IP/MPLS VPN Service Network Overview

Telecommunication operators must constantly evolve their networks to meet the needs of their customers. Building a converged, high performance, highly available, and highly flexible network to provide multiple services in a cost efficient way is the goal for today's providers. The new generation of IP/MPLS VPN service-oriented networks has become the operators' best choice to reach this goal.

Building Converged Service Networks with IP/MPLS VPN Technology

1

Multi Protocol Label Switching (MPLS) and Virtual Private Network (VPN) technologies provide features that help service providers meet the evolving needs of their customers. These technologies are essential for building the converged service networks required in today's market.

Chapter Objectives

- Identify the new trends and demands for a service provider's backbone network
- Review the evolution of MPLS technology
- Describe the innovation of multi-service VPN

This chapter briefly reviews traditional networks with legacy technologies and their limitations, and shows how the innovations of MPLS and VPN technologies overcome these limitations. It also presents the benefits of using an IP/MPLS VPN service architecture.

1.1 The Increasing Demands on Service Provider Networks

Service provider networks must evolve to keep pace with the changing times. Service providers are often classified by how much of the regional access infrastructure they own, versus how much they must contract from other providers:

- **Tier 1 operators** — The top one or two providers in a country who typically own the access infrastructure (copper or fiber) within their serving region. Tier 1 service providers are usually the first to establish infrastructures within the region — the incumbent operators.
- **Tier 2 or Tier 3 operators** — Providers that may either use the Tier 1 operator's access infrastructure or build its own infrastructure in some service areas. Tier 2 providers use a mix of their own infrastructure and some infrastructure from Tier 1 providers, while Tier 3 providers rely entirely on agreements to use infrastructure from other providers. These providers typically emerge as competitors to the already established Tier 1 providers, and are thus at a disadvantage in competing with the incumbent providers for market control.

Service providers may also be classified according to the types of services they offer to their end-customers:

- **Telco** — Traditionally offering voice services as well as business services
- **Internet Service Provider (ISP)** — Offering Internet access for residential and business customers
- **VPN Service Provider/Ethernet Service Provider** — Offering business VPN services
- **Cable Multi-System Operator (MSO)** — Offering residential and business services

An operator may offer some or all of these services to their end-customers.

Both residential (consumer) and enterprise (business) customers of service providers constantly demand new services and innovations from their service providers. Traditional Leased Line, Frame-Relay (FR), and Asynchronous Transfer Mode (ATM)

based services are characteristic of organizations that manage their own enterprise networks (with their own IT teams), but those enterprises must purchase the connectivity infrastructure (typically point-to-point leased lines or FR/ATM Permanent Virtual Connections) from a service provider. Driven by enterprise business goals and geared toward focusing on core competencies and cost reduction, enterprises have begun looking to service providers for managed connectivity solutions.

Enterprises have also been demanding more in terms of bandwidth speeds for connectivity. The old "80/20 rule" (80% of the traffic stays within the local site, and 20% of the traffic is between remote sites) is no longer valid. Because many enterprises have consolidated their data centers to a few sites, the need for higher-speed remote connectivity has become extremely important to enterprise IT managers. In addition, enterprises are now in the process of implementing bandwidth-intensive applications like video conferencing, web conferencing, and electronic image sharing across a wide area, thus prompting a need for additional bandwidth in their Wide Area Networks (WANs).

Residential services are also evolving from dial-up Internet connectivity to broadband connectivity. Services for residential customers are evolving to include triple- or quad-play services that include voice, Video on Demand (VoD), broadcast television, and Internet access.

Traditionally a service provider has separate networks for offering voice and data services. Within a data network, a traditional service provider would typically have separate networks for offering Leased Line-, FR-, and ATM-based services for business customers and a separate network offering Internet-based services (Internet access and Internet-based secure connectivity) for residential and business customers. In residential areas, TV content for consumers is most often delivered by MSOs, who have their own dedicated infrastructure (mostly cable plants). Enterprises usually use Ethernet switches and IP routers to build their LANs and purchase Leased Line services from operators to connect their remote locations.

