

ISP Security – Real World Techniques II



The Threat from Violated CPE Routers

NANOG26, Eugene, OR

Version 1.1

Kevin Houle [kjh@cert.org]

Barry Raveendran Greene [bgreene@cisco.com]



Where to get Slides and Updates

- NANOG
 - <http://www.nanog.org/mtg-0210/ispsecure.html>
- ISP Essentials Archive
 - <http://www.ispbook.com/security/>



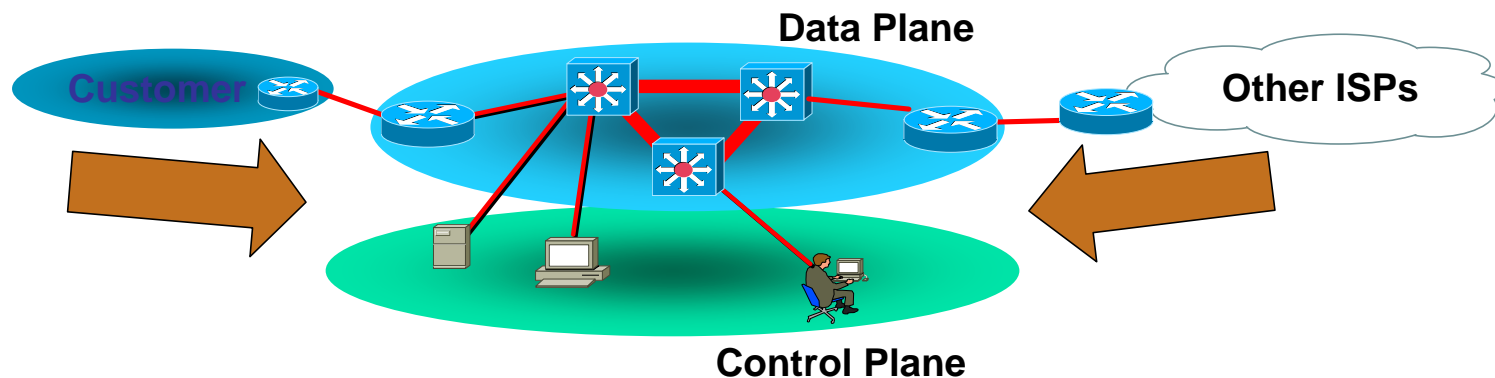
ISP Security Treats

“The wonderful thing about the Internet is that you’re connected to everyone else. The terrible thing about the Internet is that you’re connected to everyone else.”

Vint Cerf

Role of Service Providers

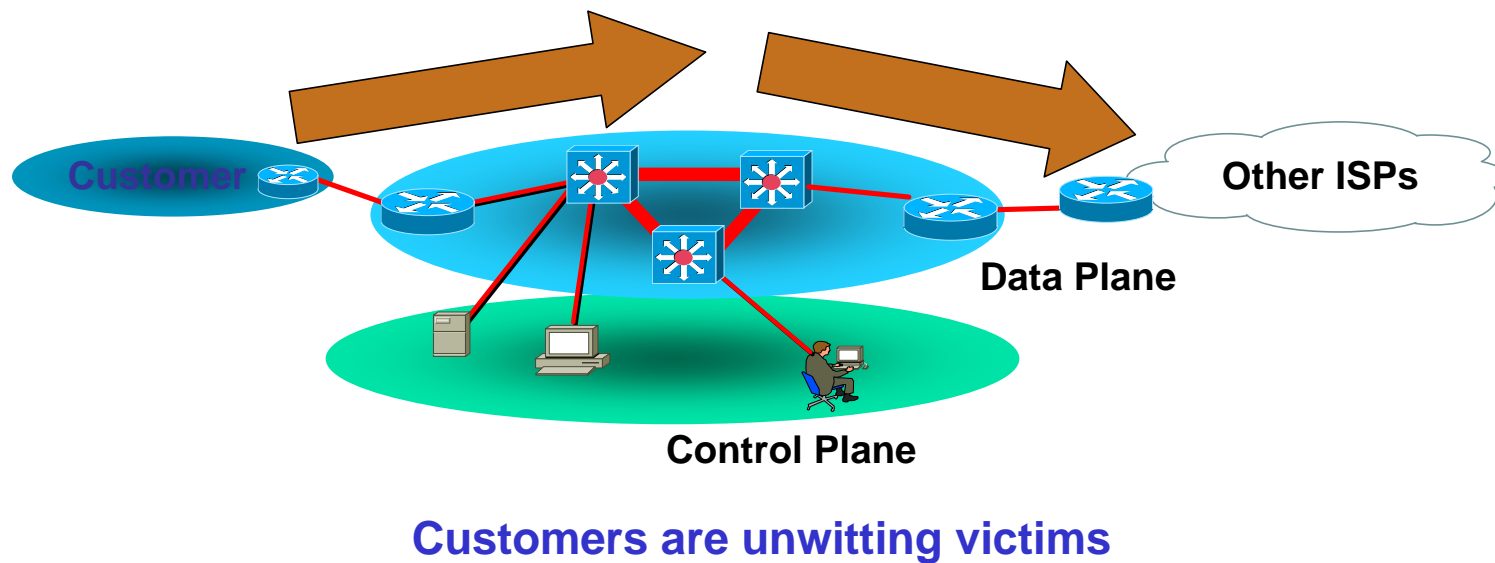
- **Deliver service in the face of mistakes, failures, and attacks**



**Protect ISP infrastructure from customers and the Internet.
Protect the data plane and control plan from each other.**

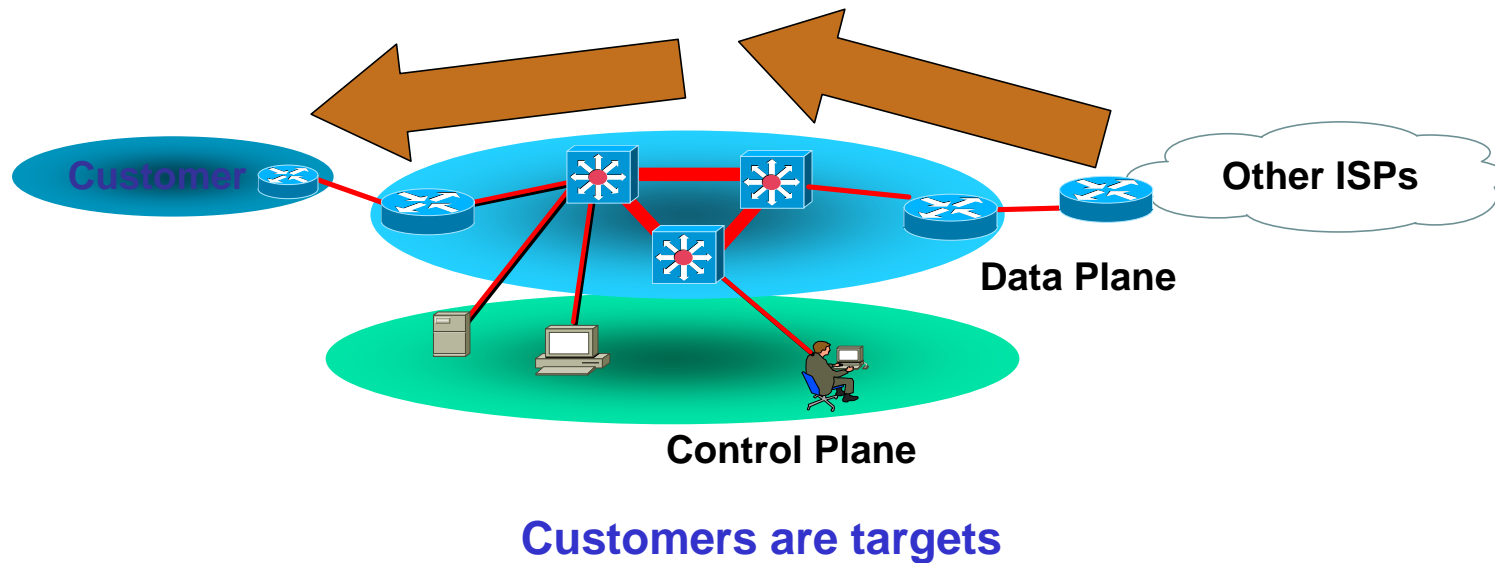
Role of Service Providers

- Help protect other peers



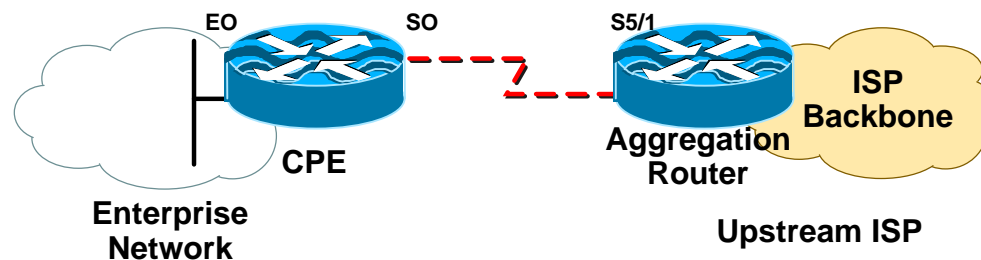
Role of Service Providers

- **Protect customers from attacks coming from the infrastructure or other customers**



Focus of the Tutorial

- Our focus is on the ISP – Customer Edge with specific focus on the Customer's CPE.
 - Why? Cause CPE configs are something that the ISP could feasible influence.



ISP Security – Real World Techniques II



- Intruders Compromising Customer CPEs
- Malicious Configuration Alteration
- Malicious Route Injection
- Alteration of Registry Information
- Denial-Of-Service Attacks Directed at CPEs



Intruders Compromising CPE

Intruders Compromising CPE

Perceived Threat & Reality

- **Perceived Threat:**

- Someone gaining control of a customer's CPE can do some nasty things.

- **Reality:**

- Intruders are actively scanning for and compromising CPE devices
 - Broadband devices
 - Customer premise routers
- Automated tools exist for scanning, compromise, and use of compromised devices

Intruders Compromising CPE



Reality

- Intruder-developed texts exist to teach others
- Lists of compromised CPE are traded in the underground
- CERT/CC aware of incidents involving thousands of impacted devices

Intruders Compromising CPE

Attack Methods

- Fingerprint scanning and traceroute to identify targets
- Targets compromised
 - Default passwords (most common)
 - Weak and well-known passwords
 - Stolen authentication credentials
 - Sniffing network traffic
 - Social engineering
 - Insider attack

Intruders Compromising CPE



Impact

- Sometimes no impact – just for fun.
- Intruder Proxy / Bounce Point / GRE Tunnel Point
- Denial-of-service for customer(s)
- Attacks against other sites
 - DDoS via automated tools
- Trust-based attacks

Intruders Compromising CPE

What can ISPs Do?

- Assume the Worse!
 - Always assume the customer's CPE is not secure. So take measures to protect your network.
 - BCP38 – Ingress Source filtering. Several techniques today (ACLs, uRPF Strict Mode, Radius Per-User ACLs, Cable source-verify).
 - BGP Ingress Route Filtering – if customer is a BGP speaking Router.

Intruders Compromising CPE

What can ISPs Do?

- Provide your customer the tools to take care of themselves.
 - #1 – Customer Service Web Page on Security. Links with procedures, vendor security pages, recommendations, and other BCPs.
 - Customer “security” alias – allow customers to sign on and get news and alerts.

