Advanced Networking | Question Bank | Answers

#	Answer
1	*4G LTE routers make use of the wireless SIM card modem to connect to the WAN (Wide Area Network) to get out to the Internet and provide LAN (Local Area Network) connectivity either via Wi-Fi or an Ethernet cable.*
2	*(i) True* *(ii) True* *(iii) True*
3	***ip route 192.168.1.0 255.255.255.0 10.1.1.2***
4	***Classful:*** *RIP v1, IGRP* ***Classless:*** *RIP v2, EIGRP, OSPF, IS-IS, BGP*
5	*The **Border Gateway Protocol (BGP)** is the only currently viable EGP and is the official routing protocol used by the Internet. And because BGP is the only EGP available, the term EGP is rarely used; instead, most engineers simply refer to BGP.*
6	*(i) **EGP:** Exterior Gateway Protocols (EGP) also referred to as inter-AS routing: Used for routing between autonomous systems. Service providers and large companies may interconnect using an EGP.* *(ii) **IGP:** Interior Gateway Protocols (IGP) also referred to as intra-AS routing: Used for routing within an AS. It is . Companies, organizations, and even service providers use an IGP on their internal networks. IGPs include RIP, EIGRP, OSPF, and IS-IS.*
7	*D) They filter traffic based on source IP addresses only.*
8	*(i) This network range could be summarized as **192.168.16.0/20**, with a subnet mask of **255.255.240.0**.* *(ii) Subtract 255.255.240.0 subnet mask from 255.255.255.255 to get the wild card mask **0.0.15.255**.* *(iii) **access-list 10 permit 192.168.16.0 0.0.15.255***
9	

#	Answer

#	Consideration	LAN	VLAN
1.	abbreviation	LAN stands for Local Area Network.	VLAN stands for Virtual Local Area Network.
2.	Cost	The cost of Local Area Network is high.	The cost of Virtual Local Area Network is less.
3.	Latency	The latency of Local Area Network is high.	The latency of Virtual Local Area Network is low.
4.	Devices used	The devices which are used in LAN	The devices which are used in VLAN are: Bridges and switches.

#	Answer

		are: Routers and switches.	
5.	*Packet advertisement*	*In the local area network, the Packet is advertised to each device.*	*In a virtual local area network, packets are sent to specific broadcast domains.*
6.	*Efficiency*	*Local area networks are less efficient than virtual local area networks.*	*Virtual local area networks are more efficient than local area networks.*

10

Description	***Command***
Create VLAN 10	***Switch(config)# vlan 10***

#	Answer

Give a name to VLAN 10	***Switch(config-vlan)# name Admin-dept***
Create VLAN 20	***Switch(config-vlan)# vlan 20***
Give a name to VLAN 20	***Switch(config-vlan)# name Finance-dept***
Exit the VLAN config. mode	***Switch(config-vlan)# exit***
Check if the VLANs were created	***Switch # show vlan brief***

11

Description	***Command***
Enter interface config. mode for fa0/2	***Switch(config)# interface fa0/2***
Set the port to access mode	***Switch(config-if)#switchport mode access***
Assign VLAN 10 to interface fa0/2	***Switch(config-if)#switchport access vlan 10***
Exit the interface	***Switch(config-if)# exit***

#	Answer

Enter interface configuration for fa0/3	***Switch(config)# interface fa0/3***
Set the port to access mode	***Switch(config-if)#switchport mode access***
Assign VLAN 20 to interface fa0/3	***Switch(config-if)#switchport access vlan 20***
Exit the interface	***Switch(config-if)# exit***

12

Device	***Interface***	***IP Address***	***Subnet Mask***	***Default Gateway***
R1	*Fa0/0*	*172.17.10.1*	*255.255.255.0*	*N/A*
R1	*Fa0/1*	*172.17.30.1*	*255.255.255.0*	*N/A*
PC1	*NIC*	*172.17.10.10*	*255.255.255.0*	*172.17.10.1*
PC3	*NIC*	*172.17.30.10*	*255.255.255.0*	*172.17.30.1*

