Cisco ISP Security Update

Lifting up the hood and checking what is really happening inside.

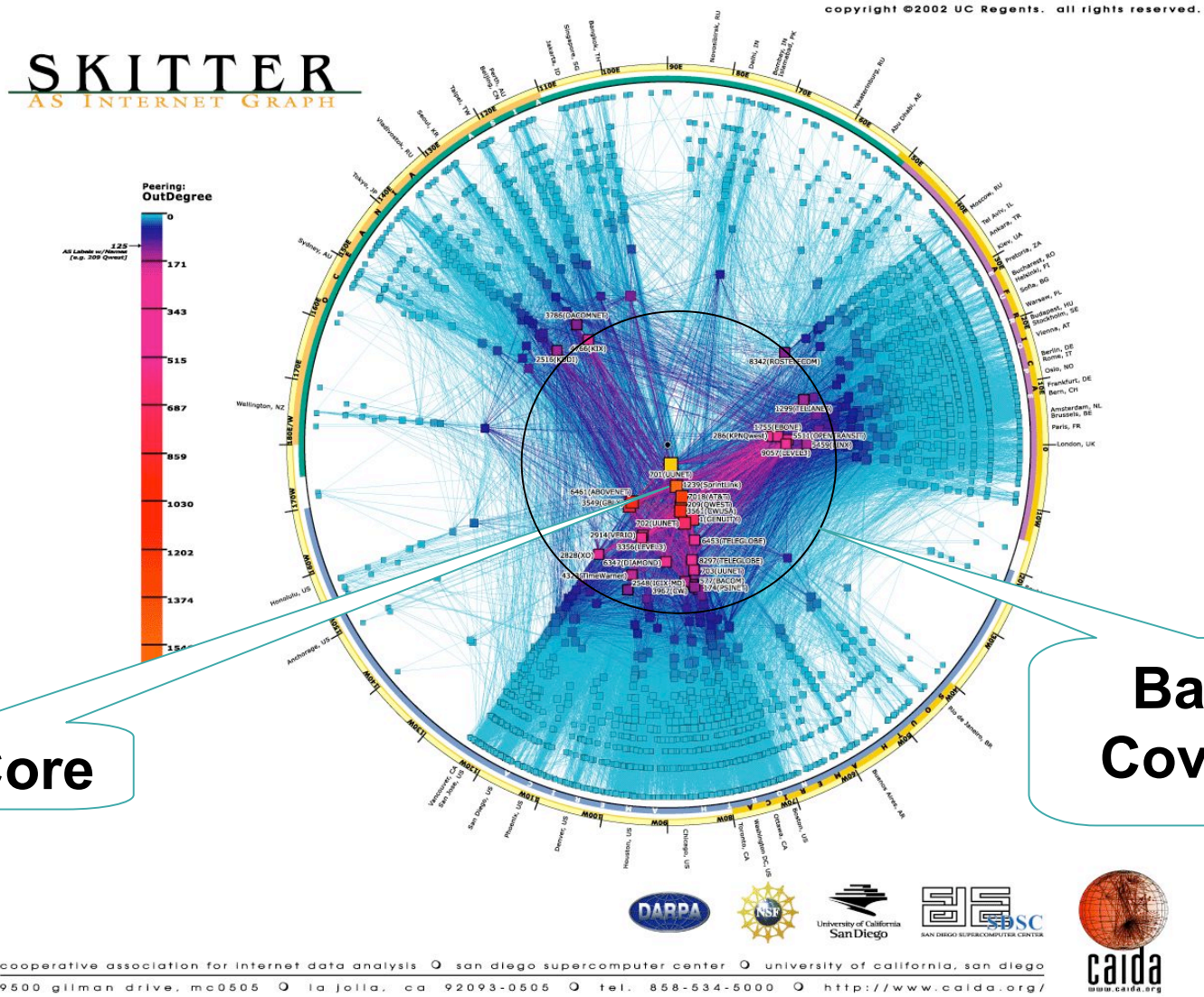
Agenda

- Cisco's ISP Security Evolution
- Reality of ISP Security
- A Realistic Look at the Router's Internal Vulnerability Points
- Example: Receive Path Protect on the Cisco 12000
- Source Based – Remote Triggered Black Hole Filtering

Before we begin ……

- **A lot of the information here is in the grey area of Corporate NDA and uncomfortable zone where public discussion might cause risk to our customers.**

What is the *Skitter Core?*



Skitter Core

Barry's Coverage

CAIDA is a program of the University of California's San Diego Supercomputer Center (UCSD/SDSC)
skitter is supported by DARPA NGI Cooperative Agreement N66001-98-2-8922, NSF ANIR Grant NCR-9711092 and CAIDA members

Cisco's ISP Security Evolution

What is happening inside Cisco to Counter the ever changing Security Risk to the Internet

Cisco and ISP Security

- Cisco has always worked with our customer to find innovative ways to counter security threats on the Net.
- What has changed in Cisco is a transition from a *reactive* mode to a *proactive* mode.
- Finding ways to optimize our rapid reaction processes (around our PSIRT Team)

Distributed Denial of Service (DDoS)

YAHOO!

amazon.com

CNN.com

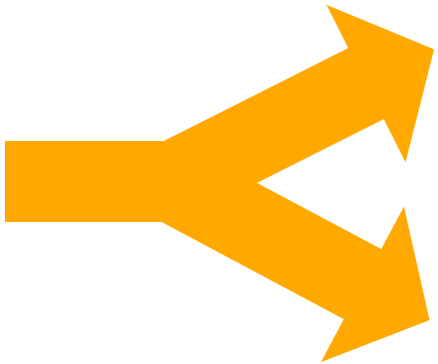
ebay

E*TRADE

Feb'00 Distributed Denial of Service (DDoS) Attacks

- Internal Effort inside of Cisco to anticipate the next target for DOS/DDOS attacks.
- *Attack-interest* internal alias created to start coordinating efforts.
- Next phase attacks anticipated to directly target routers.
- Created *Attack-Lab* to directly evaluate the attack vectors on a router.
- Engineering Empowerment to allow the broad talent pool in Cisco to get to work (more about this later).

Two path action plan …….



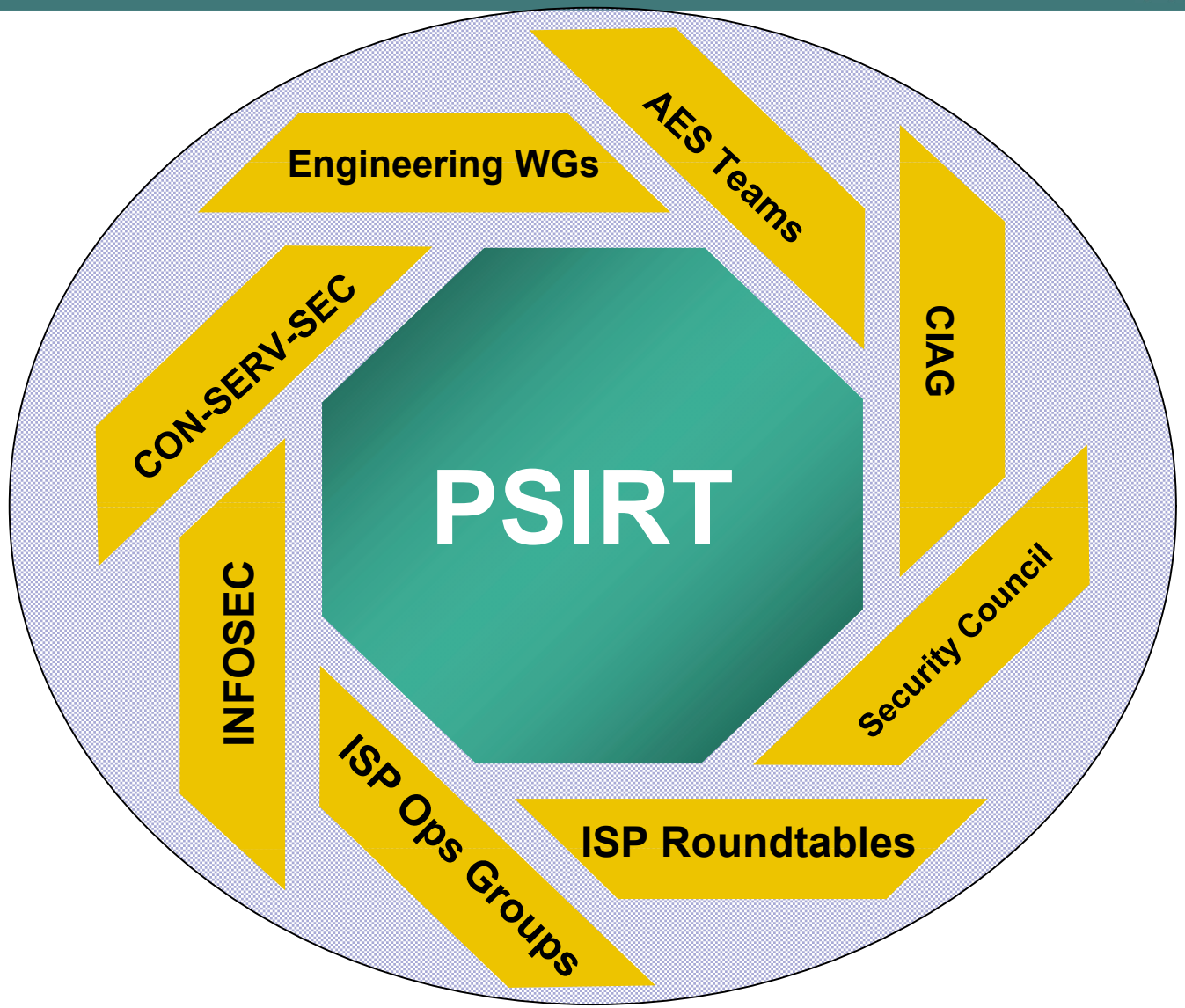
Improve our means to REACT to an incident or vulnerability

PROACTIVELY find un-explored attack vectors and mitigate them with hardware, software, and architecture solutions.

OPSEC vs Business Unit

- VPN and Security Services Business Unit (VSEC) creates and sells products.
- Operations Security (OPSEC) Community creates features, plugs vulnerabilities, and helps customers get the maximum security enhancements out of their existing networks.
- Sometimes the two communities interact. Problem is one is focused on revenue and the other is focused at keeping the Net alive.

Cisco's OPSEC Community



The Cisco PSIRT

Cisco.com

- **Product Security Incident Response Team**
- **Handling of *Cisco* product vulnerabilities**
- **Customers report *security* problems with Cisco products to PSIRT (not to TAC)**
- **The PSIRT:**
  - **… assists in finding immediate workarounds**
  - **… works with engineering to fix vulnerabilities**
  - **… escalates within Cisco if necessary**
  - **… helps customer in fixing the problem**
- **PSIRT is one of two Cisco FIRST Teams (our internal InfoSec is the second FIRST Team)**

Cisco OPSEC Philosophy

- **Security problems will always exist.**
- **We do NOT hide our vulnerabilities.**

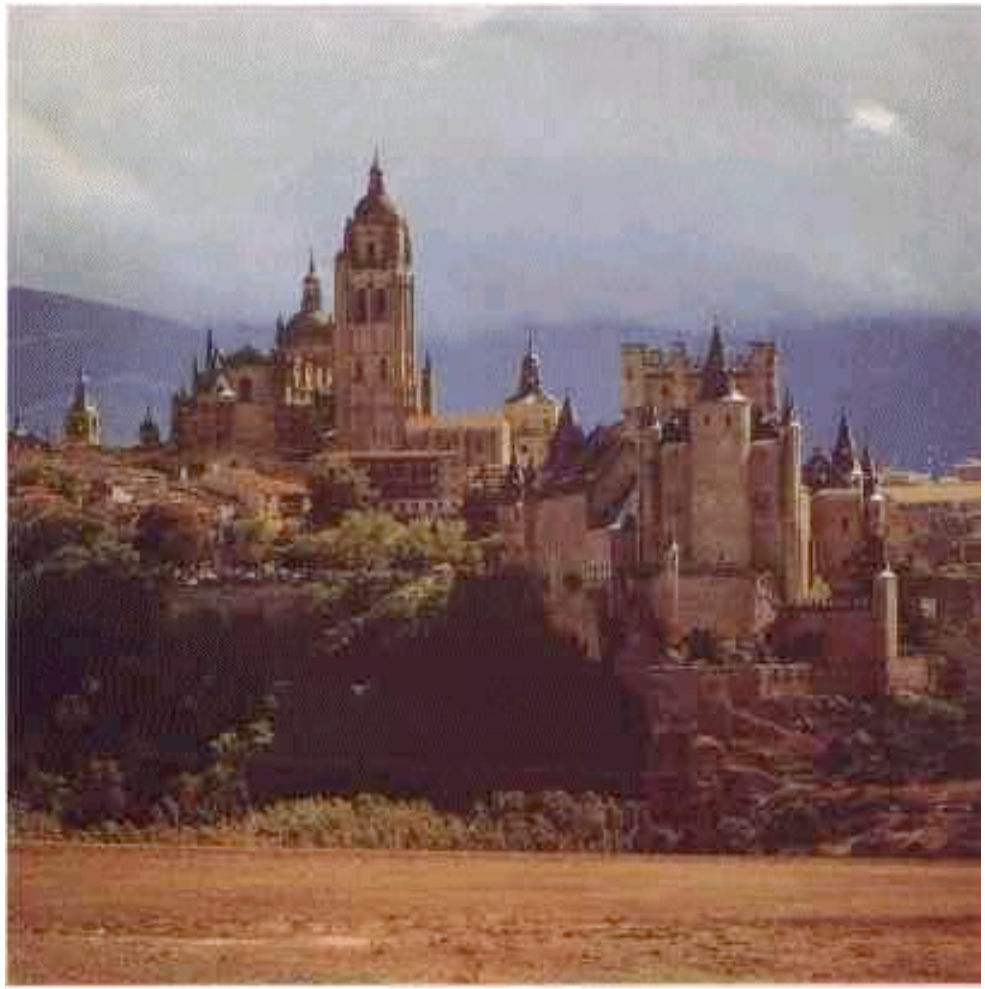
  Once a fix is executed, we announce to everyone on the entire planet at the same time.

  If a vulnerability goes *active exploit in multiple locations,* we announce to everyone, even if we do not have a fix.
- **We let our customers know, advice on how to fix problems, and help finding workarounds.**
- **We make security s/w fixes usually available for free.**

Proactively Find the Attack Vectors

- Cisco Engineers are individually pushing forward great security innovations!
- Not once has the author experienced any engineer ever “pushed back” when it comes to security. It has always been “how can I help … within the limits of my equipment?”
- The result is broad innovation in the way we build our equipment – with new techniques added to each new generation of equipment.

ALCAZAR – Infrastructure Security



Alcazar in Segovia, Spain

al·caz·ar (l-kzr, -käzr, lk-zär)
n. A Spanish palace or fortress, originally one built by the Moors.

Collected all ISP Security Roundtable feature/function ideas (and more).

Working to execute each of these features/functions and commit code into IOS.

Baseline for hardware and ASIC work.

Also referred to as:
NIS
Network Infrastructure Security
Secure IOS

Side Effect of this *Grassroots* Innovation

- **Cisco's core "security" problems are not a problem of lack of security.**

  Grassroots innovation does not bubble to the top.

  No Team dedicated to coordinate cross BU security work (working on that). Innovation spread out through Cisco's products

  No one to capture and communicate our security innovation to our customers.

- **We have a long ways to go, but *security attitude* among engineers is great!**

Reality of ISP Security

ISP's Security Attack Profile

- **Attacks are part of every day operations. One Tier 1 ISP characterizes their attack profile as the following (based on mid '2000 data):**

  90% of attacks are vindictive "script kiddy" attacks.

  These are the one ISP's customers are hit with every day. The volume of the attacks take up a lot of time.

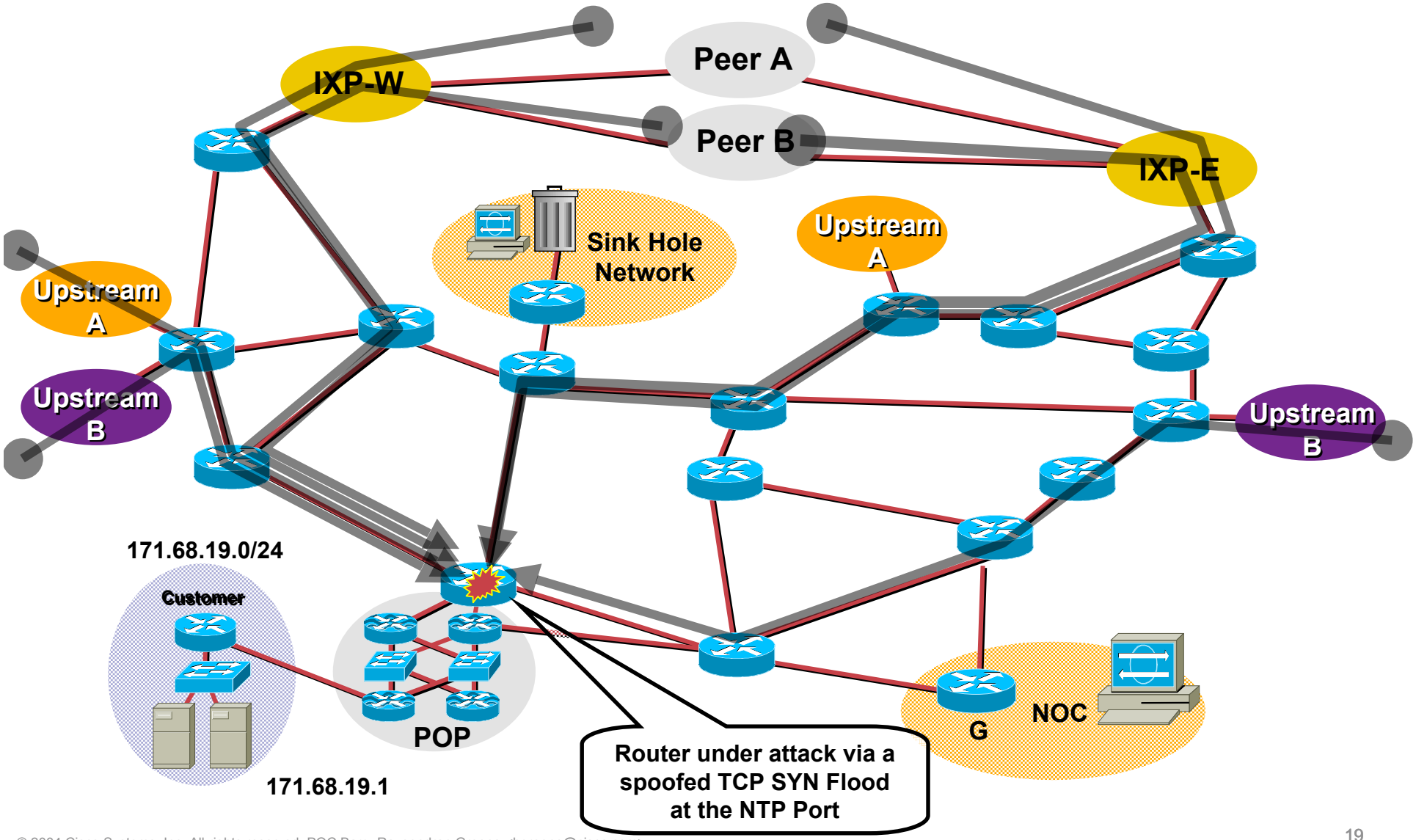
  9% are of a more serious DDOS type.

  These are the ones that cause co-lateral damage. Also one of the main visible threats.

  1% hit the infrastructure directly

  These are the ones the ISPs are really worried about.

Routers do get Directly Attacked



Routers do get Directly Attacked

- We knew back in the late ’90s that direct attack on routers were going to be one of the key Internet vulnerability points.
- The Feb 2000 DDOS attack provided Cisco to quietly shift into an accelerated path to allow routers to resist, compartmentize, and survive a direct attack.
- While there is nothing a router can do to mitigate a bandwidth saturation attack, the router should:

  Do Not Crash from the Saturation Attack (worse case CPU saturation with accessibility via console).

  Remain Accessible to the Operations Team

  Compartmentize the effects of the bandwidth saturation – allowing the other components of the router to remain functioning.

Terminology

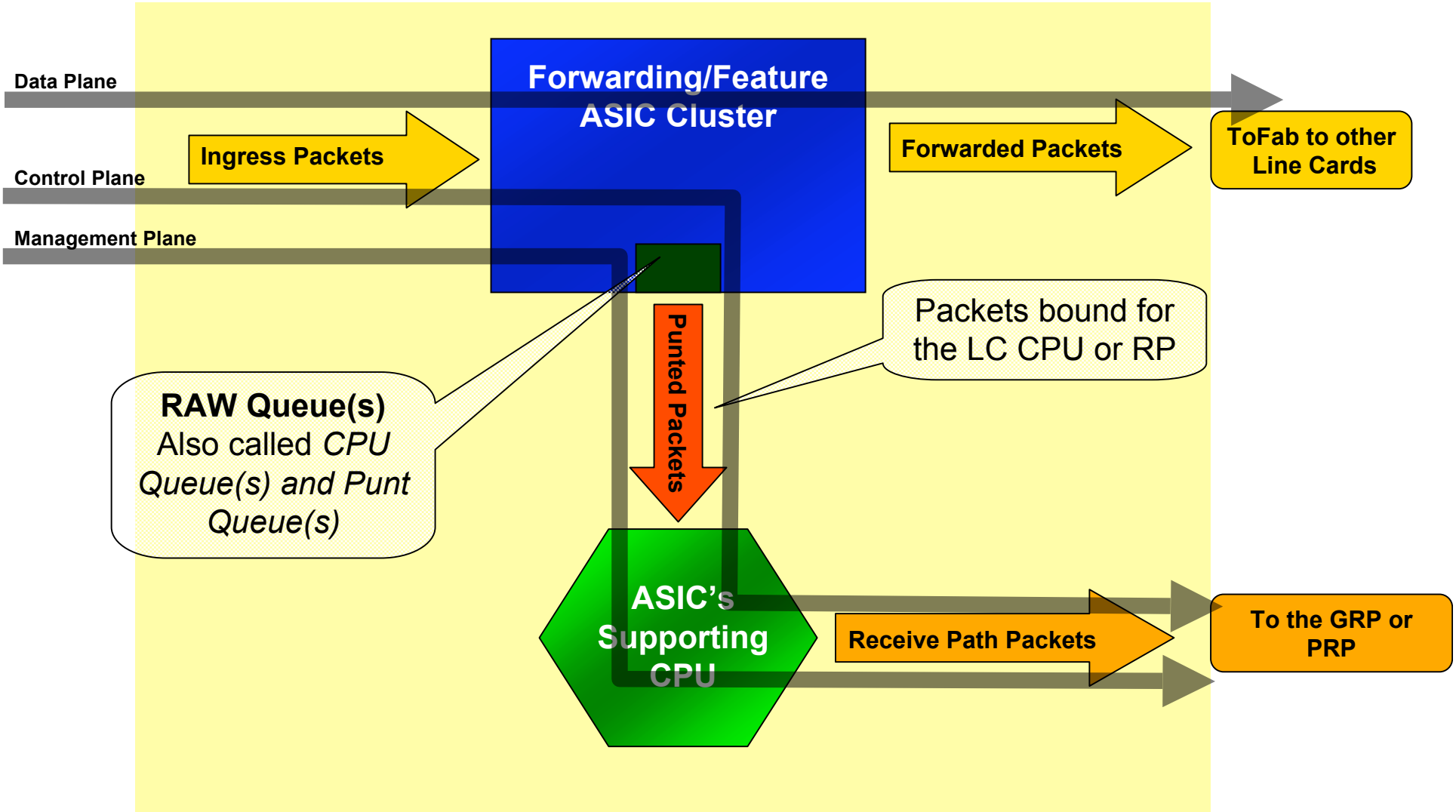
- **Three Plane Conceptual Model:**

Data Plane – Packets going through the router.