Given the ever-changing landscape of customer demands, service provider networks must keep pace by staying competitive while increasing profitability. It is evident that the approach of building separate networks is not cost-effective when a service provider must offer multiple services. The ideal way to approach network design is a solution wherein multiple services can be converged on a single network infrastructure. This is why MPLS as a technology for service provider networks has gained rapid momentum in the marketplace.

The most obvious trend is the fast growth of IP and Ethernet traffic in the network. Because of the boom of the Internet, and the invention of Gigabit Ethernet, IP/Ethernet traffic is now dominant in telecommunication networks. Residential customers require faster Internet access services and better IP service quality to support Voice over IP (VoIP). Enterprise customers are conducting more and more of their business electronically across geographically separated locations. Many bandwidth-intensive and time-sensitive IP-based applications are widely used for business-critical missions. IP data is growing in strategic importance in wireless networks. Mobile users are keen for rich IP-based multimedia services. Service providers also want to deliver television content over IPTV applications, which require a network throughput with very high bandwidth and low latency. It's clear that building a network optimal for IP/Ethernet traffic delivery is crucial to service providers.

Because enterprises are now starting to use more and more IP/Ethernet-based applications, they require their IT infrastructures to have high throughput, and to be reliable, secure, and cost-efficient. This generates a great demand for the service providers to provide VPN. VPN allows the service provider to deliver services to different customers using the same service delivery backbone network, while isolating each customer using virtual service instances to ensure privacy and security. During the past two decades, there were already many enterprises using the routed RFC2547bis VPN to achieve intranet connectivity. Now, with the fast growth of Ethernet technology, more and more business customers require bridged Layer 2 Ethernet VPN service. Layer 2 VPN gives the customers full control of their routing domains and fewer peering complications with service providers.

Service providers also look for network solutions that consolidate voice, data, and video services into one network infrastructure and allow them to serve residential and business customers from the same network. The network must be cost-efficient and robust. The network must also be capable of providing different Quality of Service (QoS) on the service provided to conform to different Service Level Agreements (SLAs).

With these new trends and demands, service providers intend to transition their networks to IP/MPLS core networks, providing various VPN services to their customers.

1.2 MPLS Overview

Multi Protocol Label Switching is a label-switching mechanism used by MPLS-capable routers or switches to exchange traffic. In the control plane, the MPLS-capable

devices assign labels to be used for certain types of traffic and distribute labels through certain label distribution protocols. Each device distributes locally assigned labels to other MPLS devices and receives label distribution information from other devices. Each device builds a Label Information Base (LIB) that stores the label information. In the data plane, each device performs MPLS encapsulation on data traffic before sending it to other MPLS devices. When an MPLS device receives MPLS-encapsulated traffic, the device makes forwarding decisions based on the MPLS label value in the MPLS encapsulation header. In MPLS data encapsulation, the MPLS header (32 bits long, containing a 20-bit numerical value used as the label value) is inserted between the Layer 2 header and the Layer 3 header of the data to be encapsulated. Therefore, MPLS is sometimes referred as a *Layer 2.5 protocol*, and the MPLS header is sometimes referred to as the *shim header*.

Before MPLS devices can forward MPLS-encapsulated traffic to each other, MPLS label distribution in the control plane must be completed. When exchanging label information, each MPLS device stores the label, as well as the label mapping information for the type of traffic that uses each label. All traffic that uses the same label is referred to as a *Forwarding Equivalent Class* (FEC). The label distribution process distributes the FEC–Label mapping information among MPLS devices. Therefore, MPLS devices form a Label Switched Path (LSP) for each FEC. The LSP is an end-to-end *connection* for traffic belonging to the same FEC to be forwarded. MPLS builds a connection-oriented path in a connectionless network.

MPLS was first introduced to improve Layer 3 routing performance of regular IP routers. For an MPLS-capable router or Layer 3 switch, MPLS label swapping is less expensive than routing IP packets. In a routed IP network, the IP packets are routed from their source to their destination hop-by-hop. When each router routes an IP packet, the router removes the Layer 2 header (usually an Ethernet header), then checks the IP header for the destination IP address. The router then must perform a lookup in its routing table to find the IP address of the next-hop interface and the egress interface's Layer 2 encapsulation information. After the next-hop lookup is completed, the router rewrites the packet by adding the new Layer 2 encapsulation header to the packet and then forwards the packet to the next-hop interface. This procedure is performed for every IP packet at every hop. With the introduction of MPLS, the routers can build MPLS LSPs for each FEC. All traffic belonging to the same FEC is MPLS-label–switched to its destination rather than routed. When a Label Switched Router (LSR) performs MPLS switching on an MPLS-encapsulated packet, the MPLS label-swapping operation is much simpler. Therefore, the IP destination lookup process

is replaced by the relatively cheaper label-swapping process. Using MPLS switching to replace IP routing is sometime referred to as a *routing shortcut*.

Furthermore, Border Gateway Protocol (BGP) can be removed from the core of the network because the LSR routers in the core of the network do not have to route these packets. As long as the MPLS label distribution process builds the LSP for each router in the core to reach all edge routers that have BGP peerings with routers outside the Autonomous System (AS), traffic across the core network can be MPLS-switched rather than IP-routed. The core router uses the MPLS label to switch the traffic to the correct edge router. BGP full mesh within the AS can be removed. Only the edge routers need to have BGP peering among each other. Using MPLS switching to remove BGP full mesh from the core network to route Internet traffic is sometimes referred to as a *BGP shortcut*. The label distribution process used by traditional MPLS-capable devices is in most cases the Label Distribution Protocol (LDP).

1.3 The MPLS Value Proposition

MPLS has evolved substantially since its early days of deployment. The reasons for using MPLS in a network have also changed. MPLS is no longer used to provide an IP routing shortcut. The two biggest changes in the MPLS technology are:

- Resource Reservation Protocol (RSVP) is extended to support MPLS label distribution — RSVP-TE. RSVP-TE (the *TE* stands for traffic engineering) brings many traffic engineering features and resiliency features to MPLS tunneling technology.
- Pseudowire (PW)-based MPLS L2VPN is implemented in many vendors' MPLS-capable routers and switches.

With these evolutions in MPLS technology, MPLS is now widely deployed in the backbone networks of service providers to provide VPN services to their customers.

The introduction of RSVP-TE into MPLS label distribution gives MPLS outstanding flexibility and reliability that the traditional routed or switched network cannot have:

- MPLS provides traffic engineering capabilities to control the data forwarding path in the network. Using RSVP-TE, MPLS routers can signal an explicitly routed LSP. The operator can manually specify the path and the hops along the path for the LSP to travel end-to-end. Therefore, operators can manipulate the data traffic paths in the network, as follows:
    - In an IP-only network, packets traveling from source nodes to destination nodes use a path that is determined by routing information

computed by IP routers. An IP-only network offers little flexibility for providing alternate paths for traffic flow. An MPLS-based network supports traffic engineering whereby an MPLS path (logical connection) can be defined to use network links that are different from the normal path taken by IP packets. This helps to better utilize links within an enterprise network.

    - With the help of the traffic engineering extensions of Open Shortest Path First (OSPF) and IS-IS, RSVP-TE allows the use of Constraint Shortest Path First (CSPF)-based MPLS tunnel path calculation. When performing path calculation, CSPF can consider criteria other than the Interior Gateway Protocols (IGP) routing metric, such as the link's bandwidth reservation and the administrative group membership (link-coloring).

