iPOP 2005
IP+Optical Network

Layer 1 Virtual Private Networks: Driving Forces and Current Status

Tomonori Takeda, NTT
takeda.tomonori@lab.ntt.co.jp

Table of Contents

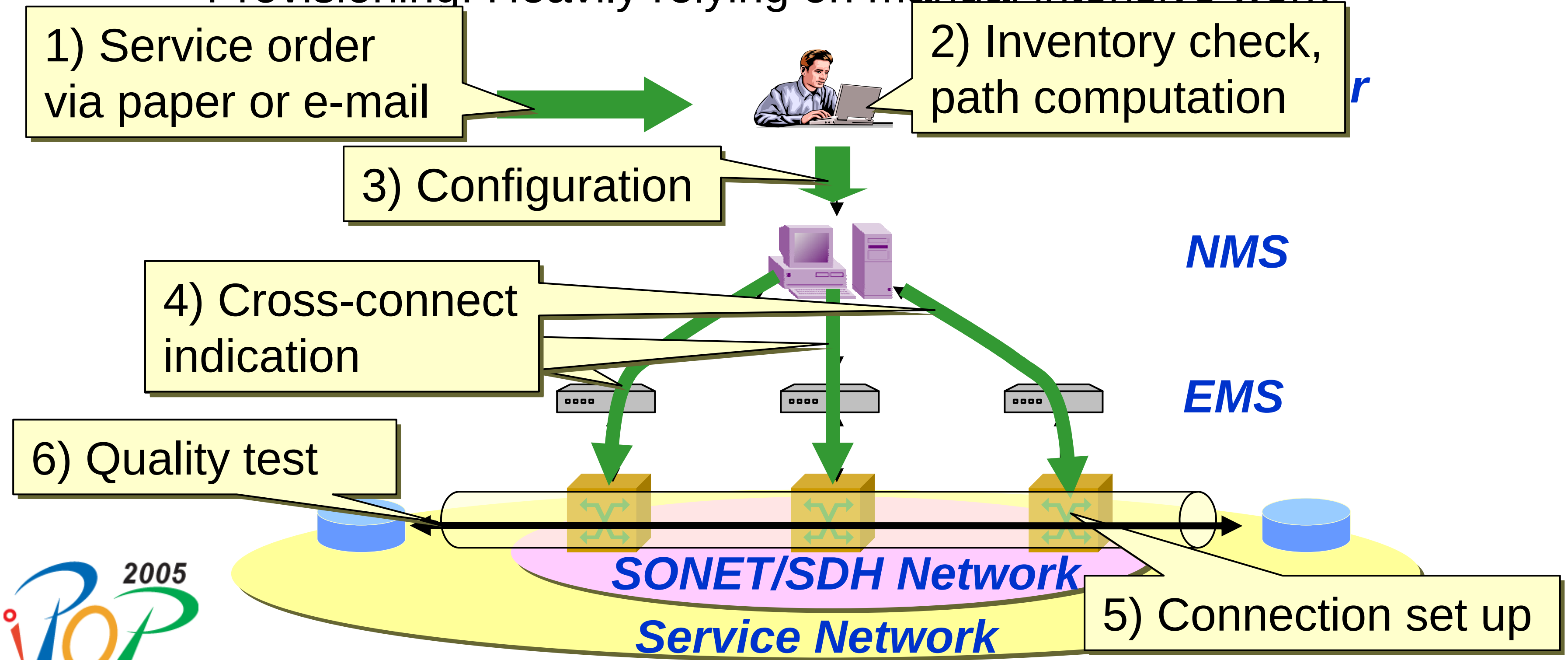
- Background
    - Requirements for Transport Network
    - Solution Approach
- Overview of L1VPNs
    - Concept
    - Impact on Operations
- Key Technical Areas and Current Status
    - Control Plane
    - Management Plane

Table of Contents

- Background
  - Requirements for Transport Network
  - Solution Approach
- Overview of L1VPNs
  - Concept
  - Impact on Operations
- Key Technical Areas and Current Status
  - Control Plane
  - Management Plane