Control Plane – The routing protocols gluing the network together.

Management Plane – The tools and protocols used to manage the device.

The Three *Planes*



Simple Risk Assessment

- **Direct Attacks on the Router usually hits on three attack vectors:**

  Bandwidth Saturation (Data plane)

  Target the Control or Management Plane (Receive Path traffic on the Control and Management Plane)

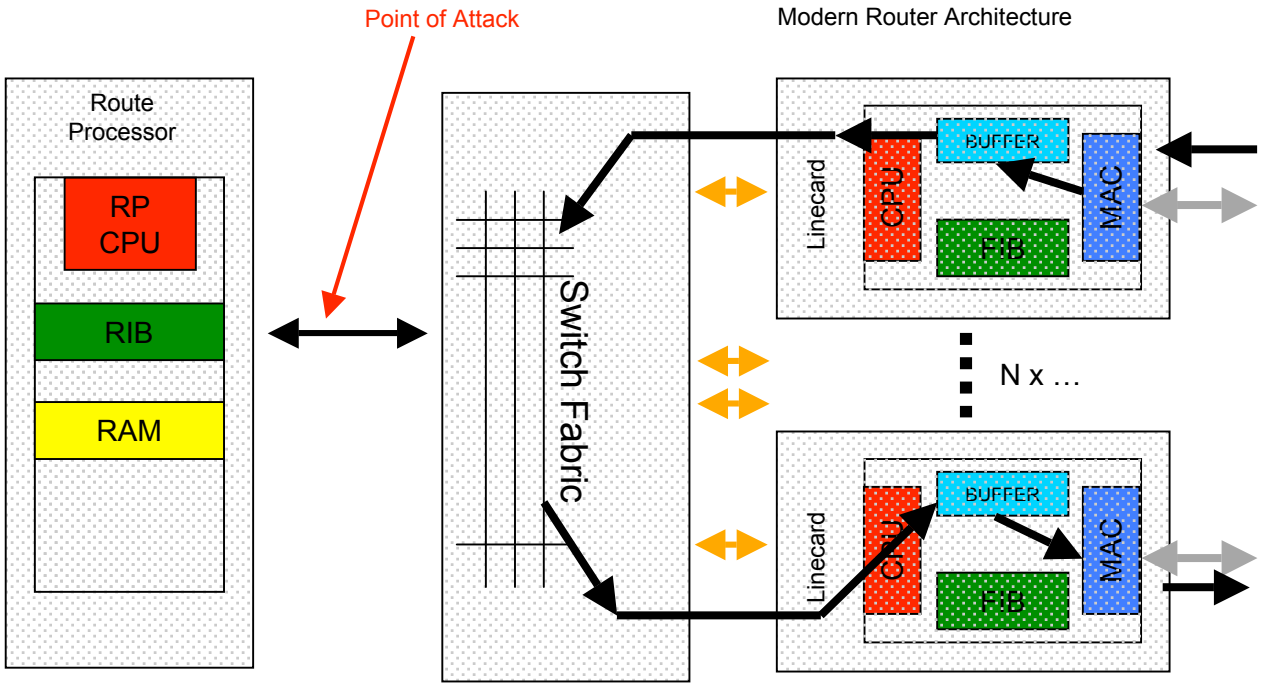
  Saturate the Punt path out of the forwarding/feature ASIC by abusing the TCP/IP standards (Data plane traffic that is punted from the forwarding/feature ASIC).

AOL's Public Security Campaign

- **Routers are optimized for traffic** through **the hardware**

  Not traffic for **the hardware**

- **What we really need is N x Line-rate decryptions (N = number of lines)**



Why does Barry call this *Not Enough*

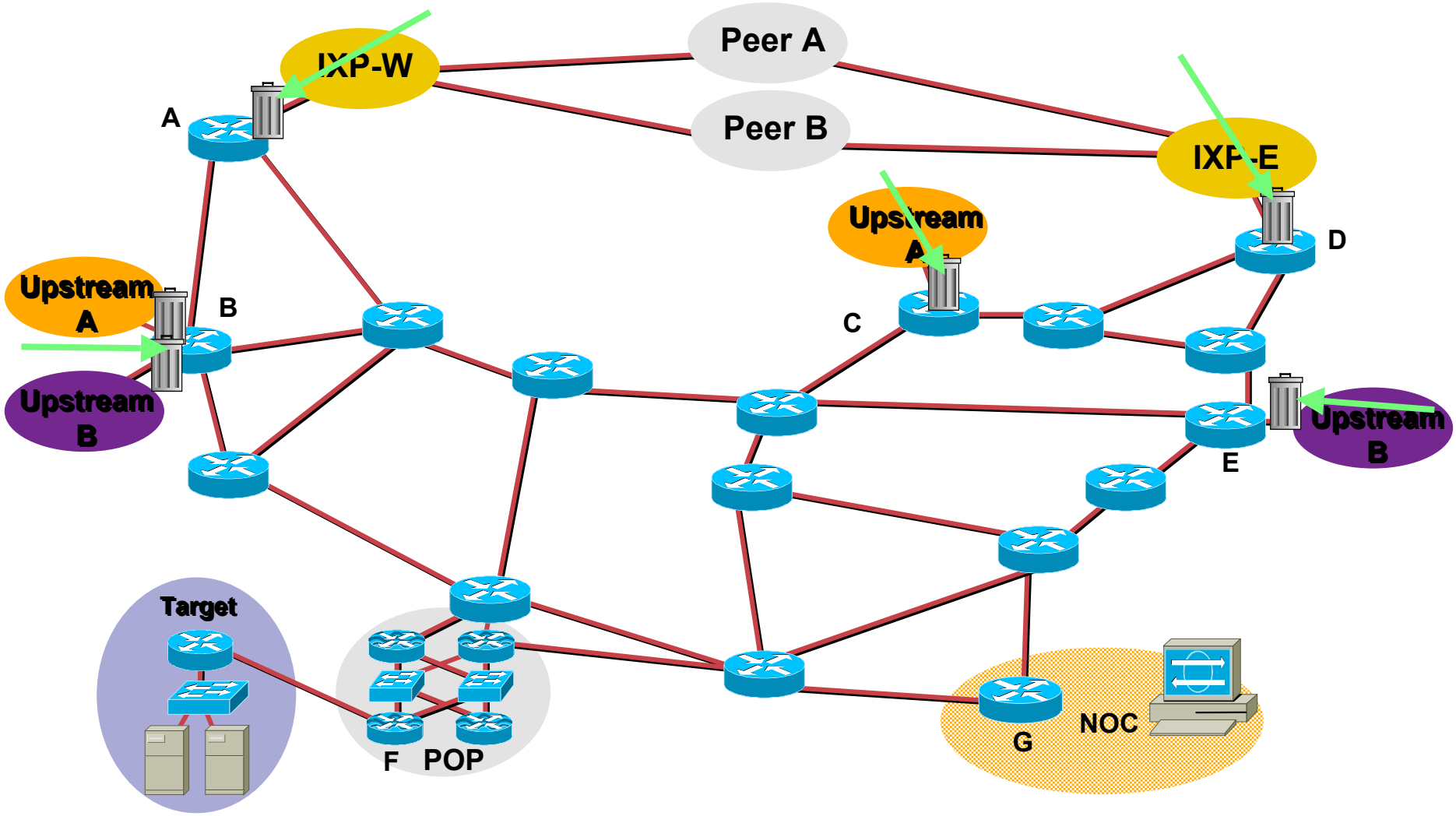
- **AOL uses traditional anti-spoof and infrastructure protection ACLs on their edge.**
  - **Hence, a wide range of attack vectors are eliminated.**
- **Cannot fixate on just eBGP peering traffic.**
  - **New attack vectors are being created every day!**
  - **History tells us that EVERY DEPLOYED DEFENCE TECHNIQE HAS BEEN BYPASSED, MARGINALIZE, AND DEFEATED.**
  - **Remember the Magnot Line!**

What is AOL doing?

- IP Address Plan tightly coupled with topology and routing. This allows for extremely efficient security rules.
- 2nd Generation Forward/Feature ASICs on their edge – allowing for data plane filters to protect their network infrastructure.

  Cisco 12XXX Engine 3 used on the edge.

2nd Generation ASICs allows for Infrastructure Packet Filtering on the Edge



Today's SP Security Techniques

Context

Objective

"All Big Networks (SPs, ASPs, ISPs, and other Big Networks) need to take action on the seven key security techniques. These security techniques are the core mitigation tools used to disrupt the mistreatment community."

Top Seven Items for the SP Security Community

- OPSEC Team in Every Major Network
- Mitigation Forums – It is all about Community
- iNOC-DBA Hotline
  (http://www.pch.net/inoc-dba/)
- Remote Triggered Black Hole Filtering
- Sink Holes
- Source Address Validation on all Customer traffic.
- BGP Prefix Filtering

Next Seven Techniques

- Receive Path ACL (and CPP)
- Back Scatter Trace Back
- Source Based Remote Triggered Black Hole Filtering
- Netflow Based Security Telemetry System
- BGP Policy Accounting
- Remote Triggered Rate Limiting
- BGP Community Filtering

You can make a difference …..

- ISPs and SPs can make a big difference in the security of the Internet.
- You can do that by preparing yourself and your network with the knowledge, tools, and techniques currently used to mitigate various Internet security issues.
- You do not have to be a expert – just someone willing to do their best to make something happen. Doing something is one step closer to operational confidence and deploy the mitigation techniques that make a difference.

Resources to Deploy when Ready

Cisco.com

- **SP/ISP/Big Network Public Archives**

  ftp://ftp-eng.cisco.com/cons/isp/security/

  www.ispbook.com

- **On-Line Bootcamp**

  http://palomar.getitmm.com/bootcamp/

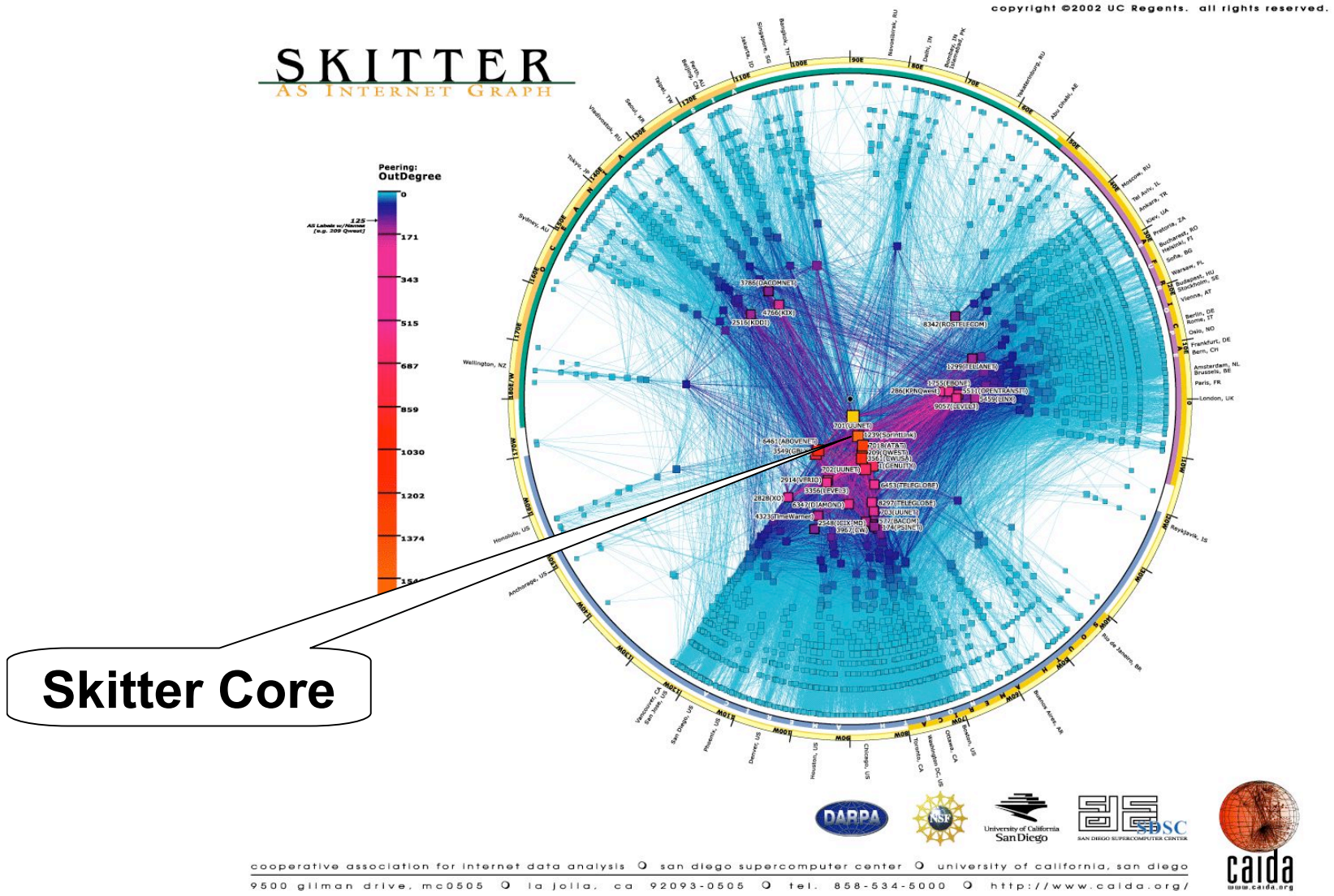
- **NANOG Security Curriculum**

  http://www.nanog.org/ispsecurity.html

Will these really make a difference?

- YES!
- They made a all the difference during Slammer.
- The Skitter Core all points to NSP-SEC and the iNOC Hotline as the key forum that classified, characterized, and contained the Slammer Worm.

What is the *Skitter Core?*



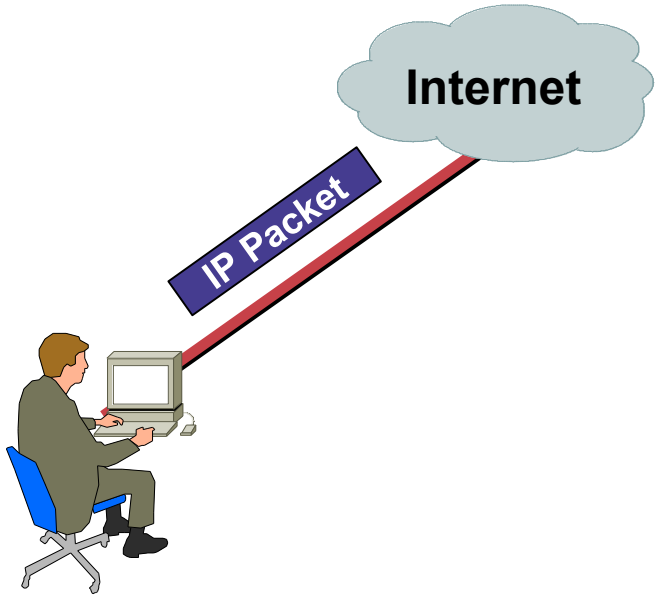
Skitter Core

CAIDA is a program of the University of California's San Diego Supercomputer Center (UCSD/SDSC)
skitter is supported by DARPA NGI Cooperative Agreement N66001-98-2-8922, NSF ANIR Grant NCR-9711092 and CAIDA members

Laws of the Internet Drive SP Security

“There are key laws of the Internet whose influences operators cannot escape. These laws drive SP Security, the design of security into the network, and how SP’s OPSEC Teams respond to Security incidents.”

Core Law: It is all about the packet ……



- It is all about the packet …..
- Once a packet gets into the Internet, someone, somewhere has to do one of two things:

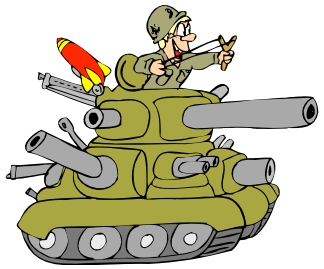
  Deliver the Packet

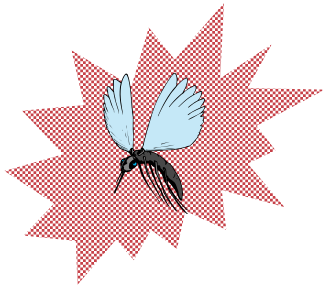
  Drop the Packet

- In the context of a DOS attack, the question is *who* and *where* will that drop that packet.

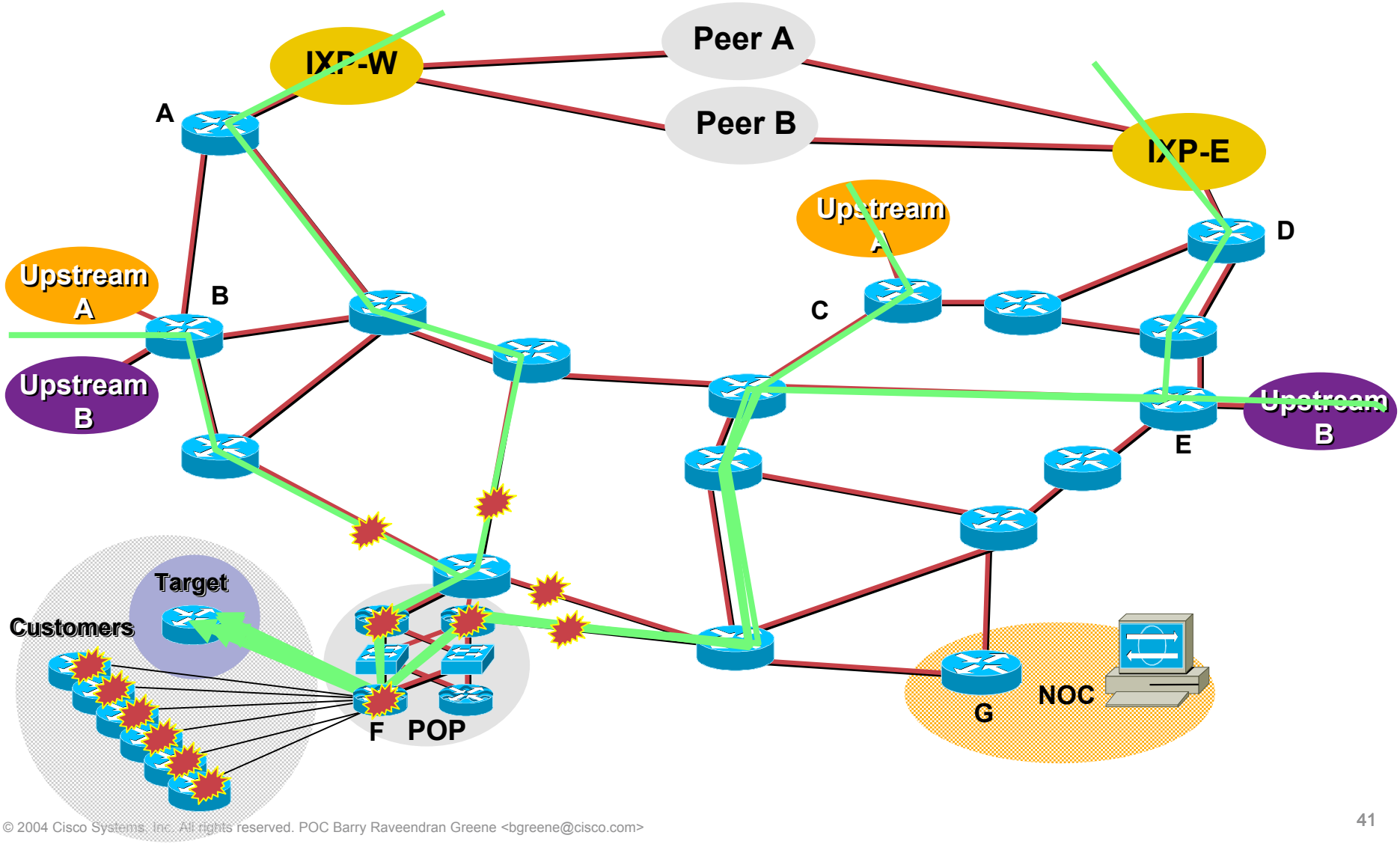
What is Co-Lateral Damage?

- 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.

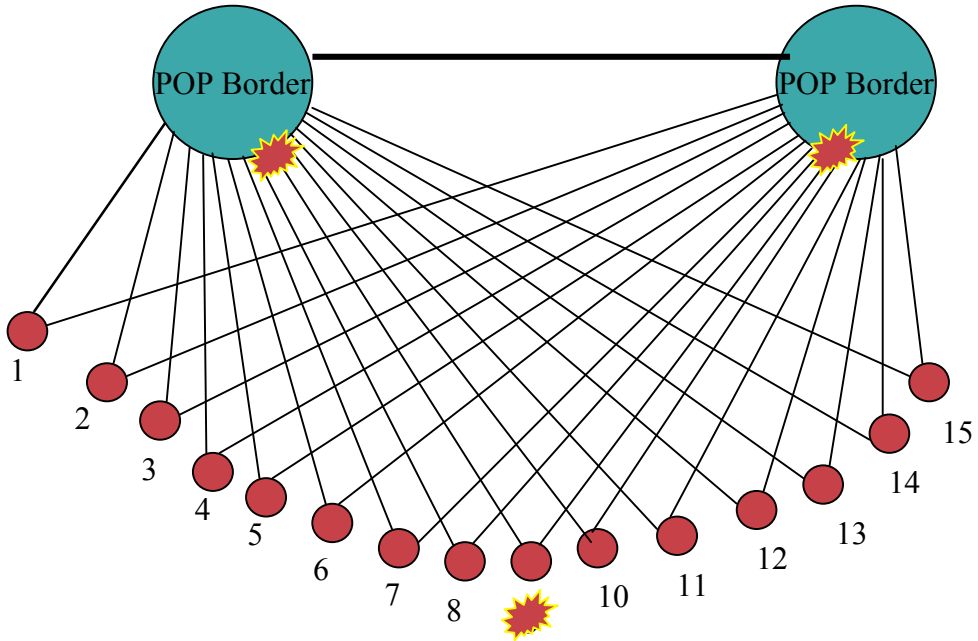


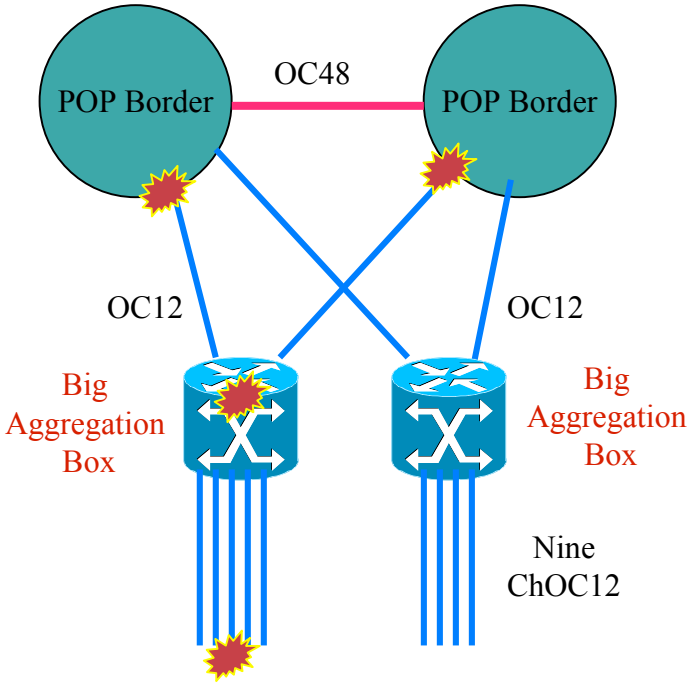


What is Co-Lateral Damage?



