Multi-Protocol Label Switching (MPLS) – Part II

TELCOM2321 – CS2520
Wide Area Networks
Dr. Walter Cerroni
University of Bologna – Italy
Visiting Assistant Professor at SIS, Telecom Program

Slides partly based on Dr. Znati's material

Label distribution

- A label is a flow identifier with local significance representing a network-wide FEC
- Binding of labels to FECs must be performed at each LSR along the LSP
  - manually
  - using a label distribution protocol (signaling protocol)
- Label distribution is strictly related to the way LSPs are established across the network
  - hop-by-hop routing
  - explicit routing

Label distribution: Hop-by-hop routing

- Hop-by-hop routing
  - relies on standard IP routing protocols to set-up LSPs
  - is capable of shortest-path routing only (no traffic engineering)

- Label Distribution Protocol (LDP)
  - IETF standard designed for hop-by-hop routing
  - each LSR discovers its neighbors (LDP peers) using a Hello message
  - LDP sessions are established between LDP peers and maintained with keepalive messages
  - LDP peers exchange information about FEC and label mappings
    - downstream on demand
    - downstream unsolicited

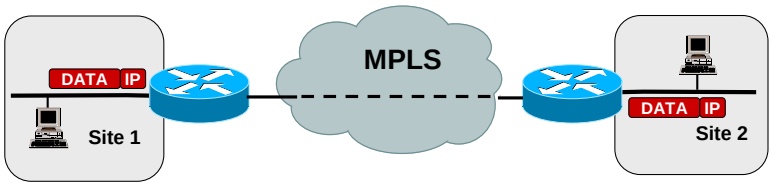
Label distribution: Explicit routing

- Explicit routing
  - ingress or egress LER explicitly specifies the LSP route
    - strictly, if all LSRs are specified
    - loosely, if only part of them are specified
  - allows full traffic engineering capabilities and connection-oriented QoS
  - requires specific, constraint-based routing protocols
    - capable of using different metrics at the same time
    - aware of current network conditions

- Label distribution protocols: extensions to existing ones
  - Constraint-based Routing LDP (CR-LDP)
  - RSVP with Traffic Engineering extensions (RSVP-TE)

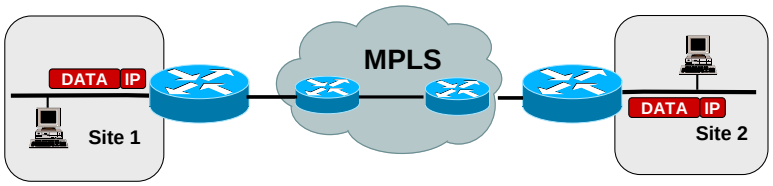
Virtual private networks

- Customer's remote sites are connected by virtual private links through the provider's network
- Traffic separation must be guaranteed
- VPNs avoid expensive leased lines
- MPLS can establish LSPs to provide VPN connectivity



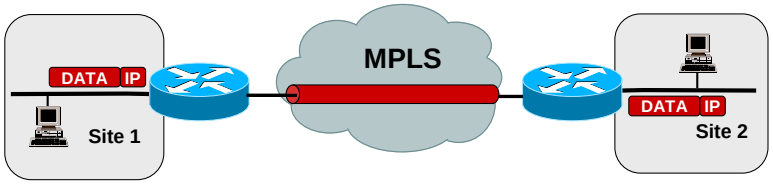
MPLS Layer-3 VPN

- MPLS network appears as an IP network
- Different customers can re-use private IP prefixes
- BGP protocol is used to advertise customer routes
  - Route Distinguisher function must be provided



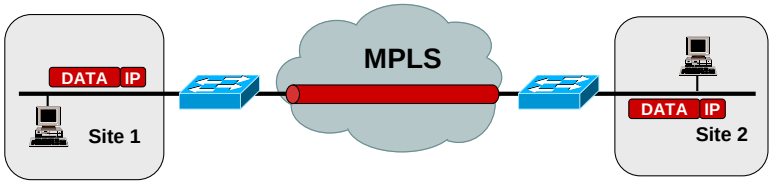
MPLS Layer-2 VPN: VPWS

- Virtual Private Wire Service (VPWS)
- Provider interconnects the customer sites via a layer-2 technology
- MPLS network appears as a point-to-point connection
  - Ethernet
  - ATM
  - Frame Relay



MPLS Layer-2 VPN: VPLS

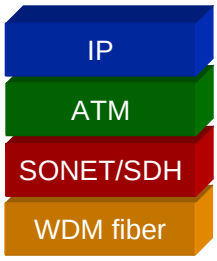
- Virtual Private LAN Service (VPLS)
- Provider interconnects the customer sites via a multipoint-to-multipoint layer-2 technology
- MPLS network appears as a segment of the same LAN as the two sites, interconnected by Ethernet switches



Multi-protocol support

- Label switching with MPLS is not limited to IP networks
- MPLS was designed to work also with other packet-based technologies
  - ATM
  - Frame Relay
- ATM and Frame Relay switches must include MPLS functionalities
- MPLS may be used as a common switching protocol over different network technologies, including non-IP networks

