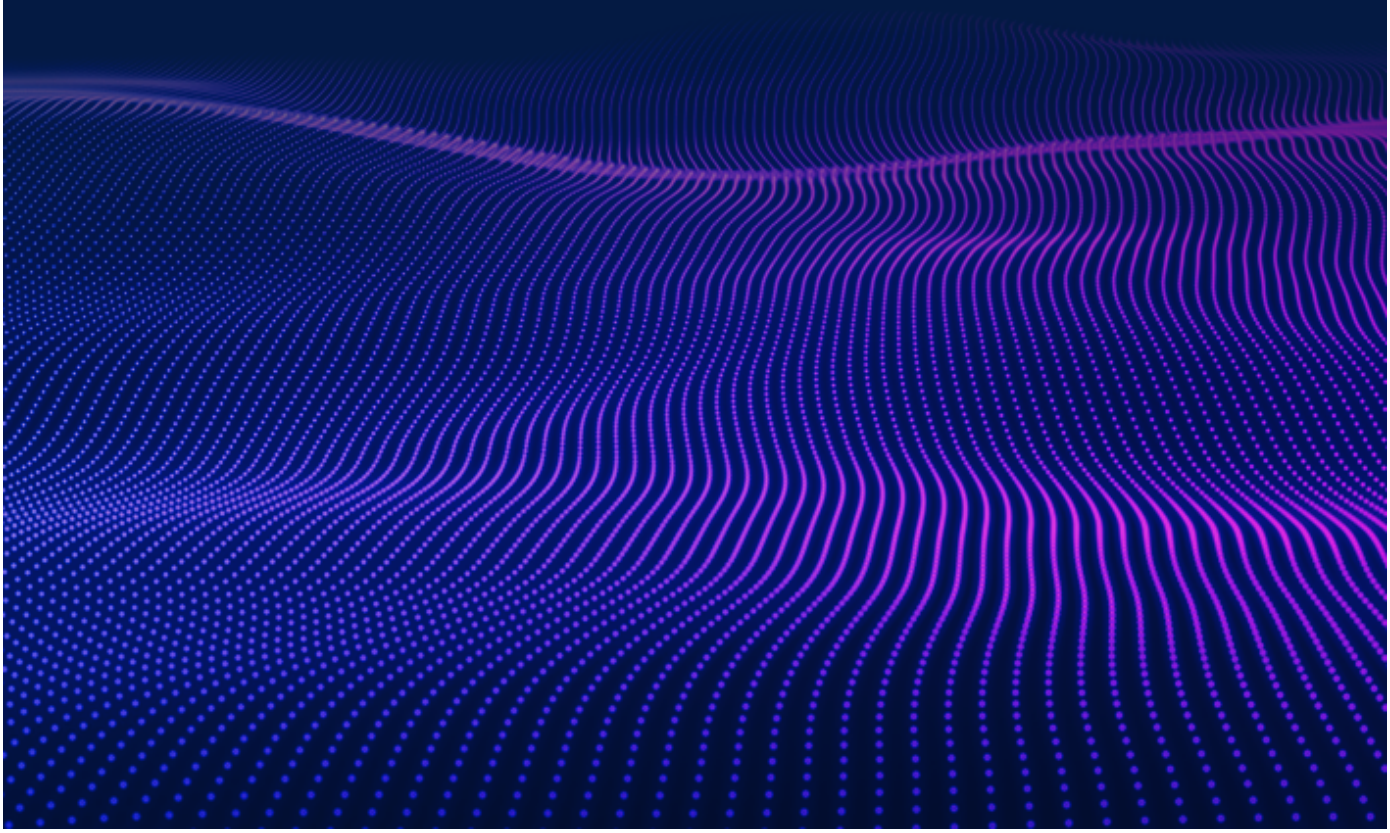
netwrix

Cisco Commands Cheat Sheet



BASIC CONFIGURATION COMMANDS

COMMAND	PURPOSE
enable	Logs you into enable mode, which is also known as user exec mode or privileged mode
configure terminal	Logs you into configuration mode
interface *fastethernet/number*	Enters interface configuration mode for the specified fast ethernet interface
reload	An exec mode command that reboots a Cisco switch or router
hostname *name*	Sets a host name to the current Cisco network device
copy *from-location to-location*	An enable mode command that copies files from one file location to another
copy running-config startup-config	An enable mode command that saves the active config, replacing the startup config when a Cisco network device initializes
copy startup-config running-config	An enable mode command that merges the startup config with the currently active config in RAM
write erase **erase startup-config**	An enable mode command that deletes the startup config
ip address *ip-address mask*	Assigns an IP address and a subnet mask
shutdown **no shutdown**	Used in interface configuration mode. “Shutdown” shuts down the interface, while “no shutdown” brings up the interface
ip default-gateway *ip-address*	Sets the default gateway on a Cisco device
show running-config	An enable mode command that displays the current configuration
description *name-string*	A config interface command to describe or name an interface
show running-config *interface interface slot/number*	An enable mode command to display the running configuration for a specific interface
show ip interface *[type number]*	Displays the usability status of interfaces that are configured for IP
ip name-server *serverip-1 serverip-2*	A configure mode command that sets the IP addresses of DNS servers

TROUBLESHOOTING COMMANDS	
ping *{hostname | system-address} [source source-address]*	Used in enable mode to diagnose basic network connectivity
speed *{10 | 100 | 1000 | auto}*	An interface mode command that manually sets the speed to the specified value or negotiates it automatically
duplex *{auto | full | half}*	An interface mode command that manually sets duplex to half, full or auto
cdp run **no cdp run**	A configuration mode command that enables or disables Cisco Discovery Protocol (CDP) for the device
show mac address-table	Displays the MAC address table
show cdp	Shows whether CDP is enabled globally
show cdp neighbors *[detail]*	Lists summary information about each neighbor connected to this device; the "detail" option lists detailed information about each neighbor
show interfaces	Displays detailed information about interface status, settings and counters
show interface status	Displays the interface line status
show interfaces switchport	Displays a large variety of configuration settings and current operational status, including VLAN trunking details
