Final Review Sheet: Solutions

1. Define the attributes of a partial mesh and a full mesh Frame Relay Network
    a. The difference between the two is that in a full meshed network every device is connected to every other device with a permanent virtual circuit while in a partially meshed network not all devices are connected with each other.
    b. Each PVC is differentiated with an address called a data-link connection identifier (DLCI).
2. Explain the purpose of inverse ARP, as well as how it uses Frame Relay broadcasts
    a. Inverse ARP dynamically creates a mapping between the Layer 3 address (IP address) and the Layer 2 address (DLCI).
    b. After a VC is up, a router announces its network layer address by sending an inverse ARP message over the VC. E.g. “I am ____ (IP address)
    c. Inverse ARP starts by learning the DLCI data link layer address via LMI messages (local management interface).
3. What is the name of the field that identifies, or addresses a Frame Relay virtual circuit?
    a. DLCI (data-link connection identifier)
4. Two advantages of Frame Relay versus leased line type of connectivity for an enterprise environment.
    a. A leased line is a dedicated, always-on circuit between two endpoints.
    b. Frame Relay is more cost effective because you can have multiple VCs running over a single access link which requires fewer overall physical links.

5. If routers have different LMIs what can they configure to work correctly?
    a. They need to have the same encapsulation configured.

6. Which of the following commands are required on the router connected to a DTE cable to make the serial link between two routers work when the 2 routers are connected using a DTE and DCE cable and no CSU DSU
    a. The clockrate 56000 is needed on the router with the DCE cable.
7. Define NAT and NAT overload.
    a. NAT allows a host without a valid registered IP address to communicate with hosts on the internet.
    b. It translates private IP addresses to addresses that can be routed on the internet.
    c. Overloading NAT means you can have multiple hosts used the same outside local address by assigning hosts port numbers from the NAT router.
8. Define the term outside local address
    a. It is the IP address that the hosts on the local network use to send and receive packets on the internet.
9. What ICMP message codes does the trace command rely on?
    a. Time to Live exceeded
10. **What are valid subnets according to CIDR?**

a. CIDR's original intent was to allow the summarization of multiple Class A, B, and C networks.

11. What is the smallest summarized route that summarizes the subnets 155.33.133.0, 155.33.134.0, 155.33.140.0, and 155.33.141.0, all with mask 255.255.255.0?
    a. 155.33.1000 0101.0 (155.33.133.0)
    b. 155.33.1000 0110.0 (155.33.134.0)
    c. 155.33.1000 1100.0 (155.33.140.0)
    d. 155.33.1000 1101.0 (155.33.141.0)
    e. Common subnet number = 155.33.1000| 0000 = 155.33.128.0
    f. Mask = 255.255.1111| 0000.0 = 255.255.240.0
12. Classful routing protocols
    a. Classful routing protocols do not transmit the mask information.
    b. RIP-1, IGRP
13. Routing Protocols that support VLSM
    a. Routing protocols that support VLSM are also classless because the send mask information along with routing information.
    b. RIP-2, EIGRP, OSPF
14. Routing protocols that do not advertise mask information along with subnet numbers?
    a. These would be classful routing protocols.
    b. RIP-1, IGRP

15. Difference between classless and classful routing?
    a. Classful routing protocols do not transmit the mask information along with subnet number, whereas classless routing protocols do transmit the mask information.
16. What allows for the successful use of a discontiguous network?
    a. A discontiguous network is the concept where routes to one subnet must pass through subnets of a different network type.
    b. Classless routing protocols support discontiguous networks
17. What is the smallest summarized route that summarizes the subnets 110.5.105.16, 110.5.105.32, and 110.5.105.48, all with mask 255.255.255.252?
    a. 110.5.105.0001 0000 (110.5.105.16)
    b. 110.5.105.0010 0000 (110.5.105.32)
    c. 110.5.105.0011 0000 (110.5.105.32)
    d. Subnet number = 110.5.105.00|00 0000 = 110.5.105.0
    e. Mask = 255.255.255.11|00 0000 = 255.255.255.192
18. Explain Administrative Distance.
    a. Administrative Distance is useful when multiple routing protocols are used to connect different networks and those routing protocols learn the same routes.
    b. Because different routing protocols using different metrics, the IOS cannot compare the metrics so administrative distance is used to tell the IOS

which routing protocol is “more believable.” The lower the number means that the routers will add that routing protocol’s routes only.

