Infrastructure Security and Protection

Gaurab Raj Upadhaya, Limelight Networks

Yusuf Bhaiji, Cisco Systems

Agenda

- Introduction to Core Security
  - Denial of Service (DoS) and Worm Review
  - Six-Phase Methodology
- Infrastructure Security
  - RFC 2827/BCP 38
  - Infrastructure ACLs
  - Flexible Packet Matching
- Network Telemetry
  - SNMP, RMON and Their Ilk
  - NetFlow for Security Purposes

Agenda (Cont.)

- Traceback Techniques
  - NetFlow Traceback Techniques
  - Attract and Analyze: Sinkholes
- Reacting to Attacks
  - Reacting with ACL
  - Reacting with BGP

Simple Methodology

- Simple methodology—expanding the scope
  - Best practices to:
    - Protect the device
    - Protect the infrastructure
- With a solid foundation in place, we turn our attention to leveraging the network itself as a security toolkit

Denial of Service (DoS) and Worm Review

What Is Core Security?

- Often thought of as “SP Security”
  - What is an SP today?
- Internal networks are no longer truly internal
  - Tunneling
  - VPN
  - Worms, worms, worms
- The infrastructure is critical; if we can’t protect it, nothing else matters
  - Edge security initiatives abound: NAC, 802.1X, HIPS (CSA), personal firewalls, etc.

Denial of Service Attacks

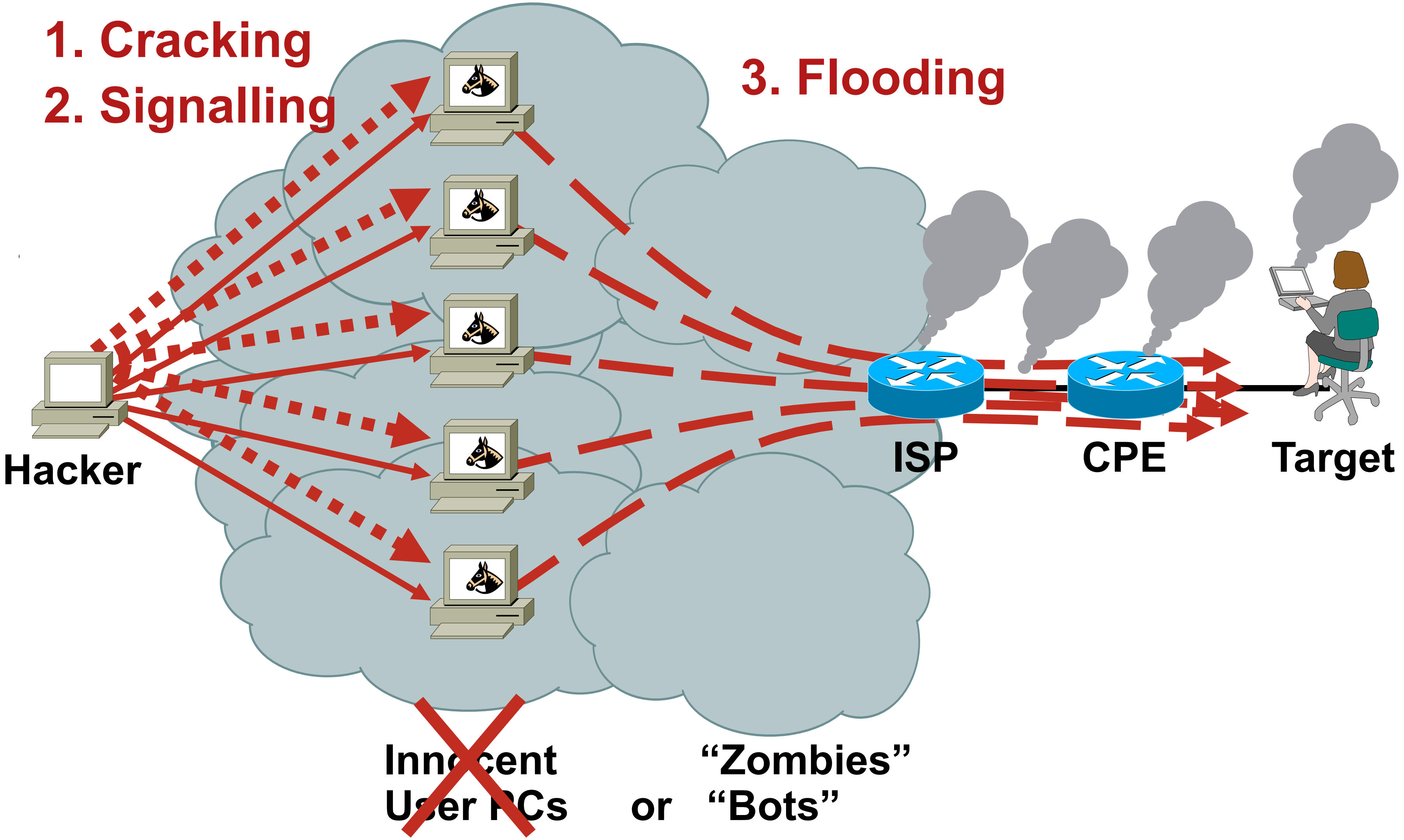
- We understand intrusions (patch, patch, patch ;-))
- What about DoS? Do “the right things” and still suffer
- The vast majority of modern DoS attacks are distributed

  DDos IS DoS
- DoS is often driven by financial motivation

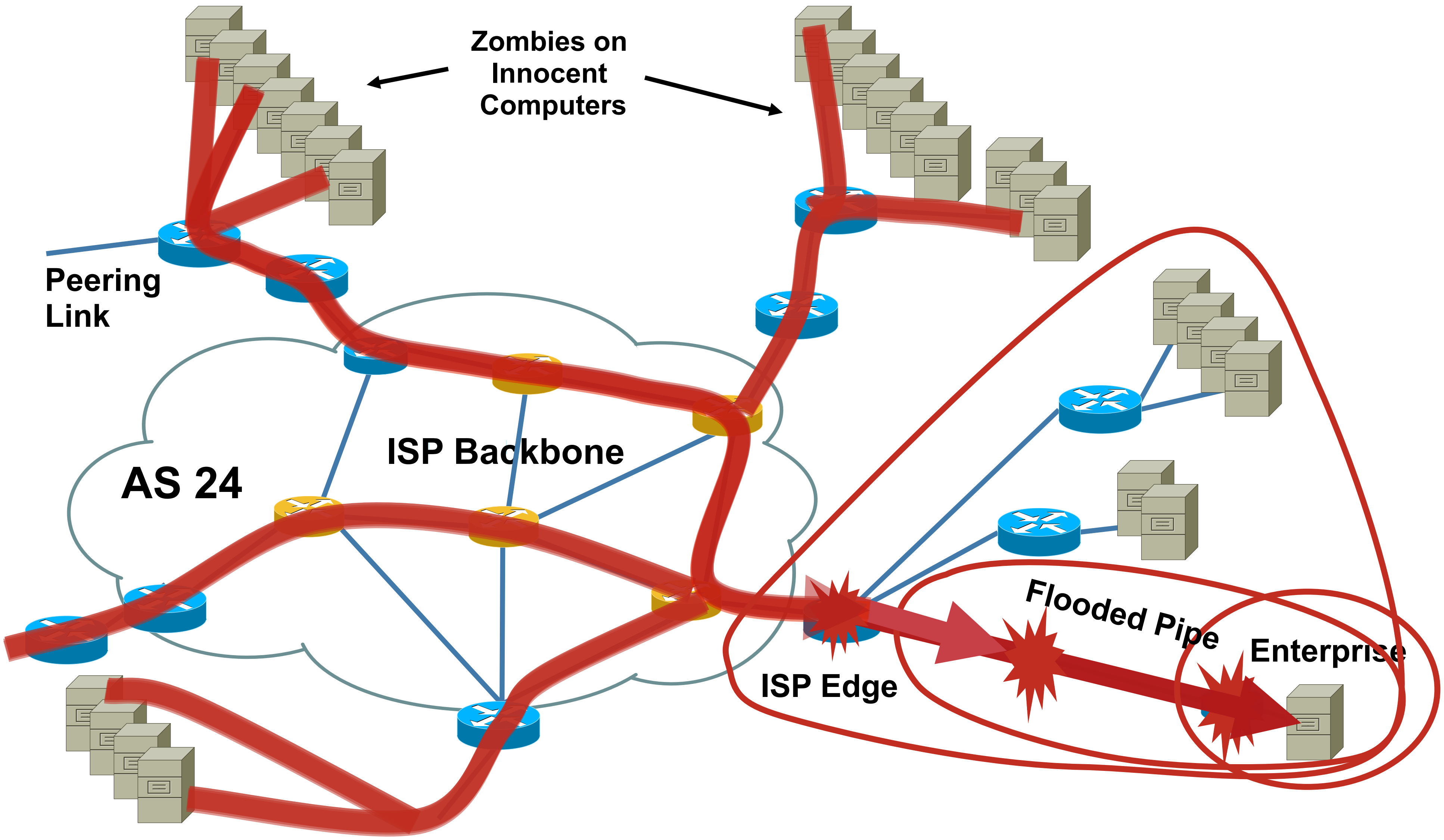
  DoS for hire :-(

  Economically-driven miscreant community
- DoS cannot be ignored; your business depends on effective handling of attacks

DoS: The Procedure



An SP View: Denial of Service



Denial of Service Trends

- Multipath
  - Truly distributed
  - DNS servers, large botnets
- Multivector
  - SYN AND UDP AND…
- Use of non-TCP/UDP/ICMP protocols
  - Get past ACLs
  - Increased awareness in community
- Financial incentive
  - SPAM, DoS-for-hire
  - Large, thriving business
  - Forces us to reassess the risk profile

Infrastructure Attacks

- Infrastructure attacks increasing in volume and sophistication

  Sites with Cisco documents and presentations on routing protocols (and I don’t mean Cisco.com)

  Presentations about routers, routing and Cisco IOS® vulnerabilities at conferences like Blackhat, Defcon and Hivercon

  Router attack tools and training are being published

- Why mount high-traffic DDoS attacks when you can take out your target’s gateway routers?
- Hijacked routers valuable in spam world, which has a profit driver
- Router compromise (0wn3d) due to weak password

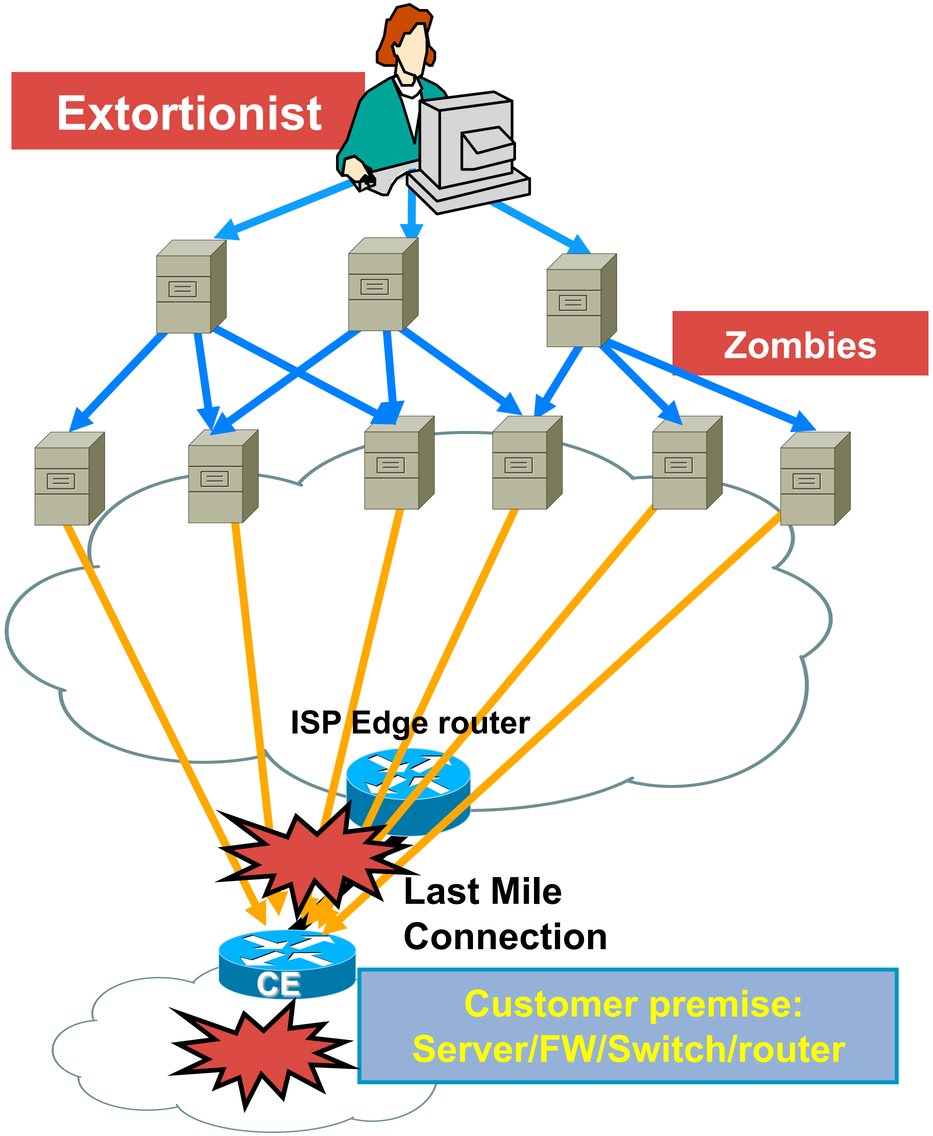
From Bad to Worms

- Worms have emerged as the new security reality
- Old worms never die
  - Millions of UPnP and Slammer packets still captured daily
- Most worms are intended to compromise hosts
- Worm propagation is dependant on network availability
- Worms and DoS are closely related
  - Secondary worm effects can lead to denial of service
  - Worms enable DoS by compromising hosts → BOTnets
- Perimeters are crumbling under the worm onslaught (VPN/mobile workers, partners, etc.)

Worms and the Infrastructure

- Worms typically infect end-stations
- To date, worms have not targeted infrastructure but secondary effects have wreaked havoc
  - Increased traffic
  - Random scanning for destination
  - Destination address is multicast
  - TTL and other header variances
- At the core SP level, the aggregate affects of a worm can be substantial
- Worm severity is escalating and evolving

Botnets Make DDoS Attacks Easy



- Botnets for Rent!
- A "Botnet" is a group of compromised computers on which extortionists have installed special programs (zombies) that can be directed to launch DoS attacks against a specific target.

  Botnets are triggered from a "central controller"

  Botnets allow for all the types of DDOS attacks: ICMP Attacks, TCP Attacks, UDP Attacks, HTTP overload

  Options for deploying Botnets are extensive and new tools are created to exploit the latest system vulnerabilities
- A relatively small Botnet can cause a great deal of damage.

  1000 home PCs with an average upstream bandwidth of 128KBit/s can offer more than 100MBit/s against a target
- The size of the attacks are ever increasing and independent of last mile bandwidth

How Do You Respond?

With Money Being the Key Driver of Miscreant Activity, Large Network Operators Need to Respond

- BCP deployment
- Execution of a broad and deep security toolkit
- Rethink some network/service architectures
- Create, staff, and train an operational security (OPSEC) team
- Practice, practice, practice

Six-Phase Methodology

Six Phases of Incident Response

Preparation

Prep the network
Create tools
Test tools
Prep procedures
Train team
Practice
Baseline your traffic

Identification

How do you know about the attack?
What tools can you use?
What's your process for communication?

Classification

What kind of attack is it?

Traceback

Where is the attack coming from?
Where and how is it affecting the network?

Reaction

What options do you have to remedy?
Which option is the best under the circumstances?

Post Mortem

What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

Preparation

Preparation—Develop and Deploy a
Solid Security Foundation

- Includes technical and non-technical components
- Encompasses best practices
- The hardest, yet most important phase
- Without adequate preparation, you are destined to fail
- The midst of a large attack is not the time to be implementing foundational best practices and processes

Preparation

- Know the enemy

  Understand what drives the miscreants

  Understand their techniques

- Create the security team and plan

  Who handles security during an event?
  Is it the security folks? The networking folks?

- Harden the devices

- Prepare the tools

  Network telemetry

  Reaction tools

  Understand performance characteristics

Identification

Identification—How Do You Know You
or Your Customer Is Under Attack?

- It is more than just waiting for your customers to scream or your network to crash
- What tools are available?
- What can you do today on a tight budget?

Identification—Ways to Detect

- Customer call
  - “The Internet is down”
- Unexplained changes in network baseline
  - SNMP: line/CPU overload, drops
  - Bandwidth
  - NetFlow
- ACLs with logging
- Backscatter
- Packet capture
- Network IPS
- Anomaly detection

Identification—Network Baselines

- NMS baselines
- Unexplained changes in link utilization

  Worms can generate a lot of traffic, sudden changes in link utilization can indicate a worm

- Unexplained changes in CPU utilization

  Worm scans can affect routers/switches resulting in increased CPU - process and interrupt switched traffic

- Unexplained syslog entries
- These are examples

  Changes don’t always indicate a security event

  Must know what’s normal in order to identify abnormal behavior

Classification

- Classification—understand the details and scope of the attack
  - Identification is not sufficient; once an attack is identified, details matter
  - Guides subsequent actions
- Identification and classification are often simultaneous

Classification

- Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router)
  - What type of attack has been identified?
  - What's the effect of the attack on the victim(s)?
  - What next steps are required (if any)?
- At the very least:
  - Source and destination address
  - Protocol information
  - Port information

Traceback

- Traceback—what are the sources of the attack?
  - How to trace to network ingress points
  - Your Internet connection is not the only vector
  - Understand your topology
- Traceback to network perimeter
  - NetFlow
  - Backscatter
  - Packet accounting

Traceback

- Retain attack data
  - Use to correlate interdomain traceback
  - Required for prosecution
  - Deters future attacks
  - Clarify billing and other disputes
  - Post mortem analysis

Reaction

Reaction—Do Something to Counter the Attack

- Should you mitigate the attack?

