

# Black Hole Routers

**Damir Rajnovic**

**Incident manager, Cisco PSIRT**

**<gaus@cisco.com>**

# What will be covered

Cisco.com

- Why?
- What?
- How?

# BHR – the Purpose

Cisco.com

- **To capture and characterize packets**
- **To assist mitigating DoS attacks**

# Why routers?

Cisco.com

- **Capturing packets on a general purpose OS (e.g., Solaris, Linux) becomes questionable above certain speed limit**

# Poor man comparison

Cisco.com

How fast packets are coming. Please note that this is only for the illustration purposes and do not represent the real performance numbers.

pps/	10000/	10 <sup>5</sup> /	10 <sup>6</sup> /	10 <sup>7</sup> /
BW (256 bytes/packet)	20.5Mbps	200Mbps	2Gbps	20Gbps
time between packets	100ms	10ms	1ms	100ns
R5000 (200MHz)	20000	2000	200	20
Pentium <sup>[1]</sup> (1.5GHz)	50000	5000	500	50

<sup>[1]</sup>An estimate of 3 cycles/instruction

# Why Not Use ACLs?

Cisco.com

- The method is described at <http://www.cisco.com/warp/public/707/22.html>

```
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
```

```
access-list 169 permit ip any any
```

- The idea is to install it on the victim's router

# Pitfalls of Using ACLs?

Cisco.com

- **ACL will degrade a router's performance**
- **Degradation severity will depend upon the following:**
  - **ACL type**
  - **ACL complexity**
  - **Router type**
  - **Network load**

# BHR – What Is It?

Cisco.com

- **It is just another router!**
- **Dedicated for this purpose only**
- **Placed somewhere in your network**
- **No customers attached to it!**
- **Physically, it can be a small subnet with multiple router and workstation**