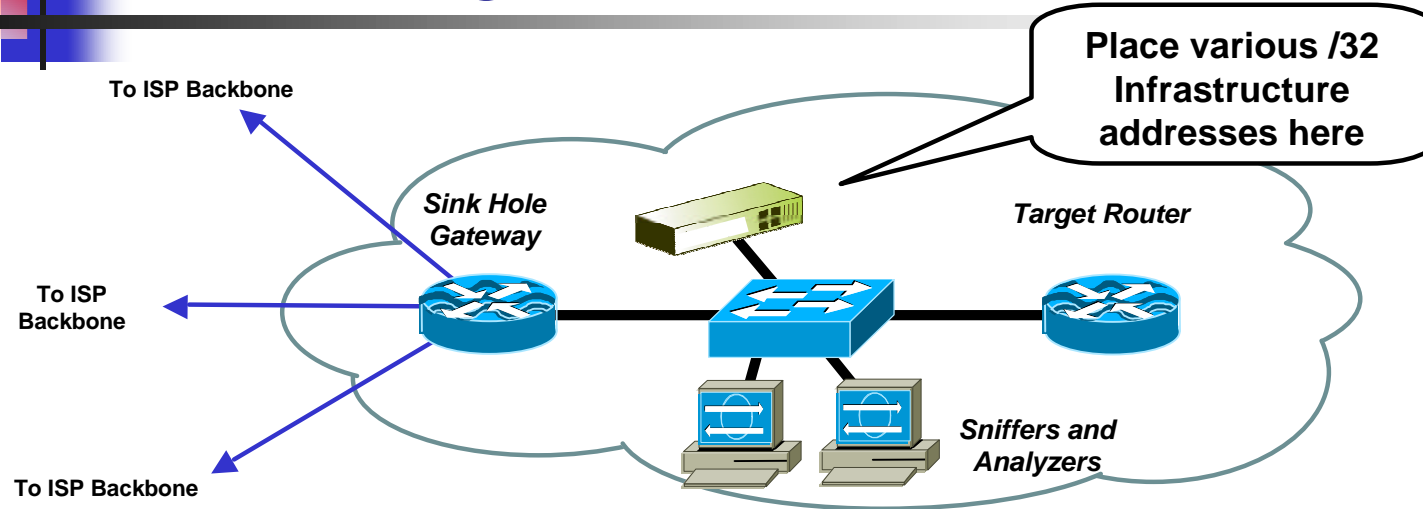
Intruders Compromising CPE

What can ISPs Do?

- Policies, Preparation, and Practice!
 - Create and Publish your security Policies.
 - Creating policies on the fly in the middle of a security incident is not advisable.
 - Prepare your Identification, Classification, Traceback, and Reaction Tools.
 - Classification ACLs
 - Sink Holes
 - Backscatter Traceback – works for customer aggregation routers as well as ISP – ISP peering points.

What can ISPs Do?

Monitoring Scan Rates & Worms



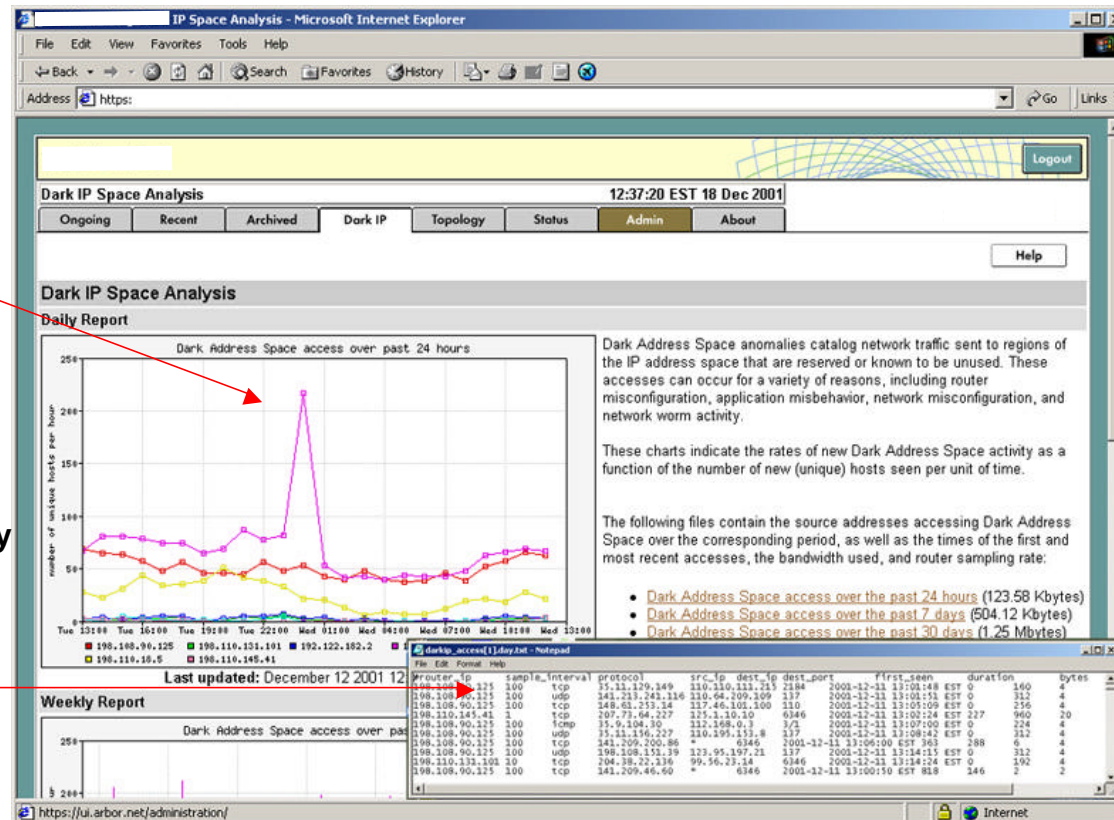
- Select /32 address from different block of your address space. Advertise them out the Sink Hole
- Assign them to a workstation built to monitor and log scans.
- Find or create a *Dark IP* Application that automatically monitor scan rates and worms ... Providing list of violated customers.

What can ISPs Do?

Monitoring Scan Rates & Worms

Operator instantly notified of Worm infection.

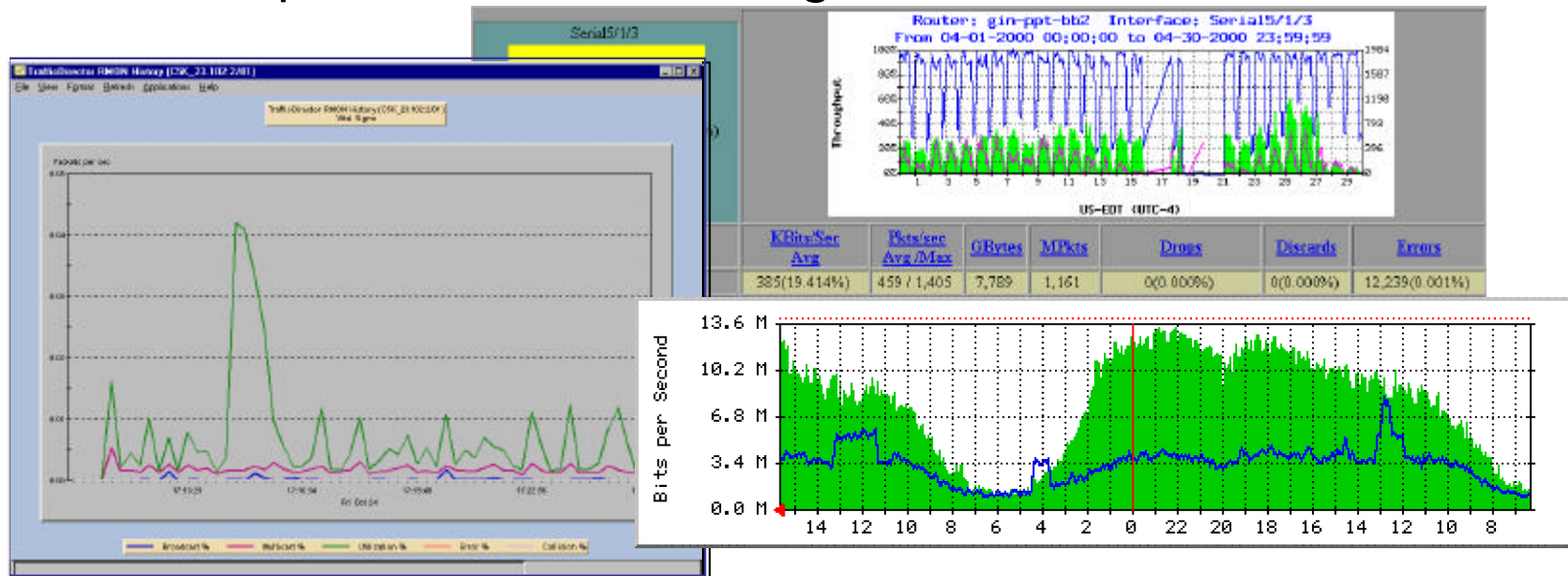
System automatically generates a list of infected hosts for quarantine and clean-up.



Intruders Compromising CPE

What can ISPs Do?

- Monitor Customer Bandwidth
 - Need to do it for traffic engineering.
 - Important for detecting attacks.



Intruders Compromising CPE

What can ISPs Do?

- Use Strong Authentication for CPE Management
 - Public key cryptography (e.g., ssh)
 - Good password policies (change defaults!)
 - Do not authenticate in the clear across untrusted networks.
 - Critical for managed CPE services. How many routers do you really have control?

Intruders Compromising CPE

What are ISPs Doing?

- **Not much!** Based on the observational evidence, ISPs are not doing much.
 - Example from Barry's home.
 - Two DSL links and one Cable link.
 - Barry has control over the CPEs for each of the three providers.
 - Two provided "security best practices web pages".
 - All three allow spoofed source addresses (I can create nice asymmetrical flows going out one and back in the other).
 - No messages from any of the three providers about software updates or security alerts (i.e. remember the SNMP fun).
 - One of the three types of CPEs provide an easy way to shutdown external access to service ports.



Malicious Configuration Alteration

Malicious Configuration Alteration

Perceive Threat & Reality

- What fun can you have once you have broken into a router?
 - Intruders continue to develop and share techniques for altering router configurations once compromised
 - HOWTO texts are publicly available for multiple platforms

Malicious Configuration Alteration

Attack Methods

- Direct privileged access into the ISP or customer's network via compromised router
- Unprotected remote management interfaces
 - HTTP
 - SNMP
 - Same community string used everywhere

Malicious Configuration Alteration



Impact

- Administrative lockout
 - Intruder changes access/privilege passwords
- Alteration of security policies
 - Removal/alteration of ACLs
 - Enabling/disabling services
 - Broadens exposure to further attacks
- The CPE turns into a *bridge* into the customer's internal trust domains (and possibly the ISP's)

Malicious Configuration Alteration



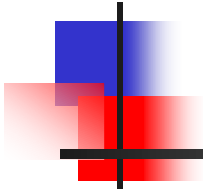
Impact

- Trash the CPE
 - “Write Erase” or delete the software image
- Alteration of layer 2 configuration
 - Interfaces may be disabled causing outages (shutdown).
- Alteration of layer 3 configuration
 - Routing protocols and policies
 - Denial-of-service
 - Traffic redirection / interception (*Cisco Sniffer*)
 - Prefix hijacking

Malicious Configuration Alteration

What can Customers and ISPs Do?

- Protect Routers from Compromise
 - Disable unneeded services
 - Restrict traffic to needed services
 - Monitor traffic with src/dst = routers
 - Use strong authentication for management
 - At least use non-default passwords!
 - Out-of-band management path
 - Authenticate and backup configurations



Malicious Route Injection

Malicious Route Injection

Perceive Threat

- Bad Routing Information does leak out. This has been from mistakes, failures, bugs, and intentional.
- Intruders are beginning to understand that privileged access to a router means route tables can be altered
- CERT/CC is aware of a small number of incidents involving malicious use of routing information
- Perceived Threat is that this will be a growth area for attackers.

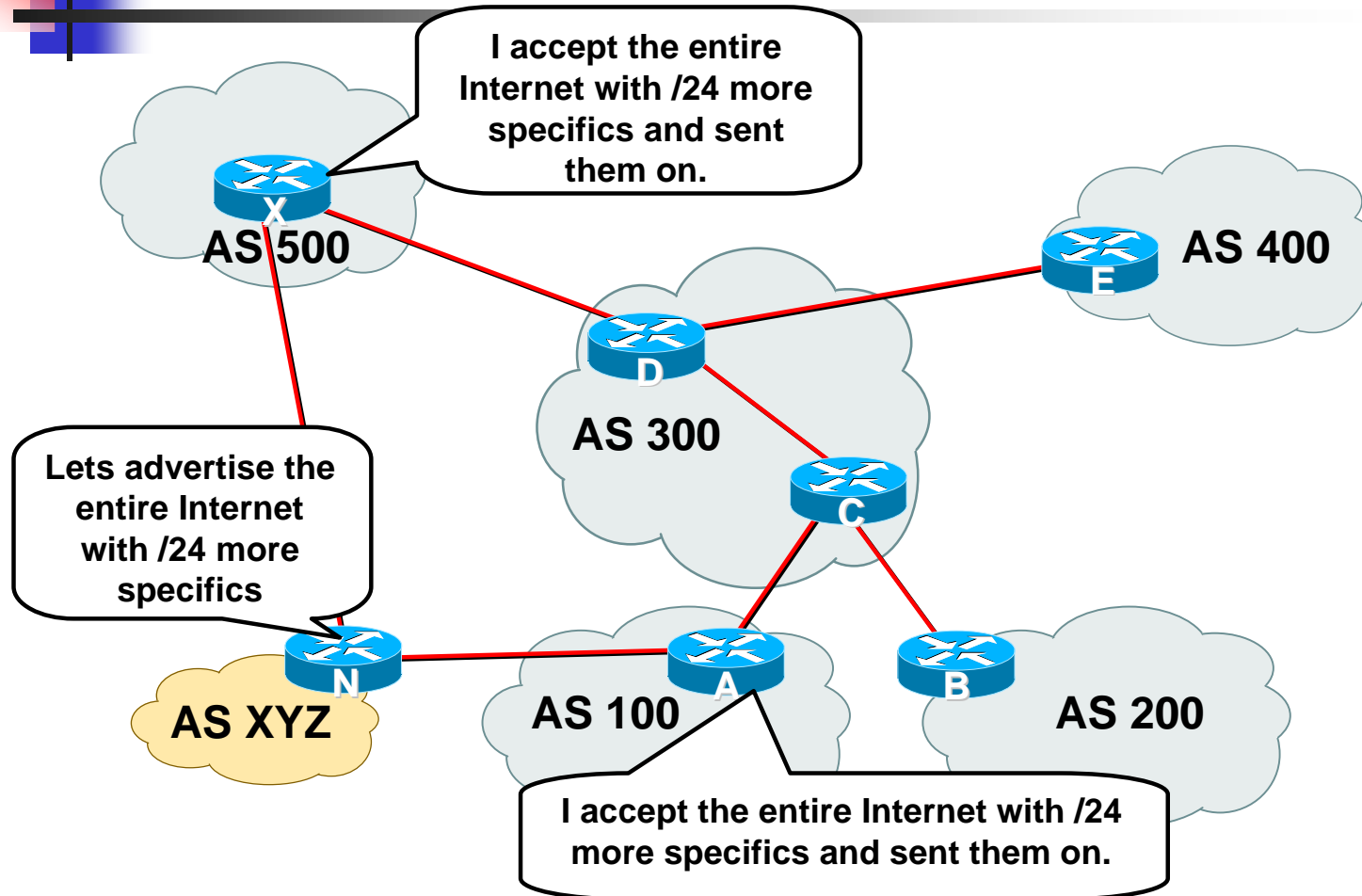
Malicious Route Injection

Reality – an Example

- AS 7007 incident used as an attack.
- Multihomed CPE router is violated and used to “de-aggregate” large blocks of the Internet.
- Evidence collected by several CERTs that hundreds of CPEs are violated.

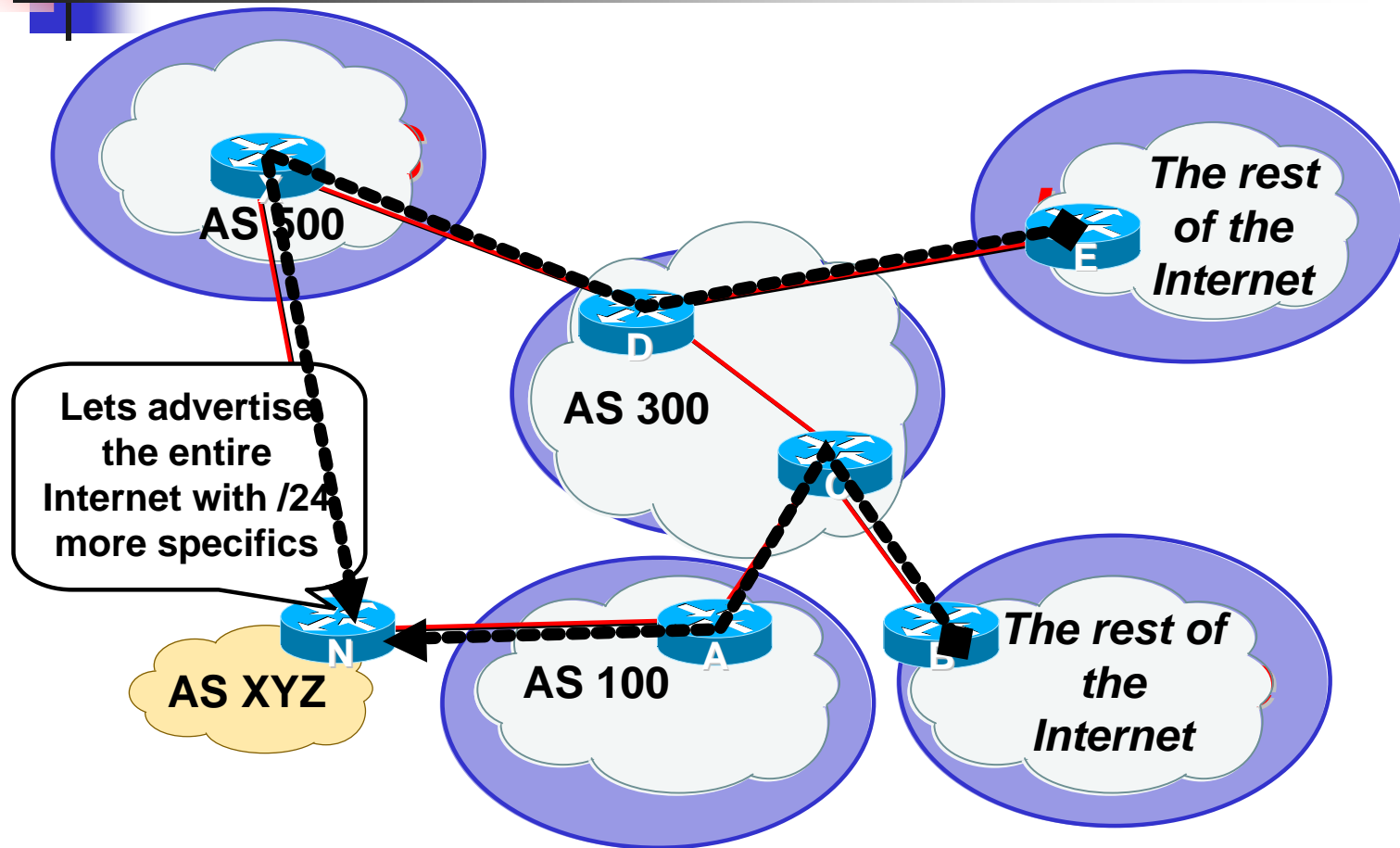
Malicious Route Injection

Reality – an Example



Malicious Route Injection

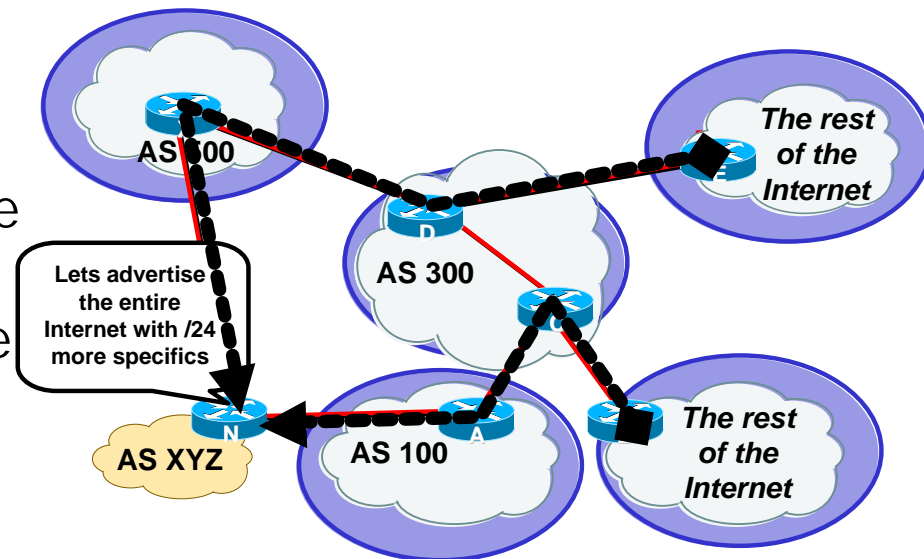
Reality – an Example



Malicious Route Injection

Reality – an Example

- Garbage in – Garbage out does happen on the Net
- AS 7007 Incident (1997) was the most visible case of this problem.
- Key damage are to those ISPs who pass on the garbage.
- Disruption, Duress, and Instability has been an Internet wide effect of Garbage in – Garbage out.



Malicious Route Injection

Attack Methods

- Good News – Risk is mainly to BGP speaking Routers.
- Bad News – Multihomed BGP Speaking customers are increasing!
- Really Bad News – Many of these routers have no passwords!
- Local layer 3 configuration alteration on compromised router
- Intra-AS propagation of bad routing information
- Inter-AS propagation of bad routing information

Malicious Route Injection



Impact

- Denial-Of-Service to Customer(s), ISP(s), and the Internet.
- Traffic Redirection / Interception
- Prefix Hijacking
- AS Hijacking

Malicious Route Injection

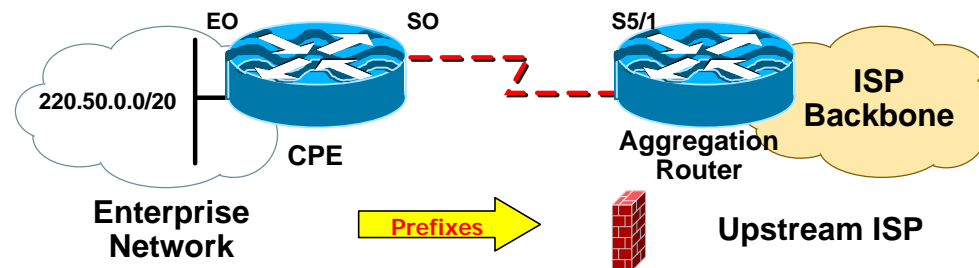
What can ISPs Do?

- Customer Ingress Prefix Filtering!
- ISPs should only accept customer prefixes which have been assigned or allocated to their downstream customers.
- For example
 - Downstream customer has 220.50.0.0/20 block.
 - Customer should only announce this to peers.
 - Upstream peers should only accept this prefix.

Malicious Route Injection

What can ISPs Do?

- Cisco Configuration Example on Upstream
router bgp 100
neighbor 222.222.10.1 remote-as 101
neighbor 222.222.10.1 prefix-list customer in
!
ip prefix-list customer permit 220.50.0.0/20
ip prefix-list customer deny 0.0.0.0/0 le 32



Malicious Route Injection

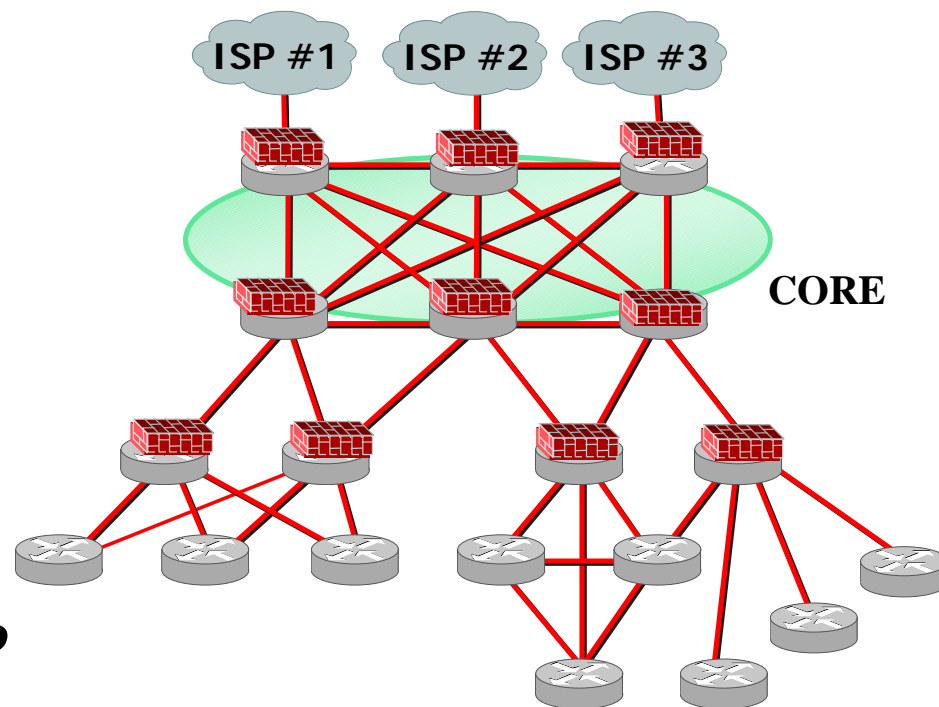
What can ISPs Do?

- Containment Filters!
 - Design your network with the principles of survivability.
 - Murphy's Law of Networking implies that the customer ingress prefix filter will fail.
 - Remember 70% to 80% of ISP problems are maintenance injected trouble (MIT).
 - Place Egress Prefix Filters on the Network to contain prefix leaks.

What can ISPs Do?

Containment Egress Prefix Filters

- Could place them on the POP/Regional Interconnects.
- Could place them on the border to the core.
- ***Should place them on the ISP peering links.***



What can ISPs Do?

Containment Egress Prefix Filters

- It is not rocket science!
- Just create a hard list of your RIR allocated prefixes.
- Cisco Configuration Example

```
router bgp 100
  network 221.10.0.0 mask 255.255.224.0
  neighbor 222.222.10.1 remote-as 101
  neighbor 222.222.10.1 prefix-list out-filter out
!
ip route 221.10.0.0 255.255.224.0 null0
!
ip prefix-list out-filter permit 221.10.0.0/19
ip prefix-list out-filter deny 0.0.0.0/0 le 32
```


What can ISPs Do?

Containment Egress Prefix Filters

- What about all my multihomed customers with prefixes from other ISPs?
- Add them to the customer ingress prefix filter.
 - You should know what you will accept.
- Add them to the master egress prefix-filter.
 - You should know what your advertising to everyone else.
 - *Bigness* is not an excuse.

Malicious Route Injection

What can ISPs Do?

- Customer Ingress Prefix Filtering
- Prefix filtering between intra-AS trust zones
- Route table monitoring to detect alteration of critical route paths



Alteration of Registry Information



Alteration of Registry Information

Perceived Threat & Reality

- Malicious People can change the RIR information for a target.

- Reality
 - IP and domain registries historically have not provided strong authentication for client transactions.
 - MAIL-FROM
 - Even when strong authentication is available at the RIR, it is commonly not used.
 - RIRs are commonly referenced to determine ownership of IP/domain assets.

Alteration of Registry Information



Reality

- Registry transactions are often the key to altering DNS delegations for IN-ADDR.ARPA and domain namespace.
- CERT/CC is aware of numerous incidents based on the attacker modifying registry information
- http://www.cert.org/vul_notes/VN-99-01.html

Alteration of Registry Information

Attack Methods

- Social engineering
 - Someone calls the NOC to change their routing policy. How do you know the person is an authorized to make the change?
- Defeating weak authentication methods
 - MAIL-FROM

Alteration of Registry Information

Impact

- Alteration of DNS glue records in top-level zones
 - Denial-of-service

- Alteration of delegated nameservers
 - Denial-of-service
 - Traffic redirection via malicious RR's
 - Bypass of DNS-based access controls
 - Alteration of information recorded by DNS-based logging mechanisms

Alteration of Registry Information

Impact

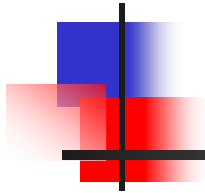
- Alteration of contact information
 - Includes domains, netblocks, and AS numbers
 - Enables social engineering attacks
- CERT/CC is aware of this technique being used to social engineer an ISP into routing a hijacked /8 prefix using a hijacked AS number

Alteration of Registry Information

What can ISPs and Customers Do?

- Demand and use strong transaction authentication methods to protect registry objects from malicious changes
- Verify critical registry records on a regular basis
- Request read-only 'freeze' for critical records

Denial-of-service Attacks Directed at Customer's CPE Routers



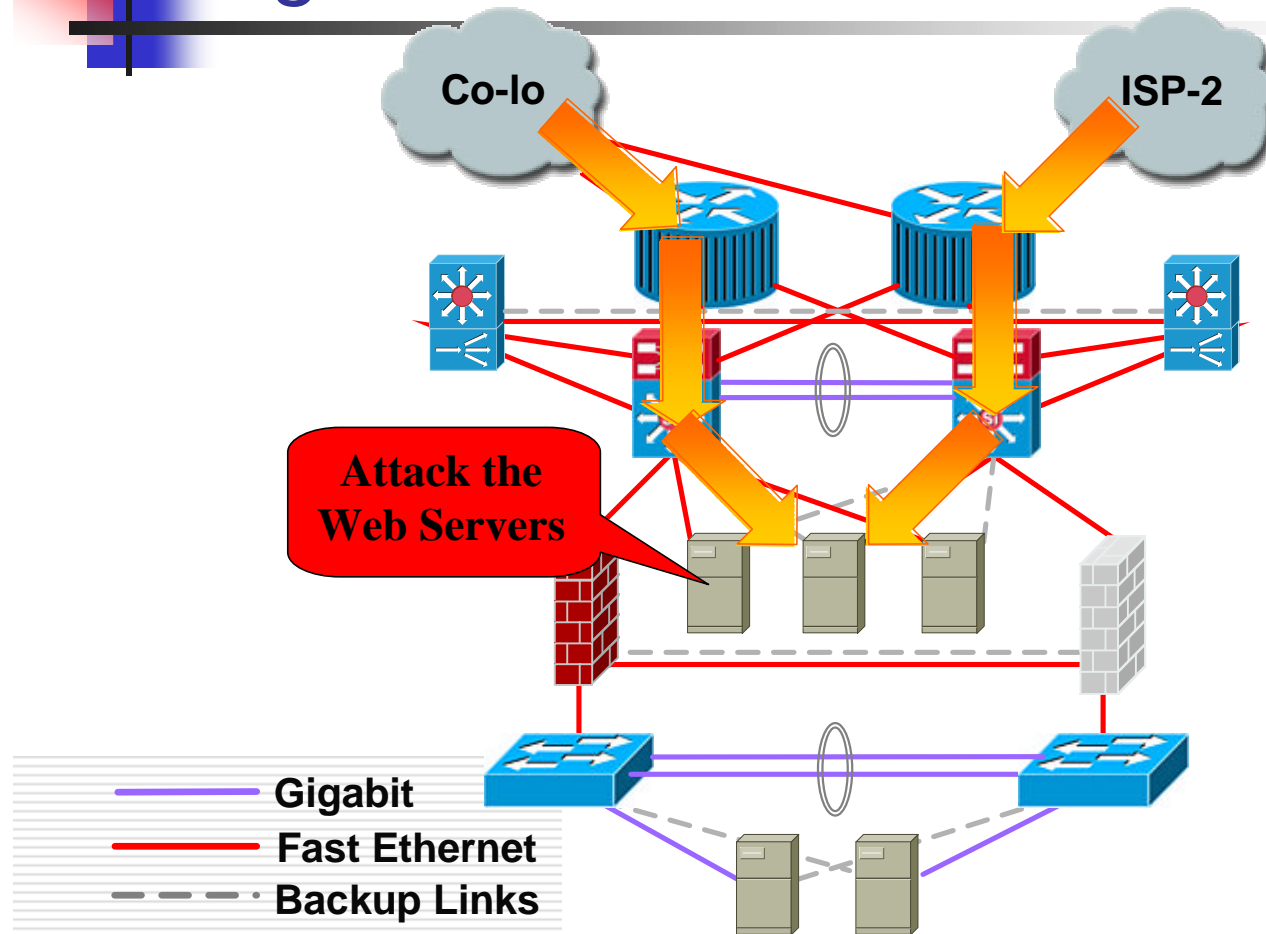
DOS the CPE

Perceived Threat

- Intruders understand that packet flooding attacks directed at routers can have broader impact than attacks directed at hosts
- The IP stack code path may be more expensive for packets directed at a router vs. packets transiting a router

