Sink Holes

A *Swiss Army Knife* ISP Security Tool

Version 1.5

Barry Raveendran Greene -- bgreene@cisco.com

Danny McPherson -- danny@arbor.net

Context

- *ISP Security Real World Techniques* endeavor to share tools and techniques that our peers are using to enhance their networks.
  - Backscatter Traceback (NANOG 23)
  - Security on the CPE Edge (NANOG 26)
  - Sink Hole (now – NANOG 28)

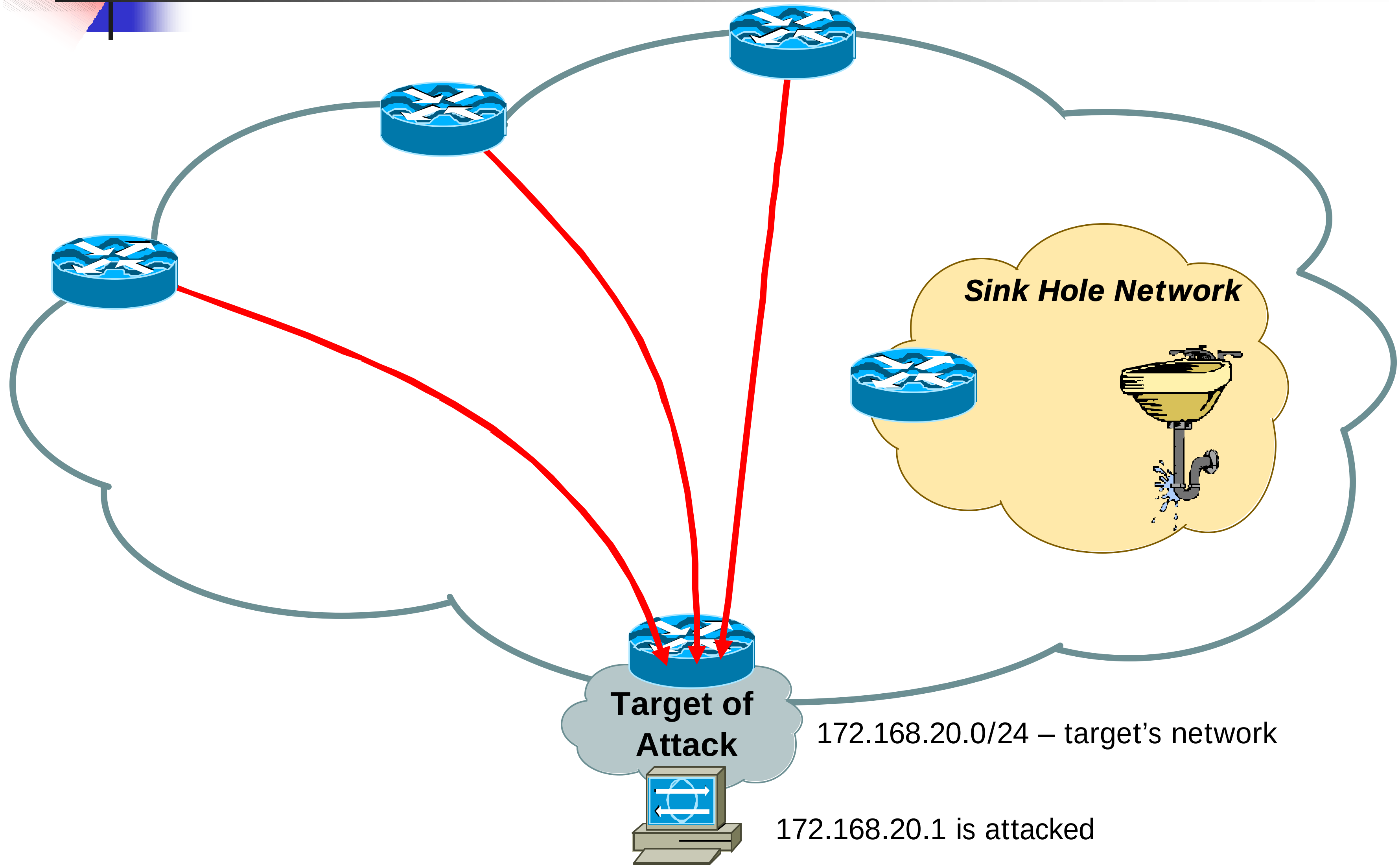
Objective

- Communicate new ISP Security Tools and Techniques that are working.
  - Generalize Concepts – with permission – experience from our peers.
  - Do not assume everyone knows the fundamentals
- Today we're working on getting everyone in-sync with *Sink Holes* …….

Sink Hole Routers/Networks

- Sink Holes are the network equivalent of a honey pot.
  - BGP speaking router or workstation built to *suck in* and assist in analyzing 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 or unused IP space)

Sink Hole Routers/Networks



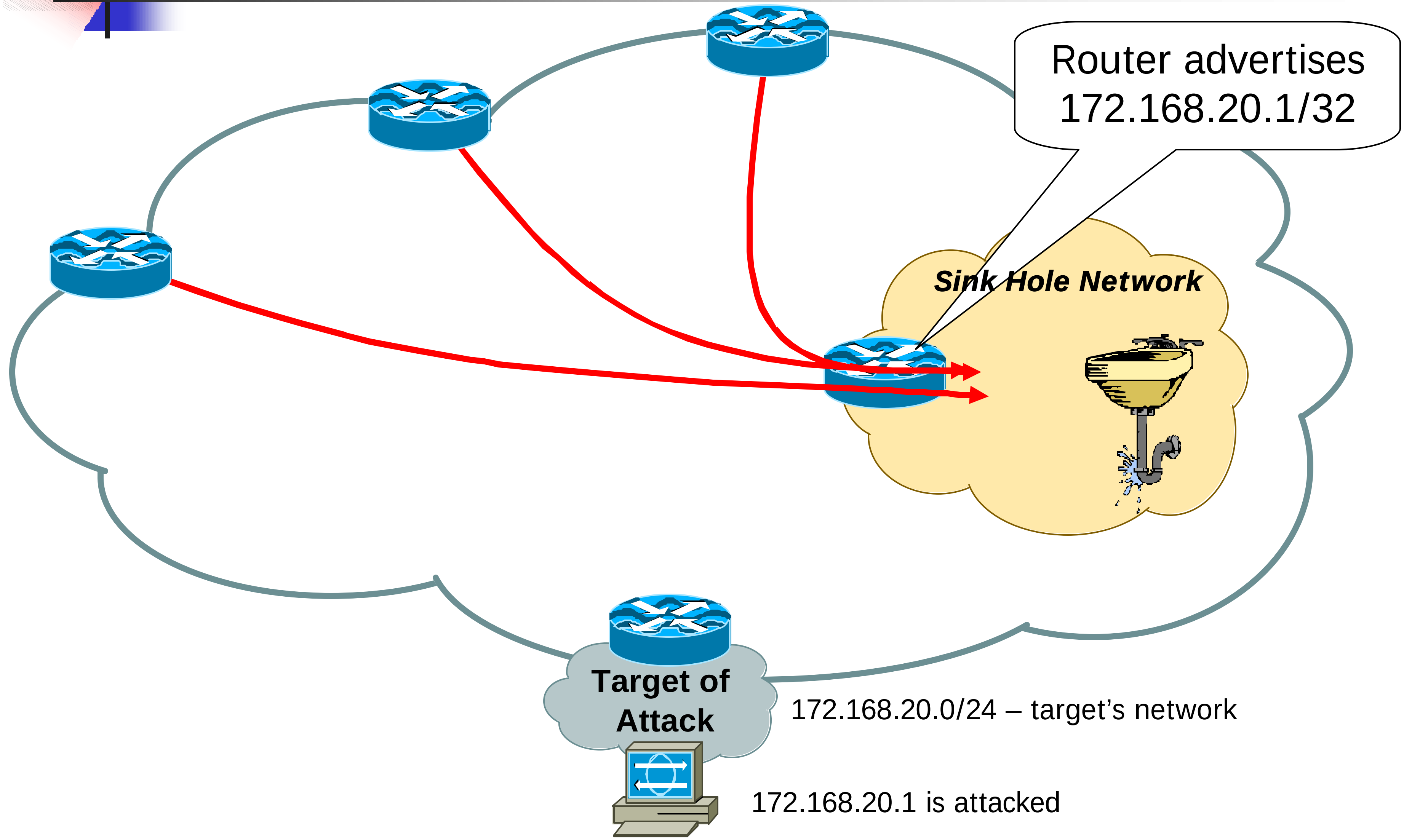
Sink Hole Network

Target of Attack

172.168.20.0/24 – target’s network

172.168.20.1 is attacked

Sink Hole Routers/Networks



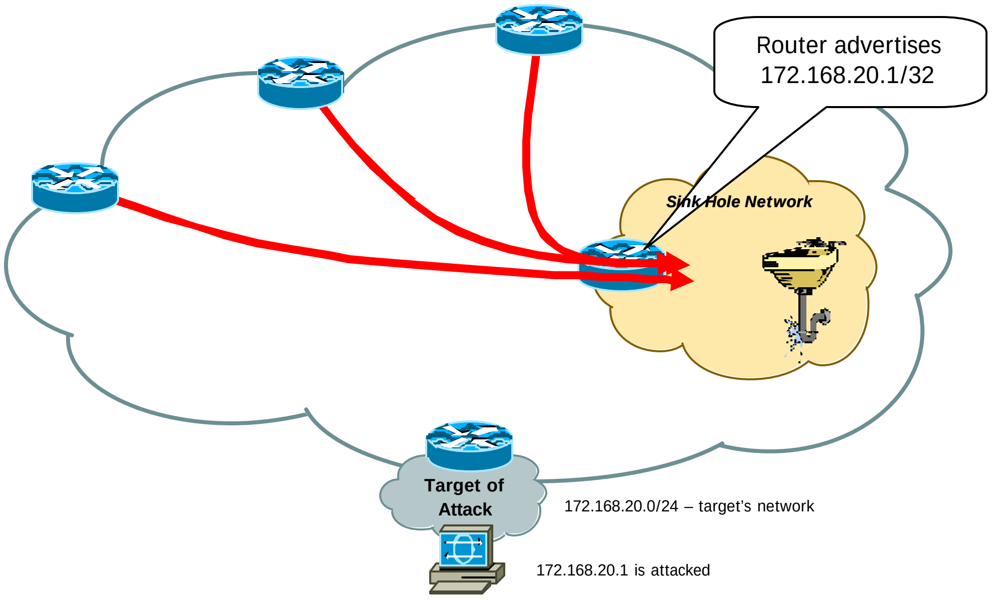
Router advertises 172.168.20.1/32

172.168.20.0/24 – target's network

172.168.20.1 is attacked

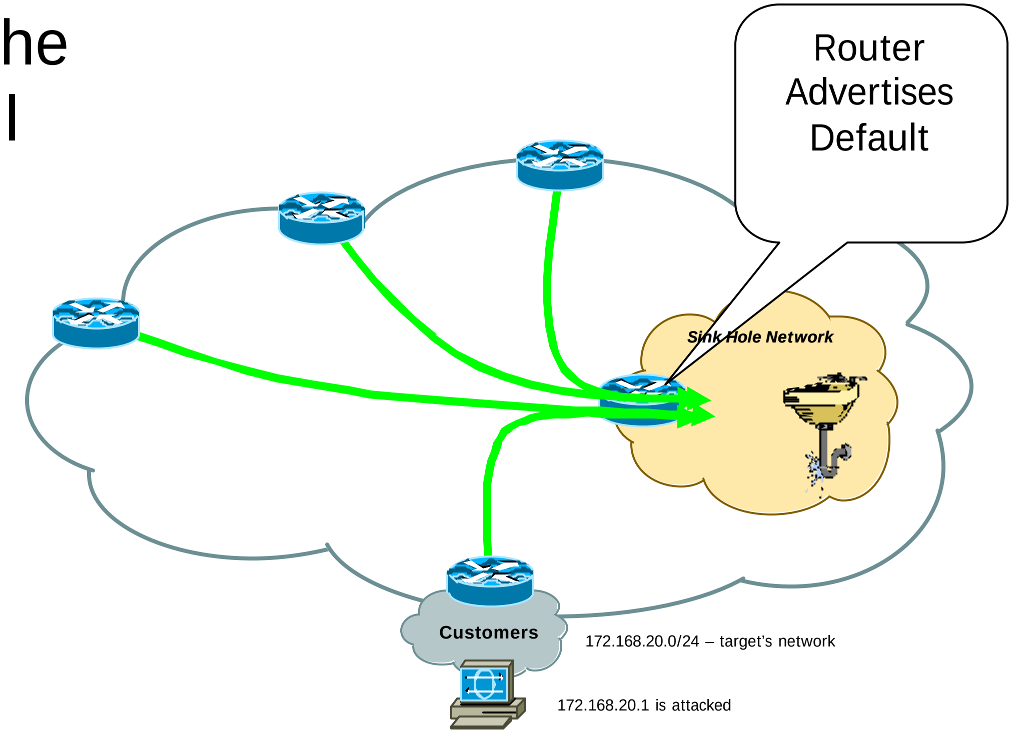
Sink Hole Routers/Networks

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


Router advertises 172.168.20.1/32
Sink Hole Network
Target of Attack
172.168.20.0/24 – target's network
172.168.20.1 is attacked

Sink Hole Routers/Networks

- Advertising Default from the Sink Hole will pull down all sorts 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.

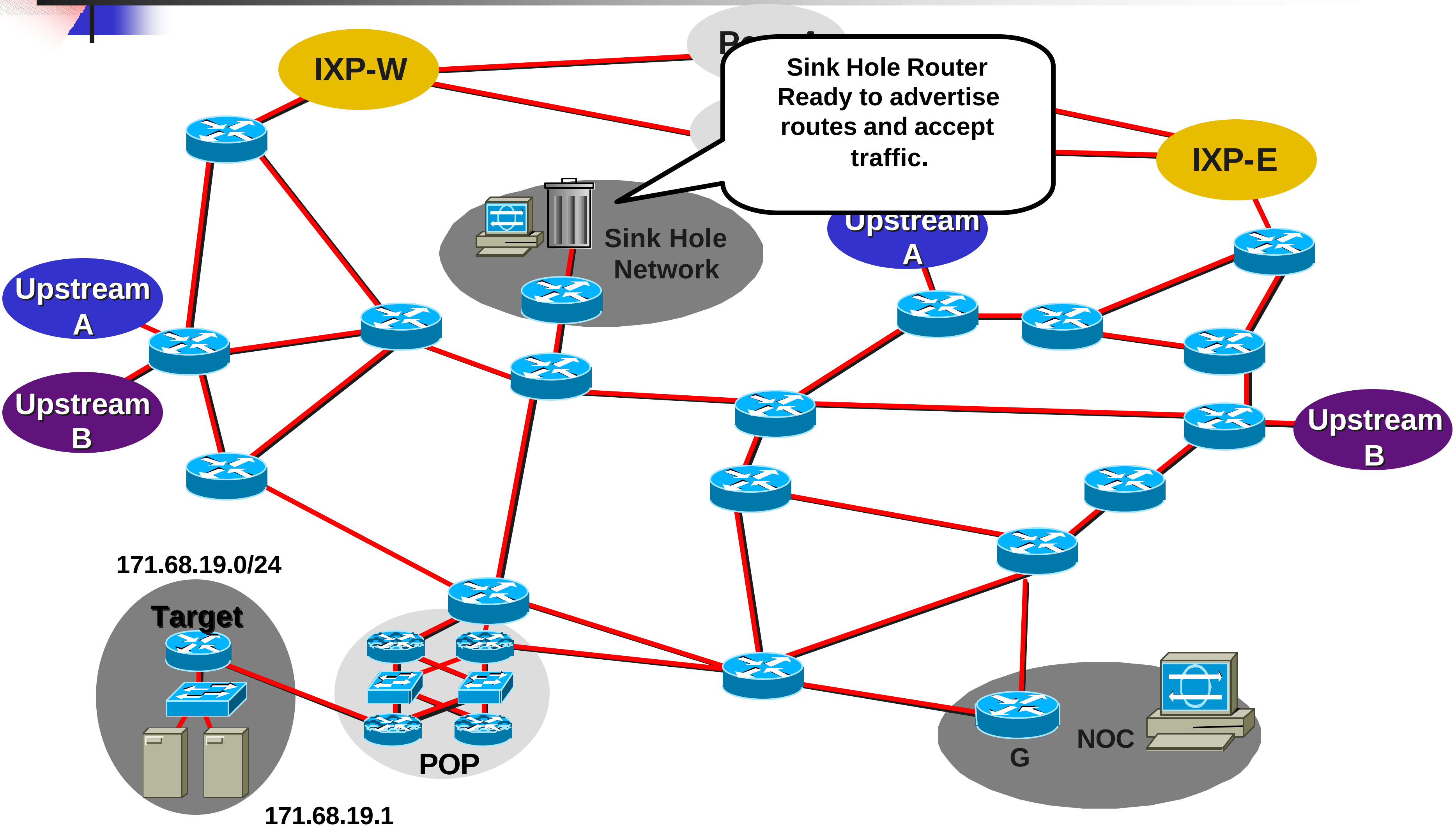


Router Advertises Default

172.168.20.0/24 – target's network

172.168.20.1 is attacked

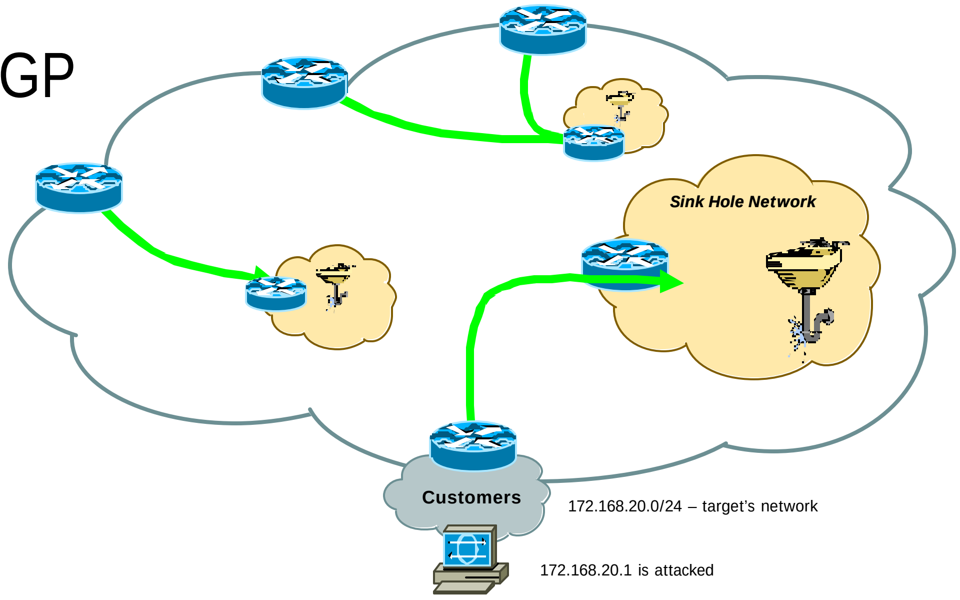
Sink Hole Routers/Networks



Sink Hole Router Ready to advertise routes and accept traffic.

