Customer-Triggered Real-Time Blackholes

Tim Battles tmbattles@att.com

Danny McPherson danny@arbor.net

Chris Morrow chris@uu.net

Agenda

- About Blackhole Routing
- Preparing the Tools
- Customer-Triggered Blackholes
- BGP Flow Specification

Before We Begin…

- How many folks in the room are responsible for network security at an ISP or enterprise?
- How many folks here employ blackhole routing today?
- How many employ source-based blackhole routing?
- How many folks here currently support customer-triggered blackhole routing?

About (D)DOS

- *It could come from anywhere; be prepared!*

About Blackhole Routing

Remote-Triggered Blackholes

- Remote-triggered Blackhole filtering is the foundation for a whole series of techniques to traceback and react to (D)DOS attacks on an ISP’s network.
- Preparation is key and does not impact ISP operations or network performance.
- Adds significant capabilities to an ISP’s security toolkit!

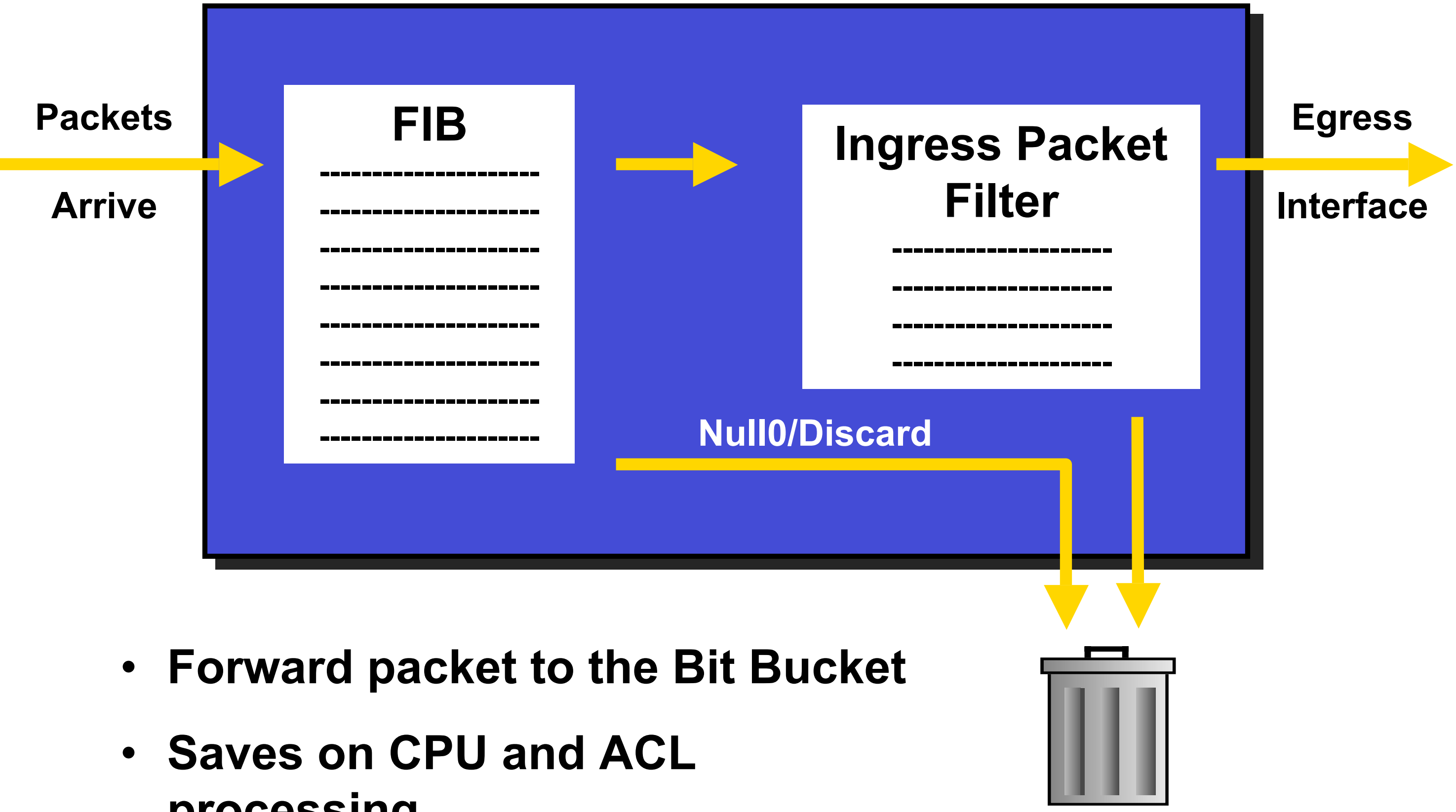
Miscellaneous

- Detection & Traceback
- ACLs are difficult to deploy (e.g., augment, deployment time, configuration management, performance, hardware support, etc..)
- NetFlow
- IP Accounting
- Raw Interface Stats

About Blackhole Routing

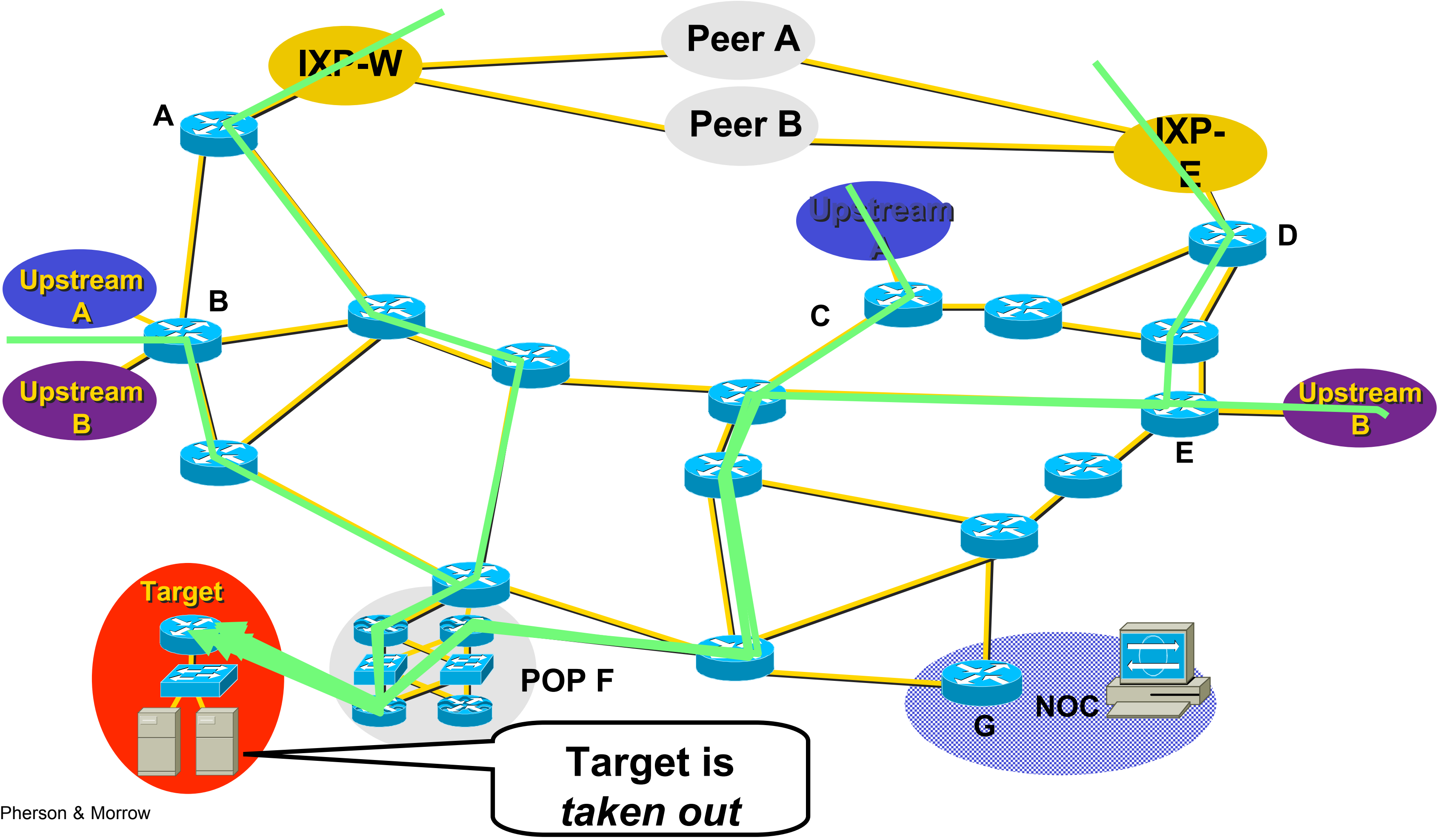
- *Blackhole Routing* or *Blackhole Filtering* results in packets being forwarded to a router's *bit bucket*, also know as:
  - Null 0
  - Discard Interface
- Initially worked only based on destination address, per it's exploit of a routers forwarding logic
- Typically results in desired packets being dropped with minimal or no performance impact.

