Politecnico di Torino

Local Area Networks: Closed Answer Questions

Fulvio Risso

March 20, 2018

License

Acknowledgments

The author would like to thank all the persons that contributed to those exercises.

Contents

1 LAN Basics

1. In the past, Wide Area Networks (WAN):
   a) Were intended as geographic networks designed mainly for low bitrate applications
   b) Were intended as shared networks designed mainly to exchange large amount of data
   c) Were intended as geographic networks designed mainly to exchange large amount of data
   d) Were intended as campus networks designed mainly to connect several buildings to each other
2. In the past, Local Area Networks (LAN):
   a) Were intended as local networks designed mainly for low bitrate applications
   b) Were intended as shared networks designed mainly to exchange large amount of data
   c) Were intended as shared networks designed mainly for "bursty" application
   d) Were intended as campus networks designed mainly to connect several buildings to each other
3. In networks based on a shared communication medium:
   a) While a station is transmitting, other stations cannot transmit
   b) While a station is transmitting, other stations can transmit only if the previous communication is not directed to them
   c) While a station is transmitting, other stations can receive and transmit at the same time
   d) All stations can transmit at any time without any risk of collision thanks to the presence of the switch
4. In a LAN:
   a) There is always a intermediate device that handles the frames
   b) All devices have the same priority in getting access to the shared communication medium
   c) All devices have the same priority in getting access to the shared communication medium, except a possible intermediate device that is privileged against other stations
   d) If needed, we can configure a possible device (e.g. server) that has higher priority in getting access to the shared communication medium
5. A shared communication medium technology is characterized by:
   a) Broadcast communication, no intermediate sistems and high flexibility
   b) Low cost, thanks to the deployment of level 2 communication devices (L2 Switch)
   c) Reliability, privacy reasonably guaranteed for users, but impossibility to have multiple communications at the same time between hosts

d) Reliability, possibility to have multiple communications at the same time between hosts, but degree of privacy

6. The OSI level named “Data Link”:

   a) Assumes that physical-layer functions are defined, which are the ones used to allow several networks technologies (e.g. Ethernet, WiFI) to communicate together

   b) Can implements multicast/broadcast addresses that can be exploited for Solicitation and Advertisement functions

   c) Defines how to generate bits over the channel

   d) Can be divided into a LCC (Link Central Control) sublevel and a MAC (Medium Access Control) sublevel

7. The OSI level named “Physical”:

   a) It is specified only for Ethernet networks

   b) It is the same in all cabled networks (e.g. Ethernet, Token Ring, FDDI), and basically is derived from the specifications of the original Ethernet

   c) It can be shared among several network technologies, witch however differ on Data-Link level (e.g., Ethernet and FDDI)

   d) It defines the way to get access to the shared communication medium

8. The LLC (Logical Link Control) sublevel:

   a) It has almost disappeared from modern networks

   b) It was never able to succeed on WiFi networks, which use another framing format instead

   c) It is present in a few protocols operating on Ethernet networks

   d) It defines 64 bit addresses to identify the level 3 protocol contained in the frame

9. The MAC (Medium Access Control) sublevel:

   a) It defines the arbitration mechanism in order to get access to the shared communication medium

   b) It defines a field named “Protocol Type” that identifies the level 3 protocol contained in the frame

   c) It is present in all LAN technologies, except in Ethernet where is usually replaced by LLC-SNAP

   d) It defines how bits must transmitted over the physical channel

10. MAC addresses:

    a) Are allocated by government authorities

    b) Are set by the user (or operating system) when the devices is used for the first time

    c) Are set by the manufacturer: the first 3 bytes identify the vendor and remaining are defined by an algorithm that generates random 24 bits numbers

d) Are set by the manufacturer in each network interface card

11. If the operating system of a station receives all the packets that are in fact received by the network interface card:

    a) The station does not have an IP address

    b) The station is connected to a switch

    c) The station has a multicast MAC address

    d) The network card is in “promiscuous” mode

12. The difference between “frame” and “packet” is:

    a) A frame identifies level 2 data, whereas a packet identify level 3 data

    b) A frame identifies level 3 data, whereas a packet identify level 2 data

    c) They are synonymous

    d) A frame identifies Ethernet data, whereas a packet identify other protocols data