Increased Risk from Co-Lateral Damage



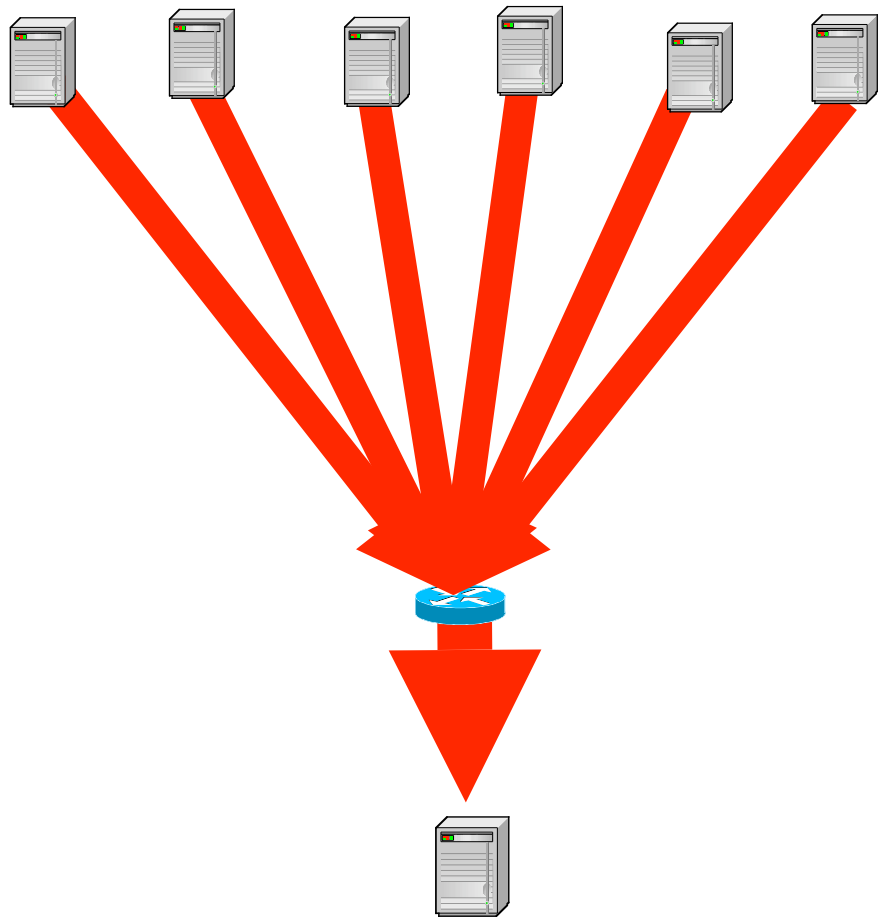


Lots of Aggregations Routers with 10s to 100s of customers per router.

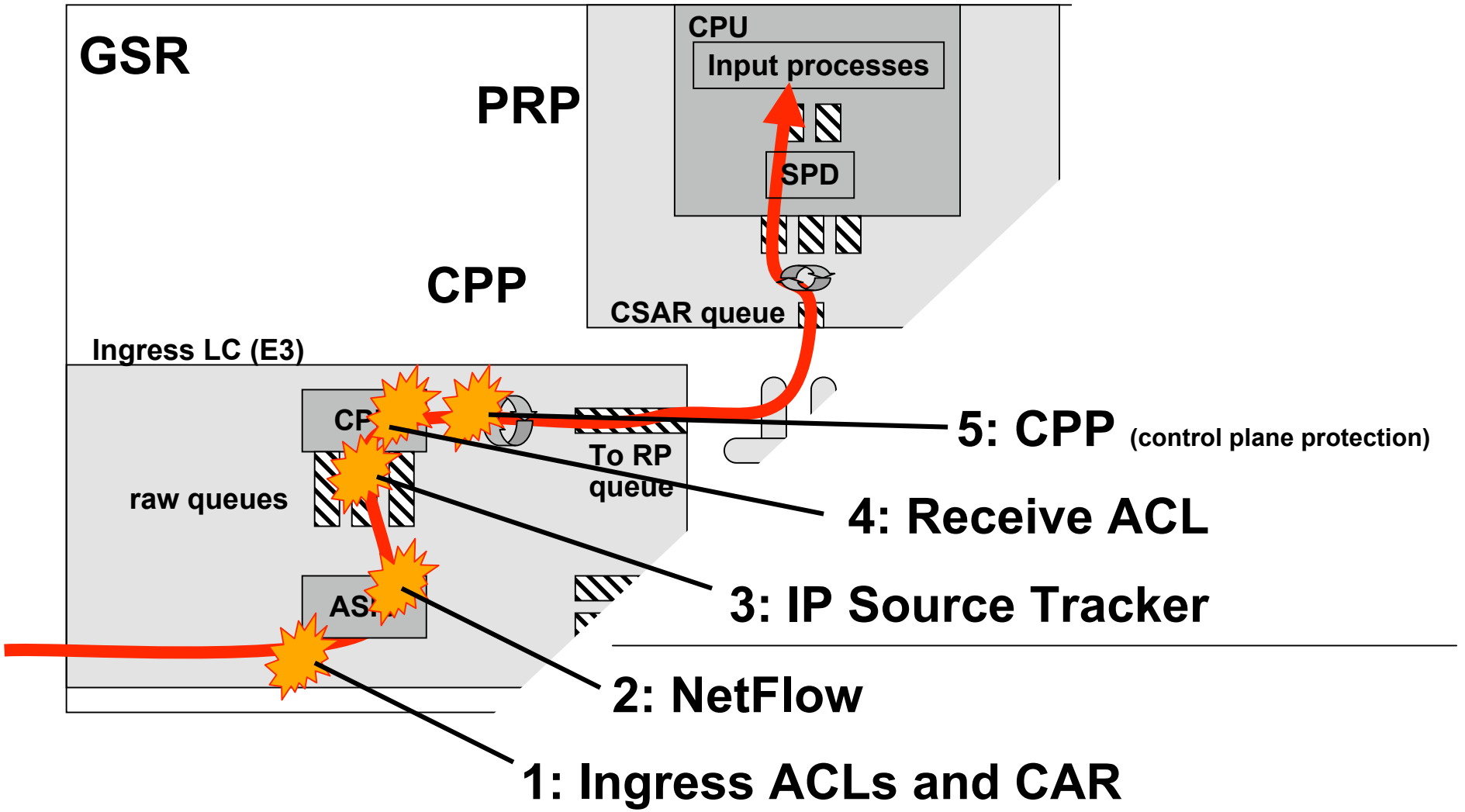
Few Aggregations Routers with 100s to 1000s of customers per router.

Who drops the packet when ……..

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

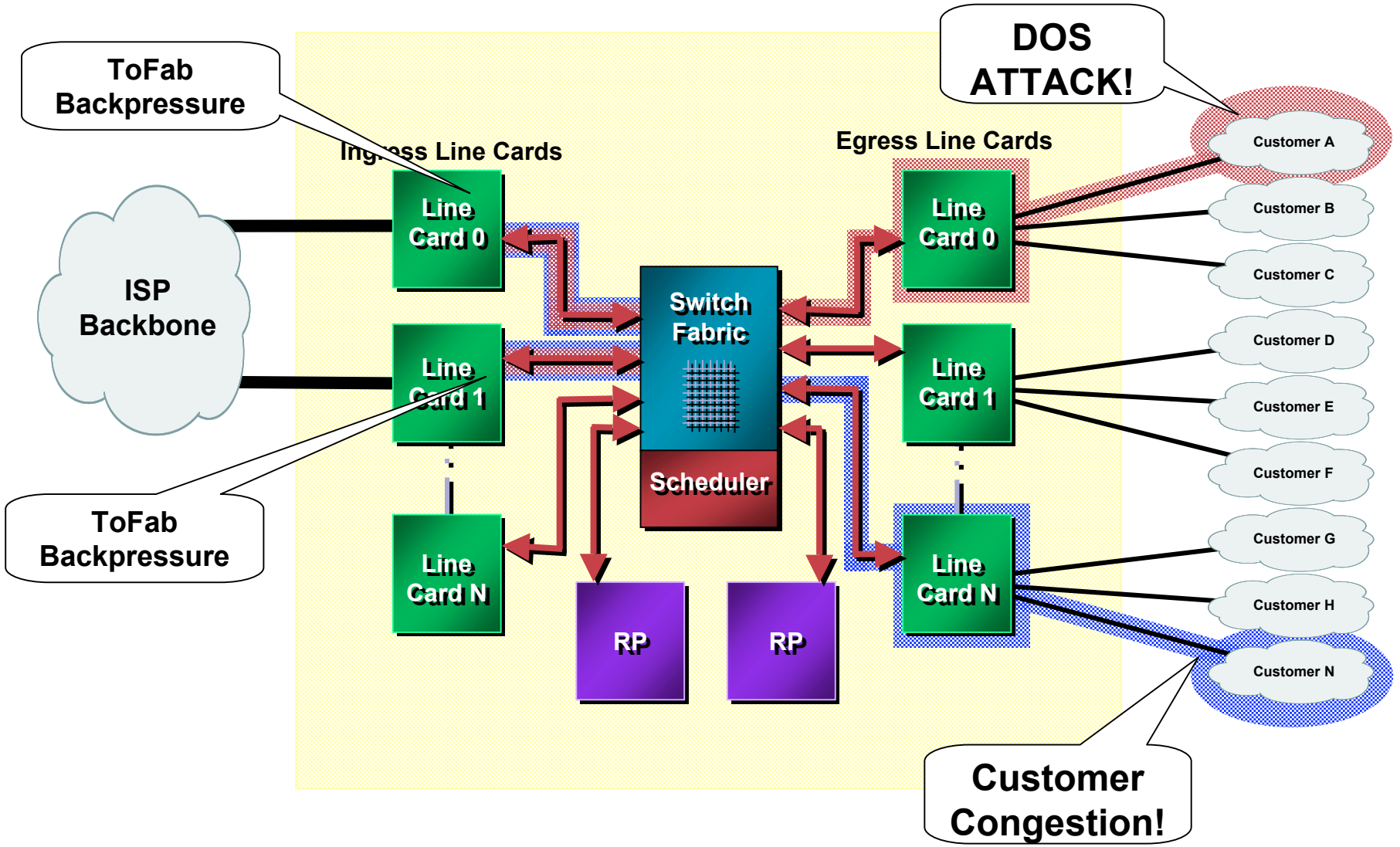


Co-Lateral Damage in the Router

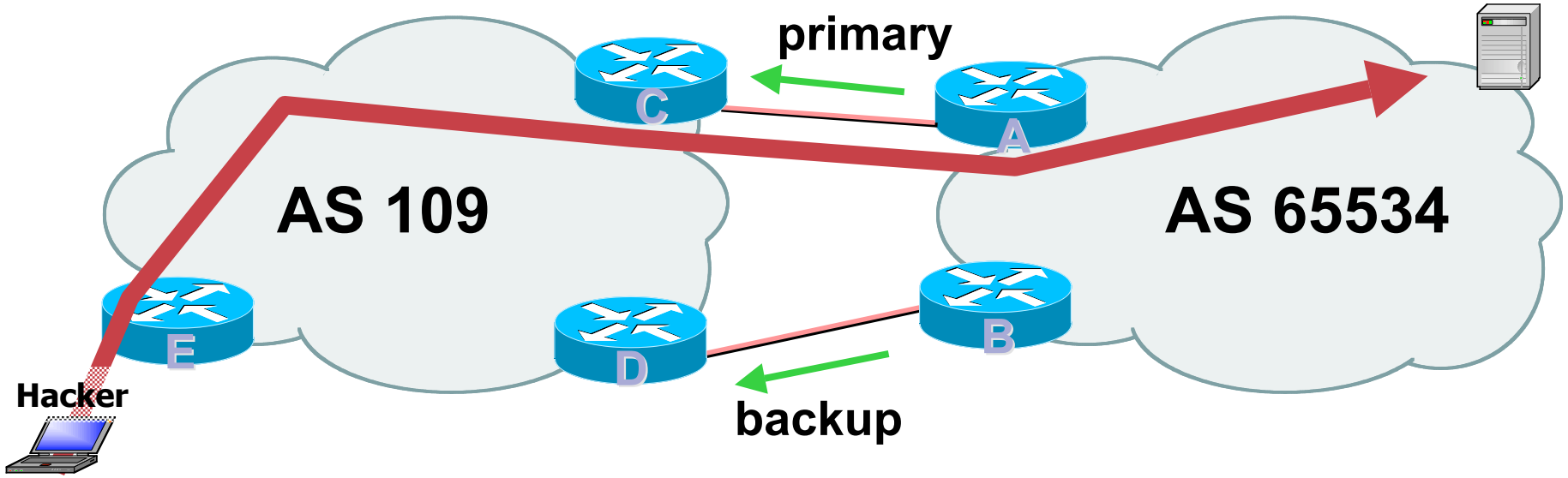


Fabric Congestion Effects on Router

Cisco.com

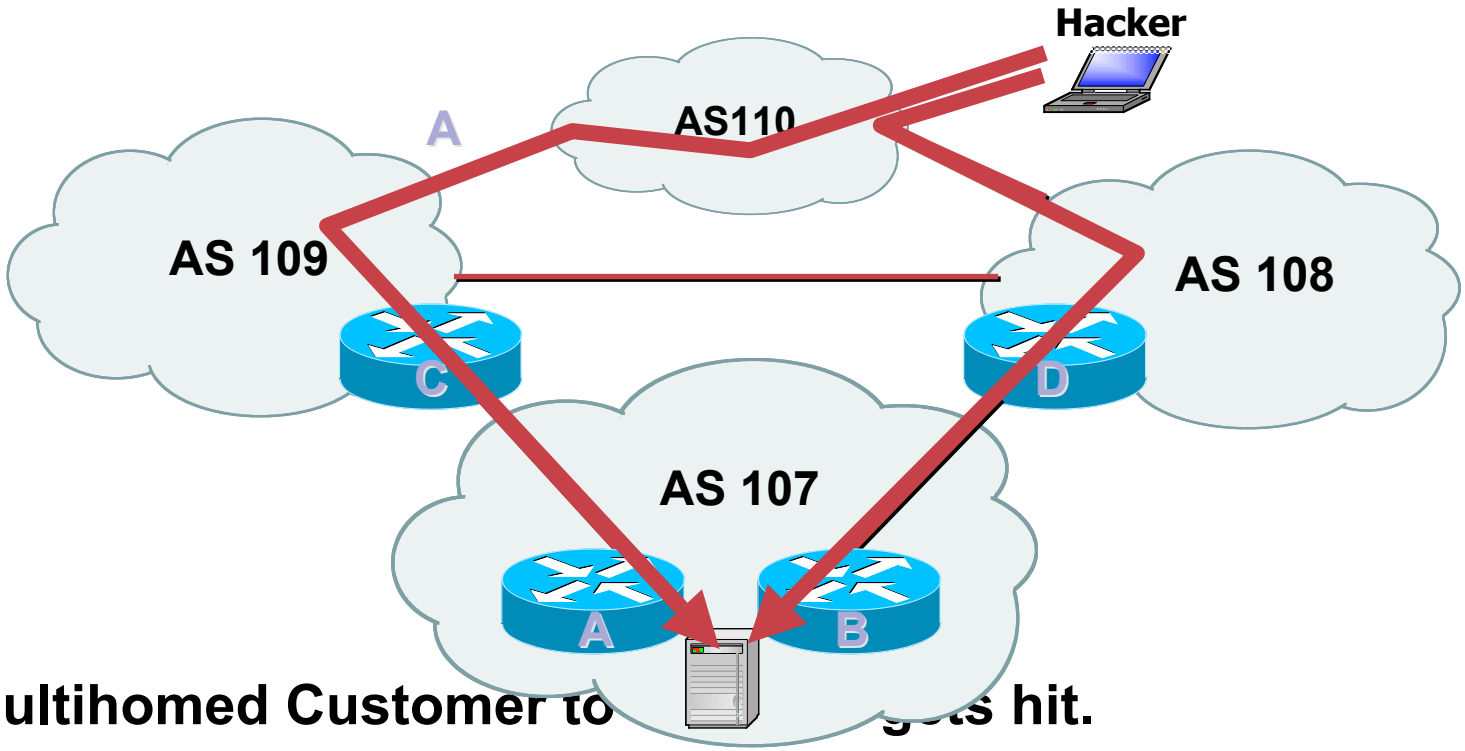


Who drops the packet when ……..



- **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?**

Who drops the packet when ……..



- **Multihomed Customer to … gets hit.**

  Line saturates, BGP drops, attack shifts OR attack aggregates!

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.

Which ones are about dropping?

- OPSEC Team in Every Major Network
- ✓Mitigation Forums – It is all about Community
- iNOC-DBA Hotline (http://www.pch.net/inoc-dba/)
- ✓Remote Triggered Black Hole Filtering
- ✓Sink Holes
- ✓Source Address Validation on all Customer traffic.
- BGP Prefix Filtering

Which ones are about dropping?

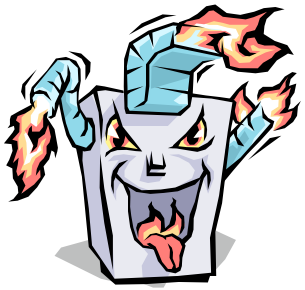
Cisco.com

- ✓ Receive Path ACL (and CPP)
- Back Scatter Trace Back
- ✓ Source Based Remote Triggered Black Hole Filtering
- Netflow Based Security Telemetry System
- BGP Policy Accounting
- ✓ Remote Triggered Rate Limiting
- BGP Community Filtering

Operational Security (OPSEC) Teams

Where are the Operations Security Teams?

- **The problem - Most Network Operation Centers (NOCs):**
  - **Do not have security plans**
  - **Do not have security procedures**
  - **Do not train in the tools or procedures**
  - **OJT (on the job training)—learn as it happens**

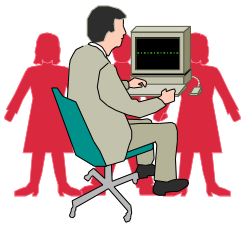


Operational Security Teams are Critical

- **It is imperative that an network's OPSEC team prepare.**
  - **Contacts for all ISPs who you inter-connect (peers, customers, and upstreams)**
  - **Contacts for all vendor's product security reaction teams.**
  - **Document your policies. Will you help your customers? Will you classify the attacks? Will you traceback the attacks? Will you drop the attacks on your infrastructure?**

Example of Team Preparation

- **Red Team/Blue Team exercises**
  - **Divide up into two teams — one defends, one attacks**
  - **Referee assigns the attackers with an objective (get this file, deface the web site, take down the target, etc.)**
  - **Defenders use network/system designs and tools/procedures to defend the target**
  - **One of the most effective ways to get your staff into the depths of TCP/IP, OS, applications, and security**



What can you do?

- Understand that a ISP Security Team is essential to their business.
- Most provider's operations is naked and exposed to the future incidents which are going to happen.
- We will have another Turbo Worm – perhaps worse than Nimda, Code Red, and Slammer.
- Are your prepared?

HOMEWORK

- Does someone in your network have an OPSEC responsibility?
- If you do not have an OPSEC Team, build one fast.

Peers working together to battle Attacks to the Net

Four Forums to Start ….