Exploits Forwarding Logic

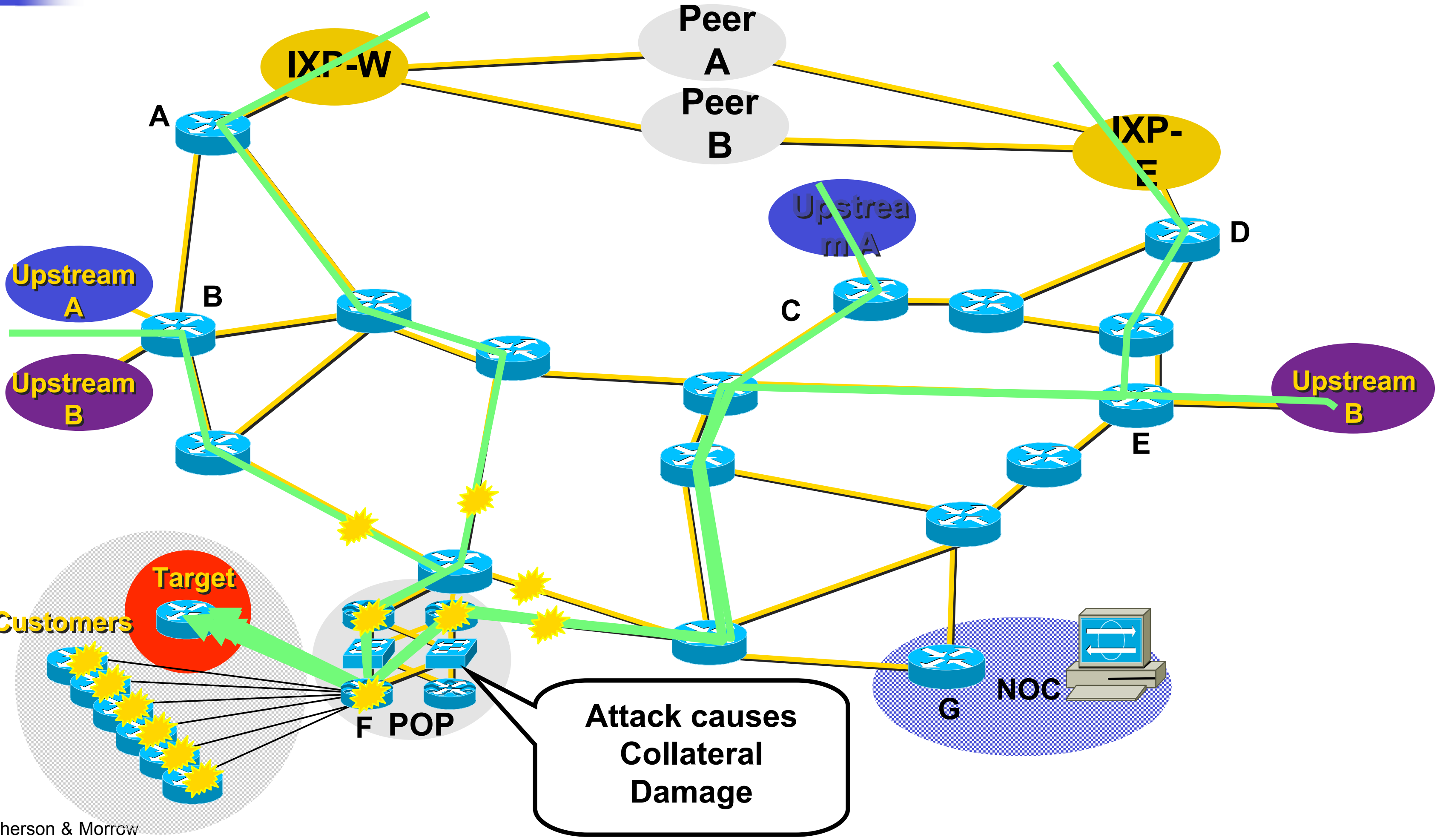


- **Forward packet to the Bit Bucket**
- **Saves on CPU and ACL processing**

Customer is DOSed – Before

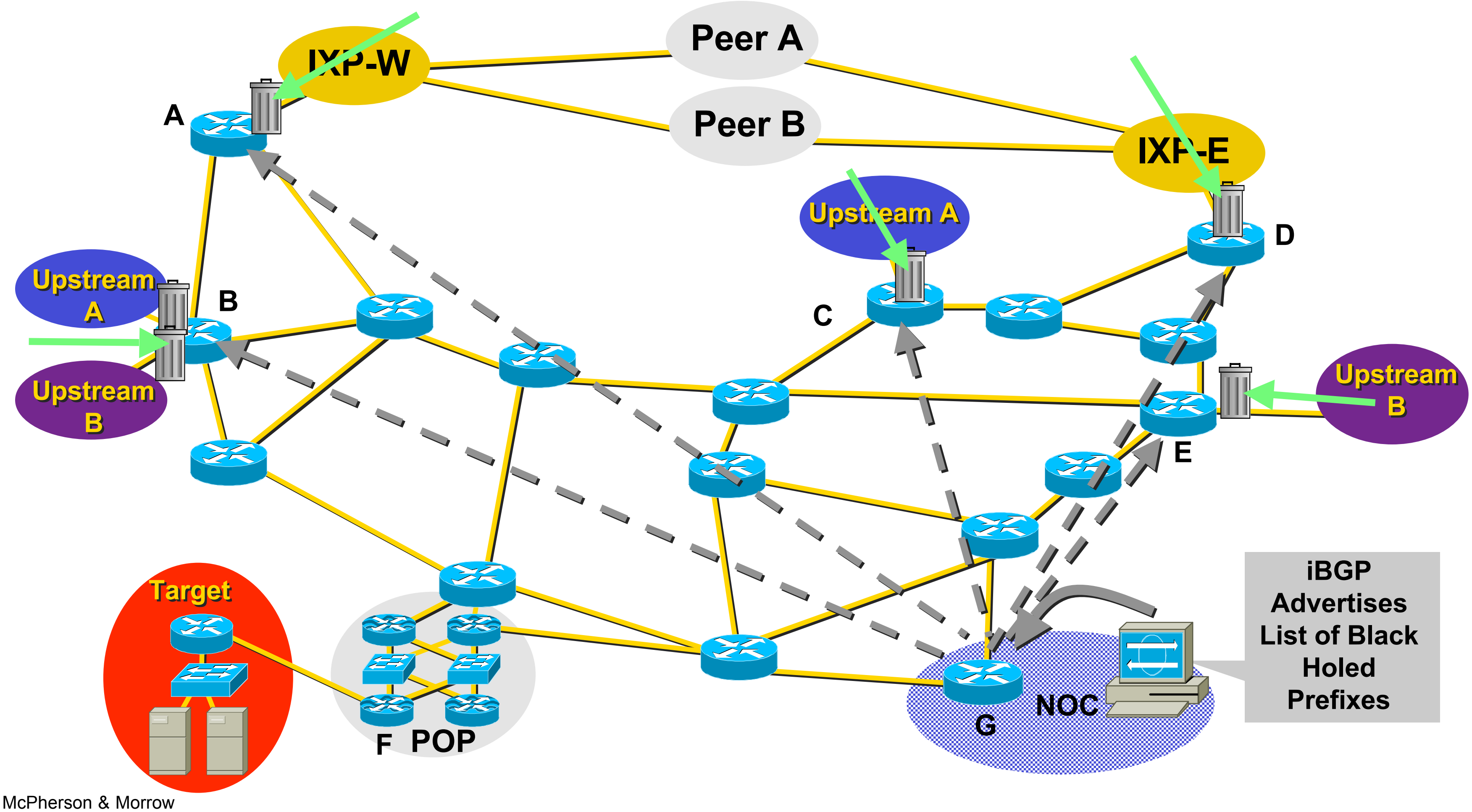


Customer is DOSed – Before – Collateral Damage



Attack causes Collateral Damage

Customer is DOSed – After – Packet Drops Pushed to the Edge



iBGP Advertises List of Black Holed Prefixes

Preparing for Blackhole Routing