  Where? How?

- No reaction is a valid form of reaction in certain circumstances
- Reaction often entails more than just throwing an ACL onto a router

Post Mortem

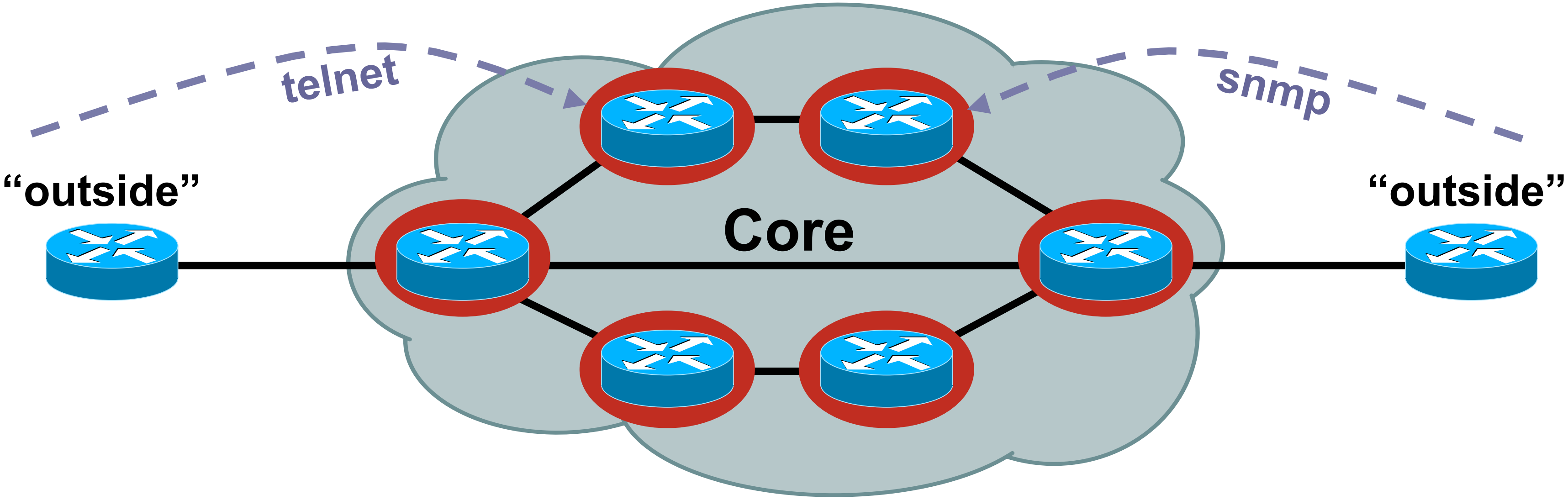
Post Mortem—Analyze the Event

- The step everyone forgets
- What worked? What didn’t? How can we improve?
- Protect against repeat occurrences?
- Was the DoS attack you handled the real threat? Or was it a smoke screen for something else that just happened?
- What can you do to make it faster, easier, less painful in the future?
- Metrics are important

  Resources, headcount, etc.

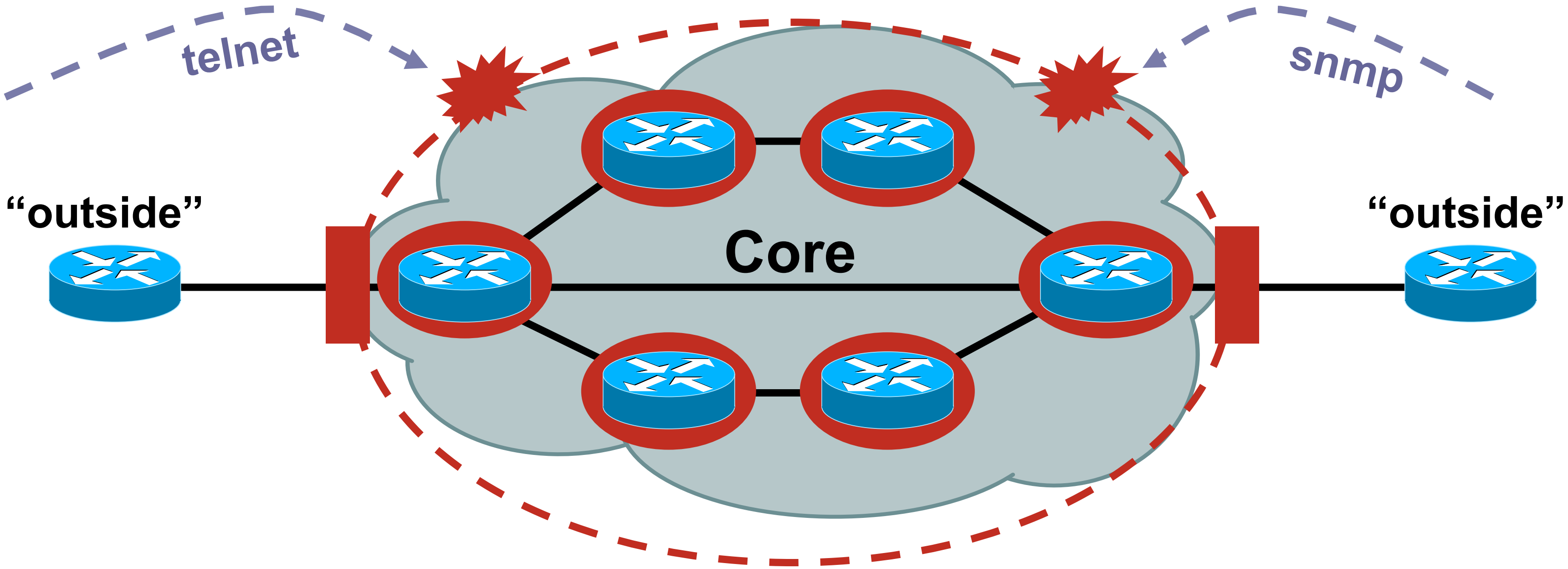
Infrastructure Security

The Old World



- Core routers individually secured
- Every router accessible from outside

The New World



- Core routers individually secured plus
- Infrastructure protection
- Routers generally not accessible from outside

RFC 2827/BCP 38

RFC 2827/BCP 38 Ingress Packet Filtering

- Packets should be sourced from valid, allocated address space, consistent with the topology and space allocation

Internet Connectivity Guidelines for BCP38

- Networks connecting to the Internet

  Must use inbound and outbound packet filters to protect the network

- Configuration example

  Outbound—only allow my network source addresses out

  Inbound—only allow specific ports to specific destinations in

BCP 38: Consequences of No Action

No BCP 38 Means That:

- Devices can (wittingly or unwittingly) send traffic with spoofed and/or randomly changing source addresses out to the network
- Complicates traceback immensely
- Sending bogus traffic is not free

BCP 38 Packet Filtering Principles

- Filter as close to the edge as possible
- Filter as precisely as possible
- Filter both source and destination where possible

Techniques for BCP 38 Filtering

- Static ACLs on the edge of the network
- Dynamic ACLs with AAA profiles
- **Unicast RPF strict mode**

Using ACLs to Enforce BCP38

- Static ACLs are the traditional method of ensuring that source addresses are not spoofed:
  - Permit all traffic whose source address equals the allocation block
  - Deny any other packet
- Principles:
  - Filter as close to the edge as possible
  - Filter as precisely as possible
  - Filter both source and destination where possible

BCP ACL Guidelines

- ISPs

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

- Customer end-sites

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

  First line of defense - never assume your ISP will do it

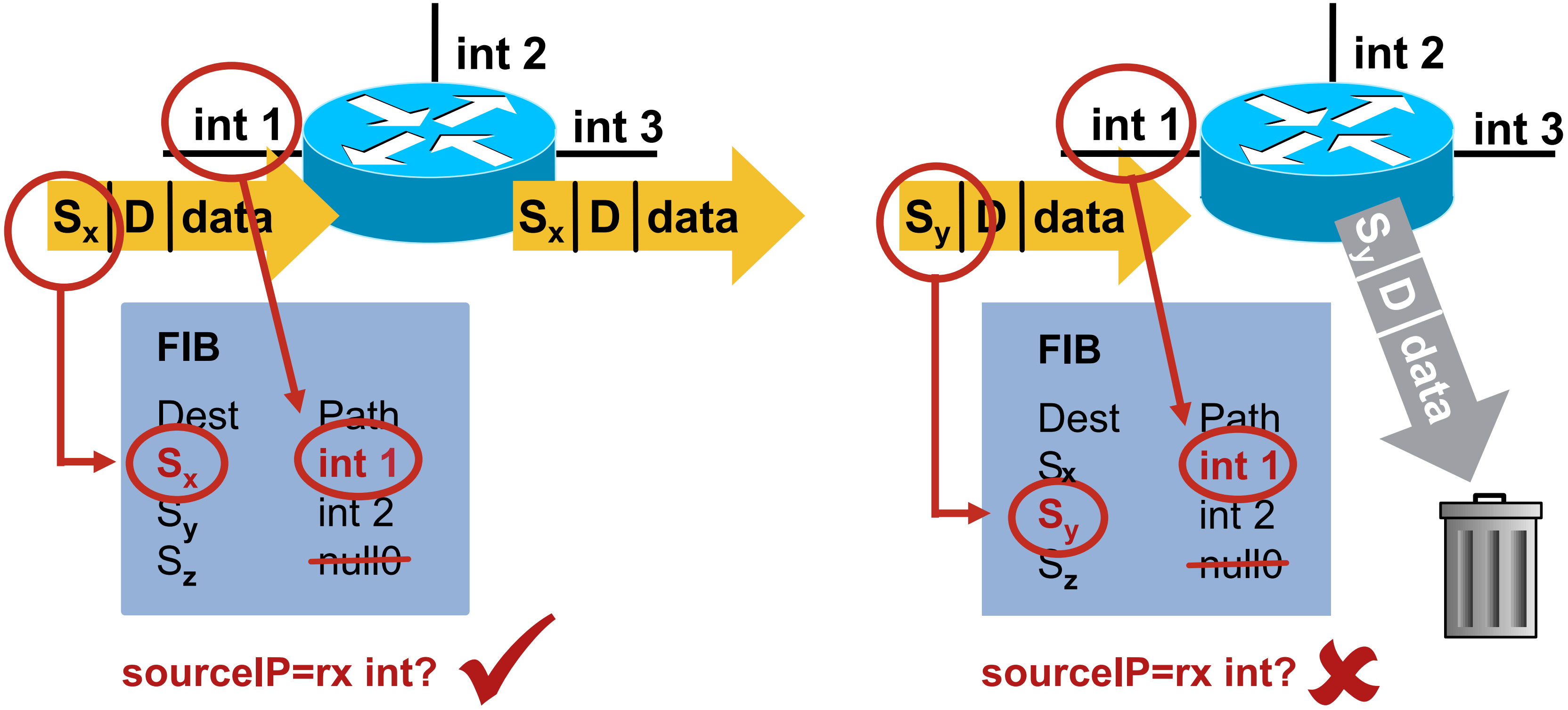
Unicast Reverse Path Forwarding (uRPF)

- CEF is required
- The purported source of ingress IP packets is checked to ensure that the route back to the source is “valid”
- Two flavors of uRPF:
    - Strict mode uRPF
    - Loose mode uRPF

uRPF—Strict Mode

router(config-if)# ip verify unicast source reachable-via rx

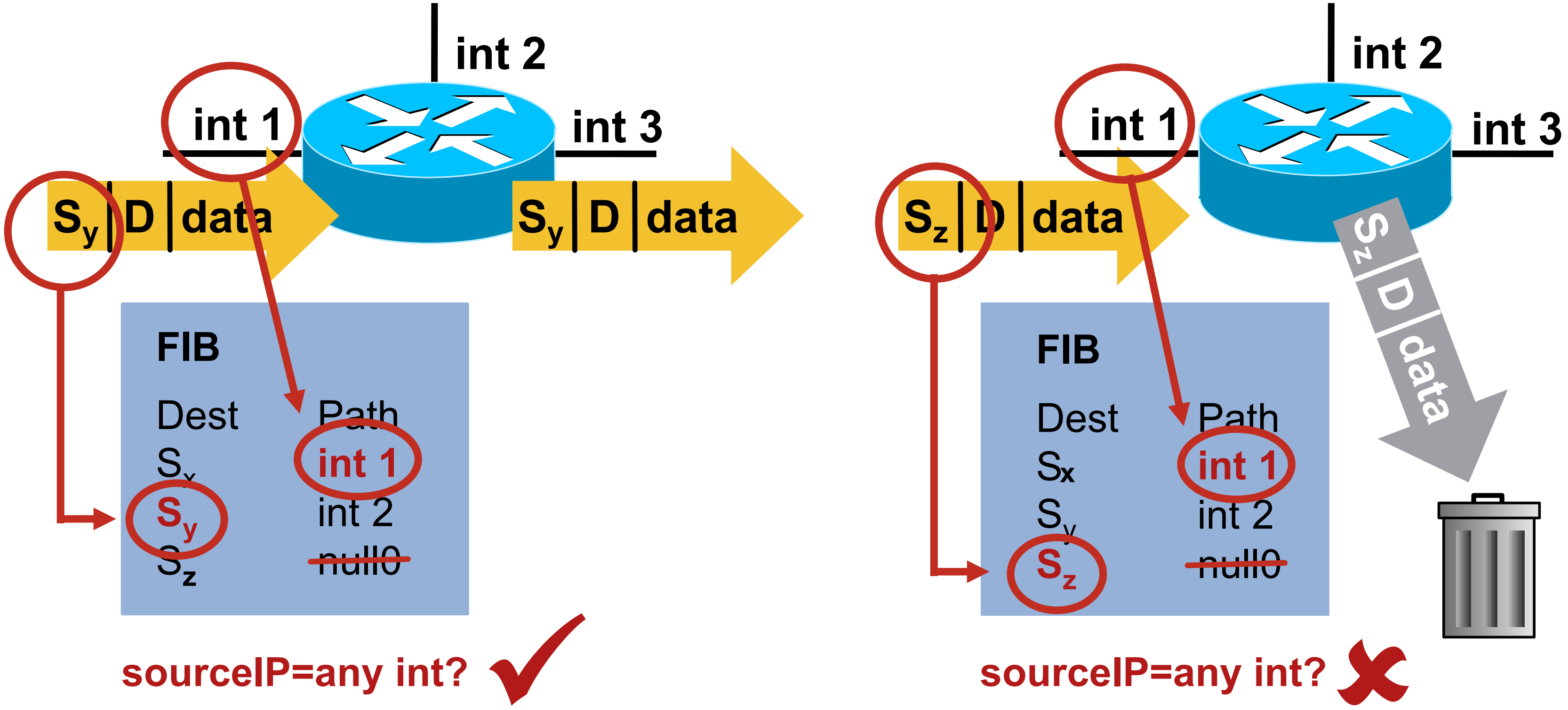
(deprecated syntax: ip verify unicast reverse-path)



IP Verify Unicast Source Reachable—Via rx

uRPF—Loose Mode

```
router(config-if)# ip verify unicast source reachable-via any
```



FIB

Dest	Path
S_x	int 1
S_y	int 2
S_z	~~null0~~

sourceIP=any int? ✓

FIB

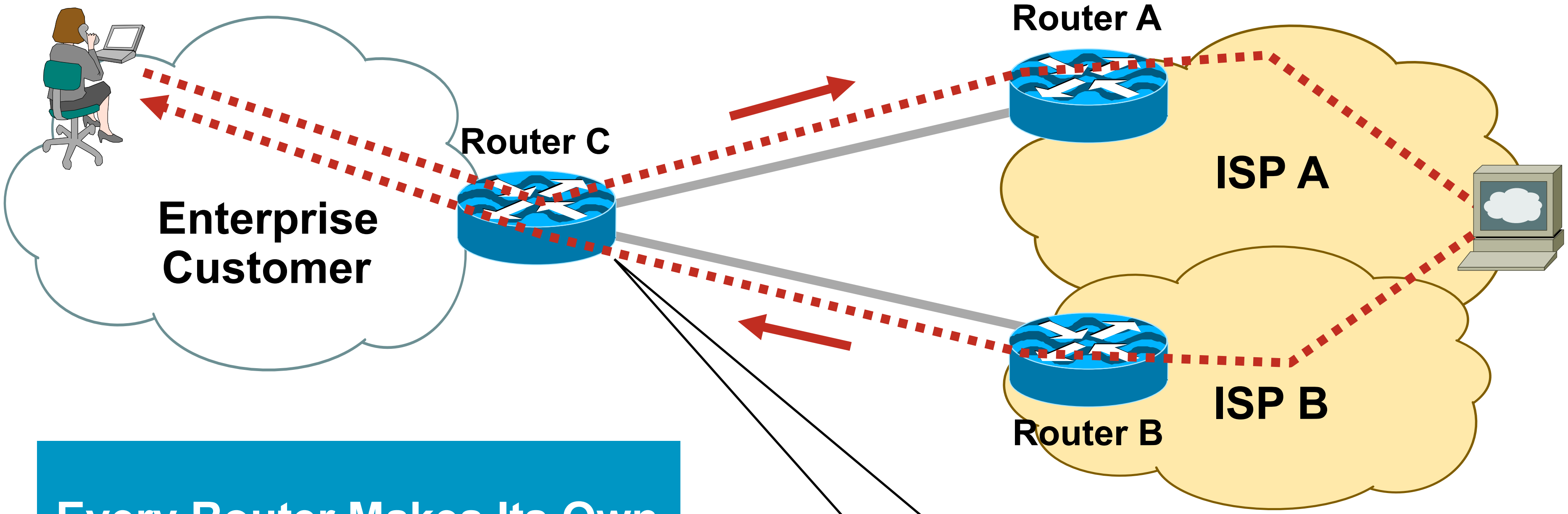
Dest	Path
S_x	int 1
S_y	int 2
S_z	~~null0~~

sourceIP=any int? ✗

IP Verify Unicast Source Reachable—Via any

uRPF and Multihomed Customers

What Is Asymmetrical Routing?



