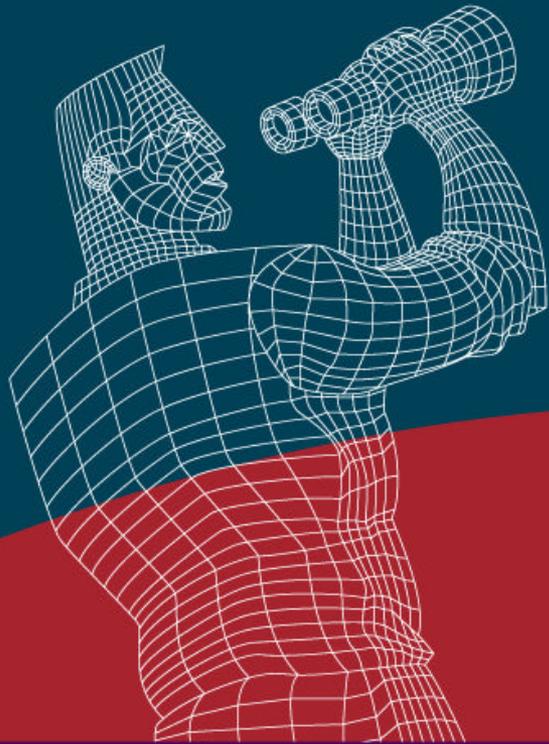
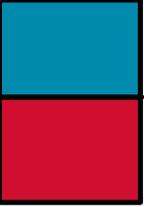


Networkers

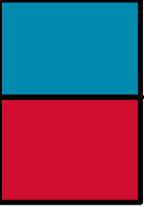


Designing Secure Enterprise Network Infrastructures



Infrastructure Security

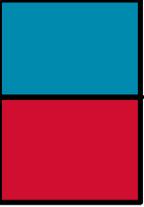




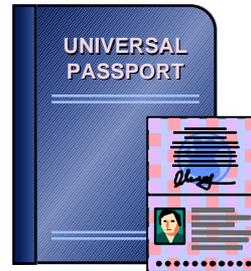
Smooth Sailing

- **Maintain a written Policy**

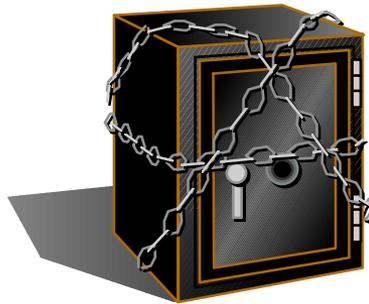




Elements of a Security Policy



- Identity



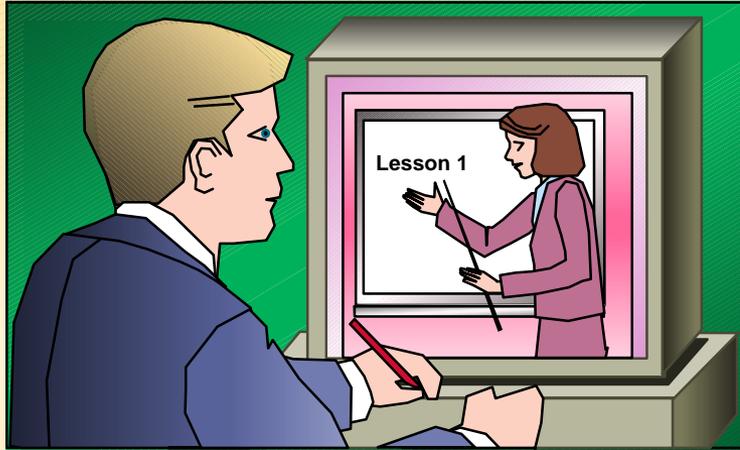
- Integrity



- Audit

Procedures and Operations

Training



Rules

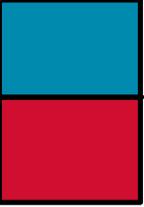


Periodic Review



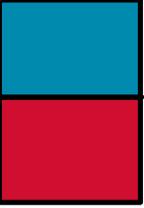
Delegation of Authority





Goals of the Session

- **Define what to protect**—anything that could cause problems if it were to stop or malfunction
- **Decide how to protect it**—good enough vs. absolute protection
- **Think about cost of protection vs. cost of loss or corruption**