2 Traffic analysis

13. If a host is connected for the first time to a shared Ethernet LAN and the user types the PING command toward an other station:

    a) It generates immediately and ICMP Echo Request packet toward the destination, since we are on a shared communication medium

    b) It generates first an ARP packet in order to know the destination MAC address of the destination host, that will reply with its IP address

    c) If the destination host belongs to a different level 3 network, it must generate a packet that discovers the MAC address of its default gateway

    d) It generates an ARP Request, that has the side effect of updating the filtering database of all stations

14. A host “A” is turned on and connected for the first time to a shared Ethernet LAN. Then, the user types the PING command toward the server “S” “www.polito.it”, which is connected to the same LAN. The first frame that will be generated on the network will be:

    a) An ARP Request toward the DNS if “S” belongs to a different level 3 network

    b) A DNS Query toward the DNS if “A” belongs to the same IP network of the DNS and the router

    c) An ARP Request containing the router IP address in the “Target IP Address” field if “S” belongs to a different IP network compared to the host

    d) An ARP Request containing the router IP address in the “Target IP Address” field if the DNS server belongs to a different IP network compared to the host

15. A frame that contains the MAC address of a router as destination address:

a) It will have the IP address of the router as destination IP address

b) It will have the IP address of a station does not belong to local LAN as destination IP address

c) It will have the IP address of a station that belongs to local LAN as destination IP address

d) It will have the IP address of the router or the one of a station that does not belong to the same IP network of the source host as destination IP address

16. Before an ICMP Echo Request packet, the trasmitting station:

    a) It always generates an ARP Request

    b) It always generates a DNS Query

    c) It always generates an ARP Request and a DNS Query

    d) It does not necessarily generate additional packets

3 Cables and Cabling

17. Main characteristics of a physical copper link, with respect to data transmission are:

    a) Propagation speed (expressed as a fraction of the light speed), impedance of the line (expressed in AWG, American Wire Gage), size of the physical copper wire

    b) Impedance of the line (expressed in AWG, American Wire Gage), size of the physical copper wire

    c) Propagation speed (expressed as a fraction of the light speed), impedance of the line, size of the physical copper wire (expressed in AWG, American Wire Gage)

    d) Propagation speed (expressed as a fraction of the light speed), impedance of the line, link length (expressed in AWG, American Wire Gage)

18. The AWG (American Wire Gage):

    a) Measures the signal attenuation

    b) Indicates the maximum noise tolerated by the cable

    c) Measures the size of the physical copper wire

    d) Measures the size of the core of a fiber optic link

19. The Cross-Talk:

    a) Is called "Alien" if it generated by a generic external source of noise

    b) Is due to attenuation of a signal into a copper wire

    c) Is due to interference generated by the other physical links in the cable

    d) It can be present if a plug is installed in the wrong way or if the wire has several curves on its path

20. With respect to fiber optic cables:

a) Multimode fibers with led technology are the most recent and have the highest bandwidth

b) Multimode fibers have low dispersion rate and high bandwidth

c) Indoor cables do not need an external metallic shield

d) Singlemode fibers with laser technology are the most recent and have the highest bandwidth

21. In structured cabling:

a) The structure usually follows a tree, in which several portions are aggregated together at different levels

b) It is a good rule to locate the Floor Distribution and the Building Distributor in the same room, so they can be connected to each other using short 10Gb cables

c) Usually a ring is preferred to a tree topology because of its robustness

d) Copper wires can span up to 100m, plus the additional patch cords at their ends (e.g. user station and network device)

22. Copper wires in a data-center:

a) Are not used due to very high high communication speed requested

b) Are heavily used throughout the entire data-center mainly for budget reasons

c) Are used in some portions of the data-center (where cables are reasonably short), mainly for budget reasons

d) Are usually used to connect disks, which are characterized by lower speed than servers

4 Ethernet

23. When transmitting on an Ethernet network, a station sends a “jamming sequence” if:

a) The current trasmission was succesfull

b) It wants to “reinforce” a collision

c) It wants to take the ownneship of the channel

d) It wants to release the channel

24. After a collision on an Ethernet network:

a) All the stations can immediately compete for the ownership of the physical channel for a new transmission

b) The stations that generate the collision (and only these ones) can compete for the ownership of the physical channel

c) Stations that generated the collision must wait a random time, called “back-off”, before competing again for the ownership of the physical channel

d) Only the station that generated collision (i.e., the station that started transmit later) must wait a random time, called “back-off”, before competing again for the ownership of the physical channel

