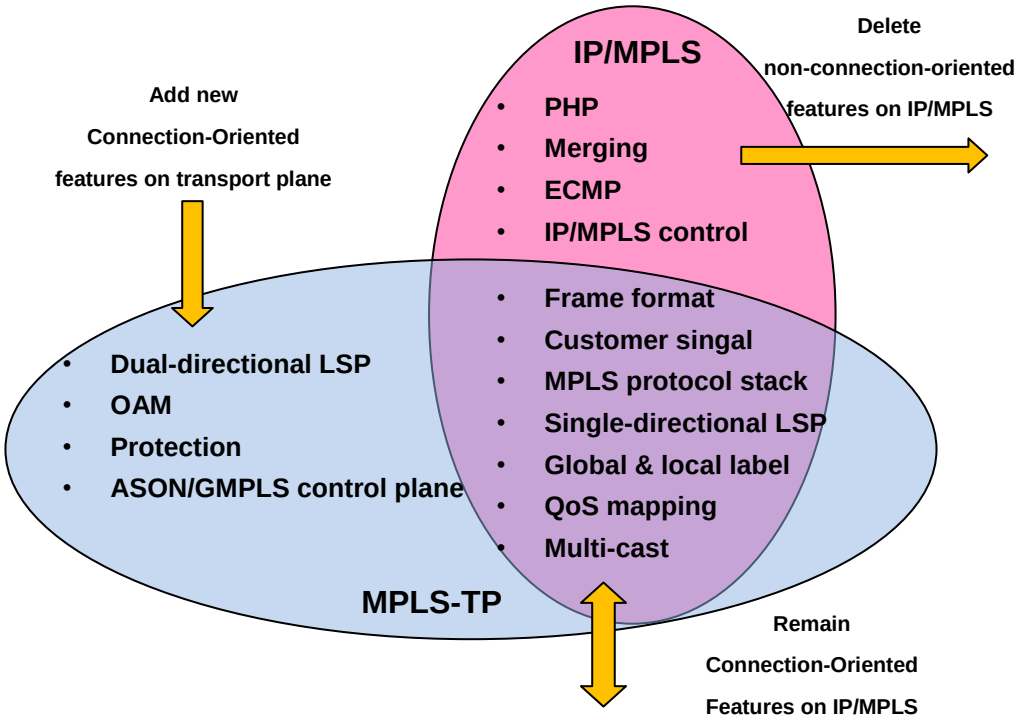
Technical Whitepaper on IP MPLS and MPLS-TP Interoperability

1 Abstract

MPLS-TP (MPLS Transport Profile) extends IP/MPLS to facilitate the evolution to packet transport. MPLS-TP is standardized by the JWT of IETF and ITU-T and is the major packet transport technology.

Compared with IP/MPLS, the MPLS-based MPLS-TP simplifies transport requirements at data forwarding layer and enhances OAM and protection. Their relationship is as follows:

Figure 1-1 The relationship between MPLS-TP and IP/MPLS



MPLS-TP includes:

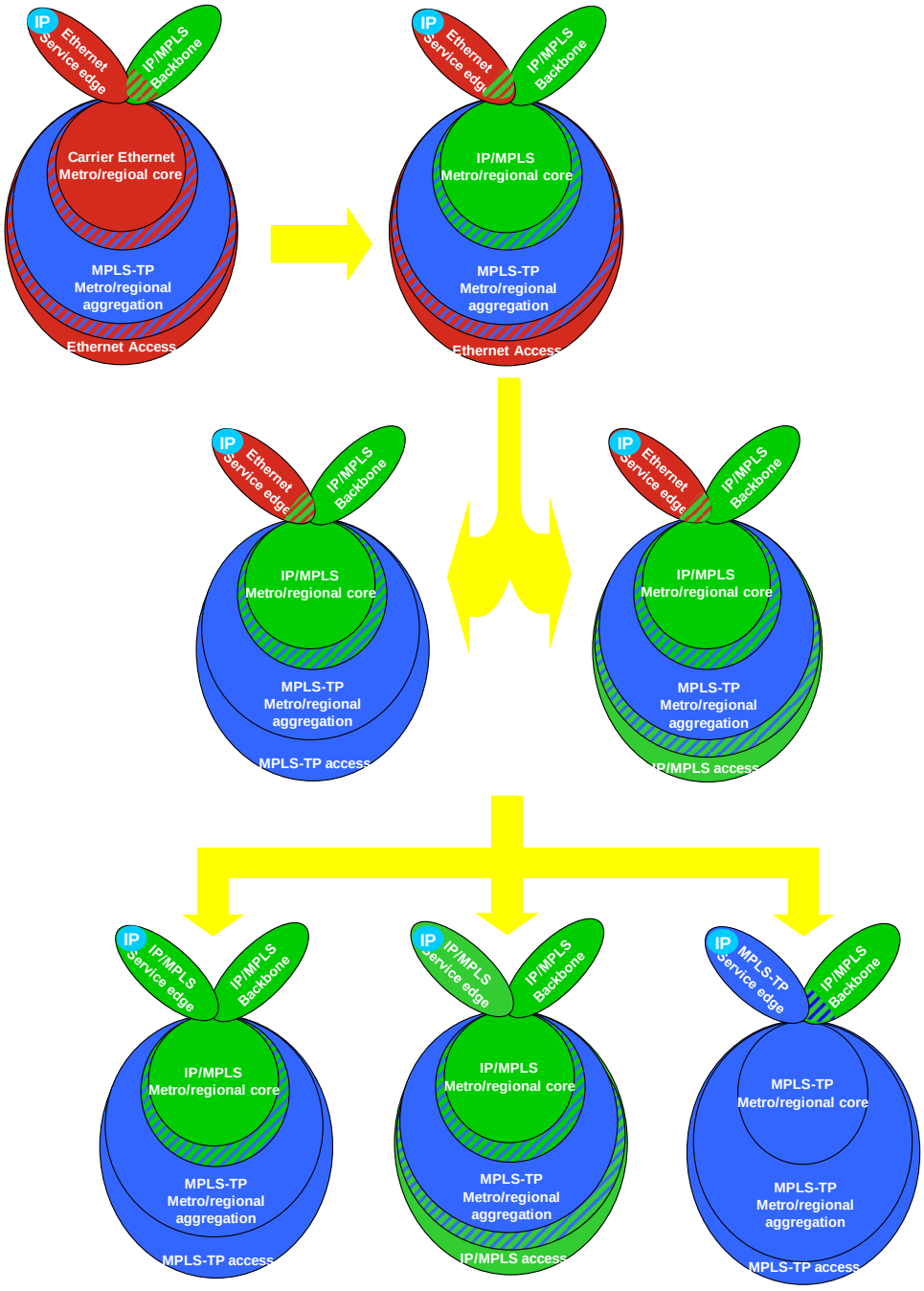
- Data plane: MPLS forwarding mechanism is still in use, but MPLS-TP employs bidirectional LSP and removes LSP convergence and PHP.
- Control plane: The equipment can be configured through NMS, and dynamic control plane operated through GMPLS is under study.
- OAM: Achieve OAM requirements of conventional SDH in a packet network, e.g., inband OAM, connectivity check/verification, AIS & CFI, and performance management.
- Protection: Support 50ms protection switching and 1:1/1+1 linear/ring protection.

