Challenges in Large IP Network Deployments

Echo Liu, Cheng Yang
www.wandl.com
Wide Area Network Design Laboratory

Agenda

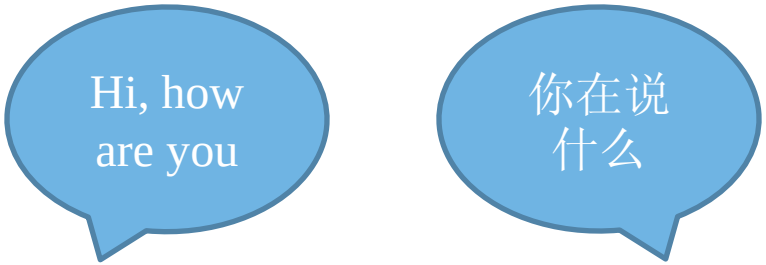
- Challenges in Large Network Deployments
- Typical Practice: Divide and Conquer
- Typical Management Solutions: SNMP + CLI
- Using SNMP
- Using CLI

Typical Practice : Divide and Conquer

- **Divide and conquer, either by region or by hierarchy, by functions**
  - By region: north, east, west, south…
  - By hierarchy: Access, distribution, core, super-core
  - By functions or service: PE, P, BGP peering, Route reflectors

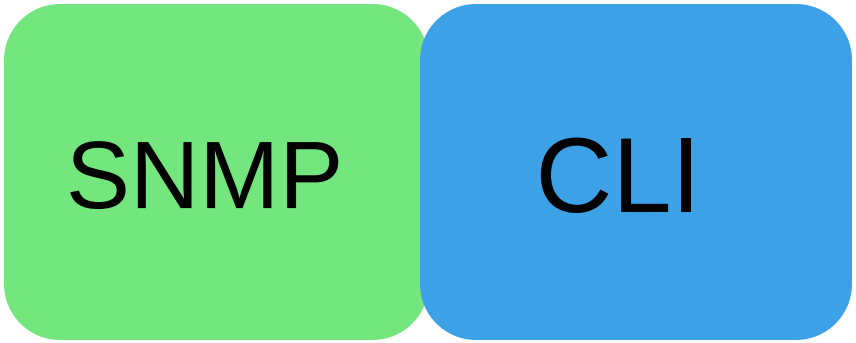
Typical Practice : Limit the vendor type

- **Try to use only one vendor for the each of the partitions**
  - ➢ Challenges is operation/support/troubleshooting
  - ➢ If multi-vendors are used, need vendor support and extensive inter-operability tests

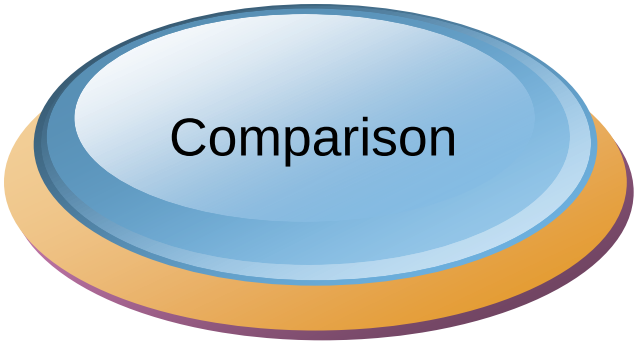


Multi vendors challenges

- **How to handle multi vendors in a large network environment**
  - For example, the network may have at least 2 or 3 router vendors among Alcatel-Lucent, Cisco, Huawei, Juniper, Redback, Tellabs, Zte, etc.



Typical Practice: SNMP + CLI



SNMP is usually used by PM and FM

- ◆a single management protocol that can be used to manage any network device from any vendor
- ◆reduces the complexity of the network management application

For configurations, changes, trouble shooting and network info, CLI is easier to use

- ◆The beauty is most information is available in the config file
- ◆ simple to use, easier for troubleshooting

APNIC

WANDL
WIDE AREA NETWORK DESIGN LABORATORY

Example CLI in multi-vendor environments

- vendor 1 : show config
- vendor 2: display current-config
- vendor 3: admin display-config
- vendor 4: show running
- vendor 5: show configuration detail
- …

