SANOG 7

Security for SPs

including-
DDOS Prevention
Wireless Security

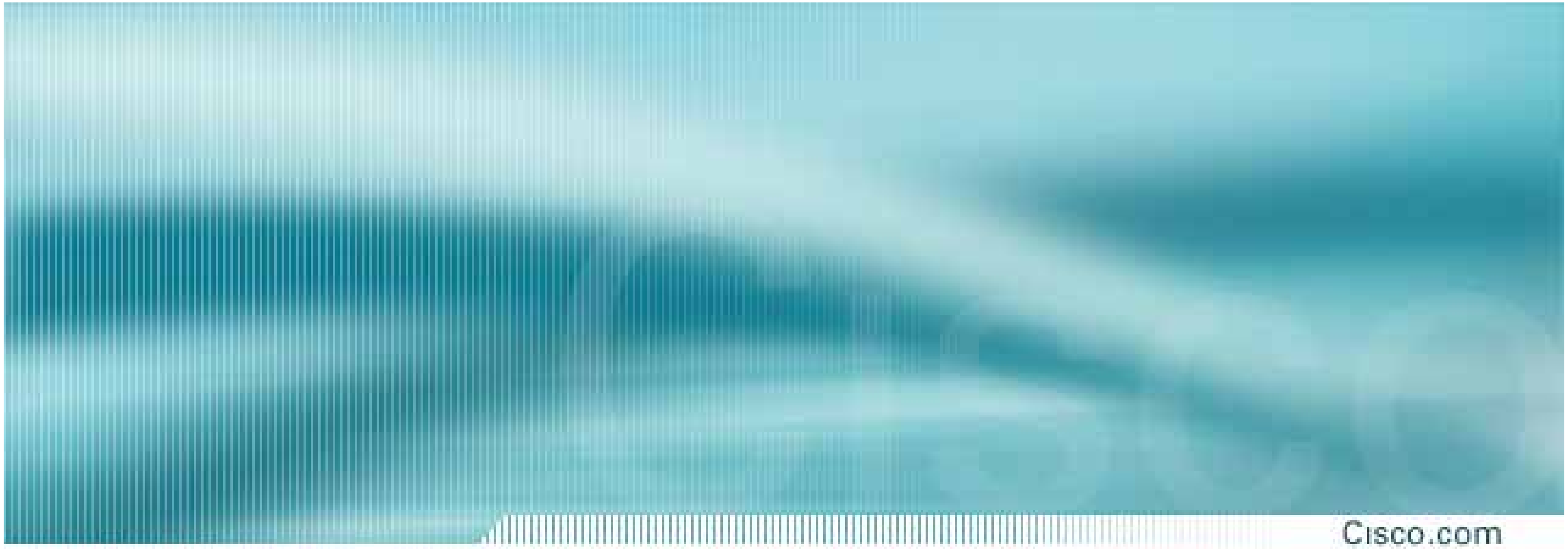
Pravin Mahajan, pmahajan@cisco.com

Mumbai

22 Jan 2006

Agenda

- Challenges
- Trends
- Threats
- The first step - Telemetry
- Next Steps –
  - Techniques
  - Modular Application to SP infrastructure
- Wireless Security
- Case Study



Security Challenges

Introduction: Emerging Threats

I LOST MY I.D. BADGE.
REPORT TO THE SECURITY OFFICE AND GET A NEW ONE.
HOLD IT! WHERE DO YOU THINK YOU'RE GOING?
TO THE SECURITY OFFICE?
NO ONE IS ALLOWED PAST THIS DESK WITHOUT AN I.D. BADGE.
OKAY...HOW DO I GO TO THE SECURITY OFFICE IF I CAN'T GO TO THE SECURITY OFFICE?
GOOD QUESTION. I GUESS YOU'LL HAVE TO SNEAK PAST ME.
LOOK OVER THERE! IT'S AN ANGEL, AND SHE'S GIVING AWAY FREE BACON!
WELL, WELL; IT SEEMS I'VE FOUND A WORTHY ADVERSARY.

E-mail: SCOTTADAMS@AOL.COM

© 2004 Scott Adams, Inc./Dist. by UFS, Inc.

9-1-04

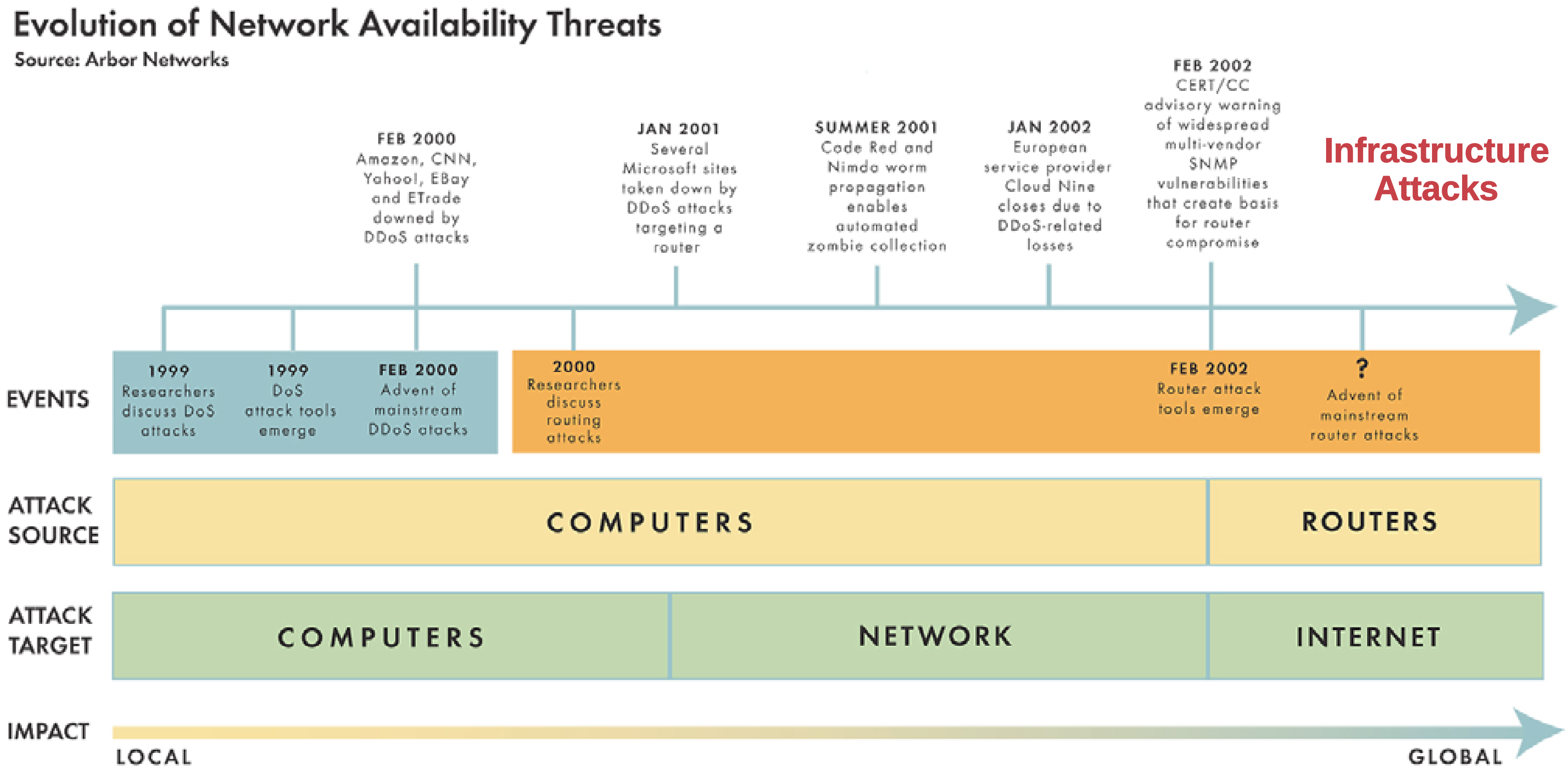
www.dilbert.com

© UFS, Inc.

Today's Reality…

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS
©2000 THE CHARLOTTE OBSERVER

Evolution of Availability Threats



Evolution of Network Availability Threats

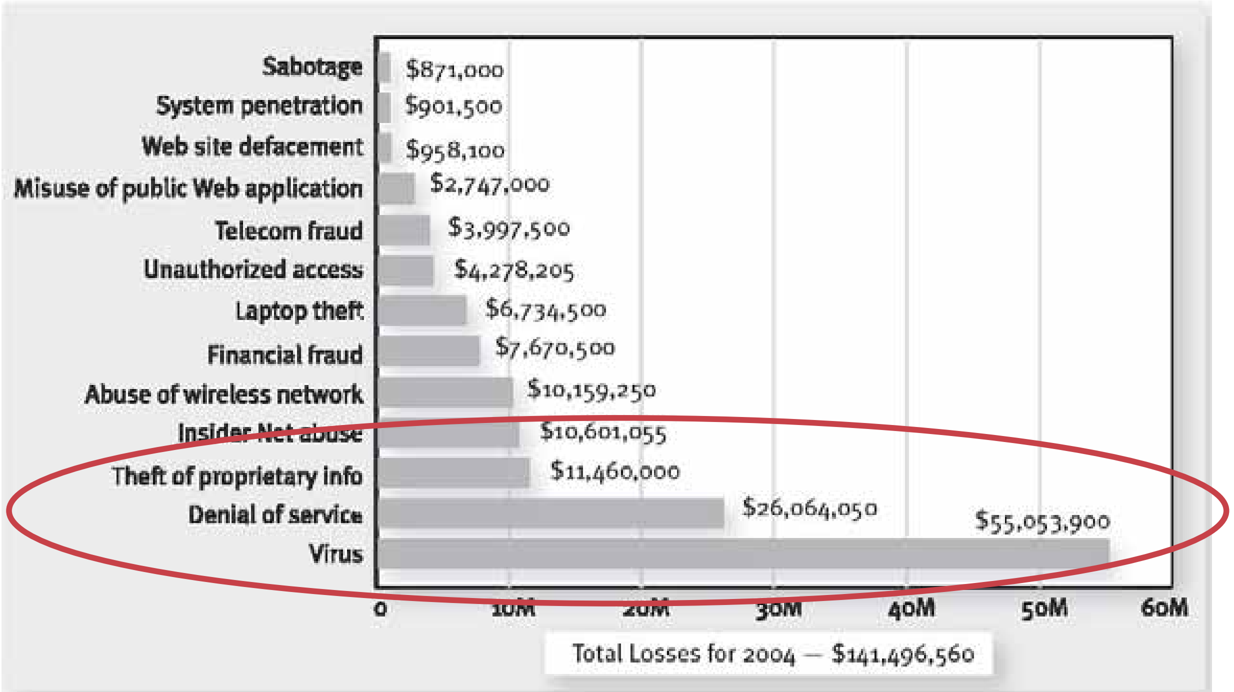
Source: Arbor Networks

Infrastructure Attacks

FEB 2000
Amazon, CNN, Yahoo!, EBay and ETrade downed by DDoS attacks
JAN 2001
Several Microsoft sites taken down by DDoS attacks targeting a router
SUMMER 2001
Code Red and Nimda worm propagation enables automated zombie collection
JAN 2002
European service provider Cloud Nine closes due to DDoS-related losses
FEB 2002
CERT/CC advisory warning of widespread multi-vendor SNMP vulnerabilities that create basis for router compromise
EVENTS
1999
Researchers discuss DoS attacks
1999
DoS attack tools emerge
FEB 2000
Advent of mainstream DDoS atacks
2000
Researchers discuss routing attacks
FEB 2002
Router attack tools emerge
?
Advent of mainstream router attacks
ATTACK SOURCE
COMPUTERS
ROUTERS
ATTACK TARGET
COMPUTERS
NETWORK
INTERNET
IMPACT
LOCAL
GLOBAL

Economic Impact of DDoS

Dollar Amount of Losses by Type:



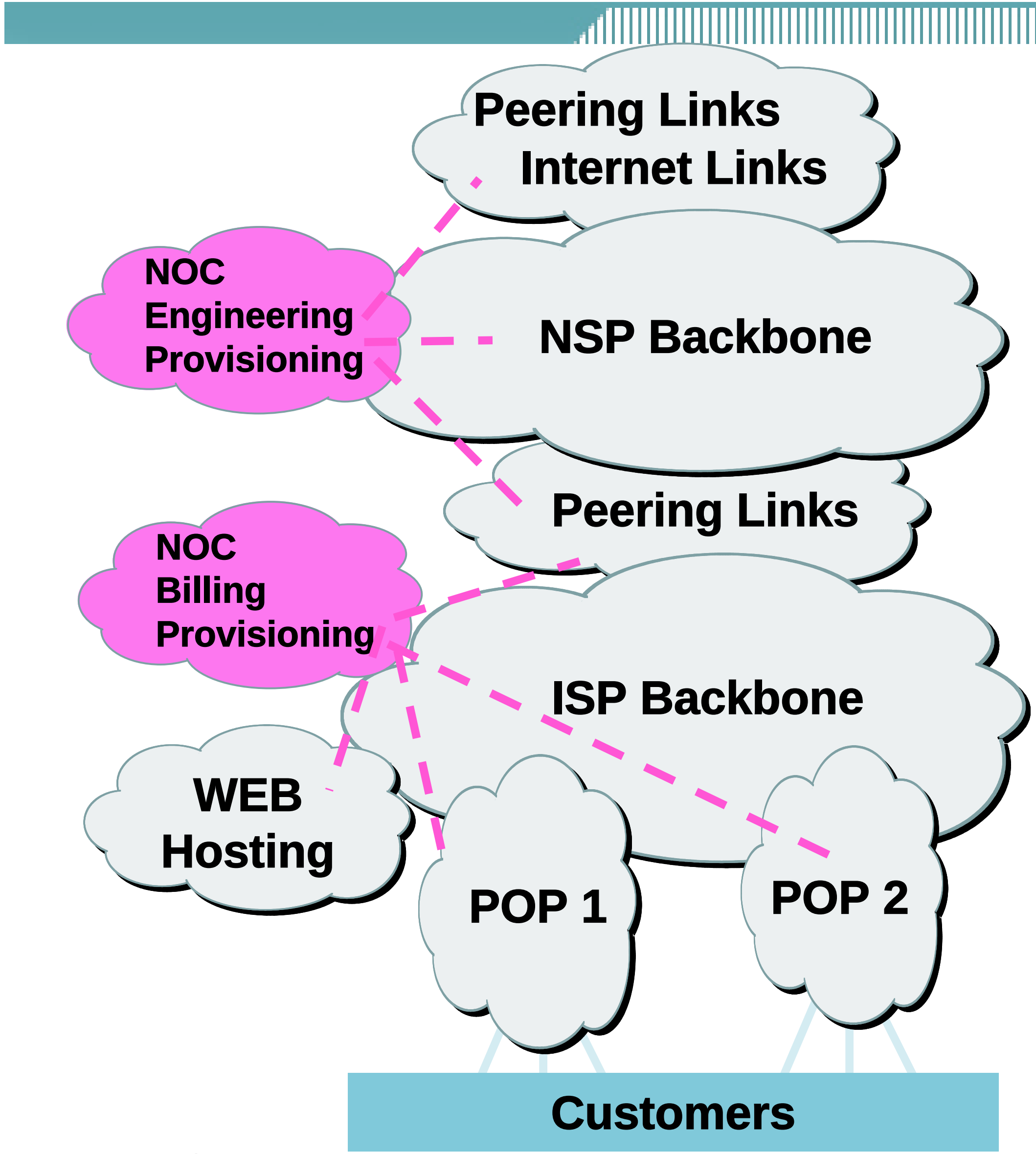
CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

DoS Is 2nd in Impact After Viruses!

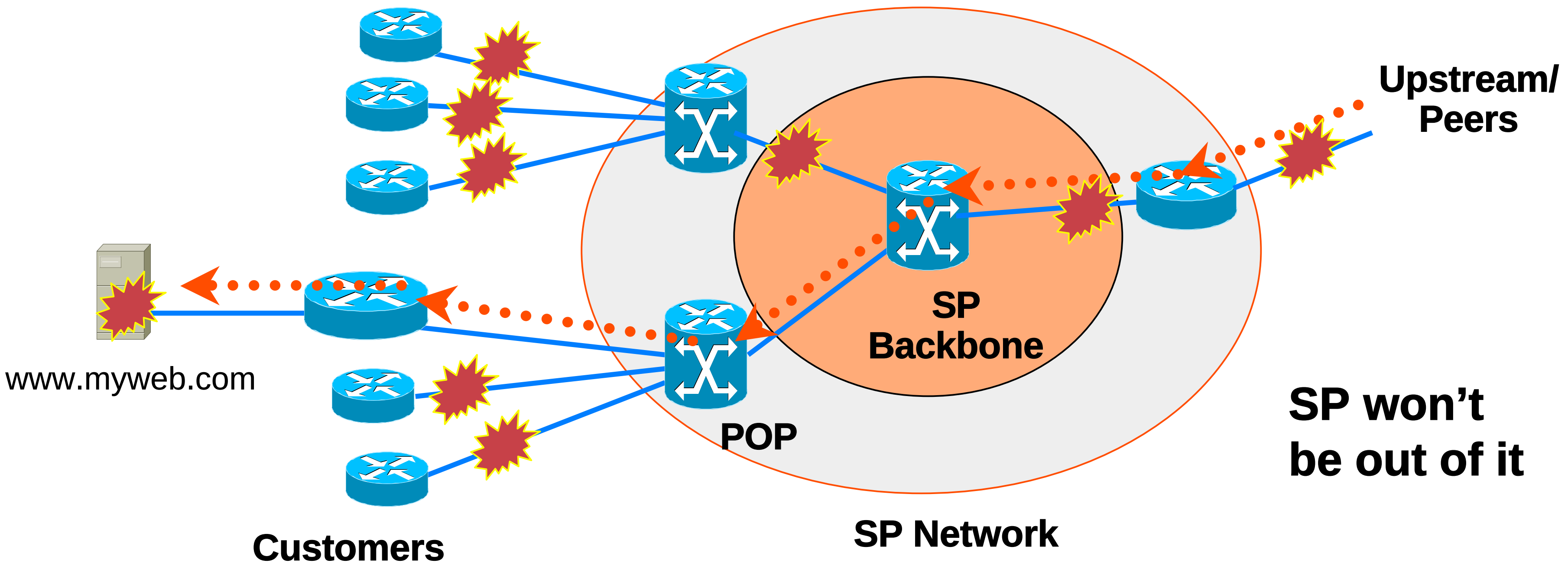
Source: CSI/FBI 2004 Computer Crime and Security Survey

The Internet today



- The new Internet Economy brought new services and new players: NSPs, ASPs, etc…
- E-commerce has become part of the business model. Customers now depend on the Internet
- Attacks targeted to customers can and do affect the infrastructure.
- Availability is not just matter of duplicating gear.

Collateral Damage



SP won't be out of it

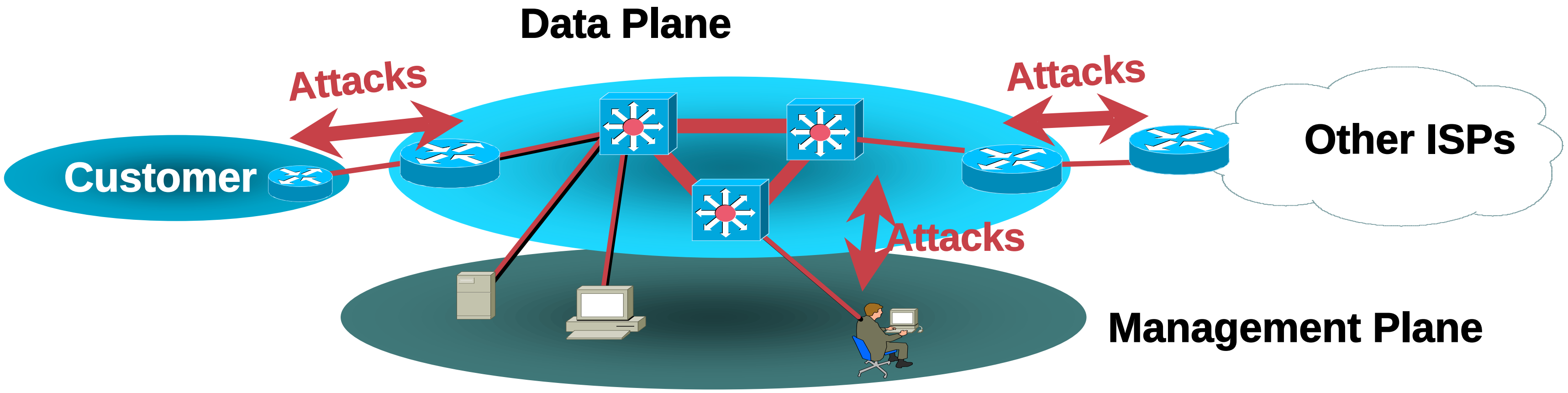
Attacks targeted to a particular customer CAN and DO affect the infrastructure

Infrastructure Attacks
a wake up call

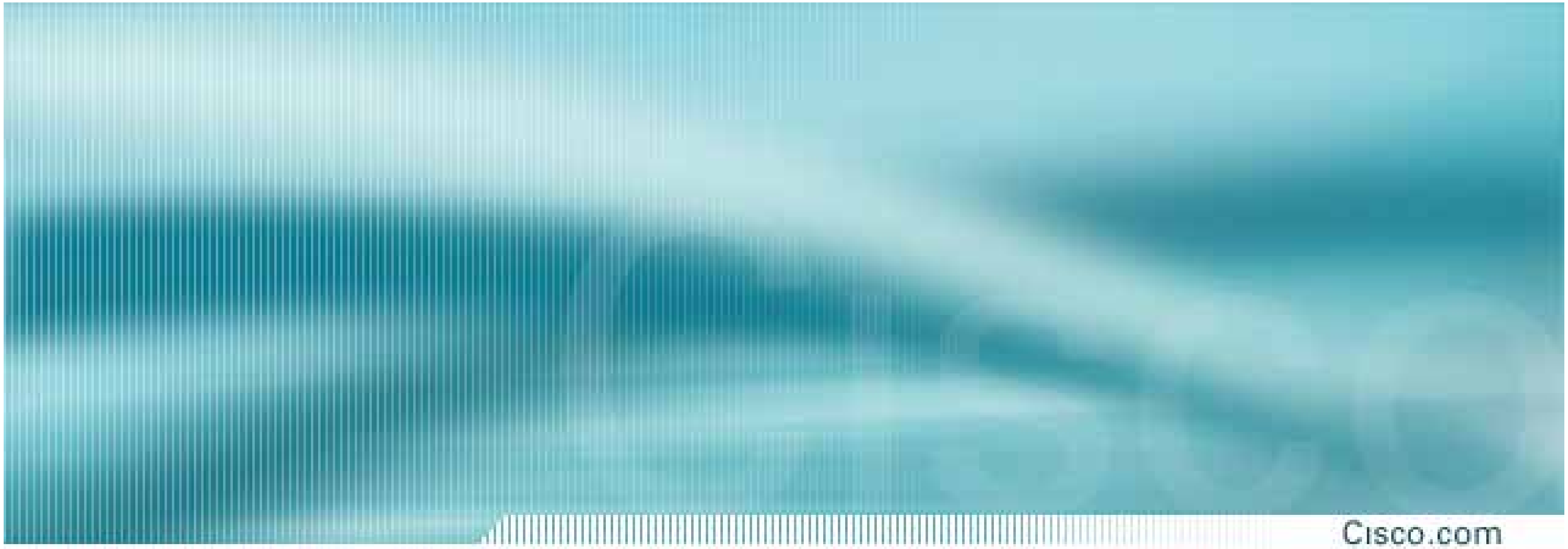
Now elements of the SP infrastructure are being directly targeted too:

- **Services: DNS, DHCP, SMTP, WWW, FTP**
- **Routers**
- **Routing**
- **…**

Role of Service Providers

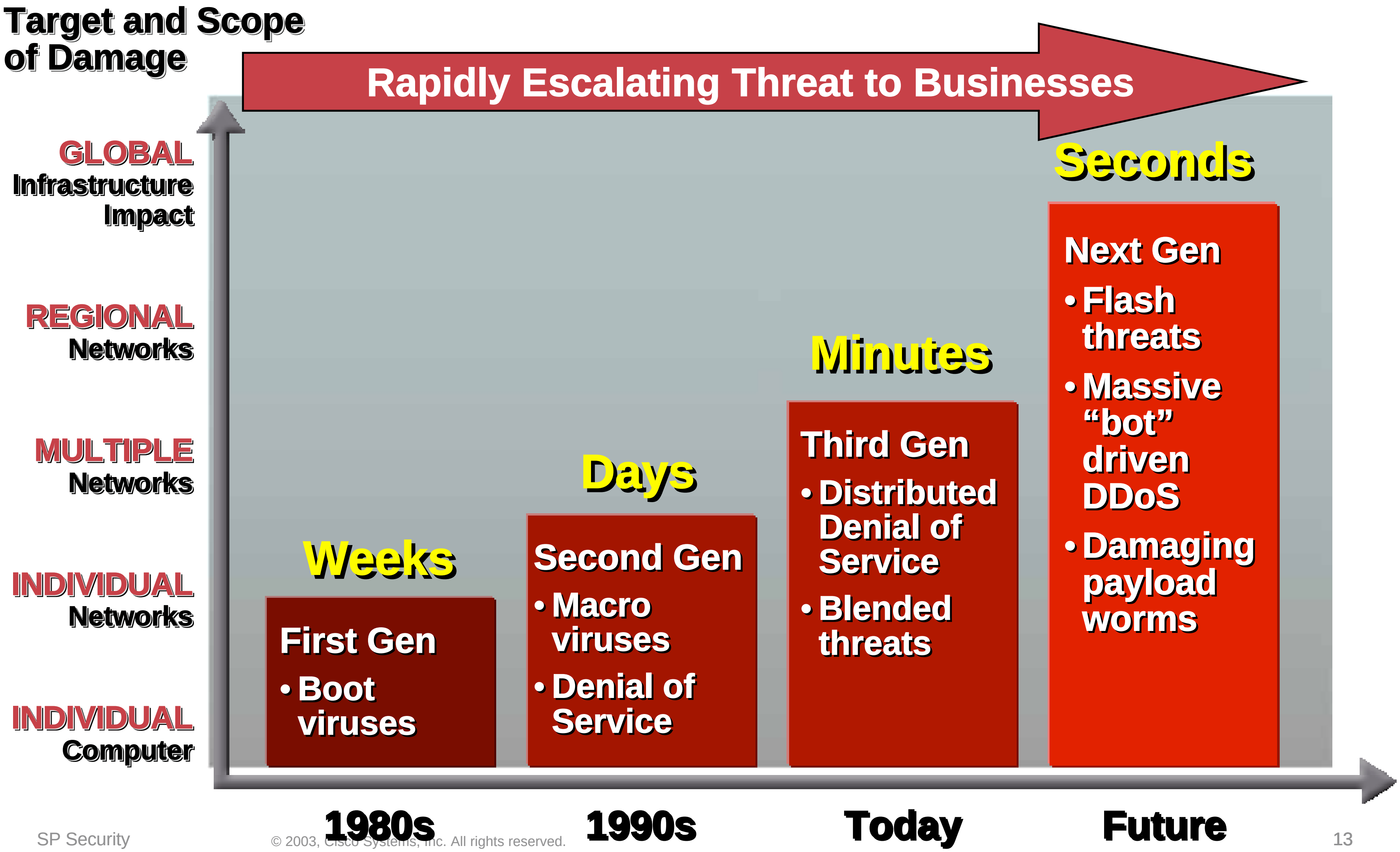


- Protect their own infrastructure (from Customers and Internet)
- Help protect other peers
- Protect customers from attacks coming from the infrastructure or other customers



Security Trends

Evolution of Security Challenges



First Gen
- Boot viruses

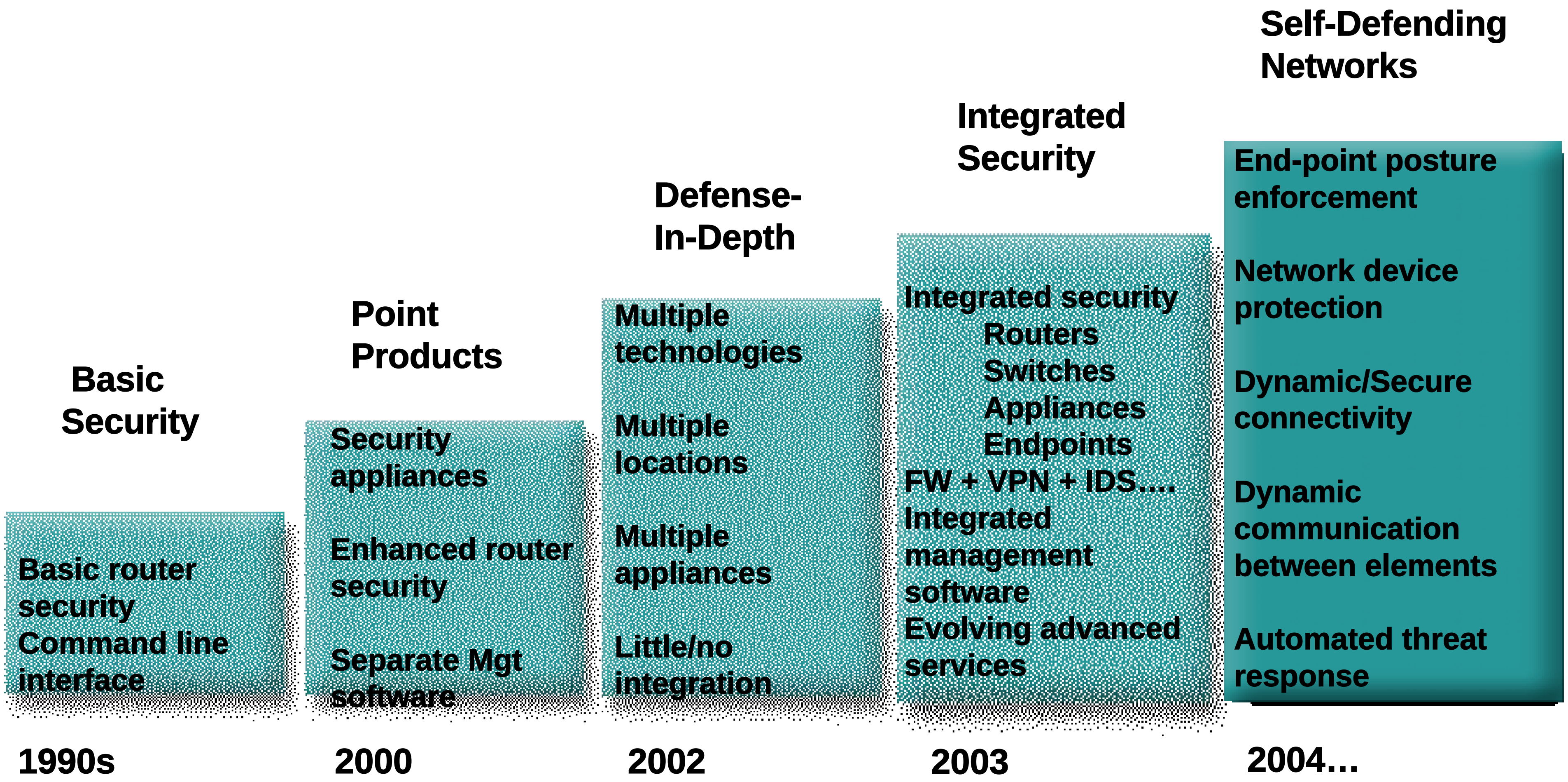
Second Gen
- Macro viruses
- Denial of Service

Third Gen
- Distributed Denial of Service
- Blended threats

Next Gen
- Flash threats
- Massive “bot” driven DDoS
- Damaging payload worms

Evolution of Security Strategies

Cisco.com



Basic Security

Basic router security
Command line interface

1990s

Point Products

Security appliances

Enhanced router security

Separate Mgt software

2000

Defense-In-Depth

Multiple technologies

Multiple locations

Multiple appliances

Little/no integration

2002

Integrated Security

Integrated security
- Routers
- Switches
- Appliances
- Endpoints

FW + VPN + IDS….
Integrated management software
Evolving advanced services

2003

Self-Defending Networks

End-point posture enforcement

Network device protection

Dynamic/Secure connectivity

Dynamic communication between elements

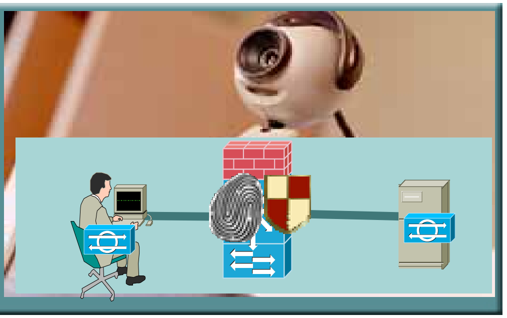
Automated threat response

2004…

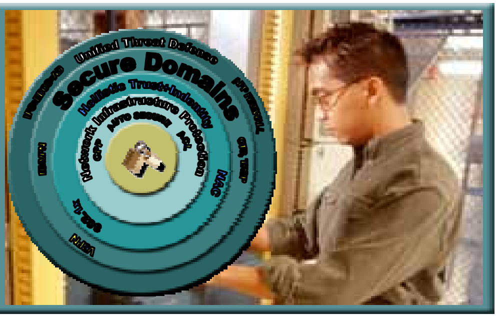
Self-Defending Network

1. Point Products → Integrated Security

2. Disparate Security Services → Collaborative Security Systems



3. Reactive Security → Adaptive Security

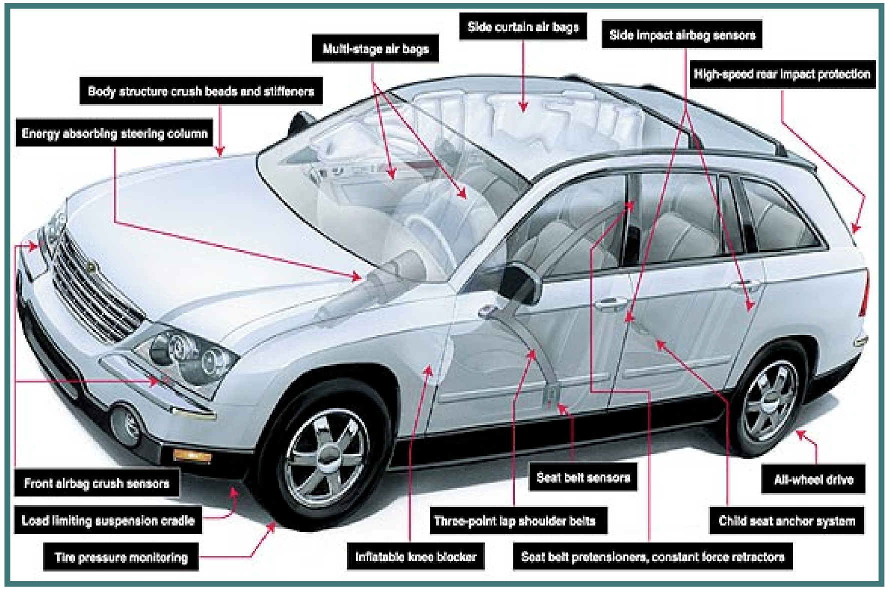


Self-Defending Network:
Controlling the Who, What, Where, When, Why and How

- **Who—allows access to data only by authorized personnel**
- **What—prevents data from ever being stored, copied, or printed outside the secure environment**
- **Where—provides layers of protection and auditing to ensure that data is only stored in a controlled location**
- **When—users process data normally, but the data never “sleeps” outside of the secure area**
- **Why—only authorized personnel allowed to process data**
- **How—data access is restricted, authenticated, and audited by the Self-Defending Network**

Self Defending Networks

From Point Products to Holistic System

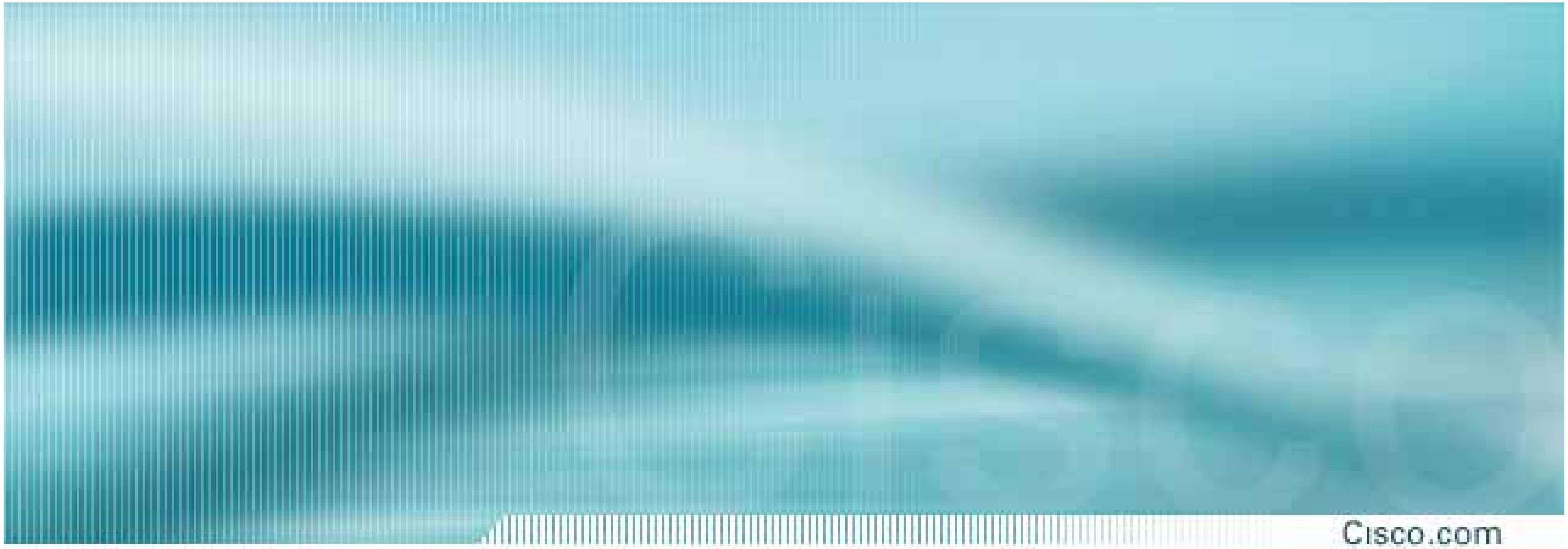

Side curtain air bags
Multi-stage air bags
Side impact airbag sensors
High-speed rear impact protection
Body structure crush beads and stiffeners
Energy absorbing steering column
Front airbag crush sensors
Load limiting suspension cradle
Tire pressure monitoring
Inflatable knee blocker
Three-point lap shoulder belts
Seat belt sensors
Seat belt pretensioners, constant force retractors
All-wheel drive
Child seat anchor system

Security as an Option

- Very complex environment
- Higher integration cost
- Security risks not mitigated
- Lower reliability

Security, INTEGRAL to the System

- Reduced complexity
- Easier deployment and management
- Security risks effectively mitigated
- Lower TCO



Threats

Introduction: The Basic Model

Types of Communication:

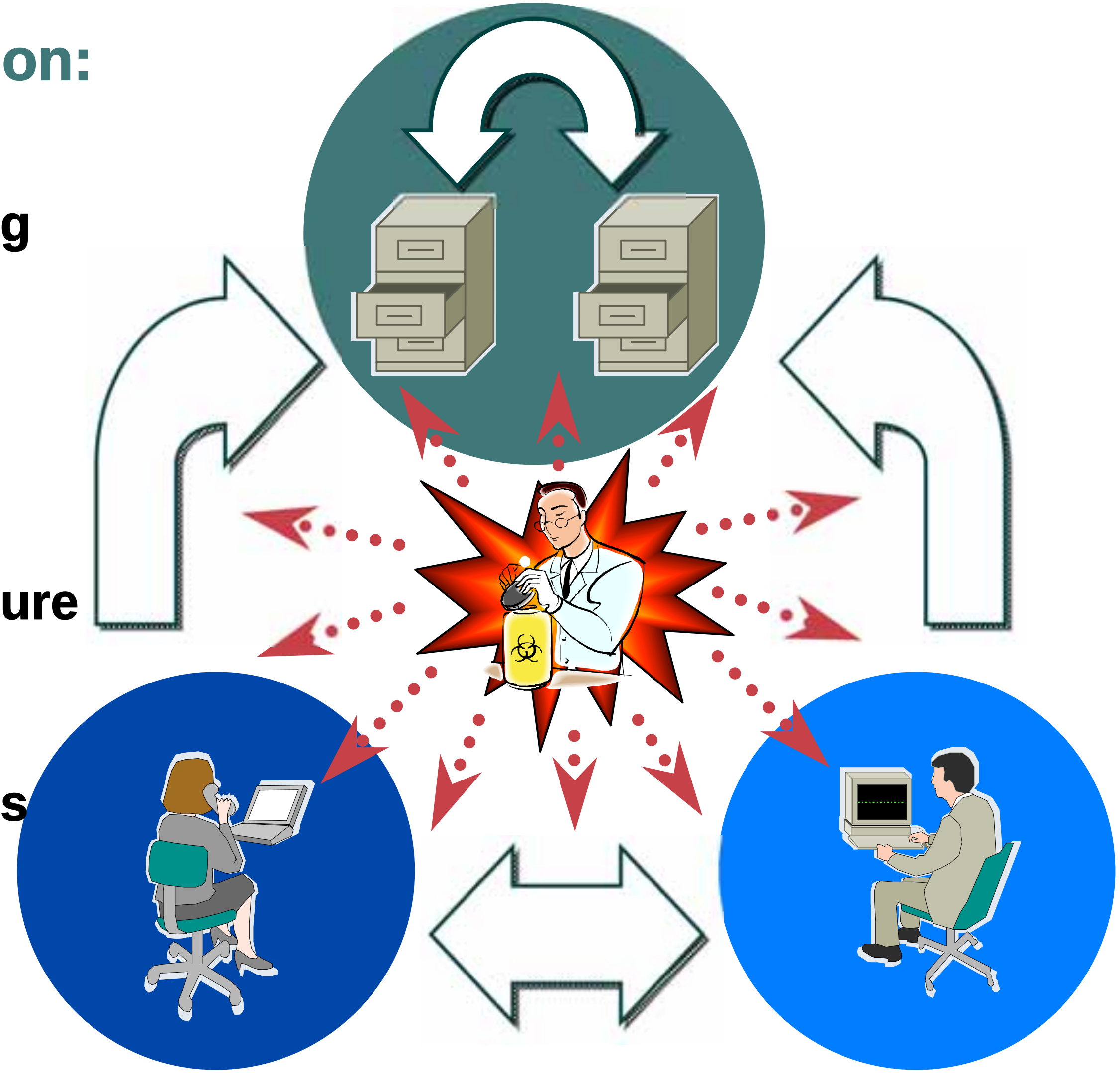
1) People Accessing Information Assets
2) People Communicating with One and Other
3) Machine to Machine Communication

Policy Primitives:

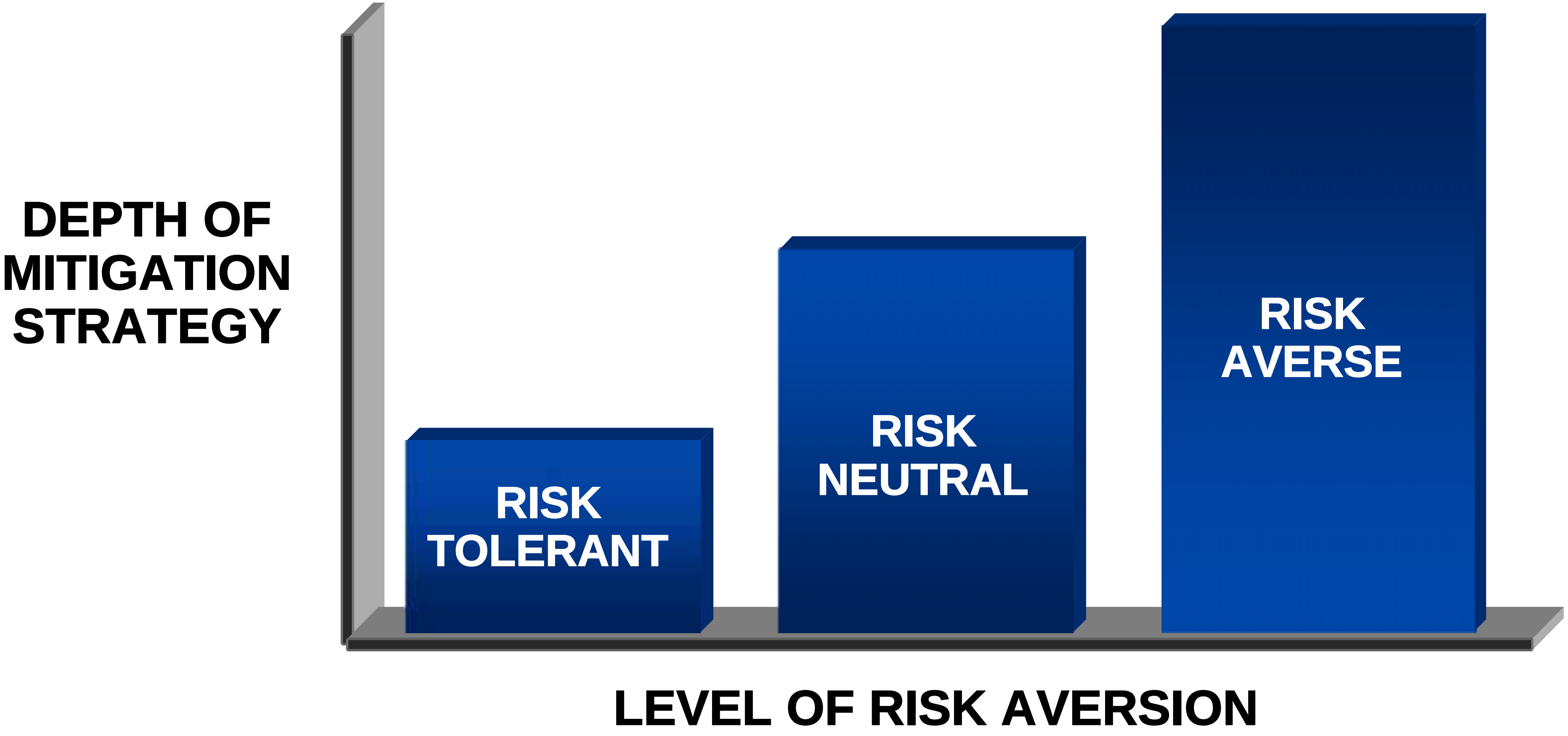
1) User / Service Identity
2) Machine Security Posture

Attack Targets:

1) End-points Themselves
2) Traffic Leaving
3) Traffic in Flight
4) Traffic Entering



Introduction: Appropriate Risk Mitigation



Conclusion: Determine in advance the level of risk appropriate to the business

Worms and Viruses

- **Virus:** Malicious piece of software that typically propagates by attaching itself to some other form of communication. May exploit a vulnerability, but always **requires human intervention** to spread.