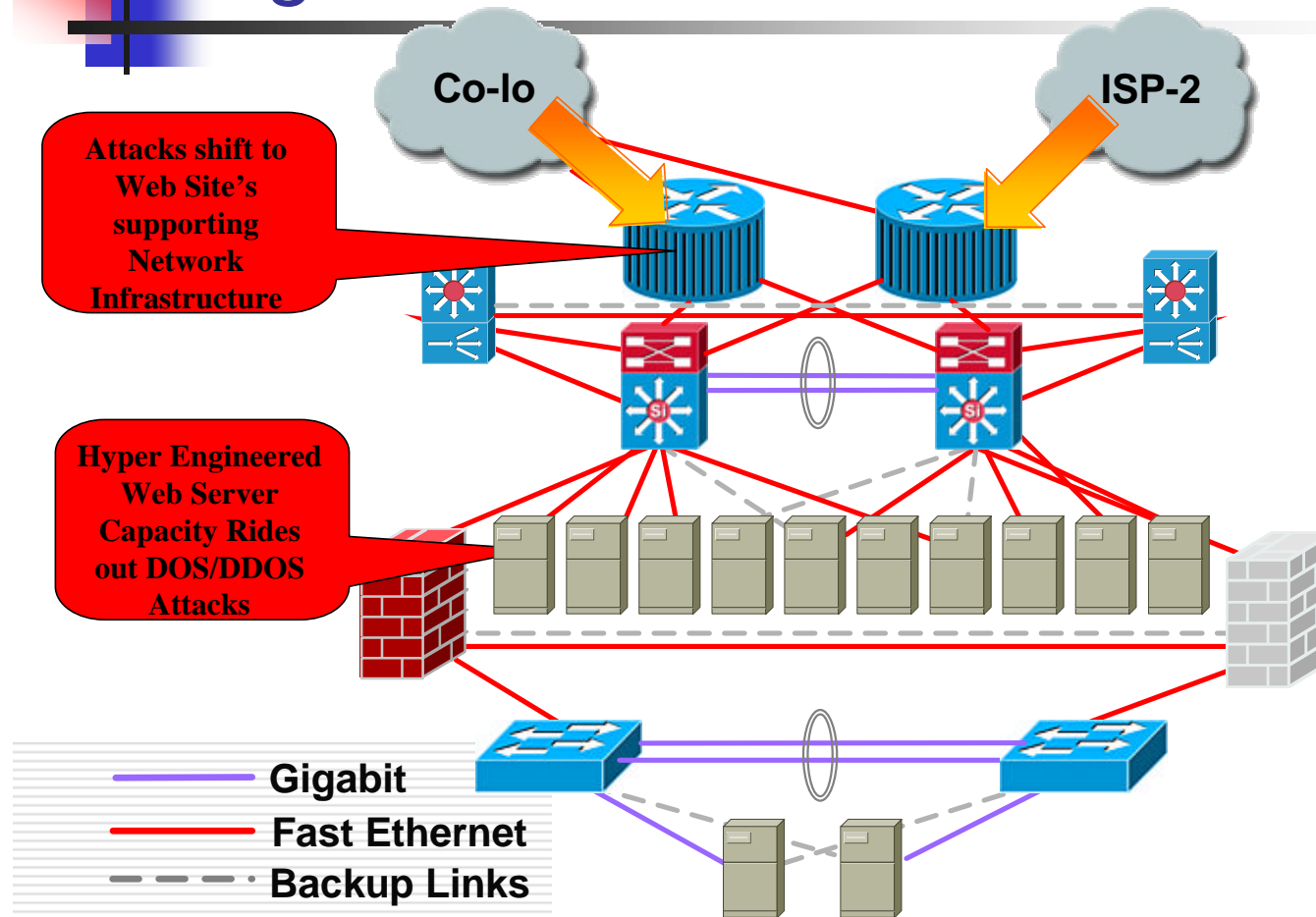
DOS the CPE

Big Sites Before Feb'00



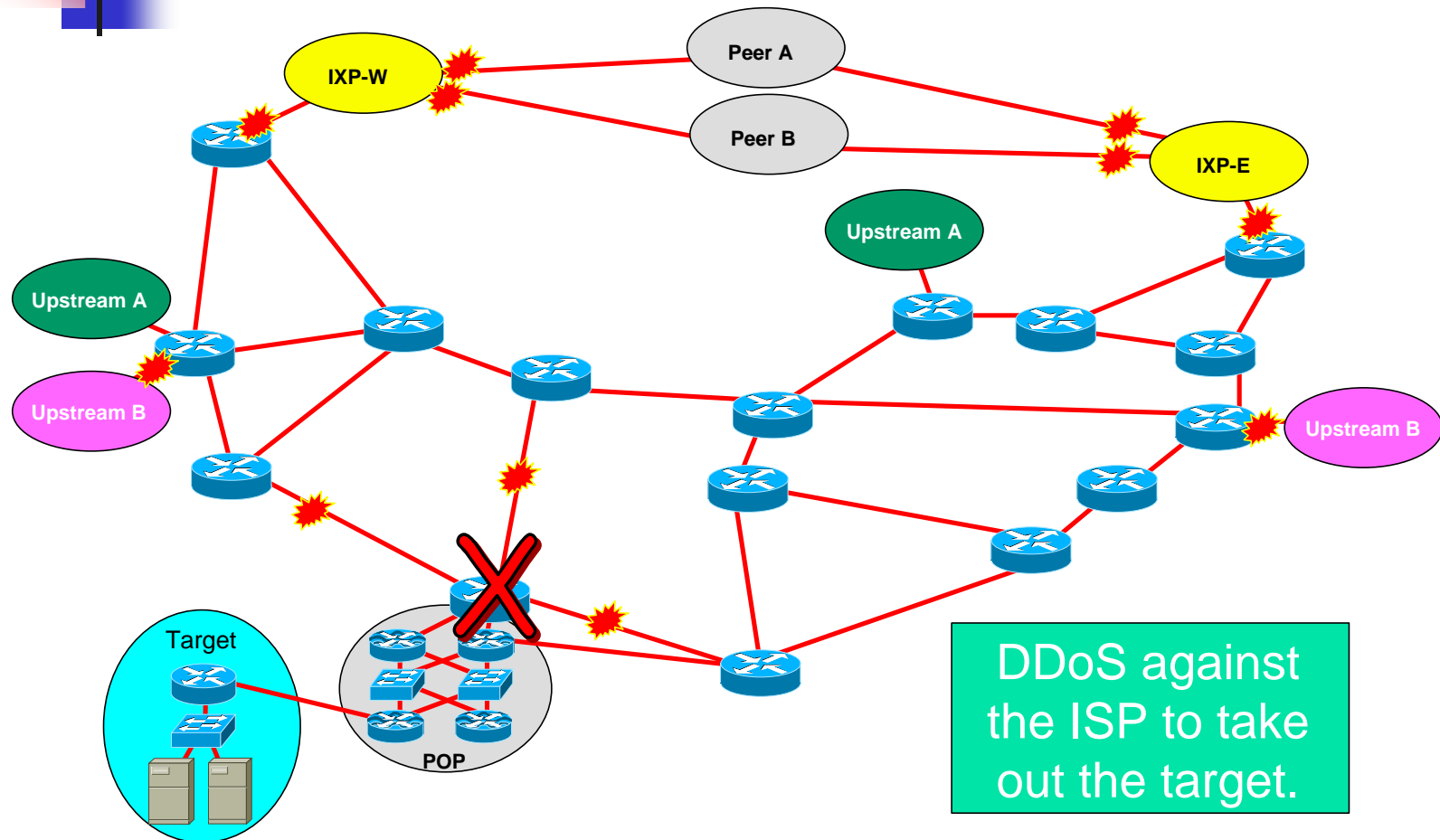
DOS the CPE

Big Sites after Feb'00



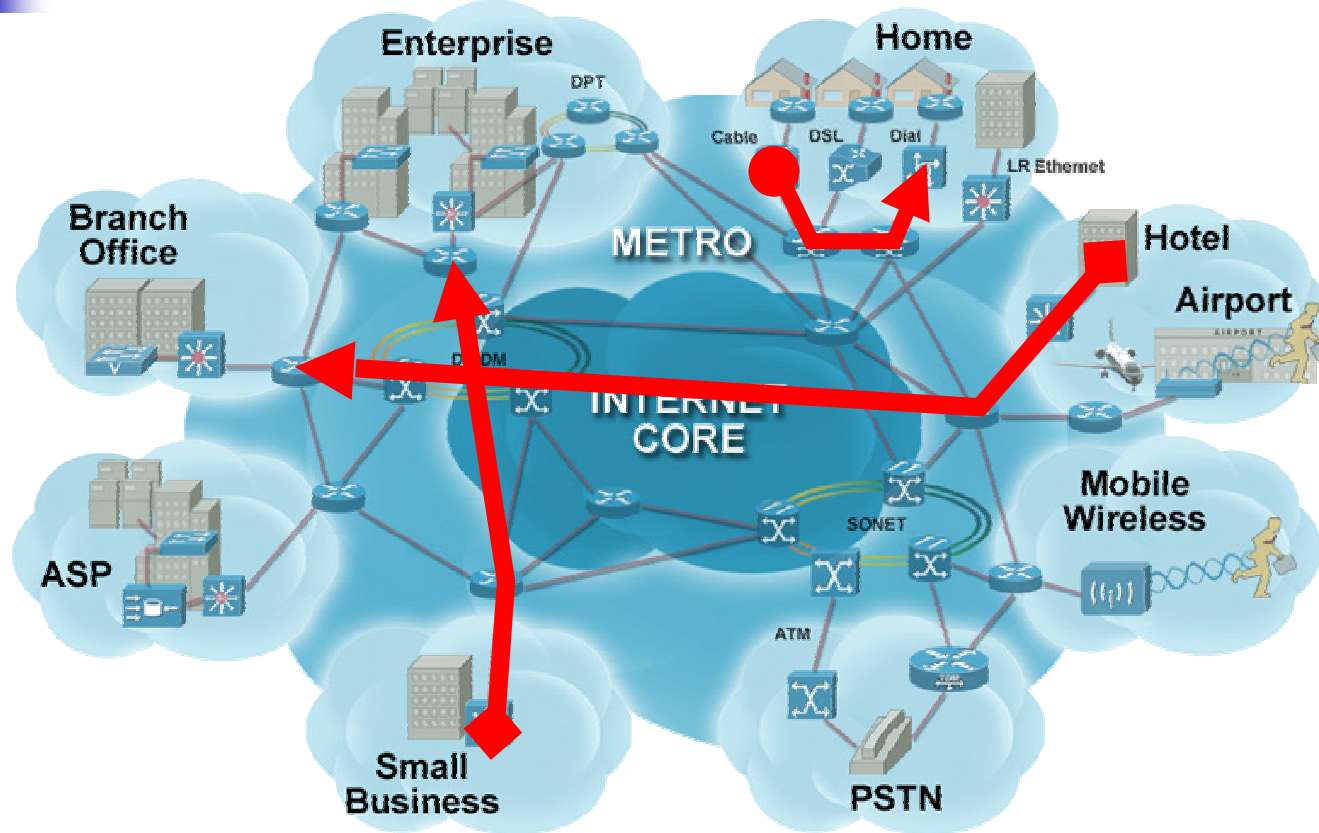
DOS the CPE

Reality – Attacks hit the ISP



DOS the CPE

Reality – Miscreant Wars!



DOS the CPE

Attack Methods

- Traceroute to discover attack target
 - Looking for something just upstream from intended victim
 - Some attacks target each router in the path
- Packet rate attacks
 - Resource consumption attack against the router
 - The ol' stack code path issue may apply
 - Router service ports (e.g., BGP, telnet, ssh, etc)

DOS the CPE

Attack Methods

- Packet size attacks
 - Bandwidth denial-of-service against layer 1
 - Resource consumption if router has more bandwidth attached at layer 1 than it's resources can handle

DOS the CPE

Impact

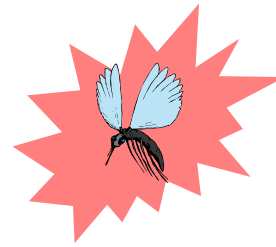


- Denial-of-service

DOS the CPE

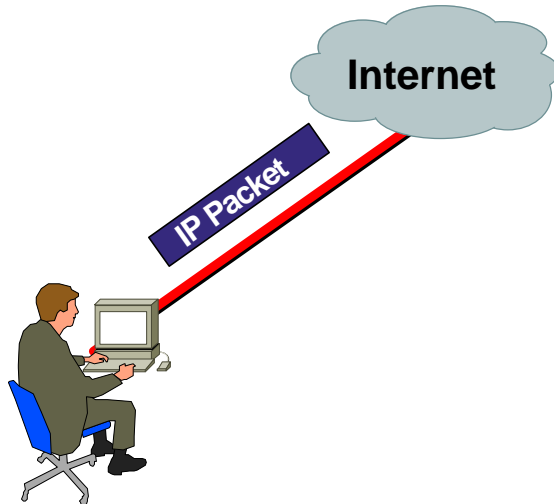
What is Co-Lateral Damage?

- Co-Lateral Damage hurts others around the target of attack.
- Some attackers work very hard to minimize co-lateral damage (cruse missile strike).
- Others do not care (use a tank to swat a mosquito).
- Co-Lateral Damage is core reason why ISPs must respond to their customer's DOS attacks.



DOS the CPE

What is Co-Lateral Damage?

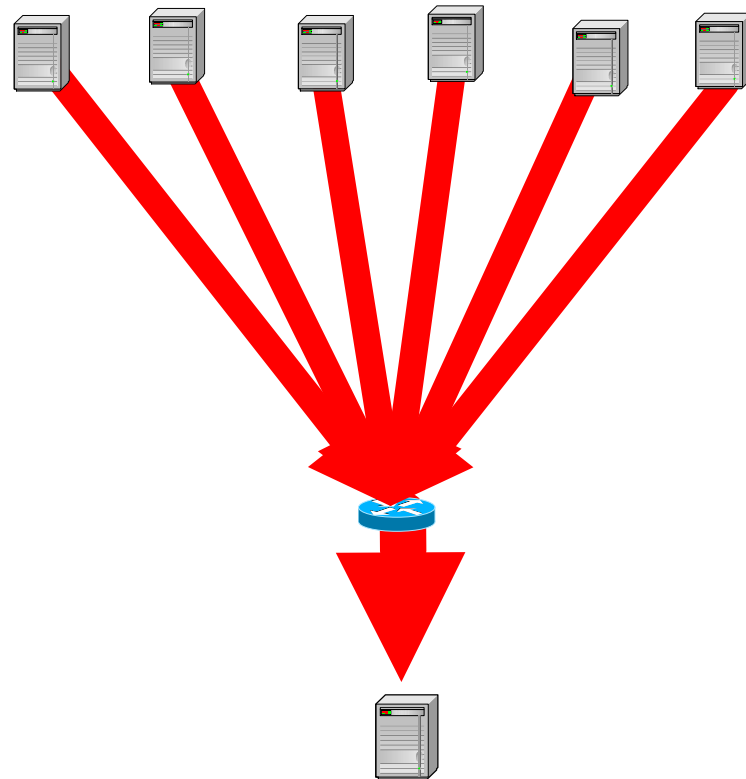


- It is all about the packet
- Once a packet gets into the Internet, someone, somewhere has to do one of two things:
 - *Deliver the Packet*
 - *Drop the Packet*
- In the context of a DOS attack, the question is who and where will that drop that packet.

