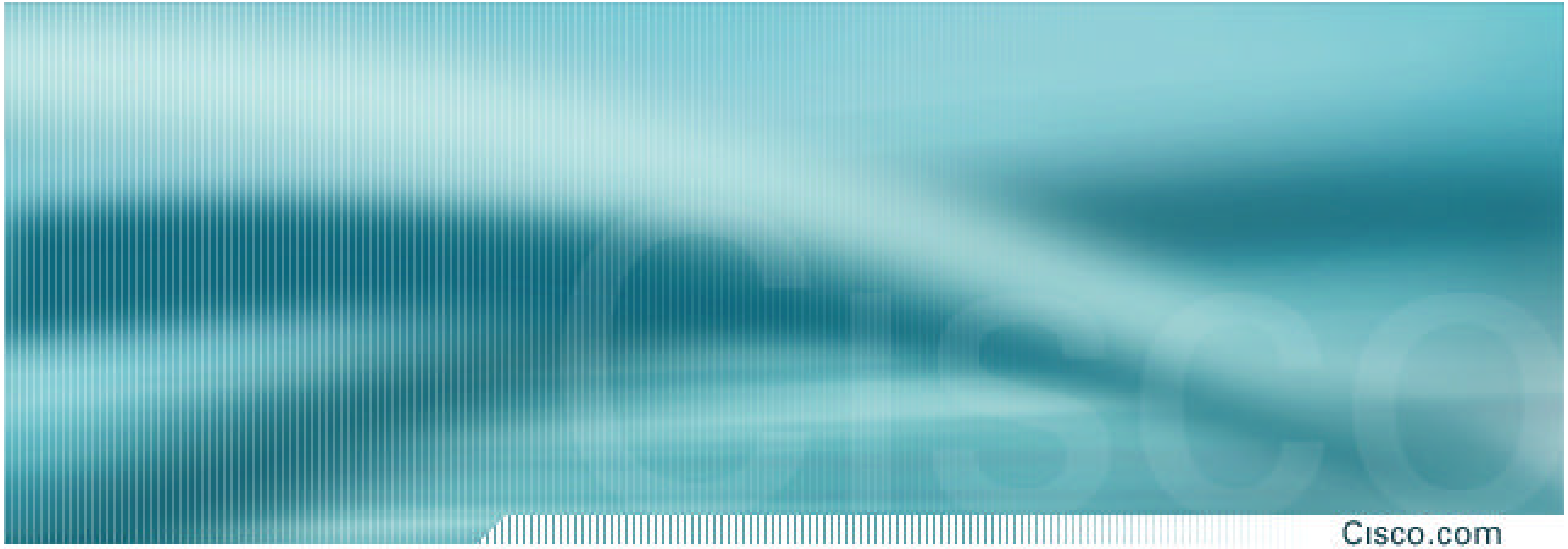


Router Security

Philip Smith <pfs@cisco.com>

AUUG Security Symposium

Brisbane

19-21 November 2001

Router Security

- Tutorial describes the key elements of router security

  Making the actual device secure

  Secure packet and route filtering when connected to a public network

  Making the network secure

  Using routers to aid the defence against DOS attacks

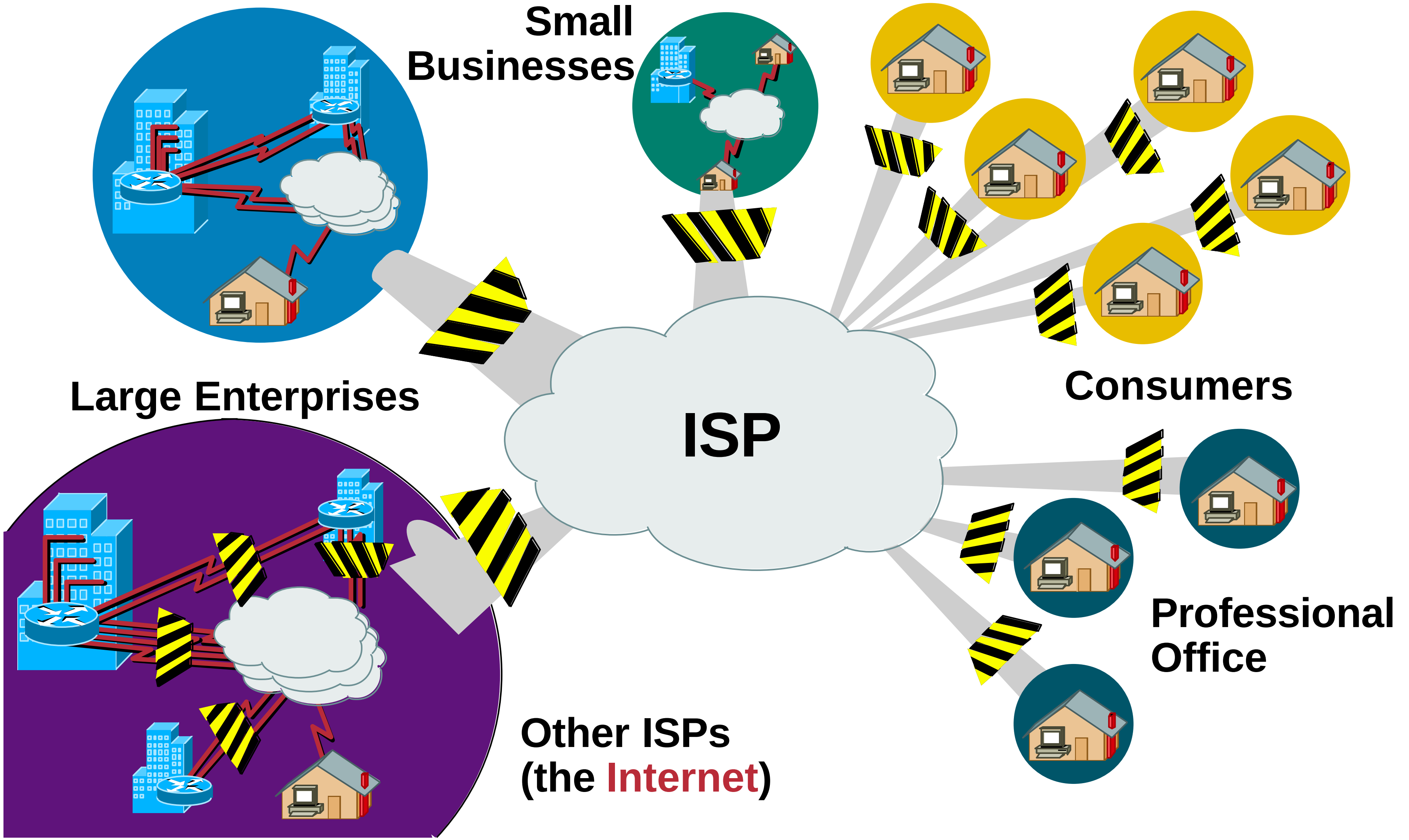
- These slides will be available at:

  www.cisco.com/public/cons/seminars/AUUG2001

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network

The Internet Today



The Internet Today

- Changing threat

  User friendly tools make it easier for the amateur cyberpunks to do more damage

  eCommerce provides a monetary motivation

  Direct attacks on the Internet’s core infrastructure means that the NET is not sacred anymore

  Common for ISPs to have several calls per day from their customers to help defend against attacks

Revenge of the Geeks

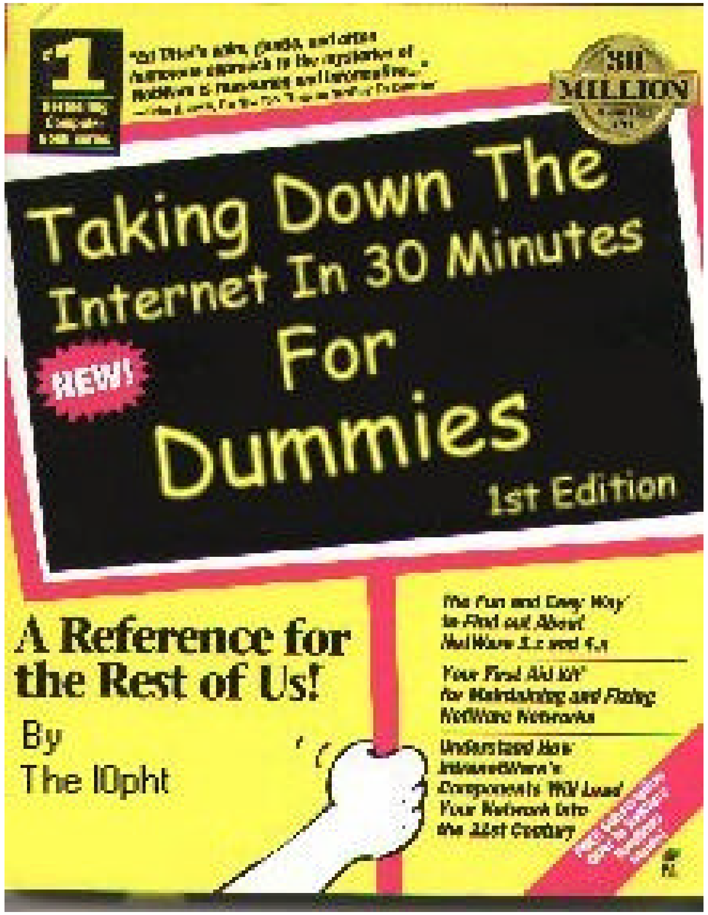
BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

Denial of Service (DoS) Goals

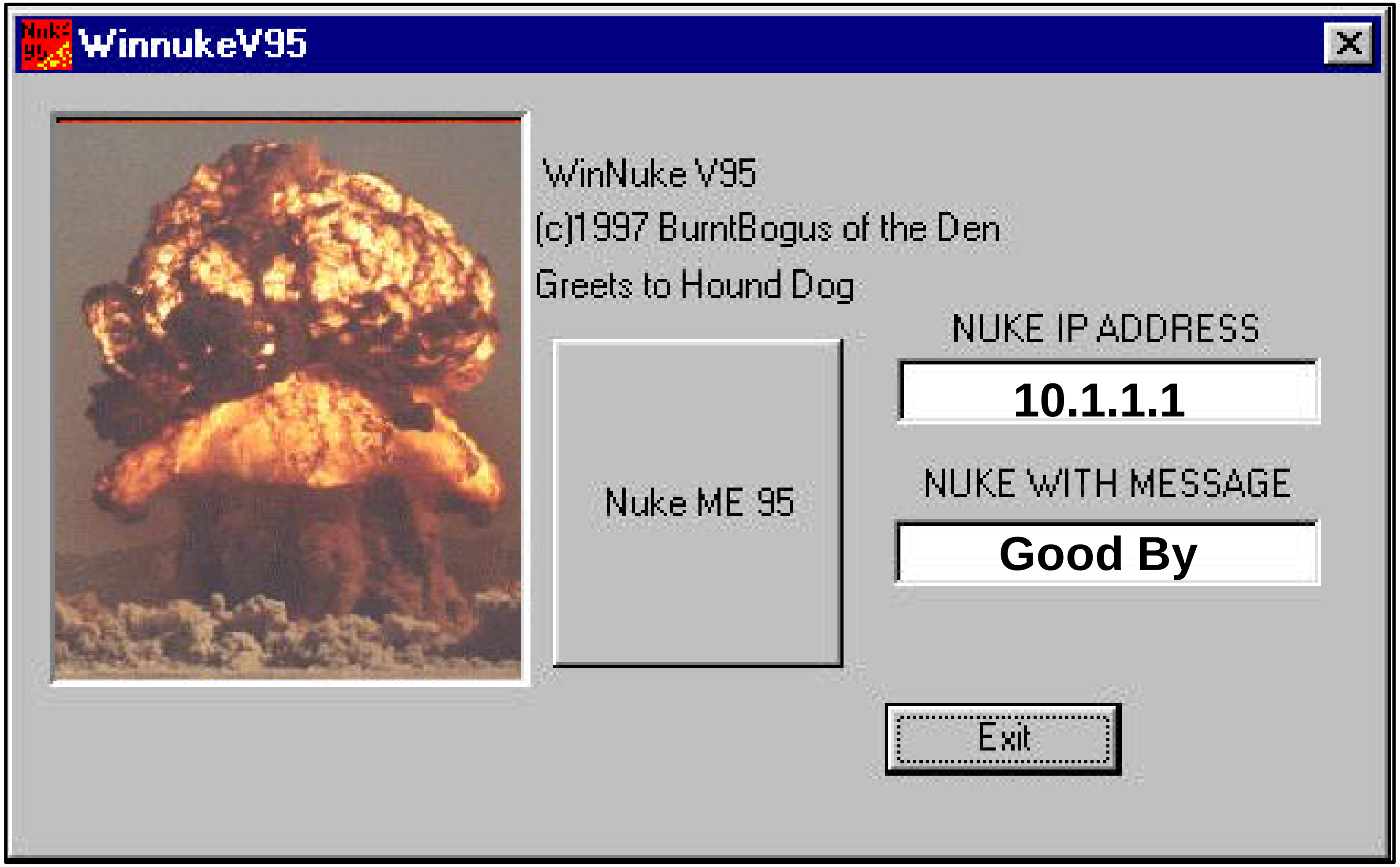
- Bring a resource or a system to its knees
- Keeps the resource too busy to attend to legitimate services
- Can be potentially directed at anything with an IP address, or reachable via an IP address
- Generally based on tool kits available on Internet
- No theft of data is involved
- Hard to determine loss
- Hard to trace back to source (bogus sources)

Motivation

- Vandalism
- Anger
- Political
- Curiosity
- Notoriety
- Malice
- Personal Gain


1
30 MILLION
Taking Down The Internet In 30 Minutes For Dummies
NEW!
1st Edition
A Reference for the Rest of Us!
By The l0pht
The Fun and Easy Way to Find out About NetWare 3.x and 4.x
Your First Aid Kit for Maintaining and Fixing NetWare Networks
Understand How IntranetWare's Components Will Lead Your Network Into the 21st Century

Attack Methods—WinNuke

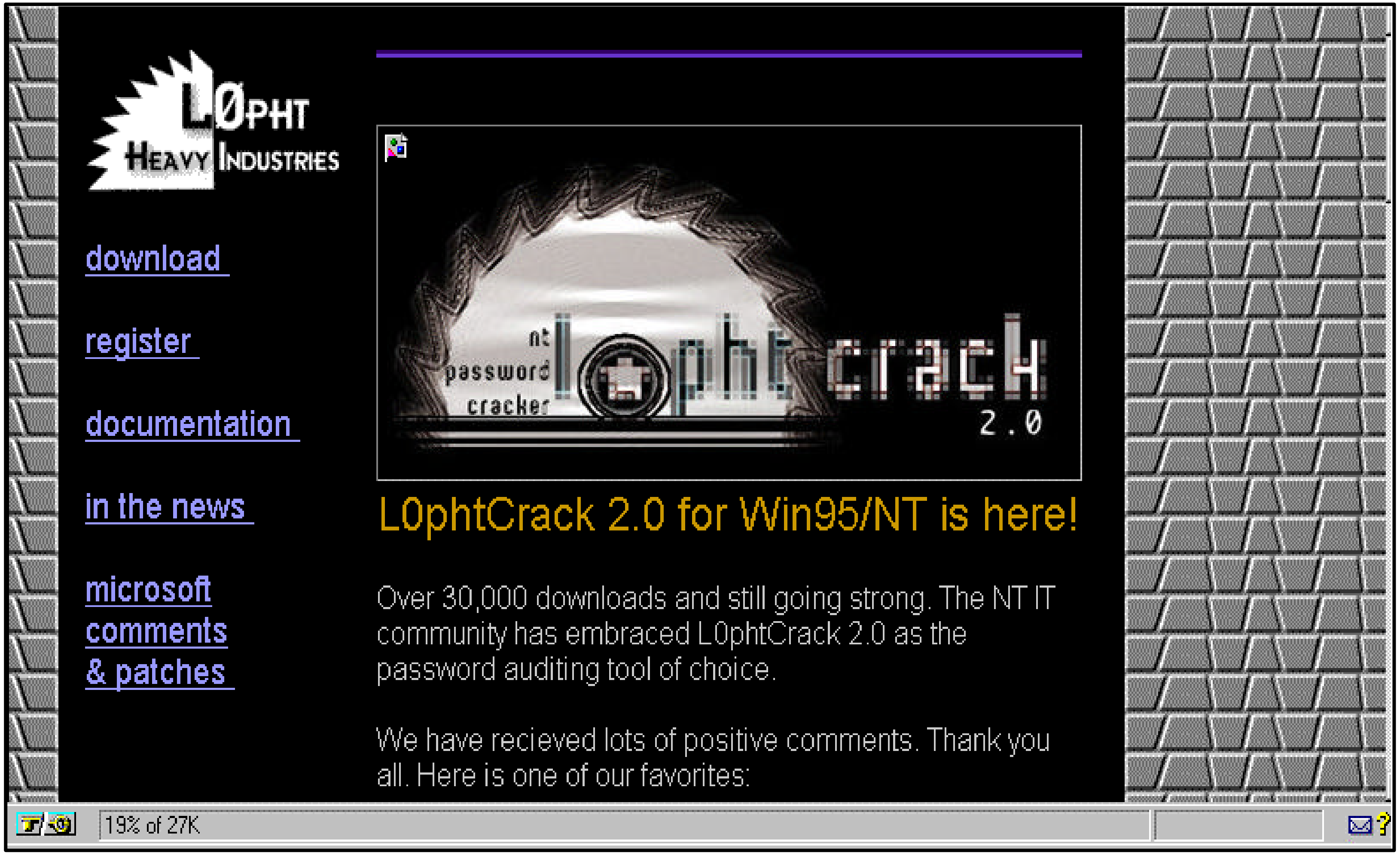


WinNuke V95
(c)1997 BurntBogus of the Den
Greets to Hound Dog

NUKE IP ADDRESS
10.1.1.1

NUKE WITH MESSAGE
Good By

Attack Methods—Crack Shareware



L0phtCrack 2.0 for Win95/NT is here!

Over 30,000 downloads and still going strong. The NT IT community has embraced L0phtCrack 2.0 as the password auditing tool of choice.

We have recieved lots of positive comments. Thank you all. Here is one of our favorites:

Service Provider Security

Cisco.com

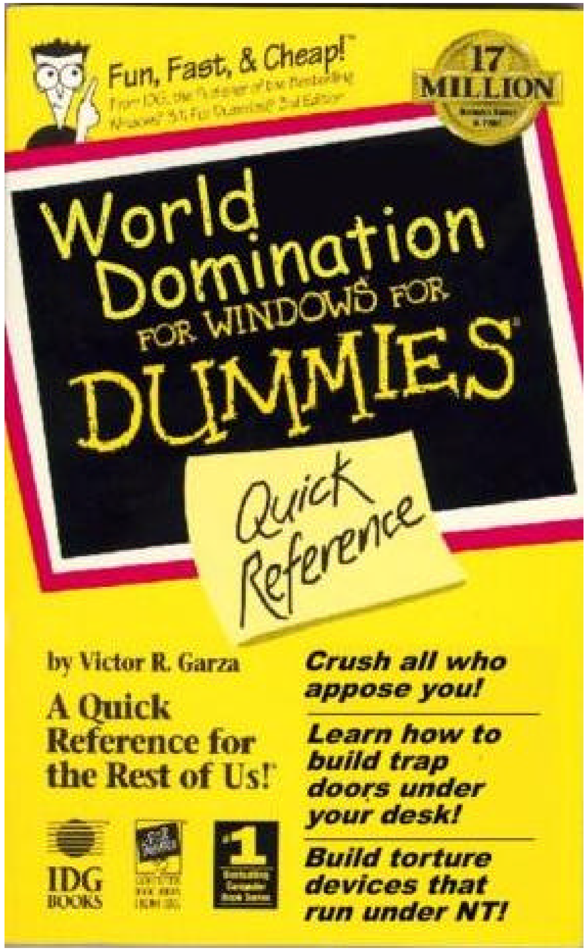
- **Service Providers need to:**

  Protect themselves

  Help protect their customers from the Internet

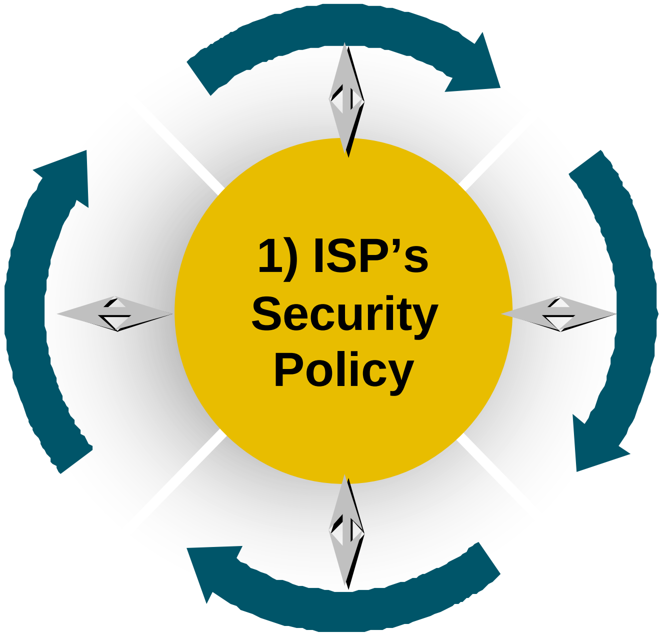
  Protect the Internet from their customers

  At any given time there are between 20 to 40 DOS/DDOS attacks on the Net


Fun, Fast, & Cheap!
17 MILLION
World Domination
FOR WINDOWS FOR
DUMMIES
Quick Reference
by Victor R. Garza
A Quick Reference for the Rest of Us!
Crush all who appose you!
Learn how to build trap doors under your desk!
Build torture devices that run under NT!
IDG BOOKS

What Do ISPs Need to Do?

Security Is Not Optional!



2) Secure
Firewall, Encryption, Authentication
(Firewalls, IPSEC, TACACS+/Radius)

1) ISP's Security Policy

3) Monitor and Respond
Intrusion Detection

4) Test
Vulnerability Scanning

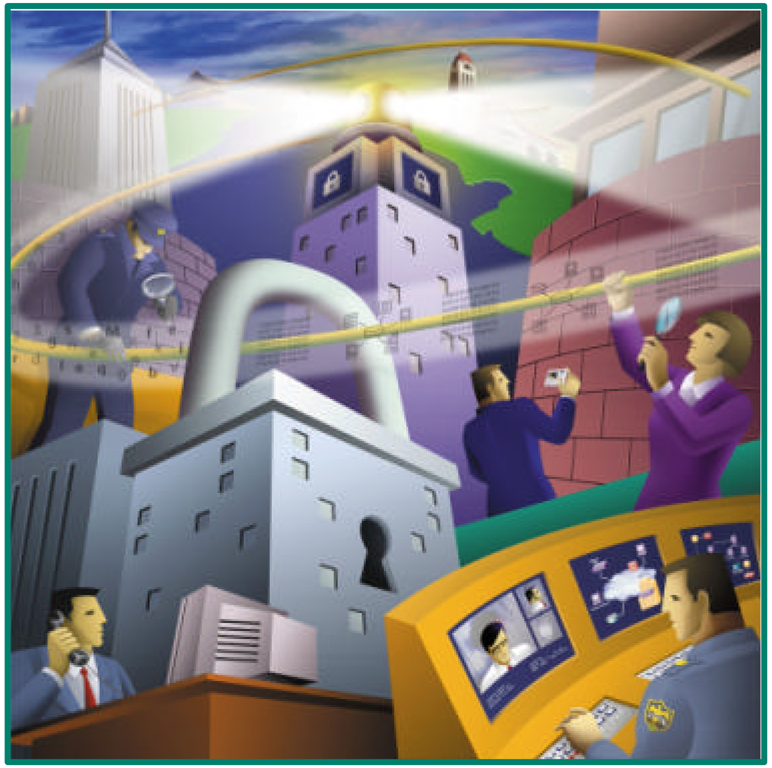
5) Manage and Improve
Network Operations and Security Professionals

What Do ISPs Need to Do?

- Implement Best Common Practices (BCPs)
  - ISP infrastructure security
  - ISP network security
  - ISP services security
- Work with operations groups, standards organisations and vendors on new solutions

Hardware Vendor’s Responsibilities

- The role of the hardware vendor is to support the network’s objectives. Hence, there is a very synergistic relationship between the ISP and the hardware vendor to ensure the network is resistant to security compromises



Hardware Vendor’s Responsibilities

- Cisco System’s example:
  - Operations people working directly with the ISPs
  - Emergency reaction teams (i.e. PSIRT)
  - Developers working with customers and IETF on new features
  - Security consultants working with customers on attacks, audits, and prosecution
  - Individuals tracking the hacker/phracker communities
  - Consultants working with governments/law enforcement officials

Network Security

- **Where to start…**

  Cisco Internet Security Advisories

  http://www.cisco.com/warp/public/707/advisory.html

  Cisco IOS documentation

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm

  RFC2196 (site security handbook)

  Cisco Networker's security sessions

Network Security

- Common misperception:

My network will be secure if I install a firewall

- Correct approach:

Every device connected to the public network needs to be properly secured

And that includes routers and switches!

- Network devices are the public network infrastructure

why compromise network security by not securing network devices?

Top 14 Vulnerabilities

- 1 – Misconfigured ACLs
- 2 – Unsecured/unmonitored remote access points
- 3 – Information leakage
- 4 – Hosts and devices running non-essential services
- 5 – Weak passwords
- 6 – User or test accounts with excess privileges
- 7 – Misconfigured Internet Servers

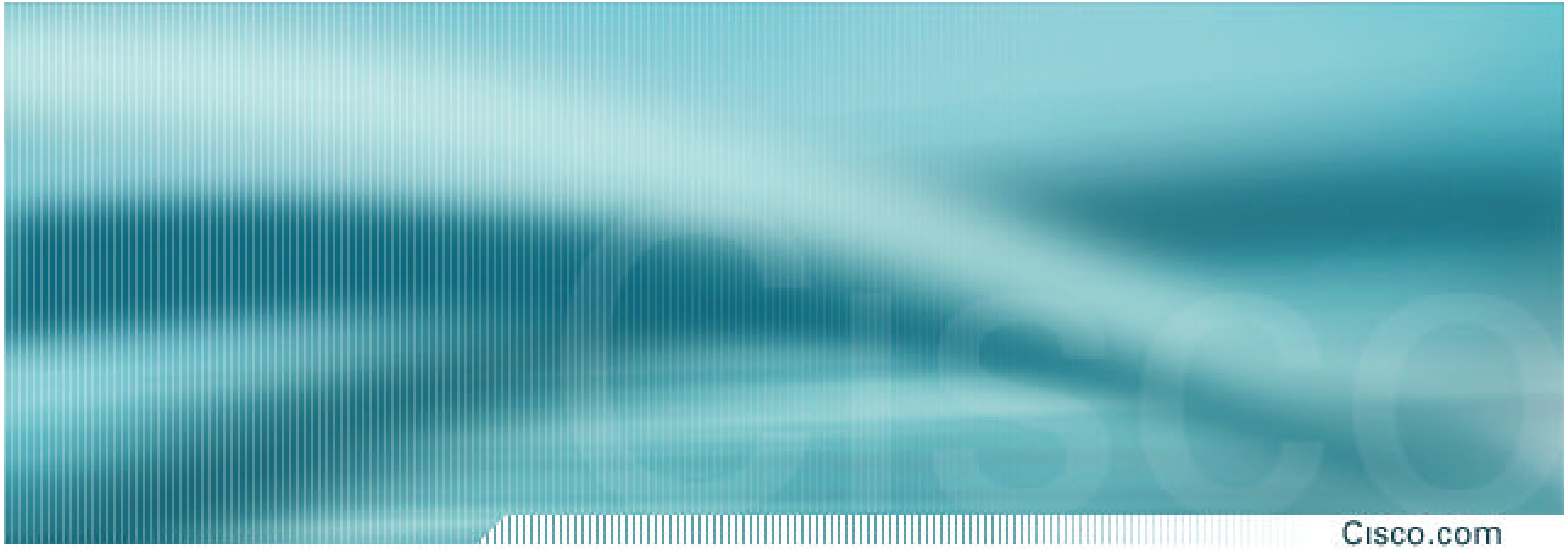
Top 14 Vulnerabilities (cont.)

- **8 – Misconfigured firewall or router ACL**
- **9 – Unpatched, outdated or vulnerable software**
- **10 – Excessive file and directory access controls**
- **11 – Excessive trust relationships**
- **12 – Unauthenticated services e.g. X-Windows**
- **13 – Inadequate logging, monitoring and detection**
- **14 – Lack of well accepted security policies/procs**

Source: ©2000 Cisco *SAFEGuarding the E-Business Network*

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network



Securing the Router

Router Security

- Routers shipped by vendors have:
  - Default configuration
  - No configured Security
  - Many services switched on to make getting started easier
- Once a router has an IP address, it is accessible to the outside world
  - Campus LAN
  - Company LAN
  - Internet

Global Services You Turn OFF

- Some services, turned on by default, should be turned off to prevent security breaches/attacks

```
no ip finger

no service pad

no service udp-small-servers

no service tcp-small-servers

no ip bootp server
```

Global Services You Turn OFF

- **Finger**

  Find out who is logged in, from where, how long for

- **PAD**

  Historical – from the days of X.25

- **Small servers**

  Tcp and udp ports < 20 are for developing IP stacks and not needed in day to day operations

- **Bootp**

  Used by systems to bootstrap themselves onto the network – e.g. X-terminals

Interface Services You Turn OFF

- Some IP features make life easy on campus LANs, but do not make sense on a public backbone
- All interfaces on an SP’s backbone router should have the following as a default:

```
no ip redirects

no ip directed-broadcast

no ip proxy-arp
```

Interface Services You Turn OFF

- IP redirects

  Router will send redirect message if it has to resend a packet through the same interface it was received on

- Direct-broadcast

  If packet intended for network broadcast address, router will physically broadcast it onto the attached network

  The cause of all SMURF attacks on the Internet

- Proxy-arp

  Dumb host sends arp request for destination – documented in RFC1027

  If router knows how to get to that destination, it will install an entry in the arp table for that destination

Cisco Discovery Protocol

- **Lets network administrators discover neighbouring Cisco equipment, model numbers and software versions**
- **Should not be needed on ISP network or a well controlled corporate backbone**

```
no cdp run
```

- **Should not be activated on any public facing interface: IXP, customer, upstream ISP – unless part of the peering agreement**
- **Disable per interface**

```
no cdp enable
```

Cisco Discovery Protocol

```
alpha>sh cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
beta7200.cisco.com  Ser 1/1        124           R        7206      Ser 2/1
sw2.cisco.com       Eth 1/1        178          T S       WS-C2924M-Fas 0/12
delta.cisco.com     Ser 2/0        146           R        3640      Ser 1/0
gamma.cisco.com     Ser 2/1        138           R        3640      Ser 1/1
```

Cisco Discovery Protocol

```
alpha>sh cdp neigh detail
-------------------------
Device ID: beta7200.cisco.com
Entry address(es):
  IP address: 192.168.9.5
Platform: cisco 7206,  Capabilities: Router
Interface: Serial1/1,  Port ID (outgoing port): Serial2/1
Holdtime : 144 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-K4P-M), Version 12.0(19)S, EARLY DEPLOYMENT
   RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 05-Oct-01 15:52 by nmasa
```

Login Banner

- Login banner displayed prior to login prompt
- Use a good login banner, or nothing at all:

```
banner login ^
  Authorised access only
  This system is the property of Galactic Internet
  Disconnect IMMEDIATELY if you are not an authorised user!
  Contact noc@net.galaxy +99 876 543210 for help.
^
```

Exec Banner

- Exec banner display after successful login
- Useful to remind users of local conditions:

```
banner exec ^
  PLEASE NOTE - THIS ROUTER SHOULD NOT HAVE A DEFAULT ROUTE!
  It is used to connect paying peers. These ‘customers’
  should not be able to default to us.
  The config for this router is NON-STANDARD
  Contact Network Engineering +99 876 543234 for more info.
^
```

Use Enable Secret

- Encryption '7' on a Cisco is reversible
- The “enable secret” password is encrypted via a one-way algorithm

```
enable secret <removed>

no enable password

service password-encryption
```

VTY and Console Port Timeouts

- Default idle timeout on async ports is 10 minutes 0 seconds

```
exec-timeout 10 0
```

- Timeout of 0 means permanent connection
- TCP keepalives on incoming network connections

```
service tcp-keepalives-in
```

VTY Security

- Access to VTYs should be controlled, not left open
- Consoles should be used for last resort admin only:

```
access-list 3 permit 221.17.1.0 0.0.0.255
access-list 3 deny   any
line vty 0 4
 access-class 3 in
 exec-timeout 5 0
 transport input telnet
 transport output none
 transport preferred none
 password 7 045802150C2E
```

VTY Security

- Use more robust ACLs with the logging feature to spot the probes on you network

```
access-list 199 permit tcp 1.2.3.0 0.0.0.255 any
access-list 199 permit tcp 1.2.4.0 0.0.0.255 any
access-list 199 deny   tcp any any range 0 65535 log
access-list 199 deny   ip any any log
!
line vty 0 4
 access-class 199 in
```

VTY Access and SSHv1

- Secure shell server supported as from IOS 12.0S and 12.1T
- Obtain, load and run appropriate crypto images on router
- Set up SSH on router

```
beta7200(config)#crypto key generate rsa
```

- Add it as input transport

```
line vty 0 4
  transport input telnet ssh
```

VTY Access and SSHv1

- Secure shell client added as from IOS 12.0(10)S and 12.1T
  - Telnet should not be used any more
- Add ssh as output transport
  - Remove telnet as a transport

```
line vty 0 4
  transport input ssh
  transport output ssh
```

VTY Access and SSHv1

- **Example:**

  Ensure you have the proper image (post 12.0(10)S with "k4p")

  ```
  e.g. c7200-k4p-mz.120-18.S1.bin
  ```

  Set up SSH on the router

  ```
  beta7200(config)#crypto key generate rsa
  ```

  Use the SSH client:

  ```
  ssh -l myuser myhost "sh users"
  ssh -l myuser -c 3des -o 5 -p 22 myhost
  ```

User Authentication

- Account per user, with passwords

```
aaa new-model
aaa authentication login neteng local
username joe password 7 1104181051B1
username jim password 7 0317B21895FE
line vty 0 4
 login neteng
 access-class 3 in
```

- Username/password is slightly more resistant to attack than a plain password

User Authentication

- Use centralised authentication system
  - RADIUS – Recommended for user authentication/accounting
  - TACACS+ – Recommended for securing the network

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa accounting exec start-stop tacacs+
ip tacacs source-interface Loopback0
tacacs-server host 221.17.1.1
tacacs-server host 221.15.35.8
tacacs-server key CKr3t#
line vty 0 4
 access-class 3 in
```

User Authentication

Cisco.com

TACACS+ Provides a Detailed Audit Trail of what Is Happening on the Network Devices

User-Name	Group-cmd		priv-lvl	service	NAS-Portname	task_id	NAS-IP-reason
bgreene	NOC	enable <cr>	0	shell	tty0	4	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	5	210.210.51.224
bgreene	NOC	no aaa accounting exec Workshop <cr>	0	shell	tty0	6	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	8	210.210.51.224
pfs	NOC	enable <cr>	0	shell	tty0	11	210.210.51.224
pfs	NOC	exit <cr>	0	shell	tty0	12	210.210.51.224
bgreene	NOC	enable <cr>	0	shell	tty0	14	210.210.51.224
bgreene	NOC	show accounting <cr>	15	shell	tty0	16	210.210.51.224
bgreene	NOC	write terminal <cr>	15	shell	tty0	17	210.210.51.224
bgreene	NOC	configure <cr>	15	shell	tty0	18	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	20	210.210.51.224
bgreene	NOC	write terminal <cr>	15	shell	tty0	21	210.210.51.224
bgreene	NOC	configure <cr>	15	shell	tty0	22	210.210.51.224
bgreene	NOC	aaa new-model <cr>	15	shell	tty0	23	210.210.51.224
bgreene	NOC	aaa authorization commands 0 default tacacs+ none <cr>	15	shell	tty0	24	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	25	210.210.51.224
bgreene	NOC	ping <cr>	15	shell	tty0	32	210.210.51.224
bgreene	NOC	show running-config <cr>	15	shell	tty66	35	210.210.51.224
bgreene	NOC	router ospf 210 <cr>	15	shell	tty66	45	210.210.51.224
bgreene	NOC	debug ip ospf events <cr>	15	shell	tty66	46	210.210.51.224

User Authentication

- **When you have TACACS+ on a router:**
  - **Do not need a local username/password**
  - **Do not give out the local enable secret**
  - **Lock them in a safe in the NOC in case of total TACACS+ failure**
- **Threat – disgruntled employees can attack/disable TACACS+**
  - **If they know the local enable secret, they could get into the routers**
- **If you really believe you need local username/passwords despite TACACS+**
  - **Can now encrypt the local password with MD5 hash**

User Authentication

- So now you can have the following:

```
aaa new-model
aaa authentication login default tacacs+ local enable
aaa authentication enable default tacacs+ enable
aaa accounting exec start-stop tacacs+
!
username joe secret 5 $1$j6Ac$3KarJszBV3VMaL/2Nio3E.
username jim secret 5 $1$LPV2$QO4NwAudy0/4AHHHQHvWj0
!
ip tacacs source-interface Loopback0
tacacs-server host 221.17.1.1
tacacs-server key CKr3t#
line vty 0 4
 access-class 3 in
```

Source Routing

- **IP has a provision to allow source IP host to specify route through Internet**
- **ISPs should turn this off, unless it is specifically required:**

```
no ip source-route
```

- ***traceroute -s* to investigate network failures – valuable tool**

if you are not using *traceroute -s* then turn off the feature!

ICMP Unreachable Overload

- All Routers which have any static route to Null0 should configure *no ip unreachables* (i.e. for BGP Advertisements).

