

CCENT CERTIFICATION ALL-IN-ONE FOR DUMMIES CHEAT SHEET

From [CCENT Certification All-In-One For Dummies](#)

By [Glen E. Clarke](#)

The CCENT certification is a new, fast-growing certification that tests your knowledge of basic Cisco device-management and networking concepts. It is a great stepping stone to the CCNA certification and other Cisco certification tracks. The CCENT exam tests your knowledge of real-world networking concepts and Cisco features found on most networks today, and this Cheat Sheet gives you quick facts and code listings to remember on test day to help you answer questions found on the CCENT certification exam.

OSI MODEL FOR THE CCENT CERTIFICATION EXAM

The CCENT certification tests you heavily on the OSI model and the different protocols and devices that run at each layer of the OSI model. The following table reviews the OSI model by giving you a description of each layer and examples of protocols and devices that run at each layer.

Layer	Description	Examples
7.	Responsible for	SMTP, DNS,

Application	initiating or services the request.	HTTP, and Telnet
6. Presentation	Formats the information so that it is understood by the receiving system.	Compression and encryption depending on the implementation
5. Session	Responsible for establishing, managing, and terminating the session.	NetBIOS
4. Transport	Breaks information into segments and is responsible for connection and connectionless communication.	TCP and UDP
3. Network	Responsible for logical addressing and routing	IP, ICMP, ARP, RIP, IGRP, and routers
2. Data Link	Responsible for physical addressing, error correction, and preparing the information for the media	MAC address, CSMA/CD, switches, and bridges
1. Physical	Deals with the electrical signal.	Cables, connectors, hubs, and repeaters

CISCO IOS BASICS FOR THE CCENT CERTIFICATION EXAM

The CCENT certification exam will test you on the basics of the Cisco Internetwork Operating System (IOS) and how to configure the IOS. The following are some key points that summarize the IOS basics to remember for the CCENT certification exam:

- **Types of Memory:** There are different types of memory on a Cisco device:
 - *ROM:* The Read-Only Memory (ROM) on a Cisco device is like the ROM on a computer in the sense that it stores the POST and the boot loader program. The boot loader program is responsible for locating the IOS.
 - *Flash:* The flash memory is used to store the Cisco IOS.
 - *RAM:* RAM is used to store things like the routing table on a router, or the MAC address table on a switch. It is also used to store the running-config. RAM is also known as volatile RAM, or VRAM.
 - *NVRAM:* Non-volatile RAM (NVRAM) is used to store the startup-config, which is copied to the running-config on bootup after the IOS is loaded.
- **The Boot Process:** For the CCENT certification exam, you need to know the high-level steps that occur when a Cisco device starts up. The following is a quick review of the boot process of a Cisco router:

- *POST*: The first thing that occurs when a Cisco device boots up is the POST routine, which is responsible for performing a self diagnostic to verify everything is functioning on the router or switch.
- *Locate IOS*: After the POST, the bootloader program, which is stored in ROM, locates the IOS in flash memory and loads it into RAM.
- *Startup-config applied*: After the IOS is loaded into memory, the bootloader program then locates the startup-config and applies it to the device.
- **Configuration Modes**: When making changes to the Cisco device, there are a number of different configuration modes, and each change is made in a specific configuration mode. The following summarizes the major configuration modes:
 - *User Exec*: When you connect to a Cisco device, the default configuration mode is user exec mode. With user exec mode, you can view the settings on the device but not make any changes. You know you are in user exec mode because the IOS prompt displays a “>”.
 - *Priv Exec*: In order to make changes to the device, you must navigate to priv exec mode, where you may be required to input a password. Priv exec mode displays with a “#” in the prompt.

- *Global Config:* Global configuration mode is where you go to make global changes to the router, such as the hostname. To navigate to global configuration mode from priv exec mode, you type **config term**, where you will be placed at the “(config)#” prompt.
- *Sub Prompts:* You can navigate to a number of different sub prompts from global configuration, such as the interface prompts to modify settings on a specific interface and the line prompts to modify the different ports on the device.

