Technical White Paper for Seamless MPLS Networking

HUAWEI

Contents

Technical White Paper for Seamless MPLS Networking

Keywords:
Seamless; MPLS; Scalability; Reliability; OAM; LDP DoD; PWE3

Abstract:
Seamless MPLS networking refers to the formation of a unified IP/MPLS control plane for all the IP devices managed by operators, including access (fixed/mobile), convergence, and backbone devices. The Seamless MPLS networking architecture greatly reduces cooperation between different network layers when services are deployed, allows operators to quickly provide services, and lowers deployment costs. Reliability/OAM detection can be deployed easily through the end to end IP/MPLS control plane and unified networking technology. This document describes the background, challenges, solution, and application scenarios of the Seamless MPLS.

1 Preface

With the wide application of Multiprotocol Label Switching (MPLS) technology, operators establish Metropolis Area Networks (MANs) and backbone networks for the bearing of integrated services by using the MPLS-based L3VPN/L2VPN solution. Generally, services and users are identified through 802.1Q or 802.1ad between access devices, MAN, and backbone networks, requiring the static configuration of interfaces between each layer. In seamless networking, the end-to-end IP/MPLS networking of all data devices managed by operators is realized, including access (fixed/mobile), convergence, and backbone devices. This is achieved by eliminating the existing 802.1Q/802.1ad interface between devices on each layer in the existing network. Thus, each layer can implement dynamic interaction, which is called 'end-to-end big networking'. This chapter describes the problems with existing networking architecture, and the benefits of Seamless MPLS architecture.

1.1 Metro Bearer Technology in the TR101 Architecture

The TR101 in the DSL forum draft specifies the DSL aggregation model in Ethernet mode.

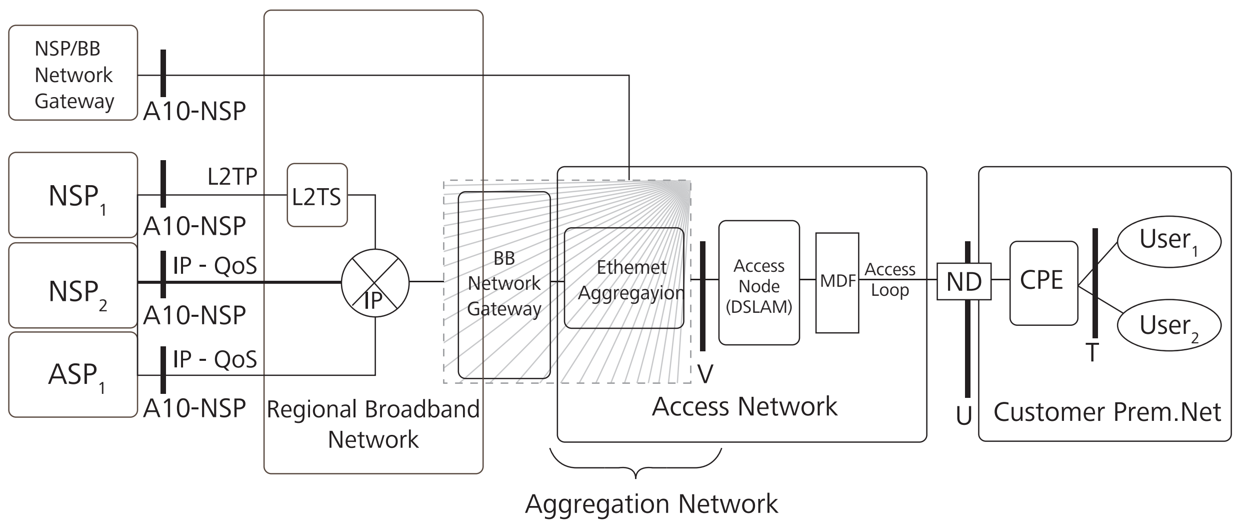

Figure 1 TR101 Ethernet DSL aggregation model

The model defines the V interface between the access node and Ethernet convergence network/node to identify different DSL ports for services and user access through the 2-layer TAG of 802.1ad (QinQ).

The mainstream networking technologies of the metro convergence network include Ethernet enhanced technology (QinQ, PBB), MPLS bearer, and L3 Hybrid. The Ethernet enhanced modes, such as QinQ and PBB, effectively improve network reliability and service flexibility. The MPLS bearer mode is one of the mainstream bearer technologies of the Ethernet convergence network, as it facilitates VLAN scalability and reliability. In L3 Hybrid mode, services are classified into edge processing services and transparently transmitted services, according to service features. For the edge processing services, the IP edge is located in the edge convergence node. Transparently transmitted services are sent to the specified POP point through the MPLS pipe. The Hybrid mode can adapt to service development requirements in the future.

In these metro convergence network technologies, the V interface specified in TR101 architecture is used. The following figure shows the bearer modes of services in the network position in MPLS mode and L3 hybrid mode.

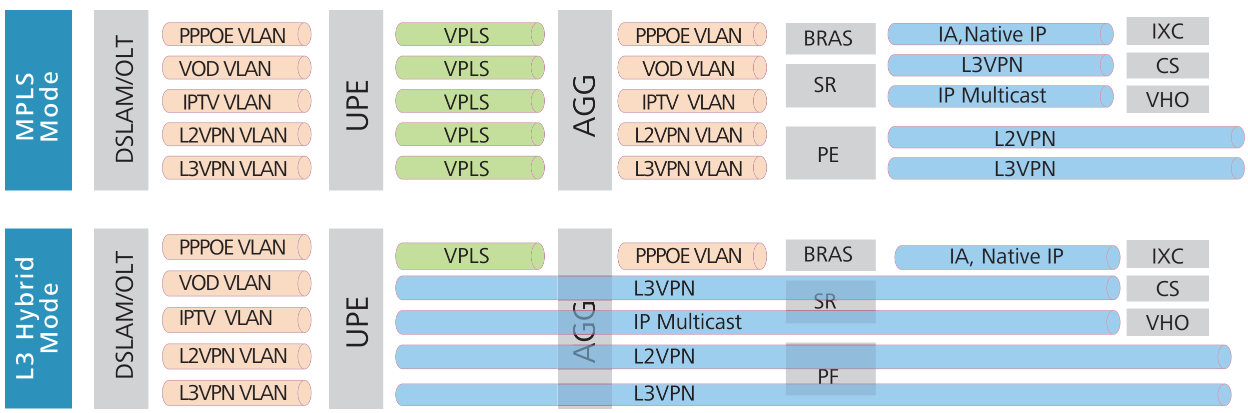

Figure 2 Service bearer model of the TR101 architecture

With the continuous development of user access requirements and services, network operators must meet these new requirements. TR101 architecture cannot meet these new requirements.

1. For FTTX access, the wholesale service mode of the ULL cannot be maintained. POP point locations vary with the scale of alternative operators. Therefore, incumbent operators must provide a more flexible connection capability at the access node (AN). In this case, the AN must identify alternative operators, services, and users.
   For TR101 architecture, the complicated VLAN planning is required on the V interface due to the limitation of the VLAN space. In a typical metro MPLS networking scenario, the VLAN must be configured in more nodes (AN, UPE, AGG, and PE) of incumbent operators if the POP point location of alternative operators is not in this local MAN.

2. Connecting the inter-metro enterprise private line is required due to the quick development of the enterprise Ethernet private line.
   Multi-point static configuration in the TR101 architecture is required. The inter-metro Ethernet private line can be provided through cooperation between the management entities on each layer.