Scaling Sink Hole Routers/Networks

- Multiple Sinkholes can be deployed within a network
- Combination of IGP with BGP Trigger
- Regional deployment
  - Major PoPs
- Functional deployment
  - Peering points
  - Data Centers
- Note: Reporting more complicated



Why Sink Holes?

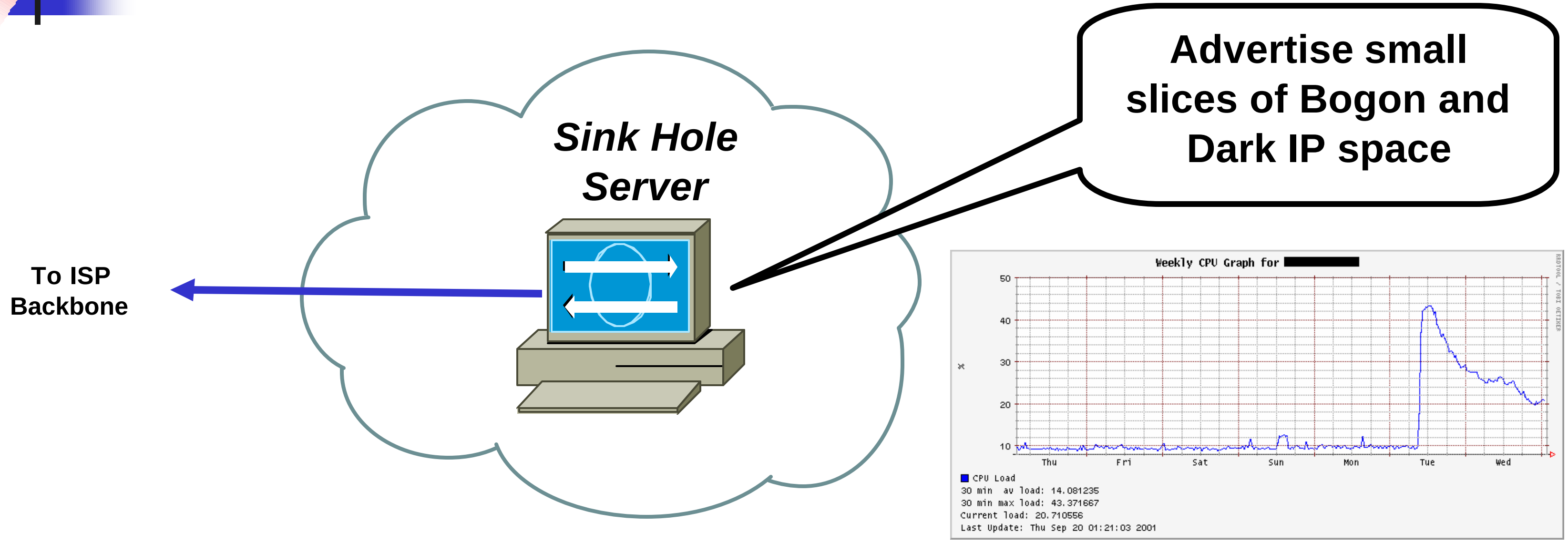
1. They work! Providers do use them in their network.
2. More uses are being found through experience and individual innovation.
3. They take preparation.

Why call the technique a *Sink Hole*?

- Sink Hole is used to describe a technique that does more than the individual tools we've had in the past:
  - Black Hole Routers – one router advertising dark IP space.
  - Tar Pits – A section of a honey net or DMZ designed to slow down TCP based attacks to enable analysis and traceback
  - Shunts – redirecting traffic to one of the router's connected interface.
  - Honey Net – a network designed to analyze and capture penetrations.

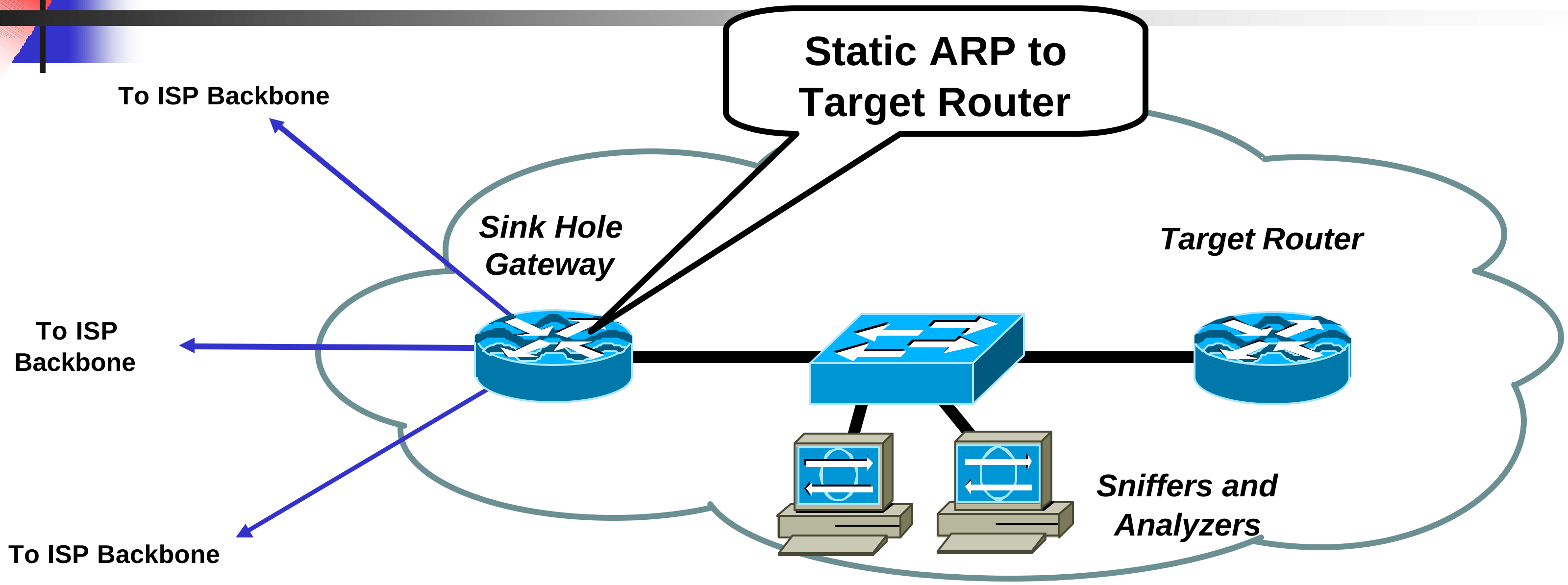
Sink Hole Basics

The Basic Sink Hole


To ISP
Backbone
Sink Hole Server
Advertise small slices of Bogon and Dark IP space
Weekly CPU Graph for [redacted]
50
40
30
20
10
%
Thu
Fri
Sat
Sun
Mon
Tue
Wed
RRDTOOL / TOBI OETIKER
■ CPU Load
30 min av load: 14.081235
30 min max load: 43.371667
Current load: 20.710556
Last Update: Thu Sep 20 01:21:03 2001

- Sinks Holes do not have to be complicated.
- Some large providers started their Sink Hole with a spare workstation with free unix, Zebra, and TCPdump.
- Some GNU or MRTG graphing and you have a decent sink hole.

Expanding the Sink Hole

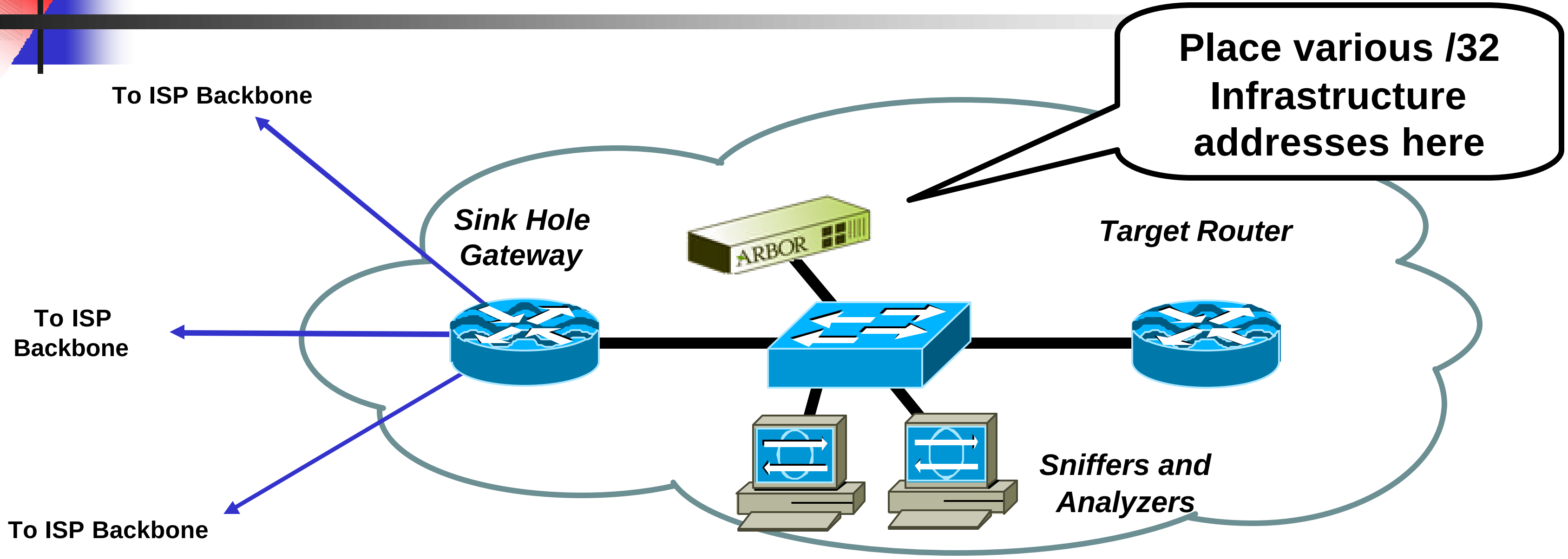


- Expand the Sink Hole with a dedicated router into a variety of tools.
- Pull the DOS/DDOS attack to the sink hole and forwards the attack to the target router.
- Static ARP to the target router keeps the Sink Hole Operational – Target Router can crash from the attack and the static ARP will keep the gateway forwarding traffic to the ethernet switch.

What to monitor in a Sink Hole?

- Scans on Dark IP.
  - Who is scoping out the network – pre-attack planning.
- Scans on Bogons.
  - Worms, infected machines, and Bot creation
- Backscatter from Attacks
  - Who is getting attacked
- Backscatter from Garbage traffic (RFC-1918 leaks)
  - Which customers have leaking networks.

Monitoring Scan Rates



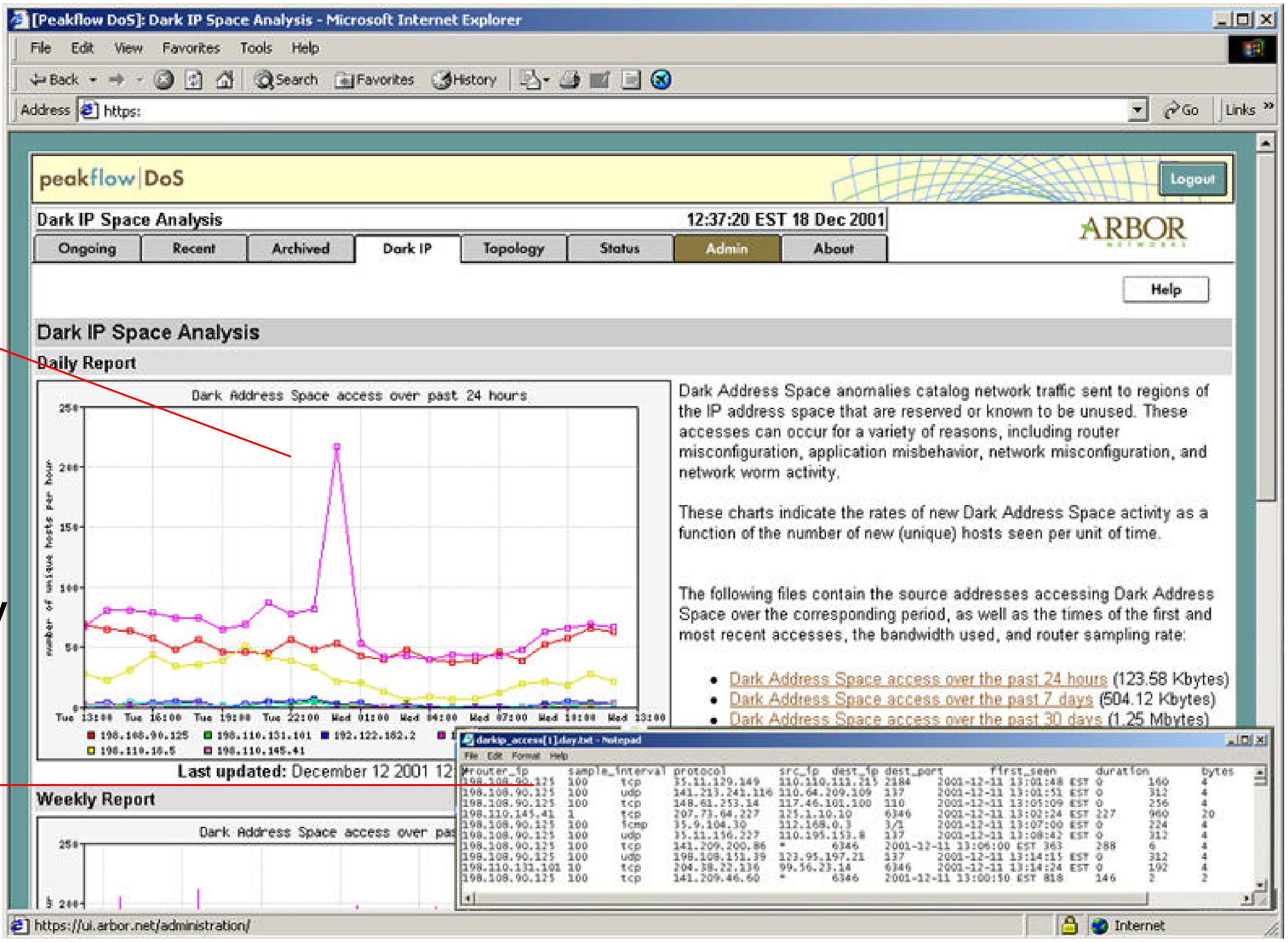
Place various /32 Infrastructure addresses here

- Select /32 address from different block of your address space. Advertise them out the Sink Hole
- Assign them to a workstation built to monitor and log scans. (Arbor Network’s *Dark IP* Peakflow module is one turn key commercial tool that can monitor scan rates.)

Worm Detection & Reporting UI

Operator instantly notified of Worm infection.

System automatically generates a list of infected hosts for quarantine and clean-up.



Dark IP Space Analysis 12:37:20 EST 18 Dec 2001

Dark IP Space Analysis

Daily Report

Dark Address Space anomalies catalog network traffic sent to regions of the IP address space that are reserved or known to be unused. These accesses can occur for a variety of reasons, including router misconfiguration, application misbehavior, network misconfiguration, and network worm activity.

These charts indicate the rates of new Dark Address Space activity as a function of the number of new (unique) hosts seen per unit of time.

The following files contain the source addresses accessing Dark Address Space over the corresponding period, as well as the times of the first and most recent accesses, the bandwidth used, and router sampling rate:

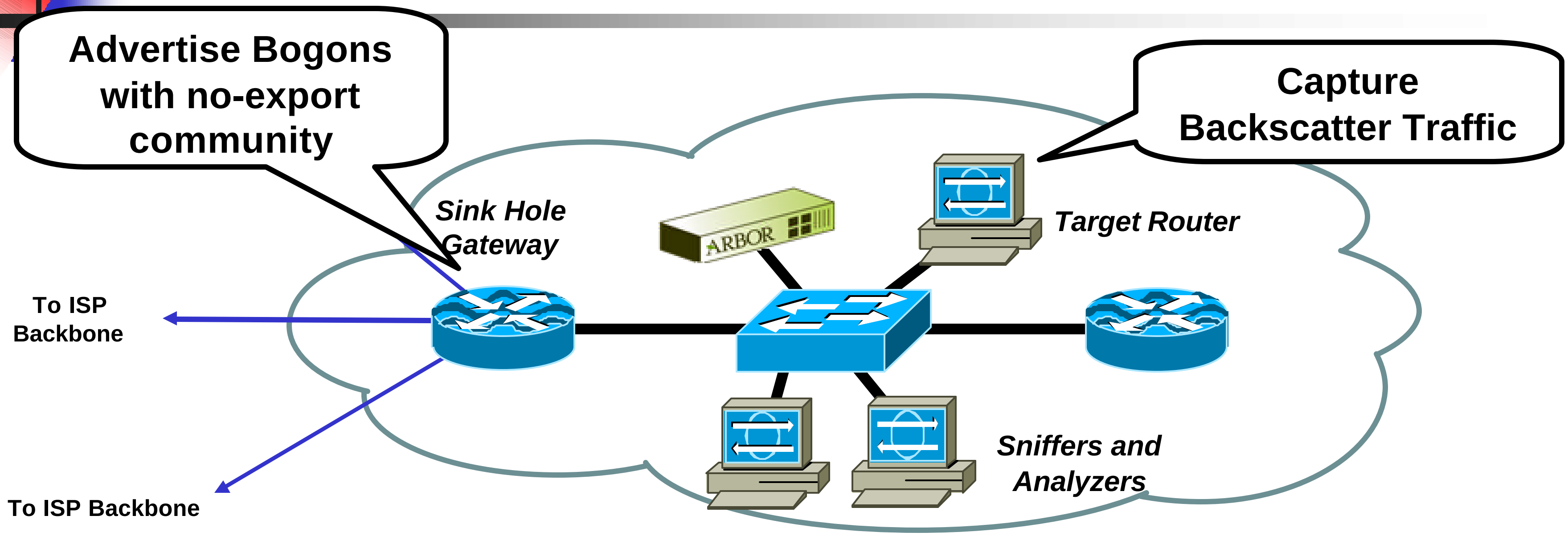
- Dark Address Space access over the past 24 hours (123.58 Kbytes)
- Dark Address Space access over the past 7 days (504.12 Kbytes)
- Dark Address Space access over the past 30 days (1.25 Mbytes)