- MPLS provides outstanding reroute performance. Network infrastructures based on FR/ATM or legacy Ethernet cannot offer quick convergence during failover.MPLS provides outstanding reroute performance using mechanisms such as Secondary (backup) LSP and Fast Reroute (FRR) that can deliver reroute times in the millisecond range:
    - **Secondary LSP** — RSVP-TE supports the concept of *LSP and LSP-Path*. It allows several (up to eight) LSP-Paths to be provisioned within the same LSP. In normal circumstances, the primary LSP-Path actively forwards traffic; if the primary LSP-Path fails, one of the secondary LSP-Paths takes over the traffic. When a hot-standby secondary LSP-Path is provisioned, the failover performance is in the tens of milliseconds range.
    - **FRR** — When using RSVP-TE to signal LSP, all routers can be aware of the entire path the LSP traverses. Therefore, each router can signal a protection LSP to take a path away from the potential failure point. If network failure happens, the MPLS router closest to the failure uses the pre-signaled protection path to protect the LSP. This is called *MPLS FRR*. FRR can provide tens of milliseconds failover time after a failure is detected.
- The pseudowire-based IP/MPLS VPN implementation makes it possible to take full advantage of the flexibility provided by MPLS. The new VPN model decouples native service processing from VPN encapsulation and allows services with different characteristics to share the same IP/MPLS backbone. The customer

service-specific service access entities are in charge of providing native format traffic to meet the customer's requirements, and the VPN service network entities are in charge of performing VPN encapsulation and de-encapsulation to transport the service across the network backbone.

Resiliency features such as pseudowire switching and pseudowire redundancy ensure end-to-end service delivery with the desired quality.

With the MPLS enhancement and the new pseudowire-based VPN service, the service provider can now deploy different types of services for many customers in a single converged backbone network using IP/MPLS technology. The IP/MPLS VPN network has the following advantages:

- **Cost Efficiency** — It eliminates the requirement for service providers to build separate networks for different types of services. All services are shared in the same backbone infrastructure. Using an IP/MPLS network with Gigabit Ethernet or 10 Gigabit Ethernet Layer 2 infrastructure significantly reduces the cost compared to the legacy technologies like ATM and FR.
- **Flexibility** — All MPLS pseudowire-based VPN services use a common service architecture, differing only in the customer-facing attachment circuit. When a new type of service is implemented, it can be smoothly deployed into the existing IP/MPLS backbone by simply adding the new type of access interface in the provider edge (PE) service router. The TE capability provided by IGP-TE and CSPF allows the operator to easily control the service traffic's forwarding paths in the core network.
- **Reliability** — The pseudowires used by VPN PE routers and the MPLS transport tunnel LSP support both redundancy and quick failover. The service architecture allows the operator to multi-home services to more than one PE router, to achieve service-peering redundancy. With the addition of the MPLS resiliency features that have quick failover, the service network can be built with high availability.
- **Scalability** — IP/MPLS VPN service is highly scalable. The IP/MPLS VPN service architecture allows the core routers (P routers) to perform MPLS switching for service traffic without being aware of each service instance. Only the PE routers in the edge of the backbone network are aware of each service instance. Only the PE routers with customer circuits attached are involved in service provisioning. All service instances sharing the same PE router are isolated by VPN encapsulation.

LDP is one of the protocols MPLS uses to signal LSP. With LDP, the MPLS router distributes labels and establishes LSPs automatically. LDP distributes labels mapped with IP prefixes; therefore, its convergence performance is dependent on the underlying routing protocol. The introduction of RSVP-TE into MPLS LSP signaling brings significant improvement to the flexibility, reliability, and performance of the IP/MPLS network's service transport mechanism. With an RSVP-TE–signaled LSP transport tunnel, an IP network can now provide carrier-level convergence performance by using resiliency features such as FRR and Secondary LSP.

The newly enhanced MPLS technology allows the operator to deliver traffic flows for many customers using many different types of services in a single converged network. It is now the new WAN backbone technology.

