MPLS Path Management

Ikuo Nakagawa, Intec NetCore, Inc.

Feb., 2005

Presentation Outline

- Background
  - MPLS is / will be de facto standard of “carrier class” backbone
  - To build a reliable & stable multi-service network
  - MPLS may be the best solution, at this moment
  - On the other hand, there are lots of issues to operate MPLS network

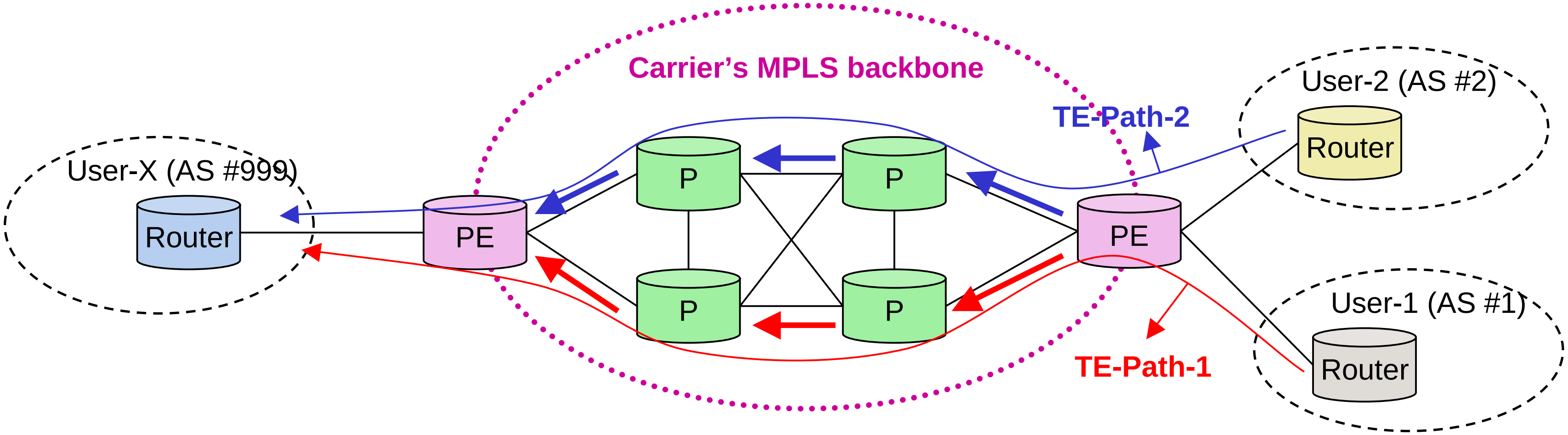
- In this presentation, we introduce
  - MPLS deployment cases
    - Cutting edge implementation cases
  - MPLS trend
    - as multi-service platform
    - requirements for MPLS network
    - issues in MPLS network operation
  - MPLS network management model
    - Concept of **“MPLS path management”**
    - Correlation mechanism based on “path”
    - Hierarchical MPLS path management

Agenda

- MPLS deployment
  - Internet
  - IP-VPN
  - L2-VPN
  - LSP service
  - Protection
- MPLS today
  - Multi-service platform
  - Requirements for MPLS network
  - Issues in MPLS network management
- MPLS network management model
  - Concept of MPLS path management
    - Provisioning
    - Assurance
    - Usage
  - Correlation in MPLS path management
  - Hierarchical MPLS path management
- Conclusion

