SUNY POLYTECHNIC INSTITUTE

PROJECT TITLE

Network Security & Privacy (Dynamic Routing Protocols with servers)

PROJECT REPORT

SUBMITTED BY

JONATHAN RAJ KATIKALA (U00348780)
ABHILASH REDDY DEVARAPALLI (U00348733)
NAVEEN VISHLAVATH (U00349623)
SAI SHREYA JILLELLA (U00349056)
SUPRIYA MURARISHETTY (U00349072)

PREPARED FOR

COMPUTER NETWORKS – CS522

SUBMITTED TO

Prof. Saumendra Sengupta

Network Security and Privacy

1st T. Venkat Narayana Rao
Dept. of CSE
Sreenidhi Institute of Science & Tech.
Yamnampet, Hyderabad, India.

2nd Md. Hashmathur Rehman
Research Scholar
Faculty of Management Studies.
ICFAI University Jharkhand.

3rd Dr.A. Govardhan
Dept. of CSE.
B.E.(CSE), M.Tech., Ph.D FIE.
Jawaharlal Nehru Technological University,
Hyderabad | JNTUH.

***Abstract*—**

Using dynamic routing protocols and web authentication services as examples, this project explores network security and privacy communication. Through the use of dynamic routing, this project aims to connect every network in the topology. Rather than doing local authentication on routers, I'll be using Radius servers and Tacacs servers.

Keywords—

Dynamic routing with authentication using radius and tacacs, Topology communication, Network Security, Pinging.

I. INTRODUCTION

My topology, which comprises of three locations, looks like this. Guelph, Waterloo, and Kitchener make up Sites A, B, and C, respectively. When you wish to establish contact outside of your network, dynamic routing is necessary. At every location, access and edge routers are present. Each edge router is linked to other edge routers at various locations. On Site A, the EIGRP protocol will be set up. On Site B, the OSPF protocol will be configured, and on Site C, the RIP protocol. These protocols serve as illustrations of dynamic routing.

II. MOTIVATION

A. Overview

As this project is about communication, the dynamic routing protocol is chosen to be implemented as per its advantages.

B. Dynamic Routing Protocol

Dynamic routing protocols are those that allow a router to automatically change its routing table in response to data from other routers in the network.

Automatic updates, scalability, and load balancing are the main things to be considered in the dynamic routing protocol. as this project has to make the communication between the networks using servers with the use of protocols. However, dynamic routing protocols also have some disadvantages, including:

Increased network overhead: Dynamic routing protocols generate more network traffic than static routing as routers exchange routing updates and advertisements.

Increased complexity: Dynamic routing protocols are more complex to configure and troubleshoot than static routing.

Compared to static routing, dynamic routing is used for the solutions to be reliable and effective as per the calculations. With these advantages, we chose the Dynamic Router Protocol to be implemented.

C. Network Security

The main factors under the network security are : Access Control; Firewall; Encryption; Monitoring; Incident Response.

Each aspect works together to make the process more accurate, giving the network administrator access to the communication flow and maintaining ongoing network connection.

As it should protect the confidentiality of the packets in the network, encryption is a necessary component. A firewall secures the system and defends against or slows down hackers, preventing packet loss in the network.

Monitoring is a crucial component that needs to be taken into account. Any interruption in the flow caused by a bad connection or an unorganized network topology causes miscommunication, which needs to be fixed as quickly as feasible. Any type of misunderstanding or disconnect should be found and fixed.

D. EIGRP (Enhanced Interior Gateway Routing Protocol)

Required Terminology for *EIGRP*[3]

Let the bandwidth be "b," the load "l," the delay "d," and the reliability be “r.” Formula be:

$$[K1 * b + (K2 * b) / (256 - l) + K3 * d] * [K5 / (r + K4)]$$

The lowest-bandwidth link on the route to the target network is considered to have the highest bandwidth.

Load is a proportion of the total traffic flowing via the lowest bandwidth link leading to the destination network at any given time.

In terms of tens of microseconds, delay is the total amount of time taken to reach the destination network. Security is a fractional representation of the reliability of the lowest-reliability link on the route to the destination network.

The composite measure for each path to a destination network is determined by EIGRP using this equation. The best path is selected, and traffic is routed along it. This path has the lowest composite metric.

E. OSPF (Open Shortest Path First)

Required terminology for *OSPF*

let reference band width be "R" and interface band width be “I." Formula be:

$$R / I$$

Reference bandwidth is a variable of choice, with a default value of 100 Mbps. The network administrator can modify this number to precisely calculate the measure.

