IOS Maintenance

Just like the manual to an appliance like a refrigerator or microwave over, we will cover basic maintenance stuff here. Later use and procedure will be covered.

Device memory: NVRAM=starting-configuration, DRAM(RAM)=running-configuration, Flash= IOS, ROM= the bootstrap aka "boothelper", the MiniIOS
Connections: RJ45 Rolled EN to USB or EIA-TIA 232 serial COM port; or just USB to USB
Remote: 9600 bits/sec, no flow control, 8N1, which means:, 8-bit ASCII, no parity, 1 stop bit
CLI modes: user EXEC (the > prompt); privileged EXEC aka enable mode (the # prompt); global config (config)#; line (config-line)#; interface (config-if)#; Without a config loaded, the rommon > prompt is used

Router and Switch Status LED Indicators

SYST	Overall system status Off = off, Green = IOS is loaded, Amber = power, but problem exists
STAT	Link: Off = not working; Solid Green = working, no traffic; Flashing/ blinking green = working, has traffic; Flashing Amber = STP is blocking
RPS	Redundant Power Supply Status
DUPLX (duplex)	Green = full, Off = half
SPEED	Solid = 100 Mbps; Flashing = 1 Gbps; Off = 10 Mbps
MODE	Cycles LEDs through STAT, DUPLX, SPEED
PORT	LEDs above each individual port

Boot order:

1) POST
2) Load bootstrap (ROM/ rommon) into RAM to run it
3) Get IOS and load it to RAM (from flash or net)
4) Locate start-config and load it as running config (looks in nvram, network, then console port)

1. **Maintaining the IOS and Configs**
   A. Backing up Saved Config
   B. Moving config files around
   C. Backing up/ selecting a boot IOS
   D. Erasing (or resetting) the device
   E. Configuration register: Reset Password/ boot to rommon
   F. Updating the IOS (licensing)

A. To backup the running and saved configuration:

Router1#copy running-config tftp
Address or name of remote host [ ]? 10.10.10.202
Destination filename [Router1-confg]?"

To restore:

Router1#copy tftp running-config (or copy tftp run)
Address or name of remote host [ ]? 10.10.10.202
Accessing tftp://10.10.10.202/ Router1-confg...
Loading Router1-confg from 10.10.10.254 (via FastEthernet0/0):
!!
[OK - 776 bytes]
776 bytes copied in 9.212 secs (84 bytes/sec)
Router1#
*Mar 7 17:53:34.071: %SYS-5-CONFIG_I: Configured from
tftp://10.10.10.202/Router1-confg by console

Remember that when you copy or merge a configuration from a TFTP server to a freshly erased and rebooted router's RAM, the interfaces are shut down by default and you must manually enable each interface with the no shutdown command.

B. Moving Config Files Around

copy {tftp | running-config | startup-config} {tftp | running-config | startup-config}
copy from-location to-location - EXEC cmd - RAM, NVRAM, TFTP or RCP servers, and flash memory.
copy running-config startup-config - saves your work to the NVRAM
copy startup-config running-config - **merges** the startup config with the running

From Cisco: "A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results"

From elsewhere: [It isn't really a "copy" at all ... you're pushing text from the source file into the front-end parser one line at a time, just as if you'd typed it in at config t. All data that was in the running configuration is kept EXCEPT what the startup config has a value for. That is, the startup config's specific data will overwrite the running-configs data, and whatever is left over in the running config is kept there.]

Note: when relevant, often with storage volumes, the UNIX-like commands work for files and directories: ls, dir, copy, more, delete, erase or format, cd and pwd, and mkdir and rmdir. Also 'show file info', 'show [volumelabel]' Cisco IFS uses the alternate term system:running-config as well as nvram:startup-config when copying the configurations on a router, although it is not mandatory that you use this naming convention
"Delete doesn't always free up space. To actually get the space back, you have to use the squeeze command." [There is no follow-up on this command when mentioned in the book!] "We can play with any file in flash memory and nothing serious will happen until we reboot. Like Partitioning a disk in *nix, changes aren't committed until written to disk. " This also is not explained in the book (Lammle)

copy running-config usbflash1:temp-copy-of-config
dir usbflash1:

Here are some more file system sources:

```
#copy running-config ?
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:  Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system"
```

C. Boot System Commands - Backup, and choose IOS file to boot from

Backing Up and Restoring the Cisco IOS

It's a good idea to verify that your flash memory has enough room to hold the new image. There are about 45 MB of flash used, but there still about 18 MB available. If you want to copy a file into flash that is more than 18 MB in size, the router will ask you if you want to erase flash.

```
Router#sh flash
-#- --length-- -----date/time------ path
1    45392400 Apr 14 2013 05:31:44 +00:00 c2800nm-advsecurityk9-mz.151-4.M6.bin
18620416 bytes available (45395968 bytes used)
```

```
Router#show version
[output cut]
System returned to ROM by power-on
System image file is "flash:c2800nm-advsecurityk9-mz.151-4.M6.bin"
[output cut]
Cisco 2811 (revision 1.0) with 249856K/12288K bytes of memory.
Processor board ID FTX1049A1AB
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
```

This router has about 256 MB of RAM, the amount of flash shows up on the last line (about 64MB). The show flash command displays all files in flash memory and the show version command shows the actual name of the file used to run the router and the location from which it was loaded.

Copy the IOS to the TFTP server as shown next:

```
Router#copy flash tftp
Source filename []?c2800nm-advsecurityk9-mz.151-4.M6.bin
Address or name of remote host []?1.1.1.2
Destination filename [c2800nm-advsecurityk9-mz.151-4.M6.bin]?[enter]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
45395968 bytes copied in 123.724 secs (357532 bytes/sec)
```

Just copy the IOS filename from either the show flash or show version command and then paste it when prompted for the source filename.

