

Enhancing Converged MPLS Data Networks with ATM, Frame Relay and Ethernet Interworking

Virtual Private Networks (VPN) are a popular way for enterprises to interconnect remote sites. Traditionally, VPNs have been based on Frame Relay, Asynchronous Transfer Mode (ATM) or Time Division Multiplex (TDM) private lines, using the service provider's ATM core network, and accounting for the majority of their data service revenues. However, the influences of a highly dynamic telecommunications market have raised demands for increased flexibility while controlling costs. New revenue opportunities are emerging for service providers to differentiate their offerings through services such as IP VPNs and the Virtual Private LAN Service (VPLS), while achieving operational efficiencies through convergence of all services on a common MPLS backbone. However, existing technologies, such as ATM, provide highly profitable services which must continue to be supported. The authors describe how network and service interworking can help to deliver profitable services over the new converged network.

ENHANCING CONVERGED MPLS DATA NETWORKS WITH ATM, FRAME RELAY AND ETHERNET INTERWORKING

New interworking challenges must be addressed to realize the benefits of a converged network infrastructure for IP and data services.

Introduction

Multi Protocol Label Switching (MPLS) has evolved from a technology designed to add packet switching performance to Internet Protocol (IP) core networks, to one that enhances manageability and resilience and adds traffic engineering and Quality of Service (QoS) features to such networks. Consequently, MPLS now has the potential to support services with levels of availability and QoS that challenge the attributes of traditional technologies, such as the Asynchronous Transfer Mode (ATM). Alongside this evolution, Ethernet leased lines and Virtual Private LAN Services (VPLS) are emerging as key new service offerings, partly because of Ethernet's popularity in the enterprise Local Area Network (LAN) environment.

New IP Virtual Private Network (VPN) services promise new revenue opportunities for service providers. Nevertheless, traditional services, such as ATM and frame relay, remain highly lucrative, while enterprises are reluctant to change their deployed corporate network infrastructures.

Service providers need to be able to generate additional revenue by broadening the range of services offered by the IP network, to extend the reach of existing Ethernet and frame relay / ATM services to new sites attached to the packet network, and to reduce capital expenditure and operating expenses. One solution is to converge existing and new services onto a common MPLS core network. The driver for this is the service provider's business need to maximize profitability while minimizing risk. It enables revenue to be generated from the broadest range of traditional and emerging services over a fixed cost infrastructure, minimizes the need to roll out a new network for each new service, and reduces the number of skilled personnel required to operate the network. It also reduces the number of network nodes that must be deployed and operated, and the time to market for new services. However, multi-service capabilities must match operational simplicity in the converged network.

New protocol interworking capabilities for MPLS networks are essential to enable service breadth to be maintained while simultaneously introducing new services.

Expectations of the Converged Packet Network

To continue to support existing services and allow operators to deploy new services, the converged packet network must match or exceed the capabilities that existing networks (e.g. ATM) provide to support currently deployed services. It must also be sufficiently flexible, scalable and cost-effective to enable new services to be deployed more economically than today. If it is to be a truly converged network, it must support current and new services without forcing the operator to build networks with separate technologies to deliver each service.

These general goals translate into a set of key requirements. First, the network must be able to cope cost-effectively with traffic growth, adapting the way in which the infrastructure accommodates future changes in service demand. Second, carrier class protection and restoration must be provided to allow flexibility both in the service availability, matching the levels specified in Service Level Agreements (SLA) for existing services and allowing differentiated offerings for new services, and in the way in which the operator delivers that SLA commitment (e.g. localized protection of a link or node, versus protection of an end-to-end path). Fault detection and diagnosis contributes to this, requiring reactive Operations, Administration and Maintenance (OAM) procedures so that an operator can detect network faults and take the appropriate action before the user's SLA is contravened, as well as proactive OAM so that faults can be located and diagnosed.

