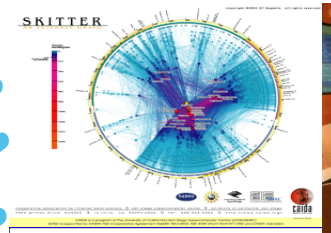
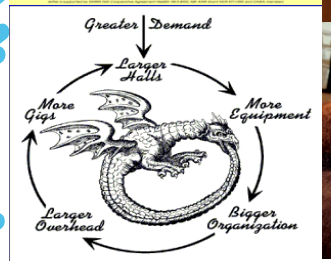
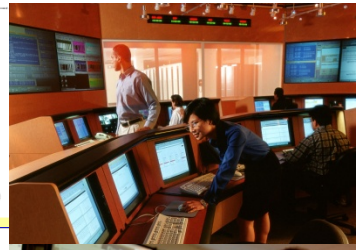
Point Protection in the Network





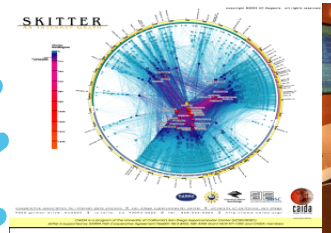


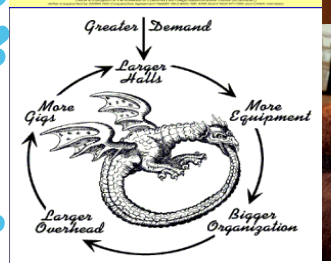
Check List

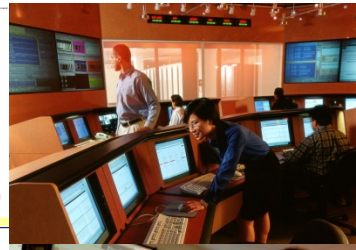
Objective: There is no “edge” in an Operator’s Network. Every point in the network must be uniquely protected from all threats inside, outside, and for all sides.

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

Realities of SP Security



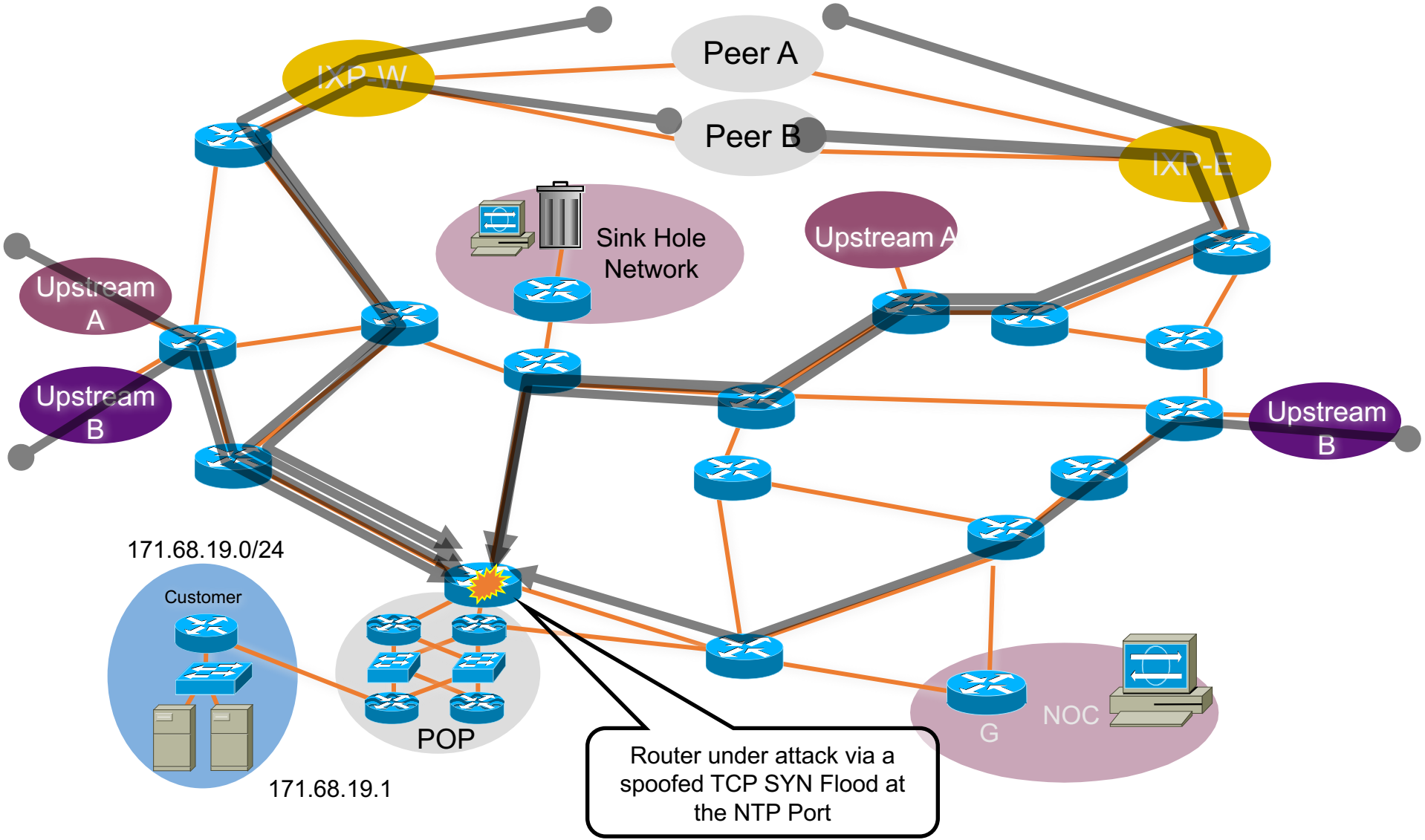




ISP's Security Attack Profile

- Attacks are part of <u>every day</u> operations. One Tier 1 ISP characterizes their attack profile as the following (based on mid '2000 data):
  - 90% of attacks are vindictive "script kiddy" attacks.
    - These are the one ISP's customers are hit with every day. The volume of the attacks take up a lot of time.
  - 9% are of a more serious DDOS type.
    - These are the ones that cause co-lateral damage. Also one of the main visible threats.
  - 1% hit the infrastructure directly
    - These are the ones the ISPs are really worried about.

Routers do get Directly Attacked



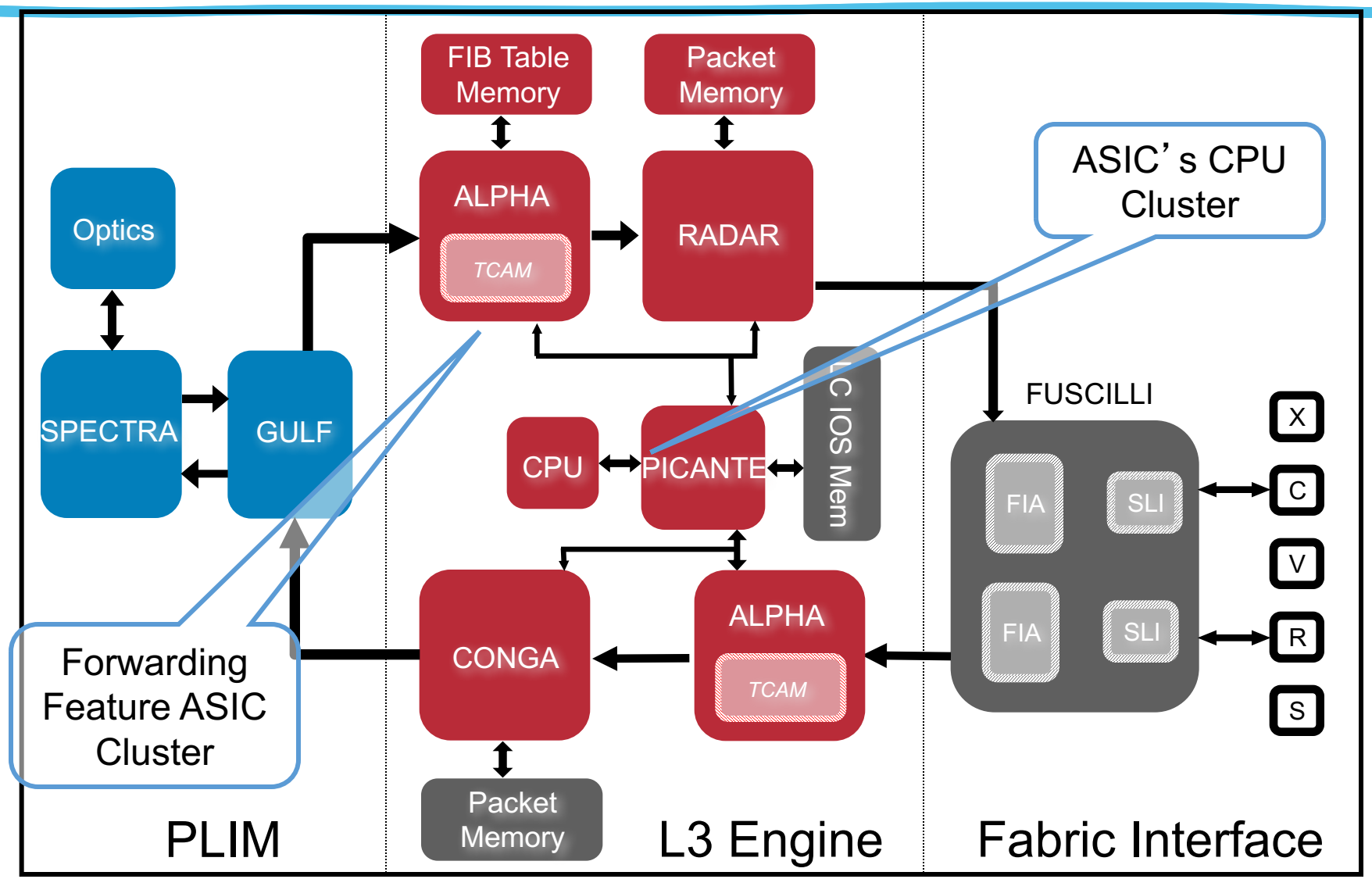
Routers do get Directly Attacked

- We knew back in the late ’90s that direct attack on routers were going to be one of the key Internet vulnerability points.
- The Feb 2000 DDOS attack provided the industry to quietly shift into an accelerated path to allow routers to resist, compartmented, and survive a direct attack.
- While there is nothing a router can do to mitigate a bandwidth saturation attack, the router should:
  1. Do Not Crash from the Saturation Attack (worse case CPU saturation with accessibility via console).
  2. Remain Accessible to the Operations Team
  3. Compartmented the effects of the bandwidth saturation – allowing the other components of the router to remain functioning.

Terminology

- Four Plane Conceptual Model:
  - Data Plane – Packets going through the router.
  - Control Plane – The routing protocols gluing the network together.
  - Management Plane – The tools and protocols used to manage the device.
  - Service Plane – The way packets are diverted and linked to high touch services.

Example – Engine 3 Line Card



IP Network *Planes of Operation*

Policy Plane: **The business glue of the network. Rules execution, decision making, Identity Collection, Stores Session Identity/Credentials, Processes Command/Query requests, AAA, Service Manager, Manages/Caches Service Profiles, and all the other components to make a productize service.**

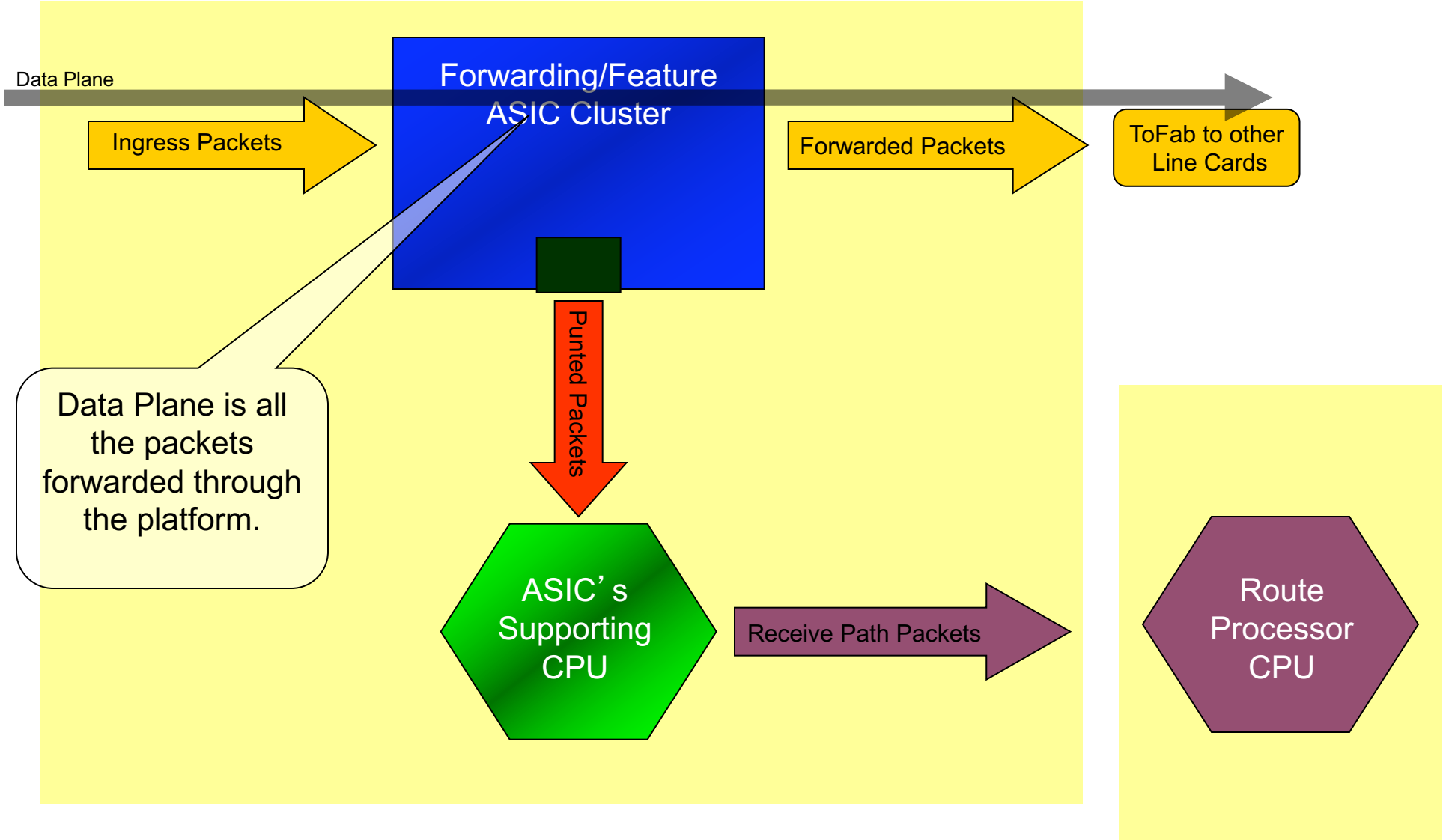
Services Plane: **Overlay "Layer 7" application flow built on the foundation of the other layers. Service insertion, application routing, application service flows and other flows separate, but dependent on the other layers.**

Management Plane: **The management plane is the logical path of all traffic related to the system management of the routing platform. In a distributed and modular environment, the management plane offers new levels of complexity, and hence, increased requirements to maintain secure access**

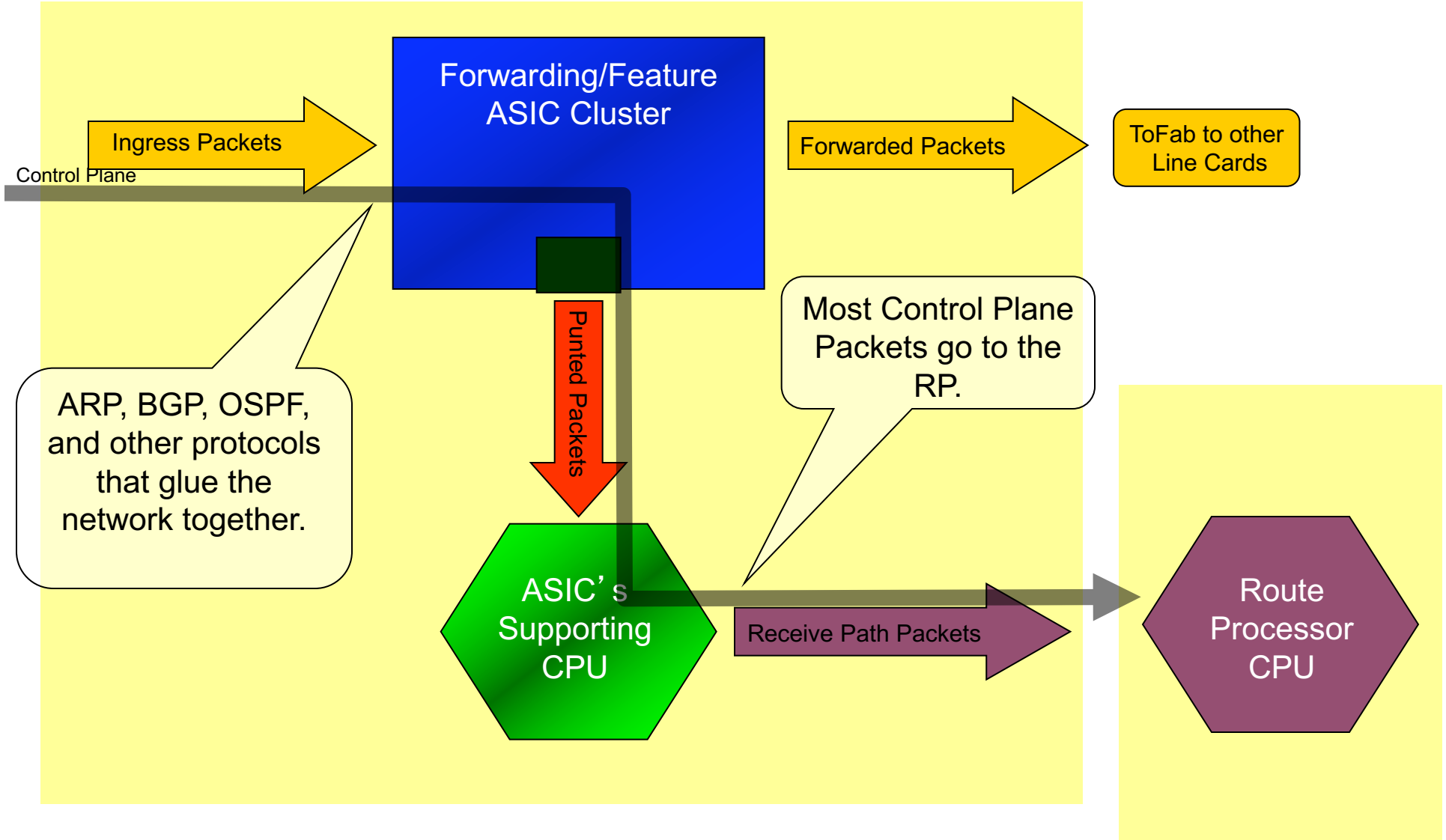
Control Plane: **The glue of the network. The control plane is where all routing control information is exchanged, making the control plane and its components a target. Because control plane resiliency depends on CPU processing power and scalability, "out-of-resources" attacks against the CPU are not uncommon.**

User/Data Plane: **The data plane receives, processes, and transmits network data between network elements, and represents the bulk of network traffic that passes to and through the router**

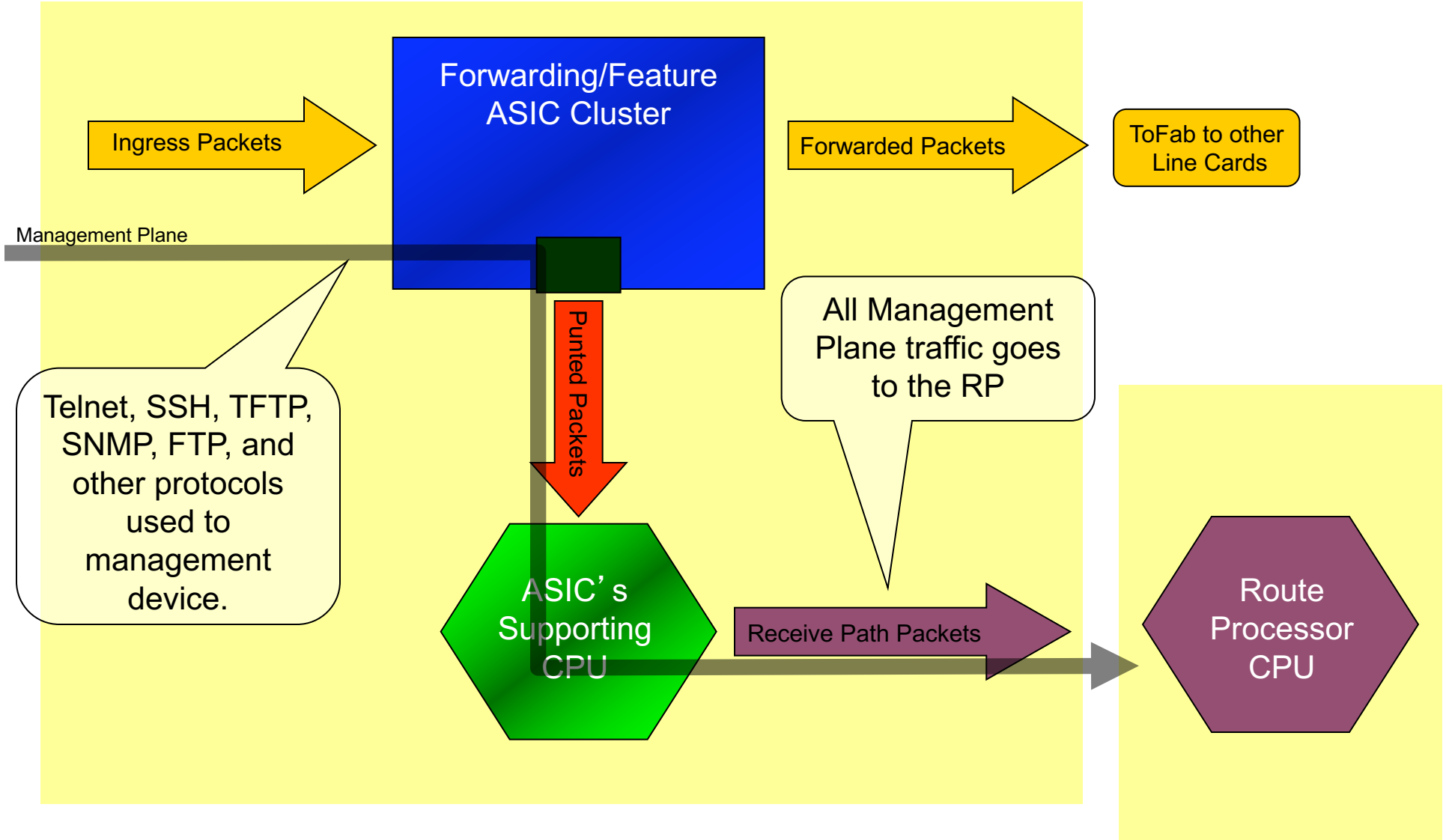
Data Plane


Data Plane
Ingress Packets
Forwarding/Feature ASIC Cluster
Forwarded Packets
ToFab to other Line Cards
Punted Packets
Data Plane is all the packets forwarded through the platform.
ASIC's Supporting CPU
Receive Path Packets
Route Processor CPU