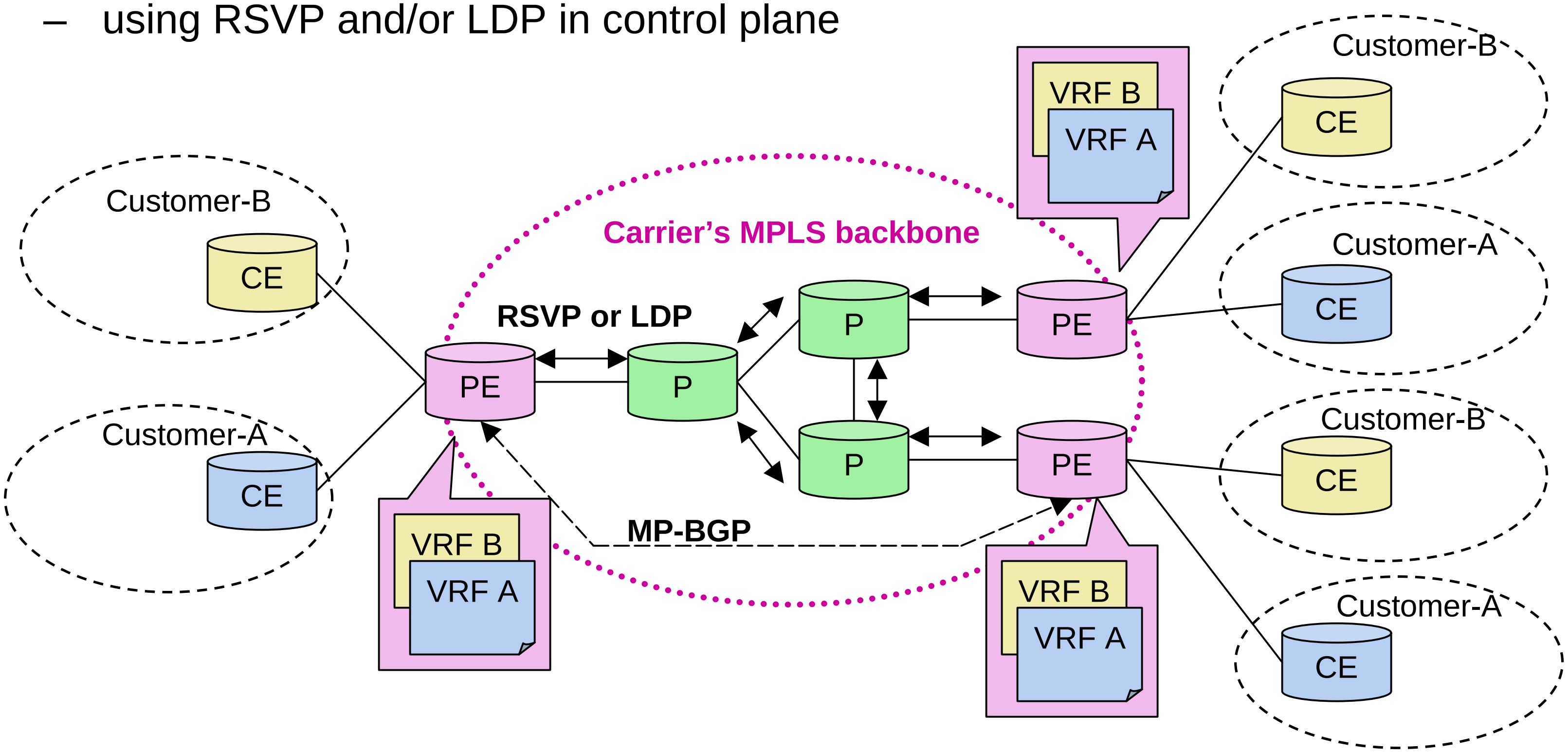
MPLS deployment: Internet

- Outline:
  - Using MPLS in the ISP’s backbone, for TE (traffic engineering).
  - Nowadays, protection (FRR, etc) is also useful.
- Protocols:
  - RSVP-TE
- Example:
  - To control traffic flow in ISP’s backbone, e.g.,
  - even if User-1 / User-2 are sending traffic to the same destination User-X
  - traffic from User-1 are transmitted through TE-Path-1 and
  - traffic from User-2 are transmitted through TE-Path-2, respectively
  - to split high volume traffic into different paths



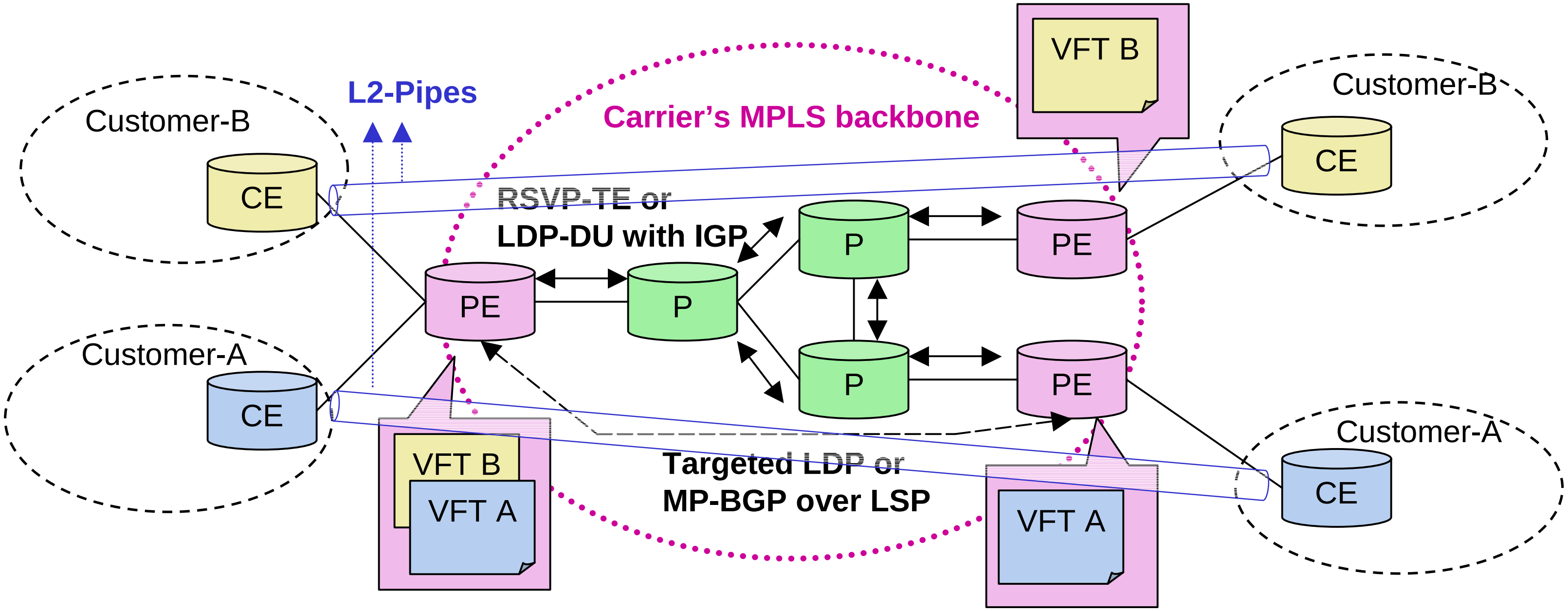
MPLS cases: IP-VPN

- Outline:
  - IP-VPN (aka MPLS-VPN) is well known application of MPLS.
  - Providing multiple virtual user network over the MPLS network.
- Protocols:
  - RFC2547bis, LDP (PE-PE), RSVP-TE (Core), and so on.
- Example:
  - Carrier's MPLS backbone provides 2 individual VPN
  - using MP-BGP between PE-PE to exchange user routes
  - using RSVP and/or LDP in control plane