- **Worm:** Malicious piece of software that self-propagates. Always exploits a vulnerability to infect, and **does not require human intervention** to spread

OUR COMPANY IS GOING TO MAKE ANTIVIRUS SOFTWARE. WHAT'S THAT TELL YOU?
scottadams@aol.com
www.dilbert.com
IT TELLS ME WE'LL SECRETLY CREATE VIRUSES THAT CAN BE DETECTED ONLY BY OUR SOFTWARE.
11-29-03 © 2003 United Feature Syndicate, Inc.
AM I CLOSE?
YOU'RE SPOOKY.

© UFS, Inc.

Worms and Viruses: What Happens

Injection

- Injection code arrives at end point
- Can either self-execute by having another process execute it, or can have a user execute it
- Some are completely self-contained, some need to pull down additional propagation and payload code to operate

Propagation

- Code replicates itself, and begins to propagate to other hosts
- Propagation can be multi-vector (Nimda)
- Mass propagation are typically why the casual user learns of these
- Can cause network-level Denial of Service (Blaster) due to massive consumption of resources

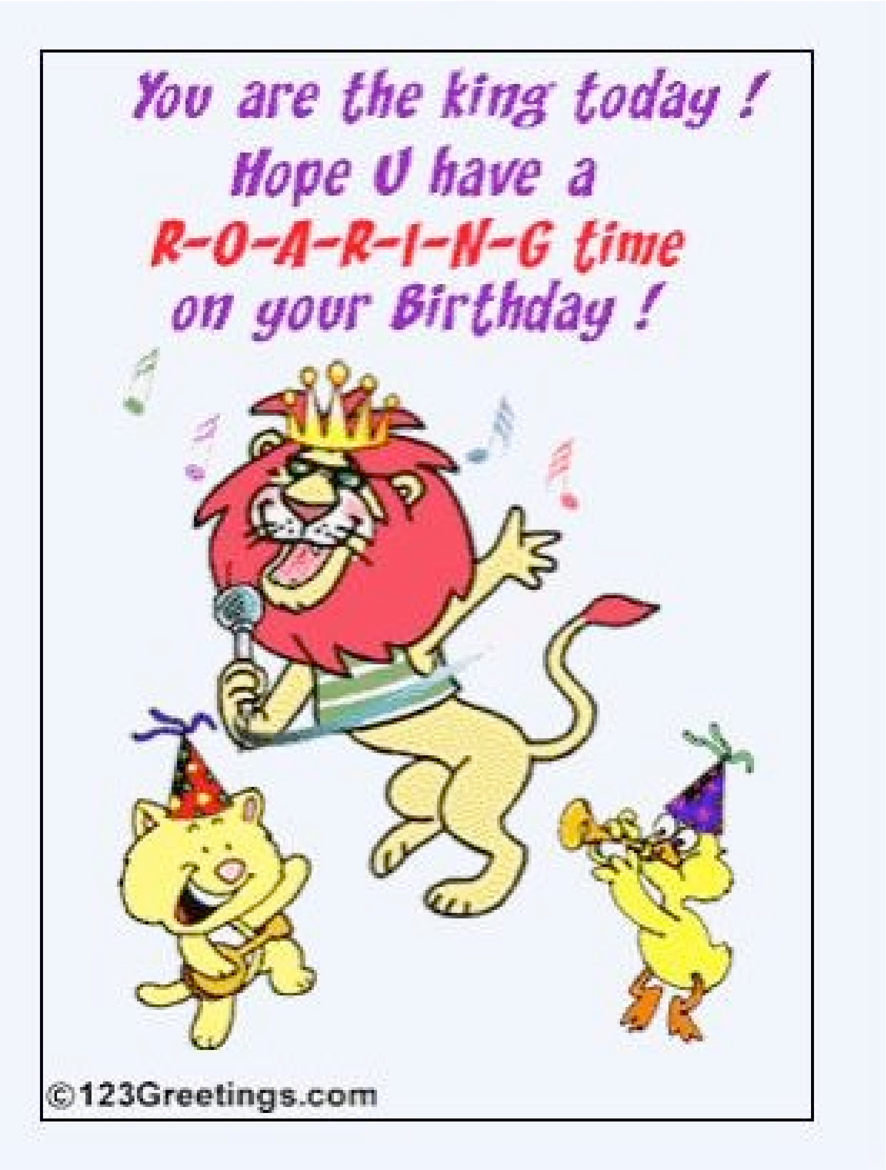
Payload

- Potential for most damaging portion of infection
- Historically, often not malicious (e.g. Slammer)
- Sometimes triggers a reboot (Nachi), often to further embed itself in the system
- Increasingly, used to install backdoors or trojans, and to patch the injection vector

Recent Trends in Worms and Viruses

- Change in ***Purpose***
  - **Shift from fame to profit**
  - **Shift from being noisy to developing an asset with economic value**
- Change in ***Expected Behavior***
  - **Less Noisy**
  - **More Sophisticated**
  - **More Variants, smaller scope of each**

A Birthday Message for You!!!



Anatomy of a Trojan

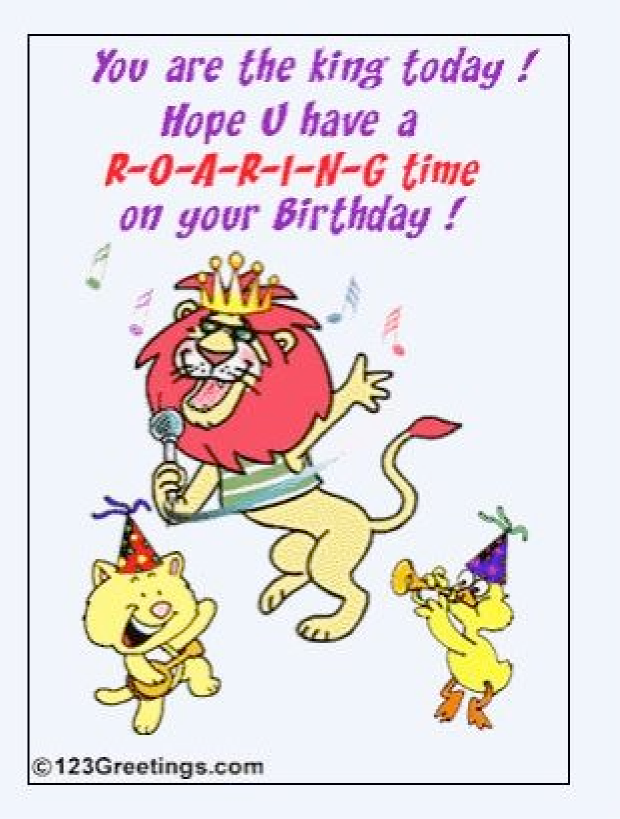
- Troj/LdPinch-BD is a password-stealing Trojan for Windows platforms
- Troj/LdPinch-BD steals information, including passwords, from various applications. Information stolen may include:

  computer details (OS version, memory, CPU etc.)
  available drives (drive letter, type and free space)
  hostname and IP address
  Windows folder volume information
  Passwords and confidential information from 'Protected Storage‘
  POP3 and IMAP server information, usernames and passwords
  FTP usernames and passwords
  RAS dial-up settings

- The Trojan may steal information relating to applications including the following:

  Mirabilis ICQ
  Opera
  CuteFTP
  WS_FTP
  Windows Commander
  Total Commander

- The Trojan attempts to download and run further malicious code.



Source: http://sophos.com/virusinfo/analyses/trojldpinchbd.html

Harvesting and Asset Development

MACHINE HARVESTING

- Creation of “bot-net” networks of thousands of compromised machines
- Used as:

  Launch points for other attacks

  Spam-nets (sold or rented to spammers)

  DDoS For Hire networks (sold or rented to attackers)

INFORMATION HARVESTING

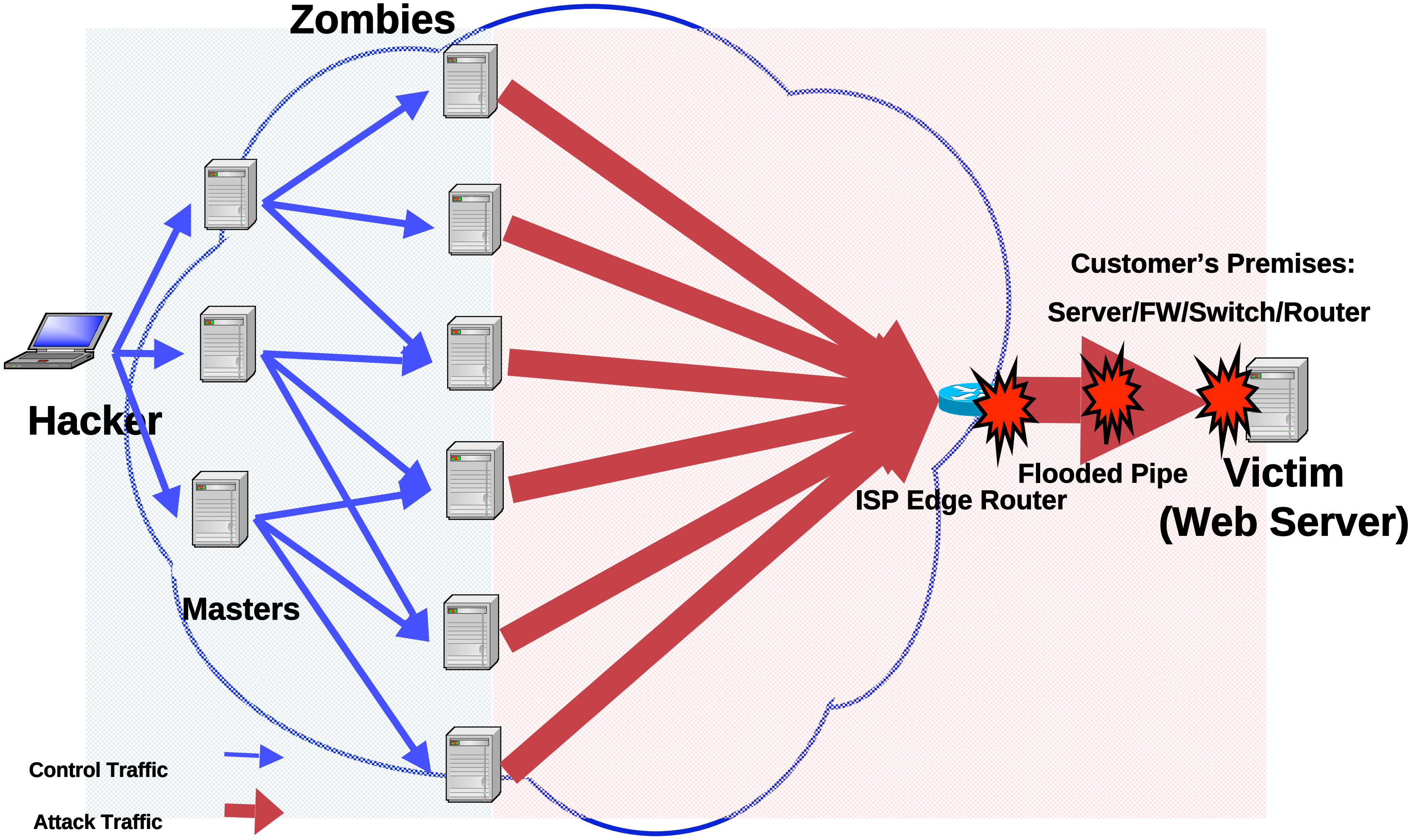
- Harvesting identity information (account names, numbers, passwords, personal information, etc)
- Used for:

  Direct sale on the open market

  Compromise other networks

  Trust-enablement for fraud (traditional cons and new cons such as phishing)

BotNet Operation



A New Class of Threat: Spyware

SPYWARE: malware that obtains or transmits personal information with intent to defraud*

ADWARE: Spyware's slightly more reputable cousin

- **Recently, Spyware has exploded as a significant security threat**
- **Can be thought of as a "drive up" virus – skip the propagation step and cut out the middle-man!**
- **Enhanced Concern: Threat to control of Confidential Information**

* From most recent draft of US Federal I-SPY act

How Spyware/Adware Gets Installed

- **Bundled in freeware/shareware**
- **Social Engineering**

  Pestering pop-ups until user clicks "yes"

  Confusing or buried EULA terms

  User doesn't read EULA

- **Drive-by Download**
- **Remote installation – no physical access necessary**
- **Via Virus or Trojan**

Denial of Service: A Refresher

- Denial of Service (DoS) attacks’ goal is to make service unavailable
- The method may target:

  A server

  A network device

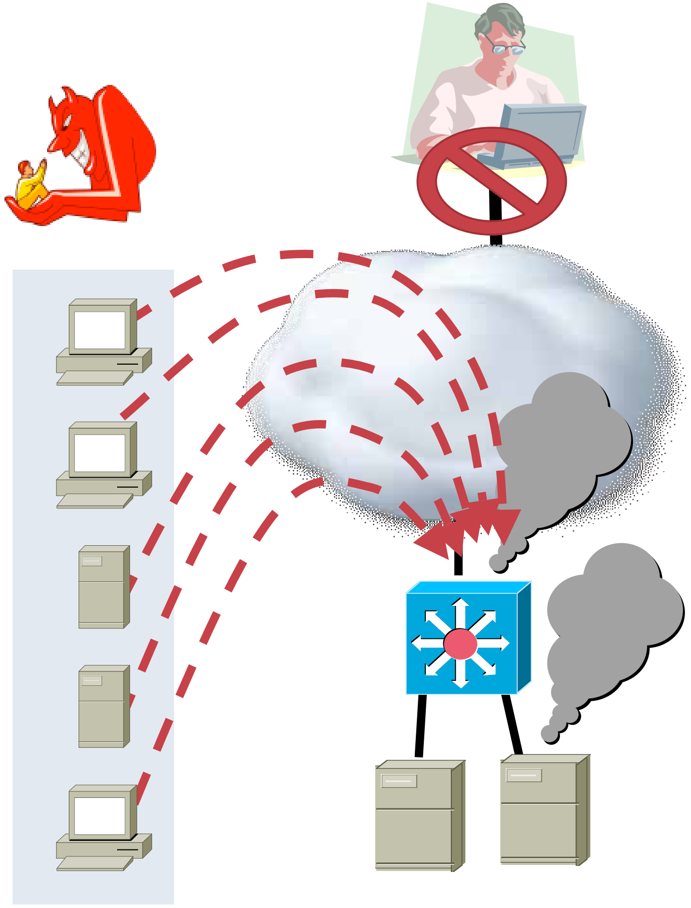
  A network
- Can be associated with:

  Source IP spoofing
- Collateral Damage includes:

  Saturation of network forwarding tables

  Exhausting processing power

  Clogging links



Denial Of Service: What's Going On

- **Basic Denial of Service**
  - Often L3/L4 based; SYN attacks common; spoofing common
  - Relatively easy to block sources and stop
- **Distributed Denial of Service**
  - Similar to a basic DoS in approach, but sources appear "random"
  - Tens of thousands of broad-band connected machines in a bot-net make it extremely difficult to track
  - Often stopped by closing down control channels
- **Emerging Threats: Application-layer Denial of Service**
  - Email DoS
  - Web Front-end DoS
  - Web-Services and XML DoS
  - IP Telephony DoS

DDoS For Hire, and DoS Extortion

- **DDoS For Hire:** **Criminal service in which for a nominal fee, a site of your choosing can be taken offline**
- **DoS Extortion:** **Criminal enterprise in which web-sites must pay a protection fee to avoid being taken offline, typically during a critical business period**

US credit card firm fights DDoS attack

The Register

US credit card processing firm Authorize.Net is fighting a sustained distributed denial of service (DDoS) attack that has left it struggling to stay online.

Glen Zimmerman, a spokesman for Authorize.Net's parent company, Lightbridge, told the Boston Globe that the attacks followed an extortion letter. Lightbridge said it was working with law enforcements officials to track down the attackers.

http://www.theregister.co.uk/2004/09/23/authorize_ddos_attack/

ONLINE EXTORTION

CSO

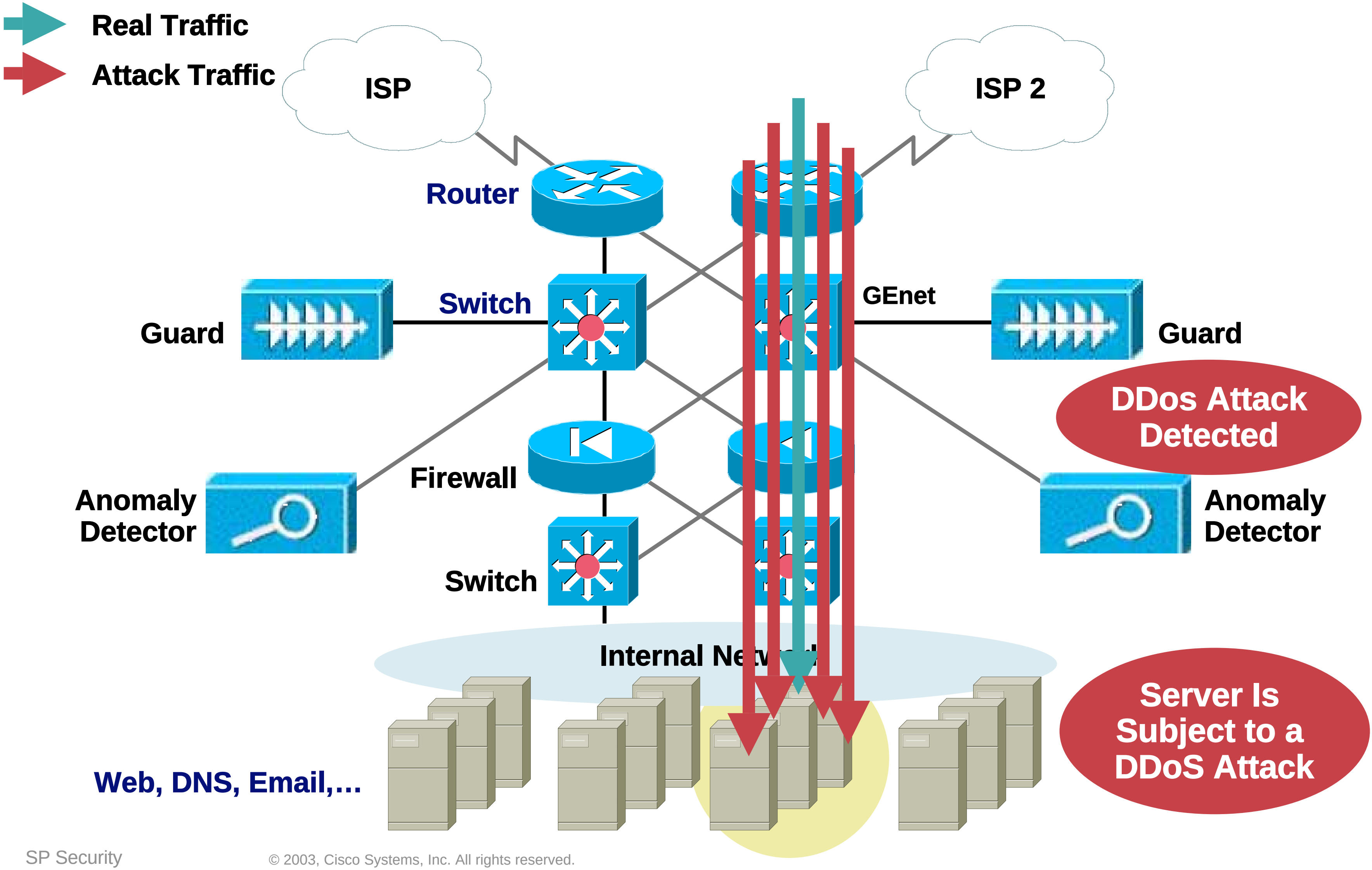
csoonline.com

How a Bookmaker and a Whiz Kid Took On an Extortionist — and Won

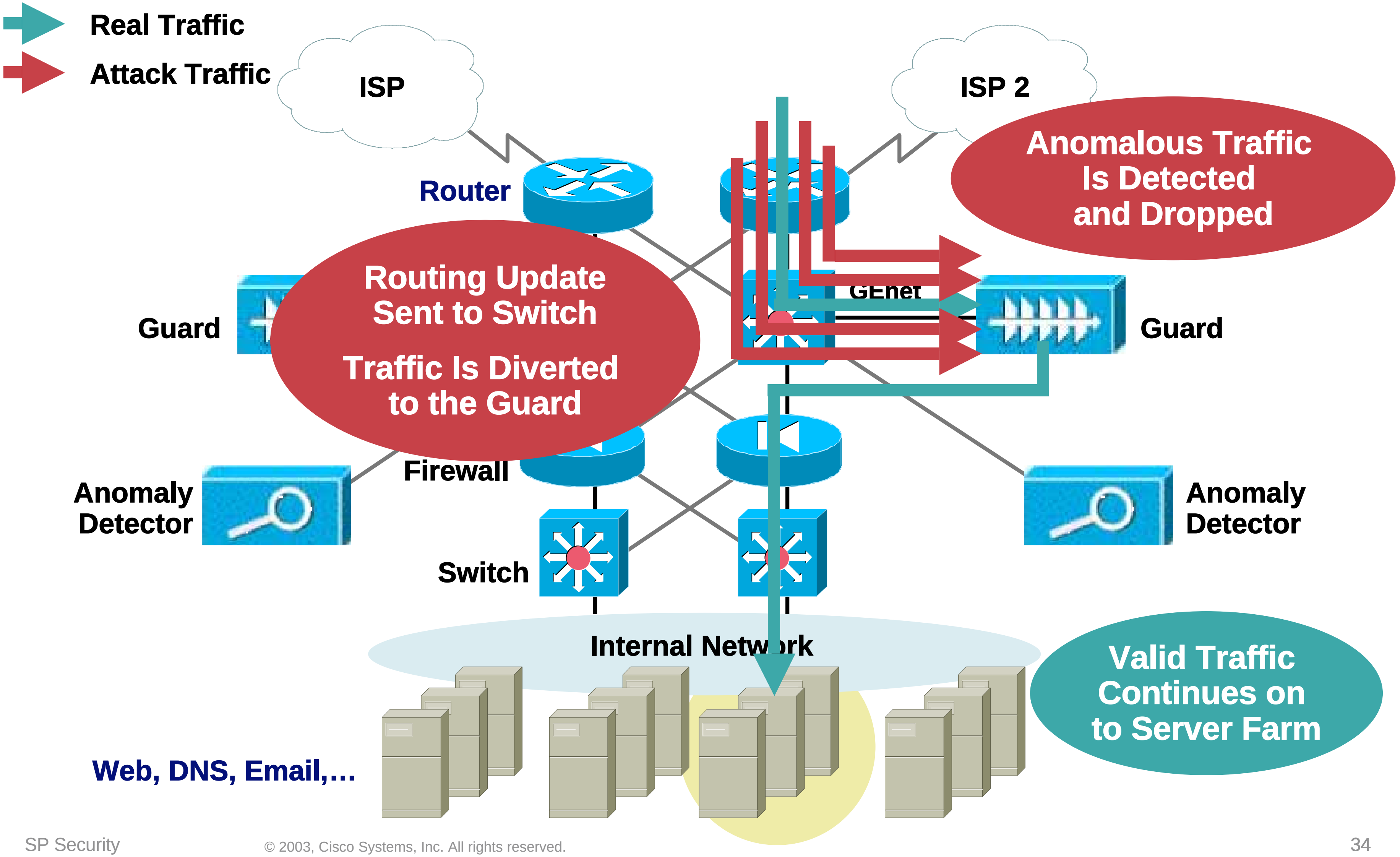
Facing an online extortion threat, Mickey Richardson bet his Web-based business on a networking whiz from Sacramento who first beat back the bad guys, then helped the cops nab them. If you collect revenue online, you'd better read this.

http://www.csoonline.com/read/050105/extortion.html

Solutions: Basic DoS and DDoS



Solutions: Basic DoS and DDoS



Routing Update Sent to Switch

Traffic Is Diverted to the Guard

Anomalous Traffic Is Detected and Dropped

Valid Traffic Continues on to Server Farm

Further Solutions: Denial of Service

- Denial of Service likely to continue to be a problem for a number of years

    Economic incentives drive behavior

- Application Denial of Service a key piece of an Application Security strategy

    Look for solutions with real DoS protective capabilities

- Partnerships are a Must

    Enterprises must work with their Providers to set up response plans

- Incident Response a Must

    Have a plan before your attacked. DoS attacks are very visible, very quickly. Timeliness of response is key

Messaging Security

- SPAM / SPIM / SPIT
  - Nuisance / Productivity Drain / DoS or Cost Imposition
  - Vector for other Frauds
- Phishing / Pharming
- Solutions:
  - IIM (Identified Internet Mail) spec
  - 2-factor auth for financials
  - Uniform policy control: Message Hygiene solutions; Endpoint Posture Compliance

SPAMity Calamity

WE HAVE A GIGANTIC DATABASE FULL OF CUSTOMER BEHAVIOR INFORMATION.
EXCELLENT. WE CAN USE NON-LINEAR MATH AND DATA MINING TECHNOLOGY TO OPTIMIZE OUR RETAIL CHANNELS!
IF THAT'S THE SAME THING AS SPAM, WE'RE HAVING A GOOD MEETING HERE.
www.dilbert.com
scottadams@aol.com
© 2000 United Feature Syndicate, Inc.
11/3/00

SPAMity Calamity

- **Evolution of SPAM:**

  Nuisance

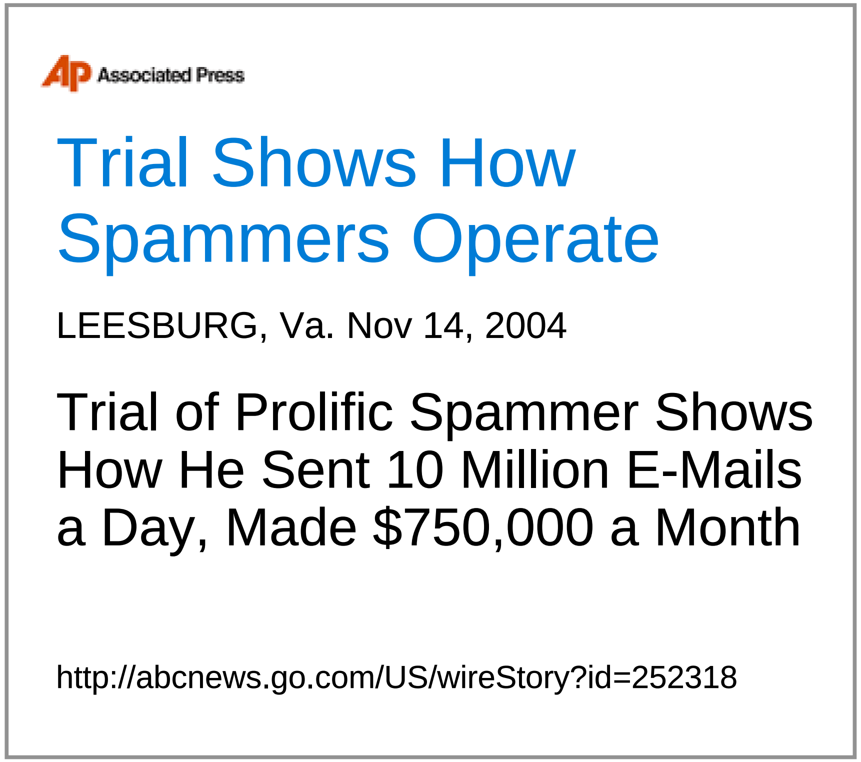
  Productivity Drain

  Offensive Content

  Vector for Fraud

- **Dominant Source Today: Bot-nets**

- **SPAM is very much an unsolved problem**



AP Associated Press

Trial Shows How Spammers Operate

LEESBURG, Va. Nov 14, 2004

Trial of Prolific Spammer Shows How He Sent 10 Million E-Mails a Day, Made $750,000 a Month

http://abcnews.go.com/US/wireStory?id=252318

The Changing Nature of Spam

- **SPAM explosion:**
  "Old Dog, New Tricks"

  SPIM—Spam over Instant Messaging

  SPIT—Spam over IP Telephony

- **Rise of Crime:**

  Fraud as a rising threat

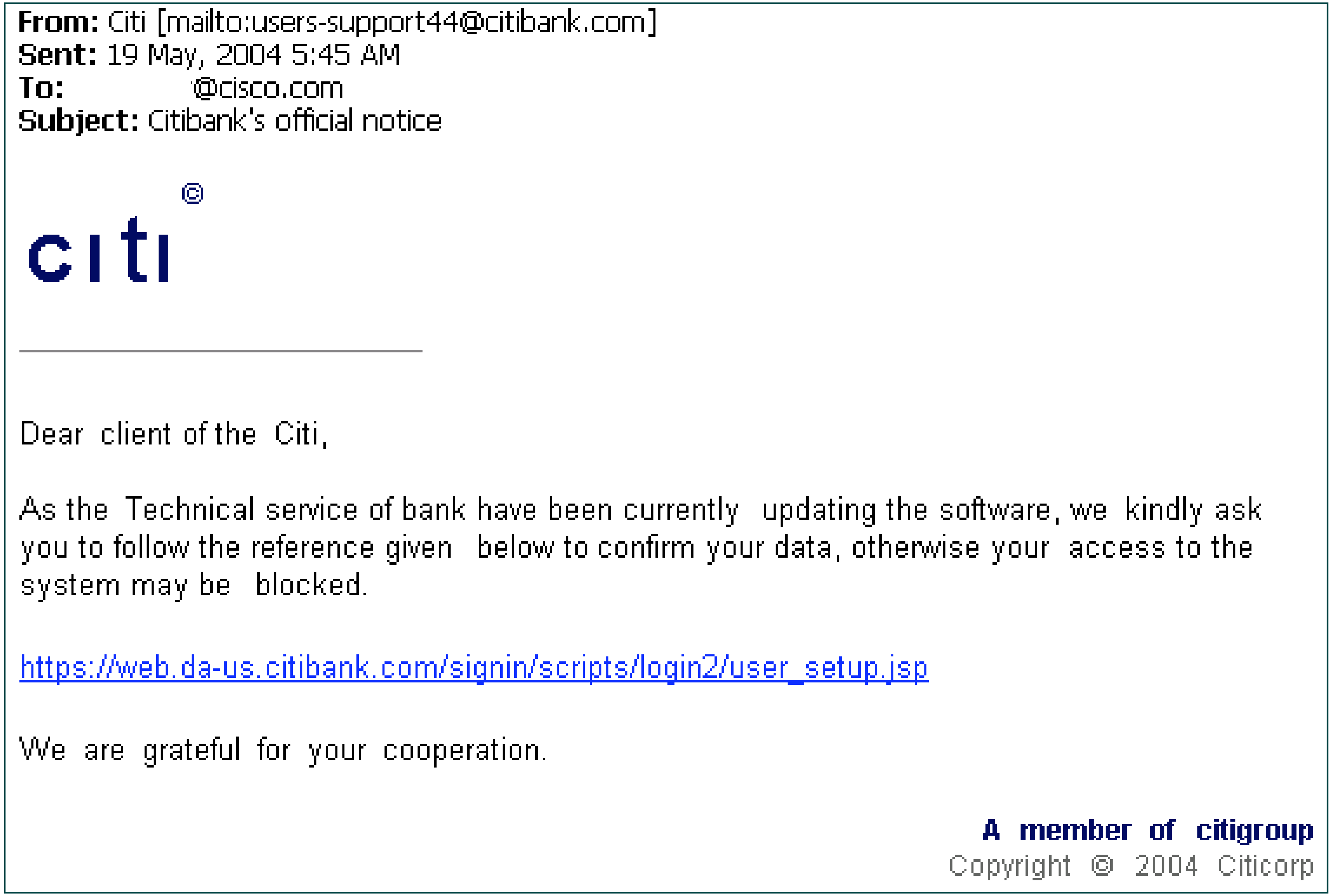
  Phishing

- **Criminalization of Spam:**

  CAN-SPAM act in US

Introduction to Phishing

Phishing Basics



From: Citi [mailto:users-support44@citibank.com]
Sent: 19 May, 2004 5:45 AM
To: @cisco.com
Subject: Citibank's official notice

citi©

Dear client of the Citi,

As the Technical service of bank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

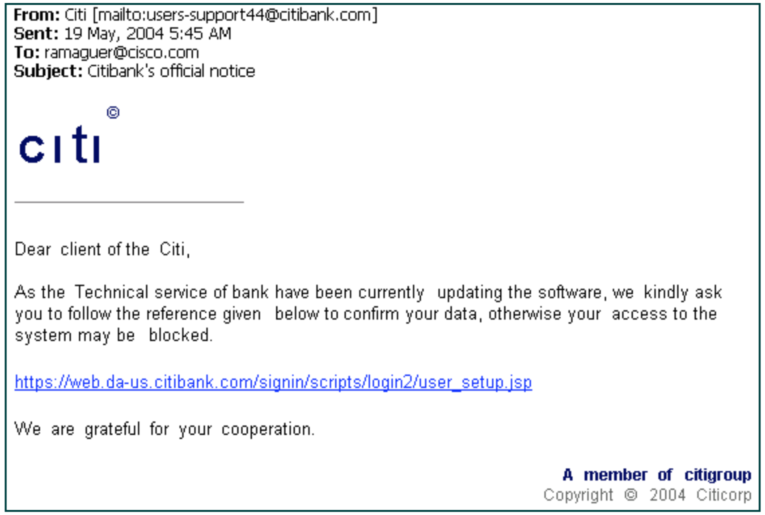
We are grateful for your cooperation.