To restore or upgrade the IOS use the copy tftp flash command. This command requires the IP address of the TFTP host and the name of the file you want to download.
Make sure the file you want to place in flash memory is in the default TFTP directory on your host (TFTP won't ask you- it will just look there)

```
Router#copy tftp flash
Address or name of remote host []?1.1.1.2
Source filename []?c2800nm-advsecurityk9-mz.151-4.M6.bin
Destination filename [c2800nm-advsecurityk9-mz.151-4.M6.bin]?[enter]
%Warning: There is a file already existing with this name
Do you want to over write? [confirm][enter]
Accessing tftp://1.1.1.2/c2800nm-advsecurityk9-mz.151-4.M6.bin...
Loading c2800nm-advsecurityk9-mz.151-4.M6.bin from 1.1.1.2 (via
   FastEthernet0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 21710744 bytes]
45395968 bytes copied in 82.880 secs (261954 bytes/sec)
Router#
```

If the file is corrupted, you'll need to do an IOS-restore from ROM monitor mode.
If you are loading a new file and you don't have enough room in flash memory to store both the new and existing copies, the router will ask to erase the contents of flash memory before writing the new file into flash memory, and if you are able to copy the IOS without erasing the old version, then make sure you remember to use the boot system flash:ios-file command.

A Cisco router can become a TFTP server host for a router system image that's run in flash memory. The global configuration command is tftp-server flash:ios-file.

After an upgrade, if you reload the router and the router now shows the rommon> prompt.

Follow these steps to save your job:

```
rommon 1 > tftpdnld
Missing or illegal ip address for variable IP_ADDRESS
Illegal IP address.
usage: tftpdnld [-hr]
  Use this command for disaster recovery only to recover an image via TFTP.
  Monitor variables are used to set up parameters for the transfer.
  (Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
  "ctrl-c" or "break" stops the transfer before flash erase begins.

  The following variables are REQUIRED to be set for tftpdnld:
          IP_ADDRESS: The IP address for this unit
       IP_SUBNET_MASK: The subnet mask for this unit
      DEFAULT_GATEWAY: The default gateway for this unit
         TFTP_SERVER: The IP address of the server to fetch from
          TFTP_FILE: The filename to fetch

  The following variables are OPTIONAL:
[unneeded output cut]
rommon 2 >set IP_Address:1.1.1.1
rommon 3 >set IP_SUBNET_MASK:255.0.0.0
rommon 4 >set DEFAULT_GATEWAY:1.1.1.2
rommon 5 >set TFTP_SERVER:1.1.1.2
rommon 6 >set TFTP_FILE: flash:c2800nm-advipservicesk9-mz.124-12.bin
rommon 7 >tftpdnld
```

From here you can see the variables you need to configure using the set command; be sure you use ALL_CAPS with these commands as well as underscore (_).From here, you need to set the IP address, mask, and default gateway of your router, then the IP address of the TFTP host.

```
Router(config)#tftp-server flash:c2800nm-advipservicesk9-mz.124-12.bin
```

There is one other way you can restore the IOS on a router, but it takes a while. You can use what is called the Xmodem protocol to actually upload an IOS file into flash memory through the console port. You'd use the Xmodem through the console port procedure if you had no network connectivity to the router or switch.

Choosing the boot IOS with the BOOT command

By default, boots the first system IOS file found in flash. Change that with the following commands:

```
Router(config)#boot system ?
  WORD   TFTP filename or URL
  flash  Boot from flash memory
  ftp    Boot from a server via ftp
  mop    Boot from a Decnet MOP server
  rcp    Boot from a server via rcp
  rom    Boot from rom
  tftp   Boot from a tftp server
Router(config)#boot system flash c2800nm-advsecurityk9-mz.151-4.M6.bin
```

Grab a IOS image and get it over to a tftp or USB then copy it to flash:

```
copy tftp flash
address or name of host [ ] ? 10.1.1.20
Source filename[ ]? c2900-universalk9-hd-SPA.152.4.bin
```

Load a new IOS and test it.

Next is a fallback routine. You can make it permanent to boot from a TFTP host, but it isn't recommended.

Router(config)#boot system tftp c2800nm-advsecurityk9-mz.151-4.M6.bin 10.1.1.2
or "boot tftp://172.16.15.112/routertest"

Another failback- longer:
If the flash IOS doesn't load and the TFTP host does not produce the IOS, load the rommon. The mini-IOS will load after six unsuccessful attempts of trying to locate the TFTP server. The router will enter ROM monitor mode if even the Mini-IOS fails to load.

Router(config)#boot system rom
Router(config)#do show run | include boot system
boot system flash c2800nm-advsecurityk9-mz.151-4.M6.bin
boot system tftp c2800nm-advsecurityk9-mz.151-4.M6.bin 10.1.1.2
boot system rom

Remove with
no boot system tftp c2800nm-advsecurityk9-mz.151-4.M6.bin 10.1.1.2

http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf010.html

D. Erasing (or resetting) the device
write erase, erase startup-config , erase nvram:
These enable-mode EXEC commands erase the startup config file. erase nvram: is the latest and preferred.
For compact Flash cards, issue the erase flash: Use erase slot0: for external cards.

To clear the running and startup configuration files, follow these steps-
- Log into switch, enter privileged EXEC mode (enable, enter password)
- Enter write erase, which erases the NVRAM file system. At the prompt, confirm.
- Enter reload, and enter no when prompted whether to save. (Otherwise, the switch will reload the current running configuration)
- Confirm that you want to reload the switch, and your switch configuration is almost clean.

R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm][enter]
[OK]
Erase of nvram: complete
R1#reload
Proceed with reload? [confirm][enter]
*Mar 7 17:56:31.059: %SYS-5-RELOAD: Reload requested by console.
Reload Reason: Reload Command.

Depending on the model, erase vlan.dat will also remove VLAN info

E. The Configuration Register - ICND2 Ch 20 Slides
The 16 bits (2 bytes) of the configuration register are read from 15 to 0, from left to right. The default configuration setting on Cisco routers is 0x2102. This means that bits 13, 8, and 1 are on. Notice that each set of 4 bits is read in binary with a value of 8, 4, 2, 1. Notice that bit 6 can be used to ignore the NVRAM contents. This bit is used for password recovery.

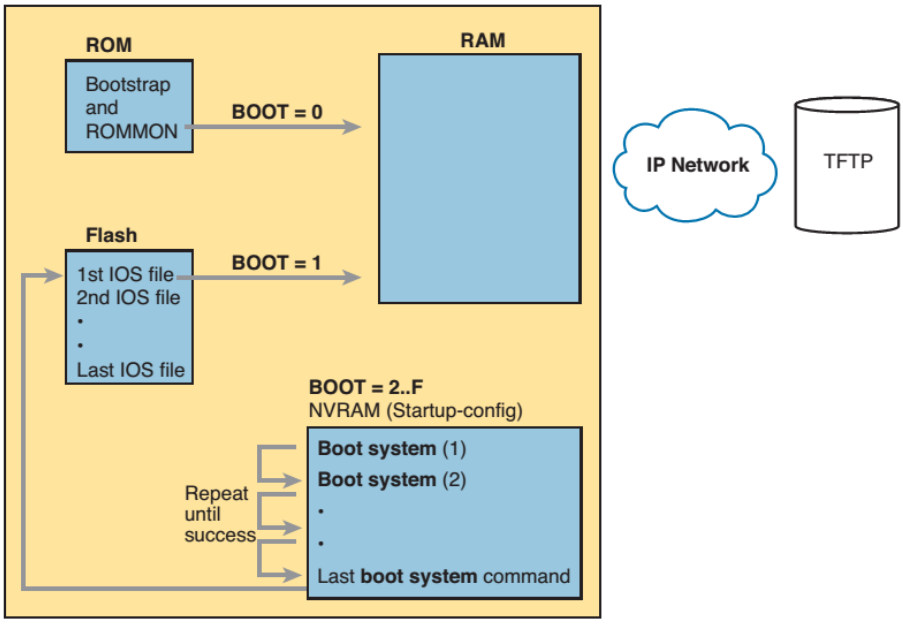
Configuration Register			**2**					**1**				**0**			**2**	
Bit number	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Binary	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0

Bit No. Hex Value Meaning/Function
00 to 03 0x0000 to 0x000F - The boot field.
Defines the source of a default Cisco IOS Software image required to run the router:
00 - (2100) Stays at the system bootstrap prompt/ rommon prompt. Manually boot the router with the b command.
01 - (2101) Boots the first IOS in onboard Flash memory (EPROM)
02-0F - (2102 - 210F) Override default netboot filename. Tells the router to boot to NVRAM, network, or then try console)
06 0x0040 Causes system software to ignore NVRAM contents.
07 0x0080 Enables the original equipment manufacturer (OEM) bit.
08 0x0100 Disables the Break function.
09 0x0200 Uses secondary bootstrap.
10 0x0400 Broadcasts Internet Protocol (IP) with all zeros.
5, 11, 12 0x0800 to 0x1000 Defines the console baud rate (the default setting is 9600 baud).
13 0x2000 Boots default Flash if network boot fails.
14 0x4000 Causes IP broadcasts to leave out network numbers.
15 0x8000 Enables diagnostic messages and ignores the contents of NVRAM.

0x2100 Stays at the system bootstrap prompt (rommon?)
0x2101 boots a system image on EPROM
0x2102 - Default: the last 2 means look at the flash IOS and NVRAM
0x2142 - Ignore startup config (NVRAM)

To change the configuration register, use the config-register command from global configuration mode:
Router(config)#config-register 0x2142
Router(config)#do sh ver
[output cut]
Configuration register is 0x2102 (will be 0x2142 at next reload)

If you save your configuration and reload the router and it comes up in setup mode, the configuration register setting is probably incorrect.



Review: Confreg - a 16-bit value - where's the IOS?
- if boot field ends in 0 use rommon
- if 1 = load first ios found on flash
- if 2-F = try number of IOS listed in "show flash (above)

"show flash" does a directory dump of sorts... gives IOS a number at far right side, which is the number of the IOS to use in confreg to specify one to use.
boot system flash - will use the first one found ;
boot system flash number (or filename) - use that one
boot system tftp filename 10.1.1.1
If the IOS doesn't load, it sends a broadcast looking for tftp server, then it guesses the filename, and finally loads the rommon to try again

Password Recovery: Boot to ROM Monitor; Config Register;
To recover a password, you need to turn on bit 6. Doing this will tell the router to ignore the NVRAM.
The configuration register value to turn on bit 6 is 0x2142.
Here are the main steps to password recovery:
1. Boot the router and interrupt the boot sequence by pressing the Ctrl+Break (or Ctrl+Shift+6 then b) as the router first reboots, which will take the router into ROM monitor mode.
2. Change the configuration register to turn on bit 6 (with the value 0x2142) and reload the router:
    monitor: command “boot” aborted due to user interrupt
    rommon 1 >confreg 0x2142
    rommon 2 >reset
3. Since no startup-config is used it asks to enter Setup mode, just say “no" and enter privileged mode.
4. Copy the startup-config file to running-config, and check that interfaces have re-enabled.
5. Reset the password with enable secret mypassword.
6. Enter "config-register 0x2102" (back to the default value).
7. Enter "copy running-config startup-config" and reload the router.
    And that serves as a reminder to always save your freshly changed configs! All should return to the previous configuration with the new "enable" password you just set.

- **Another example: removable Flash with saved config (I guess?)**
    1. Turn the router power switch off
    2. Carefully remove compact flash from the router
    3. Turn the router power switch on
    4. Watching initialization messages, waiting for ROMMON> prompt
    5. Once in ROMMON, reinsert the compact flash
    6. Set configuration register with **confreg 0x2142**
    7. Issue ROMMON **reset** command (reloads router)
    8. Watch for IOS to ask you to enter setup mode no)
    9. Log in from the console (no password) and enter enable mode
    10. Issue **copy startup-config running-config**
    11. Reset passwords with the appropriate commands
    12. Issue **copy running-config startup-config**
    13. Reset configuration register to its normal setting

In summary, the big ideas behind password recovery are as follows:
Step 1.. Boot ROMMON, either by breaking into the boot process from the console or by first removing all the flash memory.
Step 2 Set the configuration register to ignore the startup-config file (for example, confreg 0x2142).
Step 3. Boot the router with an IOS, and now you can reach enable mode from the console without needing any passwords.

Here is what the *show version* command displays:

Router1#show version
Cisco IOS Software, C2600 Software (C2600-ADVIPSERVICESK9-M)
Version 12.3(4)T4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 11-Mar-04 19:57 by eaarmas
ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
Router1 uptime is 20 minutes
System returned to ROM by power-on

System image file is "flash:c2600-advipservicesk9-mz.123-4.T4.bin"
This product contains cryptographic features and is subject to United States and ..... If you require further assistance please contact us by sending email to export@cisco.com.
Cisco 2621XM (MPC860P) processor (revision 0x300) 125952K/5120K bytes of memory.
Processor board ID JAE081160XR (3618058385)
M860 processor: part number 5, mask 2
2 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
32K bytes of NVRAM.
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102

F. Licensing - Technology Package Licenses
ipbasek9 (IP Base)- Entry-level IOS functionality
datak9 (data)- MPLS, ATM, multiprotocols, IBM support
uck9 (Unified Communications)- VoIP, IP Telephony
securityk9 (Security)- IOS firewall, IPS, IPsec, 3DES, VPN

Managing Software Activation with Cisco License Manager (CLM)
Communicates with Cisco's Product License Registration Portal
Takes information about feature purchases from any reseller
Communicates with devices to install license keys

Historically each model got their own version 2811 2821 2851 models eg
Downloaded purchased feature sets
New system - one universal image with all feature sets to activate
Individual models still get their own version
IPBASE license only given - buy license, install to activate after adding and rebooting

Manually activating
sh license udi
UDI - unique device id - shows "index 1 IPBASE" and the info index 2 security etc.,
PAK is a code you get after you upgrade with Cisco, they will ask for the PAK and UDI
They send you a license file shtjtrtjtrwjtjw.LIC
USB it over - license install usbflash: url or tftp:
Feature list current, type, and after reboot listed

Step 1. At the Cisco Product License Registration Portal (reachable from www.cisco.com/go/license), input the UDI of the router, as gathered using the show license udi command.
Step 2. At that same portal, type in the PAK for the license you purchased, as learned from your reseller or directly from Cisco.
Step 3. Copy the license key file (download or email) when prompted at Cisco's Product License Registration Portal website.
Step 4. Make the file available to the router via USB or some network server.

show license
show license feature

dir usbflash1:
license install usbflash1:FTX1628838P_201302111432454180.lic
show license will be updated with "permanent" and "lifetime"

Right-to-Use Licenses
Cisco allows an unlimited* license without a PAK through *right-to-use*
60-day trial period that works on an honor system afterwards

license boot module c2900 technology-package securityk9
show license will be updated with "right to use" and time used/left

boot system {file-url | filename}
Global command that identifies an externally located IOS image using a URL

boot system flash [flash-fs:] [filename]
Global command that identifies the location of an IOS image in flash memory

boot system rom
Global command that tells the router to load the RxBoot OS found in ROM, if one exists

boot system {rcp | tftp | ftp} filename [ip-address]
Global command that identifies an external server, protocol, and filename to use to load an IOS from an external server

reload
Enable mode EXEC command that reboots the switch or router.

copy from-location to-location
Enable mode EXEC command that copies files from one file location to another. Locations include the startup-config and running-config files, files on TFTP and RPC servers, and flash memory.

copy running-config startup-config
Enable mode EXEC command that saves the active config, replacing the startup-config file used when the switch initializes.

copy startup-config running-config
Enable mode EXEC command that merges the startup- config file with the currently active config file in RAM.

show running-config
Lists the contents of the running-config file.

write erase
erase startup-config
erase nvram:
All three enable mode EXEC commands erase the startup- config file.

show flash
Router#show flash
 -#- --length-- -----date/time------ path
1   15679252 Dec 27 2007 01:37:22 +00:00 c2800nm-ipbase-mz.124-3i.bin
2   1823 Dec 27 2007 01:45:46 +00:00 sdmconfig-2811.cfg
3   6036480 Dec 27 2007 01:46:24 +00:00 sdm.tar
4   861696 Dec 27 2007 01:46:46 +00:00 es.tar
5   1164288 Dec 27 2007 01:47:04 +00:00 common.tar

6 1038 Dec 27 2007 01:47:20 +00:00 home.shtml
7 113152 Dec 27 2007 01:47:36 +00:00 home.tar
8 1697952 Dec 27 2007 01:48:04 +00:00 securedesktop-ios-3.1.1.45-k9.pkg
9 416354 Dec 27 2007 01:48:24 +00:00 sslclient-win-1.1.3.173.pkg
38027264 bytes available (25989120 bytes used)

Basic IOS setup (passwords, usernames, ssh, lockdown tty and console)

Keyboard Shortcuts

Up/ Down arrows or Ctrl-P/ Ctrl-N	Move forward/ back in command history
Left/ Right arrows or Ctrl-B/Ctrl-F	Moves cursor forward/back without deleting characters
Backspace/ Ctrl-D	Moves cursor backward while deleting characters
Ctrl-A/ Ctrl-E	Moves cursor to the first/last character of the currently displayed command
Ctrl-Shift-6	Interrupts the current command. This and then "x" switches between ttys
Ctrl-Z	Same as end - exits config mode

show history - to view the whole history buffer
history size length - for line config mode, set the length of the history buffer
terminal history size x - current user only, only for the current login to the switch.
no history - also for line config mode, who needs a history buffer? This turns it off.

Setting passwords - basic lockdown of things

- - Set a password to enter the Privileged Exec aka "enable" mode, and "secret"
enable password mypassword
enable secret mysecret

- - Set a password to enter the 3 types of connections on the device:
For the Auxilary line, type "line aux 0", then on separate lines:
login -- login is a command here telling it to require the general password to log in
password mypassword
logging synchronous -- keeps syslog messages from popping up, interrupting typing in stuff
exec-timeout 10 10 --minutes, seconds. Default is 10 minutes. How long before an idle connection is kicked off.

Now, do exactly the same thing for the Console line (line console 0) and Telnet lines (line vty 0 15)
When you are all done, return to global configuration mode and enter:
service password-encryption <--- this is just a hash, but makes passwords unreadable in the configuration
Note: The "no service password-encryption" leaves passwords hashed; new password values will be clear text.

service password-encryption is hashed- cracked with the downloadable app
no login -- disables checking! Don't do it unless setting up the "login local" username requirement

Additional items, usernames and setting hostname, domain name for SSH setup:
hostname YourHostname
ip domain-name mydomain_name.com <--- you need to set up hostname and domain name for SSH
ntp server time-c.nist.gov version [number] <---sh ntp status to verify it's working.
[no] ip lookup <--- prevent wasting processor time resolving every IP address into DNS
[no] logging console <---- enable or prevent messages being sent to the console

Set up for usernames and SSH
username janicel password bones215

username jamesk password spock314
In "line vty 0 15" aux, and "line console 0" configurations, replace "login" by typing in "no login" then immediately, "login local" to ask for username/password to get in.

SSH configuration:
ip domain-name mydomain_name.com
crypto key generate rsa
The name for the keys will be: myusername@mydomain_name.com <--- match what you put in earlier
How many bits in the modulus [512]: 2048
ip ssh version 2

line vty 0 15 <--------- almost done- just update your lines
Choose one of these to add to your lines:
transport input telnet: Support only Telnet
transport input ssh: Support only SSH
transport input all **or** transport input telnet ssh: Support both (this is default)
transport input none: Support neither <--------DONT DO THIS.
Finally, be sure to check out your work and verify: type the global command "show ip ssh"
[you should also be able to log in with ssh -l username <ipaddress>]

logging synchronous
[no] logging console
exec-timeout minutes [seconds]
banner [motd | exec | login] delimiter banner-text delimiter

Setting Up Banners
MOTD is shown before login prompt - temp messages
Login banner is shown before login prompt AFTER MOTD banner - perm messages
Exec banner is displayed after login
Here is how you set up each. Note you need to enter a delimiter character, here % is used. Notice how you can put in line breaks, if needed:

SW1(config)# banner %
Enter TEXT message. End with the character '%'. (MOTD) Tuesday is timesheet day!
Don't forget to submit your hours today! %
SW1(config)# banner login %
Enter TEXT message. End with the character '%'. (Login) Unauthorized Access Prohibited! All activity is logged!
%
SW1(config)# banner exec %
Enter TEXT message. End with the character '%'. (Exec) Tuesday is timesheet day!
Don't forget to submit your hours today!

Here is the short version of doing everything as more of a checklist:

```
enable password mypassword
enable secret mysecret

line aux 0
login
password mypassword
logging synchronous
exec-timeout 10 10

line console 0
login
password mypassword
logging synchronous
exec-timeout 10 10

line vty 0 15
login
password mypassword
logging synchronous
exec-timeout 10 10

service password-encryption
hostname YourHostname
ntp server time-c.nist.gov version [number]
no ip lookup
no logging console

ip domain-name mydomain_name.com
username janicel password bones215
username jamesk password spock314
ip domain-name mydomain_name.com
crypto key generate rsa
        The name for the keys will be: myusername@mydomain_name.com  <--- match what you put in earlier
        How many bits in the modulus [512]: 2048
ip ssh version 2

In "line vty 0 15", "line aux 0" and "line console 0" configurations:
login local
transport input ssh   <------or "all" to allow telnet

Finally, be sure to check out your work and verify: type the global command "show ip ssh"
[you should also be able to log in with ssh -l username <ipaddress>]

banner %
banner login %
banner exec %
```

"Show" commands:

A. Show interface commands- differences in output and their meaning
 - sh int, sh ip int,- output fields and meaning; basic interface commands
B. Other show commands (arp, mac-addresses, NAT)

C. CDP
D. show vlan, sh trunk,
E. show route stuff

How to read "show interface" variants
show interfaces [type,#] - interface status, settings, and counters.
show interfaces description - one line per int, two-item status, and set description
show interfaces [type,#] status - status, settings, speed, duplex, **status code**, autonegotiation
show ip interface - shows more detailed layer 3 info on interfaces, IP addresses, access lists, etc
show ip interface brief - quick overview of which interfaces are configured with IP addresses, status, etc

About interface states [description vs status code] -serial ports (WAN) are different

Layer1/Layer2 Status	Status code	Description
Admin Down/Down	disabled	Shutdown command shut off interface
Down/ Down	notconnect	bad/wrong*/no cable; speed mismatch; other end is off or shutdown.
Up/ Down	notconnect	Shouldn't be seen on Eth. See below for serial.
Down/ Down	err-disabled	Port-security disabled: shutdown + no shutdown
Up/ Up	connected	

* need a crossover cable?

Up/Down Layer 2 issues for serial links:
keepalive disabled (HDLC - down on one end, up on the other)
mismatched encapsulation (might flicker up-down)
PAP/CHAP authentication fail - down both ends

Issues Related to Speed and Duplex
Speed mismatch - Interface status will be notconnect or down/down
Duplex mismatch - Performance counters will show problems on half-duplex end of the link
Identifying Duplex Mismatch Problems
show interfaces on each end of link to confirm settings
Watch for counter increases (runts, collisions, and late collisions)
Default Duplex Settings
If speed is 10 or 100 Mbps, default to half-duplex
If speed is 1000 Mbps, default to full-duplex

Here is the effect of hard coding the duplex/speed on one end of the link. Bad settings for a GigE interface. See how this lists on this end as autoconfigured? It just went along with what the other end said it was:

SW1# show interfaces gi0/1 status

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi0/1	Link to SW2	connected	trunk	a-half	a-100	10/100/1000BaseTX

Switches do not have a single command to disable IEEE autonegotiation; however, configuring the speed and duplex commands on one end has the side effect of disabling autonegotiation

Duplex mismatches are harder to spot. Look at the show interfaces command and watch for the runts, collisions, and late collisions counters.

Speed mismatch: If the endpoints on an Ethernet link use different speeds, both should show the interface status as notconnect or down/down.

Duplex mismatch: If the endpoints use the same speed, but different duplex settings, the interfaces will come up, but other performance counters will show problems on the half- duplex end of the link.

Use commands like **show interfaces** on each end of the link to confirm the duplex setting on each end. Watch for increases to certain counters on half-duplex interfaces. The runts, collisions, and late collision counters occur when the other device uses full duplex. (Note that these counters can also increment when legitimate collisions occur as well.)

SW1# show interfaces f0/11 status

Port	Name	Status	Vlan	Duplex	Speed	Type	
Fa0/11	link to PC1		connected		3	**a-full**	**100** 10/100BaseTX

SW1# show interfaces f0/12 status

Port	Name	Status	Vlan	Duplex	Speed	Type	
Fa0/12	link to PC2		connected		3	**a-full**	**a-100** 10/100BaseTX

SW1# show interfaces fa0/12 <--- doesn't show us if autoconfig'd like "status" does

Reading the output, spotting errors on interfaces:

http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1904.html
http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1915.html

Router# show interface fastethernet 0/1

```
Fast Ethernet0/1 is administratively down, line protocol is down
  Hardware is cxBus Fast Ethernet, address is 0000.0c35.dc16 (bia 0000.0c35.dc16)
  Internet address is 10.1.0.64 255.255.0.0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, half-duplex, RJ45 (or MII)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input never, output 2:03:52, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 1 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     5 packets output, 805 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets, 0 restarts
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Explaining the fields above

255/255 means that reliability is perfect, and load is 1/255, meaning no load.
Bandwidth is 100000 Kbit, 100,000,000, which is 100 Mbits per second, or FastEthernet. Gigabit would be 1000000. Default for serial links: MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec

Last input/ output - h:m:s since the last packet was successfully transmitted. Tells when a dead interface failed. Not updated with fast switched packets.
output hang - h:m:s since interface was last reset because transmission took too long. If hrs exceeds 24 hrs, days and hours is printed. If that field overflows, asterisks are printed.

```
     0 packets input, 0 bytes, 0 no buffer
```

Compare input "no buffer" with ignored count 2 lines down. Broadcast storms and noise bursts on serial lines are often responsible for no input buffer events.

runts, giants - Packets discarded because they are outside the min/max packet size of the medium. (any Ethernet packet <64 bytes is a runt, >1518 bytes is a giant). Runts almost always caused by collisions- if ruled out are the result of underruns or bad software on a NIC

CRC- A high count is usually noise in the network, the result of collisions, or faulty equipment transmitting bad data. Check output errors, number of collisions
frame - # of packets having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun - # of times input rate exceeded the capability to handle the data to hand to buffer
ignored - # of packets ignored by the interface because it's interface ran low on internal buffers (not the system buffers mentioned as "input buffer"). Often broadcast storms and bursts of noise
abort - Number of packets whose receipt was aborted. On a serial interface, an illegal sequence of 1 bit - usually indicates a clocking problem

watchdog - # of times watchdog receive timer expired (when receiving a packet with length over 2048 bytes
multicast - Number of multicast packets received.

input packets with dribble condition detected - frames slightly too long, but accepted anyway

packets output - Total # of messages transmitted; bytes - # of bytes, including data and MAC encapsulation, transmitted by the system.
underruns - Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.

Output errors, number of collisions aren't an indication of a problem, but changes in the number may be an indication of a problem.

output errors - Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. May not look like it adds up right - datagrams may have more than one error, and others may have errors that don't fall into any of the specific categories.

collisions: if they exceed the baseline, it could be a defective or ill behaving device, sending jabber (random or garbage data). A time domain reflectometer or TDR could be used to find unterminated Ethernet cabling, which could be reflecting signals and causing collisions. . If the number of collisions is constant, consistent, then the CRC errors could be caused by excessive noise.

<u>For noise and collisions: Use show interfaces ethernet command:</u>
Excessive noise - determine the status of the router's Ethernet interfaces. The presence of many CRC errors but not many collisions is an indication of excessive noise. Check cables to determine whether any are damaged or wrong type. Look for badly spaced taps causing reflections.
Excessive collisions - check the rate of collisions. The total number of collisions with respect to the total number of output packets should be around 0.1 percent or less. Use a TDR to find any unterminated Ethernet cables. Look for a jabbering transceiver attached to a host. (This might require host-by-host inspection or the use of a protocol analyzer.)

interface resets - Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

restarts - Number of times a Type 2 Ethernet controller was restarted because of errors.
babbles - The transmit jabber timer expired.

Late collisions occur after the first 512 bits of data (preamble) are transmitted. Possibilities are incorrect cabling (cable segments are too long for the speed), a noncompliant number of hubs, or a bad NIC. Typically detected using protocol analyzers and also verifying cabling distances and physical layer requirements.

deferred - Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier - Number of times the carrier was lost during transmission.
no carrier - Number of times the carrier was not present during the transmission.

Examples of the interface show commands:

SW1# show interfaces fa0/12 <--- doesn't show us if autoconfig'd like "status"
FastEthernet0/12 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 1833.9d7b.0e8c (bia 1833.9d7b.0e8c)
  Description: link to PC2
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1453 packets input, 138334 bytes, 0 no buffer
     Received 1418 broadcasts (325 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 325 multicast, 0 pause input
     0 input packets with dribble condition detected
     33640 packets output, 2651335 bytes, 0 underruns
0 output errors, **0 collisions**, 1 interface resets
0 unknown protocol drops
0 babbles, **0 late collision**, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

#show interface status

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/0/1		connected	100	a-full	a-1000	10/100/1000BaseTX
Gi1/0/2		connected	100	a-full	a-1000	10/100/1000BaseTX
Gi1/0/3		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/4		notconnect	1	auto	auto	10/100/1000BaseTX

#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	172.16.0.254	YES	NVRAM	up	up
Vlan2	unassigned	YES	NVRAM	up	up
Vlan3	192.168.3.1	YES	NVRAM	up	up
GigabitEthernet1/0/1	unassigned	YES	unset	up	up

Show ip interfaces will predicably be more specific to layer 3 info:
R1-Tester#show ip interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.10.10.2/24
  Broadcast address is 255.255.255.255