Every Router Makes Its Own Best Path Forwarding Decision—Resulting in Asymmetrical Routing

Strict uRPF on This i/f Will Drop Traffic from the Server

Strict uRPF and Asymmetric Routing

- Traffic originating from multihomed customers can be verified with uRPF
- Solution: make routing symmetric
- Details in ISP Essentials:

  ftp://ftp-eng.cisco.com/cons/isp/security
  (a must-read for all SP engineers)

- Loose vs. Strict uRPF reference:

  Unicast Reverse Path Forwarding Loose Mode

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00803fa70b.html

BCP 38 Filtering: Summary

- BCP 38 is an operational reality
  - It works, it is scalable
  - It is operationally deployable and maintainable
  - It works on a wide variety of equipment
  - Deployable in the vast majority of situations—
    no more excuses
- Take time to understand source address validation techniques, see which ones will work for you
- Find ways to gain operational confidence in the BCP 38 techniques
- BCP 84 lists specific filtering methods

SNMP, RMON and Their Ilk

Types of Network Telemetry

- SNMP
- NetFlow
- RMON
- BGP
- Syslog
- Packet capture
- Others

NetFlow for Security Purposes

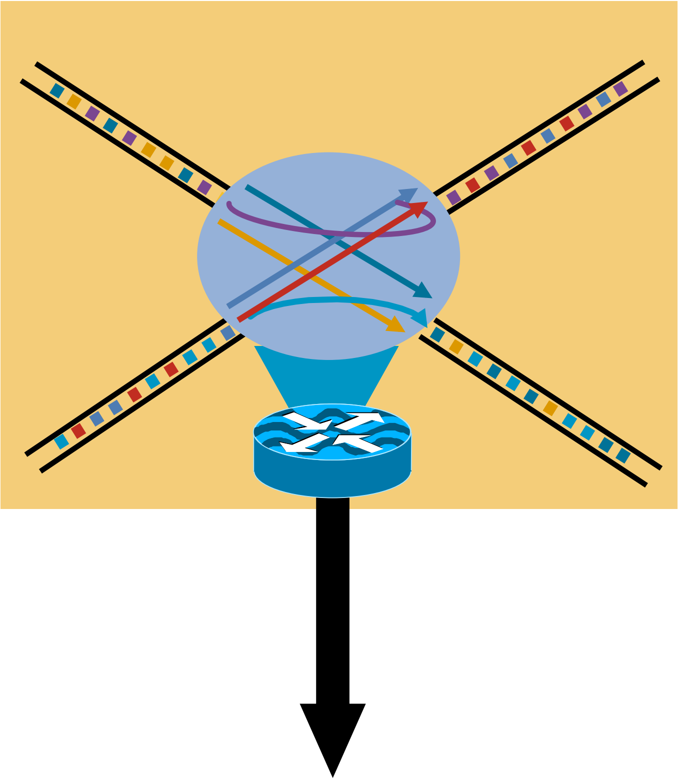
NetFlow Origination

- Developed by Darren Kerr and Barry Bruins at Cisco Systems in 1996
- Primary network accounting technology in the industry
- Emerging standard traffic engineering/capacity planning technology
- Primary network anomaly-detection technology
- Answers questions regarding IP traffic:
    - Who
    - What
    - Where
    - When
    - How
    - What cryptologists call “traffic analysis”

What Is a Flow?

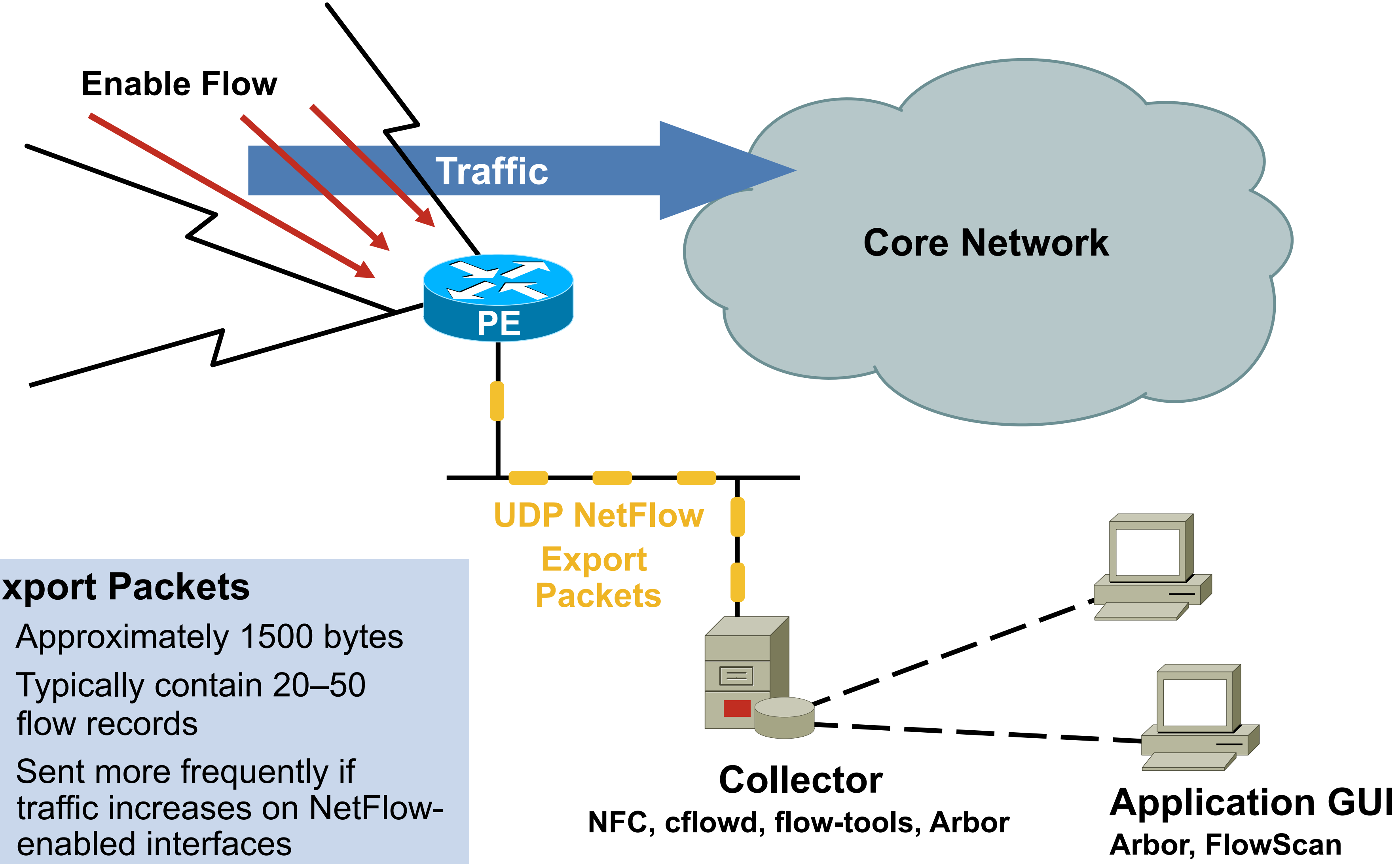
Defined by Seven Unique Keys:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (DSCP)
- Input logical interface (ifIndex)



Exported Data

Creating Export Packets



Export Packets

- Approximately 1500 bytes
- Typically contain 20–50 flow records
- Sent more frequently if traffic increases on NetFlow-enabled interfaces

Uses of NetFlow/sFLOW

Service Provider	Enterprise
Peering Arrangements SLA VPN User Reporting Usage-Based Billing DoS/Worm Detection Traffic Engineering Troubleshooting	Internet Access Monitoring (Protocol Distribution, Traffic Origin/ Destination) Associate Cost of IT to Departments More Scalable Than RMON DoS/Worm Detection Policy Compliance Monitoring Troubleshooting

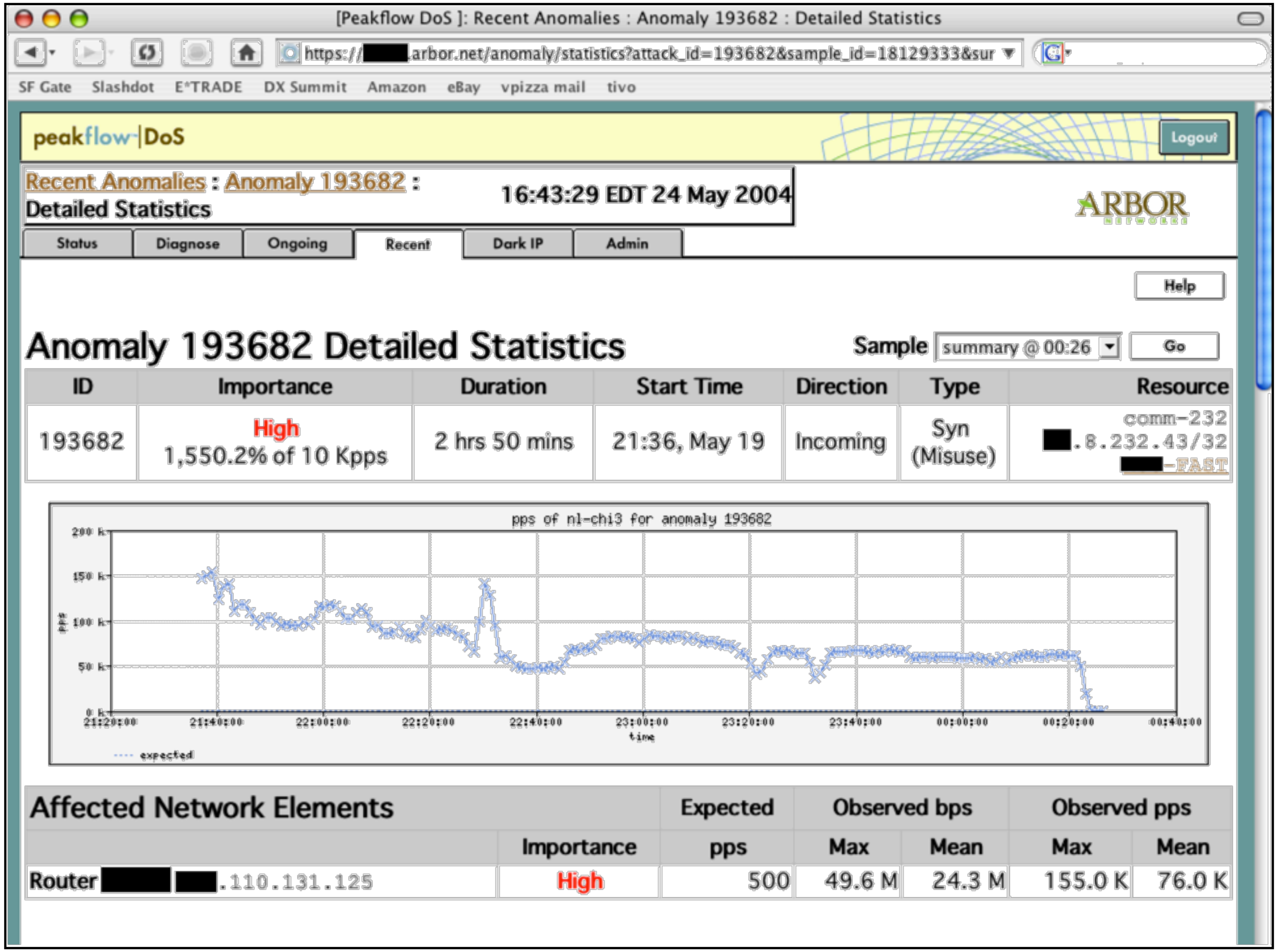
Key Concept: Scalability

- Packet capture is like a wiretap
- Flow is like a phone bill
- This level of granularity allows NetFlow to scale for very large amounts of traffic
- We can learn a lot from studying the phone bill
- Who's talking to whom, over what protocols and ports, for how long, at what speed, for what duration, etc.
- NetFlow is a form of telemetry pushed from the routers/ switches—each one can be a sensor

What Is an Anomaly?

- An event or condition in the network that is identified as a statistical abnormality when compared to typical traffic patterns gleaned from previously collected profiles and baselines

Anomaly Example: Detail


[Peakflow DoS]: Recent Anomalies : Anomaly 193682 : Detailed Statistics
https://[redacted].arbor.net/anomaly/statistics?attack_id=193682&sample_id=18129333&sur
SF Gate
Slashdot
E*TRADE
DX Summit
Amazon
eBay
vpizza mail
tivo
peakflow |DoS
Logout
ARBOR NETWORKS
Status
Diagnose
Ongoing
Recent
Dark IP
Admin
Help
Go

Recent Anomalies : Anomaly 193682 :
Detailed Statistics

16:43:29 EDT 24 May 2004

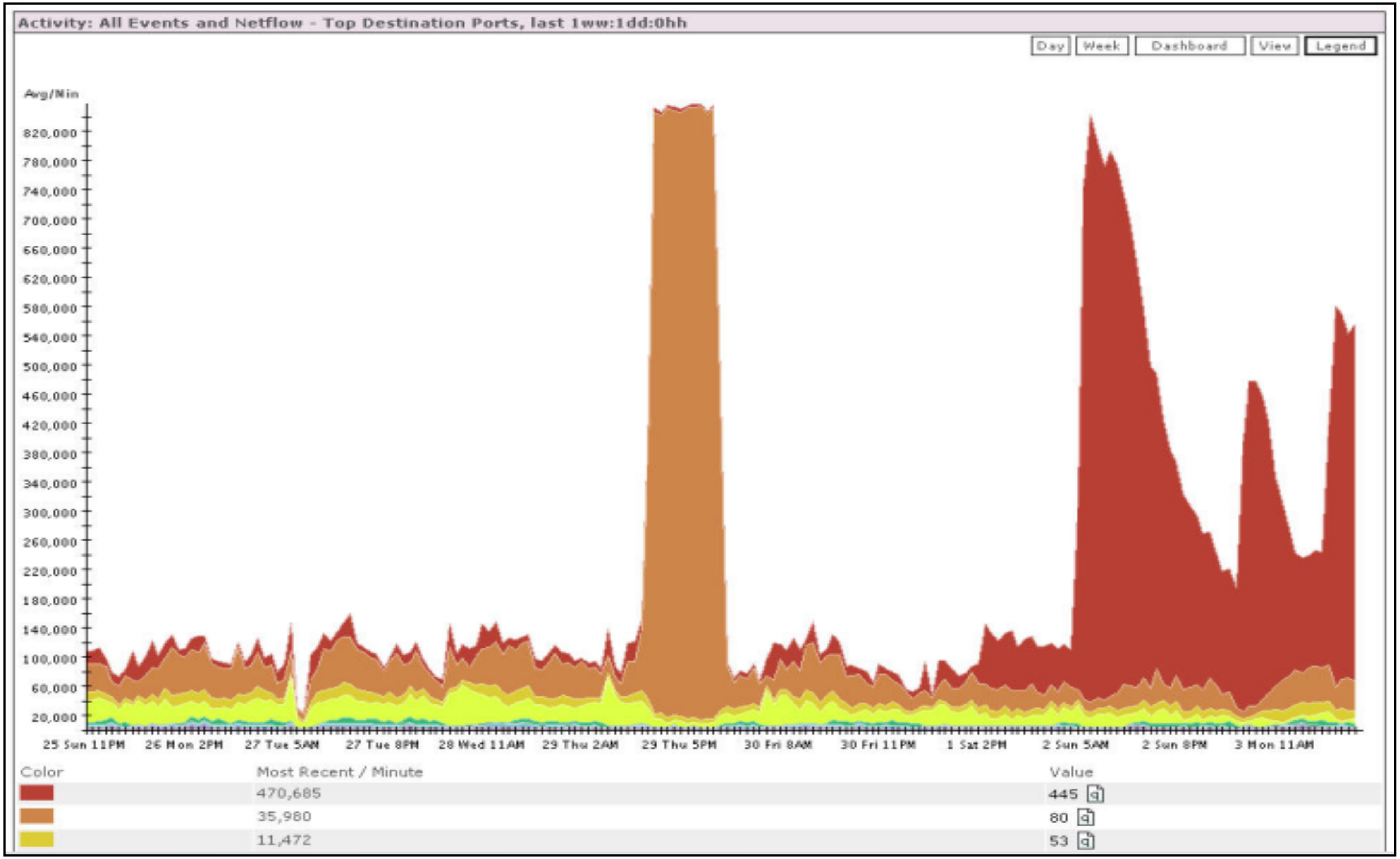
Anomaly 193682 Detailed Statistics

Sample summary @ 00:26

ID	Importance	Duration	Start Time	Direction	Type	Resource
193682	High 1,550.2% of 10 Kpps	2 hrs 50 mins	21:36, May 19	Incoming	Syn (Misuse)	comm-232 [redacted].8.232.43/32 [redacted]-FAST

Affected Network Elements		Expected	Observed bps		Observed pps	
	Importance	pps	Max	Mean	Max	Mean
Router [redacted] [redacted].110.131.125	High	500	49.6 M	24.3 M	155.0 K	76.0 K

Sasser Detection



Activity: All Events and Netflow - Top Destination Ports, last 1ww:1dd:0hh

Color	Most Recent / Minute	Value
🟥	470,685	445
🟧	35,980	80
🟨	11,472	53

Traceback Techniques

Traceback Essentials

- If source prefix is not spoofed:
  - Routing table
  - Internet Routing Registry (IRR)—whois
  - Direct site contact—ARIN, RIPE, APNIC
- If source prefix is spoofed:
  - Trace packet flow through the network
  - Find upstream connection
  - Upstream needs to continue tracing

Traceback Spoofed IPv4 Addresses

- Source: inside or outside?
- Once you have a fundamental understanding of the type of attack (source address and protocol type), you then need to trace to the ingress point
- Two main techniques:
  - Hop-by-hop
  - Jump to ingress

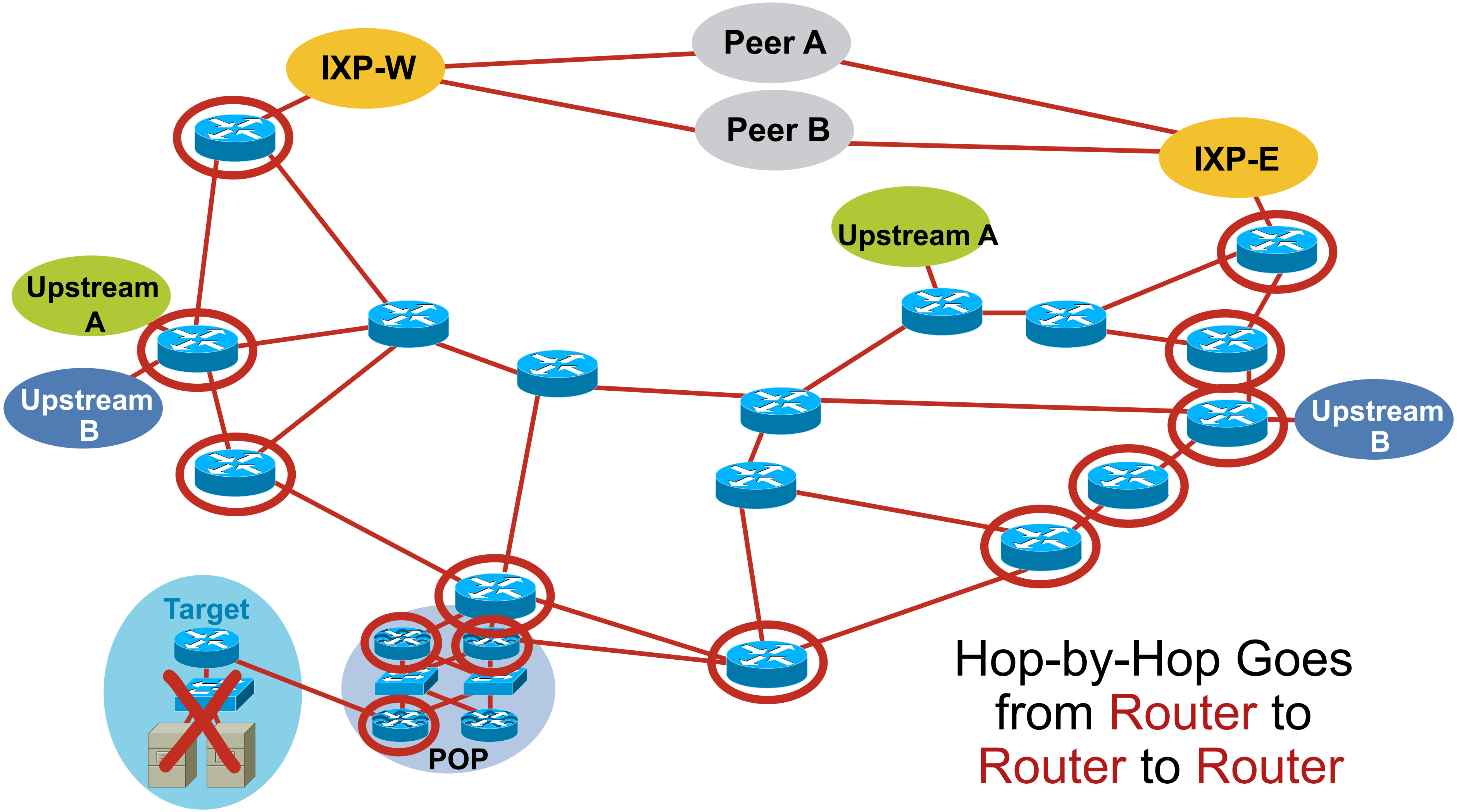
Traceback via Hop-by-Hop Technique

Hop-by-Hop Traceback 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

Target
Inside
Outside
Source

Traceback via Hop-by-Hop Technique

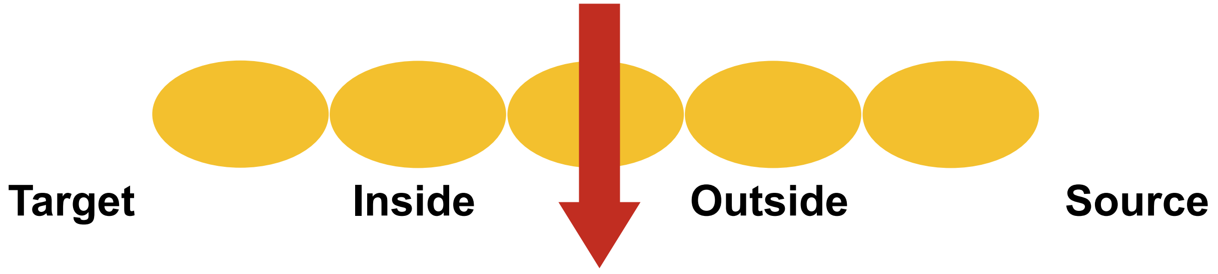


Hop-by-Hop Goes from Router to Router to Router

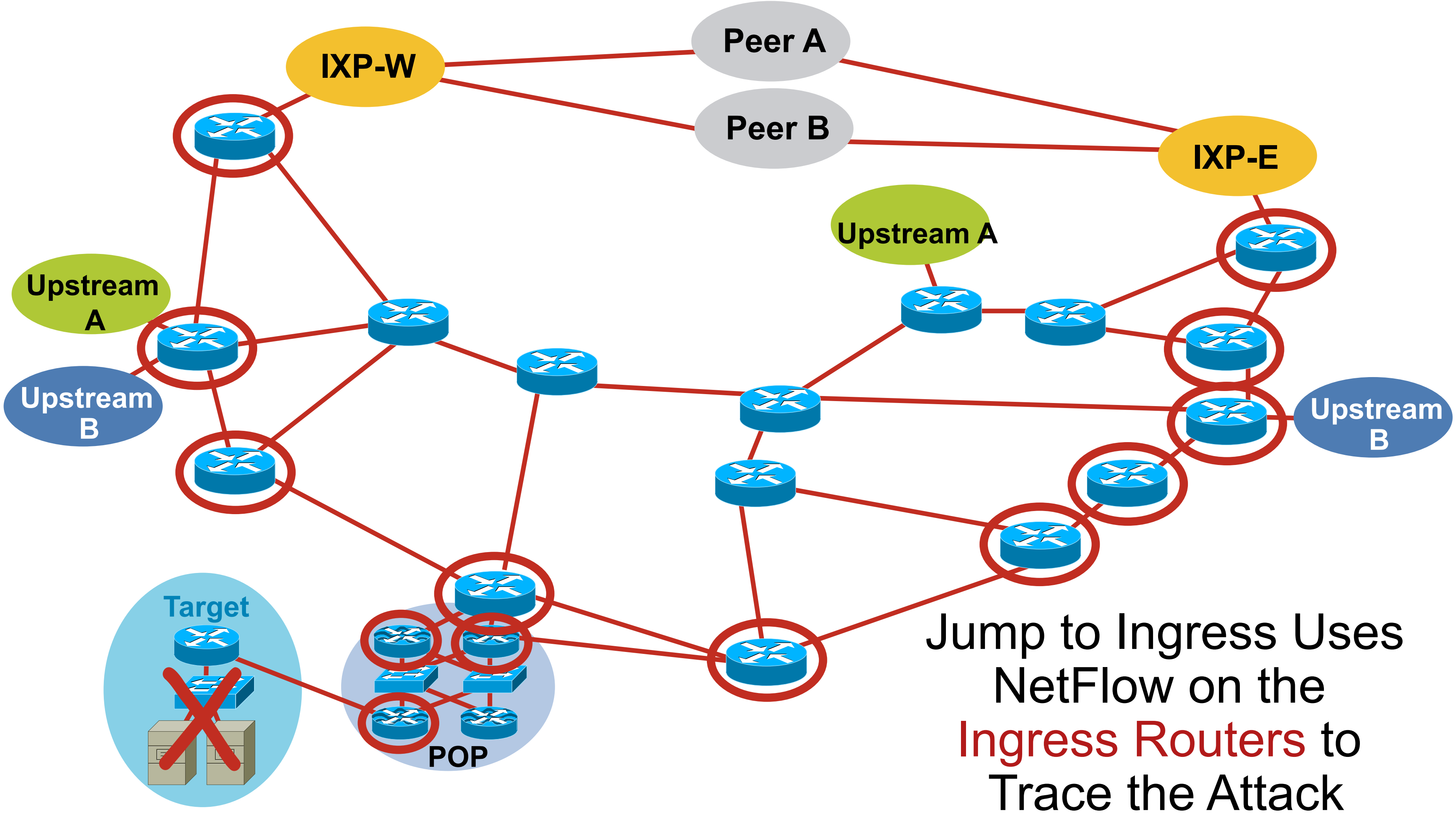
Traceback via the Jump to Ingress Technique

Jump to Ingress Tracebacks Divides the Problem in Half

- Is the attack originating from inside the network or outside the network?
- Jump to the ingress border routers to see if the attack is entering the network from the outside
- Advantage: speed—are we the source or is someone else the source?



Traceback via the Jump to Ingress Technique



Jump to Ingress Uses NetFlow on the Ingress Routers to Trace the Attack

Traceback Spoofed IPv4 Addresses

Traceback Techniques

- Apply temporary ACLs with log-input and examine the logs (like classification)
- Query NetFlow’s flow table
  - Show ip cache-flow if NetFlow is enabled
- Backscatter traceback technique
- Traceback using NetFlow telemetry

Traceback with ACLs

- Original traceback technique
- Risk: inserting change into a network that is under attack
- Risk: 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 ACLs

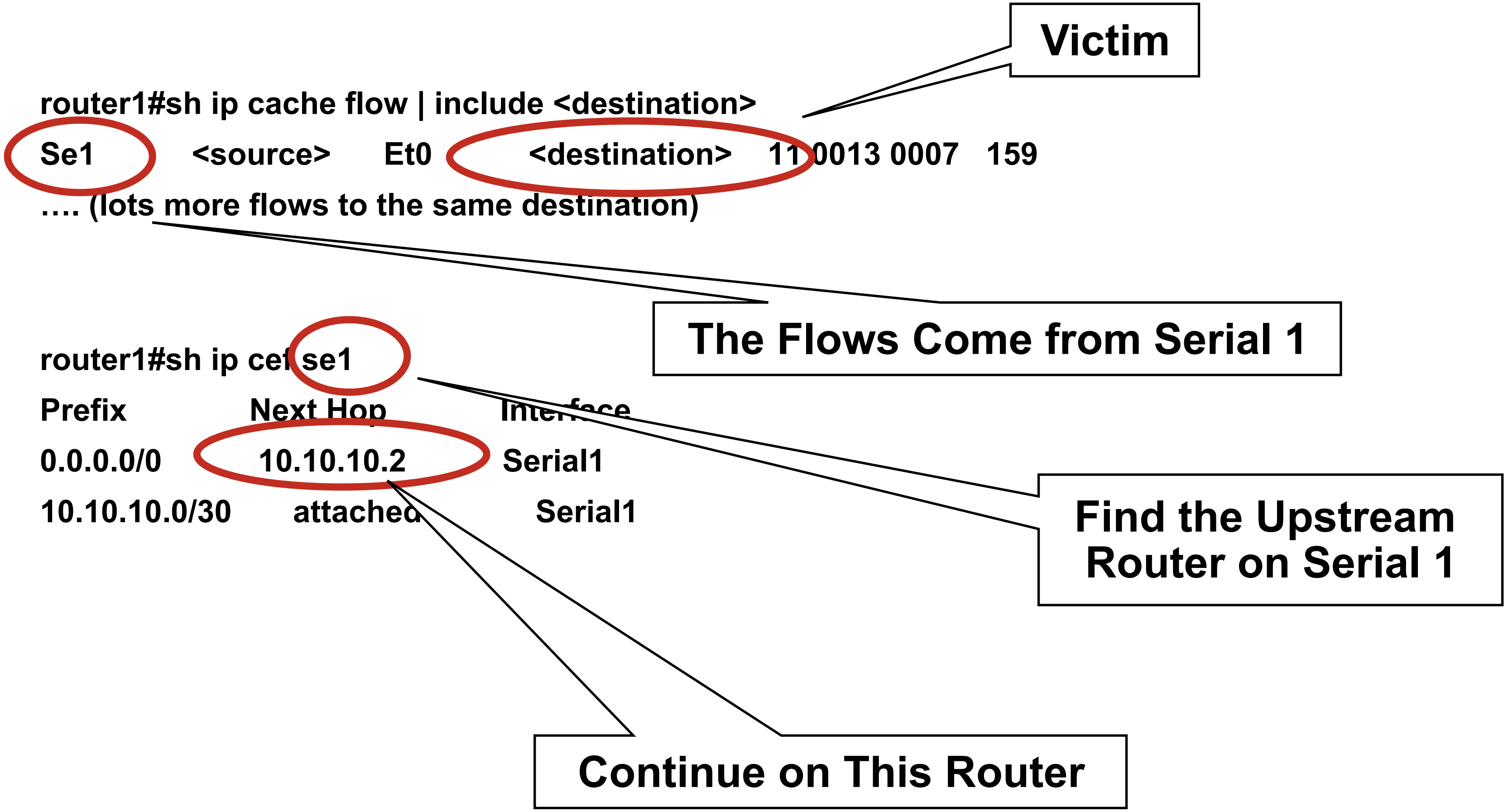
```
access-list 170 permit icmp any any echo
access-list 170 permit icmp any any echo-reply log-input
access-list 170 permit udp any any eq echo
access-list 170 permit udp any eq echo any
access-list 170 permit tcp any any established
access-list 170 permit tcp any any
access-list 170 permit ip any any

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 Output

- Validate the capture with show access-list 170; make sure it the packets we counted
- View the log with show logging for input interface:

```
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.212.72
(Serial0 *HDLC*) -> 172.19.61.10 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.154
(Serial0 *HDLC*) -> 172.19.61.10 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.15
(Serial0 *HDLC*) -> 172.19.61.10 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.142
(Serial0 *HDLC*) -> 172.19.61.10  (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.47
(Serial0 *HDLC*) -> 172.19.61.10 (0/0), 1 packet
```

Traceback with NetFlow



```
router1#sh ip cache flow | include <destination>
Se1      <source>    Et0        <destination>    11 0013 0007   159
…. (lots more flows to the same destination)

router1#sh ip cef se1
Prefix            Next Hop          Interface
0.0.0.0/0          10.10.10.2       Serial1
10.10.10.0/30        attached           Serial1
```

Victim

The Flows Come from Serial 1

Find the Upstream Router on Serial 1

Continue on This Router

Traceback with NetFlow Example
Tracing W32.Blaster Infected Hosts

W32.Blaster-Infected Hosts Attempt to Replicate to Random Systems Using Port 135, Which Is Hex 0087

