International Journal of Research
Available at
https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

Computer Networks Configuration and Security in TCP/IP Networks

Jawad Yahya Kadhim
University POLITEHNICA of Bucharest, Faculty of (FILS) Department of Engineering in Foreign Languages, Engineer, Ministry of water resources /Iraq

1.0 Abstract

A simple LAN Network in Packet Tracer version 6.3 has been created and configured, such that there is a connection throughout the entire network and also a basic secure connection against anyone who tries to breach it. The configurations and the network particularities are presented in the paper.

Packet Tracer is a program made by Cisco Systems that permits users to build network topologies. The software allows users to simulate the configuration of Cisco routers and switches through a simulated command line interface. Packet Tracer uses a drag and drop user interface. It allows users to add and remove simulated network devices.

Another option is the use of Omnet++ in order to simulate a network, which is extensible, modular, based on C++ simulation library components and frameworks.

A peer to peer application has been created where there exists a group of friends where, when someone sends a message, everyone in that group receives the message. The roles change. Sometimes a computer or a mobile phone will be a server, when the rest of the devices will be clients and sometimes the same device will be a client and one of the rest will be the server. in The peer's exchange secret messages, like in a chat.

The client should register with his/her username to the application. Any user has a username and a password. A user can "be friend" with other users. A list of his/her friends will appear on the user's screen after logging in. A user can send messages which get automatically encrypted when they are sent to the receiver. The receiver will have the option to decrypt the message which he/she received. For encryption, the Caesar cipher was used.

The application that was designed uses TCP/IP communication to connect several devices to a server. TCP is a connection-oriented protocol. In order to do communication over the TCP protocol, a connection must first be established between the pair of sockets. While one of the sockets listens for a connection request (server), the other asks for a connection (client). Once two sockets have been connected, they can be used to transmit data in both (or either one of the) directions.

1.1. Introduction

In the early years of their existence, computer networks have been used by researchers in universities for sending electronic mail (e- mail service) or to allow multiple connections to a server by officials and corporations tso share printers. In these circumstances, the security issue did not attract too much attention. Therefore, most protocols used then doesn't have the ability to encrypt data (ex. Telnet, RIP, etc.).

"Computer networks are part of the World Wide Web, shared applications and storage servers, printing systems. They use email and real time messaging tools. Application communications protocols are layered, meaning carried as payload over

other more general communications protocols" [1].
With time, people saw the tremendous potential of computer networks and how many benefits it can bring: people can share knowledge, send photos, can keep in touch with other persons, can even pay their bills or to place orders online, just stand in front of the personal computer. But these benefits bring a series of negative consequences. According to Kaspersky Security Bulletin number of attacks based on browser (browser-based attacks) - such as phishing, Java exploits, cross-site scripting, etc., increase in 2016 from 946,393,693 to 1,595,587,670.
When people use the Internet to pay bills, to purchase various products, to post personal photos or to send messages to others, in addition, they use simple passwords on their accounts that can be easy to guess, then network security becomes a big potential problem. As medicine is trying to prevent further disease while treating their current one's computer security trying to prevent potential attacks while minimizing the effects of the current attacks.

1.2. Network infrastructure

The network consists collection of systems connected to each other through any communication channel. The communication channel may consist of any physical "wired" or logical "wireless" medium and of any electronic device known as node. Computers and printers are some of the examples of nodes in a computer network and if we talk about the telecommunication network these may be mobile phones, connecting towers equipment and main control units. The characteristic of a node in the network is that; it has its own identity in the form of its unique network identification.
The main functionality of any network is to divide resources among the nodes. The network under certain rules finds resources and then shares it between the nodes in such a way that authenticity and security issues are guaranteed.
The rules for communication among network nodes are the network protocols. A protocol is the complete set of rules governing the interaction between two systems. It varies for varying different working assignments between nodes communication [2].

