BGP Security Techniques

Danny McPherson
danny@arbor.net

Agenda

- Overview & Discussion Context
- BGP Blackhole Routing
- BGP Diversion
- BGP Route Tagging
- BGP Flow Specification
- Analyzing “Dark IP” Data

Overview

- The purpose of this discussion is to both discuss BGP security techniques employed by network operators today, as well as to introduce some new mechanisms and techniques currently under development and request feedback from the community

About this talk….

- What this talk is about:
  - Using BGP as a security response tool
  - Benefits of employing unutilized/unallocated address space
- What this talk is NOT about:
  - Securing the BGP protocol (e.g., MD5 or IPSEC for Transport connection)
  - Securing information carried by BGP (e.g., prefix filters, soBGP & SBGP, RIRs & IRRs, etc..)
  - Configuration syntax - however, appropriate references provided

Interesting Notes…

- Have seen DoS attacks greater than 10Gbps aggregate capacity!
- Of 1127 DoS attacks seen on a very large network since JAN 03, only 4 employed address spoofing - "spoofing is out of vogue”?
- 140415 node botnet largest "seen" in the wild - larger botnets probable.
- Miscreants are avoiding RFC1918 and other bogon address space and explicitly targeting "easy pickens” prefixes such as 24/8.
- Miscreants often patch exploitable code once they compromise a system in order to "keep it” -- they probably install more patches than users!
- DOS attack vectors are changing (e.g., UDP brute force as opposed to TCP-based, arbitrary DDOS toolkit)