25. In order to detect collisions on an Ethernet network, we need to consider:

    a) Distance among stations, minimum frame size, signal propagation speed

    b) Distance among stations, link bandwidth, minimum frame size

    c) Distance among stations, link bandwidth, minimum frame size, signal propagation speed

    d) Number of stations on the network, collision detection speed, minimum duration of the transmission

26. To distinguish an Ethernet 2.0 (DIX) frame from an IEEE 802.3 frame:

    a) We can check the “Version” field at the beginning of frame

    b) We can check the value of the 2 bytes corresponding to the “Ethertype” field in Ethernet 2.0 (or “Length” field in IEEE 802.3)

    c) We can calculate the size of the data carried in the frame; in case this value is is lower than 64 bytes, the frame is IEEE 802.3, otherwise it is Ethernet 2.0

    d) We can look at the possible presence of an LLC SNAP envelope, that is only present in the IEE 802.3 frame

27. Frames Ethernet 2.0 (DIX) and IEEE 802.3:

    a) Are not compatible and have different sizes for the minimum frame

    b) Are compatible, even if they have different sizes for the minimum frame

    c) Are compatible, even if they have different sizes for the maximum frame

    d) Are compatible, even if only the second can contain the “Padding” field

28. In Ethernet, the Inter-frame gap is:

    a) The required silence between a frame and the following

    b) Empty data within the frame, which allow reaching the minimum frame size needed to detect a collision

    c) The set of bytes sent on the channel acting as end frame delimiter

    d) The time needed to send the bytes of the preamble (up to 7 bytes maximum)

29. The maximum collision diameter in an Ethernet network:

    a) Can be seen as the maximum length of a link between a host and a hub

    b) Can be seen as the maximum length of a link between a host and a bridge

    c) Does not change even if hubs are replaced by bridges in the network

    d) It is approximately 200m in case of copper cables

5 Ethernet: advanced features

30. What does it happen to a PC with its network interface in Full Duplex Fixed mode if it is connected to a switch with its network interface in auto-negotiation mode?
    a) The interface of the switch goes in half duplex mode and it may detect some fake collisions
    b) The interface of the switch goes automatically into Full Duplex Mode
    c) PC and switch will never be able to communicate
    d) PC and switch will communicate without problems
31. The handshake of the transmission speed among two Ethernet interfaces takes place:
    a) At layer 1
    b) At layer 2
    c) At layers 1 & 2
    d) Partially at layer 1 and partially at layer 2
32. In an Ethernet network based entirely on switches with all links in Full Duplex Mode, how many collisions we may experience?
    a) It depends on the size of the network
    b) It depends on the number of the switches
    c) It depends on the number of connected PCs
    d) We do not have collisions
33. The loss of connectivity between two L2 entities (e.g. host or switch) can be immediately detected at the physical layer if the link is in:
    a) Full duplex
    b) Half duplex
    c) Full duplex, with the other side of the link connected to a switch
    d) Generally it cannot be detected
34. A broken network cable can be immediately detected at the physical layer if the link is in:
    a) Full duplex
    b) Half duplex
    c) Full duplex, with the other side of the link connected to a switch
    d) Generally, a broken network cable will be immediately detected by the entities directly connected to the two edges of the cable itself

6 Switched Ethernet

35. The network is defined as “switched” when:
    a) It contains only switches and end stations
    b) It contains switches, hubs and end stations
    c) It contains at least one router
    d) It is based on a shared physical medium for communication
36. In a switched network:
    a) Loosing frames is a rare event thanks to the high speed of the switch
    b) There are no lost frames thanks to the fact that there are no collisions
    c) The number of lost frames may not be negligible because of congestions on the switches
    d) There are no lost frames thanks to the use of Spanning Tree protocol
37. Switches:
    a) Have only one MAC address for the entire device
    b) Have one MAC address per physical port
    c) Do not have any MAC address (they are transparent indeed)
    d) Have one MAC address per physical port plus one for each configured VLAN

