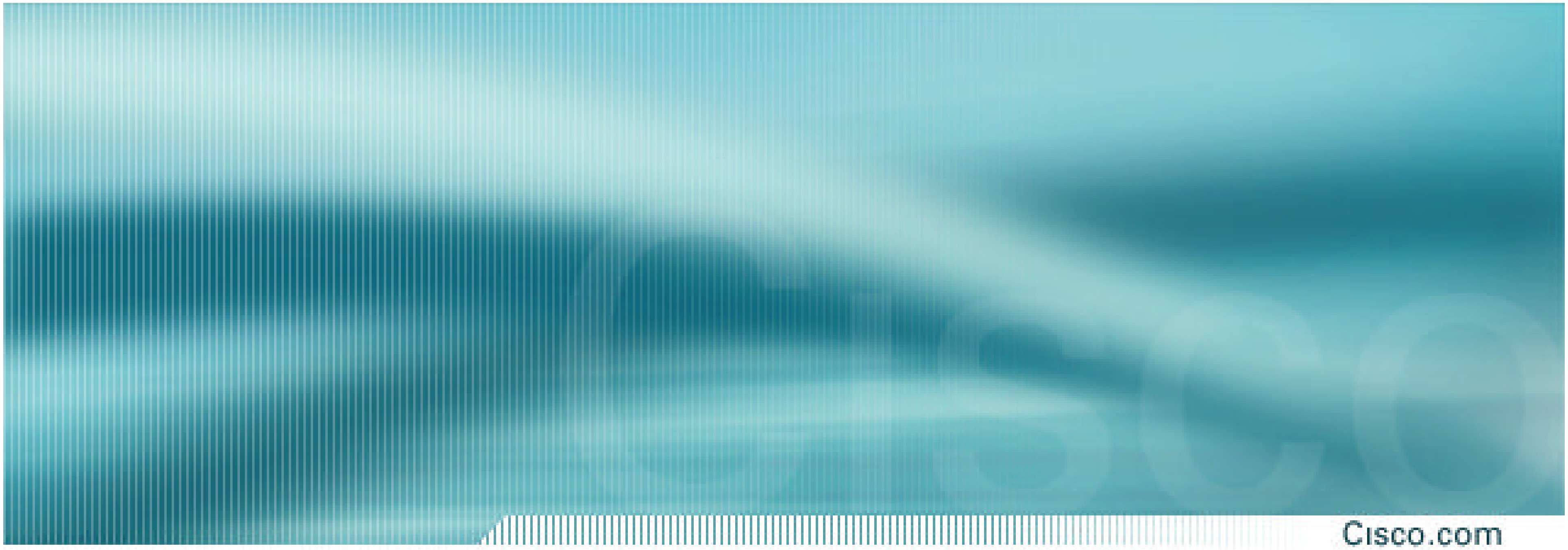
Cisco.com

Phase 1 – Preparation for the Attack

Securing the Router and the Management Plane

Six Phases to ISP Security Incident Response

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



Securing the Router

Router Security

- Routers shipped by vendors have:
  - ✓Default configuration
  - ✓No configured Security
  - ✓Many services switched on to make getting started easier
- Once a router has an IP address, it is accessible to the outside world
  - ✓Campus LAN
  - ✓Company LAN
  - ✓Internet

Global Services You Turn OFF

- Some services turned on by default, should be turned off to save memory and prevent security breaches/attacks
    - ✓ `no service finger`
    - ✓ `no service pad`
    - ✓ `no service udp-small-servers`
    - ✓ `no service tcp-small-servers`
    - ✓ `no ip bootp server`

Global Services You Turn OFF

- Finger
  - ✓Find out who is logged in, from where, how long for
- PAD
  - ✓Historical – from the days of X.25
- Small servers
  - ✓Tcp and udp ports < 20 are for developing IP stacks and not needed in day to day operations
- Bootp
  - ✓Used by systems to bootstrap themselves onto the network – e.g. X-terminals

Interface Services You Turn OFF

- Some IP features are great for campus LANs, but do not make sense on a ISP backbone
- All interfaces on an ISP’s backbone router should have the follow as a default:
  - ✓ `no ip redirects`
  - ✓ `no ip directed-broadcast`
  - ✓ `no ip proxy-arp`

Interface Services You Turn OFF

- IP redirects

  ✓Router will send redirect message if it has to resend a packet through the same interface it was received on

- Direct-broadcast

  ✓If packet intended for network broadcast address, router will physically broadcast it onto the attached network

  ✓The cause of all SMURF attacks on the Internet

- Proxy-arp

  ✓Dumb host sends arp request for destination – documented in RFC1027

  ✓If router knows how to get to that destination, it will install an entry in the arp table for that destination

Cisco Discovery Protocol

- Lets network administrators discover neighbouring Cisco equipment, model numbers and software versions
- Should not be needed on ISP network
  - ✓ `no cdp run`
- Should not be activated on any public facing interface: IXP, customer, upstream ISP – unless part of the peering agreement.
- Disable per interface
  - ✓ `no cdp enable`

Cisco Discovery Protocol

```
alpha>sh cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
beta7200.cisco.com  Ser 1/1        124           R        7206      Ser 2/1
sw2.cisco.com       Eth 1/1        178          T S       WS-C2924M-Fas 0/12
delta.cisco.com     Ser 2/0        146           R        3640      Ser 1/0
gamma.cisco.com     Ser 2/1        138           R        3640      Ser 1/1
```

Cisco Discovery Protocol

```
Defiant#show cdp neighbors detail
-------------------------
Device ID: Excalabur
Entry address(es):
  IP address: 4.1.2.1
Platform: cisco RSP2,  Capabilities: Router
Interface: FastEthernet1/1,  Port ID (outgoing port): FastEthernet4/1/0
Holdtime : 154 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-K3PV-M), Version 12.0(9.5)S, EARLY DEPLOYMENT
   MAINTEN
ANCE INTERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Fri 03-Mar-00 19:28 by htseng

Defiant#
```

Login Banner

- **Use a good login banner, or nothing at all:**

```
banner login ^
  Authorised access only
  This system is the property of Galactic Internet
  Disconnect IMMEDIATELY if you are not an authorised user!
  Contact noc@net.galaxy +99 876 543210 for help.
^
```

Exec Banner

- **Useful to remind logged in users of local conditions:**

```
banner exec ^
  PLEASE NOTE - THIS ROUTER SHOULD NOT HAVE A DEFAULT ROUTE!
  It is used to connect paying peers. These ‘customers’ should
   not be able to default to us.
  The config for this router is NON-STANDARD
  Contact Network Engineering +99 876 543234 for more info.
^
```

Use Enable Secret

- Encryption '7' on a Cisco is reversible
- The “enable secret” password encrypted via a one-way algorithm

```
enable secret <removed>

no enable password

service password-encryption
```

VTY and Console Port Timeouts

- Default idle timeout on async ports is 10 minutes 0 seconds

```
exec-timeout 10 0
```

- Timeout of 0 means permanent connection
- TCP keepalives on incoming network connections

```
service tcp-keepalives-in
```

- Kills unused connections

VTY Security

- Access to VTYs should be controlled, not left open; consoles should be used for last resort admin only:

```
access-list 3 permit 215.17.1.0 0.0.0.255
access-list 3 deny   any
line vty 0 4
 access-class 3 in
 exec-timeout 5 0
 transport input telnet ssh
 transport output none
 transport preferred none
 password 7 045802150C2E
```

VTY Security

- Use more robust ACLs with the logging feature to spot the probes on you network

```
access-list 199 permit tcp 1.2.3.0 0.0.0.255 any
access-list 199 permit tcp 1.2.4.0 0.0.0.255 any
access-list 199 deny   tcp any any range 0 65535
log
access-list 199 deny   ip any any log
```

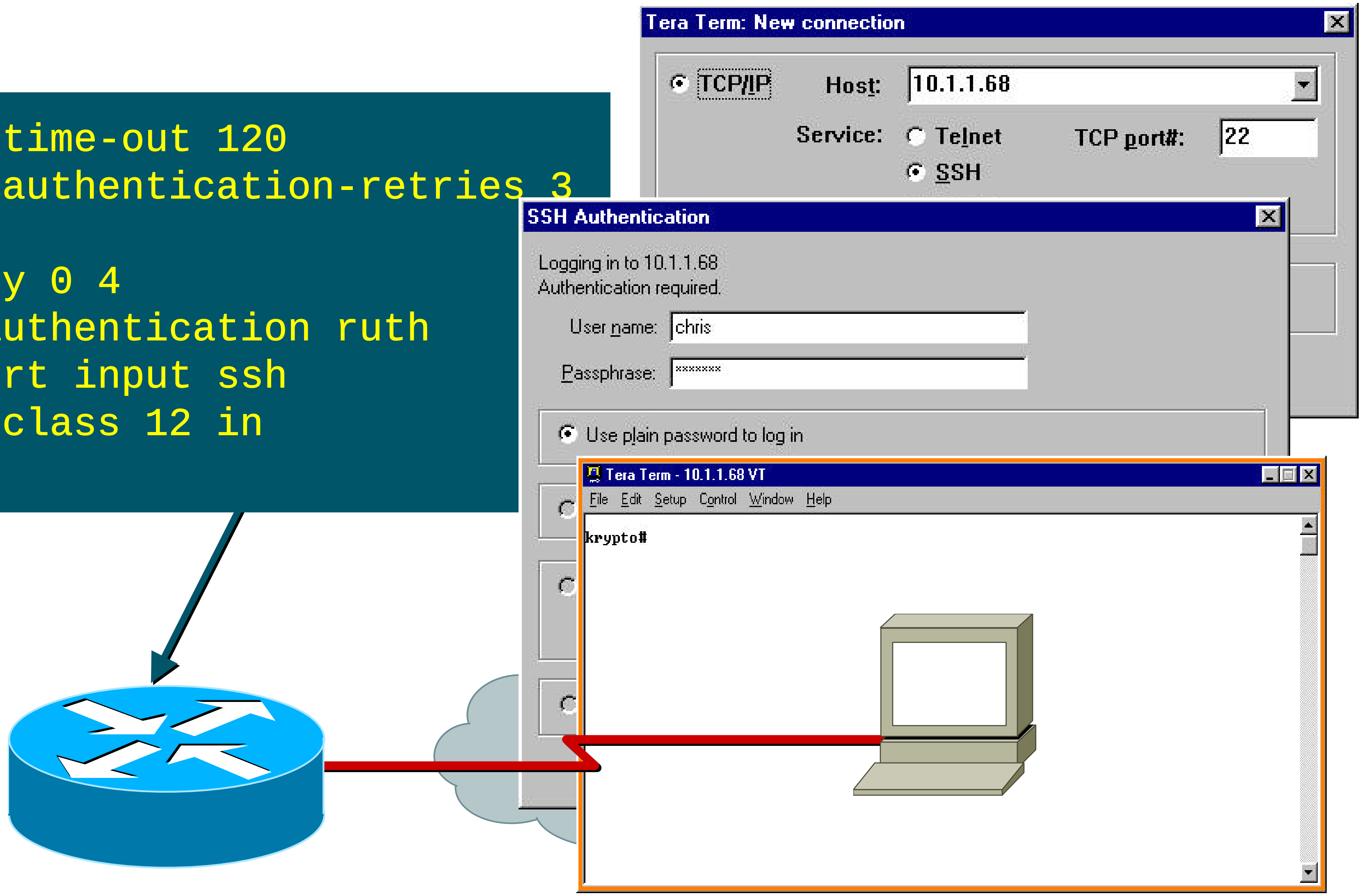
VTY Access and SSHv1

- Secure shell supported as from IOS 12.0S
- Obtain, load and run appropriate crypto images on router
- Set up SSH on router
  - ✓ `Beta7200(config)#crypto key generate rsa`
- Set up the source interface
  - ✓ `ip ssh source-interface`
- Add it as input transport

```
✓ line vty 0 4
✓   transport input telnet ssh
```