DOS the CPE

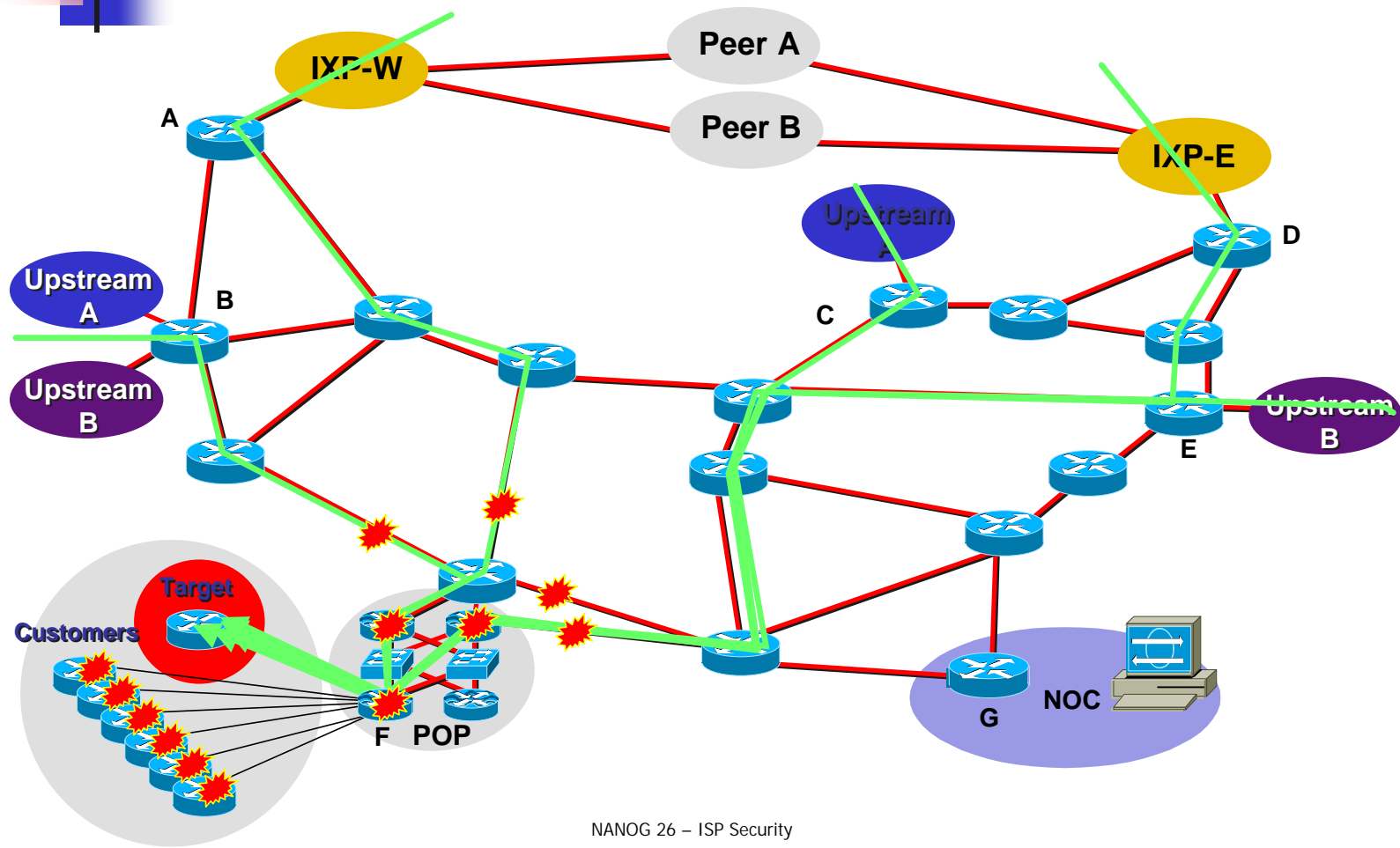
What is Co-Lateral Damage?

- Single Homed Customer's Circuit Saturates from a DOS Attack.
- Which router has the static route?
- Which router has the aggregate route?



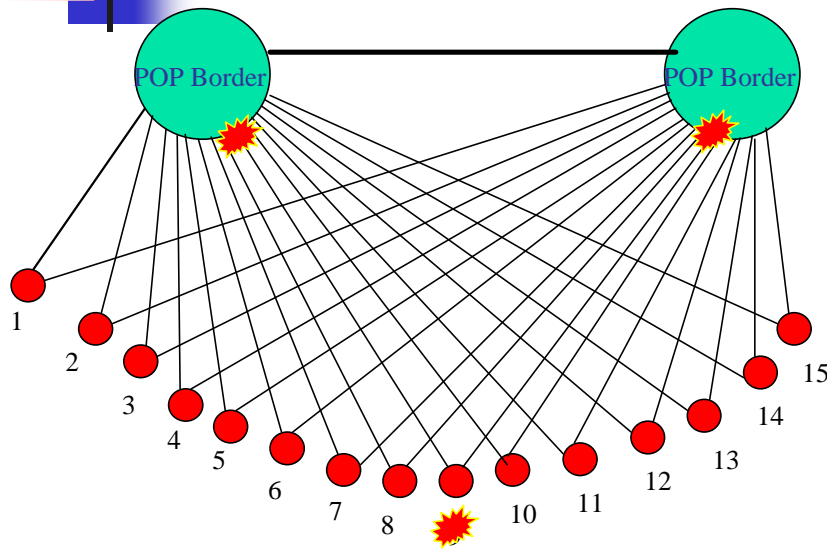
DOS the CPE

DOS Funnel and Collateral Damage

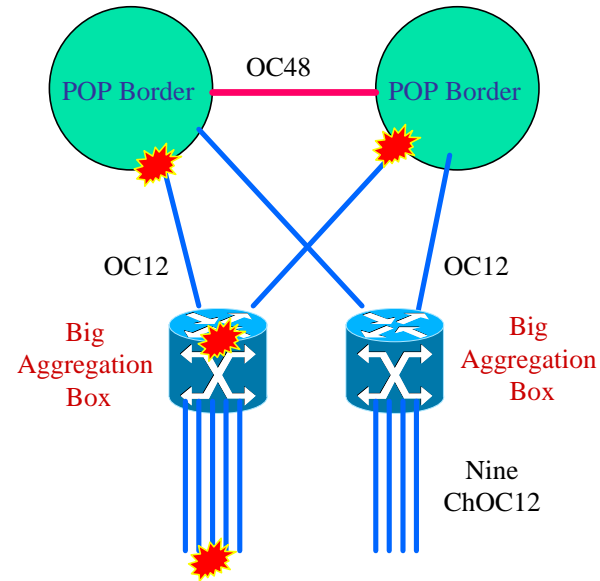


DOS the CPE

Risk Increases with Density



**Lots of Aggregations Routers
with 10s to 100s of customers
per router.**

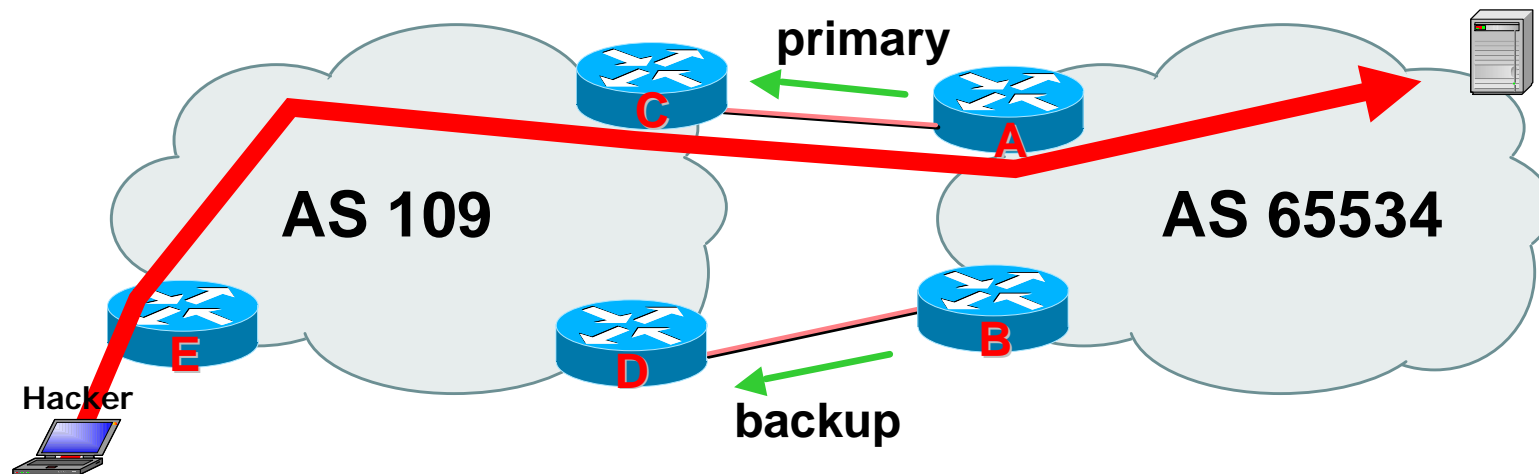


**Few Aggregations Routers
with 100s to 1000s of
customers per router.**

It is all about # of Customers per RU

DOS the CPE

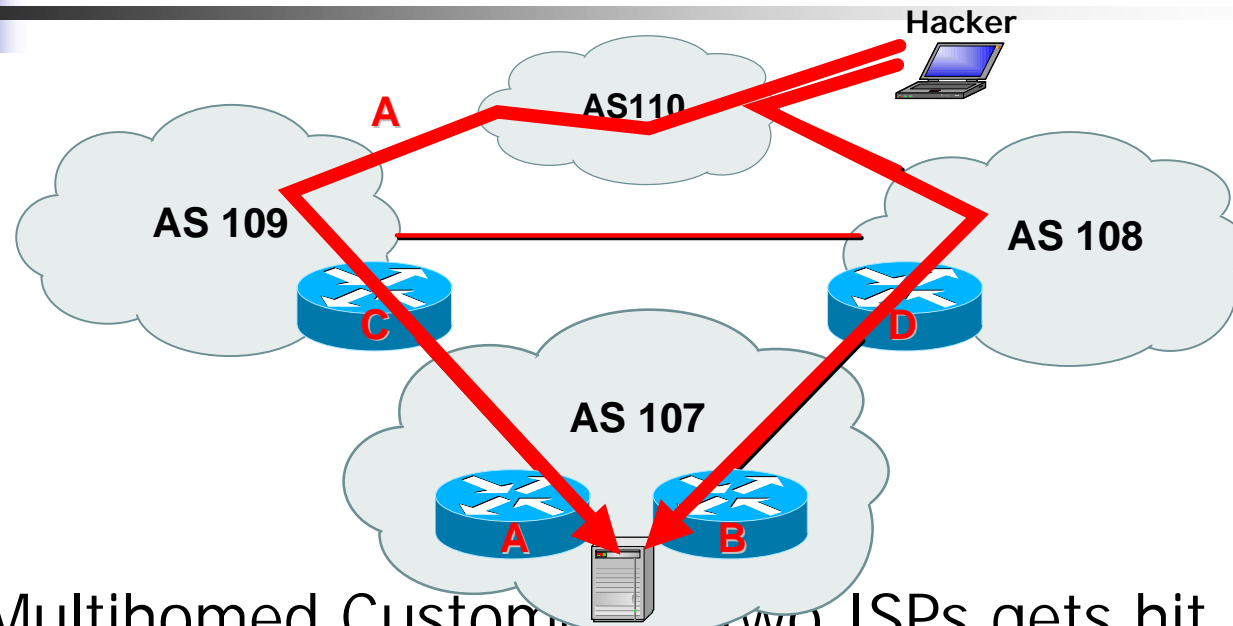
DOS Flapping



- Multihomed Customer's Primary Link get saturated?
 - Link saturation causes BGP to drop
 - BGP drop on the primary means that the back-up is used
 - Who drops the packets during convergence?
 - Back-up path saturates, dropping BGP, then what? Back to primary?

DOS the CPE

DOS Flapping



- Multihomed Customer to two ISPs gets hit.
 - Line saturates, BGP drops, attack shifts OR attack aggregates!

DOS the CPE

Co-Lateral Damage is Real

- Co-Lateral Damage is Real. If you have not yet experienced it, you will.
- How you architect your network, your routing, and your provisioning effects the extent of co-lateral damage.
- All those “VPN Tunneling Solutions” are just as vulnerable to co-lateral damage.
- What tools and techniques you prepare affects how you can mitigate the effects of co-lateral damage.
- Do nothing and you may find that a simple DOS attacks against one customer turns into a network nightmare.

DOS the CPE

What can ISPs Do?

- Policies, Preparation, and Practice!
- Prepare your Identification, Classification, Traceback, and Reaction Tools.
 - Classification ACLs
 - Sink Holes
 - Backscatter Traceback – works for customer aggregation routers as well as ISP – ISP peering points.