In a word, MPLS-TP takes the advantages of MPLS/PWE3 (based on label forwarding/multiservice support) and TDM/OTN (good O&M and fast protection switching), and supports IP, Ethernet, ATM and TDM services.

2 MPLS-TP and IP MPLS interoperability scenario

With superior reliability and flexible ETE service deployment, IP/MPLS firmly dominates bearer networks. Most operators use IP/MPLS for their core networks, while MPLS-TP shows more and more powerful service bearing capability in mobile backhaul networks as a result of complete OAM and protection mechanism.

Figure 2-1 MPLS-TP and IP/MPLS interoperability scenario



The above picture depicts the development trend of MPLS-TP and IP/MPLS application scenarios, and shows MPLS-TP and IP MPLS will coexist for a long time. MPLS-TP is applied to metro network and is inevitably connected to core-layer MPLS network, so the interconnection between MPLS-TP and MPLS is the focus all parties are concerned about. If MPLS-TP and IP/MPLS interoperability is achieved and is combined with their

positioning in existing networks, it can meet service development demands and reduce technical risks and TCO.

This paper introduces major technologies in combination with two models of MPLS-TP and IP/MPLS interoperability.

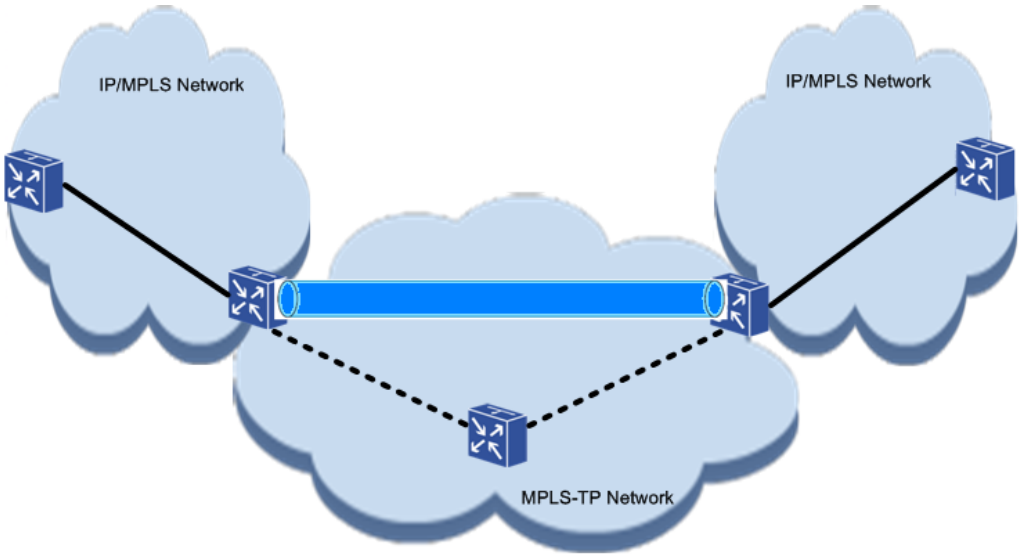
3 Key technologies

3.1 MPLS-TP and IP MPLS interoperability models

MPLS and MPLS-TP interoperability has no IETF JWT draft, but a personal draft “draft-martinotti-mpls-tp-interworking-02” which describes the models of their interoperability.

Generally, two interoperability models are available: Overlay and Peer.

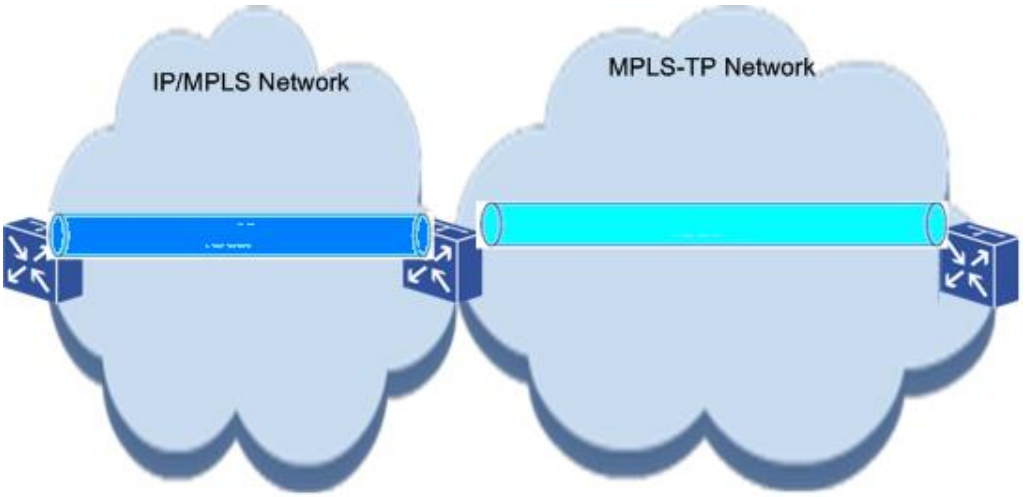
Figure 3-1 Figure 3-2 Overlay



As shown above, the overlay is the service layer of one network (e.g., MPLS-TP) for the other network (e.g., IP/MPLS). After encapsulated properly at a network boundary node, client-layer data (including control-plane data and transport-plane data) is transparently transmitted to the corresponding service-layer network boundary node via service-layer

channel (e.g., TP LSP). A service-layer network is just a hop of a client-layer network, namely, two boundary nodes in the service-layer network is considered as adjacent nodes in the client-layer network.

