



SP Security Primer 101

Peers working together to battle
Attacks to the Net
Version 2.1



Free Use

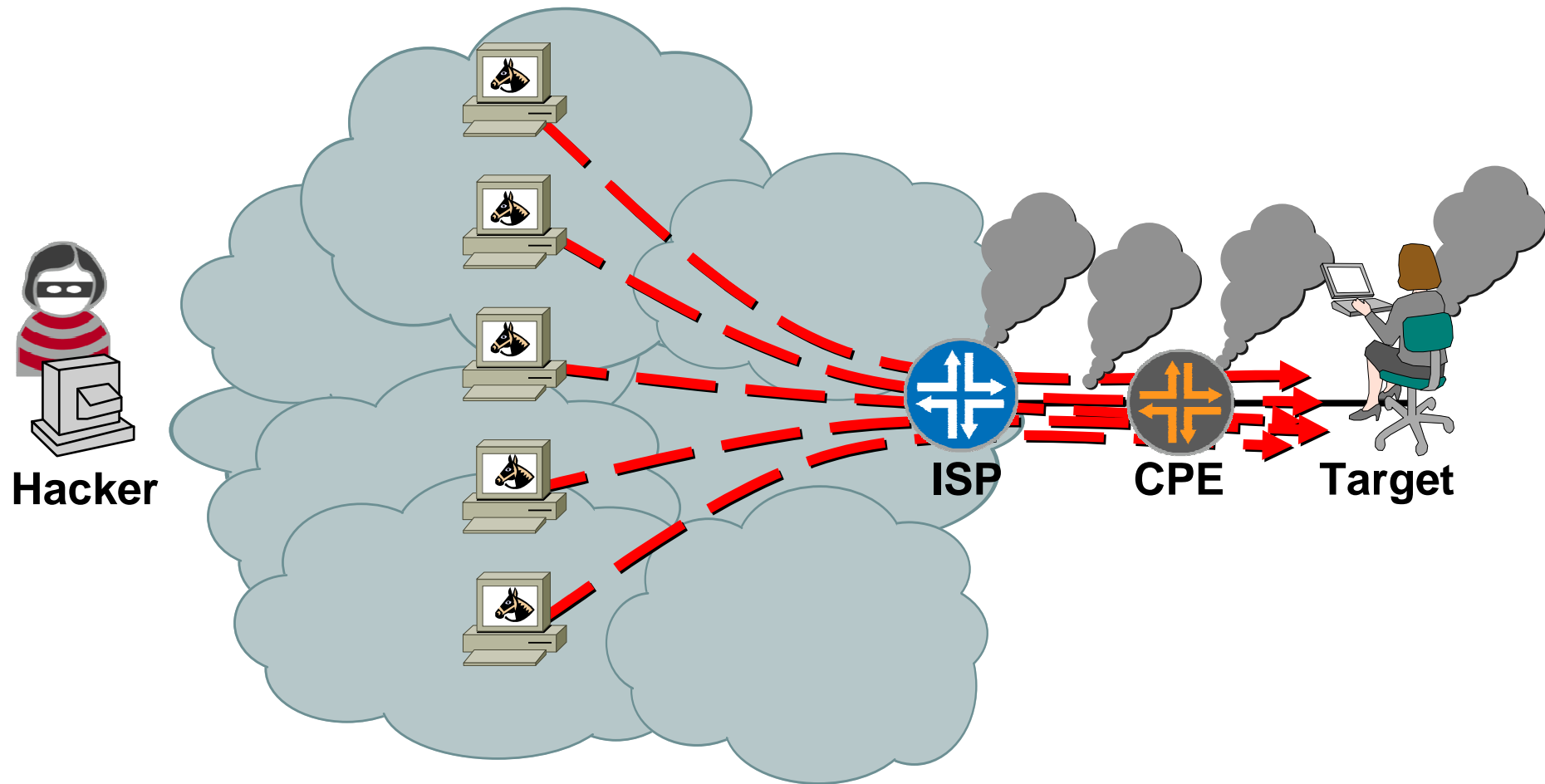
- This slide deck can be used by any operator to help empower their teams, teach their staff, or work with their customers.
- It is part of the next generation of **NANOG Security Curriculum** providing tools that can improve the quality of the Internet.



Goal

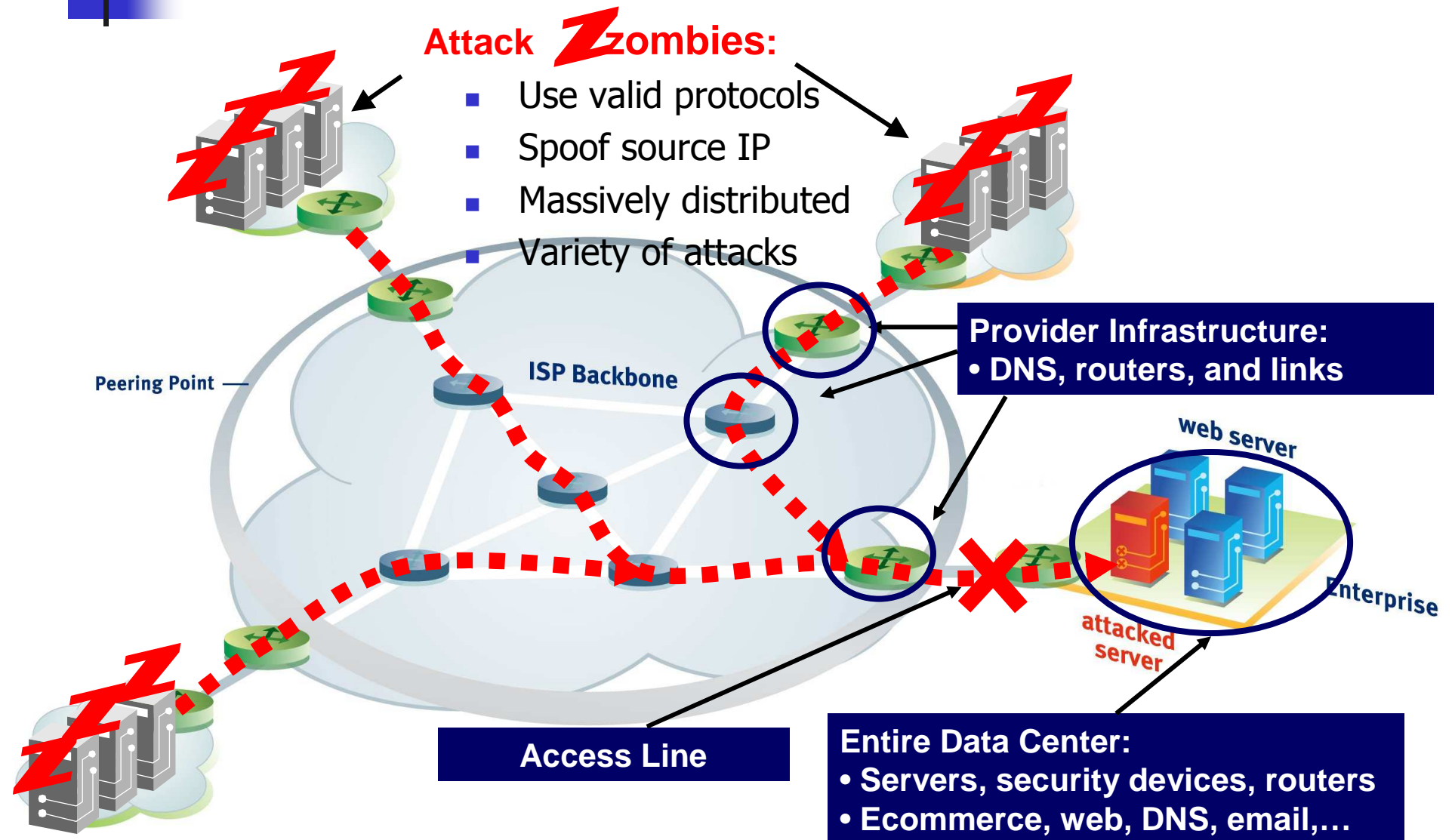
- Provide 10 core techniques/task that any SP can do to improve their resistance to security issues.
- These 10 core techniques can be done on any core routing vendor's equipment.
- Each of these techniques have proven to make a difference.

What Do You Tell the Boss?



DDoS Vulnerabilities

Multiple Threats and Targets



The SP's Watershed – Feb 2000



The screenshot shows the CNN.com website interface from February 2000. The top navigation bar includes links for MAIN PAGE, WORLD, U.S., LOCAL, POLITICS, WEATHER, BUSINESS, SPORTS, and TECHNOLOGY. The main headline reads: **'Immense' network assault takes down Yahoo**. Below this, a sub-headline states: **Cyber-attacks batter Web heavyweights**. The article text begins with: **Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack**. The date is February 9, 2000, and the time is 9:56 a.m. EST (1456 GMT). The article is categorized under **INSURGENCY on the internet**. The left sidebar contains a list of categories: SPACE, HEALTH, ENTERTAINMENT, BOOKS, TRAVEL, FOOD, ARTS & STYLE, NATURE, IN-DEPTH, ANALYSIS, and myCNN.

YAHOO!

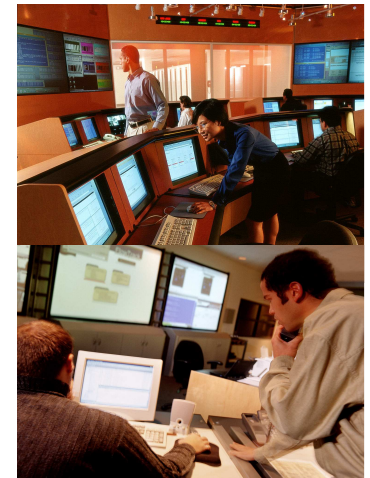
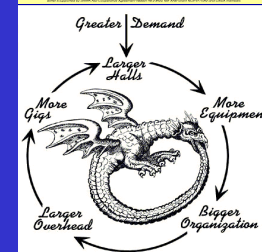
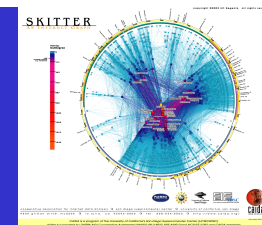
amazon.com

CNN.com

eBay

E*TRADE

Overview



The Vetted – Battling the Bad Guys

WIRED MAGAZINE: ISSUE 15.09

POLITICS : SECURITY [RSS](#)

Hackers Take Down the Most Wired Country in Europe

By Joshua Davis [✉](#) 08.21.07 | 2:00 AM



Defense minister Jaak Aaviksoo got help from NATO in the wake of the cyberattacks. Photo: Donald Milne

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were all down. The former director of the University of Tartu Institute of Experimental Physics and Technology had been the Estonian defense minister for only four weeks. He hadn't even changed the art on the walls.

An aide rushed in with a report. It wasn't just the newspapers. The leading bank was under siege. Government communications were going down. An enemy had invaded and was assaulting dozens of targets.

Outside, everything was quiet. The border guards had reported no incursions, and Estonian airspace had not been violated. The aide explained what was going on: They were under attack by a rogue computer network.

It is known as a botnet, and it had slipped into the country through its least protected border — the Internet.

FEATURE

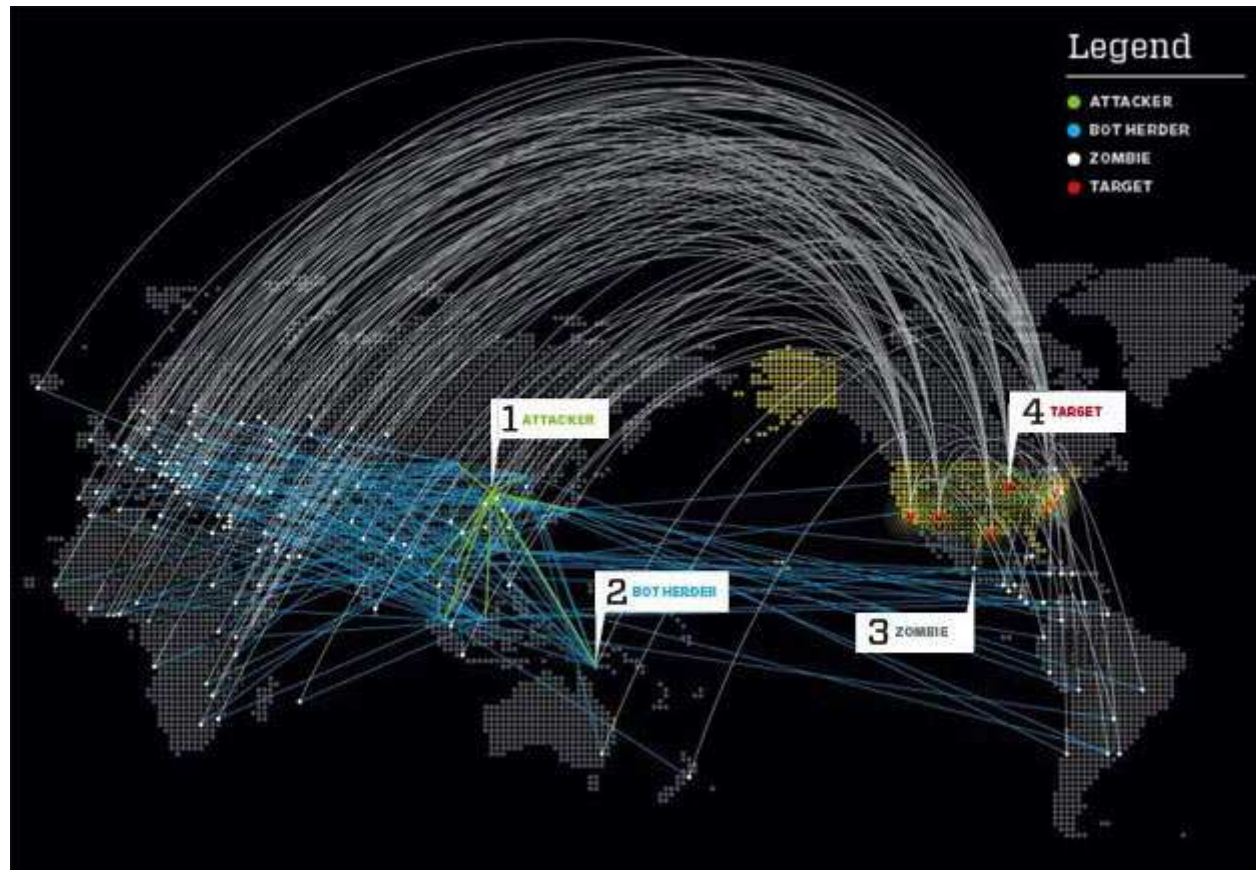


When Bots Attack



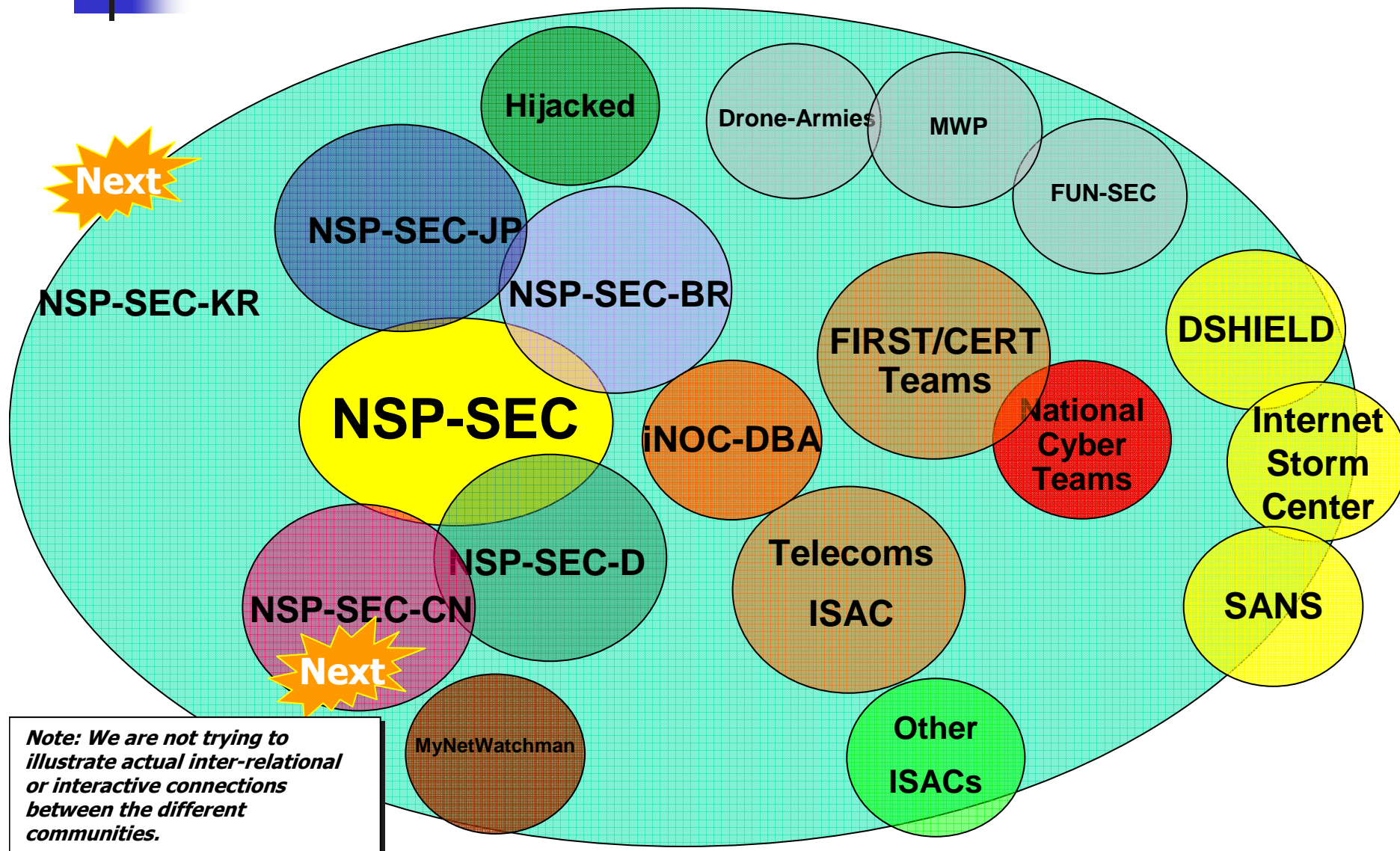
Washington Ignores

When BOTs Attack – Inter AS



http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots

Aggressive Collaboration

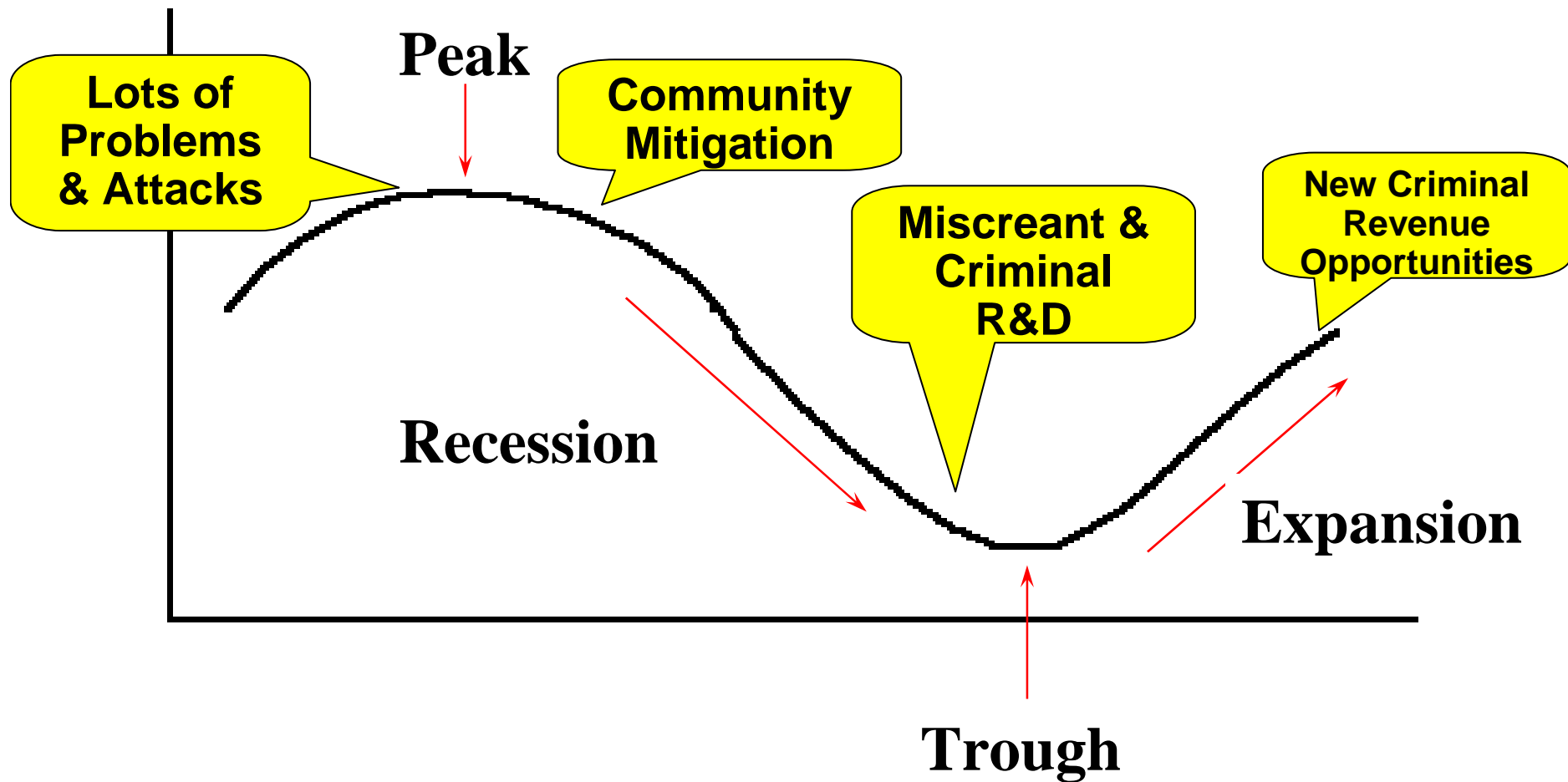




What is NSP-SEC

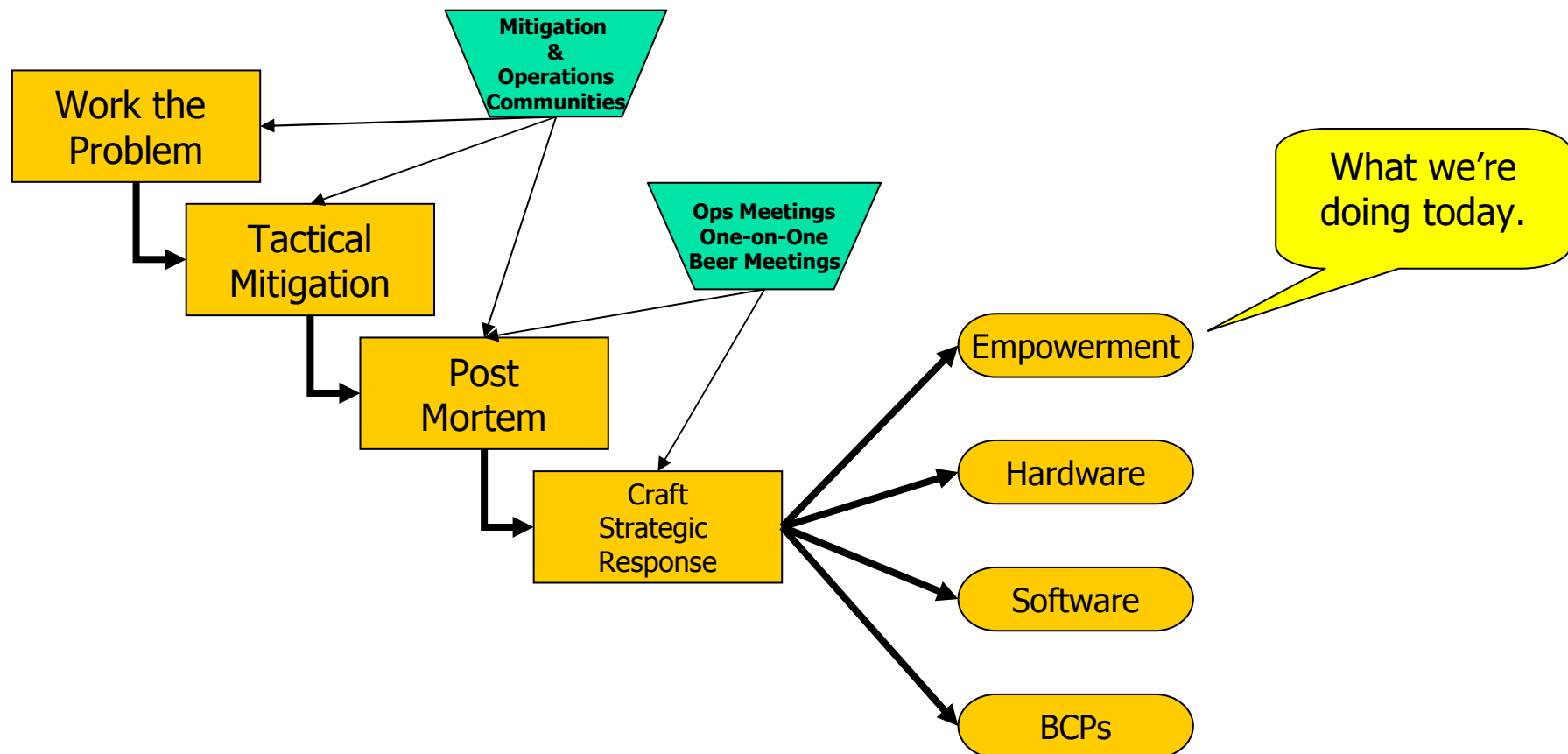
- NSP-SEC – *Closed* Security Operations
Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- <http://puck.nether.net/mailman/listinfo/nsp-security>

Economic Cycles



Parts of the Cyber Criminal Business Cycle

Where is This Coming From?





Working the 40/40/20 Rule

- Sean Donelan's (SBC) [sean@donelan.com] rule for end point patching:
 - 40% of the customers care and will proactively patch
 - 40% of the customers may someday care and fix/patch/delouse their machines
 - 20% of the customers just do not care and have never responded to any effort to fix them.



Top Ten List of things that Work

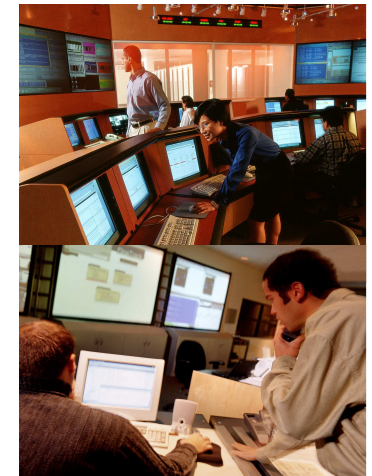
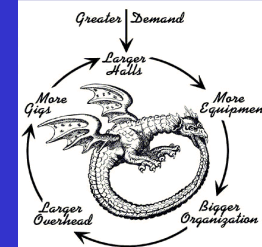
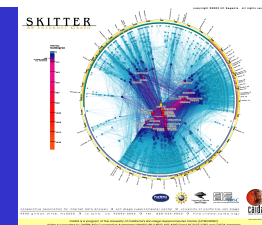
1. Prepare your NOC
2. Mitigation Communities
3. iNOC-DBA Hotline
4. Point Protection on Every Device
5. Edge Protection
6. Remote triggered black hole filtering
7. Sink holes
8. Source address validation on all customer traffic
9. Control Plane Protection
10. Total Visibility (Data Harvesting – Data Mining)

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

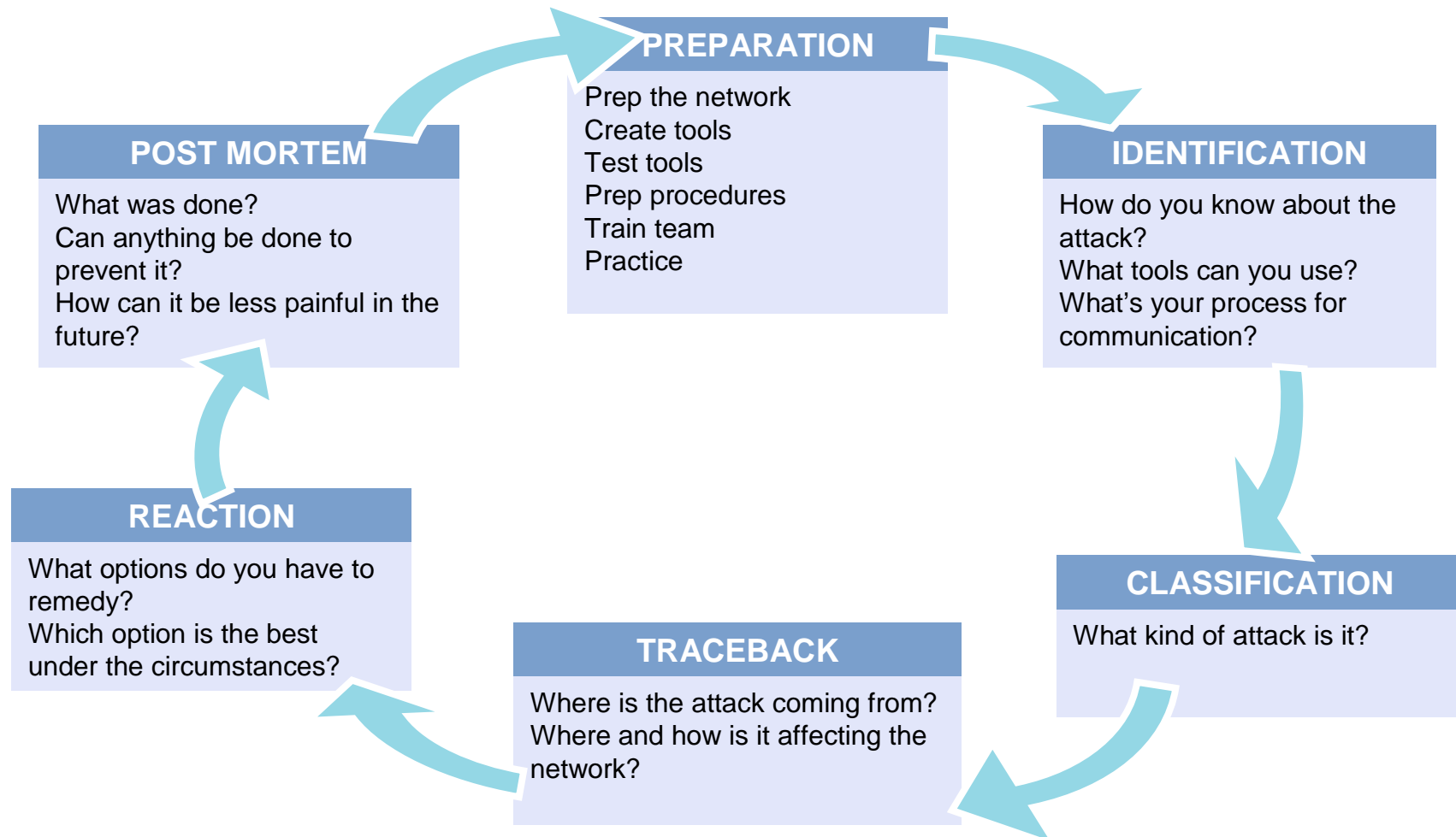
Sun Tzu

Art of War

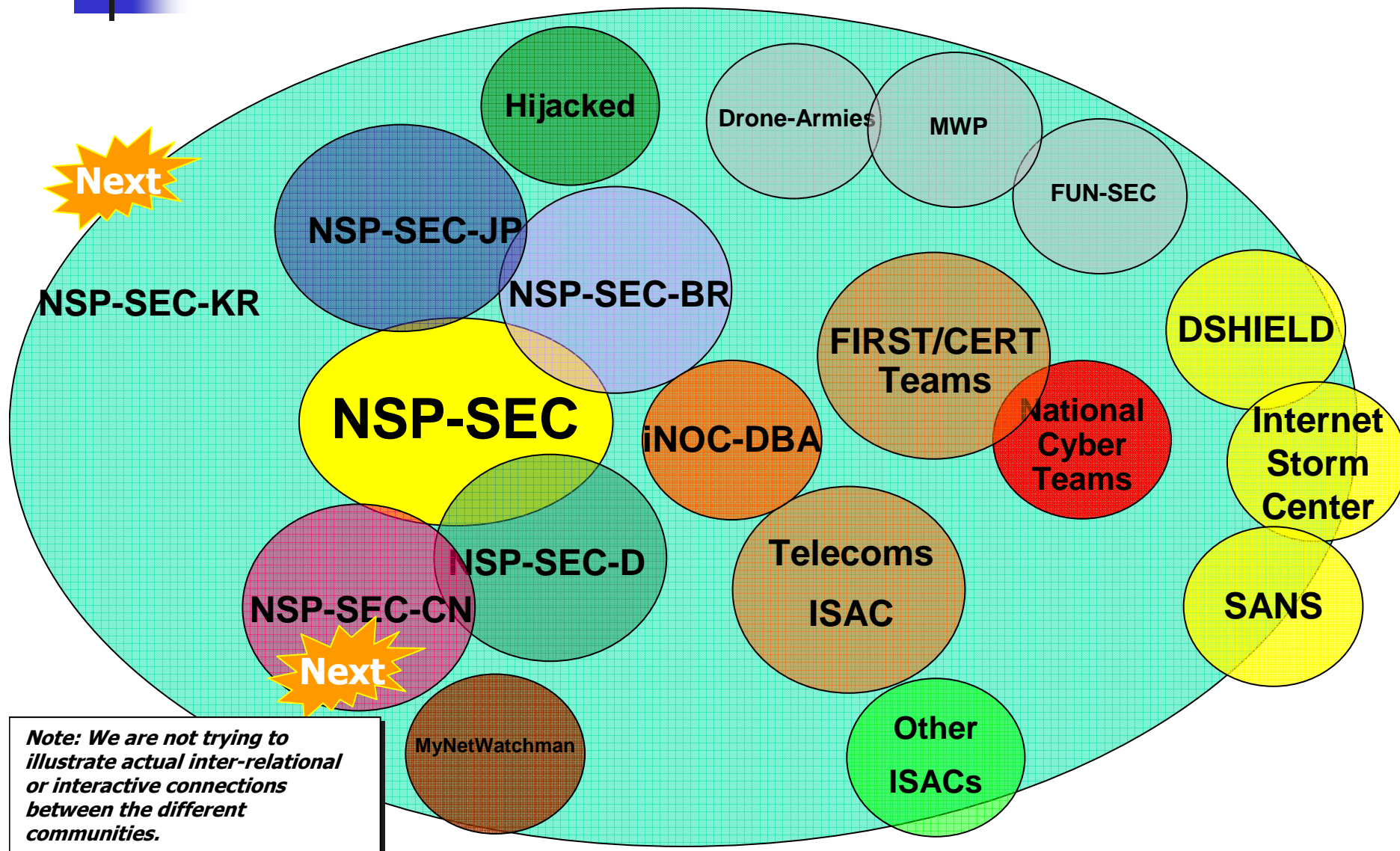
The Executive Summary



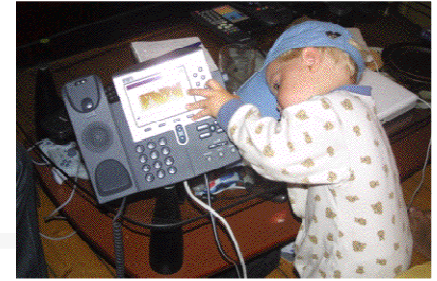
SP Security in the NOC - Prepare



Aggressive Collaboration

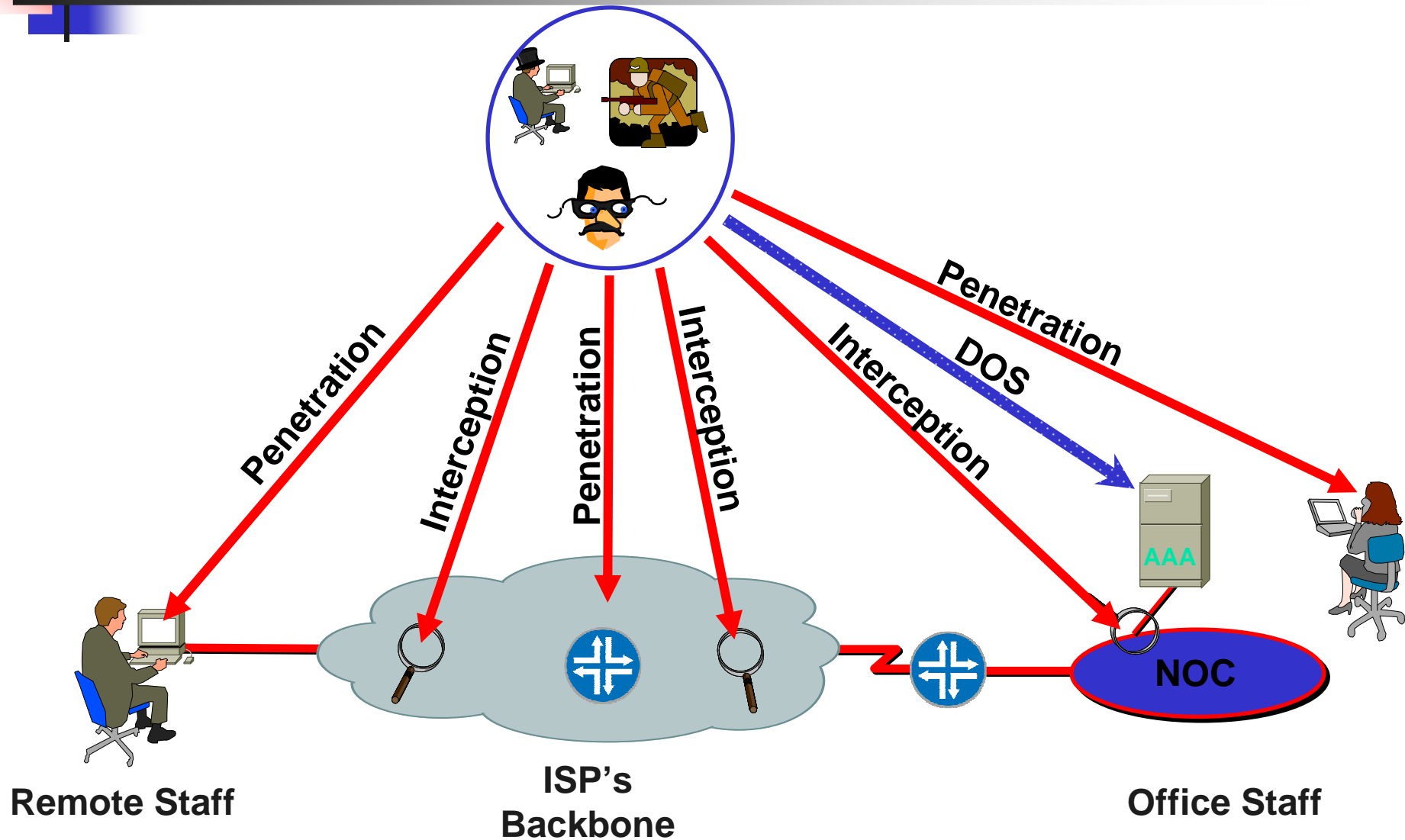


iNOC DBA Hotline

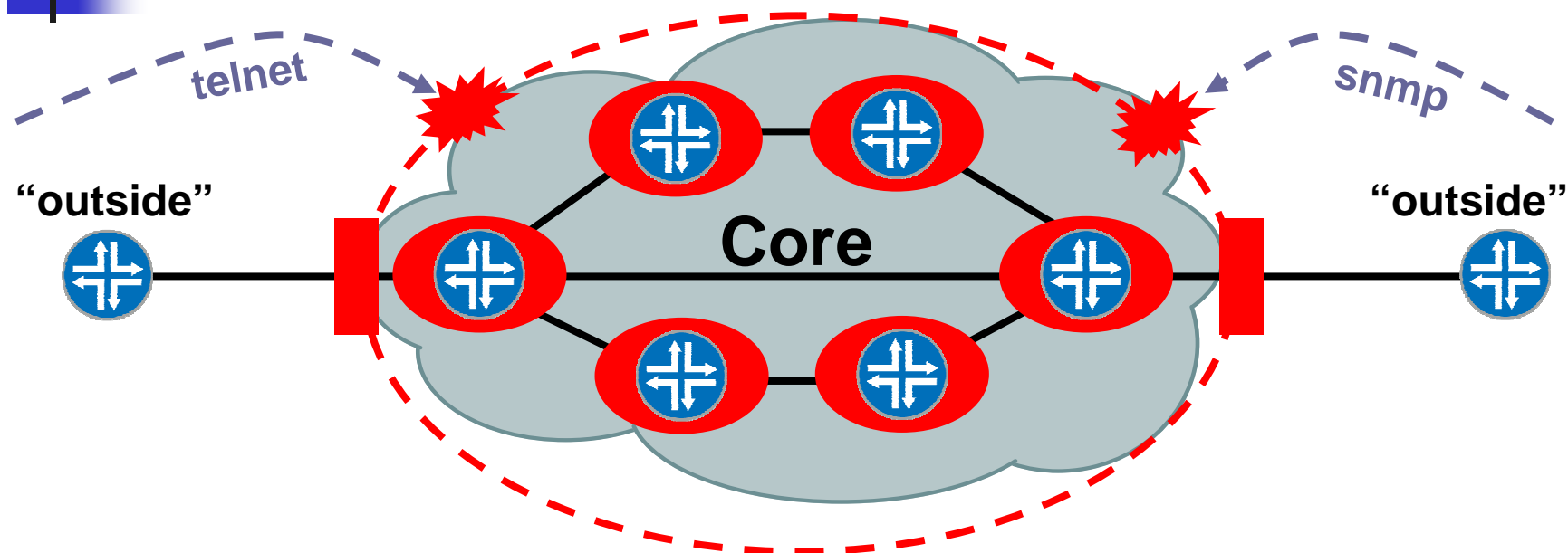


- INOC-DBA: *Inter-NOC Dial-By-ASN*
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
 - ASnumber:phone
 - 109:100 is Barry's house.
- SIP Based VoIP system, managed by www.pch.net