- Operators Meetings
- Local CERT Meetings
- DSHIELD
- NSP-SEC

Local Operators Meetings

- **NANOG**

  www.nanog.org

- **RIPE**

  www.ripe.net

- **APRICOT**

  www.apricot.net

- **SANOG**

  www.sanog.org

- **NZNOG**

Etc: http://www.nanog.org/orgs.html

Local CERTs

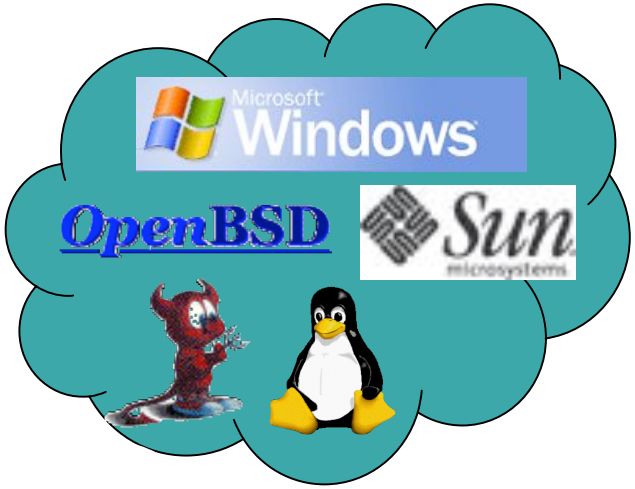
- **FIRST and CERT Teams should be having local meetings.**
- **www.first.org for list of FIRST/CERT Teams.**

DSHIELD – Distributed IDS

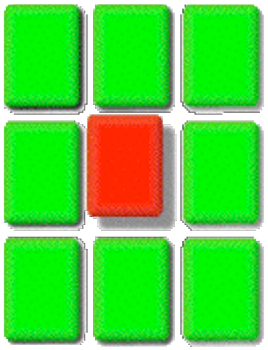
Data Collection

Analysis

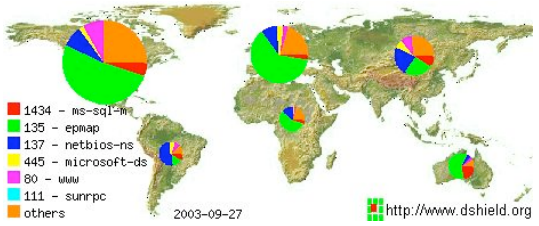
Dissemination



DShield Users



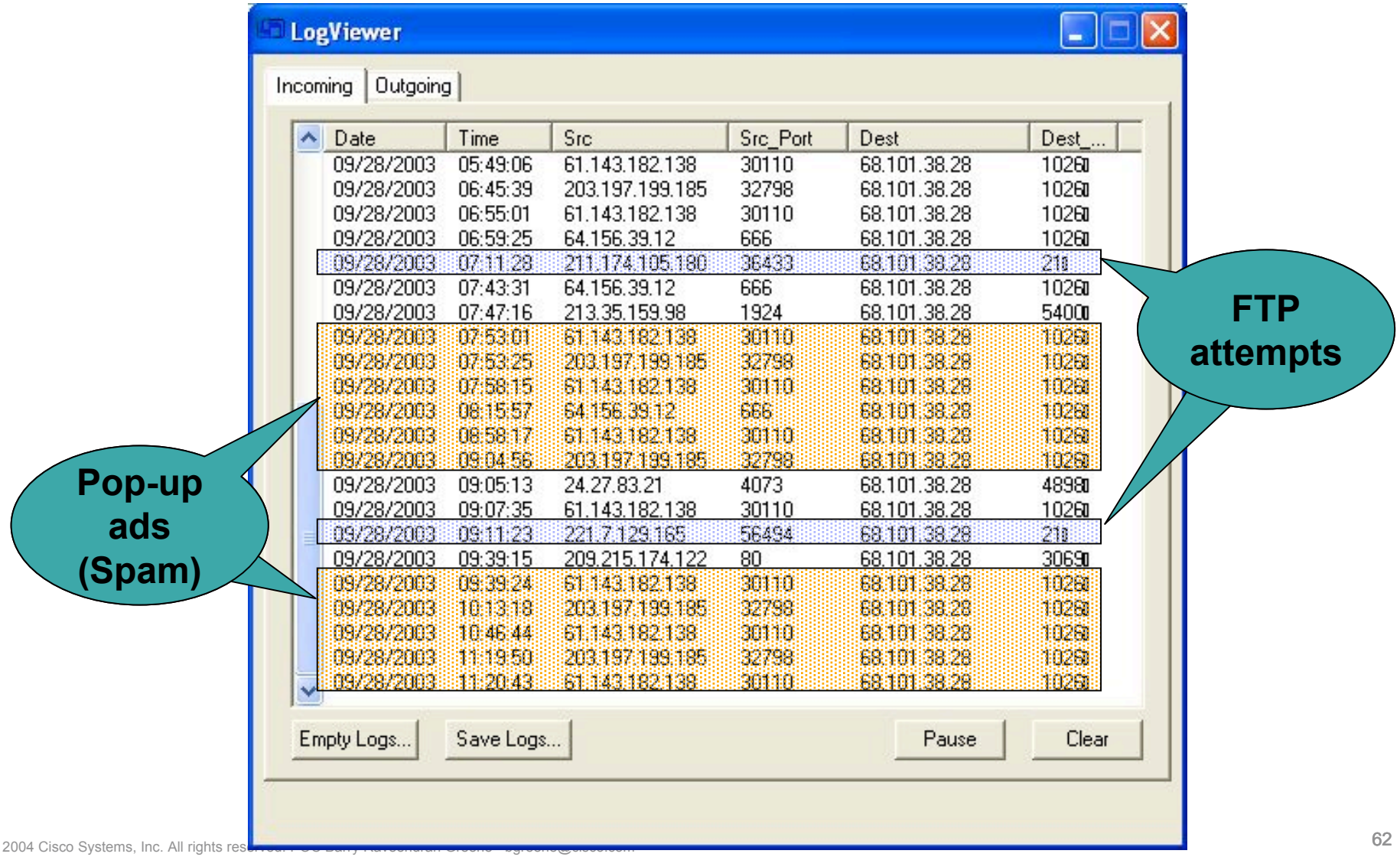
DShield.org



Top 10 Ports

Service Name	Port Number	30 day history	Explanation
ms-sql-m	1434		Microsoft-SQL-Monitor
epmap	135		DCE endpoint resolution
microsoft-ds	445		Win2k+ Server Message Block
netbios-ns	137		NETBIOS Name Service
www	80		World Wide Web HTTP
sunrpc	111		portmapper rpcbind
ssh	22		SSH Remote Login Protocol
netbios-ssn	139		NETBIOS Session Service
https	443		HTTP protocol over TLS SSL
ms-sql-s	1433		Microsoft-SQL-Server

Typical Residential Cable Modem Log



NSP-SEC

- NSP-SEC – Closed Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC: Daily DDOS Mitigation Work

I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.

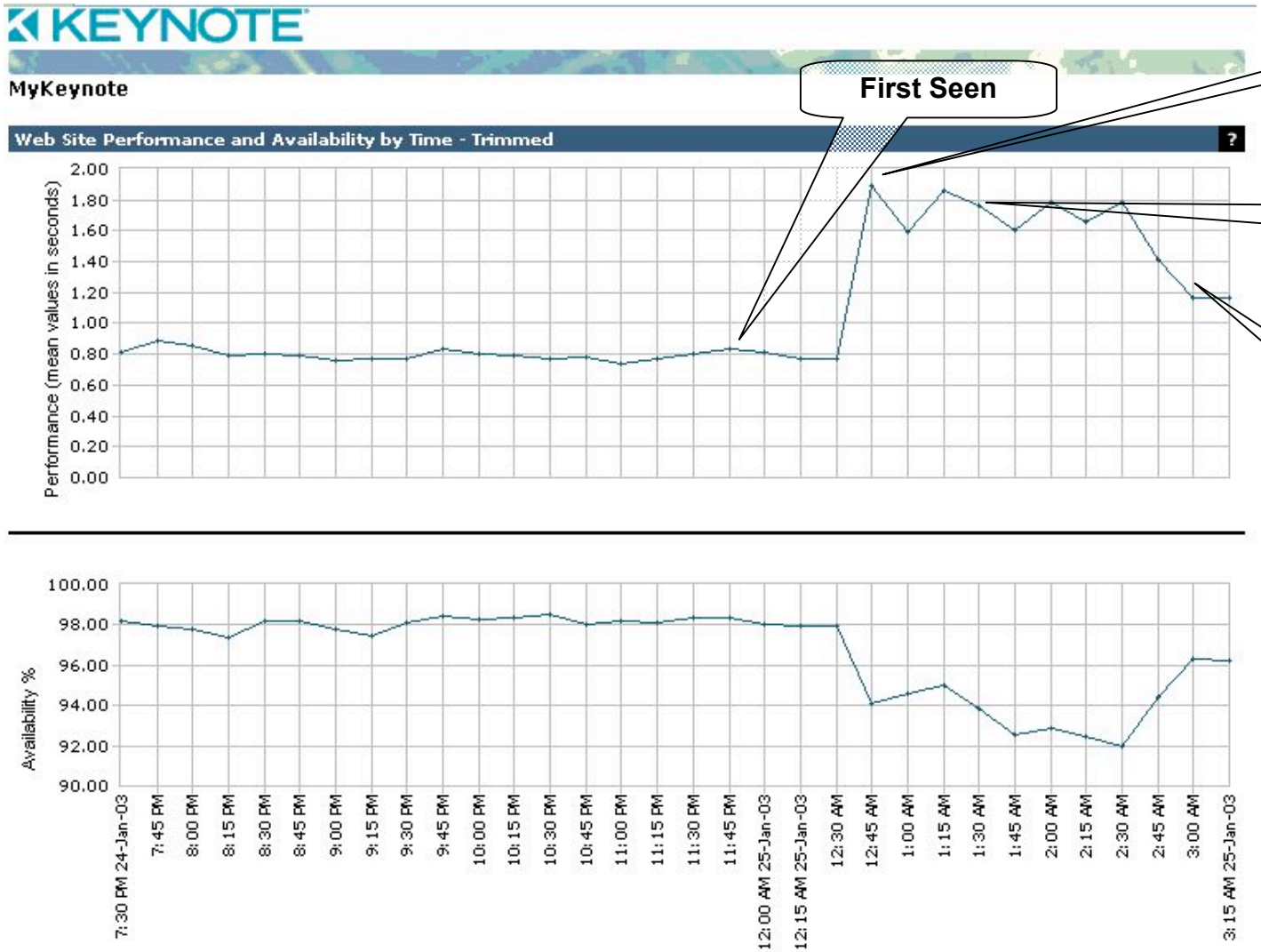
Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.

I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

NSP-SEC's Role during Slammer

- The ISPs were the first to notice something was happening.
  - Circuits saturated, routers spiking, BGP sessions flapped, and customers complained.
- NSP-SEC was the first reporter of the worm. CERT/FIRST Teams got their alert from NSP-SEC.
- NSP-SEC members were the ones who dump the packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm.

Impact of NSP-SEC's Containment



First Seen

Real Impact

Containment Starts

Containment Takes Effect

4:00 a.m. PST Containment

In the Skitter Core

NSP-SEC-DISCUSS

- **NSP-SEC is where the mitigation takes place. You do not learn anything, you are already expected to know.**
- **NSP-SEC-DISCUSS is the place to learn, consult, work on new mitigation techniques, and lurk (if you want to).**

http://puck.nether.net/mailman/listinfo/nsp-security-discuss

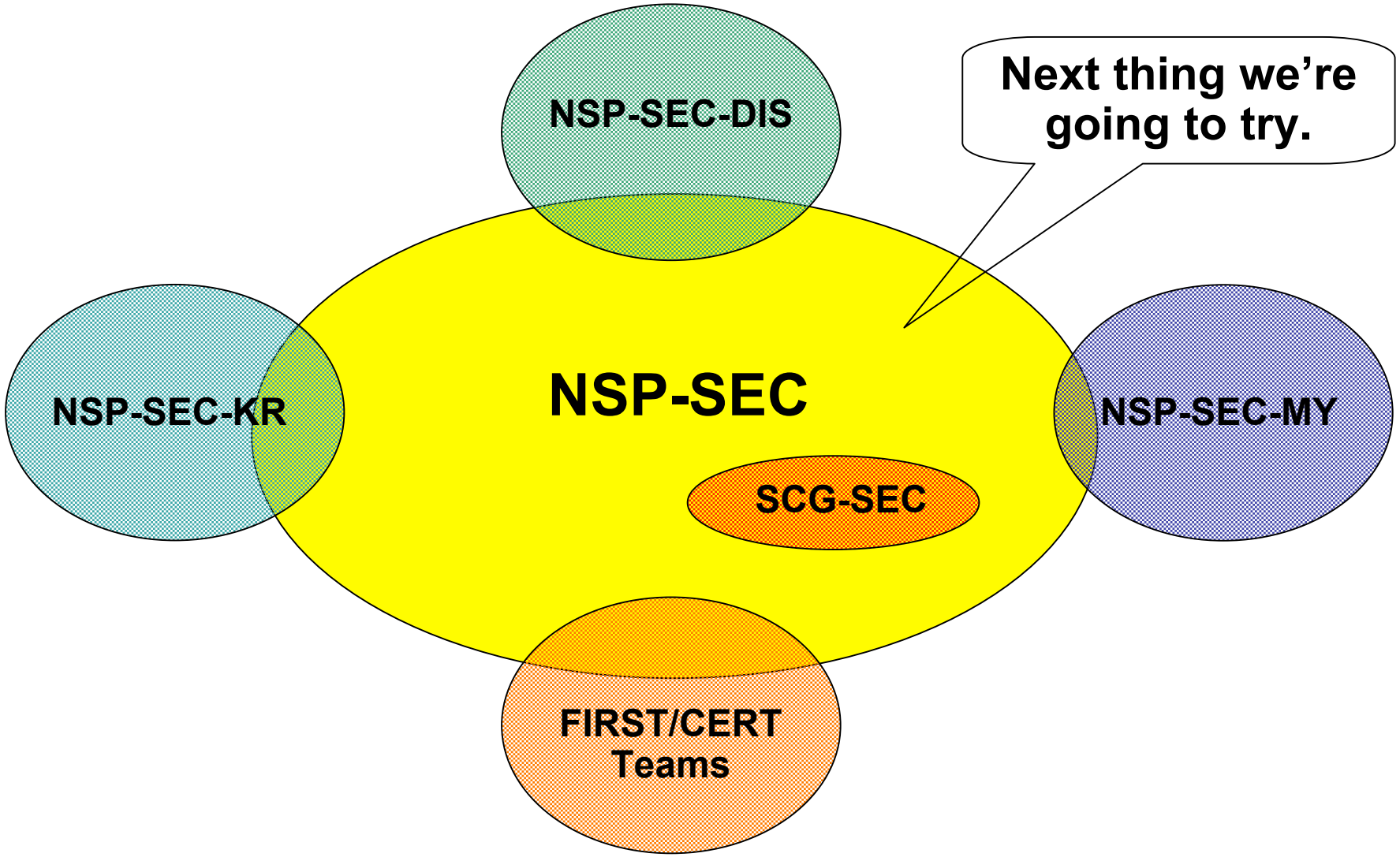
What can you do to help?

- If you configure routers, are in operations, and handle ISP Security, then apply for nsp-sec membership:

  http://puck.nether.net/mailman/listinfo/nsp-security

- NSP-SEC is looking for two or three engineers from each ISP who has the authority to configure routers and handle security incidents.

NSP-SEC – Community Spheres



HOMEWORK

- If you qualify, start the NSP-SEC application process.
- Ask your local CERT to organize meetings.
- Find a way to have a local NOG started – even if it is the NZNOG style.

iNOC Phone: The next wave of inter-NOC Communication

What is the problem?

- ISPs needed to talk to each other in the middle of the attack.
- Top Engineers inside ISPs often do not pick up the phone and/or screen calls so they can get work done. If the line is an outside line, they do not pick up.
- Potential solution – create a dedicated NOC Hotline system. When the *NOC Hotline* rings, you know it is one of the NOC Engineer's peers.

iNOC DBA Hotline

- **INOC-DBA: *Inter-NOC Dial-by-ASN***
- **The iNOC Hotline was used to get directly to their peers.**
- **Numbering system based on the Internet:**

  ASnumber:phone

  109:100 is Barry's house.
- **SIP Based VoIP system, managed by www.pch.net, and sponsored by Cisco.**

How to Participate

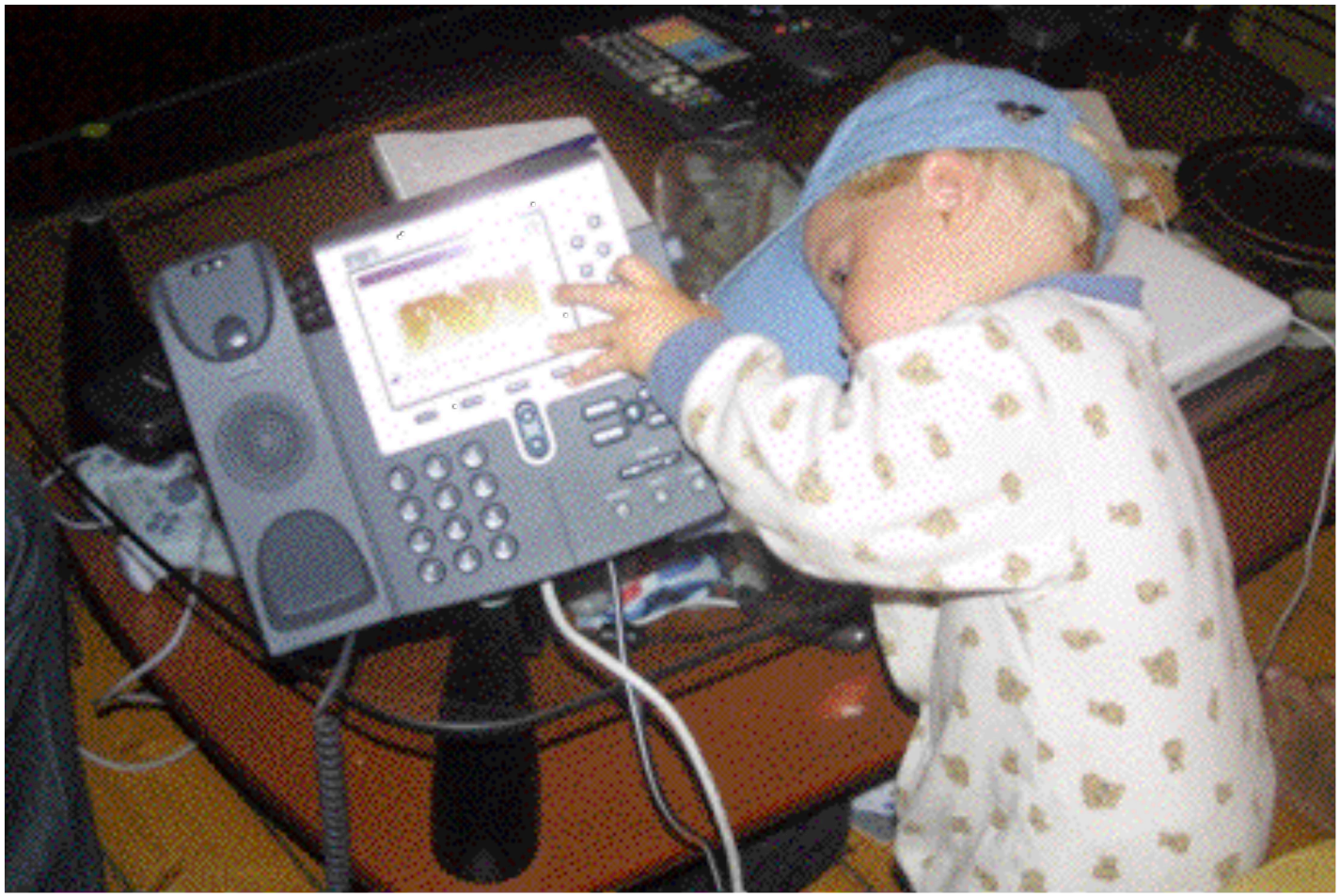
- **With your own phones:**

  PCH needs your MAC address, contact info, ASNs, and extension number.

- **With PCH phones from:**

  PCH need your contact and shipping address, ASNs, and extension number.

Is set up difficult?



How is iNOC being used today?

- Used during attacks like Slammer (Barry was using his iNOC phone at home to talk to ISPs in the early hours of Slammer).
- D-GIX in Stockholm bought 60 phones for their members (ISP's around Stockholm)
- People have started carrying around their SIP phones when traveling
- Many DNS Root Servers are using the iNOC Hotline for their phone communication.
- General Engineering consultation – ISP Engineers working on inter-ISP issues.

More Information

- General information:
  http://www.pch.net/inoc-dba/
- Mailing-list archive:
  http://www.pch.net/resources/discussion/inoc-dba/archive/

Who's participating:
http://www.pch.net/inoc-dba/directory/

Exchanges		Carriers		Associations	
LINX	SD-NAP	UUnet	AT&T	ARIN	
PAIX	LAIIX	Sprint	SBC	APNIC	
Equinix	NSP-IXP2		C&W	AOL/T-WRIPE/NCC	
AMS-IX	NOTA	Genuity	RCN	ICANN	
MAEs	OIX	Verio/NTT		TDS	ISC

What can you do to help?

- **Get a SIP Phone and join the iNOC Hotline system.**
  - **Two for each engineer – one in the office – one at home.**
  - **Slip in phone during the next sales cycle.**

HOMEWORK

- Get a SIP Based phone and sign up to the iNOC-DBA

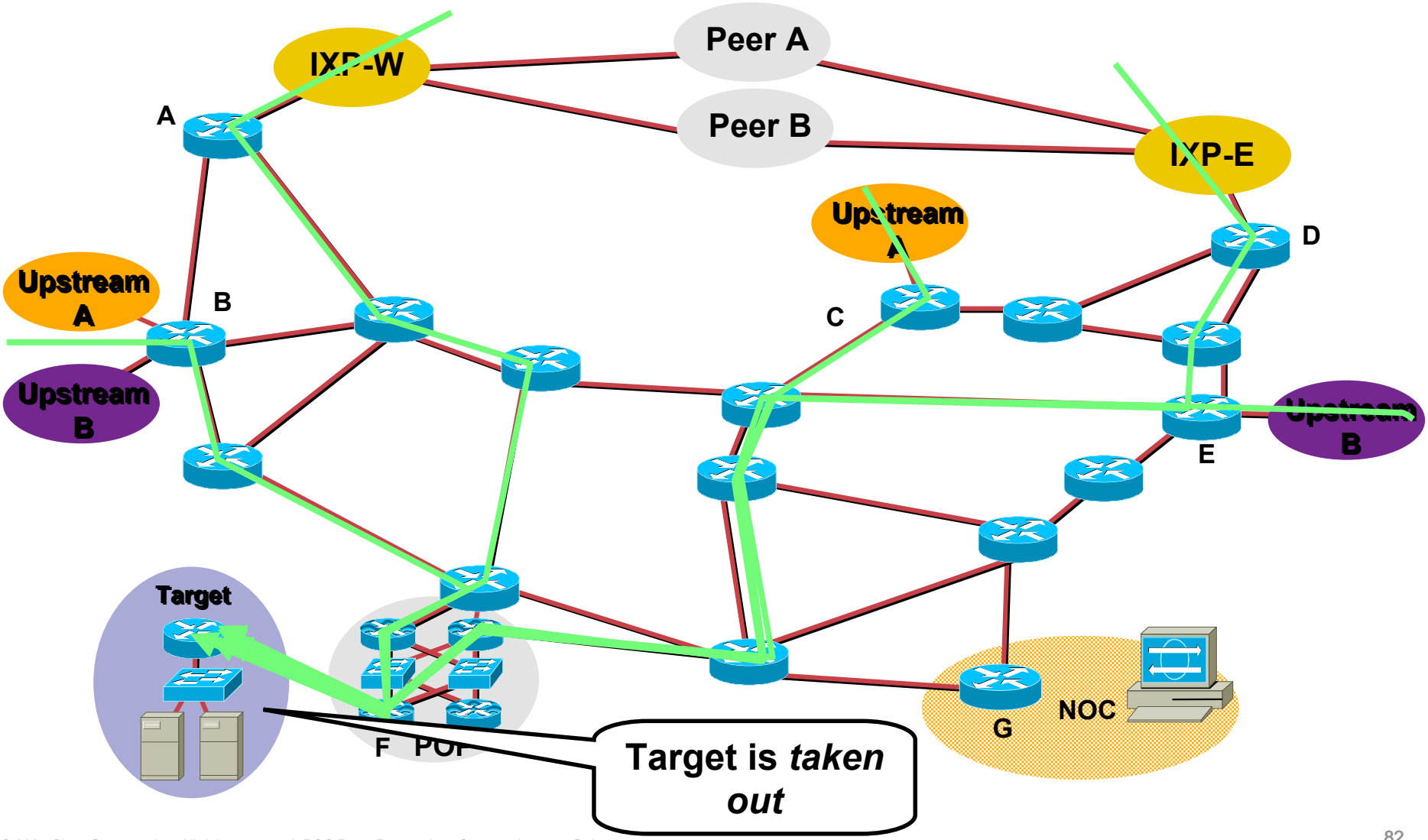
Technique: Remote Triggered Black Hole Filtering

