Phase 4 – Traceback the Attack

Six Phases to ISP Security Incident Response

- ✓ **Preparation**
- ✓ **Identification**
- ✓ **Classification**
- ✓ **Traceback**
- ✓ **Reaction**
- ✓ **Post Mortem**

Traceback Attacks to their Source

- **Valid IPv4 Source Addresses are Easy.**
  - ✓ **Gets harder with DDOS – where there are a multitude of source addresses.**
- **Spoofed IPv4 Source Addresses are more challenging.**
  - ✓ **Backscatter Traceback technique makes a difference.**
- **Inter-Provider Hand off of the traceback is the big challenge today (end of 2001).**

Traceback Essentials

- **If source prefix is not spoofed:**

  -> Routing table
  -> Internet Routing Registry (IRR)
  -> direct site contact

- **If source prefix is spoofed:**

  -> Trace packet flow through the network
  -> Find upstream ISP
  -> Upstream needs to continue tracing

Traceback Valid IPv4 Source Addresses


```
madrid% whois -h whois.arin.net 64.103.0.0
Cisco Systems, Inc. (NETBLK-CISCO-GEN-6)
  170 West Tasman Drive
  San Jose, CA 95134
  US

  Netname: CISCO-GEN-6
  Netblock: 64.100.0.0 - 64.104.255.255

  Coordinator:
    Huegen, Craig  (CAH5-ARIN)  chuegen@cisco.com
    +1-408-526-8104 (FAX) +1 408 525 2597

  Domain System inverse mapping provided by:

  NS1.CISCO.COM               192.31.7.92
  NS2.CISCO.COM               192.135.250.69
  DNS-SJ6.CISCO.COM              192.31.7.93
  DNS-RTP4.CISCO.COM              192.135.250.70

  Record last updated on 11-Jan-2001.
  Database last updated on 2-Aug-2001 23:12:13 EDT.
```

- **Use Regional Internet Registries (RIRs):**
  - ✓ **Europe: whois.ripe.net**
  - ✓ **Asia-Pac: whois.apnic.net**
  - ✓ **USA and rest: whois.arin.net**

Traceback Valid IPv4 Source Addresses

Cisco.com

```
madrid% whois -h whois.arin.net "as 109"
Cisco Systems, Inc. (ASN-CISCO)
   170 W. Tasman Drive
   San Jose, CA 95134
   US

   Autonomous System Name: CISCOSYSTEMS
   Autonomous System Number: 109

   Coordinator:
      Koblas, Michelle  (MRK4-ARIN)  mkoblas@CISCO.COM
      (408) 526-5269 (FAX) (408) 526-4575

   Record last updated on 20-May-1997.
   Database last updated on 2-Aug-2001 23:12:13 EDT.
```

