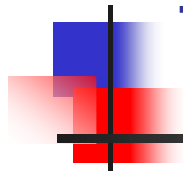
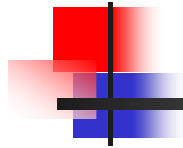


# ISP Security - Real World Techniques



Version 1.0



- Brian W Gemberling [brian@uu.net](mailto:brian@uu.net)
- Christopher L. Morrow [chris@UU.NET](mailto:chris@UU.NET)
- Barry R. Greene [bgreene@cisco.com](mailto:bgreene@cisco.com)



## Objective

---

- Empower ISPs to deploy vendor independent security incident techniques that will provide a foundation for inter-NOC cooperation to traceback the attacks to their source.



## Take Note

---

- There are no magic knobs, grand security solutions, or super vendor features that will solve the ISP Security problem.
- Likewise, there is no rocket science involved. Just hard work that is within all ISP's grasp.
- What follows are tools and techniques that might or might not work for you.

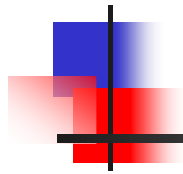


# Agenda

---

- Six Phases of how a ISP Works a Security Incident
- Foundation Techniques
- Digression on the Six Phases
- URLs

# Six Phases of How and ISP Responds to a Security Incident





## ISP Security Response

---

- ISP's Operations Team response to a security incident can typically be broken down into six phases:
  - Preparation
  - Identification
  - Classification
  - Traceback
  - Reaction
  - Post Mortem



## ISP Security Response

---

- Preparation: All the work the ISP does to prepare the network, create the tools, test the tools, develop the procedures, train the team, and practice.
  - Perhaps the most important phase of how a ISP responds to a security incident.
- Identification – How do you know you or your customer is under attack?





## ISP Security Response

---

- Classification – Understanding the type of attack and what damage is it causing.
- Traceback – From where is the attack originating?
- Reaction – Doing something to counter the attack – even if you choose to do nothing.
- Post Mortem – Analyzing what just happened. What can be done to build resistance to the attack happening again.



# Foundation Techniques

---



## Foundation Techniques

---

- Classification and Traceback ACLs
- Black Hole Filtering
- Sink Hole/Black Hole Route Server
- Backscatter Traceback Technique



## Classification and Traceback ACLs

---

- Most common technique used to tweak a router into a pseudo packet sniffer.
  - An Access List (ACL) with a series of permit statements are used to view into the traffic flow.
  - Access List Entry (ACE) counters are used to find which protocol types are potential culprits.
  - Once the protocol type is suspected, another permit ACL with log statements is used to capture some of the packet characteristics.



## Classification and Traceback ACLs

---

- 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
```



## Classification and Traceback ACLs

---

- 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)
```



## Classification and Traceback ACLs

---

- *Classification ACLs* are applied as close to the customer as possible.
  - Mainly on the customer's ingress interface to the ISP with an output ACL.
- Traceback ACLs are usually applied hop by hop – finding the ingress interface of the flow and working up to the next hop.



## Classification and Traceback ACLs

---

- Traceback spoofed source IP addresses using ACLs are 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





## Classification and Traceback ACLs

---

- 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*)



## Classification and Traceback 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
```



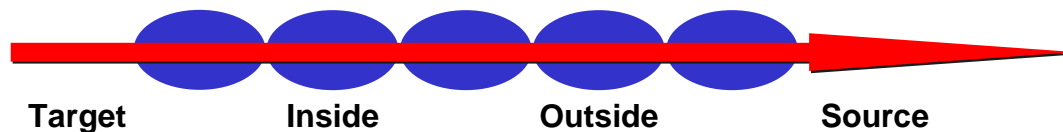
## Classification and Traceback ACLs

---

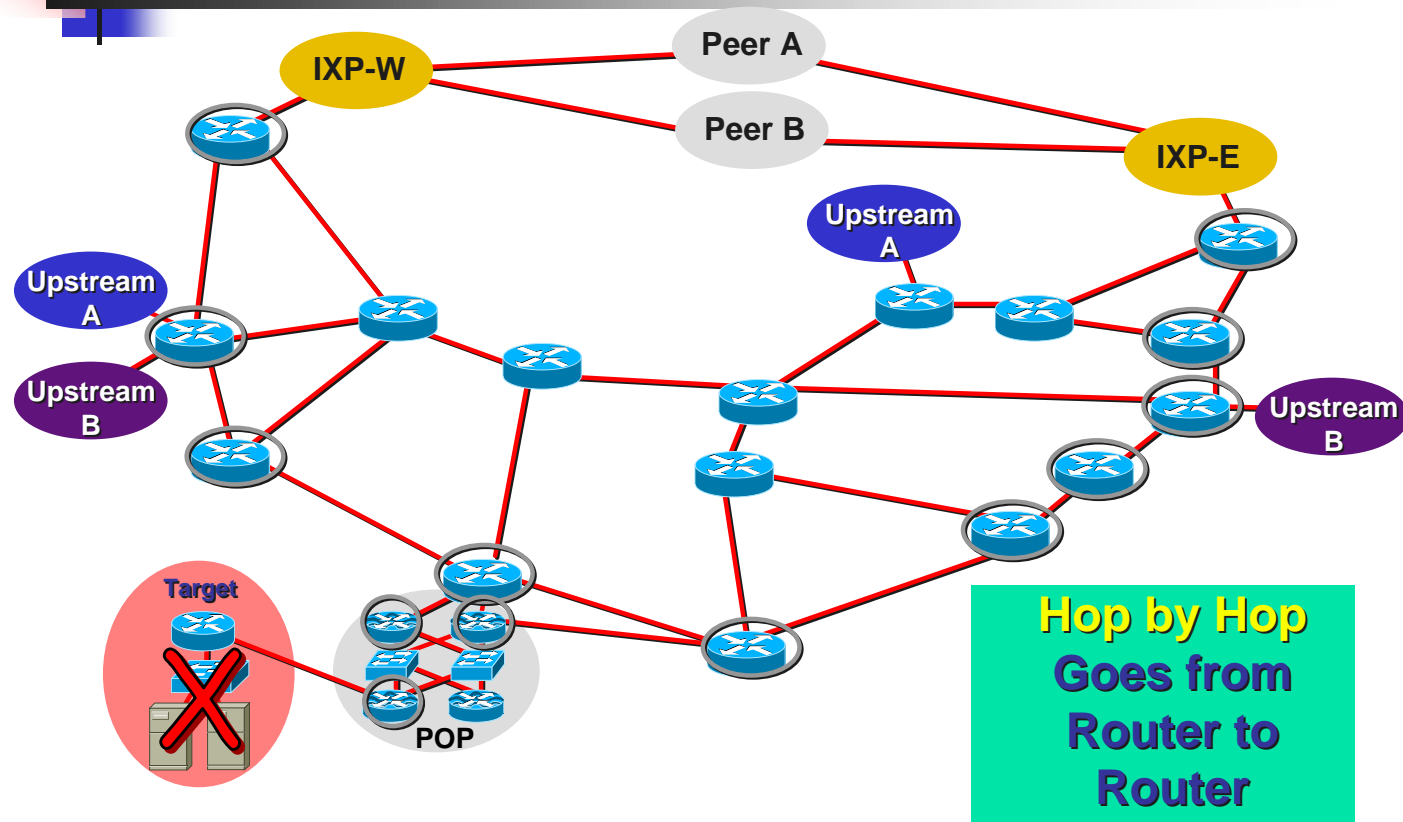
- Validate the capture with *show access-list 170*; make sure it the packets we counted
- Check the log with *show logging* for addresses:
  - %SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.212.72 (Serial0 \*HDLC\*) -> 198.133.219.25 (0/0), 1 packet
  - %SEC-6-IPACCESSLOGDP: list 170 permit icmp 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

# 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





## Classification and Traceback ACLs

---

- See the following URLs for vendor details:
  - <http://www.cisco.com/warp/public/707/22.html>
  - [http://www.juniper.net/techcenter/app\\_note/350001.html](http://www.juniper.net/techcenter/app_note/350001.html)



## Foundation Techniques

---

- Classification and Traceback ACLs
- Black Hole Filtering
- Sink Hole/Black Hole Route Server
- Backscatter Traceback Technique



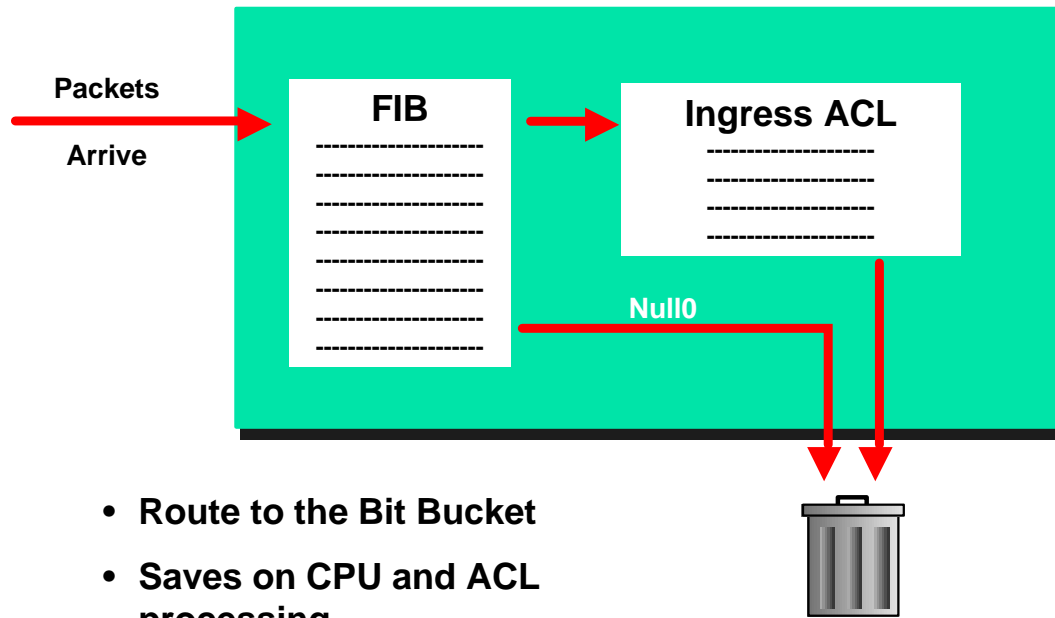
## Black Hole Filtering

---

- *Black Hole Filtering* or *Black Hole 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 (depending on the forwarding ASIC).
- Used for years as a means to "black hole" unwanted packets.



# Black Hole Filtering



## Remotely Triggered Black Hole Filtering



---

- A simple static route and BGP will allow an ISP to trigger network wide black holes as fast as iBGP can update the network.
- This provides ISPs a tool that can be used to respond to security related events or used for DOS/DDOS Backscatter Tracebacks.



## Remotely Triggered Black Hole Filtering - Preparation

---

1. Select a small block that will not be used for anything other than black hole filtering. Test Net (192.0.2.0/24) is optimal since it should not be on the Net and is not really used.
2. Put a static route with Test Net – 192.0.2.0/24 to Null 0 on every router on the network.
3. Prepare a BGP speaking router that will be used to announce the network to be Black Holed (see config example on next slide).

# Remotely Triggered Black Hole Filtering - Preparation

```
router bgp 109
.
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 50
set community no-export
set origin igp
!
Route-map static-to-bgp permit 20
```

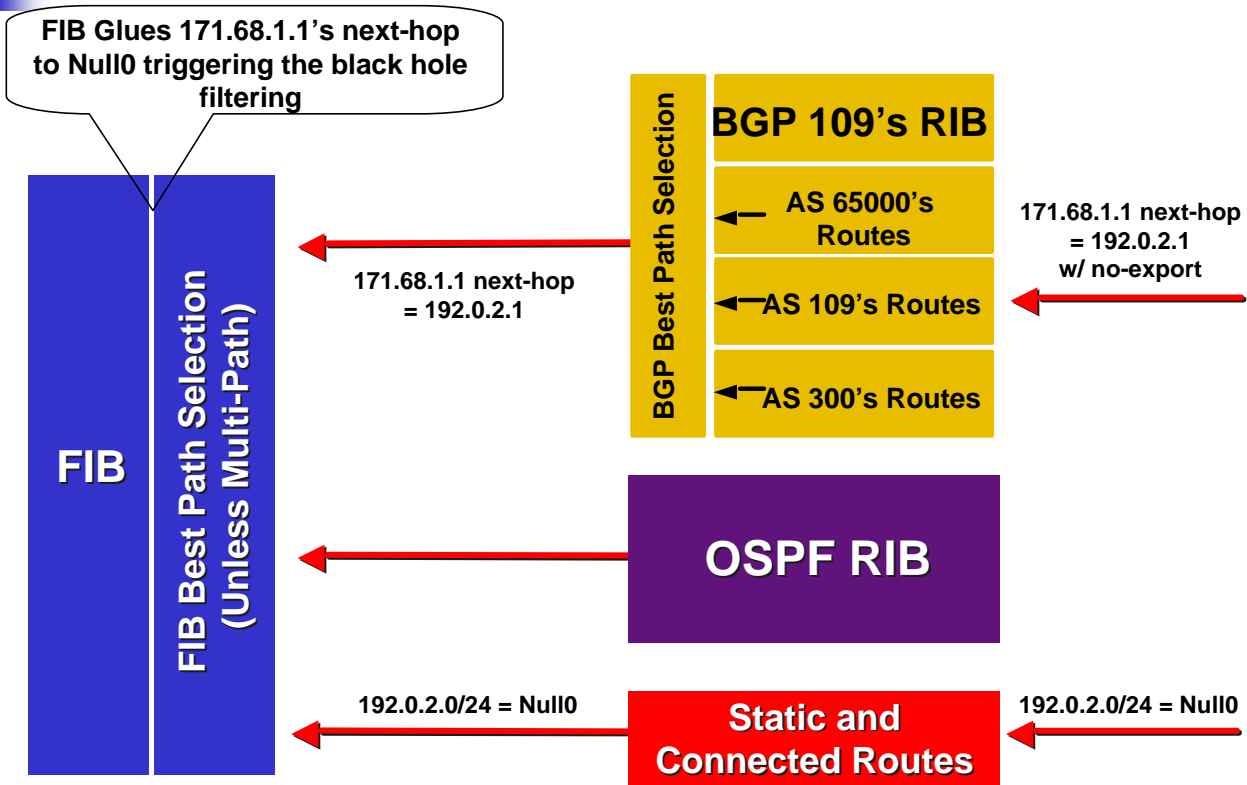
# Remotely Triggered Black Hole Filtering - Activation



1. ISP adds a static route of the destination address they wish to black hole to the advertising router. The static is added with the "tag 66" to keep it separate from other statics on the router.  

