Networking

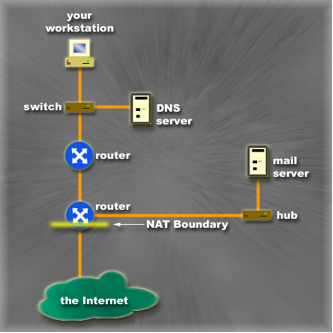
Student's Name

May 8, 2021

Institution Affiliation

**QUESTION 1**

1. Consider the below network diagram and refer to this diagram when composing your answer to the question that follows.



**Describe in as much detail as possible what happens after a computer user clicks a web link. The user's computer, shown as "your workstation" in the diagram above, is connected to a wired Ethernet LAN and has access to the Internet through its gateway router that connects to a NAT router and then to a backbone service provider (part of the Internet cloud). Explain technically how the computer establishes an internetwork connection to an Internet web server (within the Internet cloud on the diagram) and retrieves the following (ficticious) resource:**

[**http://www.boringarchives.com:8217/index.html**](http://www.boringarchives.com:1289/index.html)

**Your answer to this question should be about 1000 to 2500 words and you might want to consider discussion of the following concepts in your writing (to the best of your ability): (1) Router, (2) Switch, (3) Ethernet, (4) Internet cloud, (5) DNS Server on local LAN, (6) ARP, (7) Proxy ARP, (8) encapsulation, (9) broadcast, (10) unicast, (11) file, (12) segment, (13) packet, (14) frame, (15) bit, (16) signal, (17) frame addressing, (18) frame forwarding, (19) packet addressing, (20) packet forwarding, (21) IP, (22) TCP, (23) sliding window flow control, (24) selective reject error control, (25) three-way handshaking, (26) header fields, (27) CSMA/CD, (28) collision, (29) backoff, (30) time out, (31) soft state, (32) address translation, (33) ANDing process, (34) routing table, (35) client, (36) server, and (37) other concepts as needed (NAT for example). Do not number the concepts in your essay.**

Clicking a web link triggers numerous actions. Weblink refers to the uniform resources locator (URL), which stipulates the link’s location in a computer network. The URL comprises two parts, the protocol, and the domain name. A protocol refers to the set of rules used by the browser when communicating across the network. It includes FTP, HTTP, and HTTPS. A domain name is the unique identity part of the URL that a browser uses to reach the server. When clicking a web link, the user tries to open that web page to access a piece of information in it. From the user end, it can occur instantly, however, there are several events and components involved in that process. The major components include the browser, switches, routers, Domain Name System Server, and the internet cloud. The internet cloud hosts the web page the user is looking for. Several processes occur in each component to have successful communication. The general steps include DNS lookup to find the destination IP address, browser initiating the TCP connection with the server and request-response process.

After clicking the web link, the host computer broadcasts the ARP requests to all devices in the subnet. The net then resolves the IP address connected to the domain name. The domain names in the web link are meant to make the user remember the web pages they want to visit. However, they mean nothing to the internet. The system accesses the DNS server via the switch using the ethernet cables. The switch is the building block of the network that connects the user’s computer with the router and the DNS server. The system uses a DNS server to associate the domain name with its IP address that the internet understands. The DNS server contains the list of the domain name and their respective IP addresses. Usually, the process of domain name query has four layers with numerous steps in them.

The browser checks its cache whenever the user clicks a web link. The browser then upholds the DNS histories for a certain duration for all the internet sites the user visited recently. Thus, the first DNS query executes at this point to try to get the Ip addresses connected with the domain name. If it fails to find the IP address in the browser cache, the DNS query then executes in the operating system cache and lastly, it checks in the cache of the router. In case the aforementioned steps fail and no DNS query is achieved, then the resolver server is involved. The resolver address refers to the Internet Service provider. At the resolver server, the DNS query executes in its cache. If there is no success in the latter step, the request is forwarded root/top server. The top server never responds with no results found, but it advises the users where they can get the information they are looking for. For instance, the user is looking for an IP address of a top-level domain ending with .org, .gov, .net, and .com, the server instructs the user to get the information from Top Level Domain server.