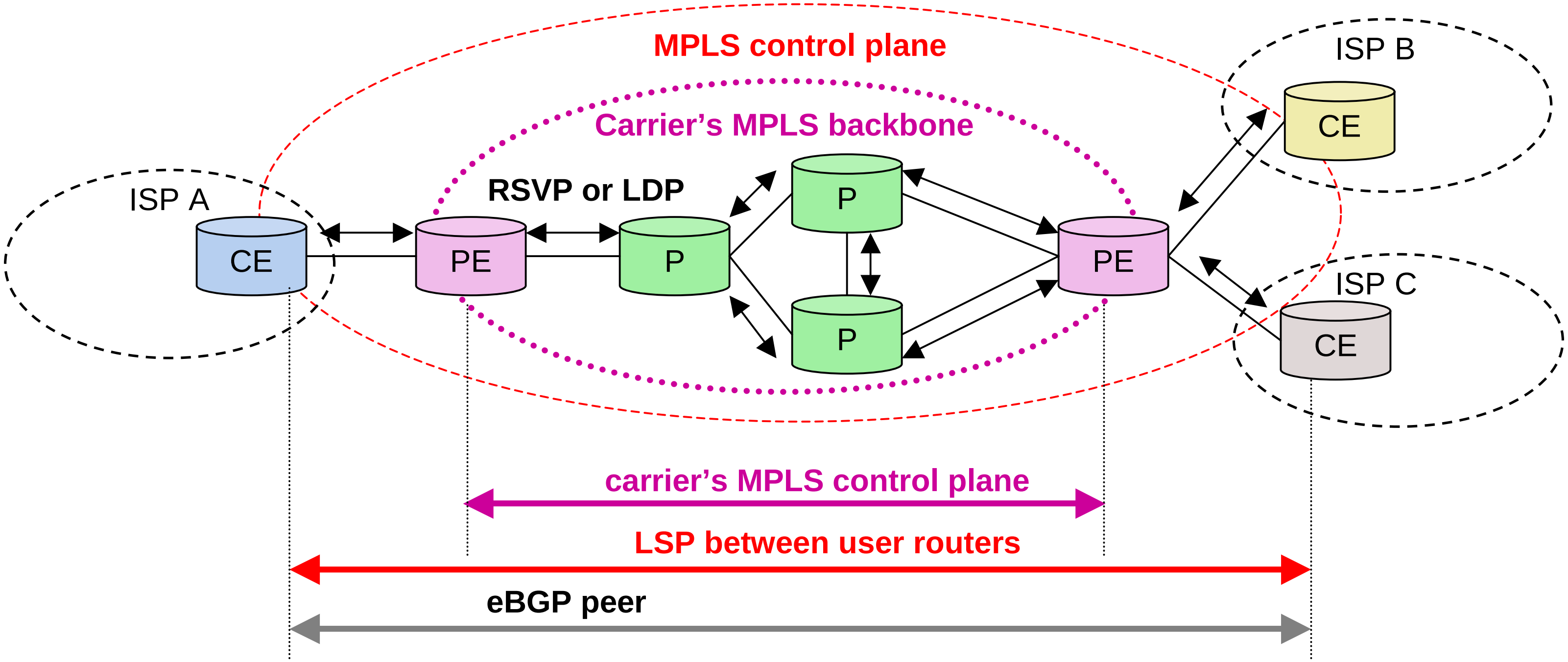
MPLS deployment: L2-VPN (EoMPLS, VPLS)

- Outline:
  - Providing layer 2 (Ethernet) services over MPLS.
  - Customers can use L2-pipe via MPLS network.
- Protocols:
  - Martini or Kompella over LDP/RSVP-TE.
- Example:
  - Carrier’s MPLS network provides 2 L-2 (Ethernet) pipes
  - using RSVP-TE and/or LDP in P and PE routers
  - using Targeted LDP or MP-BGP to establish L2 circuites



