MPLS : Hacking & Security Myth of The Beast In Core Telecommunication Network

gcsf@nowhere

WHY?

- TELCO Technology? Industry, Community, Academic?
- Ask Others to also share their high quality research
- Taking Indonesian Hacking Scene to The Higher Level (?)

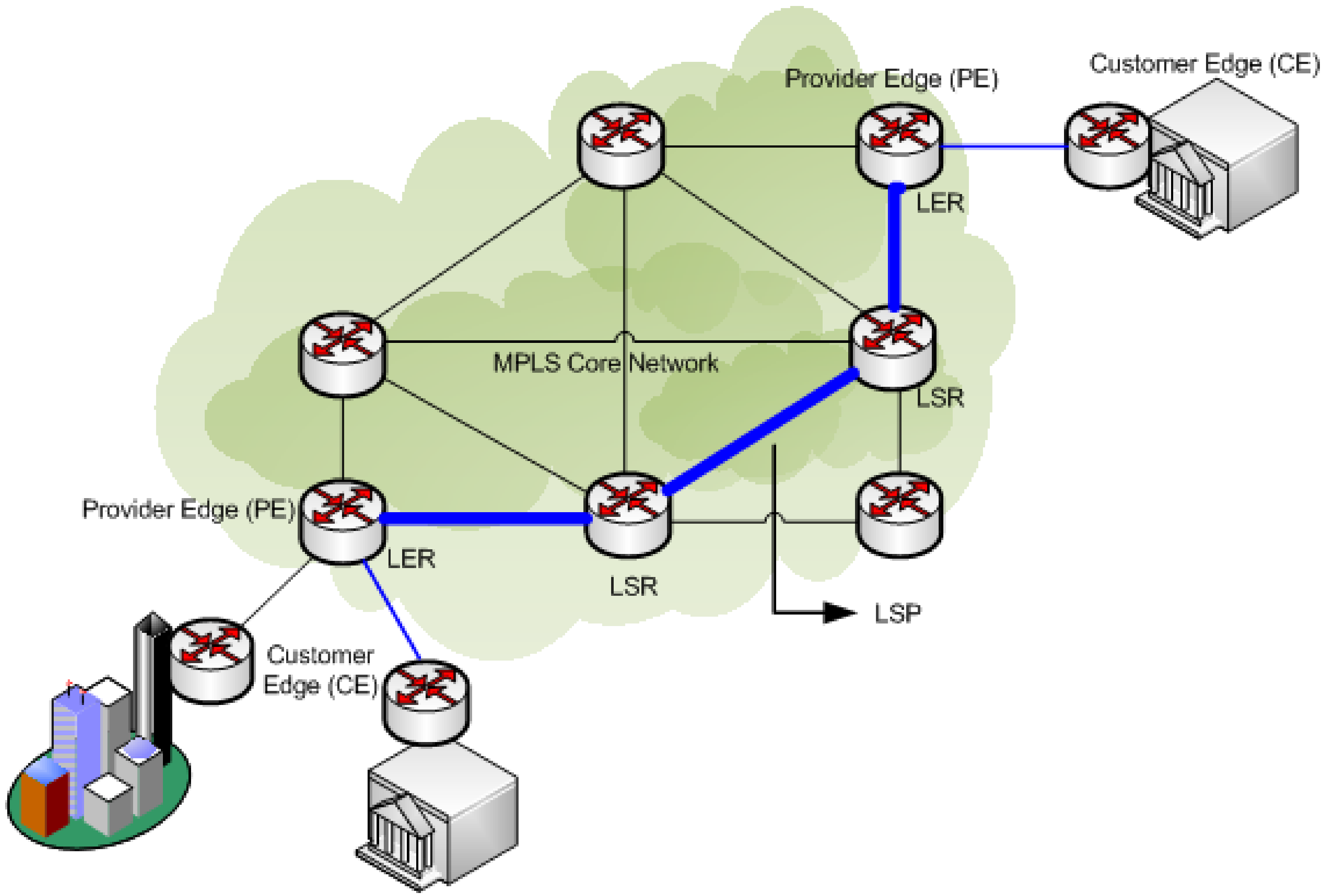
MPLS?

- MPLS is routing mechanism in high-performance network backbone
- Route the data traffic from a node to the next node based on short path labels
- Avoiding complex forwarding mechanism in routing table
- Operate in between layer 2 and layer 3 (OSI model), taking advantage on the layer 2 switching performance and layer 3 routing scalability
- MPLS Architecture is very well written on RFC 3031

MPLS Terminology?

