Final week:

file:///C:/Users/Admin/Downloads/cisco\_100-101.pdf

<https://www.9tut.com/download/CCNAquestions_Jul_7_2015.pdf>

<https://itexamanswers.net/ccna-2-v7-0-final-exam-answers-full-switching-routing-and-wireless-essentials.html>

<https://www.computernetworkingnotes.com/ccna-study-guide/ccna-exam-practice-question-with-answer-1.html>

<https://www.scribd.com/document/733041209/CCNA-200-301-PracticeQuestions-03>

Areas to focus on: WLC, Controller Based/Traditional Networks, IP Connectivity, OSPF, ACLs, Security, Routing Tables, Cables

Notes:

CUT-THROUGH FORWARDING:

* High performance
* Forwarding begins once destination MAC received
* May forward invalid frames

STORE AND FORWARD FORWARDING:

* Error checking before forwarding
* Forwarding begins after entire frame received
* Only forwards valid frames

LINK STATE INTERFACE PROTOCOLS:

* Administratively down = disabled
* down/down = layer 1 problem
* up/disabled = layer 2 problem
* up/up = operational

<https://easy-prep.org/free-ccna-practice-test/security-fundamentals-practice-test#level-1>

Jeremy’s ITLab Exam 1:

1. B, D
2. E, F
3. Lab
4. A, B, C, D, E
5. A
6. A or D
7. C
8. B, C
9. A, F
10. A, E, C,
11. B
12. A, C, E
13. C
14. A
15. A
16. D
17. A, C, D, E
18. A, B
19. C
20. B, D, E
21. B, C
22. A
23. B
24. A, D, F
25. A, B, C
26. C
27. B
28. D
29. B
30. A, B, C
31. C
32. A
33. B
34. D
35. C, D
36. A
37. D
38. C
39. C, D, E
40. A
41. B, C
42. Lab
43. A, C
44. C, D
45. D
46. B, D
47. B
48. C
49. D
50. C
51. A, C
52. C, E
53. C, D
54. Lab
55. D
56. B, C
57. A, D
58. A, B
59. A, D
60. B
61. C
62. D
63. A
64. A, D
65. B, C, F
66. D
67. B, C
68. B
69. A
70. B
71. C, D
72. B, D
73. A, C, D
74. B
75. D
76. D
77. - D?
78. B
79. B
80. A, D
81. A, D
82. A, B
83. C
84. E, F
85. B, C, F, H
86. C
87. Lab
88. B, D, E
89. C, E
90. D
91. B, E, F
92. A, B
93. B
94. B
95. A
96. B
97. C, F
98. D
99. A, B
100. B, D

74/94 = 78%

Notes:

Layer 2 switching:

* Broadcast and multicast frames are flooded
* Done from CAM table (if no address present)
* ARP table used to map L2 addresses to L3

Topologies:

* Collision domain = connection between hub/switch and end device
* Broadcast domain = router to hub/switch connection
* SUBNET = Section of network separated by router/l3 switch

Cable types:

* Fiber optic:
  + Support longer distances
  + Immune to EMI
  + Cost more
* Copper UTP:
  + Cheaper
  + More vulnerable to bending
* Straight-through cables:
  + Connects 2 devices of different type
  + Use wires 1 and 2 to transmit
  + Use wires 3 and 6 to receive data
    - Switch access port to router
* Cross-over cables:
  + Connect 2 of the same devices
    - Switch to switch
    - Used as FastEth between 100mbps auto MDIX
* Rollover cables:
  + PC COM port to switch
  + Used for initial configs
  + Light blue, DB-9 and RJ-45

Interface Errors:

* Giant:
  + message larger than MTU (default 1500)
* CRC:
  + failed input errors and CRC check
* DUPLEX mismatch:
  + Half duplex side = collision, late collision
  + Full duplex side = CRC, runts

RFC 1918 ranges:

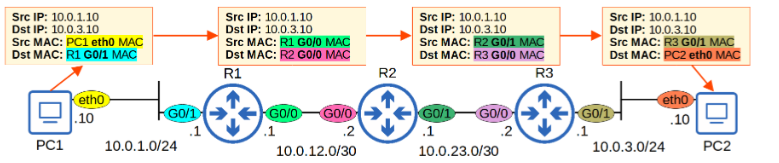
* Class A - 10.0.0.0 to 10.255.255.255
* Class B - 172.16.0.0 to 172.31.255.255
* Class C - 192.168.0.0 to 192.168.255.255

Routing table:

* Any route to a DIFFERENT destination will be added to a routing table (different subnet mask, different network address)
* AD is used to compare routes to the same destination to go in routing table
* Metric is used to compare routes to the same destination with same AD to go in routing tabl
* HOST routes always have /32 subnet mask - 255.255.255.255
* If you cannot see a clear interface that should forward a packet, GO WITH DEFAULT ROUTE! If none of your calculations are making sense…
* When more than 1 route learned via DYNAMIC ROUTING PROTOCOLS go to SAME destination, pick one with lowest AD, then lowest METRIC
* When you have several networks in a routing table all to specific hosts, and are trying to find where a packet is forwarded to… use the most specific available.. E.g. 203.0.113.113 will go to 203.0.113.96/27 because /27 includes .96 and .113
* WATCH OUT FOR FLOATING STATIC ROUTES TO SAME ADDRESS - they will only be used as backups and dont count

Router Next Hops:

* From R2 to R3 = R2’s G0/1 L2 address and R3 g0/0’s L2 address for destination



IP addressing:

* Directly connected = address / exit interface
* Fully specified = address / exit interface / next hop
* recursive/floating = address / next hop / AD
  + NOTE: always have subnet masks, IPv6 will represent this with “/x”
* IPV6:
  + <ip address> </prefix> eui-64 AND “ipv6 address autoconfig use EUI-64
    - Split in half, add FFEE, invert 7th bit
* DEFAULT ROUTE:
  + 0.0.0.0 0.0.0.0

GLBP, HSRP, VRRP:

* IP addresses:
  + GLBP = 224.0.0.102
  + HSRP = 224.0.0.2 or 224.0.0.102 for version 2
  + VRRP = 224.0.0.18

Dynamic NAT/DHCP:

* Command to define which traffic is translated - “access-list”
* Ip helper address <address of server> command = allows host to get address from server
  + REMEMBER: this is configured on Router interface CLOSEST to host
* DHCP SNOOPING
  + Configured on VLAN
* ARP INSPECTION:
  + Consults ARP ACLs
  + Consults DHCP snooping table

Port Security violation modes:

* Restrict - drops frame, message generated
* Protect - drops frame, no message
* Shutdown - err disabled state

Traditional and controller-based networks:

* Controller based network:
  + separates data and control plane
  + Control plane functions are centralised on controller, like calculating routes
* Traditional network:
  + Distributed control plane
  + Each device has own control plane using routing protocols like OSPF
  + Then calculates routes
* ACCESS layer:
  + QoS marking
  + Security services like port security
  + PoE
* DISTRIBUTION layer:
  + Aggregates
  + L2 and L3 border
  + WAN and internet connections
* CORE layer:
  + Connect multiple dist. Layers
  + Focus on speed
  + L3 connections
  + Redundancy

Network Topologies:

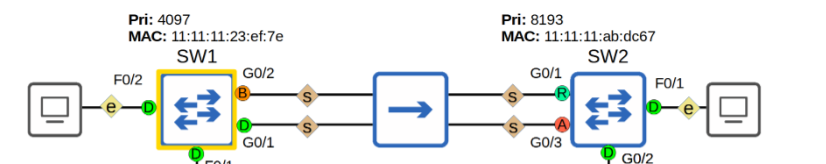
* Spine and Leaf:
  + Every leaf to every spine
  + Every spine to every leaf
  + Leaf connects to APIC, servers, etc
  + Predictable AND equal pathing
* CAPWAP tunnels:
  + Traffic goes to both SW and WLC as it moves

##### 

* + Path = PC1>AP1>SW1>WLC1>SW1>WLC1>SW1>AP2>PC2

STP:

* Root bridge is lowest priority then lowest ID
* All ports on root bridge are designated
* On the other side of a designated port will be a root port
* ROOT ports are port with shortest path/lowest cost to root bridge
* If two links have same cost, lowest value of neighbour port wins



##### TO WORK OUT A TOPOLOGY, FOCUS ON WHICH PORTS ARE ROOTS ON EACH SWITCH FIRST

##### 

CDP:

* Holdtime counts down and sends messages every 60 seconds
  + Timer will start at 180, at 120 message sent, etc

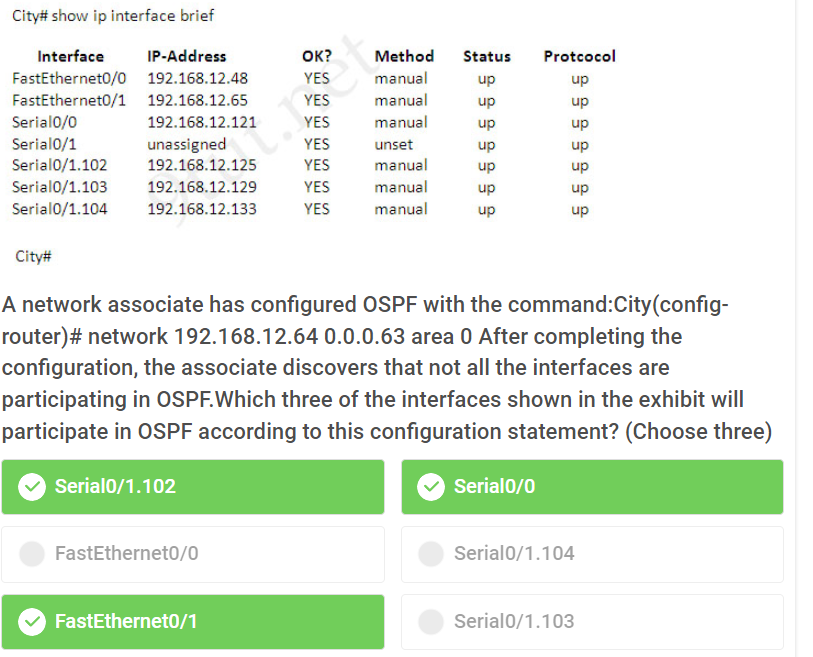
QoS:

* Platinum = voice
* Gold = video
* Silver = best effort
* Bronze = guests

QUEUING:

* FIFO = first in first out
* CBWFQ = class-based weighted fair queuing
* Round robin = cyclical order
* LLQ = low-latency queuing

OSPF:

* When asked which command will activate OSPF on a range of interfaces
  + Choose the one with an odd/interested wildcard mask (like 0.0.7.255 instead of 0.0.255.255)
* ROUTER ID takes precedence when manually configured
  + ONCE the process has been RESTARTED!!!
* NETWORK TYPES:
  + P2P = full neighbour type, no DR/BDR elected, neighbours DYNAMICALLY discovered
  + PPP, HDLC interfaces
  + BROADCAST = 2way for neighbours, full for BDR/DR - these are elected
  + OSPF, Ethernet interfaces
* NEIGHBOUR requirements:
  + AREA = match
  + SUBNET = match
  + ROUTER ID = no match
  + TIMERS = match
  + OSPF PROCESS ID = no match
    - DR OTHERS can have 2 neighbours
* OTHER NOTES:
  + OSPF provides view of entire topology
  + Calculates shortest path
  + Updates come about by event-trigger
  + To maintain a routing table, a router will take LSAs from routers and Hello Packets
  + Default EQUAL COST PATHS = 4
  + Supports VLSM
  + Confines network instability to one area of a network
  + Allows control of routing updates
* SINGLE AREA OSPF:
  + Removes need for virtual links
  + Reduces type of LSAs generated, only type 1 needed
* COMMANDS:
  + Show ip ospf database = show OSPF link states, topology info
* 
* In a question like this, the wildcard mask represents the subnet (-1), so 64… these three interfaces are in a 64 subnet from 64 - 127