Figure 3-3 Peer



As shown above, two networks are peer in the model and independently process data in their own networks, while network boundary nodes map information between two networks to transmit data.

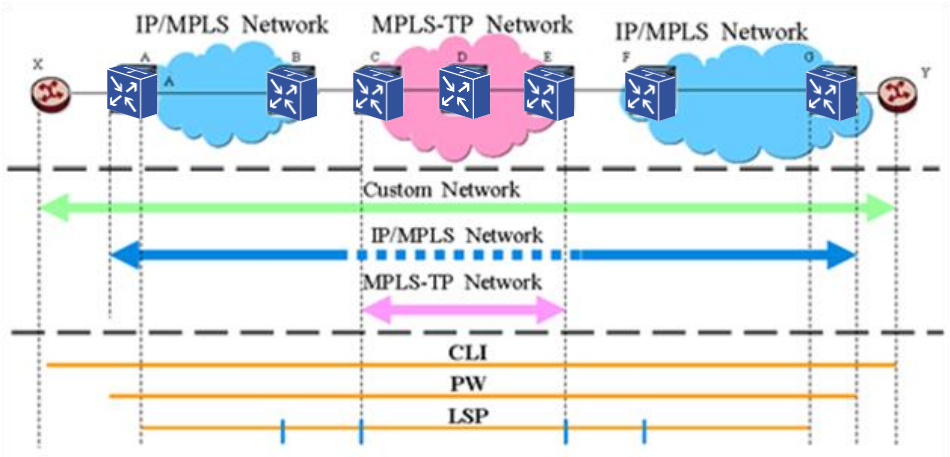
3.2 Overlay

MPLS-TP and IP/MPLS have two overlay interconnection modes: IP/MPLS over MPLS-TP and MPLS-TP over IP/MPLS.

3.2.1 IP MPLS over MPLS-TP

In IP/MPLS over MPLS-TP, LSP is created in two ways. One is to create MPLS-TP LSP, and notify IP/MPLS network in FA (Forwarding Adjacent) mode. When IP/MPLS LSP is created, the created TP LSP can be considered as a direct link to participate in the routing. The other is to create the signaling via IP/MPLS LSP to trigger TP LSP creation through RSVP-TE at TP domain edge, transparently transport IP/MPLS LSP signaling information via the created TP LSP and finally create IP/MPLS LSP.

Figure 3-4 IP/MPLS over MPLS-TP

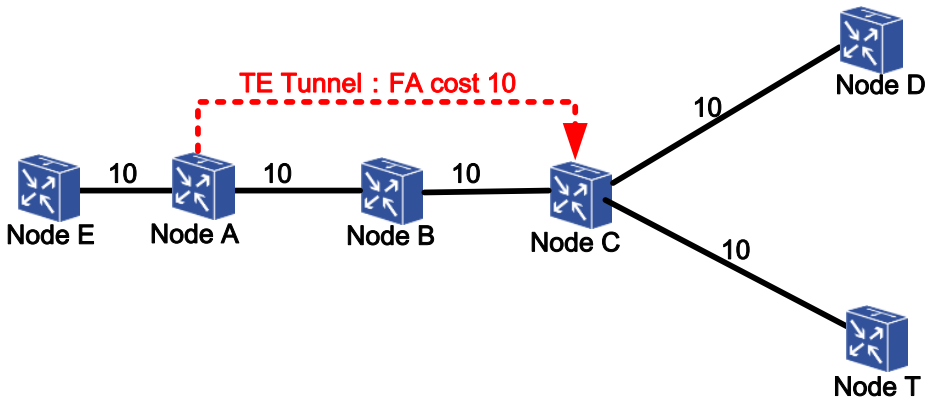


As shown above, the entire TP LSP is just a hop of IP/MPLS, and IP/MPLS data and information is transparently transmitted via TP LSP.

1.1.1.1 FA

FA (Forwarding Adjacent) means calculating the route via bidirectional TE tunnel interface in IGP/IGP-TE. The bidirectional TE tunnel works as a link for notification in IGP/IGP-TE. Thus the TE tunnel interface participates in route calculation and works as an egress interface of a specific route in the forwarding table so that a packet is forwarded via MPLS/nested MPLS rather than via IP/MPLS.

Figure 3-5 FA



As shown above, when regular IGP route is calculated, the route from A to T is A—B—C—T, and the egress interface is the interface of B. If the bidirectional TE tunnel from A to C starts FA, namely, take the TE tunnel as a link of the overhead 10 and notify IGP, A thinks the overhead from A to C is 10, and the TE tunnel interface is selected as the egress interface.

It is mentioned above that bidirectional TE tunnel participates in IGP or IGP-TE route selection in the FA mode. If TE tunnel working as a link is notified in IGP, TE tunnel interface participates in IP route calculation and works as an egress interface of a specific route in the IP forwarding table so that a packet is forwarded via MPLS rather than via IP. If TE tunnel working as a TE link is notified in IGP-TE, TE tunnel interface participates in MPLS-TE route calculation and works as an egress interface of a specific route in the MPLS forwarding table, namely, create a nested LSP. The IP MPLS over MPLS-TP mentioned here is the latter.

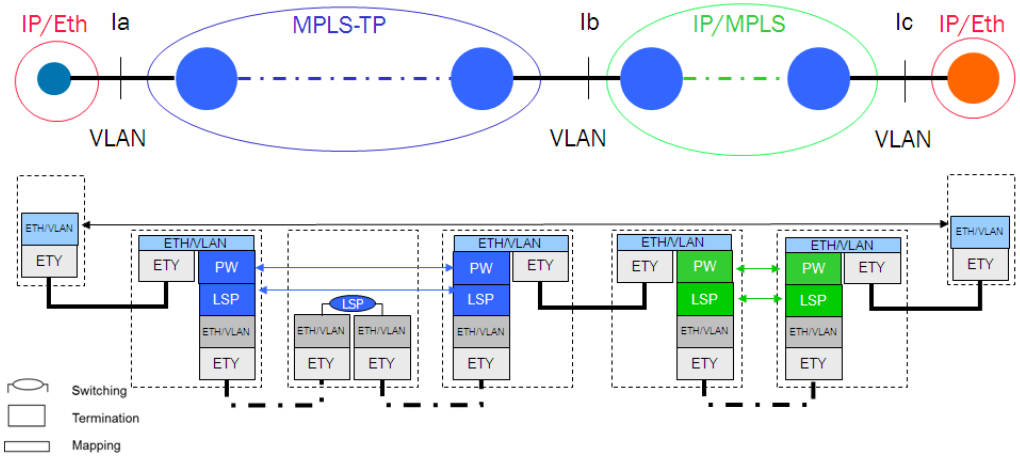
1.1.1.2 Encapsulation

In draft-martinotti-mpls-tp-interworking-02 two overlapping interconnection encapsulation is mentioned: ETH overlapping encapsulation and IP/MPLS overlapping encapsulation.

- ETH overlapping encapsulation

In this scenario, MPLS-TP works as the service layer of IP/MPLS. IP/MPLS packets are firstly encapsulated in Eth, and then Eth packets are encapsulated in pseudo-wire of MPLS-TP as shown in Figure 3-5:

Figure 3-1 ETH overlapping encapsulation

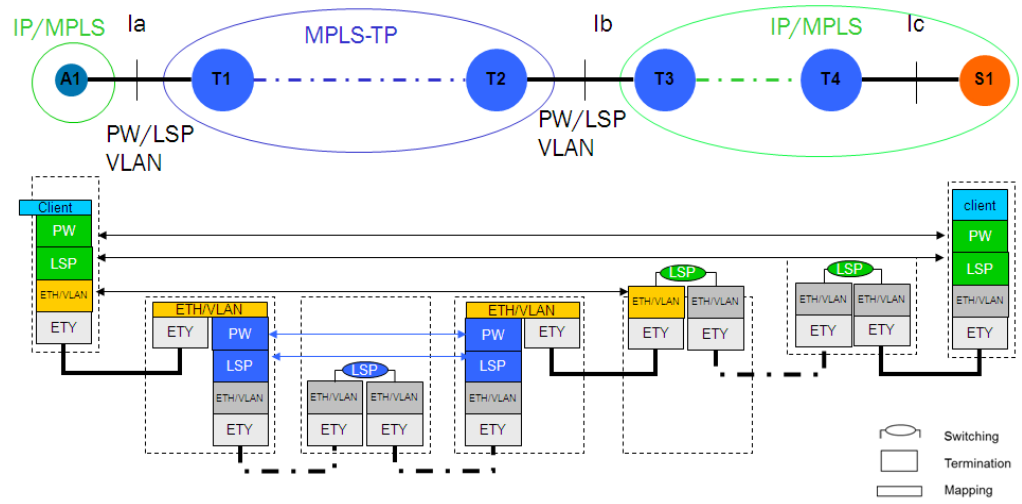


In the above figure, ETH/VLAN field in the light blue thin diagram at the edge node of the network is used for packet encapsulation and mapping. In practical application, the field may be deleted together with ETY field.

- IP/MPLS overlapping encapsulation

In this scenario, as the service layer of IP/MPLS, MPLS_TP is connected to IP/MPLS device by UNI. IP/MPLS packets are directly encapsulated into LSP in MPLS-TP (by label stack). MPLS-TP domain edge device takes processing of IP/MPLS MPLS-TP at the same time as shown in Figure 3-6:

Figure 3-6 IP/MPLS overlapping encapsulation



In the above figure, ETH/VLAN field in yellow thin diagram at the network edge node is used for packet encapsulation and mapping. In practical application, the field may be deleted together with ETY field.

In Figure 3-3, two IP/MPLS networks are connected by MPLS-TP network. Overlapping model is adopted to complete inter-operation of IP/MPLS and MPLS-TP network. MPLS-TP network is considered as the service layer of IP/MPLS network. And IP/MPLS network is considered as the customer layer of MPLS-TP network.

If we use Ethernet encapsulation, the physical layer is Ethernet. Node C and E receive the Ethernet packets from node B and F, and transport the data based on Ethernet service simulation. In this way, the interconnection protocol between IP/MPLS and MPLS-TP is not needed. MPLS_TP doesn't need to implement IP/MPLS but its encapsulation is the poorest. Using unified L3 (ETH) encapsulation, MPLS-TP and MPLS network don’t need any connection. They are considered as independent PSN with low encapsulation efficiency though.

If we use IP/MPLS encapsulation, two IP/MPLS networks are connected by MPLS-TP. MPLS-TP network is considered as the service layer of IP/MPLS network while IP/MPLS network is considered as the customer layer of MPLS-TP layer. IP/MPLS is directly encapsulated into LSP of MPLS-TP (label stack). In this way interconnection protocol is not needed for IP/MPLS device and MPLS-TP device. But MPLS-TP device needs to implement IP/MPLS functions with poor encapsulation efficiency. In other words, MPLS-TP is directly considered as service layer of MPLS. MPLS packets sent by IP/MPLS network are taken as customer layer service and encapsulated into MPLS-TP PSN.

1.1.1.3 OAM

The overlapping inter-operation model of MPLS-TP and IP/MPLS has OAM of the following layers:

- Directly connected link layer OAM: OAM on this layer could be of many types. It could be physical layer OAM but more than it, and link layer OAM mechanism.
- OAM of LSP layer in MPLS-TP network

- OAM of PW layer in MPLS-TP network
- OAM of sectional LSP layer in IP/MPLS network, which is OAM on the section of LSP between the two domain edge nodes of IP/MPLS crossing TP network.
- OAM of E2E LSP layer in IP/MPLS network.

OAM on each layer can interact with each other. For example, when TP LSP layer detects a failure, it will send AIS message to notify the failure to TP PW layer (OAM customer layer of TP LSP). But there's no related research result in standards in notification to IP/MPLS network by OAM in TP network.

1.1.1.4 Implementation Procedure

In overlapping model, the implementation steps of IP MPLS over MPLS-TP are as follows:

- Create LSP:

When MPLS-TP bears IP/MPLS network, there are two LSP establishing methods: one is to establish MPLS-TP LSP first, send notification to IP/MPLS network by FA (Forwarding Adjacent), and get the established TP LSP participated in pathing as a directly-connected link when we establish IP/MPLS LSP. The other is to establish signaling by LSP of IP/MPLS to trigger establishment of TP LSP at TP domain edge by RSVP-TE, so as to transparently transport signaling message of IP/MPLS LSP through the established TP LSP, and to finally establish IP/MPLS LSP.

- Create PW:

Configure VLAN message manually at network domain edge node, and configure the corresponding relationship between VLAN and PW at the edge node of MPLS-TP network. That is to say, we encapsulate IP/MPLS packet into a PWE3 Ethernet frame at TP network edge incoming node based on the mapping relationship of VLAN and PW, and then transport it from TP network to IP/MPLS network. We restore PWE3 Ethernet frame to IP/MPLS packet at edge incoming node of TP network based on the mapping relationship of VLAN and PW, and transport it to IP/MPLS network domain edge node.

- Configure OAM and protection:

Establish OAM and protection relationship of the corresponding layer based on the needs. The routine fast route convergence and FRR system are inherited for protection in overlapping model.

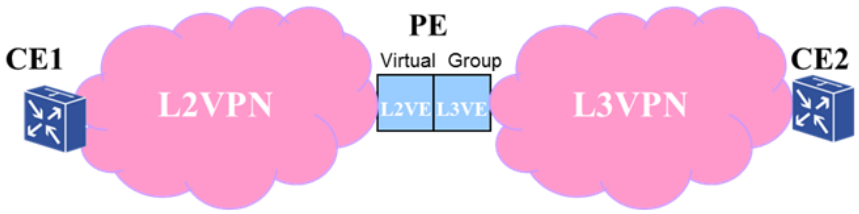
3.2.2 MPLS-TP over IP MPLS

Currently L2 technology is usually adopted to deploy in MPLS-TP. When two MPLS-TP network services cross IP/MPLS network, L2/L3 VPN bridging can be used to take inter-operation between MPLS-TP and IP/MPLS network.

1.1.1.5 L2/L3 VPN Bridging

L2/L3 VPN bridging is to integrate L2VPN and L3VPN on one device to implement logic separation and interconnection of L2 and L3 VPN in one virtual group, which is the implementation of L2VPN termination and L3VPN forwarding. Actually it's a kind of gateway bridge of L2/L3VPN by which the connection between VPN can be realized.

Figure 3-7 Logic diagram of L2/L3VPN bridging

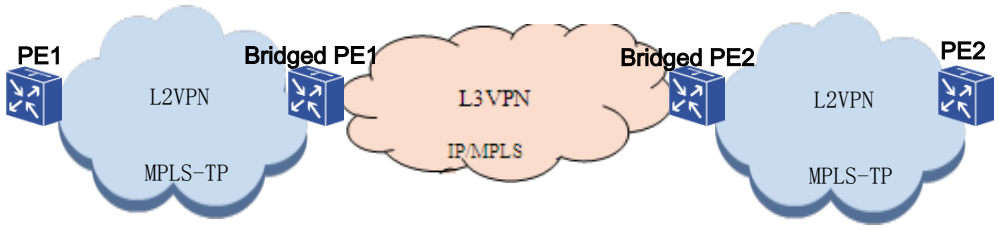


As shown in Figure 3-7, PE device can be divided into two parts: one is corresponding to L2VPN, which is called L2 Virtual Entity (L2VE). The other is corresponding to L3VPN, which is called L3 Virtual Entity. The two are integrated as Virtual Group, which has the features of both L2VPN and L3VPN.

When L2VPN packets arrive, the corresponding L2VPN information is found by port and vlan information (CIP access) or pw incoming label information (pw access). If L3 forwarding is needed (MAC of the packets are local host MAC), the corresponding L3VPN information should be obtained based on L2/L3 VPN binding relationship in the virtual group to start L3 forwarding procedure.

When L3VPN packets arrive, if the egress of L3 forwarding is a L3VE with a L2VE bound, the packets will be transmitted to the L2VE and start L2VPN forwarding procedure.

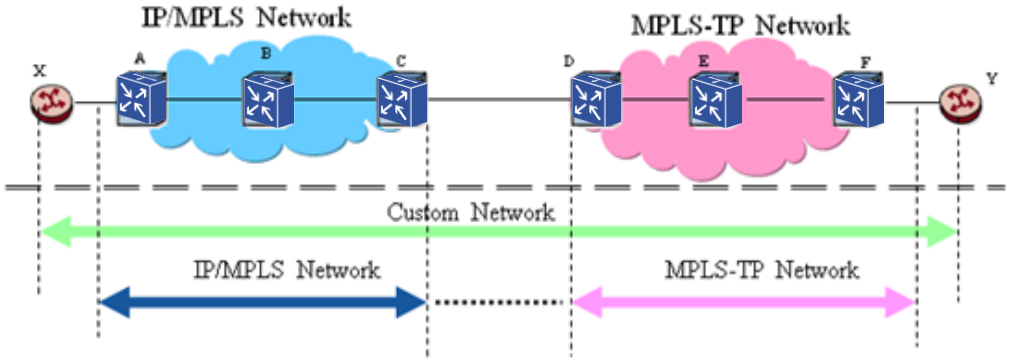
Figure 3-8 Network Interconnection by L2/L3VPN bridging



After L2/L3 VPN bridging deployment, the services all carry MPLS label during the whole process of transmission so that E2E QoS features and integrated protection switching strategy can be easily deployed, network complexity can be dramatically reduced, and network construction costs can be saved.