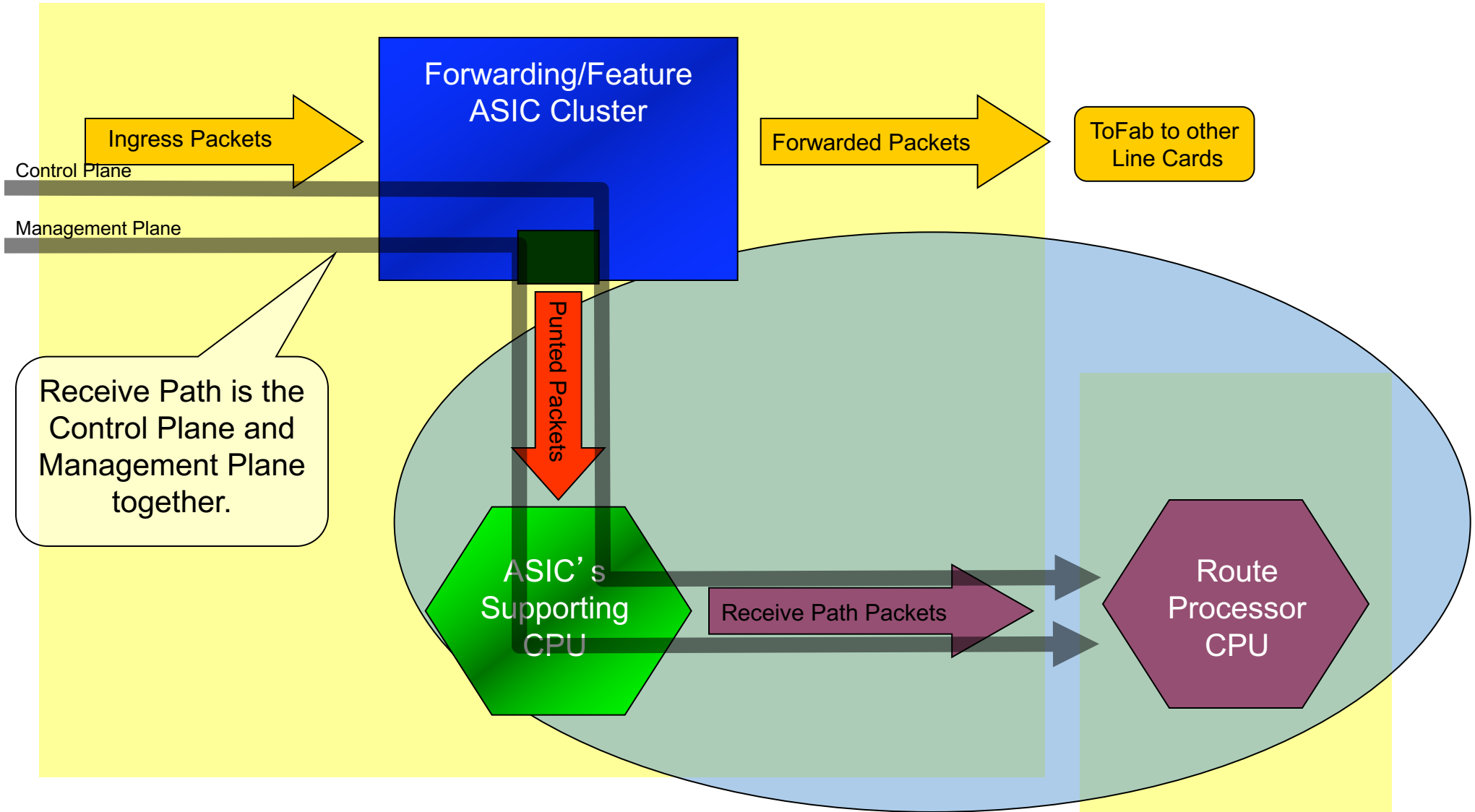
Control Plane



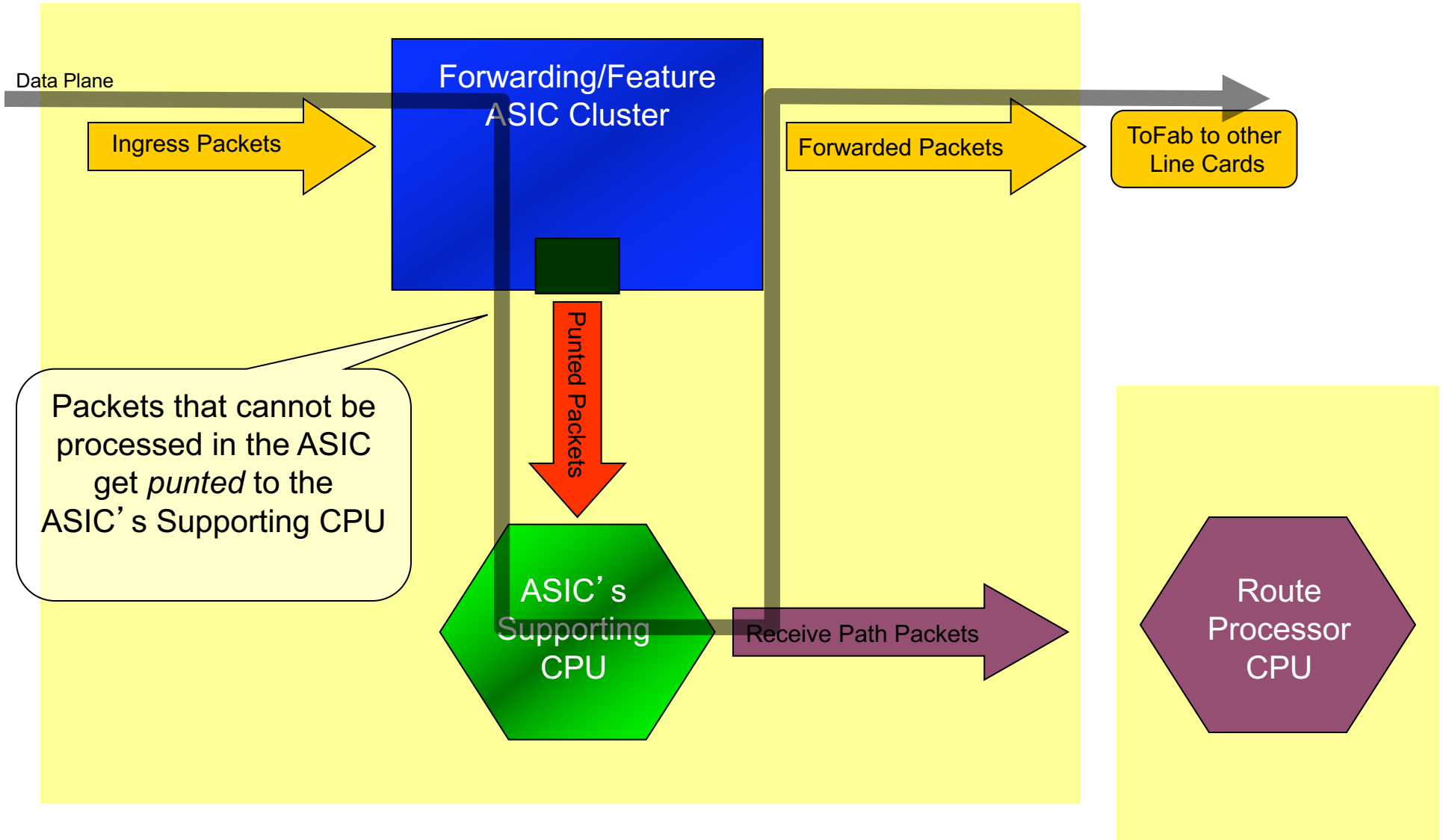
Management Plane



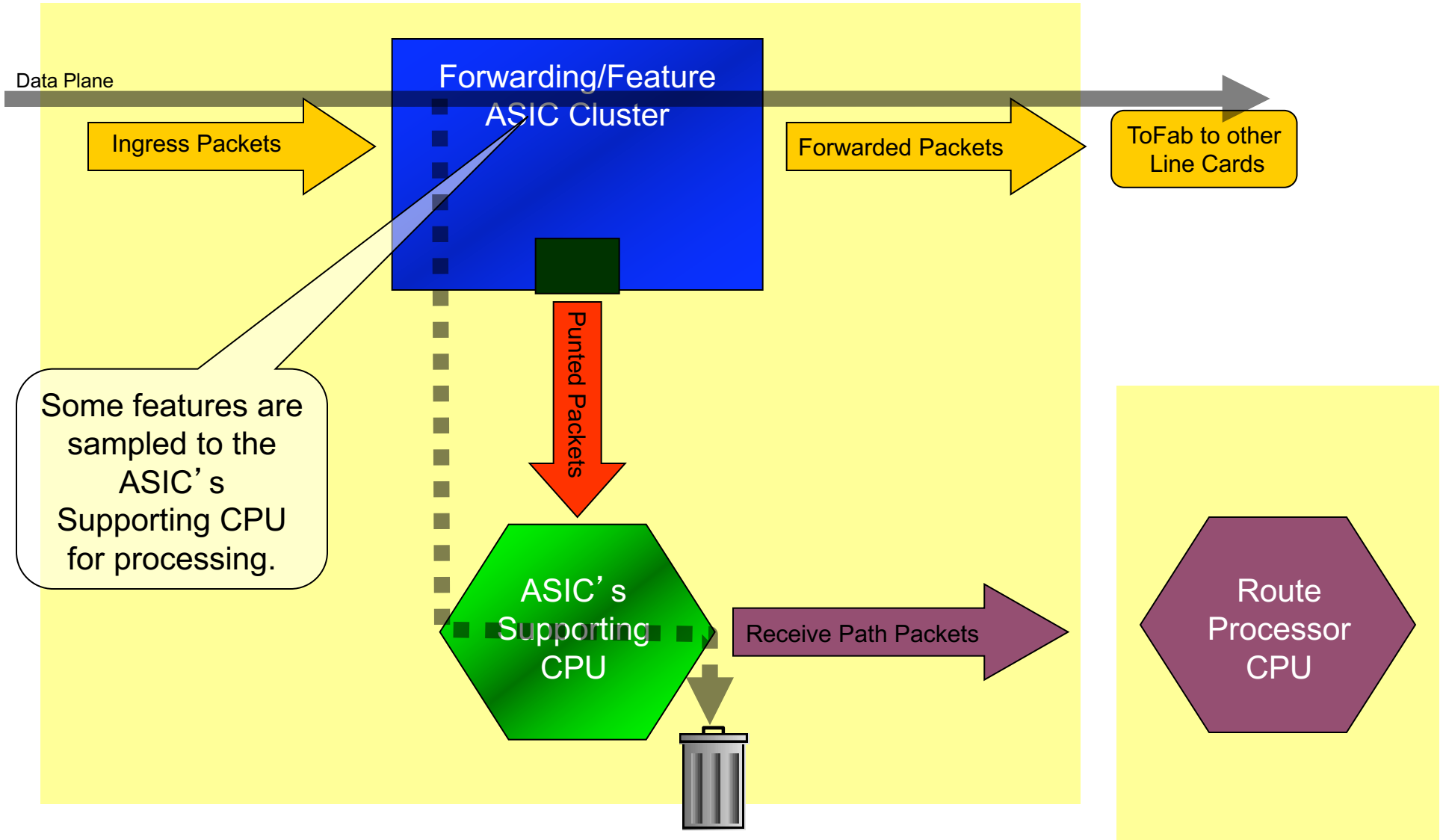
Receive Path (Control & Mgt Plane)