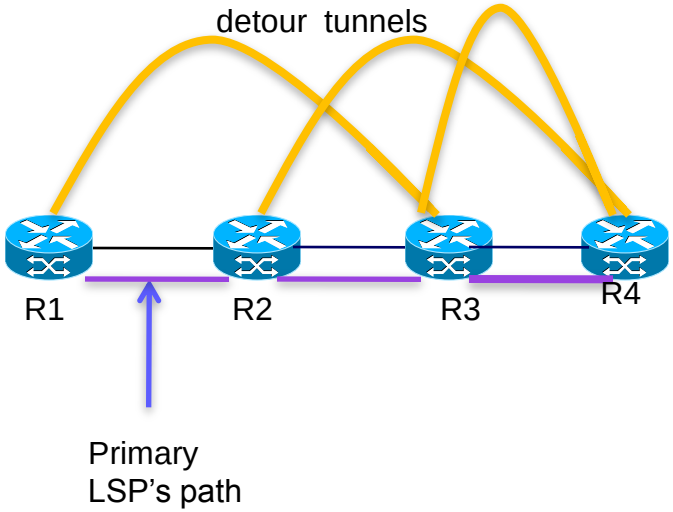
Sample CLI outputs

```
lab@WDC> display current-config
#
 sysname WDC
#
 FTP server enable
#
 info-center loghost source LoopBack0
 info-center loghost 192.168.1.120
 info-center loghost 192.168.1.130 facility local2
 #
 vlan batch 31 441 443 445 448 461 463
#
 multicast routing-enable
 multicast load-splitting source
#
 ip netstream sampler fix-packets 8 inbound
 ip netstream sampler fix-packets 8 outbound
 ip netstream export source 192.168.1.140
 ip netstream export host 192.168.1.150 2055
#
snmp-agent trap type base-trap
#
 ip netstream timeout active 1
 ip netstream timeout inactive 15
#
```

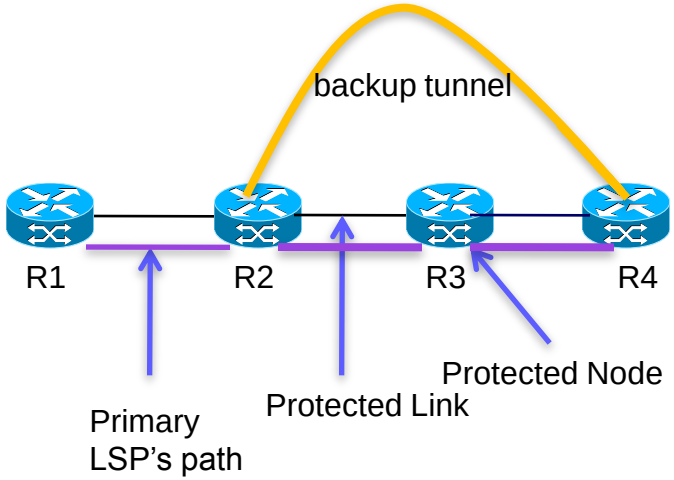
```
TPE3640#show running
Building configuration...

Current configuration : 8810 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname TPE3640
!
boot-start-marker
boot system flash c3640-p7-mz.121-3a.T.bin
boot system flash c3640-js-mz.124-7a.bin
boot-end-marker
!
logging buffered 5000 debugging
no logging console
enable secret 5 $1$hNoA$Xbwx2WJPWC8HM9Z44dhq9.
!
no aaa new-model
!
resource policy
```

Be careful

- Sometimes the same word has different meaning
  - Example: keyword "fast reroute"



vendor1 means path protection



vendor2 means link/node protection

Beware of …

- Some vendors treat MPLS TE Tunnels as Interfaces, others just call it Label Switched Paths

```
interface Tunnel102
 description _DELETED_
 ip unnumbered Loopback0
 ip ospf message-digest-key 1 md5 7 110A491744425
 ip ospf network point-to-point
 ip ospf cost 25000
 keepalive 60 3
 shutdown
 tunnel source 192.176.30.70
 tunnel destination 192.71.112.42
!
interface Tunnel202
 description _DELETED_
 ip unnumbered Loopback0
```

```
mpls {
    log-updown {
        syslog;
    }
    record;
    label-switched-path ECHO:SOFTSWITCH {
        to 192.5.15.208;
        no-cspf;
        fast-reroute;
        primary ECHO-PATH1;
        secondary ECHO-PATH2 {
            standby;
        }
        secondary ECHO-PATH4 {
            standby;
```

