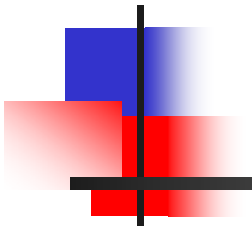


SP Security Primer 101

Peers working together to battle Attacks to the Net

Version 1.7

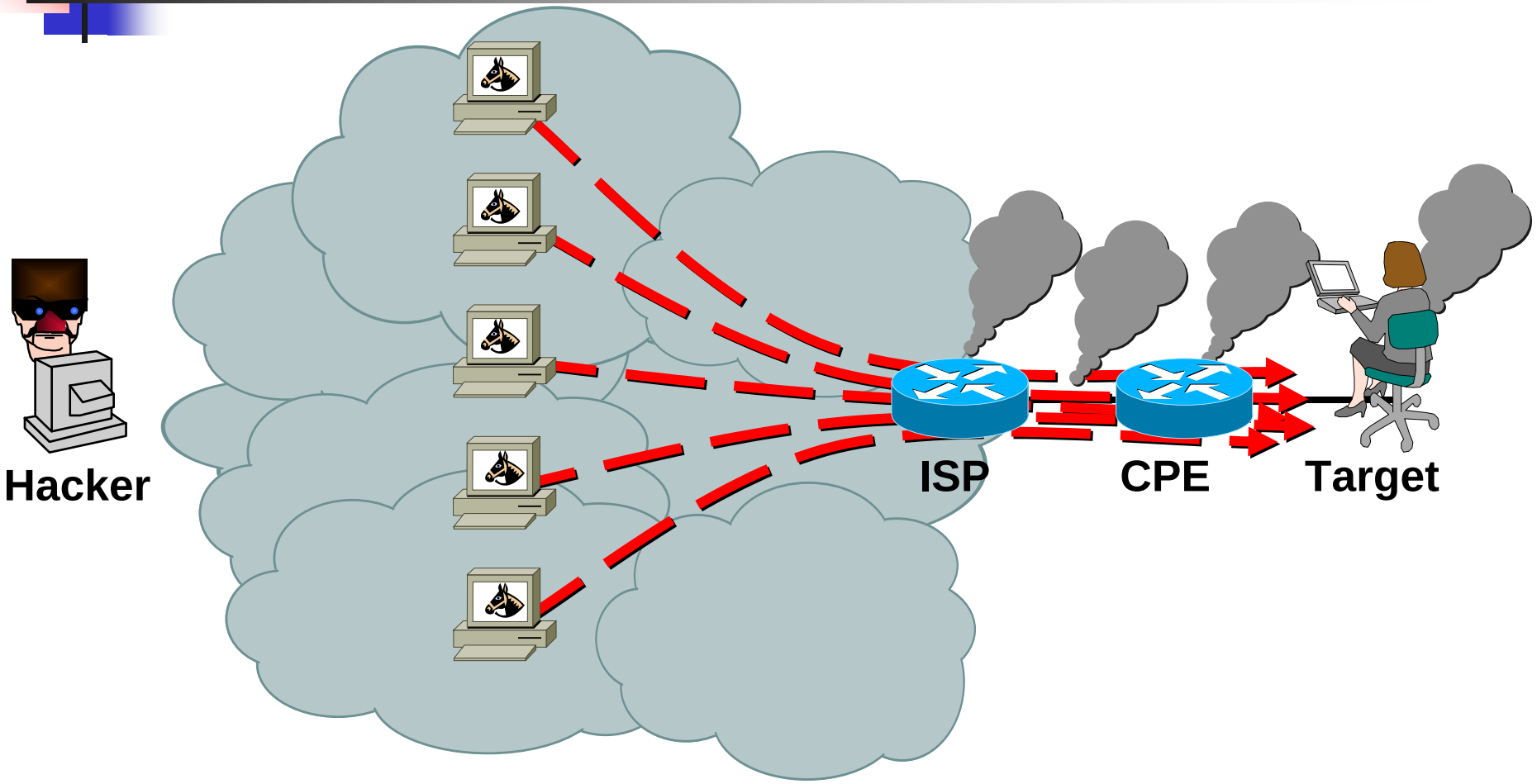
Free Use

- 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.

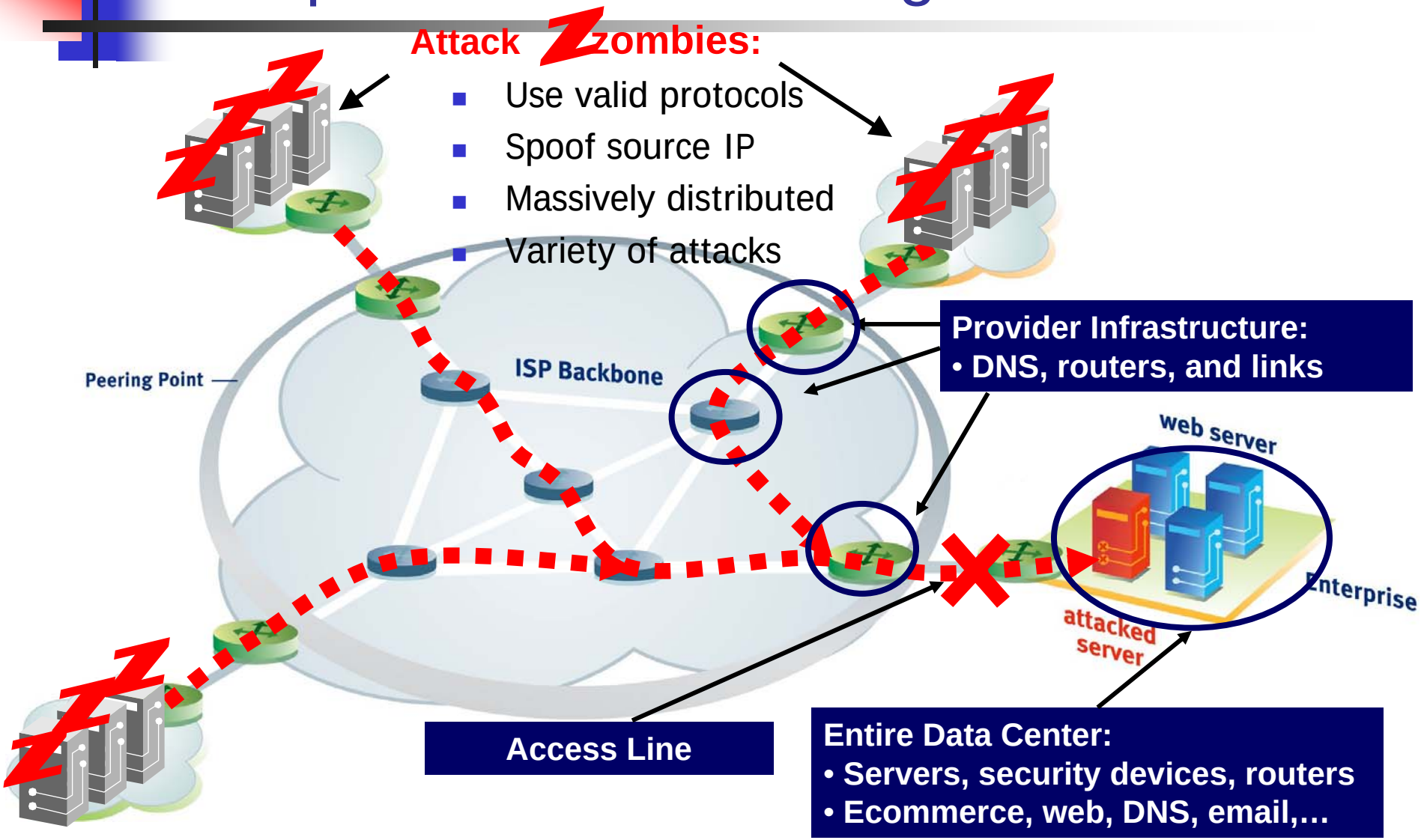
Goal

- 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

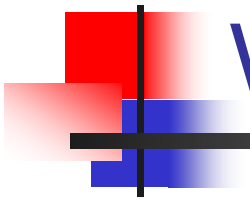
YAHOO!

amazon.com

CNN.com

ebay

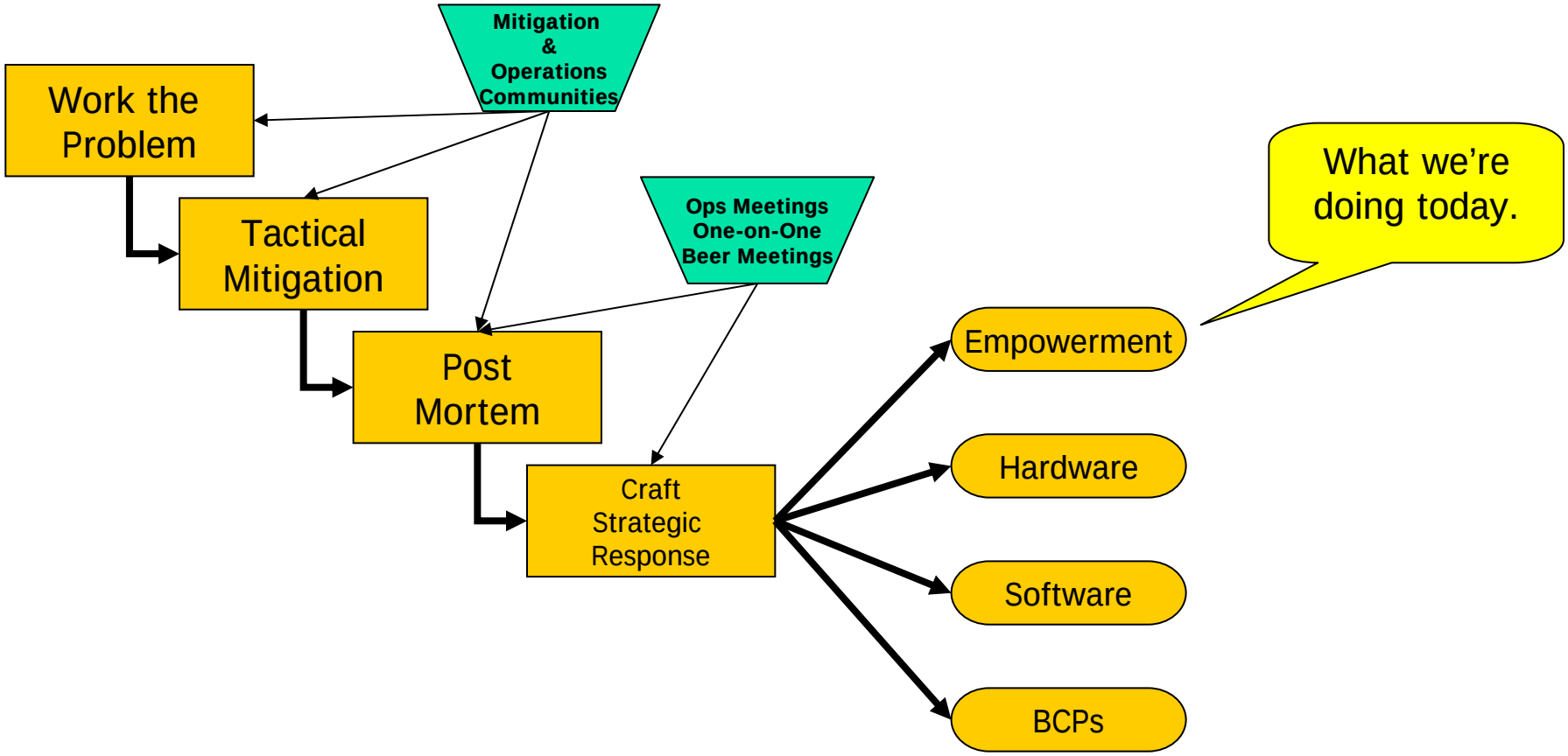
E*TRADE



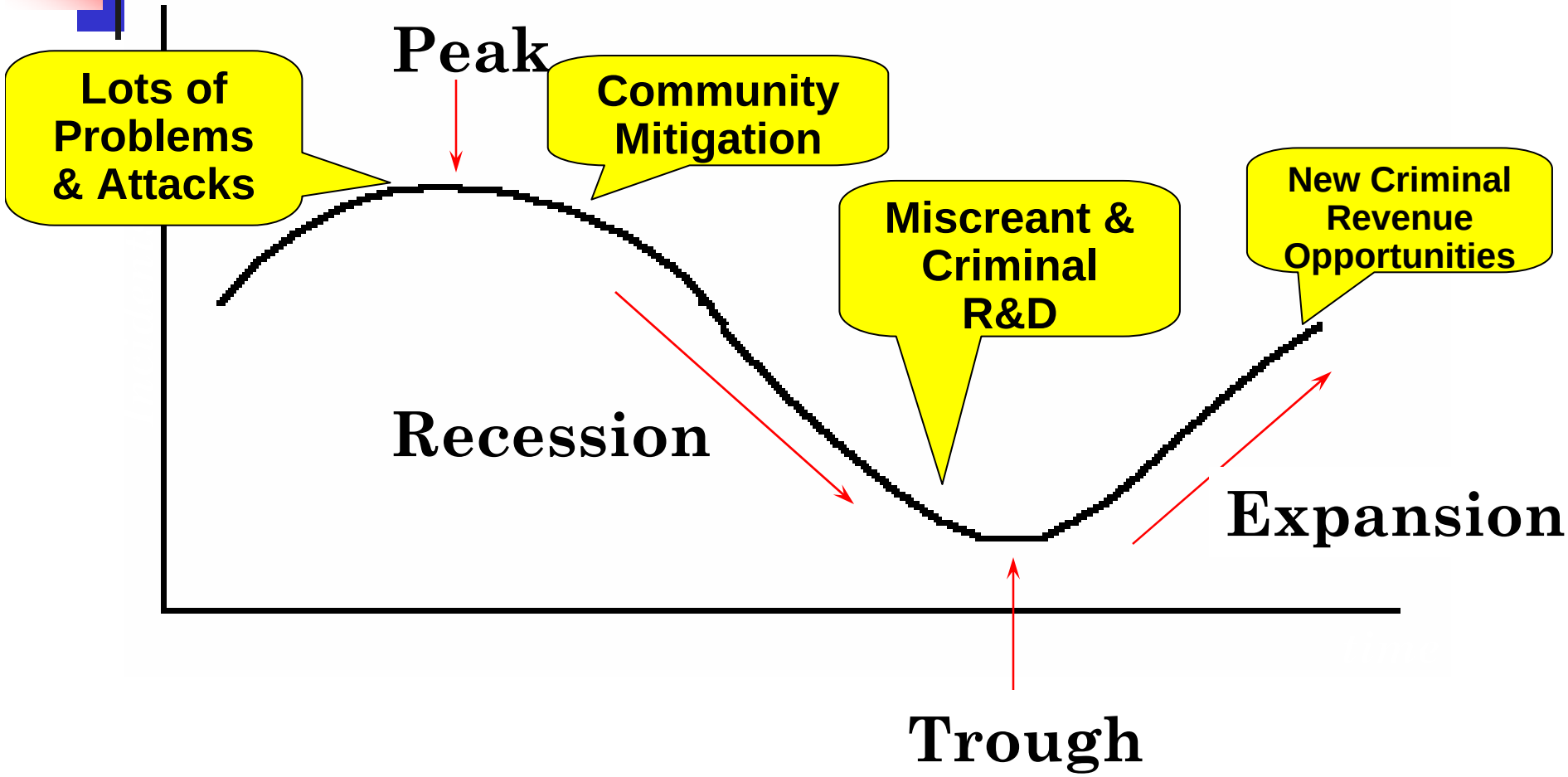
Where to go to get more?

- **NANOG Security Curriculum**
  - Sessions recorded over time which builds a library for all SPs to use for their individual training, staff empowerment, and industry improvements.
- http://www.nanog.org/ispsecurity.html

Where is This Coming From?



Economic Cycles



Parts of the Miscreant Business Cycle

Top Ten List of things that Work

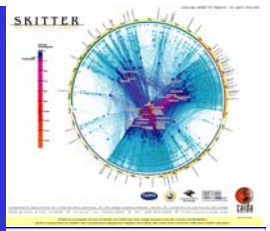
1. Prepare your NOC
2. Mitigation Communities
3. iNOC-DBA Hotline
4. Point Protection on Every Device
5. Edge Protection
6. Remote triggered black hole filtering
7. Sink holes
8. Source address validation on all customer traffic
9. Control Plane Protection
10. Total Visibility (Data Harvesting – Data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

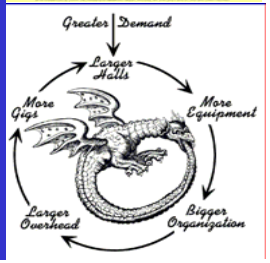
“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu

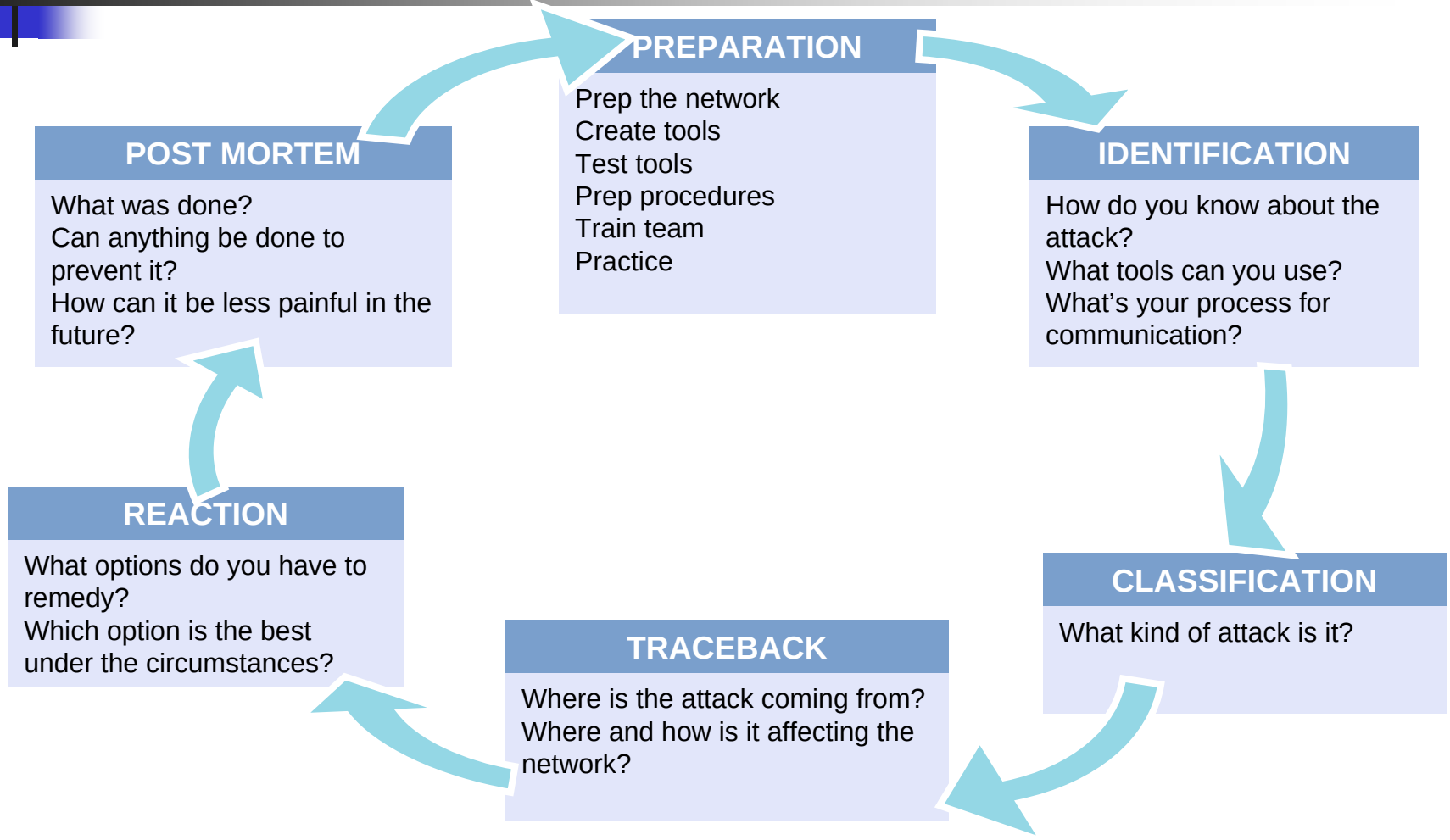
Art of War

The Executive Summary

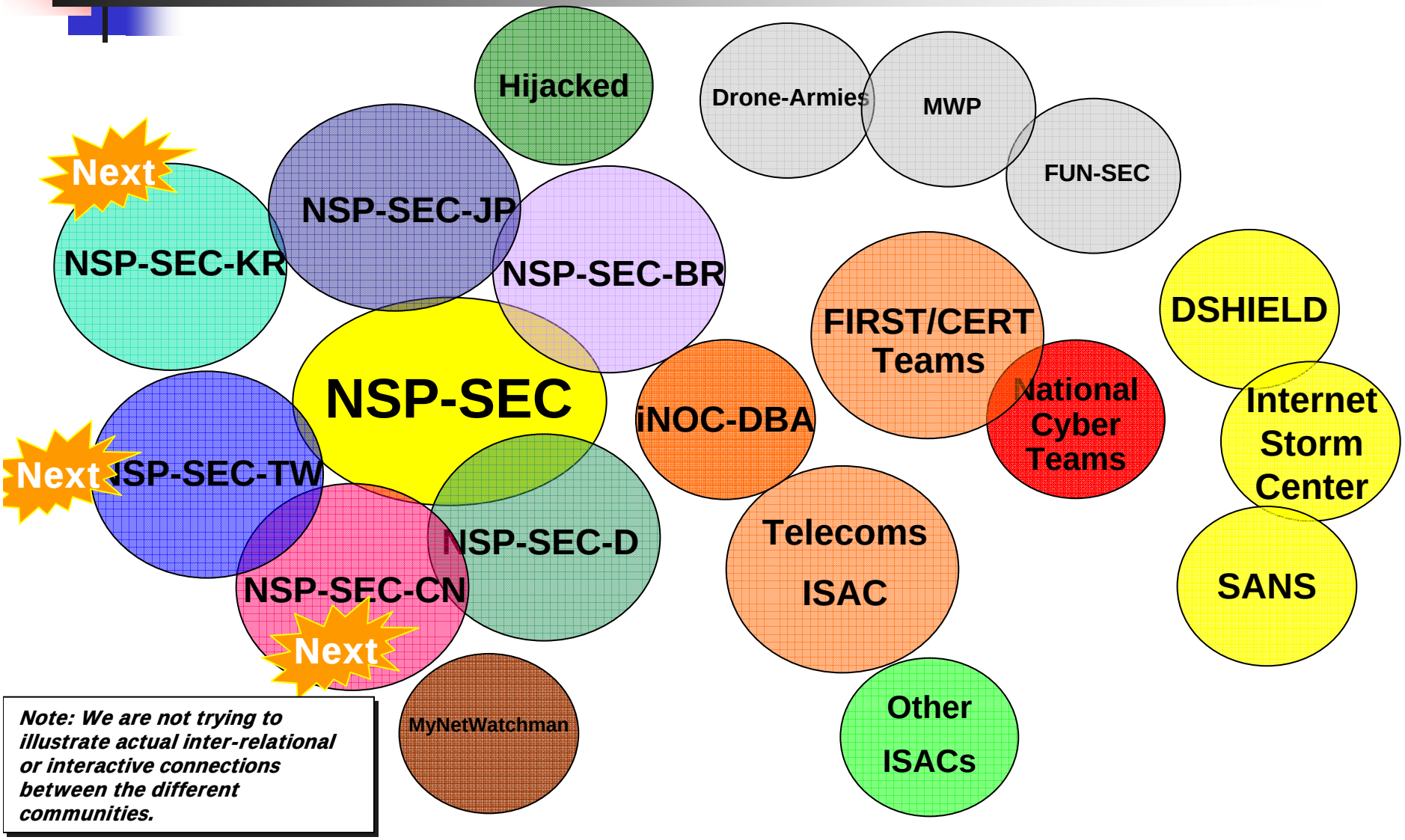




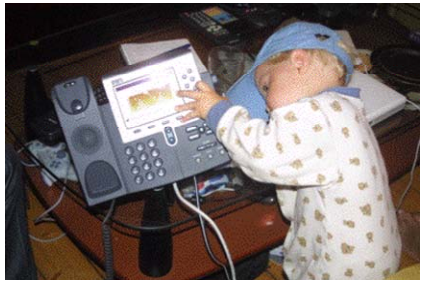
SP Security in the NOC - Prepare



Aggressive Collaboration

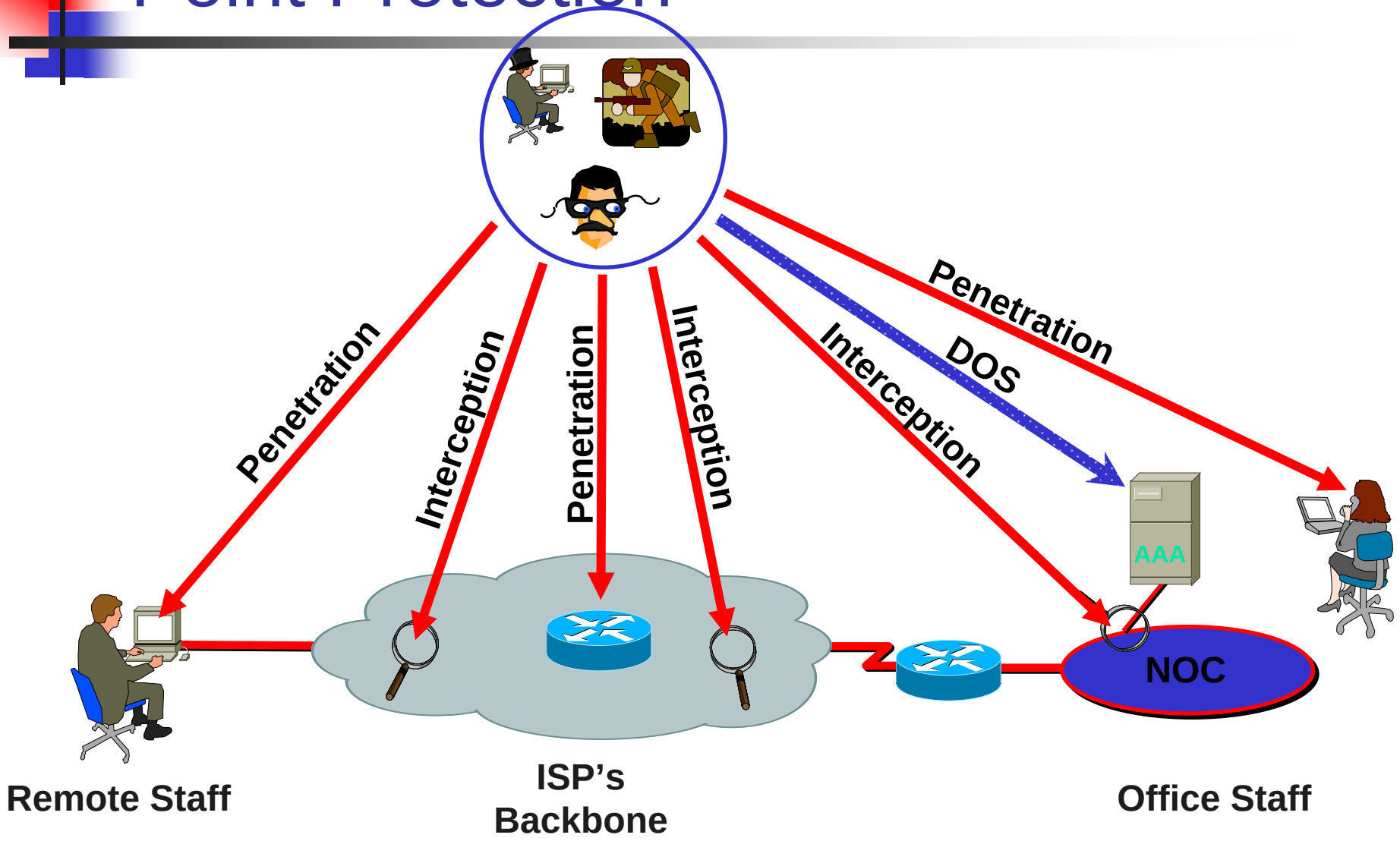


iNOC DBA Hotline

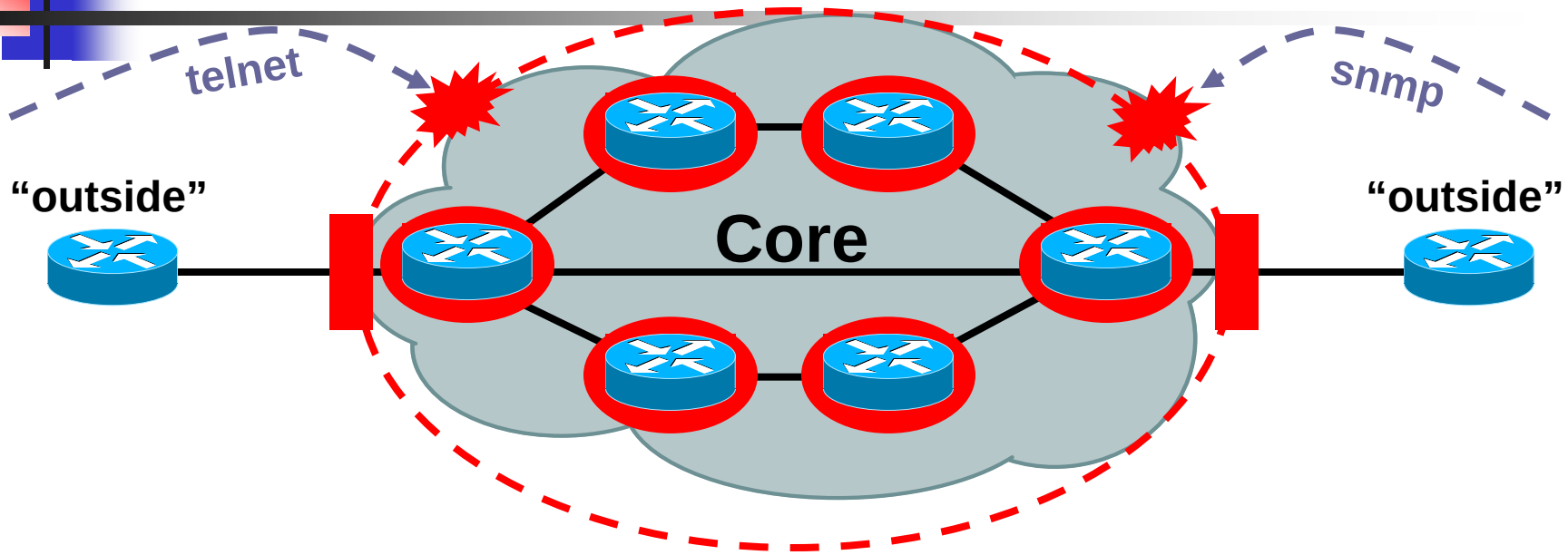


- INOC-DBA: *Inter-NOC Dial-By-ASN*
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
  - ASnumber:phone
  - 109:100 is Barry's house.
- SIP Based VoIP system, managed by www.pch.net

Point Protection

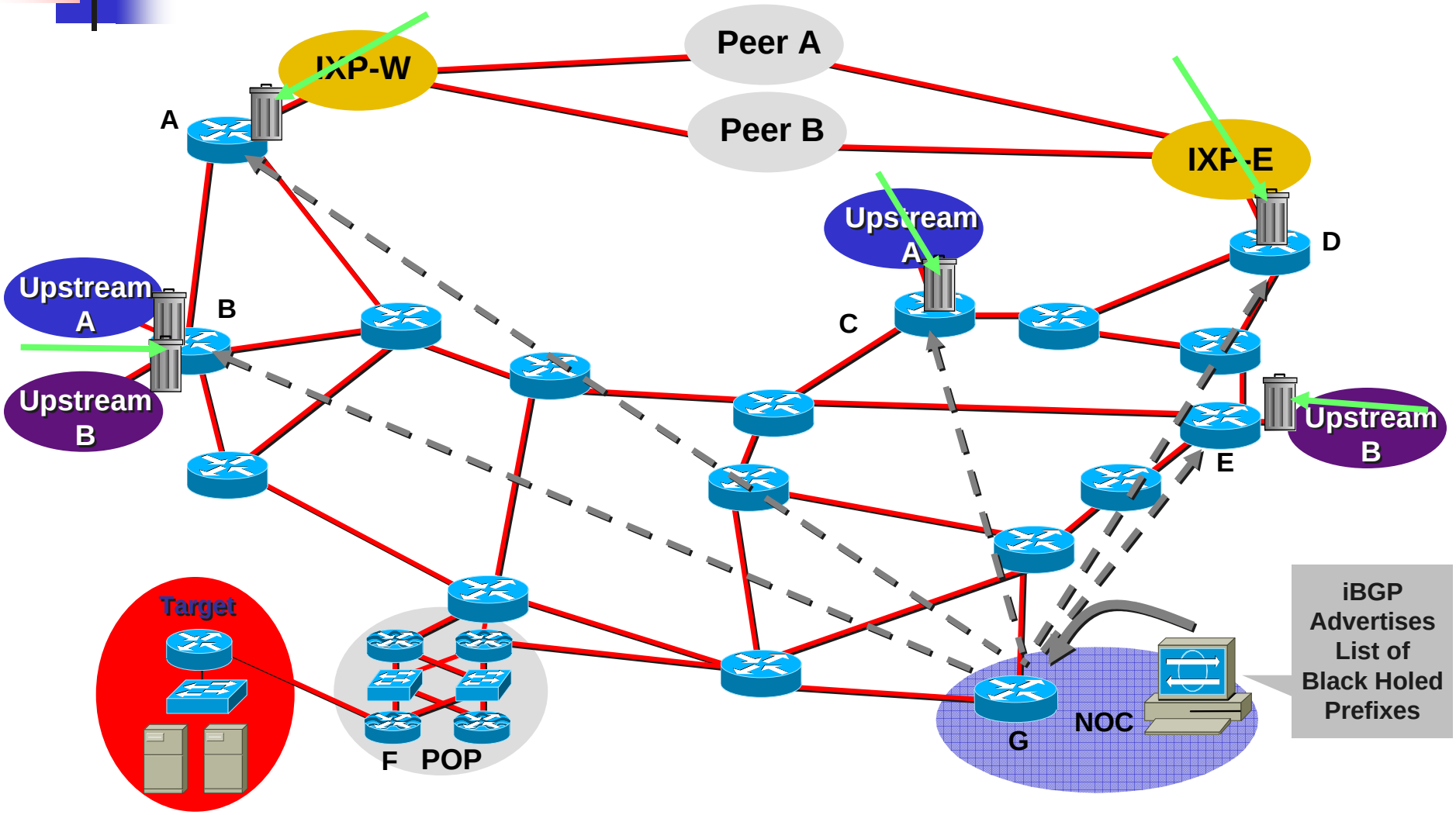


Edge Protection

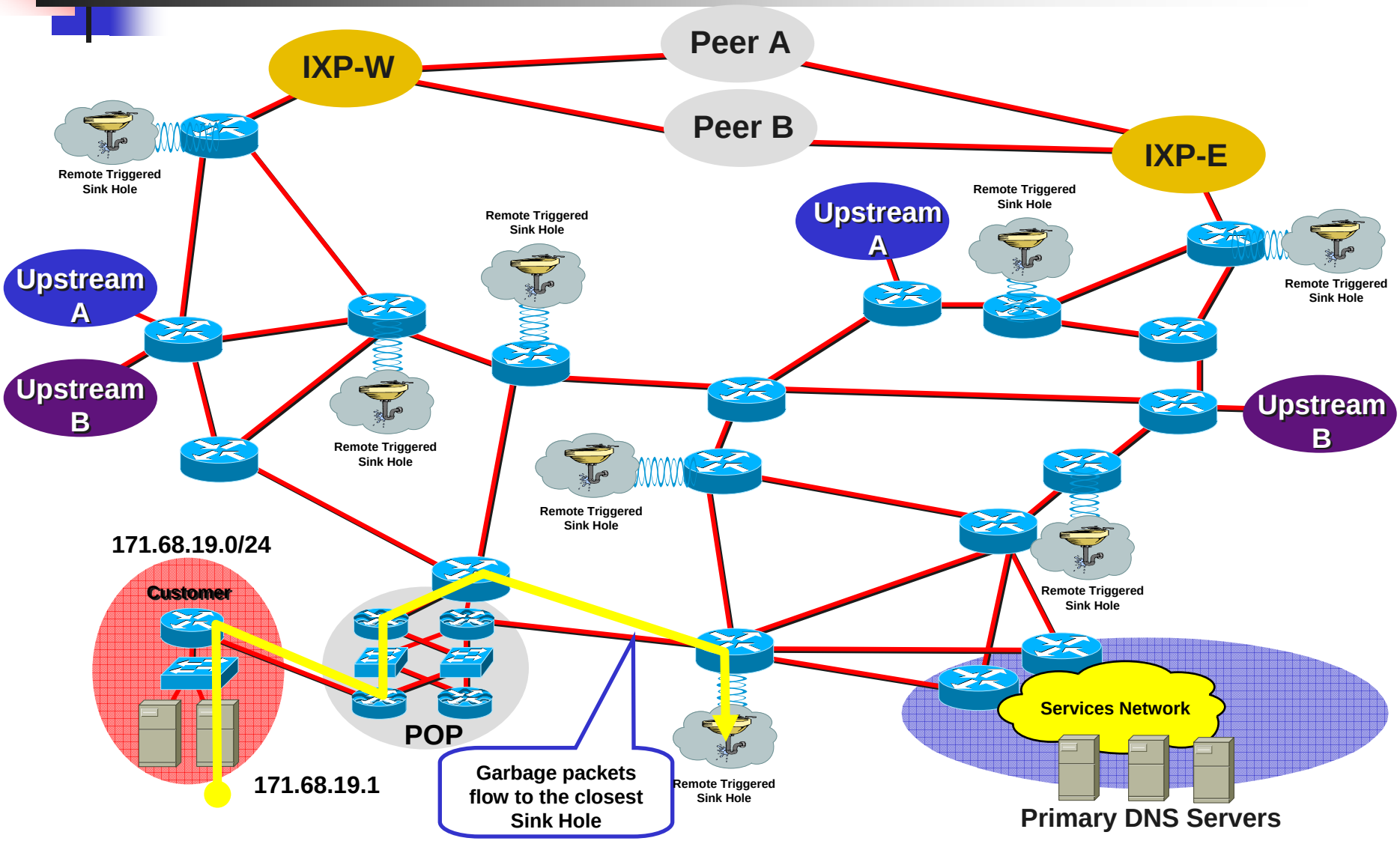


- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Destination Based RTBH

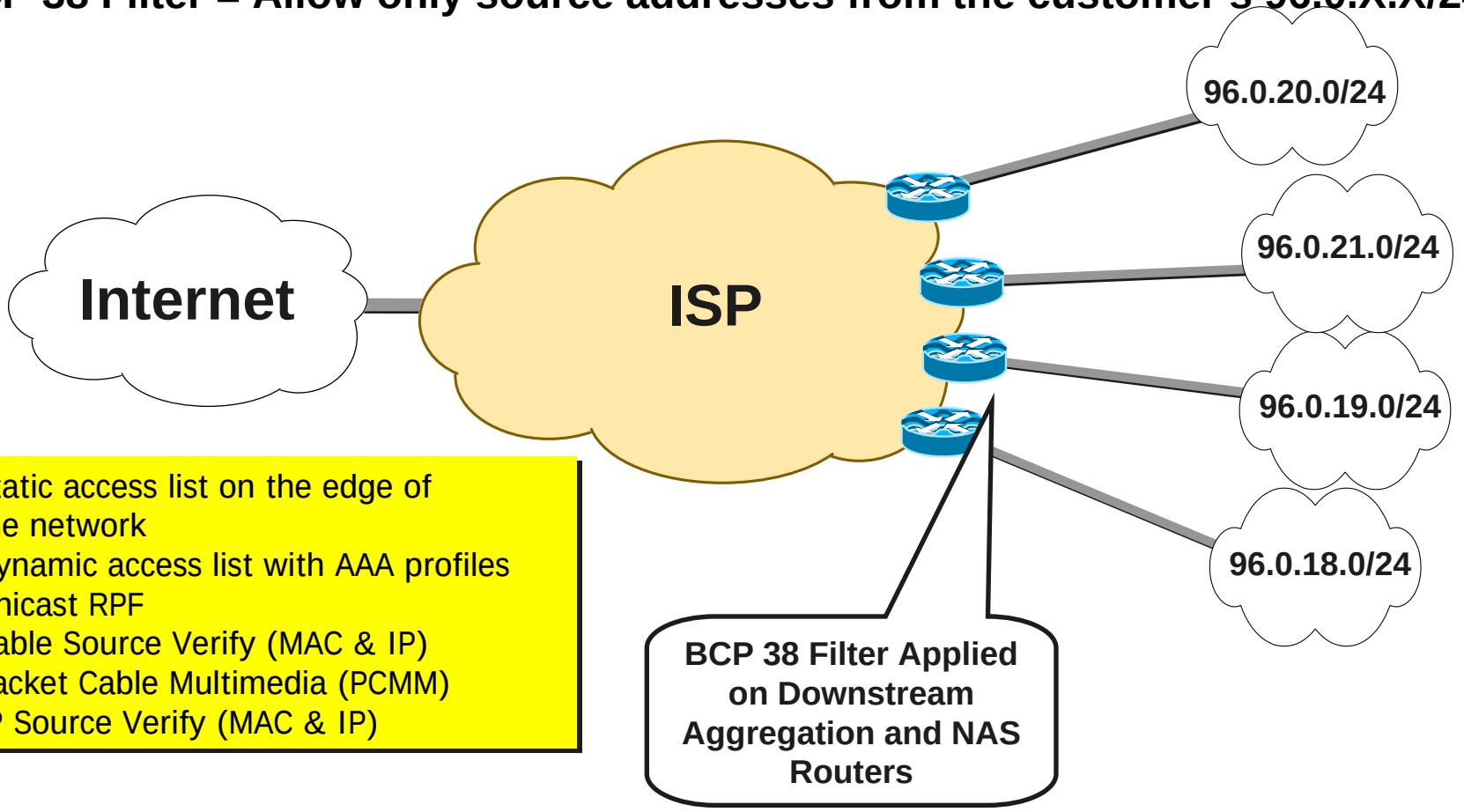


Sink Holes


IXP-W
Peer A
Peer B
IXP-E
Remote Triggered Sink Hole
Upstream A
Upstream B
Upstream A
Upstream B
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
Remote Triggered Sink Hole
171.68.19.0/24
Customer
171.68.19.1
POP
Garbage packets flow to the closest Sink Hole
Services Network
Primary DNS Servers

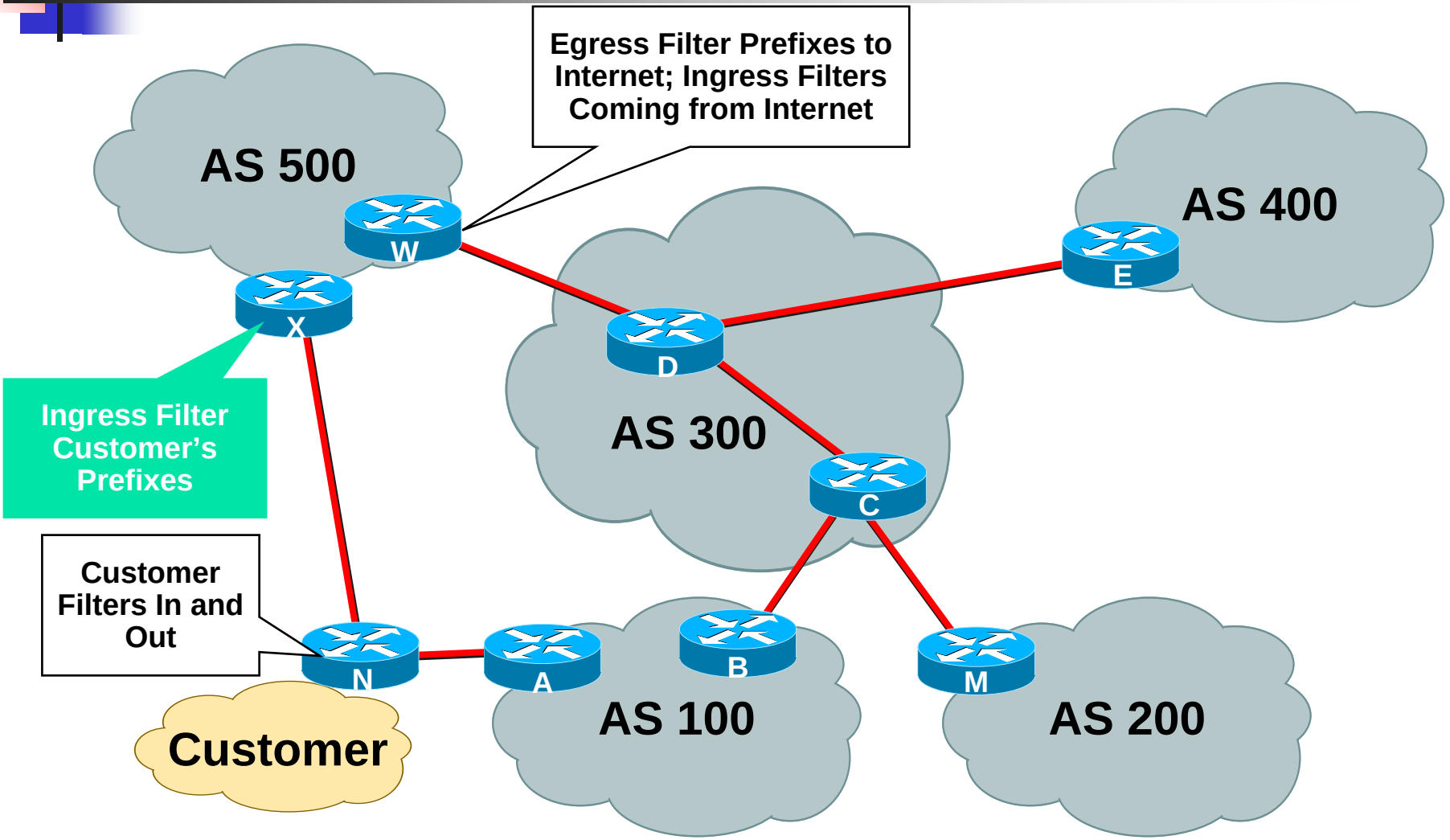
BCP 38 Ingress Packet Filtering

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



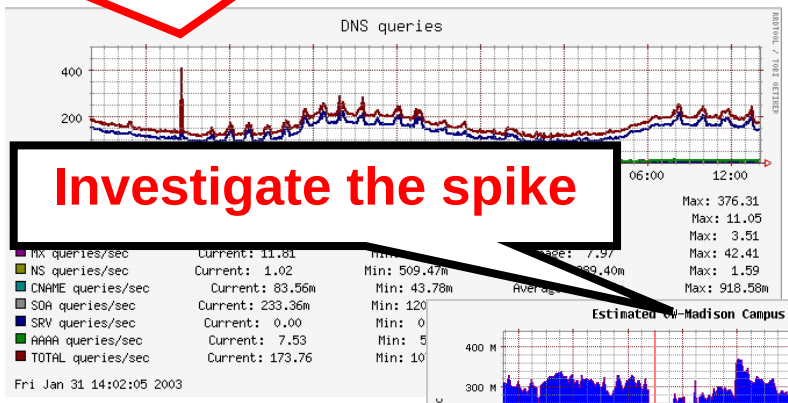
- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)

Where to Prefix Filter?

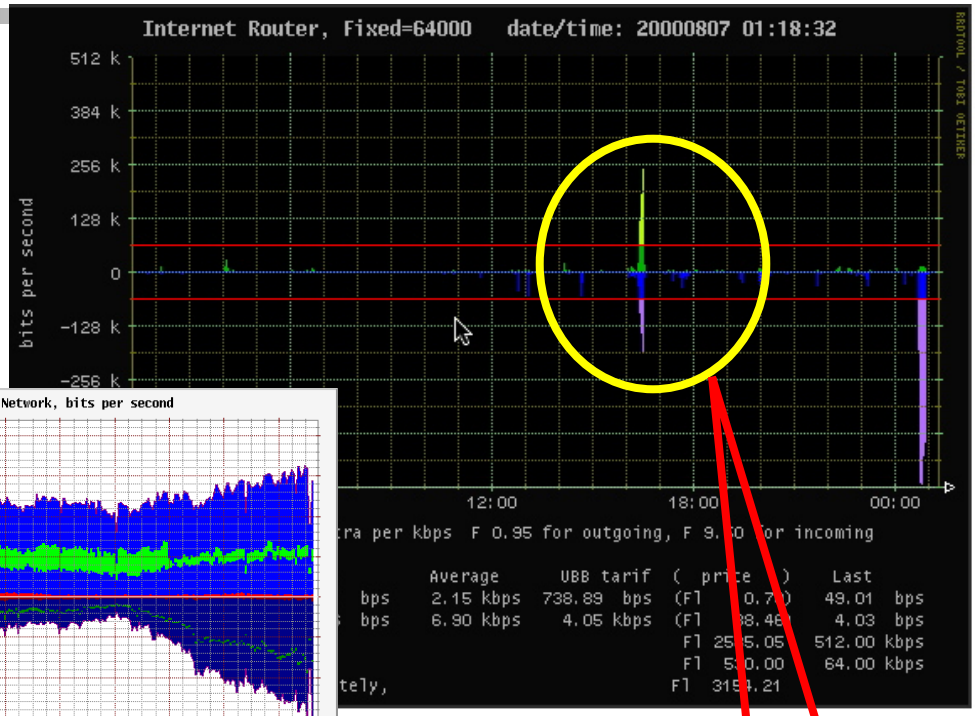


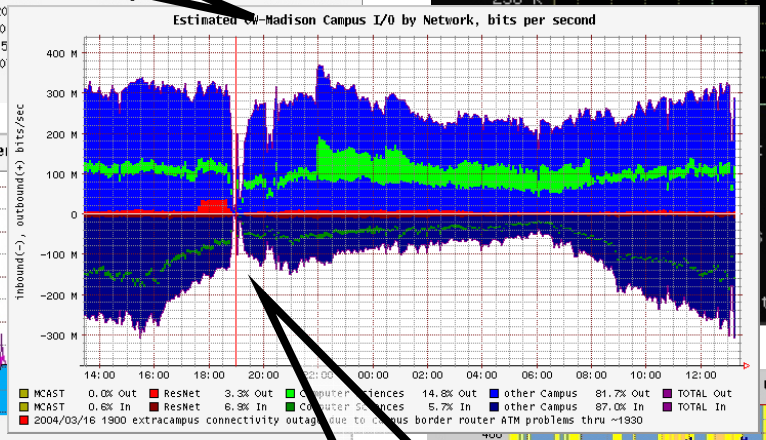
Total Visibility

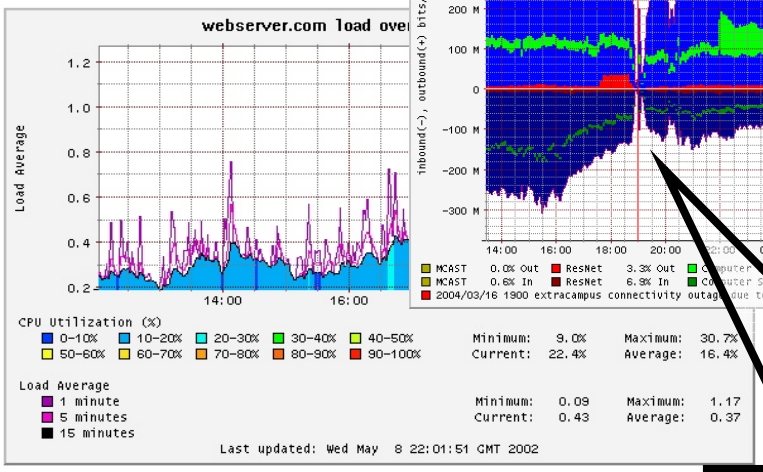
Anomaly for DNS Queries

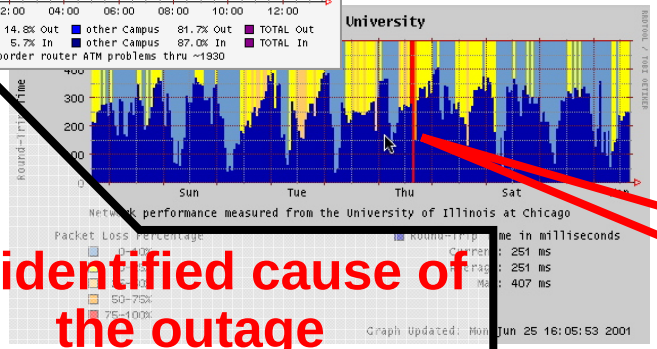


Investigate the spike









An identified cause of the outage

Thru'put Spike

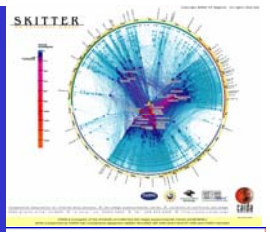
RTT Spike

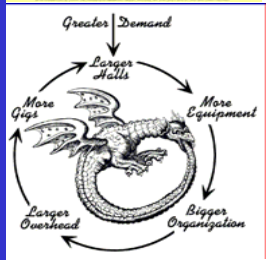
Source: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

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

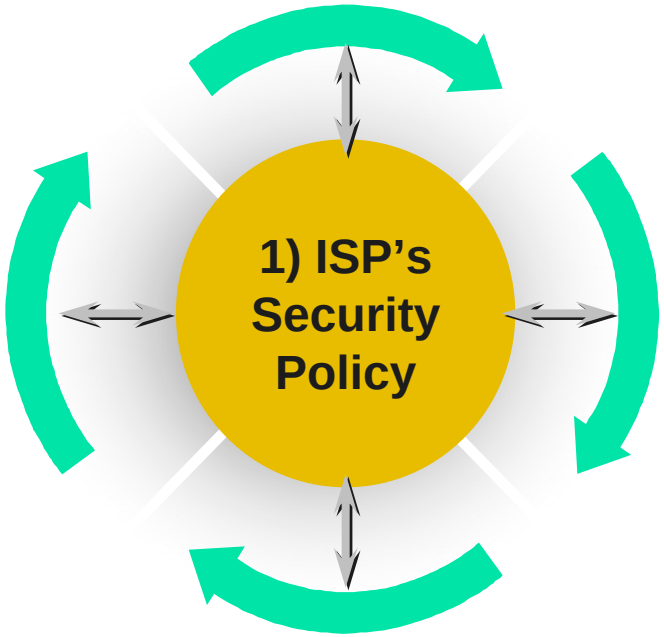
SP's/ISP's NOC Team

- An SP's/ISP's OPerational SECurity 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 incidence are a normal part of an ISP's operations!

2) Secure Resources
Firewall, Encryption, Authentication, Audit



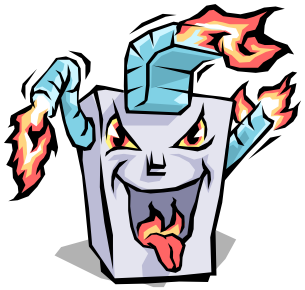
5) Manage and Improve
Post Mortem, Analyze the Incident, modify the plan/procedures

3) Monitor and Respond
Intrusion Detection, work the incidence,

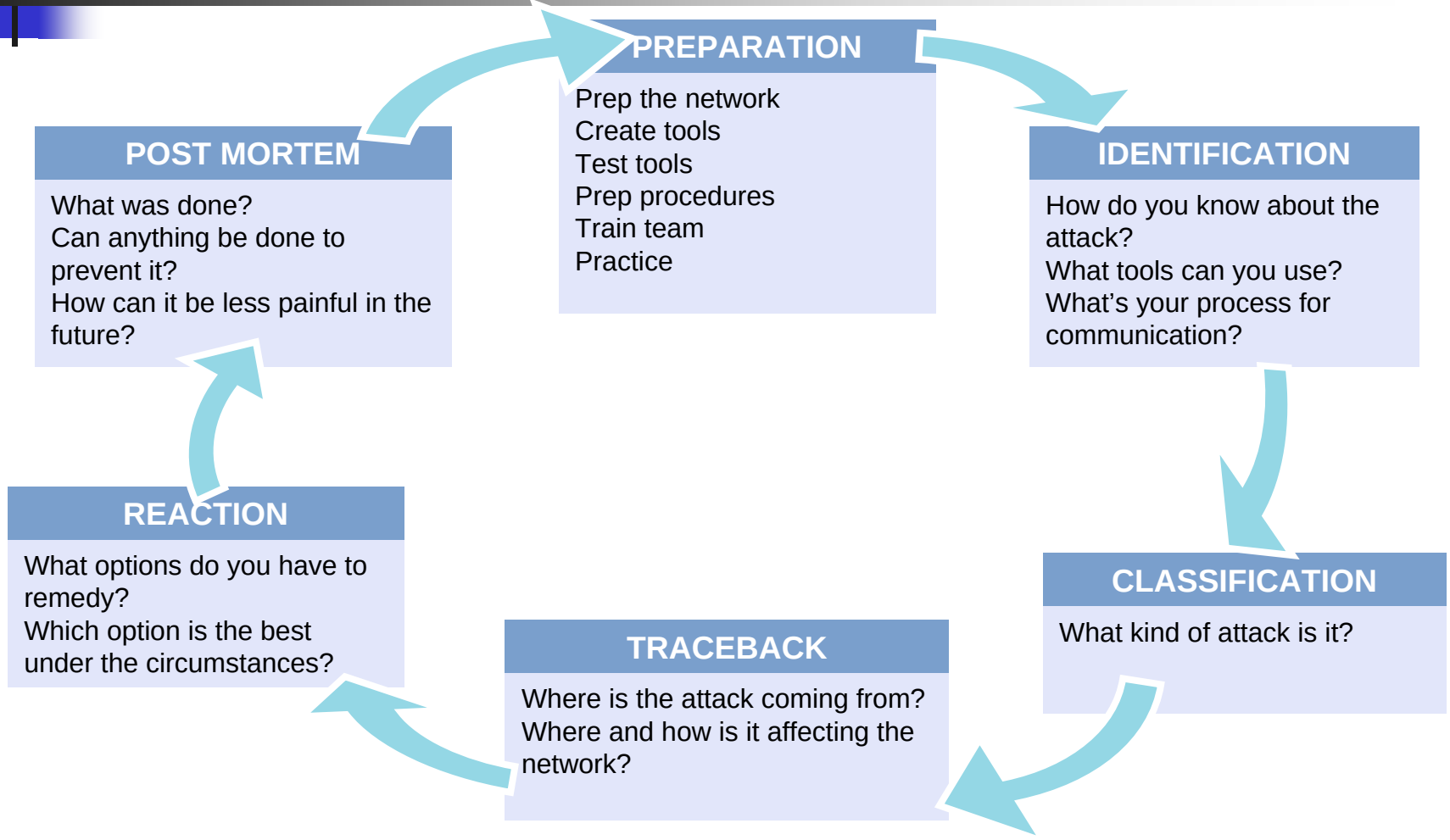
4) Test, Practice, Drill
Vulnerability Scanning

The Preparation Problem

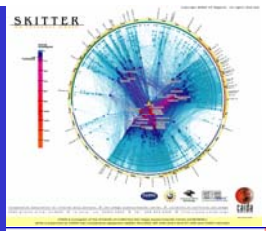
- The problem—Most ISP NOCs:
  - Do not have security plans
  - Do not have security procedures
  - Do not train in the tools or procedures
  - OJT (on the job training)—learn as it happens

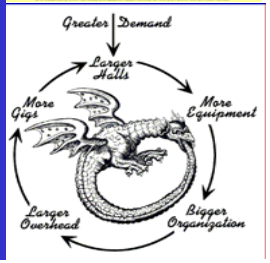


Six Phases of Incident Response



Mitigation Communities

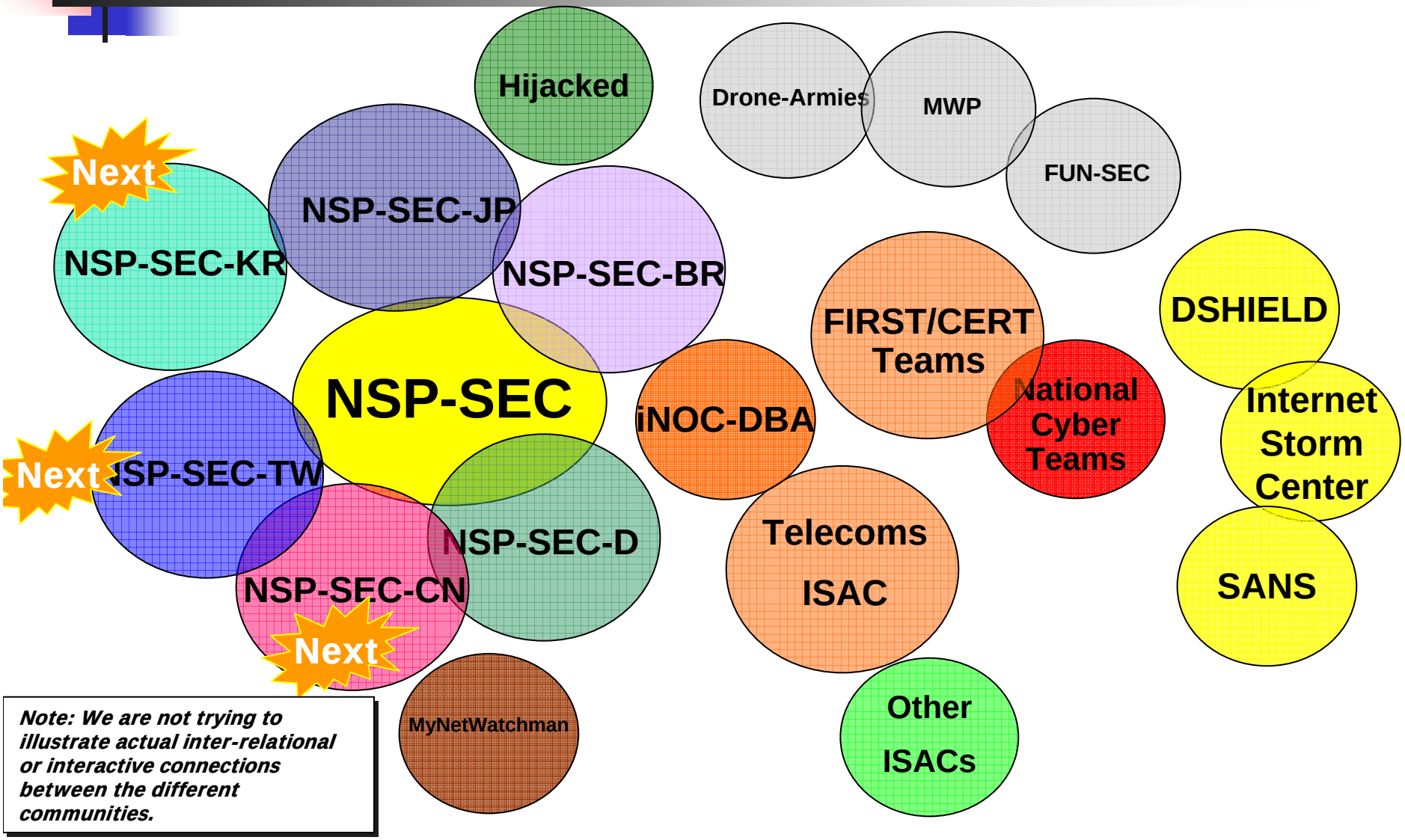




Check List

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)

SP Related Miscreant Mitigation Communities

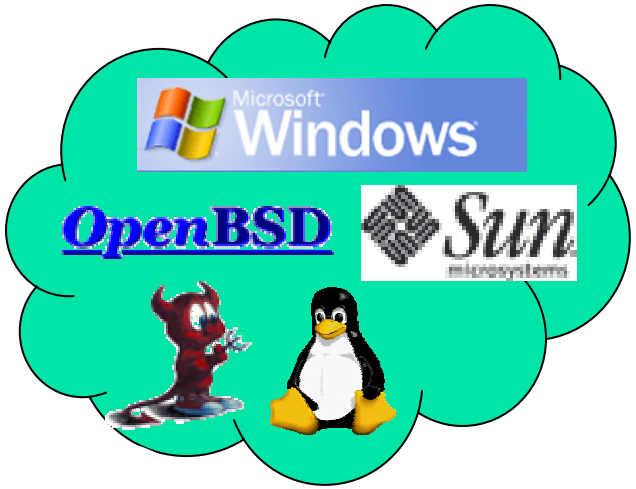


DSHIELD

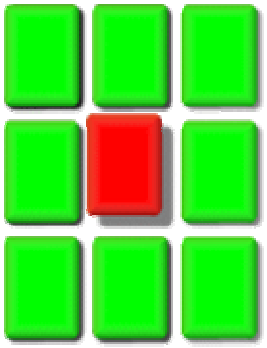
Data Collection

Analysis

Dissemination

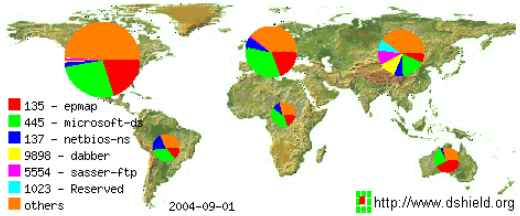


DShield Users



DShield.org

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	9098		[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

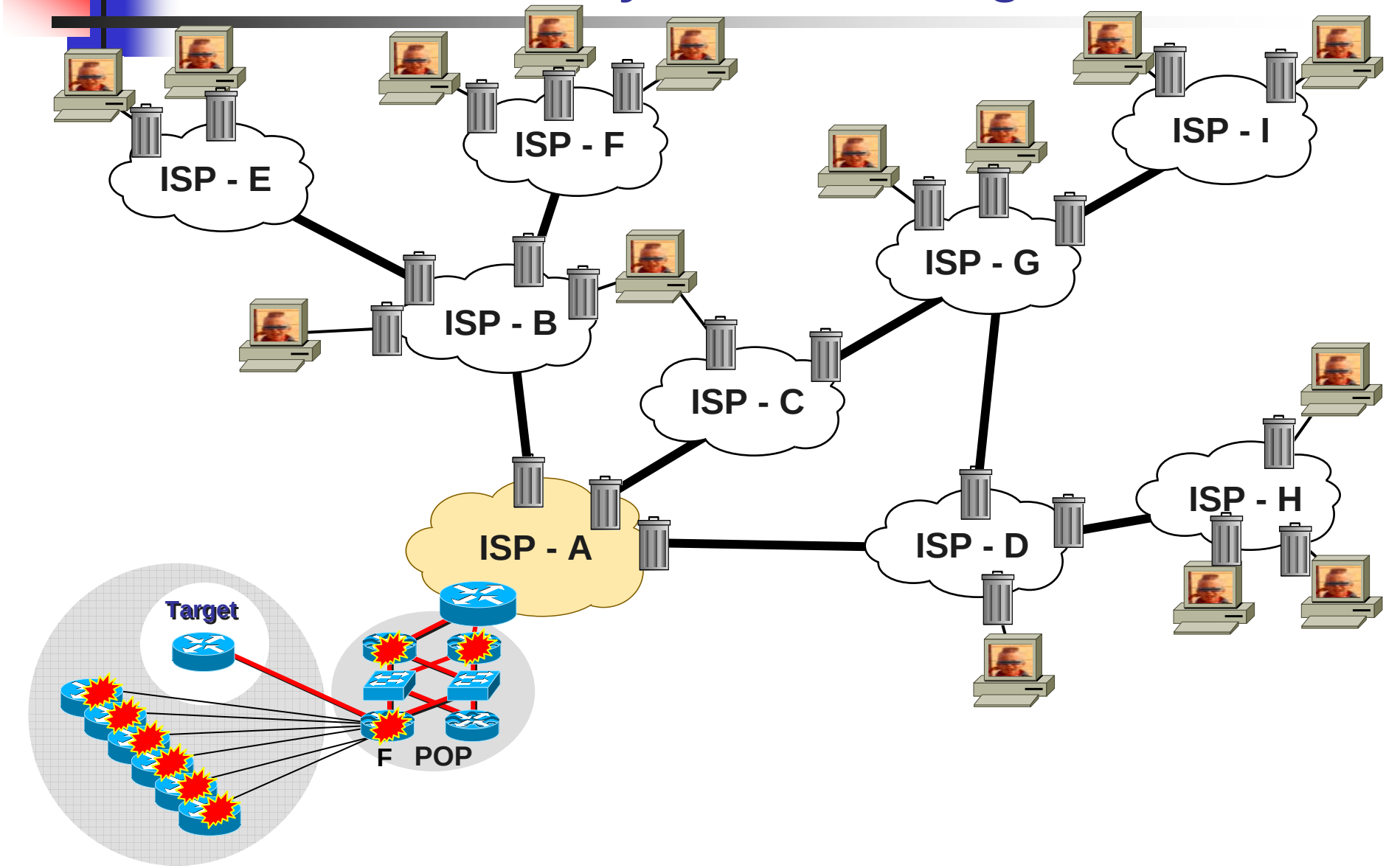
NSP-SEC: Daily DDOS Mitigation Work

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*

- 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

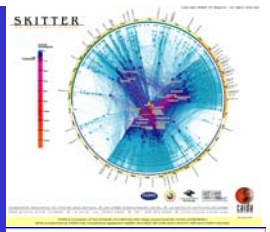
- APRICOT Security BOFs (www.apricot.net)
  Coordinators/Facilitators: Derek Tay - dt@agcx.net
  Dylan Greene - dylan@juniper.net

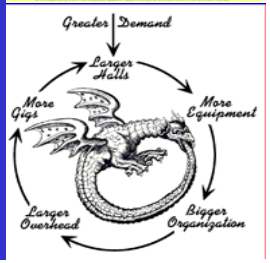
CERT & FIRST

- 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/

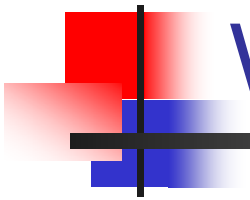
iNOC DBA


SKITTER


Greater Demand
Larger Halls
More Equipment
Bigger Organization
Larger Overhead
More Gigs

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?

- 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

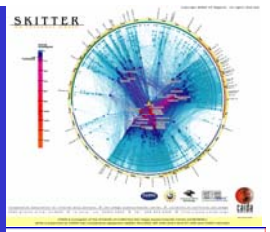
- INOC-DBA: *Inter-NOC Dial-By-ASN*
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
  - ASnumber:phone
  - 109:100 is Barry's house.
- SIP Based VoIP system, managed by www.pch.net

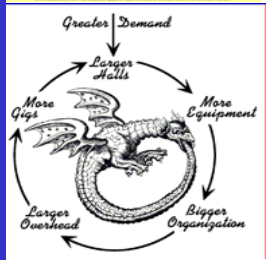
Is set up difficult?

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.

Point Protection

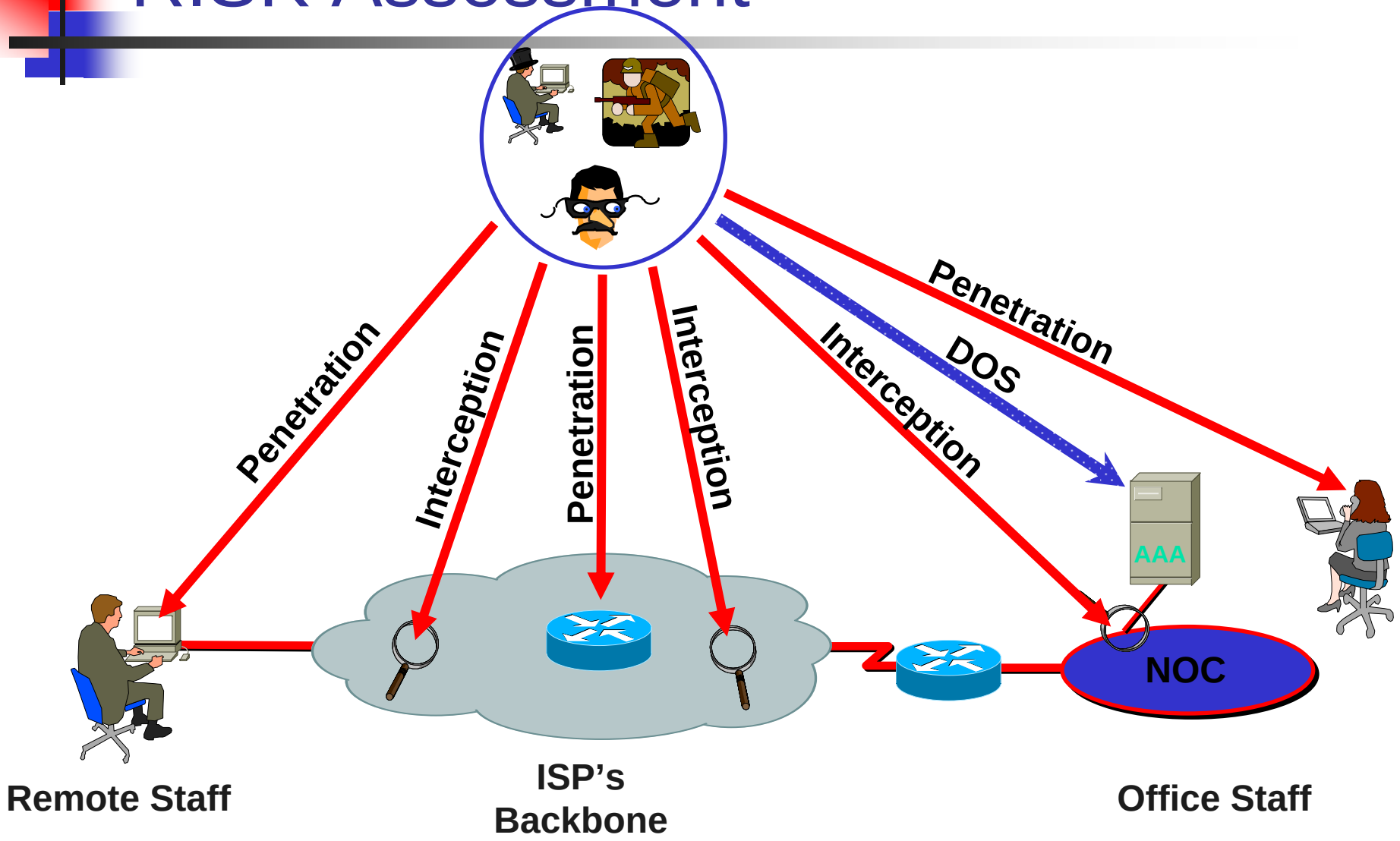




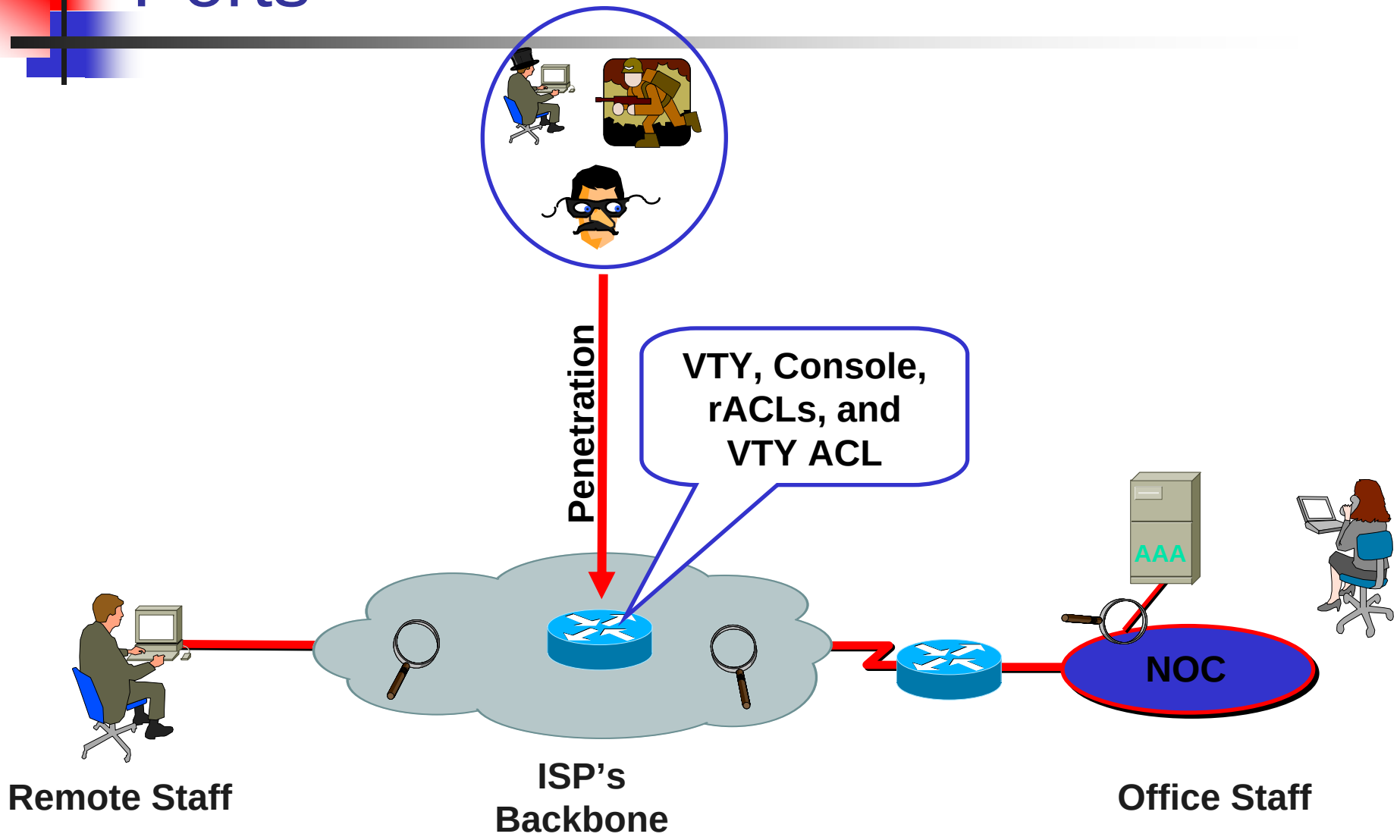
Check List

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

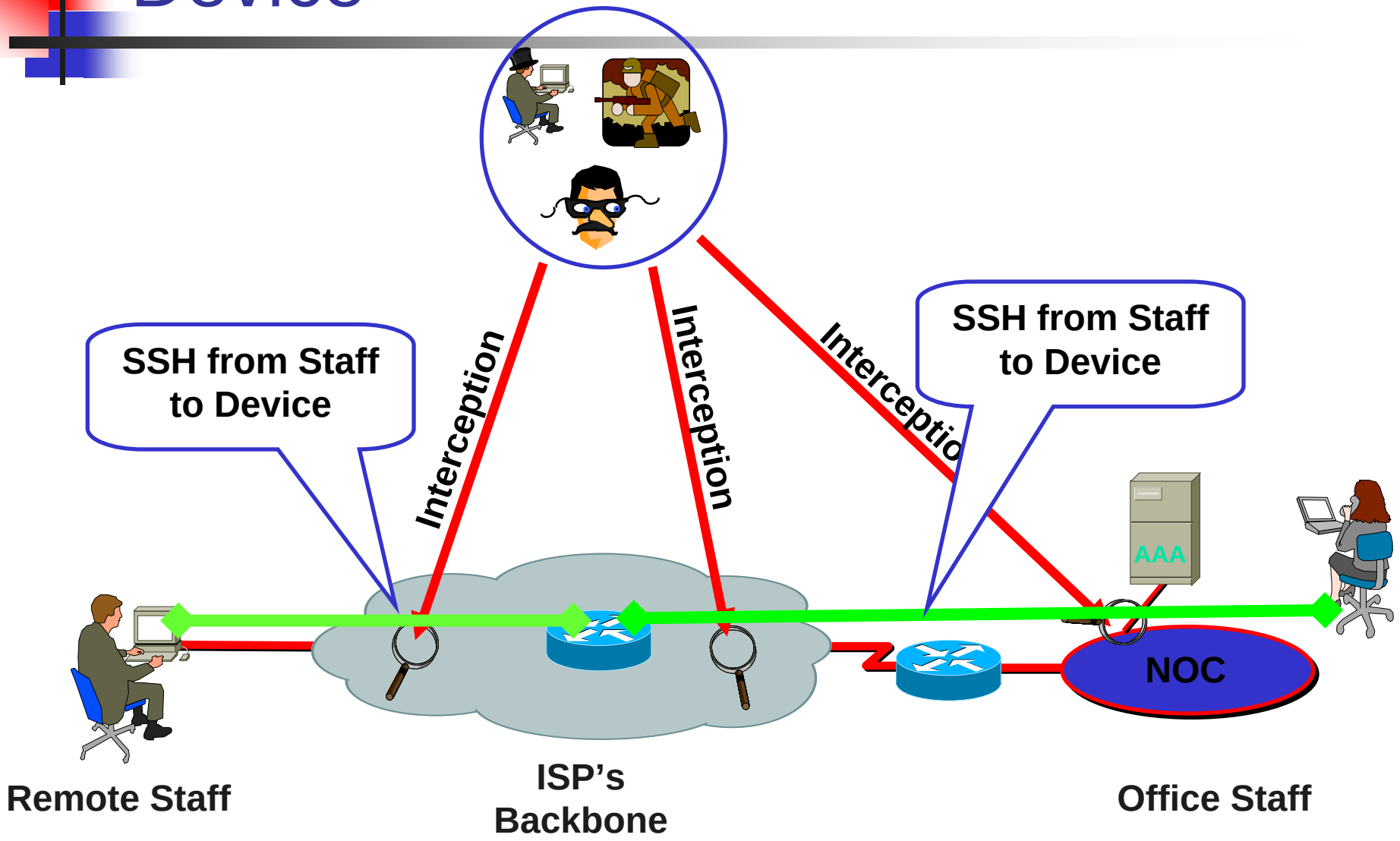
RISK Assessment



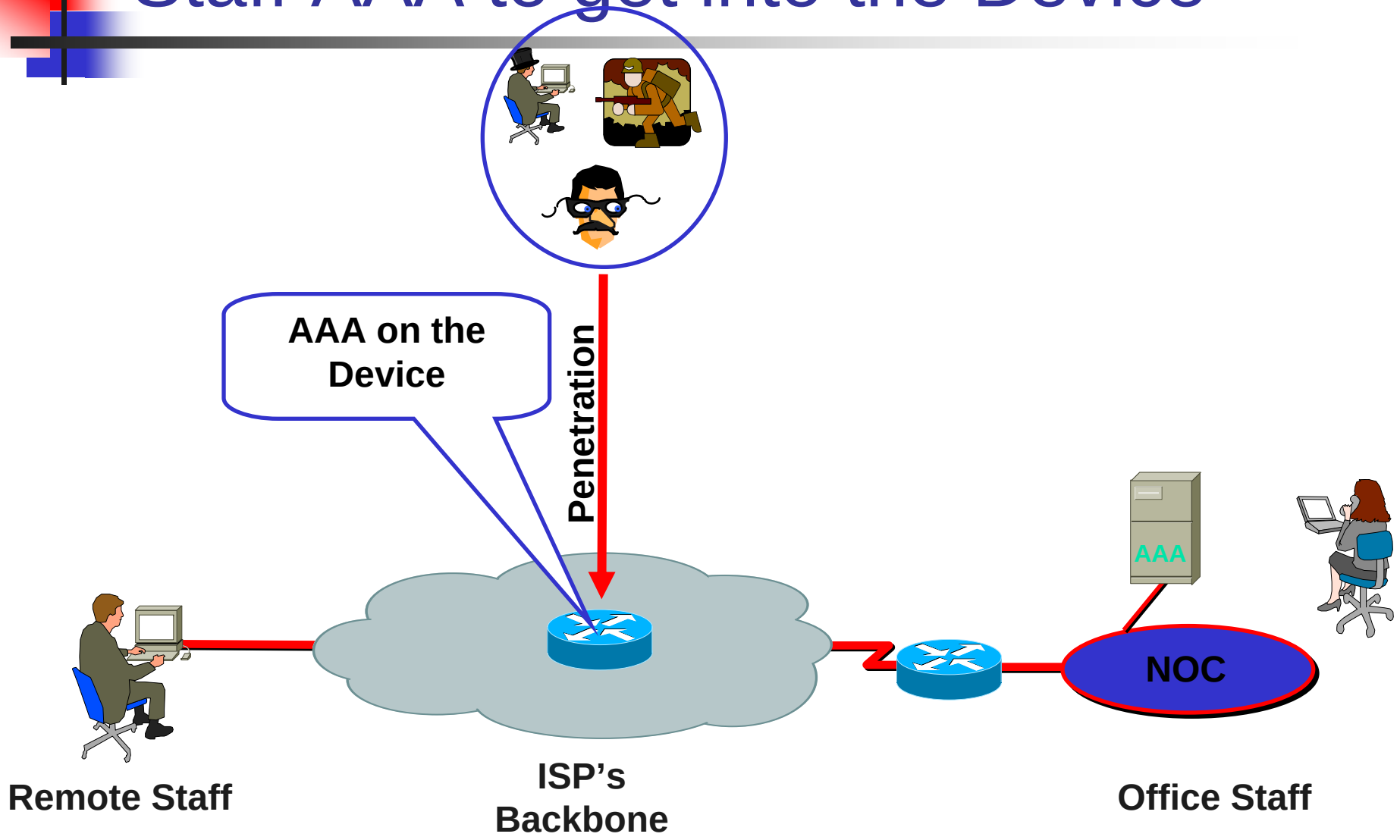
Lock Down the VTY and Console Ports



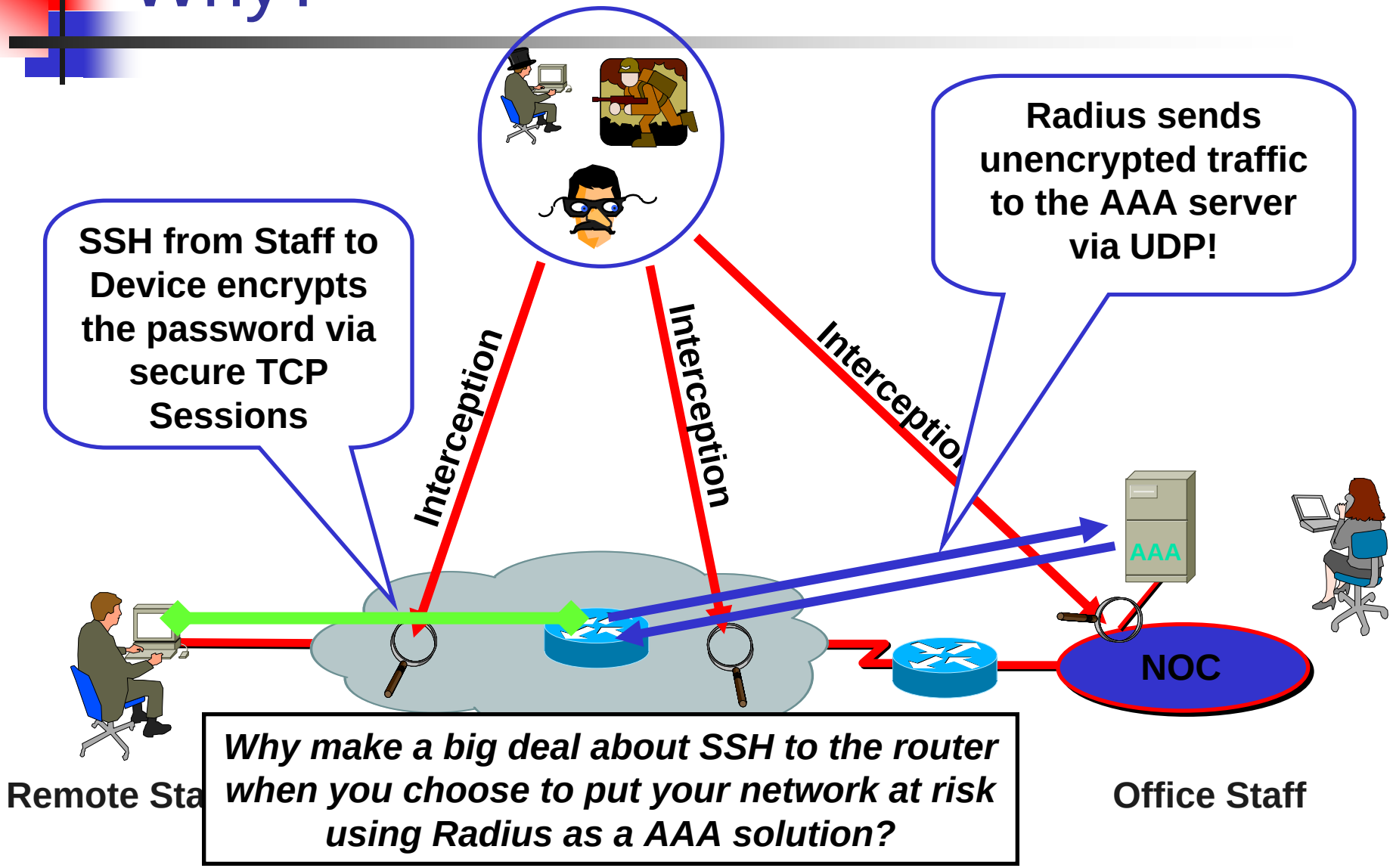
Encrypt the Traffic from Staff to Device



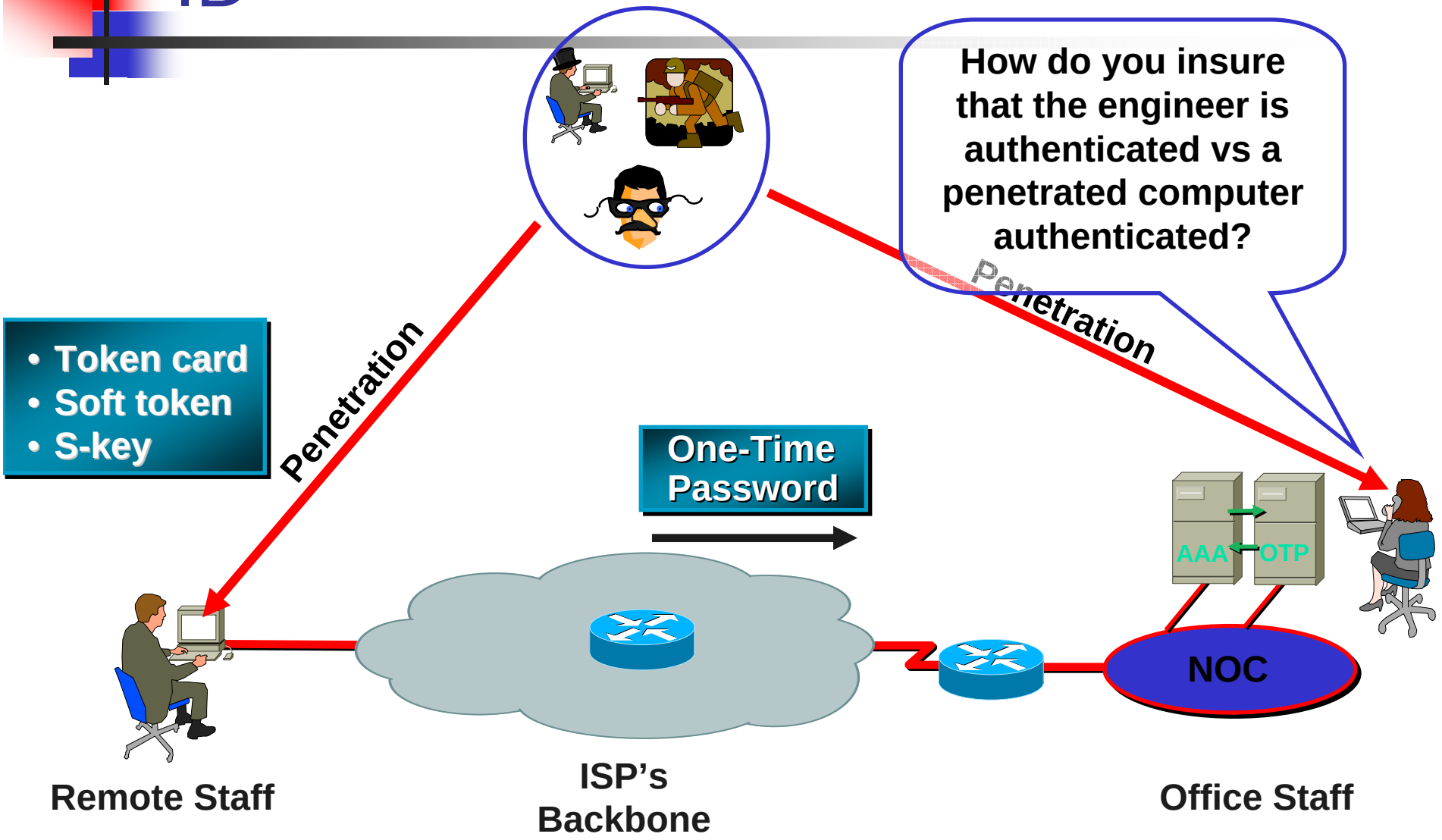
Staff AAA to get into the Device



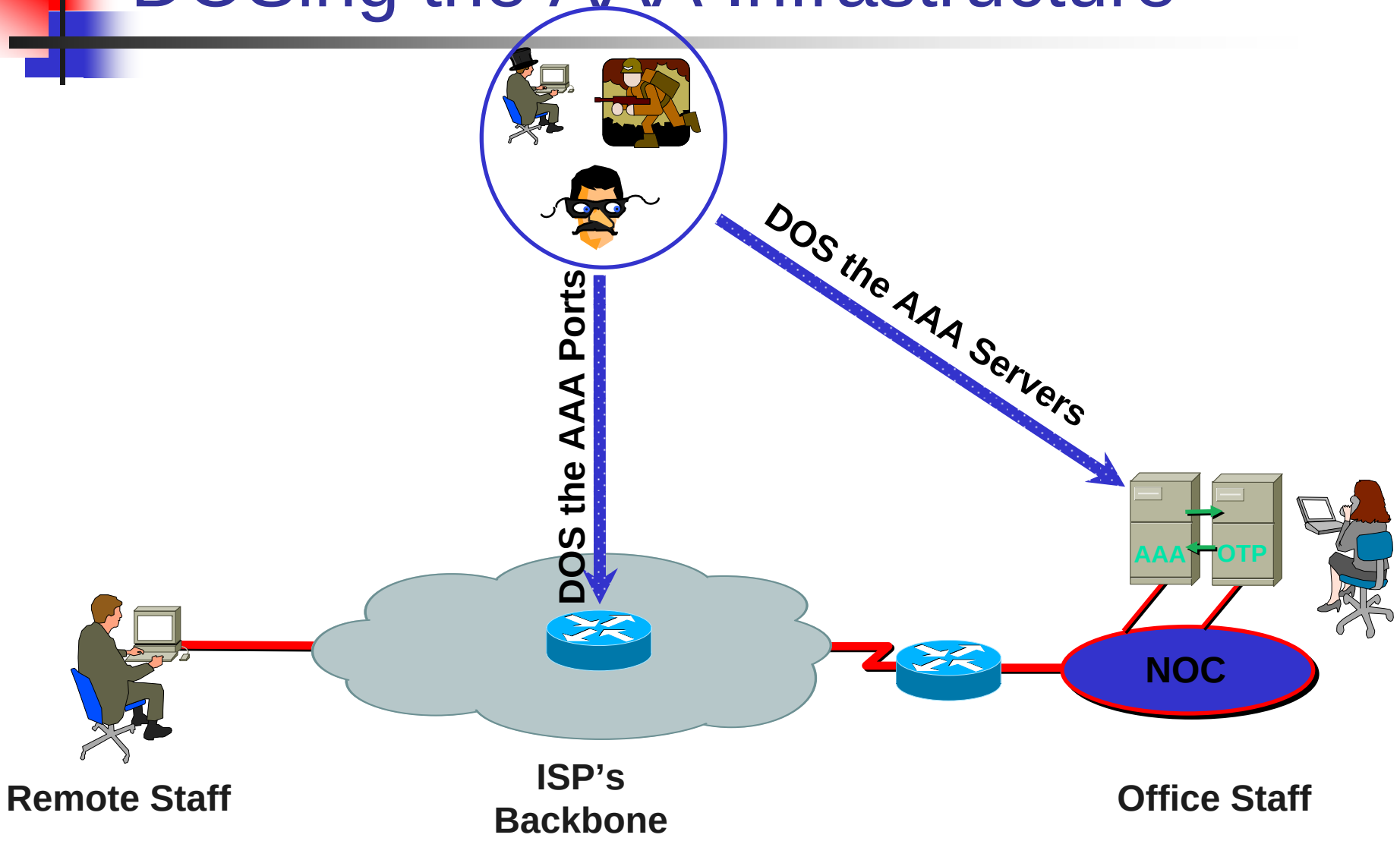
Radius is not an ISP AAA Option! Why?



One Time Password – Checking the ID

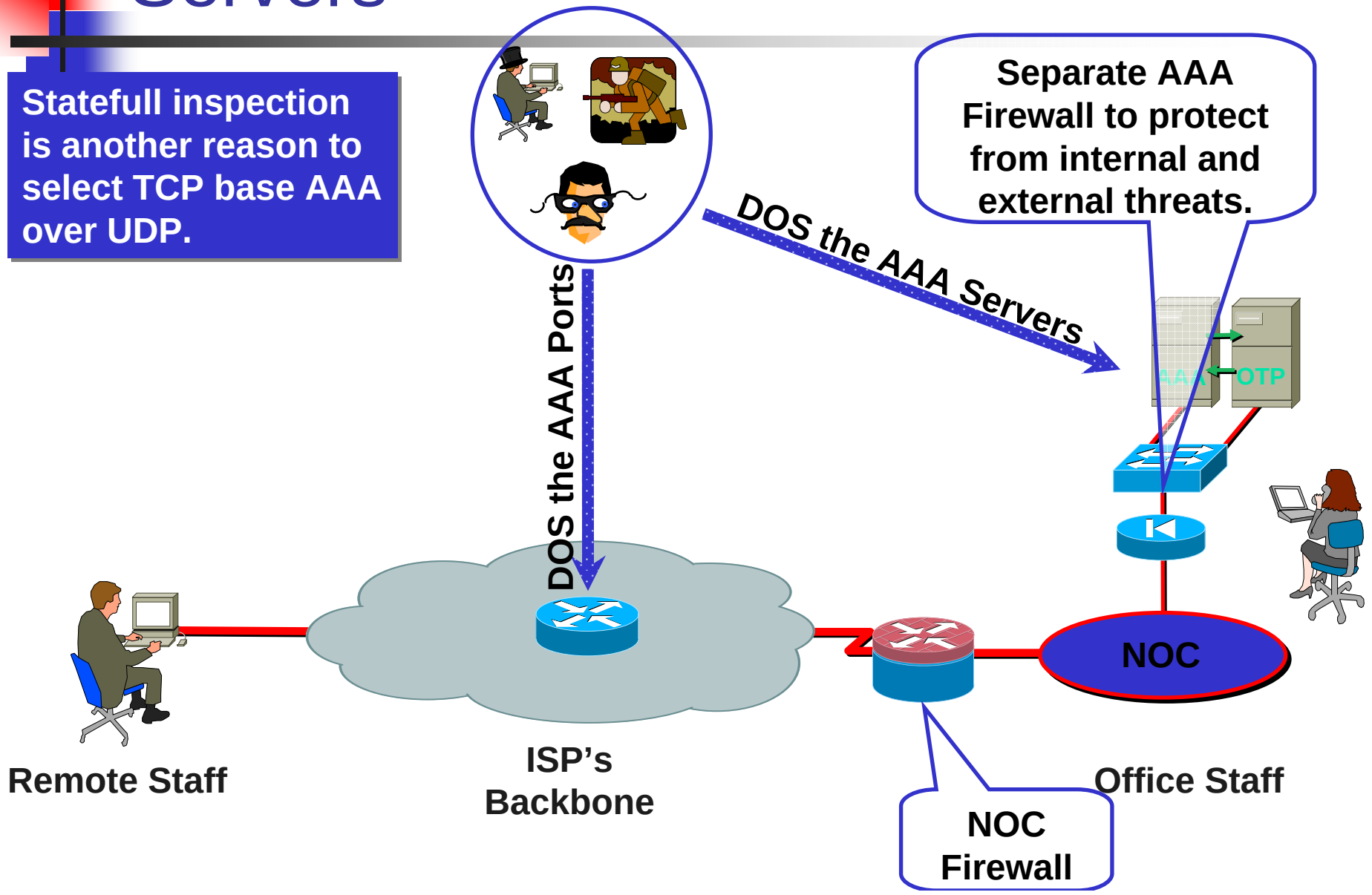


DOSing the AAA Infrastructure

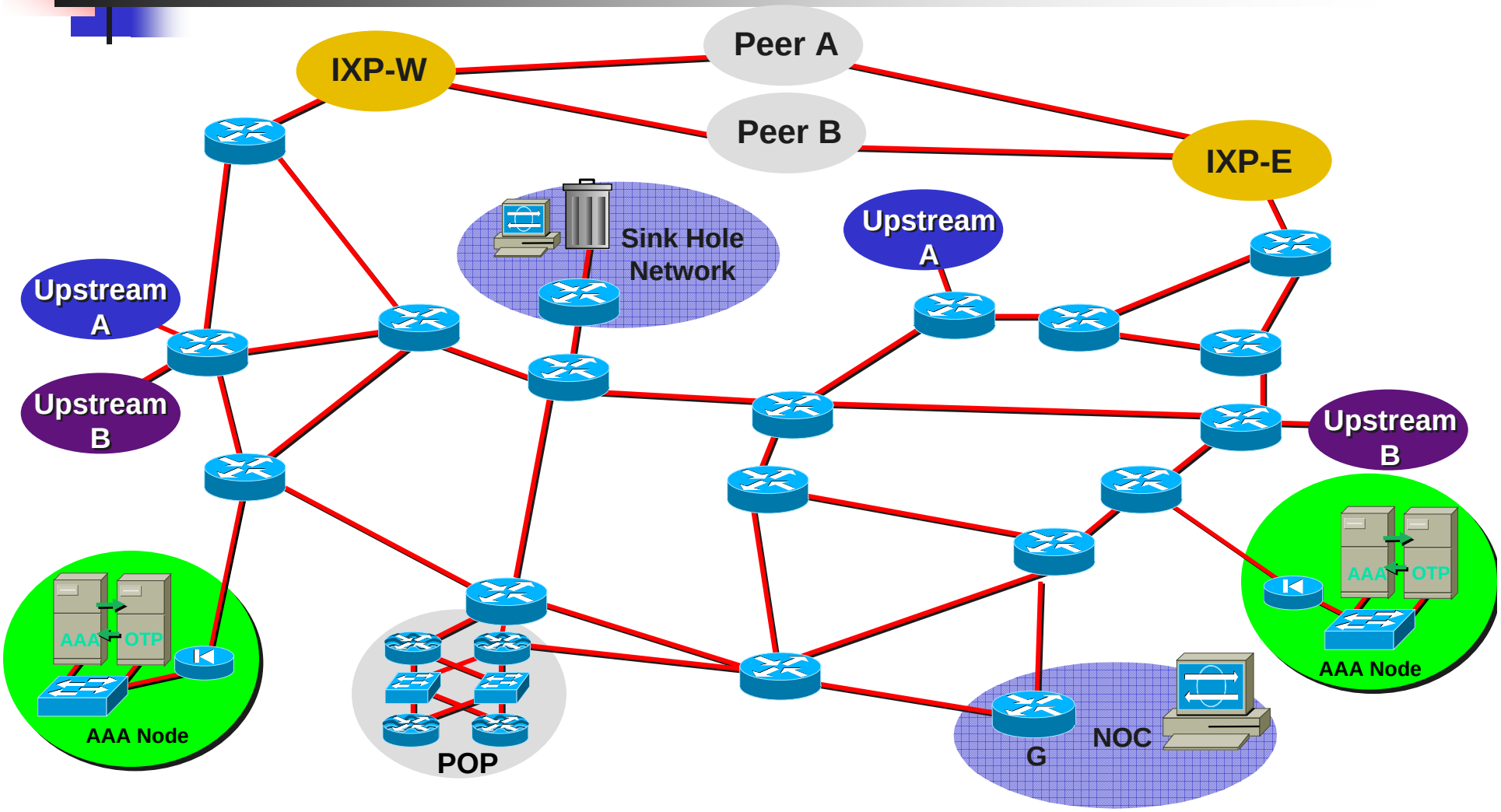


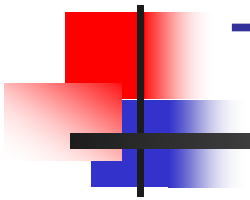
Use a Firewall to Isolate the AAA Servers

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



Distribute AAA Servers and Config Backup

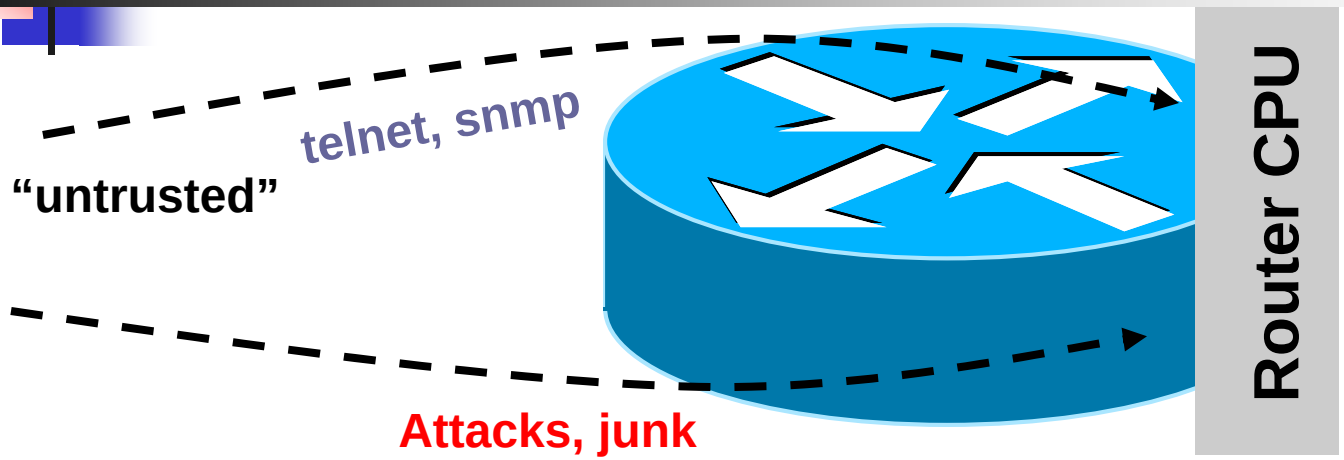




TACACS+ URLs

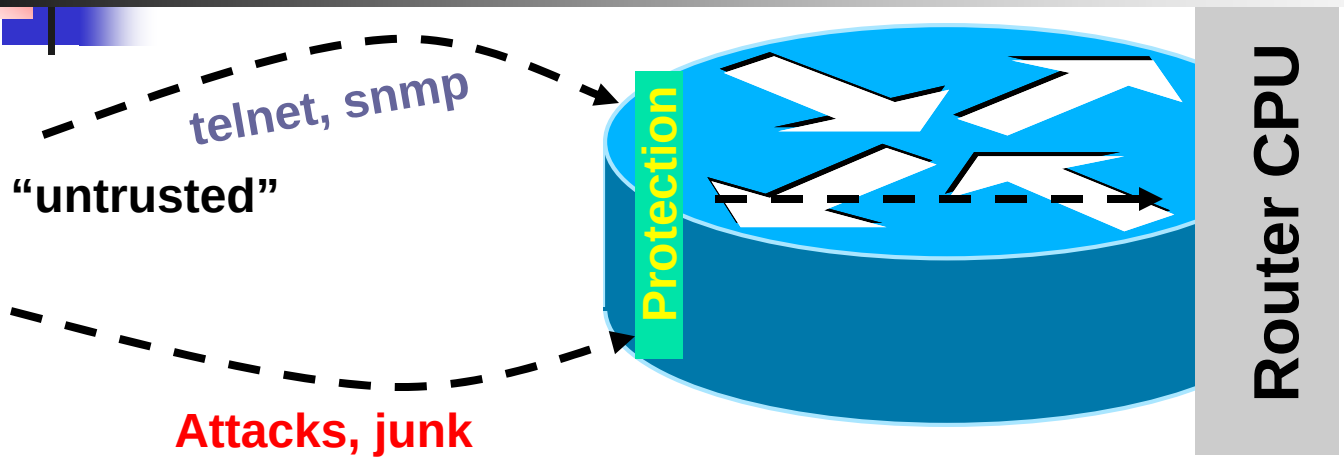
- TACACS+ Open Source
  - ftp://ftp-eng.cisco.com/pub/tacacs/
  - Includes the IETF Draft, Source, and Specs.
- Extended TACACS++ server
  - http://freshmeat.net/projects/tacpp/
- TACACS + mods
  - http://www.shrubbery.net/tac_plus/

The Old World: Router Perspective

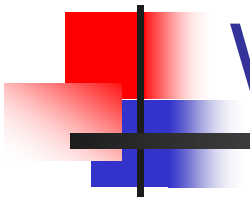


- Policy enforced at process level (VTY ACL, SNMP ACL, etc.)
- Some early features such as ingress ACL used when possible

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.

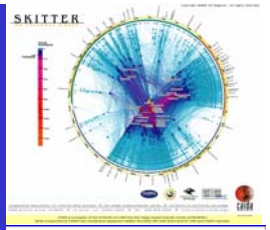
Config Monitoring

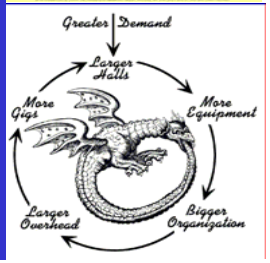
- **RANCID - Really Awesome New Cisco config Differ (but works with lots of routers)**
  - **http://www.shrubbery.net/rancid/**
  - **http://www.nanog.org/mtg-0310/rancid.html**

- **Rancid monitors a device's configuration (software & hardware) using CVS.**

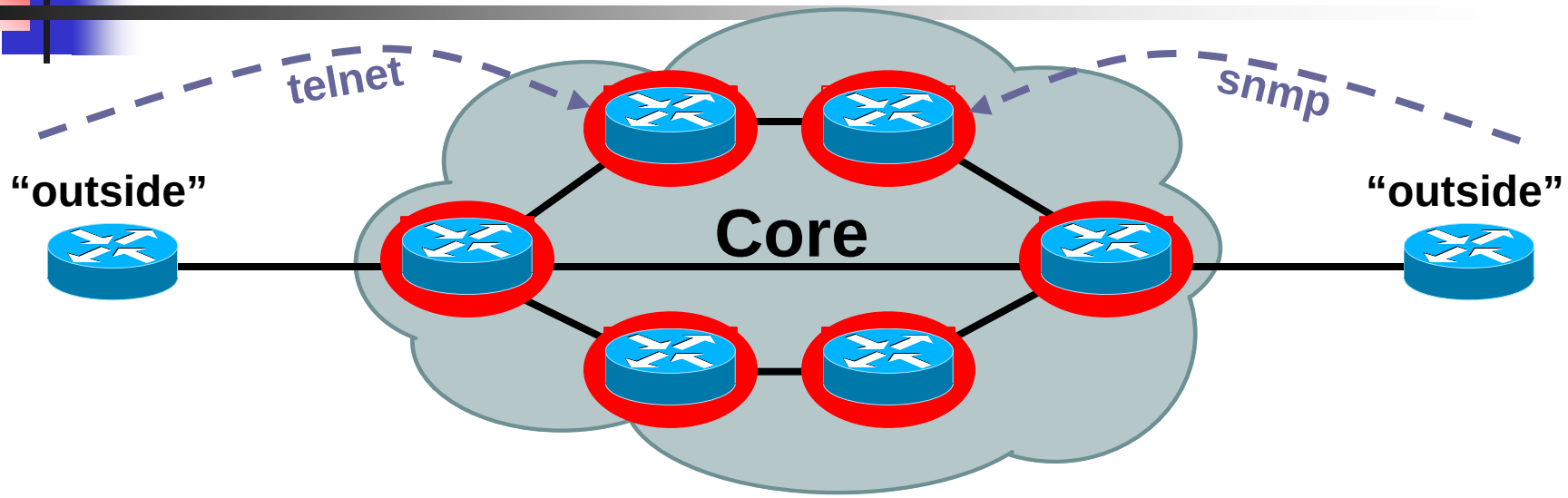
- **Rancid logs into each of the devices in the device table file, runs various show commands, processes the output, and emails any differences from the previous collection to staff.**

Edge Protection



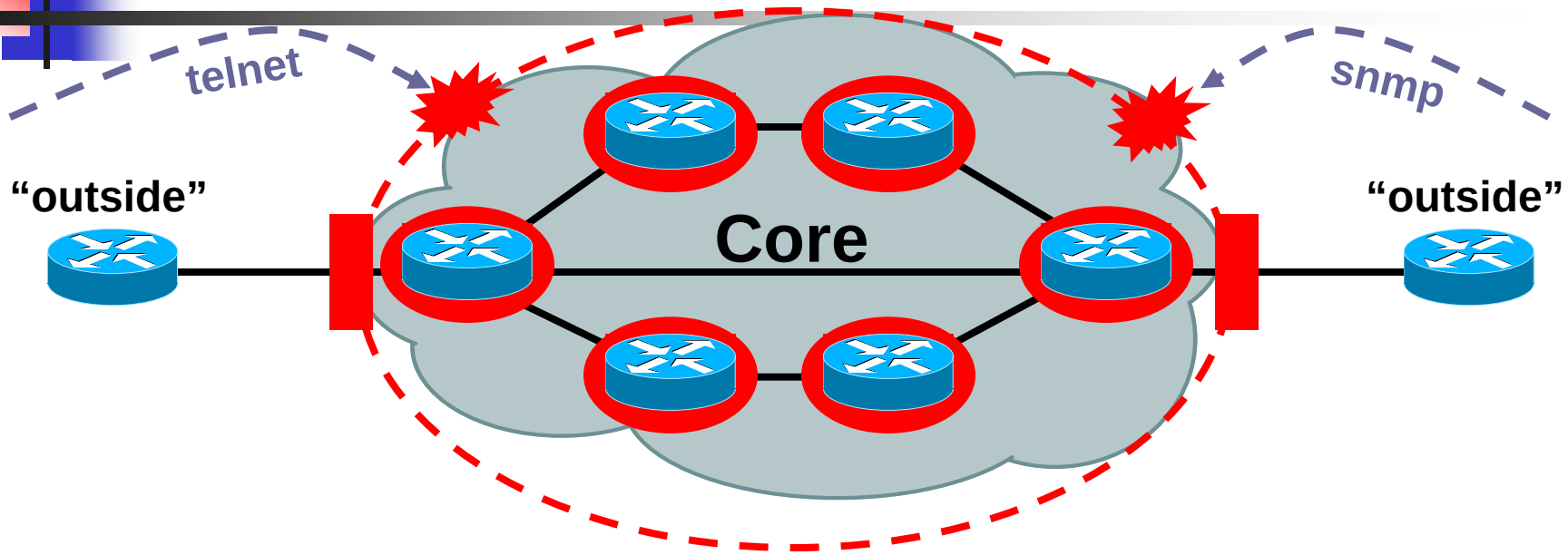


The Old World: Network Edge

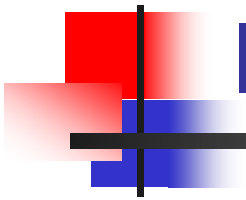


- Core routers individually secured
- Every router accessible from outside

The New World: Network Edge

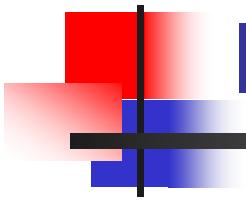


- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside



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

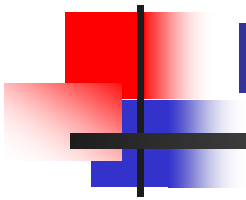


Infrastructure ACLs

- 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

A Digression: IP Fragments and Security

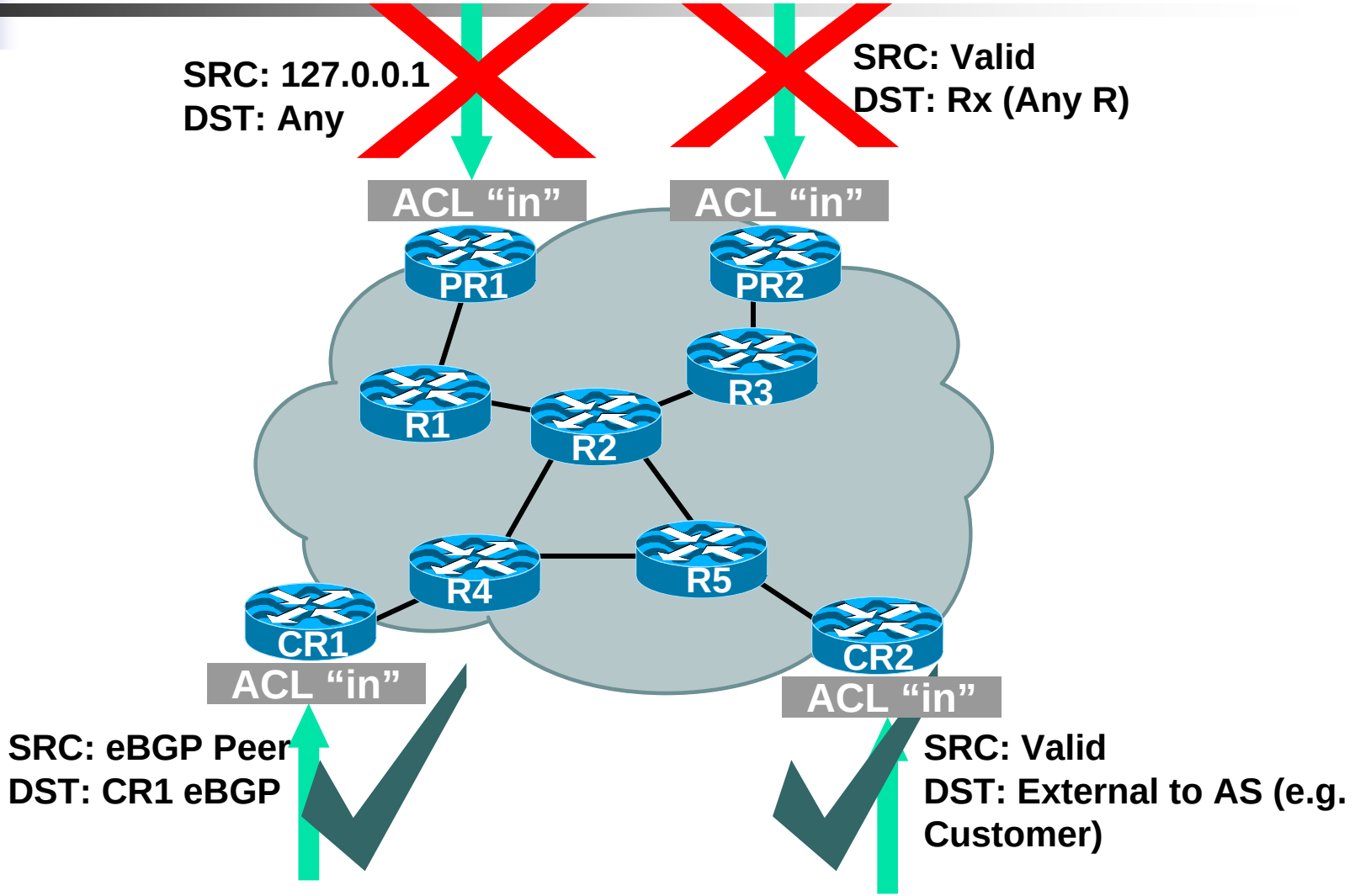
- Fragmented Packets can cause problems...
  - Fragmented packets can be used as an attack vector to bypass ACLs
  - Fragments can increase the effectiveness of some attacks by making the recipient consume more resources (CPU and memory) due to fragmentation reassembly
- ACL fragment handling...
  - By default (without the fragments keyword)...
    - Initial fragments and non-fragmented packets
      - L3 ACLs— access control entry (ACE) action executed (permit/deny) since all L3 information is available
      - L4 ACLs—ACE action executed (permit/deny) since all L4 information is available
    - Non-initial fragment packets (assuming L3 match)
      - L3 ACLs—ACE action executed (permit/deny) since all L3 information is available
      - L4 ACLs—ACE action executed (permit/deny) based on L3 info (there is no L4 info in the fragment) and protocol only
  - The ACL fragments keyword enables specialized handling behavior
    - Initial fragments and non-fragmented packets
      - L3 and L4 ACLs—the packet does not match the entry since the fragment keyword is used. The packet then "falls through" to the next line(s)
    - Non-initial fragment packets (assuming L3 match)
      - With L3 and L4 ACLs—with an L3 match (and protocol matches the IP protocol), the action of the ACE is executed (permit/deny)

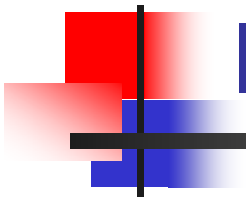


Infrastructure ACLs

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

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 ACLs

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
  - Log keyword can be used for additional detail; hits to ACL entry with *log* will increase CPU utilization: impact varies by platform
- Regardless of method, unexpected results should be carefully analyzed → do not permit protocols that you can't explain!

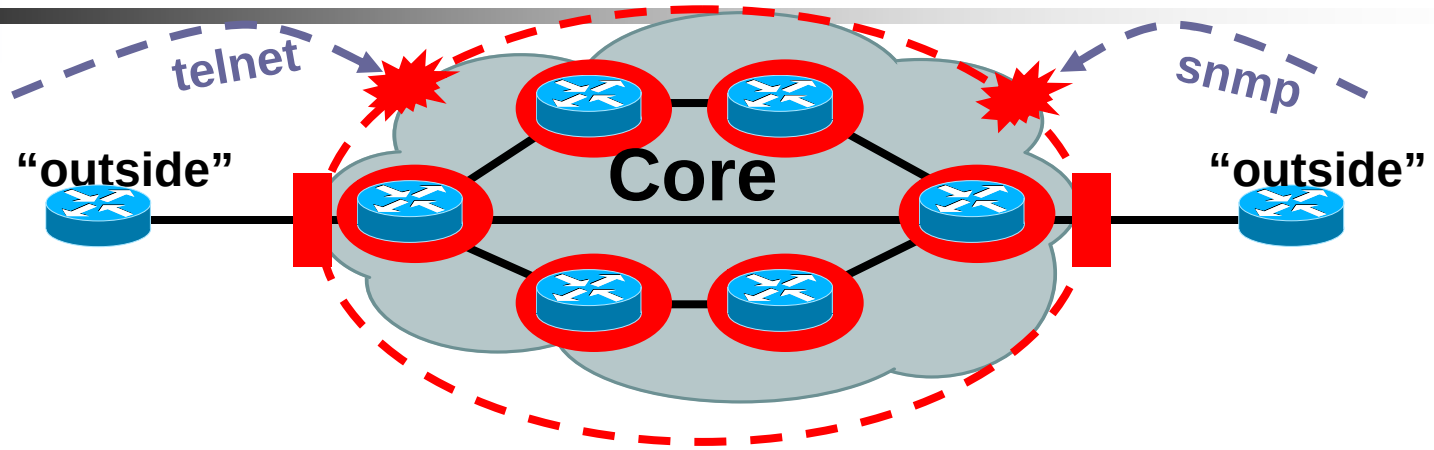
Step 2: Begin to Filter

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

Steps 3 and 4: Restrict Source Addresses

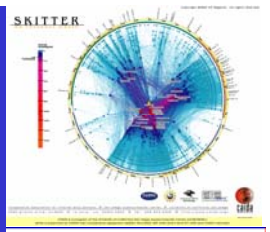
- Step 3:
  - ACL is providing basic protection
  - Required protocols permitted, all other denied
  - Identify source addresses and permit only those sources for requires protocols
  - e.g., external BGP peers, tunnel end points
- Step 4:
  - Increase security: deploy destination address filters if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

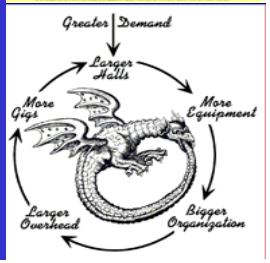
Infrastructure ACLs



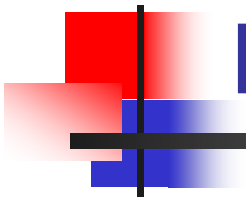
- Edge "shield" in place
- Not perfect, but a very effective first round of defense
  - Can you apply iACLs everywhere?
  - What about packets that you cannot filter with iACLs?
  - Hardware limitations
- Next step: secure the control/management planes per box

Remote Trigger Black Hole



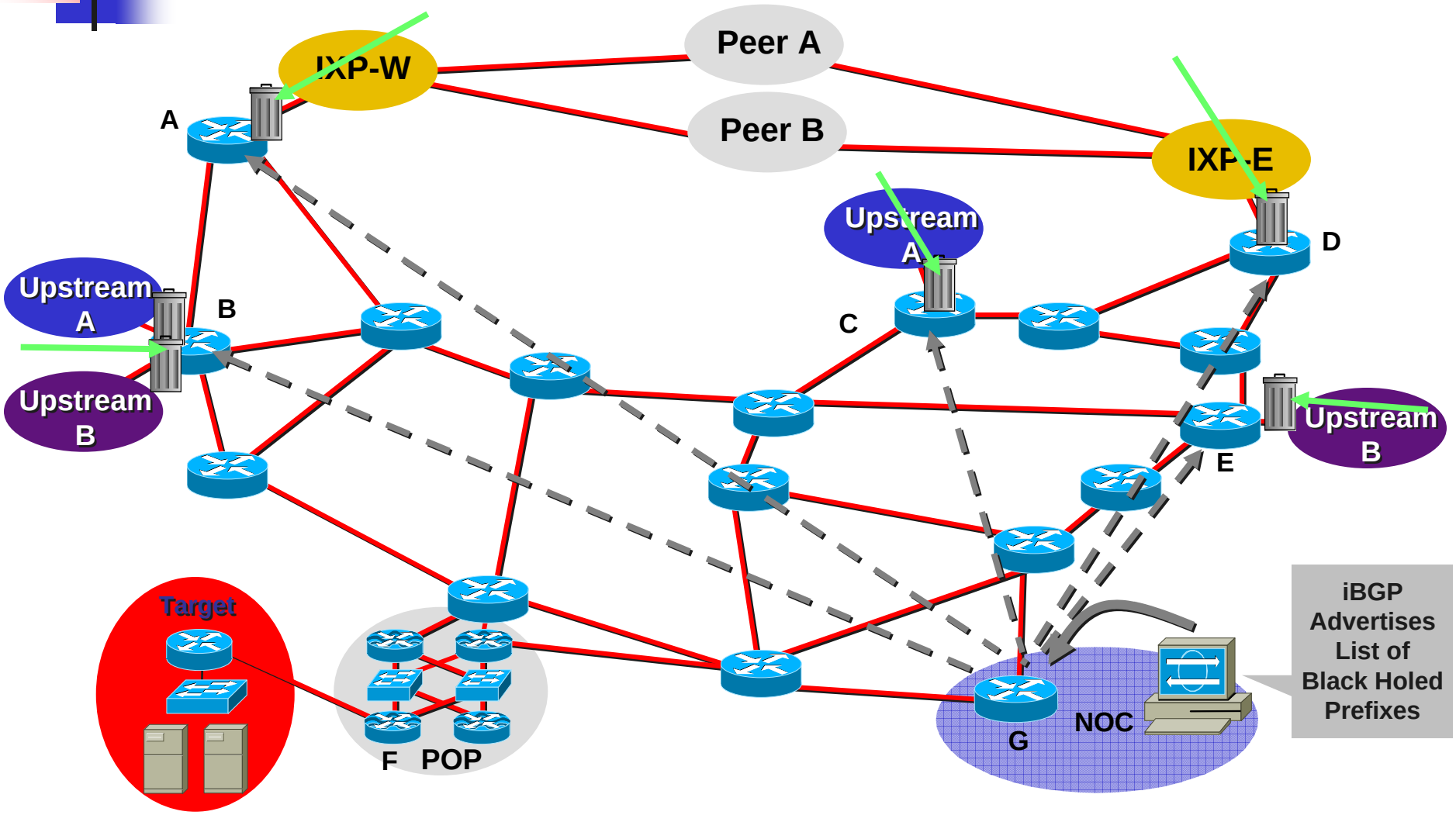


Remotely Triggered Black Hole Filtering

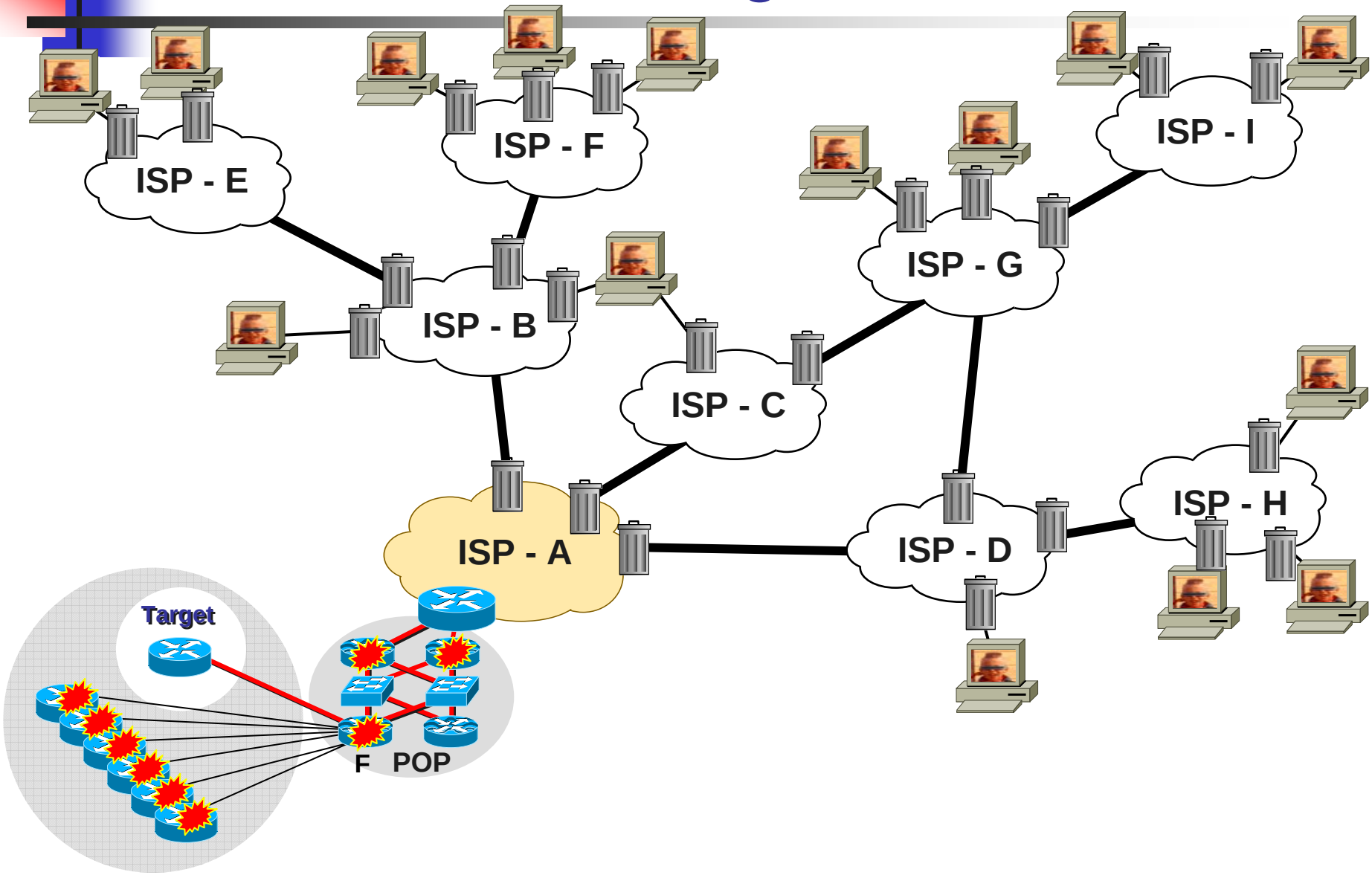


- We use BGP to trigger a network wide response to a range of attack flows.
- A simple static route and BGP will allow an ISP to trigger network wide black holes as fast as iBGP can update the network.
- This provides ISPs a tool that can be used to respond to security related events or used for DOS/DDOS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

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



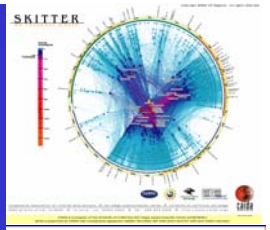
Inter-Provider Mitigation

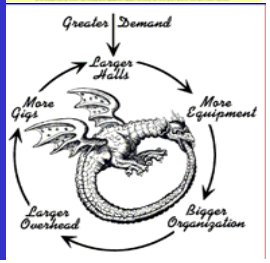


What can you do to help?

- 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)

Sink Holes

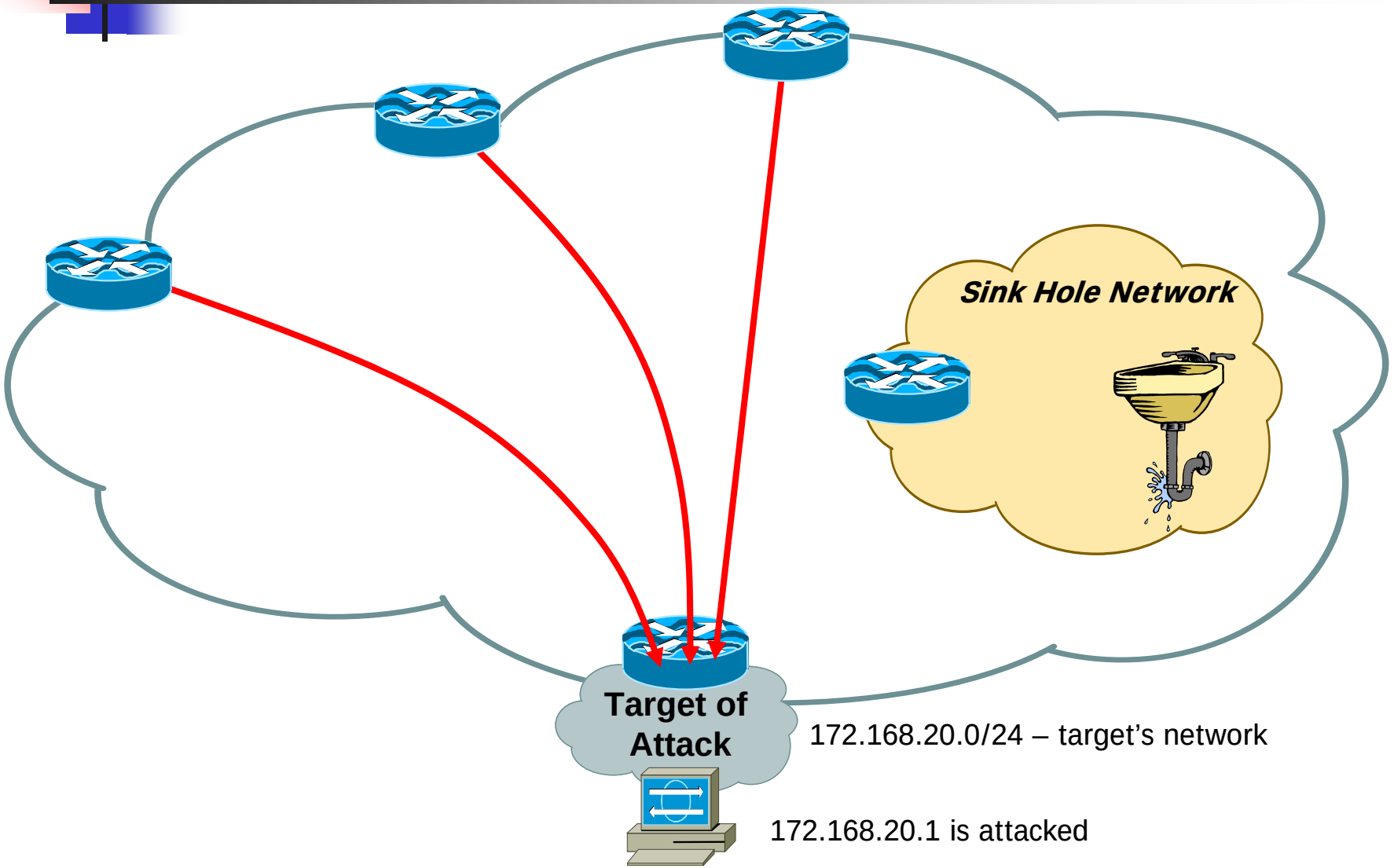

SKITTER


Greater Demand
Larger Halls
More Equipment
Bigger Organization
Larger Overhead
More Gigs

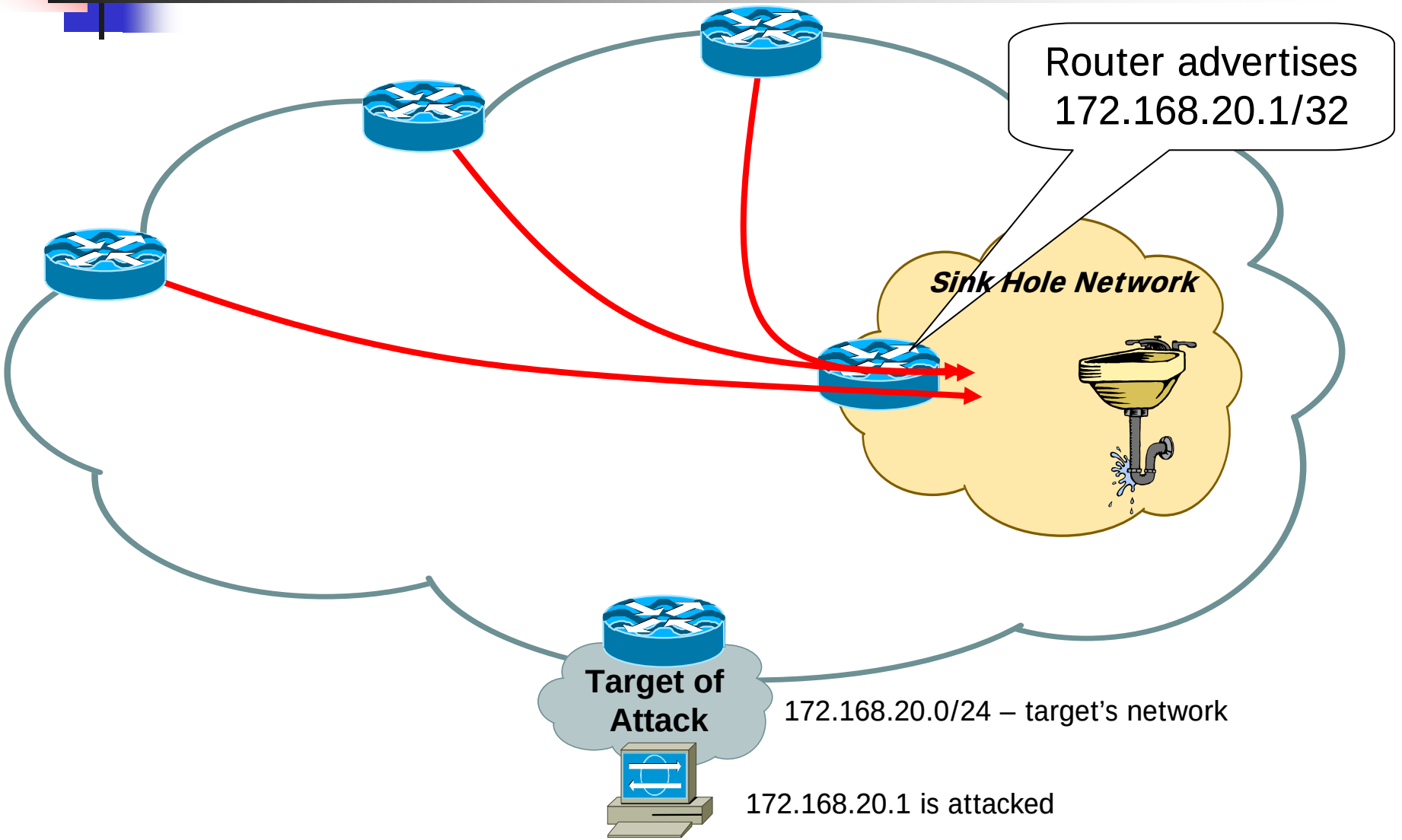
Sink Hole Routers/Networks

- 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

Sink Hole Routers/Networks

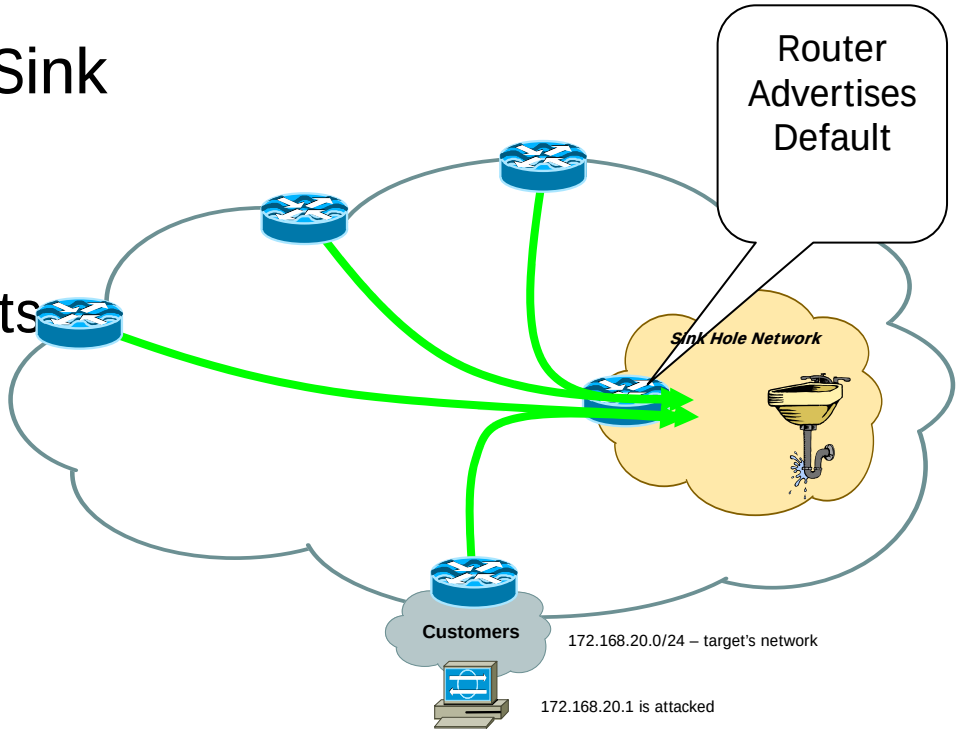


Sink Hole Routers/Networks

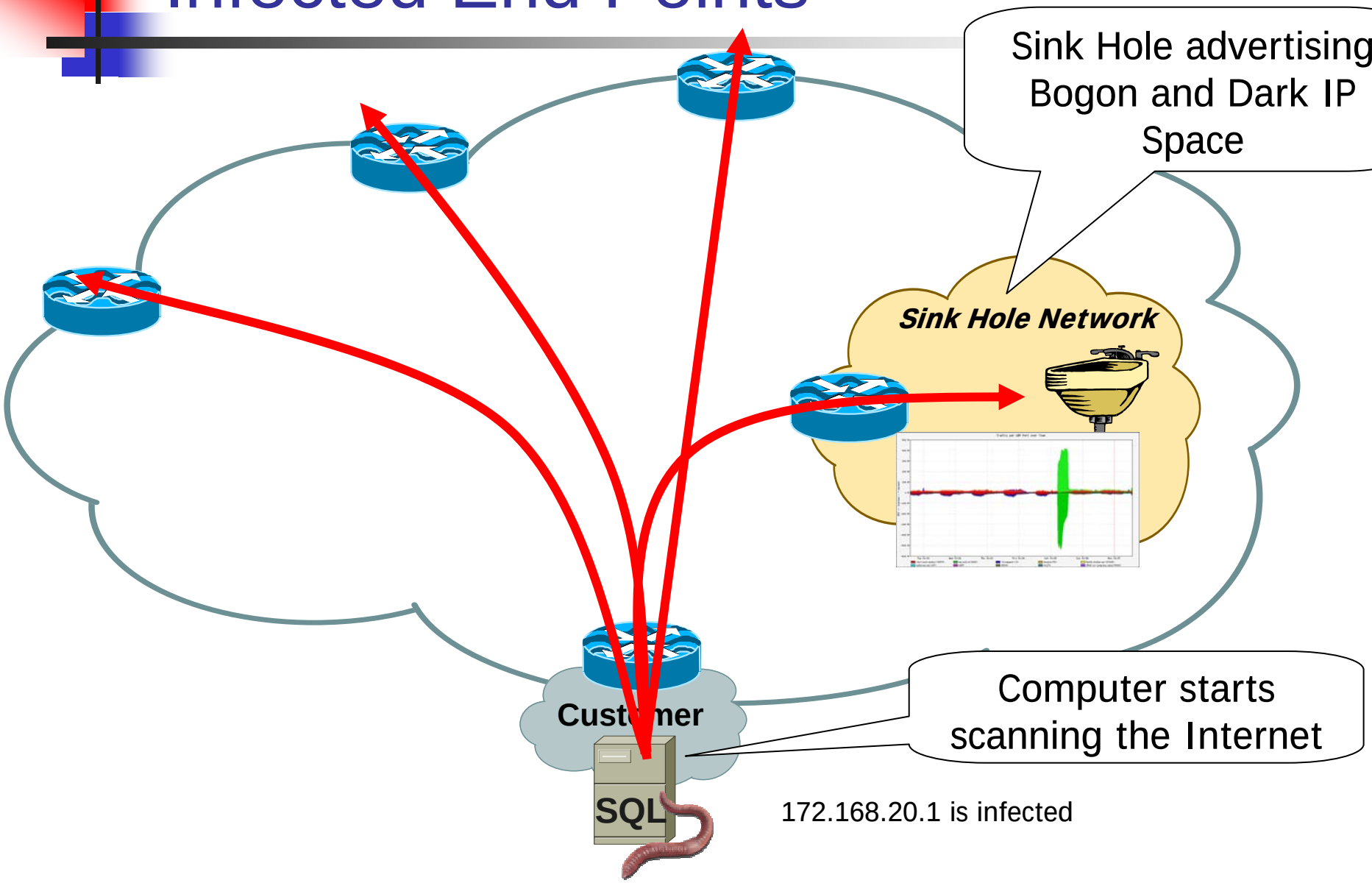


Sink Hole Routers/Networks

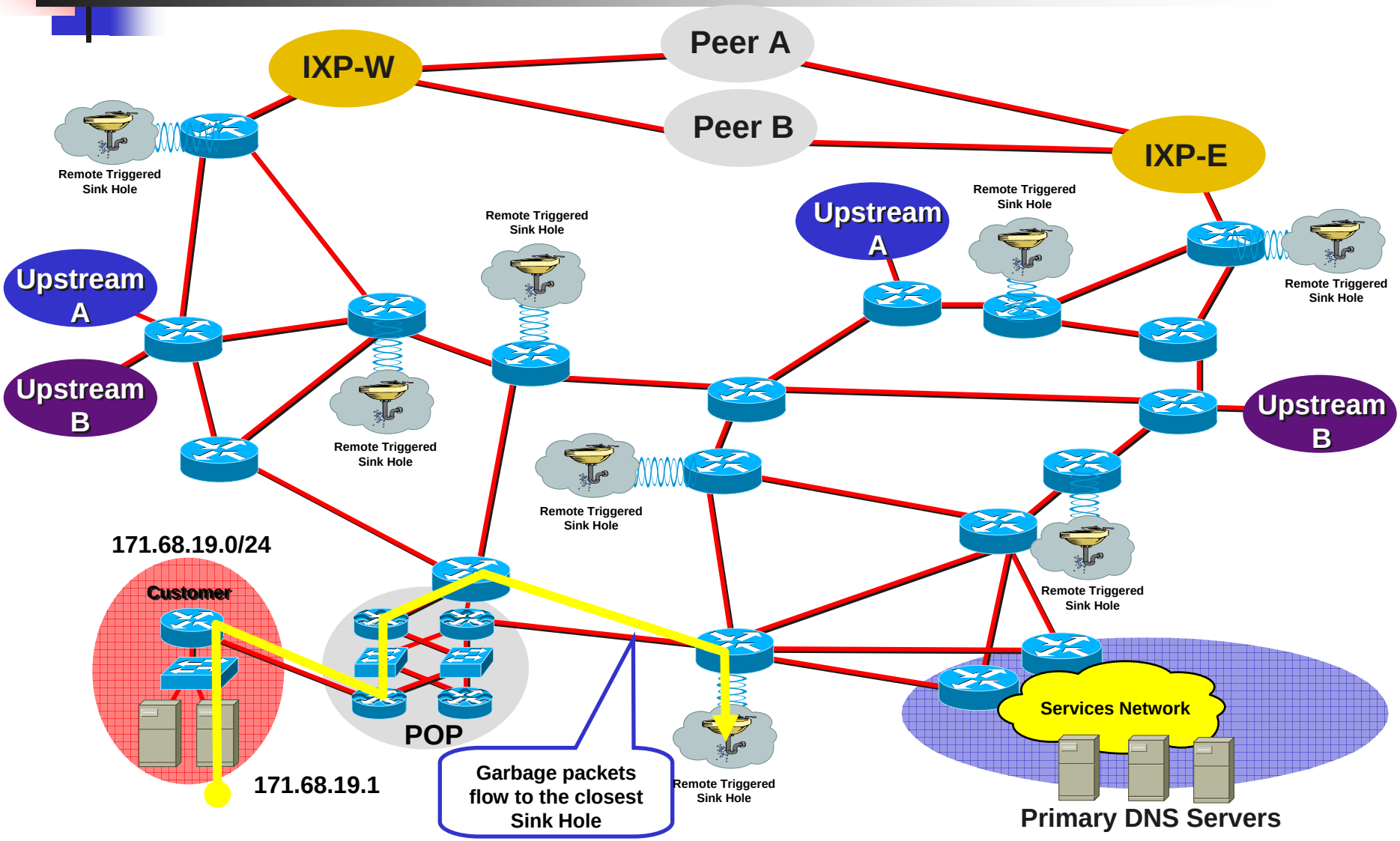
- Advertising Default from the Sink Hole will pull down all sort of *junk* traffic.
  - Customer Traffic when circuits flap.
  - Network Scans
  - Failed Attacks
  - Code Red/NIMDA
  - Backscatter
- Can place tracking tools and IDA in the Sink Hole network to monitor the noise.



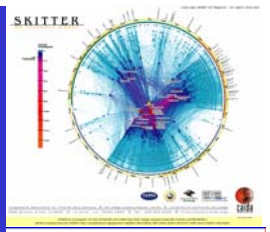
Infected End Points

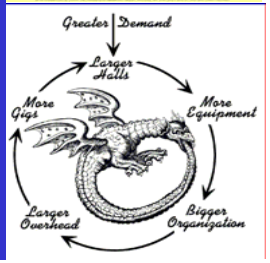


Anycast Sink Holes



Source Address Validation





BCP 38 Ingress Packet Filtering

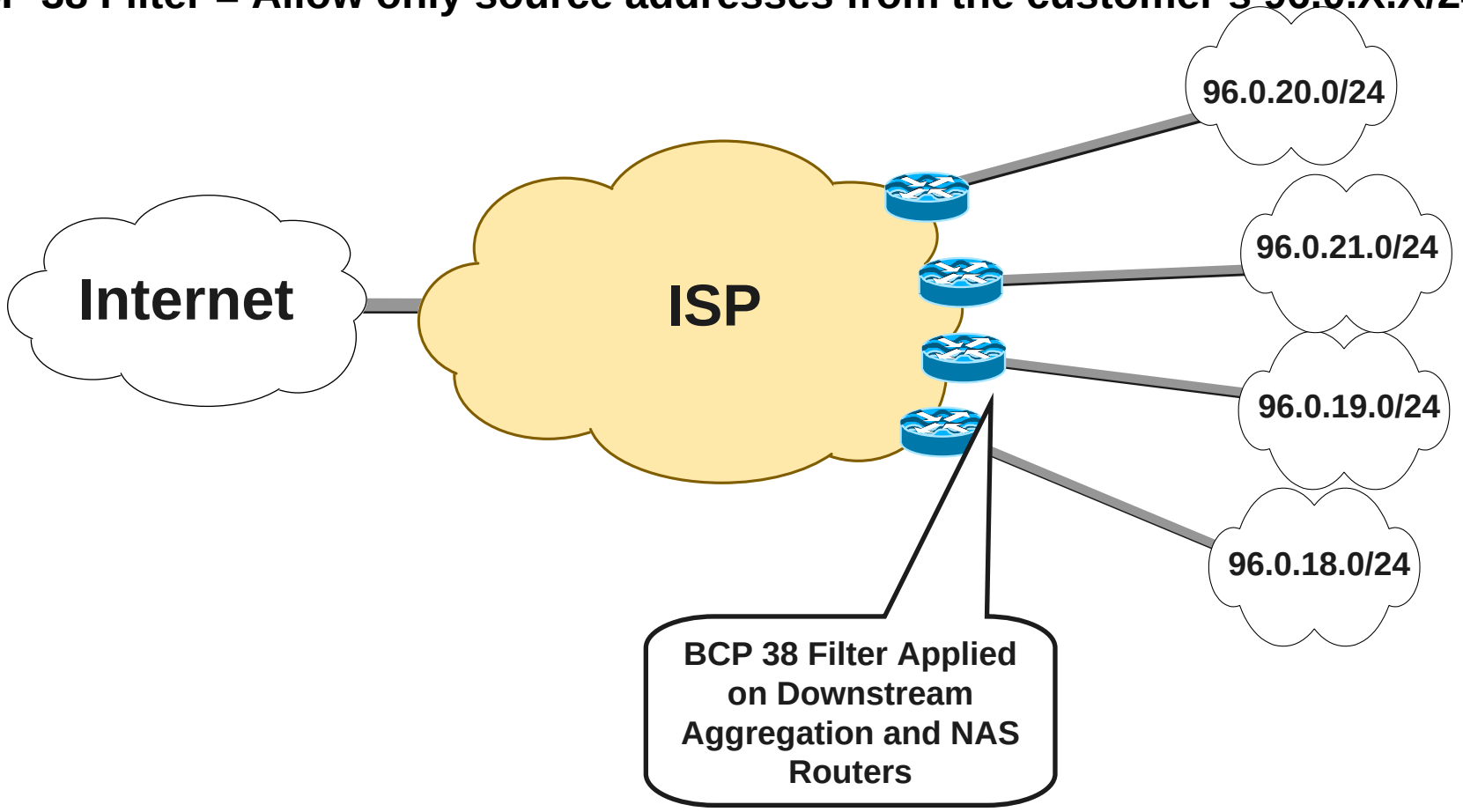
Your customers should not be sending any IP packets out to the Internet with a source address other then the address you have allocated to them!

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

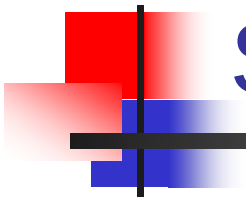


BCP 38 Packet Filtering: Principles

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

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 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.

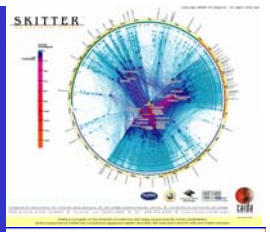
One Major ISP's Example - uRPF

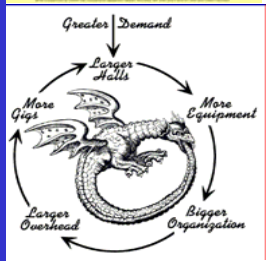
- Lessons Learned:
  - It took time and patience.
  - uRPF did not work for all customers. That is OK, uRPF is not suppose to be a *universal solution.*
  - Going slow and steady allowed the operations team to *gain a feel* of the feature's performance envelope --- with out putting the network at risk.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

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

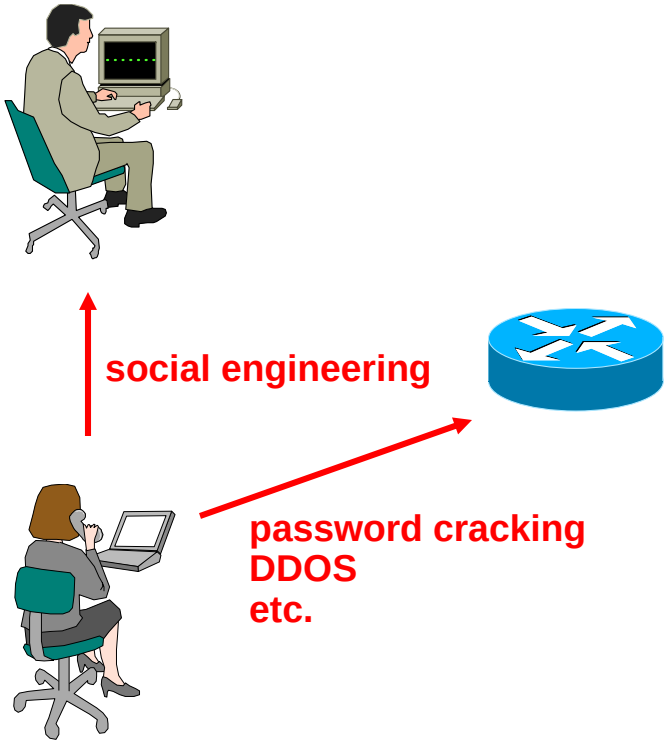
- Understanding BGP Attack Vectors will help you plan and prioritize the techniques deployed to build greater resistance into the system.
- The following documents will help you gain perspective on the realistic Risk Assessment:
  - NANOG 25 - BGP Security Update
    - http://www.nanog.org/mtg-0206/barry.html
  - 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

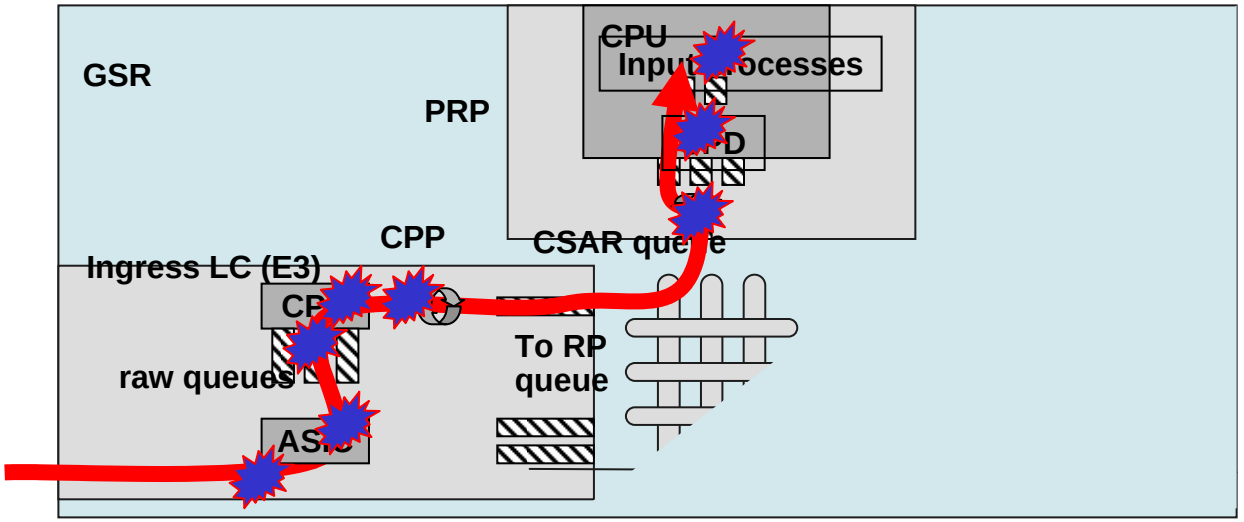
Attacking Routing Devices

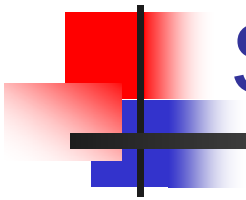
- All the normal host attack methods apply to routers
  - Social engineering
  - Password cracking
  - Denial of service
  - etc.
- What an attacker needs:
  - Access to the router
  - *(or)*
  - Access to the network



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

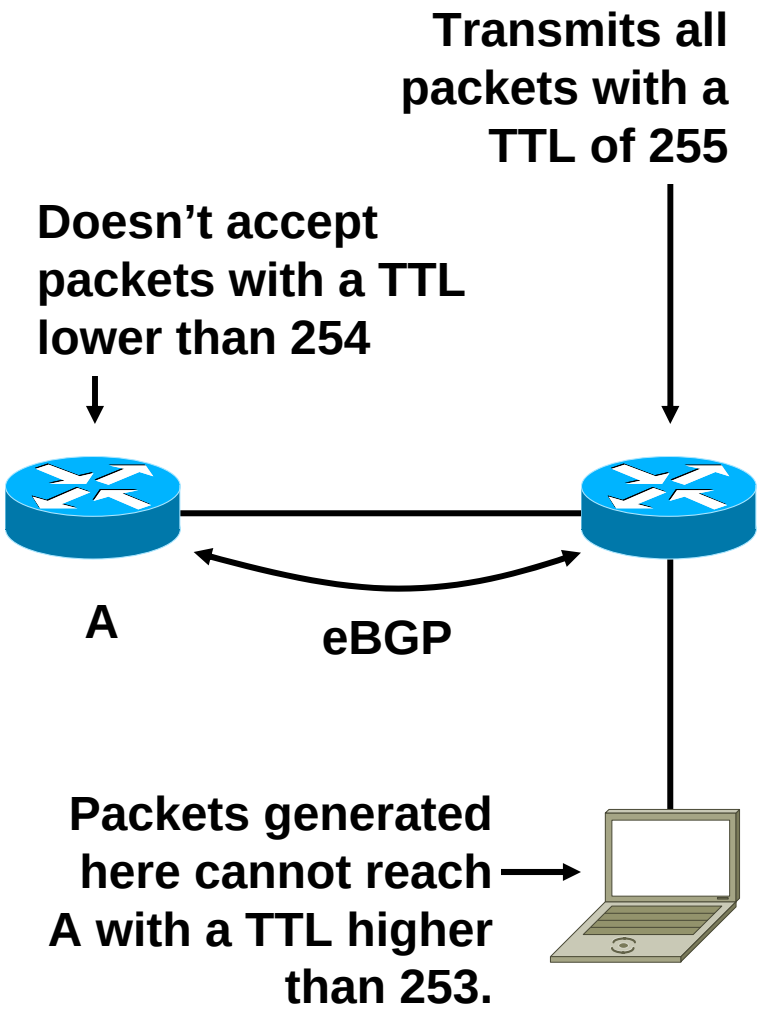
- DOS Attacks Saturating the link will knock out valid control plane packets.
- Link packet over POS, ATM, or Ethernet will drop out – which drop out the link – which drop out the FIB's next hop – which knocks out the BGP Entries
- This is a very effective brute force attack.

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)

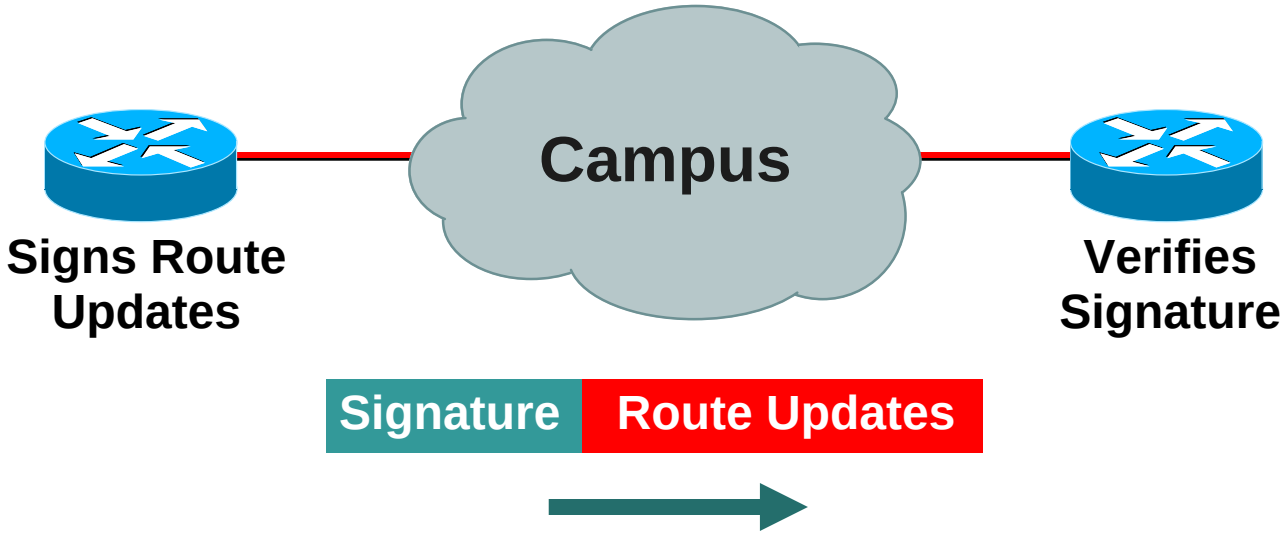
Generalized TTL Security Mechanism

- 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

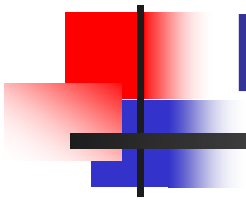
Configure Routing Authentication



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

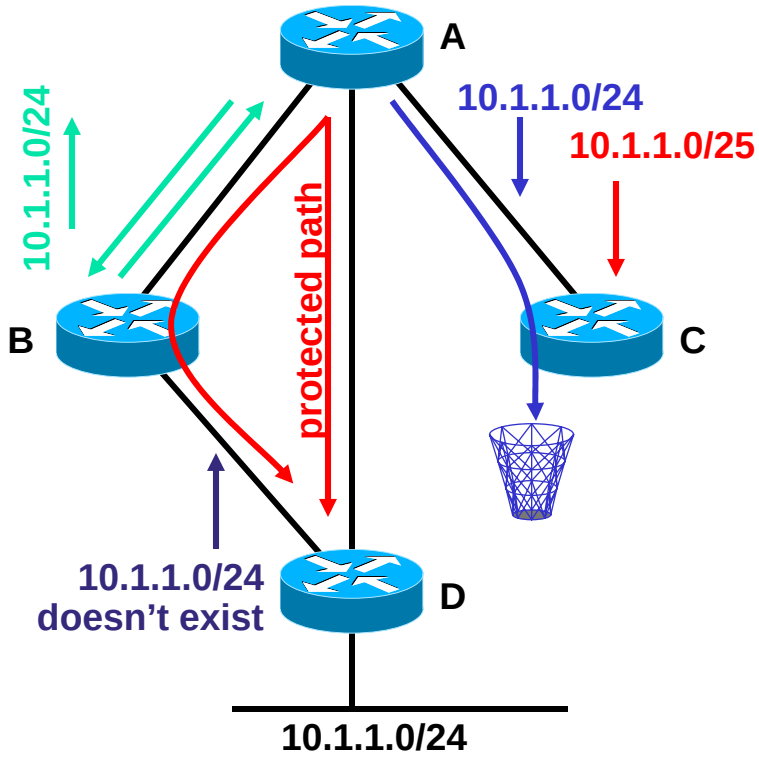


Drop the IGP

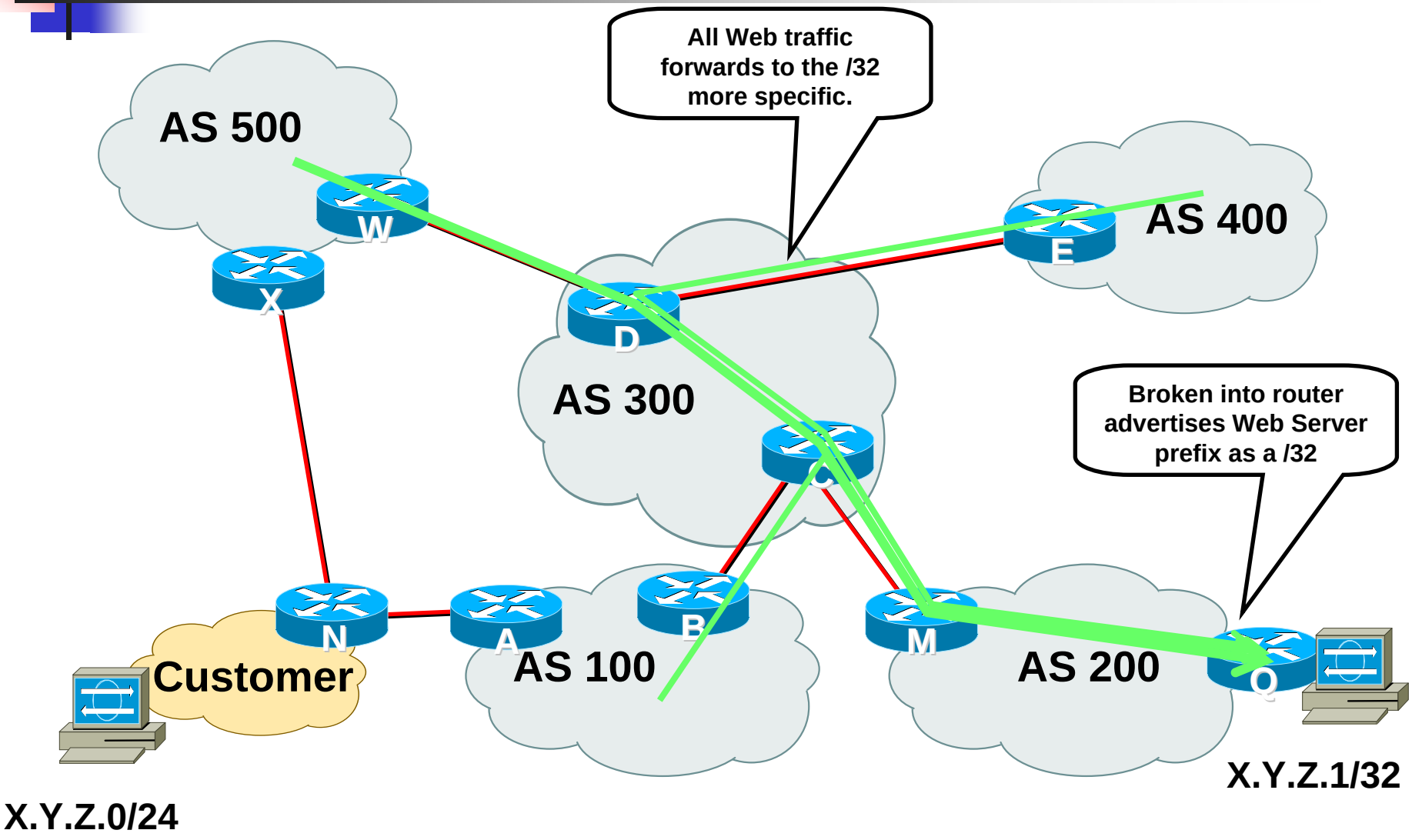
- Miscreant Success Principle - If you cannot take out the target, move the attack to a coupled dependency of the target.
- BGP's coupled dependency is the IGP it requires for recursive look-up.
- EIGRP and OSPF are both open to external attacks.

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 nonexistant destinations
  - *A longer prefix!*
- Underclaiming
  - Removing destinations



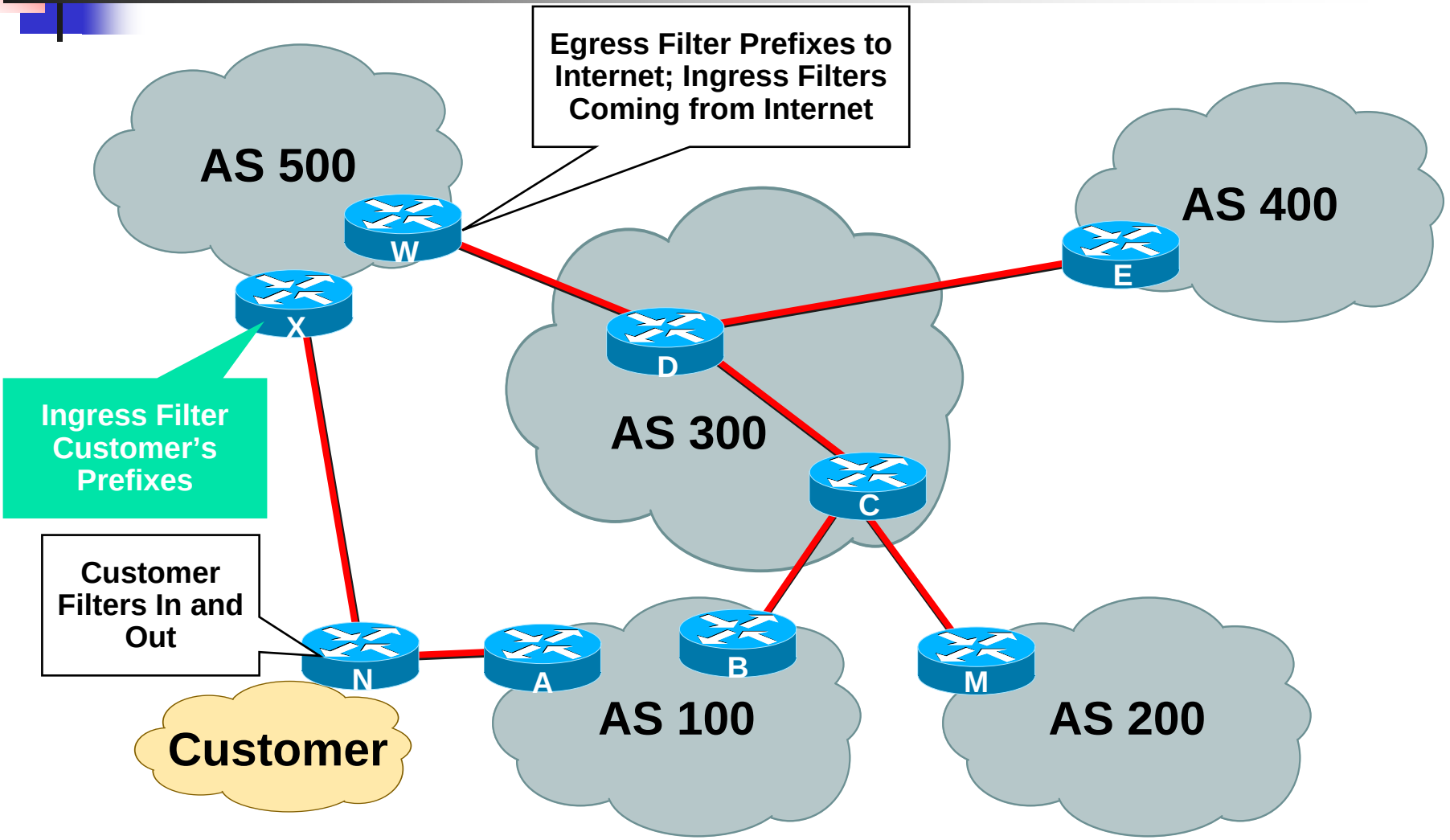
What is a prefix hijack?



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.

Where to Prefix Filter?



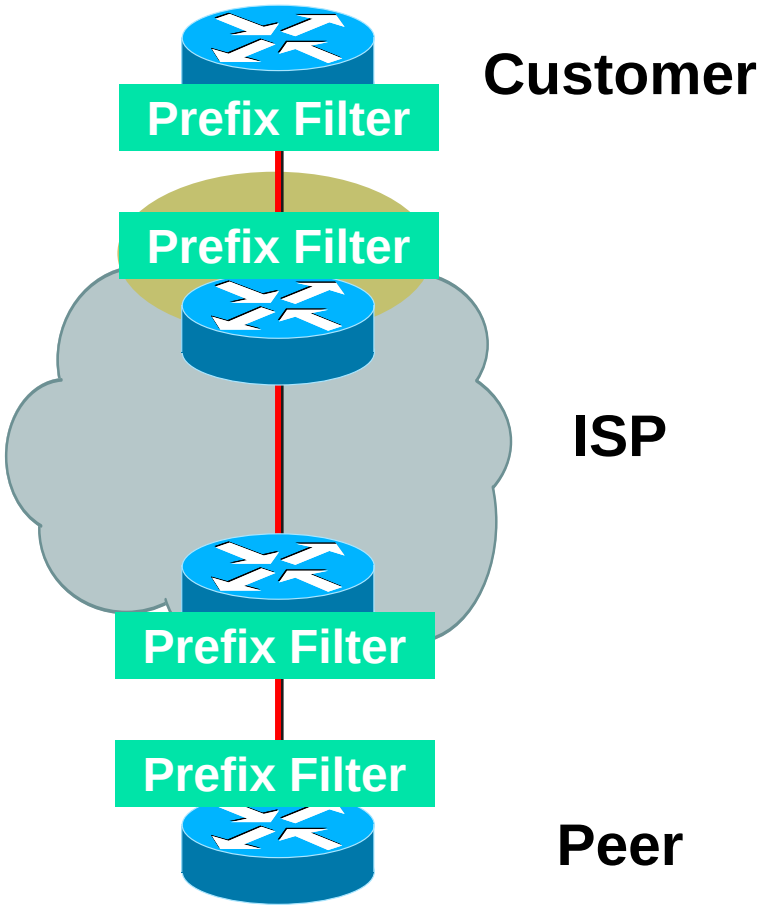
Bogons and Special Use Addresses

- 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

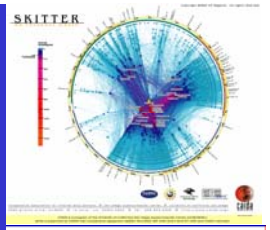
Prefix Filters: Application

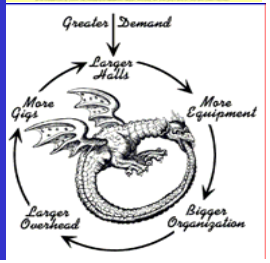
Apply Prefix Filters to All eBGP Neighbors

- To/from customers
- To/from peers
- To/from upstreams



Total Visibility

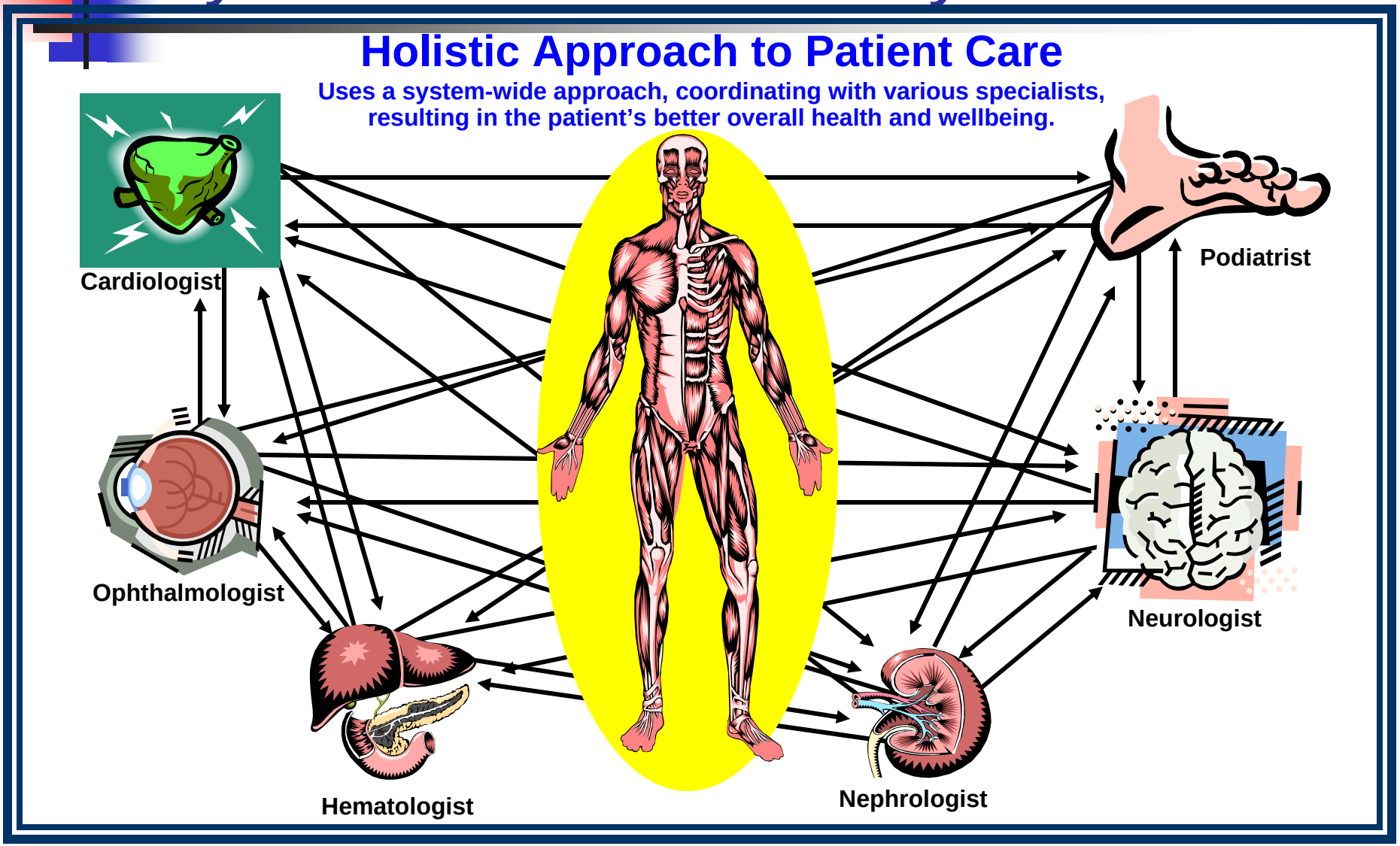




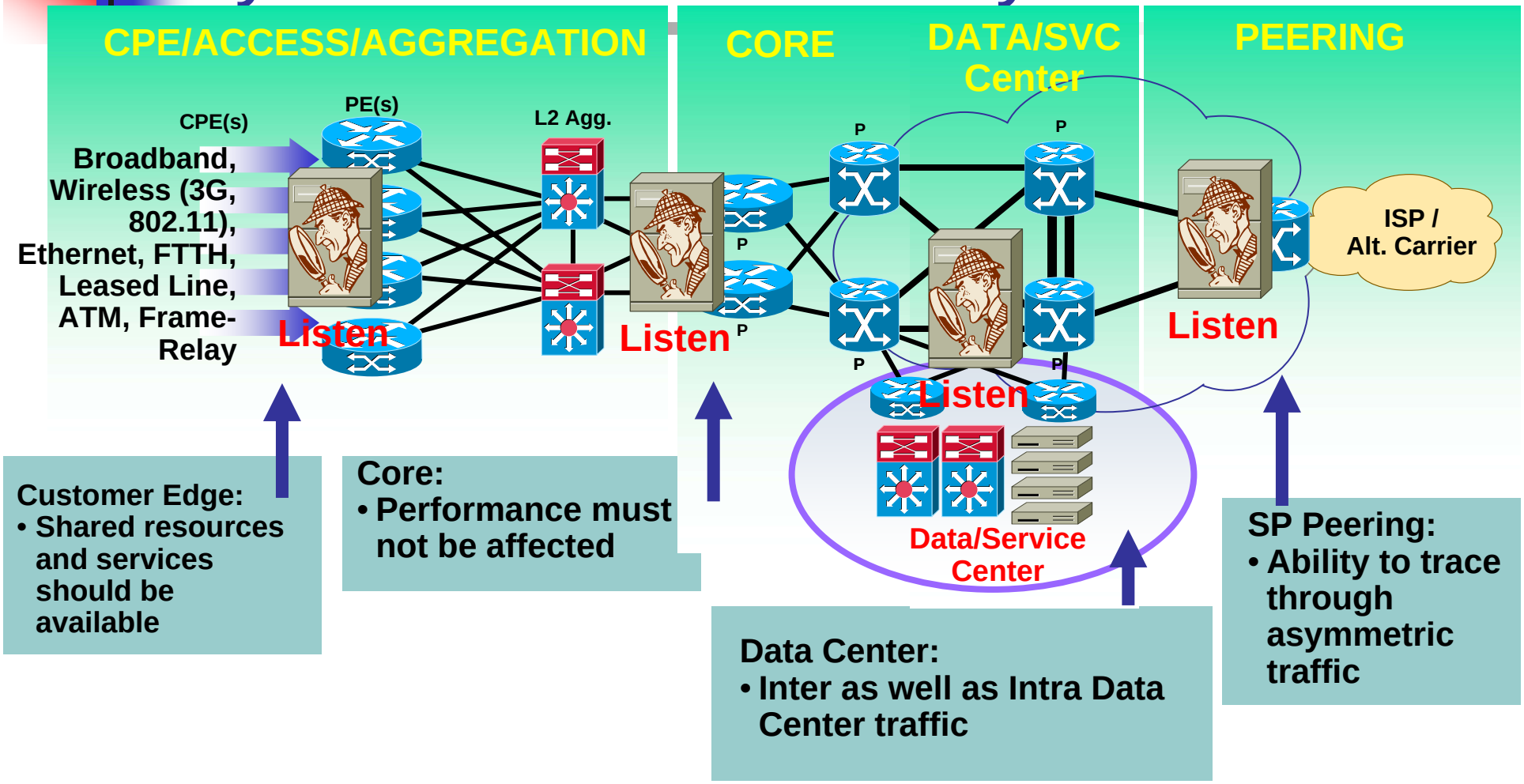
Check List

- 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 System-Wide Telemetry



Customer Edge:
- Shared resources and services should be available

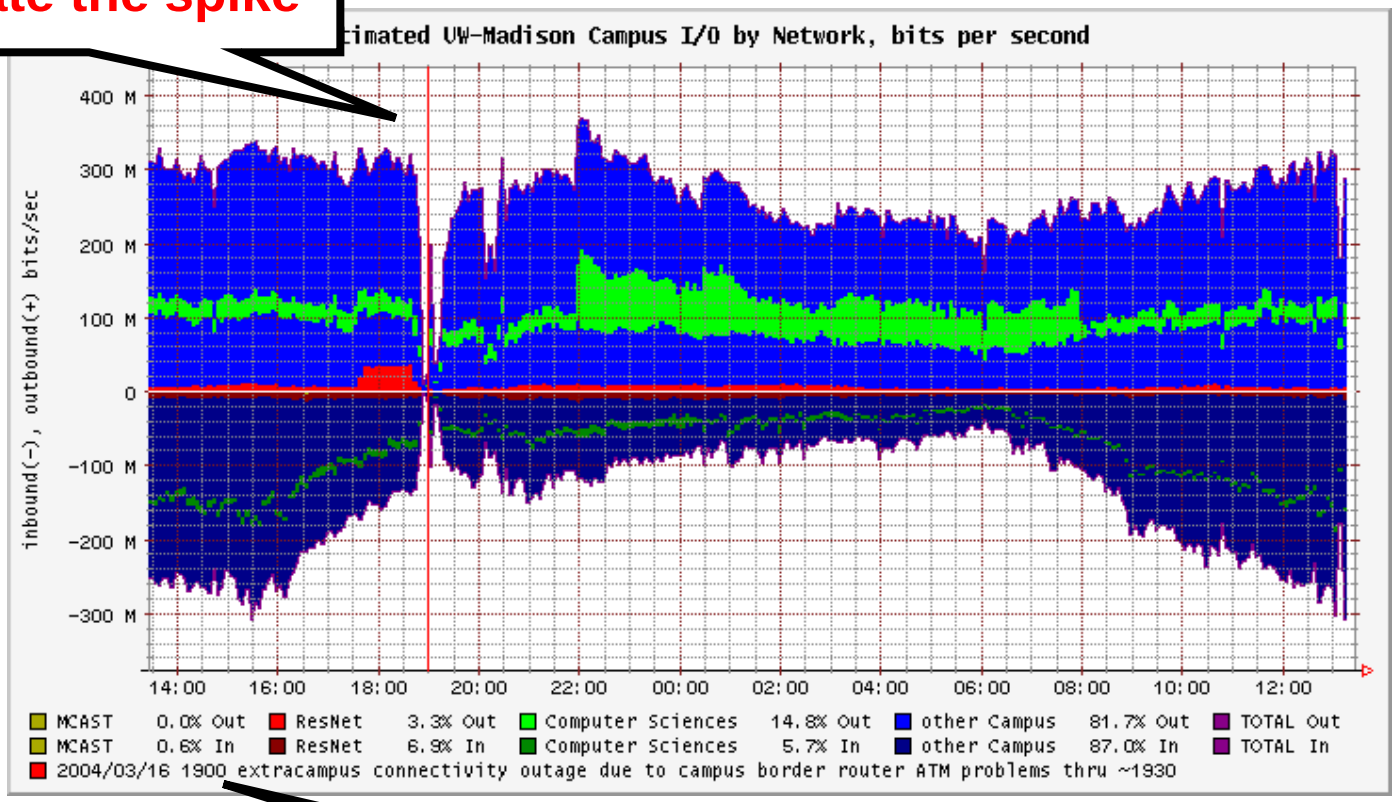
Core:
- Performance must not be affected

Data Center:
- Inter as well as Intra Data Center traffic

SP Peering:
- Ability to trace through asymmetric traffic

Open Source Tools for NetFlow Analysis Visualization—FlowScan

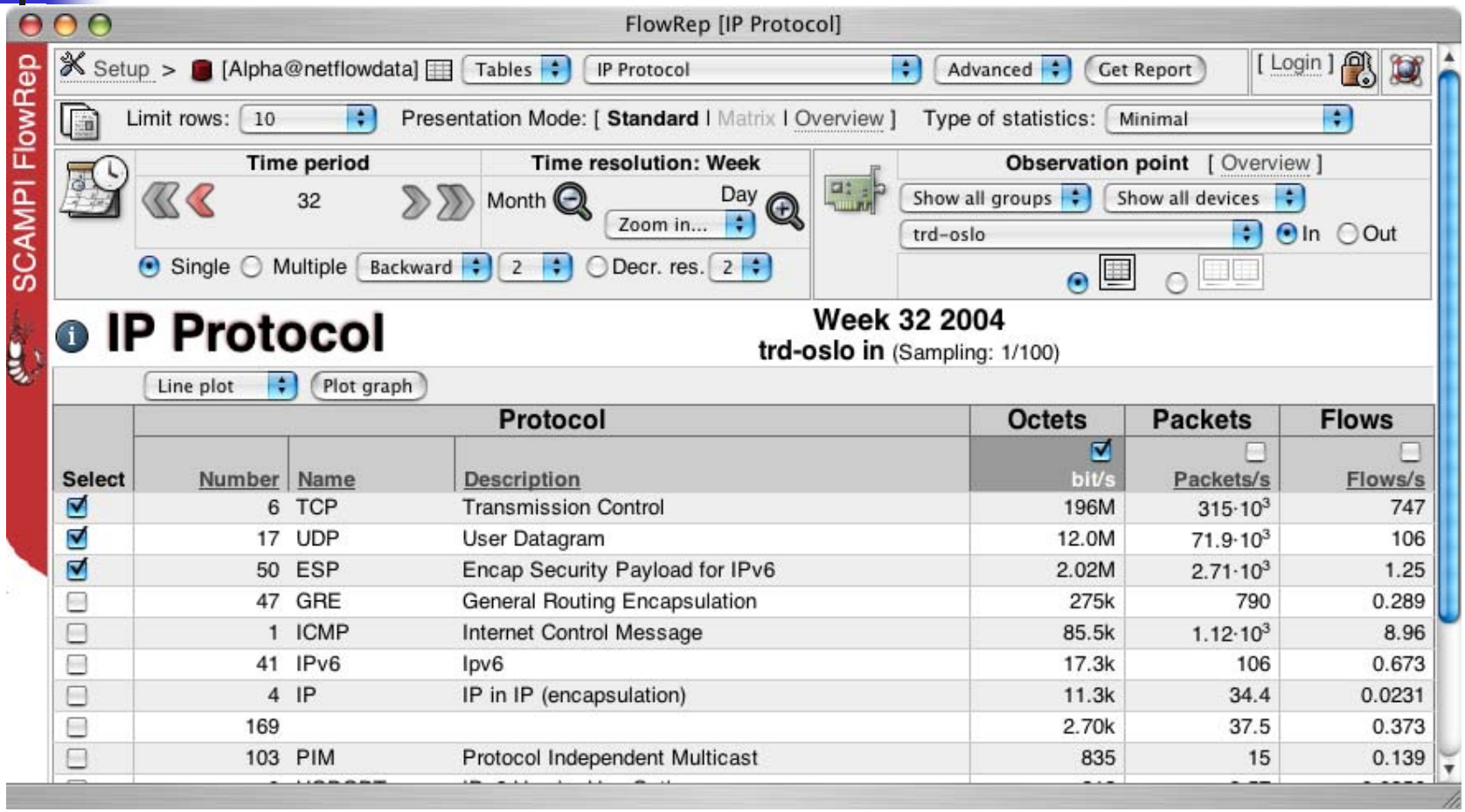
Investigate the spike



An identified cause of the outage

Source: University of Wisconsin

NetFlow - Stager

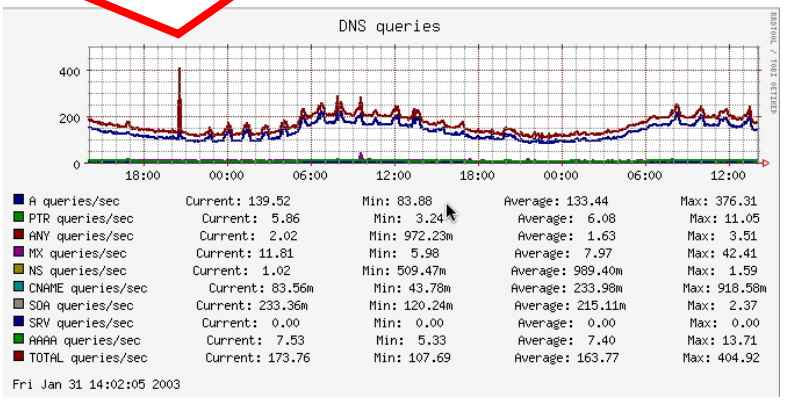


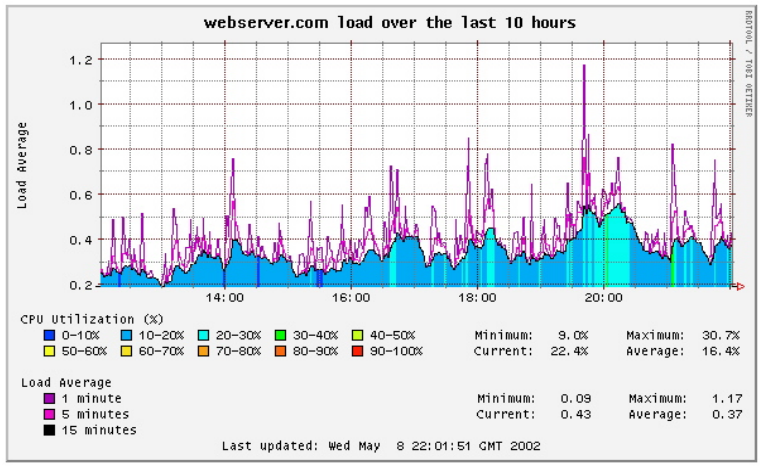
Select	Protocol Number	Name	Description	Octets bit/s	Packets Packets/s	Flows Flows/s
☑	6	TCP	Transmission Control	196M	$315 \cdot 10^3$	747
☑	17	UDP	User Datagram	12.0M	$71.9 \cdot 10^3$	106
☑	50	ESP	Encap Security Payload for IPv6	2.02M	$2.71 \cdot 10^3$	1.25
☐	47	GRE	General Routing Encapsulation	275k	790	0.289
☐	1	ICMP	Internet Control Message	85.5k	$1.12 \cdot 10^3$	8.96
☐	41	IPv6	Ipv6	17.3k	106	0.673
☐	4	IP	IP in IP (encapsulation)	11.3k	34.4	0.0231
☐	169			2.70k	37.5	0.373
☐	103	PIM	Protocol Independent Multicast	835	15	0.139

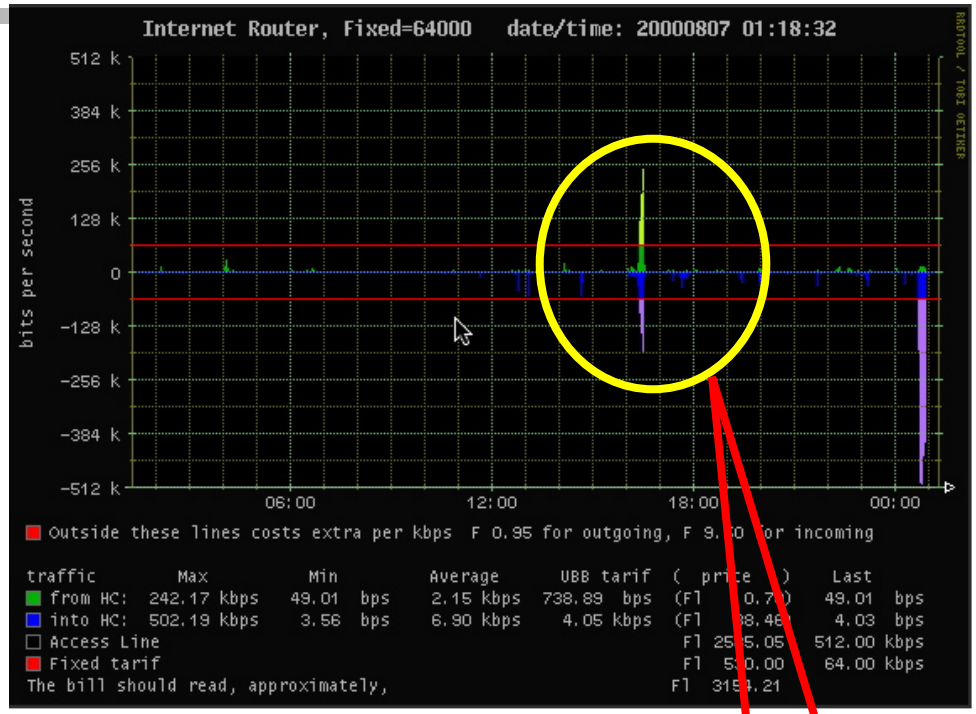
Source: UNINETT

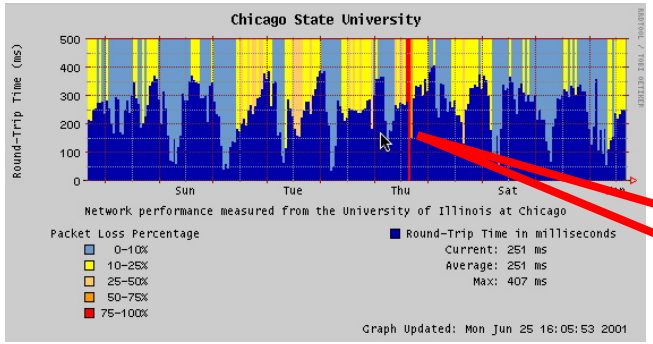
Other Visualization Techniques Using SNMP Data with RRDTool

Anomaly for DNS Queries







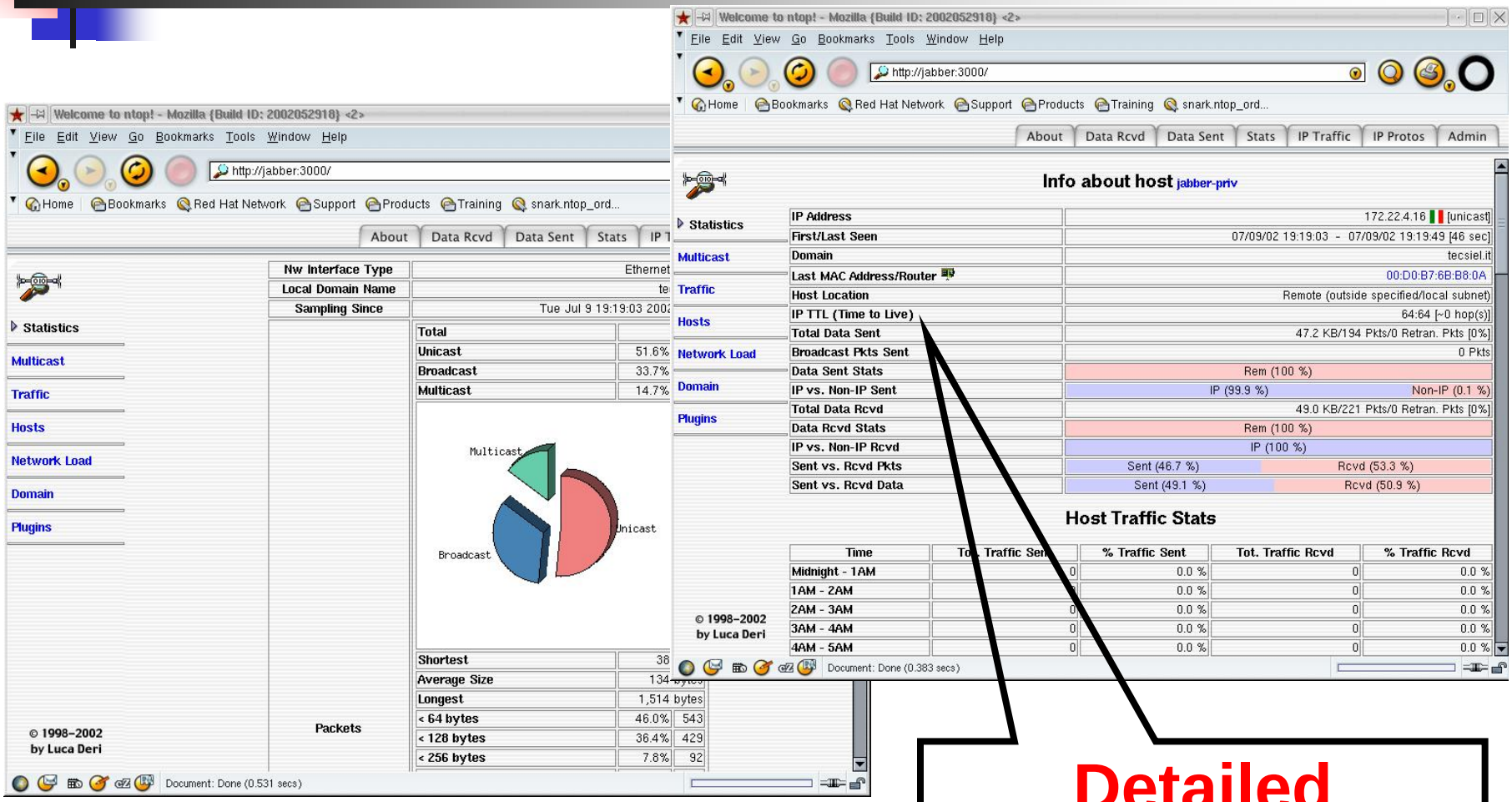


Thru'put Spike

RTT Spike

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

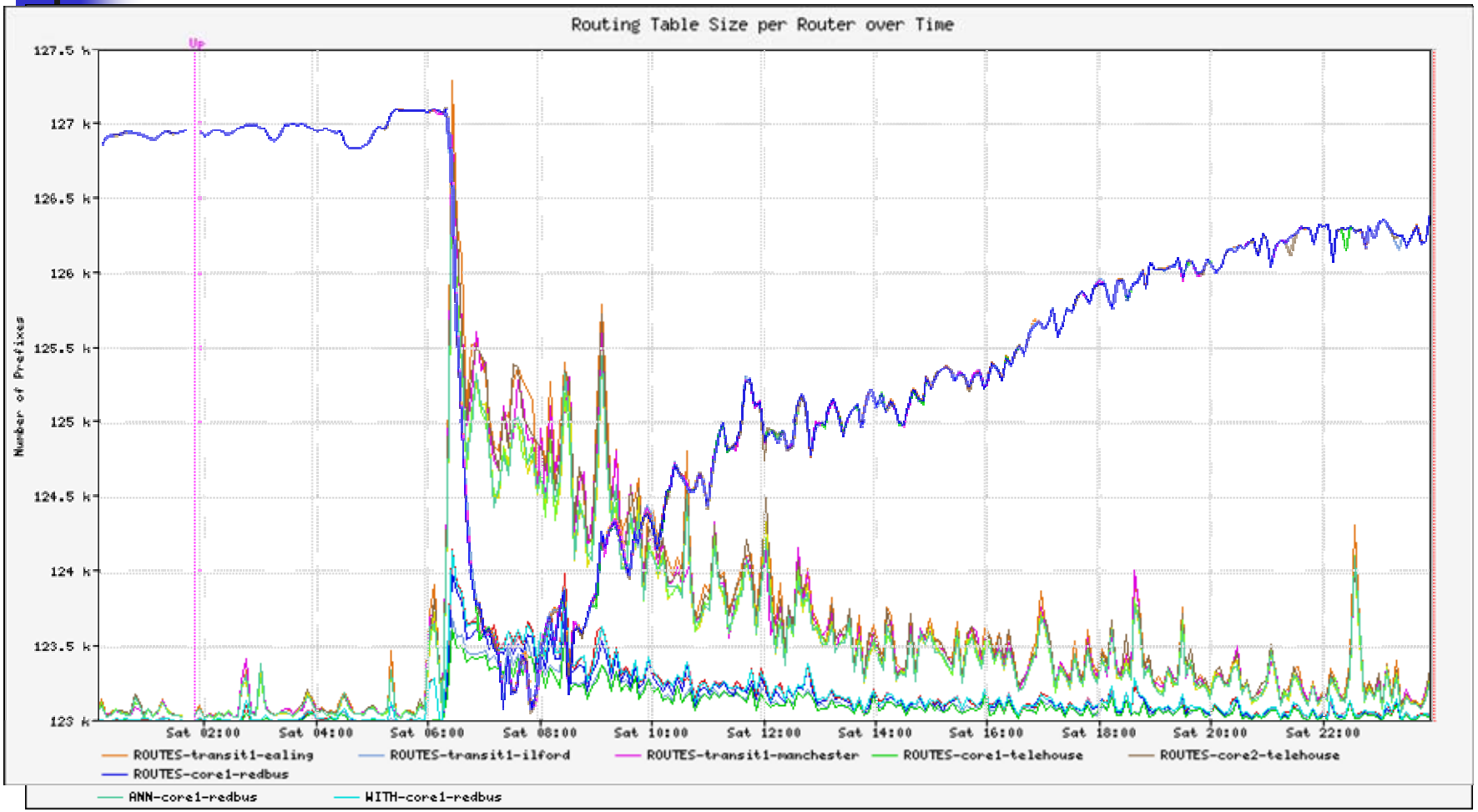
Displaying RMON—ntop Examples



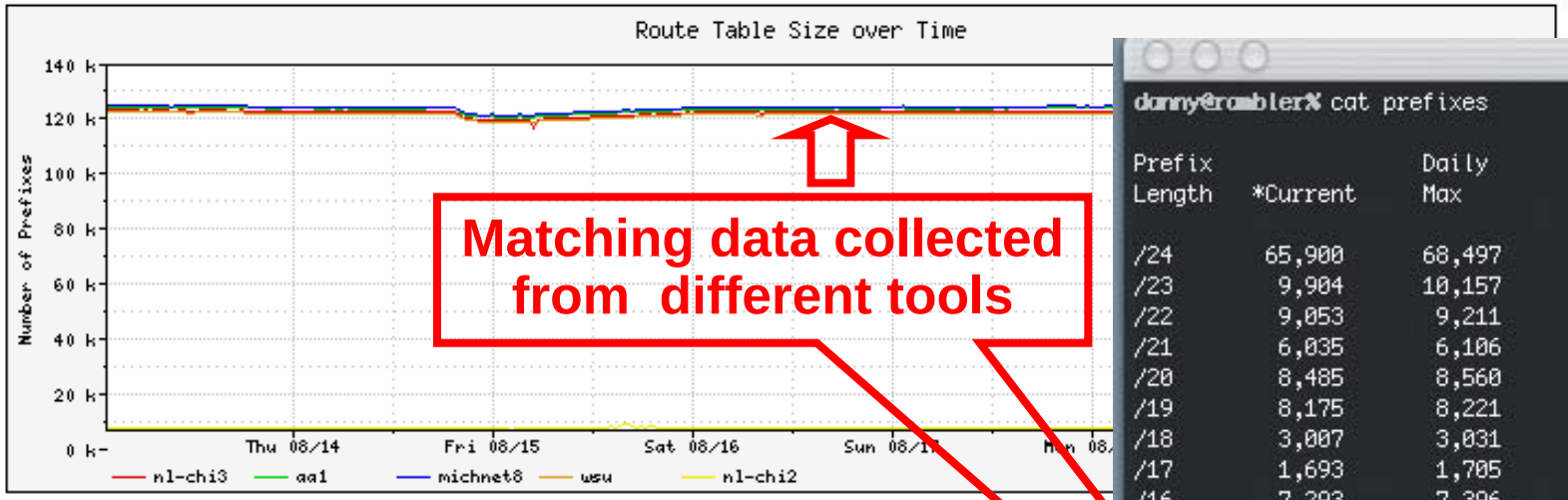
Source: http://www.ntop.org

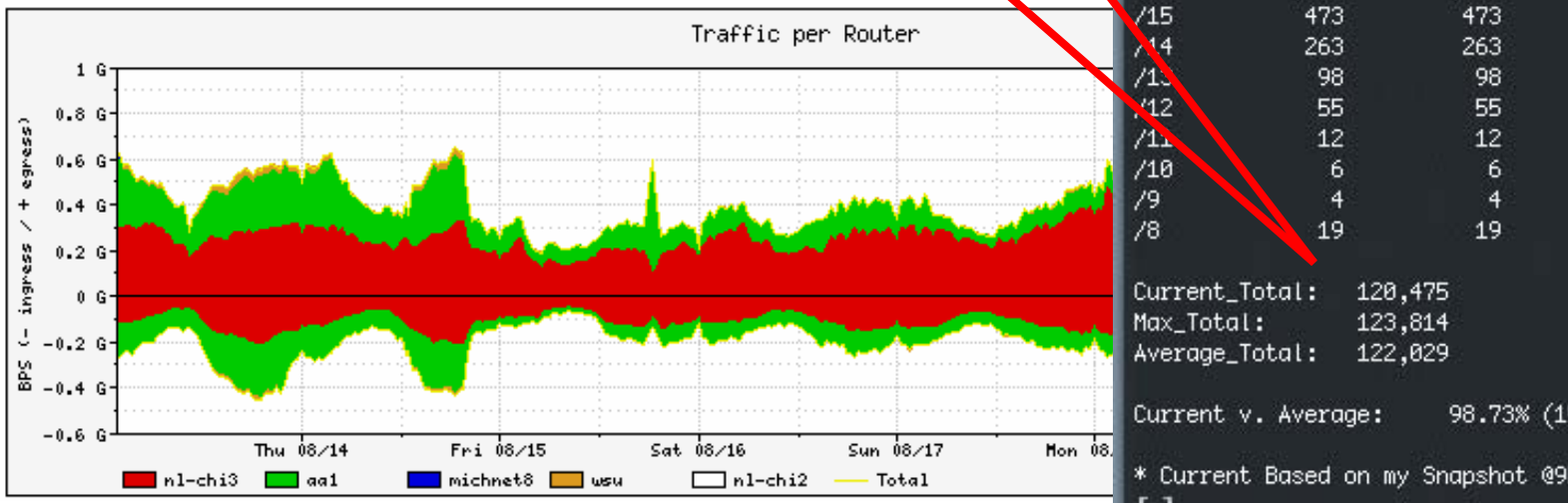
Detailed Analysis i.e. TTL

BGP Example—SQL Slammer



Correlating NetFlow and Routing Data

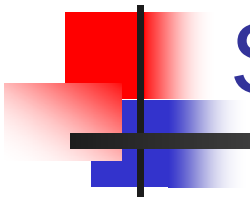




Matching data collected from different tools

tcsh — tcsh

```
donny@rambler% cat prefixes

Prefix                Daily       Daily
Length   *Current     Max         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
[~]
donny@rambler%
```



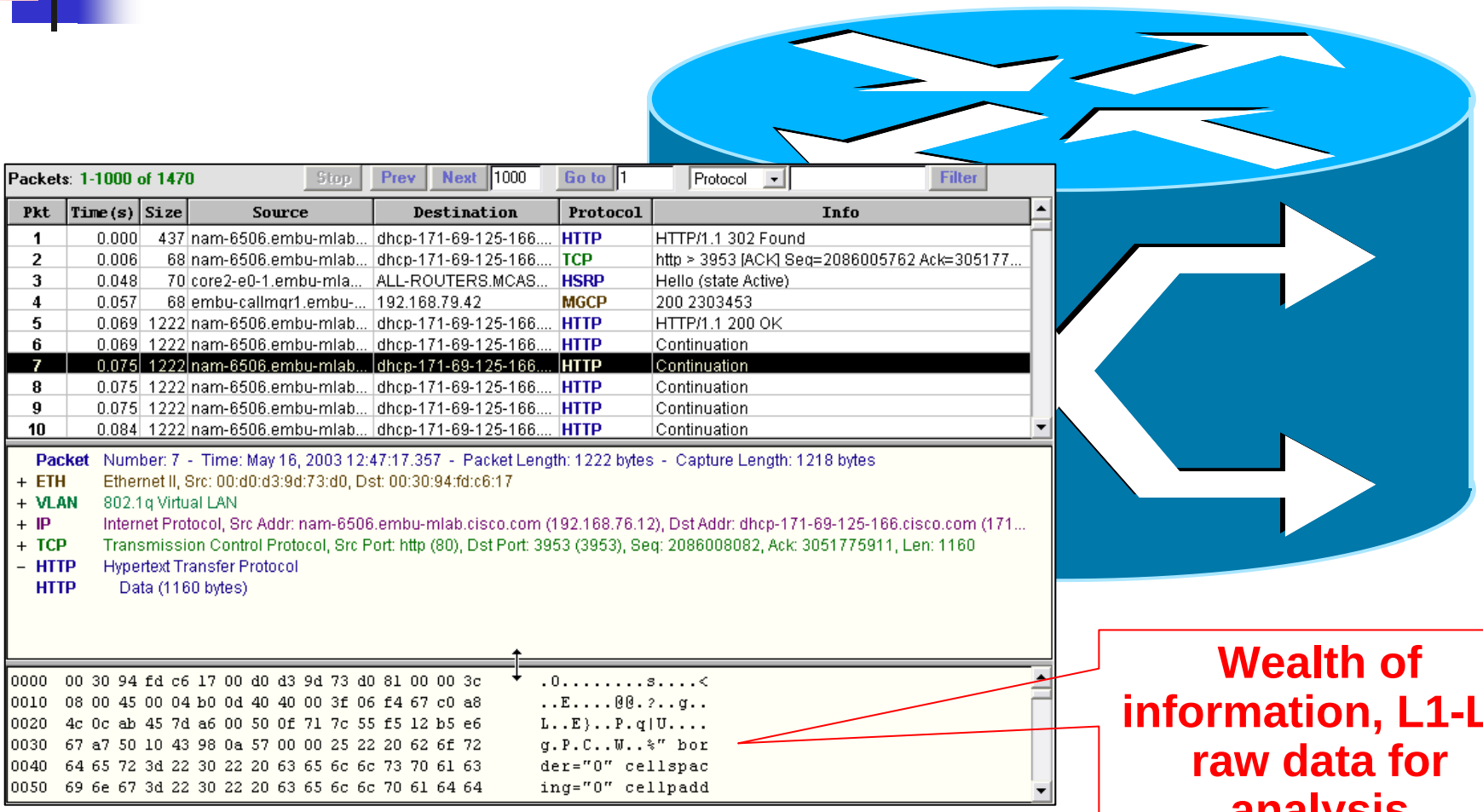
Syslog

- 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 | Stop | Prev | Next | 1000 | Go to | 1 | Protocol | Filter

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

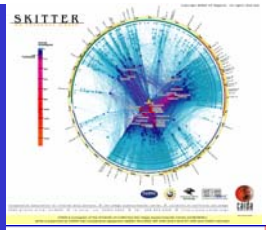
```
  Packet  Number: 7 - Time: May 16, 2003 12:47:17.357 - Packet Length: 1222 bytes - Capture Length: 1218 bytes
+ ETH     Ethernet II, Src: 00:d0:d3:9d:73:d0, Dst: 00:30:94:fd:c6:17
+ VLAN    802.1q Virtual LAN
+ IP      Internet Protocol, Src Addr: nam-6506.embu-mlab.cisco.com (192.168.76.12), Dst 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)
```

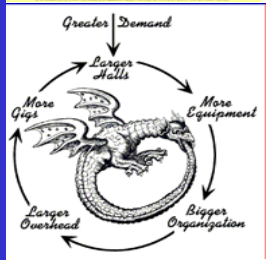
```
0000  00 30 94 fd c6 17 00 d0 d3 9d 73 d0 81 00 00 3c   .0........s....<
0010  08 00 45 00 04 b0 0d 40 40 00 3f 06 f4 67 c0 a8   ..E....@@.?..g..
0020  4c 0c ab 45 7d a6 00 50 0f 71 7c 55 f5 12 b5 e6   L..E}..P.q|U....
0030  67 a7 50 10 43 98 0a 57 00 00 25 22 20 62 6f 72   g.P.C..W..%" bor
0040  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
```

Wealth of information, L1-L7 raw data for analysis

Source: http://www.ethereal.com, Cisco Systems, Inc.

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.

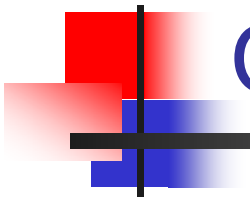
- Be prepared ! Define what to do & whom to contact for various incidents.

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

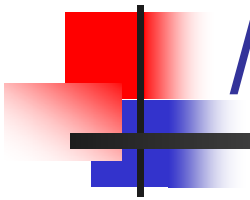
Q. Have you registered you NOC information at one of the NOC Coordination Pages?

- 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:

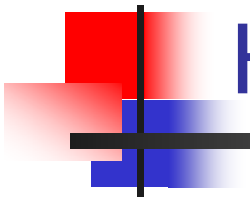
Information from Computer Associates: http://www3.ca.com/solutions/collateral.asp?CT=27081&CID=46275
Information from F-Secure: http://www.europe.f-secure.com/v-descs/sobig_e.shtml
Information from McAfee: http://vil.mcafee.com/dispVirus.asp?virus_k=100429
Information from Norman: http://www.norman.com/virus_info/w32_sobig_e_mm.shtml
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!

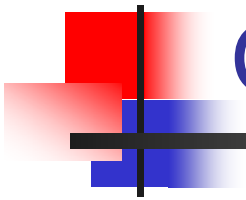
Slide 141

BRG1 Recommended

Any SP who isung IP as business should invest. It is essentials.

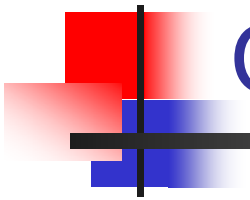
Sales tool.

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.

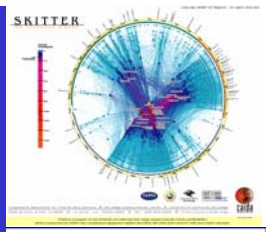
Hardware Vendor's Responsibilities

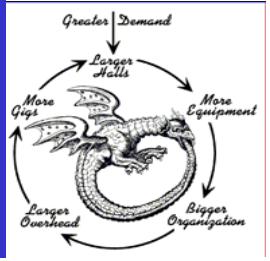
The roll of the hardware vendor is to support the network's objectives. Hence, there is a very synergistic relationship between the SP and the hardware vendor to insure the network is resistant to security compromises

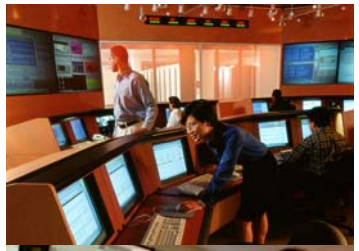
What you should expect from your vendor?

- 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

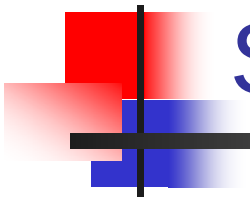
- Cisco SNMP Object Tracker—http://www.cisco.com/pcgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4
- Cisco MIBs and Trap Definitions—http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- SNMPLink—http://www.snmplink.org/
- SEC-1101/2102 give which SNMP parameters should be looked at.

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

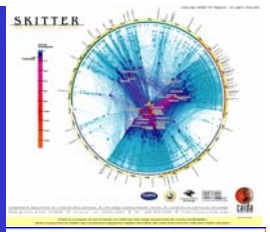
Remote Triggered Black Hole

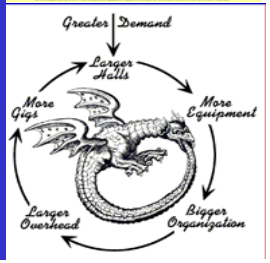
- Remote Triggered Black Hole filtering is the foundation for a whole series of techniques to traceback and react to DOS/DDOS attacks on an ISP's network.
- Preparation does not effect ISP operations or performance.
- It does adds the option to an ISP's *security toolkit.*

More Netflow Tools

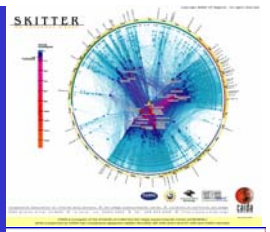
- **NfSen - Netflow Sensor**
  - http://nfsen.sourceforge.net/
- **NFDUMP**
  - http://nfdump.sourceforge.net/
- FlowCon
  - http://www.cert.org/flocon/

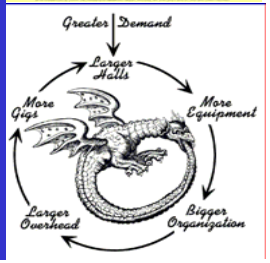
DNS Addendum



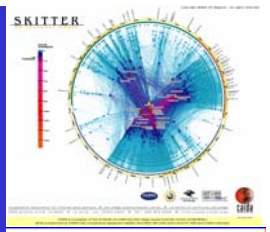


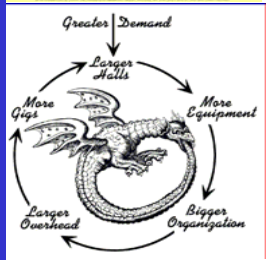
NTP Addendum





BOTNET Control Channel





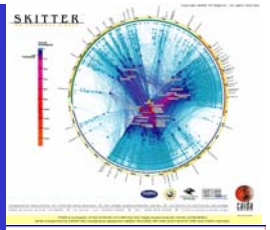
SITREP

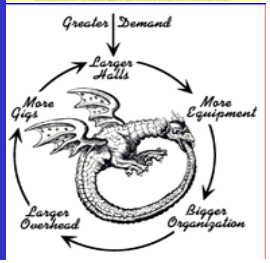
- An NSP-SEC Member has identified the IRC control channel for a BOTNET.
- The Control Channel has a primary BOTNET controller.
- The request is sent out to black hole the controller.

Process

- Step 1 – Validate the information.
- Step 2 – BGP Shunt the IP address to a sink hole prepared to get details on the BOTNET.
- Step 3 – Collect Data from the BOTNET on host inside your network.
- Step 4 – Use the data from your Sink Hole to get a list of your customers.
- Step 5 – Remediate your customers who have victimized – monitor for more violated computers trying to connect.

BOTNET Systems





Cyber Criminal's Goal

- Build a BOTNET that can be used for:
  - DDOS
  - Credit Card Harvesting (Phishing)
  - E-mail collection (SPAM)
  - Key Stroke Logging
  - Breaking into organizations, governments, and other institutions.

But what about Anti Virus?

AV engine	Country	Signature
Ahnlab	KR	no_virus
Aladdin (esafe)	IL	no_virus
Alwil (avast)	CZ	no_virus
Authentium	US	no_virus
Avira (antivir)	DE	HEUR/Crypted
BitDefender	RO	no_virus
CA (E-Trust Ino)	US	no_virus
CA (E-Trust Vet)	US	no_virus
CAT (quickheal)	IN	no_virus
ClamAV		Trojan.Crypted-4
Dr. Web	RU	no_virus
Eset (nod32)	US	no_virus
Ewido	DE	no_virus
Fortinet	US	no_virus
Frisk (f-prot)	IS	no_virus
Frisk (f-prot4)	IS	no_virus
F-Secure	FI	Hupigon.gen130
Grisoft (avg)	CZ	no_virus
Ikarus	AT	Backdoor.VB.EV
Kaspersky	RU	no_virus
Mcafee	US	no_virus
Microsoft	US	no_virus
Norman	NO	Hupigon.gen130
Panda	ES	no_virus
Prevx	GB	no_virus
Securecomputing (webwasher)	US	Heuristic.Crypted
Sophos	GB	no_virus
Sunbelt	US	VIPRE.Suspicious
Symantec	US	no_virus
TheHacker	PE	no_virus
UNA	UA	no_virus
VirusBlokAda (vba32)	BY	no_virus

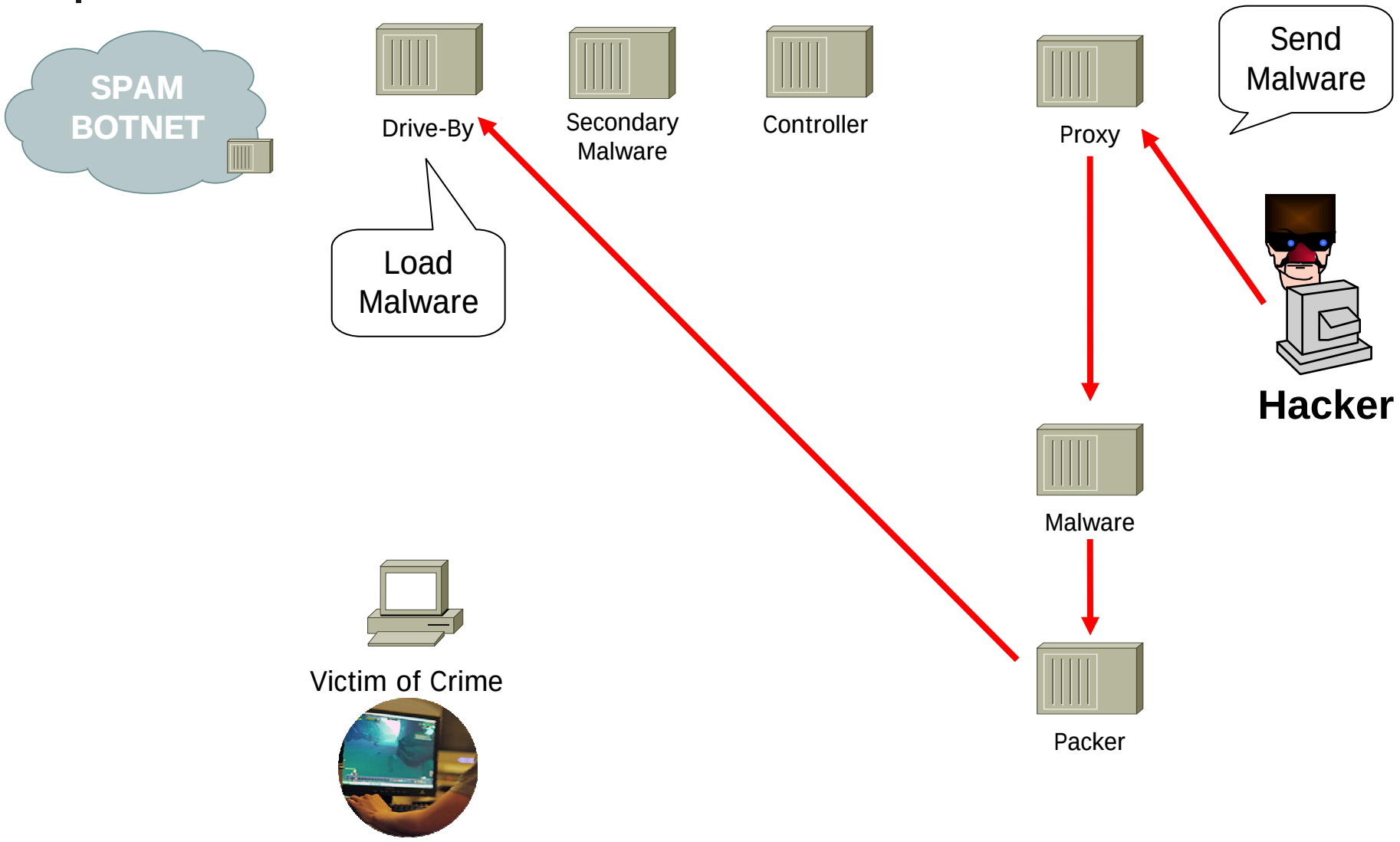
- Packing Tools allow the Cyber-Criminal to change the signature of the malware every hour on the hour.
- This bypasses the anti-virus software.

What packers are used?

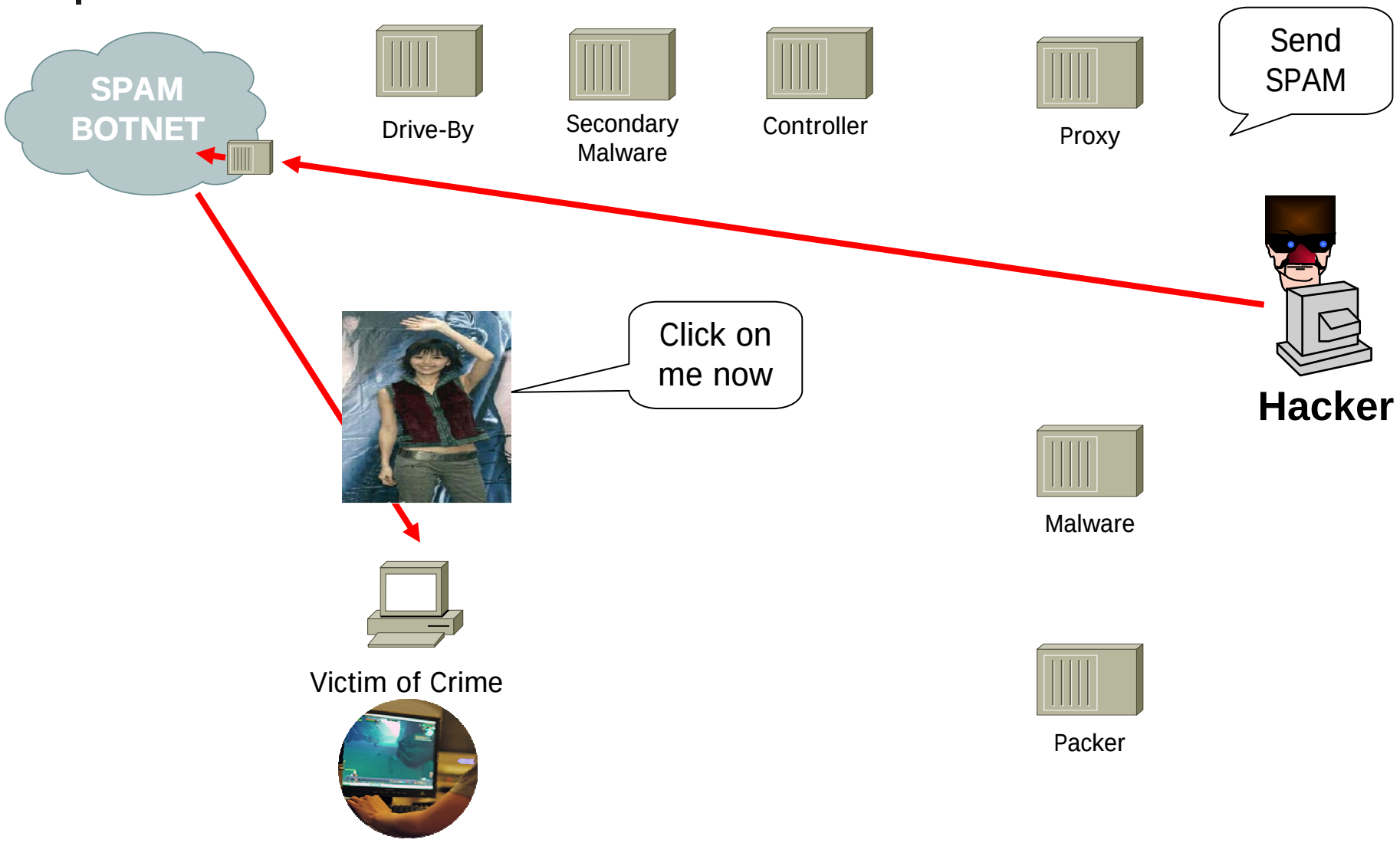
packer	md5count	percent
MEW v11SEv1.2	2,750,638	74.9659
UPX All_Versions	873,744	23.8130
Allaple_Polymorphic_Packer vna	23,647	0.6445
ASPack v2.1	5,248	0.1430
ASPack v2.12	2,263	0.0617
PE_Compact v2.X	1,554	0.0424
NullSoft_NSIS Generic	1,082	0.0295
Armadillo v1.xx-v2.xx	1,058	0.0288
Themida vna	969	0.0264
FSG V1.3x	883	0.0241

Provided by shadowserver.org

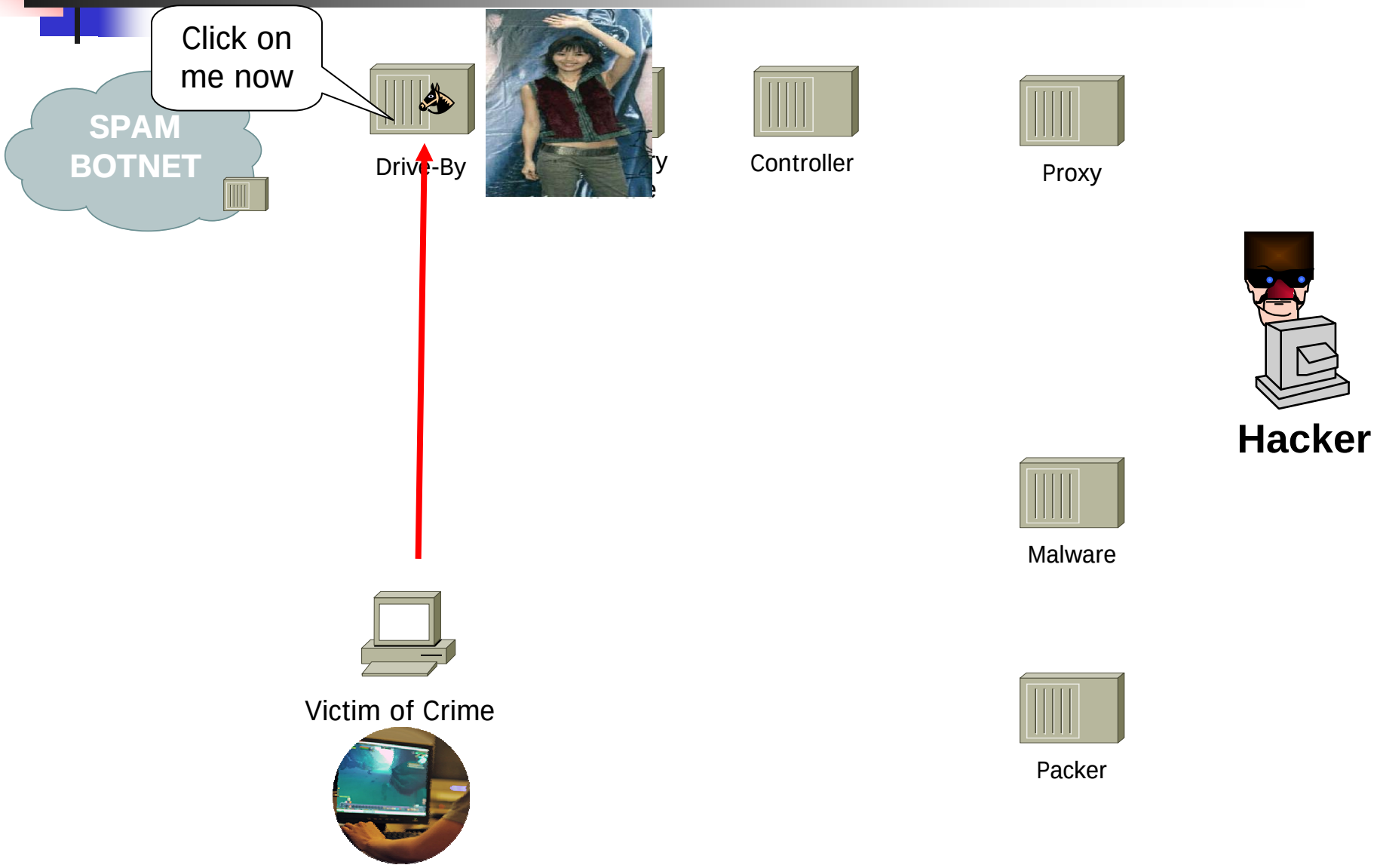
Prepare Drive-by



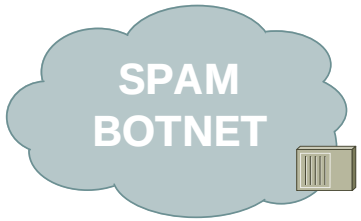
Send SPAM to get People To Click

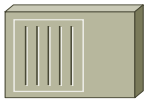


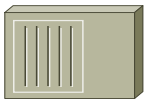
Drive By Violation

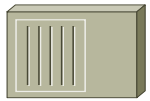


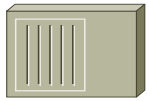
Poison Anti-Virus Updates

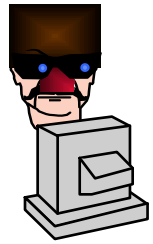


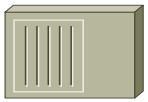

Drive-By

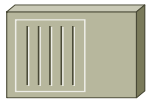

Secondary Malware


Controller

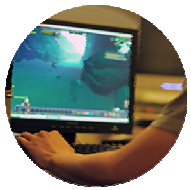

Proxy


Hacker


Anti-Virus Vendor

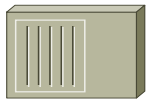

Malware


Victim of Crime

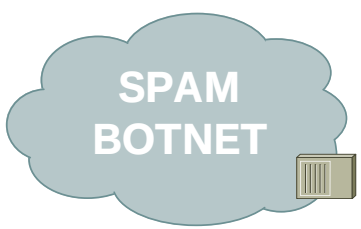


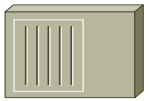
Poison the anti-virus updates

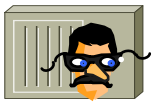
All updates to 127.0.0.1

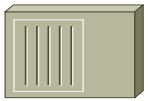

Packer

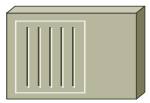
Prepare Violated Computer

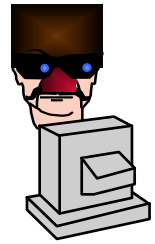


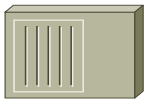

Drive-By

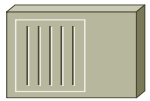

Secondary
Malware


Controller


Proxy


Hacker

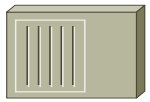

Anti-Virus
Vendor


Malware


Victim of Crime

Call to Secondary
Malware Site

Load Secondary Package


Packer

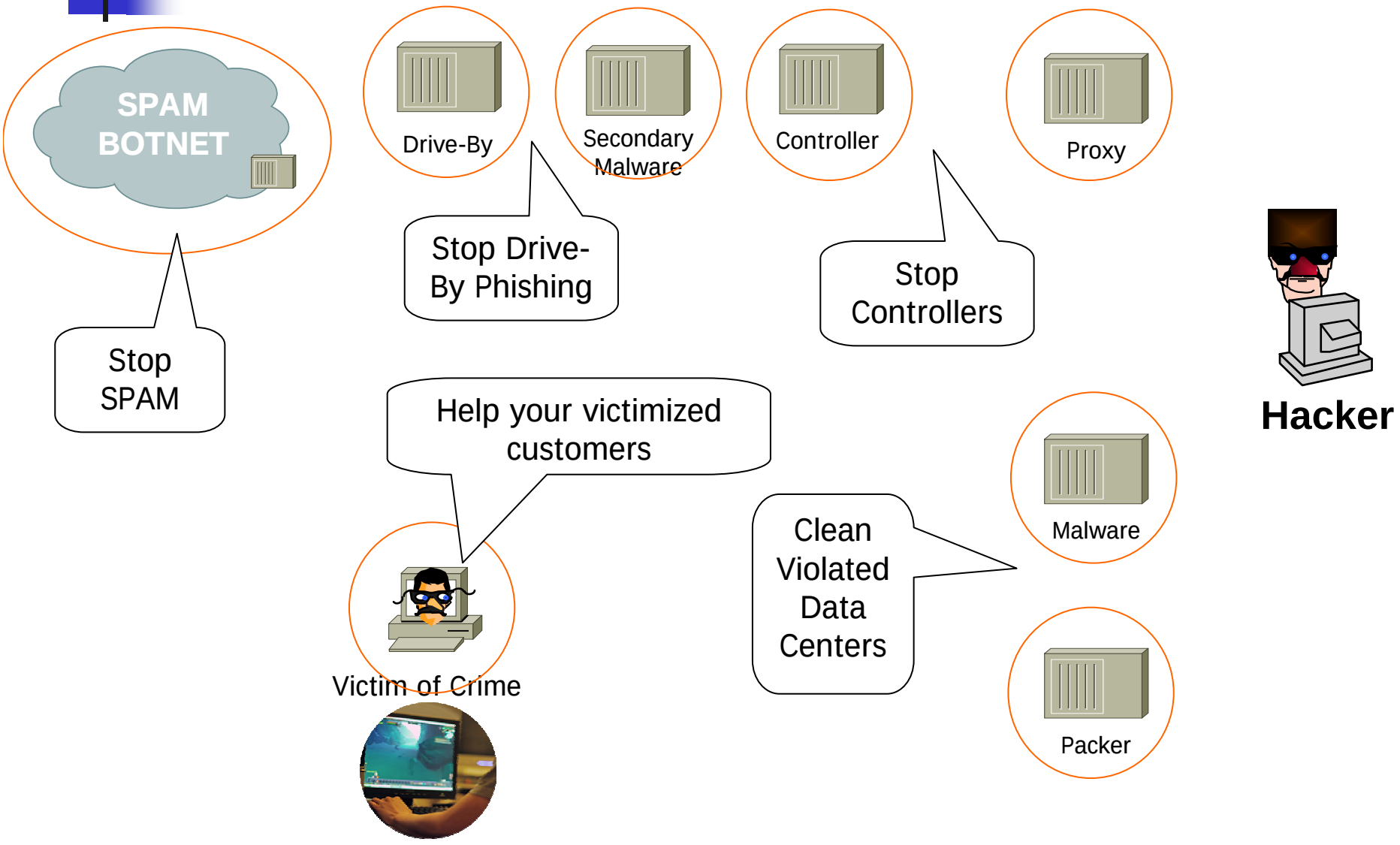
Call Home


SPAM BOTNET
Drive-By
Secondary Malware
Controller
Proxy
Hacker
Call to Controller
Report:
Operating System
Anti-virus
Location on the Net
Software
Patch Level
Bandwidth
Capacity of the computer
Malware
Packer
Victim of Crime

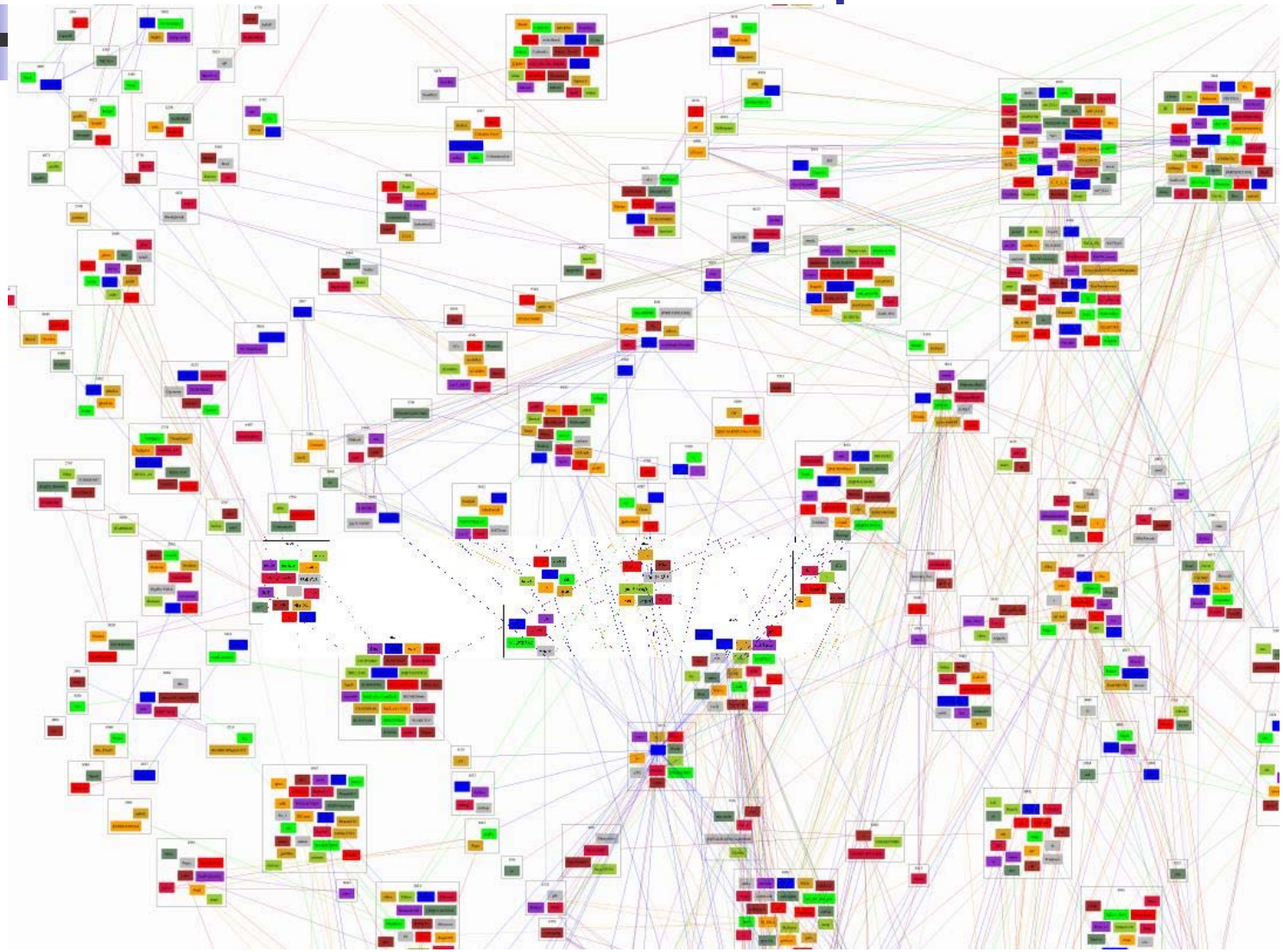
BOTHERDer – Next Steps

- Analyze the results of the BOTNET Run.
  - Look for types of systems.
  - Look for where the systems are located.
- Group the Systems into Sellable Modules
  - SPAM Systems
  - DDOS Systems
  - Phishing Systems
  - Fast Flux Systems
  - Grouped by Domains - .mil, .gov, banks, companies, & other institutions.

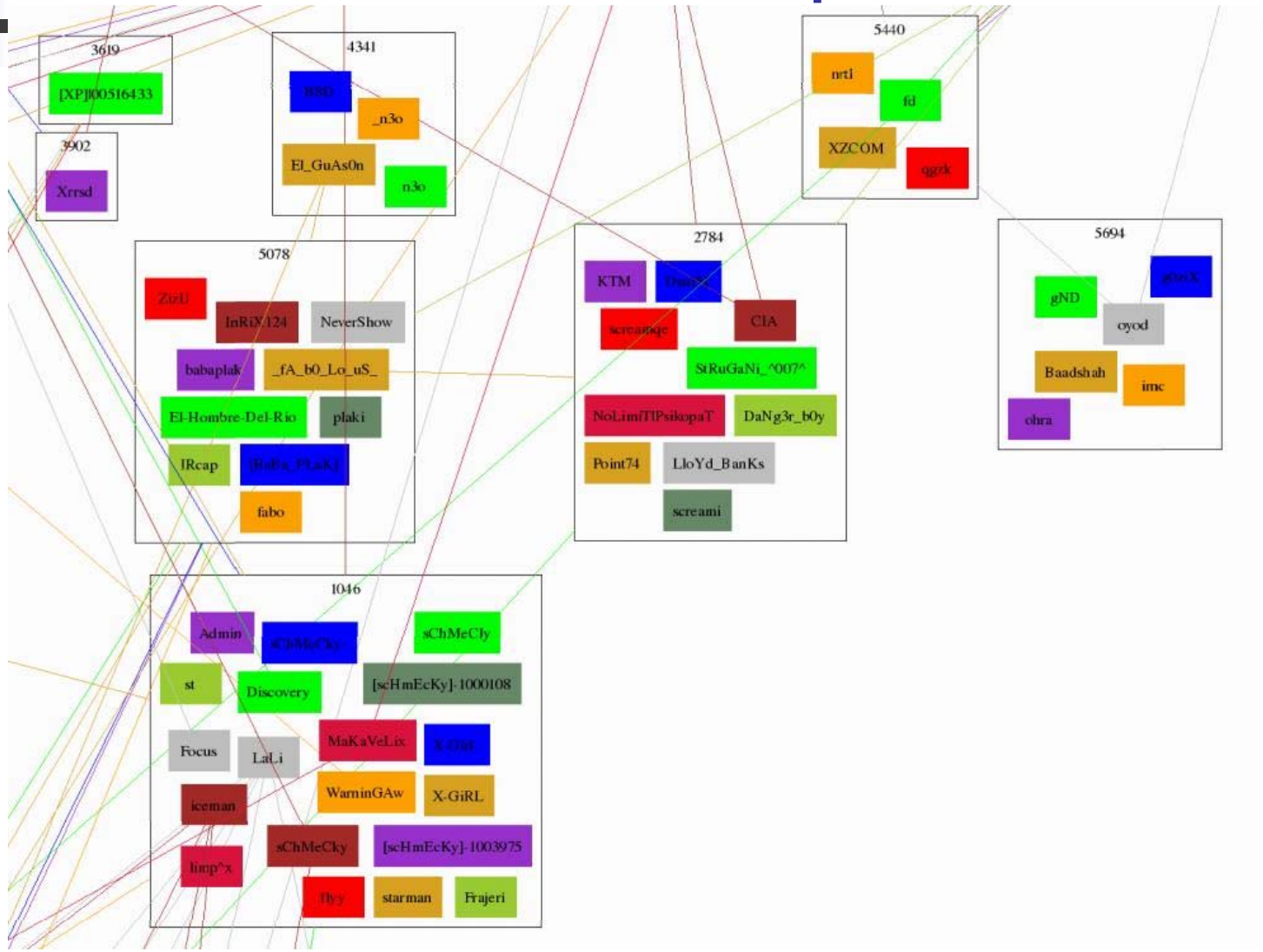
What can SPs do?



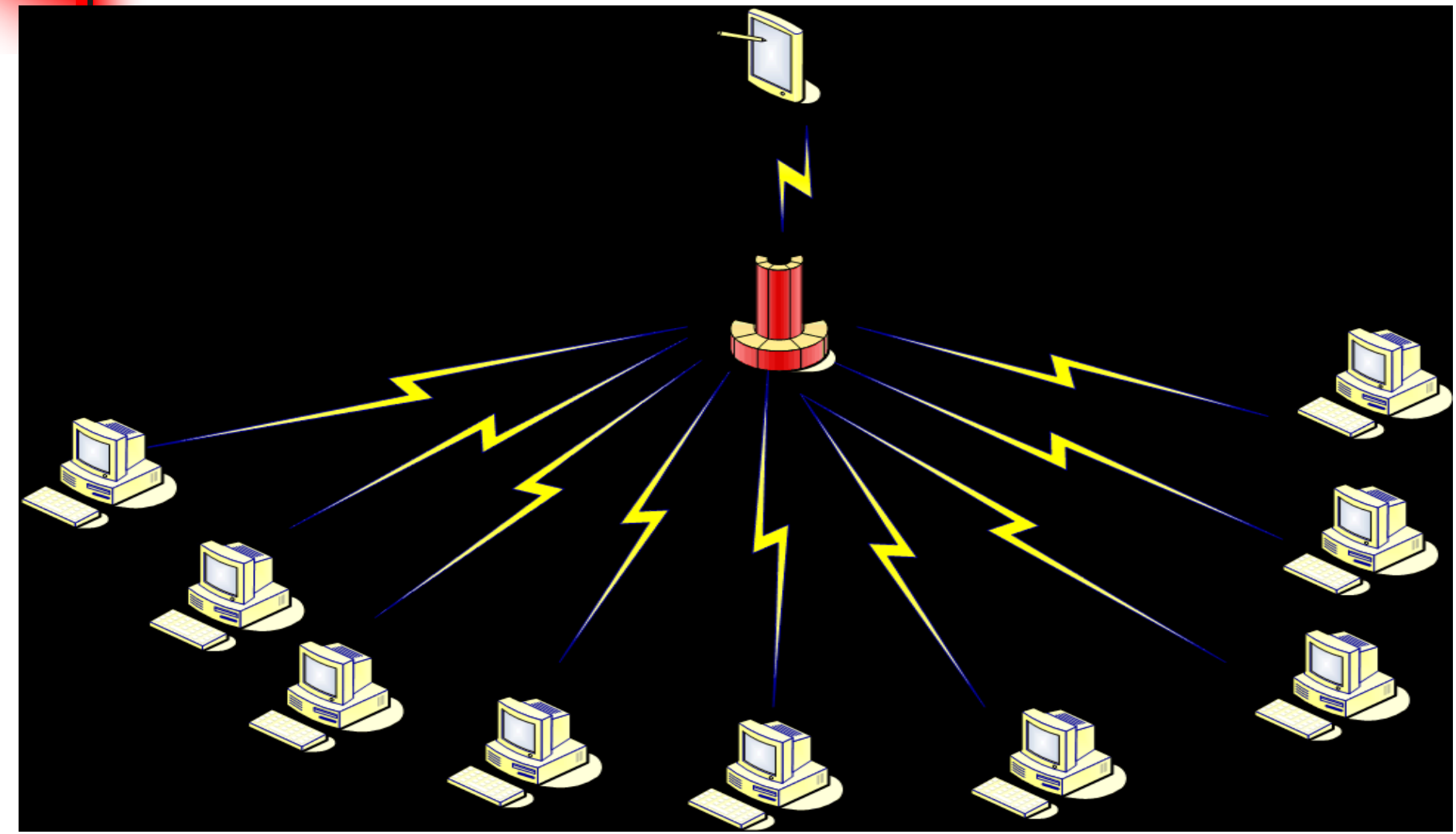
Botnets - Relationships



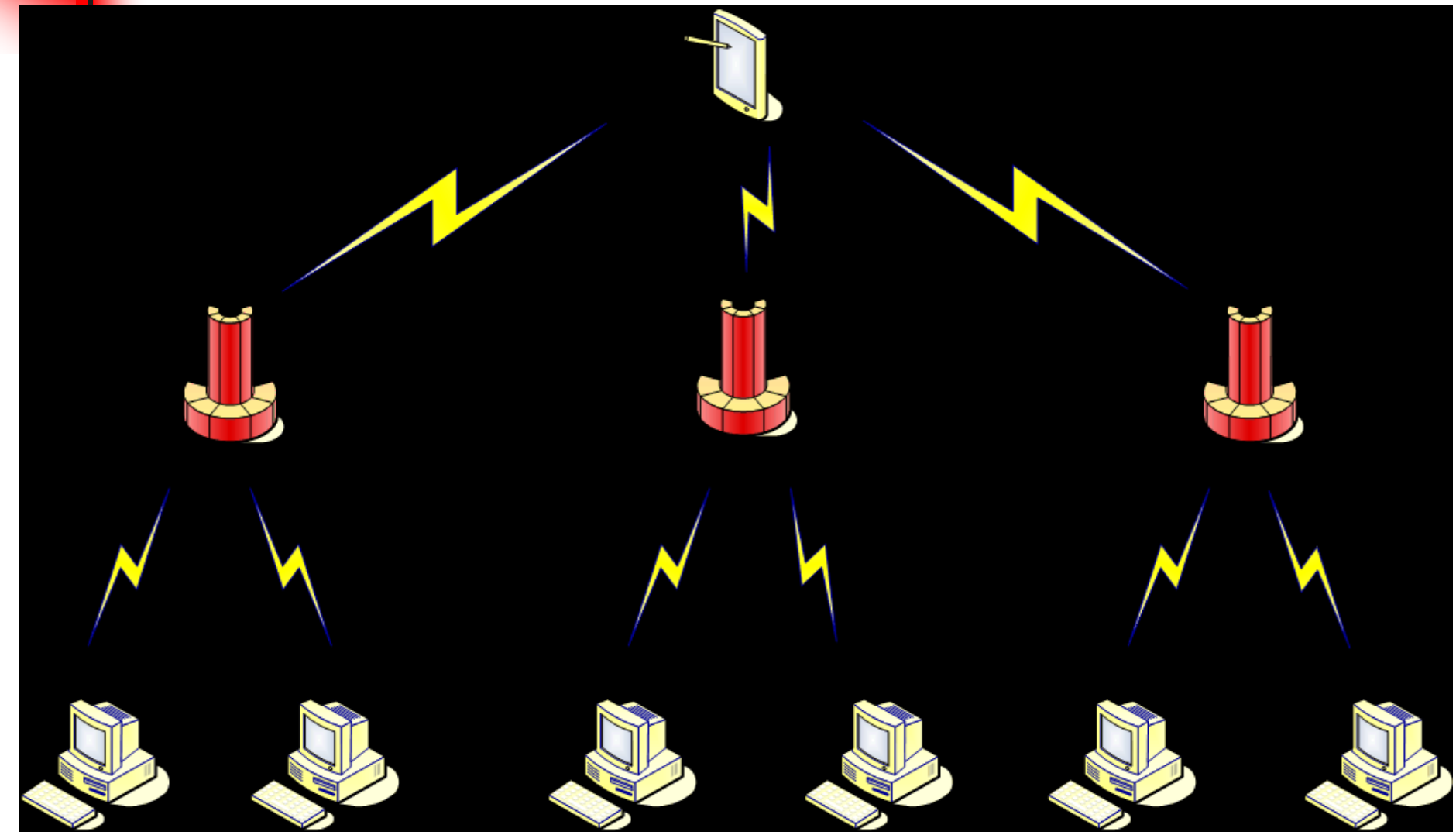
Botnets - Relationships



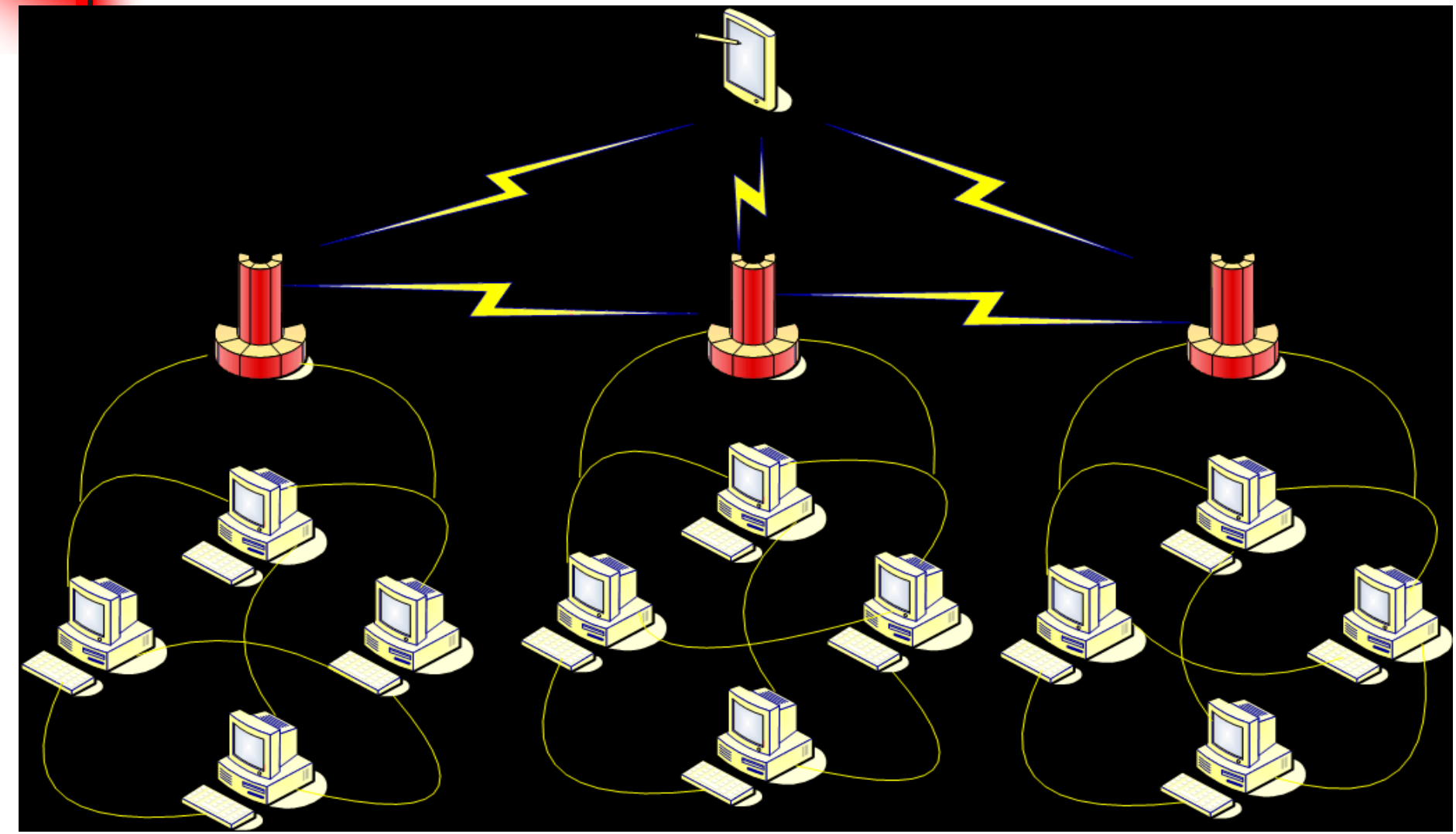
Botnet – Centralized IRC



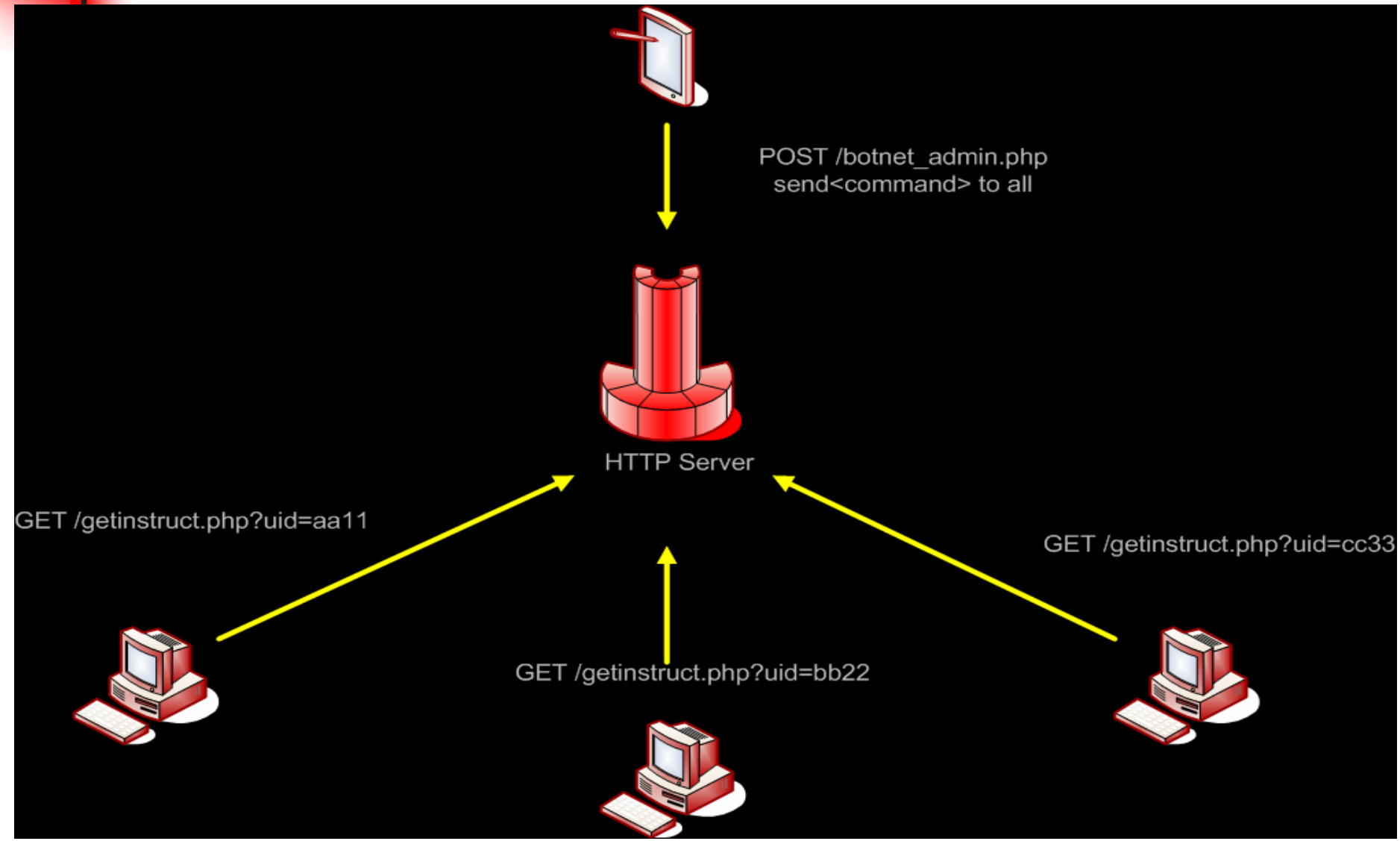
Botnet - Distributed



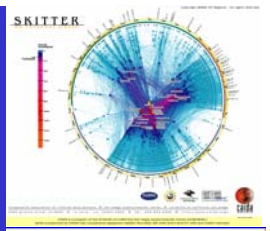
Botnet – Peer-to-Peer

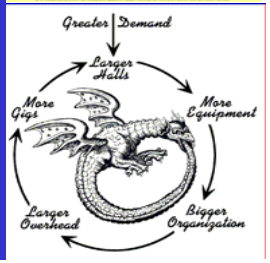


HTTP Botnet


POST /botnet_admin.php
send<command> to all
HTTP Server
GET /getinstruct.php?uid=aa11
GET /getinstruct.php?uid=bb22
GET /getinstruct.php?uid=cc33

Real Security World Concerns

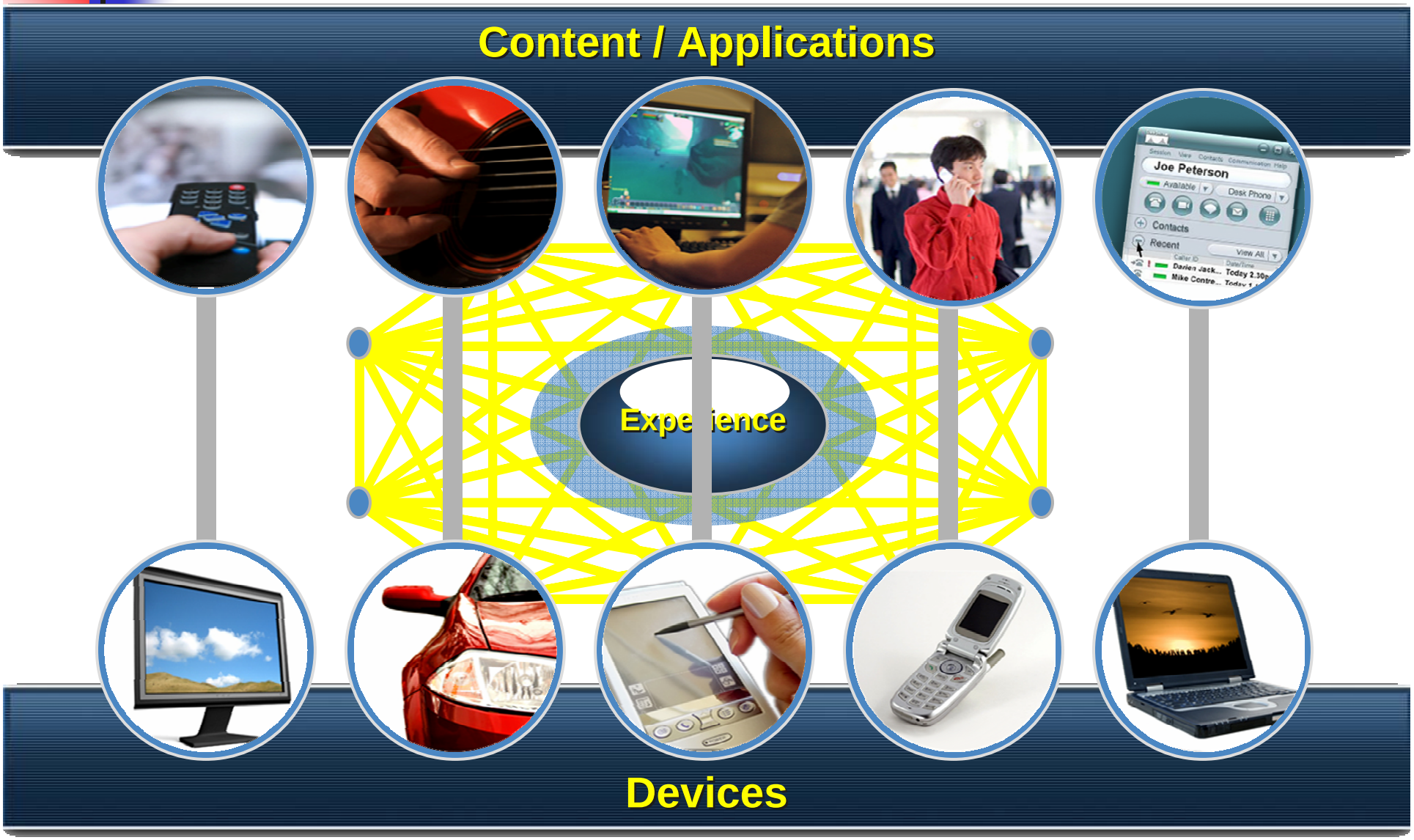




IP NGN has Won!

- Converged NGN Infrastructure – where all telecommunications services work over the same common infrastructure – is a 30 year dream now a reality.
- It is time to face the consequences of Cisco & Juniper push to make End-to-End, Paul Baran, model of TCP/IP based convergence *the* IP NGN.

IP NGN *Experience* Message .....

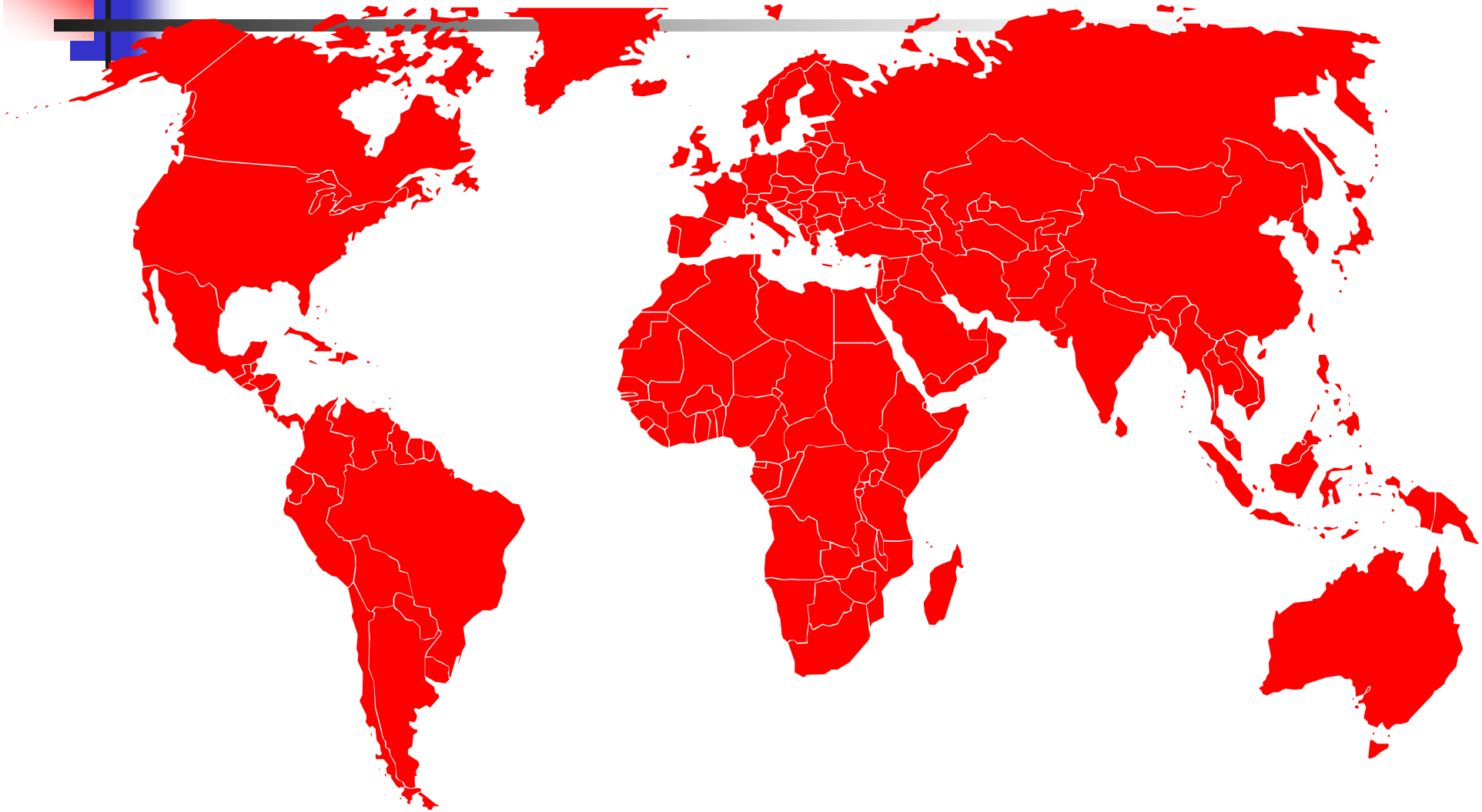


What happens when it stops working?

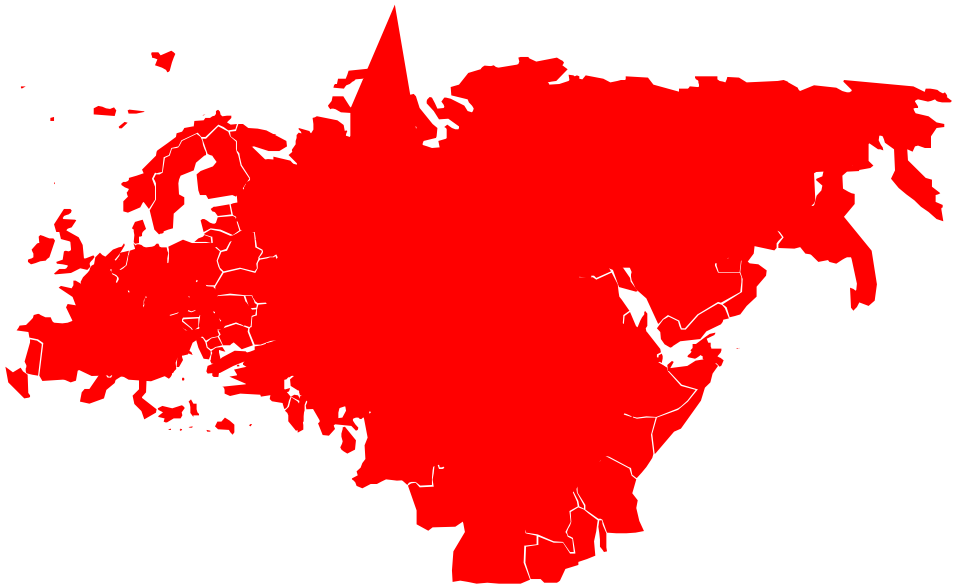
Core Principle of Mountain Climbing

- Trust your equipment – you life depends on it!
- Do you trust your equipment with your life?
- There is no other option. We're converging on IP NGN – there is no other alternative, backup plan, or alternate path.
- How is that changing things?

Our Traditional View of the World



The Reality of IP NGN – No Borders



How to project civic society and the rule of law
where there is no way to enforce the law?

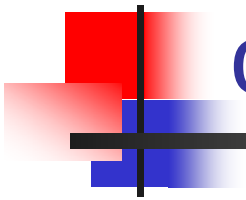
Services in a Hostile Environment

Goal: Service work - No Help Desk Calls!

SLAs are Critical to Measure Security Success!

- Delay
- Jitter
- Bandwidth
- Availability
- Packet Loss
- Out of Sequence (OoS)
- [add your favourite here]

What is ‘real’ is really hard to figure out

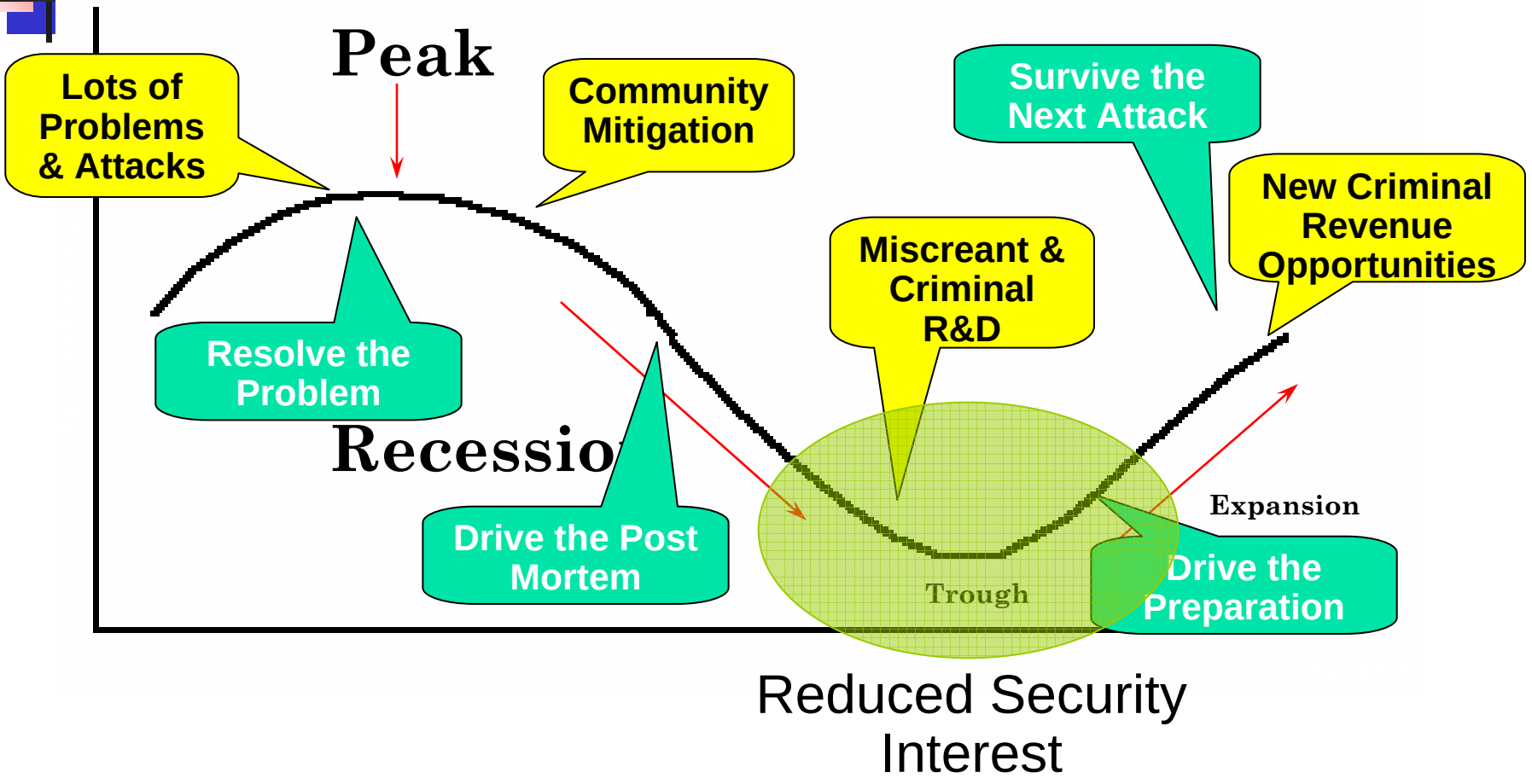


- *Trade Press* wants to sell advertisement
- *Security Pundits* likes to be visible
- *Vendors* are looking to sell their product
- *Governments* are looking for justification and increased funding and span of power
- *Researchers* are working to wow people with their work to get more grand money.
- Vulnerability Clearing Houses are trying to get people to pay attention – while getting paid to reprocess information.

The Security Trap

- If you do your Security Job well ....
  - “What are you doing and why am I spending all the money on security?”
- If you do not do you Security Job well ...
  - “Why didn’t you do something to keep this from happening!?!”

Criminal - Incident Economic Cycles



Under the Threshold

- We've done a good job keeping Networks Up and Running – the Criminals Now know the *pain threshold.*
- Consequence:
  1. Executive Management in SPs are not interested in continued investment
  2. Expertise getting reassigned off SP Security Work
  3. Criminals have bypassed traditional security prevention techniques (anti-virus) and are keeping "under the threshold" of pain.
  4. Vendors are not hearing about "SP Security" from any of their RFP negotiations (i.e. Cisco and Juniper). Vendor Product Management is not making new SP Security innovation a priority.

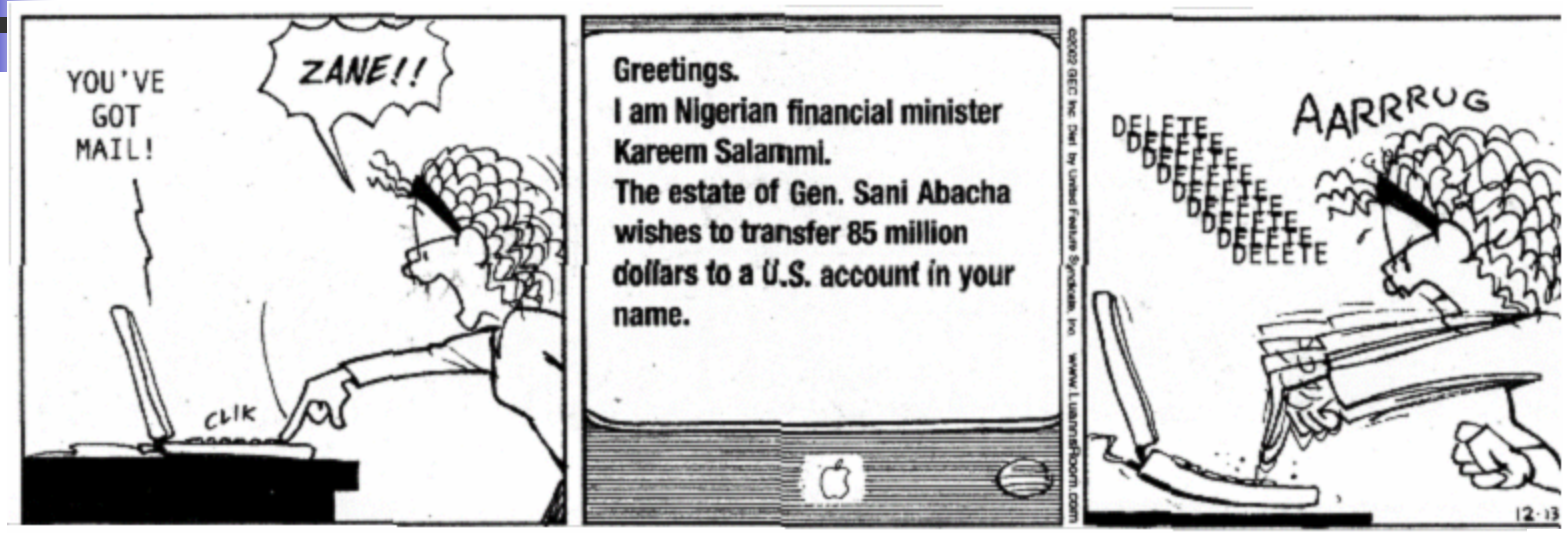
Wrong Type of Security …

- Estonia – Press is being used for little understood *agendas*.
- *China is spying* on me is not about China.
- Too many people are asking the wrong "security" questions ... hence working on the wrong security problems.
- All the regulation, standards, and "I want to help with DDOS" work is dragging us down.

Is the Industry Ready – Post Estonia Attack?

- The Estonia attacks broke principle #3 – never do anything unless there is money to be gained.
- The game has changed.
- “Tom Clancy” multi-vector attacks are now going to happen.
  - Use Cyber Disruption coordinated with physical attacks to exacerbate the impact of terror.
- What happens when 911 calls are not working over “converged” IP equipment which is not ready for this sort stress?

Summer 2007 – Social Engineering - Art



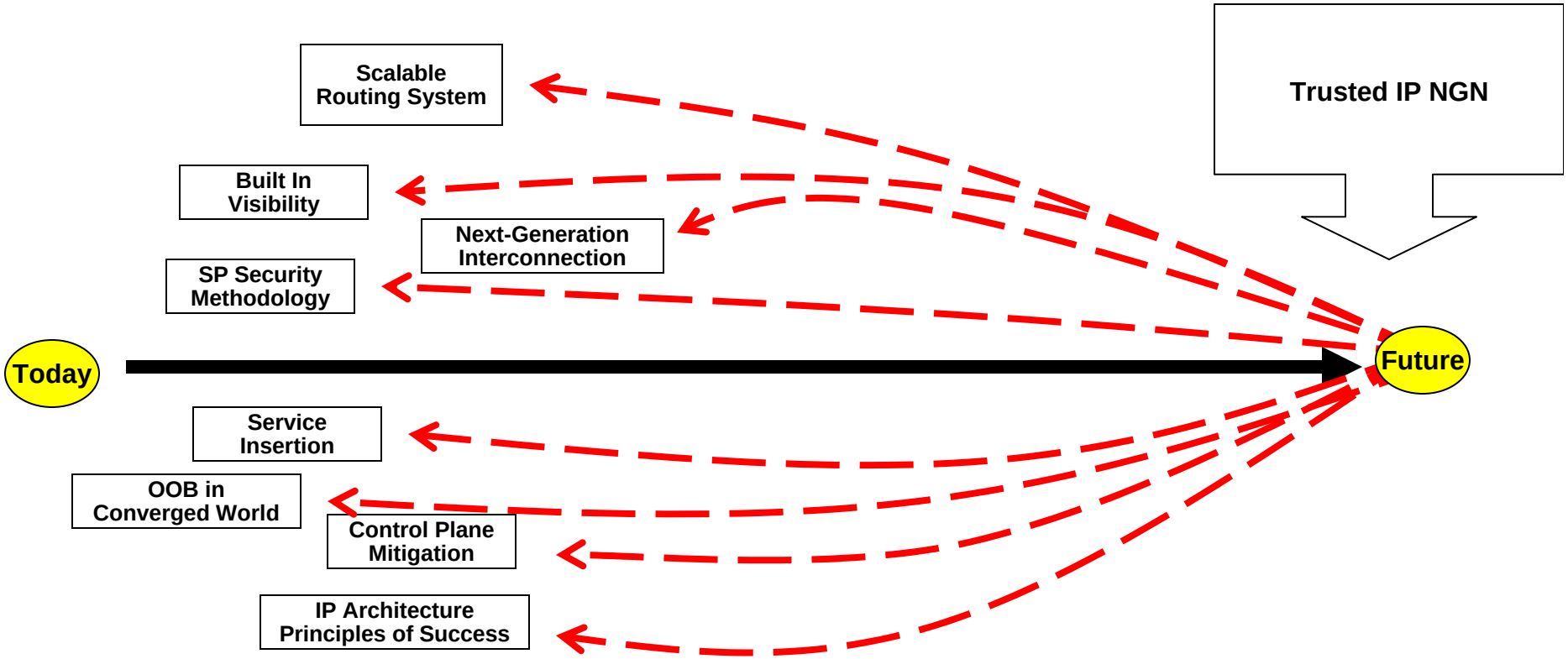
- As long as there are people out there who "click here," there will be crime on the Internet.
- The Summer of 2007 saw a polishing of the criminal's use of professional advertising techniques to get people to "click here."
- So the Criminal Economy is here to stay.

But I have Anti-Virus!

AV engine	Country	Signature
Ahnlab	KR	no_virus
Aladdin (esafe)	IL	no_virus
Alwil (avast)	CZ	no_virus
Authentium	US	no_virus
Avira (antivir)	DE	HEUR/Crypted
BitDefender	RO	no_virus
CA (E-Trust Ino)	US	no_virus
CA (E-Trust Vet)	US	no_virus
CAT (quickheal)	IN	no_virus
ClamAV		Trojan.Crypted-4
Dr. Web	RU	no_virus
Eset (nod32)	US	no_virus
Ewido	DE	no_virus
Fortinet	US	no_virus
Frisk (f-prot)	IS	no_virus
Frisk (f-prot4)	IS	no_virus
F-Secure	FI	Hupigon.gen130
Grisoft (avg)	CZ	no_virus
Ikarus	AT	Backdoor.VB.EV
Kaspersky	RU	no_virus
Mcafee	US	no_virus
Microsoft	US	no_virus
Norman	NO	Hupigon.gen130
Panda	ES	no_virus
Prevx	GB	no_virus
Securecomputing (webwasher)	US	Heuristic.Crypted
Sophos	GB	no_virus
Sunbelt	US	VIPRE.Suspicious
Symantec	US	no_virus
TheHacker	PE	no_virus
UNA	UA	no_virus
VirusBlokAda (vba32)	BY	no_virus

- Most new malware is not detectable by Anti-Virus software.
- Those that do, see it as something else – which means it may not be blocked.

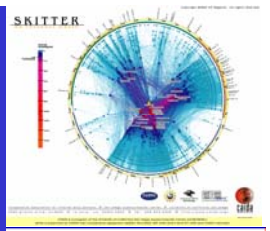
Projection Forward – Looking Back

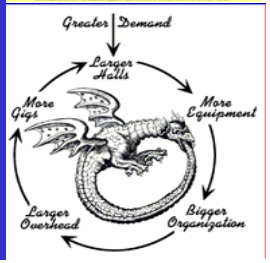


Principled Based Approach

- A principle based approach to engineering, execution, and development is a new approach to shaping our engineering direction. We will evolve, define, articulate, and execute core principles which govern the converged IP centered telecommunications community. The principles act as a compass for SP Business and Engineering direction.

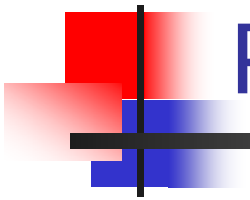
UPDATED PRINCIPLES OF THE MISCREANTS





Essential Principles

- There are key essential principles to a successful miscreant (i.e. cyber criminal).
- These principles need to be understood by SP Security professionals.
- Understanding allows one to cut to the core concerns during security incidents.
- Attacking the dynamics behind these principles are the core ways we have to attempt a disruption of the Miscreant Economy.



Principles

1. Don’t Get Caught
2. Don’t work too hard
3. Follow the money
4. If you cannot take out the target, move the attack to a coupled dependency of the target.
5. Always build cross jurisdictional attack vectors
6. Attack people who will not prosecute
7. Stay below the pain threshold

Principle 1: Do Not Get Caught!

- The first principle is the most important. It is no fun getting caught, prosecuted, and throw in jail.
  - (or in organized crime – getting killed).
- All threat vectors used by a miscreant will have an element of un-traceability to the source.
- If it can be traced, it is one of three things:
  1. A violated computer/network resources used by the miscreant.
  2. A distraction to the real action.
  3. A really dumb newbie.

Principle 2: Do not work too hard!

- Use the easiest attack/penetration vector available in the toolkit to achieve the job's objective.
- Example: If your job is to take out a company's Internet access the day of the quarterly number's announcement, would you:
  1. Penetrate the Site and Delete files?
  2. Build a custom worm to create havoc in the company?
  3. DOS the Internet connection?
  4. DOS the SP supporting the connection?

Principle 3: Follow the Money

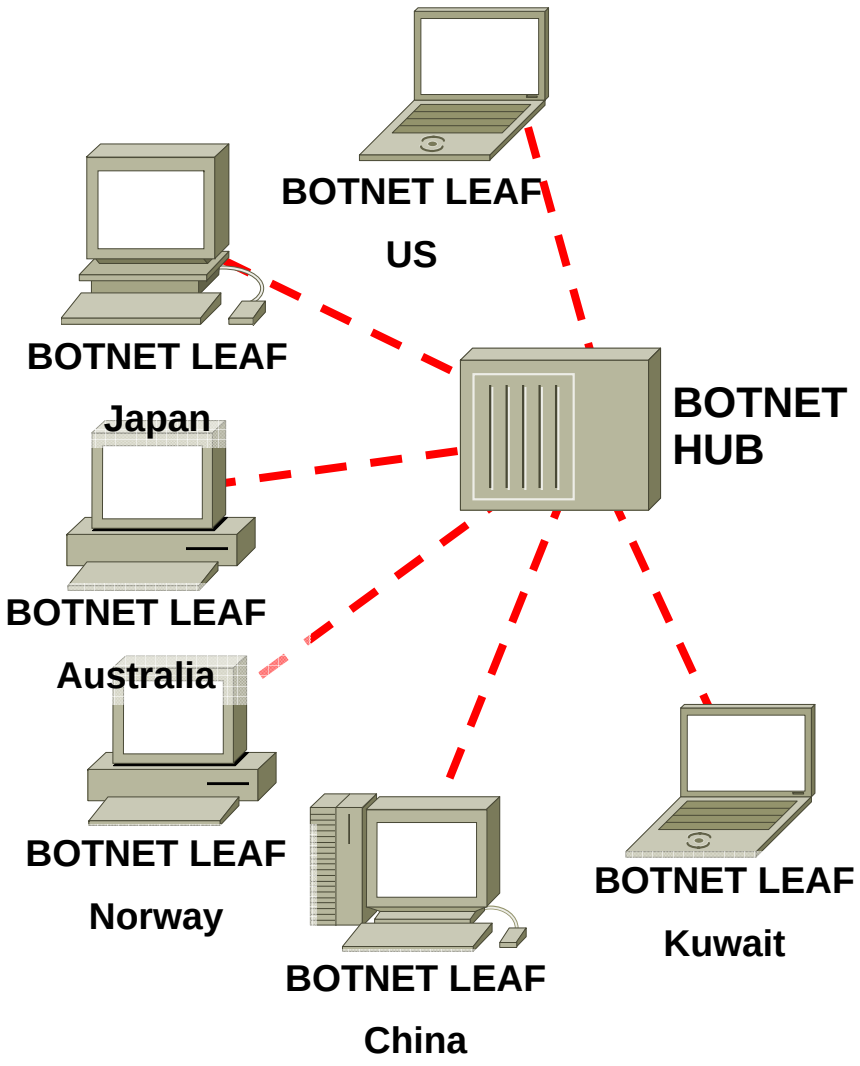
- If there is no money in the crime then it is not worth the effort.
- *Follow the money* is the flow of money or exchanged value as one miscreant transfers value to another miscreant (or the victim transfers value to the criminal).
- A *Miscreant Treat Vector* opens when the miscreant finds a way to move ‘stored value’ from the victim through the economy.
- It is worse if the cyber ‘stored value’ can cross over to normal economic exchange.

Principle 4: If you cannot take out the target ….

- If you cannot take out the target, move the attack to a coupled dependency of the target.
- There are lots of *coupled dependencies* in a system:
  - The target's supporting PE router
  - Control Plane
  - DNS Servers
  - State Devices (Firewalls, IPS, Load Balancers)

Principle 5: Always build cross jurisdictional attack vectors

- Remember – Don't get caught! Do make sure ever thing you do is cross jurisdictional.
- Even better – cross the law systems (Constitutional, Tort, Statutory, Islamic, etc.)



Principle 6: Attack people who will NOT Prosecute

- If your activity is something that would not want everyone around you to know about, then you are a miscreant target.
- Why? Cause when you become a victim, you are not motivated to call the authorities.
- Examples:
  - Someone addicted to gambling is targeted via a Phishing site.
  - Someone addicted to porn is targeted to get botted.
  - Someone addicted to chat is targeted to get botted.
  - Someone new to the Net is targeted and abused on the physical world.
  - Government, Finance, and Defense, Employees – who loose face when they have to call INFOSEC.

Principle 7: Stay below the Pain Threshold

- The *Pain Threshold* is the point where an SP or Law Enforcement would pay attention.
- If you are below the pain threshold – where you do not impact an SP's business, then the SP's Executive Management do not care to act.
- If you are below the pain threshold – where you do not have a lot of people calling the police, then the Law Enforcement and Elected Official do not care to act.
- The Pain Threshold is a matter of QOS, Resource Management, and picking targets which will not trigger action.

Guard Trust

- Miscreants will guardedly trust each other.
- They can be competitors.
- They can be collaborators
- But when there is money on the table, criminal human behavior and greed take over.

Dire Consequences

- The Miscreant Economy is not a joke. It is not a game. It is not something to play with.
  - PEOPLE DIE
- Once organized crime enter the world of the Miscreant Economy, the days of *fun* were over.