Remotely Triggered Blackhole Filtering

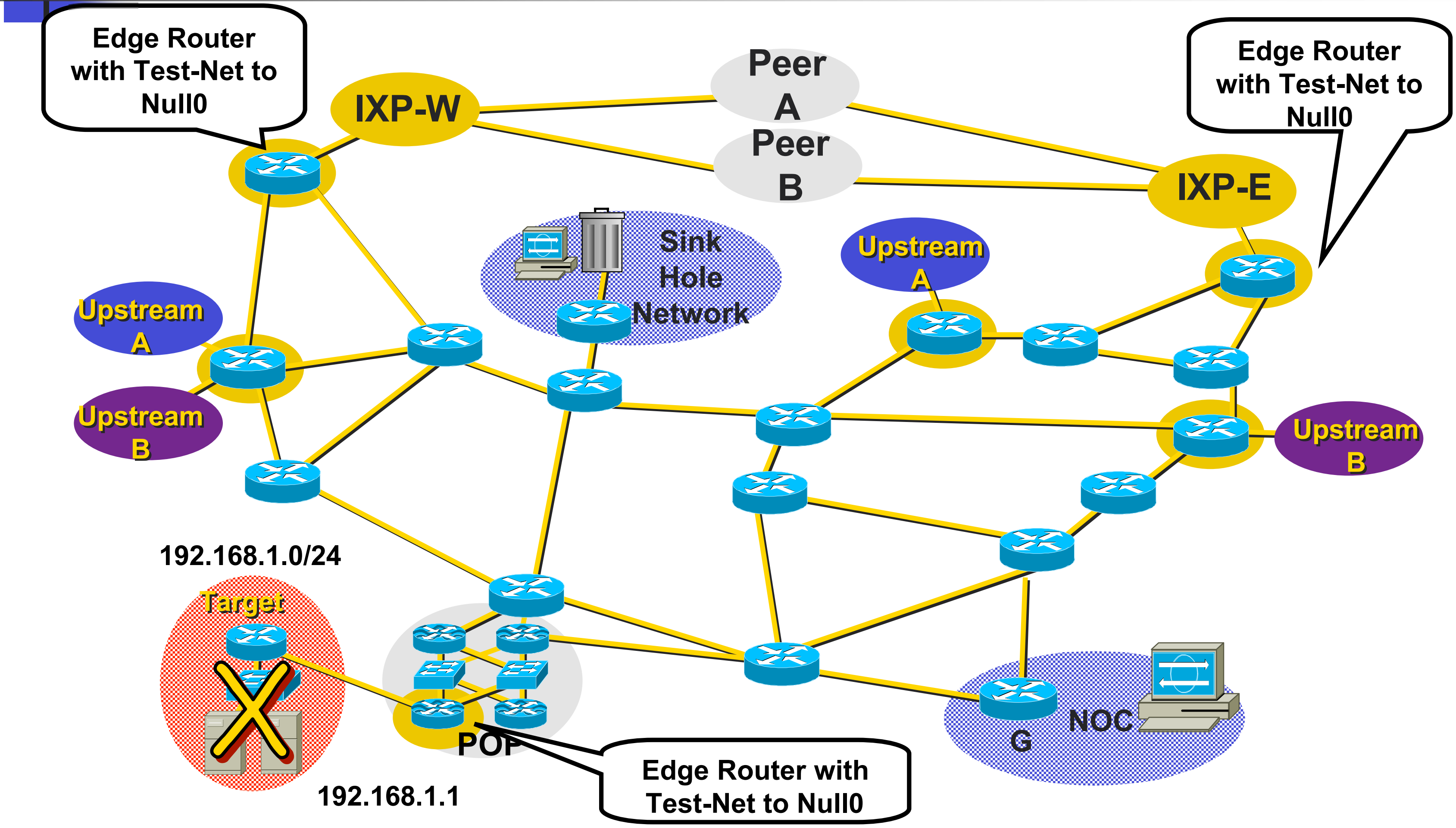
- Use BGP to trigger a network-wide response to a multi-source attack flow
- A static route and BGP will allow an ISP to trigger network-wide destination address blackholes as quickly as iBGP converges through the network.
- Provides ISPs a tool that can be used to respond to distributed denial of service events or employ techniques such as Backscatter Traceback[backscatter]