Service level differentiation is the basis for new revenue streams from the MPLS network, as it enables different services to be offered with different performance objectives (e.g. virtual leased lines, Internet access), or multiple grades of the same service (e.g. gold, silver). Intelligent edge policy decision-making is therefore required, making specific network resources visible and enabling them to be selected in order to apply different policies for routing customer traffic at the service provider edge.

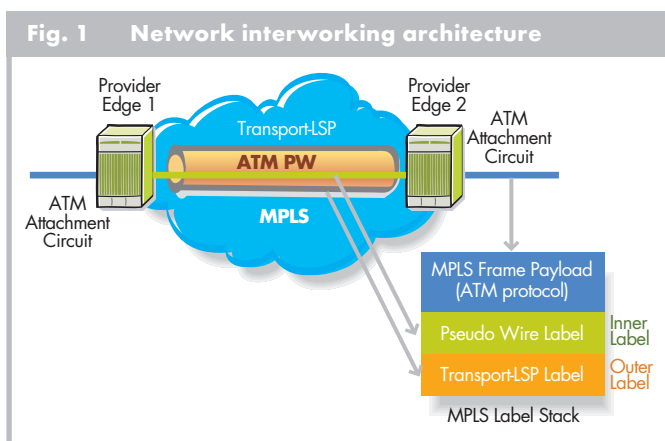
Services, such as frame relay, already benefit from many of these features over an ATM core network, thus making it possible to provide high revenue services. Convergence of existing and new services on a common MPLS network requires existing services to be carried transparently if operators are to maintain and expand their revenues, as well as seamless interworking with the new services at the user, control and management planes.

Network and Service Interworking

Network and service interworking are required to realize VPN services on a converged packet network. Network interworking, which is known as *pseudo wire emulation* in the Internet Engineering Task Force (IETF) [1], allows networks of the same link layer to communicate transparently across a network of a different link layer. Interworking is performed at the link layer and is typically carried out within the network, enabling existing and new services to be transparently consolidated.

Figure 1 shows the architecture for ATM/MPLS network interworking, as specified in the ATM Forum [2] and in the IETF [1]. One end-to-end virtual circuit of an ATM layer 2 VPN is shown. This consists of a native ATM Attachment Circuit (AC) at each end, connected by an ATM Pseudo Wire (PW), which traverses an MPLS network. ATM connections are carried transparently between edges of the MPLS core using Label Switched Paths (LSP), which behave as transparent tunnels. An ATM/MPLS InterWorking Function (IWF) resides in a Provider Edge (PE) node at each edge of the MPLS core and maps each connection to a PW multiplexed in a Transport LSP (T-LSP) by pushing a 20-bit PW label and an outer MPLS label onto encapsulated ATM user data. The ATM Forum [2] and the IETF [3] have specified four encapsulation formats for ATM:

- *N-to-1* and *1-1* modes both encapsulate ATM cells in MPLS frames; 1-to-1 mode incurs less bandwidth overhead in the process.



- *SDU* and *PDU* modes are used to carry ATM Adaptation Layer Type 5 (AAL5) Service Data Units (SDU) and Protocol Data Units (PDU), respectively.

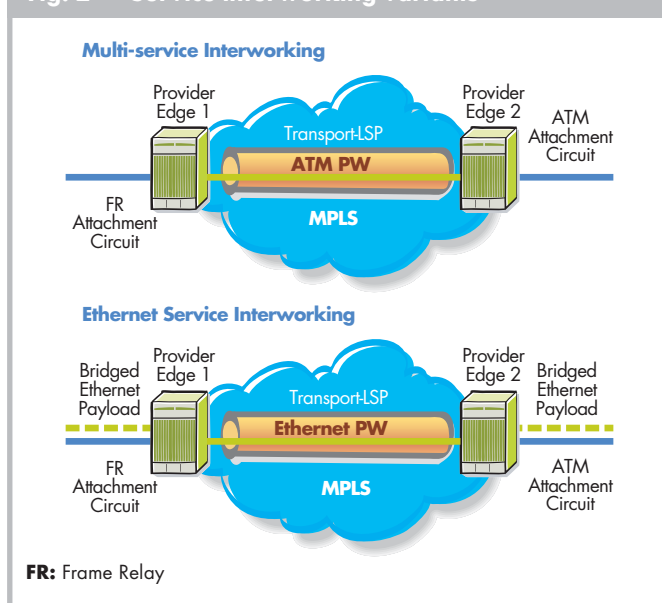
The relative merits of these encapsulation formats are analyzed in [4].