Traditional Transport Network

- Limited in flexibility, slow in provisioning
  - Network architecture: SONET/SDH controlled by proprietary NMS/EMS
  - Service order: By paper or e-mail
  - Provisioning: Heavily relying on manual intensive work



1) Service order via paper or e-mail

2) Inventory check, path computation

3) Configuration

4) Cross-connect indication

5) Connection set up

6) Quality test

Requirements

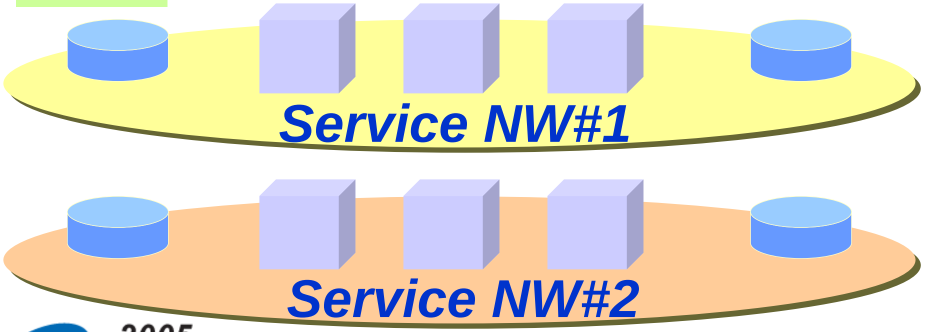
- Faster operation
  - Slow provision for increasing traffic = loss of business
- Support of unforeseen traffic increase
  - Difficult to predict when and where additional capacity is required
- Cost reduction
  - Carriers are facing more and more severe competition

- GMPLS suite of protocols realize dynamic, automatic provisioning, with standardized mechanisms

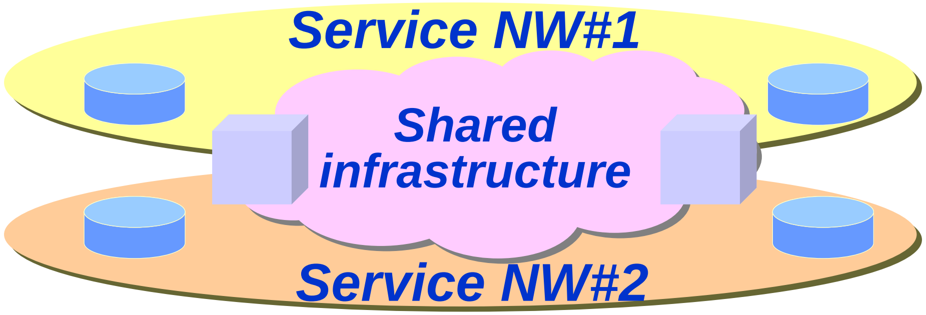
Network Model

- Separate transport network model (“Peer model”)
  - Early deployment ?
- Shared transport network model among/within carriers (“VPN”)
  - Common in large carrier networks
  - Promising
    - CAPEX/OPEX reduction
    - Risk reduction (Unforeseen future traffic increase in service networks can be multiplexed)

Peer



VPN



Transport Technologies

IP/MPLS	Layer 1 (optical, SONET/SDH)
Fine granularity (continuous capacity increase)	Coarse granularity (discrete capacity increase)
Flexibility by packet transport nature (capacity change between any pair of sites)	Flexibility by GMPLS
Packet level traffic separation	Hard traffic separation (strict QoS)
Difficulty in supporting L1 technologies	Support of any client signal → Further multiplexing
Concern on feasibility for “big fat router”	Expected to be feasible for huge capacity