Cisco IOS SSH Configuration

```
ip ssh time-out 120
ip ssh authentication-retries 3
!
line vty 0 4
login authentication ruth
transport input ssh
access-class 12 in
```



Tera Term: New connection

● TCP/IP Host: 10.1.1.68

Service: ○ Telnet ● SSH TCP port#: 22

SSH Authentication

Logging in to 10.1.1.68
Authentication required.

User name: chris

Passphrase: *******

● Use plain password to log in

Tera Term - 10.1.1.68 VT

```
krypto#
```

SSHv1 in Cisco Products

Train/ Product	Started In
S	Server—12.0(5)S, Client 12.0(10)S
T	Server—12.1(1)T, Client 12.1(3)T
Mainline	Server and Client—12.2(1)
PIX	Server—5.2
Catalyst Switches	Server—6.1.1 Release for Catalyst 4000, 5000, and 6000 Supervisor
VPN 3000	Server and Client—Release 3.0

VTY Access and SSHv1

- **SSHv1 client in IOS for router to router SSH (not in docs)**

  ssh [-l <userid>] [-c <des|3des>] [-o numberofpasswdprompts <n>] [-p <portnum>] <ipaddr|hostname> [<IOS command>]

where

-l <userid> is the user to login as on the remote machine. Default is the current user id.

-c <des|3des> specifies the cipher to use for encrypting the session. Triple des is encrypt-decrypt-encrypt with three different keys. The default is 3des if this algorithm is included in the image, else the default is des.

-o specifies the options which is currently one only numberofpasswdprompts <n> specifies the number of password prompts before ending the attempted session. The server also limits the number of attempts to 5 so it is useless to set this value larger than 5. Therefore the range is set at 1-5 and the default is 3 which is also the IOS server default.

-p <portnum> Port to connect to on the remote host. Default is 22.

<ipaddr|hostname> is the remote machine ip address or hostname

<IOS command> is an IOS exec command enclosed in quotes (ie "). This will be executed on connection and then the connection will be terminated when the command has completed.

VTY Access and SSHv1

- **Example:**
  - ✓ Insure you have the proper image (post 12.0(10)S with “k3pv”

    ```
    i.e. rsp-k3pv-mz.120-11.S3.bin
    ```

  - ✓ Set up SSH on the router

    ```
    Beta7200(config)#crypto key generate rsa
    ```

  - ✓ Use the SSH client:

    ```
    ssh -l myuser myhost "sh users"
    ssh -l myuser -c 3des -o 5 -p 22 myhost
    ```

User Authentication

- Account per user, with passwords

```
aaa new-model
aaa authentication login neteng local
username joe password 7 1104181051B1
username jim password 7 0317B21895FE
line vty 0 4
 login neteng
 access-class 199 in
```

- Username/password is more resistant to attack than a plain password

User Authentication

- Use distributed authentication system
  - ✓ RADIUS—Recommended for user accounting
  - ✓ TACACS+—Recommended for securing the network

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa accounting exec start-stop tacacs+
ip tacacs source-interface Loopback0
tacacs-server host 215.17.1.1
tacacs-server key CKr3t#
line vty 0 4
 access-class 3 in
```

User Authentication

TACACS+ Provides a Detailed Audit Trail of what Is Happening on the Network Devices

User-Name	Group-cmd		priv-lvl	service	NAS-Portname	task_id	NAS-IP-reason
bgreene	NOC	enable <cr>	0	shell	tty0	4	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	5	210.210.51.224
bgreene	NOC	no aaa accounting exec Workshop <cr>	0	shell	tty0	6	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	8	210.210.51.224
pfs	NOC	enable <cr>	0	shell	tty0	11	210.210.51.224
pfs	NOC	exit <cr>	0	shell	tty0	12	210.210.51.224
bgreene	NOC	enable <cr>	0	shell	tty0	14	210.210.51.224
bgreene	NOC	show accounting <cr>	15	shell	tty0	16	210.210.51.224
bgreene	NOC	write terminal <cr>	15	shell	tty0	17	210.210.51.224
bgreene	NOC	configure <cr>	15	shell	tty0	18	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	20	210.210.51.224
bgreene	NOC	write terminal <cr>	15	shell	tty0	21	210.210.51.224
bgreene	NOC	configure <cr>	15	shell	tty0	22	210.210.51.224
bgreene	NOC	aaa new-model <cr>	15	shell	tty0	23	210.210.51.224
bgreene	NOC	aaa authorization commands 0 default tacacs+ none <cr>	15	shell	tty0	24	210.210.51.224
bgreene	NOC	exit <cr>	0	shell	tty0	25	210.210.51.224
bgreene	NOC	ping <cr>	15	shell	tty0	32	210.210.51.224
bgreene	NOC	show running-config <cr>	15	shell	tty66	35	210.210.51.224
bgreene	NOC	router ospf 210 <cr>	15	shell	tty66	45	210.210.51.224
bgreene	NOC	debug ip ospf events <cr>	15	shell	tty66	46	210.210.51.224

User Authentication

- Ideally, when you have TACACS+ on a router, you do not give out the local username/ password nor enable password
  - ✓ Lock them in a safe in the NOC in case of total TACACS+ failure
- Problem—username/password is a reversible hash
  - ✓ Some engineer can take a config an reverse the hash
- Threat—disgruntled employees can attack TACACS+ then get into the routers

User Authentication

- **Fix is in CSCds84754**

  ✓**Added simple MD5 Encryption mechanism for username password:**

  ✓`username barry secret 5 ;2kj45nk5jnt43`

- **Now MD5 Encrypted username/passwords can be used with TACACS+ to keep the system secure from the internal security threat.**

User Authentication

- So now you can have the following:

```
aaa new-model
aaa authentication login default tacacs+ local
enable
aaa authentication enable default tacacs+ local
enable
aaa accounting exec start-stop tacacs+
ip tacacs source-interface Loopback0
tacacs-server host 215.17.1.1
tacacs-server key CKr3t#
line vty 0 4
 access-class 3 in
username joe password 6 1104181051B1
username jim password 6 0317B21895FE
```

TACACS+ URLs

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

Source Routing

- IP has a provision to allow source IP host to specify route through Internet
- ISPs should turn this off, unless it is specifically required:
  - ✓`no ip source-route`
- *traceroute-s* to investigate network failures—valuable tool; but, it you are not using *traceroute-s*, then turn off the feature!

ICMP Unreachable Overload

- Originally, all ICMP Unreachable replies were *punted* from the LC/VIP to the GRP/RP.
- The result was that the GRP/RP's CPU resources could be overloaded, just responding to ICMP Unreachables.
- *Potential Security Hole* that can be used to overload a router.
- Prevented Black Hole Filtering on Router.

ICMP Unreachable Overload

- **Problem resolved across the the LC/VIP based platforms:**

  `CSCds36541 - Traffic received on eng1 LC for null0 punted to RP`

  `CSCdr46528 - GSR eng0 LC: routes for Null0 have terrible lookup performance`

  `CSCdt66560 - Engine 2 PSA Punts Null0 Traffic to GRP`

  `CSCdt68393 - 100% CPU using Null0 to blackhole traffic under DOS`

- **All LCs and VIPs now handle the ICMP Unreachables and the *no ip unreachables* command works on all interfaces.**

ICMP Unreachable Overload

- All Routers who use any static route to Null0 should put *no ip unreachables (i.e. BGP Advertisements).*

```
interface Null0
 no ip unreachables
!
ip route <dest to drop> <mask> Null0
```

ICMP Unreachable Rate-Limiting

- New ICMP Unreachable Rate-Limiting Command:

```
ip icmp rate-limit unreachable [DF] <1-4294967295
  millisecond>

no ip icmp rate-limit unreachable [df]
```

- Turned on by default and hidden since 12.0(8)S. Default value set to 500 milliseconds.
- Peer Review with several top ISP operations engineers are recommending this be set at 2 seconds for normal and DF.

Tip: scheduler allocate

- **Schedules CPU time spent on processes versus interrupts**

Syntax:

```
scheduler allocate <interrupt> <processes>
```

<*interrupt*>: 3000-60000 Microseconds handling network interrupts

<*processes*>: 1000-8000 Microseconds running processes

Example:

```
router(config)#scheduler allocate 8000 8000
```

Very useful under heavy load!
Recommended Standard Config!

Introducing a New Router to the Network

Introducing a New Router to the Network

- **Network devices never come out of the box with a *secure* configuration.**
- **ISPs should be mindful of this fact – preparing the device before it goes live on the Network.**
  - ✓ **Hot Stage and Pre-configure the Device before deployment.**
  - ✓ **Create a *secure configuration template* to be applied when the router first comes on-line (or during a recovery phase during an outage)**

Introducing a new Router to the Network

1. Set hostname
2. Set passwords
    1. Enable secret and temporary vty passwords
3. Disable unnecessary services
    1. Global and per interface
4. Configure access-lists
    1. For vty and snmp access
    2. For live interfaces (if required)
5. Only now assign IP address and plug into network

Introducing a new Router to the Network

6. Configure TACACS+
   - Remove local vty passwords
7. Configure NTP and Logging
8. Configure SNMP (if required)
   - Check access and what is being monitored
9. Configure remaining interfaces
10. Configure routing protocols
    - Include any necessary inbound and outbound filters
11. Confirm router security on network
    - Tools like SAINT are very useful

Secure Template Sources

- ISP Essentials Materials (Security and Operational Practices)

  http://www.cisco.com/public/cons/isp/essentials/

  http://www.ispbook.com

- Improving Security on Cisco Routers

  http://www.cisco.com/warp/public/707/21.html

- Rob Thomas's Secure Configuration Templates

  http://www.cymru.com/~robt/Docs/Articles/index.html

- US National Security Agency's

  http://nsa1.www.conxion.com/cisco/download.htm

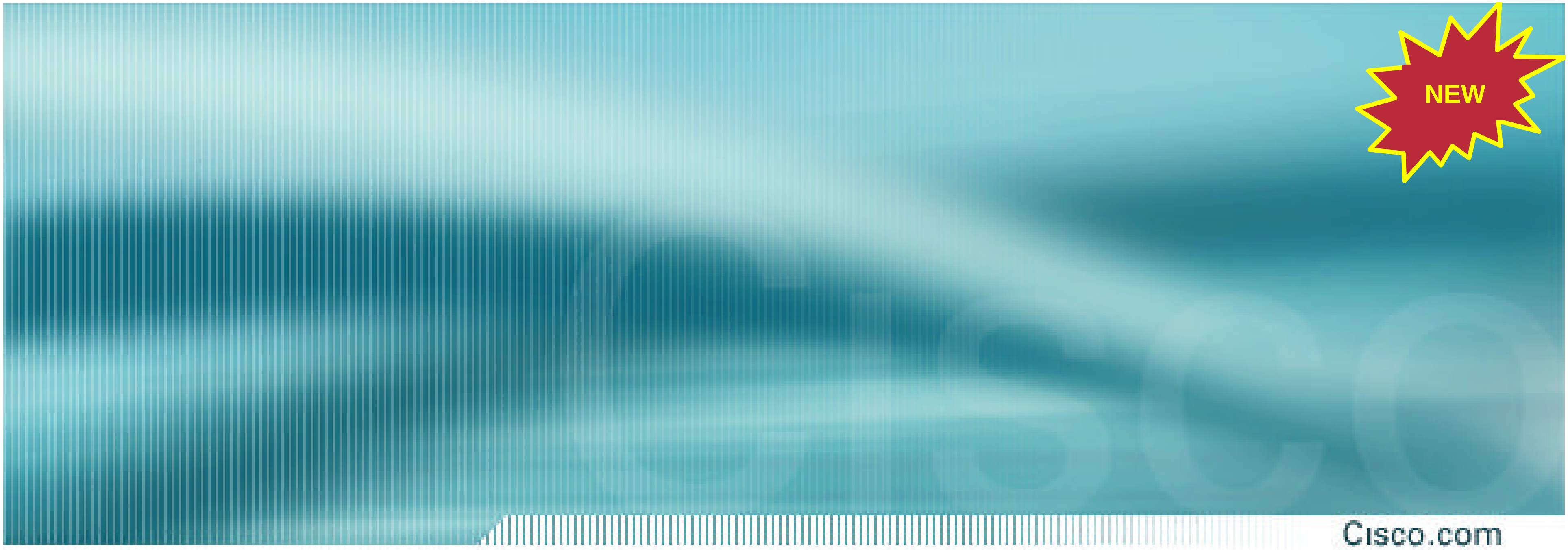
Summary

- These hints apply to routers (and switches, and any other IP infrastructure device)

- May be software release dependent

  ✓But do your research so that only necessary services are left running on the router

  ✓Beware “convenient vendor defaults” – often they are a major cause of security problems on any network



Input Hold Queue

Input Hold Queue

NEW

Cisco.com

- The is the queue that stores packets destined for the router.
- If there are to many packets, the route stores them in the input hold queue.
- Input Hold Queue is important for intial BGP convergence (when your sending the full table)
- DOS/DDOS attacks against the router can fill the input hold queue – knocking out legitimate packets.

Input Hold Queue

NEW

- Input Hold Queue is physically on the Route Processor (RP for 7500, GRP for 12000).
- Default is 75.
- Recommend 1500 (Check memory before applying – looking for 20M free)
- Applied to all interfaces

```
    interface XXXXXX
      hold-queue 1500 in
```

Input Hold Queue

NEW

```
12008-e10-2#sh inter pos 5/0
POS5/0 is up, line protocol is up
.
  Output queue 0/40, 0 drops; input queue 97/1500, 54 drops
  5 minute input rate 76502000 bits/sec, 31139 packets/sec
  5 minute output rate 72517000 bits/sec, 26560 packets/sec
.
.
```

26Mbps DOS on port 179 – non-successful spoof

Selective Packet Discard

Selective Packet Discard (SPD)

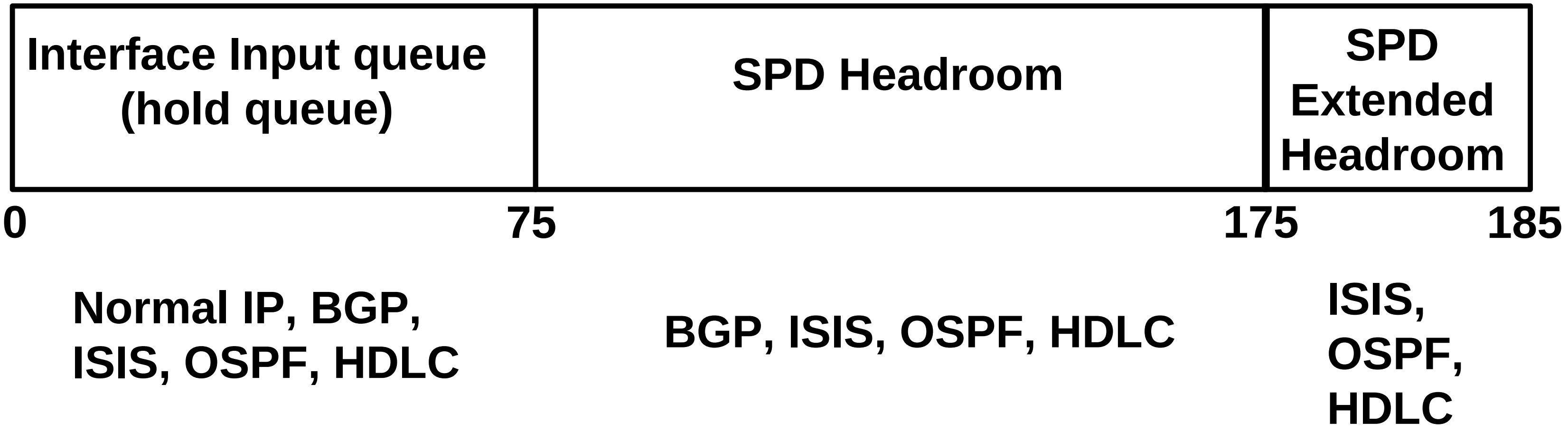
- When a link goes to a saturated state, you will drop packets; the problem is that you will drop any type of packets—including your routing protocols
- Selective Packet Discard (SPD) will attempt to drop non-routing packets instead of routing packets when the link is overloaded
  - ✓ `ip spd enable (11.1 CA & CC)`

Selective Packet Discard (SPD)

- Software Switching – SPD allows Control & Management Plane Traffic destined for the router to not get dropped when a circuit gets saturated.
- ASIC Switching – SPD allows a deeper buffer for the Control & Management Plane Traffic destined for the router – added resistance to direct DOS Attacks and buffer room for surges in control plane traffic (i.e. times of convergence).

Selective Packet Discard (SPD)

- Input Hold Queue (default 75)
- SPD Headroom (default 100)
- SPD Extended Headroom (default 10)



Interface Input queue (hold queue)

SPD Headroom

SPD Extended Headroom

0

75

175

185

Normal IP, BGP, ISIS, OSPF, HDLC

BGP, ISIS, OSPF, HDLC

ISIS, OSPF, HDLC

Selective Packet Discard

- Enabled by default from 11.2(5)P and later releases, available option in 11.1CA/CC
- 12.0 the syntax changes and the default is to enable SPD

SPD Aggressive Mode

- Attack of IP packets with bad TTL are processed switched with ICMP reply—crippling the router. Needed a way to aggressively drop these packets – leaving room for the normal Control/Management Plane traffic.

```
ip spd mode aggressive
```

Selective Packet Discard

- **Recommended Settings:**
  - ✓ **`ip spd headroom 1000` Default is 100. Experience shows that the higher settings help.**
  - ✓ **`ip spd mode aggressive` Does not work on the GSR – but does on other platforms.**

SPD Caveats and DDTS

- **CSCdu05363 - SPD Queueing is broken on GSR.**
  - ✓ **Resolved in 12.0(20.04)SP, 12.0(17)ST04, 12.0(19)S01, 12.0(20.02)ST, & 12.0(20.02)S**

Monitoring SPD Queues

- A - Throttle Count
- B - Input Drops (sum of all types of drops)
- C - Input Drops when external SPD is used (SSE)
- D - Packets dropped by SPD
- E - Flushes by the SSE.
- F - Aggressive Drops in SPD when in aggressive mode.
- G - Number of priority packets received.
- H - Number of priority packets dropped (either priority IP packets, either keepalives or ISIS packets).

```
GSR-2#sh interface pos 0/0 switching
POS0/0 Link to GSR#1
          Throttle count          Ⓐ
        Drops         RP          Ⓑ         SP           Ⓒ
  SPD Flushes       Fast          Ⓓ        SSE           Ⓔ
  SPD Aggress       Fast          Ⓕ
 SPD Priority     Inputs          Ⓖ      Drops           Ⓗ
```

Monitoring SPD Queues

- **You have a problem when you:**
  - ✓ **See the number of priority packets drop (H)**
  - ✓ **See the Fast Flushes increase.**

```
GSR-2#sh interface pos 0/0 switching
POS0/0 Link to GSR#1
          Throttle count          Ⓐ
        Drops         RP          Ⓑ         SP          Ⓒ
  SPD Flushes       Fast          Ⓓ        SSE          Ⓔ
  SPD Aggress       Fast          Ⓕ
 SPD Priority     Inputs          Ⓖ      Drops          Ⓗ
```

Monitoring SPD Modes

- **SPD has three drop modes:**
  - ✓ **NORMAL - Everything is *hunky dory***
  - ✓ **RANDOM - *min threshold* has been reached**
  - ✓ **MAX - *max threshold* has been reached**
- **There is a problem when *Current Mode* is in MAX.**

```
GSR-2#sh ip spd

Current mode: normal.

Queue min/max thresholds: 73/100, Headroom: 1000,
Extended Headroom: 100

IP normal queue: 0, priority queue: 0.

SPD special drop mode: aggressively drop bad packets
```

Open Ports on a Router

What Ports Are open on the Router?

- It may be useful to see what sockets/ports are open on the router
- *Show ip sockets* – show some of the UDP ports opened.