Also, if domain known: abuse@domain

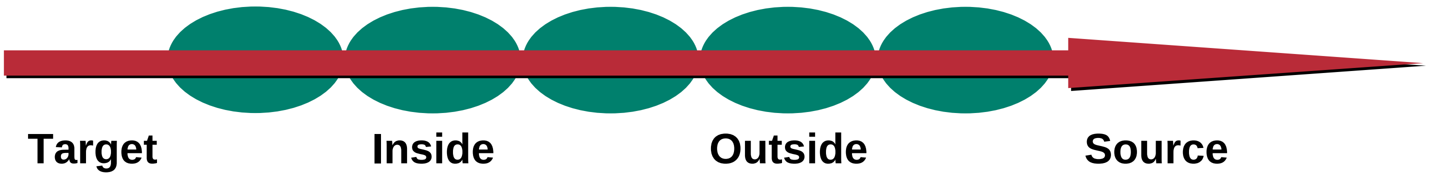
Traceback Spoofed IPv4 Addresses

- **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

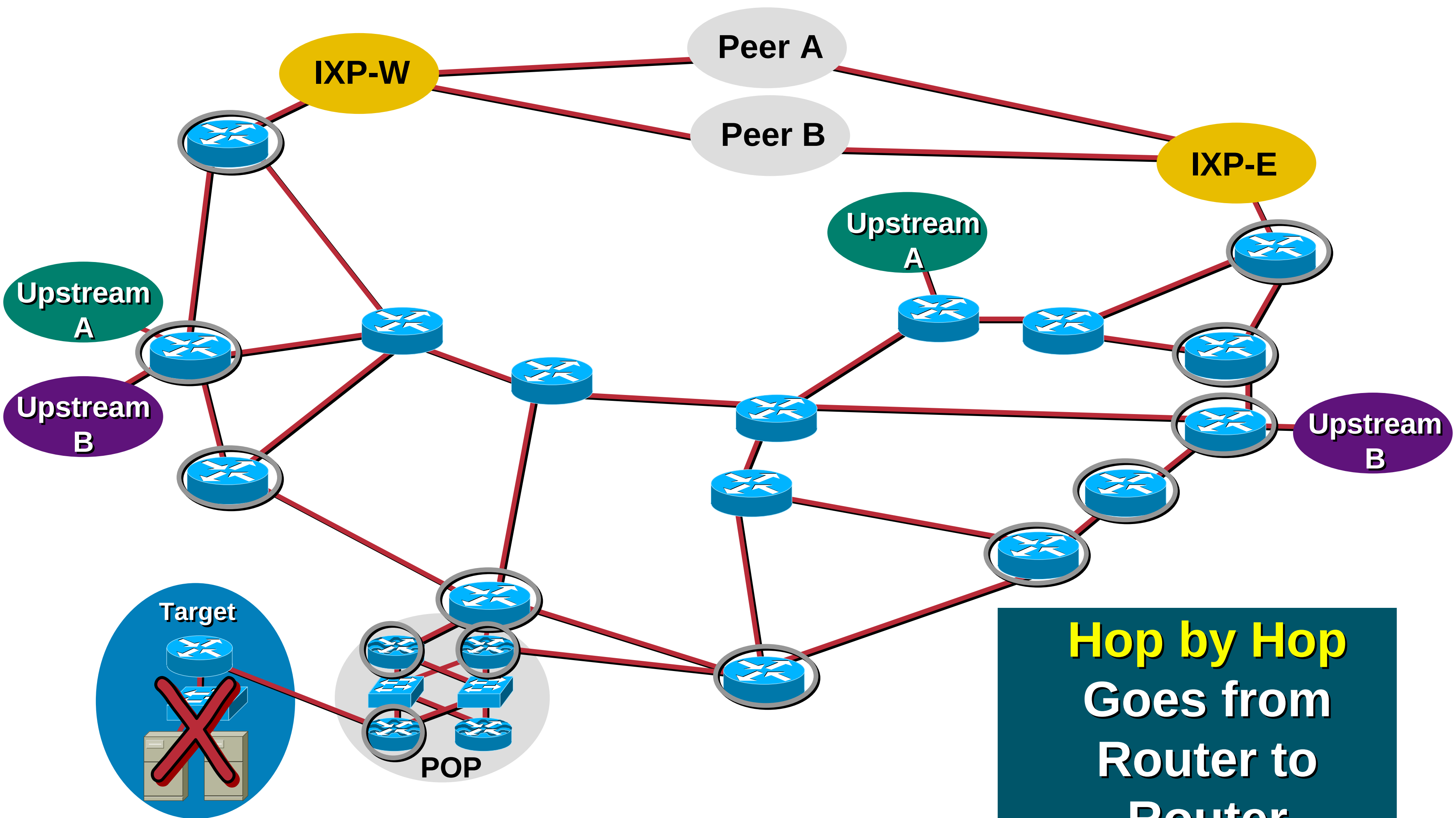
Cisco.com

- 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

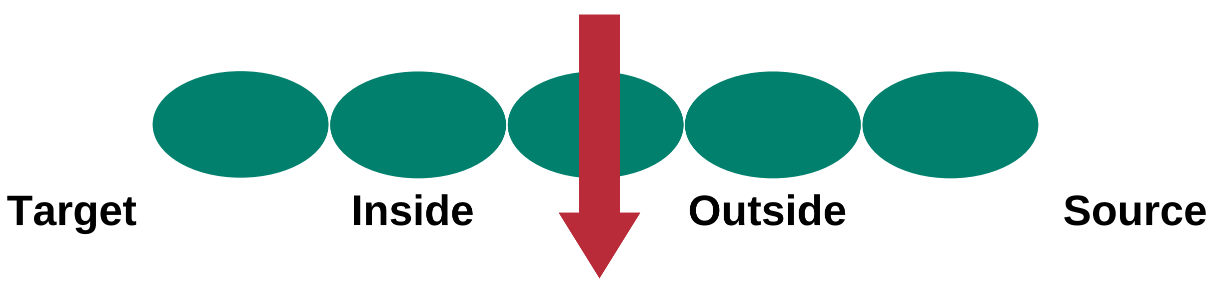
Cisco.com



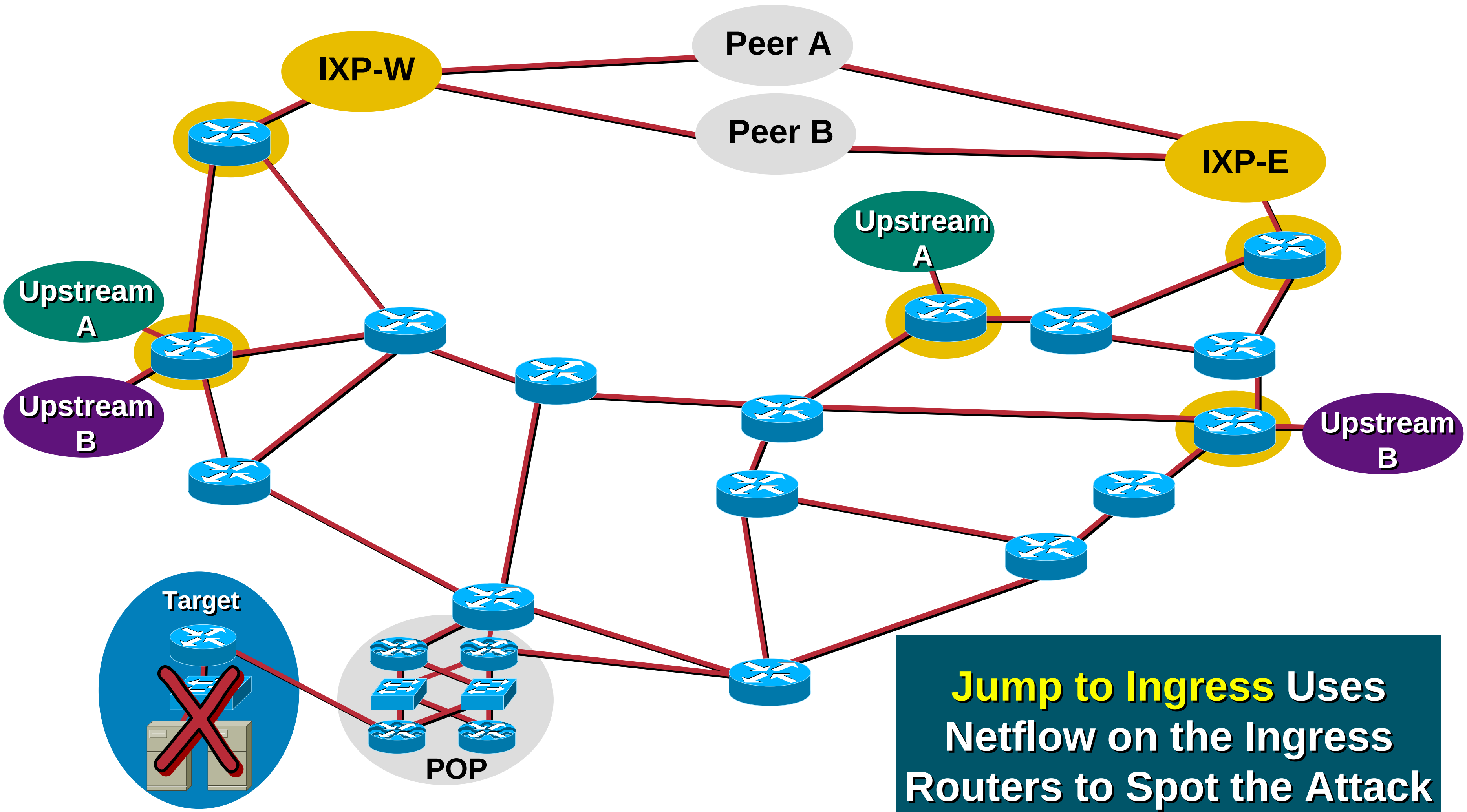
Hop by Hop Goes from Router to Router

Traceback via the Jump to Ingress Technique

- **Jump to ingress tracebacks divides the problem in half**
  - ✓ **Is the attack originating from inside the 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

Traceback Spoofed IPv4 Addresses

- Three techniques
  - ✓ Apply temporary ACLs with log-input and examine the logs (like step 2)
  - ✓ Query Netflow's flow table (if show ip cache-flow is turned on)
  - ✓ Backscatter Traceback Technique

Traceback with ACLs

Cisco.com

```
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

Cisco.com

- 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

Cisco.com

- **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!

Tracing Back with Netflow

- **Routers need Netflow enabled**

Victim

router1#sh ip cache flow | include <destination>

Se1 <source> Et0 <destination> 11 0013 0007 159

…. (lot[illegible]re flows to the same destination)

The flows come from serial 1

Find the upstream router on serial 1

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

Continue on this router

show ip cache flow

Cisco.com

```
router_A#sh ip cache flow
IP packet size distribution (85435 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2728 active, 1368 inactive, 85310 added
  463824 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-X                2      0.0         1  1440      0.0       0.0       9.5
TCP-other        82580     11.2         1  1440     11.2       0.0      12.0
Total:           82582                              11.2       0.0      12.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         132.122.25.60   Se0/0         192.168.1.1     06 9AEE 0007     1
Et0/0         139.57.220.28   Se0/0         192.168.1.1     06 708D 0007     1
Et0/0         165.172.153.65  Se0/0         192.168.1.1     06 CB46 0007     1
```

Protocol

Flow info summary

Flow details

show ip cache verbose flow

Cisco.com

```
router_A#sh ip cache verbose flow
IP packet size distribution (23597 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1323 active, 2773 inactive, 23533 added
  151644 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-other        22210       3.1         1  1440      3.1       0.0      12.9
Total:           22210       3.1         1  1440      3.1       0.0      12.9