<table>
<tr><th>#</th><th>Answer</th></tr>
<tr><td>13</td><td>
<table>
<tr><th>Device</th><th>Interface</th><th>IP Address</th><th>Subnet Mask</th><th>Default Gateway</th></tr>
<tr><td>PC1</td><td>NIC</td><td>192.168.20.1</td><td>255.255.255.0</td><td>192.168.20.1</td></tr>
<tr><td>PC3</td><td>NIC</td><td>192.168.30.1</td><td>255.255.255.0</td><td>192.168.30.1</td></tr>
<tr><td>R1</td><td>Fa0/0</td><td>192.168.20.2</td><td>255.255.255.0</td><td>N/A</td></tr>
<tr><td>R1</td><td>Fa0/1</td><td>192.168.30.3</td><td>255.255.255.0</td><td>N/A</td></tr>
</table>
(ii) Switch configuration
AS1(config)# interface fastEthernet 0/1
AS1(config-if)# switchport mode access
AS1(config-if)# switchport access vlan 20
AS1(config-if)# exit
AS1(config)# interface fastEthernet 0/2
AS1(config-if)# switchport mode access
AS1(config-if)# switchport access vlan 30
AS1(config-if)# exit
(iii) Complete the router configuration by filling the (…)
R1(config)#interface fastethernet 0/0
R1(config-if)# ip address 192.168.20.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface fastethernet 0/1
R1(config-if)# ip address 192.168.30.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
</td></tr>
<tr><td>14</td><td>

Host A checks whether the destination IP address is in its VLAN; if it is not, the traffic will be forwarded to its default gateway on interface Fa0/0 on the router.
Host A then sends an ARP request to the switch to determine the MAC address of the Fa0/0 interface on the router. Once the router replies, Host A sends the frame to the router as a unicast message, where it is then directly forwarded out the trunk interface to the

</td></tr>
</table>

<table>
<tr><th>#</th><th>Answer</th></tr>
<tr><td></td><td>
router.
3. the router receives the frame, it determines the destination IP address and interface from the routing table.
4. The router then sends an ARP request out the interface connected to the destination VLAN (VLAN 20), which corresponds to interface Fa0/1 on the router.
5. When the switch receives the message, it floods it to its ports, which then triggers Host B to reply with its MAC address.
6. The router then uses the information gathered to forward the message finally to Host B on VLAN 20 as a unicast frame through the switch.
</td></tr>
<tr><td>15</td><td>
(i)
<table>
<tr><th>Subinterface</th><th>VLAN</th><th>IP Address</th></tr>
<tr><td>G0/0/1.10</td><td>10</td><td>192.168.10.1/24</td></tr>
<tr><td>G0/0/1.20</td><td>20</td><td>192.168.20.1/24</td></tr>
<tr><td>G0/0/1.30</td><td>99</td><td>192.168.99.1/24</td></tr>
</table>
(ii) Create VLANs
<table>
<tr><th>Description</th><th>Command</th></tr>
<tr><td>Create VLAN 10</td><td>S1(config)# vlan 10</td></tr>
<tr><td>Give a name to VLAN 10</td><td>S1(config-vlan)# name LAN10</td></tr>
<tr><td>Create VLAN 20</td><td>S1(config-vlan)# vlan 20</td></tr>
<tr><td>Give a name to VLAN 20</td><td>S1(config-vlan)# name LAN20</td></tr>
<tr><td>Create VLAN 30</td><td>S1(config)# vlan 30</td></tr>
<tr><td>Give a name to VLAN 30</td><td>S1(config-vlan)# name Management</td></tr>
<tr><td>Exit the VLAN config. mode</td><td>S1(config-vlan)# exit</td></tr>
</table>
</td></tr>
</table>

#	Answer

Check if the VLANs were created	***Switch # show vlan brief***

16 *(i) The addressing table*

Device	***Interface***	***IP Address***	***Subnet Mask***	***Default Gateway***
PC A	*NIC*	*192.168.10.2*	*255.255.255.0*	*192.168.10.1*
PC B	*NIC*	*192.168.20.2*	*255.255.255.0*	*192.168.20.1*
PC C	*NIC*	*192.168.30.2*	*255.255.255.0*	*192.168.30.1*
PC D	*NIC*	*192.168.40.2*	*255.255.255.0*	*192.168.40.1*

(ii) False.