APNIC

WANDL WIDE AREA NETWORK DESIGN LABORATORY

Beware of …

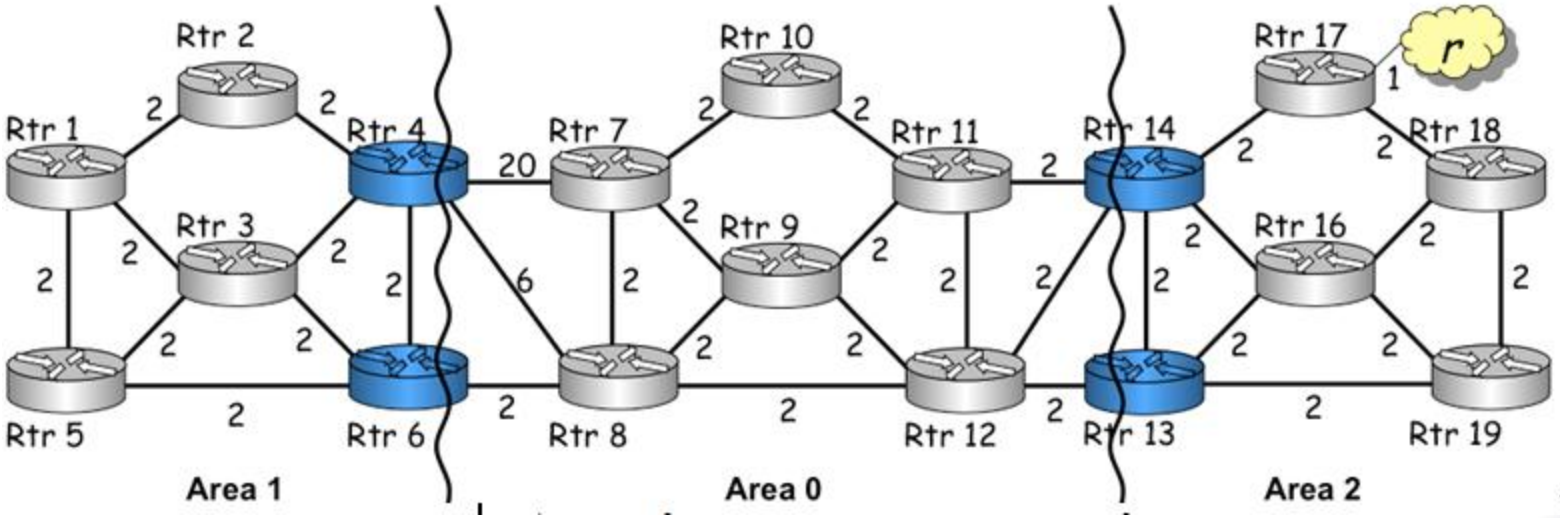
- Some vendor assume the unit is K bits
- Some vendor require you to use K, M, or G. otherwise the unit is 1 bit

```
mpls {
    label-switched-path 2-1 {
        from 2.2.2.120;
        to 1.1.1.110;
        ##
        ## '5' was inherited from group 'mpls
        ##
        metric 5;
        ##
        ## 'bandwidth' was inherited from gro
        ## '10m' was inherited from group 'mp
        ##
        bandwidth 1000;
    }
```

```
interface Tunnel2105
 ip unnumbered Loopback1
 mpls label protocol ldp
 mpls ip
 tunnel destination 192.168.1.180
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric absolute 1
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name T210
```