A member of citigroup
Copyright © 2004 Citicorp

Introduction to Phishing
Phishing Basics

PHISHING:

Email Schemes, Called “Phishing” or “Carding”, Are an Attempt to Trick Consumers into Disclosing Personal and/or Financial Information; the Emails Appear to Come from Companies with Whom Consumers May Regularly Conduct Business; Often Times the Email Threatens Termination of Accounts Unless Consumers Update Billing Information



From: Citi [mailto:users-support44@citibank.com]
Sent: 19 May, 2004 5:45 AM
To: ramaguer@cisco.com
Subject: Citibank's official notice

Dear client of the Citi,

As the Technical service of bank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

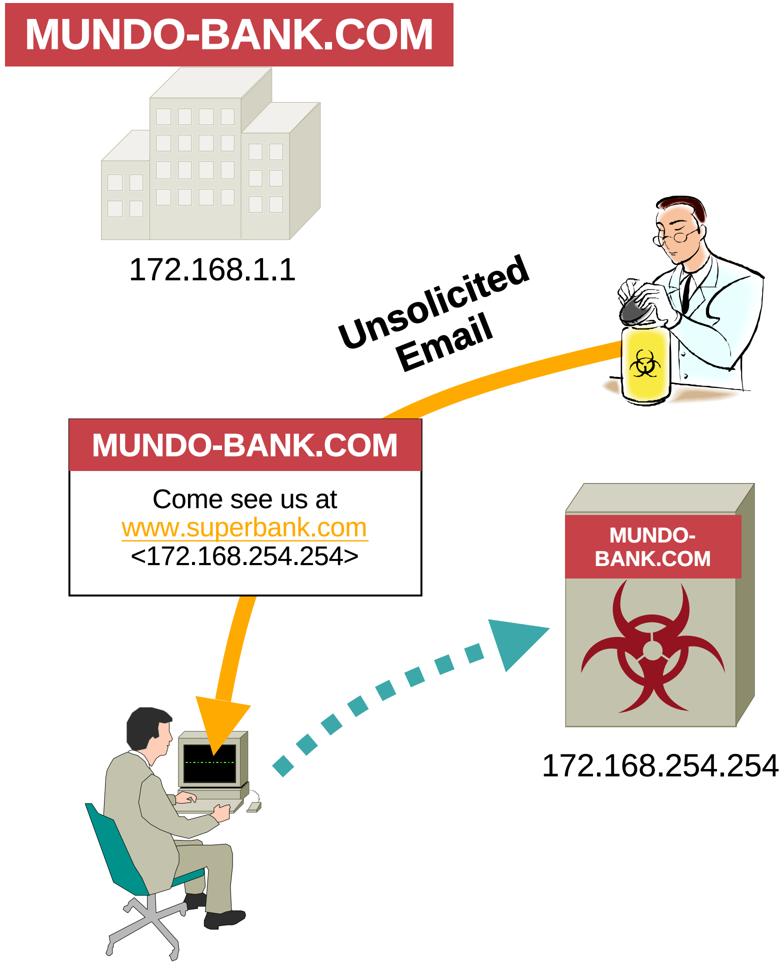
A member of citigroup
Copyright © 2004 Citicorp

In this Example, the Link Really Leads Through to:
http://web.da-us.citibank.com.userdll.com:4903/c/index.htm

Source:
www.atg.wa.gov/consumer/idprivacy/phishing.shtm

CONCLUSION: Unsolicited Email Can Be More than Just an Annoyance

New Threats: Phishing's Cousin—Pharming



MUNDO-BANK.COM

172.168.1.1

Unsolicited Email

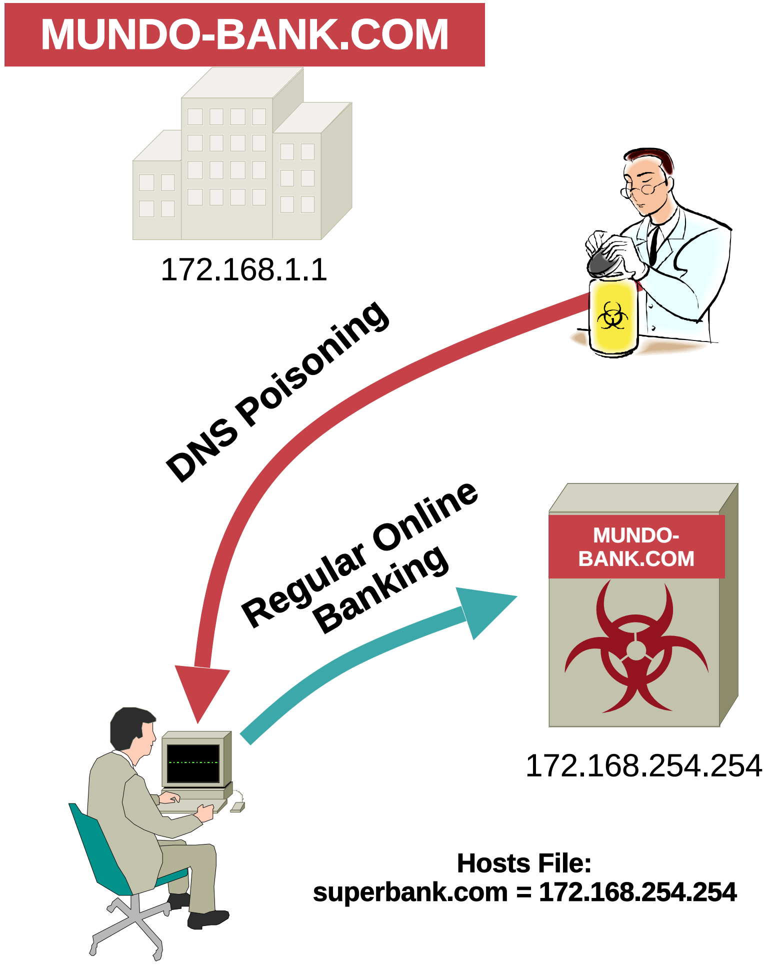
MUNDO-BANK.COM

Come see us at
www.superbank.com
<172.168.254.254>

MUNDO-BANK.COM

172.168.254.254

PHISHING



MUNDO-BANK.COM

172.168.1.1

DNS Poisoning

Regular Online Banking

MUNDO-BANK.COM

172.168.254.254

Hosts File:
superbank.com = 172.168.254.254

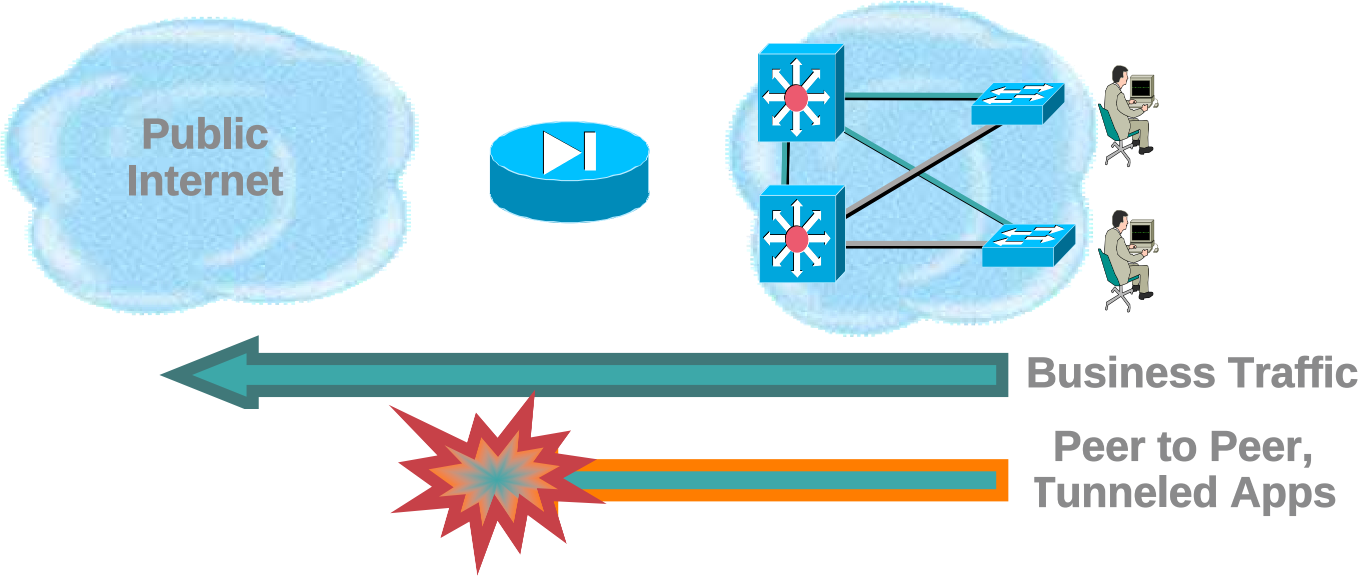
PHARMING

The Port 80 Problem

Opportunistic Applications Overloading Open Ports

Port Overloading enables violation of Security Policy:
Opportunistic applications tunnel through open outbound ports. Legacy firewalls cannot discern legitimate from illegitimate applications

Opportunistic Applications:
Peer-to-peer Apps
Instant Messaging
Remote PC Access Apps
Covert Channels



Some Solutions:

- Advanced firewalls can distinguish between applications by protocol semantics and enforce security policy

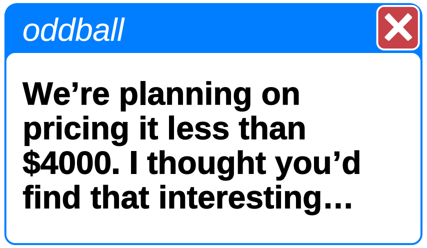
The Port 443 (SSL) Problem…

“Encrypted Port 80”

- Data confidentiality extends to network devices as well…
- Can verify compliance with SSL protocol spec, but beyond that, very difficult to enforce policy

Some Solutions:

- Protocol compliance checking
- Desktop application usage policy enforcement tools
- Destination filtering via domain/URL filtering
- Close 443 to all but well-defined business traffic



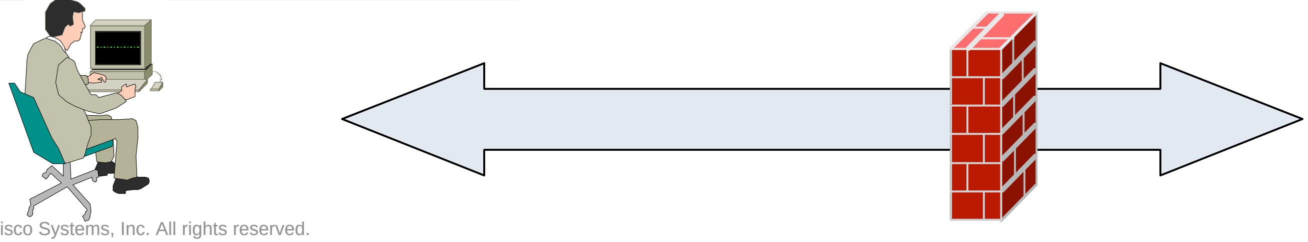
We’re planning on pricing it less than $4000. I thought you’d find that interesting…

S: 10.123.234.17
D: 123.234.123.234
Port: 443

Contents:
100010111010100110010
101100110101010001101
011010011010111001010

What is this?

Valid e-commerce?
Acceptable-use violations?
Covert channel?
Outbound attack?



Securing Web Services

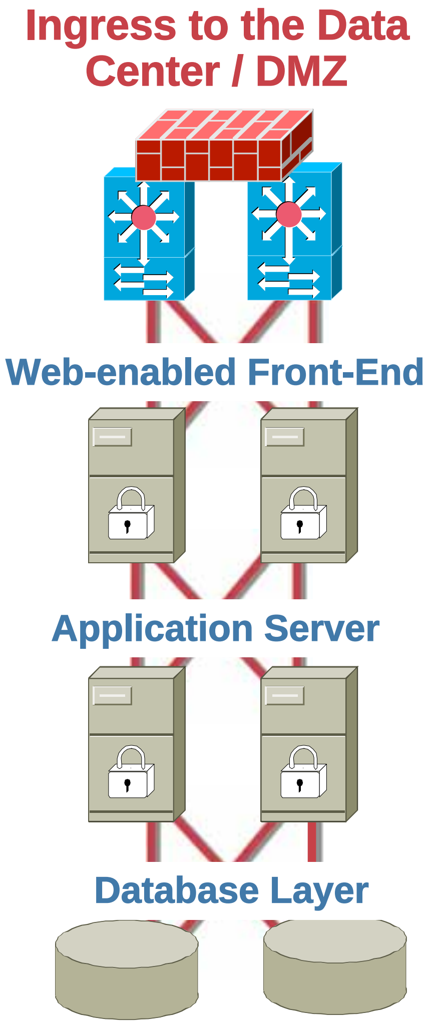
IT GIVES OUT YOUR NAME AND YOUR ADDRESS AND YOUR PHONE NUMBER!!! NOBODY'S SAFE!! WE'RE ALL NAKED!!
NEW WEB SERVICE?
NEW PHONE BOOK.
c/o
©96 COMPUTERWORLD

Web Services and XML Security

- Exposing the application layer to external entities for the first time
- Introduces new classes of credentials for access control
- Introduces new classes of attacks: X-malware, XML DoS, XPATH injection, etc.
- Allows new services for confidentiality and integrity: Field-level encryption, document signing, transformation

Some Solutions:

- Secure Coding!
- Schema validation toolsets
- Attack prevention technologies



Social Engineering

- Social Engineering Attacks: Attacks that compromise the “human” elements of business processing

  Assuming an identity to exploit trust relationships

- These forms of attack have been around forever

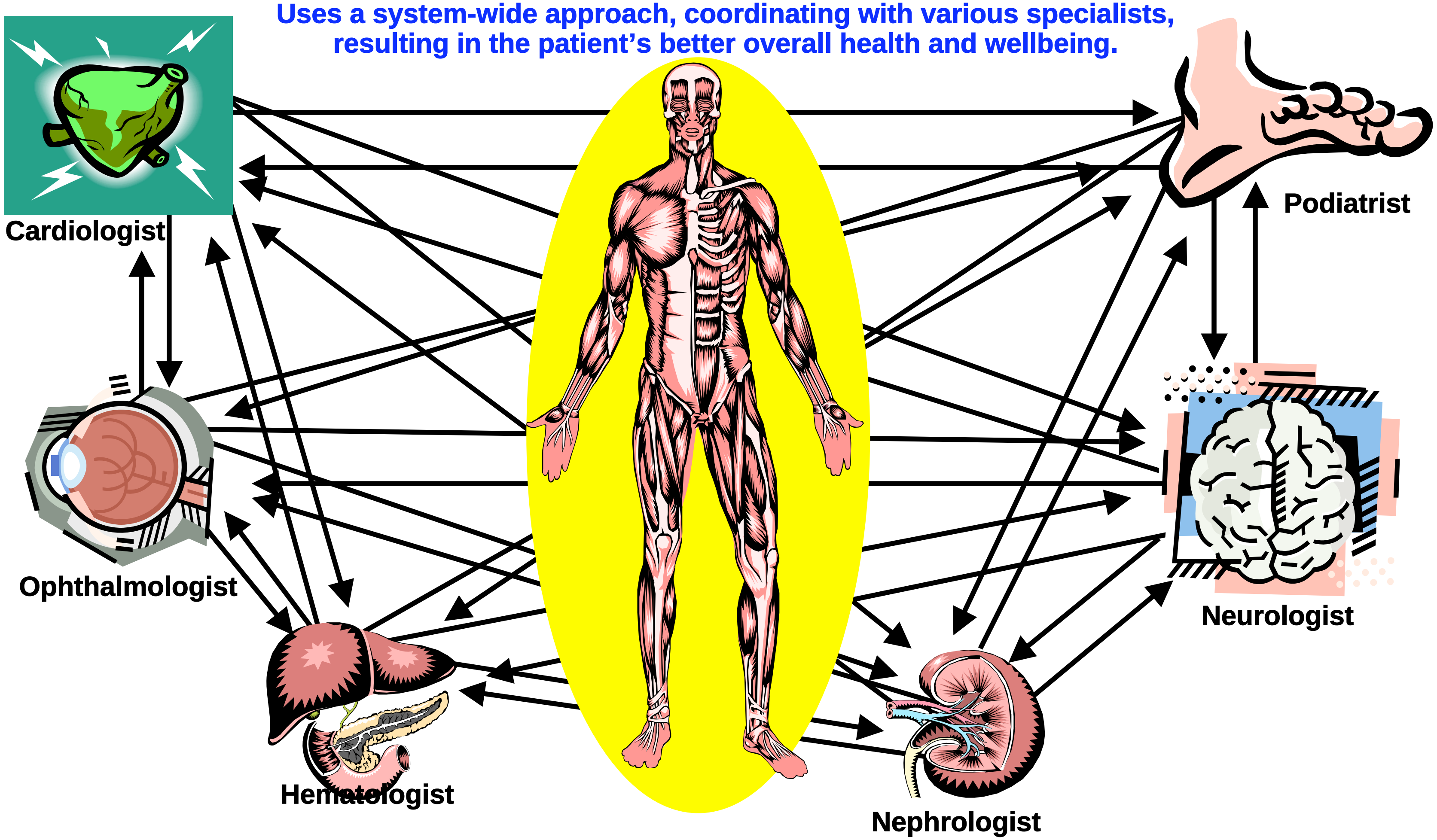
- Not an emerging threat in and of itself, but a constant “force multiplier” on new threats

The First Step - Telemetry

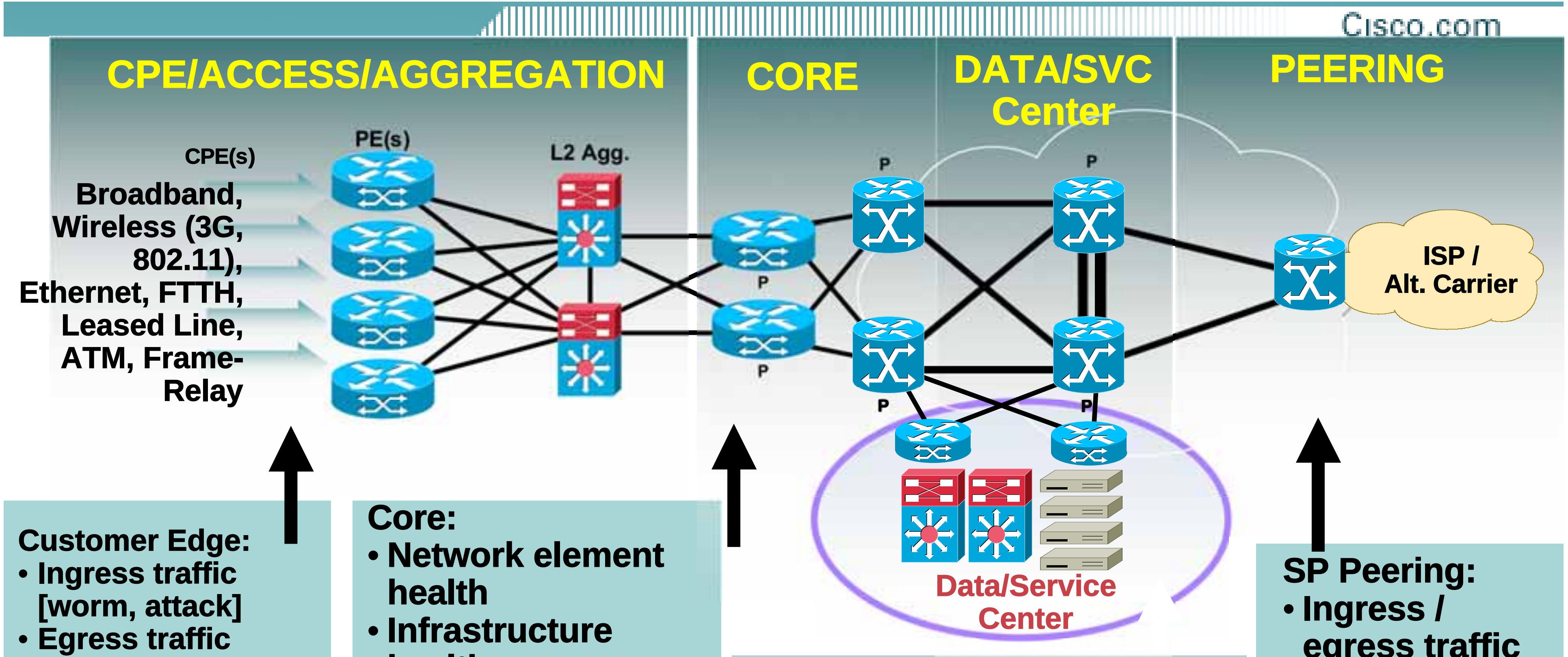
Holistic Approach to System-Wide Telemetry

Holistic Approach to Patient Care

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



Holistic Approach to System-Wide Telemetry (Cont.)



Customer Edge:
- Ingress traffic [worm, attack]
- Egress traffic [spreading worms]
- Shared resources such as DNS, SMTP and such servers
- Network element health

Core:
- Network element health
- Infrastructure health
- Performance
- Packet paths

Data Center:
- Ingress / egress traffic
- Intra Datacenter traffic due to trust relationships of servers
- Availability scheme influenced traffic patterns
- Network element health

SP Peering:
- Ingress / egress traffic
- Asymmetric traffic due to peering policy & topology
- Network element health

What Is One Listening to?

- Ingress traffic flow
- Egress traffic flow
- Network element health
  - Resources such as CPU, memory, etc.
  - # flow to build baseline and detect anomaly
  - Top talkers
  - Open ports – services etc.
- Shared services
  - DNS, SMTP, Availability related services, etc.

Understand the Concept of Data Gathering

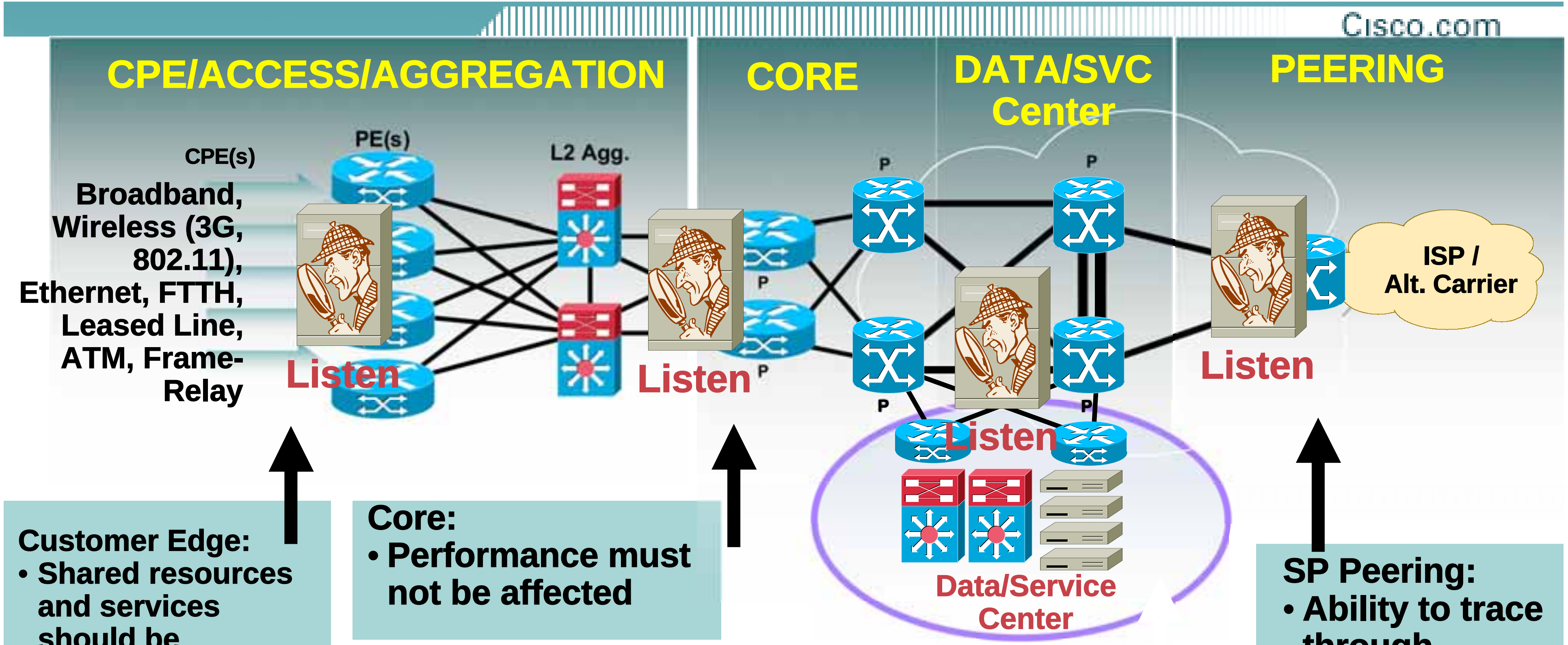
Risks and threats are NOT prevalent in one place ONLY…

Need to watch everywhere to avoid being eaten by thousand turkeys...

- **Listening to a network element**
  - **Per device listening**
  - **Local data provide information about local threats**
- **Listening to Many**
  - **Correlation is a MUST**
  - **Intelligent analysis is a MUST**

Listen

Holistic Approach to System-Wide Telemetry



Customer Edge:
- Shared resources and services should be available

Core:
- Performance must not be affected

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

SP Peering:
- Ability to trace through asymmetric traffic

Network Telemetry: Tools, Techniques and Protocols

How to Gather Data or Information?

- Proactive Telemetry
  - NetFlow
  - SNMP
  - RMON
  - Syslog
  - Network element health
  - BGP
  - DNS
- Telemetry During the Incident
  - Packet Capture
  - show commands
  - Network element health
  - Syslog

Netflow : What Is a Flow?

- **Defined by seven unique keys:**

  Source IP address

  Destination IP address

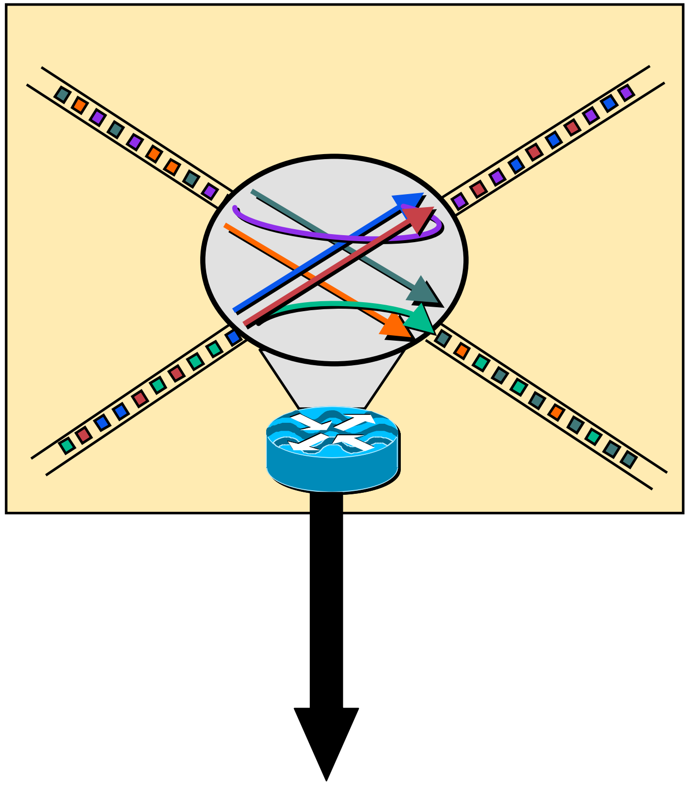
  Source port

  Destination port

  Layer 3 protocol type

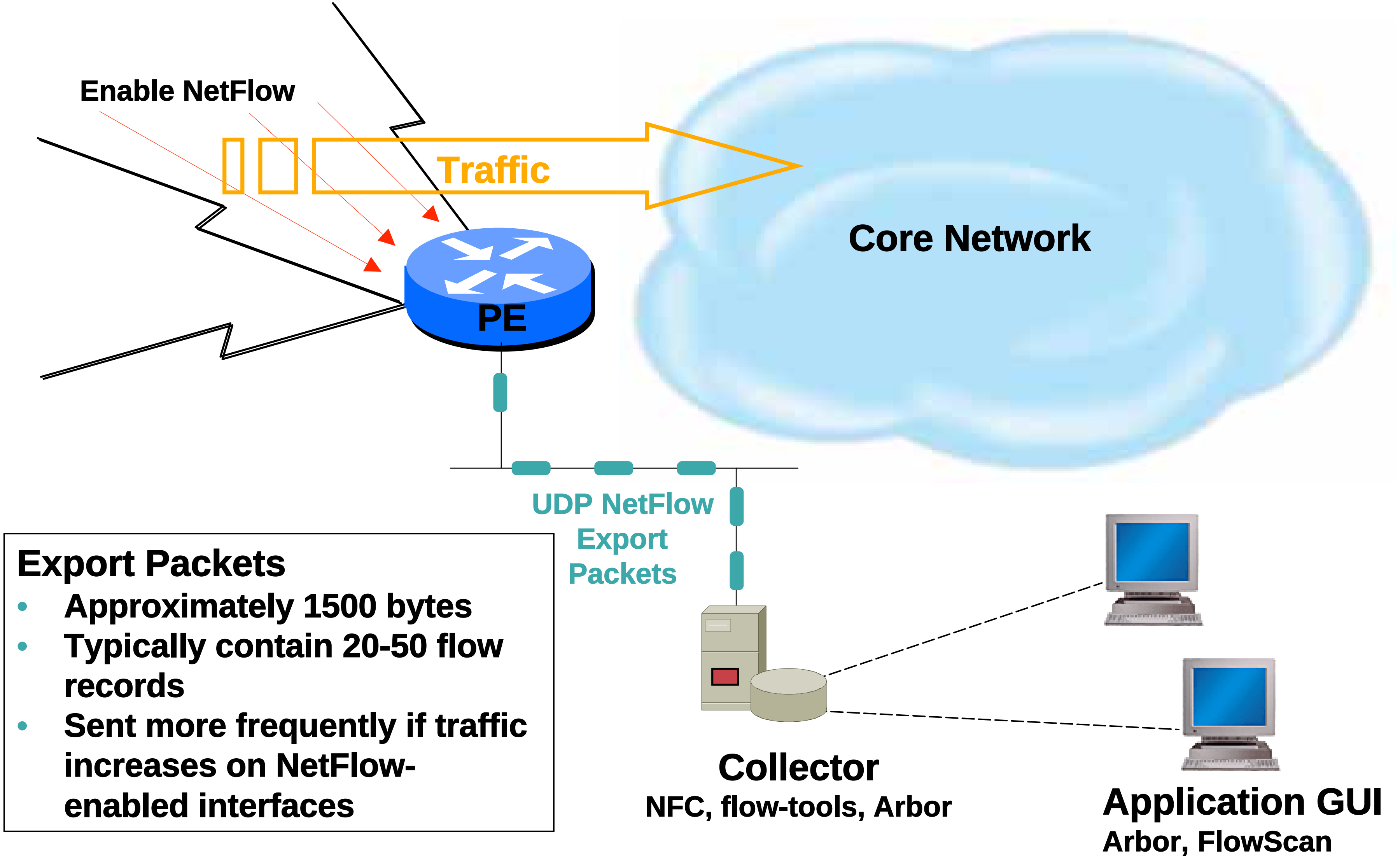
  TOS byte (DSCP)

  Input logical interface (ifIndex)



Exported Data

Netflow : Creating Export Packets



Export Packets

- Approximately 1500 bytes
- Typically contain 20-50 flow records
- Sent more frequently if traffic increases on NetFlow-enabled interfaces

Netflow : Key Concept—NetFlow Scalability

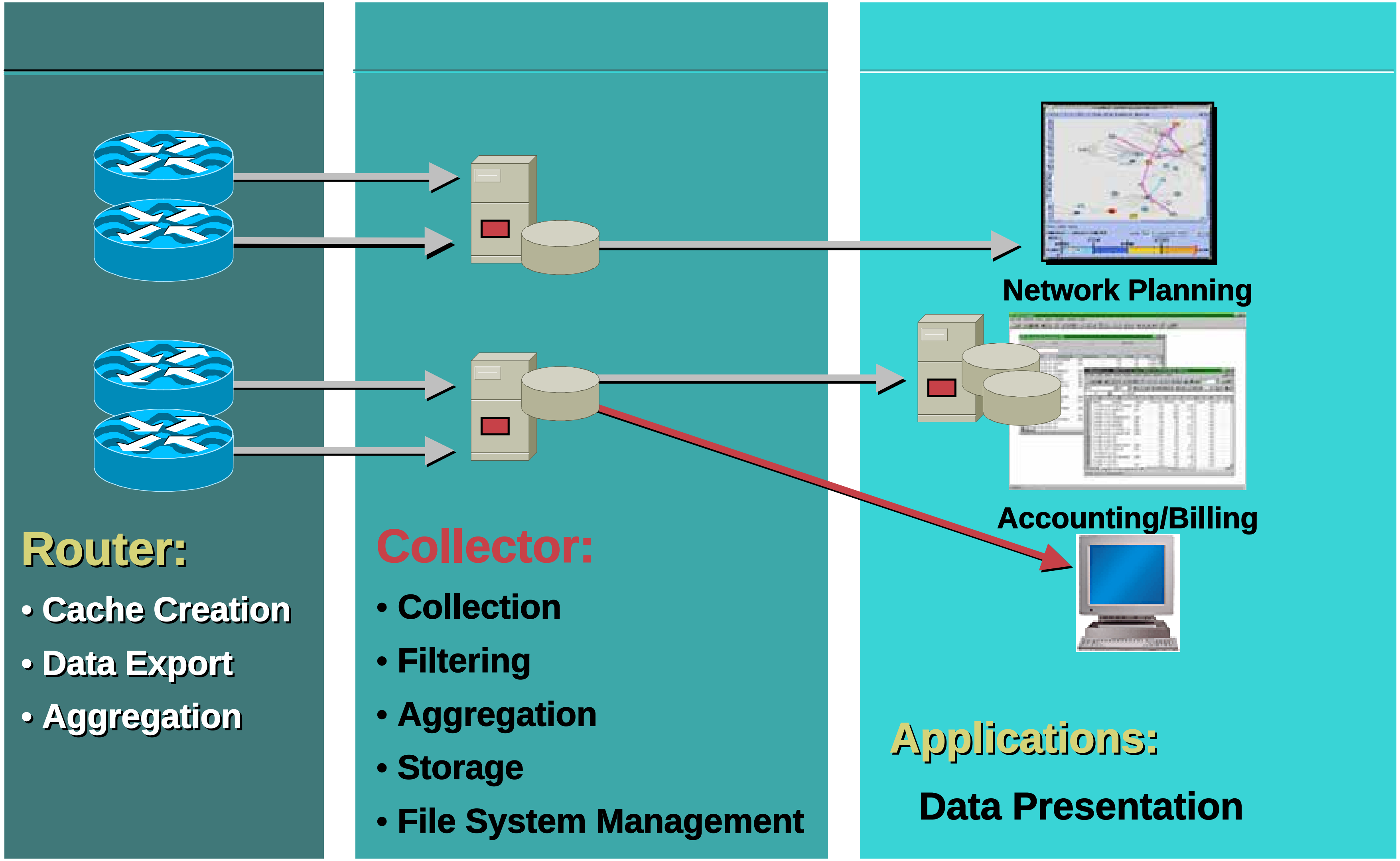
- Packet capture is like a *wiretap*
- NetFlow is like a *phone bill*
- This level of granularity allows NetFlow to scale for very large amounts of traffic

We can learn a lot from studying the phone bill!

Who’s talking to whom, over what protocols & ports, for how long, at what speed, for what duration, etc.

NetFlow is a form of *telemetry* pushed from the routers/switches - each one can be a sensor!

NetFlow Infrastructure



Router:

- Cache Creation
- Data Export
- Aggregation

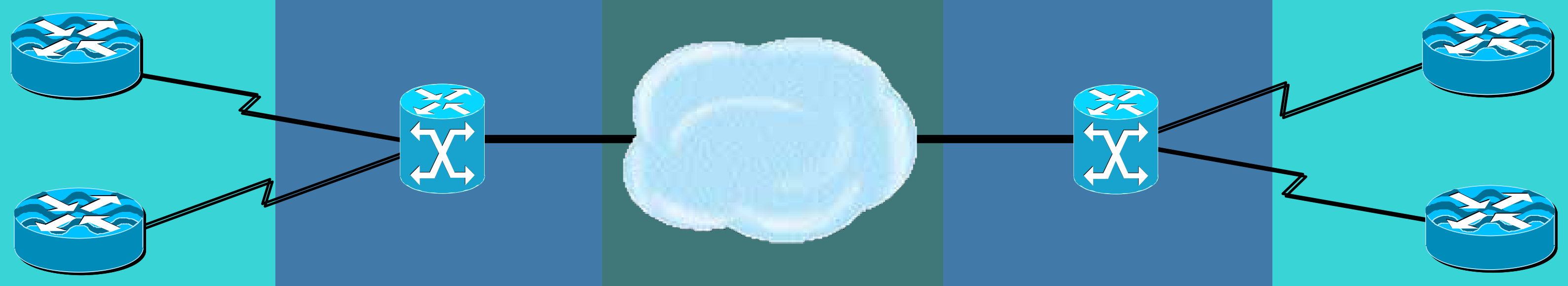
Collector:

- Collection
- Filtering
- Aggregation
- Storage
- File System Management

Applications:

Data Presentation

Where to Deploy NetFlow?

	Access	Distribution	Core	Distribution	Access
Network Layer					
Applications	• Attack Detection • User (IP) monitoring • Application monitoring	• Billing • Chargeback • AS Peer Monitoring • Attack Detection	• Traffic Engineering • Traffic Analysis • Attack Detection	• Billing • Chargeback • AS Peer Monitoring • Attack Detection	• Attack Detection • User (IP) monitoring • Application monitoring
NetFlow Features	• Aggregation Schemes (v8) • “show ip cache flow” command • Arbor Networks	• NetFlow MPLS Egress Accounting • BGP Next-hop (v9) • Arbor Networks	• MPLS Aware NetFlow (v9) • BGP Next-hop (v9) • Sampled NetFlow • Arbor Networks	• NetFlow MPLS Egress Accounting • BGP Next-hop (v9) • Arbor Networks	• Aggregation Schemes (v8) • “show ip cache flow” command • Arbor Networks

Principal NetFlow Benefits

SERVICE PROVIDER

- Peering arrangements
- SLA VPN user reporting
- Usage-based billing
- DoS/worm detection
- Traffic engineering
- Troubleshooting

ENTERPRISE

- Internet access monitoring (protocol distribution, traffic origin/destination)
- Associate cost of IT to departments
- More scalable than RMON
- DoS/worm detection
- Policy compliance monitoring
- Troubleshooting

Open Source Tools for NetFlow Analysis —The OSU Flow-Tools

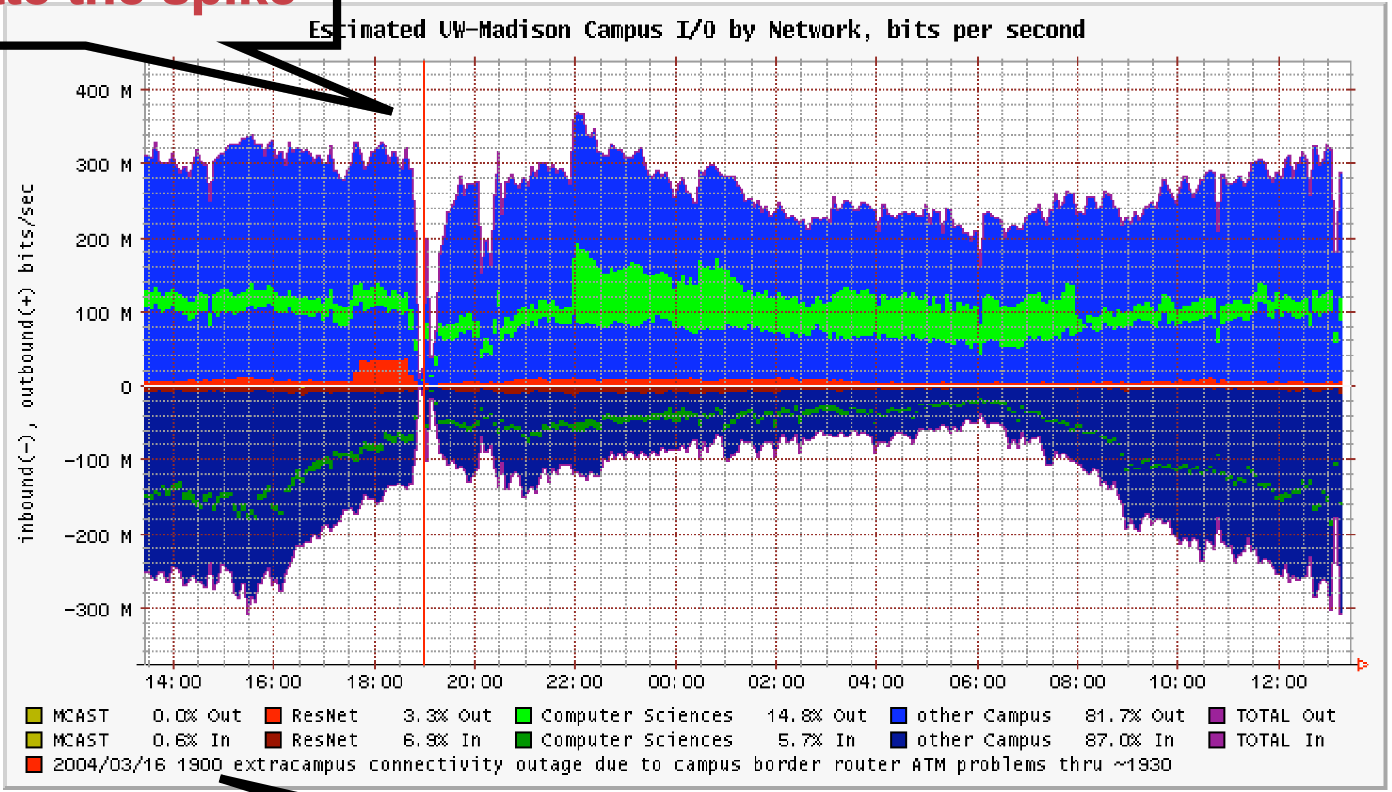
- Open source NetFlow collection and retrieval tools
- Developed and maintained by Mark Fullmer, available from http://www.splintered.net/sw/flow-tools/
- Runs on common *NIX platforms (Linux, FreeBSD, Mac OS/X, Solaris, etc.)
- Command-line tools allow for very display/sorting of specific criteria (source/dest IP, source/dest ASN, protocol, port, etc.)
- Data can be batched and imported into database such as Oracle, MySQL, Postgres, etc.
- Can be combined with other tools to provide visualization of traffic patterns
- Many other useful features - check it out today!

Open Source Tools for NetFlow Analysis Visualization—FlowScan

- Open source NetFlow graphing/visualization tools
- Developed and maintained by Dave Plonka, available from http://net.doit.wisc.edu/~plonka/FlowScan/
- Runs on common *NIX platforms (Linux, FreeBSD, Mac OS/X, Solaris, etc.)
- Makes use of NetFlow data collected via flow-tools to build traffic graphs
- Top-talkers by subnet, other types of reports supported
- Makes use of RRDTool for graphing
- Add-ons such as JKFlow module allow more detailed graphing

Open Source Tools for NetFlow Analysis Visualization—FlowScan (Cont.)