- Label Distribution Protocol (LDP)
- Label Switched Path (LSP)
- Label Switching Router (LSR)
- Label Edge Router (LER) / MPLS Edge Node
- Virtual Routing & Forwarding (VRF)
- CE/PE/P Router
- MORE? (We only describe terminology used in this document)

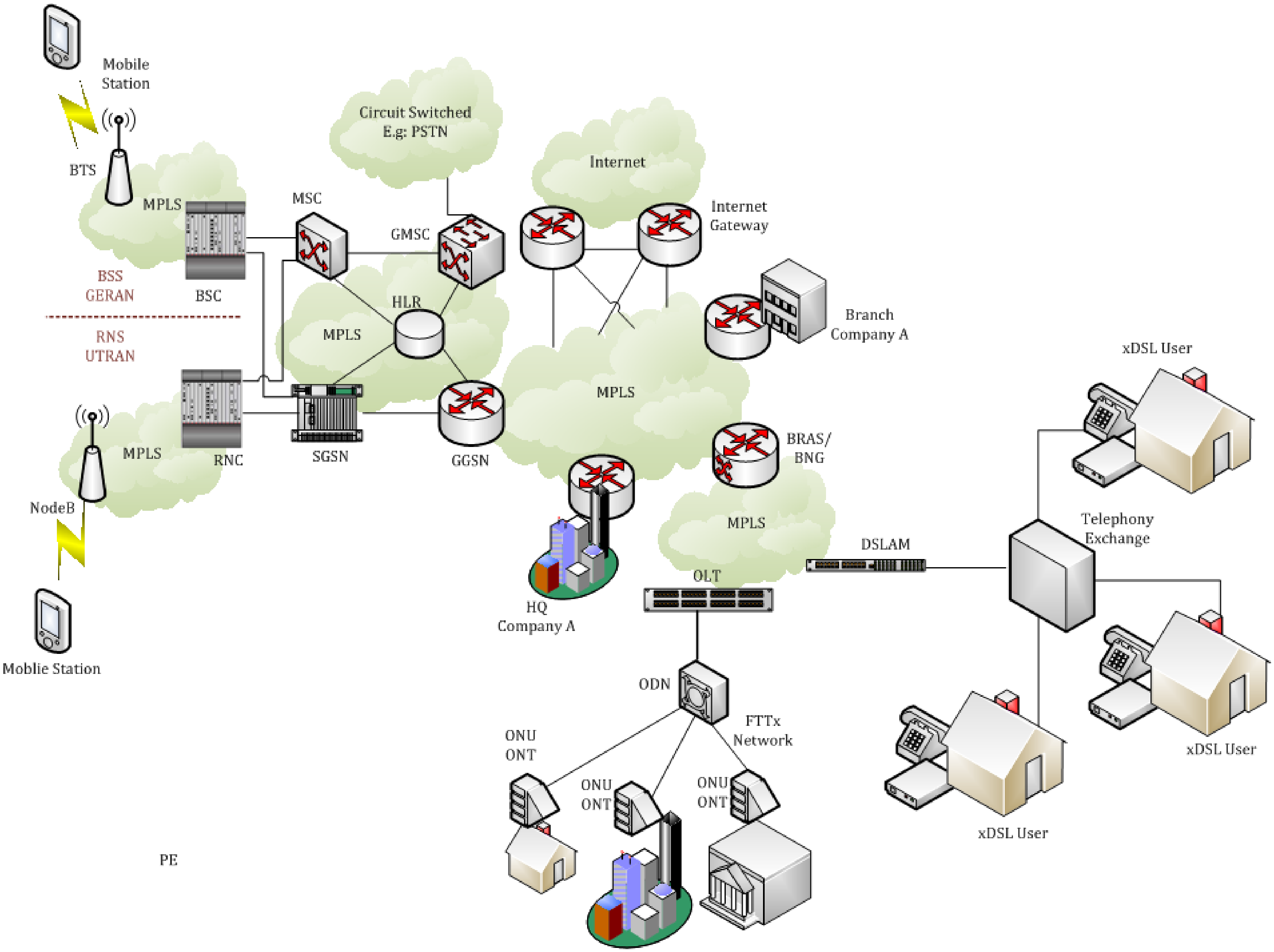
MPLS In Simple



MPLS Usage

- Virtual Private Routed Network (VPRN) – L3VPN
- Virtual Private LAN Service (VPLS) – L2VPN
- Virtual Leased Line (VLL)
- Traffic Engineering
- In order to limit this presentation, we will only discuss L3VPN

MPLS In Broadband Network



Myth - MPLS Hacking & Security?

