Cisco IOS Essential Commands

Page 1 — Command Modes and Inspection

Important: Back up the configuration and confirm console access before changing a production device. A command that is correct on one platform may behave differently on another.

Command Modes

Mode	Prompt	Enter with	Purpose
User EXEC	hostname>	Default login	Limited inspection only
Privileged EXEC	hostname#	enable	Full inspection, diagnostics, config entry
Global Config	hostname(config)#	configure terminal	Device-wide configuration changes
Interface Config	hostname(config-if)#	interface <INTERFACE>	Per-interface settings
Line Config	hostname(config-line)#	line vty 0 4	Console and VTY access settings
VLAN Config	hostname(config-vlan)#	vlan <VLAN-ID>	VLAN name and settings

exit moves back one level. end or Ctrl+Z returns to Privileged EXEC from any sub-mode.

Essential Inspection Commands — Read-Only

Command	Mode	Purpose and security note
show version	Priv EXEC	Platform, software release, uptime, hardware
show running-config	Priv EXEC	Active config in RAM — output is sensitive
show startup-config	Priv EXEC	Saved config in NVRAM — output is sensitive
show ip interface brief	Priv EXEC	All interface addresses and up/down status
show interfaces status	Priv EXEC	Switch port state, VLAN, duplex, speed
show interfaces <INTERFACE>	Priv EXEC	Detailed stats and errors for one interface
show vlan brief	Priv EXEC	VLANs and port membership
show interfaces trunk	Priv EXEC	Active trunks and permitted VLANs
show spanning-tree	Priv EXEC	STP status, root bridge, port roles
show ip route	Priv EXEC	Full routing table (C=connected, S=static)
show mac address-table	Priv EXEC	Learned MAC addresses and ports
show access-lists	Priv EXEC	ACLs and hit counters
show logging	Priv EXEC	Buffered logs — review for errors and events
show users	Priv EXEC	Active management sessions
show clock	Priv EXEC	Device time — verify for log accuracy
show ntp associations	Priv EXEC	NTP synchronisation status
show ip ssh	Priv EXEC	SSH version and status
show cdp neighbors detail	Priv EXEC	Connected Cisco devices (if CDP enabled)
show lldp neighbors detail	Priv EXEC	Connected devices via LLDP (vendor-neutral)

Cisco IOS Essential Commands

Page 2 — Common Configuration Tasks

Set hostname

```
hostname <HOSTNAME>
```

Set enable secret (prefer over enable password)

```
enable secret <STRONG-UNIQUE-SECRET>
```

Set timestamps and NTP

```
service timestamps log datetime msec
ntp server <NTP-SERVER>
```

Access banner

```
banner login #Authorised access only.#
```

Assign interface IP

```
interface <INTERFACE>
 description <PURPOSE>
 ip address <IP-ADDRESS> <SUBNET-MASK>
 no shutdown
```

SVI for switch management

```
interface vlan <VLAN-ID>
 ip address <IP-ADDRESS> <SUBNET-MASK>
 no shutdown
```

Save configuration

```
copy running-config startup-config
```

Create VLAN and assign access port

```
vlan <VLAN-ID>
 name <VLAN-NAME>
interface <INTERFACE>
 switchport mode access
 switchport access vlan <VLAN-ID>
```

Configure trunk port

```
interface <INTERFACE>
 switchport mode trunk
 switchport trunk native vlan <VLAN-ID>
 switchport trunk allowed vlan add <LIST>
```

SSH configuration

```
hostname <HOSTNAME>
ip domain name <DOMAIN>
crypto key generate rsa modulus 2048
ip ssh version 2
username <USERNAME> privilege 15
 secret <STRONG-UNIQUE-SECRET>
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
```

Basic DHCP pool

```
ip dhcp excluded-address <IP-ADDRESS>
ip dhcp pool <POOL-NAME>
 network <NETWORK> <SUBNET-MASK>
 default-router <IP-ADDRESS>
 dns-server <IP-ADDRESS>
```

Verification Commands

After configuring…	Run…	Check…
Interface IP	show ip interface brief	Status: up/up, correct address
VLAN and access port	show vlan brief	Port appears under correct VLAN
Trunk port	show interfaces trunk	VLAN in allowed and active list
SSH	show ip ssh	SSH Enabled, version 2.0
Configuration save	show startup-config	Matches running-config
ACL applied to interface	show ip interface <INTERFACE>	Inbound/outbound ACL listed

Cisco IOS Essential Commands

Page 3 — Troubleshooting Sequence

Cannot reach another subnet

Command	What to check
show ip interface brief	Interface up/up, correct address
show vlan brief	Port in correct VLAN
show interfaces trunk	VLAN allowed across trunk
show ip route	Route to destination exists
show access-lists	No ACL blocking traffic
ping / traceroute	Confirm path and return route

Switch port down or err-disabled

Command	What to check
show interfaces status	Connected/notconnect/err-disabled
show interfaces <INTERFACE>	Input errors, CRC, resets
show port-security interface	Violation count and secure MACs
show spanning-tree interface	Port role and STP state
show logging	Error reason for err-disabled port

VLAN not passing across trunk

Command	What to check
show vlan brief	VLAN exists on both switches
show interfaces trunk	VLAN in allowed and active STP list
show spanning-tree vlan	VLAN not blocked by STP

SSH access fails

Command	What to check
ping <MANAGEMENT-IP>	IP reachability from connecting host
show ip ssh	SSH enabled, version 2
show running-config | include	Local user account exists
show running-config | section	transport input ssh, login local

Cisco IOS Essential Commands

Page 4 — Security Principles and High-Risk Commands

Security Principles

Principle	Detail
Use SSH, not Telnet	transport input ssh on all VTY lines. Telnet transmits credentials in plaintext.
Prefer strong secrets	Use enable secret and username … secret. Avoid enable password. service password-encryption is not strong.
Restrict management access	Apply an ACL to VTY lines. Use a dedicated management VLAN or VRF where available.
Use named individual accounts	Avoid shared administrator accounts. Named accounts allow changes to be attributed.
Enable central logging	logging host <SYSLOG-SERVER>. Device buffer is lost on restart and not tamper-resistant.
Use accurate NTP	ntp server <NTP-SERVER>. Logs are meaningful only when the device clock is correct.
Protect configuration backups	Files may contain credentials and infrastructure details. Transmit and store securely.
Prefer SNMPv3	SNMPv1 and SNMPv2c transmit community strings in plaintext. Use SNMPv3 authPriv where supported.
Verify before saving	copy running-config startup-config only after confirming the change is correct.
Preserve console access	Confirm console or out-of-band access before changes that may disconnect you.

Commands to Treat with Extreme Caution

These commands can erase configuration, restart the device or immediately disconnect users. Require a current backup, console access

Command (name only — not for copying)	What it does
`write erase / erase startup-config`	Deletes saved configuration; device boots to defaults on next restart
`reload`	
`configure replace`	Replaces running configuration from a file
`default interface <INTERFACE>`	
`no vlan <VLAN-ID>`	Removes VLAN; disconnects all assigned ports
`shutdown (on active interface)`	

Plain-English takeaway

Confirm the command mode, inspect before changing, verify the result and save only what has been tested. Prefer SSH, named accounts, SNMPv3 and secure backup methods. Back up the configuration before any production change and keep console access available at all times.

Scan for online guide