Remotely Triggered Black Hole Filtering

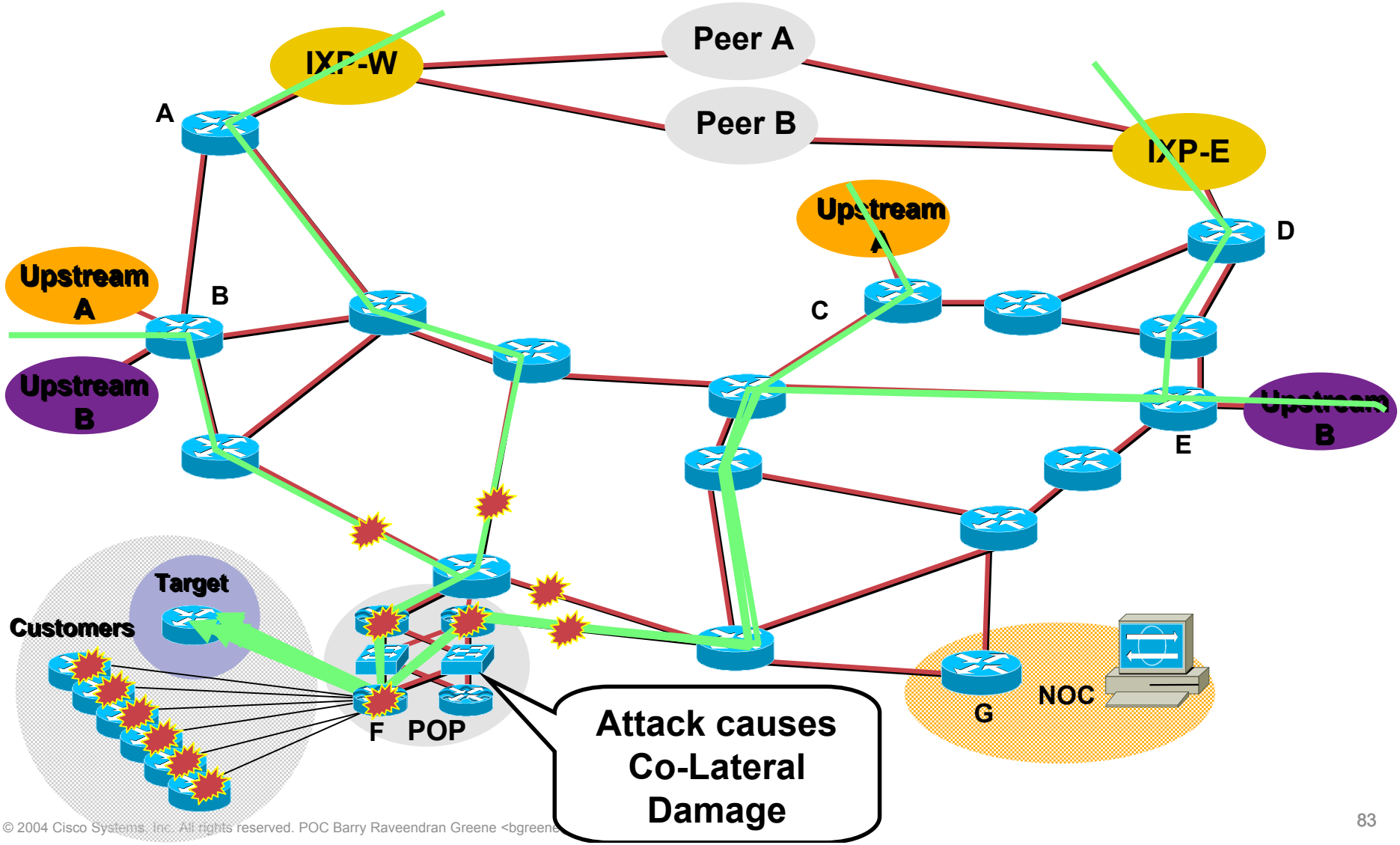
Cisco.com

- We use BGP to trigger a network wide response to a range of attack flows.
- 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.

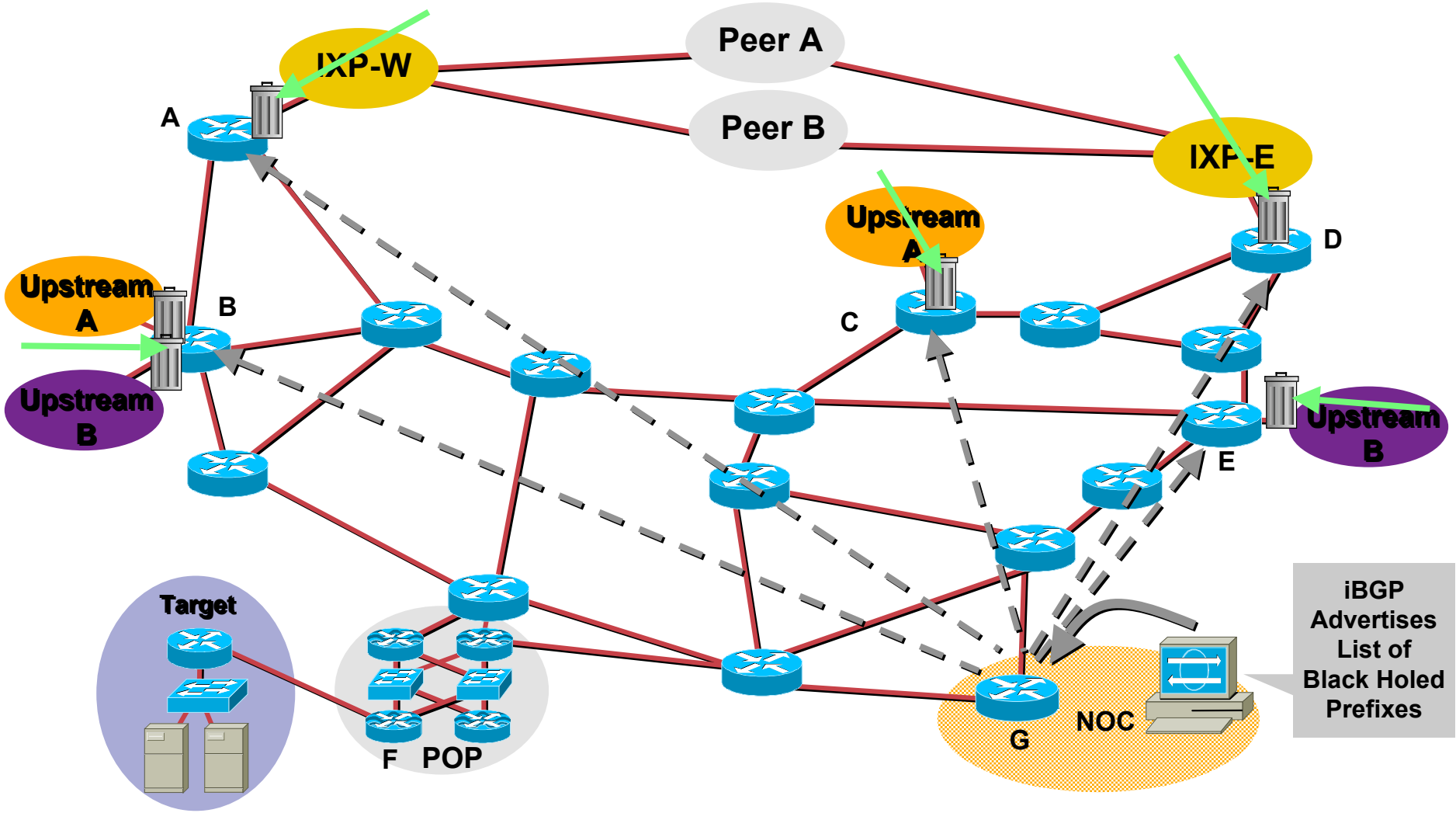
Customer is DOSed – Before



Customer is DOSed – Before – Co-Lateral Damage



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

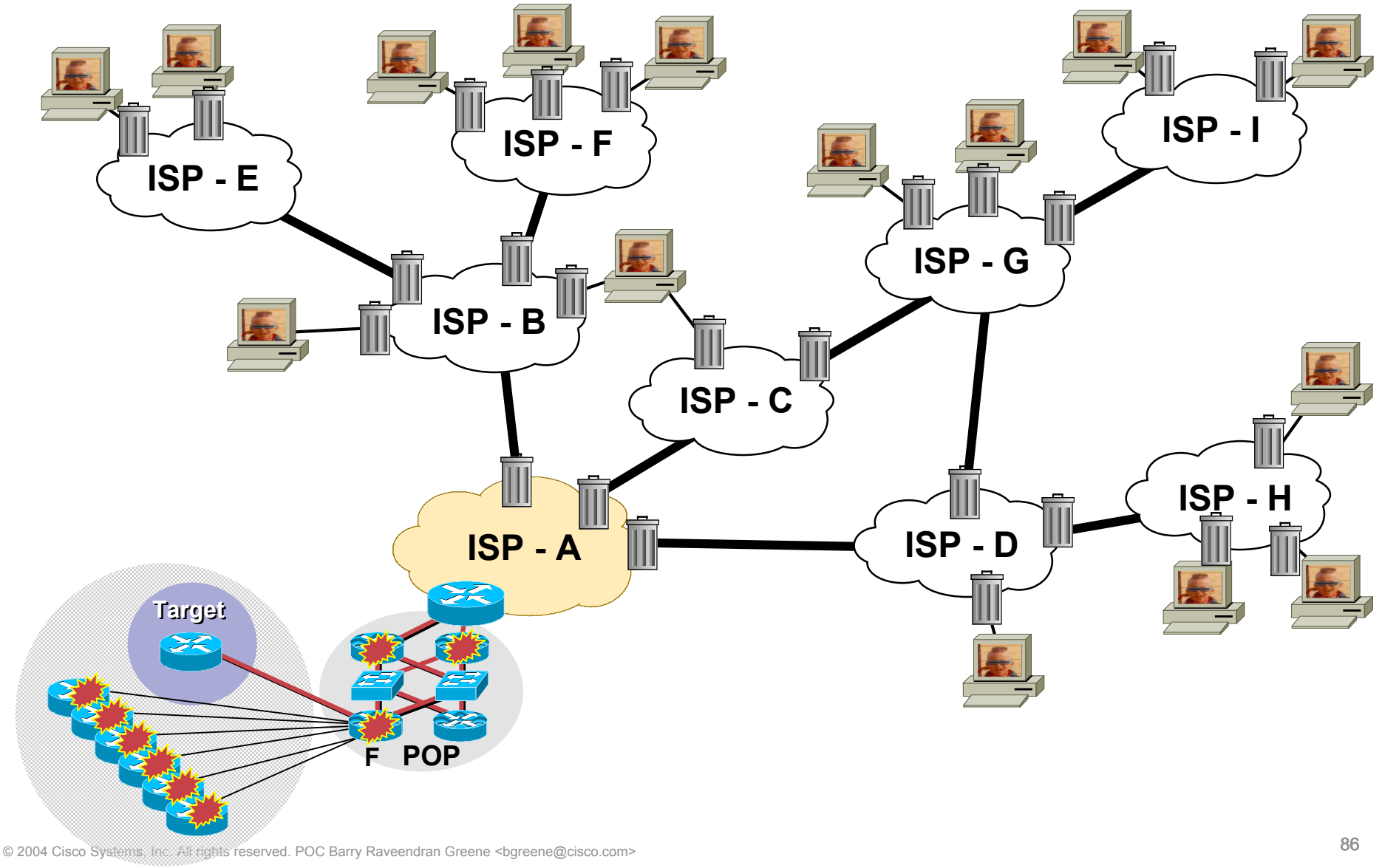


Remote Triggered Black Hole

- 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 to an ISP's *security toolkit.*

Inter-Provider Mitigation

Cisco.com



What can you do to help?

- **Remote Triggered Black Hole Filtering is the most common ISP DOS/DDOS mitigation tool.**
- **Prepare your network:**

  ftp://ftp-eng.cisco.com/cons/isp/essentials/ **(has whitepaper)**

  ftp://ftp-eng.cisco.com/cons/isp/security/ **(has PDF Presentations)**

  NANOG Tutorial:

  http://www.nanog.org/mtg-0110/greene.html **(has public VOD with UUNET)**

HOMEWORK

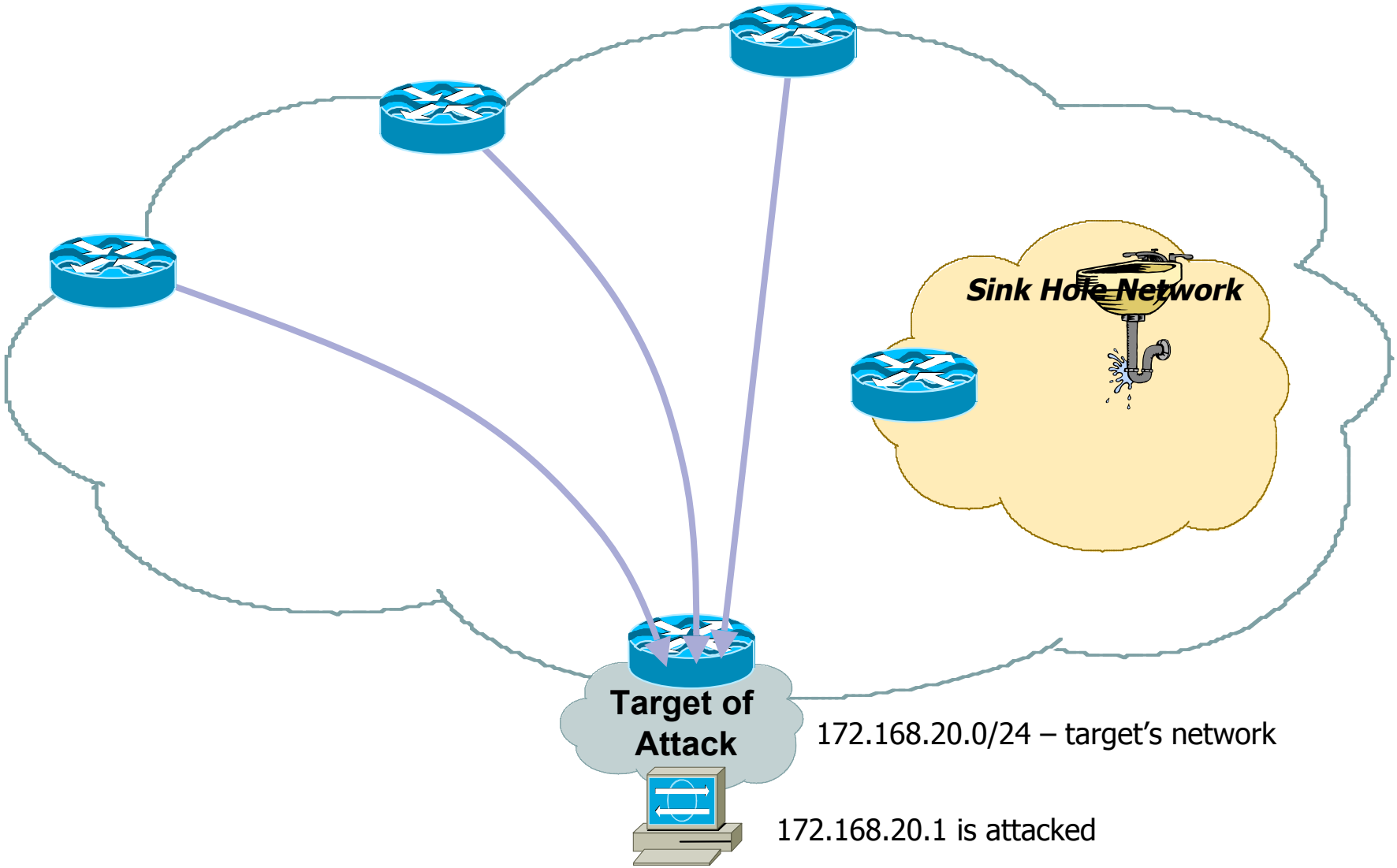
- Deploy the basics for RTBH – A static trigger to Null 0 for all your devices.
- Develop a BGP Community base plan for RTBH.

Technique: Sink Holes

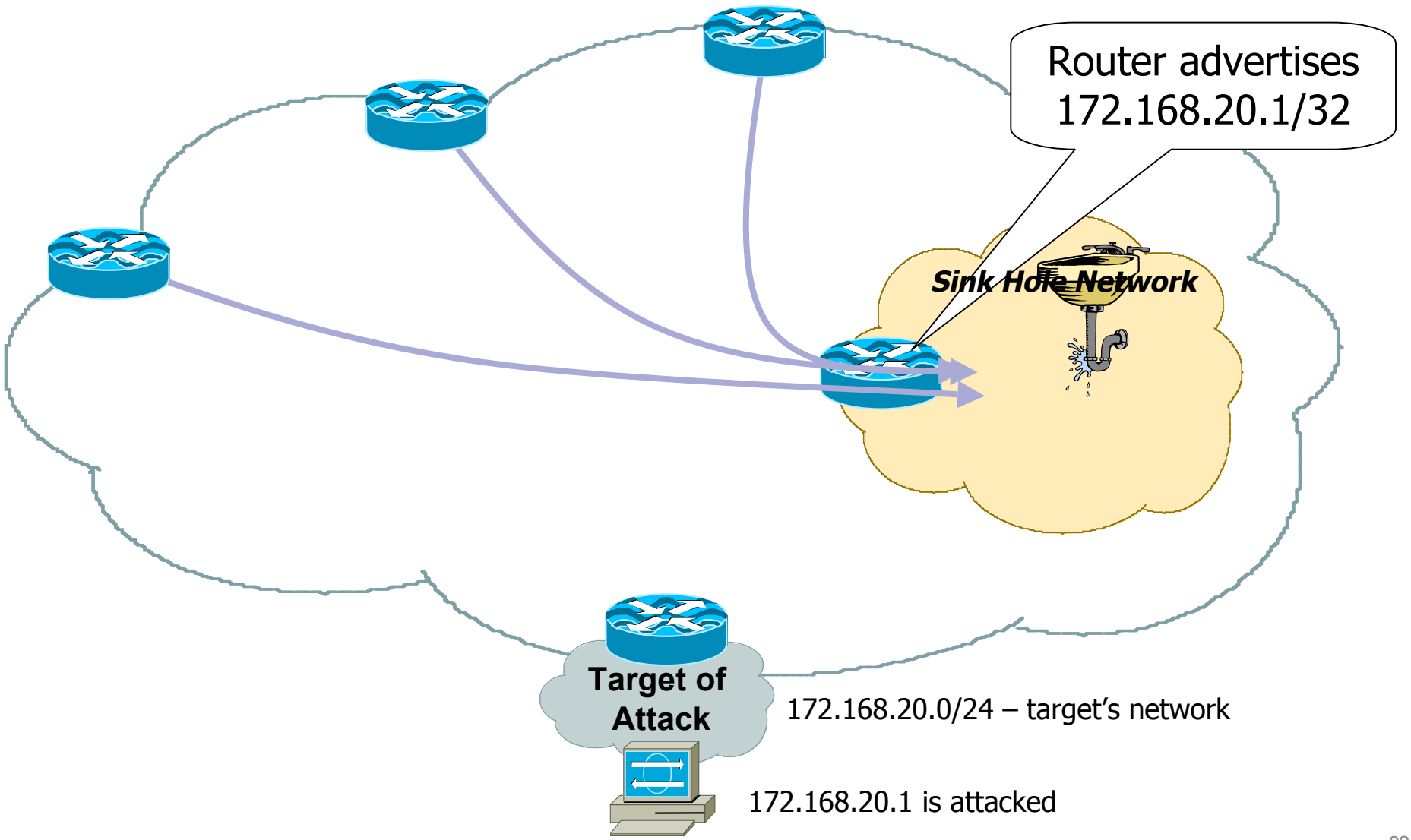
Sink Hole Routers/Networks

- **Sink Holes are a *Swiss Army Knife* security tool.**
  - **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)**

Sink Hole Routers/Networks

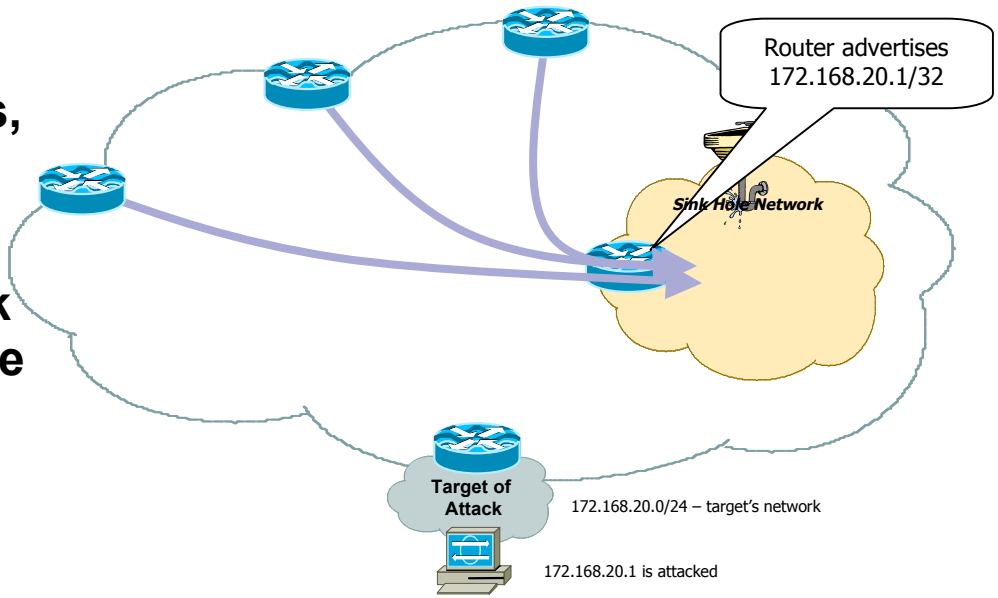


Sink Hole Routers/Networks



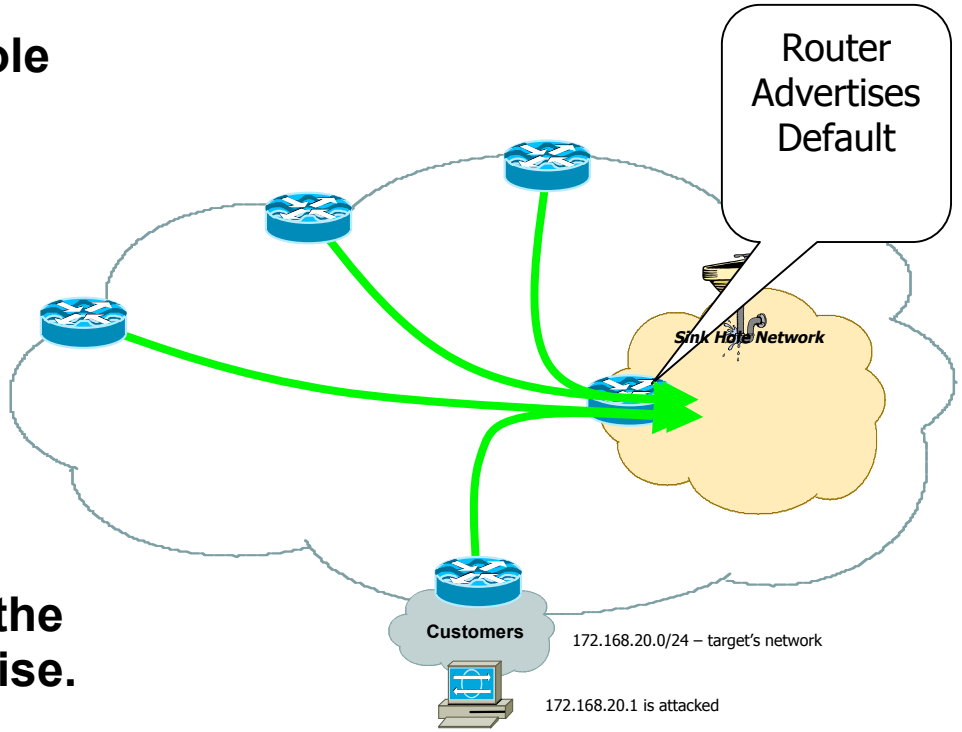
Sink Hole Routers/Networks

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

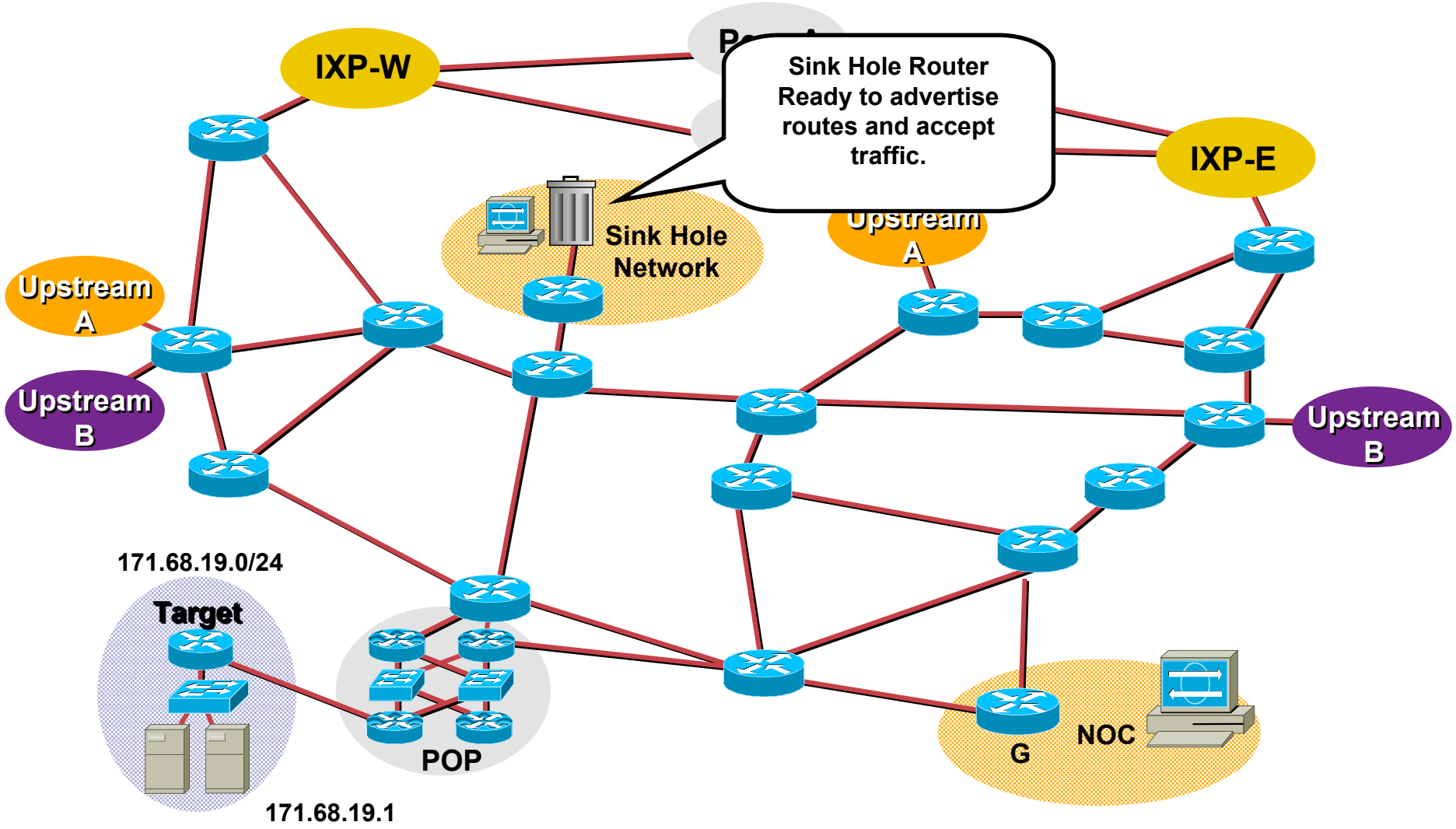


Sink Hole Routers/Networks

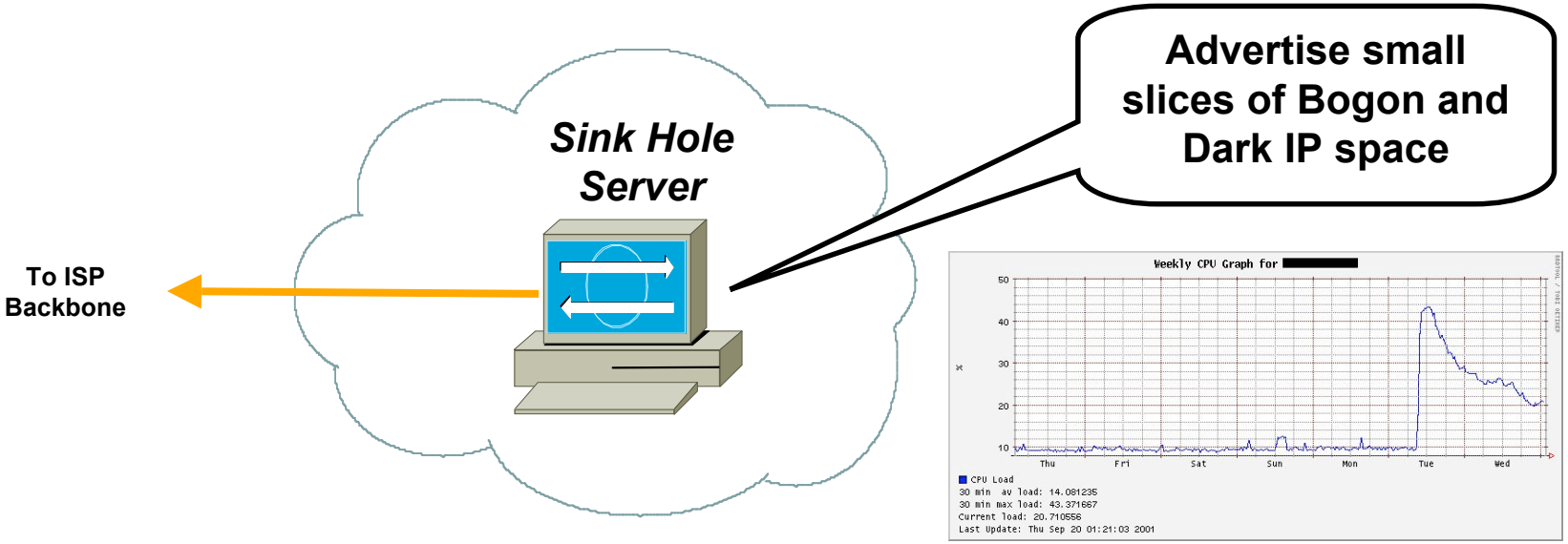
- **Advertising Default from the Sink Hole will pull down all sort of *junk* traffic.**
  - **Customer Traffic when circuits flap.**
  - **Network Scans**
  - **Failed Attacks**
  - **Code Red/NIMDA**
  - **Backscatter**
- **Can place tracking tools and IDA in the Sink Hole network to monitor the noise.**



Sink Hole Routers/Networks

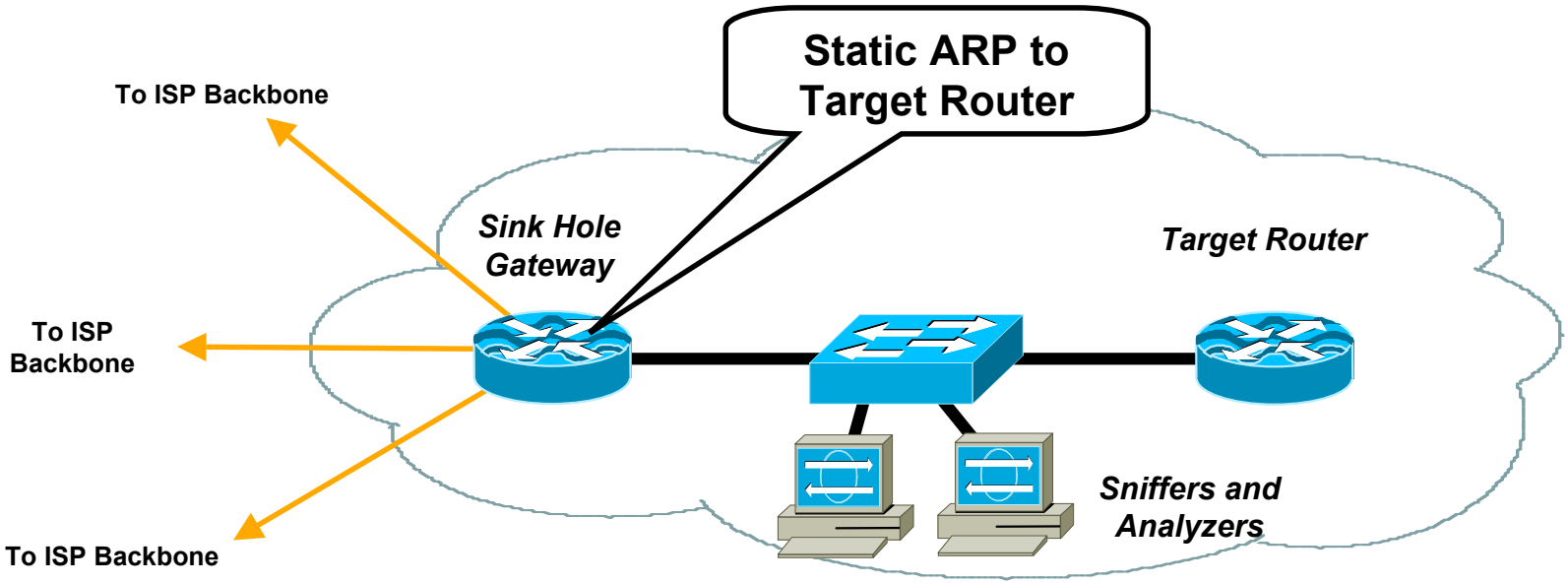


The Basic Sink Hole



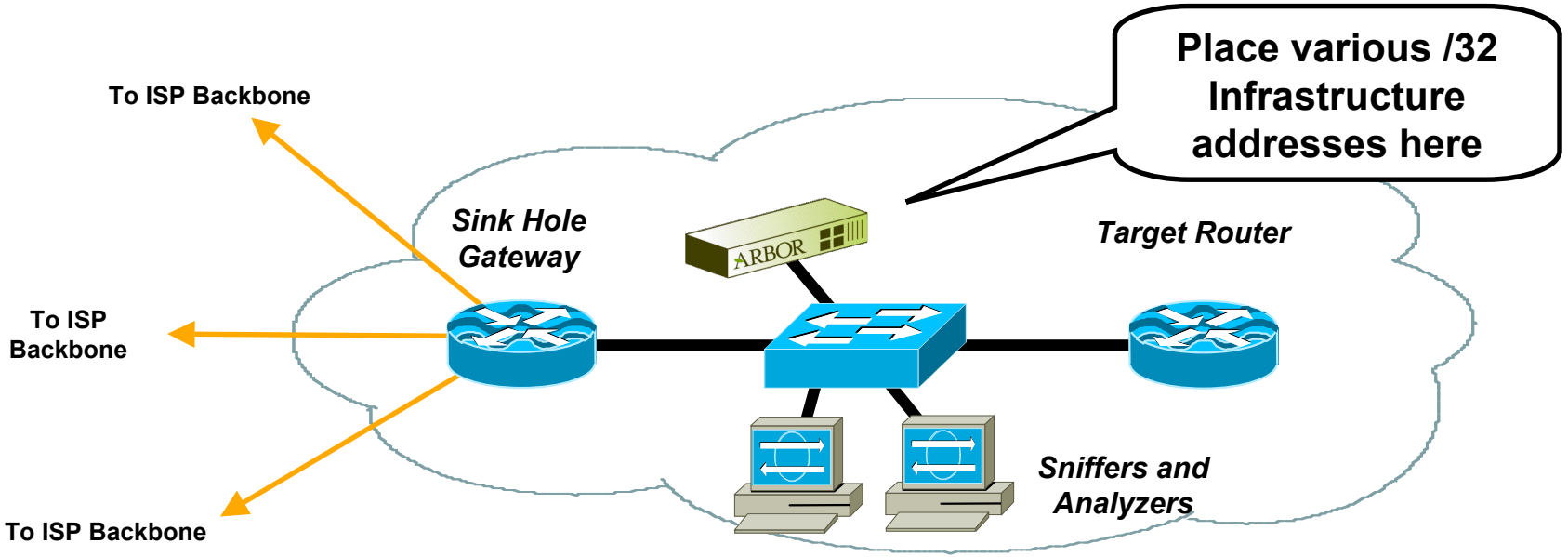
- Sinks Holes do not have to be complicated.
- Some large providers started their Sink Hole with a spare workstation with free unix, Zebra, and TCPdump.
- Some GNU or MRTG graphing and you have a decent sink hole.

Target Routers are Expendable



- Sink Hole Gateway Generates the more specific iBGP Announcement.
- 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.

Monitoring Scan Rates

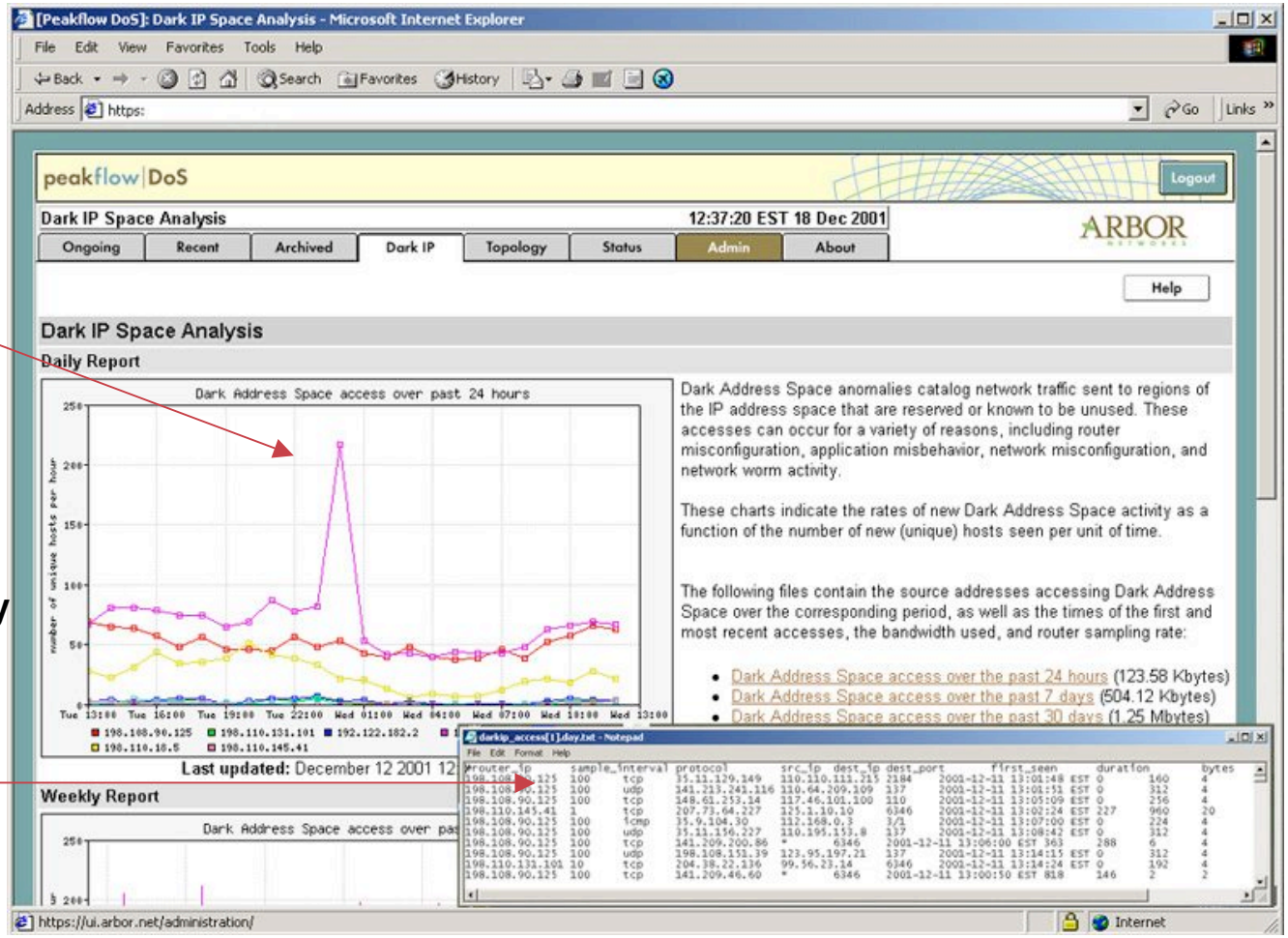


- Select /32 address from different block of your address space. Advertise them out the Sink Hole
- Assign them to a workstation built to monitor and log scans.
- Arbor Network's *Dark IP* Application is one turn key commercial tool that can monitor scan rates.

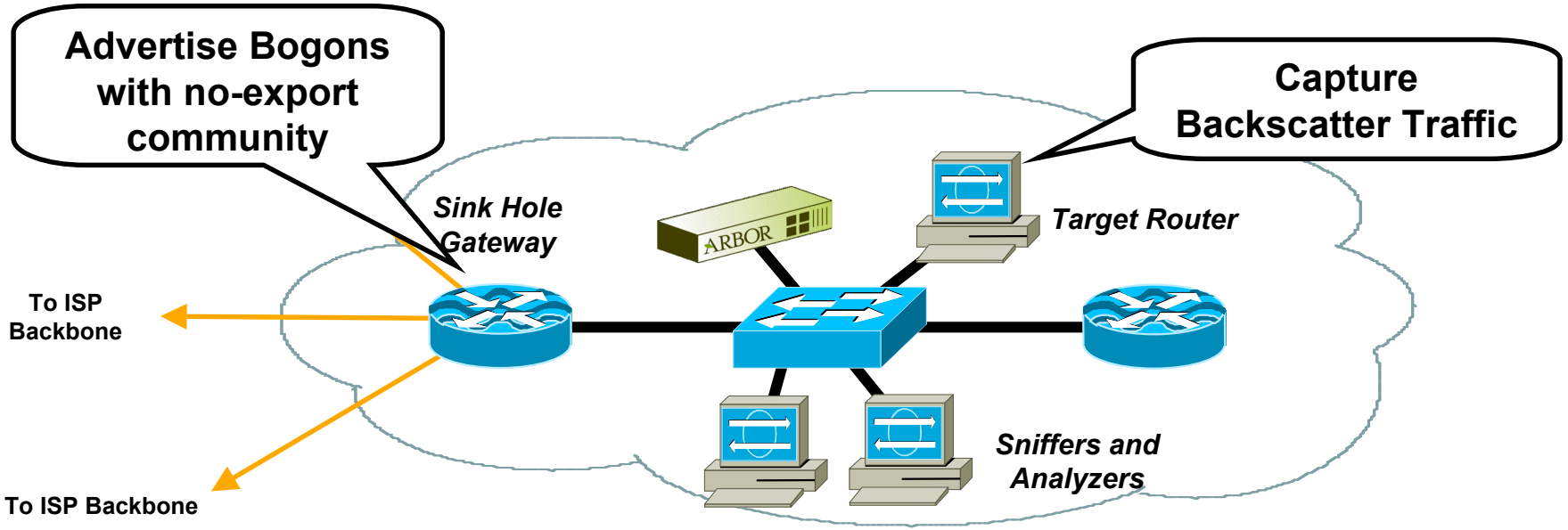
Worm Detection & Reporting UI

Operator instantly notified of Worm infection.

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

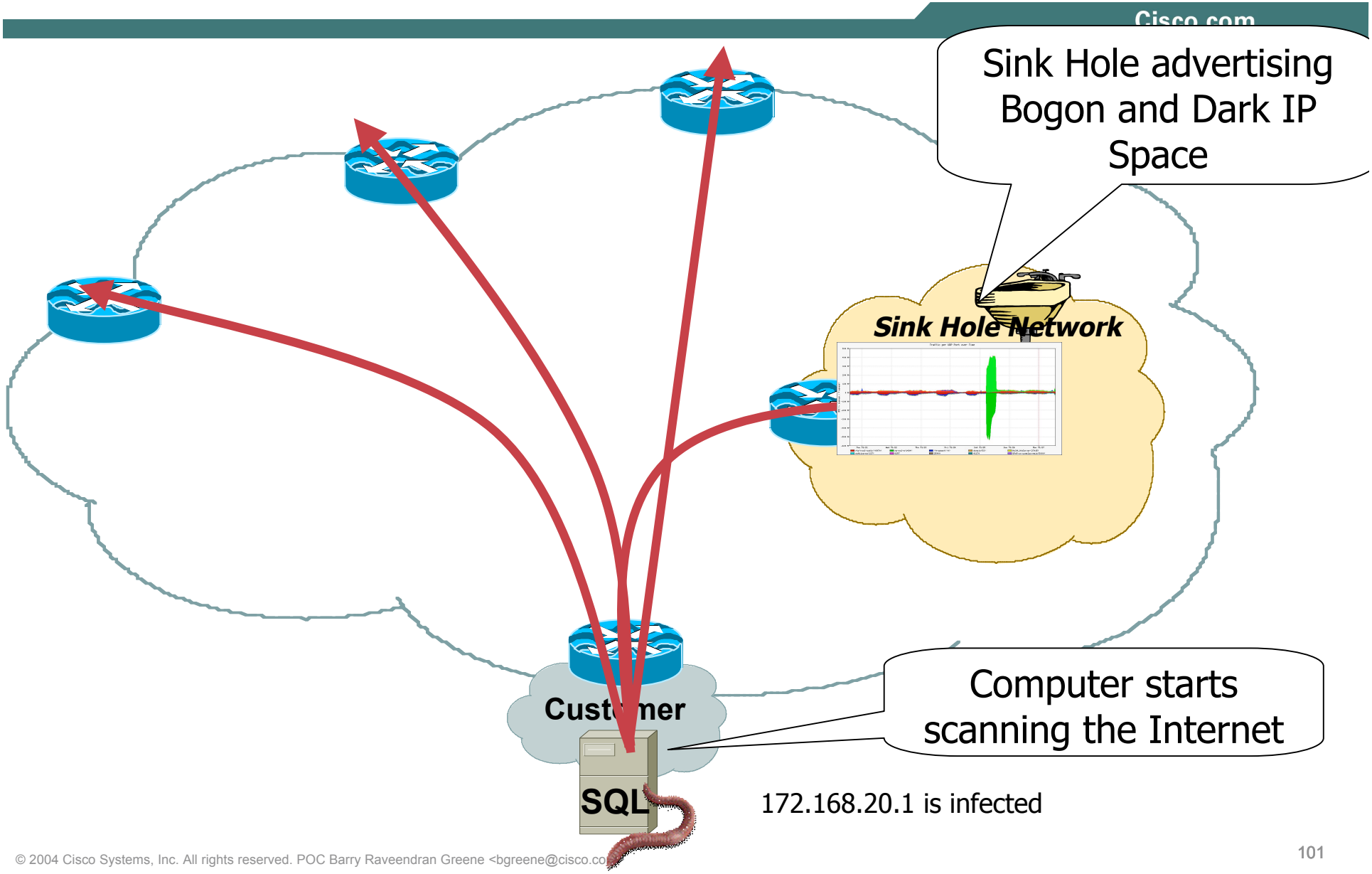


Monitoring Backscatter

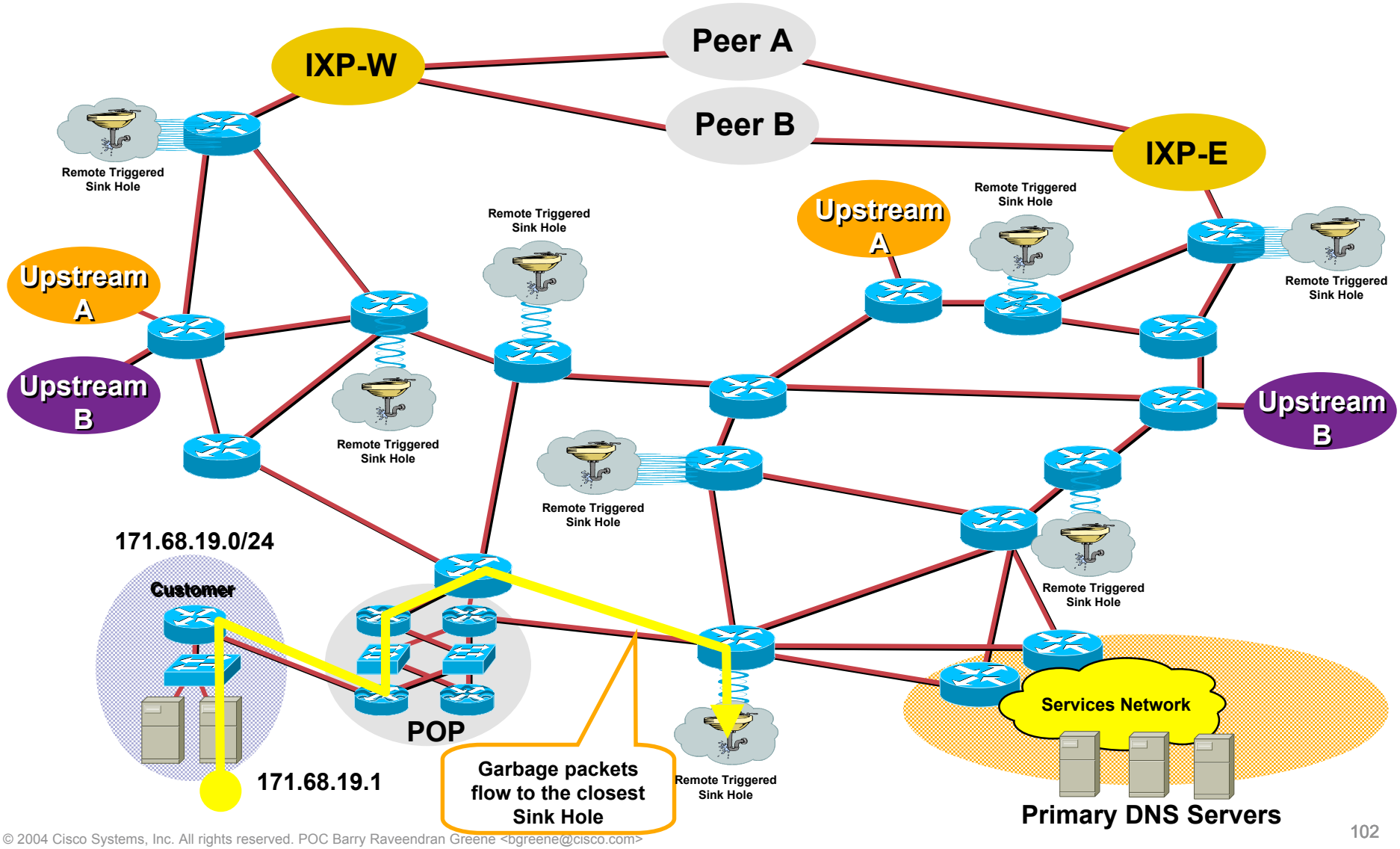


- Advertise bogon blocks with no-export and a safety community (plus ISP egress filtering on the edge)
- Static the bogon to a backscatter collector workstation (as simple as TCPdump).
- Pulls in backscatter for that range – allows monitoring.

Infected End Points

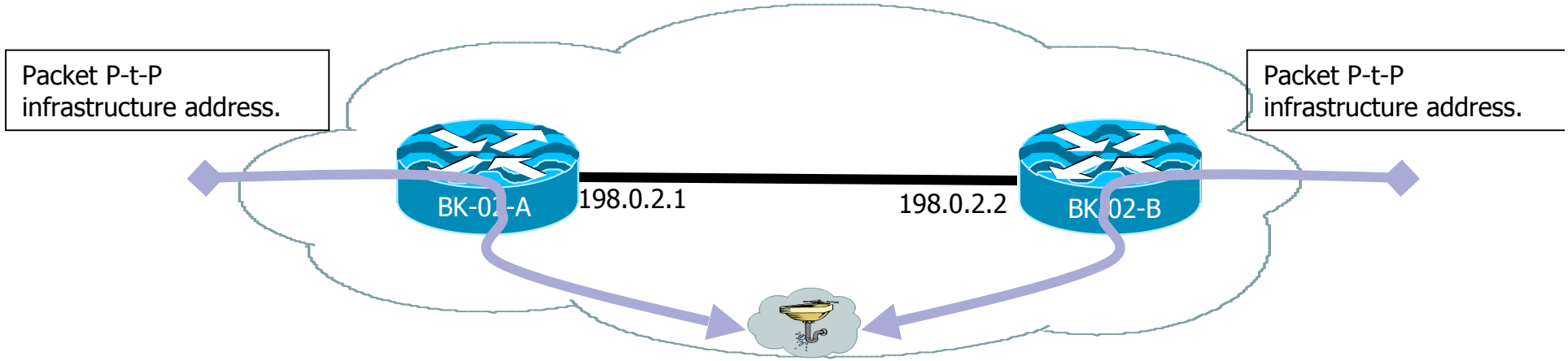


Anycast Sink Holes



Protecting the Backbone Point to Point Addresses

- **Move the Point to Point Addresses 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.**



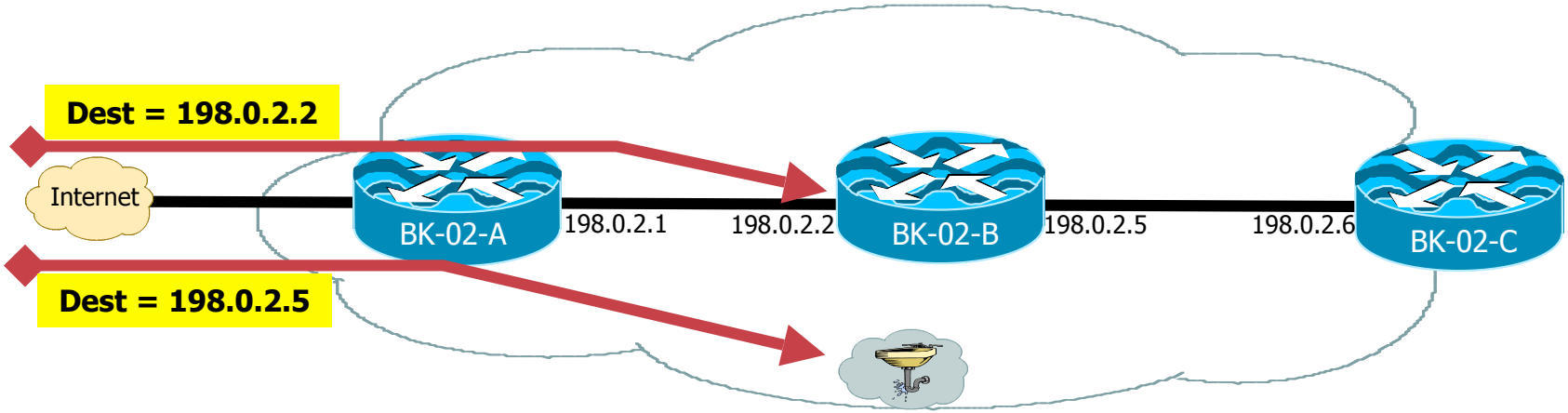
Sink Hole Module

Not Perfect – Provides Another Hurdle.

- **Will not work with the routers on the border.**

  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.



Sink Hole Module

What can you do to help?

Cisco.com

- Sink Holes are critical tools that aid ISP efforts to mitigate attacks.
- Sink Holes were valuable during Turbo Worms like Slammer.
- Build the Sink Holes now – before the next crisis.

HOMEWORK

- Deploy a basic Sink Hole to monitor worms, probes, and other activity
- Look into other uses of Sink Holes

Technique: Source Address Validation

BCP 38 Ingress Packet Filtering

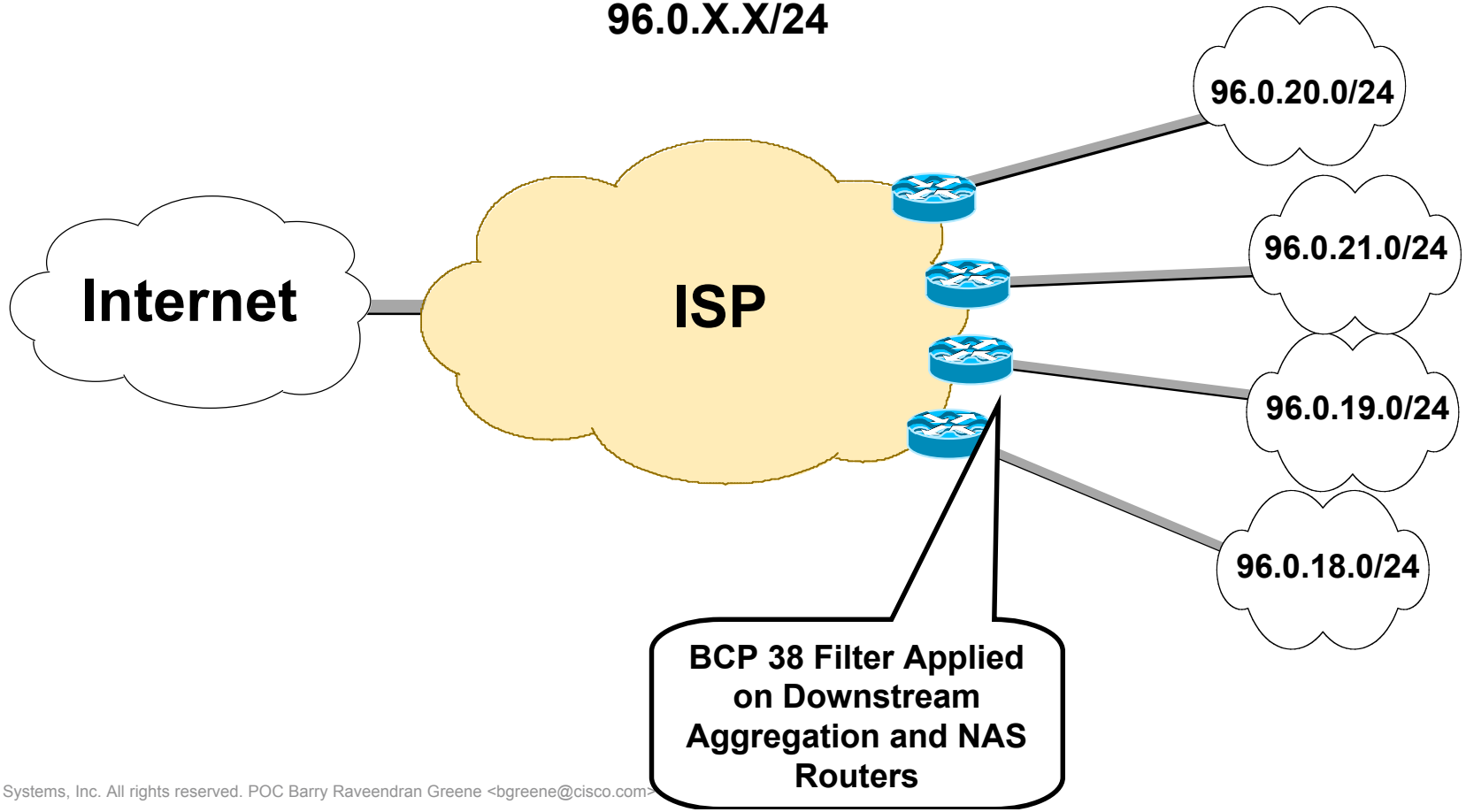
Your customers should not be sending any IP packets out to the Internet with a source address other then the address you have allocated to them!

BCP 38 Ingress Packet Filtering

- BCP 38/ RFC 2827
- Title: Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing
- Author(s): P. Ferguson, D. Senie

BCP 38 Ingress Packet Filtering

ISP's Customer Allocation Block: 96.0.0.0/19
BCP 38 Filter = Allow only source addresses from the customer's 96.0.X.X/24



BCP 38 Packet Filtering: Principles

- Filter as close to the edge as possible
- Filter as precisely as possible
- Filter both source and destination where possible

Cisco's Techniques for BCP 38 Filtering

- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF Strict Mode
- Cable Source Verify/DHCP Lease Query (DHCP)
- IP Source Verify (Catalyst Family)

Source Address Validation Works

- **Successful ISPs have extremely conservative engineering practices.**
- **Operational Confidence in the equipment, functionality, and features are a prerequisite to any new configs on a router.**
- **The core reason why ISPs have not been turning on Source Address Validation is their lack of *Operational Confidence.***

One Major ISP's Example - uRPF

- Month 1 – Cisco Lab Test and Education to help the customer gain confidence in uRPF.
- Month 2 – One port on one router – turning uRPF Strict Mode on a 16xOC3 Engine 2 LC (Cisco 12000)
- Month 3 – One LC on one router – 16xOC3.
- Month 4 – One router all customer facing LCs
- Month 5 – One POP – all customer facing LCs
- Month 6 – Several routers through out the network (other POPs)
- Month 7 – Adopted as standard config for all new customer circuits. Will migrate older customer over time.

One Major ISP's Example - uRPF

- **Lessons Learned:**

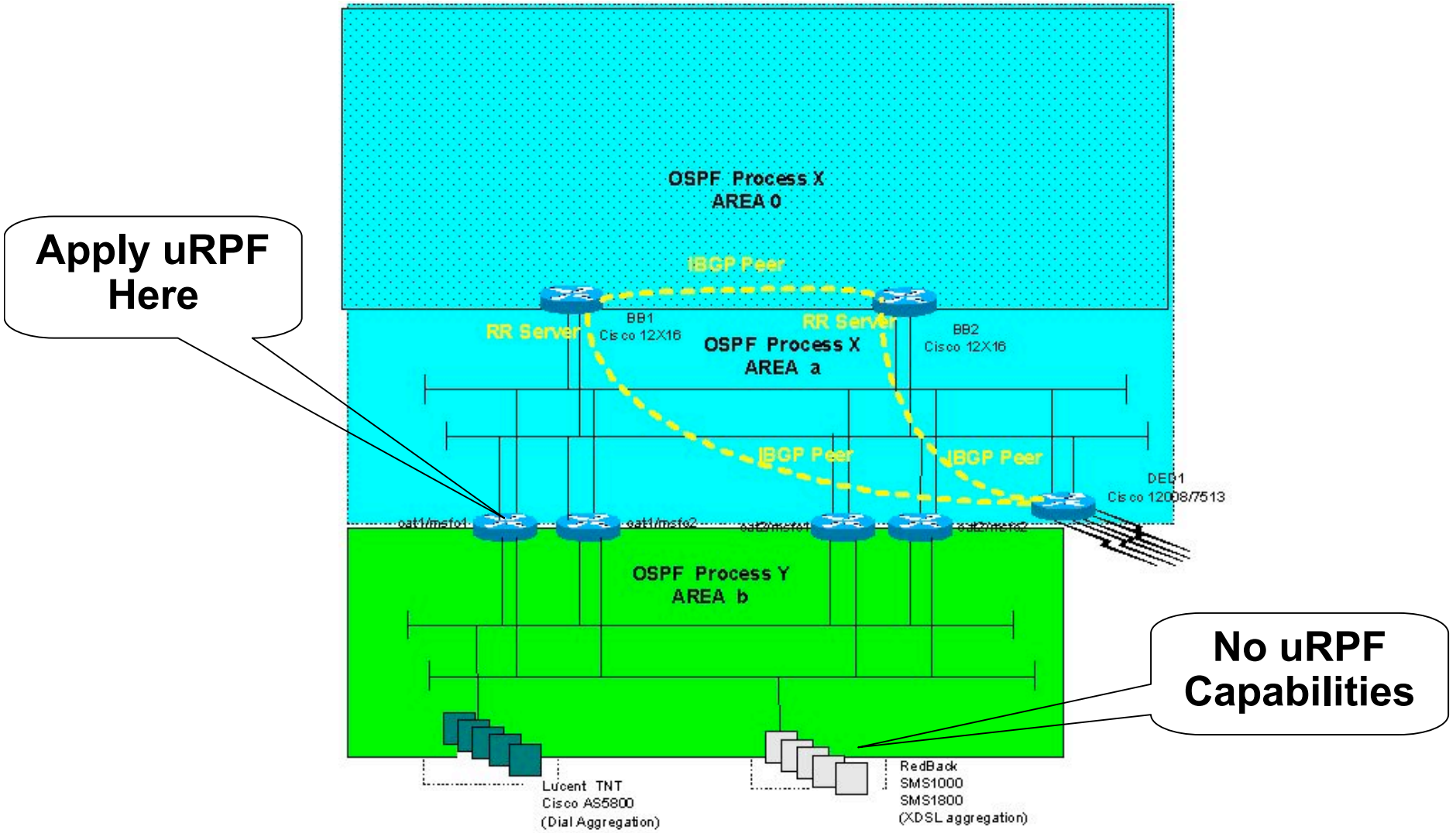
  It took time and patience.

  uRPF did not work for all customers. That is OK, uRPF is not suppose to be a *universal solution.*

  Going slow and steady allowed the operations team to *gain a feel* of the feature's performance envelope --- with out putting the network at risk.

- **It works! A year later it is a standard config with over 40K ports running uRPF Strict or Loose Mode.**

uRPF Strict Mode in the POP



What can you do to help?

- Cut the excuses. It works, it is multi-vendor, there are multiple techniques that work.
- Work towards a gradual gaining operational confidence in the BCP 38 features.
- Source Address validation works – it just take patience and persistence.

HOMEWORK

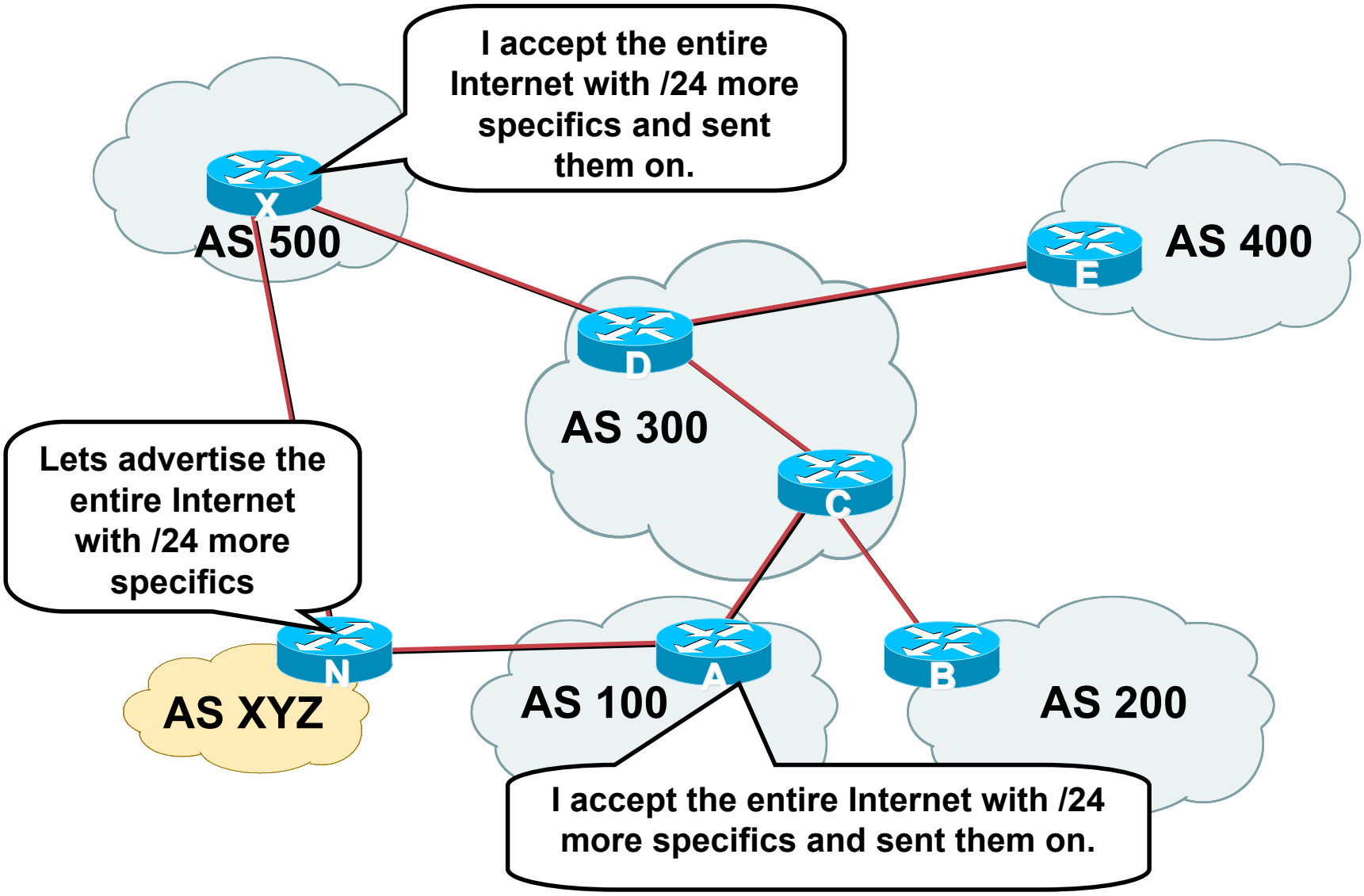
- Deploy BCP 38 in some way shape or form.
- Explore the variety of BCP 38 techniques now available to various operators.

