IOS Security

- When a Cisco router or switch is received from the factory no security is configured
- You can access the command line via a console cable with no password required
- One of the first tasks is to configure security to ensure that only authorised administrators can access the device

IOS Command Hierarchy

- hostname> — User Exec mode
- hostname# — Privileged Exec mode (‘Enable’)
- hostname(config)# — Global Configuration mode (‘Configure Terminal’)
- hostname(config-if)# — Interface Configuration mode (‘Interface *x*’)

FLACKBOX
www.flackbox.com

Basic Line Level Security

- Minimal password security can be configured through the use of static, locally defined passwords at three different levels:
  - Console line – accessing User Exec mode when connecting via a console cable
  - Virtual terminal VTY line – accessing User Exec mode when connecting remotely via Telnet or SSH Secure Shell
  - Privileged Exec Mode – entering the ‘enable’ command

Basic Line Level Security

- The levels can be used independently or in combination with each other.
- They can use the same or different passwords.

Basic Console Security

- Only one administrator can connect over a console cable at a time so the line number is always 0.
- 'Login' with no following keywords requires the administrator to enter the password configured at the line level to log in

```
R1(config)#line console 0
R1(config-line)#password Flackbox1
R1(config-line)#login
```

Basic Console Security

```
R1 con0 is now available
Press RETURN to get started.

User Access Verification
Password: <wrong password>
Password: <correct password>

R1>
```

Basic Telnet Security

- An administrator can use Telnet to connect to the CLI of a router or switch remotely over an IP connection
- IOS devices do not accept incoming Telnet sessions by default
- An IP address and virtual terminal VTY line access must be configured

Switch Management IP Address

- A Layer 2 Switch is not IP routing aware
- It does however support a single IP address for management
- A default gateway also needs to be configured to allow connectivity to other subnets

Switch Management IP Address

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.0.1
```

Basic Telnet Security

- Multiple administrators can connect at the same time. Lines are allocated on a first come first served basis
- If all configured lines are in use then additional administrators will not be able to login

```
R1(config)#line vty 0 15
R1(config-line)#password Flackbox2
R1(config-line)#login
```

Basic Telnet Security

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification

Password:<wrong password>
Password:<correct password>
R1>
```

Exec Timeout

- An administrator will be logged out after 10 minutes of inactivity by default. This applies to both the console and VTY lines
- You can edit this value with the exec-timeout command
- `no exec-timeout` or `exec-timeout 0` allows an administrator to stay logged in indefinitely

```
R1(config)#line con 0
R1(config-line)#exec-timeout 15
R1(config)#line vty 0 15
R1(config-line)#exec-timeout 5 30
```

Securing VTY Lines with Access Lists

- You can apply an Access List to control access to the VTY lines
- This can be used to limit Telnet and SSH access to only your administrator workstations

```
R1(config)#access-list 1 permit host 10.0.0.10

R1(config)#line vty 0 15
R1(config-line)#login
R1(config-line)#password Flackbox3
R1(config-line)#access-class 1 in
```

Securing VTY Lines with Access Lists

- Unauthorised source IP address:

```
C:\> telnet 10.0.0.1
Trying 10.0.0.1 …
% Connection refused by remote host
```