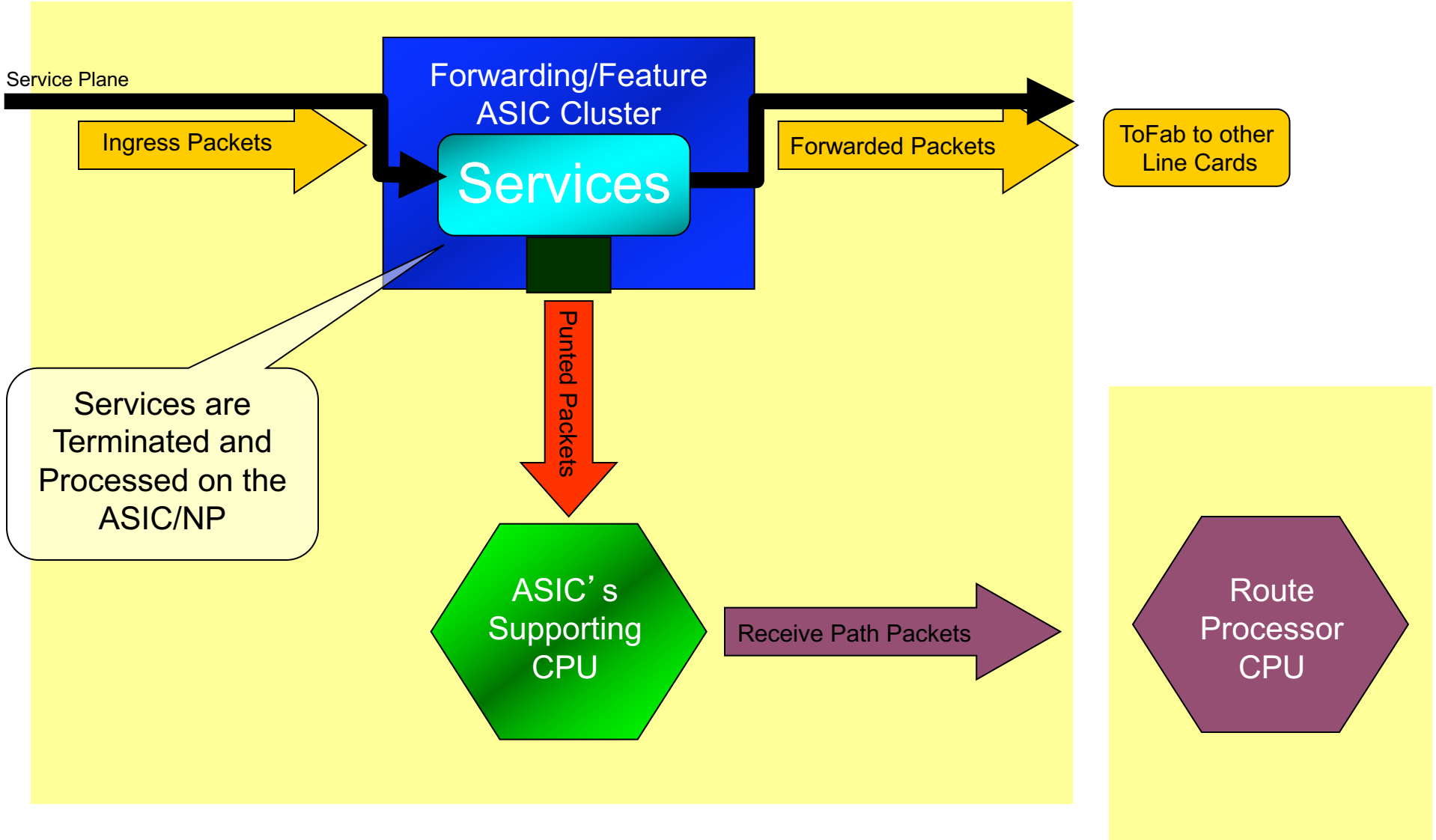
Digression - Feature Punt



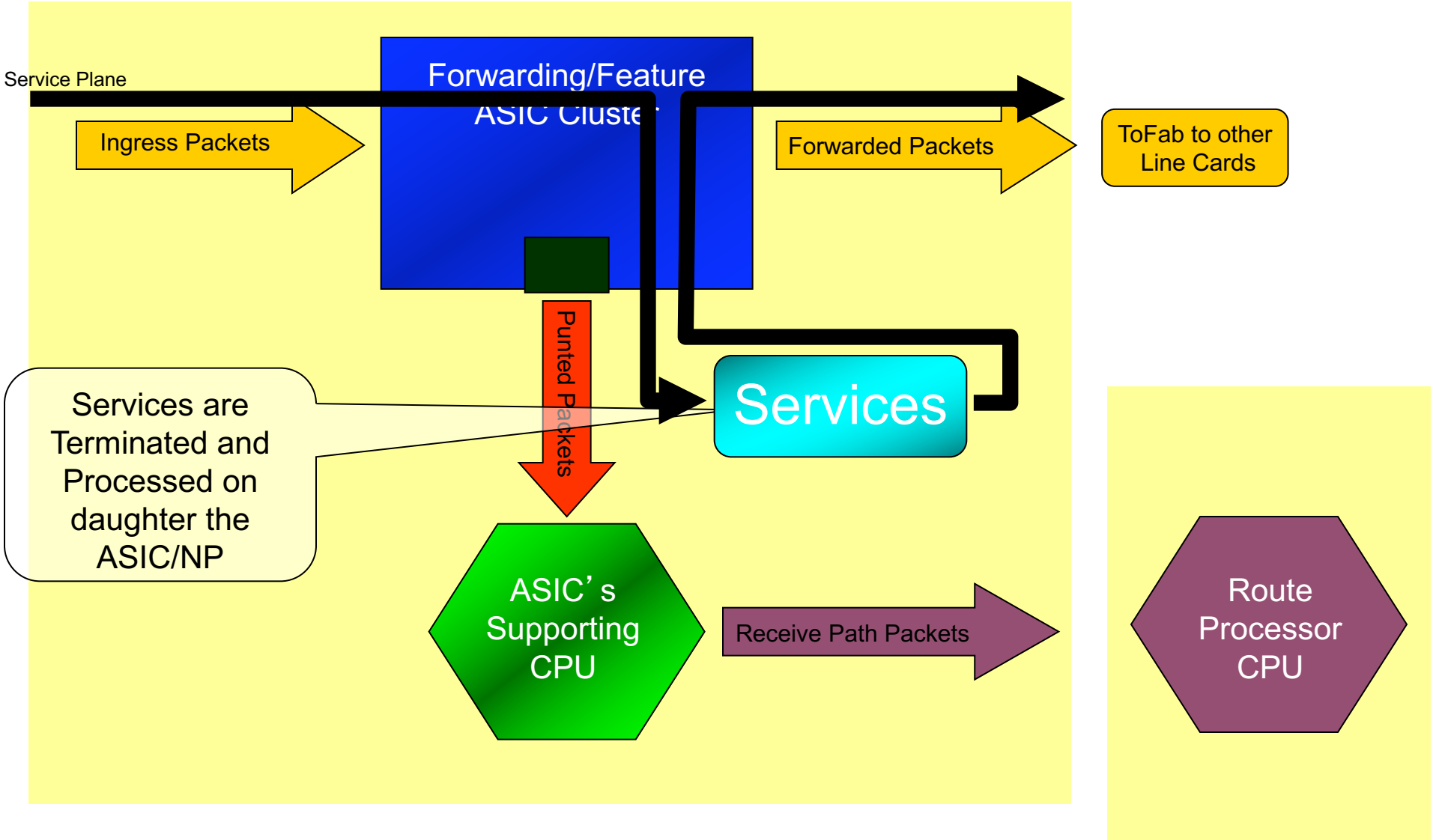
Digression - Sampled Feature



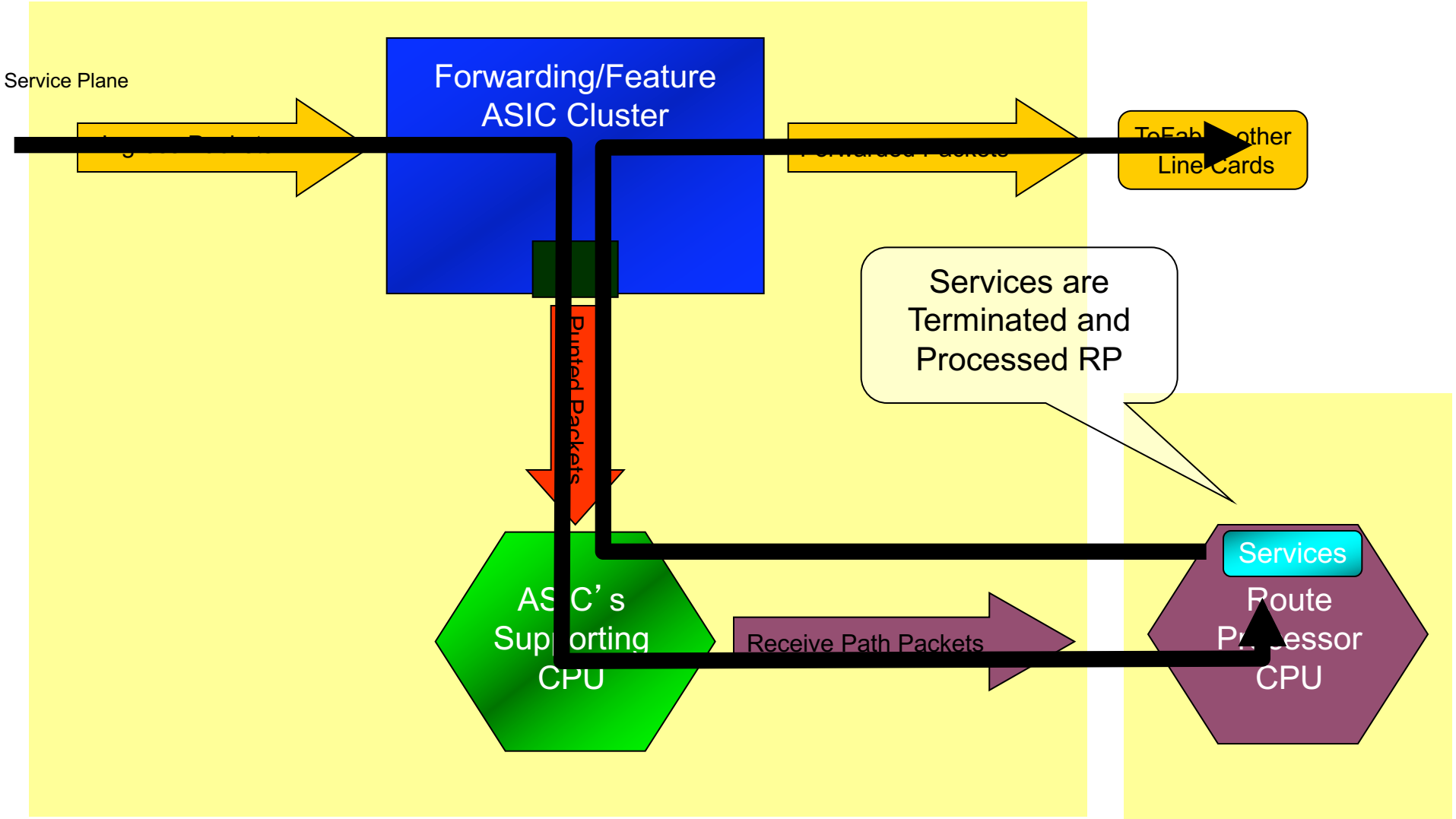
Service Plane – ASIC or NP



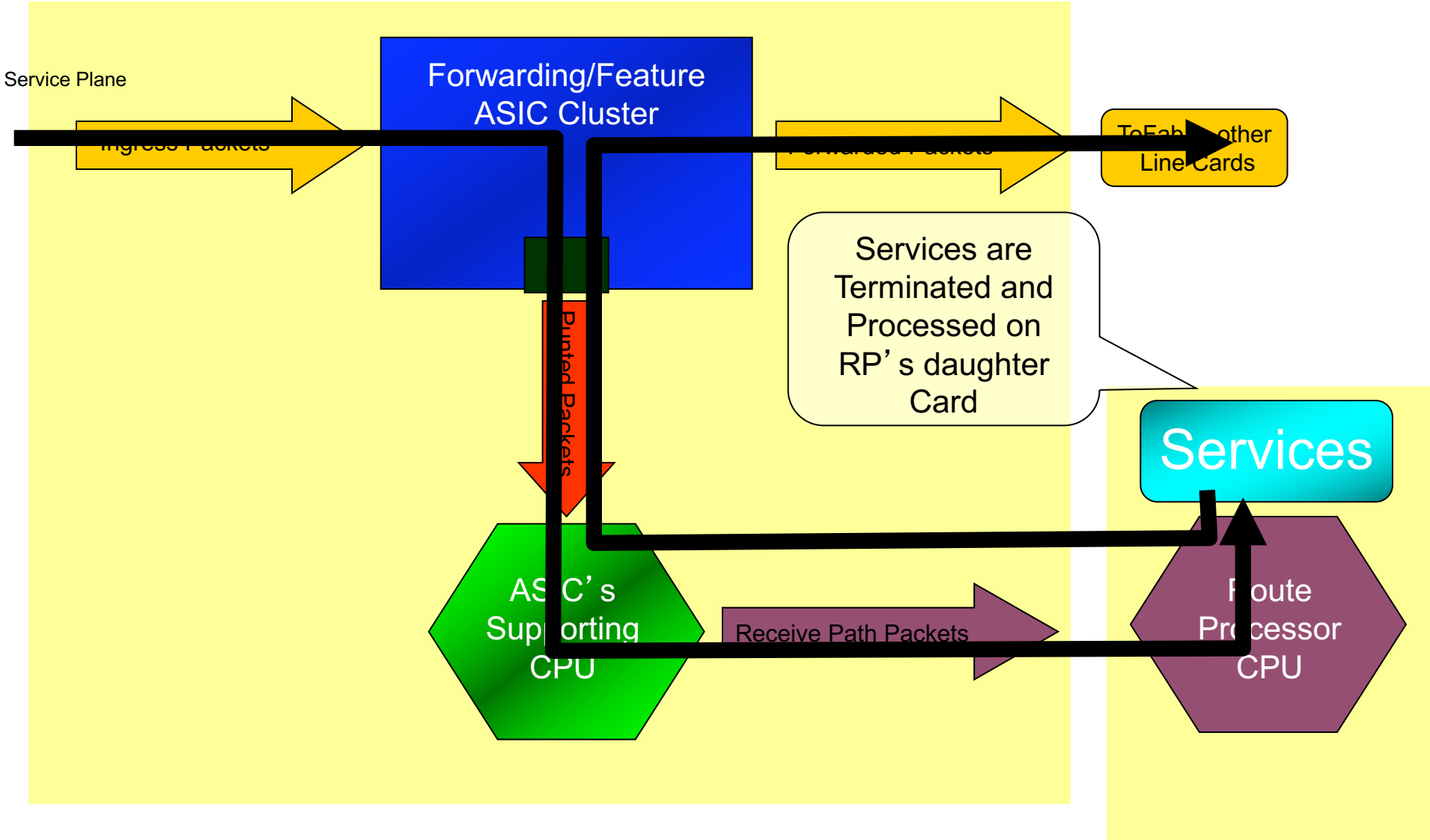
Service Plane – Daughter ASIC/NP



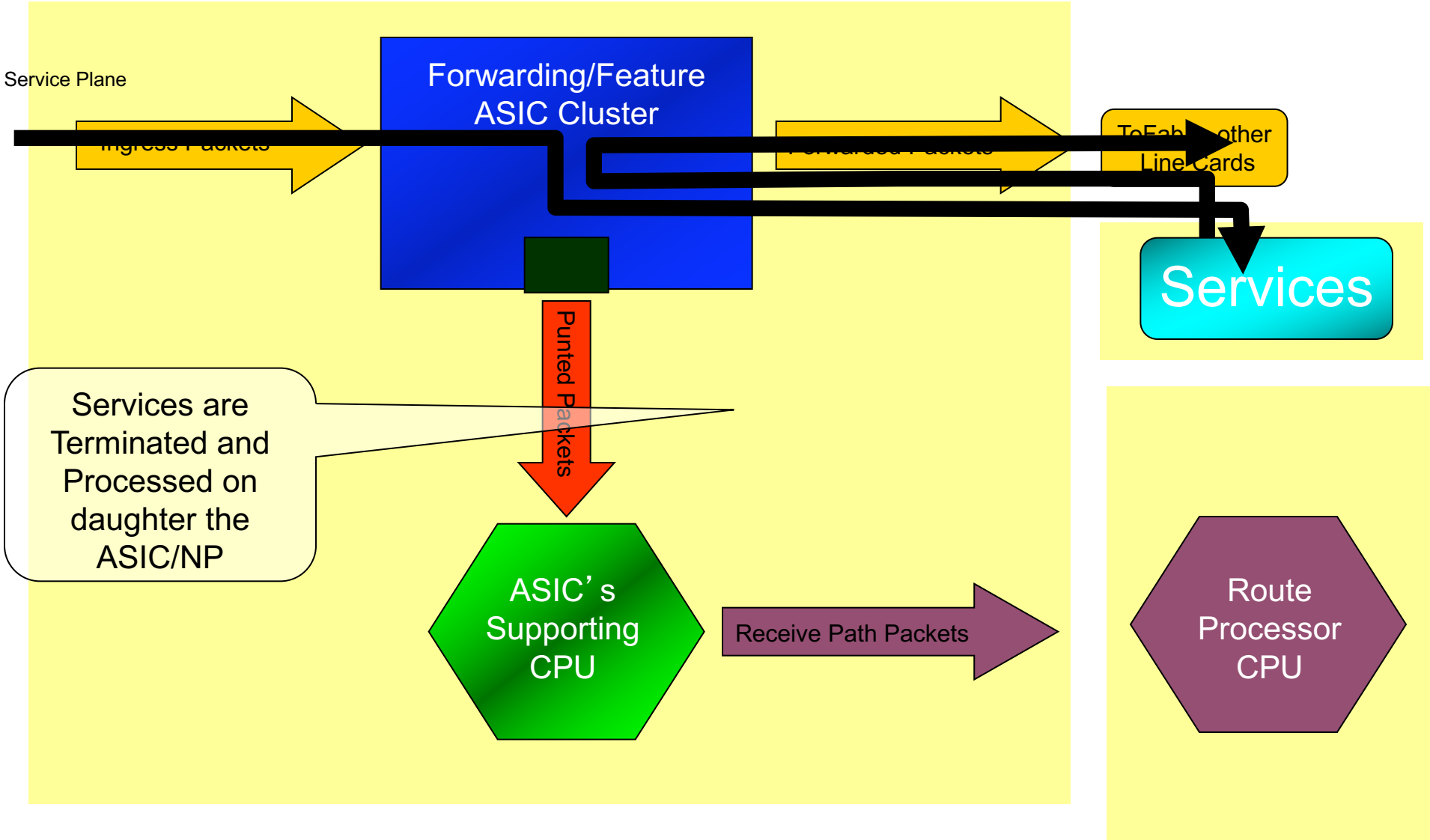
Service Plane – Route Processor



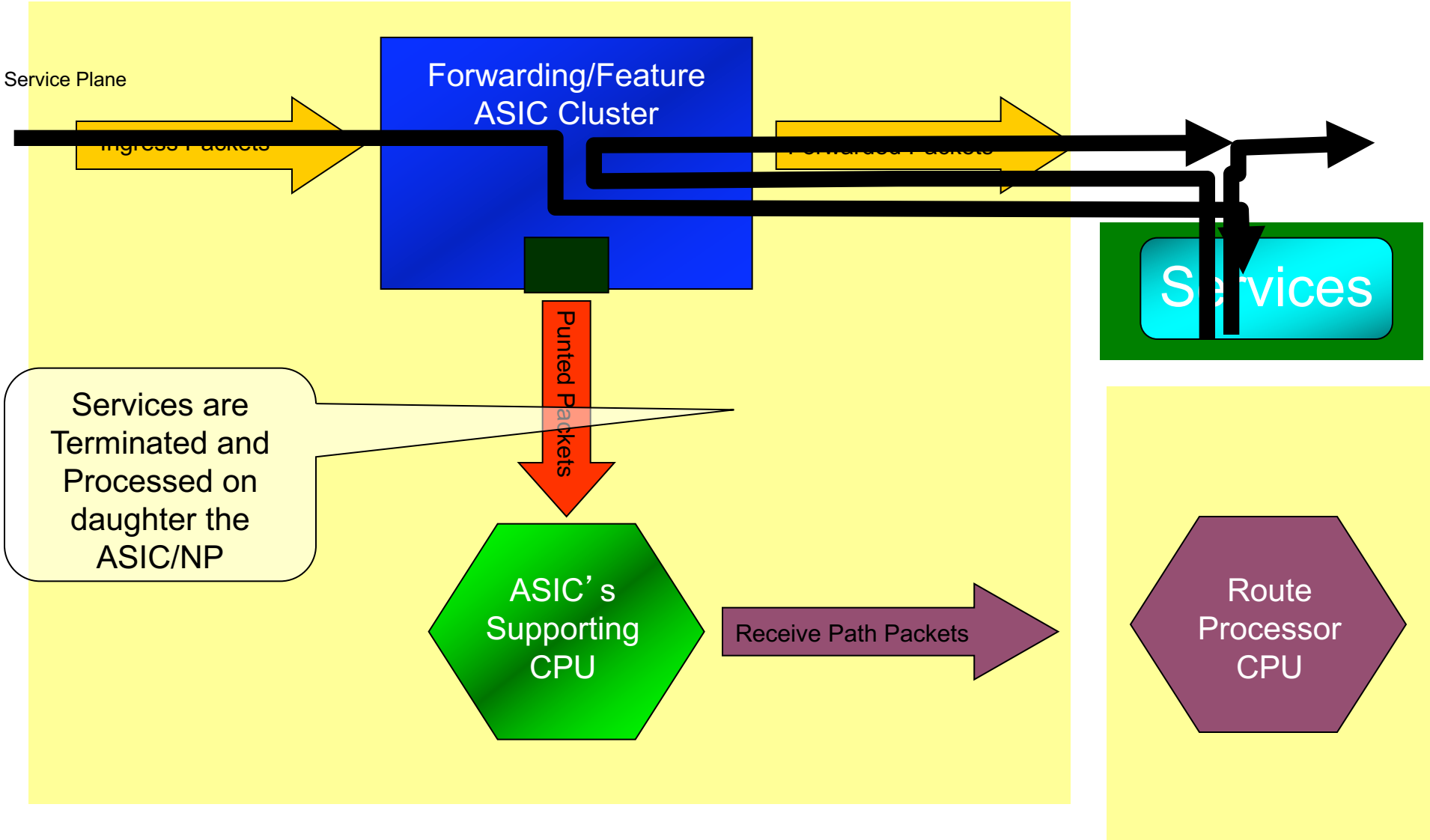
Service Plane – Daughter RP



Service Plane – Service Blade



Service Plane – Separate Box



Why Do I Need to Know This?

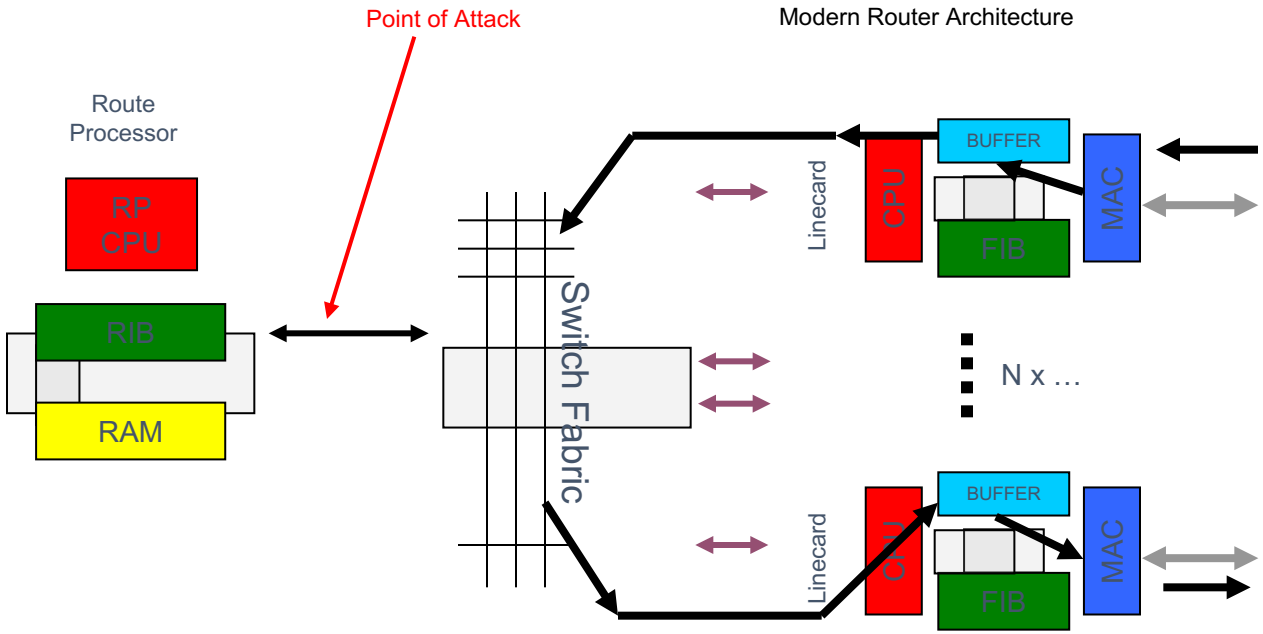
- If you do not understand the functions of each component, then:
  - You really do not understand how the equipment works
  - Do not understand how to properly test the equipment
  - Have un-realistic expectations on what the equipment can do.

Simple Risk Assessment

- Direct Attacks on the Router usually hits on three attack vectors:
  1. Bandwidth Saturation (Data plane)
  2. Target the Control or Management Plane (Receive Path traffic on the Control and Management Plane)
  3. Saturate the Punt path out of the forwarding/feature ASIC by abusing the TCP/IP standards (Data plane traffic that is punted from the forwarding/feature ASIC).

AOL's Public Security Campaign (2004)

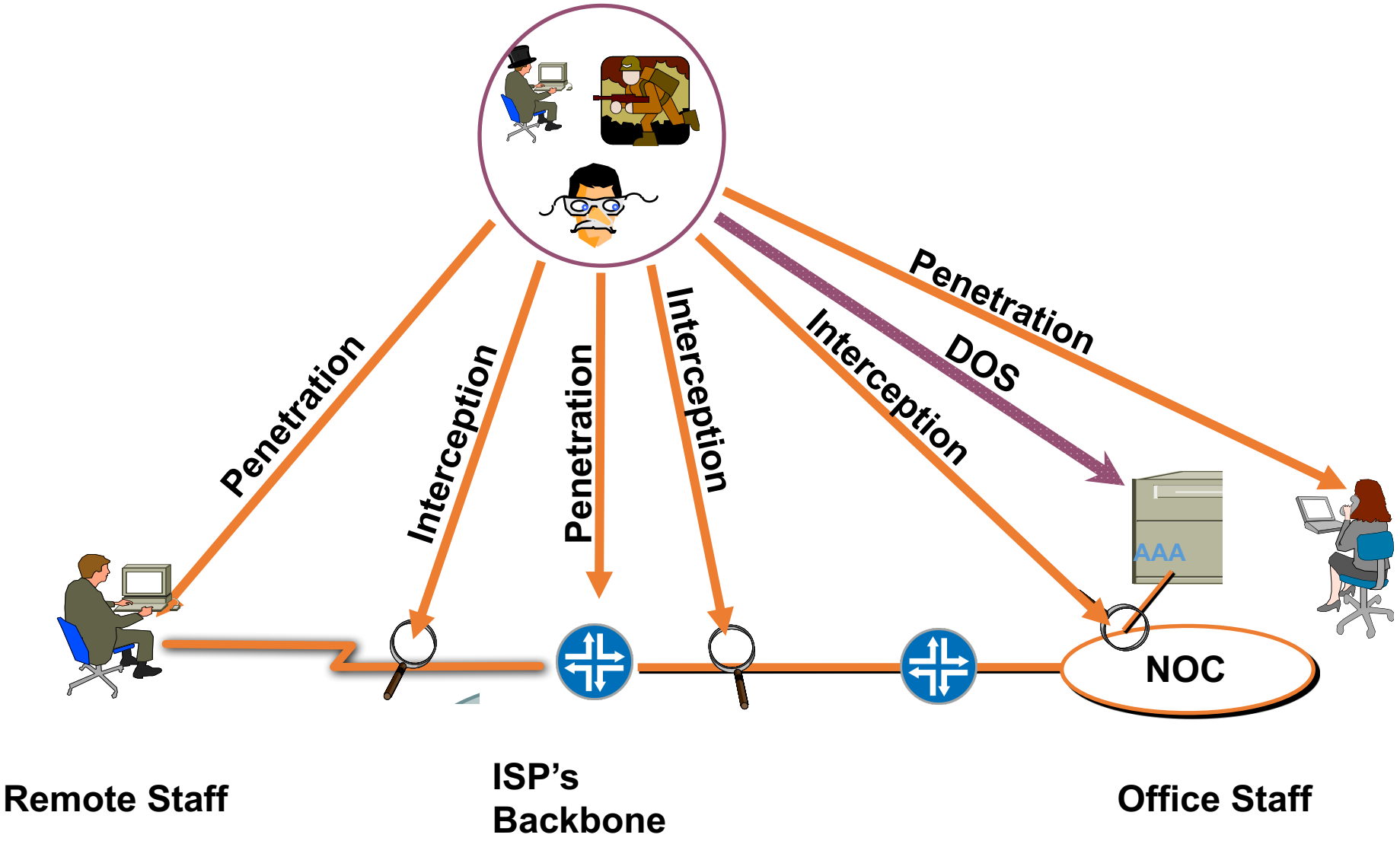
- Routers are optimized for traffic through the hardware
  - Not traffic for the hardware
- What we really need is N x Line-rate decryptions (N = number of lines)



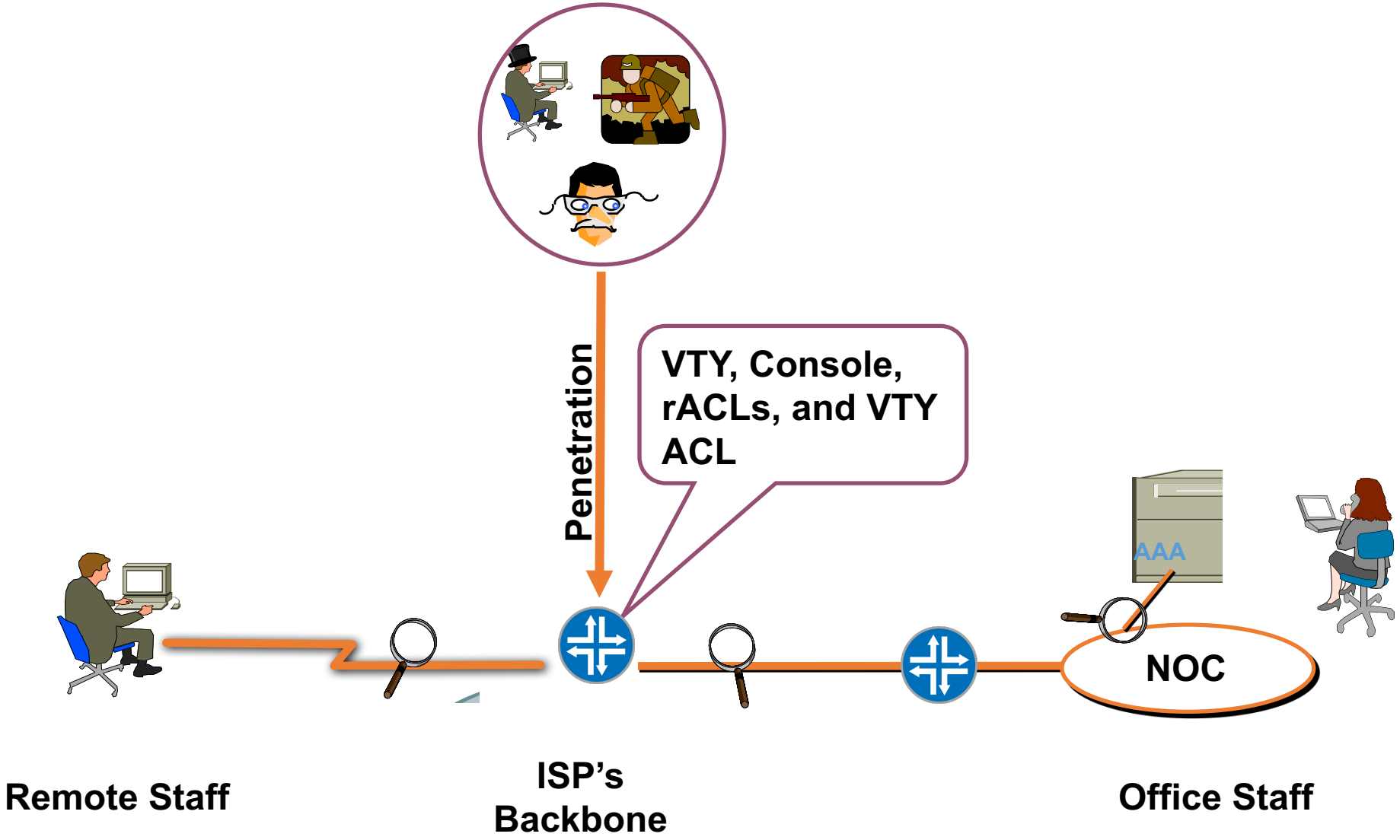
Management Plane Security

- This module is covering techniques and configuration guides to help protect the *Management Plan.*
- Some of the techniques protect both the Control Plane and Management Plane.