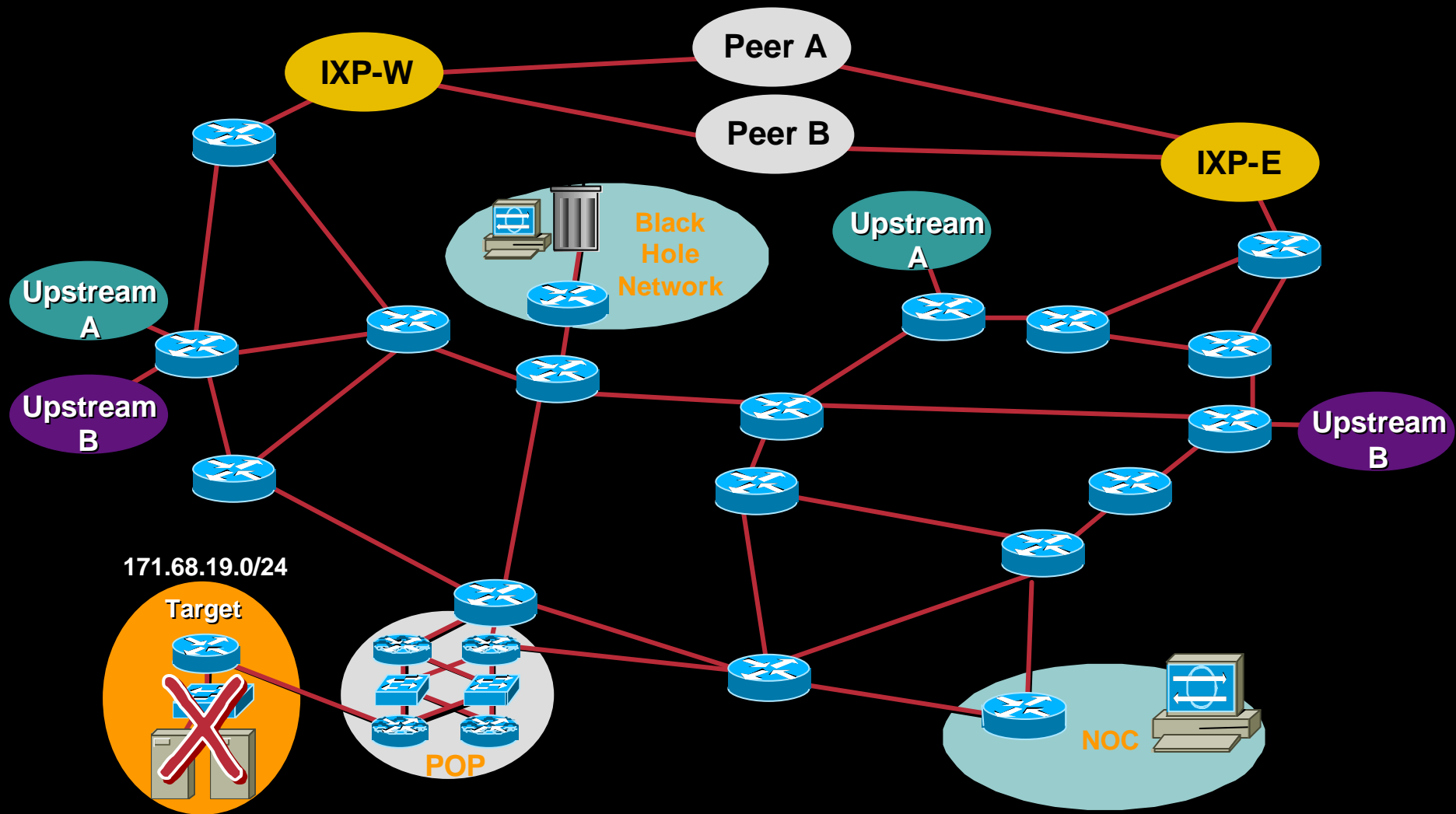
# Characteristics of the BHR

Cisco.com

- **Router with quick packet dropping capability, e.g. Cisco 7200 with the fastest Network Processing Engine (NPE)**
- **iBGP peer in your network**