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0          216.120.112.114 Se0/0          192.168.1.1     06 00  10       1
5FA7 /0  0                     0007 /0  0     0.0.0.0              1440     0.0
Et0/0          175.182.253.65  Se0/0          192.168.1.1     06 00  10       1
```

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 — Netflow on the GSR is executed and exported from the Line Cards – not the GRP. 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**

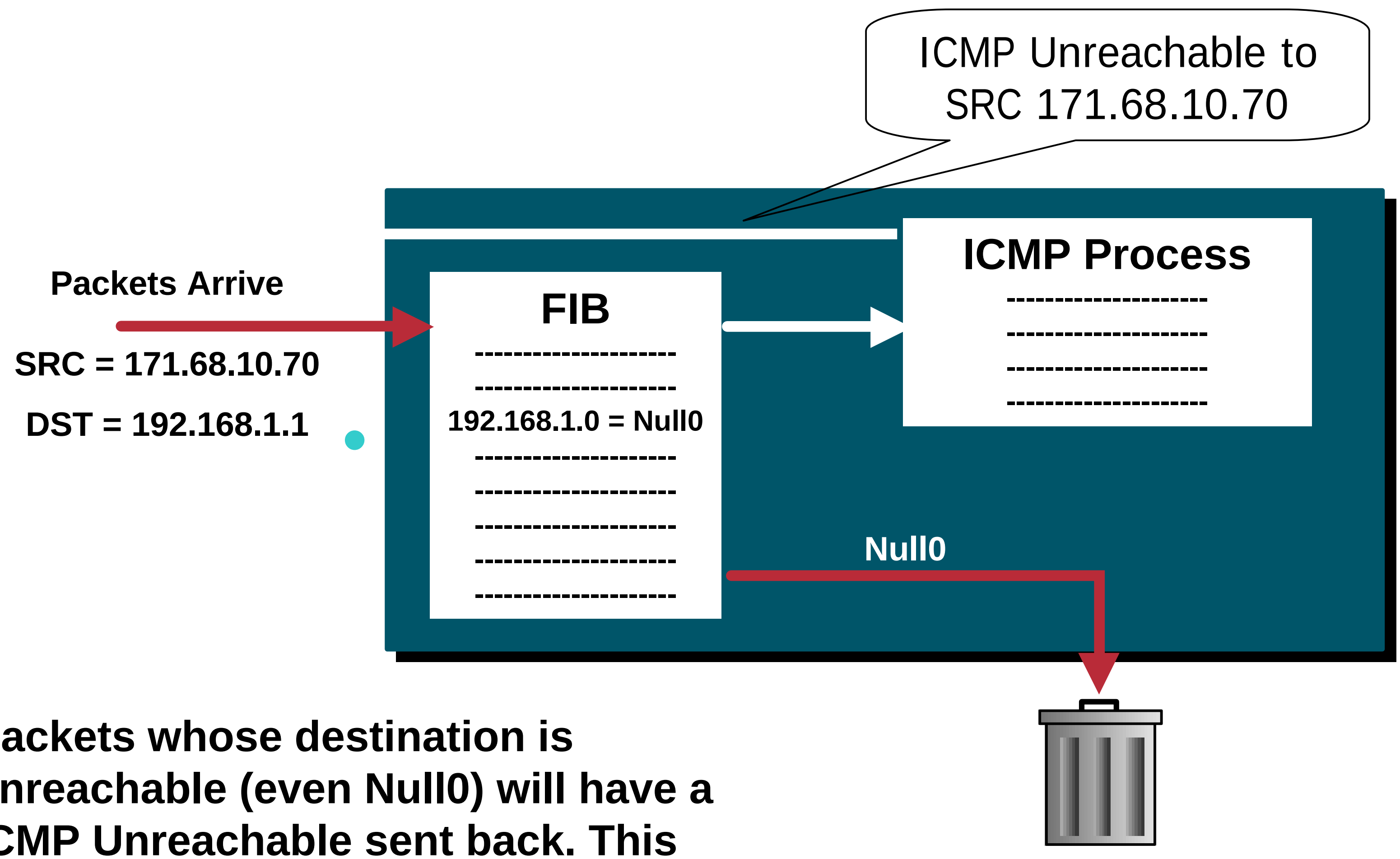
Backscatter Traceback Technique

- **Three key advantages:**
  - ✓ **Reduced Operational Risk to the Network while traceback is in progress.**
  - ✓ **Speedy Traceback**
  - ✓ **Ability to hand off from one ISP to another – potentially tracing back to it's source.**

Backscatter Traceback Technique

- **Created by Chris Morrow and Brian Gemberling @ UUNET as a means of finding the entry point of a spoofed DOS/DDOS.**
  - ✓ http://www.secsup.org/Tracking/
