Layer 1 Virtual Private Networks

- By Tomonori Takeda
takeda.tomonori@lab.ntt.co.jp

MPLS
2004

NTT

Table of Contents

- Motivation and Concept of Layer 1 VPNs
- Service Deployment Scenarios
- Service Models
- Requirements and Applicability of GMPLS
- Standardization

MPLS
2004

NTT

2

- **<u>Motivation and Concept of Layer 1 VPNs</u>**
- Service Deployment Scenarios
- Service Models
- Requirements and Applicability of GMPLS
- Standardization

Current Technologies

- Two major communication models to control optical networks with intelligent control protocols, such as GMPLS.

  - Peer Model: A device communicates with every other devices equally

  - Domain Model: A device communicates less information with external devices, compared to with internal devices (UNI, E-NNI)

MPLS 2004

NTT

Requirements

- It is likely that optical networks in carriers will be shared by multiple service networks
  - Traditionally, a carrier owns one common transport network, and multiple separate service networks (e.g., IPVPN, ISP, Ethernet Private Line)
- It is also expected to be able to provide private network-based L1 services, in addition to simple private line services (currently provided) and BoD (Bandwidth on Demand) services (can be provided by UNI interface)
  - High-speed bandwidth, flexibility to change topology on VPN user's demand easily (dynamically and securely) ….
- These requirements are not explicitly addressed by peer or domain model

MPLS 2004
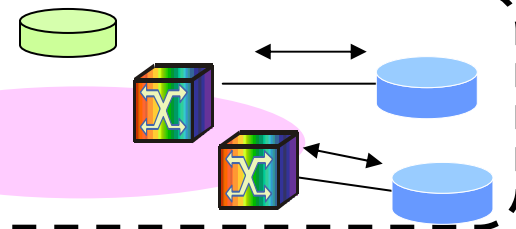
NTT

High Level Concept of L1VPNs

- Logical separation of a L1 network
  - Connectivity restriction: Connectivity is allowed only within the same VPN
  - Per VPN control and management: Control and management is separate per VPN (e.g., addressing, routing, policy)
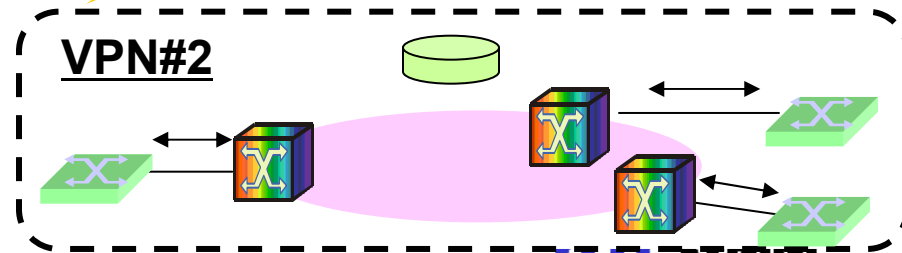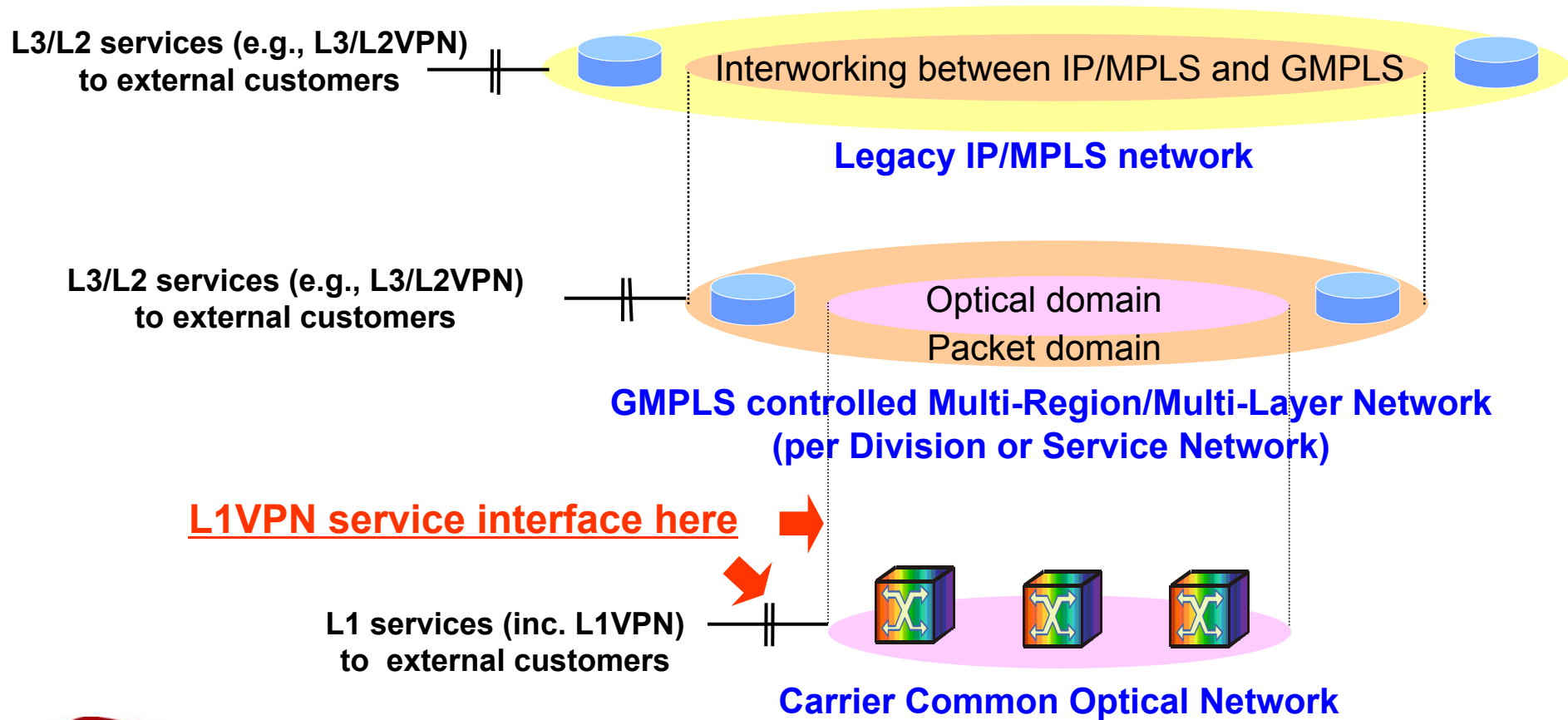
Physical topology