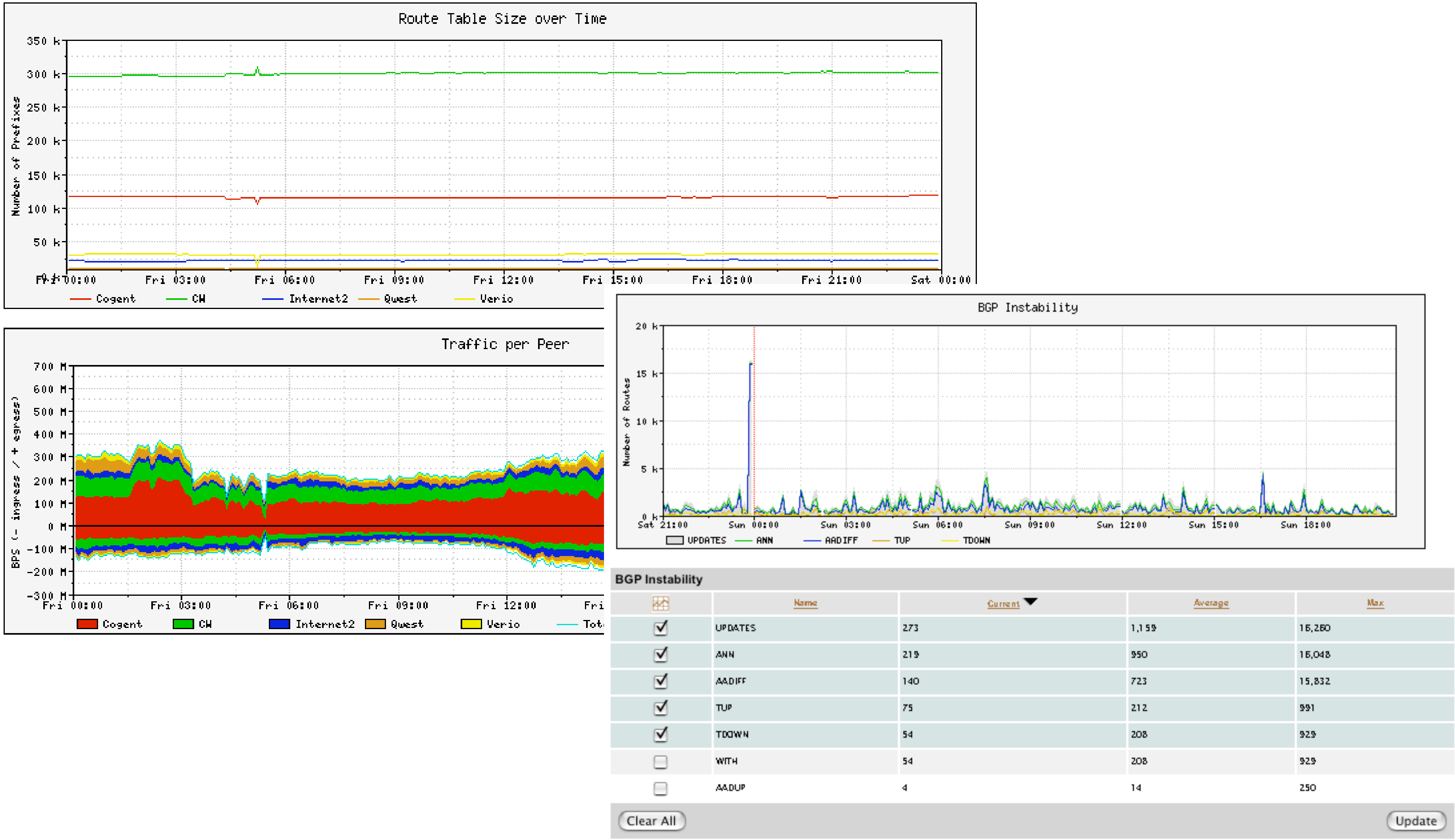
Investigate the spike



An identified cause of the outage

Source: University of Wisconsin

Netflow : Coupling Control and Data Planes



BGP Instability

	Name	Current ▼	Average	Max
☑	UPDATES	273	1,159	16,260
☑	ANN	219	950	16,048
☑	AADIFF	140	723	15,832
☑	TUP	75	212	991
☑	TDOWN	54	208	929
□	WITH	54	208	929
□	AADUP	4	14	250

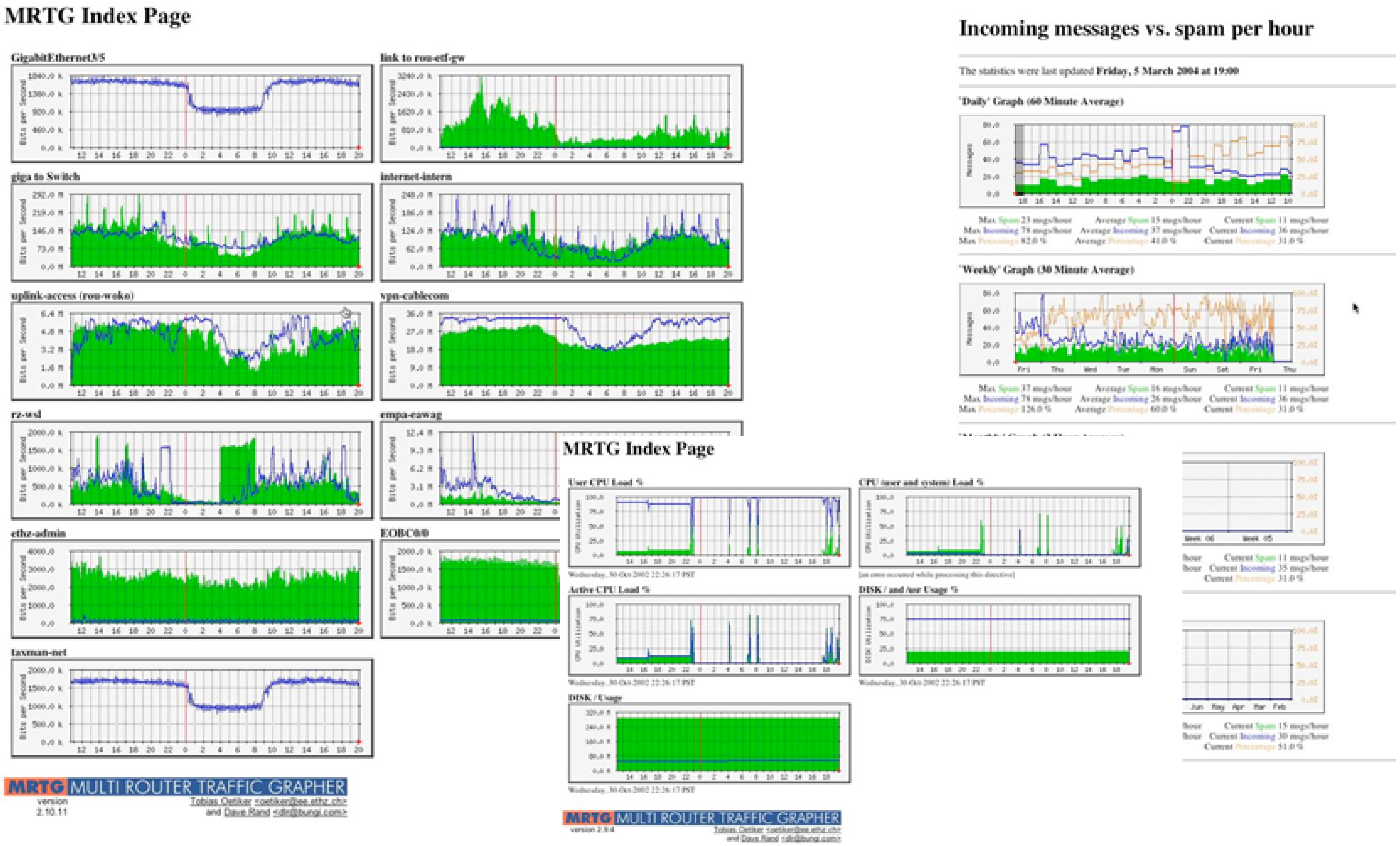
SNMP

- SNMP = Simple Network Management Protocol
- Canonical method of obtaining real-time information from network devices
- SNMPv3 provides authentication, encryption
- MIBs support polling of statistics ranging from interface bandwidth to CPU utilization to chassis temperature, etc.
- Both a ‘pull’ model for statistical polling and a ‘push’ model for trap generation based upon events such as link up/down
- Many open-source and commercial collection systems, visualization tools
- Easiest way to get into profiling of general network characteristics

Displaying SNMP Data with MRTG

- MRTG—the Multi Router Traffic Grapher
- Open source SNMP visualization toolset developed by Tobi Oetiker, available from http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- Long track-record - (in general use since 1995)
- Can be used to graph router/switch data, host performance info from systems running SNMP agents, etc. (generates HTML w/PNG images)
- Runs on Linux, FreeBSD, Mac OS/X, Solaris, other *NIX, Windows
- Written in Perl, has its own SNMP implementation

Powerful Visualization of SNMP with MRTG



MRTG Index Page

Incoming messages vs. spam per hour

The statistics were last updated **Friday, 5 March 2004 at 19:00**

'Daily' Graph (60 Minute Average)

Max Spam 23 msgs/hour Average Spam 15 msgs/hour Current Spam 11 msgs/hour
Max Incoming 78 msgs/hour Average Incoming 37 msgs/hour Current Incoming 36 msgs/hour
Max Percentage 82.0 % Average Percentage 41.0 % Current Percentage 31.0 %

'Weekly' Graph (30 Minute Average)

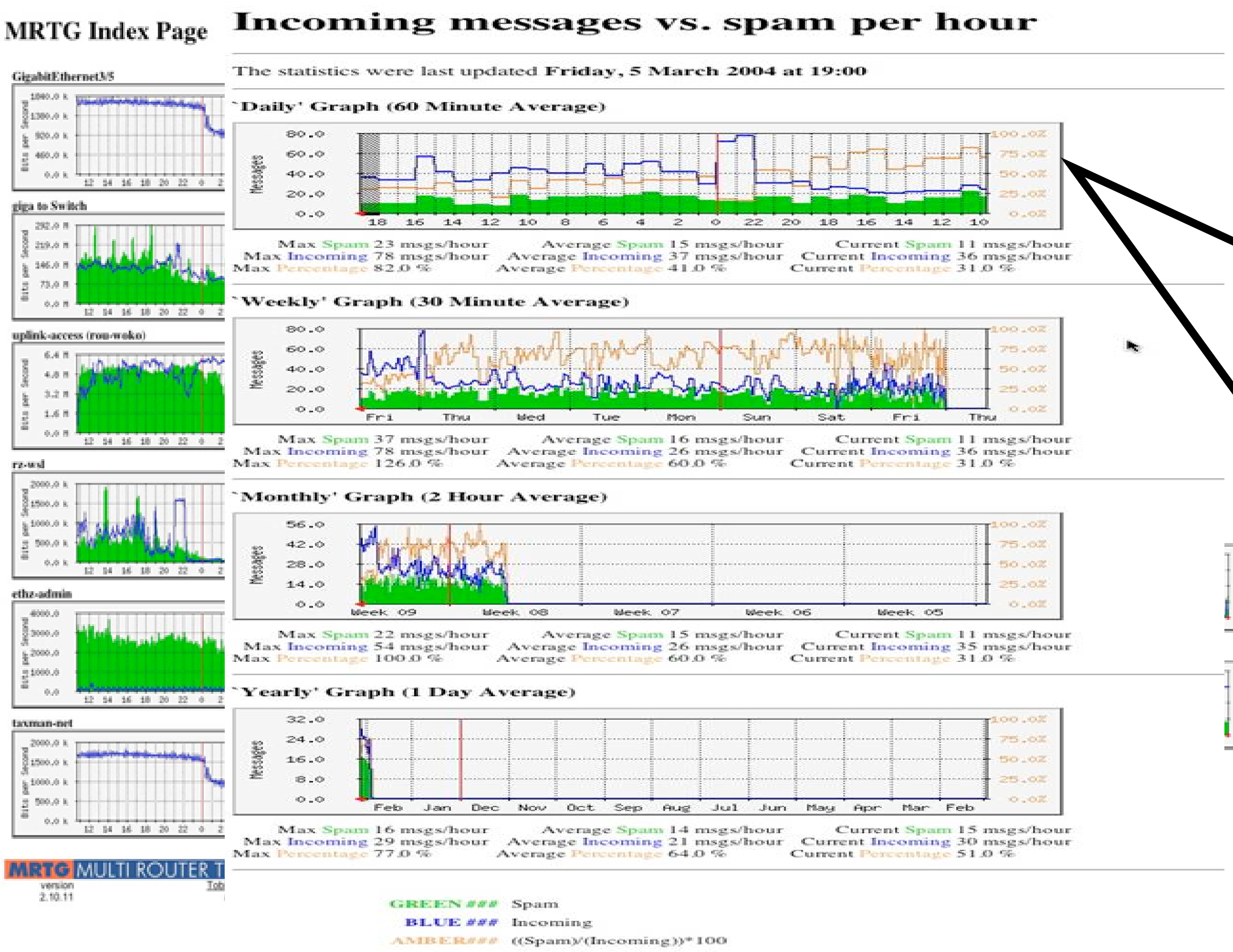
Max Spam 37 msgs/hour Average Spam 16 msgs/hour Current Spam 11 msgs/hour
Max Incoming 78 msgs/hour Average Incoming 26 msgs/hour Current Incoming 36 msgs/hour
Max Percentage 126.0 % Average Percentage 60.0 % Current Percentage 31.0 %

Wednesday, 30 Oct 2002 22:26:17 PST

[an error occurred while processing this directive]

Source: mrtg.org

Powerful Visualization of SNMP with MRTG (Cont.)



Incoming messages vs. spam per hour

The statistics were last updated **Friday, 5 March 2004 at 19:00**

`Daily' Graph (60 Minute Average)

Max Spam 23 msgs/hour   Average Spam 15 msgs/hour   Current Spam 11 msgs/hour
Max Incoming 78 msgs/hour   Average Incoming 37 msgs/hour   Current Incoming 36 msgs/hour
Max Percentage 82.0 %   Average Percentage 41.0 %   Current Percentage 31.0 %

`Weekly' Graph (30 Minute Average)

Max Spam 37 msgs/hour   Average Spam 16 msgs/hour   Current Spam 11 msgs/hour
Max Incoming 78 msgs/hour   Average Incoming 26 msgs/hour   Current Incoming 36 msgs/hour
Max Percentage 126.0 %   Average Percentage 60.0 %   Current Percentage 31.0 %

`Monthly' Graph (2 Hour Average)

Max Spam 22 msgs/hour   Average Spam 15 msgs/hour   Current Spam 11 msgs/hour
Max Incoming 54 msgs/hour   Average Incoming 26 msgs/hour   Current Incoming 35 msgs/hour
Max Percentage 100.0 %   Average Percentage 60.0 %   Current Percentage 31.0 %

`Yearly' Graph (1 Day Average)

Max Spam 16 msgs/hour   Average Spam 14 msgs/hour   Current Spam 15 msgs/hour
Max Incoming 29 msgs/hour   Average Incoming 21 msgs/hour   Current Incoming 30 msgs/hour
Max Percentage 77.0 %   Average Percentage 64.0 %   Current Percentage 51.0 %

GREEN ###	Spam
BLUE ###	Incoming
AMBER###	((Spam)/(Incoming))*100

Various type of statistics gathering and display

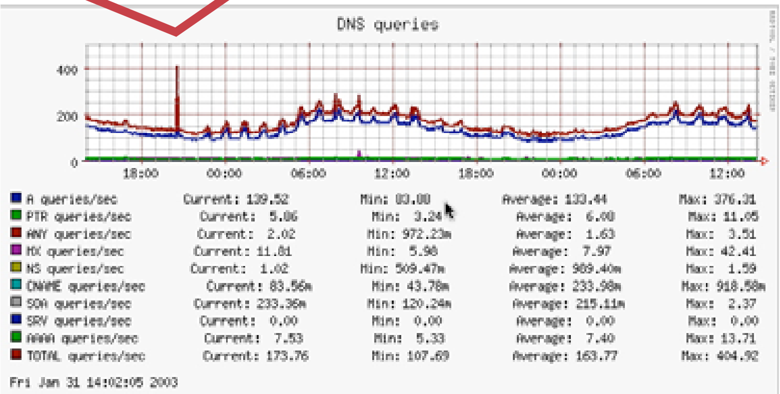
Source: mrtg.org

Other Visualization Techniques Using SNMP Data with RRDTool

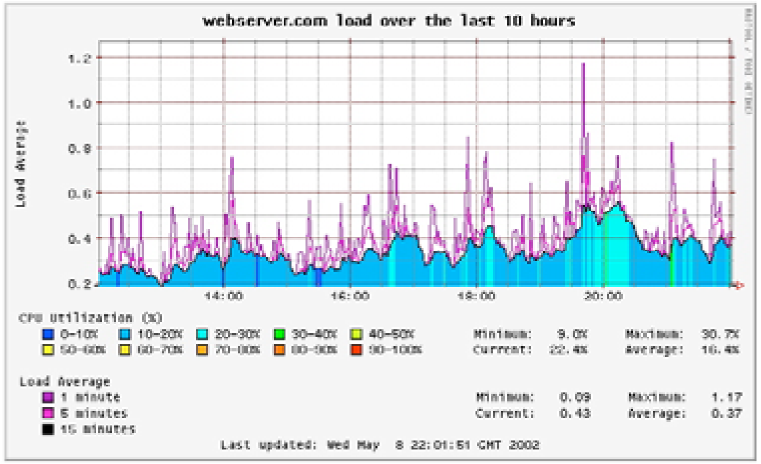
- RRDTool—the Round Robin Database Tool
- Another open source SNMP visualization toolset developed by Tobi Oetiker, available from http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
- Improved graphing performance, new types of graphs
- Can be used in conjunction with MRTG - does not do its own SNMP collection (can also be used w/NetFlow via OSU flow-tools & FlowScan)
- Runs on Linux, FreeBSD, Mac OS/X, Solaris, other *NIX, Windows
- Many nice HTML/PHP front-ends such as Cacti, Cricket, Big Sister, etc.

Other Visualization Techniques Using SNMP Data with RRDTool (Cont.)

Anomaly for DNS Queries

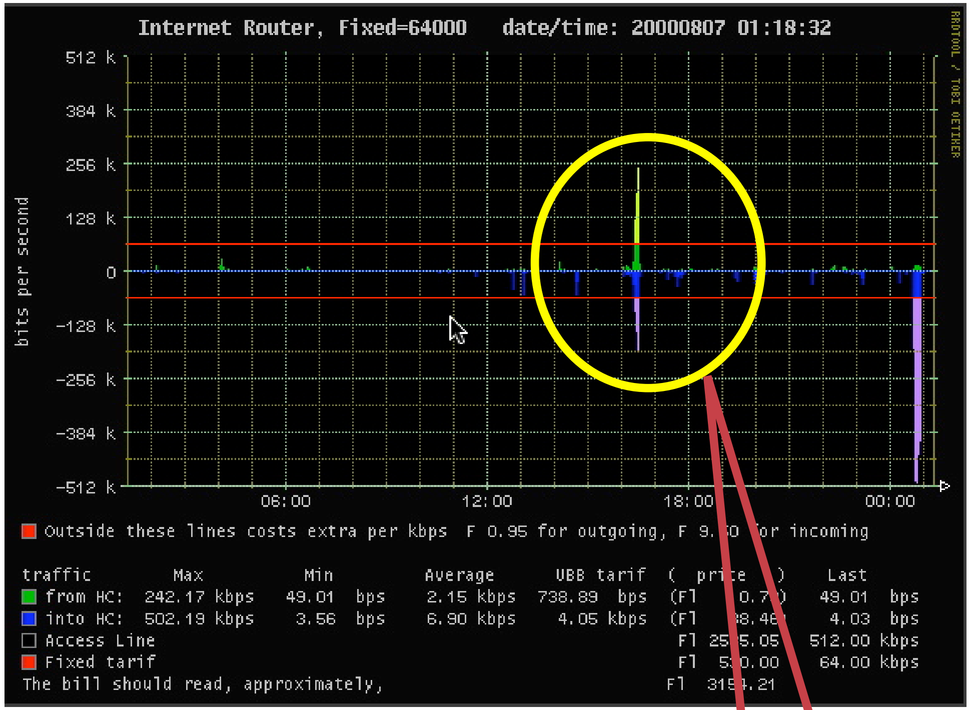


```
A queries/sec        Current: 139.52    Min: 83.88      Average: 133.44     Max: 376.31
PTR queries/sec      Current:  5.06     Min:  3.24      Average:  6.00      Max: 11.05
ANY queries/sec      Current:  2.02     Min: 972.23m    Average:  1.63      Max:  3.51
MX queries/sec       Current: 11.81     Min:  5.98      Average:  7.97      Max: 42.41
NS queries/sec       Current:  1.02     Min: 509.47m    Average: 989.40m    Max:  1.59
CNAME queries/sec    Current: 83.56m    Min: 43.78m     Average: 233.98m    Max: 918.58m
SOA queries/sec      Current: 233.36m   Min: 120.24m    Average: 215.11m    Max:  2.37
SRV queries/sec      Current:  0.00     Min:  0.00      Average:  0.00      Max:  0.00
AAAA queries/sec     Current:  7.53     Min:  5.33      Average:  7.40      Max: 13.71
TOTAL queries/sec    Current: 173.76    Min: 107.69     Average: 163.77     Max: 404.92

Fri Jan 31 14:02:05 2003
```

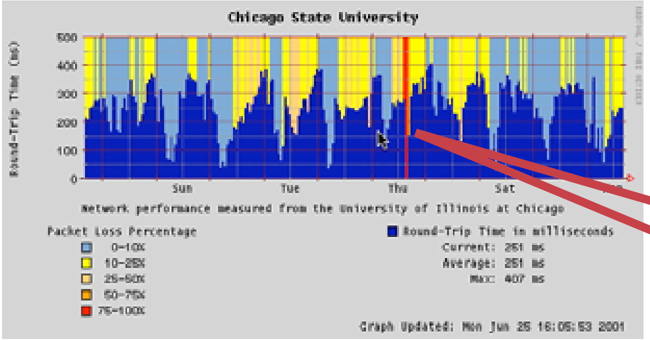


```
CPU Utilization (%)
   0-10%   10-20%   20-30%   30-40%   40-50%      Minimum:   9.0%    Maximum:  30.7%
   50-60%  60-70%   70-80%   80-90%   90-100%     Current:  22.4%    Average:  16.4%

Load Average
   1 minute                                       Minimum:   0.09    Maximum:   1.17
   5 minutes                                      Current:   0.43    Average:   0.37
   15 minutes
                 Last updated: Wed May  8 22:01:51 GMT 2002
```

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



```
Outside these lines costs extra per kbps  F 0.95 for outgoing, F 9.[illegible]0 for incoming

traffic        Max           Min         Average      UBB tarif   ( price  )     Last
from HC:   242.17 kbps   49.01  bps   2.15 kbps   738.89  bps   (Fl    0.7[illegible])   49.01  bps
into HC:   502.19 kbps    3.56  bps   6.90 kbps     4.05 kbps   (Fl  [illegible]8.46)    4.03  bps
Access Line                                                   Fl 25[illegible]5.05   512.00 kbps
Fixed tarif                                                   Fl  5[illegible]0.00    64.00 kbps
The bill should read, approximately,                         Fl  315[illegible].21
```



```
Network performance measured from the University of Illinois at Chicago

Packet Loss Percentage                       Round-Trip Time in milliseconds
     0-10%                                            Current: 251 ms
    10-25%                                            Average: 251 ms
    25-50%                                               Max: 407 ms
    50-75%
    75-100%
                                          Graph Updated: Mon Jun 25 16:05:53 2001
```

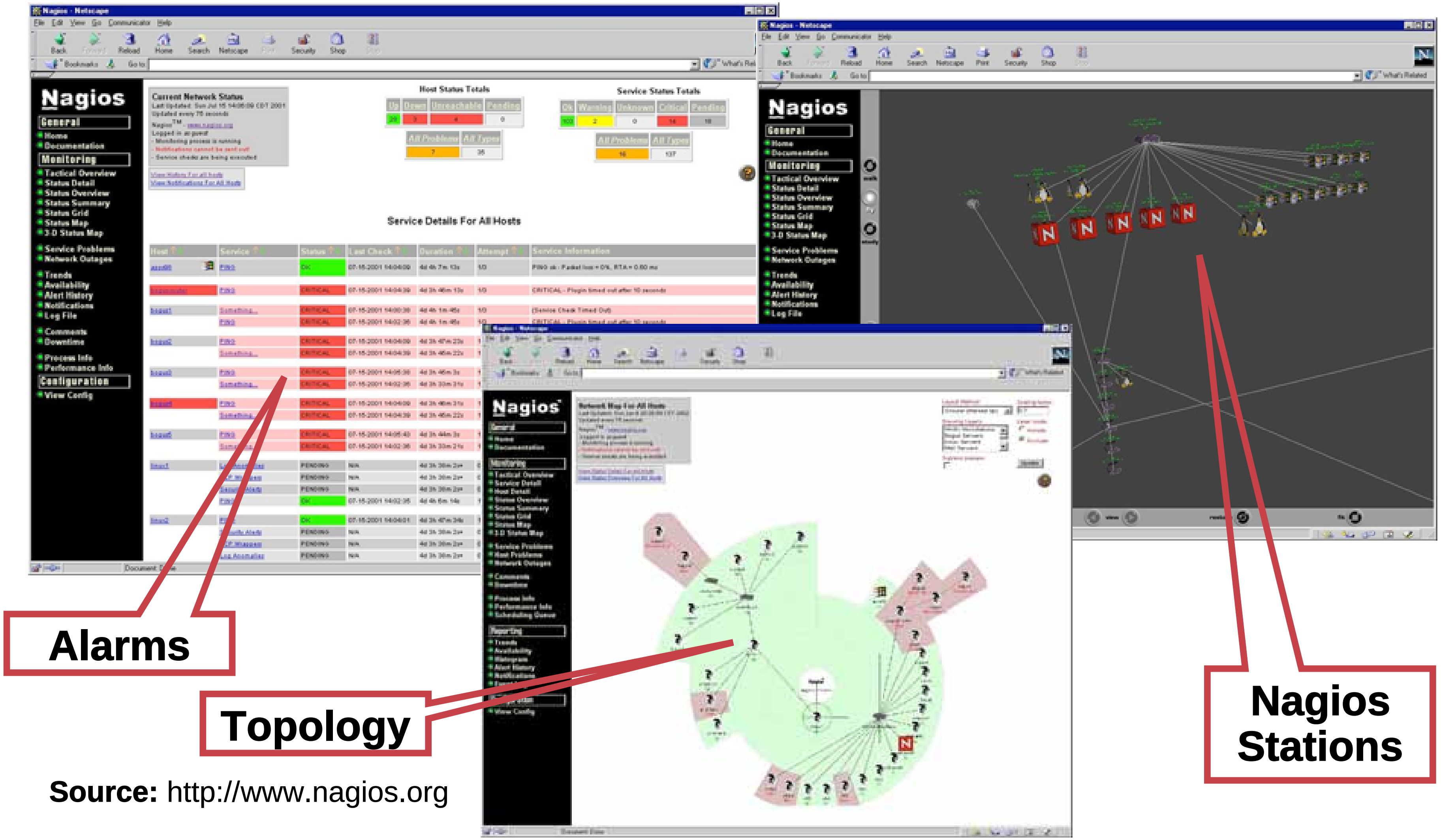
Thru'put Spike

RTT Spike

Displaying SNMP Data with NMS Station

- Can be considered as "Local telemetry"
- Network Management Systems (NMS) can serve as SNMP consoles, among other things
- Many can use SNMP traps and/or other forms of telemetry as triggers for paging, scripted actions, etc.
- Pulling information together can be useful for NOCs, operations teams
- Commercial systems such as HP OpenView, Micromuse NetCool, IBM Tivoli, CA Unicenter
- Several open source systems - Big Brother (http://bb4.com/), Big Sister (http://bigsister.graeff.com/), Nagios (http://www.nagios.org/), and others

Displaying SNMP Data with NMS—Nagios



Current Network Status
Last Updated: Sun Jul 15 14:05:09 CDT 2001
Updated every 75 seconds
Nagios™ - www.nagios.org
Logged in as guest
- Monitoring process is running
- Notifications cannot be sent out!
- Service checks are being executed

View History For all hosts
View Notifications For All Hosts

Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
[illegible]	PING	OK	07-15-2001 14:04:09	4d 4h 7m 13s	1/3	PING ok - Packet loss = 0%, RTA = 0.80 ms
[illegible]	PING	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 13s	1/3	CRITICAL - Plugin timed out after 10 seconds
[illegible]	Something...	CRITICAL	07-15-2001 14:00:38	4d 4h 1m 45s	1/3	(Service Check Timed Out)
	PING	CRITICAL	07-15-2001 14:02:38	4d 4h 1m 45s	1/3	CRITICAL - Plugin timed out after 10 seconds
[illegible]	PING	CRITICAL	07-15-2001 14:04:09	4d 3h 47m 23s	[illegible]	[illegible]
	Something...	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 22s	[illegible]	[illegible]
[illegible]	PING	CRITICAL	07-15-2001 14:05:38	4d 3h 46m 3s	[illegible]	[illegible]
	Something...	CRITICAL	07-15-2001 14:02:38	4d 3h 33m 31s	[illegible]	[illegible]
[illegible]	PING	CRITICAL	07-15-2001 14:04:09	4d 3h 46m 31s	[illegible]	[illegible]
	Something...	CRITICAL	07-15-2001 14:04:39	4d 3h 46m 22s	[illegible]	[illegible]
[illegible]	PING	CRITICAL	07-15-2001 14:05:40	4d 3h 44m 3s	[illegible]	[illegible]
	Something...	CRITICAL	07-15-2001 14:02:38	4d 3h 33m 21s	[illegible]	[illegible]
[illegible]	[illegible]	PENDING	N/A	4d 3h 30m 2s+	[illegible]	[illegible]
	[illegible]	PENDING	N/A	4d 3h 30m 2s+	[illegible]	[illegible]
	[illegible]	PENDING	N/A	4d 3h 30m 2s+	[illegible]	[illegible]
	PING	OK	07-15-2001 14:02:38	4d 4h 6m 14s	[illegible]	[illegible]
[illegible]	PING	OK	07-15-2001 14:04:01	4d 3h 47m 34s	[illegible]	[illegible]
	[illegible]	PENDING	N/A	4d 3h 30m 2s+	[illegible]	[illegible]
	[illegible]	PENDING	N/A	4d 3h 30m 2s+	[illegible]	[illegible]
	Log Anomalies	PENDING	N/A	4d 3h 30m 2s+	[illegible]	[illegible]

Alarms

Topology

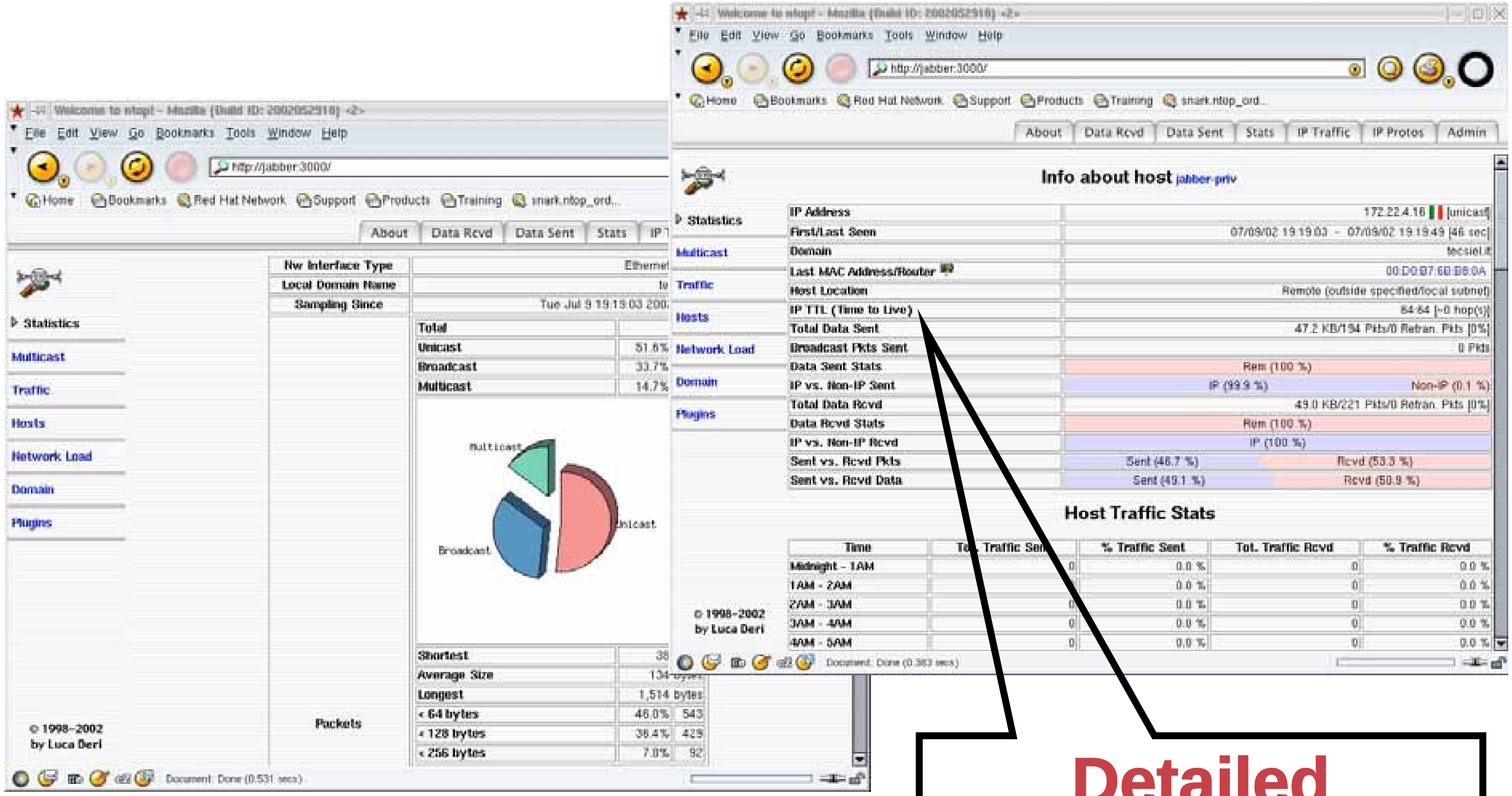
Nagios Stations

Source: http://www.nagios.org

RMON—Remote MONitoring

- RMON is a standard defining how remote probes or agents relay network traffic information back to a central console
- Not as prevalent as SNMP or NetFlow - supported mainly by commercial network management systems
- Cisco Network Analysis Module-2 (NAM-2), ntop (http://www.ntop.org) are examples of RMON probes
- Most RMON probes look at raw packets via SPAN/RSPAN and generate statistics from observed traffic
- Mini-RMON statistics available on Catalyst 6500/NAM-2, provides detailed stats from layer-2 access ports

Displaying RMON—ntop Examples


Welcome to ntop! - Mozilla {Build ID: 2002052918} <2>
File Edit View Go Bookmarks Tools Window Help
http://jabber:3000/
Home Bookmarks Red Hat Network Support Products Training snark.ntop_ord...
About Data Rcvd Data Sent Stats IP Traffic IP Protos Admin
Statistics
Multicast
Traffic
Hosts
Network Load
Domain
Plugins
Multicast
Unicast
Broadcast
© 1998-2002 by Luca Deri
Document: Done (0.531 secs)
Document: Done (0.383 secs)

Nw Interface Type	Ethernet
Local Domain Name	lo
Sampling Since	Tue Jul 9 19:19:03 200

Packets			
	Total		
	Unicast	51.6%	
	Broadcast	33.7%	
	Multicast	14.7%	
	Shortest	38	
	Average Size	134 bytes	
	Longest	1,514 bytes	
	< 64 bytes	46.0%	543
	< 128 bytes	36.4%	429
	< 256 bytes	7.8%	92

Info about host jabber-priv

IP Address	172.22.4.16 [unicast]
First/Last Seen	07/09/02 19:19:03 - 07/09/02 19:19:49 [46 sec]
Domain	tecsiel.it
Last MAC Address/Router	00:D0:B7:6B:B8:0A
Host Location	Remote (outside specified/local subnet)
IP TTL (Time to Live)	64:64 [~0 hop(s)]
Total Data Sent	47.2 KB/194 Pkts/0 Retran. Pkts [0%]
Broadcast Pkts Sent	0 Pkts
Data Sent Stats	Rem (100 %)
IP vs. Non-IP Sent	IP (99.9 %) Non-IP (0.1 %)
Total Data Rcvd	49.0 KB/221 Pkts/0 Retran. Pkts [0%]
Data Rcvd Stats	Rem (100 %)
IP vs. Non-IP Rcvd	IP (100 %)
Sent vs. Rcvd Pkts	Sent (46.7 %) Rcvd (53.3 %)
Sent vs. Rcvd Data	Sent (49.1 %) Rcvd (50.9 %)

Host Traffic Stats

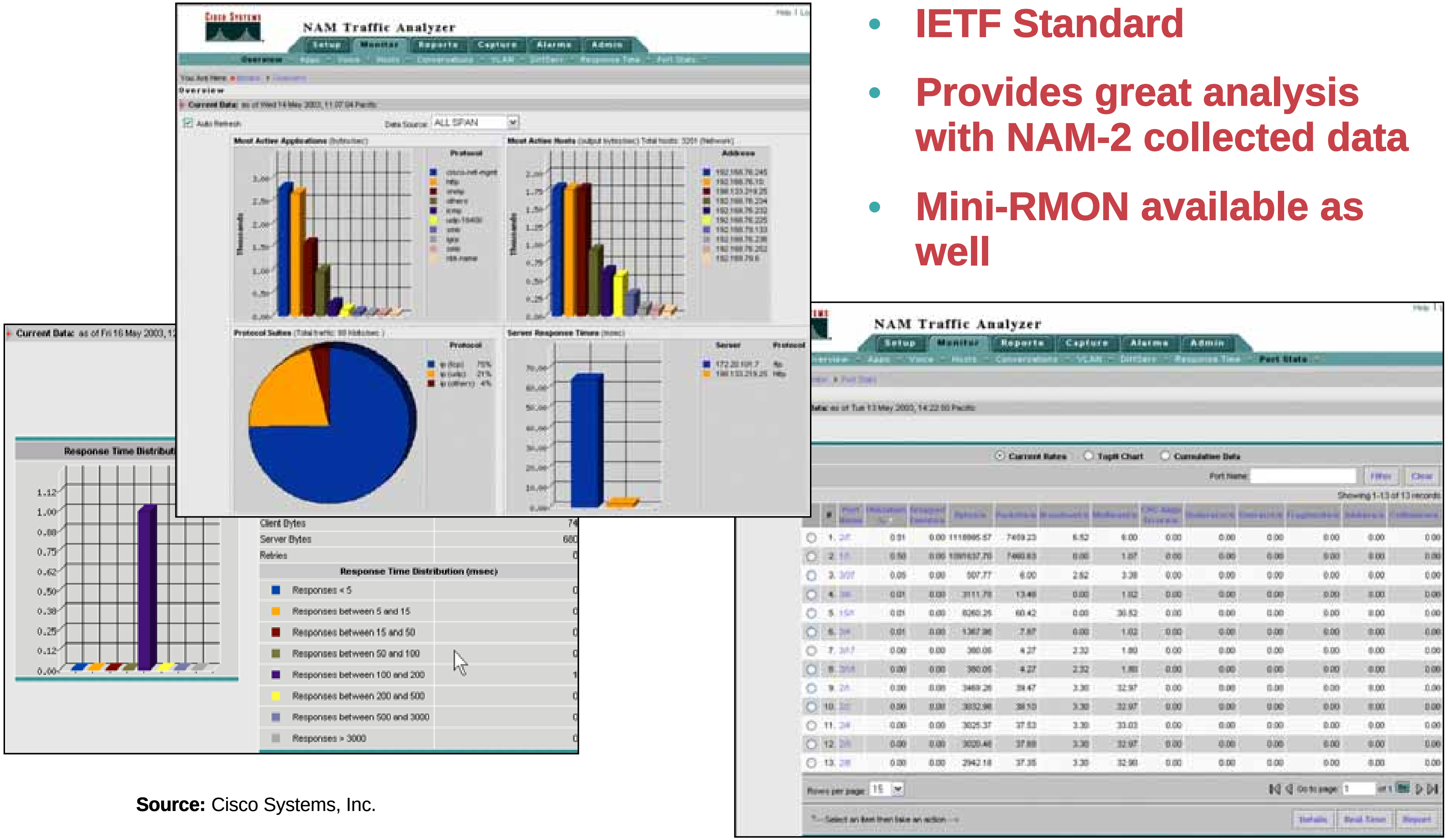
Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
Midnight - 1AM	0	0.0 %	0	0.0 %
1AM - 2AM	0	0.0 %	0	0.0 %
2AM - 3AM	0	0.0 %	0	0.0 %
3AM - 4AM	0	0.0 %	0	0.0 %
4AM - 5AM	0	0.0 %	0	0.0 %

Detailed Analysis i.e. TTL

Source: http://www.ntop.org

Value of RMON: Utilizing NAM-2 Gathered Data

- **IETF Standard**
- **Provides great analysis with NAM-2 collected data**
- **Mini-RMON available as well**



NAM Traffic Analyzer
Setup
Monitor
Reports
Capture
Alarms
Admin
Overview
Apps
Voice
Hosts
Conversations
VLAN
DiffServ
Response Time
Port Stats
Overview
Current Data: as of Wed 14 May 2003, 11:07:04 Pacific
Auto Refresh
Data Source: ALL SPAN
Most Active Applications (bytes/sec)
Most Active Hosts (output bytes/sec) Total hosts: 3201 (Network)
Protocol
Address
Thousands
Protocol Suites (Total traffic: 88 Kbits/sec)
Server Response Times (msec)
Server
Protocol
Current Data: as of Fri 16 May 2003, 1
Response Time Distribut
Current Rates
TopN Chart
Cumulative Data
Port Name:
Filter
Clear
Showing 1-13 of 13 records

Response Time Distribution (msec)	
Client Bytes	74
Server Bytes	680
Retries	0
🟦 Responses < 5	0
🟧 Responses between 5 and 15	0
🟥 Responses between 15 and 50	0
🟫 Responses between 50 and 100	0
🟪 Responses between 100 and 200	1
🟨 Responses between 200 and 500	0
▨ Responses between 500 and 3000	0
▨ Responses > 3000	0

	#	Port Name	Utilization %	Dropped Packets	Bytes/s	Packets/s	Broadcast/s	Multicast/s	CRC Align Errors/s	Undersize/s	Oversize/s	Fragments/s	Jabbers/s	Collisions/s
○	1.	[illegible]	0.51	0.00	1118885.57	7459.23	6.52	6.00	0.00	0.00	0.00	0.00	0.00	0.00
○	2.	[illegible]	0.50	0.00	1091637.75	7460.83	0.00	1.07	0.00	0.00	0.00	0.00	0.00	0.00
○	3.	[illegible]	0.05	0.00	507.77	6.00	2.52	3.38	0.00	0.00	0.00	0.00	0.00	0.00
○	4.	[illegible]	0.01	0.00	3111.78	13.48	0.00	1.02	0.00	0.00	0.00	0.00	0.00	0.00
○	5.	[illegible]	0.01	0.00	8260.25	60.42	0.00	30.52	0.00	0.00	0.00	0.00	0.00	0.00
○	6.	[illegible]	0.01	0.00	1367.98	7.87	0.00	1.02	0.00	0.00	0.00	0.00	0.00	0.00
○	7.	[illegible]	0.00	0.00	380.05	4.27	2.32	1.80	0.00	0.00	0.00	0.00	0.00	0.00
○	8.	[illegible]	0.00	0.00	380.05	4.27	2.32	1.80	0.00	0.00	0.00	0.00	0.00	0.00
○	9.	[illegible]	0.00	0.00	3469.28	39.47	3.30	32.97	0.00	0.00	0.00	0.00	0.00	0.00
○	10.	[illegible]	0.00	0.00	3032.98	38.10	3.30	32.97	0.00	0.00	0.00	0.00	0.00	0.00
○	11.	[illegible]	0.00	0.00	3025.37	37.53	3.30	33.03	0.00	0.00	0.00	0.00	0.00	0.00
○	12.	[illegible]	0.00	0.00	3020.46	37.88	3.30	32.97	0.00	0.00	0.00	0.00	0.00	0.00
○	13.	[illegible]	0.00	0.00	2942.18	37.35	3.30	32.90	0.00	0.00	0.00	0.00	0.00	0.00

Rows per page: 15

Go to page: 1 of 1

Select an item then take an action

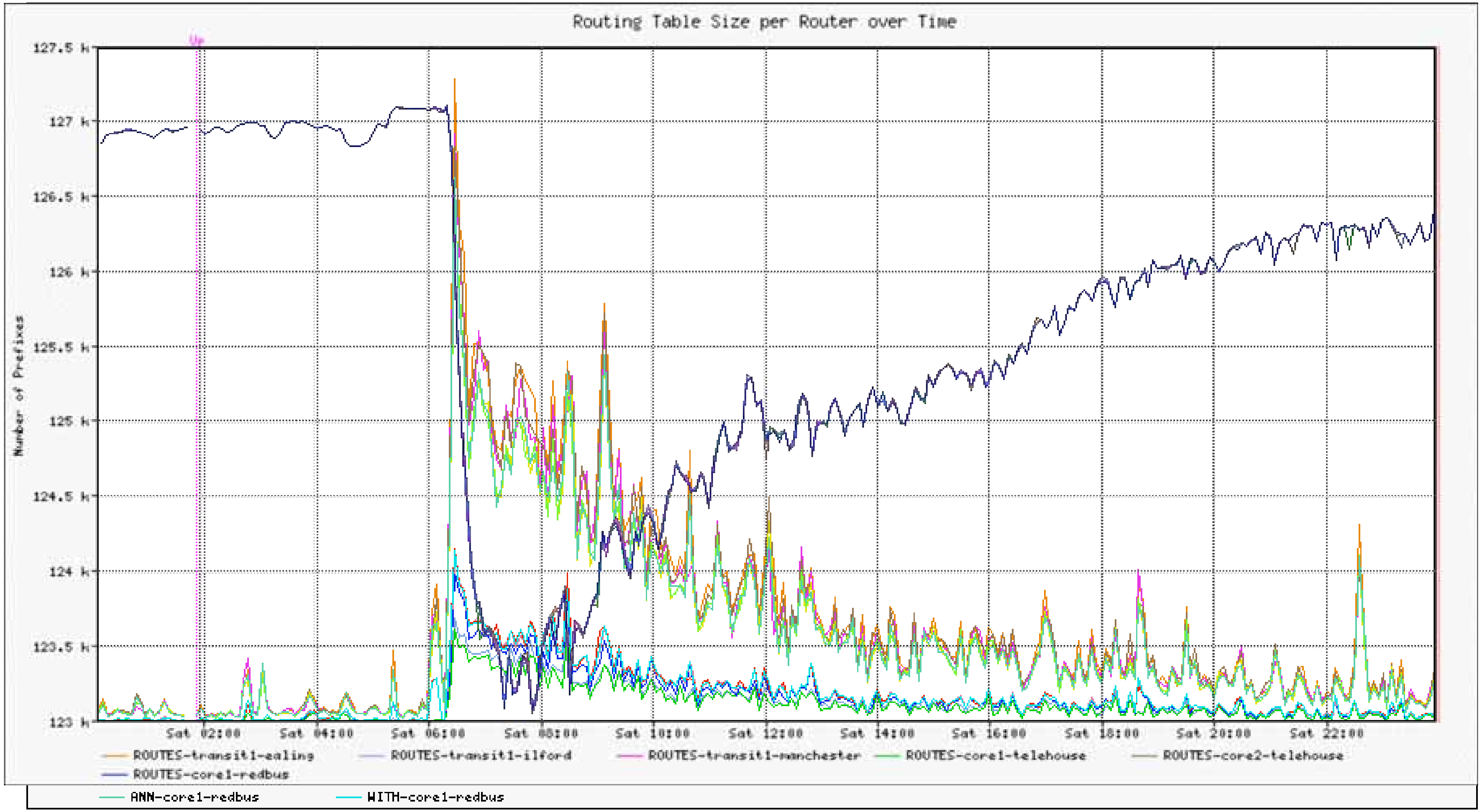
Details | Real-Time | Report

Source: Cisco Systems, Inc.

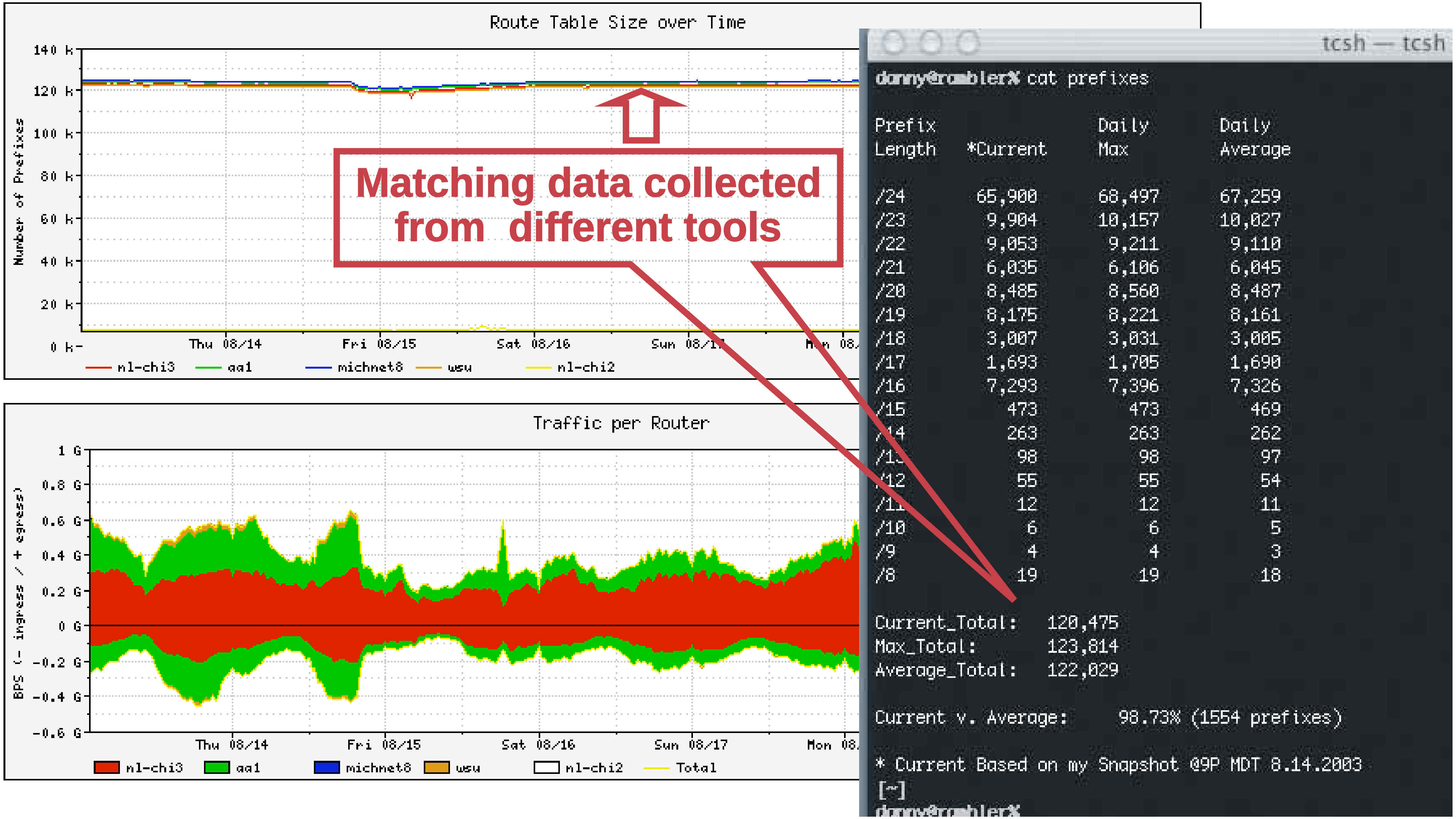
BGP—Why Do We Care?

- Large-scale network security events such as worms, DDoS attacks, etc. often produce side-effects visible in the global routing table
- Correlating BGP information with other forms of telemetry (NetFlow, SNMP, RMON, etc.) can be effective in determining the true impact of incidents

BGP Example—SQL Slammer



Correlating NetFlow and Routing Data



Matching data collected from different tools

```
dannyérambler% cat prefixes

Prefix                 Daily       Daily
Length    *Current     Max         Average

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

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

Current v. Average:      98.73% (1554 prefixes)

* Current Based on my Snapshot @9P MDT 8.14.2003
[~]
dannyérambler%
```

How to Deploy BGP?

- Start with open source tools: Zebra and Auagga
- Zebra (http://www.zebra.org) and Quagga (http://www.quagga.net) are two open source BGP daemons which can log BGP updates for further analysis
- Arbor Peakflow SP Traffic provides BGP visualization, trending, NetFlow traffic correlation, additional functionality (http://www.arbornetworks.com/products_sp.php)
- RIBs/updates available from http://archive.routeviews.org/, http://www.ripe.net/ris/index.html, http://www.renesys.com (commerical, useful monitoring tools/services for your ASN)

Syslog

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

Configuring Syslog on a Router

- Syslog data is invaluable

  Attack forensics

  Day to day events and debugging

- To log messages to a syslog server host, use the logging global configuration command

  ```
  logging host
  ```

  ```
  logging trap level
  ```

- To log to internal buffer use:

  ```
  logging buffered size
  ```

- Ensure timestamps

  ```
  service timestamps log…
  ```

Benefits of Deploying Syslog

- Syslog data can be available from a centralized SysLog server(s) as well as router's local buffer
- Deploy on routers, switches, firewall, IPS sensors and other network elements to get a holistic picture
- Analysis tools available such as Cisco MARS, SEC, ModLogAn and others
- SysLog Server such as Kiwi and syslog-ng

Network Time Protocol

- Synchronize time across all devices
- When security event occurs, data must have consistent timestamps

  From external time source

    Upstream ISP, Internet, GPS, atomic clock

  From internal time source

  Router can act as stratum 1 time source

```
ntp source loopback0
ntp server 10.1.1.1 source loopback0
```

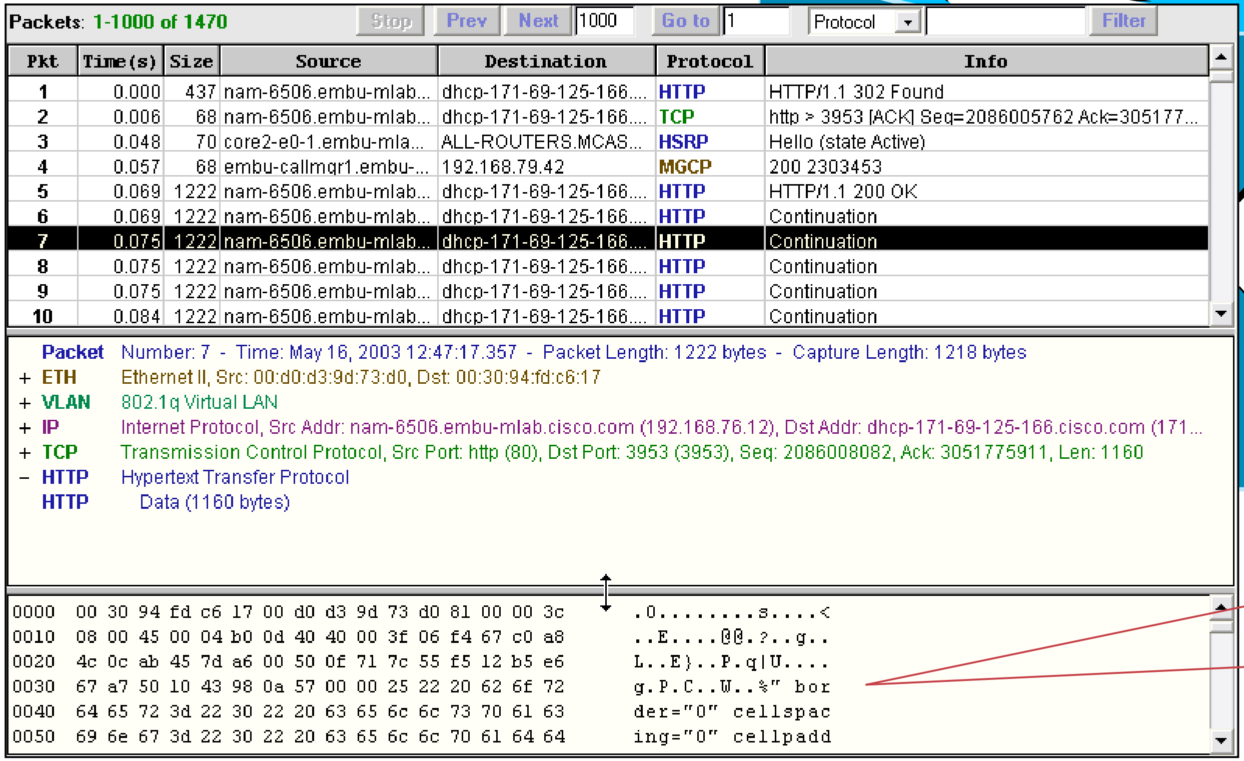
Benefits of Deploying NTP

- Very valuable on a global network with network elements in different time zones
- Easy to correlate data from a global or a sizable network with a consistent time stamp
- NTP based timestamp allows to trace security events for chronological forensic work
- Any compromise or alteration is easy to detect as network elements would go out of sync with the main 'clock'

Packet Capture

- Sometimes, there's just no substitute for looking at the packets on the wire
- SPAN/RSPAN/ERSPAN allow packet capture from Catalyst switches; ip packet export allows packet capture from routers
- Open source tools such as tcpdump, snoop, Ethereal (http://www.ethereal.com) on free *NIX or Windows allow inexpensive packet-capture solutions to be built and deployed
- Commercial tools such as Cisco NAM-2, NAI Sniffer/Distributed Sniffer, Wandel and Goltermann available
- Use macroanalytical telemetry such as SNMP, NetFlow, RMON to guide your use of microanalytical telemetry (i.e., packet capture)

Packet Capture Examples



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

```
  Packet  Number: 7 - Time: May 16, 2003 12:47:17.357 - Packet Length: 1222 bytes - Capture Length: 1218 bytes
+ ETH     Ethernet II, Src: 00:d0:d3:9d:73:d0, Dst: 00:30:94:fd:c6:17
+ VLAN    802.1q Virtual LAN
+ IP      Internet Protocol, Src Addr: nam-6506.embu-mlab.cisco.com (192.168.76.12), Dst Addr: dhcp-171-69-125-166.cisco.com (171...
+ TCP     Transmission Control Protocol, Src Port: http (80), Dst Port: 3953 (3953), Seq: 2086008082, Ack: 3051775911, Len: 1160
- HTTP    Hypertext Transfer Protocol
  HTTP      Data (1160 bytes)
```

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

Wealth of information, L1-L7 raw data for analysis

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

How to Use Packet Capture

- Mainly a reactionary tool
  - Generally a reaction after finding out that there is an anomaly
- Used in telemetry during the security event
  - Need to know where to capture the packet.
  - Sometimes, the same packet needs to be captured in multiple places
- Wealth of information
  - Informs what type of outbreak one is observing on the network
  - Provides raw data for further analysis
  - Helps by providing information on how to bring the safeguards for short term and long tem mitigation

Okay—Tell Me Where to Start From?

1. NetFlow enablement on the network elements
2. NetFlow data correlation and analysis
3. SNMP / RMON [SNMP more prevalent]
    1. CPU / Memory util
    2. Link usage and display with MRTG
4. SysLog collection and analysis
5. Monitoring to Routing, DNS queries, etc. [BGP, DNS]
6. Local and remote packet capture facility [Most have it today with sniffer, ethereal]

The Next Steps-
Best Practice Techniques

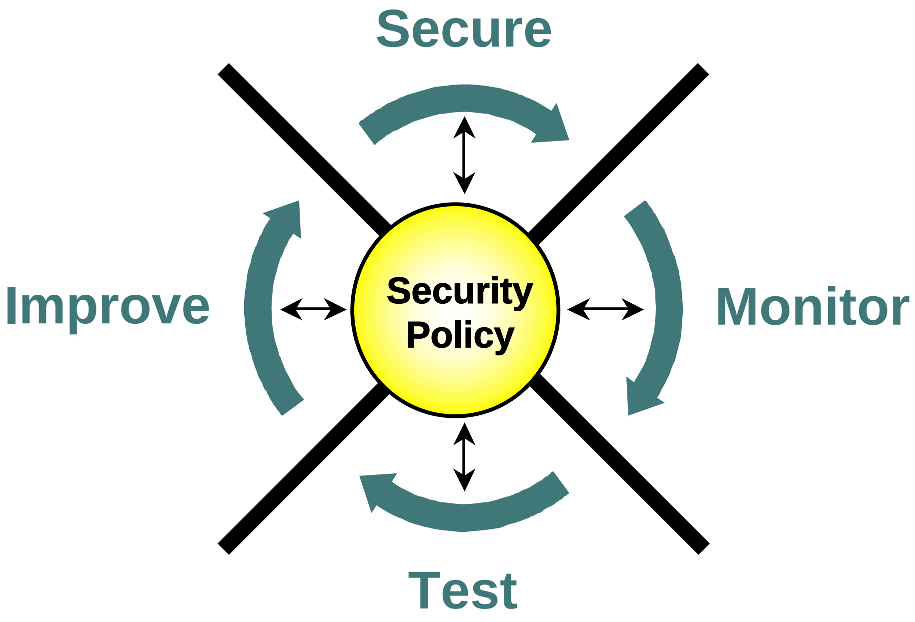
SP network security system cycle

Stage 1: Secure

Stage 2: Monitor

Stage 3: Test

Stage 4: Improve



Security Best Practices - Overview

- **Define a Security Policy and the required procedures to enforce it**

  this should include roles, responsibilities, customer contacts, etc.

- **Create an Incident Response Team**

  should work in conjunction with the NOC/SOC

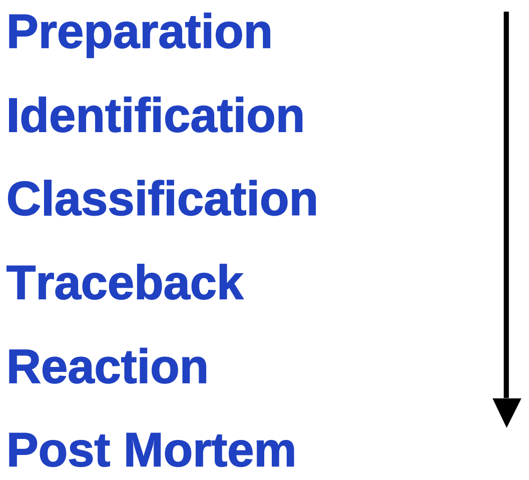
- **Establish a Relationship with other relevant organizations**

  PSIRTs, CERTs, NSPs, and peering SPs

Security Best Practices – Overview (cont’)

- Design and Implement Services with Security in mind
- Secure the infrastructure following a Modular design

  Focus on the most critical areas first
- Define a solid incident handling Procedure



Preparation

Identification

Classification

Traceback

Reaction

Post Mortem

Procedure : Preparation

- **Know the enemy**
  - Understand what drives the miscreants
  - Understand their techniques
- **Create the security team and plan**
  - Who handles security during an event? Is it the security folks? The networking folks?
  - A good operational security professional needs to be a cross between the two: silos are useless…
- **Harden the devices**
- **Prepare the tools**
  - Network telemetry
  - Reaction tools
  - Understand performance characteristics

Prepare Response Teams

- Identify key individuals/groups and create an incident response team

- Participate in and communicate to incident response forums and organizations

    FIRST

    NSP-SEC

    NANOG

    PSIRT

- Monitor emerging threats

    http://packetstormsecurity.org

    http://isc.sans.org

    Many others…

Preparing the Network

- Understanding your network is critical to preparation
- What is normal? What is healthy?
- Monitor important indexes
  - Bandwidth—peer, router, interface, application
  - Routing—hijacking, instability
  - CPU—punted traffic, “show ip traffic”
  - Traffic patterns—by AS, prefixes, ports

Preparing the Network

Harden the Network

- Secure the control plane

  Routing protocol authentication, BGP TTL check, prefix-filtering

- Secure the management plane

  Disable unnecessary services

  Secured and authenticated device access – AAA, VTY/SNMP ACL's, Out-of-band management

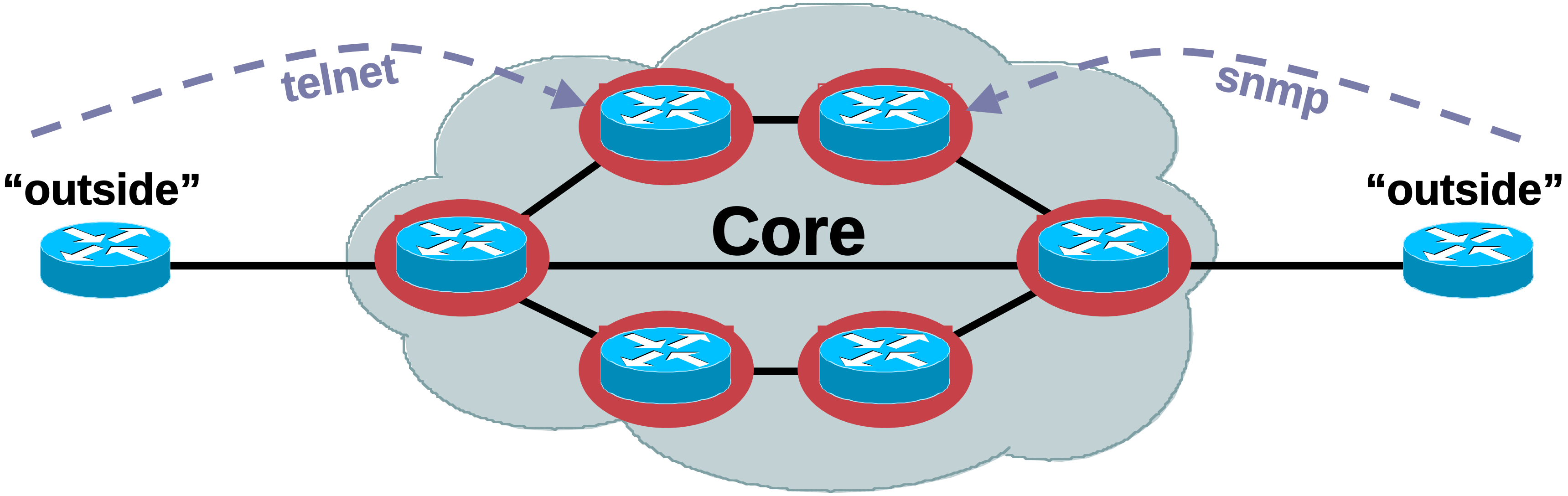
- Secure the data plane

  Anti-spoofing via strict/loose uRPF, infrastructure ACL's

- Auditing

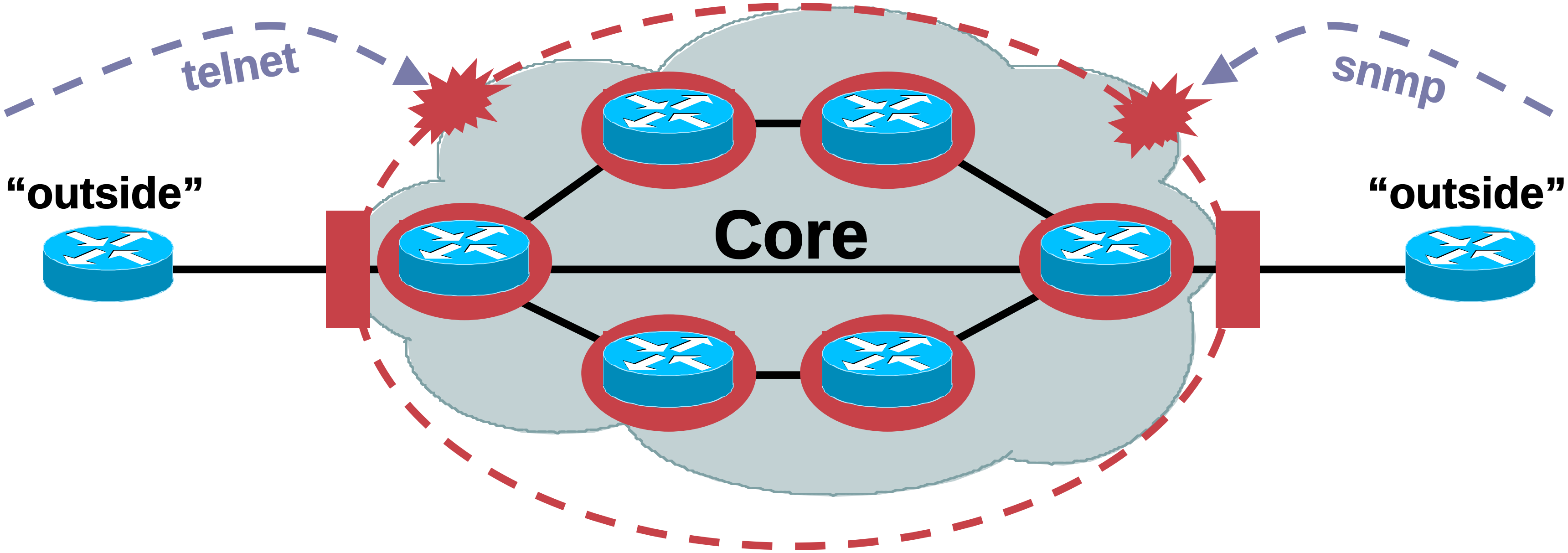
  Logging, AAA records, SNMP traps

The Old World: Network Edge



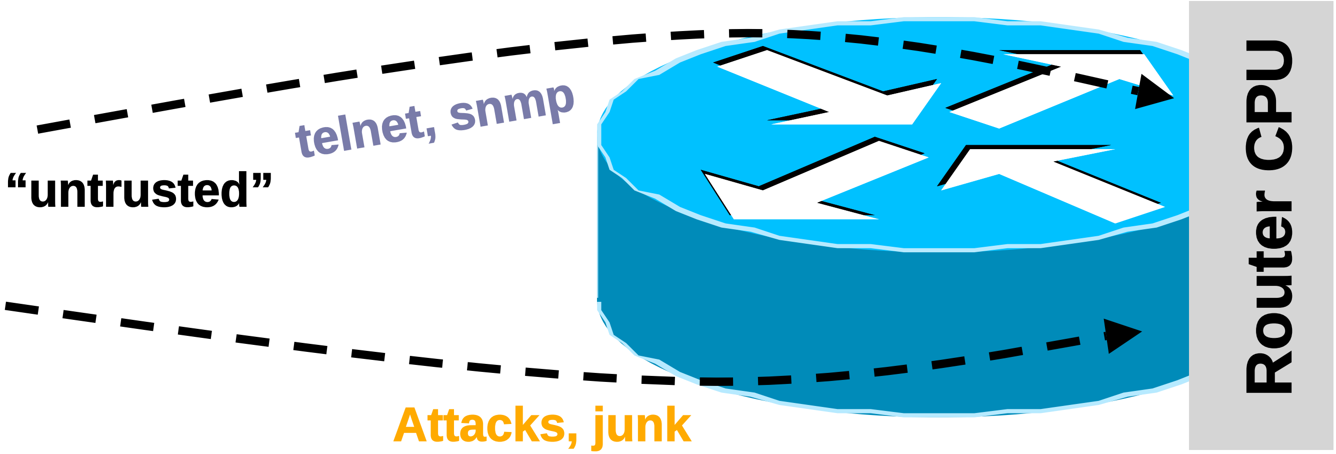
- Core routers individually secured
- Every router accessible from outside

The New World: Network Edge



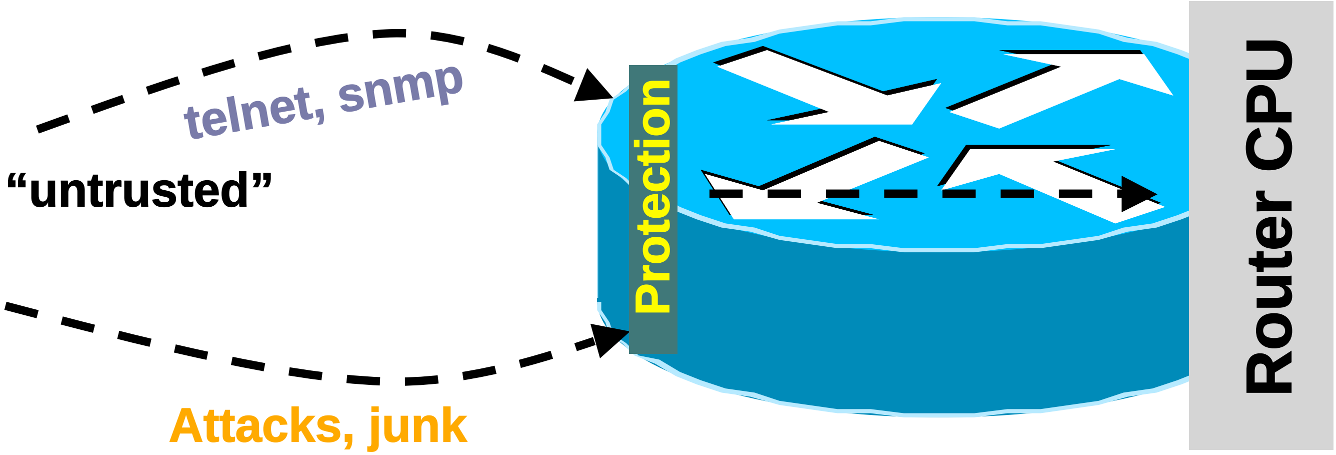
- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

The Old World: Router Perspective



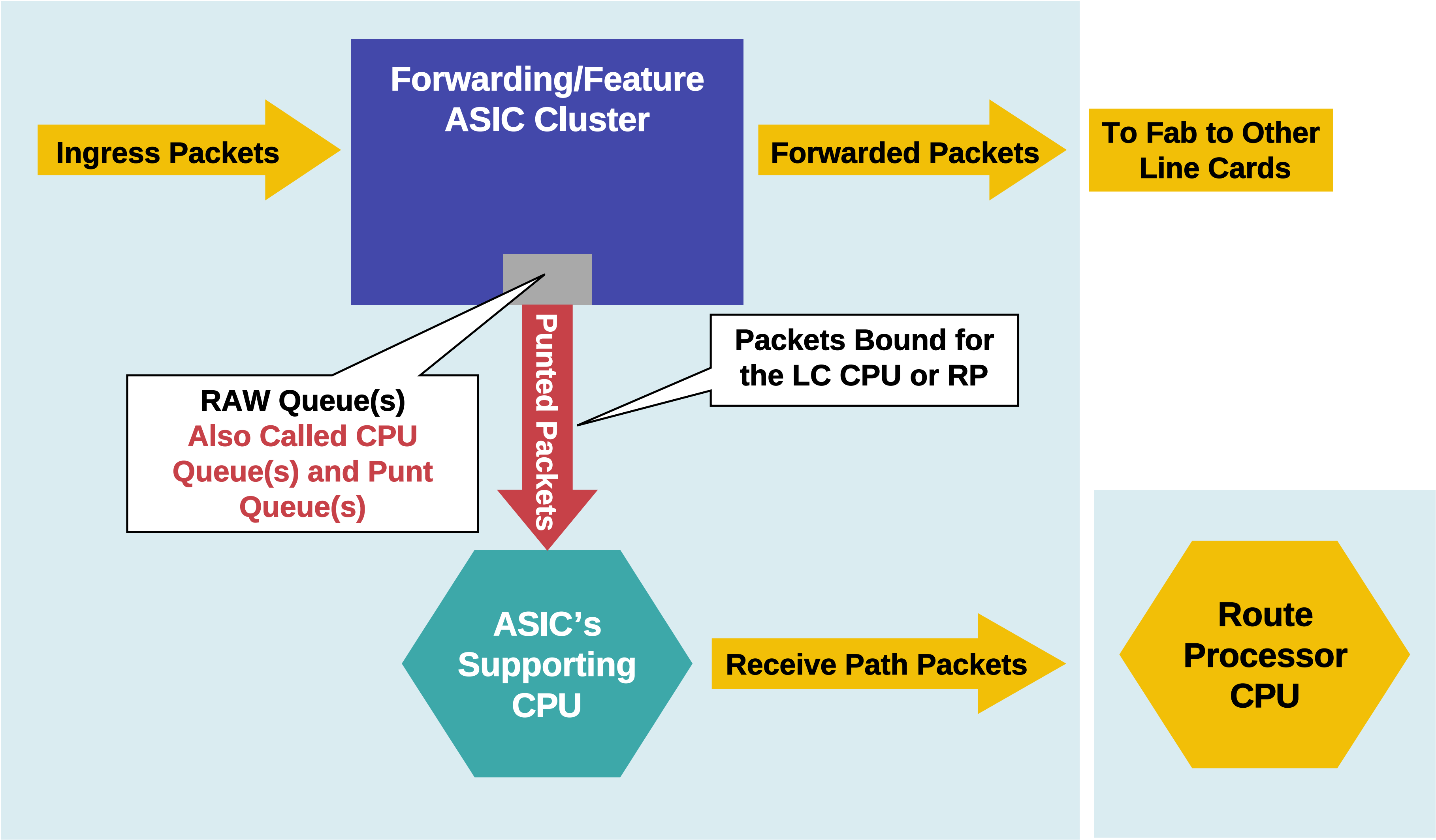
- Policy enforced at process level (VTY ACL, SNMP ACL, etc.)
- Some early features such as ingress ACL used when possible

The New World: Router Perspective

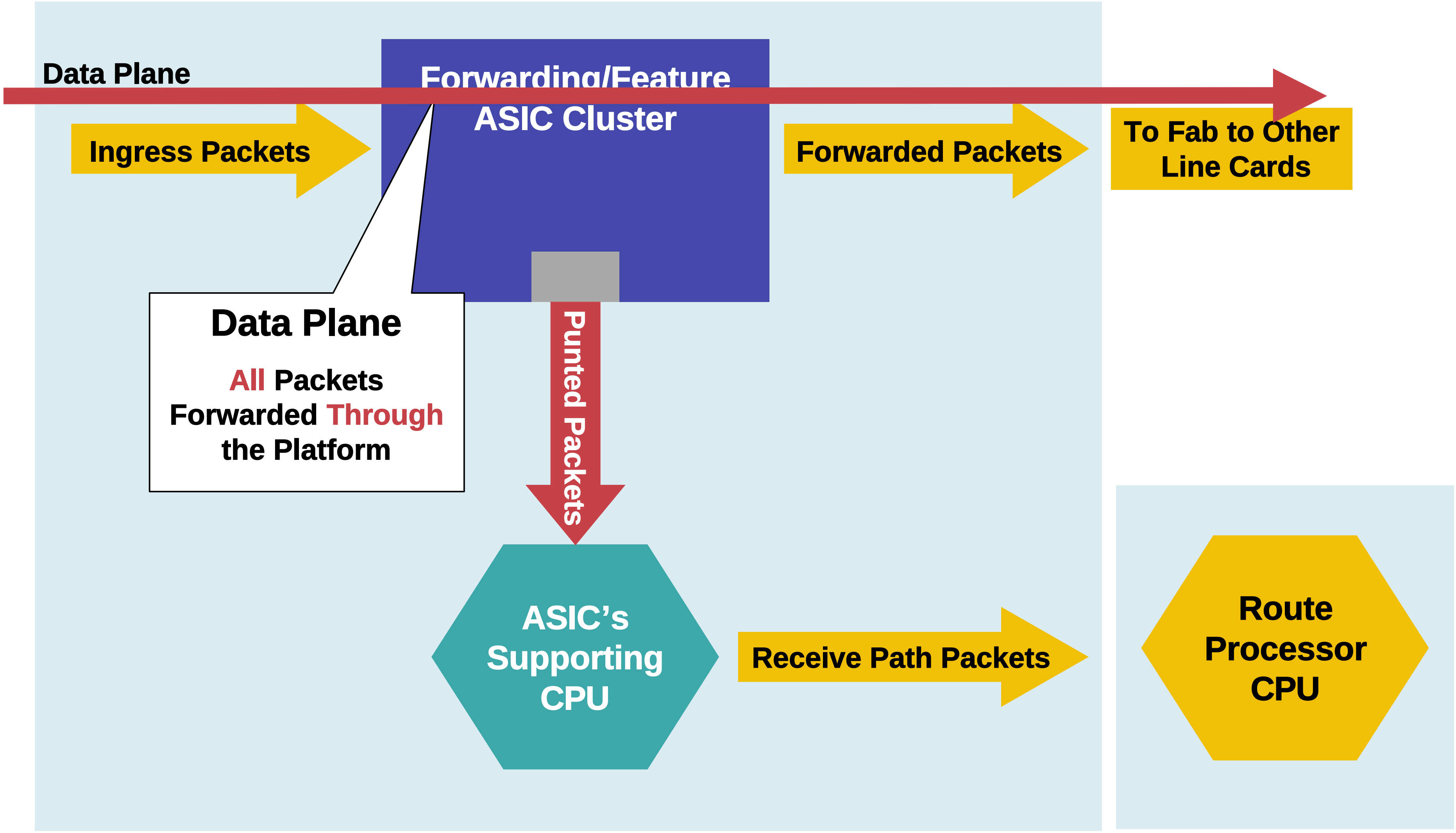


- **Central policy enforcement, prior to process level**
- **Granular protection schemes**
- **On high-end platforms, hardware implementations**

ASIC-Based Platform: Main Components


Forwarding/Feature ASIC Cluster
Ingress Packets
Forwarded Packets
To Fab to Other Line Cards
Punted Packets
Packets Bound for the LC CPU or RP
RAW Queue(s)
Also Called CPU Queue(s) and Punt Queue(s)
ASIC's Supporting CPU
Receive Path Packets
Route Processor CPU

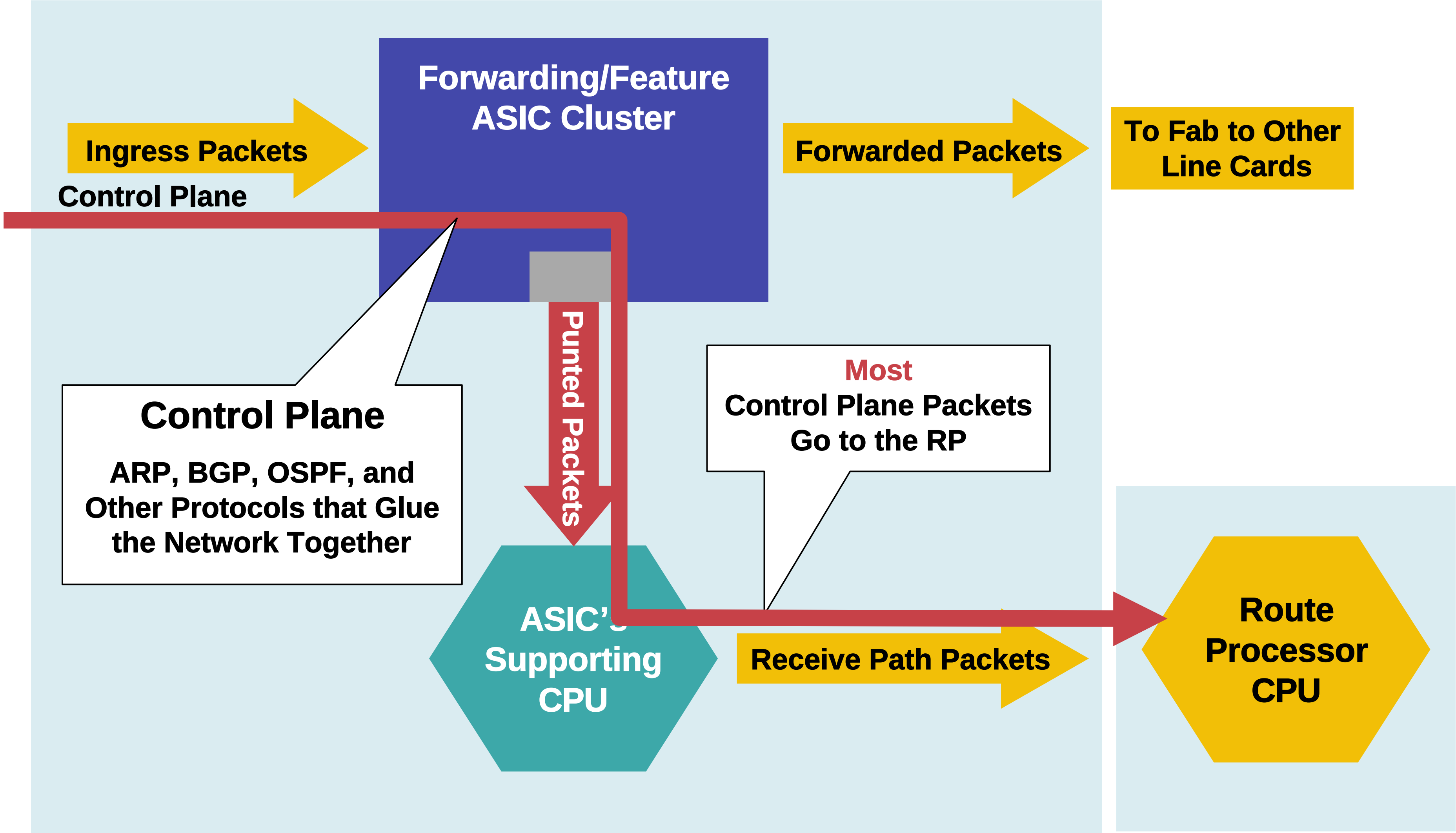
Data Plane



Data Plane

All Packets Forwarded Through the Platform

Control Plane

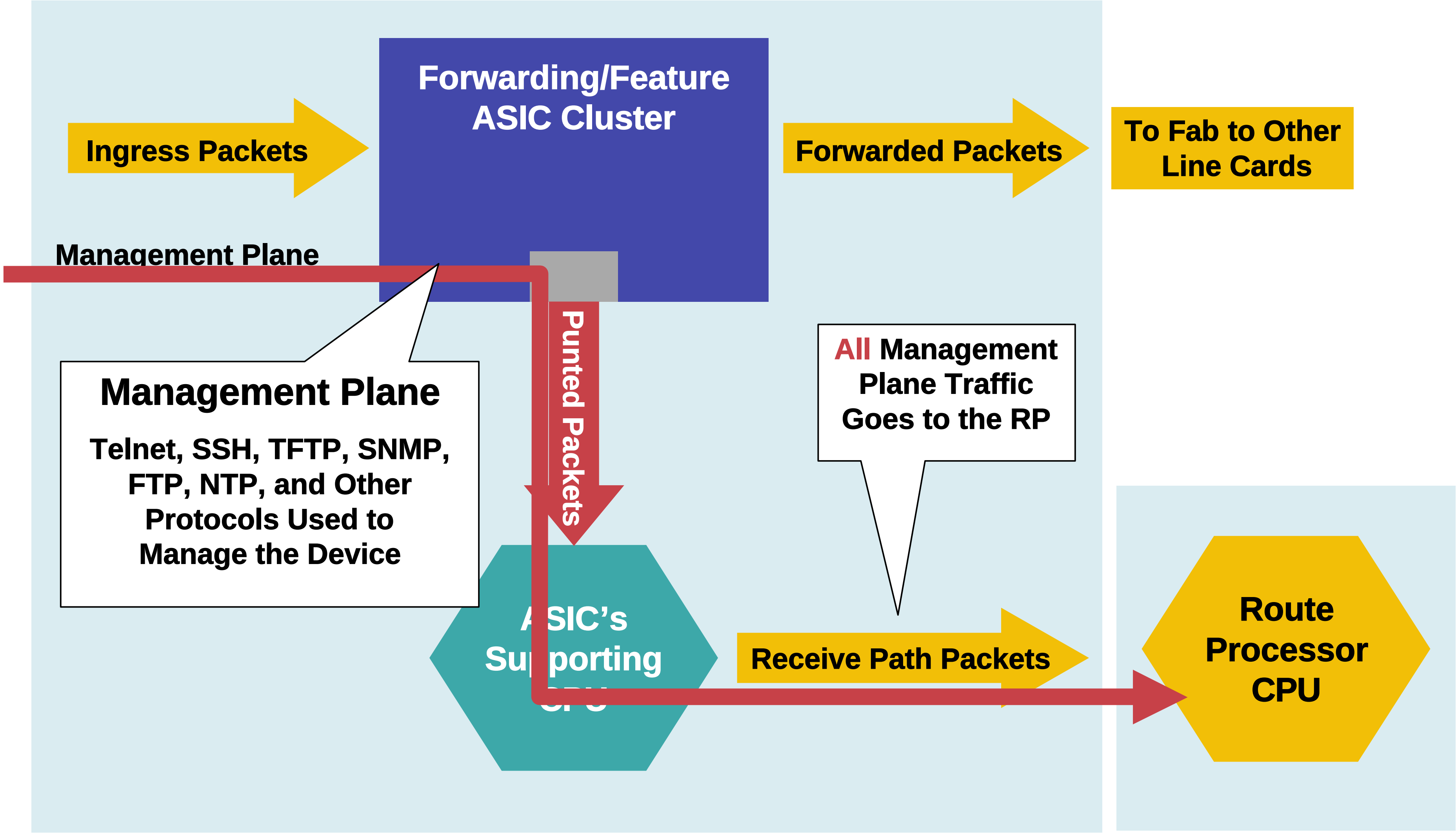


Control Plane

ARP, BGP, OSPF, and Other Protocols that Glue the Network Together

Most Control Plane Packets Go to the RP

Management Plane

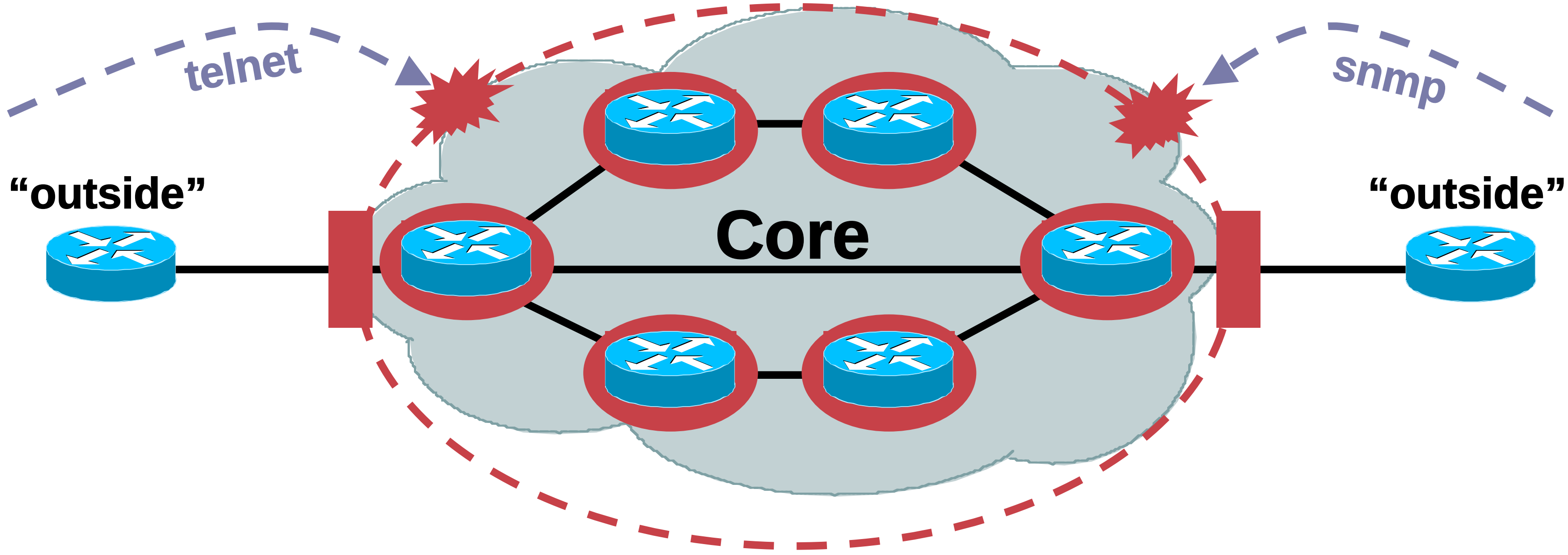


Management Plane

Telnet, SSH, TFTP, SNMP, FTP, NTP, and Other Protocols Used to Manage the Device

All Management Plane Traffic Goes to the RP

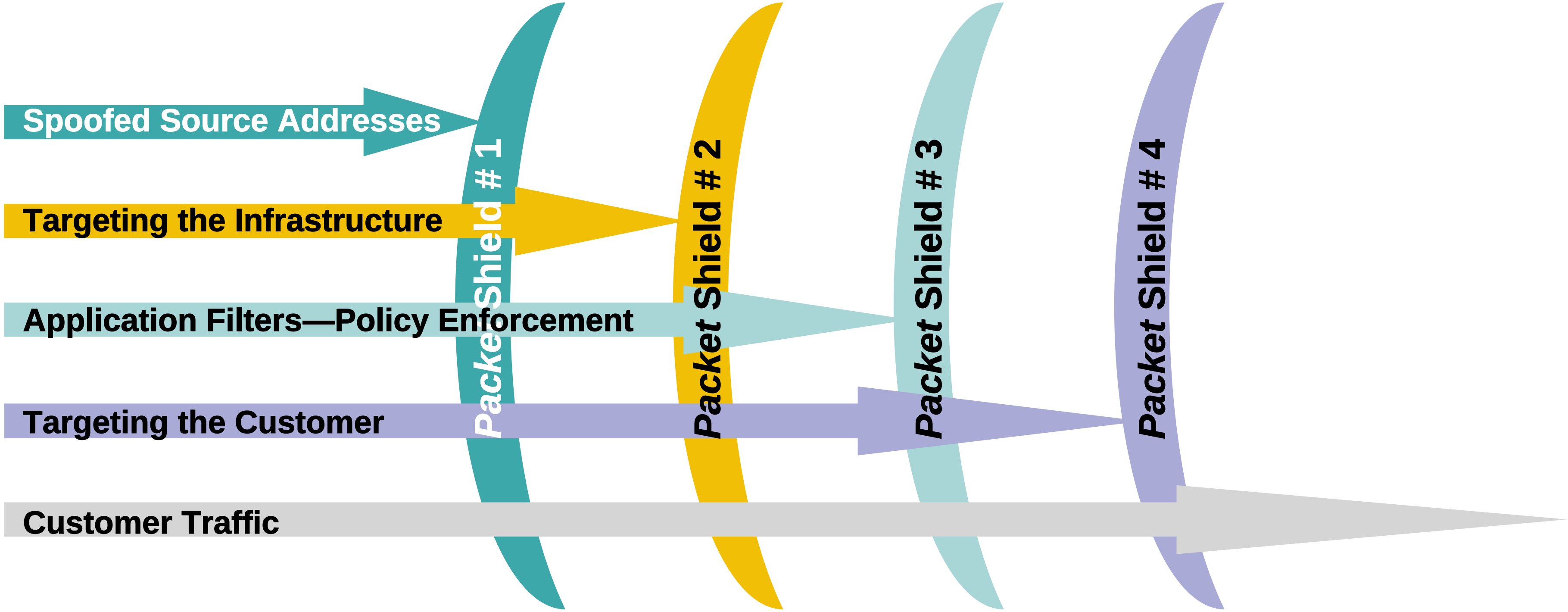
Preparing the Network—Infrastructure Protection