```
ip route 171.68.1.1 255.255.255.255 Null0 Tag 66
```
2. BGP Advertisement goes out to all BGP speaking routers.
3. Router hear the announcement, glues it to the existing static on the route, and changes the next-hop for the BGP advertised route to Null0 – triggering black hole routing.

# Remotely Triggered Black Hole Filtering - Activation



# Remotely Triggered Black Hole Filtering - Activation

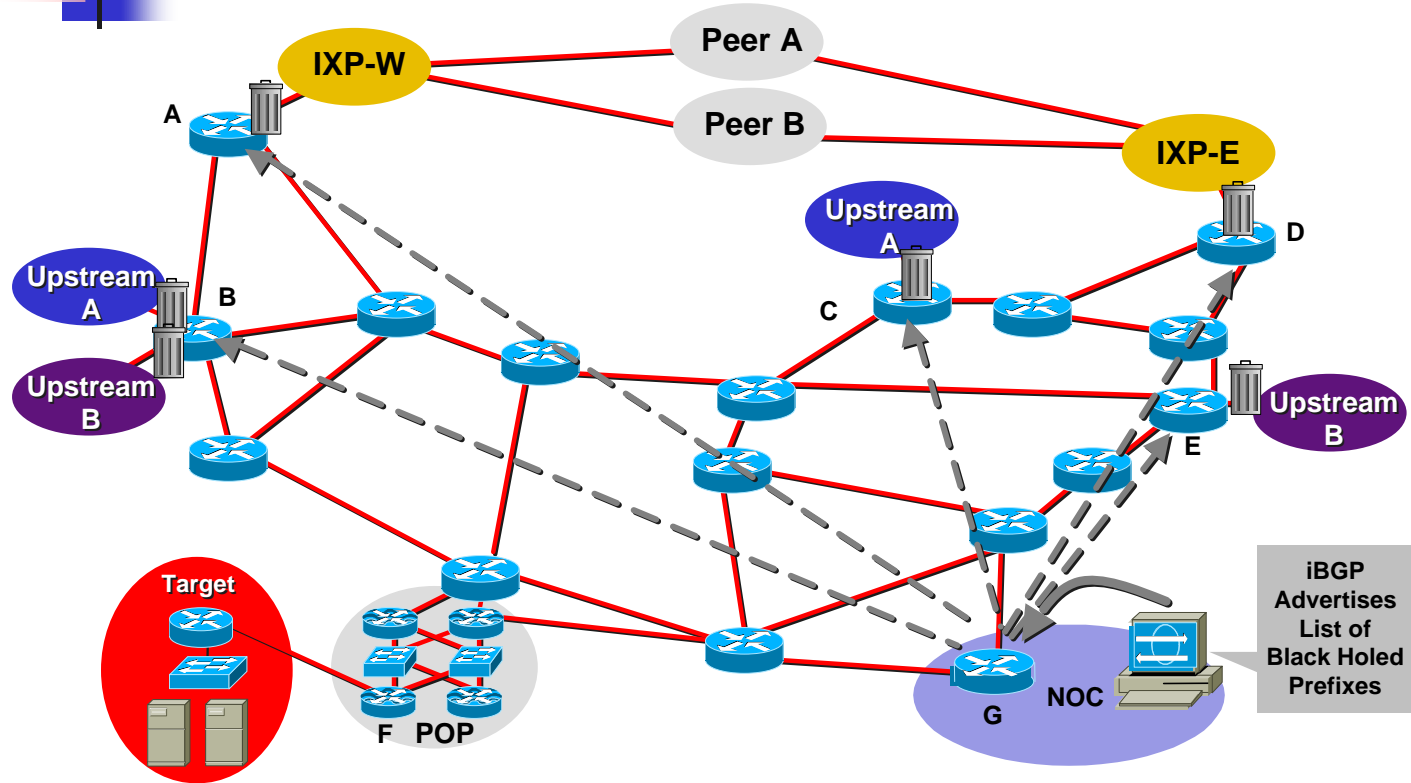
BGP Sent – 171.68.1.0/24 Next-Hop = 192.0.2.1

Static Route in Edge Router – 192.0.2.1 = Null0

171.68.1.0/24 = 192.0.2.1 = Null0

Next hop of 171.68.1.0/24 is now equal to Null0

# Remotely Triggered Black Hole Filtering - Activation







## Gotchas with Black Hole Filtering

---

- Routers were designed to forward traffic, not drop traffic.
- ASIC Based Forwarding can drop traffic at line rate.
- Processor Based Forwarding can have problems dropping large amounts of data.
- Remember the old shunt technique ....

## Gotchas with Black Hole Filtering

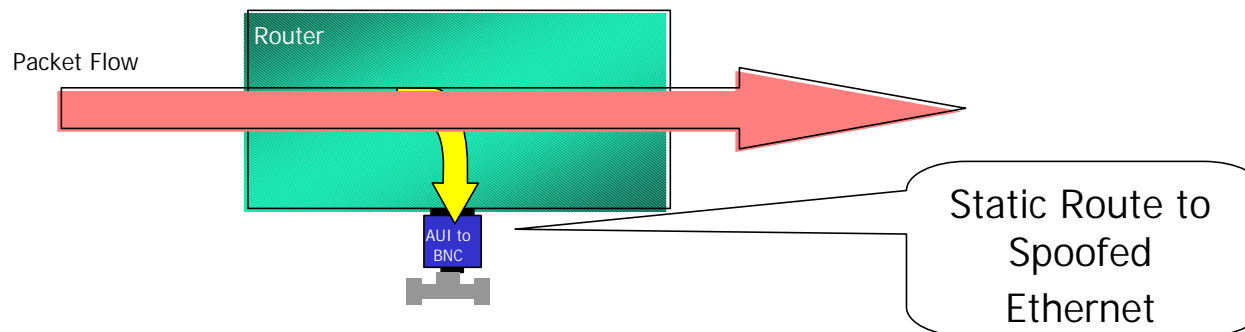
- Back in the days when this was in the core of the Internet .....



- All “drops” to Null0 were process switched.
- Fast Drops fixed the problem for a while, but traffic loads increased to the to where they could not drop at line rate anymore.
- Bottomline – Software based forwarding routers (any vendor) can forward faster then they can drop.

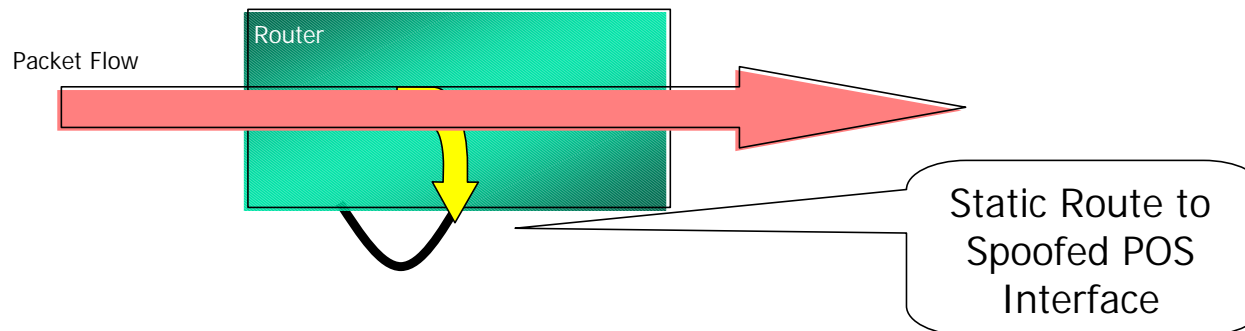
## Black Hole Shunt

- Black Hole *Shunts* are used to forward traffic out a spoofed interface.
  - Classic Example: AUI/BNC Transceiver with a T connector. A static MAC address is used with a static route.



## Black Hole Shunt

- Some ISPs used Black Hole Shunts during Code Red.
  - Routers that injected Default Sucked all traffic to them.





## Foundation Techniques

---

- Classification and Traceback ACLs
- Black Hole Filtering
- Sink Hole/Black Hole Route Server
- Backscatter Traceback Technique

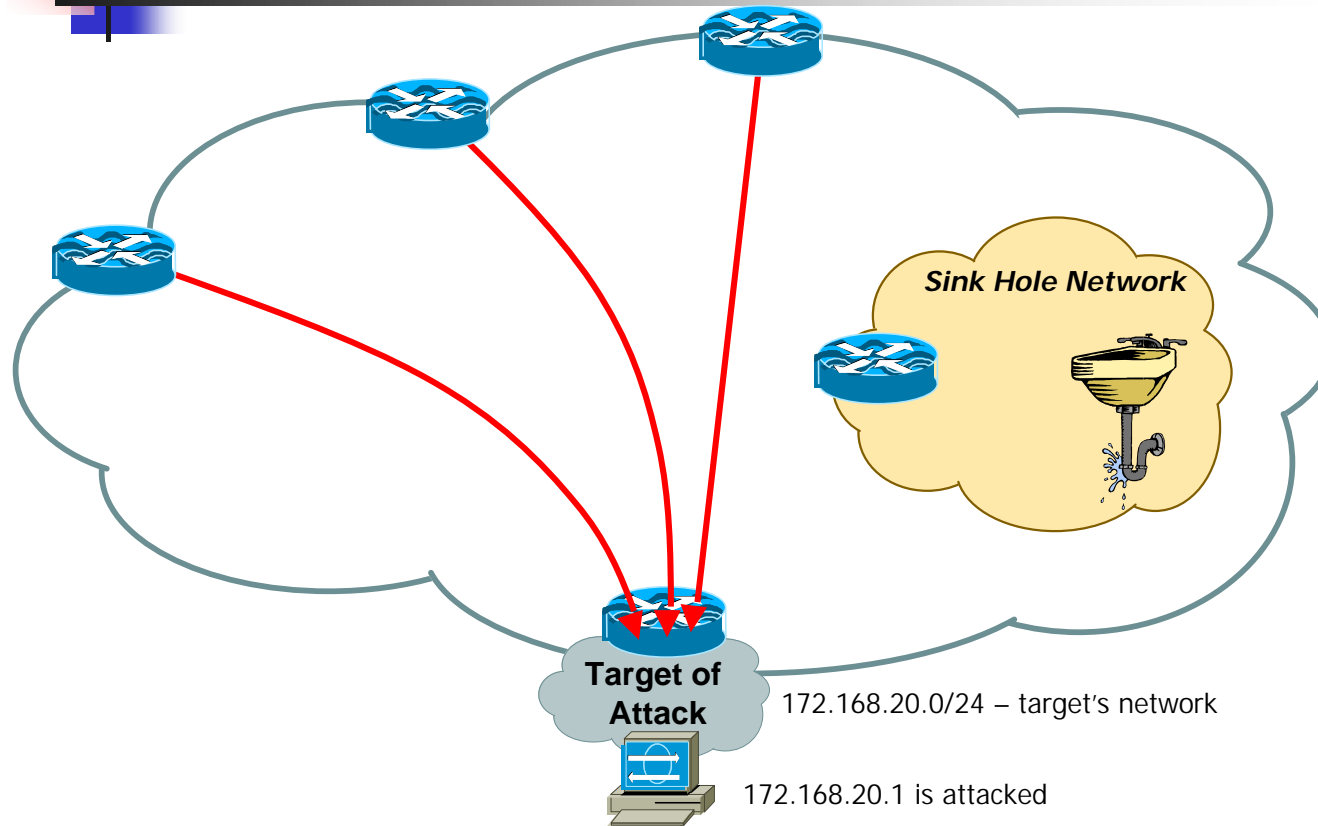


## Sink Hole Routers/Networks

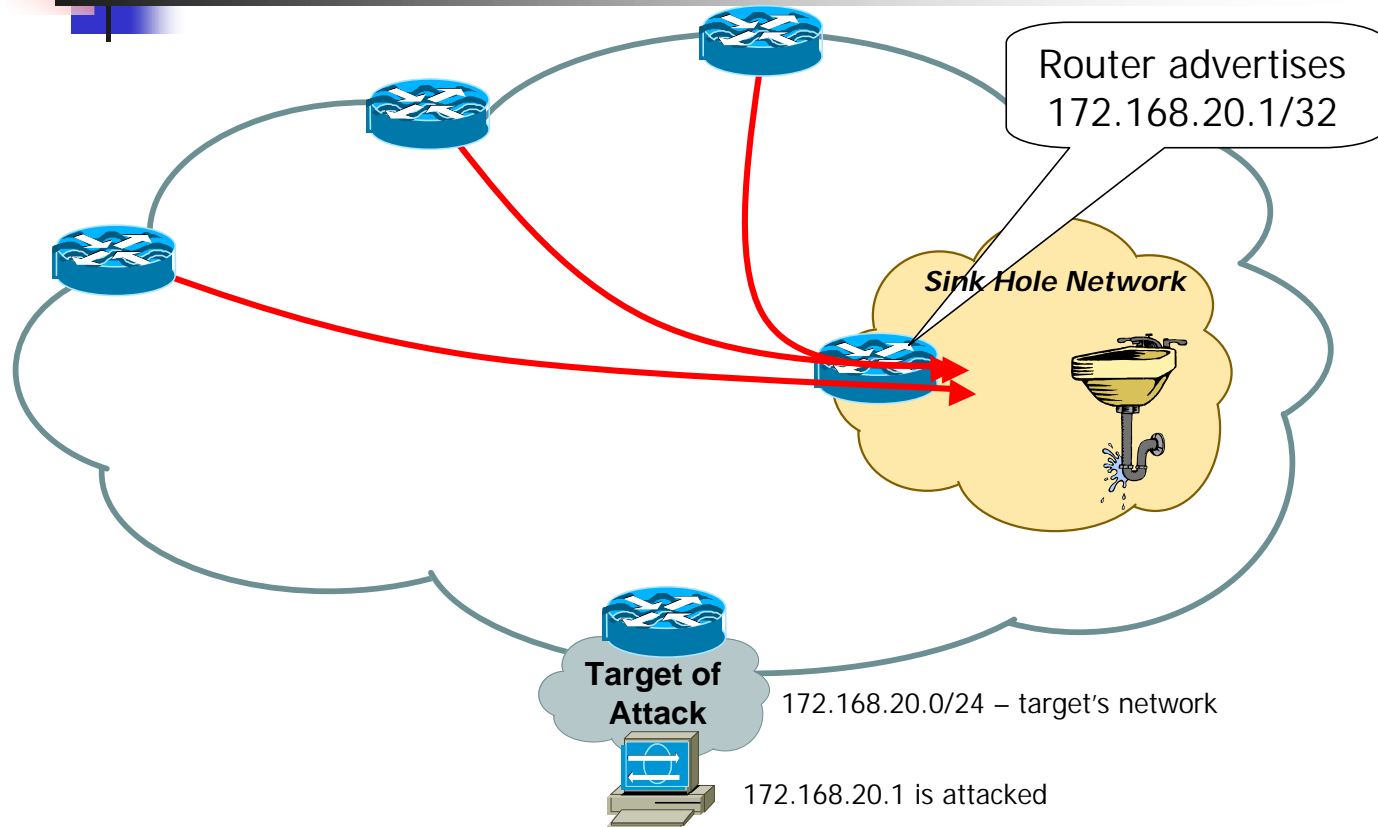
---

- Sink Holes are a the network equivalent of a honey pot.
  - BGP speaking Router or Workstation that built to *suck in* attacks.
  - Used to redirect attacks away from the customer – working the attack on a router built to withstand the attack.
  - Used to monitor *attack noise, scans*, and other activity (via the advertisement of default)

# Sink Hole Routers/Networks



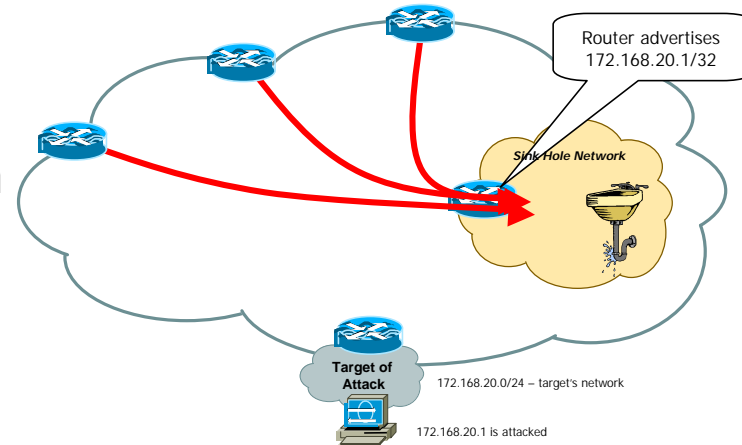
# Sink Hole Routers/Networks





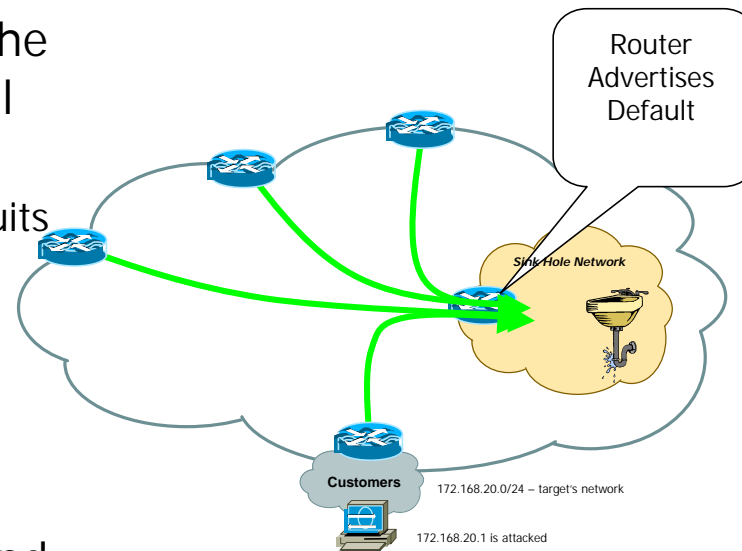
# Sink Hole Routers/Networks

- Attack is pulled off customer and your aggregation router.
- Can now do classification ACLs, Flow Analysis, Sniffer Capture, Traceback, etc.
- Objective is to minimize the risk to the network while working the attack incident.



# Sink Hole Routers/Networks

- Advertising Default from the Sink Hole will pull down all sort of *junk* traffic.
  - Customer Traffic when circuits flap.
  - Network Scans
  - Failed Attacks
  - Code Red/NIMDA
  - Backscatter
- Can place tracking tools and IDA in the Sink Hole network to monitor the noise.





## Foundation Techniques

---

- Classification and Traceback ACLs
- Black Hole Filtering
- Sink Hole/Black Hole Route Server
- Backscatter Traceback Technique



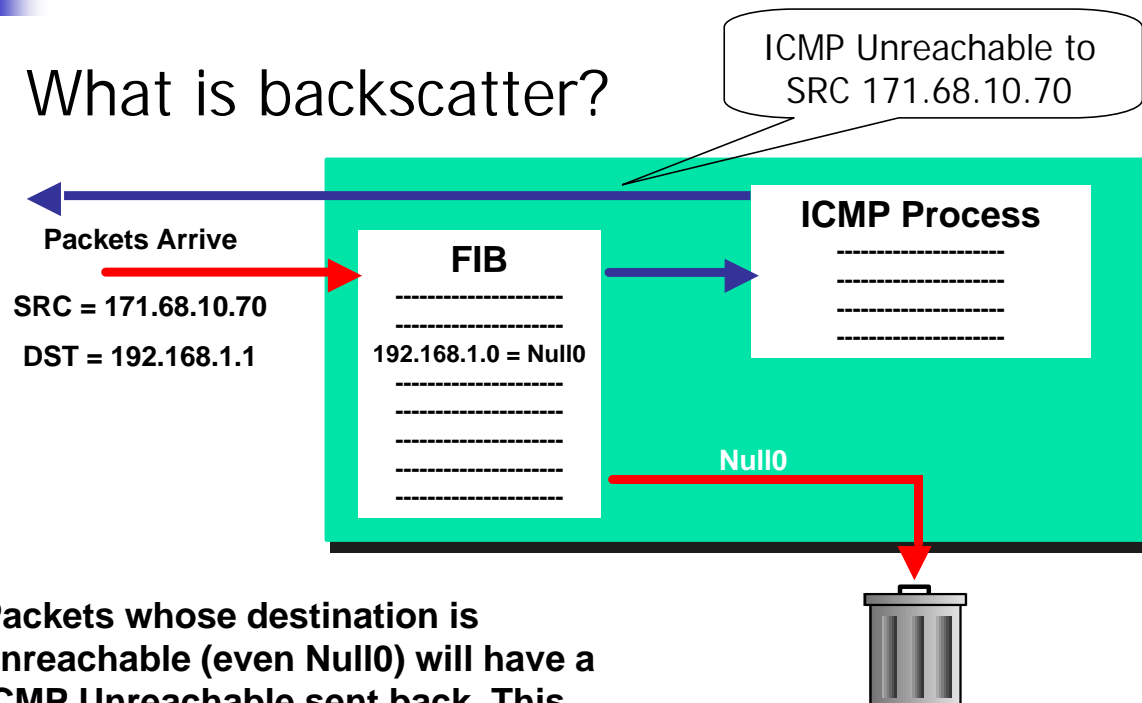
## Backscatter Traceback Technique

---

- 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

- What is backscatter?



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

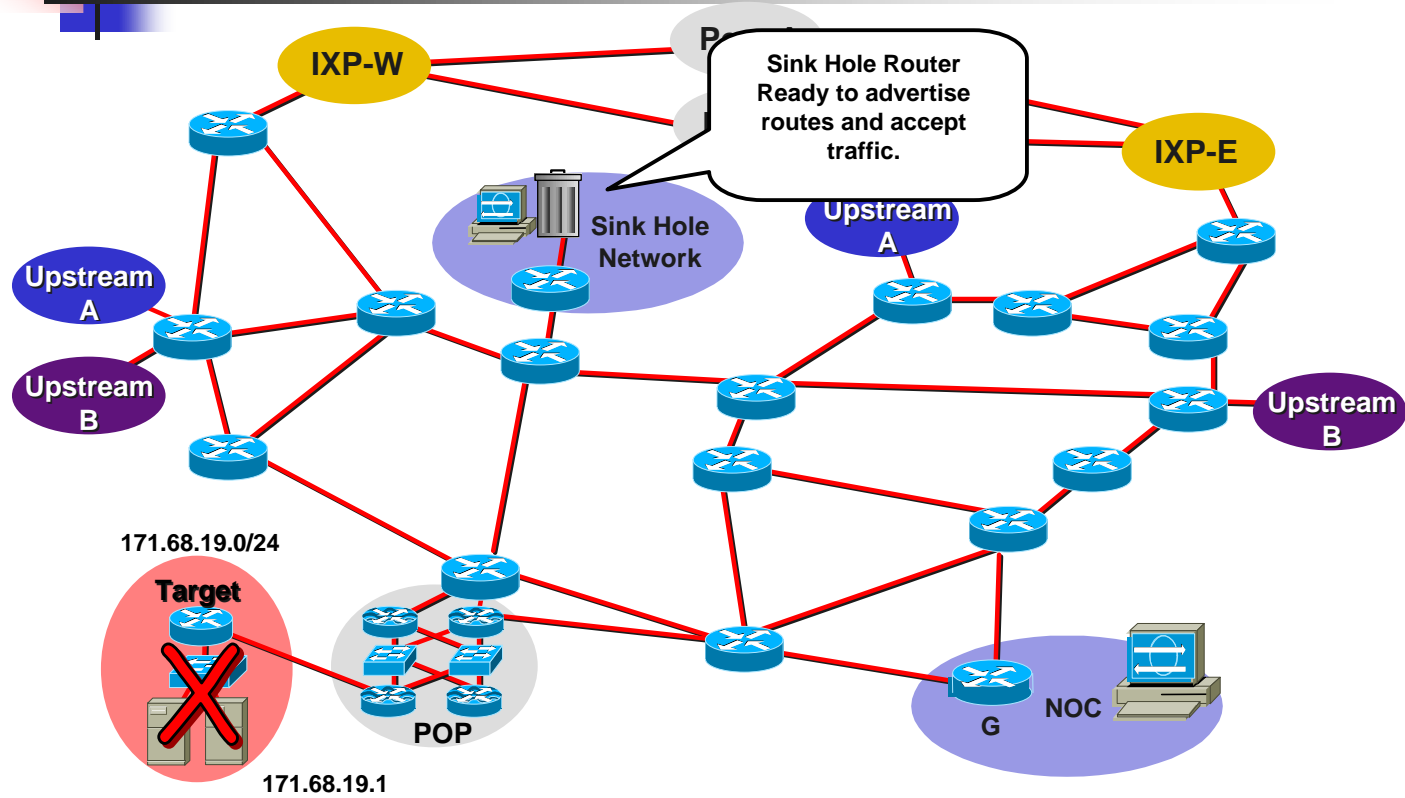


## Backscatter Traceback *Preparation*

---

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 Activation

---