7 VLANs

38. One of the reasons that motivates a network designer to use VLANs is:
    a) Faster frame forwarding
    b) Broadcast traffic reduction
    c) Simplified management of Spanning Tree
    d) Collision reduction
39. Two PCs belonging to two different VLANs:
    a) Can communicate normally by sending Ethernet frames directly to the other party
    b) Can never send Ethernet frames directly to the other party
    c) One of the two PCs must use a network interface with VLAN IEEE 802.1q tags support
    d) Both PC must use a network interface with VLAN IEEE 802.1q tags support
40. Two PCs connected to the same Hub (repeater):
    a) Can not belong to the different VLAN
    b) Will always belong to the same VLAN

c) Can belong to different VLANs if they use a network interface compatible with the IEEE 802.1q standard

d) Can belong to different VLANs if they use a network interface compatible with the IEEE 802.1q standard, but there may be some delivery problem with respect to large packets

41. Two stations configured in “trunk” mode and belonging to the same VLAN are connected to the same switch that does not support the IEEE 802.1q (VLAN) standard:

    a) The stations cannot exchange data unless a router is being used

    b) The stations cannot exchange data even if a router is being used

    c) The stations can always exchange data even if a router is not being used

    d) The stations can always exchange data even if a router is not being used, but there may be some delivery problem with respect to large packets

42. According to the IEEE 802.1q (VLAN) standard, the connection between two switches:

    a) It can be only of type “Trunk”

    b) It must never be of type “Trunk”

    c) It could be of type “Access”

    d) It could be of type “Access” only if the corresponding ports on the two switches are part of the same VLANs

43. According to the IEEE 802.1q, the GVRP protocol (GARP VLAN Registration Protocol) is useful to:

    a) Propagate automatically over the whole network the information about the existing VLANs

    b) Assign to packets belonging to different VLANs different priorities

    c) Configure dynamically the ports of a switch based on the configuration obtained from the network interface of the PC at the other side of the cable

    d) Register the traffic of different VLANs

44. According to the IEEE 802.1q standard, VLANs are configured on the switch:

    a) On each port through an appropriate operation

    b) By the manufacture and it is not possible to modify its configuration

    c) By the manufacture and it is possible to change VLANs just for a restricted number of ports

    d) Only on Trunk ports

45. According to the IEEE 802.1q, the membership of a PC to a specific VLAN can be derived from:

    a) The MAC address of the network interface of the PC, independently from the configuration of the switch

   b) The IP address of the network interface of the PC, independently from the switch configuration

   c) The MAC and IP addresses of the network interface of the PC, independently from the switch configuration

   d) The configuration of the port on the switch connected to the PC

46. A port is of type “Trunk” when:

   a) It transmits only frames that do not include the IEEE 802.1q tag

   b) It transmits only BPDU frames

   c) It transmits only frames that include the IEEE 802.1q tag

   d) It transmits only BPDU frames that includes the IEEE 802.1q tag

47. When Broadcast Storm occurs within a VLAN:

   a) The other VLANs are protected and do not perceives in any way this problem

   b) The broadcast storm occurs also in the other VLANs

   c) The broadcast storm occurs also in the other VLANs, unless a priority mechanism is being used to privilege the traffic of those VLANs

   d) The other VLAN may suffer from delays because of the traffic on the trunk links

