CSC626 Networking Fundamentals

Assignment 1

Keith Ah Sing [s2009001714]

Question 1: What type of network would you recommend and why?

Thrift Towne has the following constraints:

- zero budget allocation
- mediocre technical expertise of users
- network security is not a concern
- equipment; 4 PC's and a hub each (PC) meeting the minimum requirements of the Windows 7 operating system.

With the above constraints, a peer-to-peer network would be recommended.

Reasons

Zero budget allocation means that the network will have to be implemented with the equipment already onsite.

One of the benefits of a peer-to-peer network is that it is cheap. It does not require additional server equipment or network operating systems (NOS) in order to be implemented. The network resources and/or services already comes shipped with the Windows 7 operating system which in this case, is already installed on the 4 computers. It also does not require a network administrator to oversee the network as each user is responsible for the management and security of their own system.

Easy to manage Peer-to-peer networks do not have the complexities of a client-server network. That is, the configuring and setting up of user accounts, access restrictions, privileges etc are all left to a network engineer. Thus when there is a fault, it is not something that can be fixed by the layman. Hence, a peer-to-peer network is best suited for users with mediocre technical expertise. There is no central point of failure in a peer-to-peer network and if a computer is down, it does not affect other uses on the network and because of its simple setup, the fault is more likely to be fixable over the phone.

Network security is primarily not one of the strong suites of a peer-to-peer network as each user is responsible for the security of their own system which in-turn contributes to the overall integrity of the network. However, in this case it should not be a problem since the data being shared does not require it and as stated by the client(Thrift Towne), security is not a concern.

What type of additional equipment would Thrift Towne have to purchase make your solution work?

A peer-to-peer network would work just fine with the equipment already onsite, however a switch would route traffic more efficiently than a hub.

As a contingency, a modem/router would also be a useful investment. A peer-to-peer network can cater for up-to 10 users before signs of latency and lag in the network starts to show. Thus having a dedicated internet connection provided by a modem/router would allow cloud storage. Users can work or access data from any mobile or computing device that has an internet connection. This in-turn solves the limitations of scalability that is inherent to peer-to-peer networks.

NB: Box offers 10GB of free cloud storage per user. 1GB is equivalent to 64,782 pages of Word Documents (Data Volume Estimates and Conversions | SDS Discovery, 2020).

What roles would you assign to each of the workstations and any other equipment recommend?

Each computer acts as either a client or a server.

What type of upgrades, if any, might the workstations require to make your solution work?

Increase in physical memory and secondary storage(paging). As the number of users that access resources on a particular workstation increases, it creates a lot of overhead. This can also be mitigated by stripping off all non-essential software and loading each workstation with bare minimum software applications required to perform their task.

With the above upgrades in hardware, this should allow us to upgrade the operating system to Windows 10. Considering that as of January 14, 2020 - Microsoft ends its support for all Windows 7 operating systems. Software and security updates will no longer be provided my Microsoft. Thus with security already a concern for peer-to-peer networks, upgrading to Windows 10 should provide an extra layer of security, better performance and a more familiar user interface rather than something archaic.

Question 2: What kind of network services will help them assess their traffic situation and provide answers about possible network expansion?

- Traffic Monitoring and Control Services (eg: NetFort LAN Guardian, Wireshark)
- Hardware Diagnostics and Failure Alert Services (eg: PRTG Network Monitor)
- Security Auditing Services (eg: Nmap, Burpe Suite, Maltego)
- Asset Management Services (eg: LANsweeper)
- Address Management Services (eg: SolarWind IP Address Manager)

Possible network expansions would include implementing a load-balancer and embracing a multi-server environment. Instead of having all the service applications hosted on a single server, the service applications are split into separate servers, each of which working autonomously, solely dedicated to the services they provide.

What types of things can they find out?

With the Traffic Monitoring and Control Services , they will find information on the traffic density of their network, and the amount of data transmission activity from each of the 3 stores. This information will also include anomalies such as the data transmission activity that are not coming from the 3 stores.

Hardware Diagnostics and Failure Alert Services Here they will find information on faulty network components. Security Auditing Services Information on network breaches will be found here and also information on what security measures the network has in place.

A**sset Management Services** They will find information on how much activity each service application is receiving. For example, in the morning the time tracking and internet application services will be busy since staff are punching in and checking their mail. In the afternoon, probably the sales and and ordering service applications would show high activity.

The most telling information they would find is that their network is clogged at the server. With only one server hosting all their service applications, coupled with their high- speed internet connections – the server is not able to efficiently process the high influx of requests that are flooding in through the high bandwidth connections. Thus by dedicating a separate server for each service application, and employing a load-balancer, the workload is effectively distributed.