Agenda

I. Introduction

II. Router/Switch Self-Protection

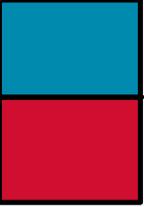
III. Resource Protection

IV. Perimeter Protection

V. Network Security Sustainment

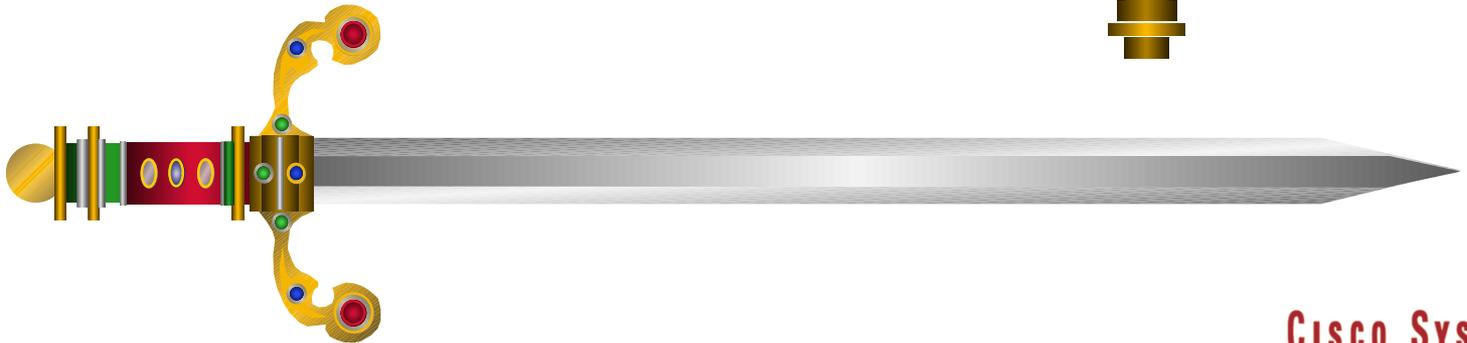
VI. Security Sustainment Validation

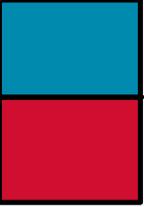
VII. Conclusions



II. Router/Switch Self-Protection

- Threats
- Avoidance Measures





Intruder Attack Points

- **The administrative interfaces**

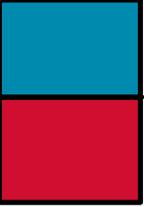
Console

Telnet

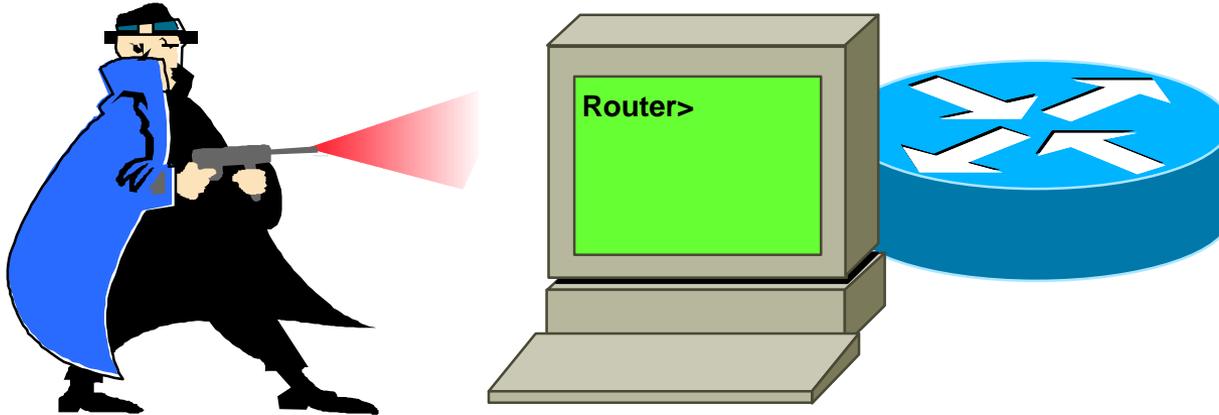
SNMP

- **Overload the data interface**
- **Overload the processor**

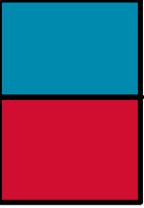




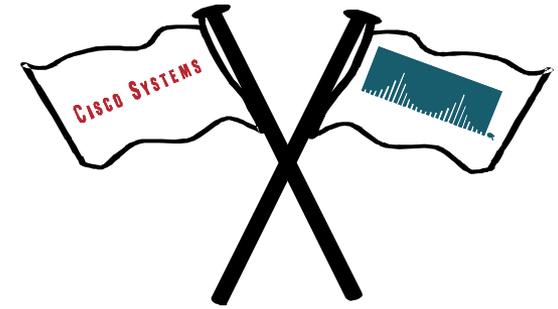
The Administrative Interface



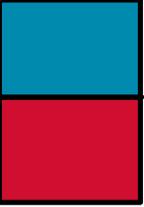
- Password Protection
- Password Encryption