Point Protection

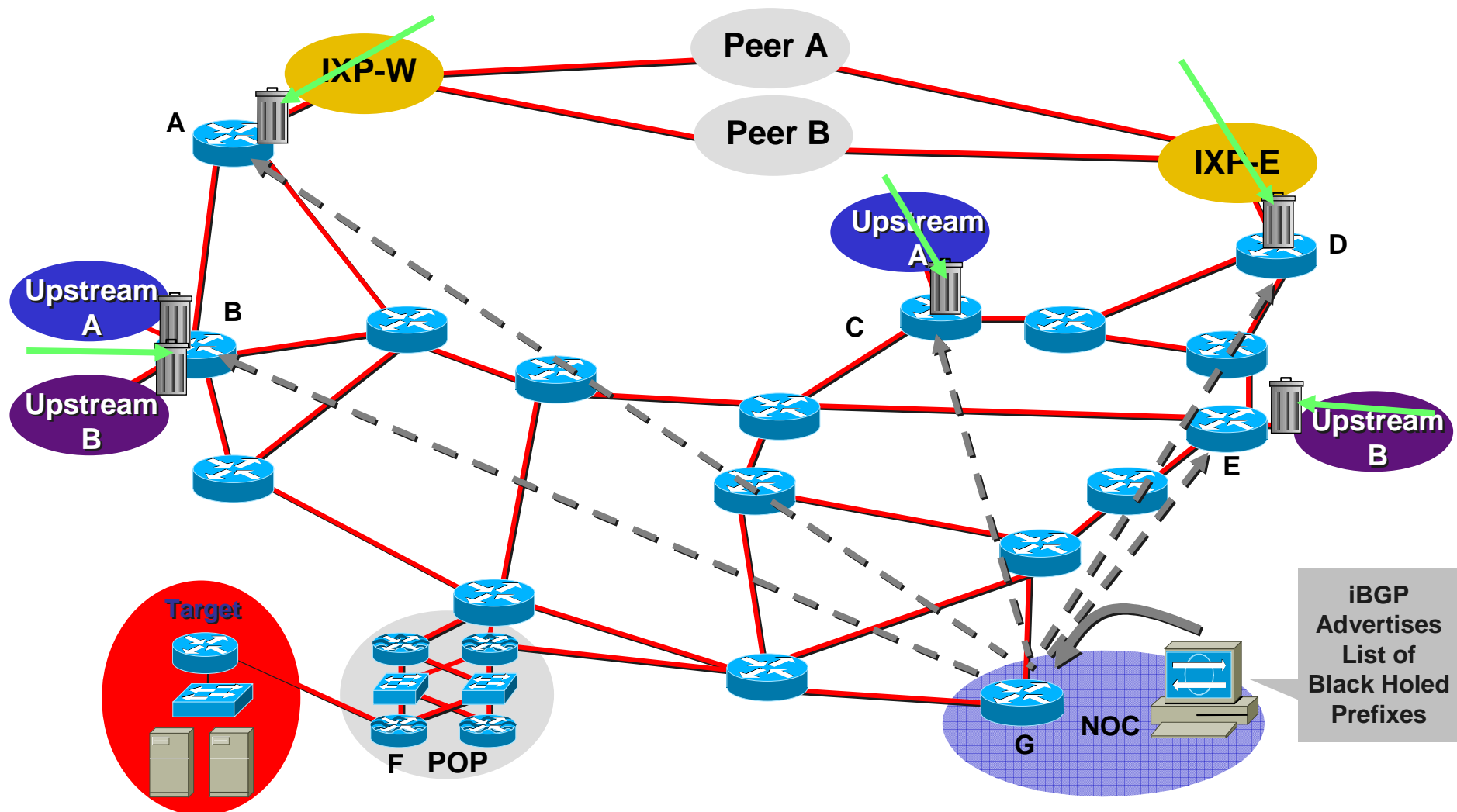


Edge Protection

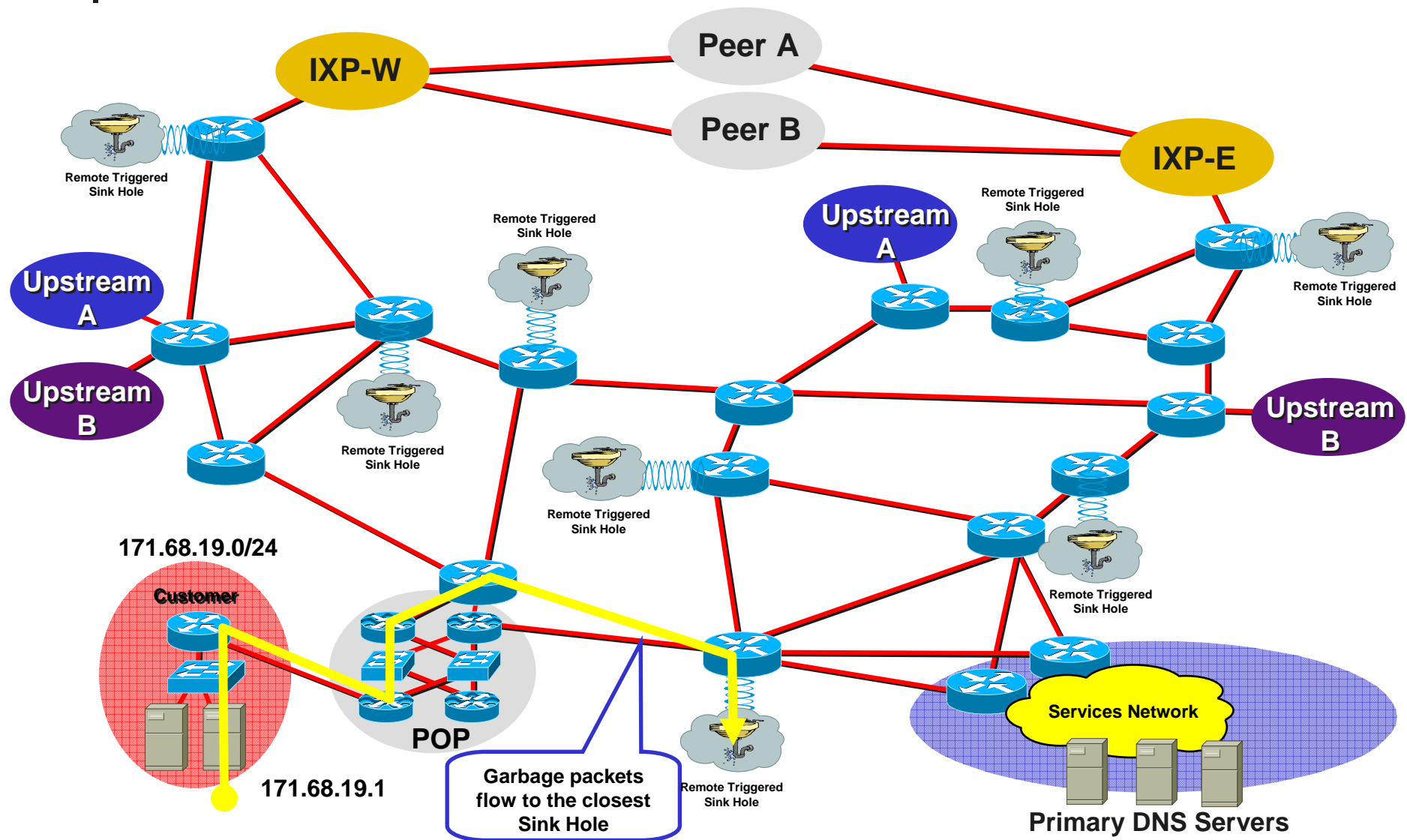


- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Destination Based RTBH



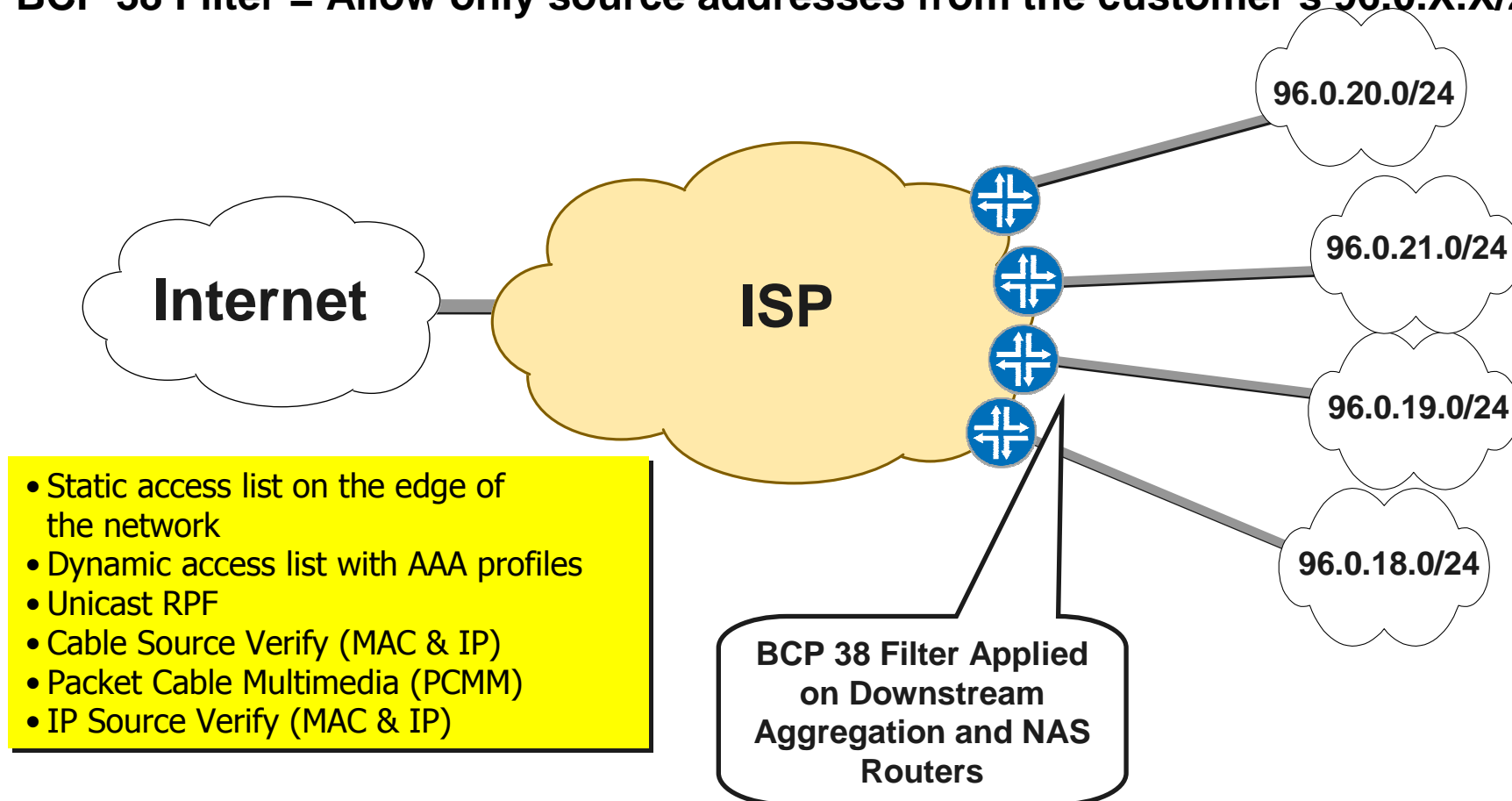
Sink Holes



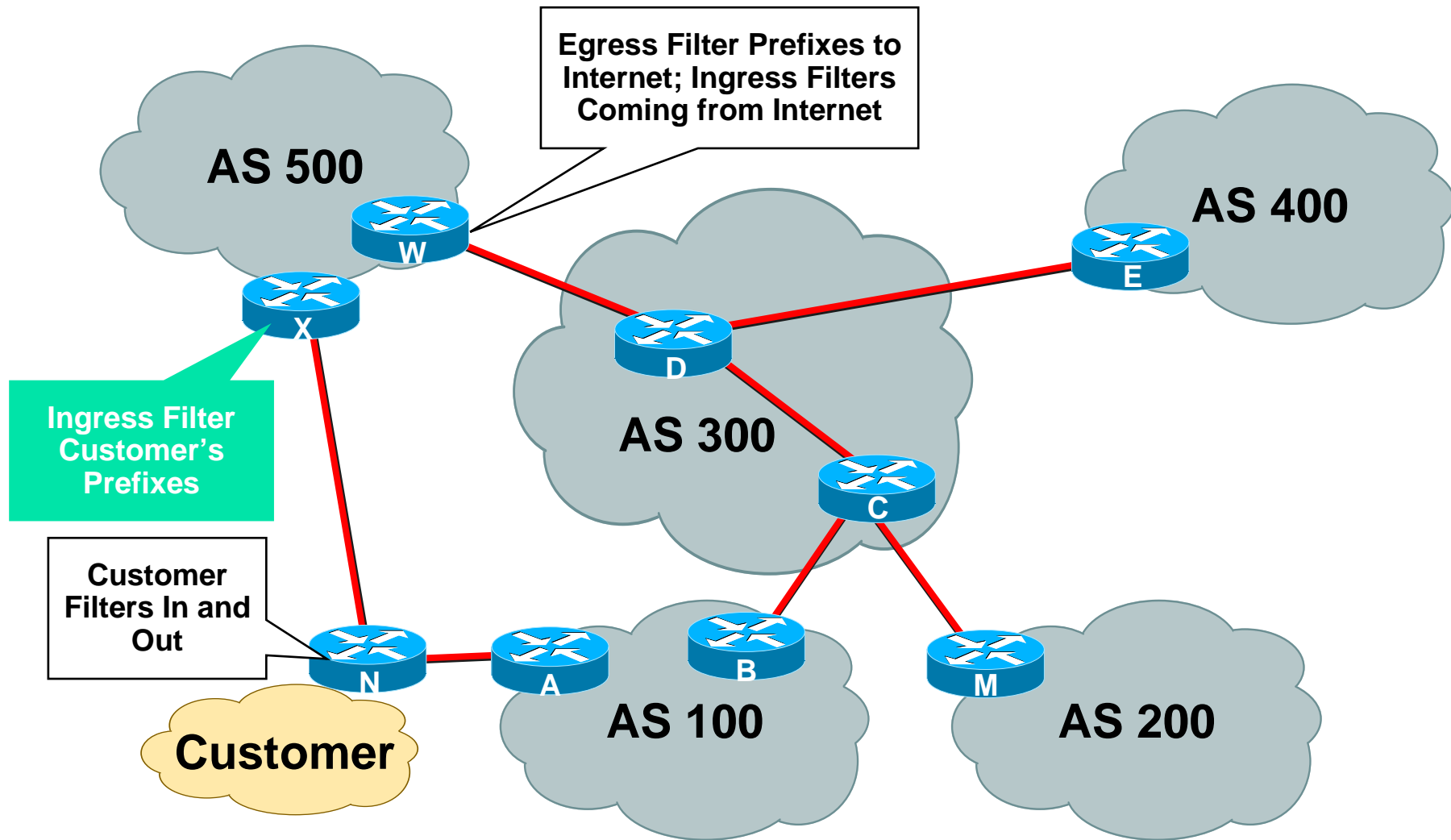
BCP 38 Ingress Packet Filtering

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



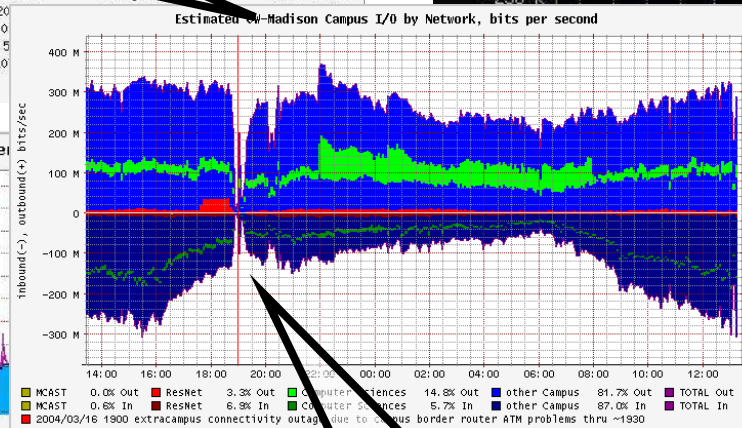
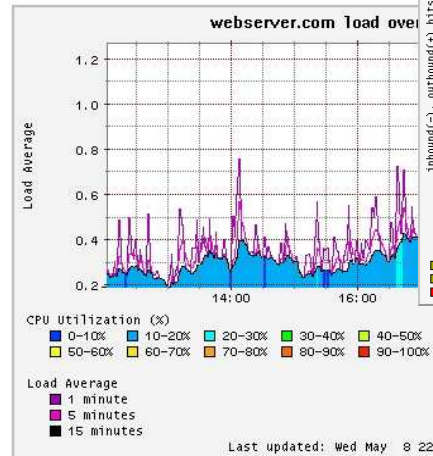
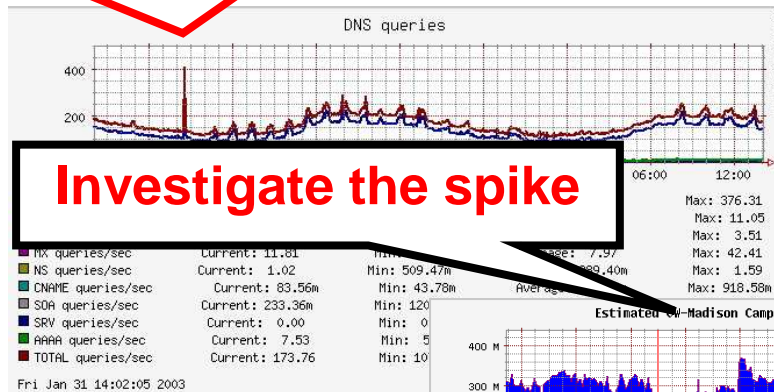
Where to Prefix Filter?



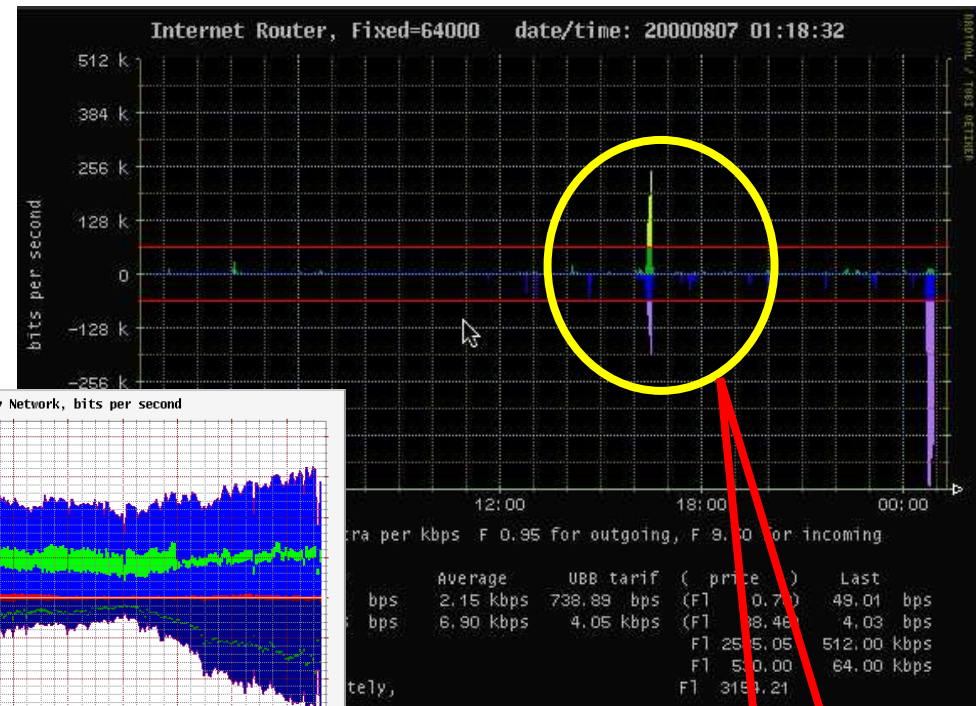
Total Visibility

Anomaly for DNS Queries

Investigate the spike



An identified cause of the outage



RTT Spike

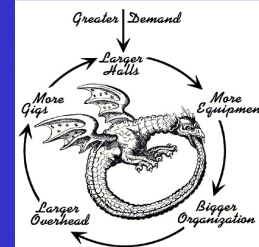
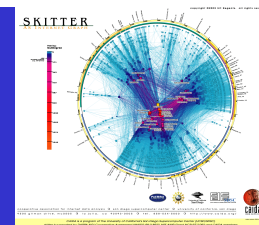
Source: <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>



What Really needs to be Done

- Consensus, Desire, but still in work
 - Core Hiding
 - Removed Coupled State Protection on Critical Infrastructure.
 - Architectural Approaches to Security
 - Re-Coloring (TOS/DSCP) at the Edge
 - Methodologies for effective SP oriented Risk Assessments.
- Working, but no Consensus
 - Common Services Ingress/Egress Port Blocking – (port 25, 53, 135, 139, 445)
 - DNS Poisoning

Prepare your NOC





SP's/ISP's NOC Team

- Every SP and ISP needs a NOC
- Anyone who has worked or run a NOC has their own list of what should be in a NOC
 - Make your own wish list
 - Talk to colleagues and get their list
 - Then try to make it happen
- No NOC is a perfect NOC—the result is always a ratio of time, money, skills, facilities, and manpower

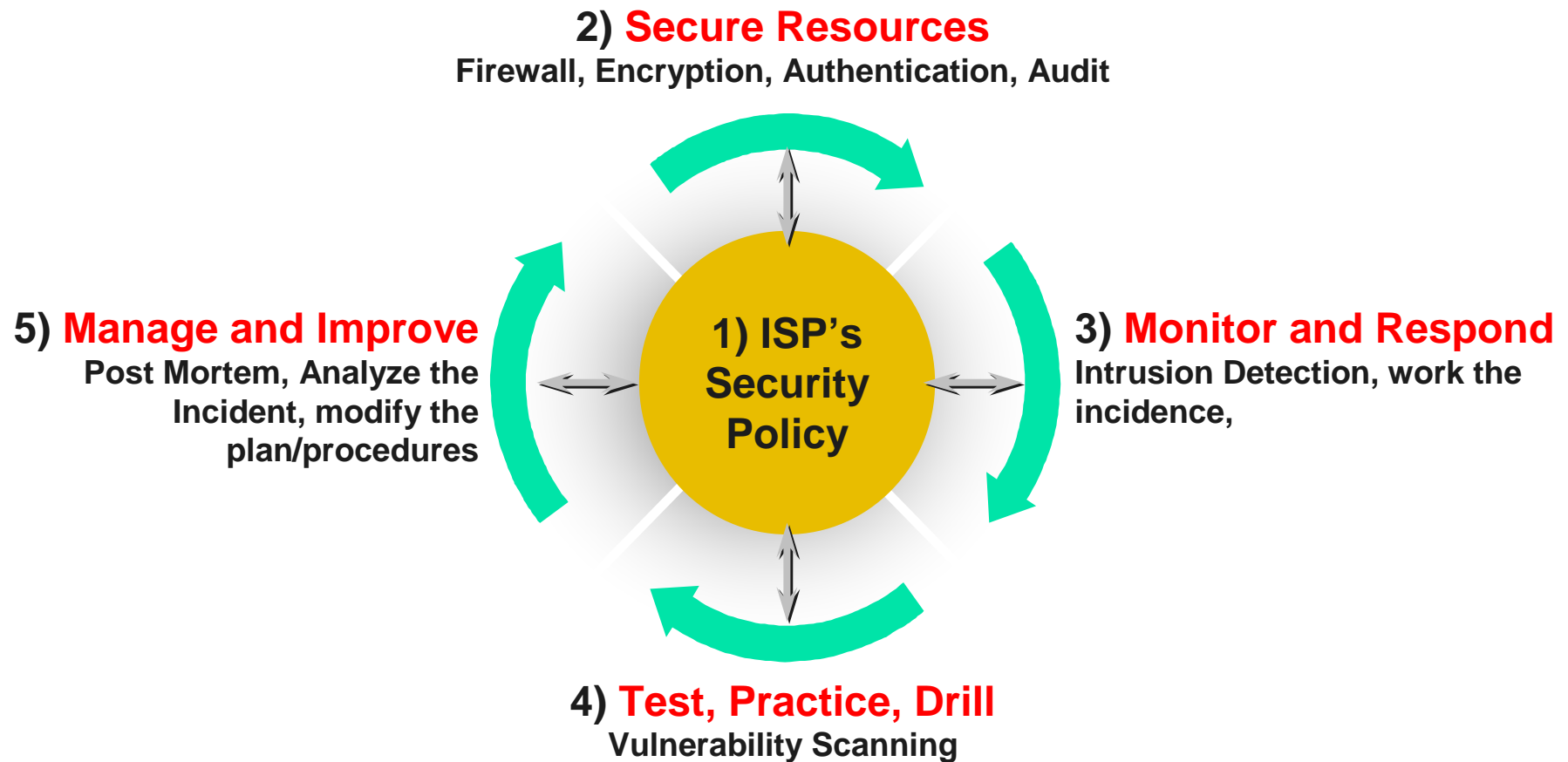


SP's/ISP's NOC Team

- An SP's/ISP's OPerational SECuriry Team can be:
 - A NOC escalation team
 - A sister to the NOC—reporting to operations
 - Integrated team with the NOC
- The OPSEC Team is a critical component of the day to day operations of a large IP Transit provider.

What Do ISPs Need to Do?

Security incidents are a normal part of an ISP's operations!



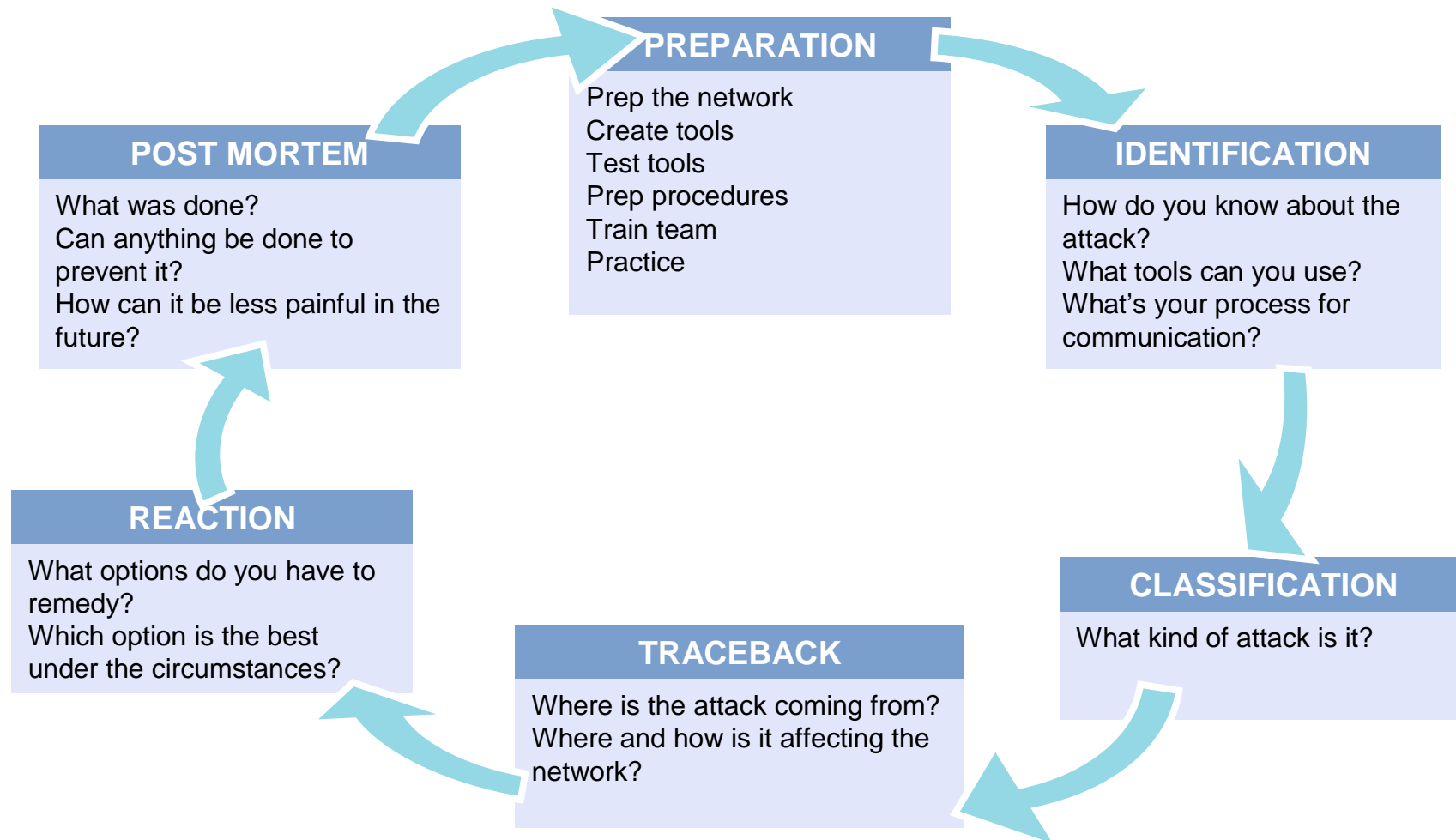
The Preparation Problem

- The problem - Most SP 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

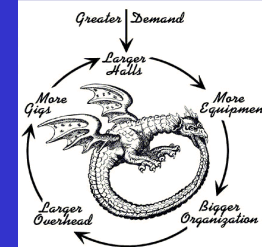
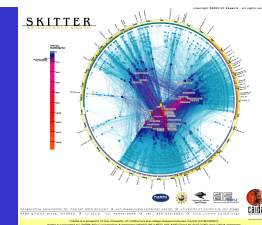




Six Phases of Incident Response



Mitigation Communities



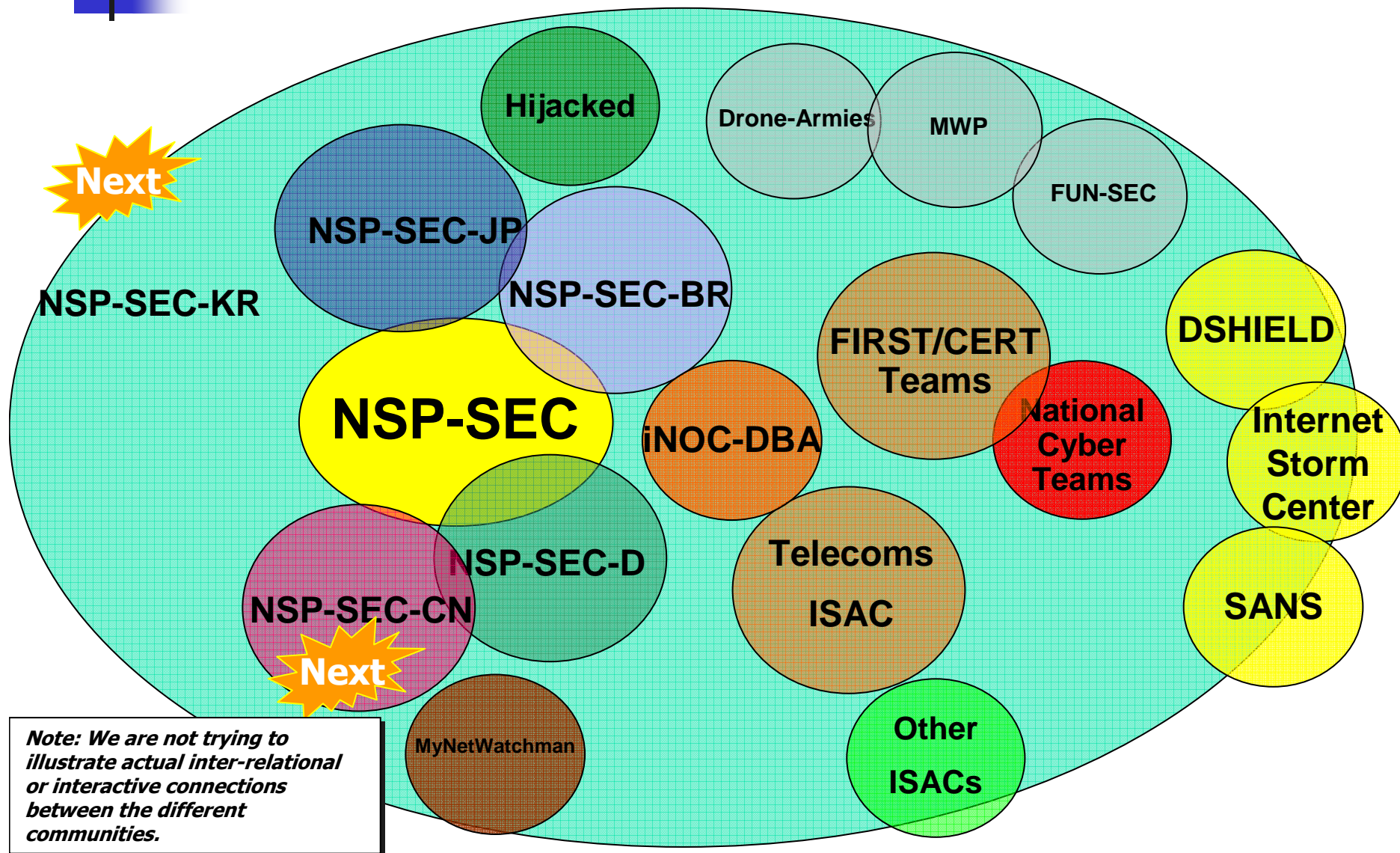


Check List



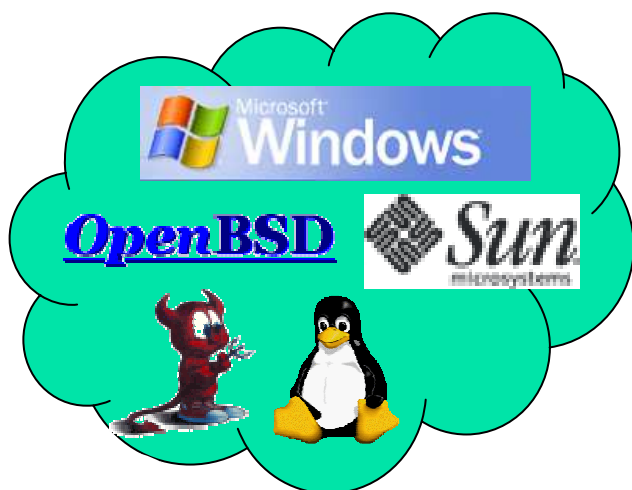
1. Essentials (see addendum slides)
2. DSHIELD
3. NSP-SEC
4. iNOC-DBA (next section)
5. Vendors (see addendum slides)
6. SP Peers and Upstreams (see addendum slides)
7. Customers (see addendum slides)
8. Law Enforcement (see addendum slides)

Aggressive Collaboration



DSHIELD

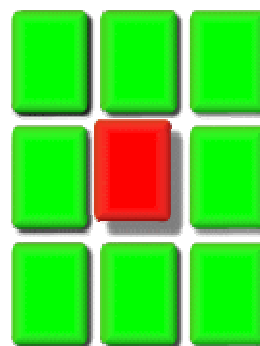
Data Collection



DSHield Users



Analysis

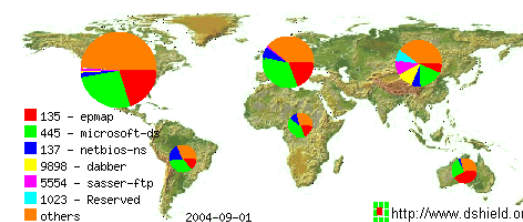


DSHield.org

Dissemination



Service Name	Port Number	30 day history	Explanation
epmap	135		DCE endpoint resolution
microsoft-ds	445		Win2k+ Server Message Block
netbios-ns	137		NETBIOS Name Service
dabber	9898		[trojan] Dabber Worm backdoor
sasser-ftp	5554		[trojan] Sasser Worm FTP Server
Reserved	1023		
ms-sql-s	1433		Microsoft-SQL-Server
ms-sql-m	1434		Microsoft-SQL-Monitor
netbios-ssn	139		NETBIOS Session Service
mydoom	3127		W32/MyDoom, W32/Novarg.A backdoor





NSP-SEC – The Details

- 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>



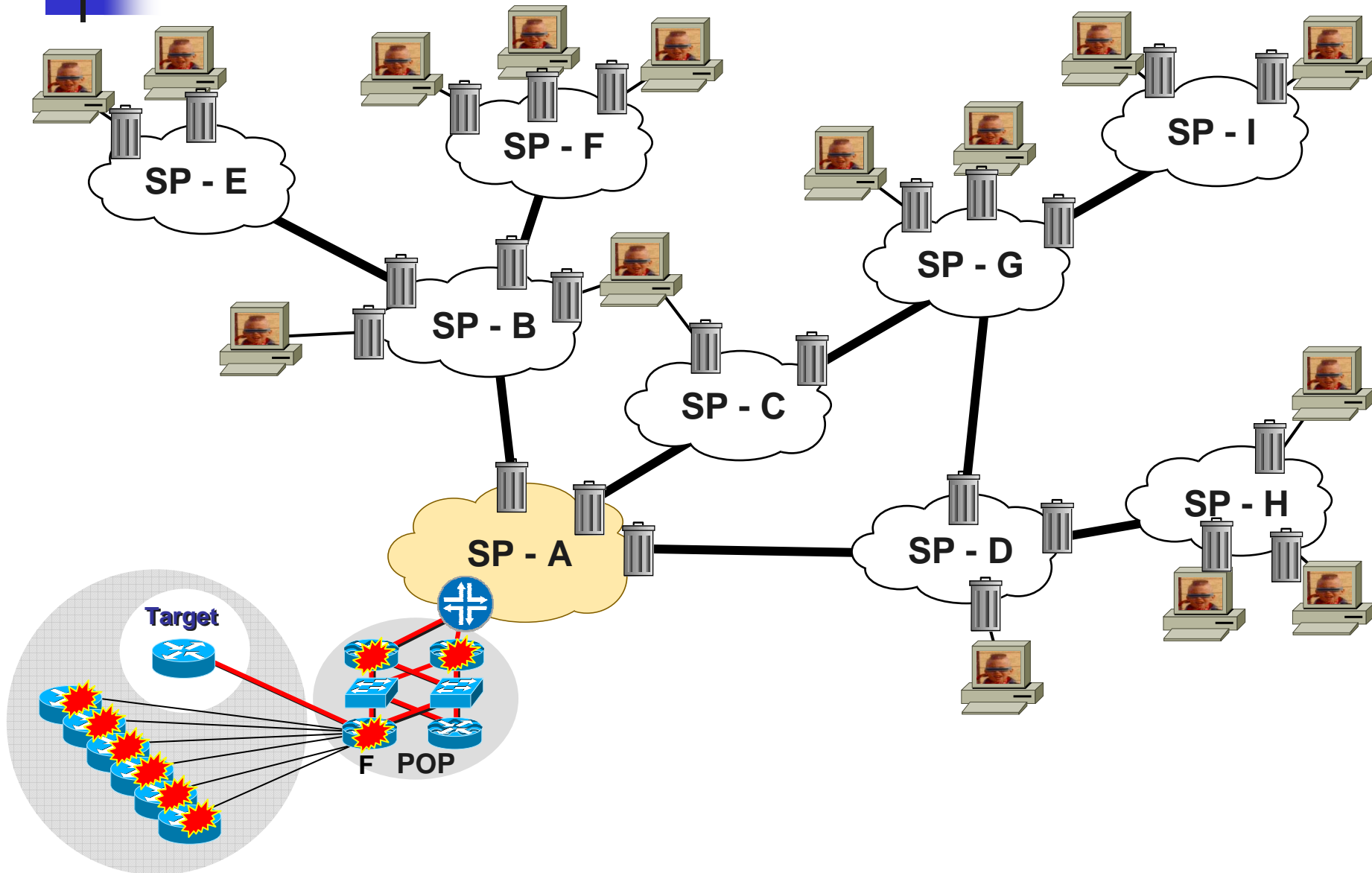
NSP-SEC: Daily DDOS Mitigation Work

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: Daily DDOS Mitigation Work





It is all about *Operational Trust*

Trust is a bet that an entity, which you cannot control, will meet expectations that are favorable to your cause.

Operational trust is the trust that is required from every person and earned by every entity to accomplish an endeavor.

- Lt Col Nicole Blatt



NSP-SEC's *Operational Trust*

- Inter-Provider Mitigation requires ***operation trust.***
 - You need to trust your colleagues to keep the information confidential, not use it for competitive gain, not tell the press, and not tell the commercial CERTS and *Virus* circus.
 - So all membership applications are reviewed by the NSP-SEC Administrators and Approved by the membership.
 - All memberships are reviewed and re-vetted every 6 months – letting the membership judge their peer's actions and in-actions.



NSP-SEC is not

- NSP-SEC is not perfect
- NSP-SEC is not to solve all the challenges of inter-provider security coordination
- NSP-SEC is not the *ultimate solution*.
- *But, NSP-SEC does impact the security of the Internet:*
 - Example: Slammer



NSP SEC Meetings

- NANOG Security BOFs (www.nanog.org)
Chaperons/Facilitators: Merike Kaeo - kaeo@merike.com
Barry Raveendran Greene bgreene@senki.org
Danny McPherson danny@arbor.net
- RIPE Security BOFs (www.ripe.net)
Coordinator: Hank Nussbacher - hank@att.net.il
- APRICOT Security BOFs (www.apricot.net)
Coordinators/Facilitators: Derek Tay - dt@agcx.net
Dylan Greene - dylan@juniper.net



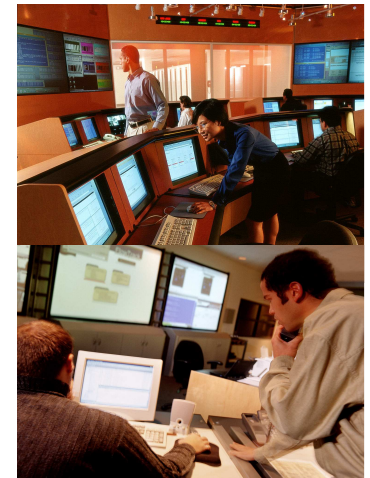
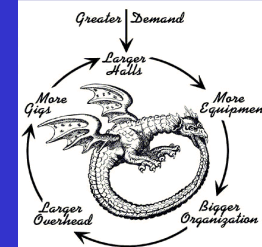
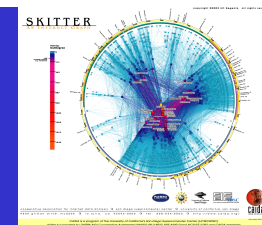
CERT & FIRST

- Find a CERT/FIRST Team to work with.
 - Important avenue of community communication - Forum of Incident Response and Security Teams
 - Consider becoming a FIRST Member.
 - Protect yourself - SP RFPs need to require FIRST/CERT Membership.



<http://www.first.org/about/organization/teams/>

iNOC DBA





Check List



- Get a SIP Phone or SIP Based soft phone.
- Sign up to iNOC-DBA
 - <http://www.pch.net/inoc-dba/>
- Find a couple of peers and try it out.



What is the problem?

- SPs needed to talk to each other in the middle of the attack.
- Top Engineers inside SPs 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
- SIP Based VoIP system, managed by www.pch.net

Is set up difficult?

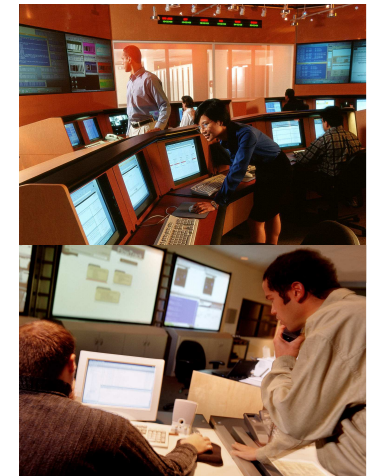
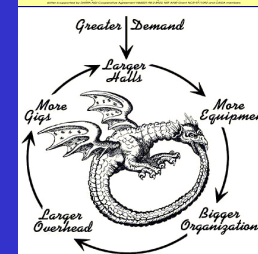
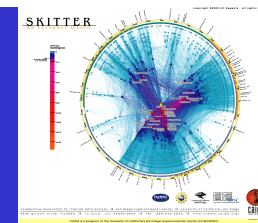




How is iNOC being used today?

- Used during attacks like Slammer
 - Barry was using his iNOC phone at home to talk to SPs in the early hours of Slammer to peers in their homes.
- 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 – SP Engineers working on inter-SP issues.

