CCNA Switch command cheat-sheet

Useful command collection for Cisco Switches. Based on Cisco Networking Academy CCNA version 6 and version 7 course material, and recommended for CCNA exam preparation.

Table of contents

Before we start: Configuration modes

Three basic configuration modes we MUST be familiar with already (you will see them below, a lot).

Mode (prompt)	Device configuration mode	"Mode change" command (current -> next)
`S1>`	EXEC mode	type `enable` to pass to next mode
`S1#`	Privileged EXEC mode	type `configure terminal` to pass to next mode
`S1(config)#`	Global congiguration mode	N/A

Common abbreviations to the commands above (separated by commas):

```
en, ena
conf t, config term
```

Important `show` commands:

Note that these commands are executed on privileged EXEC mode (`S1#` prompt).
You can execute them from global configuration mode (`S1(config)#` prompt) by adding the `do` keyword before the command.
example:
`S1(config)#do show ip interface brief`

Command	Description
`S1#show running-config`	N/A
`S1#show history`	
`S1#show interface [int-id]`	useful to detect errors or verify packets are being sent and received
`S1#show mac address-table`	

Command	Description
`S1#show port-security`	displays Port Security configuration for all interfaces
`S1#show port-security interface [int-id]`	display Port Security configuration of an interface
`S1#show vlan`	
`S1#show vlan brief`	**only** displays VLANs, statuses, names, and assigned ports
`S1#show interface vlan [id]`	
`S1#show interfaces trunk`	

Filtering information from `show` commands:

Some commands, such as `show running-config`, generate multiple lines of output.

To filter output, you can use the *pipe* (`|`) character along with a **filtering parameter** and a **filtering expression**.

Filtering parameters	Effect
`section [filtering-expression]`	shows the section of the *filtering expression*
`include [filtering-expression]`	includes all lines of output that match the *filtering expression* **ONLY**
`exclude [filtering-expression]`	excludes all lines of output that match the *filtering expression*
`begin [filtering-expression]`	shows all the lines of output **beginning from** the line that matches the *filtering expression*

Usage:

Here's an example of the usage of filtering with a `show` command:

```
R1#show running-config | include line con
```

💡 ProTip: By default, the screen of output consists of 24 lines. Should you want to change the number of output lines displayed on the terminal screen, you can use the command: `R1# terminal length [number-of-lines]`
⚠️ Unfortunately, this command is NOT supported in Cisco Packet Tracer (tested on version 7.2.2).

Managing more than one interface at the same time

When we want to execute a sequence on commands on more than one port, selecting an interface range makes the job a lot easier.
Use: `S1(config)#interface range [typeModule/firstNumber]-[lastNumber]`

typeModules	some possible abbreviations
`FastEthernet`	`f, fa, ...`
`GigabitEthernet`	`g, gi, gig, ...`

Here's an example: `S1(config)#interface range f0/1-12`

Note that you can select multiple ranges on a single command.
Here's an example: `S1(config)#interface range f0/1-12, 15-24, g0/1-2`

You might need to use it frequently on scenarios where the following blocks of commands are used.

VLANs

Configuring VLANs

Command	Description
`S1(config)#vlan [vlan-ID]`	create VLAN and assign its VLAN number
`S1(config-vlan)#name [someName]`	assign a name to the VLAN

Now it is time to assign ports to the newly created VLAN

Command	Description
`S1(config)#interface [int-id]`	remember, `interface range` might be useful
`S1(config-if)#switchport mode access`	
`S1(config-if)#switchport access vlan [vlan-id]`	assign/change port VLAN

Deleting a VLAN

Command	Description
`S1(config)#no vlan [vlan-id]`	⚠️ deletes specified VLAN
`S1(config)#delete flash:vlan.dat`	⚠️ erases **the whole VLAN database**

Removing interface(s) from a VLAN

Command	Description
`S1(config)#interface [int-id]`	
`S1(config-if)#no switchport access vlan [vlan-id]`	remove the VLAN from the port

Know the difference!