The resolver then requests the Top-Level Domain Server the IP address of that specific domain name. The work of the Top-Level Domain Server is to store the information of the domain name address which instructs the requests the resolver to get from the Authoritative Name Server (ANS). The ANS responsibility is to have all the information regarding the domain names. There it provides the IP address that is associated with that specific domain name and redirects it back to the client’s computer. On receiving, the resolver has to store the IP address in its cache to be utilized the next time the user tries to visit the same server.

From the DNS server, the switch, through packet switching, forwards the requests in form of data packets into the first network router. This router reads the information of the network address in the packet header to have the intended destination. Every router has a routing table where it uses to direct the packet to the right destination. The data packets from the sources get forwarded into the second router.

Numerous activities are done in the second router. It segments the network in local area networks and wide area networks where the internet cloud is. The second router is configured with NAT that has an interface for the global network and another interface for the local network. Whenever the packets cross the local network, NAT translates its local IP address into a public IP address. Similarly, when the packets cross the global network, NAT translates its public IP address into a private IP address. In cases where NAT’s IP addresses get exhausted, meaning no IP address to be used to access the private network or the global network, NAT drops the packet and sends a timeout message to the destination prompting the user to try again.

After getting the IP address, the browser initiates a connection with the server, following the internet protocol, TCP/IP being the most common protocol used. TCP's three-way handshake process is used to build the connection between two points. The three-way handshake process, as the name suggests, involves three stages. The first computer sends an SYN message to another computer, which sends back an acknowledgment along with another SYN message. The initial computer on receiving the acknowledgment and SYN sends an ACK message to the second computer which is the server. In case there is no connection between the client and the server, a time-out signal is sent back to the source.

If successful, the network creates a unicast communication between the client and the server. In general, after there is a successful connection between the client and the server the following processes take place. The user, through the browser, requests a piece of information from the server. Since the server has all the information, it responds with all the information the user requested including the cache-control, status-code, and the web page. The server will communicate back to the user through the second router which has the NAT that will convert the public IP address into a private IP address. The second router then forwards the data packets into the first router depending on its routing table. The first router then forwards the packets into the client computer via the switch. The browser finally displays all the information to the user’s screen. All these processes seem lengthy but the system developers have made it happen in less than seconds.

**QUESTION 2**

1. An ICMPv4 message indicating a packet could not be fragmented would have the TYPE field set to 00000011 and the CODE field set to 00000100.

 True

 False

**QUESTION 3**

1. TFTP runs on UDP port 69 while FTP runs on TCP ports 20 and 21.

** True**

 False

**QUESTION 4**

1. If the CODE bits in a TCP segment are set to 000001, the packet is a SYN packet.

 True

 False

**QUESTION 5**

1. If a router receives a datagram but the incoming datagram queue is already full, the router will discard the datagram.

 True

 False

**QUESTION 6**

1. Ethernet uses 'counted-effort' delivery semantics and has distributed access control.

 True

 False

**QUESTION 7**

1. SPF algorithms scale better than distance vector algorithms.

 True

 False

**QUESTION 8**

1. DOCSIS established universal ground rules for the transmission of packets across cable networks.

 True

 False

**QUESTION 9**

1. Because TFTP does not allow directory browsing a user must specify the desired directory before logging in to the TFTP server.

 True

 False

**QUESTION 10**

1. Short-term variance in packet travel time is known as jitter.

 True

 False

**QUESTION 11**

1. Routers store forwarding information in routing tables that include the nexthop IP address and the internet protocol address of each host.

 True

 False

**QUESTION 12**

1. DWDM can handle gradually increasing demand for capacity from customers.

 True

 False

**QUESTION 13**

1. An IP packet destined for 10.20.20.81 arrives at a router.  Which of the following routes from the routing table will be selected to forward the packet?

|  |  |  |
| --- | --- | --- |
|  |  | a) Send packets destined for 0.0.0.0/0 out port Eth0 |
|  |  | b) Send packets destined for 10.0.0.0/8 out port Eth1 |
|  |  | c) Send packets destined for 10.20.0.0/16 out port Eth2 |
|  |  | d) Send packets destined for 10.20.20.0/24 out port Eth3 |
|  |  | e) Send packets destined for 10.20.20.0/25 out port Eth4 |
|  |  | f) Send packets destined for 10.20.20.0/26 out port Eth5 |

**QUESTION 14**

1. With standard subnetting and assuming that subnet 0 cannot be used, the 12,345th useable host on the 678th useable subnet of 9.0.0.0 when borrowing 10 bits is 9.14.240.57.