# Example of BHR In a Network

Cisco.com



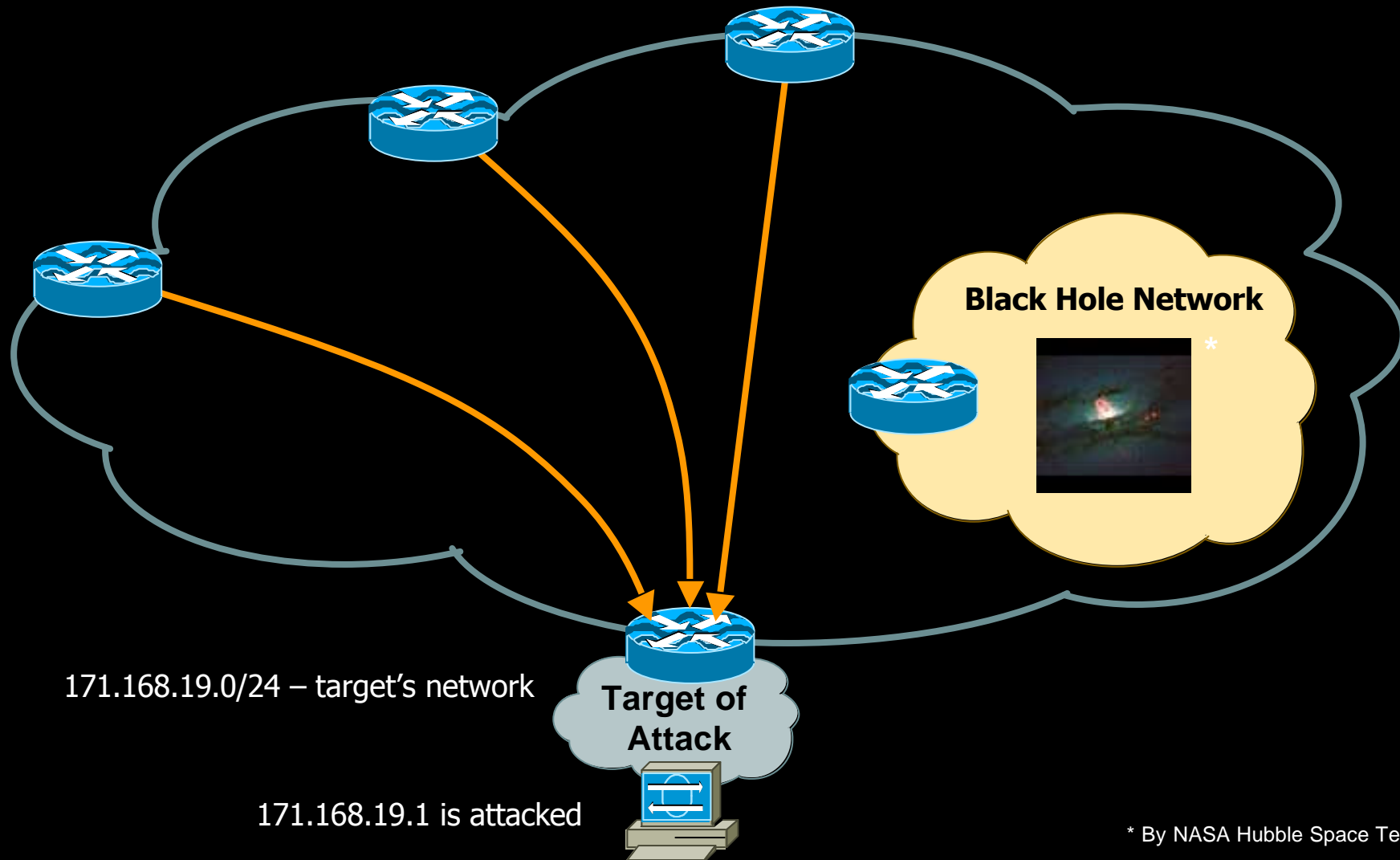
# Preparing to Analyze an Attack

Cisco.com

- **Do not do it on the victim's router**
- **Pull all the traffic to a BHR**
- **BHR should be able to withstand the attack (this is a hope!)**
- **Your links towards the BHR must be able to withstand the attack**

# Initial Stage of an Attack

Cisco.com



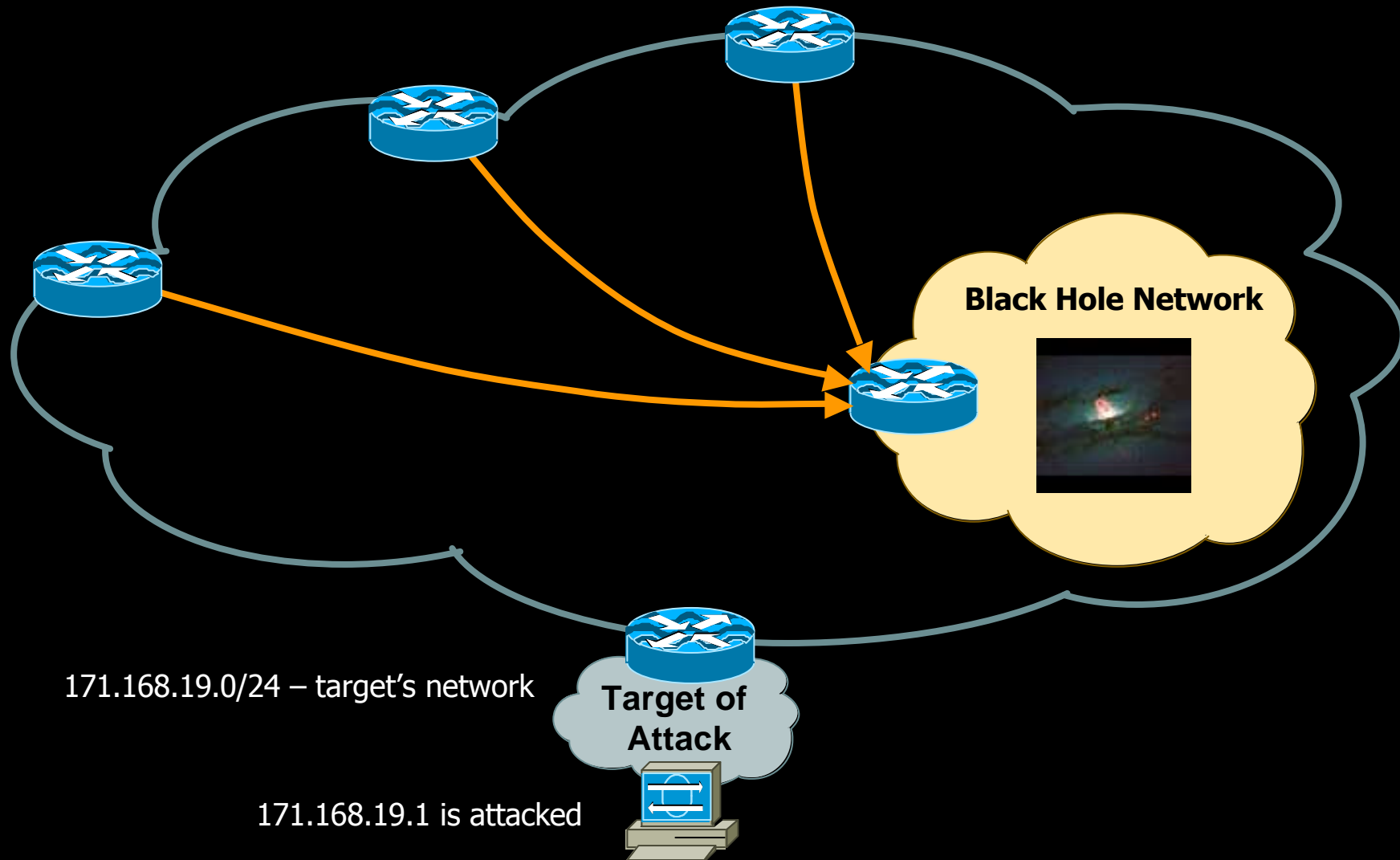
171.168.19.0/24 – target's network

171.168.19.1 is attacked

\* By NASA Hubble Space Telescope

# Divert the Traffic From the Victim

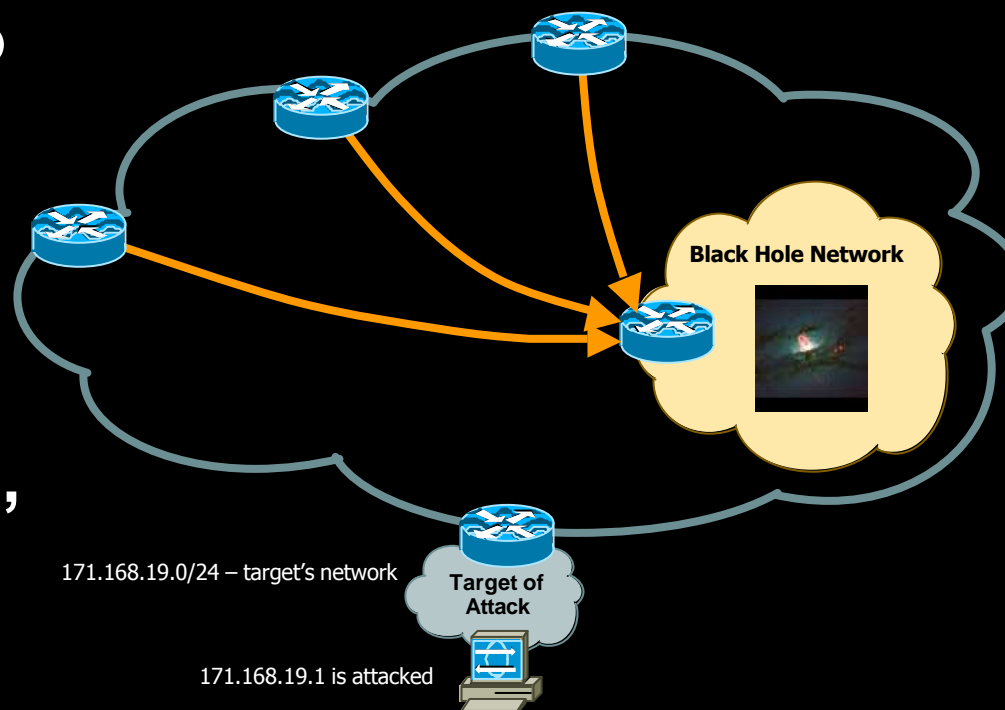
Cisco.com



# Analyze the Attack

Cisco.com

- The attack is pulled to BHR and from your aggregation router
- You can now classify the attack using ACL, Flow Analysis, Sniffer, etc.
- The objective is to minimize the risk to the network while investigating



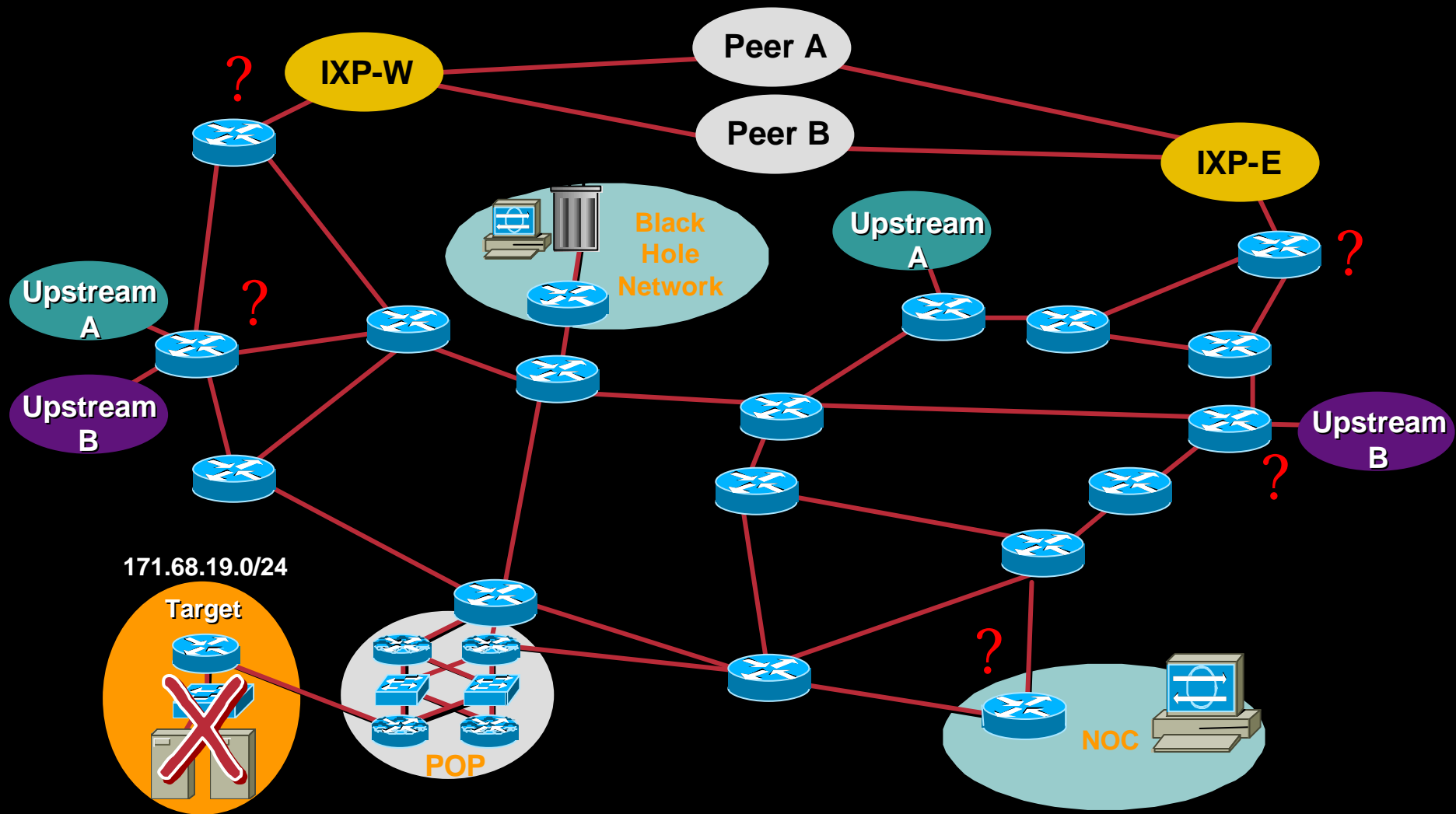
# What the Analysis Will Provide You

Cisco.com

- **What you will get:**
  - A packet type (UDP, TCP, ICMP, SYN, ACK,....) **⇒ ACL and rate limiting**
  - A volume (pps, Mbs) **⇒ Rate limiting**
  - An offending source IP addresses (dubious)  
**⇒ ACL and rate limiting**
- **What you will not get:**
  - Entry point(s) in your network