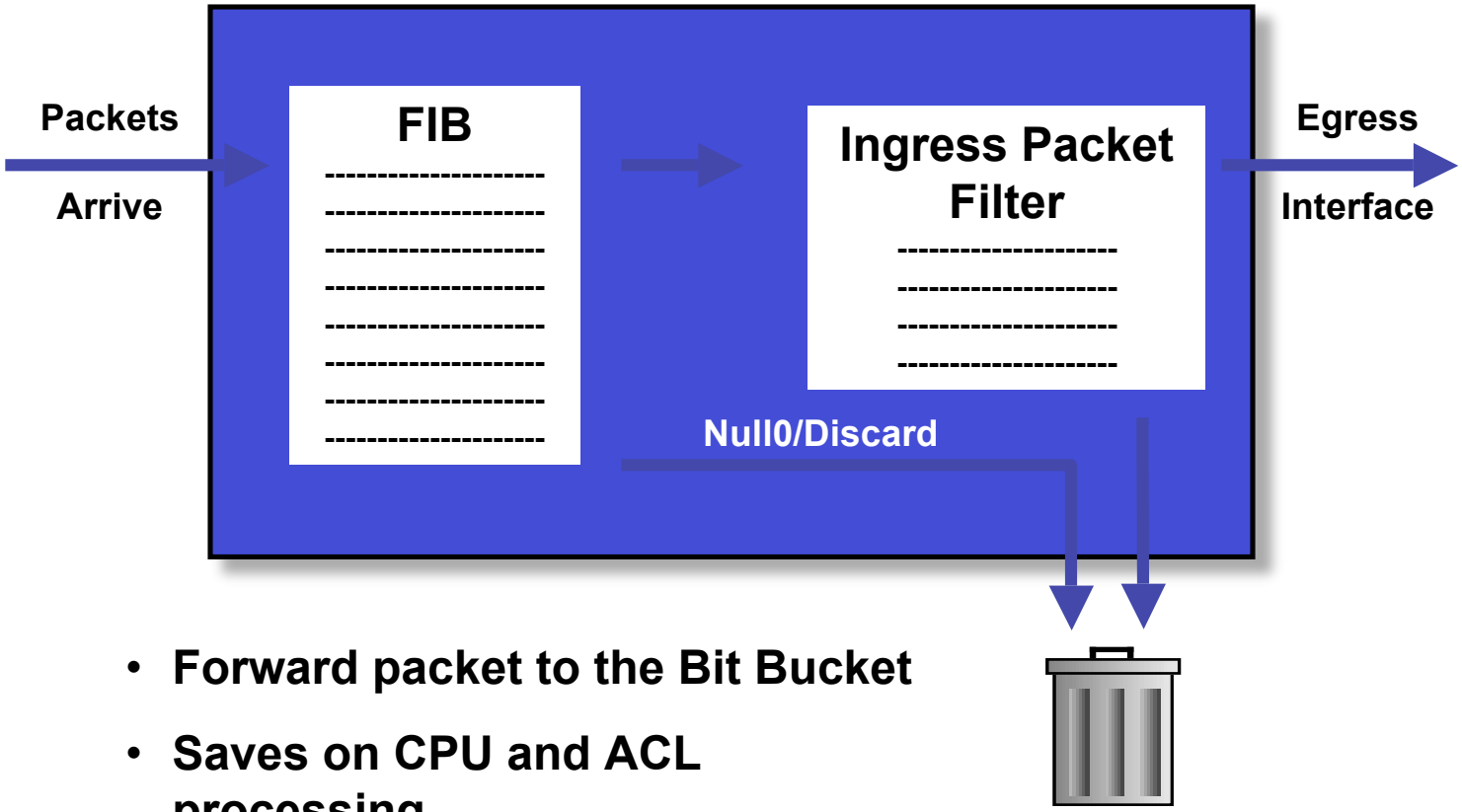
The Problem…

- The magnitude of DDOS attacks result in network instability and often times collateral damage to the network infrastructure
- Mitigation policies need to be deployed at the network ingress and propagated to upstream networks in near real-time
- ACL management, deployment and implementation/ performance implications inhibit their use considerably - consider deployment of attack mitigation policies to 2000 interfaces on 400 routers, augmenting existing policies and removing said policies once attack has ceased