Point Protection



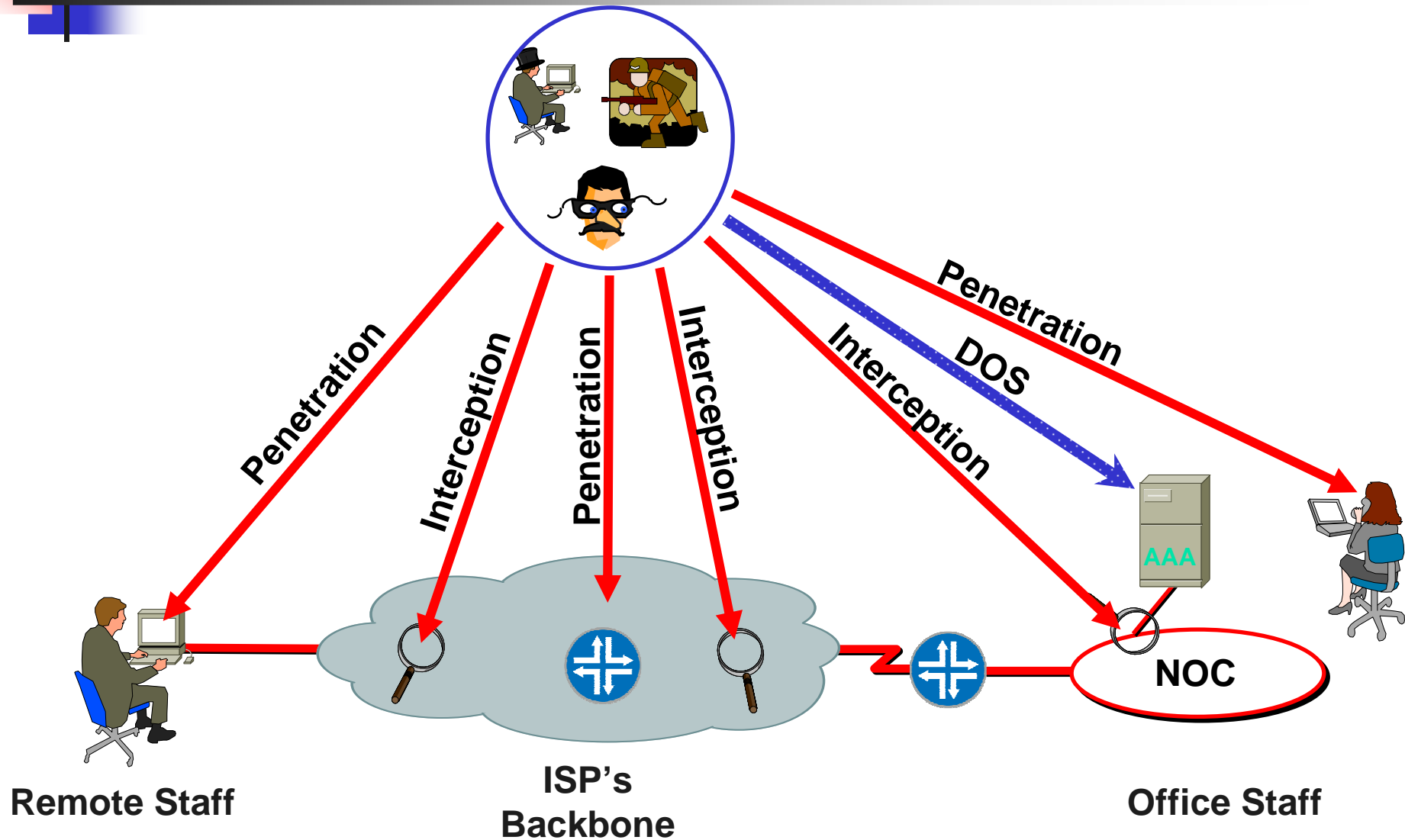


Check List

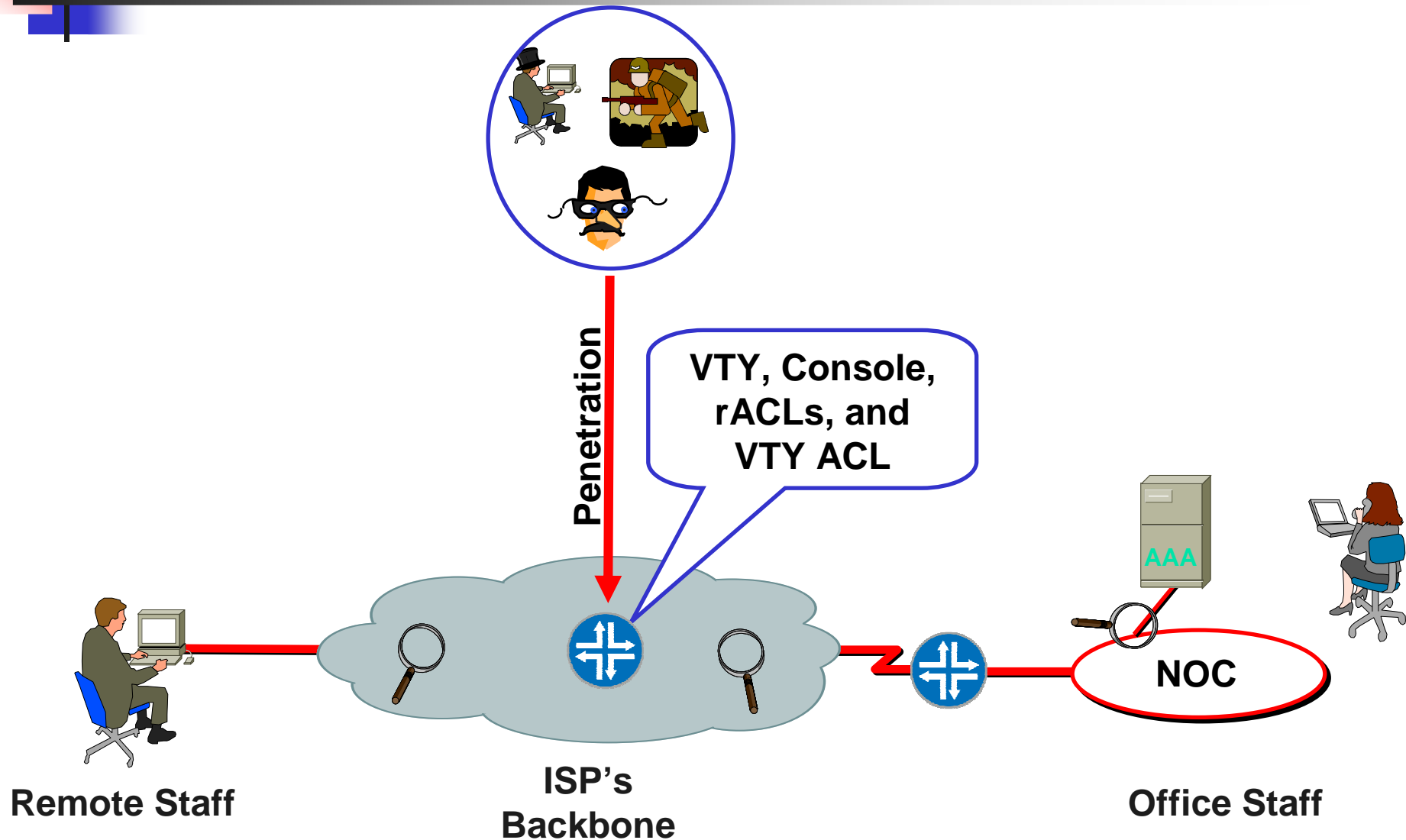


- AAA to the Network Devices
- Controlling Packets Destined to the Network Devices
- Config Audits

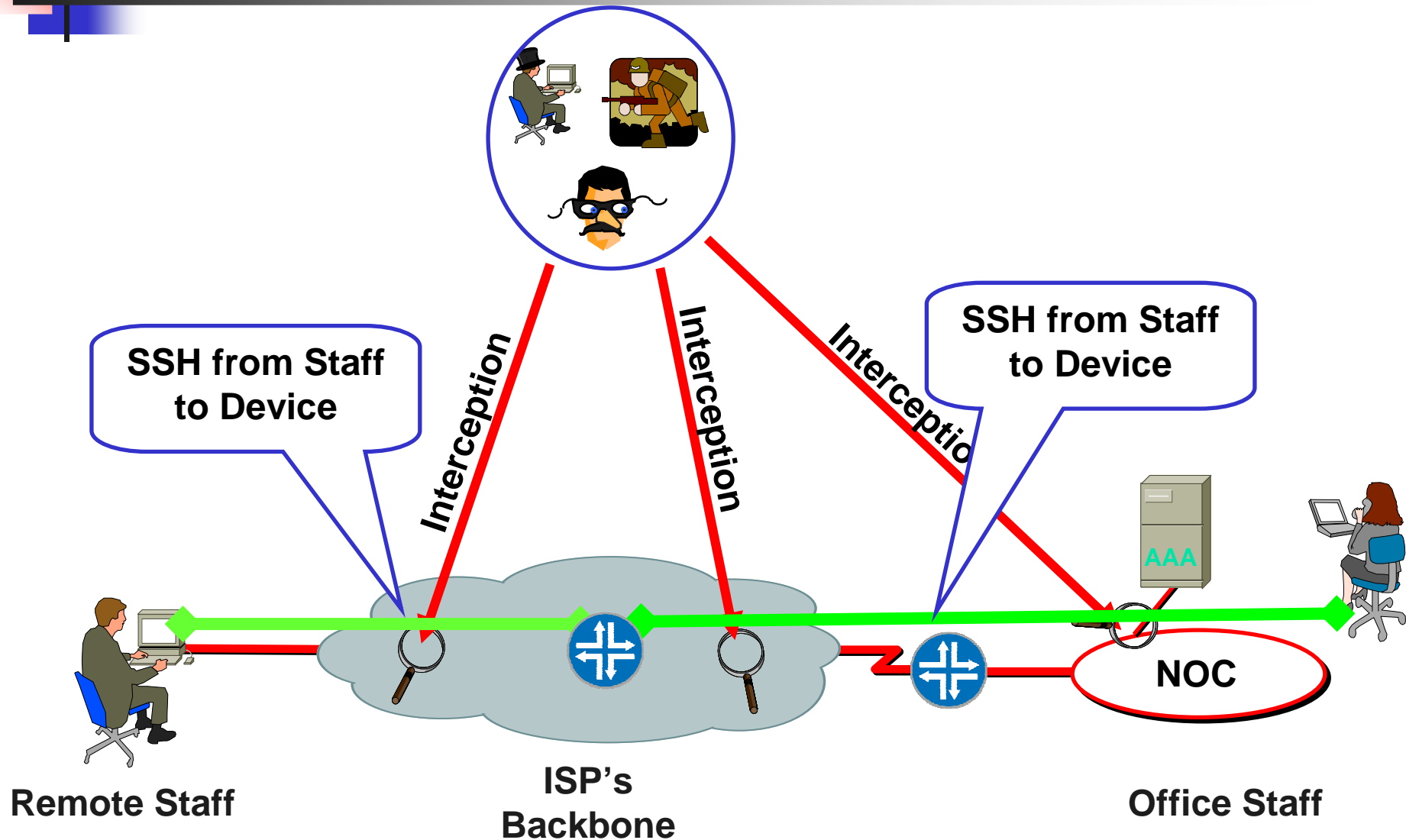
RISK Assessment



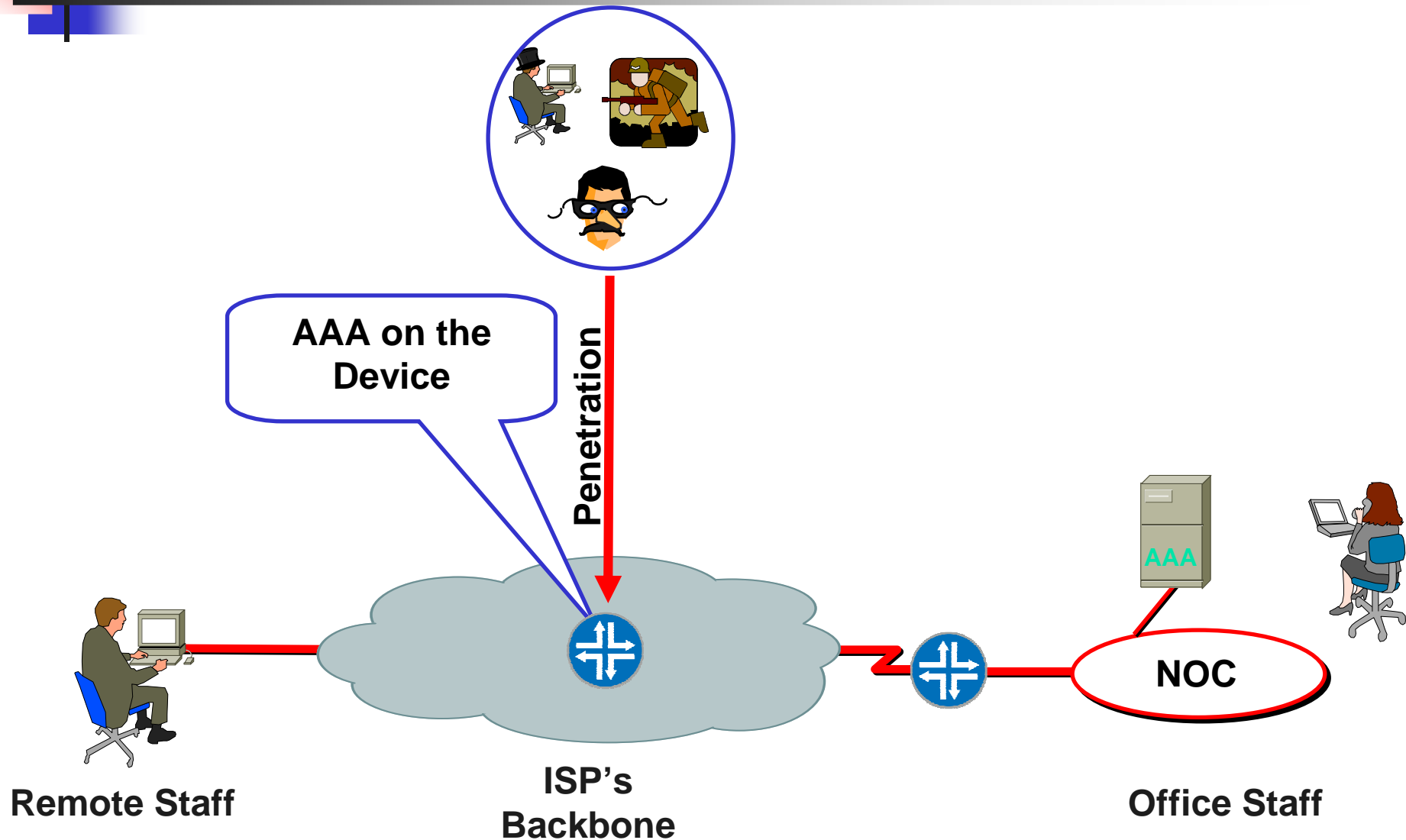
Lock Down the VTY and Console Ports



Encrypt the Traffic from Staff to Device

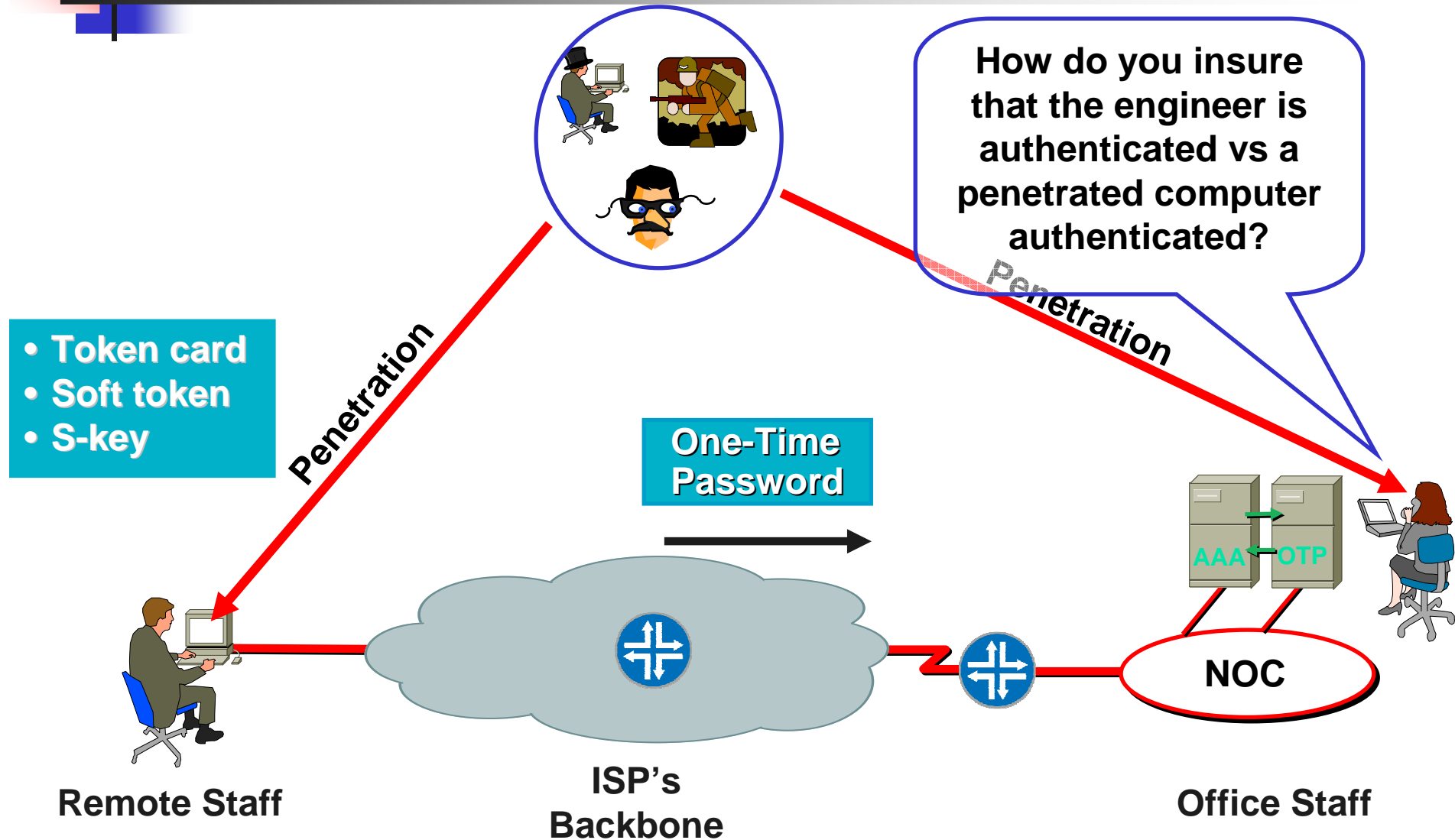


Staff AAA to get into the Device

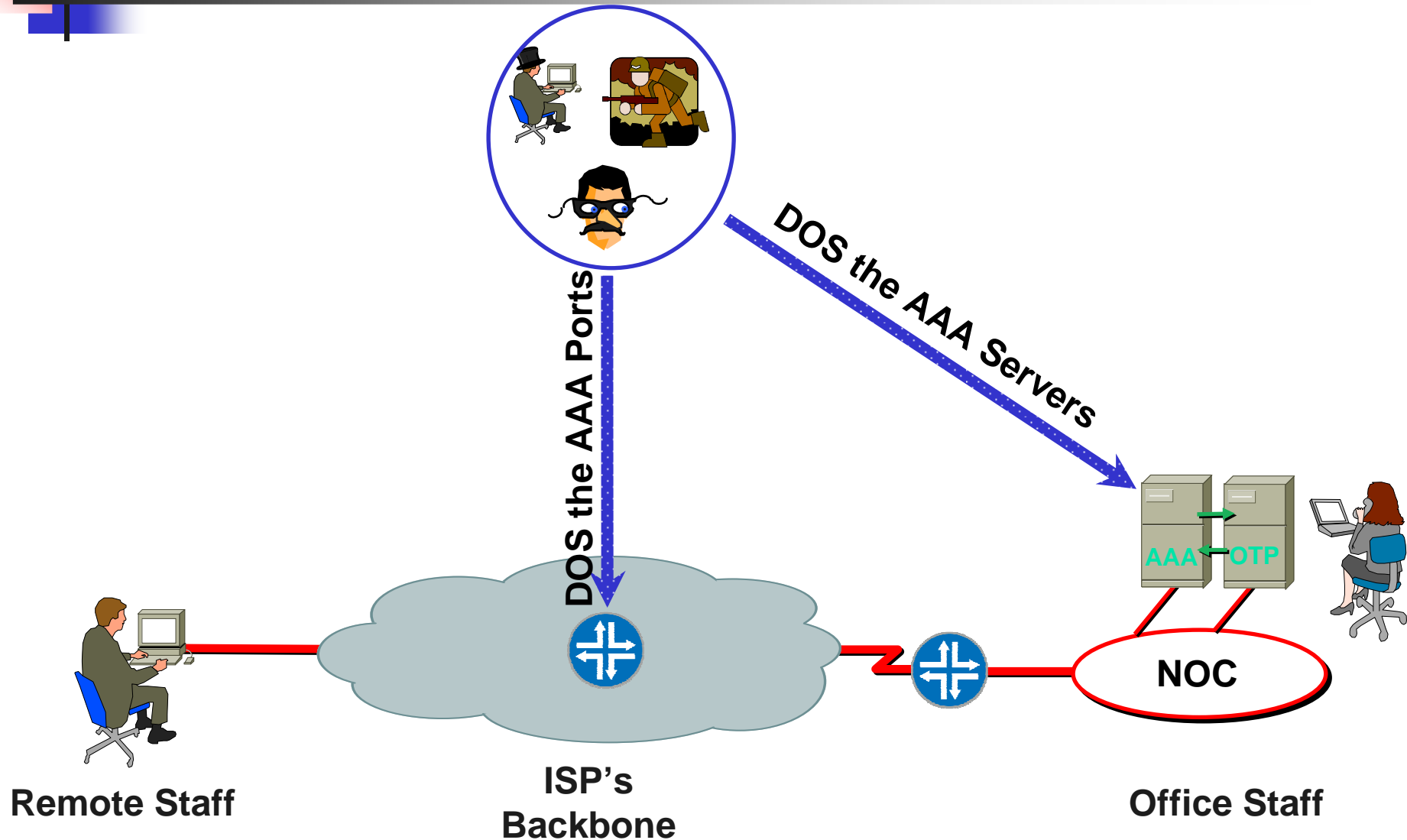




One Time Password – Checking the ID

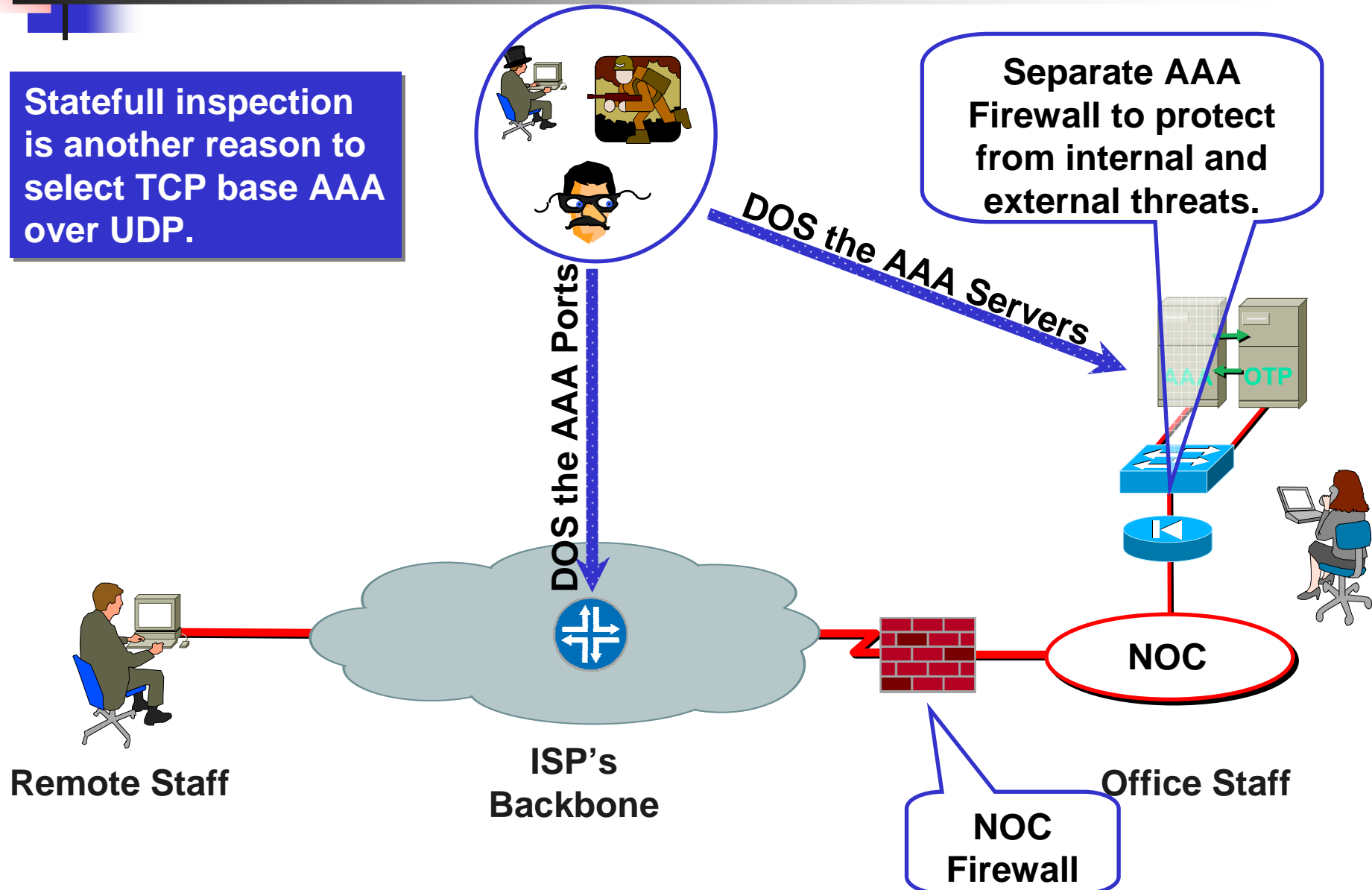


DOSing the AAA Infrastructure

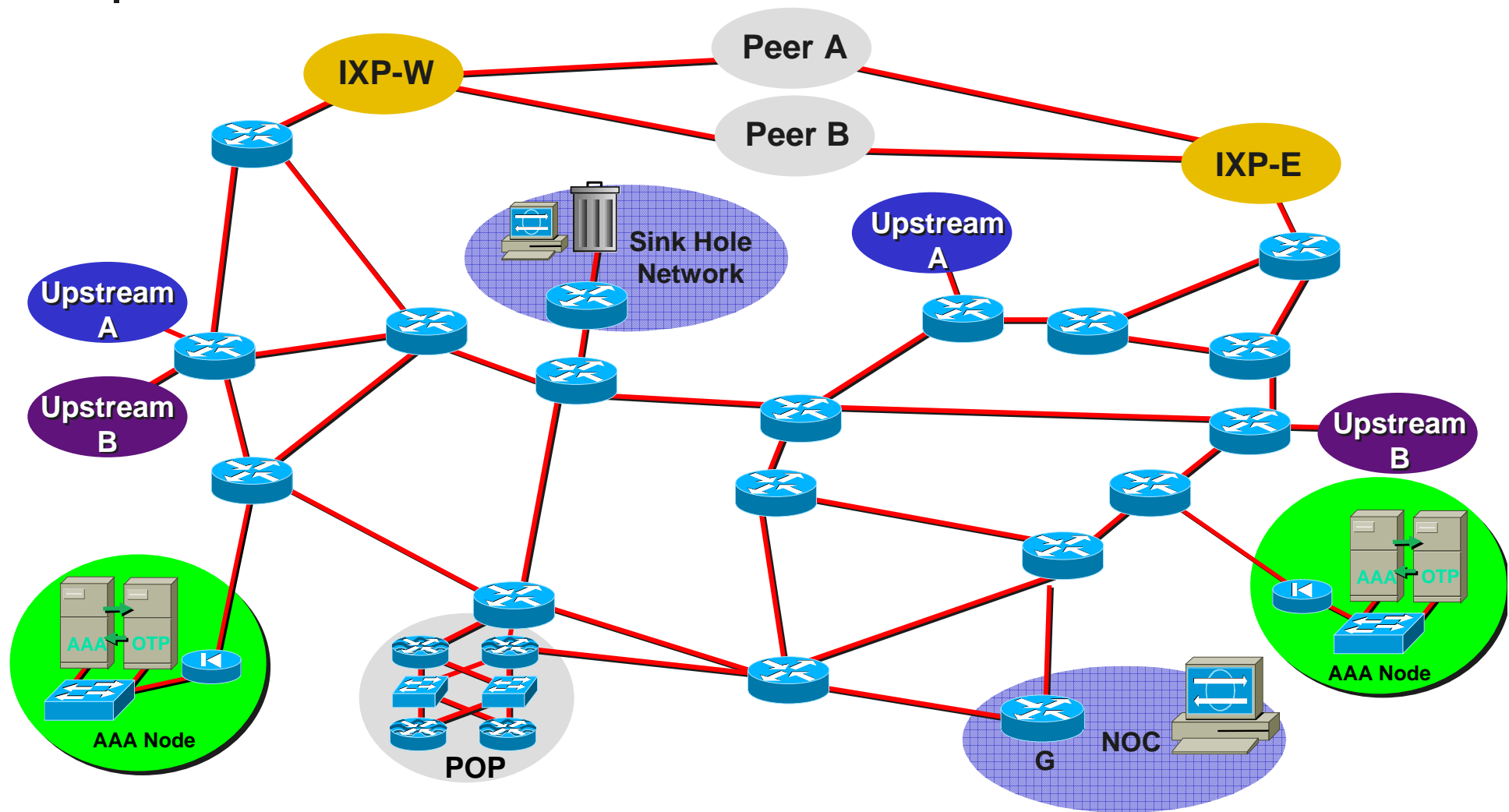


Use a Firewall to Isolate the AAA Servers

Statefull inspection is another reason to select TCP base AAA over UDP.



Distribute AAA Servers and Config Backup

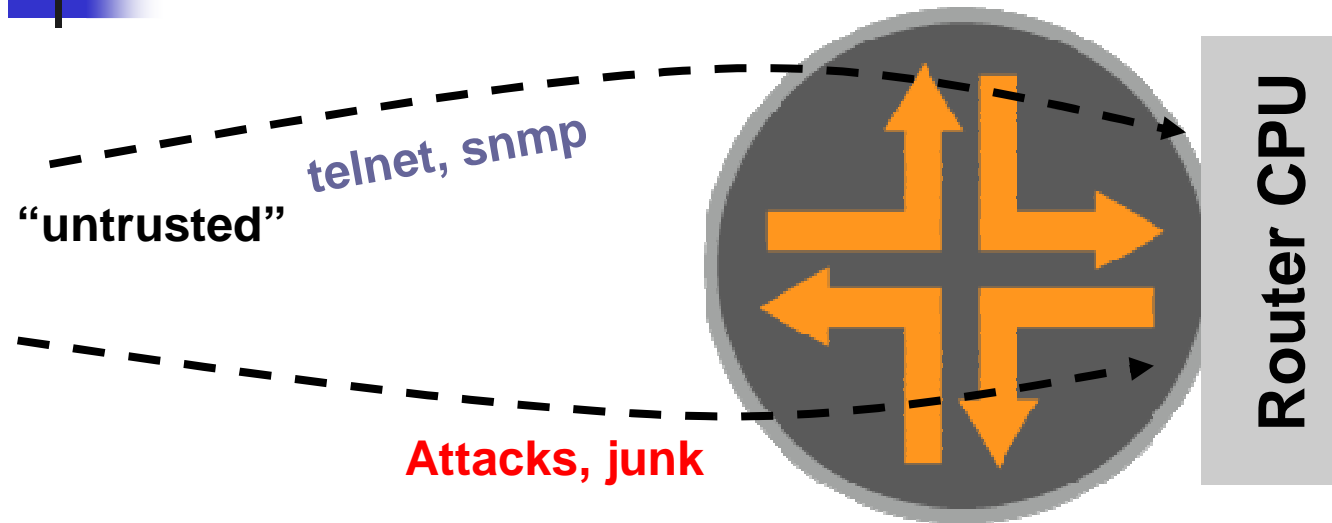




TACACS+ URLs

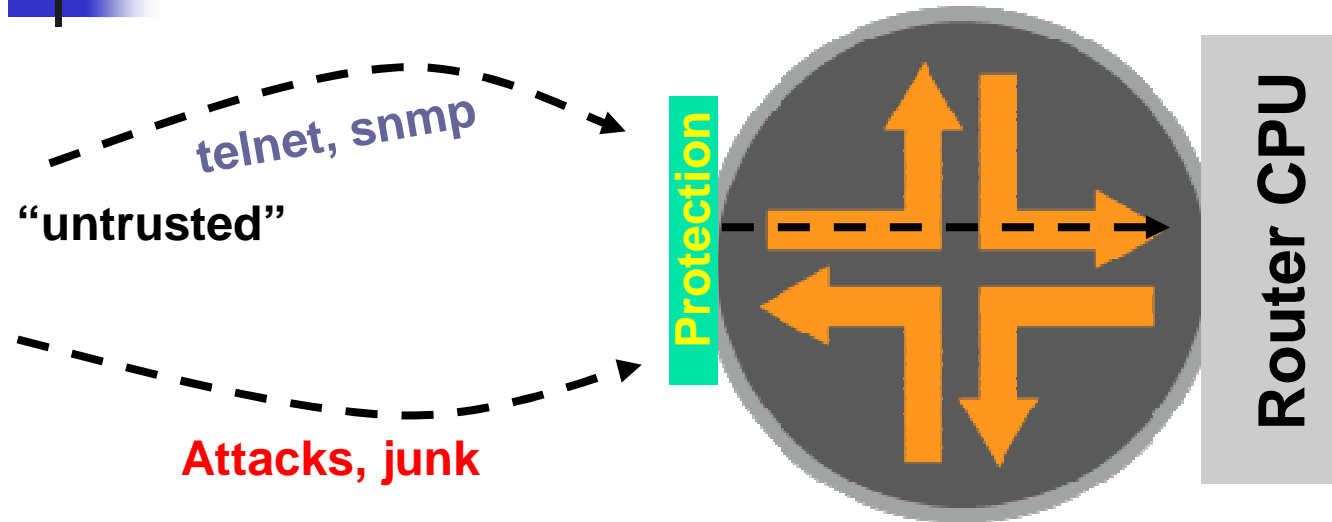
- TACACS+ Open Source
 - <ftp://ftp-eng.cisco.com/pub/tacacs/>
 - Includes the IETF Draft, Source, and Specs.
- Extended TACACS++ server
 - <http://freshmeat.net/projects/tacpp/>
- TACACS + mods
 - http://www.shrubbery.net/tac_plus/

The Old World: Router Perspective



- Policy enforced at process level (VTY ACL, Kernel ACL, SNMP ACL, etc.)
- Some early features such as ingress ACL used when possible

The New World: Router Perspective



- Central policy enforcement, prior to process level
- Granular protection schemes
- On high-end platforms, hardware implementations



Watch the Config!

- There has been many times where the only way you know someone has violated the router is that a config has changed.
- If course you need to be monitoring your configs.

Config Monitoring



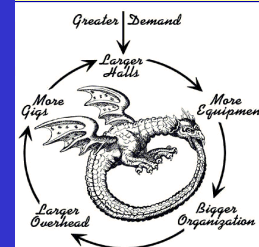
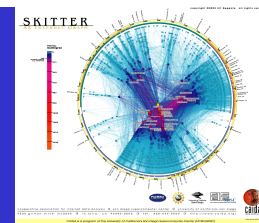
- **RANCID - Really Awesome New Cisco config Differ (but works with lots of routers – used a lot with Juniper Routers)**

<http://www.shrubbery.net/rancid/>

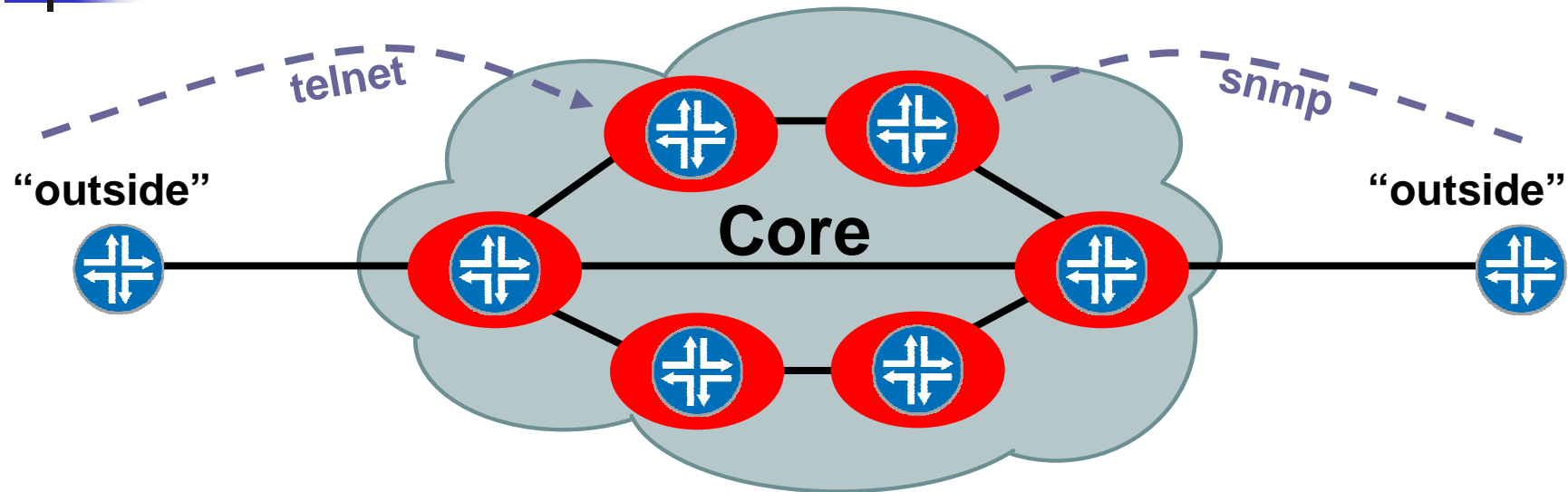
<http://www.nanog.org/mtg-0310/rancid.html>

- **Rancid monitors a device's configuration (software & hardware) using CVS.**
- **Rancid logs into each of the devices in the device table file, runs various show commands, processes the output, and emails any differences from the previous collection to staff.**

Edge Protection

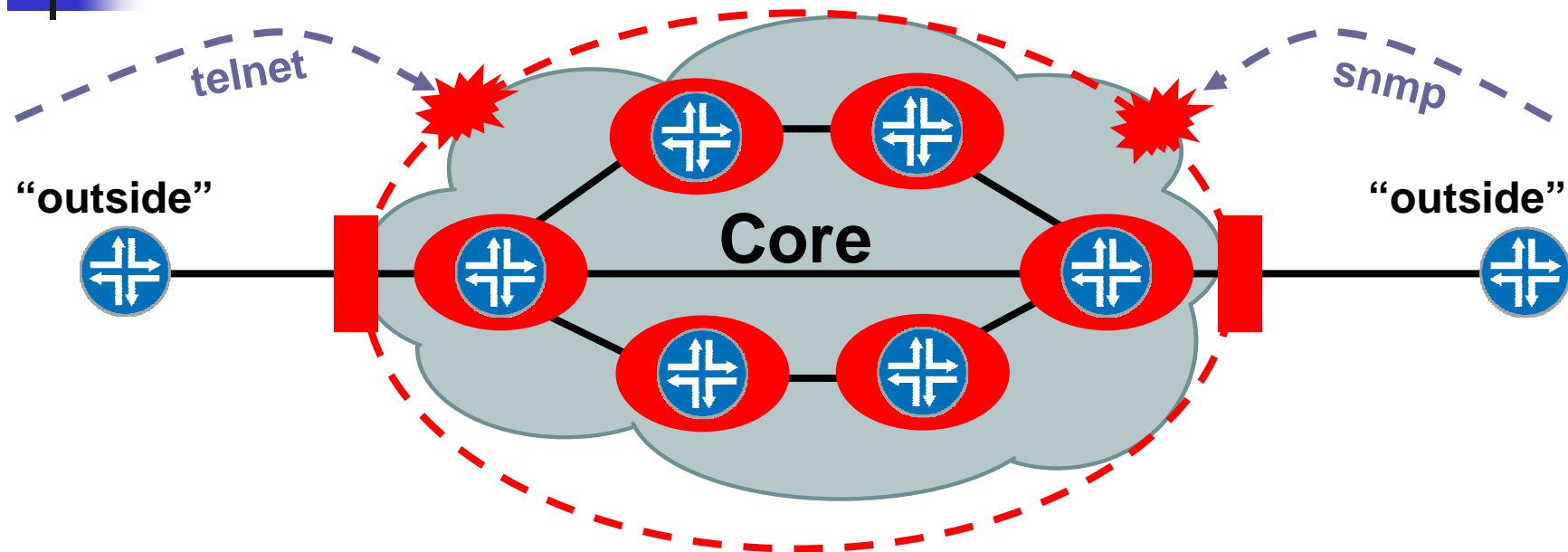


The Old World: Network Edge



- Core routers individually secured
- Every router accessible from outside

The New World: Network Edge



- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside



Infrastructure ACLs

- Basic premise: filter traffic destined TO your core routers
 - Do your core routers really need to process all kinds of garbage?
- Develop list of required protocols that are sourced from outside your AS and access core routers
 - Example: eBGP peering, GRE, IPSec, etc.
 - Use classification ACL as required
- Identify core address block(s)
 - This is the protected address space
 - Summarization is critical → simpler and shorter ACLs



Infrastructure ACLs

- Infrastructure ACL will permit only required protocols and deny ALL others to infrastructure space
- ACL should also provide anti-spoof filtering
 - Deny your space from external sources
 - Deny RFC1918 space
 - Deny multicast sources addresses (224/4)
 - RFC3330 defines special use IPv4 addressing



Digression: IP Fragments

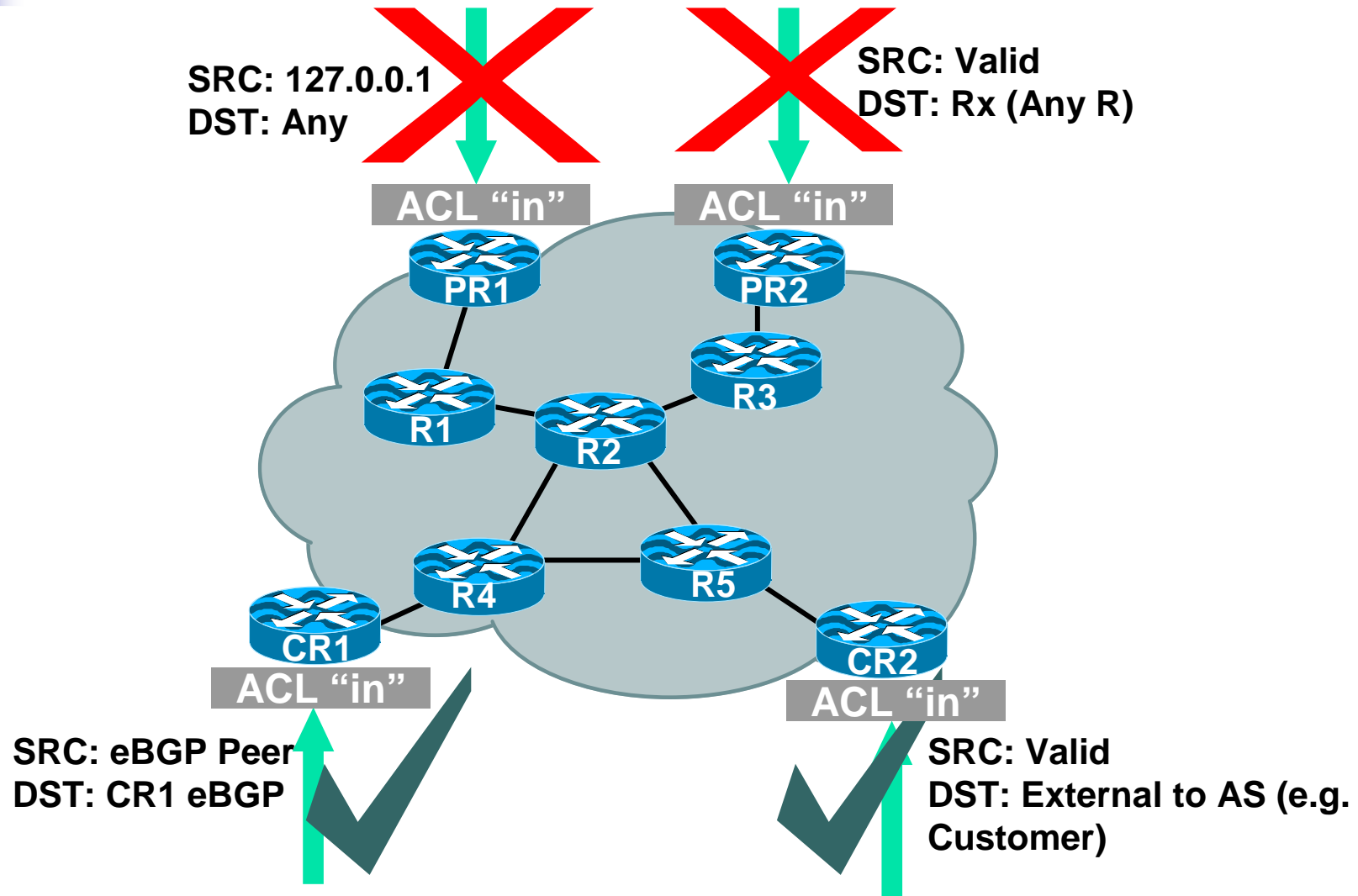
- Fragmented Packets can cause problems...
 - Fragmented packets can be used as an attack vector to bypass ACLs
 - Fragments can increase the effectiveness of some attacks by making the recipient consume more resources (CPU and memory) due to fragmentation reassembly
- Reality Check – Routers & Switches should not be receiving fragments!
 - In today's networks, management & control plane traffic should not be fragmenting.
 - If it does, it means something is BROKE or someone is attacking you.
- Recommendation – Filter all fragments to the management & control plane ... logging to monitor for errors and attacks.



