Welcome!

APNIC Security Tutorial

ISP Infrastructure Security Strategy

22 February 2005, Kyoto, Japan

In conjunction with APNIC19 / APRICOT 2005

Schedule

- Introduction to ISP infrastructure security
- Threats and Attacks types
- The six-phase strategy to managing ISP security process

Acknowledgement

Thanks to the following for their help and permission in using materials from their presentations:

- Barry Greene (Cisco Systems)
- Christopher L. Morrow (UUNET)

Introduction to ISP security

ISP security threats

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

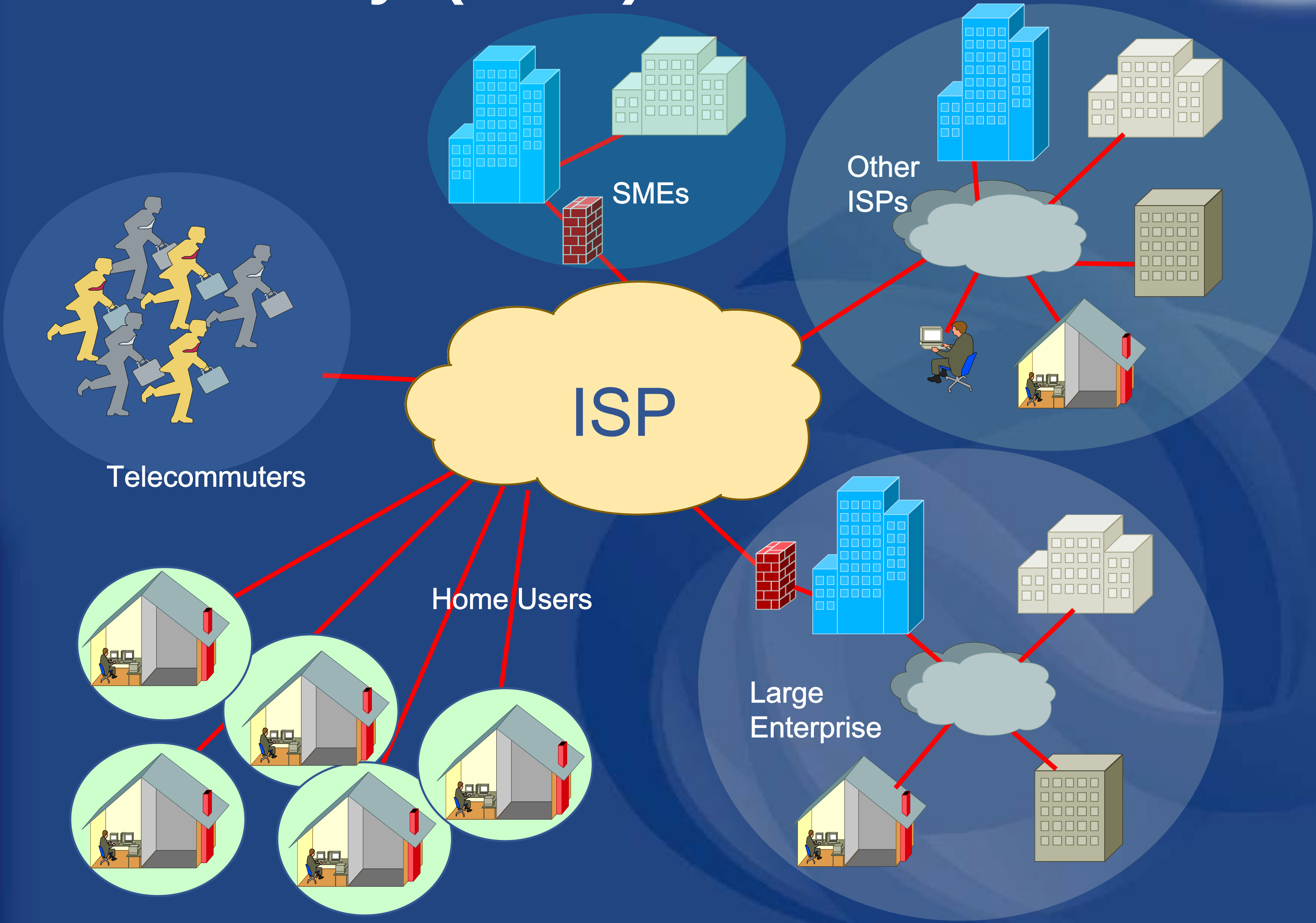
Vint Cerf

ISP’s today

Customer type

- Large enterprise
- Small and medium enterprise
- Home users
- Telecommuters
- Other ISPs

ISP’s today (cont.)

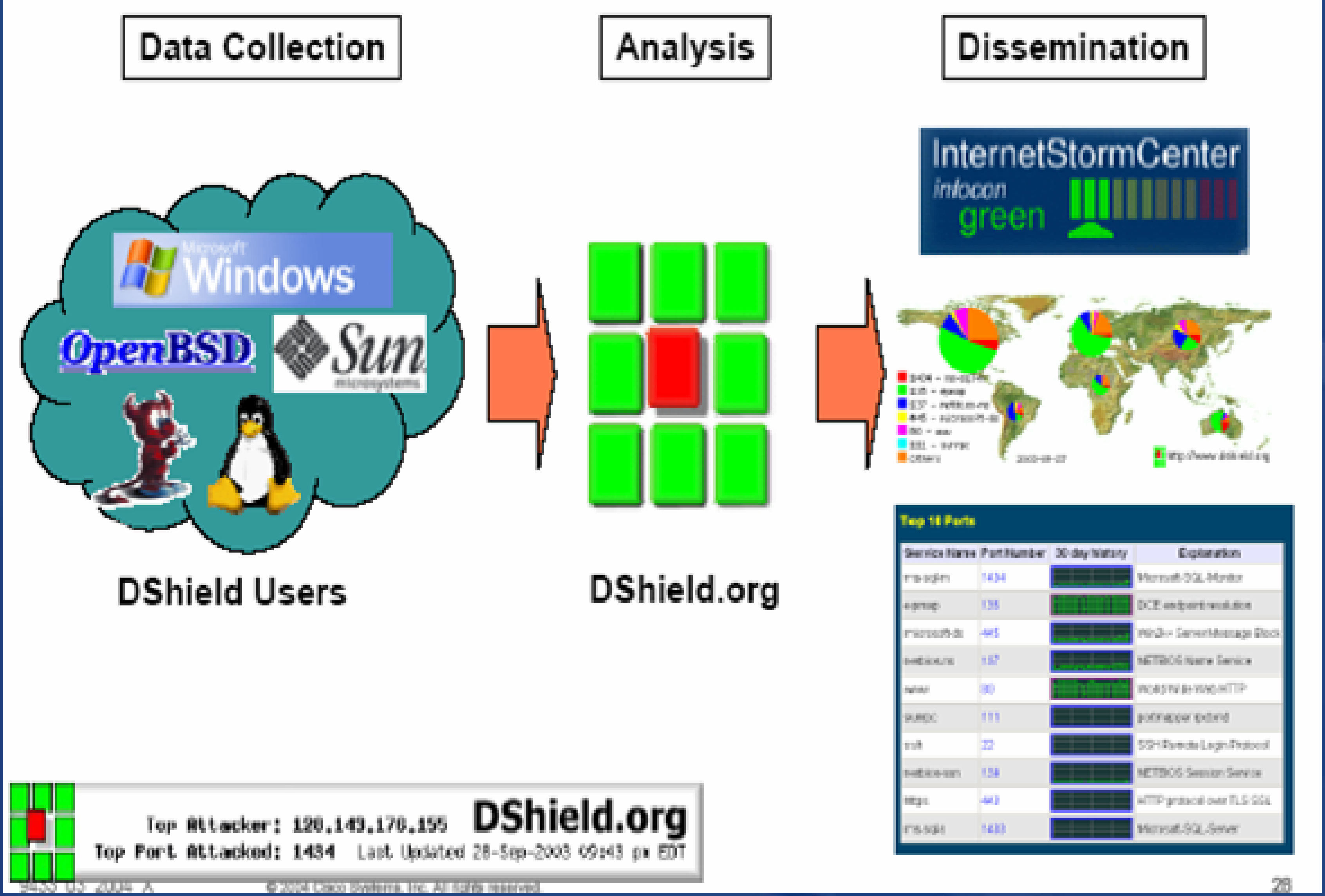


ISP’s today

Changing threat

- Hacker tools are easy to find and can cause damage to any networks connected to the internet
- eCommerce services add motivation to hackers
- Direct attacks on the internet service providers infrastructure
- ISPs regularly receive many calls per day from customers to help defend against attacks

Attack trends



DShield Users

DShield.org

Top 10 Ports

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

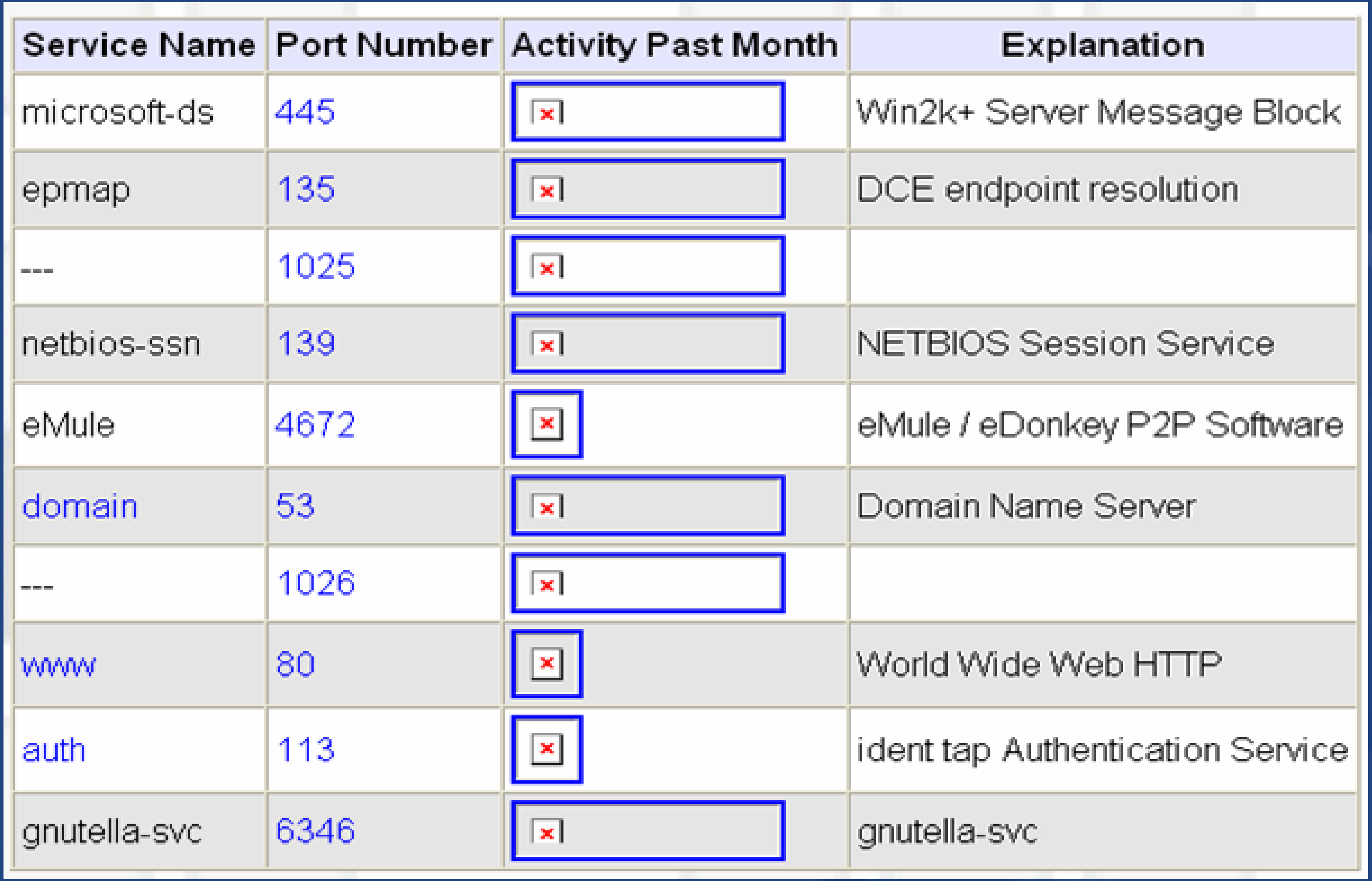
DShield.org

Top Attacker: 120.143.170.155

Top Port Attacked: 1434 Last Updated 28-Sep-2003 05:43 pm EDT

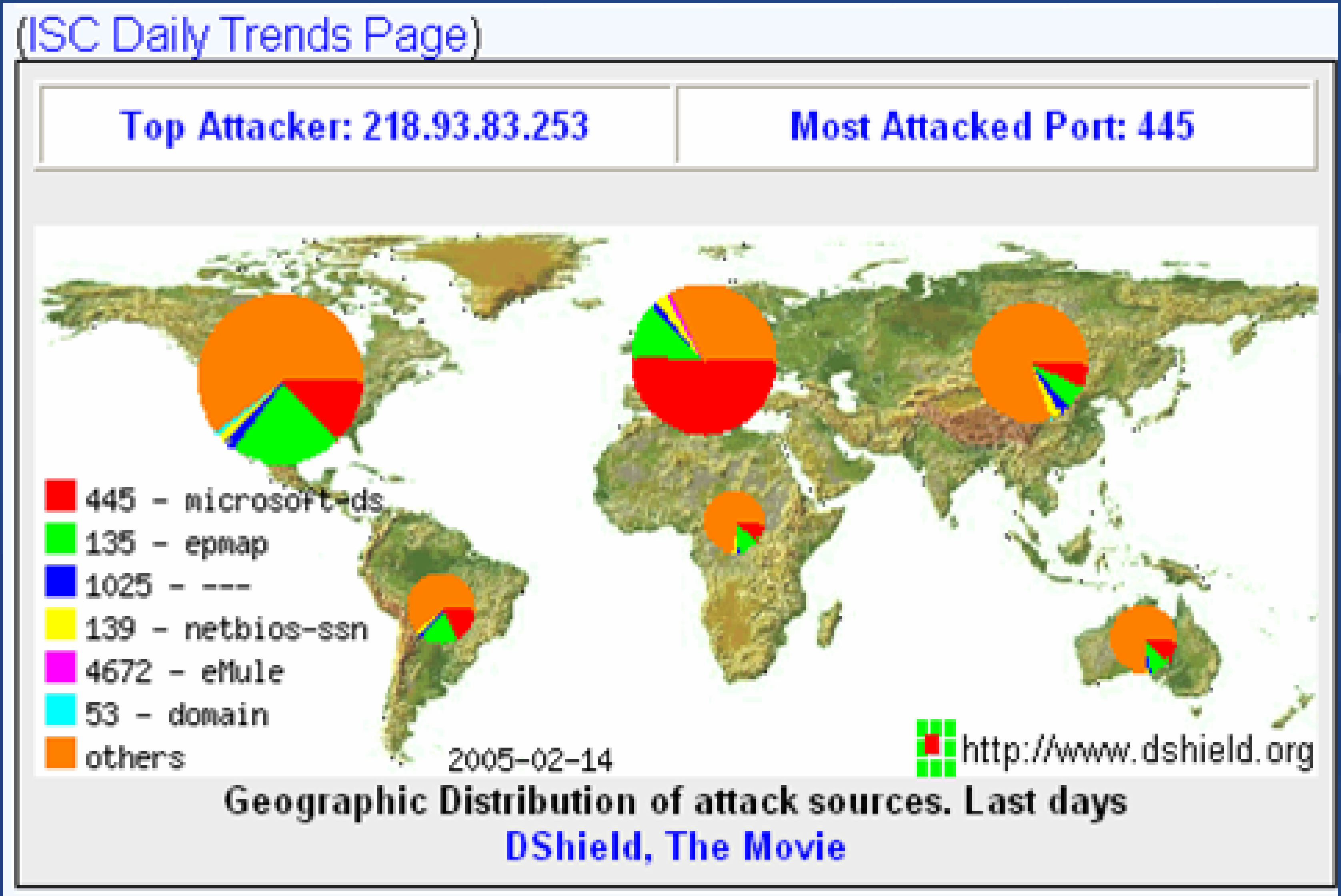
Attack trends (cont.)

- Top 10 most probed port from www.dshield.org



Service Name	Port Number	Activity Past Month	Explanation
microsoft-ds	445	☒	Win2k+ Server Message Block
epmap	135	☒	DCE endpoint resolution
---	1025	☒	
netbios-ssn	139	☒	NETBIOS Session Service
eMule	4672	☒	eMule / eDonkey P2P Software
domain	53	☒	Domain Name Server
---	1026	☒	
www	80	☒	World Wide Web HTTP
auth	113	☒	ident tap Authentication Service
gnutella-svc	6346	☒	gnutella-svc

Attacks trends distribution



(ISC Daily Trends Page)

Top Attacker: 218.93.83.253	Most Attacked Port: 445

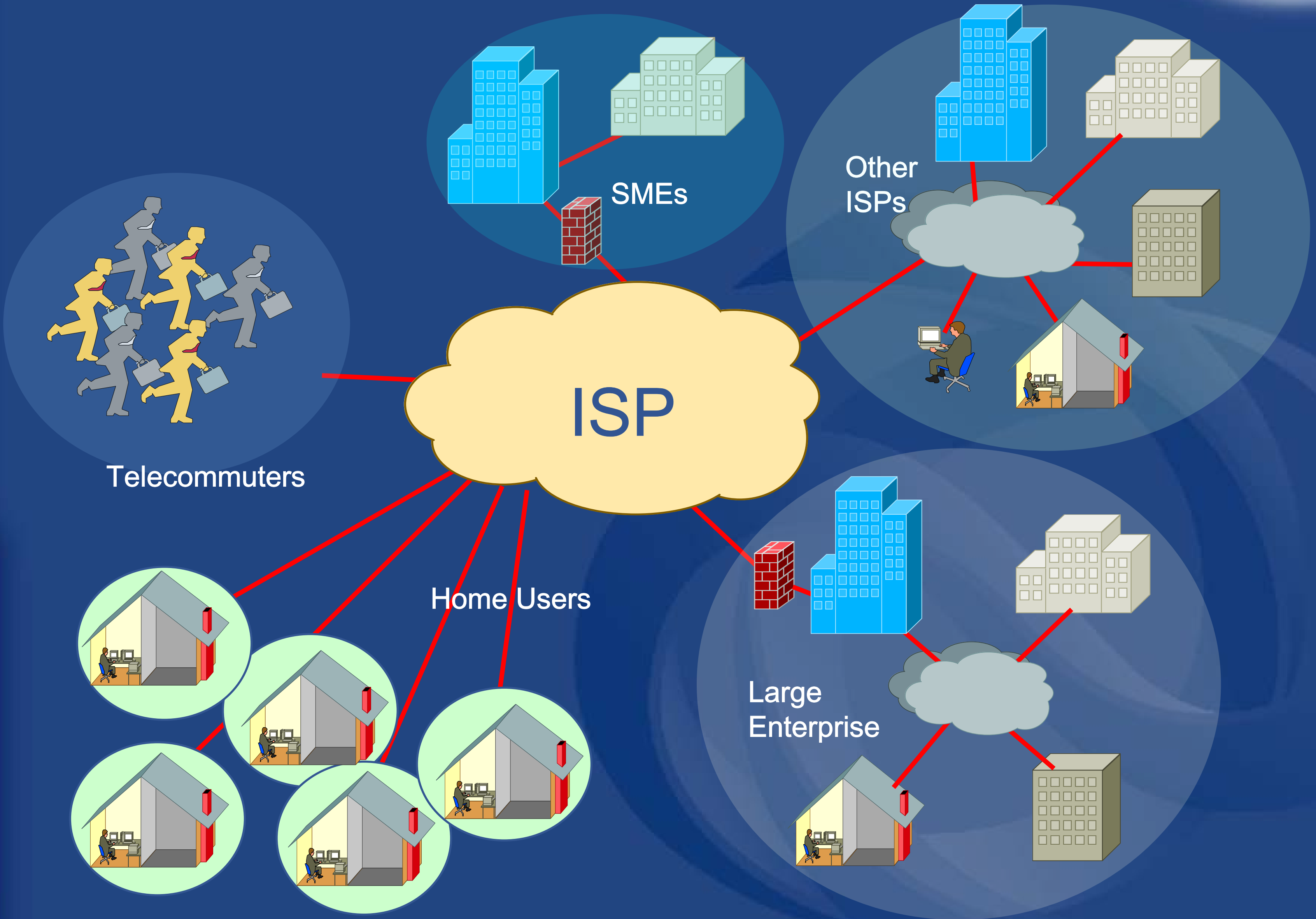
Geographic Distribution of attack sources. Last days

DShield, The Movie

ISP infrastructure

- ISP network infrastructure are the new ground for different types of attacks
  - Enterprise Networks
  - SME networks
  - Home Users
  - Telecommuters
  - Other ISPs

ISPs Network



ISP roles

Service provider roles

- Deliver better service connection to customers even though being exposed to attacks
  - – 24/7 connection availability
  - – Connection reliability
  - – Minimum hours of network down time
  - – Service level agreements

ISP roles (cont.)

- Protect other peers
- Protect customers from attack whether it is coming from:
  - Own Infrastructure
  - Other customers
  - Internet users

ISP security

Key points:

- Protect your network
- Provide protection to customers from internet users
- Protect the internet from your customers
- Always be ready for any attacks because at any given time there is a possibility…

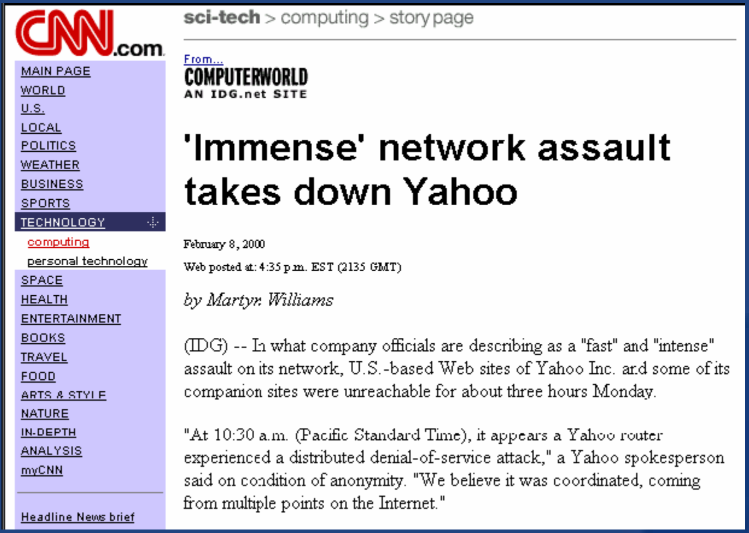
ISP security actions

First priority: protect the router from any attack.

- **Protect the router from any types of attack either** *Direct attack* **or** *Break-in*
  - **Protect the Routing Protocol from any** *Direct attack* **or** *Route insertion*
  - **Protect the Network from** *Direct attack* **or** *Redirection*
- **Conduct Trace Back measures and Stop/Rate-Limit them on the edge of the Network**
- **Collect data of the attack for further analysis and possible Law enforcement actions.**

Example of attacks to ISP's network

DOS = Denial of Service
DDOS = Distributed Denial of Service



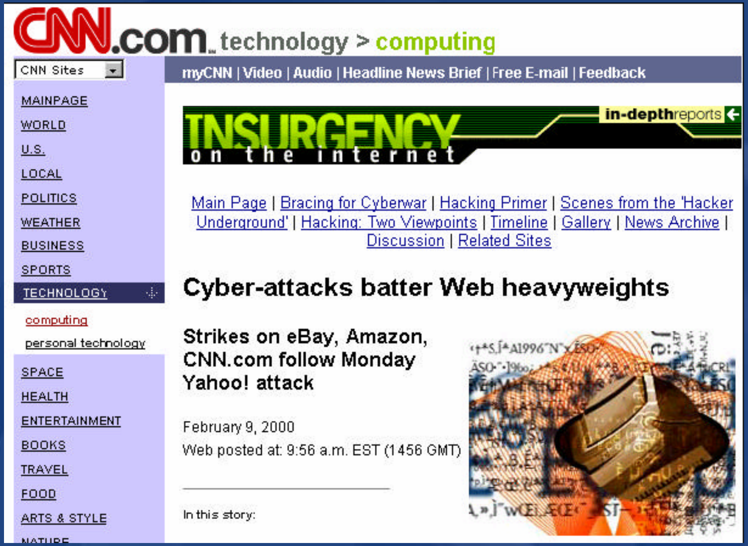
'Immense' network assault takes down Yahoo

February 8, 2000
Web posted at: 4:35 p.m. EST (2135 GMT)

by Martyn Williams

(IDG) -- In what company officials are describing as a "fast" and "intense" assault on its network, U.S.-based Web sites of Yahoo Inc. and some of its companion sites were unreachable for about three hours Monday.

"At 10:30 a.m. (Pacific Standard Time), it appears a Yahoo router experienced a distributed denial-of-service attack," a Yahoo spokesperson said on condition of anonymity. "We believe it was coordinated, coming from multiple points on the Internet."


CNN.com technology > computing
CNN Sites
myCNN | Video | Audio | Headline News Brief | Free E-mail | Feedback
MAINPAGE
WORLD
U.S.
LOCAL
POLITICS
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
BOOKS
TRAVEL
FOOD
ARTS & STYLE
NATURE
INSURGENCY on the internet
in-depth reports
Main Page | Bracing for Cyberwar | Hacking Primer | Scenes from the 'Hacker Underground' | Hacking: Two Viewpoints | Timeline | Gallery | News Archive | Discussion | Related Sites

Cyber-attacks batter Web heavyweights

Strikes on eBay, Amazon, CNN.com follow Monday Yahoo! attack

February 9, 2000
Web posted at: 9:56 a.m. EST (1456 GMT)

In this story:

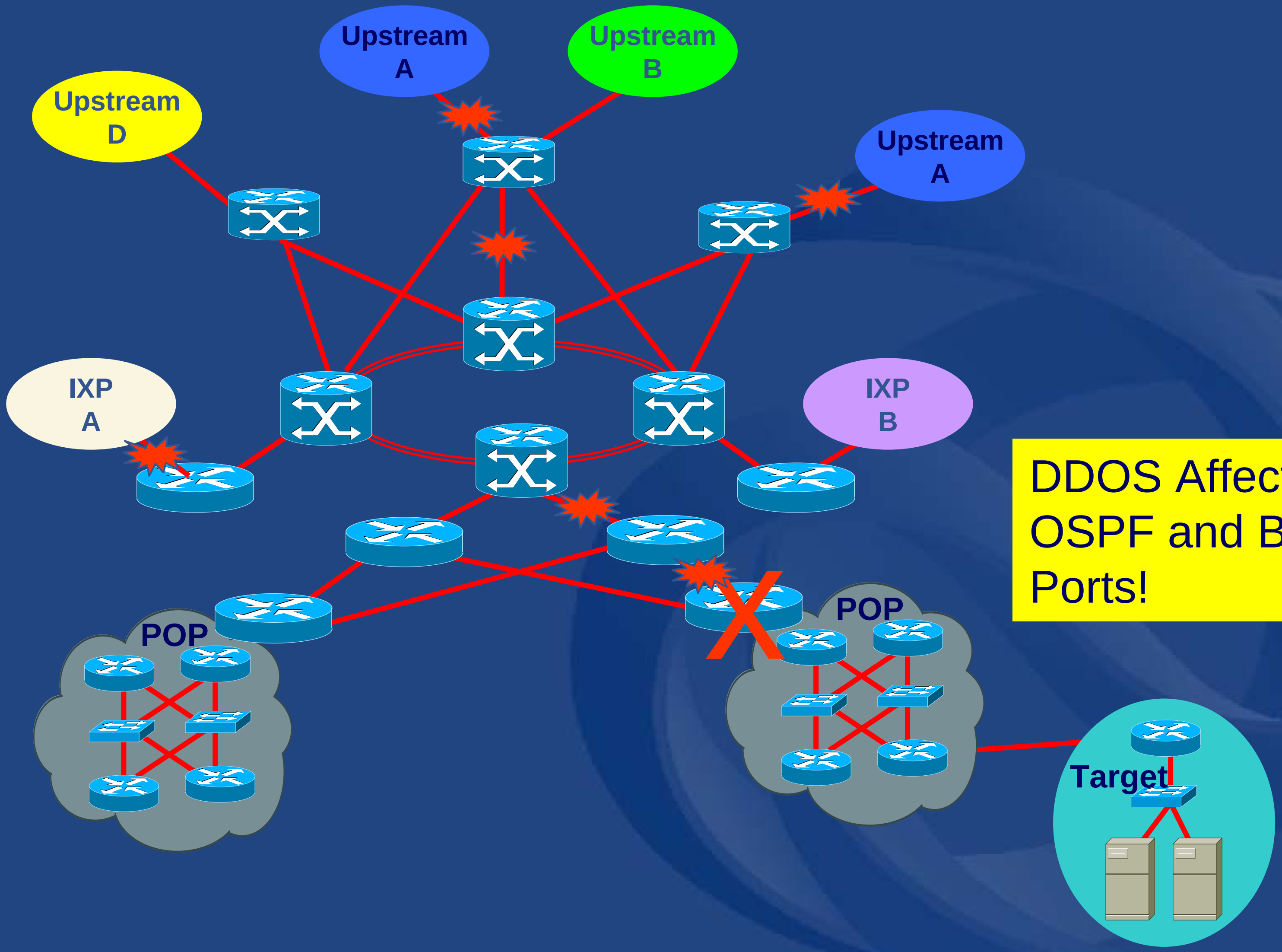
amazon.com

CNN.com

E*TRADE

ebay

DOS/DDOS attacks today



DDOS Affecting OSPF and BGP Ports!