```
interface Null0
 no ip unreachables
!
ip route <dest to drop> <mask> null0
```

ICMP Unreachable Rate-Limiting

- ICMP Unreachable Rate-Limiting Command:

```
ip icmp rate-limit unreachable [DF] <1-4294967295
  millisecond>

no ip icmp rate-limit unreachable [df]
```

- Turned on by default and hidden since 12.0(8)S. Default value set to 500 milliseconds.
- Peer Review with several top ISP operations engineers are recommending this be set at 1 second for normal and DF.

What Ports Are open on the Router?

- It may be useful to see what sockets/ports are open on the router
- *Show ip sockets*

```
gw>sh ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17 203.37.255.121    514 202.12.29.64    57617   0   0   10   0
 17 203.37.255.121    162 203.37.255.126  57556   0   0    0   0
 17 0.0.0.0           123 139.130.64.98     123   0   0    1   0
 17 203.37.255.121  39481 203.37.255.126    161   0   0    1   0
 17 202.12.29.129     514 202.12.29.64    49533   0   0   10   2
 17 203.37.255.121     49 203.37.255.126     49   0   0   11   0
```

Introducing a new Router to the Network

1. Set hostname
2. Set passwords

   Enable secret and temporary vty passwords

3. Disable unnecessary services

   Global and per interface

4. Configure access-lists

   For vty and snmp access

   For live interfaces (if required)

5. Only now assign IP address and plug into network

Introducing a new Router to the Network

6. Configure TACACS+

   Remove local vty passwords

7. Configure NTP and Logging

8. Configure SNMP (if required)

   Check access and what is being monitored

9. Configure remaining interfaces

10. Configure routing protocols

    Include any necessary inbound and outbound filters

11. Confirm router security on network

    Tools like SAINT are very useful

Summary

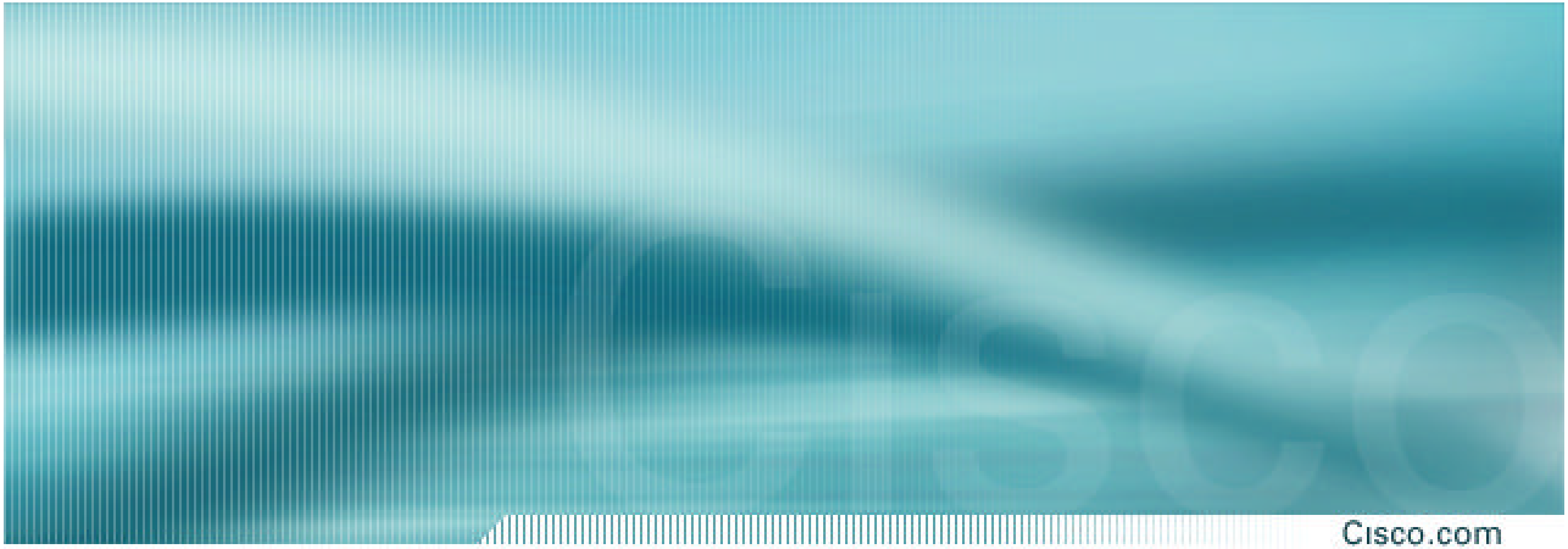
- These hints apply to routers (and switches, and any other IP infrastructure device)
- May be software release dependent

  But do your research so that only necessary services are left running on the router

  Beware “convenient vendor defaults” – often they are a major cause of security problems on any network

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network



Securing the Routing Protocols

Routing Protocol Security

- Routing protocol can be attacked

  Denial of service

  Smoke screens

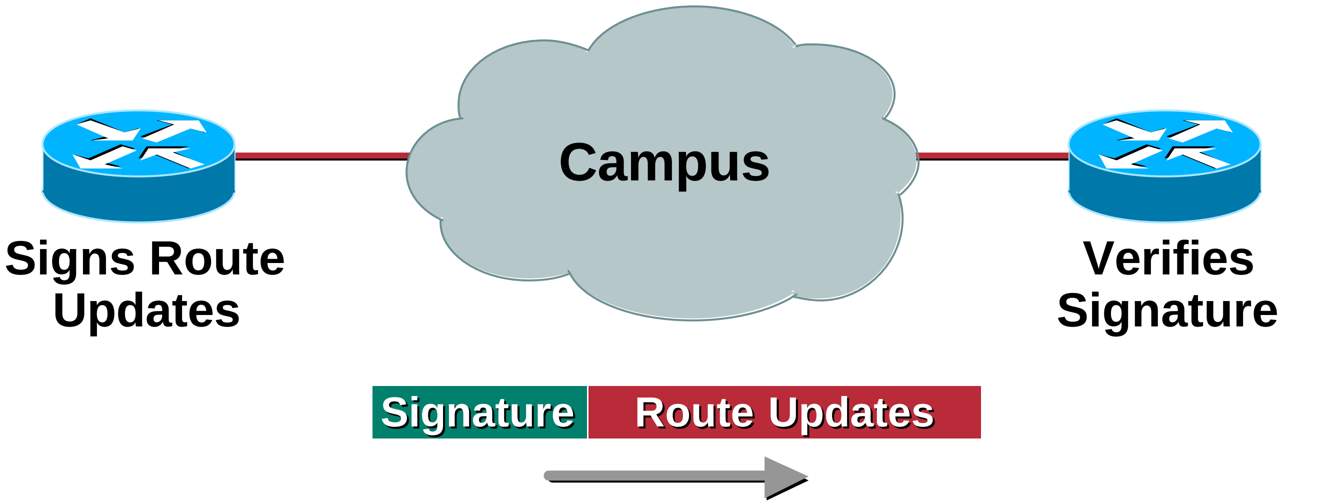
  False information

  Reroute packets

May Be Accidental or Intentional

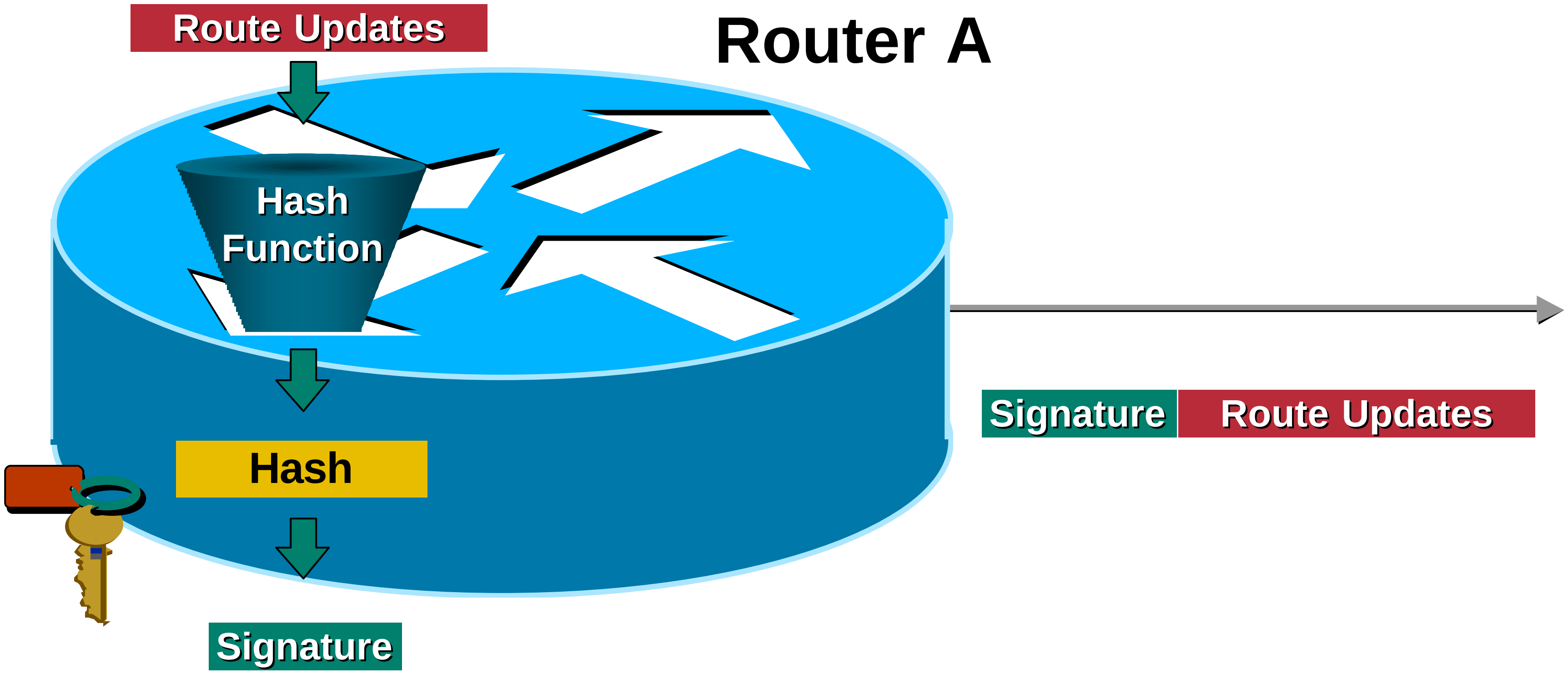
Secure Routing
Route Authentication

Configure Routing Authentication



Certifies Authenticity of Neighbour and Integrity of Route Updates

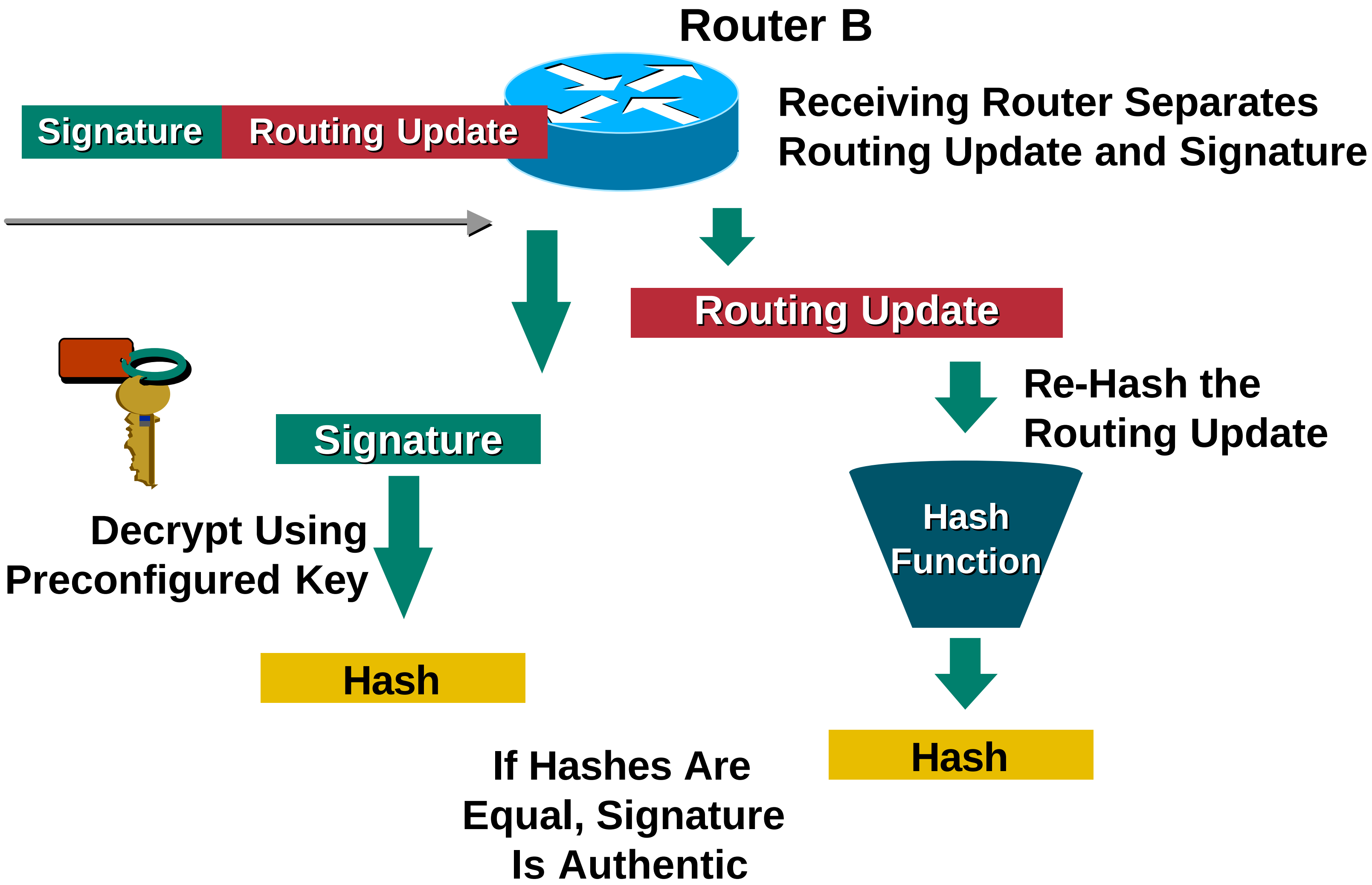
Signature Generation



Signature = Encrypted Hash of Routing Update

Signature Verification

Cisco.com


Router B

Signature | Routing Update

Receiving Router Separates Routing Update and Signature

Routing Update

Re-Hash the Routing Update

Hash

Signature

Decrypt Using Preconfigured Key

Hash

If Hashes Are Equal, Signature Is Authentic

Route Authentication

- Authenticates routing update packets
- Shared key included in routing updates

    Plain text—Protects against accidental problems only

    Message Digest 5 (MD5)—Protects against accidental and intentional problems

Route Authentication

- Multiple keys supported
  - Key lifetimes based on time of day
  - Only first valid key sent with each packet
- Supported in: BGP, IS-IS, OSPF, RIPv2, and EIGRP(11.2(4)F)
- Syntax differs depending on routing protocol

OSPF Route Authentication

- OSPF area authentication

  Two types

  Simple password

  Message Digest (MD5)

ip ospf authentication-key *key* (this goes under the specific interface)
area *area-id* **authentication** (this goes under "router ospf <process-id>")

ip ospf message-digest-key *keyid* **md5** *key* (used under the interface)
area *area-id* **authentication message-digest** (used under "router ospf <process-id>")

OSPF and ISIS Authentication Example

- **OSPF**

```
interface ethernet1
 ip address 10.1.1.1 255.255.255.0
 ip ospf message-digest-key 100 md5 cisco
!
router ospf 1
 network 10.1.1.0 0.0.0.255 area 0
 area 0 authentication message-digest
```

- **ISIS**

```
interface ethernet0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
 isis password cisco level-2
!
```

BGP Route Authentication

```
router bgp 200
 no synchronization
 log-neighbor-changes
 neighbor 4.1.2.1 remote-as 300
 neighbor 4.1.2.1 description Link to Excalabur
 neighbor 4.1.2.1 send-community
 neighbor 4.1.2.1 version 4
 neighbor 4.1.2.1 route-map Community1 out
 neighbor 4.1.2.1 password 7 cisco
```

BGP Route Authentication

- **Works per neighbour or for an entire peer-group**
- **Two routers with password mis-match:**

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP
address]:11004 to [local router's IP address]:179
```

- **One router has a password and the other does not:**

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP
address]:11003 to [local router's IP address]:179
```

Selective Packet Discard

- When a link goes to a saturated state, you will drop packets; the problem is that you will drop any type of packets—including your routing protocols
- Selective Packet Discard (SPD) will attempt to drop non-routing packets instead of routing packets when the link is overloaded

```
ip spd enable (11.1 CA & CC)
```

- Enabled by default from 11.2(5)P and later releases, available option in 11.1CA/CC
- 12.0 the syntax changes and the default is to enable SPD

Selective Packet Discard

- **Attack of IP packets with bad TTL are process switched with ICMP reply – crippling the router**

```
ip spd mode aggressive
```

- **`show ip spd`**

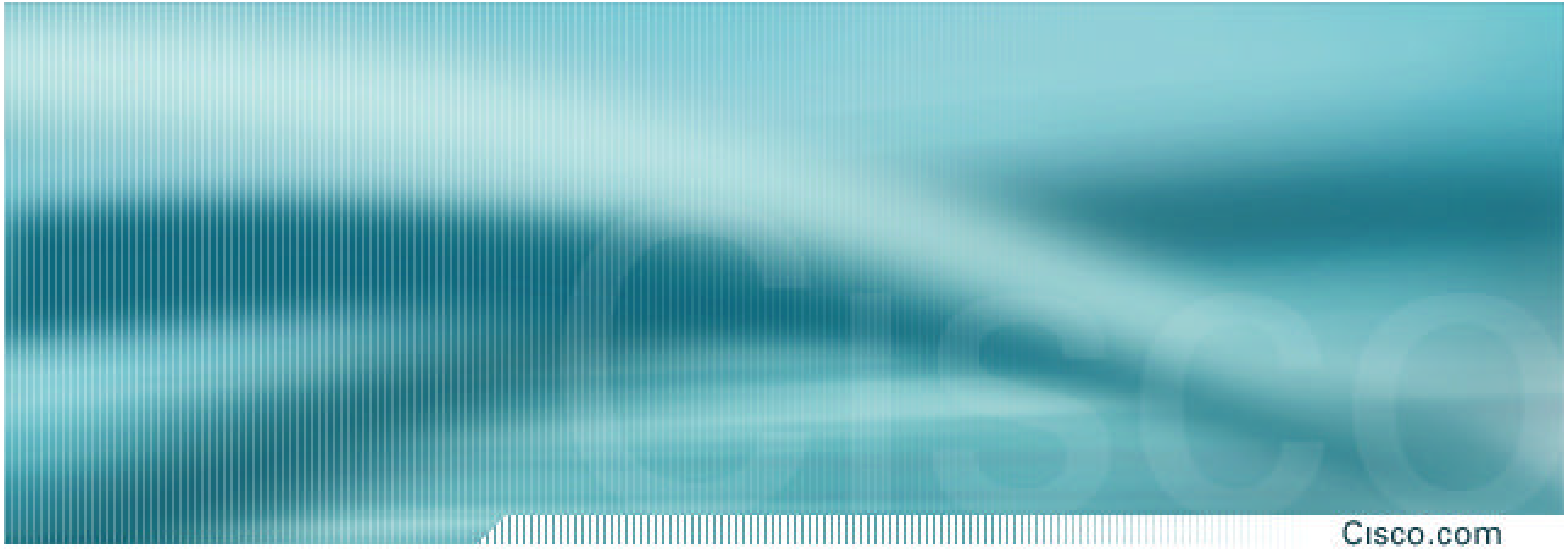
```
Current mode: normal.

Queue min/max thresholds: 73/74, Headroom: 100

IP normal queue: 2, priority queue: 0

SPD special drop mode: aggressively drop
bad packets
```

Summary

- Securing routing protocols is mandatory on any network which is part of the Internet
- Not doing so has potential to leave the network vulnerable to attack

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network



Securing the Network

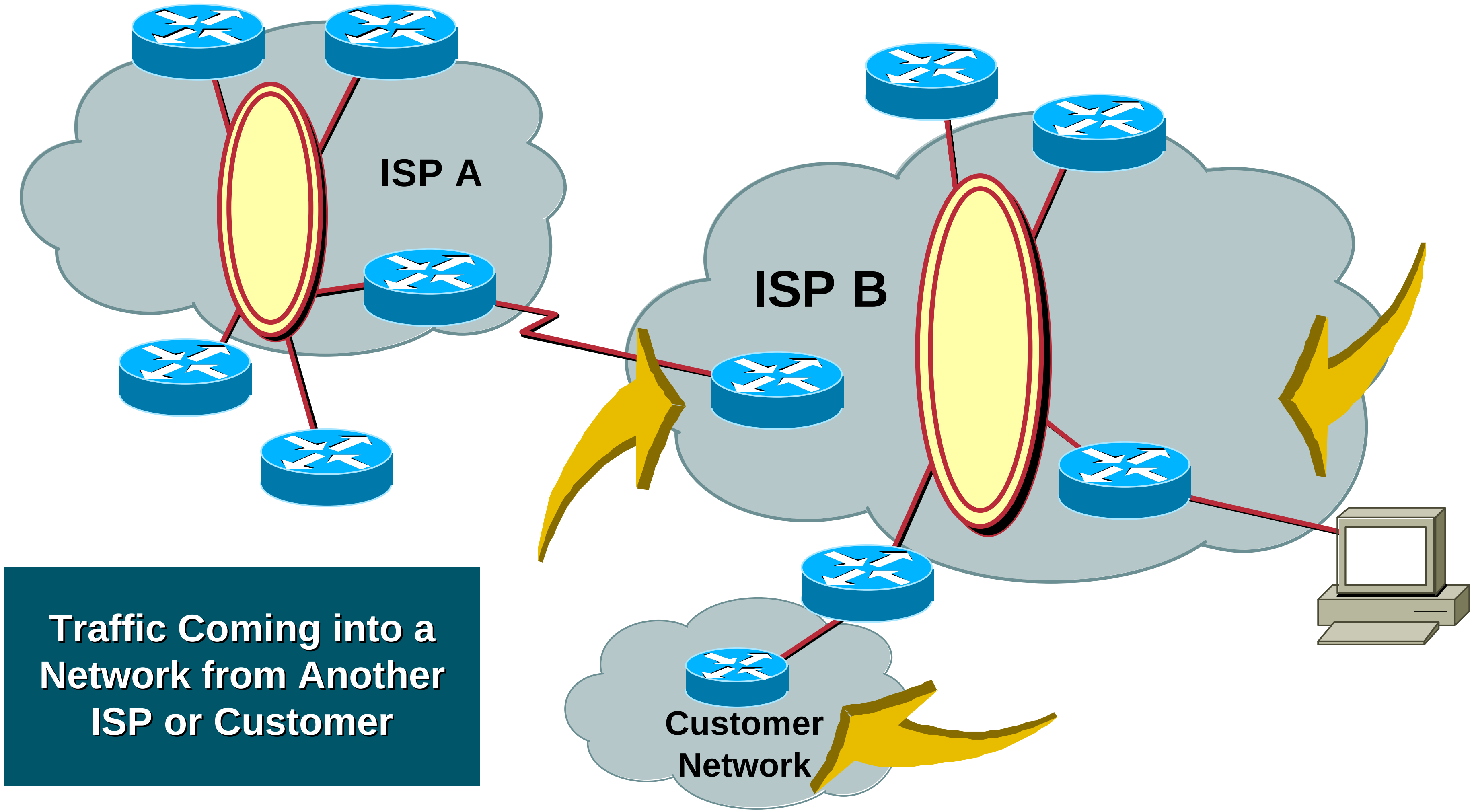
Securing the Network

- **Two mandatory ingredients for router based network security:**

  Route filtering

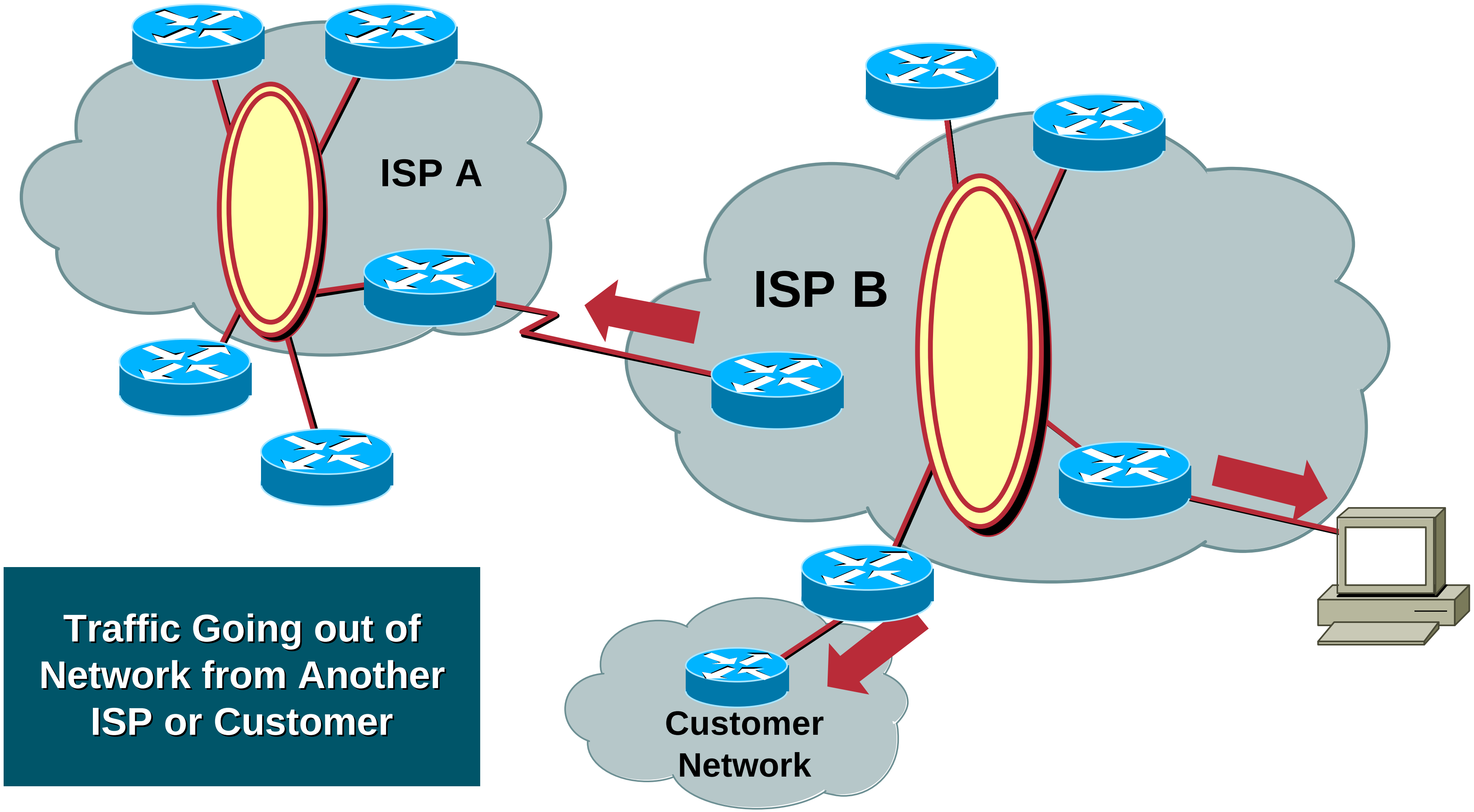
  Packet filtering

Ingress Filters—Inbound Traffic

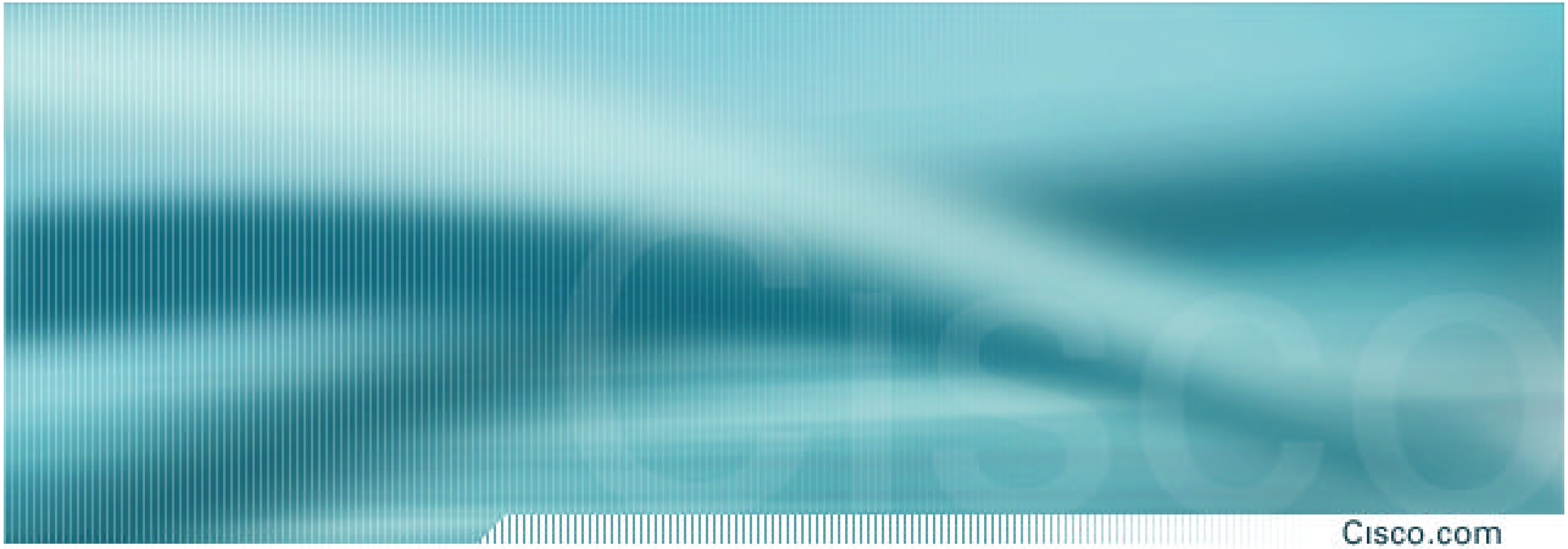


Traffic Coming into a Network from Another ISP or Customer

Egress Filters—Outbound Traffic



Traffic Going out of Network from Another ISP or Customer



Route Filtering

Ingress and Egress Route Filtering

- There are routes that should NOT be routed on the Internet
  - RFC 1918 and “Martian” networks
  - 127.0.0.0/8 and multicast blocks
  - See Bill Manning’s ID for background information:
    - ftp://ftp.ietf.org/internet-drafts/draft-manning-dsua-07.txt
- BGP should have filters applied so that these routes are not advertised to or propagated through the Internet

Ingress and Egress Route Filtering

- Quick overview

  0.0.0.0/8 – Default/broadcast & other unique properties

  127.0.0.0/8 – Host loopback network

  192.0.2.0/24 – TEST-NET, used in documentation etc

  10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 – RFC 1918 private addresses

  169.254.0.0/16 – End node auto-config in absence of DHCP

  224.0.0.0/3 – Multicast and former E-space block

Ingress and Egress Route Filtering

- Two flavours of route filtering:

  Distribute list – Widely used

  Prefix list – Increasingly used, easier syntax

- Both work fine—Engineering preference

Ingress and Egress Route Filtering

Extended ACL for a BGP Distribute List

```
access-list 150 deny ip 0.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 150 deny ip 10.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 150 deny ip 127.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 150 deny ip 169.254.0.0 0.0.255.255 255.255.0.0 0.0.255.255
access-list 150 deny ip 172.16.0.0 0.15.255.255 255.240.0.0 0.15.255.255
access-list 150 deny ip 192.0.2.0 0.0.0.255 255.255.255.0 0.0.0.255
access-list 150 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
access-list 150 deny ip 224.0.0.0 31.255.255.255 224.0.0.0 31.255.255.255
access-list 150 permit ip any any
```

Ingress and Egress Route Filtering

BGP with Distribute-list Flavour of Route Filtering

```
router bgp 200
 no synchronization
 bgp dampening
 neighbor 220.220.4.1 remote-as 210
 neighbor 220.220.4.1 version 4
 neighbor 220.220.4.1 distribute-list 150 in
 neighbor 220.220.4.1 distribute-list 150 out
 neighbor 222.222.8.1 remote-as 220
 neighbor 222.222.8.1 version 4
 neighbor 222.222.8.1 distribute-list 150 in
 neighbor 222.222.8.1 distribute-list 150 out
 no auto-summary
!
```

Ingress and Egress Route Filtering

Prefix-List for a for a BGP Prefix List

```
ip prefix-list rfc1918-sua deny   0.0.0.0/8 le 32
ip prefix-list rfc1918-sua deny   10.0.0.0/8 le 32
ip prefix-list rfc1918-sua deny   127.0.0.0/8 le 32
ip prefix-list rfc1918-sua deny   169.254.0.0/16 le 32
ip prefix-list rfc1918-sua deny   172.16.0.0/12 le 32
ip prefix-list rfc1918-sua deny   192.0.2.0.0/24 le 32
ip prefix-list rfc1918-sua deny   192.168.0.0/16 le 32
ip prefix-list rfc1918-sua deny   224.0.0.0/3 le 32
ip prefix-list rfc1918-sua permit 0.0.0.0/0 le 32
```

Ingress and Egress Route Filtering

BGP with Prefix-List Flavour of Route Filtering

```
router bgp 200
 no synchronization
 bgp dampening
 neighbor 220.220.4.1 remote-as 210
 neighbor 220.220.4.1 version 4
 neighbor 220.220.4.1 prefix-list rfc1918-sua in
 neighbor 220.220.4.1 prefix-list rfc1918-sua out
 neighbor 222.222.8.1 remote-as 220
 neighbor 222.222.8.1 version 4
 neighbor 222.222.8.1 prefix-list rfc1918-sua in
 neighbor 222.222.8.1 prefix-list rfc1918-sua out
 no auto-summary
!
```

Using BGP

- **Only accept prefixes your neighbour is entitled to send**
  - **If they originate 221.10.0.0/20, then you should only accept this prefix**