Layers in legacy WANs



Internetworking protocol to carry applications and services

Switching protocol to apply traffic engineering

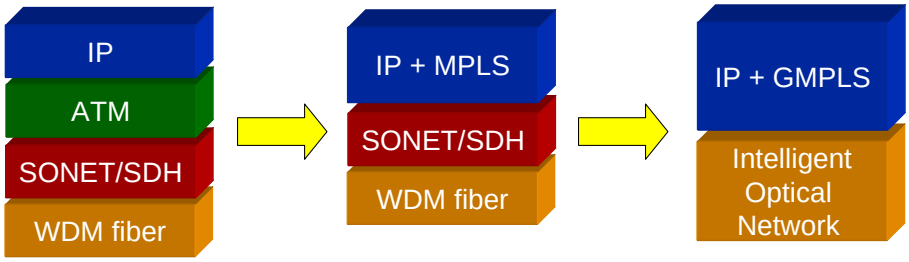
Framing protocol to provide transport and protection

Physical medium to provide multiple, high-capacity channels

IP: datagram packet switching
ATM: virtual circuit packet switching
SONET/SDH: time-division circuit switching
WDM: wavelength-division circuit switching

(De-)Layering: evolution of WANs

- Multi-layer architectures
  - have limited scalability
  - require costly management and administration operations
  - suffer from the lowest common denominator effect
- De-layering has become necessary
  - required functions must still be provided by enhanced protocols



Generalized MPLS (GMPLS)

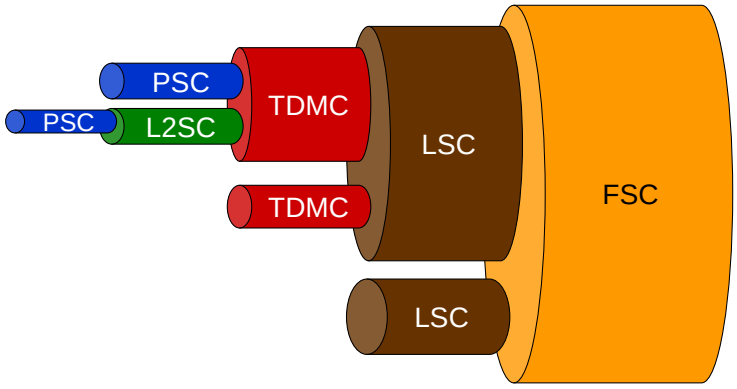
- MPLS is limited to packet-switched or cell-switched networks (IP, ATM, Frame Relay)
- LSRs have a forwarding plane that is capable of
  - recognizing either packet or cell boundaries
  - processing either packet headers or cell headers
- In GMPLS the original MPLS architecture has been extended to include LSRs based also on circuit-switching techniques
  - Time Division Multiplexing (TDM)
  - Wavelength Division Multiplexing (WDM)
  - space switching at the fiber level

GMPLS LSR interfaces

- Packet Switch Capable (PSC) interfaces
  - IP
  - MPLS
- Layer-2 Switch Capable (L2SC) interfaces
  - Ethernet
  - ATM
- Time-Division Multiplexing Capable (TDMC) interfaces
  - SONET/SDH
  - PDH
- Lambda Switch Capable (LSC) interfaces
  - Optical Cross-Connect (OXC)
- Fiber Switch Capable (FSC) interfaces
  - OXC operating at single or multiple fiber level

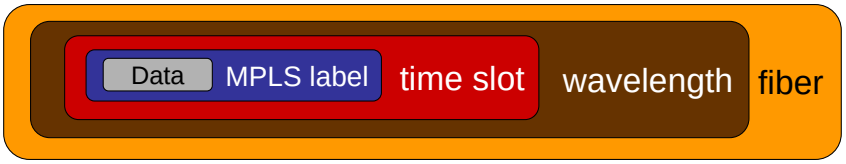
GMPLS: Nested LSPs

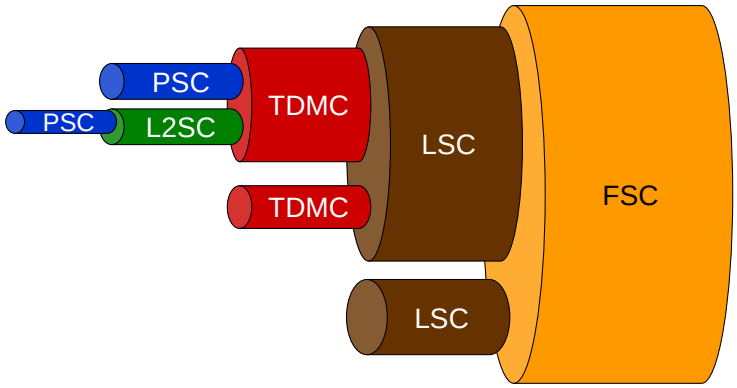
- GMPLS generalizes the nested LSP hierarchy over several layers, from packets to fibers
  - this helps in dealing with discrete nature of optical bandwidth



GMPLS: Label hierarchy

- GMPLS extends the concept of label

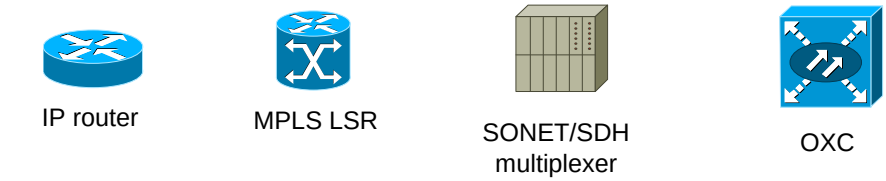


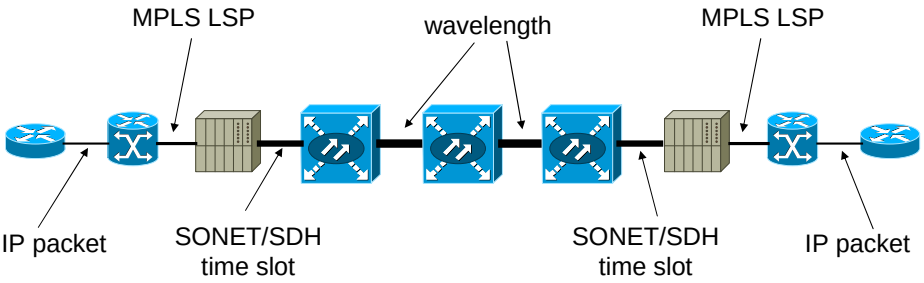


GMPLS traffic engineering

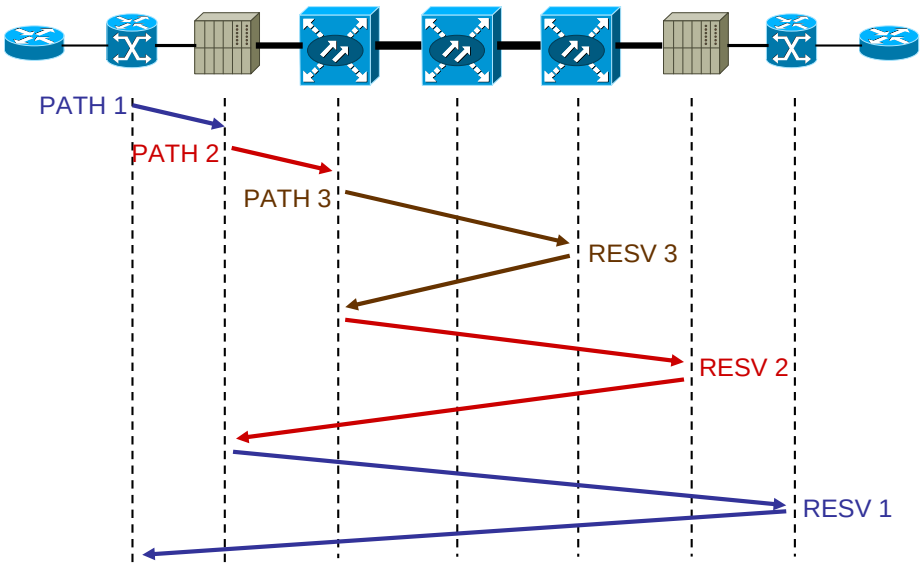
- GMPLS extends MPLS traffic engineering capabilities
- It defines additional extensions for TDMC, LSC, and FSC traffic engineering
- GMPLS extends the two signaling protocols
  - RSVP-TE
  - CR-LDP
- GMPLS extends also the routing protocols
  - OSPF-TE
  - IS-IS-TE

GMPLS path establishment





GMPLS path establishment with RSVP-TE



Link Management Protocol (LMP)

- GMPLS adjacent nodes must exchange control information for LSP management
- Control channel is now separate from data channels
  - separate link or wavelength for FSC or LSC interfaces
- LMP provides
  - control channel management
    - to establish and maintain node adjacency
  - link connectivity verification
    - to verify physical connectivity of data channels
  - link property correlation
    - to correlate data channel properties between adjacent nodes
  - fault management
    - to provide data channel protection and restoration

Protection vs. Restoration

- In case a link fails on the primary LSP, an alternate LSP is used to route information
- Protection and restoration operate on different time scales
- Protection
  - alternate LSP is pre-allocated at primary LSP setup
  - resource redundancy is required
  - protection reacts to failure rapidly
- Restoration
  - alternate LSP is dynamically established when failure occurs
  - better resource utilization
  - dynamic route calculation required, which could be computationally expensive
  - it may take longer to restore the connection

IP/MPLS/GMPLS evolution

IP	MPLS	MPLS-TE	GMPLS
Connectionless service	Connection-oriented service	MPLS + traffic engineering extensions	MPLT-TE + optical extensions
Hop-by-hop packet forwarding	Label switching	Explicit routing	Explicit routing at different granularities
Control and data plane coupling	Logical separation of control and data plane		Physical separation of control and data plane
Forwarding and control coupling	Forwarding and control decoupling		
Routing protocol	Routing and signaling protocols for LSP setup	Routing and signaling + TE extensions	Routing, signaling and LMP