# Possible Entry Points

Cisco.com



# Where To Apply Countermeasures

Cisco.com

- **By using BHR and Backscatter technique you can learn entry points of the offending traffic.**
- **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/>**

# Backscatter Concepts

Cisco.com

- **Drop the offending traffic at any entry router in the network**
- **Generate an ICMP destination unreachable for every dropped packet**
- **Collect some Unreachables from the spoofed sources at the BHR**
- **Read out which routers/interfaces are dropping the traffic**

# Backscatter - preparation

Cisco.com

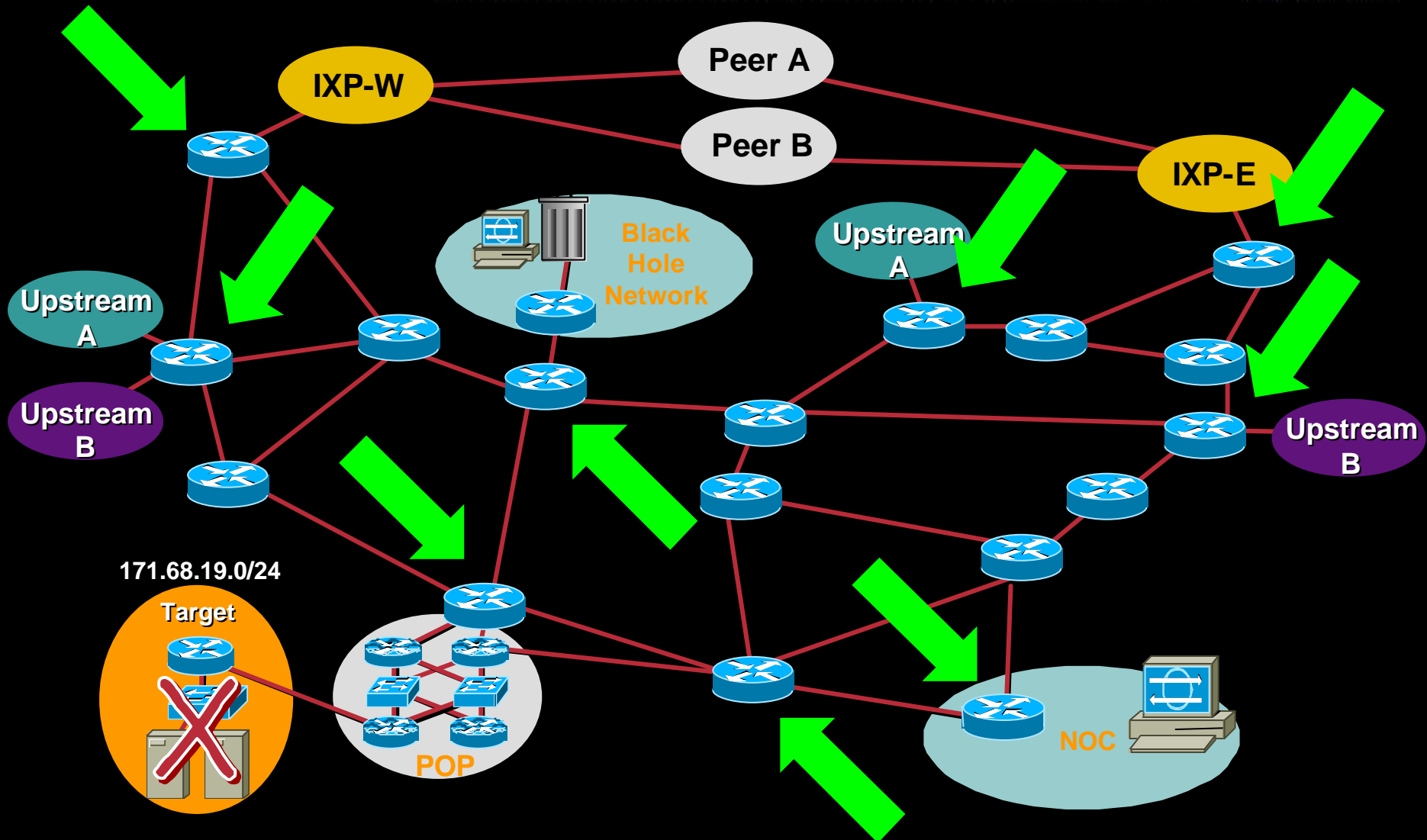
- Pick an unused IP address and route it to nowhere:

```
ip route 172.20.20.1 255.255.255.255 Null0
```