```
Router>show ip cache flow | include 0087
:
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Fa2/0 XX.XX.XX.242 Fa1/0 XX.XX.XX.119 06 0B88 0087 1
Fa2/0 XX.XX.XX.242 Fa1/0 XX.XX.XX.169 06 0BF8 0087 1
Fa2/0 XX.XX.XX.204 Fa1/0 XX.XX.XX.63  06 0E80 0087 1
Fa2/0 XX.XX.XX.204 Fa1/0 XX.XX.XX.111 06 0CB0 0087 1
Fa2/0 XX.XX.XX.204 Fa1/0 XX.XX.XX.95  06 0CA0 0087 1
Fa2/0 XX.XX.XX.204 Fa1/0 XX.XX.XX.79  06 0C90 0087 1
```

Traceback with NetFlow Telemetry

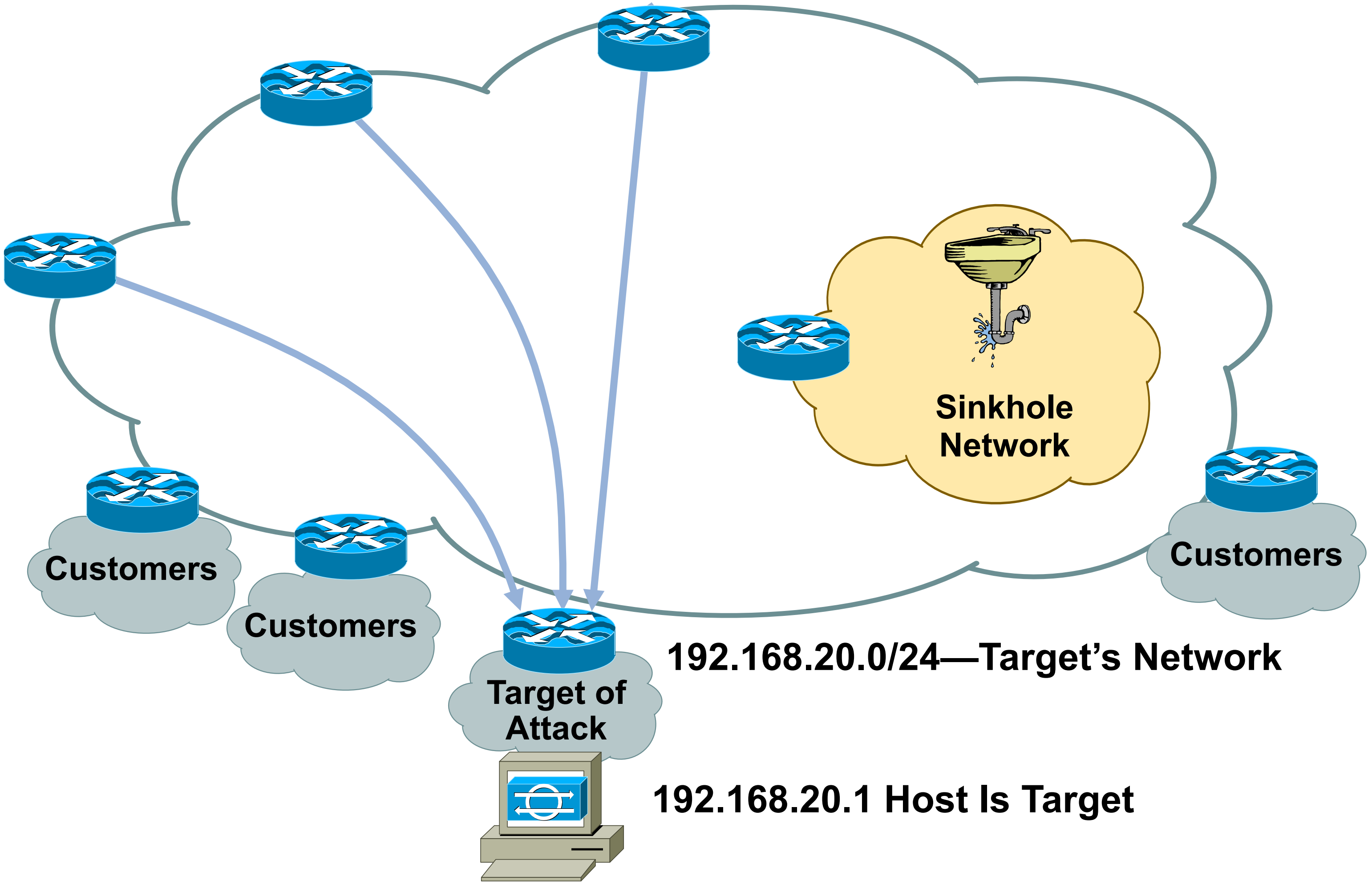
- Routers on the edge of the network can export NetFlow data reporting detailed traffic flow information
- This telemetry can be processed to detect anomalies and to traceback the attack to the source(s)
- Open source and commercial products available
- Arbor PeakFlow provides one example that has operationally proven its value

Attract and Analyze: Sinkholes

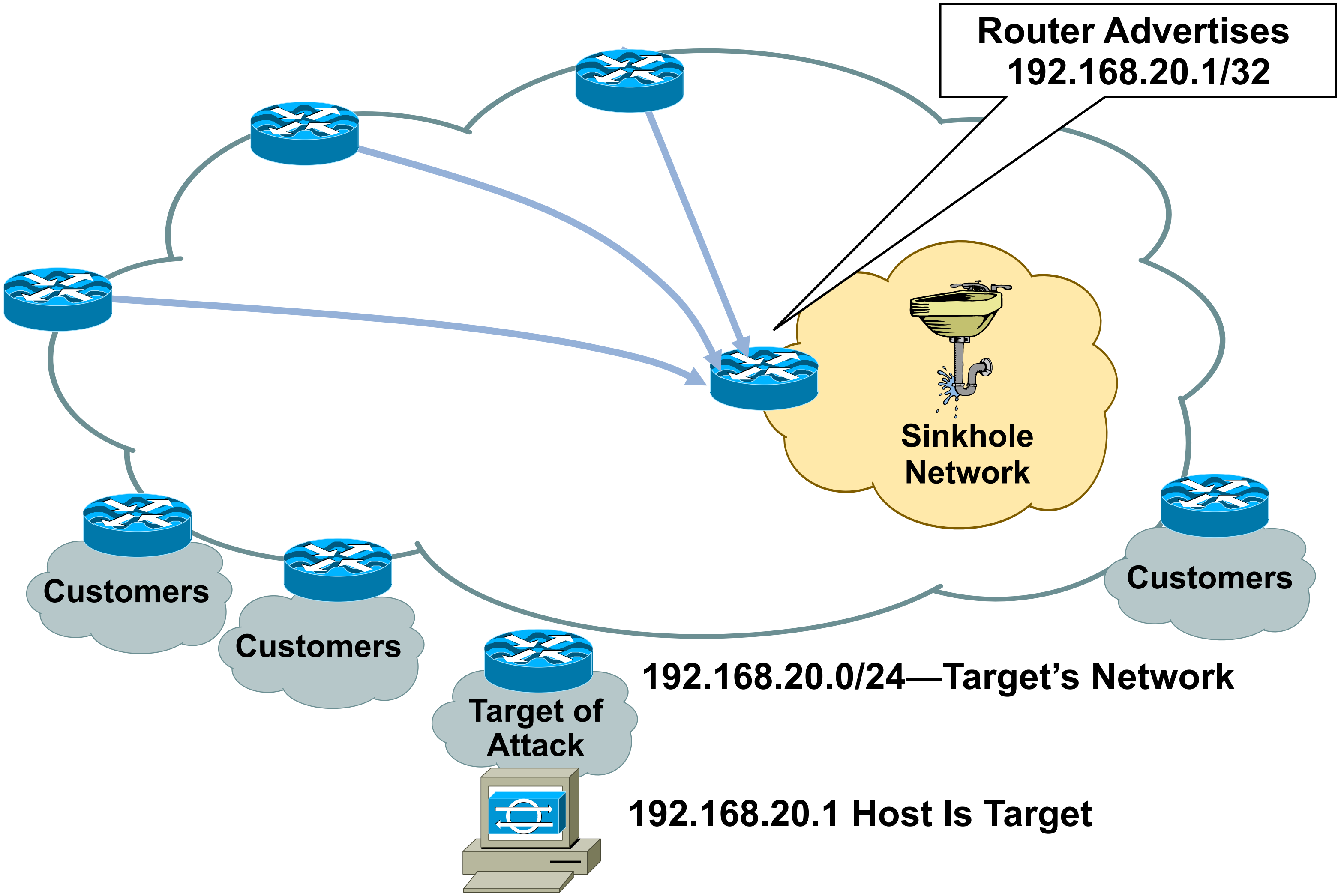
Sinkhole Routers/Networks

- Sinkholes are a topological security feature—think network honeypot
- Router or workstation built to suck in traffic and assist in analyzing attacks (original use)
- Redirect attacks away from the customer—working the attack on a router built to withstand the attack
- Used to monitor attack noise, scans, data from misconfiguration and other activity (via the advertisement of default or unused IP space)
- Traffic is typically diverted via BGP route advertisements and policies
- Leverage instrumentation in a controlled environment
  - Pull the traffic past analyzers/analysis tools

Sinkhole Routers/Networks



Sinkhole Routers/Networks



What to Monitor in a Sinkhole?

- Scans on dark IP (allocated and announced but unassigned address space)

  Who is scoping out the network—pre-attack planning, worms

- Scans on bogons (unallocated)

  Worms, infected machines, and Bot creation

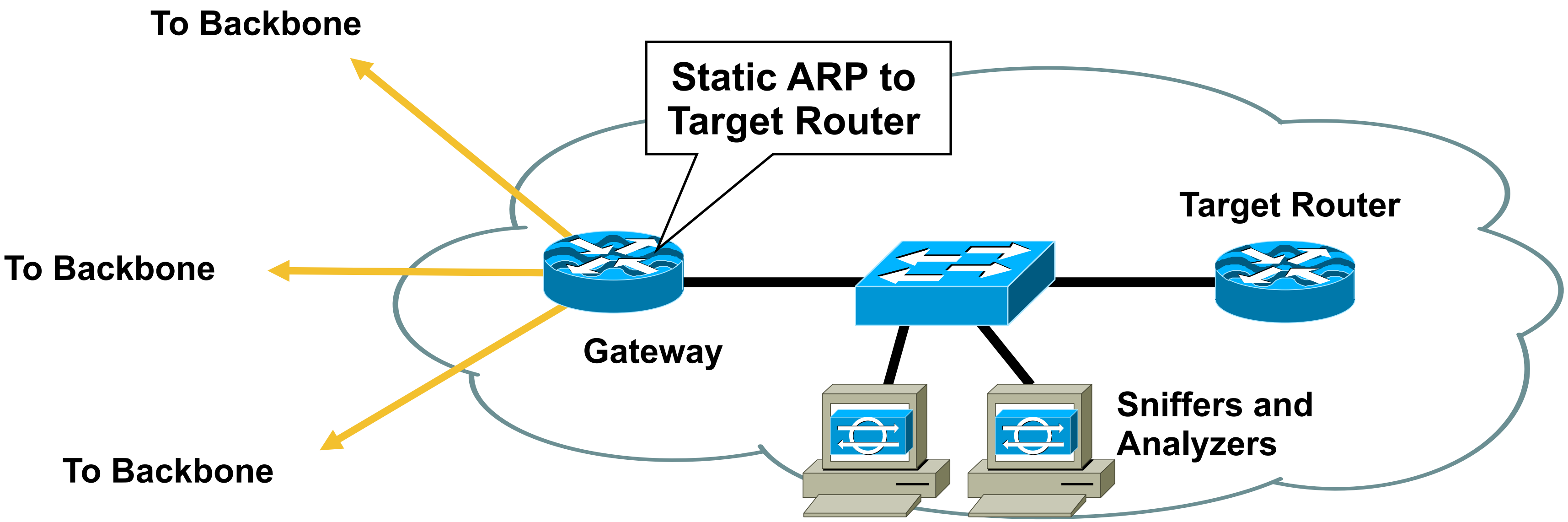
- Backscatter from attacks

  Who is getting attacked

- Backscatter from garbage traffic (RFC-1918 leaks)

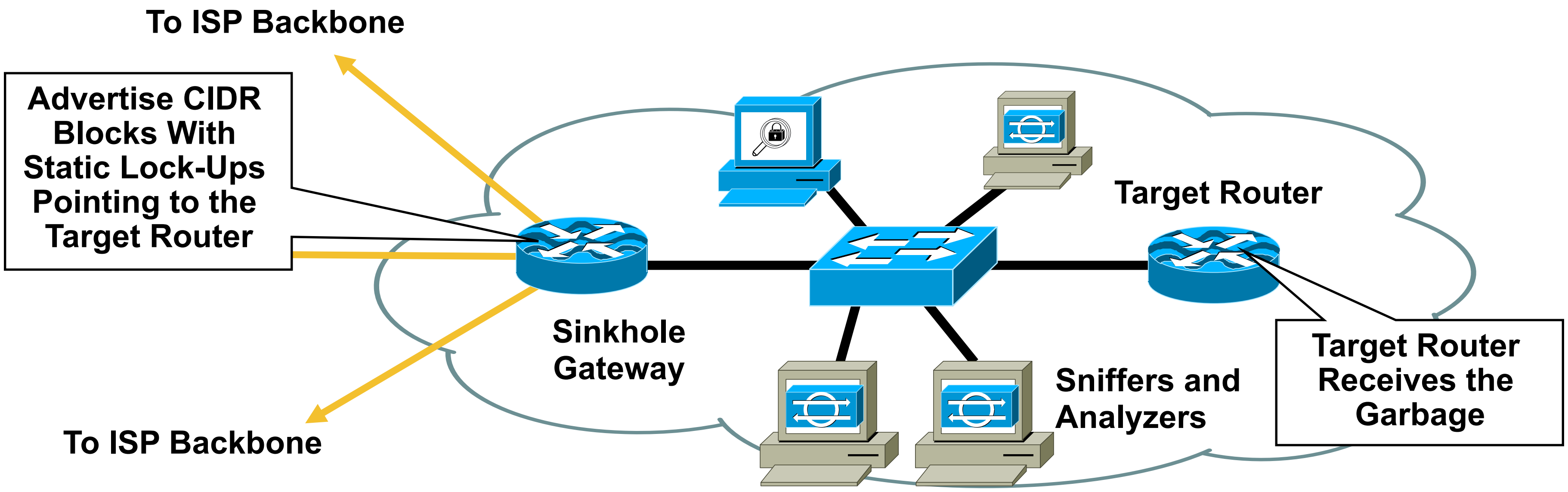
  Which customers have misconfiguration or “leaking” networks

Sinkhole Architecture



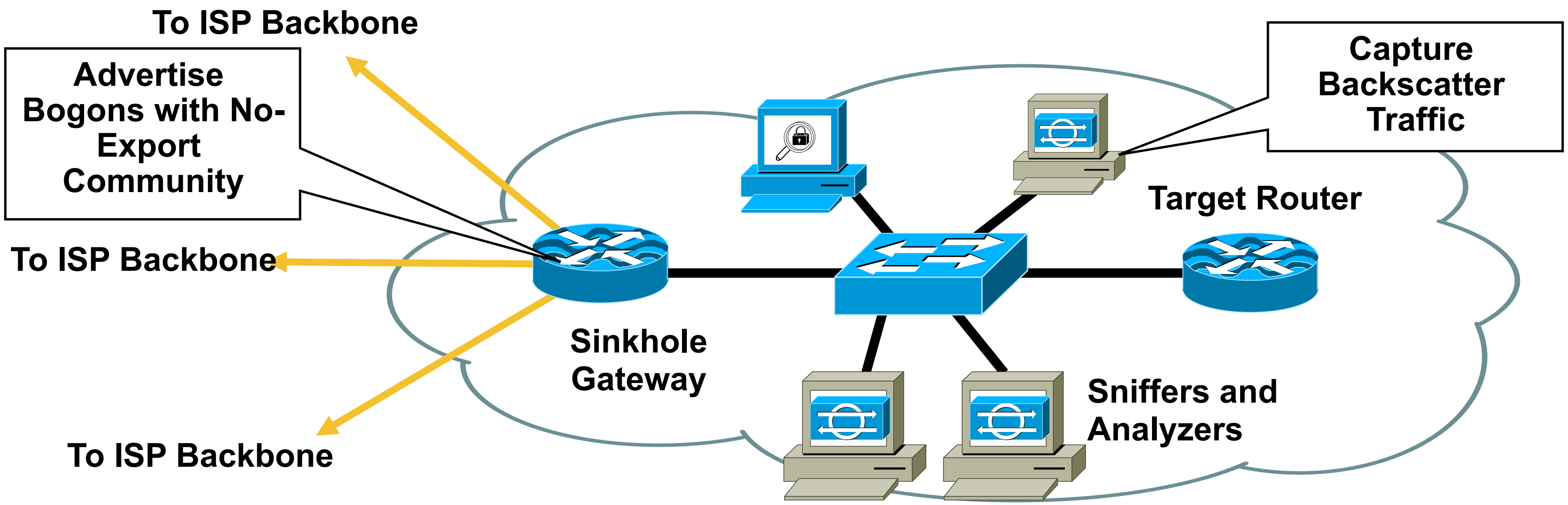
- Expand sinkhole with dedicated router into a variety of tools
- Pull DDoS attack to the sinkhole and forward data toward target router
- Static ARP to the target router keeps the sinkhole operational—target router can crash from attack and static ARP will keep gateway forwarding traffic to the Ethernet switch—rather than generating lots of ICMP error messages
- Observe trends and deviations, reserve packet detail for research and specific analysis

Sinkholes: Advertising Dark IP


To ISP Backbone
Advertise CIDR Blocks With Static Lock-Ups Pointing to the Target Router
Target Router
Sinkhole Gateway
Sniffers and Analyzers
Target Router Receives the Garbage
To ISP Backbone

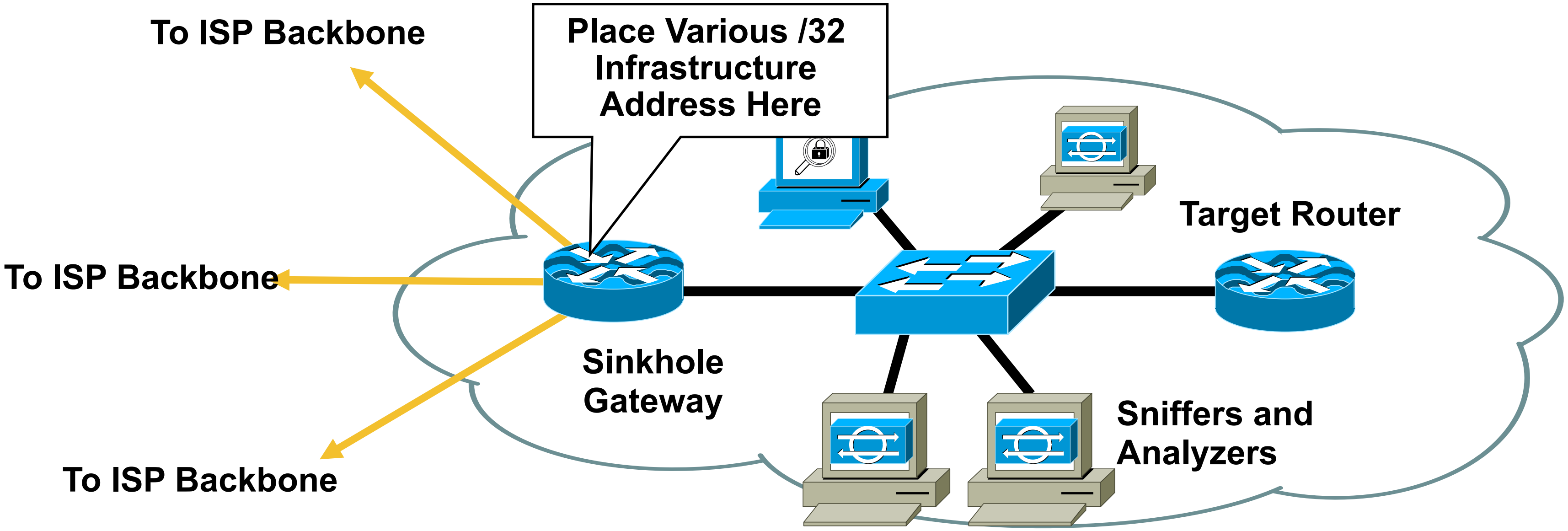
- Move the CIDR Block Advertisements (or at least more-specifics of those advertisements) to sinkholes
- Does not impact BGP routing—route origination can happen anywhere in the iBGP mesh (careful about MEDs and aggregates)
- Control where you drop the packet
- Turns networks inherent behaviors into a security tool

Monitoring Backscatter



- Advertise bogon blocks with NO_EXPORT community and an explicit safety community (plus prefix-based egress filtering on the edge)
- Static/set the BGP NEXT_HOP for the bogon to a backscatter collector workstation (as simple as TCPdump)
- Pulls in backscatter for that range—allows monitoring

Monitoring Scan Rates



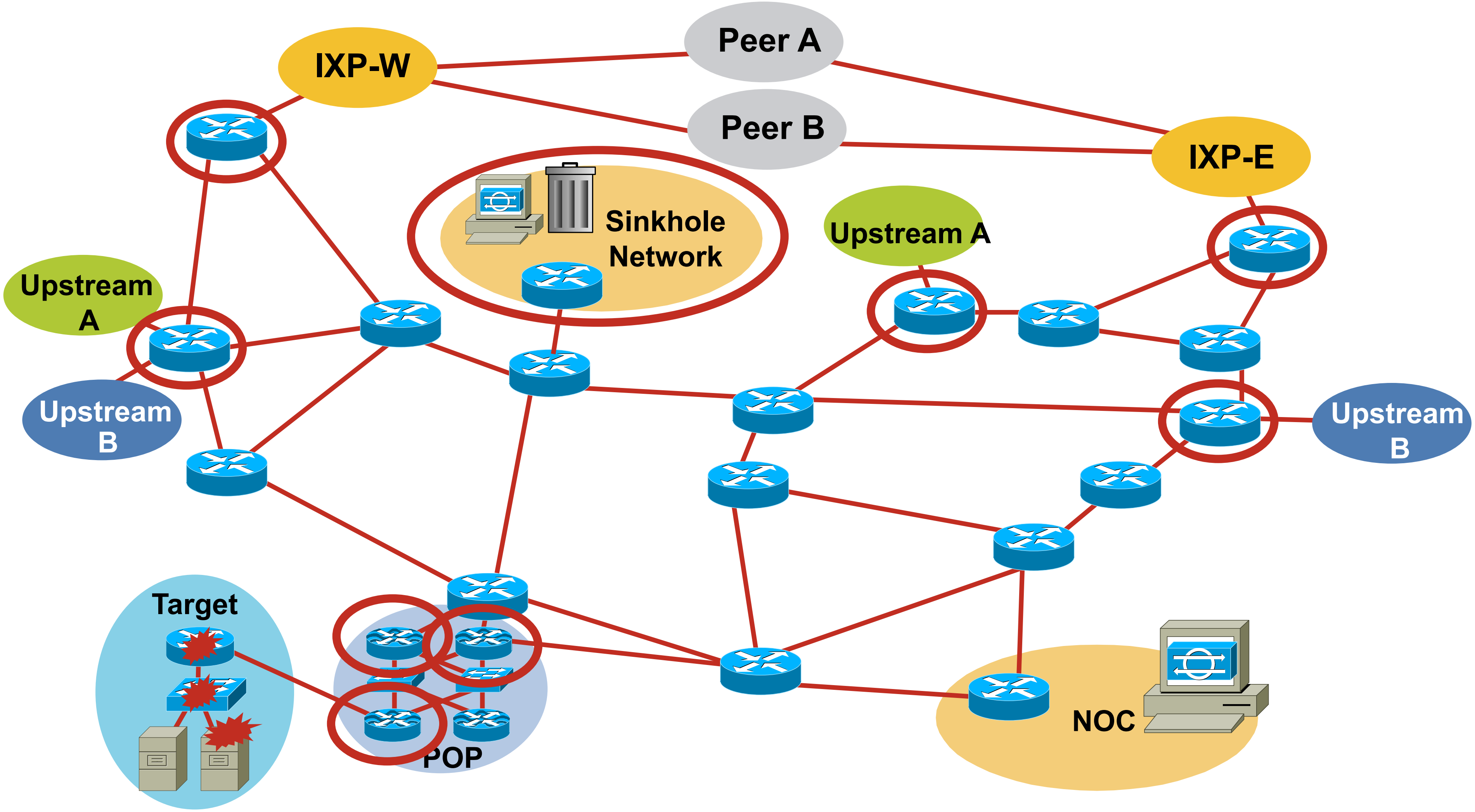
- Select /32 (or larger) address from different block of your address space; advertise them out the sinkhole
- Assign them to a workstation built to monitor and log scans (Arbor Network's Dark IP PeakFlow module is one turnkey commercial tool that can monitor scan rates via data collected from the network)

Reacting to Attacks

Reaction Tools

- Wide range of response options exists
  - Access-control lists
  - QoS tools such as CAR, traffic policing and NBAR
  - Firewalls
  - Various IPS technologies: NIDS, HIDS, anomaly detection
  - BGP triggers
  - Packet scrubbing
- Today, we will focus on core-centric tools

Where to React?



QoS at the Edge as Attack Mitigation

- Tag all ingress packets at the internet edge
- Doesn’t require application or ip address awareness
- Provides proactive and reactive mitigation:

Proactively

Knocks down ToS 5-7

Can be added to CoPP ACL’s:

```
access-list 152 permit tcp any any eq 22 dscp af13
```

Reactively

ACL’s on the fly at internal chokepoints

Scavenger QoS, see:

Scavenger-Class QoS Strategy for DoS/Worm Attack Mitigation

http://www.cisco.com/application/pdf/en/us/guest/tech/tk759/c1482/cdccont_0900aecd80295ac7.pdf

QoS at the Edge as Attack Mitigation

- Configuration

```
class-map match-all edge-color
 match any
policy-map edge-color
 class edge-color
  set dscp af13

interface GigabitEthernet0/1
 service-policy input edge-color
```

- Considerations
  - CPU impact - 3825 at 50,000 pps
    - Without tagging 12% CPU
    - With tagging 25% CPU
  - Integration with existing QoS policy
  - Treats all inbound traffic equally
    - Differentiate responses to inside connections?
    - Business critical inbound connections?
    - Recolor ToS 6/7 instead?

Reacting to an Attack with ACLs

- Traditional method for stopping attacks
- Scaling issues encountered:
    - Operational difficulties
        - Changes on the fly
        - Multiple ACLs per interface
    - Performance concerns
- How does the ACL load into the router? Does it interrupt packet flow?
- How many ACEs can be supported in hardware?
  In software?
- How does ACL depth impact performance?
- How do multiple concurrent features affect performance?

Reacting with BGP

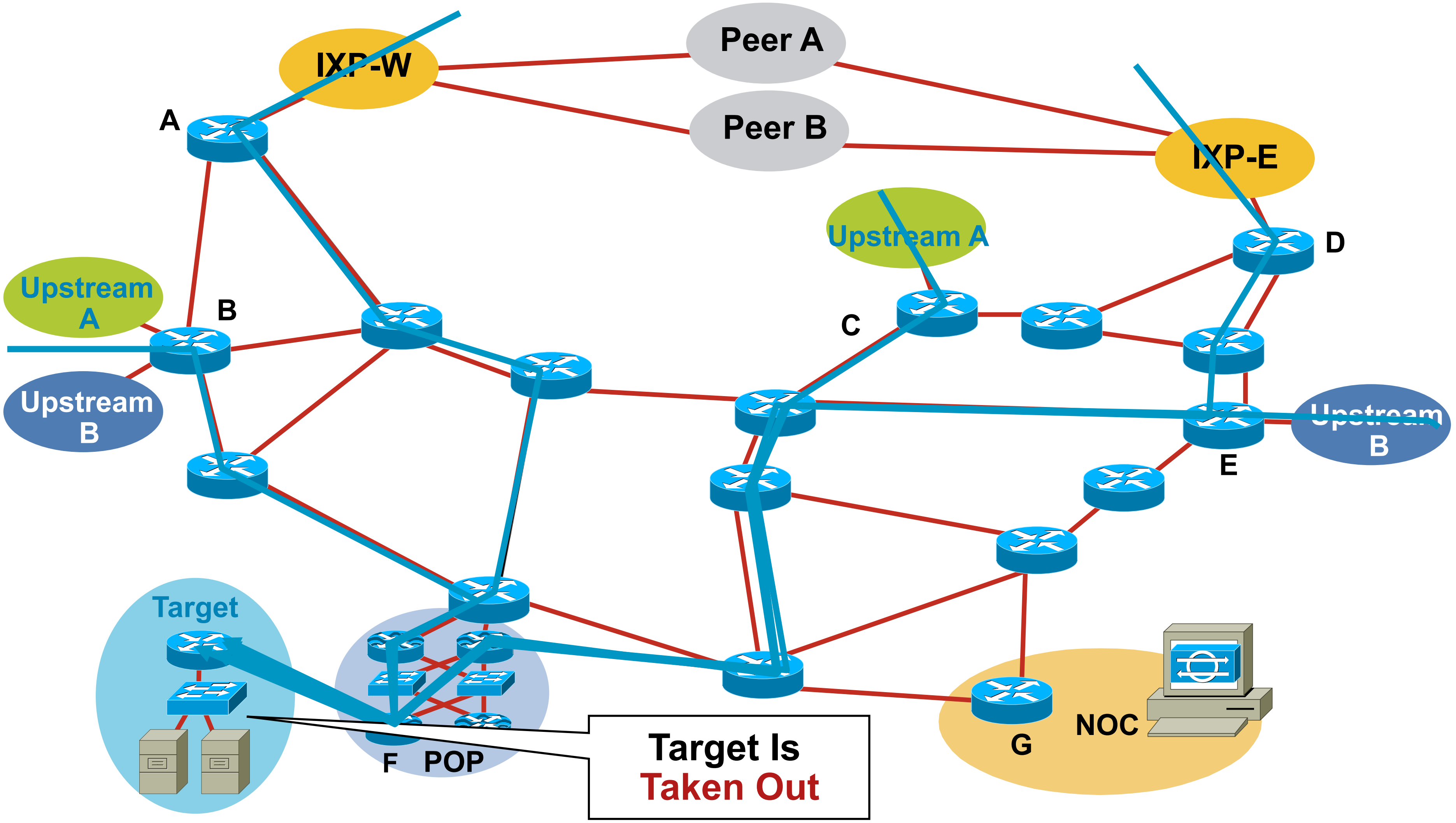
Blackhole Filtering

- Blackhole Filtering or Blackhole Routing forwards a packet to a router’s bit bucket

  Also known as “route to Null0”

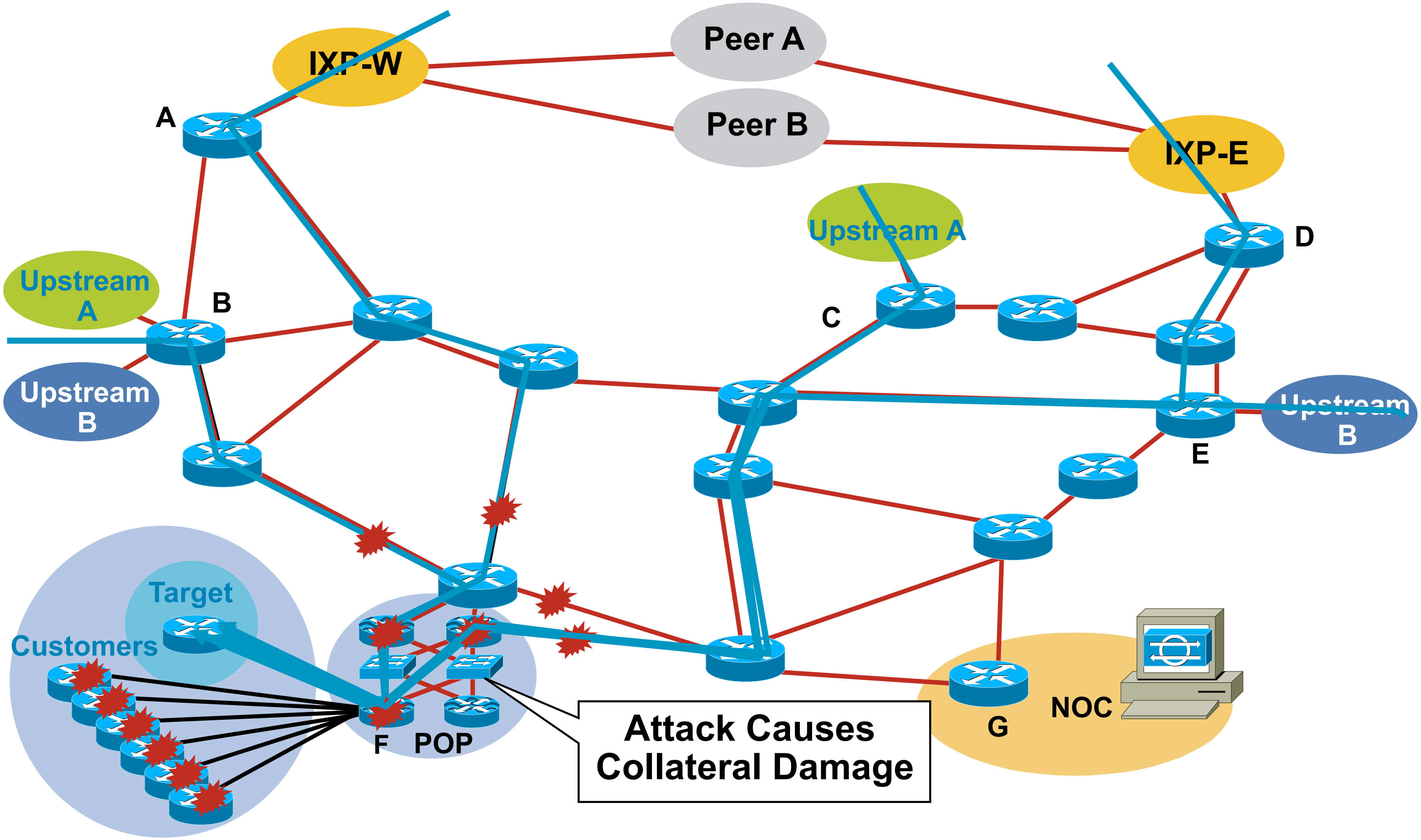
- Works only on destination addresses, since it is really part of the forwarding logic
- Forwarding ASICs are designed to work with routes to Null0—dropping the packet with minimal to no performance impact
- Used for years as a means to “blackhole” unwanted packets

Customer Is DoSed: Before



Target Is
Taken Out

Customer Is DoSed: Before—Collateral Damage



Attack Causes Collateral Damage

Remotely Triggered Blackhole Filtering

- We will use BGP to trigger a networkwide response to an attack

- A simple static route and BGP will enable a networkwide destination address blackhole as fast as iBGP can update the network

- This provides a tool that can be used to respond to security related events and forms a foundation for other remote triggered uses

- Often referred to as RTBH

Remote Triggered Blackhole

- Configure all edge routers with static route to Null0 (must use “reserved” network)

