**Logo

Description automatically generatedGraduation Project**

**Project Name : Design and implement network infrastructure of company**

**A Project Submitted in Partial Fulfillment**

**of the Requirements for the Degree of Bachelor of Science**

**in Systems and Computer Engineering**

**Submitted By**

|  |
| --- |
| **A: Mohamed Ahmed Mohamed Nour Eldean 89** |
| **B : Mohamed Ahemd Mostafa AbdElrahman 90** |
| **C : Mohamed Atef Mohamed Saber 105** |
| **D : Mostafa Sobhy Mahmoud Saleh 134** |
| **E : Mohamed AbdElkareem Hamed 158** |

**Supervised by**

**Prof. Dr. Khalel Mohamed**

**2023**

مشروع التخرج

اسم المشروع : تصميم وتنفيذ البنية التحتية لشبكة الشركة

مشروع مقدم فى الوفاء الجزئى متطلبات الحصول على درجة بكالوريوس العلوم

في هندسة النظم والحاسوب

**مقدمة من**

|  |
| --- |
| **1- محمد احمد محمد نور الدين 89** |
| **2- محمد احمد مصطفى عبدالرحمن 90** |
| **3- محمد عاطف محمد صابر جابر 105** |
| **4- مصطفى صبحى محمود صالح 134** |
| **5- محمد عبدالكريم حامد 158** |

**يشرف عليها**

**الدكتور : خليل محمد**

**2023**

# Examiner Committee

|  |  |  |
| --- | --- | --- |
| **Name** | **Rule** | **Signature** |
| Prof. Dr. | President |  |
| Prof. Dr. | Supervisor |  |
| Dr. | Member |  |

**Date**

13th of July, 2023

# ABSTRACT

- Design and implement network infrastructure of the company

The project is an infrastructure for a company consisting of a main branch and two other branches. All devices can communicate with other devices through switches and routers in the network. It is also possible to control remotely in this network. There are also some servers such as WEB and FTP servers.

The network is activated by ACL Access Control List

To control some of the internal signals and prevent or allow access.

**KEYWORDS** : Network; Routers; Switches ;

# ACKNOWLEDGEMENTS

First and foremost, we thank and praise **Allah** for providing us with the patience, strength, well-being, and skills to complete this thesis at one of the most important stages in our lives.

We would like to thank our supervisor, Professor **Khalel Mohamed**, for his support and guidance.

We would also like to acknowledge Al-Azhar Universityfor granting us to be among its respectful students.

[ABSTRACT… i](#_TOC_250084)

[ACKNOWLEDGEMENTS. i](#_TOC_250083)i

[TABLE OF CONTENTS. i](#_TOC_250082)v

[CHAPTER 1 INTRODUCTION… 8](#_TOC_250079)

* 1. [Network Infrastructure Defintion 8](#_TOC_250078)
  2. [Infrastructure consists of ? 8](#_TOC_250077)
  3. [Infrasutructure Design 9](#_TOC_250076)

1.4 Infrasutructure management………………………………………………………………………………...9

[CHAPTER 2 Switching. 1](#_TOC_250073)2

* 1. [Introduction](#_TOC_250072) 12
  2. [catalyst 2950 series](#_TOC_250071) 13

2.3 : Branches configuration ………………………………………………………………………………………...13

2.3.1 : HQ ……………………………………………………….14

2.3.2 : Branch one………………………………………….34

2.3.3 : Branch two …………………………………………44

[CHAPTER 3 Routing… 5](#_TOC_250051)6

* 1. [Introduction 5](#_TOC_250050)6

3.2 Router Configration ………………………………………………………………………………………………..63

[CHAPTER 4 ACL (Access Control List )… 8](#_TOC_250035)4

* 1. [Introduction 8](#_TOC_250034)4
  2. [ACL Configration 8](#_TOC_250033)8

**Conclosion …………………………………………………………………………………………………………………….90**

**Reference ………………………………………………………………………………………………………………………..…91**

**Chapter1 : Introduction**

**1.1 Network Infrastructure Definition**

Network infrastructure is the broader collection of fundamental components that work cohesively to run an IT network and is a critical part of an organization’s IT infrastructure.

Since an organization relies on its IT network to run mission-critical applications and business operations, ensuring the underlying network infrastructure is reliable, safe, robust, and scalable is crucial.

**1.2 What does a network infrastructure consist of?**

Network infrastructure can be a mix of hardware devices, software applications, and network services, including:

**- Hardware infrastructure**typically includes routers, switches, hubs, repeaters, gateways, bridges, and modems.

**- Software infrastructure** includes monitoring and management tools and operating systems.

**- Network services** include networking protocols such as TCP, UDP, and IP addressing.

An organization can extend its IT network by integrating with third-party services from managed service providers (MSPs) or build hybrid network infrastructure by integrating on-premises infrastructure with cloud services.

**1.3 What is network infrastructure design?**

Network infrastructure design can help you plan how to implement, monitor, and manage an IT network. A design can be created after identifying the operational requirements in terms of capacity, bandwidth, quality of service, security, and resilience.

Network infrastructure design can help you plan an IT network more efficiently. After implementation, network design can aid you when troubleshooting network issues by helping you more easily understand the roles of various components in the network and how a malfunctioning device may affect the network and other systems using the network.

In addition to planning the network infrastructure design, network administrators can also use [network topology software](https://www.solarwinds.com/network-topology-mapper) to gain visibility into network infrastructure, configuration, and performance. In addition, network configuration software can help update topology maps by scanning for changes in the network to help you better understand network infrastructure mapping, identify network architecture changes, and scale capacity more efficiently.

**1.4 What is network infrastructure management?**

Network administrators implement network infrastructure management practices to ensure the network operates optimally by [identifying performance bottlenecks](https://www.solarwinds.com/network-bandwidth-analyzer-pack/use-cases/network-bandwidth-bottleneck), remediating problems, and determining the need for scaling to support growing business operations.

Overall, network infrastructure management focuses on five aspects of networking:

1. **Network Infrastructure Monitoring:** A network infrastructure monitoring system continuously monitors the network and reports problems. For example, a router may be receiving more traffic than it can handle and crashes, impacting network availability.

**2. Configuration Management:** This aspect focuses on ensuring network devices are configured with best practices, patched, upgraded, or replaced when needed. Usually, network administrators leverage automation tools to [track and manage configuration changes](https://www.solarwinds.com/network-configuration-manager/use-cases/network-change-management) more effectively when managing more extensive IT networks.

**3. Performance Management:** This aspect focuses on analyzing a network and maintaining a required network performance level to ensure business operations aren’t negatively impacted. Some of the critical metrics relevant to performance management include available network capacity, bandwidth utilization, latency, and throughput, among others.

**4. Fault Management:** This aspect helps identify problems in an IT network and determine root causes to fix issues from recurring. Some tools even apply automated remediation through pre-defined playbooks when a problem occurs, improving efficiency and meaning time to recovery (MTTR).

**5. Security Management:**Since an IT network is critical to business operations, it is imperative to ensure it’s protected from various network-based threats and block malicious attempts to gain unauthorized access. Network administrators can use firewalls, intrusion detection and prevention systems, and log traffic monitoring tools to help ensure the network is safe and attacks are identified and blocked quickly.

Chapter 2 : switching

2.1 intro

# **What Is Network Switching?**

Switching in IT and computer networking is the transfer of data packets, or blocks of data, through a network switch. Switches transfer data from source ports on devices such as computers to destination ports on devices such as routers.

### **What is a switch?**

A switch is a hardware component in network infrastructure that performs the switching process. The switch connects network devices, such as computers and servers, to one another.

A switch enables multiple devices to share a network while preventing each device's traffic from interfering with other devices' traffic. The switch acts as a traffic cop at a busy intersection. When a data packet arrives at one of its ports, the switch determines which direction the packet is headed. It then forwards the packet through the correct port for its destination.

Some data packets might come to the switch from devices, like computers or voice-over-IP (VoIP) phones, that are attached directly to it. Other data packets might come to the switch from indirectly connected devices, through a network element such as a hub or router.

The switch knows which of the network's devices are connected to it, and it can transfer data packets between those devices directly. In other cases, data packets may be going to more-distant destinations, on other networks. A switch in such a scenario forwards the packets to a router, which then forwards them to their destinations on the network.

**2.2 : catalyst 2950 series**

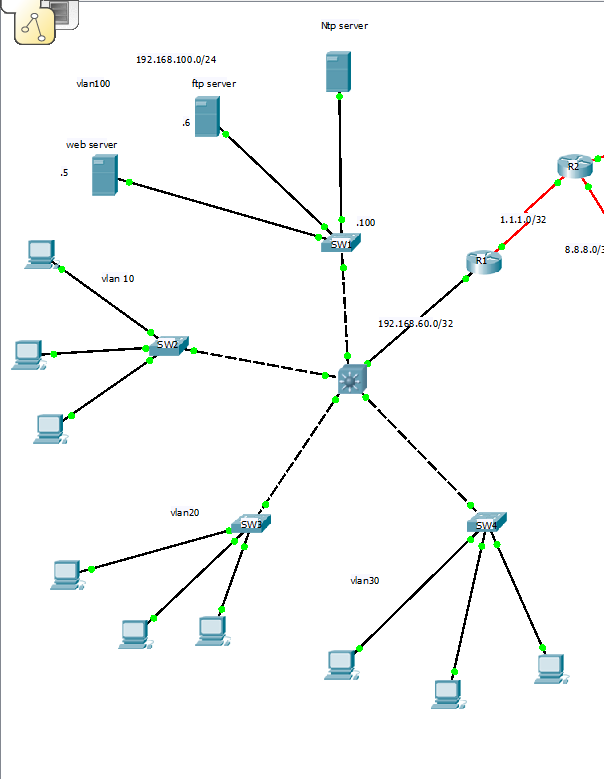
The Cisco Catalyst 2950 Series is a line of fixed-configuration, stackable, and standalone switches that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity. This product line offers two distinct sets of software features and a range of configurations to allow small, mid-sized, and enterprise branch offices, and industrial environments to select the right combination for the network edge. The Standard Image (SI) Software offers Cisco IOS functionality for basic data, video and voice services. For networks with requirements for additional security, advanced quality of service (QoS) and high availability, the Enhanced Image (EI) Software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge.

**2.3 : Branches configuration**

Our infrastructure contains three headquarter and two branches

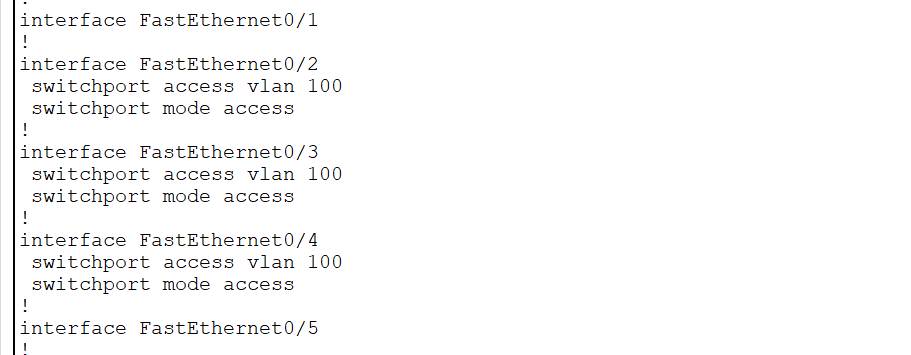
**2.3.1 : HQ**

It contains four switches, a core switch, and three servers



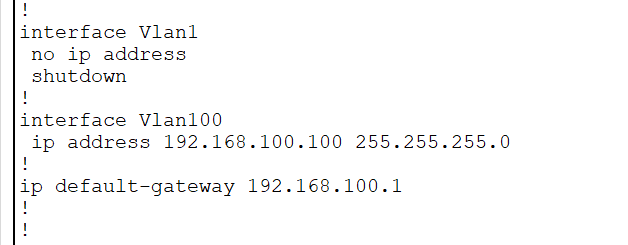
**Sw 1**

**Interface configuration**

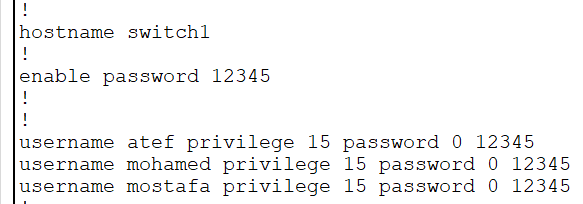


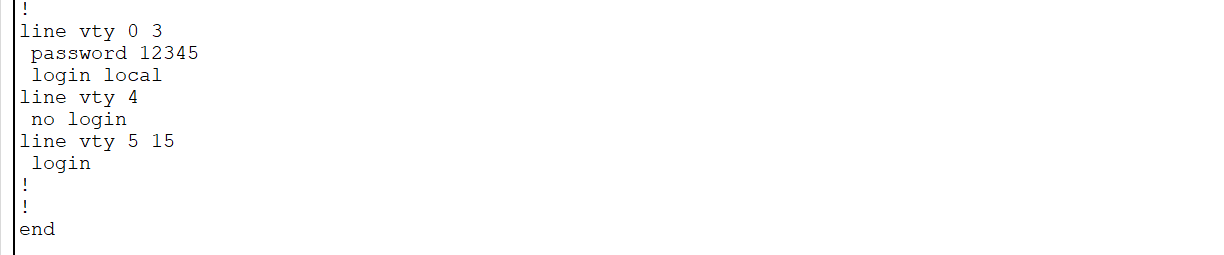
Switch 1 configuration :

**Interface vlan configuration**

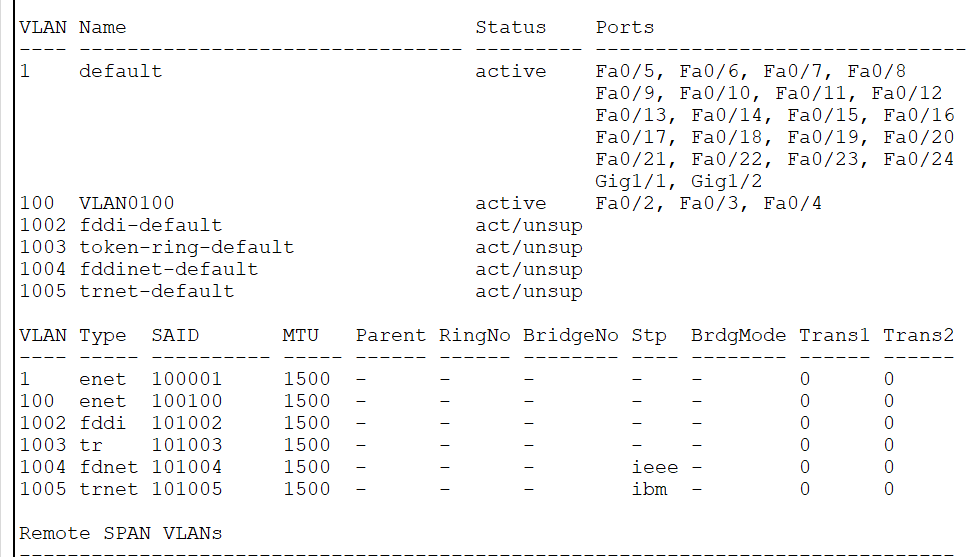


**Remote login**





**vlan configuration**

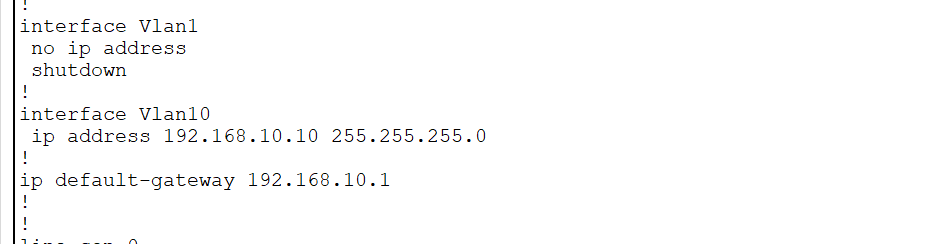


**Sw 2**

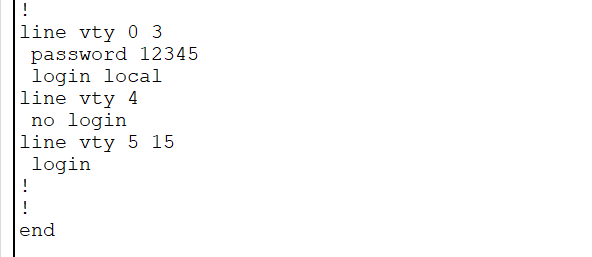
**Interface configuration**



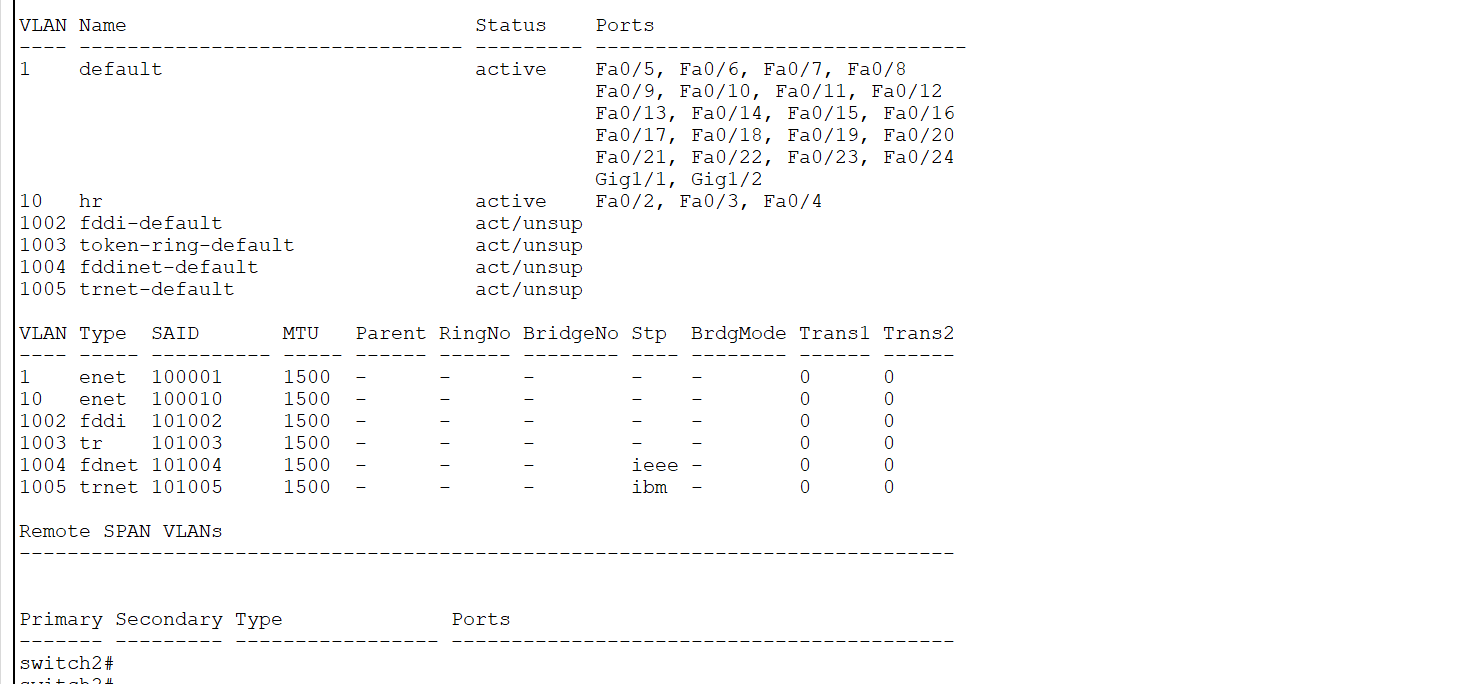
**Interface vlan configuratio**



**Remote login**

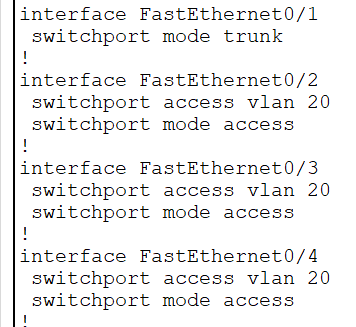


**vlan configuration**

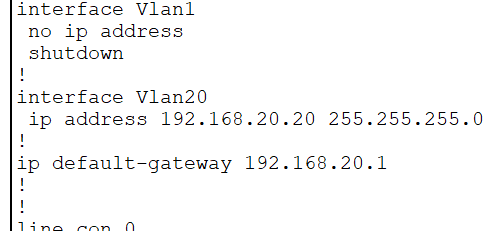


**Sw 3**

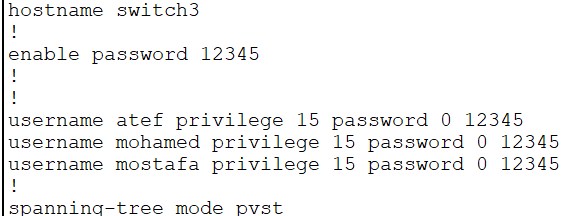