- Repeat this on every edge device

# Where are edge routers?

Cisco.com



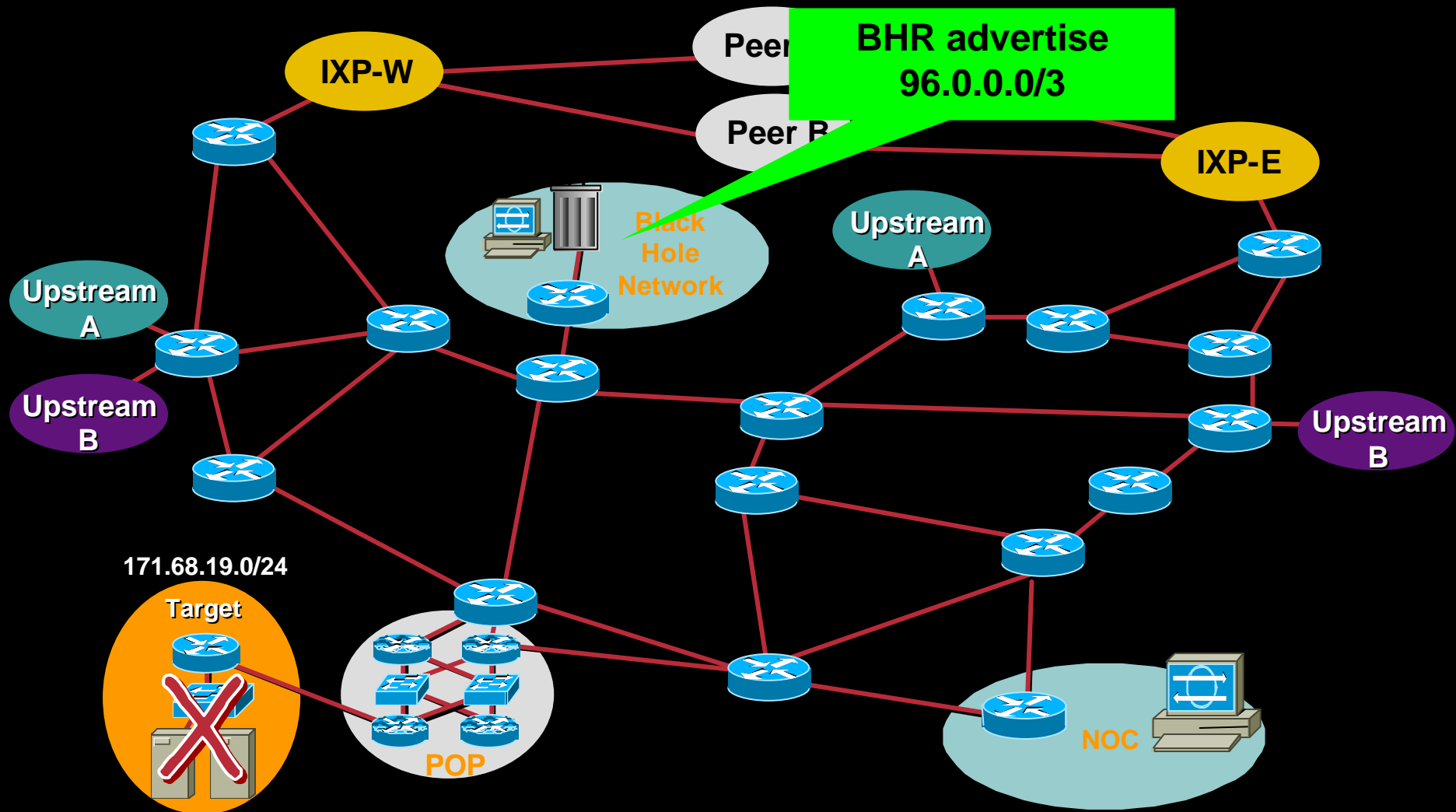
# Configuration of the BHR

Cisco.com

- **BHR 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](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.**