Last updated: December 12 2001 12

Weekly Report

```
#router_ip      sample_interval protocol    src_ip          dest_ip         dest_port    first_seen              duration      bytes
198.108.90.125  100         tcp         35.11.129.149   110.110.111.215 2184    2001-12-11 13:01:48 EST 0       160     4
198.108.90.125  100         udp         141.213.241.116 110.64.209.109  137     2001-12-11 13:01:51 EST 0       312     4
198.108.90.125  100         tcp         148.61.253.14   117.46.101.100  110     2001-12-11 13:05:09 EST 0       256     4
198.110.145.41  1           tcp         207.73.64.227   125.1.10.10     6346    2001-12-11 13:02:24 EST 227     960     20
198.108.90.125  100         icmp        35.9.104.30     112.168.0.3     3/1     2001-12-11 13:07:00 EST 0       224     4
198.108.90.125  100         udp         35.11.156.227   110.195.133.8   137     2001-12-11 13:08:42 EST 0       312     4
198.108.90.125  100         tcp         141.209.200.86  *       6346    2001-12-11 13:06:00 EST 363     288     6       4
198.108.90.125  100         udp         198.108.151.39  123.95.197.21   137     2001-12-11 13:14:15 EST 0       312     4
198.110.131.101 10          tcp         204.38.22.136   99.56.23.14     6346    2001-12-11 13:14:24 EST 0       192     4
198.108.90.125  100         tcp         141.209.46.60   *       6346    2001-12-11 13:00:50 EST 818     146     2       2
```

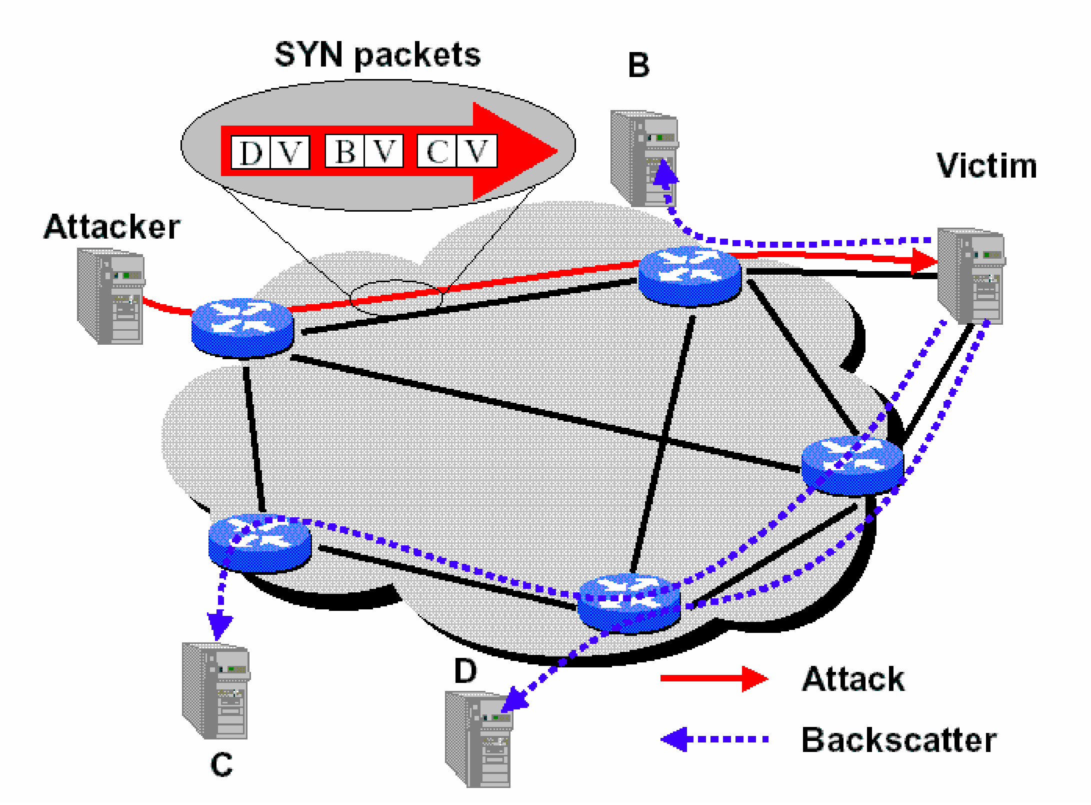
Monitoring Backscatter



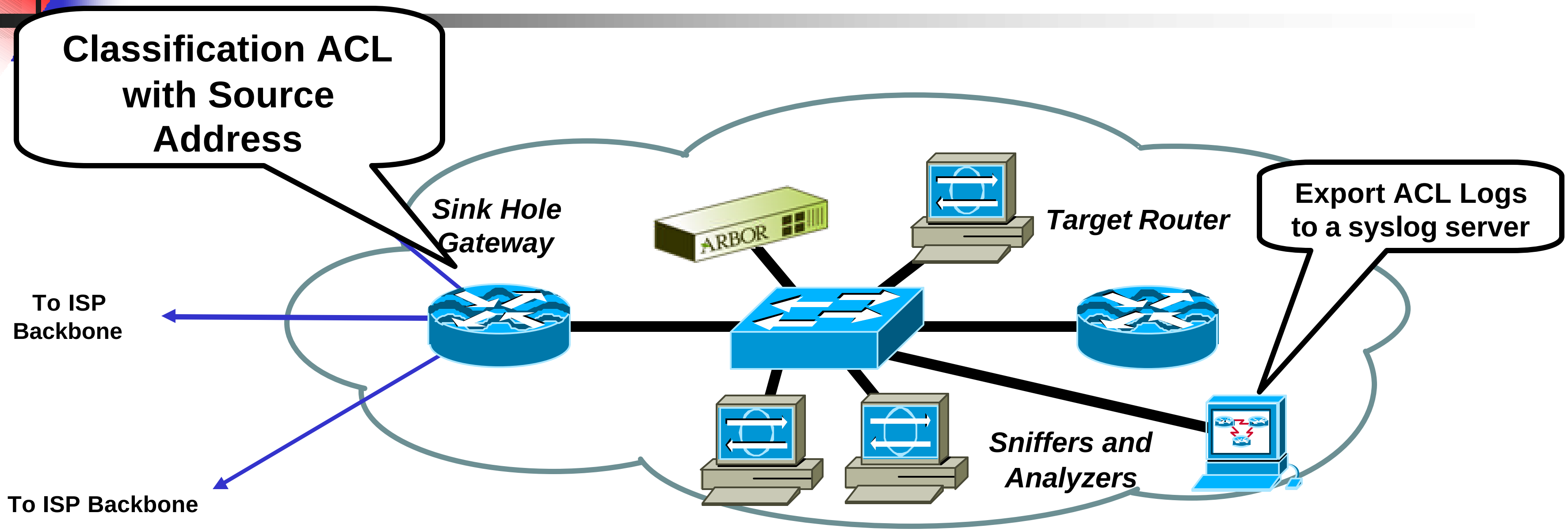
- Advertise bogon blocks with no-export and an explicit safety community (plus ISP egress filtering on the edge)
- Static the bogon to a backscatter collector workstation (as simple as TCPdump).
- Pulls in backscatter for that range – allows monitoring.

Monitoring Backscatter

- Inferring Internet Denial-of-Service Activity
  - http://www.caida.org/outreach/papers/2001/BackScatter/



Monitoring Spoof Ranges



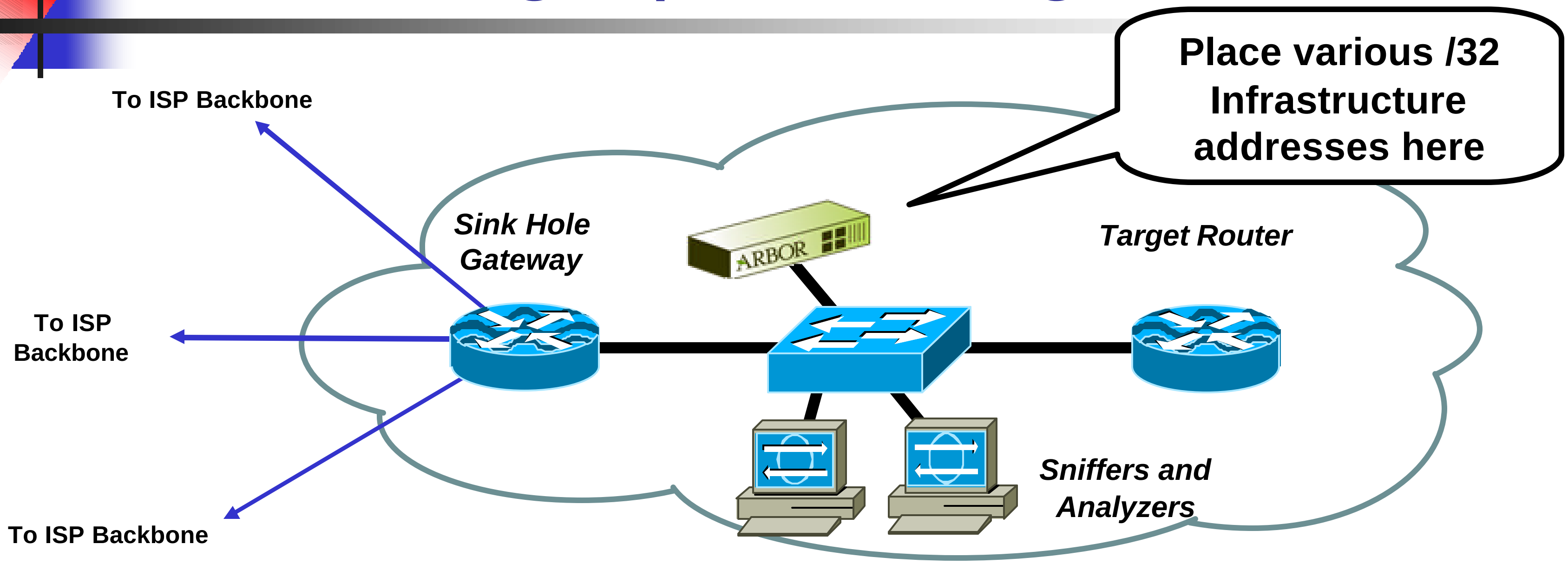
- Attackers use ranges of valid (allocated blocks) and invalid (bogon, martian, and RFC1918 blocks) spoofed IP addresses.
- Extremely helpful to know the spoof ranges.
- Set up a classification filter on source addresses.

Monitoring Spoof Ranges

Example: Jeff Null’s [jnull@truerouting.com] Test

```
Extended IP access list 120 (Compiled)
    permit tcp any any established (243252113 matches)
    deny ip 0.0.0.0 1.255.255.255 any (825328 matches)
    deny ip 2.0.0.0 0.255.255.255 any (413487 matches)
    deny ip 5.0.0.0 0.255.255.255 any (410496 matches)
    deny ip 7.0.0.0 0.255.255.255 any (413621 matches)
    deny ip 10.0.0.0 0.255.255.255 any (1524547 matches)
    deny ip 23.0.0.0 0.255.255.255 any (411623 matches)
    deny ip 27.0.0.0 0.255.255.255 any (414992 matches)
    deny ip 31.0.0.0 0.255.255.255 any (409379 matches)
    deny ip 36.0.0.0 1.255.255.255 any (822904 matches)
    .
    .
    permit ip any any (600152250 matches)
```

Monitoring Spoof Ranges



- Select /32 address from different block of your address space. Advertise them out the Sink Hole
- Assign them to a workstation built to monitor and log scans.
- Home grown and commercial tools available to monitor scan rates (Arbor Network’s *Dark IP* Application is one turn key commercial tool that can monitor scan rates.)

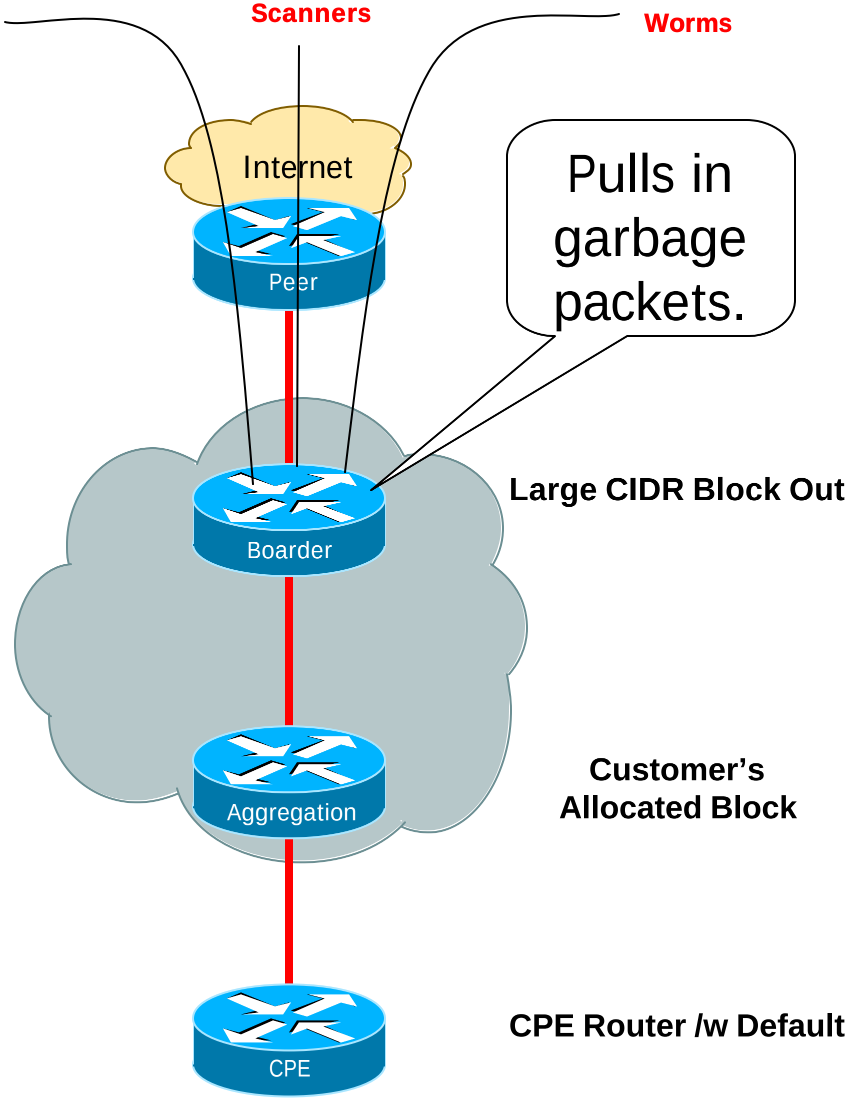
Safety Precautions

- Do not allow bogons to leak:
  - BGP “no-export” community
  - Explicit Egress Prefix Policies (community, prefix, etc.)
- Do not allow traffic to escape the sink hole:
  - Backscatter from a Sink Hole defeats the function of a *Sink Hole (egress ACL on the Sink Hole router)*

Black Hole Routers or Sink Holes?

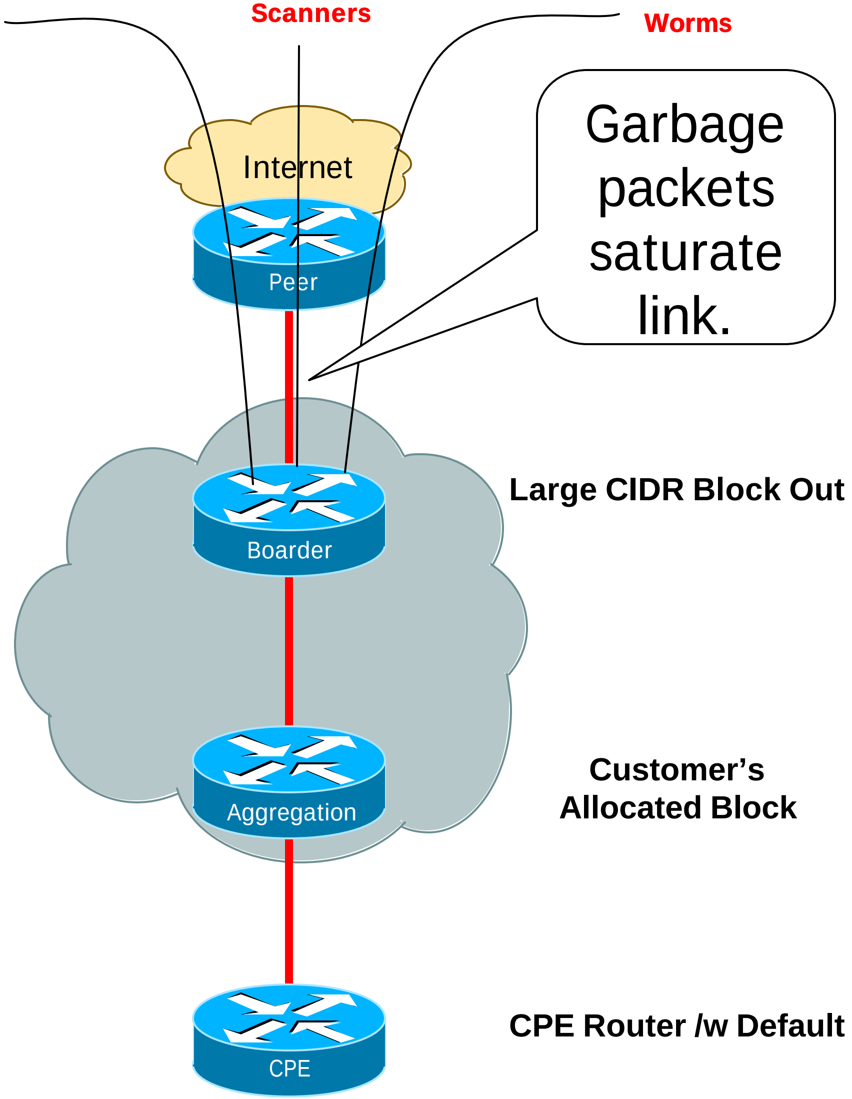
Simple Sink Holes – Internet Facing

- BCP is to advertise the whole allocated CIDR block out to the Internet.
- Left over unallocated Dark IP space gets pulled into the advertising router.
- The advertising router becomes a Sink Hole for garbage packets.