NMS
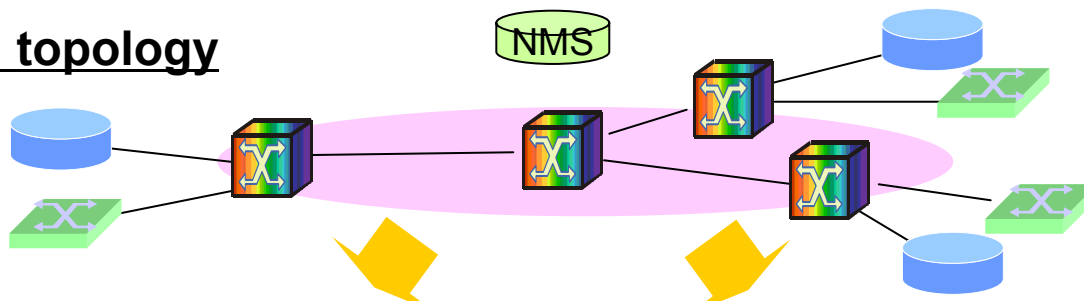
VPN#1

VPN#2

- Motivation and Concept of Layer 1 VPNs
- <u>Service Deployment Scenarios</u>
- Service Models
- Requirements and Applicability of GMPLS
- Standardization

L1VPN Service Applicability

- **L1VPN service's key features**
  - Data plane:
    - L1 interface: High-speed bandwidth, Transparency, Strict QoS (data plane separation from other customers)
  - Control and management plane:
    - L1 topology design on customer's role
    - Dynamic interface

- **L1VPN services suitable for customers who:**
  - Want to build own optical networks
  - But do not want to pay full cost for CAPEX and OPEX
  - Usually, large organization, requiring L1 control and management functionalities

Possible Future Carrier Network Architecture

L3/L2 services (e.g., L3/L2VPN) to external customers

Interworking between IP/MPLS and GMPLS

Legacy IP/MPLS network

L3/L2 services (e.g., L3/L2VPN) to external customers

Optical domain

Packet domain

GMPLS controlled Multi-Region/Multi-Layer Network (per Division or Service Network)