Step 1: Prepare all the Routers

- Allocate a small block of address space (e.g., RFC 1918 space or IANA reserved space) to be dedicated for black hole filtering. TEST-NET [RFC 3330], 192.0.2.0/24 is a potential option.
- Configure a static route on each router with your selected route, pointing to Null 0 or the discard:

```
ip route 192.0.2.1 255.255.255.255 Null0 255
ip route 192.0.2.2 255.255.255.255 Null0 199
ip route 192.0.2.3 255.255.255.255 Null0 50
```

Step 1- Prepare all the Routers w/ Trigger



Sample TEST-NET Allocation

Address Block	Purpose
192.0.2.1/32	All iBGP routers for “Drop to NULL0”
192.0.2.2/32	All Peering Edge routers drop
192.0.2.3/32	All Customer Edge routers drop
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

Step 2: Prepare the Trigger Router

- The trigger router is the device that will inject the iBGP announcement into the ISP's network
  - Should be part of iBGP mesh, but need not accept routes
  - Can be a separate router (or security tool)
  - Can be a production router
  - Can be a workstation with Zebra/GateD (interface with PERL scripts or other tools)
  - Commercial tools such as Arbor's Peakflow

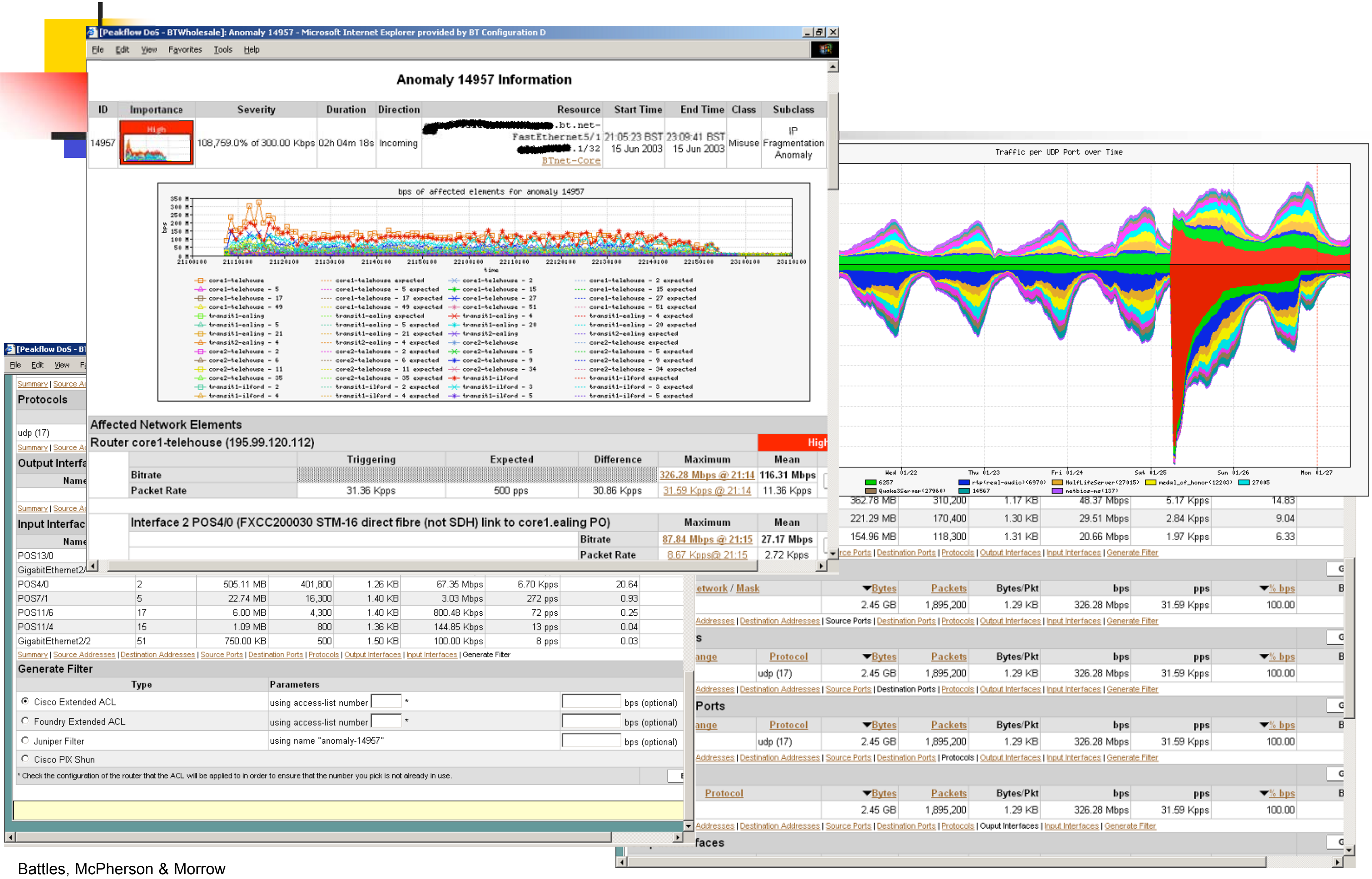
Tools Integration

- Could use to redirect to sinkhole analysis network:
  - Watch for consistent SYN-ACK storms
  - Worm detector (watch for scans, collect intel based on ports and signatures)
  - Background noise classification
  - Dark address monitoring & packet analysis
- Backscatter trigger
- No additional work after initial policy is implemented

Tools Integration (cont..)

- Recommend dedicated trigger device, via routers with AAA & OTP, etc.. or a commercial tool.
- Couple with NetFlow or SNMP Data collection tools to identify scope, scale, duration and other characteristics of an attack and provide post-mortem/forensics data analysis functions, clarify billing disputes, etc..

Attack Detection Tools..



Anomaly 14957 Information

ID	Importance	Severity	Duration	Direction	Resource	Start Time	End Time	Class	Subclass
14957	High	108,759.0% of 300.00 Kbps	02h 04m 18s	Incoming	[redacted].bt.net- FastEthernet5/1 [redacted].1/32 BTnet-Core	21:05:23 BST 15 Jun 2003	23:08:41 BST 15 Jun 2003	Misuse	IP Fragmentation Anomaly

Affected Network Elements

Router core1-telehouse (195.99.120.112) High

	Triggering	Expected	Difference	Maximum	Mean
Bitrate				326.28 Mbps @ 21:14	116.31 Mbps
Packet Rate	31.36 Kpps	500 pps	30.86 Kpps	31.59 Kpps @ 21:14	11.36 Kpps

Interface 2 POS4/0 (FXCC200030 STM-16 direct fibre (not SDH) link to core1.ealing PO)

	Maximum	Mean
Bitrate	87.84 Mbps @ 21:15	27.17 Mbps
Packet Rate	8.67 Kpps@ 21:15	2.72 Kpps

Summary | Source A

Protocols

udp (17)

Summary | Source A

Output Interfa

Name

Summary | Source A

Input Interfac

Name							
POS13/0							
GigabitEthernet2/							
POS4/0	2	505.11 MB	401,800	1.26 KB	67.35 Mbps	6.70 Kpps	20.64
POS7/1	5	22.74 MB	16,300	1.40 KB	3.03 Mbps	272 pps	0.93
POS11/6	17	6.00 MB	4,300	1.40 KB	800.48 Kbps	72 pps	0.25
POS11/4	15	1.09 MB	800	1.36 KB	144.85 Kbps	13 pps	0.04
GigabitEthernet2/2	51	750.00 KB	500	1.50 KB	100.00 Kbps	8 pps	0.03

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Generate Filter

Type	Parameters	
● Cisco Extended ACL	using access-list number ☐ *	☐ bps (optional)
○ Foundry Extended ACL	using access-list number ☐ *	☐ bps (optional)
○ Juniper Filter	using name "anomaly-14957"	☐ bps (optional)
○ Cisco PIX Shun		

* Check the configuration of the router that the ACL will be applied to in order to ensure that the number you pick is not already in use.

