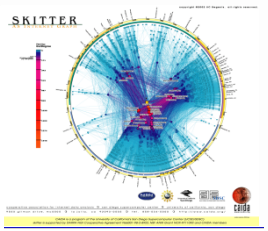
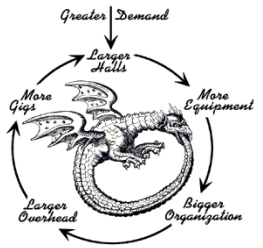
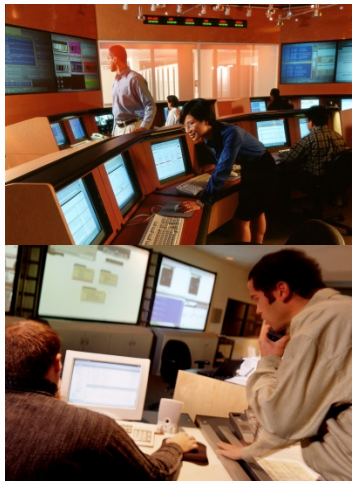
Prepare your NOC







Agenda

1. Need for SOC
2. Defining SOC Architecture
3. Building SOC Team
4. SOC Deliverables

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 (OPSEC) 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 SP's operations!

2) Secure Resources
Firewall, Encryption, Authentication, Audit

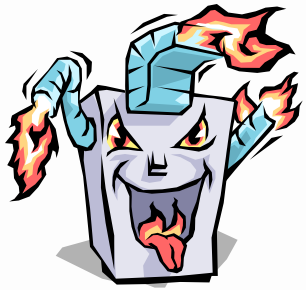
5) Manage and Improve
Post Mortem, Analyze the Incident, modify the plan/ procedures

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

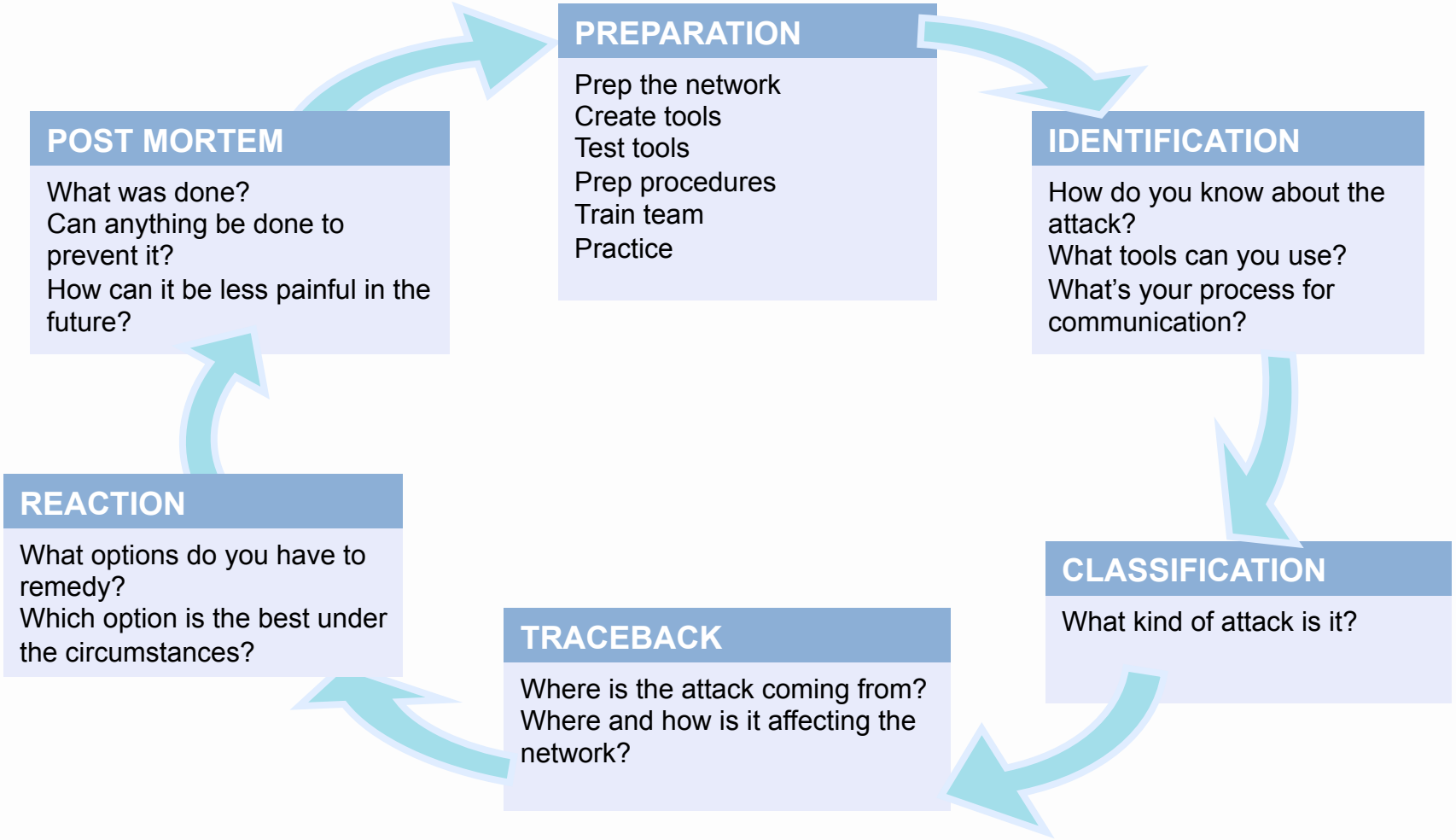
4) Test, Practice, Drill
Vulnerability Scanning

The Preparation Problem

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



Six Phases of Incident Response



Business Drivers to Build SOC

Risk management strategy for infrastructure and services

- **Infrastructure is business for SP**
  - **Risk management of critical information assets**
  - **Allow business continuity**
  - **Avoid disruption to critical services**
- **Revenue generating services**
  - **Prevent loss/contamination of data**
  - **Provide protection against lost or delayed transactions**
  - **Avoid customer service disruption**

Common SOC Functions

- **Security monitoring for risk management**
  - **Security incident detection and mitigation**
- **24x7x365 monitoring and mitigation via Security Information Management System (SIMS) data gathering**
- **Vulnerability Scanning (tactical scanning, targeted scanning and differential scanning)**
- **Security incident analysis to provide evidence with sniffing/data Forensics**
- **Intelligent analysis and correlation on gathered data**
- **Real-time and periodic reports and audits generation**
- **Change management with configuration, patches and such**
- **Protection of intellectual property, asset tracking and recovery**

Benefits

- **Reduce disruption to critical services and business processes**
  - **Reduce Risks and Security Related Downtime**
  - **Service Disruptions**
  - **Information / Data loss or Manipulation**
- **Transition Reactionary Posture to one of Preparedness**
  - **Use Expertise for Strategy Contribution – Not Response**
  - **Planned vs. Unplanned budgets / "voodoo economics" of response**
- **Threat Control and Prevention**
  - **Keep pace with evolving threat landscape**
  - **Assume more Control Fidelity**
- **Free up critical network/IT resources**
- **Maintain accountability and corporate governance**
- **Maintain privacy for employees, partners and customers**
- **Provide situational awareness**

More Benefits

- **NOC/SOC Collaboration**
  - **Operational and Situational Awareness Reporting**
  - **Incremental Security Capabilities Integral with NOC Ops Support**
- **Expert Reduction in "Signal-to-Noise Ratio."**
  - **Focus on Key and Truly Critical Issues**
- **Defined Correlation Rules and Policies -- Policy Management**
- **Central Audit Log Data Repository -- Correlation of Logs**
- **Reporting Capability -- Meaningful Reports**
- **Incident Response to Events -- 0-day Response Time**

Agenda

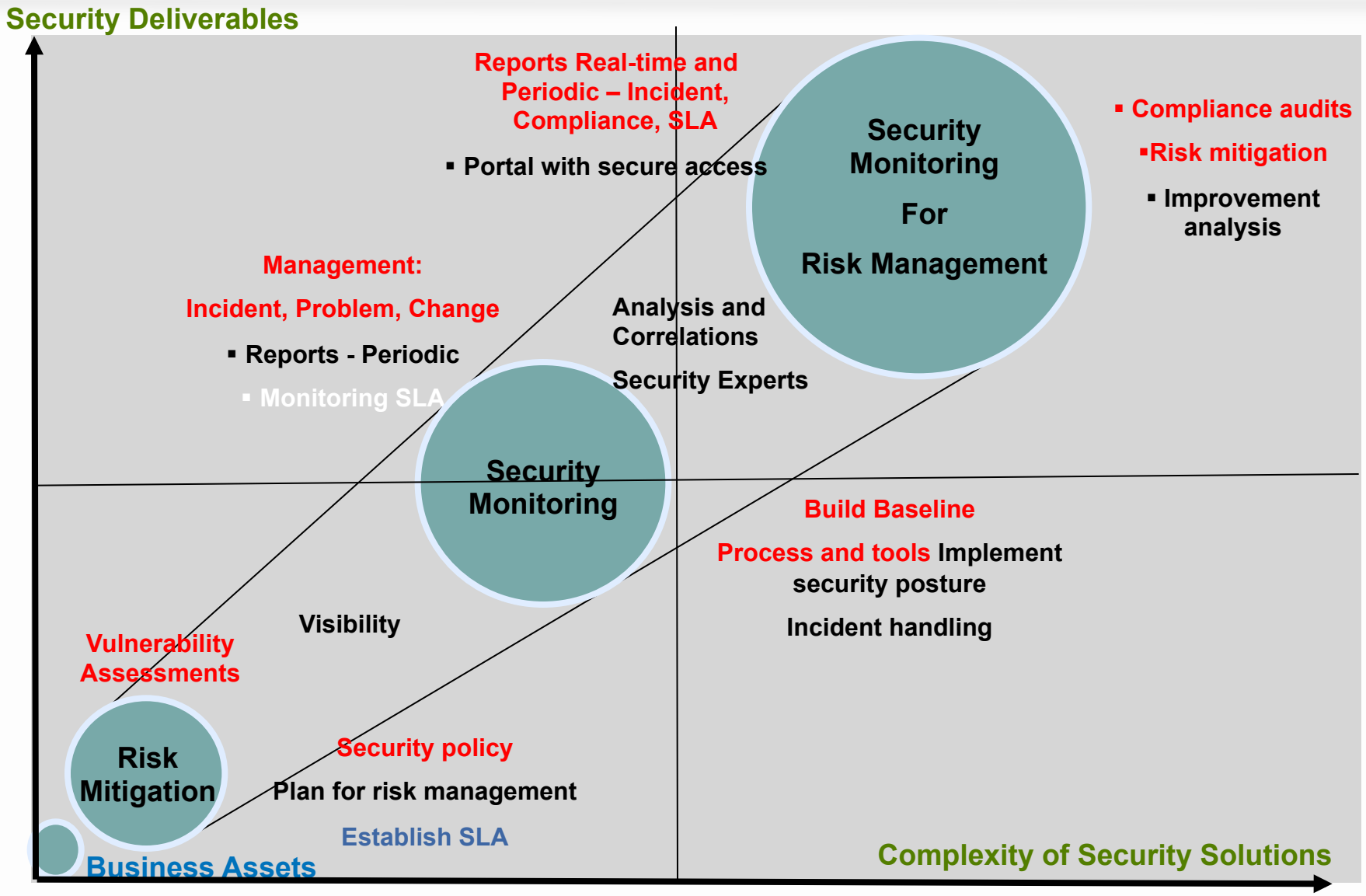
1. Need for SOC
2. Defining SOC Architecture
3. Building SOC Team
4. SOC Deliverables

Ask Questions Before Building SOC

- **In the face of ever changing threats, how can you ensure that your vital business assets and operations are protected?**
- **How do you guarantee privacy for your employees, partners, vendors and customers?**
- **How do you define & implement security policies?**

- **How do you manage vast amounts of data coming from various technologies that, while standing guard, generate an entire new set of operational support challenges?**
- **How do you maintain accountability and objective corporate governance within the organization?**

Security Operations Center



SOC Architecture Delivery

Security Experts → Expert analysis 24x7 risk management

Processes → ITIL and COBiT based process for consist risk management

Tools → Analysis and correlation for actionable security incidents

Agenda

1. Need for SOC
2. Defining SOC Architecture
3. Building SOC Team
4. SOC Deliverables

Typical SOC Requirements

- Perform real-time management and monitoring
- Expert analysis of log data collected
- Immediate response to potential security threats
- Provides rapid resolution of security problems
- Offers real-time view of the organization's security posture
- Protects companies technology investments

Typical SOC Communication

- **It is imperative that an SOC teams prepare information essential for timely response**
  - Contacts for all interconnecting ISPs (peers, vendors, customers, and upstreams)
  - Contacts for all vendor's product security reaction teams and response accountable parties
  - Document policies to define levels of support for your customers, classification of attacks, traceback of the attacks, determine response methods (will you drop the attacks on your infrastructure?)
- **Ensure you have all critical E-mail, phones, pagers, and web pages complete**
- **Ensure you have procedures in place to answer questions and communicate**

SOC Team Skill Requirements

- **SOC Team needs to know ….**
  - Everything a SP's Backbone Engineer knows
  - Everything a SP's Network Management Engineers knows
  - Everything a SP's Hosting/Content Engineer knows
  - Everything a SP's Postmaster knows
  - Everything a SP's DNS/DHCP/Addressing Engineer knows
  - Everything a CERT Engineer knows
  - Everything a Enterprise Security Engineer knows

In essence – you are looking for super engineers who are a hybrid SP Backbone and Security Engineer

Tips on Hiring SOC Team Talent

- Hire experienced, certified people
- Document and verify processes
- Maintain latest infrastructure information
- Establish SLAs with customers and peers
- Test the continuity of operations regularly
- Maintain vendor support contracts
- Leverage analysis tools
- Create incentives for analyst development
- Plan and prepare for incident response
- Evaluate and measure for process improvement

SP's OPSEC Team—Separate?

- **Traditionally, the security, InfoSec, or Information Assurance (IA) team has been totally separate from the network/systems operations organization.**
  - **The BCP in the industry to insure audit separation.**
  - **Audit gains has the consequence of in-efficient working relationship with the operations organization.**
- **With today's DDOS attacks, BOTnets, and Turbo Worms, separation and poor working relationships bog down the resolution time – impacting the services to the customers.**

SP's/ISP's SOC Team and INFOSEC Team

- **Some SPs have adopted the model of two teams:**
  - **OPSEC integrated into network/system operations**
  - **InfoSec in a separate reporting chain**
- **OPSEC team is tactical—Taking care of the daily security incidents**
- **INFOSEC team is strategic—Working on long term solutions, audits, and other items that are not time critical**

An SP's Incident Response Team

- SPs need an Incident Response Team
- The SP's Incident Response Team can be from one person to many people – depending on the size of the ISP.
  - Dedicated Team
  - Virtual Team
- Usually connected to the SP's NOC/SOC

Team and Network Preparation Assessment

SOC team must be able to answer the following:

- Are these traffic patterns normal for our network?
- What is using up all of our bandwidth?
- Angry customers are calling - what happened?
- Why can't we reach that server, network or AS?
- Has another provider hijacked our routers?
- Should we buy more transit or peer directly?
- Should we change these BGP attributes or policies?

SOC Team Communication Strategy

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?

Agenda

1. Need for SOC
2. Defining SOC Architecture
3. Building SOC Team
4. SOC Deliverables

What Do the SOC Deliverables Provide?

- **Increase Collective Visibility**
  - **Pulling Data from Variety of Sources**
  - **Aggregation of Data for further Analysis & Historic Record**
- **Expedite Correlation Capabilities**
  - **Ability to Respond Quickly; relatively real-time**
  - **Device and System Coverage**
  - **Forensic Capabilities**
- **Enable and Plan Timely Action**
  - **Reduction of Incident Impact on Business**
  - **Resulting Improvement to Service Availability / Assurance**

Typical Actions of SOC

- **Performs real-time management and monitoring of firewalls, intrusion detection systems, intrusion prevention systems, virtual private networks, patch management, asset management and other security products**
- **Enhances the institution's information security posture through continuous monitoring and management, expert analysis of log data, and immediate response to potential security threats**
- **Provides rapid resolution of security problems**
- **Offers real-time view of the organization's security posture**
- **Ensure optimal protection of mission-critical assets by providing analysis and commentary needed to adjust defenses against emerging attacks**
- **Protects companies technology investments**

SOC Deliverables

- Security Monitoring for Risk Management
- Security Posture Risk Analysis
- Secure Role-based Portal Access
  - Real-time monitoring and status of incidents / tickets
- Reports
  - Security Policy Reports
  - Security Incident Reports
    - Real-time on per incident basis as well as weekly / monthly
    - Information Required to Prepare Compliance Related Audit
  - Service Level Agreement Reports
    - Monitoring for Security Policy Compliance
    - Trends of security incidents and events
    - Service Compliance Report to Evaluate

Incident Handling Basics

What to Report

- Confirmed / Suspected Security Incident or Intrusions
- Denial of Service Attacks
- Malicious Logic / Mobile Code / Viruses
- Network Probes / Scans
- Attempts to Obtain Passwords
- Other Suspicious Behavior / Anomalies

Incident Handling Basics

Incident Report Contents

- **Incident Date / Time (UTC)**
- **System Information (Location, IP, etc.)**
- **How the Attack was Identified**
- **Attack Success Evaluation**
- **Attack Impact**
- **Corrective Actions Attempted**
- **Points of Content**

Summary

Incident Handling Terms

- **Technical Vulnerability**
- **Administrative Vulnerability**
- **Event**
- **Incident**



Incident Handling Terms

Technical Vulnerability:

A hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, resulting in the risk of compromise of information, alteration of information or denial of service

Administrative Vulnerability:

A security weakness caused by incorrect or inadequate implementation of a system's existing security features.

Practitioner's Tip: Proactively Seek Out and Eliminate Administrative Vulnerabilities to Minimize Your Risk

Incident Handling Terms

Event:
Unexpected behavior by a system that yields abnormal results or indicates unauthorized use or access, unexplained outages, denial of service, or presence of a virus

Incident:
An attempt to exploit a computer network or system such that the actual or potential adverse effects may involve fraud, waste or abuse; compromise of information; loss or damage of property or information, or denial of service. Incidents may also include:

Penetration of a System
Exploitation / Attempted Exploitation
Malicious Mobile Code / Viruses
Violations of State, US, or International Law

Agenda - Extras

1. DShield
2. What Data to Collect
3. Incident Handling Basics
4. SP's Top Ten Security Checklist

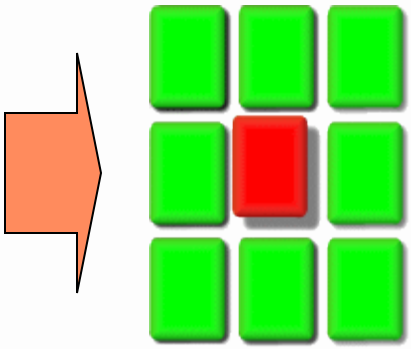
DSHIELD

Data Collection

Analysis

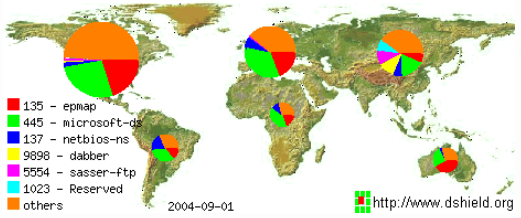
Dissemination

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	9898		[trojan] Dabber Worm backdoor
sasser-ftp	5554		[trojan] Sasser Worm FTP Server
Reserved	1023		
ms-sql-s	1433		Microsoft-SQL-Server
ms-sql-m	1434		Microsoft-SQL-Monitor
netbios-ssn	139		NETBIOS Session Service
mydoom	3127		W32/MyDoom, W32.Novarg.A backdoor



DShield - Your recent submissions - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop https://secure.dshield.org/myreports.php?day=732191&source=&target=&targetport=&dangerh=Y&danc Go Search Print

User ID: 80744914
Total lines submitted on 2004-09-02:
13

Sep-02-2004

source
target
targetport

Include 'Danger Levels': ☑ high ☑ medium ☑ low ☑ misconf.

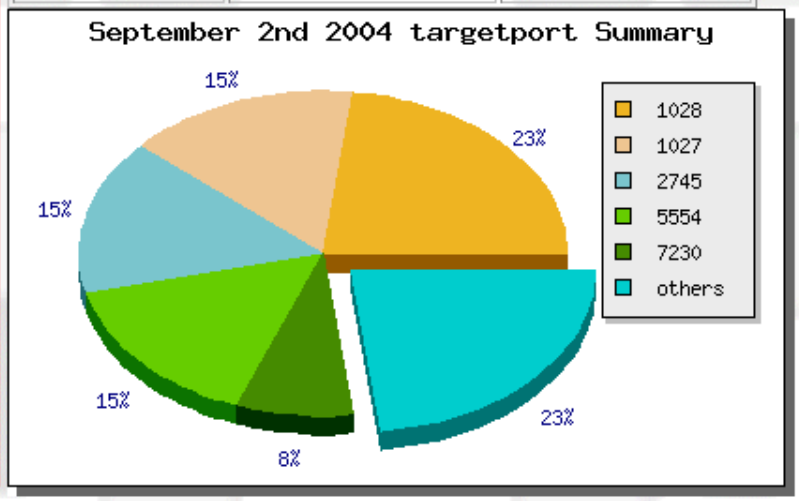
Change

Color Legend (Attack Severity based on Target Port) :

High Medium Low Possible Firewall Misconfiguration

Not all ports are assigned a 'danger level'. Unassigned ports are represented by an empty white circle (○).

Port Graph | Source Graph | Target Graph

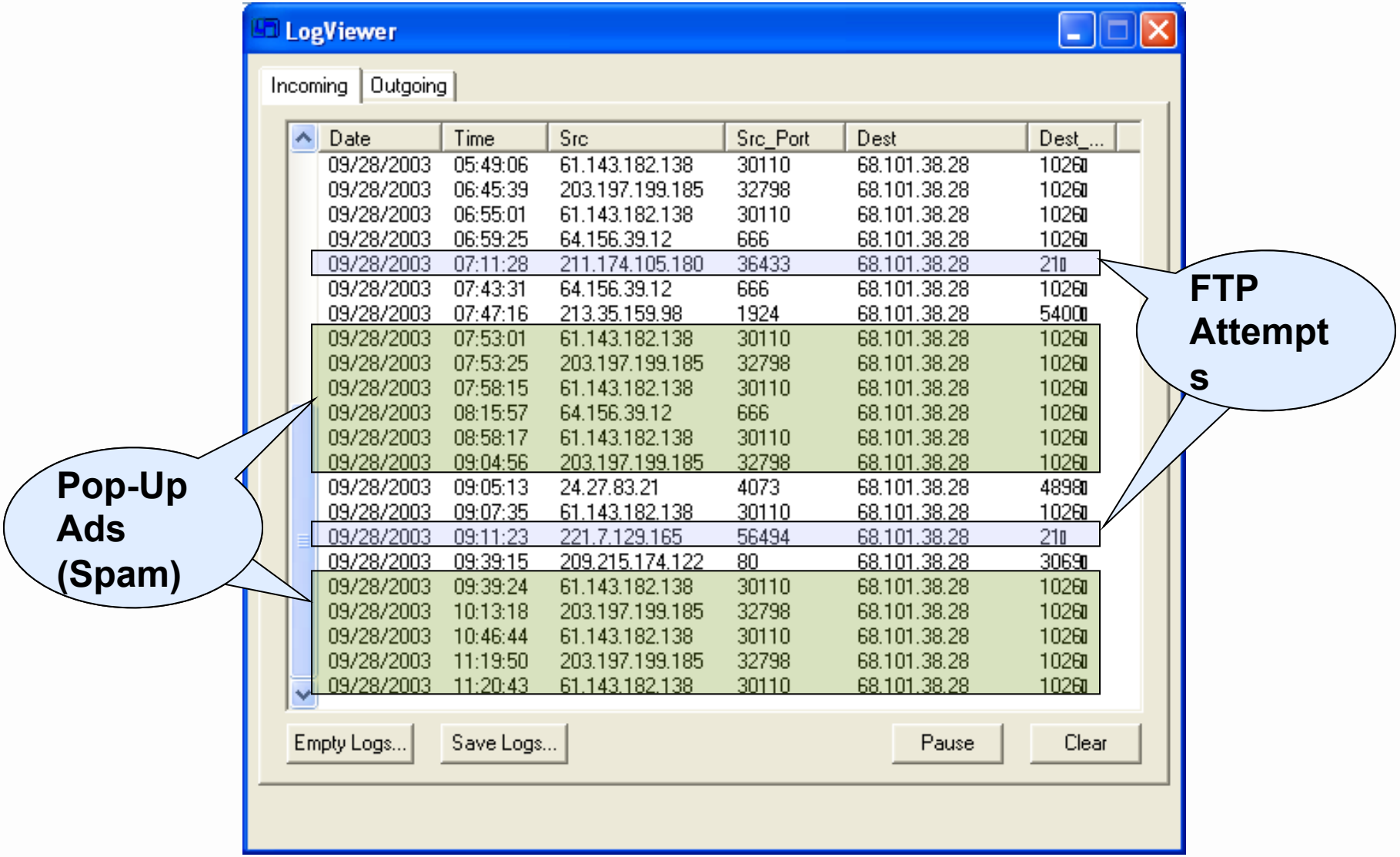


Currently showing lines 0 through 13

Next Page

Date	Time	Source	Source Port	Target	Target Port	Protocol	Danger
2004-09-02	00:53:36	012.049.017.236	10558	068.101.037.212	1028		○
2004-09-02	01:53:07	004.043.241.079	25945	068.101.037.212	1027		○
2004-09-02	02:51:24	130.238.147.250	55441	068.101.037.212	7230		○
2004-09-02	03:53:52	211.162.047.090	80	068.101.037.212	10258		○
2004-09-02	04:51:35	211.162.047.090	80	068.101.037.212	62507		○
2004-09-02	05:50:53	068.062.195.252	3697	068.101.037.212	2745		○
2004-09-02	06:54:16	068.062.126.020	2113	068.101.037.212	2745		○

Typical Residential Cable Modem Log



Features provided by DShield

- **Top 10 Most Wanted** : Top 10 offenders according to the DShield database.
- **Are you cracked ? :** If your IP address appeared in DShield's database, it would be a strong indicator that your machine was possibly cracked and is accessing other machines in a manner that their firewalls log as hostile.
- **Fight Back Program**

Data Collection and Analysis

- DShield provides a platform for users of firewalls to share intrusion information.
- Submit logs and reports
  - Ready to go client programs
  - Web Interface to manually submit your firewall logs.

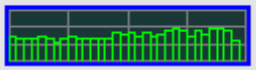
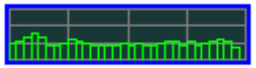
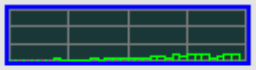
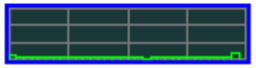
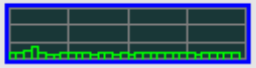
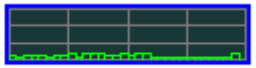
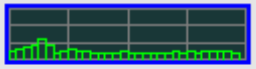
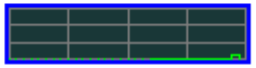
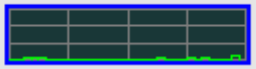
Reports and Database

- Top 10 offenders (as of 09/25/2005)

IP Address	Host Name
216.254.188.93	host-93.moseymosey.dsl.primus.ca
62.75.204.188 $^{73273}/_{49181}$ 	donau064.server4you.de
199.8.152.50 $^{1739064}/_{2242}$	
70.66.104.78	S010600500419247c.no.shawcable.net
64.239.191.96 $^{1797}/_{1776}$	www.berrycard.com
211.14.220.83	211.14.220.83.eo.eaccess.ne.jp
221.10.158.140 $^{492}/_{455}$ 	
61.132.90.9	
210.51.21.148 $^{107201}/_{16575}$ 	
221.10.158.106 $^{279}/_{154}$ 	

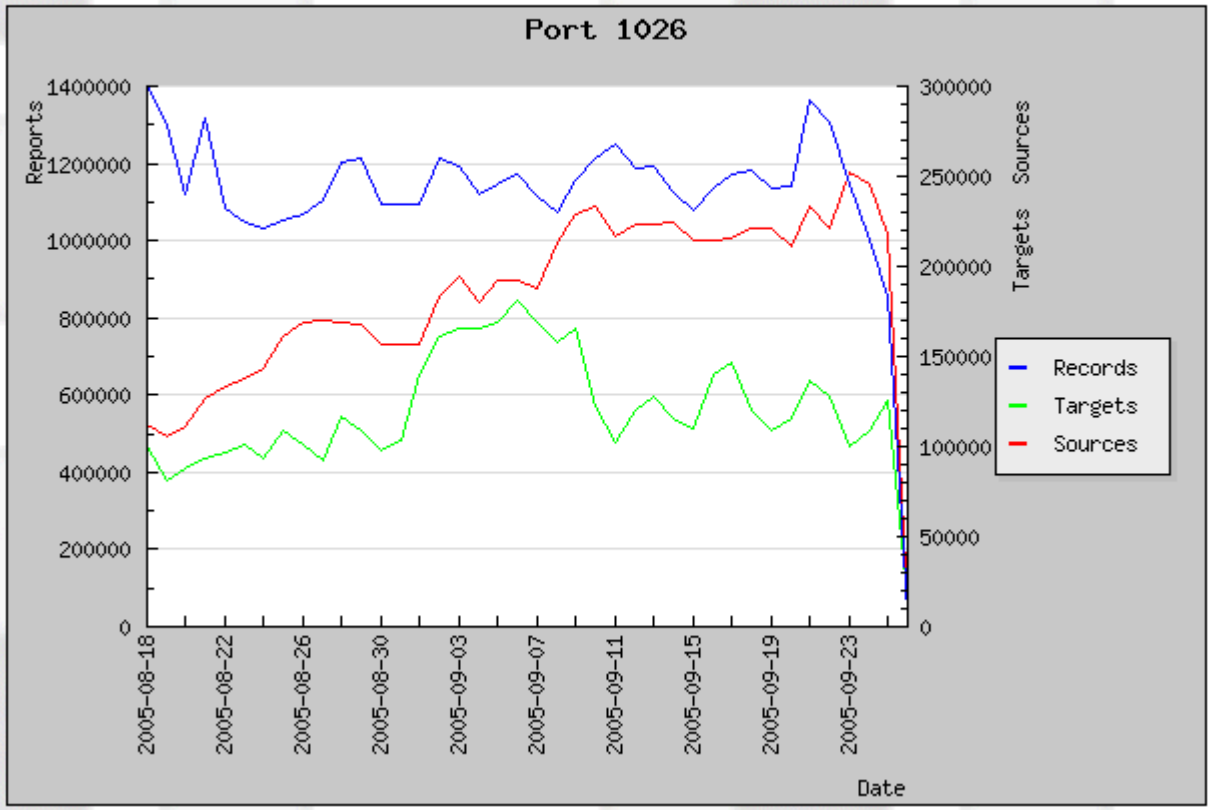
Reports and Database

- Top 10 Target Ports (as of 09/25/2005)

Service Name	Port Number	Activity Past Month	Explanation
bittorrent	6881		Bit Torrent P2P
win-rpc	1026		Windows RPC
microsoft-ds	445		Win2k+ Server Message Block
---	40000		
smtp	25		Simple Mail Transfer
netbios-ssn	139		NETBIOS Session Service
eMule	4672		eMule / eDonkey P2P Software
epmap	135		DCE endpoint resolution
filenet-rpc	32769		Filenet RPC
domain	53		Domain Name Server

Port Report

1026



Why notify victims?

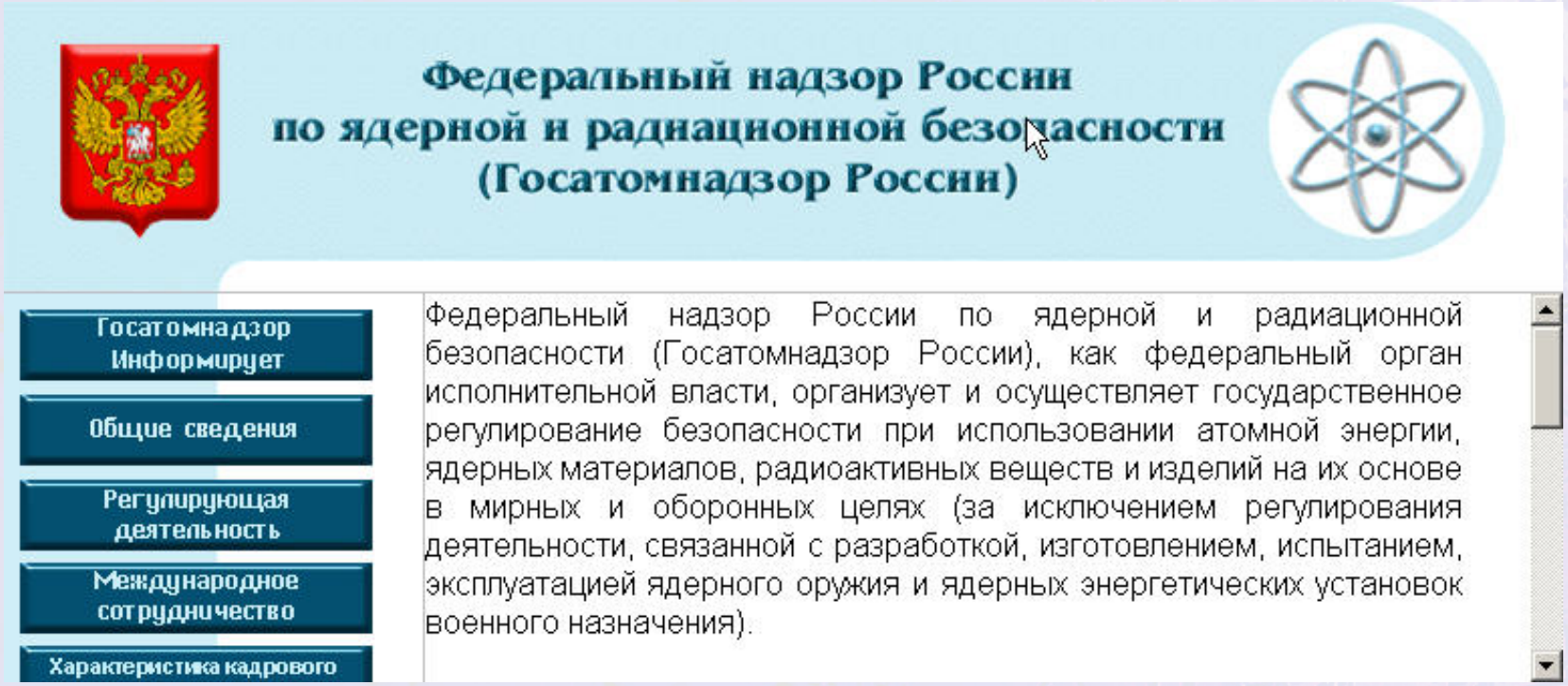
Recently, myNetWatchman detected an incident in which a host was infected with the Microsoft SQL Spida Worm. A backtrace of the offending IP yielded some interesting results…

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:        194.190.139.0 - 194.190.139.255
netname:        GAN
descr:          Central Region of GAN RF
country:        RU
admin-c:        AV753-RIPE
tech-c:         AV753-RIPE
status:         ASSIGNED PA
notify:         sam@gan.ru
notify:         ip-reg@ripn.net
mnt-by:         ROSNIIROS-MNT
changed:        ip-dbm@ripn.net 19991018
source:         RIPE
```

Slide by Lawrence Baldwin & Jaeson Schultz

GAN=The Nuclear Safety Authority of Russia



"Federal supervision of Russia on nuclear and radiating safety (Gosatomnadzor of Russia) as the federal enforcement authority, organizes and carries out state regulation of safety at use of an atomic energy, nuclear materials, radioactive substances and products on their basis in the peace and defensive purposes (except for regulation of the activity connected to development, manufacturing, test, operation of the nuclear weapon and nuclear power installations of military purpose(assignment)). "

Slide by Lawrence Baldwin & Jaeson Schultz

Agenda - Extras

1. Dshield
2. What Data to Collect
3. Incident Handling Basics
4. SP's Top Ten Security Checklist

Now, Let's Examine What You'll Collect

- Syslog
- SNMP
- RMON
- Netflow

Syslog

- Syslog output can become overwhelming
  - Open source databases (MySQL, PostGres) are often used to store syslog output for postprocessing and searching
- Facility numbers are the key to organizing syslog output on a syslog server
  - Facility Level 7 Is Default for Cisco
- The level of logging detail is important
  - Default level=6 (informational) - this can generate a *lot* of output.

Syslog (cont).

- Router Access Control List (ACL)
  - Generates a lot of information in a short span of time
  - Has a negative impact on performance.
  - Consider Netflow as an alternative.
  - Pix and FWSM are more efficient for logging.
- Cisco's CS-MARS takes syslog input from routers, switches, firewalls, IDS, VPN concentrators and combines it with other forms of telemetry in order to provide anomaly-detection and event correlation.

SNMP

- Routers generate Simple Network Management Protocol (SNMP) traps when various events take place.
- SNMP statistics can be polled from routers, switches, and other network devices.
- Tools:
  - NET-SNMP
  - MRTG
  - Cricket
  - RRDTool
  - Nagios
  - Arbor PeakFlow DoS
  - Cisco CS-MARS

SNMP - High CPU

- Spikes in CPU load on routers, switches, servers, and other devices is often an indication that an event is taking place.
- High CPU is *not* always an indicator of malicious activity. Trending is important!
- Correlating CPU utilization with other information such as network traffic statistics, routing-table changes, etc., is very useful.
- A baseline of CPU utilization over time is a good idea from a network management standpoint, and also allows us to determine if further investigation is warranted.

RMON

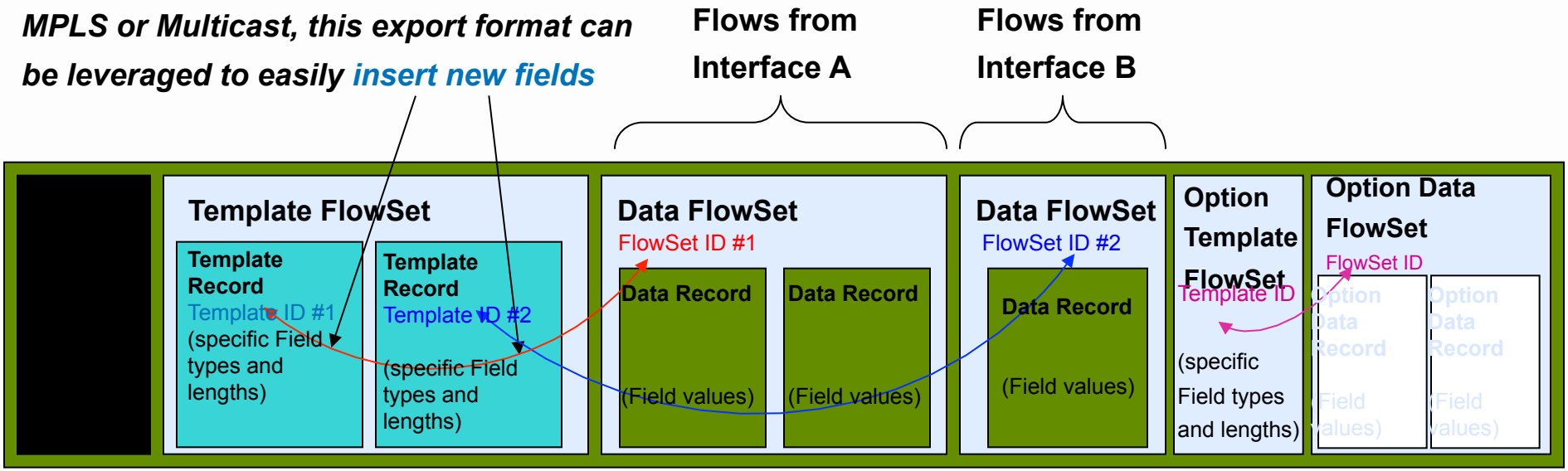
- Probes should be placed at key points within the infrastructure
- RMON Group 1 and 2 Provide Visibility
- Tools:
  - Cisco NAM-2 for the 6500/7600
    - On-board RMON statistics through a Web GUI
    - Reporting to a central RMON console
    - Packet capture and entry-level NetFlow statistics display
  - NTOP
    - Open Source
    - Displays RMON statistics via Web Server

NetFlow

- Should typically be enabled on all router interfaces where possible
- Useful for on-box troubleshooting via CLI as well as for export to analysis systems
- Ingress and egress NetFlow are now supported.
- 1:1 NetFlow is useful for troubleshooting, forensics, traffic analysis, and behavioral/relational anomaly-detection
- Sampled NetFlow is useful for traffic analysis and behavioral/ relational anomaly-detection.
- Subinterface telemetry is supported using `ip flow ingress` and `ip flow egress` commands (supersede ip route cache flow).

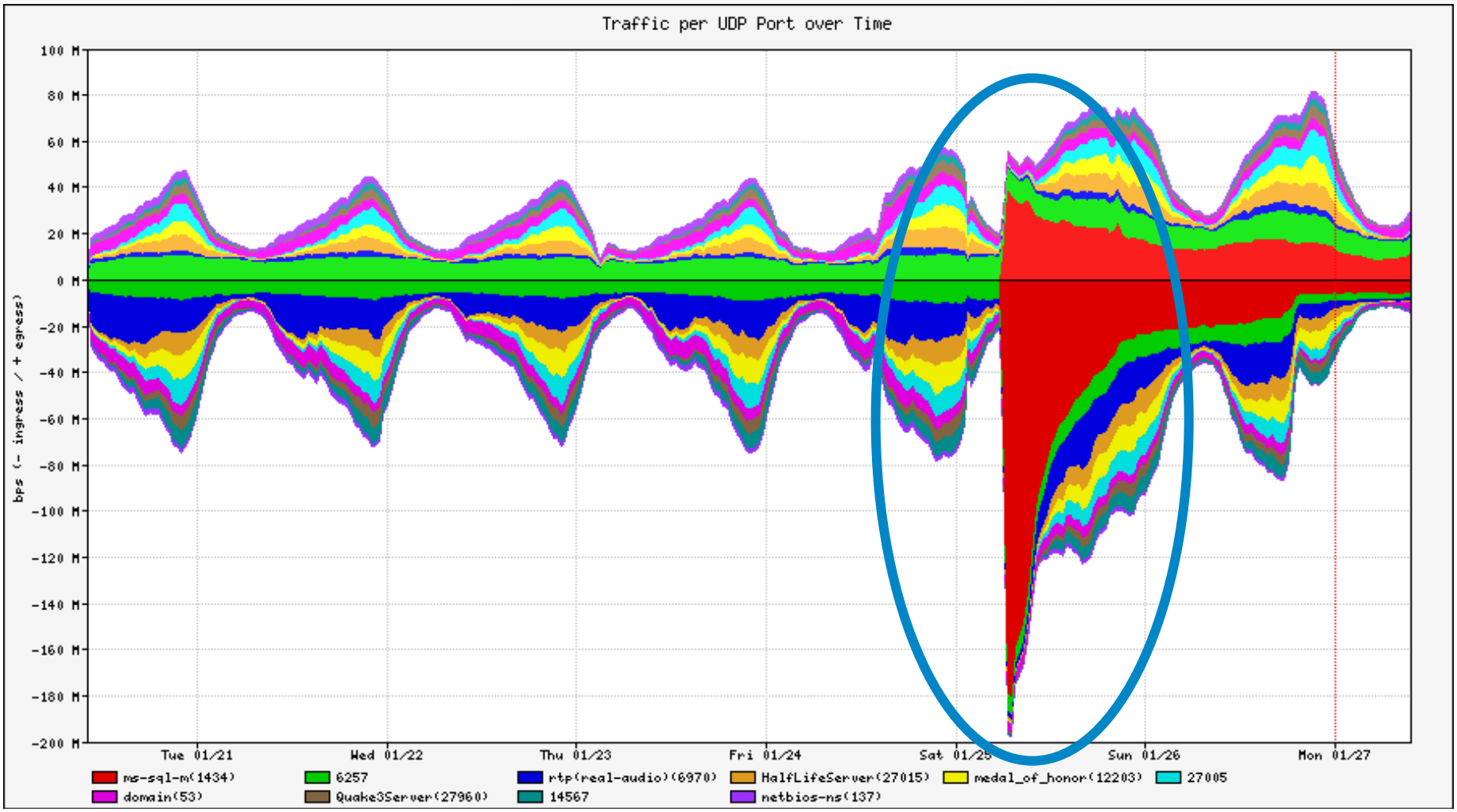
NetFlow v9 Export Packet Format

To support technologies such as MPLS or Multicast, this export format can be leveraged to easily insert new fields



- Matching ID #s is the way to associate Template to the Data Records
- The Header follows the same format as prior NetFlow versions so Collectors will be backward compatible
- Each Data Record represents one flow
- If exported flows have the same fields then they can be contained in the same Template Record e.g. unicast traffic can be combined with multicast records
- If exported flows have different fields then they can't be contained in the same Template Record e.g. BGP next-hop can't be combined with MPLS Aware NetFlow records

Example - SQL Slammer



Summary

- The Network Management Network transports telemetry for further analysis by the back office
- Telemetry is used to baseline expected behavior
- Telemetry comes in many flavors:
  - Syslog
  - SNMP
  - RMON
  - Netflow

Agenda - Extras

1. Dshield
2. What Data to Collect
3. Incident Handling Basics
4. SP Top Ten Security Checklist

Incident Handling Terms

- Technical Vulnerability
- Administrative Vulnerability
- Event
- Incident

Incident Handling Terms

Technical Vulnerability: A hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, resulting in the risk of compromise of information, alteration of information or denial of service

Administrative Vulnerability: A security weakness caused by incorrect or inadequate implementation of a system's existing security features.

Practitioner's Tip: Proactively Seek Out and Eliminate Administrative Vulnerabilities to Minimize Your Risk

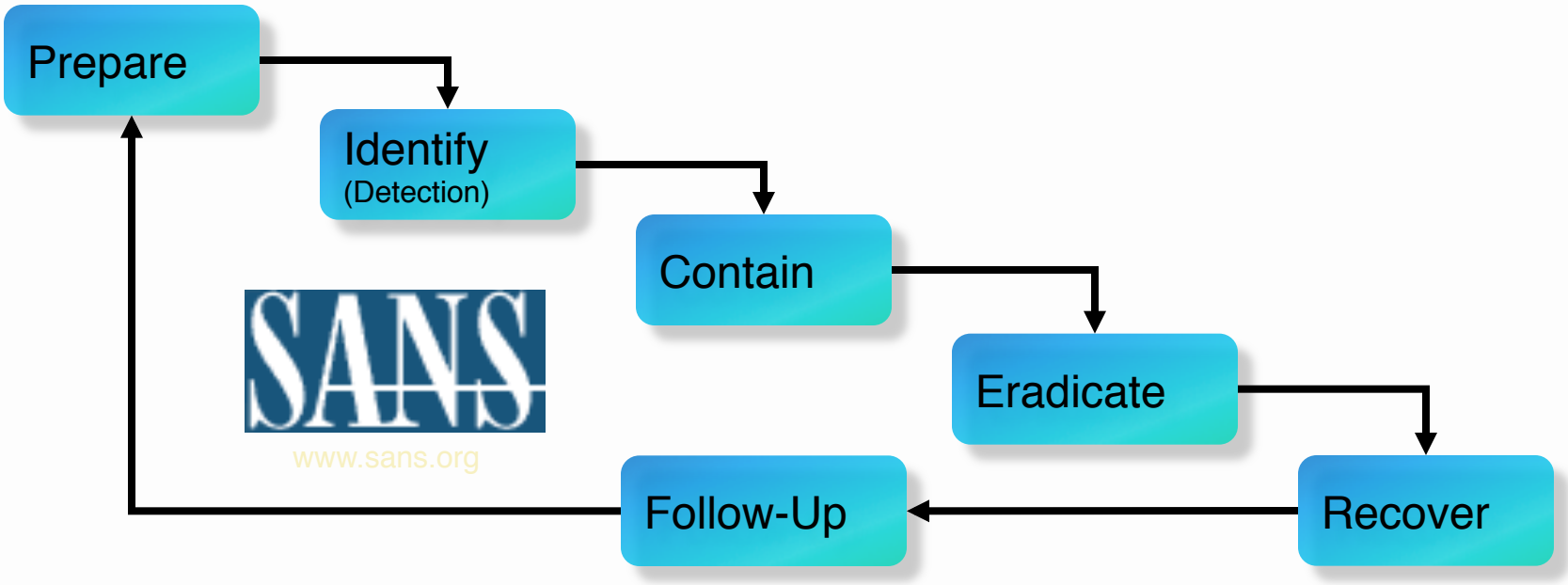
Incident Handling Terms

Event: Unexpected behavior by a system that yields abnormal results or indicates unauthorized use or access, unexplained outages, denial of service, or presence of a virus

Incident: An attempt to exploit a computer network or system such that the actual or potential adverse effects may involve fraud, waste or abuse; compromise of information; loss or damage of property or information, or denial of service. Incidents may also include:

- Penetration of a System
- Exploitation / Attempted Exploitation
- Malicious Mobile Code / Viruses
- Violations of State, US, or International Law

Incident Handling Basics



***Practitioner's Tip:* Proactive Preparation Reduces the Cost of Each Incident -- Practice Early and Often!**

Incident Handling Basics

Prepare

- Develop Policies & Practices
- Develop Incident Reporting Guidelines
- Employ Sound Defensive Principles
- Develop a Suite of Tools
- Understand the Network
- Train Your People

***Practitioner's Tip:* Practicing Response Procedures (Including Management) Proactively Enhances Response**

Incident Handling Basics

Identify
(Detection)

- Early Detection is the Key!
- Use Your (Human) Sensors Well
- Rule Out the Obvious Errors
- Report Early / Report Often

***Practitioner's Tip:* Attempt to Understand What is Happening, but Don't Try to Solve the Problem Yet!**

Incident Handling Basics

Contain

- Prevent the Spread of Compromise
  - Reduce / Remove Network Connectivity
  - Backup Critical Systems
  - Reset Passwords
- Build Go-Forward Plans Prior to Acting
- Continue to Coordinate Internally & Externally

Practitioner's Tip: *"Go Slow to Be Quick"*

Incident Handling Basics

Eradicate

- Eliminate the Root Cause of the Incident
  - Make Sure You Know the Root Cause First!
  - Ensure all Evidence is Collected Prior to Eradication
- Eliminate the Immediate Point of Vulnerability
- Improve Overall Defenses in the Enterprise

Practitioner's Tip: Avoid the Temptation to Treat the Symptoms, as it Prolongs Your Vulnerability & Exposure

Incident Handling Basics

Recover

- Restore from (Trusted) Backup
- Deploy Additional Countermeasures / Controls
- Calculate Costs / Impacts of Incident
- Transition Evidence to Legal Team
- Complete Incident Report

Practitioner's Tip: Validate all Backups, Systems, Patches, etc. Prior to Deployment in a Production Environment!

Incident Handling Basics

Follow Up

- Review / Communicate Incident Report
- Update User Awareness Training
- Evaluate Readiness Enterprise Wide
- Review / Update Security Controls
- Determine any HR / Legal Course of Action

Practitioner's Tip: Employ a Cyclical Process, as Attacks Continually Evolve…and Exploit Known Vulnerabilities!

Incident Handling Basics

What to Report

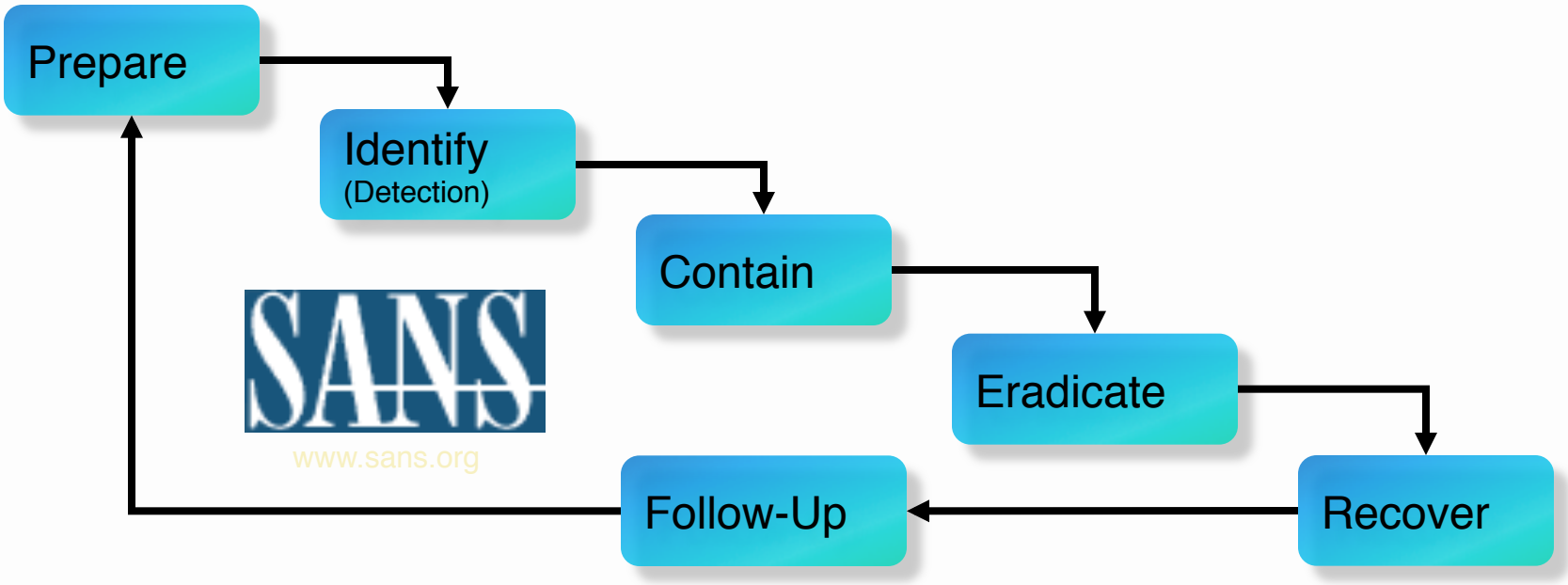
- Confirmed / Suspected Intrusions
- Denial of Service Attacks
- Malicious Logic / Mobile Code / Viruses
- Network Probes / Scans
- Attempts to Obtain Passwords
- Other Suspicious Behavior / Anomalies

Incident Handling Basics

Incident Report Contents

- Incident Date / Time (UTC)
- System Information (Location, IP, etc.)
- How the Attack was Identified
- Attack Success Evaluation
- Attack Impact
- Corrective Actions Attempted
- Points of Content

Incident Handling Basics



***Practitioner's Tip:* Proactive Preparation Reduces the Cost of Each Incident -- Practice Early and Often!**

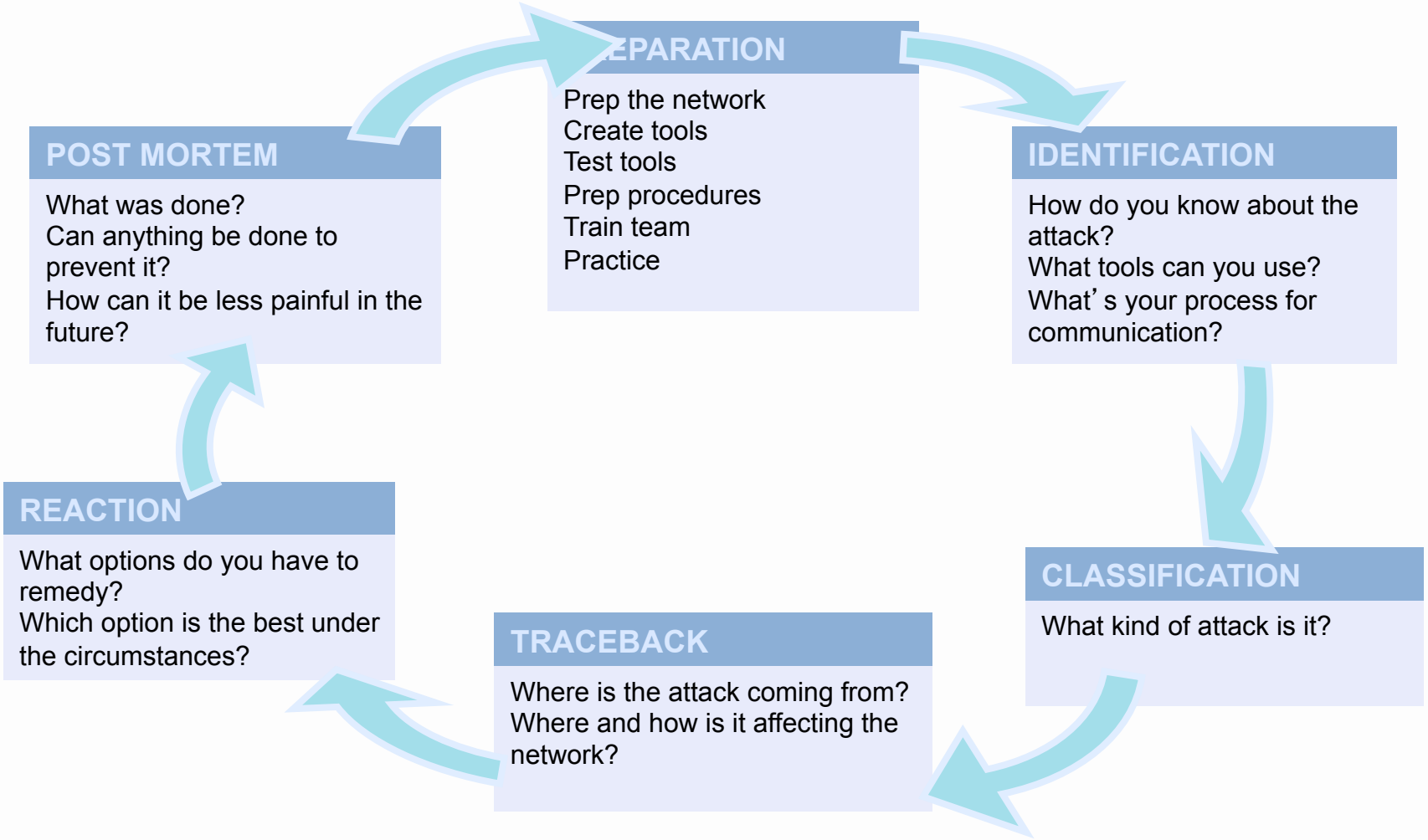
Agenda - Extras

1. Dshield
2. What Data to Collect
3. Incident Handling Basics
4. SP's Top Ten Security Checklist

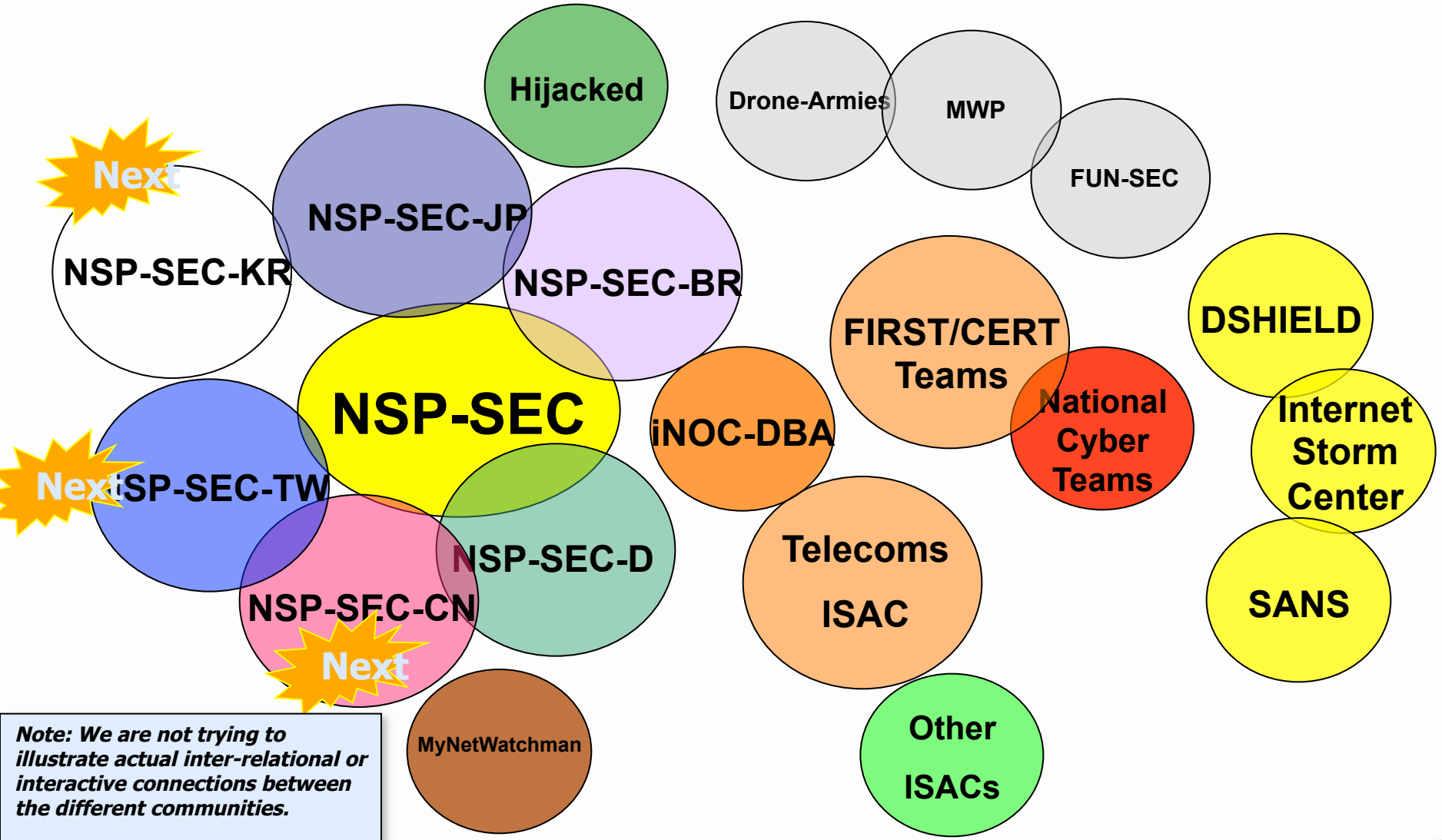
Top Ten List of things that Work

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)

SP Security in the NOC - Prepare



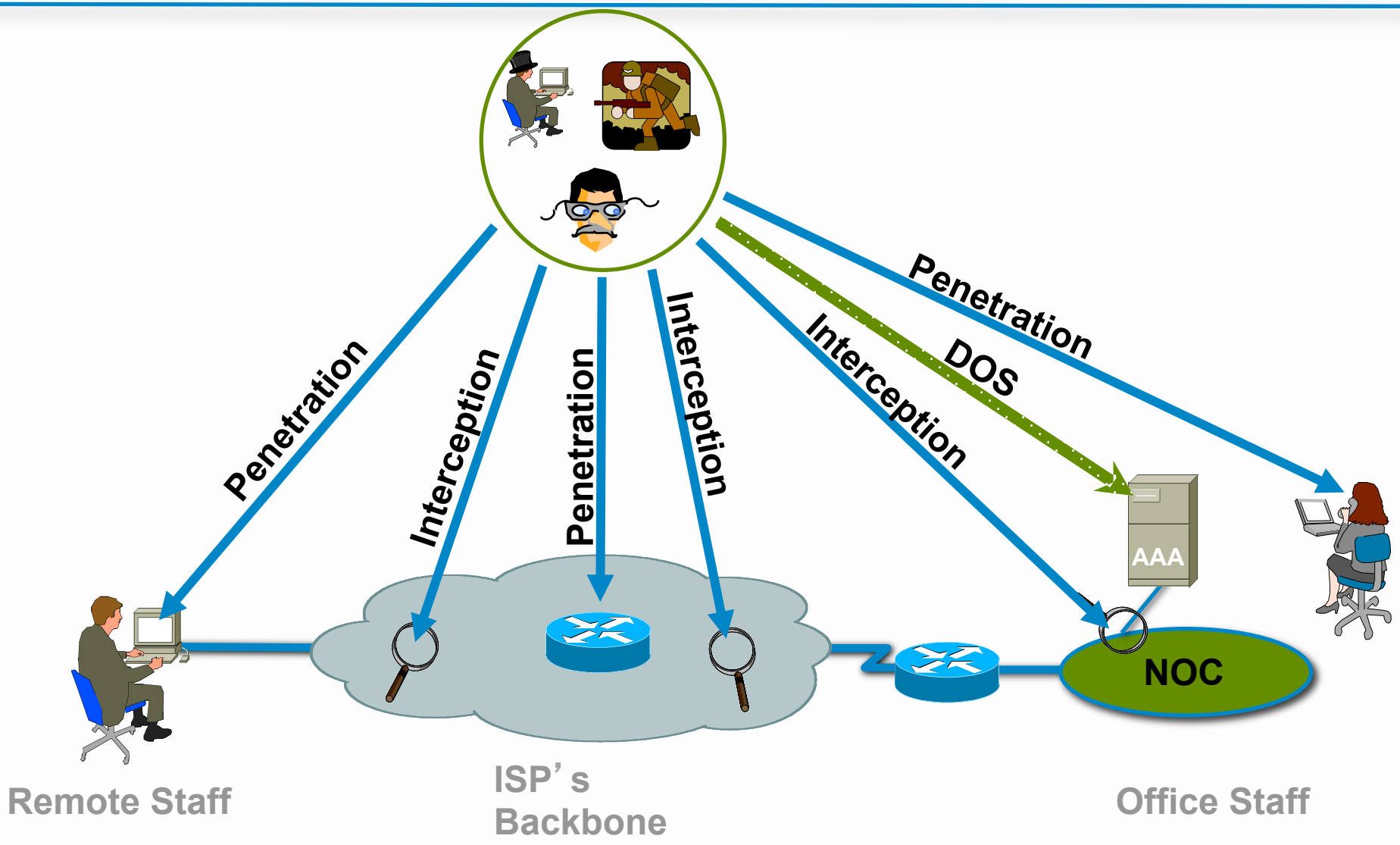
Aggressive Collaboration



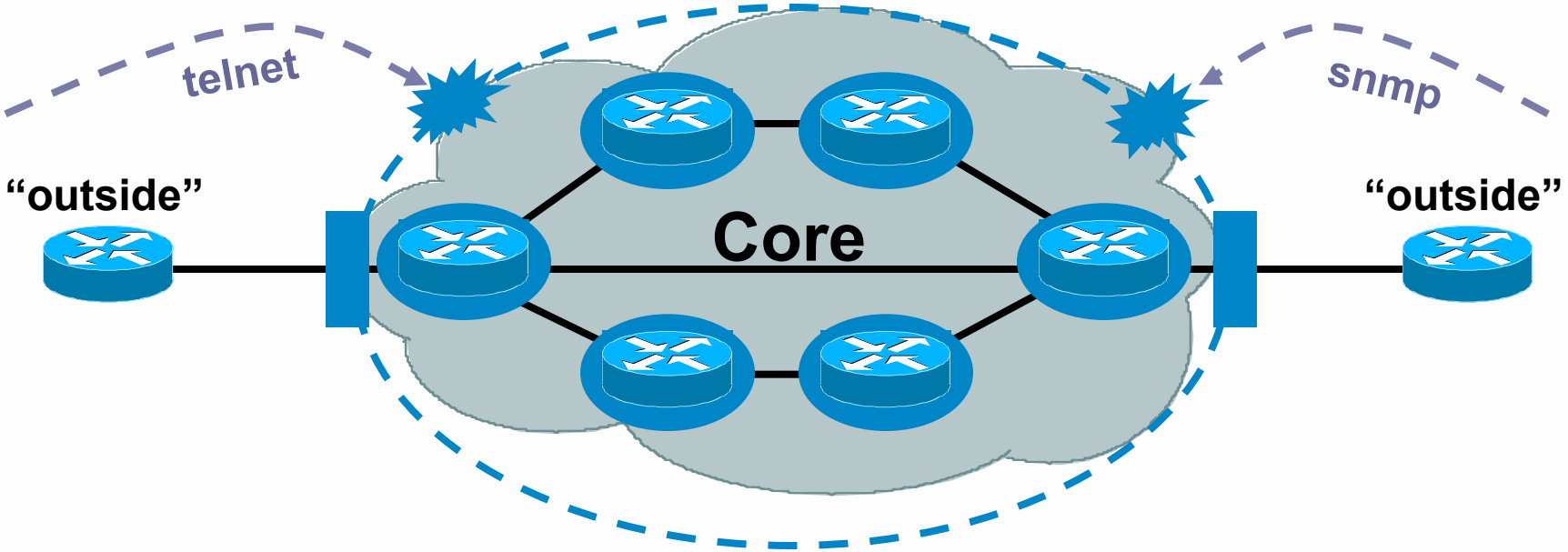
iNOC DBA Hotline

- 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, and sponsored by Cisco.

Point Protection

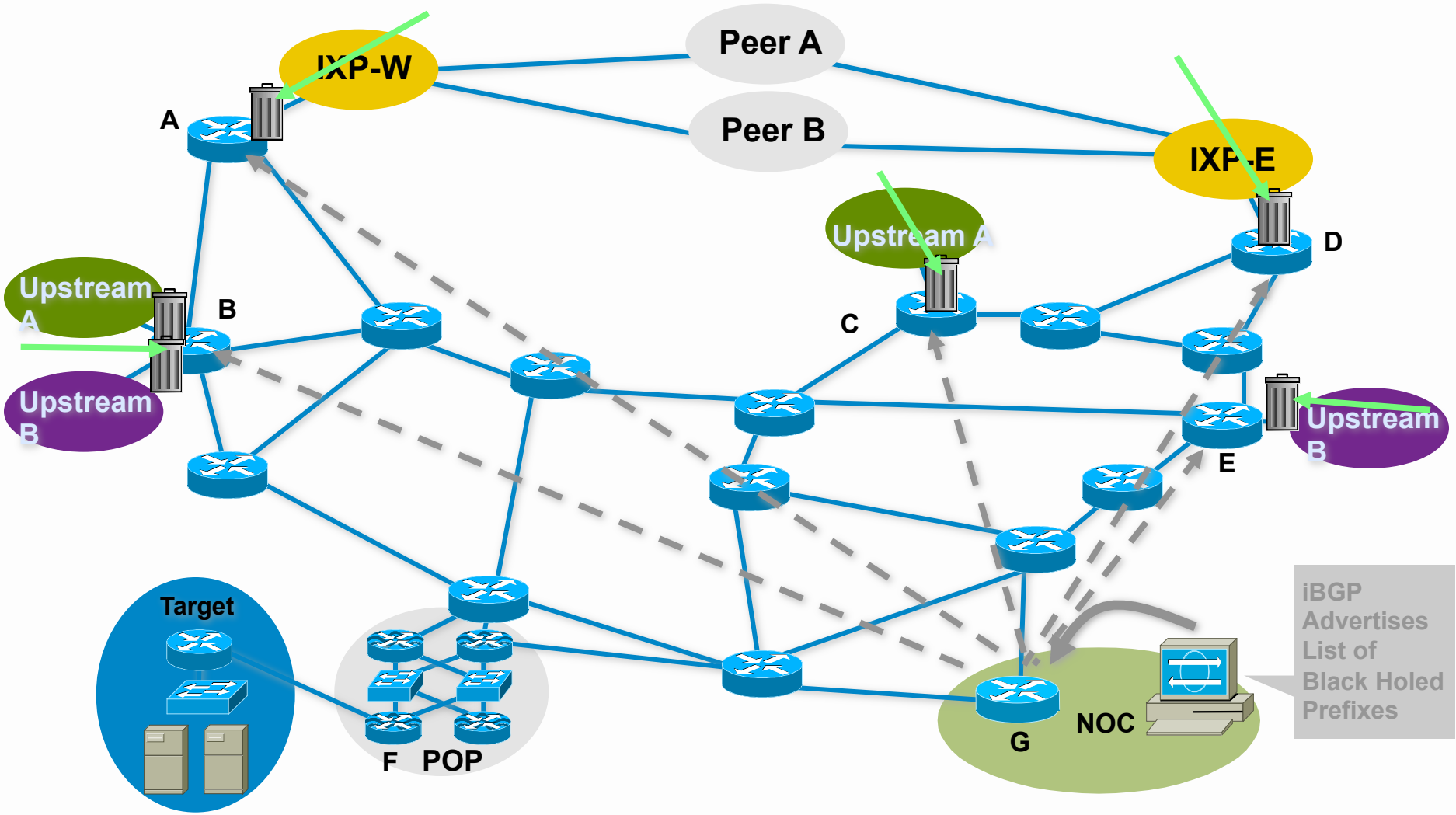


Edge Protection

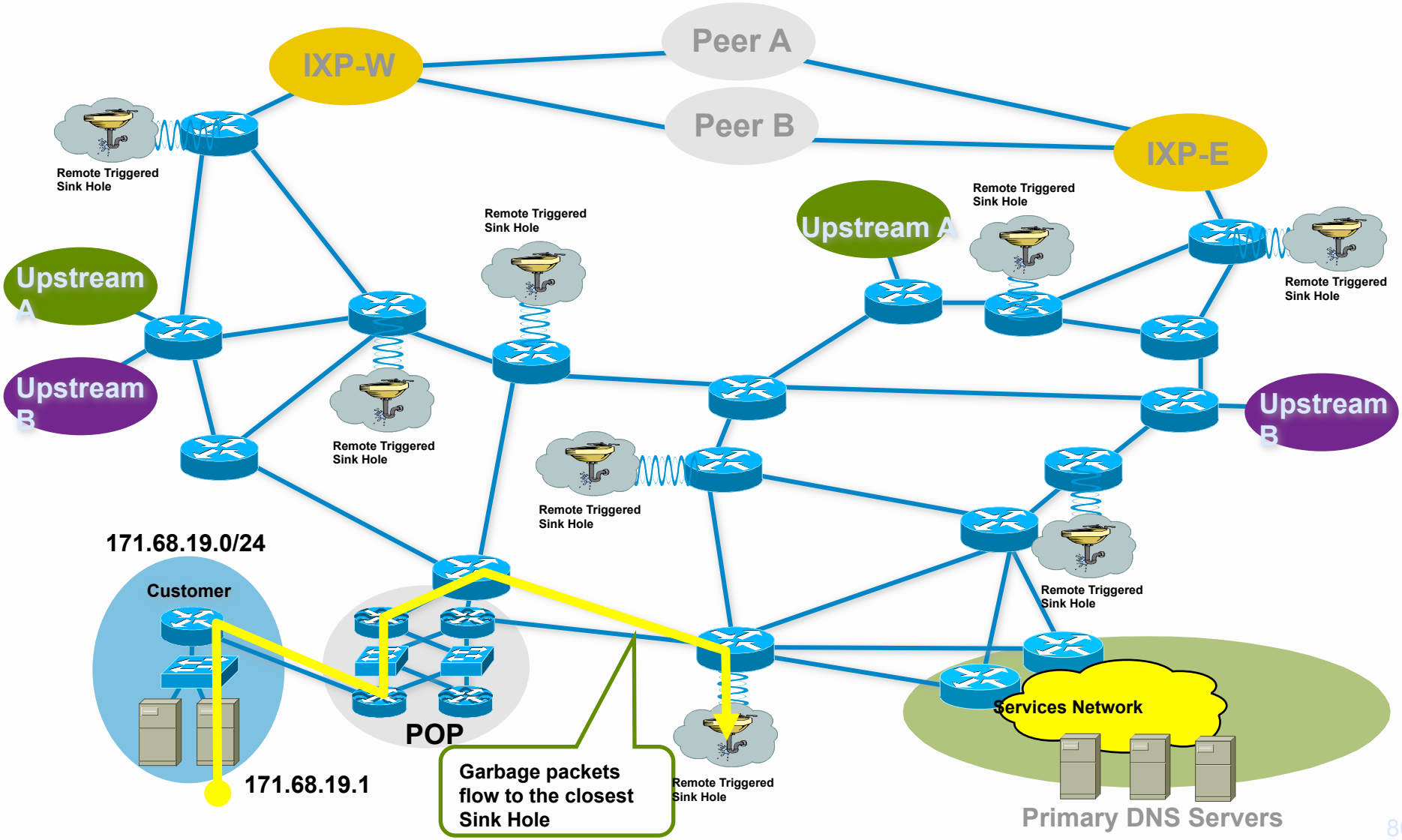


- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

Destination Based RTBH

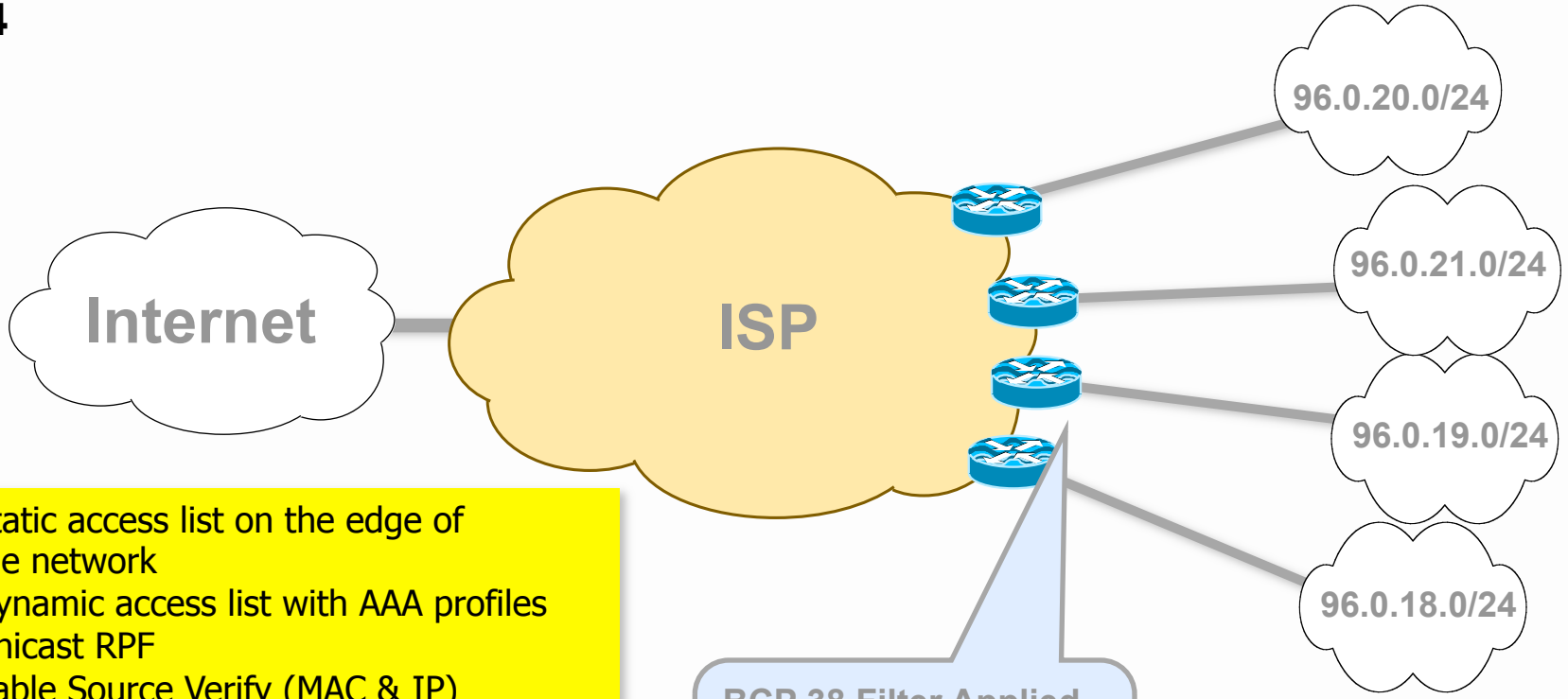


Sink Holes


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
POP
171.68.19.1
Garbage packets flow to the closest Sink Hole
Services Network
Primary DNS Servers

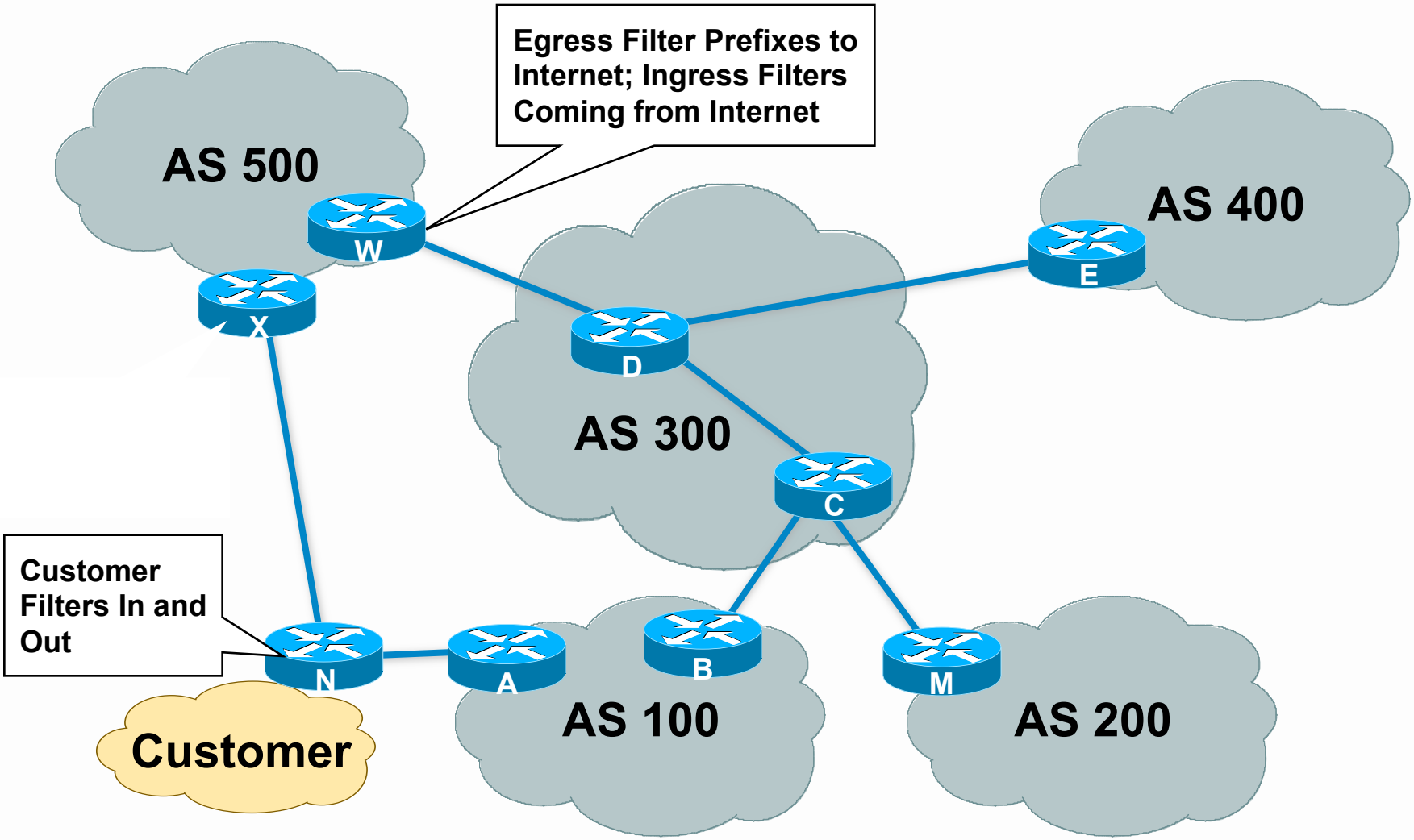
BCP 38 Ingress Packet Filtering

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



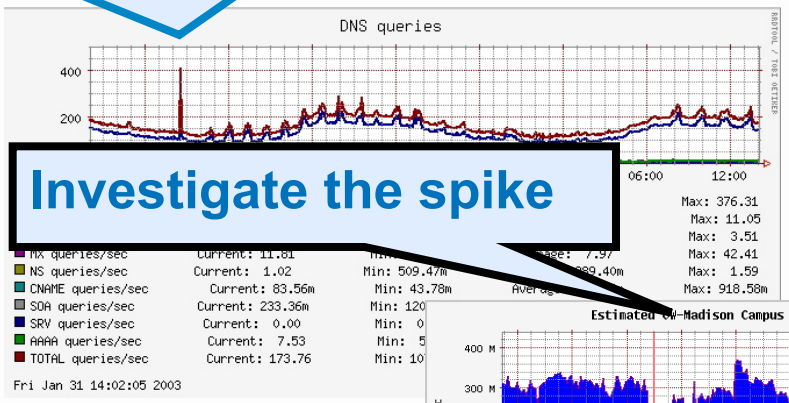
- Static access list on the edge of the network
- Dynamic access list with AAA profiles
- Unicast RPF
- Cable Source Verify (MAC & IP)
- Packet Cable Multimedia (PCMM)
- IP Source Verify (MAC & IP)

Where to Prefix Filter?

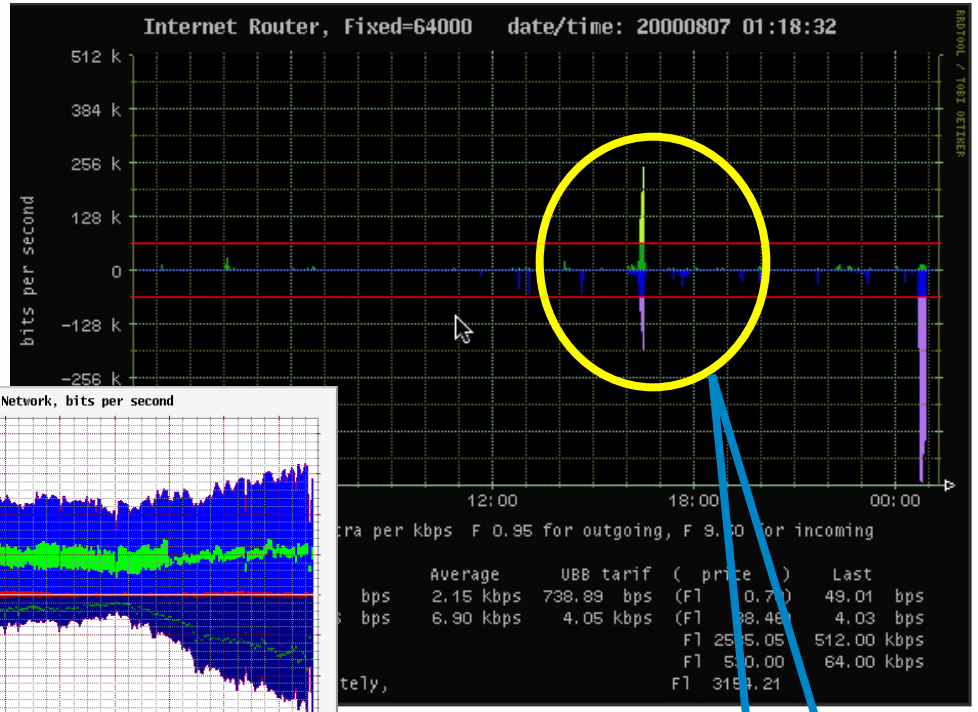


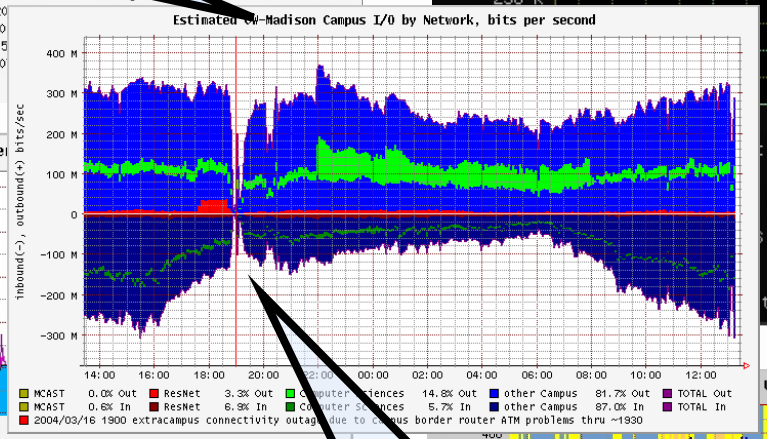
Total Visibility

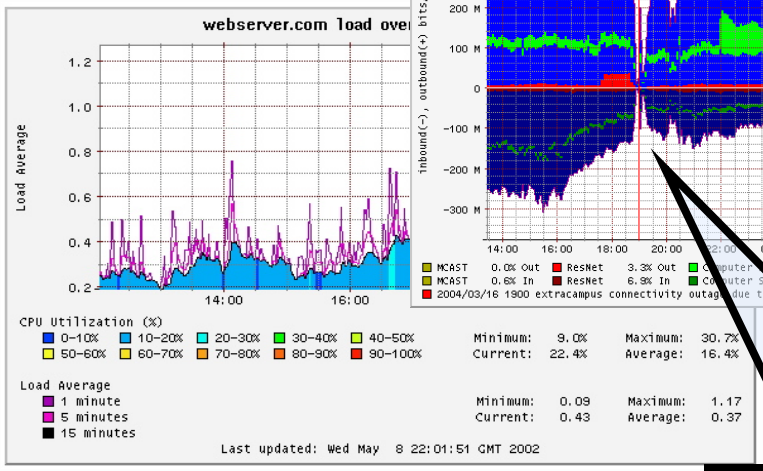
Anomaly for DNS Queries

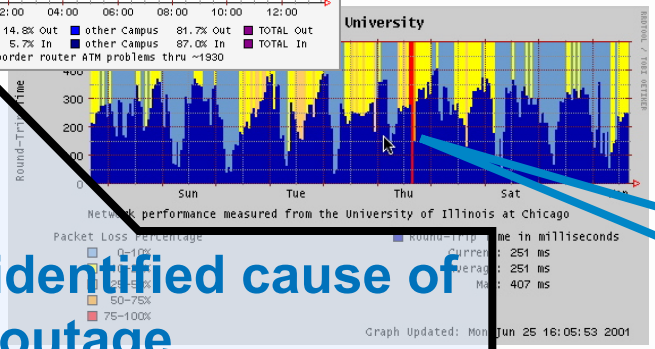


Investigate the spike









Thru' put Spike

RTT Spike

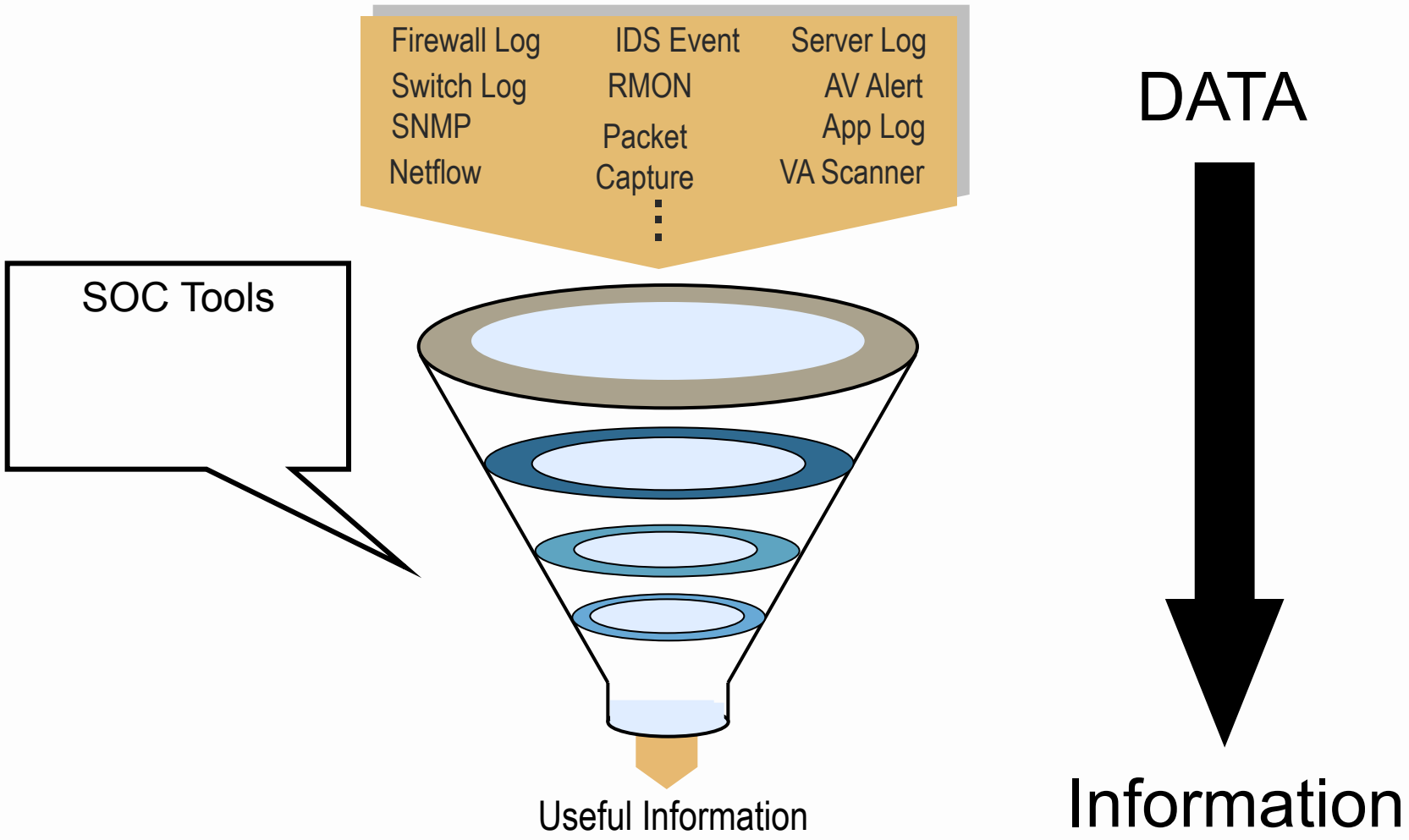
An identified cause of the outage

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

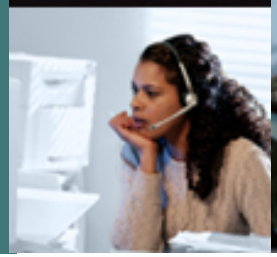
Correlation



Consequences of No Action

- SLAMMER Illustrated the difference between those SP who were prepared and those who were not.
  - NOC/Sec-Ops Teams that had the most rudimentary procedures in place (i.e. a internal contact list) where able to start their anti-Slammer action with the first 6 hours.
  - Those who did not, started after 6 hours – with the effects network wide.
- Q. Are you ready for the next Turbo Worm?
- Q. Are you ready for the next Internet wide incident?

Communications



“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 Cisco PSIRT

  Use psirt@cisco.com, security-alert@cisco.com to contact us.

  Subscribe to cust-security-announce@cisco.com for alerts.
- 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 recourse for customers, providers and others who are experiencing difficulties with the organization's Internet service.

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.cisco.com/security as an example.

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 before a crisis ….

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 center)
  - 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!

Coordination

- FIRST:
  Forum of Incident Response Teams
  http://www.first.org
- NSP-SEC
- I-NOC Phone

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?

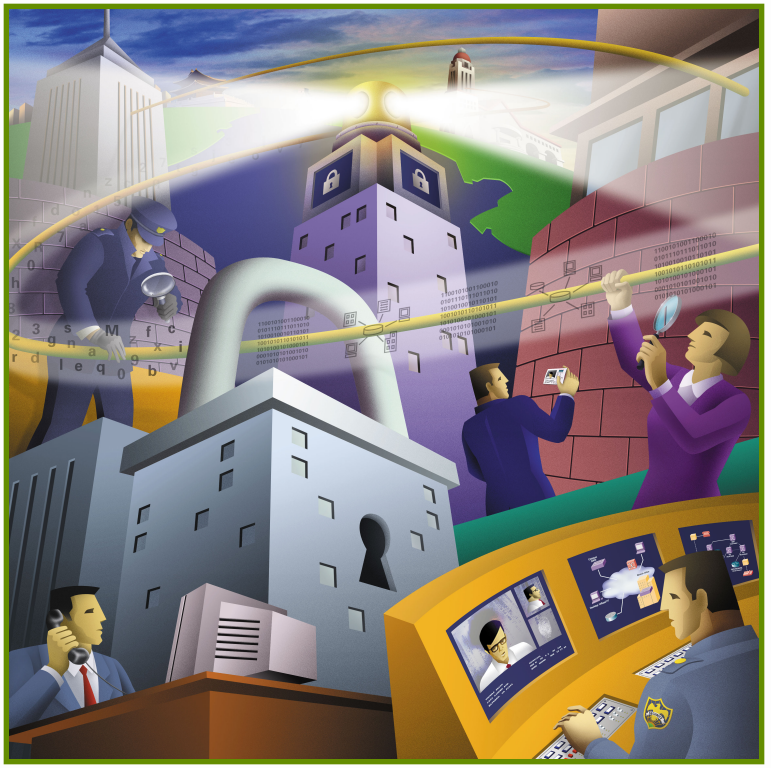
Build the Communications Channels to your Vendors

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 ISP 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.

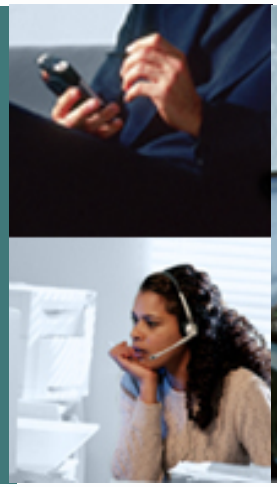
Hardware Vendor's Responsibilities

- Cisco System's example:
  - Operations people working directly with the ISPs
  - Emergency reaction teams (i.e. PSIRT)
  - Developers working with customers and IETF on new features
  - Security consultants working with customers on attacks, audits, and prosecution
  - Individuals tracking the hacker/phracker communities
  - Consultants working with governments/law enforcement officials

The Cisco PSIRT

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

Tools and Techniques



110

More Questions

- Have your taken the proactive step to be Prepared?
  - Build and Prepare OpSEC team
  - Securing the router
  - Securing the routing protocols
  - Route filtering
  - Black hole filtering
  - Sink Hole routers/networks
  - Packet filtering
  - Securing the network
  - Default routes, ISPs, and security

Phase 1 - Preparation

- Preparation is critical!
  - You know your *customers* are going to be attacked
  - It is not a matter of if but how often and how hard
  - The Internet is not a nice place anymore!
  - Think battle plans
- Militaries know the value of planning, practice, drilling and simulation
  - Those that are prepared will be victorious.

The Preparation Problem

CEO, “Customer X just called and said they’ve been DOSed for the past 12 hours. What are we doing about it?”

Operations Chief, “We’re working on it.”

CEO, “How long before it is fixed?”

Operations Chief, “We’re working on it.”

CEO, “What exactly are we doing about it?”

Operations Chief, “We’re working on it.”

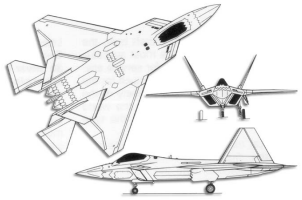
CEO, “Do you know how to get the customer up and running?”

Operations Chief, “It is all Cisco’s fault – they should fix the *DOS problem*.”

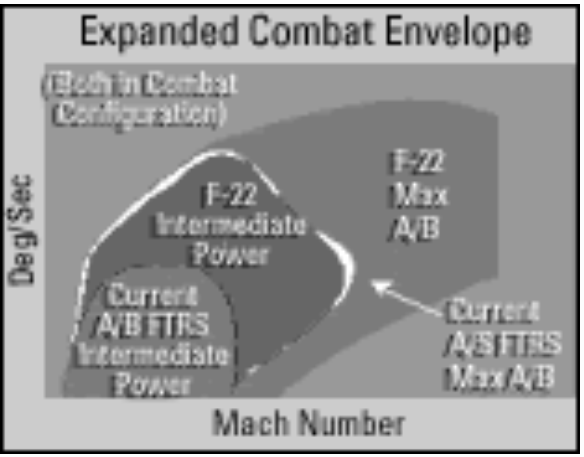
Prepare: Tools and Techniques

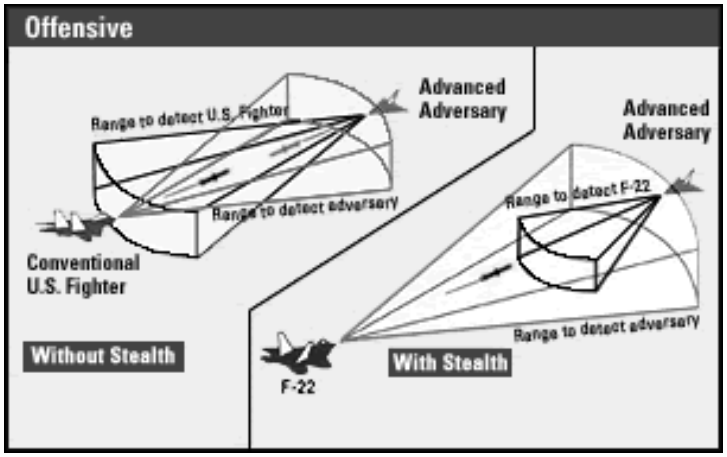
- Prepare your Tools!
  - Do you have all your SNMP tools deployed?
  - Do you have all your SYSLOG tools deployed?
  - Do you have your ACLs created?
  - Do you have your scripts created?
  - Have you built and tested your *Sink Hole* and *Backscatter* tools?
  - Etc.

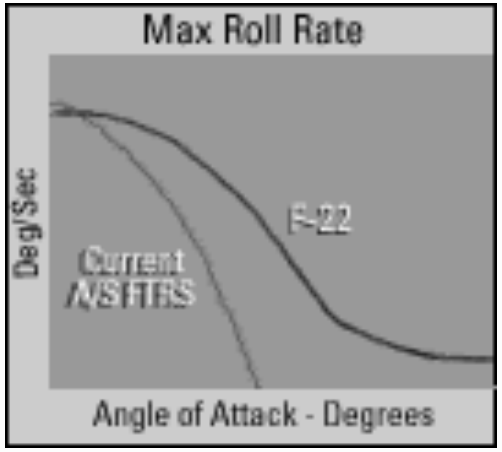
Are you pushing the *envelo*



- Know your Equipment and Infrastructure:
  - Know the Performance Envelop of all your equipment (routers, switches, workstation, etc). You need to know what your equipment is really capable of doing. If you cannot do it your self, make is a purchasing requirement.
  - Know the capabilities of your network. If possible, test it. Surprises are not kind during a security incident.







Are you pushing the *envelop?* *Get Real!*

- Operator, “I tired to push my aircraft to 70,000 ft and it stalled.”
- Vendor, “But the aircraft was only designed for a 50,000 ft ceiling.”
- Operator, “I need it to go to 70,000 ft, so you should make that happen.”
- Vendor, “But that is not going to happen, 50K ft is the only thing it can do. You knew that when you bought it.”
- Operator, “Your equipment sucks if you cannot exceed you design specs.”

Network Size and Complexity

- Are these traffic patterns normal for our network?
- What is using up all of our bandwidth?
- Angry customers are calling - what happened?
- Why can't we reach that server, network or AS?
- Has another provider hijacked our routes?
- Should we buy more transit or peer directly?
- Should we change these BGP attributes or policies?

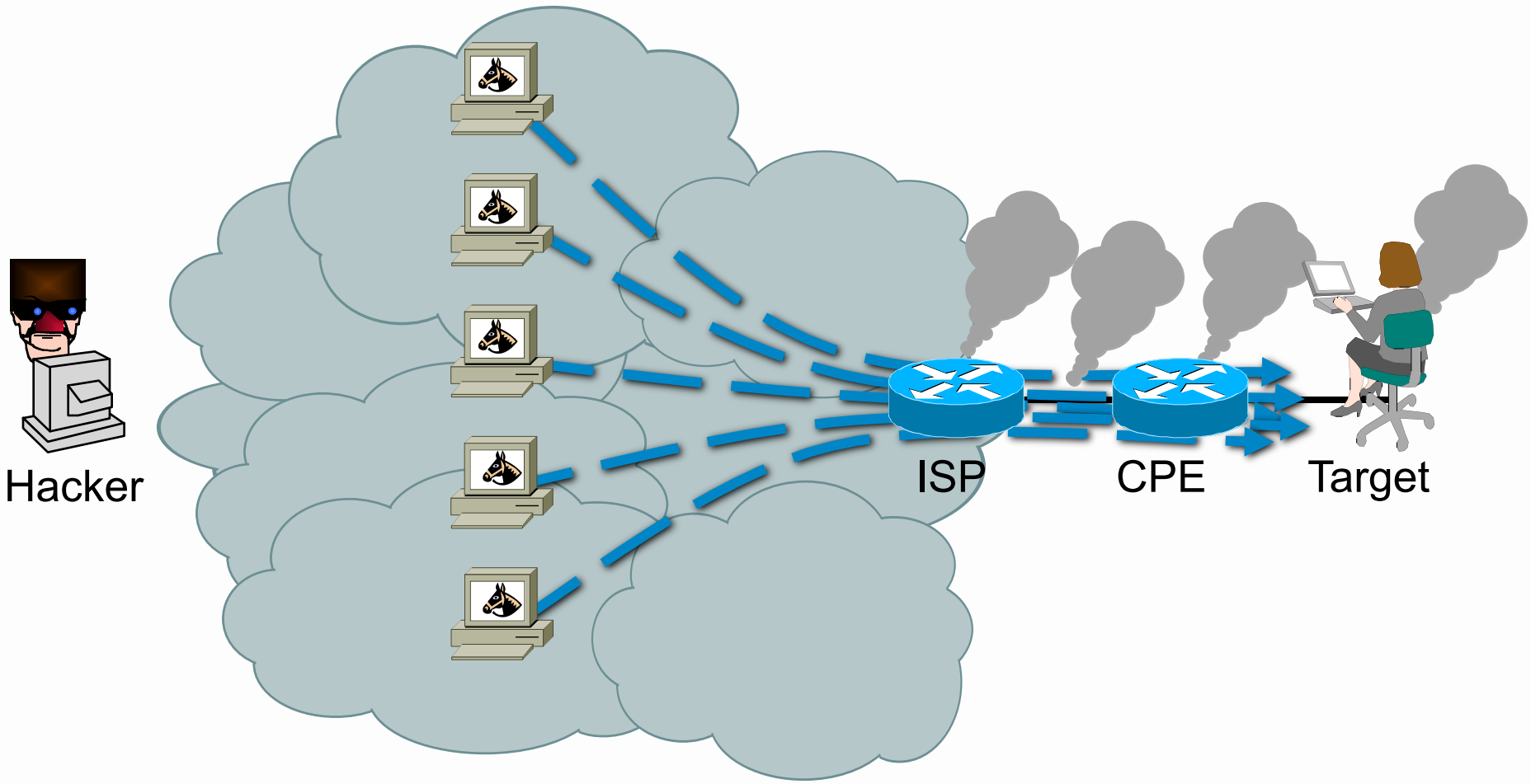
Preparation (1)

- Preparation: All the work the ISP does to prepare he network, create the tools, test the tools, develop the procedures, train the team, and practice.
  - #1 Most critical phase of how a ISP responds to a security incident.
  - Big difference between ISPs who have prepared and those who have done nothing.

What can you do?

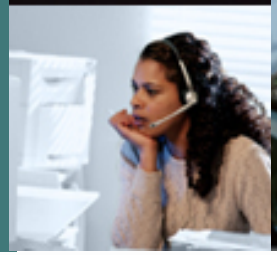
1. Ask lots of security questions. Cisco is not holding anything back, we just have way too much information for any one person to process.
2. Follow-up on security questions. Your Cisco contacts may have to dig for the answers. Don't let them get distracted.

What Do You Tell the Boss?



- Common Sense, a method to the madness of a security incident helps the team focus and work the problem with fewer digressions.
- The question is what method works in today's turbo worm environment?

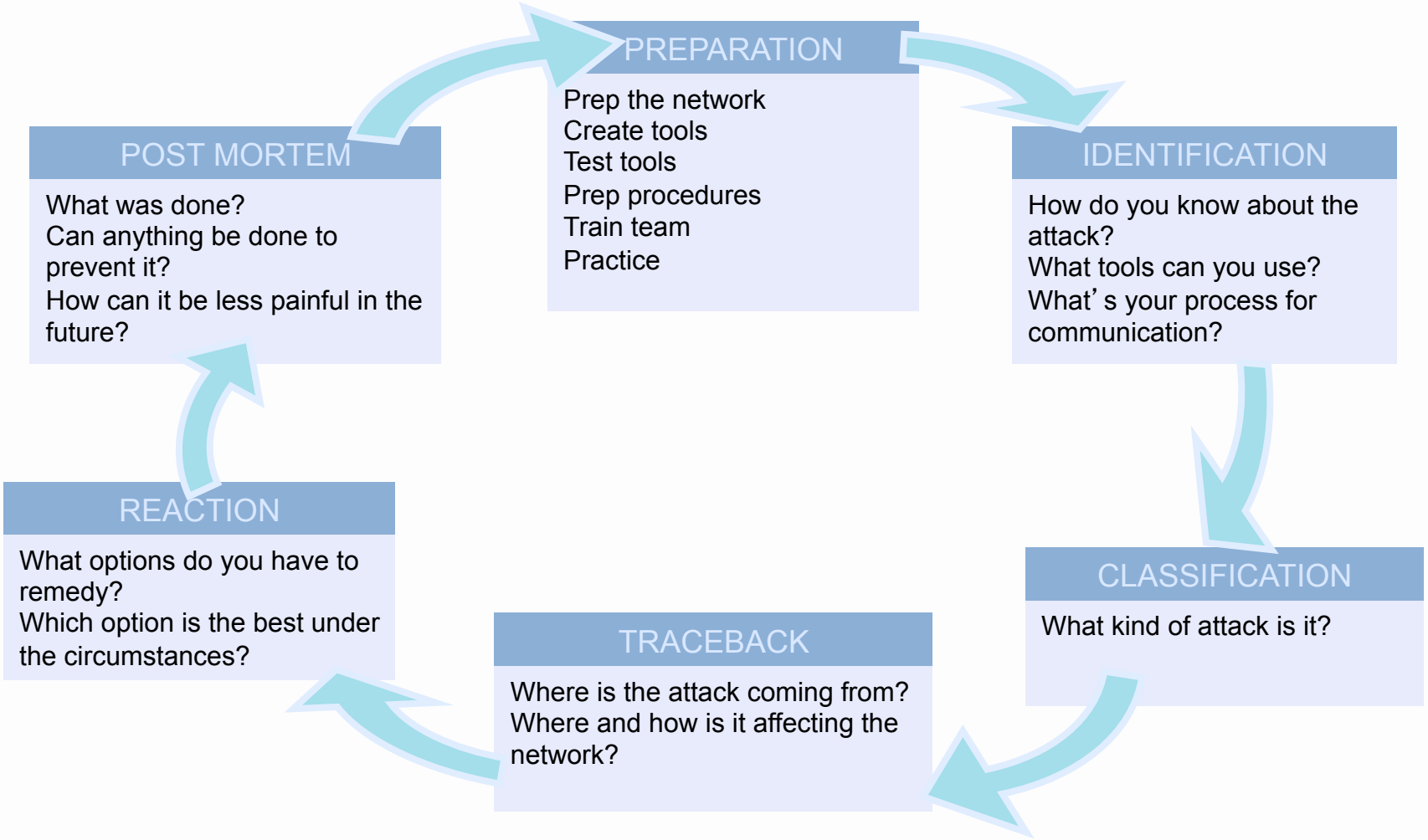
SIX-PHASE METHODOLOGY



Preparation Is Everything!

- We, the Cisco's OPSEC Community, know that preparation with a guiding methodology is the #1 difference between networks that survive the crisis and those who live weeks in network hell
- We've seen it during:
  - Code Red/Nimda
  - Slammer
  - DOS attacks
  - BotNet attacks
- Bottom line—if you do not have a method to dig yourself out of the madness, then your life as a operations engineer will be painful

Six Phases of Incident Response

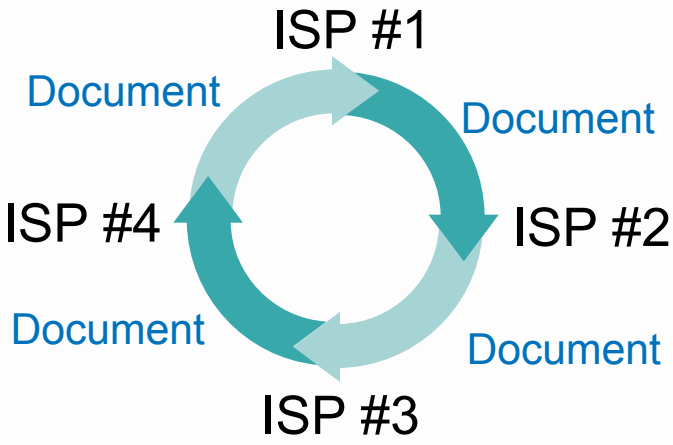


SP Security Incident Response

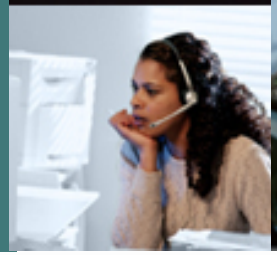
- Given that ISPs are transit networks, the way incident response happens is slightly different from other networks
- More effort is made to mitigate the effects of the attack and trace it back upstream to its source
- Working with SP Security Teams have demonstrated six distinct phases in the way ISPs response to security incidents

Where Did These Come From?

- Evolving operational model that has been adopted as a Best Common Practice (BCP)
- Cisco has been a documentation facilitator—helping to share concepts, practices, and procedures between providers
- The Six Phases approach evolved out of the Feb ’00 DDOS attack post mortem dialectic



PHASE 1
PREPARATION



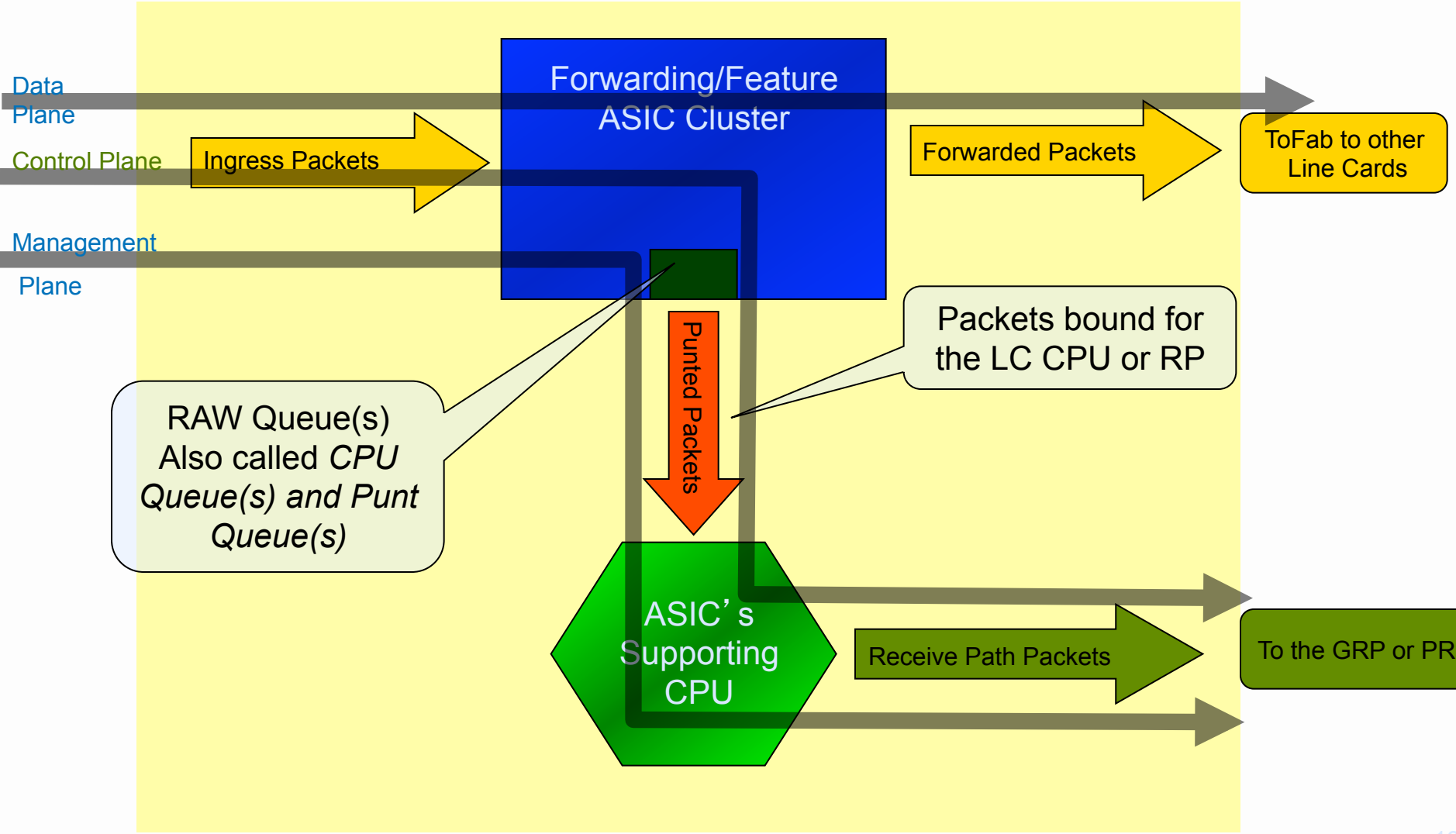
Preparation

- Preparation: All the work the ISP does to prepare he network, create the tools, test the tools, develop the procedures, train the team, and practice
  - #1 Most critical phase of how a ISP responds to a security incident
  - Big difference between ISPs who have prepared and those who have done nothing

Preparation

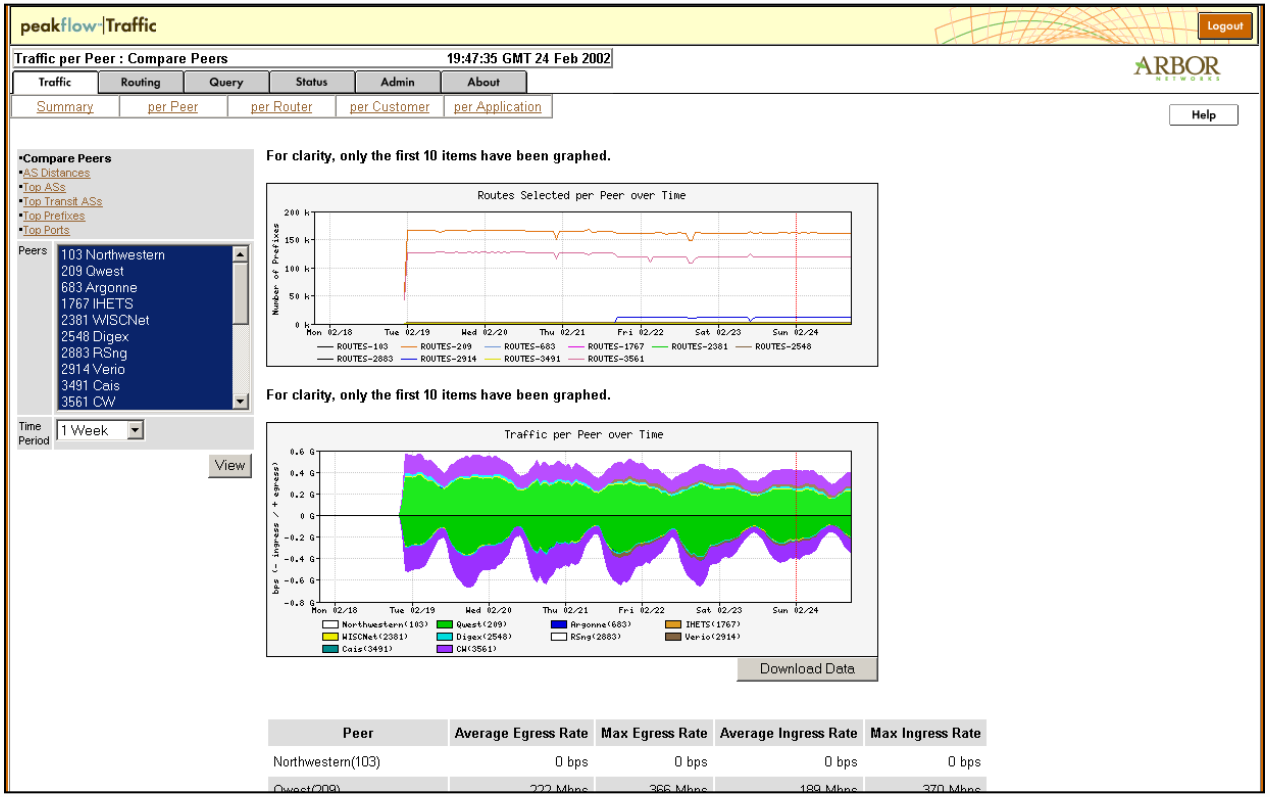
- Know the enemy
- Create the security reaction team
- Prepare the management plane
- Prepare the control plane
- Prepare the data plane
- Prepare the tools

The Three Planes



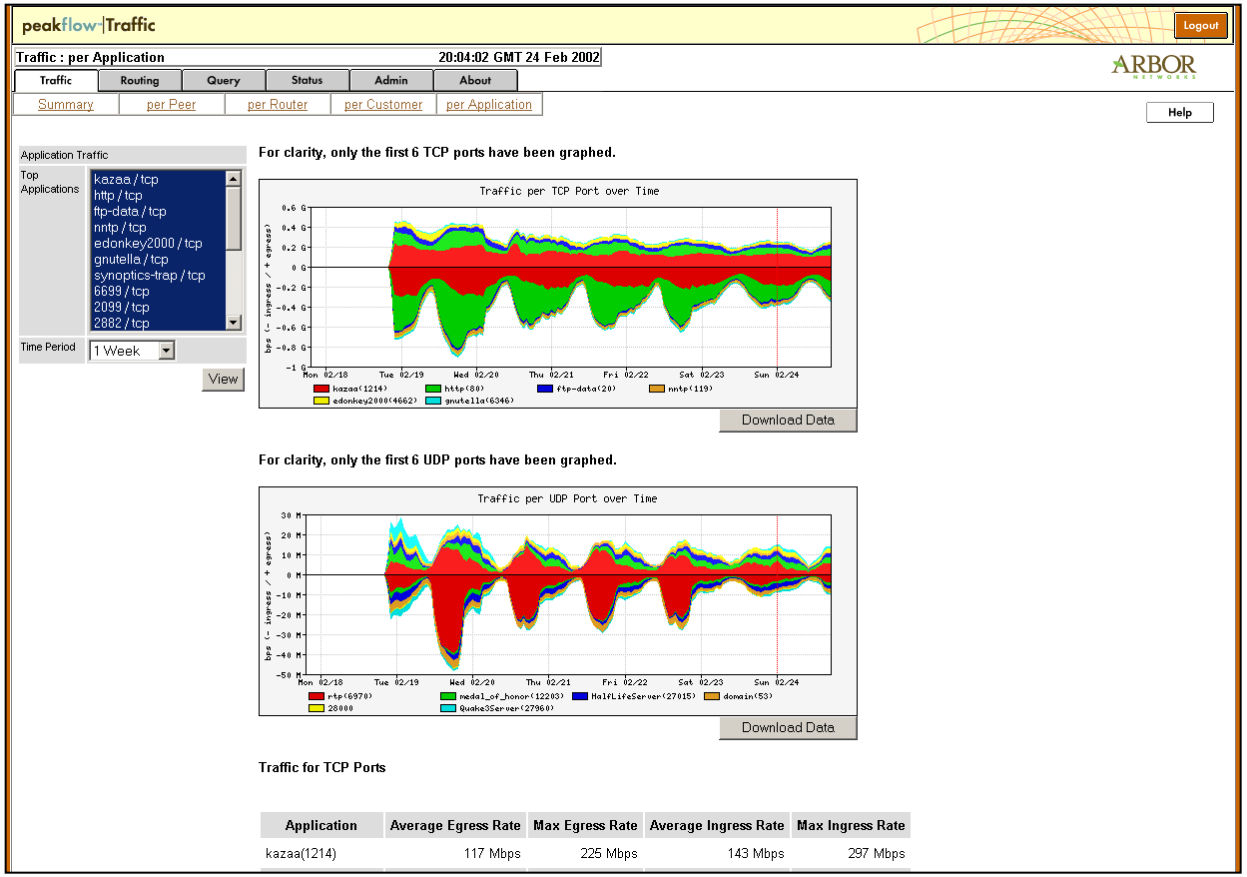
Network Traffic (Real-Time and Historical)

- Detect large shifts in traffic
- Delta (Changes)
- Track/trigger on peer traffic changes
- Monitor top ASes, transit ASes, prefixes and ports

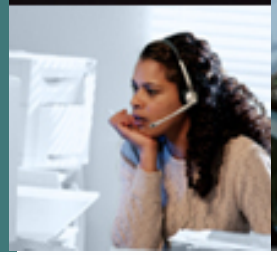


Bandwidth Consumption

- Profile network-wide utilization by:
  - Peer
  - Router
  - Interface
    - *Packet Per Seconds*
    - *Bandwdith*
  - Department / Subnet
  - Application



PHASE 2
IDENTIFICATION



Identification

- Identification—How do you know you or your customer is under attack?
  - It is more than just waiting for your customers to scream or your network to crash
  - What tools are available?
  - What companies are working on tools?
  - What can you do today on a tight budget?

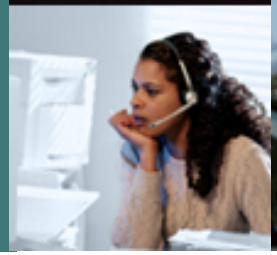
Ways to Detect

- Customer call – Most effective
- Unexplained changes in network baseline
  - SNMP: Line/CPU overload, drops
  - NetFlow
  - Arbor's Peakflow DoS (partner product)
- ACLs with logging
- Backscatter
- Sniffers

Identifying Attacks

- Proactively monitor internal and “dark IP space”
- Build baselines for all traffic to expose anomalous behavior
- Utilize tools that enable network-wide correlation of control and data planes (e.g., CPU utilization, route stability, Netflow, etc..)
- Notify your customers before they notify you—be proactive!

PHASE 3
CLASSIFICATION



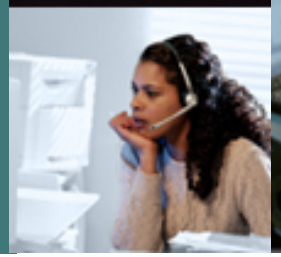
Classification

- Classification—Understanding the type of attack and what damage is it causing
  - You need to know what you (or your customer) are getting hit with
  - Determines the rest of the incident response
  - What tools are available?
  - How can you do this without crashing my router?

Classification

- What type of attack has been identified?
- Qualify and quantify the attack without jeopardizing services availability (e.g., crashing a router):
  - What type of attack has been identified?
  - What's the effect of the attack on the victim(s)?
  - What next steps are required (if any)?

PHASE 4 TRACEBACK



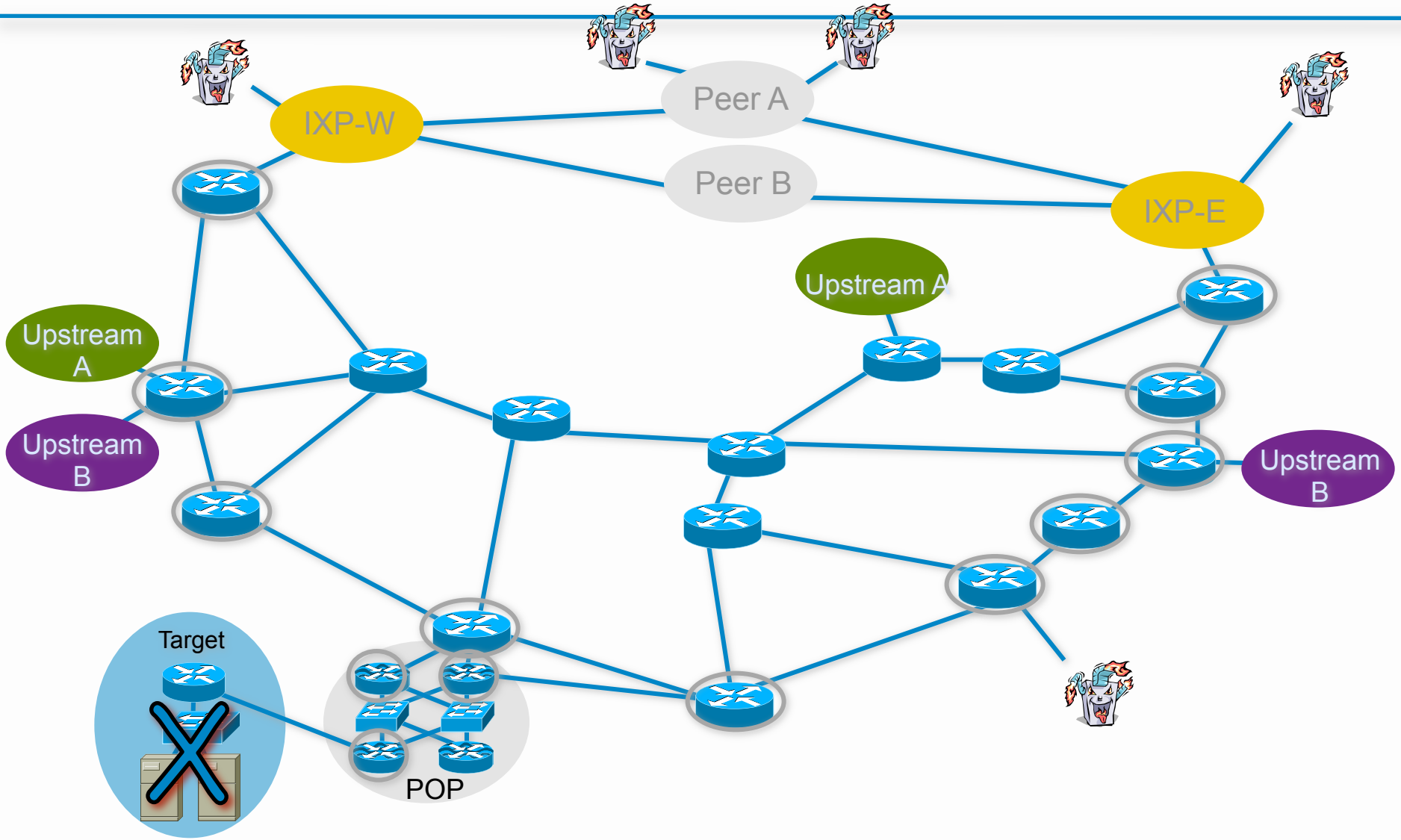
Traceback

- Traceback—From where is the attack originating?
  - Deterrence works. Traceback a few attacks to their source, capture the attacker, prosecute, and lock them up and you will have a credible deterrence.
  - Foundation techniques
  - How to traceback to the edge of the network?
  - How to continue traceback over the ISP—ISP boundary

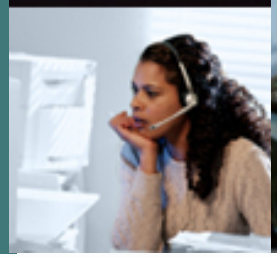
Traceback

- Traceback to network perimeter
  - Netflow
  - Backscatter
  - IP source tracker
- Retain attack data
  - Use to correlate inter-domain traceback
  - Required for prosecution
  - Deters future attacks
  - Clarify billing and other disputes
  - Post-mortem analysis

Traditional Traceback



PHASE 5
REACTION



Reaction

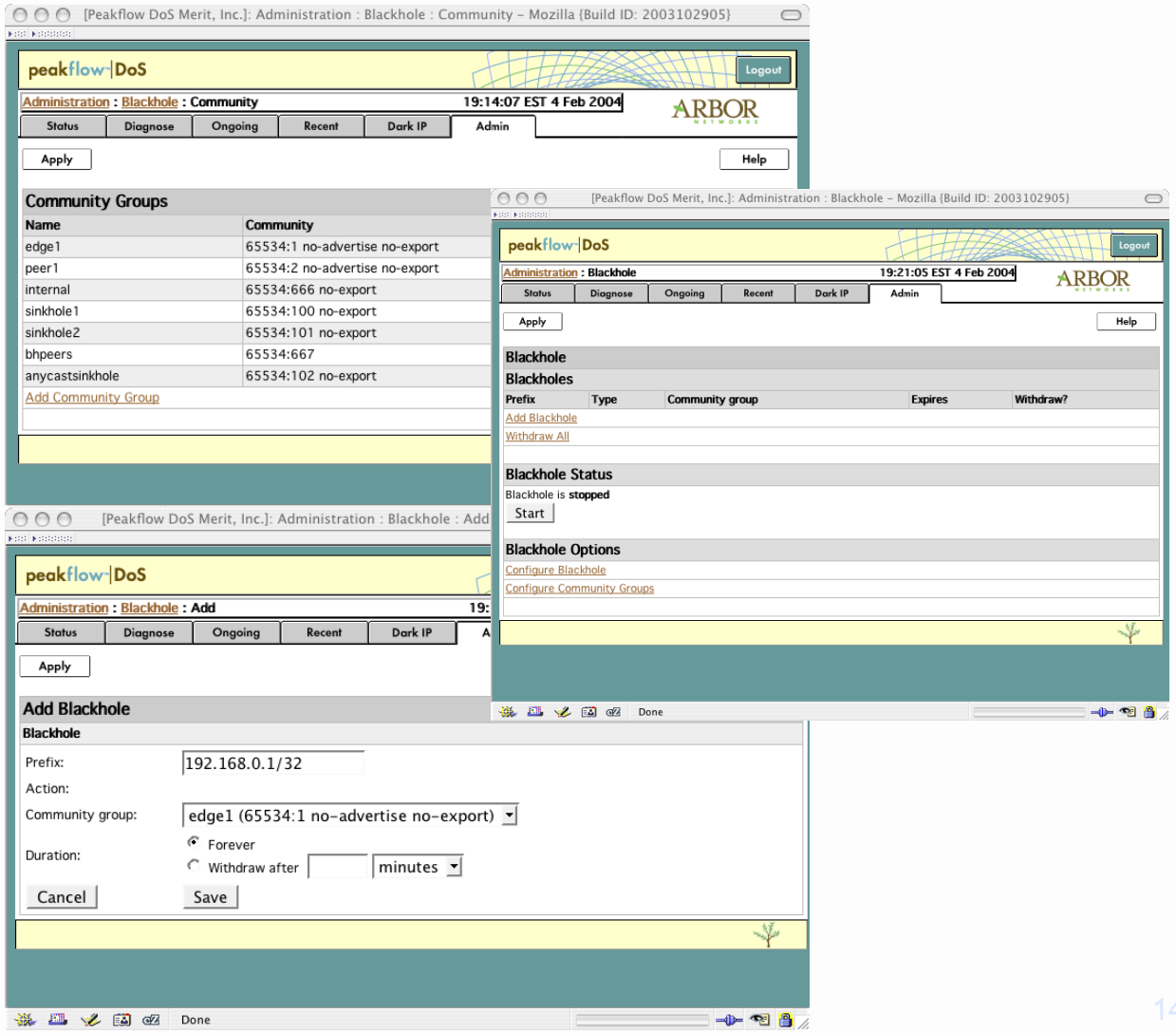
- Reaction—Doing something to counter the attack —even if you choose to do nothing
  - Should you mitigate the attack?
  - It is more then just throwing an ACL onto a router
  - How to keep the attack from shifting from your customer to your network?

Potential Responses

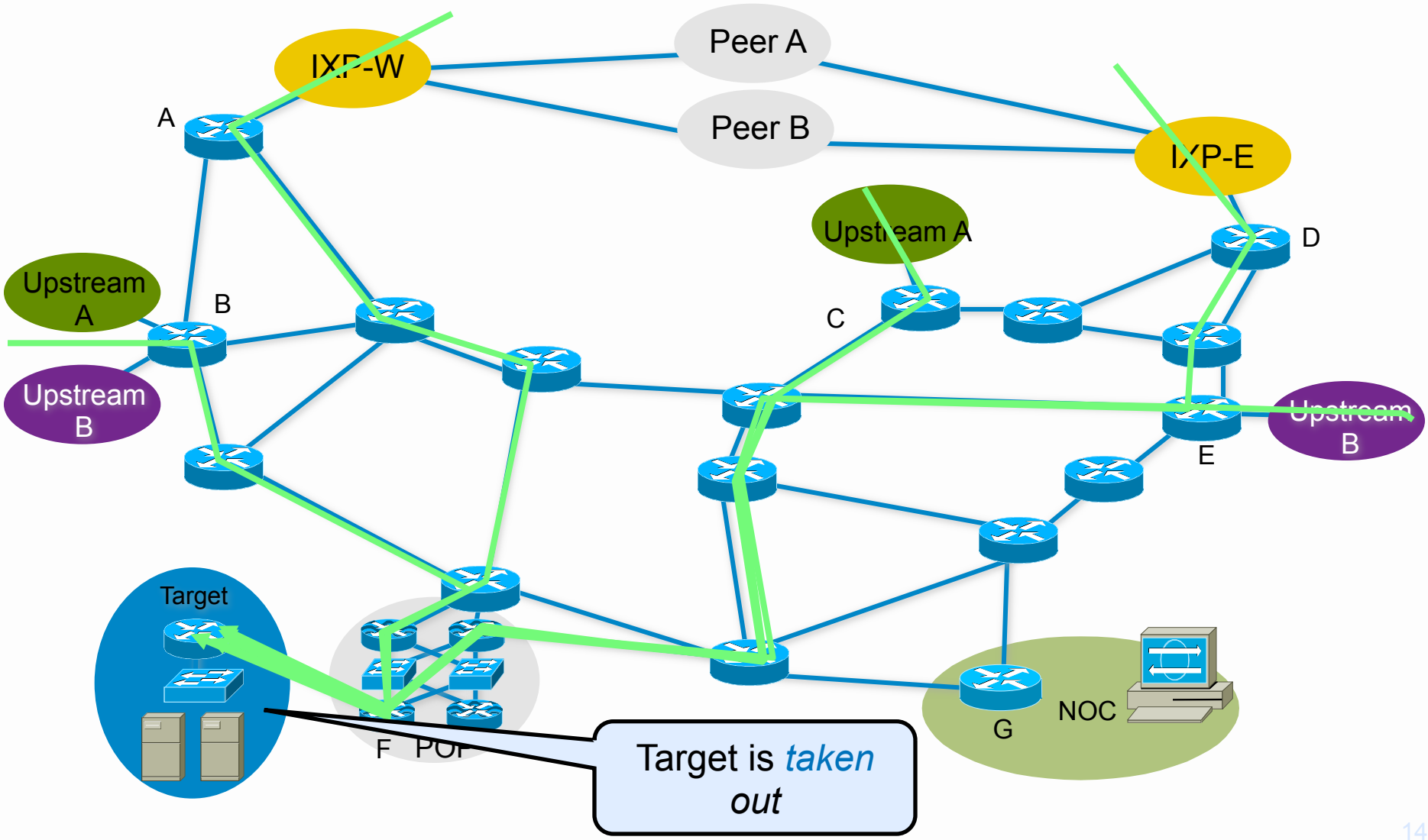
- Do nothing
- Notify customer
- Packet filters (e.g., ACLs or firewalls)
- Rate limits (e.g., CAR)
- Redirect to sinkholes and analyze or scrub packets?
- Remote-triggered drop
  - Blackhole (dst == Null 0)
  - uRPF loose check (src == Null 0)
  - Customers may perform

BGP Trigger Router Functions

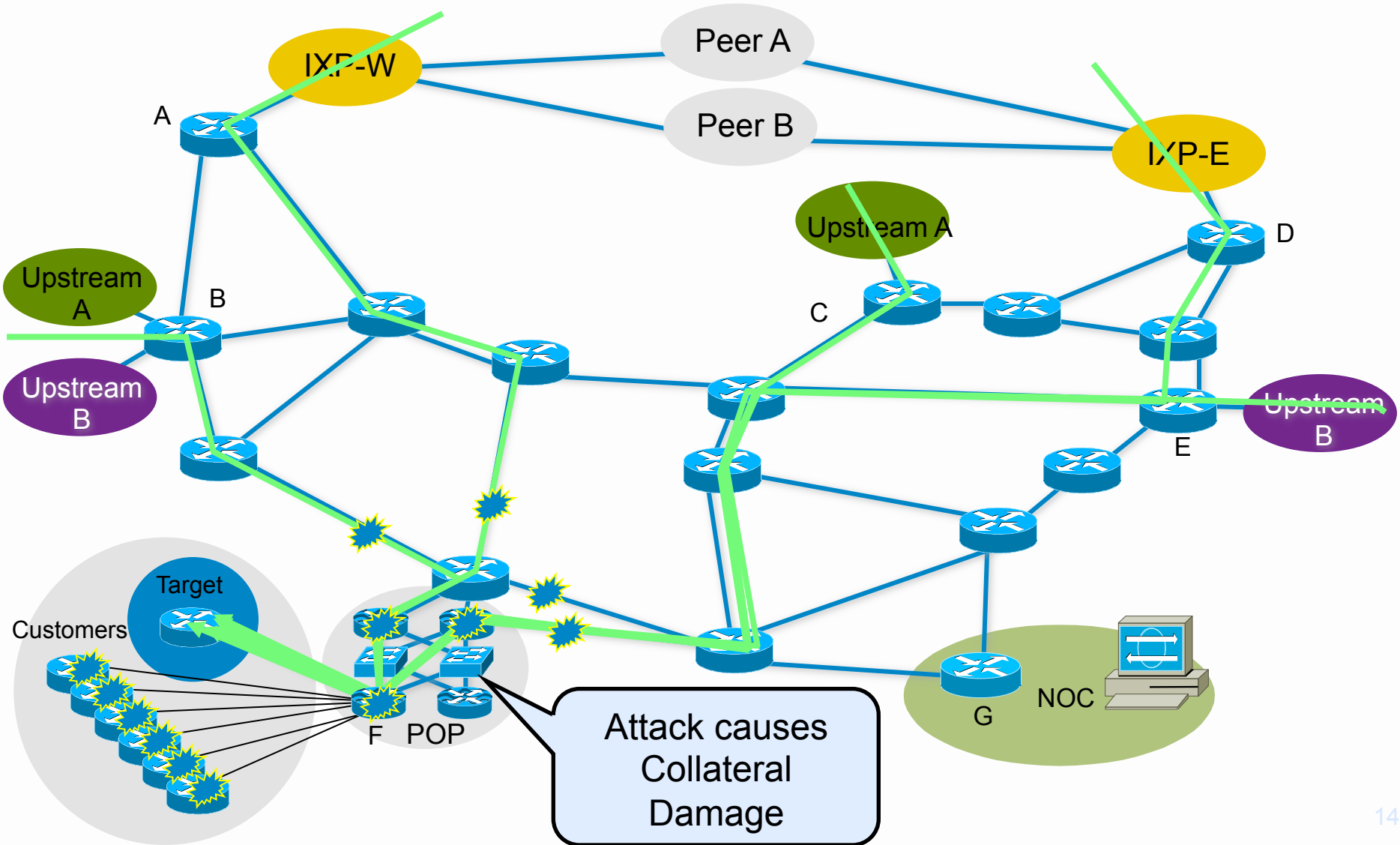
- Blackhole
  - Peering edge
  - All edge
  - Core
- Sinkhole diversion
  - Anycast
  - Centralized
  - Scrubber data



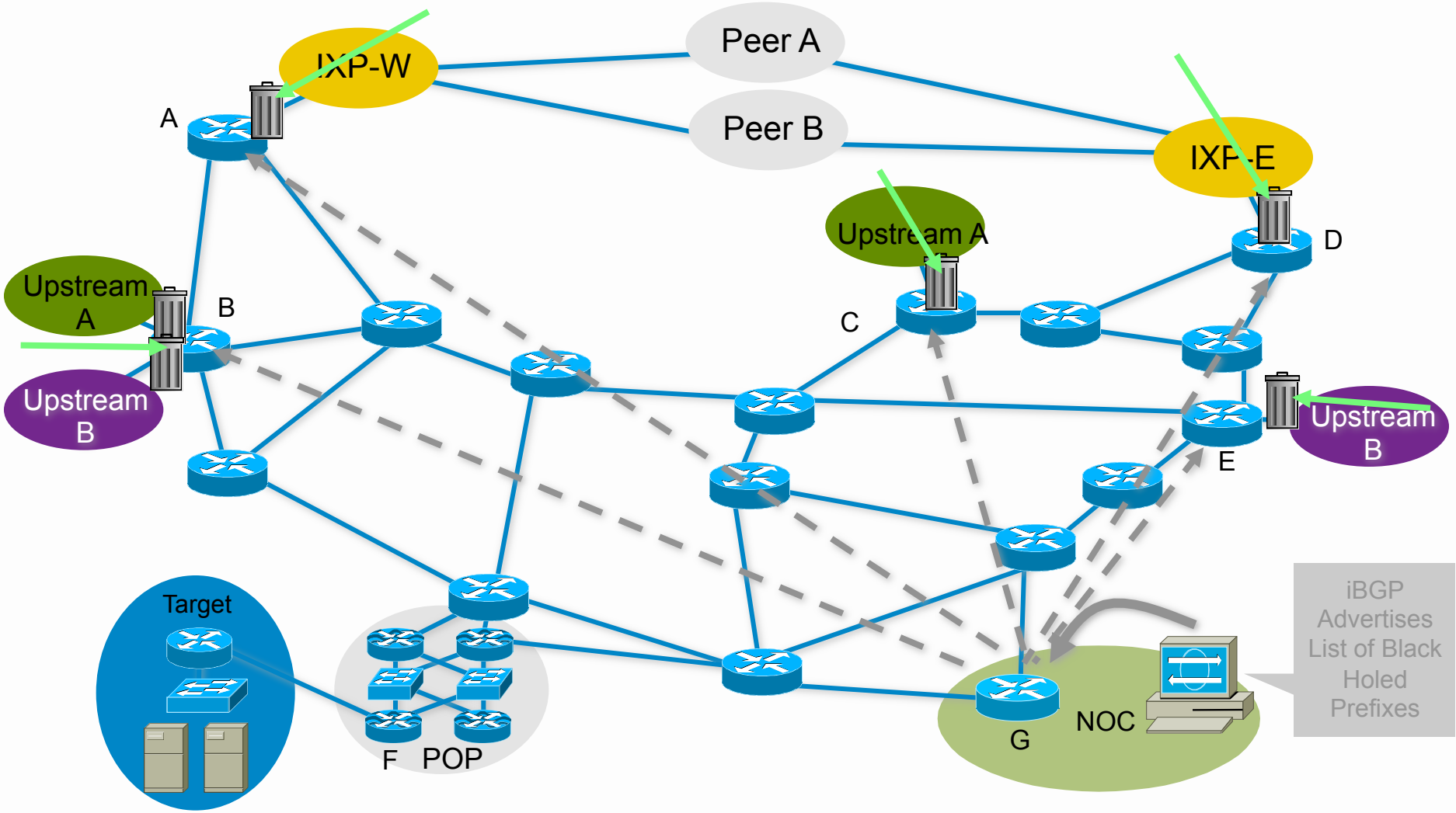
Customer Is DOSed—Before



Customer Is DOSed—Before—Collateral Damage



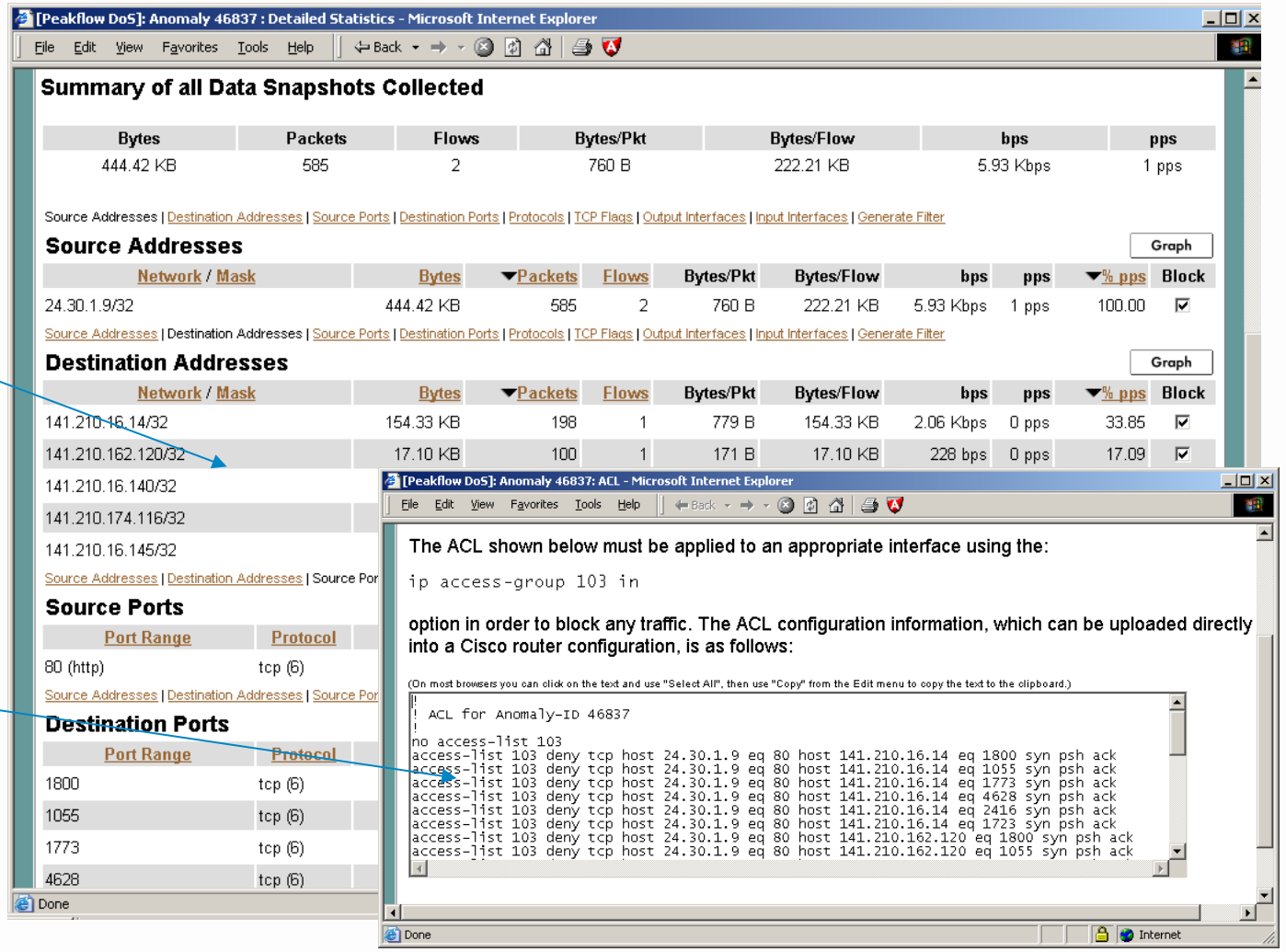
Customer Is DOSed—After—Packet Drops Pushed to the Edge



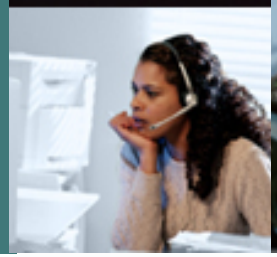
Filter

Presents a detailed fingerprint for the attack.

Generates the appropriate ACL/CAR or firewall filter for blocking attack.



PHASE 6
POST MORTEM



152

Post Mortem

- Post Mortem—Analyzing what just happened. What can be done to build resistance to the attack happening again
  - The step everyone forgets!
  - Was the DOS attack you just handled, the real threat? Or was it a smoke screen for something else that just happened?
  - What can you do to make it faster, easier, less painful in the future?

Post Mortem

- Analyze data, trends and discuss attack
- Fully history of attack(s), trends, etc..
- Determine what, if anything, could have been done to be better prepared—make appropriate modifications if necessary
- Summarize major incidents for the NOC alias
- BLOG