3. According to Fixed-Mobile Convergence (FMC) requirements, the AN must be accessed to the mobile bearer services to connect the base station and mobile gateway, including ATM, TDM, and the Ethernet.

4. The function of the IP bearer network is more important due to service access density and the migration of telecom services. Users require greater access reliability.

   In TR101 architecture, the networking technologies on each layer are not unified and different reliability solutions are used. Cooperation and interaction are complicated without a mature standard. Device manufacturers provide solutions of different reliability and the interoperability problem cannot be solved.

1.2 Introduction of Seamless MPLS Networking Technologies

With Seamless MPLS architecture, the entire network uses unified IP/MPLS networking technology, with an end-to-end control plane. As a result, the V interface between the AN and Ethernet convergence is eliminated. The above problems are solved. Through Seamless MPLS networking technology, operators can flexibly handle connection requirements so that services are provided quickly. Thus, new services are deployed quickly and service deployment costs are reduced, which strengthens the competitiveness of operators.

In addition to the V interface between the access and convergence network, the VLAN may be configured for service interconnection between the MAN and backbone network. Seamless MPLS networking can meet this requirement and enable dynamic establishment through the end-to-end MPLS pipes for inter-metro services.

In the Seamless MPLS networking model, all services can be transferred to the specified service processing points through the MPLS pipe at service access points. The entire bearer solution is simple and consistent. With the dynamic end-to-end MPLS pipe establishment capability, services can be transferred to any service processing points or peer service access points through the MPLS pipe/PWE3 pseudo wire, according to requirements.

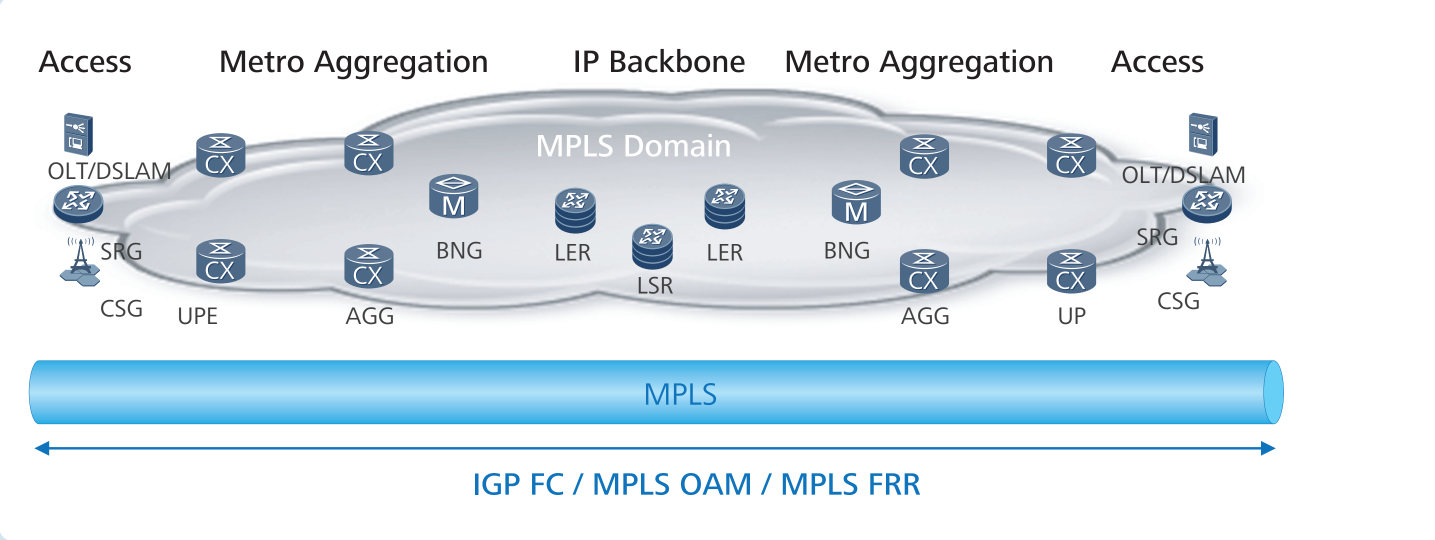

Figure 3 Seamless networking model

Seamless MPLS networking technology is not new and is widely applied to backbone networks, MANs, and the mobile backhaul. Application experiences indicate that Seamless MPLS networking is a mature and reliable bearer technology with excellent scalability. The Seamless MPLS can eliminate the gap between network layers to implement end-to-end MPLS networking.

2 The Value of Seamless Networking Technology

2.1 Unified and Simplified Bearer Technology

With seamless networking technology, the access (fixed/mobile), convergence, and backbone devices connect through the unified IP/MPLS control layer.

2.2 Flexible and Scalable Network Architecture

Future-oriented networking technology must provide a more flexible and scalable network architecture. Currently, the development of some services indicates that more flexibility and better scalability are required.

1. Service wholesale in FTTX access
   In the case of the copper access, the LLU is the main wholesale mode. In the case of the FTTX access, the LLU is not applicable. The bit stream access will become the mainstream wholesale mode.

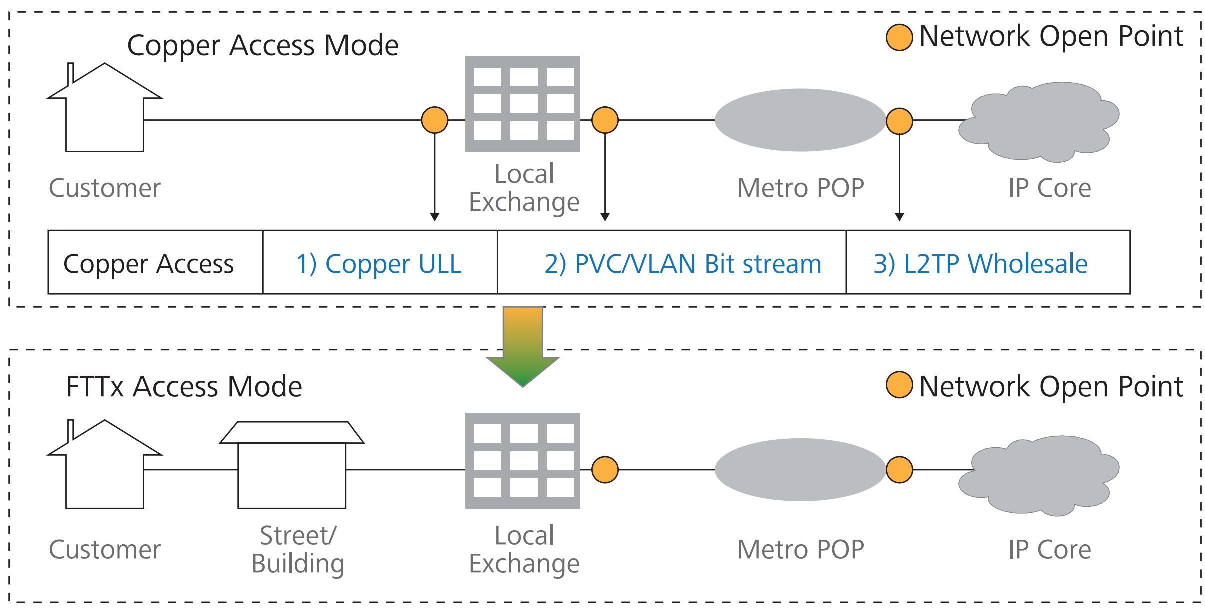

Figure 4 Service wholesale in the copper and FTTx access scenarios

The POP device can be deployed in any network layer according to the network scale of the competitor operator. For BSA wholesale, the network must be flexible and simple so that wholesale user services can be handed over to a competitor operator at any point. Through end-to-end MPLS pipes between the ANs and service transfer points, seamless architecture meets flexible connection requirements. In TR101 architecture, the AN, convergence devices, and service transfer points are configured. When the service transfer points are in the inter-metro area, the distributed nodes and backbone PE devices in the MAN must be configured.