```
!  
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 Activation

---

```
# Setup the bgp protocol to export our special policy, like redistributing, NOTE: "XXX"
# is the IBGP bgp group... we don't want to send this to customers do we?
#
set protocols bgp group XXX export BlackHoleRoutes
#
# Now, setup the policy option for BlackHoleRoutes, like a route-map if static route
# with right tag, set local-pref low, internal, no-export can't leak these or Tony Bates
# will have a fit, and set the nexthop to the magical next-hop.
#
set policy-statement BlackHoleRoutes term match-tag666 from protocol static tag 666
set policy-statement BlackHoleRoutes term match-tag666 then local-preference 50
set policy-statement BlackHoleRoutes term match-tag666 then origin igp
set policy-statement BlackHoleRoutes term match-tag666 then community add no-
export
set policy-statement BlackHoleRoutes term match-tag666 then nexthop 172.20.20.1
set policy-statement BlackHoleRoutes term match-tag666 then accept
```



## Backscatter Traceback *Preparation*

---

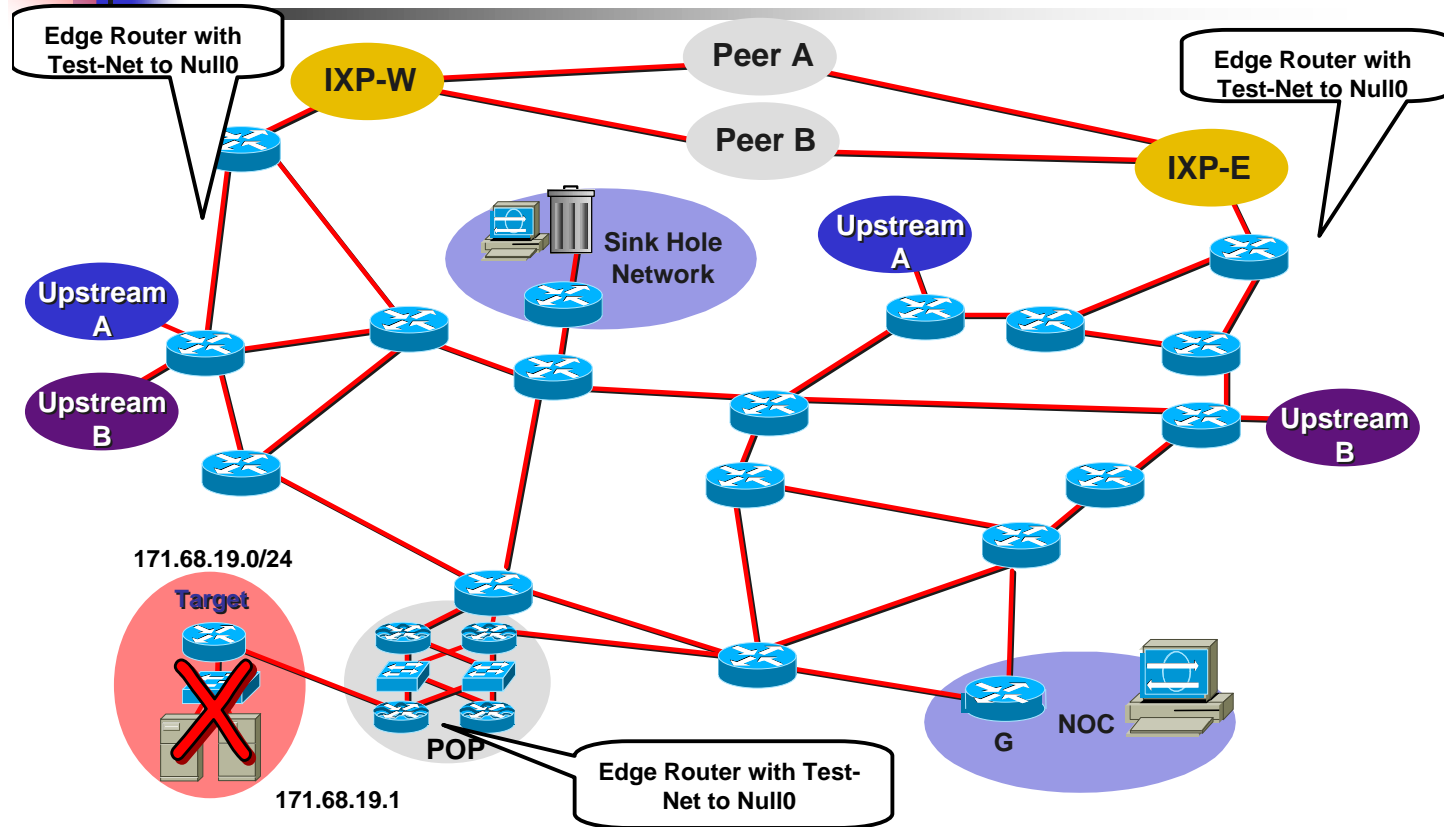
2. All edge devices (routers, NAS, IXP Routers, etc) with a static route to Null0. The Test-Net is a safe address to use (192.0.2.0/24) since no one is using it.

**Cisco:** `ip route 172.20.20.1 255.255.255.255 Null0`

**Juniper:** `set routing-options static route 172.20.20.1/32 reject install`

- Routers also need to have ICMP Unreachables working. If you have ICMP Unreachables turned off (i.e. *no ip unreachable* 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



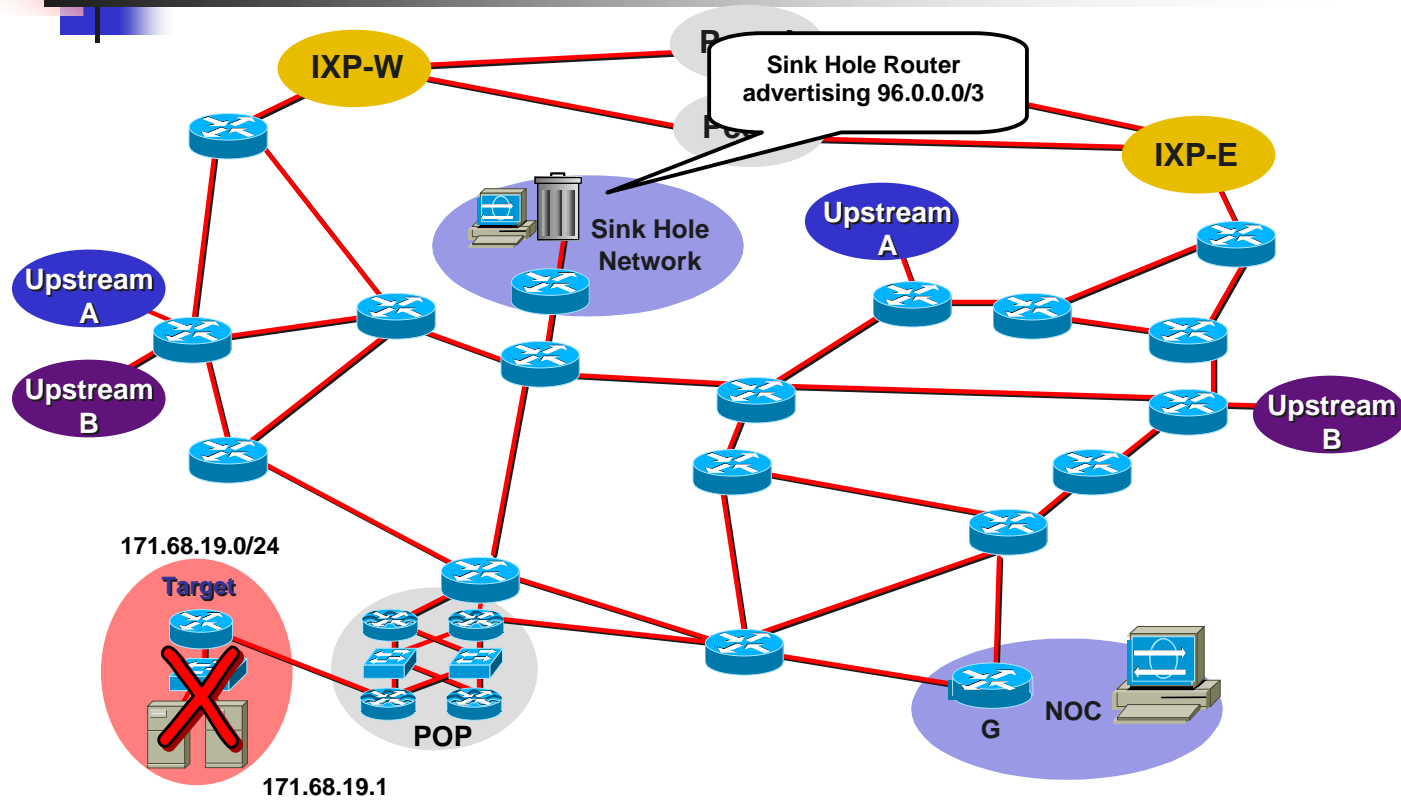


## Backscatter Traceback *Preparation*

---

3. Sink Hole Router advertising a large block of unallocated 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](http://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.