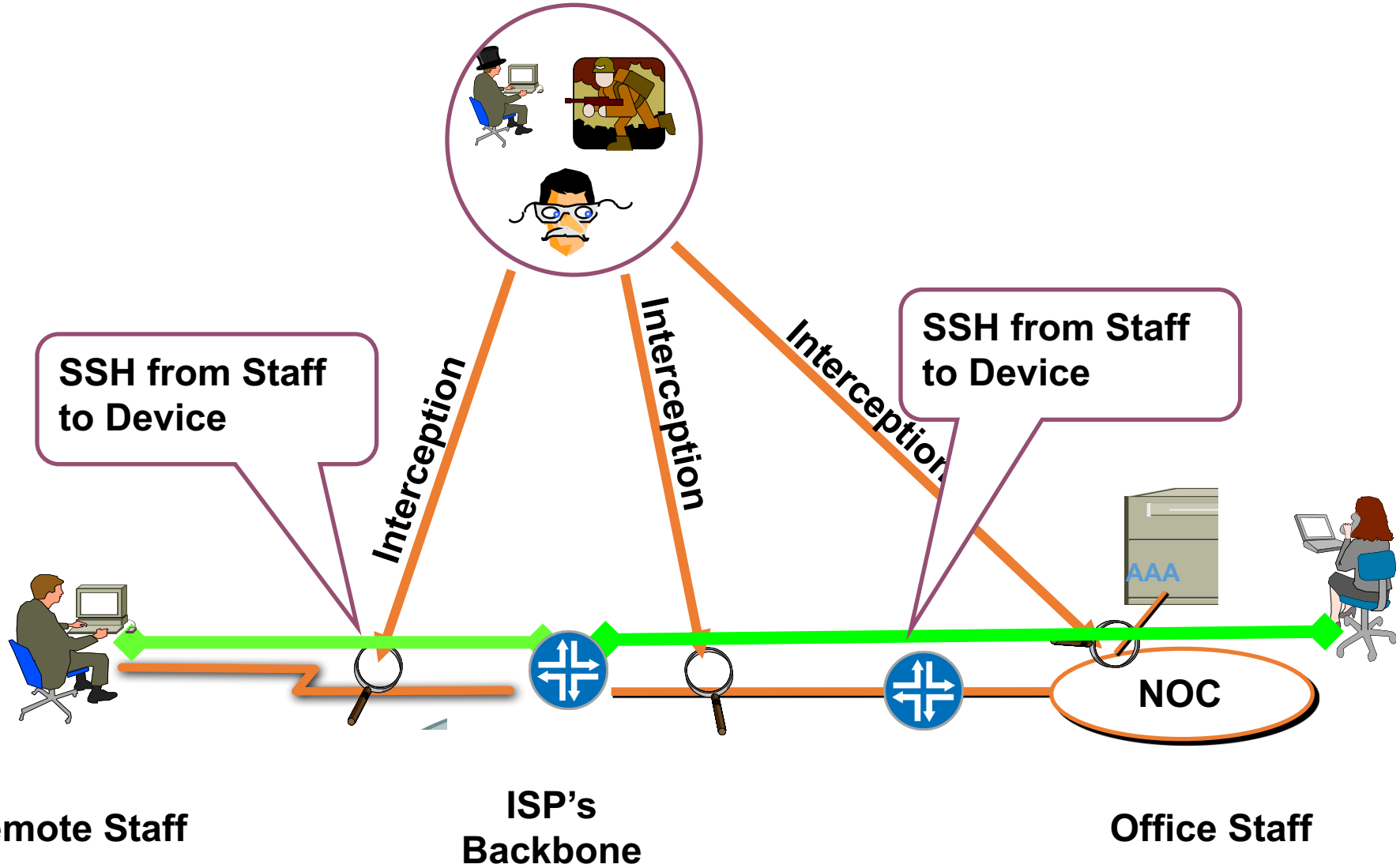
RISK Assessment



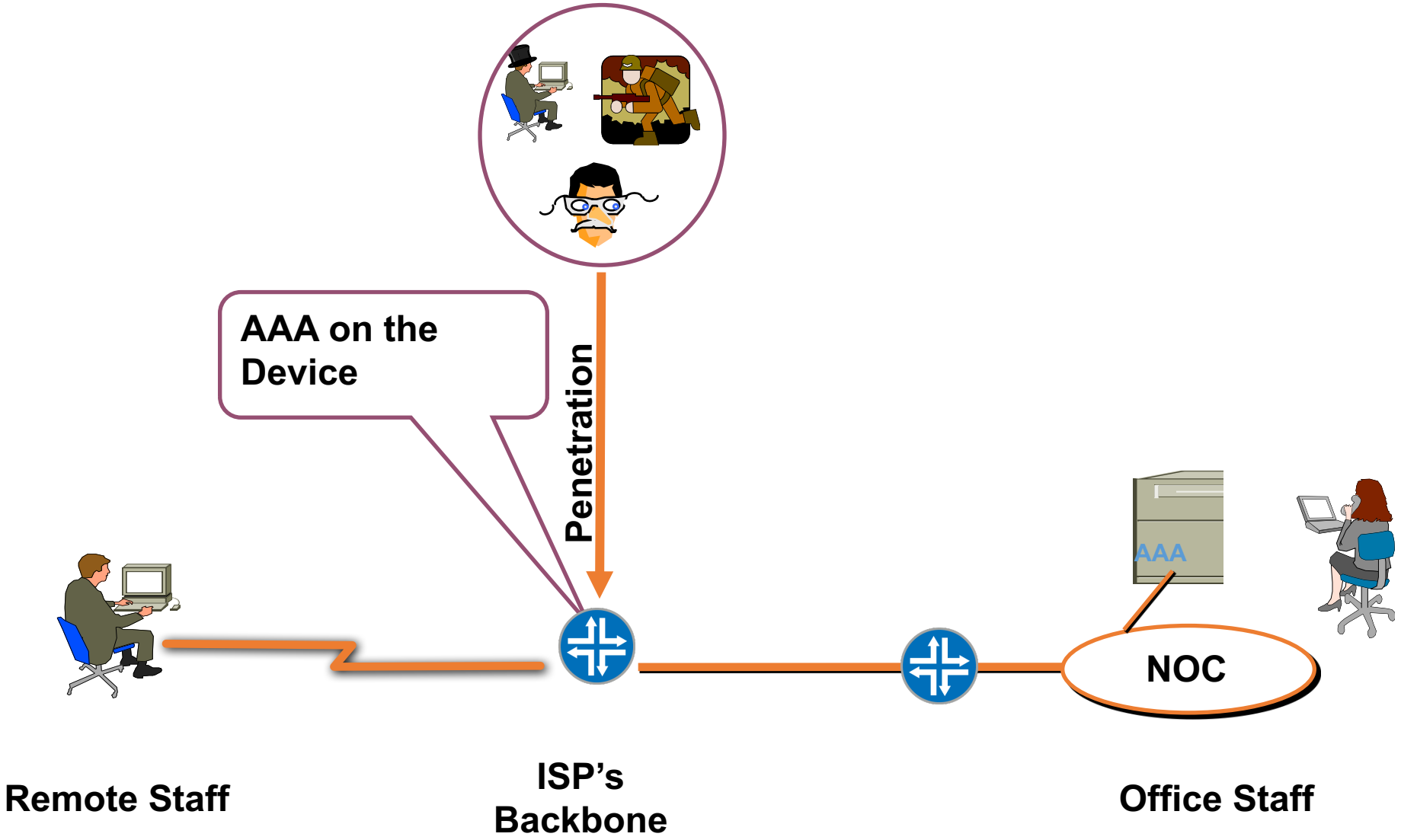
Lock Down the VTY and Console Ports



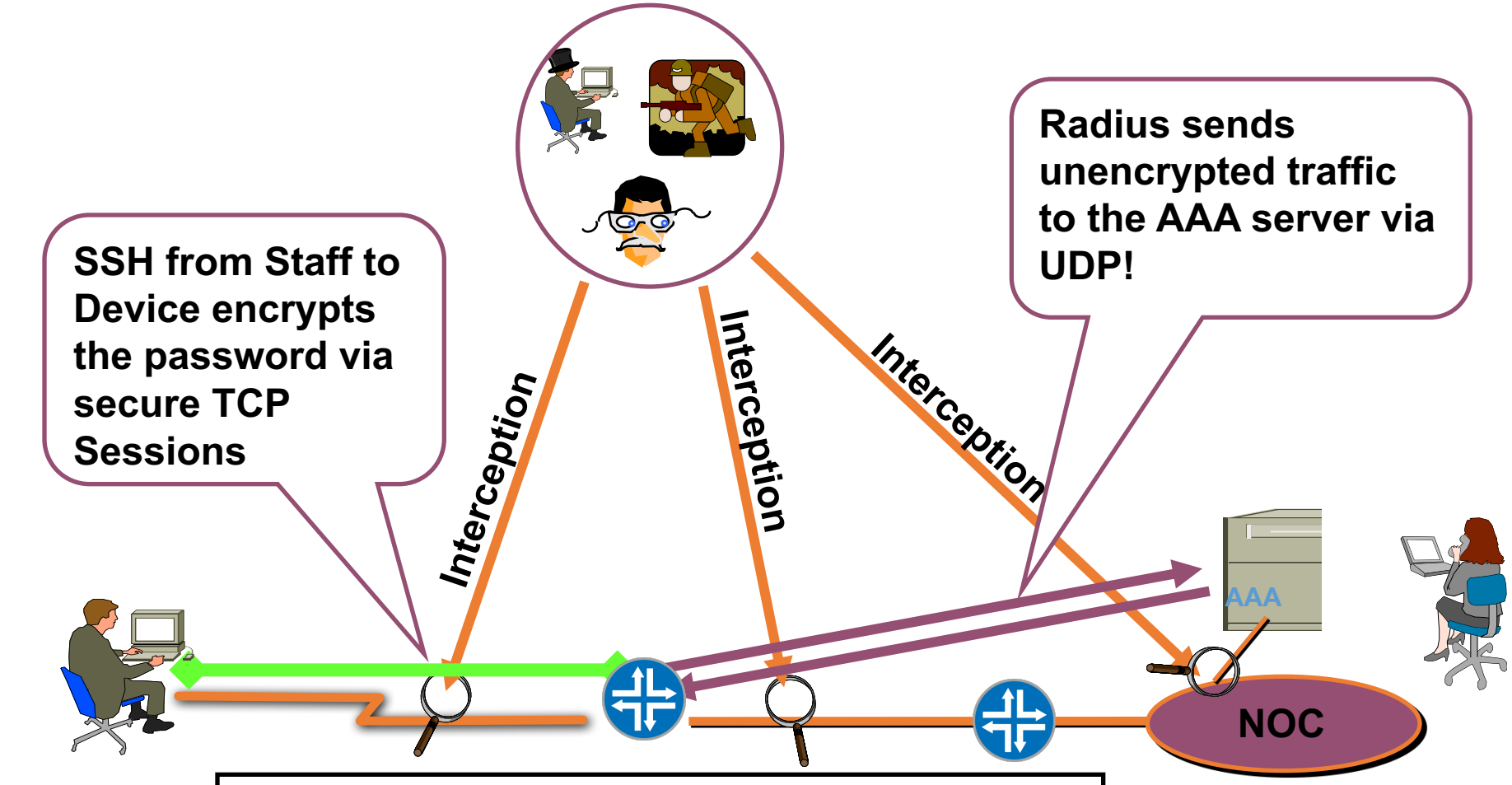
Encrypt the Traffic from Staff to Device



Staff AAA to get into the Device



Radius is not an SP AAA Option!

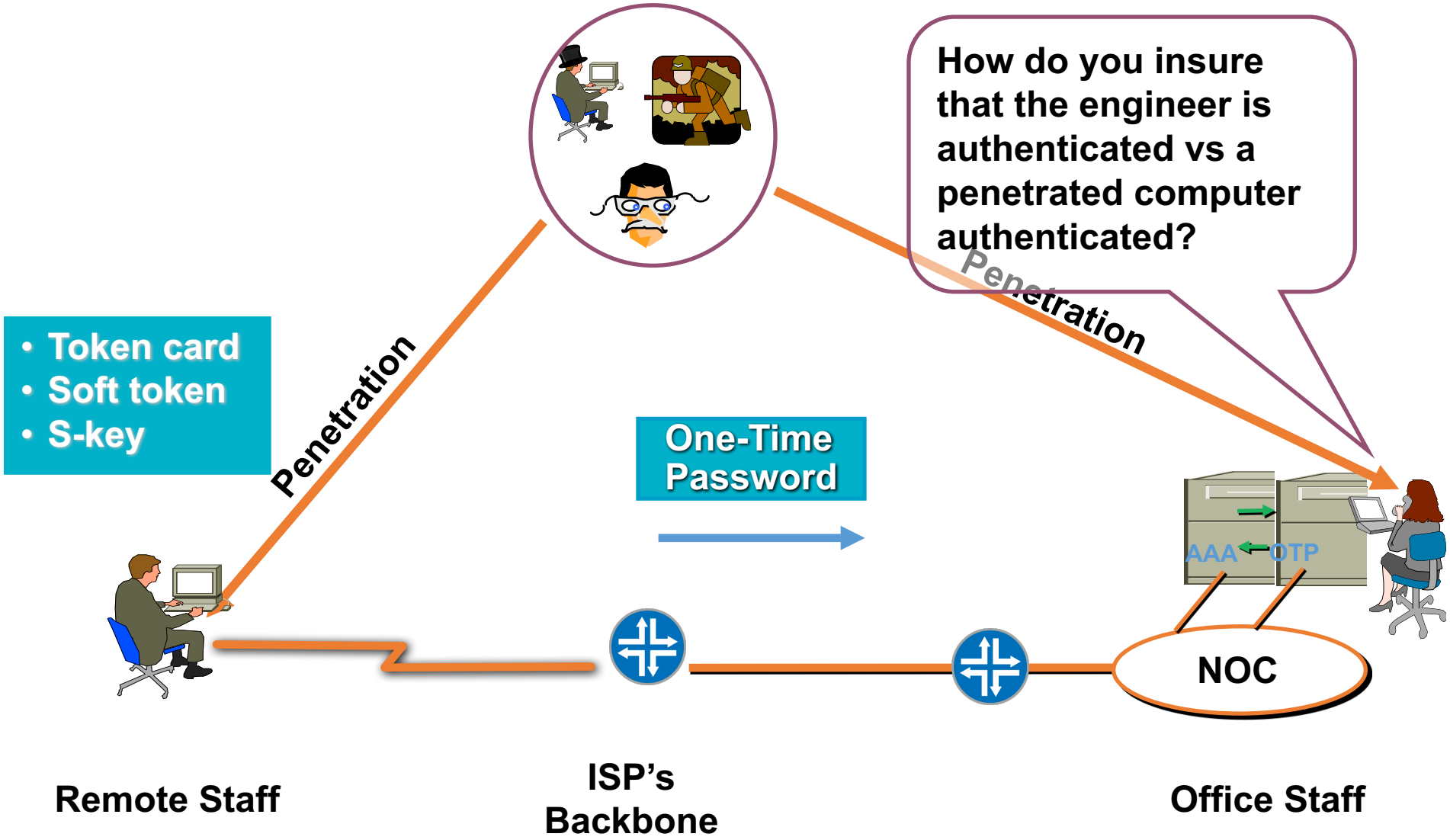


Remote Sta

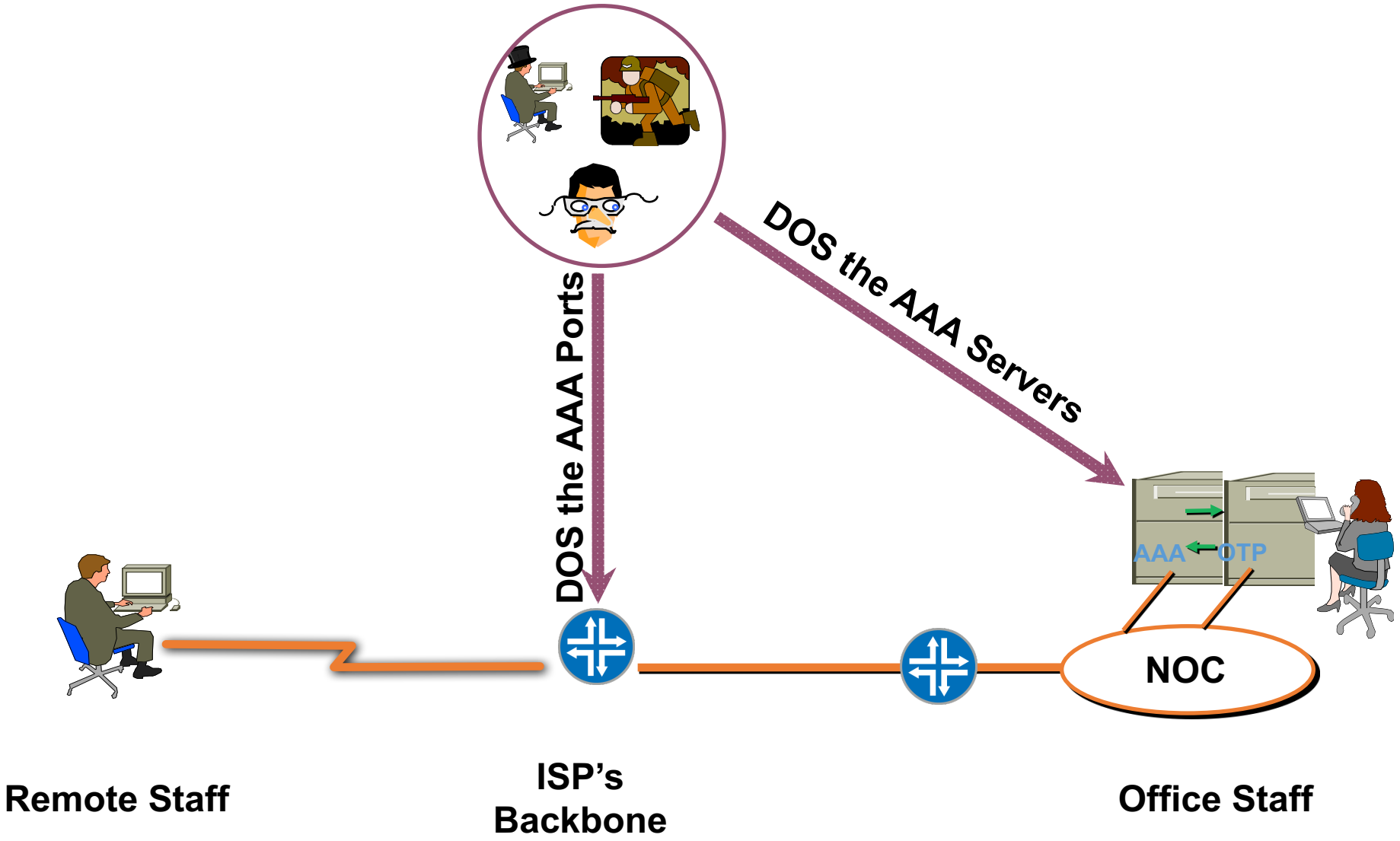
Why make a big deal about SSH to the router when you choose to put your network at risk using Radius as a AAA solution?

Office Staff

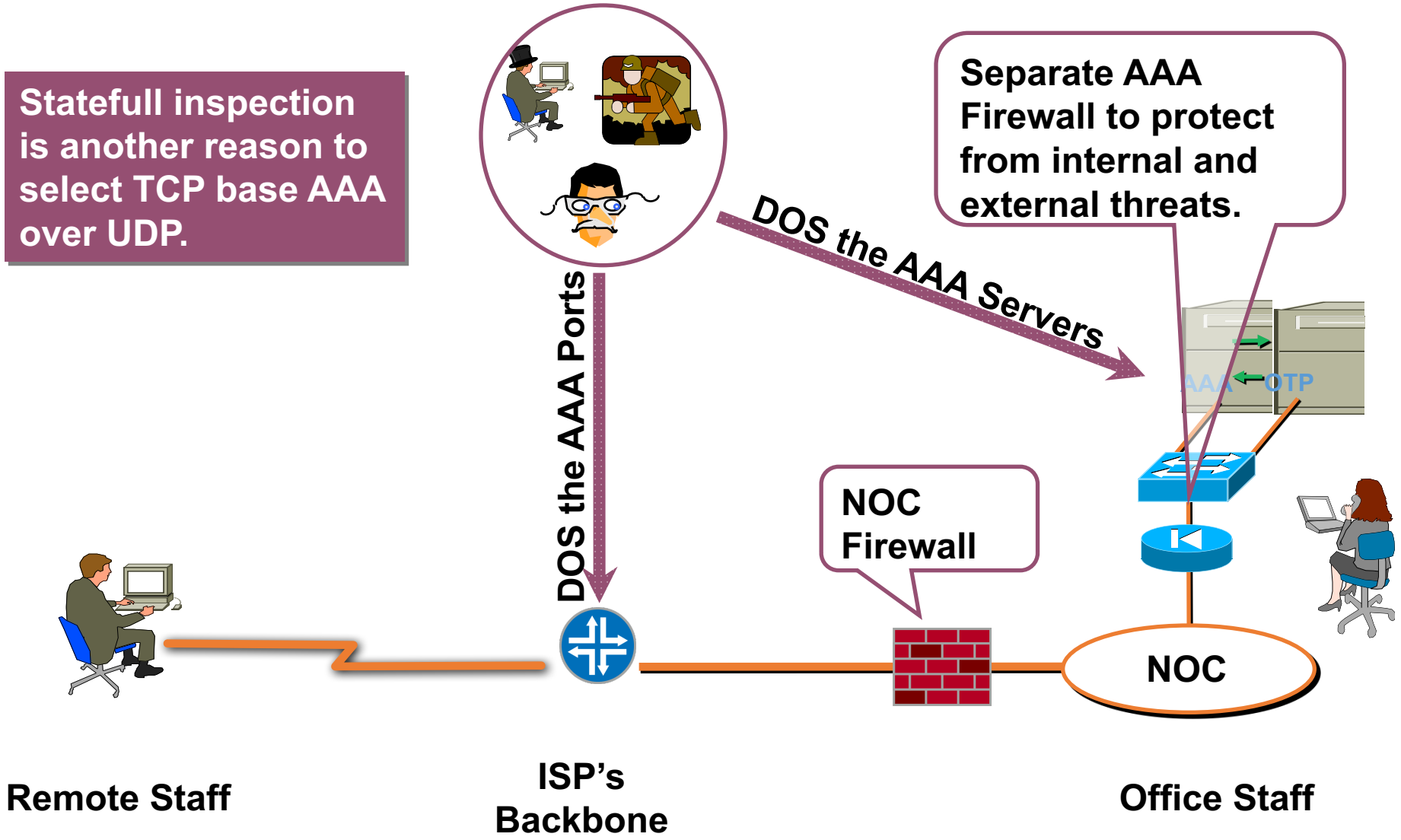
One Time Password – Checking the ID



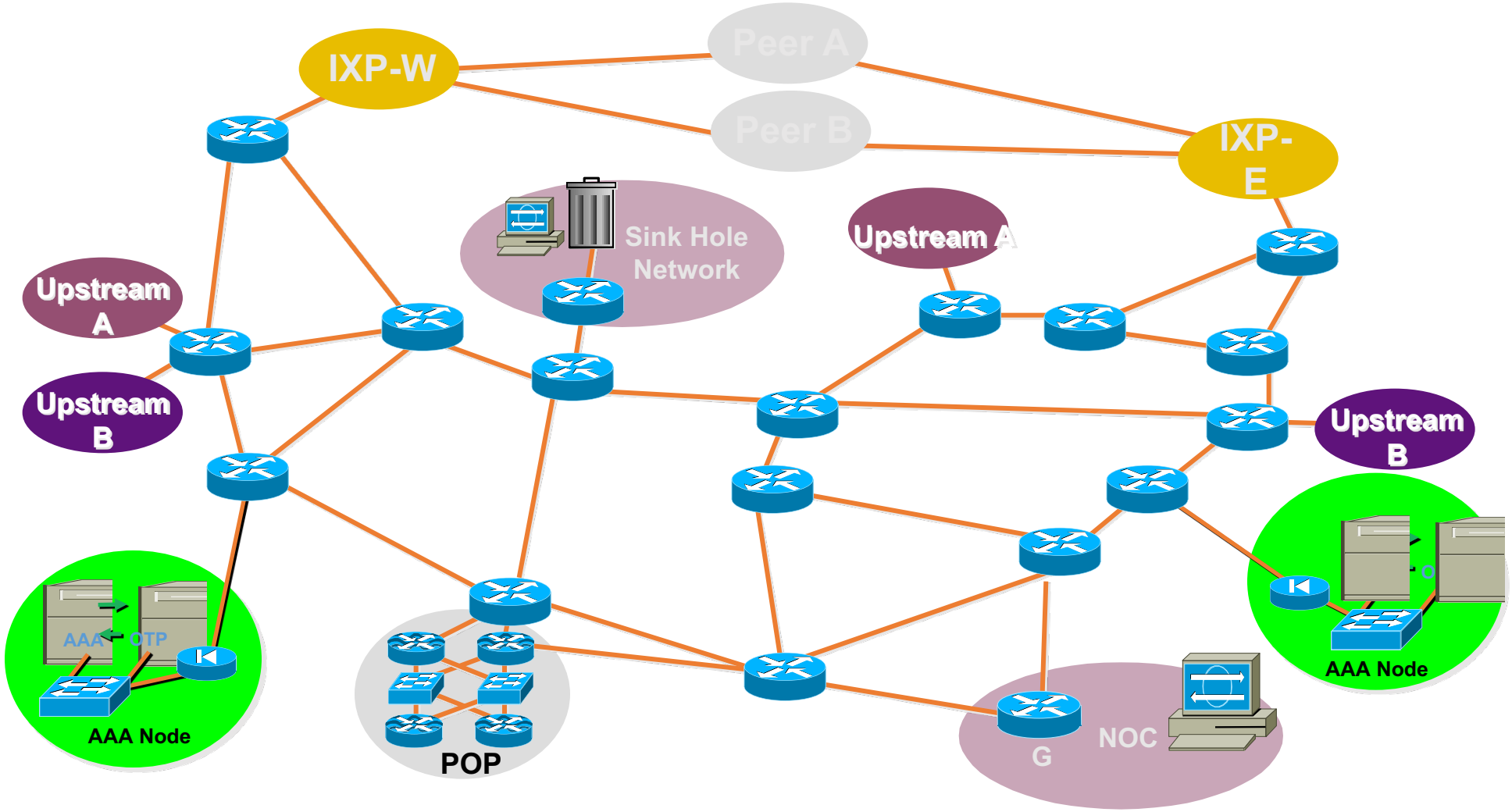
DOSing the AAA Infrastructure



Use a Firewall to Isolate the AAA Servers



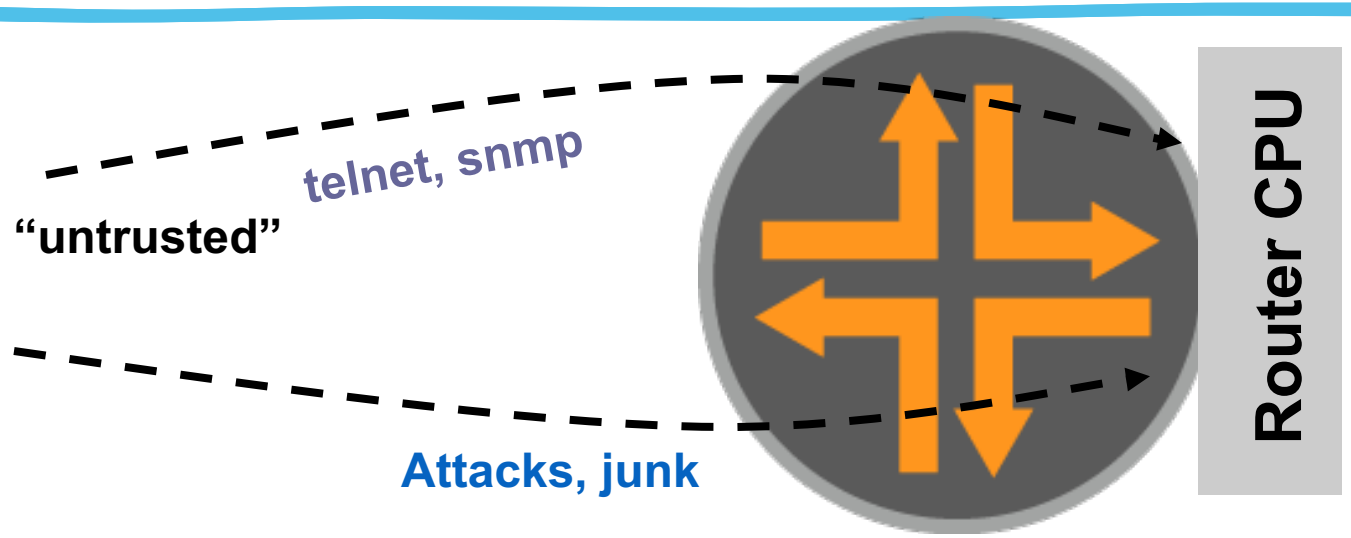
Distribute AAA Servers and Config Backup



TACACS+ URLs

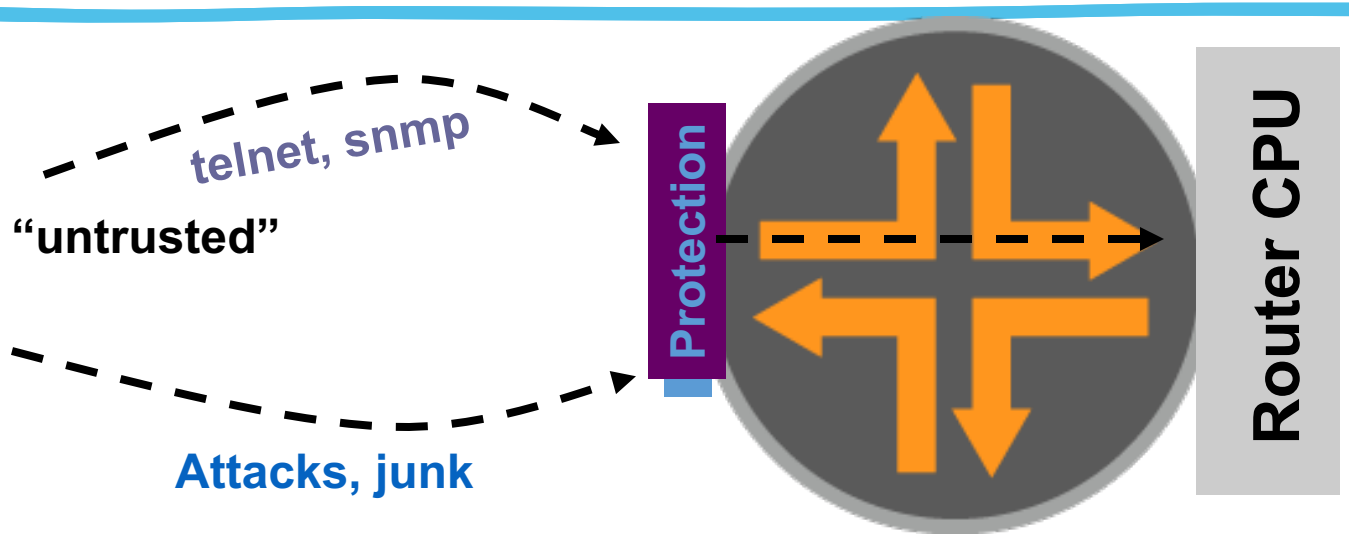
- TACACS+ Open Source
  - ftp://ftp-eng.cisco.com/pub/tacacs/
  - Includes the IETF Draft, Source, and Specs.
- Extended TACACS++ server
  - http://freshmeat.net/projects/tacpp/
- TACACS + mods
  - http://www.shrubbery.net/tac_plus/

The Old World: Router Perspective



- Policy enforced at process level (VTY ACL, Kernel 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
- Protecting The Router Control Plane draft-ietf-opsec-protect-control-plane-04

Watch the Config!

- There has been many times where the only way you know someone has violated the router is that a config has changed.
- If course you need to be monitoring your configs.

Config Monitoring

- **RANCID - Really Awesome New Cisco config Differ (but works with lots of routers – used a lot with Juniper Routers)**

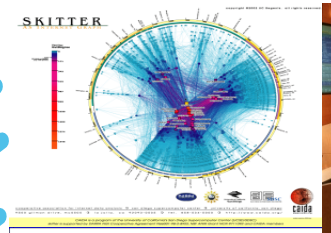
  http://www.shrubbery.net/rancid/

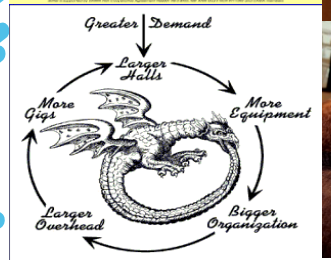
  http://www.nanog.org/mtg-0310/rancid.html

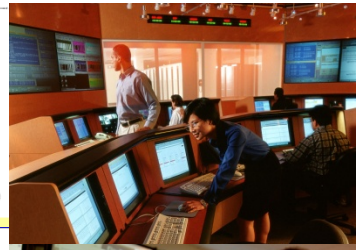
- **Rancid monitors a device's configuration (software & hardware) using CVS.**

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

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 MAINTENANCE 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.
^
```

- This is a legal requirement in some jurisdictions. Check with your legal group.

Exec Banner

- Useful to remind logged in staff 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

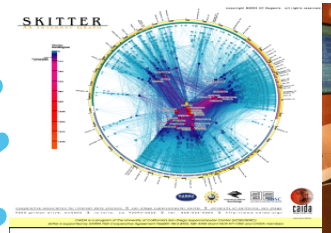
```
enable secret <removed>
no enable password
service password-encryption
```

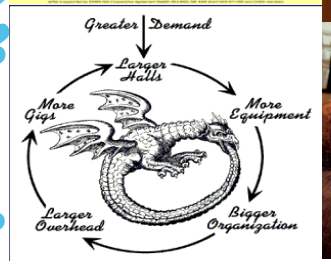
HOMEWORK

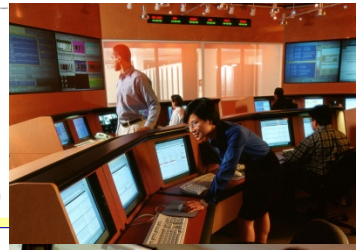
- Spot Check several router configurations. Are all these recommendations configured on your routers?
- Are banners set for the router?

© 2003 Cisco Systems, Inc. All rights reserved.

Controlling Access to the Router



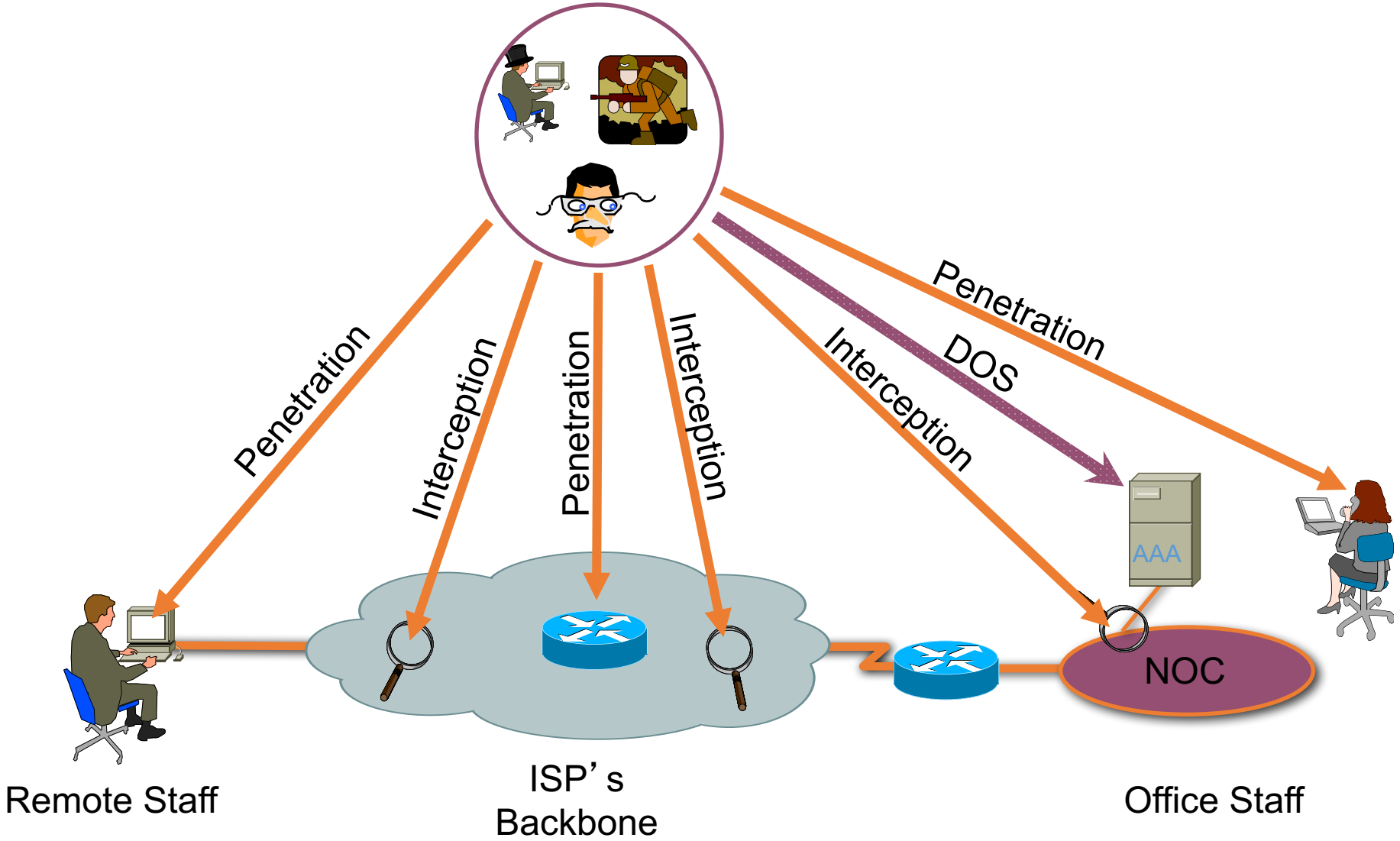




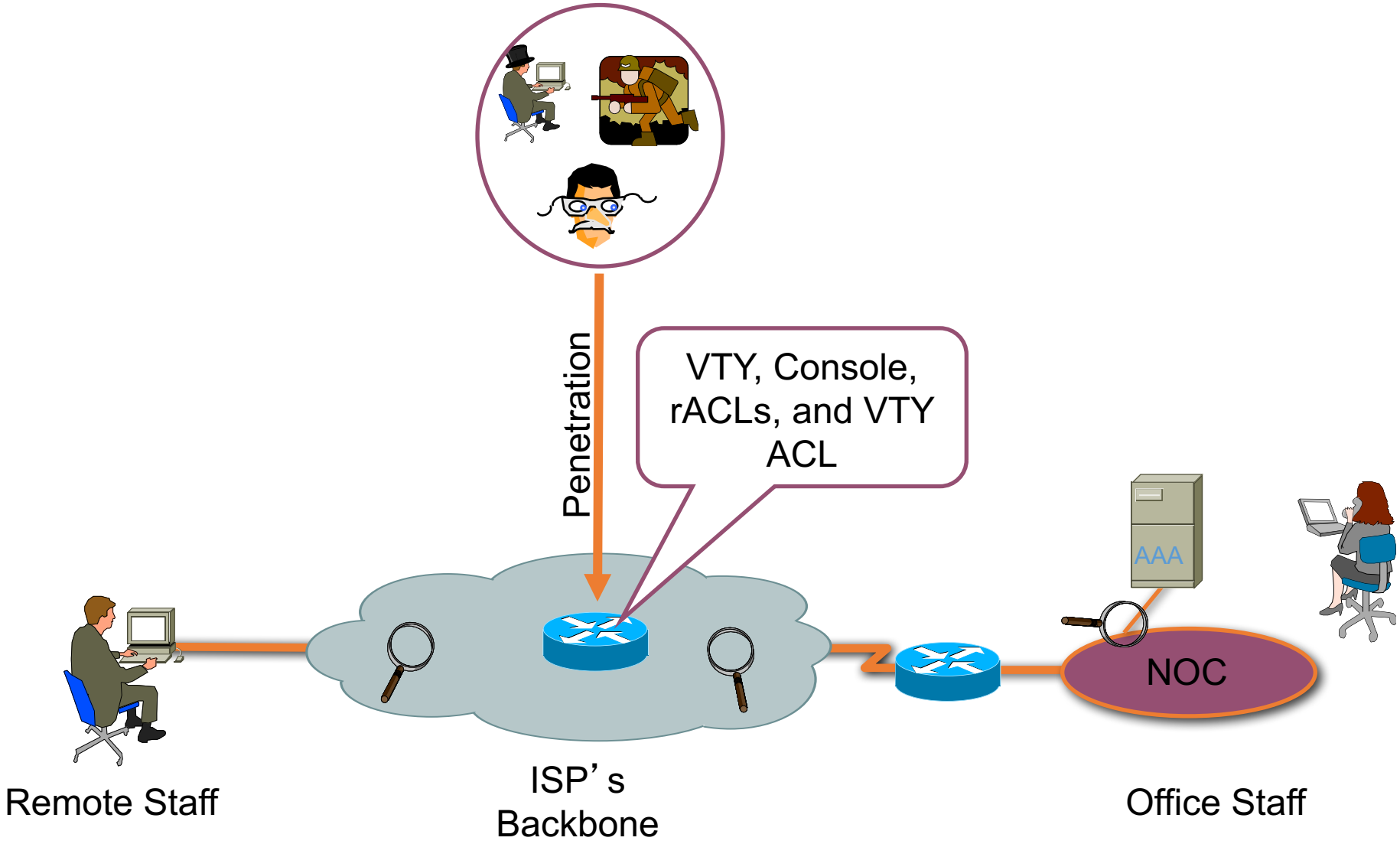
ISP Tools to Secure Access to the Router

- ✓ Lock down the Device
- ✓ Encrypted Access – SSH
- ✓ Local AAA
- ✓ External AAA with CLI Audit
- ✓ One-Time Passwords (OTP)
- ✓ Protecting the AAA Infrastructure

RISK Assessment



Lock Down the VTY and Console Ports



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

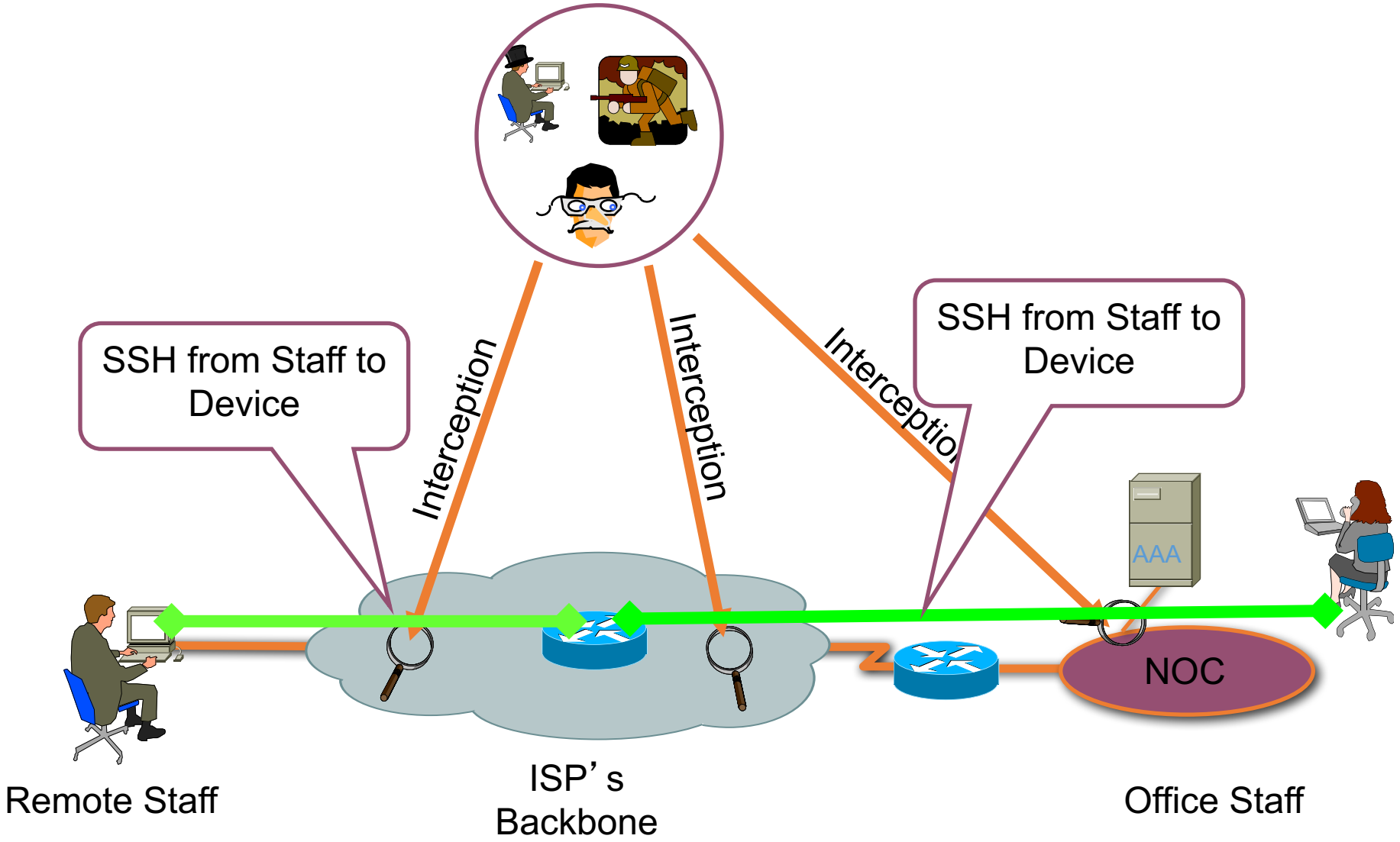
```
access-list 199 permit tcp 1.2.3.0 0.0.0.255 any
access-list 199 permit tcp 1.2.4.0 0.0.0.255 any
access-list 199 deny   tcp any any range 0 65535 log
access-list 199 deny   ip any any log
```

HOMEWORK

- Are basic AAA set with Username/Password?
- Do you have VTY ACLs?

© 2003 Cisco Systems, Inc. All rights reserved.

Encrypt the Traffic from Staff to Device

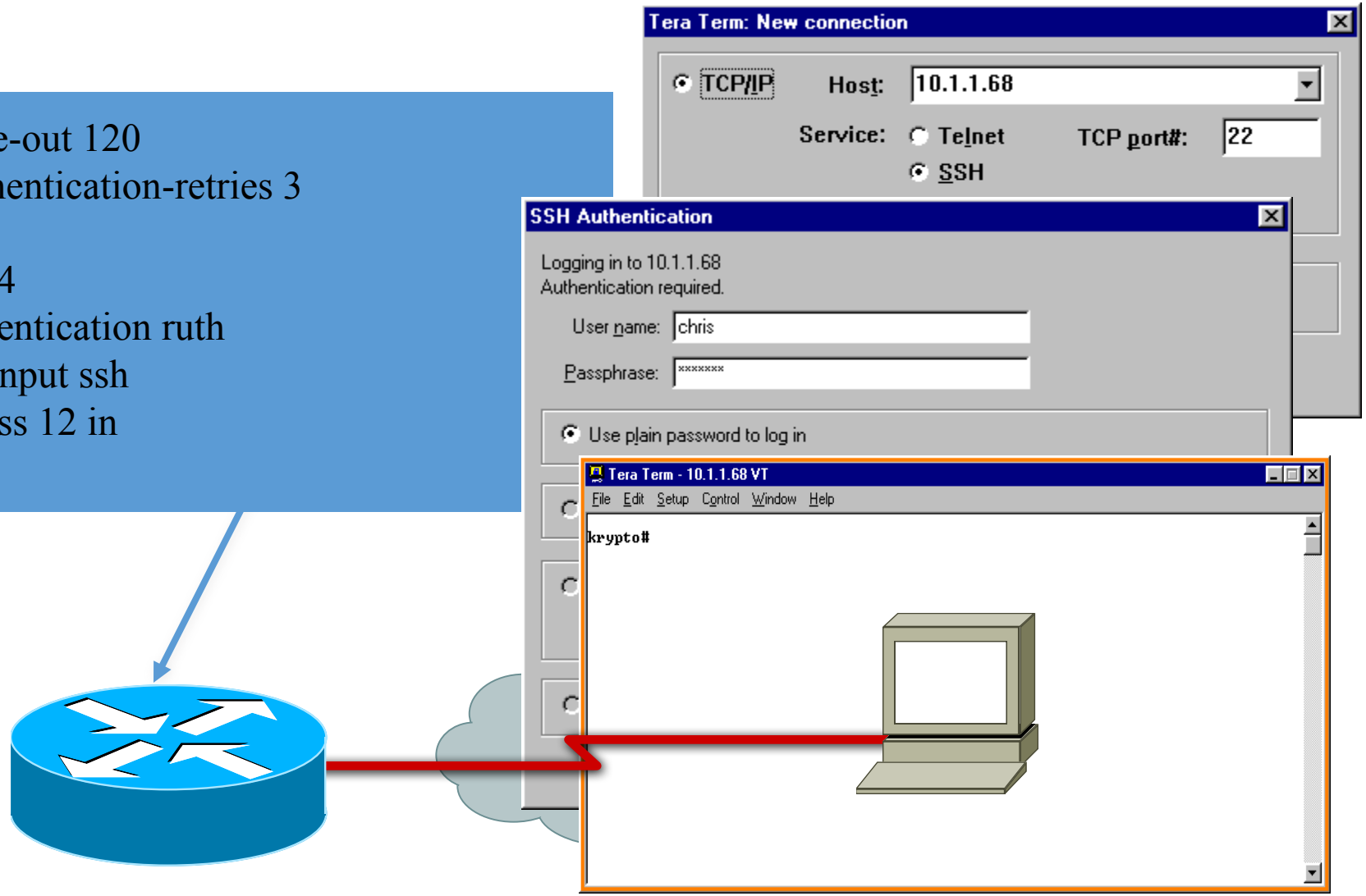


SSH Support in ISP Code

- Cisco IOS Software supports SSHv1 using protocol version 1.5. Version 2 is in the coding queue.
- SSH Server
  - Server for remote connections
- SSH Client
  - SSH connections can be generated from router to another router or to the SSH server
- SCP
  - Enables the copying of config and image files to and from the router via SSH
- SSH Terminal-Line Access (Reverse-SSH)
  - Accessing terminal lines of the router via 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
```



SSH Server Implementation

- SSH requires the crypto subsystem because the server needs the capability to generate RSA keys.
- Does not require any functionality from the IPSEC code, thus certain crypto files have been decoupled to save resources.
- The SSH server for this release works with the SSH client and with public and commercial SSH clients.
- Does not support IP Security (future).
- Supports the following authentication methods: TACACS+, RADIUS & Local Authentication

SSH Server Configuration Prerequisites

- The Router's Hostname must be configured:

```
hostname <routername>
```

- The DNS Resolver on the Router must be configured:

```
ip domain-name rtp.cisco.com
```

- Crypto Keys must be configured:

```
crypto key generate rsa
```

- Note: When crypto keys are deleted, SSH server is disabled:

```
crypto key zeroise rsa
```

SSH Server Configuration

- Turn on SSH

```
ip ssh
```

- Set up the source interface

```
ip ssh source-interface
```

- Add it as input transport

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

SSH Server Configuration (contd.)

- To terminate SSH session connection on device:
  - Disconnect ssh [vty] *session-id*
- Vty (optional): virtual terminal for remote console access
- Session-id: connection number displayed in the ‘show ip ssh’ command output
- Note: clear line vty *n* command can be used instead

SSH Server Configuration Summary

0. (Configure hostname and domain (required!))
1. # crypto key generate rsa
2. (configure user authentication)
3. # ip ssh {[timeout *sec*]} | [authentication-retries *n*]}

Generate key pair

Enable ssh

Default: 120
max: 120

Default: 3
max: 5

Later:
show ip ssh

Connection	Version	Encryption	State	Username
0	1.5	3DES	4	guest

disconnect ssh <vty-number> (same as clear vty)

debug ip ssh

SSH Client Access

- 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.

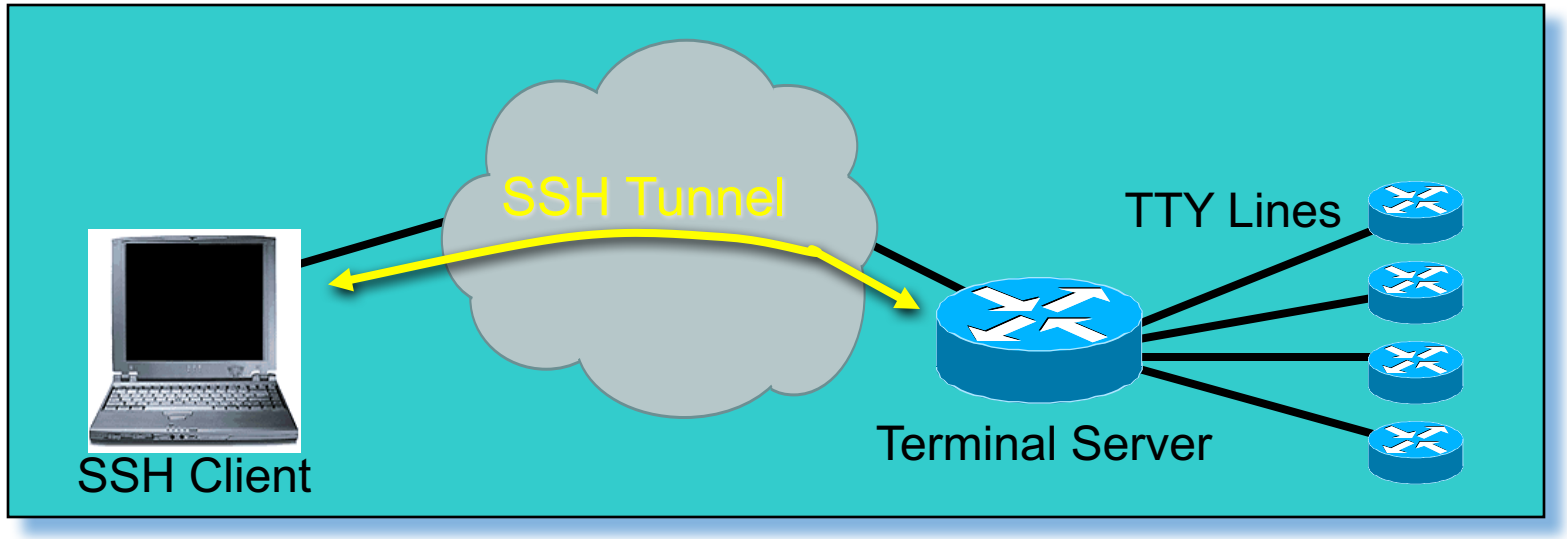
-p <portnum> Port to connect to on the remote host. Default is 22.

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

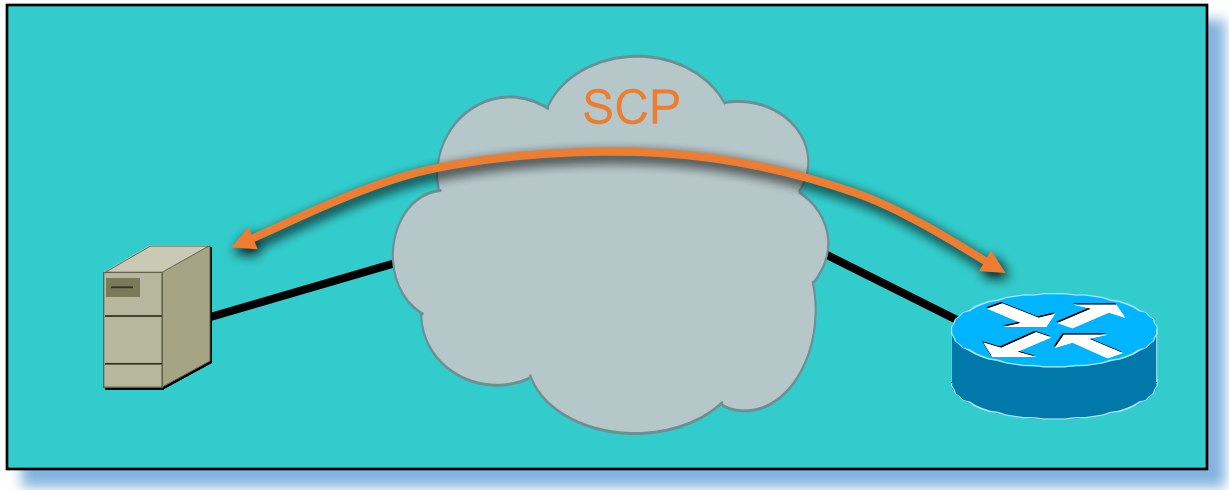
<IOS command> is an IOS exec command enclosed in quotes (ie "). This will be executed on connection and then the connection will be terminated when the command has completed.

SSH Terminal-Line Access

- How can security be increased on Telnet sessions, when using terminal servers for access to console ports in data center
- Included a feature to allow SSH access to lines in async modules, allowing encrypted access to TTY connections



Secure Copy (SCP)



- Secure File Copy with SSH encryption:
  - Router Configs
  - Router IOS Images

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18.html

Secure Copy (SCP)

```
! Server configuration, client side is always available:
aaa authentication login default local
aaa authorization exec default local
username pgustafs privilege 15 password 0 lab
ip scp server enable
! scp relies on AAA authentication and authorization to function  You'll need to configure AAA and enable for SCP server
```

Cisco IOS CLI dialogue:

```
scp -c 3des c4500-ik2s-mz.scp bstiff@cisco-lab:null:
bstiff@cisco-lab's password:
c4500-ik2s-mz.scp | 1072 KB | 67.0 kB/s | ETA: 00:01:24 | 15%
```

Uses SSH encryption hence RSA keys needs to be generated.

(crypto key generate rsa)

SSH Troubleshooting
show ip ssh

- Output with SSH enabled:
  - Switch# show ip ssh
  - SSH Enabled – version 1.5
  - Authentication timeout: 120 seconds; Authentication retries: 3
- Output with SSH disabled:
  - Switch# show ip ssh
  - %SSH has not been enabled

SSH Troubleshooting
sh ssh

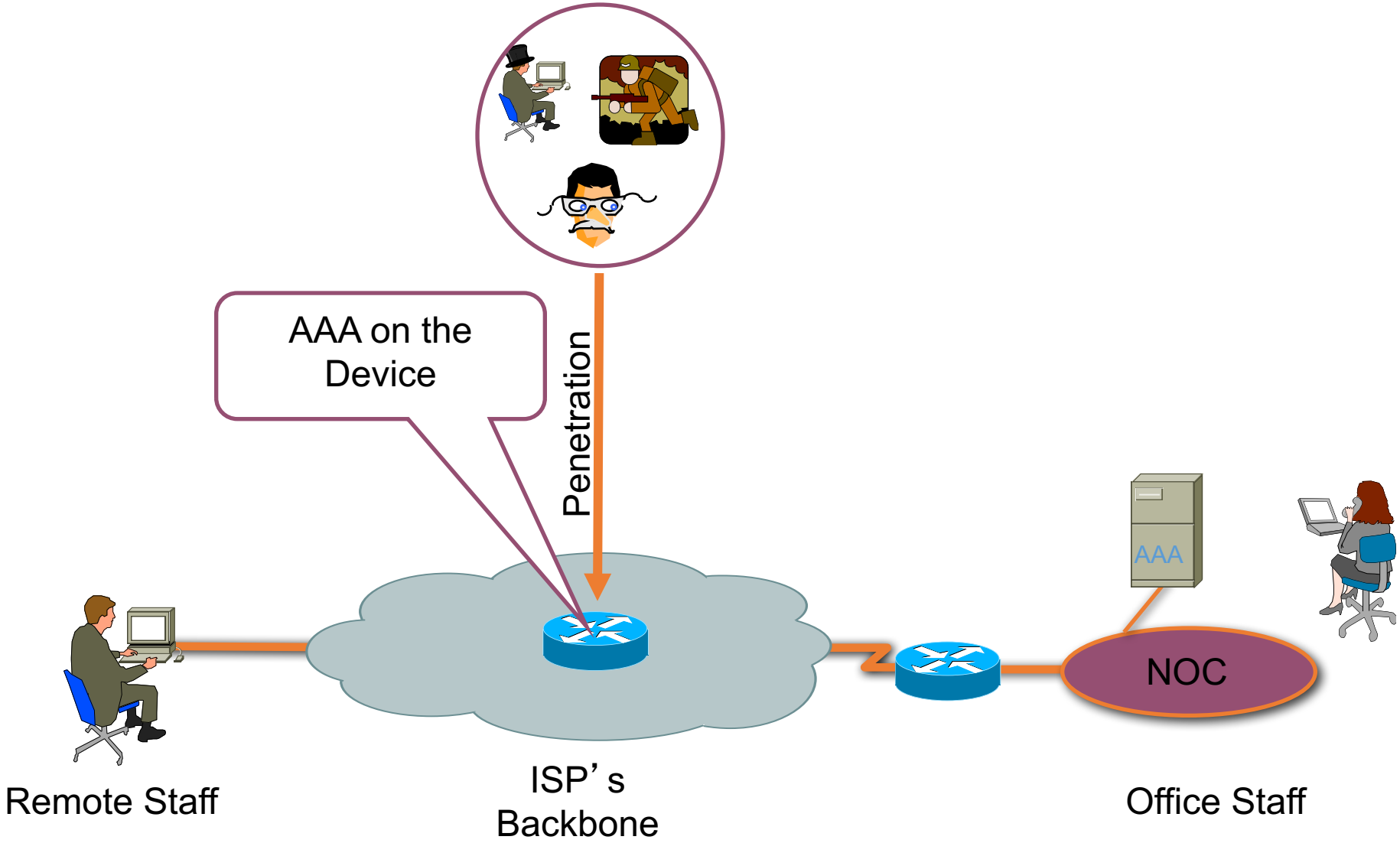
- Used to display status of SSH connections
- When SSH is enabled:
  - Switch# show ssh
  - Connection Version Encryption State Username
  - 0 1.5 3DES Session started guest
- When SSH is disabled:
  - Switch# show ssh
  - %No SSH server connections running

HOMEWORK

- Are basic AAA set with Username/Password?
- Do you have VTY ACLs?
- Are you using SSH?

© 2003 Cisco Systems, Inc. All rights reserved.

Staff AAA to get into the Device



What is ISP AAA and ISP AA?

- ISPs get network infrastructure access and customer access confused!
  - Infrastructure access needs to be Authentication, Authorization, and Accounting (AAA) are used secure your network. *Accounting* is really an *Audit* function.
    - (Focus: Operational Accountability.)
  - Customer access needs to be Authentication and Accounting (AA). Authorization is rarely used.
    - (Focus: Billing)
- Endemic problem of ISPs thinking that their existing customer accounting solution will help them secure their network.

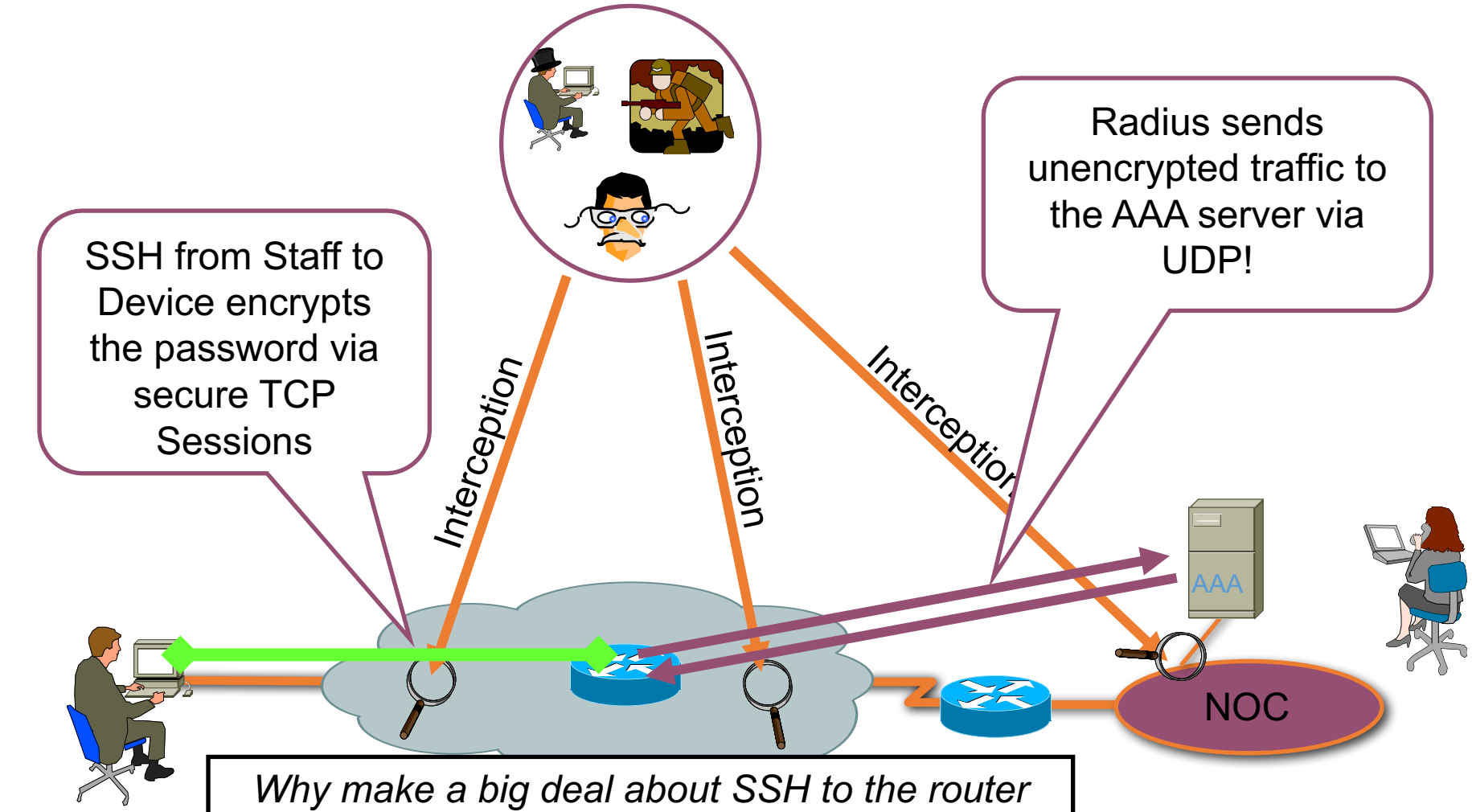
Separate Security Domains!

- Network Infrastructure Access and Customer Access are separate security domains.
  - Network Infrastructure access is controlled by the network operations team.
  - Customer access is controlled by the customer provisioning team.
- Requirement to have two AAA solutions on customer edge equipment.
  - Radius for customers
  - TACACS+/Kerberos for Network Infrastructure access.

Staff AAA – You have Two Choices!

- There are currently two industry solutions for an ISPs AAA Requirements:
  - Kerberos
  - TACACS+
- Radius <u>is not</u> an option!
- Why?

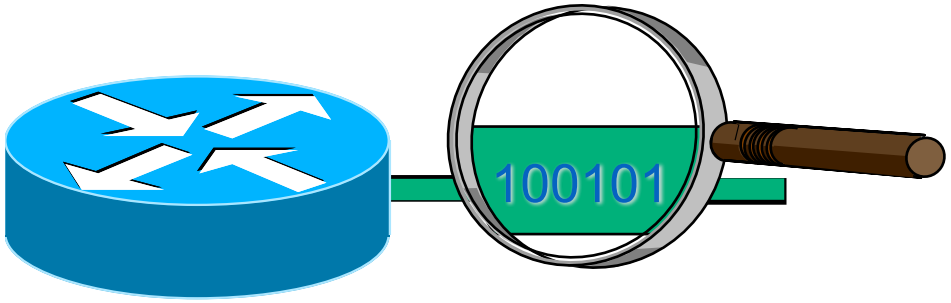
Radius is not an ISP AAA Option! Why?



Why make a big deal about SSH to the router when you choose to put your network at risk using Radius as a AAA solution?

Case of Cluelessness

- Kerberos and TACACS+ both work for network security. Any vendor who pushes *Radius* as a network security tool is clueless and is recommending a solution that puts your network at risk.
- If you need SSH, then you need encrypted communication from the router to the AAA server!



RADIUS vs. TACACS+ vs Kerberos

	RADIUS	TACACS+	KERBEROS
Uses UDP	X		
Uses TCP		X	X
Encryption	Password Only	All But Header	All But Header
Multiprotocol Support		X	
Router Mgt Acct Control		X	X
Router Mgt Auth Control		X	X
LEAP Support	X		
XAUTH Support	X	X	X

http://www.cisco.com/warp/public/480/10.html

UDP vs. TCP with AAA Protocols

- Why UDP for RADIUS:
  - If the request to a primary Authentication server fails, a secondary server must be queried.
  - The timing requirements of this particular protocol are significantly different than TCP provides.
  - The stateless nature of this protocol simplifies the use of UDP.
  - UDP simplifies the server implementation.
- Why TCP for TACACS+ & Kerberos:
  - TCP offers a connection-oriented transport, while UDP offers best effort delivery.
  - TCP provides a separate acknowledgment that a request has been received.
  - TCP provides immediate indication of an unavailable server
  - By using TCP keepalives, you can detect server crashes out-of-band with actual requests.
  - TCP offers advantages through statefull firewall inspection tools.

What to Configure?

1. Local Authentication to provide a failsafe.
2. Authentication with AAA Server with (TACACS+ used in this example).
3. Accounting/Audit with AAA Server
4. Authorization with AAA Server
5. One Time Password Solution

Simple Staff Authentication and Failsafe

- Username/Passwords on the Router are used as a back-up when the AAA system goes down.

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

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

Simple Staff Authentication and Failsafe

- 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

Simple Staff Authentication and Failsafe

- 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 <u>internal</u> security threat.

Staff Authentication

- `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`

Staff Accountability & Audit

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

Checkpoint w/ Authentication and Accounting

- 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 5 1104181051B1
username jim password 5 0317B21895FE
```

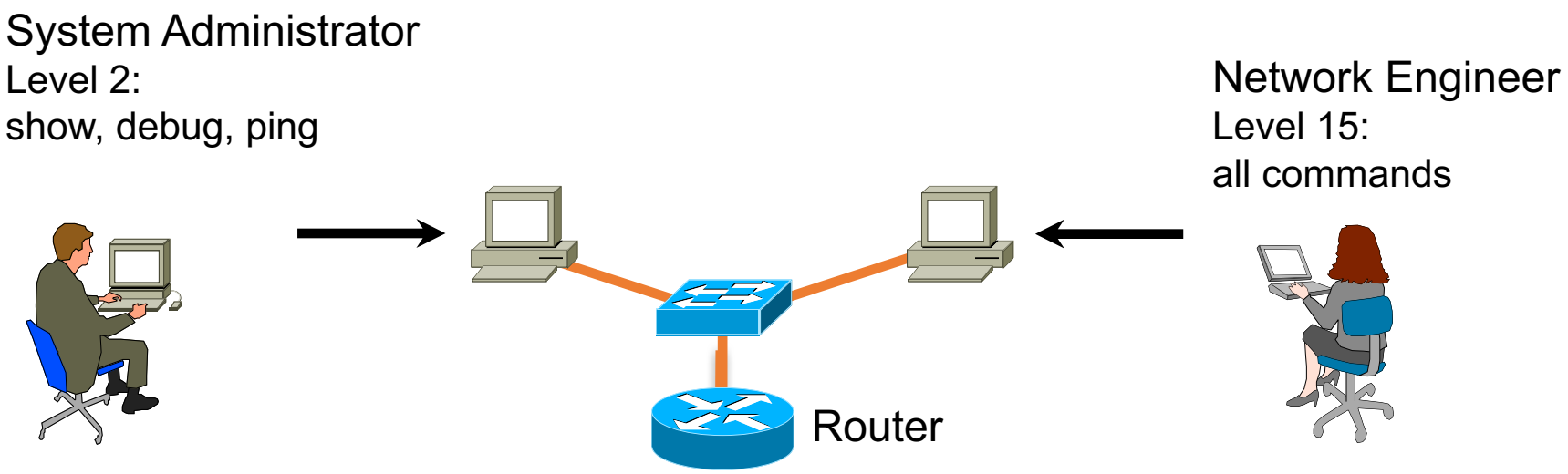
HOMEWORK

- Are basic AAA set with Username/Password?
- Do you have VTY ACLs?
- Are you using SSH?
- Are you using TACACS+ or Kerberos for staff access to all devices in a network?

© 2003 Cisco Systems, Inc. All rights reserved.

Limit Authority – Authorize Commands

- Differentiate staff authority on the router
  - Help desk
  - Operations
  - Second level/third level support
- Use privilege levels (0–15)



Set Privileges

- Set level of privilege for each user class

```
privilege configure level 5 interface
privilege interface level 5 shutdown
privilege exec level 5 show ip route
privilege exec level 5 configure terminal
privilege exec level 5 show running-config
```

Checkpoint with default Authorization

- So now you can have the following:

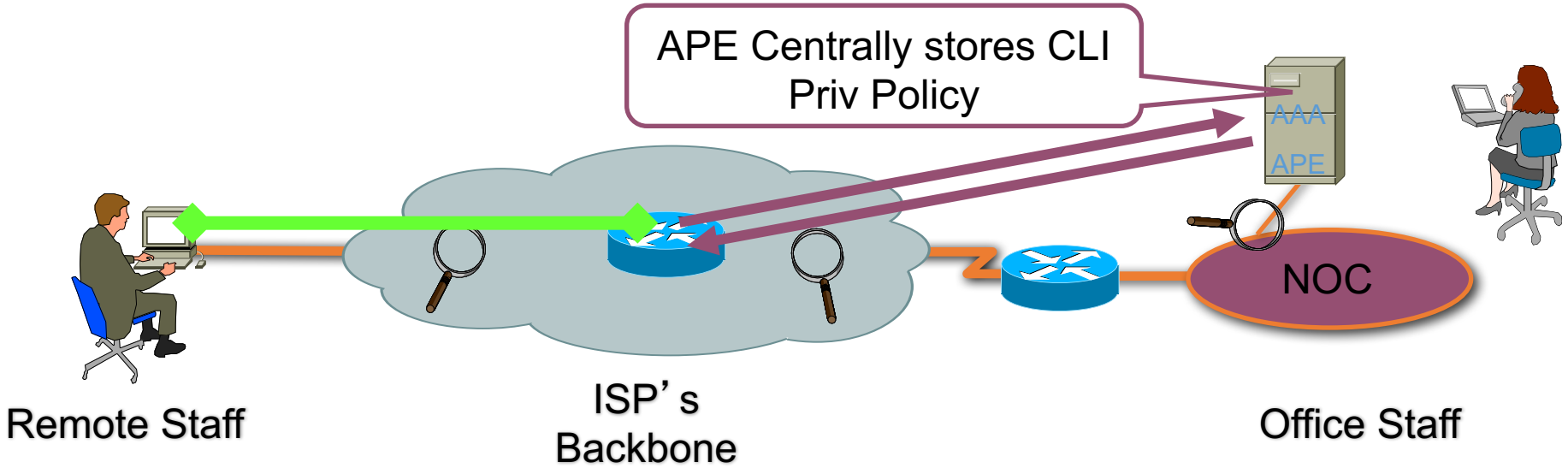
```
aaa new-model
aaa authentication login default tacacs+ local enable
aaa authentication enable default tacacs+ local enable
aaa authorization exec default tacacs+ local
aaa authorization commands 1 default tacacs+ local
aaa authorization commands 15 default tacacs+ local
aaa accounting exec start-stop 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 privilege 15 password 5 1104181051B1
username jim privilege 1 password 5 0317B21895FE
```

Note on Privilege Levels and Authorization

- Privilege Levels are a initial pain to set up and deploy.
- That pain is an *initial* pain typical of any security feature deployment.
- Once it is deployed, it value quickly out weights the deployment pain.
- Remember – Data shows that 70% of all Internet Backbone Outages are Maintenance Injected Trouble! It just takes one L1 maintenance person to redistribute BGP into the IGP.

The Answer to Priv-Level's Pain: APE

- Administrative Policy Engine (APE)
  - Replacement for the TACACS+ Server
  - Per-command authentication tables stored – per role – on APE.



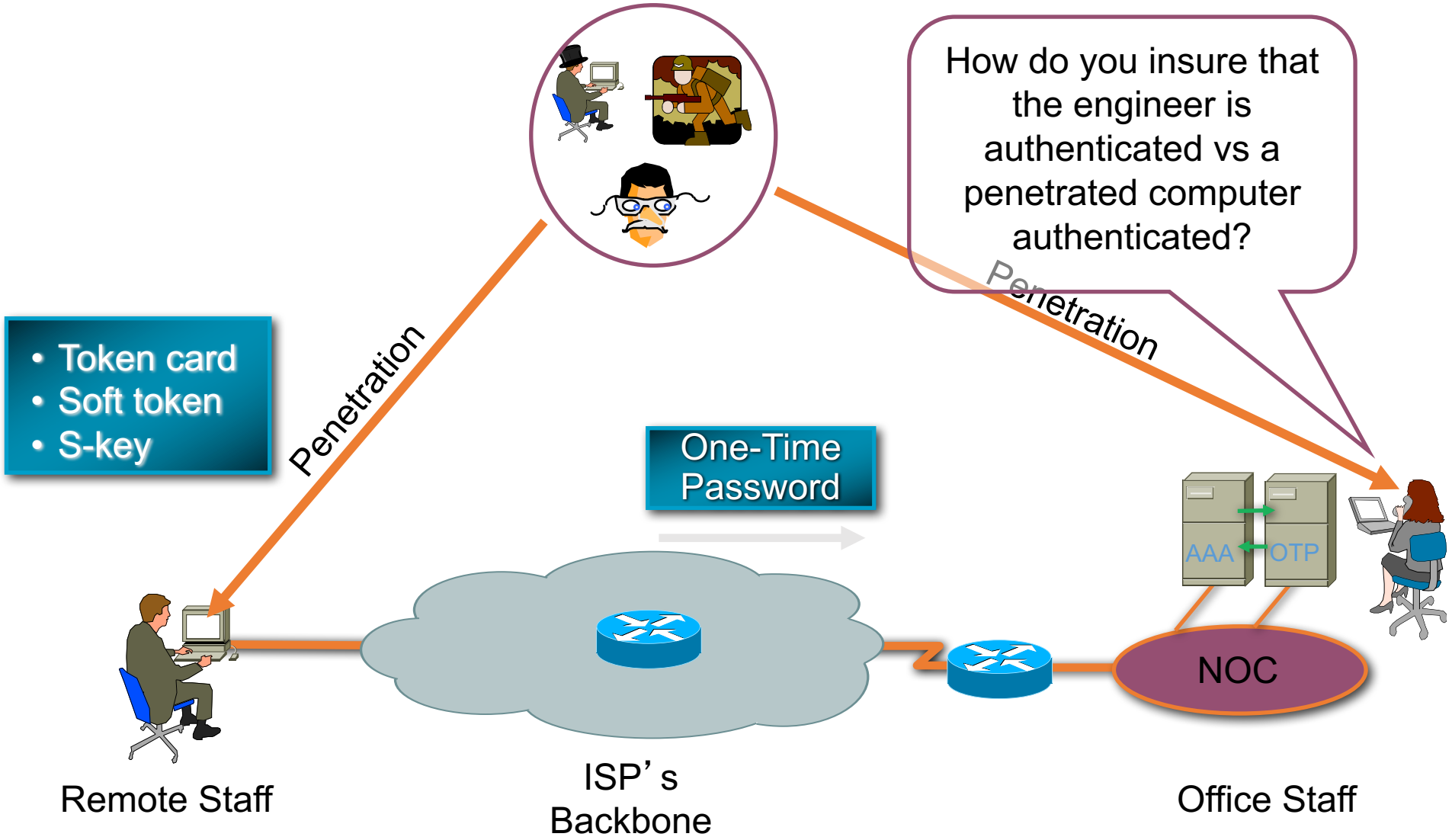
APE – Per Role – Per Command – Per Device

HOMEWORK

- Are basic AAA set with Username/Password?
- Do you have VTY ACLs?
- Are you using SSH?
- Are you using TACACS+ or Kerberos for staff access to all devices in a network?
- Are you using Privilege/Role based access with your AAA server?

© 2003 Cisco Systems, Inc. All rights reserved.

One Time Password – Checking the ID



Identity Tools

- Digital equivalents of our physical identity cards:

(older technologies)

Username + passwords
One-time passwords
Kerberos

(newer technologies) RSA keypairs, PKI
Smartcards
Biometrics

What is One Time Password

- OTP is a system that requires the person to enter their private PIN, get a single use password, and use that single use password to gain access to the system.
  - This single use password can be used only once – hence *one time password.*
- Addresses issues of password sniffing and individual identity.

Kerberos

- Centralized “permission slips” ticketing system
- Developed at MIT, now IETF standard
- Client & server authentication service
- Timed service (can expire)
- Originally username+password only, now has support for PKI as well

RSA keypairs as Identity Tools

- RSA keypairs can serve as “what you have” factor of authentication
- Prove yourself by owning a set of keys that were exclusively belong to you

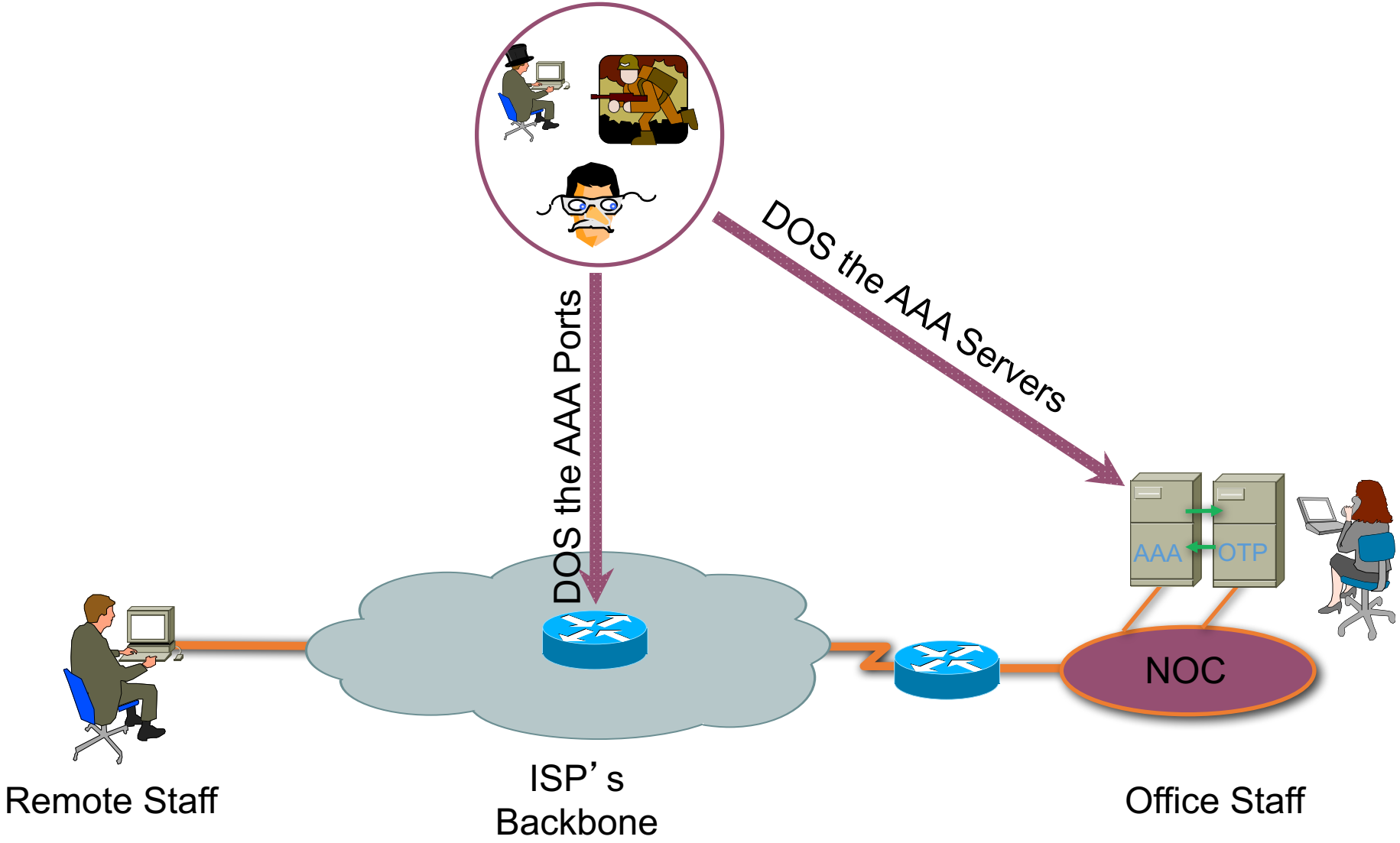
Smart Cards

- Smart cards can replace PKI desktop operations (signing and encyrpting) with more secure, card-based crypto & memory
- Smart cards are attractive because they are more secure, portable, convenient, an integration point

Fingerprints and Biometrics

- Newest, arguably the strongest, and still the most expensive technology for identity
- Standards, APIs process begun (www.biometrics.org)
- Cisco will track and support as market develops and customers deploy infrastructure required

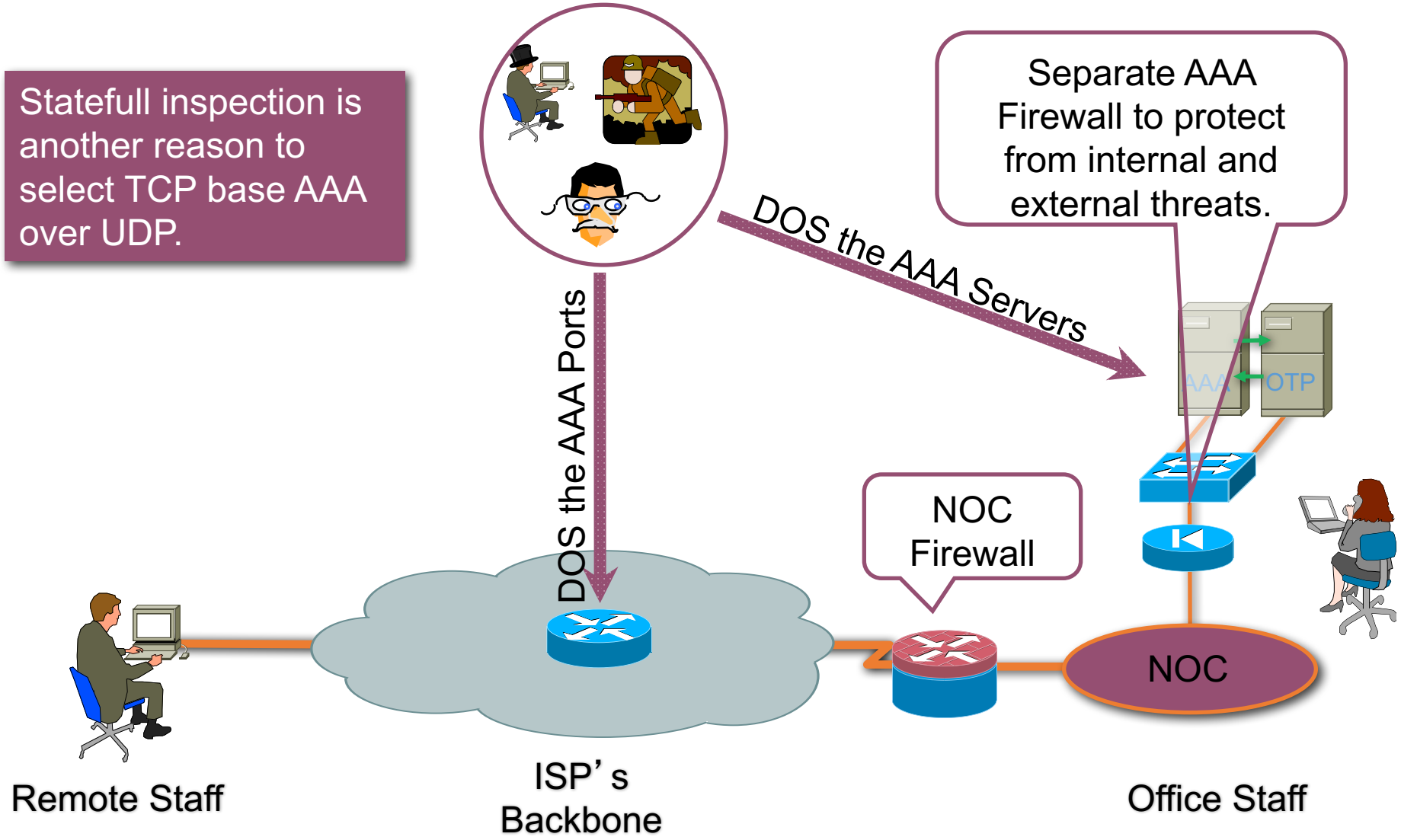
DOSing the AAA Infrastructure



How to protect the AAA Servers?

- Firewall
- Local AAA for Failsafe Access
- Distributed AAA Servers with Failover

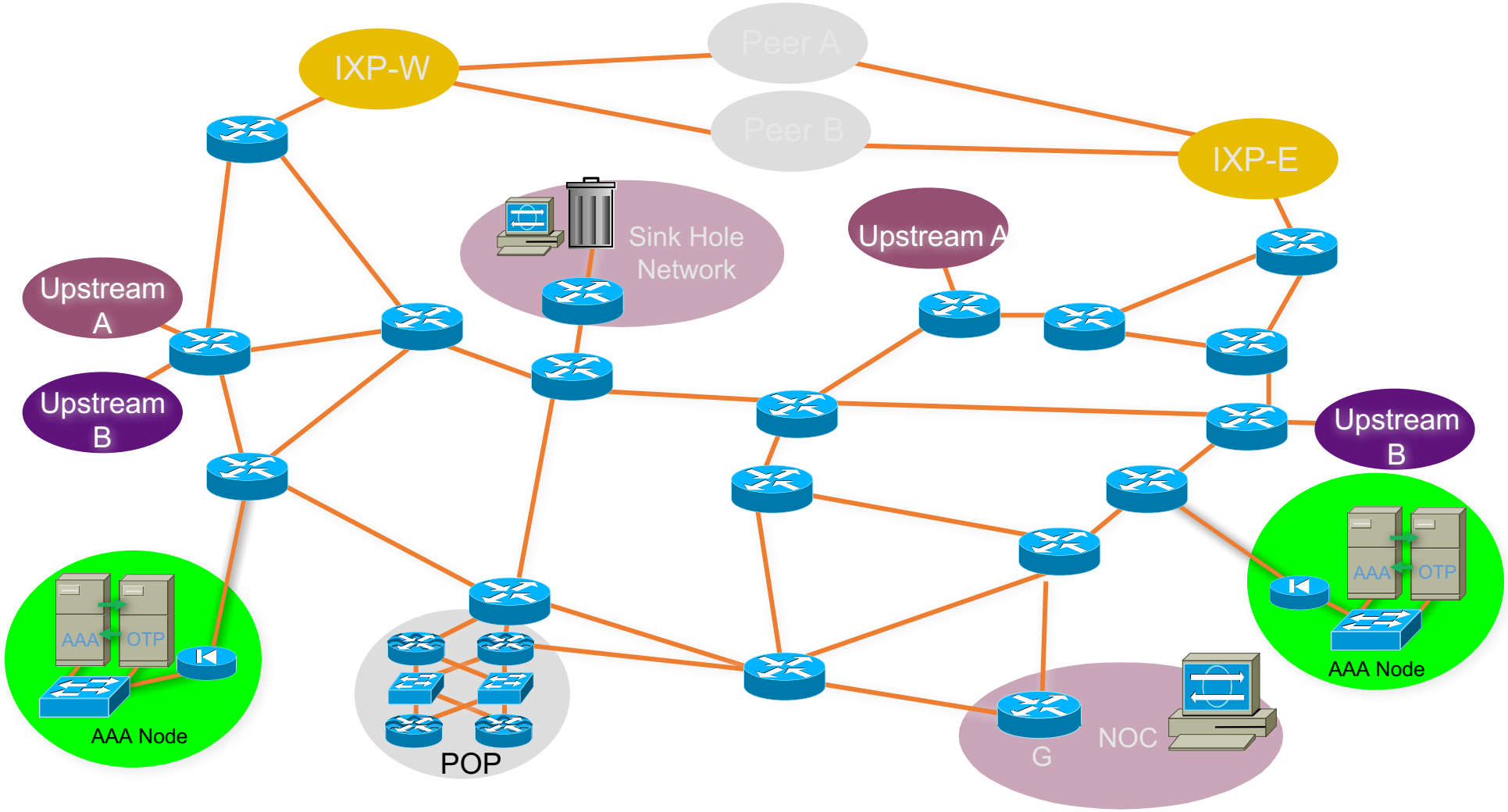
Use a Firewall to Isolate the AAA Servers



Simple Staff Authentication and Failsafe

- 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
- Take them out of the safe when total access to the AAA servers are lost.
  - Provides a automatic roll over from TACACS+/Kerberos to Local Authentication
- Keep you accessing the network while the AAA system is down from problems or an attack.

Distribute AAA Servers and Config Backup



TACACS+ Server Redundancy

Tries the first. If no response, then moves to the second. If no response then the next, until it fails on TACACS+ and moves to the next AAA option (local in this case).

```
tacacs-server host <primary ip>
tacacs-server host <secondary ip>
```

HOMEWORK

- Are basic AAA set with Username/Password?
- Do you have VTY ACLs?
- Are you using SSH?
- Are you using TACACS+ or Kerberos for staff access to all devices in a network?
- Does your AAA Servers have layered security protection?

© 2003 Cisco Systems, Inc. All rights reserved.

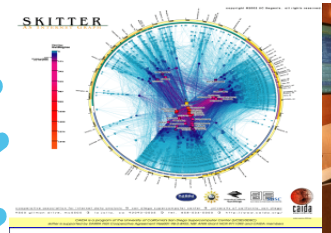
TACACS+ URLs

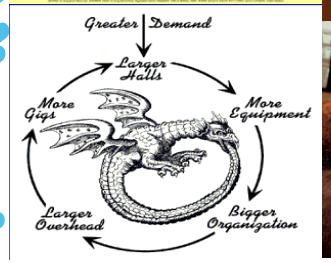
- TACACS+ Open Source
  - ftp://ftp-eng.cisco.com/pub/tacacs/
  - Includes the IETF Draft, Source, and Specs.
- Extended TACACS++ server
  - http://freshmeat.net/projects/tacpp/
- TACACS + mods
  - http://www.shrubbery.net/tac_plus/

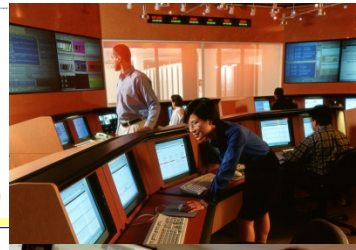
ISP Tools to Secure Access to the Router

- ✓ Lock down the Device
- ✓ Encrypted Access – SSH
- ✓ Local AAA
- ✓ External AAA with CLI Audit
- ✓ One-Time Passwords (OTP)
- ✓ Protecting the AAA Infrastructure

Resource Saturation Management







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
```

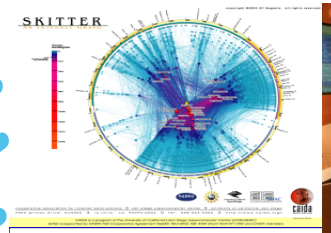
Very useful under heavy load!
Recommended Standard Config!

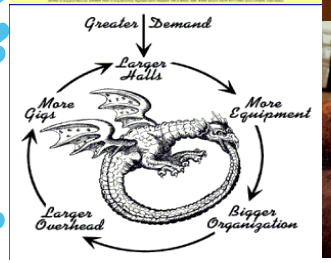
HOMEWORK

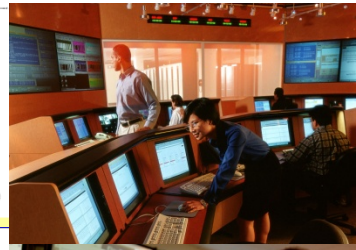
- Spot check the ICMP Unreachable settings on your Cisco IOS devices.

© 2003 Cisco Systems, Inc. All rights reserved.

Adding a 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)

TOUCHPOINT

- ✓ Routers <u>never</u> come with passwords or telnet enabled.
- ✓ Major router vendors have no *default passwords. If they do you should not buy them!*
- ✓ So anyone with a password of ‘cisco’ is someone who wants to get violated.