```
router bgp 200
 no synchronization
 bgp dampening
 neighbor 220.220.4.1 remote-as 210
 neighbor 220.220.4.1 version 4
 neighbor 220.220.4.1 prefix-list customer in
 no auto-summary
!
ip prefix-list customer permit 221.10.0.0/20
!
```

Using BGP

- **Only send prefixes you are entitled to send**

  If you originate 221.10.0.0/20, then you should only send this prefix

```
router bgp 200
 no synchronization
 bgp dampening
 neighbor 220.220.4.1 remote-as 210
 neighbor 220.220.4.1 version 4
 neighbor 220.220.4.1 prefix-list my-peer out
 no auto-summary
!
ip prefix-list customer permit 221.10.0.0/20
!
```

Using BGP

- **If you are receiving the full routing table**

  In addition to previously mentioned special use addresses, block your own prefix coming in

```
router bgp 200
 no synchronization
 bgp dampening
 neighbor 220.220.4.1 remote-as 210
 neighbor 220.220.4.1 version 4
 neighbor 220.220.4.1 prefix-list rfc1918-sua in
 no auto-summary
!
ip prefix-list rfc1918-sua <snip>
ip prefix-list rfc1918-sua deny 224.0.0.0/3 le 32
ip prefix-list rfc1918-sua deny 221.10.0.0/20 le 32
ip prefix-list rfc1918-sua permit 0.0.0.0/0 le 32
!
```

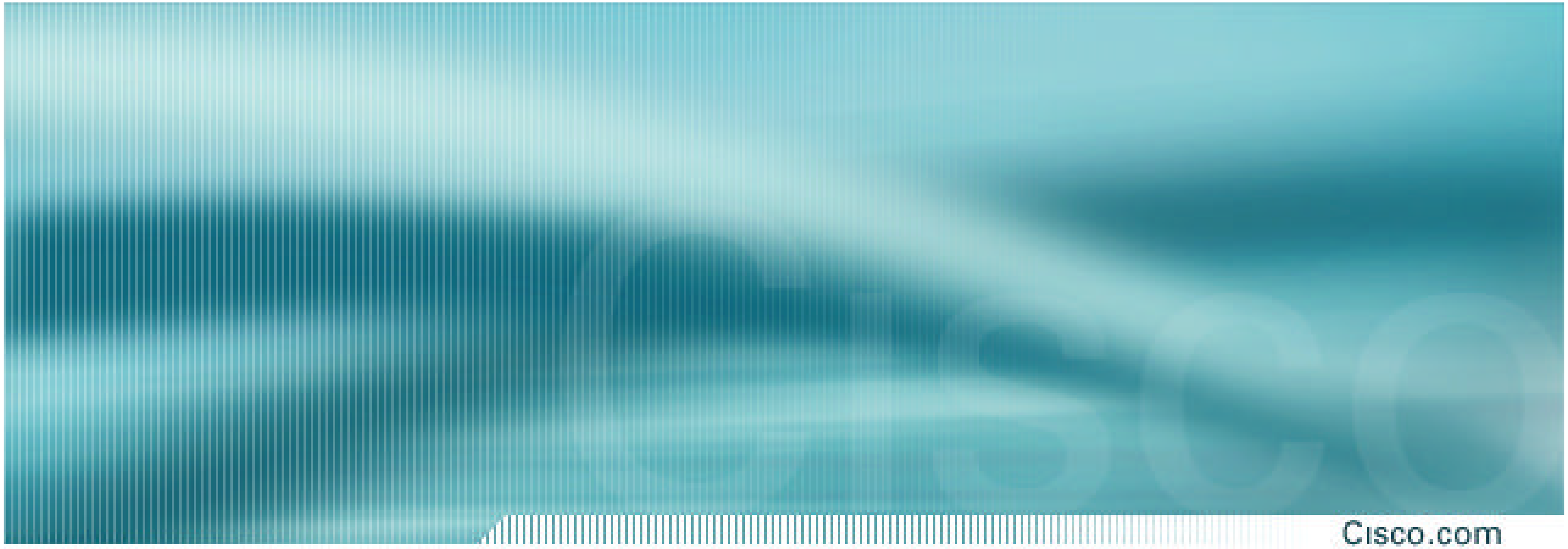
Using BGP

- General principle

  Be frugal in what you send

  Be sparing in what you receive

- Many network security and service denial instances caused by lax and careless BGP configuration



Packet Filtering

Ingress and Egress Packet Filtering

Your customers should not be sending any IP packets out to the Internet with a source address other then the address you have allocated to them!

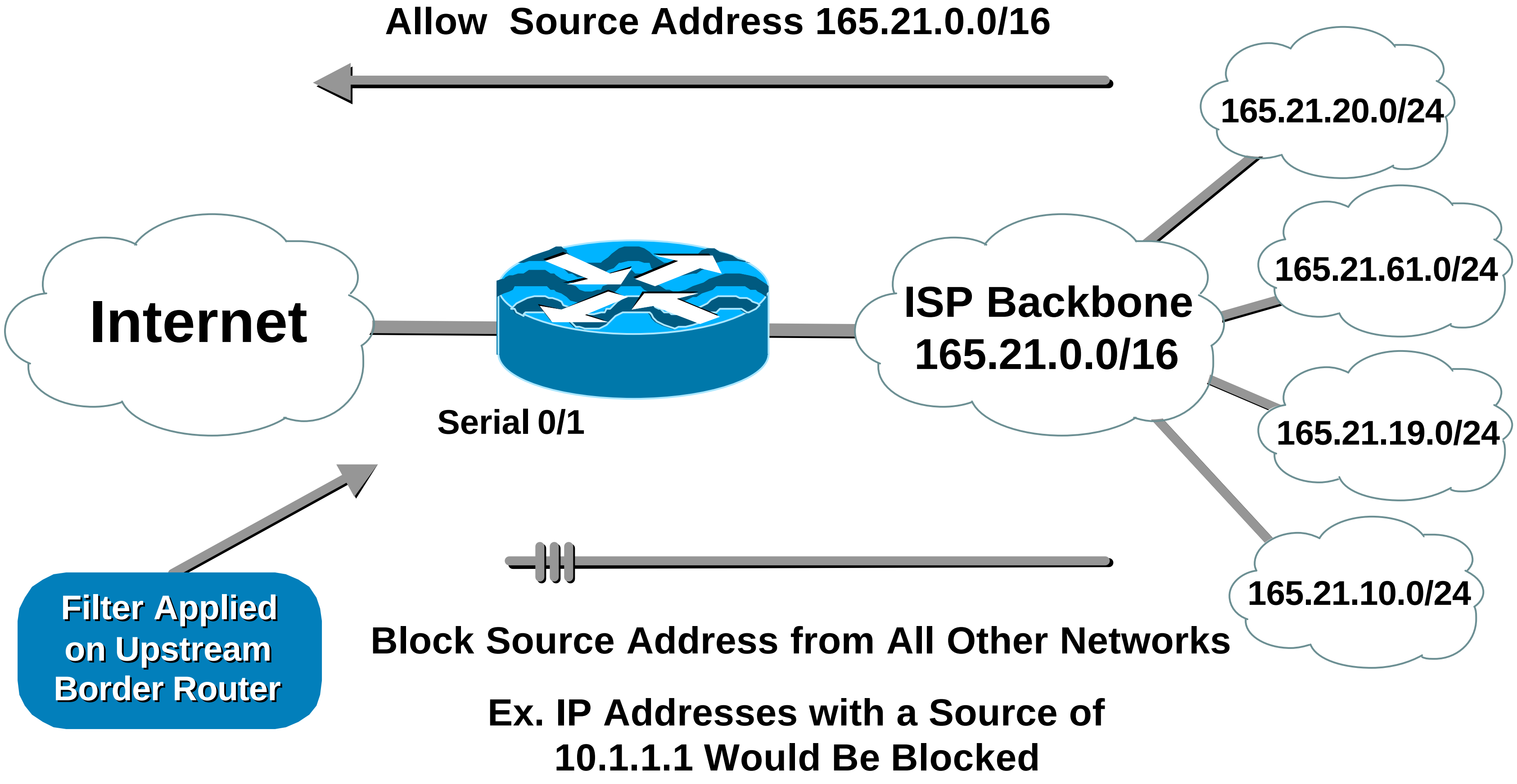
Ingress and Egress Packet Filtering

- **BCP 38/ RFC 2827**
- **Title: Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing**
- **Author(s): P. Ferguson, D. Senie**

Packet Filtering

- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Rate Limiting & Precedence Values

Egress Packet Filtering Upstream Border

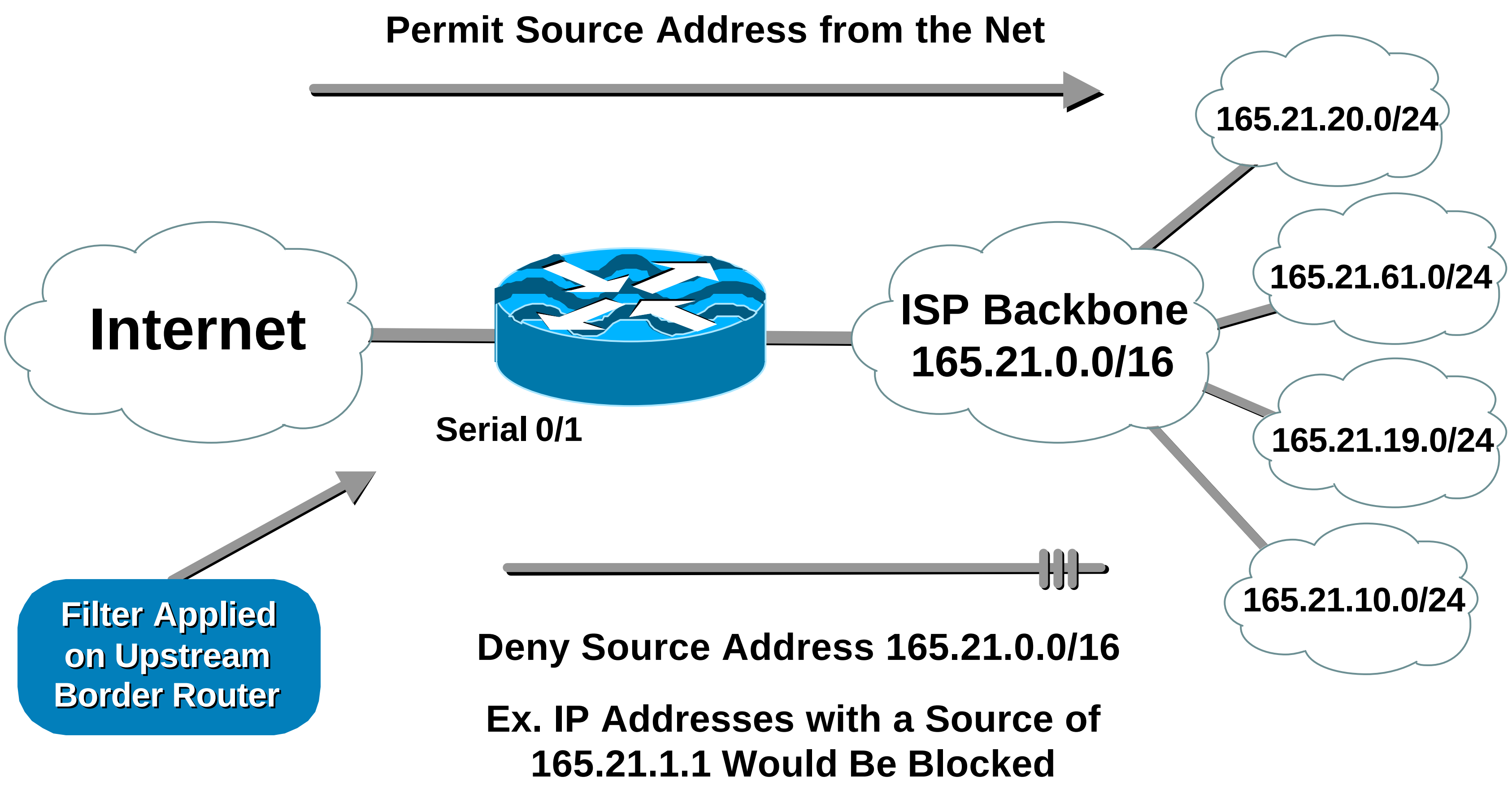


Allow Source Address 165.21.0.0/16

Block Source Address from All Other Networks

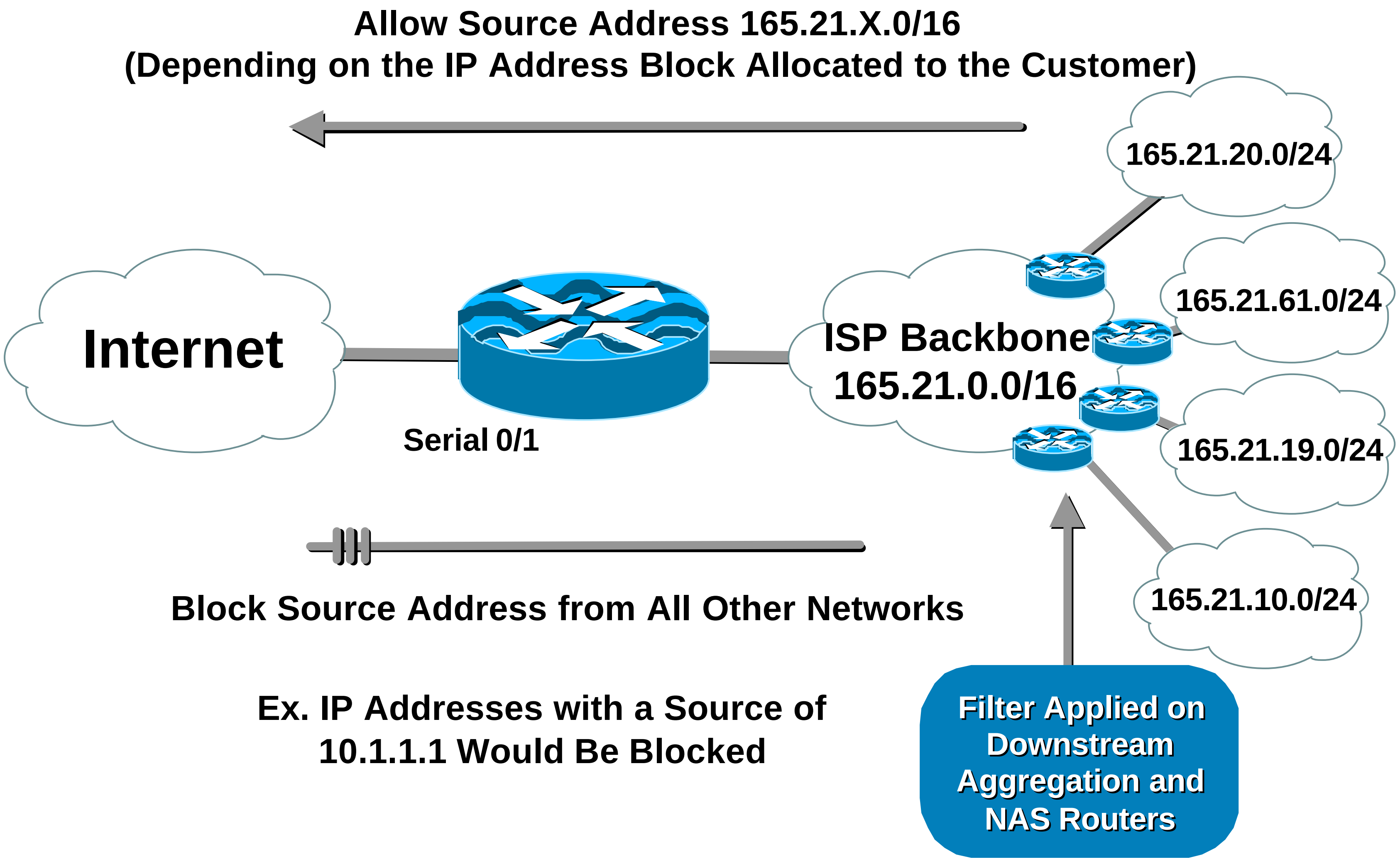
Ex. IP Addresses with a Source of 10.1.1.1 Would Be Blocked

Ingress Packet Filtering Upstream Border


Permit Source Address from the Net
Internet
Serial 0/1
ISP Backbone
165.21.0.0/16
165.21.20.0/24
165.21.61.0/24
165.21.19.0/24
165.21.10.0/24
Filter Applied on Upstream Border Router
Deny Source Address 165.21.0.0/16

Ex. IP Addresses with a Source of 165.21.1.1 Would Be Blocked

Ingress Packet Filtering Customer Edge



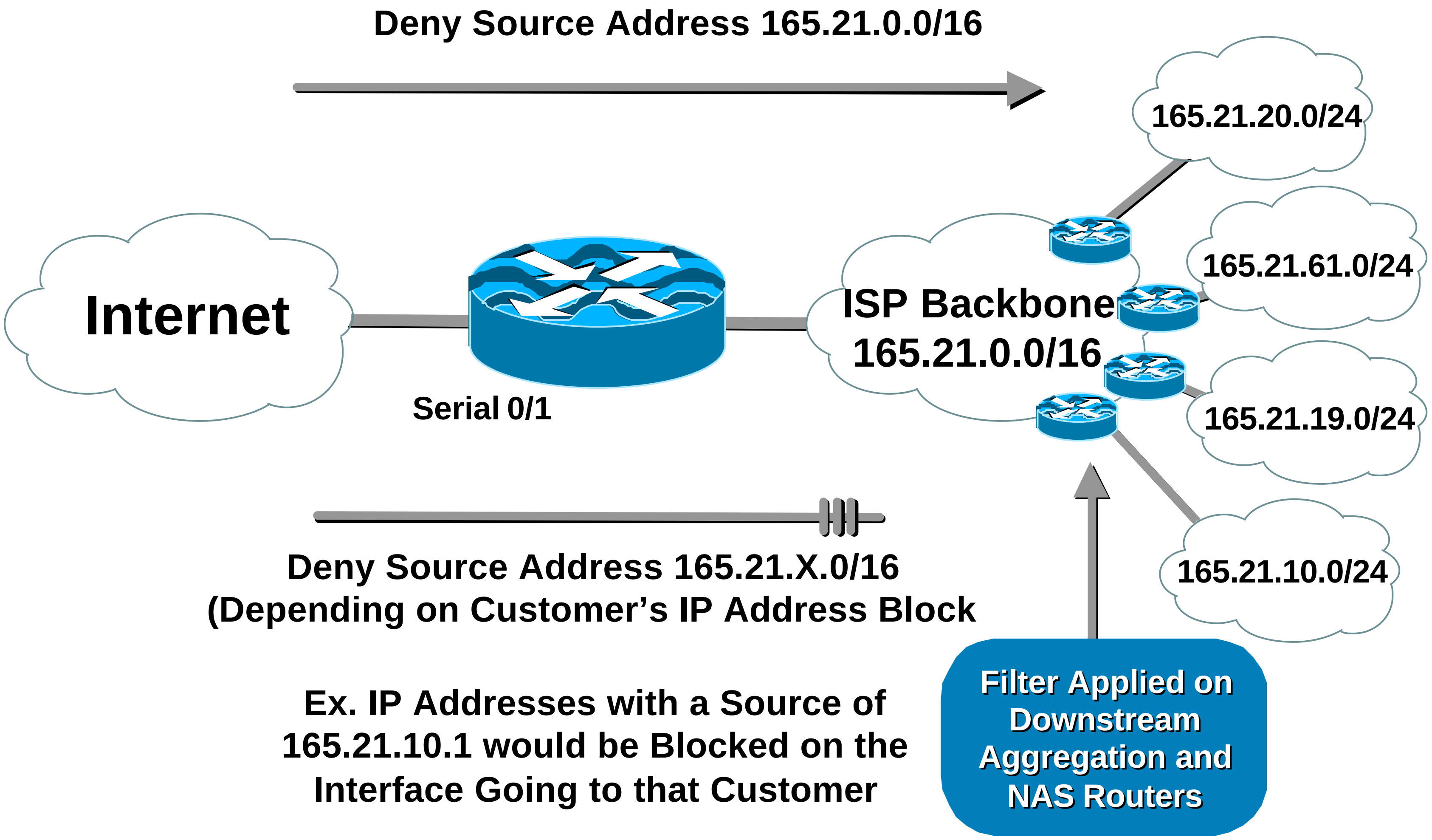
Allow Source Address 165.21.X.0/16
(Depending on the IP Address Block Allocated to the Customer)

Block Source Address from All Other Networks

Ex. IP Addresses with a Source of 10.1.1.1 Would Be Blocked

Filter Applied on Downstream Aggregation and NAS Routers

Egress Packet Filtering Customer Edge


Deny Source Address 165.21.0.0/16
Internet
Serial 0/1
ISP Backbone
165.21.0.0/16
165.21.20.0/24
165.21.61.0/24
165.21.19.0/24
165.21.10.0/24
Deny Source Address 165.21.X.0/16
(Depending on Customer's IP Address Block
Ex. IP Addresses with a Source of
165.21.10.1 would be Blocked on the
Interface Going to that Customer
Filter Applied on
Downstream
Aggregation and
NAS Routers

Guidelines

- End-site network connecting to the Internet

  MUST use inbound and outbound packet filters to protect network

- Configuration example

  Outbound – only allow my network source addresses out

  Inbound – only allow specific ports to specific destinations in

Guidelines – Example

```
interface serial 0
 description Connection to Planet ISP
 ip unnumbered Ethernet 0
 ip access-group 100 in
 ip access-group 101 out
 no ip directed-broadcast
!
access-list 100 permit icmp any any
access-list 100 permit tcp any any established
access-list 100 permit tcp any any eq 22
access-list 100 permit tcp any host 221.4.0.1 eq www
access-list 100 permit tcp any host 221.4.0.2 eq smtp
access-list 100 permit udp any host 221.4.0.3 eq domain
access-list 100 permit tcp any host 221.4.0.3 eq domain
access-list 100 permit udp any any eq ntp
access-list 100 deny   udp any any eq 2049
access-list 100 permit udp any any gt 1023
access-list 100 deny   ip any any log
!
access-list 101 permit ip 221.4.0.0 0.0.3.255 any
access-list 101 deny   ip any any log
!
```

Guidelines – Example

- **Access-list 100:**
  - **Permit icmp**
  - **Permit established tcp connections (ie block TCP-SYN)**
  - **Permit SecureShell**
  - **Allow WWW to Webserver**
  - **Allow SMTP to Mailserver**
  - **Allow DNS to Nameserver**
  - **Allow NTP for time synchronisation**
  - **Block NFS**
  - **Permit only unprivileged UDP ports**
  - **Block everything else, and log it**
- **Access-list 101:**
  - **Permit only packets from my address block out**
  - **Block everything else, and log it**

Guidelines

- ISPs

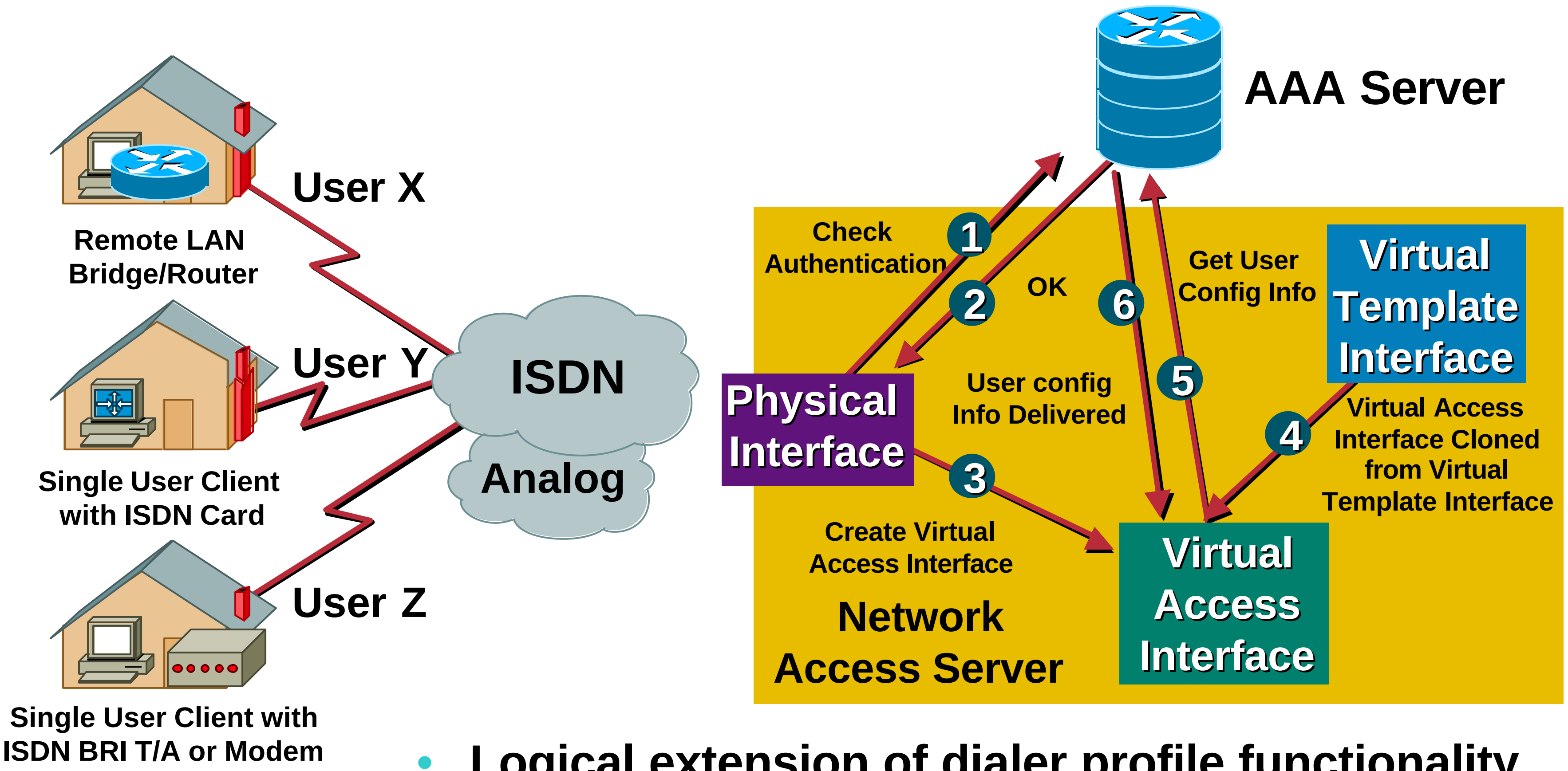
  Make sure your customers install filters on their routers – give them a template they can use

- End-sites

  Make sure you install strong filters on routers you use to connect to the Internet

  First line of defence – never assume your ISP will do it

Dynamic ACLs with AAA Virtual Profiles


AAA Server
User X
Remote LAN Bridge/Router
User Y
Single User Client with ISDN Card
User Z
Single User Client with ISDN BRI T/A or Modem
ISDN
Analog
Check Authentication
1
2
OK
6
Get User Config Info
Virtual Template Interface
Physical Interface
User config Info Delivered
5
4
Virtual Access Interface Cloned from Virtual Template Interface
3
Create Virtual Access Interface
Network Access Server
Virtual Access Interface

- Logical extension of dialer profile functionality
- ACLs stored in the Central AAA server
- Supports both Radius and Tacacs+

Dynamic ACLs with AAA Virtual Profiles

- **List of sites with information on how to configure tacacs+ and radius to download ACLs:**

  Cisco Radius

  http://www.cisco.com/warp/public/480/radius_ACL1.html#secondary

  Ascend/Radius

  http://www.hal-pc.org/~ascend/MaxTNT/radius/attrib.htm#216191

  TACACS+

  http://www.cisco.com/warp/public/480/tacacs_ACL1.html

Unicast Reverse Path Forwarding

- Checks source address of inbound packets to check that it is reachable through the inbound interface
- Efficient and very important filtering tool for edge of Internet
- Covered in detail later on!!

Rate Limiting

- Rate limiting used to limit packet floods

  Used to counter DoS attacks and aggressive probes

- Example

  To rate limit ICMP to 16kbps and TCP SYN to 8kbps:

```
interface serial 0
 description Connection to Planet ISP
 ip unnumbered Ethernet 0
 rate-limit input access-group 102 16000 8000 8000 conform-action transmit exceed-action drop
 rate-limit input access-group 103 8000 8000 8000 conform-action transmit exceed-action drop
 no ip directed-broadcast
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
access-list 103 deny   tcp any any established
access-list 103 permit tcp any any
!
```

IP Precedence

- Some Internet sites change IP precedence so their content always “gets through”

  Recommended to reset IP precedence of incoming packets to default values (unless you know of traffic which needs different precedence values)

- Example:

  Running a Voice over IP network – inbound packets with highest precedence are “more important” than VoIP traffic, and will cause havoc in the local network

IP Precedence – Example

```
interface serial 0
 description Connection to Planet ISP
 ip unnumbered Ethernet 0
 ip route-cache policy
 ip policy route-map SET-PREC
 no ip directed-broadcast
!
route-map SET-PREC permit 10
 match ip address 160
 set ip precedence routine
!
access-list 160 permit ip any any precedence priority
access-list 160 permit ip any any precedence immediate
access-list 160 permit ip any any precedence flash
access-list 160 permit ip any any precedence flash-override
access-list 160 permit ip any any precedence critical
access-list 160 permit ip any any precedence internet
access-list 160 permit ip any any precedence network
!
```

IP Precedence – Example

- Route-map matches all possible precedence values apart from “routine”
- Uses policy routing

  Make sure policy routing is fast or cef switched (process switched by default)

- “show access-list 160” will display different precedence levels of incoming packets

```
Extended IP access list 160 (Compiled)
   permit ip any any precedence priority (33137629 matches)
   permit ip any any precedence immediate (3916144 matches)
   permit ip any any precedence flash (1967437 matches)
   permit ip any any precedence flash-override (4034766 matches)
   permit ip any any precedence critical (2306059 matches)
   permit ip any any precedence internet (8024235 matches)
   permit ip any any precedence network (919538 matches)
```

Summary

- Network security is about

  Filtering prefixes exchanged between networks

  Filtering packets sent between networks

  Using the tools and recommendations – networks should comply with BCP 38

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network

Administrative and Operational Practices

Administrative and Operational Practices

- Configuration hints to aid security
  - Router features
  - Network features
  - Operational practices

Loopback Interface

- Most ISPs make use of the router loopback interface
- IP address configured is a host address
- Configuration example:

```
interface loopback 0
 description Loopback Interface of CORE-GW3
 ip address 215.18.3.34 255.255.255.255
 no ip redirects
```

Loopback Interface

- Loopback interfaces on ISP backbone usually numbered:

  Out of one contiguous block, or

  Using a geographical scheme, or

  Using a per PoP scheme

- Aim is to increase network stability, aid administration, and improve security

Configuration Management

- **Backup NVRAM configuration off the router:**
  - Write configuration to TFTP server
  - TFTP server files kept under revision control
  - Router configuration built from master database
- **Allows rapid recovery in case of emergency**

Configuration Management

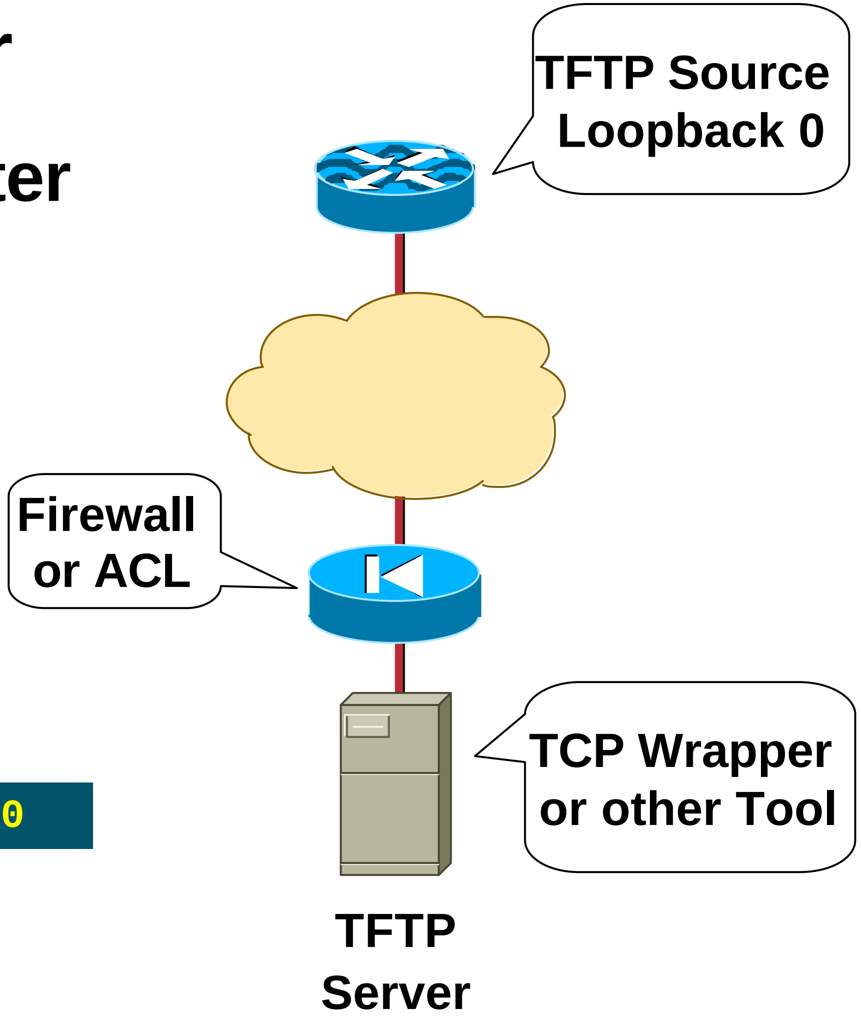
- Secure the TFTP server

  TFTP loopback 0 on router

  Firewall/ACL

  Wrapper on TFTP server which only allows the router’s loopback address

```
ip tftp source-interface Loopback0
```



FTP Client Support

- TFTP has its limitations
- FTP client support is added in IOS 12.0; this allows for FTP upload/downloads
- Remember to use the same security/redundancy options with loopback 0:

```
ip ftp source-interface loopback 0
```

FTP Client Support

```
7206-AboveNet-SJ2#copy ftp://bgreene:XXX@ftp.cisco.com slot0:

Source filename []? /cisco/ios/12.0/12.0.9S/7200/c7200-k3p-
mz.120-9.S.bin

Destination filename [c7200-k3p-mz.120-9.S.bin]?

