		OSI		Tcp/ip	PDU	Protocols	Devices + Terms
Away	All	Application		Application	Data	DNS, TFTP, FTP, SMTP, IMAP, POP3 HTTP, DHCP, Telnet, SSH, https	
pizza	People	Presentation			Data	JPG, GIF, mp3, mp4, MPEG	Compression Encryption Encoding
[illegible]	Seem	Session			Data	SMB	Creates and maintains Dialog
Throw	To	Transportation		Transport	Segments	TCP, UDP	Connectionless, connection oriented Sequence numbers, port numbers, Error correction flow control, windowing
Not	Need	Network		Internet	packets	RIP, OSPF, EIGRP, IPv4, IPv6 ICMP ARP	Connectionless, Router, logical addresses, Routing
Do	Data	Data link	LLC Mac	Network Access	Frames	Ethernet CDP, STP, PPP, HDLC, Frame relay	error detection, switching, Bridge Data link layer address NIC
Pleas	Processing	Physical			Bits	802.11 a,b,c, N, AC. TIA, EIA 568	Hub, Access point, Repeater, copper RF, Fiber, unshielded twisted pair STP

1st octet	1	2	3	4	5	6	7	8
2nd octet	9	10	11	12	13	14	15	16
				4096	2048	1024	512	256
3rd octet	17	18	19	20	21	22	23	24
4th octet	25	26	27	28	29	30	31	32
Bits / Host	128	64	32	16	8	4	2	1
Subnet	128	192	224	240	248	252	254	255

Well Known ports	0-1023	privat IPS	10.0.0.0/8
Registered ports	1024-49151		172.16.0.0/12
private / Dynamic Ports	49152-65535		192.168.0.0/16

Top level domain .com, .co, .org, .au

DHCP

→ DHCP Discover

← DHCP Offer

→ DHCP Request

← DHCP Acknowledge

Reduce Brute Force login by

- login block-for "120" attempts "3" within "60"
- executive time out "120"

Base Configuration

(conf) Hostname "any"

~~Disable~~ No IP Domain-Lookup

IP domain-name "cisco.com"

Security password min-length "5"

~~Service~~ enable Secret "Cisco"

Service password-encryption

Line con 0

Pass "Cisco"

Login

Line VTY 0 4

~~Pass~~ Login local

Transport input "ssh" "telnet"

(conf) username "cisco" password "cisco"

Crypto Key generate mod RSA 2048

Banner MOTD ^" any" ^

Router only ipv6 unicast-routing

Switch sdm prefer dual-ipv6-and ipv4 default

Routers (int) ipv6 add FE80::1 Link local

- Distance vector protocol routes entire routing information
- Routers will prefer static routes / Connected routes
- A MTU size of 1600 Can cause baby giant errors
- Private IP Address Range

Class A	10.0.0.0	to	10.255.255.255	/8	255.0.0.0
Class B	172.16.0.0	to	172.31.255.255	/12	255.240.0.0
Class C	192.168.0.0	to	192.168.255.255	/16	255.255.0.0

- WAN data link encapsulation types are Frame relay and PPP
- Flow Control is used to provide a means for the receiver to govern the amount of data sent by the sender
- OSPF supports VLSM, Can Confine network instability to one area of the network, and it allows extensive Control of routing updates
- "line protocol is up" means the interface is receiving Keepalives
- ping is also used to verify ipv6 Connectivity
- At a minimum fresh routers need to no shut ports to bring up CDP (CDP enabled by default)
- D - Eigrp^{90}, O - OSPF^{110}, S - Static^{1}, R - RIP^{120}, B - BGP, C - Connected^{0}
- Dynamic Auto is compatible with Trunk, Access, and desirable ports
- Native VLAN must be configured the same on 802.1q trunking devices
- Layer 2 switches increase the number of Collision domains and implements VLAN'S.
- Late collisions happen when a Cable is too long.
- CSMA/CD Carrier Sense Multiple Access with Collision Detection
  - Devices have to wait until lan is silent to transmit.
  - if collision happens the device that caused waits a random amount of time.
- Workstations require TCP Connection to be established before exchanging Httppackets with server
- Broadcast storms Cause Congestion on the lan
- TCP - Transmission Control protocol UDP - User Datagram Protocol