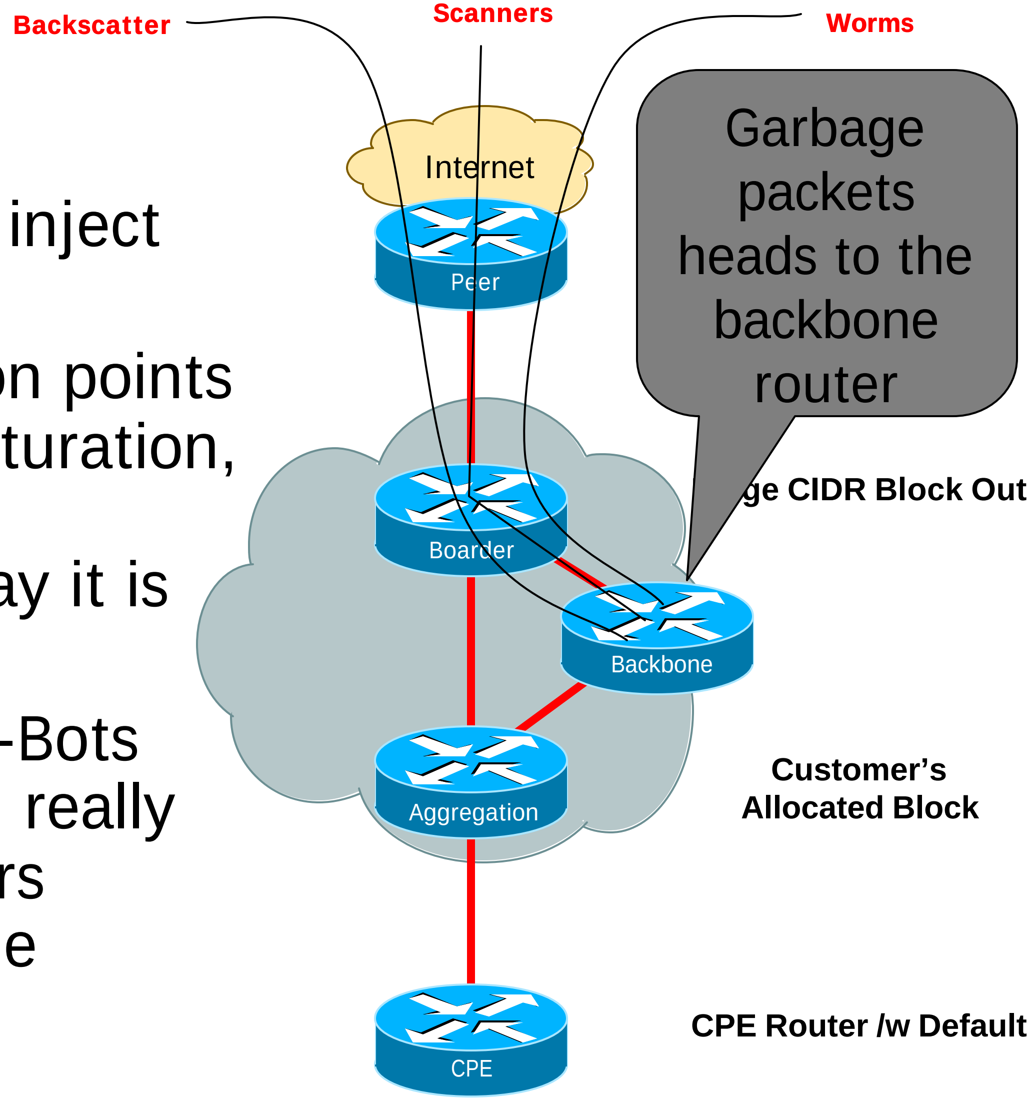
ASIC Drops at Line Rate?

- Forwarding/Feature ASICs will drop packets with no performance impact.
- Line Rate dropping will not solve the problem of garbage packets saturating the link.



Backbone Router Injecting Aggregates

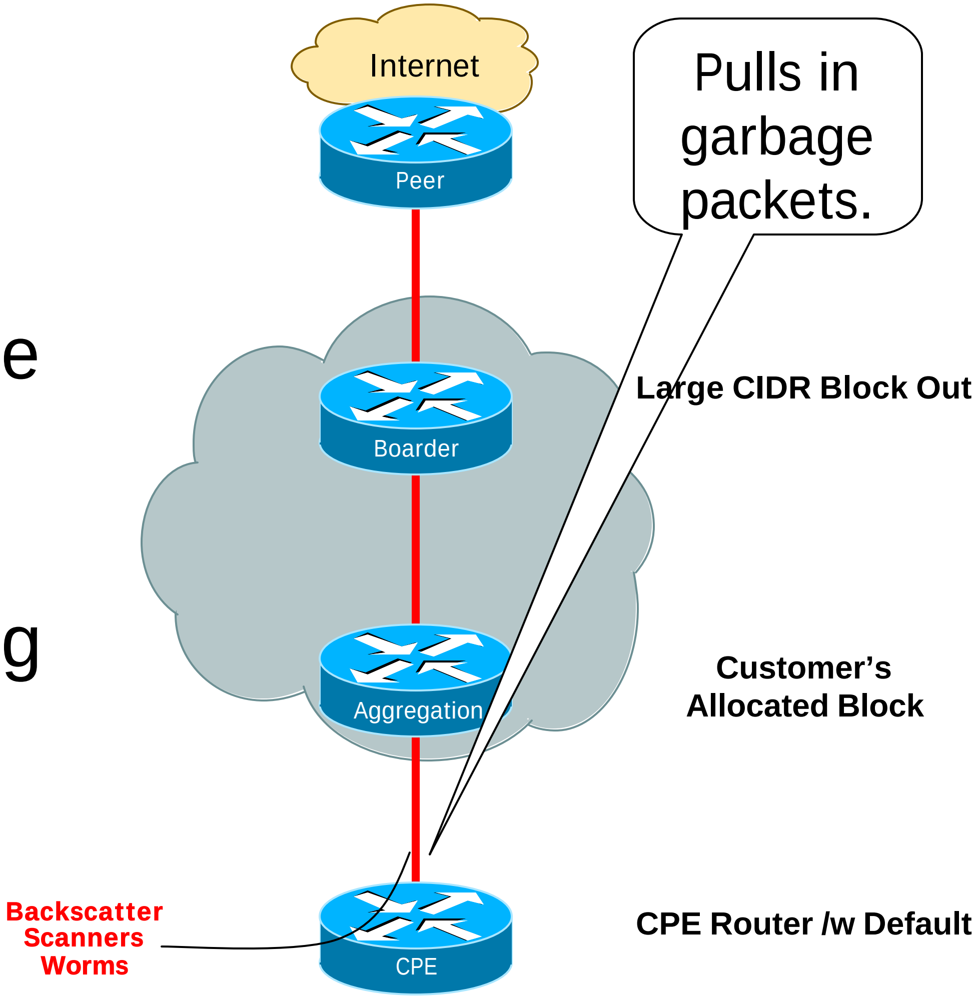
- Some ISPs use the Backbone/core routers to inject their aggregates.
- Multiple Backbone injection points alleviates issues of link saturation, but exposes the loopback addresses (at least the way it is done today).
- In a world of multiple Gig-Bots and Turbo worms, do you really want you backbone routers playing the role of garbage collectors?



Garbage packets heads to the backbone router

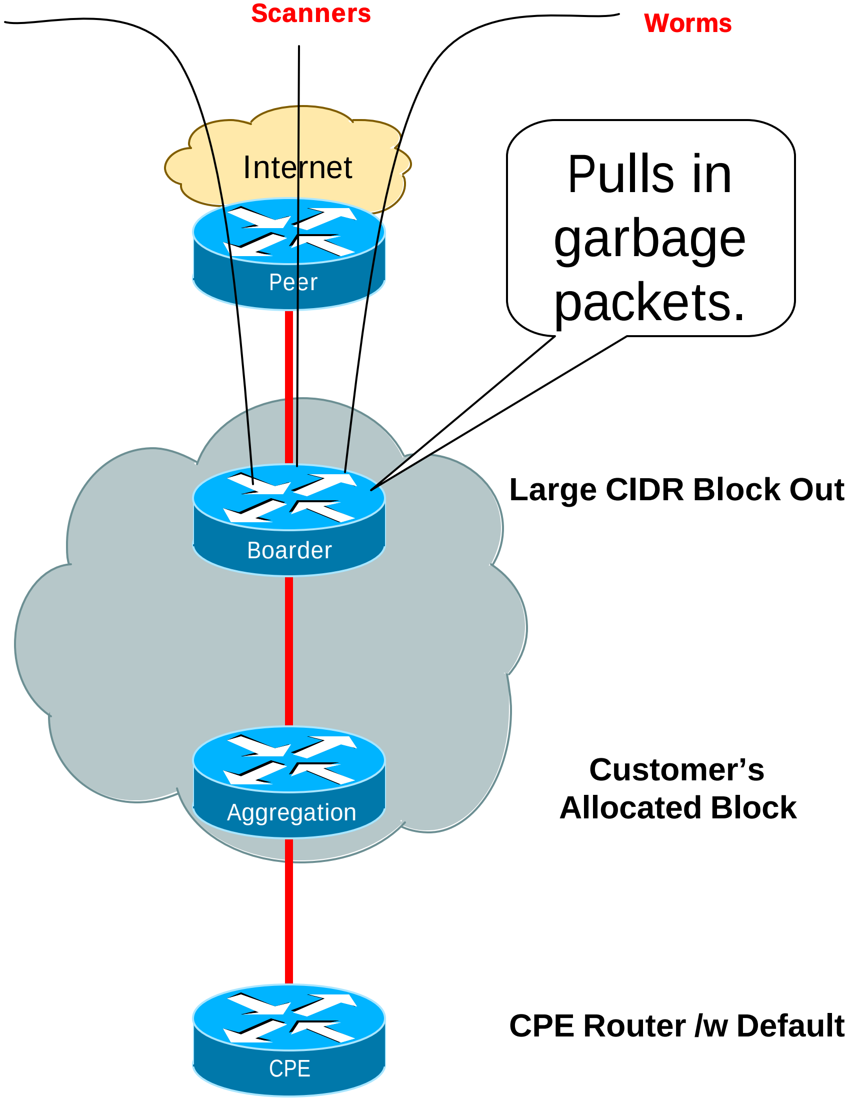
Simple Sink Holes – Customer Facing

- Defaults on CPE devices pull in everything.
- Default is the ultimate packet vacuum cleaner
- Danger to links during times of security duress.

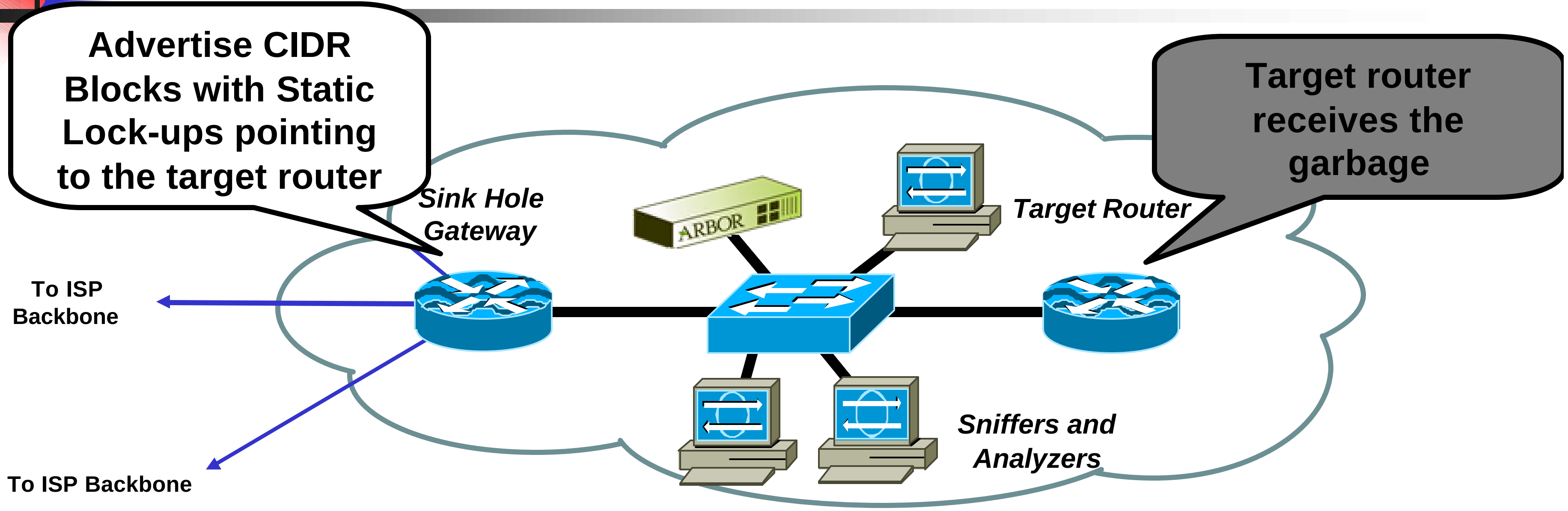


Simple Sink Holes – Impact Today

- In the past, this issue of pulling down garbage packets has not been a big deal.
- GigBots and Turbo Worms change everything
- Even ASIC-based forwarding platforms get impacted from the *RFC 1812 overhead.*



Sink Holes – Advertising Dark IP



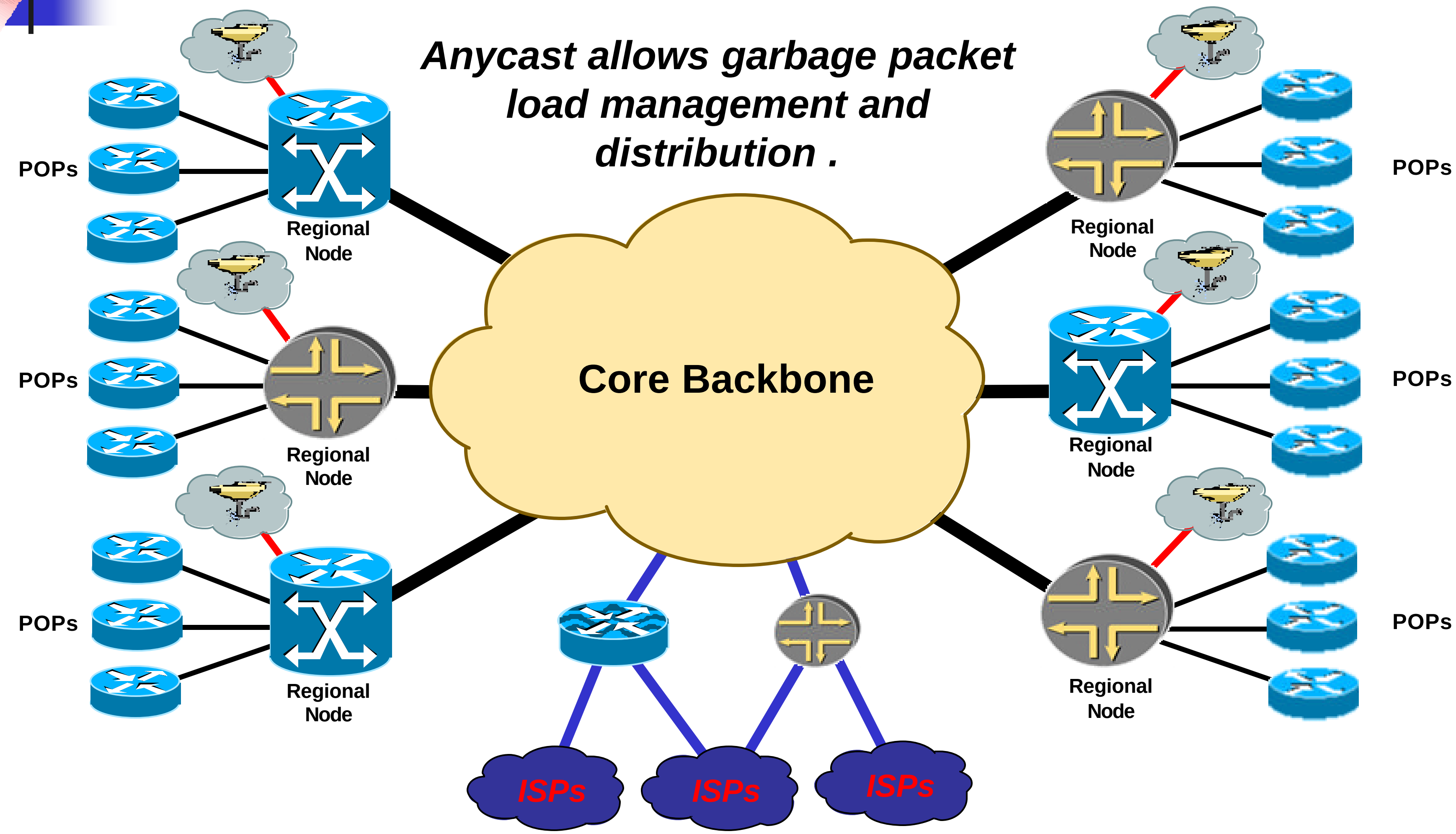
Advertise CIDR Blocks with Static Lock-ups pointing to the target router

Target router receives the garbage

- Move the CIDR Block Advertisements (or at least more-specifics of those advertisements) to Sink Holes.
- 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!

Anycast Sink Holes to Scale

Anycast allows garbage packet load management and distribution .



