KULLIYYAH OF INFORMATION & COMMUNICATION TECHNOLOGY

CSC 2201 COMPUTER NETWORKING
SEMESTER 2, 2019/2020
SECTION 04

LECTURER
DR. **ADAMU ABUBAKAR IBRAHIM**

PREPARED BY: SAGAR FAKHRU UDDIN(1730753)

TOPIC:FILE SHARING SERVICES(APPLICATION LAYER PROTOCOL)

JIGSAW GROUP: 04

DUE
<19 July 2020 >

Chapter 1 Background

Jigsaw Group Packet Tracer Simulation Panel report

Computer Network is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network. Here is the OSI-model which has seven layers. In jigsaw group we worked with all seven layer individually cover one layer by one person. We worked our way from the bottom to the top on the chosen scenario. In jigsaw group I represent Application layer. Here I try to represent an overall view of our jigsaw group worked place.

Basically we worked on OSI model. The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between computing systems are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

The 7 Layers of the OSI Model:

Physical Layer: ***Brother Fazlul Karim*** cover the physical layer part in our jigsaw group, according to his discussion we group mate understand that this layers provides a physical medium through which bits are transmitted. The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device At the physical layer, one might find “physical” resources such as network hubs, cabling, routers, switch, network adapters or modems.

Data Link Layer: In our jigsaw group ***brother Obaid Selim*** cover the Data link layer and he decried his part with the scenario of our group, after his description we understand that the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer. The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

Network Layer: Network layer was cover by ***Brother Delamou Jacques***, he described it very clearly and nicely and what I understand I try to make it described here. The network layer is responsible for receiving frames from the data link layer, and delivering them to

their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

Transport Layer: By using simulation in packet tracer, our brother in charge of TCP/IP and UDP protocol described how transport layer works. The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

Session Layer, presentation and Application layer: In our jigsaw group I did representation of Application layer protocol. In this layer there are 3 more layer and they are session, presentation and application .The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include authentication and reconnections. Second one is presentation layer which formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer. At application layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser. The application layer identifies communication partners, resource availability, and synchronizes communication.

Introduction:

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers. There is very nice example in Netacad about this topic let me described this step by step. As you have learned, the transport layer is where data actually gets moved from one host to another. But before that can take place, there are a lot of details that have to be determined so that this data transport happens correctly. This is why there is an application layer in both the OSI and the TCP/IP models. As an example, before there was streaming video over the internet, we had to watch home movies in a variety of other ways. Imagine that you videotaped some of your child's soccer game. Your parents, in another city, only have a video cassette player. You have to copy your video from your camera onto the right type of video cassette to send to them. Your brother has a DVD player, so you transfer your video to a DVD to send to him. This is what the application layer is all about, making sure that your data is in a format that the receiving device can use. Let's dive in!

My works was on File sharing services. A file-sharing service is a type of online service that provides, mediates and monitors the transfer of computer files. It a third-party service that provides the entire platform for sharing files between different users on the same or different networks. So, a file-sharing service primarily ensures that users are able to share multiple files successfully to multiple users simultaneously. Typically, a file-sharing service is an Internet or cloud service provider that hosts a number of storage servers and application-sharing software. A file-sharing service works through a combination of application sharing and cloud storage solutions. The user, using online files, selects the file to be shared. The file is uploaded to the storage servers and can be accessed using a file access URL. File-sharing services keep track of document versions, ensuring the file is delivered securely and without any alteration or illegal copying. Such services also support sending large files, which is usually impossible with email. File sharing isn't the same as network sharing. To share a file is to send it to another device such as a computer or phone. Network sharing shares a network connection so that nearby devices can access network resources.

Characteristics of File sharing services:

There is several character of any file sharing services. Here I try to describe some of them.

1: Simple, secure sharing of business data: Enterprise grade, high performance file transfer servers enable your remote workforce to securely share and access files from anywhere. This is achieved from FTS solutions that support an array of protocols including FTP/S, SCP, SFTP, WebDAV, HTTP/S.

2: Remote security and administration: Whether you're a small business or a fortune 500 company, effective File Transfer Servers provides user management and permissions that are flexible enough to cater to any environment. FTS solutions should provide your network with the ability to manage users or groups with built-in directory or by connecting to your Active Directory. This includes the ability to manage permissions to all files and locations with fine-grained policies

3: Reliability from trace-ability: Effective FTS solutions let your IT staff watch every file transfer to and from your network. This provides the ability to track every user's remote actions and see which files they have remotely accessed. Ideally this capability should operate in real-time, and includes notification of any event happening within your network

.4: End to end remote security: Last but not least, an effective FTS keeps your data safe. This includes secure authentication across browsers and within the native clients which discourages unauthorized access to your network. This security should also include a multi-factor authentication.