Accessing ftp://bgreene:XXX@ftp.cisco.com
//cisco/ios/12.0/12.0.9S/7200/c7200-k3p-mz.120-
9.S.bin...Translating "ftp.cisco.com"...domain server
(207.126.96.162) [OK]


Loading /cisco/ios/12.0/12.0.9S/7200/c7200-k3p-mz.120-9.S.bin
```

Use Detailed Logging

- Off load logging information to a logging server
- Use the full detailed logging features to keep exact details of the activities

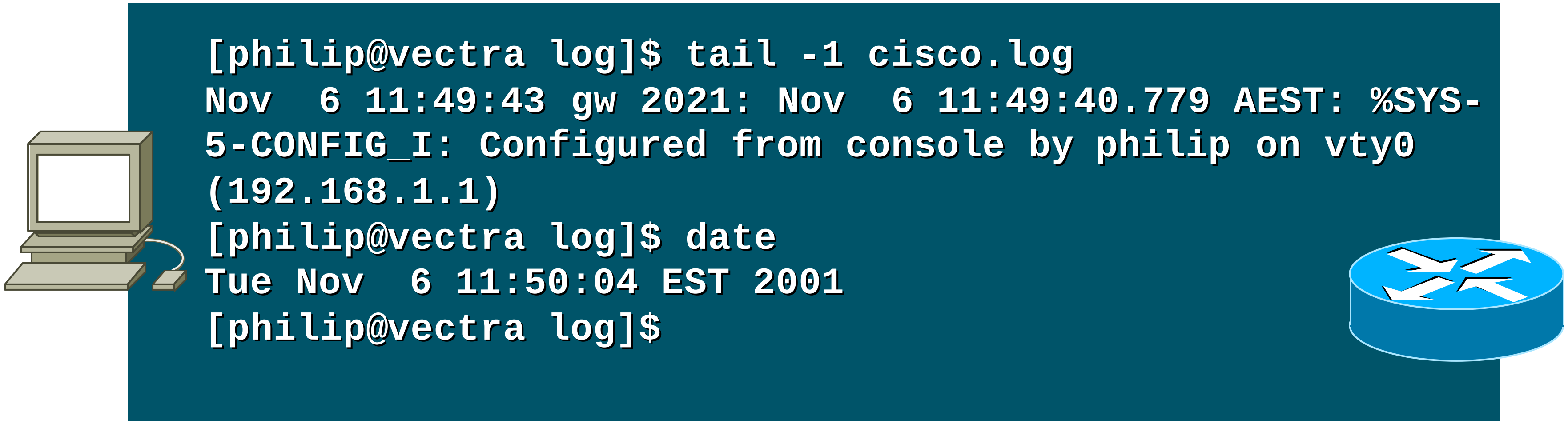
```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging buffered 16384
logging trap debugging
logging facility local7
logging 169.223.32.1
logging 169.223.55.37
logging source-interface loopback0
no logging console  ! Recommended - keeps the console port free
```

Use Detailed Logging

- Two topologies used:

  Central Syslog servers in operations center

  Syslog servers in major POPs



```
[philip@vectra log]$ tail -1 cisco.log
Nov  6 11:49:43 gw 2021: Nov  6 11:49:40.779 AEST: %SYS-
5-CONFIG_I: Configured from console by philip on vty0
(192.168.1.1)
[philip@vectra log]$ date
Tue Nov  6 11:50:04 EST 2001
[philip@vectra log]$
```

Network Time Protocol

- If you want to cross compare logs, you need to synchronize the time on all the devices
- Use NTP
  - From external time source
    - Upstream ISP, Internet, GPS, atomic clock
  - From internal time source
  - Router can act as *stratum 1* time source

Network Time Protocol

- **Set timezone**

```
clock timezone <name> [+/-hours [mins]]
```

- **Router as source**

```
ntp master 1
```

- **External time source (master)**

```
ntp server a.b.c.d
```

- **External time source (equivalent)**

```
ntp peer e.f.g.h
```

Network Time Protocol

- **Example configuration:**

```
clock timezone AEST 10
ntp update-calendar
ntp source loopback0
ntp server <other time source>
ntp peer <other time source>
ntp peer <other time source>
```

Network Time Protocol

- Network Time Protocol (NTP) used to synchronize the time on all the devices
- NTP packets leave router with loopback address as source
- Configuration example:

```
ntp source loopback0
ntp server 169.223.1.1 source loopback 1
```

Network Time Protocol

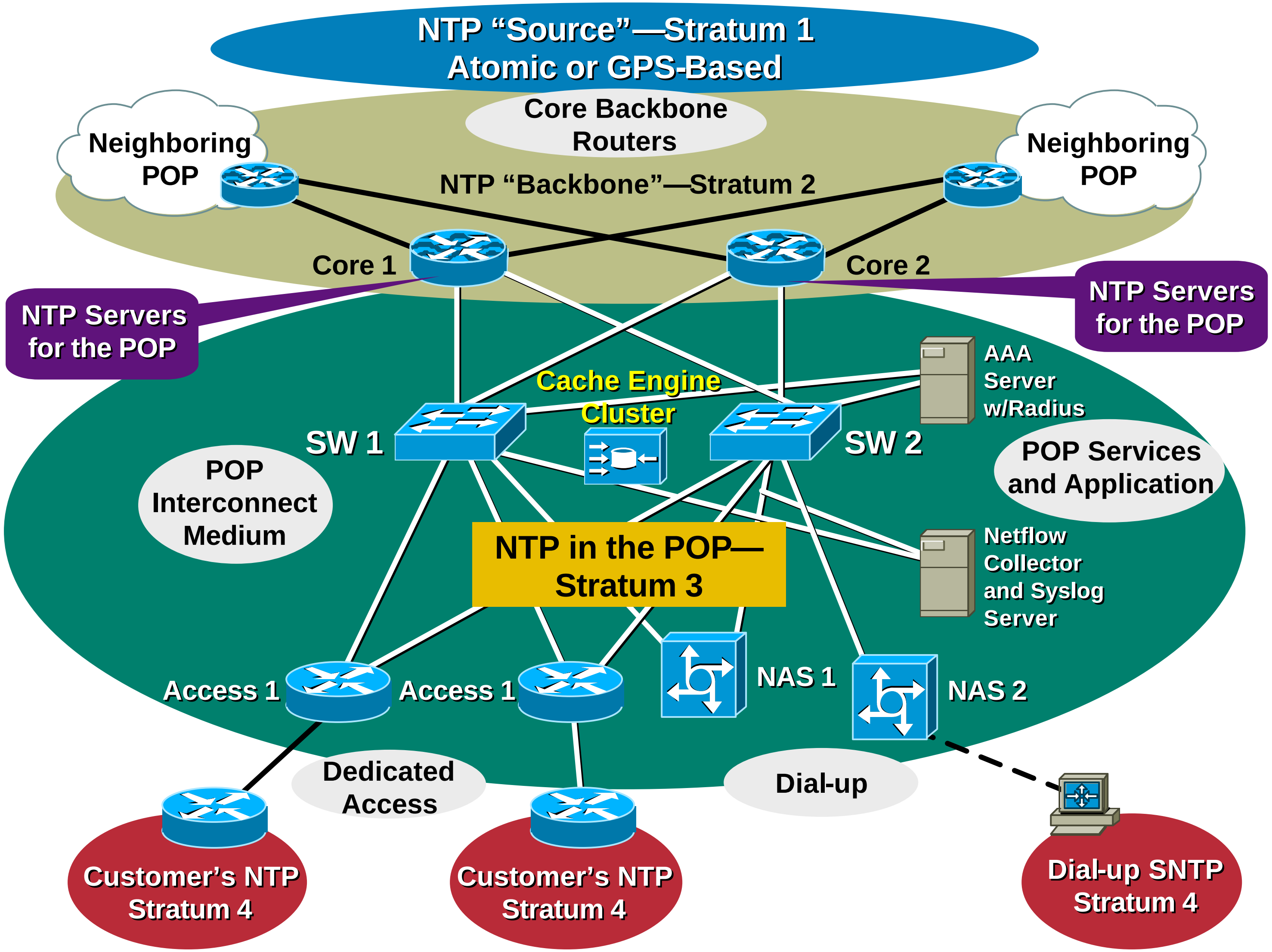
- Motivation—NTP security:

  NTP systems can be protected by filters which only allow the NTP port to be accessed from the loopback address block

- Motivation—easy to understand NTP peerings:

  NTP associations have the loopback address recorded as source address, not the egress interface

Network Time Protocol



Network Time Protocol

- **Where to get NTP reference sources?**

  http://www.eecis.udel.edu/~ntp/hardware.html

- **Attach a Telecom Solutions GPS clock to the router's AUX port:**

```
Excalabur(config)#line aux 0
Excalabur(config-line)#ntp refclock telecom-solutions pps ?
  cts   PPS on CTS
  none  No PPS signal available
  ri    PPS on RI
```

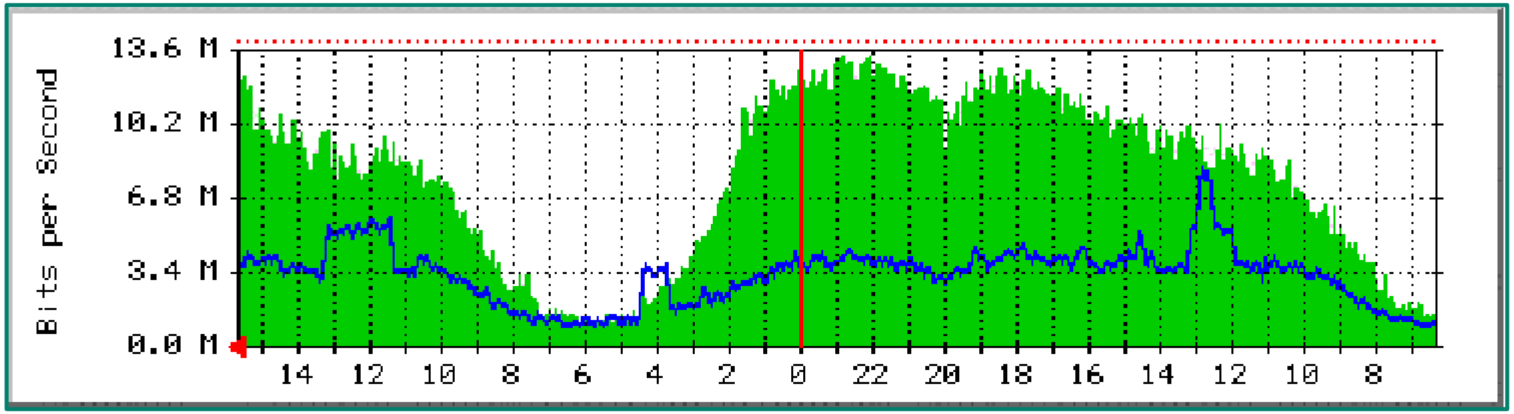
SNMPv1

- **Remove any SNMP commands if SNMP is not going to be used**
- **If SNMP is going to be used:**

```
access-list 98 permit 169.223.1.1
access-list 98 deny   any
snmp-server community 5nmc02m RO 98
snmp-server trap-source Loopback0
snmp-server trap-authentication
snmp-server host 169.223.1.1 5nmc02m
```

SNMPv1

- Recommend that all ISPs aggressively and consistently monitor their network
- Despite SNMPv2 and SNMPv3, most ISPs are still using SNMPv1 (personal observation)
- SNMPv3 supported since 12.0(6)S



HTTP Server

- HTTP server in Cisco IOS from 11.1CC and 12.0S

  Router configuration via web interface

- Disable if not going to be used (disabled by default):

```
no ip http server
```

- Configure securely if going to be used:

```
ip http server
ip http port 8765
ip http authentication aaa
ip http access-class <1-99>
```

Core Dumps

- Cisco routers have a core dump feature that will allow ISPs to transfer a copy of the core dump to a specific FTP server
- Set up a FTP account on the server the router will send the core dump to
- The server should NOT be a public server
    - Use filters and secure accounts
    - Locate in NOC with NOC staff access only
    - Enough disk space to handle the dumps

Core Dumps

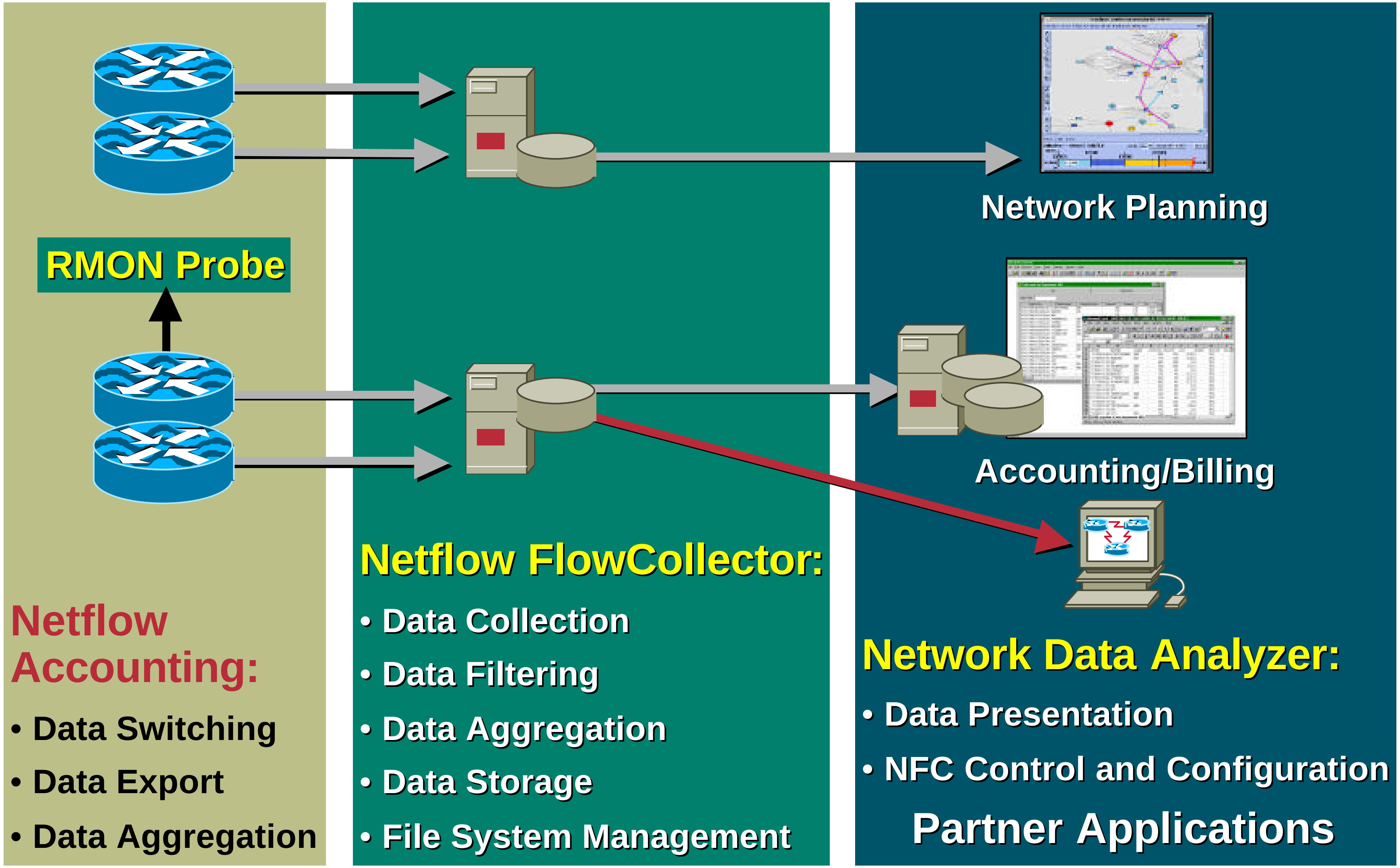
- **Example configuration:**

```
ip ftp username cisco

ip ftp password 7 045802150C2E

ip ftp source-interface loopback 0

exception protocol ftp

exception dump 169.223.32.1
```

Netflow

- Providers network administrators with “packet flow” information
- Allows:
  - Security monitoring
  - Network management and planning
  - Customer billing
  - Traffic flow analysis
- Available from 11.1CC for 7x00 and 12.0 for remaining router platforms

Netflow Infrastructure



Netflow Accounting:

- Data Switching
- Data Export
- Data Aggregation

Netflow FlowCollector:

- Data Collection
- Data Filtering
- Data Aggregation
- Data Storage
- File System Management

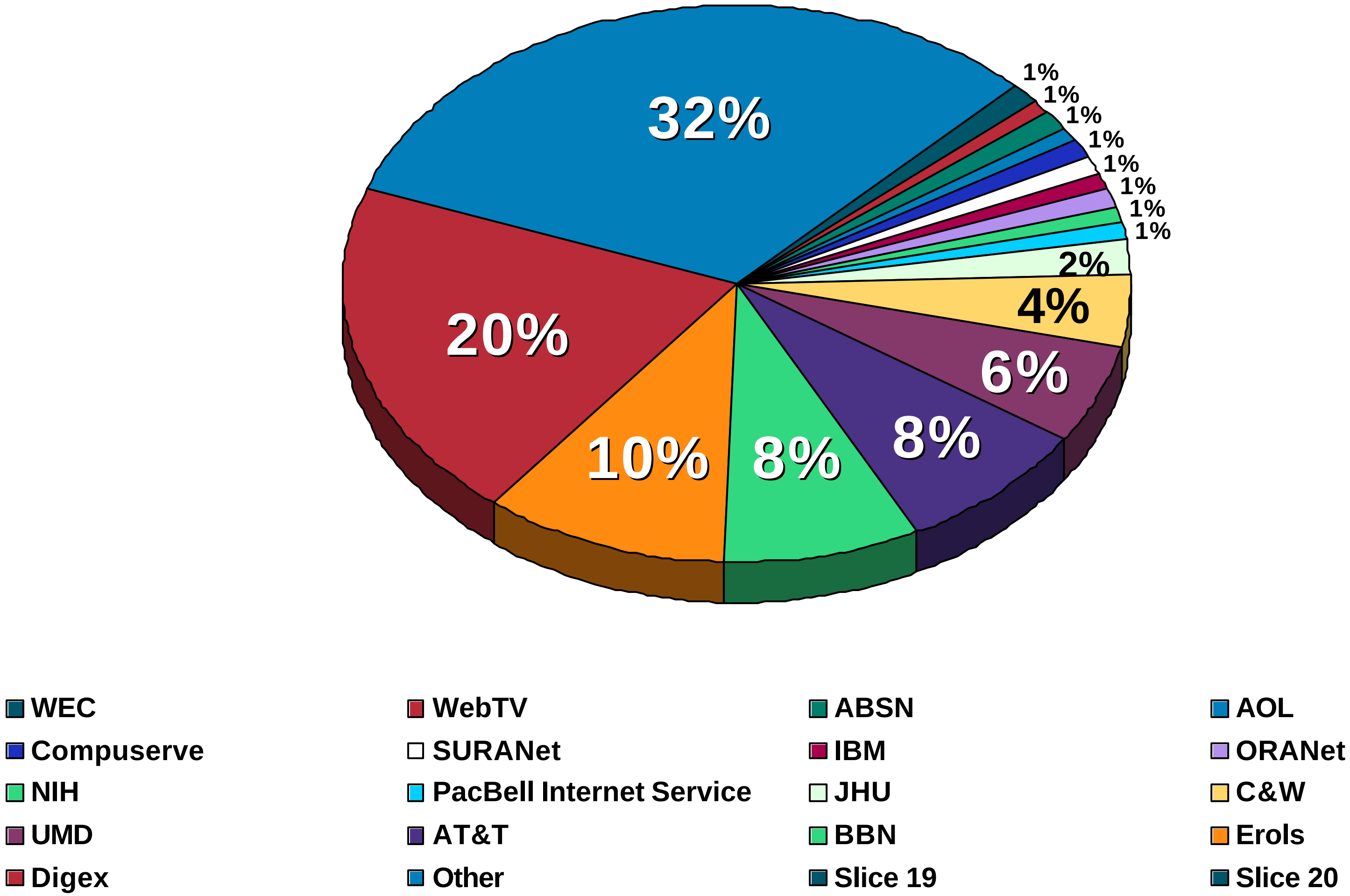
Network Data Analyzer:

- Data Presentation
- NFC Control and Configuration

Partner Applications

Netflow—Capacity Planning

Public Routers 1, 2, 3 Month of September Outbound Traffic



Netflow

- **Configuration example:**

```
interface serial 5/0
 ip route-cache flow
```

- **If CEF not configured, Netflow enhances existing switching path (i.e. optimum switching)**
- **If CEF configured, Netflow becomes a flow information gatherer and feature acceleration tool**

Netflow

- **Information export:**

  Router to collector system

  ```
  ip flow-export version 5 [origin-as|peer-as]
  ip flow-export destination x.x.x.x <udp-port>
  ```

- **Flow aggregation (new in 12.0S):**

  Router sends aggregate records to collector system

  ```
  ip flow-aggregation cache as|prefix|dest|source|proto
    enabled
    export destination x.x.x.x <udp-port>
  ```

Netflow—Simple Monitoring

- **Sample output on router:**

```
Beta-7200-2>sh ip cache flow
IP packet size distribution (14280M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .145 .403 .101 .178 .105 .017 .005 .003 .001 .000 .000 .000 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .000 .025 .001 .004 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  14369 active, 51167 inactive, 253731473 added
  1582853980 ager polls, 0 flow alloc failures
  last clearing of statistics 16w5d
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet       28284      0.0        36    71      0.2      13.4      17.7
TCP-FTP         171390      0.0        15    63      0.6       8.1      16.6
TCP-FTPD        104030      0.0       693   384     16.8      29.7       9.7
TCP-WWW       28119533      6.5        17   290    115.8       6.5      10.9
TCP-SMTP       3615725      0.8        18   266     15.7       5.6      15.5
TCP-X             1649      0.0         3    84      0.0       4.1      14.0
TCP-BGP        1483900      0.3         5   258      1.7      13.1      19.1
TCP-NNTP          2330      0.0         2    53      0.0       8.4      20.7
TCP-Frag           484      0.0         1    46      0.0       1.2      20.9
TCP-other    343437823     79.9         5   129    410.9       2.5      11.0
```

Netflow—Simple Monitoring

- Sample output on router (continued):

```
Protocol         Total     Flows    Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec      /Flow  /Pkt     /Sec     /Flow     /Flow

UDP-DNS     2513140694     585.1          3    90   1778.6       5.3      21.5
UDP-NTP        2675203       0.6          1    76      0.6       0.0      21.6
UDP-TFTP         25750       0.0          6   157      0.0      20.1      20.8
UDP-Frag           737       0.0          5   210      0.0      14.4      21.4
UDP-other   1532677302     356.8          2   154    950.7       4.3      21.6
ICMP          30784392       7.1          4   109     30.7       7.3      20.5
IGMP                31       0.0       1903  1085      0.0      89.7      21.7
IP-other        985081       0.2          8   354      1.9      13.9      20.2
Total:      4457254338    1037.7          3   123   3324.8       4.8      20.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se2/0         203.161.234.211 Fa1/0         203.37.255.97   11 0404 0035     1
Fa1/0         203.37.255.97   Se2/0         203.161.234.211 11 0035 0404     1
Fa1/0         203.37.255.97   Se2/0         203.93.111.1    11 0035 8124     1
Fa1/0         203.37.255.114  Se2/0         195.67.208.248  11 1B3A 3F04  4675
Se2/0         195.67.208.248  Fa1/0         203.37.255.114  11 3F04 1B3A  6672
Se2/0         203.93.111.1    Fa1/0         203.37.255.97   11 8124 0035     1
Fa1/0         203.37.255.97   Se2/0         203.132.224.11  11 0035 0EDC     1
Se2/0         216.154.240.8   Fa1/0         203.37.255.97   11 0424 0035    12K
Fa1/0         203.37.255.97   Se2/0         216.154.240.8   11 0035 0424    12K
Se2/0         203.132.224.11  Fa1/0         203.37.255.97   11 0EDC 0035     1
...etc...
```

Netflow

- As a security tool

  Very easy to spot port scans, address range scans, etc

  Many documented cases of ISPs using NetFlow to catch “crackers”

  First tool to use in instance of suspected or real DOS attack

Out of Band Management

- Not optional!
- Allows access to network equipment in times of failure or when under attack
- Ensures quality of service to customers

    Minimises downtime

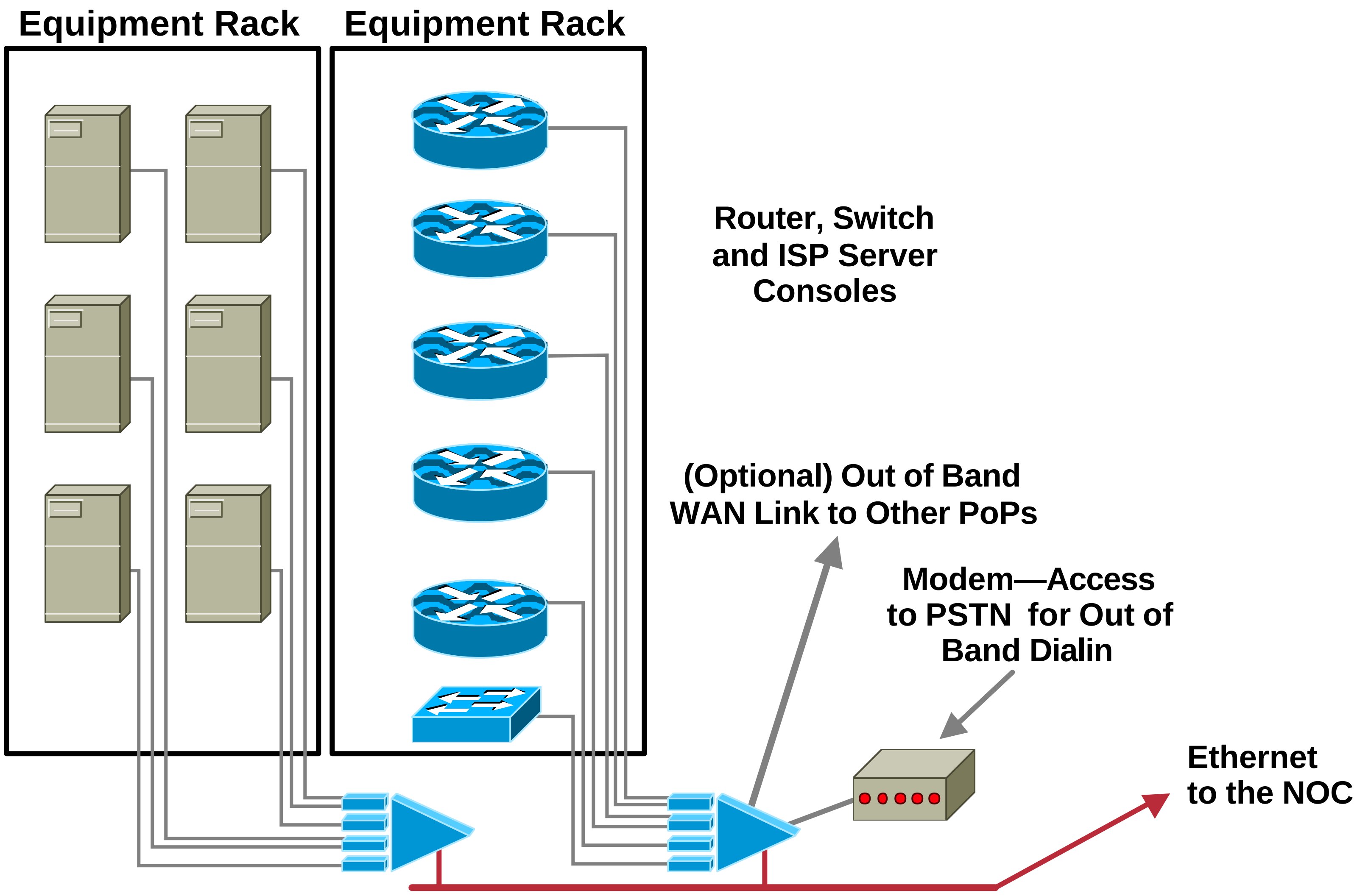
    Minimises repair time

    Eases diagnostics and debugging

Out of Band Management

- **OoB example—Access server:**
  - **Modem attached to allow NOC dial in**
  - **Console ports of all network equipment connected to serial ports**
  - **LAN and/or WAN link connects to network core, or via separate management link to NOC**
- **Full remote control access under all circumstances**

Out of Band Network



Equipment Rack

Equipment Rack

Router, Switch and ISP Server Consoles

(Optional) Out of Band WAN Link to Other PoPs

Modem—Access to PSTN for Out of Band Dialin

Ethernet to the NOC

Out of Band Management

- **OoB example—Statistics gathering:**

  Routers are NetFlow and syslog enabled

  Management data is congestion/failure sensitive

  **Ensures management data integrity
  in case of failure or unexpected network load**

- **Full remote information under all circumstances**

Out of Band Access

- **Router console port gives complete control over router**

  Ensure router is in locked cabinet

  -and/or-

  Ensure comms room is locked and only accessible by authorised personnel

  -and/or-

  Ensure premises are secure, only accessible by authorised personnel, and has a working environmental control system

  faulty airconditioning ® open doors/windows ® no security ® network devices become vulnerable

Test Laboratory

- Designed to look like a typical PoP
  - Operated like a typical PoP
- Used to trial new services or new software under realistic conditions
  - Allows discovery and fixing of potential problems before they are introduced to the network
- Used to simulate solutions or workarounds to security incidents affecting the backbone
  - Before they are deployed!

Test Laboratory

- Some ISPs dedicate equipment to the lab
- Other ISPs “purchase ahead” so that today’s lab equipment becomes tomorrow’s PoP equipment
- Other ISPs use lab equipment for “hot spares” in the event of hardware failure

Test Laboratory

- Can’t afford a test lab?

  Set aside one spare router and server to trial new services

  Never ever try out new hardware, software or services on the live network

- Every major ISP in the US and Europe has a test lab

  It’s a serious consideration

ISP NOC

- **Every ISP needs a NOC**
- **Anyone who has worked or run a NOC has their own list of what should be in a NOC**

  Make your own wish list

  Talk to colleagues and get their list

  Then try to make it happen

- **No NOC is a perfect NOC—the result is always a ratio of time, money, skills, facilities, and manpower**

NOC Communications

- NOCs need to communicate with
  - Teams inside their network
  - Customers
  - Other ISPs
- E-mail and Web pages are the most common forms of communication
- Pagers and hand phones are secondary communication tools

NOC Communications

- **Q. Does *noc@someisp.net* work?**
- **Q. Do you have a Operations Web site with:**

  Contact information

  Network policies (i.e. RFC 1998)

  Security policies and contact information

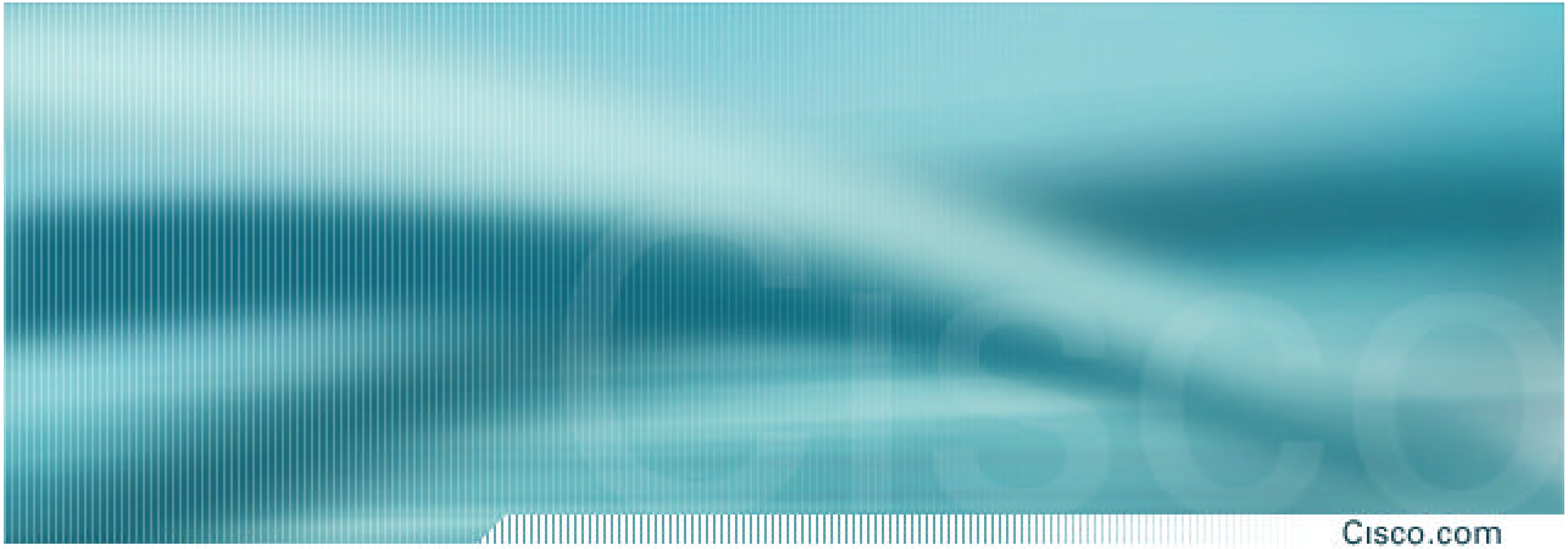
- **Q. Have you registered you NOC information at one of the NOC Coordination Pages?**

Summary

- NetFlow is primary security information tool for any network
- Use other router facilities to aid network security
- Router can be secure, but is the surrounding environment also secure?
- Don’t forget the human aspects – out of band management, knowledge of NOCs and having good test facilities all contribute to helping with network security

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network



The Unicast Reverse Path Forward Check

Reverse Path Forwarding

- Supported from 11.1(17)CC images

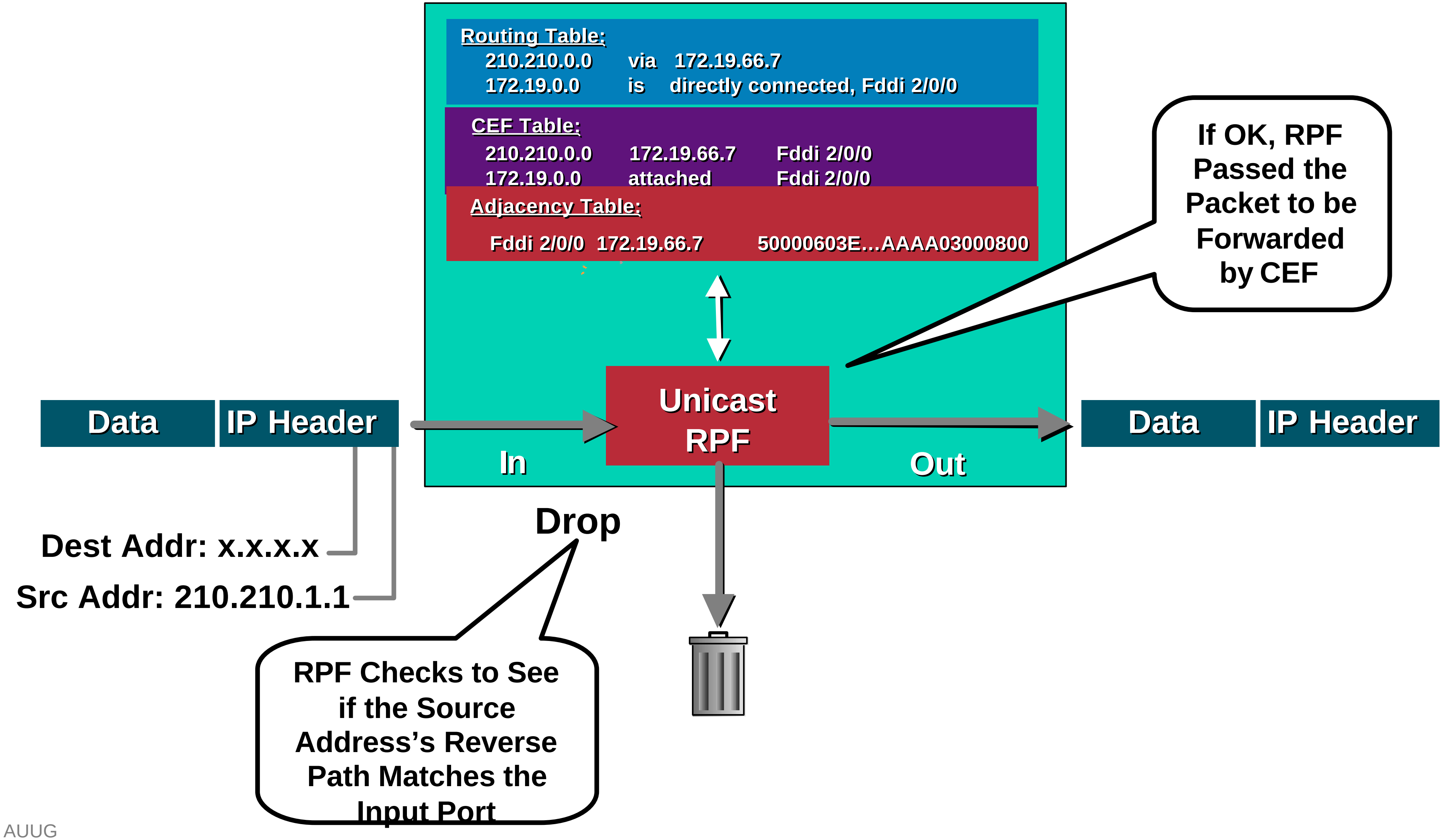
  Feature introduced in March 1998

- CEF switching must be enabled
- Source address of incoming IP packets are checked to ensure that the route back to the source uses the inbound interface
- Care required in multihoming situations
- Two Flavours of uRPF:

  Strict Mode for BCP 38/ RFC 2827 Filters on Customer Ingress Edge

  Loose Mode for ISP ⇔ ISP Edge

CEF Unicast RPF (Strict Mode)



Routing Table:

```
210.210.0.0    via   172.19.66.7
172.19.0.0     is    directly connected, Fddi 2/0/0
```

CEF Table:

```
210.210.0.0    172.19.66.7    Fddi 2/0/0
172.19.0.0     attached       Fddi 2/0/0
```

Adjacency Table:

```
Fddi 2/0/0  172.19.66.7      50000603E…AAAA03000800
```

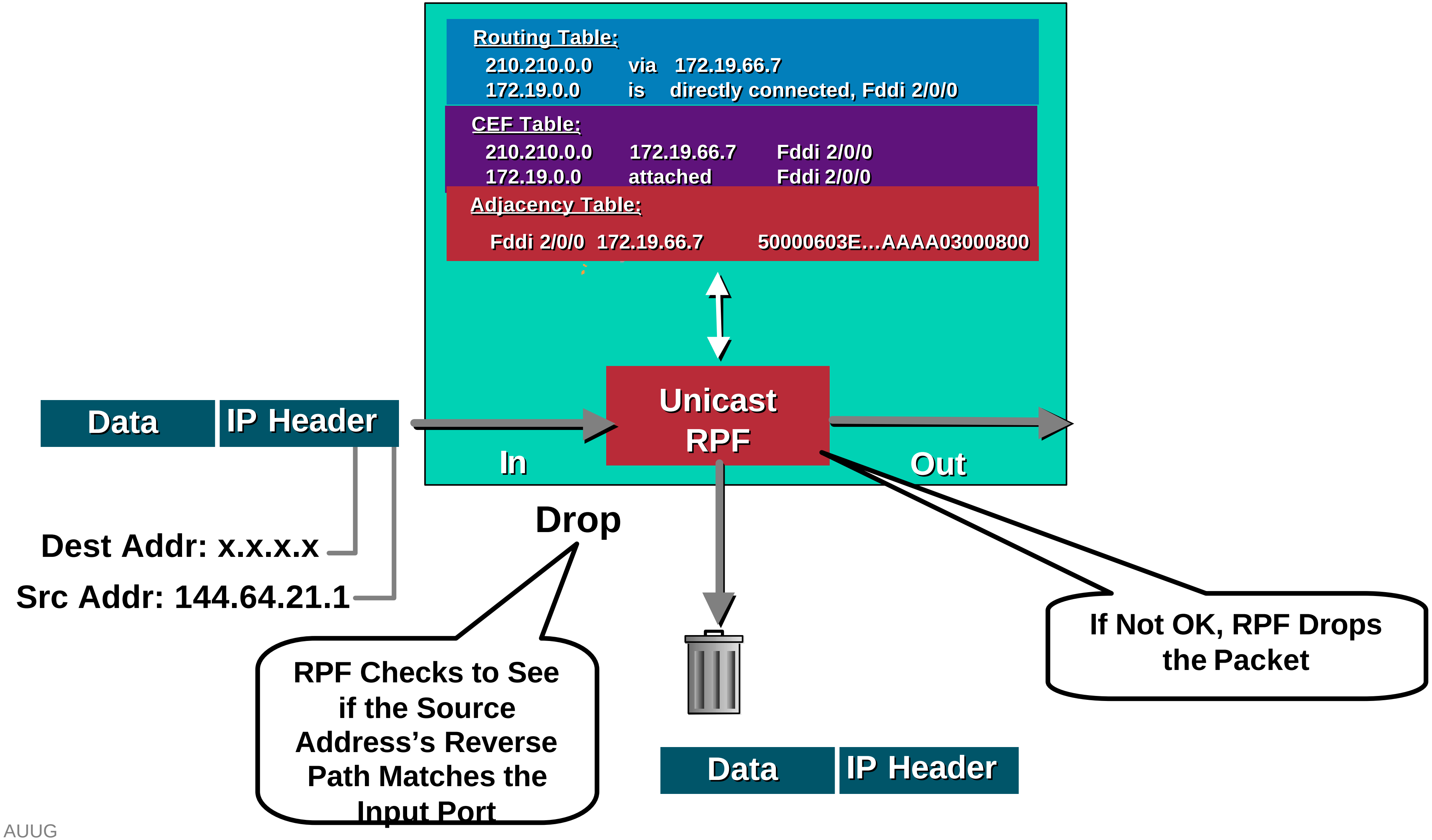
If OK, RPF Passed the Packet to be Forwarded by CEF

RPF Checks to See if the Source Address's Reverse Path Matches the Input Port

Dest Addr: x.x.x.x

Src Addr: 210.210.1.1

CEF Unicast RPF (Strict Mode)



Routing Table:

```
210.210.0.0     via   172.19.66.7
172.19.0.0      is    directly connected, Fddi 2/0/0
```

CEF Table:

```
210.210.0.0     172.19.66.7      Fddi 2/0/0
172.19.0.0      attached         Fddi 2/0/0
```

Adjacency Table:

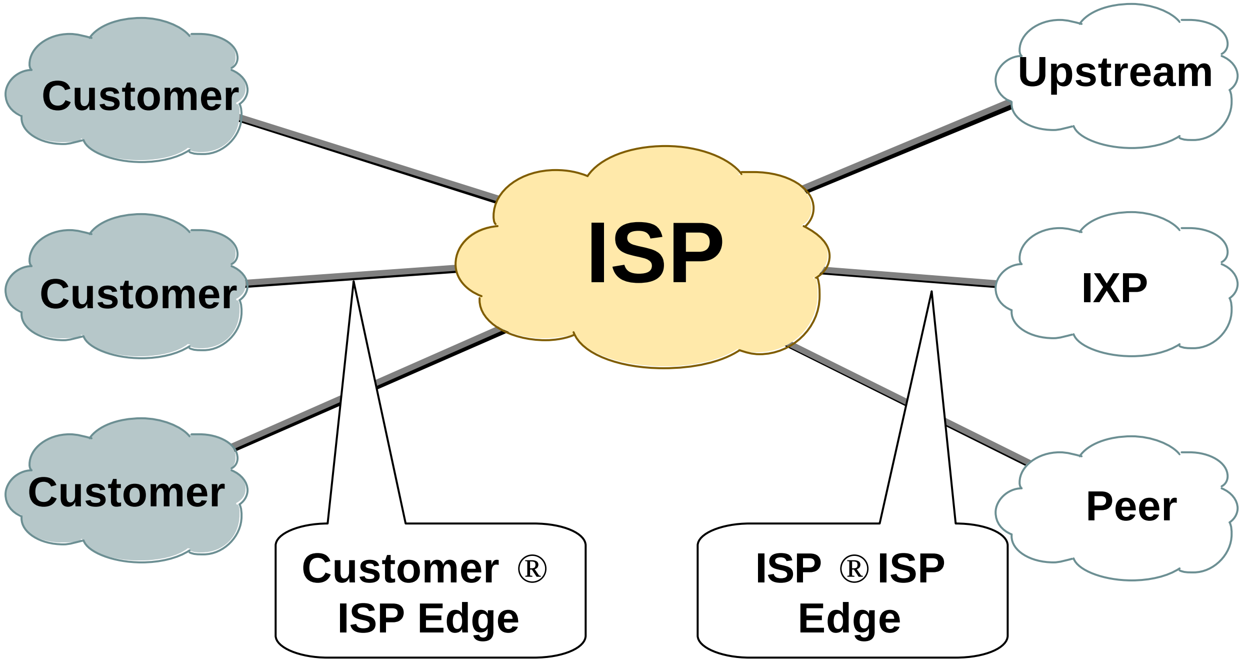
```
Fddi 2/0/0  172.19.66.7       50000603E…AAAA03000800
```

RPF Checks to See if the Source Address’s Reverse Path Matches the Input Port

If Not OK, RPF Drops the Packet

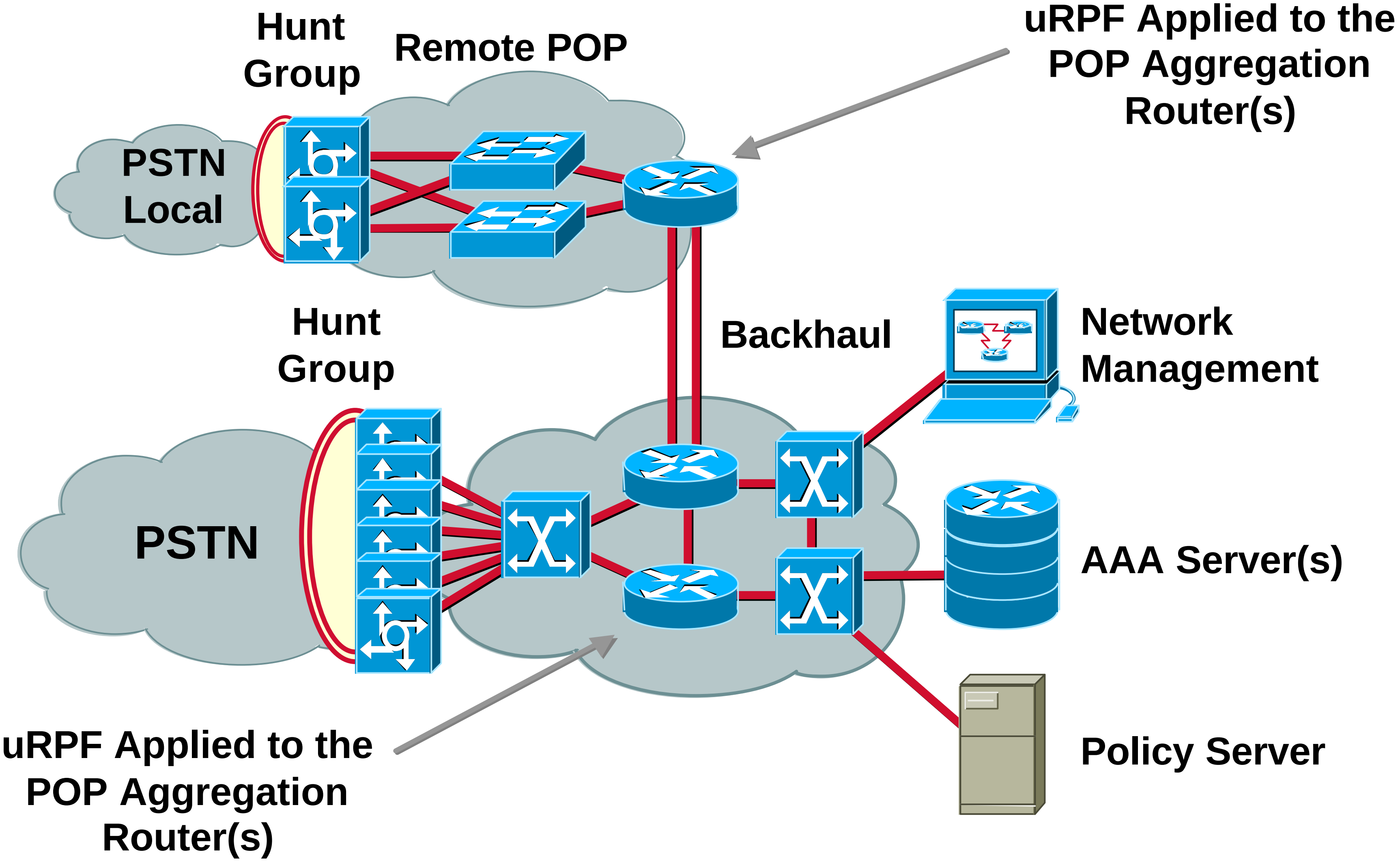
uRPF Originally Designed for the Customer®ISP Edge

- Unicast RPF was originally designed for deployment on the customer®ISP edge
- New enhancements allow it to work on the ISP®ISP edge



Where to Apply Unicast RPF (Strict Mode)?

Cisco.com



Unicast RPF Commands (Strict Mode)

- Configure RPF on the interface using the following interface command syntax:

```
[no] ip verify unicast reverse-path [<ACL>]
```

- For example on a leased line aggregation router:

```
ip cef ! or "ip cef distributed" for an RSP+VIP based
box
!
interface serial 5/0/0
  ip verify unicast reverse-path
```

- *Interface group-async* command for dial-up ports:

```
ip cef
!
interface Group-Async1
  ip verify unicast reverse-path
```

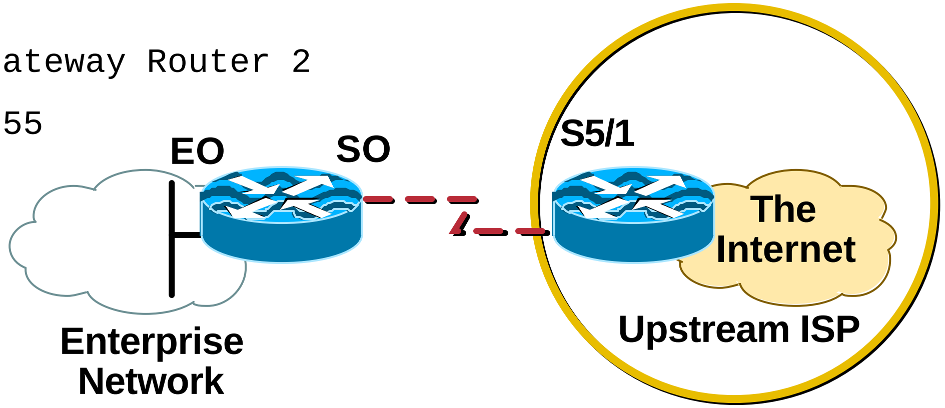
Unicast RPF Drop Logic (Strict Mode)

- **Exceptions to RPF**

```
lookup source address in forwarding database
 if the source address is reachable via the source interface
       pass the packet
    else
 if the source is 0.0.0.0 and destination is a 255.255.255.255
       /* BOOTP and DHCP */
          pass the packet
       else if destination is multicast
          pass the packet
       else
          drop the packet
```

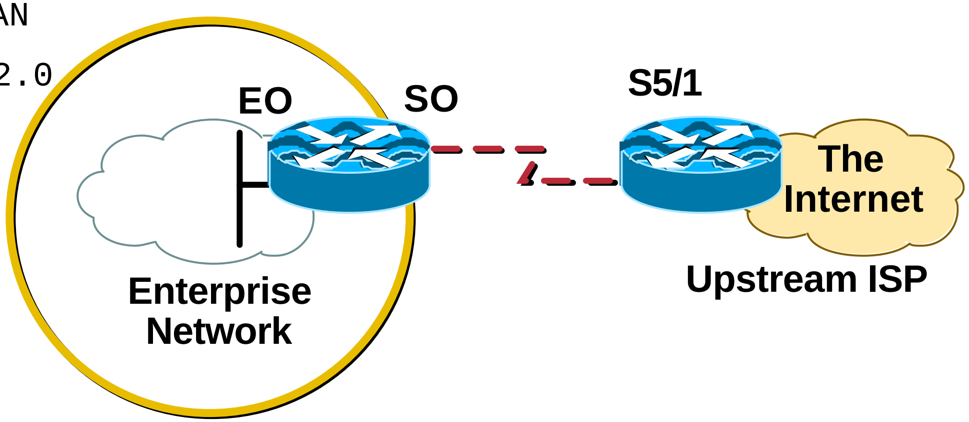
Unicast RPF—Simple Single Homed Customer Example

```
interface loopback 0
  description Loopback interface on Gateway Router 2
  ip address 215.17.3.1 255.255.255.255
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
!
interface Serial 5/0
  description 128K HDLC link to Galaxy Publications Ltd [galpub1]  R5-0
  bandwidth 128
  ip unnumbered loopback 0
  ip verify unicast reverse-path  ! Unicast RPF activated here
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
!
ip route 215.34.10.0 255.255.252.0 Serial 5/0
```



Unicast RPF—Simple Single Homed Customer Example

Cisco.com



```
interface Ethernet 0
  description Galaxy Publications LAN
  ip address 215.34.10.1 255.255.252.0
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
!
interface Serial 0
  description 128K HDLC link to Galaxy Internet Inc WT50314E  C0
  bandwidth 128
  ip unnumbered ethernet 0
  ip verify unicast reverse-path  ! Unicast RPF activated here
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
!
ip route 0.0.0.0 0.0.0.0 Serial 0
```

CEF Unicast RPF (Strict Mode)

- Unicast RPF provides

  Automatic Ingress filtering based on routing information

  Can be part of the default configuration

  Packet drops at CEF—Before the router processes spoofed packets

- If this feature is so great, why is it not used?

Why Is Unicast RPF Not Widely Deployed?

- The myth

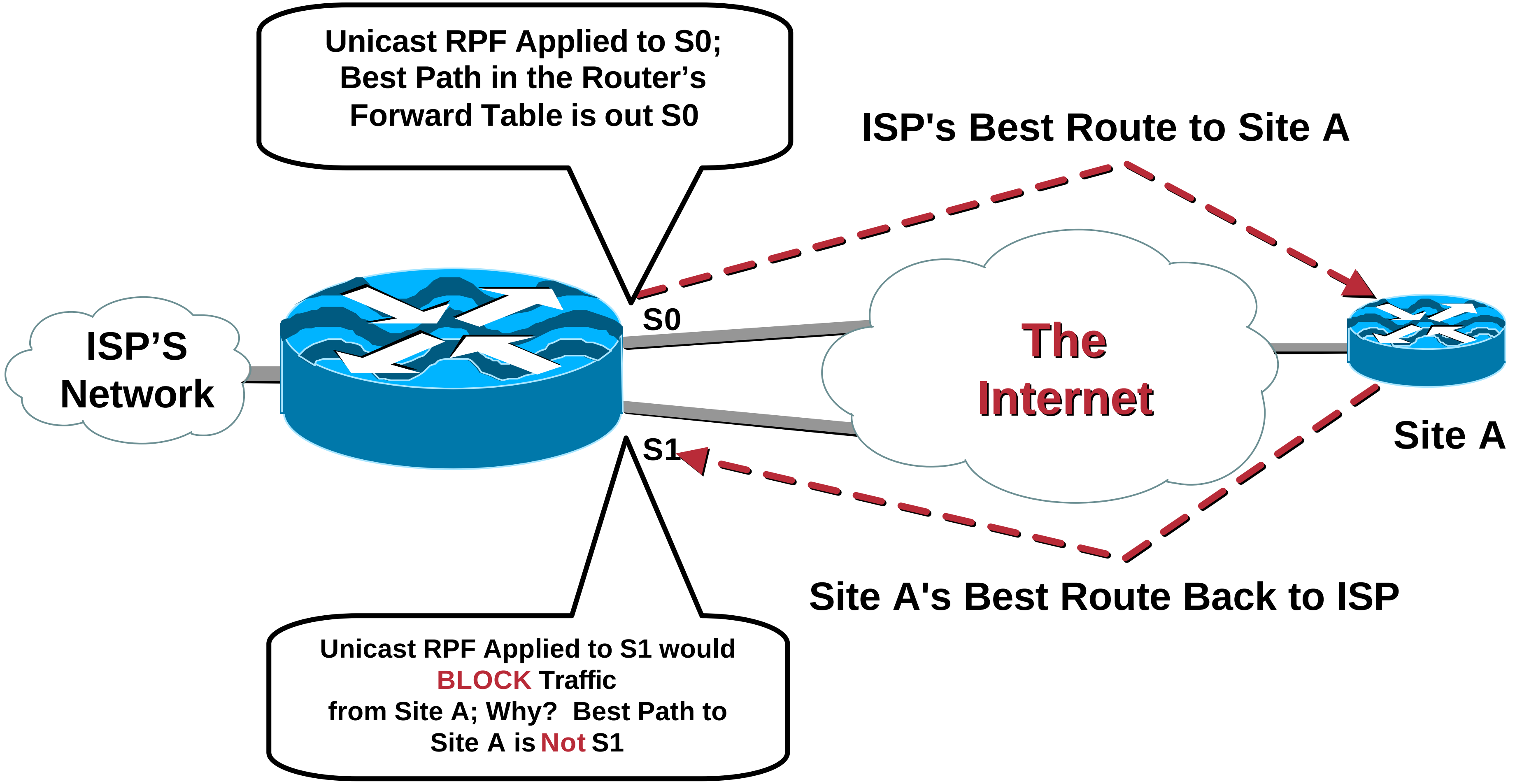
  What people say:

  Unicast RPF will not work with asymmetrical routing; since the Internet has a lot of asymmetrical routing, it will not work

  The real reason:

  ISP network engineers have not given the feature enough thought!

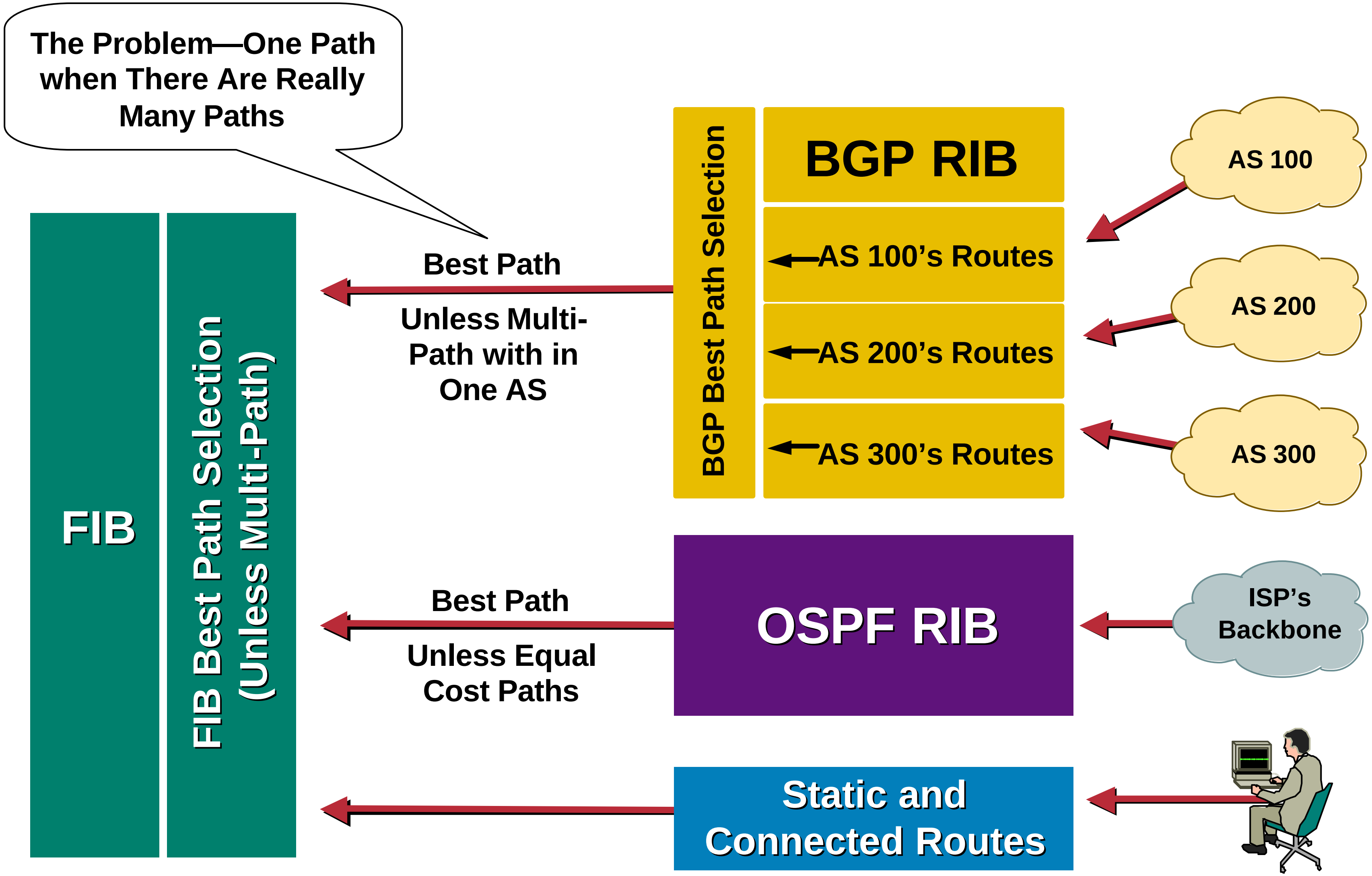
Why Is Unicast RPF Not Widely Deployed?



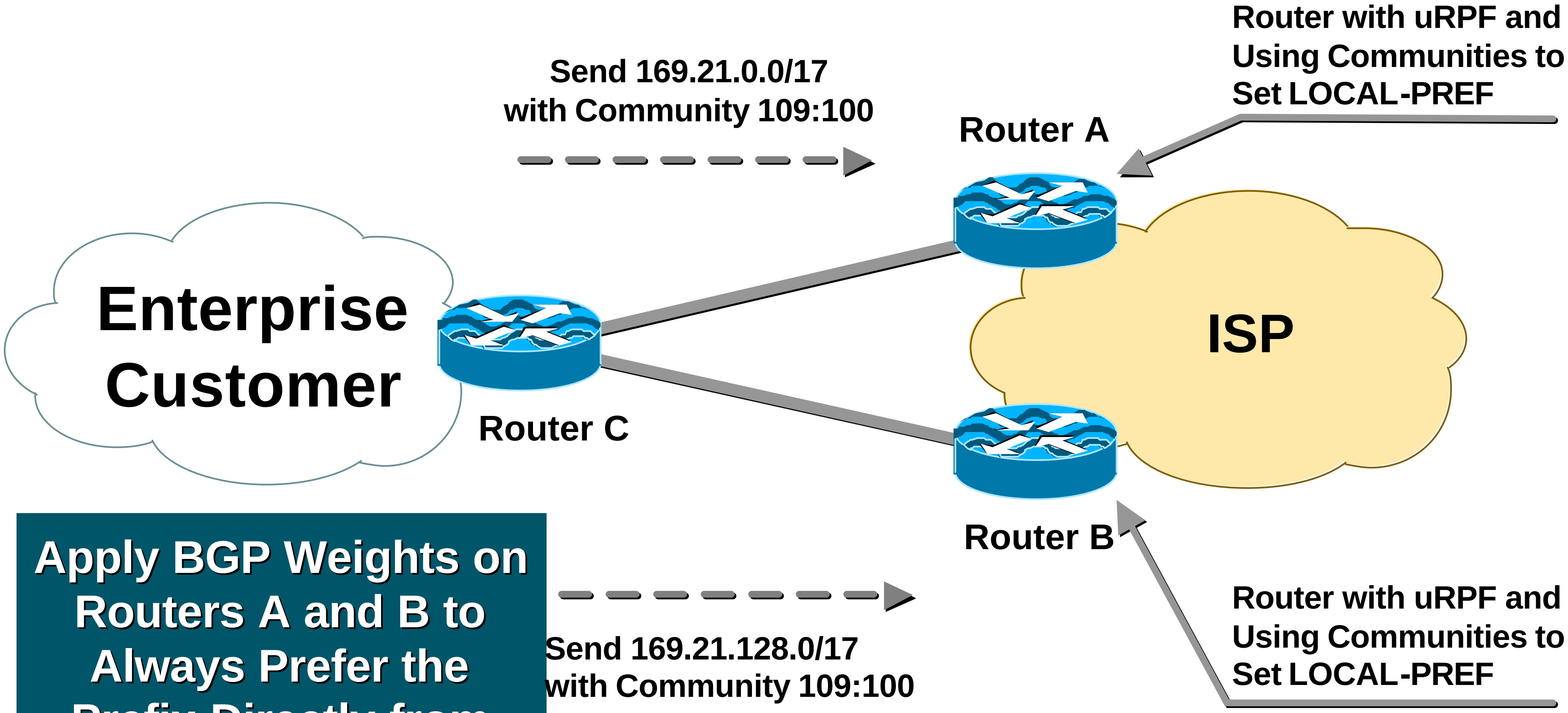
Unicast RPF Applied to S0; Best Path in the Router's Forward Table is out S0

Unicast RPF Applied to S1 would BLOCK Traffic from Site A; Why? Best Path to Site A is Not S1

Why Is Unicast RPF Not Widely Deployed?



Unicast RPF—Dual Homed Customer



Apply BGP Weights on Routers A and B to Always Prefer the Prefix Directly from Router C

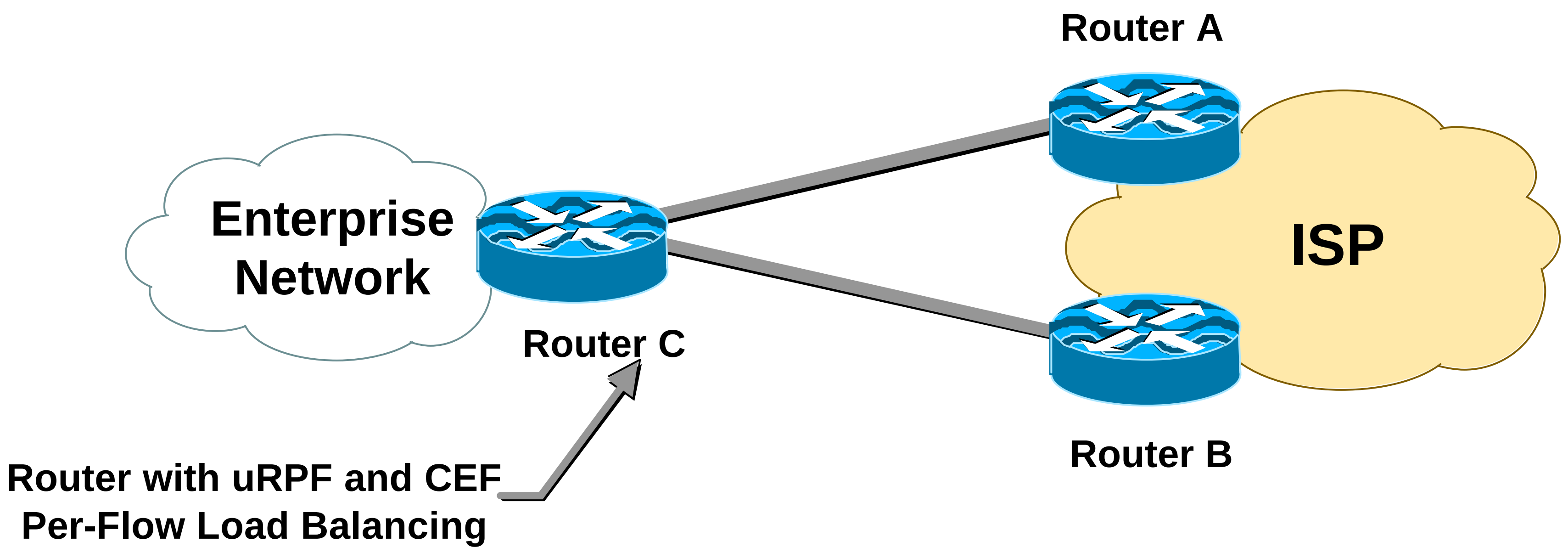
Unicast RPF — Dual Homed Customer

```
ISP Router A - Link to Customer Router C
interface serial 1/0/1
 description Link to Acme Computer’s Router C
 ip address 192.168.3.2 255.255.255.252
 ip verify unicast reverse-path
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip route-cache distributed
```

Unicast RPF — Dual Homed Customer

```
ISP Router A - Link to Customer Router C (Cont)
router bgp 109
 neighbor 192.168.10.3 remote-as 65000
 neighbor 192.168.10.3 description Multihomed Customer – Acme
Computers
 neighbor 192.168.10.3 update-source Loopback0
 neighbor 192.168.10.3 send-community
 neighbor 192.168.10.3 soft-reconfiguration inbound
 neighbor 192.168.10.3 route-map set-customer-local-pref in
 neighbor 192.168.10.3 weight 255
 .
ip route 192.168.10.3 255.255.255.255 serial 1/0/1
ip bgp-community new-format
```

Unicast RPF — Dual Homed Enterprise to One ISP



- Used to protect against spoof attacks
- Some attacks get around the RFC1918 filters by using un-allocated IP address space

Unicast RPF — Dual Homed Enterprise to One ISP

```
router bgp 65000
 no synchronization
 network 169.21.0.0
 network 169.21.0.0 mask 255.255.128.0
 network 169.21.128.0 mask 255.255.128.0
 neighbor 171.70.18.100 remote-as 109
 neighbor 171.70.18.100 description Upstream Connection #1
 neighbor 171.70.18.100 update-source Loopback0
 neighbor 171.70.10.100 send-community
 neighbor 171.70.18.100 soft-reconfiguration inbound
 neighbor 171.70.18.100 route-map Router-A-Community out
 neighbor 171.70.18.200 remote-as 109
 neighbor 171.70.18.200 description Upstream Connection #2
 neighbor 171.70.18.200 update-source Loopback0
 neighbor 171.70.18.200 send-community
 neighbor 171.70.18.200 soft-reconfiguration inbound
 neighbor 171.70.18.200 route-map Router-B-Community out
 maximum-paths 2
 no auto-summary
```

```
route-map Router-A-Community permit 10
 match ip address 51
 set community 109:70
!
route-map Router-A-Community permit 20
 match ip address 50
 set community 109:100
!
route-map Router-B-Community permit 10
 match ip address 50
 set community 109:70
!
route-map Router-B-Community permit 20
 match ip address 51
 set community 109:100
!
access-list 50 permit 169.21.0.0 0.0.127.255
access-list 51 permit 169.21.128.0 0.0.127.255
```

Unicast RPF — Dual Homed Enterprise to One ISP

```
ip route 169.21.0.0 0.0.255.255 Null 0
ip route 169.21.0.0 0.0.127.255 Null 0
ip route 169.21.128.0 0.0.127.255 Null 0
ip route 171.70.18.100 255.255.255.255 S 1/0
ip route 171.70.18.200 255.255.255.255 S 1/1
ip bgp-community new-format
!
```