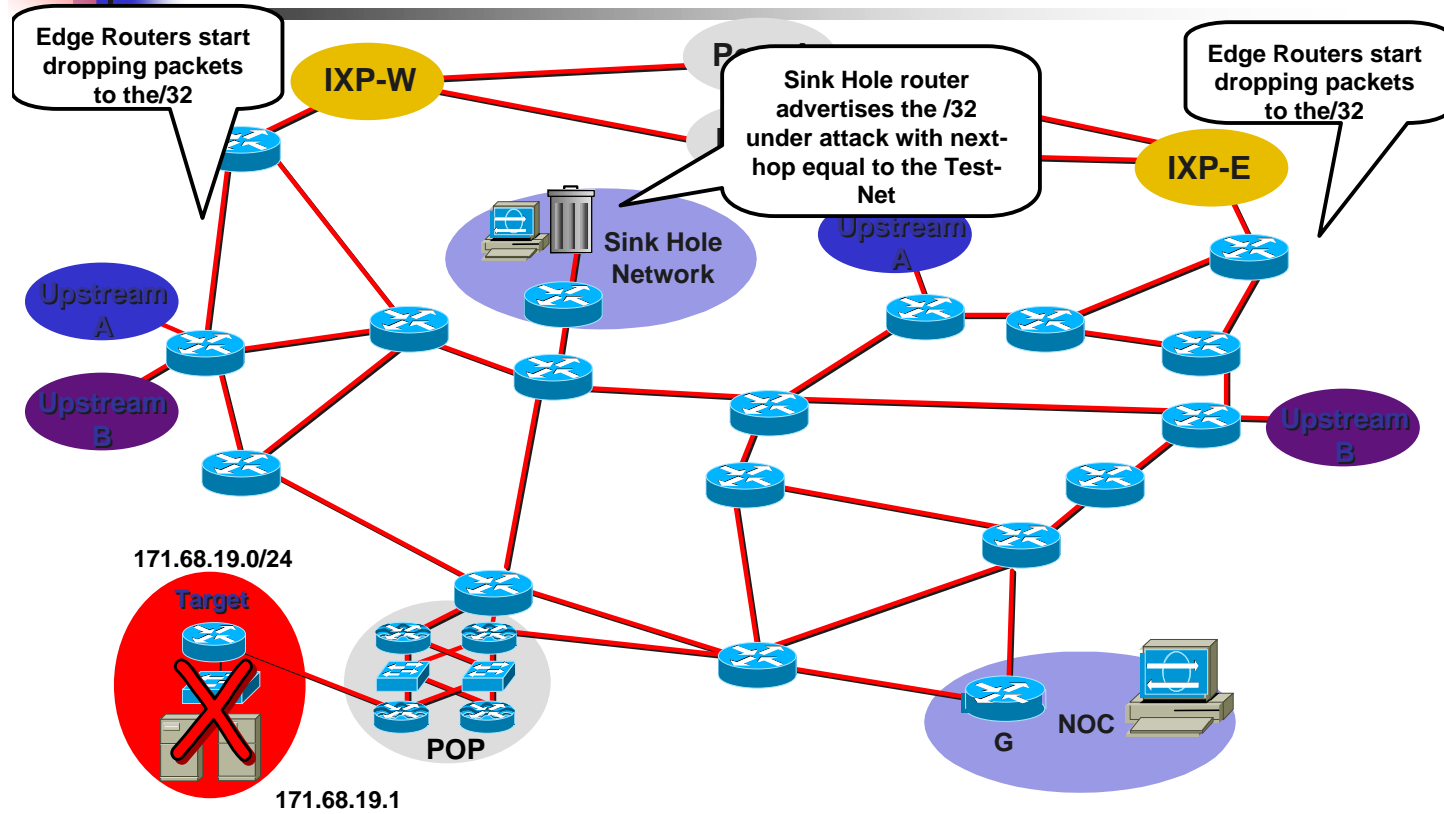
## Backscatter Traceback Activation

---

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
```
  - or
  - ```
set routing-options static route victimip/32 discard tag 666
```
  - The static triggers the routers to advertise the customer's prefix

# Backscatter Traceback Activation





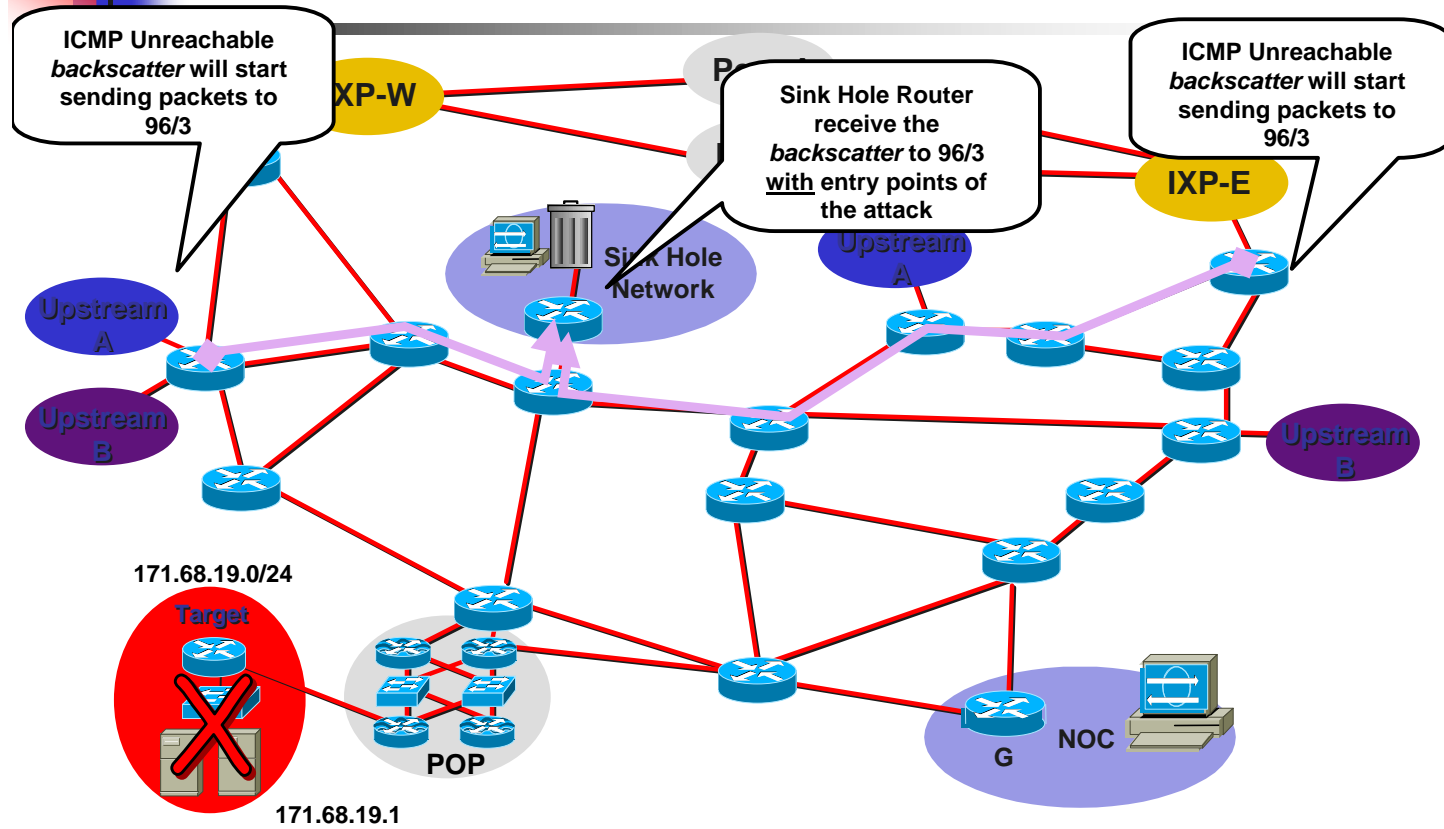


## Backscatter Traceback Activation

---

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 unreachable 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



## ISP Security Response

---

- ISP's Operations Team response to a security incident can typically be broken down into six phases:
  - Preparation
  - Identification
  - Classification
  - Traceback
  - Reaction
  - Post Mortem



Be Prepared

---



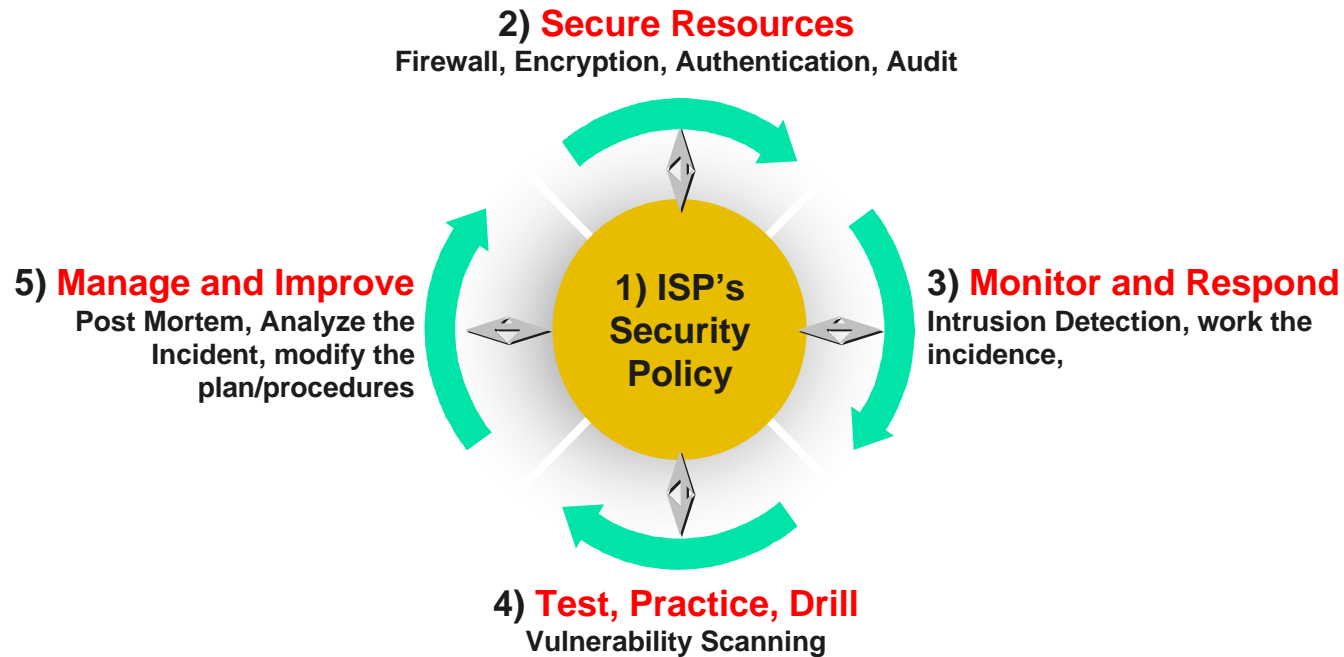
# Preparation

---

- 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.

# What Do ISPs Need to Do?

***Security incidents are a normal part of an ISP's operations!***



# 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







## Preparation

---

- It is imperative that an ISP's operations team prepare.
  - Contacts for all ISPs who you inter-connect (peers, customers, and upstreams)
  - Document your policies. Will you help your customers? Will you classify the attacks? Will you traceback the attacks? Will you drop the attacks on your infrastructure?



## Preparation

---

- Prepare you Tools!
  - Do you have your ACLs created?
  - Do you have your scripts created?
  - Have you built and tested your *Sink Hole* and *Backscatter* tools?



## Preparation

---

- Test your Tools before you really need to use them!
  - Have you tried putting a classification ACL on various parts of your network?
  - Have you tested your scripts to insure they will work?
  - Have you simulated attacks?

# 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





## Preparation

---

- Audit your network configs.
  - Secure the Router/Switch
  - Secure the Routing Protocol
  - Secure the Network



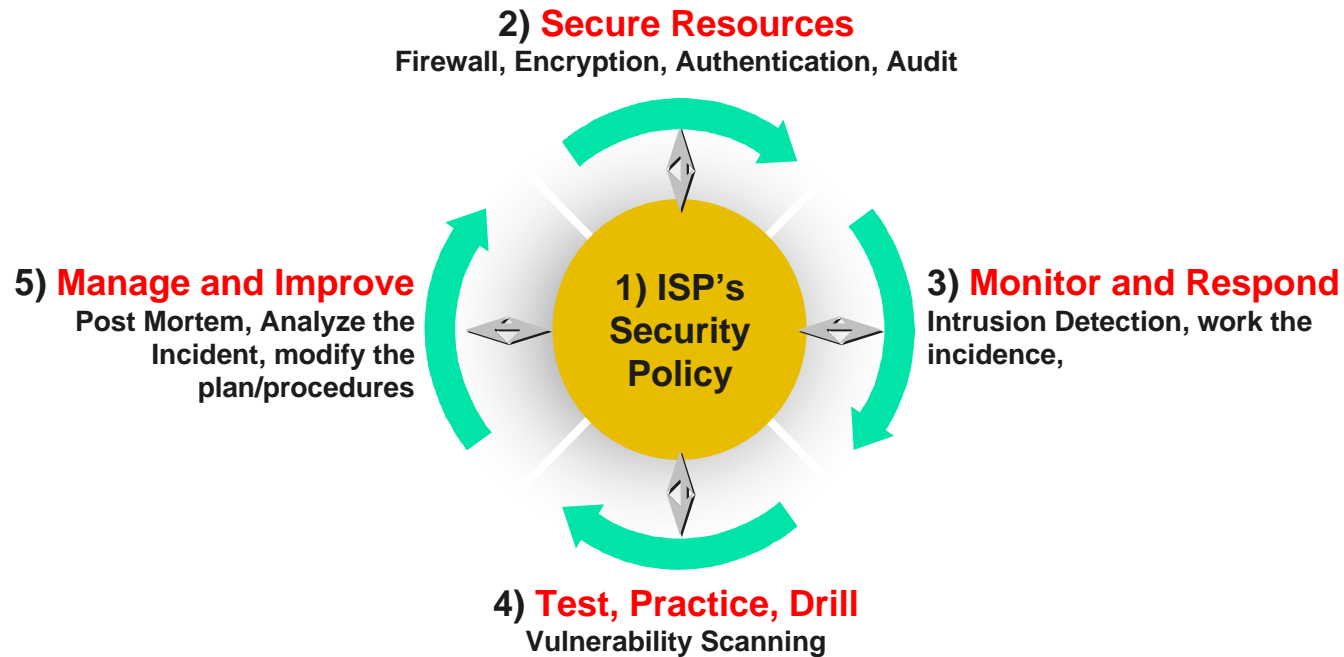
## Preparation

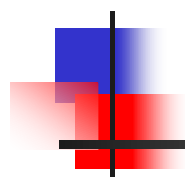
---

- Know your Equipment and Infrastructure:
  - Know the Performance Envelop of all your equipment (routers, switches, workstation, etc). You need to know what your equipment is really capable of doing. If you cannot do it your self, make is a purchasing requirement.
  - Know the capabilities of your network. If possible, test it. Surprises are not kind during a security incident.

# What Do ISPs Need to Do?

***Security incidents are a normal part of an ISP's operations!***





# DOS/DDOS Identification





## 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



## Identifying an Attack

---

- When are we your customers 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



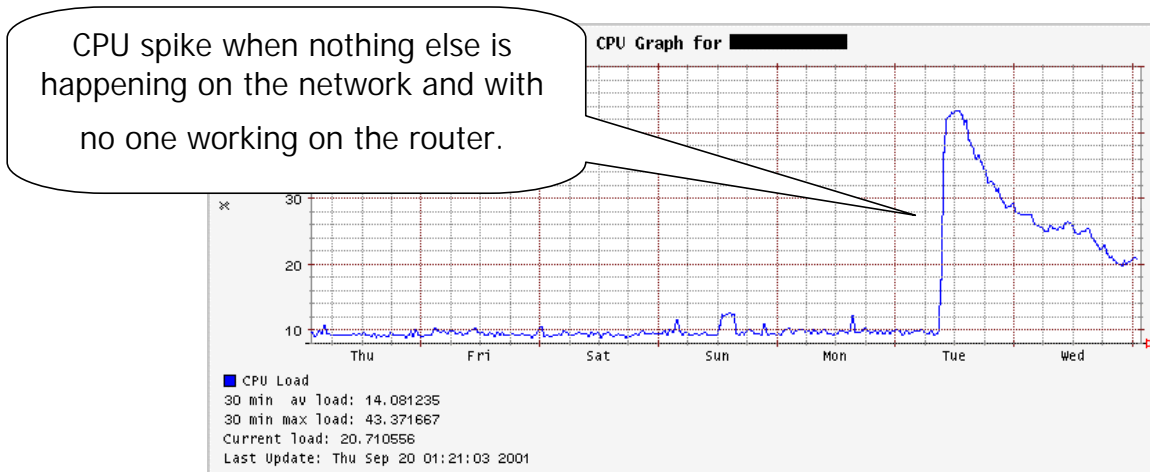
## Identifying an Attack

---

- When are you being attack?
  - NOC Alerts – is a problem in the network, a surge in traffic, a killer app, or someone attacking your network?

# Identifying an Attack

- SNMP Data abortion can signal a network problem *or* a security incident.





## Identifying an Attack

---