> 💡 When a VLAN is deleted. Any switchport assigned to that VLAN **becomes inactive**
> 💡 On the other hand, when the `no switchport access vlan [vlan-id]` is executed on a switchport, the port will be returned to VLAN 1

Configuring IEEE 802.1q trunk links

Command	Description
`S1(config)#interface [int-id]`	
`S1(config-if)#switchport mode trunk`	
`S1(config-if)#switchport trunk native vlan [vlan-id]`	

Command	Description
`S1(config-if)#switchport trunk allowed vlan [vlan-list]`	**All** allowed VLAN IDs.
`S1(config-if)#switchport trunk allowed vlan remove [vlan-id]`	🚷 **PROHIBITS ONLY** the VLAN with the specified ID on the trunk interface

💡 Tip: You might also want to check out the router commands necessary for inter-VLAN-routing via Router-On-A-Stick

Dynamic Trunking Protocol (DTP)

This Cisco proprietary protocol contributes in the configuration of trunking interfaces between Cisco switches.

💡 Remember: The **default** configuration for interfaces on Cisco Catalyst 2960 and 3650 switches is *dynamic auto*.

Command	Description
`S1(config-if)#switchport mode trunk`	configures an interface to specifically be in **trunk mode**. Also negotiates to convert the neighboring link into a trunk.
`S1(config-if)#switchport mode access`	configures an interface to specifically be in **access mode**, a NON-trunk interface, even if its neighboring interface is in mode `trunk`
`S1(config-if)#switchport mode dynamic auto`	interface will convert into a **trunk interface** if its neighboring interface is in **mode `trunk` or `desirable`** ONLY
`S1(config-if)#switchport mode dynamic desirable`	interface will convert into a **trunk interface** if its neighboring interface is in **mode `trunk`, `dynamic auto`, or `dynamic desirable`** ONLY
`S1(config-if)#switchport nonegotiate`	⛔ stops DTP negotiation, in which interfaces may engage, as you saw above, i.e., an interface will NOT change its mode even if the neighboring interface could change it through negotiation

Troubleshooting VLANs

Command	Description
`S1#show vlan`	check whether a port belongs to the expected VLAN
`S1#show mac address-table`	check which addresses were learned on a particular port of the switch, and to which VLAN that port is assigned
`S1#show interfaces [int-id] switchport`	helpful in verifying an inactive VLAN is assigned to a port

Troubleshooting Trunks

Command	Description
`S1#show interfaces trunk`	- check native VLAN id matches on both ends of link - check whether a trunk link has been established between switches

Voice VLANs

VLANs supporting voice traffic usually have quality of service (QoS). Voice traffic must have a *trusted* label.

> Note that the implementation of QoS is beyond the scope of the CCNA2 (version 6) course.

Command	Description
`S1(config)#interface [int-id]`	access interface on which the voice VLAN will be assigned
`S1(config-if)#switchport mode access`	
`S1(config-if)#switchport access vlan [vlan-id]`	
`S1(config-if)#mls qos trust cos`	set trusted state of an interface and indicate which packet fields are used to classify traffic
`S1(config-if)#switchport voice vlan [vlan-id]`	assign a voice VLAN to that port

Configuring SSH

Command	Description
`S1#show ip ssh`	Use it to verify that the switch supports SSH
`S1(config)#ip domain-name [domain-name]`	
`S1(config)#crypto key generate rsa`	
`S1(config)#username [admin] secret [ccna]`	
`S1(config)#line vty 0 15`	
`S1(config-line)#transport input ssh`	
`S1(config-line)#login local`	
`S1(config-line)#exit`	
`S1(config)#ip ssh version 2`	enable SSH version 2
`S1(config)#crypto key zeroise rsa`	⚠️ use to **delete** RSA key pair