Interface bandwidth, expressed in bits per second (bps), is the capacity of the connection between two routers.

The throughput of the entire path is constrained because OSPF utilizes the bandwidth of the link with the lowest bandwidth when calculating a path's statistic. In order to equalize the statistic across various link types with various bandwidths, the reference bandwidth is then used.

F. RIP (Routing Information Protocol)

In this protocol, the hop count is equal to the formula to acquire the requirements of Routing Information Protocol.

hop count[4]

The hop count is the total number of routers a packet must pass through in order to reach the target network.

RIP only counts the number of routers a packet must pass through in order to reach the destination network to determine the metric of a path. The hop count is referred to as this. Any path with a hop count of 16 or more is regarded as unreachable because the maximum allowed hop count in RIP is 15.

The resulting metric is an 8-bit value (1 byte), and the best route to the destination network is determined by the path with the lowest metric.

G. Radius Server

A network server type known as a RADIUS[1] (Remote Authentication Dial-In User Service) server offers network users and devices centralized authentication, authorization, and accounting (AAA) services. Users who connect to a network using a modem or virtual private network (VPN)

connection are frequently authenticated using RADIUS.

To further improve network security, RADIUS can offer extra security features like encryption and two-factor authentication.

The user authentication database, which includes each user's username, password, and other authentication information, is one crucial table. This database is searched for the user's credentials when they attempt to authenticate in order to confirm their identity.

In addition, RADIUS employs a variety of equations and algorithms for hashing, encryption, and other security-related tasks. For instance, the shared secret between the RADIUS server and client is securely hashed using the Message Digest 5 (MD5) technique by the RADIUS protocol.

H. Tacacs Server

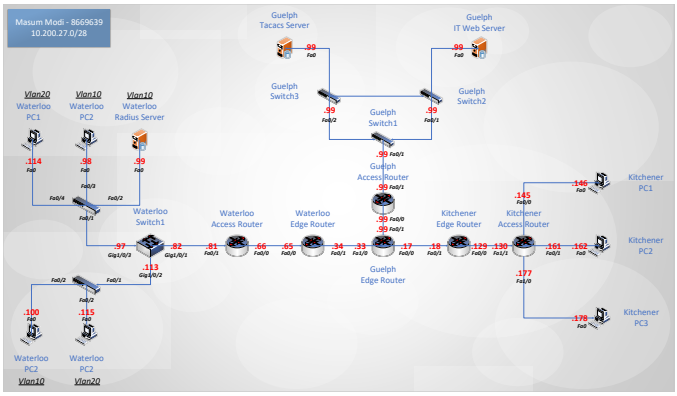
A network protocol called TACACS[2] (Terminal Access Controller Access-Control System) is used for distant network device authentication and authorization. Network appliances like routers, switches, and firewalls can access centralized authentication and authorisation services from a TACACS server.

TACACS is intended to offer both authentication and authorization services, in contrast to RADIUS, which focuses solely on providing authentication services. The network device sends a TACACS server authentication request whenever a user tries to access it. The TACACS server then uses different authentication techniques, such as username and password, digital certificates, or biometric verification, to confirm the user's identity.

To store user credentials, policies, and other configuration information, TACACS servers use a variety of tables and databases. User Authentication Database, Authorization Policy Database, and others are among them. Client Table for TACACS

TACACS also employs a number of encryption and hashing algorithms to provide safe communication between the TACACS server and network devices. Consider the three-step encryption procedure used by TACACS+, which involves communication between network devices and the TACACS server. TACACS+, for instance, employs a three-step encryption procedure that entails: Hashing, Session Key, and Initial Encryption.

Implementing all the mentioned aspects in the paper, the layout is as below:



III. ATTRIBUTE AND DEFINITION

A. Abbreviations and Units

Possible unit measurements for a project on network security and privacy:

Bandwidth : Bits per second (bps) and other multiples like kilobits per second (Kbps), megabits per second (Mbps), and gigabits per second (Gbps) are used to measure bandwidth. A crucial parameter for assessing the capacity and effectiveness of a network is bandwidth.

Latency : The amount of time it takes for a packet of data to go from one location on a network to another, measured in milliseconds (ms) or microseconds (s). For applications like online gaming and video conferencing, low latency is crucial.