Some advantages of CLI : network discovery

One can use the CLI output of “ show ospf database " to do network discovery



Another example of using CLI to do network discovery

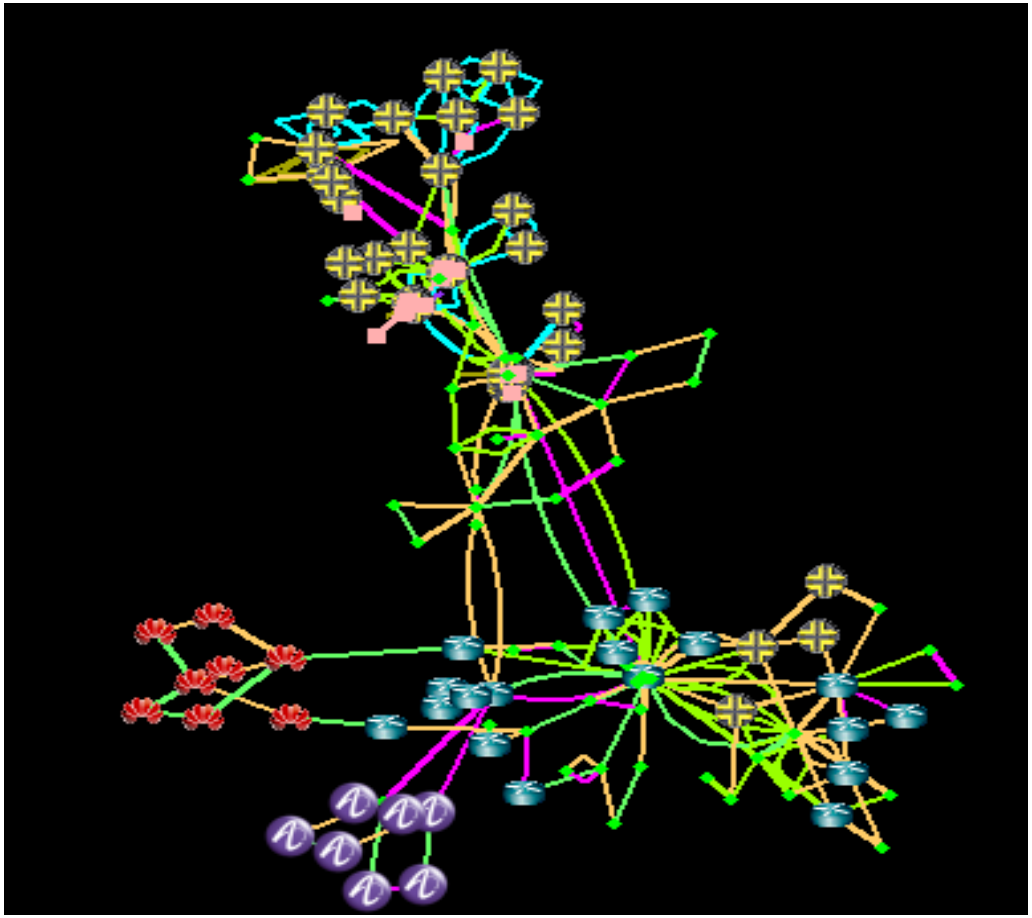
- Using CLI to discover entire MPLS TE topology
  - vendor1 : show ted database extensive
  - vendor2: show mpls traffic-eng topology
  - vendor3: display mpls te cspf tedb node
  - …

Samples of MPLS-TE Topology CLI outputs

```
lab@ECHO> show ted database extensive | no-more
TED database: 161 ISIS nodes 141 INET nodes
NodeID: ECHO-02.00(192.168.193.2) -> Overload
  Type: Rtr, Age: 111 secs, LinkIn: 2, LinkOut: 2
  Protocol: IS-IS(2)
    To: 3G-PE-RAY02.00(192.168.246.181), Local: 192.52.11.158, Remote: 192.
      Color: 0x4 green
      Metric: 10
      Static BW: 311.04Mbps
      Reservable BW: 311.04Mbps
      Available BW [priority] bps:
          [0] 237.708Mbps   [1] 237.708Mbps [2] 237.708Mbps [3] 237.708Mbps
          [4] 237.708Mbps   [5] 237.708Mbps [6] 237.708Mbps [7] 237.708Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 237.708Mbps   [1] 237.708Mbps [2] 237.708Mbps [3] 237.708Mbps
          [4] 237.708Mbps   [5] 237.708Mbps [6] 237.708Mbps [7] 237.708Mbps
```

```
echo#show mpls traffic-eng topo
My_System_id: xxx.xx.xxx.xxx (ospf 51  area 0)

Signalling error holddown: 10 sec Global Link Generation 5751

IGP Id: xxx.xx.xx.xxx, MPLS TE Id:xxx.xxx.xxx.xxx Router Node  (ospf 51  area 0)
      link[0]: Point-to-Point, Nbr IGP Id: xxx.xx.xxx.xxx, nbr_node_id:15, gen:5682
        frag_id 159, Intf Address:166.6.168.10, Nbr Intf Address:166.6.168.9
        TE metric:20, IGP metric:20, attribute flags:0x0
        SRLGs: None
        physical_bw: 2396000 (kbps), max_reservable_bw_global: 2500000 (kbps)
        max_reservable_bw_sub: 0 (kbps)

                                Global Pool     Sub Pool
            Total Allocated     Reservable      Reservable
            BW (kbps)           BW (kbps)       BW (kbps)
            ---------------     -----------     ----------
      bw[0]:           0          2500000              0
      bw[1]:           0          2500000              0
      bw[2]:           0          2500000              0
      bw[3]:           0          2500000              0
      bw[4]:           0          2500000              0
      bw[5]:           0          2500000              0
      bw[6]:           0          2500000              0
      bw[7]:        2001          2497999              0
```