Sometimes, the competitor operator needs to identify different users and services through the 2-layer VLAN TAG. To meet this requirement, the incumbent operator must identify the competitor operator and its users and services on the AN. If TR101 architecture is used, the distribution policy of the S-TAG and C-TAG must be planned carefully. In the seamless architecture, the PW identifies different competitor operators. It is easier to identify users and services.

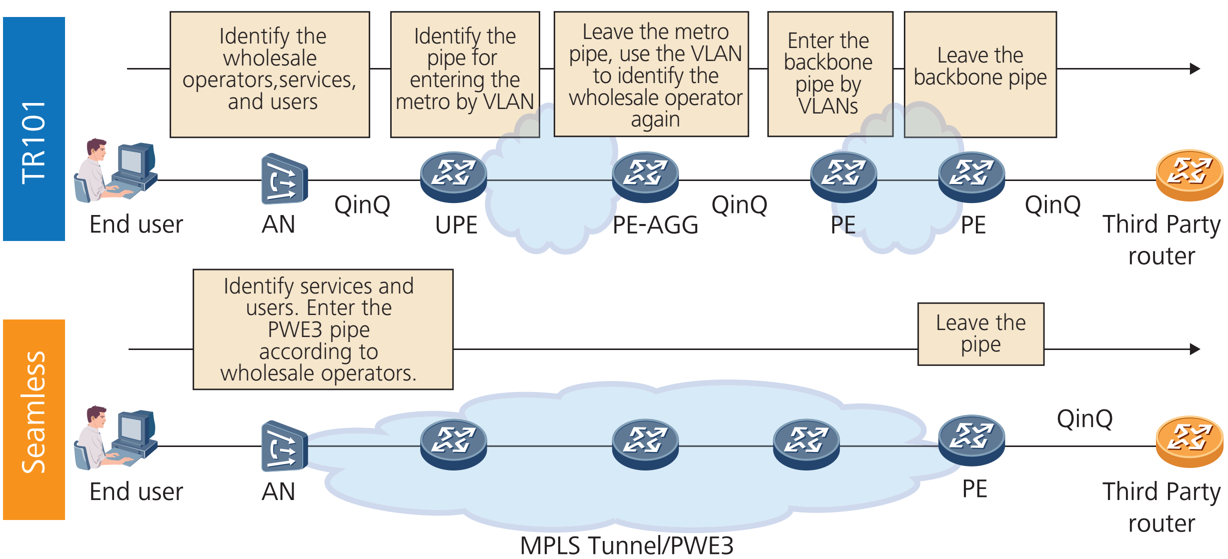

Figure 5 Service wholesale deployment comparison between the seamless and TR101

2. Deployment of inter-MAN enterprise Ethernet private services
   Enterprise Ethernet services are not limited just in the MAN. The connection of Ethernet private lines may be required between MANs. In TR101 architecture, multiple nodes such as access nodes, metro UPE, metro PE-AGG, and the backbone PE must be configured to provide Ethernet private line services between the

inter-metro DSLAMs. In addition, the VLAN planning is required.

In seamless networking, only the access nodes on both sides are configured in the dynamic PWE3 mode to provide Ethernet private line services.

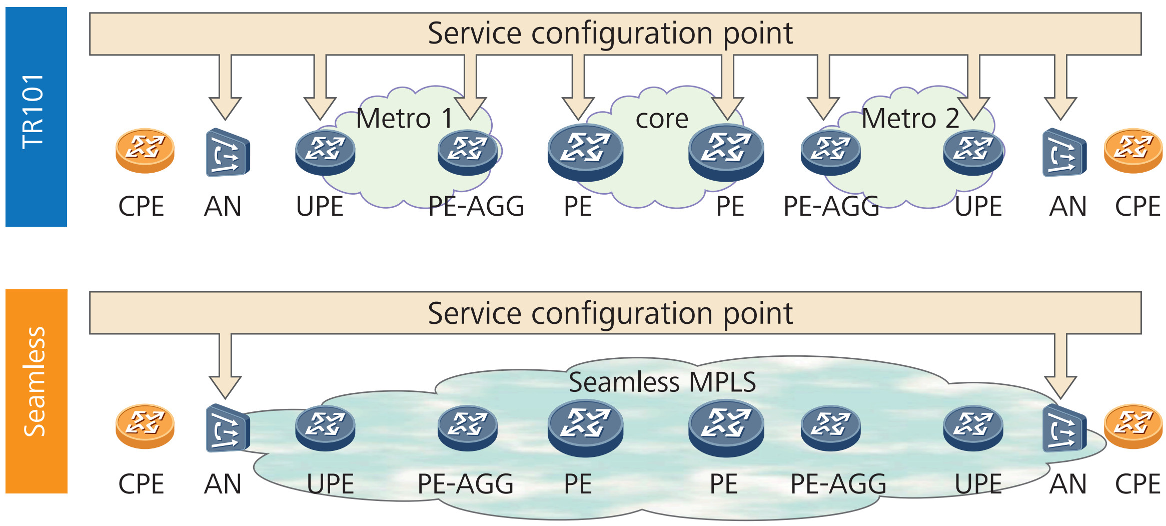

Figure 6 Comparison of deployment of inter-metro private line services between the Seamless and TR101

2.3 Quick Service Provision to Improve User Satisfaction

To provide wholesale and enterprise private line services under TR101 architecture the access, metro, and backbone devices of different layers must cooperate. For service deployment, cross-departmental coordination is required between the management entities of different layers. As a result, it takes a long time to provide services.

With seamless networking, operators need to only configure user access points. Services can be provided quickly, user satisfaction increases, and service deployment costs are reduced. Thus, operators' competitiveness is strengthened.

2.4 Maturity and Reliability of IP/MPLS and OAM Technologies

Based on IP/MPLS technology, seamless networking easily implements end-to-end protection through the reliable and mature IP/MPLS technology and OAM. The interoperability between the devices of different manufacturers is excellent.

In TR101 architecture, protection between each layer requires both IP/MPLS and Ethernet reliability to cooperate with OAM technology. Deployment is complicated and interoperability may fail.

3 Implementing the Seamless MPLS Networking Technology

3.1 Challenge of the Seamless MPLS Networking Technology

Through IP/MPLS technology, the seamless MPLS connects the access layer, convergence layer, and backbone layer, and provides flexible and scalable networking architecture for operators. It is improper to directly inherit all technologies from the old IP network.

After the devices of each layer are seamlessly connected, the scale of the IP/MPLS domain improves by orders of magnitude compared with the original networks. For example, in a network with 20,000,000 users, if each DSLAM connects 100 users in FTTC access mode, the number of nodes in the entire network is over 200,000. If each OLT connects 1000 users in FTTB/FTTH access mode, the number of nodes in the entire network is 20,000. In the original networking mode, the order of magnitude of the number of nodes in the backbone and metro route domains is in the 1,000s. Hence, the scale of the route domain in Seamless MPLS networking increases by an order of magnitude of one or two. In a large-scale network, engineers have to consider how to construct the route and MPLS tunnel, and how to guarantee the availability of the networks.