8 Spanning Tree

48. The Spanning Tree protocol is used to:

   a) Transform a network containing meshes into a tree, canceling loops

   b) Manage multiple paths in load-balancing, providing redundancy in the network

   c) Optimize the forwarding process

   d) Update the filtering database

49. The Spanning Tree protocol operates sequentially according to the following phases:

   a) Root Ports selection, Root Bridge selection, Designated Ports selection

   b) Root Bridge selection, Designated Ports selection, Root Ports selection

   c) Root Bridge selection, Root Ports selection, Designated Ports selection

   d) Root Ports selection, Designated Ports selection, Root Bridge selection

50. The Spanning Tree Protocol can have two types of Bridge Protocol Data Unit (BPDU) frames:

   a) Configuration and Topology Change Notification

   b) Configuration and Topology Advertisement

   c) Topology Change Notification and Topology Advertisement

   d) Root Bridge Election and Topology Advertisement

51. During the selection of the Root Bridge, the Spanning Tree process operates by analyzing the value of the following field present in the BPDU:
    a) Root Identifier
    b) Root Path Cost
    c) Port Identifier
    d) Bridge Priority
52. According to the standard, the tree obtained by the Spanning Tree Protocol is computed:
    a) Starting from the physical topology of the network, independently from the VLANs
    b) Starting from the already configured VLANs
    c) Starting from the already configured VLANs, creating a different tree for every VLAN
    d) Starting from the physical topology of the network, taking into account the already configured VLANs
53. We need the Spanning Tree because:
    a) The learning process in bridges cannot operate when the L2 network contains loops
    b) The forward learning process in bridges is not optimized in case of multiple paths toward the destination
    c) In case the network contains multiple paths, the load balancing algorithm can generate frame reordering problems in the destination host
    d) Frames can circulate forever since the Time-To-Live field in the Ethernet frame is not decremented by bridges
54. Given two bridges connected to the same L2 network, in which the Bridge Identifiers are `32768-00:11:22:33:44:55` and `28672-00:22:33:44:55:66`:
    a) The first will become the root bridge
    b) The second will become the root bridge
    c) The value 28672 is not a valid Bridge Priority
    d) The second bridge will become root for the VLAN 0, while the first will become root bridge for all the other VLANs

9 Rapid Spanning Tree and other evolutions

55. Differently from the Spanning Tree Protocol, the Rapid Spanning Tree Protocol:
    a) Supports networks that include Layer-1 hubs
    b) Guarantees fast convergence time
    c) Allows to use fiber optic in the network
    d) Allows to use different VLANs in the network

56. When a switch detects that one of its links gets interrupted, the Rapid Spanning Tree Protocol deletes the corresponding entries in the forwarding database:

    a) When the forward delay timer expires

    b) When the max age timer expires

    c) Immediately

    d) It will set the aging time of those entries to (Max Age - Forward Delay) and then waits for them to expire

57. The Rapid Spanning Tree protocol can guarantees a faster convergence if:

    a) All the links are point-to-point

    b) All the links operate in full-duplex mode

    c) The network does not contain circular paths

    d) The network is structured in a tree-like fashion

58. The Multiple Spanning Tree protocol is useful because:

    a) It reduces the broadcast domain of the network by dividing it into areas called Regions

    b) It works in networks that include hubs

    c) It guarantees faster convergence time with respect to STP and RSTP

    d) It makes the network more scalable, by dividing it into areas called Regions

10 QoS over LAN

59. According to the IEEE 802.1p standard, the priority can be associated to a packet:

    a) Only by the port of the switch

    b) Only by a network interface (NIC) that support this type of function

    c) Either by the port on the switch or by a network interface (NIC) that support this function

    d) Only by the application that generates the traffic

60. The port of the switch connected to a station that is able to associate the “priority” to packets must be:

    a) In Trunk or Access mode

    b) Only in Trunk mode

    c) Only in Access mode

    d) One side of the cable in Trunk mode and the other one in Access

61. The 802.1p standard defines:

    a) Several classes of service for different kinds of traffic

b) Several priorities for different kinds of traffic

c) A Best-Effort class at lower priority with other ones (configurable as you want) at higher priority

d) A group of traffic classes served by a Round Robin scheduler

62. The 802.3x standard defines:

a) A Pause packet to be used in case of host congestion

b) A Pause packet to be used in case of network congestion

c) A Pause packet to be used in case of congestion (host or switch)

d) A mechanism to assign priority to voice traffic

63. The Pause packet in the 802.3x standard:

a) Is sent to the transmitting host in order to reduce the amount of traffic injected in the network

b) Is sent to the transmitting host in order to stop temporarily the traffic injected in the network

c) Is sent to the device connected at the other side of the link in order to reduce the amount of traffic injected in the network

d) Can cause temporary interruptions of the network traffic

64. In a campus network with a 10Gbps backbone, in which we want to transport also voice traffic:

a) You do not need to configure any QoS mechanism

b) It is recommended to implement the 802.3x standard (Pause packets)

c) It is recommended to implement the 802.1p standard associating the highest priority to the voice traffic

d) It is reasonable to implement the 802.1p standard associating a portion of the transmission bandwidth to the voice traffic ("Round Robin" scheduler)

11 Link Aggregation

65. The IEEE 802.3ad standard (Link Aggregation) allows to:

a) Increase the bandwidth on a single point-to-point connection

b) Create a redundant point-to-point connection, without increasing the bandwidth

c) Create a redundant point-to-point connection and increase the bandwidth

d) Create a redundant point-to-point connection

66. In the IEEE 802.3ad standard (Link Aggregation):

a) Both devices at the two ends of the link must support the 802.3ad standard

b) Defines a maximum number of ports that can be part of the logic aggregation

c) Requires that at least one of the devices at the two ends of the link supports the 802.3ad standard

d) Allows the links that are part of a logical aggregation to have different speeds

