CCNA 200-301 Reference Document

1 Layer 1 Standards

1.1 T568A/B Pinout Standards

Pin	T568A	T568B	MDI	MDI-X
1	Green-White	Orange-White	Tx	Rx
2	Green	Orange	Tx	Rx
3	Orange-White	Green-White	Rx	Tx
4	Blue	Blue		
5	Blue-White	Blue-White		
6	Orange	Green	Rx	Tx
7	Brown-White	Brown-White		
8	Brown	Brown		

Two standard T568 pinouts exist for the *Medium-Dependent Interface* (MDI) and *MDI Crossover* (MDI-X) port standards. Computers, routers, and Layer 3 devices use the MDI standard; switches, hubs, and other Layer 2 devices use the MDI-X standard. Connections between MDI and MDI-X ports use a *straight-through* cable, where the same T568 standard terminates each end of the cable. Connections between two MDI (or two MDI-X) ports use a *crossover* cable, where different T568 standards terminate each end of the cable. Most new equipment incorporates *Auto-MDIX* circuitry to allow either cable type.

Note: The T568B standard is more commonly used for straight-through cables in North America.

1.2 Cabling Standards

Table 1.1: IEEE 802.3 Copper Standards

802.3	10BASE-T	10 Mbps	CAT3
802.3u	100BASE-T	100 Mbps	CAT5
802.3ab	1000BASE-T	1 Gbps	CAT5e
802.3z	1000BASE-SX 1000BASE-LX	1 Gbps 1 Gbps	550m Fiber 5km Fiber
802.3an	10GBASE-T	10 Gbps	CAT6a
802.3ba	40GBASE-T	40 Gbps	CAT8
802.3bz	2.5GBASE-T 5GBASE-T	2.5 Gbps 5 Gbps	CAT5e CAT5e

Table 1.2: Fiber Standards

OM1	orange	100 Mbps
OM2	orange	1 Gbps
OM3	aqua	10 Gbps 40 Gbps 100 Gbps
OM4	aqua	10 Gbps 40 Gbps 100 Gbps
OM5	lime	10 Gbps

Table 1.3: SFP Transceivers

SX SR	850 nm	**black** MMF	550 m 300 m
LX/LR	1310 nm	blue SMF	10-20 km
——	1490 nm	purple SMF	——
EX/ER ZX/ZR	1550 nm	yellow SMF	40 km 80 km

Table 1.4: Power over Ethernet (PoE)

Cisco Inline Power	ILP	7.5W	2 wire pairs
IEEE 802.3af	Type 1 PoE	15W (44-57v)	2 wire pairs $\geq$ CAT3
IEEE 802.3at	Type 2 PoE+	30W (50-57v)	2 wire pairs $\geq$ CAT5
IEEE 802.3bt	Type 3 UPoE	60W (50-57v)	4 wire pairs $\geq$ CAT5
	Type 4 UPoE+	100W (52-57v)	4 wire pairs $\geq$ CAT5

2 Layer 2 Protocols

Table 2.1: EtherType Values

`0x0800`	IPv4 Packet
`0x0806`	ARP
`0x2000`	Cisco CDP
`0x8100`	IEEE 802.1Q
`0x86dd`	IPv6 Packet
`0x8809`	Ethernet Slow Protocols
`0x8847`	MPLS Unicast
`0x8848`	MPLS Multicast
`0x8863`	PPPoE Discovery
`0x8864`	PPPoE Session
`0x88cc`	LLDP
`0x888e`	IEEE 802.1x EAPOL

Table 2.2: Layer 2 Multicast

`0000.0c07.acXX`	Cisco HSRPv1
`0000.0c9f.fXXX`	Cisco HSRPv2
`0000.5e00.01XX`	IETF VRRP
`0007.b40X.XXYY`	Cisco GLBP
`0100.5eXX.XXXX`	IPv4 Multicast
`3333.XXXX.XXXX`	IPv6 Multicast
`0100.0ccc.cccc`	Cisco CDP / VTP / UDLD
`0180.c200.000e`	IEEE 802.1AB LLDP
`0100.0ccc.cccd`	Cisco PVST+ / PVRST
`0180.c200.0000`	IEEE 802.1D STP IEEE 802.1w RSTP

Note: Each Layer 2 multicast address maps to a corresponding Layer 3 multicast address which may be used in the L3PDU. Some Layer 2 protocols do not support multicast.

2.1 Ethernet II / IEEE 802.3

Preamble	7 Bytes	10101010
SFD	1 Byte	10101011
Destination MAC	6 Bytes	
Source MAC	6 Bytes	
Type (Ethernet II) Length (802.3)	2 Bytes	EtherType (Table 2.1) Payload Length in Bytes
Data	varies	46-1500 Bytes based on MTU
FCS	4 Bytes	

Table 2.3: IEEE 802.2 Logical Link Control (LLC)

Destination Service Access Point (DSAP)	1 Byte
Source Service Access Point (SSAP)	1 Byte
Control	1-2 Bytes

Table 2.4: IEEE SubNetwork Access Protocol (SNAP)

Organizationally Unique Identifier (OUI)	3 Bytes	
Type	2 Bytes	EtherType (Table 2.1)

2.2 VLAN Tagging

Table 2.5: IEEE 802.1Q Tagging

Tag Protocol Identifier (TPID)	16 bits	EtherType (`0x8100`, Table 2.1)
TCI: Priority Code Point (PCP)	3 bits	QoS Class-of-Service (CoS) Marking (Section 6)
TCI: Drop Eligible Indicator (DEI)	1 bit	QoS Drop Eligiblity
VLAN ID	12 bits	

Table 2.6: DEPRECATED Cisco InterSwitch Link (ISL)

Destination Address	40 bits	Multicast (`01.000c.0000` / `03.000c.0000`)
Type	4 bits	Frame Type
User	4 bits	Priority Handling
Source Address	48 bits	Sending Switchport MAC
LEN	16 bits	Original Frame Length
AAAA03	24 bits	SNAP/LLC Field (`0xaaaa03`)
HSA	24 bits	Source Address OUI (`0000.0c`)
VLAN	15 bits	VLAN ID
BPDU Flag	1 bit	Flag BPDU / CDP / VTP frames
INDEX	16 bits	Diagnostics
RES	16 bits	Token Ring / FDDI Frames
Data	varies	8-196000 bit Unmodified original frame
FCS	32 bits	

Note: Industry-standard IEEE 802.1Q supports both *normal-range* VLANs (1-1005) and *extended-range* VLANs (1006-4094); Cisco ISL is deprecated.

2.3 Cisco VLAN Trunking Protocol (VTP)

Cisco VTP dynamically advertises a *VLAN Database* to participating switches over Cisco ISL and IEEE 802.1Q trunk links. Participating switches use either *VTP Server Mode* or *VTP Client Mode*, and default to VTP Server Mode with a `Config Revision Number` of 0. Each time a VTP Server's VLAN Database is locally updated, the `Config Revision Number` increments and *VTP Synchronization* occurs.

VTP Synchronization uses a *VTP Summary Advertisement* alongside 1 or more *VTP Subset Advertisements* to advertise the revised VLAN Database. VTP Servers also send out a Summary Advertisement (alongside 0 or more Subset Advertisements) every 5 minutes. To participate, newly-connected switches may send a *VTP Advertisement Request* over each trunk link that comes up. A switch only listens to VTP messages in its `VTP Management Domain` (default NONE). An MD5-encrypted `VTP Password` (default NONE) can be configured to prevent unauthorized switches from participating in the VTP Management Domain.

VTP Clients participate in VTP Synchronization but disallow local VLAN configurations. *VTP Transparent Mode* or *VTP Off Mode* switches use a local VLAN configuration instead of the VLAN Database, although they may forward VTP messages.

Table 2.7: VTP Summary Advertisement

Version	1 Byte	VTP Version (1-3)
Code	1 Byte	Summary Advertisement (`0x01`)
Followers	1 Byte	Indicates a Subset Advertisement
MgmtD Len	1 Byte	
Management Domain	32 Bytes	VTP Domain Name
Config Revision Number	4 Bytes	
Updater Identity	4 Bytes	Originating VTP Server (IP Address)
Update Timestamp	12 Bytes	Datetime of revision
MD5 Digest	16 Bytes	VTP Password hash (if configured)

Table 2.8: VTP Subset Advertisement

Version	1 Byte	VTP Version (1-3)
Code	1 Byte	Subset Advertisement (`0x02`)
Sequence Number	1 Byte	Sequence in packet stream following Summary Advertisement
MgmtD Len	1 Byte	
Management Domain	32 Bytes	VTP Domain Name
Config Revision Number	4 Bytes	
VLAN-Info Field(s)	4 Bytes	Advertised VLAN(s) (Table 2.9)

Table 2.9: The VLAN-Info Field

V-Info-Len	1 Byte
Status	1 Byte
VLAN-Type	1 Byte
VLAN-Name Len	1 Byte
ISL VLAN-ID	2 Bytes
MTU Size	2 Bytes
802.10 Index	4 Bytes
VLAN-Name	4 Bytes

Table 2.10: Advertisement Requests

Version	1 Byte	VTP Version (1-3)
Code	1 Byte	Advertisement Request (`0x03`)
Reserved	1 Byte	
MgmtD Len	1 Byte	
Management Domain	32 Bytes	VTP Domain Name
Start-Value	32 Bytes	Identifies the requested Subset Advertisement

2.4 IEEE 802.1D Spanning-Tree Protocol / IEEE 802.1w Rapid STP (RSTP)

Protocol Identifier	2 Bytes	0 for STP / PVST+
Version	1 Byte	0 for STP / PVST+ 2 for RSTP / PVRST
Message Type	1 Byte	Identify Configuration / TCN BPDUs (`0x02` for RSTP/MSTP)
Flags	1 Byte	Signals TC / TCA bits
Root ID	8 Bytes	The sender's Root BID (Table 2.11)
Root Path Cost	4 Bytes	The sender's cost to Root
Bridge ID	8 Bytes	The sender's BID (Table 2.11)
Port ID	2 Bytes	The sender's `Port Prio.Nbr`
Message Age	2 Bytes	Time since Root sent this BPDU
Max Age	2 Bytes	Time until BPDU expires
Hello Time	2 Bytes	How often Root sends BPDUs
Forward Delay	2 Bytes	Time spent in each transition state

Table 2.11: Spanning Tree Bridge ID (BID) Format

Base Priority	4 bits	Configured bridge priority (multiple of 4096)
System ID Extension	12 bits	The VLAN ID of this STP instance
System ID	48 bits	The bridge *Burned-In Address* (BIA)

Table 2.12: Spanning Tree Port Costs

Port Speed	STP IEEE Cost	Revised IEEE Cost	RSTP IEEE Cost
10 Mbps	100	100	2,000,000
100 Mbps	10	19	200,000
1 Gbps	1	4	20,000
10 Gbps	1	2	2,000
100 Gbps	-	-	200
1 Tbps	-	-	20
10 Tbps	-	-	2

Table 2.13: Spanning Tree Port States

STP State	RSTP State	Send/Receive BPDUs	Forward Data	Learn MACs
Disabled	Discarding	**No**	**No**	**No**
Blocking	Discarding	**Receive**	**No**	**No**
Listening	—	**Yes**	**No**	**No**
Learning	Learning	**Yes**	**No**	**Yes**
Forwarding	Forwarding	**Yes**	**Yes**	**Yes**

The *STP Convergence* Process:

1. **Elect Root Bridge:**

   (a) Lowest BPDU `Root ID: Priority`

   (b) Tiebreaker: lowest BPDU `Root ID: System ID`

2. **Elect *Root Ports* (RPs):**
   (a) Lowest received BPDU `Root Path Cost` + local `Port Cost` (Table 2.12)
   (b) Tiebreaker: lowest received BPDU `Sender BID`
   (c) Tiebreaker: lowest received BPDU `Port ID: Prio.Nbr`
   (d) Other RSTP link-type point-to-point ports become *Alternate Ports* (APs)
3. **Elect *Designated Ports* (DPs):**
   (a) Lowest advertised BPDU `Root Path Cost`
   (b) Tiebreaker: lowest advertised BPDU `Sender BID`
   (c) Tiebreaker: lowest advertised BPDU `Port ID: Prio.Nbr`
   (d) Other RSTP link-type shared ports on the same bridge become *Backup Ports* (BPs)
4. **Other Ports:**
   (a) Working ports become STP *Nondesignated Ports* (NDs)
   (b) Nonworking and disabled ports become STP disabled ports

Optional STP Features:

- **PortFast:** immediately transitions configured ports to Forwarding state when connected. It can be enabled on access or trunk ports, and continues to send BPDUs. Received BPDUs cause the port to revert to STP behavior.
- **BPDU Guard:** err-disables configured ports which receive a BPDU, preventing unauthorized devices from altering the STP topology. It can be globally enabled on all PortFast ports, and continues to send BPDUs.
- **BPDU Filter:** stops configured ports from sending BPDUs when configured globally; locally configured ports also ignore received BPDUs (effectively disabling STP). It can be globally enabled on all PortFast ports alongside BPDU Guard without issue; local configuration effectively disables BPDU Guard.
- **Root Guard:** protects the STP topology by disabling configured ports which receive a superior BPDU. This prevents DPs from becoming RPs. Affected ports enter the Broken (Root Inconsistent) state and are disabled by STP; they are automatically enabled when the issue is resolved. Incompatible with Loop Guard.
- **Loop Guard:** protects against undetected *Unidirectional Links* by disabling configured ports whose `Max Age` timer reaches 0. This prevents RPs and NDs from becoming DPs. Affected ports enter the Broken (Loop Inconsistent) state and are disabled by STP; they are automatically enabled when the issue is resolved. Incompatible with Root Guard.

2.5 Address Resolution Protocol (ARP)

Table 2.14: ARP Request/Reply Format

HTYPE	16 bits	L2 Protocol (1 for Ethernet)
PTYPE	16 bits	L3 Protocol (EtherType Table 2.1)
HLEN	8 bits	L2 Address Length in Bytes
PLEN	8 bits	L3 Address Length in Bytes
Operation	16 bits	Message Type (1 for Request, 2 for Reply)
Origin HW	48 bits	Source MAC
Origin IP	32 bits	Source IP
Target HW	48 bits	Destination MAC
Target IP	32 bits	Destination IP

Note: As a Layer 2 protocol, all IPv4 ARP messages are encapsulated directly within an Ethernet frame.

Dynamic ARP Inspection (DAI) is an optional switch security feature to prevent ARP poisoning and ARP DoS. It uses the *DHCP Snooping Binding Table* to filter incoming ARP messages based on their `Origin IP` and `Origin HW` fields; an ARP ACL can also be configured for hosts using static IP addresses. Optional verification checks compare the ARP `Origin/Target HW` fields against the frame `Source/Destination MAC` and ensure the ARP `Origin/Target IP` fields contain unicast values. This behavior is disabled on DAI *trusted ports*. DAI uses optional per-interface rate limits to prevent DoS attacks against the switch CPU and ARP table.

2.6 IEEE 802.11 Wireless LANs (WLANs)

Frame Control	2 Bytes	Message Type / Subtype
Duration / ID	2 Bytes	Frame Transmission Time / Client Association
Address 1	6 Bytes	Dst / Src / Rx / Tx Address
Address 2	6 Bytes	Dst / Src / Rx / Tx Address
Address 3	6 Bytes	Dst / Src / Rx / Tx Address
Sequence Control	2 Bytes	Fragmentation / Duplication Management
Address 4	6 Bytes	Dst / Src / Rx / Tx Address
QoS Control	2 Bytes	Section 6
HT Control	4 Bytes	HT Operations (802.11n and later)
Data	varies	
FCS	4 Bytes	

The original IEEE 802.11-1997 standard uses *Frequency Hopping Spread Spectrum* (FHSS) encoding within the 2.4-GHz ISM band. Each consecutive transmission uses a slightly different frequency to minimize collision risk; there are no defined discrete channels.

Direct Sequence Spread Spectrum (DSSS) encoding uses 11 overlapping channels within the 2.4-GHz ISM band, three of which are non-overlapping. *Orthogonal Frequency Division Multiplexing* (OFDM) encoding uses 23 overlapping channels within the 5-GHz U-NII band. Both are used by modern IEEE 802.11 standards along with *Carrier Sense Multiple Access / Colision Detection* (CSMA-CD) to minimize and recover from collisions.