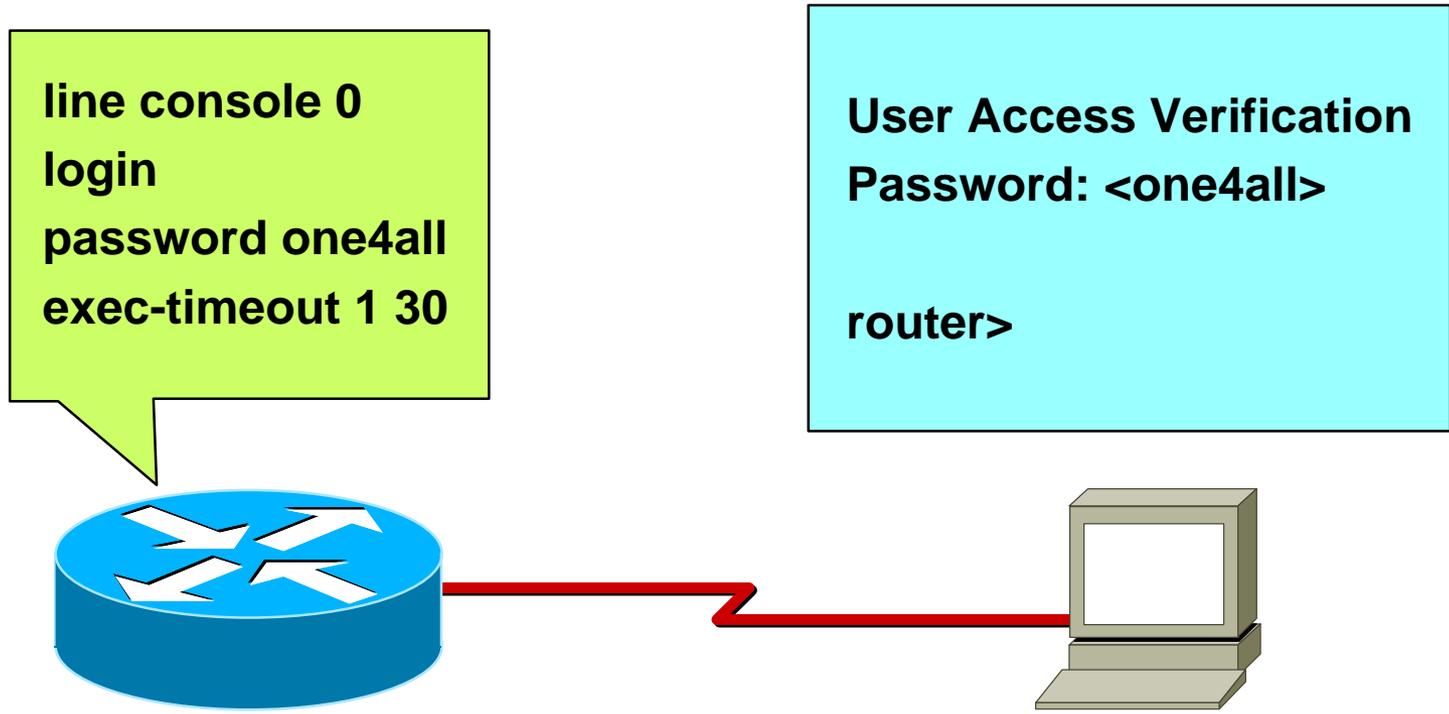
Banners



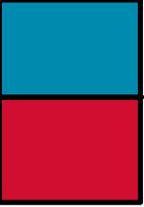
- **Select an appropriate login banner that tells who is allowed into the system**



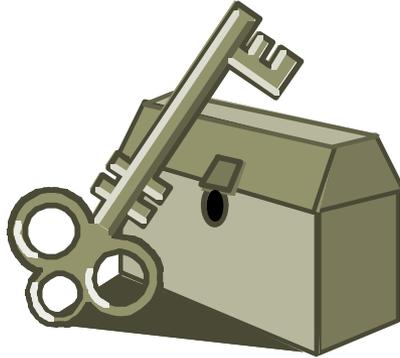
Native Passwords



The native passwords can be viewed by anyone logging in with the enabled password



Service Password-Encryption (7)

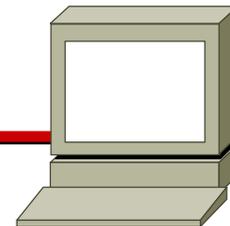
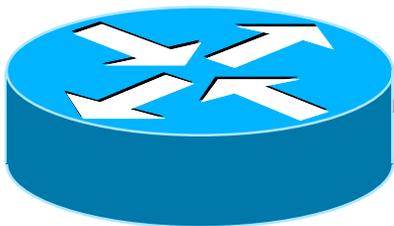


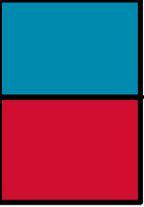
- Will encrypt all passwords on the Cisco IOS™ with Cisco-defined encryption type “7”
- Use “enable password 7 <password>” for cut/paste operations
- Cisco proprietary encryption method

Service Password-Encryption

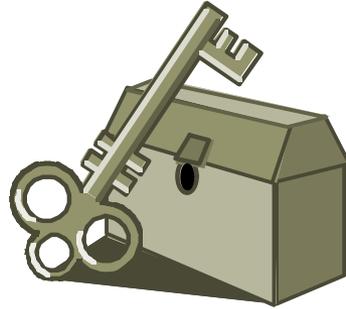
```
hostname Router
!  
enable password one4all  
!
```

```
service password-encryption  
!  
hostname Router  
!  
enable password 7 15181E00F
```





Enable Secret (5)

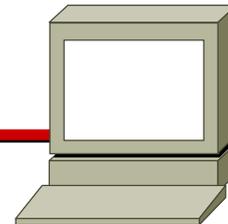
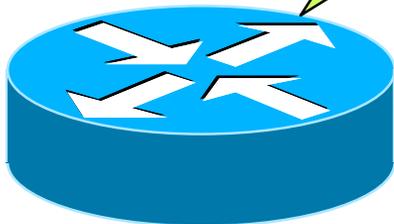


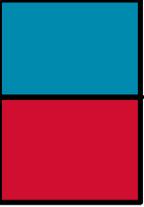
- **Uses MD5 to produce a one-way hash**
- **Cannot be decrypted**
- **Use “enable secret 5 <password>” to cut/paste another “enable secret” password**

Enable Secret (5)

```
hostname Router  
!  
enable password 1forAll
```

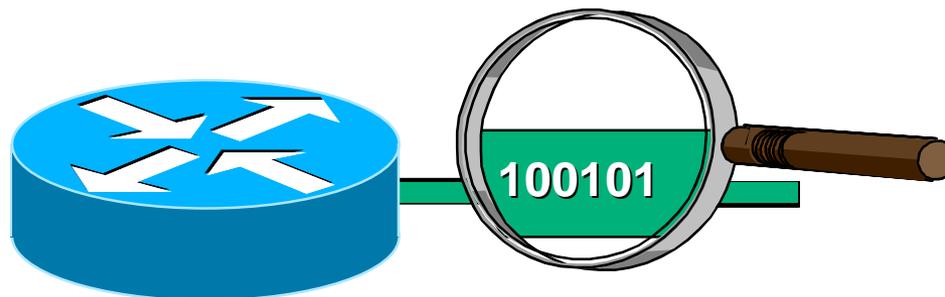
```
!  
hostname Router  
!  
enable secret 5 $1$hM3I$.s/DgJ4TeKdDkTVCJpIBw1
```





