenance using the LDP", Luca Martini, et al, IETF draft
[2] Draft-Swallow "Soft Permanent Virtual Circuit Interworking between MPLS MPLS Pseudowires and ATM: Unmapped Mode Version 1.0", George Swallow, MFA Contribution, July 2005
[3] PW-Mhop "Dynamic Placement of Multi Segment Pseudo Wires", Balus et al, IETF draft
[4] MPLS-FRR "Fast Re-route Extensions to RSVP-TE for LSP Tunnels (RFC 4090)", P. Pan et al
[5] PW-Protect "Pseudowire Protection", P. Pan, IETF draft

Acronym	Descriptor
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BGP 2547	RFC2547 – a BGP extension for MPLS VPN
DSLAM	Digital Subscriber Line Access Multiplexer
EoS	Ethernet over SONET/SDH
FEC	Forward Error Correction
FRR	Fast Re-route
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
IS-IS	Intermediate System-Intermediate System
LSP	Label-Switched Path
LDP	Label Distribution Protocol
LER	Label Edge Router
LSR	Label Switch Router
MFA Forum	MPLS/Frame Relay Alliance Forum
MPLS	Multi-Protocol Label Switching
OAM	Operation, Administration, and Management
ONT	Optical Network Terminal
OSPF	Open Shortest Path First
PON	Passive Optical Network
PoS	Packet over SONET/SDH
PNNI	Private Network-Network Interface
PW	Pseudowire
PWE3	Pseudowire Edge-to-Edge Emulation
PWid	Pseudowire ID
QoS	Quality of Service
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol for Traffic Engineering
SPVC	Soft Permanent Virtual Circuit
TDM	Time-Division Multiplexing
VPI	Virtual Path Identifier
VCI	Virtual Circuit Identifier
VCCV	Virtual Circuit Connection Verification
VLAN	Virtual LAN

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