



Battling the Snowden Effect: Securing the Management Plane

Brian Ford

Consulting Engineer

Advanced Development Group, Cisco Systems Inc.



Agenda

- Introduction
- Fundamental Security
- Login Security
- Password Security
- User Security
- Summary



Introduction

Breakdown of Trust



- While there may be untold number of examples of bad users in the past 24 months we have heard more reports of inappropriate SysAdmin behavior.
- Matthew Keys (Reuters), Edward Snowden (US NSA), others,....

What should we do?

Security Watch

TechNet
MAGAZINE

Why You Should Disable the Administrator Account

Is the 'Two-man rule' a solution?



- A.K.A. US Air Force Instruction (AFI) 91-104, "The Two Person Concept"
- N.S.A. Leak Puts Focus on System Administrators
- http://www.nytimes.com/2013/06/24/technology/nsa-leak-puts-focus-on-system-administrators.html?pagewanted=all&_r=0



Fundamental Security

Fundamental Security

- Infrastructure security is the core of network security
 - Protecting devices which pass traffic
- Securing network infrastructure
 - Management security
 - Login security
 - User Security
- Insurance: What to do in case something happens?
 - Accounting and monitoring
 - IOS Resiliency

Management Security

- Controlling method of access for management



Login Methods

- Why SSH over Telnet?
 - SSH encrypts data
 - Telnet is clear text

- Requirements for SSH
 - RSA keypair must be created on router
 - IOS image must support encryption
 - Management application must support SSH access

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

Restricting Management Access

- Only allow trusted IP addresses for management connections
- Configure access-list (ACL) to restrict login access

```
ip access-list extended LOGIN_ACL
  permit tcp host 10.1.1.100 any eq 22
!
line vty 0 4
  access-class LOGIN_ACL in
  transport input ssh
```

```
Router(config)# control-plane host
Router(config-cp-host)# management-interface FastEthernet0/0 allow ssh
```



Login Security

Login Security

- Banner on login prompts
- Password Security
- Restrict connection attempts



Login Banner



Welcome to Cisco's
Router!



Unauthorized access is not allowed.

Configuring a Banner

- Language matters
 - Requirements from legal department
 - Laws based on country and state
- The below example uses the '%' symbol as the message delineator

```
Router(config)# banner login %  
Enter TEXT message. End with the character '%'.  
This is a LOGIN banner %
```

```
Router(config)# banner exec %  
Enter TEXT message. End with the character '%'.  
This is a EXEC banner %
```

Login Banner in Use

```
[User]$ telnet 10.1.1.1
```

```
**Unauthorized access to this network device is prohibited.**  
You must have explicit permission to access or configure this  
device. All activities performed on this device are logged and  
violations of this policy may result in disciplinary action.
```

```
Username: cisco
```

```
Password: cisco
```

```
***By successfully logging in, you acknowledge that you have  
explicit permission to access and configure this device. You  
accept that all activities performed on this device are logged  
and violations of this policy may result in disciplinary action.
```

```
Router#
```

Warns user that they should back out now if they are not authorized to access the system.

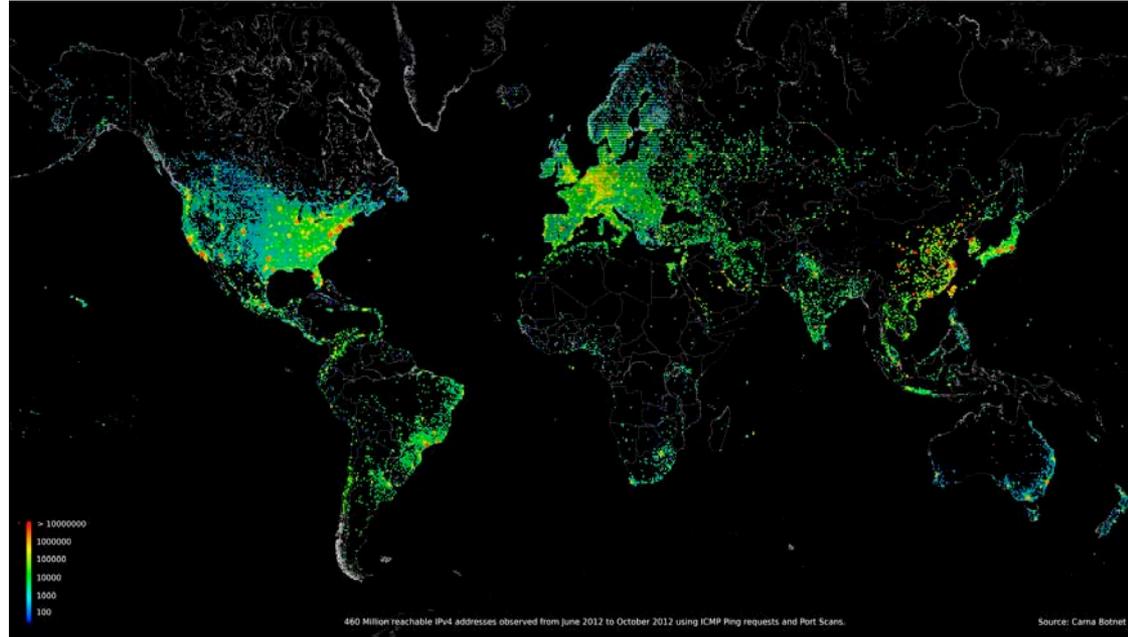
Acknowledges that user has successfully logged in and is responsible for actions.



