# - Basic Router Security -

## Enable Passwords

The *enable* password protects a router's Privileged mode. This password can be set or changed from Global Configuration mode:

```
Router(config)#  enable password MYPASSWORD
Router(config)#  enable secret MYPASSWORD2
```

The *enable password* command sets an unencrypted password intended for legacy systems that do not support encryption. It is no longer widely used.

The *enable secret* command sets an MD5-hashed password, and thus is far more secure. The *enable password* and *enable secret* passwords **cannot be identical**. The router will not accept identical passwords for these two commands.

## Line Passwords and Configuration

Passwords can additionally be configured on router **lines**, such as telnet (vty), console, and auxiliary ports. To change the password for a console port and all telnet ports:

```
Router(config)#  line console 0              Router(config)#  line vty 0 4
Router(config-line)#  login                  Router(config-line)#  login
Router(config-line)#  password cisco1234     Router(config-line)#  password cisco1234

Router(config-line)#  exec-timeout 0 0       Router(config-line)#  exec-timeout 0 0
Router(config-line)#  logging synchronous    Router(config-line)#  logging synchronous
```

The *exec-timeout 0 0* command is optional, and disables the automatic timeout of your connection. The two zeroes represent the timeout value in minutes and seconds, respectively. Thus, to set a timeout for 2 minutes and 30 seconds:

```
Router(config-line)#  exec-timeout 2 30
```

The *logging synchronous* command is also optional, and prevents system messages from interrupting your command prompt.

By default, line passwords are stored in clear-text in configuration files. To ensure these passwords are encrypted in all configuration files:

```
Router(config)#  service password–encryption
```

## ***Disabling Unnecessary Services***

Cisco IOS devices support many services that may pose a risk to the network. These services, if unneeded, should be disabled. Additionally, any interfaces that are not being used should be disabled using the *shutdown* command:

```
Router(config)#  interface ethernet0
Router(config-if)#  shutdown
```

**BOOTP** can be used by Cisco devices to load copies of the IOS to other Cisco devices, and is **enabled by default**. To disable this service:

```
Router(config)#  no ip bootp server
```

**CDP** (Cisco Discovery Protocol) allows Cisco devices to "discover" information about other directly connected Cisco devices, and is **enabled by default**. CDP can be disabled either globally or on a per-interface level:

```
Router(config)#  no cdp run

Router(config)#  interface ethernet0
Router(config-if)#  no cdp enable
```

Cisco devices can load their startup-configuration files from a remote FTP server, though this service is **disabled by default**. Either of the following commands will prevent the router from doing this:

```
Router(config)#  no boot network
Router(config)#  no service config
```

If a device name or unrecognized command is typed into the IOS command line, the IOS will attempt to resolve the name using **DNS**. By default, the IOS will broadcast (255.255.255.255) this request. To specify a specific DNS server for name resolution:

```
Router(config)#  ip name-server 192.168.1.1
```

DNS name resolution can be disabled if necessary:

```
Router(config)#  no ip domain-lookup
```

## ***Disabling Unnecessary Services (continued)***

Cisco routers, as of IOS 11.3, can function as an FTP server. This can be useful to copy configuration files back and forth from your router. However, this could also allow an unauthorized person to gain access to the router file system. This service is **disabled by default** as of IOS 12.3. To manually disable this service:

```
Router(config)#  no ftp-server write-enable
```

Earlier version of the IOS may use the following syntax:

```
Router(config)#  no ftp-server enable
```

To disable the TFTP equivalent:

```
Router(config)#  no tftp-server flash
```

The **Finger** service allows someone to query what users are logged into a device, and is **enabled by default.** This is the same information displayed when the *show users* command is inputted. To disable the finger service:

```
Router(config)#  no ip finger
Router(config)#  no service finger
```

The Cisco IOS now supports a basic **HTTP** management interface. However, access to this interface should be regulated. If the HTTP interface is unnecessary, disable it using the following command:

```
Router(config)#  no ip http server
```

A Cisco device can respond to an **ICMP Mask Request**, providing the requestor with the subnet mask of an interface, though this is **disabled by default**. To manually disable:

```
Router(config)#  interface Ethernet 0
Router(config-if)#  no ip mask-reply
```

**Source Routing** allows a sending device to dictate the exact routing path to a destination, a function which can be exploited by a malicious user. Source Routing is **enabled by default**. To manually disable:

```
Router(config)#  no ip source-route
```

## *Disabling Unnecessary Services (continued)*

**By default**, Cisco devices will respond to **ICMP Unreachable Messages**, informing the requestor which IP addresses are reachable (or not). These messages should be disabled to deny a malicious user potentially compromising information:

```
Router(config)#  interface serial 0
Router(config-if)#  no ip unreachable
```

**Network Time Protocol (NTP)** can be used to synchronize the time on all Cisco devices to a central time source. A router can function as either an NTP client or server. Useful as this is, NTP has recognized security flaws and can be compromised. NTP authentication can (and should) be utilized (explained in a different section). To completely disable NTP on an interface:

```
Router(config)#  interface ethernet 0
Router(config-if)#  ntp disable
```

**Proxy ARP** allows for resolution of Layer 2 addresses across multiple interfaces of a router. Essentially, devices in separate IP subnets can act as if they are on the same physical segment. This should NOT be enabled on any interface connecting to an untrusted network, as it could allow someone to spoof the MAC of a trusted host. Proxy ARP is **enabled by default** on **all interfaces** (….bastards!).

```
Router(config)#  interface ethernet 0
Router(config-if)#  no ip proxy-arp
```

Cisco devices support various UDP and TCP **Small Servers**, including:

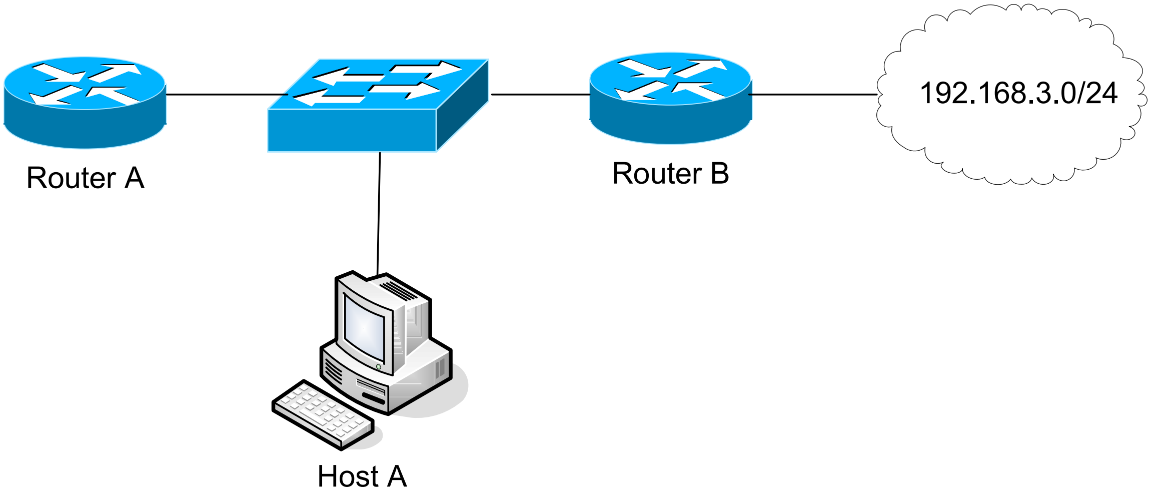
- **Echo** – echoes what you type to screen
- **Discard –** discards whatever is typed
- **Chargen –** generates a stream of ASCII data
- **Daytime –** displays system date and time

These services were enabled by default up until IOS 11.3, and now are disabled by default. All of the Small Servers were susceptible to DOS attacks, and thus should be disabled:

```
Router(config)#  no service tcp-small-servers
Router(config)#  no service udp-small-servers
```

## ***ICMP Redirects***

Cisco devices support **ICMP Redirects,** which are **enabled by default**. An ICMP redirect is sent from a router, to a particular host, telling that host about a *better* route to a particular destination.



Consider the above example, and assume that the Host points to Router A as its default gateway. When the Host sends a packet destined to 192.168.3.0, it will forward it first to Router A, which then forwards it *out the same interface again* to Router B.

If ICMP Redirects are enabled, Router A will inform the Host that Router B is the best next hop to the destination. The Host will add this to its local routing table, and send any subsequent packets destined for the 192.168.3.0 network directly to Router B.

This service could potentially be exploited by a malicious hacker. To disable ICMP Redirects:

```
Router(config)#  interface serial 0
Router(config-if)#  no ip redirect
```

(Reference: *http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094702.shtml*)