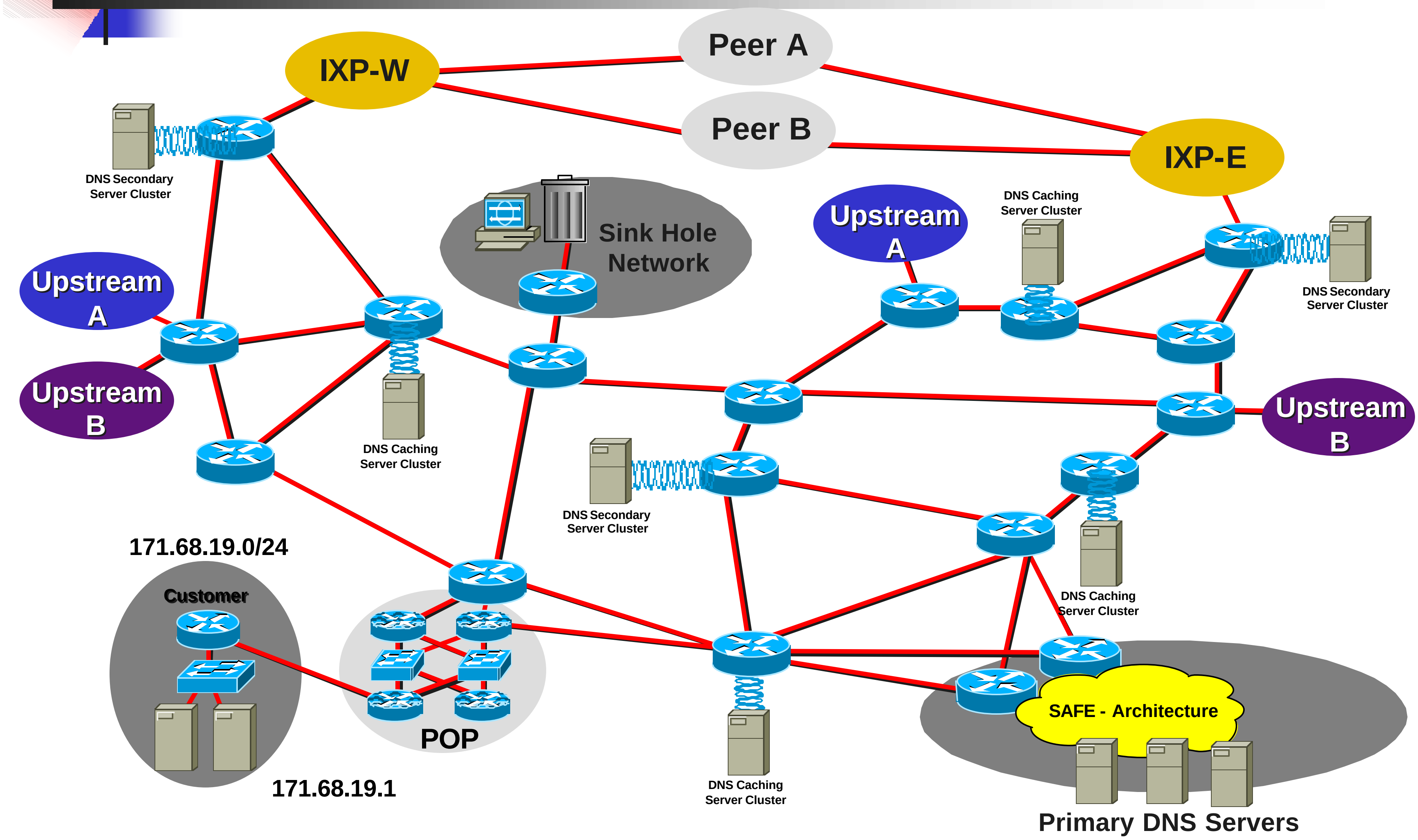
Anycasting Sink Holes

Scaling Sink Holes on existing infrastructure

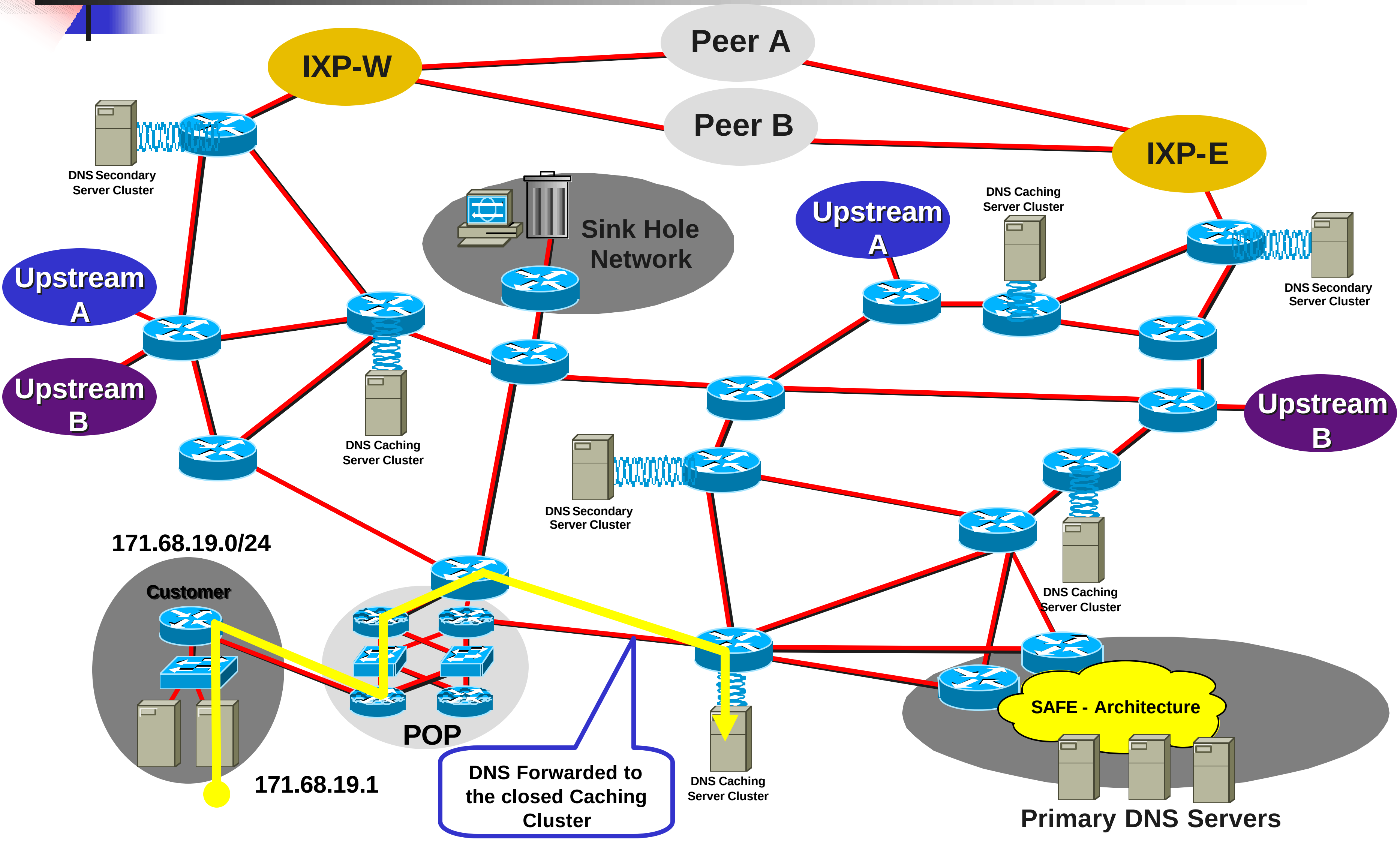
Anycast and Security: Applications

- Anycast is a technique sucessfully used in the community:
  - DNS Services
  - Distributed Sink Holes
  - Black Hole Routers - Dark IP Space Management (BGP Lock-up static routes to Null0)
  - Routing Convergance
- Anycast provides a tool to plug in Sink Holes through out an existing network.

Anycast DNS Caches

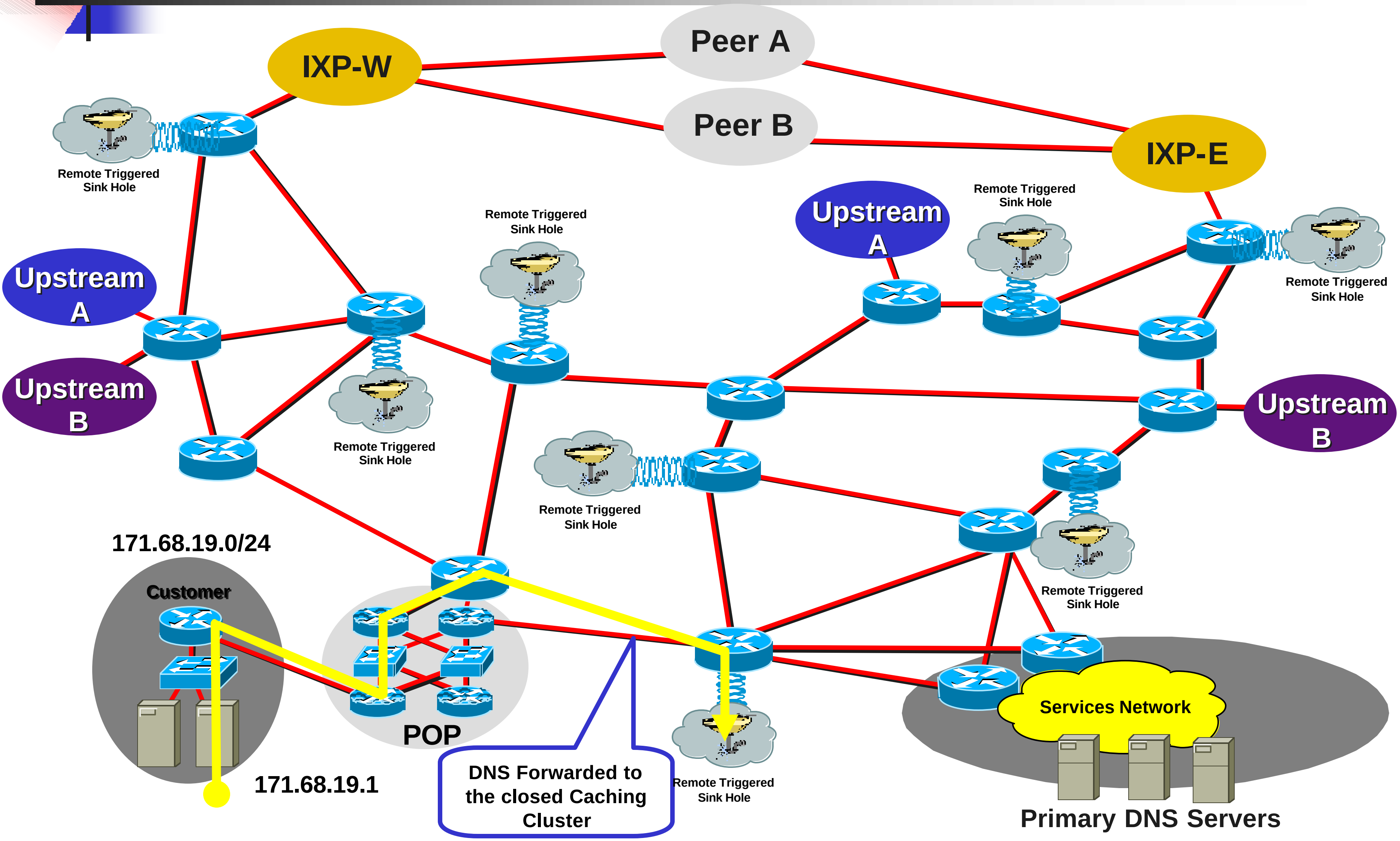

IXP-W
Peer A
Peer B
IXP-E
DNS Secondary Server Cluster
Sink Hole Network
Upstream A
DNS Caching Server Cluster
DNS Secondary Server Cluster
Upstream A
Upstream B
DNS Caching Server Cluster
Upstream B
DNS Secondary Server Cluster
DNS Caching Server Cluster
171.68.19.0/24
Customer
POP
171.68.19.1
DNS Caching Server Cluster
SAFE - Architecture
Primary DNS Servers

Anycast DNS Caches


IXP-W
Peer A
Peer B
IXP-E
DNS Secondary Server Cluster
Sink Hole Network
Upstream A
DNS Caching Server Cluster
DNS Secondary Server Cluster
Upstream A
Upstream B
DNS Caching Server Cluster
Upstream B
DNS Secondary Server Cluster
171.68.19.0/24
Customer
DNS Caching Server Cluster
POP
SAFE - Architecture
171.68.19.1
DNS Caching Server Cluster
Primary DNS Servers

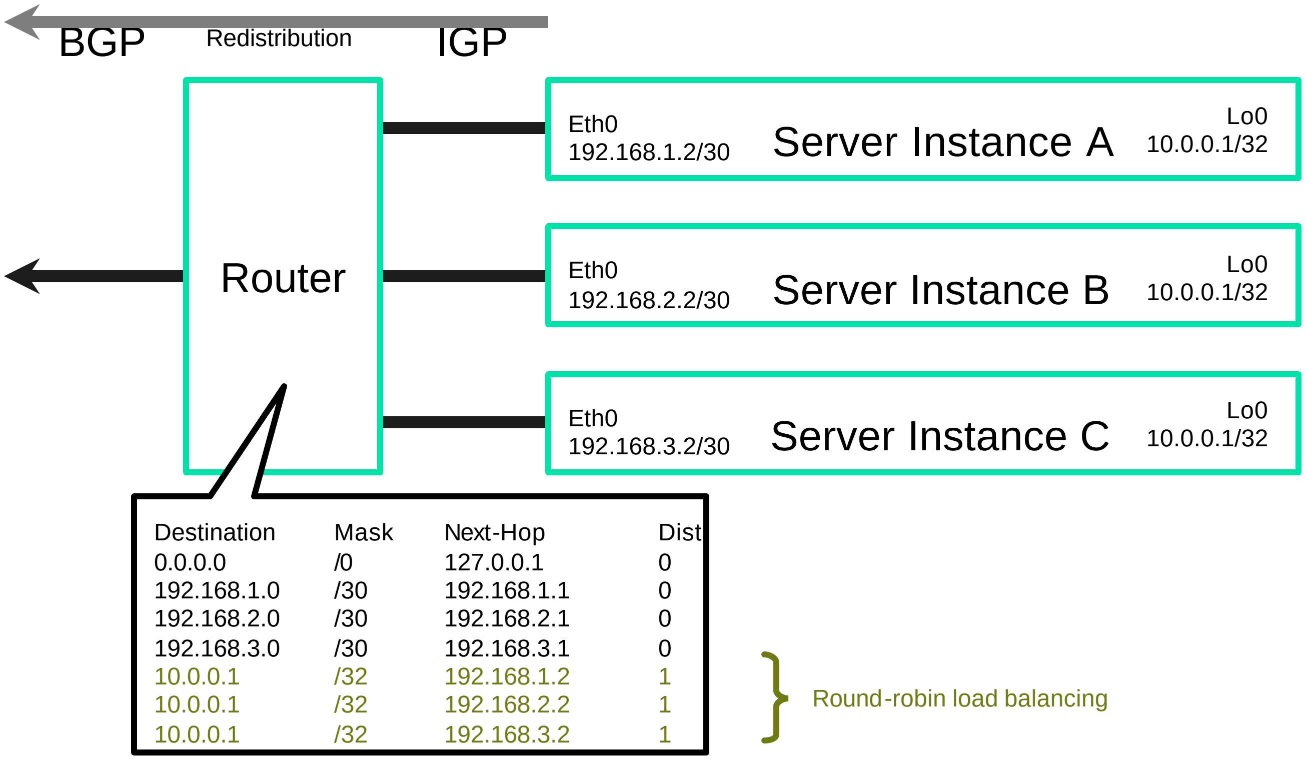
DNS Forwarded to the closed Caching Cluster

Anycast Sink Holes


IXP-W
Peer A
Peer B
IXP-E
Remote Triggered Sink Hole
Upstream A
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Upstream A
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
171.68.19.0/24
Customer
POP
171.68.19.1
Remote Triggered Sink Hole
Services Network
Primary DNS Servers

DNS Forwarded to the closed Caching Cluster

Anycast – What is needed?



Destination	Mask	Next-Hop	Dist
0.0.0.0	/0	127.0.0.1	0
192.168.1.0	/30	192.168.1.1	0
192.168.2.0	/30	192.168.2.1	0
192.168.3.0	/30	192.168.3.1	0
10.0.0.1	/32	192.168.1.2	1
10.0.0.1	/32	192.168.2.2	1
10.0.0.1	/32	192.168.3.2	1

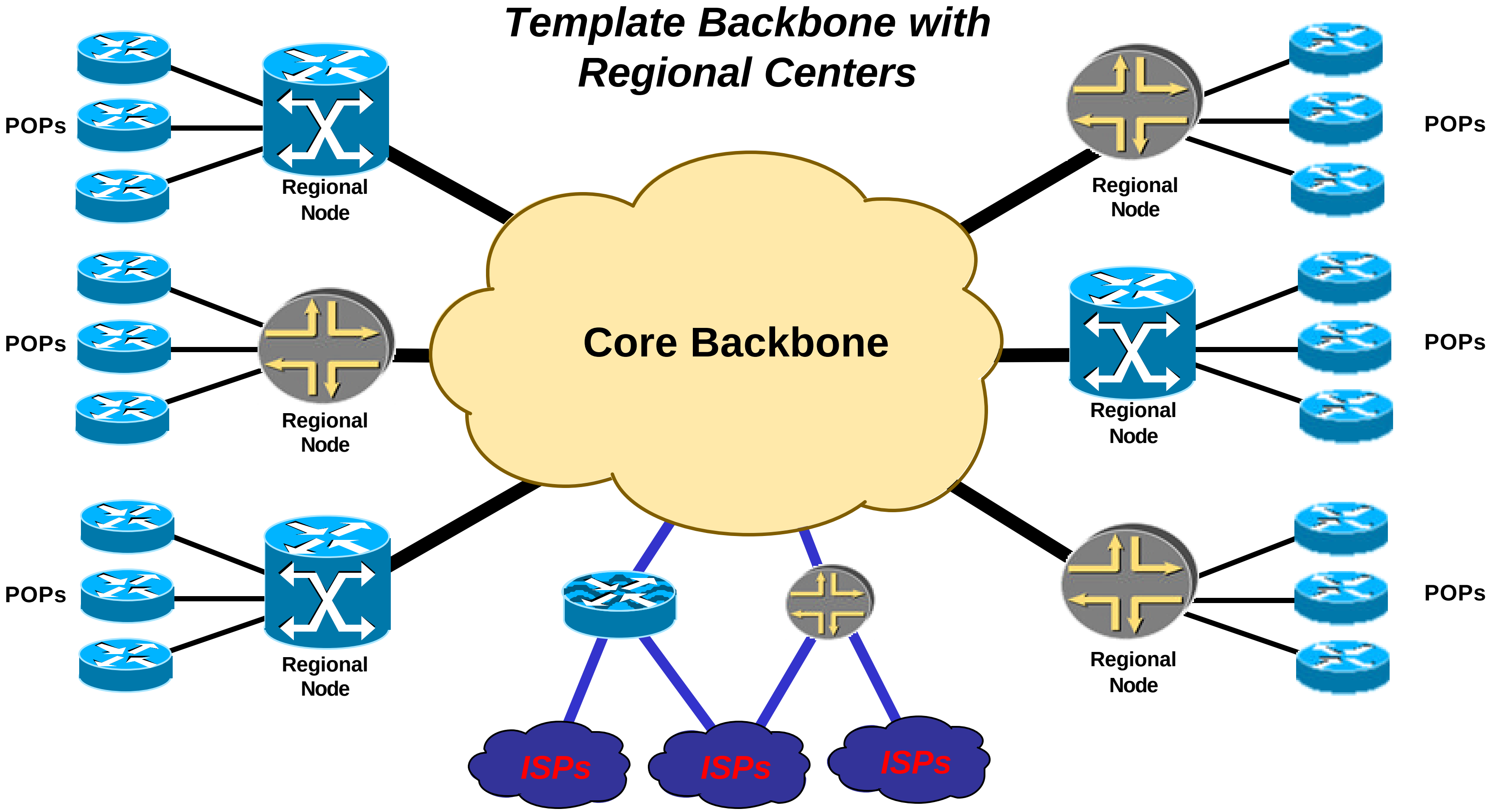
Courtesy of Bill Woodcock Packet Clearing House (www.pch..net)

- Two IP Addresses: One address for management & One address for anycasting.