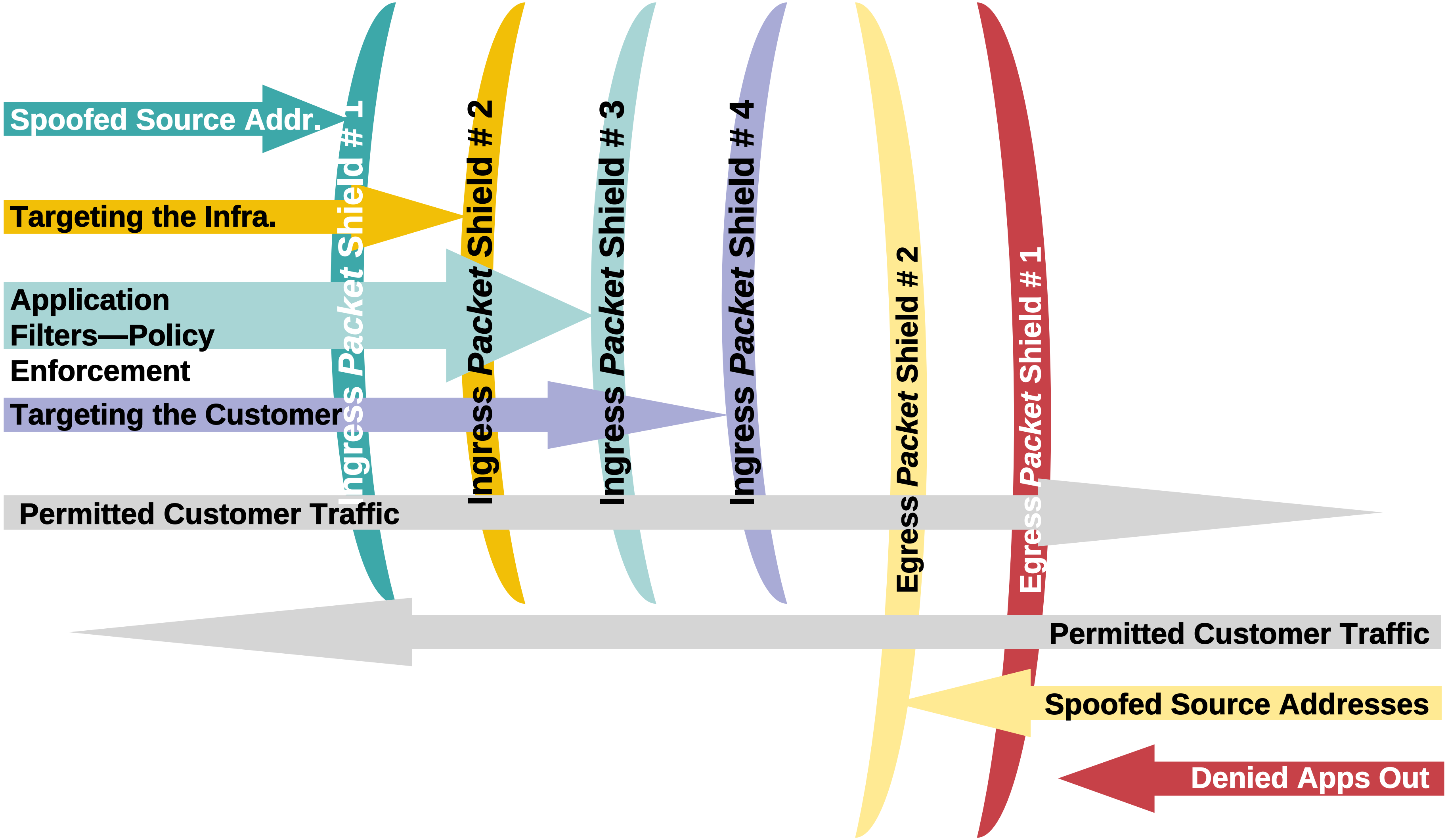
- **Techniques to secure your transit networks**

  Infrastructure ACLs, Receive ACLs, Control Plane Policing

Packet Filtering Viewed Horizontally



Packet Filtering
Remember to Filter the Return Path


Spoofed Source Addr.
Targeting the Infra.
Application Filters—Policy Enforcement
Targeting the Customer
Permitted Customer Traffic
Ingress *Packet* Shield # 1
Ingress *Packet* Shield # 2
Ingress *Packet* Shield # 3
Ingress *Packet* Shield # 4
Egress *Packet* Shield # 2
Egress *Packet* Shield # 1
Permitted Customer Traffic
Spoofed Source Addresses
Denied Apps Out

Infrastructure Protection Tools

- Infrastructure ACLs (iACLs)—Originally, the only approach
  - Create policies (ACLs or MQC) for control plane traffic to block all unwanted IP traffic destined to the core
  - Applied to ALL ingress port—affects ALL traffic (control and data plane)
- Receive Path ACLs (rACLs)—The first step…
  - Create ACLs to block unwanted IP traffic destined to the core
  - Global (single) configuration affects all “receive path” packets
  - Only affects control plane traffic
  - Only available for Cisco 12000 and Cisco 7500 routers
- Control Plane Policing (CoPP)—The newest approach
  - Extends rACLs by adding Modular QoS CLI (MQC) policing
  - Modify input path to “split” control and data plane traffic prior to input feature application

Old

New

Control Plane Policing Deployment Policies

Define Service Policy

- Start with a simplistic policy that will not disrupt network operations

  For critical, important, and normal traffic types, conform actions are "transmit"

  For undesirable traffic, all actions are unconditionally "drop" regardless of rate

  For default traffic, rate-limit the amount of traffic permitted above a certain bps

- Modify the policy over time as more confidence is gained in traffic rates—particularly for "critical" traffic

  A very low rate might discard necessary traffic, whereas a high rate might allow the Route Processor to be inundated with a flood of non-critical packets

Example Only

  The appropriate rates are dependent on platform capabilities and CPU capacity

  The appropriate rates are typically site-specific as well, depending on local topology and routing table size

- Strive for constant improvement to keep pace with new attacks, and to cover new services

Basic Control Plane Policing Service Policy

Traffic Class	Rate (bps)	Conform Action	Exceed Action
Critical	N/A	Transmit	Transmit
Important	125,000	Transmit	Transmit
Normal	15,000	Transmit	Transmit
Undesirable	8,000	Drop	Drop
Default	8,000	Transmit	Drop

Hybrid Control Plane Policing Service Policy

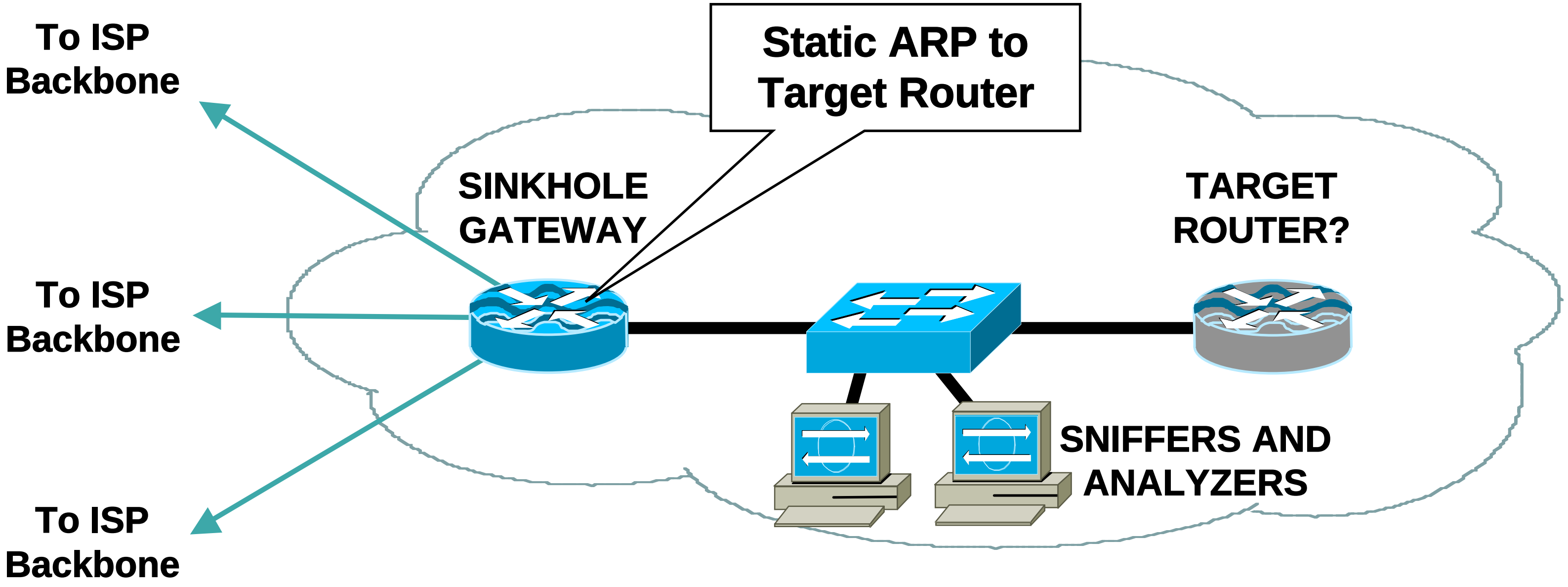
Traffic Class	Rate (bps)	Conform Action	Exceed Action
Critical	N/A	Transmit	Transmit
Important	125,000	Transmit	Drop
Normal	15,000	Transmit	Drop
Undesirable	8,000	Drop	Drop
Default	8,000	Transmit	Drop

Prepare the Tools

Sinkholes

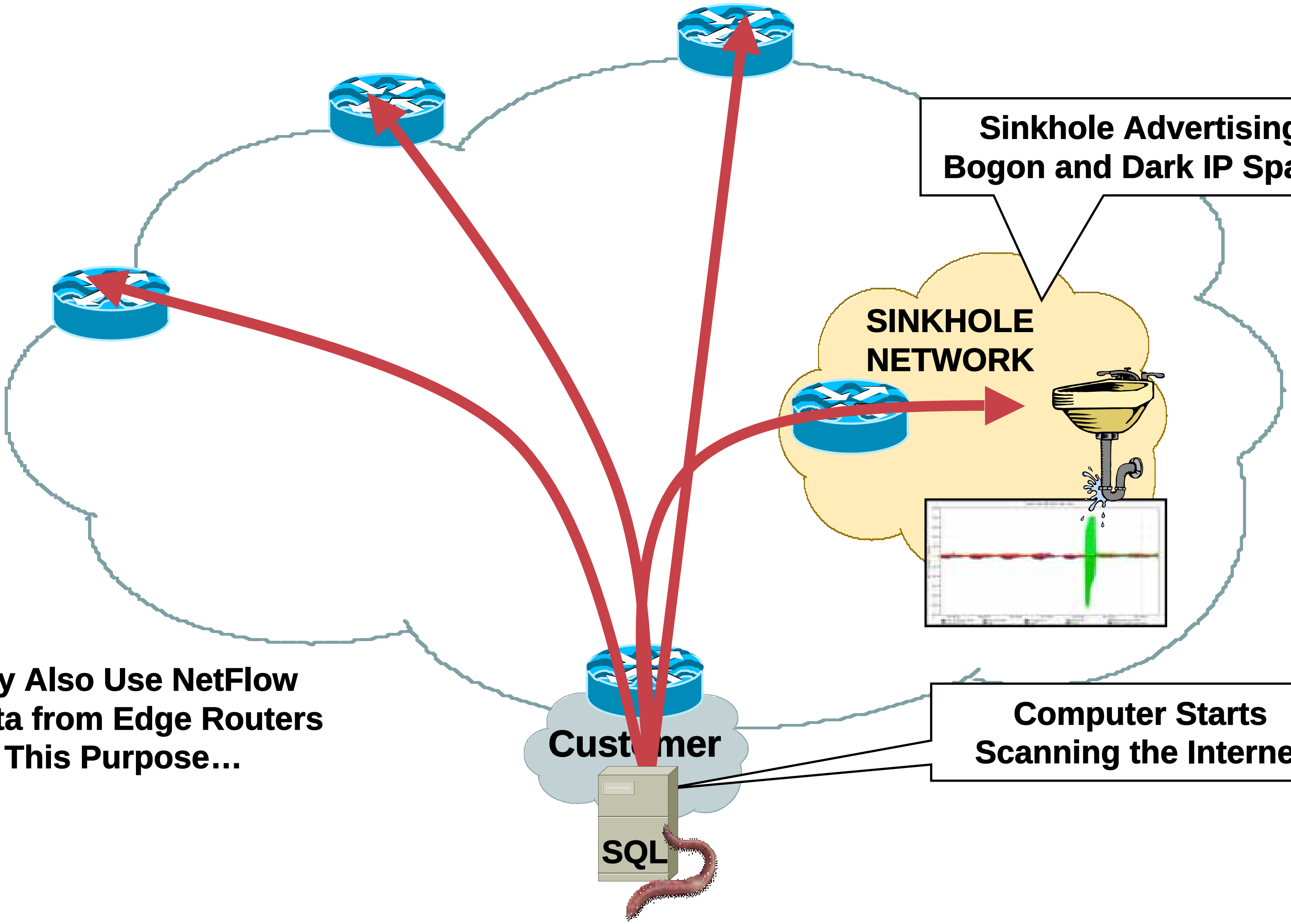
- Sinkholes are a versatile function of routing topology and hardened infrastructure
- Infrastructure protection
  - Sinkhole your core address space to minimize attack
- Identification/classification
  - Monitor dark IP space for attack noise and worm/botnet scanning
  - Redirect attacks for analysis
- Traceback
  - Use backscatter to trace spoofed hosts
- Reaction
  - Divert attacks from the victim

Sink Hole Architecture



- **Dedicated network component to attract traffic**
- **Can also be used "on demand": Pull the DoS/DDoS attack to the sinkhole**
- **Sink Hole design can also incorporate scrubbers**

Sinkholes: Worm Detection

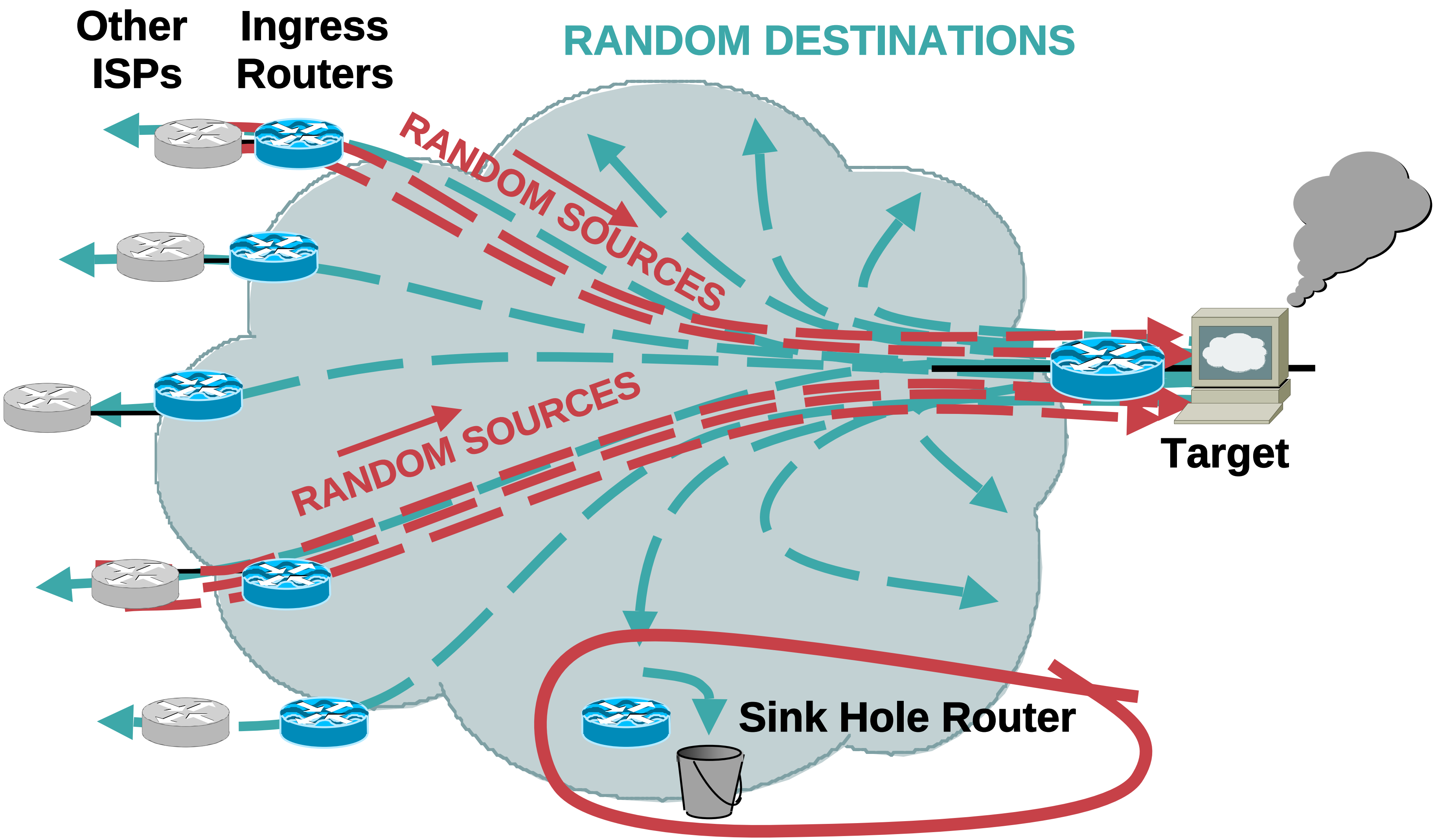


Sinkhole Advertising Bogon and Dark IP Space

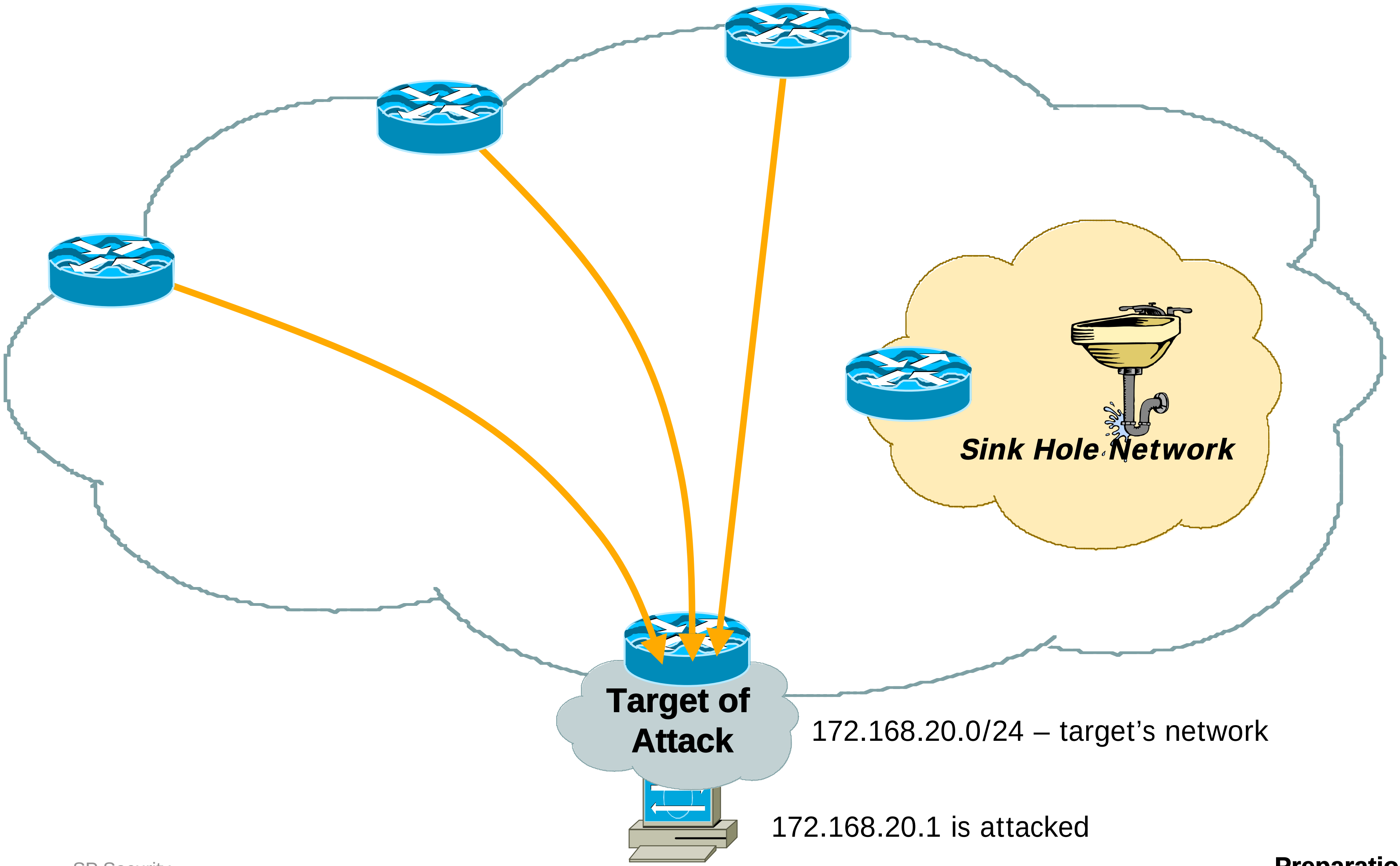
Computer Starts Scanning the Internet

May Also Use NetFlow Data from Edge Routers for This Purpose…

Backscatter Analysis of Attack Noise



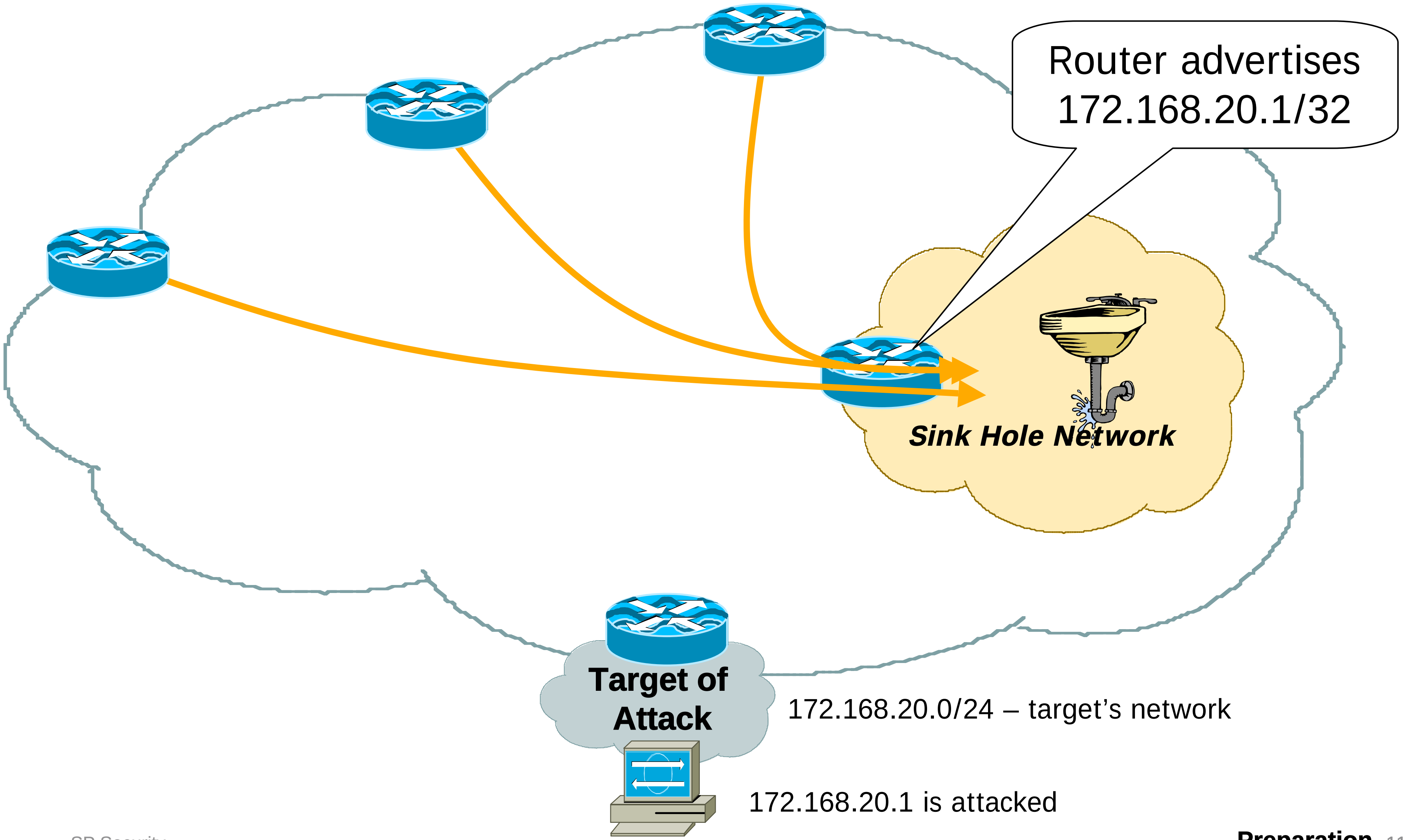
Sink Hole Routers/Networks



172.168.20.0/24 – target's network

172.168.20.1 is attacked

Sink Hole Routers/Networks



Router advertises 172.168.20.1/32

172.168.20.0/24 – target's network

172.168.20.1 is attacked

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!

Changes to Network Baselines

- SNMP data
- Unexplained changes in link utilization

    Worms can generate a lot of traffic, sudden changes in link utilization can indicate an attack or a worm

- Unexplained changes in CPU utilization

    Attack/Worm scans can affect routers/switches resulting in increased CPU both process and interrupt switched

- Unexplained syslog entries
- These are examples

    Changes don’t always indicate an attack/worm!

    Need to know what’s normal to identify abnormal behavior

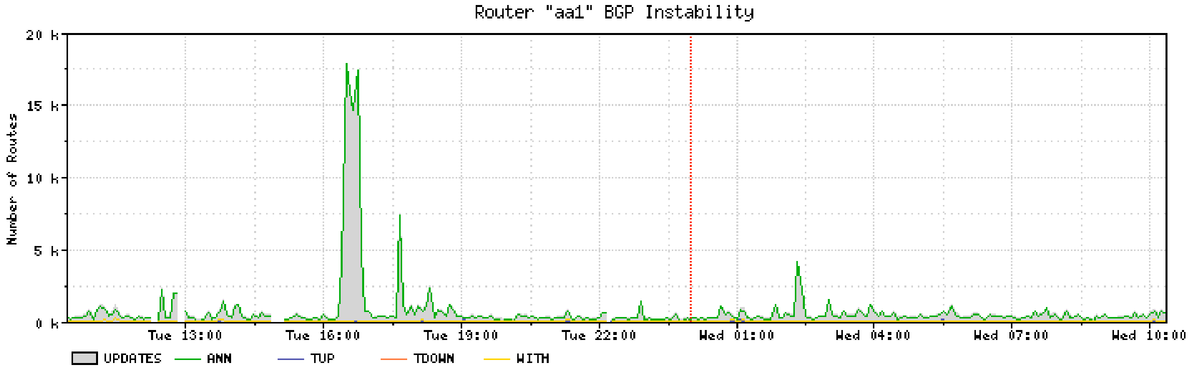
Ways to Identify DoS Attacks

- Customer/End User call
- SNMP: Line/CPU overload, drops
- NetFlow: Counting flows
- ACLs with logging
- Backscatter
- Sniffers
- Anomaly Detector

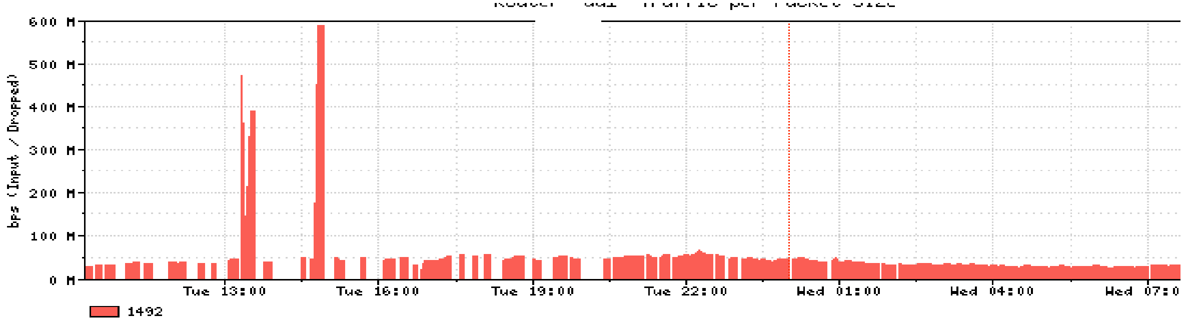
Identification Examples

Cisco.com

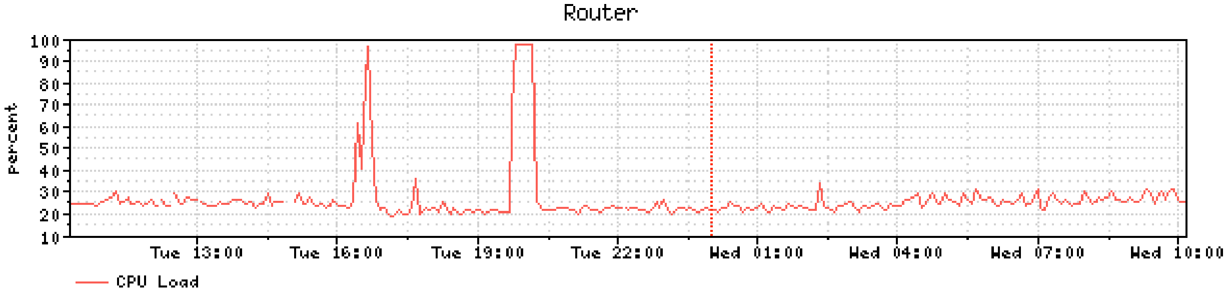
BGP Flaps



Packet Size



CPU



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 a 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)?

Ways to Classify DoS Attacks

- **NetFlow: Flow information**
- **ACLs (maybe with logging)**
- **Backscatter**
- **Sniffers**
- **Anomaly Detector**

Classifying DoS with ACLs

- Requires ACLs to be in place (for detection)

```
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)
```

Found:
- Attack type
- Interface

Looks Like Smurf Attack

- Watch performance impact
- Used on demand, not pro-active
- More used for checking than for detection
- Some ASIC based LCs do not show counters

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
  - Packet accounting
  - IP Source
- Retain attack data
  - Use to correlate inter-domain traceback
  - Required for prosecution
  - Deters future attacks
  - Clarify billing and other disputes
  - Post Mortem Analysis

Tracing DoS Attacks

- **Non-spoofed: Technically trivial (IRR)**

  But: Potentially tracing 100's of sources…

- **Spoofed:**

  IP Source Tracker: router by router

  **NetFlow:
  Automatic if analysis tools are installed
  Manually: Router by router**

  **ACLs:
  Has performance impact on some platforms
  Mostly manual: Router by router**

  **Backscatter technique:
  One step, fast, only for spoofed sources**

The Internet Routing Registry (IRR): Network Info

```
madrid% whois -h whois.arin.net  64.103.0.0

OrgName:            Cisco Systems, Inc.
OrgID:              CISCOS-2
Address:            170 West Tasman Drive
City:               San Jose
StateProv:          CA
PostalCode:         95134
Country:            US

NetRange:           64.100.0.0 - 64.104.255.255
CIDR:               64.100.0.0/14, 64.104.0.0/16
 [...]
TechHandle:         CAH5-ARIN
TechName:           Huegen, Craig
TechPhone:          +1-408-526-8104
TechEmail:          chuegen@cisco.com

OrgTechHandle:      DN5-ORG-ARIN
OrgTechName:        Cisco Systems, Inc.
OrgTechPhone:       +1-408-527-9223
OrgTechEmail:       dns-info@cisco.com
```

- **Europe: whois.ripe.net**
- **Asia-Pac: whois.apnic.net**
- **USA and rest: whois.arin.net**

Contact Information

The Internet Routing Registry (IRR): AS Info

```
madrid% whois -h whois.arin.net    as109

OrgName:            Cisco Systems, Inc.
OrgID:              CISCOS-2
Address:            170 West Tasman Drive
City:               San Jose
StateProv:          CA
PostalCode:         95134
Country:            US

ASNumber:           109
ASName:             CISCOSYSTEMS
ASHandle:           AS109
 […]
TechHandle:         MRK4-ARIN
TechName:           Koblas, Michelle
TechPhone:          +1-408-526-5269
TechEmail:          mkoblas@cisco.com

OrgTechHandle:      DN5-ORG-ARIN
OrgTechName:        Cisco Systems, Inc.
OrgTechPhone:       +1-408-527-9223
OrgTechEmail:       dns-info@cisco.com
```

- **Europe: whois.ripe.net**
- **Asia-Pac: whois.apnic.net**
- **USA and rest: whois.arin.net**

Also, if domain known: abuse@domain

Tracing Back with Netflow

- Routers need Netflow enabled

Victim

```
router1#sh ip cache flow | include <destination>
Se1        <source>     Et0        <destination>    11 0013 0007   159
.... (lots more flows to the same destination)
```

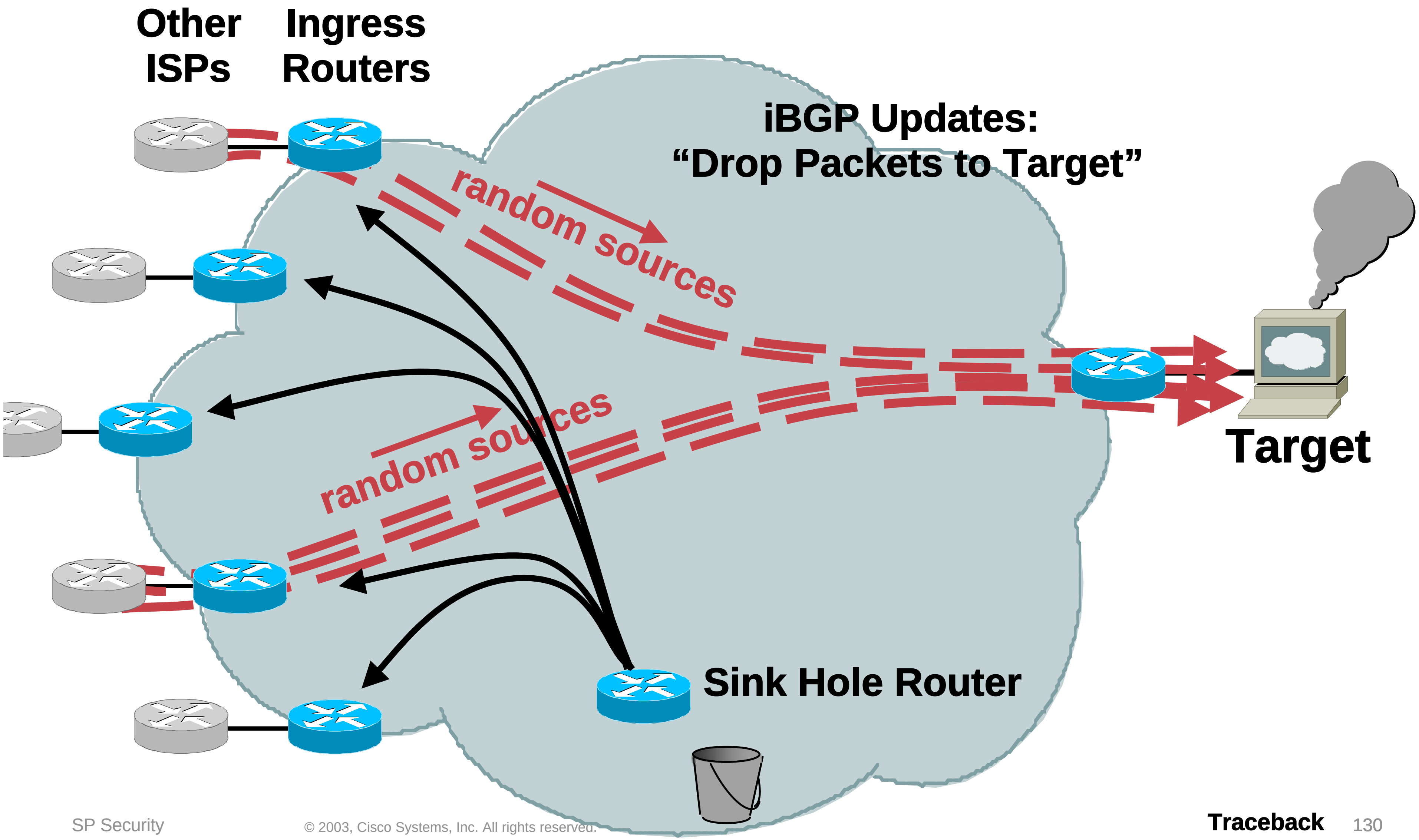
The flows come from serial 1

Find the upstream router on serial 1

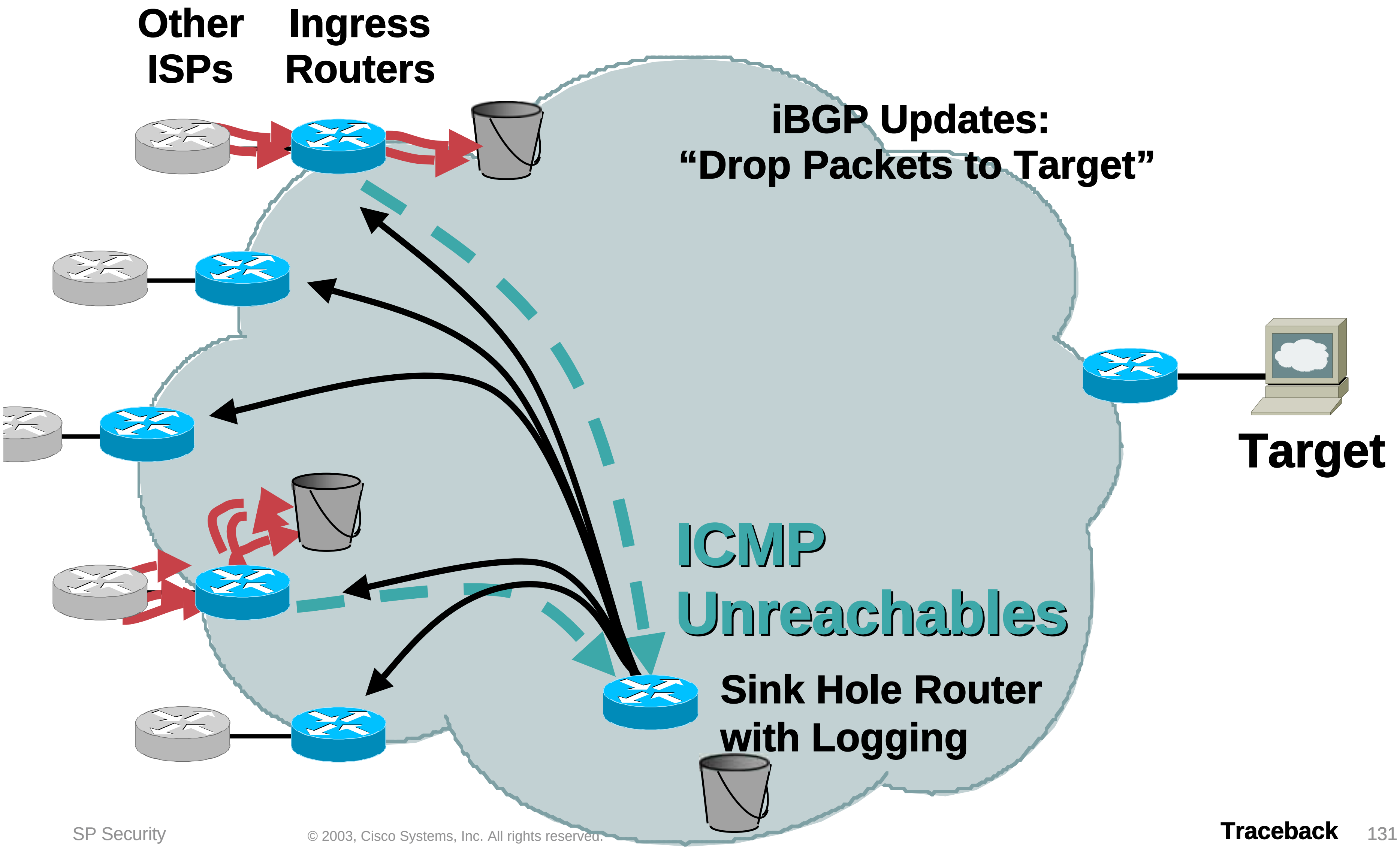
```
router1#sh ip cef se1
Prefix             Next Hop           Interface
0.0.0.0/0          10.10.10.2         Serial1
10.10.10.0/30      attached           Serial1
```

Continue on this router

Trace-Back in One Step: ICMP Backscatter



Trace-Back in One Step: ICMP Backscatter



Reaction - Incident Response Principles

1. Don’t Panic!
2. Use A Mitigation Methodology.
3. Do not make drastic changes to the network while the attack/worm is rampant.