Table 2.15: IEEE 802.11 Standards

Standard	Frequency Range	Bandwidth	Encoding	Name
-1997	2.4 GHz	2 Mbps	FHSS/DSSS	
b	2.4 GHz	11 Mbps	DSSS	
a	5 GHz	54 Mbps	OFDM	
g	2.4 GHz	54 Mbps	OFDM	
n	2.4 / 5 GHz	600 Mbps	OFDM	Wi-Fi 4 (HT)
ac	5 GHz	6.93 Gbps	OFDM	Wi-Fi 5 (VHT)
ax	2.4 / 5 GHz 6 GHz	9.6 Gbps	OFDM	Wi-Fi 6 (HE) Wi-Fi 6e
be	2.4/5/6 GHz	46 Gbps	OFDM	Wi-Fi 7 (EHT)

Table 2.16: WLC Deployment

Deployment	WLC Location	Clients	APs
Unified	Central	64,000	6,000
Cloud	Data Center	32,000	3,000
Embedded	Access Switch	4,000	200
Mobility Express	LAP	2,000	100

Table 2.17: WLC Ports and Interfaces

WLC Port	WLC Interface	VLAN	Usage
Console			Initial config
Service Port	Service Port	OOB-MGMT	Out-Of-Band mgmt (access port) bootup / system recovery
Redundancy	Redundancy Management	MGMT	In-Band mgmt (standby WLC) HA redundancy
DS	Management	MGMT	In-Band mgmt (active WLC) Form CAPWAP tunnels
DS	Virtual	Mobility Group	DHCP Relay, WebAuth
DS	Dynamic	USERS	Bind WLANs to VLANs (tunnel LAG)

Note: Only Lightweight APs require a *Wireless LAN Controller* (WLC) deployment to support WLANs. Each Autonomous AP can support multiple independent WLANs.

Autonomous AP Modes:

- **Infrastructure:** Offer BSS' on an RF Channel
- **Repeater:** Extend a BSA via retransmission
- **WorkGroup Bridge (WGB):** Bridge wired device(s) to a WLAN
- **Bridge:** Form a P2P / P2MP link between LANs
- **Mesh:** Bridge traffic across APs in a large service area

Lightweight AP (LAP) Modes:

- **Local:** Offer BSS' on an RF Channel
- **Monitor:** Monitor for IDS events / rogue APs, determine STA positions

- **FlexConnect:** Locally switch traffic if CAPWAP fails
- **Rogue Detector:** Detect rogue devices (correlate wired and wireless MACs)
- **Sniffer:** Capture WLAN traffic for analysis
- **Bridge:** Form a P2P / P2MP link or a mesh
- **Flex+Bridge:** FlexConnect on a mesh LAP
- **SE-Connect:** Detect interference sources (RF spectrum analysis)

2.7 ITU High-Level Data-Link Control (HDLC)

Flag	1 Byte	Synchronization
Address	1 Byte	Destination Node
Control	1 Byte	
Data	varies	
FCS	4 Bytes	

2.8 IETF RFC 1661 Point-to-Point Protocol (PPP) / Cisco HDLC (cHDLC)

Flag	1 Byte	Synchronization
Address	1 Byte	Destination Node
Control	1 Byte	
Type	2 Bytes	EtherType (Table 2.1)
Data	varies	
FCS	4 Bytes	

3 Layer 3 Protocols

Table 3.1: IPv4 Protocol / IPv6 Next Header Values

`0x01`	1	ICMP
`0x02`	2	IGMP
`0x04`	4	IPv4
`0x06`	6	TCP
`0x11`	17	UDP
`0x29`	41	IPv6
`0x2f`	47	GRE
`0x3a`	58	ICMPv6
`0x58`	88	EIGRP
`0x59`	89	OSPF
`0x67`	103	PIM
`0x70`	112	VRRP
`0x89`	137	MPLS-in-IP

Table 3.2: Layer 3 Multicast

224.0.0.1 `ff02::1`	All-IPv4-Nodes All-IPv6-Nodes	
224.0.0.2 `ff02::2`	All-IPv4-Routers All-IPv6-Routers	Cisco HSRPv1
224.0.0.5 `ff02::5`	All-SPF-Routers	OSPFv2 OSPFv3
224.0.0.6 `ff02::6`	All-SPF-DRs	OSPFv2 OSPFv3
224.0.0.9 `ff02::9`	All-RIP-Routers	RIPv2 RIPng
224.0.0.10 `ff02::a`	All-EIGRP-Routers All-EIGRPv6-Routers	EIGRP EIGRPv6
224.0.0.18	IETF VRRP	
224.0.0.102	Cisco HSRPv2 / GLBP	

Note: Each Layer 3 multicast address maps to a corresponding Layer 2 multicast address which may be used in the L2PDU.

Table 3.3: Route Types

Route Type	Administrative Distance	IGP Type
Connected	0	
Static	1	
BGP	20	EGP
EIGRP	90	Advanced Distance Vector
IGRP	100	Distance Vector
OSPF	110	Link-State
IS-IS	115	Link-State
RIP	120	Distance Vector
EIGRP External	170	Advanced Distance Vector
iBGP	200	EGP
DHCP	254	
Invalid	255	

Note: The routing table is populated based on each route's AD value; the route metric is a tiebreaker only for two routes to the same destination learned via the same routing protocol. A route's metric is calculated by the routing protocol. Some routing protocols are capable of multi-path load-balancing, resulting in multiple routes to the same destination under certain conditions.

3.1 RFC 791 IP Version 4

Version	4 bits	IP Version (4)
IP Header Length (IHL)	4 bits	Header Length (Bytes ÷ 5)
DS Field	8 bits	QoS Type-of-Service (ToS) Marking (Section 6)
Packet Length	16 bits	Total Packet Length
Identification	16 bits	Fragmentation
Flags	3 bits	Fragmentation
Fragment Offset	13 bits	Fragmentation
Time-to-Live (TTL)	8 bits	Loop Prevention
Protocol	8 bits	Protocol Type (Table 3.1)
Header Checksum	16 bits	
Source IP	32 bits	
Destination IP	32 bits	
Options	varies	Optional Header Fields
Data	varies	

Table 3.4: RFC 791 / RFC 1918 Addressing

RFC 791	First Octet	Address Block	RFC 1918 Block
Class A	`01XX XXXX`	0.0.0.0 - 127.0.0.0 /8	10.0.0.0 /8
Class B	`10XX XXXX`	128.0.0.0 - 191.255.0.0 /16	172.16.0.0 /12
Class C	`110X XXXX`	192.0.0.0 - 223.255.255.0 /24	192.168.0.0 /16
Class D	`1110 XXXX`	224.0.0.0 - 239.255.255.255	
Class E	`1111 XXXX`	240.0.0.0 - 255.255.255.255	

Table 3.5: IPv4 Subnetting Magic Numbers

Bit Position	1	2	3	4	5	6	7	8
Octet Mask	128	192	224	240	248	252	254	255
Addresses	128	64	32	16	8	4	2	1
Octet Wildcard	127	63	31	15	7	3	1	0

3.2 RFC 2460 IP Version 6

Version	4 bits	IP Version (6)
Traffic Class	8 bits	QoS Marking (Section 6)
Flow Label	20 bits	Experimental
Payload Length	16 bits	Data + Extension Headers Length
Next Header	8 bits	Protocol Type (Table 3.1)
Hop Limit	8 bits	Loop Prevention
Source Address	128 bits	
Destination Address	128 bits	
Data	varies	

Note: IPv6 uses a fixed 40-Byte header by sending separate IPv6 Options headers.

Table 3.6: RFC 2460 Addressing

Address Class	**Block**	**Format**
Global Unicast	Any	Prefix (P bits) + Subnet ID ($64 - P$ bits) + INT ID (64 bits)
Unique Local Unicast	`fd00::/8`	`fd` + Global ID (40 bits) + Subnet ID (16 bits) + INT ID (64 bits)
Link-Local Unicast	`fe80::/64`	`fe80:0:0:0` (64 bits) + INT ID (64 bits)
Multicast	`ff00::/12`	`ff02:0:0:0:0:1:ffXX:XXXX/104` Solicited-Node Multicast
	`ff01::/16`	Interface/Node-Local
	`ff02::/16`	Link-Local
	`ff05::/16`	Site-Local
	`ff08::/16`	Org-Local
	`ff0e::/16`	Global

Note: IPv6 does not support broadcasts, only scoped multicasts.

Modified EUI-64 Process for Unique Address Generation:

1. Split the interface MAC into 24-pit parts, inserting `0xfffe` in-between.
2. Invert the 7th bit of the resulting address.