```
interface serial 1/0/
 description Link to Upstream Router A
 ip address 192.168.3.1 255.255.255.252
 ip verify unicast reverse-path
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip load-sharing per-destination
 ip route-cache distributed
!
interface serial 1/0
 description Link to Upstream ISP Router B
 ip address 192.168.3.5 255.255.255.252
 ip verify unicast reverse-path
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip load-sharing per-destination
 ip route-cache distributed
```

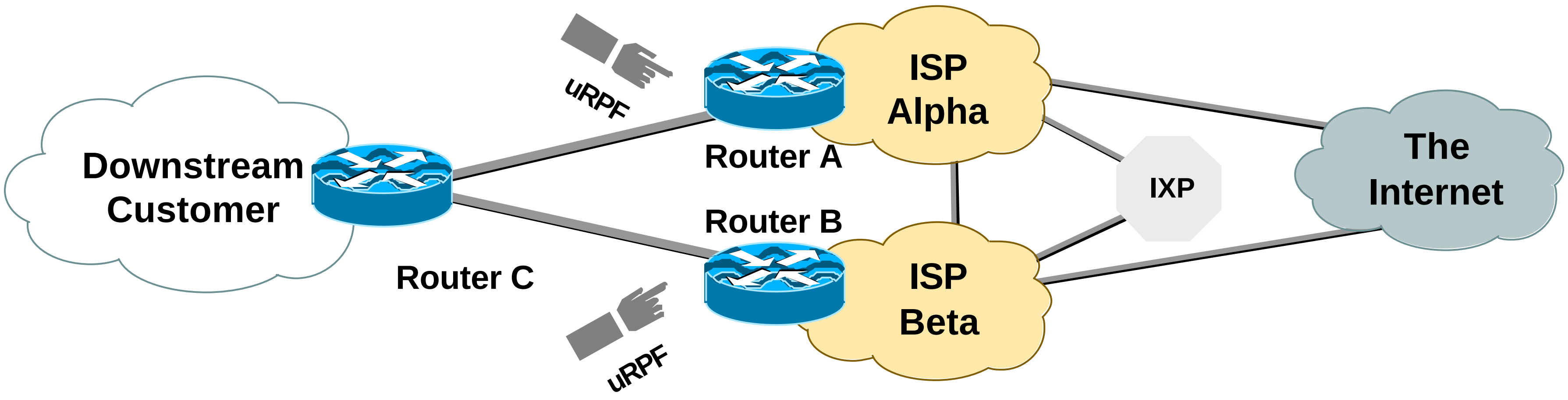
Unicast RPF — Dual Homed Enterprise to One ISP

- **The results:**

  The customer has a multihomed connection to the Internet with Unicast RPF protecting source spoofing

  The ISP provides a multihomed solution with Unicast RPF turned on

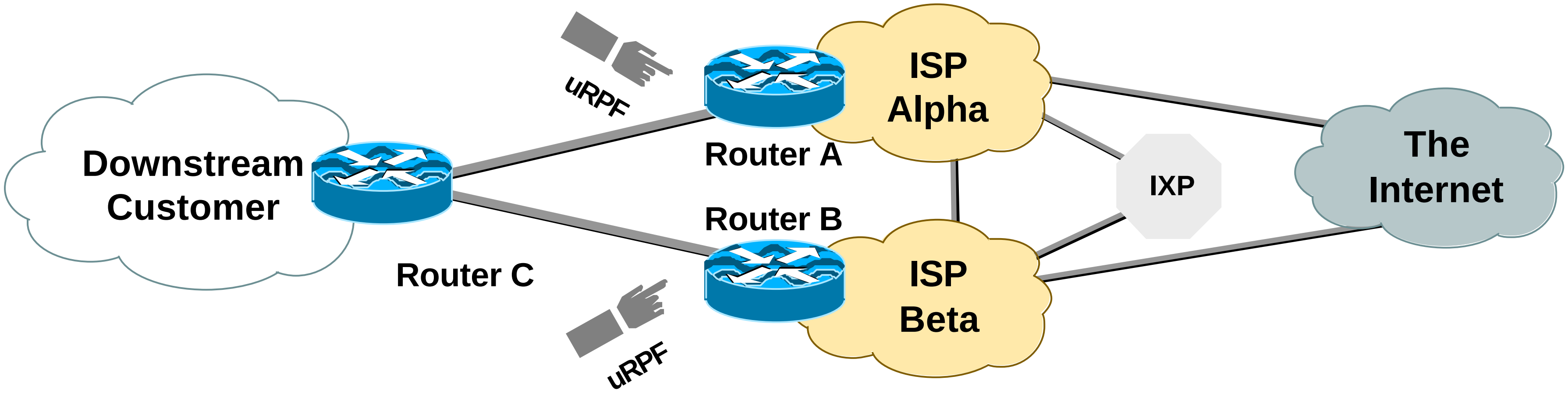
Unicast RPF — Dual Homed Enterprise to Two ISPs



- **ISP Configuration for both ISPs are similar to a dual homed customer.**

<u>BGP weight</u> is used to over ride AS path prepends

Unicast RPF — Dual Homed Enterprise to Two ISPs

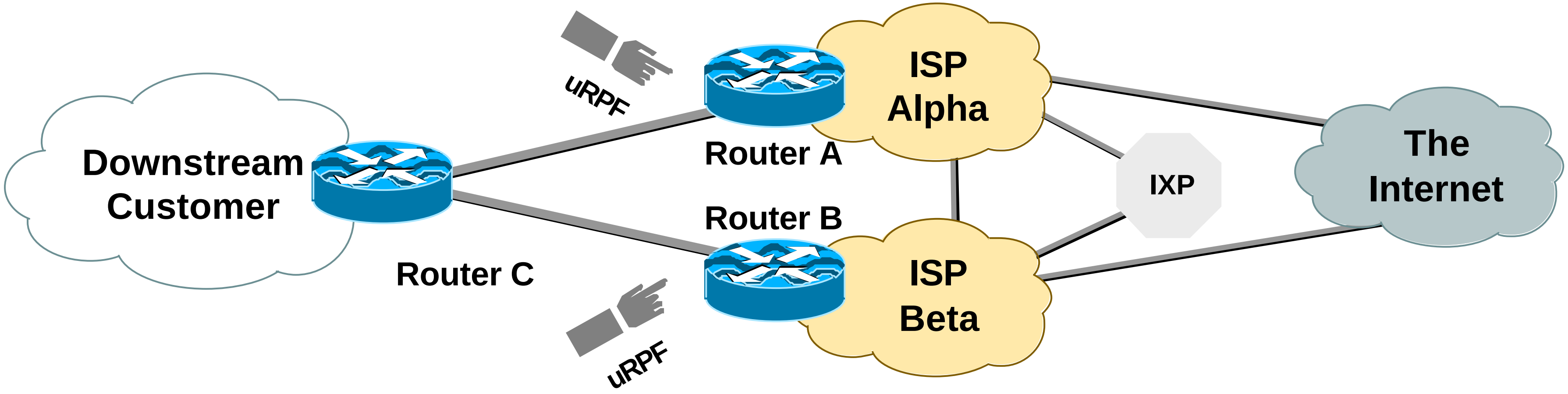


- BGP weight override an AS path prepend

  BGP weight on Router A will keep the preferred path for packets on that router to be C « A

  BGP weight on Router B will keep the preferred path for packets on that router to be C « B

Unicast RPF — Dual Homed Enterprise to Two ISPs



- Enterprise configuration cannot use **maximum-paths**

Need equal AS paths for maximum-paths to work

Unicast RPF — The ACL Bypass Option

- ACLs can now be used with Unicast RPF (Strict Mode):

  ```
  ip verify unicast reverse-path 171
  ```

- uRPF ACLs are used to:

  Allow exceptions to the Unicast RPF check

  Identify characteristics of spoofed packets being dropped by Unicast RPF

Unicast RPF — The ACL Bypass Option

- Cisco 7206 with bypass ACL

```
interface ethernet 1/1
  ip address 192.168.200.1 255.255.255.0
  ip verify unicast reverse-path 197
 !
 access-list 197 permit ip 192.168.201.0 0.0.0.255 any log-input

show ip interface ethernet 1/1 | include RPF
  Unicast RPF ACL 197
  1 unicast RPF drop
  1 unicast RPF suppressed drop
```

Unicast RPF — The ACL Bypass Option

- Cisco 7500 with a classification filter:

```
interface ethernet 0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast reverse-path 171
!
access-list 171 deny icmp any any echo log-input
access-list 171 deny icmp any any echo-reply log-input
access-list 171 deny udp any any eq echo log-input
access-list 171 deny udp any eq echo any log-input
access-list 171 deny tcp any any established log-input
access-list 171 deny tcp any any log-input
access-list 171 deny ip any any log-input
```

Unicast RPF — The ACL Bypass Option

- **Show the "log-input" results:**

  7200—logging done in the RP

  ```
  show logging
  ```

  7500—logging done on the VIP

```
Excalabur#sh controllers vip 4 logging
show logging from Slot 4:
.
4d00h: %SEC-6-IPACCESSLOGNP: list 171 denied 0 20.1.1.1
   -> 255.255.255.255, 1 packet
.
```

Unicast RPF — Operations Tools

```
Excalabur#sh cef inter serial 2/0/0
Serial2/0/0 is up (if_number 8)
  Internet address is 169.223.10.2/30
  ICMP redirects are never sent
  Per packet loadbalancing is disabled
  IP unicast RPF check is enabled
  Inbound access list is not set
```

Unicast RPF — Operations Tools

- **Other commands:**

```
show ip traffic | include RPF

show ip interface ethernet 0/1/1 | include RPF

debug ip cef drops rpf <ACL>
```

Unicast RPF — Bottom Line

- Unicast RFP is another tool to help defend the Internet
- Unicast RPF works when it is deployed within its operational envelop
- Unicast RPF does not work when just thrown into the network; give it some thought

New Unicast RPF Enhancements

- **Objectives—Allow Unicast RPF to work on an ISP-ISP Edge or ISP-Complex multihomed enterprise customer edge**

  Phase 1—Original uRPF (BCP 38/ RFC 2827)

  Phase 2—Loose check — if exist in FIB

  Phase 3—Dedicated VRF table per interface

New Unicast RPF Enhancements

- Phase 2—Loose check (if exist)

  DDTS CSCdr93424

  12.0(14)S for 7200, 7500, and GSR Engine 0 and 1

  Scheduled 12.0(19)S for GSR Engine 2

  Scheduled 12.1(8)E for CAT6K

New Unicast RPF Enhancements

- Objectives in phase 2:

  Allow for uRPF to work on the ISP⇔ISP edge of the network

  Create a new tool to drop DOS/DDOS attacks on the edge of an ISP’s network

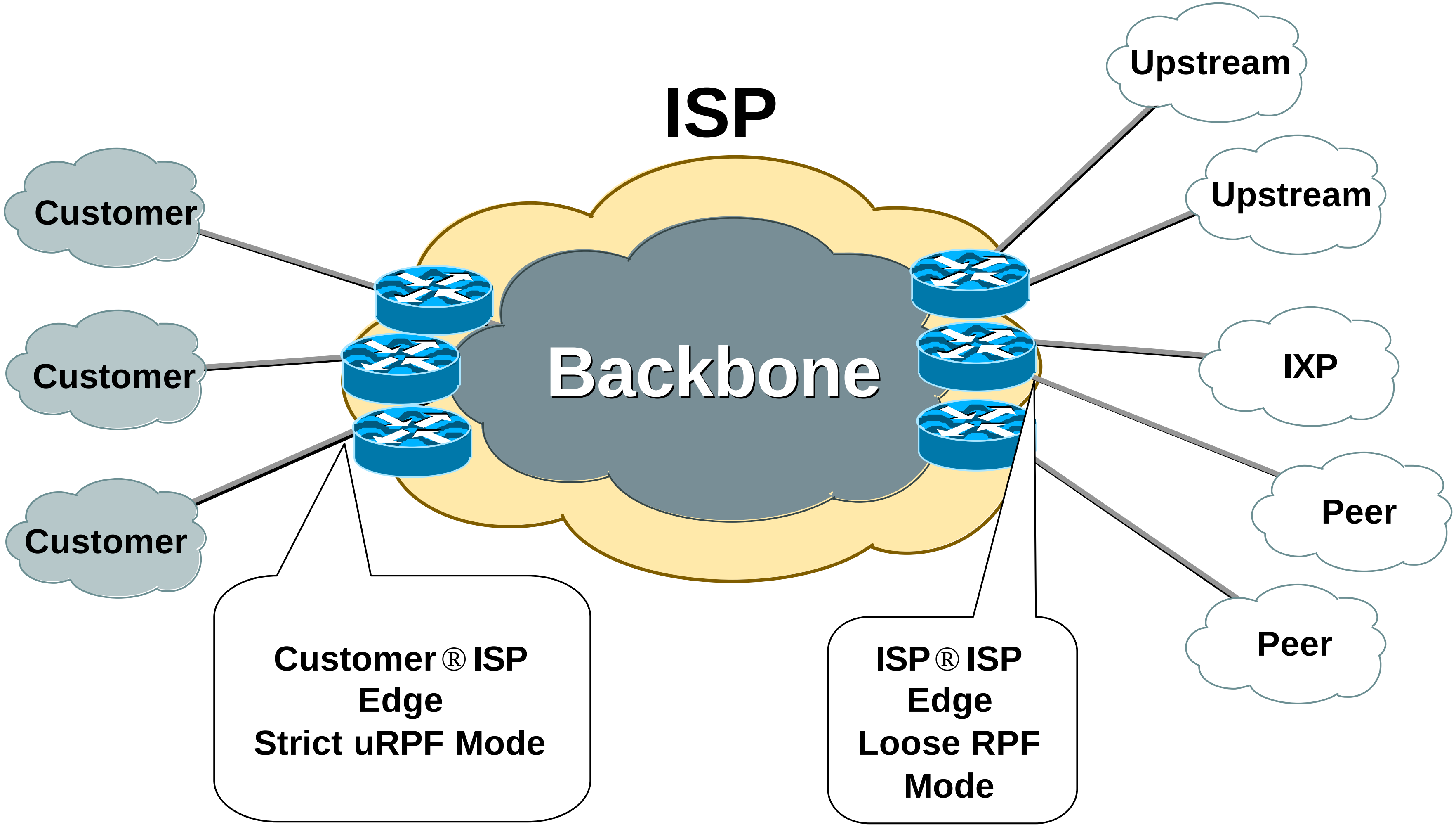
  All for the drop to be activated and controlled by a network protocol

New Unicast RPF Enhancements

- New commands from DDTS CSCdr93424:

```
ip verify unicast reverse-path [allow-self-
ping] [<list>]

ip verify unicast source reachable-via
(rx|any) [allow-default] [allow-self-ping]
[<list>]
```

uRPF Originally Designed for the Customer®ISP Edge



Customer®ISP
Edge
Strict uRPF Mode

ISP®ISP
Edge
Loose RPF
Mode

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP's Network

Cisco.com

Recent DOS Attacks and the Defence

Recent Attacks

- **Code Red**

  http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

- **NIMDA**

  http://www.cisco.com/warp/public/63/nimda.shtml

Code Red Worm Version I

- ***DoS flooding is side-effect of scanning***
- **Logic – Exploits MS-IIS URL vulnerability**
- **Flood – Specific DoS attack against www.whitehouse.gov (198.137.240.91)**
- **Scans for a list of IP addresses**
- **Scanning causes sharp traffic increase**
- **Widespread denial of service on internet**
- **Some Cisco products affected**

Code Red Worm Version I Signature

- Original CodeRed and Variant HTTP GET Request Header
- Initial infection attempt sends this large header
- Looks for a file with an .IDA extension
- Used for IDS Signature Detection

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%uc
bd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%
u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

Code Red Worm Version II

- *Same behaviour as version 1 plus more*
- *Exploits MS Indexing Server ISAPI Buffer Overflow vulernability shipping with Win2000*
- Looks up www.whitehouse.gov address via DNS
- Scans for a list of random IP addresses
- Scanning causes sharp traffic increase
- Uses more scanning/infection threads
- Copies cmd.exe into two directories
- Creates copies of explorer.exe on C:/D: and embeds trojan code for executing remote commands

Code Red Worm Version II Signature

- CodeRed Version 2 HTTP GET Request Header
- Uses XXXX as filler & different machine code
- Use for IDS Signature Detection

```
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%
u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u909
0%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0
000%u00=a HTTP/1.0
```

Code Red Detection and Prevention Techniques

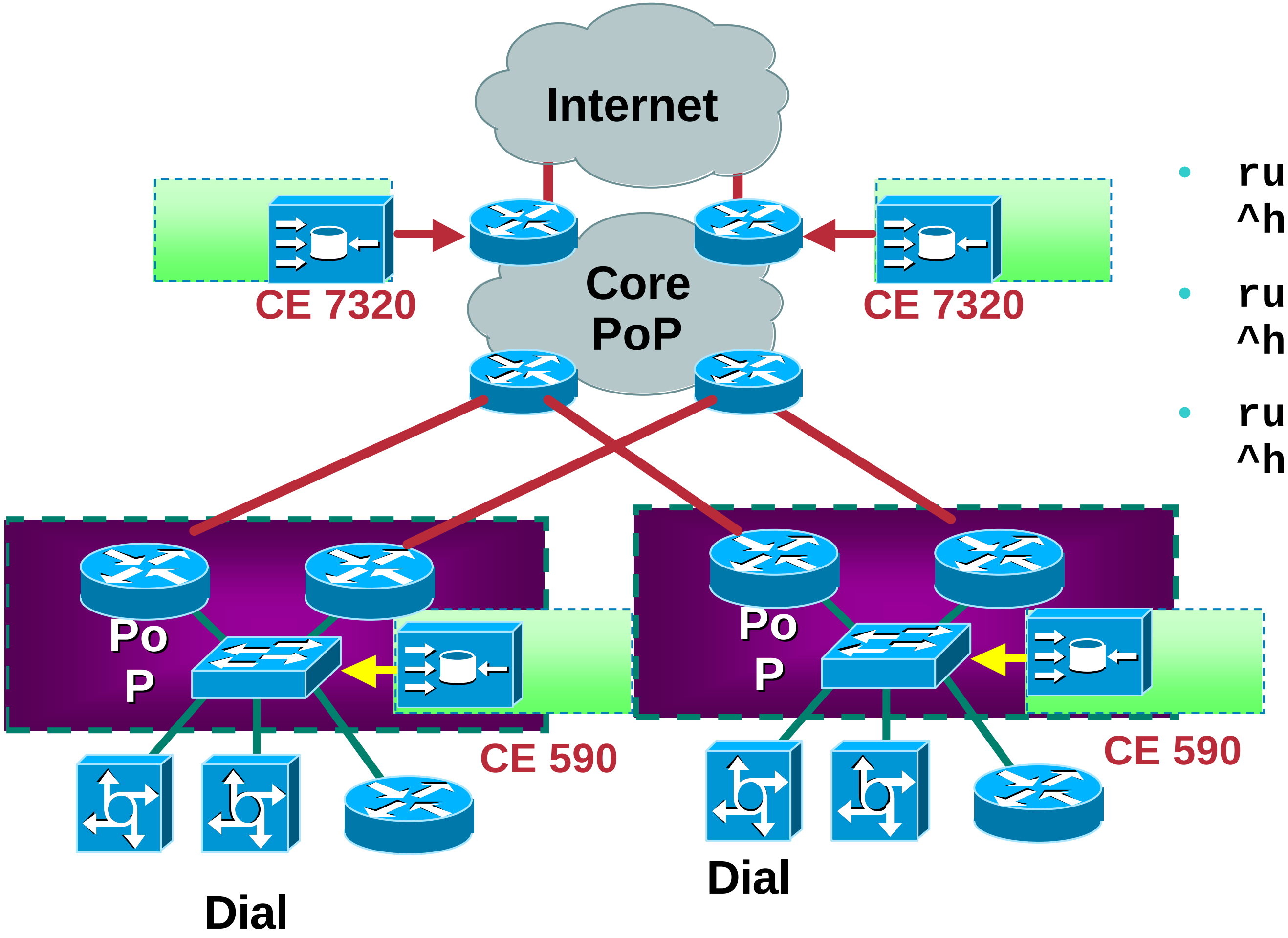
- netstat – to check Win2K/NT connections
- netflow – *sh ip cache flow* | *include 0050* on routers
- Apply Microsoft patch to IIS servers
- Configure CacheEngine with CodeRed blocking rules
- Ensure “no ip http server” on routers
- Restrict xml access on CSS11000 switch
- Use NBAR at network ingress points

  Network Based Application Recognition

  NBAR can use ACLs, PBR and CAR rate-limits

  NBAR needs CEF and IOS 12.1(5)T / (6)E

Cisco Cache Engine Rules



- `rule block url-regex ^http://.*/cmd\.exe`
- `rule block url-regex ^http://.*/root\.exe`
- `rule block url-regex ^http://.*/default\.ida`

NBAR Ingress Blocking Example using a Rate-limit

- Classify Inbound CodeRed with Class-Map

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*default.ida*"
Router(config-cmap)#match protocol http url "*x.ida*"
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*"
```

- Use Policy-Map to define rate-limit for class

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap)#police 1000000 31250 31250 conform-action drop exceed-action drop
 violate-action drop
```

- Apply policy to ingress interface to drop packets

```
Router(config)#interface ethernet 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

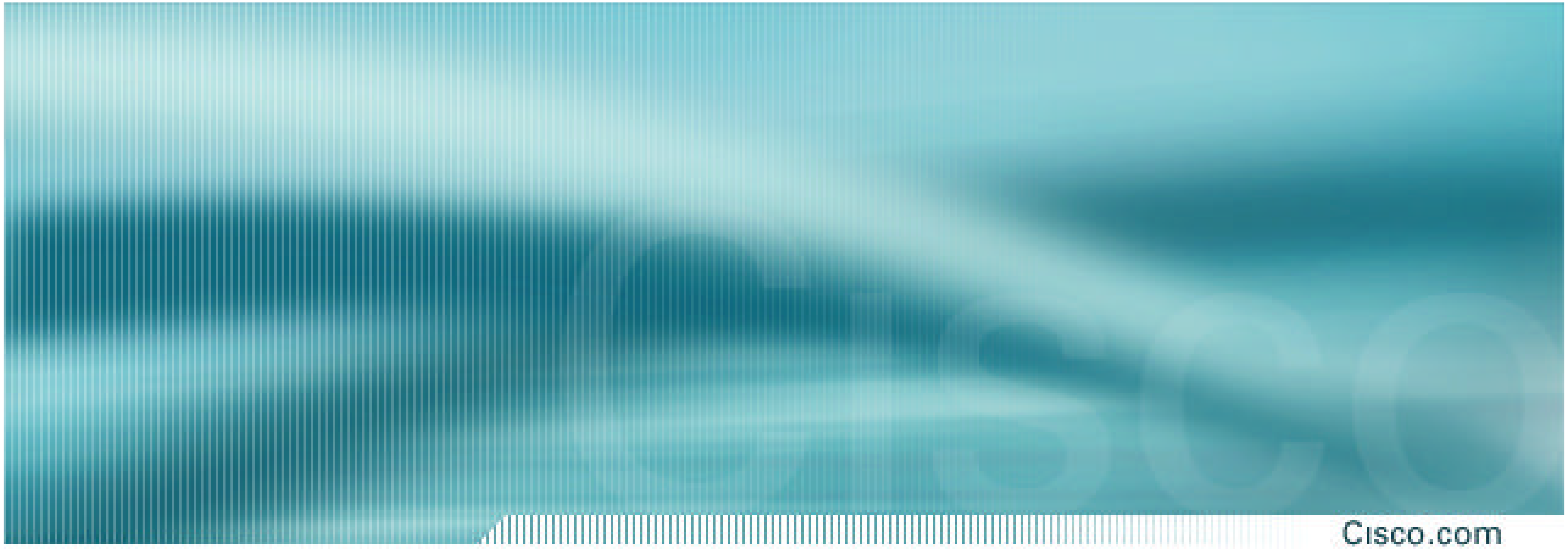
NIMDA

- Could have been more easily prevented with proper router filters on network edges and between different subnets
- NBAR can be used to catch/block certain file types
- Cisco Security Advisory (and others) documents recommendations for network filtering

  Already documented and widely used in ISP community

Router Security Agenda

- Overview
- Securing the Router
- Securing the Routing Protocols
- Securing the Network
- Administrative and Operational Practices
- Unicast Reverse Path Forwarding
- Recent DOS attacks and the defence
- Tracking DoS/DDOS Attacks through an ISP’s Network



Tracking DoS/DDoS Attacks through an ISP’s Network

Tracking DOS/DDOS Attacks through a Network

- **Five Phase Approach:**

  Preparation

  Identification

  Classification

  Traceback

  Reaction

Phase 1 – Preparation

- **Preparation is critical!**

  You know your *customers* are going to be attacked

  It is not a matter of if but how often and how hard

  The Internet is not a nice place anymore!

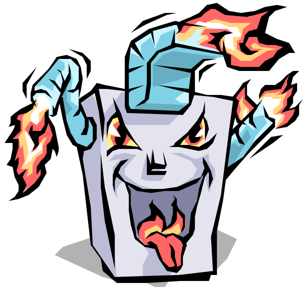
  Think battle plans

- **Militaries know the value of planning, practice, drilling and simulation**

  Those that are prepared will be victorious

Phase 1 – Preparation

- The problem – Most ISP NOCs:
  - Do not have security plans
  - Do not have security procedures
  - Do not train in the tools or procedures
  - OJT (on the job training) – learn as it happens



Phase 1 – Preparation

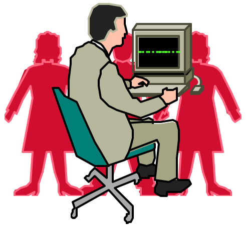
- Red Team/Blue Team exercises

  Divide up into two teams — one defends, one attacks

  Referee assigns the attackers with an objective (get this file, deface the web site, take down the target, etc.)

  Defenders use network/system designs and tools/procedures to defend the target

  One of the most effective ways to get your staff into the depths of TCP/IP, OS, applications, and security



Phase 2 – Identifying an Attack

- When are we being probed?
  - Probes happen all the time; which ones are important?
  - Probes precede an attack; if you can track specific probes, you might get a heads up that an attack is imminent
- When are we being attacked?
  - #1 way to identify that there is an attack in progress is when a customer calls the NOC
  - New ISP oriented IDS tool are in the works

Phase 3 – Classifying an Attack

- **How are we being attacked?**
  - **Once the attack starts, how do you find specifics of the attack?**
  - **Customer might provide information**
  - **Tools and procedures needed inside an ISP to specific information on the attack**
  - **Minimum source addresses and protocol type**

Phase 3 – Classifying an Attack

- **Use ACL with permit for a group of protocols to drill down to the protocol**

```
Extended IP access list 169
        permit icmp any any echo (2 matches)
        permit icmp any any echo-reply (21374 matches)
        permit udp any any eq echo
        permit udp any eq echo any
        permit tcp any any established (150 matches)
        permit tcp any any (15 matches)
        permit ip any any (45 matches)
```

See http://www.cisco.com/warp/public/707/22.html

Phase 4 – Traceback the Attack

- **From where are we being attacked (inside or outside)?**

  Once you have a fundamental understanding of the type of attack (source address and protocol type), you then need to track back to the ingress point of the network

  Two techniques—hop by hop and jump to ingress

Traceback via Hop by Hop Technique

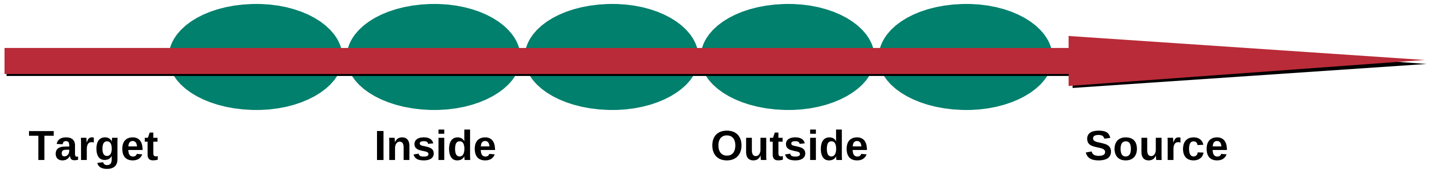
- Hop by hop tracebacks takes time

  Starts from the beginning and traces to the source of the problem

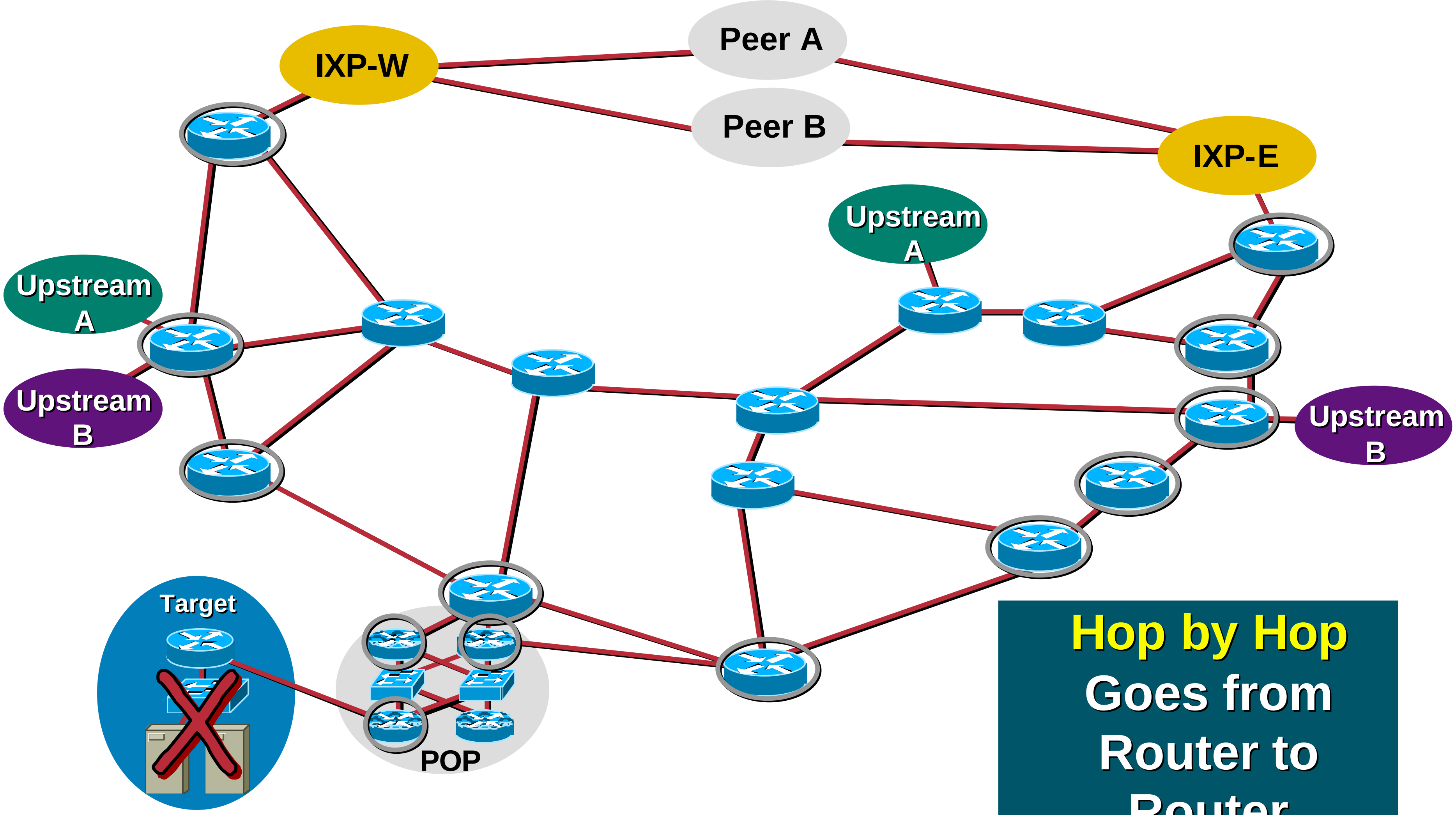
  Needs to be done on each router

  Often requires splitting—tracing two separate paths

  Speed is the limitation of the technique



Traceback via Hop by Hop Technique



Hop by Hop Goes from Router to Router

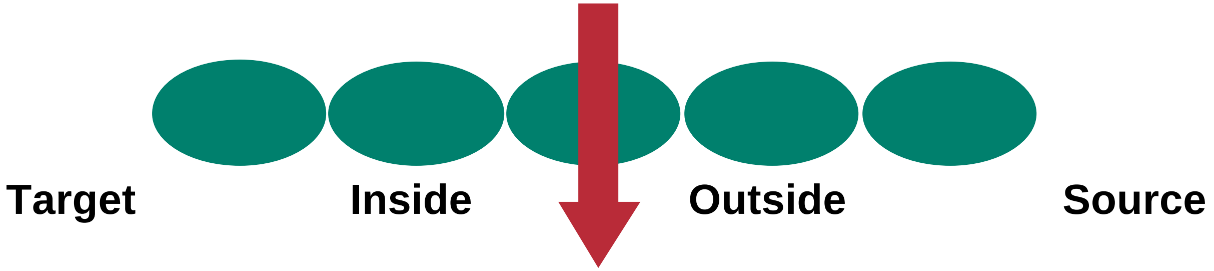
Traceback via the Jump to Ingress Technique

- **Jump to ingress traceback divides the problem in half**

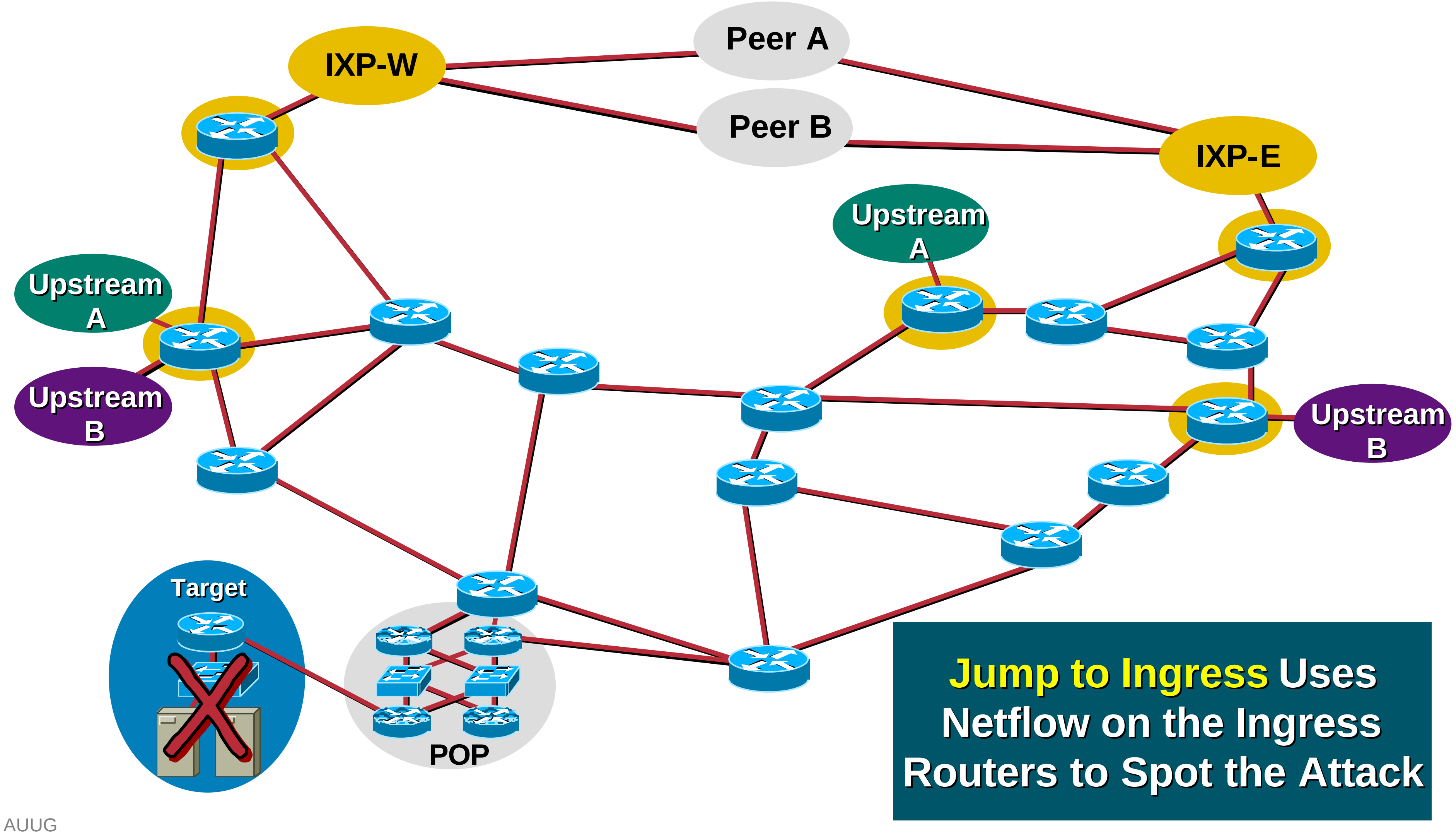
  Is the attack originating from inside the ISP or outside the ISP?

  Jumps to the ISP's ingress border routers to see if the attack is entering the network from the outside

  Advantage of speed—are we the source or someone else the source?