Topology Discovery Example



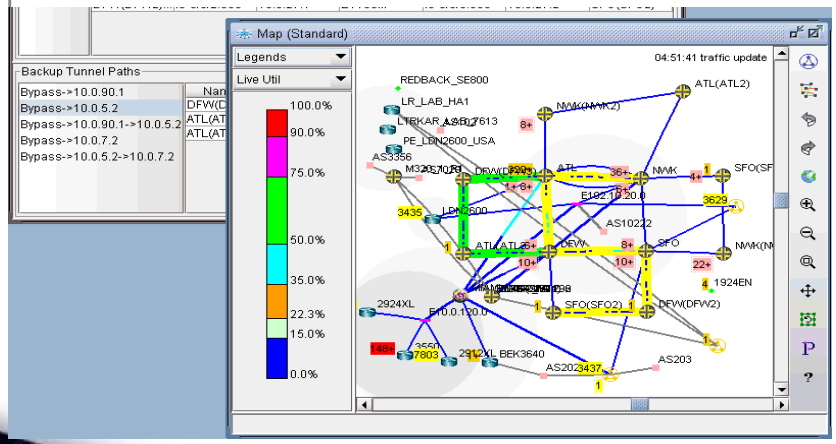
APNIC

WANDL
WIDE AREA NETWORK DESIGN LABORATORY

Using CLI to extract MPLS TE tunnel paths

vendor1 : show mpls lsp statistics ingress extensive logical-router all

```
lab@SFO> show mpls lsp statistics ingress extensive logical-router all|no-more

logical-router: SFO2
Ingress LSP: 10 sessions

10.10.0.1
  From: 10.41.0.1, State: Up, ActiveRoute: 0, LSPname: SFO2_2NWK
  Statistics: Packets 0, Bytes 0
  ActivePath:   (primary)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
*Primary                    State: Up
    SmartOptimizeTimer: 180
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 4)
10.0.27.1 S 10.0.17.2 S 10.0.9.1 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node 10=SoftPreempt
          10.0.27.1 10.0.17.2 10.0.9.1
     7 Nov  9 16:56:19 Selected as active path
     6 Nov  9 16:56:19 Record Route:  10.0.27.1 10.0.17.2 10.0.9.1
     5 Nov  9 16:56:19 Up
     4 Nov  9 16:56:19 Originate Call
     3 Nov  9 16:56:19 CSPF: computation result accepted
     2 Nov  9 16:55:49 CSPF failed: no route toward 10.10.0.1[62716 times]
     1 Oct 19 12:06:01 CSPF: could not determine self
  Created: Fri Oct 19 12:06:01 2007
```



192.168.1.112.transit_tunnel - 写字板

文件(F) 编辑(E) 查看(V) 插入(I) 格式(O) 帮助(H)