```
ip route 192.0.2.1 255.255.255.255 Null0
```

- Configure trigger router

  Part of iBGP mesh

  Dedicated router recommended

- Activate blackhole

  Redistribute host route for victim into BGP with next-hop set to 192.0.2.1

  Route is propagated using BGP to all BGP speaker and installed on routers with 192.0.2.1 route

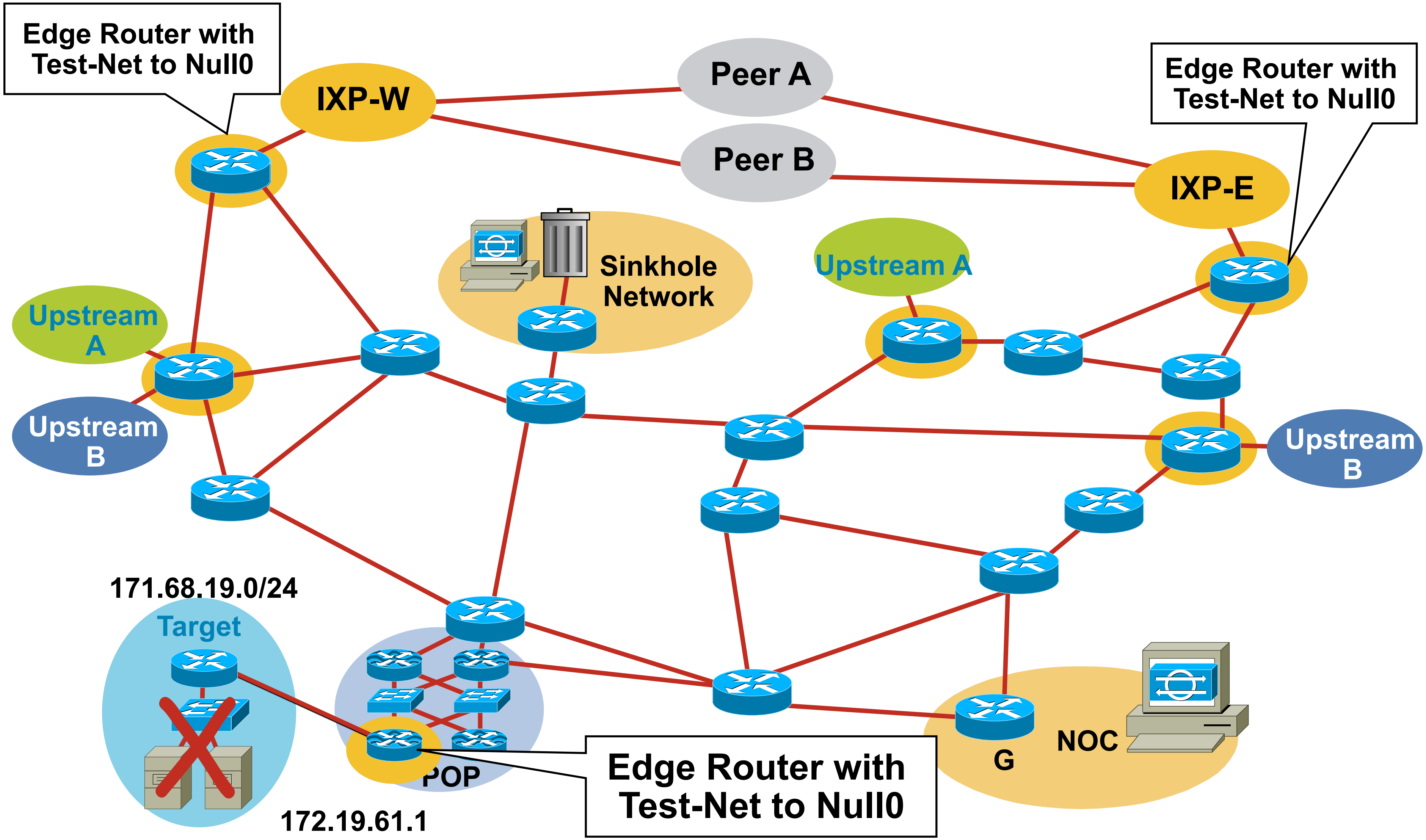
  All traffic to victim now sent to Null0

Step 1: Prepare All the Routers With Trigger

- Select a small block that will not be used for anything other than blackhole filtering; test Net (192.0.2.0/24) is optimal since it should not be in use
- Put a static route with a /32 from Test-Net—192.0.2.0/24 to Null 0 on every edge router on the network

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Step 1: Prepare All the Routers With Trigger



Step 2: Prepare the Trigger Router

The Trigger Router Is the Device that Will Inject the iBGP Announcement into the ISP’s Network

- Should be part of the iBGP mesh—but does not have to accept routes
- Can be a separate router (recommended)
- Can be a production router
- Can be a workstation with Zebra/Quagga (interface with Perl scripts and other tools)

Trigger Router’s Configuration

Redistribute Static with a Route-Map

```
router bgp 65535
.
redistribute static route-map static-to-bgp
.
!
route-map static-to-bgp permit 10
match tag 66
set ip next-hop 192.0.2.1
set local-preference 200
set community no-export
set origin igp
!
Route-map static-to-bgp permit 20
```

Match Static Route Tag

Set Next-Hop to the Trigger

Set Local-Pref

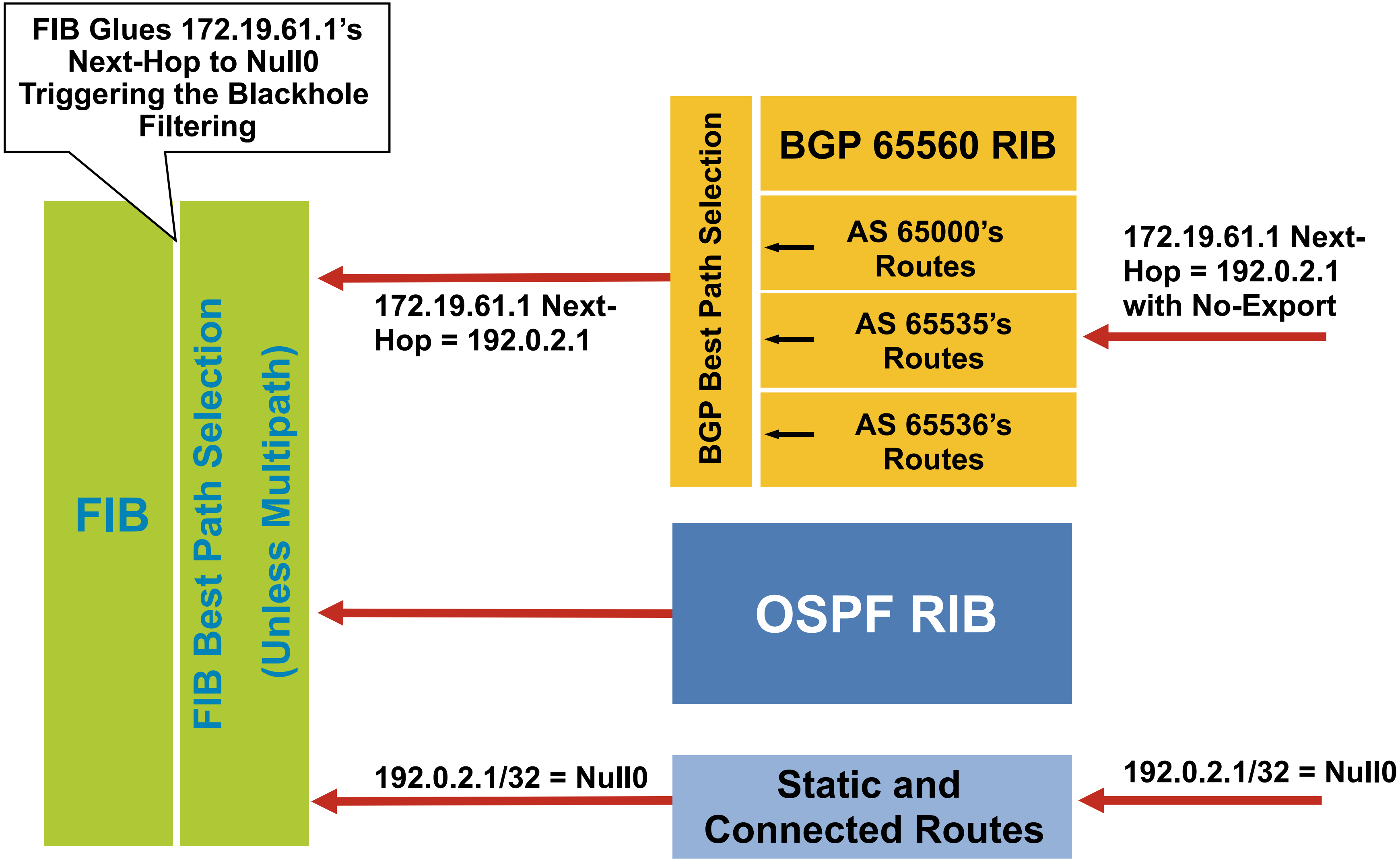
Step 3: Activate the Blackhole

- Add a static route to the destination to be blackholed; the static is added with the “tag 66” to keep it separate from other statics on the router

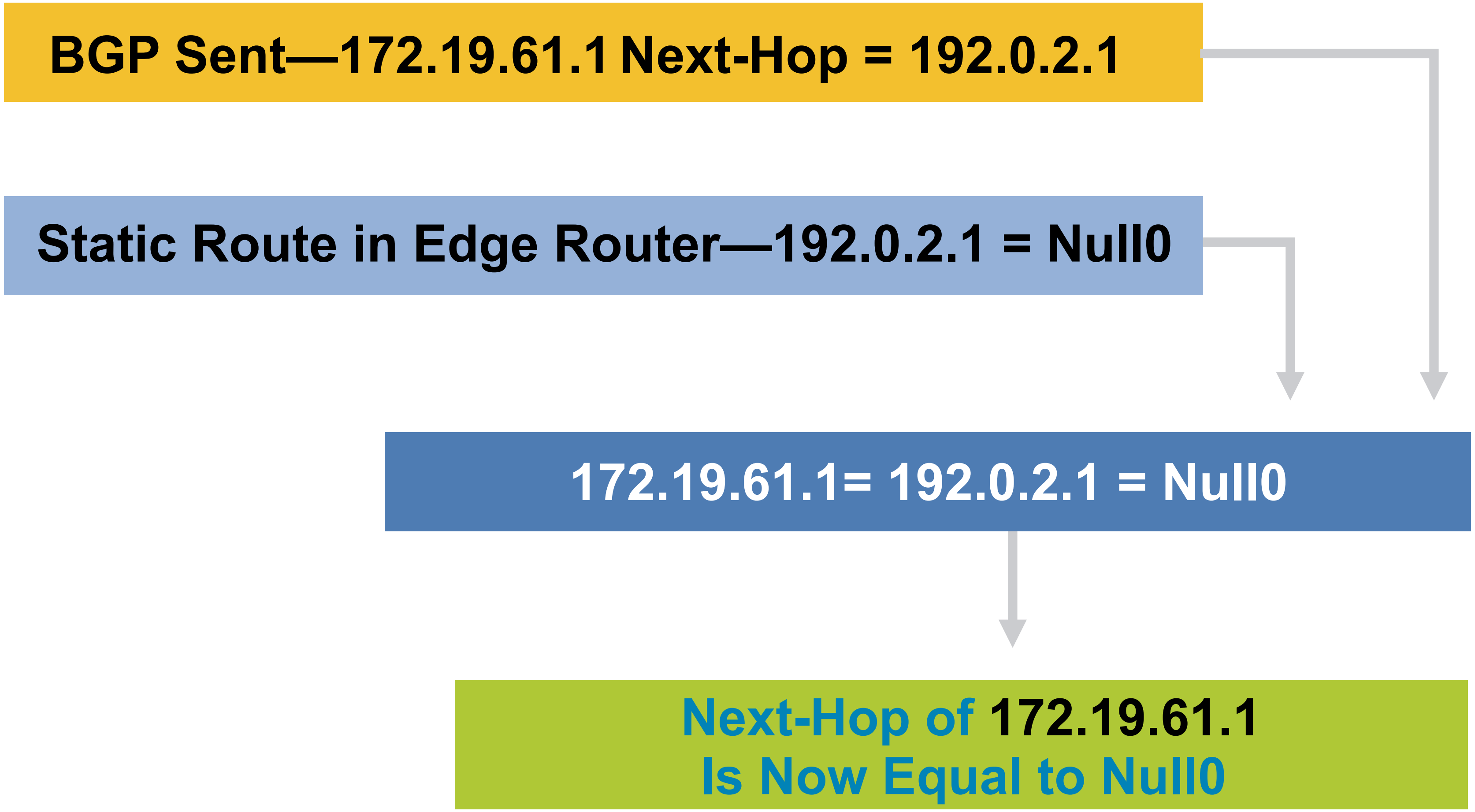
```
ip route 172.19.61.1 255.255.255.255 Null0 Tag 66
```

- BGP advertisement goes out to all BGP speaking routers
- Routers received BGP update, and “glue” it to the existing static route; due to recursion, the next-hop is now Null0

Step 3: Activate the Blackhole


FIB Glues 172.19.61.1's Next-Hop to Null0 Triggering the Blackhole Filtering
FIB
FIB Best Path Selection
(Unless Multipath)
172.19.61.1 Next-Hop = 192.0.2.1
BGP Best Path Selection
BGP 65560 RIB
AS 65000's Routes
AS 65535's Routes
AS 65536's Routes
172.19.61.1 Next-Hop = 192.0.2.1 with No-Export
OSPF RIB
192.0.2.1/32 = Null0
Static and Connected Routes
192.0.2.1/32 = Null0

Step 3: Activate the Blackhole



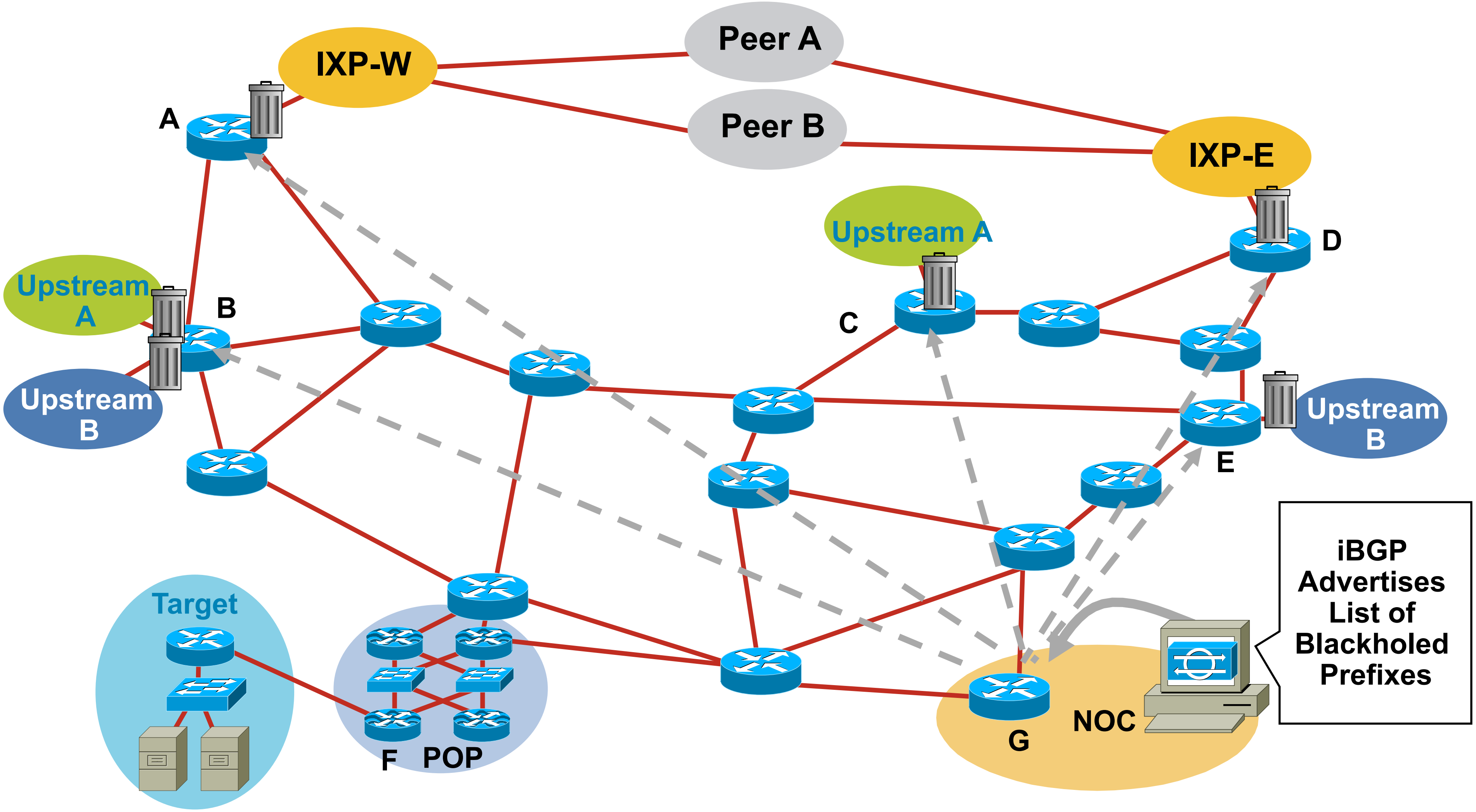
BGP Sent—172.19.61.1 Next-Hop = 192.0.2.1

Static Route in Edge Router—192.0.2.1 = Null0

172.19.61.1= 192.0.2.1 = Null0

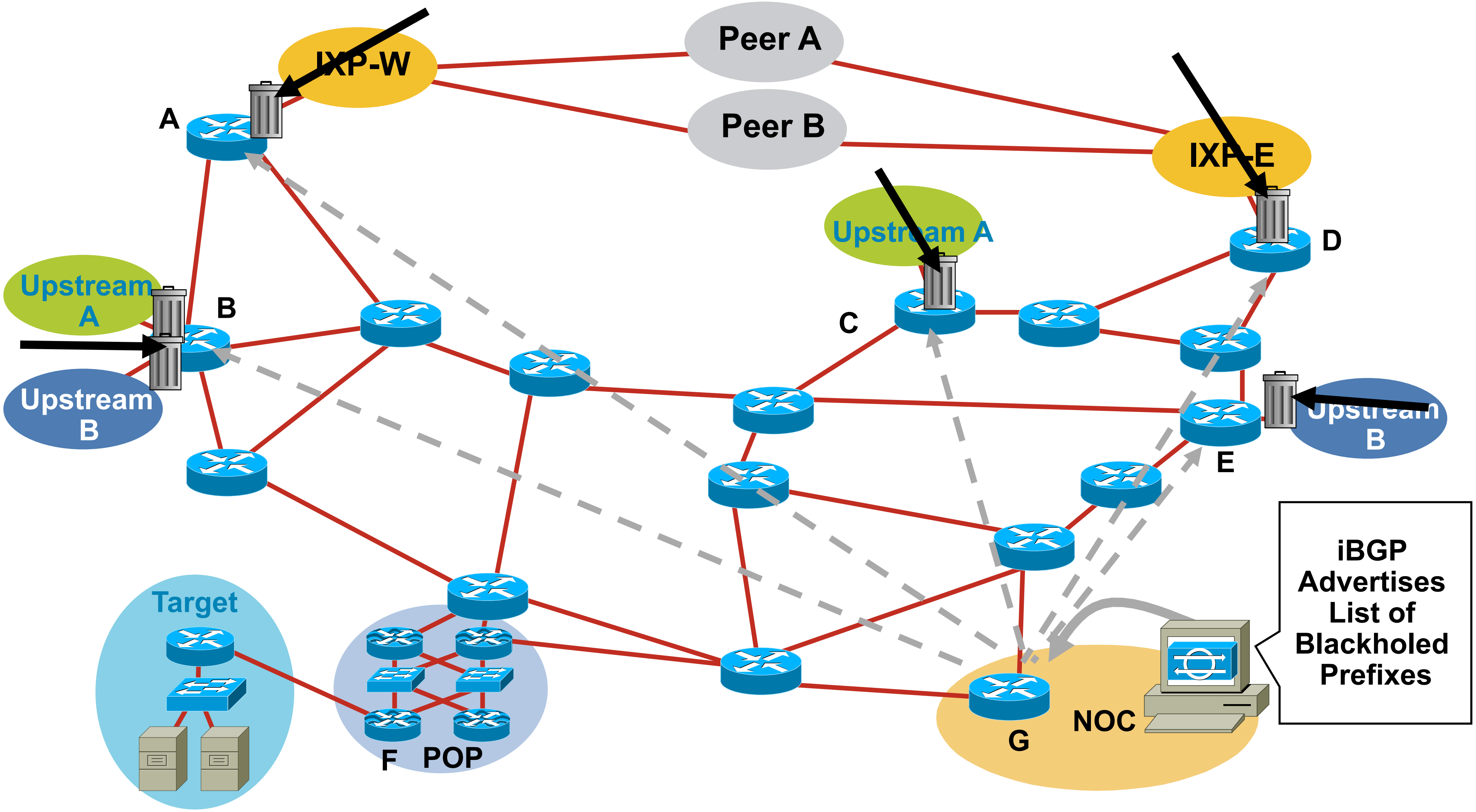
Next-Hop of 172.19.61.1
Is Now Equal to Null0

Step 3: Activate the Blackhole



iBGP Advertises List of Blackholed Prefixes

Customer Is DoSed: After—
Packet Drops Pushed to the Edge



Using Remote Triggered Blackhole

- Is this done today?

  Yes, service providers and enterprises use frequently

- Often only scaleable answer to large-scale DoS attack

  Has proven very effective

- Interprovider triggers not implemented

  Rely on informal channels

- Service: customer triggered

  Edge customers trigger the update, SP doesn’t get involved

  Implication: you detect, you classify, etc.

- White list allowed traffic to prevent self-DoS

  http://www.cymru.com/gillsr/documents/golden-networks

BGP Sinkhole Trigger

- Leverage the same BGP technique used for RTBH
- Dedicated trigger router redistributes more specific route for destination being re-rerouted
    - Next-hop set via route-map
- All BGP-speaking routers receive update
- Complex design can use multiple route-maps and next-hops to provide very flexible designs
- May require BGP on all routers

Example: BGP Sinkhole Triggers

- Sinkhole IP: 192.0.2.8
- Victim IP: 192.168.20.1
- Trigger router configuration