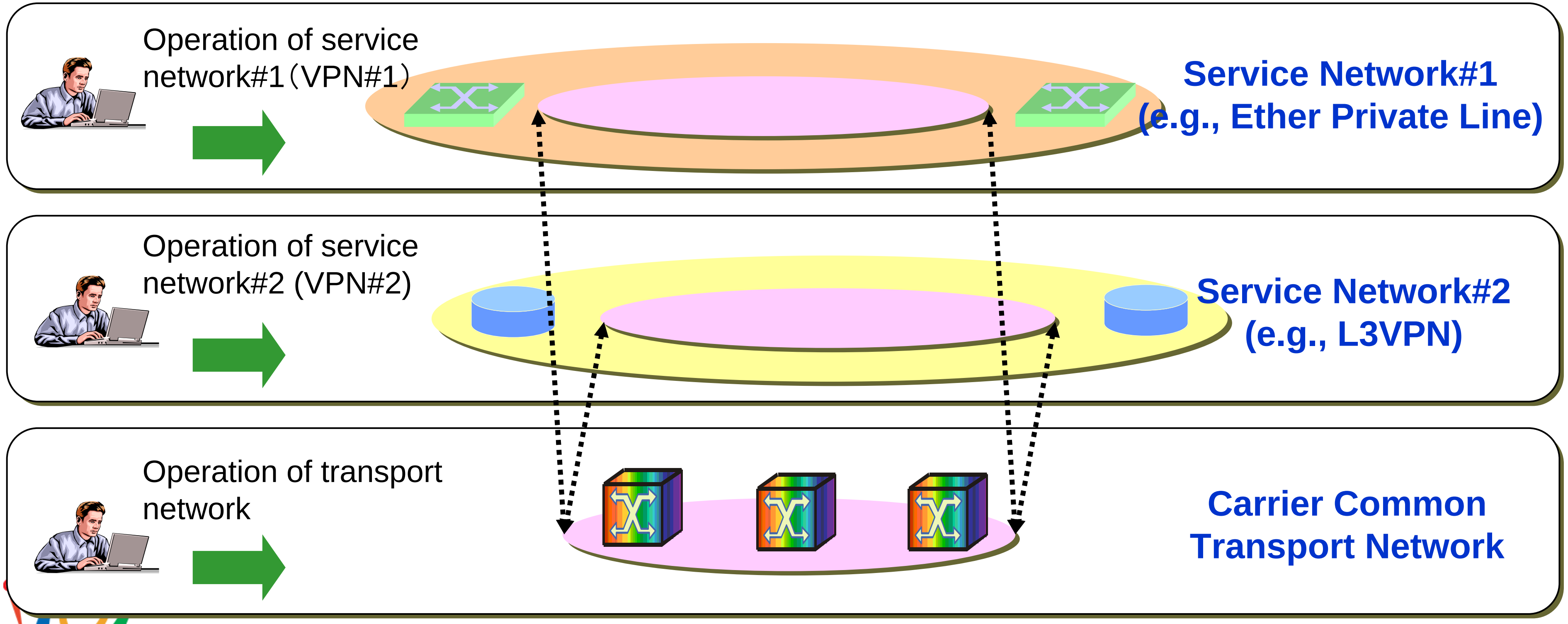
Better for massive bandwidth

Table of Contents

- Background
  - Requirements for Transport Network
  - Solution Approach
- Overview of L1VPNs
  - Concept
  - Impact on Operations
- Key Technical Areas and Current Status
  - Control Plane
  - Management Plane

Concept of L1VPNs

- Enables dynamic, automatic L1 connection provisioning, over shared L1 network
- Progressively applies standardized mechanisms (i.e., GMPLS)



Operation of service network#1（VPN#1）

Service Network#1 (e.g., Ether Private Line)

Operation of service network#2 (VPN#2)

Service Network#2 (e.g., L3VPN)