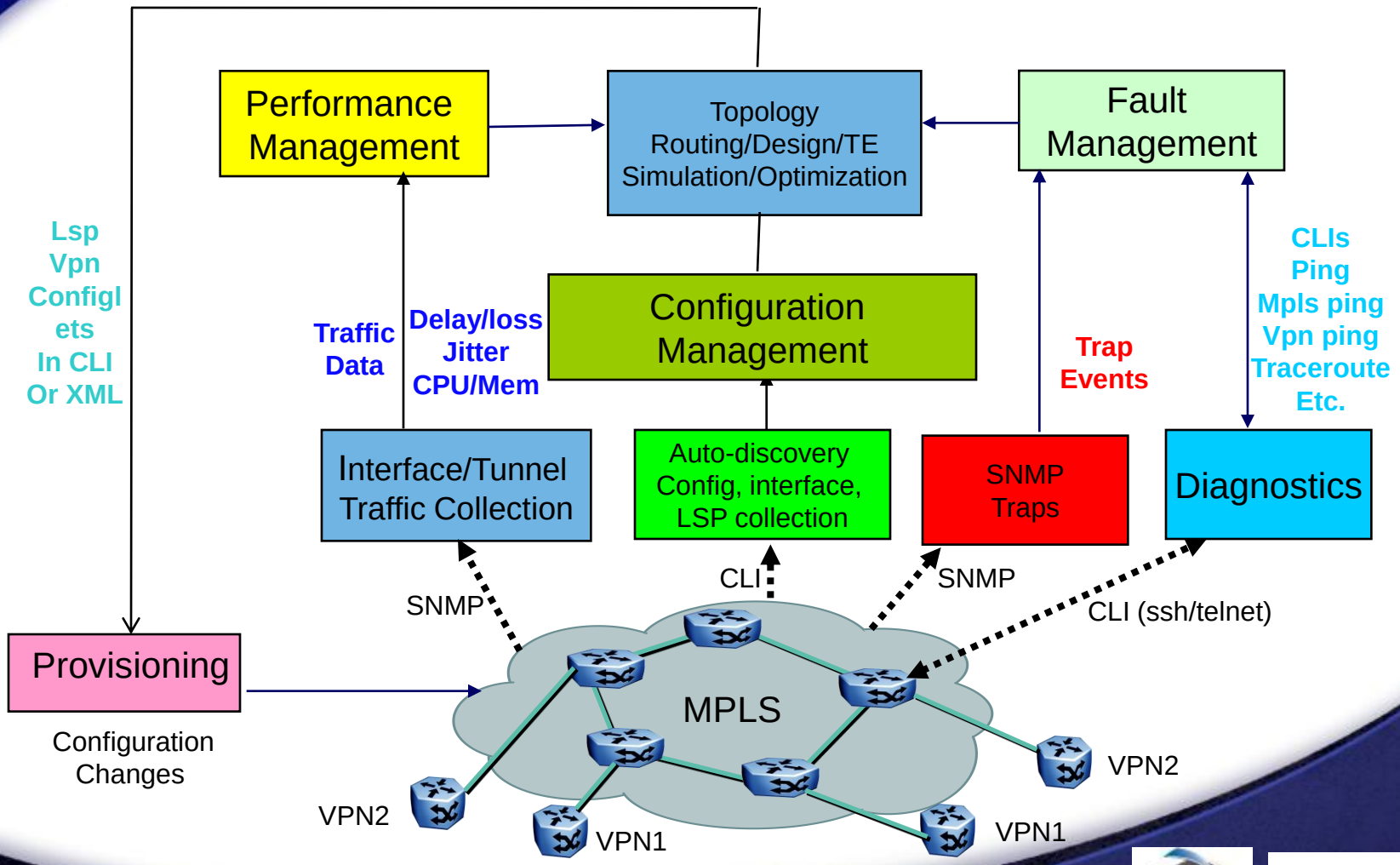
```
wandl@Ray_tst> show rsvp session ingress detail logical-router all|no-more

logical-router: r2
Ingress RSVP: 5 sessions

112.112.112.4
  From: 112.112.112.2, LSPstate: Up, ActiveRoute: 0
  LSPname: Bypass->10.0.4.9
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 100016
  Resv style: 1 SE, Label in: -, Label out: 100016
  Time left:    -, Since: Wed Feb 25 06:16:02 2009
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 40716 protocol 0
  Type: Bypass LSP
    Number of data route tunnel through: 1
    Number of RSVP session tunnel through: 0
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 1500
  PATH sentto: 10.0.4.1 (fxp2.4) 93 pkts
  RESV rcvfrom: 10.0.4.1 (fxp2.4) 98 pkts
  Explct route: 10.0.4.1 10.0.2.6
  Record route: <self> 10.0.4.1 10.0.2.6
```

Display the tunnel current path using the CLI output

APNIC

WANDL WIDE AREA NETWORK DESIGN LABORATORY

Summary


Performance Management
Topology Routing/Design/TE Simulation/Optimization
Fault Management
Lsp Vpn Configlets In CLI Or XML
Traffic Data
Delay/loss Jitter CPU/Mem
Configuration Management
Trap Events
CLIs Ping Mpls ping Vpn ping Traceroute Etc.
Interface/Tunnel Traffic Collection
Auto-discovery Config, interface, LSP collection
SNMP Traps
Diagnostics
SNMP
CLI
SNMP
CLI (ssh/telnet)
Provisioning
Configuration Changes
MPLS
VPN2
VPN2
VPN1
VPN1

Thank You !

谢　　谢！