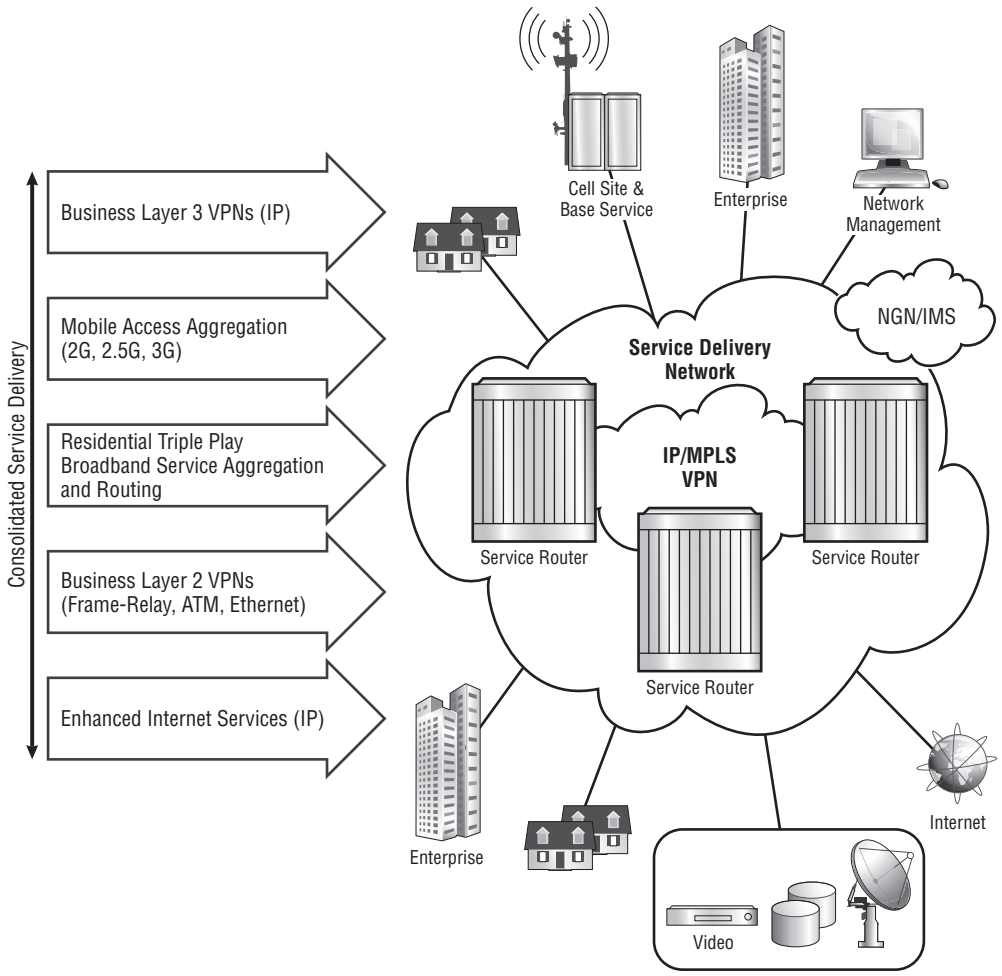
1.4 MPLS Enables Converged Multi-Service Networks

For decades, computer networks have been generally categorized as LAN, MAN, and WAN. Each type of network has its own architecture and traffic delivery mechanism. Their speeds, costs, and reliability differ too. Different types of service providers use different types of networks to provide the services for these networks. With the technology innovation and the growth of the customer demands, the requirements for networking are also changing constantly:

- The wide deployment of cost-efficient and high-throughput Ethernet switches and small IP routers brought the first wave of networking evolution. Many computers can be connected by these LAN-oriented networking devices and gain great speed to run time-sensitive applications or traffic-intense applications.
- The invention of the Internet brought the second wave of networking evolution. Computer networks all over the world can be connected by the shared public Internet backbone. This wave brought the demand for a high-performance and highly reliable backbone Internet router.
- Now, the third wave of networking evolution has arrived. With the invention of VoIP, IPTV, and other IP-based multimedia applications, ISPs not only provide access to the Internet, but they also want to provide these services with additional profit over their backbone infrastructure. These services require bandwidth and global reachability, as well as a guaranteed end-to-end QoS. To achieve this, the concept of *service router* is used. *Service routers* allocate their resources according to the requirements of different services and deliver the services with the required quality.