1.2.1 ISO / OSI model

In 1997, The International Standard Organization (ISO) designed a standard communication framework for heterogeneous systems in network. As per functionality of communication system in open world, this system is called Open System Interconnection Model (OSI). The OSI reference model provides a framework to break down complex inter-networks into such components that can more easily be understood and utilized. The purpose of OSI is to allow any computer anywhere in the world to communicate with any other, as long as both follow the OSI standards [3].
The OSI reference model is exploited into seven levels. Every level in OSI Model has its own working functionality; these levels are isolated but on the other hand cascaded to each other and have communication functionality in a proper flow between them. With reference to above standard communication framework, this set of layers known as OSI layers. Functionality of each layer is different from each and each layer has different level and labels [3]. (Shown in table 1.1)

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Table 1.1: OSI Reference Model [3]

1.3.1. Security services

From the security objectives perspective, we know four principle destinations which are perceived by any creator in the field. Each of these administrations can be actualized at various levels of the OSI or TCP/IP model design. To guarantee the security of a level we can consolidate one or more administrations which thusly can be made out of a few instruments by applying AAA (authorization, authentication, accounting).

The first objective is Authorization through data privacy, or guaranteeing that data stays open just to approved gatherings in such manner. It is the most seasoned object of cryptology. Among who don't know is still boundless sentiment that the idea of cryptography is synonymous with privacy, I am certain that is defective in light of the fact that cryptography bargains and giving numerous different destinations, which will be recorded underneath, and which have no association with mystery data. Respectability alludes to guaranteeing that data has not been modified amid transmission or by a conceivable rival.

Authentication with two unmistakable directions: substances confirmation and data validation. Confirmation of substances alludes to the presence of an insurance of the personality of a specific element. Confirmation data identifies with assurance the wellspring of the data - naturally it sureties and trustworthiness of data Authentication is for the most part firmly identified with a worldly component, clearly a put away data can be subjected to a respectability test to figure out if or not adjusted but rather can't be subjected to a trial of validness if there is not a guarantee.

In reference to computerized security, nonrepudiation intends to guarantee that an exchanged message has been sent and got by the gatherings asserting to have sent and got the message. Nonrepudiation is an approach to ensure that the sender of a message can't later deny having sent the message and that the beneficiary can't deny having gotten the message.

Accounting is done for billing or security purposes of the requested services.

1.3.2 Specific security mechanisms

OSI security architecture enumerates eight specific security mechanisms:

Encoding is utilized either to ensure the privacy of information units and activity stream data or to backing or supplement other security instruments.

Digital signature mechanisms are utilized to give an electronic simple of manually written marks for electronic archives. Like transcribed marks, computerized marks must not be forgeable; a beneficiary must have the capacity to check it, and the underwriter must not have the capacity to reject it later. In any case, not at all like written by hand marks, advanced marks fuse the information (or the hash of the information) that are agreed upon. Distinctive information along these lines result in various marks regardless of the possibility that the signatory is unaltered.

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

Access control mechanisms utilize the confirmed personalities of principals, data about these principals, or abilities to decide and authorize access rights. On the off chance that a main endeavors to utilize an unapproved asset, or an approved asset with an inappropriate sort of access, the entrance control capacity push aside the endeavor and may moreover report the occurrence for the reasons for creating a caution and recording it as a major aspect of a security review trail. Access control instruments and the qualification between optional access control and required access control have been broadly treated in the PC security writing referenced in the introduction. They are normally spoken to as far as subjects, questions, and get to rights. A subject is an element that can get to objects. It can be a host, a client, or an application. Accordingly, it is an equivalent word for important. An item is an asset to which access ought to be controlled. An article can go from a solitary information field in a document to a huge system. Access rights determine the level of power for a subject to get to an item, so get to rights are characterized for every subject-object-pair. Case of UNIX access rights incorporate read, compose, and execute.