Modifying SSH configuration

Command	Description
`S1(config)#ip ssh time-out [time]`	Change timeout setting (time in seconds)
`S1(config)#ip ssh authentication-retries [retries]`	Change number of allowed authentication attempts

Verify your newly configured settings with `S1#show ip ssh`

Port Security

🔐 Configuring Dynamic Port Security

Command	Description
`S1(config)#interface [int-id]`	
`S1(config-if)#switchport mode access`	Set interface mode to *access*.
`S1(config-if)#switchport port-security`	Enable port security on the interface
`S1(config-if)#switchport port-security violation [violation-mode]`	set violation mode (`protect` , `restrict` , `shutdown`)

> 🏆 **Best practice:** It is a best security and general practice to "hard-type" the `switchport mode access` command. This also applies to Trunk ports (`switchport mode trunk`).

🔐 Configuring Sticky Port Security

Command	Description
`S1(config)#interface [int-id]`	
`S1(config-if)#switchport mode access`	Set interface mode to *access*.
`S1(config-if)#switchport port-security`	Enable port security on the interface
`S1(config-if)#switchport port-security maximum [max-addresses]`	Set maximum number of secure MAC addresses allowed on port
`S1(config-if)#switchport port-security mac-address sticky`	Enable sticky learning
`S1(config-if)#switchport port-security violation [violation-mode]`	set violation mode (`protect` , `restrict` , `shutdown`)

🔐 ✅ Verifying Port Security & secure MAC addresses

Now that we have configured Port Security, the following commands will be handy to verify and troubleshoot.

Command	Description
`S1#show port-security interface [int-id]`	displays interface's Port Security configuration. If violations occured, they can be checked here.

Command	Description
`S1#show port-security address`	displays secure MAC addresses configured on **all switch interfaces**
`S1#show interface [int-id] status`	displays port status. Useful to verify if an interface is in `err-disabled` status.

Bringing an `err-disabled` interface back up

💡 Recall: After a violation, a port in **Shutdown violation mode** changes its status to *error disabled*, and is effectively **shut down**. To resume operation (sending and receiving traffic), we must bring it back up. Here's how:

- Access the interface configuration mode with `S1(config)#interface [int-id]`.
- Shut the interface down using `S1(config-if)#shutdown`.
- Bring the interface back up using `S1(config-if)#no shutdown`.

VLAN trunking protocol (VTP)

Command	Description
`S1(config)#vtp mode [mode]`	mode can be `server` or `client`
`S1(config)#vtp password [password]`	optional - ⚠️ password is case-sensitive
`S1(config)#vtp domain [name]`	optional - ⚠️ domain name is case sensitive as well
`S1(config)#vtp pruning`	optional - configure VTP pruning on server
`S1(config)#vtp version 2`	optional - enables VTP version 2

❗ After this, remember to enable trunk links between the *VTP domain* switches so *VTP advertisements* can be shared among the switches. This command sequence is all that's needed to get VTP running on our *VTP domain* ✅

💡 Tip: There are 3 VTP versions. Versions 1 and 2 (which are within the scope of the CCNA exam) **DO NOT** support *extended-range VLANS* (ID from 1006 to 4095). VTP version 3 (NOT covered on the CCNA exam) does support such VLANS.

VTP verification

Command	Description
`S1#show vtp status`	verify your configuration and the status of VTP on the device
`S1#show vtp password`	verify the configured VTP password
`S1#show vlan brief`	this VLAN verification command might be useful as well when verifying VTP configuration

Spanning Tree Protocol

Bridge ID configuration

Command	Description
`S1(config)#spanning-tree vlan [vlan-id] root primary`	ensures this switch has the lowest priority value
`S1(config)#spanning-tree vlan [vlan-id] root secondary`	Use if the configuration of an alternative bridge is desired. Sets the switch priority value to ensure it becomes the root bridge if the primary root bridge fails.
`S1(config)#spanning-tree vlan [vlan-id] priority [priority]`	manually configure the bridge's priority value

