VTP

Server	Client	Transparent
create/modifies/deletes VLANs	synchronizes VTP information	create/modifies/deletes VLANs
synchronizes VTP information	originates VTP advertisements	stores VLAN info in NVRAM
originates VTP advertisements	forwards VTP advertisements	forwards VTP advertisements
forwards VTP advertisements		
stores VLAN info in NVRAM		

Default mode: **Server** Default version: **1** Default domain: **null**

Higher revision number in same domain = update VLAN database to match

To reset revision to 0 = Change VTP domain or VTP mode to transparent

cAse-Sensitive Domain, Password and VTP version must match

Banner

Banner motd	Message of the day (temp)
Banner login	Message at login (permanent)
Banner exec	Message at enable (permanent)

Serial interfaces

Doesn't use ARP

Clock rate on DCE (Female)

HDLC default encapsulation

VLANs

Usable VLAN Range	1-4094 (12-bit)
Default VLANs	1,1002-1005 (5 total)
Normal Range	1-1005
Extended Range	1006-4096

Port numbers

Routing metric (best path)

Protocol	Metric
RIP	Lowest hop count
OSPF	Lowest cost
EIGRP	Highest bandwidth, lowest delay
BGP	Shortest AS path

IPv6 dynamic routing

RIPng, EIGRP for IPv6, OSPFv3, MP-BGPv4

Classless routing (includes /mask)

Classless	RIPv2, OSPF, EIGRP, BGP
Classful	RIPv1, IGRP

Static route types

Directly connected	Exit-interface
Recursive	Nexthop-IP
Fully specified	Exit-interface+nexthop IP
Floating static	Higher AD >1

Max age defaults

MAC table	300
Errdisable recovery	300

Timers

OSPF DR/BDR election

1) Highest priority (0-255, 1 = default)

2) Highest router-id (x.x.x.x)

BDR will be second highest

Change require new election and **clear ip ospf process**

OSPF default cost (100 Mbps)

Reference BW	100 Mbps	100 000 Mbps
Speed	**Cost**	**Cost**
10 Mbps	10	10000
100 Mbps	1	1000
1000 Mbps	1	100
10 000 Mbps	1	10
100 000 Mbps	1	1

Auto-cost reference-bandwidth <> (same on all OSPF routers)

OSPF multicast

OSPF Routers **HELLO**	224.0.0.5
OSPF Designated Routers **LSAs**	224.0.0.6

OSPF states

Down

Init

2-Way

Exstart

Exchange

Loading

Full

SDN architecture

TCP	UDP	TCP & UDP
FTP data (20)	DHCP server (67)	DNS (53)
FTP control (21)	DHCP client (68)	
SSH (22)	TFTP (69)	
Telnet (23)	SNMP agent (161)	
SMTP (25)	SNMP manager Trap (162)	
HTTP (80)	Syslog (514)	
HTTPS (443)	CAPWAP control (5246)	
	CAPWAP data (5247)	
Chef (10002)		
Puppet (8140)		
Ansible (22)		
Salt (4505)		
TACACS+ (49)	RADIUS (1812+1813)	

Protocol	HELLO / Holdtime
CDP (L2)	60 / 180
LLDP (L2)	30 / 120
OSPF (L3)	10 / 40 (x4)
EIGRP (L3)	5 / 15
STP forward delay (L2)	15
HSRP (L3)	3 / 10

IPv4 Protocol field	
Value	**Protocol**
1	ICMP
6	TCP
17	UDP
88	EIGRP
89	OSPF

Application layer	App --> Controller (NBI)
Control layer	SDN controller receives instructions
Infrastructure layer	Controller --> devices (SBI)

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

API

Northbound API	REST API (*format* JSON, XML, OSGi)
Southbound API	NETCONF, RESTCONF, OpenFlow, OpFlex, onePK

Automation = script to one device

Orchestration = scripts to many devices

Southbound SBI

OnePK	Cisco proprietary API
OpenFlow	uses an **imperative** SDN model
OpFlex	uses a **declarative** SDN model
NETCONF	uses XML and RPC

OSPF timers

OSPF type	Hello	Hold
Broadcast	10	40
Nonbroadcast	30	120
Point-to-point	10	40
Point-to-multipoint broadcast	30	120
Point-to-multipoint nonbroadcast	30	120

OSPF network type default

Network	Default	DR/BDR election	Manuel neighbor
Broadcast	Ethernet, FDDI	Yes	No*
Nonbroadcast	Frame Relay, X.25	Yes	Yes
Point-to-point	PPP, HDLC	No	No*
Point-to-multipoint		No	No*
Point-to-multipoint nonbroadcast		No	Yes

*Uses multicast to form neighbor adjacency

Routing algorithm

OSPF/IS-IS	Dijkstra
EIGRP	Diffusing Update ALgorithm (DUAL)
RIP	Bellman-Ford

Wireless QoS

Platinum	Voice (highest priority)
Gold	Video
Silver	Best effort (default)
Bronze	Background (lowest priority)

Dynamic routing

Linkstate	OSPF, IS-IS
Distance vector	EIGRP, RIP
Path vector	BGP

Multicast groups

Protocol	IPv4	IPv6
All notes/host broadcast	224.0.0.1	
HSRPv1	224.0.0.2	FF02::5/16
OSPF HELLO (ALL)	224.0.0.5	FF02::5
OSPF LSA (DR->DROTHER)	224.0.0.6	FF02::6
EIGRP	224.0.0.10	FF02::A
VRRP	224.0.0.18	ff02::12
GLBP	224.0.0.102	
HSRPv2	224.0.0.102	

Port status codes

Hardware status	Line Protocol status	Typical reason

Port status codes (cont)

administratively down	down	Has **shutdown** command configured
down	down	Has **no shutdown** configured, but an error on the physical layer e.g. no cable connected or the other end is shut down
up	down	Data link (L2) error e.g. wrong encapsulation HDLC-->PPP or Ethernet
up	up	All is well and good

Syslog severity

Severity level 0-7	Name
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notification
6	Informational
7	Debugging

Every Awesome Cisco Engineer Will Need Ise Daily

By default, syslog servers receive **informational messages (level 6)**.

FHRP virtual MAC

Protocol	MAC
HSRPv1	0000.0c07.ac**xx**
HSRPv2	0000.0c9f.f**xxx**
VRRP	0000.5E00.01**xx**
GLBP	007.B400.**xxyy**

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Multicast MAC addresses

Protocol	MAC
CDP	0100.0CCC.CCCC
LLDP	0180.C200.000E

IPv6 address types

Group	IPv6 address group
Global Unicast	**2**000::/3
Link-local	**fe**80::/10
Unique-Local	**fc**00::/7
Unique-Local (new)	**fd**00::/8
Multicast	**ff**00::/8
Default route	**::/0**
Loopback	**::1**

IPv6 multicast groups (FF00::/8)

FF**01**::/16	node-local
FF**02**::/16	link-local
FF**05**::/16	site-local
FF**08**::/16	organization-local
FF**0E**::/16	global

ACL range

Standard numbered	1-99
Standard named	1-99
Extended numbered	100-199
Extended named	100-199
Standard ACL as close to **destination** as possible	
Extended ACL as close to **source** as possible	

SNMP

Class	Message	Sent by
Read	Get GetNext GetBulk	NMS
Write	Set	NMS
Notification	Trap Inform	Agent
Response	Reponse	Agent

HTTP status code

Class	Response status code
1xx *inform-ational*	102 Processing
2xx *successful*	200 OK 201 Created
3xx *redirection*	301 Moved Permanently
4xx *client error*	400 Bad Request 401 Unauthorized 403 Forbidden 404 Not Found 408 Request Timeout
5xx *server error*	500 Internal Server Error

CRUD REST API (HTTP)

Purpose	CRUD operation	HTTP Verb
Create new variable	**Create**	POST
Retrieve variable	**Read**	GET
Change variable	**Update**	PUT, PATCH
Delete variable	**Delete**	DELETE

REST API encoding

Serialized format
JSON
XML
YAML

Power policing

power inline police (default)	Disables port and send syslog. Must be re-enabled with shutdown and no shutdown
power inline police action err-disable	Same as power inline police

Power policing (cont)

power inline police action log	does NOT shut down but **restarts** the interface and sends syslog

EIGRP K-values

K1	Bandwidth	Lowest bandwidth of the route
K3	Delay	Cumulative interface delay of the route

Administrative Distance (Lower is better)

Source	Default Distance	Table Entry
Directly Connected	0	C
Static	1	S
eBGP	20	B
EIGRP	90	D
OSPF	110	O
ISIS	115	i
RIP	120	R
External EIGRP	170	D EX
iBGP	200	B
Unkown	255	

Packet Forwarding Decision

1)	Longest Prefix Match /
2)	Gateway of last resort
3)	Drop

Spanning Tree

Default STP on Cisco	PVST+
PVST+ and RSTP compatible?	Yes
Rapid PVST	802.1w
Legacy STP	802.1d

By **Emil1502**
cheatography.com/emil1502/

Published 5th February, 2025.
Last updated 13th August, 2022.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

STP port election

Root bridge

1: Lowest bridge ID (superior)

Root port election

1: Lowest root cost

2: Lowest neighbor bridge ID

3: Lowest neighbor port ID

Designated port (per collision domain)

1: Interface on switch with lowest root cost

2: Interface on switch with lowest bridge ID

STP cost

Speed	Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Port states

Legacy STP (802.1D)	Rapid STP (802.1W)
Disabled Blocking Listening	Discarding
Learning	Learning
Forwarding	Forwarding

Port Roles

Legacy STP (802.1D)	Rapid STP (802.1w)
Root	Root
Designated	Designated
Blocking	Alternate
	Backup (shared link, hub)

WLC Interfaces (Logical)

Management interface	MGMT traffic, CAPWAP tunnels are formed to/from this interface

WLC Interfaces (Logical) (cont)

Redundancy MGMT interface	Two WLCs connected as 'active' and 'standby'
Virtual interface	Communicate with wireless clients e.g. relay DHCP requests
Service port interface	Out-of-band MGMT bound to service port
Dynamic interface	Used to map WLAN to a VLAN bound to port

Autonomous AP

Locally switched

Trunk/tagged between Distribution System (DS) and AP

Configured via Telnet, SSH or HTTP (GUI)

No central monitoring or management

Lightweight AP

Centrally controlled by WLC

Split-MAC architecture

Control and Provisioning of Wireless Access Points protocol (CAPWAP)

CAPWAP tunnel UDP 5246 (control) 5247 (data)

AP connect to access port

Local mode traffic can not be locally switched (default mode)

FlexConnect can be locally switched when CAPWAP is down

Modes: Local, flexConnect, monitor, sniffer, rogue detector, bridge, SE-Connect

Default console settings

9600 bits/second

8-bit ASCII

No parity bits

No flow control

1 stop bit

WLC controller

Max. 512 dynamic interfaces (WLANS)

Telnet timeout 5 min (Default)

Wireless security

Version	Authentication	Encryption+MIC
WPA	PSK	TKIP (RC4)
WPA-2	PSK	AES 128 CCMP
WPA-3	SAE (replaces PSK)	AES 256 GCMP

SAE - Simultaneous Authentication of Equals

PMF - Protected Management Frame: Protects 802.11 mgmt frames

Forward Secrecy prevents decryption after transmitted

EAP authentication

Method	Process
LEAP (Cisco)	Mutual authentication (least secure)
EAP-FAST (Cisco)	Uses a client PAC key
PEAP	1-way server side certificate
EAP-TLS	2-way server and client certificate (best)

Port violation modes

Mode	Disable interface	Increment counter	Syslog
Protect	No	No	No
Restrict	No	Yes	Yes
Shutdown	Yes	Yes	Yes

Protect+Restrict discard traffic from unauthorized MACs (filter)

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Enable SSH

1) Configure hostname *(other than Router or Switch)*

2) Configure domain name

3) Generate RSA keys

4) Transport input SSH on vty lines

Security methods

1) Something you know (Password, Pin)

2) Something you have (Card, Phone MFA)

3) Something you are (Biometric)

Site-to-site VPN (4 steps)

1) Combines session/encryption key with data and **encrypt both the data and the key**

2) The sending device **encapsulates** the encrypted data and session key and **adds a VPN header and a new IP header**

3) Sending device **sends the completed packet** to the destination device (other end of tunnel)

4) The destination or receiving device **decrypt the packet** with the sessions key

PCP CoS values (3-bit) voice

0	Best effort (default all traffic)
3	Critical application (IP phones mark call signaling traffic with 3)
5	Voice (IP phones mark voice traffic with 5)

One-way delay: 150 ms or less

Jitter: 30 ms or less

Loss: 1% or less

Voice is **AF46** expedited forwarding EF

Configuration Register

0x2102	Factory default, load IOS from flash to NVRAM
0x2100	Load ROM monitor mode
0x2142	Load IOS from Flash without startup-config

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com