(iii)
AS1(config)# interface fastEthernet 0/1
AS1(config-if)#switchport mode trunk

(iv) On the R1, configure subinterfaces for respective VLANs.
R1(config)# interface fastethernet0/0.10
R1(config-subif)# encapsulation dot10 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface fastethernet0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface fastethernet0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.168.30.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface fastethernet0/0.40

<table>
<tr><th>#</th><th>Answer</th></tr>
<tr><td></td><td>
R1(config-subif)# encapsulation dot1Q 40
R1(config-subif)# ip address 192.168.40.1 255.255.255.0
R1(config-subif)# exit
R1(config) # interface fastethernet 0/0
R1(config-if)# no shutdown
R1(config-if)# exit

(v)
R1# show ip route
</td></tr>
<tr><td>17</td><td>
(i)
<table>
<tr><th>D1 Interface</th><th>VLAN</th><th>IP Address</th></tr>
<tr><td>G1/0/6</td><td>10</td><td>192.168.10.1/24</td></tr>
<tr><td>G1/0/18</td><td>20</td><td>192.168.20.1/24</td></tr>
</table>
(ii)
D1(config)# vlan 10
D1(config-vlan)# name LAN10
D1(config-vlan)# vlan 20
D1(config-vlan)# name LAN20
D1(config-vlan)# exit
D1(config)#
</td></tr>
<tr><td>18</td><td>
<table>
<tr><th>Description</th><th>Command</th></tr>
<tr><td>Enter interface configuration for GigabitEthernet0/0/1</td><td>D1(config)# interface GigabitEthernet0/0/1</td></tr>
<tr><td>Describe the interface</td><td>D1(config-if)# description routed Port Link to R1</td></tr>
<tr><td>Change the interface from being a Layer 2 interface to a layer 3 interface</td><td>D1(config-if)# no switchport</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>#</th><th>Answer</th></tr>
<tr><td></td><td>
<table>
<tr><td>Set the IP address for the interface</td><td>D1(config-if)# ip address 10.10.10.2 255.255.255.0</td></tr>
<tr><td>Bring up the interface</td><td>D1(config-if)# no shutdown</td></tr>
<tr><td>Exit</td><td>D1(config-if)# exit</td></tr>
<tr><td>Enable IP routing</td><td>D1(config)# ip routing</td></tr>
</table>
</td></tr>
<tr><td>19</td><td>An eavesdropping attack also known as sniffing or snooping, occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices.</td></tr>
<tr><td>20</td><td>a) HTTPS creates an encrypted communication channel that protects against man in the middle (MitM) attacks.</td></tr>
<tr><td>21</td><td>(i) ssh, pi, and 192.165.0.102:

(ii)
ssh provides a secure encrypted connection between two hosts over an insecure network. This connection can also be used for terminal access, file transfers, and for tunneling other applications.

pi is a user on the remote device

192.165.0.102 is an ip address of a remote host</td></tr>
<tr><td>22</td><td>(i) D) Denial of service
(ii) Denial-of-service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a server or network resource unavailable to its intended users by disrupting services using a flood of TCP and UDP packets.</td></tr>
<tr><td>23</td><td>Here are key tips to help secure the home Wi-Fi network against unauthorized access.
Any FOUR of these are accepted.

1. Change the default name of your home Wi-Fi
2. Make your wireless network password unique and strong
3. Enable network encryption
4. Turn off network name broadcasting
5. Keep your router’s software up to date</td></tr>
</table>

#	Answer
	6. Make sure you have a good firewall *7. Use VPNs to access your network*
24	*True.*
25	*WEP*
26	*AES*
27	*A RAID (redundant array of independent disks) setup uses multiple storage drives to create a single workable storage system. This can help improve overall storage efficiency as well as protect against drive failure by incorporating backup drives.*
28	*Data migration is the process of moving data from one system to another.*
29	*A headless server is a computing device without a local interface that is dedicated to providing services to other computers and their users. Headless, in this context, basically means that the computing device has no monitor or peripherals, such as a keyboard and mouse.*
30	*1) Storage Migration* *2) Database Migration* *3) Application Migration* *4) Cloud Migration* *5) Business Process Migration* *6) Data Center Migration*