MET CS 625 Business Data Communication and Networks
Assignment 5

Review the hypothetical scenario below, then answer the subsequent questions.

Metropolis College is a smaller-size college that now has three campuses. Its main (and original) campus is located in downtown Metropolis, where about 600 students attend. About two years ago, the college established two satellite campuses in two smaller nearby towns – Angel Grove and Springfield – in an effort to better accommodate students living outside of Metropolis. Each satellite campus has one smaller classroom with a video feed to the main campus, and a lab where students can work on their assignments. Minimal network infrastructure has been setup at the satellite offices.

Choosing the right network setup is a challenge for Metropolis College given that its smaller size gives it access to fewer resources. The main campus connects to the Internet with a 10 Gbps fiber link, Angel Grove with a 7 Mbps DSL line, and Springfield with a 25 Mbps cable modem. Each campus has its own direct link to the Internet, and there are no WAN links between campuses. While Internet connectivity works well at the Metropolis campus, there are issues with Internet connectivity on both other campuses. In addition, both satellite campuses have been hacked in different ways due to network security issues. Metropolis College has hired you to identify the problems and propose solutions for their network issues.

Issue 1 – Satellite Office Speeds
Both satellite offices have Internet connectivity issues. Instructors at the Angel Grove campus often complain that the video feed to the main campus often stalls to the point that it's not viable, and they have given up using it. Students using the Angel Grove lab machines complain that the software they use, which relies heavily on Internet communications, is painfully slow, almost to the point of being unusable. While students are not happy with the software performance on the Springfield campus, they are still able to use it to get their work done. Unfortunately, the video feed for instructors on the Springfield campus has the same issues as the Angel Grove campus. As a whole, people are becoming quite frustrated with these issues, and Metropolis College is worried that they may lose students, and even possibly instructors.

With some research you discover the following Internet connectivity options exist at the Angel Grove campus.

Angel Grove Campus

Option	**Cost**
Use a DSL line at the maximum speed available, 12 Mbps.	$60 per month
Use a cable modem.	Three speeds are available: o 25 Mbps at $65 per month o 50 Mbps at $90 per month o 100 Mbps at $140 per month

You discover the following options are available at the Springfield Campus. Note that the phone and cable providers are the same between both towns, but Springfield has a fiber option.

Springfield Campus

Option	Cost
Use a DSL line at the maximum speed available, 12 Mbps.	$60 per month.
Use a cable modem.	Three speeds are available: o 25 Mbps at $65 per month o 50 Mbps at $90 per month o 100 Mbps at $140 per month
Switch to using fiber.	Three speeds are available: o 50 Mbps at $80 per month o 200 Mbps at $150 per month o 1 Gbps at $300 per month

1. ***The first item the college needs to consider is which underlying technology to use at the satellite offices (DSL, cable modem, or fiber). Compare and contrast each of these three with at least 6 points of comparison, making sure to relate them back to the college's needs at the satellite office.***

DSL	Cable modem	Fiber
A family of point – to – point technology	Cable networks are multipoint	A dedicated point – to – point
Provides high – speed transmissions over traditional telephone wires	Use hybrid fiber coaxial (HFC) networks with coaxial cables in the customer premises	Use high- speed cables made of fibers and glass
Speed: DSL, which will rarely exceed 30 Mbps at best. The theoretical max speed varies depending on the type of DSL such as ADSL and VDSL. DSL line is at the maximum speed available, 12 Mbps in this scenario.	Speed: Cable comes in at second place (it is faster than DSL). Although you can find cable connections as fast as 500 Mbps (and the theoretical limit is as high as 10 Gbps), It falls in the 25 to 100 Mbps range in this scenario.	Speed: Fiber is easily the fastest and most stable. Fiber connections in this scenario have speeds of at least 50 Mbps and can go all the way up to 1 Gbps.
Cost: Cheapest among all three. Its $60 per month in this scenario.	Cost: Multiple speed and ranges. It ranges from $65 - $140 per month depend on the speed in this scenario.	Cost: Expensive to deploy. It ranges $80 - $300 depends on the speed in this scenario.
DSL is the most widely available	Cable modems are also widely available.	Limited coverage. Service is still very limited, which means people who live in metropolitan cities have a better chance of

		finding it than those living in rural areas
Bandwidth dependent on distance from equipment	Shared bandwidth, so the bandwidth will be different depend on number of users using at the same time.	Fiber is a dedicated circuit and offers consistent, fast speeds.

