Lab 1: Static MPLS

- First lab gives a basic understanding of MPLS label swapping
- No signaling – manually assign labels – like static routing
- Understand configuration, forwarding tables, and debugging of MPLS
Routing instances and tables

Routing Instance: main
- inet.0
- inet6.0
- inet.1
- inet.2
- inet.3
- inet.4
- mpls.0

IPv4 unicast routes
IPv6 unicast routes
IPv4 multicast forwarding cache
IPv4 multicast RPF table
IPv4 routes learnt from MPLS-TE path exploration
MSDP routes
MPLS label-switch table

Routing Instance: other

Example:
main.inet.0
__juniper_private1__.inet.0

Logical routers, VPNs, virtual routers, etc, use routing instances.
Using RSVP with BGP

- RSVP is usually used together with BGP
- In that scenario, RSVP computes LSP:s that are used for BGP transit traffic
  - Traffic engineering can be made for transit traffic
- But internal traffic is sent normally using IGP/IP
- In practice: Routes of LSPs created by RSVP are placed in a separate routing table (inet.3), than the ones computed by IGP (inet.0)
  - BGP always uses inet.3 first before inet.0 when finding route to the (indirect) BGP next-hop
- In this way, all traffic to external destinations are sent via MPLS, but internal traffic (e.g. Routing and signaling) sent via IGP.
Lab 2: MPLS + RSVP

- Signaling and QoS of labelled paths using RSVP
- Create LSPs first to all other networks
- Then use traffic engineering to create LSPs to your neighbour via a detour.
- Concerning RSVP routes: We do not use BGP in this lab
  - Traffic between user networks only should go via MPLS
- Set `traffic-engineering bgp-igp`
  - Places the `rsvp` computed routes in `inet.0`
VPN Architecture 2

Connect several LAN “islands”.

![Diagram of VPN Architecture 2](image-url)
Provider-based VPNs using MPLS/RSVP/BGP

Several related variants including

- L3VPN – RFC 4364 (used to be RFC 2547"")
- L2VPN – pseudowires
- VPLS (”dynamic L2VPN”)

- These solutions all use multiprotocol BGP and VRFs (Virtual routing and forwarding) to separate between private networks.
- We will now step-wise go through the components for L3VPN
Provider-based VPNs

- CE - Customer Edge
- PE - Provider Edge
- P - Provider

- More than one customer: red and blue
- More than two sites per customer
- CE is either router or L2 device
L3VPN

Routing between LAN islands
CE/PEs exchange routing

PE - Provider Edge
CE - Customer Edge
P - Provider

Customer A
netw 1

Customer A
netw 2

Customer A
netw 1

Customer B
netw 2

Customer B
netw 3

Customer B
netw 3
View from one customer

Provider network acts as a "distributed router"
Every PE is as a linecard

Note that default route (or BGP full feed) is peered via one CE/PE, and then redistributed throughout the VPN, just as any other route.
L2VPN: View from one customer

Provider network acts as a set of wires. Learning and spanning tree can be made by attaching learning bridges as CE:s.
VPLS: View from one customer

Provider network acts as a distributed switch
Provider network performs learning (and STP)
Virtual Routing and Forwarding - VRF

- A virtual router is a subset of a physical router.
- A virtual router has its own routing processes, routing tables, forwarding tables and its own interfaces,
- Typically interfaces of virtual routers are virtual (eg VLANs)
- The virtual routers are partitioned into several *disjoint* virtual routers.
- Similar in concept to VLANs and VLAN bridges, but in L3.
VRF in a PE

Example: A router with two customers instances: VRF1 and VRF2. Need to multiplex traffic from the VRFs on same network
Using MPLS and RSVP

Establish LSP:s between border routers

Use double stacking:
- outer tag: LSP PE<-->PE
- inner tag: VPN label

Internal nodes (P-nodes) are only aware of outer tags (PE to PE)

With RSVP you set up the *outer* tag
- and can also traffic engineer the LSP:s
Using BGP: Label, RD and RT

• You need to communicate reachability information
  – Which prefixes are in which VPN?
• You also need to communicate VPN labels
  – Which label corresponds to which VPN?
• And the next-hop PE
• For this, you use MP-BGP – Multi Protocol BGP.
• The IPv4 routes are extended with a unique identifier
  – The Route distinguisher (RD)
• Typically the RD is AS:VPN#
  – Example: 650010:15
  – But there are also other techniques.
• You also need to specify VRF the route belongs to
  – This is called the Route target (RT)
  – Essentially the VRF
Example: Announcing route

- Assume PE1 has assigned RD 65010:15 to the VPN shown in the picture.
- PE1 announces the networks by prepending this RD to all routes learnt from that site making them unique.
- The nexthop of those routes are PE1.
- The inner MPLS label of that VPN is 100
- The RT is RedVPN (The VRF)
Example: Forwarding

- A lookup will be made in PE2 in RedVPN. Packets destined to 10.1/16 are sent via an LSP to PE1 (outer label)
- And tagged with inner label 100
- When they arrive on PE1, the label (100), will tell PE1 that it is the RedVPN it is targeted to.
- The packet is popped (twice)
- And an IP lookup in the RedVPN VRF will be made
- And the packet is sent towards CE1
Summary of protocols in L3VPN

- IP – basic information carrier
- MPLS – tunnels (LSPs) through the provider network
- RSVP – label distribution to setup MPLS LSPs (outer labels)
- OSPF or ISIS – Find shortest paths through provider network for RSVP and BGP
- BGP – Distribution of reachability information (prefixes), VRF information and inner VPN labels
- Additionally, you can choose yet another protocol to peer between the provider and customer. RIP?
L3VPN Summary

- L3VPN is a "peer-type" and dynamic VPN using BGP and MPLS
- This way of creating VPNs have quickly become popular.
- Easy to configure (but hard to understand)
- Drawback:
  - Customer routing tables are imported into the provider's network (PE:s)
- Suppose each customer has its own full BGP routing table (~200K routes)
- The providers routing tables will explode
- Typical encapsulation in provider's network:
L2VPN pseudo-wire

- Static, multipoint "overlay" solution
- Setup point-to-point L2 connections between every site in the VPN
  - Pseudo-wires
- Using MPLS/RSVP/BGP in a similar way as L3VPN
- L2 frames are encapsulated using IP and MPLS
- Can transform between different link-layers
- Typical encapsulation in provider's network:
Virtual Private LAN Services (VPLS)

- Dynamic, multipoint "peer" solution
- VPN services for L2 (eg switched networks)
- Backbone over IP
- Interconnects a switched L2 network
- In VPLS an IP network works as a "distributed switch"
- MPLS is used together with BGP to create "pseudo-wires" between the LAN islands.
- VPLS: Dynamic establishment of pseudo-wires
  - Bridging (learning) enabled
  - STP
- MP-BGP is used for distributing mac address learning
- Disadvantage (similar to L3VPN)
  - Provider imports MAC learning tables into network
VPLS

PE:s act as switch toward customer, but as router up-link.