DOS/DDOS attacks today (cont.)

- Attack patterns have shifted out from customer to ISP's infrastructure
  - ISPs/ IXPs *will be or could be* attacked to find a way to the target!
  - Co-location networks are now being used as reflector to hit other company's network

ISP security attack profile

- ISPs are mostly the transit path of any attacks.
- ISP *Becomes a Battlefield* when “real world” crosses into cyberworld.
  - This is a “Wake Up Call”
  - Internet security is a global Internet issue (there is no “US Internet”)

ISPs need to:

- Implement Best Current Practices (BCPs) RFC 3013, RFC 2827
  - ISP infrastructure security
  - ISP network security
  - ISP services security
  - ISP customer security
- Work with operations groups, standards organisations, security groups, and vendors on new solutions

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

Important things to note

- There are no magic knobs, grand security solutions, or super vendor features that will solve the ISP security problem.
- Likewise, there is no rocket science involved. Just hard work that is within all ISP’s grasp.

Strategy to manage ISP security process incident response

- ISPs are *transit networks,* the way incident response happens is slightly different from other networks.

- Effort should be made to mitigate the effects of the attack and trace it back *upstream* from its source.

- ISP security teams have demonstrated six distinct phases in the way ISPs should respond to security incidents.
  - Preparation, Identification, Classification, Traceback, Reaction, Post mortem

Questions?

ISP Infrastructure Security Strategy

Threats and Attack types

ISP security threats – quick recap

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

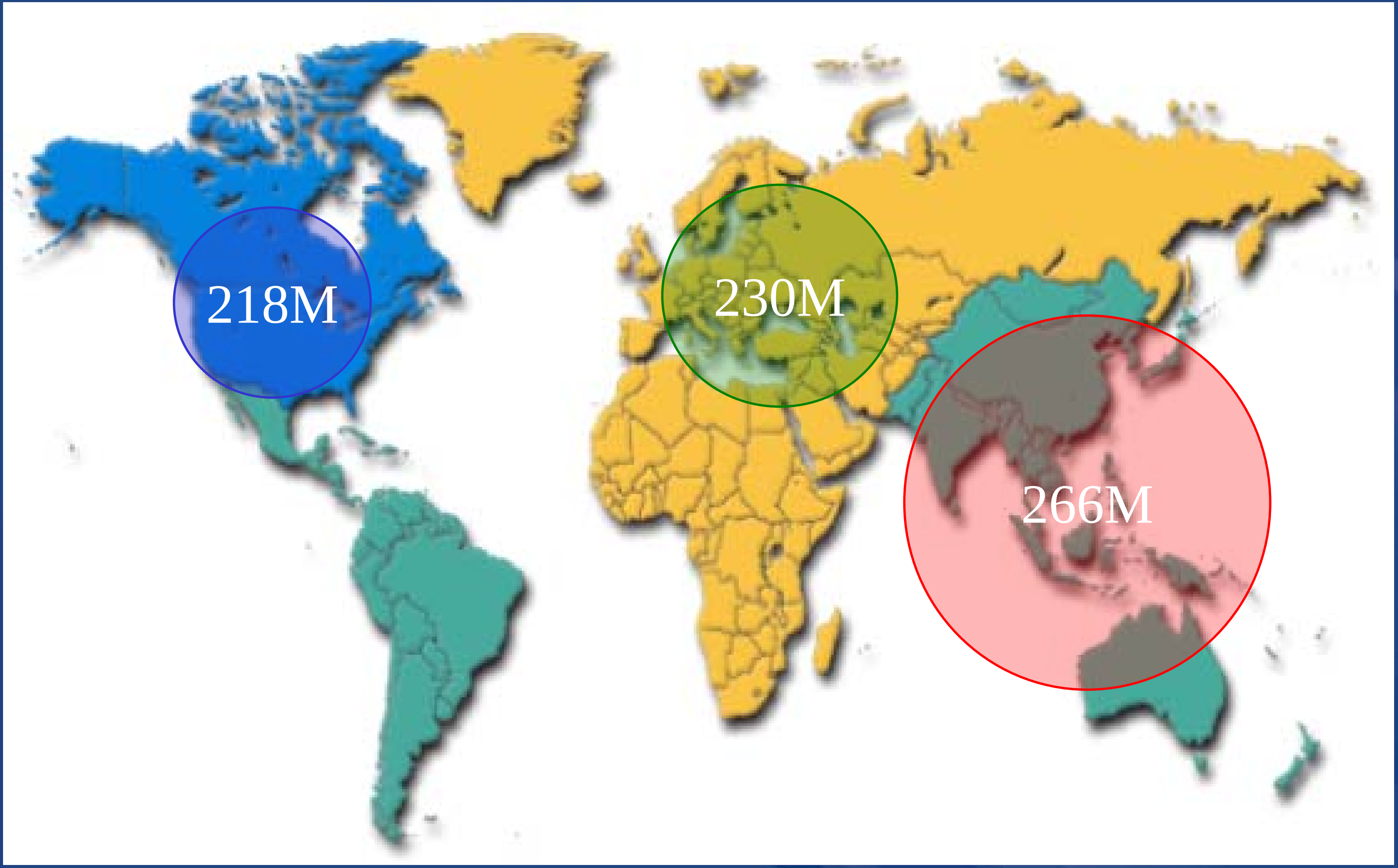
Vint Cerf

Geopolitical Transitions

- Internet is a non-American Internet – the world has just not woke up to that fact. Largest growth in Asia-Pacific
  - China second in number of home users with only 5% of its population online, Japan third, and South Korea sixth
  - Nearly 50% of all broadband deployments are in Asia-Pacific
- New technologies disproportionately deployed sooner in the Lesser Developed Countries (LDCs)
  - Wireless, broadband, IPv6
  - No existing entrenched infrastructure to replace
- Worst-case threat may not be a nation-state
  - States/groups least dependent on the Global Internet Infrastructure may have the most to gain; least to lose from its disruption
  - Large portion of Internet infrastructure within US borders

The Changing Face of the Internet

World internet users stats as of February 3, 2005



Vulnerability Trends
(Based on 2000-2004 CERT Data)

- Implementation
  - – Flaws lead to widespread intrusions despite advances in security technology
- Configuration
  - – Errors continue to be major source of vulnerabilities and easiest to remedy
- Design
  - – Inadequate security measures despite past mistakes

Technology shifts

- May minimize some threats/vulnerabilities
- Always result in new vulnerabilities
- May impact existing countermeasures

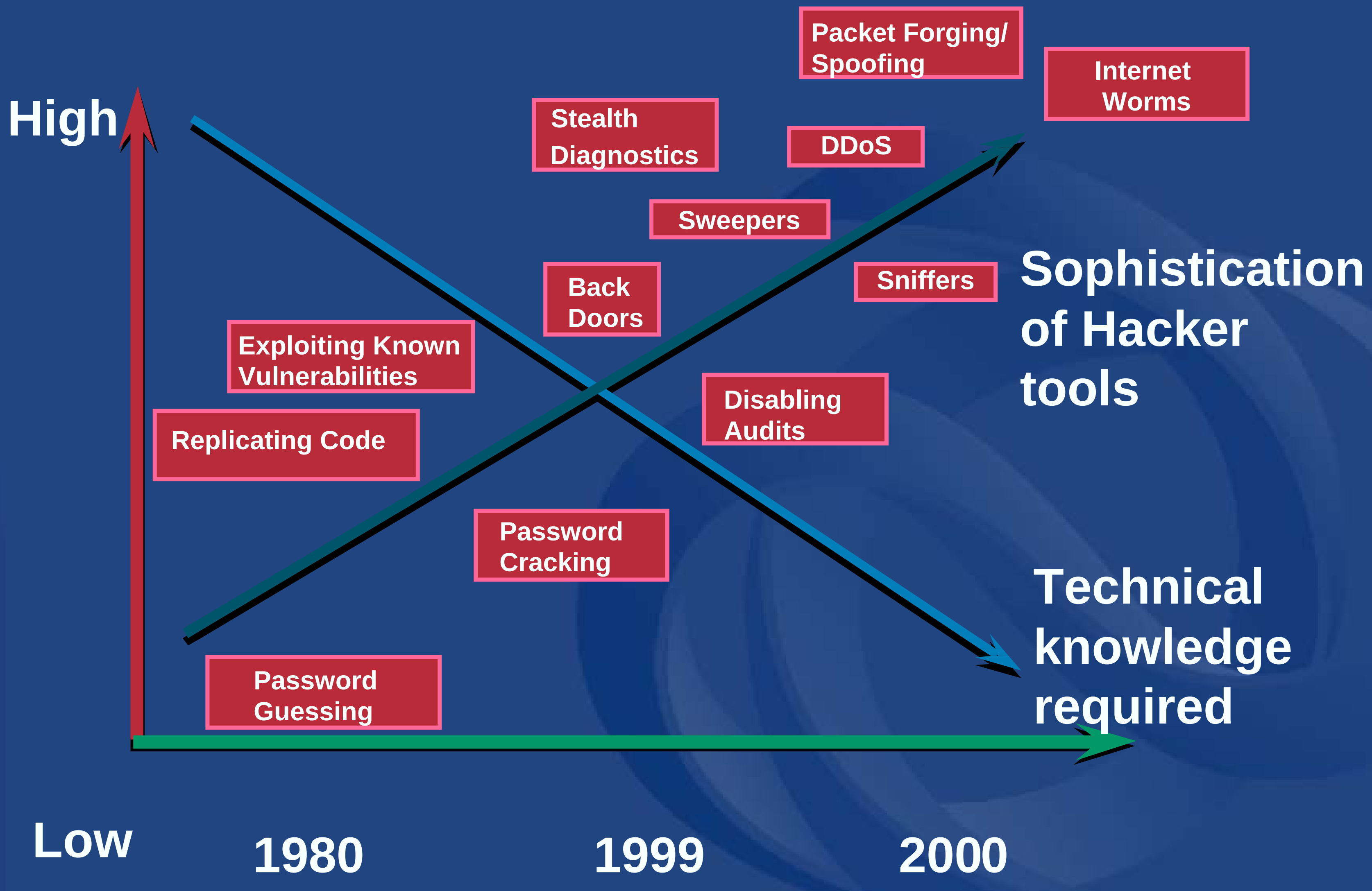
Threat Trends

(Based on 1994-2001 CERT Data)

- Exploits are forever
  - Once discovered, attack techniques persist and become increasingly automated and easy to implement

    Ex: Santy, worms, Trojans, spoofing, sniffing, denial of service, password cracking, rootkits
- Threat techniques mirror (and leverage) existing applications and technologies
  - Distribution, stealth, obfuscation, automation
- Arms race between threat techniques and countermeasures
- Attacks result in collateral damage and exposure

Exploit Trends
(Based on 1994-2001 CERT Data)



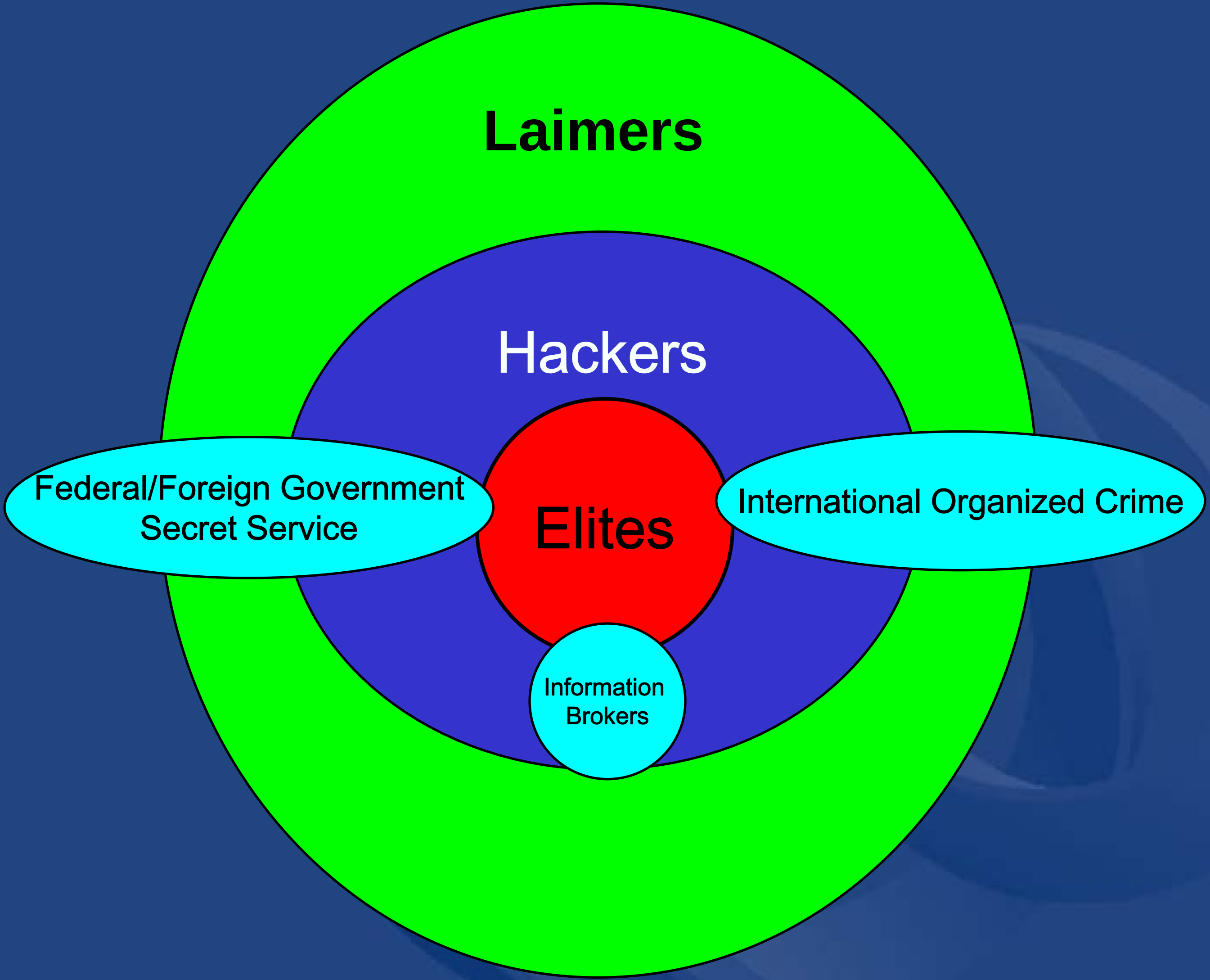
Who are the Attackers?

Who are the Attackers?

Three Broad Categories:

- Amateurs and Wannabes (Laimers)
  - Script kiddies and people who what to be the real thing, but do not want to put the hard work and patience to gain the skills
- True Hackers
  - More on these in the next slides …..
- Professionals (Elites)
  - People who are paid to attack. Organized crime, Militaries, Intelligence Organizations, Law Enforcement, and other groups ….

Hackers community hierarchy


Laimers
Hackers
Federal/Foreign Government Secret Service
Elites
International Organized Crime
Information Brokers

Hacker community

What Hackers know that you do not know

- They know the hardware/software
- Mae West/Mae East/Sprint, etc. are a great resource
- RIRs (Whois servers), Network Solutions tell them more…
- The World Wide Web is the greatest forum (IRC)
- OS flaws are there!! Hackers drive the patch/service packs
- Poorly designed application logic makes it visible…
- TCP/IP has its flaws - DNS/BIND, smtp, http, nfs, etc.
- The tools are out there...
- Bragware, The Ultimate Game! Sometimes, there is money attached to hacking

What Hackers Know

- Beginners (Aspiring Hackers)
  - Snoop, Port Scanning, IP/DNS/Mail Spoof
- Average hackers
  - Virus generators, Port scanning, All spoofing, URL/Image modifications
- Elite Hackers
  - File corruption, Destructive Virii/Bombs, Information Stealing, Session Hijacking, Erecting Beachhead for future attacks - Back doors/Trojans, Password Cracking, Modify/Remove Router ACLs, Crash Systems/Kill Networks, DoS

Common tools hackers use

Typical Hacker Tool Kit

- Multi-platform network labs with every possible OS version
- Collection of scripts/source code (dig, netcat, deshadow, etc.)
- Collection of apps (i. e. neotrace, icmp sniff, plisten, bomsquad, etc.)
- Collection of port scanners/killers (i.e, winnuke, portpro, ogre, slomo, aol-hell, etc.)
- Eavesdropping, session hijacking/sniffing tools (netcat, dnsniff, etc.)
- Password cracking technologies (l0pht crack, cisco-decrypt, getadmin, glide, pgpcrack, red button, office97crack, wingenocide, etc.)
- URL to IP address translators, and URL hijackers
- Collection virus code generators
- Credit Card generators and Demon Dialers (old but still effective)
- Web Sites that tells you BGP, ACL #, Web Server/OS version a site is running, what patches are applied, etc.

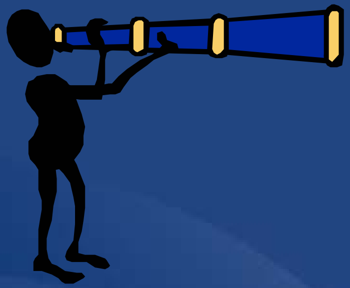
Corporate mistakes

- Poorly configured Web Servers
  - ?php, PageServices, incorrect access rights
  - Web and Application server on the same physical box on a DMZ
  - Lack of encryption
- OS or Software not patched due to lack of time
  - Old version of sendmail (spam relay anyone?)
  - Old version of BIND (map out a network without snmp?)
  - Old version of TCP/IP stack from Microsoft (Holey Stack, Bat Man!)
- OS not hardened due to lack of knowledge
  - Web server should only allow 80/443, no?! Why is inetd running? Why does /etc/services exist? How can I tune TCP/IP ports in NT? (Tune NT?! RegEdit?)

Three Key Threat Categories

Classes of threats

- Reconnaissance
  - Unauthorized discovery and mapping of systems, services, or vulnerabilities



- Access
  - Unauthorized data manipulation, system access, or privilege escalation

- Denial of Service
  - Disable or corrupt networks, systems, or services

How do these impact ISPs?

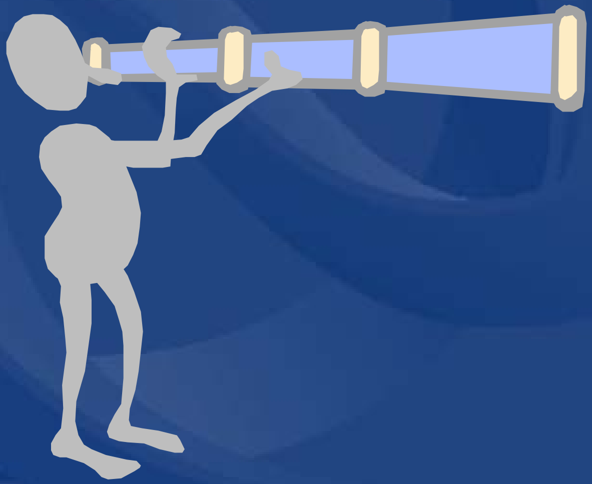
- Reconnaissance
  - Happens all the time
  - It is part of the “attack noise” of the Internet
  - along with low level attacks and backscatter
- Access
  - Break-ins on the edge of an ISP’s network (I.e. customer CPE equipment) can impact the ISP’s core
- DoS
  - The core threat to an ISP – knocking out customers, infrastructure, and services

Threat Category #1

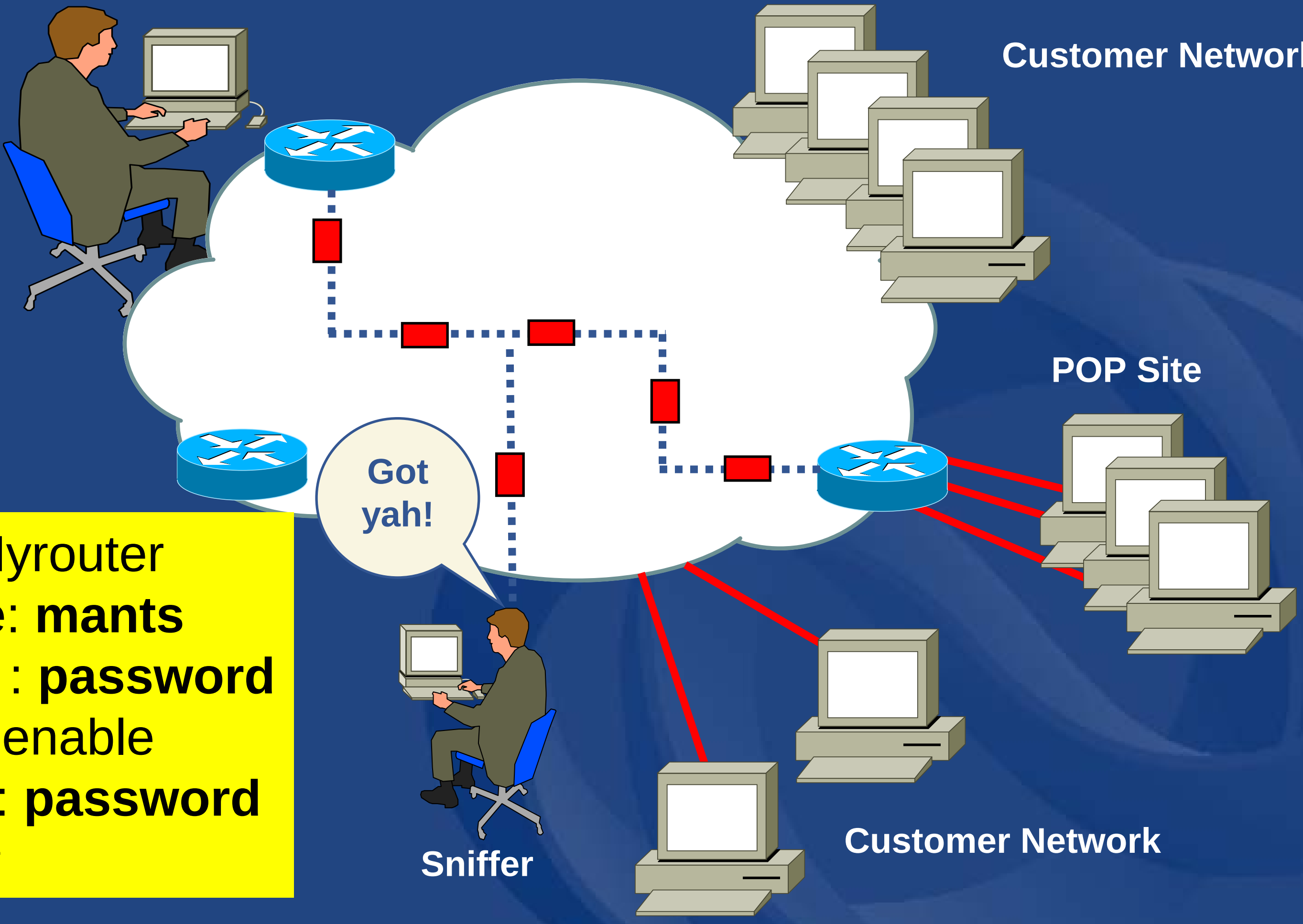
Reconnaissance

Reconnaissance methods

- Common commands and administrative utilities
  - nslookup, ping, netcat, telnet, finger, rpcinfo, File Explorer, srvinfo
- Public tools
  - Sniffers, SATAN, SAINT, NMAP, custom scripts



Network Sniffers



```
Telnet : Myrouter
Username: mants
Password : password
Myrouter>enable
Password: password
Myrouter#
```

NMAP

- Network mapper is a utility for port scanning large networks:
  - Vanilla TCP connect() scanning
  - TCP SYN (half open) scanning
  - TCP FIN (stealth) scanning
  - TCP ftp proxy (bounce attack) scanning
  - SYN/FIN scanning using IP fragments (bypasses packet filters)
  - UDP recvfrom() scanning
  - UDP raw ICMP port unreachable scanning
  - ICMP scanning (ping-sweep)
  - Reverse-ident scanning

NMAP

nmap {Scan Type(s)} [Options] <host or net list>

Examples:

To launch a stealth scan of the entire "/16" networks 166.66.0.0 and 166.67.0.0 for the popularly exploitable imapd daemon:

```
# nmap -Up 143 166.66.0.0/16 166.67.0.0/16
```

To do a standard tcp scan on the reserved ports of host <target>:

```
# nmap target
```

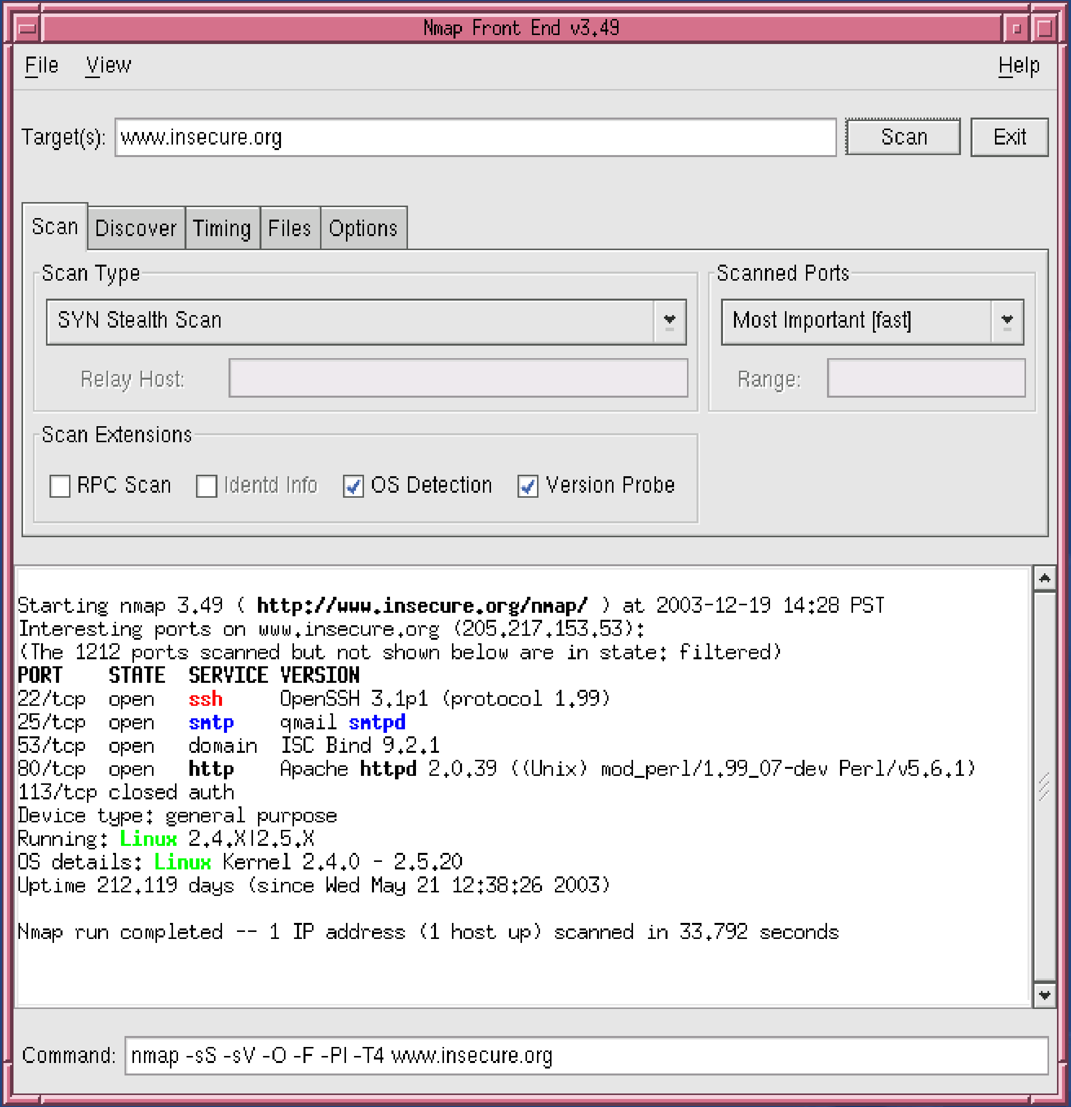
To check the "/24" network on which warez.com sits for popular services (via fragmented SIN scan):

```
# nmap -fsp 21,22,23,25,80,110 warez.com/24
```

To find hosts that are up in the "/24" 193.14.12, .13, .14, .15, ... , .30:

```
# nmap -P '193.14.[12-30].*'
```

NMAP



Target(s): www.insecure.org

Scan Type: SYN Stealth Scan

Relay Host:

Scanned Ports: Most Important [fast]

Range:

Scan Extensions: □ RPC Scan □ Identd Info ☑ OS Detection ☑ Version Probe

```
Starting nmap 3.49 ( http://www.insecure.org/nmap/ ) at 2003-12-19 14:28 PST
Interesting ports on www.insecure.org (205.217.153.53):
(The 1212 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp   open   smtp    qmail smtpd
53/tcp   open   domain  ISC Bind 9.2.1
80/tcp   open   http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212.119 days (since Wed May 21 12:38:26 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 33.792 seconds
```

Command: nmap -sS -sV -O -F -PI -T4 www.insecure.org

The scan results shows the state of the ports for each services running in the server

Why do you care?