Traceback via the Jump to Ingress Technique



Jump to Ingress Uses Netflow on the Ingress Routers to Spot the Attack

Phase 4 – Traceback the Attack

- Two techniques
  - Apply temporary ACLs with log-input and examine the logs (like step 2)
  - Query Netflow's flow table (if ip route-cache flow is turned on)

Traceback with ACLs

```
 access-list 170 permit icmp any any echo
 access-list 170 permit icmp any any echo-reply log-input
 access-list 170 permit udp any any eq echo
 access-list 170 permit udp any eq echo any
 access-list 170 permit tcp any any established
 access-list 170 permit tcp any any
 access-list 170 permit ip any any
!
 interface serial 0
   ip access-group 170 out
! Wait a short time - (i.e 10 seconds)
   no ip access-group 170 out
```

Traceback with ACLs

- Original technique for doing tracebacks
- Hazard—inserting change into a network that is under attack
- Hazard—log-input requires the forwarding ASIC to punt the packet to capture log information
- BCP is to apply the filter, capture just enough information, then remove the filter

Traceback with Netflow

- Using Netflow for hop-by-hop traceback:

```
Beta-7200-2>sh ip cache 198.133.219.0 255.255.255.0 verbose flow
IP packet size distribution (17093 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .735 .088 .054 .000 .000 .008 .046 .054 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 1257536 bytes
  3 active, 15549 inactive, 12992 added
  210043 ager polls, 0 flow alloc failures
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          35      0.0        80    41      0.0      14.5      12.7
UDP-DNS             20      0.0         1    67      0.0       0.0      15.3
UDP-NTP           1223      0.0         1    76      0.0       0.0      15.5
UDP-other        11709      0.0         1    87      0.0       0.1      15.5
ICMP                 2      0.0         1    56      0.0       0.0      15.2
Total:           12989      0.0         1    78      0.0       0.1      15.4

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Fa1/1          192.168.45.142  POS1/0         198.133.219.25  11 008A 008A     1
Fa1/1          192.168.45.113  POS1/0         198.133.219.25  11 0208 0208     1
Fa1/1          172.16.132.154  POS1/0         198.133.219.25  06 701D 0017    63
```

Spoofed Flows are Tracks in Netflow!

Traceback with Netflow

- **Generic ways to use the Netflow command:**

  show ip cache <addr> <mask> verbose flow

  show ip cache flow | include <addr>

  Proactive approach—create scripts ……

  **ssh -x -t -c [des|3des] -l <username> <IPAddr>
  "show ip cache <addr> <mask> verbose flow"**

Traceback with Netflow

- GSR—use the show controllers with sample Netflow (if LC supports SNF)

```
GSR-2# exec slot 0 sh ip cache <addr> <mask>
verbose flow
```

- 7500 with dCEF—`CSCdp91364.`

```
7500# exec slot 0 sh ip cache <addr> <mask>
verbose flow
```

- Remember! *execute-on all* to get Netflow from all the LC/VIPs.

Traceback with Netflow

- Key advantage of Netflow:

  No changes to the router while the network is under attack; passive monitoring

  Scripts can be used to poll and sample throughout the network

  IDS products can plug into Netflow

  Working on a MIB for SNMP access

Phase 5 – React to the Attack

- Do something to mitigate the impact of the attack OR stop the attack

  Options can be everything from do nothing (doing something might cause other problems) to unplug from the source of the attack (another country during a cyberwar attack)

- Most ISPs try to help their customers

  Rate-limit the attack

  Drop the packets based on a list of source addresses

- Reactions need to be fast and flexible

Phase 5 – React to the Attack

- **Three techniques used to drop or rate limit:**

  ACLs—Manual upload

  uRPF—Remote trigger via BGP

  CAR—Manual upload or remote trigger via BGP

Reacting to an Attack with ACL

- **Traditional mode of stopping attacks**
- **Scaling issues encountered:**

  Updates of ACLs on many many routers a pain

  Additive ACLs when there are multiple attacks on multiple customers are a pain

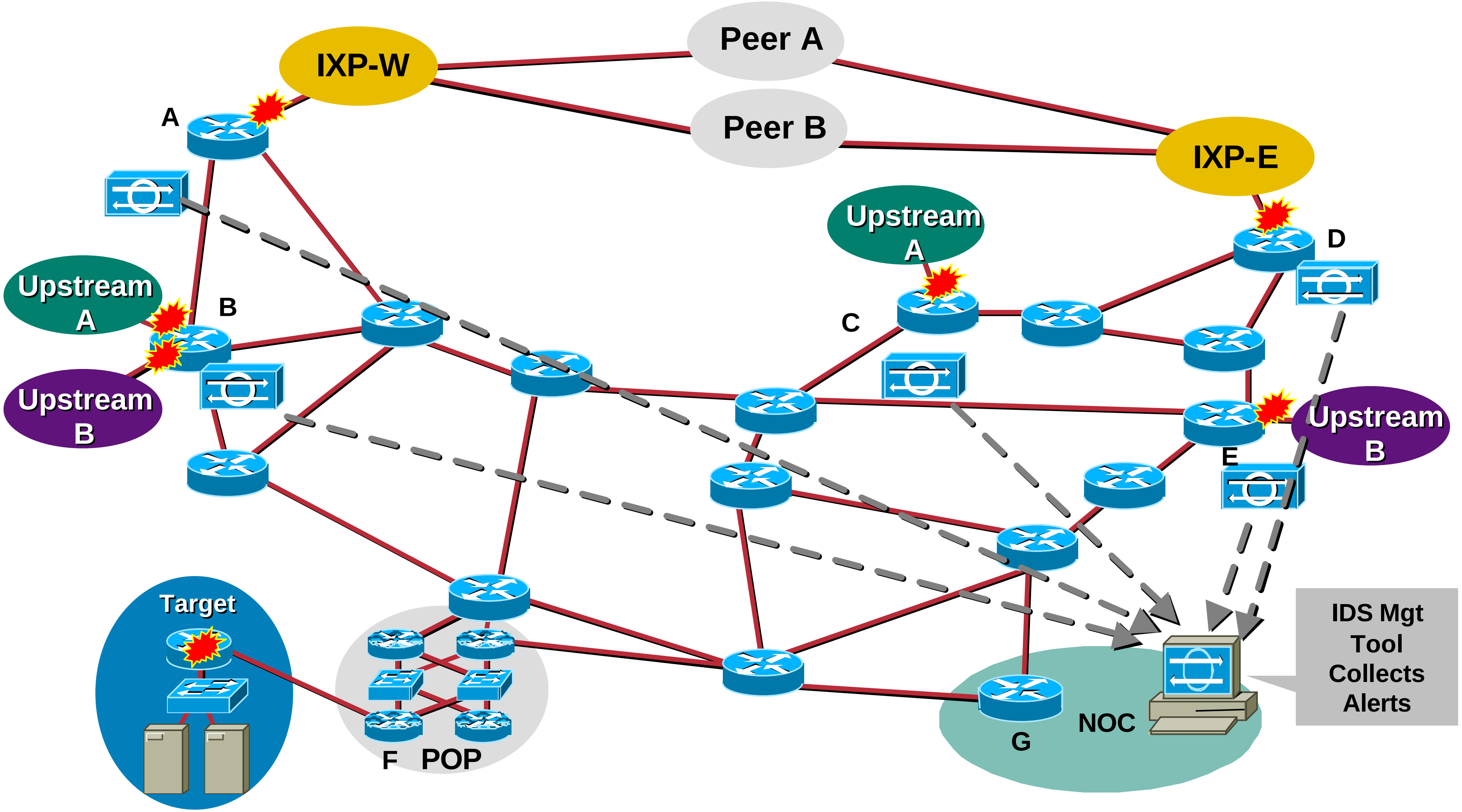
  Confusion with the "Line Rate Debate"

Reacting to an Attack with uRPF

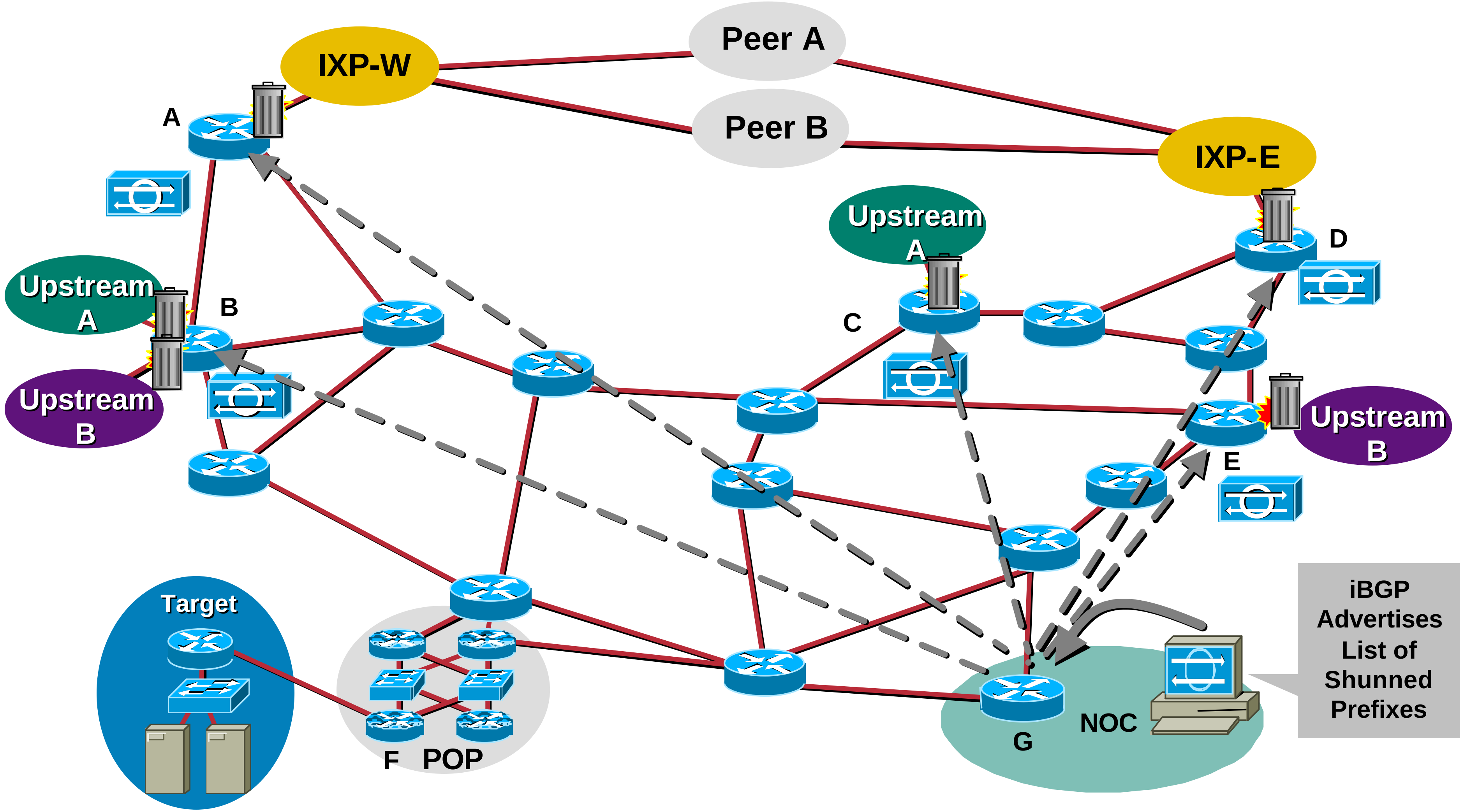
- uRPF loose check mode can be used on the ISP® ISP edge
- Can be used remote trigger drops of a DOS/DDOS flow
- Allows many many routers to be simultaneously updated with a new drop list all via a routing protocol
- Effect L3 filter (source and destination address)

Reacting to an Attack with uRPF

Cisco.com

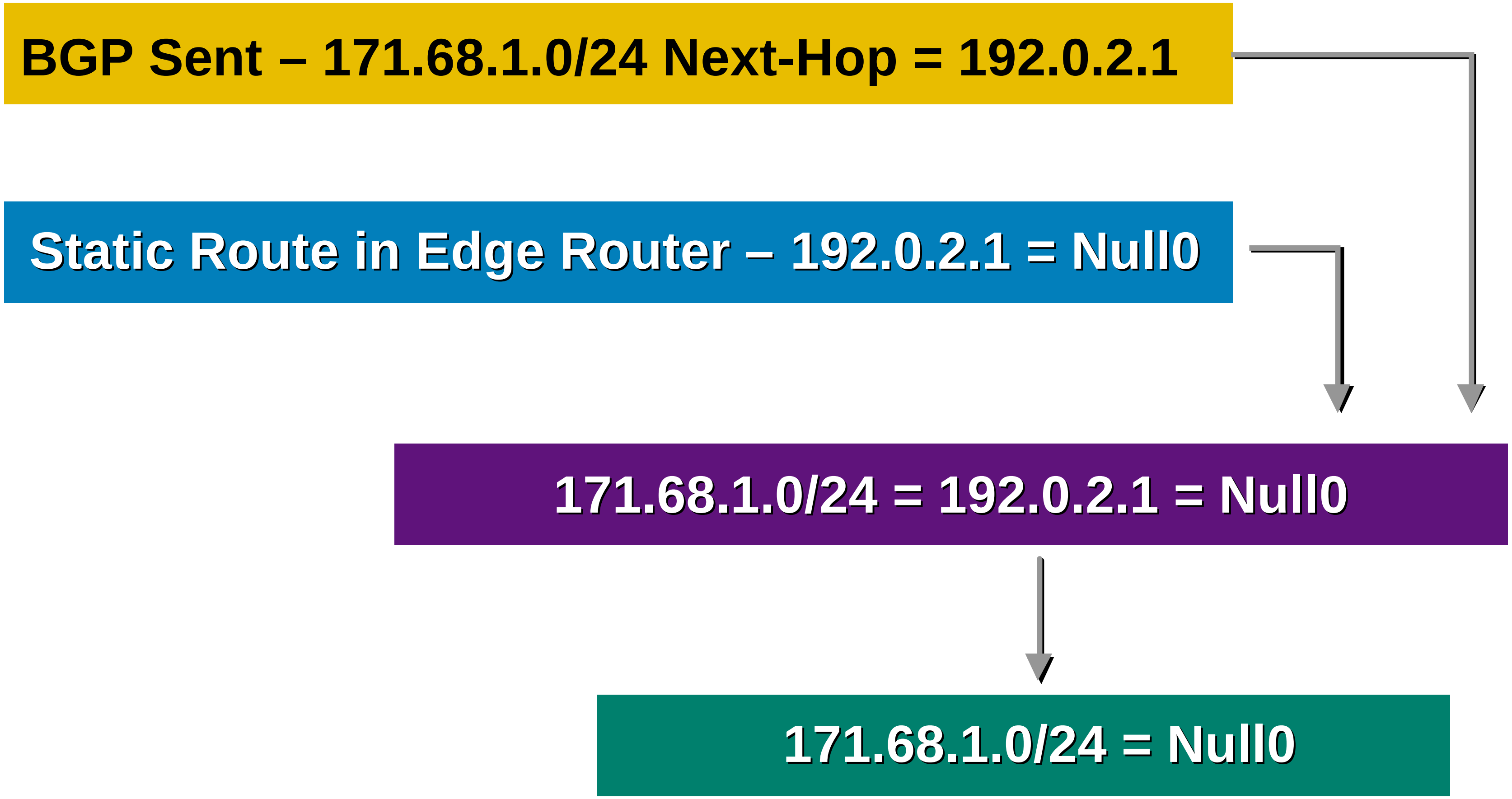


Reacting to an Attack with uRPF



iBGP Advertises List of Shunned Prefixes

Reacting to an Attack with uRPF



BGP Sent – 171.68.1.0/24 Next-Hop = 192.0.2.1

Static Route in Edge Router – 192.0.2.1 = Null0

171.68.1.0/24 = 192.0.2.1 = Null0

171.68.1.0/24 = Null0

Reacting to an Attack with uRPF

- **What is needed?**

  uRPF loose check on all border routers

  Static to Null0 with an address like the test-net on all border routers

  Way to inject a BGP advertisement into the network with a BGP community that will trigger the drop; (should include the no-export community and have good egress router filters)

Reacting to an Attack with uRPF

- Key advantages:
  - No ACL update
  - No change to the router's config
  - Drops happen in the forwarding path
  - Frequent changes when attacks are dynamic (or multiple attacks on multiple customers)

Reacting to an Attack with CAR

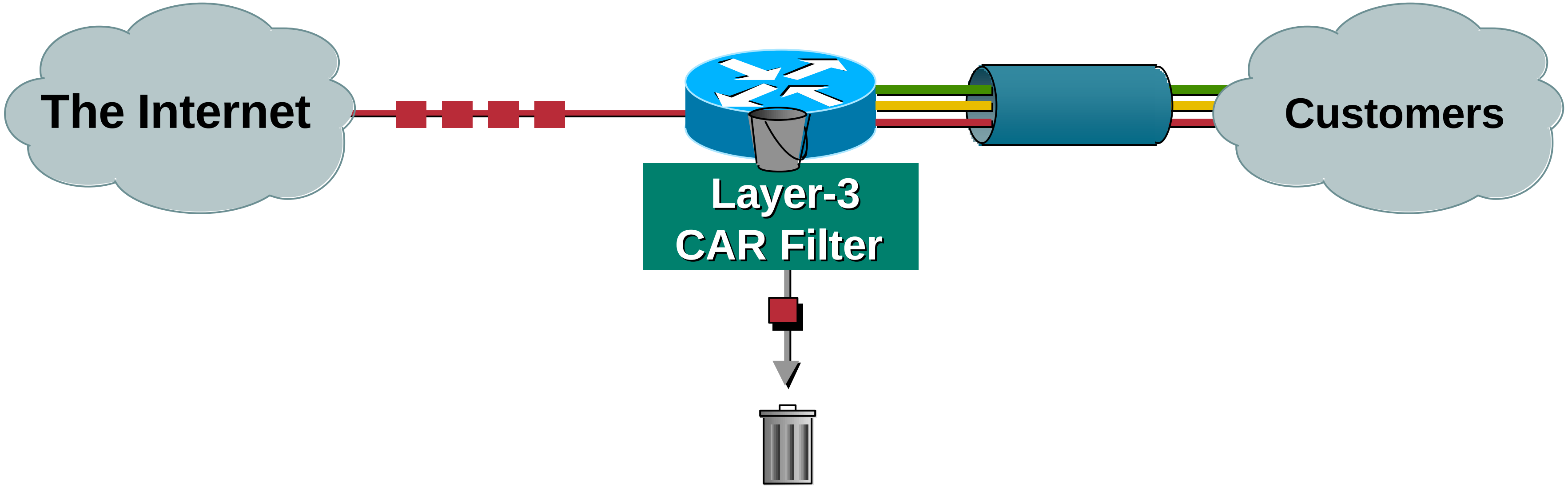
- CAR and other rate-limit features have proven to be an effective reaction to an attack

  Rate limiting attacks allow the attack to be monitored

  Data collection for law enforcement evidence can continue with rate limiting

  QOS group support (QPPB) allows for remote triggering of CAR with out logging into the router

Reacting to an Attack with CAR



- Layer-3 input and output rate limits® specifically input rate limits
- Security filters use the input rate limit to drop packets before there are forwarded through the network
- Aggregate and granular limits
  - Port, MAC address, IP address, application, precedence, QOS ID
- Excess burst policies

Reacting to an Attack with CAR

- Limit all ICMP echo and echo-reply traffic received at the borders to 256 Kbps with a small amount of burst:

```
! traffic we want to limit
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
! interface configurations for borders
interface Serial3/0/0
 rate-limit input access-group 102 256000 8000 8000
conform-action transmit exceed-action drop
```

- Multiple “rate-limit” commands can be added to an interface in order to control other kinds of traffic as well

Reacting to an Attack with CAR

- Use CAR to limit TCP SYN floods to particular hosts—without impeding existing connections; some attackers have started using very high streams of TCP SYN packets in order to harm systems

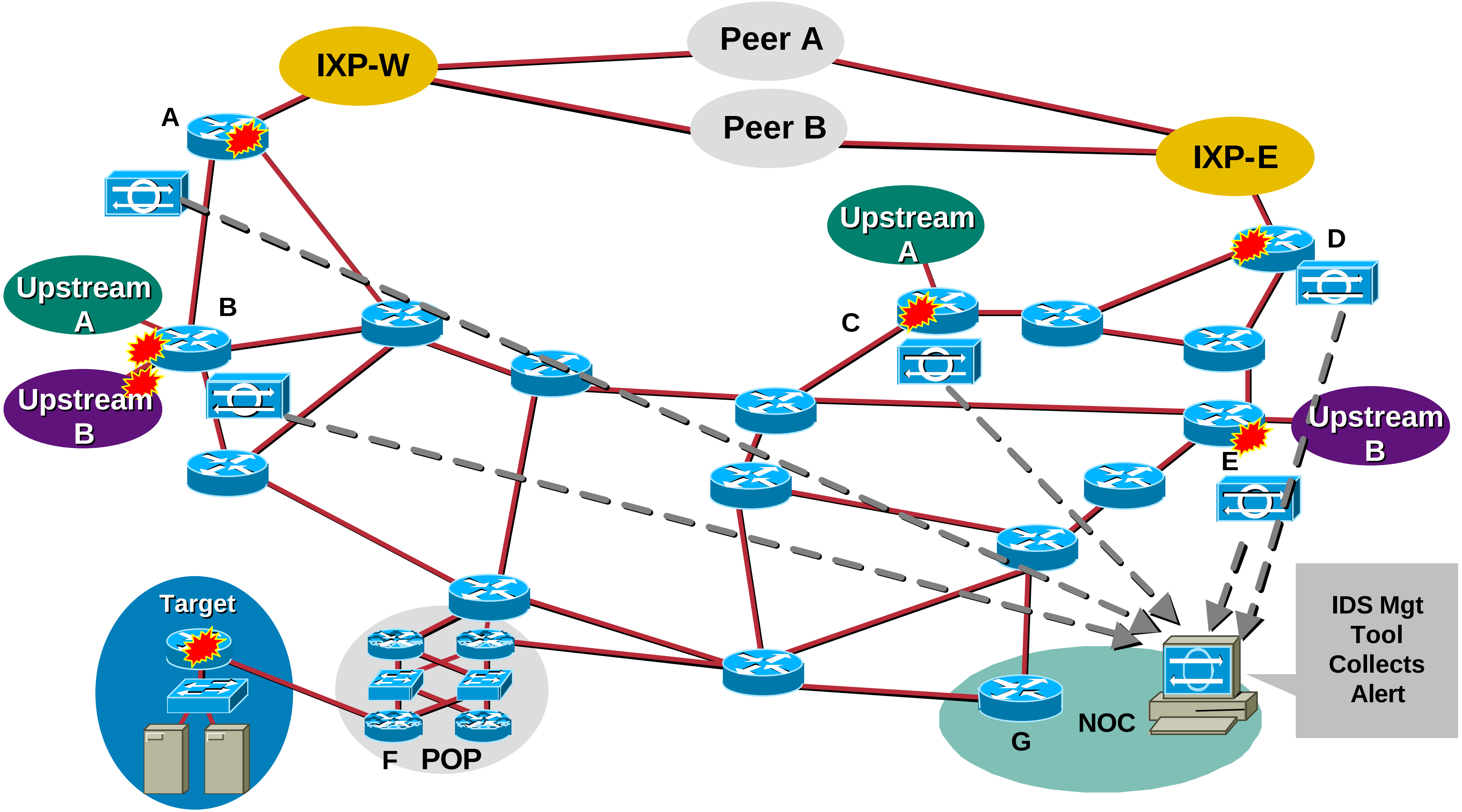
- This example limits TCP SYN packets directed at host 10.0.0.1 to 8 kbps or so:

```
! We don't want to limit established TCP sessions -- non-SYN
packets

access-list 103 deny tcp any host 10.0.0.1 established

! We do want to limit the rest of TCP (this really only
includes SYNs)

access-list 103 permit tcp any host 10.0.0.1

! interface configurations for network borders

interface Serial3/0/0

 rate-limit input access-group 103 8000 8000 8000 conform-
action transmit exceed-action drop
```

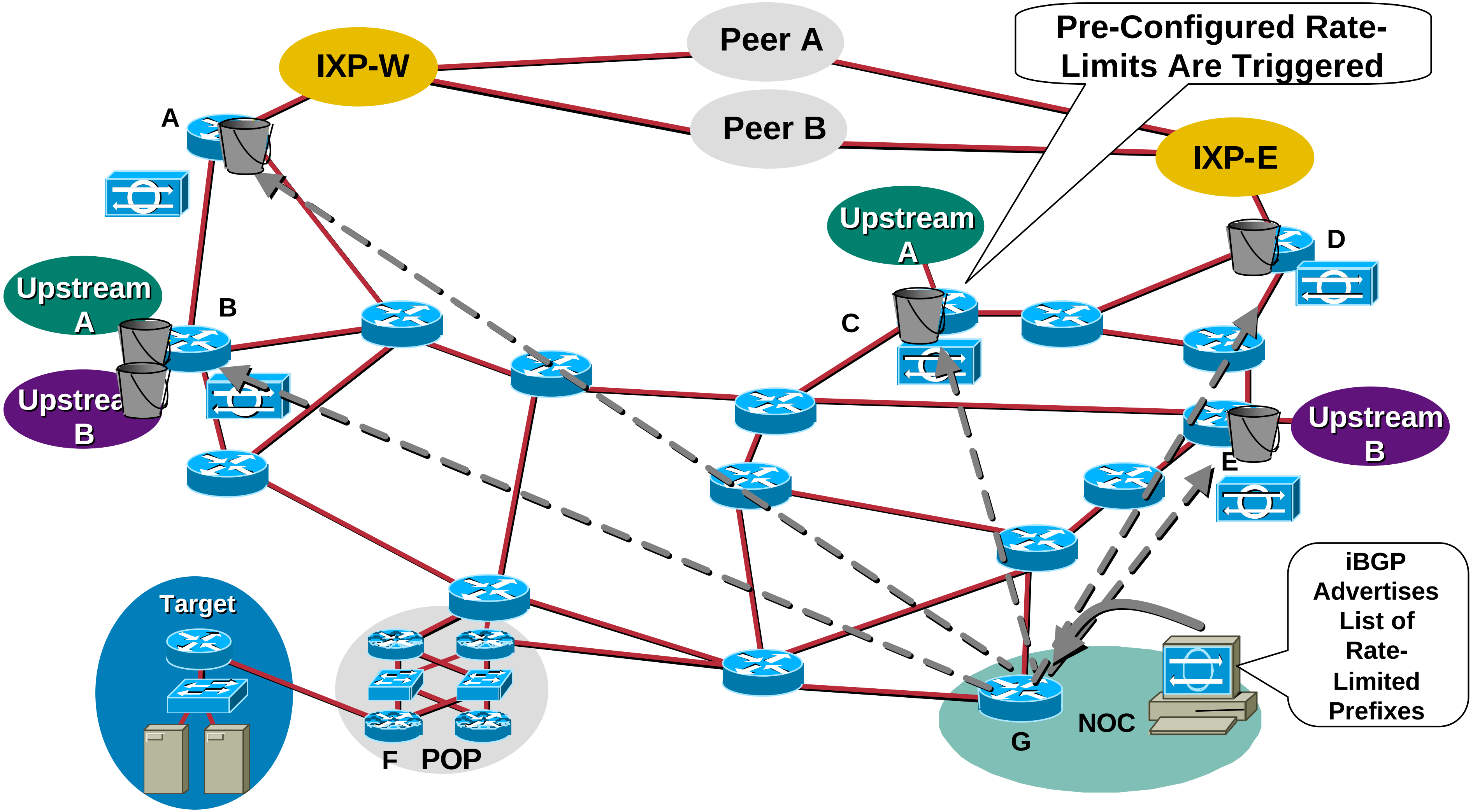
Reacting to an Attack with CAR with Remote Trigger

- CAR's rate limiting has proven to be an effective reaction tool to a DOS/DDOS attack
- The problem is how do quickly update +60 routers on the ingress of a network—especially when the attack character shifts to respond to your countermeasures?
- Answer—CAR is a FIB entry-based feature (CEF feature); so we can use a network protocol to trigger the rate limits on source/destination

Reacting to an Attack with CAR with Remote Trigger



Reacting to an Attack with CAR with Remote Trigger



Pre-Configured Rate-Limits Are Triggered

iBGP Advertises List of Rate-Limited Prefixes

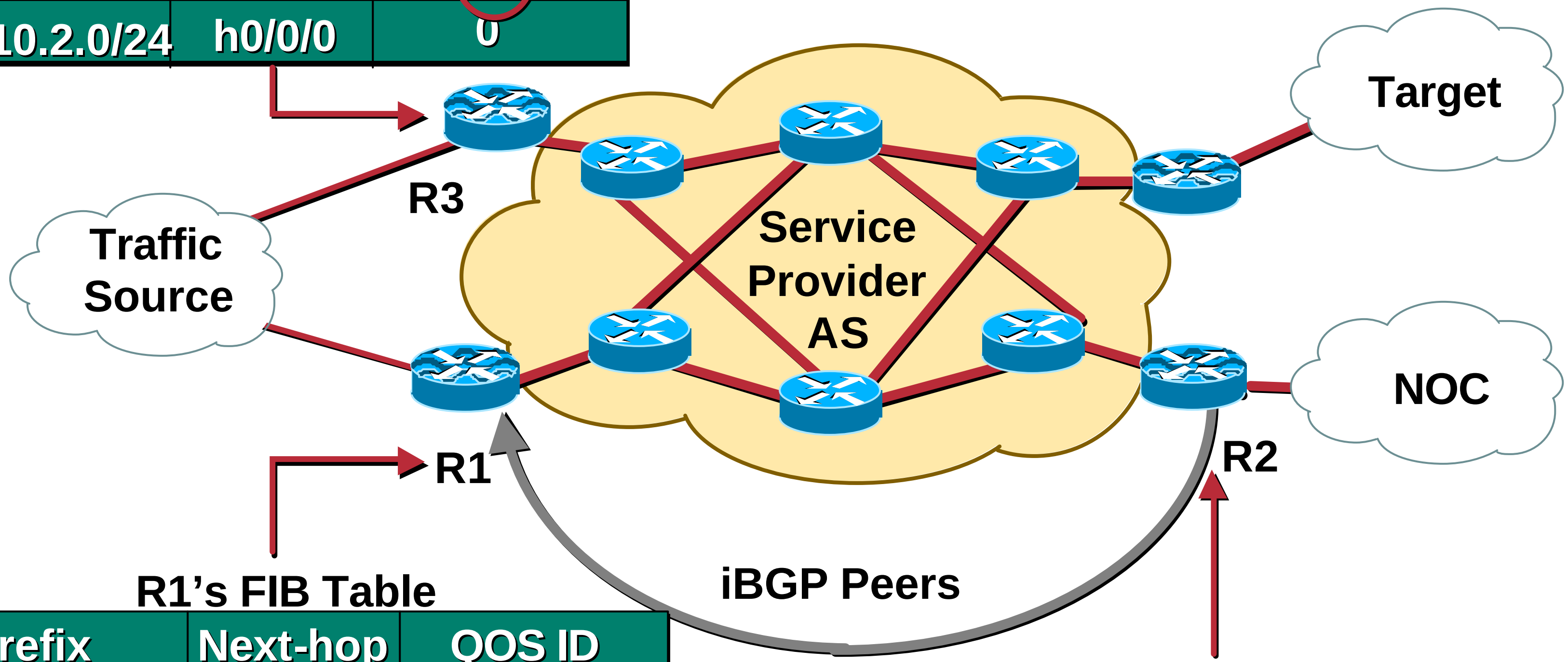
Reacting to an Attack with CAR with Remote Trigger

- **Conveys IP precedence to be used in forwarding to specified destination prefix via BGP community tag**
- **Allows ingress routers to prioritise incoming traffic**
- **Also allows IP precedence setting based on AS-path attribute or access list**
- **Inter-ISP Service Level Agreements (SLAs)**

Reacting to an Attack with CAR with Remote Trigger

R3’s FIB Table

Prefix	Next-hop	QOS ID
210.210.1.0/24	h0/0/0	66
210.210.2.0/24	h0/0/0	0



R1’s FIB Table

Prefix	Next-hop	QOS ID
210.210.1.0/24	h0/0/0	66
210.210.2.0/24	h0/0/0	0

Attack Source 210.210.1.0/24
Community 210:66 no-export

Reacting to an Attack with CAR with Remote Trigger

- NOC-Router#write term

```
router bgp 210

 network  210.210.1.0 mask 255.255.255.0
 neighbor 210.210.14.1 remote-as 210
 neighbor 210.210.14.1 route-map DOS-Trigger out
 neighbor 210.210.14.1 send-community
!
ip bgp-community new-format
!
ip route 210.210.1.0 255.255.255.0 Null0 254

access-list 1 permit 210.210.1.0 0.0.0.255
!
route-map DOS-Trigger permit 10
 match ip address 1
 set community 210:66 no-export
!
route-map DOS-Trigger permit 20
```

Note: There Are Other Ways to Originate a Prefix

Reacting to an Attack with CAR with Remote Trigger

- R1#write term

```
!
router bgp 210
 table-map DOS-Activate
 neighbor 200.200.14.4 remote-as 210
 neighbor 200.200.14.4 update-source Loopback0
!
ip bgp-community new-format
!
ip community-list 1 permit 210:66
!
route-map DOS-Activate permit 10
 match community 1
 set ip qos-group 66
!
route-map DOS-Activate permit 20
!
```

Directly Updates QOS_ID in the FIB

Matches Community and Sets the QOS Group

Reacting to an Attack with CAR with Remote Trigger

- Router 1 (cont.):

```
!
interface HSSI 0/0/0
bgp-policy source ip-qos-map
rate-limit input qos-group 66 256000 8000
8000 conform-action transmit exceed-action
drop
```

Sets the MTRIE Look up on the SRC/DST

QoS Group To Be Checked

Reacting to an Attack with CAR with Remote Trigger

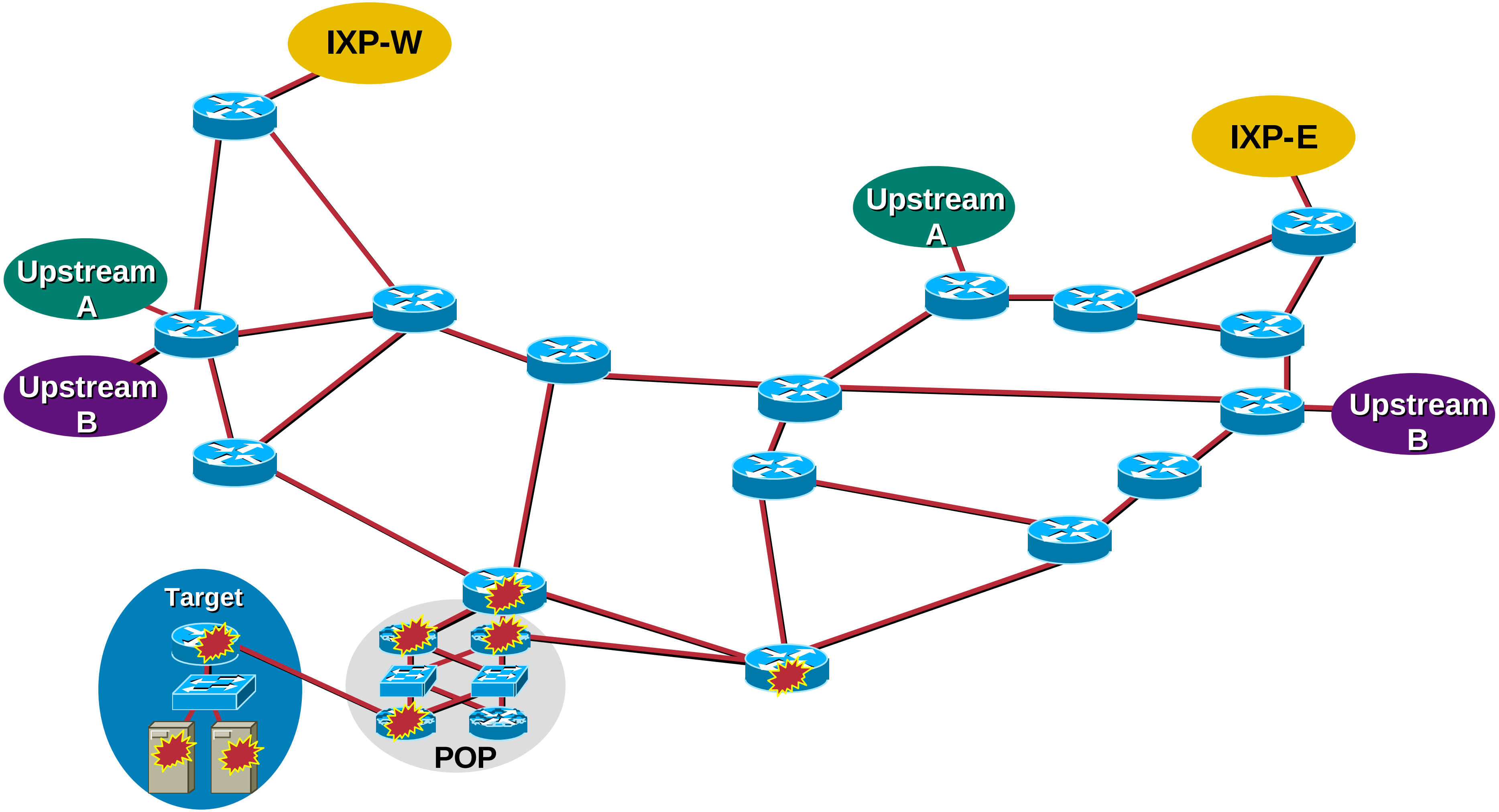
- **Caveats with CAR:**
  - **Not all platforms support the full version of CAR (I.e. Engine 2)**
  - **Not all platforms support the full version of QoS group (QPPB)**
  - **Some platforms have specialized rate limiting ASICs (7600)**
- **Bottom-line—CAR is not yet cross platform compatible (working on it)**

Example of an ISP Tracking DoS/DDoS Attacks through an ISP’s Network

Tracking Attacks—ISP POV

- Situation in the NOC
  - Alarms go off in the NOC—circuits are dropping packets
  - Major content customer calls—their site is being hit by a DoS/DDoS attack
  - Management calls, they want to know what is going on
  - Other customers call, slow network performance
  - Reporter calls—not sure how they got the NOC's number, they are looking for a quote
  - It's been 5 minutes since the first alarm went off, what do you do?!?!?!?!