19. What is the difference between VLSM and CIDR?
    a. CIDR allows routers to group routes to reduce the quantity of routing information carried by the core routers.
    b. VLSM allows networks to be broken up into variable sizes based on the needs of the subnet.
20. Which of the following subnets is not a valid summary that includes subnet 110.1.55.0 110.1.56.0 and 110.1.57.0, mask 255.255.255.0?
    a. 110.1.0011 0111.0 (110.1.55.0)
    b. 110.1.0011 1000.0 (110.1.56.0)
    c. 110.1.0011 1001.0 (110.1.57.0)
    d. Subnet number = 110.1.0011| 0000.0 = 110.1.48.0
    e. Mask = 255.255.1111| 0000.0 = 255.255.240.0
21. Distance vector loop-avoidance features of OSPF.
    a. Split horizon - advertises routes out an interface only it they were not learned from updates entering that interface.
    b. Split horizon with poison reverse - when a route fails the route is advertised on all interfaces but with an infinite-distance metric.
    c. Route poisoning - when a route fails to a subnet, the subnet is advertised with an infinite-distance metric.

d. Hold-down timer - after finding out a route has failed a router waits a period of time before believed other routing information about that subnet.
e. Triggered updates - when a route fails, an update is sent immediately rather than waiting on the update timer to expire.

22. Two OSPF features that decrease size of OSPF topology database.
    a. OSPF areas break up the network so that routers in one area know less topology information about the subnets in another area.
    b. Stub areas also allow the reduction of the topology database.

23. Compare and contrast the type of information exchanged in routing updates sent by distance vector routing protocols versus link-state protocols.
    a. Distance vector protocols advertise subnets and their associated metric values. Link-state protocols advertise information about routers and subnets in the network, along with metric information for the links. Link-state describe the full topology in the network.

24. Explain redistribution and list 2 critical factors when implementing it.
    a. Redistribution is a way to make a router exchange routes between two different routing protocols inside the router.
    b. You must consider the metrics you want to assign because the original metrics from each of the routing protocols are lost.

c. You must also consider whether the routing protocols being used are classless or classful. VLSM might not be understood in a classful routing protocol.

25. If the command router ospf 1, followed by network 192.224.0.0 0.7.255.255 area 0, with no other network commands, is configured in a router that has an Ethernet0 interface with IP address 192.232.1.1, does OSPF send updates out Ethernet0? (assume a neighbor has being discovered on such interface) Explain why or why not.
    a. No necessarily. OSPF must discover other OSPF neighbors on the interface before it advertises routing information (LSAs).
26. Which of the following routing updates will actually make it to the final routing table? Briefly explain why. (3 points)
    a. Routers put routing updates into their routing table if they have the better metric.

R 10.0.0.0/27 via Serial 0
C 20.0.0.0/24 directly connected
O 10.0.0.0/27 via Serial 2
S 30.0.0.0/24 via Serial 1
30.0.0.0/24 via Serial 2 (IGRP)
D 20.0.0.0/24 via Serial 4
O E2 10.0.0.0/24 via Eth 0
D 10.0.0.0/24 via Serial 3
D 20.0.0.0/27 via Serial 3
S 20.0.0.0/24 via Eth 1

- ~~R 10.0.0.0/27 via Serial 0~~
    - D (EIGRP) has lower admin distance
- **C 20.0.0.0/24 directly connected**
- ~~O 10.0.0.0/27 via Serial 2~~
    - D (EIGRP) has lower admin distance
- **S 30.0.0.0/24 via Serial 1**
    - ~~30.0.0.0/24 via Serial 2 (IGRP)~~

        - Static has a lower admin distance
    - ~~D 20.0.0.0/24 via Serial 4~~
        - C 20.0.0.0/24 has lower admin distance
    - ~~O E2 10.0.0.0/24 via Eth 0~~
        - D (EIGRP) has lower admin distance
    - **D 10.0.0.0/24 via Serial 3**
    - ~~D 20.0.0.0/27 via Serial 3~~
        - C 20.0.0.0/24 has lower admin distance
    - ~~S 20.0.0.0/24 via Eth 1~~
        - C 20.0.0.0/24 has lower admin distance