# BHR - preparation

Cisco.com



# BHR configuration

Cisco.com

```
router bgp 31337
!
redistribute static route-map static-to-bgp
!
! add a stanza to the route-map to set our special nexthop
!
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 Activation

Cisco.com

- **Only during attacks**
- **You must do the analysis first since the advertised block may need to be changed**
- **However, in most cases 96.0.0.0/3 should be fine since attackers are spoofing the whole IP range blindly**
- **The magic line is:**

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

# Backscatter – Packet Exchange

Cisco.com

Remote router



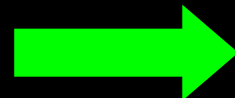
Edge router



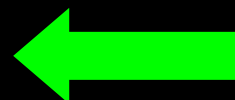
BHR



Type = TCP SYN  
Src IP = valid\_IP  
Dst IP = victim\_IP



victim\_ip routed to Null0  
generate ICMP Unreachable



Type = ICMP Unreachable  
Src IP = edge\_router\_IP  
Dst IP = valid\_IP

# Backscatter – Packet Exchange (Cont.)

Cisco.com

Remote router



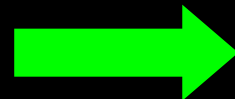
Edge router



BHR



Type = TCP SYN  
Src IP = 96.0.1.2  
Dst IP = victim\_IP



victim\_ip routed to Null0  
generate ICMP Unreachable

Type = ICMP Unreachable  
Src IP = edge\_router\_IP  
Dst IP = 96.0.1.2



# How To Display ICMPs

Cisco.com

- The result is that you will start receiving ICMPs at the BHR
- Configure BHR with this ACL

```
access-list 150 permit icmp any any unreachable log  
access-list 150 permit ip any any
```

- And you will start seeing this....

# Backscatter – the result

Cisco.com

**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**

# Combating DoS

Cisco.com

- **When you managed to determine the entry point(s), you can apply ACL and/or rate limiting to them.**
- **Do not forget to withdraw the victim\_IP route from the Null0!**

# Backscatter – Considerations

Cisco.com

- You must have ICMP Unreachables enabled on your edge routers.
- If ICMP Unreachables threaten to overload your edge device then rate limit them to some acceptable value (use `ip icmp rate-limit unreachable` command).

# BHR configuration – Juniper example

Cisco.com

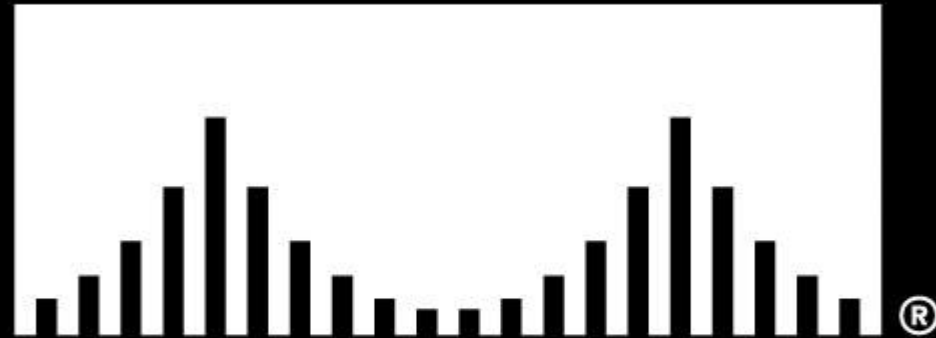
```
#Setup the bgp protocol to export our special policy, like
# redistributing, NOTE: "XXX" is the IBGP bgp group... we don't
# want to send this to customers.
set protocols bgp group XXX export BlackHoleRoutes
#
# Set static route with right tag, set local-pref low, internal, no-export
# and set the 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
```

# PSIRT contact details

Cisco.com

- **<psirt@cisco.com>** for non-emergency  
**<security-alert@cisco.com>** for emergencies
- **+1 877 228 7302** (toll-free in North America)  
**+1 408 525 6532** (elsewhere in the world)
- **Contact TAC and ask for PSIRT**
- **<http://www.cisco.com/go/psirt>**

# CISCO SYSTEMS



EMPOWERING THE  
INTERNET GENERATION