As LSPs are unidirectional, a pair of T-LSPs is required to provide bidirectional connectivity between any two PEs. These LSPs are established either by provisioning or through MPLS signaling. Since the ACs and the PW are of the same type (i.e. ATM), the resulting layer 2 VPN circuit is termed homogeneous.

Service interworking allows Customer Edge (CE) devices to exchange service layer PDUs transparently across different link layer technologies. Interworking is performed at the layer above the link layer, allowing the service providers to offer, for example, high speed Ethernet access that works transparently with their established frame relay and ATM services. Figure 2 shows two example variants of service interworking. The first is multi-service interworking in which the link layer of one attachment circuit (ATM in the figure) is extended across the MPLS network as a PW of the same type. PE1 then performs FRF8.2 service interworking [5] between the frame relay AC and the ATM link layer of the ATM PW. Other combinations of Ethernet, ATM and frame relay AC and PW can also be applied to multi-service interworking scenarios.

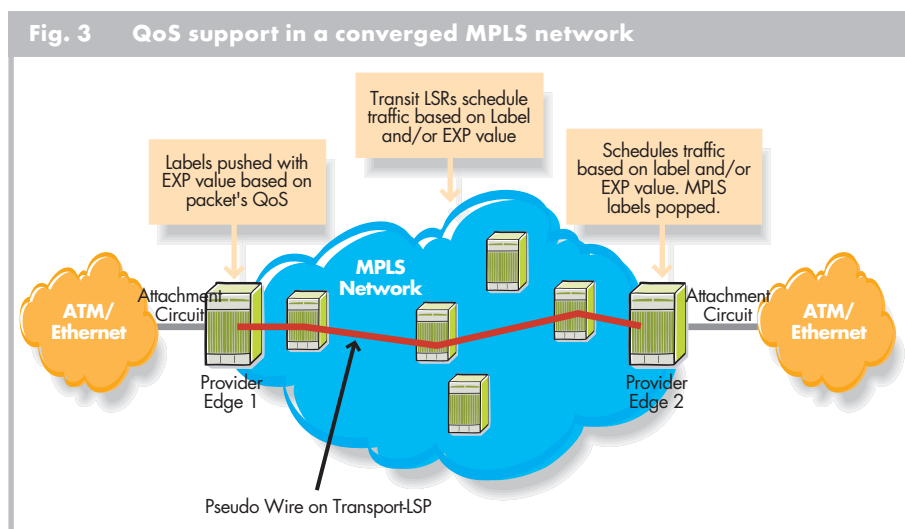
The second variant is Ethernet service interworking, which can be used to extend an Ethernet service to sites attached via Ethernet, ATM and frame relay circuits. Here, a bridged Ethernet payload is carried by

Fig. 2 Service interworking variants



the ATM and frame relay ACs. The Ethernet PDU is encapsulated in an Ethernet PW in a similar way to ATM, which is extended across the MPLS network between PE1 and PE2, thereby extending the Ethernet service layer end-to-end. If the end-to-end service is IP, in which case the ACs carry routed PDUs instead of bridged Ethernet PDUs, then an IP PW can be used. This is known as IP service interworking; the resulting layer 2 VPN circuit is heterogeneous because the ACs and PW are of different types.

One of the main contributors to the success of technologies such as ATM is the ability to guarantee QoS for user traffic. There are a number of well understood and standardized tools to support QoS, including standard service categories and conformance definitions, standard traffic parameters, connection admission control, traffic policing and shaping, and Private Network – Network Interface (PNNI) QoS-based routing. These need to be mapped to equivalent mechanisms in the MPLS network to continue to support QoS guarantees. *Figure 3* illustrates how QoS can be supported in a converged MPLS network.



If the attached network is ATM, the QoS treatment to be given to each ATM cell is implicit in the connection's service QoS commitments and the setting of the cell loss priority, while if the attached network is Ethernet, then the 802.1p bits can indicate the priority of the Ethernet frame. PE1 can map these to the EXP (Experimental) bits of the T-LSP label. The Label Switching Routers (LSR) that the T-LSP transits in the core network can then apply a DiffServ treatment (scheduling and drop priority) based on the value of the EXP bits, the T-LSP label or both. At the egress of the MPLS network, PE2 schedules traffic onto the attachment circuit link based on these values. Traffic engineering of the T-LSPs

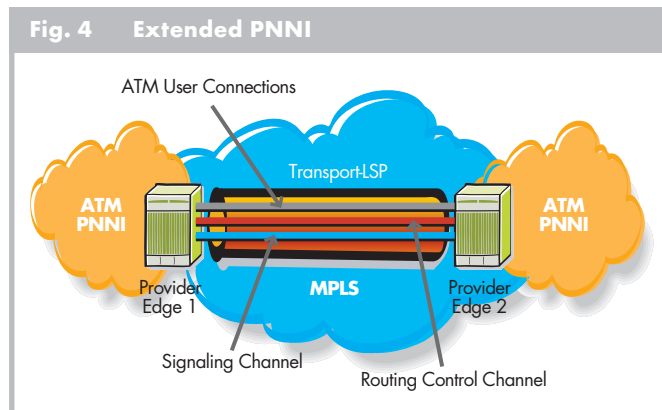
ensures that sufficient bandwidth is reserved in the MPLS network, while admission control in the PEs can be used to reserve bandwidth on the T-LSP to ensure that any QoS commitments can be met.

Control Plane Interworking

Control plane interworking is required between the disparate link layer protocols to enable dynamic end-to-end connectivity to be established. This presents a challenge because of differences in the deployment and capabilities of the ATM, frame relay, Ethernet and MPLS control planes. Consider the example of ATM/MPLS Interworking. An important capability of existing ATM networks is ATM switched services, based on Soft Permanent Virtual Connections (SPVC) and Switched Virtual Connections (SVC). SPVCs are critical in today's networks as they simplify the provisioning of ATM services and support dynamic traffic engineering and faster restoration in the event of network failure. ATM SPVCs also extend connectivity to non-ATM end-points, such as frame relay and Ethernet, on an ATM switch. Thus non-ATM services continue to drive the deployment of ATM SPVCs. By

transparently supporting ATM switched services over MPLS, existing provisioning tools and operational procedures can be used. It is therefore important to provide methods for interworking ATM switched services and MPLS pseudo wire services [6].

Three architectures for ATM/MPLS control plane interworking are discussed here. In the first, only Permanent Virtual Connections (PVC) exist. These are established by the network management system or by configuration in the ATM networks, and are carried across the MPLS network using PWs established and released using the PW control protocol [7].



The second is extended PNNI [8,9], as shown in *Figure 4*, in which a PNNI link is extended transparently across the MPLS core network between two attached ATM PNNI networks. PNNI is the protocol of choice for signaling and routing in today's ATM networks. For PNNI to establish connections on a link, a Routing Control Channel (RCC) and a signaling channel are required, each associated with a dedicated virtual channel. The RCC exchanges routing information (e.g. routing tables) between PNNI nodes at either end of the link, while the signaling channel carries ATM signaling messages.