CONFIGURING USERS AND PASSWORDS FOR THE CCENT CERTIFICATION EXAM

The CCENT certification exam will test you on basic configuration of the Cisco IOS, including setting passwords and creating users. The following are some key points that summarize configuring passwords on Cisco devices:

Command(s)	Result
<pre> R1>enable R1#config term R1(config)#enable password mypass R1(config)#enable secret mysecret </pre>	These commands are used to create an enable password and an enable secret. Remember that the enable password is stored in clear text within the configuration file while the enable secret is encrypted.

```
R1>enable
R1#config term
R1(config)#line con 0
R1(config-
line)#password
conpass
R1(config-line)#login
```

These commands are used to create a console password on the console port. Remember that after the password is set, you must specify the login command to require authentication on the port.

```
R1>enable
R1#config term
R1(config)#line aux 0
R1(config-
line)#password
auxpass
R1(config-line)#login
```

These commands are used to create an auxiliary port password on the router. Again, notice the use of the login command after setting the password; if you forget to use it then the router will not prompt for a password on that port.

```
R1>enable
R1#config term
R1(config)#line vty 0
15
R1(config-
line)#password
vtypass
R1(config-line)#login
```

These commands are used to create a password for telnet connections that are made to the device.

```
R1>enable
R1#config term
R1(config)#username
glen password
glenpass

R1(config)#line
con 0
R1(config-
line)#login local

R1(config)#line
```

These commands are used to create a username called **glen** with a password of **glenpass**. You then use the *login local* command on each of the console port, auxiliary port, and vty ports to require authentication with a username *and* password.

```
vty 0 15
R1(config-
line)#login local
```

```
R1(config)#banner
motd #
Enter TEXT message.
End with the
character '#'.
This device is for
authorized personnel
only.
Please disconnect at
once if you have not
been given permission
to access this device
#
R1(config)#
```

This command creates a message-of-the-day banner, which displays before someone logs in. This is used to give legal notice that unauthorized access is prohibited.

CONFIGURING INTERFACES FOR THE CCENT CERTIFICATION EXAM

The CCENT certification exam requires you to know how to configure basic settings on the router, such as the hostname and the interfaces. The following commands review those configuration tasks.

The following commands are used to configure the name of the router with the `hostname` command. The name of the router appears in the prompt once it is set. Notice that the hostname is changed in global configuration mode.

```
Router>enable
Router#config term
Router(config)#hostname R2
```

The following commands are used to configure the FastEthernet port on the router. Notice that the interface is referenced with the slot/port syntax on the `interface` command. The IP address is set and then the description of the interface, the speed and duplex mode are then set, and finally the port is enabled with the `no shutdown` command.

```
R2(config)#interface f0/0
R2(config-if)#ip address 25.0.0.1 255.0.0.0
R2(config-if)#description Private LAN
R2(config-if)#speed 100
R2(config-if)#duplex full
R2(config-if)#no shutdown
```

The following commands are used to configure the Serial port on the router. Notice that the interface is referenced with the slot/port syntax on the `interface` command. The IP address is set and then the encapsulation protocol (PPP or HDLC) is set. Because this is the DCE end of a back-to-back serial cable, the clock rate needs to be set, otherwise the service provider sets that. Finally, the interface is enabled with the `no shutdown` command.

```
R1>enable
R1#config term
R1(config)#interface serial 0/0
R1(config-if)#ip address 24.0.0.1 255.0.0.0
R1(config-if)#encapsulation hdlc
R1(config-if)#clock rate 64000 (only set for DCE device)
R1(config-if)#no shutdown
```

CONFIGURING NETWORK SERVICES FOR THE CCENT CERTIFICATION EXAM

This section reviews popular commands used when configuring a Cisco device for name resolution, DHCP services, and NAT. You'll need to know these for the CCENT Certification exam.

The following commands configure the hostname table on a router and display the entries in the hostname table:

```
NY-R1>enable
NY-R1#config term
NY-R1(config)#ip host BOS-R1 24.0.0.2
```

To verify that the entry has been added:

```
NY-R1(config)#exit
NY-R1#show hosts
```

The following commands enable DNS lookups and specify the DNS server of 23.0.0.200 to send DNS queries to. The domain name is also set to gleneclarke.com.

```
NY-R1>enable
NY-R1#config term
NY-R1(config)#ip domain-lookup
NY-R1(config)#ip name-server 23.0.0.200
NY-R1(config)#ip domain-name gleneclarke.com
```