Therefore, a converged multi-service network is desired by service providers to meet the new requirements. Figure 1.1 illustrates such a converged network with multiple services.

Figure 1.1 Converged Multi-Service Network



In Figure 1.1, the service delivery network provides multiple services in a single backbone network that contains service routers. The service delivery network provides various services to many enterprises and residential customers. Such a network is based on the new evolved IP/MPLS VPN service technology.

1.5 MPLS-Enabled Business VPN Services

Nowadays, more new applications running in residential and enterprise networks generate new demands for the telecommunications backbone networks:

- **Complex L3 VPN** — Many enterprise customers require VPN services with *complex* connectivity. Simply connecting all customer routers is not adequate. Layer 3 VPN is also referred to as *Virtual Private Routed Network* (VPRN). Customers require different VPN topologies such as:
    - **Extranet** — Some enterprises want to share part of their networks with partners to improve productivity while isolating other parts of their networks.
    - **Hub-Spoke VPN** — Many customers require their branch offices to be connected with their headquarters and want the traffic to be forced through the headquarters' firewall.
    - **Overlay VPN** — Customers may want to have Internet access through some of their sites while isolating the rest of their network from the Internet.
- **L2 VPN: Virtual Private LAN Service (VPLS) and Virtual Leased Line (VLL)** — Many customers want to take advantage of the simplicity of Layer 2 peering with the service provider. They want to purchase Layer 2 connectivity services (point-to-point or point-to-multipoint) from the service provider, while handling their own Layer 3 routing. Service providers also like the fact that they do not need to deal with Layer 3 routing peering and isolation with different customers, and can focus only on providing Layer 2 reachability. With the introduction of Gigabit Ethernet and 10G Ethernet in customer networks and backbone networks, VPLS and Ethernet VLL services have become very popular. VLL is also referred to as Virtual Private Wire Service (VPWS).
- **MPLS-Enabled IPTV Infrastructure** — With the new generation of IPTV solutions, delivering television content (regular definition and high definition) over IP networks has become possible and profitable. Many service providers want to use their IP backbone network to deliver TV content to compete with traditional cable service providers. Delivering IPTV content requires the backbone network to have large bandwidth and promising service quality.
- **MPLS-Enabled Mobile Infrastructure and Mobile Backhauling** — The new generation of the mobile networks provides both voice and high-bandwidth

data service through cellular services. Mobile service providers are looking for a cost-efficient and optimal solution of using a converged network to deliver both voice and data services in backbone networks.

- **Improved Access Technologies** — The significant growth of access technologies provides more bandwidth to the end subscribers. Today's Digital Subscriber Line (DSL) technology and Passive Optical Network (PON) technology can give the end-user 10-Mbps, 100-Mbps, or even higher throughput. Bandwidth-intensive applications such as IPTV, Personal TV, faster download, and online gaming can be deployed end-to-end across a backbone network.

All the above changes and new demands challenge service providers to build a high-throughput, highly reliable, and cost-efficient converged backbone network to meet the requirements of different customers. Also, service providers are looking for more revenue-generating services to sell to the customers rather than selling the *big fat pipe*. The boundary between carriers and content providers has become ambiguous. Cable TV providers are now providing Internet access and VoIP telephony services. ISPs are now providing TV content to their customers through IPTV and are using DSL and PON technology to provide Internet and voice services. Cellular providers are also providing mobile data services and delivering TV content to cellular phones thorough 2G or 3G technologies along with the mobile voice services.

