Cheatography

CISCO switching and routing config Cheat Sheet

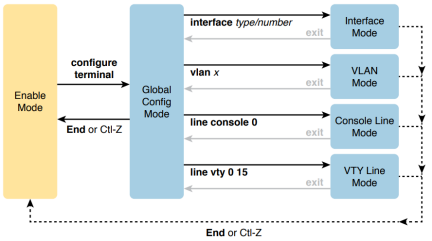
by tortilladepatatas via cheatography.com/195367/cs/40911/

IOS modes

Prompt	Name of mode	Command to access
Switch>	User exec	**disable**
Switch#	Privileged exec	**enable**
Switch(config)#	Global Config	**configure terminal**
Switch(config-if)#	Interface	**line console 0** **line vty 0 15** (telnet)
Switch(config-line)#	Line	**interface** *type number*
Switch(vlan)#	VLAN	**vlan** *number*

We can exit all modes with **exit** (immediate previous one) or **end** (straight to privileged)

Config Modes Diagram



Key Sequences for Command Edit and Recall

Keyboard Command	What Happens
Up arrow or Ctrl+P	This displays the most recently used command. If you press it again, the next most recent command appears, until the history buffer is exhausted. (The P stands for previous.)
Down arrow or Ctrl+N	If you have gone too far back into the history buffer, these keys take you forward to the more recently entered commands. (The N stands for next.)
Left arrow or Ctrl+B	This moves the cursor backward in the currently displayed command without deleting characters. (The B stands for back.)
Right arrow or Ctrl+F	This moves the cursor forward in the currently displayed command without deleting characters. (The F stands for forward.)
Backspace	This moves the cursor backward in the currently displayed command, deleting characters.

If you are used to general console interactions in linux is pretty similar

Cisco IOS Software Command Help

What You Enter	The help you get
?	Provides help for all commands available in this mode.
command ?	With a space between the command and the ?, the switch lists text to describe all the first parameter options for the command.
com?	Lists commands that start with com.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Cisco IOS Software Command Help (cont)

command parm?	Lists all parameters beginning with the parameter typed so far. (Notice that there is no space between parm and the ?.)
command parm<Tab>	Pressing the Tab key causes IOS to spell out the rest of the word, assuming that you have typed enough of the word so there is only one option that begins with that string of characters.
command parm1 ?	If a space is inserted before the question mark, the CLI lists all the next parameters and gives a brief explanation of each.

It's good practice to **always use ? when you are not sure** of what you are doing to prevent launching a successfully format-wise but that doesn't do what we intend to do because we haven't explored all possibilities!

CISCO IOS config files

Configuration Filename	Purpose	Where It Is Stored
sartup-config	Stores the initial configuration used anytime the switch reloads Cisco IOS.	NVRAM
running-config	Stores the currently used configuration commands. This file changes dynamically when someone enters commands in configuration mode.	RAM
vlan.dat	Stores information related to VLAN	Flash

Memory types: **RAM** (Working Memory and Running Configuration), **Flash** (Cisco IOS Software / Images), **ROM** (Bootstrap Program before Cisco IOS takes over), **NVRAM** (Startup Configuration)

copy running-config startup-config saves active config replacing startup **copy startup-config running-config** merges startup file with the currently active file in RAM

You can also **write** and **erase** config files

Switching Logic Actions

Deciding when to **forward a frame or when to filter a frame**, based on the destination MAC address (using the dynamically built MAC)

Preparing to **forward frames by learning MAC addresses** by examining the source MAC address of each frame received by the switch (on cases where **the forward MAC isn't in the table** the switch *floods* the ports like it was a broadcast in order to find a response and fill the table to later tries)

Preparing to **forward only one copy of the frame to the destination** by creating a (Layer 2) loop-free environment with other switches by using **Spanning Tree Protocol** (since loops can be fatal in the previous flooding mechanism). This is achieved by **blocking some ports from forwarding frames** so that only one active path exists between any pair of LAN segments. The downside is that it makes harder load balancing since redundant connections can be useful for that purpose.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Switch Verification Commands

Display interface status and configuration.	S1# **show interfaces** *interface-id*
Display current startup configuration.	S1# **show startup-config**
Display current operating configuration.	S1# **show running-config**
Display information about the flash file system.	S1# **show flash:**
Display status of system hardware and software.	S1# **show version**
Display a history of commands entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip** *interface-id*
Display the MAC address table.	S1# **show mac-address-table [dynamic|static] [vlan** *vlan_id*| **interface** *interface_id* **| adress** *MAC_adress***]**
Lists any information the switch acquires as a DHCP client. This includes IP address, subnet mask, and default gateway information.	S1# **show dhcp lease**
Lists the public and shared key created for use with SSH using the crypto key generate rsa global configuration command.	S1# **show crypto key mypubkey rsa**
Lists status information for the SSH server, including the SSH version.	S1# **show ip ssh**
Lists the switch's setting for its IPv4 default gateway.	S1# **show ip default-gateway**

MAC related command reference

Command	Purpose
show mac address-table	Shows all MAC table entries of all types
show mac address-table dynamic	Shows all dynamically learned MAC table entries
show mac address-table dynamic [vlan *vlan-number***] [interface** *interface-id***] [address** *mac-address***]**	Shows all dynamically learned MAC table entries containing any of the data depicted
show mac address-table count	Shows the number of entries in the MAC table and the total number of remaining empty slots in the MAC table
show mac address-table aging-time	Shows the global and per-VLAN aging timeout for inactive MAC table entries
clear mac address-table dynamic	Empties the MAC table of all dynamic entries
clear mac address-table dynamic [vlan *vlan-number***] [interface** *interface-id***] [address** *mac-address***]**	Clears (removes) dynamic MAC table entries: either all (with no parameters), or a subset based on VLAN ID, interface ID, or a specific MAC address

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Configure the Switch Management Interface

Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI	S1(config)# **interface vlan 1**
Configure the management interface IP address.	S1(config-if)# **ip address 192.168.1.200 255.255.255.0**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to privileged config mode.	S1(config-if)# **exit**
Set up the default gateway also in order to have internet connection	S1(config)# **ip default-gateway 192.168.1.1**
Return to privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

This process can also be carried out with the command **ip address dhcp** using then the DHCP protocol in order to assign it's ip.

Login Security Commands

Command	Purpose
line console 0	Changes the context to console configuration mode.
line vty *1st-vty last-vty*	Changes the context to vty configuration mode for the range of vty lines listed in the command.
login	Console and vty configuration mode. Tells IOS to prompt for a password.
password *pass-value*	Console and vty configuration mode. Lists the password required if the *login* command (with no other parameters) is configured.
login local	Console and vty configuration mode. Tells IOS to prompt for a username and password, to be checked against locally configured **username** global configuration commands on this switch or router.
username *name* **secret** *pass-value*	Global command. Defines one of possibly multiple usernames and associated passwords, used for user authentication. Used when the **login local** line configuration command has been used.
crypto key generate rsa [modulus *360..2048* **]**	Global command. Creates and stores (in a hidden location in flash memory) the keys required by SSH.
transport input {telnet | ssh | all | none}	vty line configuration mode. Defines whether Telnet/SSH access is allowed into this switch. Both values can be configured on one command to allow both Telnet and SSH access (the default).

In case you need to set up security to your switch connection

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Cisco Switch Port Configuration

Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode	S1(config)# **interface fastethernet 0/1**
Configure the interface duplex mode.	S1(config-if)# **duplex full**
Configure the interface speed	S1(config-if)# **speed 100**
Add some useful description please!	S1(config-if# **description Printer on 3rd floor, Preset to 100/full**
Return to general config	S1(config-if)# **exit**
Now we will configure a range	S1(config)# **interface range FastEthernet 0/11 - 20**
And add some useful information for good measure	S1(config-if-range)# **description end-users connect here**
Return to privileged EXEC mode	S1(config-if-range)# **^Z**
Save the running config to the startup config	S1# **copy running-config startup-config**

Since **Mismatched settings for the duplex mode and speed** of switch ports can cause **connectivity issues**.

We can use **shutdown** to close interfaces.

We can create virtual interfaces called subinterfaces. Those will help us when working with different logical interfaces within the same physical one. We address them like this **fa0/0.<id>**

Cisco Switch Auto-MDIX Commands

Enter global configuration mode.	**S1#** configure terminal
Enter interface configuration mode.	**S1(config)#** interface fastethernet 0/1
Configure the interface to automatically negotiate the duplex mode with the connected device.	**S1(config-if)#** duplex auto
Configure the interface to automatically negotiate speed with the connected device.	**S1(config-if)#** speed auto
Enable auto-MDIX on the interface.	**S1(config-if)#** mdix auto
Return to privileged EXEC mode.	**S1(config-if)#** end
Save the running config to the startup config.	**S1#** copy running-config startup-config

With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically corrects for any incorrect cabling.

To check we can use: `show contro llers ethern et- con troller fa 0/1 phy | include Auto-MDIX`

Verify the Status of a Switch Interface

Line Status	Protocol Status	Interface status	Typical Root Case
administr-atively down	down	disabled	The shutdown command is configured on the interface.
down	down	notconnect	No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off, (b) shutdown, or (c) error disabled.
up	down	notconnect	Not expected on LAN switch physical interfaces.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Verify the Status of a Switch Interface (cont)

down	down (err-disabled)	err-disabled	Port security has disabled the interface.
up	up	connected	The interface is working.

Possible problems with interface status

If the **interface is up and the line protocol is down**, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.

If the **line protocol and the interface are both down**, a cable is not attached or some other interface problem exists. For example, in a back-to-back connection (a connection where the transmitter of one device connects directly to the receiver of another device without a transmission media between the two devices), one end of the connection may be administratively down.

If the **interface is administratively down**, it has been manually disabled (the shutdown command has been issued) in the active configuration.

Error codes in show interfaces

Code	Explanation
Runts	Frames that did not meet the minimum frame size requirement (64 bytes, including the 18-byte destination MAC, source MAC, type, and FCS). Can be caused by collisions.
Giants	Frames that exceed the maximum frame size requirement (1518 bytes, including the 18-byte destination MAC, source MAC, type, and FCS).
Input Errors	A total of many counters, including runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
CRC	Received frames that did not pass the FCS math; can be caused by collisions.
Frame	Received frames that have an illegal format, for example, ending with a partial byte; can be caused by collisions.
Packets Output	Total number of packets (frames) forwarded out the interface.
Output Errors	Total number of packets (frames) that the switch port tried to transmit, but for which some problem occurred.
Collisions	Counter of all collisions that occur when the interface is transmitting a frame.
Late Collisions	The subset of all collisions that happen after the 64th byte of the frame has been transmitted. (In a properly working Ethernet LAN, collisions should occur within the first 64 bytes; late collisions today often point to a duplex mismatch.)

VLANs Definition and Benefits

Essentially they are **individual broadcast domains** created by the switch, which are called virtual LANs (VLAN). In order to forward packs to other VLANs we need **routing**.

Benefits of VLANs

To **reduce CPU overhead** on each device, improving host performance, by reducing the number of devices that receive each broadcast frame

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

VLANs Definition and Benefits (cont)

To **reduce security risks** by reducing the number of hosts that receive copies of frames that the switches flood (**broadcasts, multicasts, and unknown unicasts**)

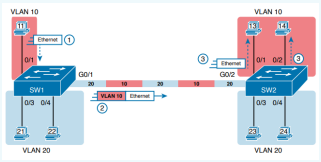
To improve security for hosts through the application of **different security policies per VLAN**

To create more **flexible designs** that **group users** by department, or by groups that work together, instead of by physical location

To solve problems more quickly, because the **failure domain for many problems is the same set of devices as those in the same broadcast domain**

To **reduce the workload for the Spanning Tree Protocol** (STP) by limiting a VLAN to a single access switch

VLAN Trunking



The use of **trunking** allows switches to **forward frames from multiple VLANs over a single physical connection** by adding a small header to the Ethernet framex.

802.1Q inserts an extra 4-byte 802.1Q VLAN header into the original frame's Ethernet header (12 bits vlan id, flag, priority and type)

Trunkind Administrative Mode Options

Common Option	Description
access	Always act as an access (nontrunk) port.
trunk	Always act as trunk port.
dynamic desirable	Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking
dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking

You can change the mode with **switchport mode trunk**.

For switches that support both ISL and 802.1Q you can use the command **switchport trunk encapsulation {fot1q | isl | negotiate}** interface subcommand to allow Dynamic Trunking Protocol to negotiate the type. Though Cisco recommends disabling trunk negotiation on most ports for better security.