The following commands configure your router as a DHCP server by setting an address pool (range of addresses to give

out) and setting up excluded addresses that are not to be given out. The lease time is set to 7 days in this example.

```
NY-R1(config)#ip dhcp pool NY_Network
NY-R1(dhcp-config)#network 23.0.0.0 255.0.0.0
NY-R1(dhcp-config)#default-router 23.0.0.1
NY-R1(dhcp-config)#dns-server 23.0.0.200
NY-R1(dhcp-config)#lease 7 0 0
NY-R1(dhcp-config)#exit
NY-R1(config)#ip dhcp excluded-address 23.0.0.1 23.0.0.15
```

The following commands configure NAT overload services on a router called NY-R1. In this example, a list of source addresses is created in access list #1, which is then used as the inside source list. The FastEthernet 0/0 port is the overloaded public address port that all inside addresses get translated to.

```
NY-R1(config)#Access-list 1 permit 10.0.0.0 0.255.255.255
NY-R1(config)#ip nat inside source list 1 interface
    FastEthernet 0/0 overload
NY-R1(config)#interface FastEthernet0/0
NY-R1(config-if)#ip nat outside
NY-R1(config-if)#interface FastEthernet0/1
NY-R1(config-if)#ip nat inside
```

BASIC SWITCH COMMANDS TO REMEMBER FOR THE CCENT CERTIFICATION EXAM

This section outlines some of the popular commands you use on a Cisco switch for the CCENT certification exam. Most of

the basic router commands, such as setting passwords and banners, work on the switch.

Command(s) / Result

```
Switch#show mac-address-table
```

Used to display the MAC address table on the switch.

```
Switch>enable
Switch#config term
Switch(config)#hostname
NY-SW1
NY-SW1(config)#
```

Used to change the hostname on the switch.

```
NY-SW1>enable
NY-SW1#config term
NY-SW1(config)#interface
vlan1
NY-SW1(config-if)#ip address 23.0.0.25
255.0.0.0
NY-SW1(config-if)#no shutdown
NY-SW1(config-if)#exit
NY-SW1(config)#ip default-gateway
23.0.0.1
```

Configures the switch for an IP address so that you can remotely connect to the switch and manage it. Also notice that the default gateway is set. If you do not set the default gateway, you will be unable to manage the switch from a different network.

```
Switch>enable
Switch#config term
Switch(config)#interface f0/5
Switch(config-if)#speed 100
Switch(config-if)#duplex full
Switch(config-if)#description Web
Server
Switch(config-if)#no shutdown
```

These commands are used to manually configure a port for 100 Mbps, full duplex, and assigns a description to the port. The port is then enabled with the no shutdown command.

```
Switch(config-if)#shutdown
```

Disables the port.

```
SW1>enable
SW1#config term
SW1(config)#interface f0/6
SW1(config-if)#switchport mode
access
SW1(config-if)#switchport
port-security
SW1(config-if)#switchport port-security
mac-address sticky
SW1(config-if)#switchport port-security
maximum 1
SW1(config-if)#switchport port-security
violation shutdown
```

This group of commands configures port security on port #6.

Port security is a way to limit which systems can connect to a switch. This code example uses a “sticky” MAC address that tells

the switch to configure the port for whatever MAC uses the port first. It then sets the maximum number of MACs for the port to 1 and shuts down the port if there is a violation.

`show port-security address`

Show the MAC addresses that have been configured for each port.

`show port-security interface
f0/6`

Show the configuration of port security on port 6.

`Switch>enable
Switch#vlan database
Switch(vlan)#vlan 2 name
Executives
VLAN 2 added:
Name: Executives
Switch(vlan)#exit`

Configures a VLAN named Executives in the VLAN database.

`Switch#show vlan`

Display a list of VLANs.

`Switch(config)#interface range f0/6 –
9
Switch(config-if-range)#switchport access
vlan 2`

Place ports 6–9 in the newly created

VLAN 2.

TROUBLESHOOTING COMMANDS FOR THE CCENT CERTIFICATION EXAM

When problems arise on Cisco devices, there are a number of `show` commands you can use to help identify what the problem is. The following table lists popular `show` commands:

Command(s)	Result
<code>show running-config</code>	Displays the running configuration stored in VRAM.
<code>show startup-config</code>	Displays the startup configuration stored in NVRAM.
<code>show ip interface brief</code>	Shows a summary of the interfaces and their status.
<code>show interfaces</code>	Displays detailed information about each interface.
<code>show interface serial 0/0</code>	Displays detailed information about a specific interface.
<code>show ip route</code>	Displays the routing table.
<code>show hosts</code>	Displays the host name table.
<code>show controller serial0/1</code>	Displays whether the serial interface is a DCE or DTE

	device.
<code>show ip protocols</code>	Displays what routing protocols are loaded.
<code>show cdp neighbors</code>	Displays basic information about neighboring devices such as name, type of device, and model.
<code>show cdp neighbors detail</code>	Displays detailed information about neighboring devices such as name, type of device, model, and IP address.

SECURITY BEST PRACTICES FOR THE CCENT CERTIFICATION EXAM

One of the most important skills to have as a CCENT is the capability of implementing basic security practices on your Cisco devices. The following are some key points to remember about securing devices when you take the CCENT exam:

- **Secure Location:** Be sure to locate your Cisco routers and switches in a secure location — a locked room where limited access is permitted.
- **Disable Ports:** In high secure environments, you should disable unused ports so that unauthorized systems cannot connect to the network.

- **Configure Port Security:** In order to control which systems can connect to the enabled ports, use port security to limit which MAC addresses can connect to which ports.
- **Set Passwords:** Be sure to configure passwords on the console port, auxiliary port, and the vty ports. Also configure the enable secret for access to priv exec mode.
- **Login Command:** Do not forget the login command after setting the password on the port. The login command tells the Cisco device that anyone connecting must log in and forces the prompt for a password.
- **Login Local Command:** If you are looking to create usernames and passwords for login, then use the *login local* command to tell the Cisco device that you wish to authenticate persons by the usernames and password configured on the device.
- **Encrypt Passwords:** Be sure to encrypt all passwords in the configuration with the *service password-encryption* command!
- **Banners:** Be sure to configure banners that do not have the word “welcome” in the message or any other inviting phrases. You want to make sure that the banners indicate that unauthorized access is prohibited.
- **Secure Communication:** To remotely manage the device, use SSH instead of telnet as the communication is encrypted.

NETWORK CABLING FOR THE CCENT CERTIFICATION EXAM

The CCENT certification tests you on the different types of cabling that are used in different scenarios. The following are some key points to remember about network cabling.

- **Rollover cable:** A rollover cable is also known as a *console cable* and gets the name *rollover* because the order of the wires from one end of the cable to the other are totally reversed, or rolled over. The rollover/console cable is used to connect a computer to the console port or auxiliary port of the router for administration purposes.
- **Back-to-back serial cable:** The back-to-back serial cable is used to connect two Cisco routers directly together over a serial link. A back-to-back serial link will have one router act as the DCE device with the clock rate set and the other router act as the DTE device.
- **Straight-through cable:** A straight-through cable is used to connect dissimilar devices together. Scenarios that use straight-through cables are computer-to-switch and switch-to-router.
- **Crossover cable:** A crossover cable has wires 1 and 2 switch positions with wires 3 and 6 on one end and is used to connect similar devices together. Scenarios that use crossover cables are computer-to-computer, switch-to-switch, and computer-to-router (they are both hosts).

- **Coaxial cable:** A network cable type used in old Ethernet environments, such as 10Base2 and 10Base5. Coaxial cable is seen in high-speed Internet connections with cable companies today.
- **Fiber optic cable:** A unique cable type that has a glass core which carries pulses of light as opposed to copper cable carrying electrical signals (coax and twisted pair cabling).

NETWORK DEVICES AND SERVICES OVERVIEW FOR THE CCENT CERTIFICATION EXAM

You can be sure to get a few questions on the CCENT certification exam that test your knowledge of types of devices and different network services. The following are some key points to remember about devices and services:

NETWORK DEVICES

- **Hub:** A hub is a layer-1 device that is used to connect systems together. When a hub receives data in the form of an electrical signal, it sends the data to all other ports in hopes the destination system is at one of those ports. All ports on the hub create a single collision domain and a single broadcast domain.
- **Repeater:** A repeater is a layer-1 device that is used to amplify the signal. As the signal travels along the network, it gets weaker due to interference, so the

purpose of the repeater is to regenerate that signal so it can travel more distance.