The Network

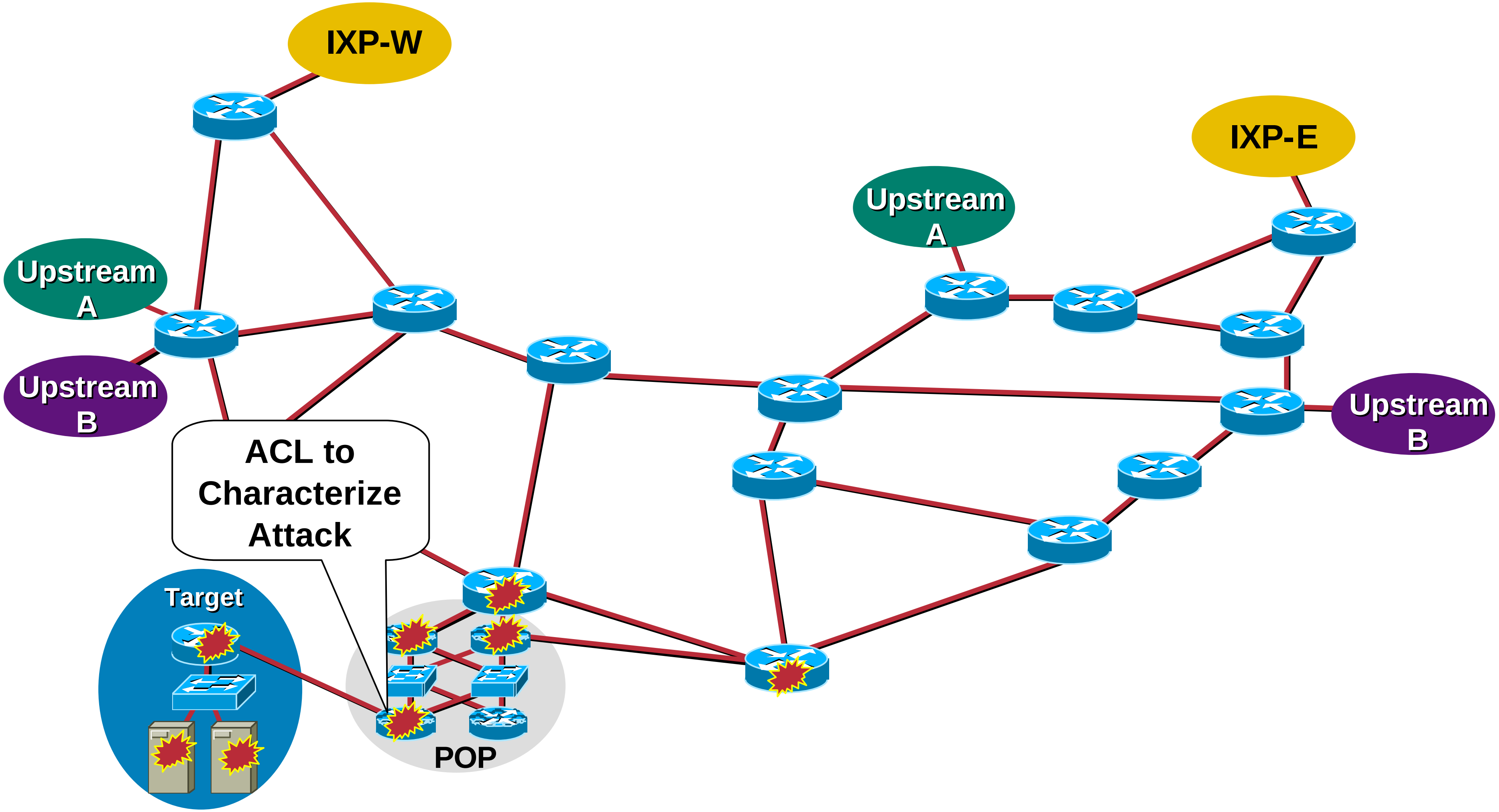

IXP-W
IXP-E
Upstream A
Upstream B
Upstream A
Upstream B
Target
POP

Step 1 – Classifying the Attack

- **Use ACL to find out the characteristics of the attack**

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any range 0 65535
access-list 169 permit ip any any
interface serial 0
ip access-group 169 out
```

Step 1 – Classifying the Attack



ACL to Characterize Attack

Step 1 – Classifying the Attack

- **Use the show access-list 169 to see which protocol is the source of the attack:**

```
Extended IP access list 169
        permit icmp any any echo (2 matches)
        permit icmp any any echo-reply (21374 matches)
        permit udp any any eq echo
        permit udp any eq echo any
        permit tcp any any established (150 matches)
        permit tcp any any (15 matches)
        permit ip any any (45 matches)
```

Step 2 – Capture a Source IP

- Tracing spoofed source IP addresses is a challenge
- Tracing needs to happen hop by hop
- The first step is to use the ACL “log-input” function to grab a few packets
- Quick in and out is needed to keep the router from overloading with logging interrupts to the CPU

Step 2 – Capture a Source IP

- Preparation

  Make sure your logging buffer on the router is large

  Create the ACL

  Turn off any notices/logging messages to the console or vty (so you can type the command *no access-group 170)*

Step 2 – Capture a Source IP

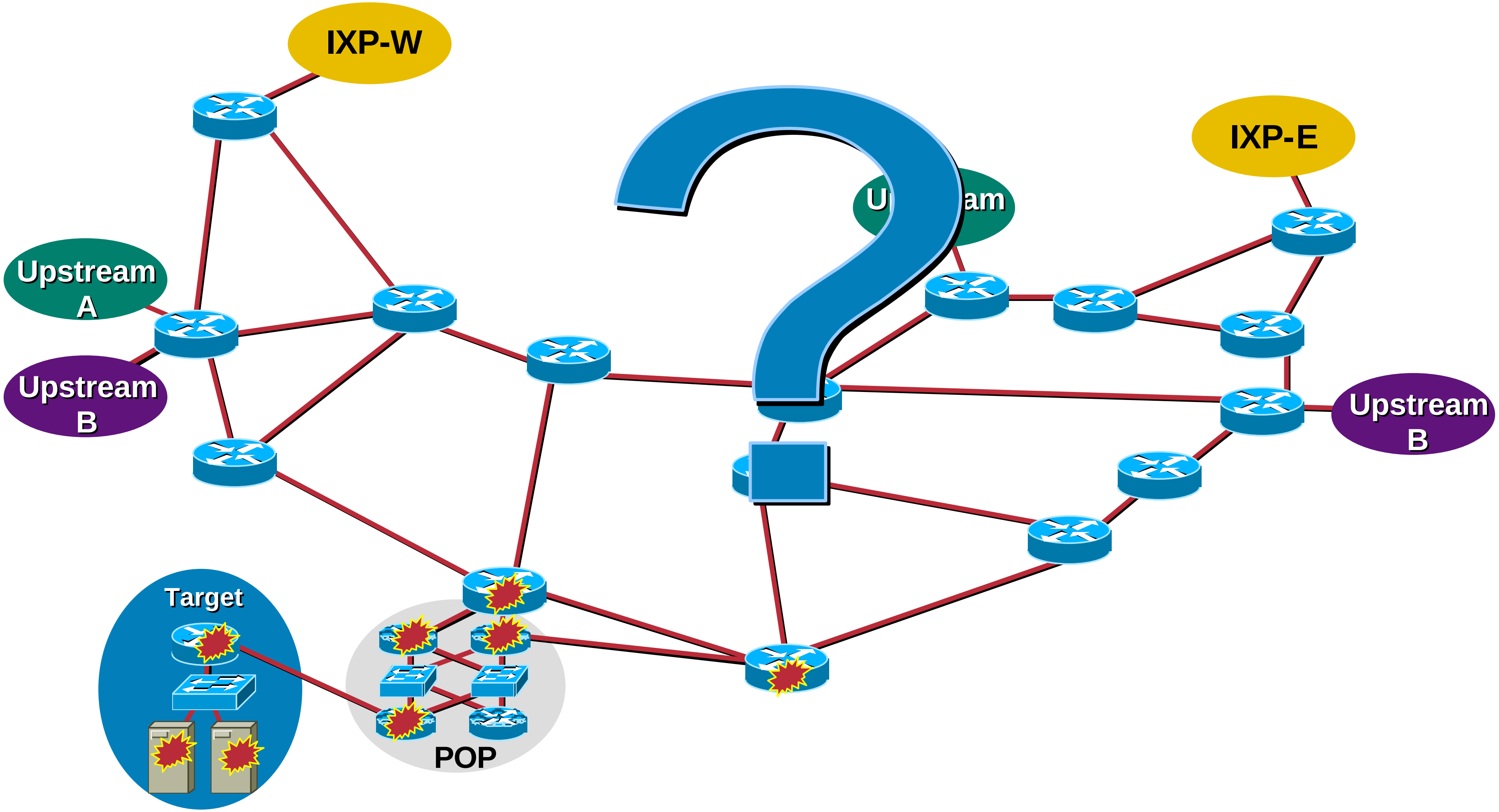
```
 access-list 170 permit icmp any any echo
 access-list 170 permit icmp any any echo-reply log-input
 access-list 170 permit udp any any eq echo
 access-list 170 permit udp any eq echo any
 access-list 170 permit tcp any any established
 access-list 170 permit tcp any any
 access-list 170 permit ip any any

 interface serial 0
   ip access-group 170 out
! Wait a short time - (i.e 10 seconds)
   no ip access-group 170 out
```

Step 2 – Capture a Source IP

- Validate the capture with *show access-list 170*; make sure it the packets we counted
- Check the log with *show logging* for addresses:

```
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.212.72
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.154
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.15
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.142
(Serial0 *HDLC*) -> 198.133.219.25  (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.47
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet
```

Step 3 – Tracing the Source

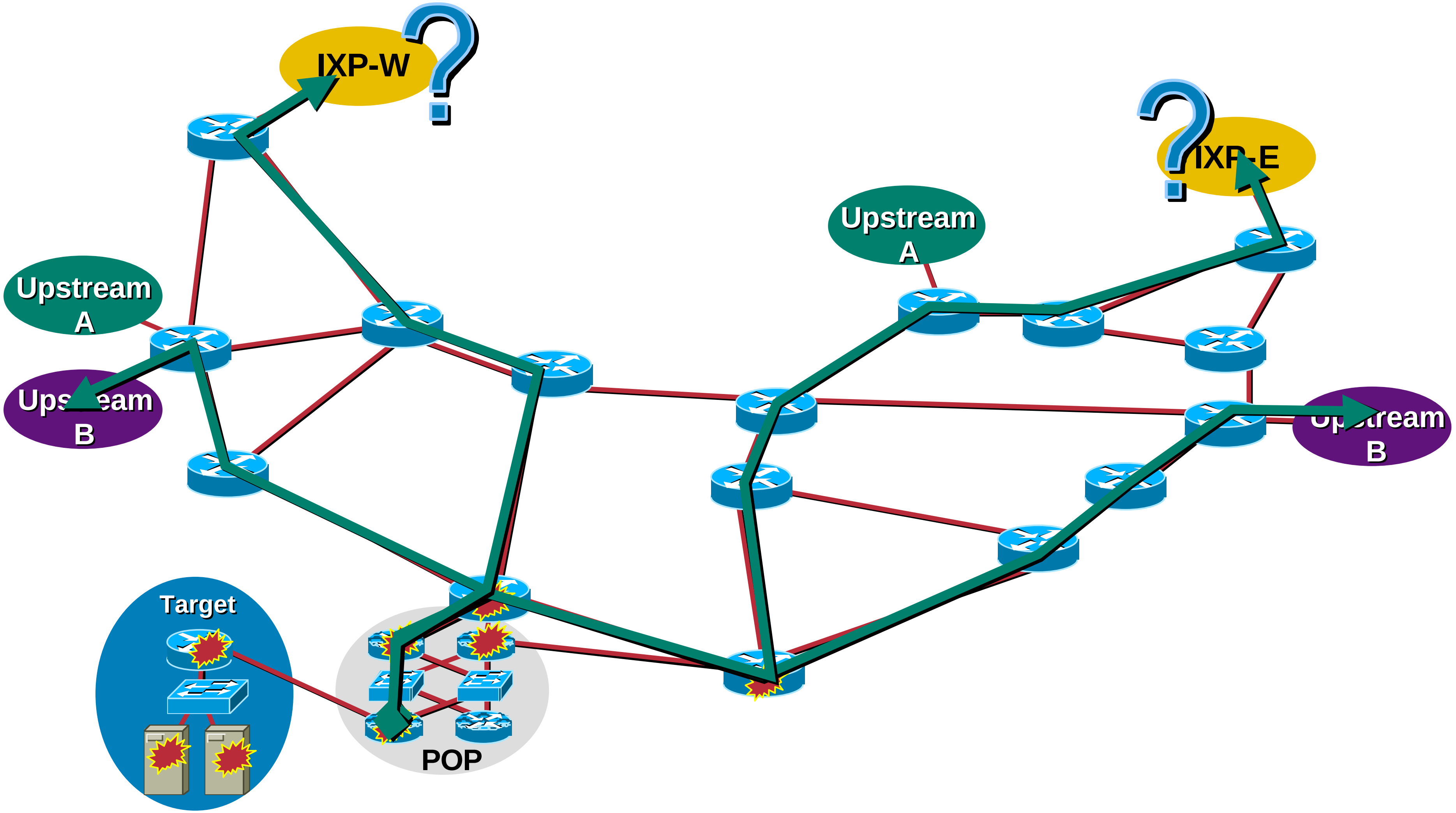


Step 3 – Tracing the Source

- Using Netflow for hop-by-hop traceback:

```
Beta-7200-2>sh ip cache 198.133.219.0 255.255.255.0 verbose flow
IP packet size distribution (17093 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .735 .088 .054 .000 .000 .008 .046 .054 .000 .009 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 1257536 bytes
  3 active, 15549 inactive, 12992 added
  210043 ager polls, 0 flow alloc failures
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          35      0.0        80    41      0.0      14.5      12.7
UDP-DNS             20      0.0         1    67      0.0       0.0      15.3
UDP-NTP           1223      0.0         1    76      0.0       0.0      15.5
UDP-other        11709      0.0         1    87      0.0       0.1      15.5
ICMP                 2      0.0         1    56      0.0       0.0      15.2
Total:           12989      0.0         1    78      0.0       0.1      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa1/1         192.168.45.142  POS1/0        198.133.219.25  11 008A 008A     1
Fa1/1         192.168.45.113  POS1/0        198.133.219.25  11 0208 0208     1
Fa1/1         172.16.132.154  POS1/0        198.133.219.25  06 701D 0017    63
```

Step 3 – Tracing the Source

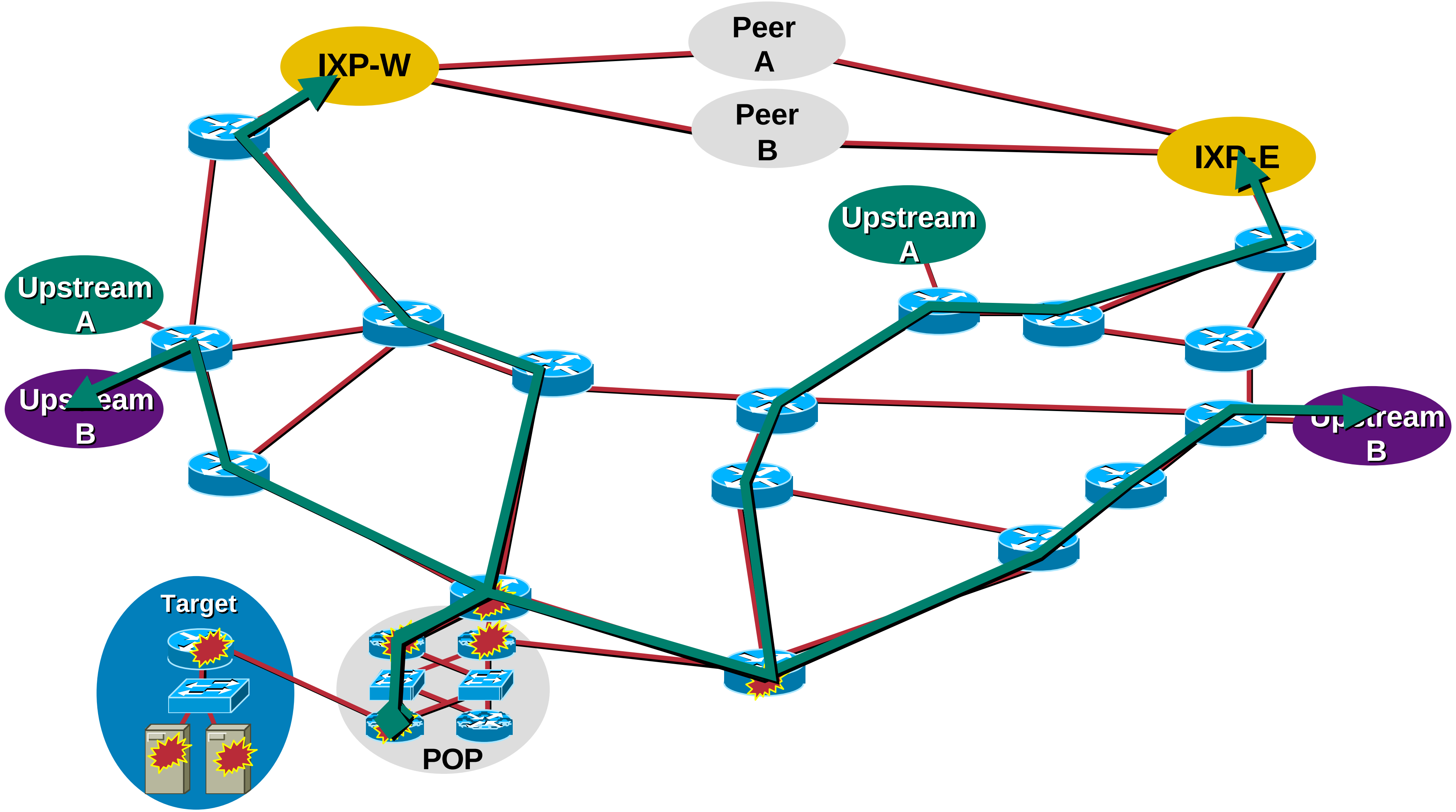


Step 3 – Tracing the Source

- **Tracing across a shared access medium (I.e. like IXPs) require that ACL technique**

```
May 23 4:30:04.379: %SEC-6-IPACCESSLOGP: list 170 permitted
   icmp 192.168.45.142(0)(FastEthernet3/0/0 00d0.bc83.58a0)
   -> 198.133.219.25 (0), 1 packet

May 23 4:30:05.379: %SEC-6-IPACCESSLOGP: list 170 permitted
   icmp 192.168.45.142(0)(FastEthernet3/0/0 00d0.bc83.58a0)
   -> 198.133.219.25 (0), 1 packet

May 23 4:30:06.379: %SEC-6-IPACCESSLOGP: list 170 permitted
   icmp 192.168.45.142 (0)(FastEthernet3/0/0 00d0.bc83.58a0)
   -> 198.133.219.25 (0), 1 packet
```

Step 3 – Tracing the Source



Troubleshooting Split

- **Split in the security reaction team’s flow:**

  One team starts calling NOCs

    Upstream 2, Peer A, and Peer B

  Other team drops filters in to push the packet drops to the edge of the network

Step 4 – Pushing the Packet Drops to the Edge

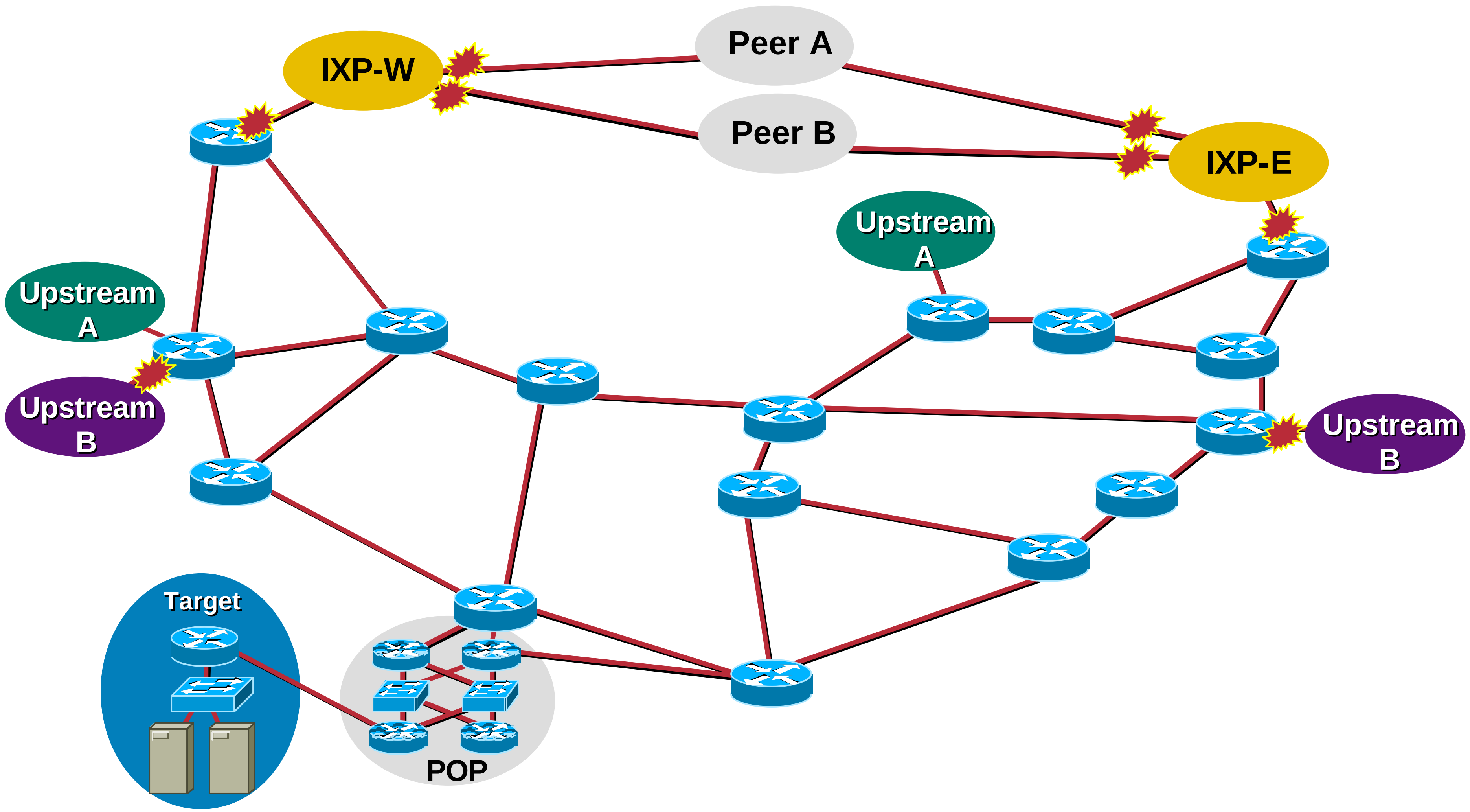
- Options:
  - Rate limit the attack with CAR (input feature)
  - ACL to drop the packets
  - uRPF (perhaps)
  - Drop the connection to the peer/upstream

Step 4 – Pushing the Packet Drops to the Edge

- **Select rate limiting option; limit ICMP echo-reply for everyone and limit the peer’s traffic**

```
interface FastEthernet3/0/0

  rate-limit output access-group 2020 256000 16000
24000 conform-action transmit exceed-action drop

  rate-limit input access-group rate-limit 100 8000000
64000 80000 conform-action transmit exceed-action drop

!

access-list 2020 permit icmp any any echo-reply

access-list rate-limit 100 00d0.bc83.58a0
```

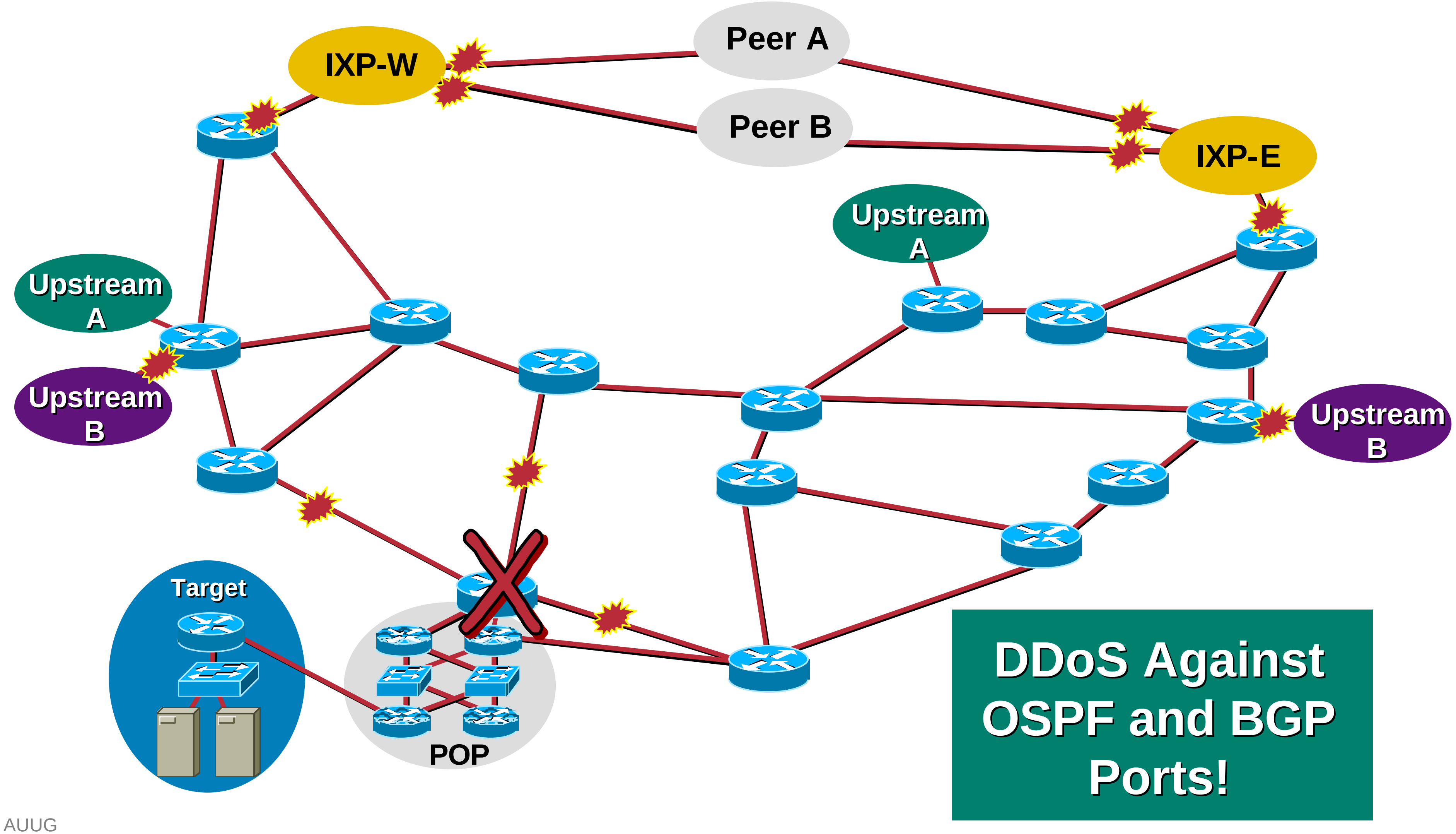
Step 4 – Pushing the Packet Drops to the Edge



Check Point

- SitRep—attack still in progress—packets being dropped at the ISP edge
- Work with upstream and peer ISP NOCs to continue the trace back to the sources
- Collect evidence—work with customer and call your legal team

Alert!



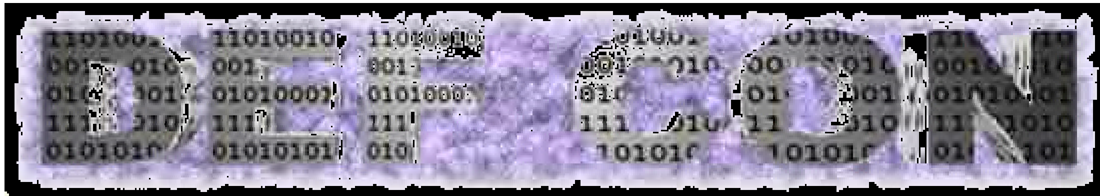
DDoS Against OSPF and BGP Ports!

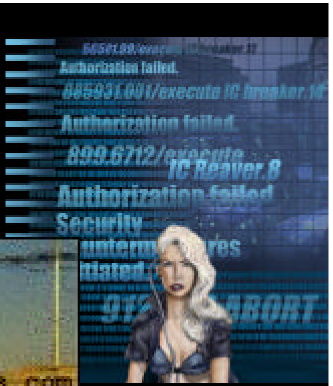
Next Phase of the Attack

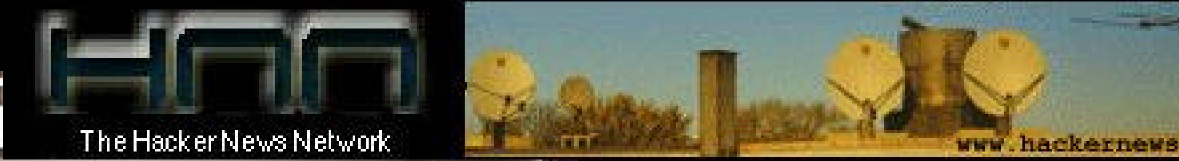
- The attackers have shifted the attack to their target's infrastructure

    ISPs and IXPs have and will be directly attacked to get at the target!

    ISP's routers are being directly attacked to take out the target



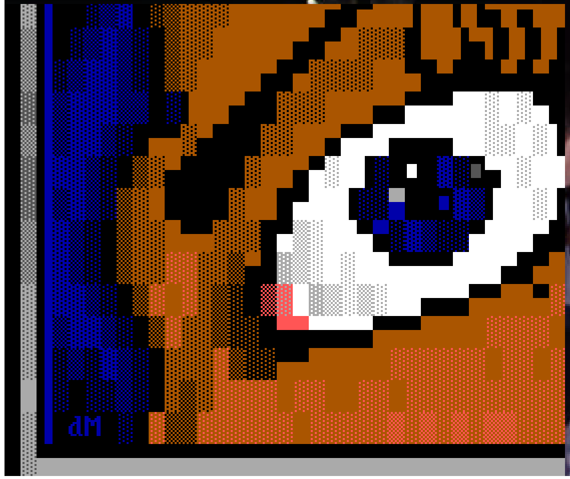




Are

You

Ready?



In Case You Wondering…

- How to work a DoS attack against the routing protocol?

  Out of band access to the router!

  Rate limits on traffic to the routing protocol

  ACLs to block outside traffic to the routing protocol ports

DDoS Links

- http://www.denialinfo.com/
- http://www.staff.washington.edu/dittrich
- http://www.sans.org/y2k/DDoS.htm
- http://www.nanog.org/mtg-9910/robert.html
- http://cve.mitre.org/
- http://packetstorm.securify.com/distributed/

Router Security Summary

- Tutorial has covered

  Securing the Router

  Securing the Routing Protocols

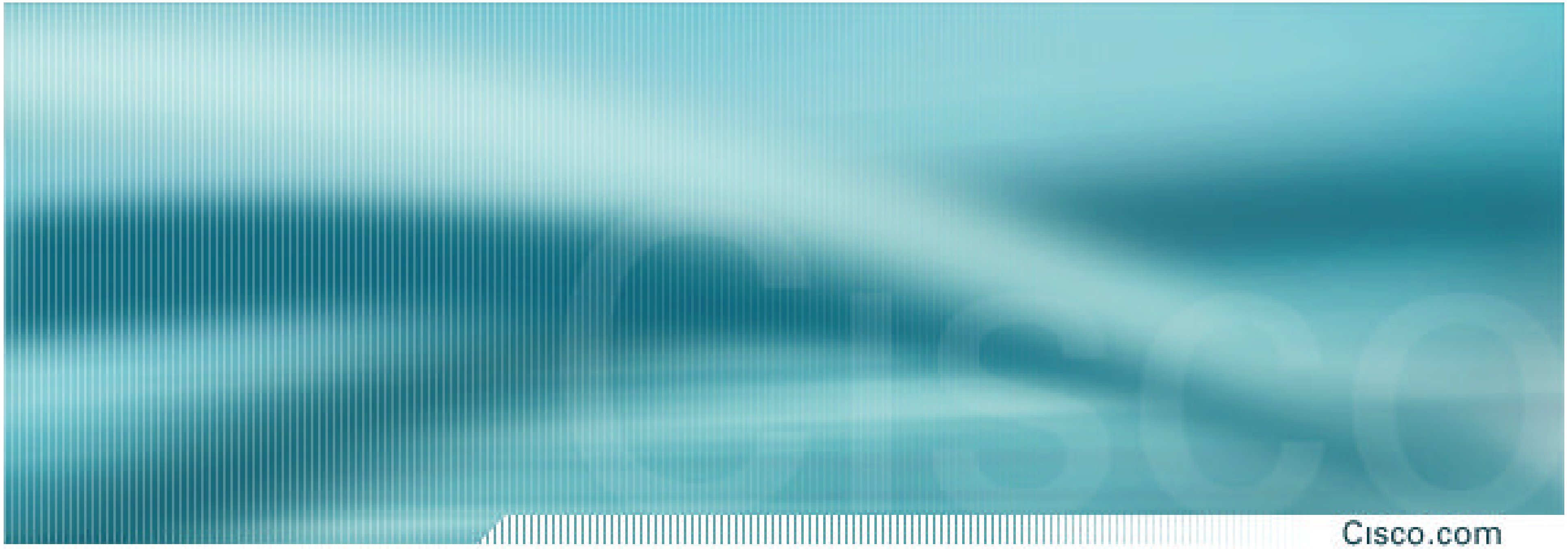
  Securing the Network

  Administrative and Operational Practices

  Unicast Reverse Path Forwarding

  Recent DOS attacks and the defence

  Tracking DoS/DDOS Attacks through an ISP's Network



Router Security

End of Tutorial