- Reconnaissance is part of the “security noise of the Internet.” It doesn’t bother me
  - Wrong!
- The more information you have, the easier it will be to launch a successful attack:
  - Map the network
  - Profile the devices on the network
  - Exploit discovered vulnerabilities
  - Achieve objective

Why do you care? (cont.)

- Reconnaissance is a tool to give you an indication of an imminent attack
  - Warfare principle #1 – know your enemy!
  - That means an attacker needs to map their target, knowing it inside and out. Not doing this means an ineffective attack or a chance of getting caught. This gives ISPs a tool – watching the people mapping them
  - History has shown the amateur community to be very “me too.” So many times, dramatic increases in reconnaissance activities indicate multiple attacks
- Sink Holes and Syslog mining are great tools to metric the ISP’s reconnaissance activities

Threat Category #2

Access

Access methods

- Exploiting passwords
  - Brute force
  - Cracking tools

- Exploit poorly configured or managed services
  - anonymous ftp, tftp, remote registry access, nis, …
  - Trust relationships: rlogin, rexec, …
  - IP source routing
  - File sharing: NFS, Windows File Sharing

Access Methods (cont.)

Exploit application holes

- Mishandled input data: access outside application domain, buffer overflows, race conditions
- Protocol weaknesses: fragmentation, TCP session hijacking
- Trojan horses: Programs to plant a backdoor into a host

Threat Category #3

Denial of Service

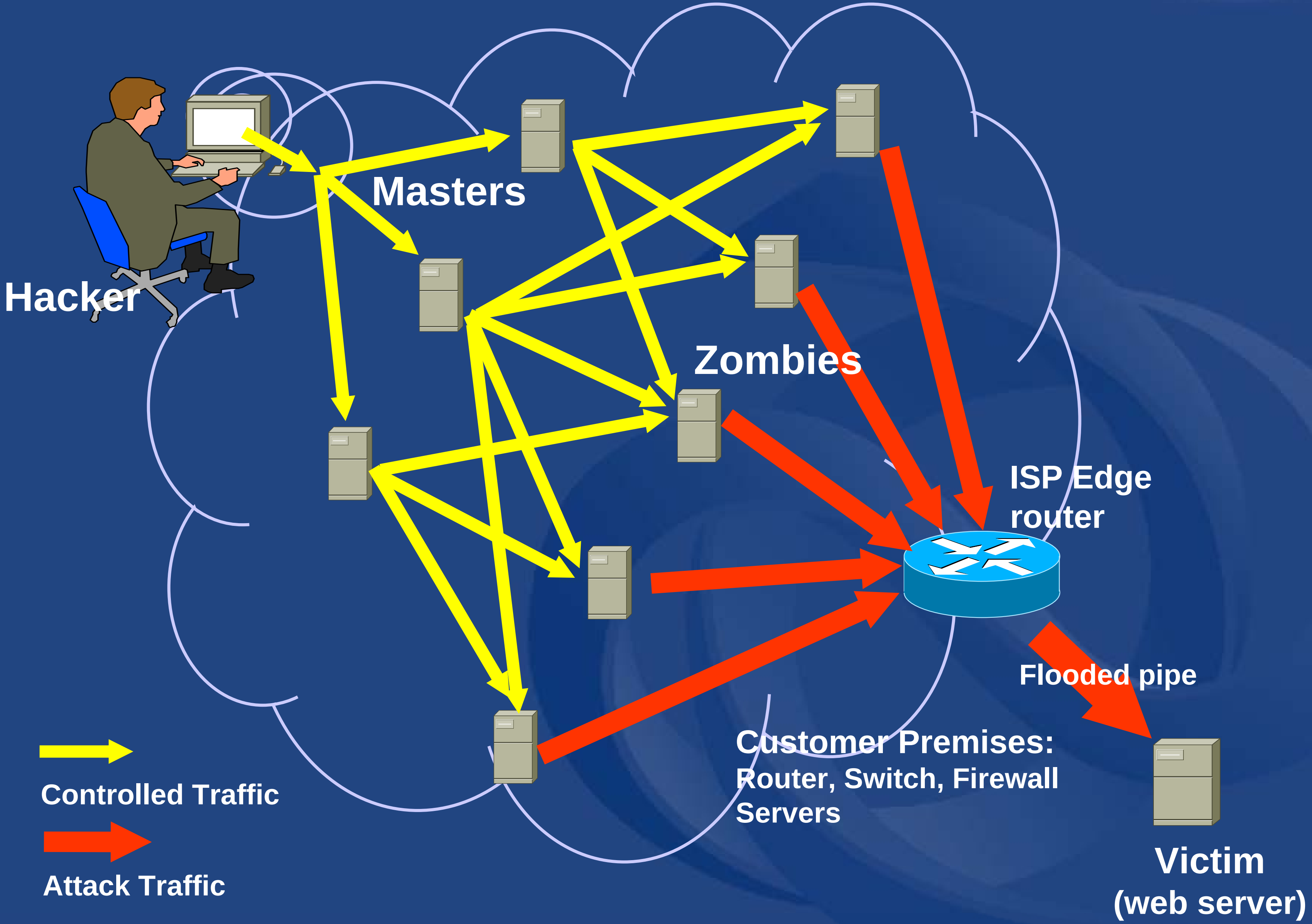
Denial of Service Methods

- Resource Overload
  - Disk space, bandwidth, buffers, ...
  - Ping floods, SYN flood, UDP bombs, ...
- Software bugs
  - Out of Band Data Crash: Ping of death, fragmentation…
- Toolkits: TRINOO,Tribal Flood Net and friends
- Distributed attacks for amplification

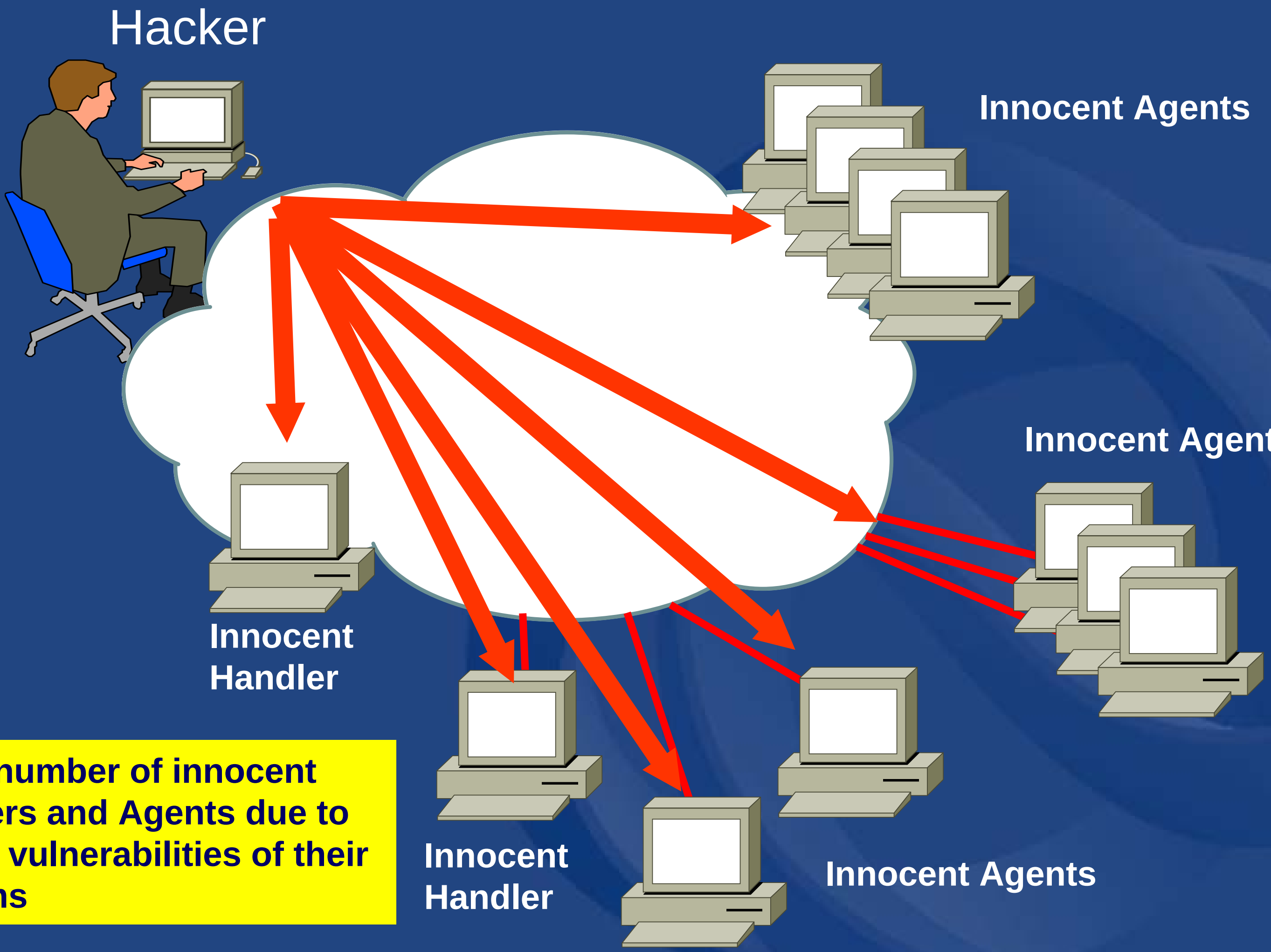
Denial of Service and ISPs

- DoS can ….
  - target an ISP
  - target an ISP’s customer
  - target the core of the Internet
- DoS cannot be ignored by an ISP. It always come back to bite you
- Example: Co-lateral Damage
  - Attack on a customer’s T1 applies back pressure and effects lots of other customers

DoS inside ISPs

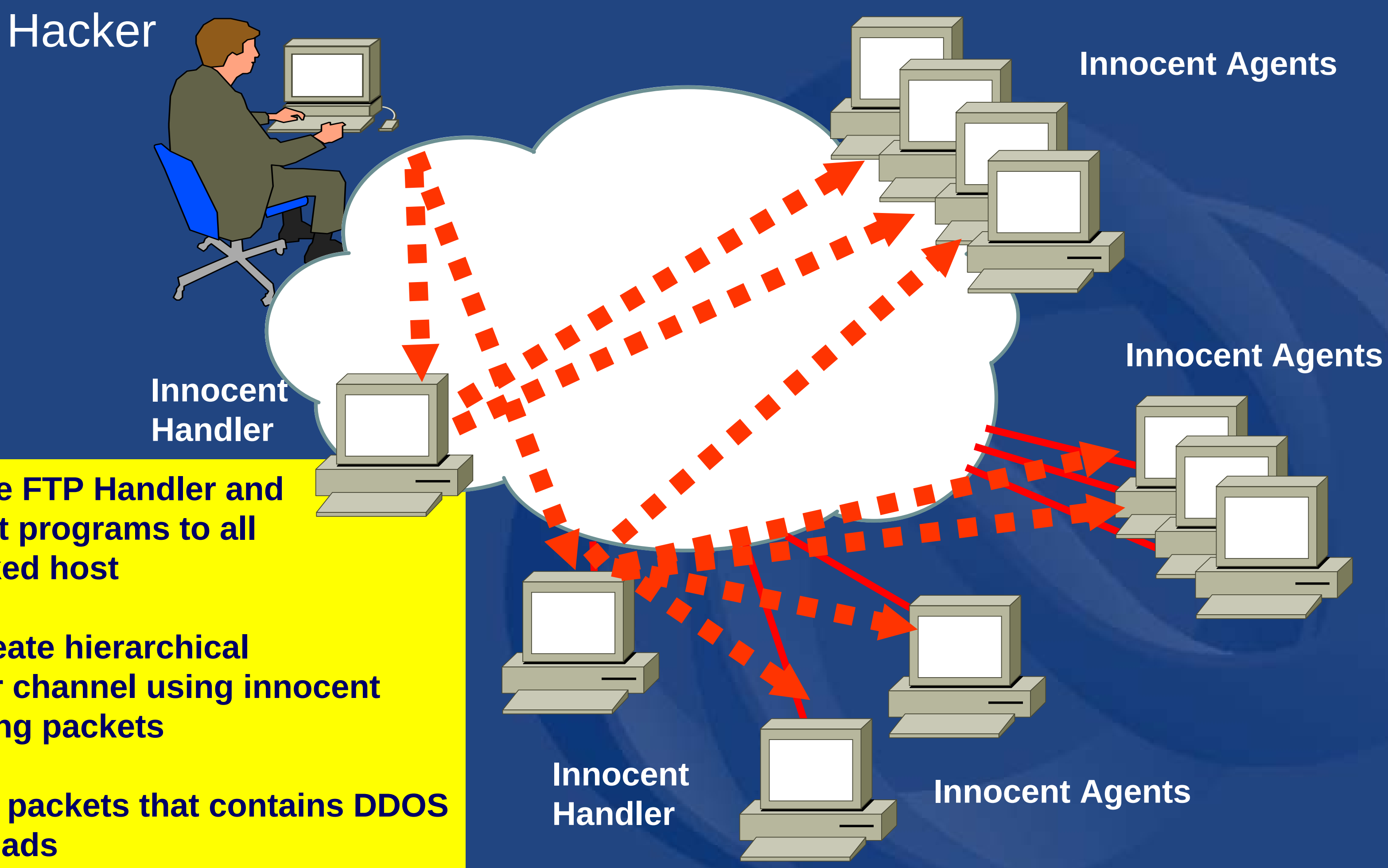


DDoS Step 1: crack handlers and agents



Large number of innocent Handlers and Agents due to known vulnerabilities of their systems

DDoS Step 2: Install trojan & covert communication channel

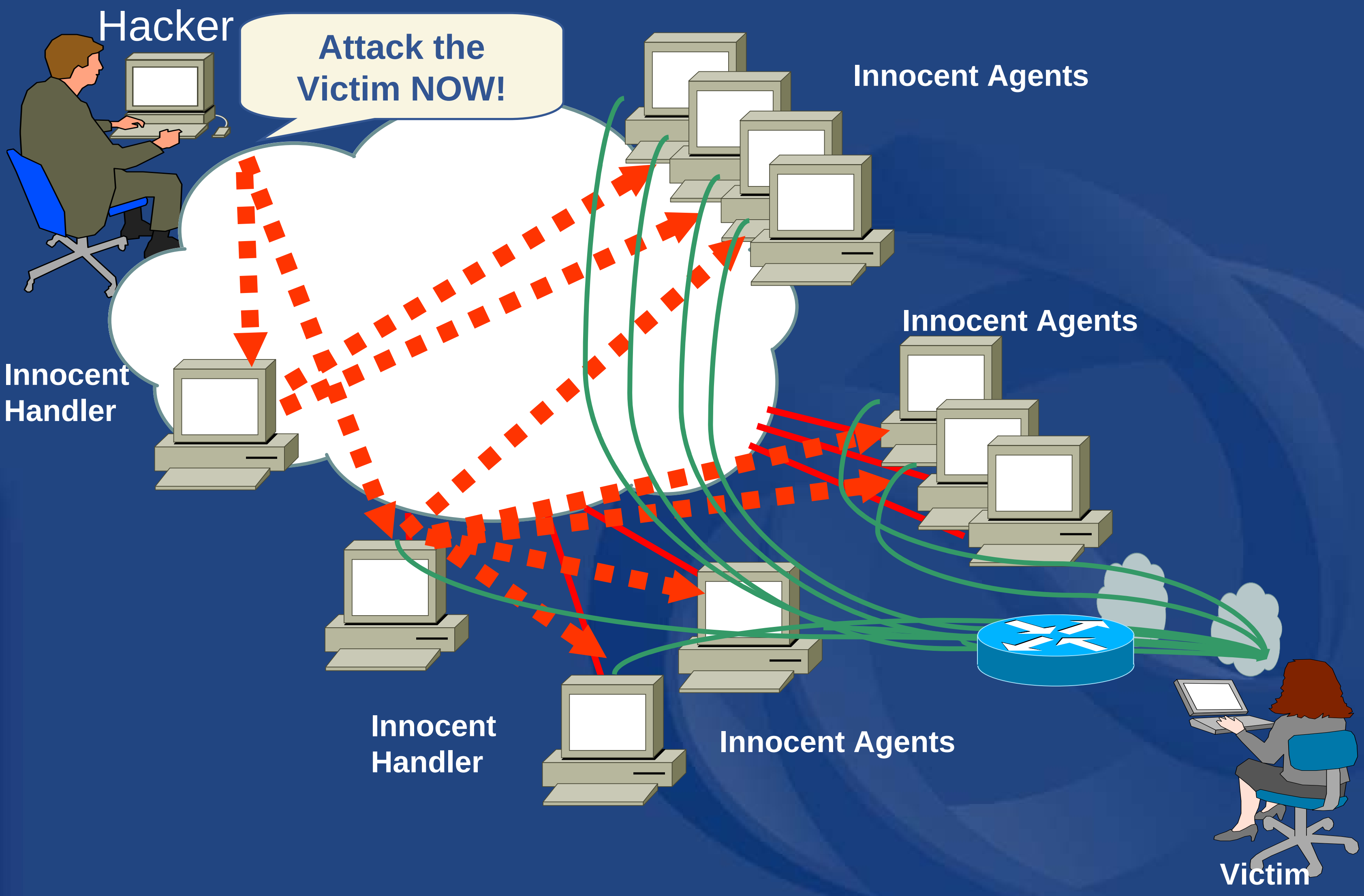


1. Use FTP Handler and Agent programs to all cracked host

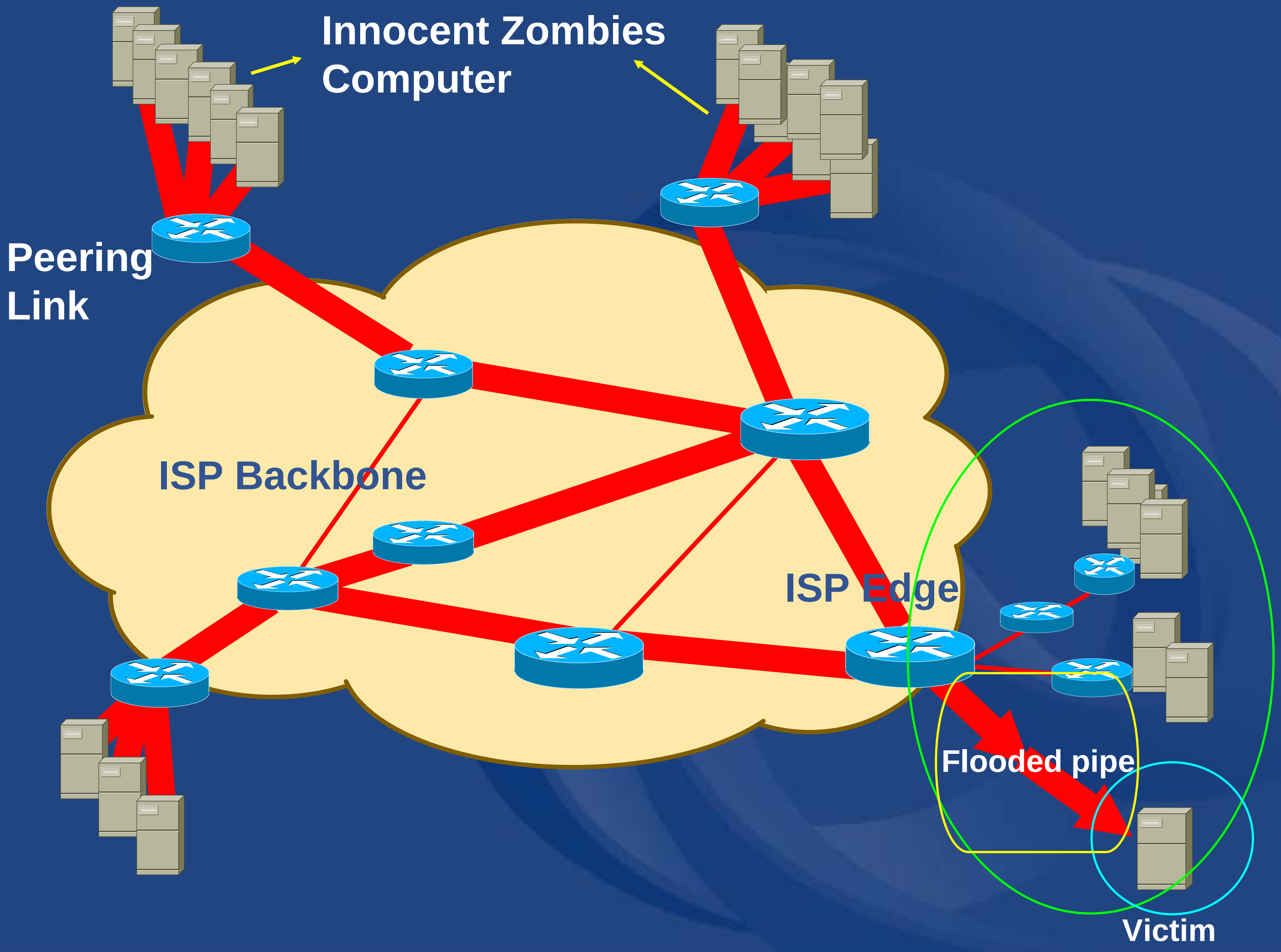
2. Create hierarchical cover channel using innocent looking packets

ICMP packets that contains DDOS payloads

DDoS Step 3: launch the attack



DDoS from external network



DDoS attack characteristics

- DDoS Arrays (handlers and agents) are maintenance intensive
  - Take time and effort to create
- Launching attacks from an agent can be considered a one shot weapon
  - Once the attack is launched, there is a risk of traceback
  - If someone traces back to the agent, they could watch and wait to see if the perpetrator returns to the agent

TCP DDoS reflection attacks

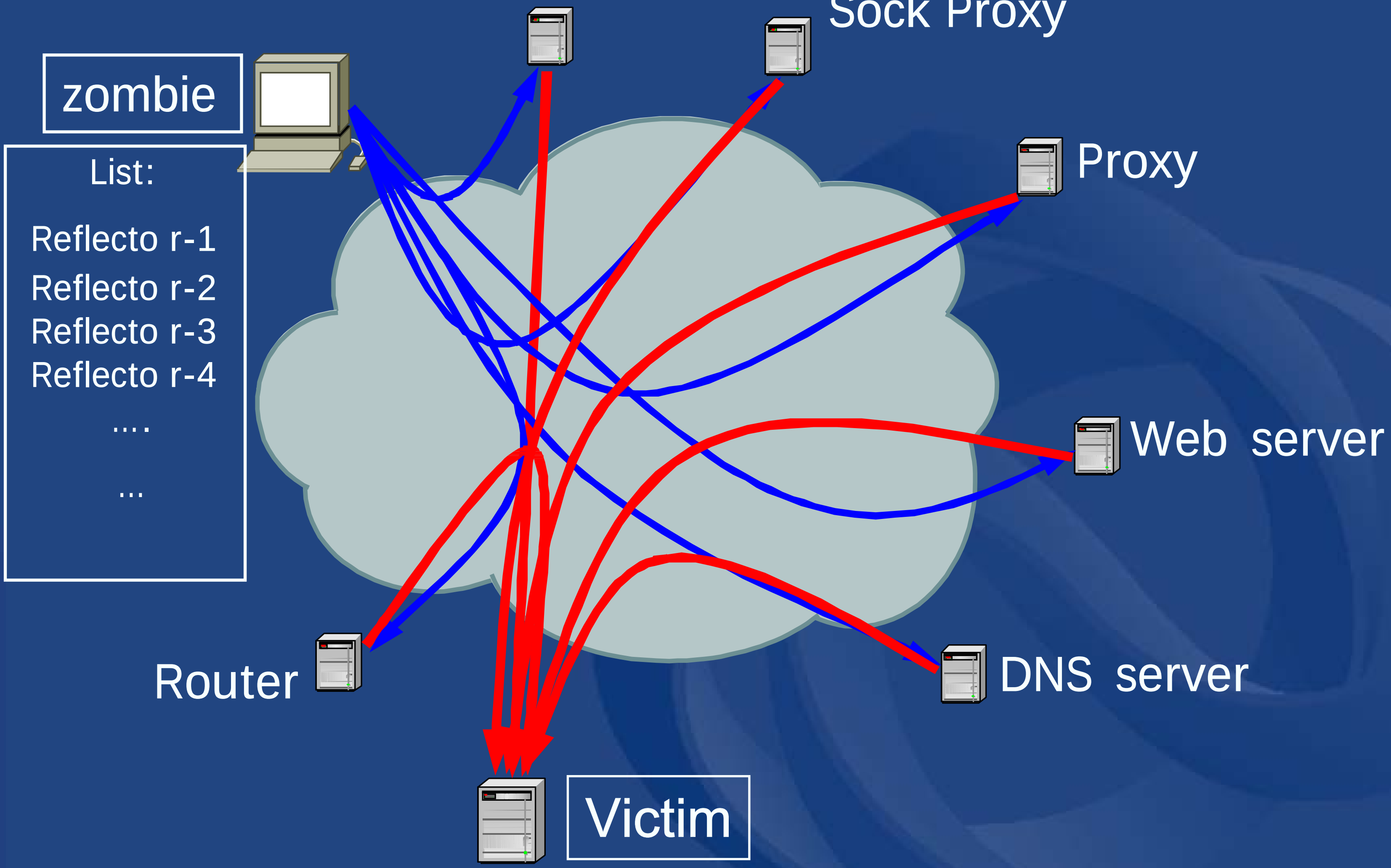
- Newer DDoS technique using TCP basics
- Similar to DNS reflection attack on register.com
  - No requirement to compromise hosts

- Traffic looks normal
- Attack sources are legitimate and spread over the entire Internet
- Sites acting as reflector will likely not notice performance degradation
- No easy attack mitigation options see (RFC2827)

TCP DDoS reflection attacks (cont.)

- Reflectors = returns a packet if one is sent
  - Web servers, DNS servers and *routers*
- Returns SYNACK or RST in response to a SYN or other TCP packets with ACK or query reply in response to a query or ICMP Time Exceeded or Host Unreachable in response to particular IP packets
  - Attackers spoof IP addresses from a zombie
- http://www.aciri.org/vern/papers/reflectors.CCR.01.pdf
- http://staff.washington.edu/dittrich/misc/ddos/grc-syn.txt

TCP DDoS step 1

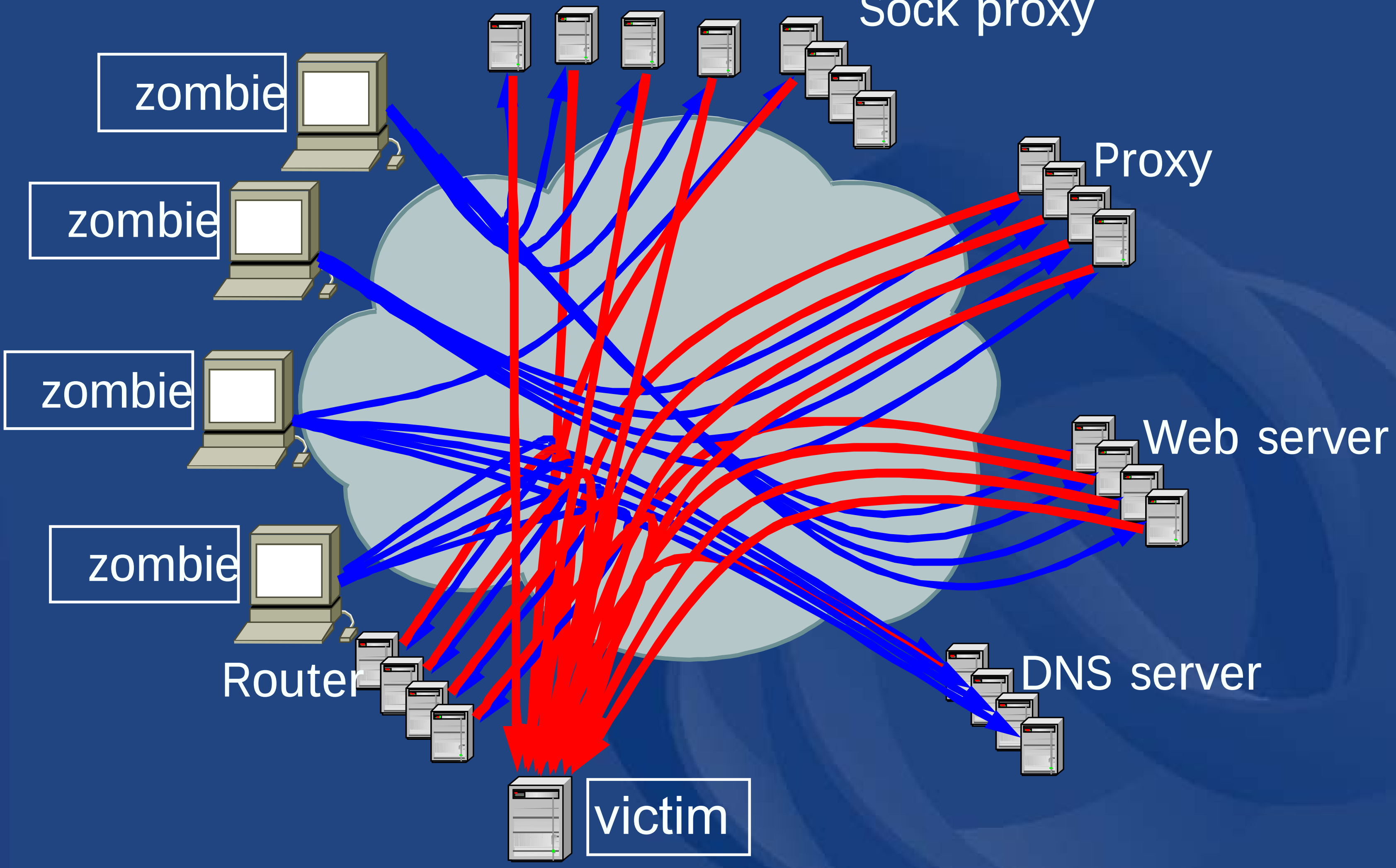


zombie

List:

Reflecto r-1
Reflecto r-2
Reflecto r-3
Reflecto r-4
....
...

TCP DDoS step 2



Other attacks

Attacks & exploits happening via other protocols

- MAC Addresses
- HTTP
- CDP
- DHCP
- RPC
- DNS
- ……………….. and many more

Questions?

ISP Infrastructure Security Strategy

Phases of security strategy to manage ISP security process

- Preparation -

Methodology

- Common sense, "Don't Panic" madness of a security incident helps the team focus and work the problem with fewer digressions. "stay focus"
- The question is what method works in today's environment?

Preparation is everything!

- Preparation with a guide methodology is the #1 difference between networks that survive the crisis
- Prepared to take the effect measures?
  - Code Red/Nimda
  - Slammer
  - DoS Attacks
  - Worms
  - Prefix Hijacks
  - Penetration Attacks
  - Botnet Attacks

  - Bottom Line – if you don't have a method to let yourself out, then your life as an operations engineer/administrator will be painful.

Security phases…..

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post Mortem

Where these came from?

- Evolving operational model that has been adopted as Best Current Practices (BCP) RFC 3013
- It evolved out of the Feb ’00 DDoS attack post analysis

Security phases….

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post Mortem

Preparation OPS teams

- ISP’s operations team must prepare!
  - Contacts for all ISPs connected
    - peers, customers, upstreams
  - Contacts for all vendor’s product security reaction teams
    - All equipment vendors you have
  - Documented policies
    - Will you help your customers?
    - Will you classify the attacks?
    - Will you traceback the attacks?
    - Will you drop the attacks on your infrastructure?

Preparation network

- Prepare the tools!
  - Create Access Control Lists (ACLs)
    - Infrastructure, rACL
  - Prepare automated scripts
  - Built and test the tools like Sink Hole and Backscatter tools
- Prepare the defense tools
  - Black Hole Filtering, BGP prefix and community filtering

Preparation

- Test the tools before implementing to the production network
  - – Classify ACLs on various parts of the network
  - – Test scripts to insure they will work?
  - – Prepare a simulated labs to simulate the attacks
    - Setup teams to simulate the attacks
      - – Attackers
      - – Defenders

Preparation

- Create incident response teams
- Formulate procedures & policies required for incident response and ensure response team members are very familiar with them
- Prepare the management, control & data planes (e.g., routing policies, appropriate hardware, lab & field verification, etc..).
- Employ & become familiar with tools that automate incident handling and allow you to “know your network & your enemy” (e.g., Arbor’s Peakflow)!
- Know your network and understand your tools capabilities
- Know your enemy and his weapons

Before we get to the details .....

- It is absolutely essential that you have a firm grasp on the core fundamentals of the ISP Routing architecture!

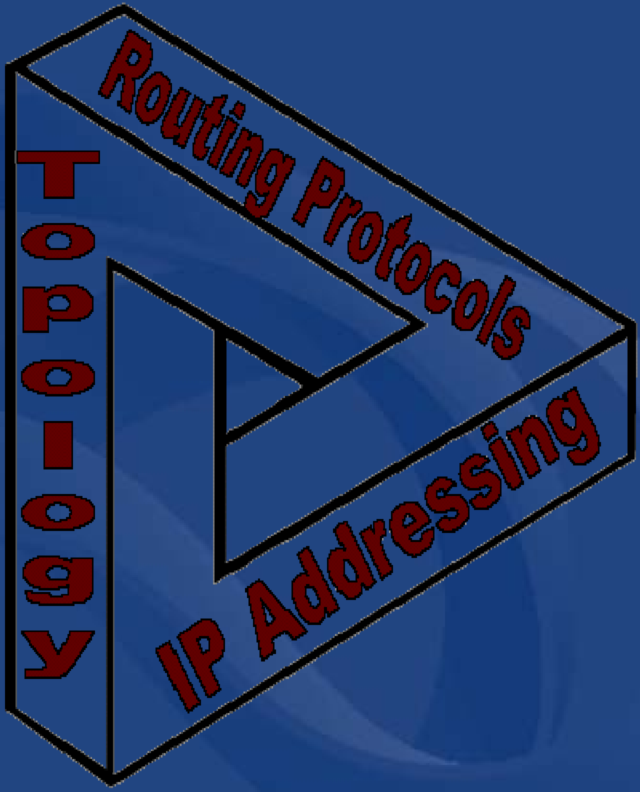
Routing Protocols and Architectures

How routing protocols effect the ISP Architecture

Routing protocols effect on ISP architecture

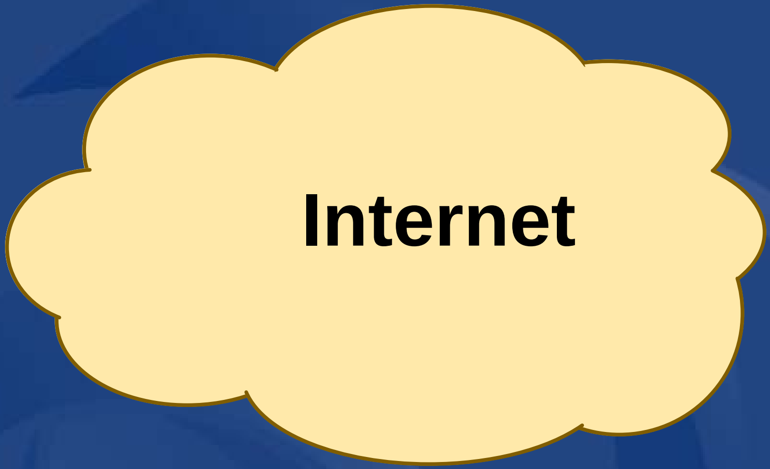
- Routing protocols inter-act with IP addressing and topology to provide the glue that makes it all work

- Poor routing protocol planning is often the first indication that a network if having scaling problems



In the beginning…

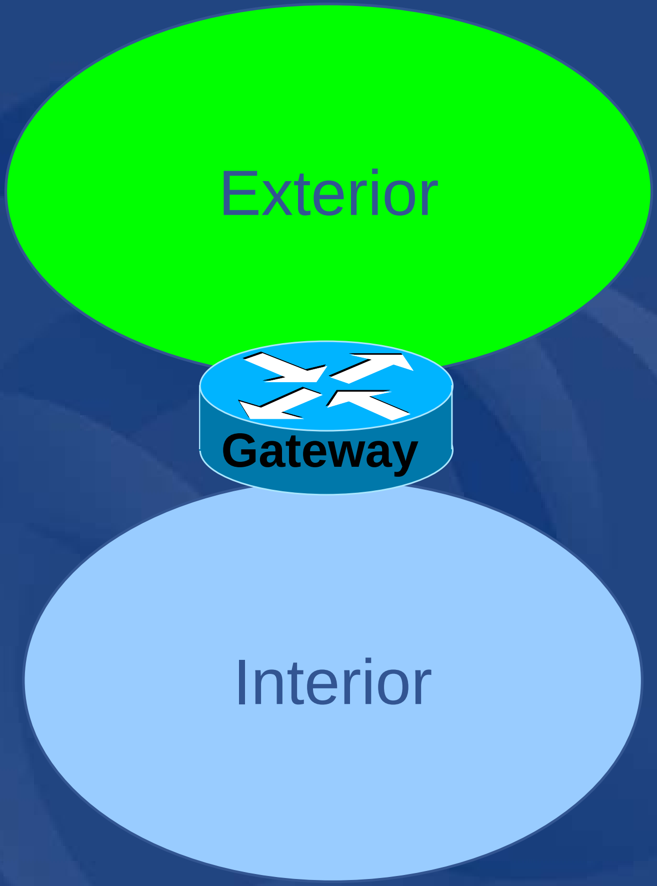
- In the beginning, the internet was flat
  - – No structure
  - – No routing protocols
  - – No hierarchy



Internet

First scaling architecture

- Flat networks would not scale, so structure and hierarchy was added:
  - Interior Gateway Protocols (IGP)
  - Exterior Gateway Protocols (EGP)
- Worked for enterprise networks (IGP = internal to the enterprise)
- An EGP by itself was not enough for ISPs



Interior vs Exterior routing protocols

IGP

- Automatic neighbor discovery
- Generally trust your peers
- Most reachability information shared
- Bind router in a network together

EGP

- Configured peers
- Outside connection" peer trust minimal
- Administrative bound reachability
- Binds networks together (Internets)

Interior vs Exterior routing protocols (cont.)

IGP	EGP
– Carries ISP infrastructure information only	– Carries customer routes and reachability to other autonomous systems
– Smaller and speed of convergence	– Large tables with stability as a priority
– Tied to the network topology	– Relatively independent of network topology

IGPs and EGPs have two different functions inside an ISP

Interior (OSPF or ISIS)

- Glues the internal network together
- Propagates next-hop locations
- Fast convergence and redundancy

Exterior (BGPv4)

- Glues the internet together
- Carries customer networks in iBGP
- Stability on the internet

BGP vs. OSPF/ISIS

- Internal Routing Protocols (IGPs)
  - Examples are ISIS and OSPF
  - Used for carrying infrastructure addresses
  - Not used for carrying Internet prefixes or customer prefixes

BGP vs. OSPF/ISIS

- BGP is used internally (iBGP) and externally (eBGP)
- iBGP can carry:
  - Some/all internet prefixes across backbone
  - Customer prefixes
- eBGP is used to:
  - Exchange prefixes with other ASes
  - Implement routing policy

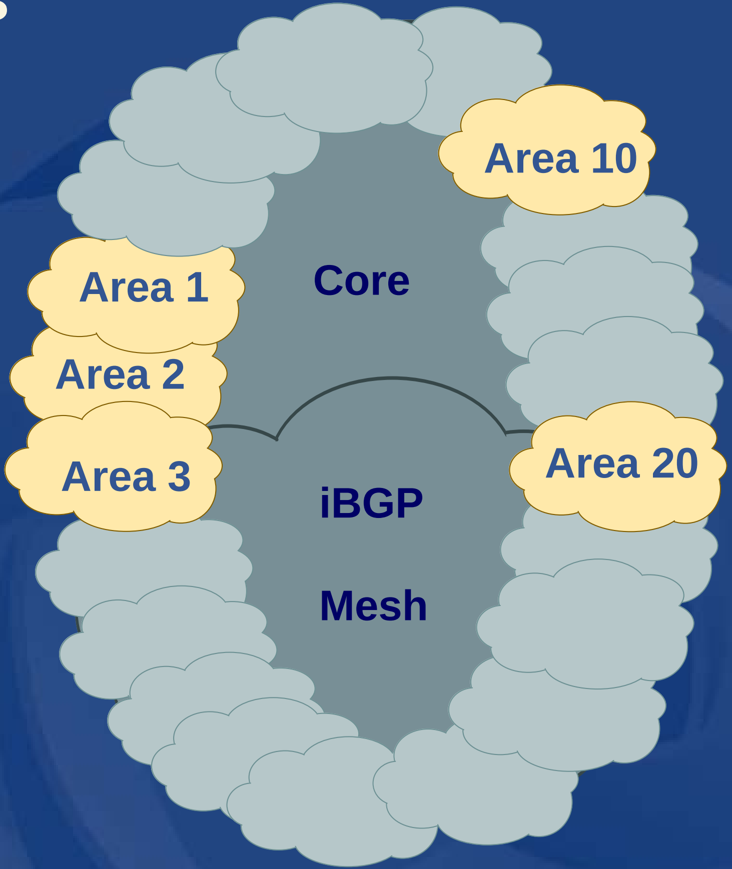
BGP vs. OSPF/ISIS (cont.)

- Do not:
  - – Distribute BGP prefixes into an IGP
  - – Distribute IGP routes into BGP
  - – Use an IGP to carry customer prefixes

YOUR NETWORK WILL NOT SCALE

Today's IGP/EGP hierarchy

- IGP carries only core links plus peering address information
- BGP carries all the routes
- Reset BGP Next-hop to loopback.
  - Security, stability, and efficiency

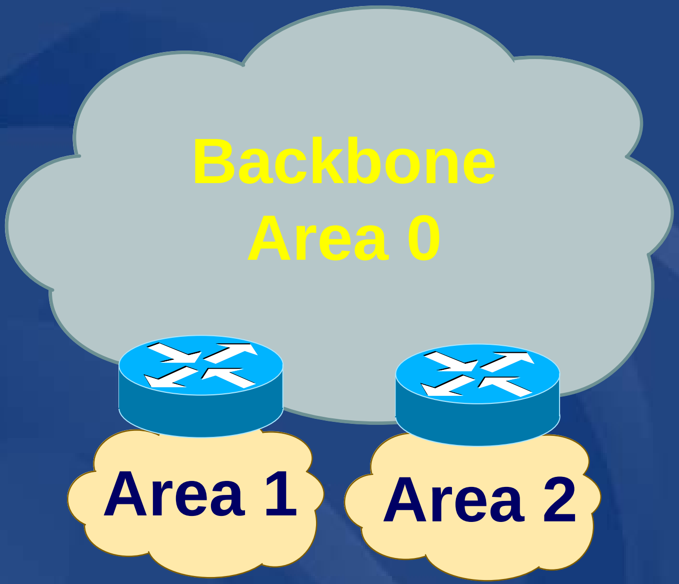


Increased stability

Routing protocols and architecture

- OSPF/ISIS hierarchy should, where possible, match topology hierarchy

- Results in marked reduction in routing traffic

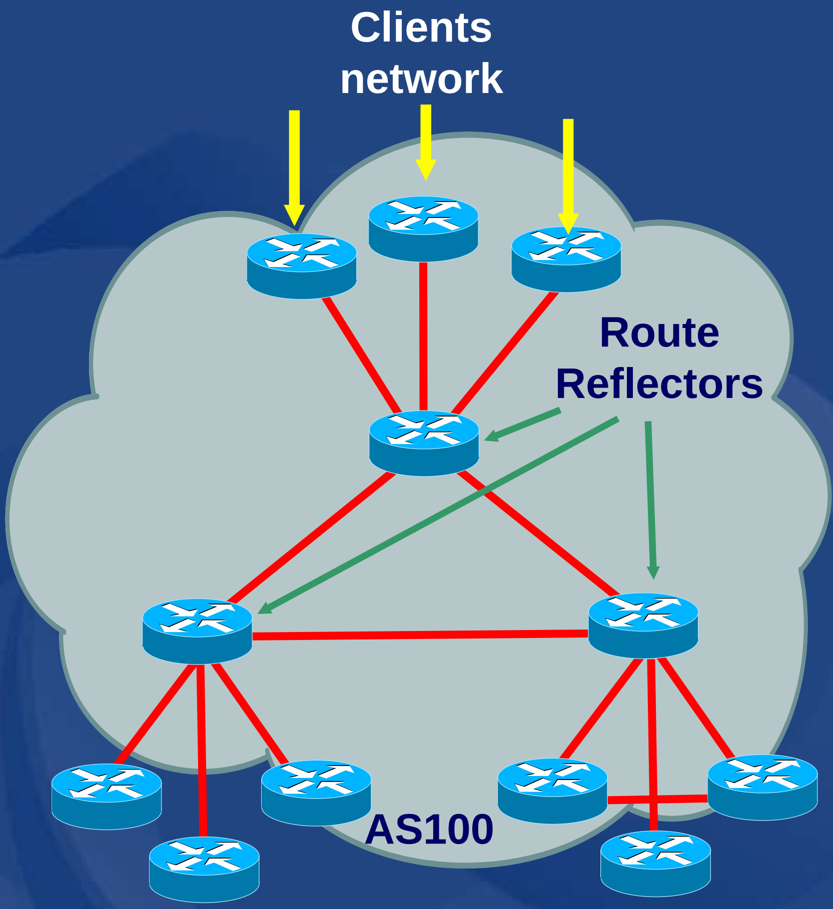


Routing protocols and architecture

- BGP route reflector or confederation hierarchies should where possible match the network’s topologies

- Good synergy would be productive to a healthy network

- No congruency could mean complex problems that are hard to resolve

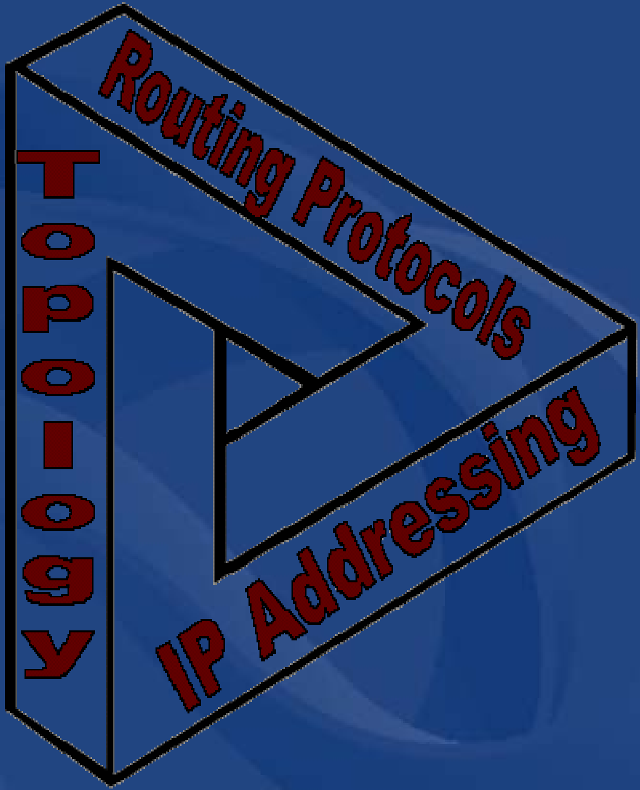


IP Addressing and Architecture

How IP addressing effect the ISP’s architecture

Why is IP address essential to ISP security?

- Effective addressing, route aggregation, and security are key to keeping the operational security overhead low.
- Critical to the scalability and success of an ISP's network
- Ignored, bad addressing policies will result in:
  - Higher cost
  - Longer deployment times
  - Complex troubles, and increased routing table convergence times



Address space

- Approach upstream ISP or consider RIR/NIR membership for address space
- Supply addressing plan when requested
  - Remember addressing should be classless
  - Address allocation are according to needs and not want
- In assigning addresses to backbone and other network layers - remember scalability
- Some examples follow…

Principles of addressing

- Separate customer and infrastructure address pools
  - Manageability
    - Different personnel manage infrastructure and assignments to customers
  - Scalability
    - Easier renumbering - customers are difficult, infrastructure is easy

Principles of addressing (cont.)

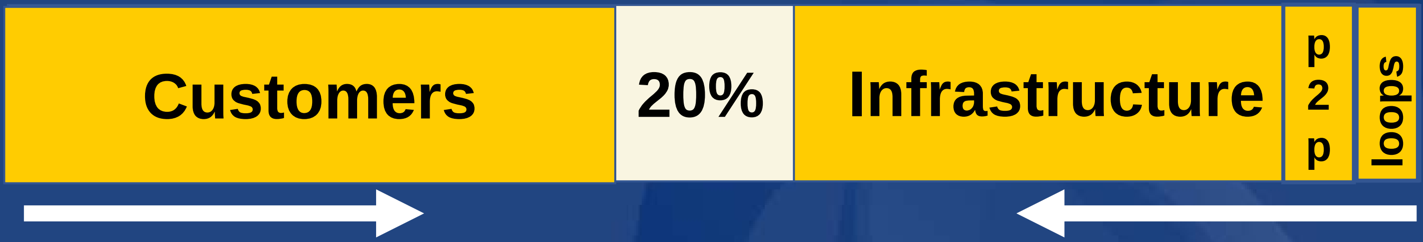
- Further separate infrastructure
  - In the IGP:
    - P2P addresses of backbone connections
    - Router loopback addresses
  - Not in the IGP:
    - RAS server address pools
    - Virtual web and content hosting LANs
    - Mail, DNS servers

Principles of addressing (cont.)

- Customer networks
  - Carry in iBGP
  - Do not put in IGP - ever
- Do not need to aggregate customer assigned address space
  - iBGP can carry in excess of unique 200,000 prefixes, no IGP is designed to do this.

Management - simple network

- First allocation from APNIC
  - Infrastructure is known, customers are not
  - 20% free is trigger for next request

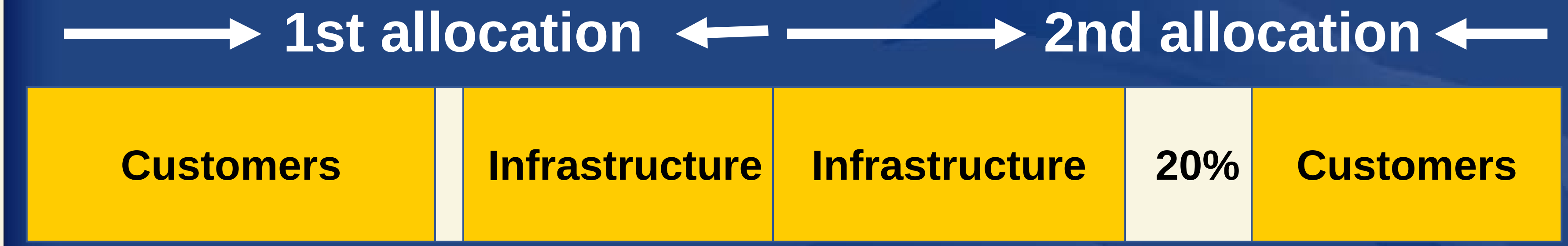


Customers | 20% | Infrastructure | p2p | loops

  - Grow usage of blocks from edges
  - Assign customers sequentially

Management - simple network

- If second allocation is contiguous



1st allocation

2nd allocation

Customers

Infrastructure

Infrastructure

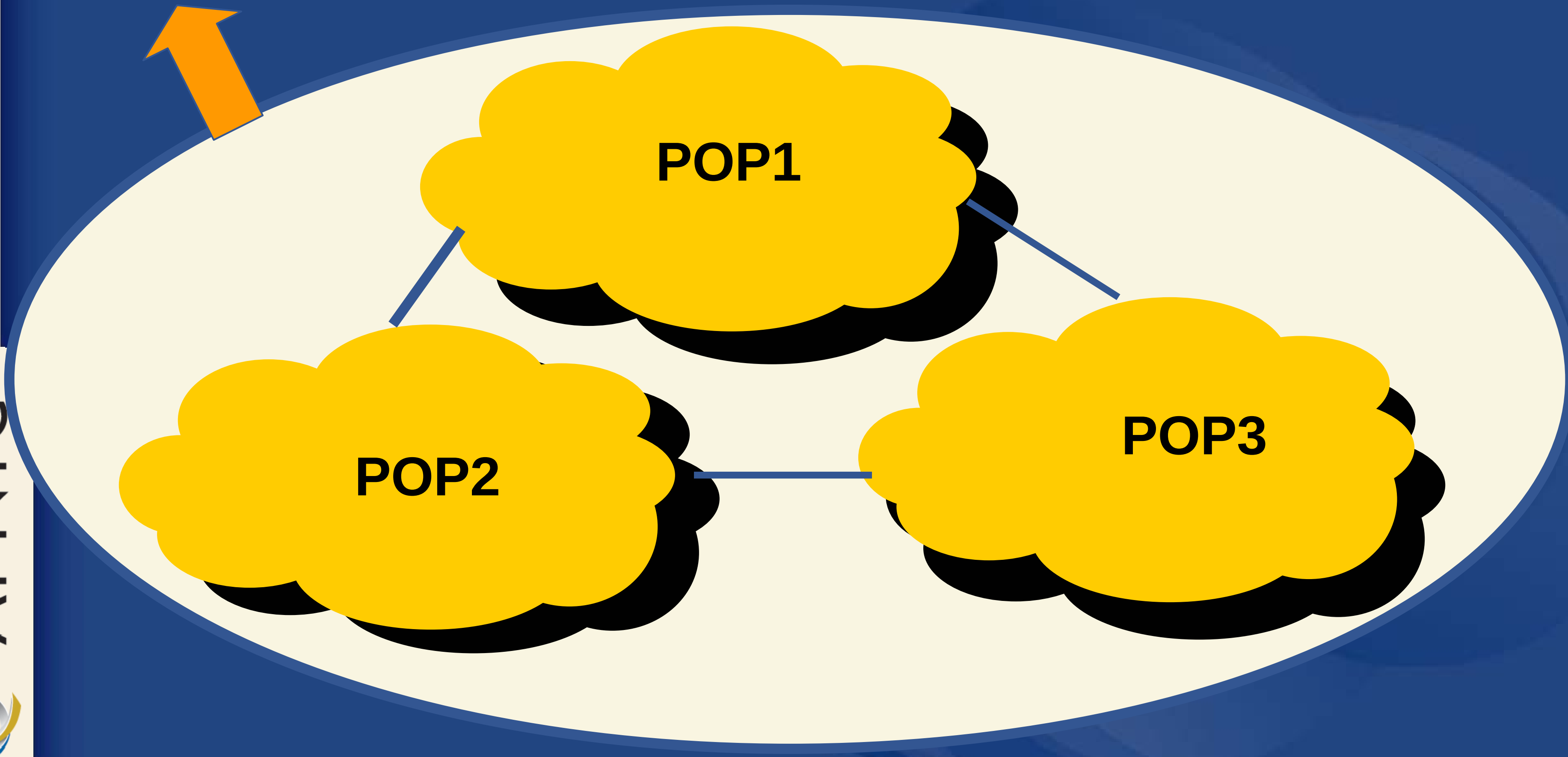
20%

Customers

  - Reverse order of division of first block
  - Maximise contiguous space for infrastructure
    - Easier for debugging
  - Customer networks can be discontiguous

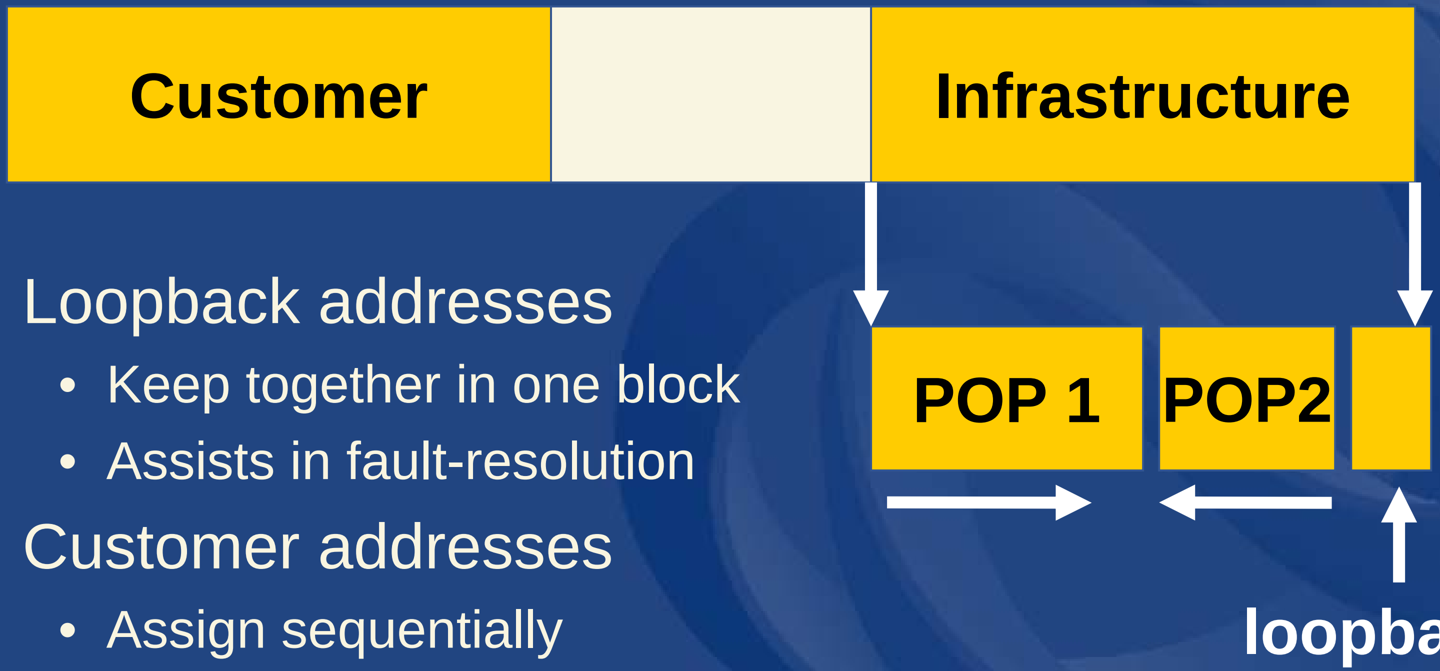
Management - many POPs

- WAN link to single transit ISP



Management - many POPs

- POP sizes
  - Choose address pool for each POP according to need



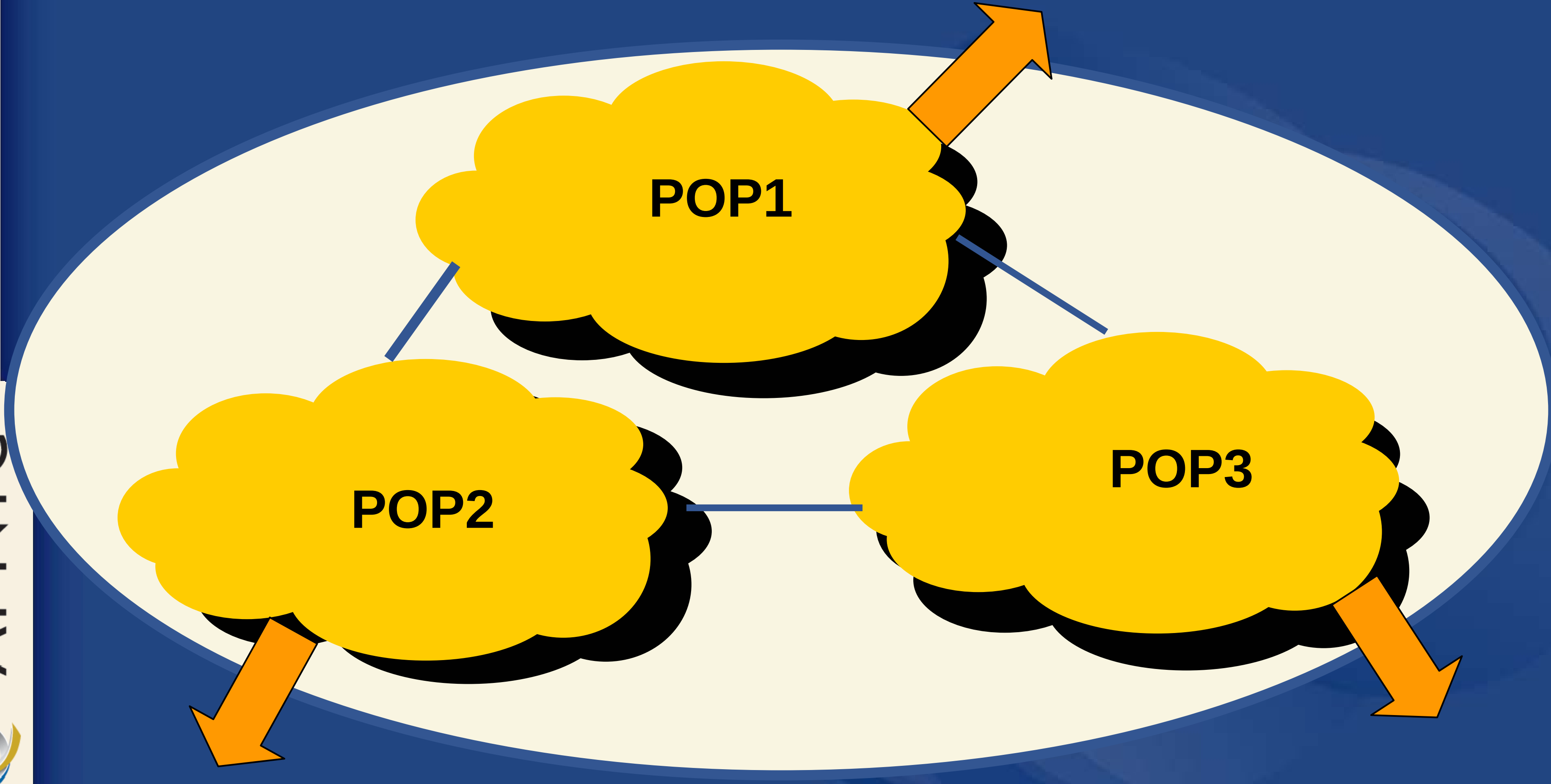
  - Loopback addresses
    - Keep together in one block
    - Assists in fault-resolution
  - Customer addresses
    - Assign sequentially

Management - many POPs

- /21 minimum allocation not enough for all your POPs?
  - Deploy addresses on infrastructure first
- Common mistake
  - Reserving customer addresses on a per POP basis
- Do not constrain network plans due to lack of address space
  - Re-apply once address space has been used

Management - multiple exits

- WAN links to different ISPs



Management - multiple exits

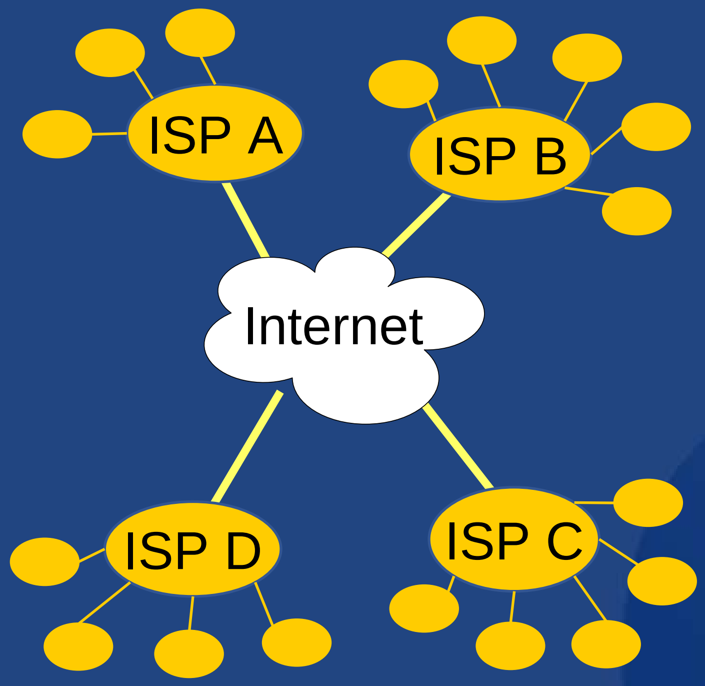
- Create a ‘national’ infrastructure pool

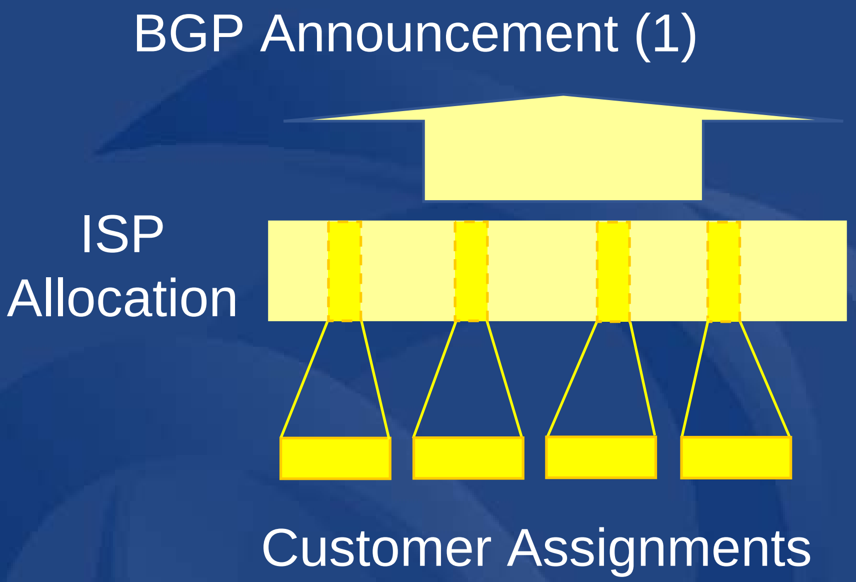
National Infrastructure	20% free	POP1	POP2	POP3

  – Carry in IGP
    - Eg. loopbacks, p2p links, infrastructure connecting routers and hosts which are multiply connected

  – On a per POP basis
    - Consider separate memberships if requirement for each POP is very large from day one

Route Summarisation (Aggregation)





- **Example - Summarising IPv4 addresses in a network**

Questions

ISP Infrastructure Security Strategy

Phases of security strategy to manage ISP security process

- Identification -

Security phases

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post Mortem

Identification

- Identify who is under attack
  - Own infrastructure
  - Customer infrastructure
- It is more than just waiting for customers to scream or your own network to crash
- Tools are available in the market
- Company working with tools
- Things you do on a tight budget

Ways to detect attacks

- Customer call

- Unexplained changes in network baseline
  - SNMP: Link, CPU overload, packet drops
  - Netflow (example from Cisco)
  - Arbor’s Peakflow DoS

- ACLs with logging
- Backscatters
- Sniffers
- Intrusion Detection Systems (IDS)

Identifying an attack

- Proactively monitor internal and customers network behavior
- Build baseline for all traffic expose anomalous behavior
- Utilise tools the allows network-wide correlation
- Notify customers before they notify you – be proactive!

Identifying an attack (cont.)

When are we being probed?

- Probes happen all the time; which ones are important?
- Probes precede an attack; if you can track specific probes, you might get a heads up that an attack is imminent

Identifying an attack (cont.)

When are your customers being attacked?

- #1 way to identify that there is an attack in progress is when a customer calls the NOC
- New ISP oriented Detection tools are available and do work
- SNMP and Netflow
- Peer notification – upstream

Identifying an attack (cont.)

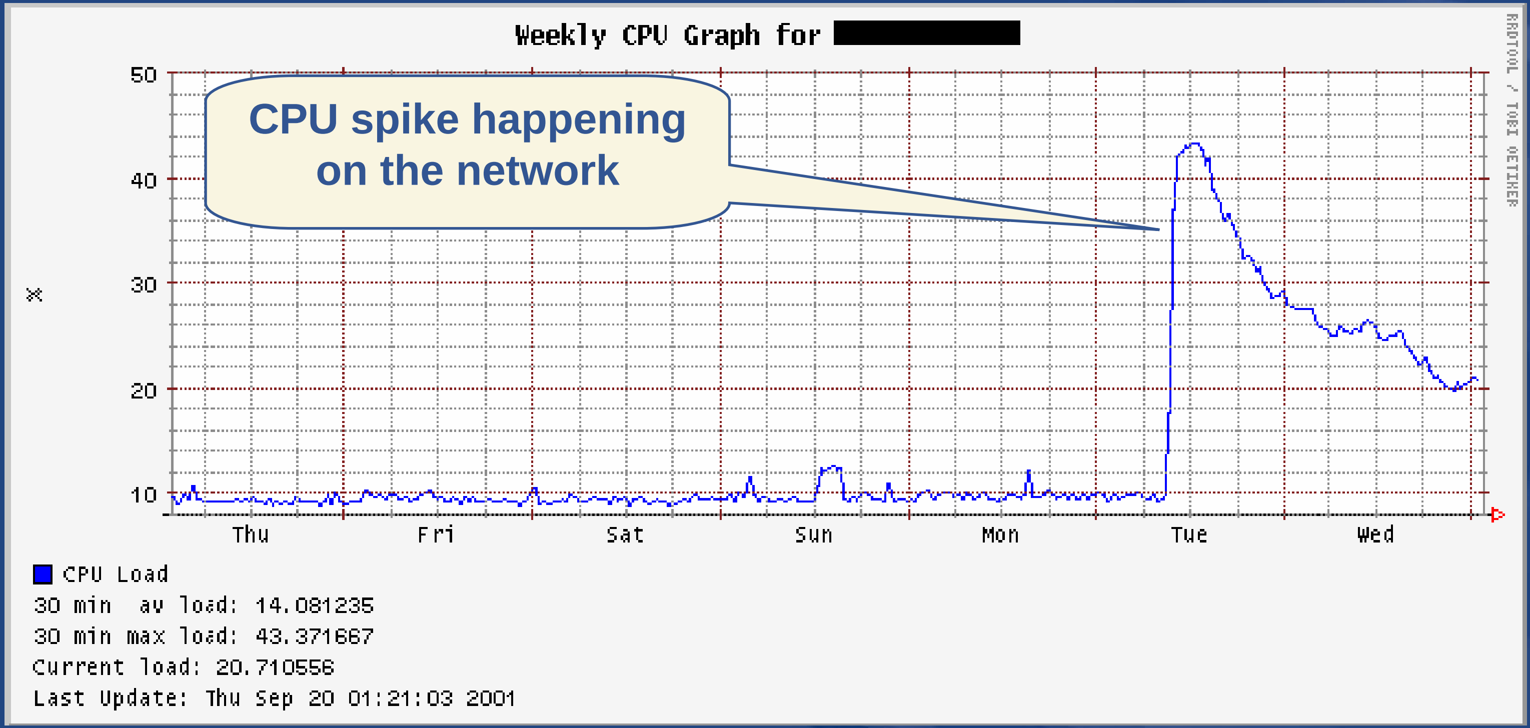
When are you being attack?

- NOC Alerts – is a problem in the network, a surge in traffic, a killer app, or someone attacking your network?

© Peter Krogh www.peterkrogh.com 301-933-2468

Identifying an attack (cont.)

- SNMP data abortion can signal a network problem *or* a security incident



CPU spike happening on the network

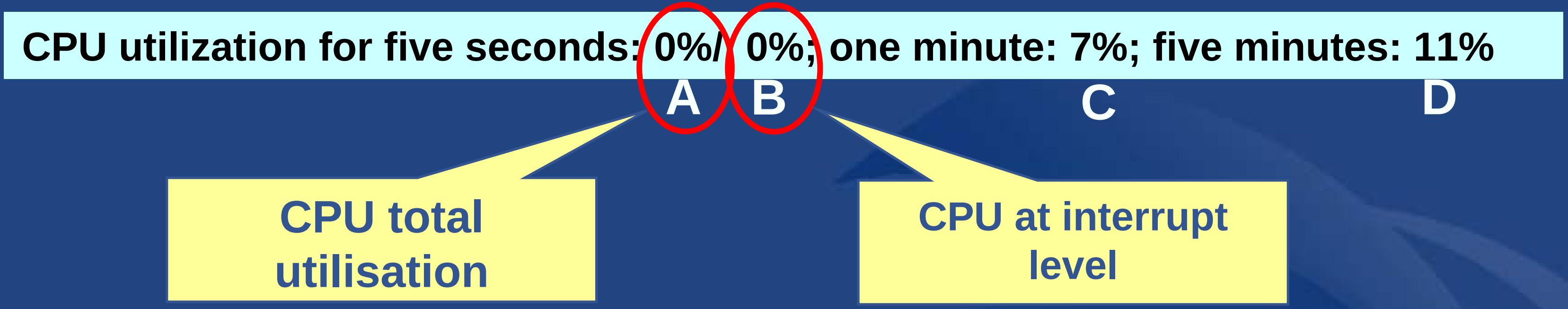
```
■ CPU Load
30 min  av load: 14.081235
30 min max load: 43.371667
Current load: 20.710556
Last Update: Thu Sep 20 01:21:03 2001
```

Identification tools

- SNMP
  - Watching the baseline and tracking variations/surges
  - Also looking for specific triggers (CPU and input buffer drops are the top two)
- SYSLOG
  - Watching the baseline
  - Looking for specific triggers (SNMP Authentication Failure)
  - Watching the ACL Logs
- Netflow
  - Anomaly Detection Tools
  - Triggers on flow table overloads

CPU load indicators

Identifying an attack through CPU load



```
CPU utilization for five seconds: 0%/ 0%; one minute: 7%; five minutes: 11%
```

- A: Total CPU load
- B: CPU at interrupt level (note: B <= A)
- A-B: Process switched traffic, CPU processes

(See: http://www.cisco.com/warp/public/63/highcpu.html)

Identifying an attack through CPU load (cont.)

```
CPU utilization for five seconds: 0%/ 0%; one minute: 7%; five minutes: 11%
                                   A     B                C                D
```

If A˜ B: “Too much traffic to forward”

- Interrupts: Packet switching (fast switching)

If A >> B: “Too much central processing”

- Packets to/from the router (eg SNMP, ICMPs, vty and console, IPsec (w/o h/w), routing, …)
- Process switched packets or switching problem

Identifying an attack through CPU load (cont.)

If A˜ B (Packet rate getting too high)

Check interfaces to find the source:

- check interface status
  - Watch load and drops
- check interface switching status
  - Watch throttles (-> drops due to overload)
  - Protocol stats (IP, ARP, …)

Identifying an attack through CPU load (cont.)

- Input Queue drops might means an attack
  - Check the Queue values
  - Default input queue values make the router vulnerable to resource saturation attacks.

```
Output queue 0/40, 0 drops; input queue 97/1500, 54 drops
5 minute input rate 76502000 bits/sec, 31139 packets/sec
5 minute output rate 72517000 bits/sec, 26560 packets/sec
```

Identifying an attack through CPU load (cont.)

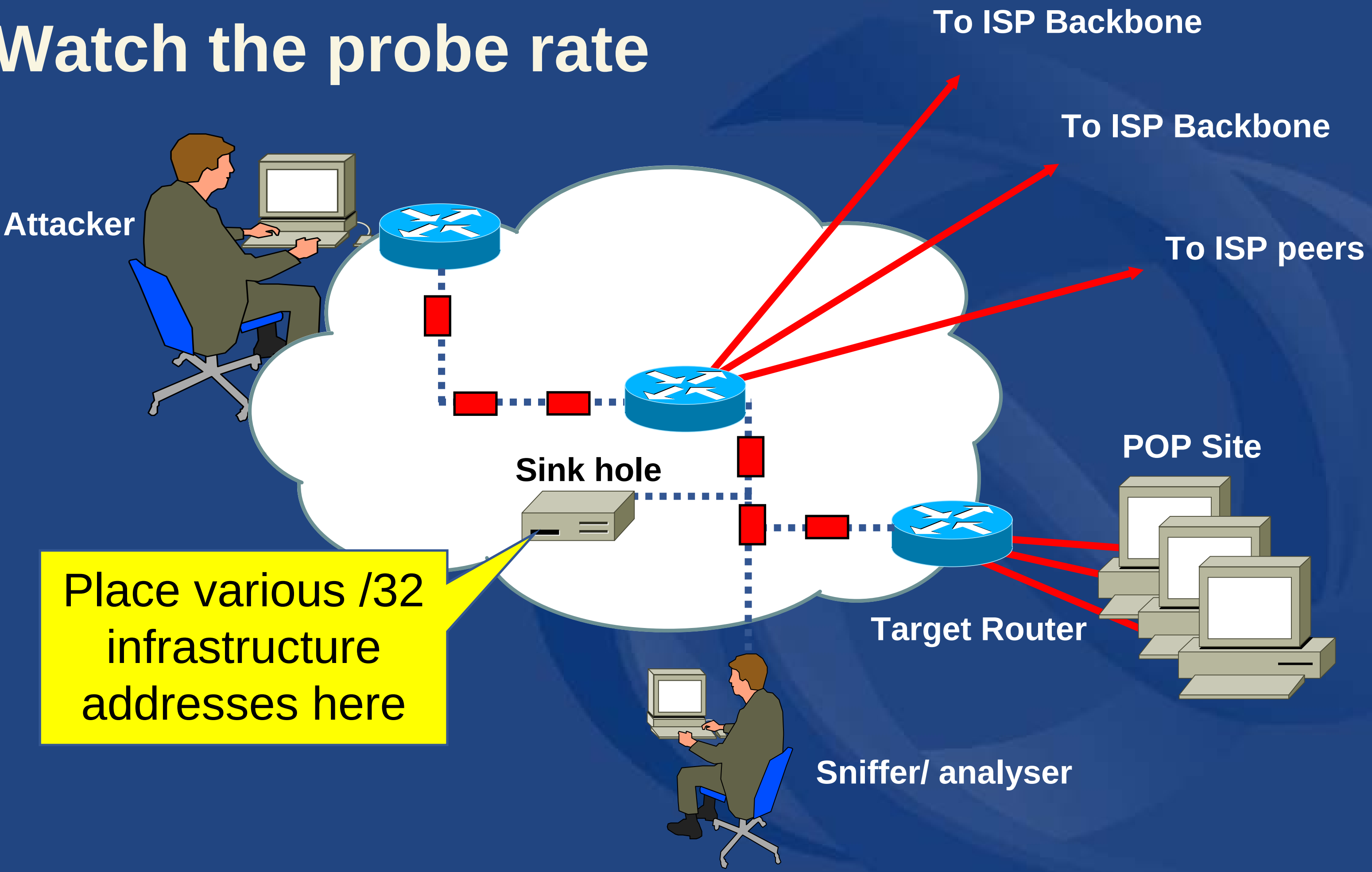
If A>>B (CPU too busy)

- Switching problems:
  - Cache misses: If flow not in cache, ask CPU!
  - DoS: spoofed addresses -> many cache misses
- Packet from/to router:
  - Routing, ARP, ICMP, SNMP, console, telnet, … Watch out: Too many ICMP could come from a route null0; use **no ip unreachables** or **ICMP Unreachable Rate-Limit**
- Packet with options (could be DoS)

Sink Holes as an attack identification tool

Sink Holes and attack identification

- Watch for backscatter
- Watch the probe rate



Place various /32 infrastructure addresses here

Sink Holes and attack identification (cont.)

Statistics from CAIDA‘s study (using just backscatter analysis)

- – 4,000 attacks per week
- – 40 - 200 concurrent attacks / hour
- – Most last 10 min’s - 2 hours (avg 1/2 hour)
- – Romania (15%) and Brazil (7%)

Identifying an attack

What about those detection systems?

- Try them
- Sink Hole network is a good place to put them (sucks in all the junk and lets the IDS sort it out)
- Always be on the lookout for a new tool, trick, feature, or capability

Questions

ISP Infrastructure Security Strategy

Phases of security strategy to manage ISP security process

- Classification -

Security phases

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post mortem

Classification

- Classification – understanding the type and damage effects of the attacks
- Know which component are getting hit
  - Own network
  - Customer network
- Determine the rest of the incident response
- Tools available in the market
- Doing it without crashing the router

Classification (cont.)

- What type of attack has been identified?
- Quality and quantity of the attack without jeopardising the services availability
  - Type of attack has been identify?
  - Effect of the attack on the victim(s)?
  - Next steps requirements (if needed)?

Classifying an attack

How are we being attacked?

- – Once the attack starts, how do you find specifics of the attack?
- – Customer might provide information
- – Tools and procedures needed inside an ISP to specific information on the attack
- – Minimum source addresses and protocol type

Classification objectives

Classification is all about collecting data so that you can gauge the risk for the next phases

- What is the target’s IP address and port?
- What is the protocol type?
- What is the rate of the attack?
- What are the source addresses?

With this information you can traceback and consider a reaction/counter-measure

Classification ACLs

Classification ACLs

Most common technique used to tweak a router into a pseudo packet sniffer

- An Access Control List (ACL) with a series of permit statements are used to view into the traffic flow
- Access List Entry (ACE) counters are used to find which protocol types are potential culprits
- Once the protocol type is suspected, another permit ACL with log statements is used to capture some of the packet characteristics

Characterising and tracing packet floods using Cisco routers

http://www.cisco.com/warp/public/707/22.html

Classification ACLs

Use ACL to find out the characteristics of the Attack

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any range 0 65535
access-list 169 permit ip any any

interface serial 0
ip access-group 169 out
```

Classification and traceback ACLs

Use the show access-list 169 to see which protocol is the source of the attack:

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374
    matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

Classification and traceback ACLs (cont.)

- *Classification ACLs* are applied as close to the customer as possible
  - Mainly on the customer's ingress interface to the ISP with an output ACL
- Once you know what protocol type, you can dig into more specifics by logging some of the packets
  - The first step is to use the ACL "log-input" function to grab a few packets
  - Quick in and out is needed to keep the router for overloading with logging interrupts to the CPU

Classification and traceback ACLs (cont.)

Preparation

- Make sure your logging buffer on the router is large
- Create the ACL
- Turn off any notices/logging messages to the console or vty (so you can type the command *no access-group 170*
- Be ready to remove the ACL! Only need a couple of packets

Classification and traceback ACLs (cont.)

```
access-list 170 permit icmp any any echo
access-list 170 permit icmp any any echo-reply log-input
access-list 170 permit udp any any eq echo
access-list 170 permit udp any eq echo any
access-list 170 permit tcp any any established
access-list 170 permit tcp any any
access-list 170 permit ip any any

interface serial 0
ip access-group 170 out
! Wait a short time - (i.e 10 seconds)
no ip access-group 170 out
```

Classification and traceback ACLs (cont.)

- Validate the capture with *show access-list 170*; make sure it the packets we counted

- Check the log with *show logging* for addresses:

```
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.212.72 (Serial0
*HDLC*) -> 198.133.219.25 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.154 (Serial0
*HDLC*) -> 198.133.219.25 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.15 (Serial0
*HDLC*) -> 198.133.219.25 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.142 (Serial0
*HDLC*) -> 198.133.219.25 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.47 (Serial0
*HDLC*) -> 198.133.219.25 (0/0), 1 packet
```

Classification ACLs - hints

- Create preset Classification ACLs and put them on every router
  - The will only be used when you need them
  - Allows for standard procedures to be used

Sink Hole classification technique

Sink Hole classification technique

- Is it worth the risk to make config changes while a customer is under attack on a aggregation router with hundreds of customers connected to it?
  - Config changes when the network is under duress can and will cause more problems (it is not an “IOS” think – this applies to any network)
- What would help is if the attack flow can be shifted from the target (i.e. customer) to some other router where the risk is manageable
- Enter the Sink Hole router
  - Similar to a Unix HoneyPot

Sink Hole classification technique (cont.)

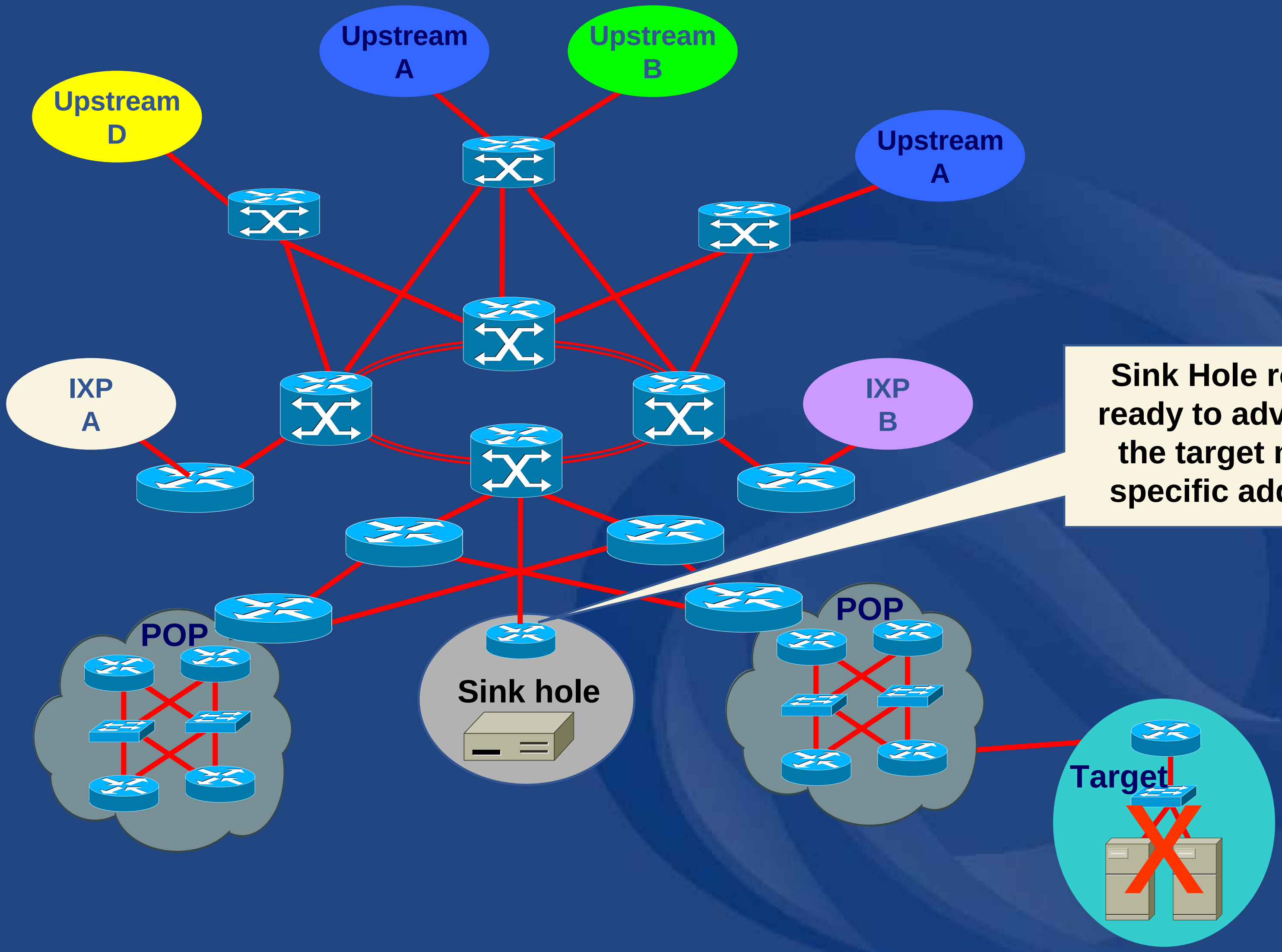
Sink Hole router preparation:

1. Router with really fast packet dropping capability, software features, and a connection to the network (were traffic to it would not endanger the network)

2. BGP session (Route Reflector Client). The target's more specific address will get advertised from here

3. Packet Filters, syslog exports, and a way to analyze the logs from the ACL's log-input

Sink Hole classification technique (cont.)



Sink Hole router ready to advertise the target more specific address

Sink Hole classification technique (cont.)

Sink Hole classification – Activation

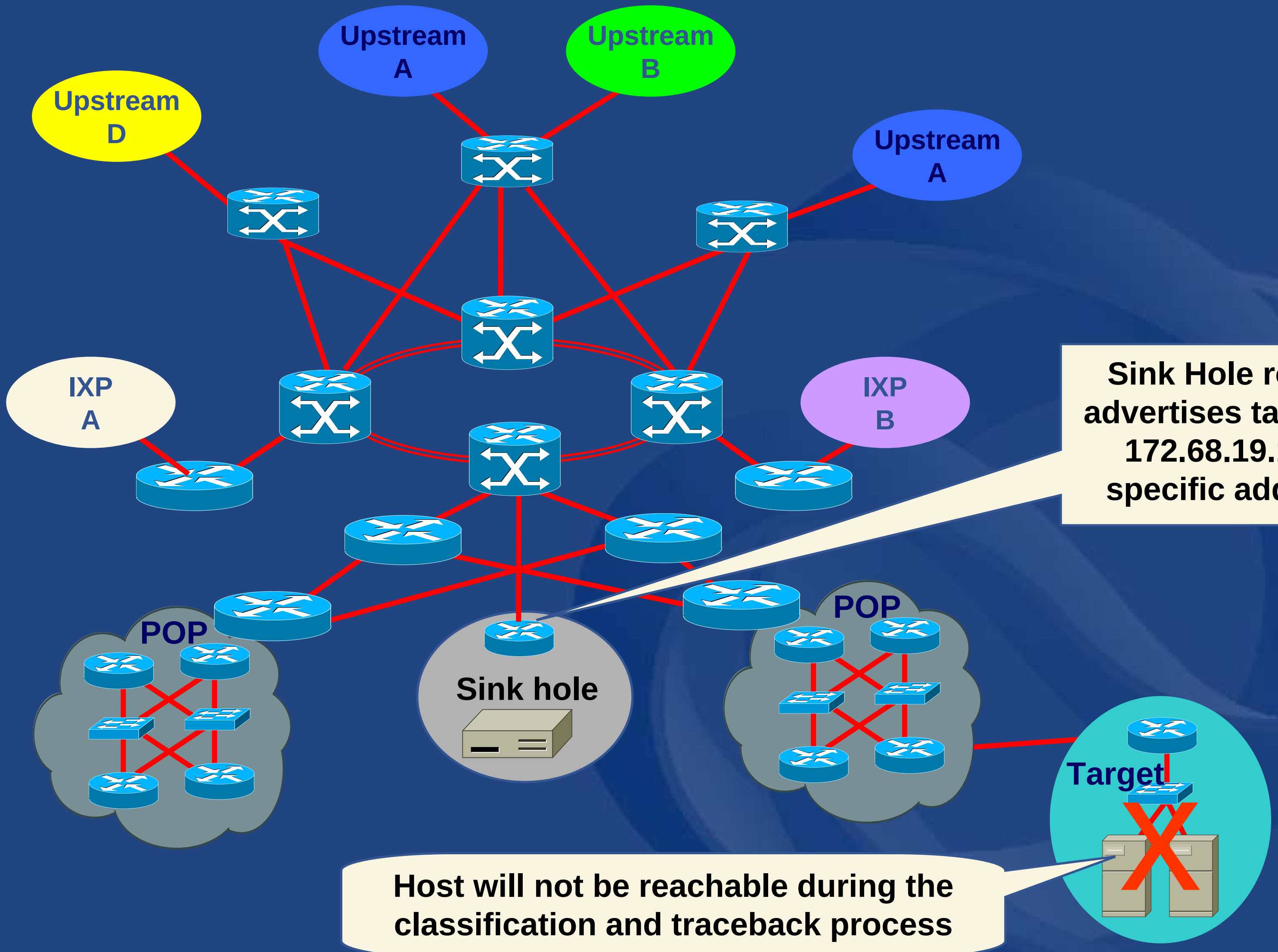
1. Customer notifies ISP that they are under attack and need help. ISP lets the customer know that they will take the targeted host's IP address and redirect it to classify and traceback (see Backscatter Traceback technique)

2. Sink Hole Router advertises the /32 address that is under attack

3. All traffic for that /32 shifts to the Sink Hole Router. ACL Packet Classification, Netflow classification or host based (specialized box) is done on a section of the ISPs network built to be attacked

4. Massive Aggregation Router is not touched

Sink Hole classification Technique



Sink Hole router advertises target IP 172.68.19.1/32 specific address

Host will not be reachable during the classification and traceback process

Sink Hole – How to classify?

Now that you have the attack flow heading into the sink hole, how do you classify the attack?

- ACL Classification
- Netflow Classification
- Sniffer/Ethereal Classification
- TCPDump Classification

Questions?

ISP Infrastructure Security Strategy

Phases of security strategy to manage ISP security process

- Traceback -

Security phases

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post Mortem

Traceback

- Traceback – finding information from where the attack coming from
- 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
- Traceback to the edge of the networks
- Continue traceback over ISPs boundary

Traceback (cont.)

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

Traceback attacks to their source

- Valid IPv4 source addresses are easy
  - Gets harder with DDoS – where there are a multitude of source addresses
- Spoofed IPv4 source addresses are more challenging
  - Backscatter Traceback technique makes a difference
- Inter-provider hand off of the traceback is the big challenge today

Traceback essentials

- If source prefix is not spoofed:
  - Routing table
  - Internet Routing Registry (IRR)
  - direct site contact
- If source prefix is spoofed:
  - Trace packet flow through the network
  - Find upstream ISP
  - Upstream needs to continue tracing

Traceback valid IPv4 source addresses

Use Regional Internet Registries (RIRs):

RIPENCC:	whois.ripe.net
APNIC:	whois.apnic.net
ARIN:	whois.arin.net
LACNIC :	whois.lacnic.net

```
$ whois –h whois.apnic.net 202.12.29.173

inetnum:      202.12.28.0 - 202.12.29.255
netname:      APNIC-AP
descr:        Asia Pacific Network Information Center, Pty. Ltd.
descr:        Level 1 - 33 Park Road.
descr:        Milton QLD 4064
descr:        Australia
country:      AU
admin-c:      AIC1-AP
tech-c:       NO4-AP
mnt-by:       APNIC-HM
changed:      technical@apnic.net 19980918
status:       ASSIGNED PORTABLE
source:       APNIC
```

Traceback valid IPv4 source addresses (cont.)

```
$ whois –h whois.apnic.net 202.12.29.173

inetnum:     202.12.28.0 - 202.12.29.255
netname:  APNIC-AP
descr:    Asia Pacific Network Information Center, Pty. Ltd.
descr:       Level 1 - 33 Park Road.
descr:       Milton QLD 4064
descr:       Australia
country:     AU
admin-c:     AIC1-AP
tech-c:      NO4-AP
mnt-by:      APNIC-HM
changed:     technical@apnic.net 19980918
status:      ASSIGNED PORTABLE
source:      APNIC
```

```
role:        APNIC Infrastructure Contact
address:     Level 1
address:     33 Park Road
address:     Milton QLD 4064
country:     AU
phone:       +61 7 3858 3100
fax-no:      +61 7 3858 3199
e-mail:      helpdesk@apnic.net
admin-c:     DNS3-AP
tech-c:      NO4-AP
nic-hdl:     AIC1-AP
remarks:     Infrastructure Contact for APNICs own-use
network blocks
notify:      dbmon@apnic.net
mnt-by:      MAINT-APNIC-AP
changed:     hm-changed@apnic.net 20020211
source:      APNIC
```

Traceback spoofed IPv4 addresses

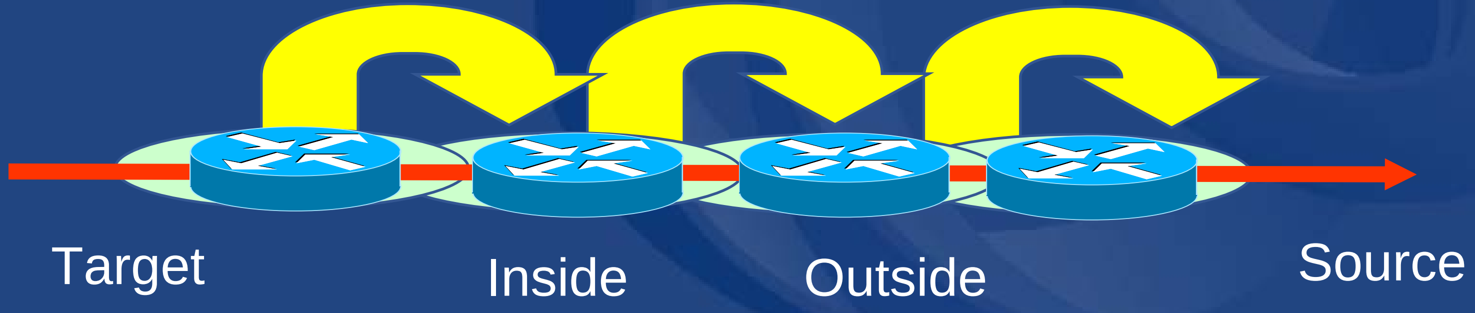
From where are we being attacked (inside or outside)?

- Once you have a fundamental understanding of the type of attack (source address and protocol type), you then need to track back to the ingress point of the network
- Two techniques — hop by hop and jump to ingress

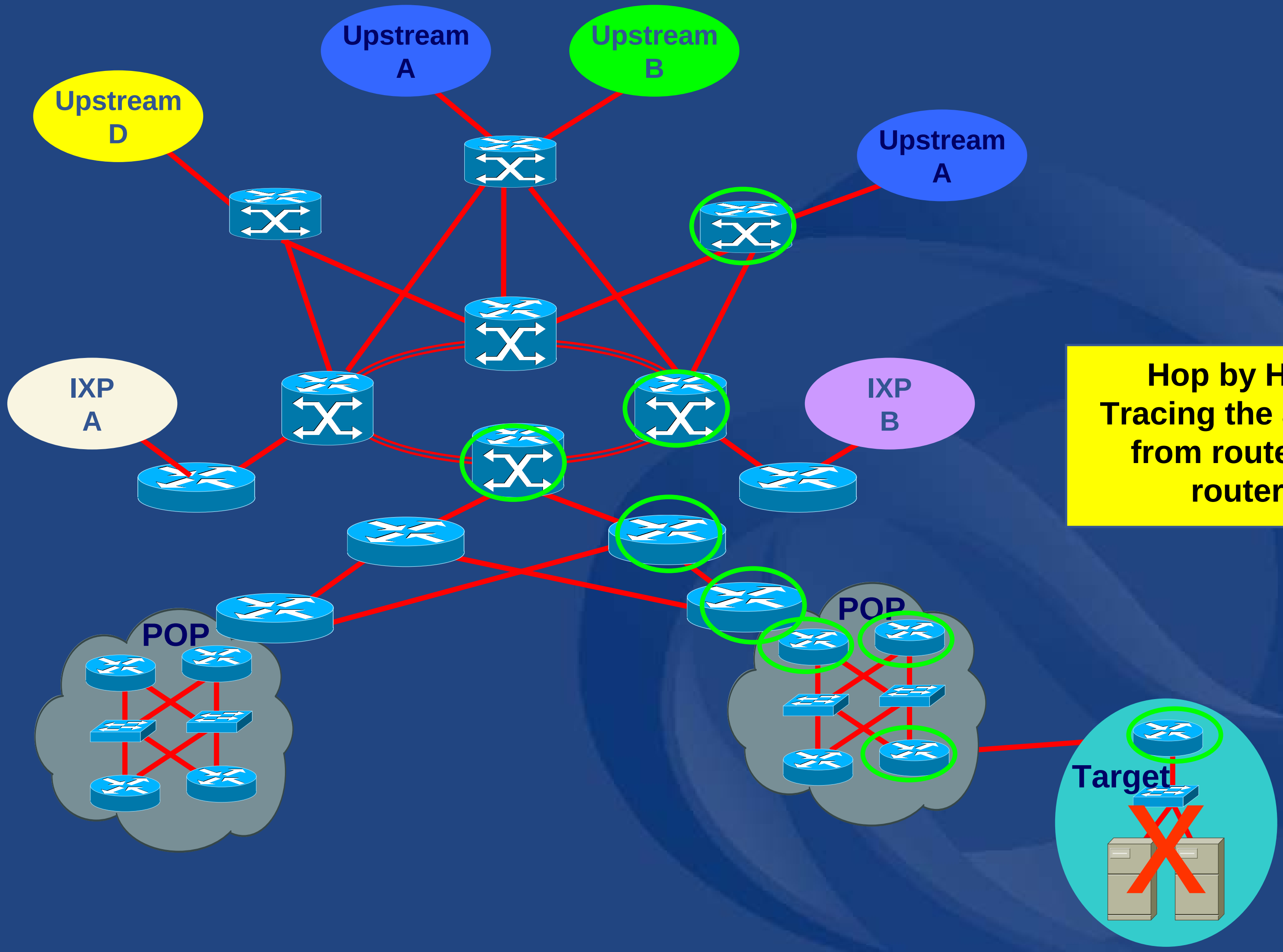
Traceback via Hop by Hop technique

Hop by hop tracebacks takes time

- Starts from the beginning and traces to the source of the problem
- Needs to be done on each router
- Often requires splitting—tracing two separate paths
- Speed is the limitation of the technique



Traceback - Hop by Hop technique (cont.)

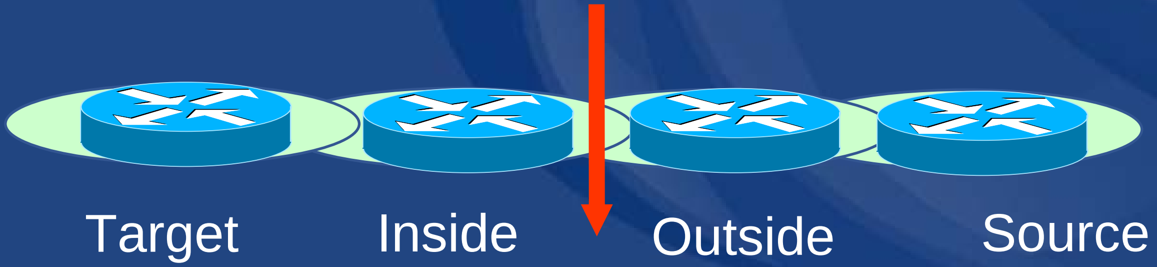


Hop by Hop Tracing the attack from router to router

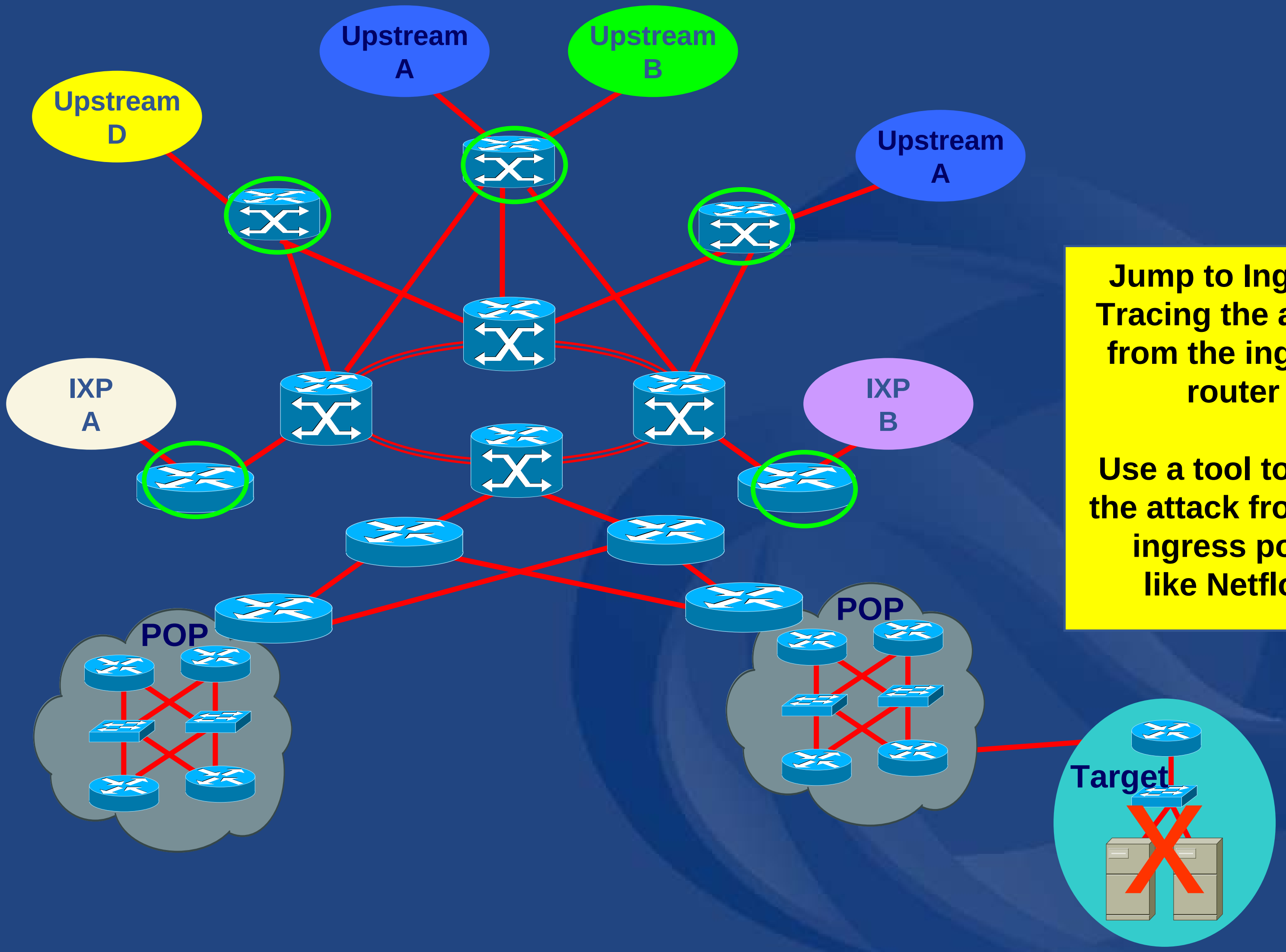
Traceback - Jump to Ingress technique

Jump to ingress tracebacks divides the problem in half

- Is the attack originating from inside the ISP or outside the ISP?
- Jumps to the ISP’s ingress border routers to see if the attack is entering the network from the outside
- Advantage of speed—are we the source or someone else the source?



Traceback - Jump to Ingress Technique (cont.)



Jump to Ingress Tracing the attack from the ingress router

Use a tool to spot the attack from the ingress point like Netflow

Traceback spoofed IPv4 addresses (cont.)

The techniques:

- Apply temporary ACLs with log-input and examine the logs
- Backscatter traceback technique

Traceback with ACLs