- **Bridge:** A bridge is a layer-2 device that creates multiple network segments. The bridge maintains a table in memory of what systems reside on what segments by their MAC addresses. When data reaches the bridge, the bridge filters the traffic by only sending the data to the network segment that the destination system resides on. The purpose of the bridge is that it filters traffic by sending the data only to the segment where the destination system resides. Each segment on the bridge creates a separate collision domain, but it is all one broadcast domain.
- **Switch:** The switch, another layer-2 device, is an improvement on a bridge in the sense that each port on the switch acts as a network segment. The switch filters traffic by sending the data only to the port on the switch where the destination MAC address resides. The switch stores each MAC address and the port the MAC address resides on in an area of memory known as the *MAC address table*. Each port on the switch creates a separate collision domain, but all ports are part of the same broadcast domain.
- **Router:** A router is a layer-3 device that handles routing of data from one network to another network. The router stores a listing of destination networks in the routing table which is found in memory on the router.

NETWORK SERVICES

- **DHCP:** The DHCP service is responsible for assigning IP addresses to hosts on the network. When a client boots up, it sends a DHCP discover message, which is a broadcast message designed to locate a DHCP server. The DHCP server responds with a DHCP Offer, offering the client an IP address. The client then responds with a DHCP request message asking for the address before the server responds with a DHCP ACK to acknowledge that the address has been allocated to that client.
- **DNS:** The DNS service is responsible for converting the Fully Qualified Domain Name, (FQDN) such as www.glenecclarke.com to an IP address.
- **NAT:** Network Address Translation is responsible for converting the internal address to a public address that is used to access the Internet. NAT offers the benefit of being able to purchase only one public IP address and have a number of clients on the network use that one IP address for Internet access. NAT also offers the security benefit that the internal addresses are not used on the Internet — helping to keep the internal addresses unknown to the outside world. There are two types of NAT to know for the CCENT certification exam:
 - *Static NAT:* Static NAT is the mapping of one internal address to one public address. With static

NAT, you will need multiple public addresses to allow internal clients to access the Internet.

- *NAT overloading*: A more popular form of NAT, NAT overloading is the concept that all internal addresses get translated to the one public address on the NAT device.
- **Web services**: There are a number of Web services you should be familiar with for the CCENT certification exam:
 - *POP3/IMAP4*: POP3 and IMAP4 are the Internet protocols for receiving email over the Internet.
 - *SMTP*: SMTP is the Internet protocol for sending email over the Internet. SMTP servers are also known as *email servers*.
 - *HTTP*: HTTP servers are also known as *Web servers* and are used to host Web sites. HTTP is a protocol that is used to send the Web page from the Web server to the Web client.
 - *FTP*: FTP is an Internet protocol used to transfer files over the Internet. The files are hosted on FTP servers, which are then downloaded to any clients on the Internet.

CONFIGURING ROUTING FOR THE CCENT CERTIFICATION EXAM

Routing protocols will certainly come up on your CCENT certification exam. This section reviews popular commands

that deal with routing and routing protocols, such as RIPv1 and RIPv2.

Command(s)	Result
<code>ip routing</code>	Enables routing on the router. Should be on by default.
<code>no ip routing</code>	Disables routing on the router.
<code>show ip route</code>	Displays the routing table.
<code>ip route 23.0.0.0 255.0.0.0 22.0.0.2</code>	Adds a static route to the router for the 23.0.0.0 network and sends any data for that network to the 22.0.0.2 address (next hop).
<code>no ip route 23.0.0.0 255.0.0.0 22.0.0.2</code>	Deletes the static route from the routing table.
<code>ip route 0.0.0.0 0.0.0.0 22.0.0.2</code>	Sets the gateway of last resort on the router to forward any packets with unknown destinations to the 22.0.0.2 address.
<code>ROUTERB>enable ROUTERB#config term ROUTERB(config)#router rip ROUTERB(config-</code>	Configures the router for RIPv1. RIP is a dynamic routing protocol that is used to

```
router)#network  
26.0.0.0  
ROUTERB(config-  
router)#network  
27.0.0.0
```

share routing information with other routers running RIP. In this example, RIP will share knowledge of the 26.0.0.0 and the 27.0.0.0 networks.

```
ROUTERB>enable  
ROUTERB#config term  
ROUTERB(config)#router  
rip  
ROUTERB(config-  
router)#network  
26.0.0.0  
ROUTERB(config-  
router)#network  
27.0.0.0  
ROUTERB(config-  
router)#version  
2
```

To configure the router for RIPv2, you use the same commands but add the “version 2” command at the end.

```
show ip protocols
```

Display what routing protocols are running on the router.

```
debug ip rip
```

Enable RIP debugging, which will display RIP related messages on the screen as RIP-related events occur (packets are sent and received).

```
no debug all
```

Turns off debugging once you are done troubleshooting RIP.