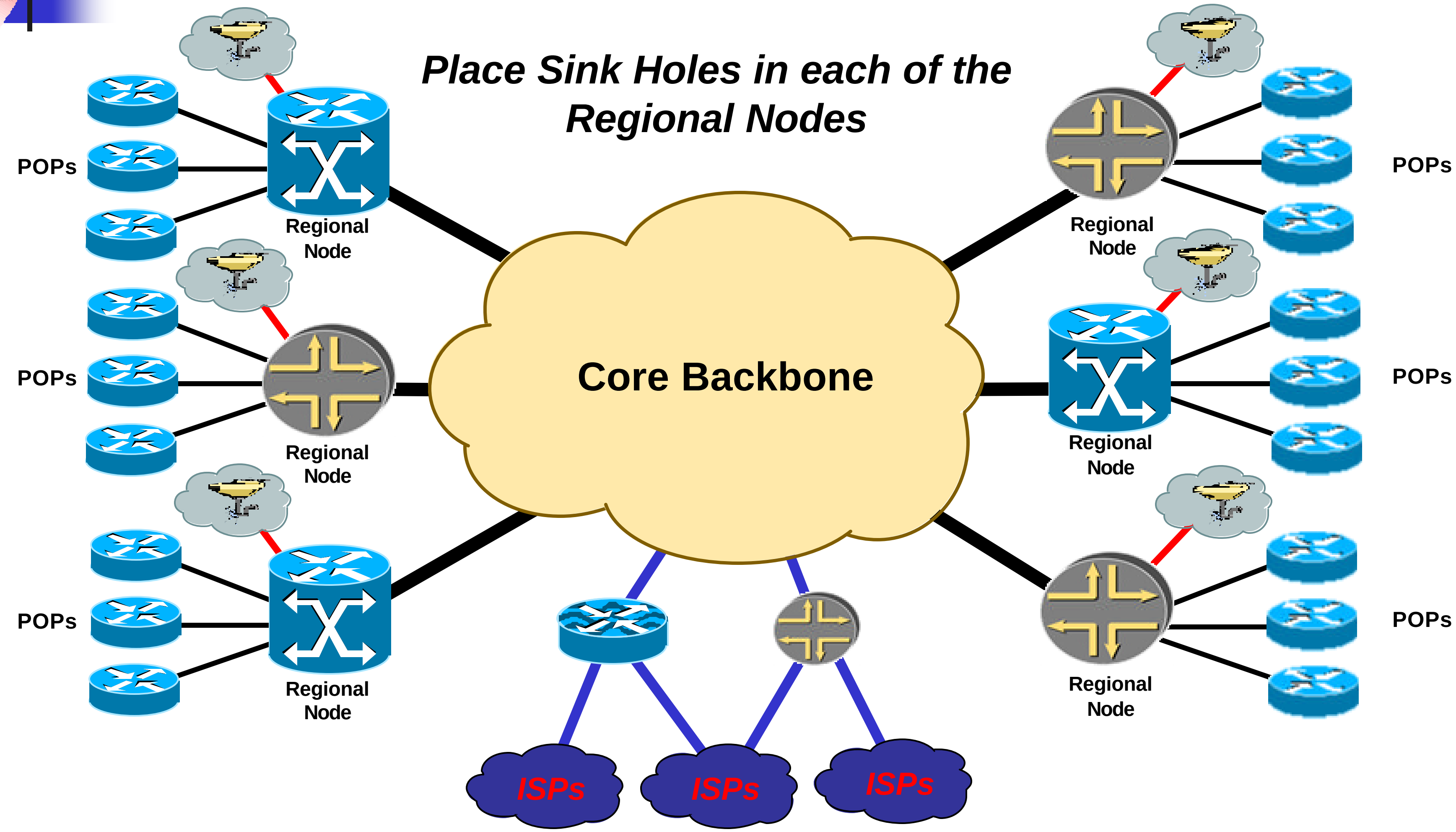
Anycast and Sink Holes

- Sink Holes are designed to pull in attacks.
- Optimal placement in the network requires mindful integration and can have substantial impact on network performance and availability
- A single Sink Hole might require major re-architecting of the network
- Anycast Sink Holes provide a means to distribute the load throughout the network.

Anycast Sink Holes Example



Anycast Sink Hole Placement


Place Sink Holes in each of the Regional Nodes

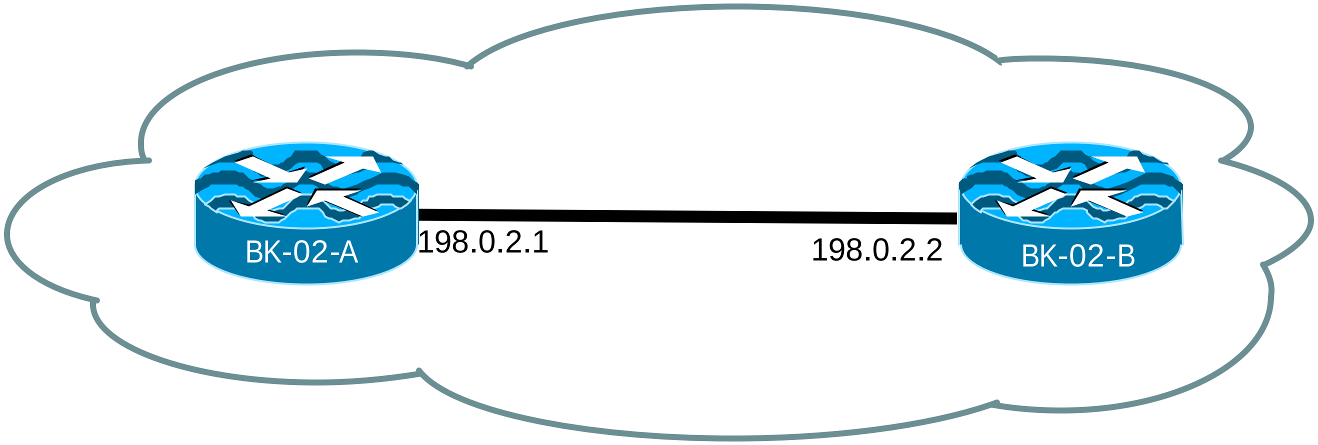
Anycast Sink Holes

- Anycast Sink Holes are in their early stages.
- Placement and control of the trigger routers are the two interesting challenges.
- These challenges will dissolve as more operational experience is gained.

Using Sink Holes to Protect Infrastructure Point to Point Links

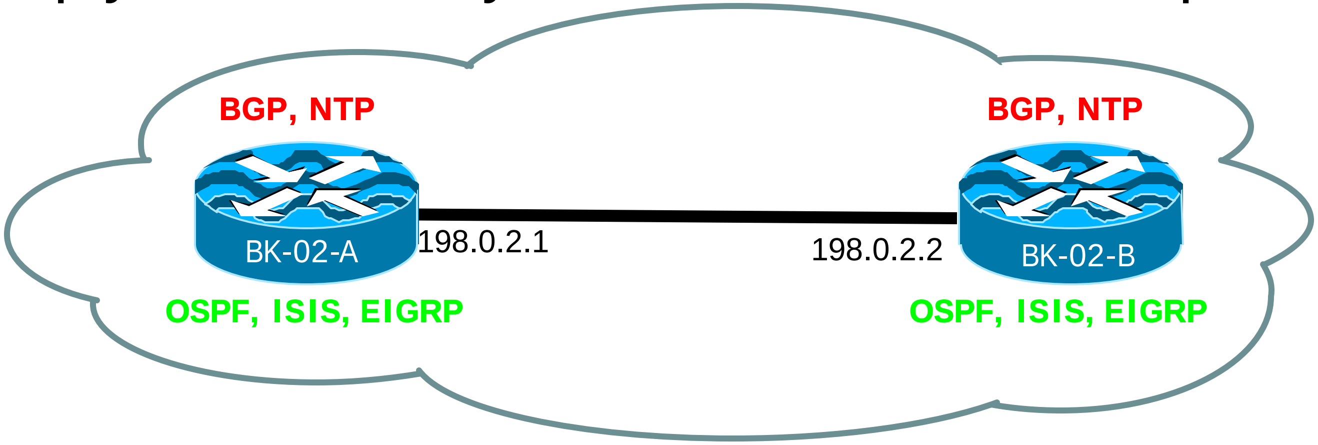
Protecting the Backbone Point to Point Addresses

- Do you really need to reach the Backbone router's Point to Point Address from any router other than a directly connected neighbor?



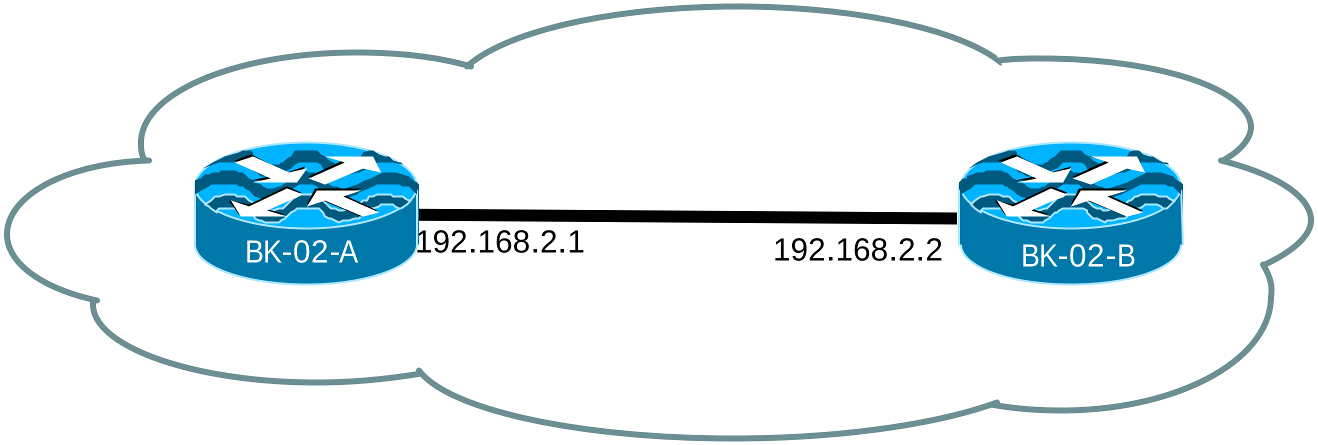
Protecting the Backbone Point to Point Addresses

- What could break?
  - Network protocols are either loopback (BGP, NTP, etc.) or adjacent (OSPF, IS-IS, EIGRP).
  - NOC can Ping the Loopback (alhough some tools such as HP OV may have issues).
  - Traceroutes reply with the correct address in the reply. Reachability of the source is not required.



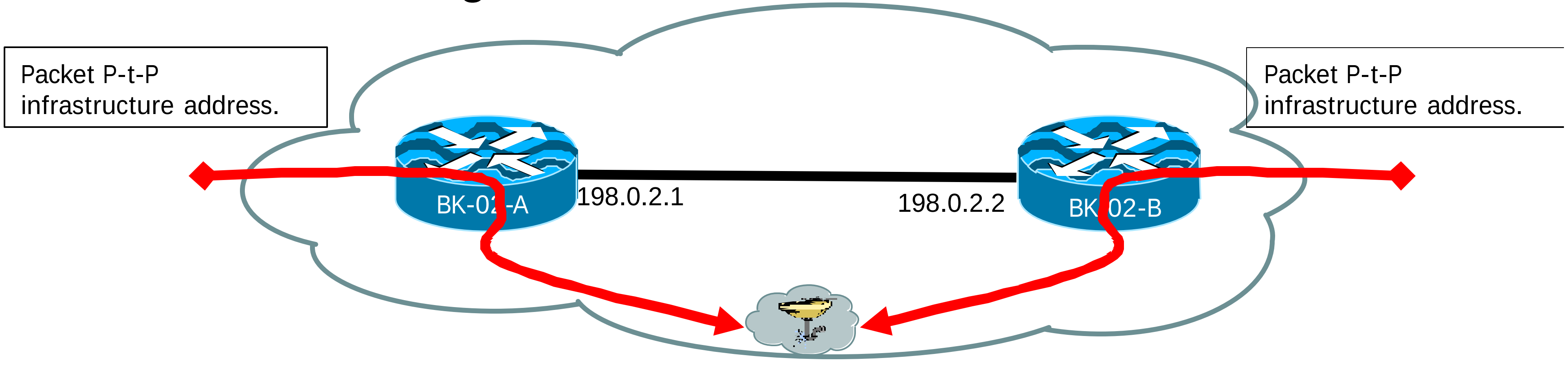
Protecting the Backbone Point to Point Addresses

- What have people done in the past:
  - ACLs – Long term ACL management problems.
  - RFC 1918 – Works – against the theme of the RFC – Traceroute still replies with RFC 1918 source address.
  - Does not protect against a reflection attack.



Protecting the Backbone Point to Point Addresses

- Move the Point to Point Address blocks to IGP based Sink Holes.
  - All packets to these addresses will be pulled into the Sink Hole.
  - People who could find targets with traceroute cannot now hit the router with an attack based on that intelligence.
  - Protects against internal and reflection based attacks.



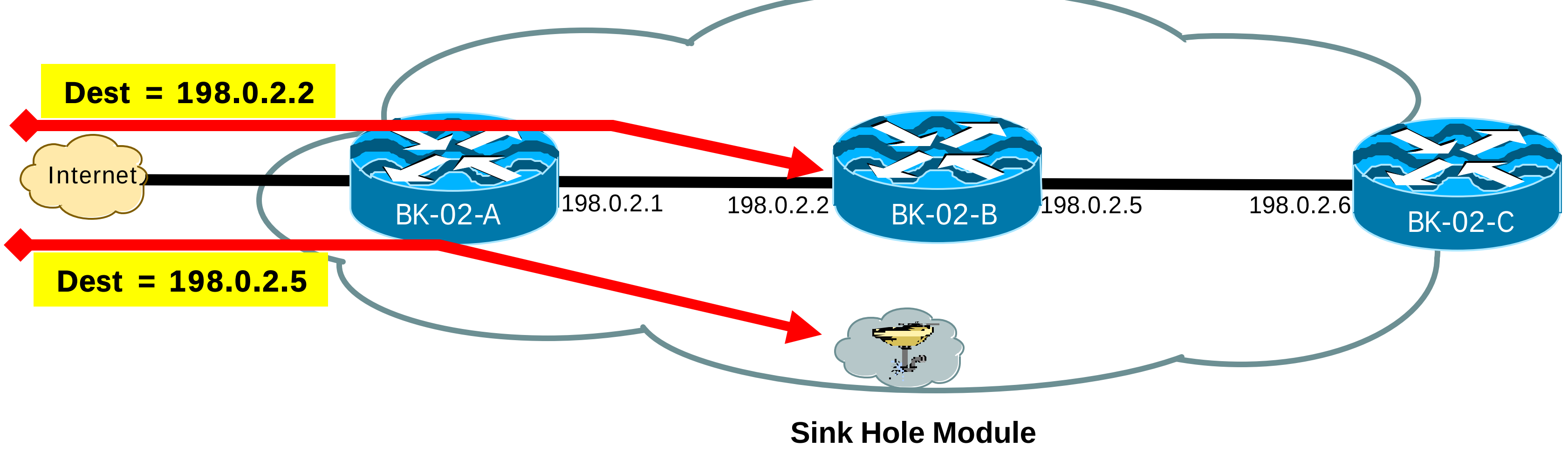
Packet P-t-P infrastructure address.

Packet P-t-P infrastructure address.

Sink Hole Module

Not Perfect – Just Another Hurdle.

- Will not work with the routers on the border.
  - By default, C (Connected) prefixes override all BGP injected prefixes from the Sink Hole (you want this to happen).
  - Basic security principle – increment layers of security – there is never a perfect solution – just additional hurdles – the more hurdles the better.



Dest = 198.0.2.2

Internet

BK-02-A

198.0.2.1

198.0.2.2

BK-02-B

198.0.2.5

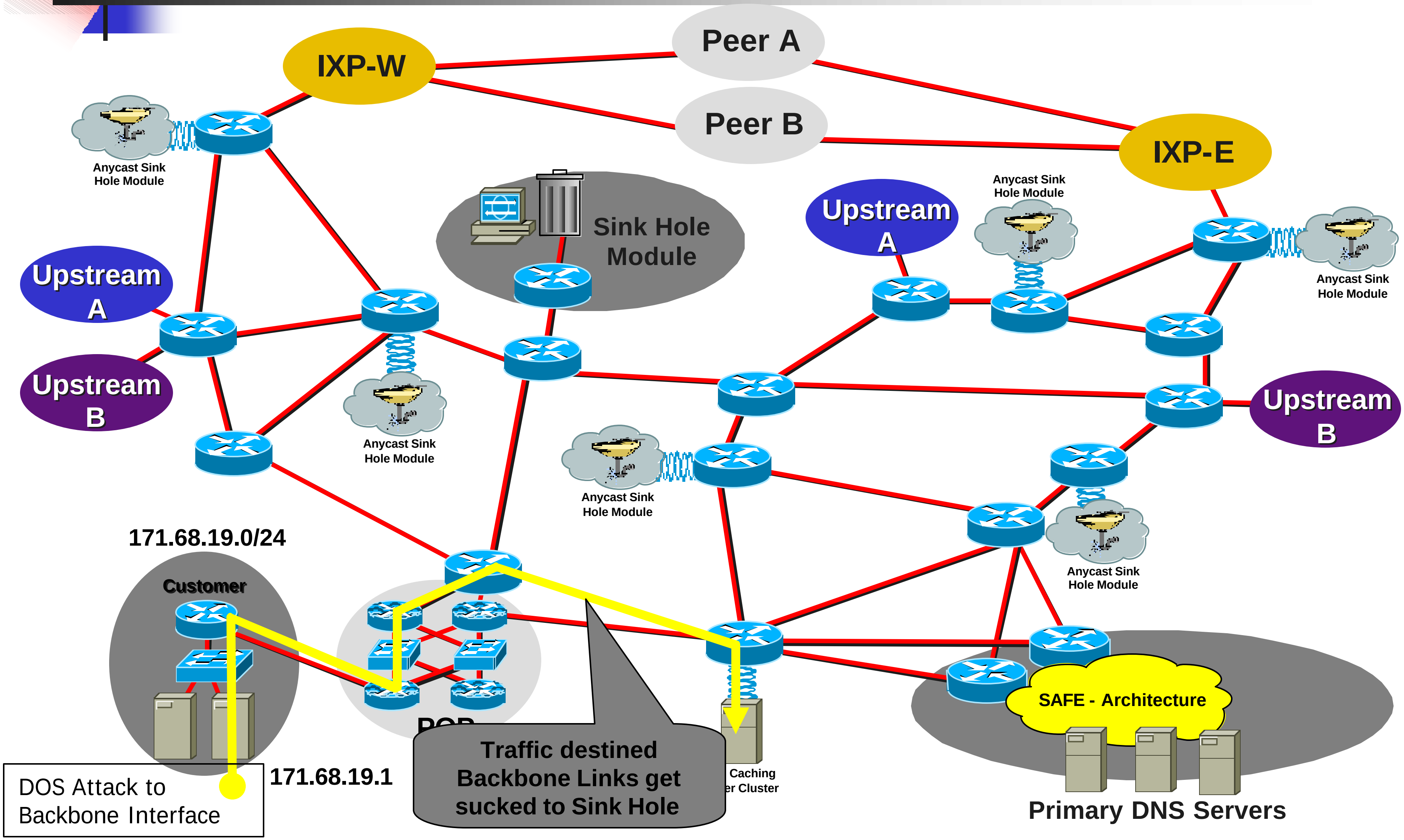
198.0.2.6

BK-02-C

Dest = 198.0.2.5

Sink Hole Module

Protecting the Backbone Point to Point Addresses

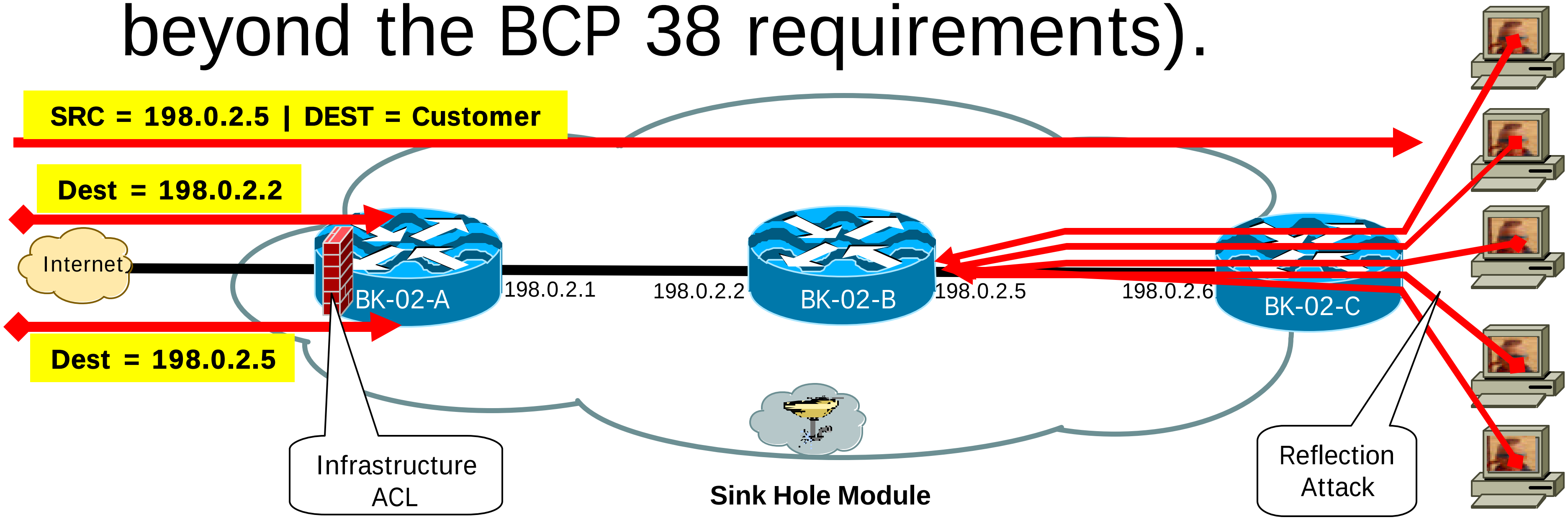


DOS Attack to Backbone Interface

Traffic destined Backbone Links get sucked to Sink Hole

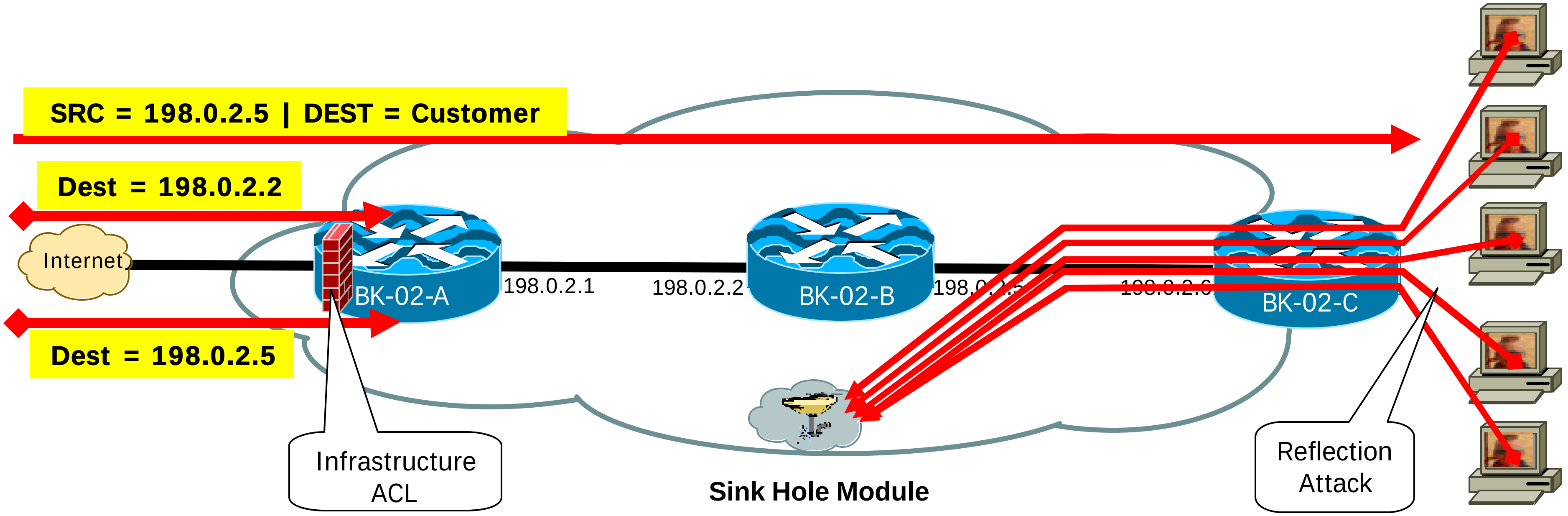
What if I do an ISP Edge ACL?

- Anti-Spoof and Anti-Infrastructure ACLs are encouraged on the edge. But ....
- Need to be everywhere to achieved desired effect – including the customer edge (this is beyond the BCP 38 requirements).



What if I do an ISP Edge ACL?

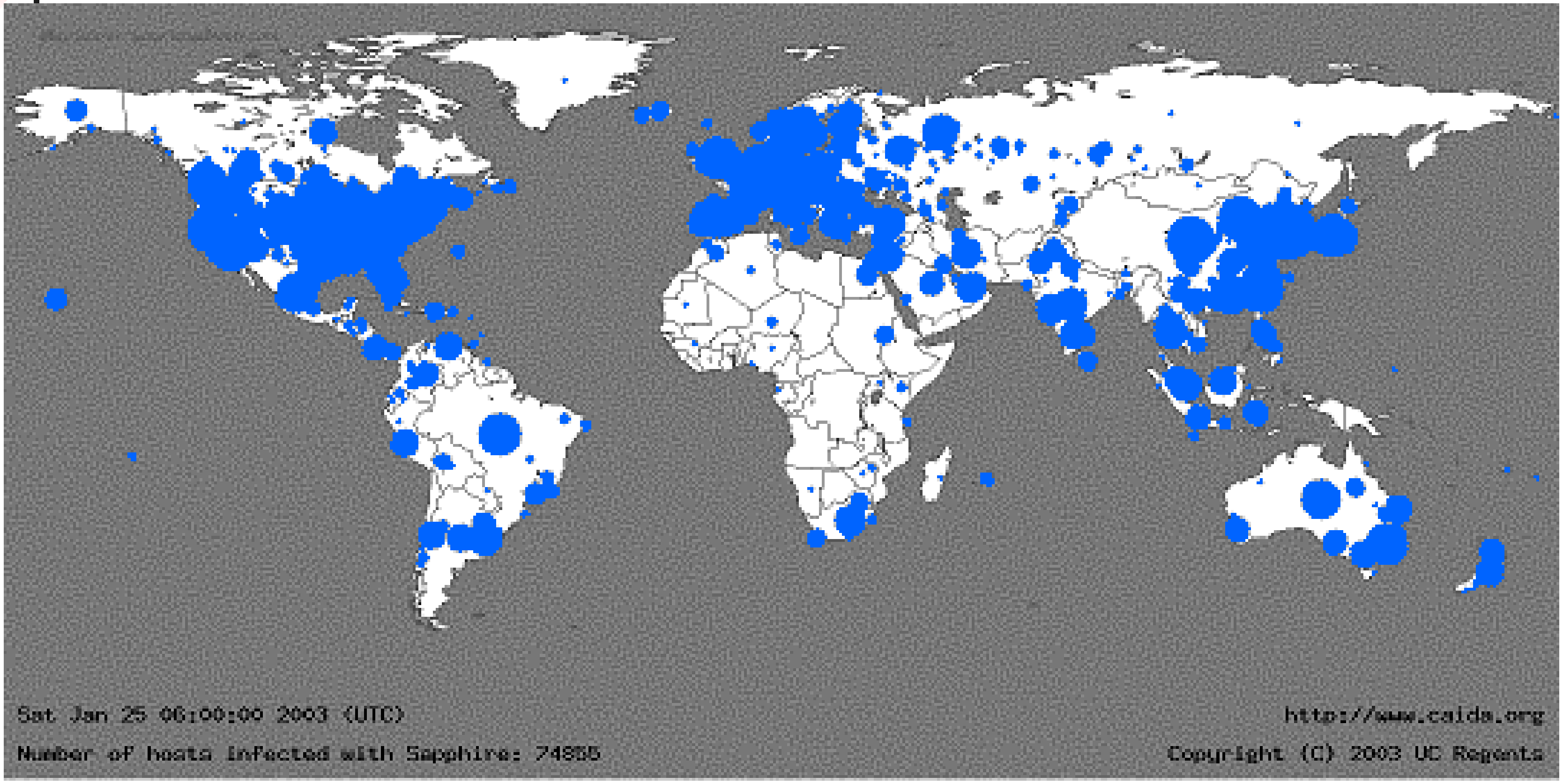
- Anti-Spoof and Anti-Infrastructure ACLs can be combined with Sink Holing the Infrastructure Blocks.
- Remember – it is all about adding *hurdles.*



Sink Holes and Turbo Worms

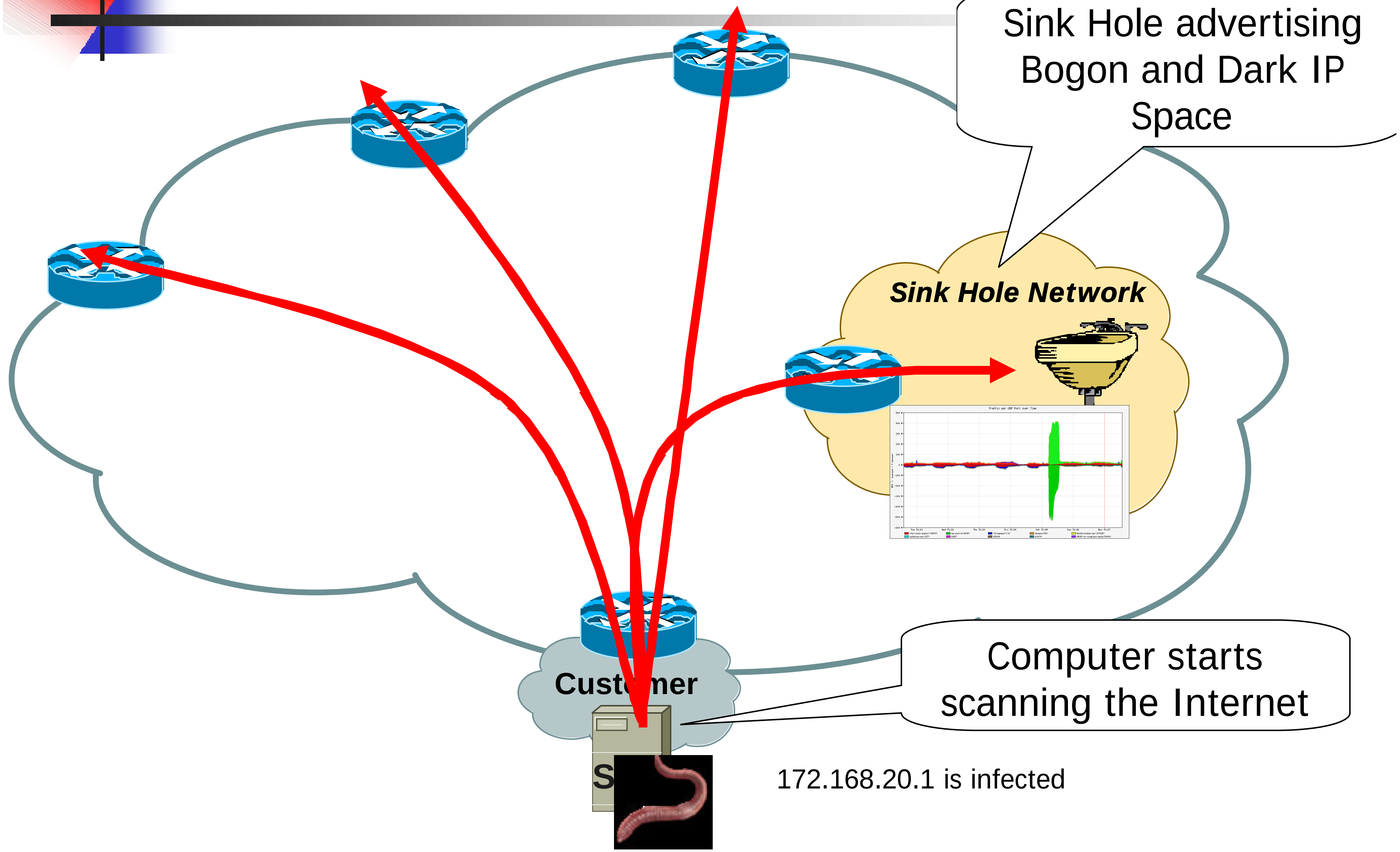
Are you ready for the next one?

The SQL Slammer Worm:
30 Minutes After “Release”


Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

- Infections doubled every 8.5 seconds
- Spread 100X faster than Code Red
- At peak, scanned 55 million hosts per second.

Infected End Points

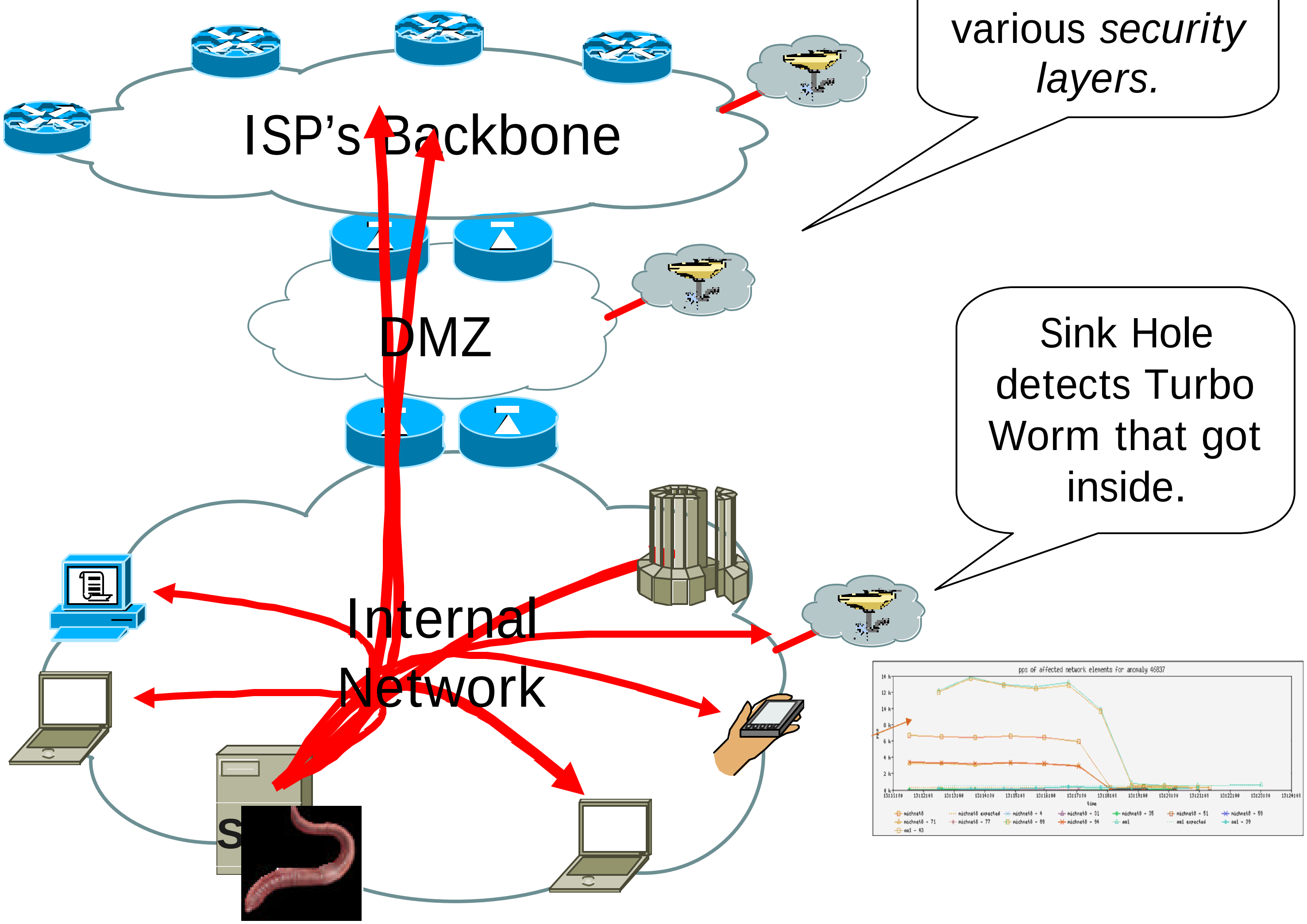


Sink Hole advertising Bogon and Dark IP Space

Computer starts scanning the Internet

172.168.20.1 is infected

Expect Turbo Worms from All Directions!