Here, a set of one or more T-LSPs between two PEs represents a single hop PNNI link. PNNI is tunneled through a T-LSP by mapping each RCC and the signaling channel to a PW. The ATM Forum [8] specifies extensions to PNNI to enable it to negotiate the values of PW labels and their mapping to the corresponding Virtual Channel Identifier (VCI) and Virtual Path Identifier (VPI) of the ATM connections, as well as the PW encapsulation mode. While this requires a PNNI protocol stack to be implemented on the PEs, no changes are needed to the existing edge ATM networks or the MPLS core network.

It is a simple method for control plane interworking because there is no need for direct protocol interworking. Furthermore, only a partial mesh of T-LSPs is required across the MPLS network. PNNI can route connections via transit PEs at the edge of the MPLS core, maintaining the same scaling properties and resilience as current ATM networks. Today, PNNI is deployed to rapidly reroute connections from a primary route on which a link fails to an alternative route, thus maximizing the availability of the ATM service. Extended PNNI continues to provide protection in this manner. The high call arrival rates expected on the alternative route have no impact on the MPLS core since they are tunneled over the T-LSP. Extended PNNI thus minimizes the load on core routers, maximizing the network availability and minimizing the impact on other services.

The third form of ATM/MPLS control plane interworking is SPVC/PWE3 (Pseudo Wire Emulation Edge to Edge) interworking, as shown in *Figure 5* [6,10]. This allows ATM SPVCs to be extended between ATM PNNI networks and PVC networks. In *Figure 5*, PNNI signaling and routing are supported on PE1, while PE2 only needs to support the PW control protocol [7]. PNNI routing is terminated on PE1, and PNNI signaling messages are interworked with the PW control protocol. PE1 is configured with the externally reachable addresses at PE2 and advertises these to the ATM network. ATM setup signaling messages that arrive at PE1 from the ATM PNNI network cause a label-mapping message to be sent to PE2, which responds with a PW label-mapping message containing the PW label that PE1 must use for the ATM connection.

Although this allows interworking with non-PNNI enabled PEs, the PW control protocol message cannot carry information such as ATM connection traffic parameters. Therefore it is preferable if the calls originate in the ATM network rather than on PE2. Furthermore, the signaled ATM connection cannot extend beyond PE2, because PE2 does not know what traffic parameters to associate with the connection.

Management Plane Interworking

User and control plane interworking enable services to be carried transparently across the MPLS network. However, technologies such as ATM include a comprehensive set of OAM tools that can rapidly detect and correct defects before they can affect services. These facilities must be maintained when the core network migrates to a common packet technology, such as MPLS. A number of OAM mechanisms are currently being defined for MPLS networks (e.g. MPLS OAM, LSP Ping) and pseudo wires (e.g. Virtual Circuit Connection Verification; VCCV) [11]. Defect indication models for both homogeneous and heterogeneous layer 2 VPN circuits, including a generic architecture for the PE and potential defect locations (*Figure 6*), are described elsewhere [12]. Each PE is modeled as a layer 2 interface to which the ATM, frame relay or Ethernet AC is connected, a PW termination function, an MPLS layer that terminates the transport LSP, and an IP layer providing edge routing on an MPLS network-facing layer 2 interface. Defects can be located in the attached networks, on the PE AC interface, on the PE MPLS interfaces and in the MPLS network itself.

In the homogeneous case, the AC link layer is extended transparently across the MPLS network in a PW, carrying OAM for the native service in-band. It is used for both AC and PW defect indication. This is useful for ATM, which has a comprehensive set of in-band OAM tools, but is not possible for frame relay or Ethernet, which rely on out-of-band defect indications.