WIRELESS NETWORKING TERMINOLOGY FOR THE CCENT CERTIFICATION EXAM

At its most basic, wireless communication is the sending and receiving of data through airwaves. But the CCENT certification exam expects you to understand wireless terminology and concepts. The following are some key points to remember for the exam:

Know the following organizations that help define wireless:

- **Institute of Electrical and Electronics Engineers (IEEE):** Creates the wireless standards, such as 802.11a/b/g/n
- **Federal Communications Commission (FCC):**Regulates the use of wireless devices (licenses of frequencies)
- **WiFi-Alliance:** Ensures compatibility of wireless components. The WiFi-Alliance is responsible for testing and certification of wireless devices.

Know the two types of wireless networks:

- **Ad hoc mode:** No wireless access point is used. The wireless clients communicate in a peer-to-peer environment.
- **Infrastructure mode:** Uses a wireless access point

Know the IEEE Standards for wireless:

- **802.11a:** A wireless standard that uses the 5 GHz frequency range and runs at 54 Mbps.
- **802.11b:** A wireless standard that uses the 2.4 GHz frequency range and runs at 11 Mbps. The WiFi standard

was created and 802.11b is part of that standard. This is the frequency used by cordless phones and microwaves, so you may experience interference from those devices. As a correction, you can change the channel of the wireless network or purchase phones that use a different frequency.

- **802.11g:** A wireless standard, which is compatible with 802.11b, that also uses the 2.4 GHz frequency range and runs at 54 Mbps.
- **802.11n:** A new wireless standard that can use either the 2.4 GHz frequency range or the 5 GHz frequency range and is compatible with 802.11a/b/g. 802.11n has a transfer rate of approximately 150 Mbps.

Other wireless terms to know for the exam:

- **Basic Service Set (BSS):** A wireless network consisting of one access point using an SSID. If you had three access points, each using a different SSID, then this would be three BSS networks.
- **Extended Service Set (ESS):** A wireless network comprising multiple access points using the same SSID.

Be sure to know the configuration requirements to set up an ESS:

- The SSID on each access point must be the same.
- The range of the access points must overlap by 10% or more.
- Each access point must use a different channel.

Know the difference between the different wireless encryption types:

- **Wired Equivalent Privacy (WEP):** An old wireless encryption protocol that involves configuring a pre-shared key on the access point and the wireless client that is used to encrypt and decrypt data. WEP uses the RC4 encryption algorithm with the pre-shared key and is not considered secure due to the way the key is used. WEP supports 64-bit and 128-bit encryption.
- **WiFi Protected Access (WPA):** The improvement on WEP that adds the TKIP protocol in order to perform key rotation to help improve on the fact that WEP uses a static key. WPA has two modes: *personal mode* involves configuring a pre-shared key, and *enterprise mode* can use an authentication server such as RADIUS.
- **WiFi Protected Access 2 (WPA2):** Improves upon WPA by changing the encryption algorithm to the *Advanced Encryption Standard* (AES) and supports both personal mode and enterprise mode.

The following are some key points regarding best practices to improve the security of your wireless network:

- **Disable wireless:** If you aren't using wireless, then disable the wireless functionality on the wireless router.
- **Change the SSID:** Make sure you change the SSID to something meaningless. You don't want the SSID set to a value that will help the hacker identify the building

you're in because he could move closer to the building to get a stronger signal.

- **Disable SSID broadcasting:** After disabling SSID broadcasting, the router won't advertise the existence of the wireless network. This makes it harder for someone to connect because they have to manually configure their client for the SSID name.
- **Implement MAC filtering:** MAC filtering allows you to limit who can connect to the wireless network by the MAC address of the network card.
- **Implement encryption:** Be sure to encrypt wireless traffic with WEP, WPA, or WPA2. WPA2 is the most secure of the three.