```
7206-UUNET-SJ#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY
OutputIF
 17 192.190.224.195   162 204.178.123.178  2168   0   0    0   0
 17   --listen--          204.178.123.178    67   0   0    9   0
 17 0.0.0.0           123 204.178.123.178   123   0   0    1   0

 17 0.0.0.0             0 204.178.123.178   161   0   0    1   0
```

What Ports Are open on the Router?

- Two steps required for TCP ports:
  - ✓ show tcp brief all
  - ✓ show tcp tcb

```
GSR-1#sh tcp bri all
TCB         Local Address            Foreign Address       (state)
52F6D218    60.20.1.2.11002          60.20.1.1.179         ESTAB
52F7065C    50.20.1.1.179            50.20.1.2.11007       ESTAB
52F6CD8C    *.*                      *.*                   LISTEN
537D0944    *.179                    60.20.1.1.*           LISTEN
537CE2C4    *.179                    50.20.1.2.*           LISTEN
```

What Ports Are open on the Router?

- Take the TCB you want more information on and use the *show tcp tcb* command:

```
GSR-1#sh tcp tcb 52F7065C

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Local host: 50.20.1.1, Local port: 179

Foreign host: 50.20.1.2, Foreign port: 11007


Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0
bytes)

.

.
```

Security Audit Tools/Port Scanners

NEW

- IOS give many false positives.
- Ports are perceived to be open when often they are not connected to a service.
- Varies with IOS Version and Audit Tool
- ION is cleaning this up.
- Request – when you find them, please open a Bug (DDTS). Worst that can happen is that the Bug will be a duplicate.

Protect the Cisco 12000’s GRP

Receive Path ACL

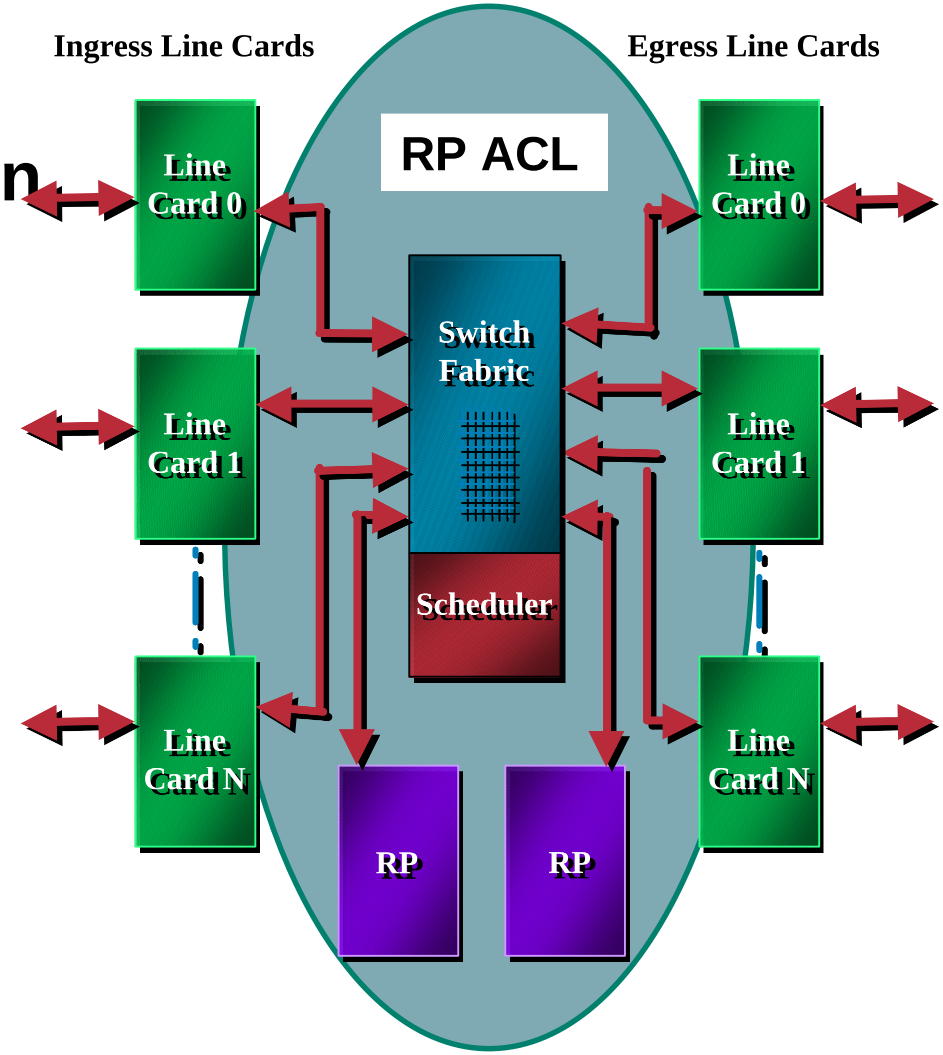
- Packets with a destination address for any interface on the router is punted out of the forwarding path as a *receive adjacency*.
- The receive path (queues, buffers, processing capacity, etc) is one of the areas on a router that can be overloaded in a DOS/DDOS attack on a router.
- Receive Path ACL

  ✓Official release – 12.0(22)S

  ✓Special Waiver granted for 12.0(21)S2 maintenance throttle. Maintenance throttles are not to have new features, but core ISP customers and PSIRT asked for the waiver in the best interest of the Internet.

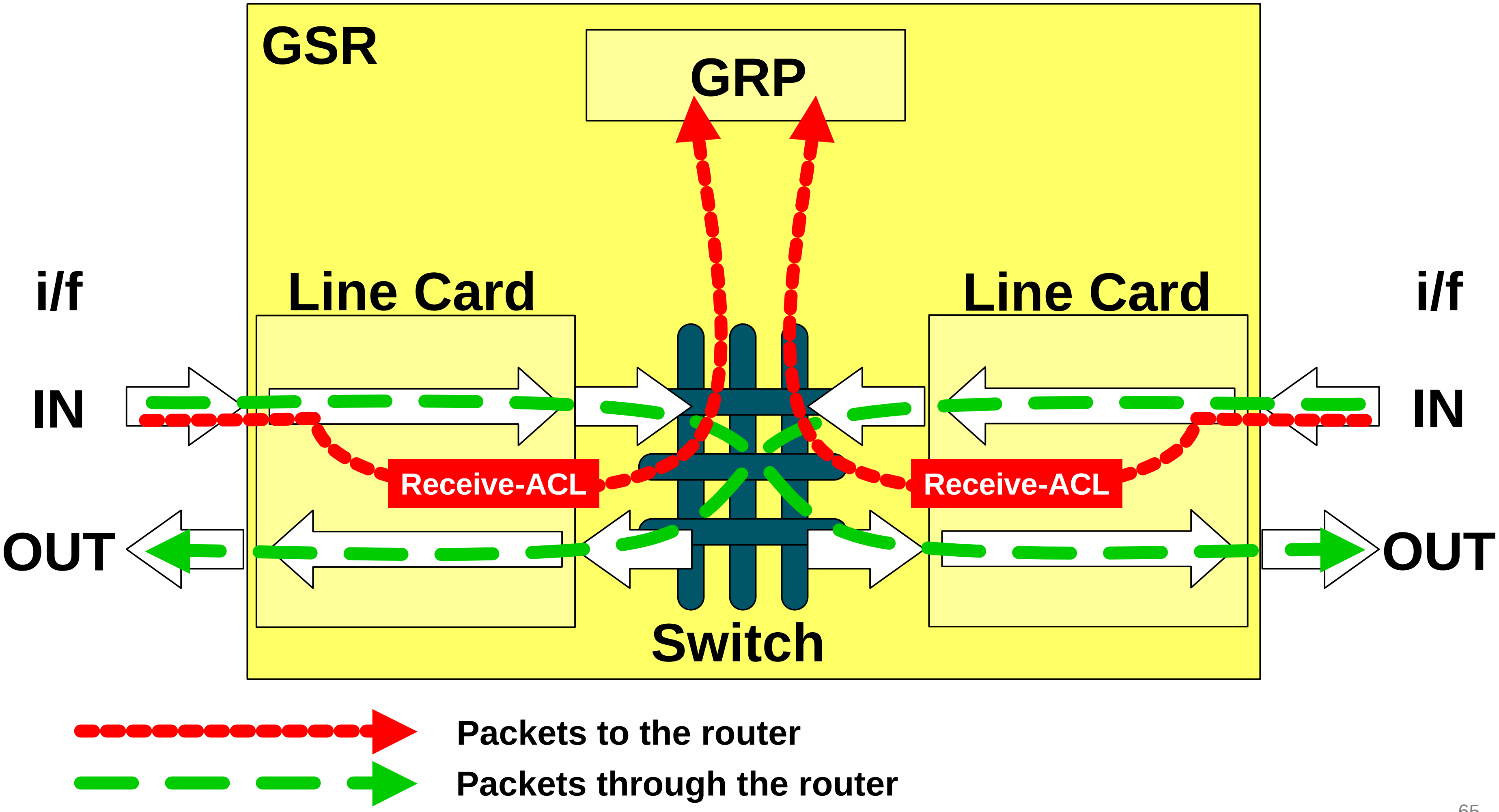
Receive Path ACL

- Standard, Extended, or Turbo ACL is created on the GRP. This ACL is then pushed down to all the Line Card's CPU.
- The ACL is executed on all receive adjacency packets before they are queued to be sent to the GRP.
- Cisco 12XXX first, then other platforms.



Receive Path ACLs (currently in beta on 12.0(20)S)

[no] ip receive access-list <num>



RP ACL – What's Next?

- Move to 7500, 10000, and other platforms.
- Add a Rate Limit Function
  - ✓ ACLs can and will be spoofed.

Administrative and Operational Practices

Administrative and Operational Practices

- Configuration hints to aid security
  - ✓ Router features
  - ✓ Network features
  - ✓ Operational practices

Loopback Interface

- Most ISPs make use of the router loopback interface
- IP address configured is a host address
- Configuration example:

```
interface loopback 0
 description Loopback Interface of CORE-GW3
 ip address 215.18.3.34 255.255.255.255
 no ip redirects
```

Loopback Interface

- Loopback interfaces on ISP backbone usually numbered:

  ✓Out of one contiguous block, or

  ✓Using a geographical scheme, or

  ✓Using a per PoP scheme

- Aim is to increase network stability, aid administration, and improve security

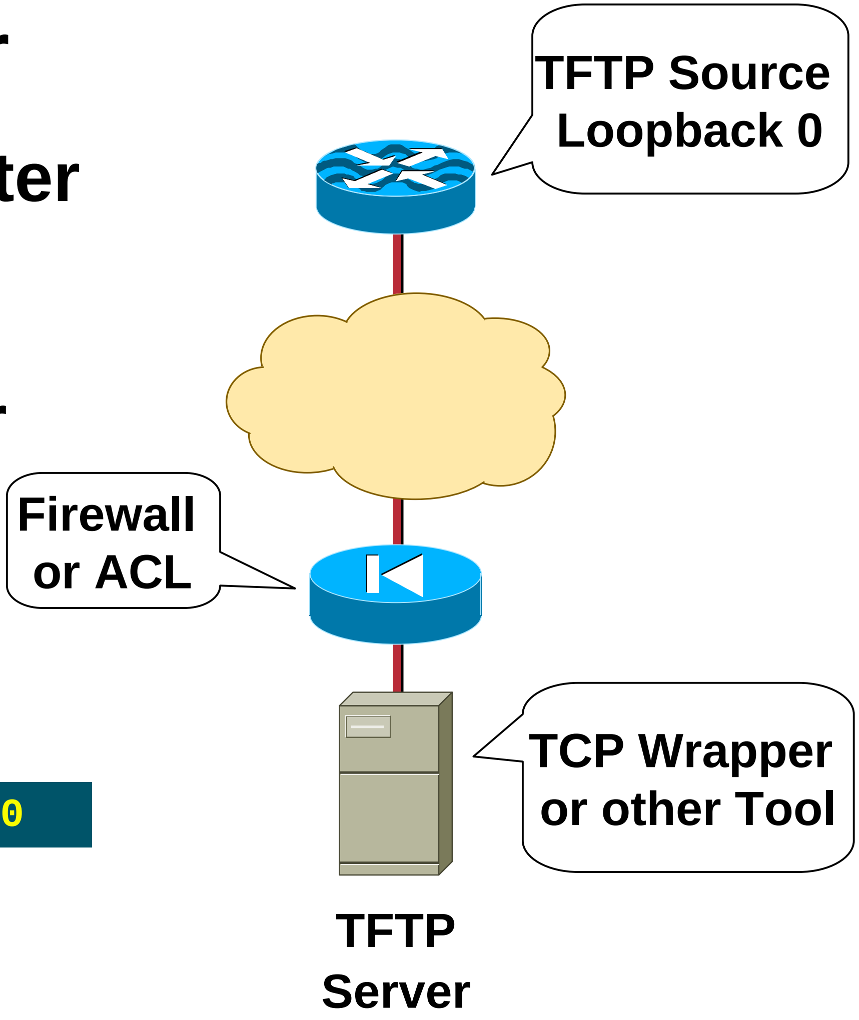
Configuration Management

- Backup NVRAM configuration off the router:
  - ✓Write configuration to TFTP server
  - ✓TFTP server files kept under revision control
  - ✓Router configuration built from master database
- Allows rapid recovery in case of emergency

Configuration Management

- Secure the TFTP server
  - ✓ TFTP loopback 0 on router
  - ✓ Firewall/ACL
  - ✓ Wrapper on TFTP server which only allows the router's loopback address

```
ip tftp source-interface Loopback0
```



FTP Client Support

- TFTP has its limitations
- FTP client support is added in IOS 12.0; this allows for FTP upload/downloads
- Remember to use the same security/redundancy options with loopback 0:

```
ip ftp source-interface loopback 0
```

FTP Client Support

```
7206-AboveNet-SJ2#copy ftp://bgreene:XXX@ftp.cisco.com slot0:

Source filename []? /cisco/ios/12.0/12.0.9S/7200/c7200-k3p-
mz.120-9.S.bin

Destination filename [c7200-k3p-mz.120-9.S.bin]?

Accessing ftp://bgreene:XXX@ftp.cisco.com
//cisco/ios/12.0/12.0.9S/7200/c7200-k3p-mz.120-
9.S.bin...Translating "ftp.cisco.com"...domain server
(207.126.96.162) [OK]


Loading /cisco/ios/12.0/12.0.9S/7200/c7200-k3p-mz.120-9.S.bin
```

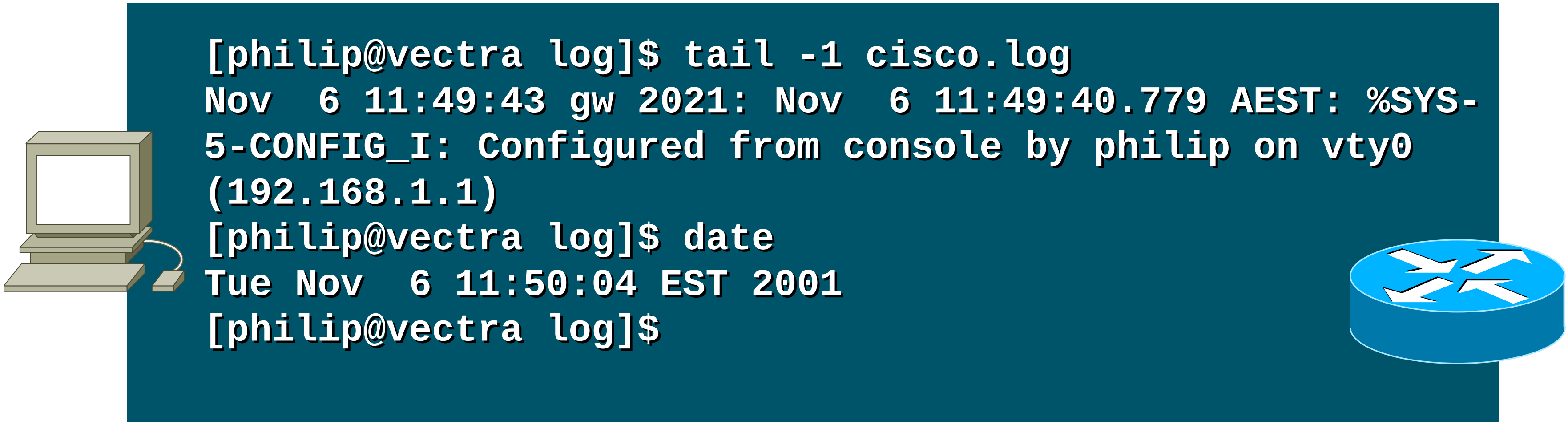
Use Detailed Logging

- **Off load logging information to a logging server**
- **Use the full detailed logging features to keep exact details of the activities**

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging buffered 16384
logging trap debugging
logging facility local7
logging 169.223.32.1
logging 169.223.55.37
logging source-interface loopback0
no logging console  ! Recommended - keeps the console port free
```

Use Detailed Logging

- Two topologies used:
  - ✓ Central Syslog servers in operations center
  - ✓ Syslog servers in major POPs



```
[philip@vectra log]$ tail -1 cisco.log
Nov  6 11:49:43 gw 2021: Nov  6 11:49:40.779 AEST: %SYS-
5-CONFIG_I: Configured from console by philip on vty0
(192.168.1.1)
[philip@vectra log]$ date
Tue Nov  6 11:50:04 EST 2001
[philip@vectra log]$
```

Network Time Protocol

- If you want to cross compare logs, you need to synchronize the time on all the devices
- Use NTP

  ✓From external time source

  Upstream ISP, Internet, GPS, atomic clock

  ✓From internal time source

  ✓Router can act as *stratum 1* time source

Network Time Protocol

- Set timezone

```
clock timezone <name> [+/-hours [mins]]
```

- Router as source

```
ntp master 1
```

- External time source (master)

```
ntp server a.b.c.d
```

- External time source (equivalent)

```
ntp peer e.f.g.h
```

Network Time Protocol

- Example configuration:

```
clock timezone AEST 10
ntp update-calendar
ntp source loopback0
ntp server <other time source>
ntp peer <other time source>
ntp peer <other time source>
```

Network Time Protocol

- Network Time Protocol (NTP) used to synchronize the time on all the devices
- NTP packets leave router with loopback address as source
- Configuration example:

```
ntp source loopback0
ntp server 169.223.1.1 source loopback 1
```

Network Time Protocol

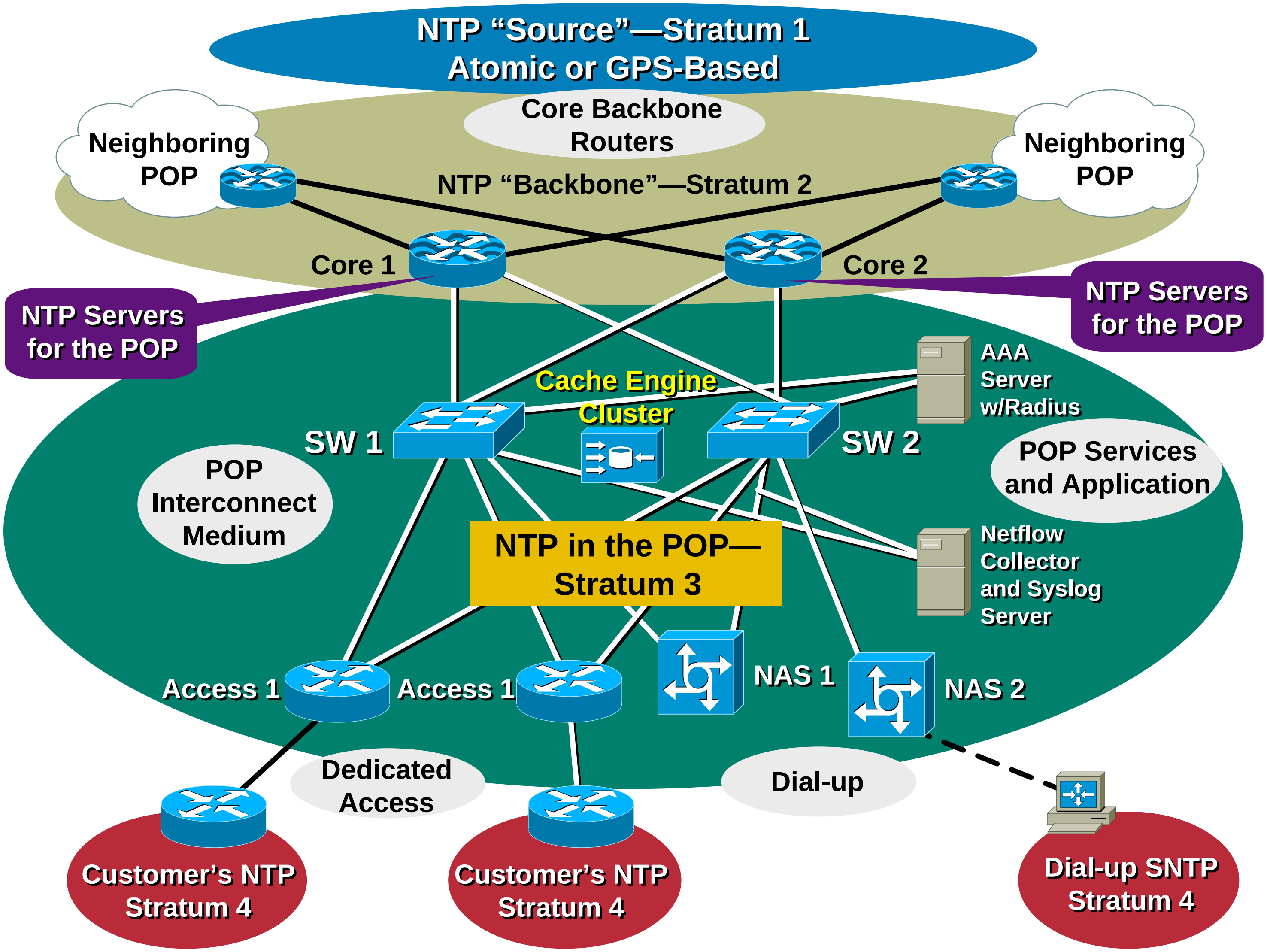
- **Motivation—NTP security:**

  ✓NTP systems can be protected by filters which only allow the NTP port to be accessed from the loopback address block