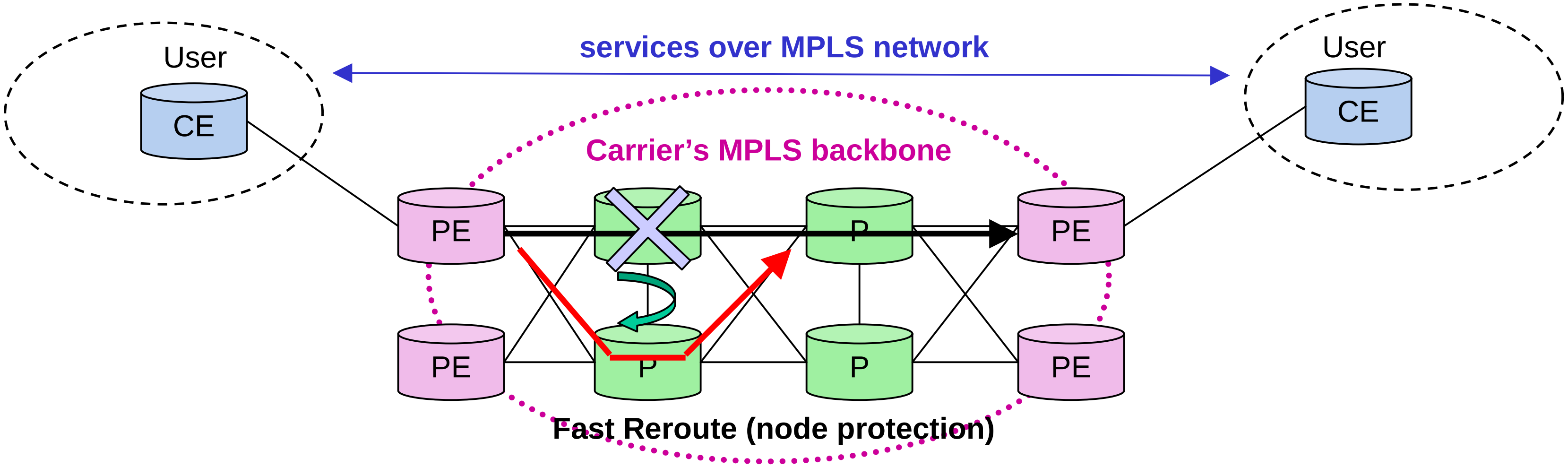
MPLS deployment: LSP service

- Outline:
  - Providing LSP between user routers. (aka MPLS-IX)
  - user routers establish LSP and eBGP peer between each other
  - user can exchange full routes (carrier does NOT care about routes)
- Protocols:
  - RFC2547bis, LDP, RSVP-TE (Core)
- Example:
  - Carrier’s MPLS backbone provides LSP between user ISPs
  - Using RSVP or LDP between P and PE
  - Using LDP between user routers



MPLS deployment: Protection

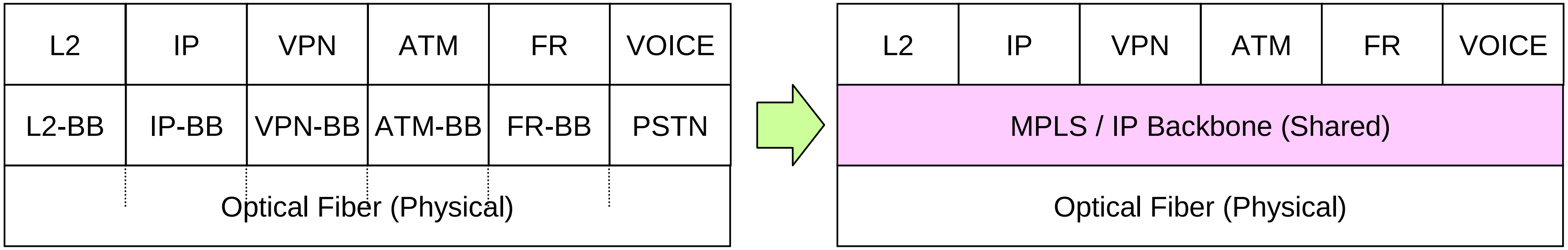
- Outline:
  - Mainly used in backbone
  - Protect a LSP by pre-defined backup LSP
  - 3 types: path protection, node protection, link protection
  - changing path to pre defined backup LSP makes service downtime shorter.
- Protocols:
  - RSVP-TE (Core), FRR and so on.
- Example:
  - User's services (IP, IP-VPN, L2-VPN and so on) are provided over protected LSPs
  - a LSP (black) has pre defined backup LSP (red)
    - with node protection, in this example
  - In case of router failure, path change occurs (to red path)



Fast Reroute (node protection)

MPLS today

- MPLS is de fact standard for multi-service platform
  - MPLS allows to provide
    - Internet (normal IP traffic with or without TE)
    - IP-VPN / L2-VPN / LSP service
    - ATM / FR
  - Migration legacy services with MPLS technology
    - Single “MPLS” backbone provide multi-services
    - Migrate not only IP or IP-VPN but also Ethernet, ATM, FR, etc
    - Carriers’ class reliability with MPLS
      - “Protection” technology provides reliable data-path
    - Sharing bandwidth in backbone
      - MPLS backbone is a packet network
      - TE (Traffic Engineering) enable bandwidth control for services.



L2	IP	VPN	ATM	FR	VOICE
L2-BB	IP-BB	VPN-BB	ATM-BB	FR-BB	PSTN
Optical Fiber (Physical)					

L2	IP	VPN	ATM	FR	VOICE
MPLS / IP Backbone (Shared)					
Optical Fiber (Physical)					

Operation and Management of “MPLS” Core backbone is Key in the next generation!

MPLS today

- Requirements for MPLS network
  - MPLS network has a lot of requirements
  - Because, it has to provide multi-services, e.g.,
    - Internet
      - bandwidth, bandwidth and bandwidth
        >>> fat pipe
    - IP-VPN / L2-VPN / LSP service
      - latency should be same as light speed
        >>> network topology
      - down time should be < 1[sec] in case of trouble
        >>> protection
    - ATM or FR
      - latency and jitter are critical to emulate services
        >>> network topology and queue mechanism
      - shorter down time is also required, < 50[ms] in case of trouble
        >>> protection