BGP Blackhole Routing

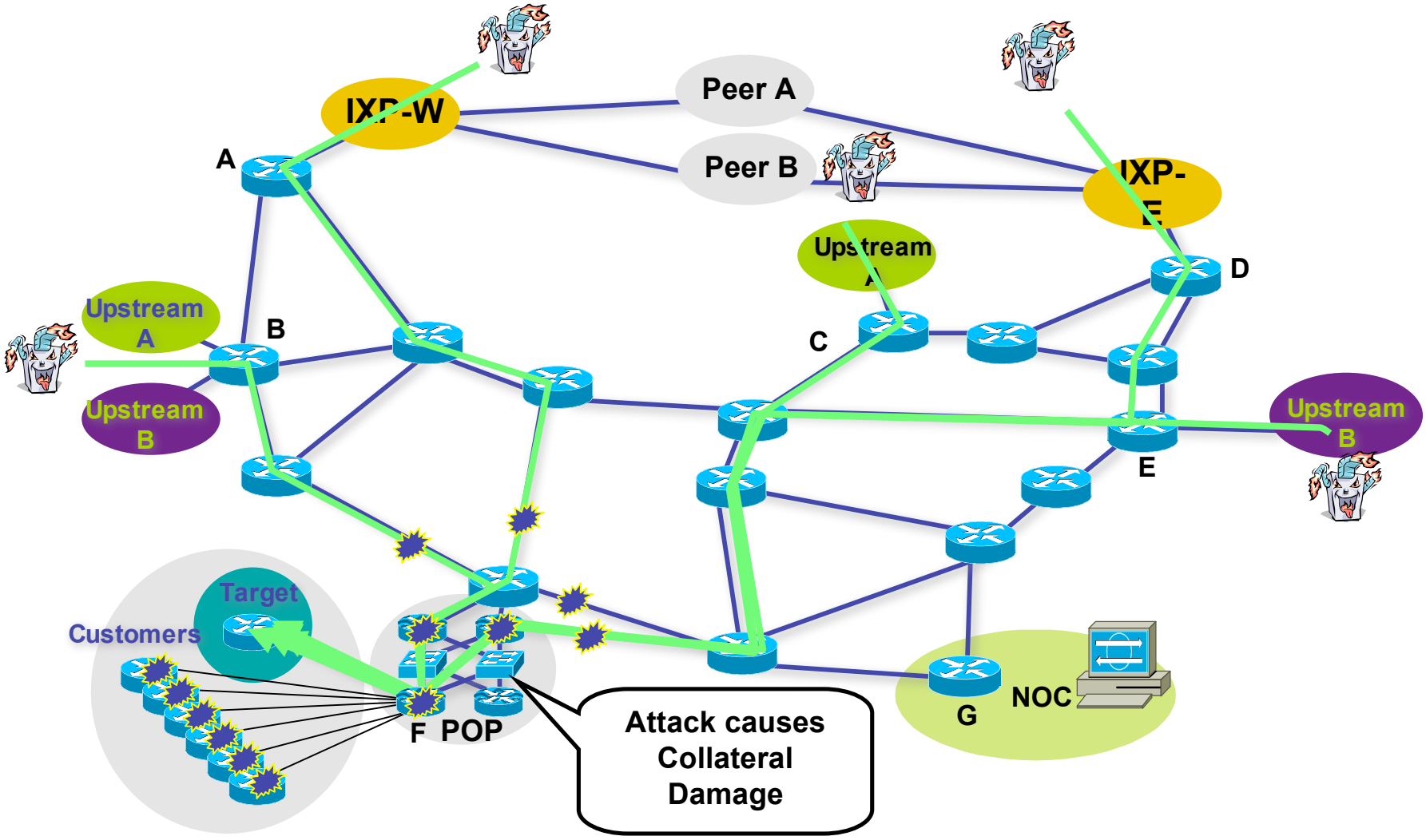
- Commonly referred to as *BGP Real-Time Blackhole Routing (RTBH),* or *Blackhole Filtering*; results in packets being forwarded to a routers bit bucket, also known as:
  - Null Interface
  - Discard Interface
- Several Techniques:
  - Destination-based BGP Blackhole Routing
  - Source-based BGP Blackhole Routing (coupling uRPF)
  - Customer-triggered
- Exploits router's forwarding logic - typically results in desired packets being dropped with minimal or no performance impact
- Enables BGP Backscatter Traceback Technique