In addition, a large number of access devices, such as DSLAMs and OLTs, are available in the network, taking up a high ratio of network investment. Hence, the introduction of the IP/MPLS should not obviously affect the cost of access devices. In Seamless MPLS networking, the complexity of the access device control plane and performance specifications of the forwarding layer must be reduced. The following table lists the typical specification of the IP/MPLS capacity for access devices by a European telecom operator.

Parameter	Routing Protocol	IP FIB	LDP control layer	LDP forwarding table	BGP
Specifications	Static route	2	200	200	Not supported

3.2 Seamless MPLS Area-Based Networking

In the area-based networking mode, all devices belong to the same autonomous system (AS). The IGP (OSPF/ISIS) is used to exchange route information between nodes. The devices of each metro are divided into different IGP areas. The IP backbone devices constitute backbone areas or a level-2 area to ensure that the number of nodes in each area is appropriate. The access node may adopt static routing, without supporting the dynamic IGP protocol.

As shown in Figure 7, the entire route domain of the Seamless MPLS is divided into three layers: the backbone node, metro convergence node, and AN node. Serving as the ABR, the PE in the backbone network converges area routes and advertises them to other areas, which reduces the route capacity requirements of each device. Besides reducing the routing table capacity of each device, route area-based deployment is helpful for isolating inter-area faults and enabling fast route convergence.

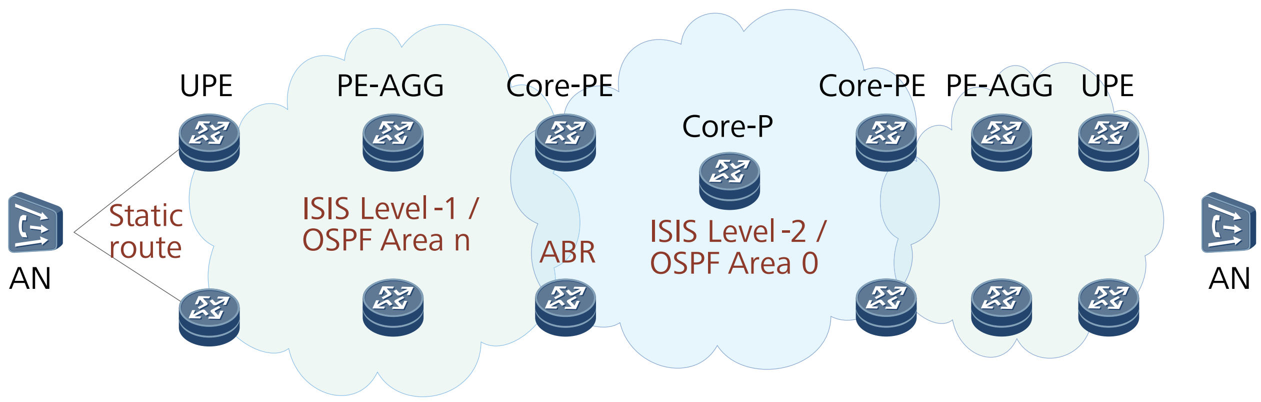

Figure 7 Seamless MPLS route area-based deployment

PW labels are distributed in end-to-end T-LDP mode. Tunnel labels are distributed in hierarchical mode. See Figure 8. In the dynamic IGP range, the LDP DU label release mod is used. The LDP DoD label release mode is used between the UPE and AN. The AN must be cost-effective; therefore, DoD mode allows the AN to request the needed labels on demand. As a result, the specification requirement of the MPLS forwarding table is reduced. The LDP DU labels are distributed to the edge of the area according to a certain policy. In the backbone area (or level-2), the route label is distributed to the common area (level-1). The route label of common areas is not distributed to the backbone area. In this way, the UPE can establish the LSP tunnel to the edge direction in any area.

The inter-area labels are distributed in Labeled BGP (RFC 3107) mode. The iBGP runs through the UPE. Many UPEs are available; therefore, the 2-level reflector structure is used. The Core-PE functions as the UPE reflector of this area, and the core-RR functions as the Core-PE reflector. The Core-PE is not a simple reflector. Upon receipt of the BGP Label from the UPE, the Core-PE changes the Next-hop of this label route information to the Core-PE, and re-allocates the labels. When the Core-RR receives the label route information, it reflects it to the UPE, without changing any information.

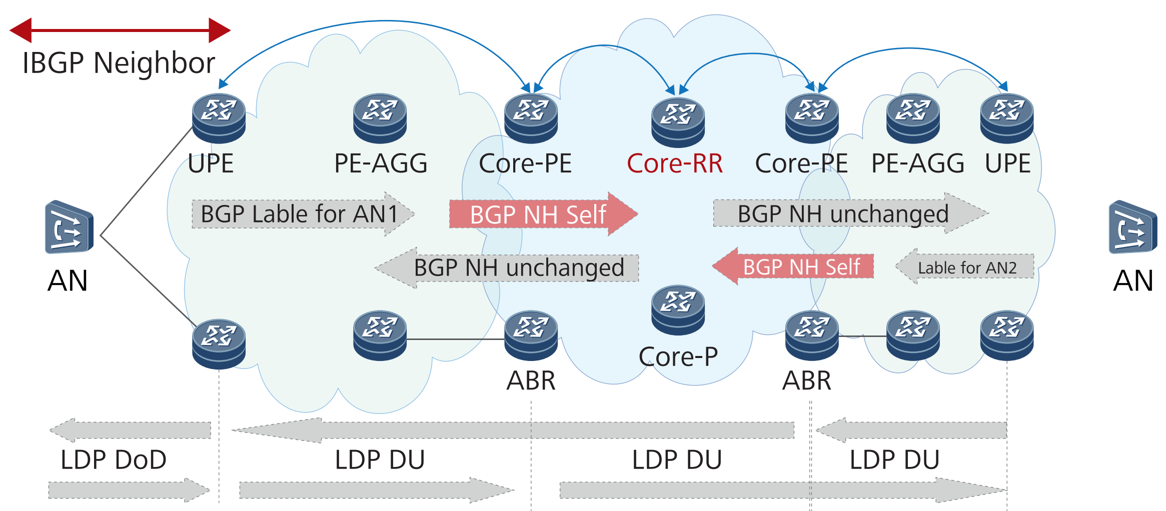

Figure 8 Seamless MPLS label release area-based deployment

Figure 9 shows a label release and forwarding instance. The PW label is directly allocated through the T-LDP session between DSLAM-A and DSLAM-B. The external LSP tunnel from DSLAM-A to DSLAM-B is actually divided into four segments:

Segment 1: LDP DoD label from the DSLAM-A to the UPE-A, which is the DSLAM-B label requested by the DSLAM-A from the UPE-A on demand. According to the self BGP label table, the UPE-A searches the DSLAM-B to allocate to the DSLAM-A LDP label and establish the matching relation between them (many-to-one).

Segment 2: Two-layer tunnel from the UPE-A to ABR-B. The external layer is the tunnel established in the LDP DU mode from the UPE-A to the ABR-B. The internal layer is the tunnel distributed to the DSLAM-B through the Labeled BGP for the UPE-A by the ABR-B. The labels of the external tunnel are changed hop by hop during forwarding. The labels of the internal tunnel are invisible between the UPE-A and ABR-B, and remain unchanged.

Segment 3: Tunnel from the ABR-B to the UPE-B. This segment is similar to segment 2, which is a two-layer tunnel.

Segment 4: Tunnel from the UPE-B to the DSLAM-B. This tunnel is obtained through the UPE-B request to the DSLAM-B in LDP DoD mode according to the static route.