27. Can we obtain successful network connectivity if our routers are using RIPv1 and our subnets came from a single Class B network and all of them have a mask /29? Why or why not?
    a. Yes, because all the routes are within a single Class B network so even though VLSM is using RIPv1 will still be able to route packets.
28. Given the IP address 167.88.99.66 and the mask 255.255.192.0, what is the broadcast address?
    a. 256-192 = 64 => magic number
    b. Subnet number = 167.88.64.0
    c. Mask = 64 = 2^6 = 24-6 = 18 => /18
    d. Broadcast address = 167.88.127.255
29. Given the IP address 190.1.42.3 and the mask 255.224.0.0, what are the assignable IP addresses in this subnet?
    a. 256-224 = 32 => magic number
    b. Subnet number = 190.0.0.0
    c. Mask = 32 = 2^5 = 16-5 = 11 => /11
    d. Assignable addresses = 190.0.0.1 - 190.31.255.254

30. What is the valid IP range if you change the mask to the previous to a /21?
    a. 24-21 = 3 => 2^3 = 8 => 256 - 8 = 248
    b. 190.1.42.3 /21 => 255.255.248.0
    c. Magic Number = 256 - 248 = 8
    d. Subnet number = 190.1.40.0
    e. Assignable address = 190.1.40.1 - 190.1.47.254
31. You design a network for a customer who wants the same subnet mask on every subnet. The customer will use a network 10.0.0.0 and needs 1228 subnets, each with 18 hosts maximum. What subnet mask would you use to allow the most growth in subnets? Which mask would work and would allow for the most growth in the number of hosts per subnet?
    a. 18 hosts = 2^5 => 32 is magic number
    b. one /24 subnet has 8 32 host subnets, one /16 has 256 /25 subnets, one /16 has 256*8 /32 subnets = 2048 /32 subnets
    c. you need 129 /24 subnets to get at least 1228 subnets each with at least 32 hosts.
    d. 10.0.0.0 /16 will work.
32. What are the valid subnets that can be obtained from the IP range assuming default class mask for each of them? 180.137.189.0 /13?
    a. Class B network 128-191, network is 16 bits long, default mask in /16, third octet is for subnetting
    b. 16-13 = 3 => 2^3 = 8, 256-8 = 248

c. 180.137.180.0 255.248.0.0

d. Network number = 180.136.0.0

e. 180.136.0.0 /16, 180.137.0.0 /16, 180.138.0.0 /16 …

f. 180.136.0.0 - 180.143.0.0

33. List all the subnets that would allow 50 users each, which can be created, from the following IP range: 150.150.164.0 /22

    a. 50 = 2^6 = 64 => 192 => 32-6 = /26

    b. /22 = 24-22 = 2 => magic number = 2^2 = 4

    c. 150.150.164.64 /26, 150.150.164.128 /16, 150.150.164.192 /16 … 150.150.167.192 /16

34. Explain how a switch in VTP transparent mode treats VTP messages received from a VTP server.

    a. A switch in transparent mode forwards VTP advertisements received from other switches while ignoring the information in the VTP message.

35. Explain the steps to configure SSH access to a switch.

36. What is the function of the “neighbor” command in OSPF?

    a. The “neighbor” command allows you to configure static neighbors in an ospf process on non-broadcast networks. You give the address of the neighbors.

37. Must all members of the same VLAN be in the same collision domain, the same broadcast domain, or both?

a. A collision domain is a set of NICs for which a frame sent by one NIC could result in a collision with a frame sent by any other NIC.
b. A broadcast domain is a set of NICs for which a broadcast frame sent by one NIC is received by all other NICs in the same broadcast domain.
c. A VLAN is essentially a broadcast domain.
d. All members of a VLAN are part of the same broadcast domain. They might be in the same collision domain, but only if all devices in the VLAN

38. Explain the use of DR and BDR on OSPF, also how a DR is selected.
    a. A designated router is the router that broadcasts OSPF routing information to all other routers.
    b. A BDR is the the router that take over the DR's job if it fails.
    c. A DR is elected when OSPF is established on more than one router. It is selected if it has the highest the OSPF priority and/or the highest router id.
39. Explain the advantages and disadvantages of STP.
    a. An advantage of STP is that it avoids packet loops within a network. It allows for redundant paths.
    b. A disadvantage of STP is that it is slow to reconverge.
40. Explain the four port states of STP
    a. Blocking - no frames are forwarded or received
    b. Listening - port received BPDUs and waits to make sure there aren't any better hellos.

c. Learning - bridge learns new location of MAC addresses without forwarding.
d. Forwarding - frames are forwarded, still learns MAc addresses

41. List and explain different switching methods supported by a switch.
    a. circuit switching - provides dedicated bandwidth between two points, but only for a certain duration.
    b. packet switching - provides virtual circuits between pairs of sites, with contracted traffic rates for each VC.
42. How is root bridge selected for STP?
    a. Priority -> lowest MAC address
43. How does a switch decide to forward a frame and out what interface?
    a. A switch learns MAC addresses and based on previously learned MAC address in an address table decides if and where to forward a frame.
44. Write the Ipv6 address that a computer would create assuming it has a mac address of 01:19:DB:28:CE:38?
    a. Insert fffe into the middle => 01:19:DBFF:FE28:CE:38
    b. Prepend fe80 => fe80::0119:DBFF:FE28:CE38
    c. Invert the 2nd least significant bit of hex 01 => 0000 0001 = 0000 0011
    d. Link-local ipv6 address = fe80::0319:DBFF:FE28:CE38
45. What does MPLS stand for and give three uses.
    a. MPLS stands for multiprotocol label switching.

b. Data is directed on short path labels instead of network addresses with avoids address routing lookups.
c. MPLS can be using to build VPNs.
d. MPLS tunnels can be used to transport both IPv4 and IPv6 packets. (AToM)

46. Similarities between FR and MPLS

a. They both route packets using techniques other than IP addresses.

47. Does MPLS forward data based on a routing table?

a. Yes, in a way. Each MPLS router maintains an LFIB (label forwarding information base) where labels are looked up are forwarding is determined.

48. Does each router in the MPLS cloud check destination IP?

a. No. Only the ingress LSR (label switched router) and the egress LSR use the destination IP to determine how and where to forward a packet.

49. Two drawbacks of overlay networks

a. An overlay network is a virtual network built on top of another network.
b. There is overhead when it comes to encapsulation and processing.
c. Load balancing is obfuscated by encapsulation.
d. Packets from an overlay network may run into problems with firewalls.

50. 3 Uses of IPsec

a. You can authenticate packets coming from hosts.
b. You can encrypt data being sent to hosts.

c. You can ensure data integrity.

51. How does IPsec work? What is the difference between transport mode and tunnel mode?
    a. IPsec is protocol that secures communications. It uses cryptographic security services over IP networks.
    b. Transport mode - only the payload of the IP packet is encrypted and/or authenticated.
    c. Tunnel mode - the entire IP packet is encrypted and/or authenticated. It is then encapsulated and sent over a tunnel.
52. What is the value of concepts such as authentication and data integrity while establishing IPSec Tunnels?
    a. Authentication allows a host to verify if the packet sent to came from the host it expected it to come from.
    b. Data integrity means that the packet sent from a host was not modified or tampered with.
    c. The point of IPSec tunnels is to make sure authentication happens and data integrity is successful.
53. On which layer does MPLS work?
    a. MPLS operates between layer 2 and layer 3. This is sometimes referred to as layer 2.5.
54. Are LSPs full duplex or half duplex?

a. LSPs are half duplex. Duplex traffic requires two LSPs, one LSP to carry traffic in each direction.

55. Explain the MPLS operation in the diagram.

a. **Ingress/Egress:** R6 and R1 act as both egress and ingress routers. The egress routers add MPLS labels to packets with the ingress routers remove them. They are know as edge LSRs.

b. **LSRs:** All of the routers seen in the diagram are label switching routers because they all are part of MPLS tunnels that route traffic with MPLS labels.

c. **Transit Routers:** R2, R5, R3, R4 are transit routers because the forward packets based on labels only. Transit routers are also known as regular, old label switching routers.

d. **LSP:** It looks like there is a label switched path from R1->R2->R5->R6 and R1->R3->R4->R6.

e. **FEC:** When an unlabeled packet enters an ingress router, the router determines the forward equivalence class of the packet and then labels it appropriately. FEC describes a set of packets with similar characteristics which may be bound to the same MPLS label.