Infrastructure ACLs

- Infrastructure ACL must permit transit traffic
 - Traffic passing through routers must be allowed via permit IP any any
- iACL is applied inbound on ingress interfaces
- Fragments destined to the core can be filtered via the iACL

Infrastructure ACL in Action





Iterative Deployment

- Typically a very limited subset of protocols needs access to infrastructure equipment
- Even fewer are sourced from outside your AS
- Identify required protocols via classification ACL
- Deploy and test your iACLs



Step 1: Classification

- Traffic destined to the core must be classified
- NetFlow can be used to classify traffic
 - Need to export and review
- Classification ACL can be used to identify required protocols
 - Series of permit statements that provide insight into required protocols
 - Initially, many protocols can be permitted, only required ones permitted in next step
 - ACL Logging can be used for additional detail; hits to ACL entry with *logging might increase CPU utilization*: impact varies by vendor/platform
- Regardless of method, unexpected results should be carefully analyzed → **do not permit protocols that you can't explain!**



Step 2: Begin to Filter

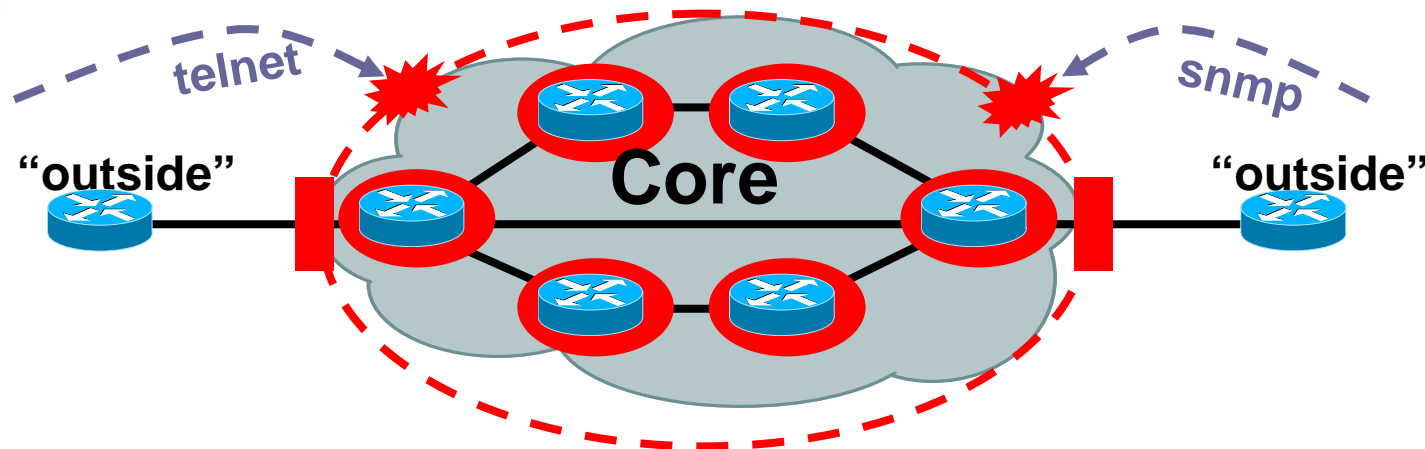
- Permit protocols identified in step 1 to infrastructure only address blocks
- Deny all other to addresses blocks
 - Watch access control entry (ACE) counters
 - ACL logging can help identify protocols that have been denied but are needed
- Last line: permit anything else ← permit transit traffic
- The iACL now provides basic protection and can be used to ensure that the correct suite of protocols has been permitted



Steps 3 & 4: Restrict Source Addresses

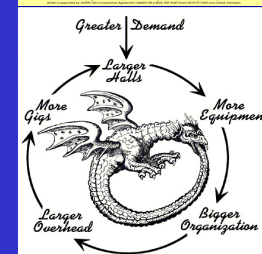
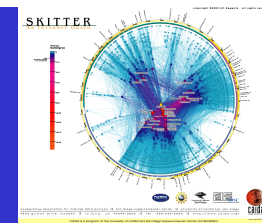
- Step 3:
 - ACL is providing basic protection
 - Required protocols permitted, all other denied
 - Identify source addresses and permit only those sources for requires protocols
 - e.g., external BGP peers, tunnel end points
- Step 4:
 - Increase security: deploy destination address filters if possible

Infrastructure ACLs



- Edge "shield" in place
- Not perfect, but a very effective first round of defense
 - Can you apply iACLs everywhere?
 - What about packets that you cannot filter with iACLs?
 - Hardware limitations
- Next step: secure the control/management planes per box

Remote Trigger Black Hole

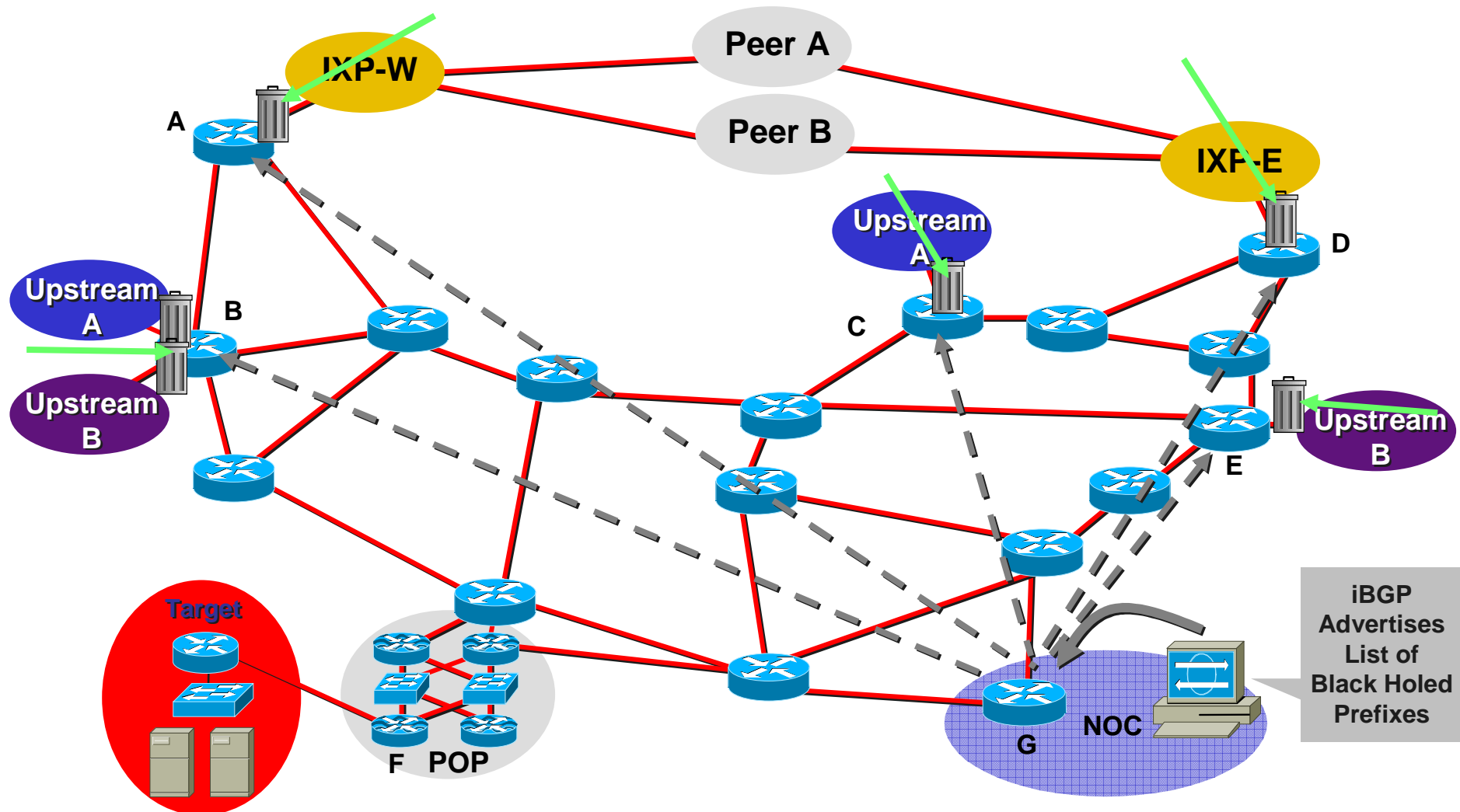




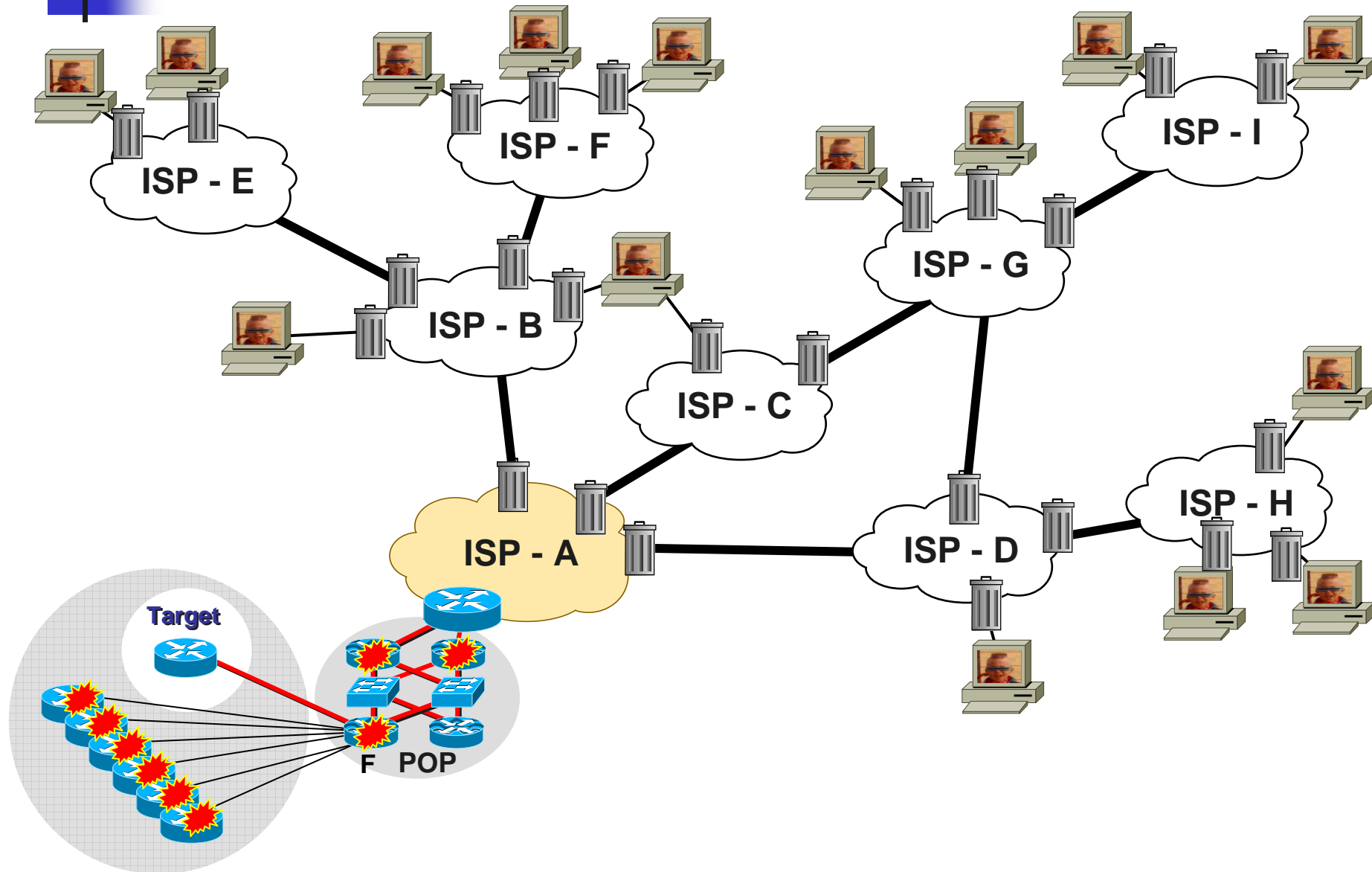
Remotely Triggered Black Hole Filtering

- We use BGP to trigger a network wide response to a range of attack flows.
- A simple static route and BGP will allow an SP to trigger network wide black holes as fast as iBGP can update the network.
- This provides SPs a tool that can be used to respond to security related events or used for DOS/DDOS Backscatter Tracebacks.

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



Inter-Provider Mitigation

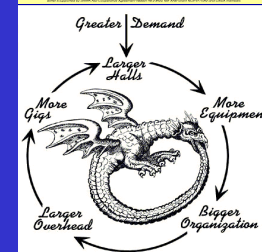
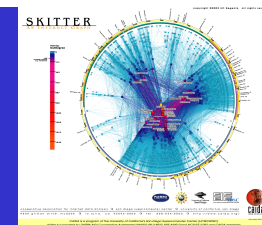




What can you do to help?

- 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)
 - Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", RFC 3882, September 2004.

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)
 - <http://www.nanog.org/mtg-0306/sink.html>



Why *Sinkhole*?

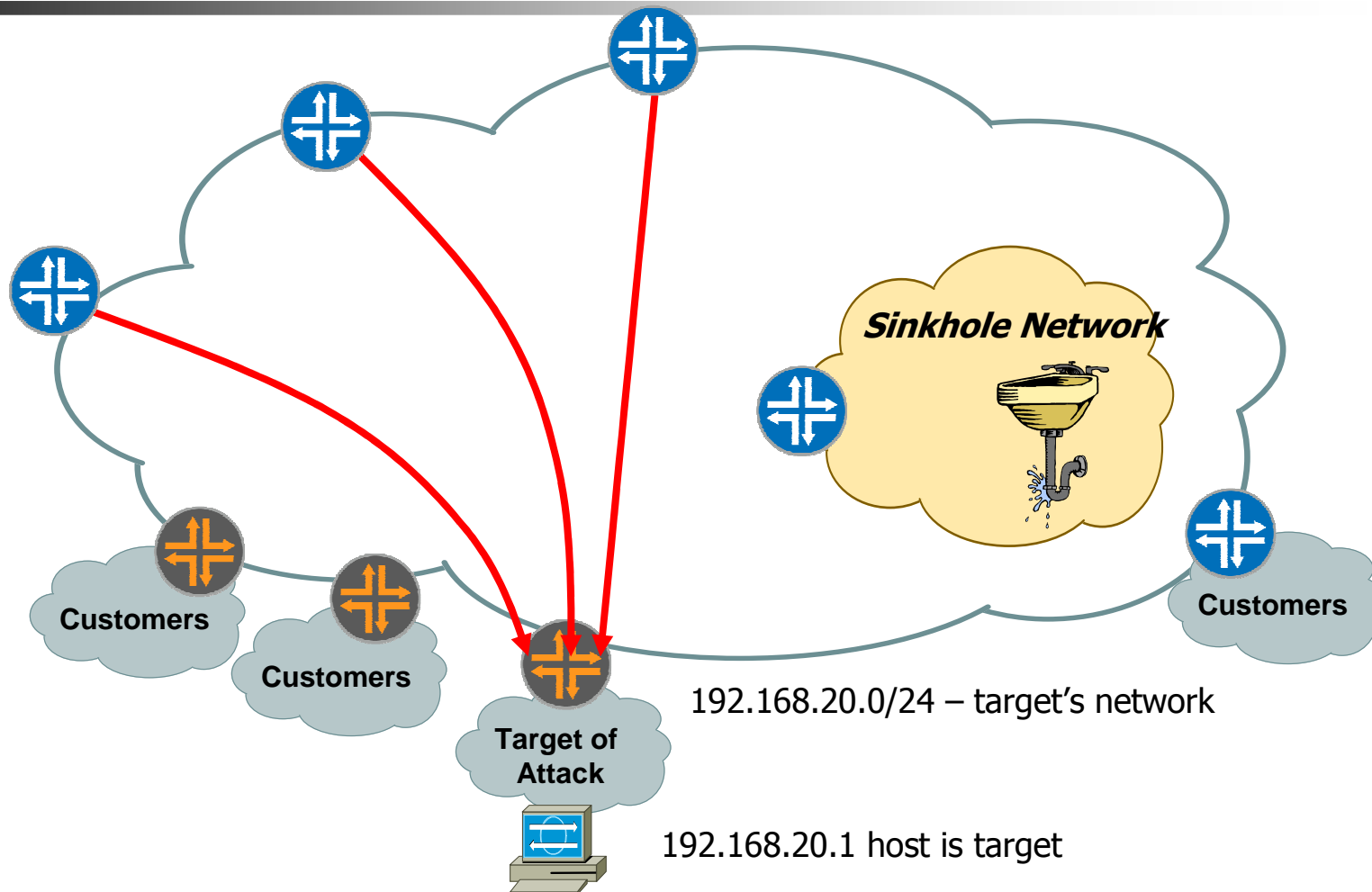
- Sinkhole is used to describe a technique that does more than the individual tools we've had in the past:
 - **Blackhole Routers** – Technique used to exploit a routers forwarding logic in order to discard data, typically in a distributed manner, triggered by routing advertisements.
 - **Tar Pits** – A section of a honey net or DMZ designed to slow down TCP based attacks to enable analysis and traceback. Often used interchangeably with Sinkhole.
 - **Shunts** – Redirecting traffic to one of the router's connected interfaces, typically to discard traffic.
 - **Honey Net** – A network of one or more systems designed to analyze and capture penetrations and similar malicious activity.
 - **Honey Pot** - A system designed to analyze and capture penetrations and similar malicious activity.



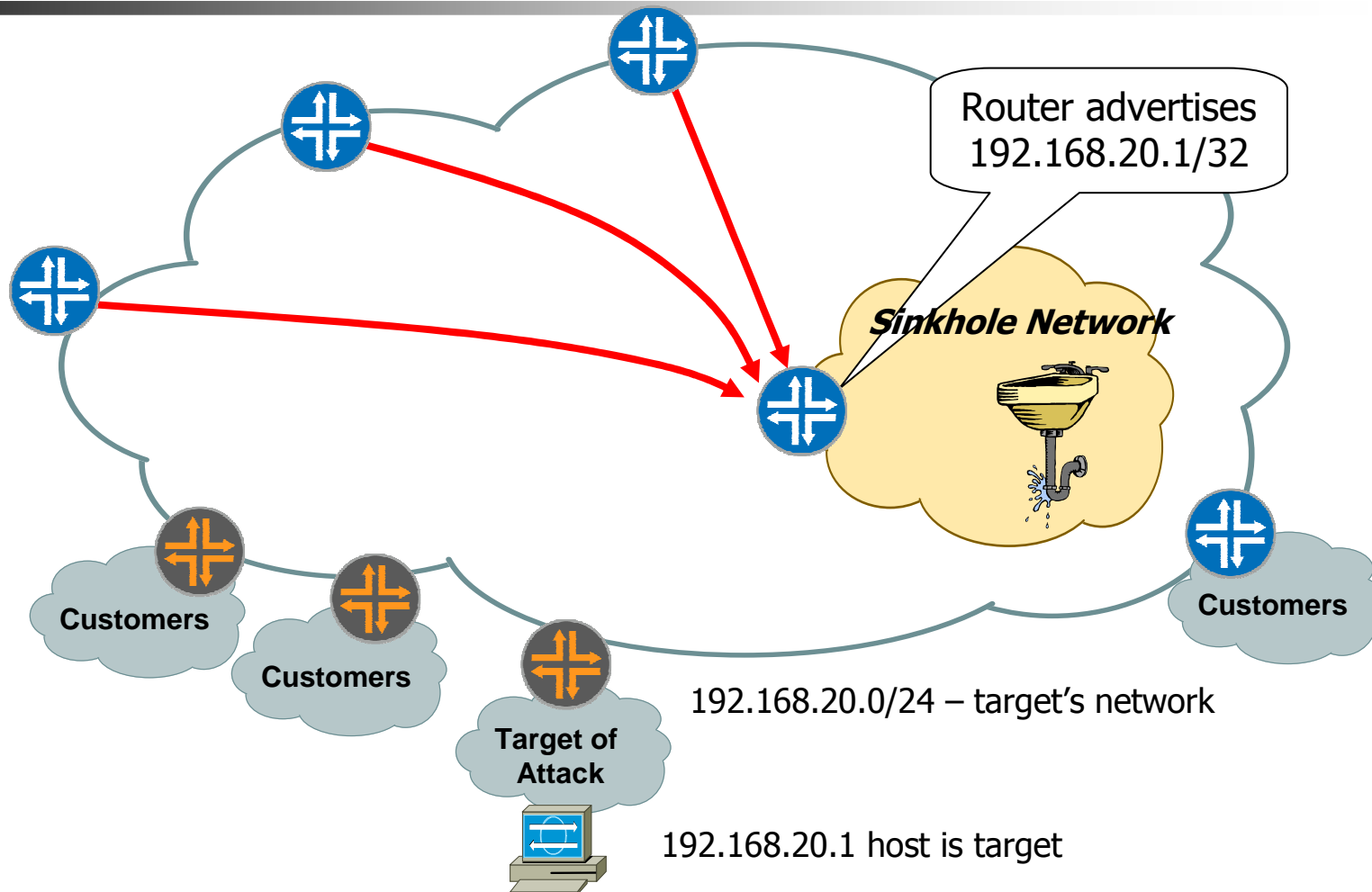
Sinkhole Routers/Networks

- Sinkholes are the network equivalent of a ***honey pot***, also commonly referred to as a ***tar pit***, sometimes referred to as a ***blackhole***.
 - Router or workstation built to *suck in* and assist in analyzing attacks.
 - Used to redirect attacks away from the customer – working the attack on a router built to withstand the attack.
 - Used to monitor *attack noise, scans, data from mis-configuration* and other activity (via the advertisement of default or unused IP space)
 - Traffic is typically diverted via BGP route advertisements and policies.

Sinkhole Routers/Networks

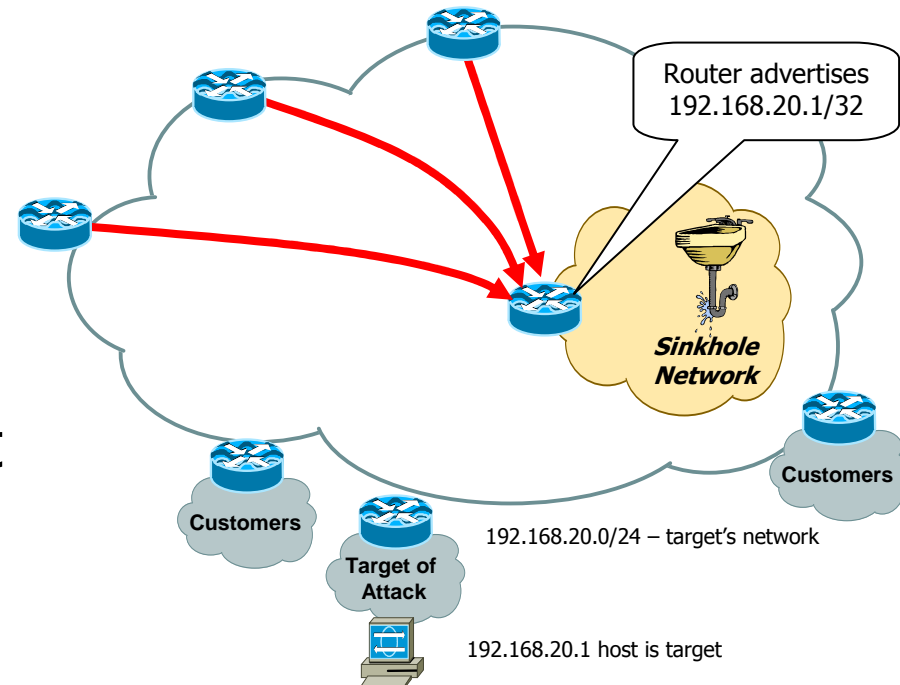


Sinkhole Routers/Networks

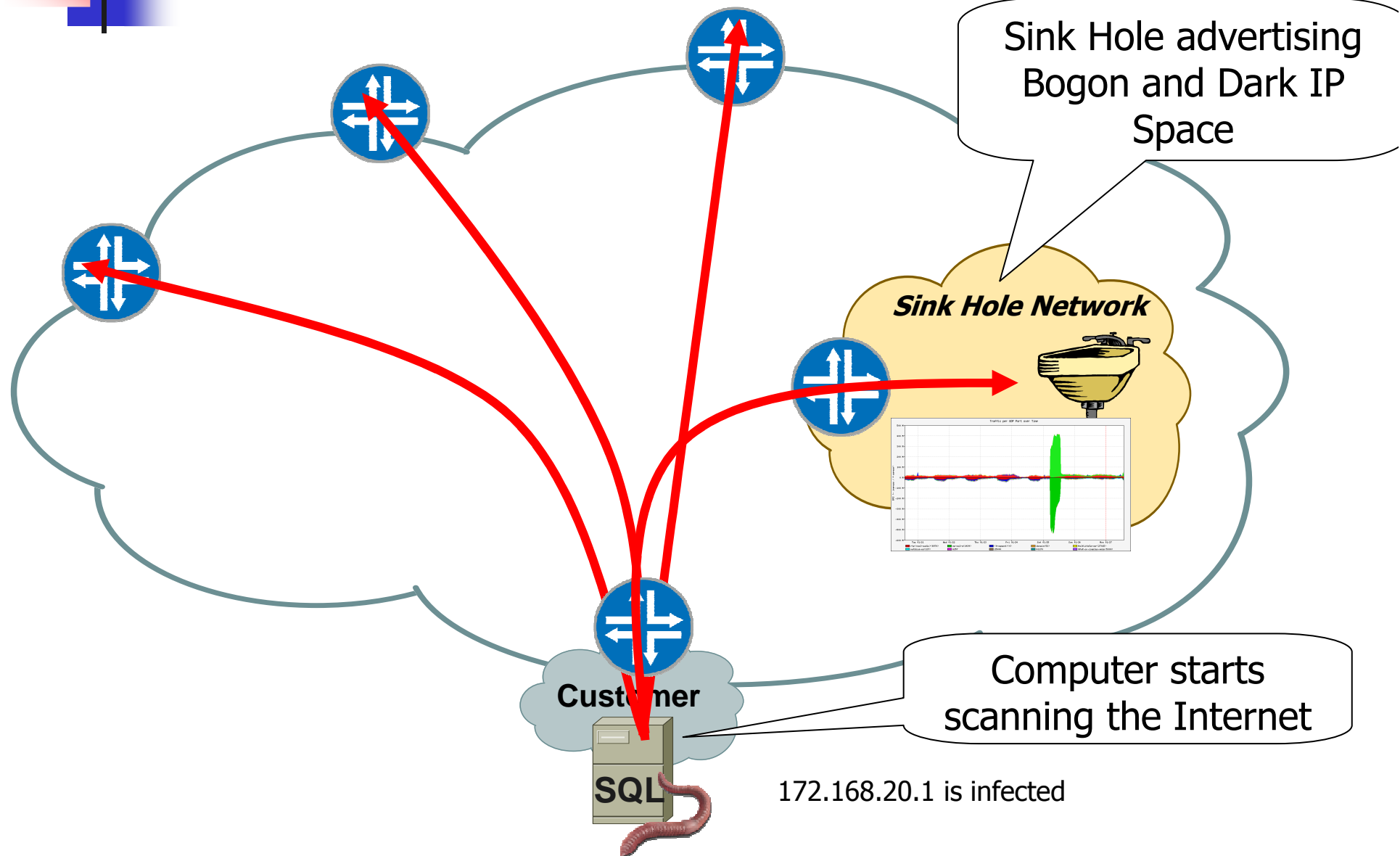


Sinkhole Routers/Networks

- Attack is pulled away from customer/aggregation router.
- Can now apply classification ACLs, Packet Capture, Etc...
- Objective is to minimize the risk to the network while investigating the attack incident.

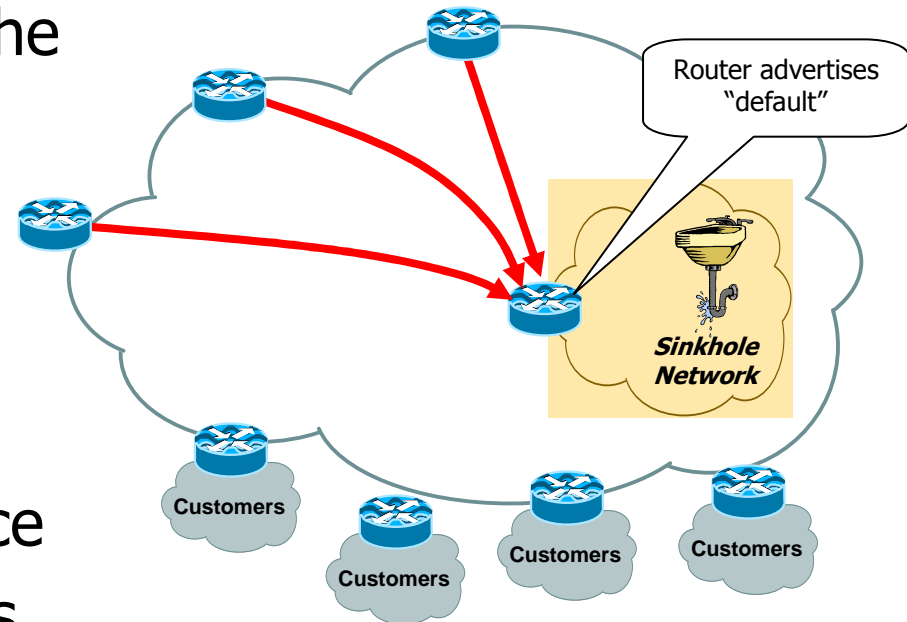


Infected End Points



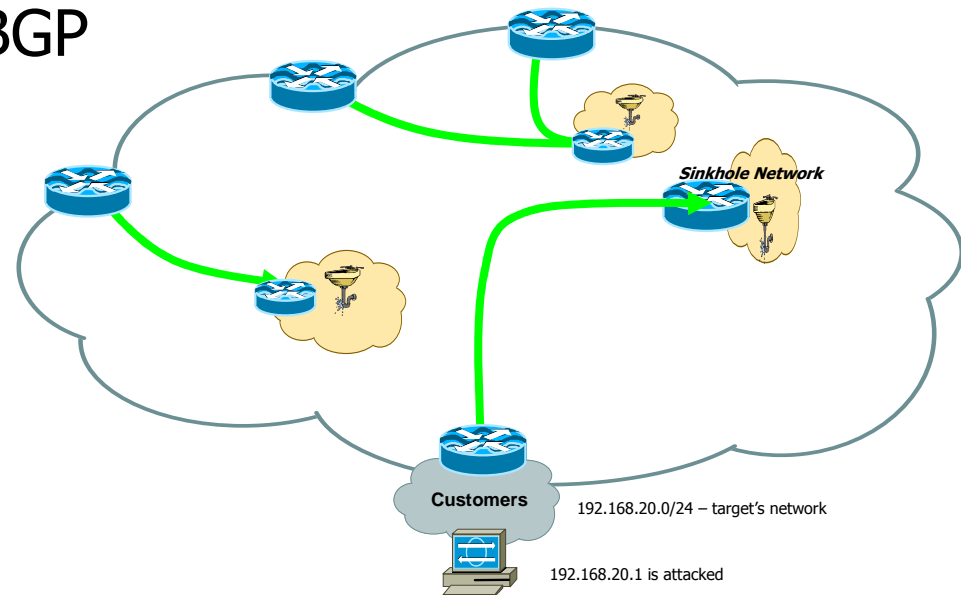
Sinkhole Routers/Networks

- Advertising “default” from the Sinkhole will pull down all sorts of *garbage* traffic:
 - Customer Traffic when circuits flap
 - Network Scans to unallocated address space
 - Code Red/NIMDA/Worms
 - Backscatter
- Can place tracking tools in the Sinkhole network to monitor the noise.



Scaling Sinkhole Networks

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

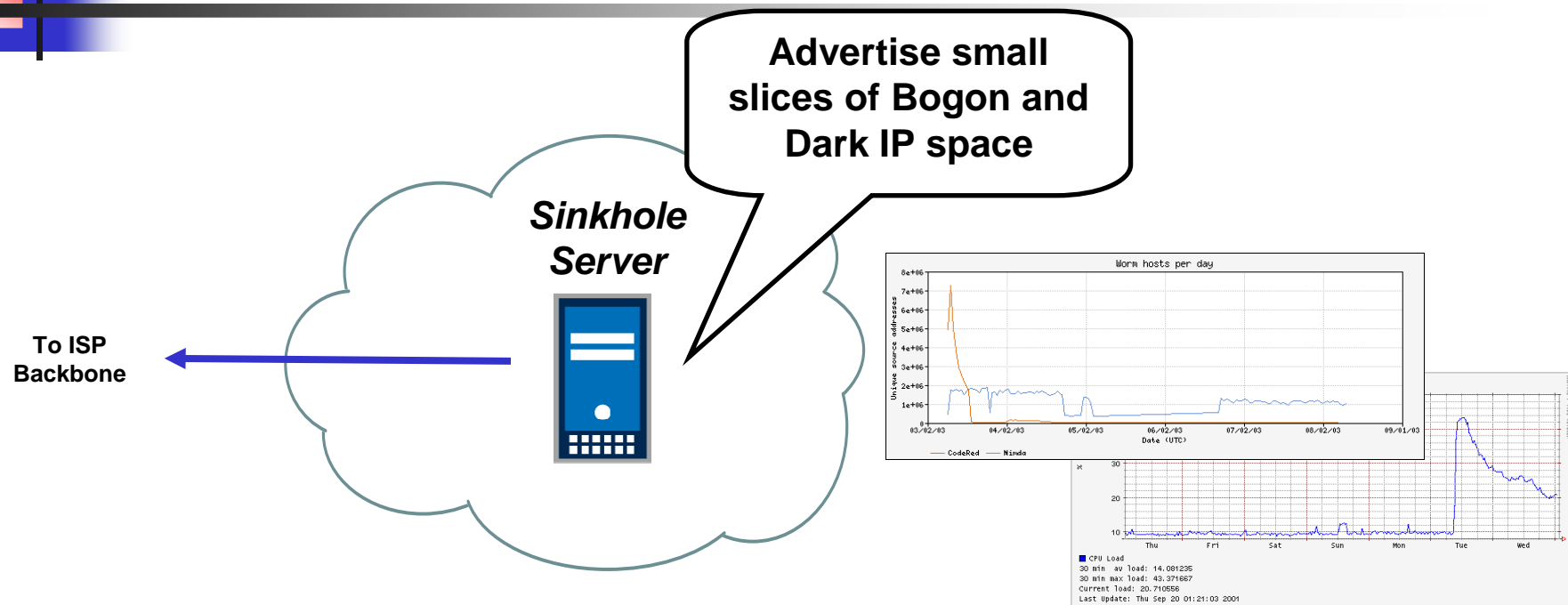




Why Sinkholes?

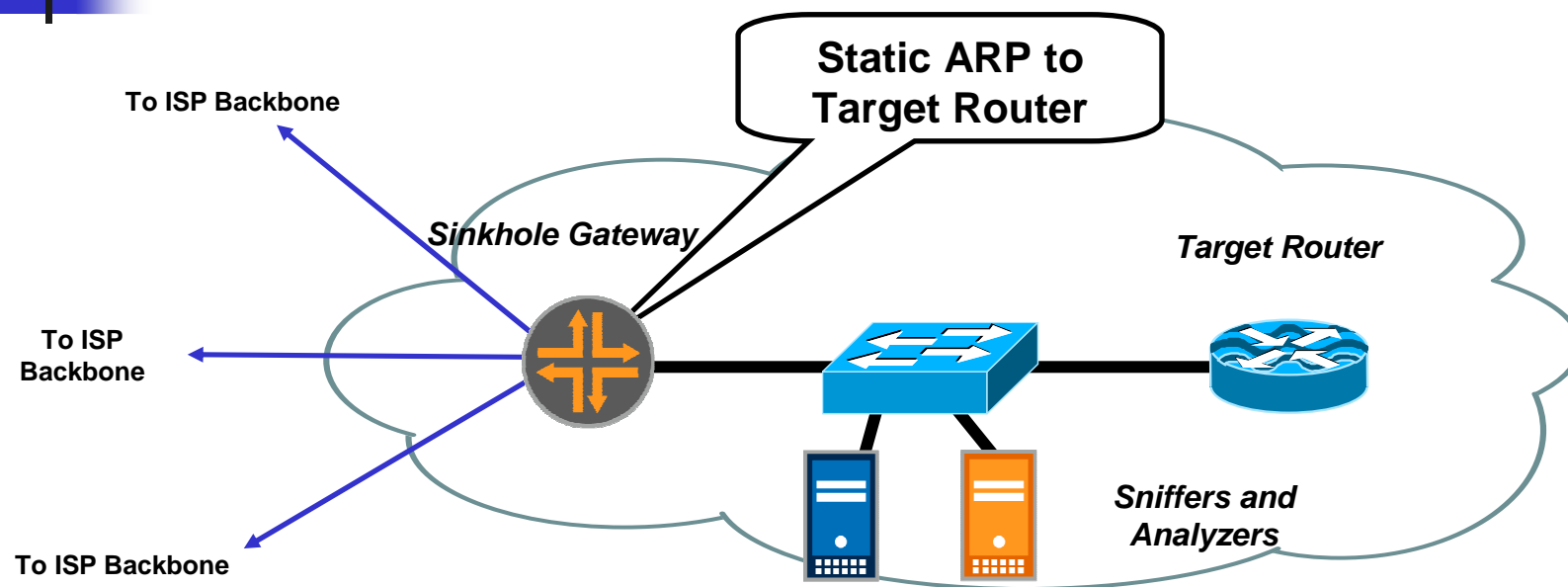
- They work! Providers and researchers use them in their network for data collection and analysis.
- More uses are being found through experience and individual innovation.
- Deploying Sinkholes correctly takes preparation.

The Basic Sinkhole



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

Expanding the Sinkhole



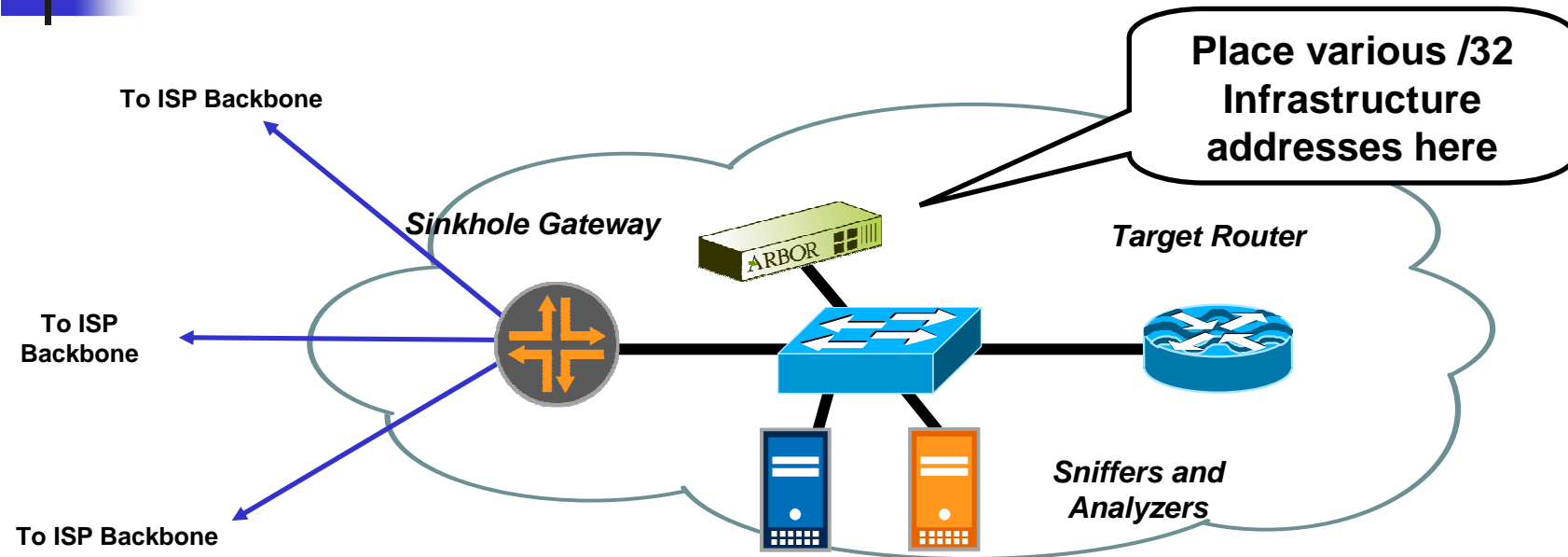
- Expand the Sinkhole with a dedicated router into a variety of tools.
- Pull the DOS/DDOS attack to the sinkhole and forwards the attack to the target router.
- Static ARP to the target router keeps the Sinkhole Operational – Target Router can crash from the attack and the static ARP will keep the gateway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



What to monitor in a Sinkhole?

- Scans on Dark IP (allocated & announced but unassigned address space).
 - Who is scoping out the network – pre-attack planning.
- Scans on Bogons (unallocated).
 - Worms, infected machines, and Bot creation
- Backscatter from Attacks
 - Who is getting attacked
- Backscatter from Garbage traffic (RFC-1918 leaks)
 - Which customers have misconfiguration or “leaking” networks.

Monitoring Scan Rates

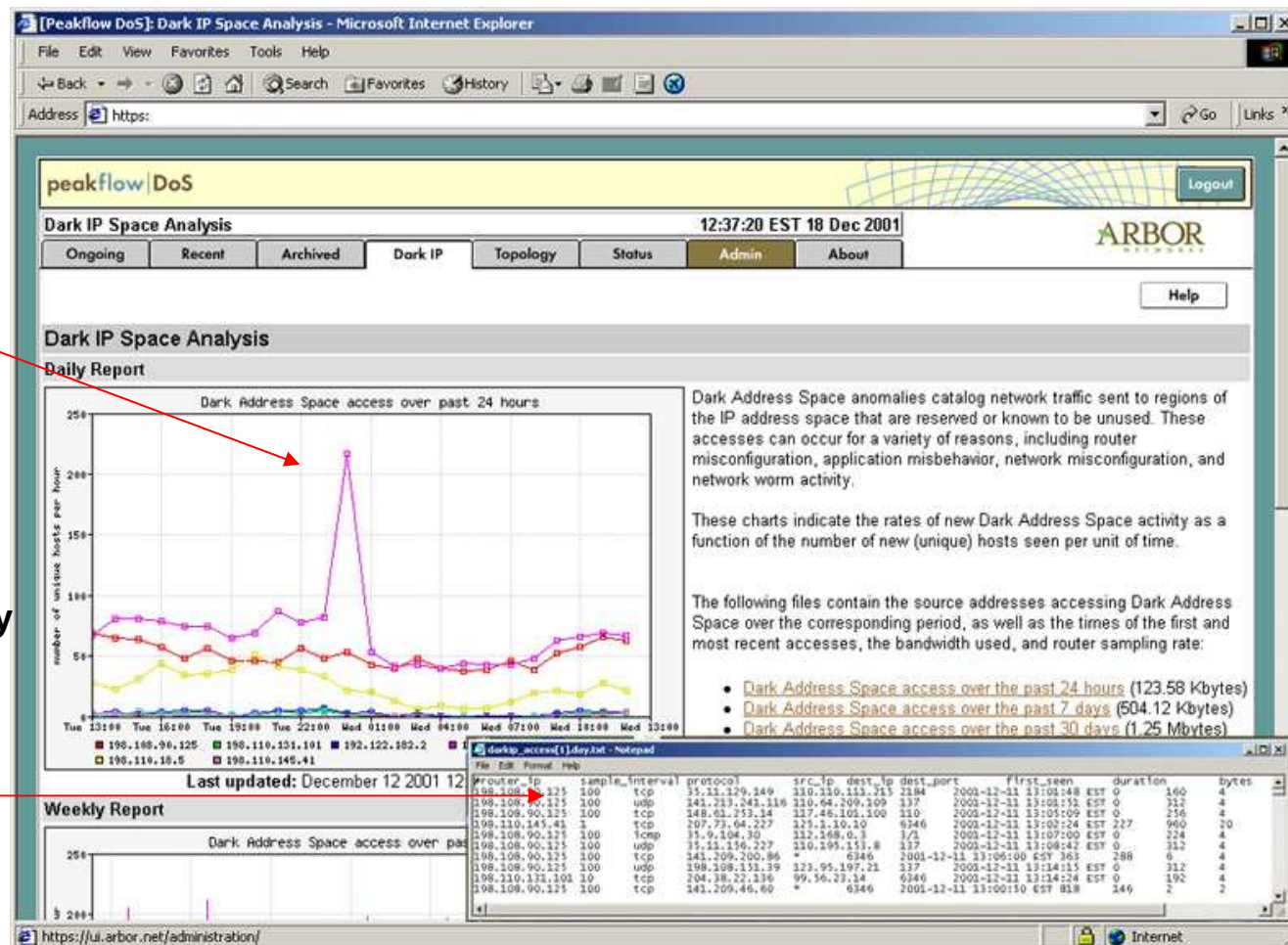


- Select /32 (or larger) address from different block of your address space. Advertise them out the Sinkhole
- Assign them to a workstation built to monitor and log scans. (Arbor Network's *Dark IP* Peakflow module is one turn key commercial tool that can monitor scan rates via data collected from the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

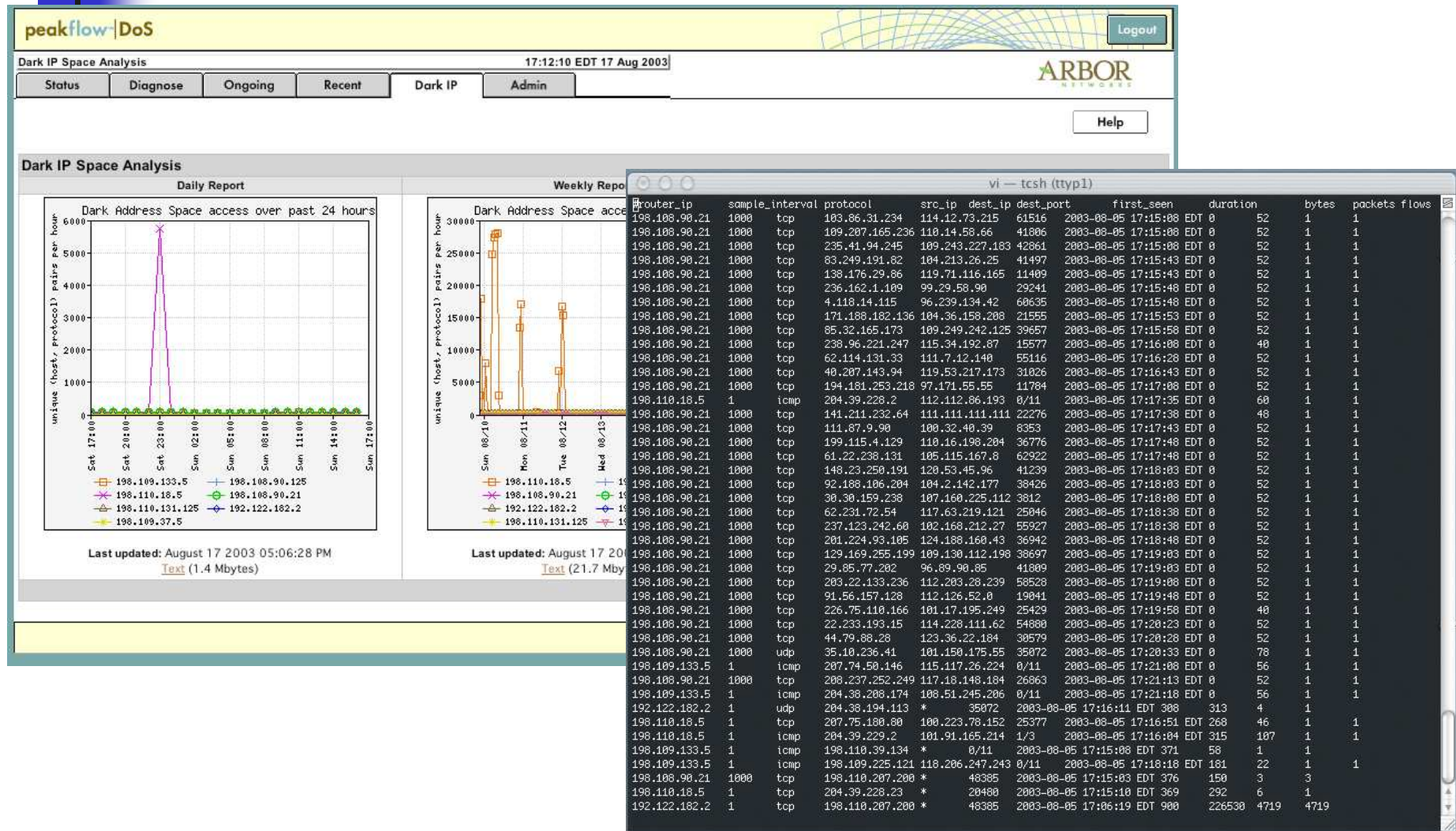
Worm Detection & Reporting UI

Operator instantly notified of Worm infection.

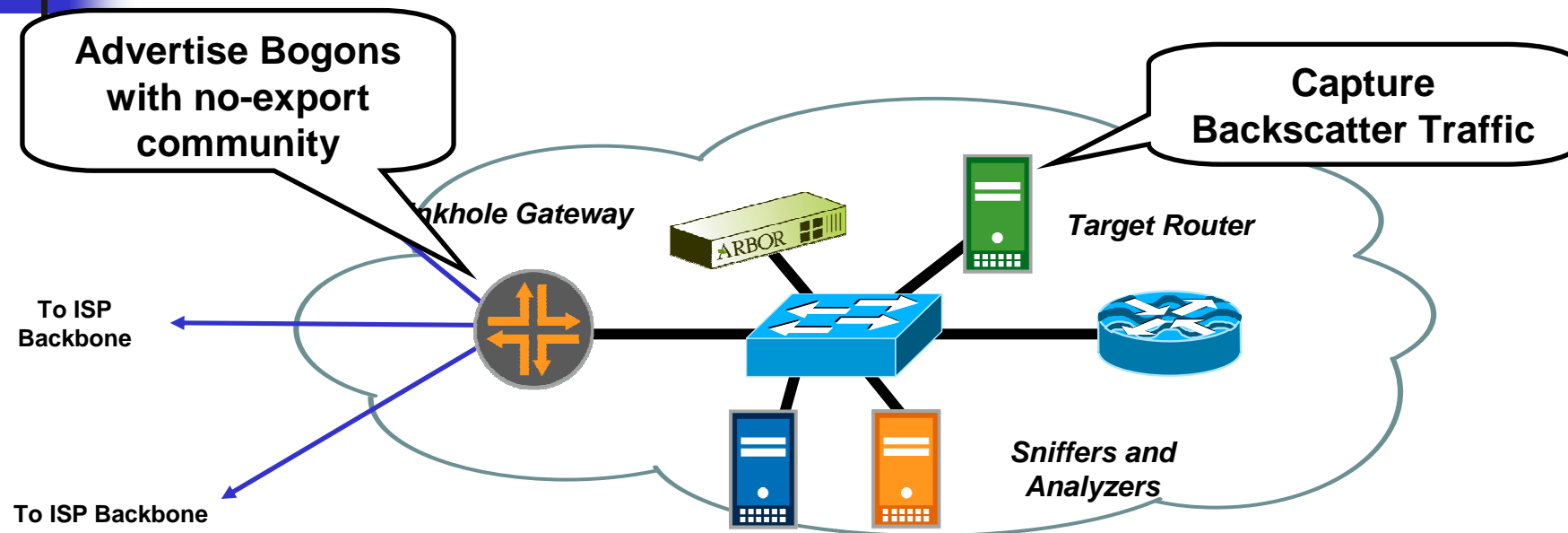
System automatically generates a list of infected hosts for quarantine and clean-up.