 True

 False

**QUESTION 15**

1. Mapping from high level addresses to low level addresses is known as address resolution.

 True

 False

**QUESTION 16**

1. A directed broadcast puts all ones except the least significant bit in the host portion of the IP address.

 True

 False

**QUESTION 17**

1. The IAB organization has two main subgroups, the IRSG and the IETF.

 True

 False

**QUESTION 18**

1. Research that eventually led to the establishment of the Internet was started by the Advanced Research Projects Agency.

 True

 False

**QUESTION 19**

1. Classful addressing helps relieve the IPv4 address exhaustion problem by allowing appropriately sized blocks of addresses to be assigned.

 True

 False

**QUESTION 20**

1. NAT, PAT and IP Subnetting are techniques that have extended the life of IPv4 by delaying the consumption of IP addresses.

 True

 False

**QUESTION 21**

1. To reduce waste when subnetting, borrow exactly half the host bits.

 True

 False

**QUESTION 22**

1. Theoretically, the fifth useable subnet of 101.0.0.0 using mask 255.1.1.1 is 101.1.0.1 assuming subnet 0 cannot be used.

 True

 False

**QUESTION 23**

1. Which one of the following addresses is a valid IPv6 address?

|  |  |  |
| --- | --- | --- |
|  |  | 2001:1:0:4F3A:206:AE14 |
|  |  | 2001:1:0:4F3A:0:206:AE14 |
|  |  | 2001:1:0:4F3A::206:AE14 |
|  |  | 2001:1::4F3A:206::AE14 |
|  |  | None of the above |

**QUESTION 24**

1. What IPv4 header fields have been removed from the IPv6 header?

|  |  |  |
| --- | --- | --- |
|  |  | Version, fragmentation fields, Header Checksum, and Padding. |
|  |  | Version, Header Length, fragmentation fields, and Header Checksum. |
|  |  | Header Length, fragmentation fields, Header Checksum, and Flow Label. |
|  |  | Header Length, fragmentation fields, Header Checksum, and Padding. |
|  |  | None of the above |

**QUESTION 25**

1. What type of transport did the ADSL Forum recommend in the first phase of VoDSL?

|  |  |  |
| --- | --- | --- |
|  |  | Internet Protocol version 4 |
|  |  | Asynchronous Transfer Mode |
|  |  | Frame Relay |
|  |  | SONET STM-1 |
|  |  | All of the above |
|  |  | None of the above |

**QUESTION 26**

1. Which of the following is present in VoDSL, VoCable and conventional POTS networks?

|  |  |  |
| --- | --- | --- |
|  |  | queueing delay and jitter |
|  |  | jitter and echo |
|  |  | echo and signaling |
|  |  | cross talk and lost packets |
|  |  | Queuing delay, jitter and echo |
|  |  | cross talk, lost packets, and signaling |

**QUESTION 27**

1. What differs from PPTP by allowing tunnels to support more than one connection?

|  |  |  |
| --- | --- | --- |
|  |  | L2TP |
|  |  | L2F |
|  |  | IPSec |
|  |  | All of the above |
|  |  | L2TP and L2F only |
|  |  | None of the above |

**QUESTION 28**

1. A VPN must provide which critical function to ensure security for data?

|  |  |  |
| --- | --- | --- |
|  |  | Authentication |
|  |  | Authorization |
|  |  | Accounting |
|  |  | Data Transparency |
|  |  | All of the above |
|  |  | None of the above |

**QUESTION 29**

1. What does DWDM allow the transmission of over the optical layer?

|  |  |  |
| --- | --- | --- |
|  |  | Voice and e-mail |
|  |  | Video and multimedia |
|  |  | Data |
|  |  | All of the above |
|  |  | Voice, e-mail and data only |
|  |  | None of the above |