362.78 MB	310,200	1.17 KB	48.37 Mbps	5.17 Kpps	14.83
221.29 MB	170,400	1.30 KB	29.51 Mbps	2.84 Kpps	9.04
154.96 MB	118,300	1.31 KB	20.66 Mbps	1.97 Kpps	6.33

rce Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

etwork / Mask	▼Bytes	Packets	Bytes/Pkt	bps	pps	▼% bps	B
	2.45 GB	1,895,200	1.29 KB	326.28 Mbps	31.59 Kpps	100.00	

Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

s

ange	Protocol	▼Bytes	Packets	Bytes/Pkt	bps	pps	▼% bps	B
	udp (17)	2.45 GB	1,895,200	1.29 KB	326.28 Mbps	31.59 Kpps	100.00	

Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Ports

ange	Protocol	▼Bytes	Packets	Bytes/Pkt	bps	pps	▼% bps	B
	udp (17)	2.45 GB	1,895,200	1.29 KB	326.28 Mbps	31.59 Kpps	100.00	

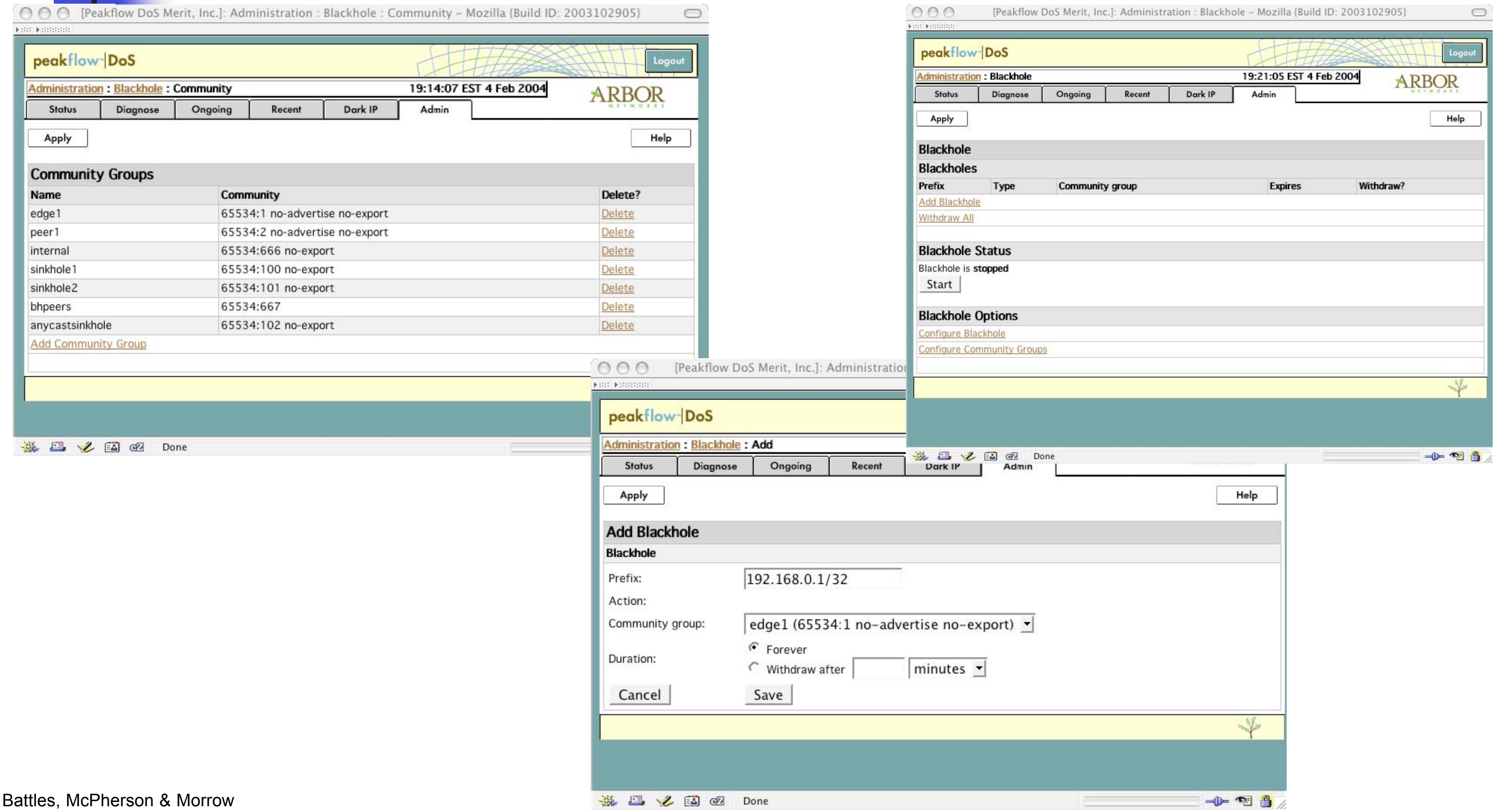
Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Protocol	▼Bytes	Packets	Bytes/Pkt	bps	pps	▼% bps	B
	2.45 GB	1,895,200	1.29 KB	326.28 Mbps	31.59 Kpps	100.00	

Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Ouput Interfaces | Input Interfaces | Generate Filter

faces

Commercial Tools…



[Peakflow DoS Merit, Inc.]: Administration : Blackhole : Community - Mozilla {Build ID: 2003102905}

Administration : Blackhole : Community 19:14:07 EST 4 Feb 2004

Community Groups

Name	Community	Delete?
edge1	65534:1 no-advertise no-export	Delete
peer1	65534:2 no-advertise no-export	Delete
internal	65534:666 no-export	Delete
sinkhole1	65534:100 no-export	Delete
sinkhole2	65534:101 no-export	Delete
bhpeers	65534:667	Delete
anycastsinkhole	65534:102 no-export	Delete

Add Community Group

[Peakflow DoS Merit, Inc.]: Administration : Blackhole - Mozilla {Build ID: 2003102905}

Administration : Blackhole 19:21:05 EST 4 Feb 2004

Blackhole

Blackholes

Prefix	Type	Community group	Expires	Withdraw?