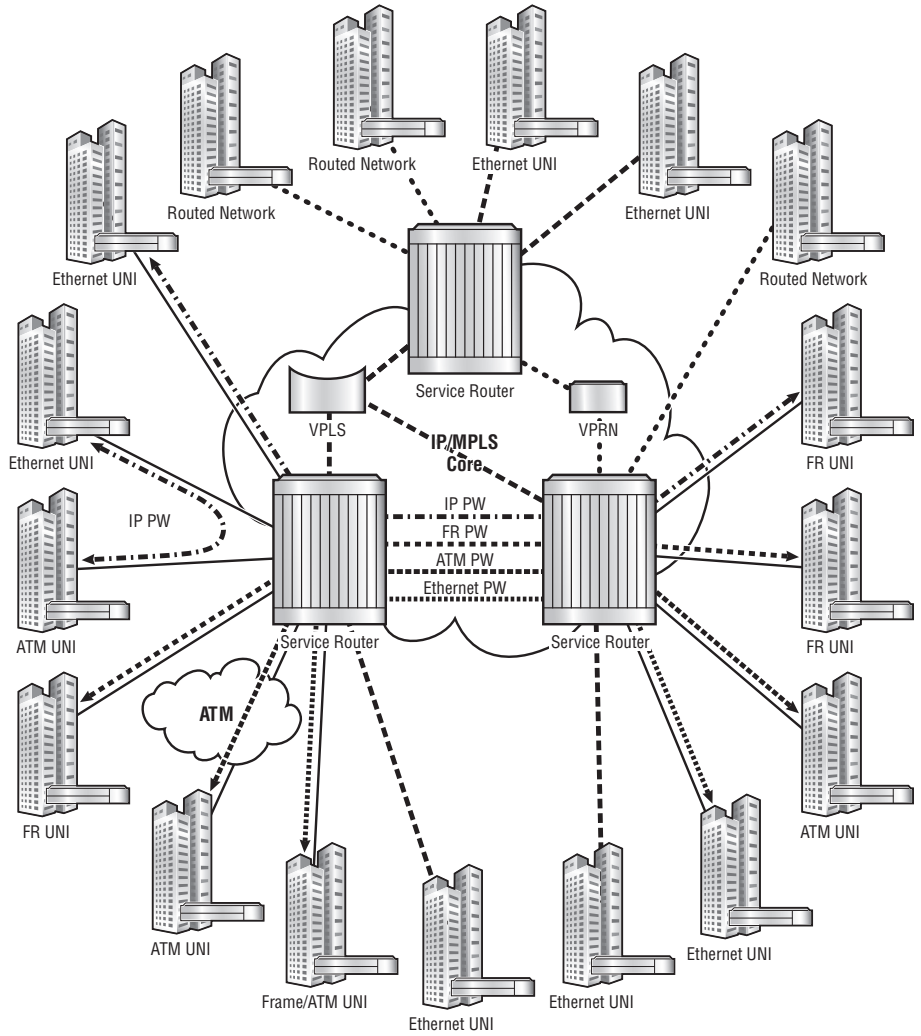
The evolution of IP/MPLS VPN technology provides a solution for all of these types of service providers. With IP/MPLS VPN technology, all types of services can be provided in a single converged MPLS service backbone network, as follows:

- The high-throughput backbone (usually connected with Gigabit Ethernet or 10 Gigabit Ethernet) provides enough bandwidth to deliver bandwidth-demanding applications such as IPTV.
- The flexible IP/MPLS VPN technology allows multiple services such as voice, data, broadcast TV, mobile backhauling, and ATM/FR circuits to be provisioned in a single network.
- The advanced QoS functions allow differentiation among different types of services and customers and treat the different types of traffic flows in their network based on their unique characteristics. Delivering guaranteed service quality to fulfill SLAs while using available resources in the network to serve statistically multiplexed subscribers can be achieved simultaneously.