3.3 Peer Model

Figure 3-9 Peer model



In Figure 3-9, MPLS-TP and IP/MPLS are connected by a section of link. In this situation peer model can be used to complete inter-operation of IP/MPLS and MPLS-TP network. MPLS-TP and IP/MPLS are in one layer.

At present, MPLS-TP and IP/MPLS peer interconnection model has two interconnection systems: one is MS-PW system in which PW inside the network domain is established respectively in each network. The network domain edge node works as SPE to take the

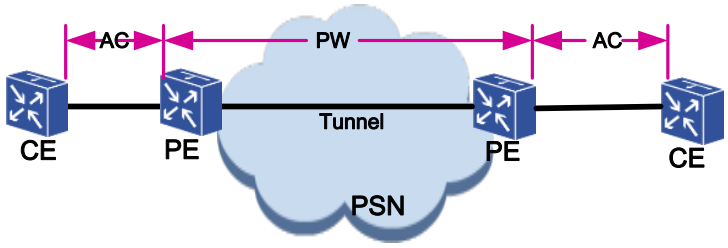
PW in the network domain as sub-PW so as to establish E2E MS-PW crossing MPLS-TP and IP/MPLS network. The other is SS-PW+LSP stitching system in which PW inside the network domain is established respectively in each network. These LSP are stitched at network domain edge node to compose an E2E stitched LSP crossing MPLS-TP and IP/MPLS. The stitched LSP is used to bear PW (a common PW which is SS-PW).

3.3.1 MS-PW

Here we will introduce several concepts first: PWE3, SS-PW, and MS-PW.

PWE3 (Pseudo-Wire Emulation Edge to Edge) is a L2 service bearing technology that tries to truly emulate as much as possible the basic behaviors and features of ATM, frame relay, Ethernet, low-speed TDM (Time Division Multiplexing) circuit and SONET/SDH. In PE of PSN, PWE3 takes LDP/RSVP as signaling protocol. It emulates various L2 services (such as L2 data packets and bit flows) at CE (Customer Edge) by tunnel (which could be MPLS tunnel, GRE, L2TPv3 or others), and transparently transmits L2 data of CE end. The basic diagram of PWE3 is shown in Figure 3-10:

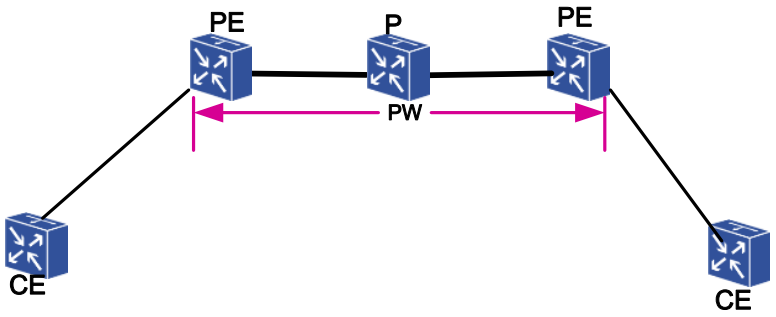
Figure 3-10 Basic diagram of PWE3



PWE3 can be divided into SS-PW and MS-PW based on networking type:

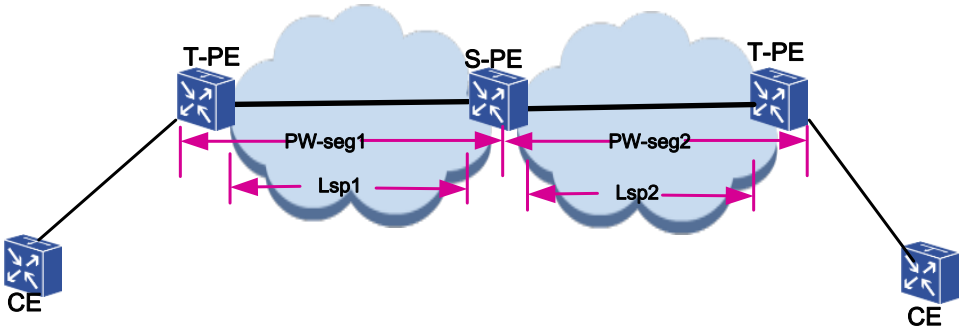
Single-Segment Pseudo-Wire is a PW directly established between T-PE and T-PE without label switching of PW Label as shown in Figure 3-11:

Figure 3-11 SS-PW



Multi-Segment Pseudo-Wire is multiple PW segments between T-PE and T-PE as shown in Figure 14. The forwarding system for T-PE in multiple segments is the same with that for T-PE in single segment except multi-segment PW needs to connect the single-segment PW on two sides by PW switching device S-PE, and complete PW label switching at S-PE.

Figure 3-12 MS-PW



MS-PW is usually used in the following scenarios:

- As the source and destination PEs are not in the same service area, signaling connection or tunnels cannot be built between the two PEs.
- The signaling on the source and destination PEs are different.
- Although the access device can run MPLS, it can't build many LDP sessions. In other words, it cannot realize full-mesh LDP session. At this moment, the access device can be used as T-PE, and the high-performance device S-PE is used as the

switching point of the LDP session. Then set more PW S-PEs (Switching PE) as the switching point of the LDP to converge the bearer PW in the tunnel.

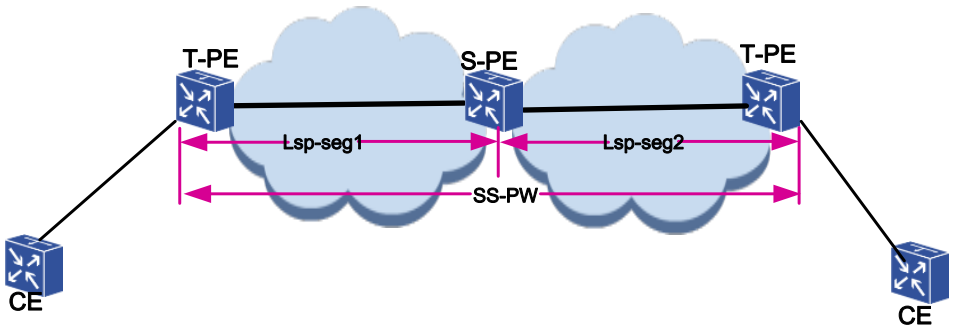
The multi-segment pseudo-wire allows multiple PWs between the source and the destination PEs. The PW switching device S-PE is used to connect the single PW at the both sides together, and implement the PW-layer label switching at the S-PE site. Helping the user out of the scenario in which single-end PW cannot be built between the source and destination PEs, the multi-segment pseudo-wire technology satisfies different application requirements in cross-local network, cross-operator and cross-control platform scenarios. In addition, this technology can meet the requirements of deploying the network in a static, dynamic or hybrid way.

In the peer-to-peer scenario shown in the figure 3-9, if the multi-segment pseudo-wire is used, i.e. one tunnel is built in the two networks respectively, the boundary node message will firstly pop up tunnel labels for PW label switching. Then the labels will be encapsulated to another network tunnel. In this process, the IP/MPLS boundary node and the MPLS boundary node need to implement PW label switching.

3.3.2 LSP stitching

As the figure 13 shows the LSP stitching means there are multiple segment LSPs between the T-PEs. Each section of LSP in the LSP stitching is an average LSP. The only task is to connect the single LSP at both sides via the LSP S-PE in the LSP stitching and implement the LSP-layer label switching at the S-PE.

Figure 3-13 LSP stitching



LSP stitching differs from MS-PW only in different levels. The LSP stitching connects the single LSPs at the both sides on the S-PE. However, the MS-PW connects the single PW at the both sides on the S-PE.

As shown in the peer-to-peer scenario, if LSP stitching is used which means one tunnel passes through two networks at the same time, the boundary node is only used for tunnel label switching. In this method, the IP/MPLS boundary node, MPLS boundary node and the service X/Y should interconnect their protocols. The encapsulation efficiency is great. The entire process equals to an independent ss-pw process with changing PSN Tunnel. Besides, the tunnel label switching is required at the two PSN network boundary nodes.

3.3.3 OAM

In the peer-to-peer operating model of the MPLS-TP and IP/MPLS, the definition to OAM in using MS-PW and LSP stitching are different.

The OAM in using MS-PW peer-to-peer operating model refers to:

- Direct-connected OAM. There can be many sorts of OAM, including but not limited to physical layer OAM and link layer OAM mechanisms.
- The end-to-end OAM on LSP layer, including end-to-end LSP OAM on the MPLS-TP network and end-to-end LSP OAM on the IP/MPLS network.
- The end-to-end OAM on the Pw layer, i.e. MS-PW OAM in the MPLS-TP and IP/MPLS networks.

The OAM in using LSP stitching peer-to-peer operating model refers to:

- Direct-connected OAM. There can be many sorts of OAM, including but not limited to physical layer OAM and link layer OAM mechanisms.
- The end-to-end OAM on each sub-LSP layer, including the OAM on the end-to-end LSP of the MPLS-TP network and the OAM on the end-to-end LSP of the IP/MPLS network.
- The end-to-end OAM of the LSP layer, i.e. the LSP stitching OAM crossing the MPLS-TP and IP/MPLS networks.

- The end-to-end OAM on the PW layer.

The OAMs on different layers may interact with each other. But the standards of the announcement from the LSP OAM to the PW OAM in the MS-PW mechanism and the announcement from the sub-LSP layer OAM to the LSP stitching OAM in the LSP stitching mechanism are still under research.

3.3.4 Working Process

In the peer-to-peer model, the interaction between the MPLS-TP network and the IP MPLS network includes the following steps:

- Create LSP

First of all, build intra-segment LSP in the networks respectively.

If the LSP stitching mechanism is used, the administrator should stitch two LSPs (sub-LSP) at both networks to one LSP manually at the network boundary node (SPE), i.e. build LSP stitching relationship on the SPE. In this way, the end-to-end LSP stitching crossing the MPLS-TP network and the IP/MPLS network can be built.

- Create PW

If the MS-PW mechanism is used, the administrator should stitch two PWs (PW fragment) at both networks to one PW manually at the network boundary node (SPE), i.e. build PW stitching relationship on the SPE. In this way, the end-to-end MS-PW crossing the MPLS-TP network and the IP/MPLS network can be built.

If the LSP stitching mechanism is used, the administrator can keep using this LSP stitching to build the end-to-end Pw crossing the MPLS-TP network and the IP/MPLS network. Besides, this PW is a single-segment PW.

- Configure OAM and protection

Build the proper OAM and protection relationship according to the requirements. The protection in the peer-to-peer model usually keeps the regular fast route convergence mechanism and FRR mechanism. In addition, to avoid S-PE single-point failure, one

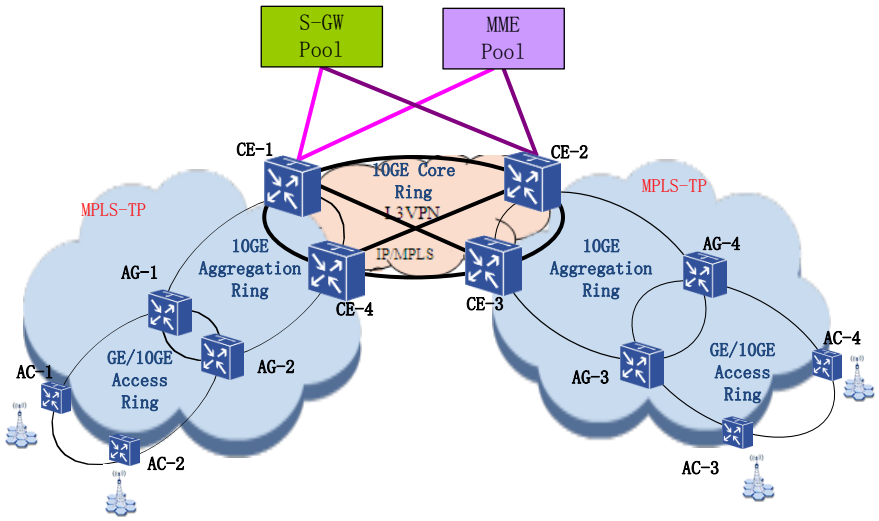
PW/LSP for protection can be configured. This protection PW/LSP does not pass the S-PE mentioned above.

4 Application scenario

4.1 The overlapping interconnection scenario of the L2/L3 VPN bridging in the LTE environment

In most LTE scenarios, the access aggregation deploys the MPLS-TP and the core layer deploys the IP/MPLS. L2/L3 VPN bridging mode can be used to realize the interconnection of two networks.

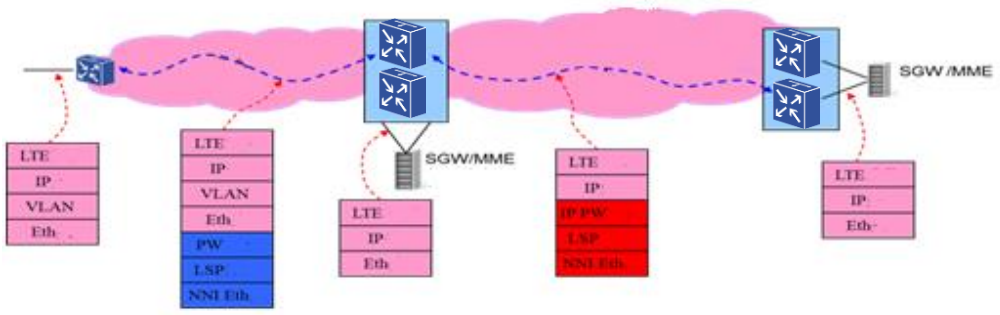
Figure 4-1 The overlapping scenario of the L2/L3 VPN bridging in the LTE environment



As the figure 4-1 shows, the access layer and the aggregation layer use EVPL service to access and converge the S1 and X2 services to the core node. Then core layer devices use te L2/L3 VPN bridging technology to map the EVPL service to one VRF entity. At the same time, the L3VPN in the core layer is used to realize flexible scheduling of the S1 and X2 services to satisfy the LTE bearer requirements.

In the entire forwarding process, the message encapsulation format is as shown in the figure 4-2. The access convergence servies are encapsulated via the L2VPN PW. They are forwarded via the L3VPN. Implement the L2/L3 bridging on the aggregation core boundary node, and finish the interconnection between the MPLS-TP and the IP/MPLS.

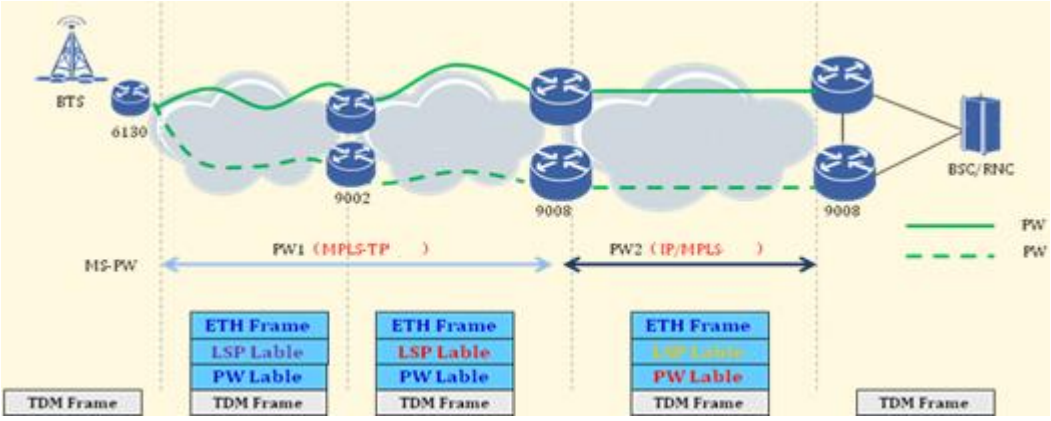
Figure 4-2 The message encapsulation format of the L2/L3 VPN bridging scenario



4.2 The peer-to-peer interconnection scenario in MS-PW environment

If MS-PW is used for implementing the MPLS-TP and the IP/MPLS network interconnection, ZTE MS-PW mechanism includes Dhi PW 3-point bridge solution and MS-PW all-connection redundant protection solution. It gives comprehensive support to the dynamic, static and the hybrid application scenarios.

Figure 4-3 The peer-to-peer interconnection scenario in the MS-PW environment



As the figure 4-3 shows, the access convergence layer deploys MPLS-TP, the core layer deploys IP/MPLS, and the MS-PW is used to interconnect the two networks. In other words, build the corresponding PW fragment in the MPLS-TP and the IP/MPLS networks respectively. Use the aggregation core boundary node as S-PE to stitch the PW fragments at the both sides of the S-PW to one MS-PW. In the PW fragment, the messages can only be sent according to the outer LSP label. On the S-PE, the inner PW label is distributed to the next PW fragment. Check the corresponding LSP information. In this way, the messages are transferred by another network after implementing two-layer label switching on the S-PE.

In the dynamic MS-PW and redundant protection scenarios, MC-APS/MC-LAG, ICCP, and MC-PW APS protocols can be configured on the corresponding devices. Please refer to the *MS-PW Technical White Paper* for the specific information.

5 Abbreviation

Table 5-1 Abbreviation

Abbreviation	Full Name
AC	Attachment circuit
CE	Customer Edge
CP	Control Plane
DP	Data Plane
ETH	Ethernet MAC Layer
ETY	Ethernet Physical Layer
IWF	Interworking Function
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switch Router
MAC	Media Access Control
MEP	Maintenance Association End Point
MIP	Maintenance Association Intermediate Point
MP	Management Plane

Abbreviation	Full Name
MPLS	Multi-Protocol label Switch
NE	Network Element
OAM	Operations, Administration and Maintenance
PE	Provider Edge
PSN	Packet Switched Network
PW	Pseudowire