- **Combines the Sink Hole router, Backscatter Effects of Spoofed DOS/DDOS attacks, and remote triggered Black Hole Filtering to create a traceback system that provides a result within 10 minutes.**

Backscatter Traceback Technique



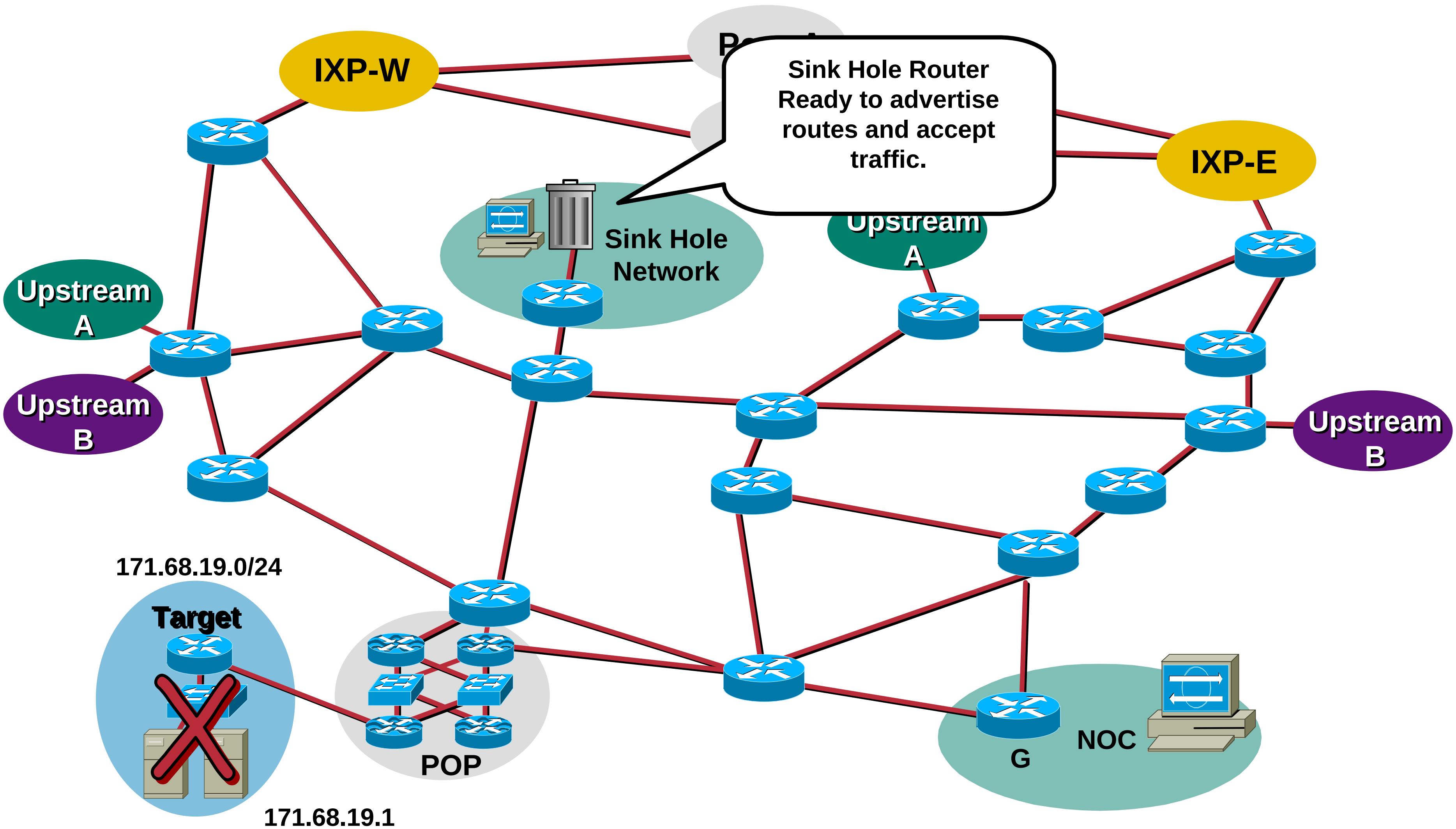
Packets whose destination is unreachable (even Null0) will have a ICMP Unreachable sent back. This "unreachable noise" is backscatter.

Backscatter Traceback *Preparation*

1. **Sink Hole Router/Network connected to the network and ready to classify the traffic. Like before, BGP Route Reflector Client, device to analyze logs, etc.**

   - ✓ **Can use one router to do both the route advertisement and logging OR break them into two separation routers – one for route advertisement and the other to accept/log traffic**
   - ✓ **Can be used for other Sink Hole functions while not using the traceback technique.**
   - ✓ **Sink Hole Router can be a iBGP Route Reflector into the network.**

Backscatter Traceback ***Preparation***



Backscatter Traceback ***Preparation***

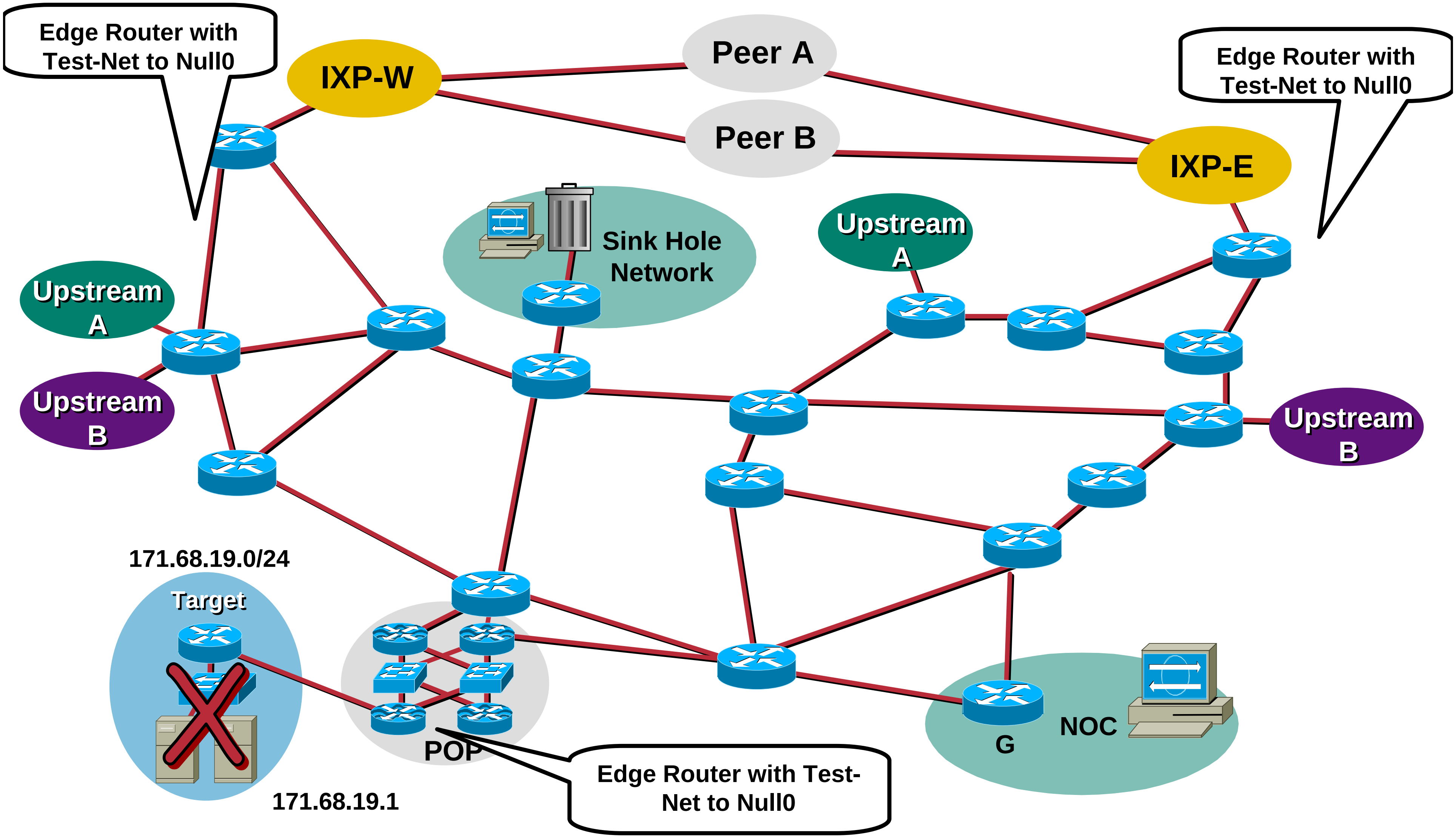

```
router bgp 31337
!
! set the static redistribution to include a route-map so we can filter
! the routes somewhat... or at least manipulate them
! redistribute static route-map static-to-bgp
!
! add a stanza to the route-map to set our special next hop
!
 route-map static-to-bgp permit 5
 match tag 666
 set ip next-hop 172.20.20.1
 set local-preference 50
 set origin igp
```

Backscatter Traceback *Preparation*

2. **All edge devices (routers, NAS, IXP Routers, etc) with a static route to Null0. The Test-Net is a safe address to use (192.0.2.0/24) since no one is using it.**

   - ✓ Cisco: **ip route 172.20.20.1 255.255.255.255 Null0**
   - ✓ **Routers also need to have ICMP Unreachables working. If you have ICMP Unreachables turned off (i.e. *no ip unreachables* on a Cisco), then make sure they are on.**
   - ✓ **If ICMP Unreachable Overloads are a concern, use a ICMP Unreachable Rate Limit (i.e. *ip icmp rate-limit unreachable* command on a Cisco).**

Backscatter Traceback *Preparation*

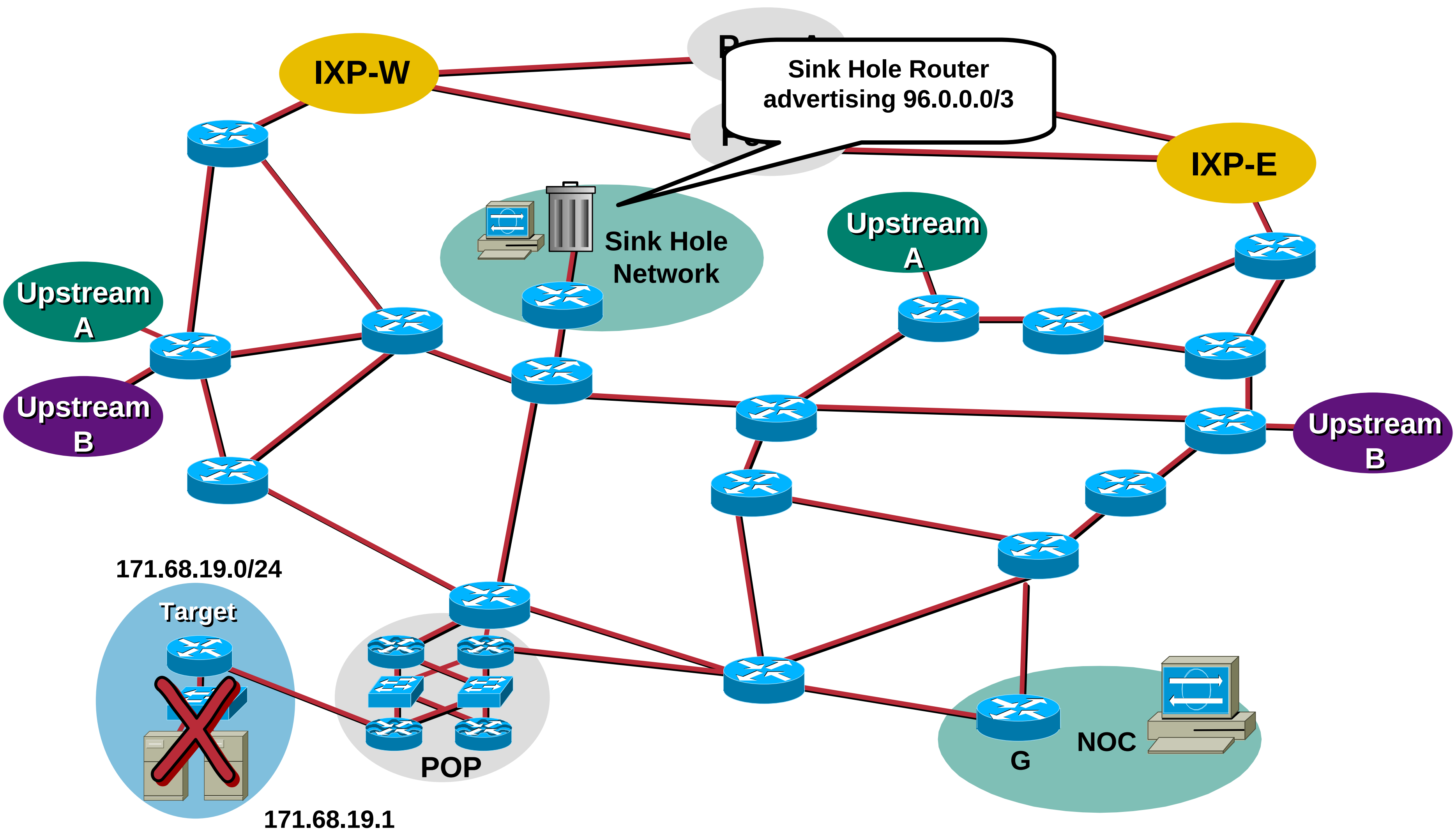


