How to Cisco

```
Who am I?
https://www.linkedin.com/in/propatriavigilans/
https://raymondrizzo.com
```

Switching

Basic Commands

Mode	Command	Description
SW	`enable`	Logs into enable mode
SW#	`write erase`	Reset configuration to factory default
SW#	`erase startup-config`	Another way to erase
SW#	`copy running-config startup-config`	Save running configuration
SW#	`reload`	Reboot device
SW#	`show mac address-table`	Show switch MAC Address table
SW#	`configure terminal`	Logs into configuration mode
SW#	`ping [destination]`	Ping IP or DNS address *(Optionally, add source [local-interface-ip] address)*
SW#	`show running-config`	Show current running configuration
SW#	`show startup-config`	Show startup configuration
SW#	`show running-config | begin [case-sensative-string]`	Show current running configuration starting at specified string
SW#	`show running-config | include [case-sensative-string]`	Include configuration items matching the specified string

Mode	Command	Description
ANY	`CTRL+SHIFT+6`	Interrupt running command/process

FTP

Mode	Command	Description
SW1#	`show flash`	Show contents of flash://
SW1(config)#	`ip ftp username [username]`	Set the username for FTP
SW1(config)#	`ip ftp password [a-strong-password]`	Set the password for FTP
SW1#	`copy flash ftp`	Copy file from flash to FTP. *(May require colon[:] at the end)*
SW1#	`copy flash tftp`	Copy file from flash to TFTP. *(May require colon[:] at the end)*

Basic Security

Mode	Command	Description
SW1#	`show users`	See who is logged into a device
SW1(config)#	`enable password [password]`	Set plain text enable password *(Please don't use this)*
SW1(config)#	`enable secret [password]`	Set encrypted enable secret
SW1(config)#	`username [User-Name] privilege {1..15} password [password]`	Create a user with an unencrypted password
SW1(config)#	`service password-encryption`	Encrypts any plain-text passwords in the configuration

AAA / RADIUS

Mode	Command	Description
SW1(config)#	`aaa new-model`	Enable AAA
SW1(config)#	`aaa authentication login default group radius local`	Set default login group for RADIUSand allow local failback on communication timeout
SW1(config)#	`aaa authorization exec default group radius local`	Set default authorization group for RADIUS and allow local failback on communication timeout
SW1(config)#	`radius-server host [aaa-host-address] auth-port 1812 acct-port 1813`	Set RADIUS server address on default ports
SW1(config)#	`radius-server host [aaa-host-address] key [strong-shared-key]`	Set encryption key to cisco for specified server
SW1(config)#	`line console 0`	Select console line 0
SW1(config-line)#	`login authentication default`	Set line login method to default group
SW1(config)#	`line vty 0 4`	Select VTY ports
SW1(config-line)#	`login authentication default`	Set line login method to default group

Telnet

I really *shouldn't* have to say why this shouldn't be used, but **don't use this since it's unencrypted**.

Mode	Command	Description
SW1(config)#	`line vty {0..15} {0..15}`	Configure telnet concurrent sessions

Mode	Command	Description
SW1(config-line)#	`password [password]`	Set password for telnet connections
SW1(config-line)#	`login`	Require logins for telnet sessions
SW1(config-line)#	`transport input telnet`	Specify telnet connections only

SSH

Mode	Command	Description
SW1(config)#	`hostname [Host-Name]`	Define a hostname for the device
SW1(config)#	`ip doman-name [Domain-Name]`	Define a domain name
SW1(config)#	`username [User-Name] password [password]`	Create a privileged user with an encrypted password]
SW1(config)#	`crypto key generate rsa`	Generate RSA key *(768+ required for SSHv2)*
SW1(config)#	`ip ssh version 2`	Select SSHv2
SW1(config)#	`line vty {0..15}`	Configure SSH for concurrent sessions
SW1(config-line)#	`login local`	Require local logins for SSH sessions
SW1(config-line)#	`transport input ssh`	Specify SSH connections only

NTP

Mode	Command	Description
SW1#	`show clock`	See current date and time

Mode	Command	Description
SW1(config)#	`clock timezone GMT -5`	Set timezone to -5UTC
SW1(config)#	`ntp master 1`	Set this as the NTP master clock
SW1(config)#	`clock summer-time GMT recurring second sun mar 2:00 first sun nov 2:00`	Set DST start time to the second Sunday of March and end on the first Sunday of November
SW1(config)#	`ntp source [interface-type-[x/x|xx/x/xx]]`	Allow this interface to serve NTP for network
SW1(config)#	`ntp server [ntp-host-address]`	Set NTP server synchronization with google
SW1(config)#	`do show ntp associations`	See any NTP associations on the device

SNMP

Mode	Command	Description
SW1(config)#	`access-list {1..99|100..199} permit host [snmp-host-address]`	Create ACL that allows one host
SW1(config)#	`access-list {1..99|100..199} deny any log`	Deny and log all other attempts to SNMP
SW1(config)#	`snmp-server community [snmp-community-name] ro {1..99|100..199}`	Set read only SNMP server with set community string for ACL
SW1(config)#	`snmp-server host [snmp-host-address] version 2c [snmp-community-name]`	Send SNMP2C messages to NMP collector with defined community string
SW1(config)#	`snmp-server group [snmp-group-name] priv`	Create encrypted SNMPv3 server with encrypted logins

Mode	Command	Description
SW1(config)#	`snmp-server user [snmp-user-name] [snmp-group-name] v3 auth sha [a-strong-password] priv aes 256 encryptpass access {1..99|100..199}`	Create user Ray with an encrypted password
SW1(config)#	`snmp-server host [snmp-host-address] informs version 3 pri [snmp-user-name]`	Send SNMP v3 messages encrypted to SNMP collector with verification of receipt

Syslog

Mode	Command	Description
SW1#	`terminal monitor`	Show syslog on ssh/telnet connections
SW1#	`show logging`	Check console/monitor/buffer logging status
SW1(config)#	`logging console`	Configure console logging options
SW1(config)#	`logging [syslog-server]`	Send logs to DNS name or IP address
SW1(config)#	`logging trap [logging-level]`	Set logging level *(Default = Informational)*

VLANs

Mode	Command	Description
SW1#	`show vlan / show vlan brief`	Shows all VLANS and non-trunk interfaces associated with VLANs
SW1(config)#	`vlan [VLAN-ID]`	Enter VLAN config mode *(Also creates VLAN in dat file)*

Mode	Command	Description
SW1(config-vlan)#	`name [ASCII-Name]`	Set name for VLAN
SW1(config-vlan)#	`remote-span`	Add the remote Switch Port Analyzer to the VLAN

VTP

Mode	Command	Description
SW1#	`show vtp status`	Shows VTP operational status and mode
SW1(config-if-range)#	`no vtp`	Safe bet is to disable this on every interface and only use it explicitly

CDP

Best practice would be to disable this globally, and only enable on trusted interfaces.

Mode	Command	Description
SW1(config)#	`cdp run`	Enables CDP globally
SW1(config)#	`cdp timer {5..254}`	Default = 60 seconds
SW1(config)#	`cdp holdtime {10..255}`	
SW1(config)#	`cdp no run`	Disables CDP globally
SW1(config-if)#	`no cdp enable`	Disables CDP per interface
SW1#	`show cdp neighbor`	Shows brief CDP neighbor information
SW1#	`show cdp neighbor detail`	Shows detailed CDP neighbor information

Mode	Command	Description
SW1#	`show cdp neighbor [interface-type-[x/x|xx/x/xx]] detail`	Show CDP information from one specific interface neighbor
SW1#	`show cdp`	Shows global CDP information (like timers)

LLDP

Best practice would be to disable this globally, and only enable on trusted interfaces.

Mode	Command	Description
SW1(config)#	`lldp run`	Enables LLDP globally
SW1(config-if)#	`no lldp transmit`	Do not trammit LLDP L2 messages on interface
SW1(config-if)#	`no lldp receive`	Ignore any LLDP L2 messages received on interface
SW1#	`show lldp [interface-type-[x/x|xx/x/xx]]`	Show LLDP stats and neighbor on interface
SW1#	`show lldp neighbors`	Shows brief LLDP neighbor informatio
SW1#	`show lldp entry [XXX]`	Details information regarding

Spanning Tree

Mode	Command	Description
SW1#	`show spanning-tree`	Show spanning tree configuration
SW1(config)#	`spanning-tree mode rapid-pvst`	Enable Cisco Rapid Per-VLAN Spanning Tree
SW1(config)#	`spanning-tree mode pvst`	Enable ieee STP

Mode	Command	Description
SW1(config)#	`spanning-tree mode mst`	Enable MST STP *Additional configuration required that is not shown*
SW1(config)#	`spanning-tree portfast default`	Enable portfast on all interfaces by
SW1(config)#	`spanning-tree bpduguard enable`	Don't receive BPDUs on this interface
SW1(config)#	`spanning-tree bpdufilter enable`	Don’t send or receive PBDUs on this interface

Interface Configuration

Mode	Command	Description
SW1#	`show interfaces`	Show interface configuration, counters, and line status
SW1#	`show interface status`	Shows interface line status
SW1#	`show interfaces switchport`	Shows configuration, line status and VLAN information for all switchports
SW1#	`show interfaces trunk`	Shows interface configuration and VLAN information for only trunk ports
SW(config)#	`interface fastEthernet 0/1`	Configure Fast Ethernet interface
SW1(config-if)#	`switchport mode trunk`	Set switchport to trunk port
SW(config-if)#	`interface gigabitEthernet 1/0/1`	Configure Gigabit Ethernet interface
SW1(config-if)#	`speed {10|100|1000|auto}`	Specify link speed for interface

Mode	Command	Description
SW1(config-if)#	`duplex {auto|full|half}`	Specify duplex speed for interface
SW1(config-if)#	`switchport access vlan {1..4094}`	Set VLAN for access port
SW1(config-if)#	`shutdown`	Disable interface
SW1(config-if)#	`no shutdown`	Enable interface

L2 EtherChannel

Mode	Command	Description
SW1(config)#	`interface range [interface-type-[x/x|xx/x/xx]]-[xx]`	Configure range of interfaces to be used in EtherChannel
SW1(config-if-range)#	`channel-group {1..model-dependent} mode on`	Enable static EtherChannel
SW1(config-if-range)#	`do show etherchannel summary`	Check EtherChannel status
SW1(config-if-range)#	`no channel-group mode on`	Disable static EtherChannel

L2 PAgP

Mode	Command	Description
SW1(config)#	`interface range [interface-type-[x/x|xx/x/xx]]-[xx]`	Configure range of interfaces to be used in PAgP
SW1(config-if-range)#	`channel-group {1..model-dependent} mode auto / desirable`	Enable PAgP on both sides (any combination other than auto on both)

Mode	Command	Description
SW1(config-if-range)#	`do show etherchannel summary`	Check EtherChannel status
SW1(config-if-range)#	`do show port-channel {1..model-dependent} etherchannel`	Check EtherChannel
SW1(config-if-range)#	`no channel-group mode on`	Disable PAgP
SW1(config-if-range)#	`no channel-group {1..model-dependent}`	Remove ports from channel group
SW1(config)#	`no interface port-channel {1..model-dependent}`	Delete channel group

L2 LACP

Mode	Command	Description
SW1(config)#	`interface range [interface-type-[x/x|xx/x/xx]]-[xx]`	Configure range of interfaces to be used in LACP
SW1(config-if-range)#	`channel-group {1..model-dependent} mode active / passive`	Enable PAgP on both sides (any combination other than passive on both)
SW1(config-if-range)#	`do show port-channel {1..model-dependent} etherchannel`	Check EtherChannel detailed stats
SW1(config-if-range)#	`do show etherchannel summary`	Check EtherChannel status
SW1(config-if-range)#	`no channel-group mode on`	Disable PAgP
SW1(config-if-range)#	`no channel-group {1..model-dependent}`	Remove ports from channel group

Mode	Command	Description
SW1(config)#	`no interface port-channel {1..model-dependent}`	Delete channel group

L3 EtherChannel

Mode	Command	Description
SW1(config)#	`interface range [interface-type-[x/x|xx/x/xx]]-[xx]`	Configure range of interfaces to be used in EtherChannel
SW1(config-if-range)#	`no switchport`	Change switchport to routed port
SW1(config)#	`interface port-channel {1..model-dependent}`	Configure actual port channel interface
SW1(config-if-range)#	`channel group {1..model-dependent} mode on`	Enable static EtherChannel
SW1(config-if)#	`ip address [ip-address] [subnet-mask]`	Set IP address for interface
SW1(config-if)#	`do show etherchannel summary`	Check EtherChannel status

Port Security

Mode	Command	Description
SW1(config-if)#	`switchport port-security`	Enables default port-security config *(1 MAC Address and shutdown violation)*
SW1(config-if)#	`switchport port-security violation shutdown`	Sets port security Shutdown mode
SW1(config-if)#	`switchport port-security violation protect`	Sets port security Protect mode

Mode	Command	Description
SW1(config-if)#	`switchport port-security violation restrict`	Sets port security Restrict mode
SW1(config-if)#	`switchport port-security maximum {1..132}`	Maximum number of allowed MAC Addresses on port before triggering violation. Up to 132 allowed *(platform dependent)*
SW1(config-if)#	`switchport port-security mac-address [mac-address]`	Define MAC Address to allow on port
SW1(config-if)#	`switchport port-security mac-address sticky`	Allow switch to learn MAC addresses *(up to maximum)*
SW1#	`show port-security`	General port-security information
SW1#	`show port-security address`	Port-security statistics
SW1#	`show port-security interface [interface-type-[x/x|xx/x/xx]]`	Port-security information for specific interface

Err-disable Recovery

Mode	Command	Description
SW1#	`show errdisable recovery`	See which errdisable timers are enabled.
SW(config)#	`errdisable recovery interval 30`	Recover after 30 seconds. Will err-disable again if security condition is not cleared

Mode	Command	Description
SW(config)#	`errdisable recovery cause all`	Enable err-disable recovery for all causes
SW(config)#	`errdisable recovery cause [specific-cause]`	Enable err-disable recovery for individual cause: arp-inspection bpduguard channel-misconfig *(STP)* dhcp-rate-limit dtp-flap gbic-invalid inline-power 12ptguard link-flap loopback mac-limit pagp-flap port-mode-failure pppoe-ia-rate-limit errdisable recovery cause psecure-violation psp sfp-config-mismatch security-violation small-frame storm-control udld vmps
SW#	`show errdisable flap-values`	Show flap reasons and current settings
SW(config)#	`errdisable flap-setting cause [specific-cause] max-flaps {1..100} time {1..120}`	Set values for individual flap causes: pagp-flap dtp-flap link-flap *I need to find the min-max*

SPAN (Switch Port Analyzer / Mirror)

Mode	Command	Description
SW(config)#	`no monitor session {1..model-dependent}`	Clear any previous settings
SW(config)#	`monitor session {1..model-dependent} destination vlan {1..4094}`	Set output VLAN for SPAN
SW(config)#	`monitor session {1..model-dependent} destination interface [interface-type-[x/x|xx/x/xx]]`	Set output interface for SPAN
SW(config)#	`monitor session {1..model-dependent} destination remote vlan {1..4094}`	Set output VLAN for RSPAN
SW(config)#	`monitor session {1..model-dependent} source`	Set interface/VLAN for to monitor with SPAN

IPv4 Subnets

Class C

CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Networks	2	4	8	16	32	64	128	256
Hosts	256	128	64	32	16	8	4	2
Mask	128	192	244	240	248	252	254	255
Value	128	64	32	16	8	4	2	1
Bit	8	7	6	5	4	3	2	1

Class B

CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Networks	2	4	8	16	32	64	128	256

CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	65536	32768	16384	8192	4096	2048	1024	512
Mask	128	192	244	240	248	252	254	255
Value	128	64	32	16	8	4	2	1
Bit	8	7	6	5	4	3	2	1

CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Networks	512	1024	2048	4096	8192	16384	32768	65536
Hosts	256	128	64	32	16	8	4	2
Mask	128	192	244	240	248	252	254	255
Value	128	64	32	16	8	4	2	1
Bit	8	7	6	5	4	3	2	1

Class A

CIDR	/9	/10	/11	/12	/13	/14
Networks	2	4	8	16	32	64
Hosts	16777216	8388608	4194304	2097152	1048576	524288
Mask	128	192	224	240	248	252
Value	128	64	32	16	8	4
Bit	8	7	6	5	4	3

CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Networks	512	1024	2048	4096	8192	16384	32768	655
Hosts	65536	32768	16384	8192	4096	2048	1024	512
Mask	128	192	244	240	248	252	254	255
Value	128	64	32	16	8	4	2	1

CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Bit	8	7	6	5	4	3	2	1

CIDR	/25	/26	/27	/28	/29	/30	
Networks	131072	262144	524288	1048576	2097152	4194304	
Hosts	256	128	64	32	16	8	
Mask	128	192	244	240	248	252	
Value	128	64	32	16	8	4	
Bit	8	7	6	5	4	3	

IPV6

If something is perfect, why reinvent the wheel? The following two items are from Wikipedia. https://en.wikipedia.org/wiki/IPv6_address

Multicast

Address	Description	Available Scopes
ff0X::1	All nodes address, identify the group of all IPv6 nodes	Available in scope 1 (interface-local) and 2 (link-local): • ff01::1 → All nodes in the interface-local • ff02::1 → All nodes in the link-local
ff0X::2	All routers	Available in scope 1 (interface-local), 2 (link-local) and 5 (site-local): • ff01::2 → All routers in the interface-local • ff02::2 → All routers in the link-local • ff05::2 → All routers in the site-local

Address	Description	Available Scopes
ff02::5	OSPF/IGP	2 (link-local)
ff02::6	OSPF/IGP designated routers	2 (link-local)
ff02::9	RIP routers	2 (link-local)
ff02::a	EIGRP routers	2 (link-local)
ff02::d	All PIM routers	2 (link-local)
ff02::1a	All RPL routers	2 (link-local)
ff0X::fb	mDNSv6	Available in all scopes
ff0X::101	All NTP servers	Available in all scopes
ff02::1:1	Link name	2 (link-local)
ff02::1:2	All-dhcp-agents (DHCPv6)	2 (link-local)
ff02::1:3	Link-local multicast name resolution	2 (link-local)
ff05::1:3	All-dhcp-servers (DHCPv6)	5 (site-local)
ff02::1:ff00:0/104	Solicited-node multicast address.	2 (link-local)
ff02::2:ff00:0/104	Node information queries	2 (link-local)

IPv6 Addressing

Prefix	Precedence	Label	Usage
::1/128	50	0	Localhost
::/0	40	1	Default
::ffff:0:0/96	35	4	IPv4-mapped IPv6 address
2002::/16	30	2	6to4

Prefix	Precedence	Label	Usage
2001::/32	5	5	Teredo tunneling
fc00::/7	3	13	Unique local address
::/96	1	3	IPv4-compatible addresses *(deprecated)*
fec0::/10	1	11	Site-local address *(deprecated)*
3ffe::/16	1	12	6bone *(returned)*