Exploits Forwarding Logic

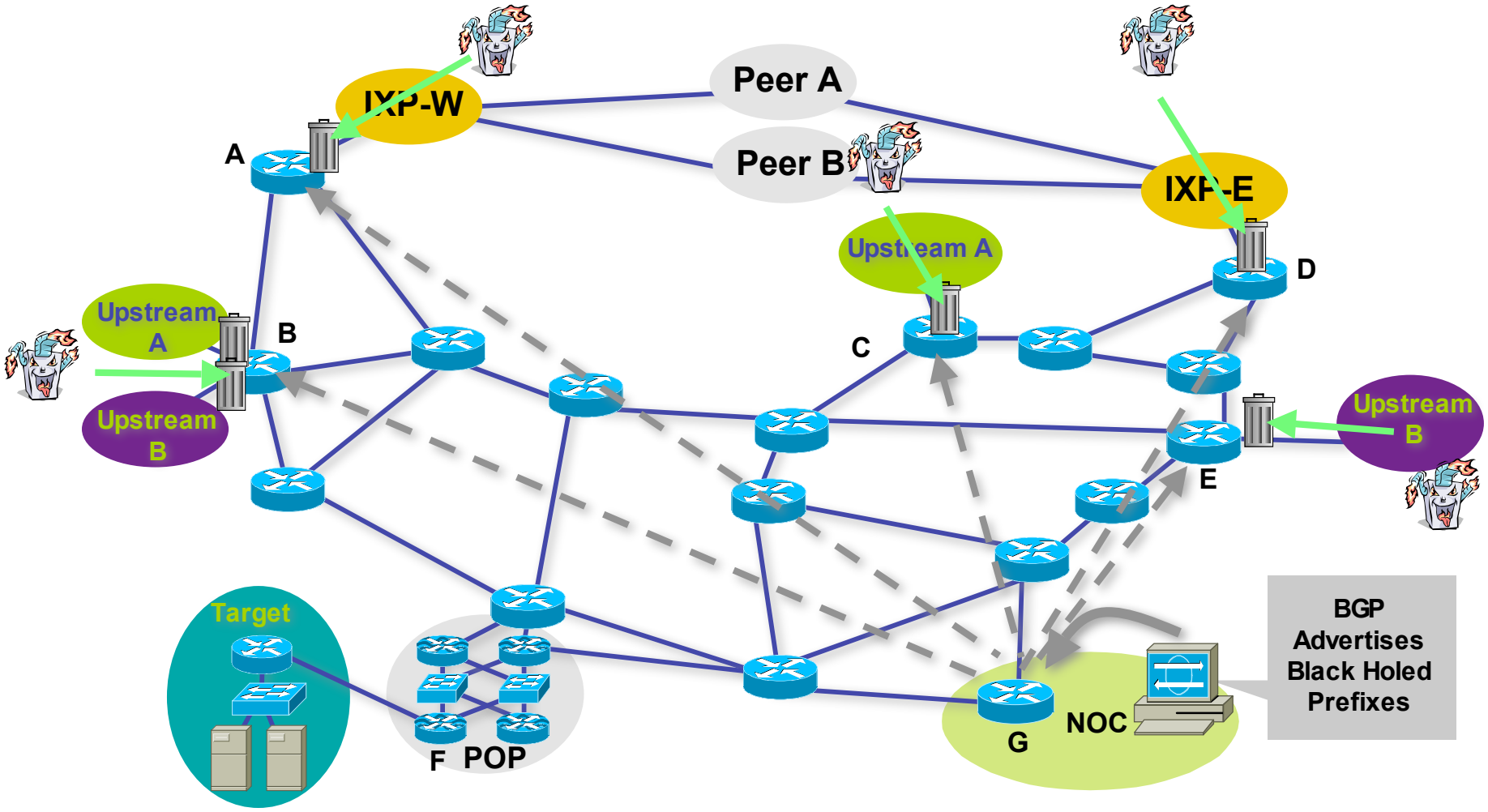


- **Forward packet to the Bit Bucket**
- **Saves on CPU and ACL processing**

Customer is DOSed – Before – Collateral Damage

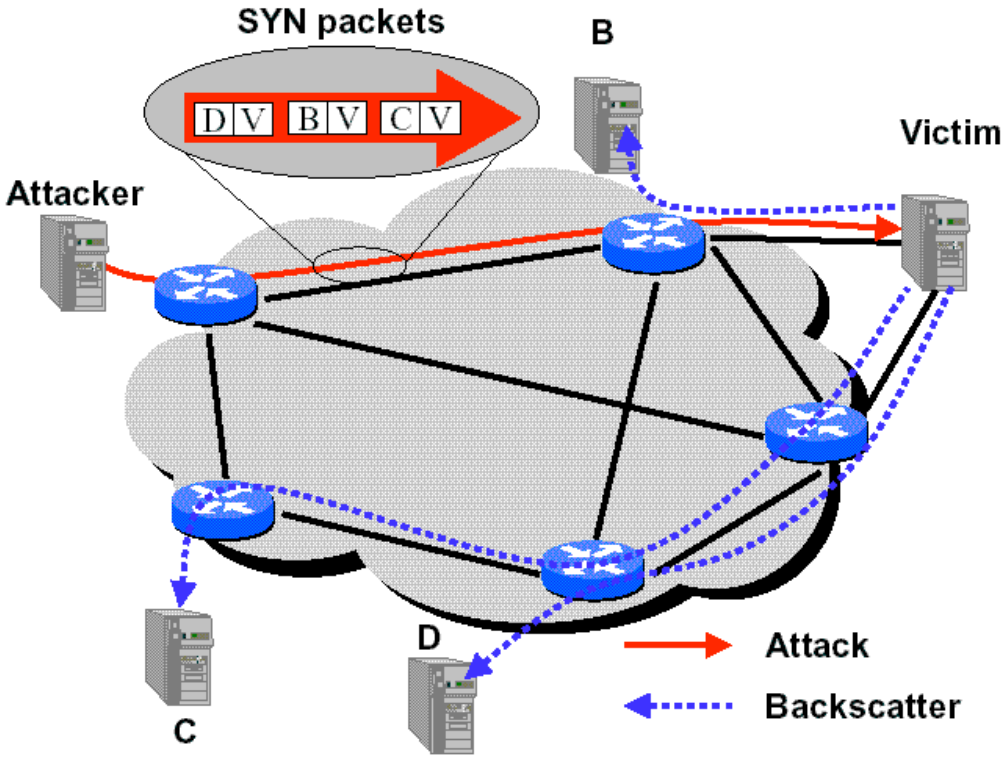


Customer is DOSed – After – Packet Drops Pushed to Network Ingress



Monitoring Backscatter

- Inferring Internet Denial-of-Service Activity
  - http://www.caida.org/outreach/papers/2001/BackScatter/
- Backscatter Traceback (NANOG 23)