Packet Loss : Data packets that are lost or rejected during transmission are referred to as "packet loss," which is quantified as a percentage. Network performance might suffer from high packet loss, which can also be a sign of security.

Encryption Strength : The number of bits utilized to encode data is referred to as the encryption strength, which is measured in bits. The encryption is stronger and it is more difficult for unauthorized parties to access or decipher the data when there are more bits in use.

The strength and complexity of the used authentication techniques, such as the length and complexity of the passwords, multi-factor authentication, and biometric authentication, are used to determine the level of authentication. These measures are not all-inclusive and can be changed depending on the network security and privacy project's particular focus.

Data transfer rate : Bits per second (bps) or multiples such as kilobits per second (Kbps), megabits per second (Mbps), and gigabits per second (Gbps) are used to measure the speed of data transport. This gauges how quickly data can be sent across a network.

Packet size: The size of each data packet sent over a network, expressed in bytes. Larger packets could take longer to transmit and might be more susceptible to eavesdropping, which can have an impact on network performance and security.

Key length: Key length describes the size of the cryptographic key used to encrypt data and is expressed in bits. Since they are more difficult to crack, longer keys typically provide stronger security.

SSL/TLS certificate key length : The length of the key used to secure SSL/TLS certificates, expressed in bits, is referred to as the SSL/TLS certificate key length. In general, sensitive applications should use longer keys because they provide higher security.

VPN tunneling protocols : VPN tunneling protocols[6][7][8] is the level of encryption used to protect VPN connections, measured in bits. Greater security is offered by stronger protocols, but performance may be affected.

These devices can be used to compare various technologies and configurations as well as to measure and assess a network's performance and security.

B. Some Common Mistakes

Misconfigured routing protocol:

Misconfiguring the dynamic routing protocol is one of the most frequent errors. The network administrator may, for instance, install various routing protocols on various routers or incorrectly configure parameters like the network address, subnet mask, or AS number.

Incorrect subnet mask: Using the wrong subnet mask when establishing the routing protocol is another usual mistakes. Due to the fact that the routing protocol uses the network address and subnet mask to establish the network borders and the optimum route to a destination network, this can result in routing problems.

Incorrect routing metric: When determining the best route to a destination network, the routing metric is a crucial component. The routing protocol may select a less-than-ideal path or not be able to connect to the destination network at all if the routing metric is specified improperly.

Firewalls Issues: Firewalls occasionally prevent communication between routers using dynamic routing protocols. This may occur if the firewall is not set up to permit traffic related to the routing protocol or if it rejects the multicast packets that the routing protocol uses to communicate routing information.

Link failure: The routing protocol must recalculate the optimum route to the destination network when a link fails. The communication between the three networks may be hampered if the routing protocol does not recognize the connection loss or if it does not have a backup path.

Network congestion: The dynamic routing protocol may not be able to update its routing table in a timely manner if there is network congestion or significant traffic on the network. Suboptimal pathways or routing problems may result from this.

It is crucial to appropriately organize and configure the dynamic routing protocol, check that the network topology and addressing are accurate, and monitor the network for any problems or failures if you want to avoid making these mistakes.

IV. Required Terms in Sites

DHCP : Dynamic host configuration protocol

HTTP : Hypertext Transfer protocol

DHCP v6 : Dynamic Host Configuration Protocol version 6

TFTP : Trivial File Transfer Protocol

DNS : Domain name system

SYSLOG : System Logging Protocol

AAA : Authentication, Authorization, and Accounting (AAA) services.

NTP : Network Time Protocol

FTP : File transfer protocol

IoT : Internet of Things

VM Management : Virtual machine

Radius EaP : Extensible Authentication Protocol

Modules in this project are :

PT-HOST-NM-1CE: Copper Ethernet (10Mb).

PT-HOST-NM-1CFE: Copper Fast Ethernet (100Mb)

PT-HOST-NM-1CGE: Copper Gigabit Ethernet (1000Mb)

PT-HOST-NM-1FFE: Fiber Fast Ethernet (100Mb)

PT-HOST-NM-1FGE: Fiber Gigabit Ethernet (1000Mb)

PT-HOST-NW-1W: WiFi 2.4 Ghz (equivalent to WMP300N)