- **Motivation—easy to understand NTP peerings:**

  ✓NTP associations have the loopback address recorded as source address, not the egress interface

Network Time Protocol



Network Time Protocol

- Where to get NTP reference sources?
  - ✓ http://www.eecis.udel.edu/~ntp/hardware.html

- Attach a Telecom Solutions GPS clock to the router’s AUX port:

```
Excalabur(config)#line aux 0
Excalabur(config-line)#ntp refclock telecom-solutions pps ?
  cts   PPS on CTS
  none  No PPS signal available
  ri    PPS on RI
```

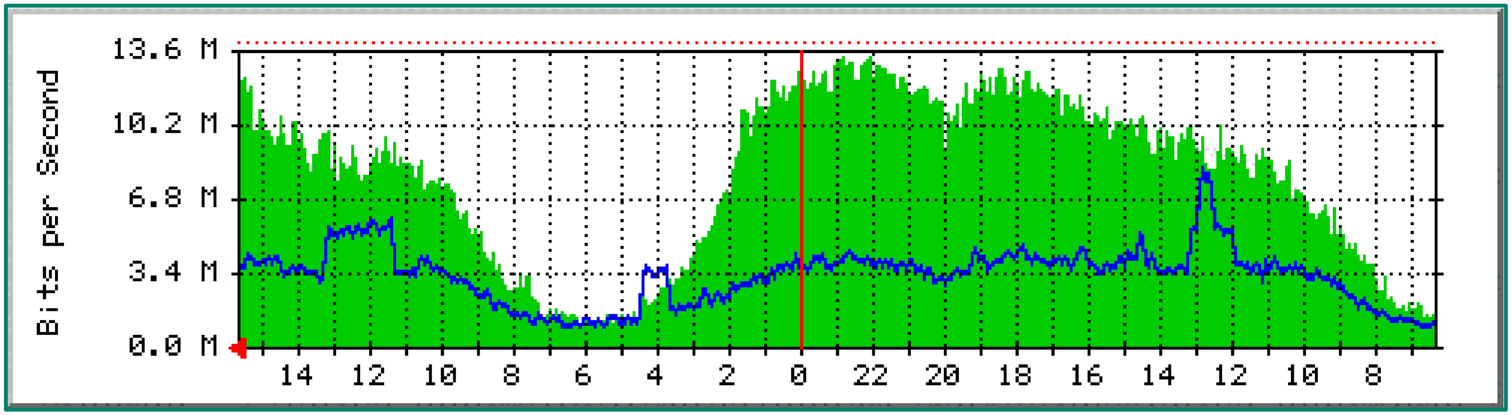
SNMPv1

- **Remove any SNMP commands if SNMP is not going to be used**
- **If SNMP is going to be used:**

```
access-list 98 permit 169.223.1.1
access-list 98 deny   any
snmp-server community 5nmc02m RO 98
snmp-server trap-source Loopback0
snmp-server trap-authentication
snmp-server host 169.223.1.1 5nmc02m
```

SNMPv1

- Recommend that all ISPs aggressively and consistently monitor their network
- Despite SNMPv2 and SNMPv3, most ISPs are still using SNMPv1 (personal observation)
- SNMPv3 supported since 12.0(6)S



HTTP Server

- HTTP server in Cisco IOS from 11.1CC and 12.0S
  - ✓ Router configuration via web interface
- Disable if not going to be used (disabled by default):

```
no ip http server
```

- Configure securely if going to be used:

```
ip http server
ip http port 8765
ip http authentication aaa
ip http access-class <1-99>
```

Core Dumps

- Cisco routers have a core dump feature that will allow ISPs to transfer a copy of the core dump to a specific FTP server
- Set up a FTP account on the server the router will send the core dump to
- The server should NOT be a public server
  - ✓Use filters and secure accounts
  - ✓Locate in NOC with NOC staff access only
  - ✓Enough disk space to handle the dumps

Core Dumps

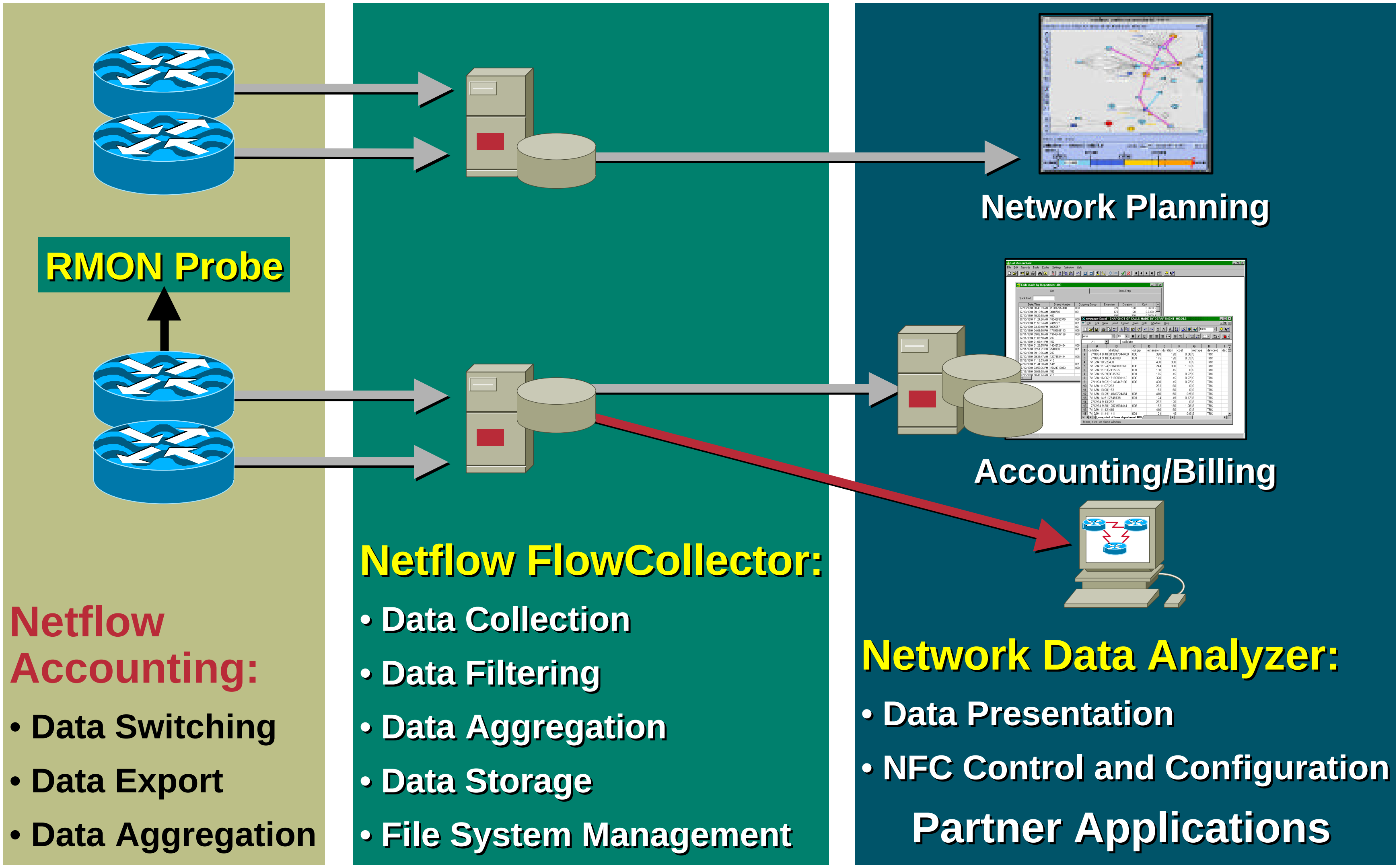
- **Example configuration:**

```
ip ftp username cisco
ip ftp password 7 045802150C2E
ip ftp source-interface loopback 0
exception protocol ftp
exception dump 169.223.32.1
```

Netflow

- Providers network administrators with “packet flow” information
- Allows:
  - ✓Security monitoring
  - ✓Network management and planning
  - ✓Customer billing
  - ✓Traffic flow analysis
- Available from 11.1CC for 7x00 and 12.0 for remaining router platforms

Netflow Infrastructure



Netflow Accounting:

- Data Switching
- Data Export
- Data Aggregation

Netflow FlowCollector:

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

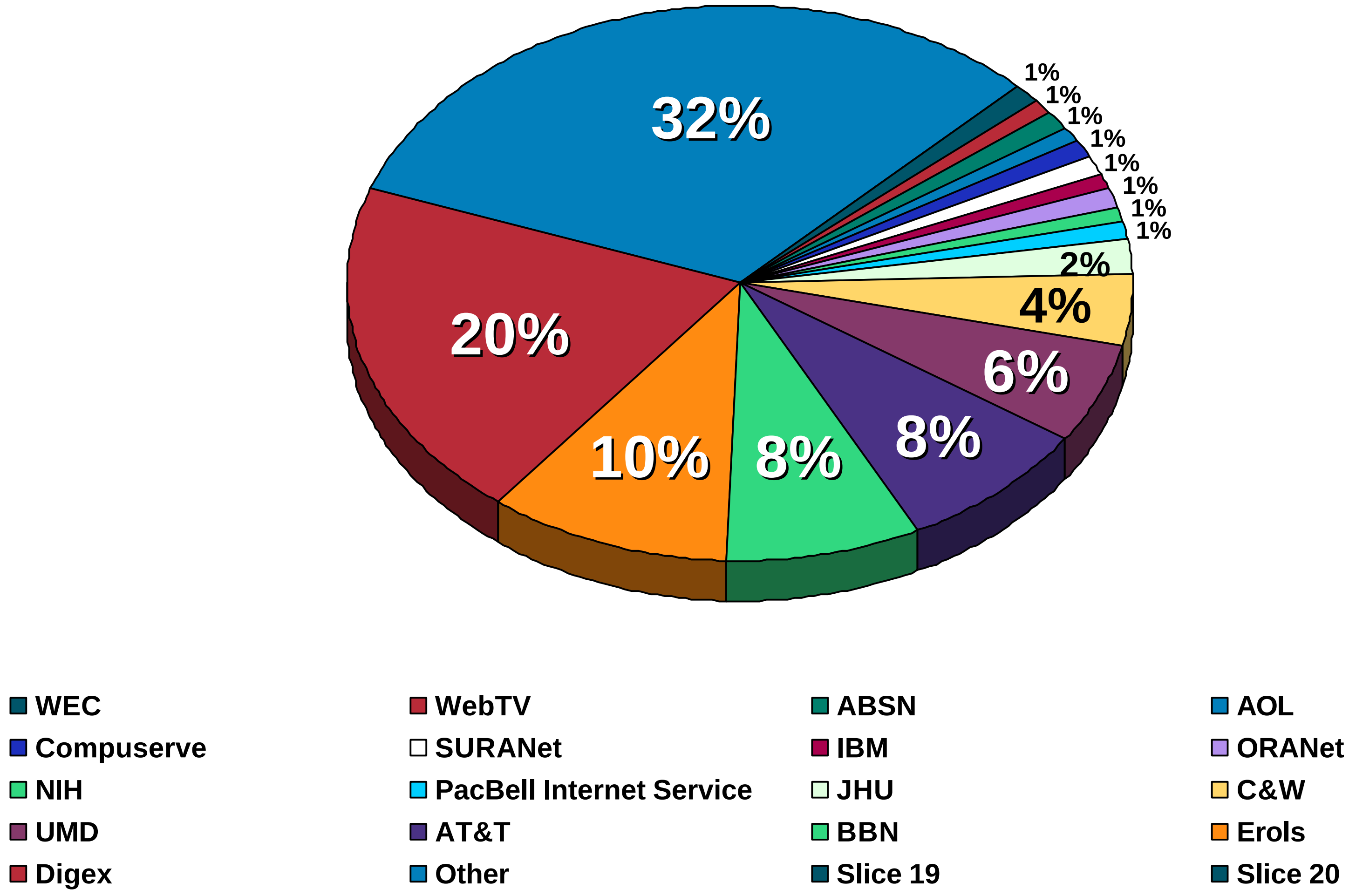
Network Data Analyzer:

- Data Presentation
- NFC Control and Configuration

Partner Applications

Netflow—Capacity Planning

Public Routers 1, 2, 3 Month of September Outbound Traffic



Netflow

- Configuration example:
  - ✓ `interface serial 5/0`
  - ✓ `ip route-cache flow`
- If CEF not configured, Netflow enhances existing switching path (i.e. optimum switching)
- If CEF configured, Netflow becomes a flow information gatherer and feature acceleration tool

Netflow

- Information export:
  - ✓ Router to collector system

    ```
    ✓ ip flow-export version 5 [origin-as|peer-as]
    ✓ ip flow-export destination x.x.x.x <udp-port>
    ```

- Flow aggregation (new in 12.0S):
  - ✓ Router sends aggregate records to collector system

    ```
    ✓ ip flow-aggregation cache as|prefix|dest|source|proto
    ✓   enabled
    ✓   export destination x.x.x.x <udp-port>
    ```

Netflow—Simple Monitoring

- **Sample output on router:**

```
Beta-7200-2>sh ip cache flow
IP packet size distribution (14280M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .145 .403 .101 .178 .105 .017 .005 .003 .001 .000 .000 .000 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .000 .025 .001 .004 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  14369 active, 51167 inactive, 253731473 added
  1582853980 ager polls, 0 flow alloc failures
  last clearing of statistics 16w5d
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet       28284      0.0        36    71      0.2      13.4      17.7
TCP-FTP         171390      0.0        15    63      0.6       8.1      16.6
TCP-FTPD        104030      0.0       693   384     16.8      29.7       9.7
TCP-WWW       28119533      6.5        17   290    115.8       6.5      10.9
TCP-SMTP       3615725      0.8        18   266     15.7       5.6      15.5
TCP-X             1649      0.0         3    84      0.0       4.1      14.0
TCP-BGP        1483900      0.3         5   258      1.7      13.1      19.1
TCP-NNTP          2330      0.0         2    53      0.0       8.4      20.7
TCP-Frag           484      0.0         1    46      0.0       1.2      20.9
TCP-other    343437823     79.9         5   129    410.9       2.5      11.0
```

Netflow—Simple Monitoring

- **Sample output on router (continued):**

```
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

UDP-DNS     2513140694    585.1         3    90   1778.6       5.3      21.5
UDP-NTP        2675203      0.6         1    76      0.6       0.0      21.6
UDP-TFTP         25750      0.0         6   157      0.0      20.1      20.8
UDP-Frag           737      0.0         5   210      0.0      14.4      21.4
UDP-other   1532677302    356.8         2   154    950.7       4.3      21.6
ICMP          30784392      7.1         4   109     30.7       7.3      20.5
IGMP                31      0.0      1903  1085      0.0      89.7      21.7
IP-other        985081      0.2         8   354      1.9      13.9      20.2
Total:      4457254338   1037.7         3   123   3324.8       4.8      20.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se2/0         203.161.234.211 Fa1/0         203.37.255.97   11 0404 0035     1
Fa1/0         203.37.255.97   Se2/0         203.161.234.211 11 0035 0404     1
Fa1/0         203.37.255.97   Se2/0         203.93.111.1    11 0035 8124     1
Fa1/0         203.37.255.114  Se2/0         195.67.208.248  11 1B3A 3F04  4675
Se2/0         195.67.208.248  Fa1/0         203.37.255.114  11 3F04 1B3A  6672
Se2/0         203.93.111.1    Fa1/0         203.37.255.97   11 8124 0035     1
Fa1/0         203.37.255.97   Se2/0         203.132.224.11  11 0035 0EDC     1
Se2/0         216.154.240.8   Fa1/0         203.37.255.97   11 0424 0035    12K
Fa1/0         203.37.255.97   Se2/0         216.154.240.8   11 0035 0424    12K
Se2/0         203.132.224.11  Fa1/0         203.37.255.97   11 0EDC 0035     1
...etc...
```

Netflow

- As a security tool
  - ✓ Very easy to spot port scans, address range scans, etc
  - ✓ Many documented cases of ISPs using NetFlow to catch “crackers”
  - ✓ First tool to use in instance of suspected or real DOS attack

Out of Band Management

Terms

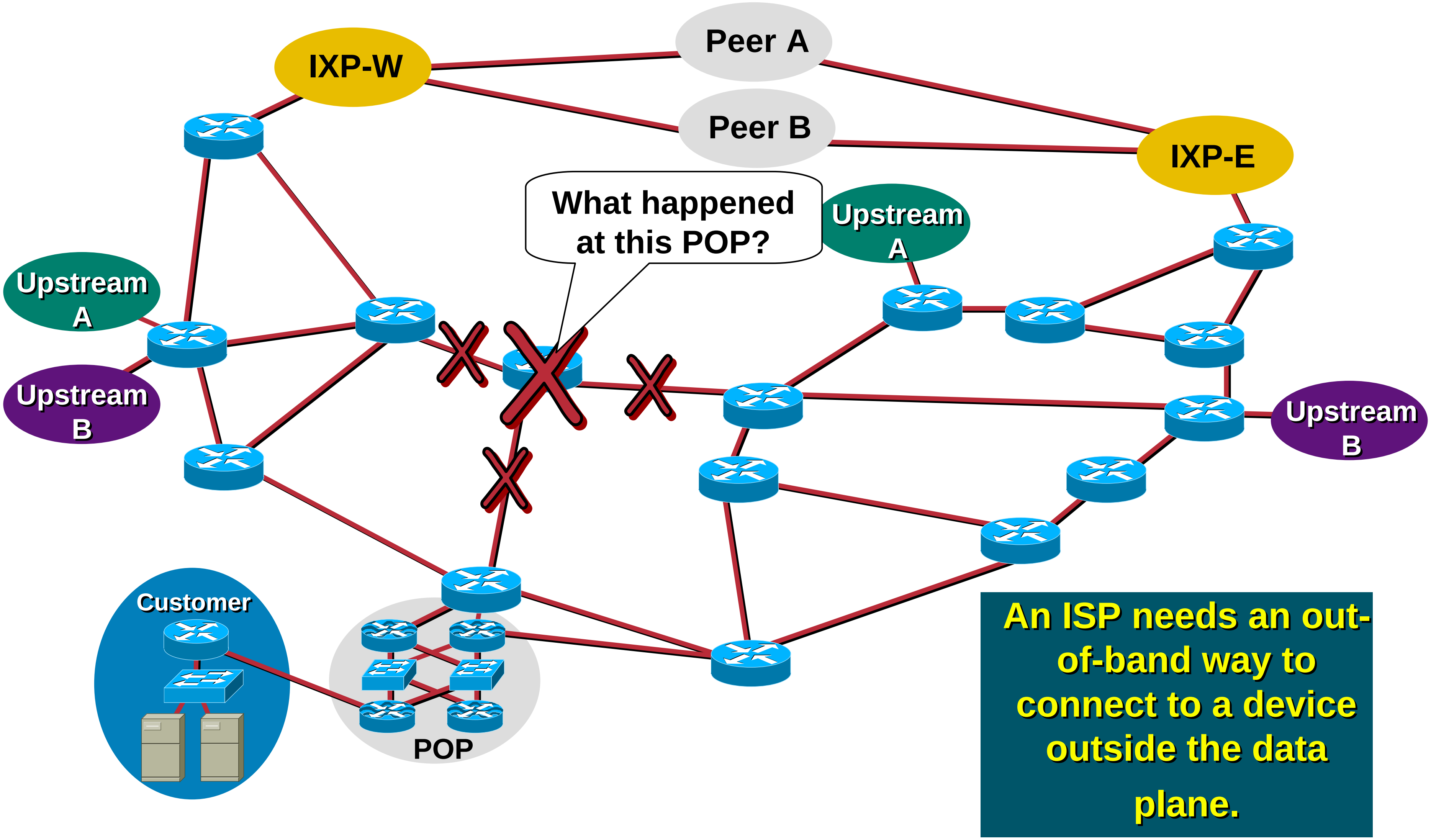
- **Traffic through/to a router/switch can be broken into three planes:**

  ✓**Data Plane – The user/customer traffic in which the router/switch forwards from one port to another port.**

  ✓**Control Plane – The routing/synchronization protocols used to communicate forwarding information to each router/switch. (i.e. OSPF, ISIS, BGP, NTP)**

  ✓**Management Plane – The configuration, management , and accounting protocols used to take care of the router/switch. (i.e. Telnet, RSH, SSH, SNMP, RMON, Netflow, Syslog, software upgrade)**

Router Crash? Cable Cut? DOS?