67. The IEEE 802.3ad standard (Link Aggregation) has some limitations:

   a) It exists a maximum number of ports that can be part of the logic aggregation

   b) The aggregation can be used only on full duplex links

   c) The aggregation can be used only on half duplex links

   d) The links that are part of an aggregation must have different speeds

68. The IEEE 802.3ad standard (Link Aggregation) has some limitations:

   a) On the maximum number of ports that can be part of the logic aggregation

   b) On the load balancing traffic criteria, that must be necessarily based on L2 information

   c) On the links that are part of the aggregation, that must have the same speed

   d) On the use of the Spanning Tree Protocol, that is not supported on logical aggregated links

69. A motivation for the IEEE 802.3ad standard (Link Aggregation) is:

   a) Allows to create a redundant connection in addition to a existing point-to-point link

   b) Allows the concurrent usage of multiple links between 2 switches even in presence of the Spanning Tree Protocol

   c) Makes the update of the filtering database faster, even when the Spanning Tree Protocol is used

   d) Avoids congestions in the network due to the better utilization of the available bandwidth

70. In case of the Link Aggregation standard, identify which sentence is wrong:

   a) The links that are grouped in the same logical aggregate must have the same speed

   b) The links that are grouped in the same logical aggregate must operate in full-duplex mode

   c) The links that are grouped in the same logical aggregate must be attached to the same devices (unless some virtualization technologies such as Cisco VSS are used)

   d) The links that are grouped in the same logical aggregate must be connected to a switch whose ports have the same Port Priority

12 IGMP Snooping

71. The IGMP Snooping mechanism allows:

a) To detect the presence of hosts over the LAN that are member of a multicast IPv6 group

b) To detect the presence of hosts over the LAN that are member of a multicast IPv4 group

c) To detect the presence of hosts over the LAN that are member of a multicast IPv6 or IPv4 group

d) To detect the presence of hosts over the LAN that are member of a IPv4 or IPv6 network

72. The IGMP Snooping function:

    a) Is normally implemented on all level 3 devices present on the LAN

    b) Is normally implemented on level 2 devices present on the LAN

    c) Is needed in order to debug the possible multicast traffic present on the LAN

    d) Is occasionally used in modern devices, whereas it was important in the past

73. In the IGMP Snooping function:

    a) Router intercepts IGMP membership Report packets

    b) Switch intercepts IGMP membership Report packets

    c) Router intercepts both IGMP membership Query/Report packets

    d) Switch intercepts IGMP membership Query/Report packets

74. The IGMP Snooping function:

    a) Affects all multicast traffic on the LAN

    b) Affects all IP multicast traffic on the LAN

    c) Affects a part of IP multicast traffic on the LAN

    d) Affects the part of IP multicast traffic that does not make use of the IGMP protocol

13 Router redundancy (HSRP, VRRP)

75. The HSRP and VSRP protocols are used to:

    a) Propagate automatically the information related to the presence of VLANs in the network

    b) Assign different priorities to packets belonging to different VLANs

    c) Manage automatically the configuration (trunk/access) of the switch ports according to the configuration of the network interface of the PC connected on the other side of the cable

    d) Provide default gateway redundancy

76. A LAN in which the VRRP/HSRP protocols are active:

   a) ARP replies are generated by the two routers in load balancing
   b) ARP replies are always generated by the router that booted first
   c) ARP replies are always generated by the primary router
   d) ARP replies are always generated in multi cast

77. The track functionality of the HSRP protocol can be used to:
   a) Set automatically the IP address of the HSRP virtual router
   b) Set dynamically the MAC address of the HSRP virtual router
   c) Influence the selection of the interface in Active state according to the status of another interface
   d) Influence the selection of the interface in Active state according to the IP address configured on the router

78. HSRP messages are encapsulated in:
   a) TCP
   b) UDP
   c) Directly into IP packets
   d) Directly into Ethernet frames

79. VRRP messages are encapsulated in:
   a) TCP
   b) UDP
   c) Directly into IP packets
   d) Directly into Ethernet frames

80. In HSRP, the two main routers in a LAN can assume the following states:
   a) Master or Slave
   b) Active or Standby
   c) Master or Backup
   d) Active or Inactive

81. In VRRP, the routers in a LAN can assume the following states:
   a) Master or Slave
   b) Active o Standby
   c) Master or Backup
   d) Active or Inactive