```
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP CEF turbo switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled

R1#show interface capabi Fa0/1
FastEthernet0/1
  Model:                 WS-C2950-12
  Type:                  10/100BaseTX
  Speed:                 10,100,auto
  Duplex:                half,full,auto
  UDLD:                  yes
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(none),tx-(none)
  Fast Start:            yes
  CoS rewrite:           yes
  ToS rewrite:           yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            Yes
  Dot1x:                 Yes
```

Finally, there are plenty of interface types you can specify/ configure:

```
Interface (specific) configuration mode:
Switch(config)#interface ?
  Async Async interface
```

```
  BVI     Bridge-Group Virtual Interface
  CTunnel         CTunnel interface
  Dialer  Dialer interface
  FastEthernet    FastEthernet IEEE 802.3
  Filter  Filter interface
  Filtergroup     Filter Group interface
  GigabitEthernet         GigabitEthernet IEEE 802.3z
  Group-Async     Async Group interface
  Lex     Lex interface
  Loopback        Loopback interface
  Null    Null interface
  Port-channel    Ethernet Channel of interfaces
  Portgroup       Portgroup interface
  Pos-channel     POS Channel of interfaces
  Tunnel          Tunnel interface
  Vif     PGM Multicast Host interface
  Virtual-Template        Virtual Template interface
  Virtual-TokenRing       Virtual TokenRing
  Vlan    Catalyst Vlans
  fcpa    Fiber Channel
  range   interface range command
```

B. Other show commands

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.3.123          21   001c.23f9.d931  ARPA   FastEthernet0/0
Internet  192.168.3.75            7   0025.648f.c6be  ARPA   FastEthernet0/0
Internet  192.168.3.39            -   001e.7ae0.4740  ARPA   FastEthernet0/0
```

```
#show mac-address-table
          Mac Address Table
 -------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
All     0100.0ccc.cccd    STATIC      CPU
All     0180.c200.0000    STATIC      CPU
```

show mac-address-table dynamic - to see known MACs - only dynamically added entries
show mac address-table [mac] [dynamic | multicast | static] [interface slot / port] [vlan vlan-id]
(first version was used until IOSv12.1, mac address-table is more recent; many support either)
[(a lot of MACs may be listed for CPU use- for hidden processes (CGMP, PAGP, GARP, CDP, VTP, DTP)]

The forward-filter table is often called the content addressable memory (CAM) table, even though CAMs were replaced with ASICs a long time ago. CAMs were mostly used in bridges.

```
2911#show ip nat translations tcp | include 6.6
tcp 202.130.101.34:36662  192.168.6.1:36662     198.20.8.246:443      198.20.8.246:443
tcp 202.130.101.34:50000  192.168.6.6:50000     ---                   ---
tcp 202.130.101.34:64694  192.168.6.20:64694    108.168.151.6:80      108.168.151.6:80
tcp 202.130.101.34:50626  192.168.6.53:50626    122.224.118.210:80    122.224.118.210:80
```

Categories
- spanning tree
- ports and port security
- vlans
- routing tables
- neighbors

Separate commands sections: routing, switching (STP), port security
(separate from explanation of what things are)

terminal monitor - EXEC command - send a copy of all syslog including debug msgs, to the issuer.
logging synchronous, no logging

end, Ctrl-Z
Exits config mode and goes back to enable mode from any of the configuration submodes.

exit - config mode - just moves back to the next higher mode in configuration mode.
quit - an EXEC command that disconnects the user from the CLI session.
reload - Enable mode EXEC command that reboots the switch or router.

debug all, no debug all, undebug all
EXEC command to disable all currently enabled debugs.

show startup-config - lists the contents of startup config (initial config) file in NVRAM.
show running-config - lists the contents of currently active config in RAM (DRAM)

2911#show control-plane host open-ports
Active internet connections (servers and established)

Prot	Local Address	Foreign Address	Service	State
tcp	*:22	*:0	SSH-Server	LISTEN
tcp	*:23	*:0	Telnet	LISTEN
tcp	*:22	192.168.6.20:59831	SSH-Server	ESTABLIS
tcp	*:22	60.11.255.77:37264	SSH-Server	ESTABLIS
tcp	*:443	*:0	HTTP CORE	LISTEN
tcp	*:443	*:0	HTTP CORE	LISTEN
udp	*:61934	*:0	IP SNMP	LISTEN
udp	*:67	*:0	DHCPD Receive	LISTEN
udp	*:161	*:0	IP SNMP	LISTEN
udp	*:162	*:0	IP SNMP	LISTEN
udp	*:1975	*:0	IPC	LISTEN

Cisco Discovery Protocol helps verify information in network diagram
Even though CDP detail can give IP addresses, CDP is data link protocol on layer 2.
show cdp - shows if CDP is enabled globally, lists the default update and holdtime timers.
show cdp interface [type,#] - if CDP is enabled, update and holdtime timers on interfaces.
show cdp traffic - global stats for CDP advertisements sent and received.
---
show cdp neighbors [type,#] - One line for each neighbor (interface)
show cdp neighbors detail - Large set of info (approx 15 lines) for every neighbor.
show cdp entry * - exactly the same as "sh cdp neighbors detail"
show cdp entry name - same info as show cdp neighbors detail, only for the named neighbor.
---

cdp run/ no cdp run - Global commands that enable or disable CDP for the entire switch or router.
cdp enable/ no cdp enable - enable and disable, respectively, CDP for a particular interface.
Disable CDP on any machine on an untrusted network (exposed to the internet)