PT-HOST-NW-1W-A: WiFi 5 Ghz

PT-HOST-NM-1W-AC: WiFi 2.4 and 5 Ghz

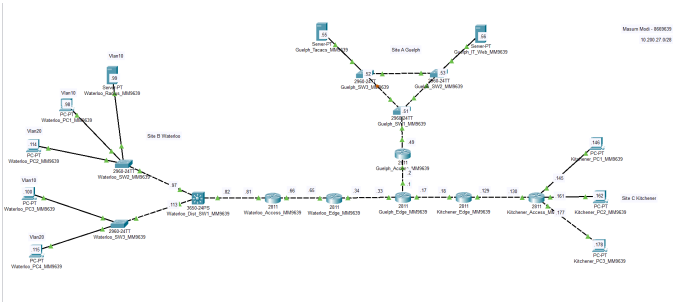
PT-HOST-NM-3G/4G: Cellular 3G / 4G

From the above, *AAA(authentication service)* is the location where the server will have the credentials to validate the connection within the network. As it belongs to the Radius Server.

V. Implementation on Packet Tracer

The topology, which consists of three sites, is as follows. Waterloo is the name of Site A. Kitchener is Site B, and Guelph is Site C. When you wish to establish contact outside of your network, dynamic routing is necessary.

At every location, access and edge routers are present. Each edge router is linked to other edge routers at various locations. On Site A, the EIGRP protocol will be set up. On Site B, the OSPF protocol will be configured, and on Site C, the RIP protocol. These protocols serve as illustrations of dynamic routing.



Access routers display the protocol used at their own locations. The EIGRP protocol will be visible on the Waterloo Access Router because that is how it is configured.

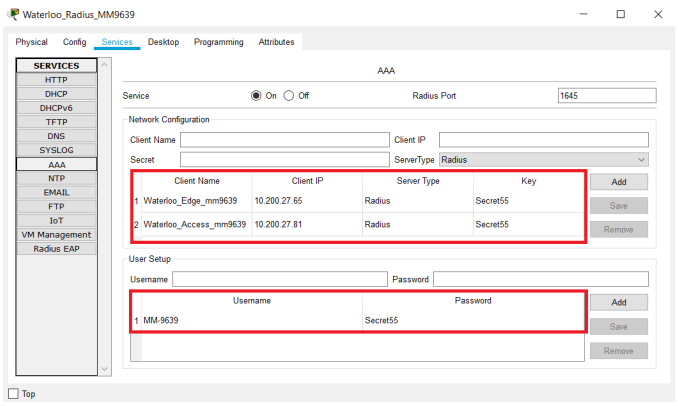
On the other hand, edge routers show both their own protocols and those of the sites to which they are linked. Site A and Site C will be redistributed through Kitchener, the edge router of Site B.

When a different protocol is utilized on nearby routers, redistribution occurs. Redistribution would not be required to be configured if every router used EIGRP.

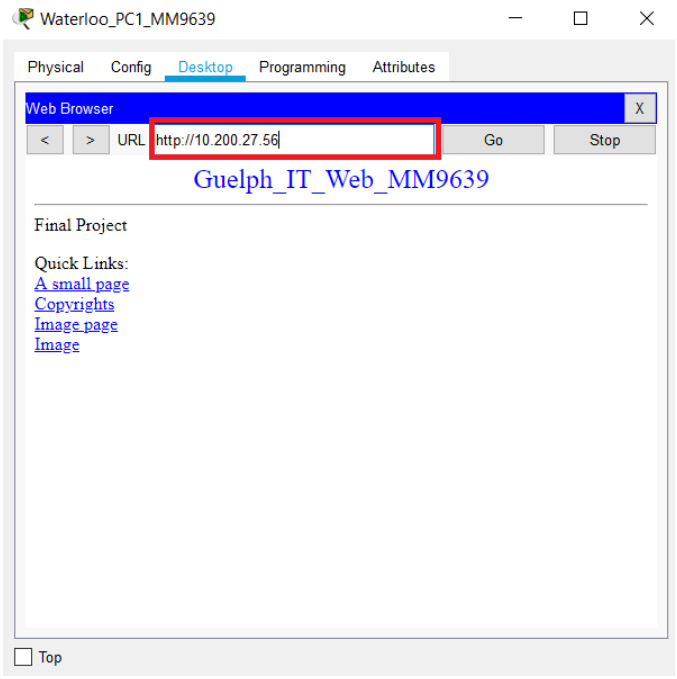
Because the routers with which Site B's Edge router is communicating use a different protocol for Waterloo and Guelph, redistribution on the Edge router is essential.