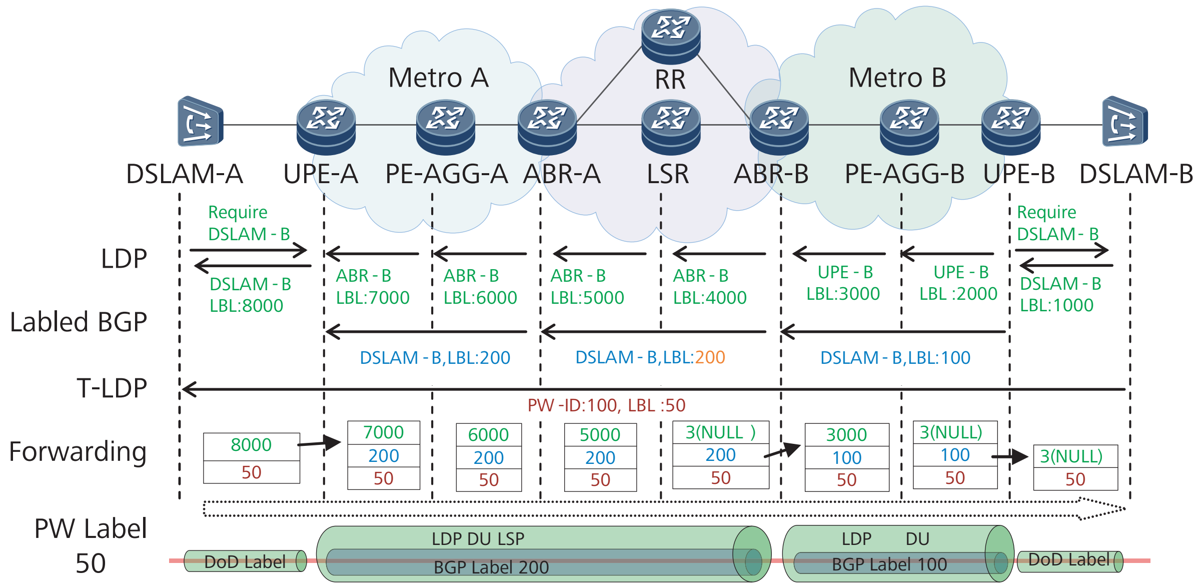

Figure 9 Seamless MPLS control and forwarding instance (uni-directional)

In the above route and label release mode, the number of routes and labels of each node are reduced. The entire networking solution features excellent scalability. The following table lists the node route and labels of the above solutions.

Node		AN	UPE	AGG	Core-PE	Core-P
IGP route	Description	Default static route	Specific routes in this area. Convergence route of other areas	Specific routes in this area. Convergence route of other areas	Specific routes in this area and backbone area. Convergence route of other areas	Specific routes in the backbone area. Convergence route of other areas
	Typical value	2	2000	2000	3000	1000
LDP label	Description	Request on demand	All nodes in this area. All nodes in the backbone area.	All nodes in this area. All nodes in the backbone area.	All nodes in this area. All nodes in the backbone area.	All nodes in the backbone area.
	Typical value	200	3000	3000	3000	1000
BGP label	Description	None	All nodes	None	Control layer: all nodes Forwarding layer; all nodes in this area.	None
	Typical value	None	200,000	None	2000 (forwarding layer)	None

3.3 Seamless MPLS AS-Based Networking

In the AS-based networking mode, each metro and backbone are in different AS domains. The metro can use the private AS number. The IGP protocol is independently deployed on each AS domain. EBGP switching route information is used between the metro and backbone area. When the EBGP advertises route information, routes are converged. As a result, the number of routes decreases. Route deployment of the access nodes is the same as area-based networking; that is, static route mode.

Label distribution is similar to that in area-based networking. The LDP DU mode is used in the AS-domain. In the inter-AS domain, labeled BGP is used to release label routes. The DoD is used between the AN and UPE. In ASBR position, the BGP labels perform bidirectional Next-Hop Self operations. The labels are re-allocated locally. Therefore, the requirements for BGP label forwarding table capacity at the metro egress and Core-PE position is high.

Figure 10 shows the distribution of routes and labels in AS-based networking.

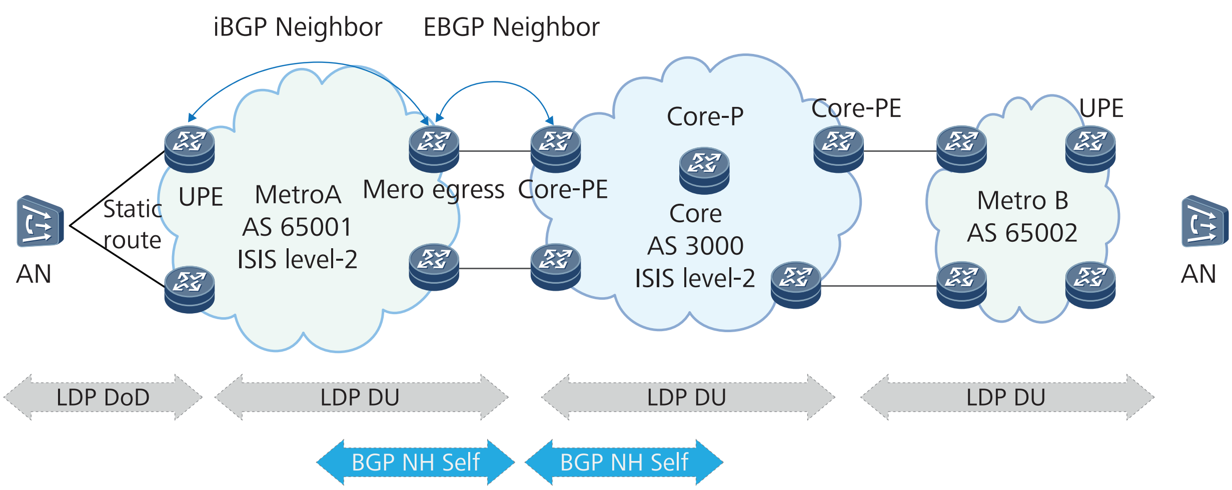

Figure 10 Seamless MPLS AS-based route/label release

4 Key Technologies

4.1 Inter-area LDP

According to the LDP specification RFC5036, the IP address information in the FEC should be checked when the LDP label route information is received. When the IP address matches the route information in the local IP route table, the label information is valid. Actually, the above solution does not comply with this specification. In the UPE location, the LDP LSP to all backbone nodes must exist. When the route is advertised, the ABR aggregates the routes of the backbone area. In the UPE, the specific route to the backbone node is unavailable. The address in the LDP FEC fails to locate the accurately matched route information. At the access nodes, only the default route is configured. The label information of any node must be requested on demand.

To meet Seamless MPLS networking requirements, the LDP Extension for Inter-Area Label Switched Paths (RFC 5283) extends the restriction in the LDP specification. The precision matching principle is changed to the maximum length matching principle. If the address prefix in the FEC has the maximum matching item in the IP route table and the next hop of both is consistent, the label information is valid. The extension supports the hierarchical deployment of the Seamless MPLS inter-area route and labels.

4.2 Service Driven LDP DoD

On the AN nodes, the number of LDP label tables must be restricted. If the LDP DU mode is used, the filtering policy must be configured on the AN nodes. In this mode, a large number of policy tables must be maintained. When the policy is changed, a mechanism is unavailable to notify the upstream UPE to re-transmit the LDP label information.