- The highly reliable service routing engine provides hot redundancy in the control plane. MPLS resiliency provides carrier-level convergence performance to protect services from network failures. Service outages can be minimized.

Figure 1.2 illustrates an IP/MPLS VPN service network.

Figure 1.2 An IP/MPLS VPN Service Network



The invention and implementation of the pseudowire-based IP/MPLS VPN solution gives service providers a scalable and secure approach to providing services to multiple customers using the same backbone network while efficiently isolating customer traffic.

- The pseudowire-based VPN model decouples the role of the customer-facing edge routers (Provider Edge, or PE, routers) and the role of backbone-transiting routers (Provider, or P, routers). MPLS pseudowires connect PE routers to customer-facing service instances. The MPLS backbone network only transits pseudowire-encapsulated VPN traffic end-to-end, hiding the details of the core network topology from the service. Therefore, the service-aware PE router can be focused on providing access to customer devices, multiplexing and de-multiplexing traffic from multiple services, and making VPN forwarding decisions. The P routers are in charge of providing highly available, high-throughput *forwarding pipes* with guaranteed QoS.
- The pseudowire-based IP/MPLS VPN model provides different types of services using the same IP/MPLS backbone. These services include:
    - **VLL** — A highly scalable point-to-point piping service that carries customer traffic between two customer sites. VLL services support many legacy access technologies, such as ATM, FR, Ethernet, and Circuit Emulation Service (CES).
    - **VPLS** — A multipoint-to-multipoint Ethernet bridging service that bridges customer Ethernet traffic among geographically separated locations.
    - **VPRN** — A multipoint-to-multipoint IP routing service that routes customer IP traffic among different sites and exchanges customer routes among these sites. VPRN services can provide various service topologies such as Intranet, Extranet, Overlay VPN, or Hub-Spoke VPN.
- The pseudowire-based VPN model unifies the service deployment architecture in the network. Different types of VPN services for different customers use the same VPN infrastructure: Service instances in each customer-facing PE router are connected by the end-to-end pseudowire(s), and PE routers are connected to each other by Service Distribution Paths (SDPs) using Generic Routing Encapsulation (GRE) or MPLS tunneling. Different types of services share the

same MPLS backbone with a similar core-facing configuration. Services differ only in Service Access Point (SAP) configuration in the service instances of local PE routers. This unified service deployment module makes the backbone network easier to maintain and expand.

- The pseudowire-based IP/MPLS VPN services are standardized and supported by multiple vendors, and therefore multi-vendor interoperability can be achieved.

Summary

Traditional telecommunications service providers build different network infrastructures to provide different types of services to different customers. These separate network infrastructures create high operational expenses and capital expenses. Different types of networks are incompatible with each other, and the resources cannot be shared.

New applications such as IPTV and the fast growth of Internet applications such as voice, video, and gaming demand more bandwidth and service quality from the service provider. Service providers want to provide multiple services to maximize their revenue. Converged networks with multi-service capability, high performance, high availability and cost efficiency are required to achieve these goals.

The innovation of pseudowire-based IP/MPLS VPN technology provides a solution to the service providers. By implementing an IP/MPLS VPN service routing backbone network, service providers can deploy different types of services (e.g., L2VPN, L3VPN, Internet Routing, Triple Play, and VoIP) over a converged IP/MPLS backbone network.

- IP/MPLS service routing with high-throughput Ethernet connections provides a cost-efficient solution for the deployment of a scaled network.
- IP/MPLS VPN service architecture makes it possible to deliver multiple services in a single backbone network, and the uniform service architecture reduces the operation and management overhead of the network.
- MPLS resiliency features ensure that the network has outstanding convergence performance. Minimum service outages during network failures are guaranteed.

These innovations allow service providers to meet the evolving needs of their customers by providing multiple services using a single converged network.