Automate Quarantine of Infected Hosts



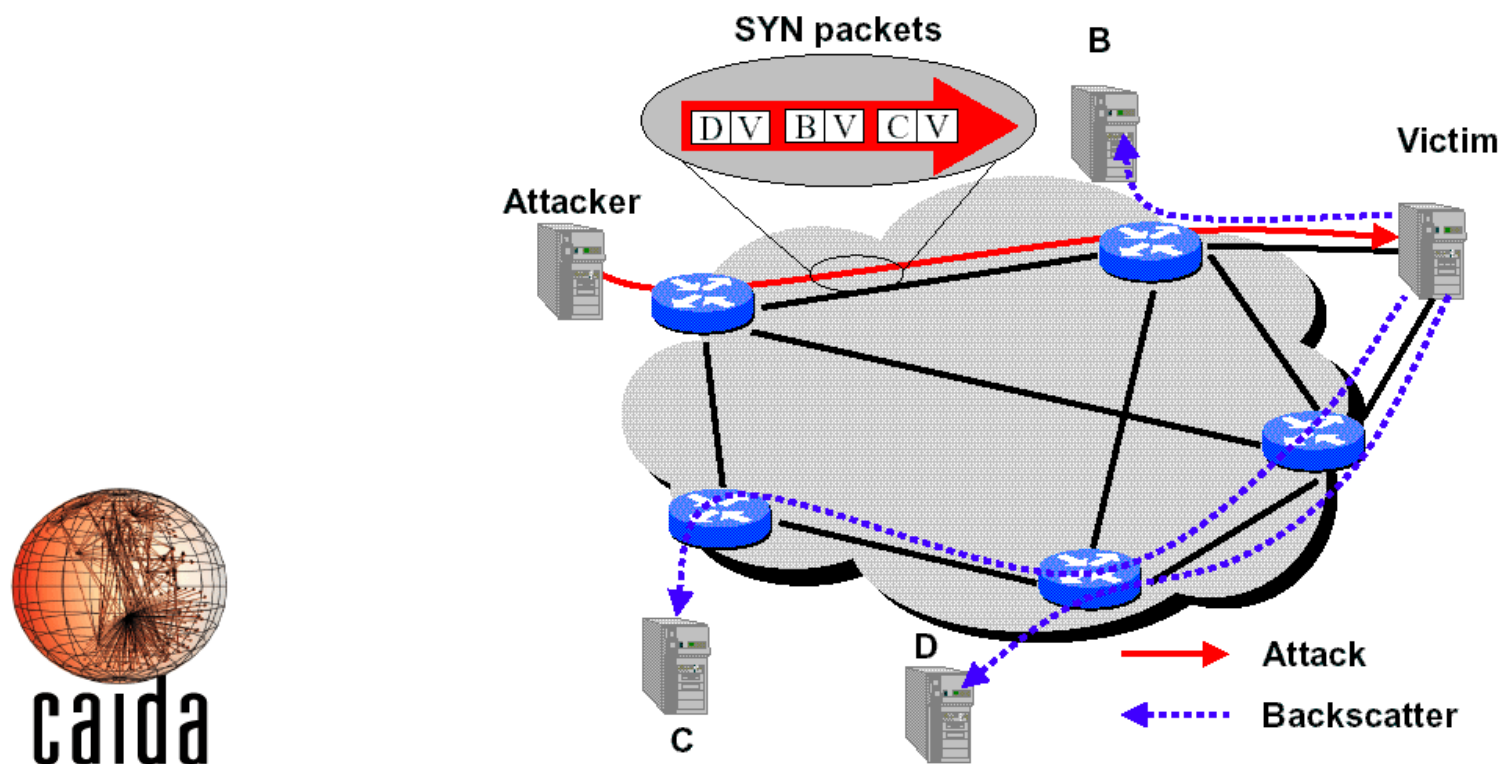
Monitoring Backscatter



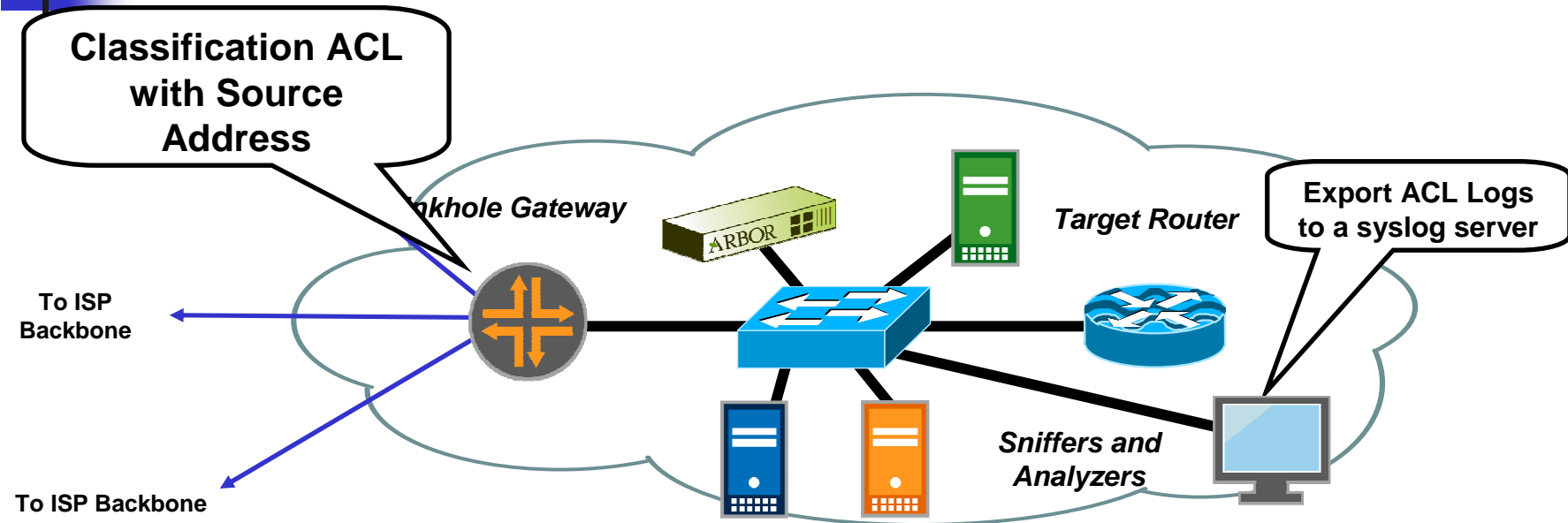
- Advertise bogon blocks with NO_EXPORT community and an explicit safety community (plus prefix-based egress filtering on the edge)
- Static/set the BGP NEXT_HOP for the bogon to a backscatter collector workstation (as simple as TCPdump).
- Pulls in backscatter for that range – allows monitoring.

Monitoring Backscatter

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



Monitoring Spoof Ranges



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

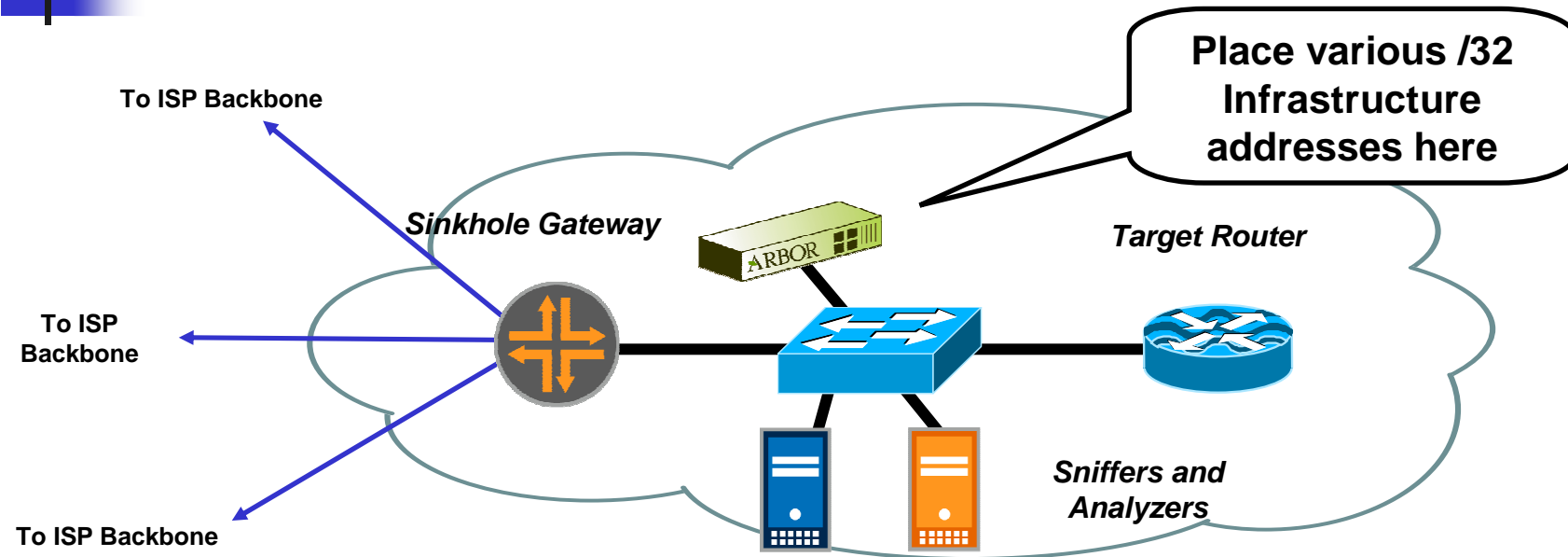


Monitoring Spoof Ranges

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

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

Monitoring Spoof Ranges



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

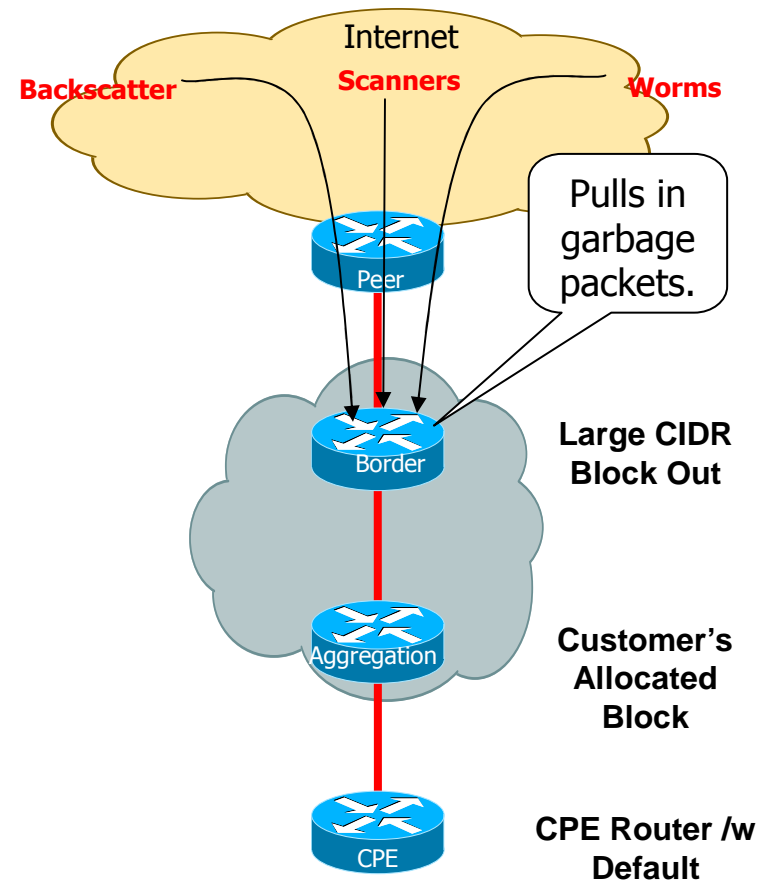


Safety Precautions

- Do not allow bogons to leak:
 - BGP “NO_EXPORT” community
 - Explicit Egress Prefix Policies (community, prefix, etc.)
- Do not allow traffic to escape the sinkhole:
 - Backscatter from a Sinkhole defeats the function of a *Sinkhole* (*egress ACL on the Sinkhole router*)

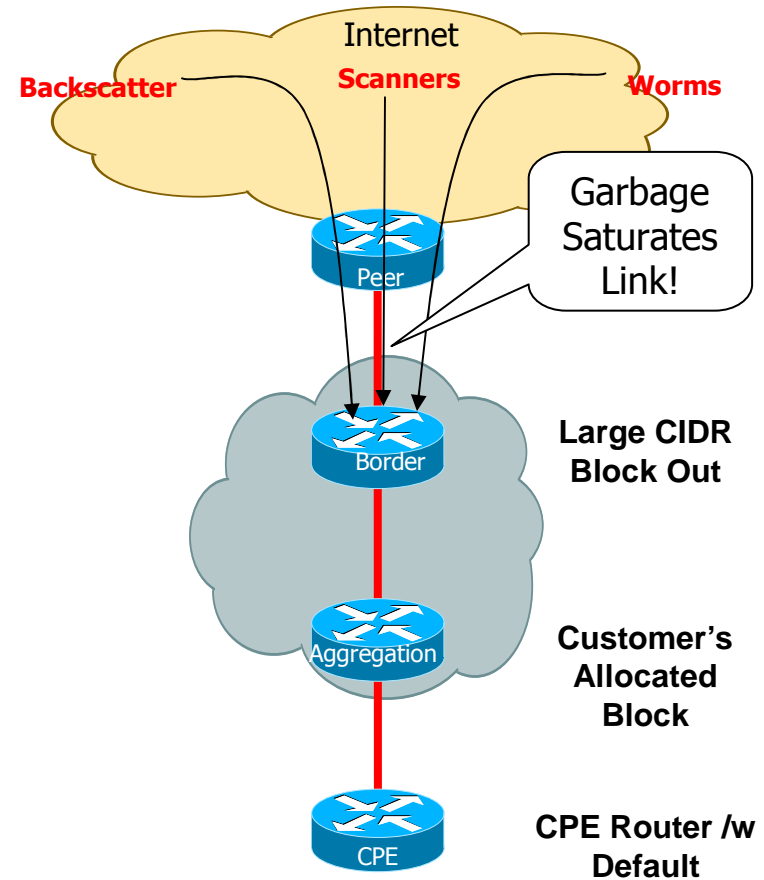
Simple Sinkholes – Internet Facing

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



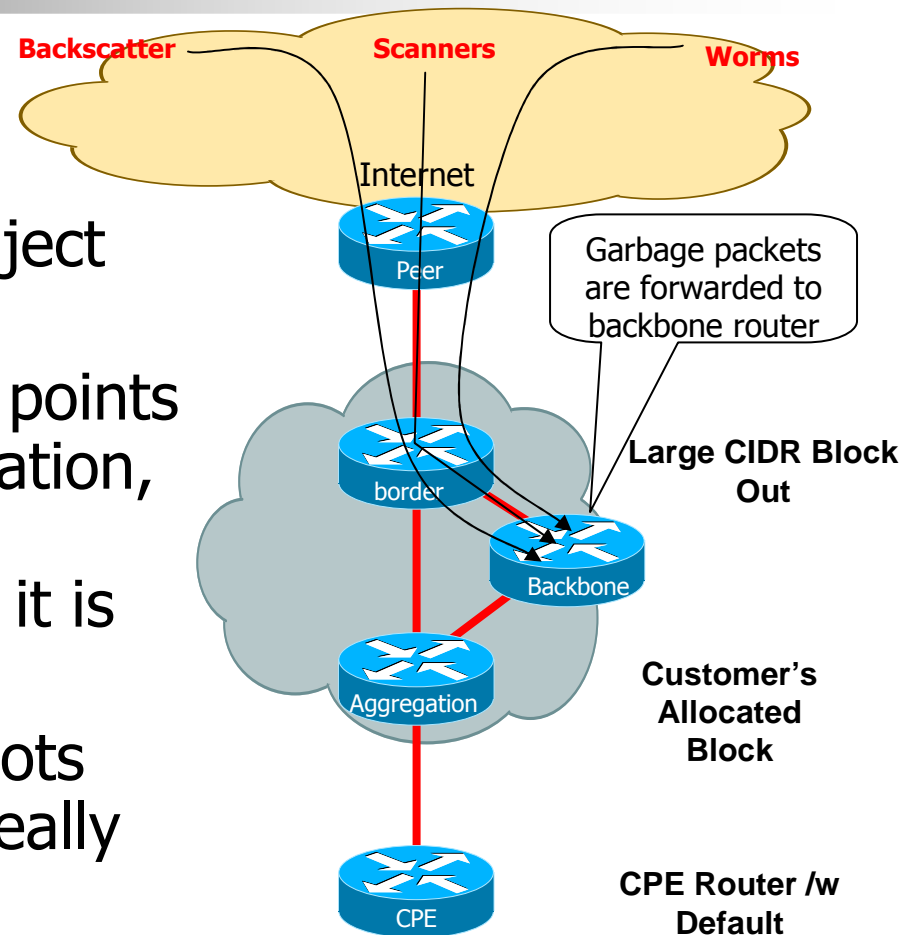
ASIC Drops at Line Rate?

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

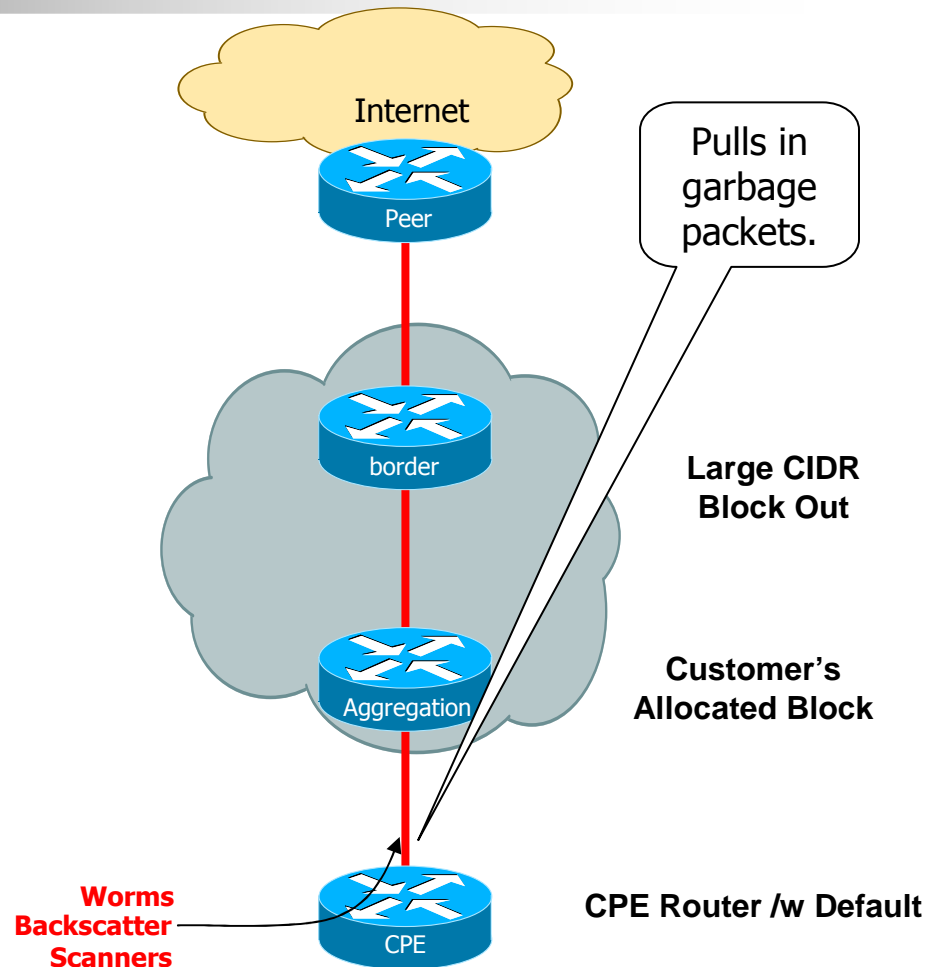


Backbone Router Injecting Aggregates

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

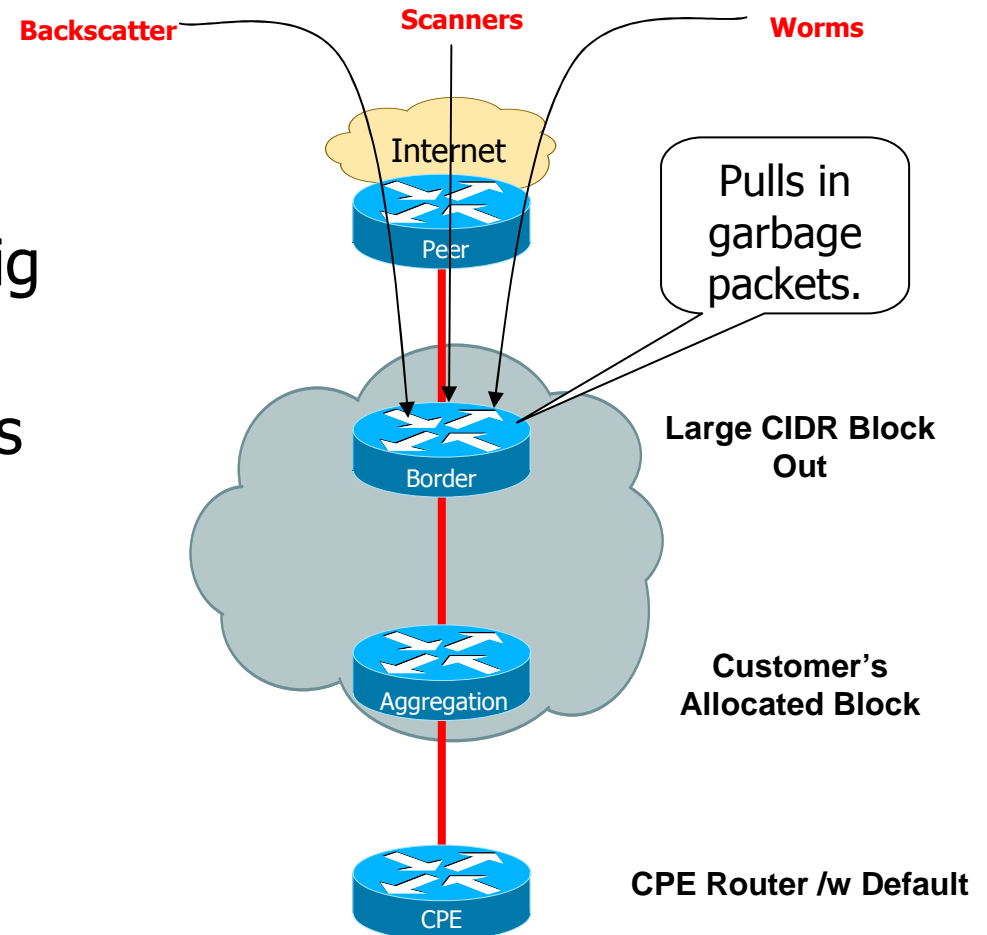


- Defaults on CPE devices pull in everything.
- Default is the ultimate packet vacuum cleaner
- Danger to links during times of security duress.

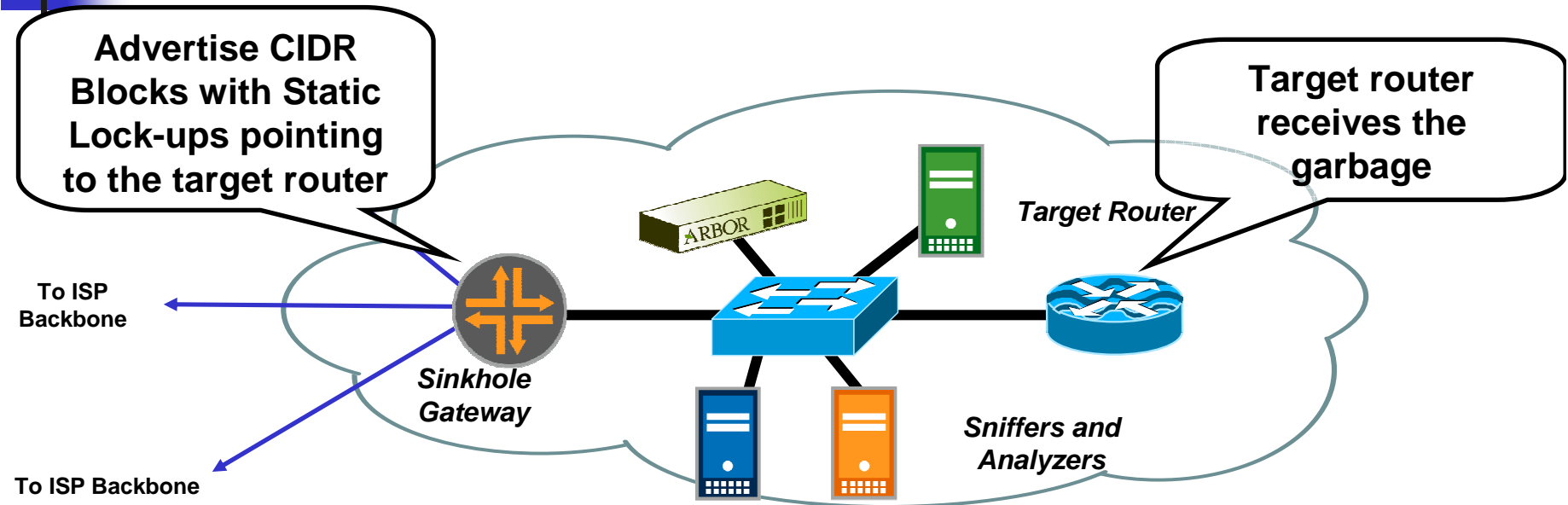


Simple Sinkholes – Impact Today

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

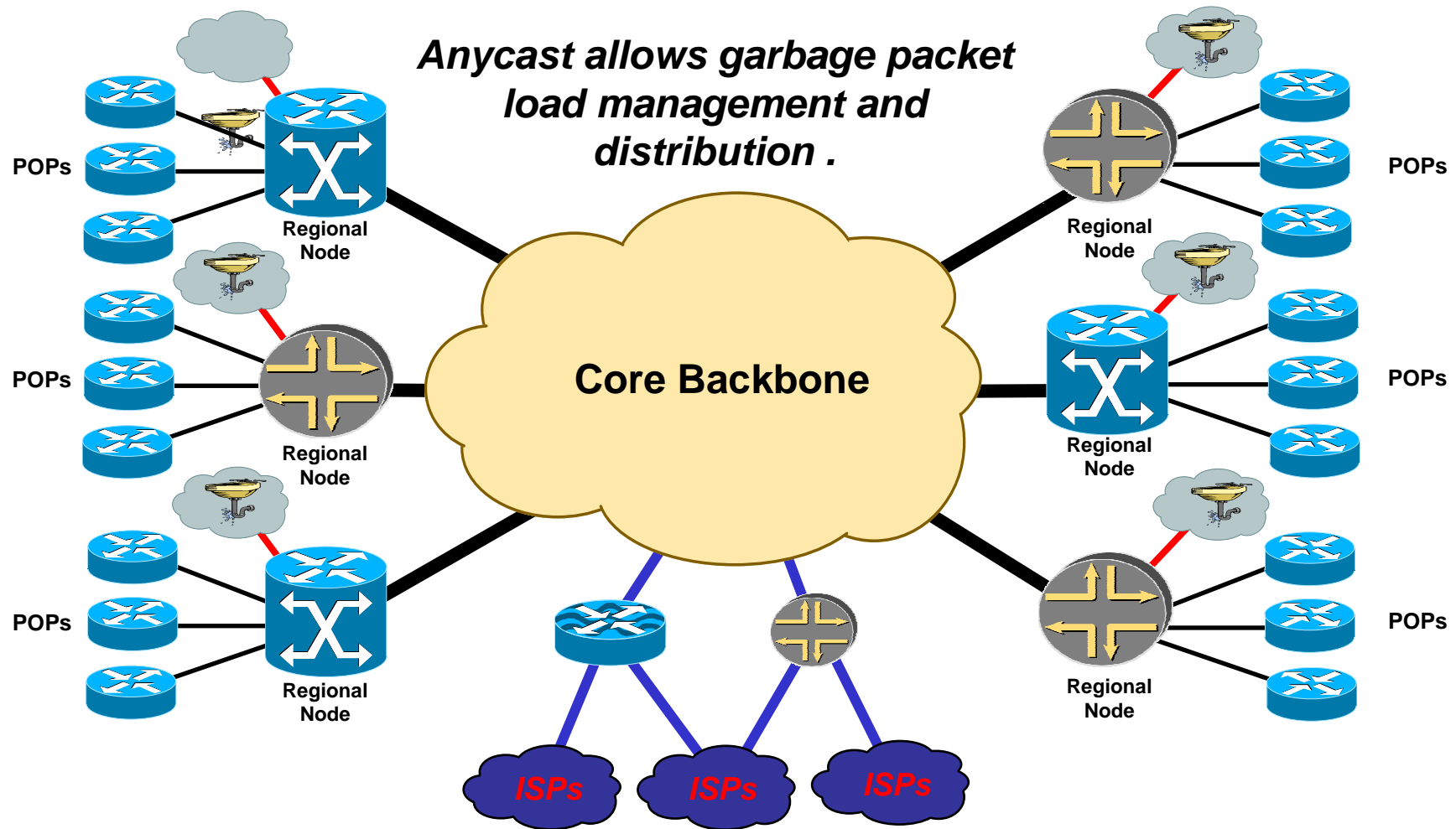


Sinkholes – Advertising Dark IP

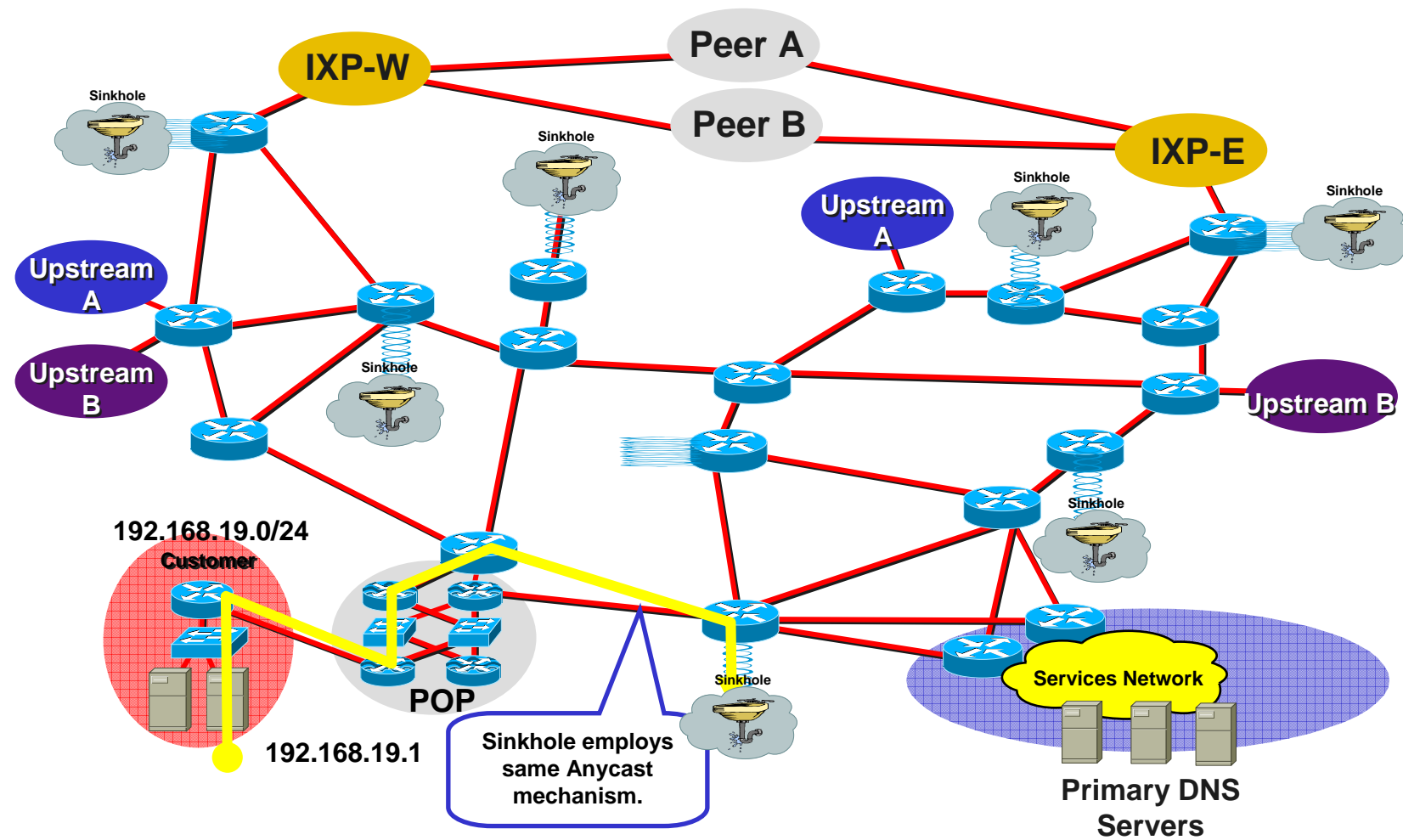


- Move the CIDR Block Advertisements (or at least more-specifics of those advertisements) to Sinkholes.
- Does not impact BGP routing – route origination can happen anywhere in the iBGP mesh (careful about MEDs and aggregates).
- Control where you drop the packet.
- Turns networks inherent behaviors into a security tool!

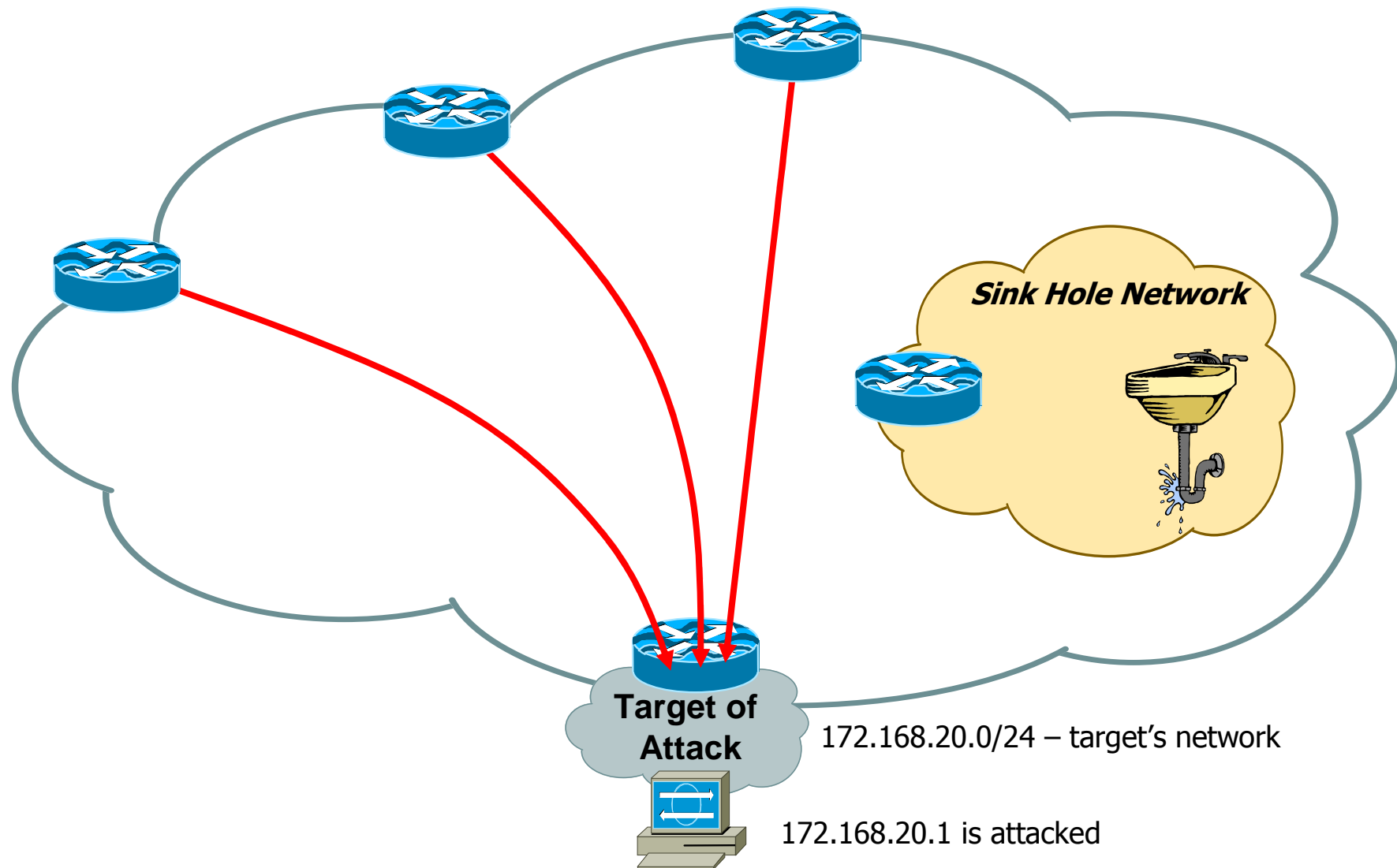
Anycast Sinkholes to Scale



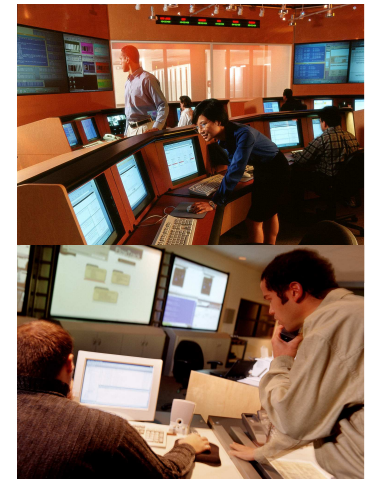
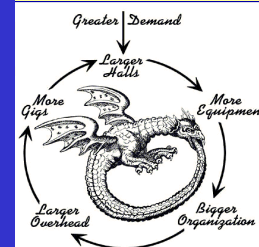
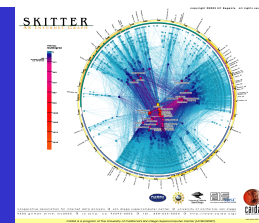
Anycast Sinkholes



Sink Hole Routers/Networks



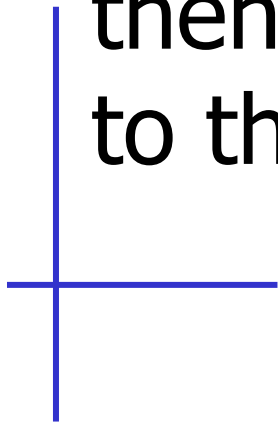
Source Address Validation





BCP 38 Ingress Packet Filtering

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





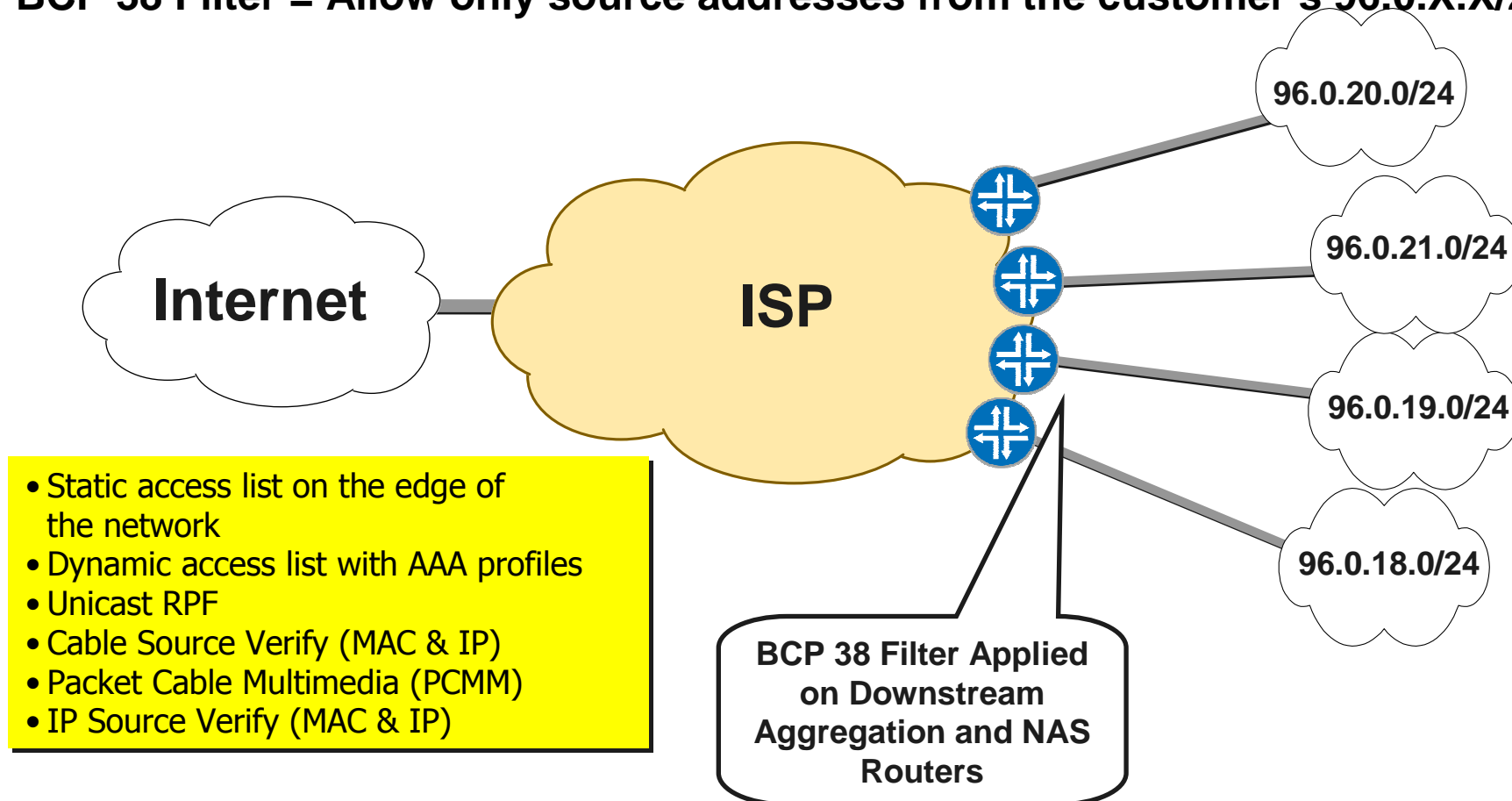
BCP 38 Ingress Packet Filtering

- 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



Many *Working* Techniques

- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)



Source Address Validation Works

- Successful SPs 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 SPs 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

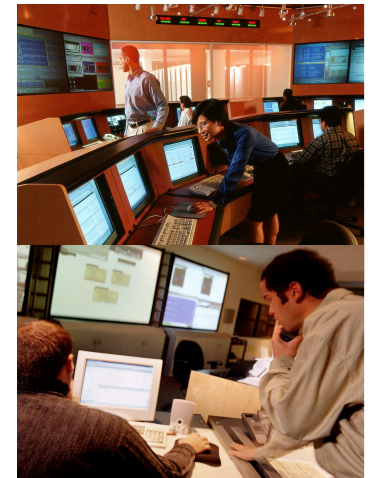
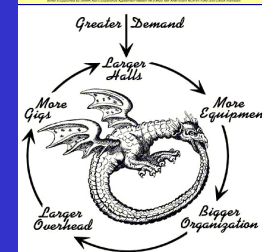
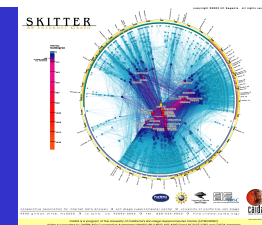
- Lessons Learned:
 - It took time and patience.
 - uRPF did not work for all customers. That is OK, uRPF is not suppose to be a *universal solution*.
 - Going slow and steady allowed the operations team to *gain a feel* of the feature's performance envelope --- with out putting the network at risk.
- It works! A year later it is a standard config with over 40K ports running uRPF Strict or Loose Mode.



What can you do to help?

- Cut the excuses! BCP 38 is an operational reality!
- Walk them through source address validation techniques, see which ones will work for you, and do not expect more than a 80% success rate.
- Find ways to gain operational confidence in the BCP 38 techniques.
- Source Address validation works – it just take patience and persistence.