<u>**L1VPN service interface here**</u>

L1 services (inc. L1VPN) to external customers

Carrier Common Optical Network
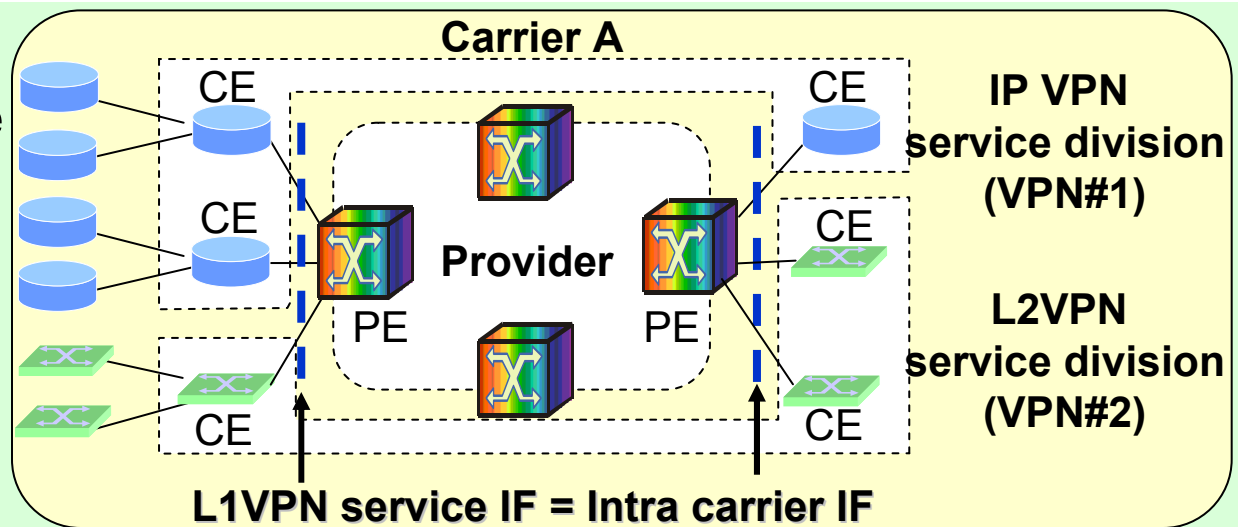
L1VPN Usages

External usage
= Carrier's Carrier

- L1 network wholesale to other carriers
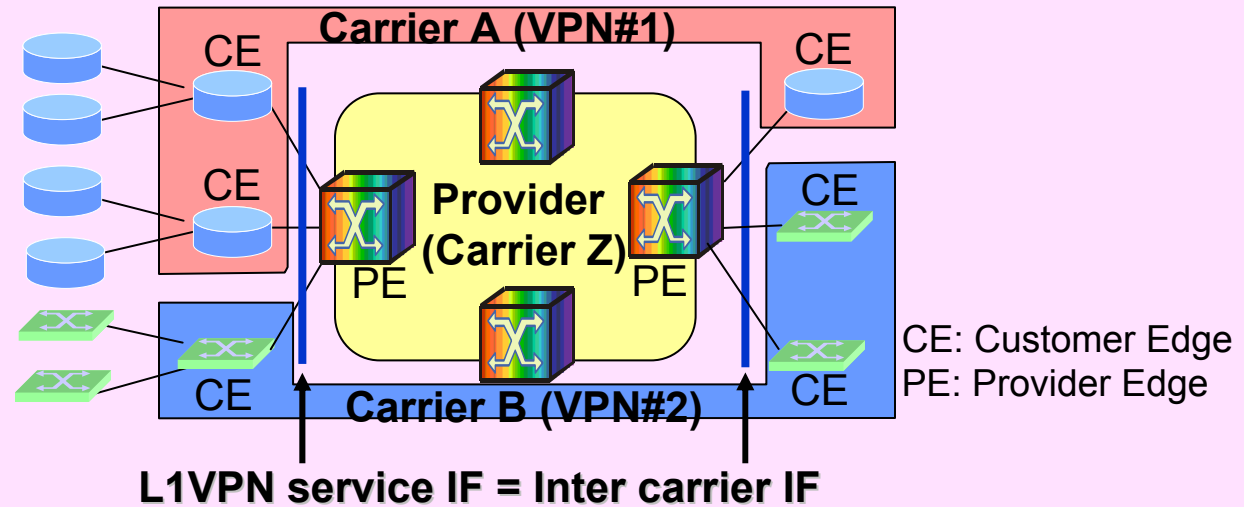
Internal usage
= Multi service backbone

