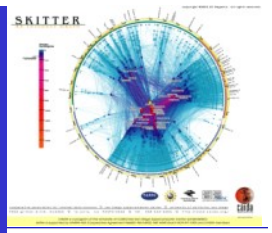
ISP and NSP Security Workshop

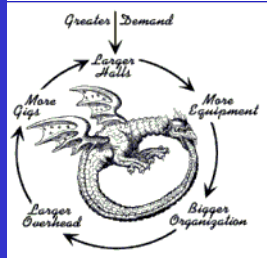
APRICOT 2013

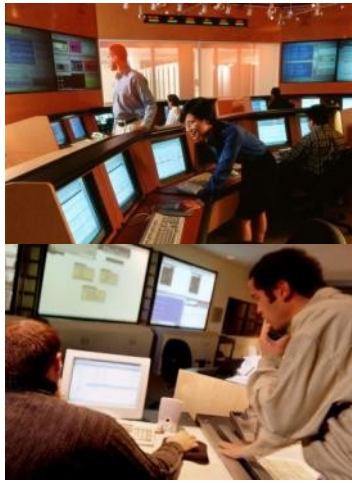
Day 1

Infrastructure Security

Infrastructure Security



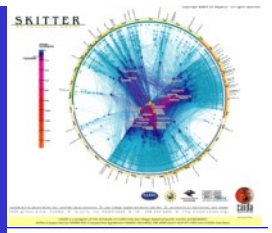


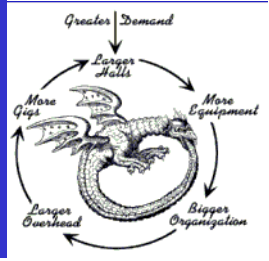


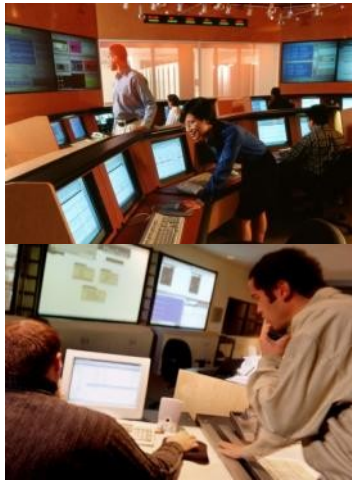
Infrastructure Security

- Best Common Practice [BCP]
  - Secure Router Access
  - Edge Protection
  - Remote triggered black hole filtering
  - Sink holes
  - Source address validation on all customer traffic
  - Control Plane Protection

Secure Router Access



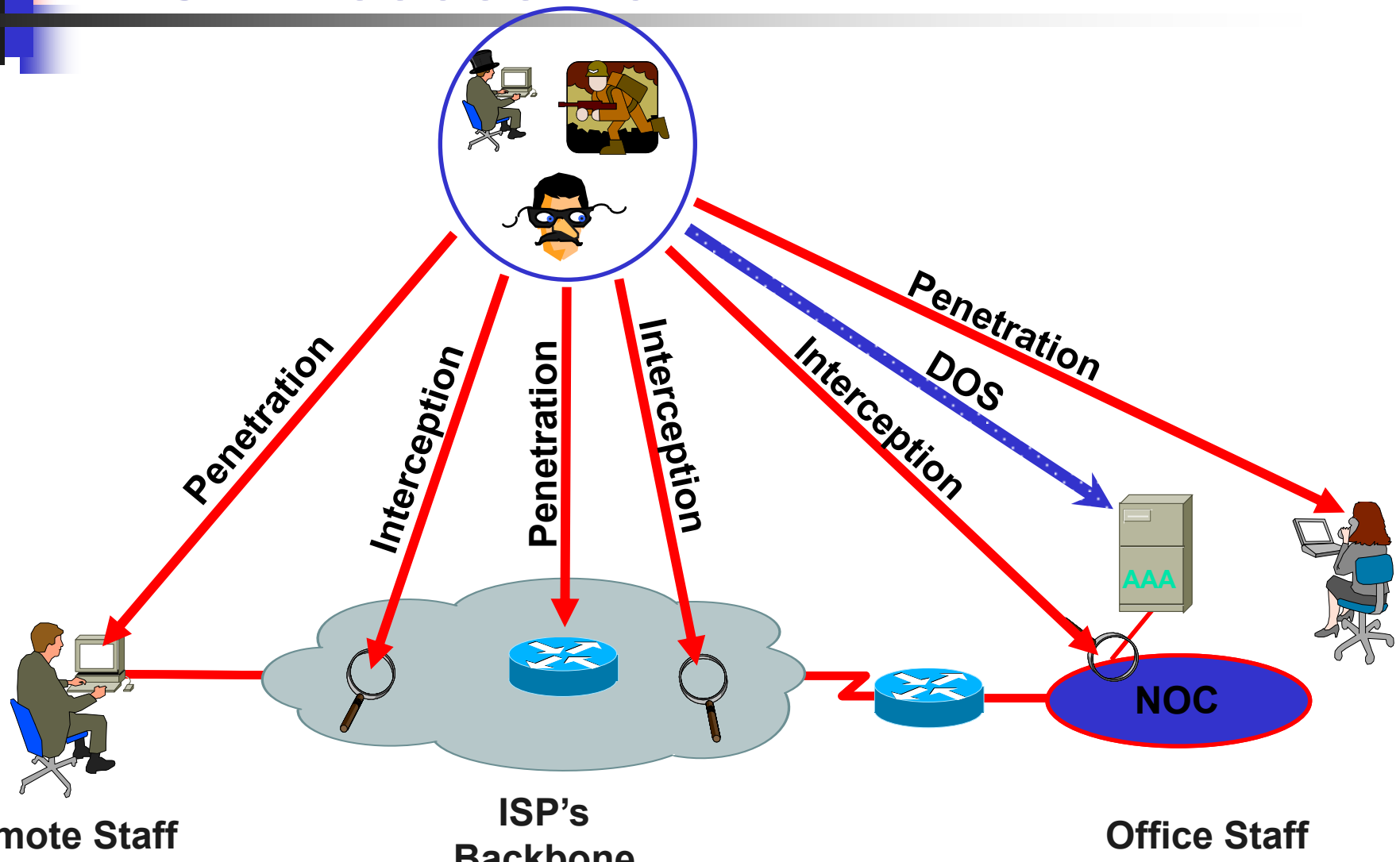




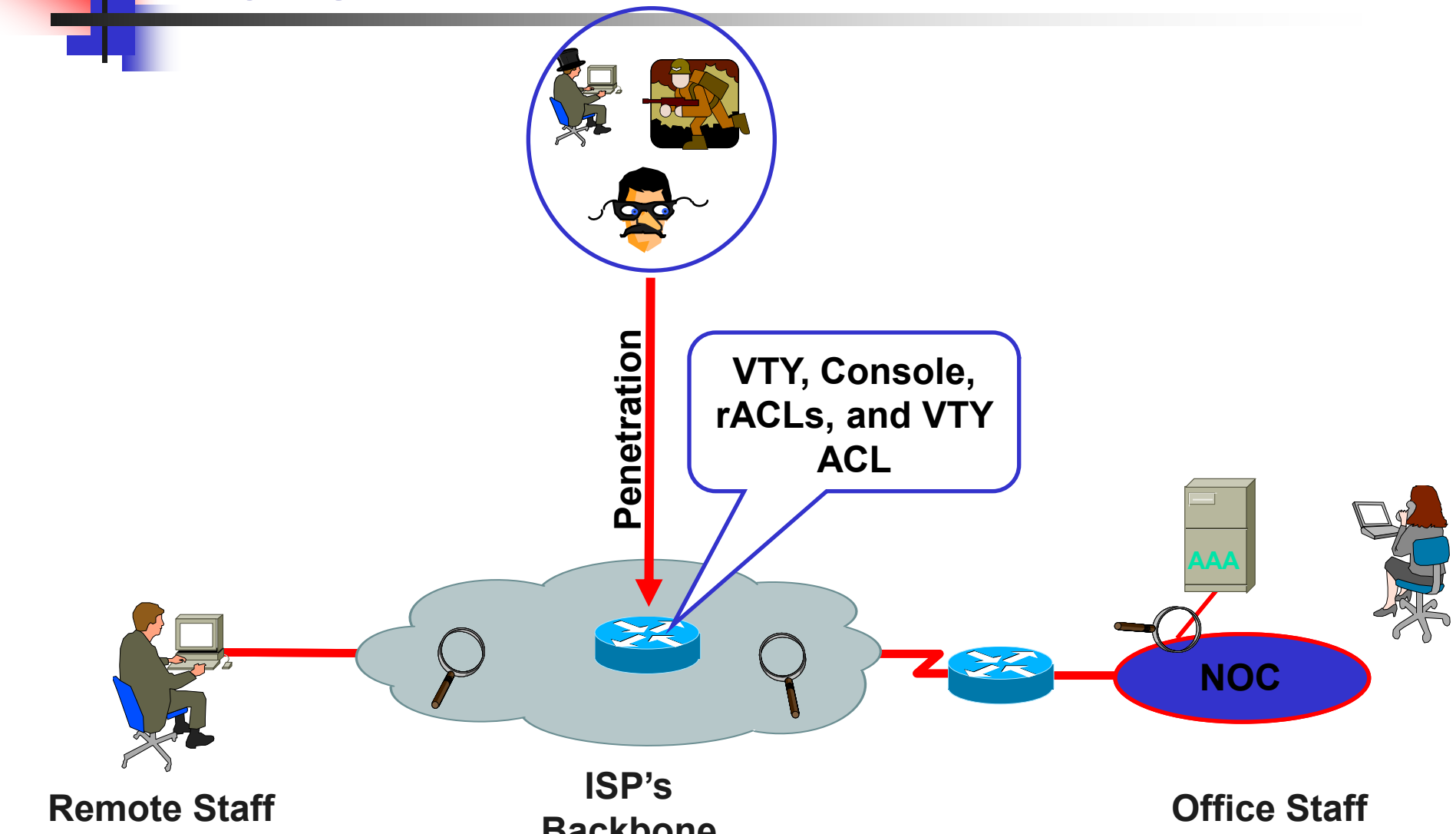
Check List

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

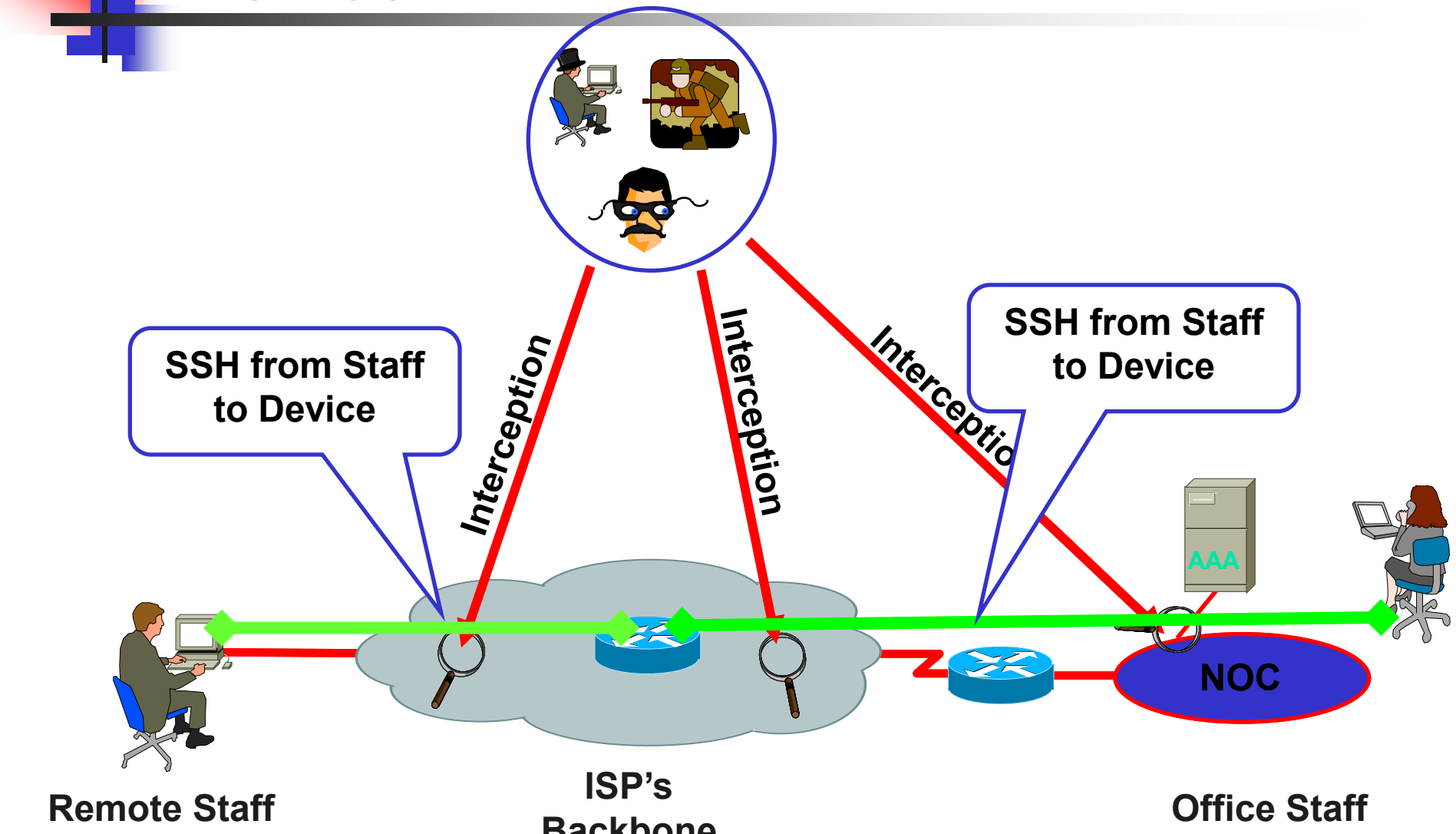
RISK Assessment



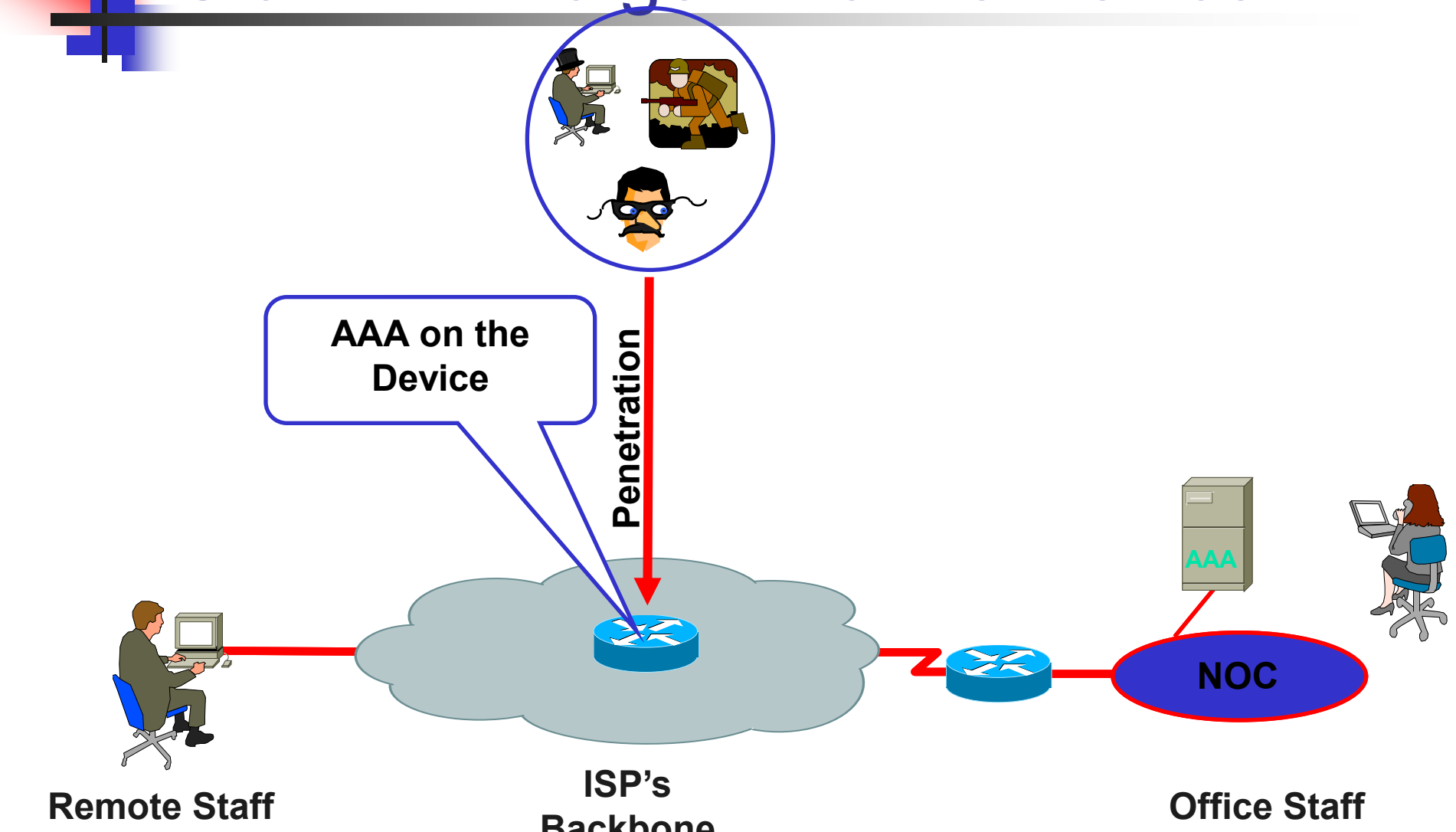
Lock Down the VTY and Console Ports



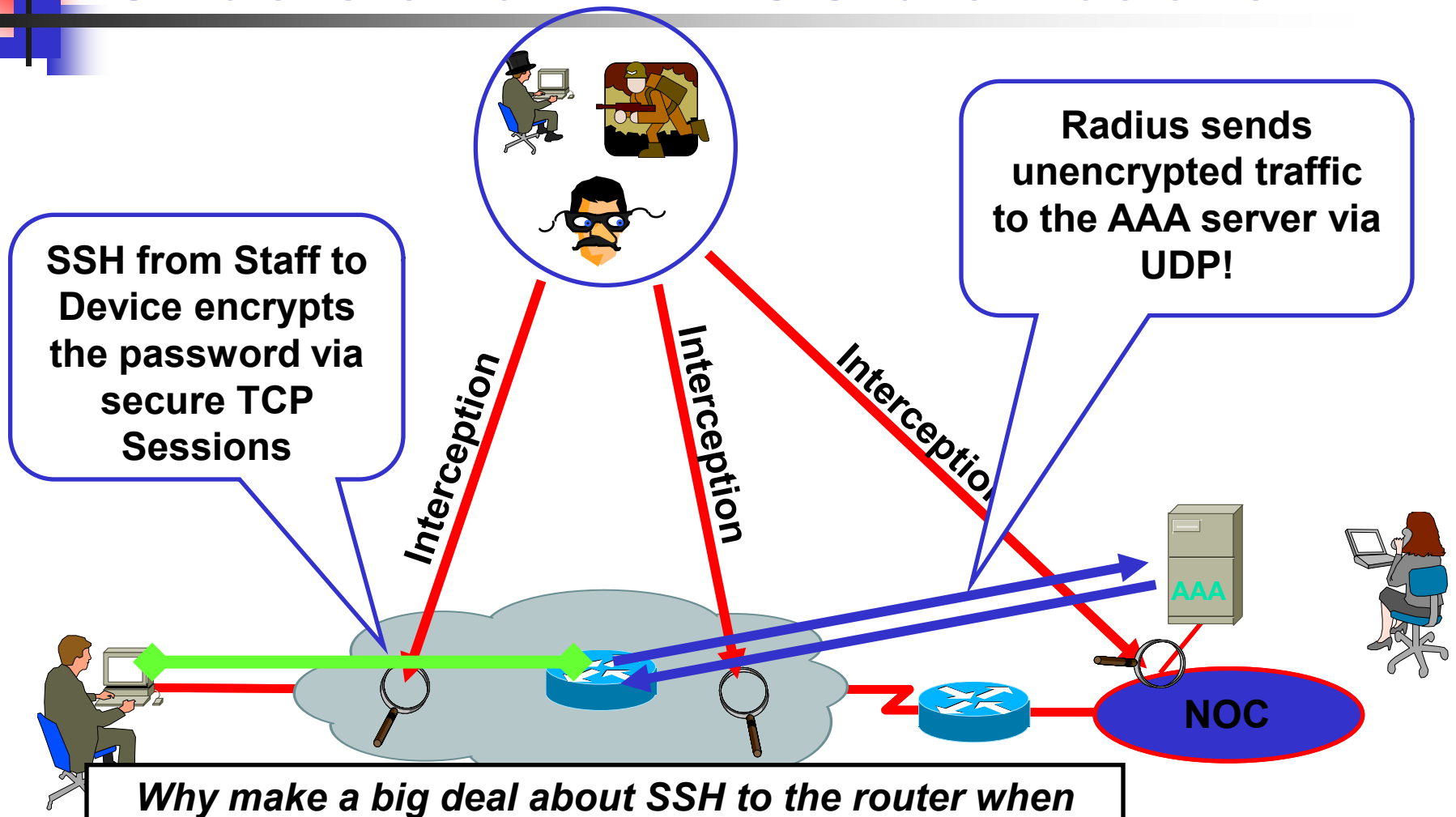
Encrypt the Traffic from Staff to Device



Staff AAA to get into the Device

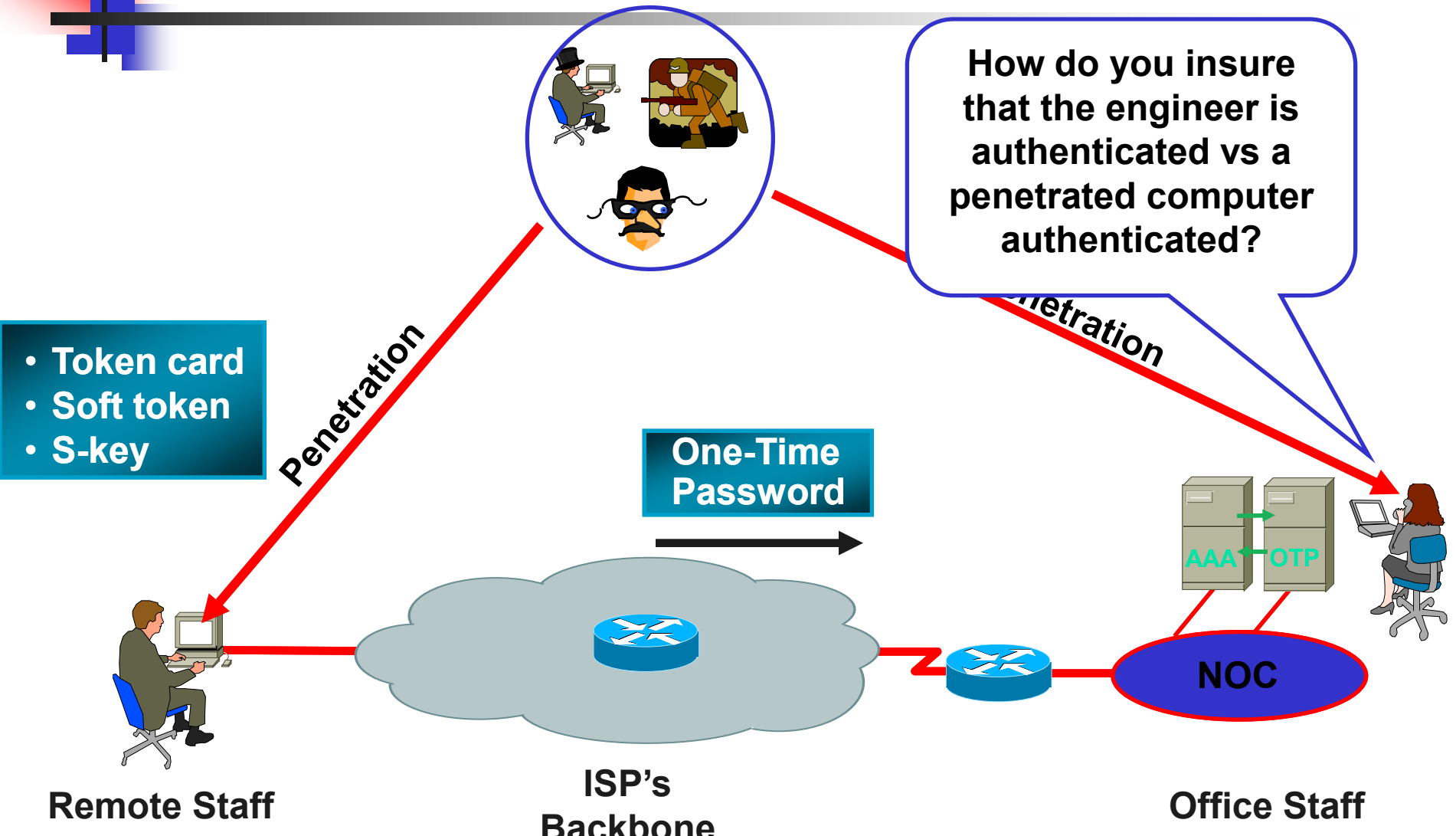


Understand RADIUS drawbacks

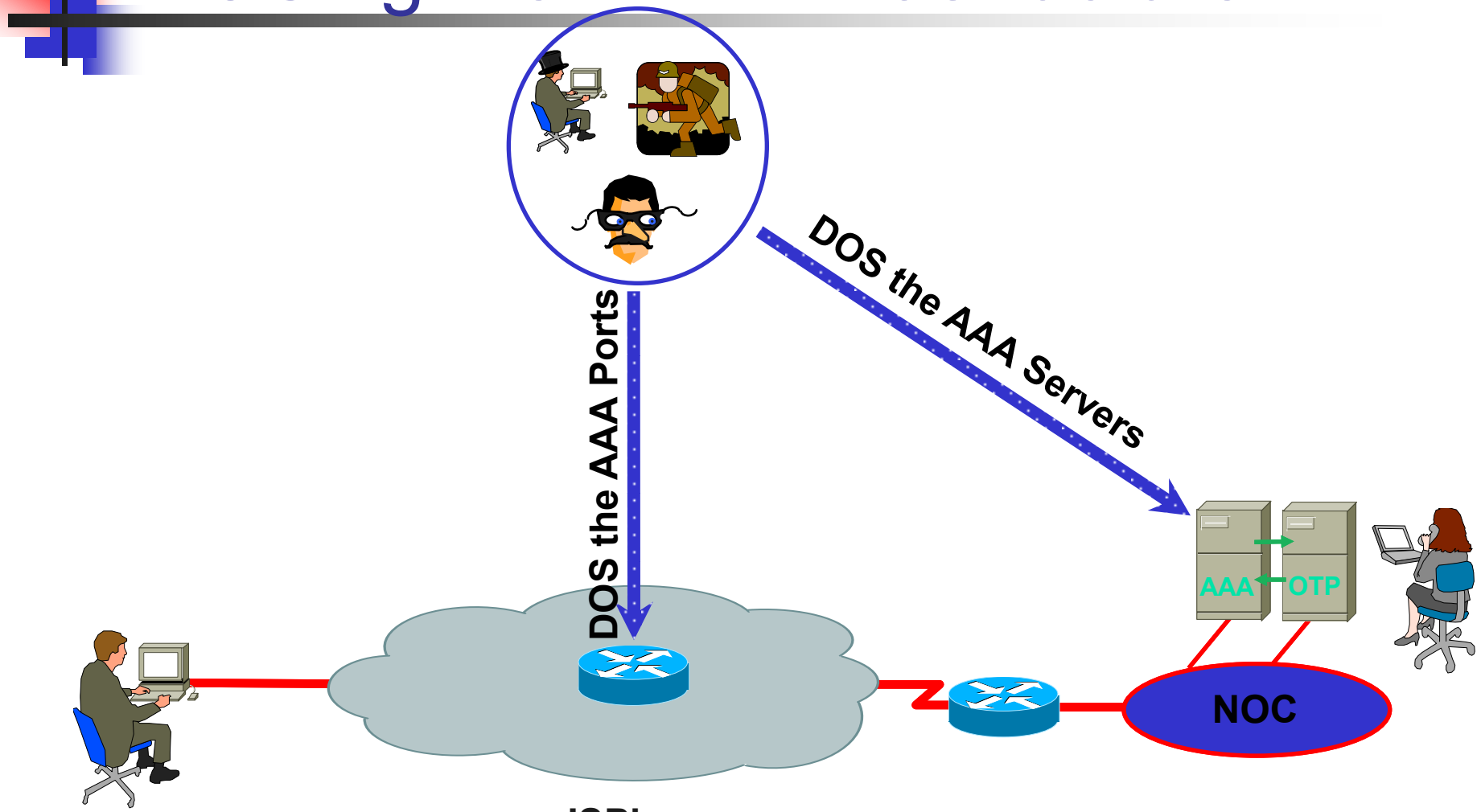


Why make a big deal about SSH to the router when Radius as a AAA solution introduces other risks? Are those risks manageable or appropriate?

One Time Password – ID Check

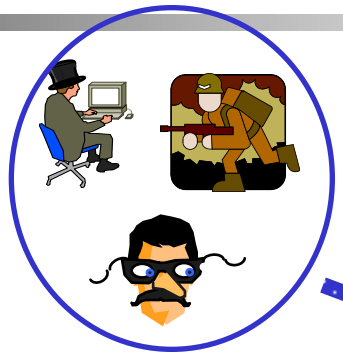


DOSing the AAA Infrastructure



Use a Firewall to Isolate the AAA Servers

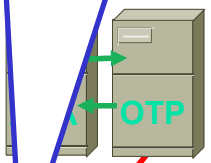
Statefull inspection is another reason to select TCP base AAA over UDP.



Separate AAA Firewall to protect from internal and external threats.

DOS the AAA Servers

DOS the AAA Ports



NOC

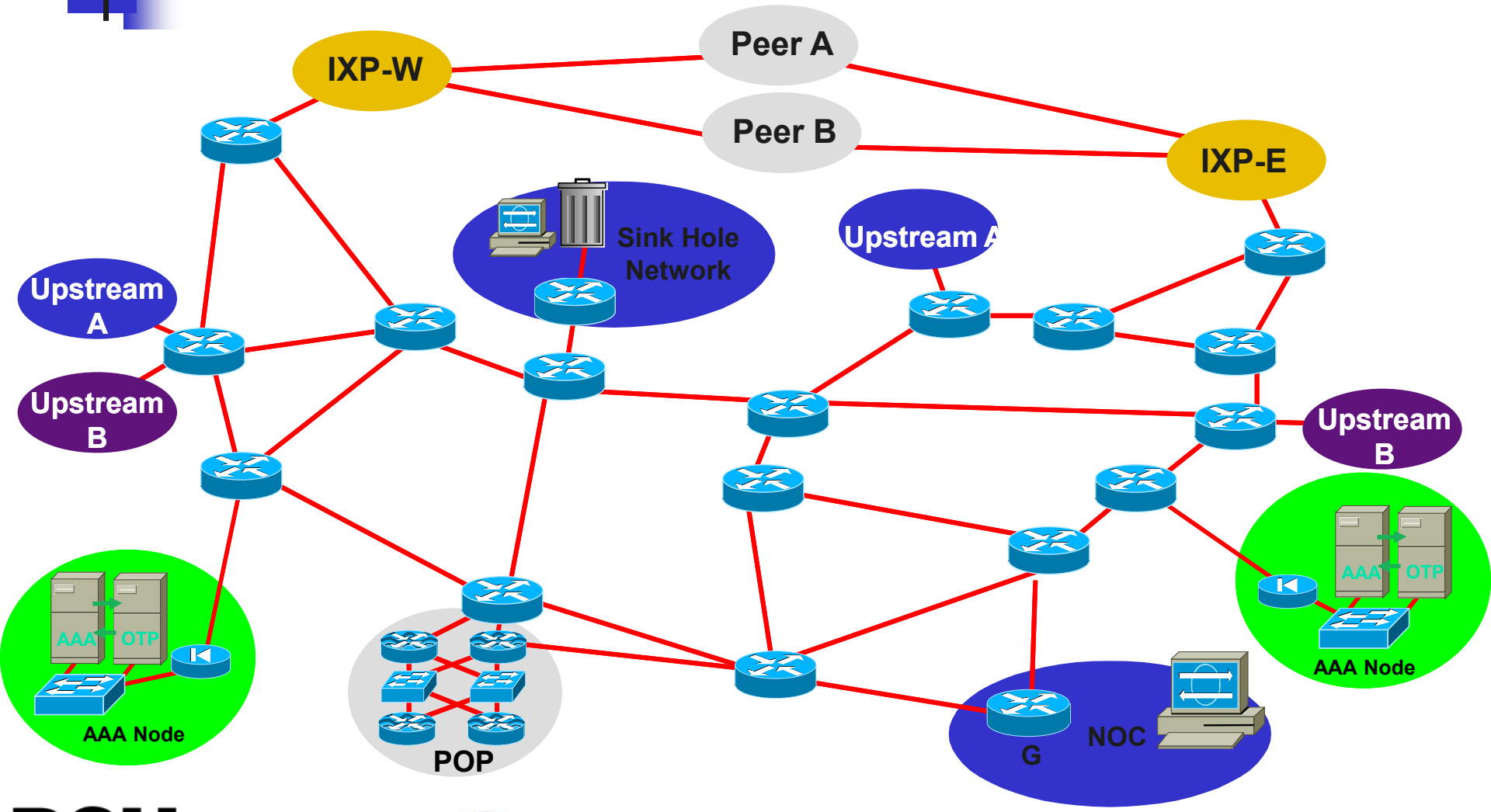
Remote Staff

ISP's Backbone

Office Staff

NOC Firewall

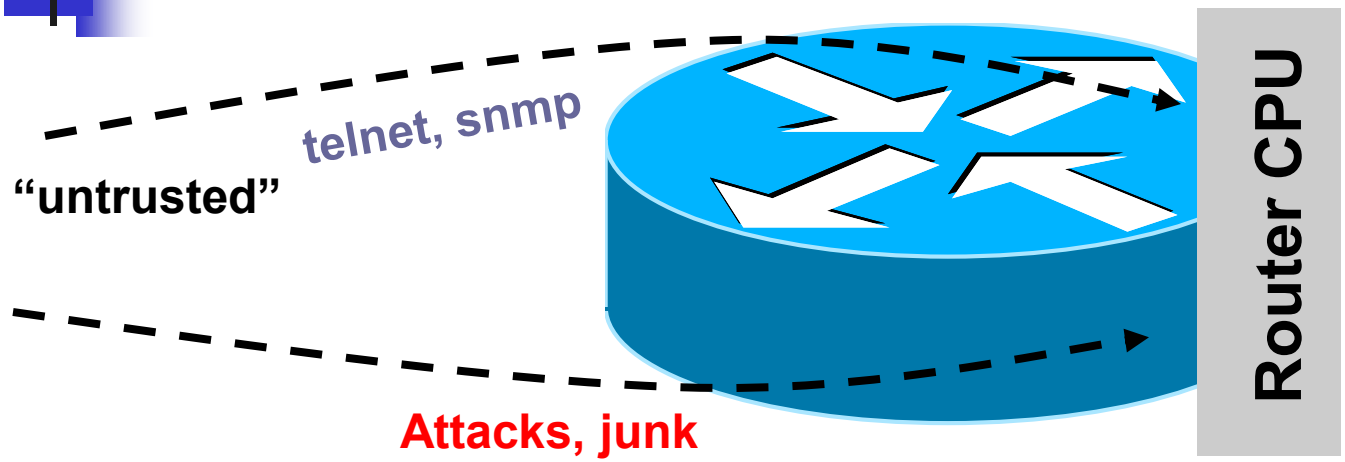
Distribute AAA Servers and Config Backup



TACACS+ URLs

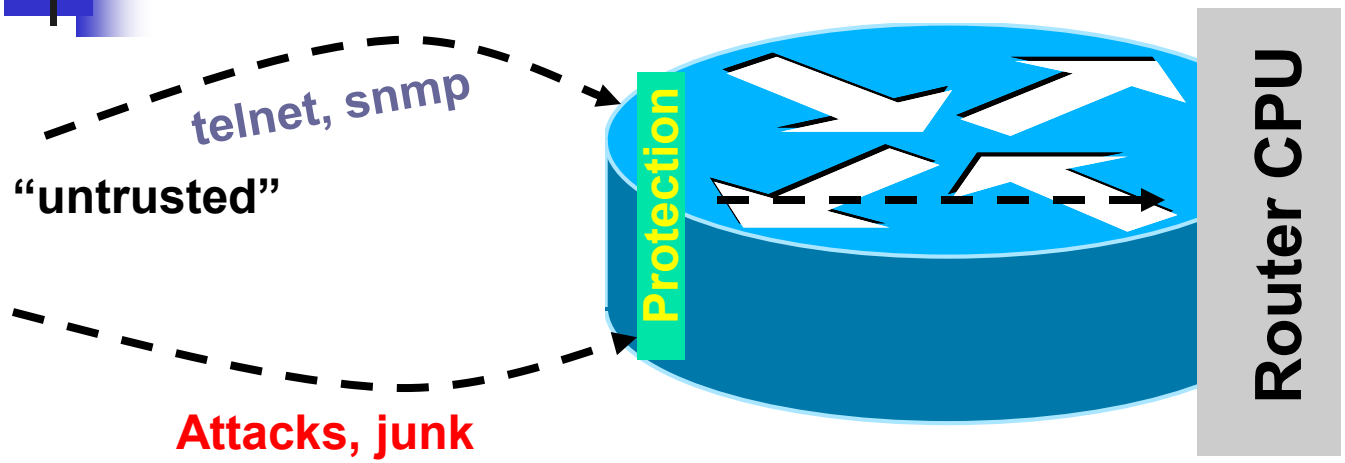
- TACACS+ Open Source
  - ftp://ftp-eng.cisco.com/pub/tacacs/
  - Includes the IETF Draft, Source, and Specs.
- Tac_plus
  - http://www.pro-bono-publico.de/projects/
- TACACS + mods
  - http://www.shrubbery.net/tac_plus/

The Old World: Router Perspective



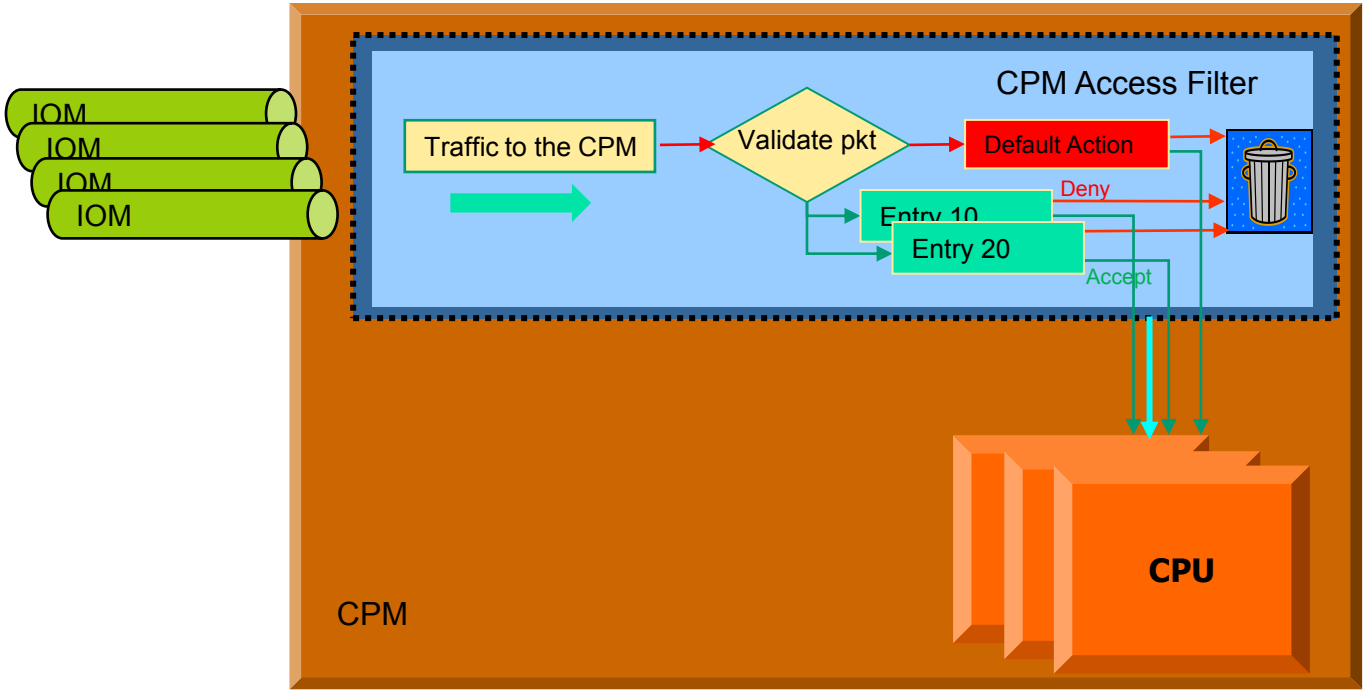
- Policy enforced at process level (VTY ACL, SNMP ACL, etc.)
- Some early features such as ingress ACL used when possible

The New World: Router Perspective

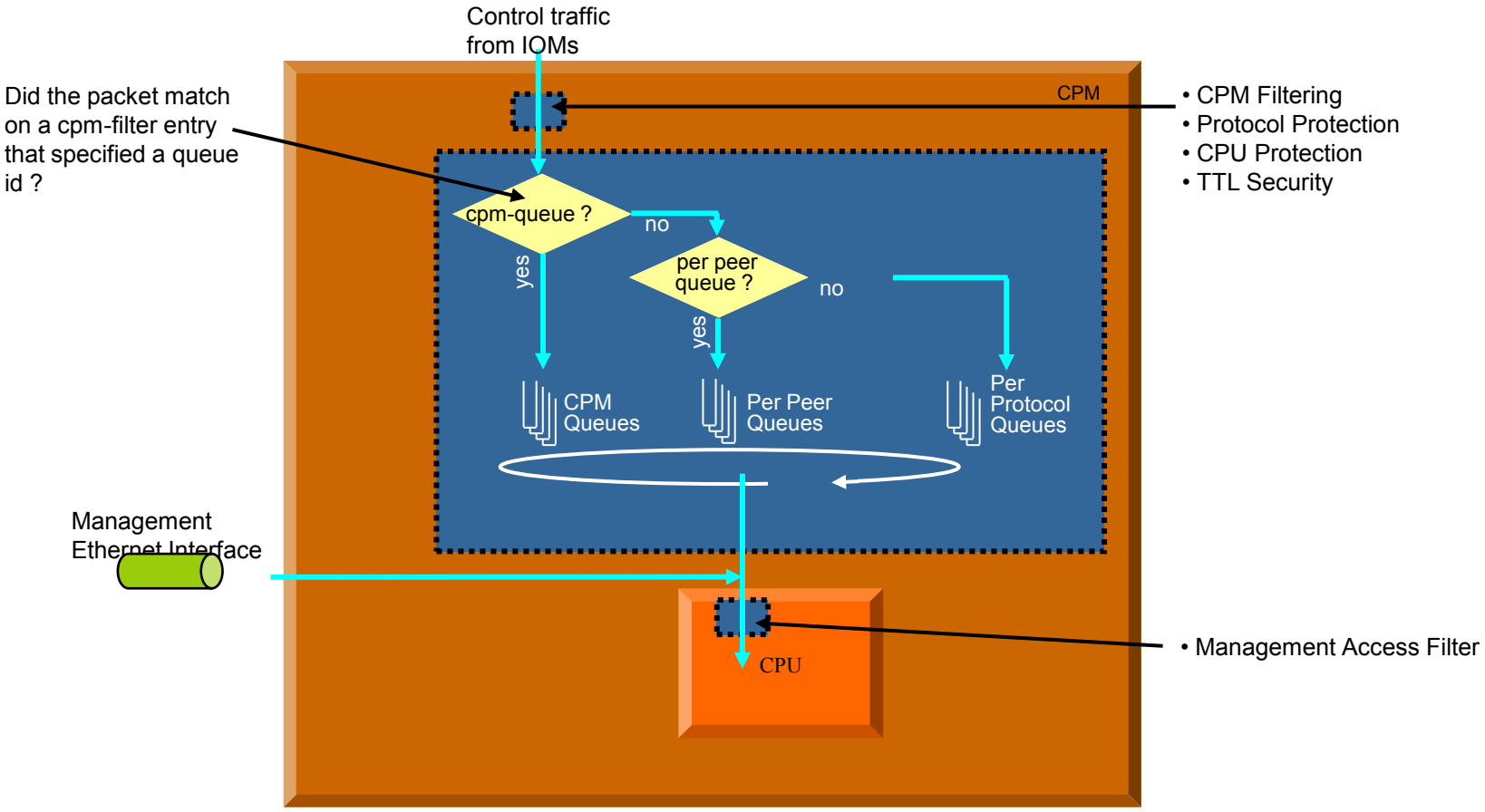


- Central policy enforcement, prior to process level
- Granular protection schemes
- On high-end platforms, hardware implementations

Hardware control plane protection



Hardware control plane protection



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.
- Of course you need to be monitoring your configs.

Config Monitoring

- **RANCID** - Really Awesome New Cisco config Differ (but works with lots of routers)

  http://www.shrubbery.net/rancid/
  http://www.nanog.org/meetings/nanog26/presentations/stephen.pdf

- 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.

Controlling access

Securing the box

- Identify what services to what networks
  - Classic prudent policy
  - Allow what you know
  - Then deny all!

Securing Physical Access

- No method of configuring a system can protect it if physical access is not secure
- Attackers with physical access can:
  - Physically harm and degrade the system
  - Perform password recovery and obtain access to the CLI
  - Attach a tap and packet sniffer to obtain traffic captures
  - Do other nefarious things limited only by their imagination…

Protect your systems from unauthorized physical access!

Securing Logical Access

- Logical access is more difficult to secure
  - Attackers do not require physical access to logically access the system
- Terminal servers can provide backdoor. For you or an attacker
  - Some extra logins/ features are available from console
- One of many ways to protect your systems from unauthorized logical access is to secure it with user names and passwords

Agenda: Configuring Administrator Authentication

- Why Secure CLI Access Is Needed
- ➔ Configuring Administrator Authentication
- Configuring Login Users and Classes
  - Creating Users
  - Creating Login Classes
  - Setting the Idle Timeout

Administrator Authentication

- By default, Juniper Networks routers have only a single user configured, called *root*
  - Juniper Networks routers do not have a default password configured for the root account.
- Alcatel-Lucent systems have a default account called *admin*
- Cisco has no console login password or enable password
- Systems with root accounts with no passwords do not last long on the Internet

Configure the administrator account with a difficult-to-guess password as the first step in securing the system!

Agenda: Configuring Login Users and Classes

- Why Secure CLI Access Is Needed
- Configuring Root Authentication
- ➔ Configuring Login Users and Classes
  - Creating Users
  - Creating Login Classes
  - Setting the Idle Timeout

IOS Role-Based CLI Views commands

- Enable AAA using the 'aaa new-model' global config command
  - aaa new-model
- Configure the AAA default list to use the router's local database for authentication and authorization
  - aaa authentication login default local
  - aaa authorization exec default local
- Configure AAA console authorization
  - aaa authorization console
- Access the root view. You need to first configure a secret or enable password before you can access the root view. configure a secret password = cisco)
  - Edge_C38#conf t
- Enter configuration commands, one per line. End with CNTL/Z.
  - Edge_C38(config)#enable secret cisco
  - Edge_C38(config)#^Z
  - Edge_C38#
  - Edge_C38#enable view
  - Password: secret_password

IOS Role-Based CLI Views commands

- Edge_C38#
- Create the Operator view
- Configure a password for this view
  - Ping
  - Show controllers
  - Show interfaces
  - Show version
- parser view operator
  - password 5 opspassword
  - commands exec include ping
  - commands exec include show version
  - commands exec include show controllers
  - commands exec include show interfaces

Setting the Idle Timeout

```
[edit system login class restricted-operator]
lab@R5# set idle-timeout 10
```

JUNOS

```
R5(config)#   line  vty o 4

R5(config)#   exec timeout 0 10
```

IOS

- No idle-timeout by default
  - Set the time, in minutes, after which an idle user is automatically disconnected
  - User session is sent warning messages 5 minutes, 1 minute, 10 seconds, and on session shutdown

Is Any Remote Access Secure?

- No remote access to the router is completely secure
  - The issue:
    - Nothing is ever completely secure
    - We need remote access to the router
    - We must minimize the risk
  - The defaults:
    - CLI access is available only on the console port
    - No access is available on the auxiliary port without configuration
    - No other method of remote access is available without configuration

Remote Access Methods

- Remote access methods available on most platforms:
  - Remote access to the CLI
    - Telnet (Client and server)
    - SSH (Client and server)
    - Rlogin (Server, client available in the shell, JUNOS)
  - Remote access to the file system, (JUNOS)
    - FTP (client and server)
    - SCP (client and server)
  - Other remote access
    - Finger (server, client available in the shell)
    - SNMP

Telnet and FTP Servers

- Telnet and FTP
  - Provide convenient access to the CLI and file system
  - Both the Telnet and FTP Servers are disabled by default
  - Everything transmitted (including the password) is sent in cleartext on the wire
  - Custom packet sniffers are available to search for and reassemble the passwords in a both Telnet and FTP sessions
  - The root user can never log in with Telnet or FTP
  - Both protocols provide only availability
    - Confidentiality and integrity are not protected

Enabling the Telnet Server

- The following command enables Telnet access
  - Disabled by default

  JUNOS
- [edit system]
- lab@R1# set services telnet

- [edit system]
- lab@R1# show
- services {
- telnet;
- }

IOS

```
R1(config)# line vty 0 4
R1(config)# login
R1(config)# password
  Uj%$3
```

Additional Telnet Options

- Options:
  - The connection limit establishes the maximum number of concurrent sessions (JUNOS default = 75) (IOS default = 5)
  - The rate limit establishes the maximum number of connections allowed per minute (JUNOS default = 150)

SSH Clients

- Many SSH implementations are available
  - Putty
  - TeraTerm
  - OpenSSH
  - Many commercial servers and clients

Enabling SSH - IOS

```
cry key generate rsa

ip ssh time-out 60
ip ssh authentication-retries 2


!--- Step 4: By default the vtys' transport is Telnet. In this
   case,
!--- Telnet is disabled and only SSH is supported.


line vty 0 4
transport input SSH
```