Backscatter Traceback *Preparation*

3. **Sink Hole Router advertising a large block of un-allocated address space with the BGP no-export community and BGP Egress route filters to keep the block inside. 96.0.0.0/3 is an example.**

   - **Check with IANA for unallocated blocks:**
     `www.iana.org/assignments/ipv4-address-space`
   - **BGP Egress filter should keep this advertisement inside your network.**
   - **Use BGP *no-export* community to insure it stays inside your network.**

Backscatter Traceback *Preparation*



Backscatter Traceback ***Activation***

- **Activation happens when an attack has been identified.**
- **Basic Classification should be done to see if the backscatter traceback will work:**
  - ✓ **May need to adjust the advertised block.**
  - ✓ **Statistically, most attacks have been spoofed using the entire Internet block.**

Backscatter Traceback *Activation*

Cisco.com

1. Sink Hole Router Advertises the /32 under attack into iBGP with.

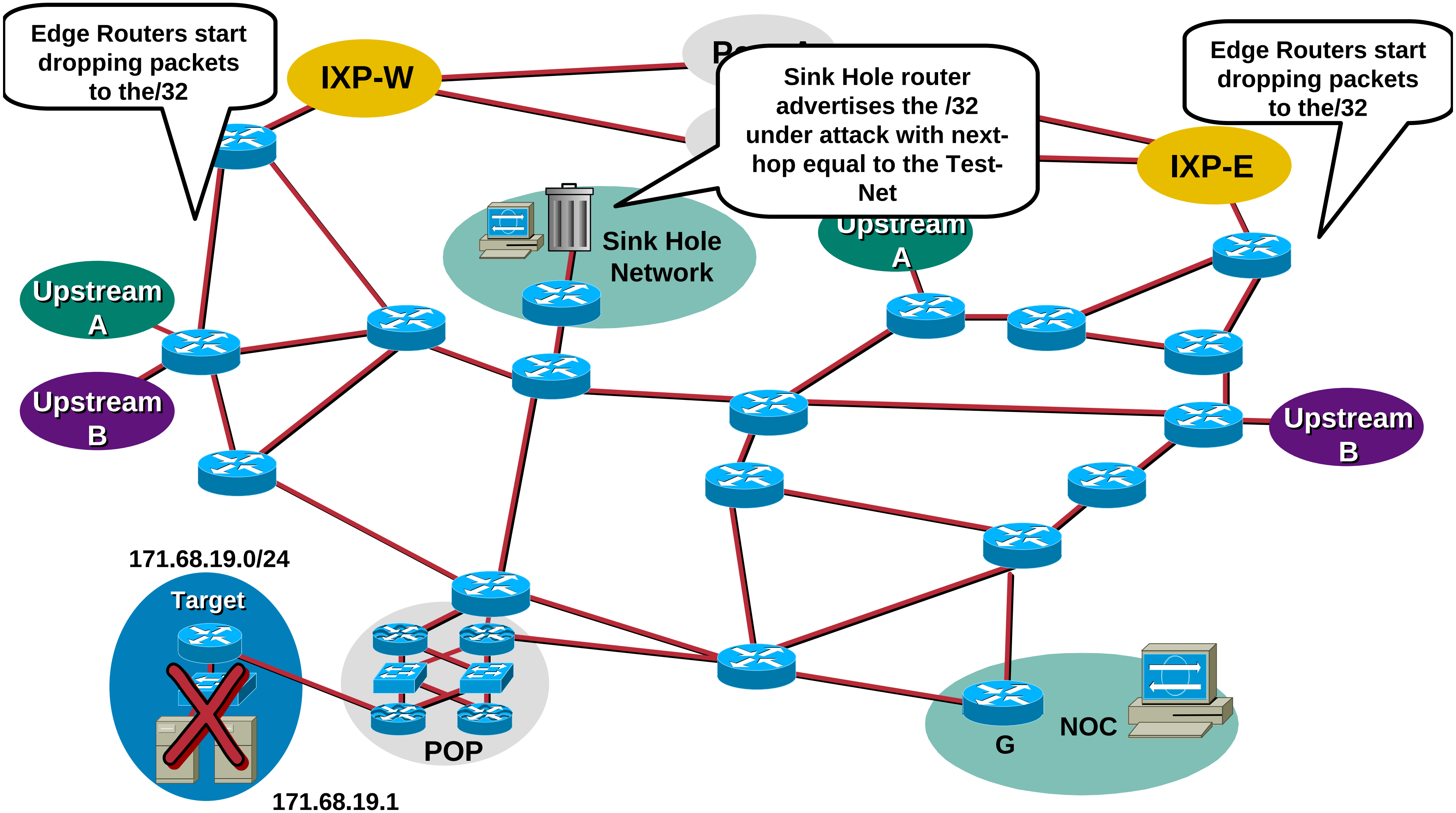
Advertised with a static route with the “666” tag:

```
ip route victimip 255.255.255.255 Null0 tag 666
```

The static triggers the routers to advertise the customer’s prefix

Backscatter Traceback *Activation*

Cisco.com



Backscatter Traceback *Activation*

Cisco.com

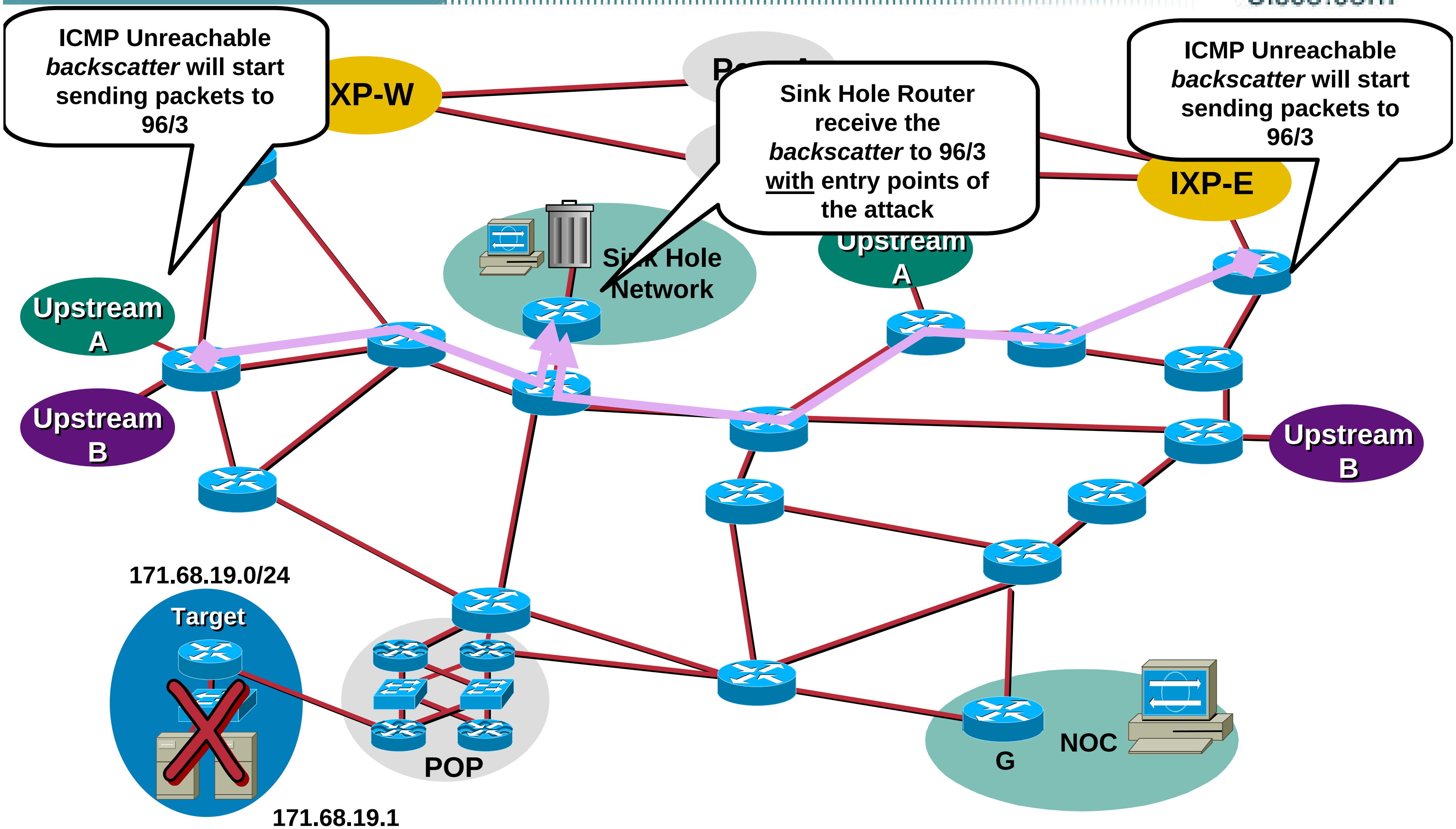
2. **Black Hole Filtering is triggered by BGP through out the network. Packets to the target get dropped. ICMP Unreachable Backscatter starts heading for 96.0.0.0/3.**

   Access list is used on the router to find which routers are dropping packets.

```
access-list 101 permit icmp any any unreachables log

access-list 101 permit ip any any
```

Backscatter Traceback ***Activation***



Backscatter Traceback ***Activation***

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.47.251.104 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.70.92.28 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.222.127.7 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.96.223.54 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.14.21.8 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.105.33.126 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.77.198.85 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18 -> 96.50.106.45 (3/1), 1 packet

Questions

- **Pulling down all the traffic into a Sink Hole could be very dangerous.**
  - ✓ **Yes. Make sure you've integrated in the network so when it melts down, it will not impact the network.**
- **Advertising large chunks of address space (I.e. 64/8) to do the backscatter traceback could be dangerous.**
  - ✓ **Murphy's Law of Networking – Layered checks should be used – Egress BGP filtering + no-export community.**