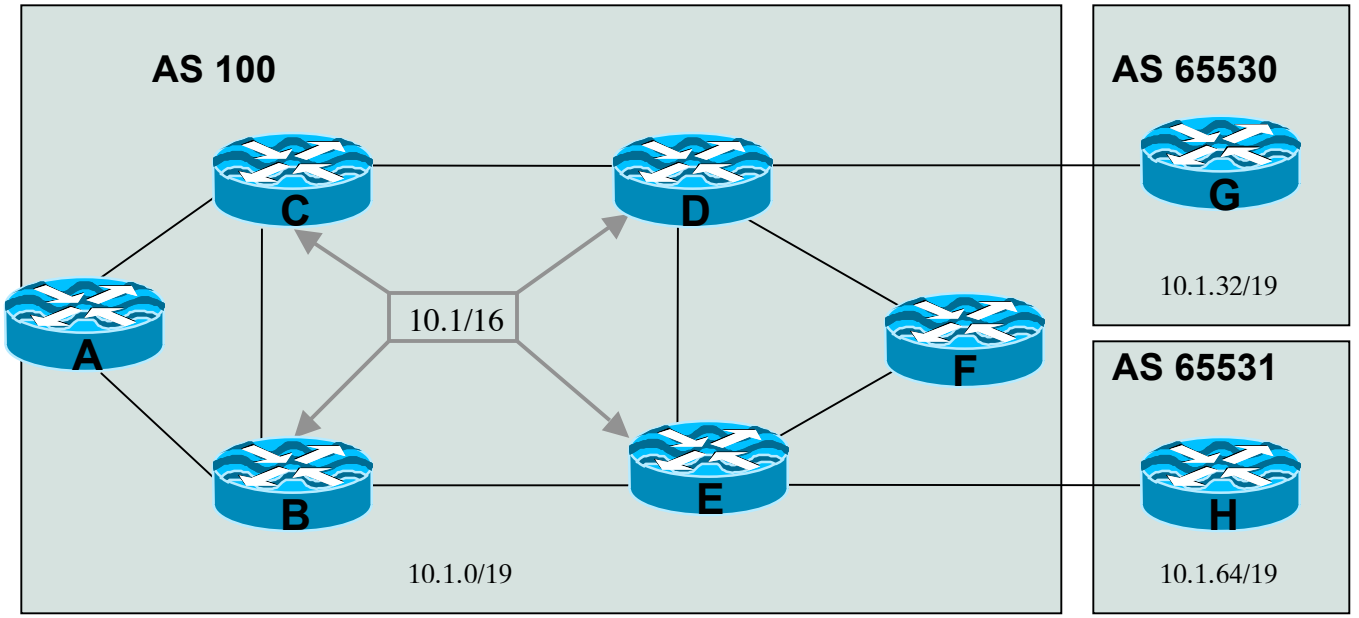
Beyond Destination-based RTBH

- Employing uRPF in conjunction with RTBH can provide source-based solution v. destination-based
- Why not allow customer triggered blackholing for more-specifics of their prefixes?