Data integrity mechanisms are utilized to ensure the uprightness of either single information units and fields inside these information units or groupings of information units and fields inside these arrangements of information units. Note that information respectability instruments, all in all, don't secure against replay assaults that work by recording and replaying already sent legitimate messages. Additionally, securing the trustworthiness of a succession of information units and fields inside these information units for the most part requires some type of unequivocal requesting, for example, grouping numbering, time-stamping, or cryptographic tying.

Authentication exchange mechanisms are utilized to confirm the asserted personalities of principals. As per ITU-T referral, we utilize the term solid to allude to a validation trade system that utilizations cryptographic strategies to secure the messages that are traded, and powerless to allude to a verification trade instrument that does not do as such. By and large, feeble validation trade systems are powerless against uninvolved wiretapping and replay assaults.

Traffic padding mechanisms are utilized to secure against activity examination assaults. Movement cushioning alludes to the era of spurious occasions of correspondence, spurious information units, and spurious information inside information units. The point is not to appear if information that are being transmitted really speak to and encode data. Subsequently, movement cushioning components must be helpful on the off chance that they are ensured by some kind of an information privacy administration.

Routing control mechanisms can be utilized to pick either powerfully or by prearrangement particular courses for information transmission. Imparting frameworks may, on recognition of persevering latent or dynamic assaults, wish to teach the system administration supplier to build up an association through an alternate course. Correspondingly, information conveying certain security marks might be taboo by a security approach to go through specific systems or connections.

Notarization mechanisms can be utilized to guarantee certain properties of the information conveyed between two or more substances, for example, its honesty,

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

inception, time, or goal. The confirmation is given by a trusted outsider (TTP) in a tried way.

2 Security ciphers

2.1 Problem information

A peer to peer application has been created where there exists a group of friends where, when someone sends a message, everyone in that group receives the message. The roles change. Sometimes a computer or a mobile phone will be a server, when the rest of the devices will be clients and sometimes the same device will be a client and one of the rest will be the server. in The peer's exchange secret messages, like in a chat.

The client should register with his/her username to the application. Any user has a username and a password. A user can "be friend" with other users. A list of his/her friends will appear on the user's screen after logging in. A user can send messages which get automatically encrypted when they are sent to the receiver. The receiver will have the option to decrypt the message which he/she received. For encryption, the Caesar cipher was used.

2.2 General views

The application that was designed uses TCP/IP communication to connect several devices to a server. TCP is a connection-oriented protocol. In order to do communication over the TCP protocol, a connection must first be established between the pair of sockets. While one of the sockets listens for a connection request (server), the other asks for a connection (client). Once two sockets have been connected, they can be used to transmit data in both (or either one of the) directions.

In order to start the application, the Server interface is firstly opened to start the outgoing server as it can be seen in Figure 4.1.

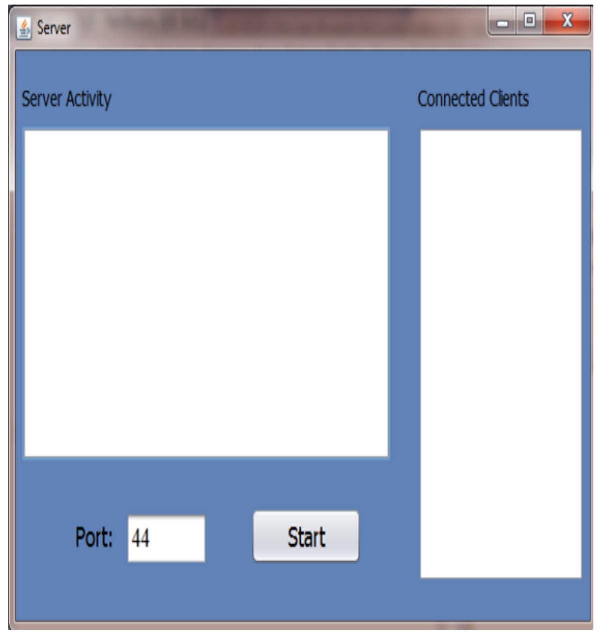
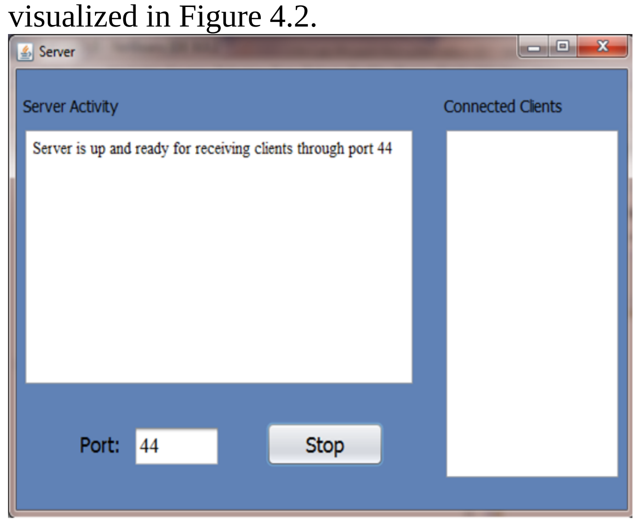


Figure 4.1: Server graphical user interface

The default address will be the computer IPv4 address, "localhost" while the port may be set to any available port. Afterwards the Start button is clicked and the Server will be open for connections.

After the server has started, a message will be displayed in the "Server Activity" dialog box, which will be either: "Server is up and ready for receiving clients through port X" or "Port X is not available". This can be visualized in Figure 4.2.



p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

Figure 4.2: Server establishment

To demonstrate that the connection actually works, two server frames can be opened and the connection to the same port can be tried, as in Figure 4.3.

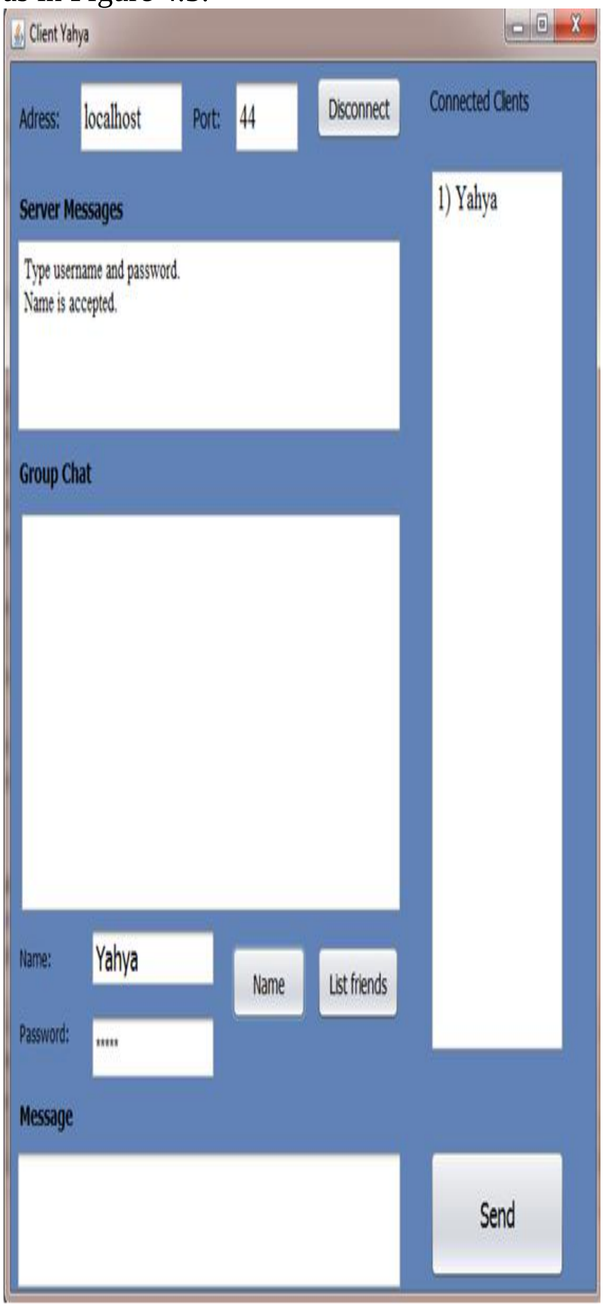


Figure 4.4: User graphical interface

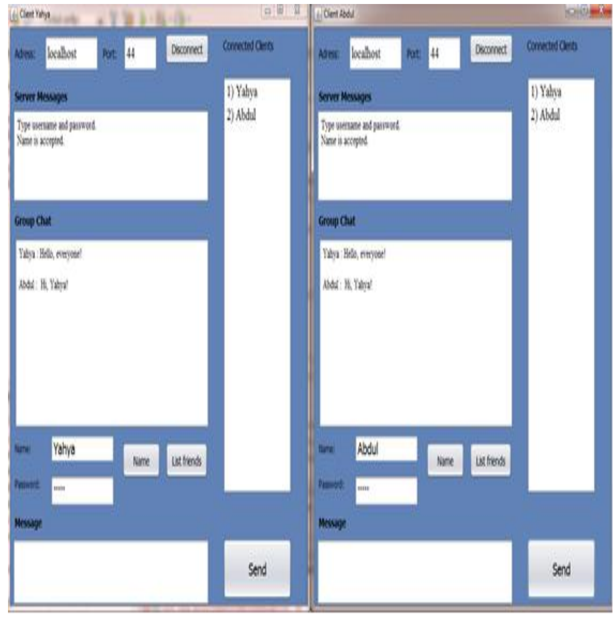


Figure 4.6: Chat room

3 Implementation

3.1 Server Implementation

The Server part has been implemented in two stages: The Server class and its Graphical User Interface.

First of all, in order for the application to be a viable chat, a TCP/IP connection was used with Java sockets. The connection starts on a Button Action Performed from the GUI that sends a request to the Server class to start the connection as coded in Figure 4.7.

```
int port;
try {
      port = Integer.parseInt(textPort.getText().trim());
}catch(NumberFormatException e) {

    textServer.append("Invalid port number\n");
    return;
 }

server = new Server( port , this );
new ServerRunning().start();
buttonStart.setText("Stop");
textPort.setEditable(false);
```

Figure 4.7: Running a Server instance

In the Server class, if the start () method is called it will try to open a new Server Socket and while the server is up it will update the server information as well as display a message to the user (see Figure 4.8).

```
public class Server{

    private final ArrayList<DataOutputStream> socketList;
    private final ArrayList<String> connectedClientsNameList;
    private final ArrayList<MyConnection> connectionsList;
    private ServerSocket serverSocket;
    private Socket clientSocket;
    private final int port;
    private final ServerGUI gui;
    private boolean serverIsUp;

    Server( int port , ServerGUI gui ){
        socketList = new ArrayList<>();
        connectedClientsNameList = new ArrayList<>();
        connectionsList = new ArrayList<>();
        this.port = port;
        this.gui = gui;
    }
```

Figure 4.8: Server class fragment

Inside the Server class is defined an inner class Connection that handles the connection data (in Figure 4.9) by taking the client socket, the socket list, the connected users list as well the input/output clients and rendering the data.

4. Encryption

For the message transmission, it was used an encryption method. When the message is sent, it is encrypted and when the user receives it, it is decrypted. The method of encryption is Caesar Cypher, used with an offset of 4 (all bits are shifted with 4 position and, when the string is decrypted, the bits are shifted back to their original place see figure 5.13). This ensures that the message is secret across the transmission line. The encrypted messages are printed to the standard output to prove the correctness of the encryption method.