Password of Caution

- Even passwords that are encrypted in the configuration are not encrypted on the wire as an administrator logs into the router

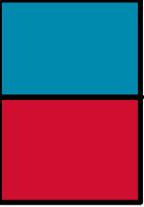


Use Good Passwords



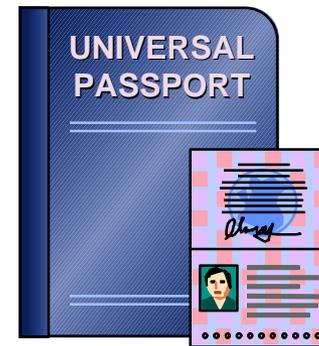
**hmm..., How about
“Pancho”?**

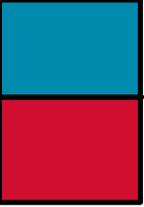
- **Do not use passwords that can be easily guessed**



Authentication Mechanisms

- **Local Password**
- **Kerberos**
- **TACACS+**
- **RADIUS**
- **One-time Passwords**





Cisco IOS TACACS+ Authentication

```
version 11.2
!  
service password-encryption  
!  
hostname Router  
!  
aaa new-model  
aaa authentication login billy tacacs+ enable  
aaa authentication login bobby tacacs+ local  
enable secret 5 $1$hM3l$.s/DgJ4TeKdDk...  
!  
username bill password 7 030E4E050D5C  
!
```

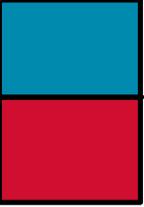
Encrypts passwords with encryption (7).

Define list “billy” to use TACACS+ then the enable password

Define list “bobby” to use TACACS+ then the local user and password

“enable secret” overrides the (7) encryption

Define a local user and password for “bill”



Cisco IOS TACACS+ Authentication

```
tacacs-server host 10.1.1.2
tacacs-server key <key>
!
line con 0
 login authentication billy
line aux 0
 login authentication billy
line vty 0 4
 login authentication bobby
 length 29
 width 92
!
end
```

Defines the IP address of the TACACS+ server

Defines the “encryption” key for communicating with the TACACS+ server

Uses the authentication mechanisms listed in “billy” —TACACS+ then enable password

Uses the authentication mechanisms listed in “bobby” —TACACS+ then a local user/password

PIX TACACS+ Authentication

PIX Version 4.0.7

enable password BjeuCKspwqCc94Ss encrypted

passwd nU3DFZzS7jF1jYc5 encrypted

tacacs-server host 10.1.1.2 <key>

aaa authentication telnet outbound 0.0.0.0 0.0.0.0 tacacs+

aaa authentication ftp outbound 0.0.0.0 0.0.0.0 tacacs+

aaa authentication http outbound 0.0.0.0 0.0.0.0 tacacs+

no snmp-server location

no snmp-server contact

telnet 10.1.1.2 255.255.255.255

mtu outside 1500

mtu inside 1500

: end

[OK]

Telnet Password

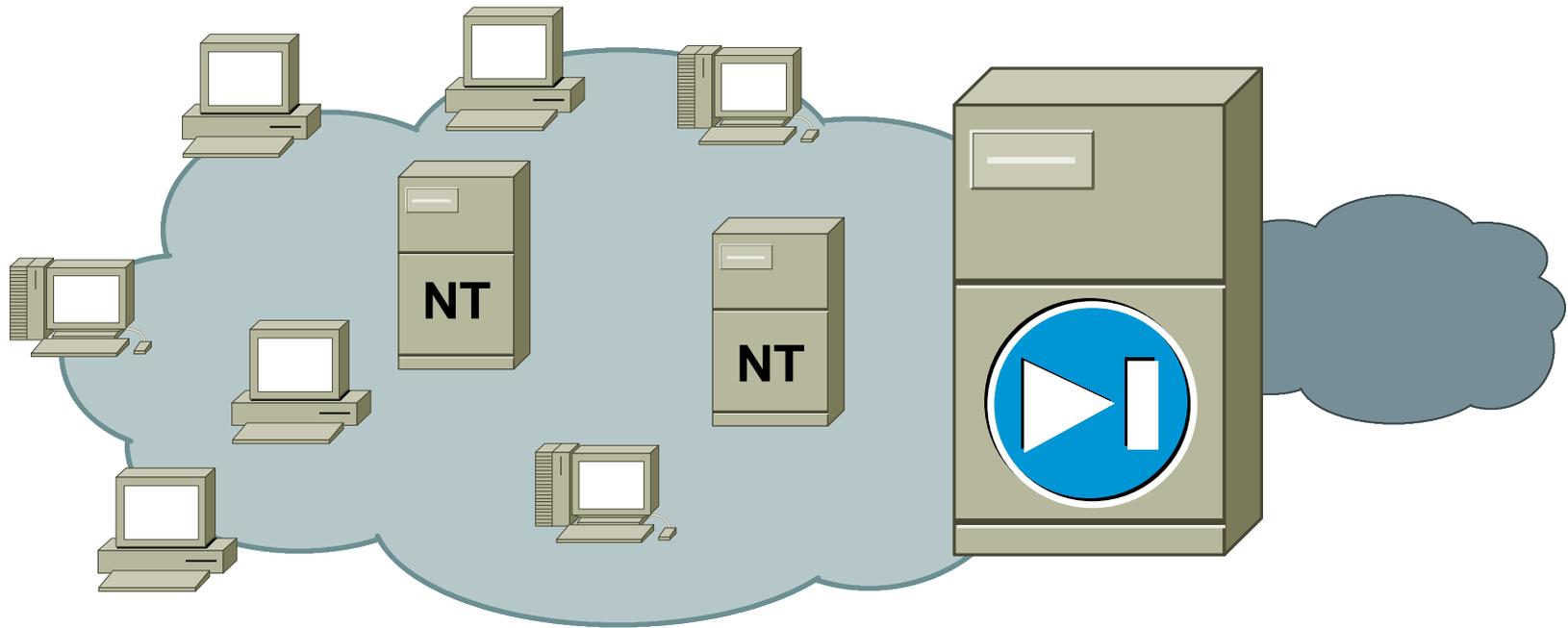
Enable Password

Defines the IP address of the TACACS+ server and the key

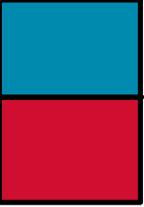
Defines the services that require authentication

Defines the device that can Telnet into the PIX

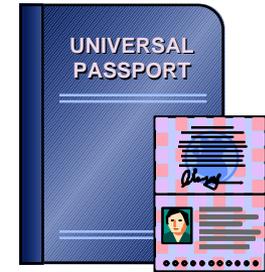
Centri Authentication



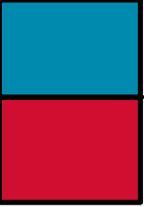
- **Security policies are associated with Windows NT users**



Enable Authentication

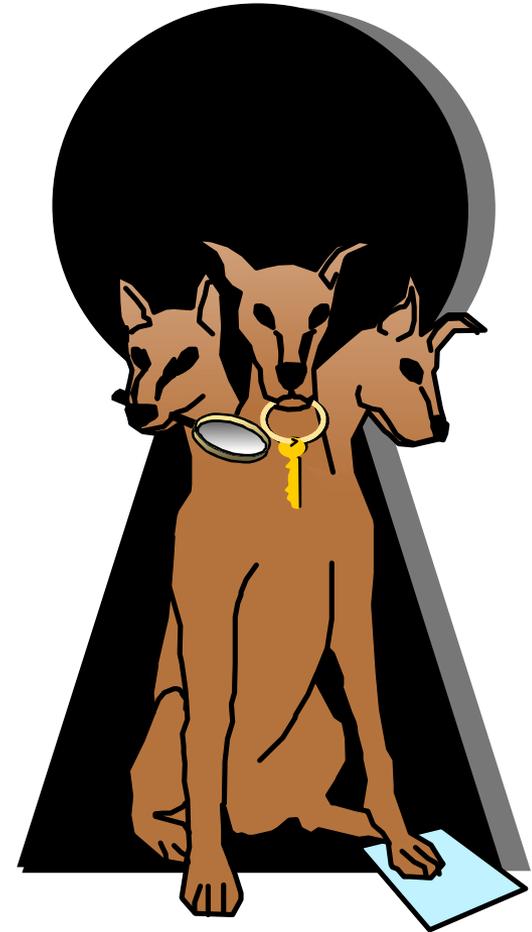


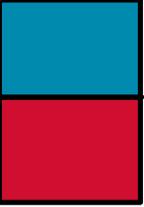
- **Cisco IOS—Can use the same authentication mechanisms for “enable” as the “login” starting in Cisco IOS 11.3**
- **PIX—Will start using additional authentication mechanisms for the Console and “enable”**



Encrypted Telnet Sessions

- **Kerberos v5**
- **Strong Authentication within the session**
- **Relies heavily upon DNS and NTP**



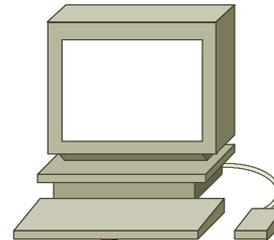
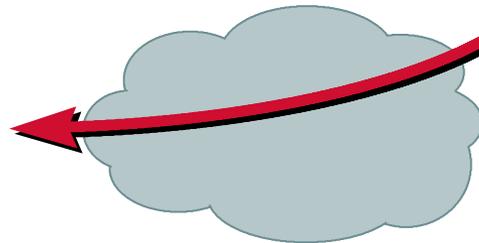


One-Time Passwords

- **May be used with TACACS+ or RADIUS**
- **The same “password” will never be reused by an authorized administrator**
- **Key Cards—CryptoCard token server included with CiscoSecure**
- **Support for Security Dynamics and Secure Computing token servers in Cisco Secure**

Restrict Telnet Access

```
access-list 12 permit 172.17.55.0 0.0.0.255  
line vty 0 4  
access-class 12 in
```

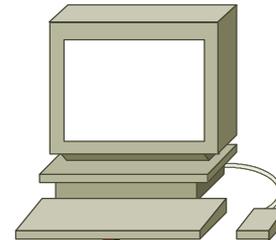
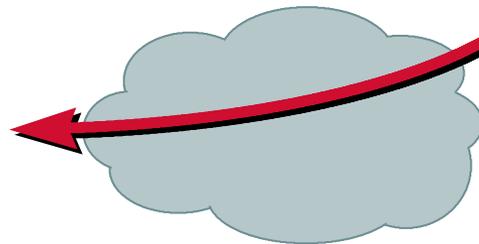


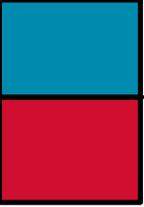
SNMP Access Control

RO—Read Only

RW—Read + Write

```
access-list 13 permit 192.85.55.12
access-list 13 permit 192.85.55.19
snmp-server community public RO 13
```



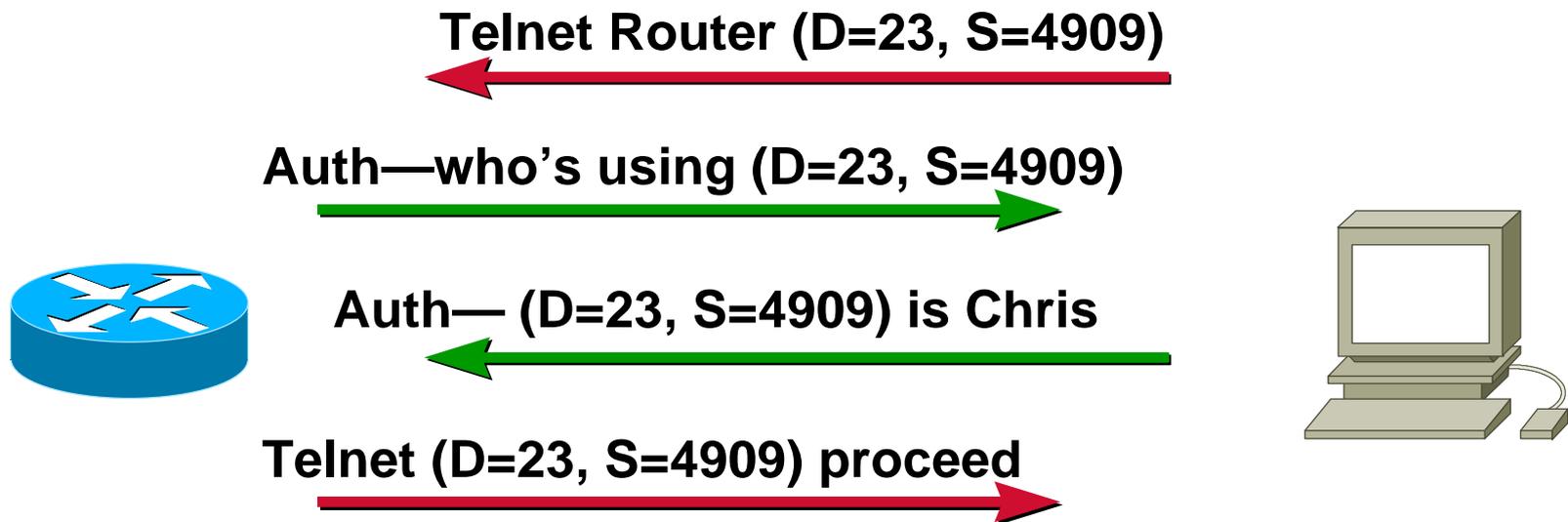


SNMP

- **Version one sends cleartext communitystrings and has no policy reference**
- **Version two addresses some of the known security weaknesses of SNMP version one**
- **Version three is being worked on**

Identification Protocol

- The Identification Protocol (Auth) can be enabled for sessions to the router



RFC 1413: Identification Protocol

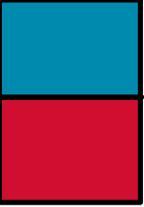
“The information returned by this protocol is at most as trustworthy as the host providing it...”

Resource Deprivation Attacks

```
version 11.2
!  
no service udp-small-servers  
no service tcp-small-servers  
!
```



- **Echo (7)**
- **Daytime (13)**
- **Discard (9)**
- **Chargen (19)**



Resource Deprivation Attacks

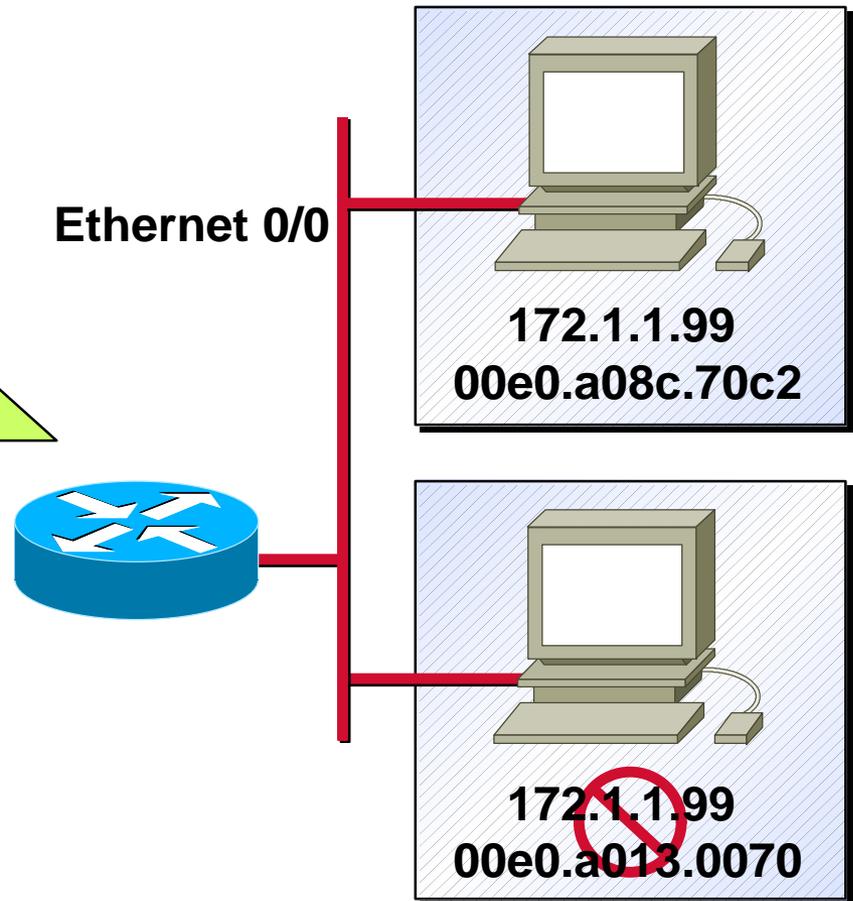
```
version 11.2  
!  
no service finger  
no service udp-small-servers  
no service tcp-small-servers  
!
```

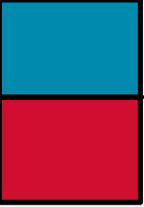


- **Finger (79)**

ARP Control

```
!  
arp 172.1.1.99 00e0.a08c.70c2 arpa  
!  
interface ethernet 0/0  
ip address 172.1.1.100 255.255.0.0  
!
```





Administrator Authorization Levels



- **Sixteen administrative levels that can be used to delegate authority**
- **Cisco IOS commands can be associated with a level**

```
privilege exec level 9 show
enable secret level 9 <AllinOne>
enable secret 5 <OneinAll>
```

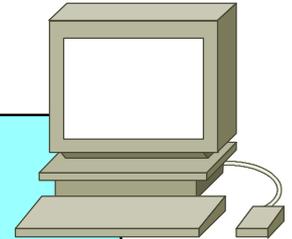
```
Router# show priv
Current privilege level is 15
Router# disable
Router>enable 9
Password:
Router# show priv
Current privilege level is 9
Router#
```

Audit Trail—Cisco IOS Syslog

```
unix% tail cisco.log
Feb 17 21:48:26 [10.1.1.101.9.132] 31: *Mar  2 11:51:55 CST:
  %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.1.2)
unix% date
Tue Feb 17 21:49:53 CST 1998
unix%
```

```
version 11.2
service timestamps log datetime localtime show-timezone
!
logging 10.1.1.2
```

```
Router>sho clock
*11:53:44.764 CST Tue Mar 2 1993
Router>
```



Audit Trail—PIX Syslog

```
unix% tail pix.log
```

```
Feb 20 07:46:25 [10.1.1.1.2.2] Begin configuration: reading from terminal  
Feb 20 07:46:29 [10.1.1.1.2.2] 111005 End configuration: OK  
Feb 20 07:46:32 [10.1.1.1.2.2] 111001 Begin configuration: writing to memory  
Feb 20 07:46:32 [10.1.1.1.2.2] 111004 End configuration: OK
```

```
unix%
```

```
PIX Version 4.0.7
```

```
enable password zS7kFj3ZL2VDF3uN encrypted
```

```
passwd zS7kFj3ZL2VDF3uN encrypted
```

```
hostname mypix
```

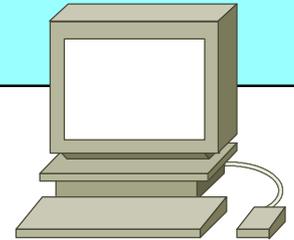
```
no failover
```

```
names
```

```
syslog output 20.6
```

```
no syslog console
```

```
syslog host 10.1.1.2
```



Bookmarks Location:

Home

Logout

Help

Tasks

Tools

Admin

- 24 Hour Reports
- Availability
- Inventory
- Software Management
- Syslog Analysis
 - Severity Level Summary**
 - Standard Reports
 - Custom Reports
 - Custom Report Summary

Select Dates



Select dates to include in the severity level summary.

Dates

- Today
- All
- Feb 16 (Monday)
- Feb 15 (Sunday)
- Feb 14 (Saturday)
- Feb 13 (Friday)
- Feb 12 (Thursday)
- Feb 11 (Wednesday)

Back

Finish

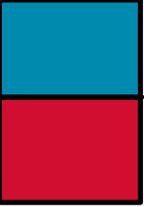
Help

**Use a tool to analyze
your logs and
generate reports**

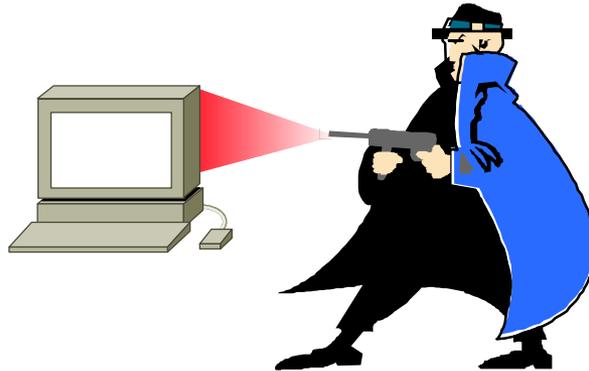


100%





III. Resource Protection

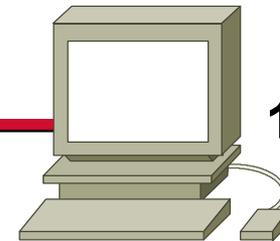
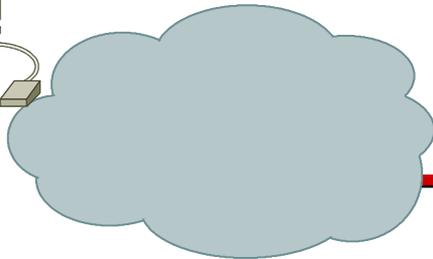
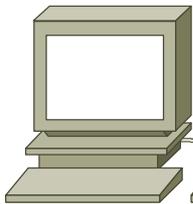


- **Individual Resources**
- **Threats**
- **Avoidance measures**

Spoofting

```
interface Serial 1
ip address 172.26.139.2 255.255.255.252
ip access-group 111 in
no ip directed-broadcast
!
interface ethernet 0/0
ip address 10.1.1.100 255.255.0.0
no ip directed-broadcast
!
Access-list 111 deny ip 127.0.0.0 0.255.255.255 any
Access-list 111 deny ip 10.1.0.0 0.0.255.255 any
```

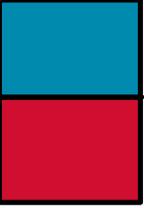
172.16.42.84



10.1.1.2

IP (D=10.1.1.2 S=10.1.1.1)





ICMP Filtering

Extended Access List:

```
access-list 101 permit icmp any any <type> <code>
```

Summary of Message Types

0 Echo Reply

3 Destination Unreachable no ip unreachables (IOS will not send)

4 Source Quench

5 Redirect no ip redirects (IOS will not accept)

8 Echo

11 Time Exceeded

12 Parameter Problem

13 Timestamp

14 Timestamp Reply

15 Information Request

16 Information Reply

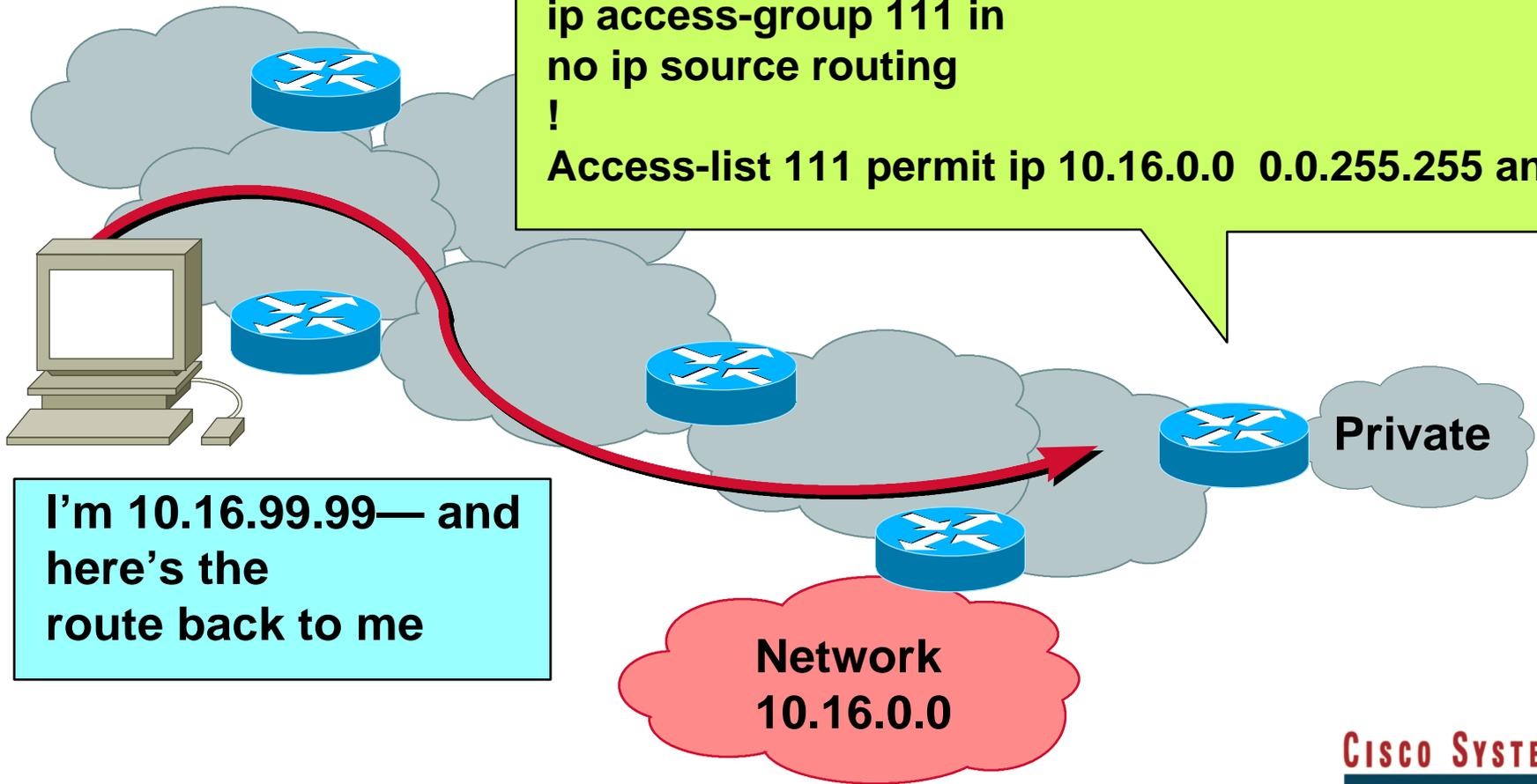
ICMP Codes are not shown

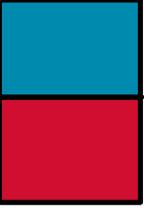
RFC 792: INTERNET CONTROL MESSAGE PROTOCOL



Source Routing

```
interface Serial 1
ip address 172.16.139.2 255.255.255.252
ip access-group 111 in
no ip source routing
!  
Access-list 111 permit ip 10.16.0.0 0.0.255.255 any
```





Choose “next talk” to continue viewing this presentation

(The length of this presentation made it necessary to split it in two parts. In all other cases, “next talk” takes you to the next presentation.)