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

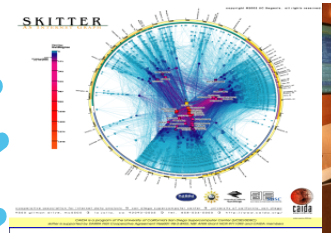
Secure Template Sources

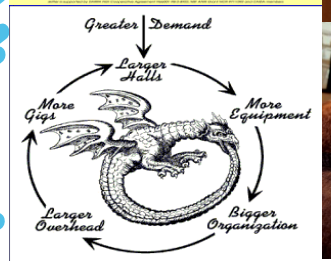
- ISP Essentials Materials (Security and Operational Practices)
  http://www.cisco.com/public/cons/isp/essentials/
  http://www.ispbook.com
- Improving Security on Cisco Routers
  http://www.cisco.com/warp/public/707/21.html
- Rob Thomas's Secure Configuration Templates
  http://www.cymru.com/~robt/Docs/Articles/index.html
- US National Security Agency's
  http://nsa1.www.conxion.com/cisco/download.htm

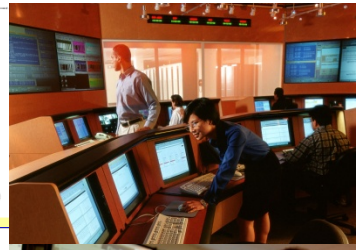
Summary

- 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

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

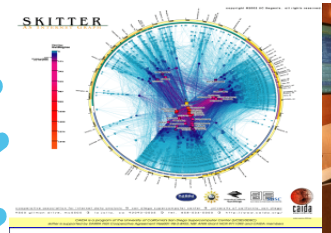
- IOS give many false positives.
- Ports are perceived to be open when often they are not connected to a service.
- Varies with IOS Version and Audit Tool
- ION is cleaning this up.
- Request – when you find them, please open a Bug (DDTS). Worst that can happen is that the Bug will be a duplicate.

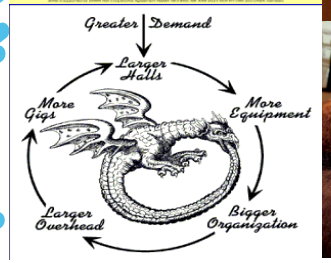
HOMEWORK

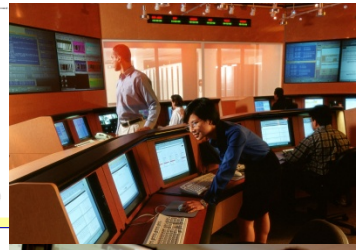
- Spot Check Routers checking what ports are open on them.
- Double check with a NMAP Scan on one or more of your routers.

© 2003 Cisco Systems, Inc. All rights reserved.

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

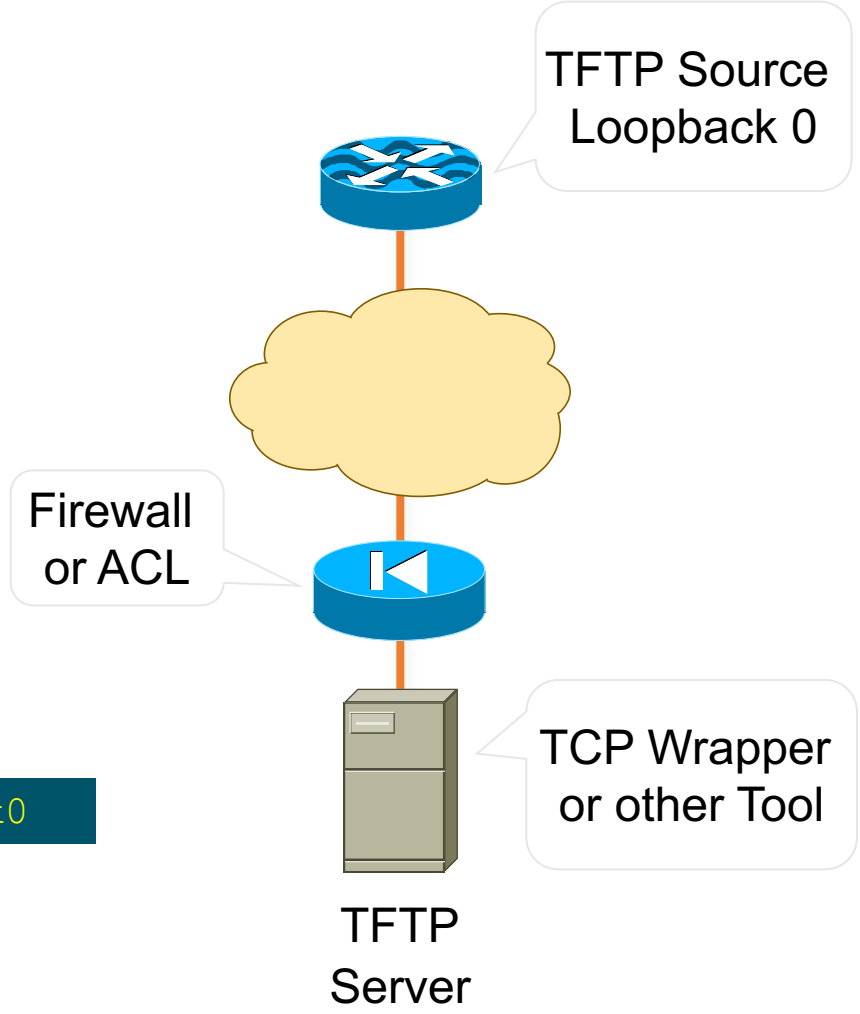
Configuration Management

- 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
```

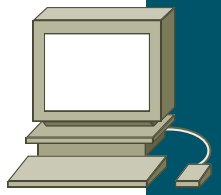
Use Detailed Logging

- 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
```

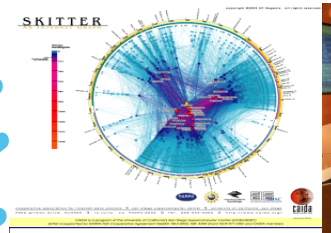
Use Detailed Logging

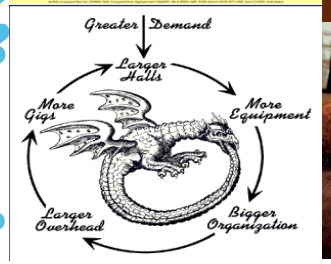
- Two topologies used:
  - Central Syslog servers in operations center
  - Syslog servers in major POPs

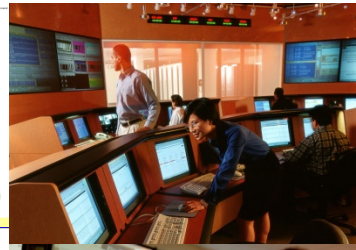


```
[philip@vectra log]$ tail -1 cisco.log
Nov  6 11:49:43 gw 2021: Nov  6 11:49:40.779 AEST: %SYS-
5-CONFIG_I: Configured from console by philip on vty0
(192.168.1.1)
[philip@vectra log]$ date
Tue Nov  6 11:50:04 EST 2001
[philip@vectra log]$
```

Time Synchronization & NTP







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

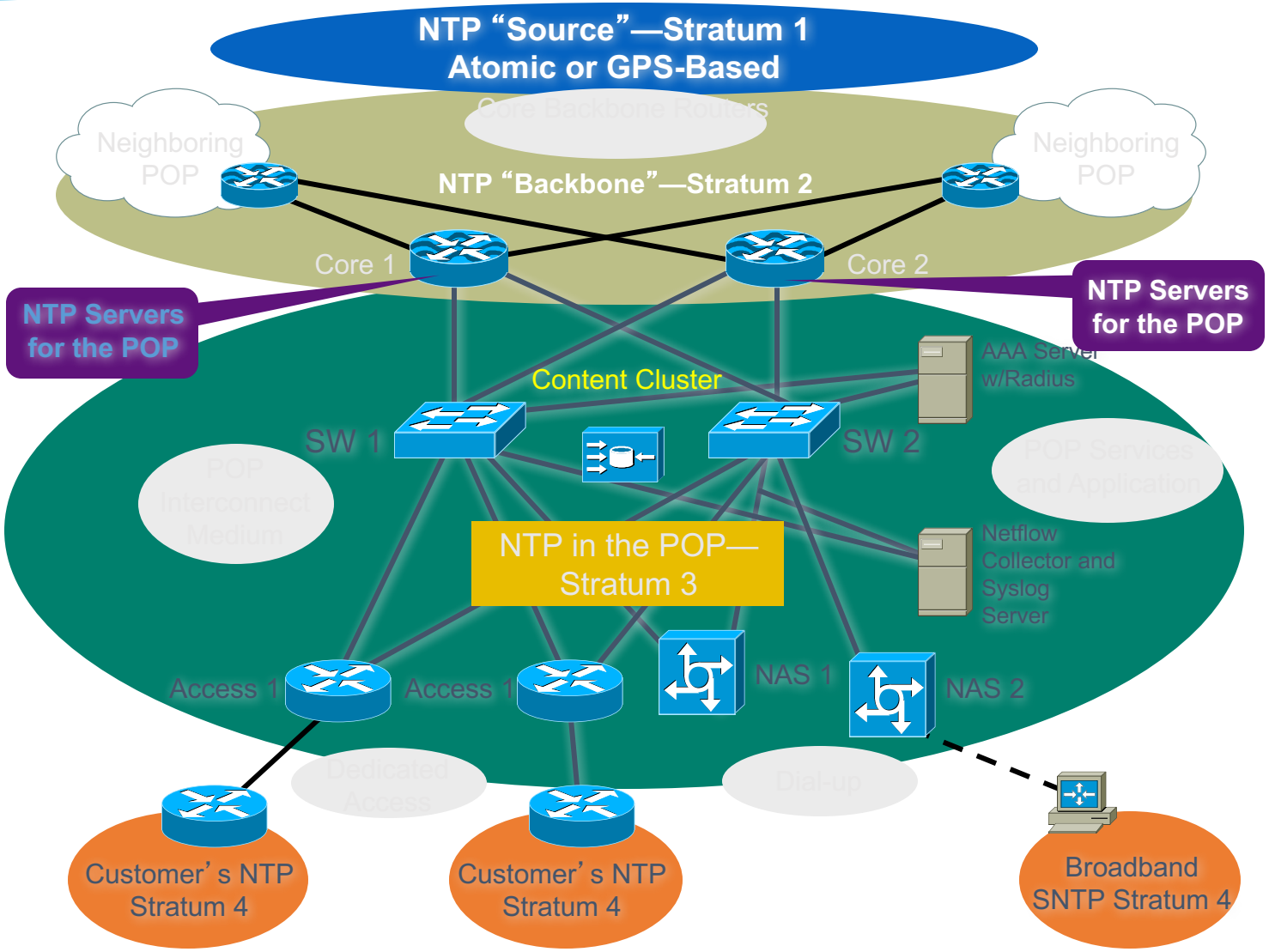
- Network Time Protocol (NTP) used to synchronize the time on all the devices
- NTP packets leave router with loopback address as source
- Configuration example:

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

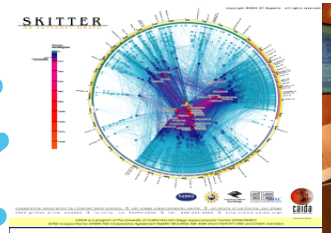
Network Time Protocol

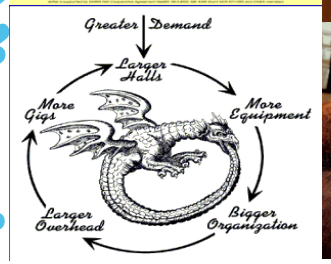
- Motivation—NTP security:
  - NTP systems can be protected by filters which only allow the NTP port to be accessed from the loopback address block
- Motivation—easy to understand NTP peerings:
  - NTP associations have the loopback address recorded as source address, not the egress interface

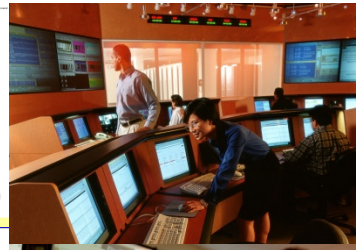
Network Time Protocol



Out of Band Management



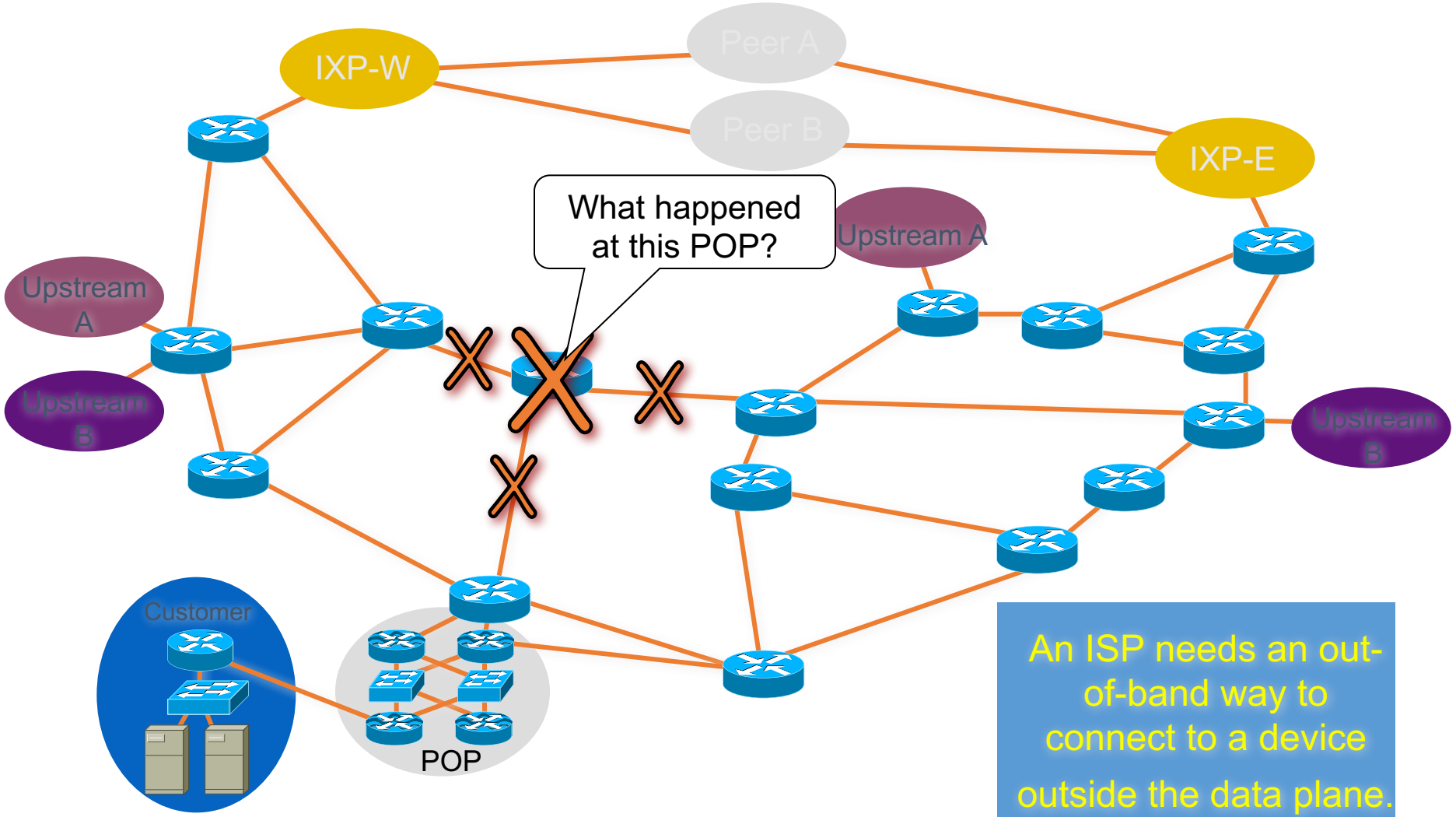




Terms

- 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?



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

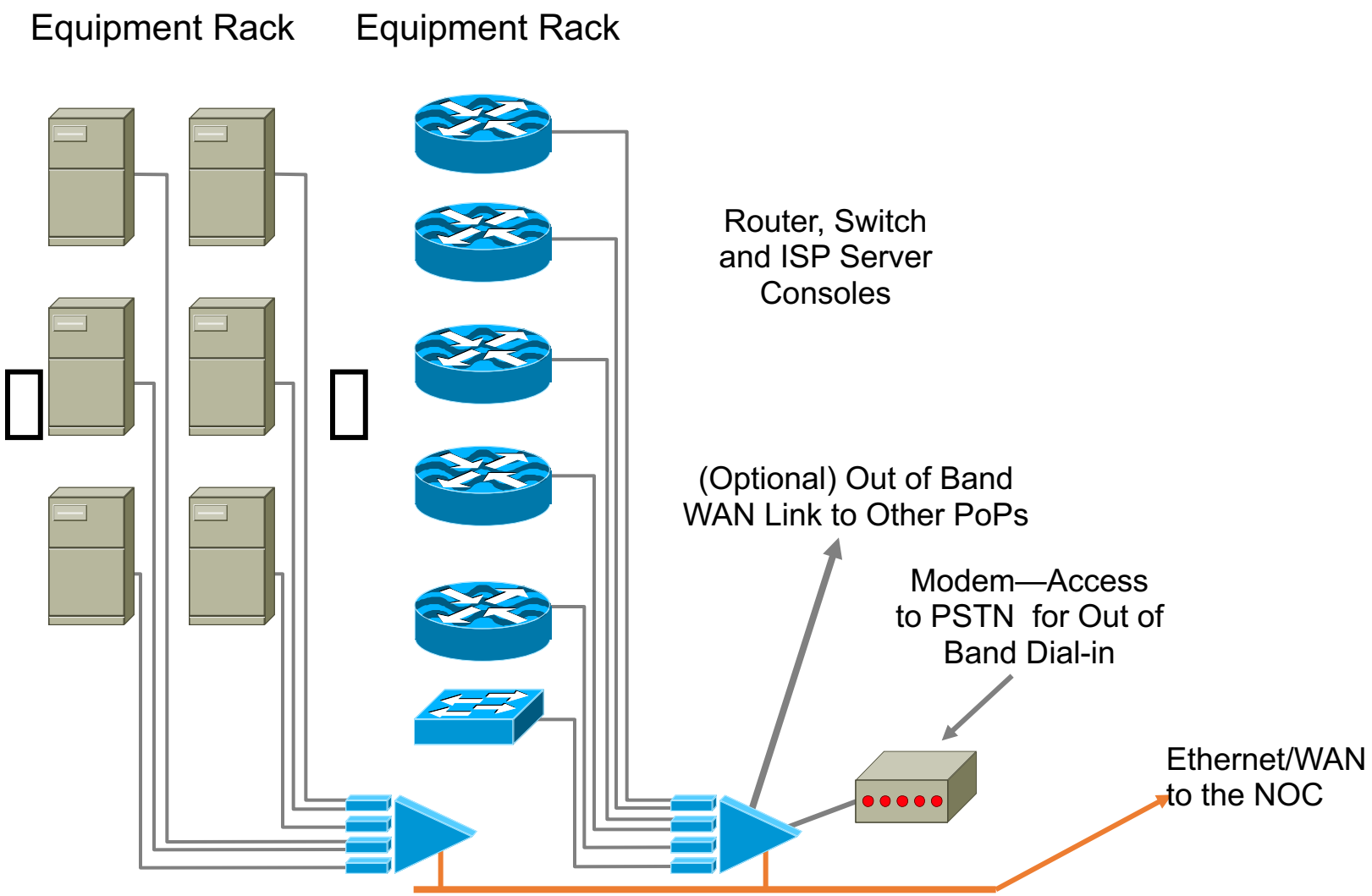
Out of Band Management (OOB)

- 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*

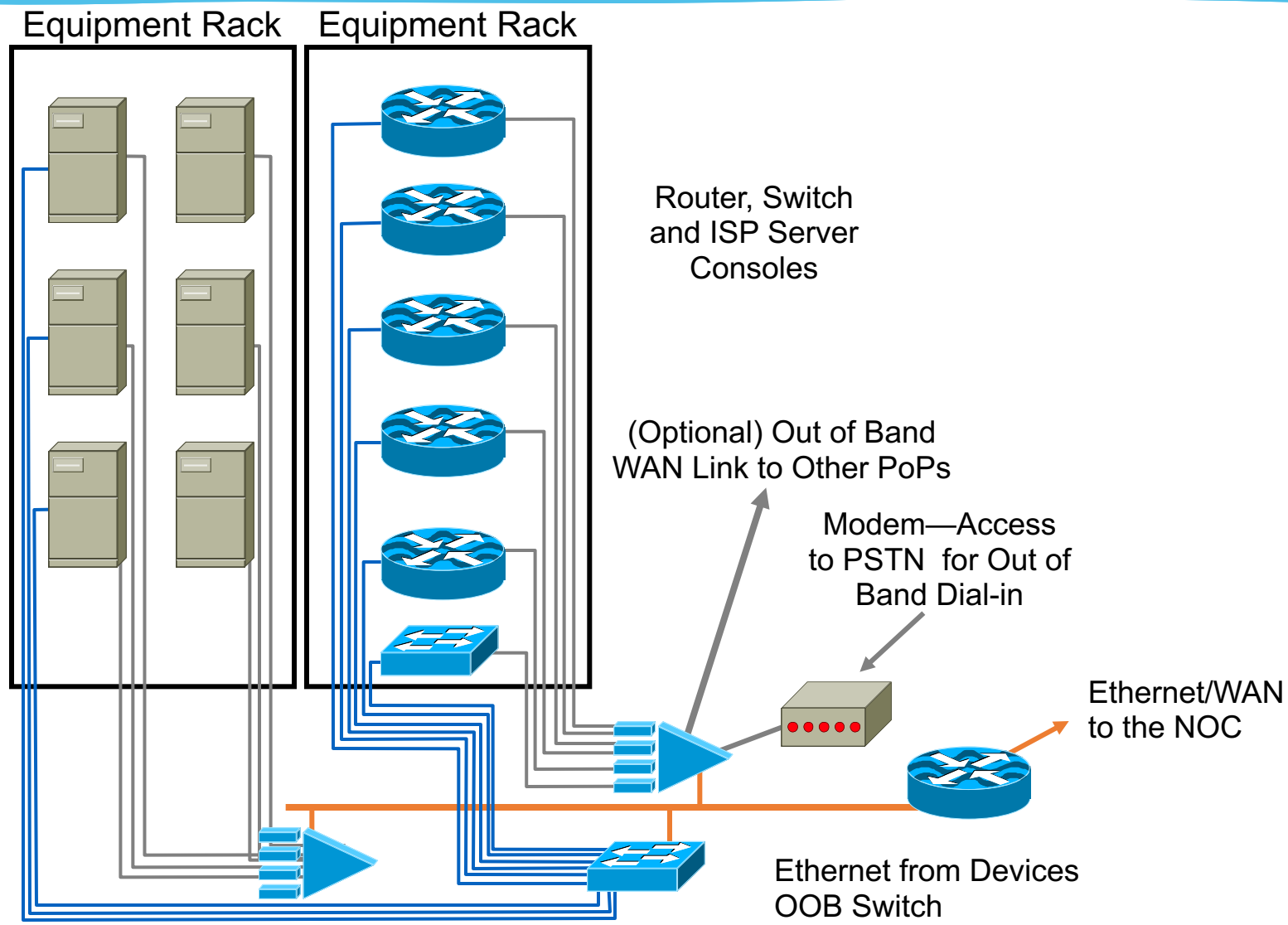
Traditional Reverse Telnet OOB



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



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.

HOMEWORK

- Do you have an Out of Band Network?
- If not, why not?

© 2003 Cisco Systems, Inc. All rights reserved.