2. ***Which technology and speed would you recommend for Internet connectivity at Angel Grove and Springfield? Explain why you believe this to be the best choice for each campus.***

Angel Grove Campus: There are only two option such as DSL and Cable modern. According to the scenario that even though Springfield connects with 25 Mbps cable modern but it still experiencing bad issue with video feed. In contrast, students are not happy with software performance, but they are still able to use to get work done, with all those logics I would recommend cable modern technology with 50 Mbps or 100 Mbps internet connectivity for Angel Grove campus. So, it will help the campus in getting better internet which will help the students in completing their work without much delay as well as video feed for instructor without any problem. They can choose one of those depend on their spending budget as well.

Springfield Campus: There are 3 options such as DSL, Cable Modem and Fiber. With the same logics that Springfield connects with 25 Mbps cable modern but it still experiencing bad issue with video feed. In contrast, students are not happy with software performance, but they are still able to use to get work done. Also, Springfield campus has fiber option, Therefore, I have 2 recommendations for this campus. Firstly, I would recommend cable modern technology with 50 Mbps or 100 Mbps speed internet connectivity. Secondly, I would recommend fiber technology with 50 Mbps or 200 Mbps or 1 Gbps speed for internet connectivity. The internet connectivity speeds are dependent on their spending budgets for both recommendations as well. But the fiber option is the better option because they also provide 50 Mbps but cheaper price compares with cable modem, they also have higher speed options but more expensive. There are many advantages of using fiber option such as support high data transmission in both uploads and downloads, strong connection, and it provides a very good quality of cable.

Issue 2 – Metropolis Campus Hacked

A server, which resides on the main campus, and which acts as the repository for student grades, was hacked. The incident actually went undiscovered for about three weeks, when it was discovered by happenstance by an instructor. She noticed the web grading program showing different grades for a couple of prior students than what she had assigned. She alerted the college's small I.T. department, which used the only evidence they had on the matter – an audit log and a monthly backup file. The department discovered through the audit log that the attacker illegally gained access and downloaded all grades in the system, and that the attacker had actually carried out the hack at the lab in the Springfield campus! By comparing the backup file with the current data, they also discovered that a few specific student grades had been altered. Thankfully only a few grades were altered, but this raised the question if those few students were involved with the attack. Regardless, the college is

scrambling to upgrade security on their network to prevent this and other kind of attacks in the future.

The server room at the Metropolis campus currently has only one network security control, which is a packet filtering firewall that sits between the Internet link and the server room. That firewall is configured to prevent inbound traffic coming in over a few ports, and outbound traffic leaving the campus over a few ports.

3. As one familiar with network security, you recognize it is essential that the campus secure its network perimeter so that only those authorized can gain access. Identify and describe two points of entry onto the main campus's network that could potentially be used by an intruder to gain access to the network. Make sure to explain to the firm how the intruder could have gained access through each point of entry.

a. The first point of entry onto the main campus's network could be through Internet because according to the scenario that each campus has its own direct link to the Internet, and there are no WAN links between campuses. There is only one network security control which is packet filtering firewall, this firewall is only configured to prevent inbound and outbound traffic over a few ports not all ports.

b. The second point of entry could be using Trojan horse tool to access to server room. When the user downloads and plays a music file, it plays normally and the attached Trojan software silently installs a small program that enables the attacker to take complete control of the user's computer, so the user is unaware that anything bad has happened. The attacker then simply connects to the user's computer and has the same access and controls as the user and getting access to the server to change the grades.

4. Explain the mechanics of how the packet filtering firewall could be used to help secure Metropolis College's network perimeter, for each of the points of entry described in #3. Would anything need to change with the firewall's current setup to provide this network security?