Add Blackhole

Withdraw All

Blackhole Status

Blackhole is **stopped**

Start

Blackhole Options

Configure Blackhole

Configure Community Groups

[Peakflow DoS Merit, Inc.]: Administration

Administration : Blackhole : Add

Add Blackhole

Blackhole

Prefix: 192.168.0.1/32

Action:

Community group: edge1 (65534:1 no-advertise no-export)

Duration: ● Forever ○ Withdraw after ____ minutes

Cancel Save

Trigger Router’s Configuration

```
router bgp 65501
.
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
```

Redistribute Static with a route-map

Match Route Tag

Set BGP NEXT_HOP to the Trigger

Set LOCAL_PREF

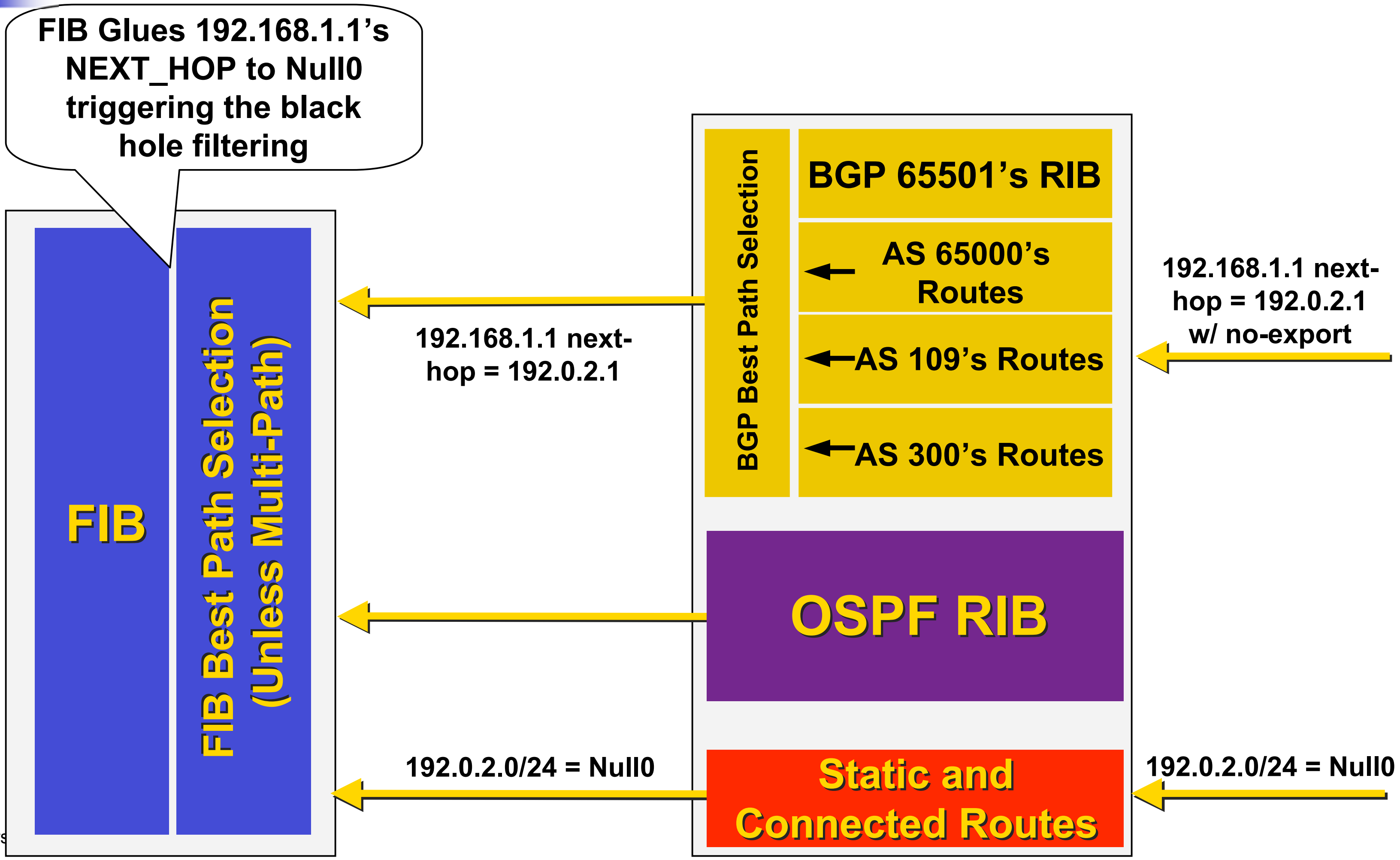
Step 3: Activate the Blackhole

- ISP adds a static route to the advertising router for the destination address they wish to blackhole. The route is added with *tag 66* to keep it separate from other static routes on the router.

```
ip route 192.168.1.1 255.255.255.255 Null0 Tag 66
```

- BGP Advertisement goes out to all BGP speaking routers
- Routers hear the announcement, glues it to the existing static route on the route, changes the BGP NEXT_HOP for the advertised route to Null 0
- Packets bound for destination are forwarded to Null 0/discarded

Step 3 – Activate the Black Hole



FIB Glues 192.168.1.1's NEXT_HOP to Null0 triggering the black hole filtering

FIB

FIB Best Path Selection (Unless Multi-Path)

