**NAME: Donghang He**

* **Chapter 10: pg 279 - Question # 5 (was page#290 in 12th edition): Explain one reason why you might experience long response times in getting a Web page from a server in your own city.**

If the other organization uses a different local tier 3 ISP, which, in turn, uses a different regional tier 2 ISP for its connection into the Internet, the message may have to travel all the way to the nearest IXP, which could be in Chicago, Dallas, or New York, before it can move between the two separate parts of the Internet.

* **Chapter 10: pg 279 - Question # 16 (was page#290 in 12th edition): Explain how WiMax works.**

**WiMax** is the commercial name for a set of standards developed by the IEEE 802.16 standards group. WiMax is a family of technologies that is much like the 802.11 Wi-Fi family. It reuses many of the Wi-Fi components and was designed to connect easily into Ethernet LANs. WiMax can be used as a fixed wireless technology to connect a house or an office into the Internet, but its future lies in its ability to connect mobile laptops and smartphones into the Internet.

Although WiMax can be used in fixed locations to provide Internet access to homes and offices, we will focus on mobile use as this is likely to be the most common use. Mobile WiMax works in much the same way as Wi-Fi. The laptop or smartphone has a WiMax network interface card (NIC) and uses it to establish a connection to a WiMax access point (AP). Many devices use the same AP, so WiMax is a shared multipoint service in which all computers must take turns transmitting. Media access control is controlled access, using a version of the 802.11 point coordination function (PCF).

WiMax uses the 2.3, 2.5, and 3.5 GHz frequency ranges in North America, although additional frequency ranges may be added. The maximum range is from 3 to 10 miles, depending on interference and obstacles between the device and the AP. Most WiMax providers in the United States are using effective ranges of 0.5–1.5 miles when they install WiMax APs.

* **Chapter 11: pg 333 - Question # 13 (was question#14 on page#346 in 12th edition): How does a denial-of-service attack differ from a distributed denial-of-service attack?**

The key difference between DoS and DDoS attacks is that the latter uses multiple internet connections to put the victim’s network offline whereas the former uses a single connection. DDoS attacks are more difficult to detect because they are launched from multiple locations so that the victim can’t tell the origin of the attack. Another key difference is the volume of attack leveraged, as DDoS attacks allow the attacker to send massive volumes of traffic to the victim’s network.

It is important to note that DDoS attacks are executed differently to DoS attacks as well. DDoS attacks are executed through the use of botnets or networks of devices under the control of an attacker. In contrast, DoS attacks are generally launched through the use of a script or a DoS toollike Low Orbit Ion Cannon. (**Dos vs DDoS Attacks**)

* **Chapter 11: pg 333 - Question # 40 (was question#43 on page#346 in 12th edition): What are the three major ways of authenticating users? What are the pros and cons of each approach?**

Gaining access to an account can be based on something you know, something you have, or something you are.

The most common approach is something you know, usually a password. Before users can log in, they need to enter a password. Unfortunately, passwords are often poorly chosen, enabling intruders to guess the mand gain access. Some organizations have moved to passphrases which, as the name suggests, are a series of words separated by spaces.

About a third of organizations go beyond this and are requiring users to enter a password in conjunction with something they have, which is called two-factor authentication because the password is the first factor and the object is the second.

In high-security applications, a user may be required to present something he or she is, such as a finger, hand, or the retina of the eye for scanning by the system. These biometric systems scan the user to ensure that the user is the sole individual authorized to access the network account.

* **Chapter 11: pg 367 - Question # 4 (was page#382 in 12th edition): Describe what configuration management encompasses.**

Configuration Management is the process of organizing and maintaining information about all the components of a computer network. When a network needs repair, modification, expansion or upgrading, the administrator refers to the network configuration management database to determine the best course of action. This database contains the locations and network addresses of all hardware devices, as well as information about the programs, versions and updates installed in network computers. People think of configuration management as its just managing the configurations of the network devices, but configuration management covers a lot more than this.

* **Chapter 11: pg 367 - Question # 22 (was page#382 in 12th edition): What is server virtualization?**

A special device called a load balancer or virtual server acts as a traffic manager at the front of the server farm. All requests are directed to the load balancer at its IP address. When a request hits the load balancer, it forwards it to one specific server using the server’s IP address. Sometimes a simple round-robin formula is used (requests go to each server one after the other in turn); in other cases, more complex formulas track how busy each server actually is. If a server crashes, the load balancer stops sending requests to it, and the network continues to operate without the failed server. Load balancing makes it simple to add servers (or remove servers) without affecting users. You simply add or remove the server(s) and change the software configuration in the load balancer; no one is aware of the change.