The Downstream on Demand (DoD) LDP distribution mode meets the Seamless MPLS AN node requirement. The labels can be requested dynamically according to service requirements. When label forwarding tables are reduced, flexible service change requirements are met.

Label distribution in DoD mode requires the AN node to be configured with the request policy. When services are changed, the DoD request policy must be changed, along with the service configuration. Configuration and maintenance workloads increase. The service driven LDP DoD can meet the AN node's future flexible connection requirements to automatically configure DoD request policies and avoid the repeated configuration workload.

4.3 MPLS Load-Balancing Label (MPLS Flow Label)

In TR101 networking architecture, packets between the access node and UPE are encapsulated in VLAN/QinQ mode. The load can be balanced according to user MAC addresses and IP addresses. After migration to the Seamless MPLS networking architecture, the UPE functions as the P node. Current load-balancing technology is implemented based on PW granularity. The number of PWs on the access node is limited and PW traffic is not balanced. Hence, load-balancing based only on PW granularity causes seriously unbalanced loads. As a result, bandwidth scalability between the access node and UPE is affected. The following table lists the typical services of the AN. The bandwidth distribution of each service is unbalanced. The corresponding PW bandwidth of the HIS service takes up more than 70% of the total bandwidth. PW granularity cannot implement load-balancing.

Services	Bandwidth	Description
PW1	800M	HIS service. Connects to the BRAS.
PW2	200M	IPTV live service. Connects to the SR.
PW3	100M	Wholesale service. Connects to the SP BRAS
PW4	10M	Enterprise private line 1. Connects to other DSLAMs in the domain
PW5	2M	Enterprise private line 2. Used for the inter-domain connection

When the single stream is carried in the PW, the packet load in the PW is balanced (ECMP or Trunk) to multiple links. As a result, packets may be disordered and user services affected. When the single PW carries large traffic (for example, PW corresponding to the HIS, containing the online traffic of a large number of users), all packets of each traffic are carried over the same link, without affecting the services of other users.

In the current load balancing mechanism, it is difficult for node P to perform load-balancing by traffic on the PW. Hence, the MPLS Flow Label is added to the ingress PE of the PW. The PE node can identify the flow, with the understanding of the services carried on the PW. Intermediate nodes need to only balance nodes by label, so implementation is simplified. After the flow label is added, the packet encapsulation of the PW is as follows:

LDP Label
BGP Label
PW Label
MPLS Flow Label
Control Word (optional)
Payload

Node P performs load-balancing according to the L4 label stack information. The specific flow L4 label information in the PW is the same, which ensures that all packets in the flow are not dissembled to different egresses. In the PW, various flows can be balanced to different links because the flow labels are different. In this way, the PW is balanced according to the load of flows.

When the carried MPLS Flow Label needs to be established on the PW, both ends need to notify each other about various issues, such as whether to support the Flow Label, and whether the packets carry the

Flow Label. In this way, basic forwarding is not affected when either party does not support the corresponding function.

4.4 Fast Convergence Technology

The Seamless MPLS networking adopts unified IP/MPLS technology. The mature and reliable IP/MPLS technology enables end-to-end fast protection switching when different vendors' devices are networked. The service protection process in the Seamless MPLS networking is described below.

The network and bearer of the Seamless MPLS are hierarchical. Accordingly, the protection technology is hierarchical. For example, in the area-based networking solution, the LSP tunnel between the ANs is divided into four segments. The roles of the tunnels in the node vary with links. Hence, the convergence modes are different in the case of failure.

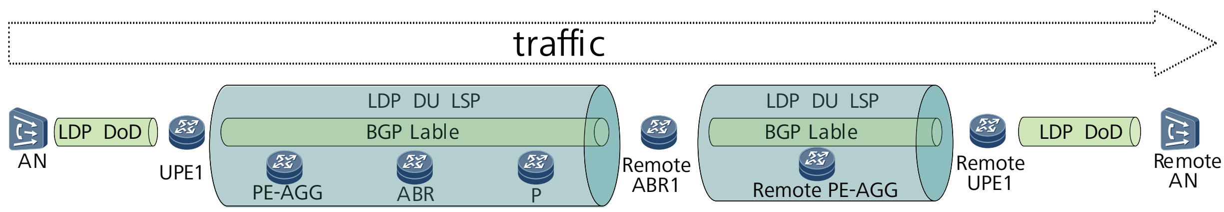

Figure 11 Roles of the nodes in the Seamless MPLS area-based solution

As the basis for the reliability of Seamless MPLS networking, the fast convergence technology of the IGP and BGP guarantee quick path recovery in the control layer. In the forwarding layer, FRR technology can accelerate service convergence.

4.4.2 LDP FRR Convergence Technology

In the LDP layer, LDP FRR technology implements the fast convergence of the LDP LSP. In the LDP FRR technology, the device uses the optimal route of the LDP as the forwarding entry, simultaneously uses the second best route of the LDP as the backup path, and stores it in the forwarding table. When the optimal next hop is faulty, the backup path/label is used directly for forwarding.

The BFD detection technology quickly detects the connection of the optimal next hop to implement the convergence rate of 50 ms.
The usage of the LDP FRR convergence technology is limited. For example, in the ring networks, the second best next hop sends packets to this node. As a result, the forwarding ring is formed.

For dual-homing networking of the AN, the ring does not exist. In this case, LDP FRR technology can be used.

The networking of the nodes above the UPE is complicated. The ring may exist. In this case, the Loop Free Alternates (IGP LFA) defined in the RFC5286 is used to check whether the ring exists. The LFA is used to check whether the second best path has a ring according to IGP link status information. If the LFA detects a ring, the node does not use LDP FRR convergence technology. In most cases, the LDP FRR can be applied.

In comparison to the FRR technology of the RSVP TE, LDP FRR protection is single point, not end-to-end. The LDP FRR can be deployed if there are a large number of tunnels in Seamless MPLS networking. TRSVP TE FRR protection technology may be deployed for certain services or on certain network layers.

4.4.3 BGP FRR Convergence Technology

The LDP FRR rapidly switches paths if a link fails. When the BGP node (including the UPE/ABR) is faulty, it depends on the convergence of the label BGP. For common BGP convergence technology, convergence is performed in the control layer and then the forwarding entry is delivered. The entire convergence time may reach the second level. The BGP next hop separation technology can increase the convergence speed of the control layer. The carrier-class reliability requirement is not met.

The BGP FRR adopts the direct switching mode in the forwarding layer. The LDP Label/BGP Label of the second best BGP neighbor is directly stored in the forwarding list as the backup. When the fast detection mechanism (such as the BFD) detects that the best BGP neighbor is faulty, the system directly switches to the backed up entry for a quicker convergence performance.

The following table summarizes the convergence technology and performance of the unidirectional flow if a fault occurs.

Fault Location	AN-UPE Link or UPE Node	UPE-Remote Inter-ABR Link or Node	Remote ABR Node	Remote ABR - Remote inter-UPE Link or Node	Remote UPE Node	Remote UPE - Remote AN Link
Fault detection	AN-UPE BFD	Single-hop BFD detection between points	UPE-remote ABR multi-hop BFD detection	Single-hop BFD detection between points	Remote ABR - Remote UPE multi-hop BFD detection	Remote UPE - Remote AN BFD detection
Switching Operation	LDP FRR	LDP FRR IGP FC	BGP FRR	LDP FRR IGP FC	BGP FRR	BGP route cancellation
Convergence Performance	50 ms	50 ms	200 ms	50 ms	200 ms	Subsecond (only the service of this AN is affected)

4.5 OAM Technology

In the unified IP/MPLS control layer, the entire network is maintained and managed through consistent OAM technology, which greatly reduces the inter-department coordination time and the definition of inter-department responsibility. The fault can be quickly and proactively detected, located, and handled, which improves QoE.