- What about those Intrusion Detection Systems (IDS)?
  - Try them.
  - Sink Hole Network is a good place to put them (sucks in all the junk and lets the IDS sort it out).
  - Always be on the lookout for a new tool, trick, feature, or capability.



# DOS/DDOS Classification

---



## 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



## Classifying an Attack

---

- Classification is critical to your reaction. If you are not sure of the characteristics of the attack, your reaction to the attack could add to the problem.





## 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>



## *Sink Hole Classification Technique*

---

- Is it worth the risk to make config changes while a customer is under attack on a aggregation router with hundreds of customers connected to it?
  - Config changes when the network is under duress can and will cause more problems (it is not an “IOS” think – this applies to any network)
- What would help is if the attack flow can be shifted from the target (i.e. customer) to some other router where the risk is manageable.
- Enter the Sink Hole Router.
  - Similar to a Unix Honey Pot.

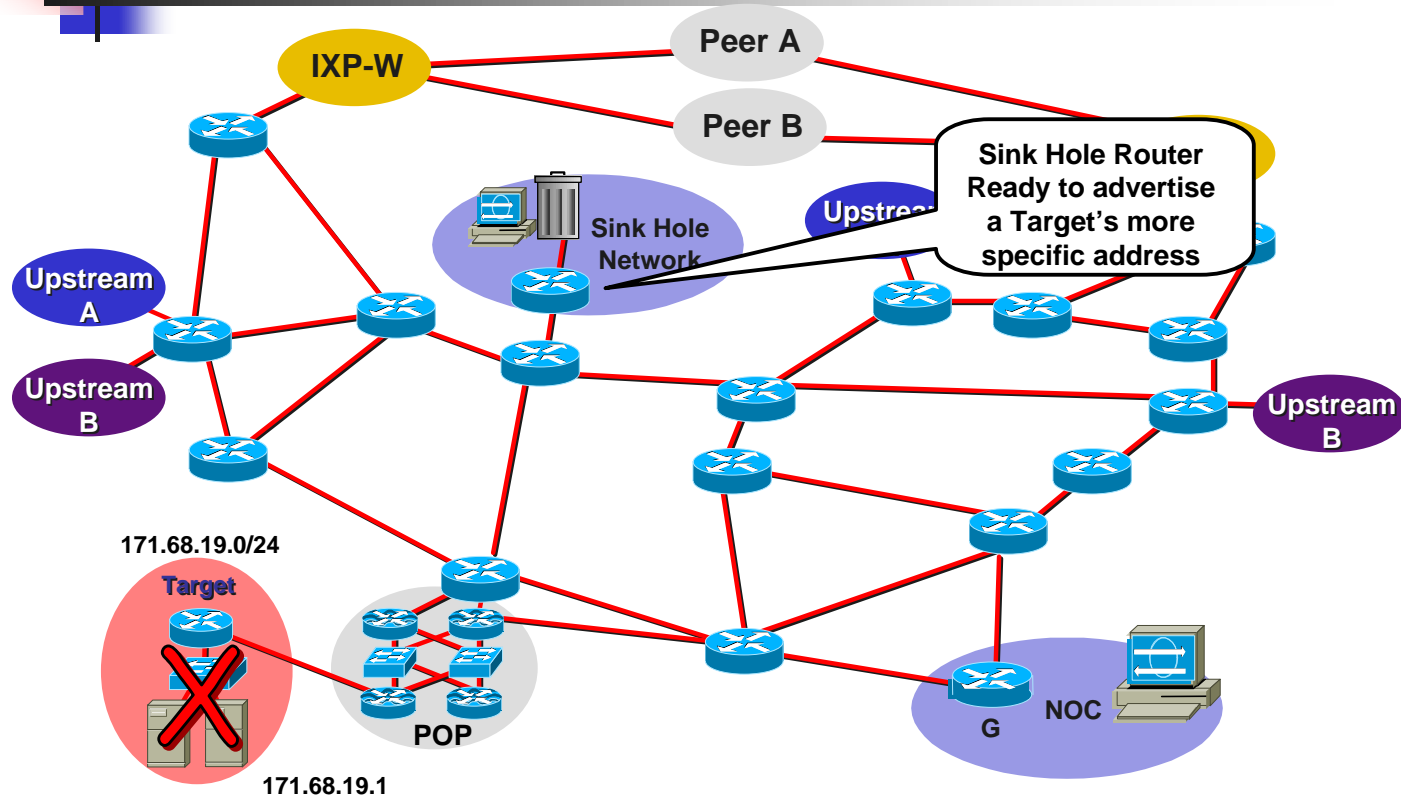


## *Sink Hole* Classification Technique

---

- Sink Hole Router Preparation:
  1. Router with really fast packet dropping capability, software features, and a connection to the network (were traffic to it would not endanger the network). Think 7200 with the fastest NPE you can get.
  2. BGP session (Route Reflector Client). The target's more specific address will get advertised from here.
  3. Packet Filters, syslog exports, and a way to analyze the logs from the ACL's log-input.

# Sink Hole Classification Technique



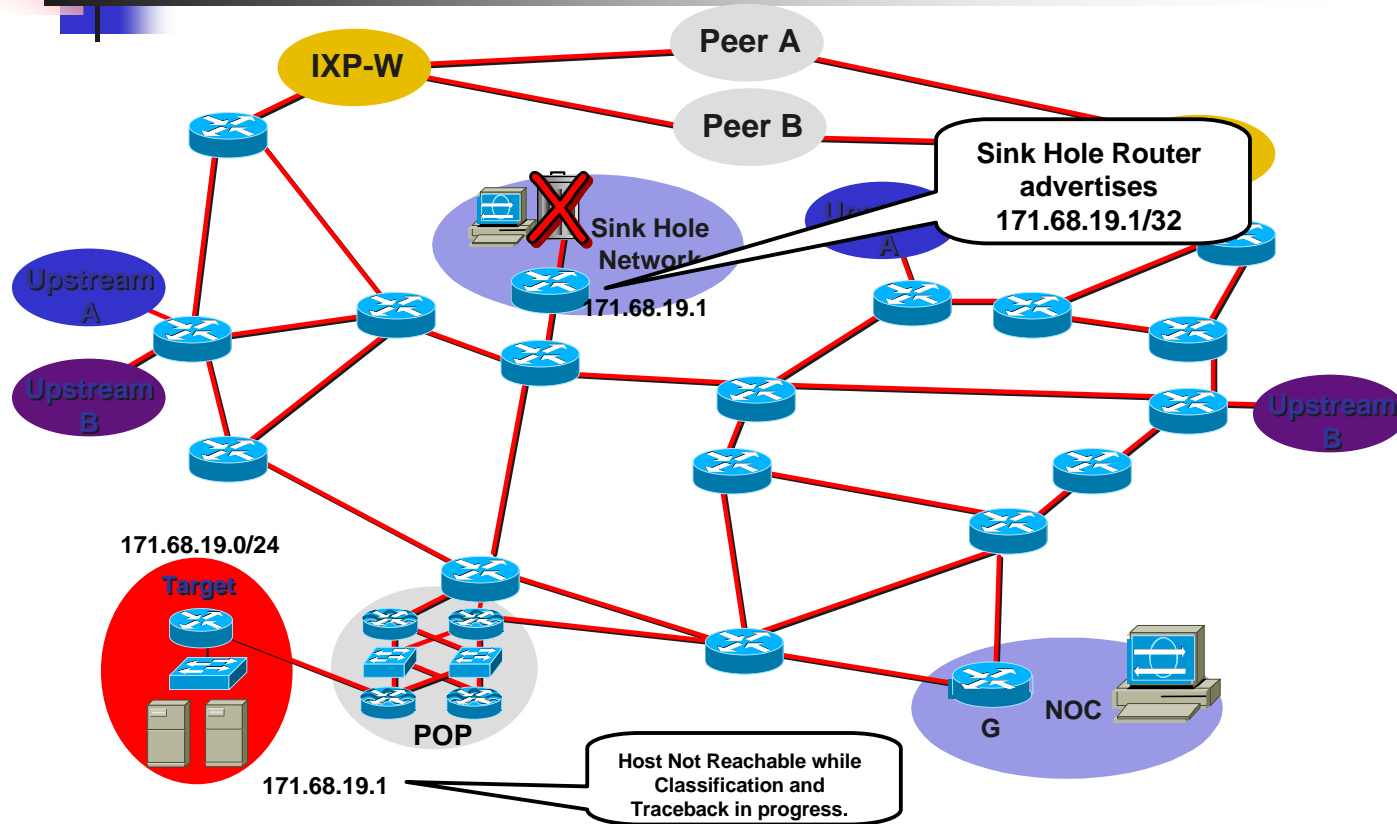


## *Sink Hole Classification Technique*

---

- Sink Hole Classification – Activation
  1. Customer notifies ISP that they are under attack and need help. ISP lets the customer know that they will take the targeted host's IP address and redirect it to classify and traceback (see Backscatter Traceback technique).
  2. Sink Hole Router advertises the /32 address that is under attack.
  3. All traffic for that /32 shifts to the Sink Hole Router. ACL Packet Classification, Netflow Classification, or host based (specialized box) is done on a section of the ISPs network built to be attacked.
  4. Massive Aggregation Router is not touched.

# Sink Hole Classification Technique





# DOS/DDOS Traceback

---



## Traceback the Attack

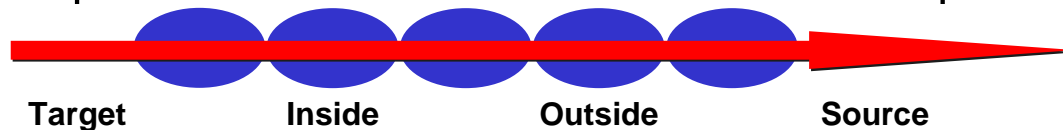
---

- 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
  - Three techniques— **hop by hop**, **jump to ingress**, and **backscatter**.

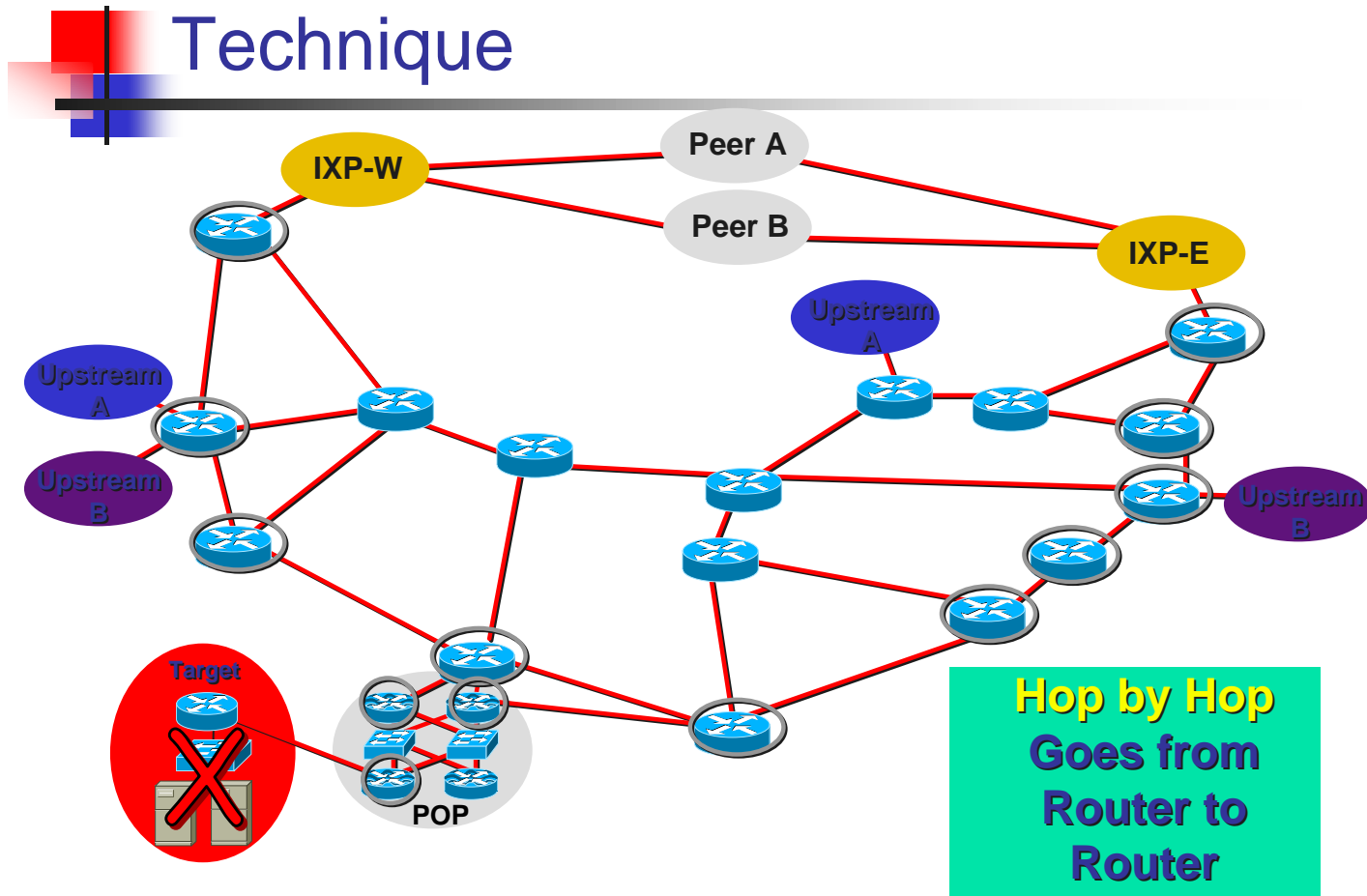


# Traceback via Hop by Hop Technique

- 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

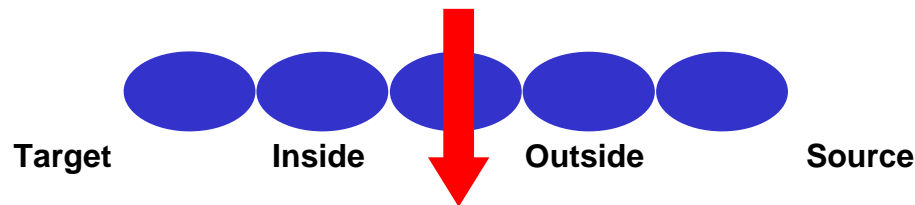


# Traceback via Hop by Hop Technique

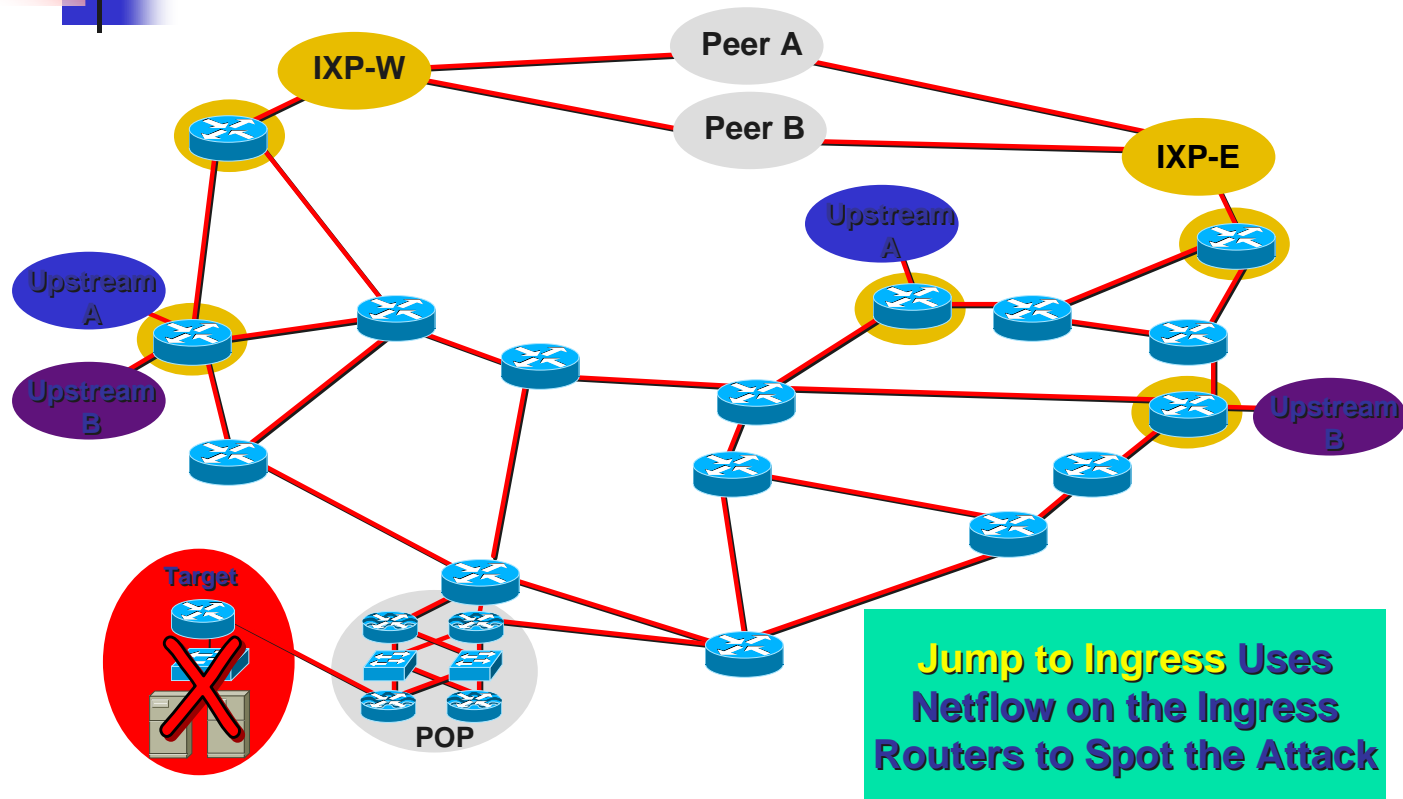


# Traceback via the Jump to Ingress Technique

- 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





## Traceback the Attack

---

- Two techniques for *hop by hop* or *jump to ingress*.
  - 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)



## 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