82. In the transmission of HSRP messages, the TTL field of the corresponding IP packet is set:
   a) To a random value; when the packet arrives to the router it will be discarded automatically, thus avoiding the forwarding out of the LAN

b) To value “255” and the routers are forced to discard HSRP messages that contain a TTL different from 255

c) To value “0”, thus avoiding that the packet is forwarded out of the LAN

d) To value “1”, thus avoiding that the packet is forwarded out of the LAN

83. In the transmission of VRRP messages, the TTL field of the corresponding IP packet is set:

    a) To a random value; when the packet arrives to the router it will be discarded automatically, thus avoiding the forwarding out of the LAN

    b) To value “255” and the routers are forced to discard HSRP messages that contain a TTL different from 255

    c) To value “0”, thus avoiding that the packet is forwarded out of the LAN

    d) To value “1”, thus avoiding that the packet is forwarded out of the LAN

84. In the HSRP protocol, the load balancing functionality on geographical links:

    a) Is provided automatically

    b) Is provided automatically only for the traffic exiting towards the Internet

    c) Is provided automatically only for the incoming traffic in the LAN

    d) Can be provided only for the traffic exiting towards the Internet

    e) Is not under the control of the HSRP protocol

85. In case of failure of a geographical link connected to an HSRP router in Active state:

    a) The HSRP protocol might change the status of the interface in Active state when the function “track” is enabled

    b) The HSRP protocol automatically elects the other router as Active

    c) The HSRP protocol will not change the status of the routers (i.e. the current router will still be Active)

    d) The HSRP protocol will send an ICMP Router Redirect message to all the hosts on the LAN in order to force them to change their default gateway and to use the second router

86. The phenomenon of flooding of packets on networks that have a redundant default gateway managed by HSRP:

    a) Can occur when there are asymmetric paths (ingress/ egress) of traffic

    b) Can happen only in case of problems on the Spanning Tree Protocol

    c) Can happen only in case some broadcast frames are transmitted

    d) Can never happen

14 Multilayer switches

87. We usually define a wire-speed (or full-speed) Layer-3 switch if it is able to:
    a) Send packets only in full-duplex mode
    b) Send packets only in half-duplex mode
    c) Send packets in both full-duplex and half-duplex mode
    d) Forward an amount of packets equal to the traffic received on all its network interfaces at the same time and at their full rate
88. Layer 4 switches are devices with hardware support to execute operations:
    a) Based on information of Layer 4 and lower layers
    b) Based on information of Layer 4 and higher layers
    c) Based only on Layer 4 information
    d) Based only on Layers 3 and 4 information

15 Network Design at L2/3

89. In the design of the core portion of a campus network, it should be better to select network devices:
    a) That are able to compute quickly the routing tables
    b) That are able to manage very big routing table
    c) With high data forwarding capacity
    d) That are able to support a high number of different data link technologies
90. In case of a network that uses multilayer switches (L2-L3 switches):
    a) Each link that connects a host to the switch is served by an IP network with netmask /30
    b) Each device (switch) has an IP address for each VLAN
    c) The network manager can decide, for each interface of the switch, if it must be configured at level 2 or level 3
    d) We need to use VLANs
91. In case of a network that uses multilayer switches (L2-L3 switches), with the Spanning Tree turned on:
    a) We need first to determine the outcome of Spanning Tree, and then which are the HSRP active/standby routers
    b) We need first to determine which are the HSRP active/standby routers, and then the outcome of Spanning Tree

c) The HSRP active/standby routers and outcome of Spanning Tree are independent issues, although we should determine both

d) We need to determine the outcome of Spanning Tree

92. In case of a network that uses multilayer switches (L2-3 switches):

a) Paths are more optimized if the root bridge overlaps with the possible active router determined by HSRP/VRRP

b) Paths are more optimized if the root bridge does not overlap with the possible active router determined by HSRP/VRRP

c) The path determined by the Spanning Tree and the possible active router determined by HSRP/VRRP are indipendent concepts and therefore they do not affect how traffic is propogated over the network

d) Paths mainly depend on the configuration of level 3 addresses associated with VLANs

16 Content Delivery Networks and Server Load Balancing

93. In a Content Delivery Network, the content of a server (e.g. web pages) are replicated and:

a) Distributed over the network, provided that all servers are physically close together

b) Distributed over the network, provided that all servers are physically far each other

c) Distributed over the network, no matter of the physical location of servers

d) Distributed over the network, provided that all servers belong to the same IP subnet