BGP Diversion Techniques

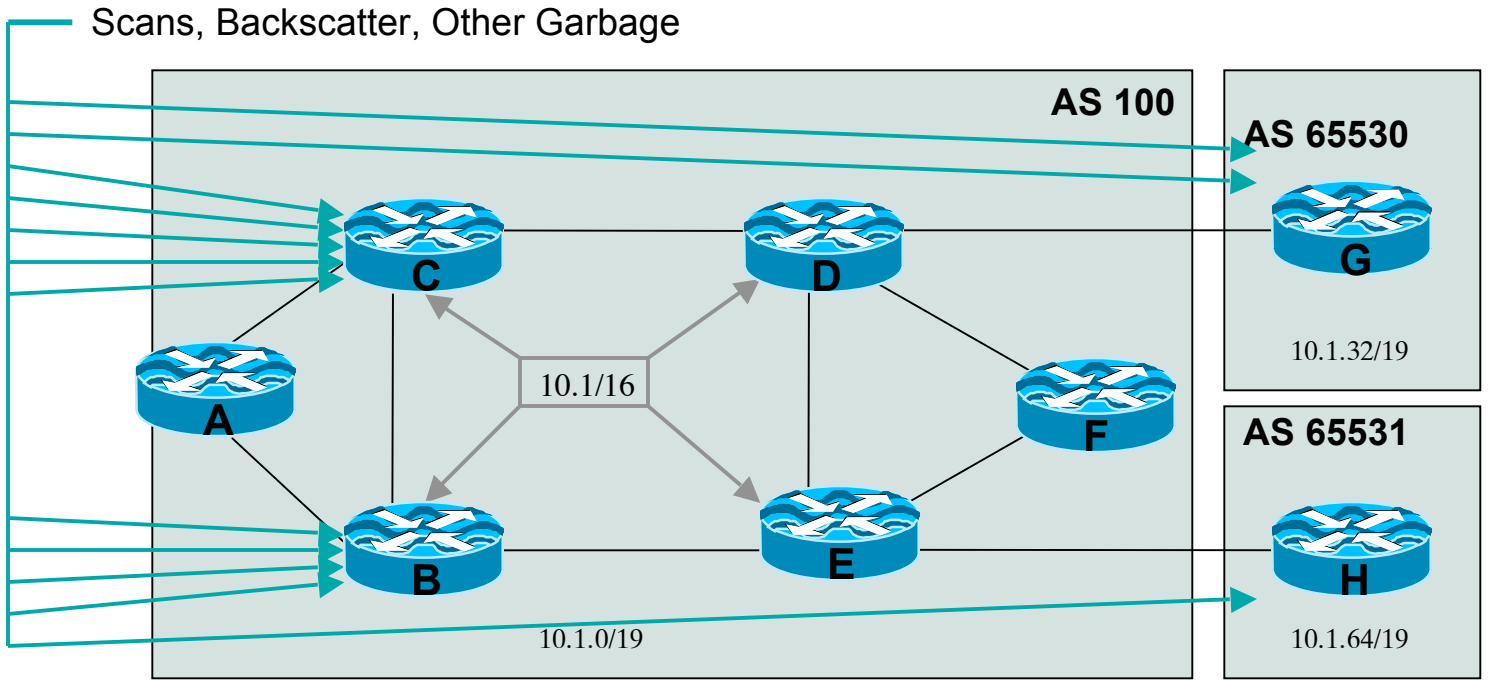
- Rather than employing BGP to simply discard traffic (and often effectively complete a Denial of Service attack), use BGP to divert traffic to data analysis or packet “scrubbing” centers, often referred to as *Sinkholes*
- Divert via resetting BGP next hop to IP address of analysis system(s) or matching community tags that result in different BGP next hops being assigned for a given prefix (or PBR, or static, or…)

Typical Aggregate Sources



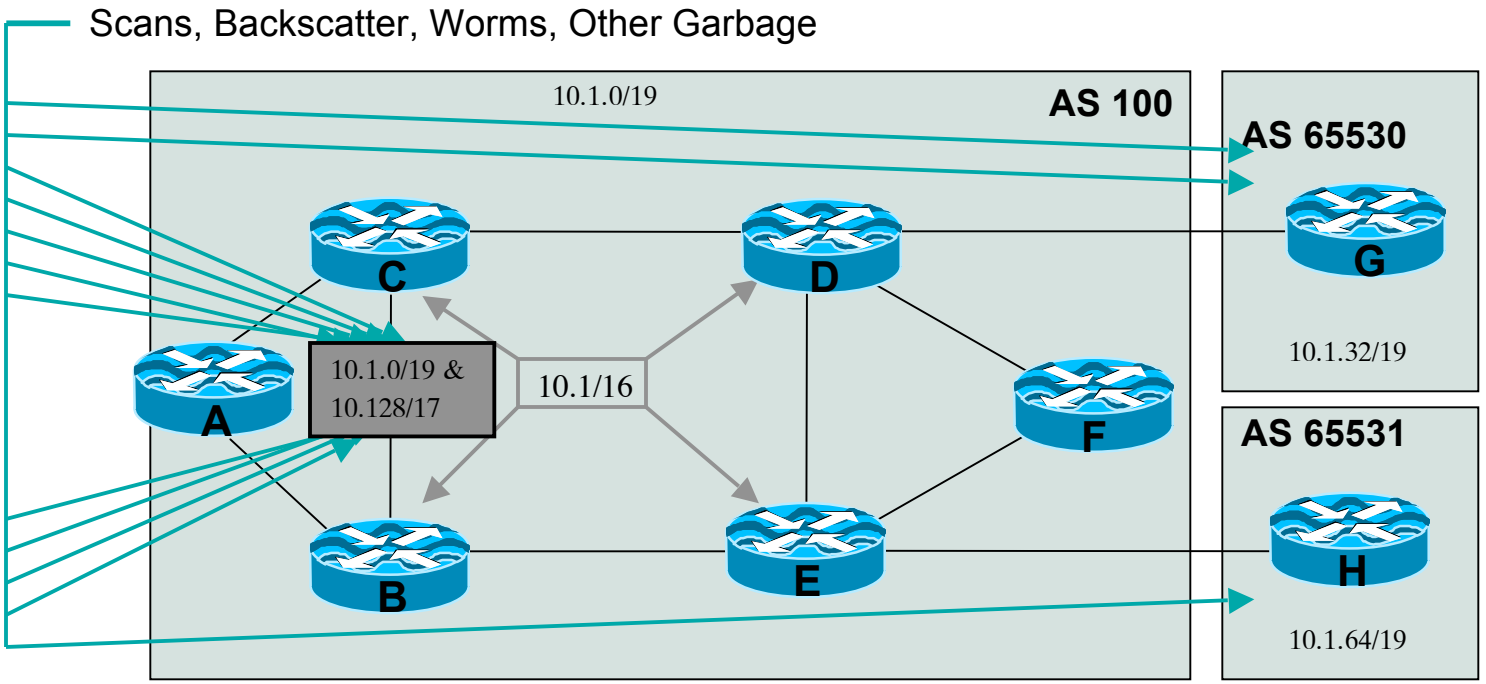
- 10.1/16 allocated to AS 100
- 10.1.0/19 used for infrastructure
- 10.1.32/19 AS 65530
- 10.1.64/19 AS 65531
- 10.1/16 (10.1.96-10.1.255.255) implicitly nailed to null interface on core routers (C,B,D&E)

Routers Collect Garbage Data



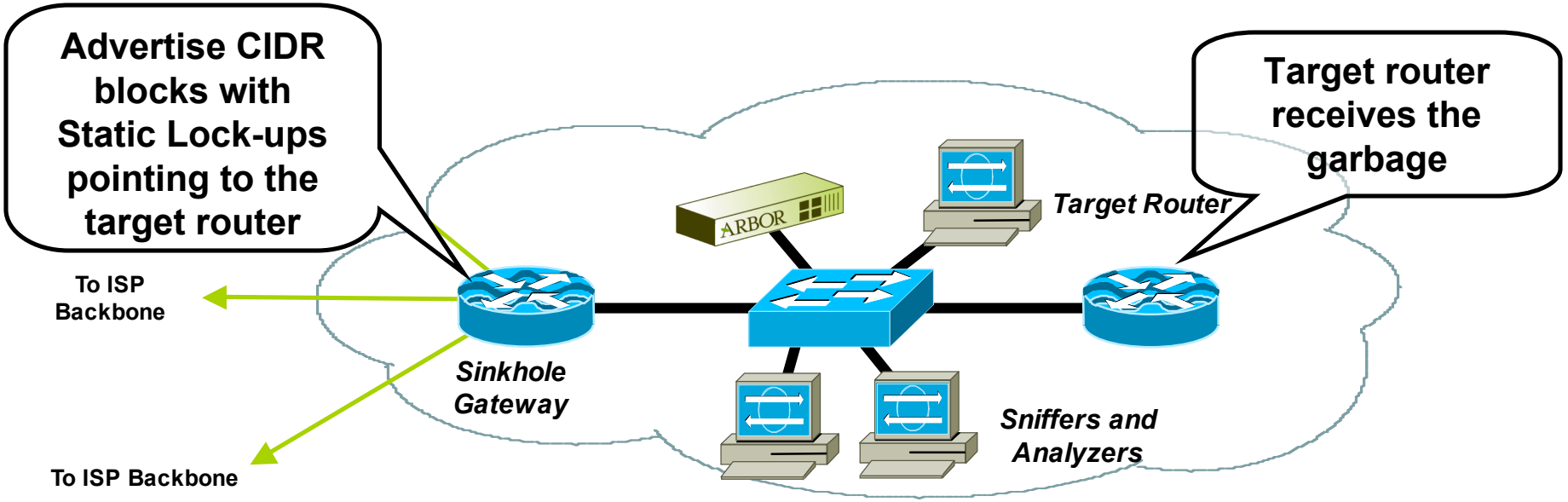
- Routers collect all the garbage (backscatter, scans, etc..) destined for 10.1/19, 10.1.96/19 & 10.1.128/17 addresses
- Routers are required to process data, send ICMP unreachables, etc..