show interfaces trunk	Lists information about the currently operational trunks and the VLANs supported by those trunks
show vlan **show vlan brief**	Lists each VLAN and all interfaces assigned to that VLAN but does not include trunks
show vtp status	Lists the current VTP status, including the current mode

ROUTING AND VLAN COMMANDS	
ip route *network-number network-mask {ip-address | interface}*	Sets a static route in the IP routing table
router rip	Enables a Routing Information Protocol (RIP) routing process, which places you in router configuration mode
network *ip-address*	In router configuration mode, associates a network with a RIP routing process
version 2	In router configuration mode, disables automatic summarization
no auto-summary	In router configuration mode, disables automatic summarization
passive-interface *interface*	In router configuration mode, sets only that interface to passive RIP mode. In passive RIP mode, RIP routing updates are accepted by, but not sent out of, the specified interface
show ip rip database	Displays the contents of the RIP routing database
ip nat *[inside | outside]*	An interface configuration mode command to designate that traffic originating from or destined for the interface is subject to NAT
ip nat inside source *{list{access-list-number | access-list-name}} interface type number[overload]*	A configuration mode command to establish dynamic source translation. Use of the "list" keyword enables you to use an ACL to identify the traffic that will be subject to NAT. The "overload" option enables the router to use one global address for many local addresses.
ip nat inside source static *local-ip global-ip*	A configuration mode command to establish a static translation between an inside local address and an inside global address
vlan	Creates a VLAN and enters VLAN configuration mode for further definitions
switchport access vlan	Sets the VLAN that the interface belongs to
switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link
switchport access	Assigns this port to a VLAN

vlan vlan-id *[name vlan-name]*	Configures a specific VLAN name (1 to 32 characters)
switchport mode *{ access | trunk }*	Configures the VLAN membership mode of a port. The access port is set to access unconditionally and operates as a non-trunking, single VLAN interface that sends and receives non-encapsulated (non-tagged) frames. An access port can be assigned to only one VLAN. The trunk port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router
switchport trunk *{encapsulation { dot1q }*	Sets the trunk characteristics when the interface is in trunking mode. In this mode, the switch supports simultaneous tagged and untagged traffic on a port
encapsulation dot1q vlan-id	A configuration mode command that defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance

DHCP COMMANDS	
ip address dhcp	A configuration mode command to acquire an IP address on an interface via DHCP
ip dhcp pool name	A configuration mode command to configure a DHCP address pool on a DHCP server and enter DHCP pool configuration mode
domain-name *domain*	Used in DHCP pool configuration mode to specify the domain name for a DHCP client
network *network-number [mask]*	Used in DHCP pool configuration mode to configure the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server
ip dhcp excluded-address *ip-address [last-ip-address]*	A configuration mode command to specify IP addresses that a DHCP server should not assign to DHCP clients
ip helper-address *address*	An interface configuration mode command to enable forwarding of UDP broadcasts, including BOOTP, received on an interface
default-router *address[address2 … address8]*	Used in DHCP pool configuration mode to specify the default router list for a DHCP client

SECURITY COMMANDS	
password *pass-value*	Lists the password that is required if the login command (with no other parameters) is configured
username *name* **password** *pass-value*	A global command that defines one of possibly multiple user names and associated passwords used for user authentication. It is used when the login local line configuration command has been used
enable password *pass-value*	A configuration mode command that defines the password required when using the **enable** command
enable secret *pass-value*	A configuration mode command that sets this Cisco device password that is required for any user to enter enable mode
service password-encryption	A configuration mode command that directs the Cisco IOS software to encrypt the passwords, CHAP secrets, and similar data saved in its configuration file
ip domain-name *name*	Configures a DNS domain name
crypto key generate rsa	A configuration mode command that creates and stores (in a hidden location in flash memory) the keys that are required by SSH
transport input *{telnet | ssh}*	Used in vty line configuration mode, defines whether Telnet or SSH access is allowed into this switch. Both values can be specified in a single command to allow both Telnet and SSH access (default settings)
access-list *access-list-number {deny | permit} source [source-wildcard] [log]*	A configuration mode command that defines a standard IP access list
access-class	Restricts incoming and outgoing connections between a particular vty (into a basic Cisco device) and the addresses in an access list
ip access-list *{standard | extended} {access-list-name | access-list-number}*	A configuration mode command that defines an IP access list by name or number

permit source *[source-wildcard]*	Used in ACL configuration mode to set conditions to allow a packet to pass a named IP ACL. To remove a permit condition from an ACL, use the “no” form of this command
deny source *[source-wildcard]*	Used in ACL configuration mode to set conditions in a named IP ACL that will deny packets. To remove a deny condition from an ACL, use the “no” form of this command
ntp peer *<ip-address>*	Used in global configuration mode to configure the software clock to synchronize a peer or to be synchronized by a peer
switchport port-security	Used in interface configuration mode to enable port security on the interface
switchport port-security maximum maximum	Used in interface configuration mode to set the maximum number of secure MAC addresses on the port
switchport port-security mac-address *{mac-addr | {sticky [mac-addr]}}*	Used in interface configuration mode to add a MAC address to the list of secure MAC addresses. The “sticky” option configures the MAC addresses as sticky on the interface
switchport port-security violation *{shutdown | restrict | protect}*	Used in interface configuration mode to set the action to be taken when a security violation is detected
show port security *[interface interface-id]*	Displays information about security options configured on the interface

MONITORING AND LOGGING COMMANDS	
logging *ip address*	Configures the IP address of the host that will receive the system logging (syslog) messages
logging trap level	Used in configuration mode to limit messages that are logged to the syslog servers based on severity. Specify the number or name of the desired severity level at which messages should be logged
show logging	Enable mode command that displays the state of system logging (syslog) and the contents of the standard system logging buffer
terminal monitor	Used in interface configuration mode to enable port security on the interface
switchport port-security maximum maximum	An enable mode command that tells Cisco IOS to send a copy of all syslog messages, including debug messages, to the Telnet or SSH user who issues this command

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social

Simplify Monitoring of Cisco Devices

with Netwrix Auditor for Network Devices

Get detailed audit information on configuration changes.

Track successful and failed VPN logon attempts.

Stay on top of each attempt to log in directly to a Cisco device.

Continuously monitor devices for hardware malfunctions.

Download Free 20-Day Trial