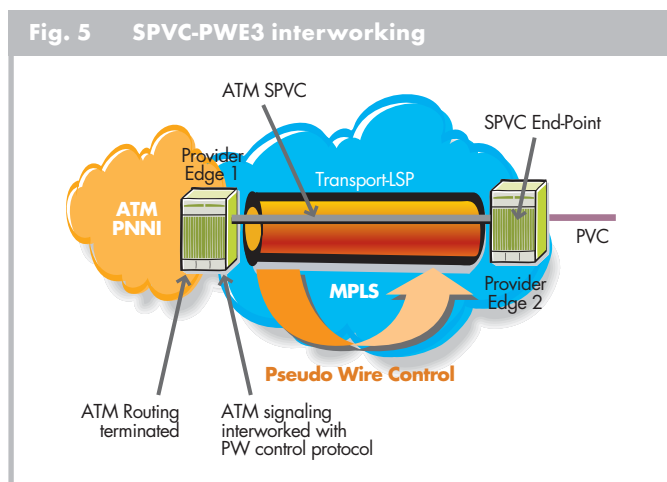


Figure 7 shows an example of defect handling for the homogeneous ATM case. CE2 is informed of a failure of the ATM circuit at (a) as follows: failure of a connection in the ATM network at (a) will result in an ATM Alarm Indication Signal (AIS) OAM cell (1) being sent downstream to PE1. This OAM cell is encapsulated along with other ATM traffic on the PW and sent across the PW to PE2, where it is forwarded on the ATM AC to CE2 to indicate failure of the ATM circuit. CE2 then acknowledges with an ATM Reverse Defect Indicator (RDI), since this is the terminating node in the OAM segment.

In the heterogeneous case, the AC link layer is terminated at the PE. Therefore, native service OAM always terminates at the AC endpoint in a PE. This requires a PW-specific defect indication, such as out-of-band PW status signaling [7]. In-band ATM OAM can still be used where the PW type is ATM (e.g. for frame relay - ATM multi-service interworking).

Figure 8 illustrates how defect notifications are propagated in an ATM-Ethernet heterogeneous layer 2 VPN circuit. An ATM AIS is sent to PE1 following a failure of the ATM network at (a). However, since there is no equivalent in-band Ethernet OAM alarm, a PW status signaling message [7] indicating a "down" state is sent between PE1 and PE2. This is translated into an ATM AIS on the ATM AC to CE2. Note that since the ATM AIS is not sent beyond PE1, PE1 terminates the OAM segment and responds with an ATM RDI to CE1.

Conclusion

Service providers are deploying MPLS to support new IP and Ethernet based VPN services, as well as to improve the management of their IP infrastructures. However, existing services, such as ATM and frame relay, account for a high proportion of data service revenues,

Fig. 6 Defect locations in network and service interworking

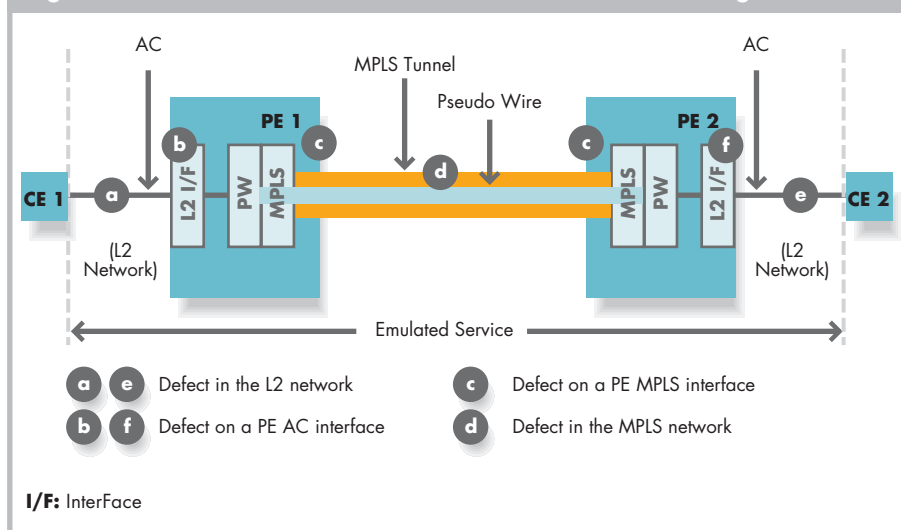


Fig. 7 Defect notification propagation for a homogeneous layer 2 VPN circuit

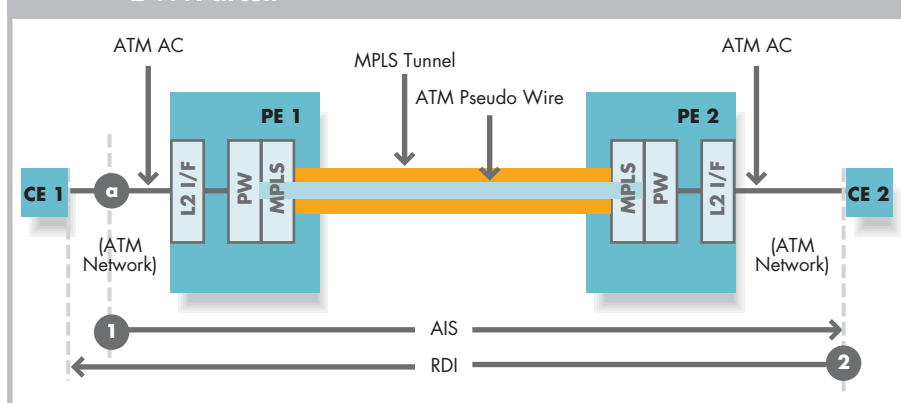
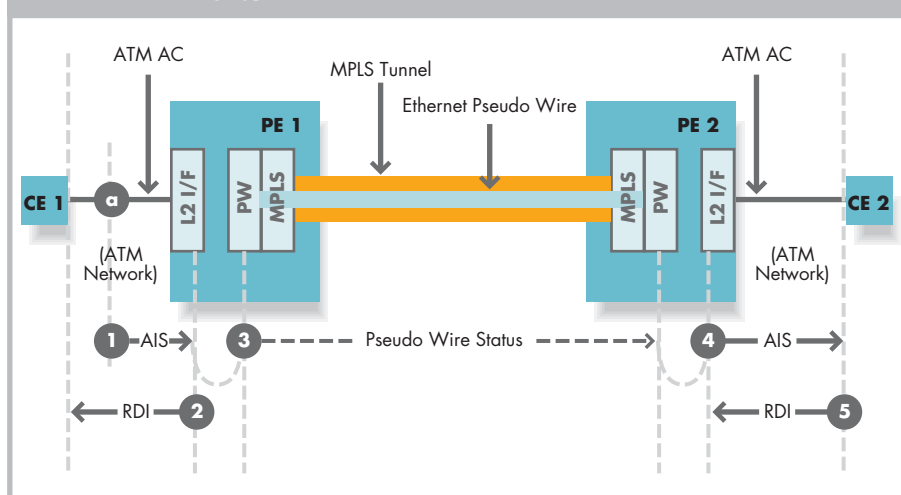


Fig. 8 Defect notification propagation for a heterogeneous layer 2 VPN circuit



so carriers are looking to maintain these alongside the new services in order to maximize service breadth while minimizing risk.

New developments in network and service interworking promise to allow both traditional and new services to be delivered over a converged packet infrastructure, thus controlling the operational and capital costs associated with a comprehensive service portfolio. However, this vision must be matched with an understanding of the interworking requirements and capabilities at the user, control and management planes. Control and user plane transparency must be matched with the ability to detect and diagnose faults in a timely manner.

Standardization bodies, such as the IETF, the MPLS & Frame Relay Alliance and the ATM Forum, are defining transparent interworking between new MPLS networks and traditional services, as well as developing new MPLS-based services such as VPLS. Alcatel has taken a lead in developing standards and implementations for the architecture and user plane, interworking with PNNI, and fault management interworking. These are required to realize the financial and operational benefits of a converged infrastructure, minimizing the cost of its evolution, while simultaneously retaining and expanding the existing customer base.

References

- [1] IETF PWE3: "PWE3 Architecture", *draft-ietf-pwe3-arch-07.txt*, March 2003.
- [2] ATM Forum Technical Committee: "ATM-MPLS Network Interworking", *AF-AIC-0178.001*, August 2003.

- [3] IETF PWE3: "Encapsulation Methods for Transport of ATM Over IP and MPLS Networks", *draft-ietf-pwe3-atm-encap-06.txt*, July 2004.
- [4] Frame Relay Forum: "Frame Relay / ATM PVC Service Interworking Implementation Agreement", *FRF.8.2*, February 2004.
- [5] M. Bocci, J. Guillet: "ATM in MPLS-Based Converged Core Data Networks", *IEEE Communications Magazine*, January 2003.
- [6] D. Watkinson et al: "Framework for PNNI to PSN Interworking", *draft-watkinson-l2vpn-pnni-psn-framework-01.txt; Internet Draft*, July 2004.
- [7] IETF PWE3: "Pseudowire Setup and Maintenance using LDP", *draft-ietf-pwe3-control-protocol-08.txt*, July 2004.
- [8] ATM Forum Technical Committee: "ATM-MPLS Network Interworking Signaling Specification, Version 1.0", *AF-CS-0197.000*, August 2003.
- [8] M. Bocci et al: "Signaling Interworking for Asynchronous Transfer Mode Virtual Private Wire Service", *draft-bocci-l2vpn-pnni-mpls-iw-01*, July 2004.
- [9] Swallow et al: "Soft Permanent Virtual Circuit Interworking between PWE3 and ATM", *draft-swallow-pwe3-spvc-iw-01.txt; Internet Draft*, July 2004.
- [10] M. Aïssaoui, D. Watkinson, M. Bocci: "OAM in a Converged IP/MPLS Network", *Alcatel Telecommunications Review*, 4th Quarter 2004, pp 464-469 (this issue).
- [11] M. Aïssaoui et al: "OAM Procedures for VPWS Interworking", *draft-aissaoui-l2vpn-vpws-iw-oam-01.txt; Internet Draft*, July 2004.



Matthew Bocci is Director, Technology and Standards, in the Internet Protocol Division, Europe and South Regional Support Center, London, UK. He is a Regular Member of the Alcatel Technical Academy. (Matthew.Bocci@alcatel.co.uk)



Mustapha Aïssaoui is a member of the Product Line Management in the Internet Protocol Division MultiService WAN Product Group, Kanata, Canada. (Mustapha.Aissaoui@alcatel.com)



David Watkinson is Senior IP/MPLS Architect for the Alcatel 7670 RSP in the Internet Protocol Division MultiService WAN Product Group, Kanata, Canada. He is a Regular Member of the Alcatel Technical Academy. (David.Watkinson@alcatel.com)

Abbreviations

AC	Attachment Circuit
AAL5	ATM Adaptation Layer Type 5
AIS	Alarm Indication Signal
ATM	Asynchronous Transfer Mode
CE	Customer Edge
EXP	EXPerimental bits
IETF	Internet Engineering Task Force
I/F	InterFace
IP	Internet Protocol
IWF	InterWorking Function
LAN	Local Area Network
LSP	Label Switched Path
LSR	Label Switching Router
MPLS	Multi Protocol Label Switching
OAM	Operations, Administration and Maintenance
PDU	Protocol Data Unit
PE	Provider Edge
PNNI	Private Network - Network Interface
PVC	Permanent Virtual Connection
PW	Pseudo Wire
PWE3	Pseudo Wire Emulation Edge to Edge
QoS	Quality of Service
RCC	Routing Control Channel
RDI	Reverse Defect Indicator
SDU	Service Data Unit
SLA	Service Level Agreement
SPVC	Soft Permanent Virtual Connection
SVC	Switched Virtual Connection
T-LSP	Transport LSP
VCCV	Virtual Circuit Connection Verification
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network