A packet-level firewall (packet filtering firewall) examines the source and destination address of every network packet that passes through it. It only allows packets into or out of the organization's networks that have acceptable source and destination addresses.

The firewall examines each packet, which comprises user data and control information, and tests them according to a set of pre-established rules. If the packet completes the test successfully, the firewall allows it to pass through to its destination. It rejects those that don't pass the test. Firewalls test packets by examining sets of rules, protocols, ports, and destination addresses.

The current firewall is configured to prevent inbound traffic coming in over a few ports, and outbound traffic leaving the campus over a few ports. So, we need to apply configure to prevent both inbound traffic and outbound traffic to all ports.

We also can install Intrusion prevention systems (IPSs) which are designed to detect an intrusion and take action to stop it.

5. Identify a second kind of firewall not yet used, explain the mechanics of how it works to protect networks in general, and explain how this firewall could be used to secure the points of entry identified in #3.

A second kind of firewall can be use is an application-level firewall which examines the contents of the application-level packet and searches for known attacks. Application-layer firewalls have rules for each application they can process.

Application-level firewalls can use stateful inspection, which means that they monitor and record the status of each connection and can use this information in making decisions about what packets to discard as security threats.

Many application-level firewalls prohibit external users from uploading executable files. In this way, intruders (or authorized users) cannot modify any software unless they have physical access to the firewall. Some refuse changes to their software unless it is done by the vendor. Others also actively monitor their own software and automatically disable outside connections if they detect any changes.

6. There are additional ways to secure points of entry other than using firewalls. For each point of entry identified in #3 for the campus' network, identity and describe a device or method that could be used to secure it other than a firewall.

One way to secure points of entry is using Intrusion prevention systems which are designed to detect an intrusion and take action to stop it. There are two general types of IPS, and many network managers choose to install both. The first type is a network-based IPS, an IPS sensor is placed on key network circuits. An IPS sensor is simply a device running a special operating system that monitors all network packets on that circuit and reports intrusions to an IPS management console. The second type of IPS is the host- based IPS, which is a software package installed on a host or server. The host-based IPS monitors activity on the server and reports intrusions to the IPS management console.

Another way is preventing social engineering by training end users on phishing and clicking, even though training end users not to divulge passwords may not eliminate social engineering attacks, but it may reduce their effectiveness so that hackers give up and move on to easier targets.

Another way is using user authentication method such as two-factor authentication. Two-factor authentication commonly employs the user's mobile phone. The user installs an app on his or her mobile phone (Duo is a common one) and adds this app information to his or her account. When the user logs in, the software sends an alert to the app, which asks the user to confirm or deny the login. This greatly increases security, because an attacker must physically have the user's mobile phone and be able to login to it, as well and knowing the user's password.

Issue 3 – Eavesdropping

Several applications used by the college's lab connect over the public Internet to the main office. You recognize that this has major security implications in that unauthorized people can potentially eavesdrop on the communications.

7. You further recognize that at the very least, directly encrypting the communications between the client and server in the application would protect against this eavesdropping. Explain to the college the purpose of encryption and how it would protect the applications' communications.

Encryption consists of encoding information so that only authorized parties can read the content of the information they exchange.

Encryption is the process of disguising information, whereas decryption is the process of restoring it to readable form. When information is in readable form, it is called plaintext; when in encrypted form, it is called ciphertext.

Encryption can be used to encrypt files stored on a computer or to encrypt data in transit between computers. This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet.

To unlock the message, both the sender and the recipient must use an encryption key. The key is a relatively small numeric value (a collection of algorithms that translates and untranslated data back to a readable format. The larger the key, the more secure the encryption.

There are two fundamentally different types of encryptions: symmetric and asymmetric. With symmetric encryption, the key used to encrypt a message is the same as the one used to decrypt it. With asymmetric encryption, the key used to decrypt a message is different from the key used to encrypt it.

8. Also explain the differences between symmetric and asymmetric encryption, making sure to cover the topics below.

a) **the number of keys involved**
b) **key management and distribution**
c) **mathematical operations performed on data**
d) **relative speed**

Symmetric encryption	Asymmetric encryption
Symmetric algorithms use the same key for both encryption and decryption.	Asymmetric algorithms use 2 keys: one for encryption and another for decryption.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
Less secured due to use a single key for encryption.	Much safer as two keys are involved in encryption and decryption.