- Ping - Echo request to address, wait for reply, address replys back default timeout cisco 2 sec
- Enabling port security and adding "Sticky" adds dynamically learned mac's to run config
- Port security is used to Prevent unauthorized hosts from accessing the lan
- Physically securing network equipment should be part of any Comprehensive Security plan
- "NTP Master" sets the local device as the reference Clock Source
- Stratum indicates the distance between a device and its time source
- Default source of NTP message is the interface of the next hop for server peer
- First 24 bits of a MAC address is the OUI Organizational Unique Identifier
- Data must be encapsulated to traverse the network
- Full-duplex Ethernet networks remove Collisions, require dedicated ports and require network interface Cards (NIC) that can operate in full-duplex
- Smtp → application Layer, TCP → Transport Layer, IP → internet layer, Ethernet → Network access layer
- Network layer headers Contain the address of destination hosts
- TCP/IP Stack model Combines physical and data link layers into the network access layer
- FTP is connection oriented, TFTP is connection Less Oriented
- Flow label is new in ipv6
- 11111100 begins a unique local IPv6 address in binary
- According to IANA, ISPs assign IPv6 addresses to end users
- Three approaches to Migrating from ipv4 addressing to ipv6 is

    Configure ipv4 tunnels between ipv6 islands

    Use proxying and translation to translate ipv6 packets into ipv4 packets

    enable dual-stack routing

- IPv6 eliminates broadcasts and replaces them with multicasts
- Default DHCP Binding Lease time is 24 hours

Ospf Router-id's are chosen by highest IP of Loopback when no ID is specified

- Routers running link-state routing protocols use hello packets and LSAs from other routers to build and maintain its topological database

- Directly connected Routes have an administrative distance of Ø
- EIGRP Summary routes have an administrative distance of 5
- Link-state routing protocols provide common view of entire topology, Calculates shortest path, and Utilizes event triggered updates
- Default routes keep routing tables small and allow connectivity to remote networks
- RIP v2 has same max hop as =15 initial v1, it allows classless routing and supports authentication
- Administrative distance of Directly connected routes is Ø
- Passive-interfaces prevent hello messages on an interface
- Rip is a dynamic routing protocol that uses only hop count
- LSA - Link State Advertisement
- IP address of the remote router for forwarding packets is indicated by next hop in Routing table
- ICND1 Complete Administrative distance ranks routing protocols according to their preferences.
- STP uses path cost to determine which port to block on (Highest Mac) non-root bridge
- STP uses Lowest mac to determine root bridge
- Eigrp Redistribute static, OSPF is Default information originate
- OIA - is a Route from another area (ospf)
- OSPF uses link local for source and global unicast for destination
- OSPF multicast 224.0.Ø.5-6 and FFØ2::5 and FF02::6
- OSPF LSA1 is inter area
- OSPF LSA 2 is multi access
- OSPF LSA 3 is intra area
- OSPF LSA 4 is ASBR
- OSPF LSA 5 is summary ASBR
- Link state routing builds entire topology (ospf, ISIS)
- Switchport Host adds portfast, makes Access port and disables bpdu
- VTP Client with a higher revision will update entire domain.

- Switches by default try to trunk. auto mode with auto will not trunk
- VTP default Mode is server
- OSPF Election 1) Highest priority 2) highest Router ID 3) highest Loopback, 4) highest active interface
- StP Port Roles
1) Root Port (RP)
2) Designated (D)
3) Alternate (A only RSTP)
4) Blocking

Classic Spanning tree	Rapid Spanning tree
Blocking	Discarding
Listening	
Learning	Learning
Forwarding	Forwarding

default 32768 - highest 61440 inc of 4096
- Spanning-tree Root bridge is elected by 1) Priority, 2) BID, 3) Lowest Mac
- Link state routing protocols use the link router interface ip address, the network link and the cost of the link as link state information for locally connected links
- Protocol-dependent modules route different Layer 3 protocols.
- Autonomus system numbers function as a process ID in the operation of a router
- Two valid OSPF v3 destination addresses are FF02::5 (broadcast) and FE80::42 (link local)
- Eigrp uses lowest configured bandwith of any interface along the route to calculate the bandwidth to a destination network
- Ospf route with a OE1 is an external route advertised by a ASBR
- Ospf router election process is -
  1) Router uses explicitly configured router ID
  2) Router uses highest ip of loopback
  3) Router uses highest ip of active interfaces
  4) Router will display console message to configure the router-ID
- Show ipv6 protocols can show all ospf enabled interfaces
- VTP transfers vlan database across trunks, server mode stores vlan.dat and vlans can be created modified and deleted on the Server Switch
- by default Cisco devices can have 4 equal cost routes to same destination
- best to manually add vlan.dat from server when adding a switch

- Externally learned EIGRP routes show up as EX
- Eigrp (redistribute static), OSPF (Default information originate)
- Three effects of using local span are:
  - It doubles the load on the Forwarding engine
  - It Prevents span destination from using port Security
  - It doubles internal switch traffic
- Two device classes used over Serial links are DCE and DTE.
- Autonomous system number and ip are used to identify neighbors in BGP
- VLANs can experiance slowness due to duplex mismatch.
- RSTP defines new port roles and is compatible with the original 802.1D STP
- EIGRP successor routes are used to forward traffic to a destination and may be backed up by a feasible successor route.
- Encapsulation is a feature that facilitates the tagging of frames on specific VLANS
- ESP is used when Confidentiality is required on a IPsec Link
- Discarding and Forwarding are two states of RSTP when the network has converged
- Same AS number is required for EIGRP to establish adjacencys
- Three benefits of running TACACS are:
  - device-administration packets are encrypted in their entirety
  - It allows the users to be authenticated against a remote server
  - It supports access-level authorization for commands
- Packet-Loss and Hardware forwarding issues can cause inter-Vlan slowness
- Cloud Computing requires High Speed broadband
- GRE Sends packets in plain text
- IGP may use Dijkstra or Bellman-Ford algorithm
- ACL APIC-EM Path runs on Layer 4
- Aggregated chassis technology reduces Management overhead and requires only one IP address per VLAN
- RADIUS only encrypts the password

- Stacked switches reduce management complexity and have a single management interface
- Port Filter ACL's are applied first
- Link Local addresses must be configured on all IPv6 interfaces
- Accept, Reject, Error and continue are all responses from a TACACS daemon
- APIC-EM path trace ACL's check ingress and egress interfaces.
- Ospf uses Dijkstra, Rip uses Bellman-Ford and EIGRP uses DUAL
- Link state protocol uses instant updates
- BGP goes through active, idle and open sent states when establishing peer sessions
- Show Snmp group can show current SNMP Security model
- If proxy ARP is configured on multiple devices, the internal L2 network becomes vulnerable to DDoS
- QOS provides checksum and inspection
- CGMP is not compatible with HSRPv1
- IaaS and PaaS may require network infrastructure redesign
- CHAP uses MD5 for peer authentication.
- MPLS can provide Authentication header and VPN
- debug ppp negotiation and debug dialer packet help troubleshoot a failed pppoe link
- QoS can be marked by ip precedence, DSCP and discard Class
- Remote logging can be enabled With "terminal monitor" and "logging host ip add"
- Port priority value can be modified to create a preferred forwarding interface
- 1 ACL per direction, per "Protocol" layer 3, per interface
- Router-id must be configured to Enable EIGRPv6
- Switch access ports drop packets with 802.1Q tags
- Double tagging attack was mitigated by changing the native VLAN to an unused VLAN
- HSRP active router is chosen by highest ip add and configured priority
- RSTP significantly reduces topology reconvening time after a link failure
- RSTP expands the STP port roles by adding the alternate and backup roles
- RSTP provides a faster transition to the forwarding state on point-to-point links than STP does

- HSRP ip address acts as a default route for that interface.
- Load value in show interface port-channel 1 etherchannel is the number of source-destination pairs
- PVST+ uses 802.1q to tunnel information.
- RSTP Root ports point towards the root bridge Connection
- HSRP produces a virtual mac address starting with $\overset{\text{IPv4}}{00{:}00}$ or $\overset{\text{IPv6}}{00{:}05}$
- Show ip interface can show you interfaces affected by ACL's.
- in QoS ports are untrusted by default.
- When an active HSRP router is preempted by a higher priority router it goes into "Speak" state
- DHCP snooping can validate address requests and filter out invalid messages
- APIC-EM can verify ACL's
- Poison reverse is a learned neighbor with an infinate metric on the route
- A Switch must be in VTP Server or Transparent mode before configuring a VLAN
- ICMP packet ttL is default 255 and is decremented 1 every hop
- SNMP view records can be used to restrict OID Groups
- Default port security mode is Shutdown
- QoS can mark ip precedence, DSCP and discard class
- TACACS+ allows for separate authentication
- APIC-EM requires source address and Destination address to run
- APIC-EM automates network actions and makes network Functions programmable
- Pinging the remote network is the best way to verify a host path
- Enterprise Managed VPN saves Money while securing WAN
- EIGRP internal routes show up as "D"