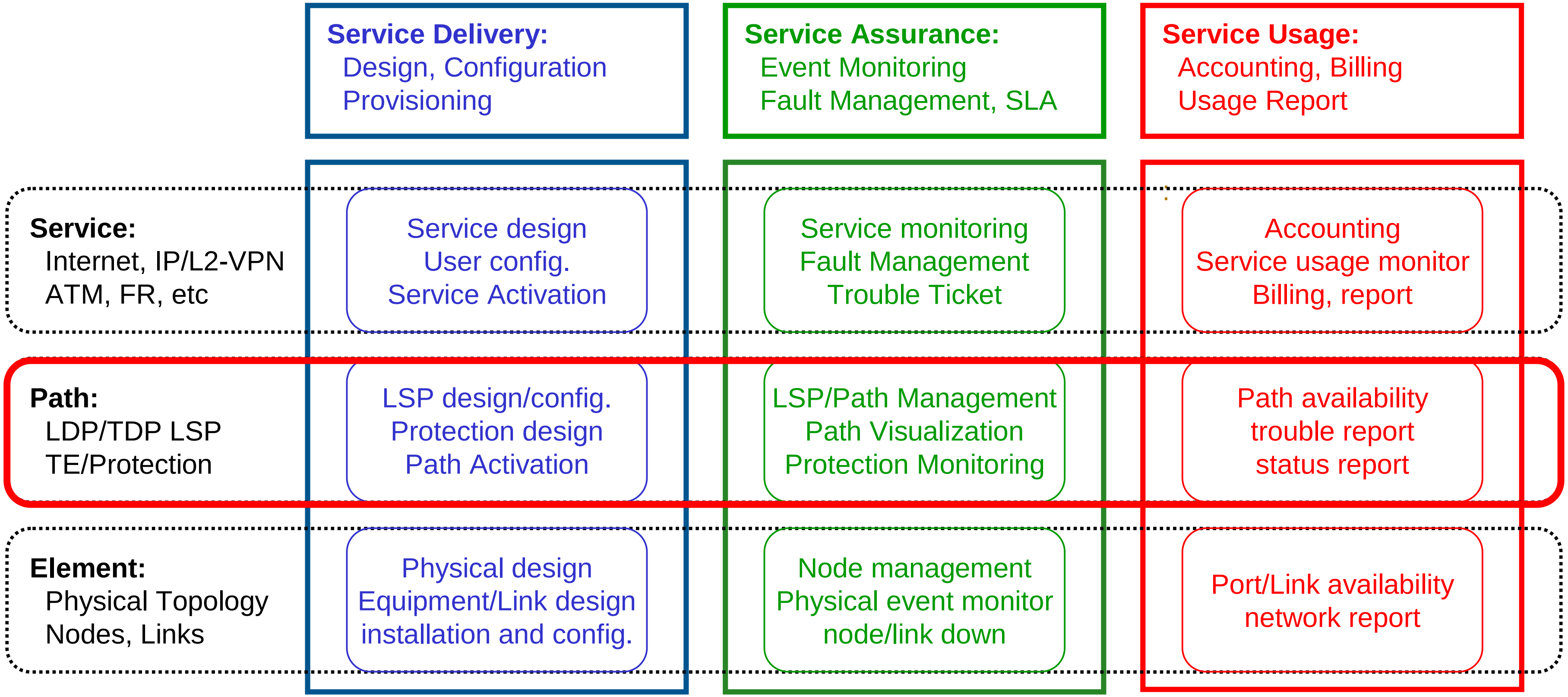
MPLS today

- Issues for managing “Path” in MPLS network
  - design “path” resources for traffic engineering is also a key
    - God hand?
      - Just “a” key guy in a network can design path” resources
    - Both of bandwidth and protection simulation is required
      - But, it is hard to implement “God hand”
  - operators have very few method to see “paths”
    - operators always “walk through CLI” to manage “path”
      - with a lot of human resources!
    - even MPLS ping / MPLS trace do not provide enough information
      - it provides only aliveness of a LSP
    - In other words, less tools exists to manage MPLS “network”
      - need visualization and a kind of database
  - operators do NOT have much information about:
    - relationship between services and “path” (service)
      - hard to check IP-VPN information on LSP
    - relationship primary “path” / backup “path” (protection)
      - hard to check backup path status
    - relationship “path” and physical links
      - hard to visualize MPLS “path” w/ several information

Do operators need to “walk through CLI”?

MPLS network management model

- Action matrix for MPLS network management (outline)
  - 3 actions: provisioning, assurance and usage
  - 3 layers: service, path and element
- “Path” management is most important in MPLS network
  - Elements generate **paths** for data traffic
  - Any service is bound to a **path** on MPLS network



	Service Delivery: Design, Configuration Provisioning	**Service Assurance:** Event Monitoring Fault Management, SLA	**Service Usage:** Accounting, Billing Usage Report
Service: Internet, IP/L2-VPN ATM, FR, etc	Service design User config. Service Activation	Service monitoring Fault Management Trouble Ticket	Accounting Service usage monitor Billing, report
Path: LDP/TDP LSP TE/Protection	LSP design/config. Protection design Path Activation	LSP/Path Management Path Visualization Protection Monitoring	Path availability trouble report status report
Element: Physical Topology Nodes, Links	Physical design Equipment/Link design installation and config.	Node management Physical event monitor node/link down	Port/Link availability network report

Path Provisioning

- Backbone provisioning
  - implementation of a new network or changing the network
  - P and PE routers
  - inventory, topology, signaling, IGP/BGP, etc.
  - design & simulation of the network topology
    - simulation of paths and their backup paths to reroute
    - bandwidth parameters for each links or paths
    - even when, changing or upgrading interfaces / circuits
  - configuration
    - generating router commands & consistency check
    - installation of router commands
  - etc

- Service provisioning – for Service Order (SO)
  - adding a new customer or deleting a customer
  - PE and CE (for managed services) routers
  - several steps for each services (IP-VPN, L2-VPN, ATM, FR, etc)
  - configuration of user services
    - basic IP connectivity, signaling, IGP/BGP, VRF, VC
    - defining services parameters such as QoS/CoS, bandwidth, etc
  - configuration
    - generating router commands & consistency check
    - installation of router commands
  - etc

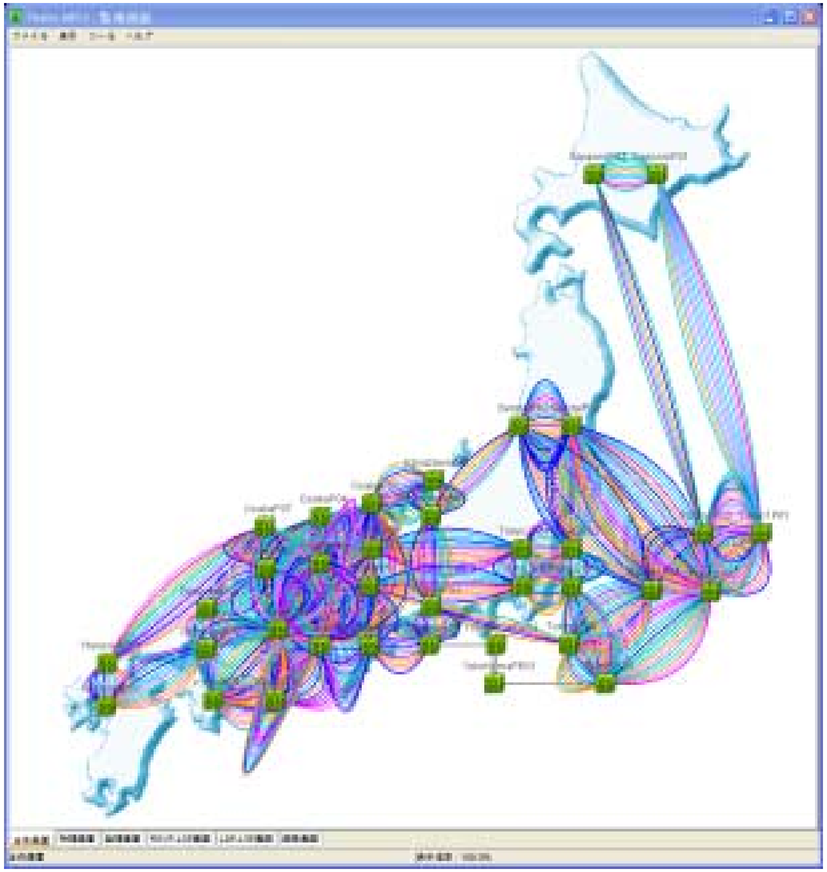
Path Assurance

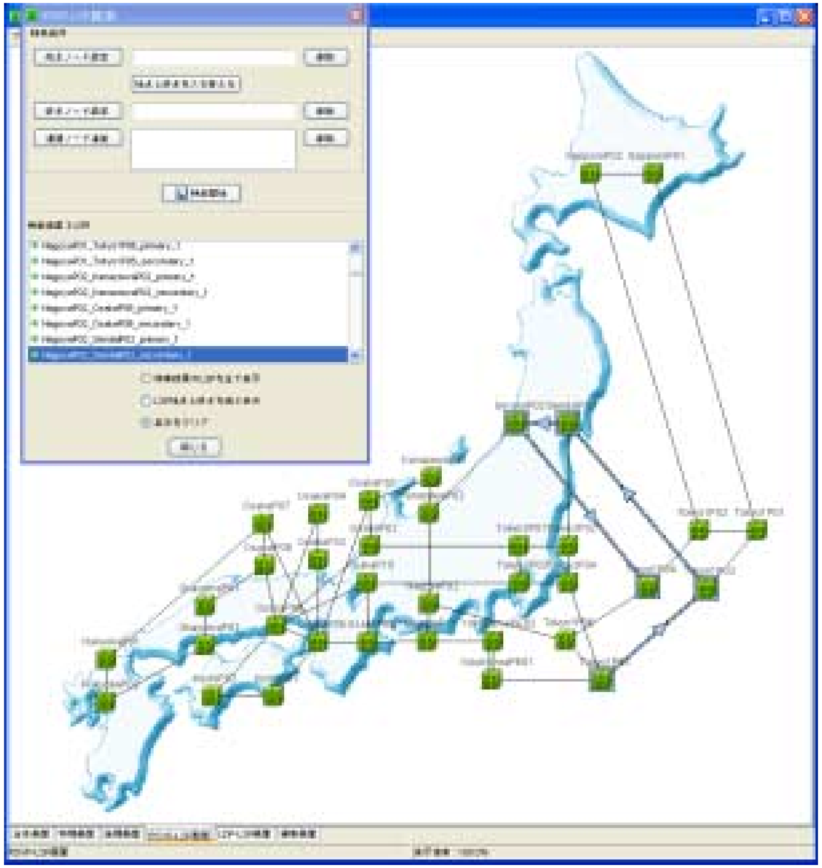
- Backbone monitoring & trouble shooting
  - path monitoring & trouble shooting on P and PE routers
  - anything which consist paths, e.g., inventory, topology, signaling, IGP/BGP, etc.
  - monitoring:
    - path visualization – view logical path topology
    - path status monitoring – active, inactive, backup
    - path traffic monitoring
    - alarm monitoring for MPLS LSP
  - trouble shooting:
    - path status check (with active or passive check, ex: LSP ping/trace)
    - path consistency check
  - etc

