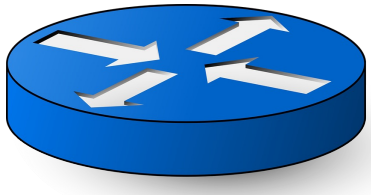


Router

router wont forward broadcast frame

IP Class

Table 11-2 RFC 1918 Private Address Space

Class of Networks	Private IP Networks	Number of Networks
A	10.0.0.0	1
B	172.16.0.0 through 172.31.0.0	16
C	192.168.0.0 through 192.168.255.0	256

IPV6

- IPV6 is 128 Bits in length
- IPV6 uses NDP which is the equivalent of ARP
- IPV6 Have the link-local address which is FE80

IPV6 NDP Functions

Key Topic

Table 25-3 NDP Function Summary

Function	Protocol Messages	Who Discovers Info	Who Supplies Info	Info Supplied
Router discovery	RS and RA	Any IPv6 host	Any IPv6 router	Link-local IPv6 address of router
Prefix/length discovery	RS and RA	Any IPv6 host	Any IPv6 router	Prefix(es) and associated prefix lengths used on local link
Neighbor discovery	NS and NA	Any IPv6 host	Any IPv6 host	Link-layer address (for example, MAC address) used by a neighbor
Duplicate Address Detection	NS and NA	Any IPv6 host	Any IPv6 host	Simple confirmation whether a unicast address is already in use

Summary of IPv6 Address Types

Key Topic

Table 24-5 Summary of IPv6 Address Types and the Commands That Create Them

Type	Prefix/Address Notes	Enabled with What Interface Subcommand
Global unicast	Many prefixes	**ipv6 address** *address/prefix-length* **ipv6 address** *prefix/prefix-length* **eui-64**
Unique Local	FD00::/8	**ipv6 address** *prefix/prefix-length* **eui-64**
Link local	FE80::/10	**ipv6 address** *address* **link-local** Autogenerated by all **ipv6 address** commands Autogenerated by the **ipv6 enable** command
All hosts multicast	FF02::1	Autogenerated by all **ipv6 address** commands
All routers multicast	FF02::2	Autogenerated by all **ipv6 address** commands
Routing protocol multicasts	Various	Added to the interface when the corresponding routing protocol is enabled on the interface
Solicited-node multicast	FF02::1:FF /104	Autogenerated by all **ipv6 address** commands

IPV6 Multicast Scope

as noted in Table 24-4.

Key Topic

Table 24-4 IPv6 Multicast Scope Terms

Scope Name	First Quartet	Scope Defined by...	Meaning
Interface-Local	FF01	Derived by Device	Packet remains within the device. Useful for internally sending packets to services running on that same host.
Link-Local	FF02	Derived by Device	Host that creates the packet can send it onto the link, but no routers forward the packet.
Site-Local	FF05	Configuration on Routers	Intended to be more than Link-Local, so routers forward, but must be less than Organization-Local; generally meant to limit packets so they do not cross WAN links.
Organization-Local	FF08	Configuration on Routers	Intended to be broad, probably for an entire company or organization. Must be broader than Site-Local.
Global	FF0E	No Boundaries	No boundaries.

IPV6 Local-Scope Multicast Address

Table 24-3 Key IPv6 Local-Scope Multicast Addresses

Short Name	Multicast Address	Meaning	IPv4 Equivalent
All-nodes	FF02::1	All-nodes (all interfaces that use IPv6 that are on the link)	224.0.0.1
All-routers	FF02::2	All-routers (all IPv6 router interfaces on the link)	224.0.0.2
All-OSPF, All-OSPF-DR	FF02::5, FF02::6	All OSPF routers and all OSPF-designated routers, respectively	224.0.0.5, 224.0.0.6
RIPng Routers	FF02::9	All RIPng routers	224.0.0.9
EIGRPv6 Routers	FF02::A	All routers using EIGRP for IPv6 (EIGRPv6)	224.0.0.10
DHCP Relay Agent	FF02::1:2	All routers acting as a DHCPv6 relay agent	None

IPV6 Routing Protocols

Table 22-2 IPv6 Routing Protocols

Routing Protocol	Defined By	Notes
RIPng (RIP next generation)	RFC	The "next generation" is a reference to a TV series, *Star Trek: the Next Generation*.
OSPFv3 (OSPF version 3)	RFC	The OSPF you have worked with for IPv4 is actually OSPF version 2, so the new version for IPv6 is OSPFv3.
EIGRPv6 (EIGRP for IPv6)	Cisco	Cisco owns the rights to the EIGRP protocol, but Cisco also now publishes EIGRP as an informational RFC.
MP BGP-4 (Multiprotocol BGP version 4)	RFC	BGP version 4 was created to be highly extendable; IPv6 support was added to BGP version 4 through one such enhancement, MP BGP-4.

VPN Comparison

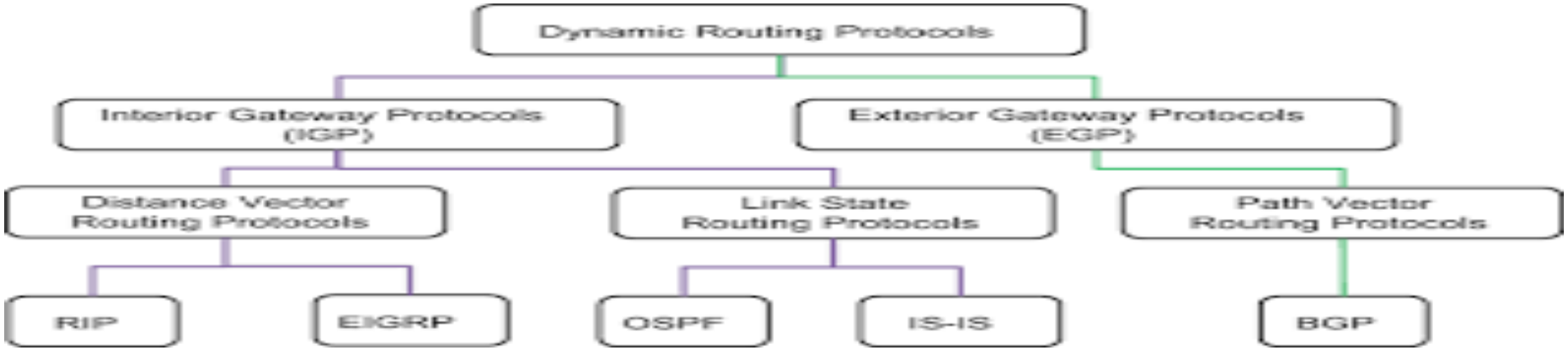
Table 14-4 Comparisons of Site-to-Site and Remote Access VPNs

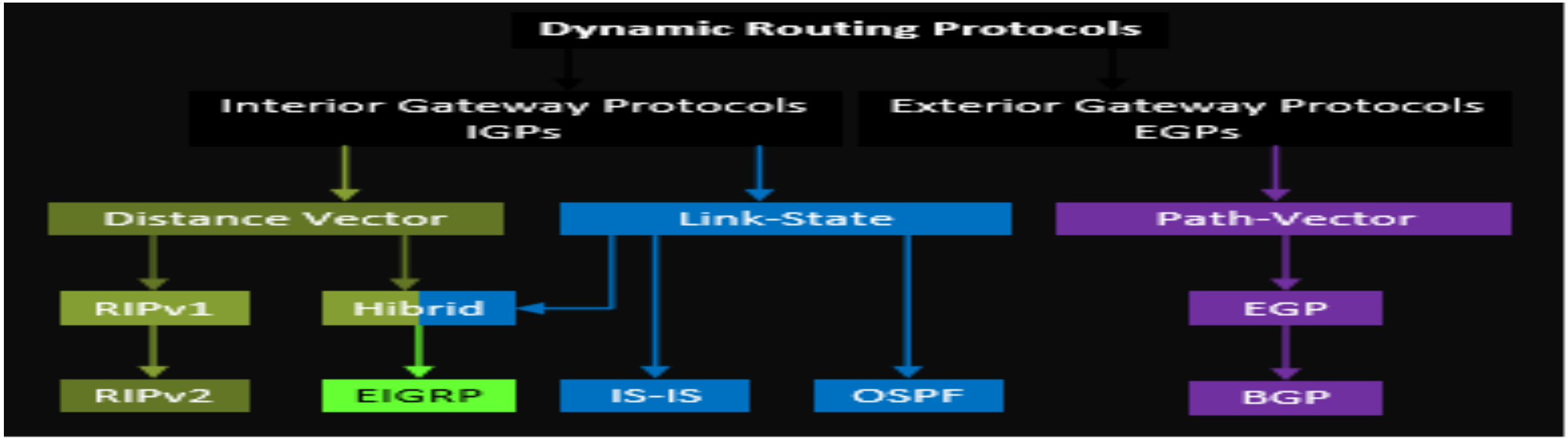
	Remote Access	Site-to-Site
Typical security protocol	TLS	IPsec
Devices supported by one VPN (one or many)	One	Many
Typical use: on-demand or permanent	On-demand	Permanent

Protocols

- RIP and EIGRP are Distance Vector Protocol
- OSPF and IS-IS Are Link State Protocol
- Link state Routing Protocol is Faster than Distance vector
- Lower Metric is considered a Better
- For a static route to be less preferred than a dynamic routing protocol the AD has to be higher

Dynamic Routing Protocol





OSPF Neighbors Adjacency Requirements

Key Topic

Table 21-3 Neighbor Requirements for OSPF

Requirement	Required for OSPF	Neighbor Missing if Incorrect
Interfaces must be in an up/up state.	Yes	Yes
Access control lists (ACL) must not filter routing protocol messages.	Yes	Yes
Interfaces must be in the same subnet.	Yes	Yes
They must pass routing protocol neighbor authentication (if configured).	Yes	Yes
Hello and hold/dead timers must match.	Yes	Yes
Router IDs (RID) must be unique.	Yes	Yes
They must be in the same area.	Yes	Yes
OSPF process must not be shut down.	Yes	Yes
Neighboring interfaces must use same MTU setting.	Yes	No
Neighboring interfaces must use same OSPF network type.	Yes	No

OSPF Types and Key Behaviors

Key Topic

Table 21-2 Two OSPF Network Types and Key Behaviors

Network Type Keyword	Dynamically Discovers Neighbors	Uses a DR/BDR
broadcast	Yes	Yes
point-to-point	Yes	No

OSPF Equal Cost

Table 20-3 Faster Interfaces with Equal OSPF Costs

Interface	Interface Default Bandwidth (Kbps)	Formula (Kbps)	OSPF Cost
Serial	1544 Kbps	100,000 / 1544	64
Ethernet	10,000 Kbps	100,000 / 10,000	10
Fast Ethernet	100,000 Kbps	100,000/100,000	1
Gigabit Ethernet	1,000,000 Kbps	100,000/1,000,000	1
10 Gigabit Ethernet	10,000,000 Kbps	100,000/10,000,000	1
100 Gigabit Ethernet	100,000,000 Kbps	100,000/100,000,000	1

OSPF Design Terminology

Key Topic

Table 19-7 OSPF Design Terminology

Term	Description
Area Border Router (ABR)	An OSPF router with interfaces connected to the backbone area and to at least one other area
Backbone router	A router connected to the backbone area (includes ABRs)
Internal router	A router in one area (not the backbone area)
Area	A set of routers and links that shares the same detailed LSDB information, but not with routers in other areas, for better efficiency
Backbone area	A special OSPF area to which all other areas must connect—area 0
Intra-area route	A route to a subnet inside the same area as the router
Interarea route	A route to a subnet in an area of which the router is not a part

OSPF Network States and their Meanings

Table 19-5 Stable OSPF Neighbor States and Their Meanings

Neighbor State	Term for Neighbor	Term for Relationship
2-way	Neighbor	Neighbor Relationship
Full	Adjacent Neighbor Fully Adjacent Neighbor	Adjacency

OSPF LS Types

LS Type	Advertisement Description
1	Router Link advertisements. Generated by each router for each area it belongs to. They describe the states of the router link to the area. These are only flooded within a particular area.
2	Network Link advertisements. Generated by Designated Routers. They describe the set of routers attached to a particular network. Flooded in the area that contains the network.
3 or 4	Summary Link advertisements. Generated by Area Border routers. They describe inter-area (between areas) routes. Type 3 describes routes to networks, also used to aggregate routes. Type 4 describes routes to ASBR.
5	AS external link advertisements. Originated by ASBR. They describe routes to destinations external to the AS. Flooded all over except stub areas.

LS Type	Link State ID (In the high level view of the database when a router is referenced, this is called Link ID)
1	The origin Router ID (RID).
2	The IP interface address of the network Designated Router.
3	The destination network number.
4	The router ID of the described AS boundary router.
5	The external network number.

OSPF Link Types

Link Type	Link ID (This applies to individual Links)
Point-to-Point	Neighbor Router ID
Link to transit network	Interface address of DR
Link to stub network (In case of loopback mask is 255.255.255.255)	Network/subnet number
Virtual Link	Neighbor Router ID

The **Link Data** is the IP address of the link, except for stub network where the link data is the network mask.

Link Type	Link Data
Stub network	Network Mask
Other networks (applies to router links only)	Router - associated IP interface address

Default Administrative Distance

Table 19-4 Default Administrative Distances

Route Type	Administrative Distance
Connected	0
Static	1
BGP (external routes [eBGP])	20
EIGRP (internal routes)	90
IGRP	100
OSPF	110

Administrative Distances

Route Type	Administrative Distance
IS-IS	115
RIP	120
EIGRP (external routes)	170
BGP (internal routes [iBGP])	200
DHCP default route	254
Unusable	255

Routing Protocol Comparison

Table 19-3 Interior IP Routing Protocols Compared

Feature	RIPv2	EIGRP	OSPF
Classless/sends mask in updates/supports VLSM	Yes	Yes	Yes
Algorithm (DV, advanced DV, LS)	DV	Advanced DV	LS
Supports manual summarization	Yes	Yes	Yes
Cisco-proprietary	No	Yes[1]	No
Routing updates are sent to a multicast IP address	Yes	Yes	Yes
Convergence	Slow	Fast	Fast

IP IGP Metrics

Key Topic

Table 19-2 IP IGP Metrics

IGP	Metric	Description
RIPv2	Hop count	The number of routers (hops) between a router and the destination subnet
OSPF	Cost	The sum of all interface cost settings for all links in a route, with the cost defaulting to be based on interface bandwidth
EIGRP	Calculation based on bandwidth and delay	Calculated based on the route's slowest link and the cumulative delay associated with each interface in the route

HSRP

Key Topic

Table 12-2 Three FHRP Options

Acronym	Full Name	Origin	Redundancy Approach	Load Balancing Per...
HSRP	Hot Standby Router Protocol	Cisco	active/standby	subnet
VRRP	Virtual Router Redundancy Protocol	RFC 5798	active/standby	subnet
GLBP	Gateway Load Balancing Protocol	Cisco	active/active	host

ACL Types

- Standard numbered ACLs (1–99)
- Extended numbered ACLs (100–199)
- Additional ACL numbers (1300–1999 standard, 2000–2699 extended)
- Named ACLs
- Improved editing with sequence numbers

ACL Application Consideration

- Place extended ACLs as close as possible to the source of the packets that will be filtered. Filtering close to the source of the packets saves some bandwidth.
- Remember that all fields in one **access-list** command must match a packet for the packet to be considered to match that **access-list** statement.
- Use numbers of 100–199 and 2000–2699 on the **access-list** commands; no one number is inherently better than another.

- Using names instead of numbers to identify the ACL, making it easier to remember the reason for the ACL
- Using ACL subcommands, not global commands, to define the action and matching parameters
- Using ACL editing features that allow the CLI user to delete individual lines from the ACL and insert new lines

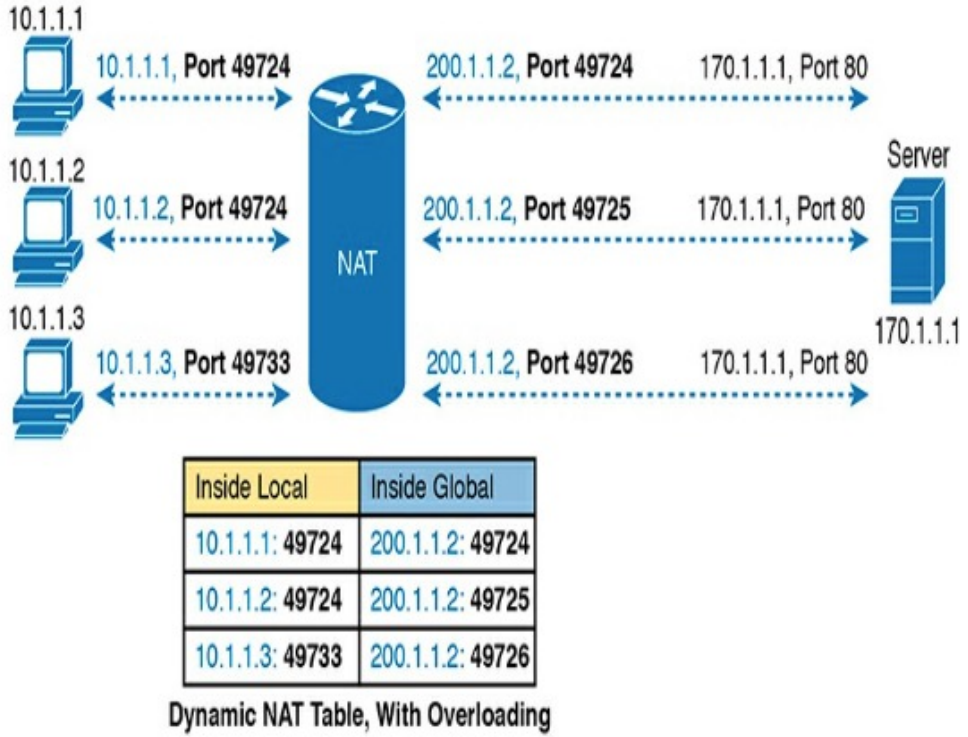
Topic

- Place extended ACLs as close as possible to the source of the packet. This strategy allows ACLs to discard the packets early.
- Place standard ACLs as close as possible to the destination of the packet. This strategy avoids the mistake with standard ACLs (which match the source IPv4 address only) of unintentionally discarding packets that did not need to be discarded.
- Place more specific statements early in the ACL.
- Disable an ACL from its interface (using the **no ip access-group** interface subcommand) before making changes to the ACL.

NAT

Term	Values in Figures	Meaning
Inside local	10.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective: it is inside the enterprise. **Local:** Means not global; that is, local. It is the address used for that host while the packet flows in the local enterprise rather than the global Internet. **Alternative:** Think of it as inside private, because this address is typically a private address.
Inside global	200.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective. **Global:** Means global as in the global Internet. It is the address used for that host while the packet flows in the Internet. **Alternative:** Think of it as inside public, because the address is typically a public IPv4 address.
Outside global	170.1.1.1	With source NAT, the one address used by the host that resides outside the enterprise, which NAT does not change, so there is no need for a contrasting term. **Alternative:** Think of it as outside public, because the address is typically a public IPv4 address.
Outside local	—	This term is not used with source NAT. With destination NAT, the address would represent a host that resides outside the enterprise, but the address used to represent that host as packets pass through the local enterprise.

NAT OVERLOAD



Inside Local	Inside Global
10.1.1.1: **49724**	200.1.1.2: **49724**
10.1.1.2: **49724**	200.1.1.2: **49725**
10.1.1.3: **49733**	200.1.1.2: **49726**

Dynamic NAT Table, With Overloading

Figure 10-8 *NAT Overload (PAT)*

Switch

- Layer 2 Switch

Forward Packets Based on Destination MAC Address

switches receive broadcast frame flooded to all of the ports except the one that received the broadcast frame

VLANS from 1 to 1005 exist in switches by default can not be deleted

Traffic from multiple VLANs can be allowed over a trunk link

TCP VS UDP

TCP	UDP
Secure	Unsecure
Connection-Oriented	Connectionless
Slow	Fast
Guaranteed Transmission	No Guarantee
Used by Critical Applications	Used by Real-Time Applications
Packet Reorder Mechanism	No Reorder Mechanism
Flow Control	No Flow Control
Advanced Error Checking	Basic Error Checking (Checksum)
20 Bytes Header	8 Bytes Header
Acknowledgement Mechanism	No Acknowledgement
Three-Way Handshake	No Handshake Mechanism
DNS, HTTPS, FTP, SMTP etc.	DNS, DHCP, TFTP, SNMP etc.

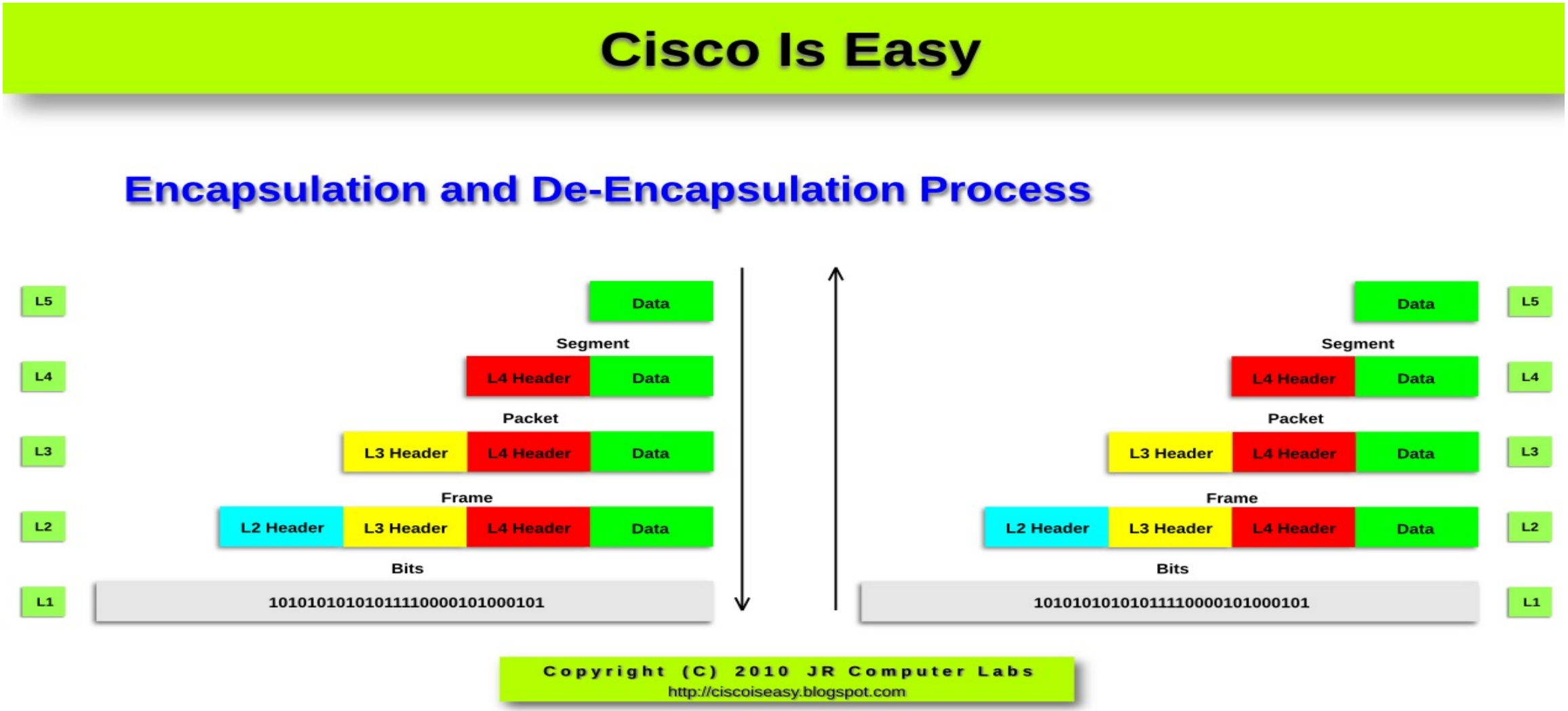
TCP UDP Protocols

Application	Protocol	Port Number
File Transfer Protocol FTP Client	TCP	20
File Transfer Protocol FTP Server	TCP	21
Secure Shell SSH	TCP	22
Telnet	TCP	23
Simple Mail Transport Protocol SMTP	TCP	25
Domain Name System DNS	UDP / TCP	53
Dynamic Host Configuration Protocol DHCP	UDP	67,68
Trivial File Transfer Protocol TFTP	UDP	69
Hypertext Transfer Protocol HTTP	TCP	80
Post Office Protocol 3 POP3	TCP	110
Simple Network Management Protocol SNMP	UDP	161
Hypertext Tranfer Protocol Secure HTTPS	TCP	443

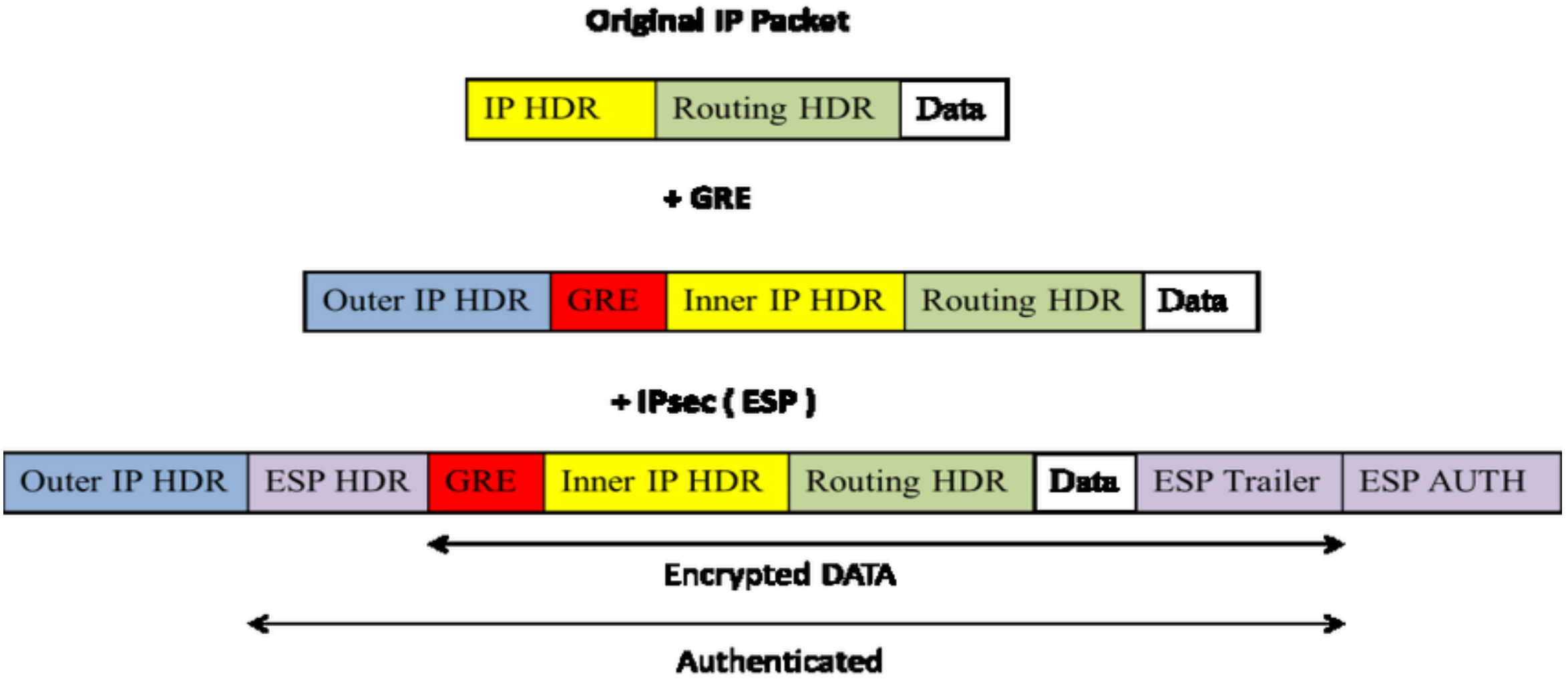
BPDU Structure

- Ipv4 packet structure the fields of the ipv4 header
- combination of data and layer 4 header is called a segment
- combination of data layer 4 header layer 3 header is called Packet

Encapsulation Decapsulation Process



GRE IPSEC Encapsulation of a Packet



- AutoMDIX allows devices to detect which pin their neighbors are on and adjust the pins
- vlan tagging switches will tag all vlan over the trunk port
- ISL and 802.1q are the 2 protocol for trunking ISL is cisco propietary 802.1q is industry standard ISL is no longer used
- 802.1q tag is inserted in a field between the ethernet header the tag is 4 bytes or 32 bit
- 802.1q has a featured called the native vlan wich is vlan 1 by default
- when a switch received a untagged frame it will asume it belongs to the native vlans

Switch Operation

- DTP is a Cisco proprietary protocol that allows interfaces to negotiate trunks
- For security considerations dtp should be disabled in all interfaces
- Switch port in dynamic desirable will activate negotiate to form a trunk with other switches
- a switch in dynamic auto will not actively try to form a trunk but just passible
- static access means a static port that belongs to a vlan wich doesnt change
- a switch in dynamic auto will form a trunk with the other switches if the other switch is in dynamic desirable
- a switch port in access mode will stop dtp from sending dtp frames

- VTP allows to configure vlans on a central server switch
- 3 vtp mode that switches operates server client and transparent
- server mode switches can add modified or delete vlans
- vtp advertisement are sent only on trunk ports
- vtp client cannot add modified or delete vlans they just syncronized with the highest revision
- for switches to syncronize among devices they need to have the same domain name
- switches in transparent mode doesn not participate in the vtp domain it have its own database it just forward vtp information if they are in the same domain

VTP

Key Topic

Table 8-3 Expected Trunking Operational Mode Based on the Configured Administrative Modes

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

Administrative Mode with Switch port Mode Command

Key Topic

Table 8-2 Trunking Administrative Mode Options with the **switchport mode** Command

Command Option	Description
access	Always act as an access (nontrunk) port
trunk	Always act as a trunk port
dynamic desirable	Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking
dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking

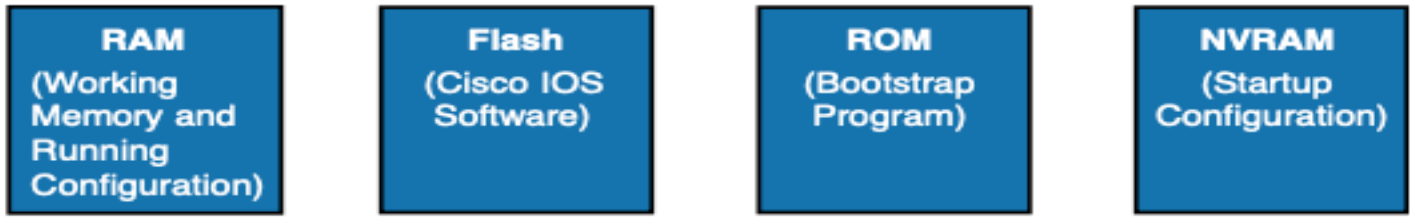
Lan Switches Interfaces Code

Key Topic

Table 7-2 LAN Switch Interface Status Codes

Line Status	Protocol Status	Interface Status	Typical Root Cause
administratively down	down	disabled	The **shutdown** command is configured on the interface.
down	down	notconnect	No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off, (b) **shutdown**, or (c) error disabled.
up	down	notconnect	Not expected on LAN switch physical interfaces.
down	down (err-disabled)	err-disabled	Port security has disabled the interface.
up	up	connected	The interface is working.

Switches Memory Types and IOS



Key Topic

Table 4-5 Names and Purposes of the Two Main Cisco IOS Configuration Files

Configuration Filename	Purpose	Where It Is Stored
startup-config	Stores the initial configuration used anytime the switch reloads Cisco IOS.	NVRAM
running-config	Stores the currently used configuration commands. This file changes dynamically when someone enters commands in configuration mode.	RAM

EtherChannel Formation

Will an EtherChannel Form?

LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

EtherChannel Load Distribution

Table 10-4 EtherChannel Load Distribution Methods

Configuration Keyword	Math Uses...	Layer
src-mac	Source MAC address	2
dst-mac	Destination MAC address	2
src-dst-mac	Both source and destination MAC	2
src-ip	Source IP address	3
dst-ip	Destination IP address	3
src-dst-ip	Both source and destination IP	3
src-port	Source TCP or UDP port	4
dst-port	Destination TCP or UDP port	4
src-dst-port	Both source and destination TCP or UDP port	4

STP

- STP is a layer 2 protocol
- Classic STP is an industry-standard protocol STP prevents layer 2 loops by placing the ports in a blocking state
- VTP enable hello BPDU out of every interface every 2 seconds
- The switch with the lowest bridge ID is elected the root bridge
- in the root bridge, all ports are forwarding
- For a tight breaker the MAC address is used the lowest MAC address will break the thigh
- All switches have 3267 as the default ID

- PVST run a different stp instance per vlan one interface could be forwarding in one vlan and blocking in the other
- all interfaces in the root bridge are designated ports
- when switch boots its a root bridge it will give its position up if it receives a higher BPDU wich mean the lowest ID
- there is one root port on each switch except for the root bridge
- the lowest port ID is the root Port
- each port has a default number of 128
- Blocking and forwarding are stable states
- Listening and learning are transitioning state
- none designated ports are in blocking states
- interfaces in the blocking states does not send traffic but they do receive BPDU
- only designated and root port enter in a forwarding state

The most common spanning tree protocols

PROTOCOL	IEEE STANDARD	SWITCH	DESCRIPTION
Spanning Tree Protocol (STP)	IEEE 802.1D	stp	The original STP version
Rapid STP (RSTP)	IEEE 802.1w	rstp	An evolution of STP 802.1D that addresses the STP convergence time gap issue with enhanced BPDU exchange
Multiple STP (MSTP)	IEEE 802.1s	mstp	A format for mapping multiple VLANs into the same spanning tree to reduce processing on the switch
Per-VLAN Spanning Tree (PVST+)	Cisco protocol based on 802.1D	pvst	An 802.1D enhancement that provides a separate STP instance for each VLAN configured in the network
Rapid PVST+	Cisco protocol based on 802.1w	rapid-pvst	An 802.1w enhancement that provides a separate STP instance for each VLAN, enabling faster convergence times

STP Standard

Key Topic

Table 10-2 STP Standards and Configuration Options

Name	Based on STP or RSTP?	# Trees	Original IEEE Standard	Config Parameter
STP	STP	1 (CST)	802.1D	N/A
PVST+	STP	1/VLAN	802.1D	**pvst**
RSTP	RSTP	1 (CST)	802.1w	N/A
Rapid PVST+	RSTP	1/VLAN	802.1w	**rapid-pvst**
MSTP	RSTP	1 or more*	802.1s	**mst**

STP Port States

Key Topic

Table 9-10 Port States Compared: STP and RSTP

Function	STP State	RSTP State
Port is administratively disabled	Disabled	Discarding
Stable state that ignores incoming data frames and is not used to forward data frames	Blocking	Discarding
Interim state without MAC learning and without forwarding	Listening	Not used
Interim state with MAC learning and without forwarding	Learning	Learning
Stable state that allows MAC learning and forwarding of data frames	Forwarding	Forwarding

STP Port Roles

are instructive about how RSTP works. Table 9-9 lists these RSTP port roles.

Key Topic

Table 9-9 Port Roles in RSTP

Function	Port Role
Port that begins a nonroot switch's best path to the root	Root port
Port that replaces the root port when the root port fails	Alternate port
Switch port designated to forward onto a collision domain	Designated port
Port that replaces a designated port when a designated port fails	Backup port
Port that is administratively disabled	Disabled port

STP Timers

Key Topic

Table 9-7 STP Timers

Timer	Default Value	Description
Hello	2 seconds	The time period between Hellos created by the root.
MaxAge	10 times Hello	How long any switch should wait, after ceasing to hear Hellos, before trying to change the STP topology.
Forward delay	15 seconds	Delay that affects the process that occurs when an interface changes from blocking state to forwarding state. A port stays in an interim listening state, and then an interim learning state, for the number of seconds defined by the forward delay timer.

STP Default Port Cost

Key Topic

Table 9-6 Default Port Costs According to IEEE

Ethernet Speed	IEEE Cost: 1998 (and Before)	IEEE Cost: 2004 (and After)
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	N/A	200
1 Tbps	N/A	20

STP/RSTP Reason for Forwarding or Blocking

Key Topic

Table 9-3 STP/RSTP: Reasons for Forwarding or Blocking

Characterization of Port	STP State	Description
All the root switch's ports	Forwarding	The root switch is always the designated switch on all connected segments.
Each nonroot switch's root port	Forwarding	The port through which the switch has the least cost to reach the root switch (lowest root cost).
Each LAN's designated port	Forwarding	The switch forwarding the Hello on to the segment, with the lowest root cost, is the designated switch for that segment.
All other working ports	Blocking	The port is not used for forwarding user frames, nor are any frames received on these interfaces considered for forwarding.

Key Topic

Table 8-3 Expected Trunking Operational Mode Based on the Configured Administrative Modes

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

[1] When two switches configure a mode of "access" on one end and "trunk" on the other, problems occur. Avoid this combination.

Layer 3 Switch

- Routes Traffics

Routes Traffic Similar to a router when enabling routing Mode

Port Security Violations

Table 6-2 Actions When Port Security Violation Occurs

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

CDP Commands

Table 9-3 show cdp Commands That List Information About Neighbors

Command	Description
show cdp neighbors [*type number*]	Lists one summary line of information about each neighbor or just the neighbor found on a specific interface if an interface was listed
show cdp neighbors detail	Lists one large set (approximately 15 lines) of information, one set for every neighbor
show cdp entry *name*	Lists the same information as the **show cdp neighbors detail** command, but only for the named neighbor (case sensitive)

LLDP Commands

Topic

- **[no] lldp run:** A global configuration command that sets the default mode of LLDP operation for any interface that does not have more specific LLDP subcommands (**lldp transmit**, **lldp receive**). The **lldp run** global command enables LLDP in both directions on those interfaces, while **no lldp run** disables LLDP.
- **[no] lldp transmit:** An interface sub-command that defines the operation of LLDP on the interface regardless of the global [**no**] **lldp run** command. The **lldp transmit** interface subcommand causes the device to transmit LLDP messages, while **no lldp transmit** causes it to not transmit LLDP messages.
- **[no] lldp receive:** An interface subcommand that defines the operation of LLDP on the interface regardless of the global **[no] lldp run** command. The **lldp receive** interface subcommand causes the device to process received LLDP messages, while **no lldp receive** causes it to not process received LLDP messages.

POE

- Power policing prevents a POE to take to much power
- solution to prevent tail drop is random early detection

QOS

- NBAR performs a deep packet inspection beyond TCP all the way up to layer 7
- Classification gives priority To traffic over others
- PCP field is in the trunk is referred to as COS
- in the ipv4 Header, there is a byte called TOS type of service
- standard IPP marking is Similar to PPC
- DF default forwarding is the marking for Best Effort
- EF expedited forwarding is for the required low-loss
- AF Assure Forwarding highest packets will be forwarded compared to low packets
- Low Latency Queuing creates a priority Que
- QOS Platinum should be used for voice silver is the best effort by default gold for video traffic bronze is the lowest option for Background traffic

QOS Clasifiers

Topic

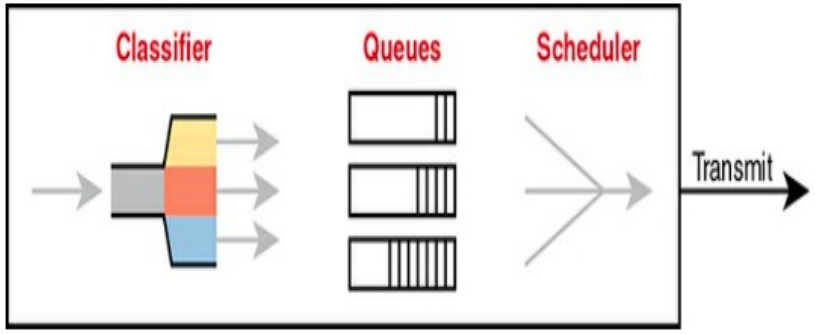


Figure 11-14 *Queuing Components*

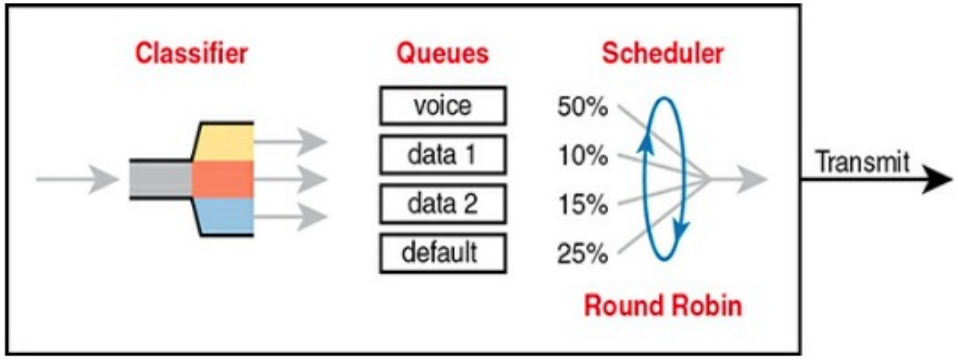
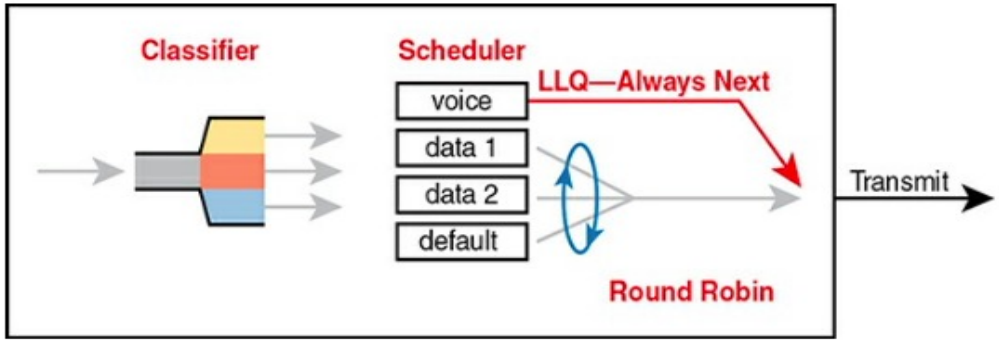


Figure 11-16 *Round Robin Not Good for Voice Delay (Latency) and Jitter*

Topic



Syslog Severity Levels

Keyword	Numeral	Description	
Emergency	0	System unusable	Severe
Alert	1	Immediate action required	
Critical	2	Critical Event (Highest of 3)	Impactful
Error	3	Error Event (Middle of 3)	
Warning	4	Warning Event (Lowest of 3)	
Notification	5	Normal, More Important	Normal
Informational	6	Normal, Less Important	
Debug	7	Requested by User Debug	Debug

Figure 9-3 *Syslog Message Severity Levels by Keyword and Numeral*

Security

Table 4-4 Summary of Human Security Vulnerabilities

Attack Type	Goal
Social engineering	Exploits human trust and social behavior
Phishing	Disguises a malicious invitation as something legitimate
Spear phishing	Targets group of similar users
Whaling	Targets high-profile individuals
Vishing	Uses voice calls
Smishing	Uses SMS text messages
Pharming	Uses legitimate services to send users to a compromised site
Watering hole	Targets specific victims who visit a compromised site

Malware Types

Table 4-3 Summary of Malware Types

Characteristic	Trojan Horse	Virus	Worm
Packaged inside other software	Yes	No	No
Self-injected into other software	No	Yes	No
Propagates automatically	No	No	Yes

- **User awareness:** All users should be made aware of the need for data confidentiality to protect corporate information, as well as their own credentials and personal information. They should also be made aware of potential threats, schemes to mislead, and proper procedures to report security incidents. Users should also be instructed to follow strict guidelines regarding data loss. For example, users should not include sensitive information in emails or attachments, should not keep or transmit that information from a smartphone, or store it on cloud services or removable storage drives.
- **User training:** All users should be required to participate in periodic formal training so that they become familiar with all corporate security policies. (This also implies that the enterprise should develop and publish formal security policies for its employees, users, and business partners to follow.)
- **Physical access control:** Infrastructure locations, such as network closets and data centers, should remain securely locked. Badge access to sensitive locations is a scalable solution, offering an audit trail of identities and timestamps when access is granted. Administrators can control access on a granular basis and quickly remove access when an employee is dismissed.

Commands and Encoding Types for the **username secret** Command

Table 5-3 Commands and Encoding Types for the **username secret** Command

Command	Type	Algorithm
username *name* [**algorithm-type md5**] **secret** *password*	5	MD5
username *name* **algorithm-type sha256 secret** *password*	8	SHA-256

WIRELESS

- Type of Wireless Connection

WEP WPA WAP2

RF is an electromagnetic frequency

CSMA/CD is used in wired connections to recover collision CSMA/CA is used in wireless to avoid collision

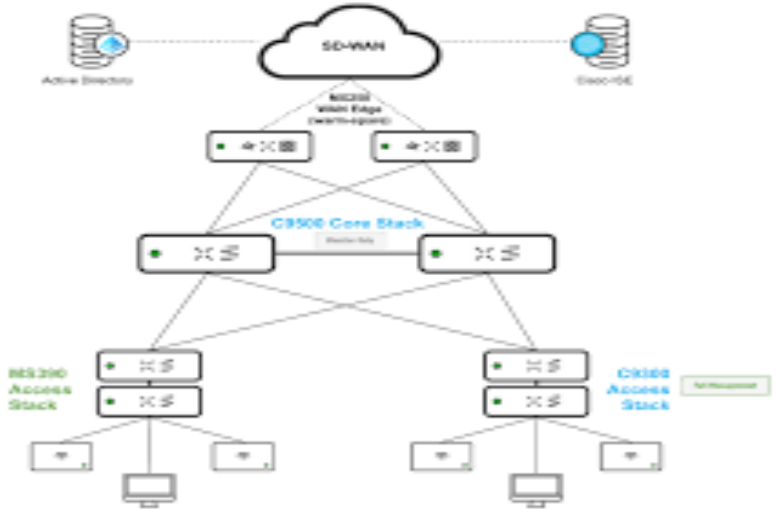
Wi-Fi use 2 bands 2.4 ghz and 5 ghz

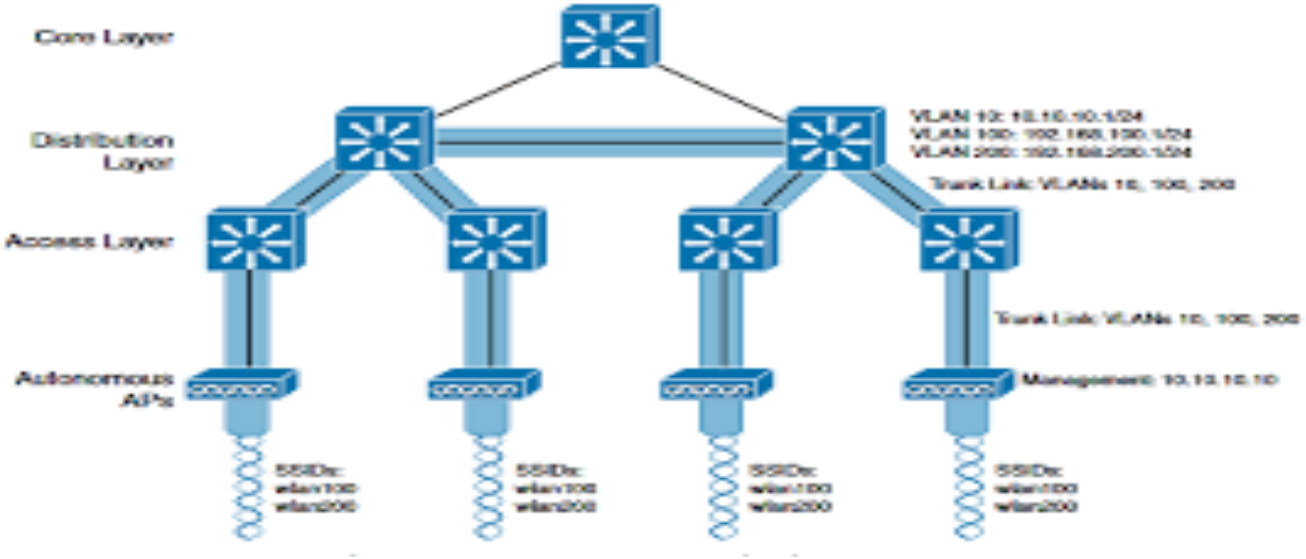
- Wi-Fi 6 has expanded to the 6GHZ band
- channel bonding can be used to combine the channel
- IBSS is a wireless connection in which 2 devices connect directly without using an AP This is called ad-hoc
- BSS clients connect to each other Via AP but not directly with each other
- When you move between AP in an extended service set is called Roaming
- MBSS (Mesh Basic Set Service) is used when is difficult to run an ethernet connection to the AP
- MBSS in Repeater Mode can extend the range

Wireless Architecture

- Beacons are sent periodically to AP to advertise BSS
- There are 3 types of wireless LAN deployment Autonomous Lightweight and cloud
- Autonomous AP does not rely on a WLC (Wireless LAN controller) they are configured individually This is fine for Small Network
- a Wireless LAN architecture with Controller a CAPWAP tunnel is created
- WLC provide channel assignment
- In sniffer mode the AP is dedicated to capturing packets it doesn't BSS for the Client

- Cloud base architecture is between Autonomous AP and split architecture one example is Meraki
- Lightweight AP Are Managed By a Centralized controller Cloud Base AP is Managed by a Central Device like Cisco Meraki

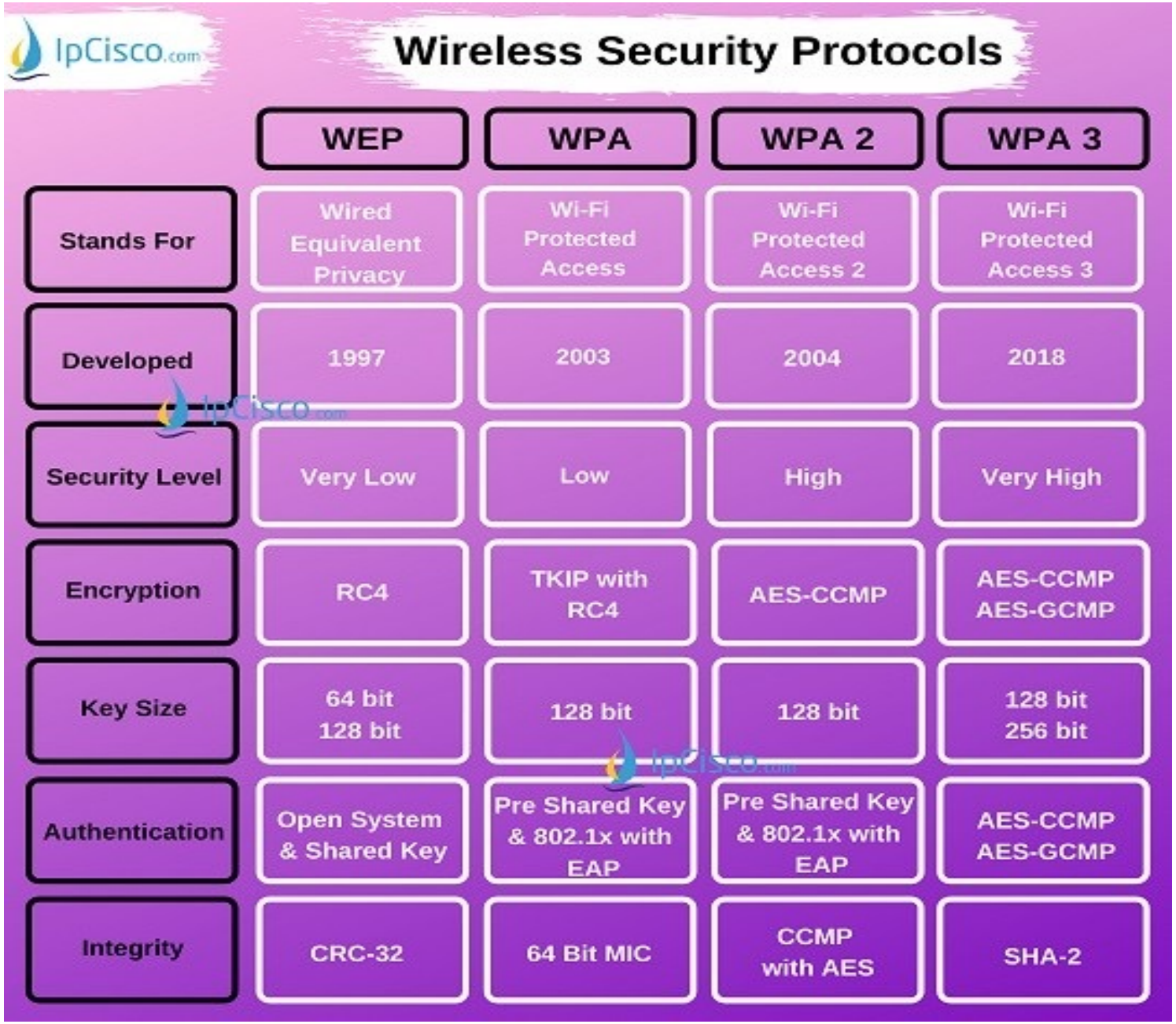




Wireless Encryption

- all client must be authenticated before they can join the SSID
- integrity ensured the message is not modified in transit for that a MIC is added
- Open authentication is the first standard client sends the request and the AP accepts all is not secure
- WEP is another way of authentication it provides encryption it uses RC4 wep is not secured regardless of the lenght of the Key
- EAP is a framework where other methods are based on
- in EAP used authenticator authentication server and the suplicant

- LEAP is the improvement for for WEP is vulnerable and is not used anymore
- EAP-TLS required certification in the client and the server
- TKIP is based on WEP but has more security Features TKIP is more Secure than WEP
- CCMP is more secure it uses WPA2 it uses AES for counter mode
- GCMP is more secure and more efficient than CCMP it is used in Wi-Fi protected 3
- PSK is used to generate encryption KEy
- all 3 WPA use personal and enterprise mode
- SAE protects the 4 way handshake using Personal Mode
- WLC only supports static LAG and the port is supposed to be configured to mode on


IpCisco.com
Wireless Security Protocols
WEP
WPA
WPA 2
WPA 3
Stands For
Wired Equivalent Privacy
Wi-Fi Protected Access
Wi-Fi Protected Access 2
Wi-Fi Protected Access 3
Developed
1997
2003
2004
2018
Security Level
Very Low
Low
High
Very High
Encryption
RC4
TKIP with RC4
AES-CCMP
AES-CCMP AES-GCMP
Key Size
64 bit 128 bit
128 bit
128 bit
128 bit 256 bit
Authentication
Open System & Shared Key
Pre Shared Key & 802.1x with EAP
Pre Shared Key & 802.1x with EAP
AES-CCMP AES-GCMP
Integrity
CRC-32
64 Bit MIC
CCMP with AES
SHA-2

Wireless Characteristics

Key Topic

Table 26-3 Basic Characteristics of Some IEEE 802.11 Amendments

Amendment	2.4 GHz	5 GHz	Max Data Rate	Notes
802.11-1997	Yes	No	2 Mbps	The original 802.11 standard ratified in 1997
802.11b	Yes	No	11 Mbps	Introduced in 1999
802.11g	Yes	No	54 Mbps	Introduced in 2003
802.11a	No	Yes	54 Mbps	Introduced in 1999
802.11n	Yes	Yes	600 Mbps	HT (high throughput), introduced in 2009
802.11ac	No	Yes	6.93 Gbps	VHT (very high throughput), introduced in 2013
802.11ax	Yes	Yes	4x 802.11ac	High Efficiency Wireless, Wi-Fi6; expected late 2019; will operate on other bands too, as they become available

Authentication and Encryption Comparison

Key Topic

Table 28-2 Comparing WPA, WPA2, and WPA3

Authentication and Encryption Feature Support	WPA	WPA2	WPA3*
Authentication with **Pre-Shared Keys?**	Yes	Yes	Yes
Authentication with **802.1x?**	Yes	Yes	Yes
Encryption and MIC with **TKIP?**	Yes	No	No
Encryption and MIC with **AES and CCMP?**	Yes	Yes	No
Encryption and MIC with **AES and GCMP?**	No	No	Yes

Wireless Security Mechanism

Key Topic

Table 28-3 Review of Wireless Security Mechanisms and Options

Security Mechanism	Type		Type Expansion	Credentials Used
Authentication Methods	Open		Open Authentication	None, other than 802.11 protocol
	WEP		Wired Equivalent Privacy	Static WEP keys
	802.1x/EAP (Extensible Authentication Protocol)	LEAP	Lightweight EAP	Deprecated; uses dynamic WEP keys
		EAP-FAST	EAP Flexible Authentication by Secure Tunneling	Uses protected access credential (PAC)
		PEAP	Protected EAP	AS authenticated by digital certificate
		EAP-TLS	EAP Transport Layer Security	Client and AS authenticated by digital certificate
Privacy & Integrity Methods	TKIP		Temporal Key Integrity Protocol	N/A
	CCMP		Counter/CBC-MAC Protocol	N/A
	GCMP		Galois/Counter Mode Protocol	N/A

L2 Wireless Lan Security

scheme to use. Table 29-2 lists the types that are available.

Key Topic

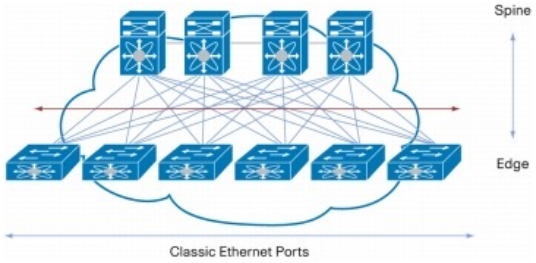
Table 29-2 Layer 2 WLAN Security Type

Option	Description
None	Open authentication
WPA+WPA2	Wi-Fi protected access WPA or WPA2
802.1x	EAP authentication with dynamic WEP
Static WEP	WEP key security
Static WEP + 802.1x	EAP authentication or static WEP
CKIP	Cisco Key Integrity Protocol
None + EAP Passthrough	Open authentication with remote EAP authentication

Frequency Unit

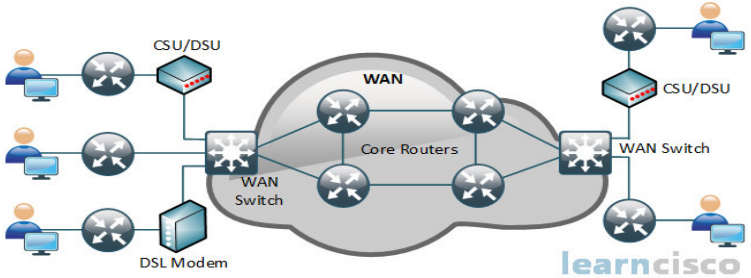
Table 26-2 Frequency Unit Names

Unit	Abbreviation	Meaning
Hertz	Hz	Cycles per second
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1,000,000 Hz
Gigahertz	GHz	1,000,000,000 Hz



Design

- TIER 3 TIER 2
- Tier 2 design includes the core and distribution Together is called the collapse design
- Tier 3 design is set up in the following way Core Distribution and Access
- Spine leaf Design All of the Spine is connected to Leaf switches Leaf switches cannot be connected to leaf switches Spine switches cannot be connected to spine Switches



WAN TECHNOLOGIES

- SITES TO SITES

CE and PE
hub and spoke the central site is called the hub the branches connected are called the spoke traffic can be controlled which one can enter and can not

MPLS are shared networks the label switching allows VPN to separated traffic between router

CE mean costumer routers PE routers are provider router and the P

- MPLS label use MPLS label to decide where to send the router
- when forming LAYER 3 VPN in MPLS a routing protocol can be used or a static route can be set between the CE and PE
- When using LAYER 2 VPN the connection will be transparent to the customer
- IPSEC does not support broadcast or Multicast
- GRE creates tunnel like IPSEC but it does not encrypt the original packet so its not secured but it encapsulated broadcast and multicast
- DMVPN is a cisco develop product that allows you to create a full mesh VPN
- remote to site VPN use TLS
- VPN Client software like cisco anyconnect are installed on end devices then the end devices create a tunnel to the remote device

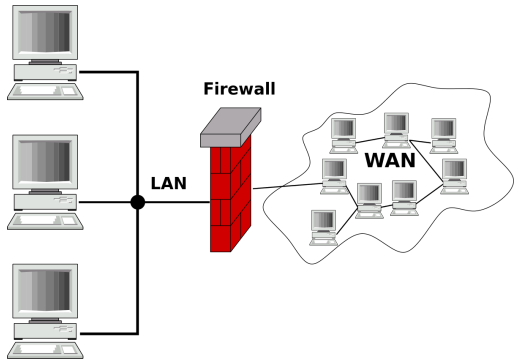
Metro Ethernet

Metro Ethernet Access

Name	Speed	Distance
100BASE-LX10	100 Mbps	10 Km

Technet24

Ethernet Line Service	E-Line	Point-to-point	Two customer premise equipment (CPE) devices can exchange Ethernet frames, similar in concept to a leased line.
Ethernet LAN Service	E-LAN	Full mesh	This service acts like a LAN, in that all devices can send frames to all other devices.
Ethernet Tree Service	E-Tree	Hub and spoke; partial mesh; point-to-multipoint	A central site can communicate to a defined set of remote sites, but the remote sites cannot communicate directly.



Firewalls

- Firewalls forward traffic based on rules it controls what enters into the network or goes out

Firewalls Types

Topic

- **Traditional firewall:** An NGFW performs traditional firewall features, like stateful firewall filtering, NAT/PAT, and VPN termination.
- **Application Visibility and Control (AVC):** This feature looks deep into the application layer data to identify the application. For instance, it can identify the application based on the data, rather than port number, to defend against attacks that use random port numbers.
- **Advanced Malware Protection:** NGFW platforms run multiple security services, not just as a platform to run a separate service, but for better integration of functions. A network-based antimalware function can run on the firewall itself, blocking file transfers that would install malware, and saving copies of files for later analysis.
- **URL Filtering:** This feature examines the URLs in each web request, categorizes the URLs, and either filters or rate limits the traffic based on rules. The Cisco Talos security group monitors and creates reputation scores for each domain known in the Internet, with URL filtering being able to use those scores in its decision to categorize, filter, or rate limit.
- **NGIPS:** The Cisco NGFW products can also run their NGIPS feature along with the firewall.

- **Traditional IPS:** An NGIPS performs traditional IPS features, like using exploit signatures to compare packet flows, creating a log of events, and possibly discarding and/or redirecting packets.
- **Application Visibility and Control (AVC):** As with NGFWs, an NGIPS has the ability to look deep into the application layer data to identify the application.
- **Contextual Awareness:** NGFW platforms gather data from hosts —OS, software version/level, patches applied, applications running, open ports, applications currently sending data, and so on. Those facts inform the NGIPS as to the often more limited vulnerabilities in a portion of the network so that the NGIPS can focus on actual vulnerabilities while greatly reducing the number of logged events.
- **Reputation-Based Filtering:** The Cisco Talos security intelligence group researches security threats daily, building the data used by the Cisco security portfolio. Part of that data identifies known bad actors, based on IP address, domain, name, or even specific URL, with a reputation score for each. A Cisco NGIPS can perform reputation-based filtering, taking the scores into account.
- **Event Impact Level:** Security personnel need to assess the logged events, so an NGIPS provides an assessment based on impact levels, with characterizations as to the impact if an event is indeed some kind of attack.

Cabling

- Straight Through Crossover ethernet cables
- Crossover cable is used to connect switch to switch and router to Router
- Straight Through Cable is used to connect PC to a switch or Router
- Copper UTP Cable can be used up to 100 meter
- Standards for Fiber Cable 100 base lx speed 1gbs multimode or single mode up 550 km standard 802.3z

- 10gbase -SR 10GBS MULTIMODE 400 KM standard 802.ae
- 10GBASE-LR 10GBS SINGLE MODE 10KM standard 802.ae
- 10BASE-ER 10GBS SINGLE MODE 30 KM standard 802.ae
- Crossover cable is used to connect switch to switch and router to Router
- Straight Through Cable is used to connect the PC to a switch or Router
- Copper UTP Cable can be used up to 100 meter
- 10 base t is 10 m 100 base t is 100 meter 1000 base t is 100 meter 10 g base t 100 meter
- 10 base T fast ethernet cable use 2 pair of cable or only 4 fair pair pin position at 1 and 2 switches receive data in PIN and 1 and 2

- on the switch pin 3 and 6 is used to transmit data on the PC 3 and 6 is used to receive Data
- on a router transmit data on pin 1 and 2 and receive in 3 and 6

Table 2-4 A Sampling of IEEE 802.3 10-Gbps Fiber Standards

Standard	Cable Type	Max Distance*
10GBASE-S	MM	400m
10GBASE-LX4	MM	300m
10GBASE-LR	SM	10km
10GBASE-E	SM	30km

* The maximum distances are based on the IEEE standards with no repeaters

Key Topic

Table 2-2 Examples of Types of Ethernet

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

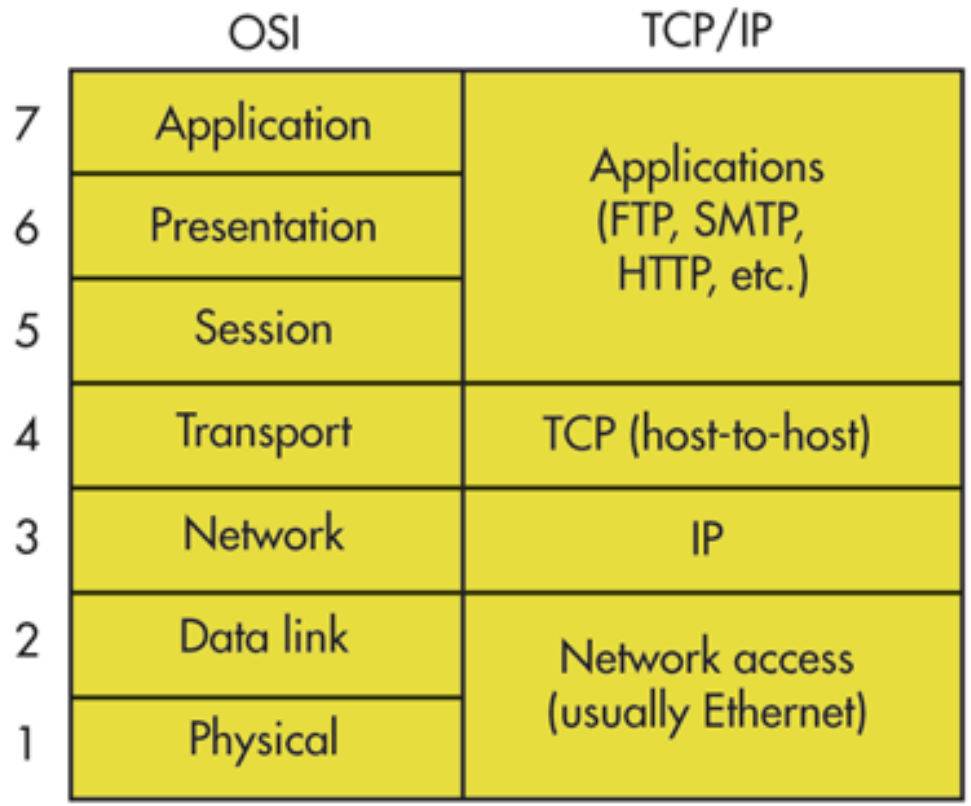
Cabling Comparison

Key Topic

Table 2-5 Comparisons Between UTP, MM, and SM Ethernet Cabling

Criteria	UTP	Multimode	Single-Mode
Relative Cost of Cabling	Low	Medium	Medium
Relative Cost of a Switch Port	Low	Medium	High
Approximate Max Distance	100m	500m	40km
Relative Susceptibility to Interference	Some	None	None
Relative Risk of Copying from Cable Emissions	Some	None	None

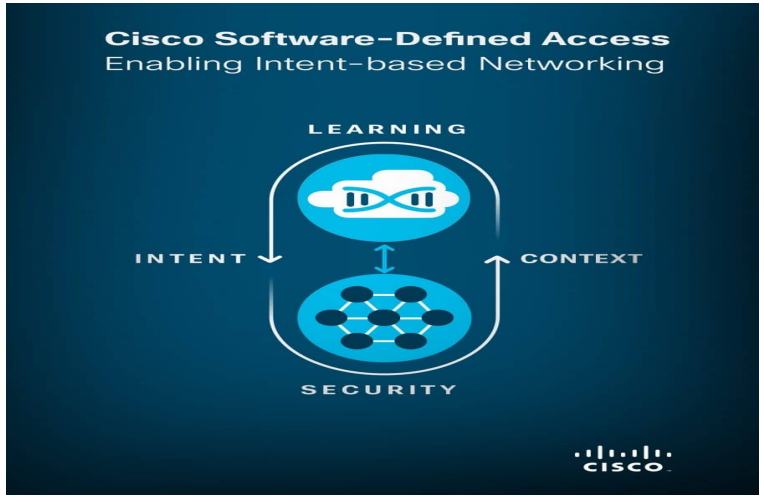
OSI


OSI
TCP/IP
7
Application
6
Presentation
5
Session
Applications
(FTP, SMTP,
HTTP, etc.)
4
Transport
TCP (host-to-host)
3
Network
IP
2
Data link
1
Physical
Network access
(usually Ethernet)

TCP/IP Architectural and Protocol

Table 1-2 TCP/IP Architectural Model and Example Protocols

TCP/IP Architecture Layer	Example Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Internet	IP, ICMP
Data Link & Physical	Ethernet, 802.11 (Wi-Fi)



Automation and Programmability

- XML YANG YAML
- HTTPS uses CRUD API and HTTP uses Rest API as the communication protocol
- SDN is a approach to network that centralized the control plane in a controller
- Data serialization is the process of storing data in a file

- Jason allows to representation Variables with text Variables are containers that store Values
- JSON can be used to store Data and Exchange Data
- in JSON white space is insignificant they don’t change the meaning of the data
- A string is a text value surrounded by double quotes
- number is a numeric value is not surrounded by quotes
- A Boolean is a data type that can be only true or False
- A null is the absence of data value
- objects are surrounded by double quotes a key which is String is surrounded by double quotes as well
- The key and the value are separated by a comma
- Objects within objects is called nested objects
- an A Array is a series of values separated by comma

XML

- Like Jason white space means nothing
- the key is tagged with the value in the middle
- XML is quite similar to HTML it uses tagges
- YAML is another serialization data language
- YAML is used by ansible
- in YAML white space is significant YAML Start with 3 Hifens ---

Underlay and Overlay

- the underlay is the physical underlining like physical devices underlay is a bunch of switches
- the overlay is the virtual physical network built on top of the physical network
- SDA uses a protocol called VXLAN to Build tunnels fabric is the term we use for the overlay and underlay as a hole
- the edge nodes connect to the end host and the Border nodes connect devices outside the SD-Access example connecting to wan devices

- Configuration Management tools like Ansible Puppet and Chef allow us to do massive configurations of devices
- Ansible is written in Python Ansible is agentless Ansible uses ssh to connect to devices make configuration changes get information etc ansible uses a push model Ansible server called the control mode playbook is the blueprint of the task and these files are written in YAML you also need the inventory file and templates
- Puppet and chef use the Pull Model
- Puppet is written in Ruby puppet is agent-based the server is called Puppet Master and uses TCP 8140 and use Pull Model
- Chef like Puppet is agent-based and use a pull Mode TCP port 1002 Chef File uses DSL Which is a proprietary Language written in Ruby
- Puppet and chef both communicate using HTTP
- devices that communicate between the SBI are netconf and Restconf

API Comparison

Table 18-2 Comparing CRUD Actions to REST Verbs

Action	CRUD Term	REST (HTTP) Verb
Create new data structures and variables	Create	POST
Read (retrieve) variable names, structures, and values	Read	GET
Update or replace values of some variable	Update	PATCH, PUT
Delete some variables and data structures	Delete	DELETE

Ansible Puppet and Chef Comparison

Table 19-2 Comparing Ansible, Puppet, and Chef

Action	Ansible	Puppet	Chef
Term for the file that lists actions	Playbook	Manifest	Recipe, Runlist
Protocol to network device	SSH, NETCONF	HTTP (REST)	HTTP (REST)
Uses agent or agentless model	Agentless	Agent*	Agent
Push or pull model	Push	Pull	Pull

* Puppet can use an in-device agent or an external proxy agent for network devices.

SNMP Messages

SNMP Message Types

The ONS 15454 SNMP agent communicates with an SNMP management application using SNMP messages. The following table describes these messages.

Table 1. ONS 15454 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request.
set-request	Provides remote network monitoring (RMON) MIB.
trap	Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager.