NETWORK DESIGN FOR AN E-COMMERCE WEBSITE

COMPUTER COMMUNICATIONS - 18CSS202J

MINI PROJECT - CT4

Department and Branch: NWC, CSE
Register Numbers:
RA2111029010017, RA2111029010043, RA2111029010009, RA2111029010033
Section: Q2

TABLE OF CONTENTS

ABSTRACT

With the advancement of technology, online shopping has become one of the most common aspects of our everyday lives. This kind of virtual shopping is possible with the help of e-commerce (electronic commerce) websites, which work on the principles of not only programming and coding in the designing and development of websites, but also primarily concepts of networks that are involved in establishing connections between users and the servers of the website. Expanding on this idea, the main aim of this project is to design a network that enables the smooth functioning of an ecommerce website that provides services to customers and clients who use the website. The network is designed to provide high availability, scalability, redundancy, and security to support the online business operations that are associated with using the website. A generic e-commerce website in line with the context of the work carried out in this project will have its main components as receiving and storing of information from the customer, placing of orders, and payment processes, all of which require appropriate connections and communication with databases, which is to be established through the network that will be designed in this project. This report covers the features and services involved, requirements for establishing the network, the configurations and the overall design of the network, and the outputs that are derived as a result of implementing the network on the virtual platform cisco packet tracer. The primary combination taken into consideration is that of OSPF, VLAN and ACL, which is compared with the combination of RIP v2, Subnetting and VPN. These are discussed in detail through the sections of the report.

PROBLEM STATEMENT:

This project aims to design and implement a network for a generic e-commerce website, which involves the basic tasks of providing customer information, placing orders, and payment transactions. Different combinations of methods will be explored, and the most appropriate network design will be derived and discussed at the end of the report.

FEATURES AND SERVICES

The main features of the network for a generic e-commerce website that this project will focus on are as follows:

1. **High availability:** Ensures that the website is available to and accessible by users at all times, even during potential network failures that may occur. This is where redundancy is employed.
2. **Redundancy:** This is achieved through the use of redundant servers, switches, routers, and internet connections to ensure that the network continues to operate even in the event of the failure of a component.
3. **Scalability:** Works on accommodating increasing traffic and growing business needs, with the rise in customers using the website. Load balancing comes into play in this scenario.
4. **Load Balancing:** Focusses on distributing traffic across multiple servers to improve performance and ensure that the network can handle high traffic loads, thereby improving the scalability of the network as well.
5. **Security and Segments:** Through the segmentation of the network, in terms of payment processing and customer details, information about the customers that may be sensitive can be protected, thus enhancing the security of the network, and the respective processes that are carried out. Segmentation is particularly established through the separation of different parts of the networks into logical subgroups.

These features and services work on improving the performance of the network and its stability. This is explored in detail in the following sections of the report.

NETWORK REQUIREMENTS

The requirements for an e-commerce website network using OSPF, VLANs, and ACLs are as follows:

Routers: At least two routers are deployed at each site (Site 1 and Site 2). These routers should support OSPF and be configured with OSPF Area 0.

Switches: Managed switches are deployed at each site (Site 1 and Site 2). The switches should have support for VLANs and ACLs.

VLANs: The network should be segmented into logical groups using VLANs. The following VLANs are created:

- VLAN 2 (sales): This VLAN should be used for sales-related activities.
- VLAN 4 (prod): This VLAN should be used for production servers and activities.
- VLAN 8 (acct): This VLAN should be used for accounting-related activities.
- VLAN 15 (admin): This VLAN should be used for administrative tasks.
- VLAN 25 (Site-2): This VLAN should be used to connect to the other site.

Access Control Lists (ACLs): ACLs are used to control access to sensitive data and prevent unauthorized access. They are configured to restrict traffic between VLANs and to prevent unauthorized access to sensitive servers. For example, ACLs are configured to allow access to the web server (192.0.2.100) only from specific IP addresses, such as the admin host (198.51.100.5) and the internet host (198.51.100.10). This is illustrated in figure 1, the network diagram of the combination of OSPF, VLANs and ACLs.

IP addressing: Each VLAN has its own subnet, and IP addressing is planned accordingly, as shown below:

- Sales VLAN (VLAN 2): 192.168.2.0/24
- Production VLAN (VLAN 4): 192.168.4.0/24
- Accounting VLAN (VLAN 8): 192.168.8.0/24
- Admin VLAN (VLAN 15): 192.168.15.0/24
- Site-2 VLAN (VLAN 25): 192.168.25.0/24

Security: The network is secured using encryption, firewalls, and other security measures to protect sensitive data, through the utilization of ACLs. Firewalls are to be configured to block all traffic to the web server except for traffic from authorized hosts.

Monitoring: The network is to be monitored using network monitoring tools to ensure that it is operating optimally and to detect any potential issues. Some examples of network monitoring systems that can be used are SolarWinds Network Performance Monitor (NPM), PRTG Network Monitor, Nagios, Zabbix.

Documentation: The network is to be thoroughly documented, through network diagrams, IP addressing schemes, VLAN configurations, ACL configurations, and other relevant information describing aspects of its construction, design and functioning.

NETWORK SEGMENTATION

The network is segmented into logical groups using VLANs. Each VLAN represents a specific group of devices and has its own subnet. This allows for better management and security of the network. The segmentation of the network with reference to this project is described as follows:

- VLAN 2 (sales) is used for sales-related activities, such as accessing sales-related databases and applications.
- VLAN 4 (prod) is used for production servers and activities, such as hosting the e-commerce website and managing orders.
- VLAN 8 (acct) is used for accounting-related activities, such as accessing financial databases and applications.
- VLAN 15 (admin) is used for administrative tasks, such as managing network devices, configuring ACLs, and monitoring the network.
- VLAN 25 (Site-2) is used to connect to the other site, which suggests that there is another site connected to the network.

By segmenting the network into VLANs, each group of devices can be managed and secured separately, which helps to reduce the risk of security breaches and network downtime. Additionally, it enables network administrators to apply different network policies to each VLAN and to control the traffic flow between VLANs, allowing for better network performance and security.

NETWORK COST ESTIMATION

The total cost of the network would be approximately ₹ 4,16,925. This is derived through the following costs:

5 Cisco switches at ₹ 18,625 each, for a total of ₹ 93,125
6 Cisco routers at ₹ 25,375 each, for a total of ₹ 1,52,250
2 Cisco servers at ₹ 28,500 each, for a total of ₹ 57,000
12 computers at ₹ 9,375 each, for a total of ₹ 1,12,500

Note: The conversion rate used here is 1 USD = 74.25 INR, and prices may vary depending on location and vendor.

Furthermore, the cost estimation provided here is only an approximate figure and does not account for any additional expenses that may arise, such as the cost of additional hardware or software that may be required to fully implement the network. It is important to also consider other factors such as installation and configuration expenses, ongoing maintenance costs, and support costs when planning a network implementation.

NETWORK DIAGRAMS

OSPF + VLANs + Access Control Lists (ACLs)

The following diagram illustrates the combination of **OSPF, VLANs, and Access Control Lists (ACLs)** concepts as methodologies that are involved in the designing of the network for the e-commerce website:

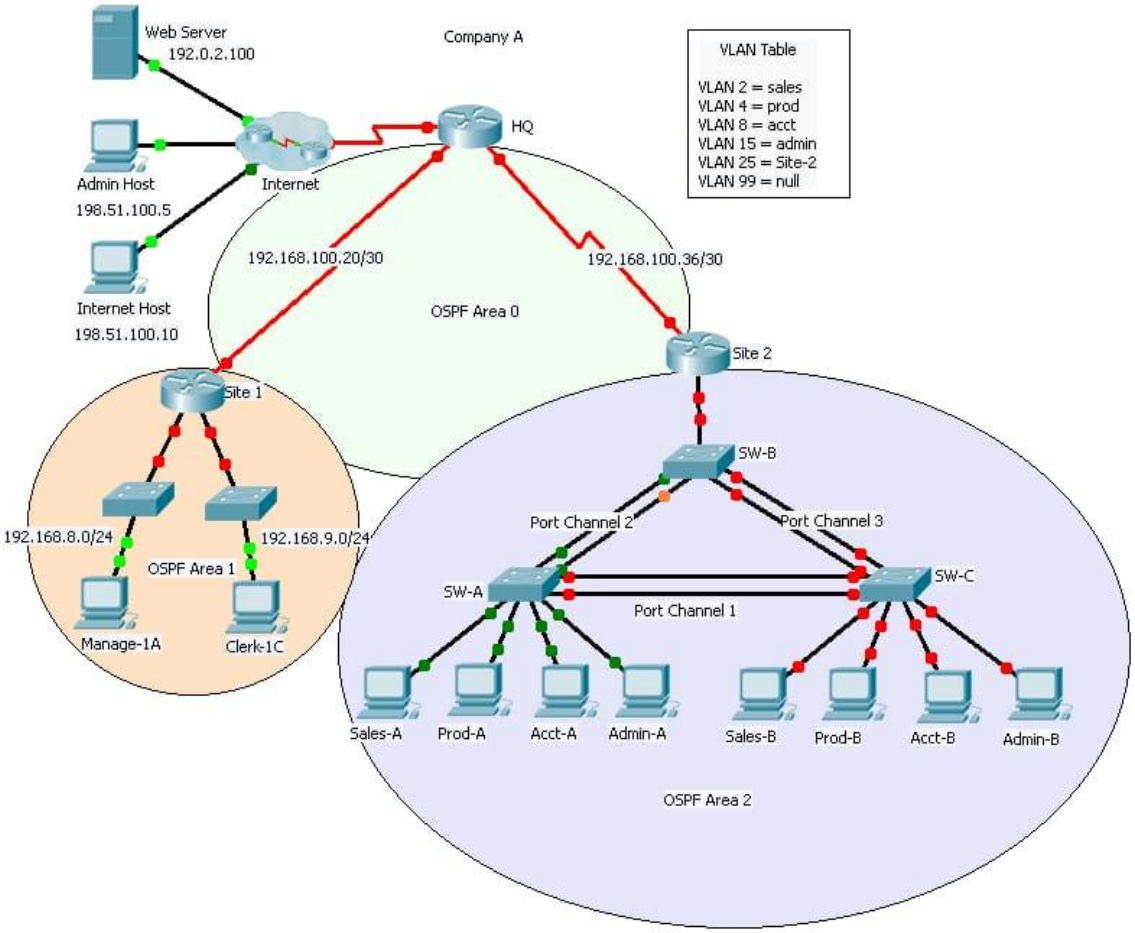

Fig 1: Network Diagram of OSPF + VLANs + Access Control Lists (ACLs)

RIP v2 + Subnetting + Virtual Private Network (VPN)

The following diagram illustrates the combination of **RIP v2, Subnetting and Virtual Private Network (VPN)** concepts as methodologies that are involved in the designing of the network for the e-commerce website:

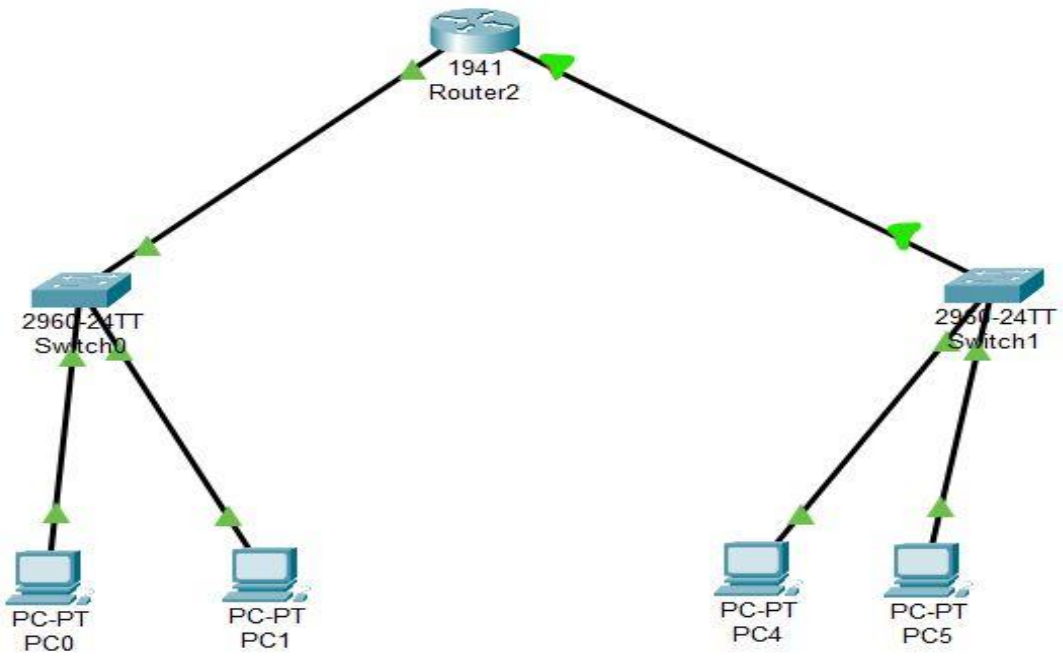

Fig 2: Network Diagram of RIP v2 + Subnetting + Virtual Private Network (VPN)

Background information and relevance of the combination of methodologies used in the above network designs:

OSPF refers to “Open Shortest Path First”", and is an Interior Gateway Protocol (IGP) involving dynamic routing for the internet, and is used in distributing IP routing information through a single AS (Autonomous System) in an IP network. VLAN refers to a “Virtual Local Area Network ", which allows the division of workstations into different LAN segments, thereby automatically limiting the access to only specific groups of users. ACLs, also known as Network Access Control Lists, basically act like a firewall - they are a collection of conditions that permit or deny access, thus providing security by

blocking unauthorized users from accessing any sensitive information/resources, and directing authorized users to access the appropriate resources.

The diagram in figure 1 illustrates three areas of OSPF 0, OSPF 1 and OSPF 2. In OSPF area 0, the router representing the HQ is connected to the internet, as well as the two routers present in the other OSPF areas. OSPF area 1 consists of a router representing site 1, which is further connected to two switches, followed by two end devices representing the manager and the clerk. Lastly, OSPF area 2 consists of a router representing site 2, which is connected to a switch that is linked further with more switches, and end devices representing the sales and product managers, account holders and admins.

The diagram in figure 2 represents the basic connection of the networks, where the router is connected to the internet, and is the key device through which the switches, indicating the Sales and Marketing departments are connected to the HQ, similar to the network design in figure 1. Each of the departments has several computers connected to its switch, each of which represent the sales and product managers, account holders and admins, as in figure 1. This figure is a simplified representation of the structure in figure 1, primarily focussing on the routing aspects, owing to the combination of selected methodologies involved in the network.

IMPLEMENTATION

The implementation of an e-commerce network using ***OSPF, VLANs, and ACLs*** in Cisco Packet Tracer involves the following sequence of steps:

1. Create a network topology in Cisco Packet Tracer.
2. Configure OSPF on all the routers in the network topology. Use the command "router ospf [process ID]" to enable OSPF, and then configure the network interfaces using the "network [network address] [wildcard mask] area [area ID]" command.
3. Create VLANs on the switches in the network topology using the command "vlan [vlan ID]" and assign the appropriate network interfaces to each VLAN.
4. Configure ACLs on the routers in the network topology using the command "access-list [ACL number] [permit/deny] [source IP address] [destination IP address] [protocol] [port number]".
5. Apply the ACLs to the appropriate network interfaces using the command "ip access-group [ACL number] [in/out]".

Once these steps are completed, the e-commerce network will have OSPF-enabled routers for efficient routing, VLANs for logical separation of network traffic, and ACLs for filtering network traffic based on specific rules. These features help to ensure secure and reliable communication between devices and reduce the risk of unauthorized access to sensitive data.

The Implementation of an e-commerce network using ***RIP v2, Subnetting and VPN*** for e-commerce website using Cisco Packet tracer is as follows:

1. Plan the network topology and identify the subnets for different purposes
2. Divide the network into smaller subnets with sufficient IP addresses
3. Enable RIP v2 commands and configure network interfaces
4. Create a secure VPN connection between the website and remote users/sites using required protocols
5. Apply security measures such as firewall rules or ACLs to protect the network against cyber threats

The above implementation will ensure efficient routing, as well as secure and reliable communication for the e-commerce website.

CONCLUSION

Thus the network has been designed for an e-commerce website by following the techniques and applications of OSPF, VLANs and ACLs, as well as for RIP v2, Subnetting and Virtual Private Network (VPN). Through comparisons between the two, it can be concluded that, a safe and effective solution for e-commerce networking may be offered through the use of OSPF, VLANs, and ACLs. Data packet routing is quick and dependable thanks to OSPF. Different types of network traffic can be logically separated using VLANs, which also add an extra layer of security. To further restrict network access, ACLs filter traffic in accordance with predefined criteria. While RIP v2, subnetting and VPN are a good combination by themselves, they would be more effective together in the case of smaller, and simpler scenarios. On the contrary, the combination of OSPF, VLAN and ACL is a lot more effective for establishing networking for larger, and much more complex networks. By implementing these technologies, organizations may improve consumer experiences, provide dependable and secure communication across devices, and lower their risk of data breaches. However, it is important to note that the selection of either RIP v2 with subnetting and VPN or OSPF with VLAN and ACL depends on various factors, such as the size and complexity of the network, the availability and expertise of the IT personnel, the performance and security requirements, and the available budget and resources. It's essential to evaluate these options carefully and select the one that best satisfies the specific requirements of the e-commerce website network.