💡 Recall: priority values are between 0 and 61,440.
⚠️ The priority value can only be a multiple of 4096

Bridge ID Verification

Command	Description
`S1#show spanning-tree`	verify current spanning-tree instances and root bridges

PortFast and BPDU guard

Must only be configured on interfaces connected point-to-point to an end device

Command	Description
`S1(config)#interface [int-id]`	access the interface
`S1(config)#interface range [int-type] [lowest-id]-[highest-id]`	access a range of contiguous interfaces if necessary
`S1(config-if)#switchport mode access`	as a good practice, hard-type this command so the switchport is in access mode
`S1(config-if)#spanning-tree portfast`	enables PortFast on the access port(s)
`S1(config-if)#spanning-tree bpduguard enable`	enables BPDU Guard on the access port(s)
`S1(config)#spanning-tree portfast default`	⚠️ configures PortFast to be the default for all switch interfaces
`S1(config)#spanning-tree bpduguard default`	⚠️ configures BPDU Guard to be the default for all switch interfaces

PortFast and BPDU guard verification

Command	Description
``S1#show running-config	begin spanning-tree``
`S1#show running-config interface [int-id]`	display the current configuration portion corresponding to the interface

Configuring Rapid PVST+

PVST+ is the STP flavor operating by default on Cisco switches. To configure Rapid PVST+, we just need to type a global command.

Command	Description
`S1(config)#spanning-tree mode rapid-pvst`	configure Rapid PVST+ as the STP mode on the switch
`S1(config-if)#spanning-tree link-type point-to-point`	specify that a link is point-to-point

Command	Description
`S1#clear spanning-tree detected-protocols (interface [int-id])`	forces renegotiation with neighboring switches on all interfaces or the specified interface

General STP verification commands

Command	Description
`S1#show spanning-tree`	display STP information - useful to find information about the bridge you are in, and the root bridge at a glance
`S1#show spanning-tree active`	display STP information for active interfaces only
`S1#show spanning-tree brief`	at-a-glance information for all STP instances running on the switch
`S1#show spanning-tree detail`	detailed information for all STP instances running on the switch
`S1#show spanning-tree interface [int-id]`	STP information for the specified interface
`S1#show spanning-tree vlan [vlan-id]`	STP information for the specified VLAN
`S1#show spanning-tree summary`	summary of STP port states

EtherChannel

Command	Description
`S1(config)#interface range [start-int]-[end-int]`	start by selecting the interfaces to be bundled into a **single logical link**, i.e., the EtherChannel.
`S1(config-if-range)#channel-group [number] mode [mode]`	specify the group ID (`1` to `6` , inclusive) and operation mode of the EtherChannel

Command	Description
`S1(config)#interface port-channel [number]`	enter the **port channel interface configuration mode** to change settings

PortChannel interface additional configuration

Command	Description
`S1(config-if)#switchport mode trunk`	set the interface in trunking mode, so it can carry traffic of multiple VLANs
`S1(config-if)#switchport trunk native vlan [native-vlan-id]`	specify the link's native VLAN
`S1(config-if)#switchport trunk allowed vlan [vlan-id-1 (,vlan-id-2,...)]`	specify allowed VLANs (VLAN IDs) on trunk link
`S1(config-if)#switchport trunk allowed vlan add [vlan-id-1 (,vlan-id-2,...)]`	**add** VLANs to the list of **already allowed** VLANs on the trunk link

⚠️ The **EtherChannel negotiation protocols** you use for your interface bundles **MUST MATCH ON BOTH ENDS**, whether it is LACP, PAgP (Cisco Proprietary), or no protocol (`on` mode).

Available EtherChannel modes

EC mode	Description
`active`	Enable LACP unconditionally
`auto`	Enable PAgP only if another PAgP device is detected.
`desirable`	Enable PAgP unconditionally
`on`	Enable EtherChannel only
`passive`	Enable LACP only if another LACP device is detected

Back to beginning of section