What happened at this POP?

An ISP needs an out-of-band way to connect to a device outside the data plane.

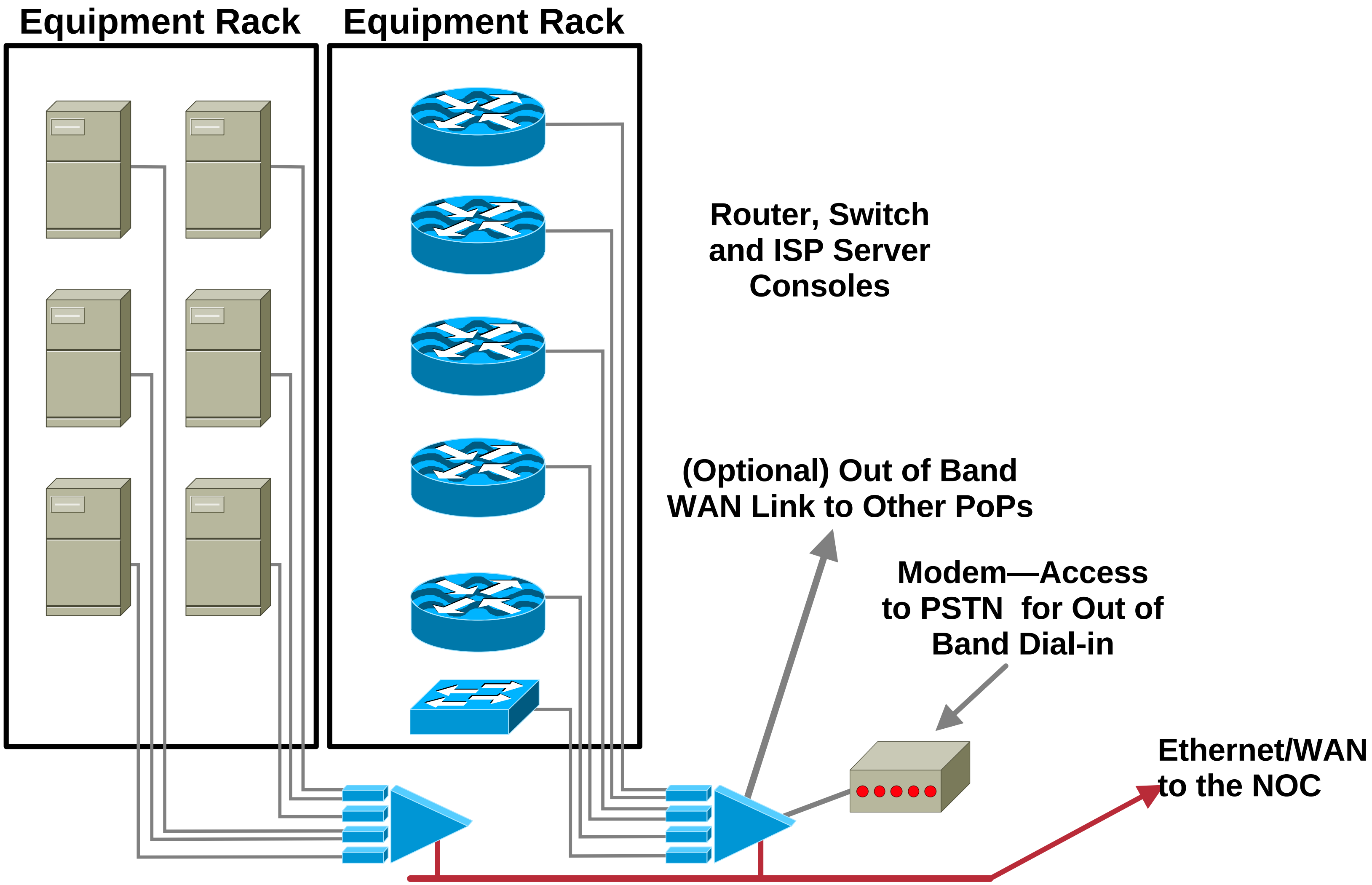
Out of Band Management (OOB)

- OOB is a critical requirement for today's ISPs!
- Allows access to network equipment in times of failure or when under attack
- Creates an isolated path for accounting and management information.
- Ensures quality of service to customers
  - ✓Minimizes downtime
  - ✓Minimizes repair time
  - ✓Eases diagnostics and debugging

Traditional Reverse Telnet OOB

- OOB example—Access Server with reverse telnet:
  - ✓ Modem attached to the access server to allow NOC dial in in case of total POP isolation
  - ✓ Console ports of all network equipment connected to async ports of the access server – NOC reverse telnets through the async ports into the console of the POP.
  - ✓ Access server's LAN and/or WAN link connects to network core (least preferred) or via separate management network to NOC
- *Full remote control access under all circumstances*

Traditional Reverse Telnet OOB



Equipment Rack

Equipment Rack

Router, Switch and ISP Server Consoles

(Optional) Out of Band WAN Link to Other PoPs

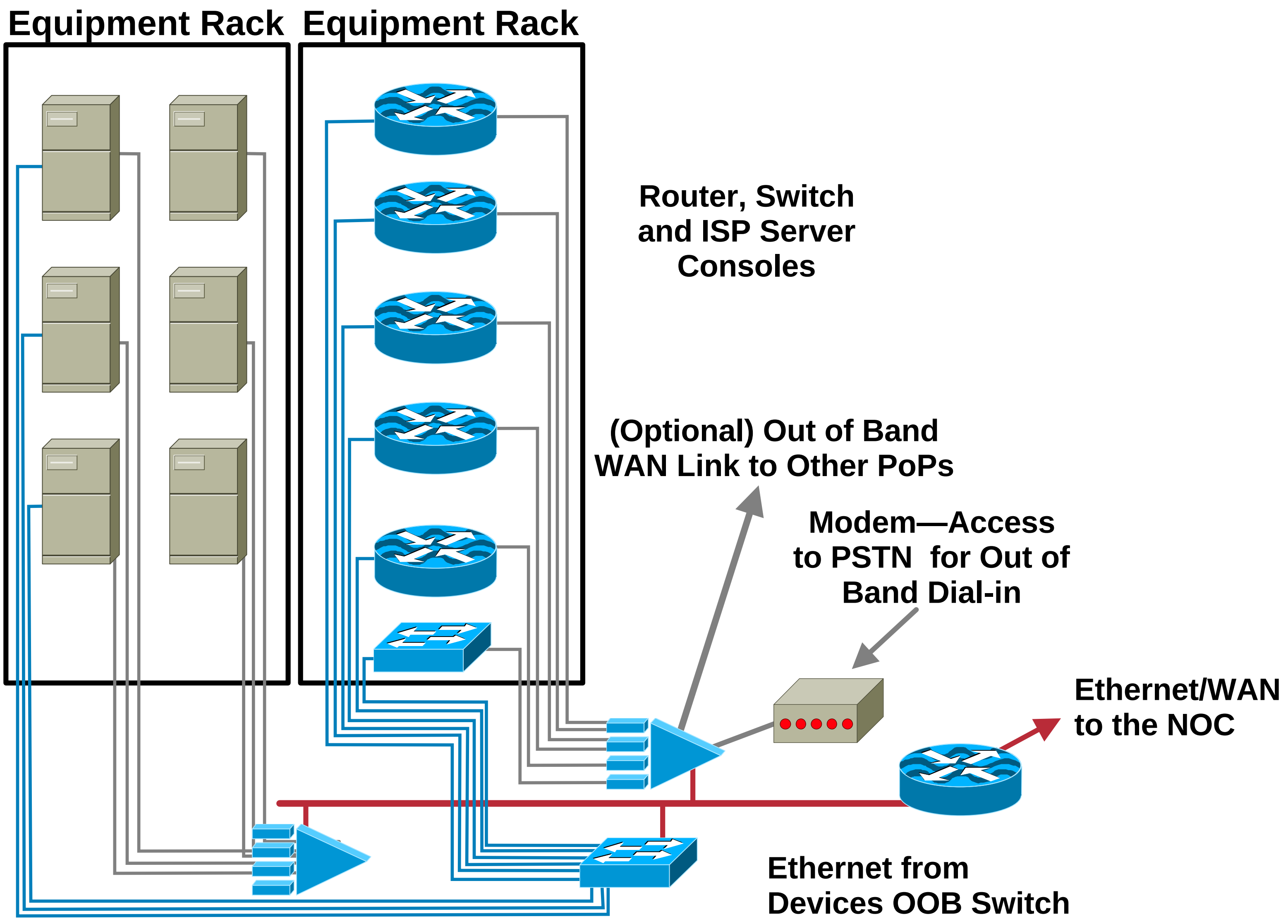
Modem—Access to PSTN for Out of Band Dial-in

Ethernet/WAN to the NOC

OOB Second Generation

- Statistics and accounting protocols are sensitive to congestion (i.e. UDP based).
- Separate data networks are installed to move the statistics and accounting information to the NOC
  - ✓Routers are NetFlow, SNMP, and syslog enabled
  - ✓Management data is congestion/failure sensitive
  - ✓Ensures management data integrity
    in case of failure or unexpected network load
- *Full remote information under all circumstances*

OOB Second Generation


Equipment Rack
Equipment Rack
Router, Switch and ISP Server Consoles
(Optional) Out of Band WAN Link to Other PoPs
Modem—Access to PSTN for Out of Band Dial-in
Ethernet/WAN to the NOC
Ethernet from Devices OOB Switch

Secure the OOB Devices and Console Access

- Router console port gives complete control over router

  ✓Ensure router is in locked cabinet

  ✓-and/or-

  ✓Ensure comms room is locked and only accessible by authorized personnel

  ✓-and/or-

  ✓Ensure premises are secure, only accessible by authorized personnel, and has a working environmental control system

  faulty air conditioning ® open doors/windows ® no security ® network devices become vulnerable

What if you do not implement OOB?

- ISPs who do not implement OOB management carry the risk of increased downtime.
- While Cisco makes every effort to not have software crashes, when we do crash, we make every effort to *crash softly.*
  - ✓*Crashing softly* means you reboot the box and come back up.
- Do not rely on soft crashes. There are situations (i.e like DOS/DDOS) where the router will get caught in a cycle of failure (crash, reboot, crash, reboot, crash, reboot, etc.)
- When this happens, in-band management is useless. OOB or sending someone physically to the site is the only option.