```
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  |

**Spoofed Flows  
are Tracks in  
Netflow!**

| SrcIf | SrcIPAddress   | DstIf  | DstIPAddress   | Pr | SrcP | DstP | Pkts |
|-------|----------------|--------|----------------|----|------|------|------|
| Fal/1 | 192.168.45.142 | POS1/0 | 198.133.219.25 | 11 | 008A | 008A | 1    |
| Fal/1 | 192.168.45.113 | POS1/0 | 198.133.219.25 | 11 | 0208 | 0208 | 1    |
| Fal/1 | 172.16.132.154 | POS1/0 | 198.133.219.25 | 06 | 701D | 0017 | 63   |





## 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



## 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.



# DOS/DDOS Reaction

---



## DOS/DDOS Reaction

---

- Remember – once you actively do something to mitigate the attack, you have made a choice of entering the game. You now become a fair game target.
- It is OK to make a choice to do nothing. You've classified and done the traceback for your customer.
- It is OK to continue the traceback to the next ISPs upstream of the attack.



## React to the Attack

---

- Doing 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 cyber war 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

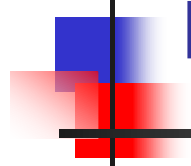


## React to the Attack

---

- Three techniques used to drop or rate limit:
  - ACLs—Manual upload
  - uRPF—Remote trigger via BGP
  - CAR—Manual upload or remote trigger via BGP





# Post Mortem

---



## Post Mortem

---

- Learning from your mistakes is essential.
- Do not wait until the next attack to implement the lessons of the last attack.
  - Take time after each incident to see if processes, procedures, tools, techniques, and configurations can be improved.
  - It is an arms race. Those who learn from this mistakes excel.