3.3 RFC 792 Internet Control Message Protocol (ICMP) / RFC 4443 ICMPv6

Type	8 bits	Message Type (Tables 3.7 + 3.8)
Code	8 bits	Message Subtype / Status Code (Tables 3.7 + 3.8)
Checksum	16 bits	
Header Data	32 bits	Message-specific fields
Payload	varies	

Table 3.7: ICMP Type.Code Values

`0.0`	Echo Reply
`3.X`	Destination Unreachable
`8.0`	Echo Request
`9.0`	Router Advertisement
`10.0`	Router Solicitation
`11.X`	Time Exceeded

Table 3.8: ICMPv6 Type.Code Values

`1.X`	Destination Unreachable
`2.0`	Packet Too Big
`3.X`	Time Exceeded
`128.0`	Echo Request
`129.0`	Echo Reply
`133.0`	NDP RS
`134.0`	NDP RA
`135.0`	NDP NS
`136.0`	NDP NA
`137.0`	NDP Redirect

3.4 RFC 4861 ICMPv6 Neighbor Discovery Protocol (NDP)

ICMPv6 NDP offers core functionality for IPv6 networks, including *Neighbor Discovery*, *Router Discovery*, *Stateless Address Autoconfiguration* (SLAAC), and *Duplicate Address Detection* (DAD).

- **Router Solicitation (RS) / Router Advertisement (RA):** Layer 3 default gateway discovery request/reply (replaces DHCP / DHCPv6). RS messages are sent to All-IPv6-Routers multicast; RA messages are sent to a unicast target address or to All-IPv6-Hosts multicast.

- **Neighbor Solicitation (NS) / Neighbor Advertisement (NA):** Layer 2 address discovery request/reply (replaces IPv4 ARP requests). NS messages are sent to a solicited-node multicast target address; NA messages are sent to a unicast target address or to All-IPv6-Hosts multicast.

The SLAAC Process:

1. The IPv6 host learns the IPv6 prefix used on the link, from any router, using NDP RS/RA messages.

2. The IPv6 host builds an IPv6 unicast address using the learned prefix and a (random / EUI-64) generated interface ID.

3. Before using the address, the IPv6 host uses DAD to ensure that no other IPv6 host is already using the same address.

The DAD Process:

1. The IPv6 host sends an NDP NS message, listing its own IPv6 unicast address as the `Target Address`.
2. If no other IPv6 host uses that address, then no host should reply with an NDP NA message; the host is safe to use that address on the IPv6 network.
3. If another IPv6 host uses that address, they reply with an NA message. The local host receives an NDP NA message and avoids using that address until the issue is resolved.

Table 3.9: NDP RS

Type	8 bits	Message Type (133)
Code	8 bits	Message Subtype (0)
Checksum	16 bits	
Reserved	32 bits	Unused (0)
Options	varies	

Table 3.10: NDP NS

Type	8 bits	Message Type (135)
Code	8 bits	Message Subtype (0)
Checksum	16 bits	
Reserved	32 bits	Unused (0)
Target Address	128 bits	
Options	varies	

Table 3.11: NDP RA

Type	8 bits	Message Type (134)
Code	8 bits	Message Subtype (0)
Checksum	16 bits	
Current Hop Limit	8 bits	Default IPv6 Hop Count Value
Managed Address Flag	1 bit	Indicates DHCPv6 Address Services
Other Config Flag	1 bit	Indicates DHCPv6 Other Services
Reserved	6 bits	Unused (0)
Router Lifetime	16 bits	Default Router Lifetime
Reachable Time	32 bits	Neighbor Unreachability Detection
Retransmit Time	32 bits	Time between NS message retransmissions (ms)
Options	varies	

Table 3.12: NDP NA

Type	8 bits	Message Type (136)
Code	8 bits	Message Subtype (0)
Checksum	16 bits	
From Router Flag	1 bit	Identifies sender as router
Solicited Flag	1 bit	Indicates soliciation by NDP NS
Override Flag	1 bit	Overrides existing cache entry
Reserved	29 bits	Unused (0)
Target Address	128 bits	
Options	varies	

Note: Unlike IPv4 ARP, ICMPv6 NDP messages are encapsulated within an IPv6 packet.

3.5 Open Shortest Path First (OSPFv2)

OSPFv2 is a link-state IGP for dynamic routing which maintains a *Link-State Database* (LSDB) representing the internetwork of connected OSPF routers within an *OSPF area*. Each OSPF router forms OSPF neighbor relationships with connected OSPF routers using a series of OSPF messages and *OSPF neighbor states*, which synchronize their LSDBs.

Table 3.13: OSPF LSA Types

LSA Type	Source	Conditions
Type 1 Router LSA	SPF-Routers	1 per intra-area router
Type 2 Network LSA	SPF-DRs	1 per DR/BDR subnet
Type 3 Summary LSA	ABRs	1 per inter-area subnet
Type 5 AS-External LSA	ASBRs	1 per AS-External network

Table 3.14: OSPF Link-State Advertisement (LSA) Header

LS Age	2 Bytes	Seconds since LSA originated
Options	1 Byte	
LS Type	1 Byte	LSA Type (Table 3.13)
Link-State ID	4 Bytes	Determined by `LS Type`
Advertising Router	4 Bytes	Advertising Router `RID`
LS Sequence Number	4 Bytes	Used by routers to judge LSAs
LS Checksum	2 Bytes	Checksum of LSA (excluding `LS Age`)
Length	2 Bytes	Length of LSA + header (Bytes)

Each LSDB is a collection of *OSPF Link-State Advertisements* (LSAs) whose contents describe the internetwork according to their LSA type (Table 3.13). Note that the number of OSPF routers, OSPF areas, and other variables determine the number and type of LSAs within the LSDB.

Table 3.15: OSPF Hello

Version	1 Byte	OSPF Version Number (2)
Type	1 Byte	OSPF Packet Type (1)
Packet Length	2 Bytes	Header + Packet Length in Bytes
Router ID	4 Bytes	Advertising Router `RID`
Area ID	4 Bytes	Advertising Router's Area ID
Checksum	2 Bytes	
AuType	2 Bytes	OSPF Authentication Type (0-2)
Authentication	8 Bytes	Determined by `AuType`
Network Mask	4 Bytes	Sending interface's netmask
Hello Interval	2 Bytes	OSPF `Hello` Interval
Options	1 Byte	
Rtr Pri	1 Byte	Interface OSPF Priority
Router Dead Interval	4 Bytes	OSPF `Dead` Interval
Designated Router	4 Bytes	OSPF DR IP Address
Backup Designated Router	4 Bytes	OSPF BDR IP Address
Neighbor	varies	Known Neighbor `RID`(s)

OSPF Hello packets are used for neighbor discovery and maintenance. OSPF routers use it to learn each other's `RID` in neighbor state **INIT** and determine whether they are OSPF-compatible.

OSPF routers are compatible if their `RID`s are unique and if their `Version`, `Area ID`, `Network Mask`, `Hello Interval`, and `Router Dead Interval` match. If OSPF authentication is configured, the `AuType` and `Authentication` must also match. Two OSPF-compatible routers move on to neighbor state **2WAY**, are considered OSPF neighbors, and are ready to begin the 2-way LSDB exchange process

DR/BDR elections may take place among OSPF routers connected to the same subnet. One OSPF router is elected the *Designated Router* (DR) and another is elected the *Backup Designated Router* (BDR), with the remaining routers becoming *DROthers*. The router with the highest `Rtr Pri` value becomes the DR, with the highest `RID` serving as tiebreaker; the runner-up becomes the BDR and there is no preemption. The DR/BDR routers become fully-adjacent neighbors with all OSPF routers in the subnet; DROther routers remain in 2WAY state with each other.

Table 3.16: OSPF Database Description (DD)

Version	1 Byte	OSPF version number (2)
Type	1 Byte	OSPF Packet Type (2)
Packet Length	2 Bytes	Header + Packet Length in Bytes
Router ID	4 Bytes	Advertising Router `RID`
Area ID	4 Bytes	Advertising Router's Area ID
Checksum	2 Bytes	
AuType	2 Bytes	OSPF Authentication Type (0-2)
Authentication	8 Bytes	Determined by `AuType`
Interface MTU	2 Bytes	IP MTU in Bytes
Options	1 Byte	
Reserved	5 bits	0
Initial	1 bit	1 indicates first DD packet
More	1 bit	1 indicates more DD packets follow
Master/Slave	1 bit	1 indicates master, 0 indicates slave
DD Sequence Number	4 Bytes	sequence number of DD packets
LSA Headers	varies	LSA header(s)

OSPF DD packets are used by both routers to summarize and compare their local LSDBs. The *master router* (higher `RID`) enters neigbor state **EXSTART** by sending an OSPF DD packet, which initializes the LSDB exchange process. The *slave router* (lower `RID`) enters neighbor state **EXCHANGE** by responding with its own OSPF DD packet.

Table 3.17: OSPF Link-State Request (LSR)

Version	1 Byte	OSPF Version Number (2)
Type	1 Byte	OSPF Packet Type (3)
Packet Length	2 Bytes	Header + Packet Length in Bytes
Router ID	4 Bytes	Advertising Router `RID`
Area ID	4 Bytes	Advertising Router's Area ID
Checksum	2 Bytes	
AuType	2 Bytes	OSPF Authentication Type (0-2)
Authentication	8 Bytes	Determined by `AuType`
LS Type	4 Bytes	Requested LSA Type (Table 3.13)
Link-State ID	4 Bytes	Determined by `LS Type`
Advertising Router	4 Bytes	Sending Router's `RID`

Table 3.18: OSPF Link-State Update (LSU)

Version	1 Byte	OSPF Version Number (2)
Type	1 Byte	OSPF Packet Type (4)
Packet Length	2 Bytes	Header + Packet Length in Bytes
Router ID	4 Bytes	Advertising Router `RID`
Area ID	4 Bytes	Advertising Router's Area ID
Checksum	2 Bytes	
AuType	2 Bytes	OSPF Authentication Type (0-2)
Authentication	8 Bytes	Determined by `AuType`
Number of LSAs	4 Bytes	
LSAs	varies	LSA(s)

Table 3.19: OSPF Link-State Acknowledgment (LSAck)

Version	1 Byte	OSPF Version Number (2)
Type	1 Byte	OSPF Packet Type (5)
Packet Length	2 Bytes	Header + Packet Length in Bytes
Router ID	4 Bytes	Advertising Router `RID`
Area ID	4 Bytes	Advertising Router's Area ID
Checksum	2 Bytes	
AuType	2 Bytes	OSPF Authentication Type (0-2)
Authentication	8 Bytes	Determined by `AuType`
LSA Headers	varies	LSA header(s) to be acknowledged

Both routers enter the neighbor state **LOADING** after the LSDB exchange process has been initiated. The master router requests certain LSAs using OSPF LSR packets (Table 3.17). The slave router responds with OSPF LSU packets (Table 3.18) containing the requested LSAs, which the master router acknowledges using OSPF LSAck packets (Table 3.19). This process then reverses, with the slave router requesting LSAs that the master router supplies. Once the LSDB exchange process has been completed, both routers enter neighbor state **FULL**, indicating they are *fully-adjacent OSPF neighbors*.

OSPF routers apply *Djistrka's Shortest-Path First* (SPF) algorithm to their LSDB to calculate the best routes to each network, which are dynamically added to the routing table. This calculation depends on the size of the LSDB, and is performed independently for each OSPF area. Each OSPF area must connect to *backbone area* 0 via an OSPF *Area Border Router* (ABR). An OSPF *Autonomous System Border Router* (ASBR) within backbone area 0 connects the local *Autonomous System* to one or more external AS.

4 Layer 4 Protocols

Table 4.1: Well-Known Ports

TCP	20	FTP Data
TCP	21	FTP Control
TCP	22	SSH / SFTP
TCP	23	Telnet
TCP	25	SMTP
TCP	49	Cisco TACACS+
	53	DNS
UDP	67	DHCP Server
UDP	68	DHCP Client
UDP	69	TFTP
TCP	80	HTTP
TCP	110	POP3
UDP	123	NTP
UDP	161	SNMP Agent
UDP	162	SNMP Manager
TCP	443	HTTPS
UDP	514	Syslog
TCP	989	FTPS Data
TCP	990	FTPS Control

Table 4.2: Registered Ports

UDP	1812	RADIUS Auth
UDP	1813	RADIUS Accounting
TCP	1985	Cisco HSRP
UDP	5246	CAPWAP Control
UDP	5247	CAPWAP Data

Note: *Well-Known Ports* range from 0-1023, *Registered Ports* range from 1024-49151, and *Ephemeral Ports* range from 49152-65535.

4.1 RFC 768 User Datagram Protocol (UDP)

Source Port	2 Bytes	Tables 4.1 + 4.2
Destination Port	2 Bytes	Tables 4.1 + 4.2
Length	2 Bytes	Header + Data Length in Bytes
Checksum	2 Bytes	
Data	varies	

4.2 RFC 793 Transmission Control Protocol (TCP)

Source Port	2 Bytes	Tables 4.1 + 4.2
Destination Port	2 Bytes	Tables 4.1 + 4.2
SEQ Number	4 Bytes	Windowing / Flow Control (SEQ flag)
ACK Number	4 Bytes	Windowing / Flow Control (ACK flag)
Data Offset	4 bits	
Reserved	6 bits	Future Use (0)
Flags	6 bits	Connection Management
Window	2 Bytes	Connection Window Size
Checksum	2 Bytes	
Urgent	2 Bytes	Last urgent data byte (URG flag)
Data	varies	

Note: TCP is stateful, while UDP is stateless. Protocols using UDP must implement their own reliability functions. See QUIC over UDP for maintaining state over UDP.

5 Layer 5 Applications

5.1 RFC 2131 Dynamic Host Configuration Protocol (DHCP)

Message Type	1 Byte	Message Type (request/reply)
HTYPE	1 Byte	L2 Protocol (1 for Ethernet)
HLEN	1 Byte	L2 Address Length in Bytes
Hops	1 Byte	Optionally boot via relay agent
Transaction ID	4 Bytes	Identifies client-server exchange (random)
Seconds	2 Bytes	Time since client began request
Broadcast Flag	1 bit	broadcast/unicast replies
Reserved	15 bits	Future Use (0)
Client IP	4 Bytes	Current Client IP
Your IP	4 Bytes	Your Client IP
Next Server IP	4 Bytes	Next server in bootstrap process
Relay Agent IP	4 Bytes	Boot via relay agent
CHADDR	16 Bytes	Client Hardware Address
Server Name	64 Bytes	Optional Server Hostname
File Name	128 Bytes	Optional Boot File
Magic Cookie	4 Bytes	Identifies DHCP over Bootp (`0x63.82.53.63`)
Options	varies	One or more option headers (Table 5.1)

Table 5.1: DHCP Options

Option Code	Value
1	Subnet Mask
3	Default Router
6	DNS Server
28	Broadcast Address
43	WLC IP Address
50	Requested IP Address
51	Address Lease Time
53	DHCP Message Type
54	DHCP Server ID
55	Parameter Requests
58	Renewal Time Value
59	Rebinding Time Value
66	TFTP Server IP Address
82	Relay Agent Information
150	TFTP Server List
255	End

DHCP Snooping is an optional switch security feature to prevent DHCP Poisoning and DHCP DoS attacks. It generates the *DHCP Snooping Binding Table* by observing DHCP flows and mapping observed DHCP `CHADDR` to the corresponding packet `Source IP`, frame `Source MAC`, VLAN, and local incoming switchport. It ensures consistency between table entries and subsequent DHCP client messages, additionally filtering all DHCP server messages by default. This behavior is disabled on DHCP Snooping *trusted ports*. DHCP Snooping uses optional per-interface rate limits to prevent

DoS attacks against the switch CPU and DHCP Servers.

DHCP Relay is optionally configured on the default gateway's LAN interface when the DHCP server exists in a non-local subnet. This feature causes the default gateway to insert DHCP Option 82 into received DHCP client messages, forwarding them to the DHCP server (and vice versa) as unicast packets. It is automatically enabled alongside DHCP Snooping (called the *DHCP Snooping Information Option*.

6 RFC 2475 Quality of Service (QoS)

PCP7	**CS7**			
Network Control	56 `0x38`			
PCP6	**CS6**			
Internetwork Control	48 `0x30`			
PCP5	**CS5**			**EF**
Voice	40 `0x28`			46 `0x2e`
PCP4	**CS4**	**AF41**	**AF42**	**AF43**
Video	32 `0x20`	34 `0x22`	36 `0x24`	38 `0x26`
PCP3	**CS3**	**AF31**	**AF32**	**AF33**
Critical Apps	24 `0x18`	26 `0x1a`	28 `0x1c`	30 `0x1e`
PCP2	**CS2**	**AF21**	**AF22**	**AF23**
Excellent Effort	16 `0x10`	18 `0x12`	20 `0x14`	22 `0x16`
PCP1	**CS1**	**AF11**	**AF12**	**AF13**
Background	8 `0x08`	10 `0x0a`	12 `0x0c`	14 `0x0e`
PCP0	**CS0**			
Best Effort	0 `0x00`			

Note: `CS` values use bit-pattern `XXX000`, resulting in an $8X$ DSCP value. `AF` values use bit-pattern `XXXYY0`, resulting in an $8X + 2Y$ DSCP value.

Table 6.1: QoS Fields

QoS Marking Field	Protocol
IEEE 802.1p (CoS / PCP)	IEEE 802.1Q (Table 2.5)
IEEE 802.11	QoS Control (Subsection 2.6)
RFC 791 IPP (CS)	OLD IPv4 ToS Byte
RFC 2474/3168 (DSCP)	NEW IPv4 ToS Byte (Subsection 3.1)
RFC 2460 Traffic Class (DSCP)	IPv6 (Subsection 3.2)
EXP	MPLS

Quality of Service (QoS) is defined across several standards to provide preferential treatment for certain traffic. They define groups of QoS markings (shown above) as well as header fields used to mark QoS traffic. QoS-configured devices employ *Classification* to identify QoS traffic and apply specifically configured actions, including *Marking*, *Queuing*, *Policing*, *Shaping*, and/or *Congestion Avoidance* features. Marking is typically done by an initial device, simplifying Classification for downstream devices. QoS characterizes network traffic according to the following metrics:

- **Bandwidth:** The speed of a link in *bits-per-second* (bps), or the capacity of the link to send a number of bits per-second.

- **One-Way Delay:** The time between sending one packet and that same packet arriving at the destination host.
- **Round-Trip Delay:** One-way delay plus the time for the receiveer to send a packet back; the time to send one packet between two hosts and receive one back.
- **Jitter:** The variation in one-way delay between any consecutive packets sent by the same application.
- **Loss:** The number of lost messages expressed as a percentage of sent packets.

Certain types of traffic have strict requirements for these metrics, which must be met in order to ensure a good end-user experience. Technical limitations may also require much higher bandwidth per-flow for certain traffic (e.g. video).

Table 6.2: Traffic QoS Requirements

Traffic	One-Way Delay	Jitter	Loss
Voice Over IP (VoIP)	< 150 ms	< 30 ms	$< 1\%$
Video	200-400 ms	30-50 ms	0.1-1%

Note: A majority of loss occurs due to normal network operations, but may involve faulty hardware or network congestion.

7 Appendix

Table 7.1: Protocol Timers

Protocol	Timer	Default Value
MAC Table	Aging-Time	300 s
STP	Hello	2 s
	Forward Delay	15 s
	Max Age	20 s (10∗ `Hello`)
RSTP	Hello	2 s
	Max Age	6 s (3∗ `Hello`)
CDP	Update	60 s
	Hold	180 s (3∗ `Update`)
LLDP	Send	30 s
	Hold	120 s (4∗ `Send`)
Errdisable	Recovery	300 s
Port Security	Aging	300 s
OSPF	Hello	10 s
	Dead	40 s (4∗ `Hello`)
	LSA Age	30 mins per-LSA

Table 7.2: Protocol Priority Values

Protocol	Priority	Default Value
STP/RSTP	0 - 61,440	32,768
OSPF	0 - 255	1
HSRP	1 - 255	100
VRRP	1 - 254	100
NTP	1 - 15	8

Note: The MAC Table is also referred to as the *Forwarding Information Base* (FIB) or *Content Addressable Memory* (CAM) table.

Table 7.3: Cisco Encryption Algorithms

Type	Algorithm	Salt	Secure?
0	cleartext		**NO**
4	PBKDF2-SHA-256		**NO**
5	MD5	32 bits	**WEAK**
6	AES-128		**YES**
7	Vigenere		**NO**
8	PBKDF2-SHA-256	80 bits	**YES**
9	Scrypt	80 bits	**YES**

Table 7.4: ASCII Values

32	64	96	0x20	0x40	0x60	SP	@	‘
33	65	97	0x21	0x41	0x61	!	A	a
34	66	98	0x22	0x42	0x62	“	B	b
35	67	99	0x23	0x43	0x63	#	C	c
36	68	100	0x24	0x44	0x64	$	D	d
37	69	101	0x25	0x45	0x65	%	E	e
38	70	102	0x26	0x46	0x66	&	F	f
39	71	103	0x27	0x47	0x67	‘	G	g
40	72	104	0x28	0x48	0x68	(	H	h
41	73	105	0x29	0x49	0x69	)	I	i
42	74	106	0x2a	0x4a	0x6a	*	J	j
43	75	107	0x2b	0x4b	0x6b	+	K	k
44	76	108	0x2c	0x4c	0x6c	,	L	l
45	77	109	0x2d	0x4d	0x6d	-	M	m
46	78	110	0x2e	0x4e	0x6e	.	N	n
47	79	111	0x2f	0x4f	0x6f	/	O	o
48	80	112	0x30	0x50	0x70	0	P	p
49	81	113	0x31	0x51	0x71	1	Q	q
50	82	114	0x32	0x52	0x72	2	R	r
51	83	115	0x33	0x53	0x73	3	S	s
52	84	116	0x34	0x54	0x74	4	T	t
53	85	117	0x35	0x55	0x75	5	U	u
54	86	118	0x36	0x56	0x76	6	V	v
55	87	119	0x37	0x57	0x77	7	W	w
56	88	120	0x38	0x58	0x78	8	X	x
57	89	121	0x39	0x59	0x79	9	Y	y
58	90	122	0x3a	0x5a	0x7a	:	Z	z
59	91	123	0x3b	0x5b	0x7b	;	[	{
60	92	124	0x3c	0x5c	0x7c	<	\	|
61	93	125	0x3d	0x5d	0x7d	=	]	}
62	94	126	0x3e	0x5e	0x7e	>	^	~
63	95	127	0x3f	0x5f	0x7f	?	_	DEL

Table 7.5: SI Prefixes

Z	Zetta	10^{21}	sextillion
E	Exa	10^{18}	quintillion
P	Peta	10^{15}	quadrillion
T	Tera	10^{12}	trillion
G	Giga	10^{9}	billion
M	Mega	10^{6}	million
k	Kilo	10^{3}	thousand
h	Hecto	10^{2}	hundred
da	Deka	10^{1}	ten
d	deci	10^{-1}	tenth
c	centi	10^{-2}	hundredth
m	milli	10^{-3}	thousandth
μ	micro	10^{-6}	millionth
n	nano	10^{-9}	billionth
p	pico	10^{-12}	trillionth

Table 7.6: Binary Prefixes

Yi	Yobi	2^{80}
Zi	Zebi	2^{70}
Ei	Exbi	2^{60}
Pi	Pebi	2^{50}
Ti	Tebi	2^{40}
Gi	Gibi	2^{30}
Mi	Mebi	2^{20}
Ki	Kibi	2^{10}

Figure 7.1: IEEE 802.1x / IEEE 802.11i Extensible Authentication Protocol (EAP)

Authentication Methods	Open Authentication (Open)		None (other than 802.11 conformity)
	Wired Equivalent Privacy (WEP)		Static WEP keys
	802.1x / 802.11i Extensible Authentication Protocol (EAP)	Lightweight EAP (LEAP)	Dynamic WEP keys (deprecated)
		EAP Flexible Authentication by Secure Tunneling (EAP-FAST)	Protected Access Credential (PAC)
		Protected EAP (PEAP)	AS authenticated by digital certificate
		EAP Transport Layer Security (EAP-TLS)	Client and AS authenticated by digital certificate
Privacy and Integrity Methods	Temporal Key Integrity Protocol (TKIP)		WPA-PSK / WPA Enterprise
	AES Counter/CBC-MAC Protocol (CCMP)		WPA2-PSK / WPA2 Enterprise
	AES Galois/Counter Mode Protocol (GCMP)		WPA3-PSK / WPA3 Enterprise

7.1 Official Standards

OFFICIAL STANDARD	ALTERNATIVE	REFERENCE
RFC 1661 PPP	ITU HDLC / Cisco HDLC	Subsections 2.7 + 2.8
IEEE 802.3 Ethernet		Subsection 2.1
IEEE 802.2 LLC/SNAP		Tables 2.3 + 2.4
IEEE 802.3u FastEthernet		Subsection 1.2
IEEE 802.3af/at/bt PoE/UPoE	Cisco ILP	Table 1.4
IEEE 802.1Q VLAN Trunking	Cisco ISL/DTP/VTP	Subsections 2.2 + 2.3
IEEE 802.1AB LLDP	Cisco CDP	
IEEE 802.1D/w STP/RSTP	Cisco PVST/PVRST	Subsection 2.4
IEEE 802.1s MSTP		
IEEE 802.3AD LACP	Cisco PAgP	
IEEE 802.11 WLAN	Wi-Fi Alliance	Subsection 2.6
IEEE 802.11i EAP		Figure 7.1
IEEE 802.1x Access Control		Figure 7.1
RFC 791/1918 IPv4	RFC 2460 IPv6	Subsections 3.1 + 3.2
RFC 792 ICMP	RFC 4443 ICMPv6	Subsection 3.3
ARP	RFC 4861 NDP	Subsections 2.5 + 3.4
RFC 1631/3022 NAT		
RFC 2328 OSPF	EIGRP / RIP / ...	Subsection 3.5
RFC 5798 VRRP	Cisco HSRP/GLBP	
RFC 2475 QoS		Section 6
RFC 768 UDP	RFC 793 TCP	Subsections 4.1 + 4.2
RFC 959 FTP	TFTP / SFTP / FTPS /	
RFC 1305/5905 NTP		
RFC 1065 SNMP		
RFC 5424 Syslog		
RFC 2131 DHCP		Subsection 5.1
RFC 3046 DHCP Relay		Subsection 5.1
RFC 7230 HTTP		
RFC 4301 IPSec	RFC 7568 TLS	

7.2 Cisco IOS Configuration Examples

Layer 2 Interface Configuration:

```
configure terminal
  int F0/1
    mac-address MAC
    bandwidth KBPS
    duplex {half | full | auto}
    speed {MBPS | auto}
    description TEXT

show interface [INT] [status | switchport]
```

VLAN Configuration:

```
configure terminal
  vlan VLAN_ID
    name TEXT
    [no] shutdown
  [no] shutdown vlan VLAN_ID
  int F0/1
    switchport trunk encapsulation {ISL | dot1Q}
    switchport mode {trunk | dynamic {desirable | auto}}
    switchport nonegotiate
    switchport trunk allowed vlan VLAN_LIST
    switchport trunk native vlan VLAN_ID
    [no] shutdown
  int range F0/2 - 12
    switchport mode access
    switchport {access | voice} vlan VLAN_ID
    [no] shutdown
  vtp mode {server | client | transparent | off}
  vtp domain TEXT
  vtp password PASSWORD
  [no] vtp pruning
  vtp version 2

show int [INT] status
show int [INT] switchport
show int [INT] trunk
show vlan brief
show vlan id VLAN_ID
show vtp {status | password}
```

Link Aggregation Configuration:

```
configure terminal
  port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip
     > | src-dst-ip | src-port | dst-port | src-dst-port}
  int range F0/13 - 16
    [no] switchport
    [no] shutdown
    channel-group 1 mode {on | desirable | auto | active | passive}
  int Po1
    [no] switchport
    [no] shutdown

show etherchannel [CHANNEL] {summary | port-channel}
```

```
show etherchannel load-balance
test etherchannel load-balance interface INT mac SRC_MAC DST_MAC
```

Port Security Configuration:

```
configure terminal
  errdisable recovery cause psecure-violation
  errdisable recovery interval SECS
  int range F0/2 - 12
    switchport mode {access | trunk}
    switchport port-security violation {protect | restrict | shutdown}
    switchport port-security maximum MAX
    switchport port-security mac-address {MAC | sticky}
    switchport port-security aging type {absolute | inactivity}
    switchport port-security aging time MINS
    switchport port-security aging static
    switchport port-security
  mac address-table aging-time SECS [vlan VLAN_ID]

show int [INT] [status]
show port-security [interface INT]
show mac address-table [static | secure] [vlan VLAN_ID | interface INT]
clear mac address-table dynamic [vlan VLAN_ID | interface INT | address MAC]
show mac address-table aging-time
show errdisable recovery
```

CDP / LLDP Configuration:

```
configure terminal
  [no] {cdp | lldp} run
  {cdp | lldp} timer SECS
  {cdp | lldp} holdtime SECS
  int range F0/2 - 12
    [no] cdp enable
    [no] lldp {transmit | receive}

show {cdp | lldp}
show {cdp | lldp} traffic
show {cdp | lldp} interface [INT]
show {cdp | lldp} neighbors [detail] [INT]
show {cdp | lldp} entry NEIGHBOR
```

Spanning Tree Configuration:

```
configure terminal
  errdisable recovery cause bpduguard
  spanning-tree mode {pvst | rapid-pvst | mst}
  spanning-tree pathcost method {long | short}
  spanning-tree [vlan VLAN_ID] root {primary | secondary}
  spanning-tree [vlan VLAN_ID] priority {32768 | 28672 | 24576 | ...}
  spanning-tree portfast [edge | network] [bpduguard | bpdufilter] default
  spanning-tree loopguard default
  int Po1
    spanning-tree [vlan VLAN_ID] cost PORT_COST
    spanning-tree [vlan VLAN_ID] port-priority PORT_PRIO
    spanning-tree [vlan VLAN_ID] link-type {point-to-point | shared}
    spanning-tree portfast [disable | [edge | network] [default | trunk]]
    spanning-tree {bpduguard | bpdufilter} {enable | disable}
    spanning-tree guard {root | loop | none}
```

```
show spanning-tree [bridge | summary]
show spanning-tree [vlan VLAN_LIST | interface INT]
```

Authenticated NTP Configuration:

```
configure terminal
  clock timezone CST -6 0
  clock summer-time CDT recurring 2 SUNDAY MAR 02:00 1 SUNDAY NOV 02:00
clock set HH:MM:SS DATE MONTH YEAR
clock {update-calendar | read-calendar}
configure terminal
  ntp authenticate
  ntp authentication-key 1 md5 PASSWORD
  ntp trusted-key 1
  ntp master STRATUM
  ntp {peer | server} {A.B.C.D | HOSTNAME} key 1
  ntp update-calendar
  ntp source loopback 0

show ntp status
show ntp associations [detail]
show {clock | calendar} [detail]
```

Logging and SNMP Configuration:

```
terminal monitor
configure terminal
  logging console {0-7 | emergency | alert | critical | error | warning |
     > notification | informational | debug}
  logging monitor {0-7 | emergency | alert | critical | error | warning |
     > notification | informational | debug}
  logging buffered [MEMSIZE] {0-7 | emergency | alert | critical | error |
     > warning | notification | informational | debug}
  logging [host] {A.B.C.D | HOSTNAME}
  logging trap {0-7 | emergency | alert | critical | error | warning |
     > notification | informational | debug}
  [no] service {timestamps | sequence-numbers}
  snmp-server community PASSWORD {ro | rw}
  snmp-server contact TEXT
  snmp-server location TEXT
  snmp-server host {A.B.C.D | HOSTNAME} [trap | inform] version 2c PASSWORD
  snmp-server enable traps TRAPS_LIST

{show | clear} logging
show snmp {community | contact | location | host}
```

DHCP Snooping and DAI Configuration:

```
configure terminal
  errdisable recovery cause dhcp-rate-limit
  errdisable recovery cause arp-inspection
  ip dhcp snooping
  ip dhcp snooping vlan VLAN_LIST
  [no] ip dhcp snooping information option
  ip arp inspection vlan VLAN_LIST
  ip arp inspection validate {[src-mac] [dst-mac] [ip]}
  int Po1
    ip dhcp snooping trust
```

```
    ip arp inspection trust
  int F0/1
    ip arp inspection trust
  int range F0/2 - 12
    ip dhcp snooping limit rate MAX
    ip arp inspection limit rate MAX [burst-interval SECS]

show ip dhcp snooping [binding]
show ip arp inspection [statistics | interfaces]
```

Layer 3 Interface Configuration:

```
configure terminal
  sdm prefer lanbase-routing
  ip routing
  ipv6 unicast-routing
  int F0/0.SUBINT
    encapsulation dot1q VLAN_ID [native]
    ip address {A.B.C.D M.M.M.M | dhcp}
    {ipv6 enable | ipv6 address {ADDRESS/PREFIX_LENGTH [link-local | anycast] |
       > PREFIX/64 eui-64 | dhcp | autoconfig}}
    [no] shutdown
  int vlan VLAN_ID
    ip address {A.B.C.D M.M.M.M | dhcp}
    {ipv6 enable | ipv6 address {ADDRESS/PREFIX_LENGTH [link-local | anycast] |
       > PREFIX/64 eui-64 | dhcp | autoconfig}}
    [no] shutdown
  int F0/1
    [no] switchport
    ip address {A.B.C.D M.M.M.M | dhcp}
    {ipv6 enable | ipv6 address {ADDRESS/PREFIX_LENGTH [link-local | anycast] |
       > PREFIX/64 eui-64 | dhcp | autoconfig}}
    [no] shutdown
    ip helper-address DHCP_SERVER

show sdm prefer
show {ip | ipv6} interface [brief | INT]
show interfaces [INT] [status | switchport]
show protocols [INT]
show dhcp lease
show ip default-gateway
show vlans
```

IP Routing Configuration:

```
configure terminal
  router ospf 1
    router-id {A.B.C.D | VALUE}
    auto-cost reference-bandwidth MBPS
    maximum-paths 4
    distance 110
    default-information originate [always]
    [no] passive-interface {INT | default}
    [no] network A.B.C.D W.W.W.W area AREA
    [no] shutdown
  int S0/0/0
    ip ospf 1 area AREA
    ip ospf network {point-to-point | broadcast}
    ip ospf cost PORT_COST
```

```
    ip ospf priority 0-255
    ip ospf hello-interval SECS
    ip ospf dead-interval SECS
    ip ospf authentication message-digest
    ip ospf message-digest-key 1 md5 PASSWORD
    ip ospf authentication-key 1
  router rip
    version 2
    no auto-summary
    [no] network NETWORK_ID
    [no] passive-interface INT
    default-information originate
    maximum-paths VALUE
    distance AD
    [no] shutdown
  router eigrp AS_VALUE
    eigrp router-id A.B.C.D
    no auto-summary
    [no] network A.B.C.D [W.W.W.W]
    [no] passive-interface INT
    default-information originate
    maximum-paths VALUE
    variance VALUE
    distance INTERNAL_AD EXTERNAL_AD
    [no] shutdown
  ip route A.B.C.D M.M.M.M {[EXIT_INT] [NEXT_HOP]} [AD] [permanent]
  ipv6 route PREFIX/LENGTH {[EXIT_INT] [NEXT_HOP]} [AD] [permanent]

show {ip | ipv6} protocols
show ip ospf
show ip ospf interface [INT | brief]
show ip ospf neighbor
show ip ospf database
clear ip ospf [PROCESS_ID] process
show {ip | ipv6} route [connected | local | static | ospf | ...] [ADDR]
show ip arp
show ipv6 neighbors
```

VRF Configuration:

```
configure terminal
  ip vrf VRF_NAME
  int F0/0
    ip vrf forwarding VRF_NAME
    ip address {A.B.C.D M.M.M.M | dhcp}
    [no] shutdown
show ip vrf
show ip route vrf VRF_NAME
ping vrf VRF_NAME [ADDRESS]
```

FHRP Configuration:

```
configure terminal
  int F0/0
    standby version 1-2
    standby GROUP_ID ip A.B.C.D
    standby GROUP_ID priority 1-255
    standby GROUP_ID preempt
    standby GROUP_ID description TEXT
```

```
    vrrp GROUP_ID ip A.B.C.D [secondary]
    vrrp GROUP_ID priority 1-254
    vrrp GROUP_ID preempt [delay minimum SECS]
    vrrp GROUP_ID description TEXT

show standby [brief]
show standby neighbors [INT]
show vrrp [brief | GROUP_ID]
show vrrp interface INT [brief]
```

DHCP Services Configuration:

```
configure terminal
  service dhcp
  ip dhcp excluded-address FIRST_IP [LAST_IP]
  ip dhcp pool POOL_NAME
    network A.B.C.D {M.M.M.M | /CIDR}
    domain-name TEXT
    default-router A.B.C.D
    dns-server A.B.C.D
    lease {DAYS HRS MINS | infinite}
    option 43 ip WLC_IP
    option 66 ip TFTP_IP

show ip dhcp pool POOL_NAME
show ip dhcp binding
```

ACL Configuration:

```
configure terminal
  access-list {1-99 | 1300-1999} {permit | deny} {[host] SRC_IP | SRC_IP SRC_WC
     > | any} [log]
  access-list {100-199 | 2000-2699} {permit | deny} {ip | icmp} {host SRC_IP |
     > SRC_IP SRC_WC | any} {host DST_IP | DST_IP DST_WC | any} [log]
  access-list {100-199 | 2000-2699} {permit | deny} {tcp | udp} {host SRC_IP |
     > SRC_IP SRC_WC | any} [{eq | neq | lt | gt | range} SRC_PORT] {host
     > DST_IP | DST_IP DST_WC | any} [{eq | neq | lt | gt | range} DST_PORT]
     > [log]
  access-list {1-199 | 1300-2699} remark TEXT
  ip access-list standard {ACL_NAME | ACL_ID}
    [no] [SEQ] {permit | deny} {[host] SRC_IP | SRC_IP SRC_WC | any} [log]
    [no] [SEQ] remark TEXT
    no SEQ
  ip access-list extended {ACL_NAME | ACL_ID}
    [no] [SEQ] {permit | deny} {ip | icmp} {host SRC_IP | SRC_IP SRC_WC | any}
       > {host DST_IP | DST_IP DST_WC | any} [log]
    [no] [SEQ] {permit | deny} {tcp | udp} {host SRC_IP | SRC_IP SRC_WC | any}
       > [{eq | neq | lt | gt | range} SRC_PORT] {host DST_IP | DST_IP DST_WC |
       > any} [{eq | neq | lt | gt | range} DST_PORT] [log]
    [no] [SEQ] remark TEXT
    no SEQ
  int S0/0/0
    ip access-group {ACL_ID | ACL_NAME} {in | out}
  line vty 0 15
    access-class {ACL_ID | ACL_NAME} {in | out}

show access-lists
show ip access-lists
```

NAT Services Configuration:

```
configure terminal
  int F0/0
    ip nat inside
  int S0/0/0
    ip nat outside
  ip nat inside source static INSIDE_LOCAL INSIDE_GLOBAL
  ip nat pool POOL_NAME FIRST_IP LAST_IP netmask M.M.M.M
  access-list 1 permit A.B.C.D [W.W.W.W]
  ip nat inside source list 1 pool POOL_NAME [overload]
  ip nat inside source list 1 interface S0/0/0 overload

show ip nat translations
show ip nat statistics
```

QoS Configuration:

```
configure terminal
  class-map [match-all | match-any] CMAP_NAME
    match protocol PROTOCOL
  policy-map PMAP_NAME
    class CMAP_NAME
      set ip dscp {EF | AFXY | CSX | BINARY}
      priority percent BANDWIDTH
      bandwidth percent BANDWIDTH
  int F0/0
    service-policy {input | output} PMAP_NAME

show run | section policy-map
```

WLC WLAN Configuration:

1. Create a new WLC Dynamic Interface:
   - `Name` (31 or fewer ASCII characters)
   - `VLAN ID` (Integer value 1-1001, 1007-4094 inclusive)
2. Create a new WLC WLAN:
   - `Profile Name` (32 or fewer ASCII characters)
   - `SSID` (32 or fewer ASCII characters)
   - `WLAN ID` (Integer value 1-512 inclusive)
3. Configure the new WLAN:
   - Bind the Dynamic Interface to the WLAN.
   - Enable the WLAN on the WLC.
   - Enable broadcasting of the WLAN SSID by APs.
4. Secure the new WLAN:
   - Set `Layer 2 Security` to **WPA+WPA2**, enabling the `WPA2` checkbox.
   - Set `WPA2 Encryption` to **AES/TKIP/CCMP/GCMP**.
   - Enable the `PSK` checkbox.
   - Set the `PSK Format` to **ASCII** and enter the PSK value.