- Service monitoring & trouble shooting
  - monitoring & trouble shooting of services: IP-VPN, L2-VPN, ATM, FR, etc
  - PE and CE (for managed services) routers
  - monitoring:
    - basic IP connectivity or service availability (active or passive monitoring)
    - traffic monitoring
    - QoS/CoS monitoring
  - trouble shooting:
    - testing service status, by both of MPLS OAM, Service OAM
    - checking consistency of routing or VRF instances
  - etc

An example of MPLS path visualization

- Operators need to manage really many paths
  - visualization makes “understanding paths” easy
  - many information related to path should be visualized, as well
    - status, bandwidth, traffic, protection, and so





Path Usage

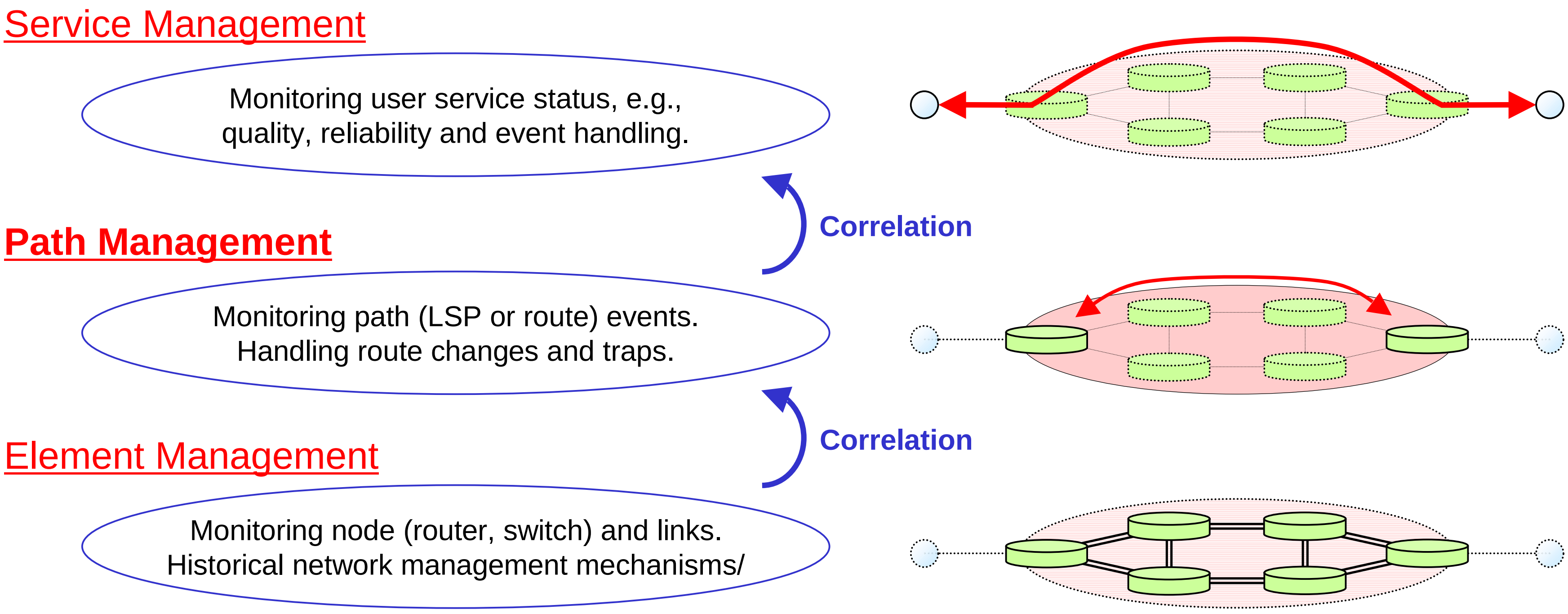
- Accounting & reporting mechanism are very specific for carriers or providers
  - because it depends on user databases and business models

- Accounting & reporting of backbone network (for backbone design, etc)
  - traffic monitoring for LSP (P and PE)
    - LSP bound for services (IP-VPN or L2-VPN or LSP-service)
    - bandwidth monitoring for traffic engineering
    - QoS/CoS monitoring for priority services
  - statistics for path status or path changes
    - downtime, delay, jitter, and so on
    - for SLA (service level agreement) for the backbone
  - etc

- Accounting & reporting of MPLS services (for service management)
  - accounting in PE
  - depends on services: IP-VPN, L2-VPN, ATM, FR, etc
  - monitoring:
    - traffic per customer
    - QoS/CoS overload
  - statistics for services
    - availability, traffic, errors (loss)
    - for SLA (service level agreement) per customer
  - etc

Correlation in MPLS path management

- In case of trouble
  - Operators have to describe the reason of the trouble
- Several layers exist in a MPLS network
  - lots of services (Internet, IP-VPN / L2-VPN, ATM / FR, and so on)
  - path, of course (by MPLS signaling)
  - elements (routers, circuits, and so on)
- Operators have to monitor and/or understand relationship between layers
  - e.g., LSP bound for services, elements which consists LSP, and so on
  - “Correlation” mechanism provides relationship between layers



Service Management

Monitoring user service status, e.g., quality, reliability and event handling.

Correlation

Path Management

Monitoring path (LSP or route) events. Handling route changes and traps.