**QUESTION 30**

1. Which technology provides a means of securing the interactions between domain name servers?

|  |  |  |
| --- | --- | --- |
|  |  | PreshareDNSA |
|  |  | DNSAuth |
|  |  | DNSSEC |
|  |  | AutoDSP |
|  |  | IPSEC |
|  |  | None of the above |

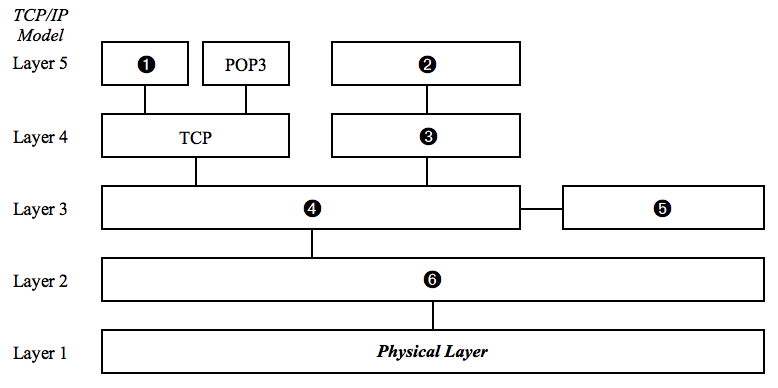
**QUESTION 31**

1. A 100 hour DHCP lease is granted to a workstation. A) How long can the workstation wait in the rebind state before it's lease expires? ... and B) How long can the workstation use the lease in the bound state before it has to request an extension of it's lease?

|  |  |  |
| --- | --- | --- |
|  |  | A: 12.5 hours B: 37.5 hours |
|  |  | A: 12.5 hours B: 50 hours |
|  |  | A: 50 hours B: 37.5 hours |
|  |  | A: 50 hours B: 12.5 hours |
|  |  | A: 87.5 hours B: 12.5 hours |
|  |  | A: 12.5 hours B: 87.5 hours |

**QUESTION 32**

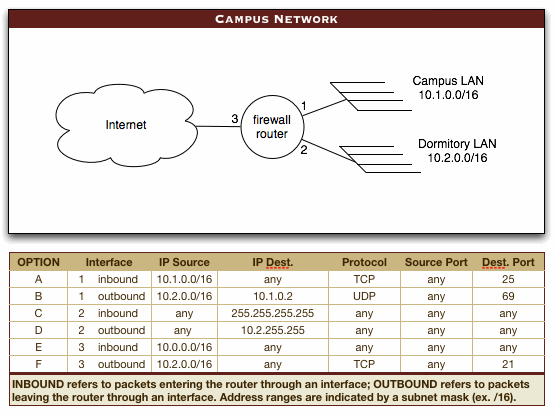
After reviewing the graphic, read the statements below and place a check mark beside each statement that is true. Leave false statements unchecked.



|  |  |  |
| --- | --- | --- |
|  | a. | TFTP and DNS protocols belong in Box 2. |
|  | b. | DHCP and IMAP belong in Box 1. |
|  | c. | Ethernet, 802.11 (WiFi), PPP and BGP belong in Box 6. |
|  | d. | IPv4 may be in Box 5 if IPv6 is in Box 4 and vice versa. |
|  | e. | When ICMPv6 is in Box 4, ICMPv4 may be in Box 5. |
|  | f. | SNMP may occur in either Box 1 or Box 2. |

**QUESTION 33**

1. Review the following diagram.



By reviewing the diagram and the potential packet filters listed, match the filtering concepts presented below with the right packet filters (identified by an OPTION letter).

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | a. | Would block packets coming in from the Internet that have a source IP address that is part of the reserved private address space. | | Option E |
| |  |  | | --- | --- | | b. | Prevents forwarding limited broadcasts. | | Option C |
| |  |  | | --- | --- | | c. | Prevents forwarding of directed broacasts. | | Option B |
| |  |  | | --- | --- | | d. | Prevents Dormitory LAN hosts from connecting to the TFTP server on the Campus LAN. | | Option B |
| e. Prevent hosts on the Dormitory LAN from connecting to FTP servers on the Internet. | Option F |
| f. Prevent hosts on the Campus LAN from connecting to a send mail server not on the 10.1.0.0/16 network segment. | Option A |
|  |  |

Bottom of Form