802.11 IEEE standards:

* 2.4ghz = 802.11, 802.11b, 802.11g, 802.11n
* 5ghz = 802.11a, 802.11n, 802.11ac
* Message TYPES:
  + MANAGEMENT = beacon/probes/association/authentication
  + CONTROL = RTS, CTS, ACK
  + DATA = packets

Trunks:

* Trunk + Trunk = trunk
* Trunk + dynamic desirable = trunk
* Trunk + dynamic auto = trunk
* Trunk + access = invalid
* Access + trunk = invalid
* Access + dynamic desirable = access
* Access + access = access
* Access + dynamic auto = access
  + For WLAN LAG group will be on + on
* Trunk group number does not need to match on BOTH switches
  + DOES need to match for each interface one one side

VLANs:

* Voice VLANs send all tagged traffic, do not need trunk
* Each interface can have a diff. Native VLAN
* Native VLAN should match on both sides of connection
* VLAN configuration happens in (config-if)
* Improve security by differentiating sensitive data from other traffic
* BROADCAST STORMS = mitigated by adding broadcast domains, smaller size, bigger #
* Creates more logical networks that use same infra
* Greatly simplify adding/moving/changing hosts on a network

WAN:

* DSL = SOHO
* Cable internet = SOHO
* Leased Line = medium/large network
* MPLS = medium/large network

Wireless:

* Security:
  + WEP < WPA/WPA2 <WPA3
* WPA3:
  + GCMP for encryption
  + SAE for authentication
* WPA/WPA2:
  + CCMP for encryption
  + PSK for authentication
    - PSK can be hexadecimal OR ASCII
* WLC interfaces:
  + Dynamic interface = WLANs to VLANs
  + Redundancy management interface = connect to WLC pair (standby)
  + Management interface = in band management (ssh/https), CAPWAP between APs
  + Service port interface = Out of band management
* APs:
  + DATA traffic = not sent to controller
* CPU ACCESS CONTROL LIST:
  + Filters traffic for WLC

NTP:

* Commands:
  + Ntp master <stratum #> = configures router as NTP server

Internet Protocols:

* FTP data 20 TCP
* FTP control 21 TCP
* SSH 22 TCP
* Telnet 23 TCP
* SMTP 25 TCP
* HTTP 80 TCP
* POP3 110 TCP
* HTTPS 443 TCP
* DHCP server 67 UDP
* DHCP client 68 UDP
* TFTP 69 UDP
* SNMP agent 161 UDP
* SNMP manager 162 UDP
* Syslog 514 UDP
* DNS 53 TCP & UDP
* IPsec = site to site VPNs
* GRE = creates tunnels
* TLS = remote access VPNs

Passwords:

* Enable password,enable secret = to access privileged exec mode with en
  + Enable secret overrides enable password
* Config-line password = CLI access

Automation:

* Ansible:
  + Uses SSH
  + Agentless
  + YAML
  + Port 22
  + push
* Terraform:
  + Uses DSL
  + Written in GO
  + Agentless
* Puppet/Chef:
  + Pull model
  + Ruby
* REST API CALLS:
  + 1xx = informational
  + 2xx = success
  + 3xx - redirection
  + 4xx = client error
  + 5xx = server error
* BENEFITS:
  + Reduced OpEx
  + Faster network deployments and changes

Containers and VMs:

* Containers:
  + Boot up faster
  + Use less resources
* VMs:
  + Use VMM
  + Can have multiple on one PC

ACLs:

* Typical ACL view:



* Standard ACLs:
  + On interface closest to destination from router
  + Access-list
* Extended ACLs:
  + On interface closest to source
  + Access-list
  + Use ports and protocols
  + Filter based on destination port
  + Apply OUTBOUND and to interface with Ip access-group

JeremysITLab Exam 2:

1. C, D
2. B, D
3. C
4. B, C
5. A, C, D, E
6. A, C, F
7. B, D, E
8. B

##### C, D, F

1. B, D
2. B
3. A
4. C
5. A, C
6. D
7. C
8. B, D
9. A, D
10. Lab
11. B, C, E
12. C
13. C
14. B
15. E, F
16. B, D
17. B
18. A, B, F
19. B
20. B, D, E/F
21. D, E, F
22. A, D
23. B, E
24. C
25. D
26. C
27. C
28. A
29. B, D
30. C, F
31. B, C
32. C/D
33. B
34. A, B, C, D
35. C
36. -
37. D
38. C
39. D
40. A
41. A
42. B
43. B
44. B
45. A
46. B
47. A, D
48. D
49. B, C
50. B, C, F
51. A
52. B
53. D
54. A, B
55. A, C
56. D
57. A, B
58. C
59. B
60. C, G
61. C
62. B
63. A, C, D
64. B
65. D
66. A,B
67. D -
68. Lab
69. B
70. B, C
71. C
72. C
73. B
74. A
75. -
76. C, E
77. \*
78. A, C
79. B
80. C
81. B, E
82. C -
83. B, D, F
84. -
85. D
86. A
87. C
88. B, C
89. A. B
90. -
91. B, C, D

Interfaces:

* SPEED mismatch = interface DOWN
* Duplex mismatch = COLLISIONS

Cables:

* Categories:
  + Cat6 - 10000baseT, 10gbps (10,000mbps), 100m
  + Cat5e = 1000BASET, 1gbps (1000mbps), 100m
  + Cat5 = 100baseT, 100mbps, 100m
  + Cat3 = 10baseT, 10mbps, 100m
* All cables are 100m
* baseT name matches speed in mbps

Wireless:

* Configuring interfaces:
  + Done in CONTROLLER tab as interfaces are on the controller

IPv6:

* Anycast/unicast:
  + 2001 (UNICAST WILL JUST GO TO ONE DESTINATION)
* Link Local addresses
  + Created by default with Ipv6 enable command ALONG with originally planned IP you create
  + If they are used as a next hop, must specify interface otherwise NOT VALID

CDP:

* PORT connected to another router:
  + First listed, NOT outgoing port (that is where current router sends from)
* AP modes:
  + Local = default, BSSs (multiple)
  + FlexConnect = BSSs (multiple), tunnels incase WLC goes down
  + Sniffer = captures 802.11 traffic for analysis, no BSSs
  + Monitor = no BSSs, detects rogues
  + Bridge/mesh = bridges between sites

Automation and SDN:

* Terraform:
  + written GO
* REST APIs:
  + Uniform, client-server, stateless, cacheable (or not), layered, Code on demand (THESE ARE ALL CONSTRAINTS)
* SDN Architecture LAYERS:
  + APPLICATION layer = scripts/apps
  + CONTROL layer = SDN controller, processes instructions from apps
  + INFRASTRUCTURE layer = network devices, fabric/overlay/underlay, etc
* PLANES:
  + CONTROL plane:
    - Provides info to data plane
    - Protocols L3 and L2
  + DATA plane:
    - Storing info in tables
    - Forwards traffic
    - ACLs, QoS, encapsulation
  + MANAGEMENT plane:
    - Authenticates, authorises, accounts

Traditional Network Architecture:

* ACCESS LAYER:
  + en d hosts
  + QoS marking
  + DAI, port security
  + PoE
* DISTRIBUTION LAYER
  + Aggregates
  + L2 and L3 border
  + WAN and internet connection
* CORE layer
  + Large networks
  + Focus on speed
  + L3 connections ONLY
  + OSPF, etc.
  + Redundancy

Ports:

* FTP:
  + DATA = 20
  + CONTROL = 21
  + User authentication

First-Hop Redundancy Protocols:

* GLBP, HSRP, VRRP
* Virtual MACs:
  + GLBP = 0007.b400…
  + HSRP = 0000.0c07, 0000.0c9f…
  + VRRP = 0000.5e00…

Port Security:

* DHCP snooping:
  + applied globally and per VLAN
* DAI:
  + Enabled per VLAN only

NAT:

* IP NAT translations:
  + Inside local = host on inside network (host A, source)
  + Inside global = router’s interface to host on inside network
  + Outside global = router’s interface to outside network
  + Outside local = host on outside network (host B, destination)