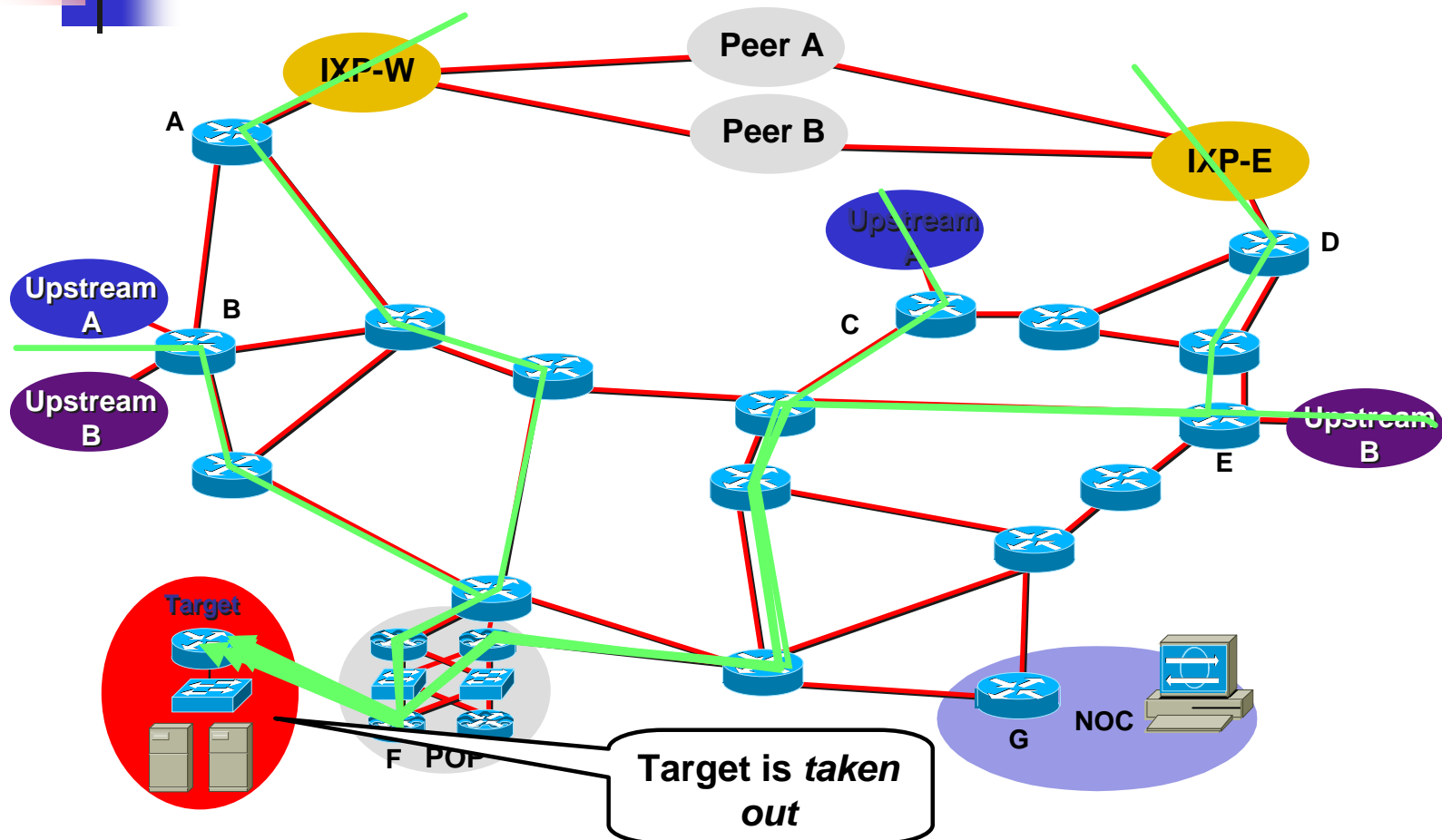
What can ISPs Do?

Remote-Triggered Black Hole

- We use BGP to trigger a network wide response to an attack flow.
- Push the packet drop to the edge of the network.
- 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.

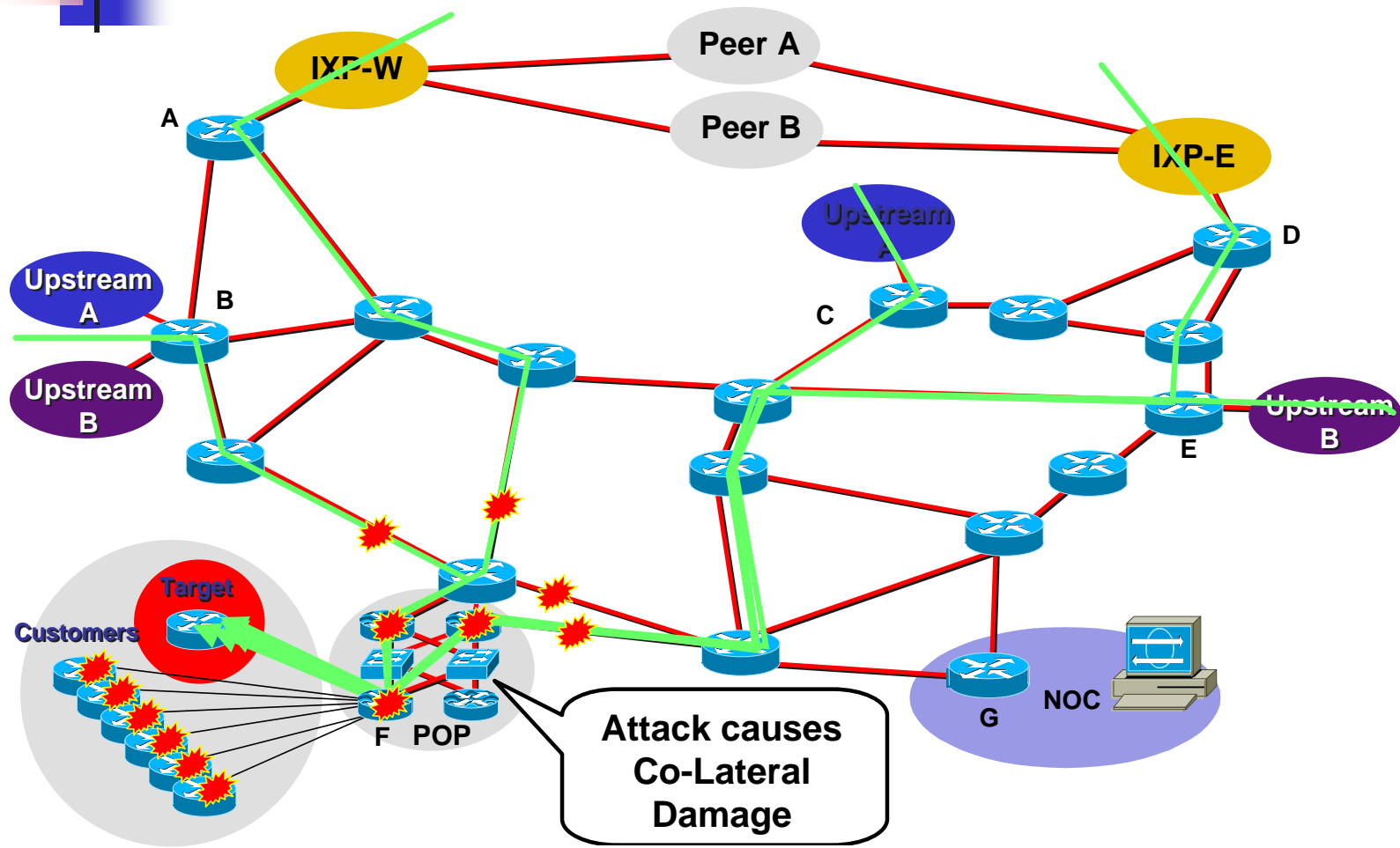
What can ISPs Do?

Remote-Triggered Black Hole



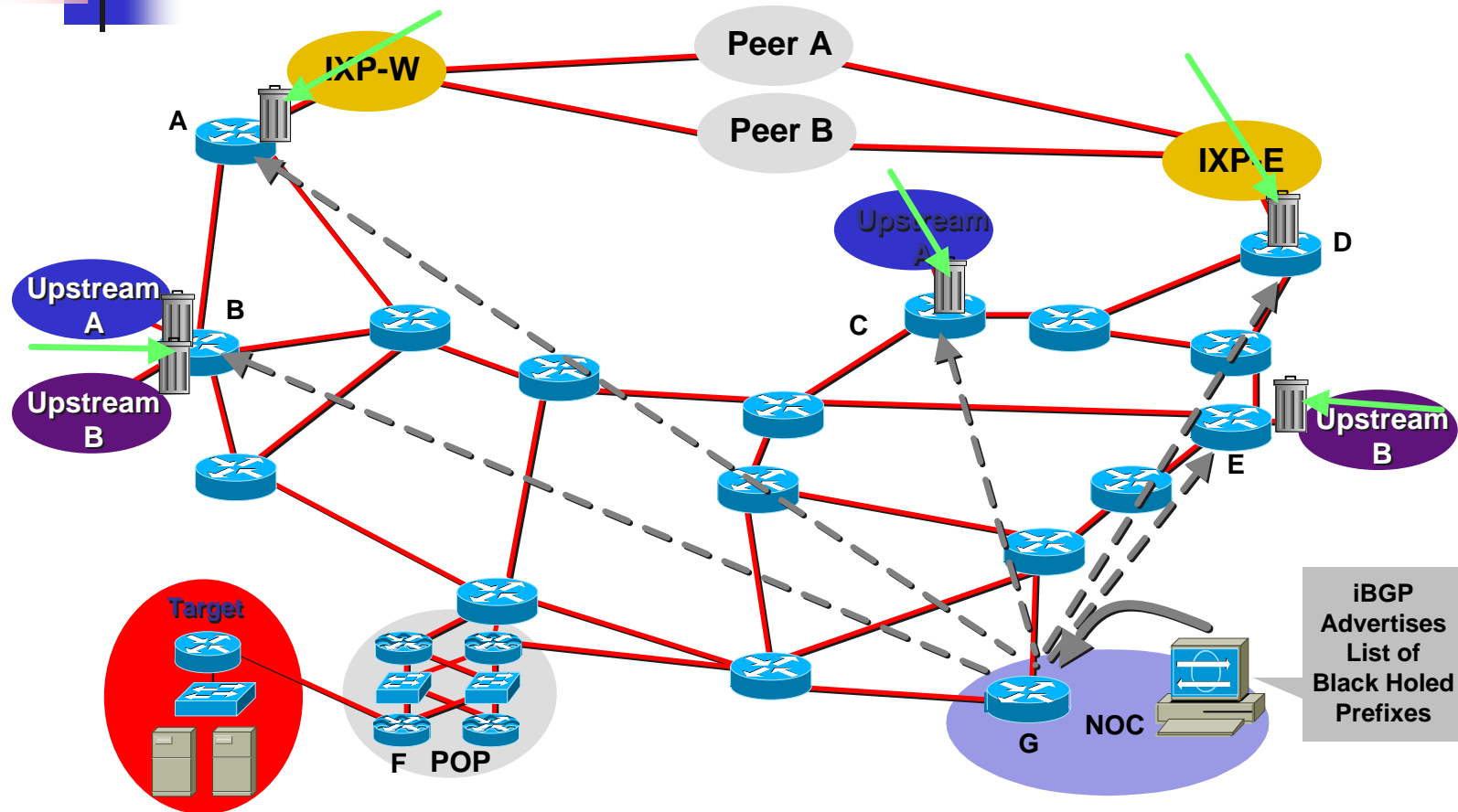
What can ISPs Do?

Remote-Triggered Black Hole



What can ISPs Do?

Remote-Triggered Black Hole



What can ISPs Do?

Remote-Triggered Black Hole

- Remote Triggered Black Hole filtering is the foundation for a whole series of techniques to traceback and react to DOS/DDOS attacks on an ISP's network.
- Preparation does not effect ISP operations or performance.
- It does adds the option, providing a valuable ISP's *security toolkit*.