```
access-list 170 permit icmp any any echo
access-list 170 permit icmp any any echo-reply log-input
access-list 170 permit udp any any eq echo
access-list 170 permit udp any eq echo any
access-list 170 permit tcp any any established
access-list 170 permit tcp any any
access-list 170 permit ip any any

interface serial 0
ip access-group 170 out
! Wait a short time - (i.e 10 seconds)
no ip access-group 170 out
```

Traceback with ACLs

- Original technique for doing tracebacks
- Hazard - inserting change into a network that is under attack
- Hazard - log-input requires the forwarding ASIC to punt the packet to capture log information
- BCP is to apply the filter, capture just enough information, then remove the filter

Backscatter traceback technique

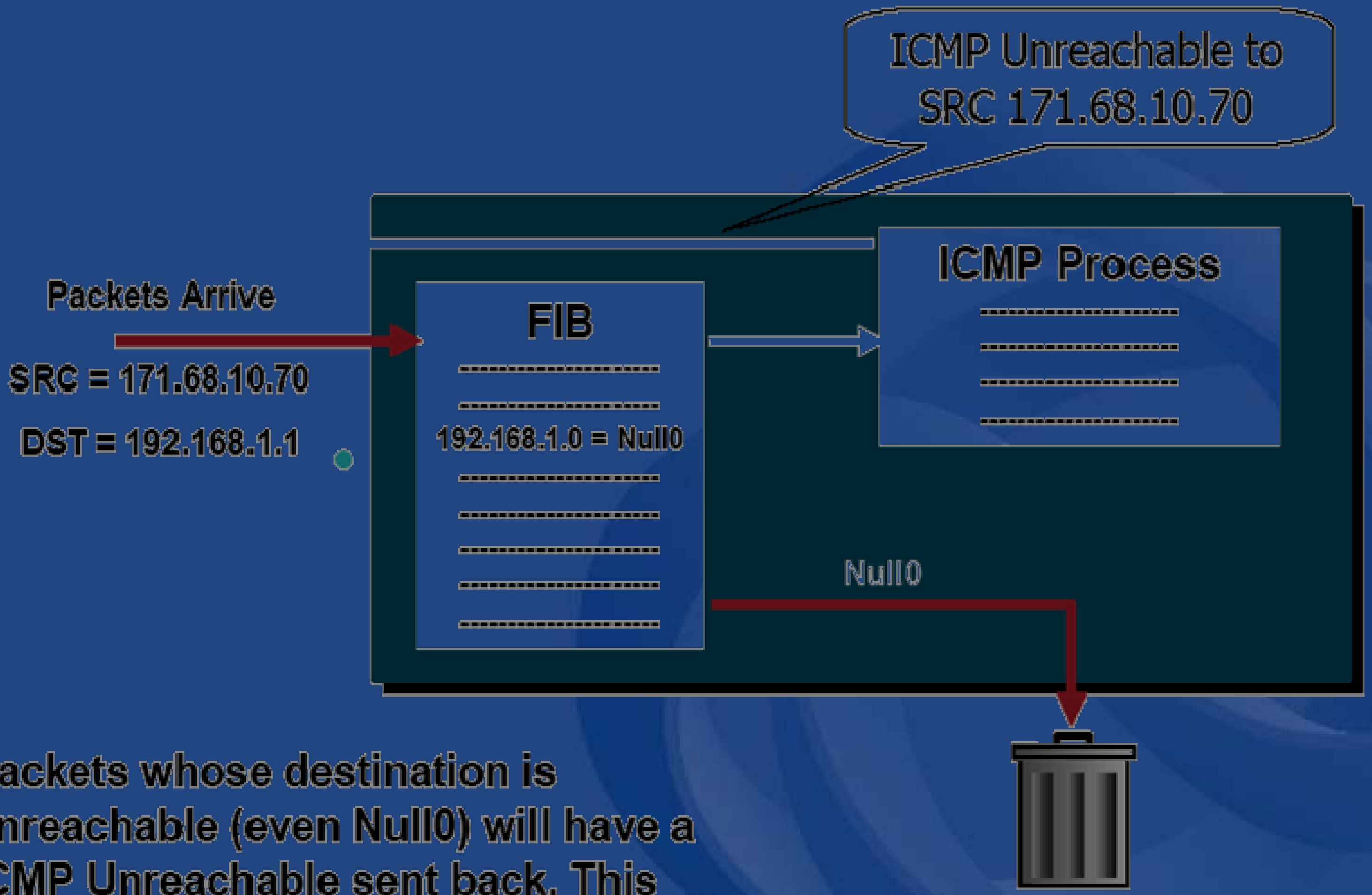
Three key advantages:

- Reduced operational risk to the Network while traceback is in progress
- Speedy Traceback
- Ability to hand off from one ISP to another – potentially tracing back to it's source

Backscatter traceback technique (cont.)

- Created by Chris Morrow and Brian Gemberling @ UUNET as a means of finding the entry point of a spoofed DOS/DDOS
  - http://www.secsup.org/Tracking/
- Combines the Sink Hole router, Backscatter effects of Spoofed DOS/DDOS attacks, and remote triggered Black Hole Filtering to create a traceback system that provides a result within 10 minutes

Backscatter traceback technique (cont.)



Packets whose destination is unreachable (even Null0) will have a ICMP Unreachable sent back. This "unreachable noise" is backscatter.

Backscatter traceback preparation

1. Sink Hole Router/Network connected to the network ready to classify the traffic and a device to analyze logs, etc

   – Use one router to do both the route advertisement and logging OR break them into two separation routers

     - one for route advertisement and the other to accept/log traffic

   – It can also be used for other Sink Hole functions while not using the traceback technique

   – Sink Hole Router can be a iBGP Route Reflector into the network

Backscatter traceback preparation (cont.)

```
router bgp 31337
!
! set the static redistribution to include a route-map so we can filter
! the routes somewhat... or at least manipulate them
! redistribute static route-map static-to-bgp
!
! add a stanza to the route-map to set our special next hop
!
route-map static-to-bgp permit 5
match tag 666
set ip next-hop 172.20.20.1
set local-preference 50
set origin igp
```

Backscatter traceback preparation (cont.)

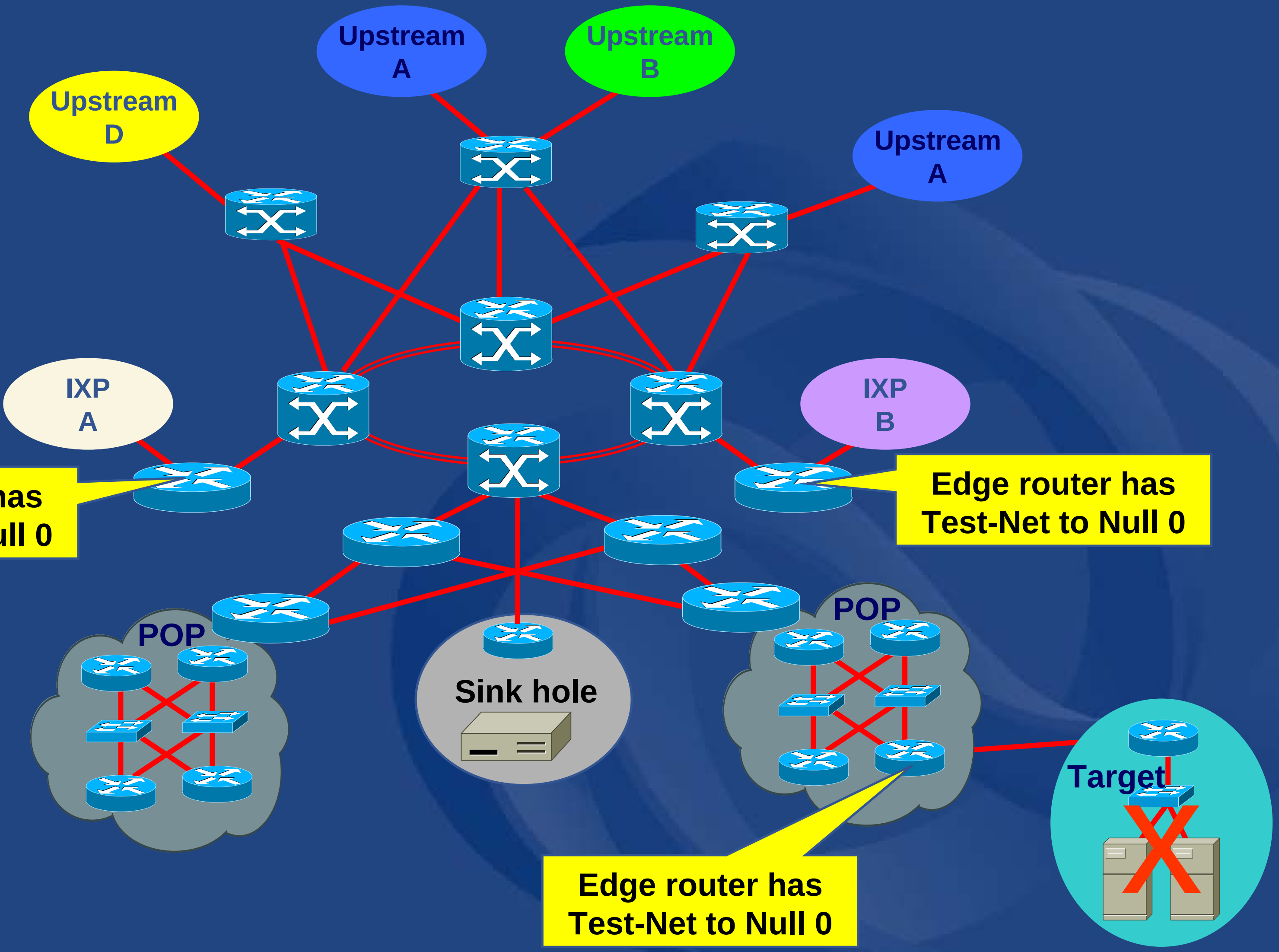
2. All edge devices (routers, NAS, IXP Routers, etc) with a static route to Null0. The Test-Net is a safe address to use (192.0.2.0/24) since no one is using it

   – Cisco: **ip route 172.20.20.1 255.255.255.255 Null0**

   – **Routers also need to have ICMP Unreachables working. If you have ICMP Unreachables turned off (i.e. *no ip unreachables* on a Cisco), then make sure they are on**

   – **If ICMP Unreachable Overloads are a concern, use a ICMP Unreachable Rate Limit (i.e. *ip icmp rate-limit unreachable* command on a Cisco)**

Backscatter traceback technique



Edge router has Test-Net to Null 0

Edge router has Test-Net to Null 0

Edge router has Test-Net to Null 0

Backscatter traceback preparation (cont.)

3. Sink Hole Router advertising a large block of unallocated address space with the BGP no-export community and BGP Egress route filters to keep the block inside. 96.0.0.0/3 is an example

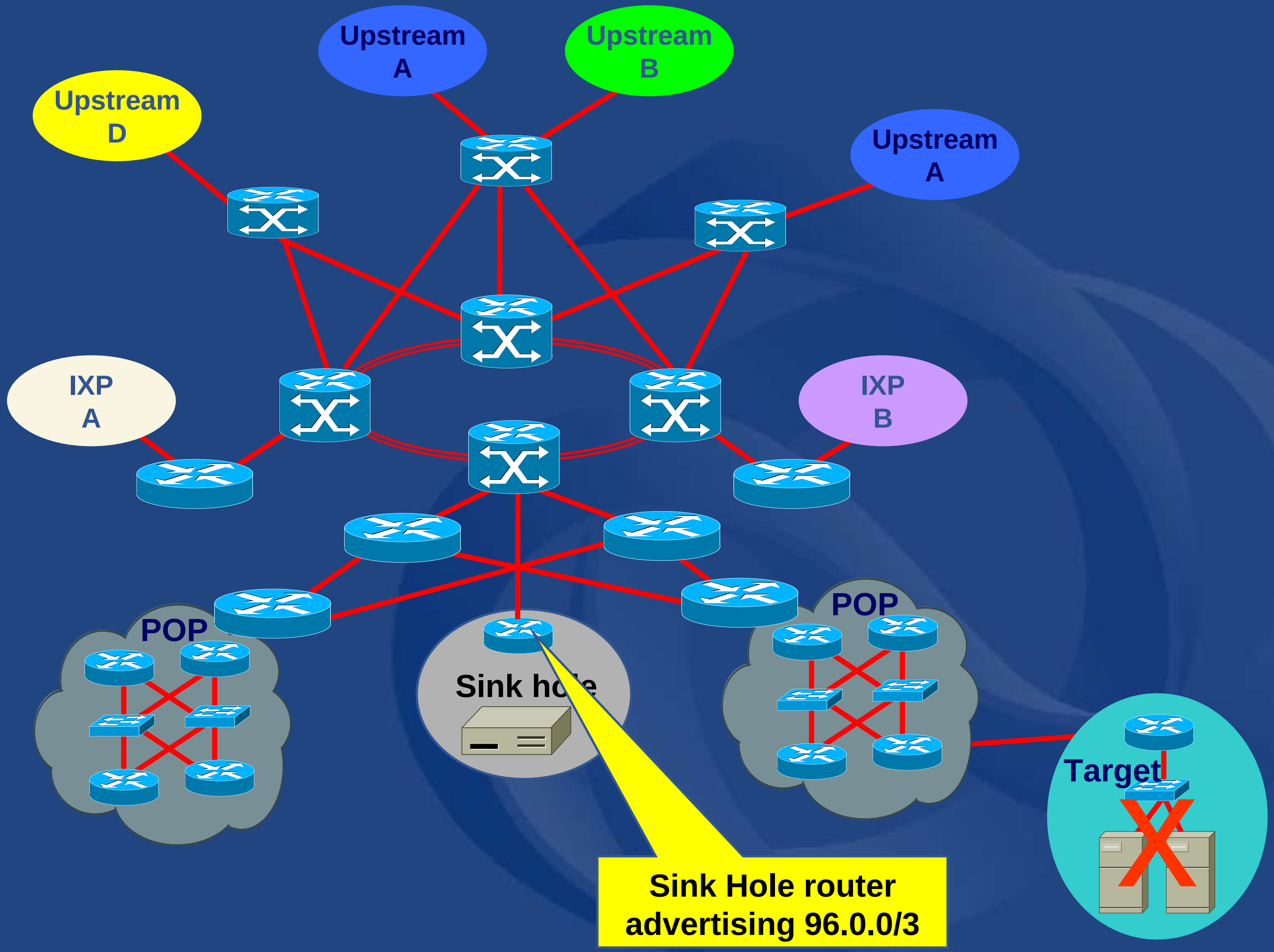
   – Check with IANA for unallocated blocks:

     www.iana.org/assignments/ipv4-address-space

   – BGP Egress filter should keep this advertisement inside your network

   – Use BGP *no-export* community to insure it stays inside your network

Backscatter traceback technique



Sink Hole router advertising 96.0.0.0/3

Backscatter traceback activation

- Activation happens when an attack has been identified
- Basic Classification should be done to see if the backscatter traceback will work
  - May need to adjust the advertised block.
  - Statistically, most attacks have been spoofed using the entire Internet block

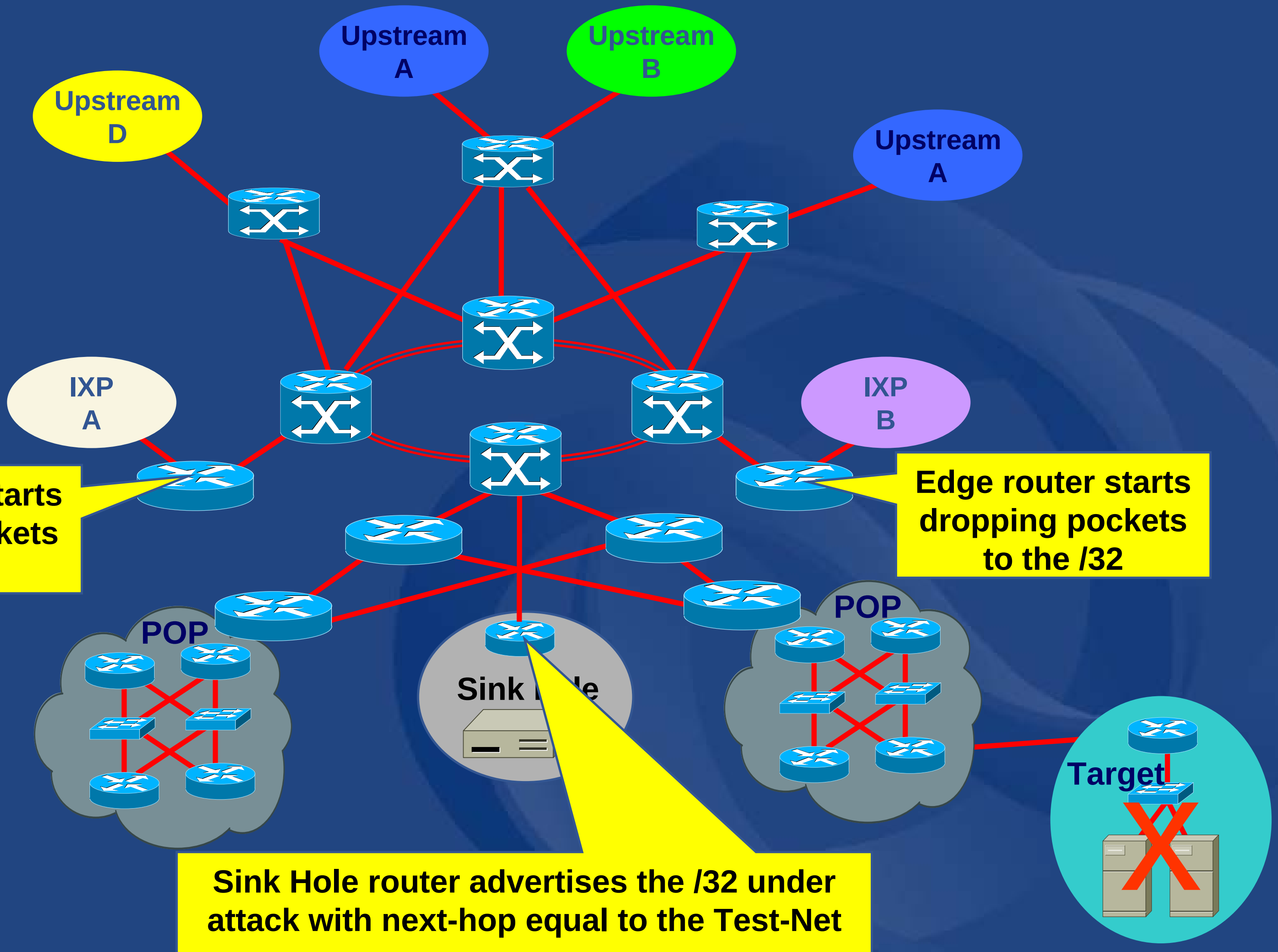
Backscatter traceback activation (cont.)

1. Sink Hole router advertises the /32 under attack into iBGP with. Advertised with a static route with the “666” tag:

```
ip route victimip 255.255.255.255 Null0 tag 666
```

The static triggers the routers to advertise the customer’s prefix

Backscatter traceback activation (cont.)



Edge router starts dropping pockets to the /32

Edge router starts dropping pockets to the /32

Sink Hole router advertises the /32 under attack with next-hop equal to the Test-Net

Backscatter traceback activation (cont.)

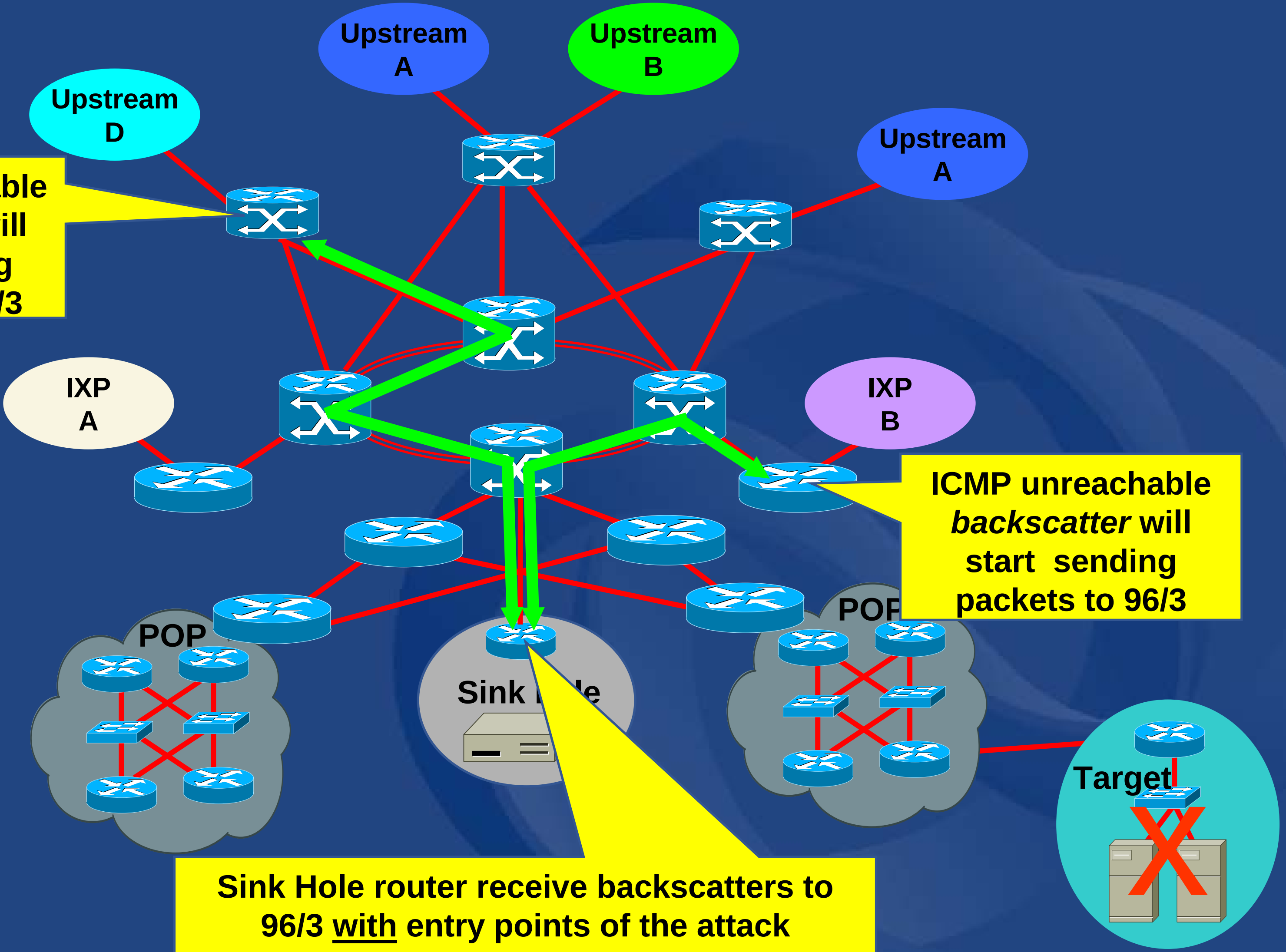
2. Black Hole Filtering is triggered by BGP through out the network. Packets to the target get dropped. ICMP Unreachable Backscatter starts heading for 96.0.0.0/3

   – Access list is used on the router to find which routers are dropping packets

```
access-list 101 permit icmp any any unreachables log

access-list 101 permit ip any any
```

Backscatter traceback activation (cont.)



ICMP unreachable *backscatter* will start sending packets to 96/3

ICMP unreachable *backscatter* will start sending packets to 96/3

Sink Hole router receive backscatters to 96/3 with entry points of the attack

Backscatter traceback activation (cont.)

```
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.47.251.104 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.70.92.28 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.222.127.7 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.96.223.54 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.14.21.8 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.105.33.126 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.77.198.85 (3/1), 1 packet
SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18
-> 96.50.106.45 (3/1), 1 packet
```

Questions

- Pulling down all the traffic into a Sink Hole could be very dangerous
  - Yes. Make sure you’ve integrated in the network so when it melts down, it will not impact the network
- Advertising large chunks of address space (I.e. 64/8) to do the backscatter traceback could be dangerous
  - Murphy’s Law of Networking – Layered checks should be used – Egress BGP filtering + no-export community

Traceback summary

- Hop by Hop traceback never really work
  - Know how it works, but look to the operationally feasible techniques
- Backscatter Traceback works with a wide range of attacks
  - It is not just UUNET anymore
  - Successful inter-provider tracebacks are happening

Questions?

ISP Infrastructure Security Strategy

Phases of security strategy to manage ISP security process

- Reaction -

Security phases

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post Mortem

Reaction

- Reaction – Doing something to counter the attack
  - Should you mitigate the attack?
  - Can router ACL do the job?
  - How to keep customer attack from shifting to your network

Potential responses

- Do nothing about the attack
- Notify the customer
- Enable packet filters
- Enable Rate Limits
- Redirect to Sinkholes and analyse the packets
- Activate remote-triggered drop
    - Black hole (destination = Null port)
    - Customers may perform

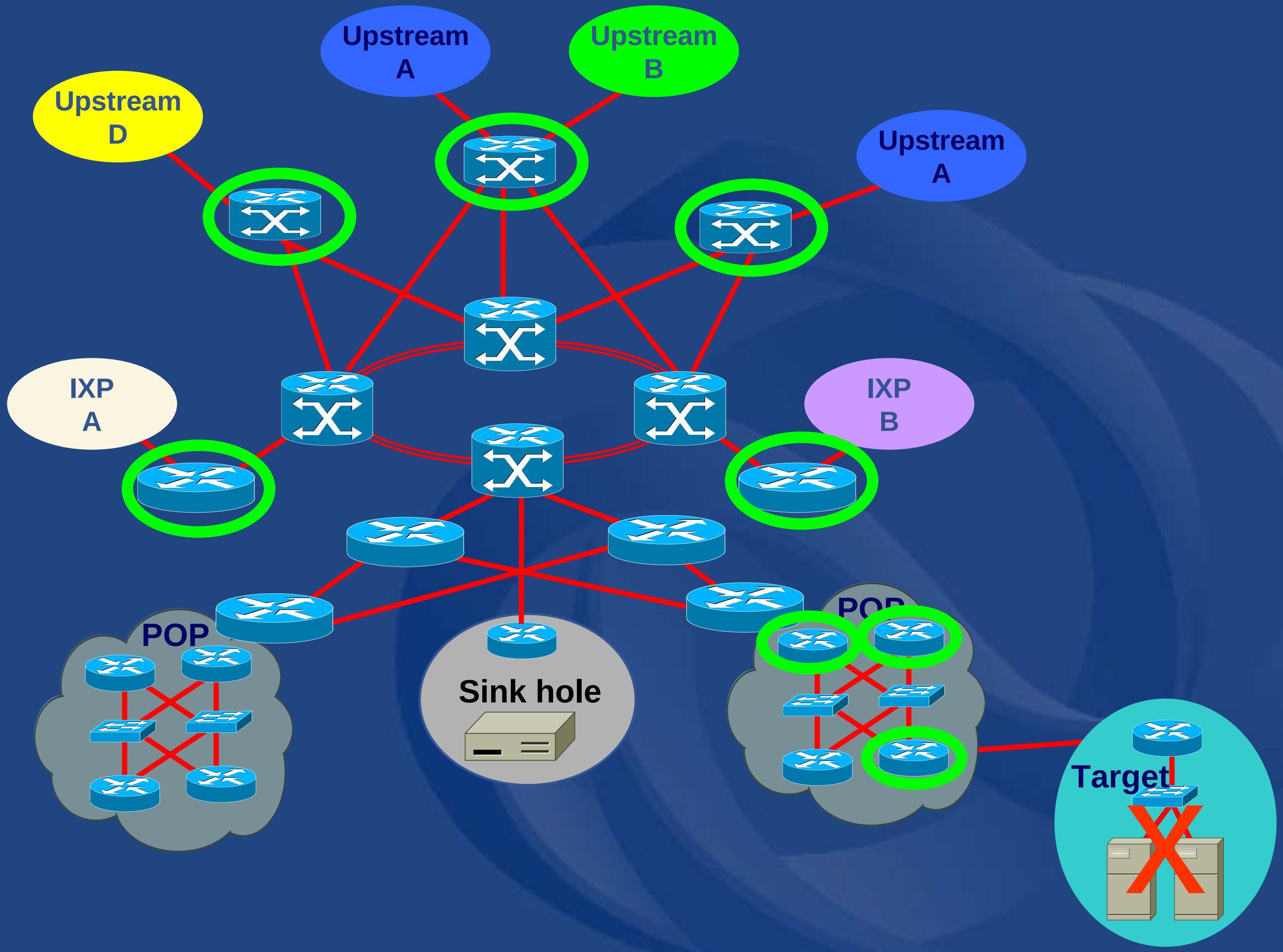
React to the attack

- Do something to mitigate the impact of the attack OR stop the attack
  - Options can be everything from:
    - do nothing
    - doing something but might cause other problems
    - unplug from the source of the attack

- Most ISPs try to help their customers
  - Rate-limit the attack
  - Drop the packets based on a list of source addresses

NOTE: **Reactions need to be fast and flexible**

Where to react?



React to the attack

Techniques used to drop or rate limit:

- ACLs - Manual upload
- uRPF - Remote trigger via BGP
- CAR - Manual upload or remote trigger via BGP
- Sink Holes

Reacting with ACLs

Reacting to an attack with ACL

- Traditional way to stop attacks
- Scaling issues encountered:
  - Updates of ACLs on many routers is a pain ☹
  - Additive ACLs when there are multiple attacks on multiple customers are a pain ☹

Know your ACLs

- Mission specific ASICs have injected mass confusion in the market
- Vendor Marketing and FUD wars confused the operators to understand the way to do with the ACLs on their equipment
- Find ways to run your own test
- Discover the “ACL performance envelop”

What needs to know

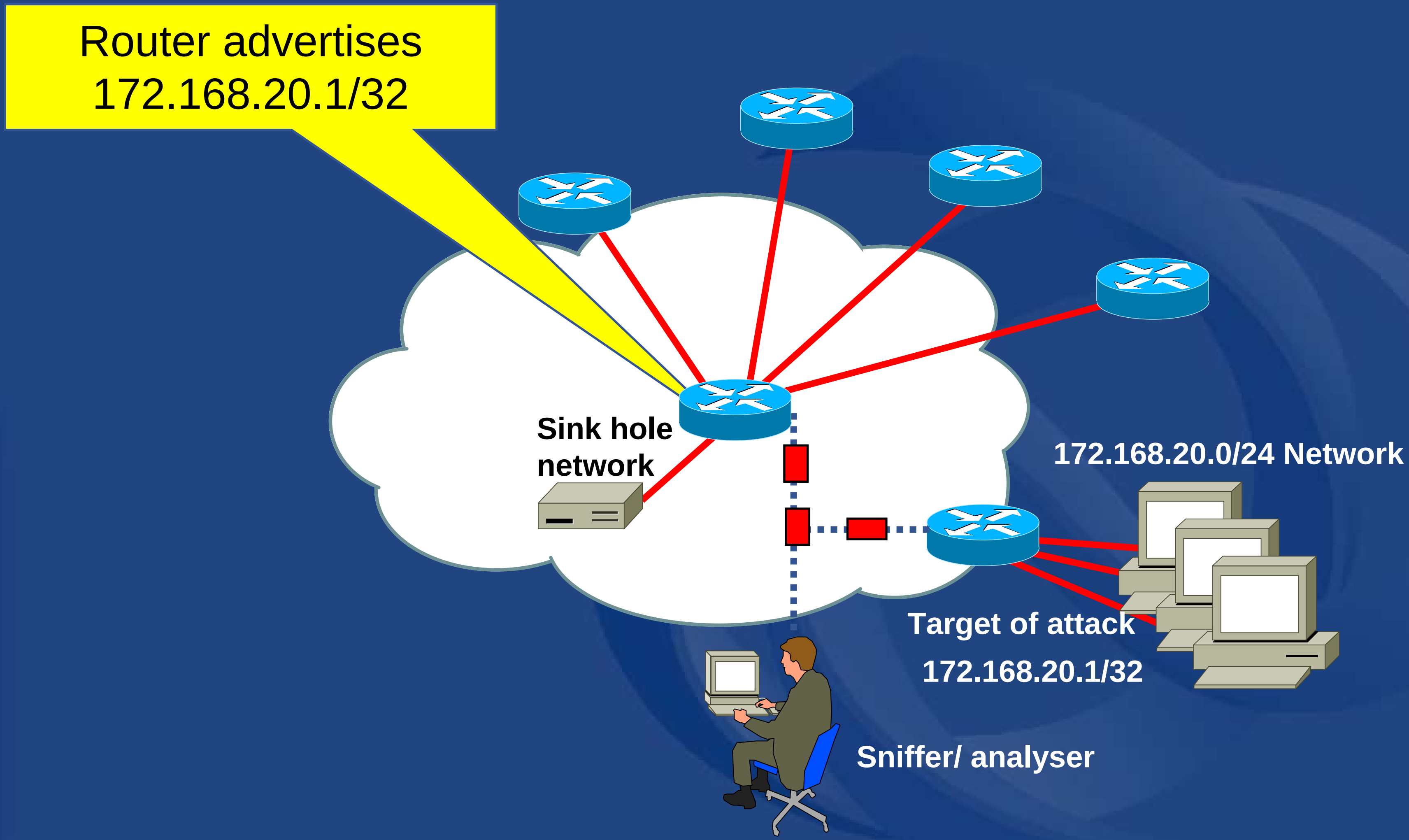
- Know the ACLs behavior with the router
  - How does the ACL load into the router?
    - Does it interrupt packet flow?
- Know the ASICs capacity for ACLs to avoid before getting punted to the supporting CPU?
- Understand effects of prefix range vs performance?
- Understand the effect of enabling multiple features vs performance?

Bottomline

- ISP Security Engineers have not time for Marketecture and slanted competitive bakeoffs
- Know the ACL’s performance envelop, to avoid any surprises!!
- ACLs do work through out network equipments. But always remember and need not to forget the “slammer”

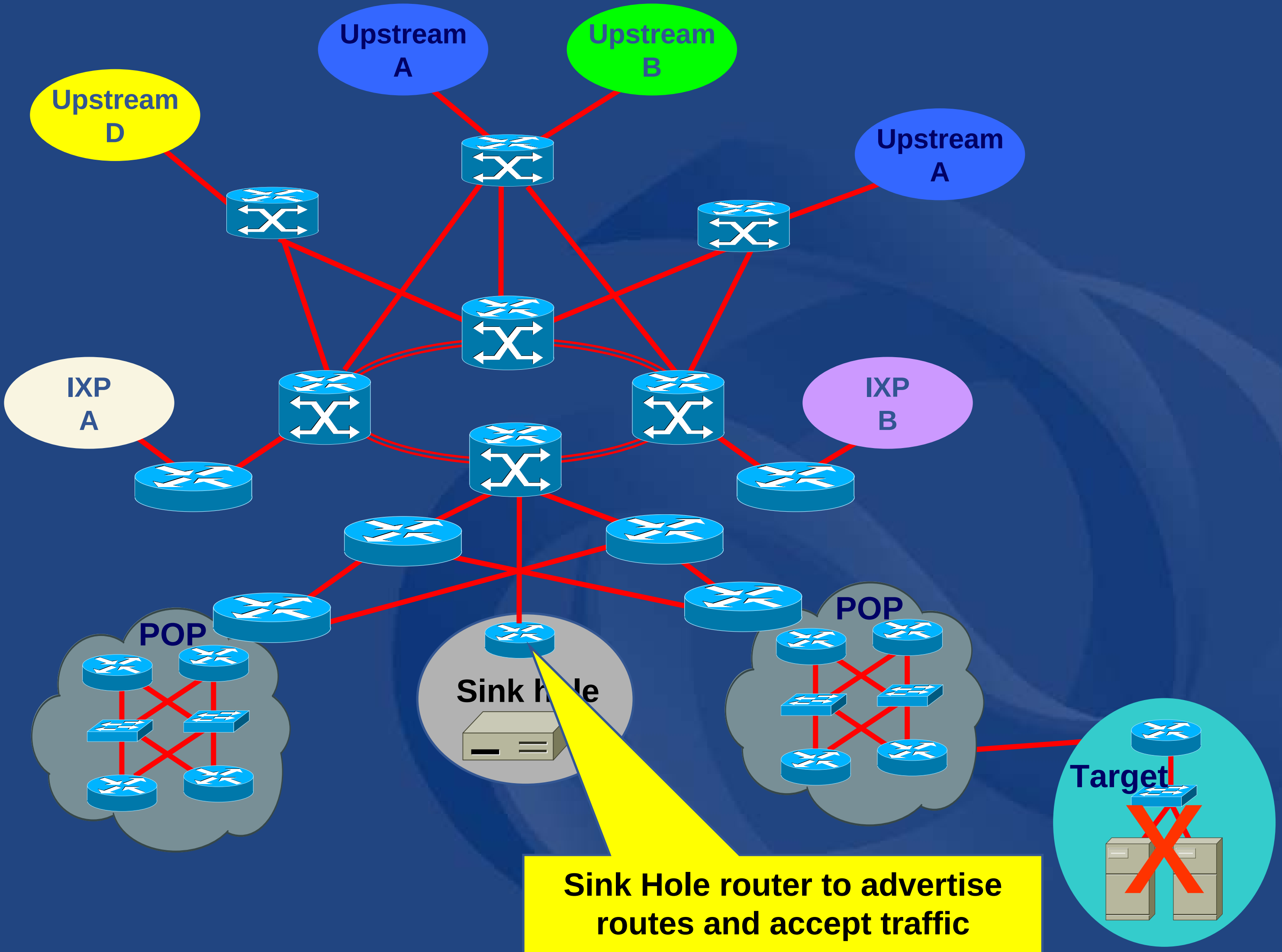
Reacting with Sink Holes

Sink Hole routers/networks



Router advertises 172.168.20.1/32

Sink Hole routers/networks (cont.)



Sink Hole router to advertise routes and accept traffic

Trigger router’s configuration

```
router bgp 109
.
redistribute static route-map static-to-bgp
.
!
route-map static-to-bgp permit 10
match tag 66
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export
set origin igp
!
route-map static-to-bgp permit 20
```

Considering the risk

Considering the risk

- By participating and doing something about an attack on someone else,
  - Customer networks
  - Other networks
- ISPs stop being a conduit and then becoming an active player in the game
  - The ISP is being part of the game and more likely get counter attacked for shutting down the original attack on the target

Questions?

ISP Infrastructure Security Strategy

Phases of security strategy to manage ISP security process

- Post Mortem -

Security phases

- Preparation
- Identification
- Classification
- Traceback
- Reaction
- Post Mortem

Post Mortem

- Post Mortem - analysing what just happened. Preparing measures to be taken to build resistance to the attack if it happens again
  - – It is a step that everyone mostly forget ☹
    - Is DOS attack that has happened the real threat?
    - Or just an smoke screen for something else that just happened?
  - – Things to do to make reactions to attacks faster, easier, less painful in the future?

Post Mortem (cont.)

- Analyse data, trends and discuss and document the attack
- Full history of the attack(s), trends, etc..
- Determine the effects
  - – What are affected?
  - – What else is affected?
  - – What if we have this in place?

Post analysis

- In reality a problem does not end when a short-term resolution is realized

- A problem ends only after completion of the following steps:
  - Conduct thorough analysis of the root cause of the attack(s)
  - Implement a long term fix to avoid it from happening again
  - Confirm the completion of fix with the affected clients

- While it is possible to determine that a root cause cannot be identified, that determination must be diligently arrived at through a level of rigor appropriate to the impact that may result if the problem recurs

Post analysis

- Learning from your mistakes is essential
- Do not wait until the next attack to implement the lessons of the last attack
  - Give time after each incident to see if processes, procedures, tools, techniques, and configurations can be improved
  - It is an arms race, those who learn from this mistakes do excel

Post analysis (cont.)

- #1 mistake of military planner is underestimating the capabilities and commitment of the enemy

- #2 mistake of military planner is thinking of *Fighting the Last War*

- This observation directly applies to ISP security

Analyse the event

- What systems were used to gain access
- What systems were accessed by the intruder
- What information assets were available to those systems?
- What did the intruder do after obtaining access?
- What is the intruder currently doing?

That means digging deep

Snort: http://www.snort.org/

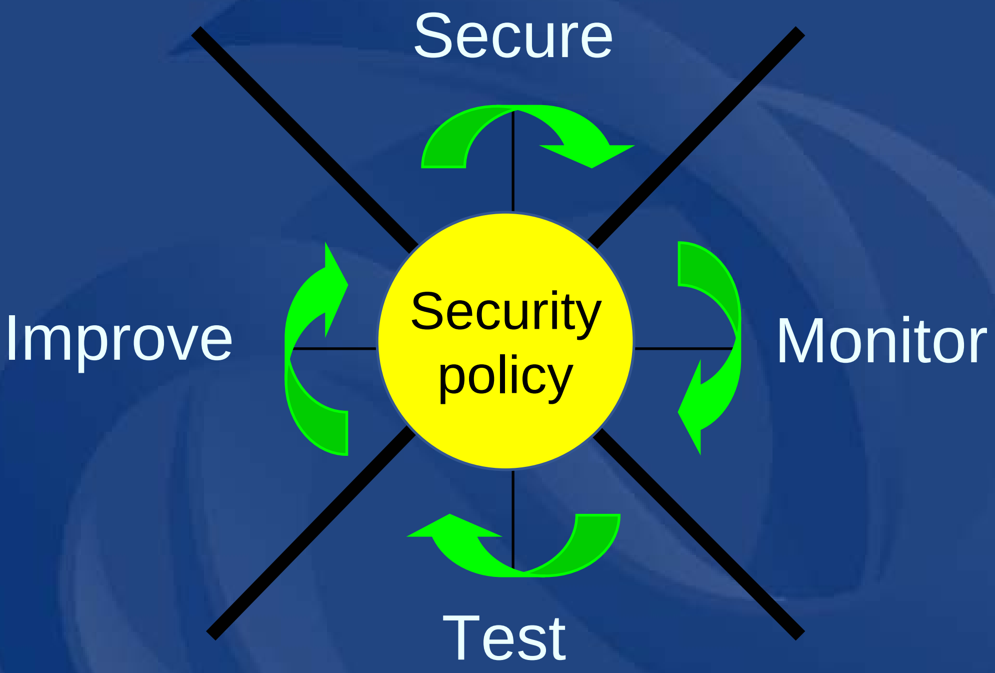
```
snort -v -d -e > snortfile.txt

07/23-07:27:09.153735 0:50:4:9D:73:81 -> 0:50:4:9D:7C:80 type:0x800
len:0x87

192.168.4.1:23 -> 192.168.4.6:1062 TCP TTL:64 TOS:0x0 ID:6245 DF
*****PA* Seq: 0x6E540C18 Ack: 0x27521710 Win: 0x7D78
TCP Options => NOP NOP TS: 197126 184309
FF FB 01 0D 0A 52 65 64 20 48 61 74 20 4C 69 6E .....Red Hat Lin
75 78 20 72 65 6C 65 61 73 65 20 36 2E 30 20 28 ux release 6.0 (
48 65 64 77 69 67 29 0D 0A 4B 65 72 6E 65 6C 20 Hedwig)..Kernel
32 2E 32 2E 35 2D 31 35 20 6F 6E 20 61 6E 20 69 2.2.5-15 on an i
36 38 36 0D 0A 686..
```

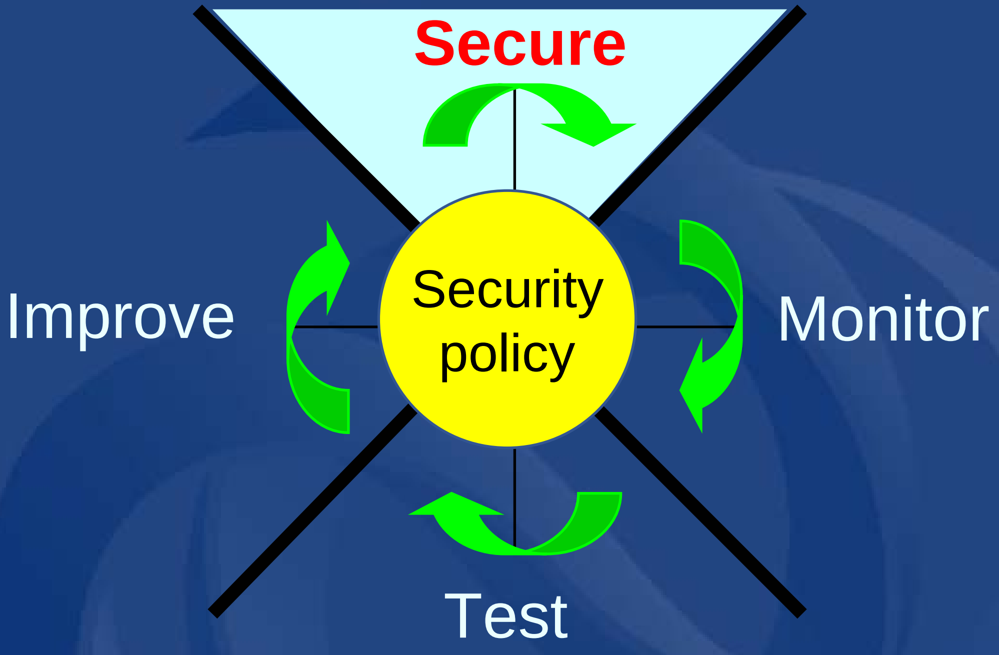
Network security as a continuous process

- Network security is a continuous process built around a security policy
  - Step 1: Secure
  - Step 2: Monitor
  - Step 3: Test
  - Step 4: Improve



Securing the network

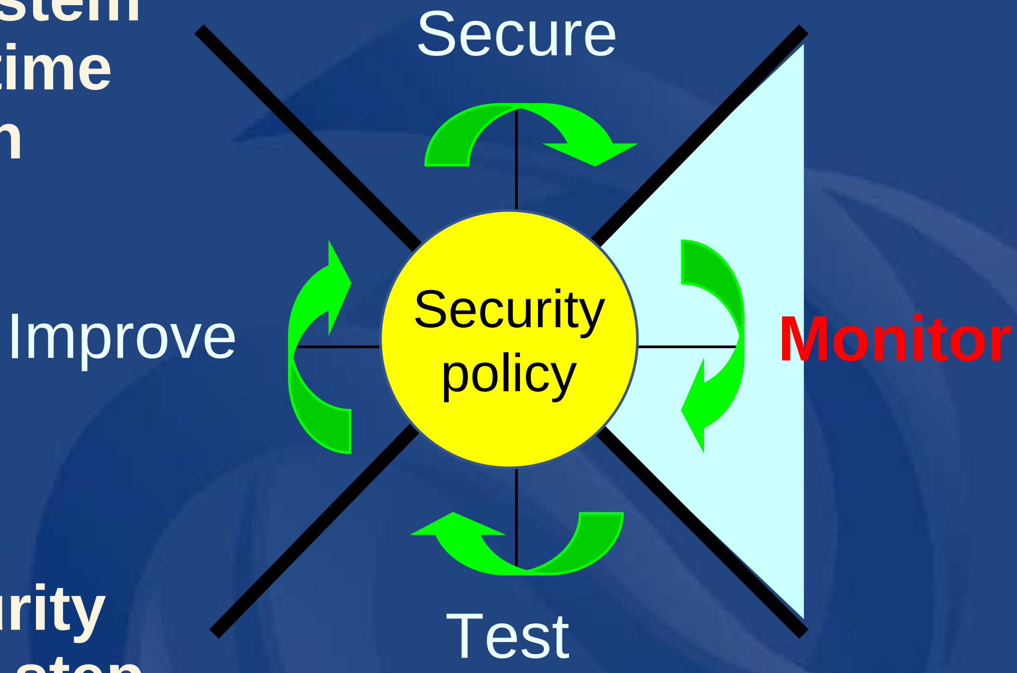
- Implement security solutions
  - Authentication, access controls, firewalls, encryption, patching, and so on
- Stop or prevent unauthorized access or activities and to protect information



Monitoring security

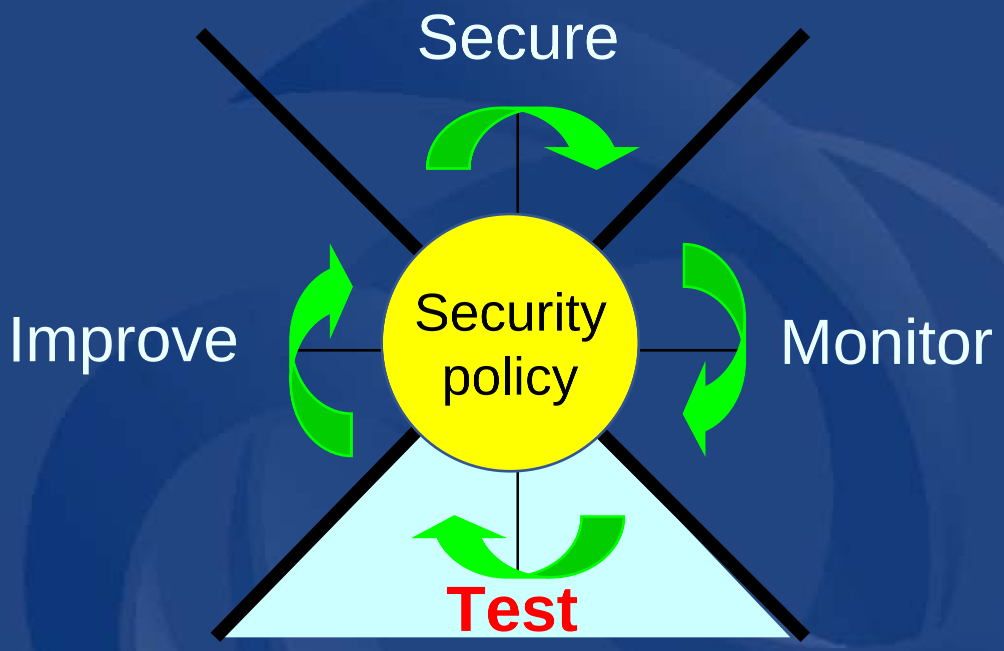
- Detect violations to the security policy System auditing and real-time intrusion detection

- Validates the security implementation in step one



Testing security

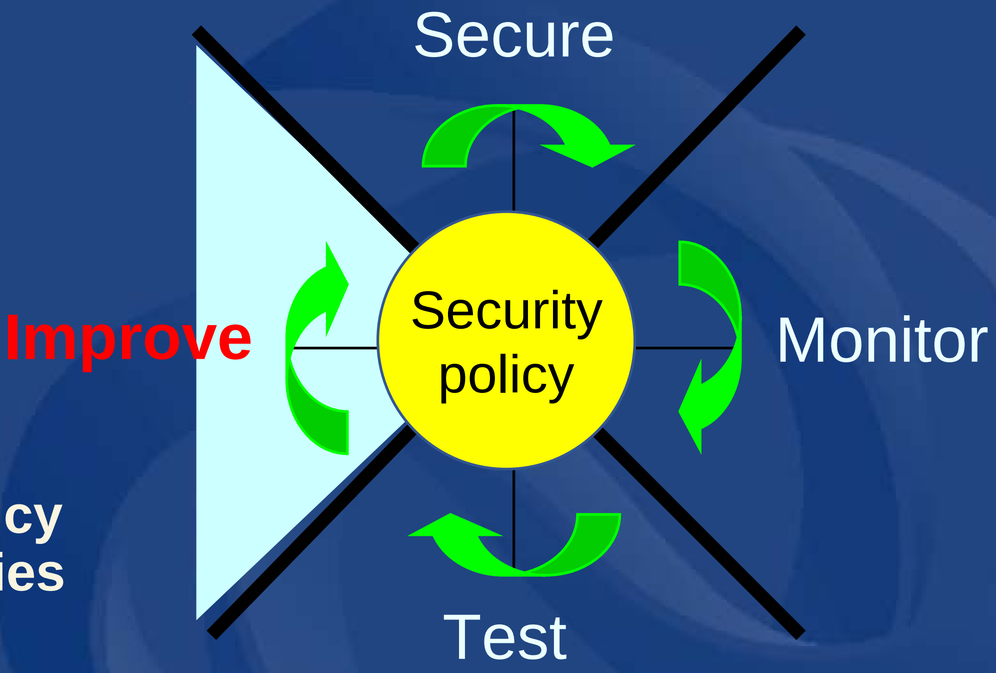
- Validates effectiveness of security policy implementation through system auditing and vulnerability scanning



Improving security

- Use information from the monitor and test phases, make improvements to the security implementation

- Adjust the security policy as security vulnerabilities and risks are identified



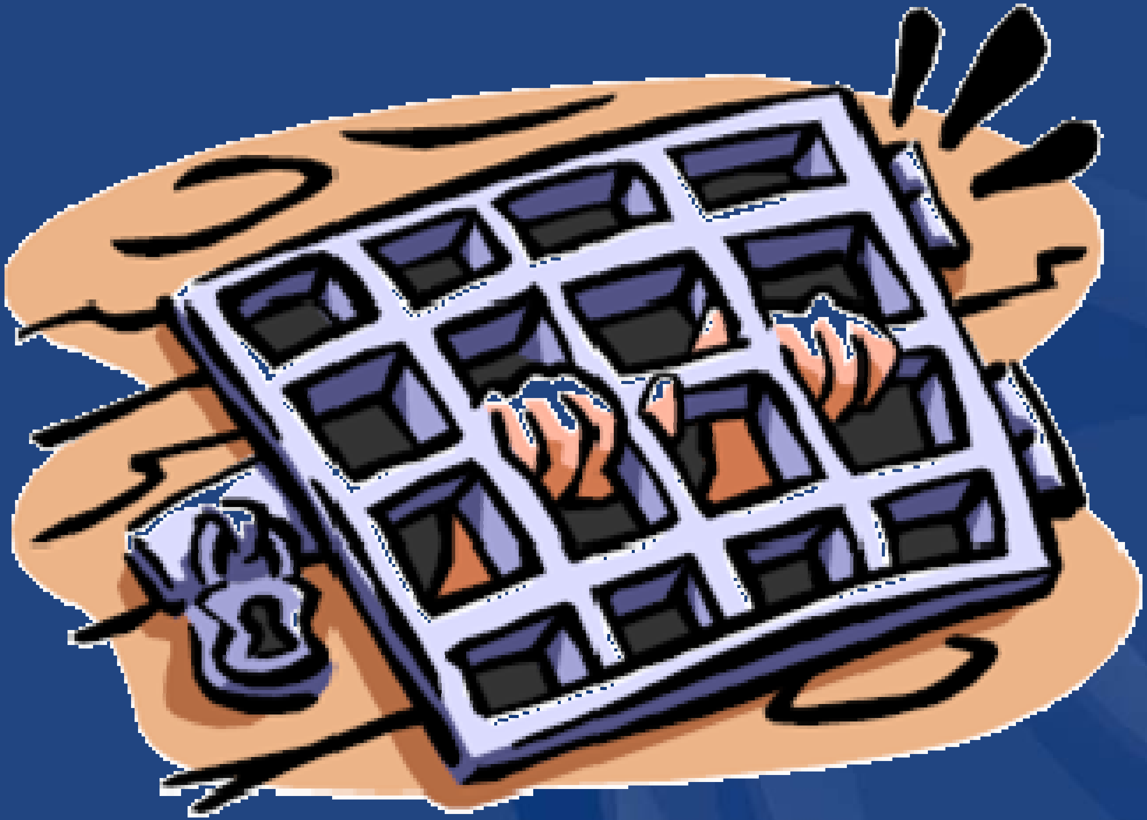
Evidence

- You cannot wait until after the incident to start thinking about evidence
- Three Phases of Evidence collection:
  - Evidence Capture
  - Evidence Analysis
  - Reporting & Testifying
- Chain of evidence must be maintained
  - A break in the chain will ruin the case

End Goal - Deterrence

"Deterrence prevents an adversary from doing something that you don't want him to do by threatening him with unacceptable punishment if he carries out that behavior."

End Goal - Deterrence



Questions?