The entire network is deployed with hierarchical OAM. On the link layer, the link-level fault can be detected and located through detection technology on the link. On the tunnel layer, tunnel connectivity is detected online in real time through the BFD for LSP, and MPLS OAM (Y.1711). LSP ping/traceroute can locate failures and faults in service provision. MPLS-TP-OAM performance monitoring technology monitors the performance indexes of tunnel bearer services in real time. On the PW layer, the VCCV monitors the connectivity of the PW in real time. The MPLS-TP OAM for PW and Y.1731 for PW/VPLS monitors the specific service performance indexes in real time. For the OAM packets between user devices, unified MPLS technology easily implements transparent transmission.

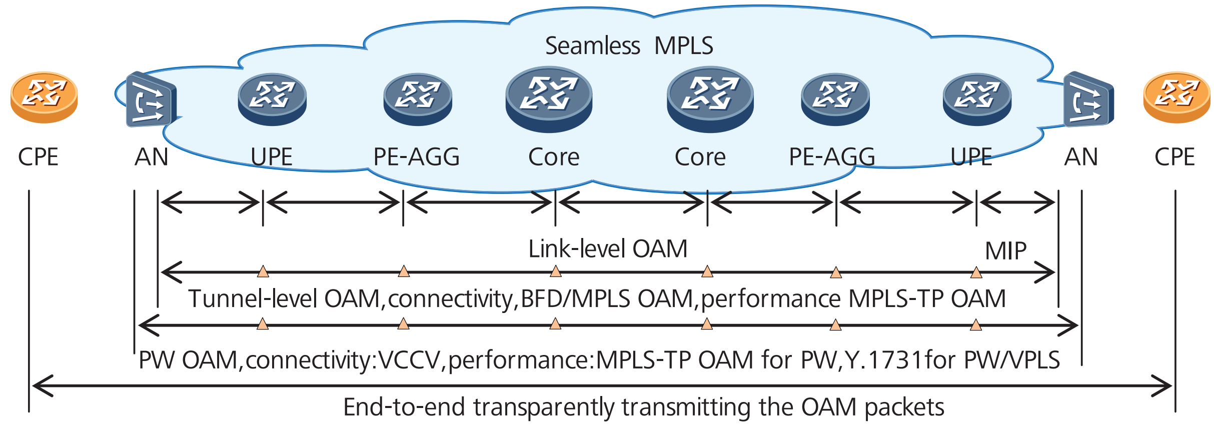

Figure 12 Unified OAM deployment

5 Applications

5.1 Flexible Service Wholesale

The Seamless MPLS architecture meets flexible service wholesale requirements, as shown in Figure 13. Service transfer points vary with the competitor operator, and the AN nodes need to transport user flows to the corresponding transfer points according to the competitor operators. In Seamless MPLS networking architecture, the AN node can directly establish the PW connection with the service transfer point, and be perceived by intermediate devices. Deployment is simple. According to the requirements of competitor operators, user location and the service label can be identified on the AN. The VLAN flags of different competitor operators can be overlapped without bottlenecking the number of competitor operators or users. End-to-end service protection measures can be conveniently implemented.

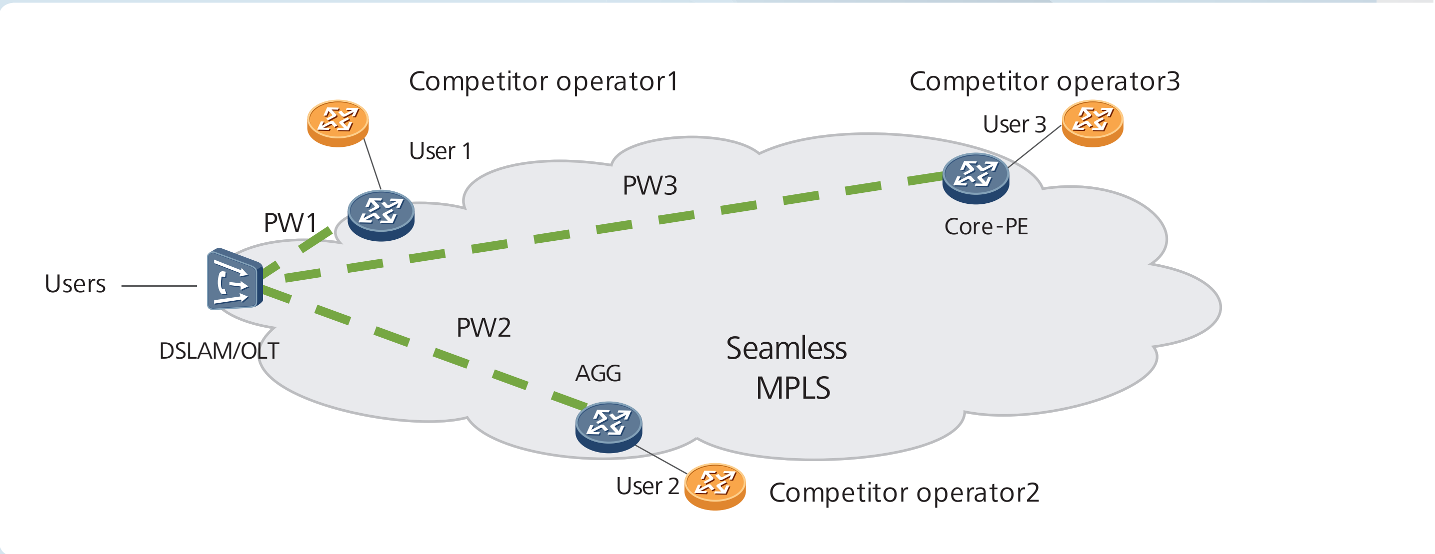

Figure 13 Deployment of flexible service wholesale

5.2 Inter-Metro VPLS Private Line

In the Seamless MPLS networking architecture, the VPLS service can be conveniently deployed across the entire network without the restriction of the VLAN.

A large number of nodes are available in the entire network. The VPLS must be hierarchically deployed. In this way, this avoids the problems related to full neighbor connections and the forwarding efficiency of the broadcast/unknown packets.

See Figure 14. The VPLS service is deployed in the 3-layer H-VPLS architecture. The H-VPLS core layer is constructed between the ABRs. The UPE is the convergence layer, and is accessed to the ABR of this area through the PW. For the CPE accessed in the DSLAM, the DSLAM is accessed to the UPE through the PW. UPE location can be directly accessed to the CPE in Ethernet/VLAN mode. In 3-layer architecture, the number of PWs converged in each layer is limited; for example, the UPE is accessed to 100 DSLAMs, and the ABR is accessed to 20 UPEs. If the DSLAM is directly connected to the ABR through the PW, the pressure of the PW on the ABR is high. The topology of the PW is close to the actual physical topology to reduce PW overlapping on the single link, which improves the forwarding efficiency of the broadcast/ unknown unicast packets.

To reduce the workload of adding the service access points in the VPLS instance and ease VPLS deployment, the BGP Auto-Discovery H-VPLS can be deployed in the core and convergence layer nodes (ABR and UPE) to automatically discover the new service access points. The new service access points are processed between the DSLAM and UPE in static configuration mode. When the DSLAM does not support the BGP, you can configure only the DSLAM and UPE to provide services in the scenario of adding the single VPLS service access point.