192.168.1.1 next-hop = 192.0.2.1

192.0.2.0/24 = Null0

BGP Best Path Selection

BGP 65501's RIB

AS 65000's Routes

AS 109's Routes

AS 300's Routes

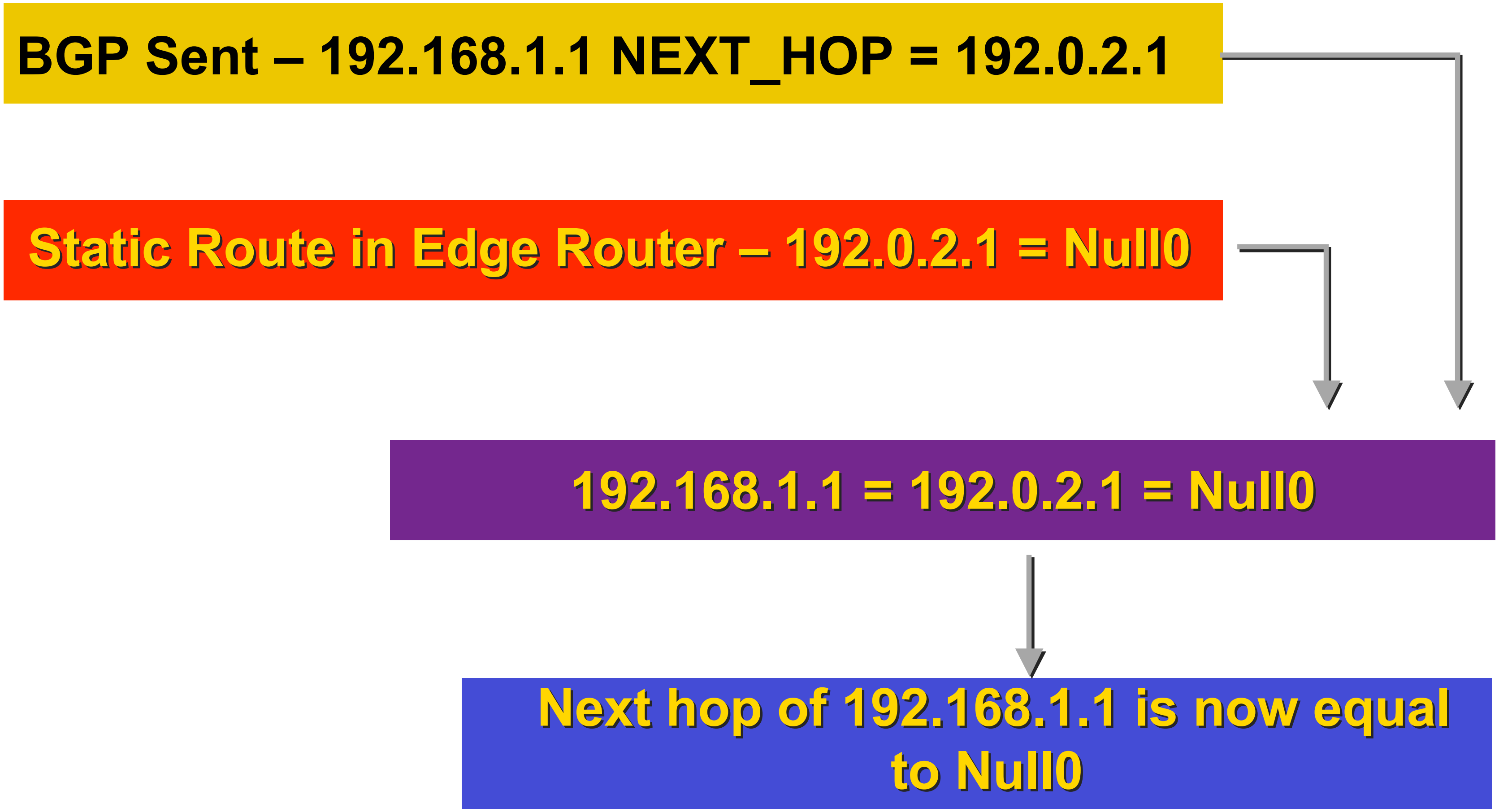
OSPF RIB

Static and Connected Routes

192.168.1.1 next-hop = 192.0.2.1 w/ no-export

192.0.2.0/24 = Null0

Step 3 – Activate the Black Hole



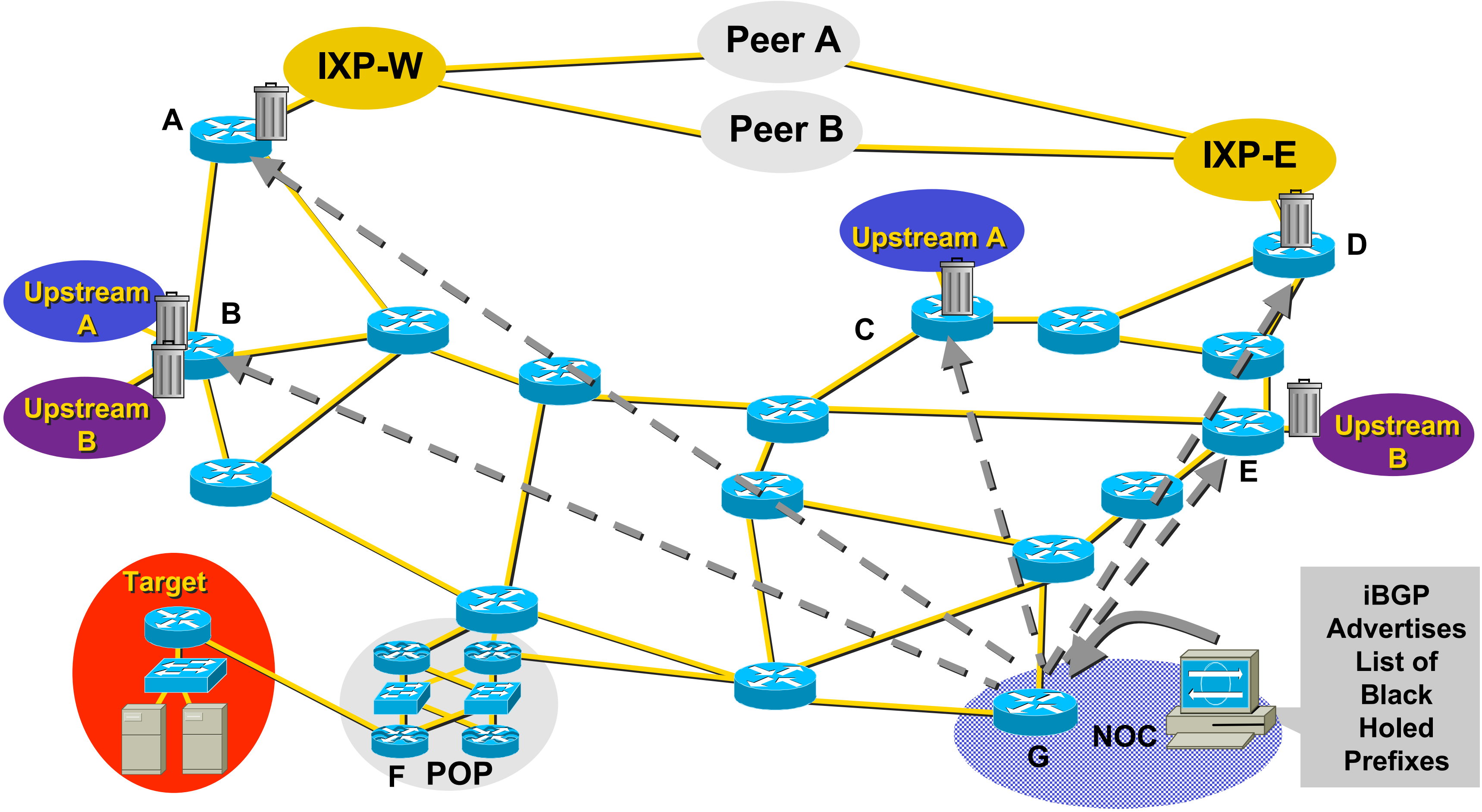
BGP Sent – 192.168.1.1 NEXT_HOP = 192.0.2.1