- Provider Edge (PE) router
- Encryption support
- Traffic Sniffing
- MPLS Label
- Label Distribution Protocol
- Border Gateway Protocol

REFERENCE : ERNW.DE

PE Router

- Usually to be shared among customers
- Multiple CE router from multiple customers is connected to the single PE router
- Still, the security relies on the trust model of provider private network
- Missing configuration of PE router? (E.G: Mgmt Access)
- A customer sending crafted packet to PE to deny services

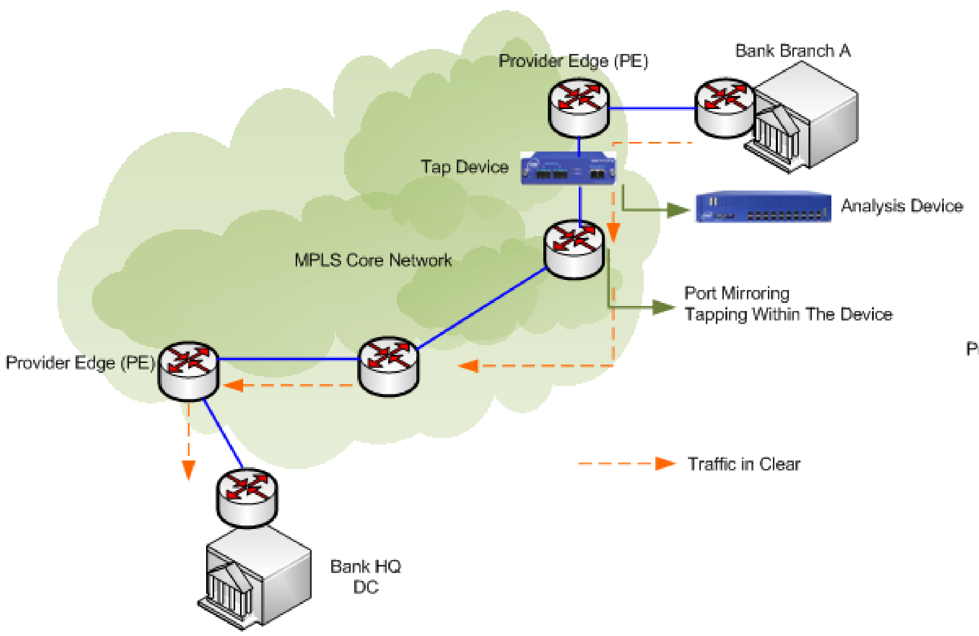
Encryption Support

- MPLS doesn’t provide encryption mechanism
- Encryption of traffic in core telco relies on the encryption mechanism of higher OSI level
- The security relies on the trust model of provider private network
- There are some appliance that can be used to help the traffic encryption (Eg: SafeNet, Senetas)
- IPSEC over MPLS?

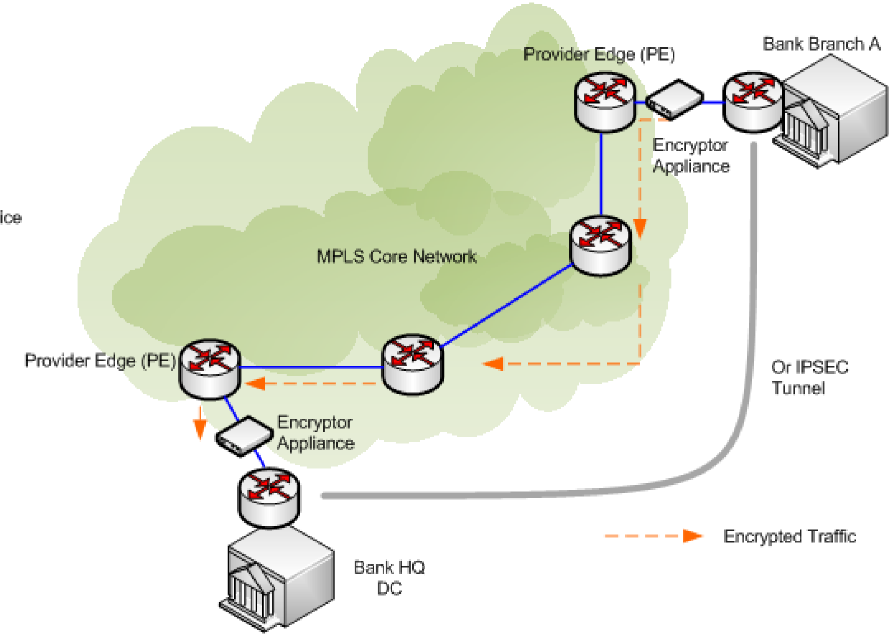
Traffic Sniffing?

- P/PE Router?
- Remember, by default no encryption support!
- Cisco Embeded Packet Capture (EPC)
- Cisco “debug packet” with hiden option “dump”
- Juniper “set forwarding-options packet-capture”
- Port Mirroring is commonly used
- Appliance is also commonly used (E.g: VSS, NetOptics)
- DPI? LI?

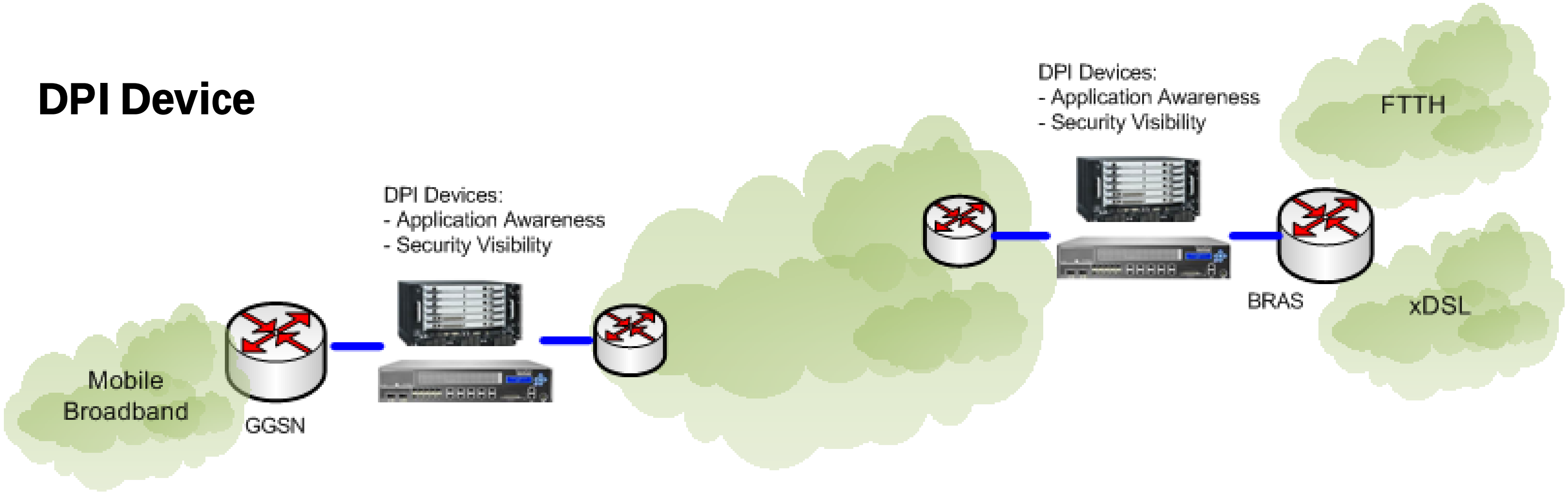
Network Tapping



Encryption



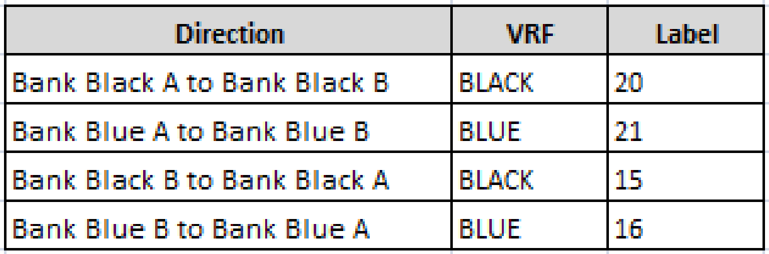
DPI Device



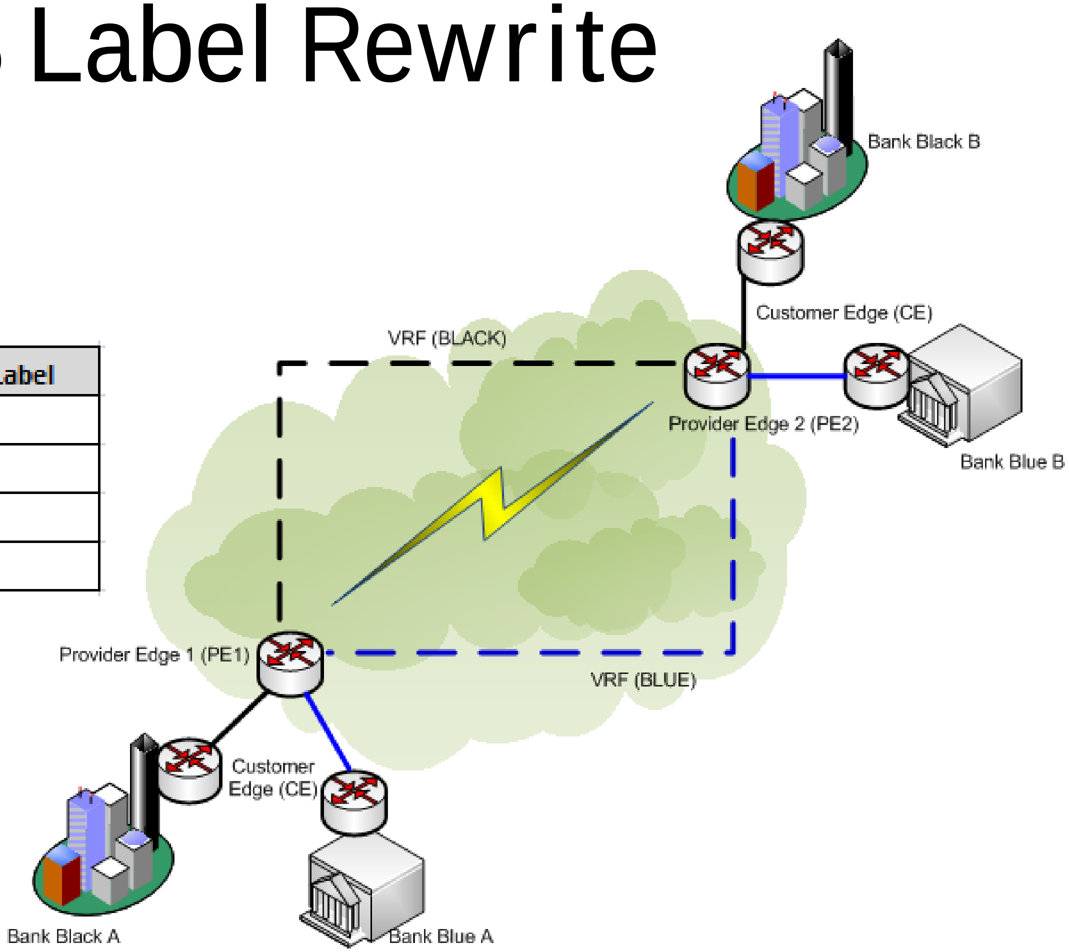
MPLS Label

- Injection of labeled traffic from customer CE router
  - RFC 2547, labeled traffic from non trusted sources must be discarded
- Injection of labeled traffic from Internet
  - Again RFC 2547, labeled traffic from non trusted sources must be discarded
- MPLS label rewriting in MPLS backbone
  - Possible, can be reproduced in the Lab, hard (impossible?) to implement in the real backbone

MPLS Label Rewrite

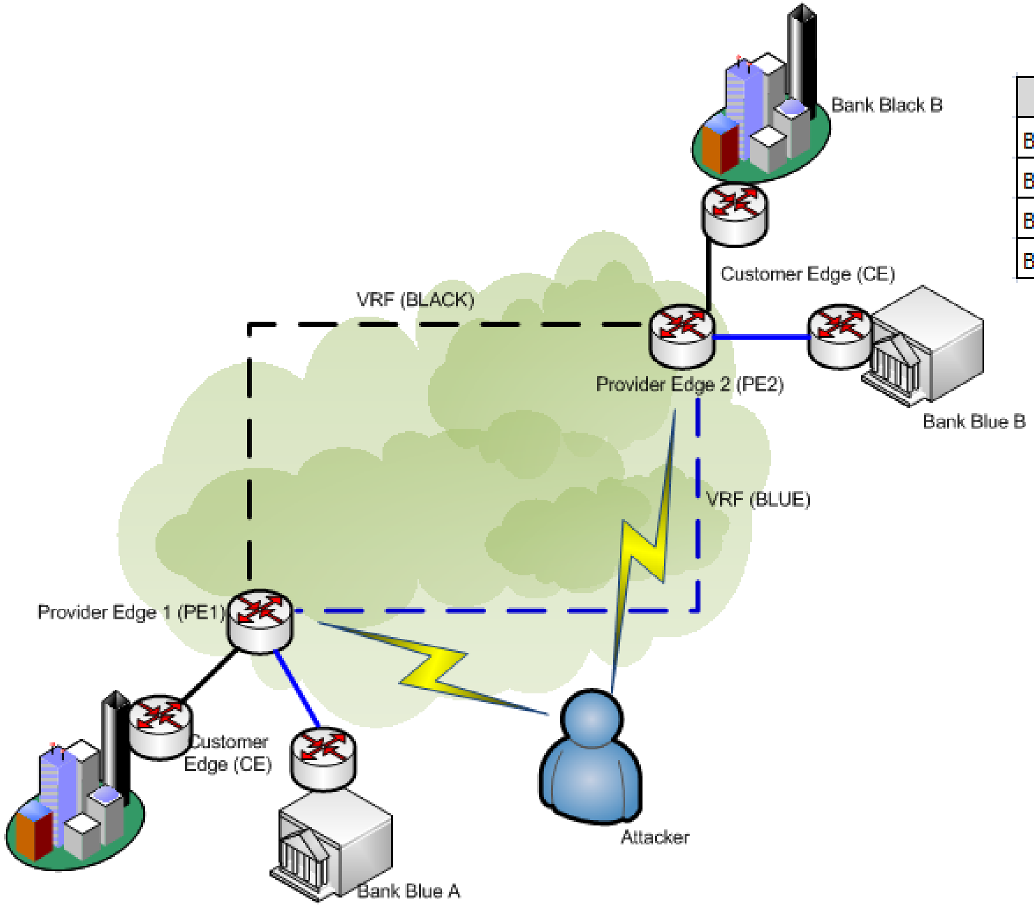


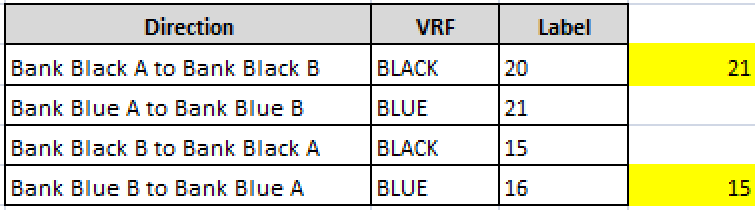
Direction	VRF	Label
Bank Black A to Bank Black B	BLACK	20
Bank Blue A to Bank Blue B	BLUE	21
Bank Black B to Bank Black A	BLACK	15
Bank Blue B to Bank Blue A	BLUE	16



- MPLS, as previously stated, use label to forward traffic
- VRF "Black" & "Blue" in PE, store routing table virtually separated, hence overlap network between Bank "Black" & Bank "Blue" can be forwarded correctly
- Bank "Black" can only communicate with Bank "Black" using VRF Black
- Bank "Blue" can only communicate with Bank "Blue" using VRF Black

MPLS Label Rewrite





Direction	VRF	Label	
Bank Black A to Bank Black B	BLACK	20	21
Bank Blue A to Bank Blue B	BLUE	21	
Bank Black B to Bank Black A	BLACK	15	
Bank Blue B to Bank Blue A	BLUE	16	15

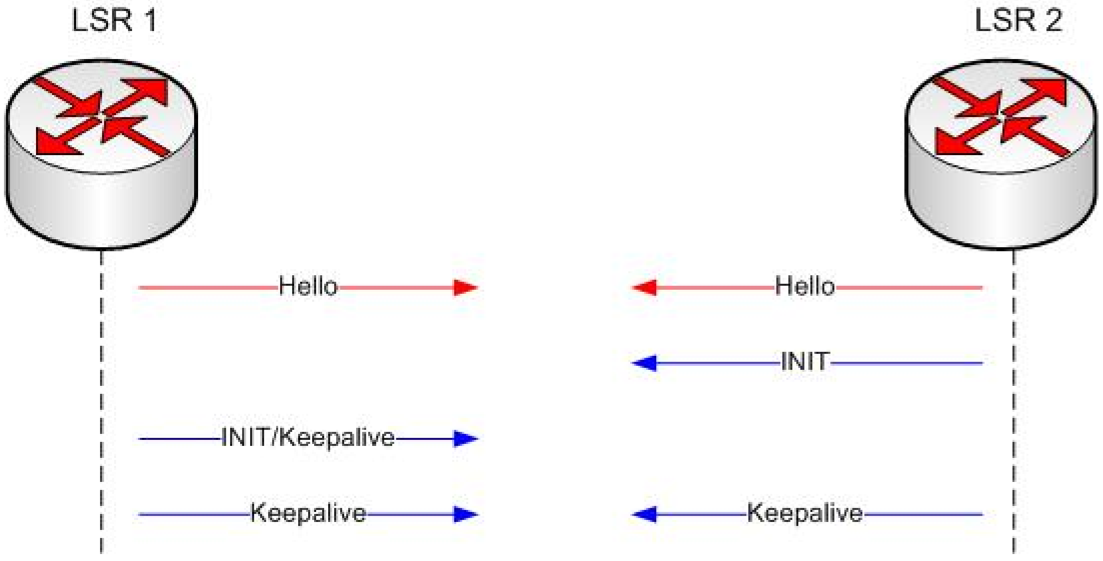
- Bank “Black” has overlap network with Bank “Blue”
- Hence, VRF “Black” and “Blue” has same routing entry
- Attacker change label for traffic PE1 to PE2 with 21 & PE2 to PE1 with 15 (see table)
- PE2 only know that traffic from PE1 with label 21 is for Bank “Blue”
- PE1 only know that traffic from PE2 with label 15 is for Bank “Black”
- Bank “Black” can communicate with Bank “Blue”
- Reproduce in lab, hard (impossible?) in real MPLS network

- Someone in “Man In The Middle” position between PE1 & PE2 can rewrite the MPLS Label
- Whoever they are, they can redirect traffic so Bank “Black” can communicate with Bank “Blue”

Label Distribution Protocol

- Protocol used by MPLS routers to exchange label mapping information
- UDP 646 for Hello, TCP 646 for establishing LDP Session
- Two MPLS routers that established LDP session called LDP Peers
- Exchange of information (advertisement) is bi-directional between LDP Peers
- Very well documented on RFC 5036

- Discovery Message
- Session Message
- Advertisement Message
- Notification Message



LDP Session Establishment (SRC: Wikipedia)

LDP Message Injection

- LDP is used to maintain LSP databases that are used to forward traffic through MPLS Network
- How if someone can inject label mapping message to LSR?
- Attacker needs access to the MPLS backbone so he can:
  1. Announce & maintain the presence of LSR (Hello/Discovery Message)
  2. Establish & maintain LDP session (Session Message)
  3. Send advertisement with label mapping message & change label database to redirect the traffic ☺
- Again, hard (impossible?) in real MPLS network but can be reproduced in lab with specific conditions/requirements

Border Gateway Protocol

- MP-BGP, in MPLS network, usually runs between PE router
- It is used to route network which their routing table is in VRF
- Attacker needs access to MPLS backbone either for:
  - Intercept & tamper initial MP-BGP exchange OR
  - Withdraw routes & insert new one (BGP Update with spoofed NLRI)
- Again, hard (impossible?) in real MPLS network but can be reproduced in lab with specific conditions/requirements

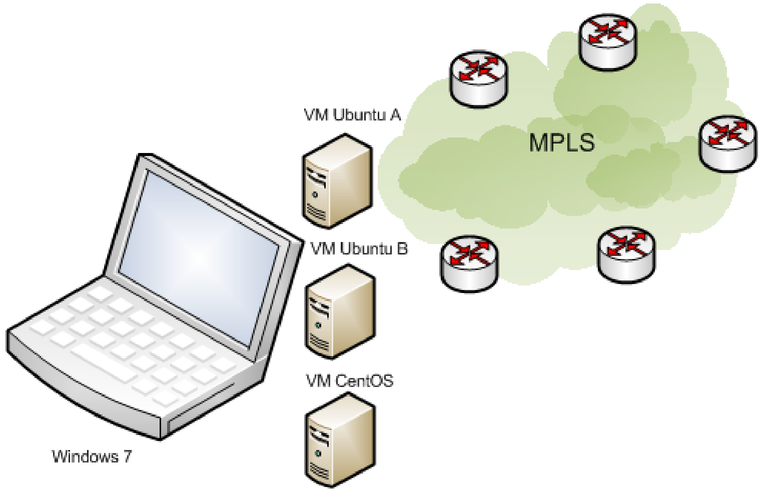
AN EXAMPLE

PROVIDED BY LOKI PROJECT / ERNW.DE

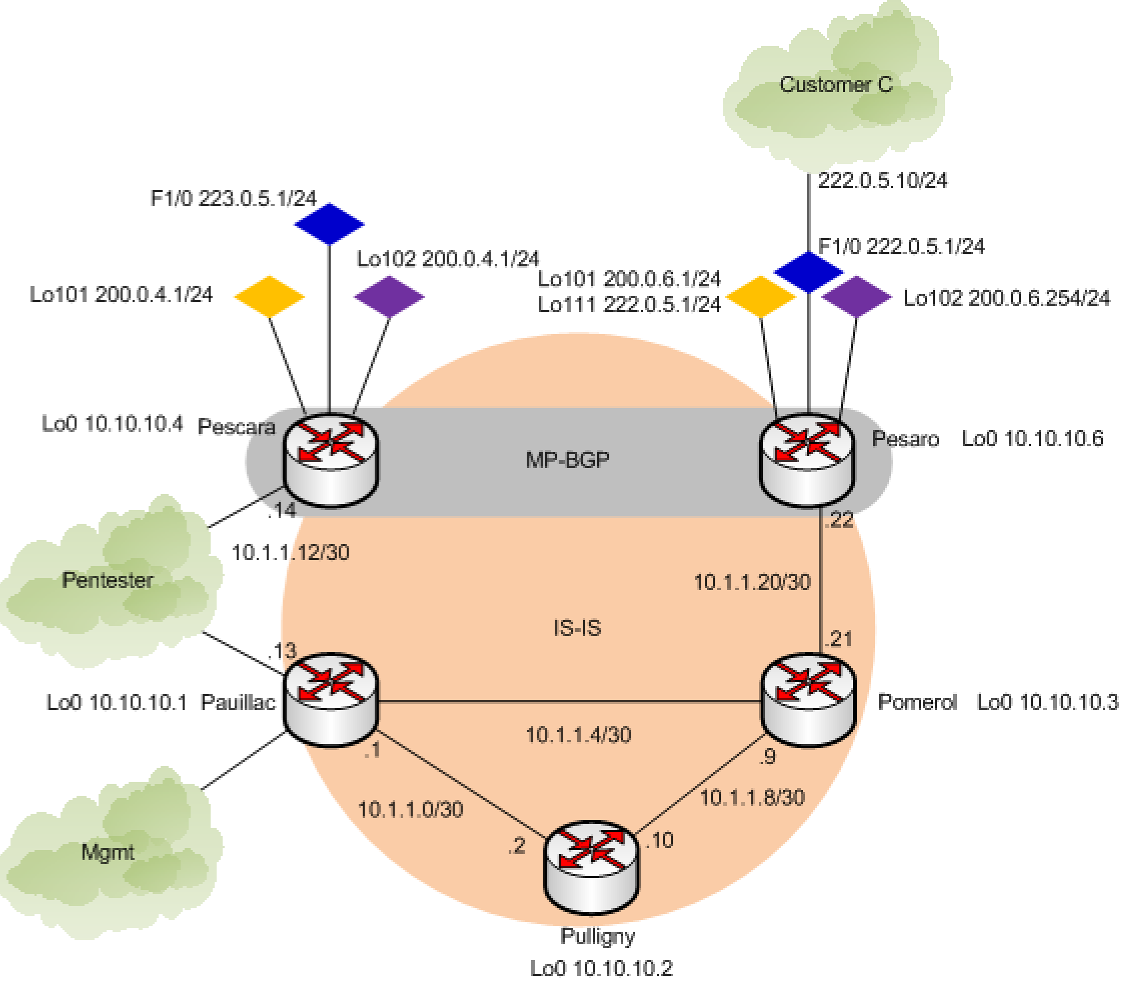
- MPLS (We Only Use This For The Document)
  - LDP, MPLS Label Rewrite
- ROUTING
  - RIP, OSPF, EIGRP, BGP
- HOT-STANDBY
  - HSRP, HSRPv2, BFD, VRRP, VRRPv3
- ARP
  - Spoofing, MAC Flooding
- ICMPv6
- DOT1Q
- TCP-MD5

DEMO

DEMO TOPOLOGY



MORE



DISCUSSION?! Q & A

THANK YOU ☺