Password Security

Enhanced Password Security

- 500,000 devices on internet have default password of **root**
- Password Restriction
- Password Encryption methods
 1. Password Encryption service
 2. SHA256/MD5 hash



Password Restriction

- Cisco IOS routers do not restrict passwords by default
- Password restriction ensures local passwords adhere to the following rules
 - Must contain characters from at least three of the following classes:
 1. lowercase letters
 2. uppercase letters
 3. digits
 4. special characters
 - Cannot have a character repeated more than three times consecutively.
 - Cannot be the same as the associated username.
 - Cannot be variant of the word “cisco”.

```
Router(config)#aaa new-model
```

```
Router(config)#aaa password restriction
```

Password Encryption

- Service encryption uses a Cisco proprietary encryption algorithm
 - Encryption is based on a Vigenere cipher
 - Weak security because is it a polyalphabetic substitution

```
Router(config)#enable password cisco
Router#show run | include enable
enable password cisco
```

```
Router(config)#service password-encryption
Router#show run | include enable
enable password 7 02050D480809
```

Service Password-Encryption

- Below is a tool from the first hit on Google
 - Search term: **cisco service password-encryption cracker**



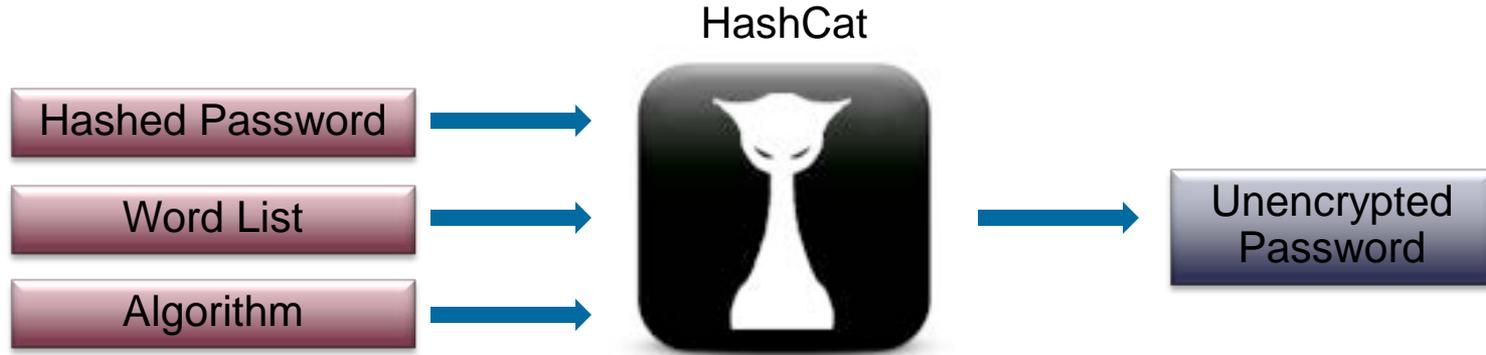
SHA/MD5 Password Protection

- One way hash algorithm that is not reversible
- SHA256 is the default encryption for IOS routers (Starting in 15.0.1S)

```
Router(config)#enable secret ?
 0      Specifies an UNENCRYPTED password will follow
 4      Specifies an SHA256 ENCRYPTED secret will follow
 5      Specifies an MD5 ENCRYPTED secret will follow
LINE   The UNENCRYPTED (cleartext) 'enable' secret
level  Set exec level password
Router(config)#enable secret cisco
```

```
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
enable password cisco
```