ISP 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 ISP Security Teams have demonstrated six distinct phases in the way ISPs response to security incidents.

Capacity as a Solution

- **To many sorts of attacks, a common solution is to add more capacity**
- **Not every problem gets solved this way**

  Think about collateral damage
- **Challenge is to solve all the problems in the most economically feasible way**

Using IP Routing as a Security Tool

- ISPs use routing to get packets from customers to the Internet
- ISPs use routing to engineer traffic through their network
- ISPs manipulate traffic to get the most out of their available bandwidth
- What is the problem with manipulating bad traffic to get the most out of available bandwidth?

Using IP Routing as a Security Tool

- IP Routing can be used to manipulate traffic on the ISPs network to:

  Null0 (Black Hole)

  Shunts

  Sink Hole

  Analysis Devices

  Clean up Devices

  Rate-Limit

Using IP Routing as a Security Tool

- And it is all done via BGP….
  - Uses a BGP “trigger router”
  - One router on the network connected via an iBGP route reflector that injects “trigger update”
  - The BGP Update packet

Source Based Remote Triggered Black Hole Filtering

- What do we have?

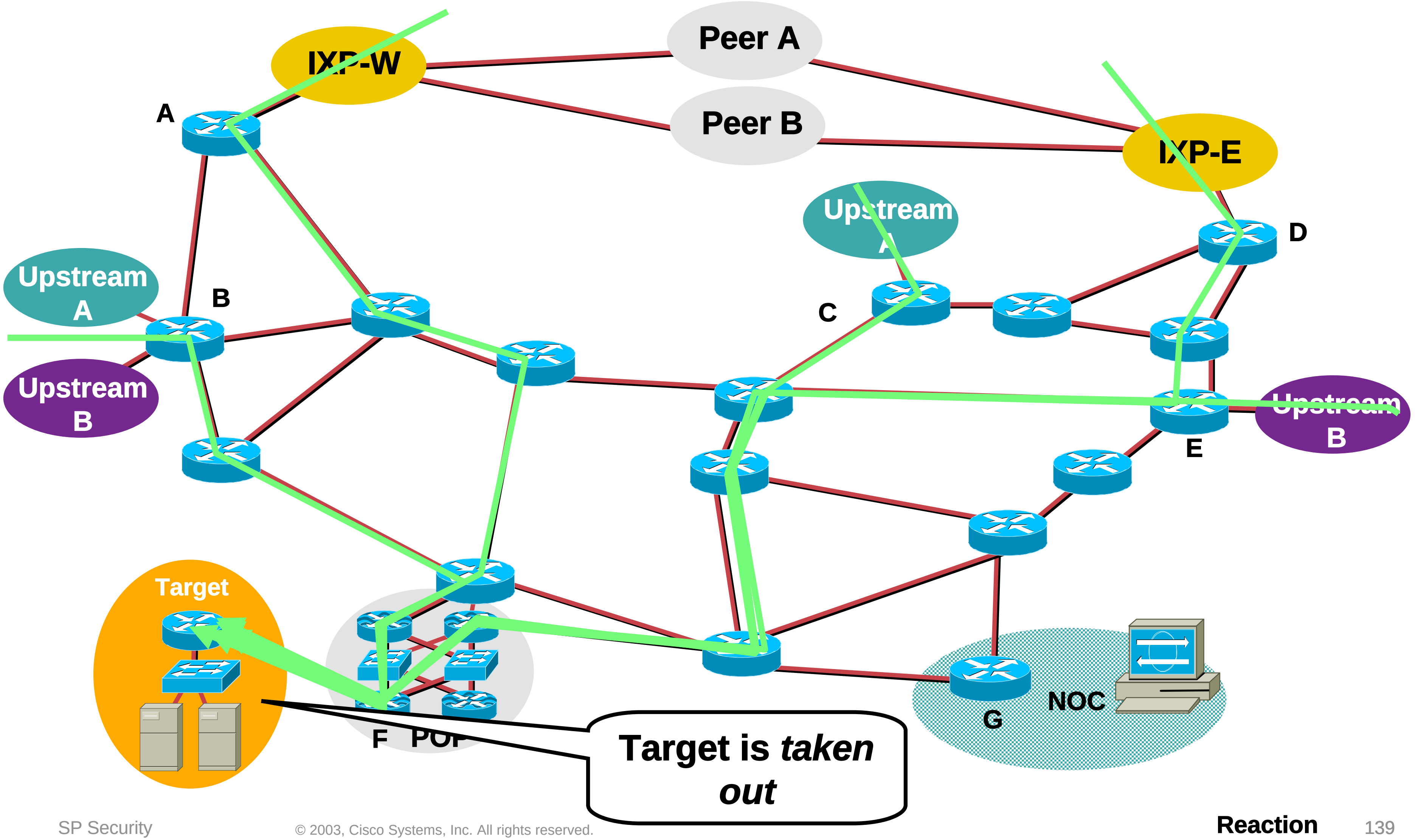
  Black Hole Filtering—If the **destination** address equals Null 0 we drop the packet.

  Remote Triggered—Trigger a prefix to equal Null 0 on routers across the Network at iBGP speeds.

  uRPF Loose Check—If the **source** address equals Null 0, we drop the packet.

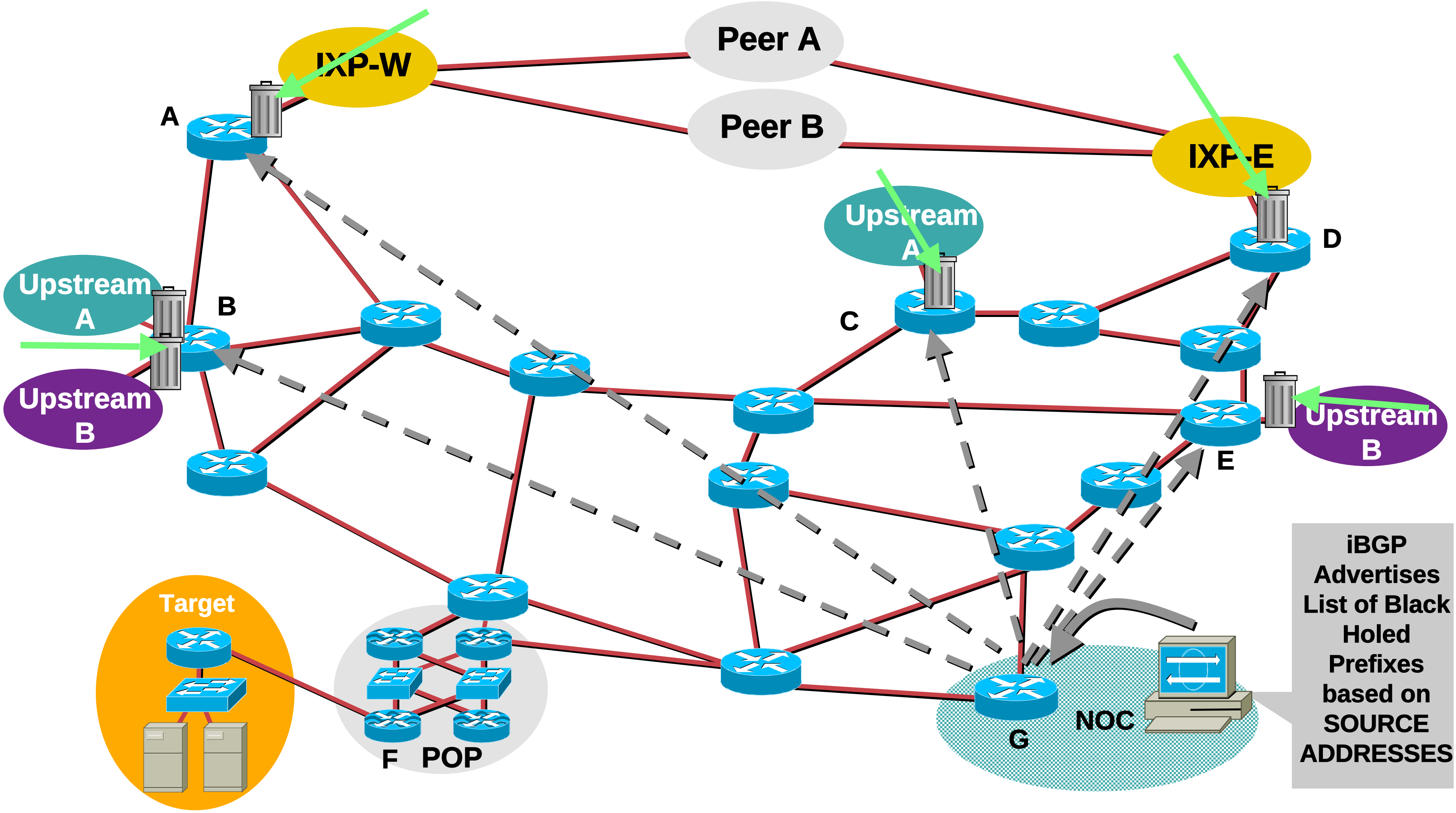
- Put them together and we have a tool to trigger drop for any packet coming into the network whose source or destination equals Null 0!

Customer Is DOSed—Before



Target is *taken out*

Customer Is DOSed—After



iBGP Advertises List of Black Holed Prefixes based on SOURCE ADDRESSES

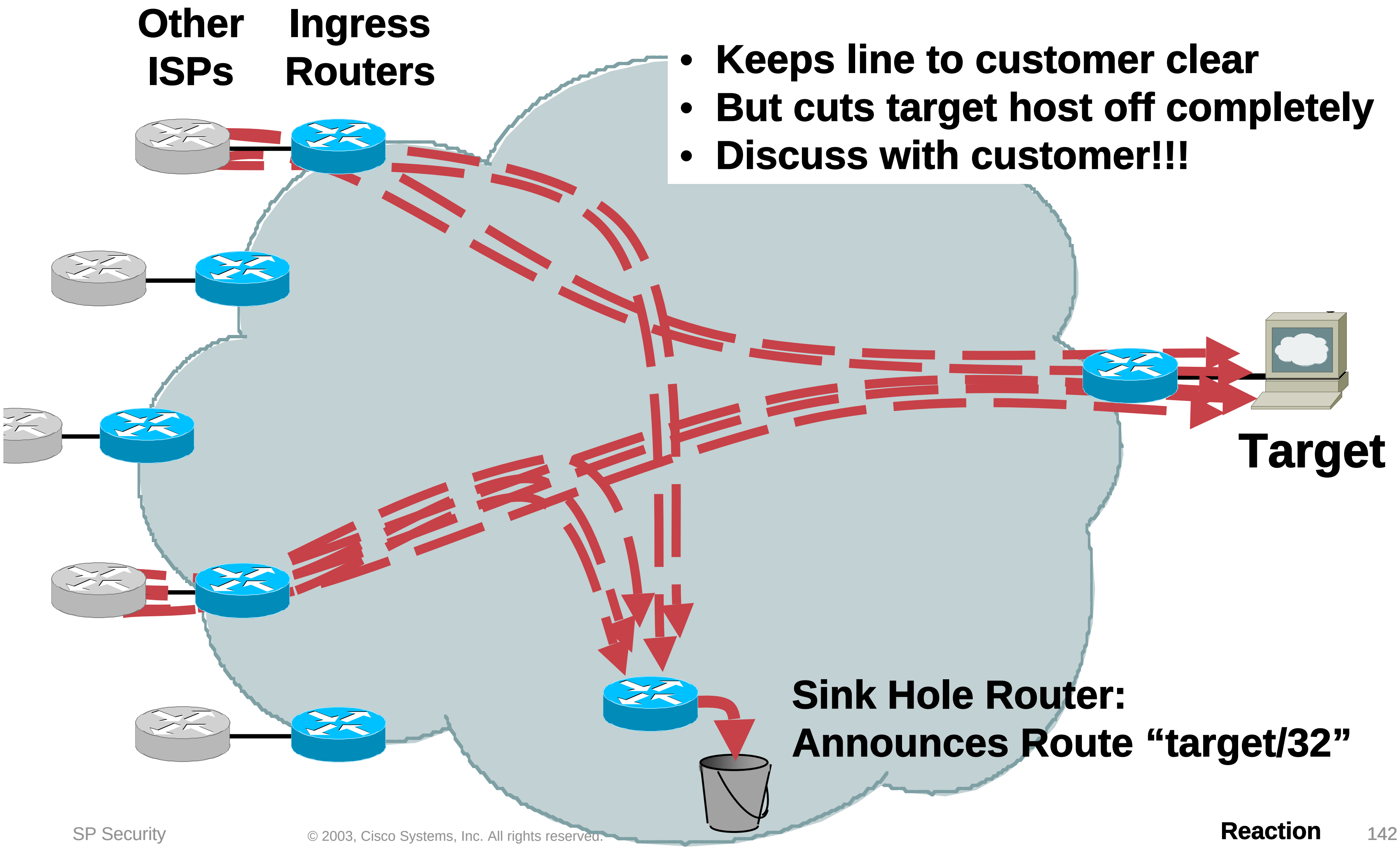
Mitigation: Packet “Scrubbing”

- Use the same BGP mechanism to redirect traffic to scrubbing devices
- Activate redirection:

  Redistribute host route for victim into BGP with next-hop set to scrubbing devices

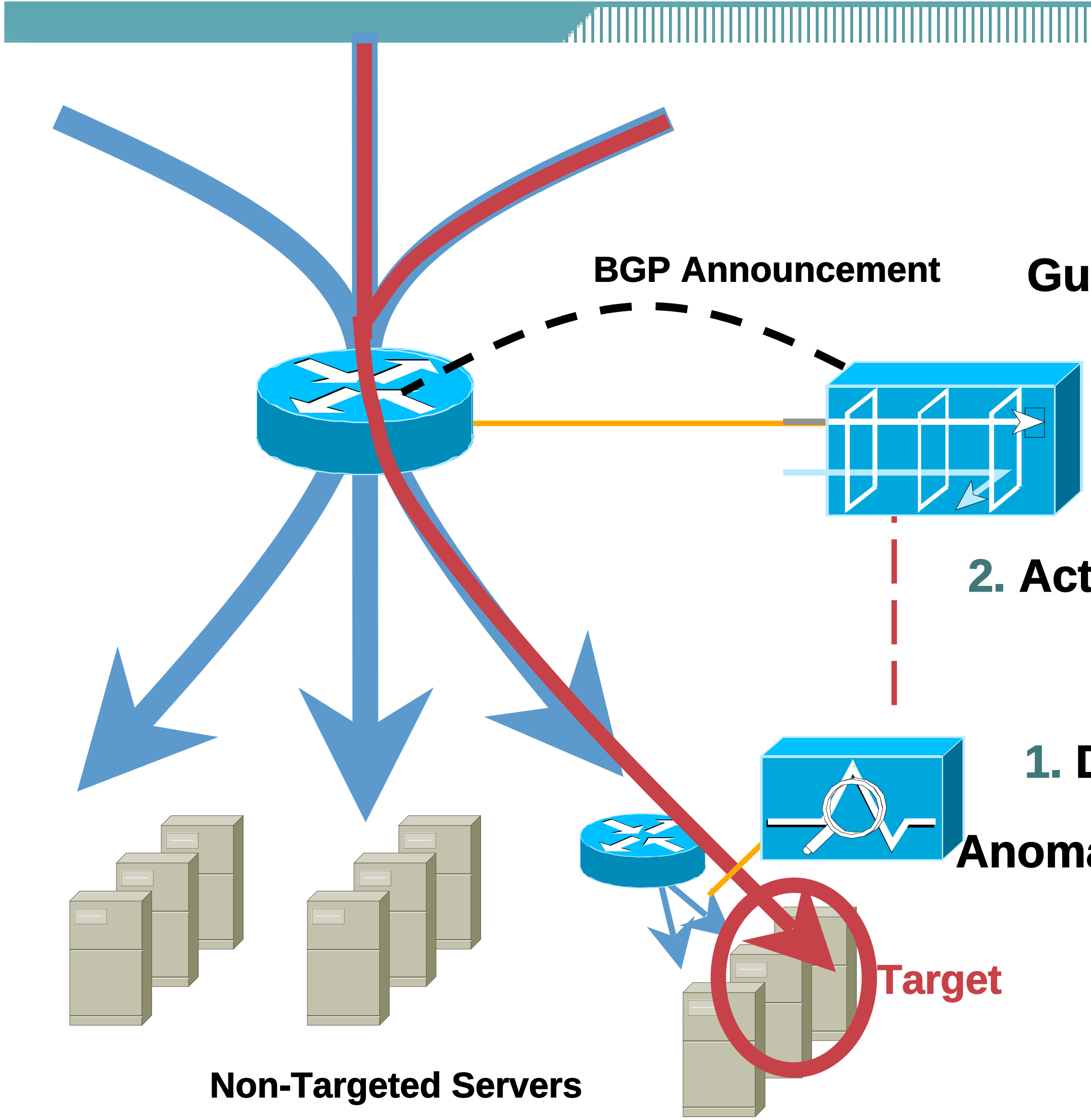
  Route is propagated using BGP to all BGP speaker and traffic redirected
- When attack is over, BGP route can be removed to return to normal operation

Re-Directing Traffic from the Victim



- Keeps line to customer clear
- But cuts target host off completely
- Discuss with customer!!!

Guard: Packet Scrubbing



BGP Announcement

Guard

3. Divert Only Target’s Traffic

2. Activate: Auto/Manual

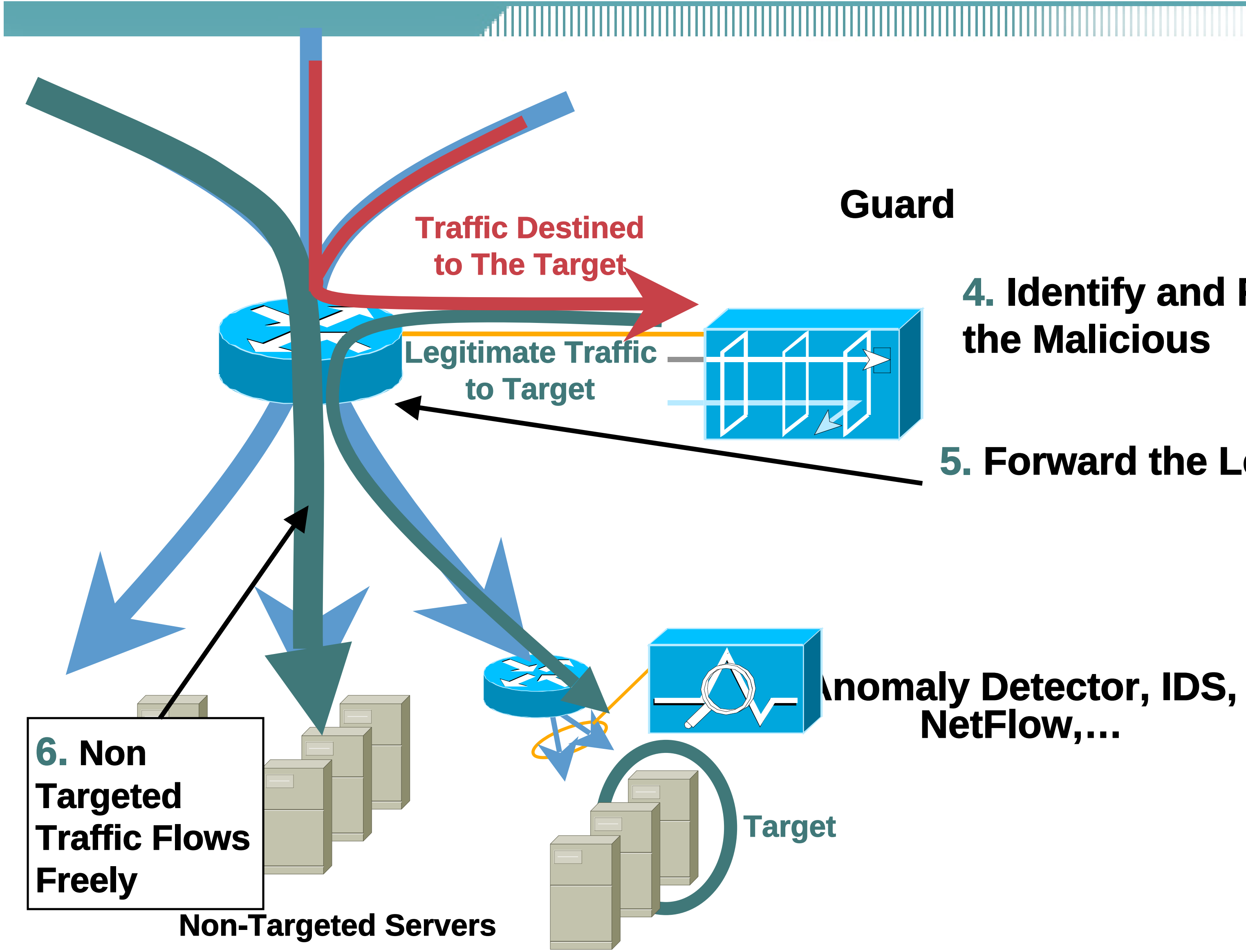
1. Detect

Anomaly Detector, IDS, NetFlow…

Target

Non-Targeted Servers

Guard: Packet Scrubbing


Guard
Traffic Destined to The Target
Legitimate Traffic to Target
4. Identify and Filter the Malicious
5. Forward the Legitimate
Anomaly Detector, IDS, NetFlow,…
Target
6. Non Targeted Traffic Flows Freely
Non-Targeted Servers

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

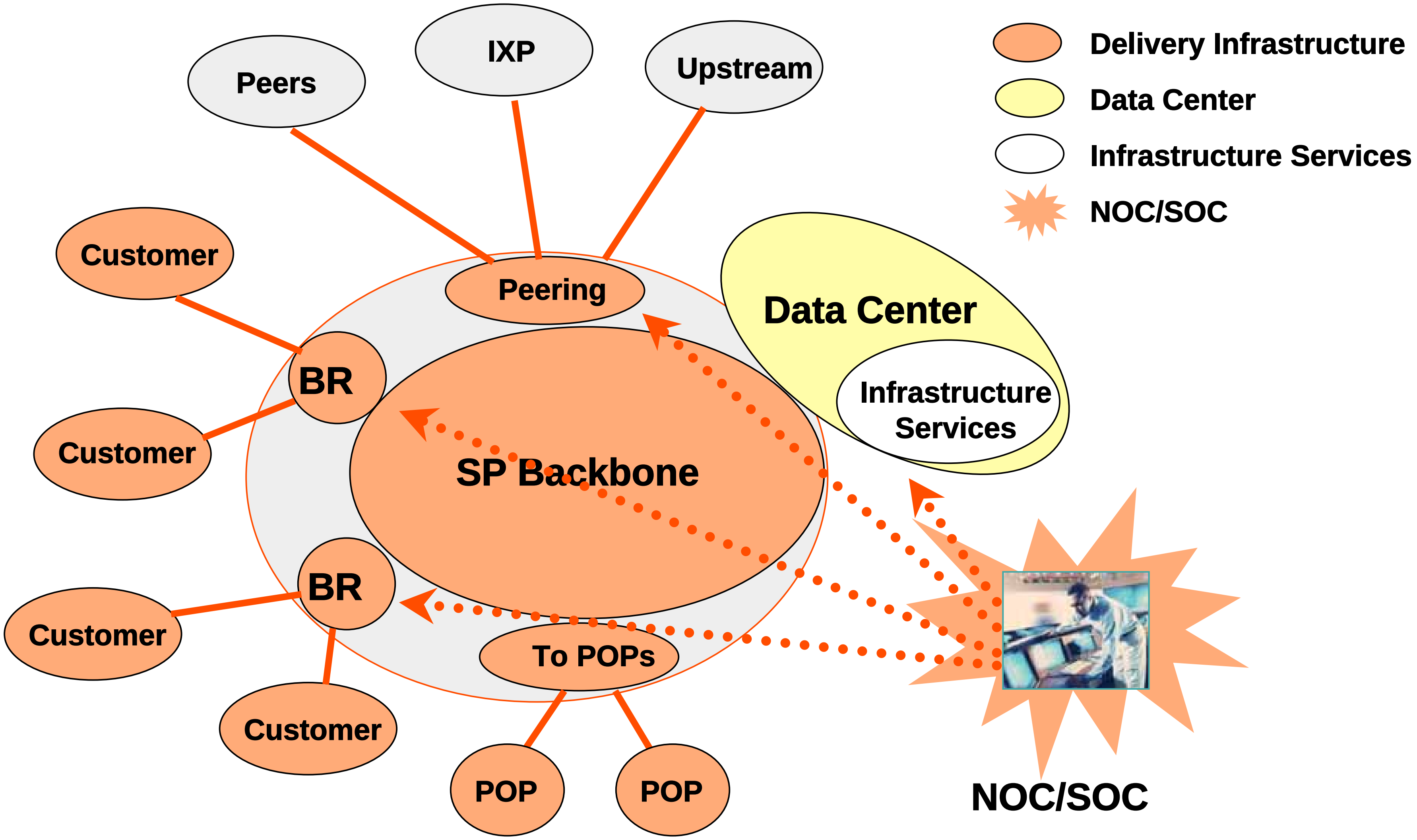
- Analyze data, trends and discuss attack
- Fully history of attack(s), trends, etc..
- Determine what, if anything, could have been done to be better prepared—make appropriate modifications if necessary

Post Mortem Activities

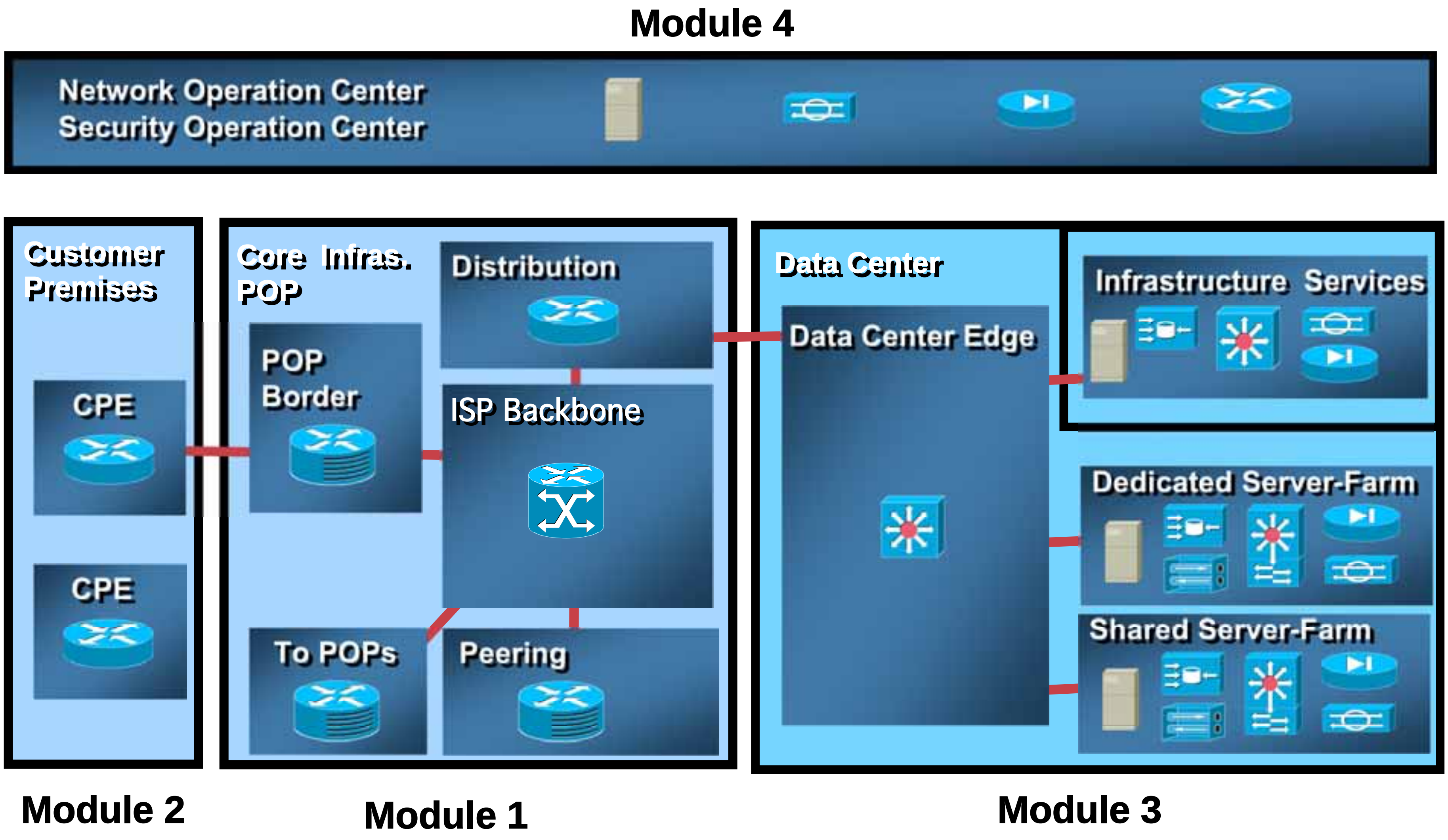
- Assess Incident Response Team Role
  - Full Representation?
  - Single/centralized Point of Contact?
- Review and Update Technical AND Operational Functions and Procedures
- Quantify impact of downtime
  - Financial
  - Operational
- What can we do better next time?

The Next Steps-
Modular Application of Techniques
to SP Infrastructure

SP Network Infrastructure



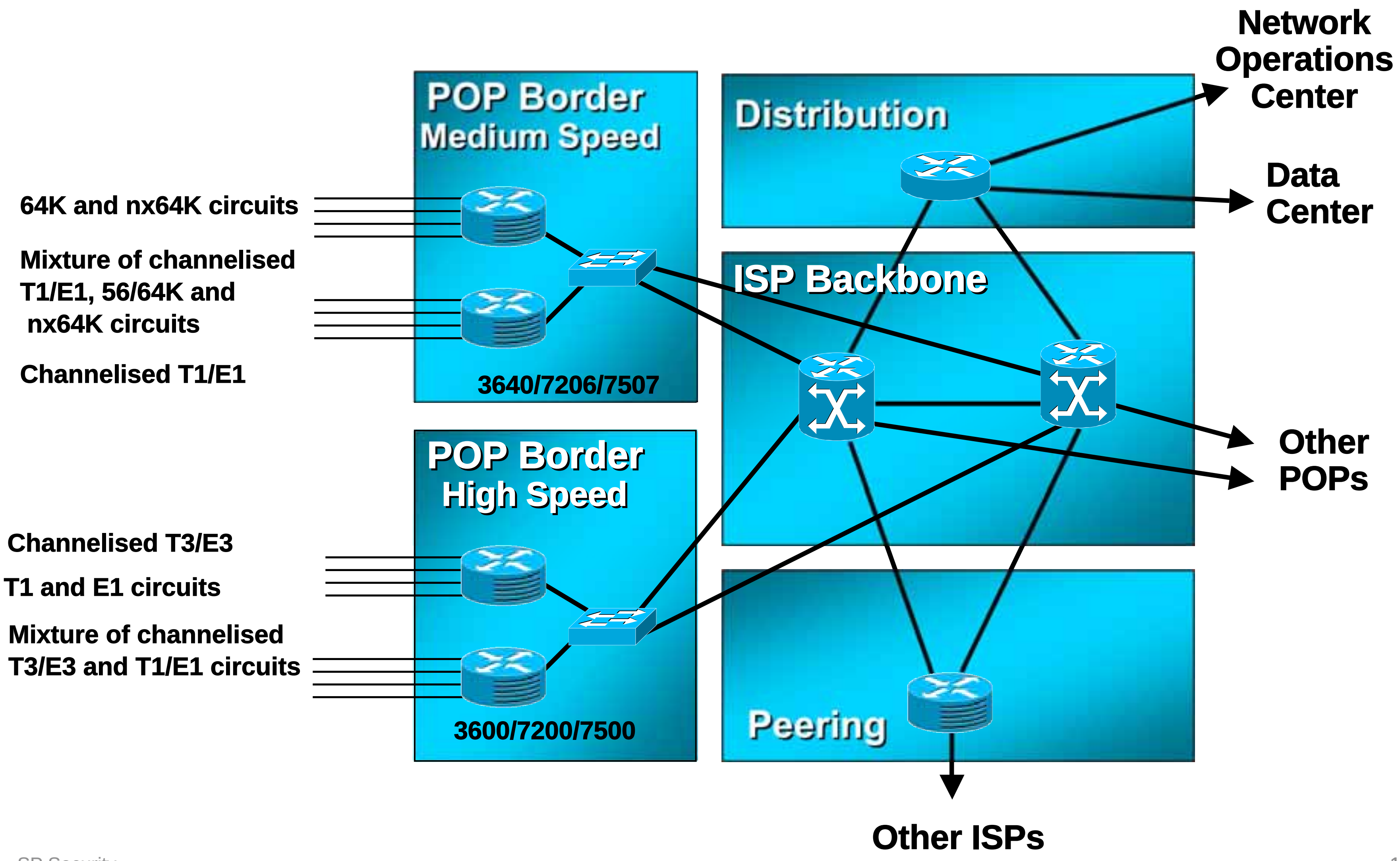
SP Functional Blocks



Why and the benefits of Modular Design

- Systematic approach where security is implemented throughout the network rather than point products
- Multiple layers of control provides higher security
- It allows you to focus on the most critical areas first
- Facilitates the enforcement of the security policy
- Contains the effects of attacks
- More flexible to adapt to keep up with the always changing threats

Module I - Typical POP & Core Infrastructure



POP and Core typical threats

- Network Reconnaissance
- Denial of Service
- Viruses and Worms
- IP Spoofing
- Direct Exploits
- Routing Disruption
- ……..

Securing POP & Core Infrastructure Module

- **Harden routers and switches**

  Prevents DoS and Direct attacks to routers and switches

- **Secure Dynamic Routing Exchange**

  Route Authentication, Route Filters prevent attacks on the Dynamic Routing

- **Deploy packet filters**

  Mitigates DoS attacks, spoofed attacks, reconnaissance, viruses/worms and direct attacks

- **Attack detection, traceback and containment**

Securing POP & Core Infrastructure Module
Harden routers and switches

- IOS hardening
  - –Set strong passwords
  - –Enable secure access
  - –Configure banners
  - –Disable unnecessary global and interface services
  - –Autosecure
  - –.....
- Selective Packet Discard (SPD)
  - –Prioritize control packets
- Control ICMP Unreachable
- ……

Securing POP & Core Infrastructure Module
Secure Dynamic Routing Exchange

- **Secure Routing Route Authentication**
  - –**Plain text**
  - –**HMAC-MD5**
- **Control Routing Updates**
  - –**Dynamic Routing Filter on Customers**
  - –**Dynamic Routing Filter to Peers**
  - –**Dynamic Routing Filter from Peers**
- **……….**

Securing POP & Core Infrastructure Module
Deploy packet filters

- Packet Filters
  - –RFC 2827 BCP 38 Packet Filtering (source address spoofing)
  - –BCP 38 Ingress Packet Filtering
  - –Static BCP 38 Filtering
  - –Unicast RPF (strict mode)
  - –……….

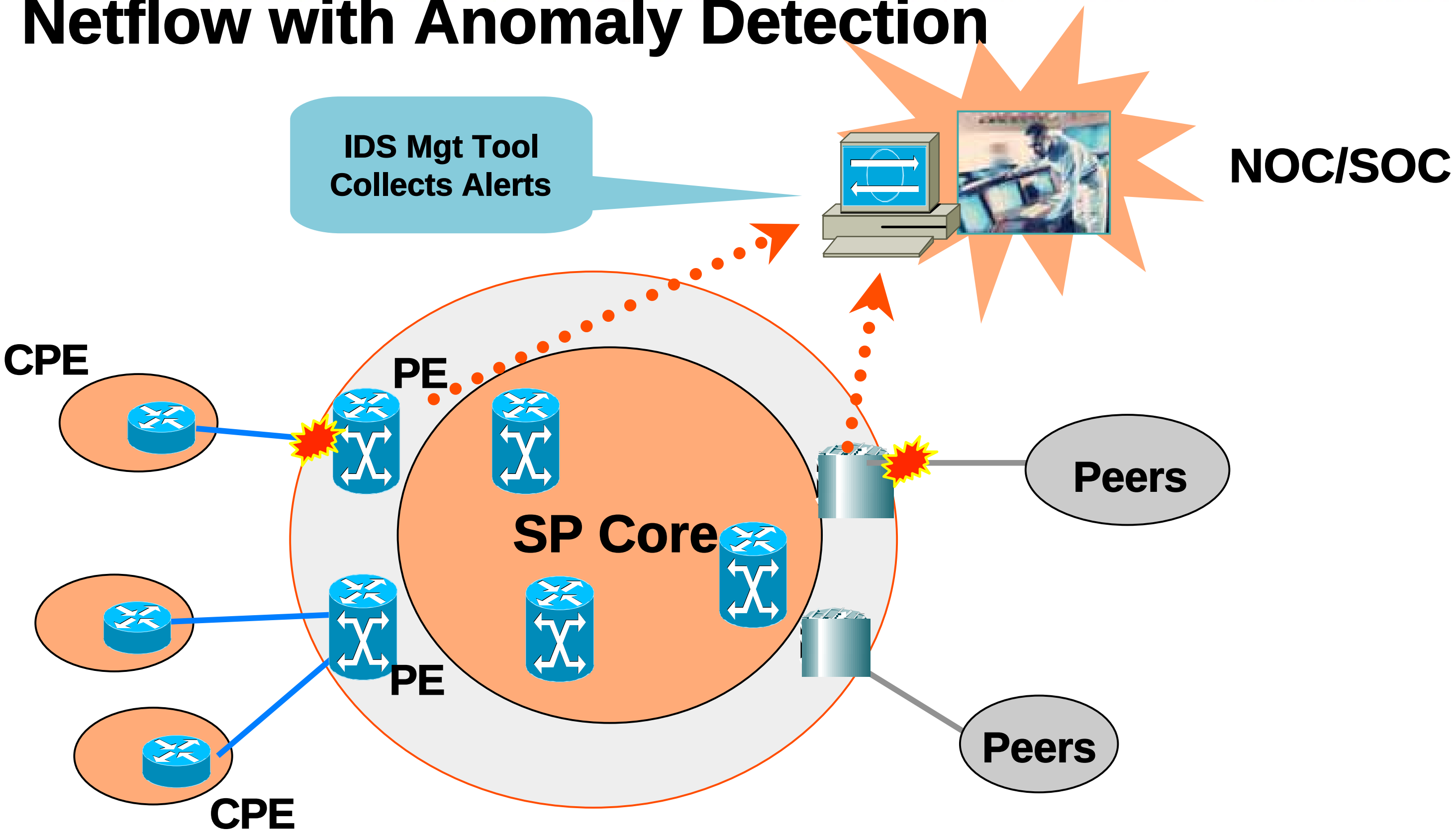
Securing POP & Core Infrastructure Module
Attack detection, traceback and containment

- Netflow
- Intrusion Detection System alerts
- Sink hole routers/networks
- Unusual CPU load – reported via SNMP
- Circuits Saturated
- BGP Session Flapping
- Customer calls
- ....

Securing POP & Core Infrastructure Module

Attack detection, traceback and containment

Netflow with Anomaly Detection



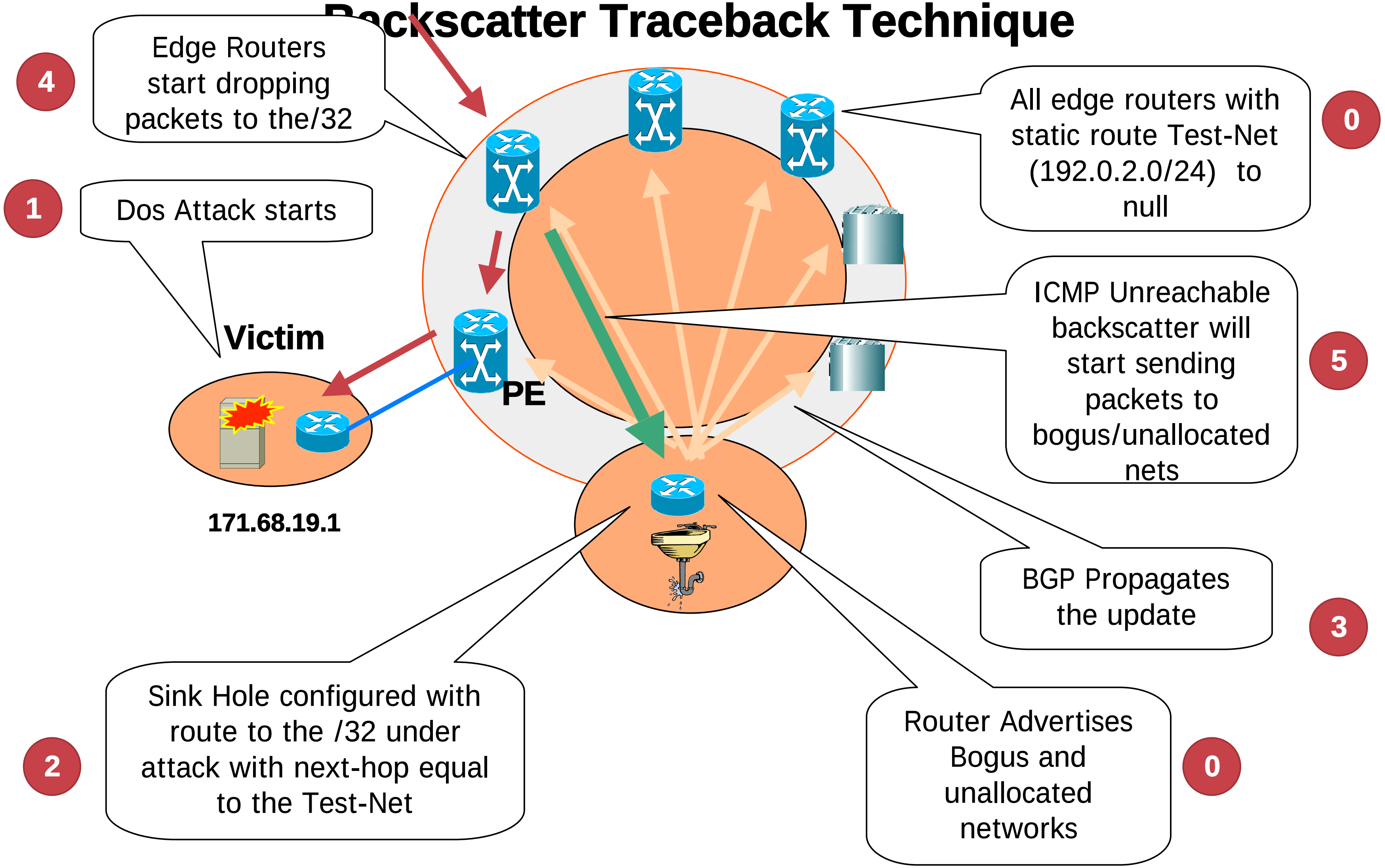
The IDS uses Netflow to collect data on the flows through the network, looking for matches to known attacks while watching for new *anomalies* in the data flow

Securing POP & Core Infrastructure Module Attack detection, traceback and containment

1. **Apply temporary ACLs with log-input and examine the logs**
2. **Query Netflow’s flow table**
   - No changes to the router while the network is under attack; passive monitoring
   - Scripts can be used to poll and sample throughout the network
   - IDS products can plug into Netflow
   - Working on a MIB for SNMP access
3. **Backscatter Traceback Technique**
   - 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.

Securing POP & Core Infrastructure Module Attack detection, traceback and containment

Backscatter Traceback Technique

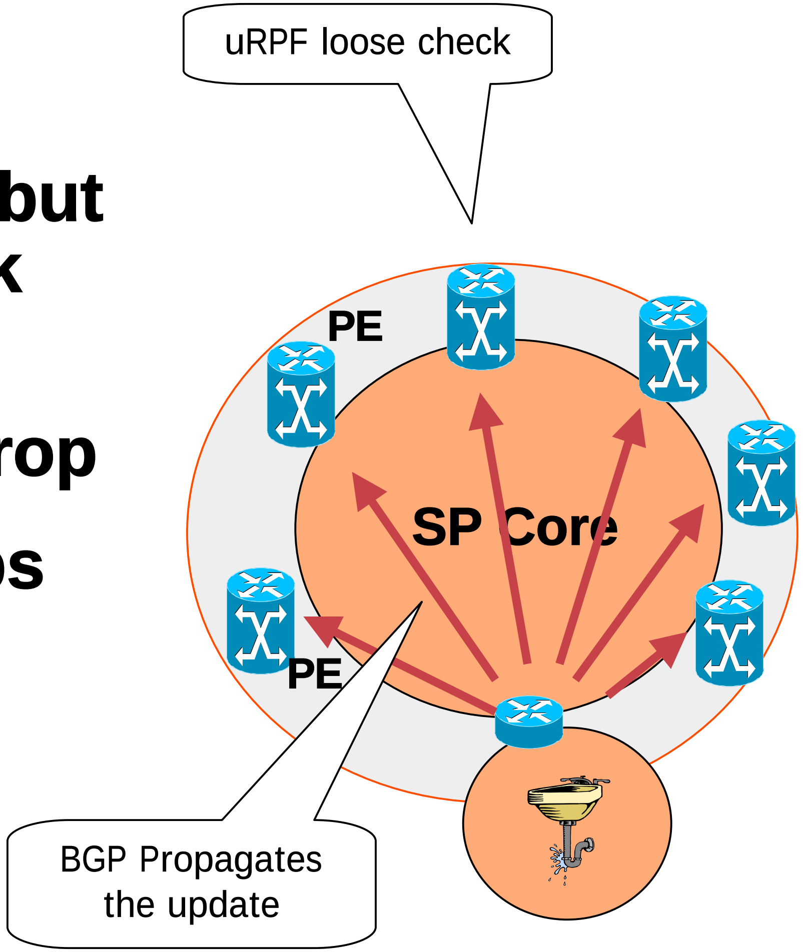

4
Edge Routers start dropping packets to the/32
1
Dos Attack starts
Victim
171.68.19.1
PE
0
All edge routers with static route Test-Net (192.0.2.0/24) to null
5
ICMP Unreachable backscatter will start sending packets to bogus/unallocated nets
BGP Propagates the update
3
2
Sink Hole configured with route to the /32 under attack with next-hop equal to the Test-Net
Router Advertises Bogus and unallocated networks
0

Securing POP & Core Infrastructure Module
Attack detection, traceback and containment

- ACLs—Manual upload/dynamic upload
- uRPF—Remote trigger via BGP
- CAR—Manual upload or remote trigger via BGP
- ……..

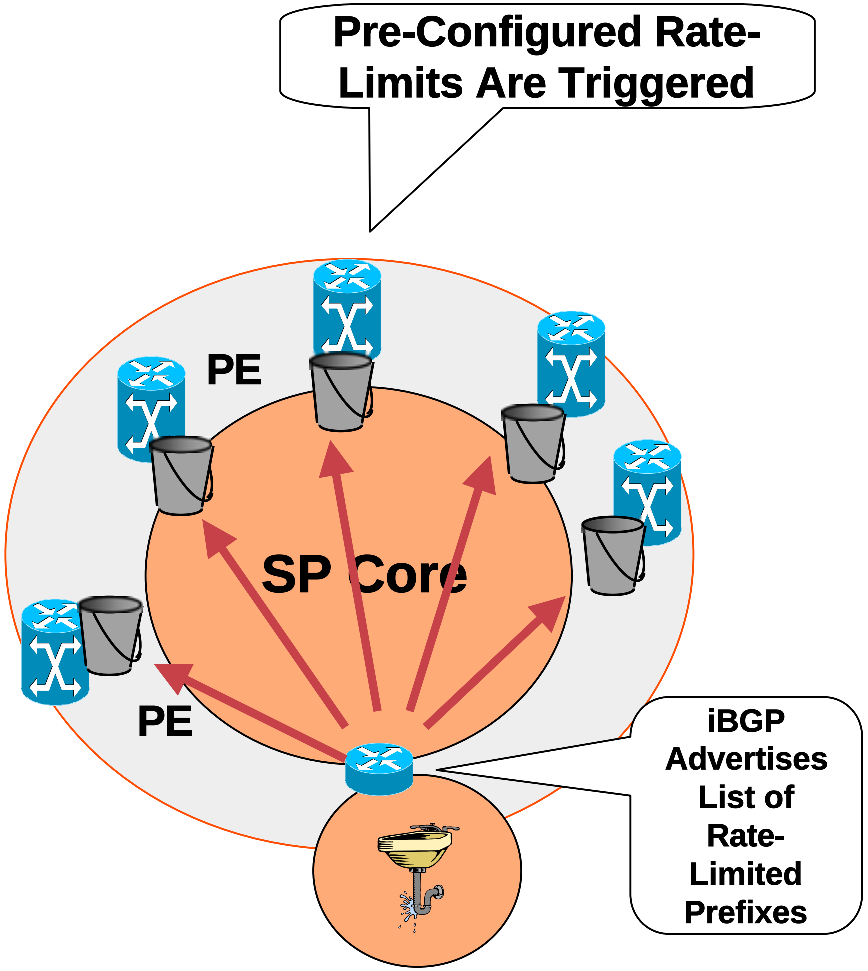
Remote Triggered uRPF

- **Same as Backscatter Traceback Technique but with uRPF loose check on all border routers**
- **If source = null then drop**
- **static to null also drops on destination**



Remote Triggered CAR

- **Quality Policy Propagation with BGP (QPPB) empowers CAR to use updates triggered by BGP. This enables a network protocol to trigger the rate limits on source/destination**



Pre-Configured Rate-Limits Are Triggered

iBGP Advertises List of Rate-Limited Prefixes

Module II - Secure Customer Premises

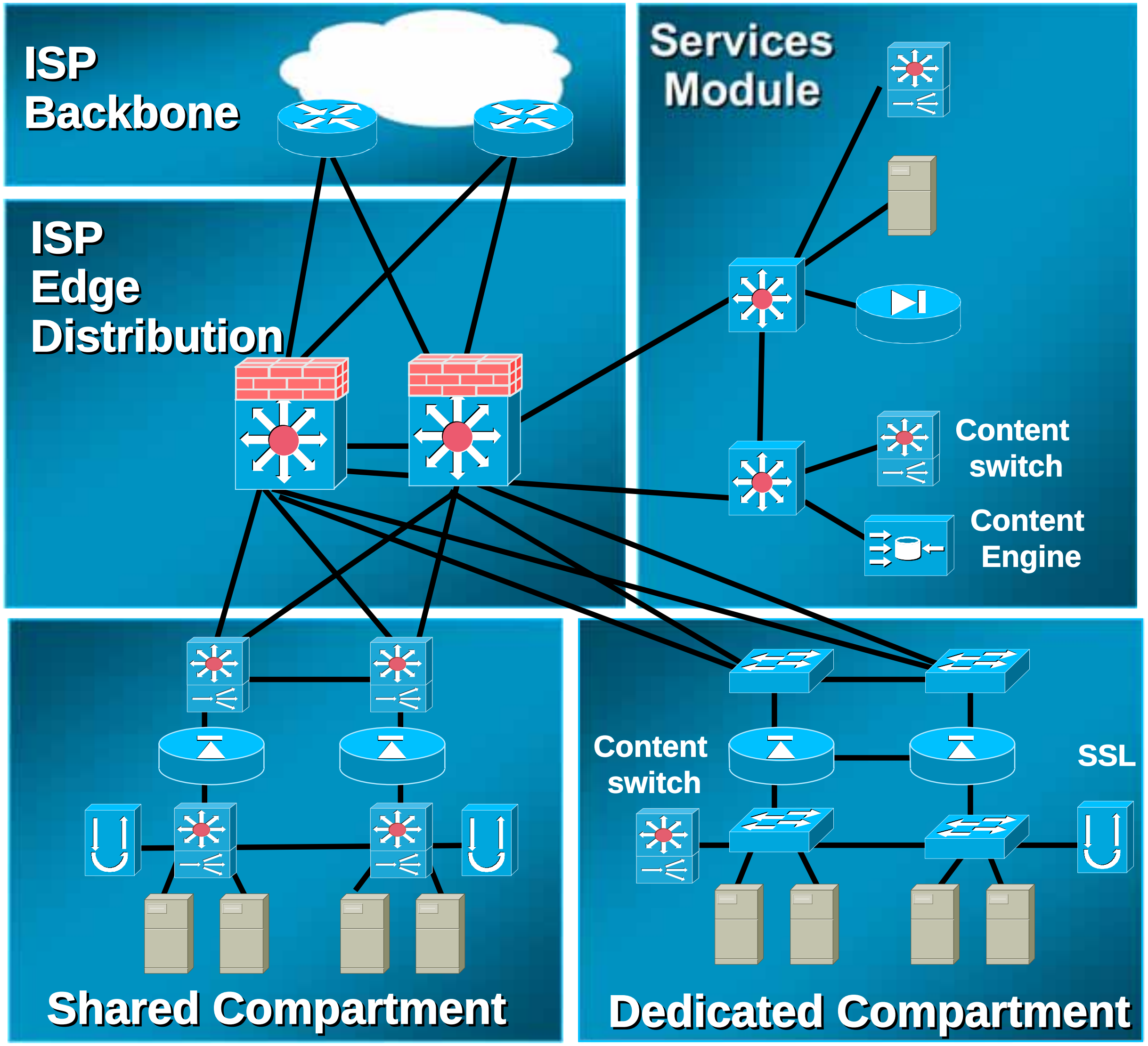
- Secure deployment and provisioning
- Secure management and configuration
- Integrated Security at the CPE

Secure Provisioning and Deployment

Provisioning and deployment are the phases in which the devices are the most vulnerable:

- Not all devices come with secure defaults
- Initial configurations may include more items than needed for initial setup (i.e. unnecessary services)
- The protocols and applications used for initial configuration may not be secure
- Deployment may not include the authentication of the new device
- Pre-configure the new device with a secure configuration prior to its deployment (consider even before shipping)
- Once connected, use secure access for initial setup
- For high volume deployments use a hierarchical management solution
- Access Control\Authorization Using AAA

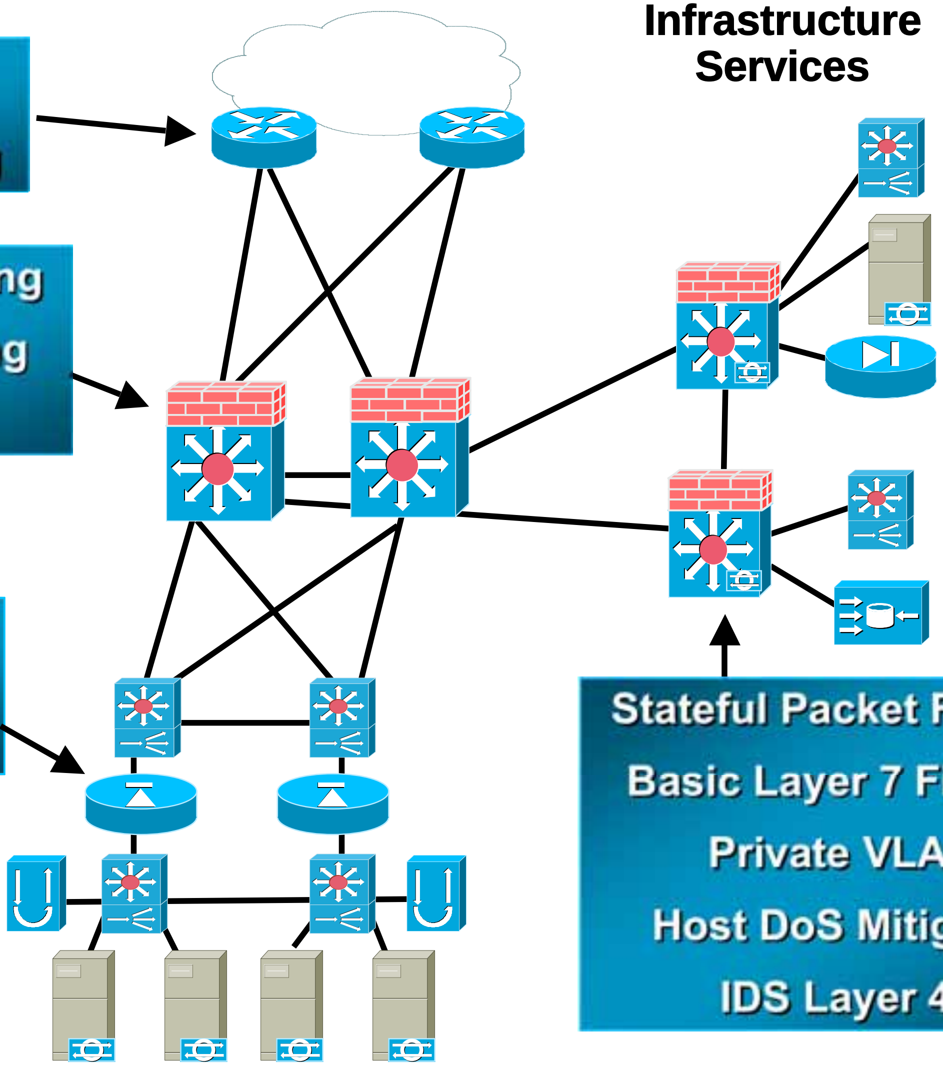
Module III - Secure Data Center



IDC Security Highlights

- Core, Distribution, Access model
- Resilience at layer 2 and 3
- Uses Scaling Modules
- Provides Baseline Content Services
- Access: Layer 2 VLAN separation
- Distribution: Aggregate VLANs, routing and layer 3 filtering
- Core: Provides L3 connectivity

Secure Data Center Design



Spoof Mitigation

(D)DoS Rate-Limiting

Stateful Packet Filtering

Basic Layer 7 Filtering

DoS Mitigation

Stateful Packet Filtering
Basic 7 Layer Filtering
Host DoS Mitigation

Host IDS Local Attack Mitigation

Stateful Packet Filtering

Basic Layer 7 Filtering

Private VLANs

Host DoS Mitigation

IDS Layer 4-7

Module IV - Secure NOC/SOC module

- Protect the NOC

  Separate physical networks (NOC vs. campus)

  Separate address space (192.168.25x.xxx)

  -Not routed anywhere else

  Firewall between management subnet and rest of SP campus

  -Chokepoint to protect NOC functions

  NIDS and HIPS on the management subnet

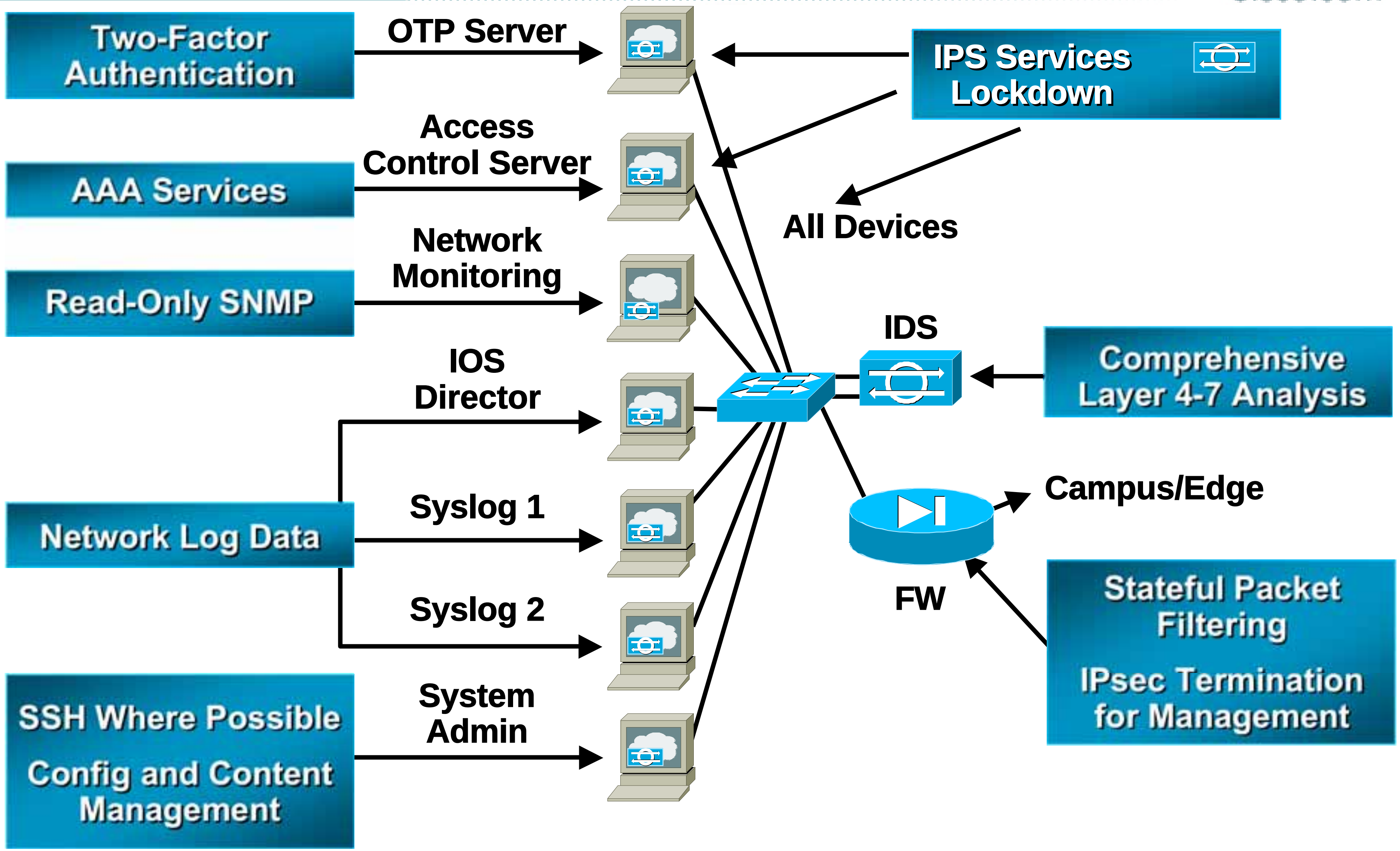
  One-Time Passwords (OTPs) for authentication of administrators

  IPSec for remote administrative access to the NOC

Module IV - Secure NOC/SOC module - cont’d

- Secure remote management of CPE devices
  - Consider Out-Of-Band (OOB) management network
    - Dedicated physical management interfaces on all remote managed devices
    - Alternatively a high availability backup option
  - Secure transport
    - IPsec for always-up SNMP\MIB\syslog access
      - SNMP read-only
      - Pre-shared keys (no wildcard) or PKI
    - SSL, SSH, or IPsec RA for troubleshooting

Secure NOC/SOC module Design



Two-Factor Authentication

AAA Services

Read-Only SNMP

Network Log Data

SSH Where Possible

Config and Content Management

IPS Services Lockdown

Comprehensive Layer 4-7 Analysis

Stateful Packet Filtering

IPsec Termination for Management

Wireless Security
A Quick Glance

Wireless LAN Security Hierarchy

Open Access

No Encryption,
Basic Authentication

Public “Hotspots”

Basic Security

40-bit or 128-bit
Static WEP Encryption

Home Use

Enhanced Security

WPA, 802.1X,
TKIP Encryption,
Mutual Authentication,
Dynamic Keys

Business

Remote Access

Virtual
Private
Network
(VPN)

Business
Traveler,
Telecommuter

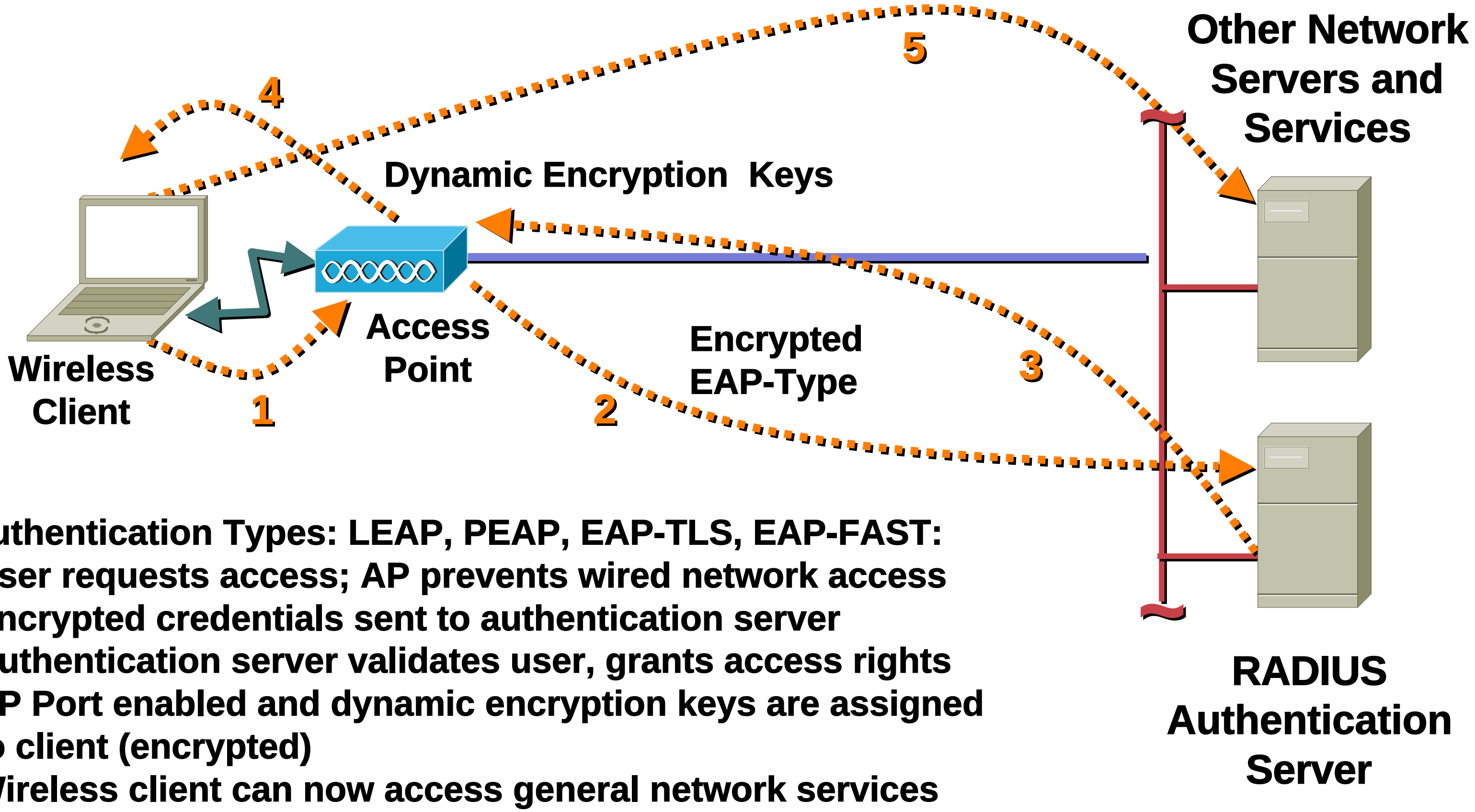
Basic Wireless LAN Security
802.11 Security Vulnerabilities

- **Shared, static Wired Equivalent Privacy (WEP) keys**
  - No centralized key management
  - Poor protection from variety of security attacks
- **No effective method to deal with lost or stolen client adapters**
  - Possessor of client adapter has access to WLAN and any network resource for which no network logon is required
  - Re-keying of all WLAN devices is required
- **Lack of integrated user administration**
  - No central authentication entity
  - Potential to identify user by MAC address, not username
  - No usage accounting and auditing. No means to detect unusual activity
- **Lack of effective message integrity**
  - Management and data frames use ineffective CRC for integrity check.

Wireless LAN Security Authentication and Encryption

- **Authentication**
  - IEEE 802.11 Authentication: Open or shared-key – Not secure
  - Static WEP Keys – Unable to send or receive without correct keys. Device can be stolen. Keys can be cracked
  - MAC Address Authentication – Device-based. Address can be spoofed
  - IEEE 802.1X: EAP Types – LEAP, EAP-FAST, PEAP and EAP-TLS, EAP-TTLS. Component of new standard for WLAN security. Supports mutual authentication and dynamic, per-user, per-session encryption keys
  - Wi-Fi Protected Access (WPA) - 802.1X is a required component of the WPA standard. WPA is tested with EAP-TLS but works with all EAP types including Cisco LEAP.
- **Encryption**
  - IEEE 802.11 WEP - Standard for encryption
    - Uses RC4 algorithm - known vulnerabilities
    - Keys can be static and shared among many clients or, as with 802.1X, keys can be dynamic and unique for each client
  - Temporal Key Integrity Protocol (TKIP): Enhancements to RC4-based WEP
    - Cisco TKIP and WPA TKIP available
    - Key Hashing or Per-packet keying, Message Integrity Check (MIC) and Broadcast Key Rotation
  - Advanced Encryption Standard (AES)

Enhanced Wireless LAN Security
802.1X Protocol in WLAN Environment



EAP Authentication Types: LEAP, PEAP, EAP-TLS, EAP-FAST:

1. User requests access; AP prevents wired network access
2. Encrypted credentials sent to authentication server
3. Authentication server validates user, grants access rights
4. AP Port enabled and dynamic encryption keys are assigned to client (encrypted)
5. Wireless client can now access general network services securely

Enhanced Wireless LAN Security 802.1X for 802.11 Benefits

- Open, extensible and standards based solution
- Leverages existing standards: EAP (Extensible Authentication Protocol), RADIUS
- Strong authentication with support for a variety of authentication types
- User-based identification
- Dynamic key management
- Better multicast capability
- Centralized policy control - authentication, authorization and accounting
- Session timeout triggers re-authentication and new encryption key

New Security Enhancements Mitigate Network Attacks

Attack	**Authentication:** Open **Encryption:** Static WEP	**Authentication:** Cisco LEAP, EAP-FAST, EAP-TLS or PEAP **Encryption:** Dynamic WEP	**Authentication:** Cisco LEAP, EAP-FAST, EAP-TLS or PEAP **Encryption:** Cisco TKIP, WPA-TKIP, AES
Man-in-the-Middle	Vulnerable	Vulnerable	Protected**
Authentication Forging	Vulnerable	Protected	Protected
Weak Key Attacks	Vulnerable	Vulnerable	Protected
Packet Forgery	Vulnerable	Vulnerable	Protected
Brute Force Attacks	40-bit WEP Vulnerable	Protected *	Protected *

Protected from War Driving

Protected from Script Kiddies

Protected from War Driving

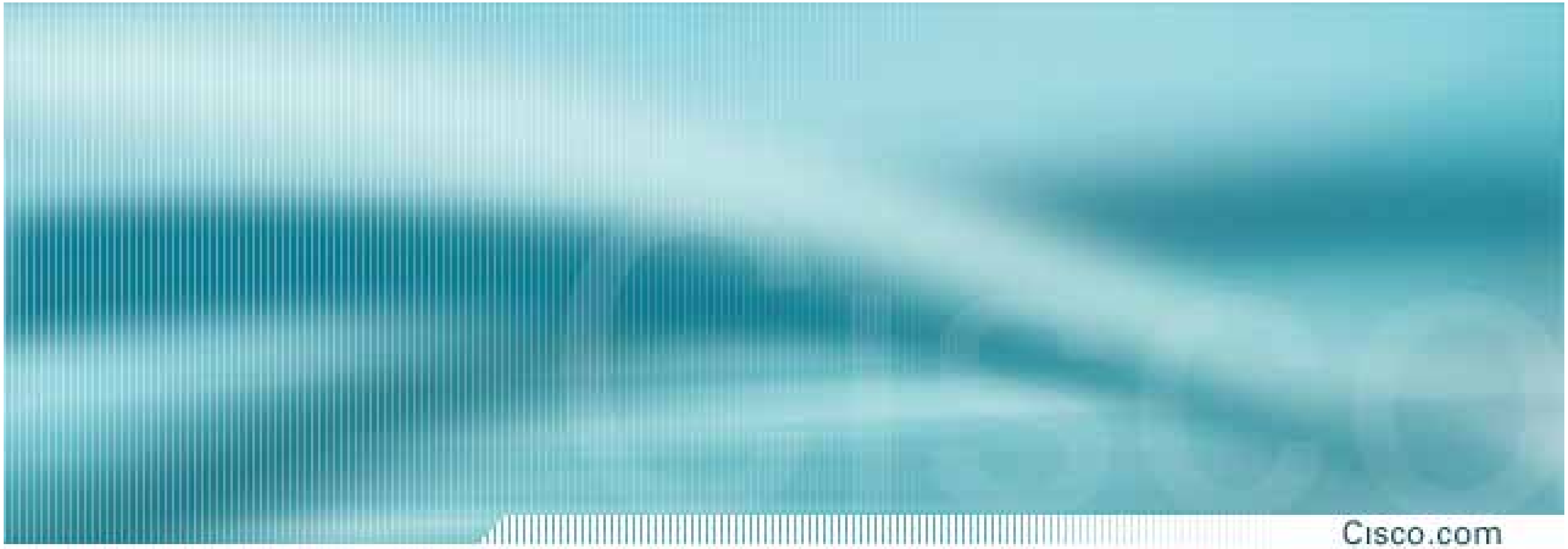
Protected from Script Kiddies

Protected from Professionals

Protected from War Driving

* Cisco LEAP requires strong passwords

** PEAP vulnerable when used with legacy authentication

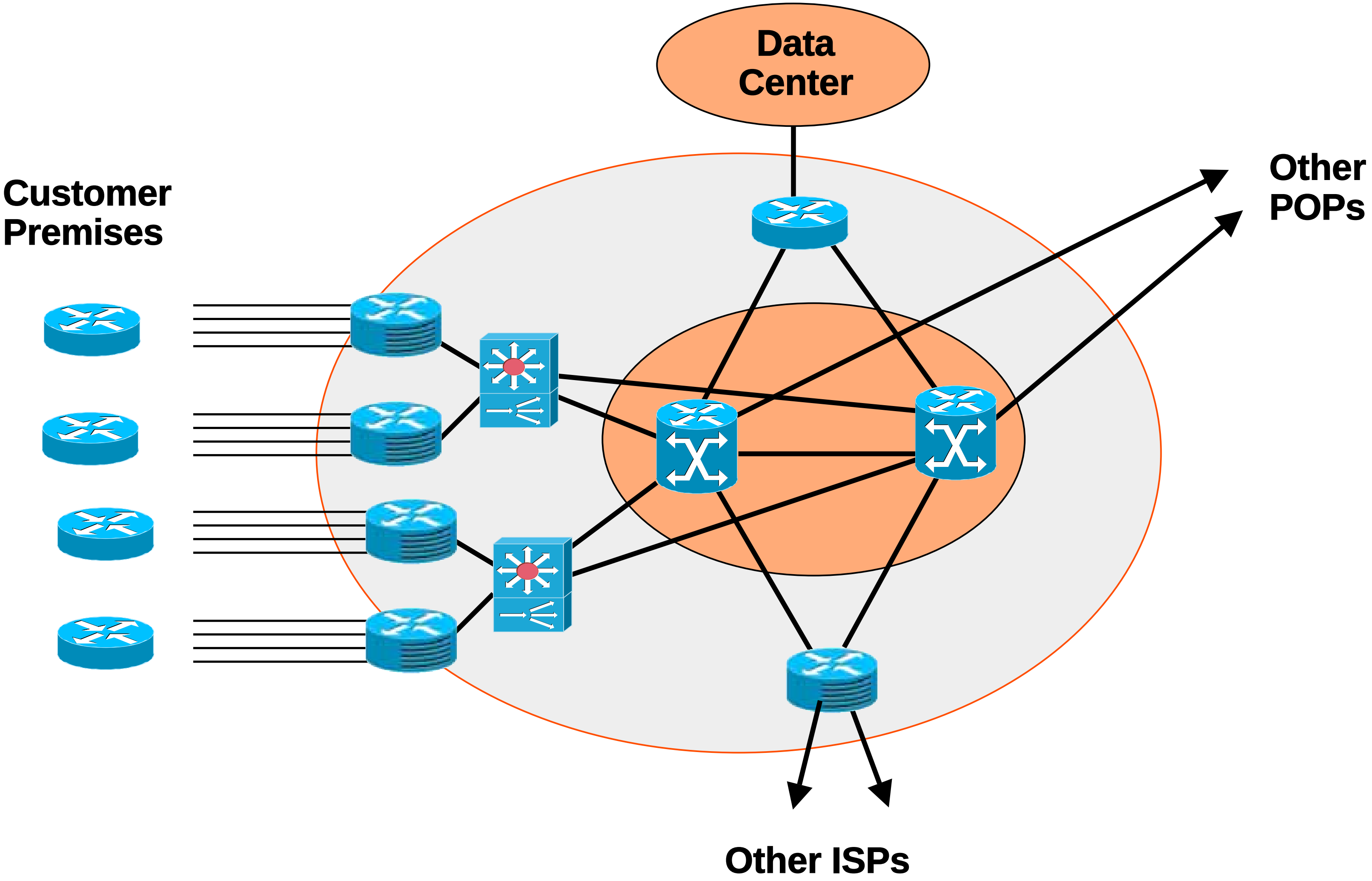


Case Study

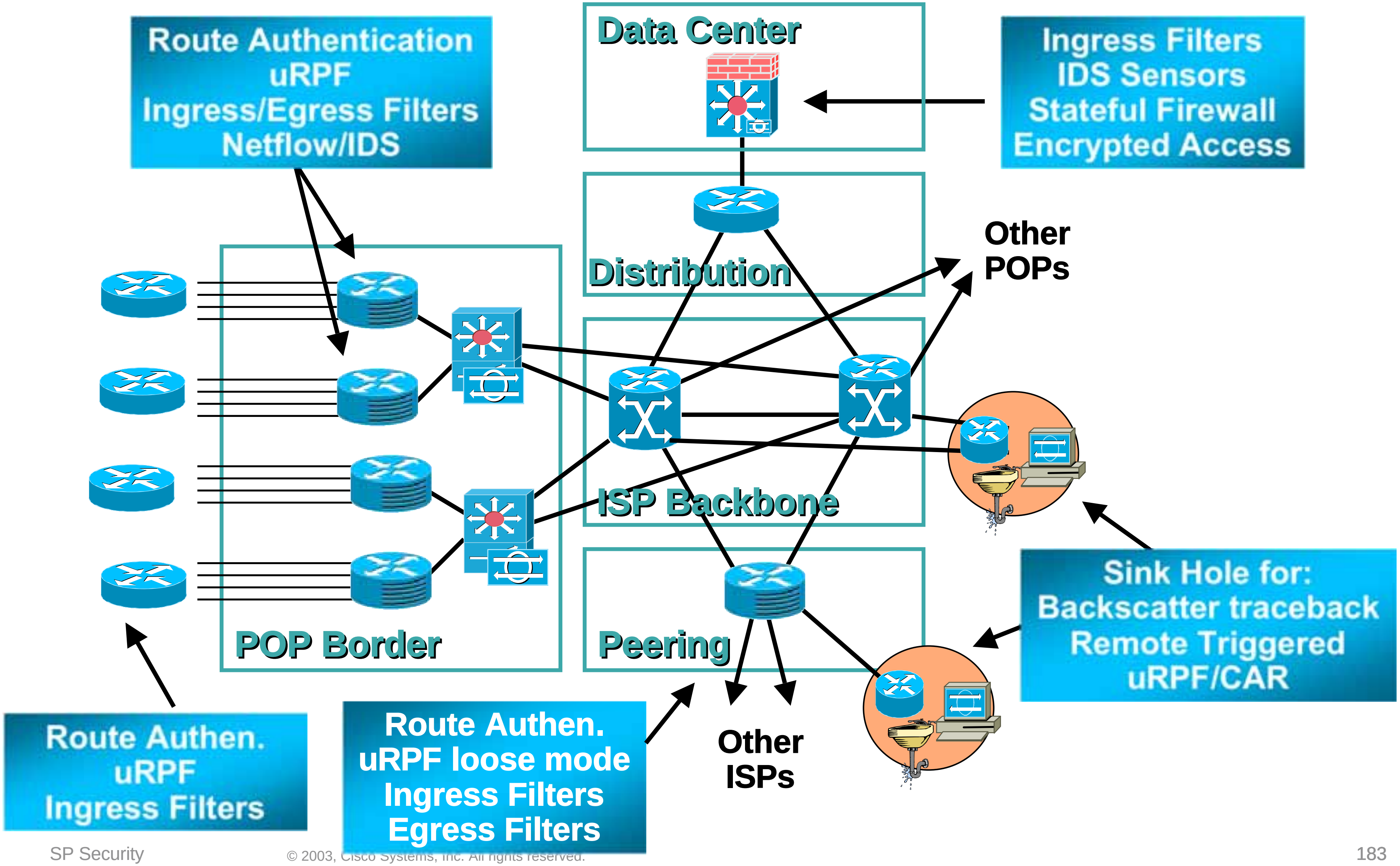
Example Customer Profile

- Major US Service Provider
- Services:
  - Broadband Internet Access
  - IP VPNs
  - VoIP
  - Web Hosting
- Incident Response Team deals with 1 DoS a day in average

Example Customer Network Topology



Example Customer Security Modular Design



Route Authentication
uRPF
Ingress/Egress Filters
Netflow/IDS

Ingress Filters
IDS Sensors
Stateful Firewall
Encrypted Access

Sink Hole for:
Backscatter traceback
Remote Triggered
uRPF/CAR

Route Authen.
uRPF
Ingress Filters

Route Authen.
uRPF loose mode
Ingress Filters
Egress Filters

What have they done to improve?

Attack Detection

Before:

- check resources such as CPU, input queues
- Backscatter analysis using tools such as snoop and tcpdump
- Use ACLs to confirm attacks.

Now:

- Netflow at border routers.
- IDS Sensors at Data Center and aggregation points

Results:

- More attacks are being detected
- Attack detection and mitigation times have been significantly reduced

What have they done to improve?

Traceback source of attacks

Before:

- Hop by hop using ACLs with logging.

Now:

- Backscatter Traceback Technique

Results:

- Traceback in minutes
- Works under large scale attacks
- Easy to hand over to peer SPs

Conclusions

- What we covered-

    Challenges, Trends, Threats

    Telemetry, Techniques, Application

- SP Security is a real issue, need an integrated system
- Integrate security throughout the network, not point products
- Define Security Policies and related Procedures
- Telemetry – Get a grip on what’s going on
- Modularize – Break the tasks into layered items

The Last Word…

YOU FOOL! HOW COULD YOU BE SO STUPID?
www.dilbert.com
scottadams@aol.com
YOU FOOL! HOW COULD YOU BE SO STUPID?
3/29/03 © 2003 United Feature Syndicate, Inc.
YOU STUPID COFFEE MUG!!

Copyright © 2003 United Feature Syndicate, Inc.

- **New threats enter, old threats leave, but the core risk mitigation strategies stay the same**
- **However, the shift from Fame to Profit as the dominant motivation is changing the paradigm of threat management**
- **Tomorrow’s threats will be different than today's—plan ahead to maintain flexibility**

CISCO SYSTEMS