Sink Holes at various *security layers.*

Sink Hole detects Turbo Worm that got inside.

Turbo Worms - Conclusion

- The nature of the threat dictates that you need to prepare before it happens.
- 30 minutes just enough time to react with what you have.
  - Remember the post-Slammer analysis – Slammer's search algorithms were "broken"
- Sink Holes are one tool that has proven their value – especially with worm mitigation (after containment).

Know Your Network -- Be Prepared!

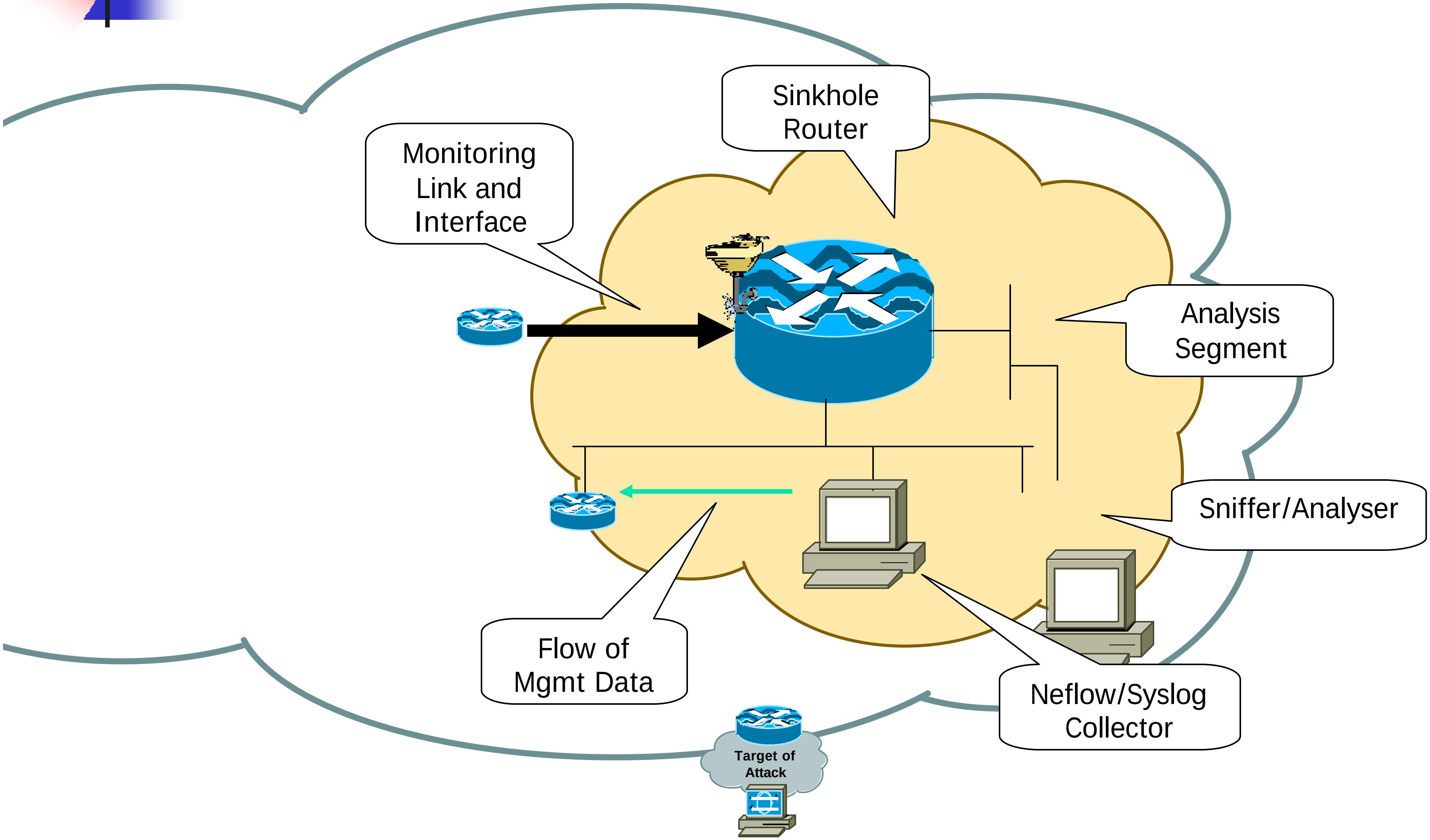
Questions?

Addendum - Materials

Sinkholes - Addendum

Construction

Sinkhole Router



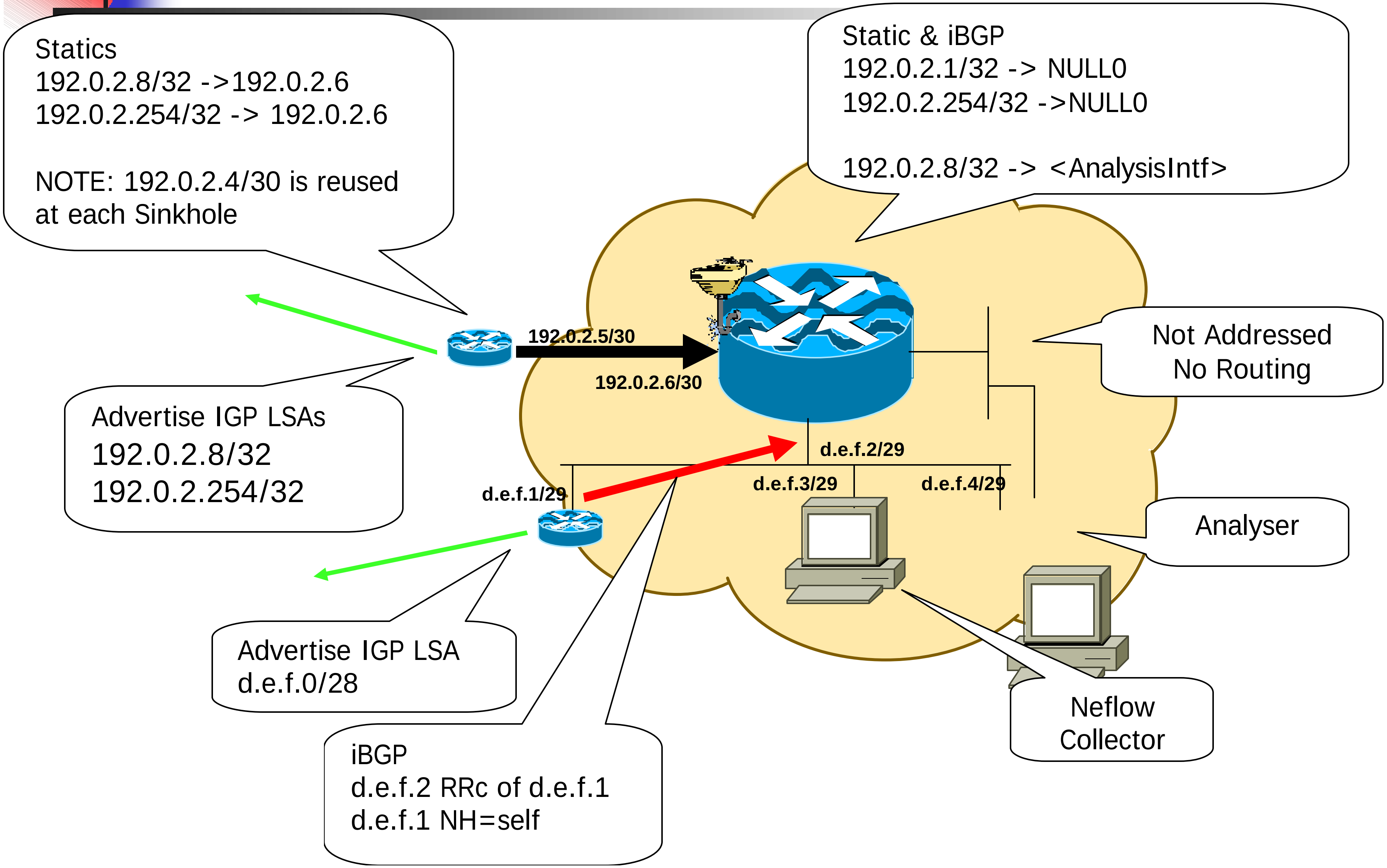
Guidelines

- No IGP on Sinkhole
- iBGP
  - Peering sessions via Management Interface
  - Sinkhole is a RRc
- Monitoring Interface to data-plane only
- Routes injected into IGP by router servicing the Monitoring Link

TestNet Address Allocation

Address Block	Purpose
192.0.2.1/32	All iBGP routers for “Drop to NULL0”
192.0.2.4/30	Monitor Link addresses NOTE: provision these addresses in all Sinkholes
192.0.2.254	ANYCAST Sinkhole Address
192.0.2.8 -> balance	Sinkhole Diversion Addresses

Sinkhole Router - Routing



Statics
192.0.2.8/32 ->192.0.2.6
192.0.2.254/32 -> 192.0.2.6

NOTE: 192.0.2.4/30 is reused
at each Sinkhole

Static & iBGP
192.0.2.1/32 -> NULL0
192.0.2.254/32 ->NULL0

192.0.2.8/32 -> <AnalysisIntf>

Not Addressed
No Routing

Advertise IGP LSAs
192.0.2.8/32
192.0.2.254/32

Analyser

Advertise IGP LSA
d.e.f.0/28

Neflow
Collector

iBGP
d.e.f.2 RRc of d.e.f.1
d.e.f.1 NH=self

BGP Triggers for Sinkholes - Addendum

Configuration

Trigger Router’s Config

```
router bgp 100
.
redistribute static route-map static-to-bgp
.
!
route-map static-to-bgp permit 10
 description – Std Redirect For Edge Drop
 description - Use Static Route with Tag of 66
 match tag 66
 set origin igp
 set next-hop 192.0.2.1
 set community NO-EXPORT
!
```

Trigger Router’s Config

```
!
route-map static-to-bgp permit 20
 description – Redirect For Sinkhole NULL0 Drop
 description - Use Static Route with Tag of 67
 match tag 67
 set origin igp
 set next-hop 192.0.2.8
 set community NO-EXPORT 67:67
!!
```

Trigger Router’s Config

```
!
route-map static-to-bgp permit 30
 description – Redirect For Sinkhole Analysis
 description - Use Static Route with Tag of 68
 match tag 68
 set origin igp
 set next-hop 192.0.2.8
 set community NO-EXPORT 68:68
!!
```

Trigger Router’s Config

```
!
route-map static-to-bgp permit 40
 description – Redirect For ANYCAST Sinkhole
 description - Use Static Route with Tag of 69
 match tag 69
 set origin igp
 set next-hop 192.0.2.254
 set community NO-EXPORT 69:69
!!
```

Trigger Router’s Config

```
!
route-map static-to-bgp permit 50
 description – Redirect For ANYCAST Sinkhole Analysis
 description - Use Static Route with Tag of 70
 match tag 70
 set origin igp
 set next-hop 192.0.2.254
 set community NO-EXPORT 70:70
!
route-map static-to-bgp permit 100
```

Sinkhole Triggers

```
! Drop all traffic at edge of network
ip route 172.168.20.1 255.255.255.255 null0 tag 66
!
! Redirect victim traffic to Sinkhole
ip route 172.168.20.1 255.255.255.255 null0 tag 67
!
! Redirect victim traffic to Sinkhole for Analysis
ip route 172.168.20.1 255.255.255.255 null0 tag 68
```

ANYCAST Triggers

```
! Redirect victim traffic to ANYCAST Sinkhole
ip route 172.168.20.1 255.255.255.255 null0 tag 69
!
! Redirect victim traffic to ANYCAST Sinkhole
! for Analysis
ip route 172.168.20.1 255.255.255.255 null0 tag 70
```

Sinkhole Router – Config

```
router bgp 100
.
 Neighbor peer-group INTERNAL
 neighbor INTERNAL route-map Redirect-to-Sinkhole in
 neighbor INTERNAL remote-as 100
 neighbor d.e.f.1 peer-group INTERNAL
!
route-map Redirect-to-sinkhole permit 10
 description - Send to Router's NULL0 Interface
 match community 67:67
 set ip next-hop 192.0.2.1
!
```

Sinkhole Router – Config

```
route-map Redirect-to-sinkhole permit 20
 description - Send to Router's Analyser Intf
 match community 68:68
 set ip next-hop 192.0.2.8
!
```

Sinkhole Router – Config

```
route-map Redirect-to-sinkhole permit 30
 description – ANYCAST drop
 match community 69:69
 set ip next-hop 192.0.2.1
!
```

Sinkhole Router – Config

```
route-map Redirect-to-sinkhole permit 40
 description – Anycast Analysis
 match community 70:70
 set ip next-hop 192.0.2.8
!
Route-map Redirect-to-sinkhole permit 100
```

Sinkhole Router – Routing

```
! For Std drop
ip route 192.0.2.1 255.255.255.255 null0
!
! For Analysis
ip route 192.0.2.8 255.255.255.255 interface FA0/0
!
! Bogus ARP for 192.0.2.8 to stop ARP request
ip arp 192.0.2.8 00.00.0c.99.99.99 arpa
!
! For ANYCAST Sinkhole Services
ip route 192.0.2.254 255.255.255.255 null0
```

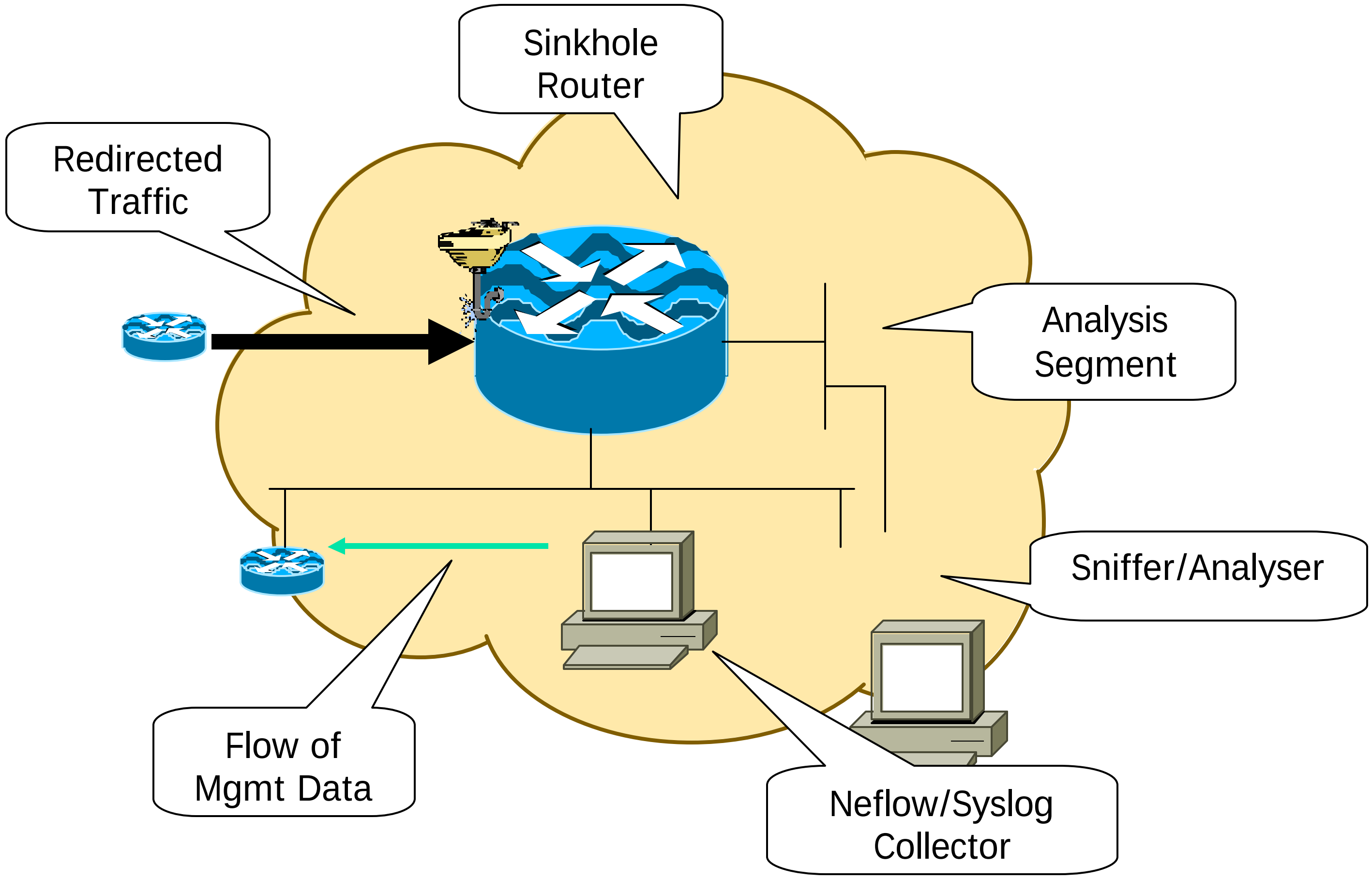
Sinkhole Router – Routing

- No Default static route in Sinkhole.
  - Sinkhole must not loop traffic back out Management Interface.
  - Telnet access via router servicing the Sinkhole's Management Segment.

Sinkhole Router – Routing

- No Default static route in Sinkhole.
  - Sinkhole must not loop traffic back out Management Interface.
  - Telnet access via router servicing the Sinkhole’s Management Segment.

Sinkhole Router



Sinkhole Analysis Services

- Local Netflow Collector and Analyser
- Local Syslog Server
- Analyser remotely controlled
  - I.e. VNC or Telnet

Results / Benefits

- Traffic pulled from Victim
- Control collateral damage
- iBGP Triggered
- Allows attack flow analysis

In-Depth Analysis

- Be careful: you must contain any attack traffic, do not become a victim as well
  - Outbound filtering: do not let sever connect back out at will
  - Outbound filter ACE hits (and IP logs) will provide additional information