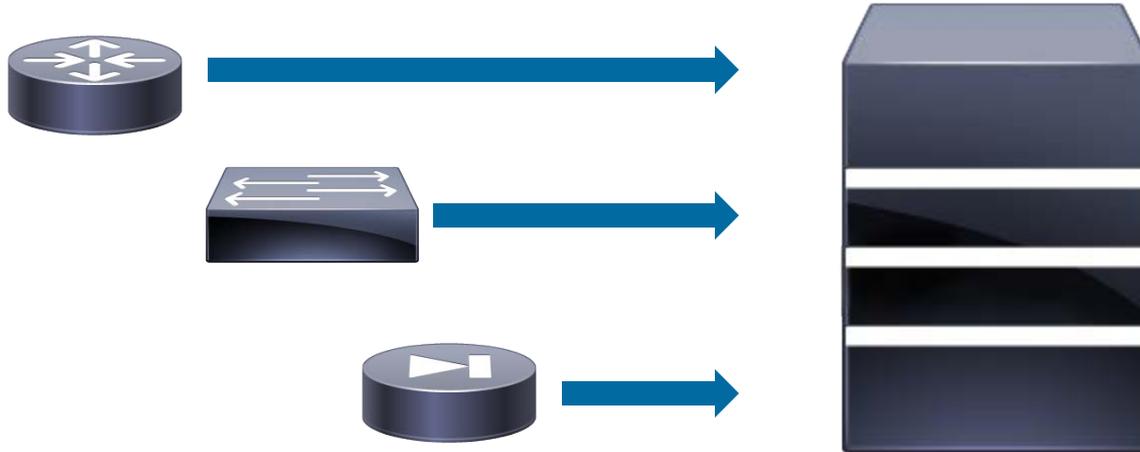
Password Cracking



- ArsTechnica case study cracked 45% of a 17,000 hashed password list in 90 seconds using above technique
- SHA256/MD5 hashes are protected using a salt
 - Salt is a random sequence of characters added to end of password before hash

Access Control Server (ACS) Integration

- Configuring ACS server
- Passwords are only as safe as their storage medium
- ACS integration provides a centralized services to store passwords
- Compromised configurations provide no insight into passwords



One Time Passwords (OTP)

- One time passwords are used to restrict access for temporary users
 - Introduced in 12.4

```
Router(config)#username TAC one-time secret cisco
```

- ACS OTP provides two tier authentication
 - Use secure token to generate password
 - New password for login each session



Session Limits

- Configuring restrictions on brute force attacks will mitigate the effectiveness of the attack by delaying success

Password Length	Time to Crack
12 digit password	6 months
12 digit password + login restriction	758 billion years

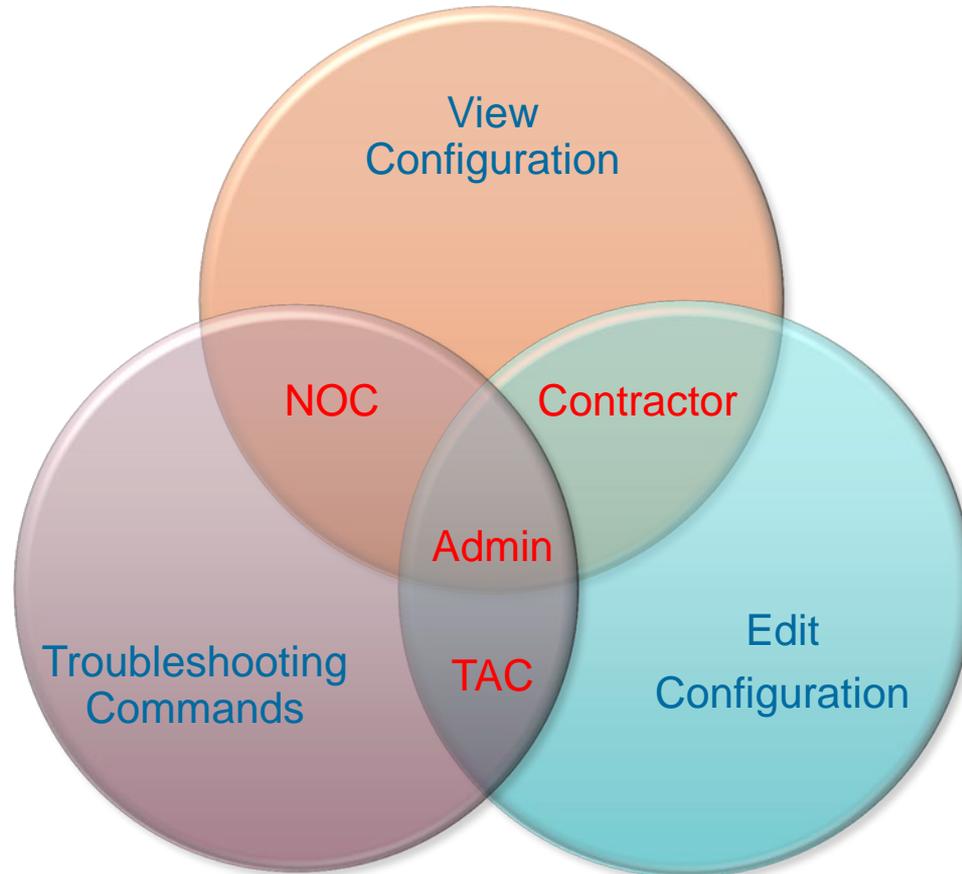
```
login block-for 30 attempts 3 within 10
```

- Login block for failed login attempts

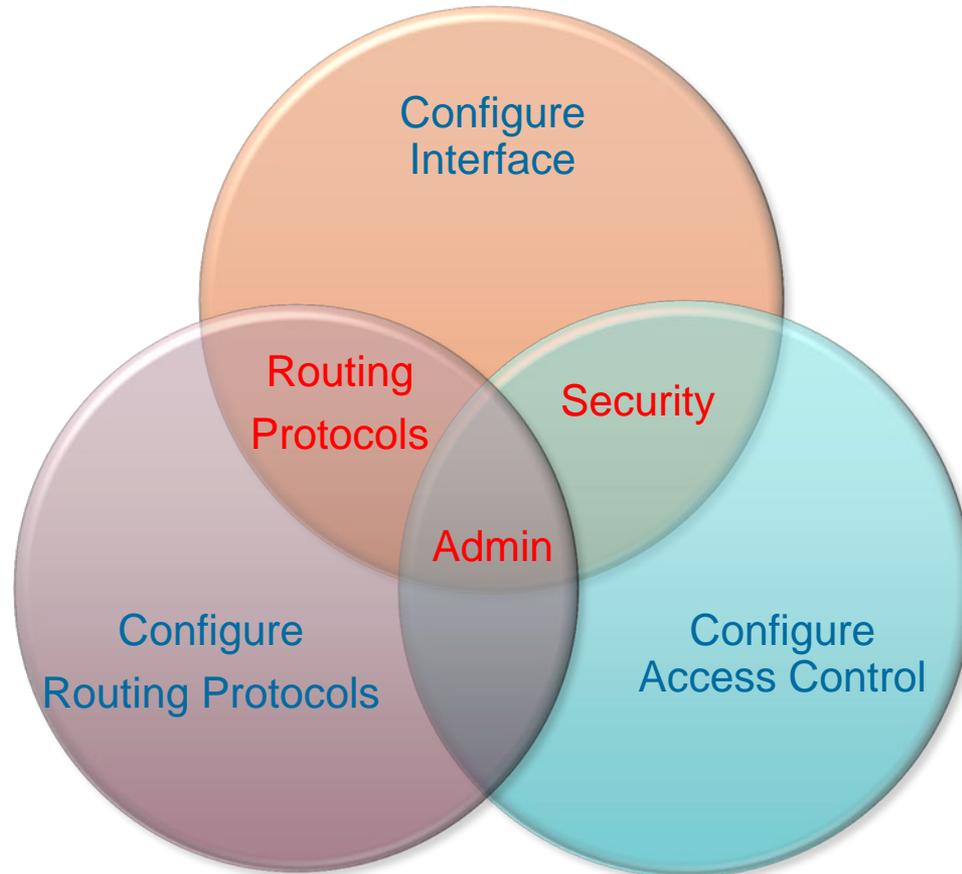


User Security

Functionality Based User Security



Command Based User Security



Privilege Levels

User EXEC Mode

- Privilege Level 0
- Can only enable

```
Router>
```

Privileged EXEC Mode

- Privilege Level 1
- View status of router

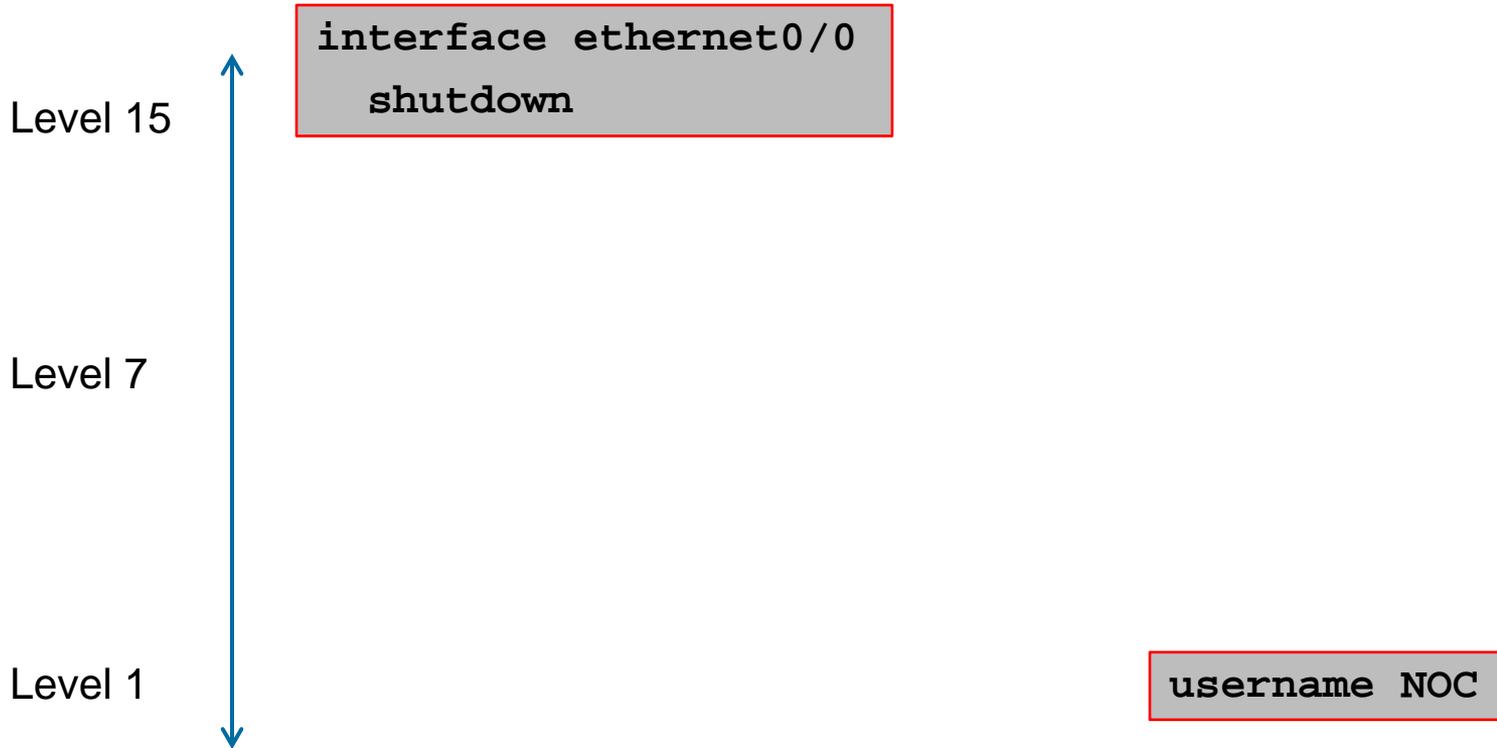
```
Router#
```

Global Configuration Mode

- Privilege Level 15
- Configuration commands

```
Router(config)#
```

Changing Privilege Levels of Commands



Role Based Access Control

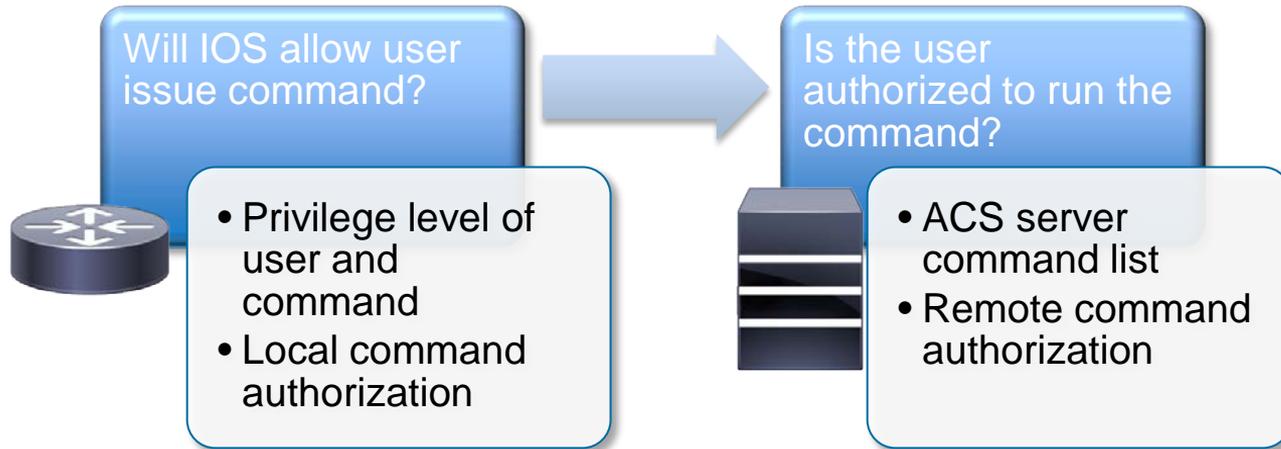
- Creates views so users can only view a subset of commands in the parser
- Provides more detailed control over CLI access
- Assigned views to each user with restriction
 - Commands seen in parser
 - Commands allowed to be issued
- Superviews can be used to aggregate functionality

```
parser view INTERN
  secret
  commands exec include show version
  commands exec include show
```

- Introduced in 12.3(7)

Remote Command Authorization

- Centralized server to verify commands before execution
 - User gets command authorization set based on device
 - Scalable solution for large network environments
- Router will communicate with ACS to verify command before execution



Insurance

- If router is compromised
 - How to mitigate the impact?
 - Restore device back to last known working condition?
- Mitigating the impact of configuration changes
 - Configuration Archive
 - IOS Resiliency
- Tracking down the source of the change
 - Command Accounting



Configuration Backup and Rollback

- Stores configuration periodically to destination location

```
archive
  path disk0:myconfig_backup
  maximum 5
  time-period 1440
```

- Force a configuration archive

```
Router# archive configuration
```

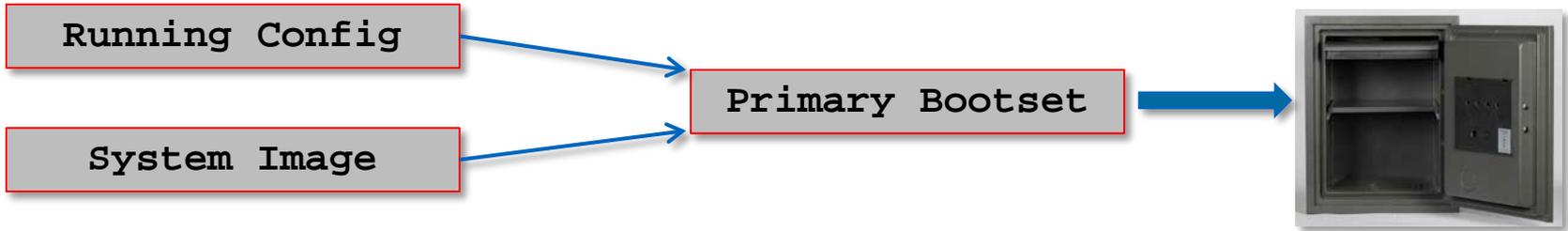
- Rollback configuration

```
Router# configure replace disk0:myconfig_backup-<date>
```

- Introduced 12.3(7)T

IOS Resiliency

- Saves a copy of the **running-config** and **system image** onto local storage
 - This is called the **primary bootset**
 - **Primary bootset** can be used to restore a previous image and config
- Feature can only be disabled by a console session
 - Can be initially enabled via any CLI session



- Introduced in 12.3(8)T

Network Accounting

- Log command history to location
 - Local archive
 - ACS
- Tracks configuration changes
 - Per-session
 - Per-user
- Introduced 12.4(11)T

```
archive
log config
logging enable
logging size 200
hidekeys
notify syslog
```

```
Router#show archive log config all
```

idx	sess	user@line	Logged command
1	8	NOC@vty0	interface Ethernet0/2
2	8	NOC@vty0	shutdown





Summary

Summary of Security Best Practices

- Control **management access** to trusted IPs and interfaces
- Use **login banner** as notification tool
- Configure **secure passwords** stored on a **centralized server**
- Control authenticated user movement by using **command authorization**
- **Archive configurations** for insurance
- Enforce **command accounting** to track changes on device
- Protect **control plane** by rate limiting or dropping traffic to CPU



Thank you.





CISCO