ISSN: 2456–5474 RNI No.UPBIL/2016/68367 Vol.-6* Issue-5* June- 2021
Innovation The Research Concept

Organisation Network Security

Paper Submission: 02/06/2021, Date of Acceptance: 14/06/2021, Date of Publication: 25/06/2021

Nishi Srivastava
Network Engineer,
Dept. of Computer Science & Engineering,
IPST, Kanpur, Uttar Pradesh, India

Sakshi Srivastava
Network Engineer,
Dept. of Computer Science & Engineering,
IPST, Kanpur, Uttar Pradesh, India

Abstract

"Organisation of Network Security" is one of the biggest concerns when we talk about something related to an organization development or a firm globalization since all of that requires a highly secured procedures to be embedded in the deep roots of the respective norms and when it comes to an organization network then it would definitely cost a much bigger than the actual practiced methods. An organization network serves as the biggest asset for the employees and co-workers working in it since it is the basic duty or we can say the foremost responsibility of an organization to serve a smooth secure network to their working partners because then only an organization can ensure off a better and highly good results from their employees. Nowadays cyber-crimes and malicious attacks are very common and also at their highest peak, the only basic aspect we all need to look after is the SECURITY.Network Security implies the protection of whole network from unauthorized and illegal access.

Keywords: DHCP, Routing, Nating, ACL's, Frame-relay, Switching (VLAN, VTP).

Introduction

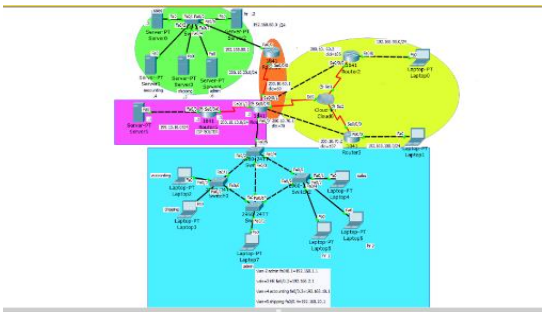
Network Security is simply a process of securing and safeguarding the network from any outside hackers and attackers who are trying to enter in the network and perform all destructive activities like illegal and non-authentic procedures and implementations. This process of securing our network through hackers and attackers a lot of modifications can be done in the security-implementation-procedures. With the increased use of electronic media in our personal lives as well as businesses, the possibility of security breach and its major impact has increased. The theft of personal identity, credit card information, and other important data using hacked user names and passwords have become common these days

Apart from all this we can alsoimplement further methodologies for achieving a good result in security point of view-

1. Security Policies and Procedures.
2. Implementing Good Security Measures.
3. Information Security Processes.
4. Implementing Security Policy.
5. Access Control lists (ACL'S).
6. Authentication & Authorization.
7. Wireless Security and Physical Security.

Experimental Setup

The organization network security which contains 6 modules. Each module is being represented by different colors as shown above.



Step-1
DHCP

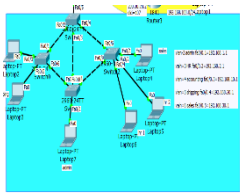


Fig a(i)

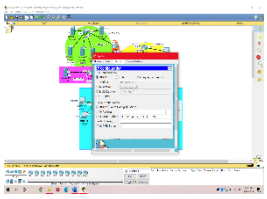


Fig a(ii)

Represented by color: Blue

Fig a (i) describes that all the end users (laptops) areconfigured automatically with DHCP configuration.

Fig a(ii) describes the working of DHCP in which a window showing IP configuration is configured with automatically assigned IP addresses along with their subnet mask and default gateway.

Step: 2
Routing

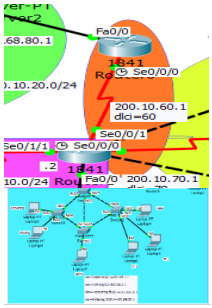


Fig b(i)

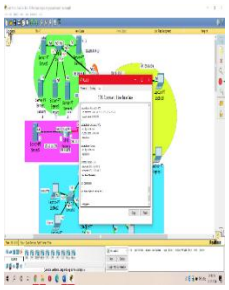


Fig b(ii)

Represented by: Orange

The orange part in the above shows a router that is connected by another router through serial-DCE's cables and a routing protocol EIGRP (Extended-Interior Gateway Routing Protocol) is being configured on each of the router. Routing is a process of connecting devices that are from different networks so that communication can be made possible between them.

Fig b (i) shows the diagrammatic connection of routers through serial DCE'S cables.

Fig b (ii) shows the EIGRP command which is running on each router for connectivity to different network.