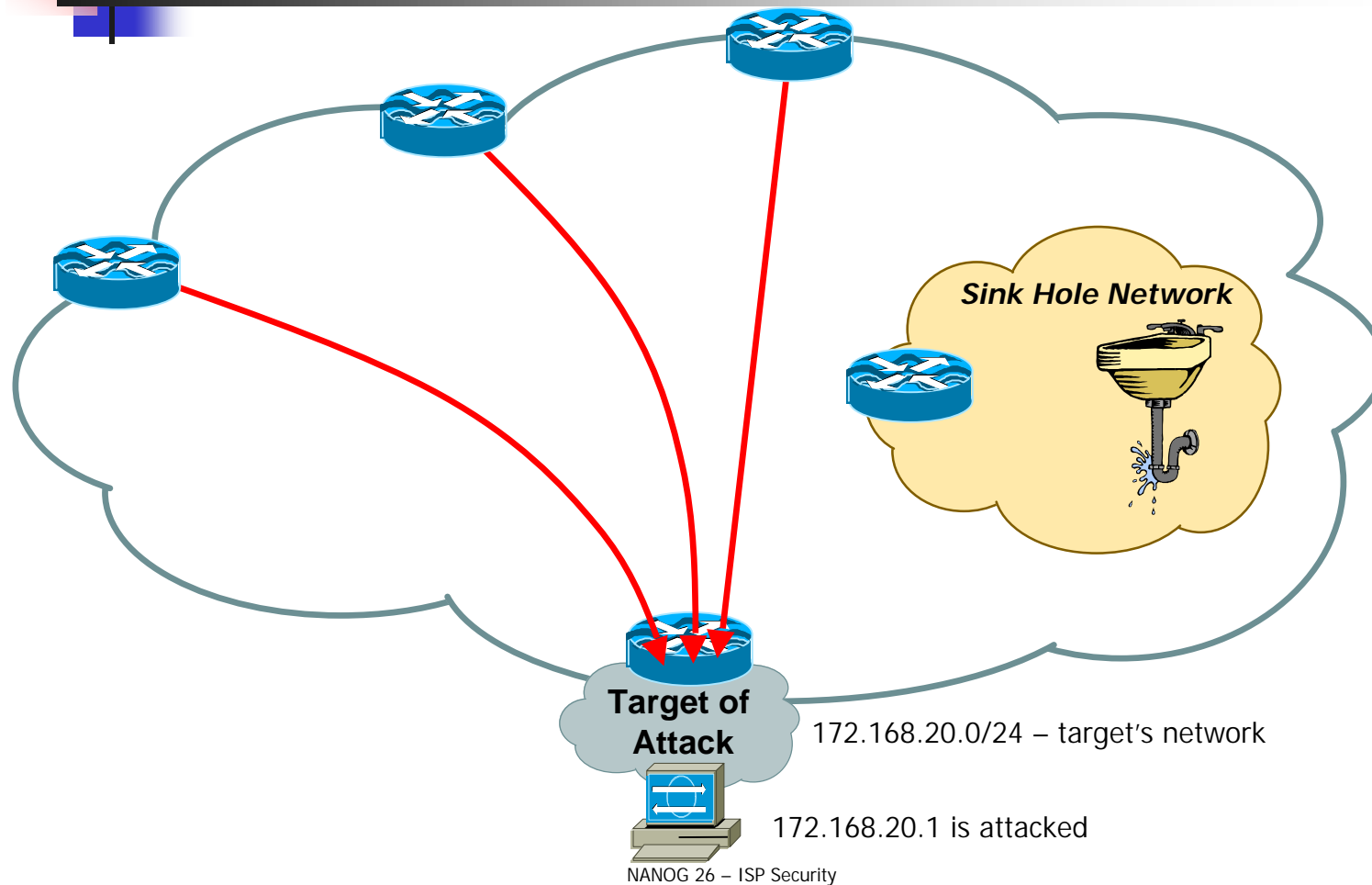
What can ISPs Do?

Sink Hole Routers/Networks

- Sink Holes are versatile security tools.
 - 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)

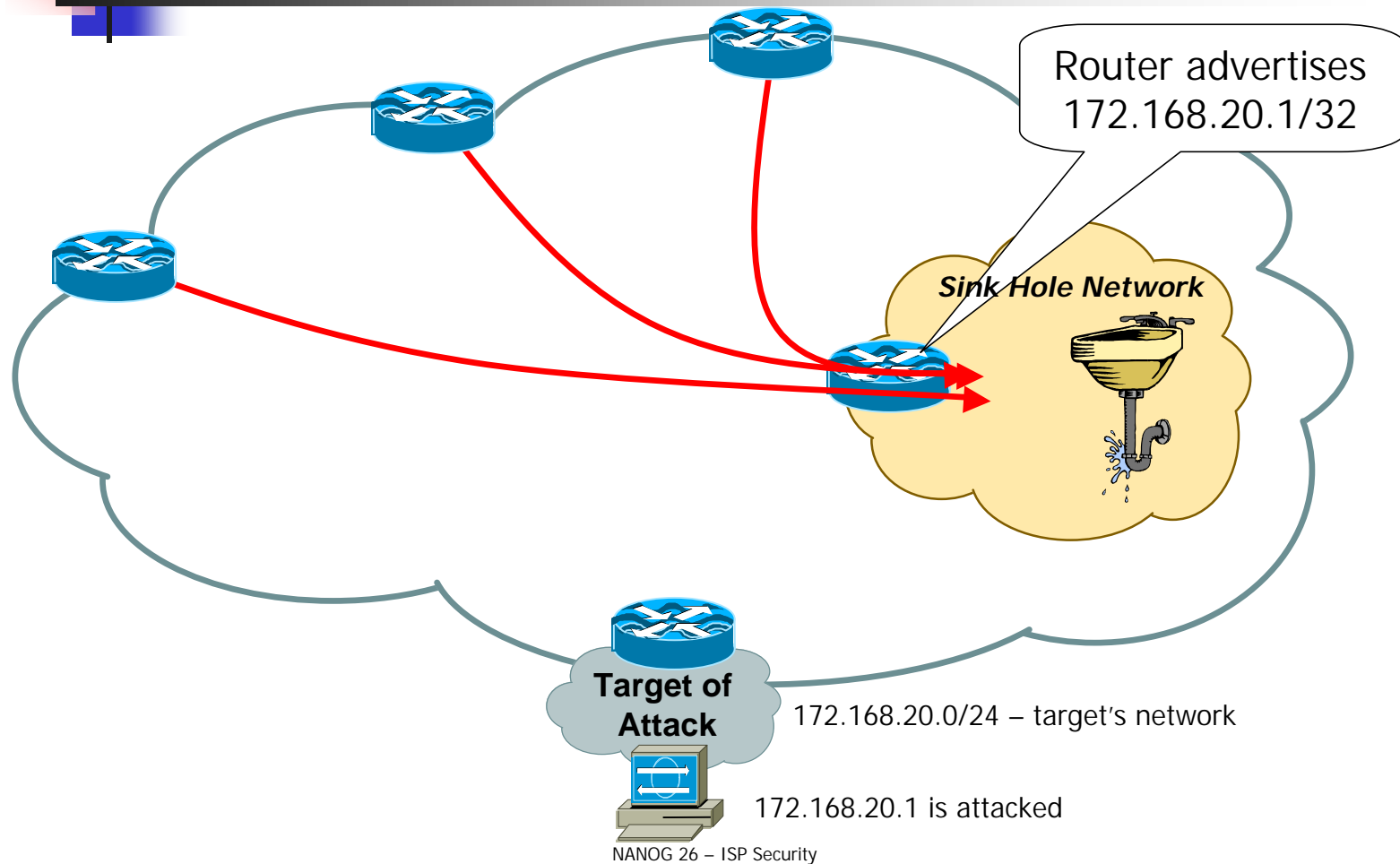
What can ISPs Do?

Sink Hole Routers/Networks



What can ISPs Do?

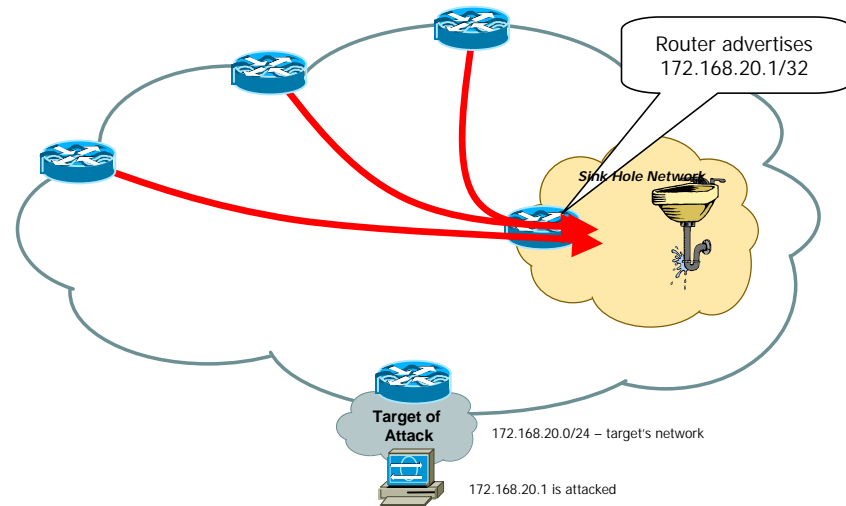
Sink Hole Routers/Networks



What can ISPs Do?

Sink Hole Routers/Networks

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



DOS the CPE

What can Customers Do?

- Assume that one day you will be attacked.
- Prepare!
 - Have the security contacts for each of your upstream ISPs.
 - Be prepared to switch IP addresses for critical services that are under attack.
 - Move the service under attack to a new /32 as the original /32 is black holed by the ISP.
 - Be on all your vendor's security vulnerability mailing list and PATH your software.

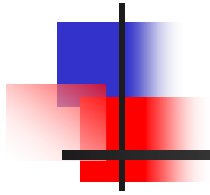


Summary



Summary

- Intruders are actively pursuing attacks against routing infrastructure
- ISPs have a vested interest to do something to protect themselves from violated CPEs.
- Next Steps
 - NANOG Security BOF – Monday Night
 - Nsp-security Forum. Peers in the NSP/ISP Operations community actively working together to combat attack.
 - <http://puck.nether.net/mailman/listinfo/nsp-security>



Q&A



More Information



More Information

- Denial of Service information page
 - <http://www.denialinfo.com/>
- IOS Essentials—Features every ISP should consider
 - <http://www.ispbook.com>
- RFC 2827 “Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing”
 - <ftp://ftp.isi.edu/in-notes/rfc2827.txt>
- Distributed systems intruder tools workshop report
 - http://www.cert.org/reports/dsit_workshop.pdf
- CERT advisories
 - <http://www.cert.org/>
- FIRST
 - <http://www.first.org/>



More Information

- “Tackling Network DoS on Transit Networks”: David Harmelin, DANTE, March 2001 (describes a detection method based on netflow)
[\[http://www.dante.net/pubs/dip/42/42.html\]](http://www.dante.net/pubs/dip/42/42.html)
- “Inferring Internet Denial-of-Service Activity”: David Moore et al, May 2001; (described a new method to detect DoS attacks, based on the return traffic from the victims, analysed on a /8 network; very interesting reading)
[\[http://www.caida.org/outreach/papers/backscatter/index.xml\]](http://www.caida.org/outreach/papers/backscatter/index.xml)
- “The spread of the code red worm”: David Moore, CAIDA, July 2001 (using the above to detect how this worm spread across the Internet) [\[http://www.caida.org/analysis/security/code-red/\]](http://www.caida.org/analysis/security/code-red/)



More Information

DoS Tracing:

- “Tracing Spoofed IP Addresses”: Rob Thomas, Feb 2001; (good technical description of using netflow to trace back a flow)
[\[http://www.enteract.com/~robt/Docs/Articles/tracking-spoofed.html\]](http://www.enteract.com/~robt/Docs/Articles/tracking-spoofed.html)

Honeypots and Honeynets:

- Honeypots: Tracking Hackers
<http://www.tracking-hackers.com/>

IETF RFCs:

- **RFC 2179 Network Security For Trade Shows.** A. Gwinn. July 1997. (Format: TXT=20690 bytes)



More Information

“DoS attacks against GRC.com”: Steve Gibson, GRC, June 2001 (a real life description of attacks from the victim side; somewhat disputed, but fun to read!)

<http://grc.com/dos/grcdos.htm>

Improving Security on Cisco Routers

<http://www.cisco.com/warp/public/707/21.html>

Increasing Security on IP Networks

<http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2016.htm>

Paper from S. Fluhrer (Cisco Systems), I. Mantin and A. Shamir (Weizmann Institute)

www.crypt0.com/papers/others/rc4_ksaproc.ps

Other security tools

www.insecure.org/tools.html



More Information

- CAIDA paper “Inferring Internet Denial-of-Service Activity”

■ www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf