LAB 1: STOPPING OTHER SERVICES

There are quite a few services that are not necessary for the functioning of your router. You should disable all of them.

Global config

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no ip finger
router (config)# no ip bootp server
router (config)# no ip name-server
router (config)# no service config
router (config)# no boot network
router (config)# no service pad
```

Interface config

```
router (config)# int eth0/0
router (config-if)#no ip proxy-arp
router (config-if)#no ip mask-reply
router (config-if)#no ip redirects
```

Blocking ICMP Redirects and ICMP directed broadcast on interfaces. ICMP broadcast is well known smurf attack.

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# int eth0/0
router (config-if)#no ip redirects
router (config-if)#no ip directed broadcast
router (config-if)#^Z
```

Blocking ICMP Redirects from reaching your router, you should do this on your edge / border routers

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 105 deny icmp any any redirect
router (config)# access-list 105 permit ip any any
router (config)# int Fa0/0
router (config-if)#ip access-group 105 in
router (config-if)#^Z
```

LAB 2: DISABLING CDP

Cisco Discover Protocol. It's a protocol used by Cisco routers/switches to find information about connected routers. On the internet, this means like publishing full information about your Cisco devices. CDP should be disabled on all routers and switches.

Disabling CDP Globally

```
router#show cdp neigh


router#conf t
Enter Configuration Commands, one per line.
router (config)# no cdp run
router (config)#^Z
router #
```

Disabling CDP on a particular interface

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# int eth0/0
router (config-if)#no cdp enable
router (config-if)#^Z

router#show cdp neigh

router#show cdp neigh detail
```

LAB 3: SETTING UP WARNING BANNERS

Configure Login Banner

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# banner login $
Enter TEXT message. End with the Character  '!'.
Warning !!!
This system belongs to ISP Lahai. Any unauthorized access to
this system will violate laws of the country and will result
in procecution.
$
!
router (config)#^Z
router (config)#
```

Setting up Information to users.

Configure Exec Banner

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# banner exec $
Enter TEXT message. End with the Character  '!'.
IMPORTANT Information
Please be careful with the commands you issue in this
mode.Take a backup of any configuration changes before writing
them to the router.
$
```

LAB 4: MANAGING THE PASSWORDS

Setting up console Password

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line console 0
router (config-line)# login
router (config-line)# password console-password
router (config-line)#^Z
router #
```

Setting up Aux Password

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line aux 0
router (config-line)# login
router (config-line)# password aux-password
router (config-line)#^Z
router #
```

Setting up Virtual Terminal (VTY) Password

Since there are more than one VTYs, the configuration is slightly different

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line vty 0 4
router (config-line)# login
router (config-line)# password vty-password
router (config-line)#^Z
```

Checking the new configuration

```
router#sh run
line con 0
     password console-password
     login
line aux 0
     password aux-password
     login
line vty 0 4
     password vty-password
```

```
     login
```

Enabling Encryption

```
router (config)# service password-encryption
router (config)# ^Z
```

Enabling privilege level password

```
router (config)# enable secret enable-secret
router (config)# ^Z
```

If you have enable password, instead of a enable secret, the secret takes precedence over the password. As usual, please use the password encryption and save the configuration.

Enabling Local Usernames

```
router (config)# username gaurab password gaurab-pass
router (config)# ^Z
```

Creating Local username without password

```
router (config)# username system nopassword
router (config)# ^Z
```

Enabling Local Authentication on VTY terminal

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line vty 0 4
router (config-line)# login local
router (config-line)#^Z
router #
```

Disabling login on AUX port

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# line aux 0
router (config-line)# login local
router (config-line)# no password
router (config-line)# transport input none
router (config-line)# no exec
router (config-line)# exec-timeout 0 1
router (config-line)#^Z
router #
```

In the above example, note the tricky way to completely disable login. First you enable local login, but do not assign a password, which will disallow anyone from logging in. If you do 'no login', it'll allow password less access to everyone.

LAB 5: SECURING THE VTY ACCESS

Limiting Access by IP Address

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 10 permit 192.168.0.1
router (config)# access-list 10 permit 192.168.0.240
router (config)# access-list 10 deny any
router (config)# line vty 0 4
router (config-line)# access-class 10 in
router (config-line)#^Z
router #wr
```

Setting up timeout

```
router (config)# line vty 0 4
router (config-line)# exec-timeout 5 0
router (config-line)#^Z
router #wr
```

LAB 6: SECURING HTTP ACCESS

Limiting Http Server by IP

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# access-list 20 permit 192.168.0.1
router (config)# access-list 20 deny any
router (config)# ip http access-class 20
router (config)#^Z
```

Disabling Http server

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# no ip http server
router (config)#^Z
router #wr
```

LAB 7: CONFIGURING NTP

If you want your system to become an authoritative NTP server from which other internal routers or machines can synchronise, you can achieve this with the following command

R1(**config)# ntp master**

Now we instruct our Cisco router to obtain its updates from the NTP Master

R2(config)# **ntp server x.x.x.x (Loopback address of the master)**

Using and Cofiguring NTP Service. Again you can use access lists

```
router#conf t
Enter Configuration Commands, one per line.
router (config)# ntp server 192.168.0.1
router (config)# ntp master 10
router (config)# ntp access-group peer 5
router (config)#^Z


access-list 5 permit x.x.x.x
access-list 5 permit y.y.y.y
access-list 5 deny any
```