What other kinds of services might they also use, given their network configuration?

- Backup and restoration services (Cobalt Iron)
- Software distribution services (allows the installation of software on a number of workstations, from one PC).
- Email services (Microsoft Exchange)

Question 3: Do you advise the Scoops chain to change its server's NOS to Linux? Why or why not?

Would advise against the migration to Linux based servers. Full advantage of the Linux based systems are in the command-line. It has a steep learning curve, kernel updates could cause certain applications to stop working. Would be difficult to troubleshoot. Drivers for new hardware may take time to surface. And installing of drivers aren't a straight forward process. May require other dependencies before installation can take place. Requires administrators that are well versed with Linux/Unix based systems.

	Windows Server 2008	**Linux Fedora**
Cost	Licensed Propriety Software	Open Source (Free)
Ease of Use	User-friendly, intuitive operations through user-interface	Steep learning curve, provides GUI but plethora of operations are available via command-line interface.
Support	Provides long term support for all versions.	Strong community support via forums, mailing lists, IRC's and telegram.
Reliability	- Drivers for hardware are easily available. - supports a large number of third-party applications. - compatible with popular Microsoft programs. - updates are seamless	- drivers for latest hardware may take time to be released. - support for third party applications and popular Microsoft programs may require extra dependencies. - some applications may not play nice with new kernel updates.
Remote Access	- uses the remote Desktop protocol. Requires configuration. - also provides VPN remote access.	- Remote access is integrated inside Terminal/shell - ssh is available by default.
Mail Service Capabilities	- Microsoft Exchange is the go to for all mail service capabilities. - allows for backup and restoration of emails - provides full administrative control over users - allows administrator to set security parameters	- setup and configuration can be a daunting task - may require expert to manage and setup - provides all the capabilities of Windows mail services, however requires configuration. - Common email application used is Exim.

Question 4: How will the process differ if the student is sending or retrieving information to or from a secure server?

The client requests a web page by typing in its URL into a web browser. The Application Layer then uses the HTTP protocol to compile a GET request which contains information about what web page the client wants, the server it is requesting it from, the version of HTTP it is using, and the clients information.

This data then arrives at the Presentation layer in the form of text(ASCII). The presentation layer then translates this text into bits and bytes, compresses it so that it takes less time to reach its destination and encrypts it in-case it gets captured en-route to its destination.

The session layer then establishes a communication session with the web server, it is responsible for keeping the session secure, re-establishing the session when it is broken and terminating the session when done. NB: the session layer protocols are no longer used for web page retrieval or file sharing in modern networks (Dean, 2013).

When the data arrives to the Transport layer, it is then segmented into small data units called segments. Each segment contains a port number and a sequence number. The port number helps to direct each segment to the correct application(web browser) and the sequence number helps to re-assemble segments in the correct order. A checksum is added to each segment to ensure that the segments arrive at their destination and arrive uncorrupted. Any segments that are lost or corrupted are resent.

These data segments are then passed to the Network Layer which is responsible for the logical addressing, path determination, and routing of the data to the destination web server. The IP protocol attaches a header to each segment. The header contains the source and destination IP's, encapsulates it into a packet and then determines the best way the packet can be routed to the destination web server.

When the packet reaches the Data Link layer, it is encapsulated into a frame. A head and a tail frame is added to the packet. The head frame contains the clients and web server's mac addresses and the tail contains a frame check sequence (FCS) for error-detection. The frame is then finally passed to the Physical Layer.

Here the Physical Layer converts the frames into signals and then transmits it over a some transmission media. The signals can either be an electrical signal in case of copper cables, light in case of fibre optic cables and radio waves. Which type of signal is generated depends on the type of media transmission used.

At the destination web server the order of the process happens in reverse. The signal is collected by the Physical Layer and passed to the Data Link Layer. The mac address and FCS is then verified and the headers and trailers stripped off the frame reviling the packet which is then passed to the Network Layer. The ip address and checksum is again verified and the headers are then stripped, passing the segment to the Transport Layer. Here the Transport layer arranges the data into the correct sequence and determines which application it is sent to by the port number. The Presentation layer performs decompression and decryption on the data and finally sends it to the Application Layer. From here the HTTP protocol takes control. The specific web page is then retrieve and the process of encapsulation starts all over again for the web page to be sent to the client.

What Application layer protocol is required?

Hypertext Transfer Protocol (HTTP) protocol is used.

Explain to the student how each OSI model layer contributes to data arriving in the correct place without errors.

As stated above, the Application layer compiles a request that contains information about which web page is specifically requested, the web server it is hosted on, version of HTTP used and other client information.

This is then sent to the Presentation layer where it is formatted, compressed and encrypted. Data is formatted to a form that is usable in the receiving end(web server). Compression allows the data to be transferred faster and encryption ensures security i.e if the data is captured en route to its destination, it can not be read.

The Session layer opens up a session with the destination server and any information that is tunneled through the session is tagged with a session ID. As there will be many existing and new sessions created, a session ID allows the Session Layer to distinguish between sessions. If a session is broken, the Session Layer reinstates the session.

The Transport Layer segments the data into smaller data units called segments. Each segment contains a port number and a sequence number. The port number helps to direct each segment to the correct application(web browser) and the sequence number helps to re-assemble segments in the correct order. A checksum is added to each segment to ensure that the segments arrive at their destination and arrive uncorrupted. Any segments that are lost or corrupted are resent.

The IP protocol in the Network Layer attaches a header to each segment creating a packet. The header contains the IP addresses of both the client and the server. The Network Layer then determines the best path to route the packet to the destination address.

When the packet reaches the Data Link layer, it is encapsulated into a frame. A head and a tail frame is added to the packet. The head frame contains the clients and web server's mac addresses and the tail contains a frame check sequence (FCS) for error-detection. The frame is then finally passed to the Physical Layer.

Here the Physical Layer converts the frames into signals and then transmits it over a transmission medium.

Question 5: Discuss Virtualization

Virtualization refers to the act of creating a virtual(rather than actual) version of something, including virtual computer hardware platforms, storage devices and computer network resources. (Virtualization,2020) . While the term may sound modern, it has been around since the 1960's primarily used on mainframe computers. Its use has broadened since its inception and one common way it is used today is to run multiple operating systems(called virtual machines) on a single computer via a hypervisor (propriety or open source software software that creates and manages virtual machines).

Some of the reasons why an organization would implement virtualization include legacy hardware; applications built for outdated hardware can still be run, sandboxing; virtual machines provide an environment to rigorously test software and facilitate its deployment and saves money; fewer machines, less electricity consumed, less space occupied.

Some of the drawbacks of virtualization include compatibility issues; not all hardware and software supports virtualization. High upfront costs; in the long run virtualization saves money, however the cost of implementation is high and may include unexpected expenses and educating staff on the management, use and troubleshooting of hypervisors. Security risks; the hypervisor runs with high privileges since it is responsible for managing the virtual machines on the host system. Thus compromising the hypervisor provides a single point of failure allowing access to all the virtual machines it currently manages.

Comparison of different hypervisor

	Virtual Box	**Vmware Workstation**	**Hyper-V**
Cost	Free	Propriety Software however, provides a trial period.	Free with conditions and limitations eg: Hyper-V server is free however comes with command line interface only. Is available on 64bit versions of Windows Pro, Enterprise and Education. Not available on Windows Home Edition I.e upgrade to Pro is required.
Supported Host Operating Systems	Cross-platform	Does not support Mac OS; however offers Vmware Fusion which provides the same virtualization features as Vmworkstation but for Mac users	Can only run on x86-64 systems running Windows
Supported Guest Operating Systems	Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD and more.	Supports more than 200 operating systems including: Windows 10,Windows 8.X,Windows 7, Windows XP, Ubuntu , Red Hat, Debian	Typically used for windows Server OS's, however also provides support for Free BSD and Linux(SUSE10,RHEL6, CENTOS6)
Support For 3D Graphics	Supports only older versions of DirectX and OpenGL – video memory limited to 256MiB	Supports Directx10.1 and OpenGL 3.3 for 3D applications – Video memory limited to 3GB	Does not support 3D Graphics
Maximum virtual hardware specs for a Virtual Machine	Upto 48 CPU's, 8 TB virtual Hard disks, 256GB of RAM.	Upto 16 CPU's, 8 TB virtual Hard disks, 64GB of RAM.	Upto 64 CPU's, 64 TB virtual Hard disks, 1TB of RAM.

References

En.wikipedia.org. 2020. Virtualization. [online] Available at: <https://en.wikipedia.org/wiki/Virtualization> [Accessed 13 March 2020].

Sdsdiscovery.com. 2020. Data Volume Estimates And Conversions | SDS Discovery. [online] Available at: <https://www.sdsdiscovery.com/resources/data-conversions/> [Accessed 14 March 2020].

Dean, T., 2013. Network+ Guide To Networks. Boston, Mass.: Course Technology/Cengage Learning.

Zacker, C., 2020. Comptia Network+ Training Kit (Exam N10-005) | Microsoft Press Store. [online] Microsoftpressstore.com. Available at: <https://www.microsoftpressstore.com/store/comptia-network-plus-training-kit-exam-n10-005-9780735662759> [Accessed 16 March 2020]

2011. *Networking Fundamentals*. Hoboken, N.J.: Wiley.