Correlation

Element Management

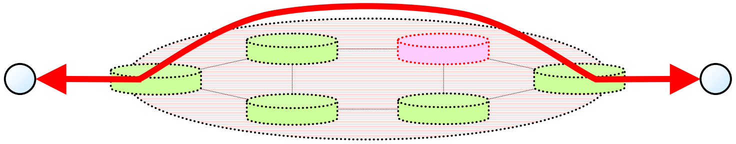
Monitoring node (router, switch) and links. Historical network management mechanisms/

Correlation in MPLS path management

- What's happen when a route has a trouble?
  - when a router has a hardware trouble, e.g., "element" failure occurs
  - paths which has the router on them, also have troubles, e.g., "path" re-route
  - services provided over those paths also have influence
- Correlation works as following (as shown in figures):
  - service management layers can detect "an event"
  - alarm events (paths and elements), and
  - notify status of service network (ex. using primary path or backup up, or down, etc)

Service Management

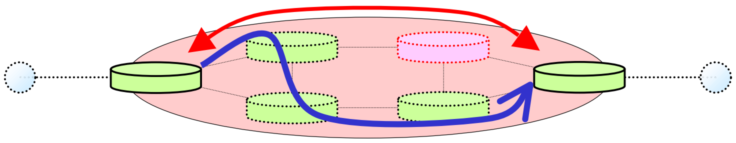
User and service info.
(type, status) in DB ⇨ Detecting service down.
Notify/Report service down time.



Correlation

Path Management

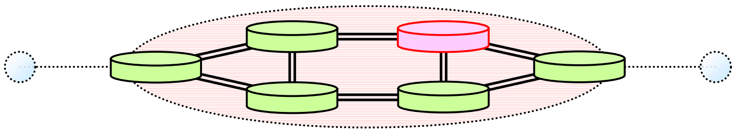
Path info.
(status, backup) in DB ⇨ Detecting path change.
Backup status, reroute time.



Correlation

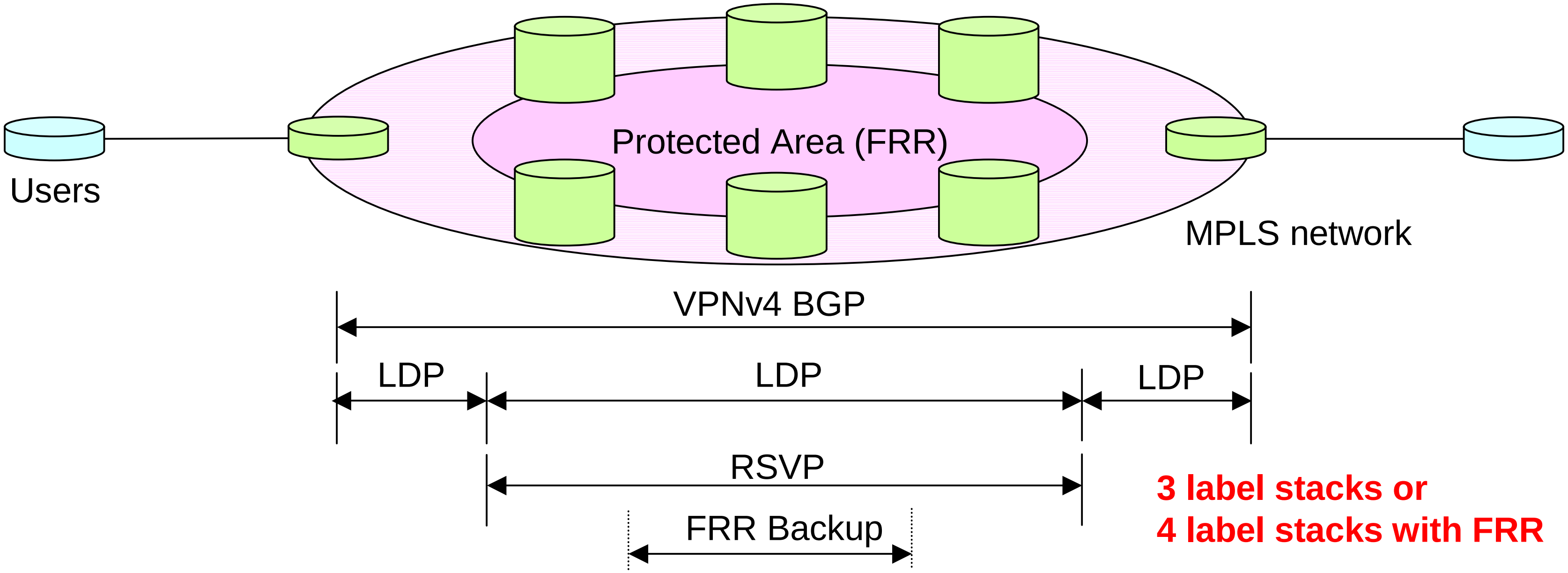
Element Management

router, link information
(config., status) in DB ⇨ Detecting router/link failure or
any physical failure.



Hierarchical MPLS path management

- Hierarchical LSP exists in a MPLS network
  - for example:
    - services labels (for IP-VPN, L2-VPN, etc) created by BGP4 (Service)
    - LSP between PE routers created by LDP (Service Edge)
    - LSP for protection purpose created by RSVP-TE (Core)
    - Paths for FRR and/or protected paths (Backup)
- We need operation and management for each paths
  - need suitable information for each paths
  - correlation of hierarchical LSP is also required



3 label stacks or
4 label stacks with FRR

Conclusion

- Recently, MPLS is / will be de facto standard of carriers' backbone
  - provides multi-service platform, such as
    - Internet
    - IP-VPN / L2-VPN
    - ATM / FR
  - with protection technology (for reliability or stability)
  - but, operators have lots of issues

- In MPLS network management
  - 3 actions and 3 layers exist to manage in MPLS network
    - provisioning, assurance and usage
    - service, path and element
  - "MPLS path management" is a key
    - correlation mechanism
    - hierarchical MPLS path management