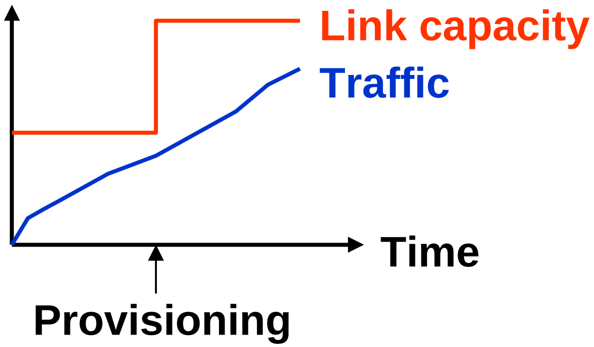
Operation of transport network

Carrier Common Transport Network

Example Application Scenarios

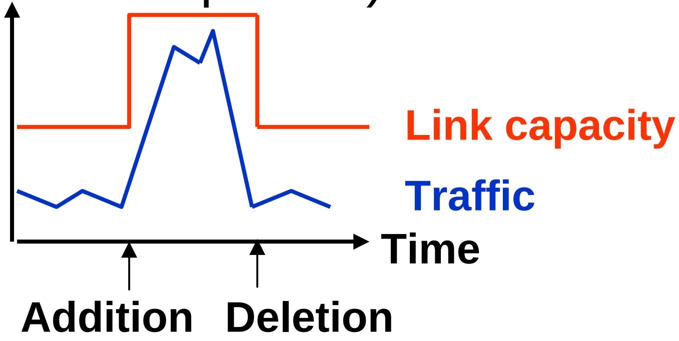
Provisioning

- Mid-to-Long term traffic increase



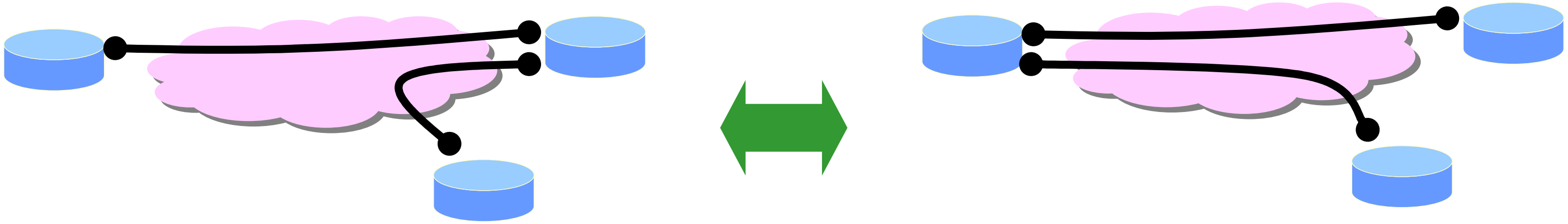
Tentative capacity addition

- Tentative traffic (e.g., by failure, or tentative traffic pattern)