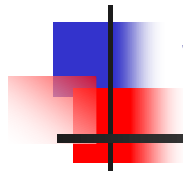


## Post Mortem

---

- *Fighting the Last War* is the #2 mistake of military planner.
- Underestimating the capabilities and commitment of your enemy is the #1 mistake of military planners.
- This observation directly applies to ISP Security.

# Default Routes, ISPs, and Security



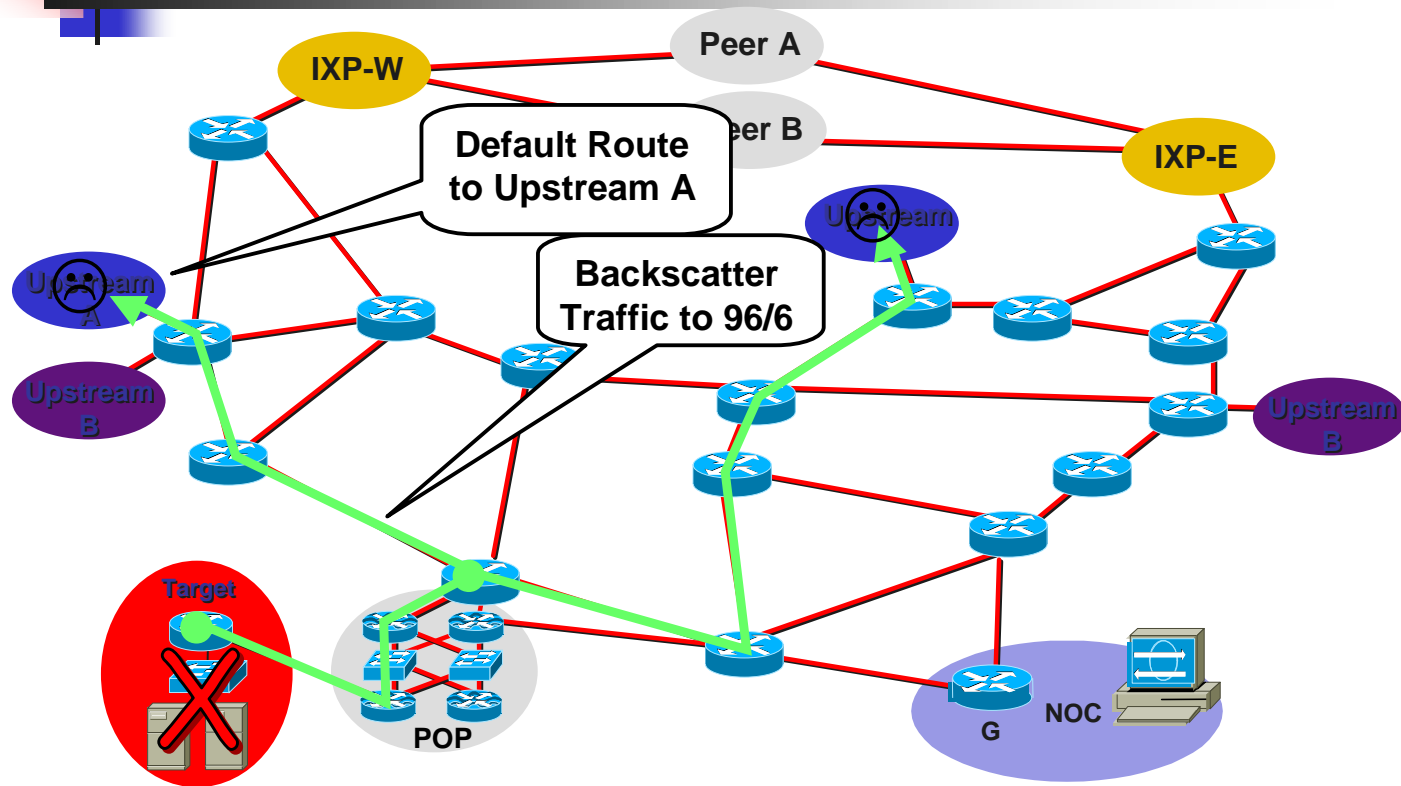


## Avoid Default Routes

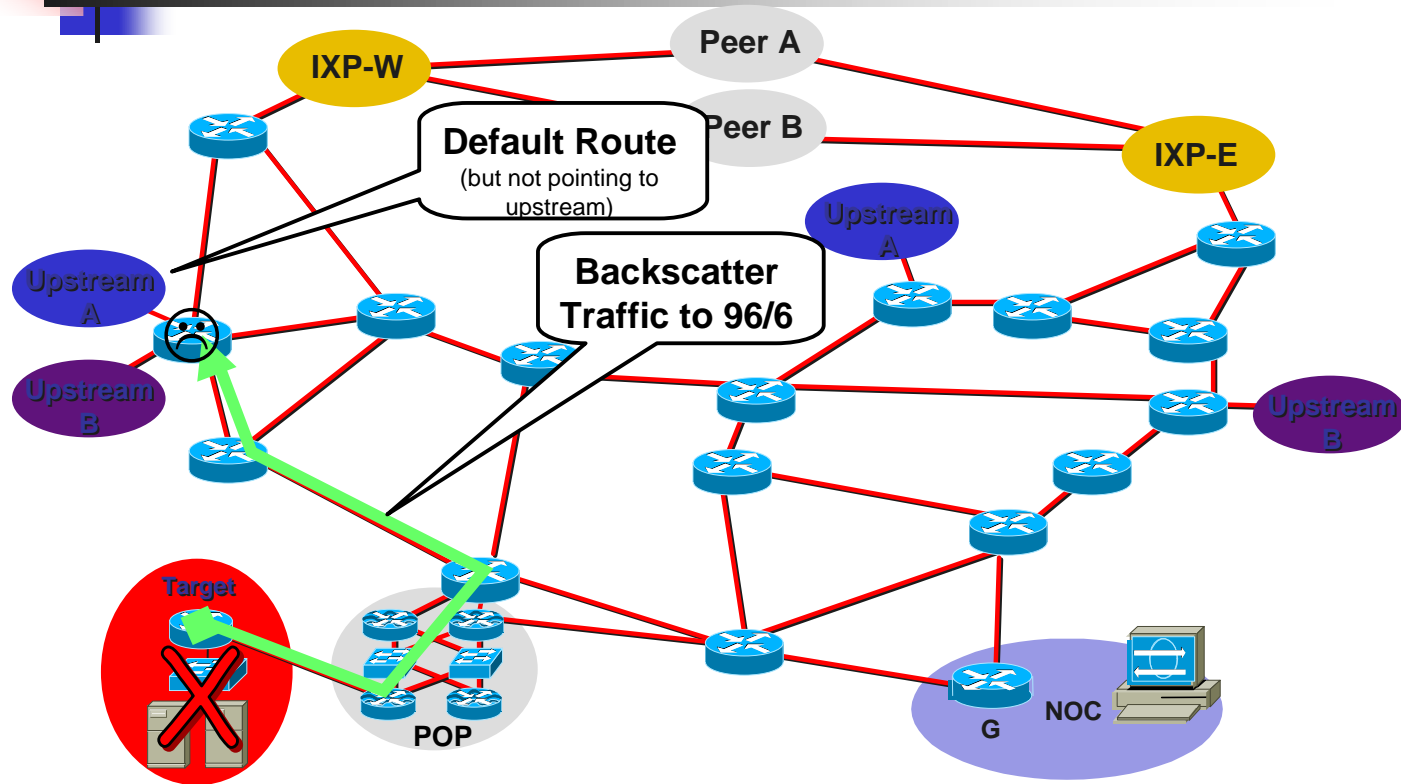
---

- ISPs with full BGP feeds should avoid default routes.
- DOS/DDOS attacks use spoofed addresses from the un-allocated IPV4 space.
  - See <http://www.iana.org/assignments/ipv4-address-space> for the latest macro allocations.
- Backscatter traffic from DOS/DDOS targets need to go somewhere. If there is a default, then this traffic will go to this one router and get dropped.
- Dropping backscatter traffic might overload the router.

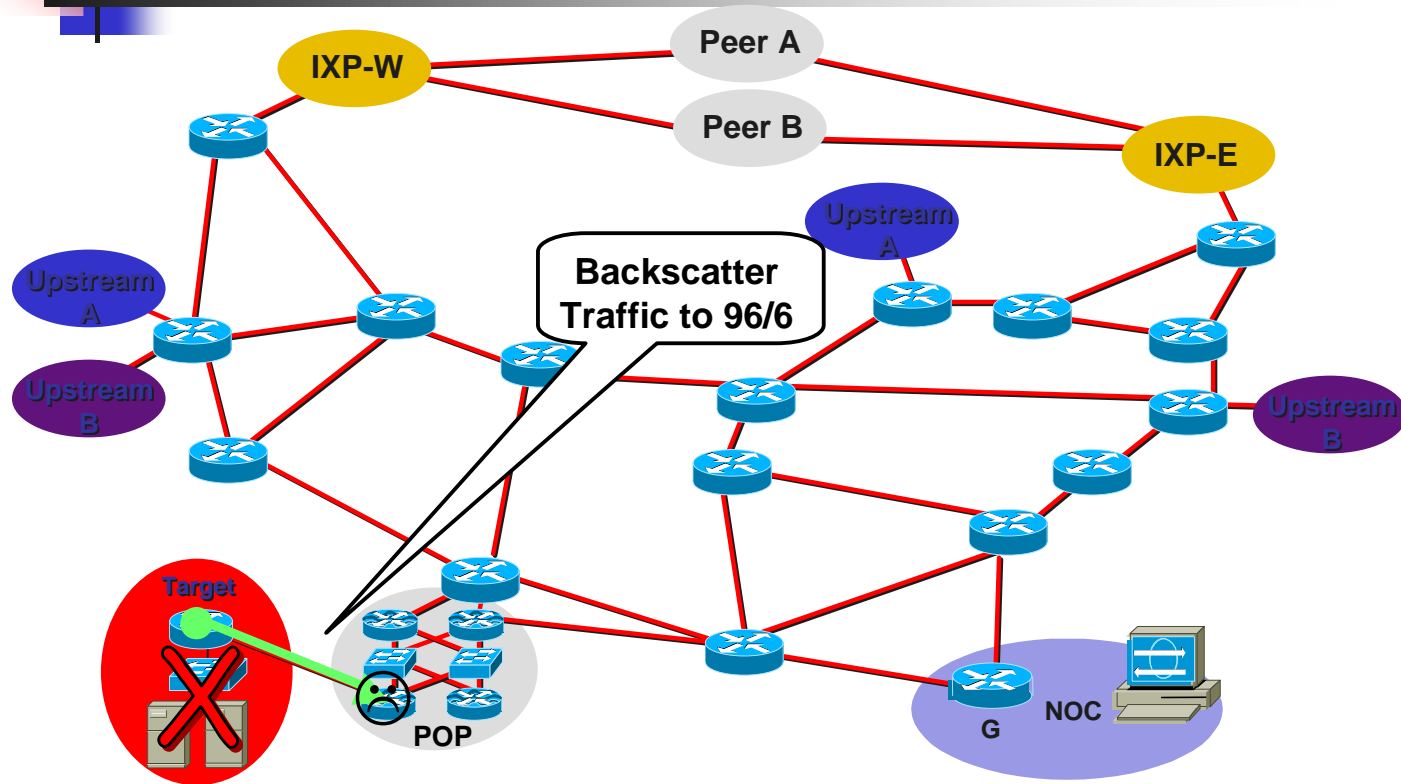
# Network with Default Route – Pointing to Upstream A



# Network with Default Route – But not Pointing to Upstream



# Network with No Default Route





## Default Route and ISP Security - Guidance



---

- Engineer Default Route with ISP Security as one of the factors.
  - Most just engineer default with routing/forwarding as the only factor
- If you need to use default, best to forward it upstream or to a Sink-Hole network engineered for packet drops.



## DDoS Links

---

- <http://www.denialinfo.com/>
- <http://www.staff.washington.edu/dittrich>
- <http://www.fbi.gov/nipc/trinoo.htm>
- <http://www.sans.org/y2k/DDoS.htm>
- <http://www.nanog.org/mtg-9910/robert.html>
- <http://cve.mitre.org/>
- <http://packetstorm.securify.com/distributed/>
- <http://www.cisco.com/public/cons/isp/security/>