You can also use **show interfaces trunk** to see the trunked interfaces

VLAN Configuration Reference

Command	Description
vlan *vlan-id*	Global config command that both creates the VLAN and puts the CLI into VLAN configuration mode
name *vlan-name*	VLAN subcommand that names the VLAN
[no] shutdown	VLAN mode subcommand that enables (no shutdown) or disables (shutdown) the VLAN
[no] shutdown vlan *vlan-id*	Global config command that has the same effect as the [no] shutdown VLAN mode subcommands
vtp mode {server | client | transparent | off}	Global config command that defines the VTP mode
switchport mode {access | dynamic {auto | desirable} | trunk}	Interface subcommand that configures the trunking administrative mode on the interface
switchport access vlan *vlan-id*	Interface subcommand that statically configures the interface into that one VLAN

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

VLAN Configuration Reference (cont)

switchport trunk encapsulation {dot1q | isl | negotiate}	Interface subcommand that defines which type of trunking to use, assuming that trunking is configured or negotiated
switchport trunk native vlan *vlan-id*	Interface subcommand that defines the native VLAN for a trunk port
switchport nonegotiate	Interface subcommand that disables the negotiation of VLAN trunking
switchport voice vlan *vlan-id*	Interface subcommand that defines the voice VLAN on a port, meaning that the switch uses 802.1Q tagging for frames in this VLAN
switchport trunk allowed vlan {add | all | except | remove} *vlan-list*	Interface subcommand that defines the list of allowed VLANs
show interfaces *interface-id* **[switchport|-trunk]**	Lists information about any interface regarding administrative settings and operational state / Lists information about all operational trunks

Creating a VLAN

Command	Meaning
SW1(config)# **vlan 2**	Create the VLAN and to move the user into VLAN configuration mode.
SW1(config-vlan)# **name Hugos-vlan**	Create a name for the VLAN. If not configured, the VLAN name is VLANZZZZ, where ZZZZ is the four-digit decimal VLAN ID.
SW1(config-vlan)# **exit**	Go back
SW1(config)# **interface range fastet-hernet 0/13 - 14**	Used to move into interface configuration mode for each desired interface.
SW1(config-if)# **switchport access vlan 2**	Specify the VLAN number associated with that interface. Using this on a not yet created vlan **will create one**, be careful with this
SW1(config-if)# **switchport mode access**	Make this port always operate in access mode (that is, to not trunk)
SW1(config-if)# **end**	Go back
SW1# **show vlan brief**	Show what we have created

Configuration Command Reference

Command	Description
spanning-tree mode {pvst | rapid-pvst | mst}	Global configuration command to set the STP mode.
spanning-tree [*vlan vlan-number* **] root primary**	Global configuration command that changes this switch to the root switch. The switch's priority is changed to the lower of either 24,576 or 4096 less than the priority of the current root bridge when the command was issued.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

Configuration Command Reference (cont)

spanning-tree [*vlan vlan-number* **] root secondary**	Global configuration command that sets this switch's STP base priority to 28,672.
spanning-tree vlan *vlan-id* **priority** *priority*	Global configuration command that changes the bridge priority of this switch for the specified VLAN.
spanning-tree [vlan *vlan-number* **] cost** *cost*	Interface subcommand that changes the STP cost to the configured value.
spanning-tree [vlan *vlan-number* **] port-priority** *priority*	Interface subcommand that changes the STP port priority in that VLAN (0 to 240, in increments of 16).
channel-group *channel-group-number* **mode {auto | desirable | active | passive | on}**	Interface subcommand that enables EtherChannel on the interface.
show spanning-tree	Lists details about the state of STP on the switch, including the state of each port.
show spanning-tree vlan *vlan-id*	Lists STP information for the specified VLAN.
show etherchannel [*channel-group-number* **] {brief | detail | port | portchannel | summary}**	Lists information about the state of EtherChannels on this switch.

Command Reference for Routing (Basic)

Command	Description
Interface *type number*	Global command that moves the user into configuration mode of the named interface.
ip address *address mask*	Interface subcommand that sets the router's IPv4 address and mask.
show interfaces [*type number*]	Lists a large set of informational messages about each interface, or about the one specifically listed interface.
show ip interface brief	Lists a single line of information about each interface, including the IP address, line and protocol status, and the method with which the address was configured (manual or Dynamic Host Configuration Protocol [DHCP]).
show protocols [*type number*]	Lists information about the listed interface (or all interfaces if the interface is omitted), including the IP address, mask, and line/protocol status.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com