SIMPLE PASSWORDS

By default, the console port is wide open to user EXEC and privileged EXEC (enable). By default, network ports (VTY) are not open.

"Shared" Passwords—passwords with no username attached.

Setting basic shared passwords for access to a switch:

```
SW> enable
SW# configure terminal
SW(config)#
```

Now you can configure either the console port or vty access via network connections (telnet/ssh)

CONSOLE PORT	NETWORK ACCESS
`SW(config)# line console 0`	`SW(config)# line vty 0 15`
`SW(config-line)# password cisco`	`SW(config-line)# password cisco`
`SW(config-line)# login`	`SW(config-line)# login`
	! This will also require a working IPv4 config:
	! - Set the default gateway
	! - Set an IP address on a VLAN interface (SVI)

Password to Secure Privileged Exec (enable)

```
SW(config)# enable secret class
```

Using a secret password instead of "enable password class" encrypts the password in the config-if

USER ACCOUNTS

First, (optionally) get rid of the userless passwords under the console and vty lines

```
SW(config-line)# no password
```

and change "login" to "login local." For brevity, commands are omitted and just config shown:

```
username myUser secret myPass
```

Again, using "secret" instead of "password" obscures the password in running-config

```
line console 0
 login local
```

"local" tells it to use username entries like the one above for user names and passwords. Because we replaced the command "login" with "login local," removing shared passwords was optional. They wouldn't work anyway because the user would be prompted for a username.

```
line console 0
 login local
```

Note: the book is completely neglecting the "password" command/parameter in favor of "secret."

EXTERNAL AUTHENTICATION SERVERS

AAA (Authentication, Authorization, and Accounting) Server—centralizes usernames and passwords, enabling system-wide updates. RADIUS and TACACS+ protocols are used to connect the switch to the AAA server with encryption for the user verification process.

SSH

SSH (Secure SHell)—Just like telnet, SSH uses the local username & password with "login local" on the vty lines. In addition, it requires the generation of an RSA crypto key pair, which in turn requires that the switch's hostname and domain-name be set.

```
hostname SW
ip domain-name precisionforesight.com
crypto key generate rsa
                    SSH version 2 requires 768 bits minimum
```

By default, both SSH and telnet servers are running on Cisco devices and both are allowed into the vty lines. You can increase security by disabling support for telnet. Some possible combinations:

```
transport input all
transport input telnet ssh
                    Same thing
transport input none
                    The default
transport input ssh
transport input telnet
```

You can also show ssh status and connections:

```
SW# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3

SW# show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0     IN   aes128-cbc  hmac-md5     Session started       MyAccount
0          2.0     OUT  aes128-cbc  hmac-md5     Session started       MyAccount
```

ENABLING IPV4 ON A SWITCH

Telnet, SSH, and SNMP all require L3 access to the switch for remote monitoring and configuration. With routers, this isn't a problem because they are natively L3 devices and would naturally have IP addresses. Switches, on the other hand, don't need a L3 IP address to forward L2 frames and adding one doesn't change the switching behavior.

SVI (Switched Virtual Interface)—Switches are covered in Ethernet jacks and adding a special one for their own management traffic would be silly, so we'll put the switch's own IP address on a virtual interface, e.g. VLAN 1. Some complications:

- There needs to be at least one physical interface on the switch that is assigned to that VLAN
- Traffic to/from the SVI will be on the corresponding VLAN, so that needs to be accessible from the rest of your network, perhaps through a trunk or interfaces on that VLAN

To get traffic off the VLAN and (sub)net of the SVI, you'll need a default gateway. Combined with the SVI, the configuration could look like:

```
ip default-gateway 192.168.0.1
interface vlan 1
 ip address 192.168.0.5 255.255.255.0
 no shutdown
```

DHCP—you can also allow the switch to configure itself, using a DHCP server.

```
interface vlan 1
 ip address dhcp
 no shutdown
```

IP Verification Commands

```
S1# show dhcp lease
Temp IP addr: 10.0.0.2  for peer on Interface: Vlan1
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 10.0.0.1, state: 3 Bound
   DHCP transaction id: 2050
   Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
Temp default-gateway addr: 10.0.0.1
   Next timer fires after: 11:56:57
   Retry count: 0   Client-ID: cisco-000c.85ca.e280-Vl1
   Client-ID hex dump: 636973636F2D303030632E383563612E
                       653238302D566C31
   Hostname: S1

S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 000c.85ca.e280 (bia 000c.85ca.e280)
  Internet address is 10.0.0.2/24
```

(Output shortened.) No clue given here whether the address is static or DHCP unless DHCP fails, in which case it'll say "Internet address will be negotiated using DHCP."

```
S1# show ip default-gateway
10.0.0.1
```

CONVENIENCE CONFIGS

Command History Buffer

```
SW# show history
SW# terminal history size 20
```

Current session only

```
SW(config-line)# history size 20
```

For the console or vty lines

Other

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

Don't do a DNS lookup on typos, thinking that I was trying to telnet

```
SW(config-line)# logging synchronous
```

If the system interrupts my typing with a log message, it'll reprint what I had typed so I don't lose my place.

```
SW(config-line)# exec-timeout 0 0
```

Don't hang up because my keyboard is idle. This command can also be used to set a specific idle timeout. First number minutes, second is seconds. 10 mins. default. Two zeroes disable timeout.