```
router bgp 100
redistribute static route-map static-to-bgp

route-map static-to-bgp permit 10
 match tag 66
 set origin igp
 set next-hop 192.0.2.8  <-- sinkhole address, not Null0
 set community NO-EXPORT

ip route 192.168.20.1 255.255.255.255 Null0 tag 66
```

- All traffic destined to 192.168.20.1 will be redirected to the sinkhole

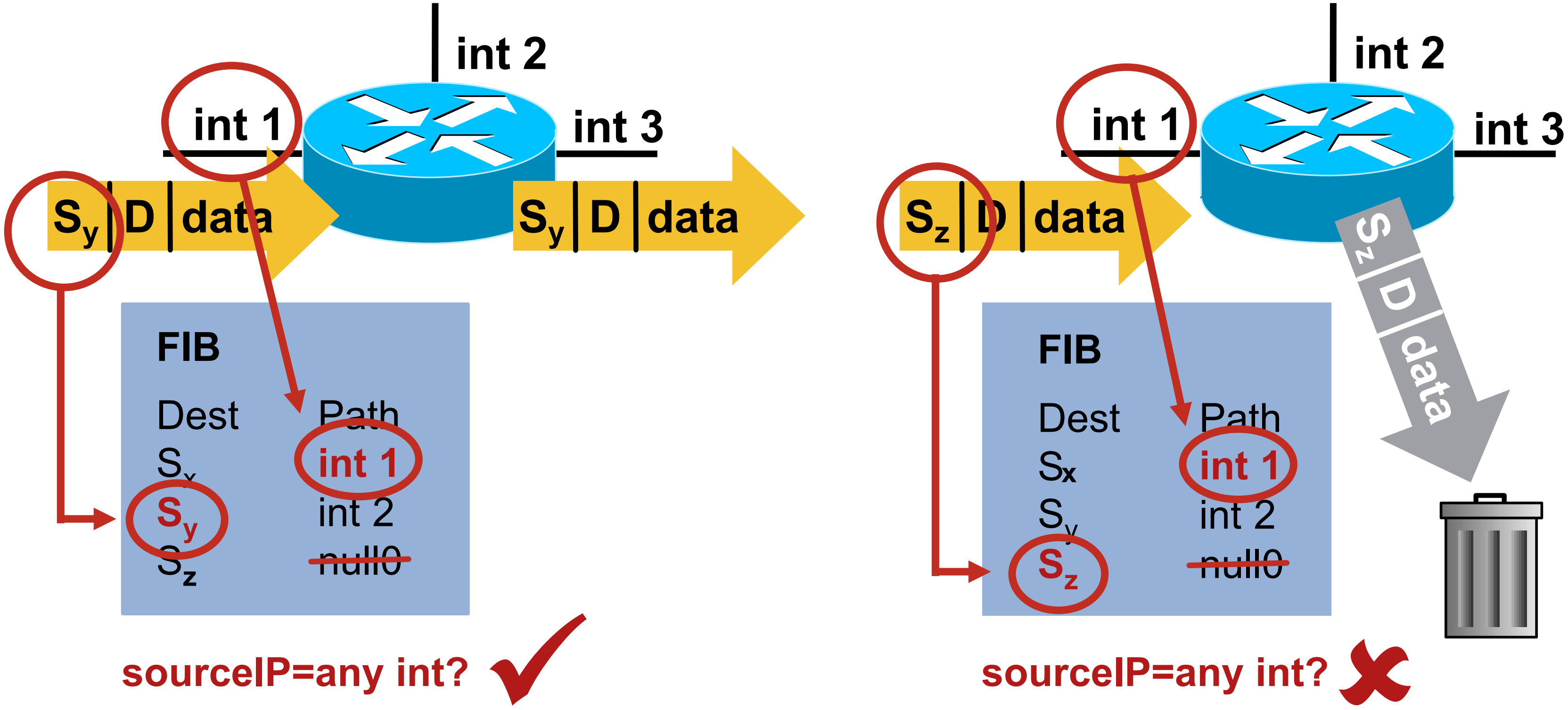
Flipping RTBH Around

Triggered Source Drops

- Dropping on destination is very important
  - Dropping on source is often what we really need
- Reacting using source address provides some interesting options:
  - Stop the attack without taking the destination offline
  - Filter command and control servers
  - Filter (contain) infected end stations
- Must be rapid and scalable
  - Leverage pervasive BGP again

Quick Review: uRPF—Loose Mode

router(config-if)# ip verify unicast source reachable-via any



IP Verify Unicast Source Reachable—Via any

Source-Based Remote Triggered

Blackhole Filtering

Uses the Same Architecture as Destination-Based Filtering + Unicast RPF

- Edge routers must have static in place
- They also require Unicast RPF
- BGP trigger sets next hop—in this case the "victim" is the source we want to drop

Source-Based Remote Triggered

Blackhole Filtering

- What do we have?

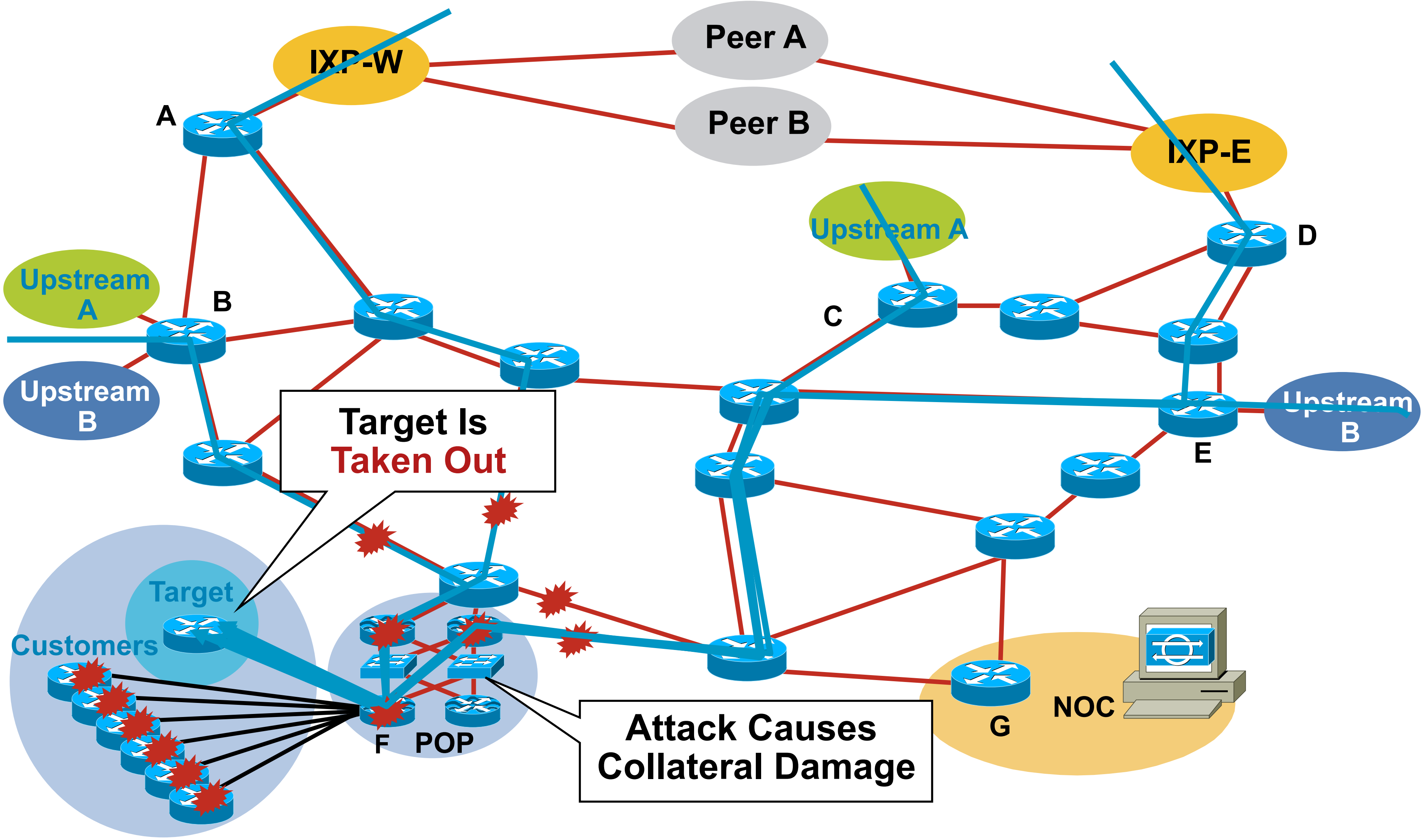
  Blackhole Filtering—if the destination address equals Null0, we drop the packet

  Remote Triggered—trigger a prefix to equal Null0 on routers across the Network at iBGP speeds

  uRPF Loose Check—if the source address equals Null0, we drop the packet

- Put them together and we have a tool to trigger drop for any packet coming into the network whose source or destination equals Null0

Customer Is DoSed: Before



Target Is Taken Out

Attack Causes Collateral Damage

Community-Based Trigger

- BGP community-based triggering allow for more fined tuned control over where you drop the packets
- Three parts to the trigger:

  Static routes to Null0 on all the routers

  Trigger router sets the community

  Reaction routers (on the edge) matches community
  and sets the next-hop to the static route to Null0

BGP: Not Just For Routing, Anymore

- “I don’t want to use BGP as a routing protocol”
    - Think of BGP as a signaling protocol
    - Routing protocols operate as “ships in the night”
- BGP has a unique property among routing protocols: arbitrary next hops can be administratively defined
- There is no need to actually carry routes in BGP
    - Deploy iBGP mesh internally and do not use it for routing
    - Under normal conditions, BGP holds zero routes
    - When used for drops, only the blackholed addresses are in the table
- If BGP is used for inter-region routing, drop boundaries can be both local within a campus and global
    - Use communities to “scope” the drops

Internal Source-Based Drops

- Both source and destination drops can be used internally
  - Source drops likely the most interesting case
  - Destination drops still result in target DoS
  - Don’t forget the Internet and WAN edges
- Provides a very effective mechanism to handle internal attacks
  - Drop worm infected PCs off the network
  - Drop “owned” devices off the network
  - Protect the infrastructure
  - Whitelist to prevent self DoS

Source-Based RTBH

Key Advantages

- No ACL update
- No change to the router's configuration
- Drops happen in the forwarding path
- Frequent changes when attacks are dynamic (for multiple attacks on multiple customers)

References

- DoS detection:

  “Tackling Network DoS on Transit Networks”: David Harmelin, DANTE, March 2001

  http://www.dante.net/pubs/dip/42/42.html

  “Inferring Internet Denial-of-Service Activity”: David Moore et al, May 2001

  http://www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf

  “The Spread of the Code Red Worm”: David Moore, CAIDA, July 2001

  http://www.caida.org/analysis/security/code-red/

- DoS tracing:

  “Tracing Spoofed IP Addresses”: Rob Thomas, Feb 2001
  (good technical description of using NetFlow to trace back a flow)

  http://www.cymru.com/Documents/tracking-spoofed.html

- Other:

  “DoS Attacks against GRC.com”: Steve Gibson, GRC, June 2001 (a real-life description of attacks from the victim side; somewhat disputed, but fun to read)

  http://grc.com/dos/grcdos.htm

  SECURITY@CISCO

  http://www.cisco.com/security/

NetFlow—More Information

- Cisco NetFlow home

  http://www.cisco.com/en/US/tech/tk812/tsd_technology_support_protocol_home.html

- Linux NetFlow reports HOWTO

  http://www.dynamicnetworks.us/netflow/netflow-howto.html

- Arbor Networks PeakFlow SP

  http://www.arbornetworks.com/products_sp.php

SNMP—More Information

- Cisco SNMP object tracker

  http://www.cisco.com/pcgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4

- Cisco MIBs and trap definitions

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- SNMPLink

  http://www.snmplink.org/

RMON—More Information

- IETF RMON WG

  http://www.ietf.org/html.charters/rmonmib-charter.html

- Cisco RMON home

  http://www.cisco.com/en/US/tech/tk648/tk362/tk560/tsd_technology_support_sub-protocol_home.html

- Cisco NAM product page

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

Packet Capture—More Information

- tcpdump/libpcap home

  http://www.tcpdump.org/

- Vinayak Hegde's Linux Gazette article

  http://linuxgazette.net/issue86/vinayak.html

Syslog—More Information

- Syslog.org

  http://www.syslog.org/

- Syslog logging with PostGres HOWTO

  http://kdough.net/projects/howto/syslog_postgresql/

- Agent Smith explains Syslog

  http://routergod.com/agentsmith/

BGP—More Information

- Cisco BGP home

  http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html

- Slammer/BGP analysis

  http://www.cs.colostate.edu/~massey/pubs/conf/massey_iwdc03.pdf

- Team CYMRU BGP tools

  http://www.cymru.com/BGP/index.html

Traceback—Direct Contact Information

- APNIC—reporting network abuse: spamming and hacking

  http://www.apnic.net/info/faq/abuse/index.html

- RIPE—reporting network abuse: spamming and hacking

  http://www.ripe.net/info/faq/abuse/index.html

- ARIN—network abuse: FAQ

  http://www.arin.net/abuse.html

References

- Product security:
  - Cisco’s product vulnerabilities
    - http://www.cisco.com/en/US/products/products_security_advisories_listing.html
  - Cisco Security Center
    - http://www.cisco.com/security
- ISP essentials:
  - Technical tips for ISPs every ISP should know
    - ftp://ftp-eng.cisco.com/cons/isp/
- Technical tips:
  - Troubleshooting High CPU Utilization on Cisco Routers
    - http://www.cisco.com/warp/public/63/highcpu.html
  - The “show processes” command
    - http://www.cisco.com/warp/public/63/showproc_cpu.html
  - NetFlow performance white paper
    - http://www.cisco.com/en/US/partner/tech/tk812/technologies_white_paper0900aecd802a0eb9.shtml
- Mailing list:
  - cust-security-announce@cisco.com: all Cisco customers should be on this list