**Interface configuration**

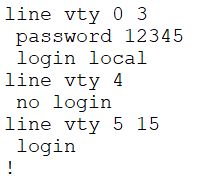


**Interface vlan configuration**

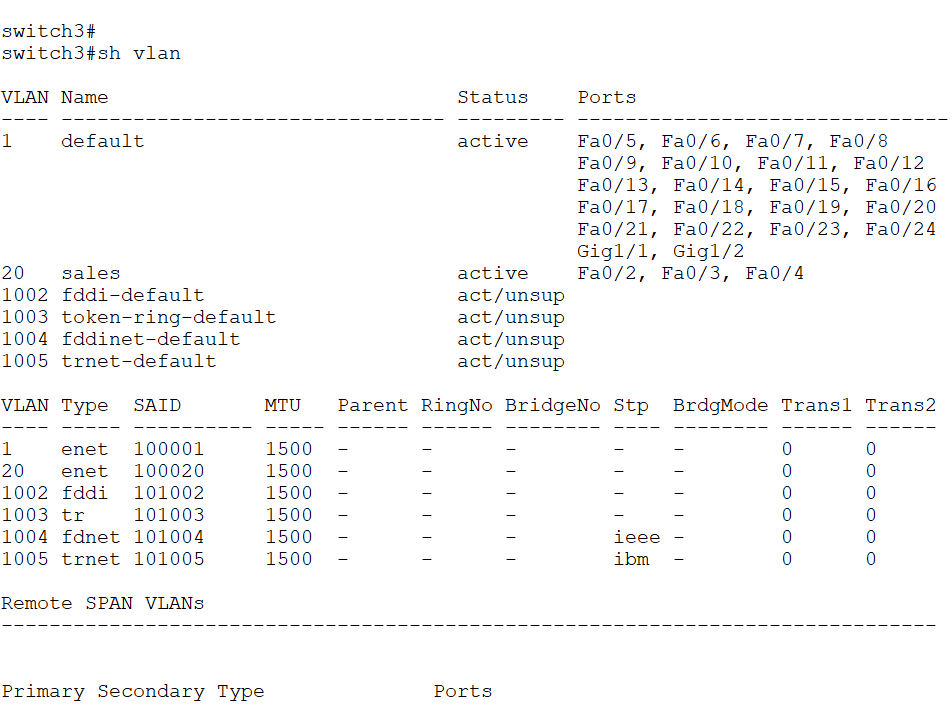


**Remote login**



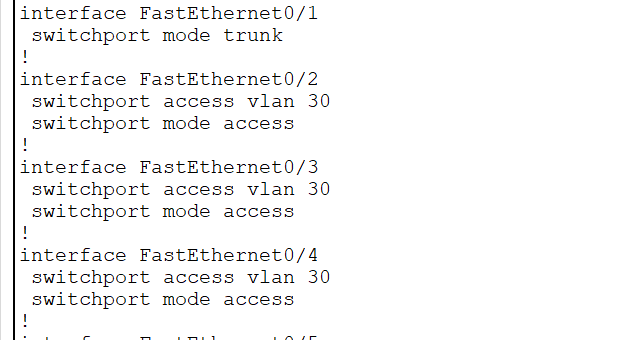


**vlan configuration**

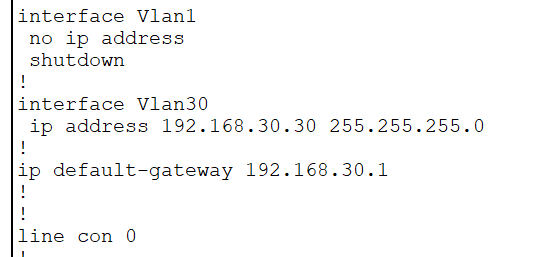


**Sw 4**

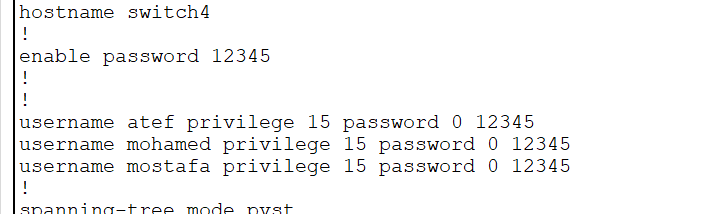
**Interface configuration**

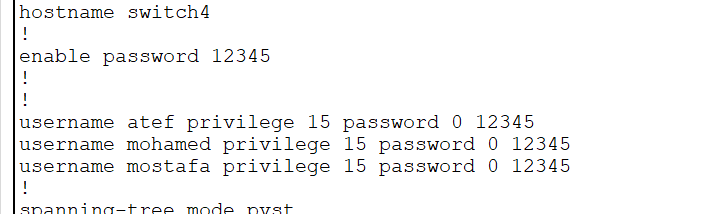


**Interface vlan configuration**

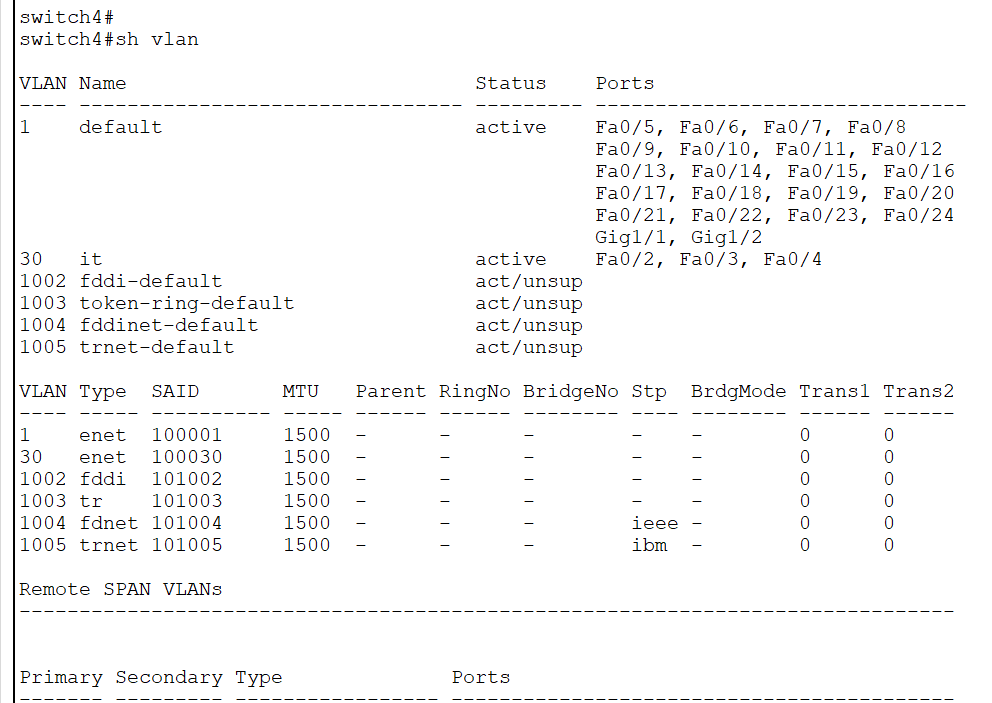