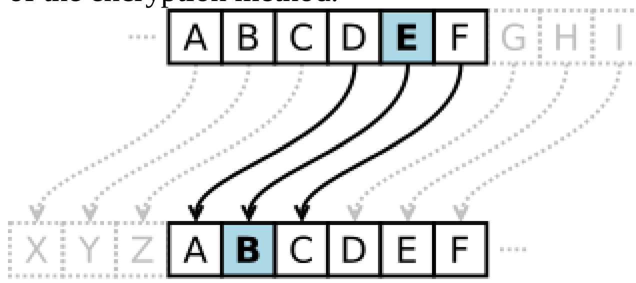


Figure 5.13: SSH Architecture

5 Conclusions

In less than a generation, the information revolution and the introduction of computers in every dimension of society has changed the world. Predictions of some important people in engineering field come true and the world turns into a "global village" where there are no borders for business, communications and commerce. Information is the currency of the Internet economy; information security technologies have a huge impact on how organizations lead electronic business and thus achieve their strategic objectives.

This paper discusses the importance of information security technologies in the information society, and explaining the advantages of adopting information security technologies.

Packet Tracer is just for learning. It is quite simple and GUI oriented. It serves for the purpose of subnetting, routing, wireless communication. But, regarding the network simulators, Omnet++ is a better option. This simulator is powerful, but more time is needed in order to understand it.

Omnet++ has some good GUI basic modules and it allows you to learn simple things easily from tutorials. Omnet++ is a

very versatile simulator, but the versatility comes at the cost of added complexity.
In Omnet++ you should already be familiar with C++, and be prepared to write lots of it. Omnet++ also contains a rich set if libraries that allow you to model wireless networks, GSM networks, vehicular ad-hoc networks or peer-to-peer networks.

Although the Internet is facing with a higher grade of security threats that does not affected its spread on a global scale. We know that it is impossible to totally remove all the attackers, but by using security knowledge we can control our networks.

References

[1] "Computer networks", David Wetherall, Andrew Tanenbaum, Pearson Prentice Hall, 2011.

[2] “The TCP/IP guide - the benefits of networking models”, Charles M. Kozierok, retrieved July 10, 2016, from http://www.tcpipguide.com/free/t_TheBenef itsof
NetworkingModels.htm.

[3] “OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection”, H. Zimmermann, IEEE Transactions on Communications, vol. 28, issue 4, 1980, pp. 425-432.

[4] "Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution", retrieved July 20, 2016, from https://www.diva-portal.org/smash/get/diva2:832701/FULLTEXT01.pdf..

[5] “The TCP/IP guide: A comprehensive, illustrated Internet protocols reference”, Charles M. Kozierok, No Starch Press,US, 2005, pp. 104-110.

[6] “The TCP/IP Protocol Suite”, retrieved July 15, 2016, from http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf/

[7] “TCP dump”, retrieved July 16, 2016, from http://www.usenix.org/publications/login/1998-8/tcpdump.html/

[8] “Network security essentials: Applications and standards: International version”, William Stallings, Pearson Education, US, 2010, pp. 81 – 94.

[9] “The TCP/IP guide - the benefits of networking models”, retrieved July 10, 2016, from http://www.tcpipguide.com/free/t_TheBenefitsofNetworkingMsodels.htm

[10] “Data Encryption Algorithm”, retrieved July 25, 2016, from http://www.searchsecurity.techtarget.com/definition/International-Data-Encryption-Algorithm/

[11] “GRE tunnel”, retrieved July 26, 2016, from http://www.searchnetworking.techtarget.com/answer/What-is-the-difference-between-a-GRE-tunnel-and-IPsec-tunnel/

[12] “8 advantages of using VPN”, retrieved July 24, 2016, from Industry News, https://www.ibvpn.com/2010/02/8-advantages-of-using-vpn/

[13] “SSL/TLS”, retrieved July 25, 2016, from https://www.sans.org/reading-

room/whitepapers/protocols/ssl-tls-beginners-guide-1029
[14] "Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution,", retrieved July 20, 2016, https://www.diva-portal.org/smash/get/diva2:832701/FULLTEXT01.pdf.