Mathematically: C = F(P,K), P = F-1(C, K) Plaintext, P—The original data message Encryption algorithm, F—Algorithms that perform transformations on the plaintext Secret key, K—Input to the encryption algorithm with instructions on what to do Ciphertext, C—Scrambled message Decryption algorithm, F-1—Encryption algorithms run in reverse	In general, in this algorithm, *C = E(PU, P)*, followed by *P = D(PR, C)* or *C = E(PR, P)*, followed by *P = D(PU,C)* E is the encryption function D is the decryption function PU is the public key PR is the private key
- To maintain confidentiality, every two parties who want to communicate must have their own secret, shared key. The total number of keys that must be managed for *n* communicating parties is equal to *n * (n – 1) / 2*, which can be a very large number even for moderate values of *n*. - Key would have to be hand-delivered	if two parties wish to communicate with each other, there is no need to exchange keys beforehand. Each knows the other's public key from the listing in a public directory and can communicate encrypted information immediately. The key management problem is reduced to the on-site protection of the private key.

9. Which of these two types of encryption would you recommend for the college's applications?

I would recommend both type of encryption for the college's application. Because Symmetric encryption is faster than Asymmetric encryption and Symmetric encryption is preferable in the large data. And because of Asymmetric encryption is more secure because it uses different keys for the encryption and decryption process, when a message is encrypted using a public key, it can only be decrypted using a private key.

Tying It Together

10. Taking a step back and looking at Metropolis College's network as a whole, would establishing private WAN links between the campuses make for a more performant, reliable, and secure network? Explain.

Yes, establishing private WAN links between the campuses make for a more performant, reliable, and secure network because:

- Using WAN circuits to connect the different campuses so students on any campus can access resources on any campus.
- WAN provides a direct communication mechanism between the main and satellite campuses.

- Setting up a WAN allows to share sensitive data with all campuses without having to send the information over the Internet.

- IT department might find this solution easier to implement and support, as it may allow them to consolidate multiple services in a single dashboard.

11. What would be the advantages and disadvantages of making the architectural change described in #10?

Advantages:

- Setting up a WAN allows you to share sensitive data with all your sites without having to send the information over the Internet.

- WANS often use leased lines instead of broadband connections to form the backbone of their networks → increase bandwidth.

- Lower latency and packet loss inside the WAN.

- Provides dedicated network among all campuses.

- Using WAN circuits to connect the different campuses so students on any campus can access resources on any campus.

Disadvantages:

- WANs are complicated and complex, so they are rather expensive to set up.

- WANs open the way for certain types of internal security breaches, such as unauthorized use, information theft, and malicious damage to files.

- Maintaining a WAN is a challenge. Must be able to detect failures before they occur and reduce data center downtime as much as possible, regardless of the reasons.

- Requires more administrative control than the public networks.

12. What other changes, administratively or technically, could take place to help secure the college's network? Identify and describe at least two.

a. Device failure protection.

Because every computer network device, cable, or leased circuit will fail eventually, so the best way to prevent a failure from impacting business continuity is to build redundancy into the network.

- Redundancy in devices and circuits
- Uninterruptible power supplies
- Failover server clusters or high – availability clusters.

b. Disaster Protection.

- A disaster is an event that destroys a large part of the network and computing infrastructure in one part of the organization.
- Storing data in multiple locations and avoiding locations prone to natural disasters
- College should have a clear disaster recovery plan, which should address various levels of response to several possible disasters and should provide for partial or complete recovery of all data, application software, network components, and physical facilities

Your assignment will be evaluated according to the following rubric.

	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 Assignment Grade:			

Use the **Ask your Facilitator Discussion Board** if you have any questions regarding how to approach this assignment.

Save your assignment as ***lastnameFirstname_assignment5.doc*** and submit it in the *Assignments* section of the course.

For help uploading files please refer to the *Technical Support* page in the syllabus.