Why not Divert to Sinkhole?



- Why not divert garbage to sinkhole, if not for further analysis, at least to off-load data processing from routers
- Traffic forwarded to sinkhole for analysis, removes processing overhead from routers
- Provide collection point for further analysis

Sinkholes – Advertising Dark IP



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

BGP Route Tagging

- Employ same technique as previously discussed mechanisms to tag routes (usually via BGP Communities) in order to apply some firewall, packet filter, rate limit, quality of service or similar policy to packets matching the prefix (or attributes identified by the policy)
- E.g., Cisco's BGP Policy Propagation (BPP)

BGP Flow Specification

- Defined in:
  - http://www.ietf.org/internet-drafts/draft-marques-idr-flow-spec-02.txt
- Specifies procedures for the distribution of flow specification rules via BGP
- Defines AN application for the purpose of packet filtering 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 way 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/Initially: DDOS/Worm Mitigation
- Continue evolution from:
  - Destination-based blackhole routing
  - uRPF/source-based BGP blackhole routing
- To:
  - Much more precise/granular mechanism that contains all the benefits of it's predecessors
- At least one implementation complete, another (more?) on the way

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

About Dark IP…

- Various IP address classifications
  - **RFC 1918** (e.g., 10/8, 172.16/12 & 192.168/16)
  - **Bogon** addresses are address blocks that have not yet been allocated by IANA or a RIR (e.g., APNIC or ARIN)
  - **Dark IP** addresses have been allocated to a network operator and are currently being advertised, but have not yet been allocated to end-users/customers; typically subsets of allocated blocks
  - **Active** address space has been allocated to end-users/customers and end systems

Packets to Dark IP Destinations

- Limited set of traffic destined for these IP addresses:
  - Broken/Misconfigured
  - Scanning/Malicious
  - Backscatter
  - No legitimate traffic to these IP addresses
- Monitor traffic to detect deviations, reconnaissance activities, etc..

Dark IP Monitor

- Can monitor via packet collection, flow analysis, etc..
- Can also monitor RFC1918 address space in this manner, assuming no use internally
- Can even use flow-based monitoring to monitor all traffic of this type *n* network-wide - even production traffic.

The Internet Motion Sensor Project

- University of Michigan led research project
- Distributed on many networks, monitoring 10s of millions of unique “Dark IP” address blocks
- Utilizes BGP diversion and Dark IP monitoring
  - W/Throttled active responders
  - Correlation and alerting agents, etc..
- For more information: http://ims.eecs.umich.edu

References

- Backscatter Traceback (NANOG 23)
- Security on the CPE Edge (NANOG 26)
- Sinkholes (NANOG 28)
- Customer-Triggered Real-time Blackholes (NANOG 30)
- APRICOT 2004 - “ISP Security: Deploying and Using Sinkholes”
- http://www.ietf.org/internet-drafts/draft-marques-idr-flow-spec-02.txt
- http://www.nanog.org (Index of Talks)
- The Internet Motion Sensor http://ims.eecs.umich.edu
- **The Internet Motion Sensor: A distributed blackhole monitoring system**. *NDSS ’05,* San Diego, CA, February 2005.
- **Tracking Global Threats with the Internet Motion Sensor**. *Presentation at NANOG 32*, October 2004.
- **Toward Understanding Distributed Blackhole Placement**. In WORM’04: *Proceedings of the 2004 ACM workshop on Rapid Malcode,* 2004.

Questions?

danny@arbor.net