SW2# **show cdp neighbors**
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
SW1	Gig 0/2	154	S I	WS-C2960	Gig 0/1
SW3	Gig 0/1	170	S I	WS-C2960	Gig 0/2
R1	Fas 0/10	134	R S I	CISCO2901	Gig 0/1

SW1# **show cdp neighbors**
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
SW2	Gig 0/1	170	S I	WS-C2960-	Gig 0/2
SW3	Gig 0/2	167	S I	WS-C2960-	Gig 0/1

SW2# **show cdp entry R1**

Device ID: R1
Entry address(es):
IP address: 2.2.2.9
Platform: Cisco CISCO2901/K9 Capabilities: Router Switch IGMP
Interface: FastEthernet0/9 Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 148 sec
Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team
advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):

SW3# **show cdp neighbors**
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
SW1	Gig 0/1	167	S I	WS-C2960-	Gig 0/2
SW2	Gig 0/2	176	S I	WS-C2960-	Gig 0/1

Configuring Switchports for Trunking and Access, plus related display commands
switchport mode {access | trunk}
switchport access vlan vlan-number -- defines the VLAN interface resides in.
switchport trunk encapsulation [dot1q | isl] -- almost always use dot1q - you may have to do this first.
switchport mode dynamic auto | dynamic desirable
dynamic auto - becomes a trunk if the neighboring interface is set to trunk or desirable
dynamic desireable - becomes a trunk if neighboring interface is set to ANY trunk mode *(default!)*
switchport nonegotiate - prevents generating DTP frames, or converting dynamically to anything
switchport trunk allowed vlan 4,6,12,15 --this should eliminate vlans not specifically listed
switchport trunk allowed vlan [remove 4-8 | all | none]
no switchport trunk native vlan
no switchport trunk vlan 4

show interfaces [type,#] switchport - settings, status, trunking, access/voice/native VLAN
show interfaces [type,#] trunk - lists info on trunks (or the specific trunk) and the VLANs
show vlan brief, show vlan - each VLAN and all assigned interfaces, but no trunks!
show vlan [vlan] - access and trunk ports in the VLAN.
show vtp status - VTP mode, configuration and status info

Port Security

no ip http server
no service tcp-small-servers
no service udp-small-servers
#(config-line)access-class 3 in <---- add an access list to a VTY = "class" instead of "group" for interfaces

As soon as you enable port-security, it defaults to violation shutdown and a maximum of 1 MAC address.
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address aa.bb.cc.dd.ee.ff [sticky, often used with maximum]
switchport port-security maximum <value>
    the max number of MAC addresses that can be assigned - default is one.
    A max value can also be set if it's a switch connected - receiving frames for multiple MACs
switchport port-security violation {protect | restrict | shutdown}
        protect: unauthorized frames would just be dropped
        restrict: authorized frames would be dropped and violations count toggled
        shutdown: disable the interface (err-disabled - this is the default action)
show port-security interface

To open an interface shut down with port-security, you first issue "shutdown", then "no shutdown"

Switch#sh ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.255.8	YES	DHCP	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down

The above output shows the default routed port found on all Cisco switches (VLAN 1), plus nine switch FastEthernet interface ports, with one port being a Gigabit Ethernet port used for uplinks to other switches.

A 2800 ISR Cisco routers with two FastEthernet interfaces along with two serial WAN interfaces (ISR is "Integrated Svc Router"):

Router>sh ip int brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.255.11	YES	DHCP	up	up
FastEthernet0/1	unassigned	YES	unset	administ. down	down
Serial0/0/0	unassigned	YES	unset	administ. down	down
Serial0/1/0	unassigned	YES	unset	administ. down	down

The show protocols, show controllers, setting the DTE Clock rate on DCE end

Remember that a DTE serial cable acts as a straight-through cable, and does not swap the transmit and receive pair, while the DCE cable does swap the pairs like a crossover. When they connect together (DTE=male, DCE=female) between a router and a DSU/CSU, the DCE end (DSU/CSU) provides the clock rate.
Some versions of IOS will automatically implement a default clock rate 2000000 command on serial interfaces that have a DCE cable connected to them. While helpful, this speed might be too high for some types of back-to-back serial cables, so consider using a lower speed in lab.

```
Router#sh protocols
Global values:
  Internet Protocol routing is enabled
Ethernet0/0 is administratively down, line protocol is down
Serial0/0 is up, line protocol is up
  Internet address is 100.30.31.5/24
Serial0/1 is administratively down, line protocol is down
Serial0/2 is up, line protocol is up
  Internet address is 100.50.31.2/24
Loopback0 is up, line protocol is up
  Internet address is 100.20.31.1/24

R1#sh controllers s0/0
HD unit 0, idb = 0x1229E4, driver structure at 0x127E70
buffer size 1524 HD unit 0,
DTE V.35 clocks stopped
cpb = 0xE2, eda = 0x4140, cda = 0x4000

R1#sh ip interface s0/0
Serial0/0 is up, line protocol is down
  Internet address is 192.168.10.2/24
```

Broadcast address is 255.255.255.255

No CSU/DSU is connected to provide clocking for R1. This means the DCE end of the cable will be providing the clock rate- in this case, the R2 router. The show ip interface indicates that the interface is up but the protocol is down, which means that no keepalives are being received from the far end. In this example, the likely culprit is the result of bad cable, or simply the lack of clocking

```
R2(config)#int s0/0/0
R2(config-if)#clock rate ?
        Speed (bits per second)
  1200
            (cut) ...
  8000000
  <300-8000000>    Choose clockrate from list above
R2(config-if)#clock rate 1000000

R1#sh controllers serial 0/0
HD unit 0, idb = 0x1229E4, driver structure at 0x127E70
buffer size 1524 HD unit 0, V.35 DTE cable

R2#sh controllers serial 0/1
HD unit 1, idb = 0x12C174, driver structure at 0x131600
buffer size 1524 HD unit 1, V.35 DCE cable
```