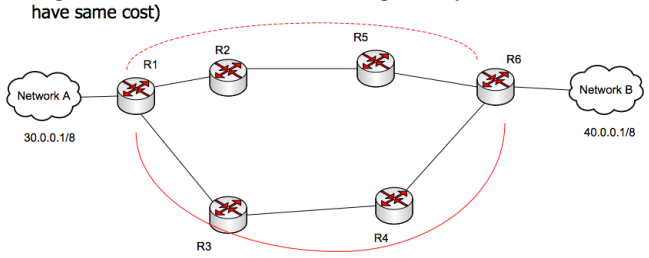
f. Penultimate routing: Routers 2, 5, 3, 4 perform this function. They remove the outermost label of an MPLS tagged packet before the packet is passed to an adjacent LER (Label Edge Router) Routers 1,6.

g. **Label Distribution Protocol**: This goes on between all routers. It is a way to exchange label and reachability information.

h. **Resource Reservation Protocol:** MPLS uses RSVP to manage LSPs. Network constraints such as available bandwidth and explicit hops are taken into consideration when routing labeled packets on LSPs.

i. **IGP (Interior Gateway Protocol):** IGP is a protocol used to exchange routing information between gateways within an autonomous system. For example: distance-vector, link-state routing. MPLS works in conjunction with IP and its routing protocols such as IGP. It is build on top of IP networks.

55) **(10 points max)** Explain MPLS operation with respect to the following diagram and the involvement of the following terms: (Assume all the links have same cost)



a) IGP Routing selection and purpose
b) Label Switched Path
c) Label Switching Routers
d) Ingress Router
e) Transit Router
f) Penultimate Router
g) Egress Router
h) Label Distribution Protocol
i) Forward Equivalence Class
j) Resource Reservation Protocol

60. Show how data is encapsulated (use diagram), consider that you are encrypting a credit card number, which is fed into a website (port 80). Show all headers/trailers involved from layer 7 to layer 2 (assume Ethernet at layer 2, and tunnel mode encryption)

61. Show how to create a NAT pool, and how to use it in a router with 3 ports, one on the private subnet 20.20.20.0/24 one on the private subnet of 30.30.30.192/26 and another on the public network 120.120.120.0/24, assume you have 10 public IP addresses to use. NAT pool should only be used by SIP (port 5060)
    a. On interfaces facing the private subnets
        i. ip nat inside
    b. On interface facing public
        i. ip nat outside
    c. Create access list
        i. ip access-list 101 natpool_acl permit 20.20.20.20 /24
        ii. ip access-list 101 natpool_acl permit 30.30.30.192 /26
    d. Create nat pool
        i. ip nat pool natpool1 120.120.120.1 120.120.120.10 prefix-length 24
    e. Assign access list to nat pool
        i. ip nat inside source list natpool_acl pool natpool1 5060
62. Explain how an IPSec session is established between 3 peers. Explain the function/involvement of each of the following components:

    a) **ESP** - (encapsulating security payload) - provides authenticity, integrity, and confidentiality protection of packets. It has tunnel mode and transport mode.

    b) **AH** - (authentication header) - used to guarantee integrity and authentication of IP packets.

    c) **ISAKMP** - (internet security association and key management protocol) - protocol for establishing cryptographic keys and authenticating peers.

    d) **Diffie-Hellman** - is a public-key cryptography protocol. It allows two parties to establish a shared secret key.

e) **Transform Set** - combines an encryption method and an authentication method for data. Use during the association negotiation with ISAKMP.

f) **IKE Phase 1** - (Internet Key Exchange) - established a secure authenticated communication channel using DH. Creates a bi-directional ISAKMP Seurity Association (SA).

g) **IKE Phase 2** - IKE peers negotiate SAs on behalf of other services like IPsec.

h) **ACLs** -

i) **Message Authentication codes -** short piece of information used to authenticate a message.

j) **Encryption algorithm -** AES, DES, HMAC-SHA

k) **Pre-shared Keys -** keys manually put on a device for authentication.

l) **Tunnel Timeout -**

m) **Crypto map** -