I now have a Tacacs server in Site A that handles authentication. at a same way, I utilize a radius server at Site B to carry out authentication. I activated the AAA services on the Tacacs server and added two clients (the Access and Edge routers) along with their corresponding IP addresses and passwords. I also established a user and assigned it a password. When this is configured, each time I access the network device, it will prompt me for my username and password.

After configuring AAA services, authentication will now be handled by the server rather than on local computers. It will give authentication and check the login and password against the server database. The Radius server on Site B goes through the identical procedure.



To view the webpage, launch the Tacacs server at position 19.



Let's talk about VLAN trunking[5] at Site B now. All interfaces in Layer 3 switching will be in trunk mode. Additionally, the ports on Switches 1 and 2 that are directed at Layer 3 switches will also be in trunk mode. Inter-VLAN routing will start after this is completed. In other words, communication between two separate VLANs will be possible. Let's build VLANs 10 and 20 in the layer 3 switch to accomplish this.

Give those VLAN interfaces IP addresses. Add the radius server, PC1, PC2, PC3, PC4, and other endpoints to the VLANs. PC1, PC4, and the Radius Server are each allocated to VLAN 10. PC2 and PC3 are given access to VLAN20.

Since routing has been successfully implemented, I can ping every device on the network.

I'll ping other devices from all sites from PC1 at the Kitchener site.

The configuration of dynamic routing protocols used for network communication is done.

The project implementation as per the requirements is done, and I'm enclosing the documents on the Google Cloud related to the outputs or screenshots of the compilation.

https://drive.google.com/drive/folders/1qoHeKe8wXfPUKuL2j8BuI9s-VW2h8uym?usp=sharing

CONCLUSION

In conclusion, by enabling network devices to communicate routing data and dynamically modify their routing tables in response to changes in the network topology, the implementation of dynamic routing protocols between three separate sites can significantly improve network performance and reliability.

It's essential to ensure the security and dependability of communication between network devices and the central authentication servers (Radius and TACACS). Centralized authentication, authorisation, and accounting services for network devices are provided by Radius and TACACS servers.

TACACS servers offer both authentication and authorization services, whereas Radius servers focus primarily on authentication. In addition to using different encryption and hashing algorithms to enable safe communication between the server and network devices, both servers use a variety of tables and databases to store user credentials, decisions, and other config data.

Overall, network managers may provide a dependable and secure network infrastructure for their organizations by adopting dynamic routing protocols with secure authentication and authorisation services.

AKNOWLEDGE

I acknowledge how important it is to design dynamic routing protocols among three separate sites in order to improve network performance and dependability. I am also aware of the crucial roles that Radius and TACACS servers play in supplying network devices with centralized services for authentication, authorization, and accounting.

I am aware that TACACS servers offer both authentication and authorization services, but Radius servers focus solely on providing authentication services. I also understand that in order to ensure secure communication between the server and network devices, both servers make use of various tables, databases, and encryption algorithms.

Overall, I accept the significance of a safe and reliable network infrastructure for enterprises, which can be achieved by adopting dynamic routing protocols with secure authentication and authorisation services.

REFERENCES

1. Radius server Documentation: *https://freeradius.org/documentation/*
2. Tacacs Server Documentation: *https://tacacs.net/documentation/*
3. *Cisco Training White Paper*, Global Knowledge Training LLC, 2013, archived from the original on 15 October 2013, retrieved 17 September 2013
4. Jeff Doyle & Jennifer Carroll (2005). CCIE Professional Development: Routing TCP/IP Volume I, Second Edition. ciscopress.com. p. 170. ISBN 9781587052026.
5. "VLANs and Trunking". Cisco Press. 2002-10-25. Retrieved 2012-03-15.

Tunneling Protocol

6. Pack, D. J., Streilein, W., Webster, S., & Cunningham, R. (2002). Detecting HTTP tunneling activities. MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB.
7. Dang, F., Li, Z., Liu, Y., Zhai, E., Chen, Q. A., Xu, T., ... & Yang, J. (2019, June). Understanding fileless attacks on linux-based iot devices with honeycloud. In Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (pp. 482-493).
8. Raman, D., Sutter, B. D., Coppens, B., Volckaert, S., Bosschere, K. D., Danhieux, P., & Buggenhout, E. V. (2012, November). DNS tunneling for network penetration. In International Conference on Information Security and Cryptology (pp. 65-77). Springer, Berlin, Heidelberg.