- Support of multiple services within the same carrier

Carrier A (VPN#1)

Provider (Carrier Z)

Carrier B (VPN#2)

CE: Customer Edge
PE: Provider Edge

L1VPN service IF = Inter carrier IF

Carrier A

Provider

IP VPN service division (VPN#1)

L2VPN service division (VPN#2)
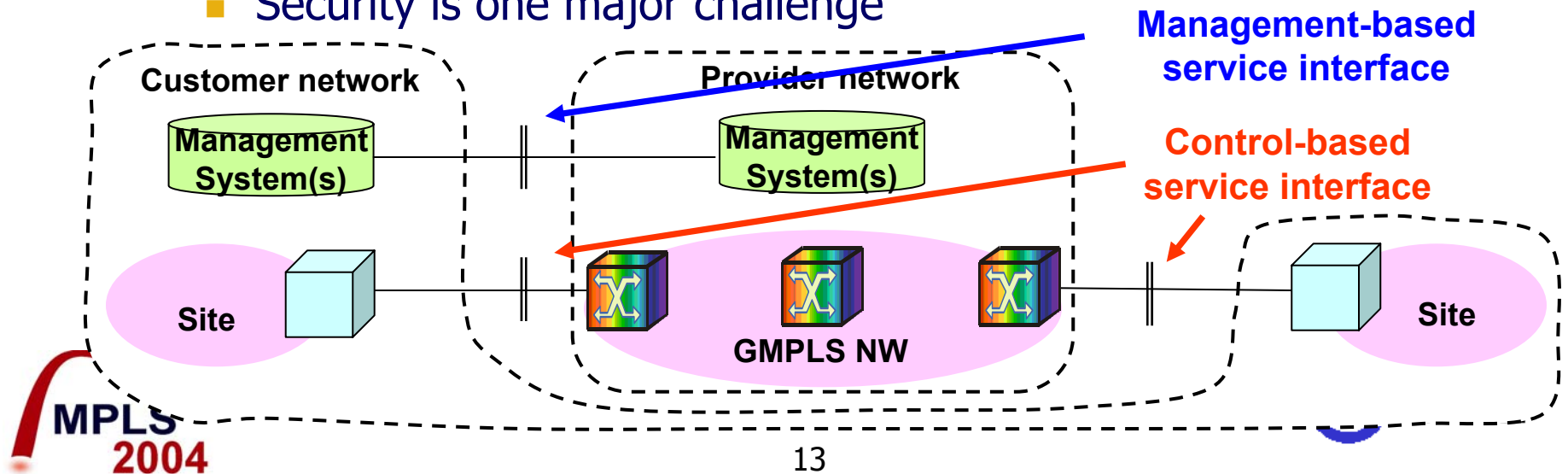
L1VPN service IF = Intra carrier IF

- Motivation and Concept of Layer 1 VPNs
- Service Deployment Scenarios
- <u>Service Models</u>
- Requirements and Applicability of GMPLS
- Standardization

Overview of L1VPN Service Models

- Types of service interface
  - Management-based: e.g., http
  - Control-based: e.g., signaling
- Functions over the service interface (in control-based service interface)
  - Signaling-based
  - Signaling and routing
- In real commercial networks, it will be desired that multiple service models are supported (for various customers needs)
  - Management-based service model as supporting non-GMPLS capable networks
  - Signaling and routing service model as supporting GMPLS capable networks

Management-based / Control-based

- Management-based
  - Can support legacy networks (non-GMPLS capable networks)
- Control-based
  - Fast failure notification
  - Seamless operation: If a customer network is GMPLS-based, a VPN can be controlled by GMPLS end-to-end
  - Security is one major challenge

Signaling-based / Signaling and Routing

- Signaling-based
  - Limited functionalities
- Signaling and routing (CE-PE VPN routing)
  - Complete end-to-end GMPLS operation of a VPN
    - Traffic engineering
    - Disjoint end-to-end LSPs
    - LSPs between devices inside customer sites

Customer network

Provider network

Site

GMPLS NW

Site
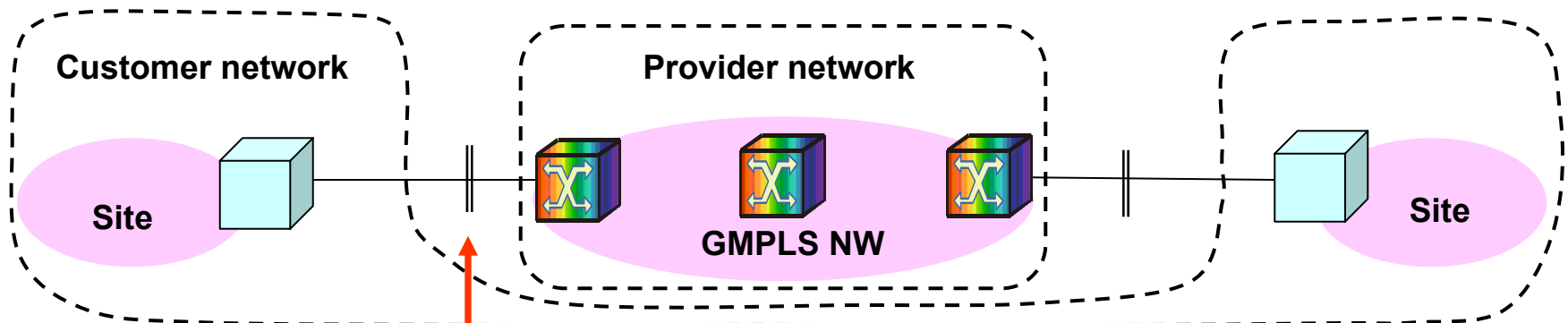
Signaling-based
Signaling and routing

MPLS 2004

NTT

- Motivation and Concept of Layer 1 VPNs
- Service Deployment Scenarios
- Service Models
- <u>Requirements and Applicability of GMPLS</u>
- Standardization

Key Requirements of L1VPNs

- Private address support
- Connectivity restriction
- Auto-discovery
- CE-PE VPN routing
- Resource management per VPN
- Security

- Remarks on protocol design:
  - CE-PE protocols should be simple (hopefully no L1VPN specific protocol enhancement)
  - Protocols should be maximally reused for various service models

Applicability of GMPLS to L1VPNs

- Two solution IDs relevant to L1VPNs
  - GMPLS UNI (Overlay) draft-ietf-ccamp-gmpls-overlay
    - Supports VPN connection establishment by using FA-LSP concept
  - GVPN (Generalized VPN) draft-ouldbrahim-ppvpn-gvpn-bgpgmpls
    - Applies BGP-based auto-discovery and GMPLS protocols
    - Supports CE-PE VPN routing by using Virtual Router concept
- These two IDs provide sufficient level of baseline specifications for L1VPNs, but there are additional work areas to meet requirements

Possible Additional Work Areas

- Resource management per VPN
  - Management of resources a VPN can use (shared/dedicated)
  - Solution approach: Routing extensions, or policies
- Enhancement of CE-PE VPN routing
  - Leakage of dedicated portion of the provider network to CEs
  - Solution approach: Routing extensions
- Areas existing solution IDs are not explicitly mentioning
  - PE-PE control channel (should be logically separate per VPN)
- etc.

- One question: Is it reasonable to implement BGP in OXC ?
  - For auto-discovery, reachability exchange, CE-PE routing ??
  - Alternatives: IGP (OSPF), Server ….
- Inter-domain discussion may be relevant
  - Use of BGP, security (confidentiality) …

MPLS 2004

NTT

- Motivation and Concept of Layer 1 VPNs
- Service Deployment Scenarios
- Service Models
- Requirements and Applicability of GMPLS
- <u>Standardization</u>

Standardization Efforts of L1VPNs

- Service requirements and high level architecture done in ITU-T SG13
- Framework ID submitted to the IETF based on SG13 documents
    - Motivation, concept, service scenarios, service models, etc.
- Applicability ID submitted to the IETF
    - To show how existing GMPLS can be applied
    - To show possible additional work areas for enhancement
- Protocol work is expected to follow
- Discussion in the L1VPN Mailing List, under the care of CCAMP WG
    - https://www1.ietf.org/mailman/listinfo/l1vpn
- Possibility to be added to a new CCAMP charter item

MPLS 2004

NTT