There are arguably several different flavors of file transfer servers on the market. Few, however, have ease of use security, remote capabilities and reliability as core features.

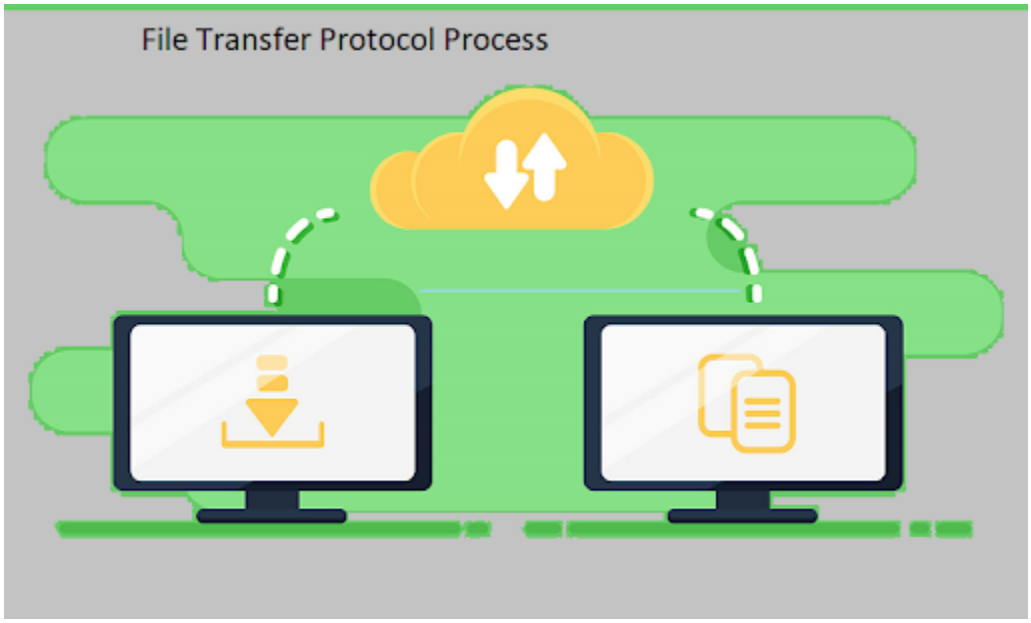
As long as your network administrators use these key criteria when selecting an FTS solution, their network's back-end will always have a robust and secure backbone.

Types/Categories:

There are different types of file sharing services. Here those are.

File transfer protocol programs (FTP):

File transfer protocol is one of many different protocols that dictate how computers behave on the internet. Other such protocols include the Hypertext Transfer Protocol (HTTP), the Internet Message Access Protocol (IMAP), and the Network Time Protocol (NTP). FTP enables computers on the internet to transfer files back and forth, and is an essential tool for those building and maintaining websites today The most common file transfer system on the internet to date is known as the File Transfer Protocol or FTP. FTP is used to access or edit files among a set number of users with a password. The users can then gain access to the files shared from an FTP server site. Many FTP sites offer public file sharing or allow users to view or download files using a public password.

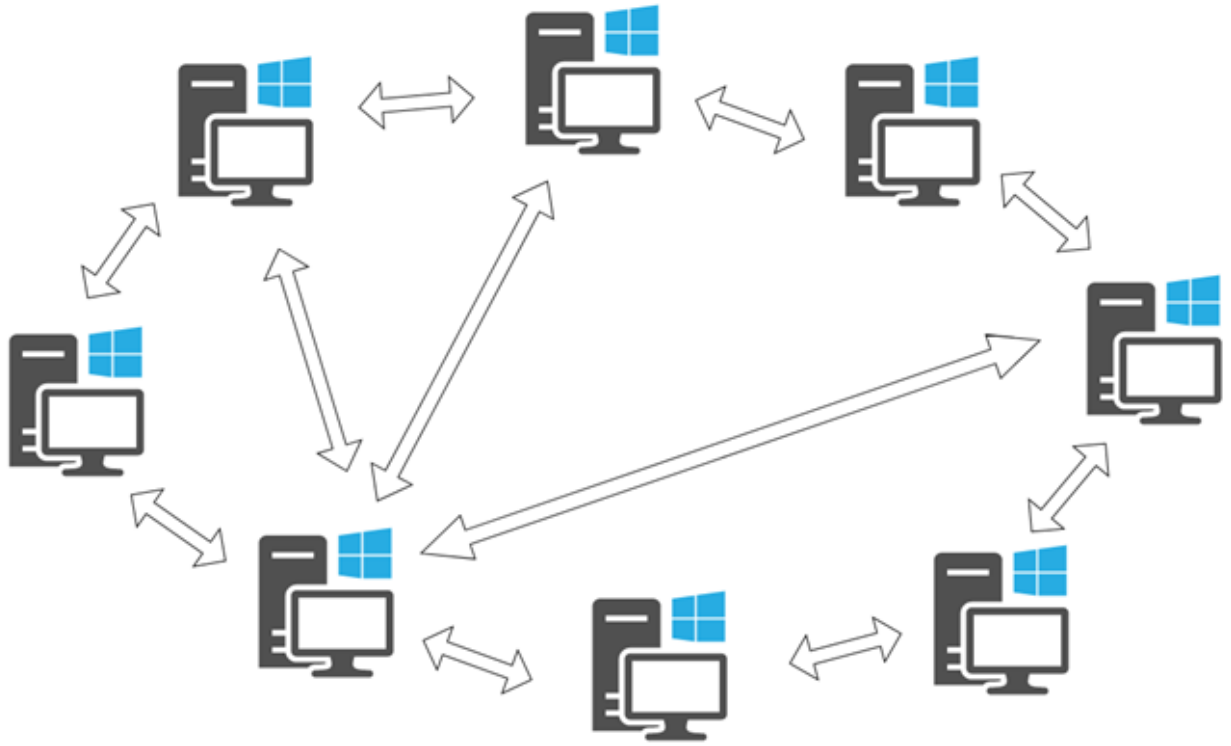


In order to use FTP, a user must first download an FTP client (or access an FTP client through a web browser). A client is the software that will allow you to transfer files.

Example: Cyberduck, Firefox

Peer-to-peer networks:

Peer-to-peer networking involves computer hardware and software to communicate without the need for a central server. This type of file sharing indicates the direction of digital files over a p2p network where the files are located on one's computer and shared with other members rather than on the main server. Peer-to-Peer File Sharing systems are no longer just a new fad technology. They have become ingrained in our Internet culture. You have to remember that just because Samantha is hosting a file that she says is a video of the Olympics, that doesn't mean that it really is the Olympics. It could be some sort of Trojan or malware. Nowadays, many botnets are built using Peer-to-Peer File sharing systems.



Most corporate organizations do not use Peer-to-Peer File sharing systems for business purposes. So the easiest way to protect against abuse is to take steps to prevent their usage within your organization. You can do this by blocking access to any external servers or services that are used to control the peer-to-peer software. You can also internally block any ports that are used by peer to peer system to talk to each other.

Example: Instant Messaging services such as Skype are a type of p2p network

Removable storage media:

This involves anything that can be removable from a device or computer. The user can transfer or insert files from their device onto the removable storage media and then physically hand it to whomever they would like to share the files with.

These can include an FTP server for security purposes, asking for a valid login and password from others to allow access.

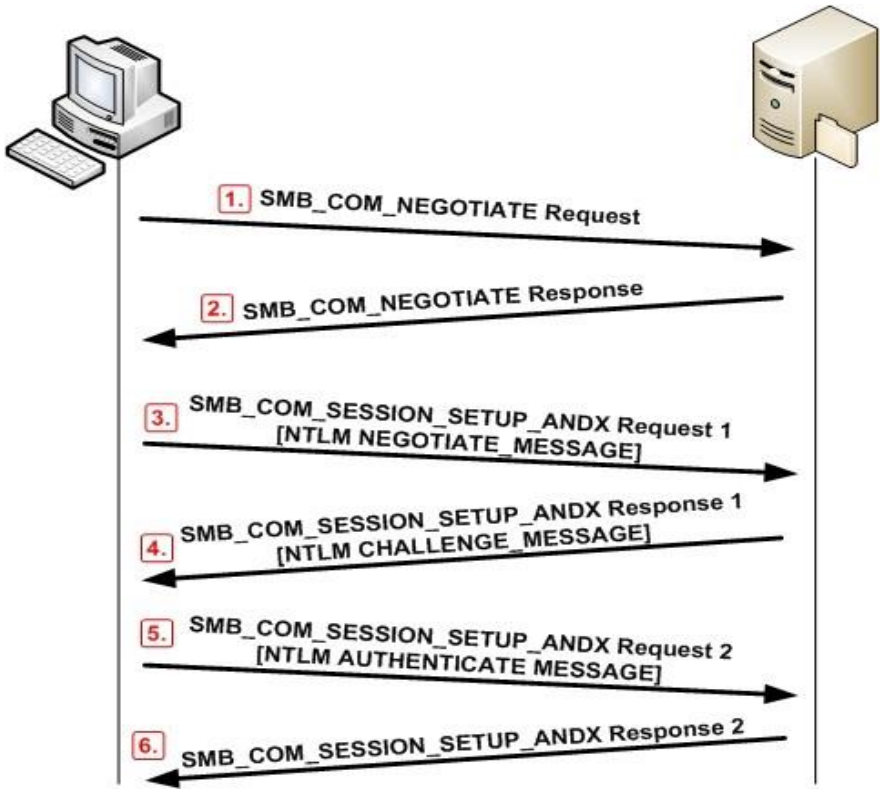
Example: Memory sticks, optical discs, memory cards and removable hard disks

Online file sharing services: Online file sharing services include web services that allow users to store or share data on the internet for personal or professional use. One member may upload photos, documents, PDFs, etc. to an online file sharing platform which allows others to download these files using the same platform.

Example: Dropbox, Resilio, Tresorit

The Server Message Block Protocol (SMB protocol): It is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network. It can also carry transaction protocols for inter process communication. The SMB protocol enables an application -- or the user of an application -- to access files on a remote server, as well as other resources, including printers, mail slots and named pipes. Thus, a client application can open, read, move, create and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request. The SMB protocol is known as a response-request protocol, meaning that it transmits multiple messages between the client and server to establish a connection. An early dialect of the SMB protocol, Common Internet File System (CIFS), gained notoriety as a chatty protocol that bogged down wide area network (WAN) performance due to the combined burdens of latency and CIFS' numerous acknowledgments.

The SMB protocol operates in Layer 7, also known as the application layer, and can be used over TCP/IP on port 445 for transport. Early dialects of the SMB protocol use the application programming interface (API) NetBIOS over TCP/IP, or legacy protocols such as the Internetwork Packet Exchange or NetBEUI. Today, communication with devices that do not support SMB directly over TCP/IP requires the use of NetBIOS over a transport protocol, such as TCP/IP



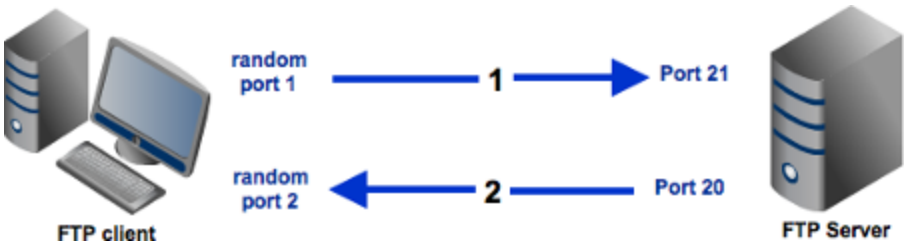
.

Implementation/Implication (20 Marks):

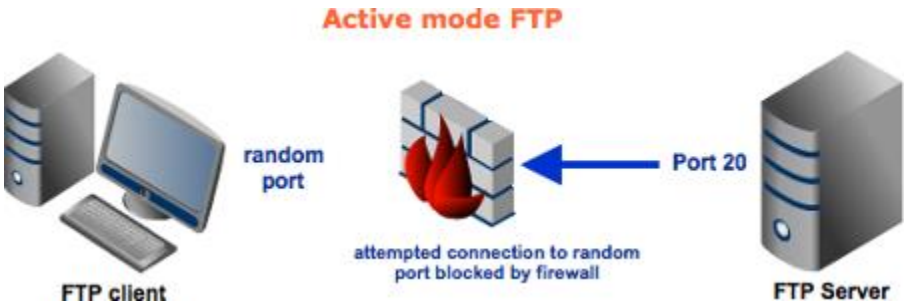
Usually implementation means realization of an application, or execution of a plan, idea, model, design, specification, standard, algorithm, or policy. So, here I will describe the application of different file sharing services specially FTP and SMB.
Application of File Transfer protocol: FTP connection needs two parties to establish and communicate on the network. To do that, users need to have permission by providing credentials to the FTP server. Some public FTP servers may not require credentials to access their files. The practice is common in a so-called anonymous FTP.

There are two distinct communication channels while establishing an FTP connection. The first one is called the command channel where it initiates the instruction and response. The other one is called a data channel, where the distribution of data happens.

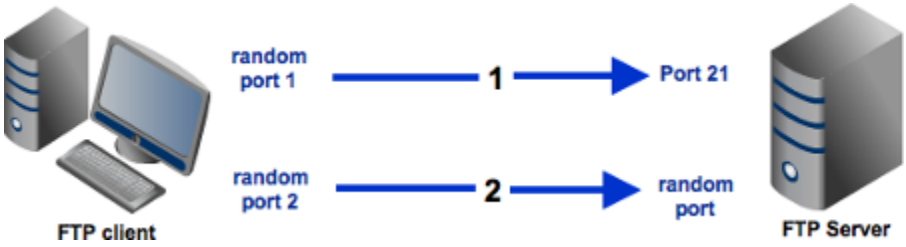
To get or transfer files, an authorized user will use the protocol to request on creating changes in the server. In return, the server will grant that access. This session is known as the active connection mode.



The distribution in active mode might face a problem if a firewall is protecting the user's machine. The firewall usually does not allow any unauthorized sessions from an external party.



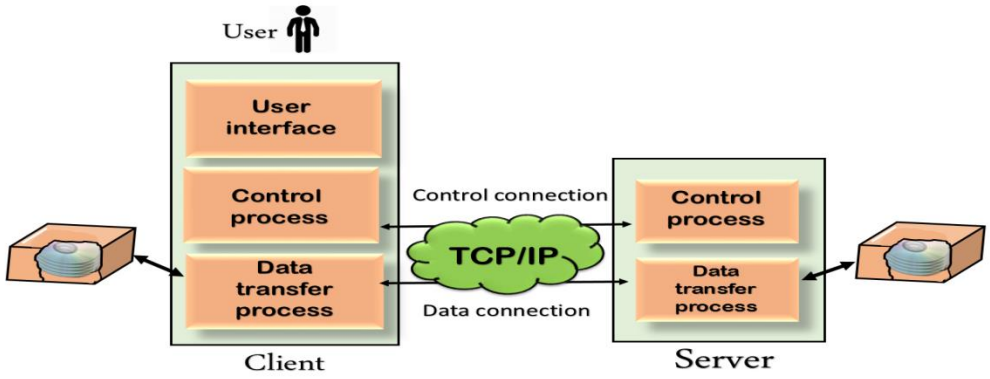
The *passive* mode is used if that issue occurs. In passive mode, the user establishes both command and the data channel. This mode then asks the server to *listen* rather than to attempt to create a connection back to the user.



There are three approaches on how to establish an FTP connection. A very simple method is using a command line FTP, such as using Command prompt for Windows or Terminal in Mac/Linux. Developers still use it today for transferring files using FTP.

A user also can use a web browser to communicate with the FTP server. A web browser is more convenient when users want to access large directories in the server. Yet, it's often less reliable and slower than using a dedicated FTP program.

Today, the most common practice to use FTP, especially for a web developer, is by using an FTP client.



An FTP client provides more freedom compared to the command line and web browser. It is also easier to manage and more powerful compared to the other methods.

There are also more features available whilst using such a client. For example, it allows users to transfer large files and use the synchronizing utility.

Implementation of Server message Block: The SMB protocol enables an application -- or the user of an application -- to access files on a remote server, as well as other resources, including printers, mail slots and named pipes Thus, a client application can open, read, move, create and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request.

The SMB protocol is known as a response-request protocol, meaning that it transmits multiple messages between the client and server to establish a connection.

Although its main purpose is file sharing, additional SMB Protocol functionality includes the following:

- Dialect negotiation
- Determining other SMB Protocol servers on the network, or network browsing
- Printing over a network
- File, directory, and share access authentication. File and record locking
- File and directory change notification
- Extended file attribute handling
- Unicode support
- Opportunistic locks.

Microsoft Windows operating systems since Windows 95 have included client and server SMB protocol support. Samba, an open source server that supports the SMB protocol, was released for UNIX systems.

A client and server may implement different variations of SMB, which they negotiate before starting a session.

Chapter 2: Literature Review

Eligibility criteria (20 Marks):

The following links gives me a brief description about the file sharing services and protocols.

I chose this link for a brief details about FTP and this link described it nicely https://www.cloudwards.net/what-is-ftp/, it was published *Branko and the writer was Vlajin,file last updated on 29 march 2020.* I visit those link for more details about File transfer protocolshttp://www.pcwebopedia.com/TERM/F/FTP.html,http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF#page=24, http://www.krollontrack.com/glossaryterms.

I go those links for Understanding Server Message Block protocol:https://en.wikipedia.org/wiki/Server_Message_Block#SMB_2.1, https://www.samba.org/cifs/docs/what-is-smb.html,http://images.slideplayer.com/22/6382552/slides/slide_62.jpg,http://slideplayer.com/slide/6851808/,https://www.samba.org/cifs/docs/what-is-smb.html,http://wesmorgan.blogspot.com/2011/10/data-throughput-with-http-smb-and-nrpc.html.

Those entire links described the file sharing services very clearly and logically and written in English. And these papers are easier to understand comparing tom other reports. It is also free in Google and more convenient. From those first reports I came to know about details about file transfer protocol and there a lot a researcher put their opinion about file sharing services.

Information resources:

1) http://www.pcwebopedia.com/TERM/F/FTP.html,

Fenwick & West LLP, FWPS Citing Webopedia Computer Dictionary,

Published on: eDiscovery Terminology (11/6/2005).

2) All about File sharing services: IEEE.org

Published in: IEEE Systems Journal (Volume: 12 , Issue: 1 , March 2018)

Page(s): 473 - 484

Date of Publication: 07 July 2016

ISSN Information: INSPEC Accession Number**:** 17649982

DOI: 10.1109/JSYST.2016.2580299

Publisher: IEEE

3) https://en.wikipedia.org/wiki/Server_Message_Block#SMB_2.1

Publish on: Wikipedia.com

4) http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF#page=24

Writer: Fenwick & West LLP

Publish on: Citing Applied Discovery's Glossary

Published date: 11/6/2005

4) http://www.krollontrack.com/glossaryterms

Witter: Kroll Ontrack,

Published on: Glossary *of Terms*,

Search criteria:

The search criteria vary depending on the object for which you are searching. Examples of search criteria include the name, created date, last updated date, and lifecycle state of the object.

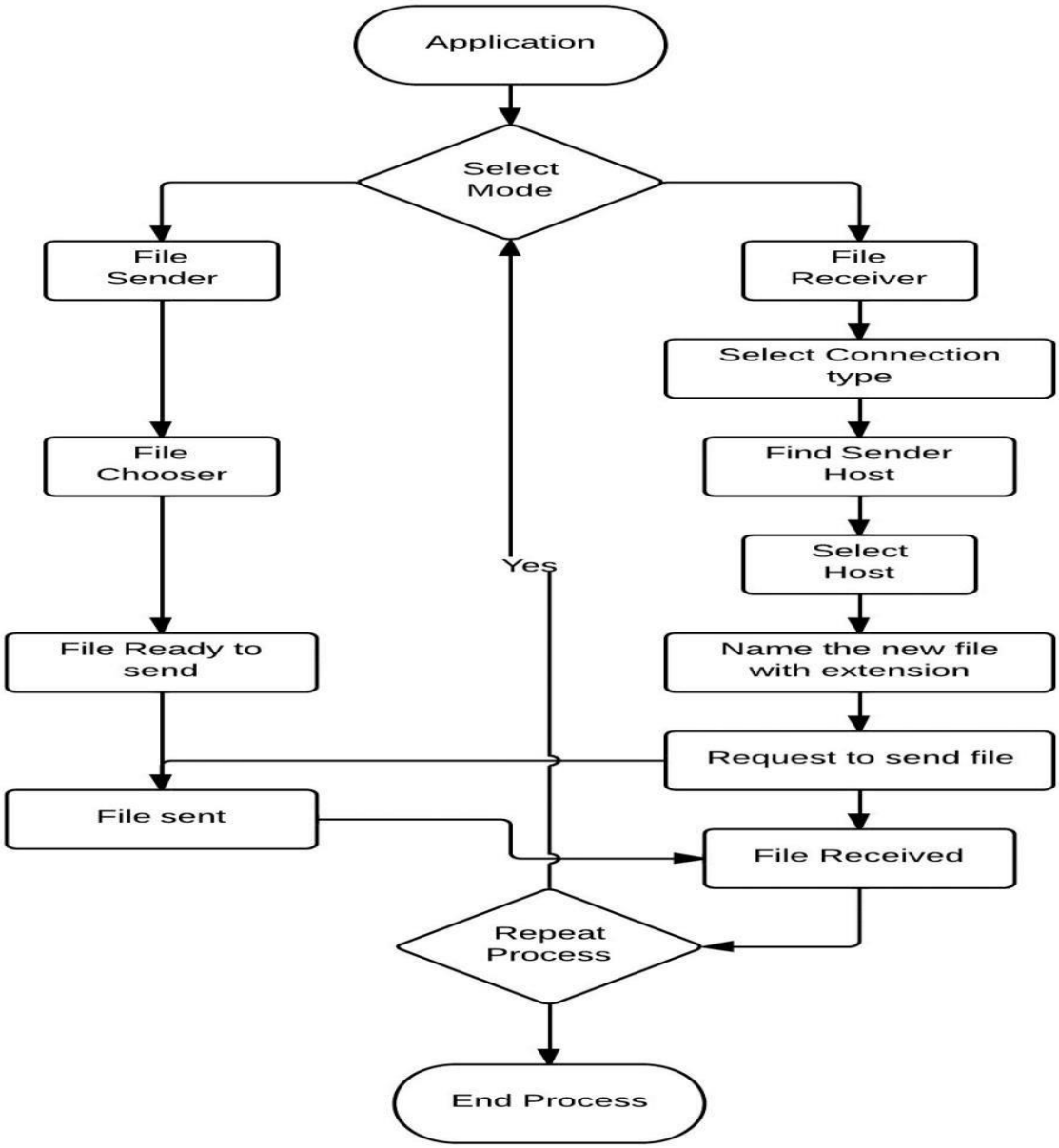
For instance: Firstly, I attempt to look by composing document sharing administrations in Application layer convention. At that point I saw a huge amount of theme has showed up. At that point I search by document sharing convention. In any case, I didn't get adequate data which I was searching for.). I use some of those Keywords: File Sharing service, file transfer protocol, characteristics of file sharing services, server message block. At that point I compose document move convention and server message square independently in various pursuit. I likewise use what's the need of those documents sharing convention. Search techniques were assessed against the best quality level set, just as an autonomous arrangement of CRTs remembered for past methodical surveys. When performing writing looks for an orderly audit it is critical to utilize a wide scope of assets and looking through techniques to distinguish every single pertinent examination. The three most significant databases to consider are MEDLINE (PubMed through LHL), Embase, and the Cochrane Central Register of Controlled Trials (CENTRAL). MEDLINE, doesn't sufficiently catch the writing for a deliberate audit [30, 31]. Looking through more than one database is quite often vital and is a significant advance all the while. The peruser needs this data to evaluate the nature of the survey. MEDLINE, and the name of the host alludes to the stage on which the database is given, for example, Ovid, Silver Platter, and EBSCO. The date a pursuit was directed ought to incorporate the month, day, and year. A long time secured by the hunt is those years the inquiry was constrained to or the years secured by the database if no restrictions were applied.
Sources for finding databases:

- UAB Libraries Databases
- Cochrane Handbook, Bibliographic databases
- ULRICHSWEB - search journal titles in the relevant subject area and check the *Abstracting & Indexing Databases* listed for that journal.

Synthesis of the results of the previous research studies reviewed (40 Marks):

File sharing is the practice of distributing or providing access to digitally stored information, such as computer programs, multimedia (audio, images and video), documents or electronic books. It may be implemented through a variety of ways. Either by using client server or by peer to peer methodology file sharing is conducted. Nowadays sharing files is a major part of the network usage. Files are being shared between multiple of users and thus creating a load on the network. Thus optimizing file sharing is important for the network to be efficient. The objective of this thesis was to study different file sharing algorithms and chose one that would create an optimized file sharing solution for a

local area network using peer to peer method. Among different optimizing algorithms Ant Colony Optimization (ACO) was chosen and compared other available algorithms. Based on that, we have tried to develop a file sharing application within a local area network using the concept of peer to peer file sharing methodology named FAaNS. Thus this research gives an overview of the ACO algorithm, reasons behind choosing ACO and then finally the development of the file sharing application which will detect the nodes that have the files for sharing and will share the files optimally between nodes. This flowchart makes my understanding on research paper one more easy, that's why I shared it here also because this is main concept of this paper.



In second research the author tries to make understand about more details on FTP. This paper has been presented at the Computer Network Protocols Symposium, held in Liege (Belgium) in February 1978 and organized by the University of Liege. The permission to reprint this paper is gratefully acknowledged. This paper presents a File Transfer Protocol (FTP) which can be used to transfer files between heterogeneous computer systems connected by a communication network. The basic mechanisms as well as the set of protocol commands and responses have been defined in the context of a general architecture. A simplified architecture, to help first implementations is also proposed. This can easily be extended to the more general one. The proposed protocol is completely compatible (even identical in some areas) with the currently proposed Virtual Terminal Protocol (VTP). A file transfer protocol has been defined which provides the necessary mechanisms to transfer a file safely from one place to another over a network. Conversions between file structures can be performed so far only on a limited number of "standard" structures (e.g. sequential text files). Otherwise file structures must be compatible and transfer be performed in transparent mode. File identification problems have not been touched. They are considered to be more general problems, belonging to the area of a network job control language. Local conventions only are used here to identify a file.

Chapter 3: Analysis and Interpretation

The goal of your part in the chapter (File sharing services):

It wasn't too long ago that the only way you could collaborate with others on a project was to schedule physical meetings, and bring everything along with you. And if you didn't get everything accomplished in that meeting, you had to plan *another.* And *another* until the project was complete. Now, thanks to modern online file sharing and collaboration methods, receiving opinions and answers from others on the work is possible without ever leaving your desk.

File sharing allows a number of people to use the same file or file by some combination of being able to read or view it, write to or modify it, copy it, or print it. Typically, a file sharing system has one or more administrators. Users may all have the same or may have different levels of access privilege. A file-sharing service primarily ensures that users are able to share multiple files successfully to multiple users simultaneously. Typically, a file-sharing service is an Internet or cloud service provider that hosts a number of storage servers and application-sharing software. A file-sharing service works through a combination of application sharing and cloud storage solutions. The user, using online files, selects the file to be shared. The file is uploaded to the storage servers and can be accessed using a file access URL.

Anytime, anywhere, with anyone: Storing files on any file sharing services makes it easy to share files with everyone such as people in the company, people in the office, people moving in the field service, people working in the teleworking and satellite offices, and even business partners.

It can protect confidential documents. File sharing services provide several mechanism to protect confidential documents such as password-protected download link to pass the file, set the access period of the folder, insert the acquisition time and the name of the acquired

Tools used for presentation of your part in the chapter (20 Marks):

This means which ways are used among text, audio, video, image, table, figures, drawings animations and display etc have been used for my part in the chapter. For my part there is no video part in the lesson. It is consisting of text, table, figures, and image. All the required elements as well as additional justification were given already. I use figures, table, and text to make easy understanding. For analyzing file sharing services, I took help form Cisco Packet tracer, Netacad, Internet, Some websites, Microsoft word.

Strategic presentation of your part in the chapter (20 Marks):

Strategies are the details action-oriented items that we implement to achieve the objectives. Strategic presentation of my part in the chapter means how Netacad present is my part. In my topics it is File transfer protocol and server message block, Netacad gives short description of around 15 lines with some pictures. The best thing in Netacad on this topics the description by image .they described how FTP works and how sever message block work. The most important thing is the two types of connection in file transfer protocol are control connection which connected by using TCP port 21 and other one data connection which connected by TCP port 20. The data passing in the network strategy is designed to base on which type of data sending, location, IP address. In Netacad FTP and SMB is basically described by using text, explaining figure. It can be said Netacad is presenting my part by text explaining image or image explaining text. There are numerous strategies as well as the justification. Such as: video explaining text or text explaining video, table explaining text or text explaining table, figure explaining text or text explaining figure, animations explaining text or text explaining animations. For my part strategic presentation include the description of Multiple Separate Communications using text to image.

Interpretation (40 Marks):

File sharing has caused many people to become more efficient. Previously, files were only able to be shared by physically carrying the file around in some manner. Whether this meant using a paper file or using a floppy disk or flash drive, the file had to be on your person in order to be usable. With file sharing, worrying about carrying something on your person is a thing of the past. File sharing enables users to place files on a single network and be able to access these files from anywhere. Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may

have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Since many people now carry around devices that are not able to access certain drives, file sharing came right in time. Smart phones and portable internet devices, like eReaders that can access the internet, are able to pull and access files without the headache of worrying about how to gain access through physical means. For many people, this means the world is now a lot more portable and lightweight.

With the high points of the files, sharing has come many different controversies. One thing that people should remember with file-sharing networks is that it is possible, like with any other internet ability, to be hacked into. Since file-sharing networks can carry sensitive information, it is important to remember online safety tips. Be sure not to give your password to anyone else, especially if you use the file-sharing network for personal files. Also, be aware of who you let into the network. Do not allow the unknown individual to access a -sharing network with personal information. This can lead to further hacking or even worse for those who are involved. Make sure that the network is only accessible by those you trust. Although there are different positive points to file-sharing programs, such as Citrix ShareFile, there are also negatives that come along with the programs as well.

Keep in mind that there can always be glitches when dealing with products that operate off a network or online. There could be possible downtime, which can lead to issues accessing your items. Keep in mind that these things can happen temporarily. The best thing to do during any lagging or downtime issues it to get in touch with those who run your sharing network to diagnose the problem.

Though there are some negatives to file sharing, using a file share program is still a good idea for all. Remember to follow the general rules to keep yourself safe online, so that you do not run into many issues with your file sharing hosting.