In the H-VPLS, the ABR is the core node. If many VPLS instances are accessed, the pressure on the device MAC address table specification is high. PBB+H-VPLS technology can handle the problem. In an actual deployment scenario, the PBB can be encapsulated on the UPE. For the packets reported through the PW by the DSLAM or the packets reported through the Ethernet by the CPE, the user MAC addresses (C-MAC) are filtered. The MAC address (B-MAC) of the destination UPE is visible only on the ABR. The number of visible MAC addresses of the ABR is greatly reduced. The scalability of VPLS service deployment is improved. For PBB and VPLS interoperability, see the Technical White Paper for PBB + VPLS.

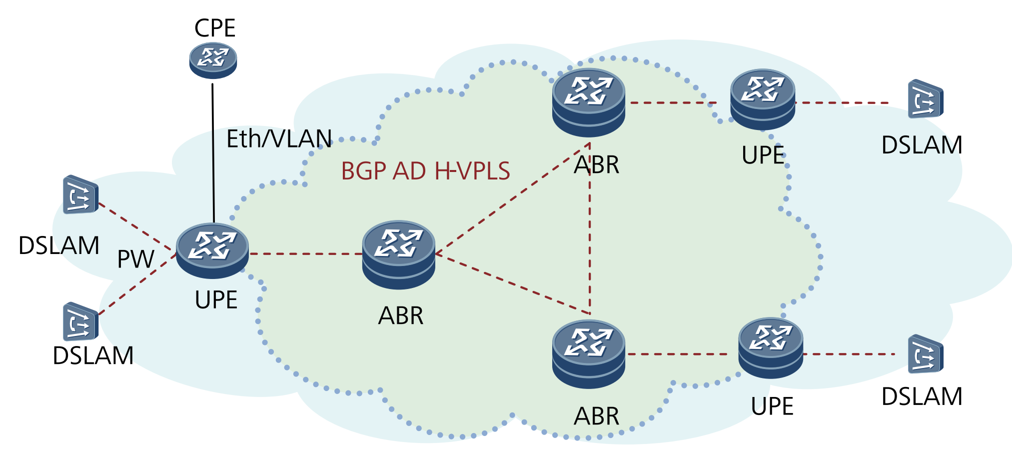

Figure 14 H-VPLS service deployment solution

5.3 ATM DSLAM Migration

In the existing networks of many operators, the ATM DSLAM is widely applicable to the access of individual users and enterprise private lines. ATM switch vendors are gradually phasing out the lists of mainstream equipment suppliers. The migration of the ATM convergence network is necessary; there are too many access nodes in the network. Operators cannot meet the upgrade and reconstruction costs if ATM DSLAMs are switched to the IP DSLAM all at once. In this case, gradual migration is more feasible; that is, IP DSLAM converging the ATM DSLAM.

In Seamless MPLS network architecture, the IP DSLAM can directly send services to the corresponding egress through the PWE3, without the intermediate ATM links.

For individual user services, if the BRAS still keeps the ATM interface, the original ATM convergence network function can be implemented through the ATP PWE3 between the IP DSLAM and AGG node. If the BRAS migrates to the Ethernet interface, the conversion from the PPPOA to PPPOE and from the IPOA to IPOE is performed on the IP DSLAM. Data is sent to the BRAS through the Ethernet PWE3.

For the enterprise private line service, the ATM PWE3 can be directly established between the IP DSLAMs to transparently transmit ATM services.

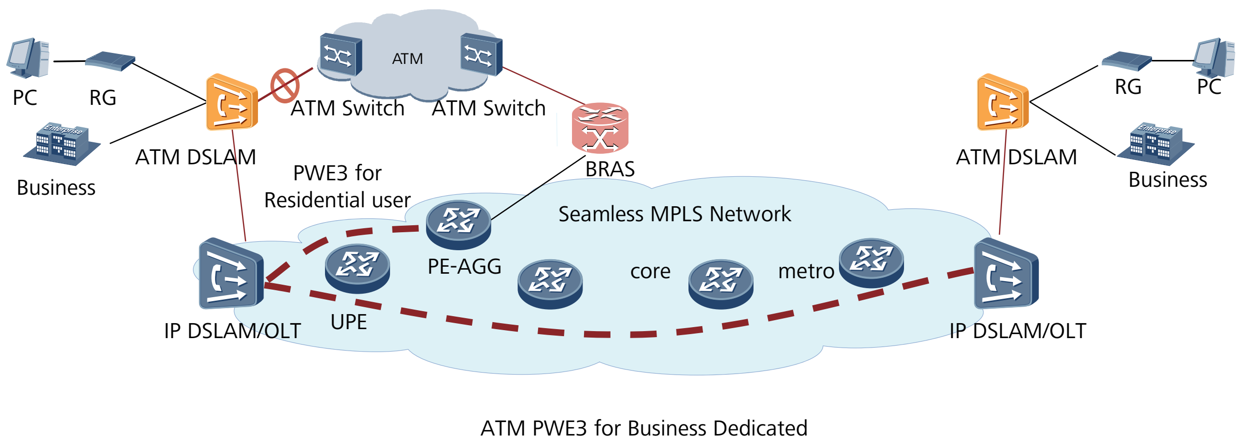

Figure 15 ATM service migration scenario

6 Conclusion

With the simplified and unified network architecture, the Seamless MPLS solves the O&M and reliability problems due to the isolation of each network layer. The Seamless MPLS provides flexible and scalable network architecture for operators.

7 Appendix A References

1. N. Leymann,, Seamless MPLS Architecture, draft-leymann-mpls-seamless-mpls-00
2. Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031
3. Andersson, L., Minei, I., and B. Thomas, "LDP Specification", RFC 503
4. Rekhter, Y. and E. Rosen, "Carrying Label Information in BGP-4", RFC 3107
5. Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364
6. Decraene, B., Le Roux, JL., and I. Minei, "LDP Extension for Inter-Area Label Switched Paths (LSPs)", RFC 5283
7. S. Bryant, C. Filsfils, U. Drafz, V. Kompella, J. Regan, S. Amante, Flow Aware Transport of MPLS Pseudowires, draft-bryant-filsfils-fat-pw-03
8. D.Katz, D.Ward, Bidirectional Forwarding Detection, draft-ietf-bfd-base-11
9. K. Kompella, Y. Rekhter, Ed., Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling, RFC 4761
10. M. Vigoureux, D. Ward, M. Betts, Requirements for OAM in MPLS Transport Networks, draft-ietf-mpls-tp-oam-requirements-03

8 Appendix B Acronyms and Abbreviations

Abbreviation/Acronym	Full Spelling
MPLS	Multi-Protocol Label Switch
AN	Access Node
PE	Provider Edge
CE	Customer Edge
UPE	User-facing PE
AGG	Aggregation Node
LLU	Local Loop Unbundling
FTTC	Fiber to the Curb
FTTB	Fiber to the building
FTTH	Fiber to the home
IGP	Interior Gateway Protocol
ABR	Area Border Router
ASBR	Autonomous System Border Gateway
(LDP) DoD	Downstream on Demand
(LDP) DU	Downstream Unsolicited
FIB	Forwarding Information Base
BFD	Bidirectional Forwarding Detection
FRR	Fast Reroute
ECMP	Equal cost Multiple Path
PW	Pseudo wire
RSVP	Resource ReSerVation Protocol
VPLS	Virtual Private LAN Service
H-VPLS	Hierarchical VPLS
PBB	Provider Backbone Bridge

Huawei Technologies Co., Ltd.
Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518219
People's Republic of China

Website: http://www.huawei.com
Email: support@huawei.com