Static Route in Edge Router – 192.0.2.1 = Null0

192.168.1.1 = 192.0.2.1 = Null0

Next hop of 192.168.1.1 is now equal to Null0

Step 3 – Activate the Black Hole



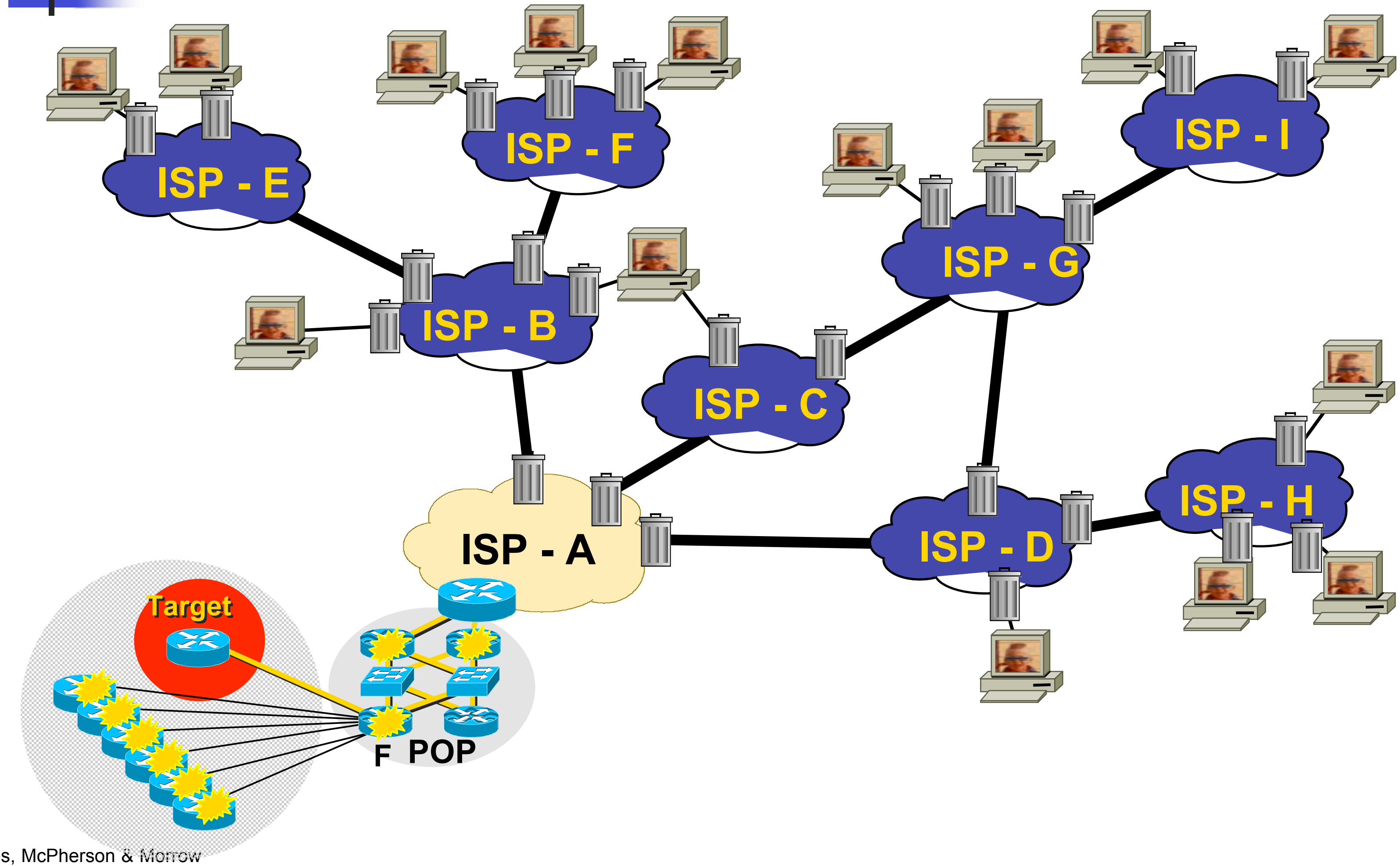
Community Based Trigger

- BGP Community-based triggering allows for more granular control over where you drop the packets.
- Three parts to the trigger:
  - Static routes to Null 0 on all the routers.
  - Trigger router sets the community and advertises the BGP update.
  - Reaction Routers (on the edge) matches community and sets the next-hop to the static route which maps to Null0.

Why Community Based Triggering?

- Flexibility, allows for more control on the DOS/DDOS reaction:
  - Community #1 can be for all routers in the network.
  - Community #2 can be for all peering routers. No customer routers – Preserves customer-customer connectivity if the victim is within your AS.
  - Community #3 can be for all customers (e.g., to push a inter-AS traceback to the edge of your network).
  - Trigger Communities per ISP Peer can be used to only black hole on one ISP Peer’s connection. Allows for the DOSed customer to have partial service.

Inter-Provider Mitigation



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, especially architectures that require exception path punts for dropped packets.
- BGP RIB and subsequent FIB entries utilize CPU and memory resources and should be tracked.
- 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 where they could not drop at line rate anymore.
- Bottom-line – Software based forwarding routers (any vendor) can forward faster then they can drop.

uRPF & Source-based Blackholes

- Source-based blackholes are achievable as well, though likely don’t make sense on the customer-facing front.

Customer-Triggered Blackholes

Deploy BGP Policy Set

- Accept more-specifics of customer routes with destination-based BGP blackholing community attached.
- No source-based blackholing
- Only accept more-specifics of customer prefixes

Accepting Longer Prefixes

- Only accept more-specifics of customer-allocated/advertised space.
- Policy depends on ingress prefix filtering policies
  - Explicit filters and any mask-length filters require preceding more-specific & community colored route-acceptance
  - Looser policies are perhaps less work but leave more room for errors
  - Define prefix-length acceptance criteria

More on customer-triggered..

- MTTR decrease
- Customer driven, removes some liability
- Customer:
  - When you want
  - Where you want it
  - Your timeline, not the ISPs!
- Tag received routes with NO_EXPORT community (and likely, NO_ADVERTISE, though a direct BGP session with the peer is then required)
- Policies and announcement authority should be verified regularly, exception reporting should be automated

Enhanced Policy Language

- Specifies explicit prefix filters with exception policy that matching defined communities for blackhole or other.
- Complements explicit filtering without adding twice the configuration overhead to introduce acceptance of more-specifics for blackholing.

BGP Flow Specification

Draft Information

- Available at:
  - http://www.tcb.net/draft-marques-idr-flow-spec-00.txt
  - Currently expired from IETF Internet-Drafts directory, hope to post new version soon.
- Authors:
  - Jared Mauch
  - Danny McPherson
  - Robert Raszuk
  - Pedro Marques
  - Nischal Sheth

Draft Overview

- Specifies procedures for the distribution of flow specification rules via BGP.
- Defines application for the purpose of packet filtering [other] in order to mitigate (distributed) denial of service attacks
- Defines procedure to encode flow specification rules as BGP NLRI which can be used in any why the implementer desires.

What’s A Flow Specification?

- A flow specification is an n-tuple consisting of several matching criteria that can be applied to IP packet data.
- May or May not include reachability information (e.g., NEXT_HOP).
- Well-known or AS-specific COMMUNITIES can be used to encode/trigger a pre-defined set of actions (e.g., blackhole, PBR, rate-limit, divert, etc..)
- Application is identified by a specific (AFI, SAFI) pair and corresponds to a distinct set of RIBs.
- BGP itself treats the NLRI as an opaque key to an entry in its database.

What’s it for?

- Primarily: DDOS Mitigation
- Continue evolution from:
  - Destination-based blackhole routing
  - uRPF/source-based BGP blackhole routing
- To:
  - Much more precise mechanism that contains all the benefits of it’s predecessors

We Need Operator Feedback

- Is this useful?
- What’s missing (e.g., more flexible specification language)
- Does this belong in BGP?
- What are our alternatives?
- Comments to authors are welcome!
  - flow-spec@tcb.net

References

- [backscatter]
- [RFC 3330]
- ftp://ftpeng.cisco.com/cons/isp/security
- Other?

Acknowledgements

- Barry Greene
- Brian Gemberling

Comments/Questions/Other?