Step-3

Fig c(ii) This diagram shows all the NAT commands that are being configured on the main router

Step-4

Access-Control-Lists

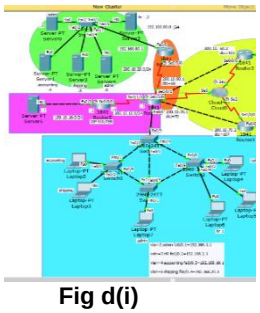


Fig d(i)

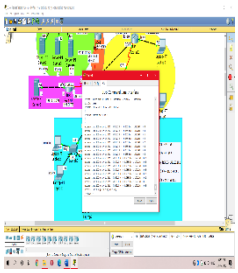


Fig d(ii)

Represented by-Green

Fig d(i) There are five different departments namely Admin, hr, accounting, shipping and sales and acl's are working such that like for ex only admin Department can send packets to admin servers only And rest for all the access is denied.

Fig d (ii) this figure is simply showing all the ACLCommands that are configured on the router.

NATING

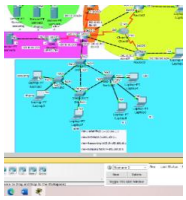


Fig c(i)

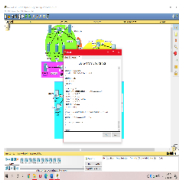


Fig c(ii)

Represented by: -Pink

Fig c(i) Nating is simply defined as Network Address Translation that translates a private IP address to the public IP addresses.

Step-5
Frame-Relay

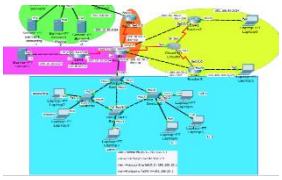


Fig e(i)

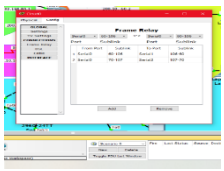


Fig e(ii)

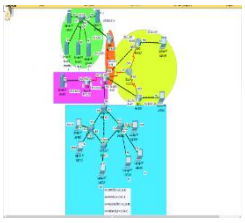
Represented by: - Yellow

Fig e(i) The yellow portion of the fig represents the setup of Frame-Relay which is configured through FR Switch

It basically connects the different remote-locations and uses a DLCIvalue to transfer the packets to destination.

Fig e (ii) This fig shows the ports and sub links that are connected to different remote -locations.

Step 6 Switching (Vlan and Vtp)



Figf(i)

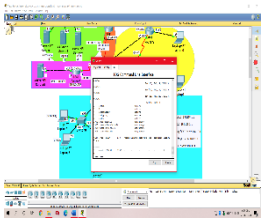


Fig f(ii)

Represented by: blue

Fig f(i) shows the compete experiment that have been completed in 6 steps and here blue portion represents the Switching portion that includes the creation of multiple VLAN's and VTP is also enabled on the main switch that is made the server switch and through VTP i.e. the Virtual Trunking Protocol all the info of vlan's are shared on the connecting switches that are made client switches.

Fig f(ii) this fig shows the vlan's that are created on the CLI of switch.

Objectives of the Study

"Organisation Network Security" deals with security of the entire organization from various security breaches or malware attacks that are very common nowadays. This project basically embodies all the security traits that are implemented in order to protect our organization network. As we know automation is at its sound peak so do the attacks or vulnerabilities too, therefore the highest requirement is to protect our network so that we can ensure a smooth-running flow of the main asset of on organization i.e., "DATA". This project contains advanced security implementations and solutions in concern with security breaches issues in an organization.

Conclusion

Network security is an important field that is getting more and more attention as the internet expands. The security threats and internet protocol should be analysed to determine the necessary security technology. The security technology consists of mostly various hardware devices. In addition network Security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined

together .Securing the network is just as important as securing the computers and encrypting the message.
Points that must be considered when developing a secure network are-:

1. Confidentiality: Information in the network remains private.
2. Authentication: Ensure the users of the network are who they say they are.
3. Integrity: Ensure the message has not been modified in transit.
4. Authorization (access): providing authorized users to communicate to and from.

References

1. *Halsall, F. (2001) Multimedia Communications, Addison Wesley.*
2. *ITU-T X.509 (2000) Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks, International Telecommunication Union.*
3. *King, T. and Newson, D. (1999) Data Network Engineering, Kluwer. Peterson, L. L. and Davie, B. S. (1996) Computer Networks: A Systems Approach, Morgan Kaufmann.*
4. *RFC 2401 (1998) Security Architecture for the Internet Protocol, Kent, S., Atkinson.*
5. *Schneider, B. (1996) Applied Cryptography, 2nd edn, Wiley.*
6. *Stallings, W (1999) Cryptography and Network Security, Prentice Hall.*
7. *Stallings, W (2001) SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, 3rd edn, Addison Wesley.*
8. *Anderson, R. (2001) Security Engineering: A Guide to Building Dependable Distributed Systems.*
9. *Wiley. BS 7799-2 (2002) Information Security Management Systems – Specification with Guidance for Use, British Standards Institution.*
10. *Ellis, J. and Speed, T. (2001) the Internet Security Guidebook, Academic Press.*
11. *ISO/IEC 17799 (2000) Information Technology – Code of Practice for Information.Security Management, International Organization for Standardization.*
12. *Tanenbaum, A. S. (1996) Computer Networks, 3rd edn, Prentice Hall.*