Control Plane Protection





BGP Attack Vectors

- Understanding BGP Attack Vectors will help you plan and prioritize the techniques deployed to build greater resistance into the system.
- The following documents will help you gain perspective on the realistic Risk Assessment:
 - NANOG 25 - BGP Security Update
 - <http://www.nanog.org/mtg-0206/barry.html>
 - NANOG 28 - BGP Vulnerability Testing: Separating Fact from FUD
 - <http://www.nanog.org/mtg-0306/franz.html>
- Look for the *updates* links to get the latest risk assessments.
 - http://www.cisco.com/security_services/ciag/initiatives/research/projectsummary.html

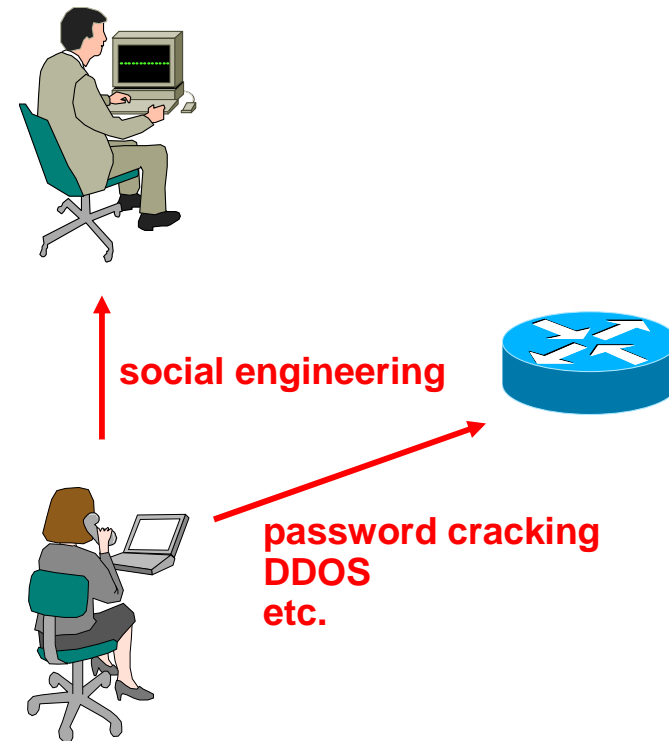


Whacking the BGP Session

- Four Macro Ways you can Whack the BGP Session:
 - Saturate the Receive Path Queues:
BGP times out
 - Saturate the link: link protocols time out
 - Drop the TCP session
 - Drop the IGP causing a recursive loop up failure

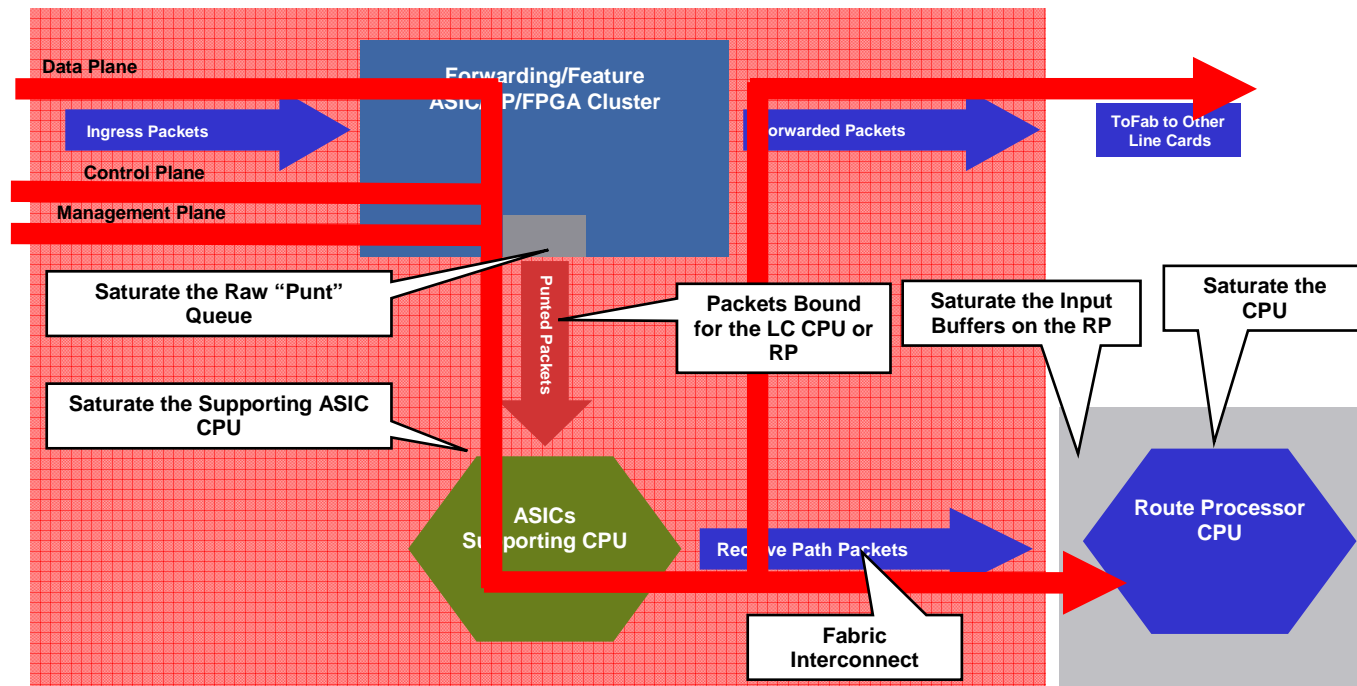
Attacking Routing Devices

- All the normal host attack methods apply to routers
 - Social engineering
 - Password cracking
 - Denial of service
 - etc.
- What an attacker needs:
 - Access to the router
 - *(or)*
 - Access to the network



Saturate the Receive Path Queues

- Routers usually have various *receive path* queues that are hit as the packet heads for the TCP Stack.
- Saturation Attacks fill these queues – knocking out valid packets from the queues.
- Consequence: BGP Times out – Dropping the BGP Session





Saturate the Link

- DOS Attacks Saturating the link will knock out valid control plane packets.
- Link packet over POS, ATM, or Ethernet will drop out – which drop out the link – which drop out the FIB's next hop – which knocks out the BGP Entries
- This is a very effective brute force attack.

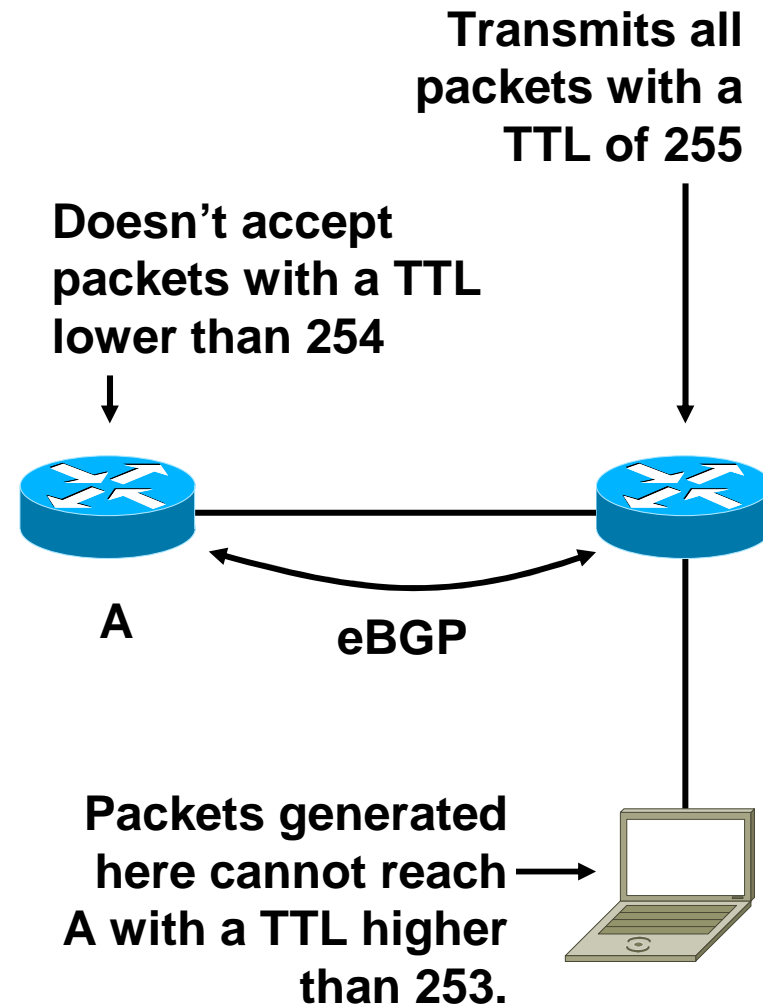


Drop the TCP Session

- Dropping the TCP Session was thought to require a breath of packets.
- TCP Session can be dropped with a RST or a SYN (per RFC).
- Successful L4 Spoof is required
 - Match source address
 - Match source port
 - Match destination address (obvious)
 - Match destination port
 - Match Sequence Number (now just get inside the window)

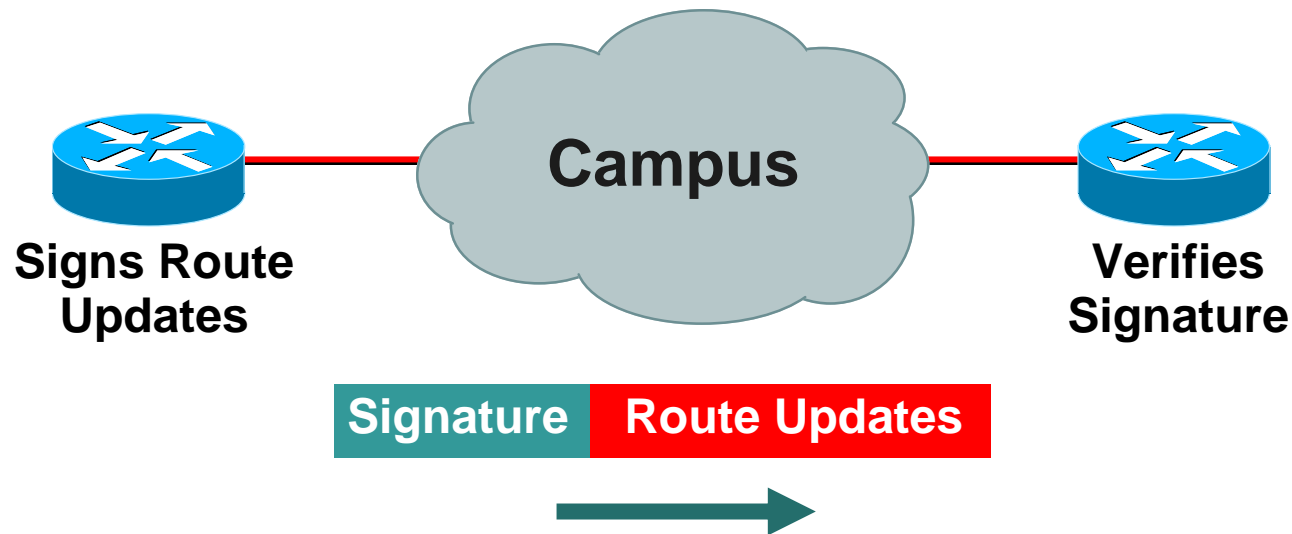
Generalized TTL Security Mechanism

- GTSH is a hack which protects the BGP peers from multihop attacks.
- Routers are configured to transmit their packets with a TTL of 255, and to reject all packets with a TTL lower than 254 or 253.
- A device which isn't connected between the routers cannot generate packets which will be accepted by either one of them.



Secure Routing - Route Authentication

Configure Routing Authentication



Certifies **Authenticity** of Neighbor
and **Integrity** of Route Updates



Peer Authentication

- MD5 Peer authentication can protect against:
 - Malformed packets tearing down a peering session
 - Unauthorized devices transmitting routing information
- MD5 Peer authentication cannot protect against:
 - Reset routing protocol sessions due to denial of service attacks
 - Incorrect routing information being injected by a valid device which has been compromised

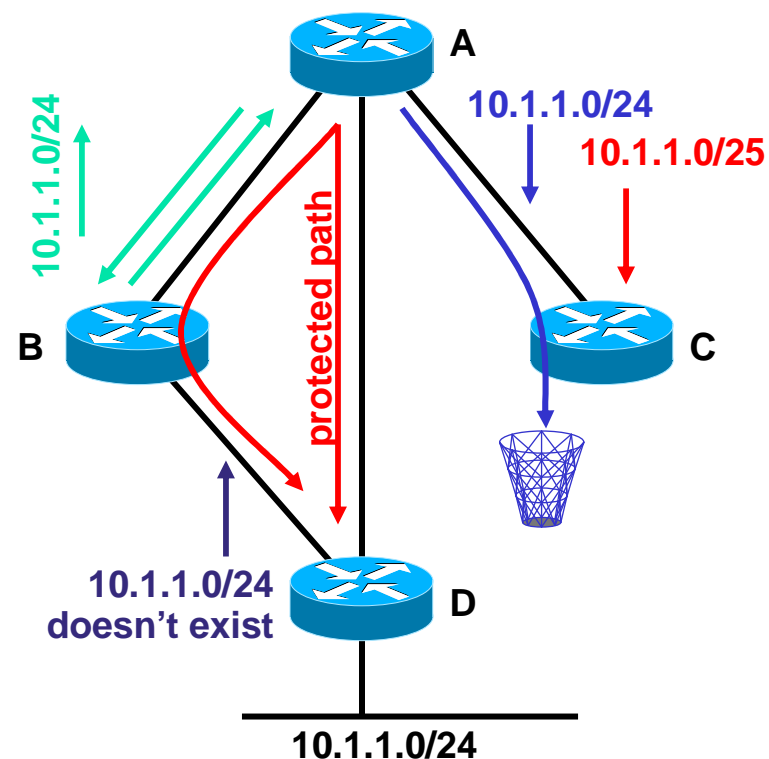


Drop the IGP

- Miscreant Success Principle - If you cannot take out the target, move the attack to a coupled dependency of the target.
- BGP's coupled dependency is the IGP it requires for recursive look-up.
- EIGRP and OSPF are both open to external attacks.

Attacking Routing Data

- How could you attack routing data?
- Modification
 - Direct traffic along an unprotected path
 - Direct traffic into a black hole
 - Create a routing loop
- Overclaiming
 - Injecting nonexistent destinations
 - *A longer prefix!*
- Underclaiming
 - Removing destinations



Pakistan and YouTube

Pakistan Blocks YouTube Video Access

February 24, 2008 12:17 PM PST

YouTube blames Pakistan outage

Posted by Greg Sandoval

Updated, 9:40 p.m. to add YouTube's explanation outage.

YouTube suffered a two-hour long, system-wide outage the company said was triggered by a network bas

SADAQAT JAN | February 24, 2008 09:04 AM EST | **AP**

Read More: [Pakistan](#), [Pakistan Blocks Youtube](#), [Pakistan Elections](#), [Pakistan Youtube](#), [Pervez Musharraf](#), [Youtube](#), [Youtube Pakistan Anti-Islamic Movies](#), [Breaking Politics News](#)



Email ▶
Print ▶
Comments ▶



ISLAMABAD, Pakistan — Pakistan's government has banned access to the video-sharing Web site YouTube because of anti-Islamic movies that users have posted on the site, an official said Sunday.

The Pakistan Telecommunication Authority told the country's 70 Internet service providers Friday that the popular Web site would be blocked until further notice.

The authority did not specify what the offensive material was, but a PTA official said the ban responded to a media trailer for an upcoming film by

<http://www.ripe.net/news/study-youtube-hijacking.html>



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.

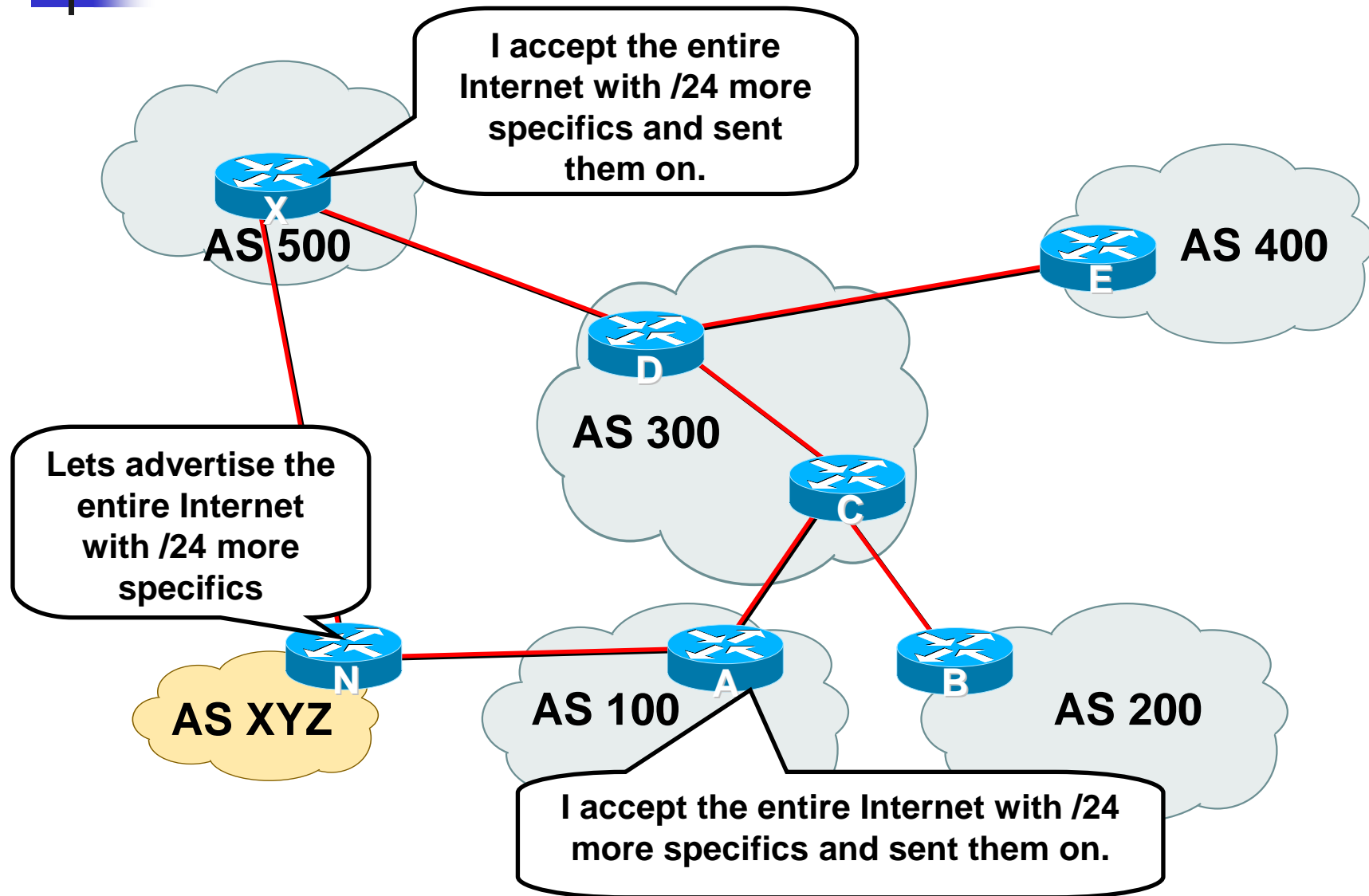


Malicious Route Injection

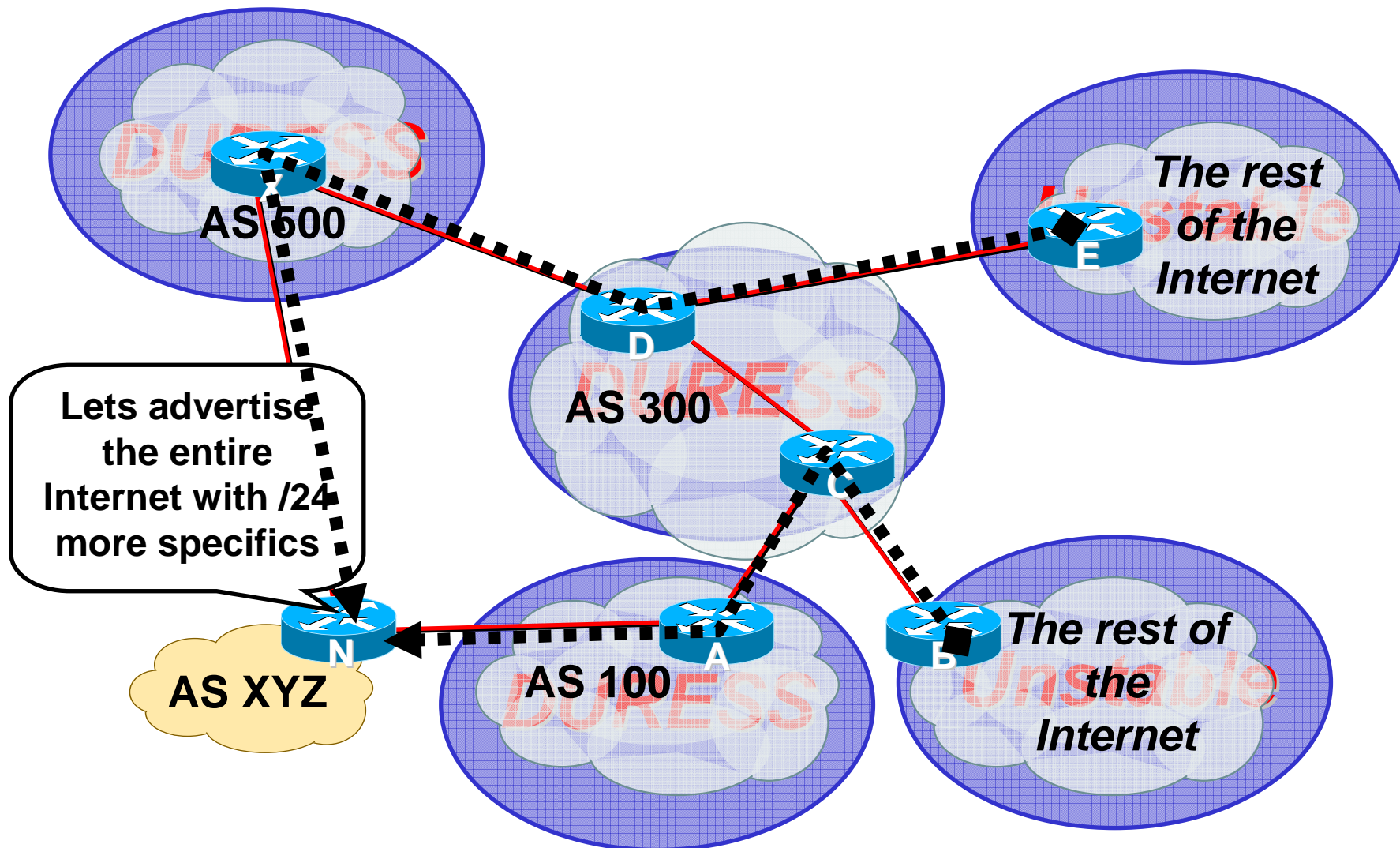
Reality – an Example

- 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.

Garbage in – Garbage Out: What is it?

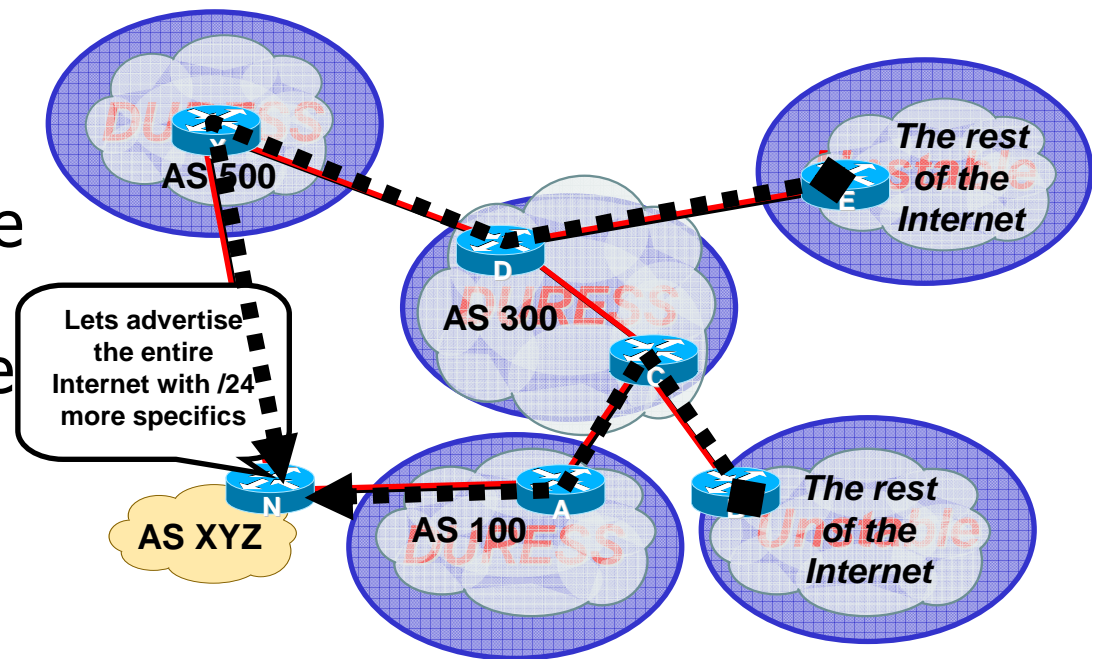


Garbage in – Garbage Out: Results



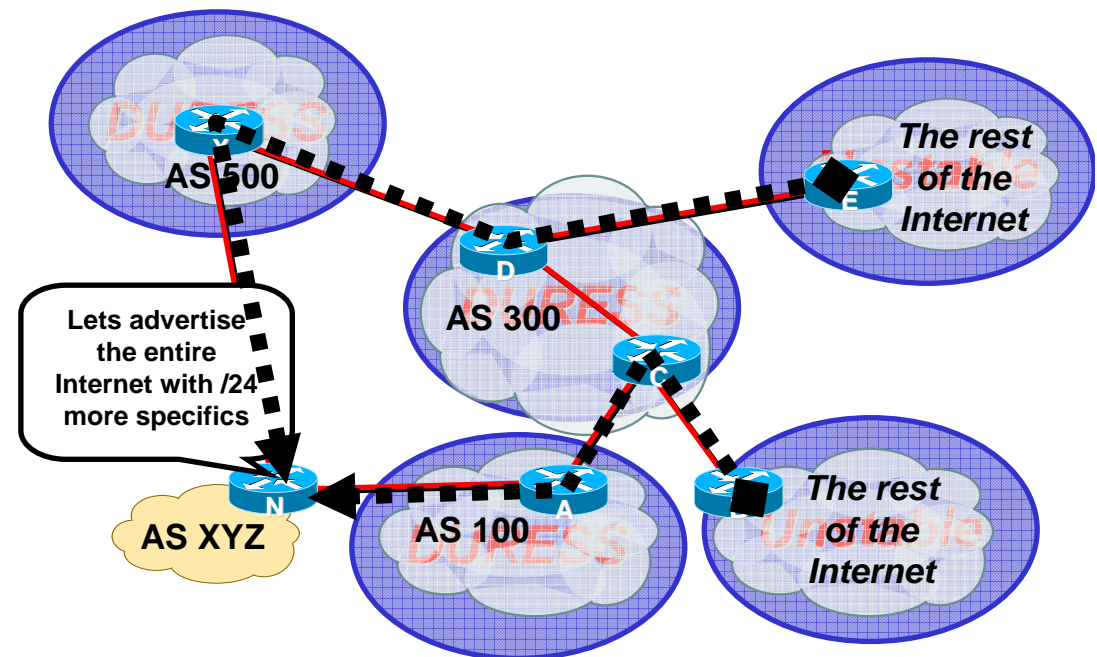
Garbage in – Garbage Out: Impact

- 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 your advertisements
- Net Police Filtering
 - Mitigate the impact when it happens
- Prefix Filtering and Max Prefix Limits



Malicious Route Injection

Attack Methods

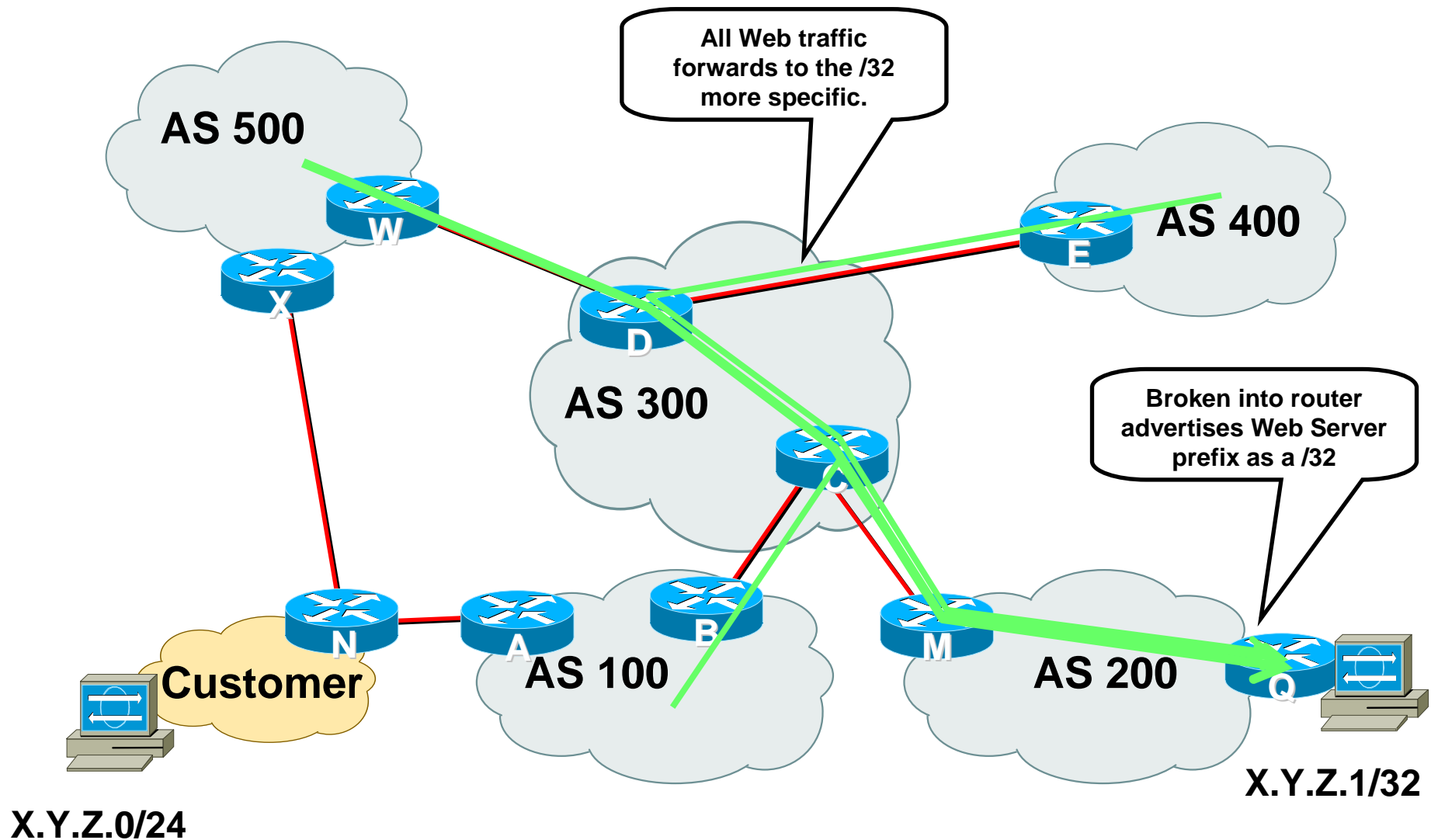
- Good News – Risk is mainly to BGP speaking Routers.
- Bad News – Multihomed BGP Speaking customers are increasing!
- Really Bad News – Many of these routers have no passwords!
- Local layer 3 configuration alteration on compromised router
- Intra-AS propagation of bad routing information
- Inter-AS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

Malicious Route Injection

Impact

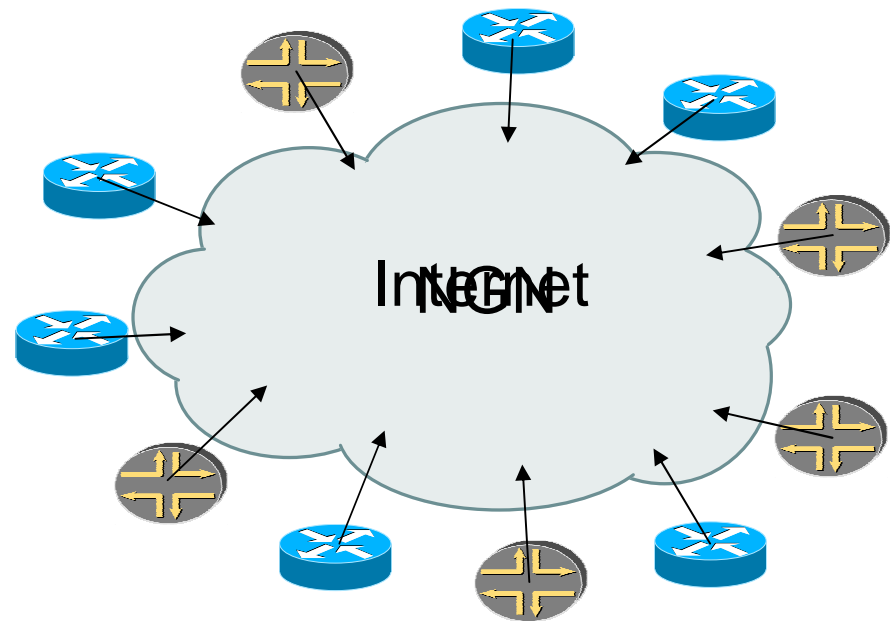
- Denial-Of-Service to Customer(s), ISP(s), and the Internet.
- Traffic Redirection / Interception
- Prefix Hijacking
- AS Hijacking

What is a prefix hijack?



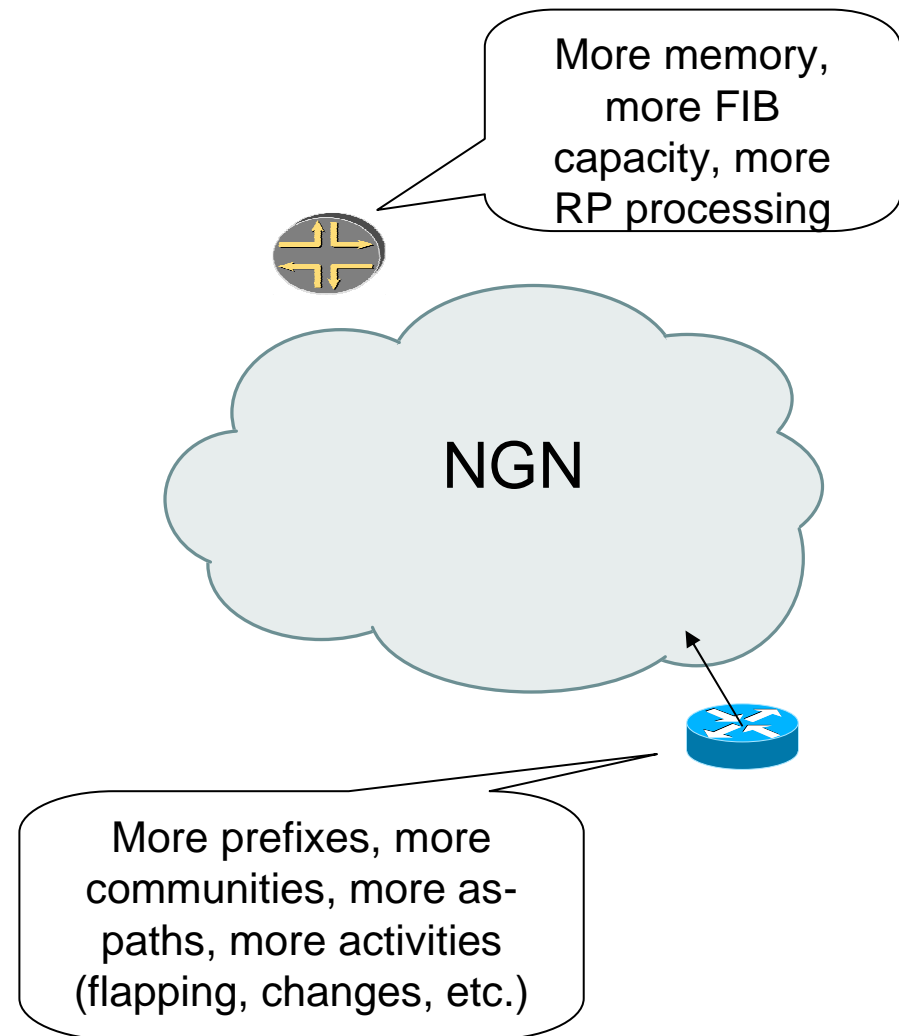
What could be worse?

- The Miscreant Economy Trades violated “BGP Speaking” routers. Get 20 in different parts of the Internet.
- Take each, pick your targets, and start disaggregating.



Why?

- Today's (and tomorrow's) NGN will be different from the past
- A business on one side of the planet will force you into OPEX and CAPEX expenditure!



Malicious Route Injection

What can ISPs Do?

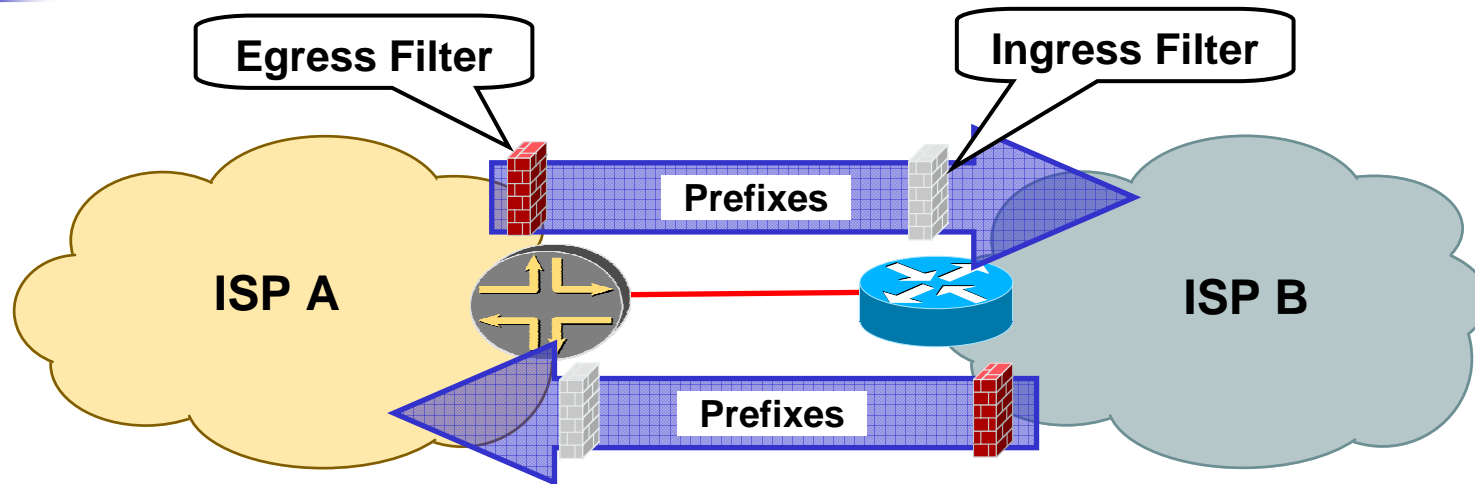
- Customer Ingress Prefix Filtering!
- ISPs should only accept customer prefixes which have been assigned or allocated to their downstream customers.
- For example
 - Downstream customer has 220.50.0.0/20 block.
 - Customer should only announce this to peers.
 - Upstream peers should only accept this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



BGP Peering Fundamentals

- BGP Peering assumes that something could go wrong with the policy filters between the neighboring routers.
- Filters are all created to mutually reinforce each other. If one policy filter fails, the policy filter on the neighboring router will take over – providing redundancy to the policy filters.
- This mutually reinforcement concept used BGP peering filters are created are also called guarded trust, mutual suspicion, or Murphy Filtering.

Guarded Trust



- SP A trust SP B to send X prefixes from the Global Internet Route Table.
- SP B Creates a egress filter to insure only X prefixes are sent to SP A.
- SP A creates a mirror image ingress filter to insure SP B only sends X prefixes.
- SP A's ingress filter reinforces SP B's egress filter.

Malicious Route Injection

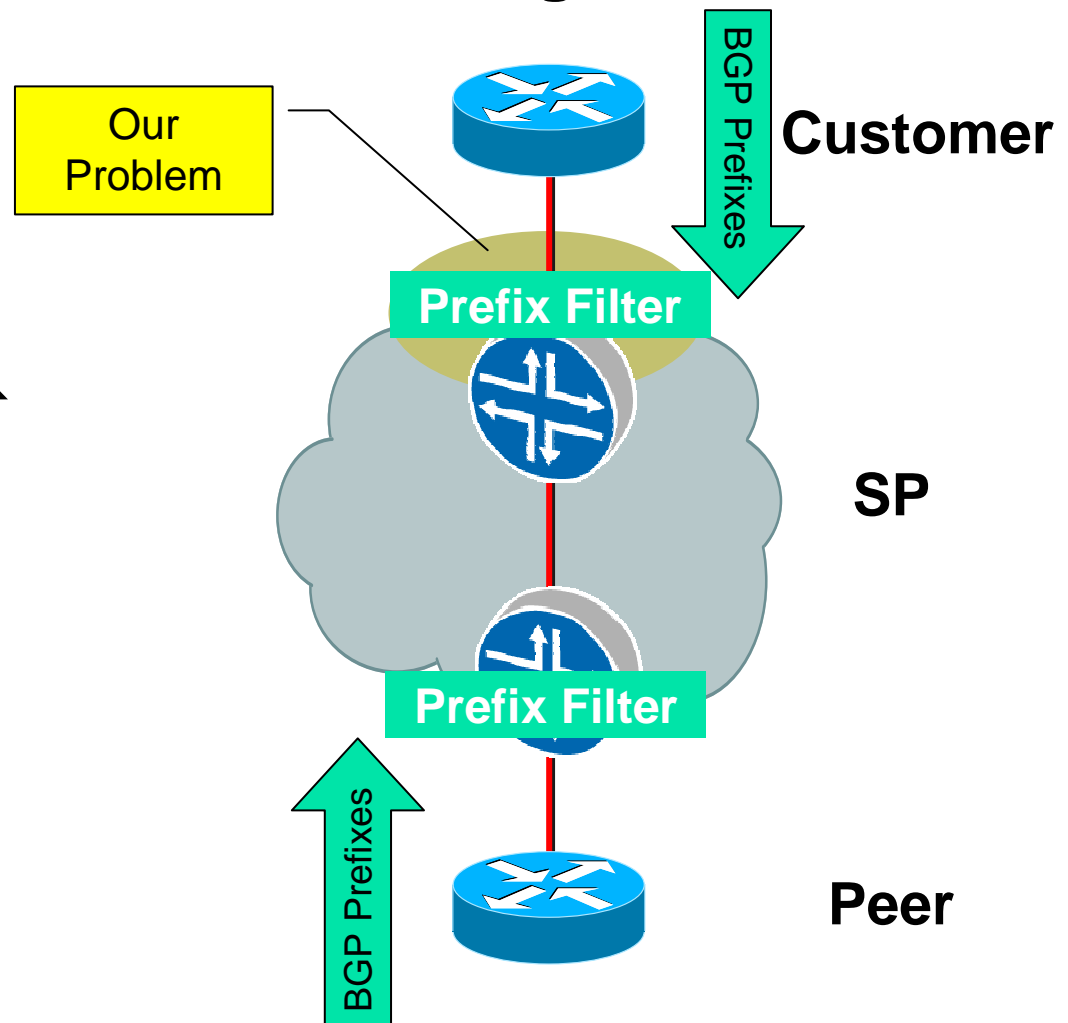
What can SPs Do?

- Know your network – What to filter, where to filter.
- Customer Ingress Prefix Filtering!
- SPs 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.

Prefix Filters: In

Apply Prefix Filters to All eBGP Neighbors

- From Customers
- From Peers & Upstreams



Malicious Route Injection

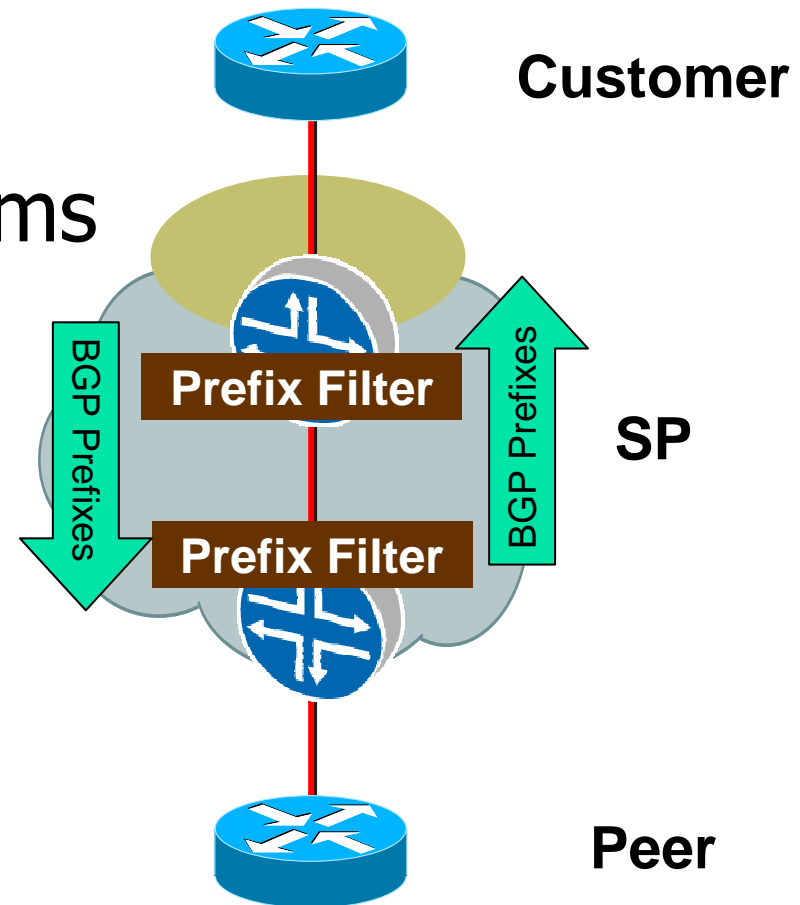
What can ISPs Do?

- 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.

Prefix Filters: Out

Apply Prefix Filters to All eBGP Neighbors

- To Customers
- To Peers & Upstreams

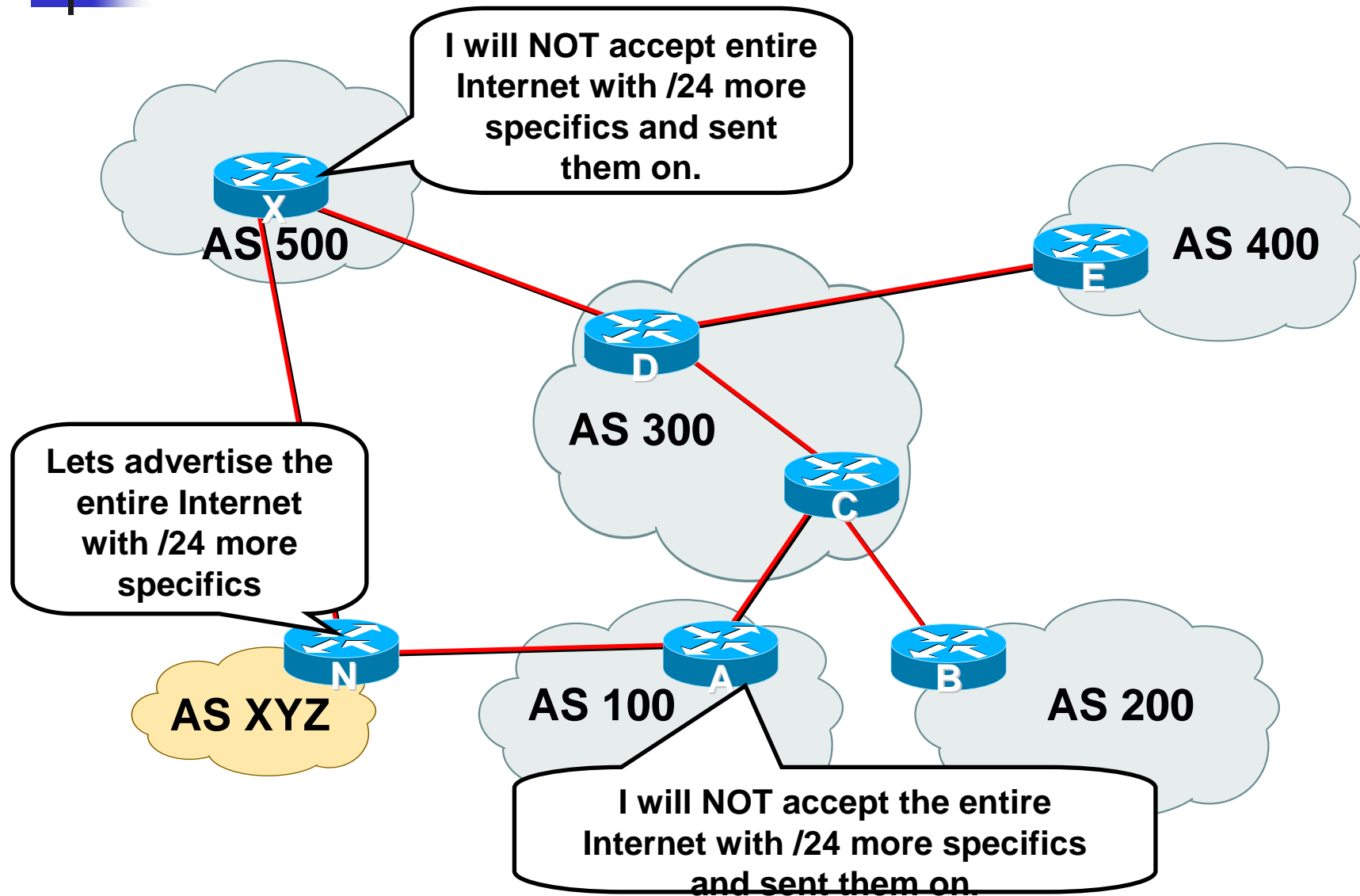


What can ISPs Do?

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 you're advertising to everyone else.
 - *Bigness* is not an excuse.

Containment Filters



Malicious Route Injection

What can ISPs Do?

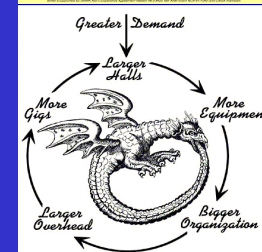
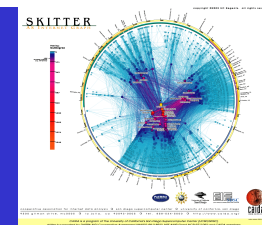
- Customer Ingress Prefix Filtering
- Prefix filtering between intra-AS trust zones
- Route table monitoring to detect alteration of critical route paths
- SPAMers are using route-hijacking.



Bogons and Special Use Addresses

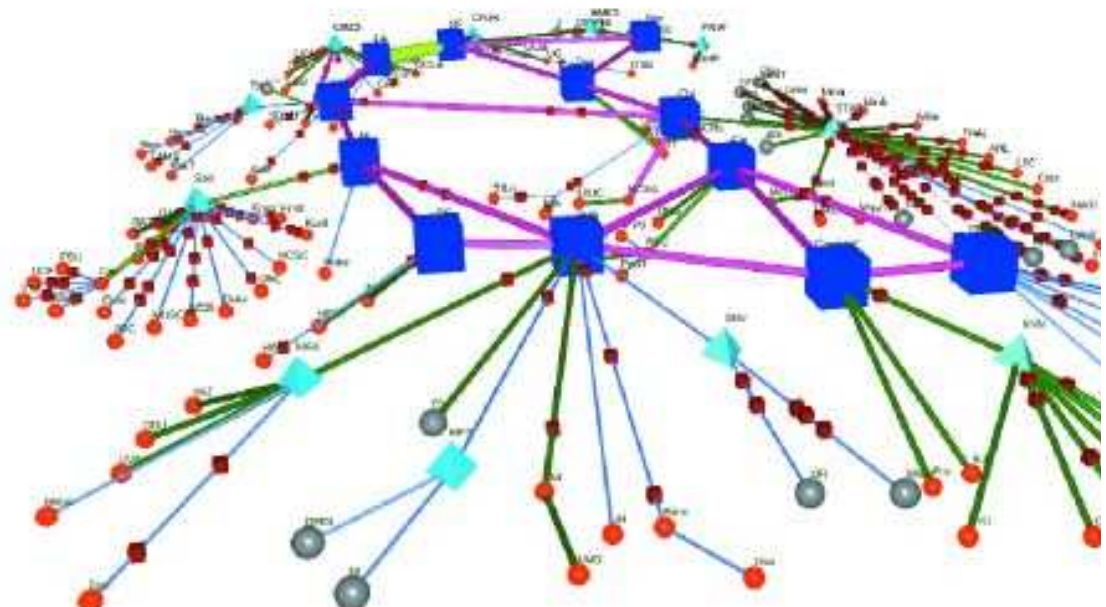
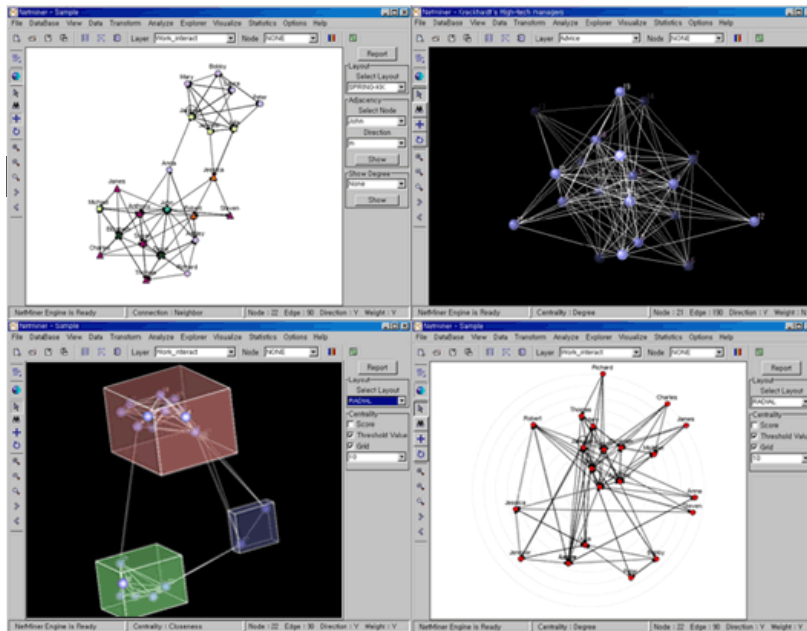
- IANA has reserved several blocks of IPv4 that have yet to be allocated to a RIR:
 - <http://www.iana.org/assignments/ipv4-address-space>
- These blocks of IPv4 addresses should never be advertised into the global internet route table
- Filters should be applied on the AS border for all inbound and outbound advertisements
- Special Use Addresses (SUA) are reserved for special use :-)
 - Defined in RFC3330
 - Examples: 127.0.0.1, 192.0.2.0/24

Total Visibility



What Is Meant by 'Telemetry'?

Te·lem·e·try— a **technology** that allows the **remote measurement and reporting of information of interest** to the system designer or operator. The word is derived from Greek roots *tele* = **remote**, and *metron* = measure





Check List

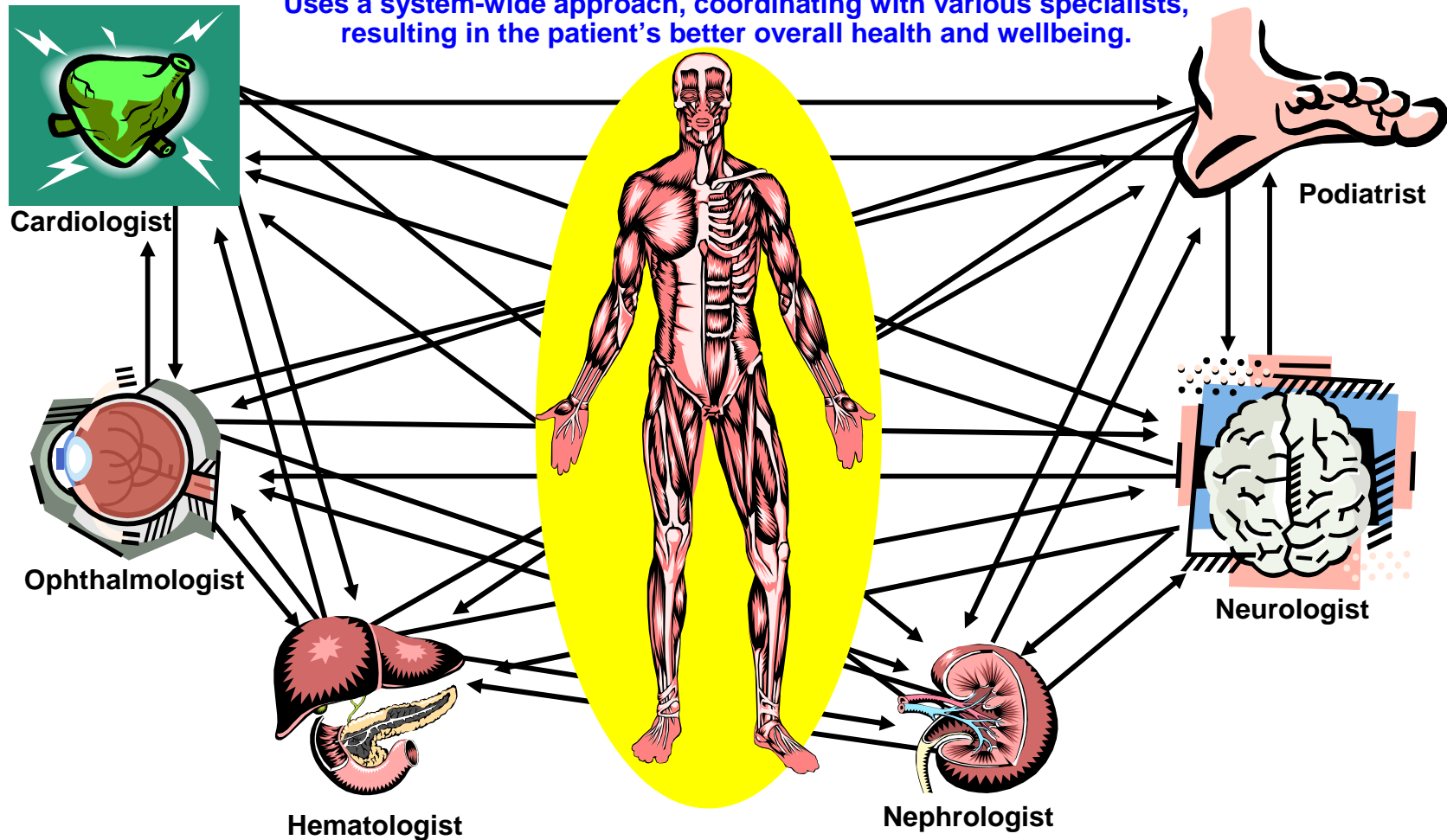


- Check SNMP. Is there more you can do with it to pull down security information?
- Check RMON. Can you use it?
- Check Netflow. Are you using it, can you pull down more?
- See addendum for lots of links.

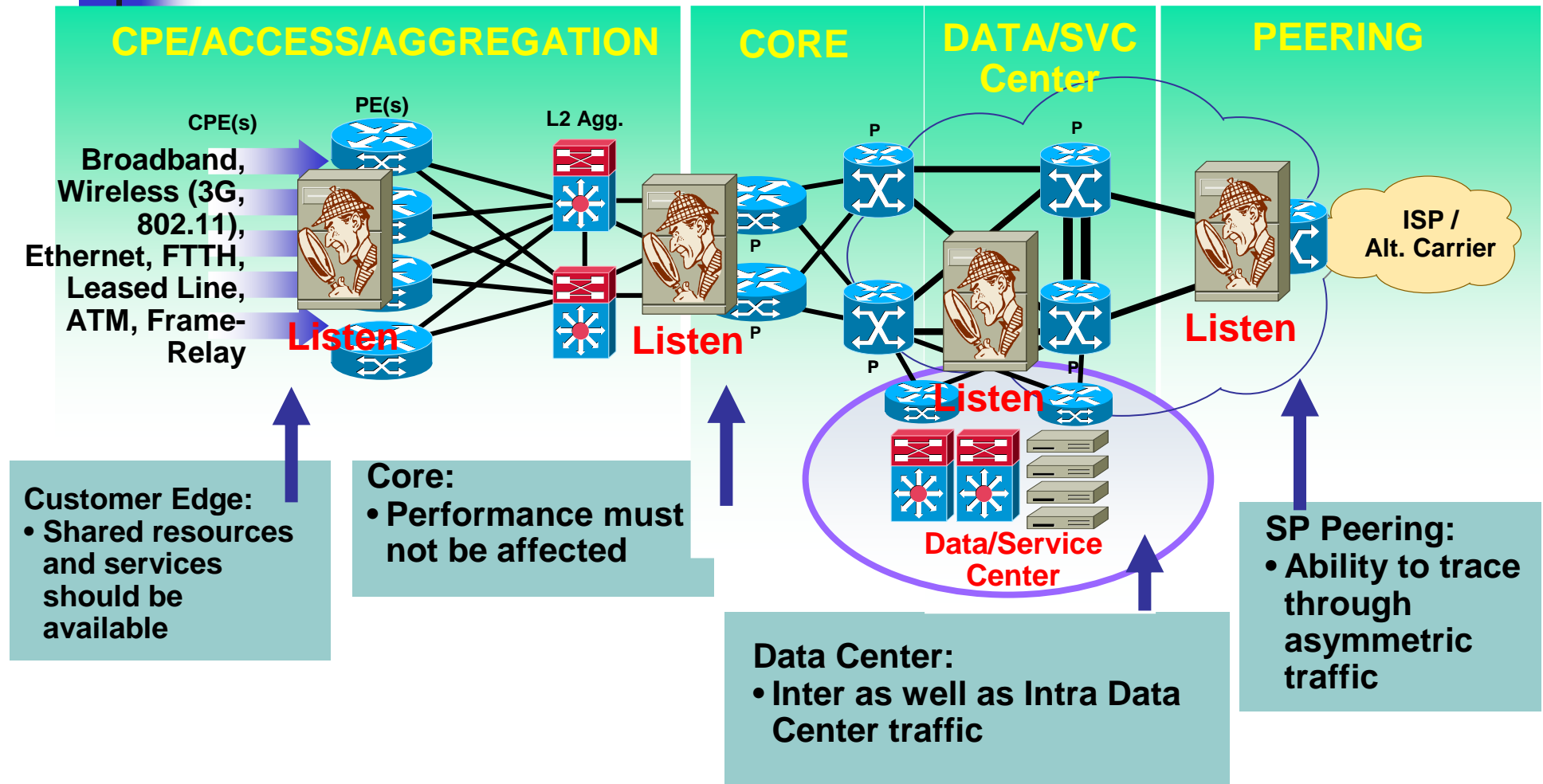
Holistic Approach to System-Wide Telemetry

Holistic Approach to Patient Care

Uses a system-wide approach, coordinating with various specialists, resulting in the patient's better overall health and wellbeing.

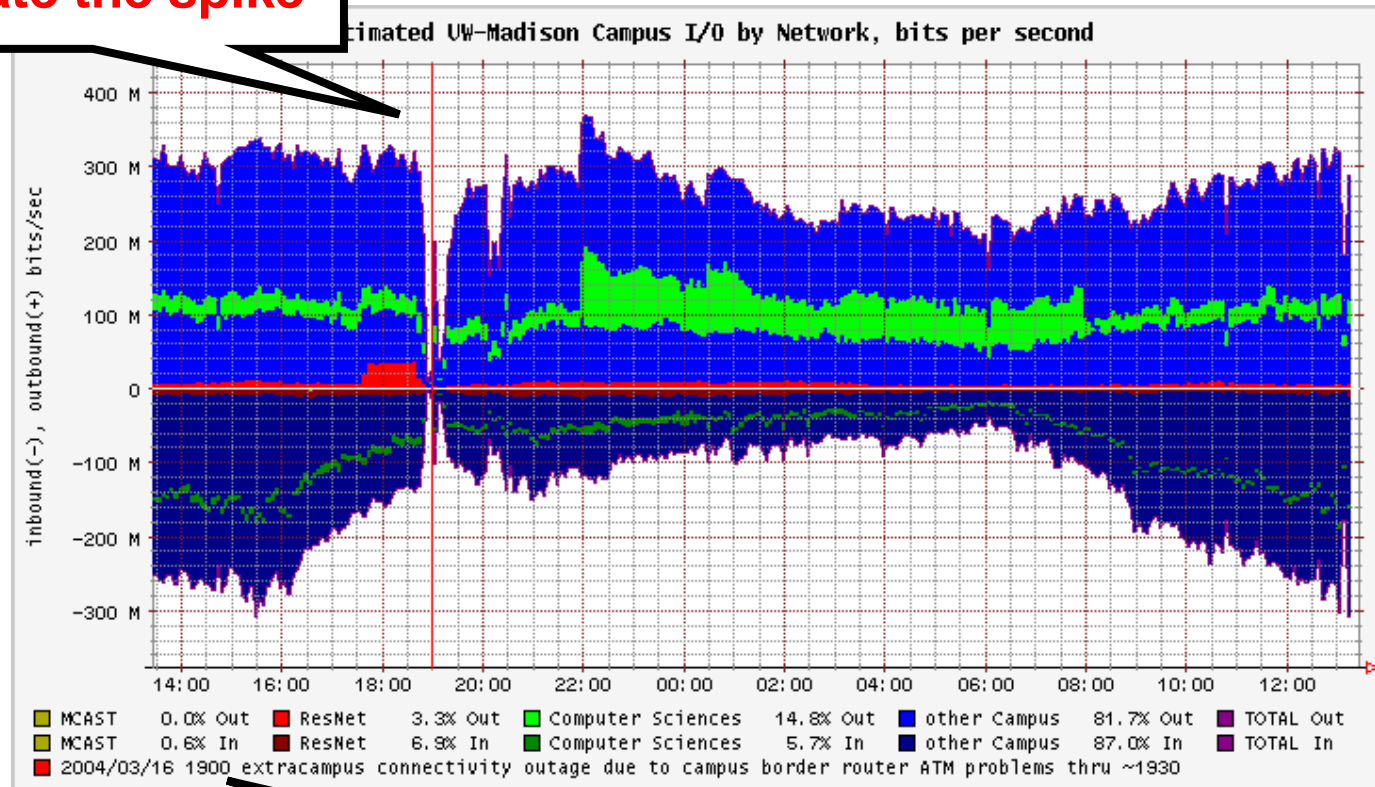


Holistic Approach to System-Wide Telemetry



Open Source Tools for NetFlow Analysis Visualization—FlowScan

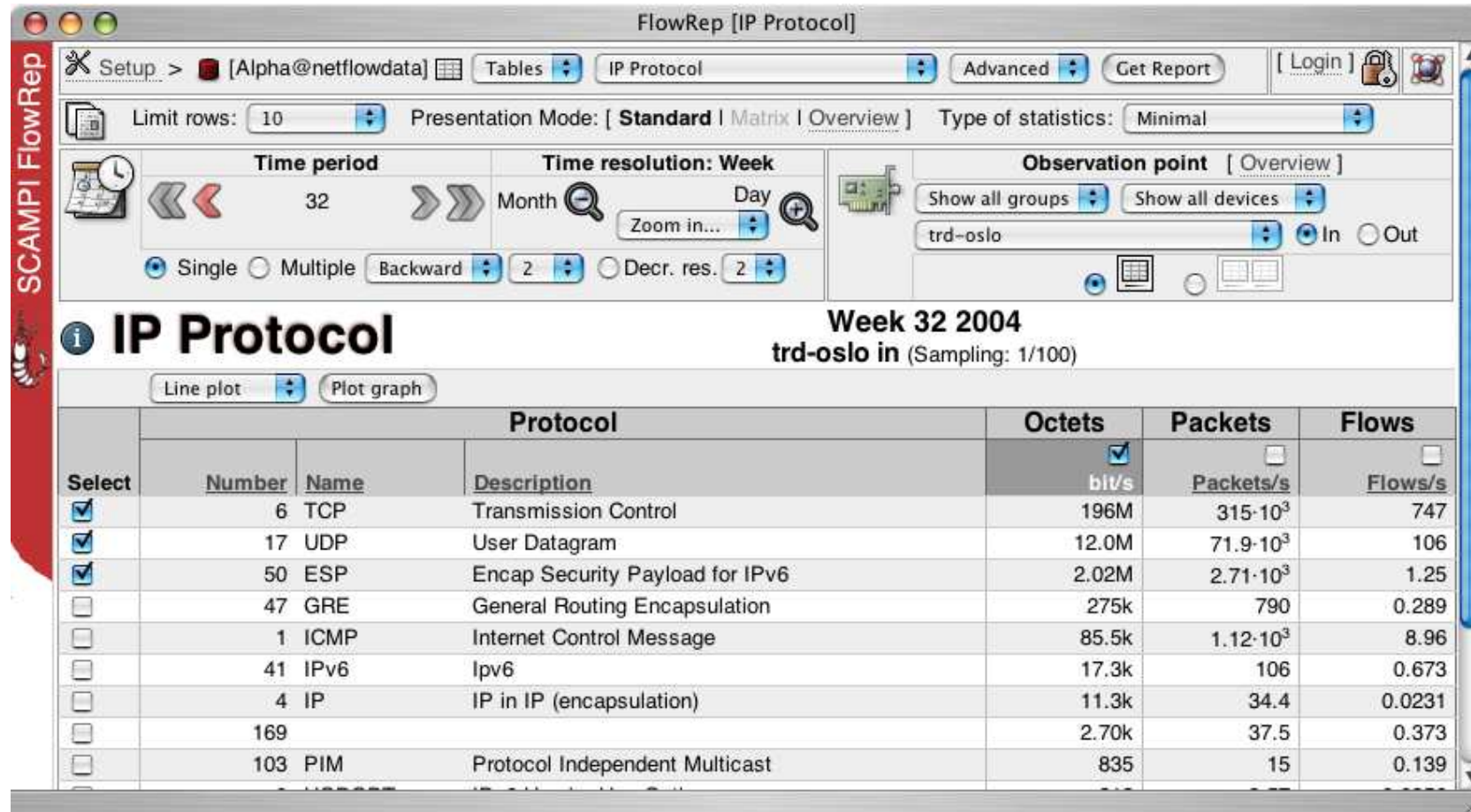
Investigate the spike



Source: University of Wisconsin

**An identified cause of
the outage**

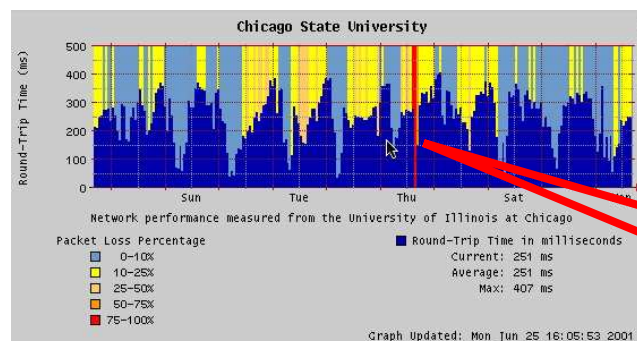
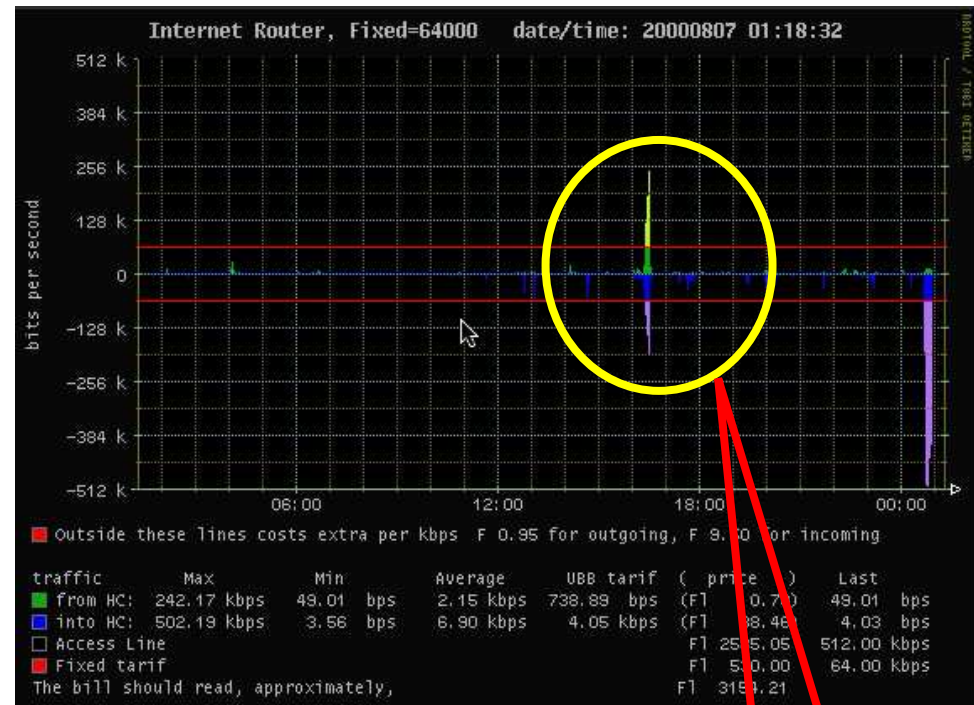
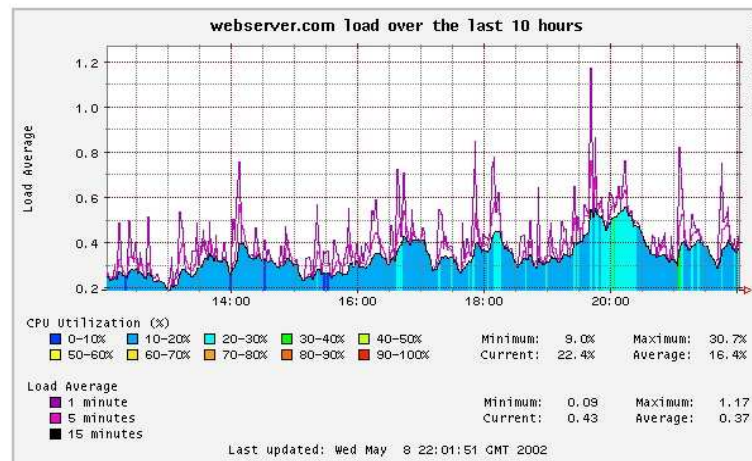
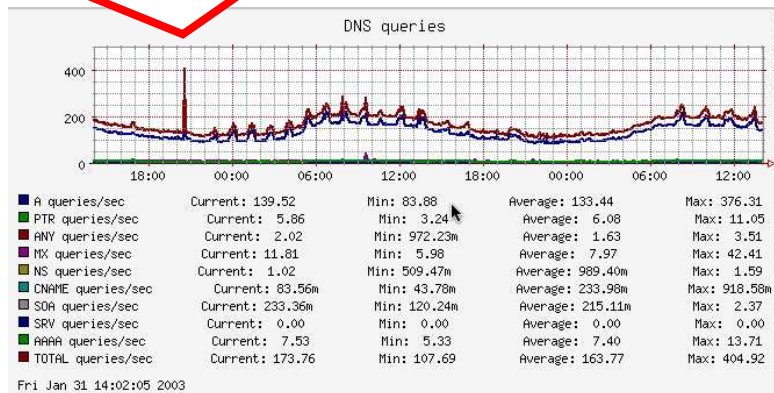
NetFlow - Stager



Source: UNINETT

Other Visualization Techniques Using SNMP Data with RRDTool

Anomaly for DNS Queries

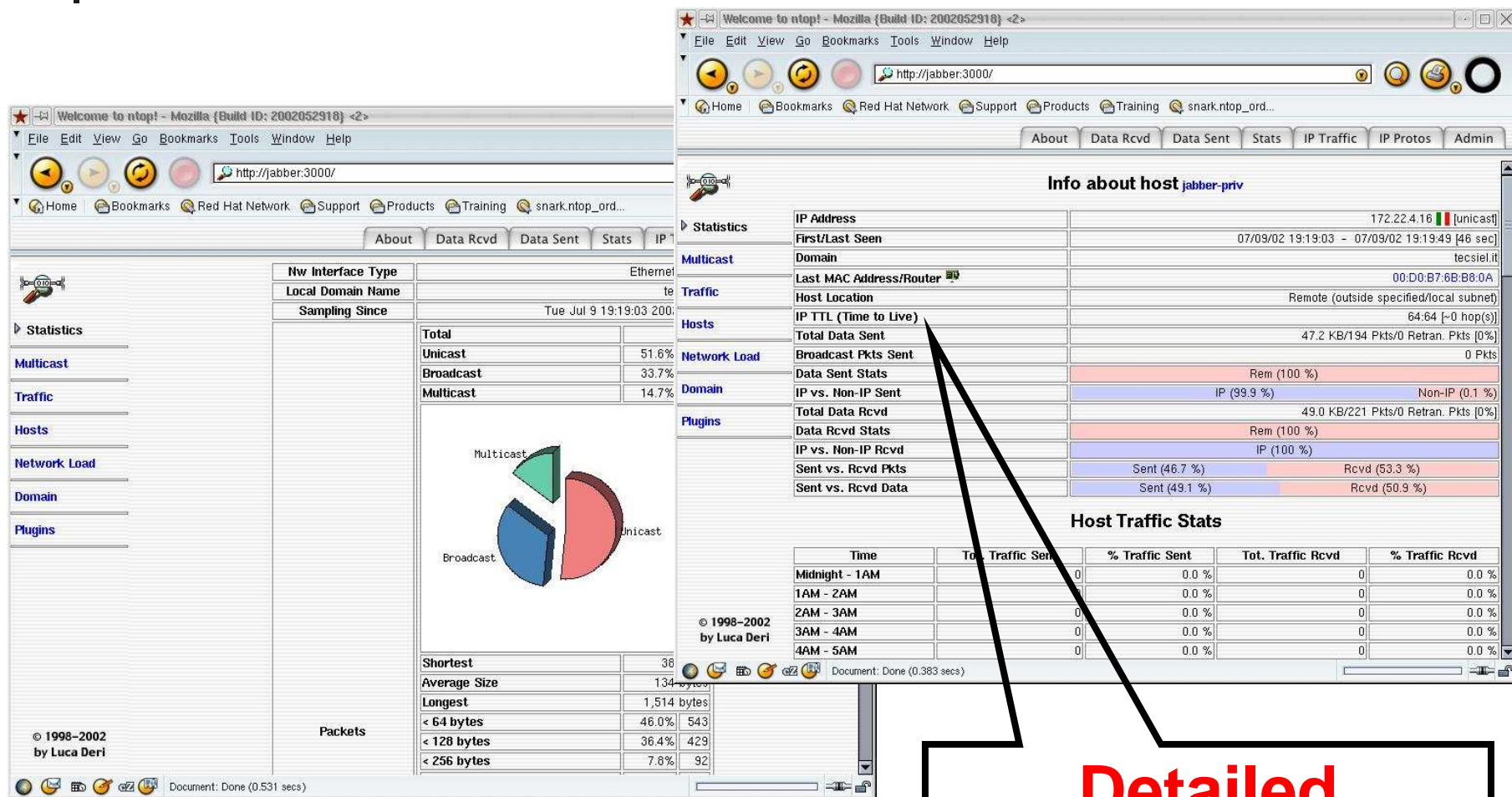


Thru'put Spike

RTT Spike

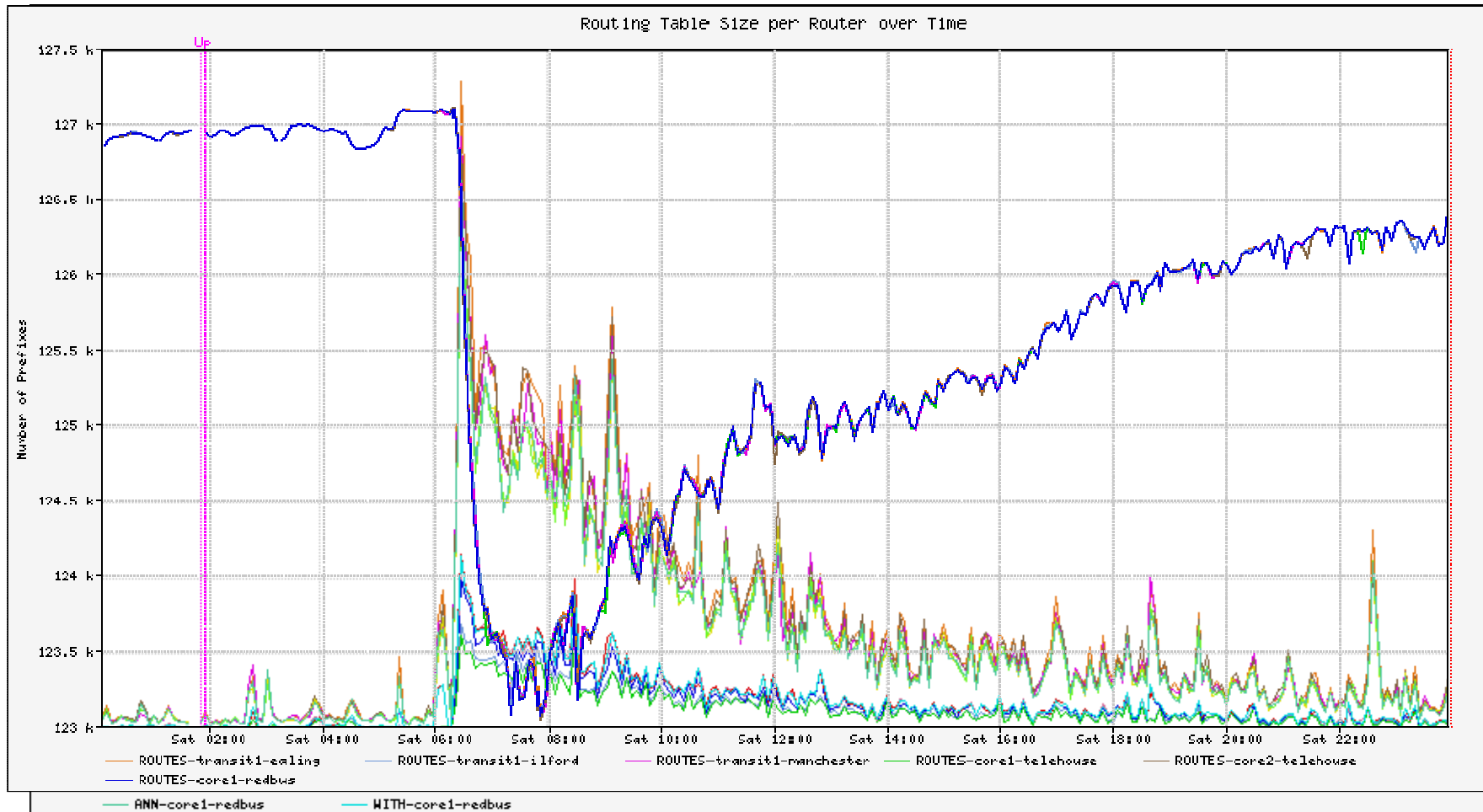
Source: <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>

Displaying RMON—ntop Examples

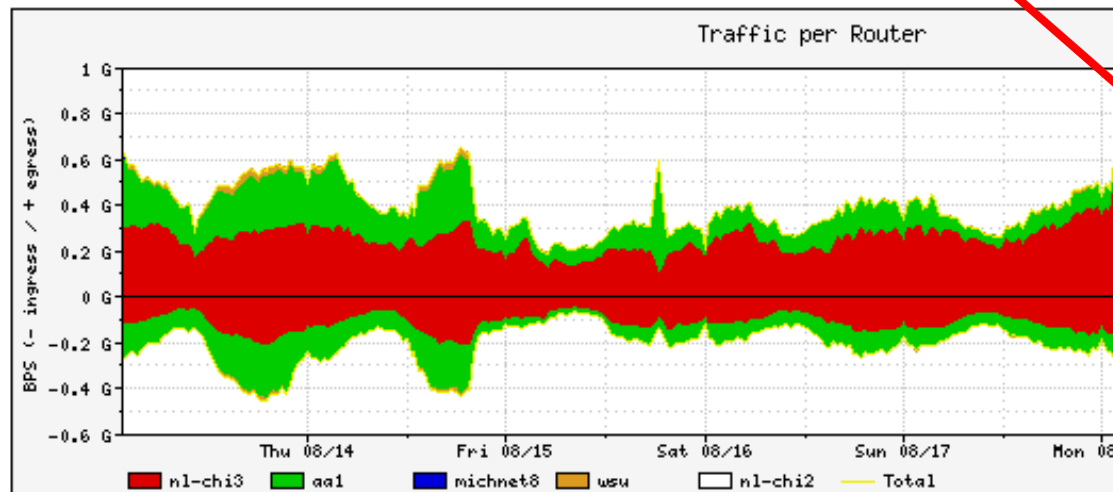
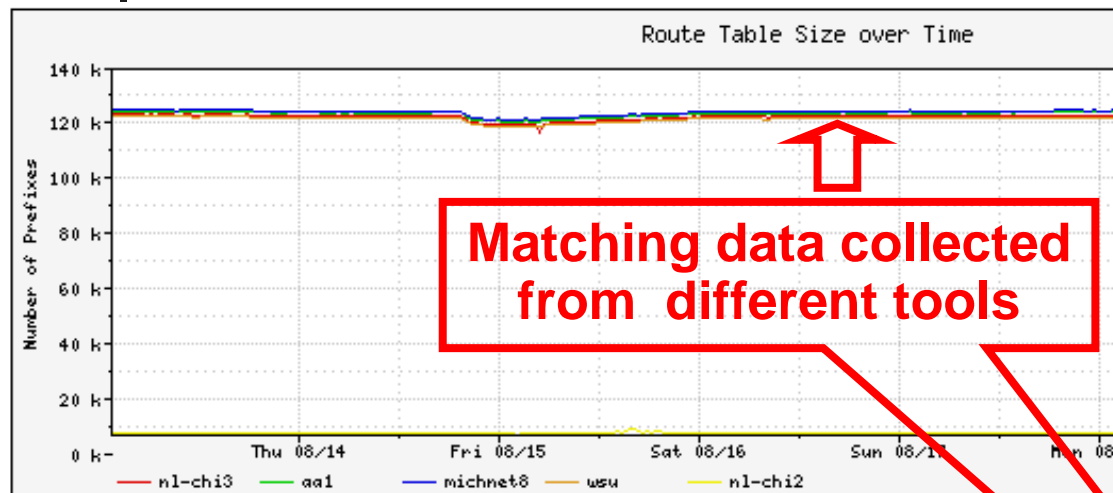


Source: <http://www.ntop.org>

BGP Example—SQL Slammer



Correlating NetFlow and Routing Data



tcsh — tcsh

```
danny@rambler% cat prefixes
```

Prefix Length	*Current	Daily Max	Daily Average
/24	65,900	68,497	67,259
/23	9,904	10,157	10,027
/22	9,053	9,211	9,110
/21	6,035	6,106	6,045
/20	8,485	8,560	8,487
/19	8,175	8,221	8,161
/18	3,007	3,031	3,005
/17	1,693	1,705	1,690
/16	7,293	7,396	7,326
/15	473	473	469
/14	263	263	262
/13	98	98	97
/12	55	55	54
/11	12	12	11
/10	6	6	5
/9	4	4	3
/8	19	19	18

Current_Total: 120,475
Max_Total: 123,814
Average_Total: 122,029

Current v. Average: 98.73% (1554 prefixes)

* Current Based on my Snapshot @9P MDT 8.14.2003

[~]
danny@rambler%



Syslog

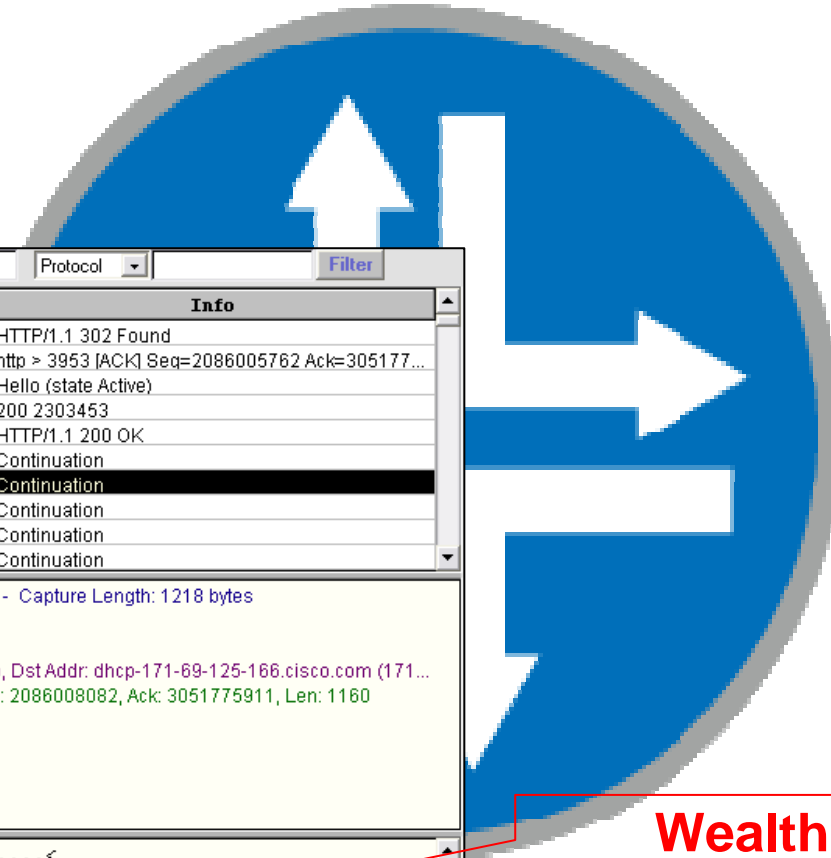
- De facto logging standard for hosts, network infrastructure devices, supported in all most routers and switches
- Many levels of logging detail available—choose the level(s) which are appropriate for each device/situation
- Logging of ACLs is generally contraindicated due to CPU overhead—NetFlow provides more info, doesn't max the box
- Can be used in conjunction with Anycast and databases such as MySQL (<http://www.mysql.com>) to provide a scalable, robust logging infrastructure
- Different facility numbers allows for segregation of log info based upon device type, function, other criteria
- Syslog-ng from http://www.balabit.com/products/syslog_ng/ adds a lot of useful functionality—HOW-TO located at <http://www.campin.net/newlogcheck.html>



Benefits of Deploying NTP

- Very valuable on a global network with network elements in different time zones
- Easy to correlate data from a global or a sizable network with a consistent time stamp
- NTP based timestamp allows to trace security events for chronological forensic work
- Any compromise or alteration is easy to detect as network elements would go out of sync with the main 'clock'
- Did you there is an NTP MIB? Some think that we may be able to use "NTP Jitter" to watch what is happening in the network.

Packet Capture Examples



Packets: 1-1000 of 1470

Pkt	Time(s)	Size	Source	Destination	Protocol	Info
1	0.000	437	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	HTTP/1.1 302 Found
2	0.006	68	nam-6506.embu-mlab...	dhcp-171-69-125-166...	TCP	http > 3953 [ACK] Seq=2086005762 Ack=305177...
3	0.048	70	core2-e0-1.embu-mla...	ALL-ROUTERS.MCAS...	HSRP	Hello (state Active)
4	0.057	68	embu-callmgr1.embu...	192.168.79.42	MGCP	200 2303453
5	0.069	1222	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	HTTP/1.1 200 OK
6	0.069	1222	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	Continuation
7	0.075	1222	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	Continuation
8	0.075	1222	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	Continuation
9	0.075	1222	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	Continuation
10	0.084	1222	nam-6506.embu-mlab...	dhcp-171-69-125-166...	HTTP	Continuation

Packet Number: 7 - Time: May 16, 2003 12:47:17.357 - Packet Length: 1222 bytes - Capture Length: 1218 bytes

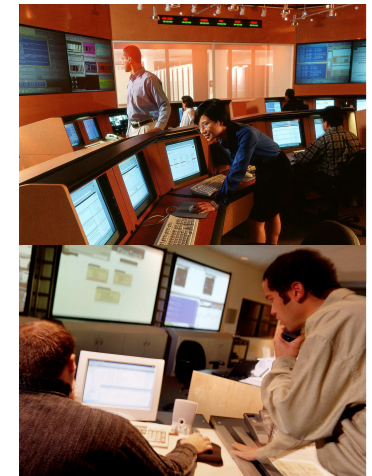
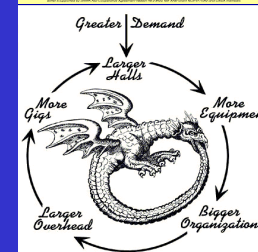
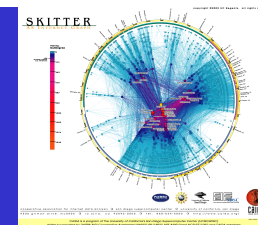
- + **ETH** Ethernet II, Src: 00:d0:d3:9d:73:d0, Dst: 00:30:94:fd:c6:17
- + **VLAN** 802.1q Virtual LAN
- + **IP** Internet Protocol, Src Addr: nam-6506.embu-mlab.cisco.com (192.168.76.12), Dst Addr: dhcp-171-69-125-166.cisco.com (171...)
- + **TCP** Transmission Control Protocol, Src Port: http (80), Dst Port: 3953 (3953), Seq: 2086008082, Ack: 3051775911, Len: 1160
- **HTTP** Hypertext Transfer Protocol
- HTTP** Data (1160 bytes)

```
0000  00 30 94 fd c6 17 00 d0 d3 9d 73 d0 81 00 00 3c  .0.....s....<
0010  08 00 45 00 04 b0 0d 40 40 00 3f 06 f4 67 c0 a8  ..E....00.?.g..
0020  4c 0c ab 45 7d a6 00 50 0f 71 7c 55 f5 12 b5 e6  L..E)...P.qIU...
0030  67 a7 50 10 43 98 0a 57 00 00 25 22 20 62 6f 72  g.P.C..W..%" bor
0040  64 65 72 3d 22 30 22 20 63 65 6c 6c 73 70 61 63  der="0" cellspac
0050  69 6e 67 3d 22 30 22 20 63 65 6c 6c 70 61 64 64  ing="0" cellpadd
```

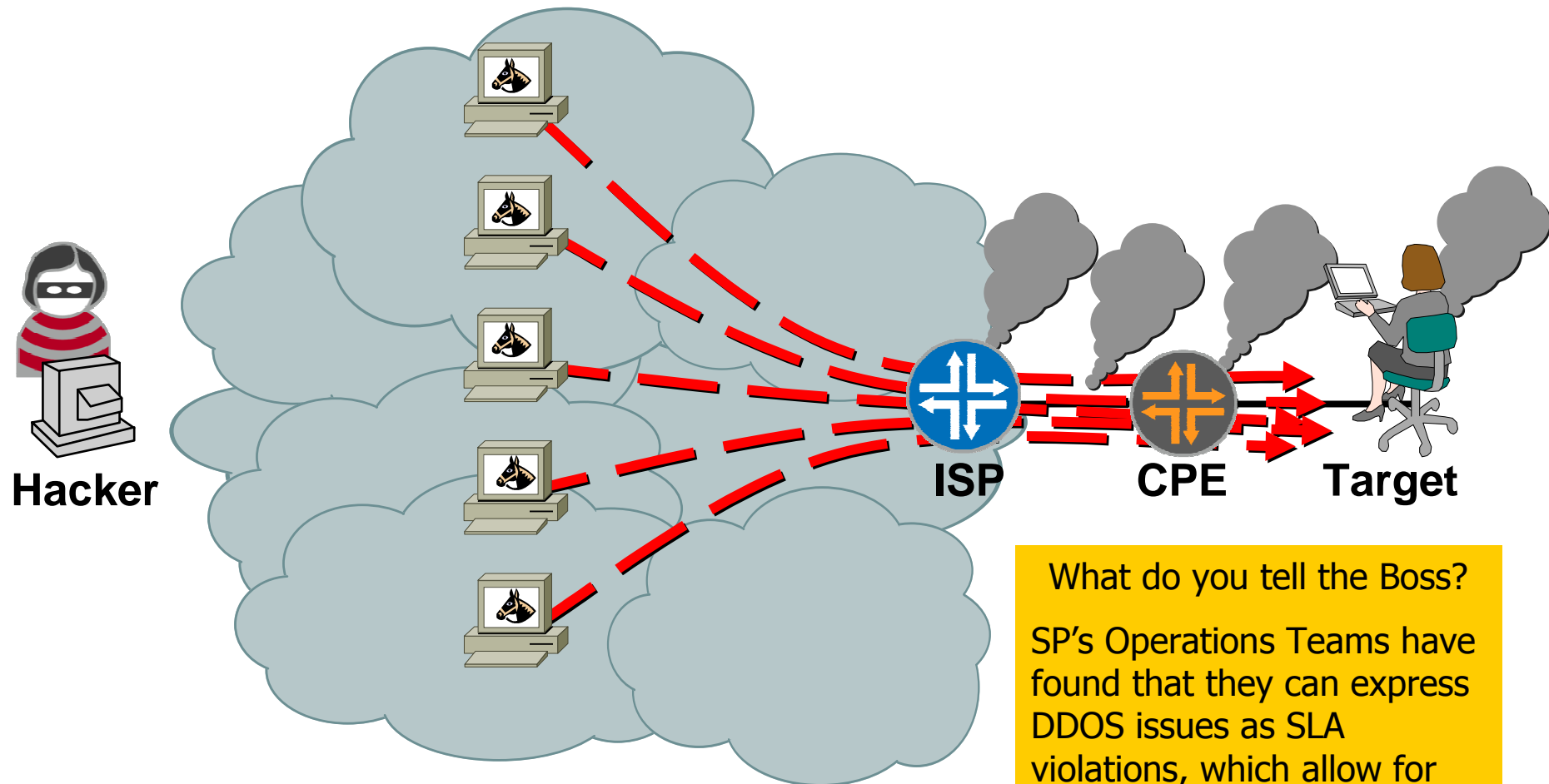
Source: <http://www.ethereal.com>

Wealth of
information, L1-L7
raw data for
analysis

Putting the Tools to Work – DDOS Attack



DDOS = SLA Violation!



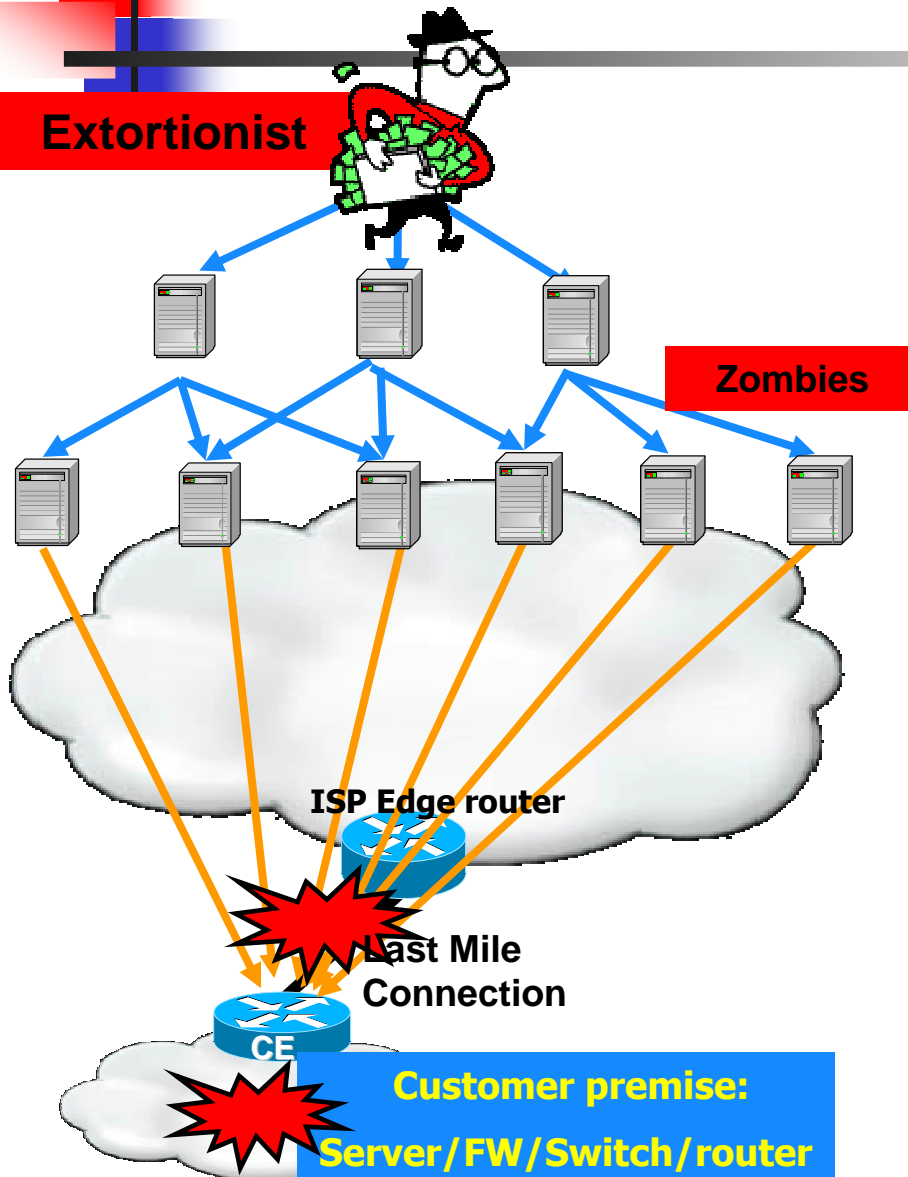
What do you tell the Boss?

SP's Operations Teams have found that they can express DDOS issues as SLA violations, which allow for their management to understand why they need to act.

BOTNETS – Making DDoS Attacks Easy

2 for 1 Special

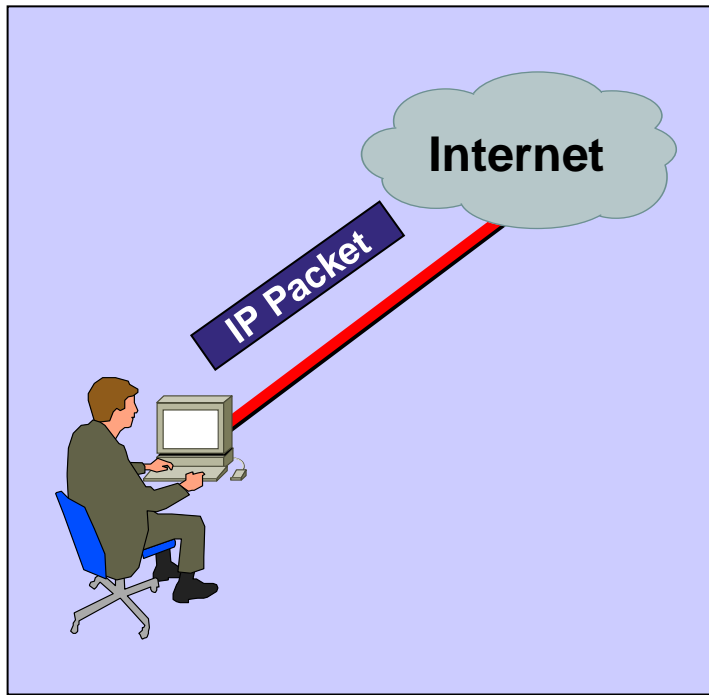
Extortionist



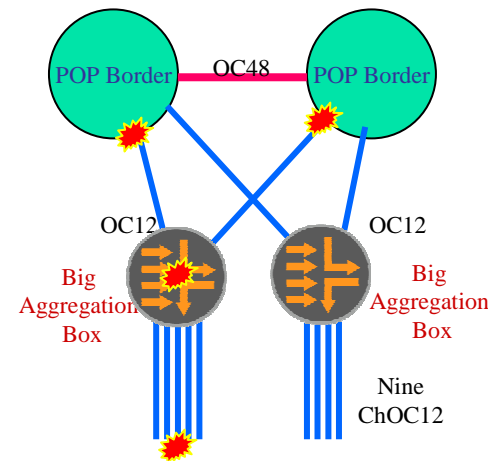
BOTNETs for Rent!

- A BOTNET is comprised of computers that have been broken into and planted with programs (zombies) that can be directed to launch attacks from a central controller computer
- BOTNETs allow for all the types of DDOS attacks: ICMP Attacks, TCP Attacks, and UDP Attacks, http overload
- Options for deploying BOTNETs are extensive and new tools are created to exploit the latest system vulnerabilities
- A relatively small BOTNET with only 1000 zombies can cause a great deal of damage.
- For Example: 1000 home PCs with an average upstream bandwidth of 128KBit/s can offer more than 100MBit/s
- Size of attacks are ever increasing and independent of last mile bandwidth

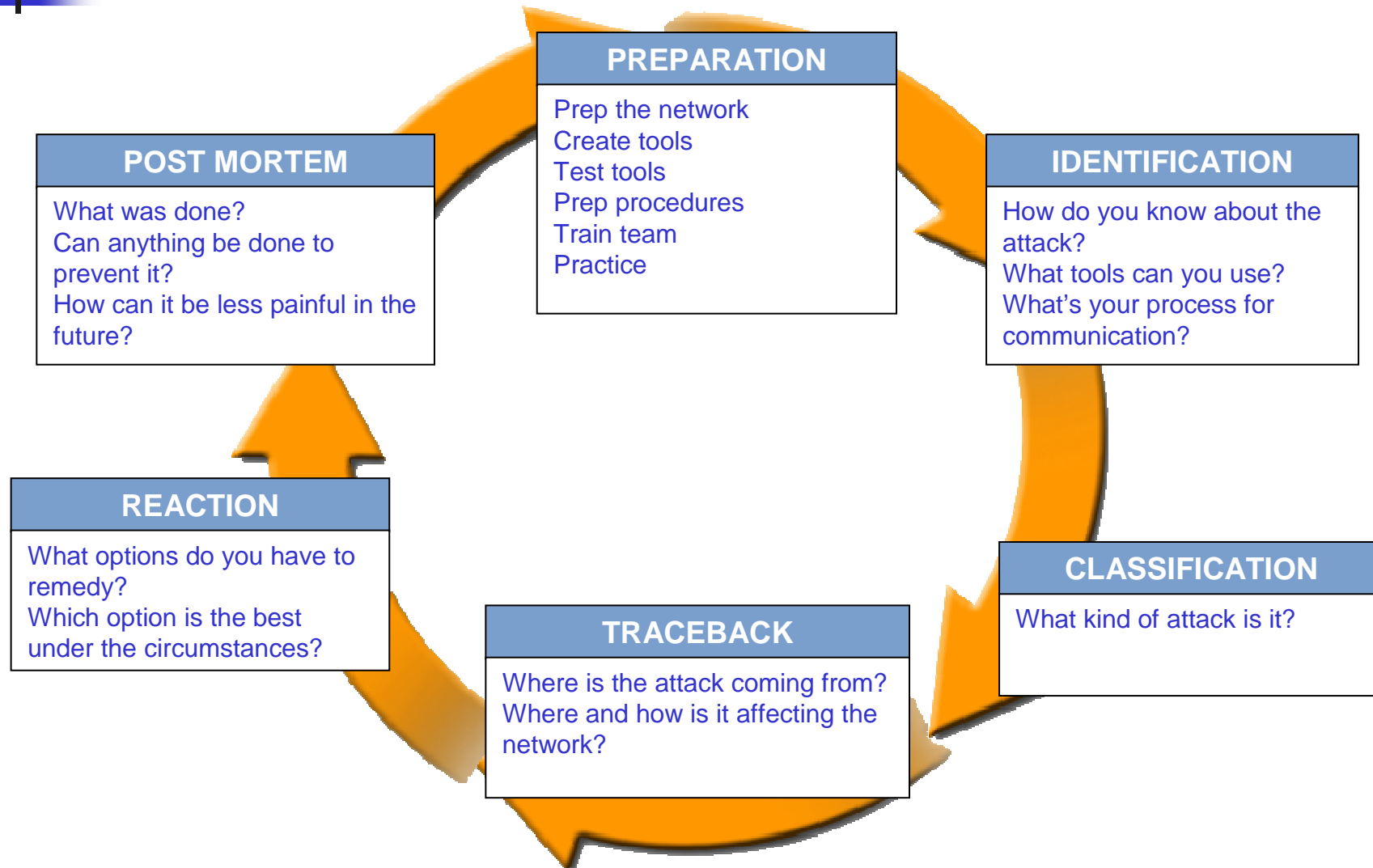
It is all about the packet



- 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 DoS attacks, the questions are who and where will the "drop the packet" action occur?



Six Phases of Incident Response

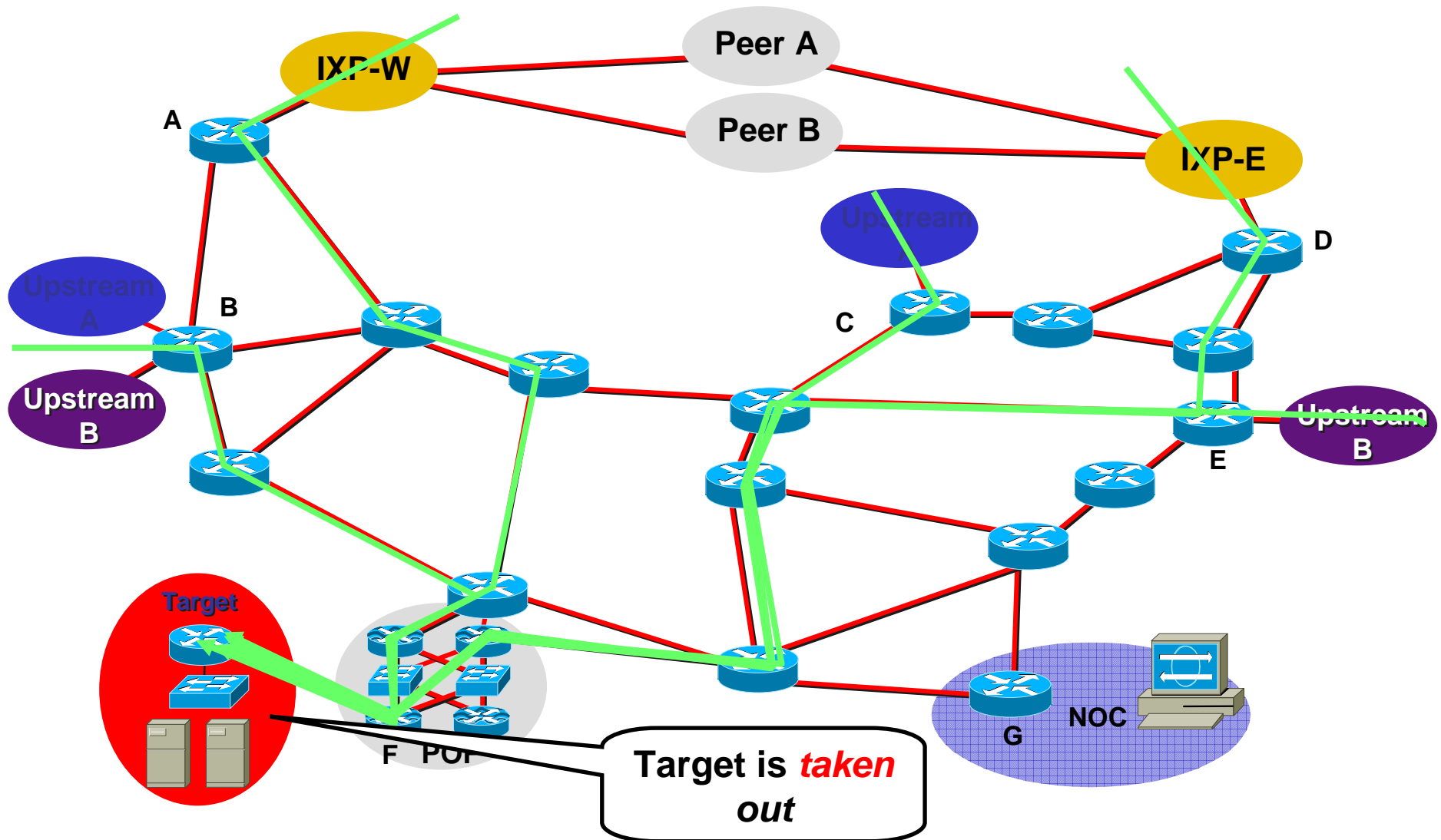




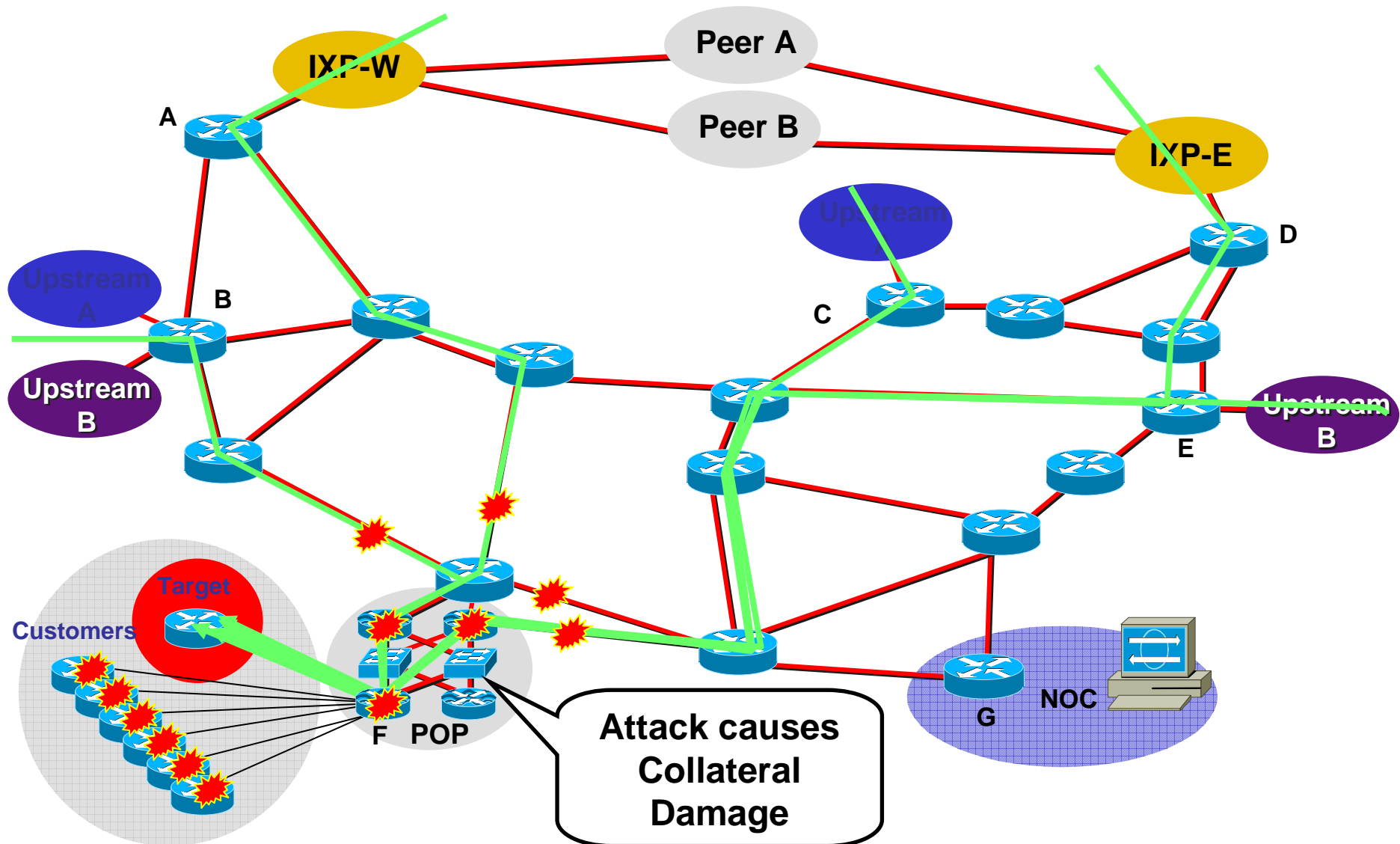
SITREP

- Everything is normal in the Network.
- Then alarms go off – something is happening in the network.

Customer Is DOSed—Before



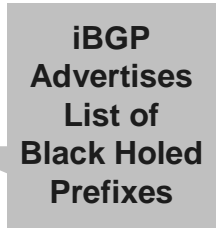
Customer Is DOSed—Before— Collateral Damage





SITREP – Attack in Progress

- Attack on a customer is impacting a number of customers.
- COLATERAL DAMAGE INCIDENT!
- Immediate Action: Solve the Collateral Damage issues.

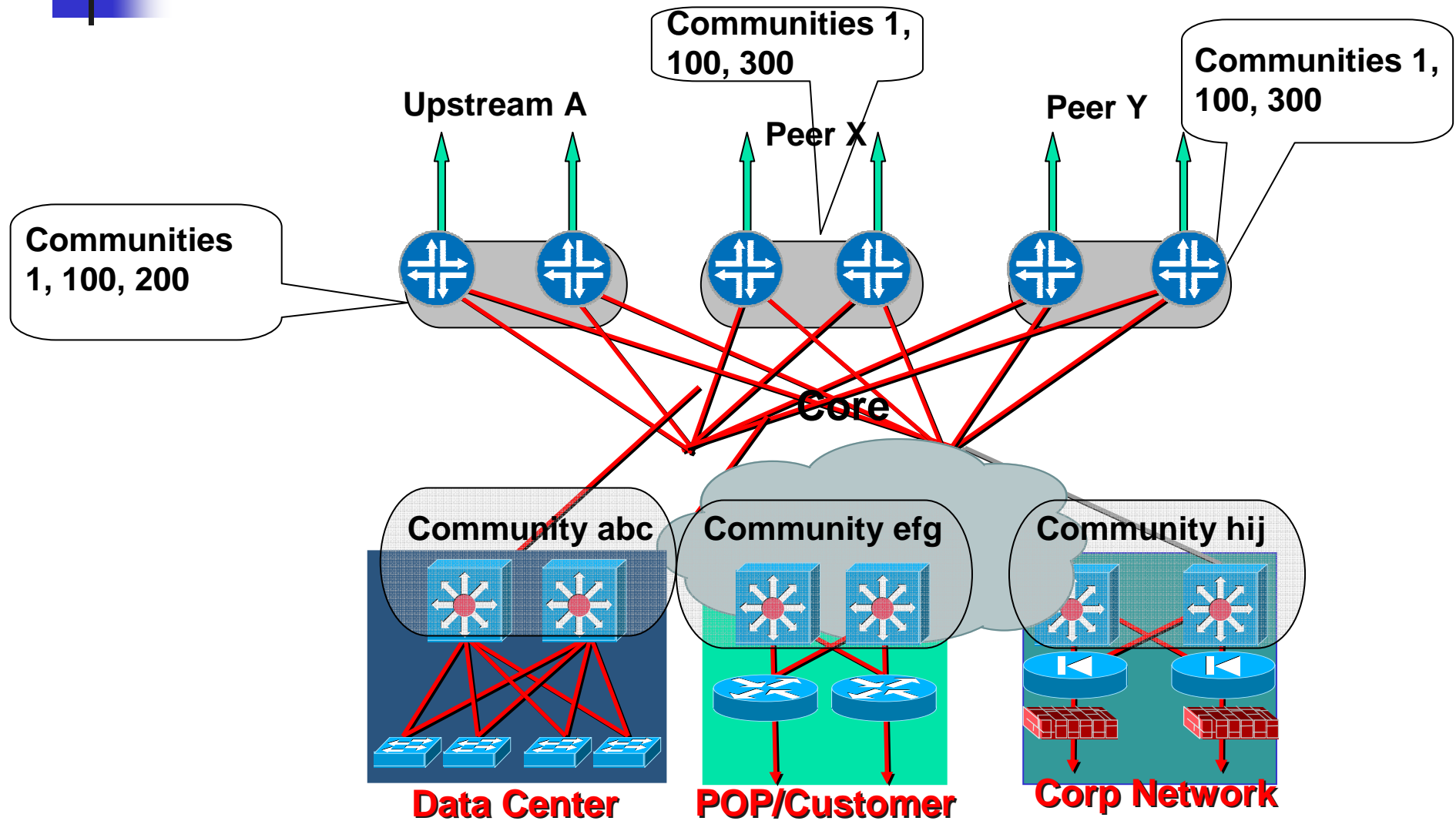




SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Options:
 - Sink Hole a part of the traffic to analyze.
 - Watch the DOS attack and wait for Attack Rotation or cessation.
 - Activate “Clean Pipes” for a Full Service Recovery.

Remote Triggered Drops and Communities

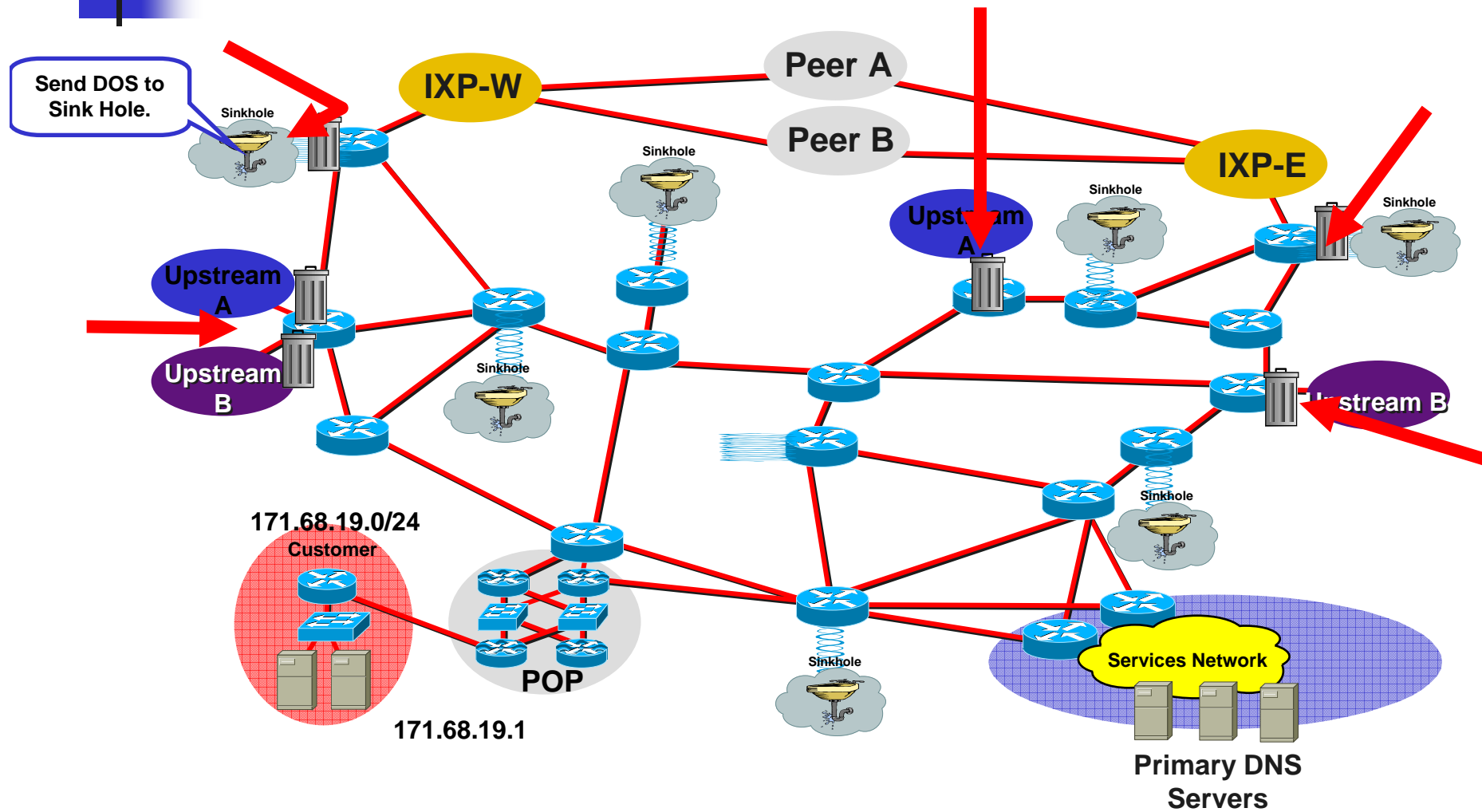




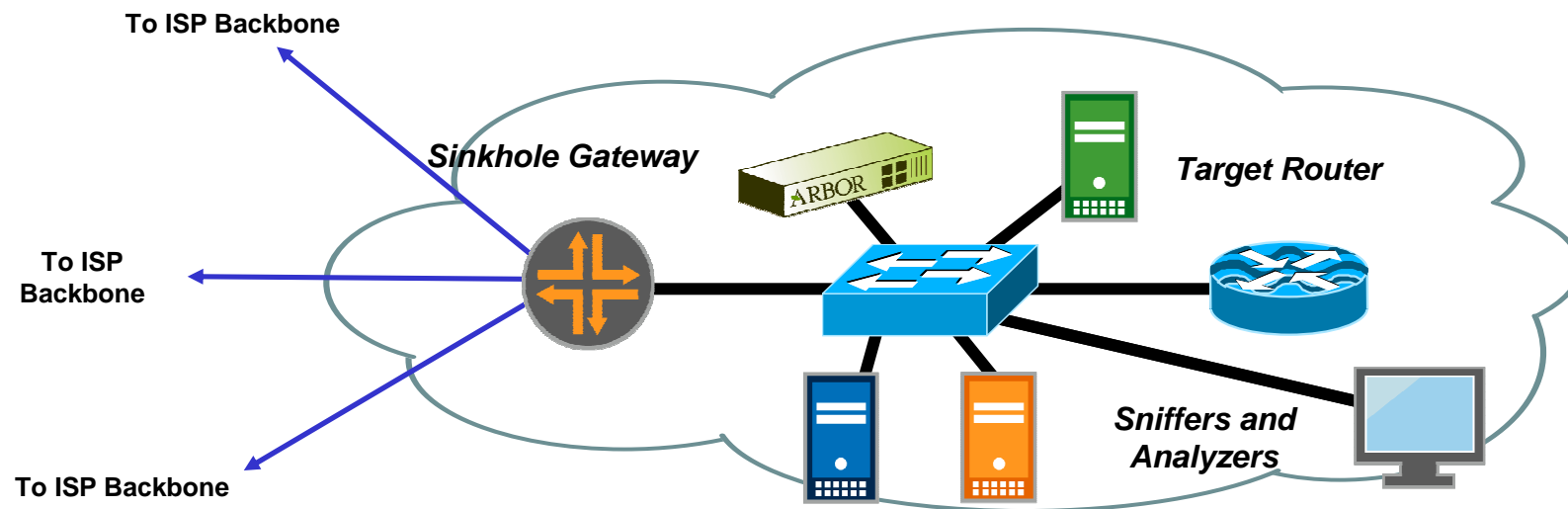
SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Action: Monitor the Attack & Get more details on the Attack – Use BGP Community based triggering to send one regions flow into a Sink Hole

BGP Community Trigger to Sinkhole



Analyze the Attack



- Use the tools available on the Internet and from Vendors to analyze the details of the attack.
- This will provide information about what you can or cannot do next.



SITREP – Attack in Progress

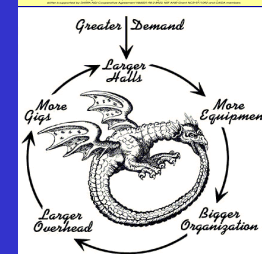
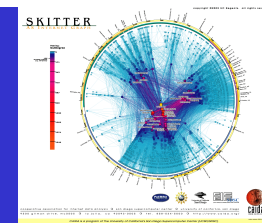
- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Action: Provide the Customer who is the victim with a Clean Pipes FULL SERVICE RECOVERY (off to vendor specific details).



What is Full Service Recovery

- “Clean Pipes” is a term used to describe *full service recovery*. The expectations for a full service recovery is:
 - DDOS Attack is in full force and ALL customer services are operating normally – meeting the contracted SLA.
 - The Device used for the full service recovery is not vulnerable to the DDOS & the infrastructure is not vulnerable to collateral damage.
- Full Service Recovery/Clean Pipes products are very specialized. Talk to the appropriate vendor.

SUMMARY

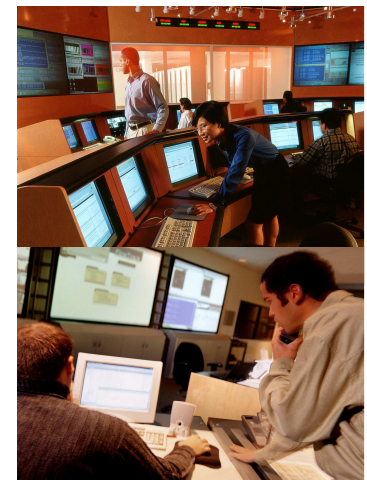
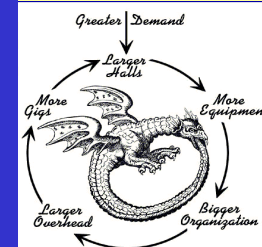
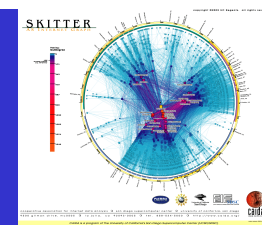





These Top 10 are a Basic Foundation

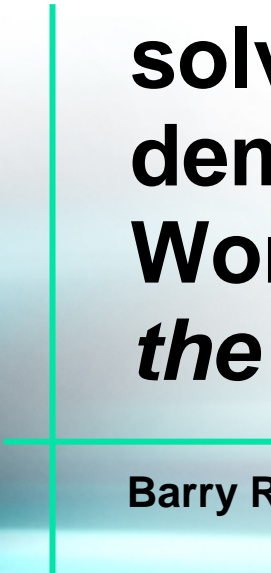
- These 10 techniques are proven as the foundation for all the SP Security developments deployed and used today.
- They are a starting point – opening the door for other techniques which help a SP save money, meet customer SLAs, and keep their business moving forward.

Communications Addendum





“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”



Barry Raveendran Greene



Preparation as Empowerment

- It is imperative that an SP's operations team prepare by empowering them for action.
 - 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?



Important Points

- Create your company's Computer Emergency Response Team
- Know your peers (neighboring CERTs), build relationships
- Get on NSP-SEC mailing list and on iNOC Phone
- Know Each's Vendors Security Team

Example: psirt@cisco.com, security-alert@cisco.com and www.cisco.com/security to contact Cisco Systems.

- Be prepared ! Define what to do & whom to contact for various incidents.



Step #1 – Take Care of Your Responsibilities

- Before knocking on doors to collect information on others, it is best that you take the time to insure you are fulfilling your responsibilities to facilitate communications.
- Make sure you have all the E-mail, phones, pagers, and web pages complete.
- Make sure you have procedures in place to answer and communicate.



OPSEC Communications

- Operations teams have a responsibility to communicate with
 - All peers, IXPs, and transit providers
 - Teams inside their organization
 - Customers connected to their network
 - Other ISPs in the community
- E-mail and Web pages are the most common forms of communication
- Pagers and hand phones are secondary communication tools



OPSEC Communications

Q. Does noc@someisp.net work?

Q. Does security@someisp.net work?

Q. Do you have an Operations and Security Web site with:

- Contact information
- Network policies (i.e. RFC 1998+++)
- Security policies and contact information

Q. Have you registered you NOC information at one of the NOC Coordination Pages?

- <http://puck.nether.net/netops/nocs.cgi>



SOC's Public Mailboxes

- RFC 2142 defines E-mail Aliases all ISPs should have for customer – ISP and ISP – ISP communication
- Operations addresses are intended to provide

MAILBOX	AREA	USAGE
-----	-----	-----
ABUSE	Customer Relations	Inappropriate public behavior
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries



/Security Web Page

- New Industry Practices insist that every IT company has a /security web page. This page would include:
 - Incident Response contacts for the company.
 - 7*24 contact information
 - Pointers to best common practices
 - Pointer to company's public security policies
 - Etc.
- See www.microsoft.com/security, www.cisco.com/security or www.juniper.net/security as an examples.



Emergency Customer Contact List

- E-mail alias and Web pages to communicate to your customer
 - Critical during an Internet wide incident
 - Can be pushed to sales to maintain the contact list
 - Operations should have 7*24 access to the customer contact list
 - Remember to exercise the contact list (looking for bounces)



Exercising the Customer Contact List

■ Use Internet warning to look for bounces

Dear Customers,

You are receiving this email because you have subscribed to one or more services with Infoserve. We have received a virus alert from security authorities and we believe that you should be informed (please see information below). If you do not wish to be included in future information service, please click "Reply" and type "Remove from subscription" in the subject field.

We have received warning from security authorities on a new virus, W32.Sobig.E@mm. W32.Sobig.E@mm is a new variant of the W32.Sobig worm. It is a mass-mailing worm sends itself to all the email addresses, purporting to have been sent by Yahoo (support@yahoo.com) or obtained email address from the infected machine. The worm finds the addresses in the files with the following extensions: .wab .dbx .htm .html .eml .txt

You should regularly update your antivirus definition files to ensure that you are up-to-date with the latest protection.

For more information, please follow the following links:

Information from Computer Associates:	http://www3.ca.com/solutions/collateral.asp?CT=27081&CID=46275
Information from F-Secure:	http://www.europe.f-secure.com/v-descs/sobig_e.shtml
Information from McAfee:	http://vil.mcafee.com/dispVirus.asp?virus_k=100429
Information from Norman:	http://www.norman.com/virus_info/w32_sobig_e_mm.shtml
Information from Sophos:	http://www.norman.com/virus_info/w32_sobig_e_mm.shtml
Information from Symantec:	http://www.symantec.com/avcenter/venc/data/w32.sobig.e@mm.html
Information from Trend Micro:	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.E



Remember to Communicate

- Make sure there is someone behind all the E-mail aliases
- It is of no use to have a mean for people to communicate with your when you have no one behind the alias/phone/pager/web page to communicate back
- Many aliases are **unmanned**—with E-mail going into limbo



CERTs (Computer Emergency Response Teams)

- Origin: The Internet Worm, 1988
- Creation of “The” CERT-CC (co-ordination centre)
 - Carnegie Mellon University, Pittsburgh
 - <http://www.cert.org/>
- The names vary:
 - IRT (Incident Response Team)
 - CSIRT (Computer security incident response team)
 - ... and various other acronyms
- Start with the following URLs:
 - www.cert.org
 - www.first.org



How to Work with CERTs

- Confidentiality
- Use signed and encrypted communication
Use PGP, S/MIME or GPG, have your key signed!
- CERTs coordinate with other CERTs and ISPs
- CERTs provide assistance, help, advice
- They do not do your work!

Slide 210

BRG1

Recommended

Any SP who is using IP as business should invest. It is essential.

Sales tool.

Barry Raveendran Greene, 11/17/2005



Collecting Information from Peers

- Do you have the following information for every peer and transit provider you interconnect with?
 - E-mail to NOC, abuse, and security teams
 - Work phone numbers to NOC, abuse, and security teams
 - Cell Phone numbers to key members of the NOC, abuse, and security teams
 - URLs to NOC, abuse, and security team pages
 - All the RFC 1998+++ remote-triggered communities



Questions

- Q. Do you have the NOC and Security Contacts for every ISP you are peered?
- Q. Do you test the contact information every month (E-mail, Phone, Pager)?
- Q. Have you agreed on the format for the information you will exchange?
- Q. Do you have a customer security policy so your customers know what to expect from your Security Team?



Over Dependence on Vendors–Danger!

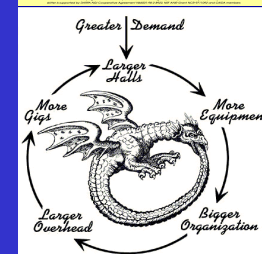
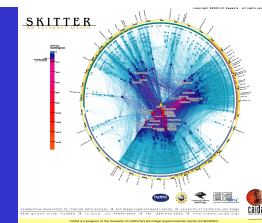
- Operators who use their Vendors as Tier 2 and higher support endanger their network to security risk.
 - Vendors are partners with an operator. They should not maintain and troubleshoot the entire network.
 - Way too many operators today see a problem on a router and then call the vendor to fix it.
 - This is not working with Turbo Worms.



What you should expect from your vendor?

- Expect 7x24 Tech Support (paid service)
- You should not expect your vendor to run your network.
- Membership in FIRST
(<http://www.first.org/about/organization/teams/>)

Total Visibility Addendum





NetFlow—More Information

- Cisco NetFlow Home—
<http://www.cisco.com/warp/public/732/Tech/nmp/netflow>
- Linux NetFlow Reports HOWTO—
<http://www.linuxgeek.org/netflow-howto.php>
- Arbor Networks Peakflow SP—
http://www.arbornetworks.com/products_sp.php



More Information about SNMP

- Cisco SNMP Object Tracker—
<http://www.cisco.com/cgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4>
- Cisco MIBs and Trap Definitions—
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>
- SNMPLink—<http://www.snmplink.org/>
- SEC-1101/2102 give which SNMP parameters should be looked at.



RMON—More Information

- IETF RMON WG—
<http://www.ietf.org/html.charters/rmonmib-charter.html>
- Cisco RMON Home—
http://www.cisco.com/en/US/tech/tk648/tk362/tk560/tech_protocol_home.html
- Cisco NAM Product Page—
<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html>



BGP—More Information

- Cisco BGP Home—
http://www.cisco.com/en/US/tech/tk365/tk80/tech_protocol_family_home.html
- Slammer/BGP analysis—
http://www.nge.isi.edu/~masseyd/pubs/massey_iwdc03.pdf
- Team CYMRU BGP Tools—
<http://www.cymru.com/BGP/index.html>



Syslog—More Information

- Syslog.org - <http://www.syslog.org/>
- Syslog Logging w/PostGres HOWTO—
http://kdough.net/projects/howto/syslog_postgresql/
- Agent Smith Explains Syslog—
<http://routergod.com/agentsmith/>



Packet Capture—More Information

- tcpdump/libpcap Home—
<http://www.tcpdump.org/>
- Vinayak Hegde's Linux Gazette article—
<http://www.linuxgazette.com/issue86/vinayak.html>



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*.



More Netflow Tools

- **NfSen - Netflow Sensor**
 - <http://nfsen.sourceforge.net/>
- **NFDUMP**
 - <http://nfdump.sourceforge.net/>
- **FlowCon**
 - <http://www.cert.org/flocon/>