BGP Prefix Filtering

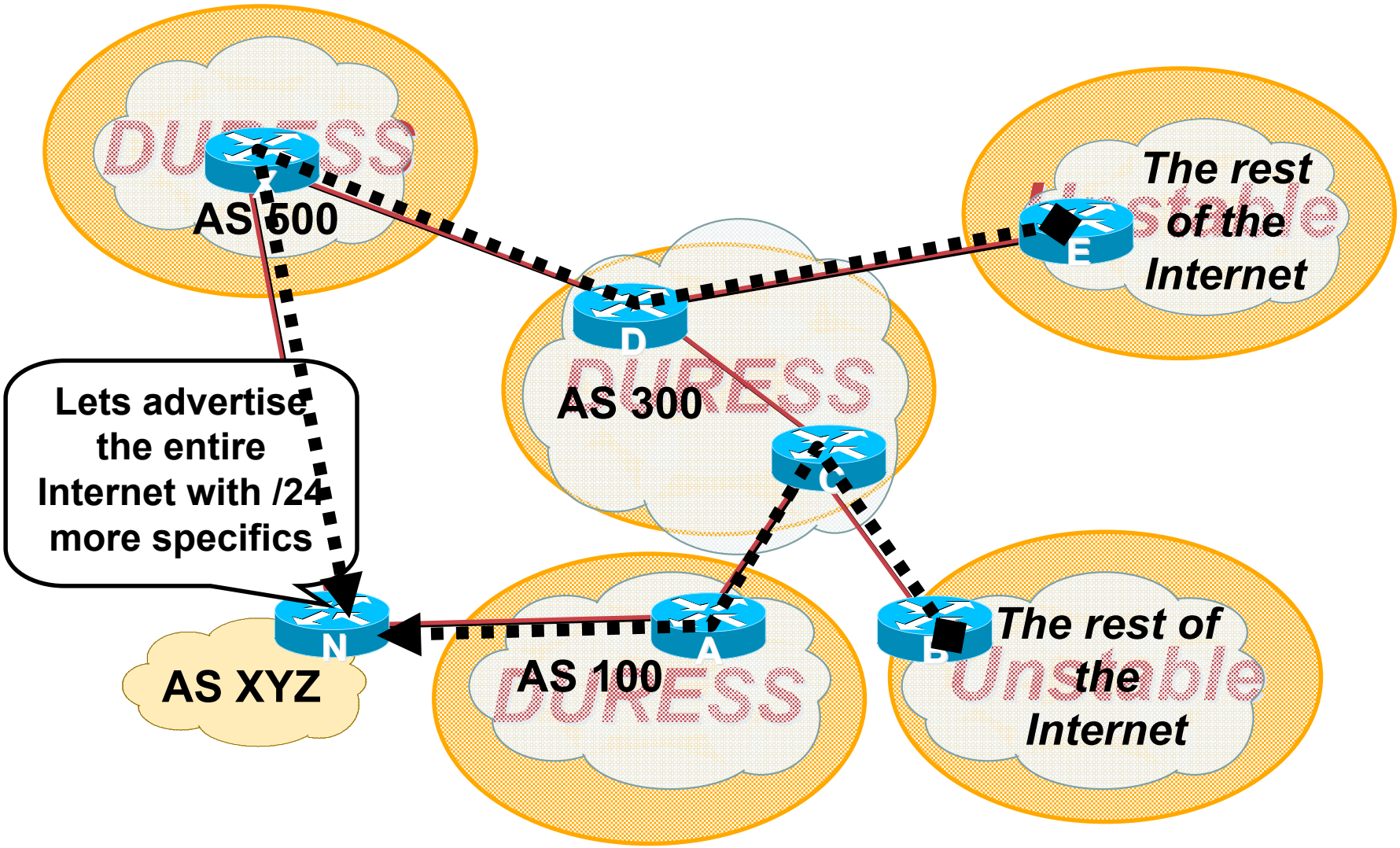
BGP Prefix Filtering

- All BGP Prefixes coming into your network and leaving your network need to be filtered to enforce a policy.
- The problem is most ISPs are not:
  - Filtering Comprehensively
  - Filtering their customer's prefixes
  - Filtering prefixes going out of their network.

Garbage in – Garbage Out: What is it?

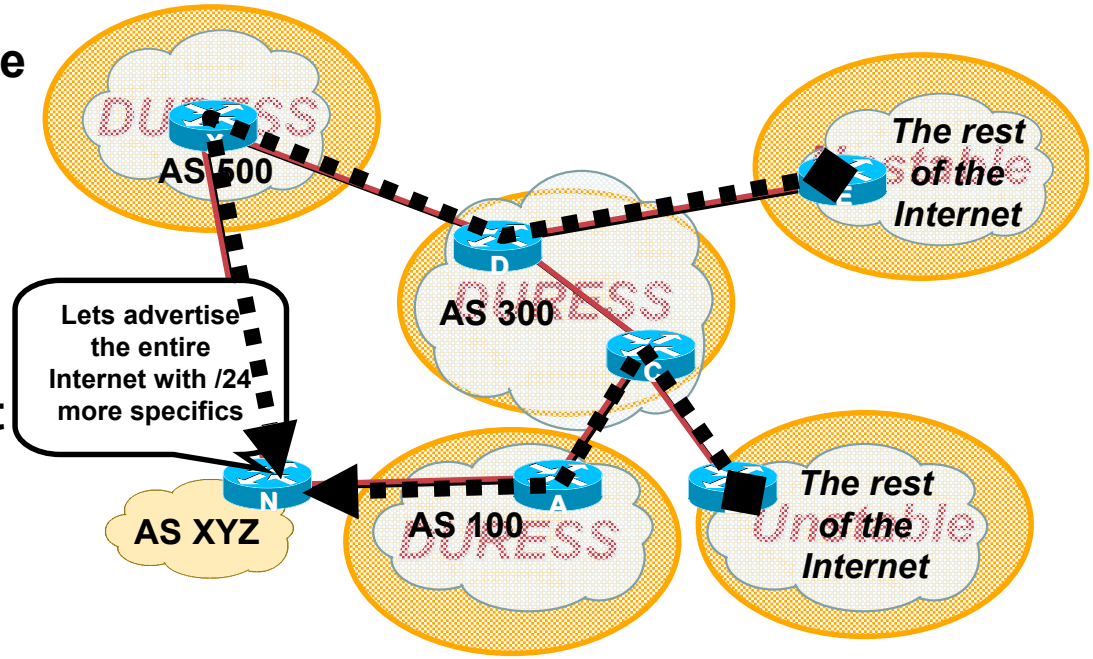


Garbage in – Garbage Out: Results



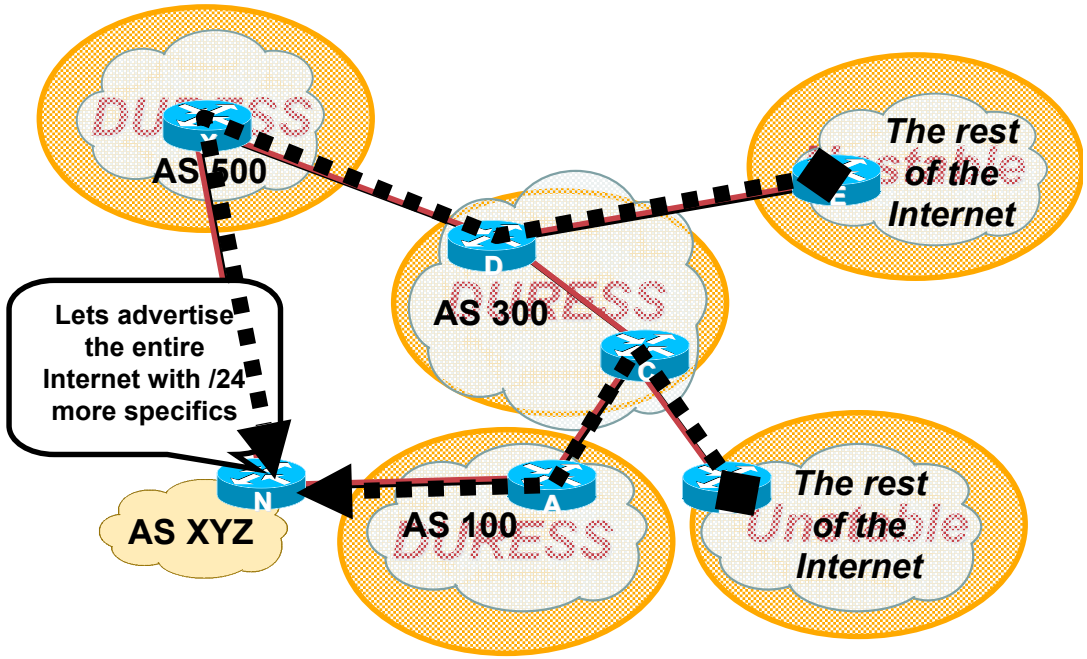
Garbage in – Garbage Out: Impact

- 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.

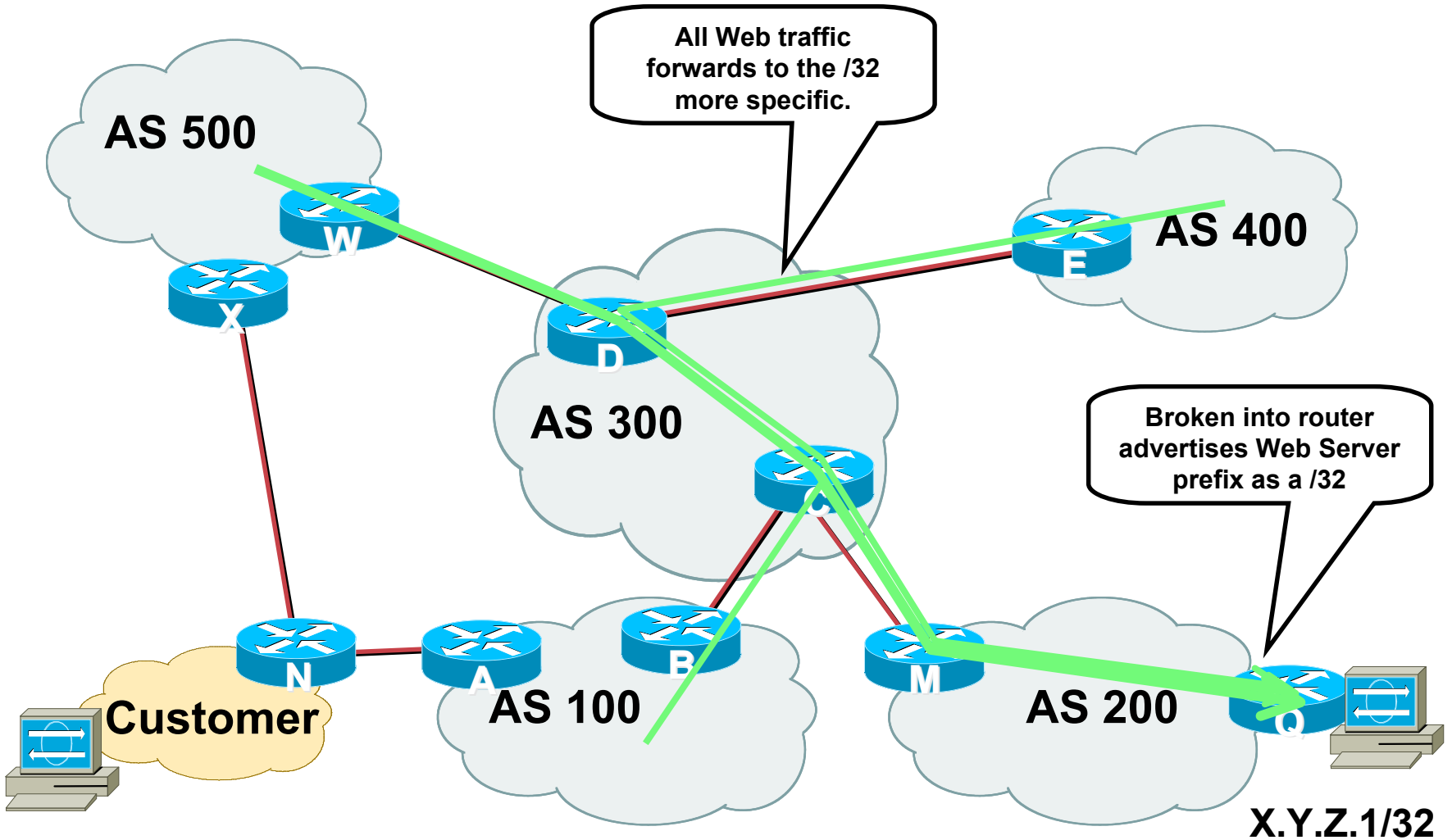


Garbage in – Garbage Out: What to do?

- **Take care of your own Network.**
  - **Filter your customers**
  - **Filter you advertisements**
- **Net Police Filtering**
  - **Mitigate the impact when it happens**
- **Prefix Filtering and Max Prefix Limits**

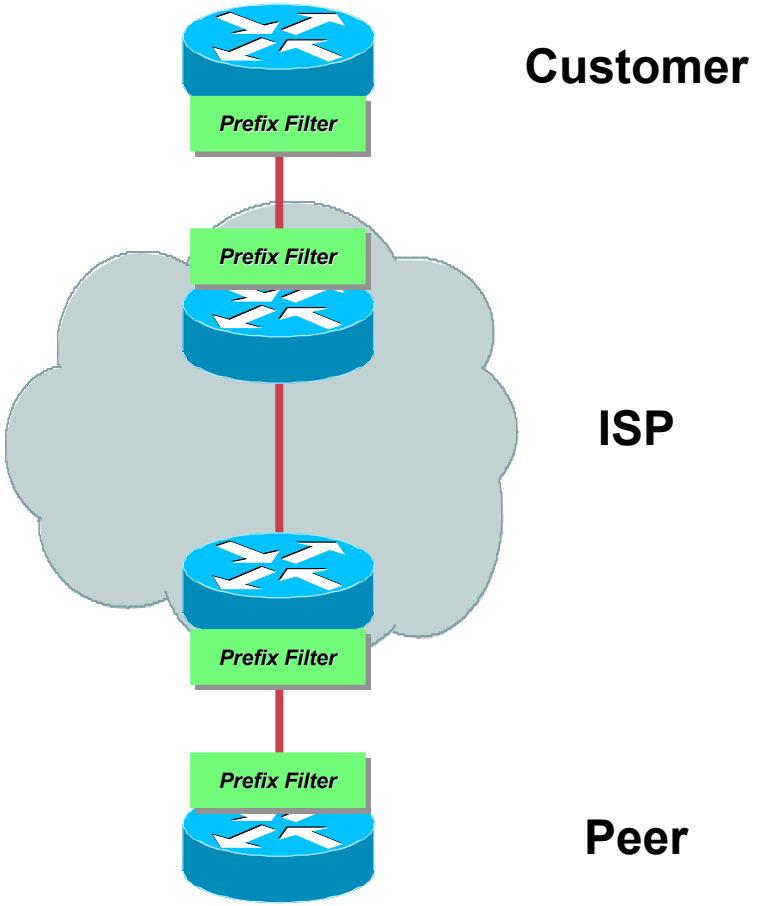


What is a prefix hijack?



Where to Prefix Filter?

- Customer's Ingress/Egress
- ISP Ingress on Customer (may Egress to Customer)
- ISP Egress to Peer and Ingress from Peer
- Peer Ingress from ISP and Egress to ISP



Receiving Customer Prefixes

- **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 220.50.0.0/2
ip prefix-list customer deny 0.0.0.0/0 le 32
```

Prefix Filter Bogons and RIR Blocks

- **The hard work is done for you via the Bogon Project:**

  http://www.cymru.com/Bogons/index.html

- **Cisco Template by Barry Greene**

  ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/

- **Juniper Template by Steven Gill**

  http://www.qorbit.net/documents.html

Other BGP Security/Policy Techniques

- BGP Community Filtering
- MD5 Keys on the eBGP and iBGP Peers
- Max Prefix Limits
- RFC 1998 +++
- BGP Dampening with RIPE-299

What can you do to help?

- Prefix Filter your customers.
- Prefix Filter the Bogons and police other prefixes coming into your network.
- Prefix Filter what you send to the Internet.
- Protect your self
- Protect the Internet
- Stop the BGP Prefix Injection technique

HOMEWORK

- Ingress BGP Prefix Filters should be applied tonight!
  - Use the templates
- Egress BGP Prefix Filters should be applied next.
- All BGP speaking customers should have ingress prefix filters applied.

What next?

Next Seven Techniques

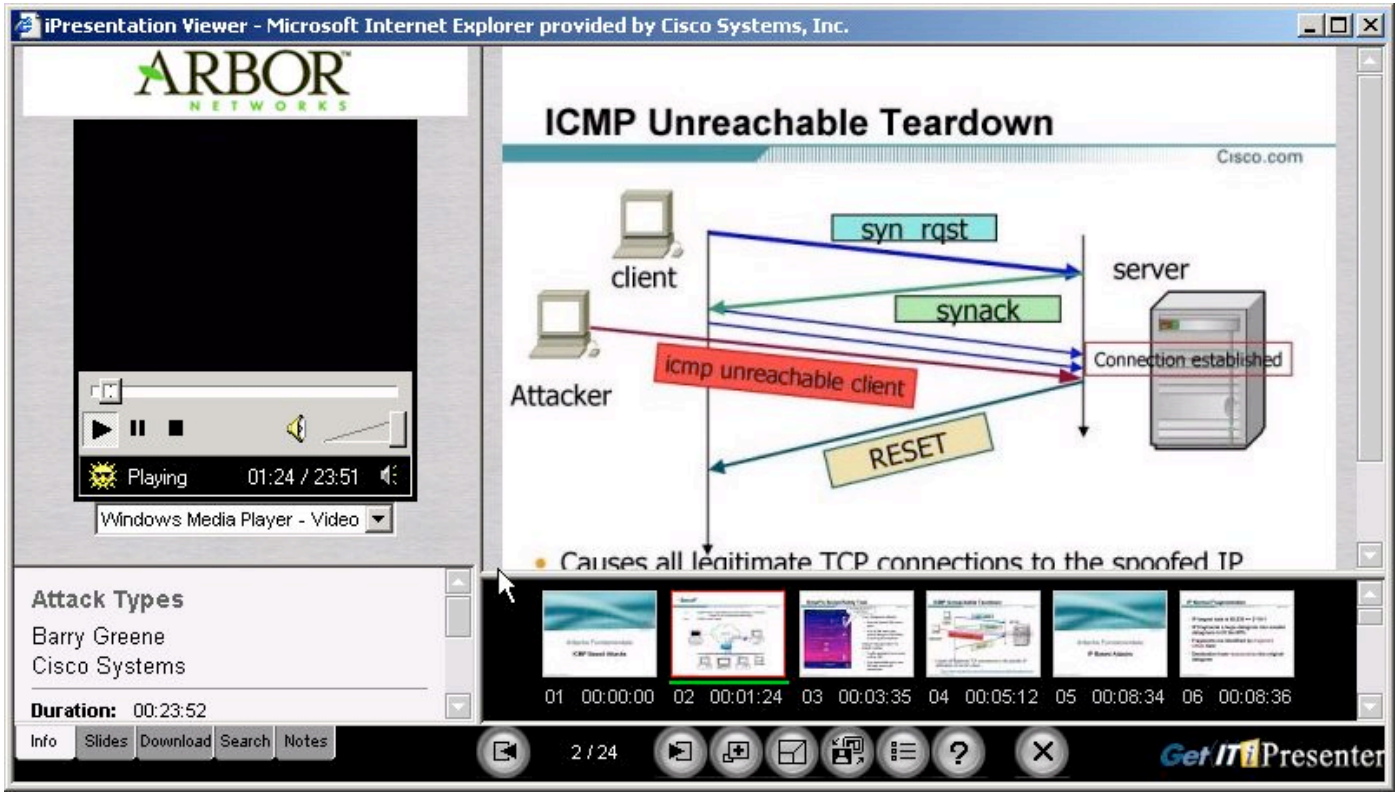
- Receive Path ACL (and CPP)
- Back Scatter Trace Back
- Source Based Remote Triggered Black Hole Filtering
- Netflow Based Security Telemetry System
- BGP Policy Accounting
- Remote Triggered Rate Limiting
- BGP Community Filtering

What's After the *Next Seven?*

- DNS Infrastructure Security
- Customer Support and *De-Worming* Self Help Site
- NOC and SOC Security
- Co-Lo and Web Hosting Security
- SMTP Server Security (New Anti-SPAM Techniques)

Where are the VODs

- **When ever possible, Video on Demand (VODs) are done of the SP/ISP/ASP/Big Network Bootcamp materials.**
- **http://palomar.getitmm.com/bootcamp/**



Pull down these slides ….

- ftp://ftp-eng.cisco.com/cons/seminars/
- ftp://ftp-eng.cisco.com/cons/isp/security/

What do you do next?

1. Pull down the rest of my materials.

   ftp://ftp-eng.cisco.com/cons/isp/security/

2. Get Cisco ISP Essentials (Cisco Press)

3. Check some of the latest NANOG materials – example Vijay Gill's (AOL) NANOG26 presentation

   http://www.nanog.org/mtg-0210/ppt/vijay.pdf

4. Pull down the Router Security Requirement Draft:

   http://www.port111.com/docs/

5. Learn Anycast!

SP Security Specialist

- There are too few ISP Security Specialist in the world.
- Looking for people who know:
  - All of the items in a enterprise security world.
  - How ISP Backbones are build, run, and operated.
  - How the Internet is glued together.
  - Broad understanding of our entire product line with the ability to get deep quick.
  - Ability to write and communicate to customers.

Q and A