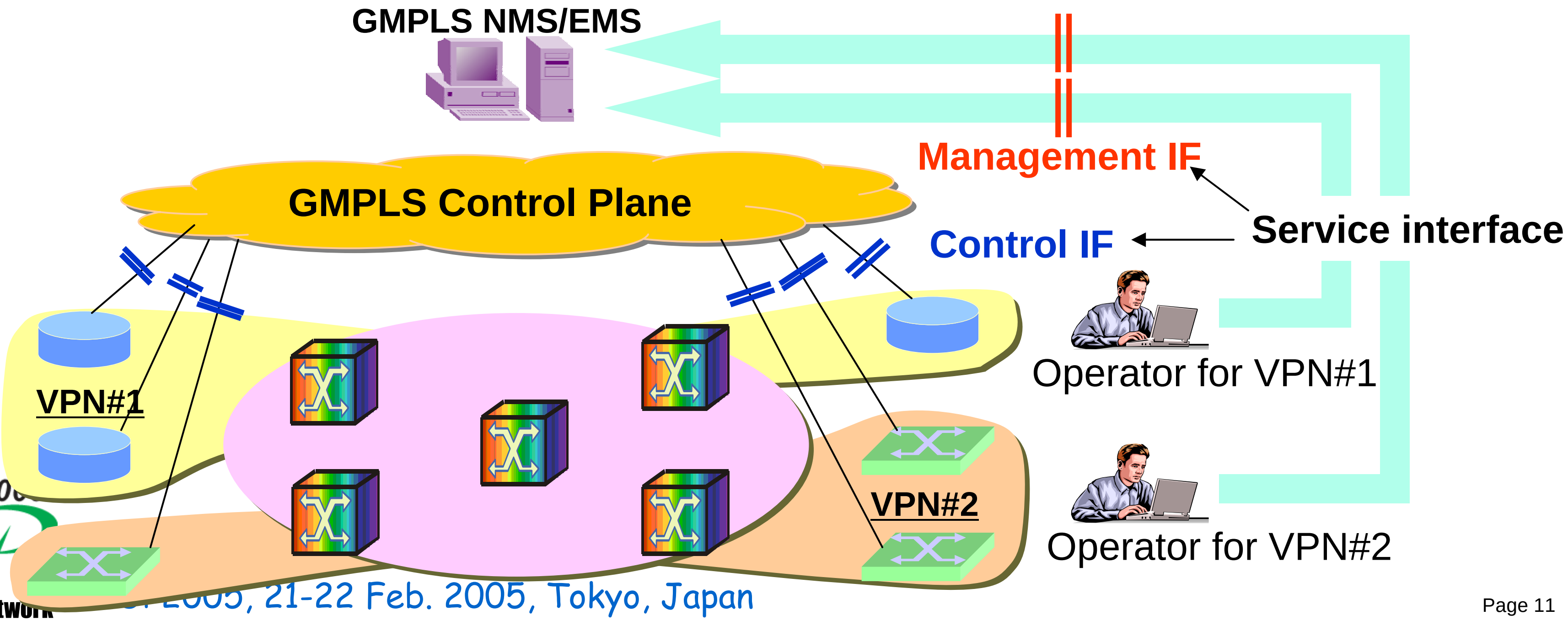
Dynamic topology reconfiguration

- Noon-to-night traffic variation



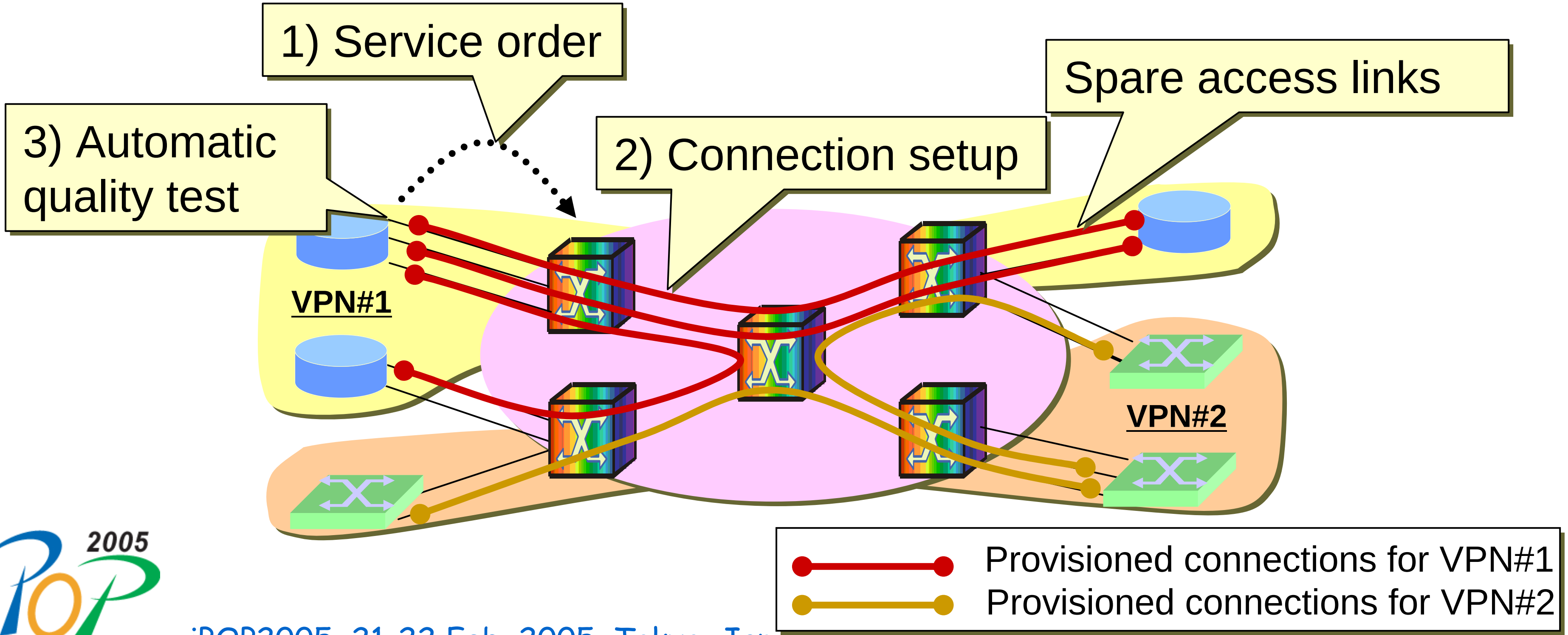
L1VPNs Service/Architectural Models

- Network control and management
  - Virtual separation of L1 network controlled and managed by GMPLS
- Service interface
  - Control plane and/or Management plane
- Factors for consideration
  - GMPLS usage, trust relationship, etc



Impact on Operations

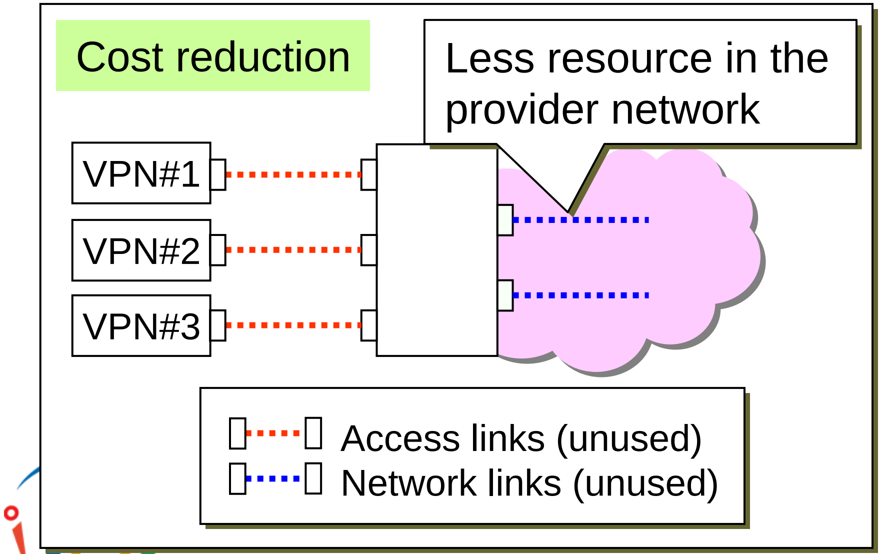
- Operation transition by dynamic, automatic provisioning
  - Spare access links (including hardware package order and installation)
  - Automatic provisioning without human interruption



1) Service order
3) Automatic quality test
2) Connection setup
Spare access links
VPN#1
VPN#2
Provisioned connections for VPN#1
Provisioned connections for VPN#2

Analysis

- Is it economically feasible to prepare spare access links?
  - If traffic is growing rapidly, this is a MUST
- Then, why you wait and rely on dynamic provisioning, rather than set up a connection at that time?
  - Cost reduction: Resource reduction in the provider network, low-cost service
  - Flexibility: For traffic increase between arbitrary pair of sites (“VPN” service)
- If access links are cheap, or have multiplexing capabilities (e.g., WDM IF, Channelized IF), makes more sense

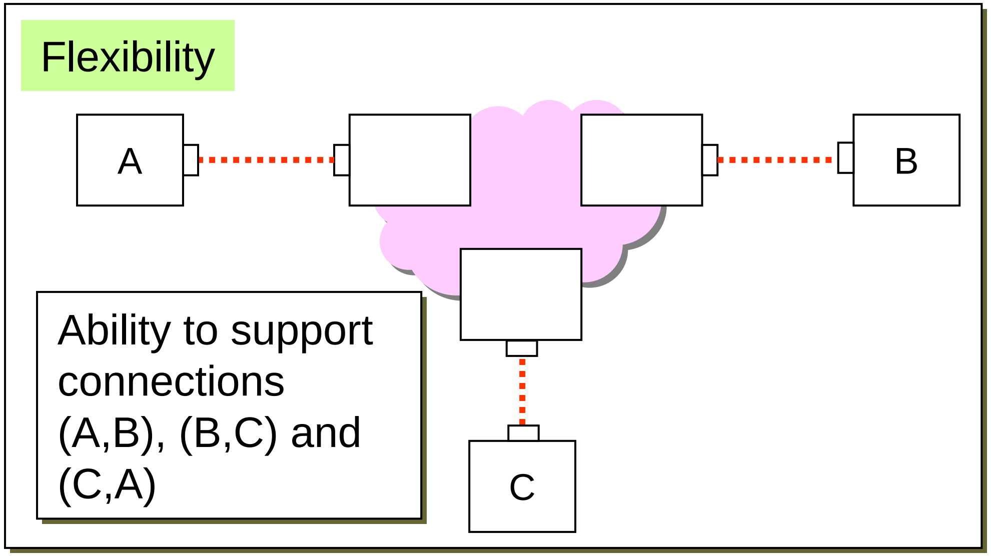


Cost reduction

Less resource in the provider network

Access links (unused)

Network links (unused)



Flexibility

Ability to support connections (A,B), (B,C) and (C,A)

Table of Contents

- Background
  - Requirements for Transport Network
  - Solution Approach
- Overview of L1VPNs
  - Concept
  - Impact on Operations
- Key Technical Areas and Current Status
  - Control Plane
  - Management Plane

Key Technical Areas

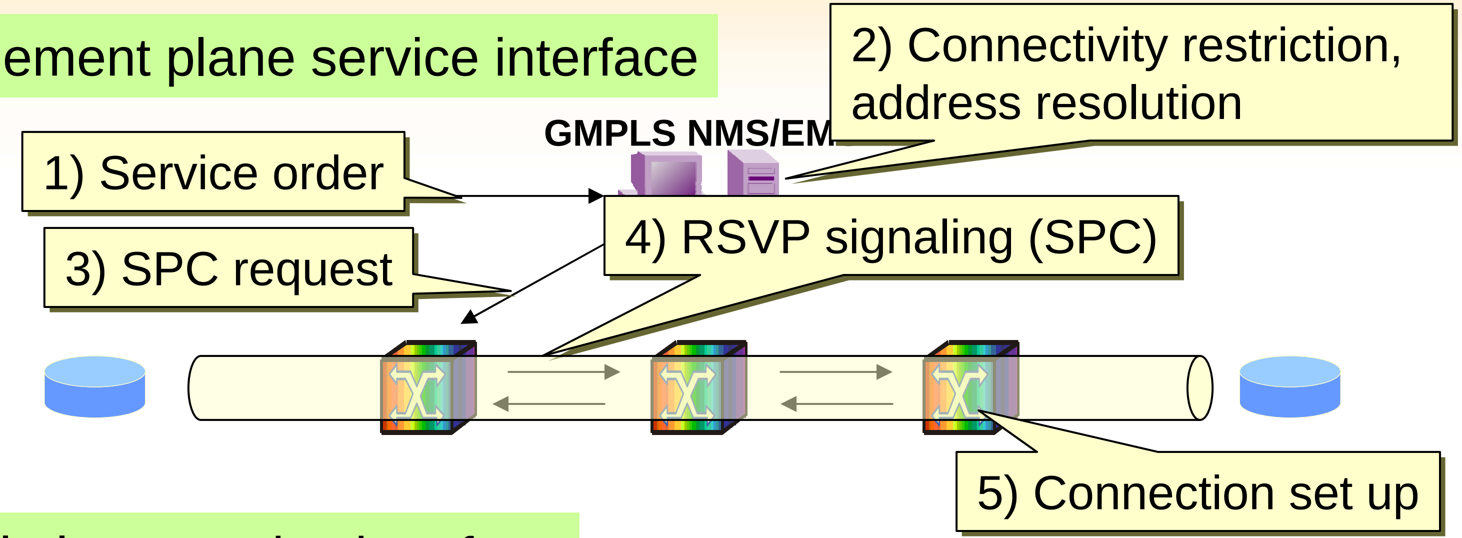
- Control Plane
  - Interface definition, protocol specifications
- Operation and Management Functionalities
  - Automatic quality test tool
  - Network planning tool
    - When to upgrade network
  - Service management
    - Security/Confidentiality
    - Accounting

Control Plane

- Various types of interface definition, depending on trust relationship and customer requirements in ITU-T and IETF
  - Management plane service interface
    - Management-based service model
  - Control plane service interface
    - Signaling-based service model
    - Signaling and routing service model
- Various pieces of existing GMPLS protocols, on-going discussion for a common framework and further enhancement in IETF
  - L1VPN framework (draft-takeda-l1vpn-framework)
  - L1VPN applicability (draft-takeda-l1vpn-applicability)
  - GMPLS UNI (draft-ietf-ccamp-gmpls-overlay)
  - GVPN (draft-ouldbrahim-ppvpn-gvpn-bgpgmpls)
- Some early testing accomplished in interoperability test event

GMPLS usage for L1VPNs

Management plane service interface



GMPLS NMS/EM

1) Service order

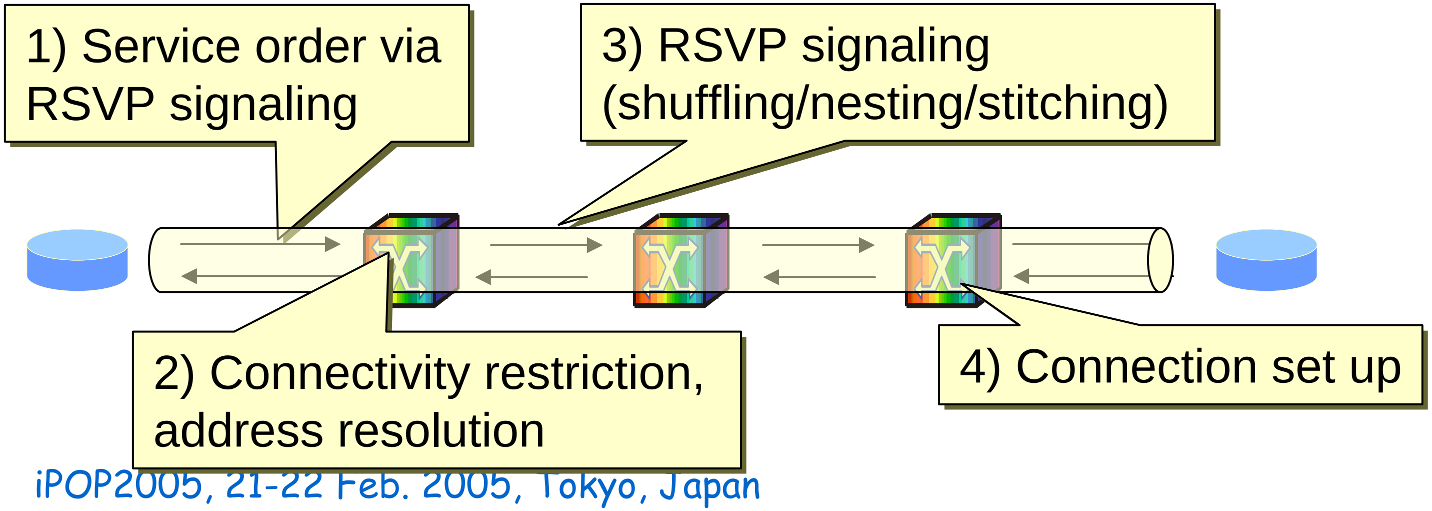
2) Connectivity restriction, address resolution

3) SPC request

4) RSVP signaling (SPC)

5) Connection set up

Control plane service interface



1) Service order via RSVP signaling

2) Connectivity restriction, address resolution

3) RSVP signaling (shuffling/nesting/stitching)

4) Connection set up

Thank you !

Please visit the exhibition booth (@NTT) for demos and additional information