* **REFERENCES:**

Business Data Communications and Networking (13th Edition) [Fitzgerald, Dennis, Durcikova]

**Dos vs DDoS Attacks: The Differences and How To Prevent Them**

https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/

* **ASSIGNMENT GRADING RUBRIC:**

**\*\*\* DO NOT REMOVE BELOW GRADING RUBRIC FROM YOUR SUBMISSION \*\*\***

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Grade** | **Qualities Demonstrated by the Assignment Submission** | **Grade Assigned** |
| **Content (70%)**  **Measures the quality of the content in the assignment** | A+ 🡺 100 | The content demonstrates exceptional understanding of all relevant subject matter and its inter-relationships. All major relevant issues are thoroughly covered, and all content is very focused and on-topic. There is no known way to improve the content, and there are absolutely no technical or coverage errors present. |  |
| A 🡺 96 | The content demonstrates exceptional understanding of all relevant subject matter and its inter-relationships. All major relevant issues are thoroughly covered, and all content is very focused and on-topic. At most one insignificant technical or coverage error may be present |
| A- 🡺 92 | The content demonstrates deep understanding of all relevant subject matter and its inter-relationships. All major relevant issues are covered, and all content is on-topic. |
| B+ 🡺 88 | The content demonstrates understanding of all relevant subject matter and its inter-relationships. Almost all major relevant issues are covered, and the content is at least reasonably on-topic. |
| B 🡺 85 | The content demonstrates understanding of most relevant subject matter and its inter-relationships. Almost all major relevant issues are covered, and all content is at least reasonably on-topic. |
| B- 🡺 82 | The content demonstrates moderate understanding of much relevant subject matter and its inter-relationships. There is reasonable coverage of major relevant issues, and the content is at least reasonably on-topic. |
| C+ 🡺 78 | The content demonstrates some understanding of relevant subject matter and its inter-relationships. Some major relevant issues are covered, and at least some content is on-topic. |
| C 🡺 75 | The content demonstrates understanding of a small portion of the relevant subject matter and its inter-relationships. Some major relevant issues are covered, and at least a small portion of the content is on-topic. |
| C- 🡺 72 | The content demonstrates little understanding of and insight into the relevant subject matter and its inter-relationships. A small portion of the major relevant issues are covered. The focus of the content may be off topic or on insubstantial or secondary topics |
| D 🡺 67 | The content demonstrates almost no understanding of or insight into the relevant subject matter and its inter-relationships. Almost none of the major relevant issues are covered, and the content may be almost entirely off-topic. |
| F 🡺 0 | The content demonstrates no understanding of or insight into the relevant subject matter and its inter-relationships. No major relevant issues are covered, and the content is entirely off-topic. |
| **Exposition (30%)**  **Measures how well the content is expressed** | A+ 🡺 100 | The presentation of all ideas and designs is exceptionally clear and persuasive; the entire submission is exceptionally organized. There is no known way to improve the clarity or organization of the submission. |  |
| A 🡺 96 | The presentation of all ideas and designs is exceptionally clear and persuasive; the entire submission is exceptionally organized. There may be at most one insignificant way to improve the clarity or organization of the submission. |
| A- 🡺 92 | The presentation of all ideas and designs is very clear and persuasive; the entire submission is very organized. |
| B+ 🡺 88 | The presentation of all ideas and designs is clear and persuasive; the entire submission is organized. |
| B 🡺 85 | The presentation of most ideas and designs is clear and persuasive; most of the submission is organized. |
| B- 🡺 82 | The presentation of most ideas and designs is generally clear; most of the submission is reasonably organized. |
| C+ 🡺 78 | Some parts of the submission are hard to understand; some parts are disorganized. |
| C 🡺 75 | About half of the submission is hard to understand; about half is disorganized. |
| C- 🡺 72 | Most parts of the submission are hard to understand; most parts are disorganized. |
| D 🡺 67 | Almost all of the submission is hard to understand and disorganized. |
| F 🡺 0 | The entire submission is hard to understand and disorganized. |
| **OVERALL GRADE:** | | |  |