94. In a DNS-based Content Delivery Network:

a) The DNS answers to users' HTTP requests redirecting them to the nearest cache

b) The DNS answers to domain names requests (e.g "cnn.com") redirecting them to the nearest DNS cache

c) The DNS returns an IP address according to the requested DNS name (e.g. "www.cnn.com") and the source IP address of the client

d) The DNS returns an IP address according to the requested DNSname (e.g. "www.cnn.com") and the destination IP address of the client

95. A Load Balancing Server can operate according to the following principles:

a) Content-unaware (layer 4 switching) and Content-aware (layer 7 switching)

b) Content-unaware (layer 7 switching) and Content-aware (layer 4 switching)

c) Content-unaware (layer 4 switching) and DNS-based Routing

d) DNS-based Routing and Content-aware (layer 7 switching)

96. A Content-unaware Load Balancing Server is able to distribute the load according to:

a) Information present in layer 3, 4 protocols and to the DNS name requested

b) Information present in layer 3 and 4

c) Information present in layer 4 and 7

d) Information present in layer 2, 3, 4 and 7

97. A Sticky Connection:

    a) Identifies an HTTP connection whose state must be maintained for the entire duration of connection

    b) Identify the set of HTTP connections that share some common state (e.g. shopping chart)

    c) Requires that the Server Load Balancer forwards the traffic of a user always to the same physical server

    d) Requires that the web server involved in the transaction stores user data on the same disk of the Storage Area Network

98. In the event that a user connects to a web service that is powered by a battery of physical servers behind a Load Balancer Server, the use of cookies within HTTP sessions:

    a) It may be necessary to handle sticky connections

    b) It may be necessary to store the credentials of a user

    c) It is a technique commonly used to violate privacy of the user

    d) It is a technique to create persistent pop-ups on the user desktop

17 Storage Area Networks

99. Which one among the following points does not apply to Network Attached Storage (NAS):

    a) Most operating systems are able to mount a shared disk without additional drivers

    b) The NAS is able to operate on Wide Area Networks

    c) Minimum impact on existing infrastructure

    d) The client have full control over the disc

100. A Network Attached Storage (NAS):

    a) It is typically used to allow the client to boot from the network

    b) It is typically used to share the disks on Wide Area Networks

    c) Allows clients to have full control over the disc

    d) It has a minimal impact on network infrastructure and existing software

101. In Storage Area Networks (SAN), the virtualization of the storage space is implemented at:

    a) File system level

b) Physical level (blocks on the disk)

c) At choice, File System or Physical level (blocks on the disk)

d) Physical level (blocks on the disk) as long as you use a set of specific File Systems

102. A possible protocol stack used in a Storage Area Network (SAN) is:

a) Fiber Channel - Ethernet

b) Fiber Channel - IP - Ethernet

c) iSCSI - UDP - IP - Ethernet

d) CIFS - TCP - IP - Ethernet

18 802.1x

103. The IEEE 802.1x standard describes the behavior of the EAPoL authentication protocol, which is used to allow the communication between:

a) Supplicant and Authentication server

b) Authenticator and Authentication server

c) Supplicant and Authenticator

d) Supplicant and Authenticator, and then between Authenticator and Authentication server

104. The EAPoL protocol defined in the standard IEEE 802.1x is a:

a) Layer 2 protocol

b) Layer 3 protocol

c) Layer 4 protocol

d) Layer 7 protocol

105. Inside the IEEE 802.1x specification, the RADIUS protocol:

a) Defines the necessary data to the authentication of the user

b) Transports the data concerning the authentication of the user to the RADIUS authentication server

c) Allows the RADIUS authentication server to communicate with the server that keeps the database of the users (es. LDAP, Active Directory, etc.) in the selected domain

d) Allows the exchange of appropriate authentication messages between the client (supplicant) and the access Server (Authenticator)

106. The dynamic associations of a port on a switch to a VLAN that depends on the user that is currently connecting over that port:

a) Cannot be done

b) Is the default solution in VLAN configuration

c) Can be done through a particular extension of the protocol 802.1x

d) Can be done only if the user station has the port configured as “trunk”

107. The protocol 802.1x recognizes the user according to:

a) Proper credentials (e.g. Username/password)

b) The MAC address of the Network Interface Card (NIC) of the user

c) The IP address configured on the interface of the host

d) The DNS name associated to the user