**Remote login**





**vlan configuration**



**Core sw**

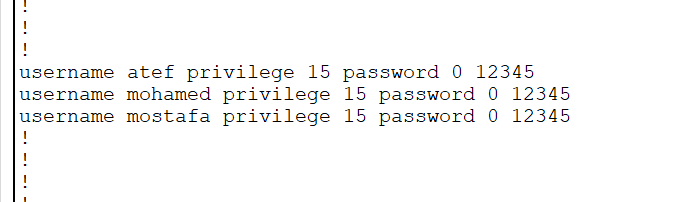
**Interface configuration**



**Interface vlan configuration**



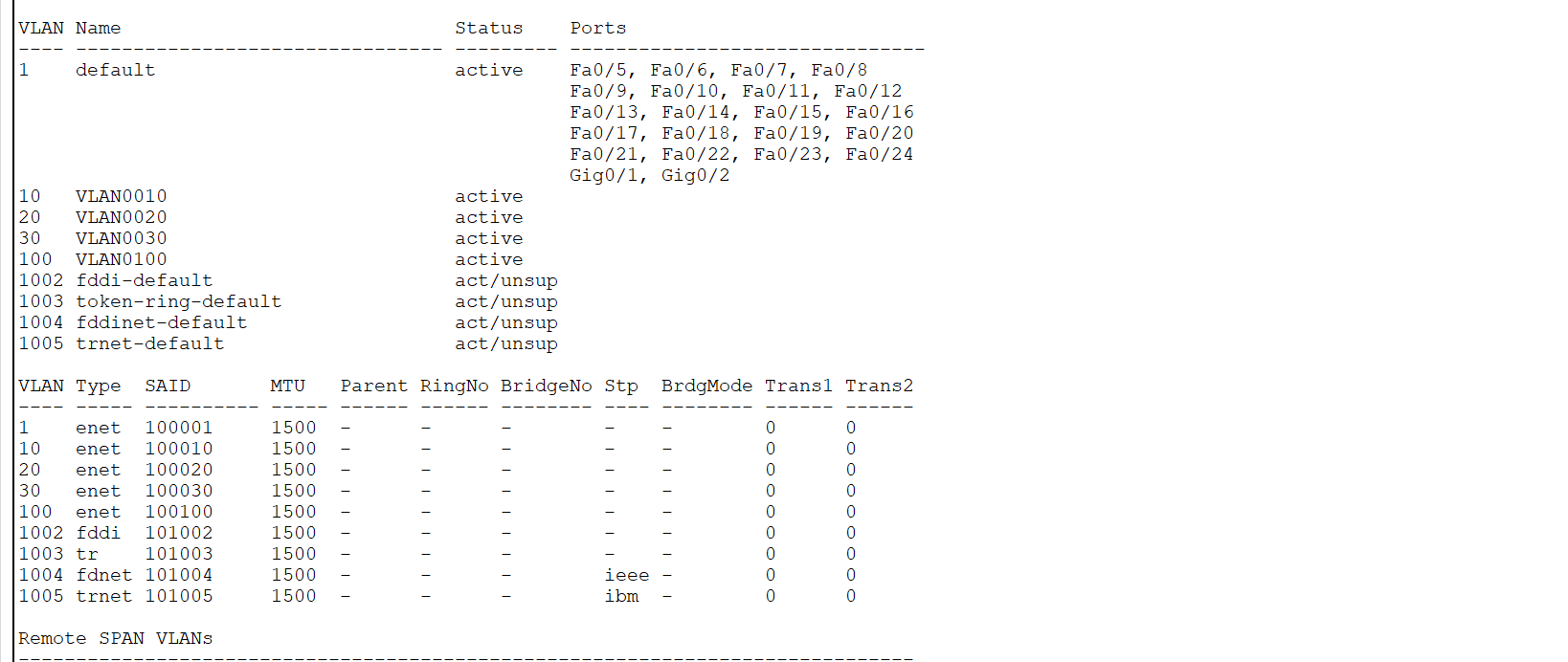
**Remote login**



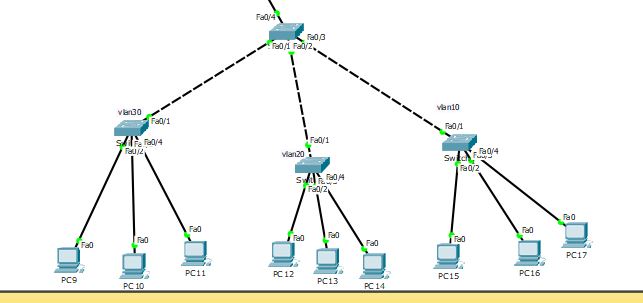
**routing configuration**



**vlan configuration**



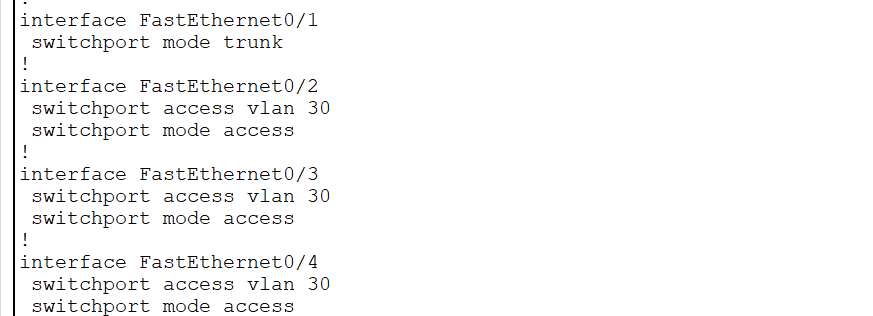
2.3.2: Branch 1



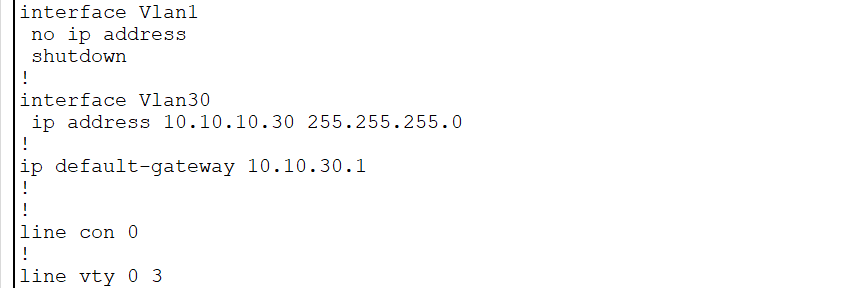
It contains four switches.

**Sw 1**

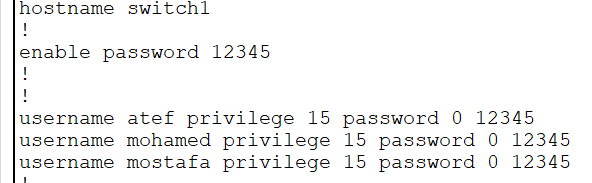
**Interface configuration**



**Interface vlan configuration**

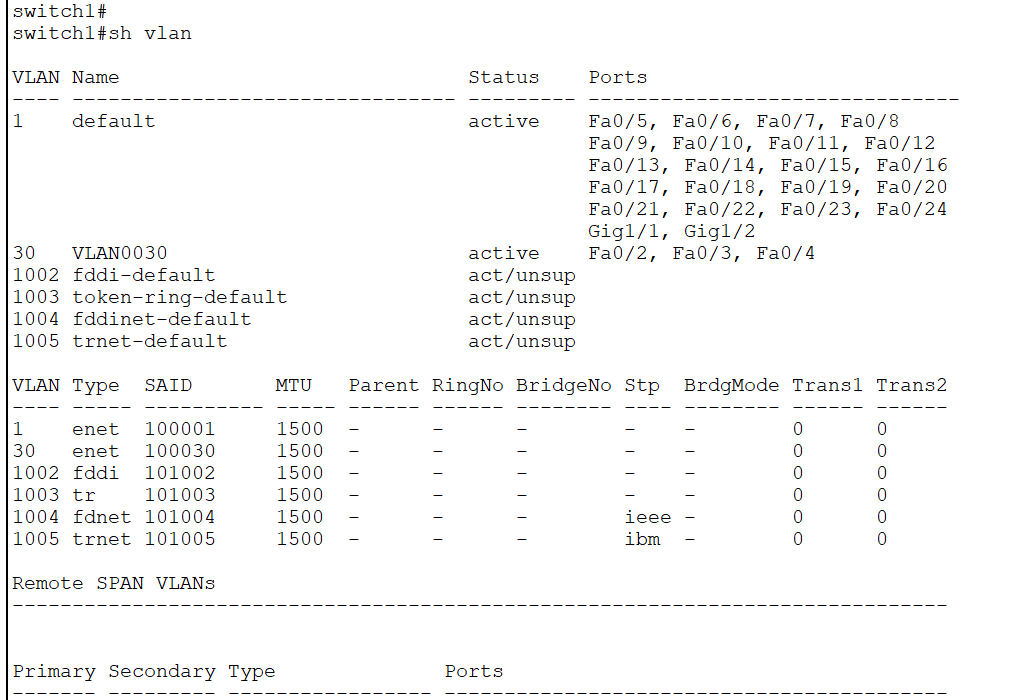


**Remote login**





**vlan configuration**

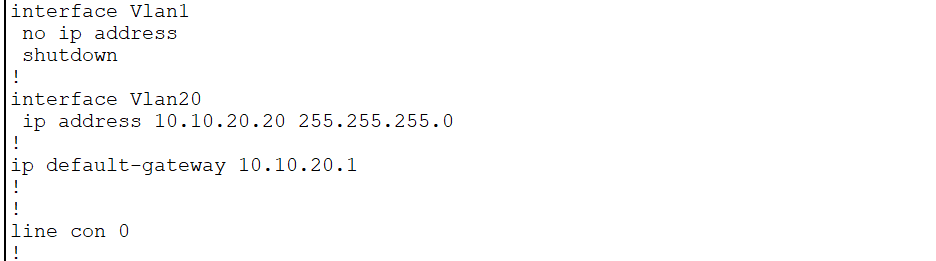


**Sw2**

**Interface configuration**

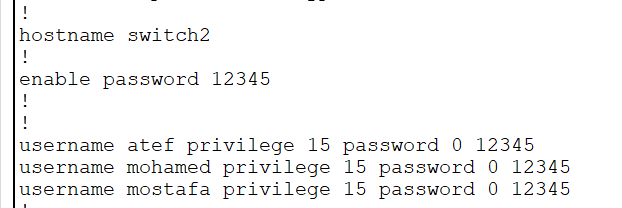


**Interface vlan configuration**

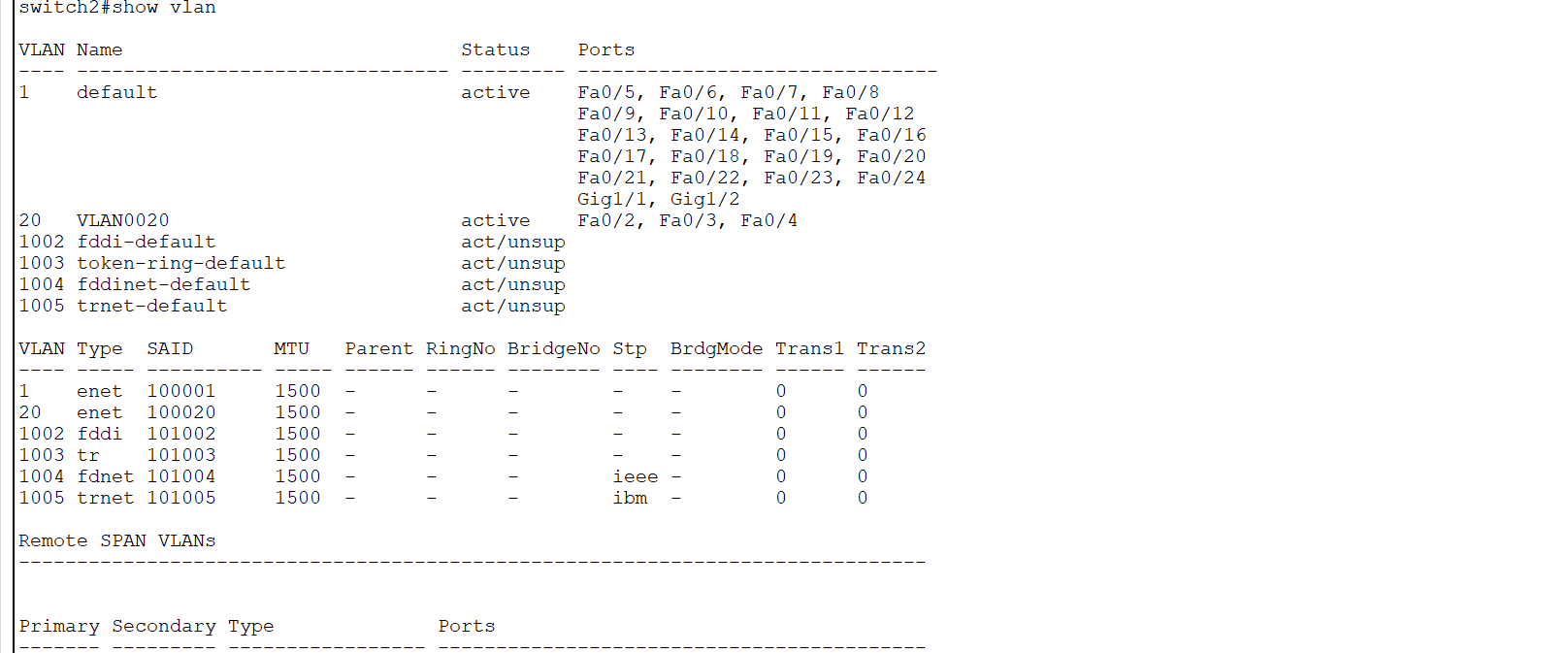


**Remote login**





**vlan configuration**



**Sw 3**

**Interface configuration**



**Interface vlan configuration**

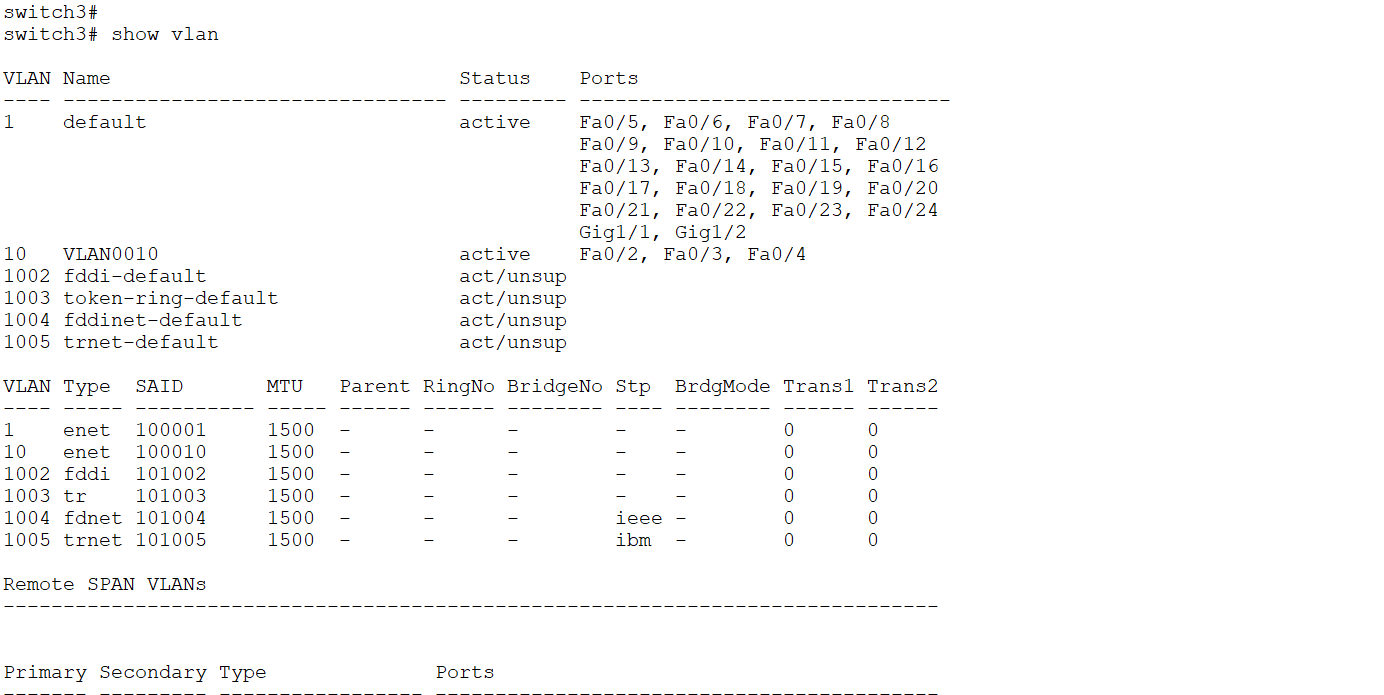


**Remote login**

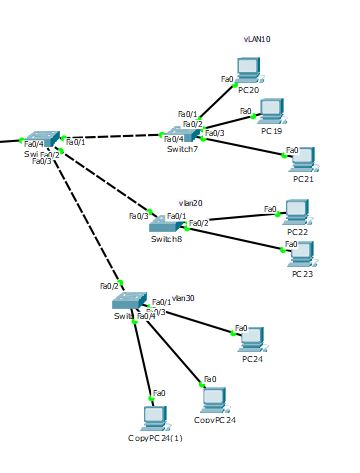




**vlan configuration**



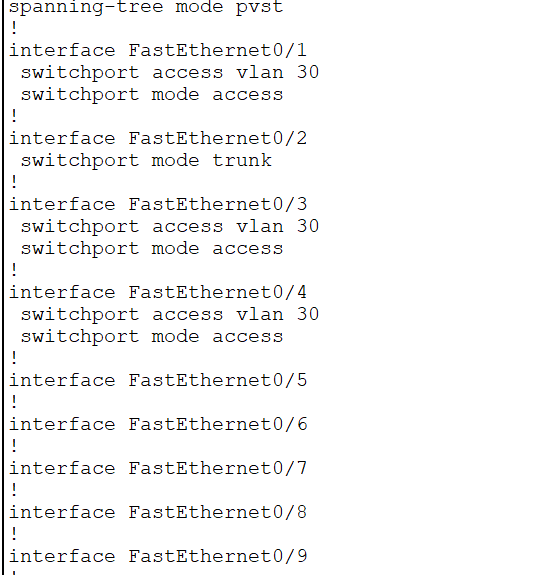
2.3.3: Branch 2



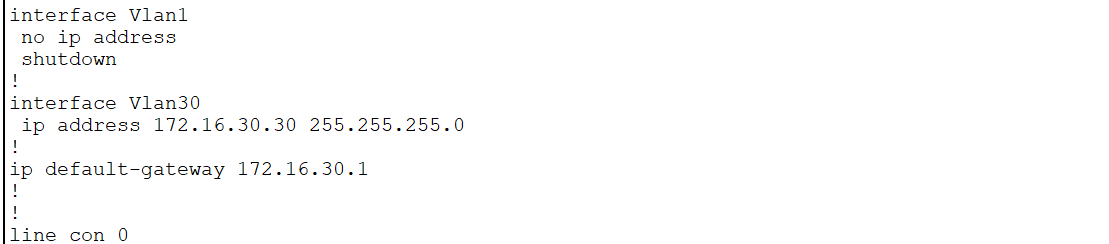
It contains four switches.

**Sw 1**

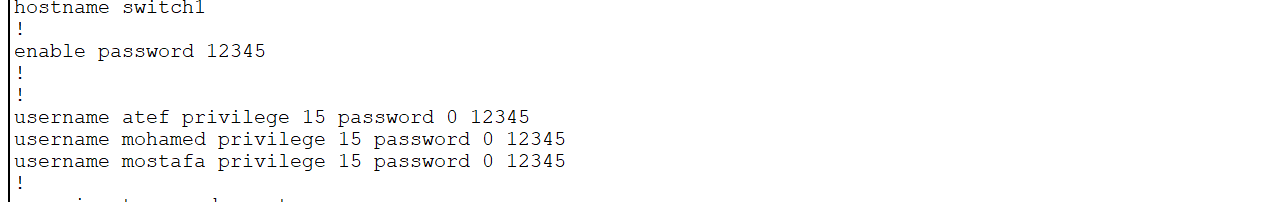
**Interface configuration**



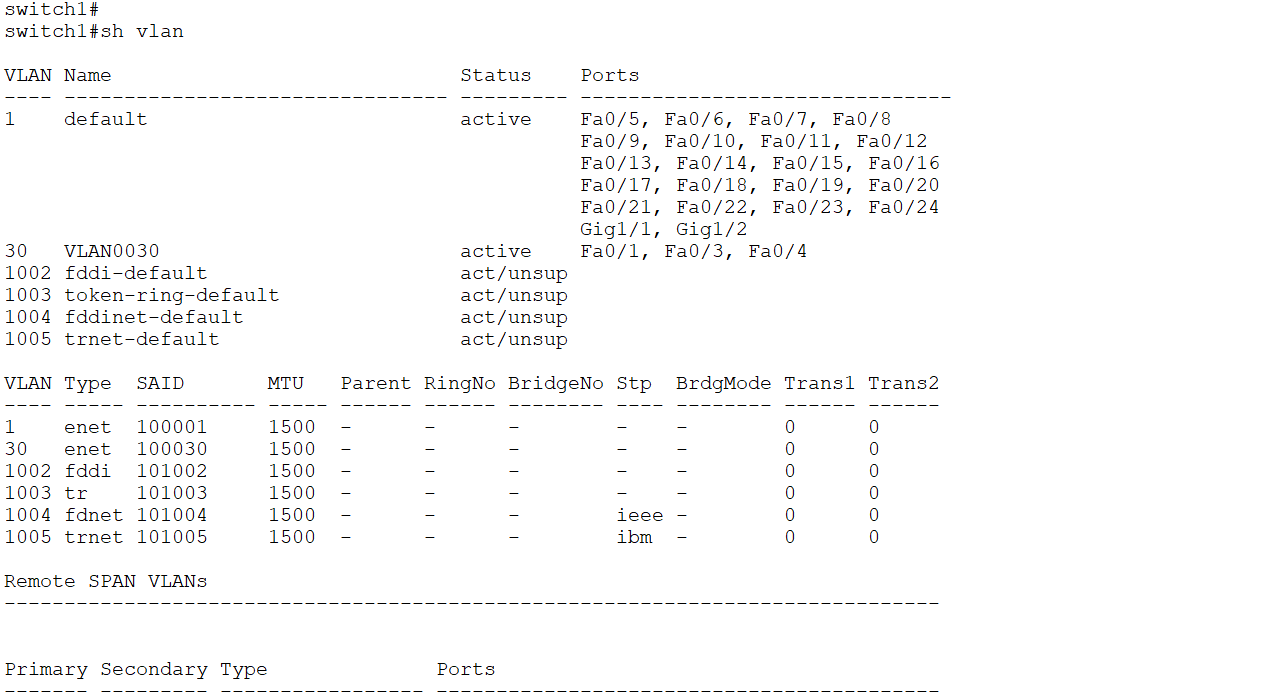
**Interface vlan configuration**



**Remote login**



**vlan configuration**



**Sw2**

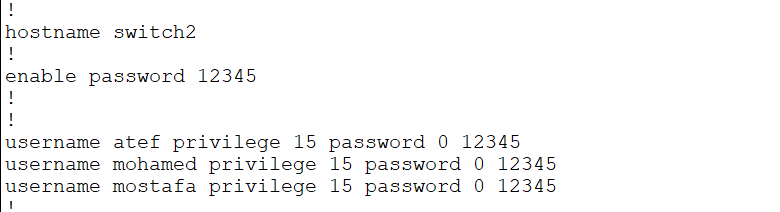
**Interface configuration**



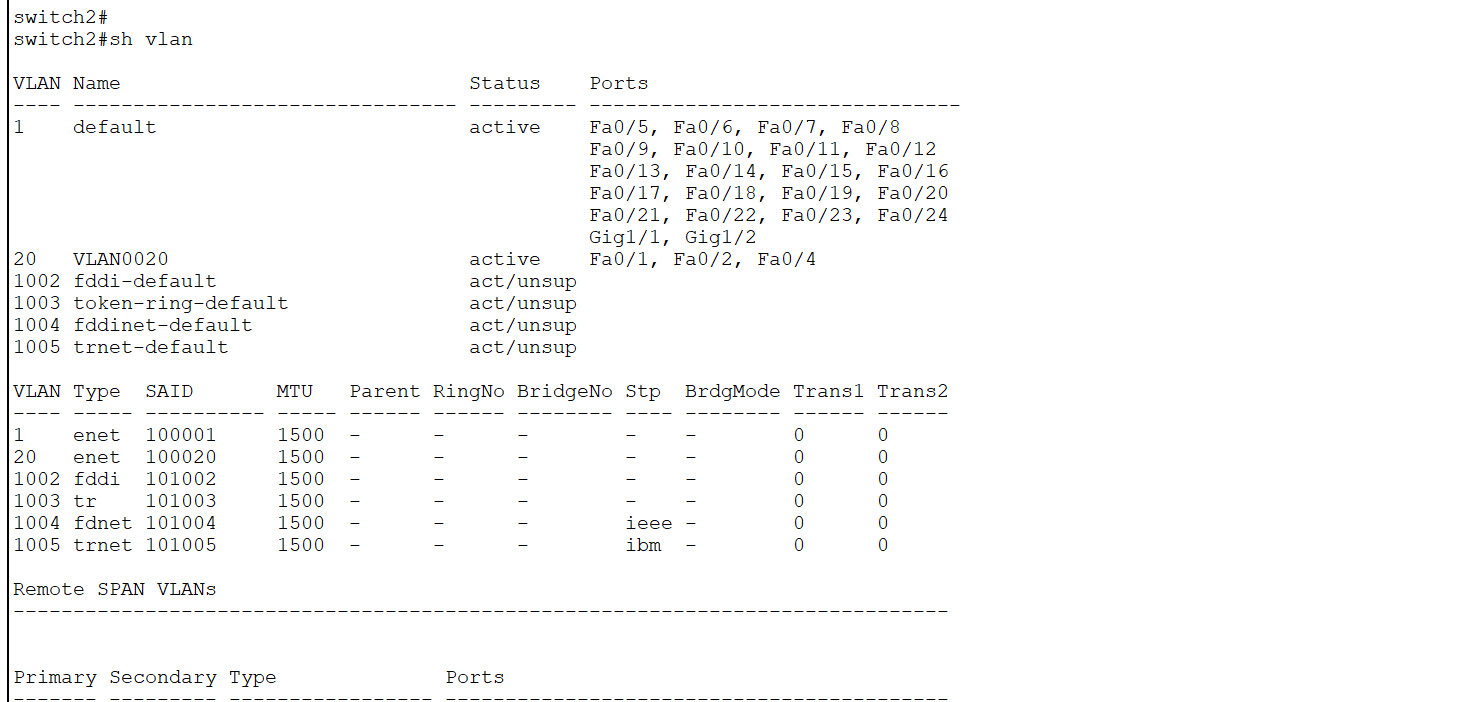
**Interface vlan configuration**



**Remote login**



**vlan configuration**

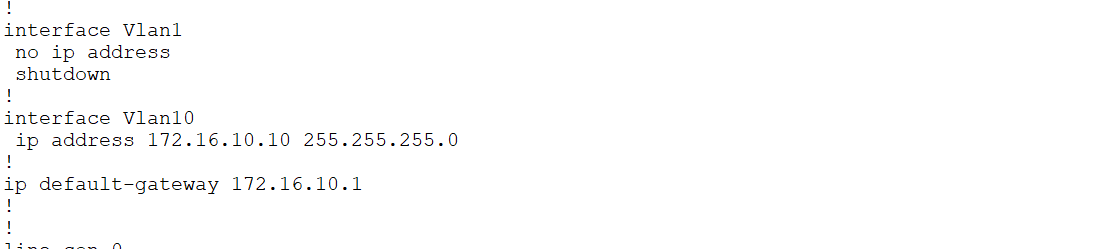


**Sw3**

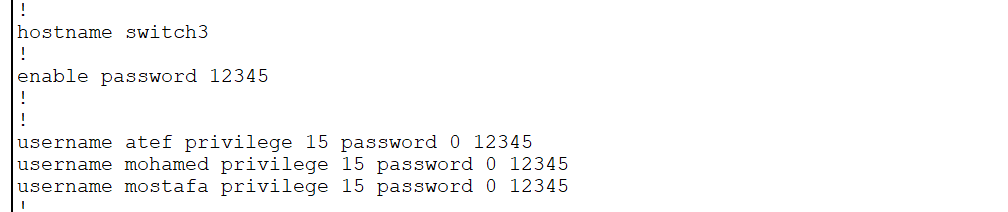
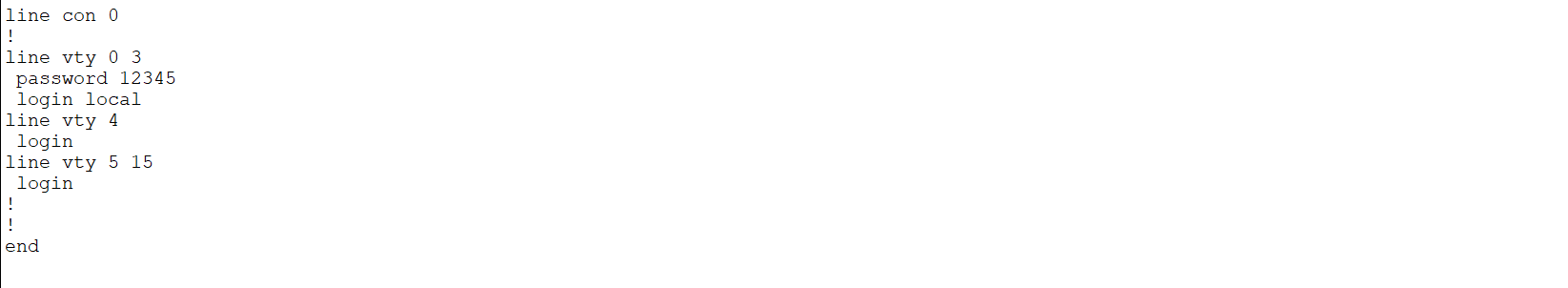
**Interface configuration**



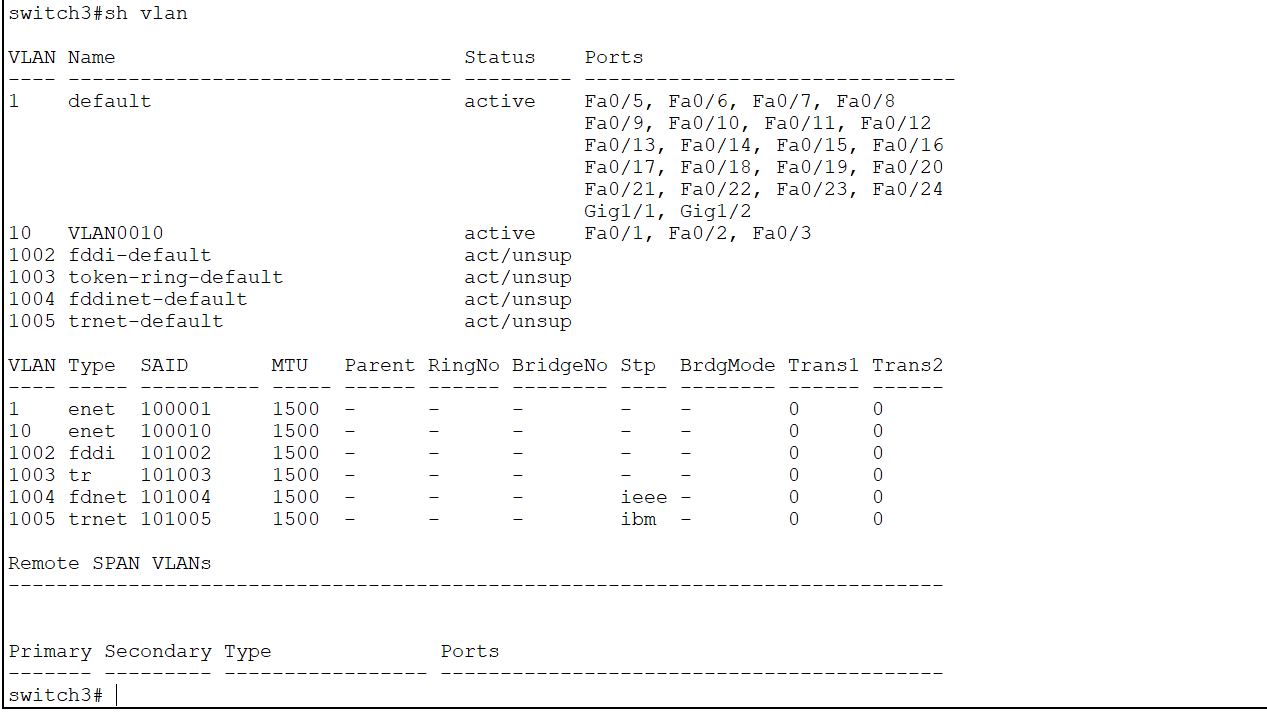
**Interface vlan configuration**



**Remote login**



**vlan configuration**



## Chapter 3 :  **Routing**

**3.1:Introduction**

**What is routing?**

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths. Routing is the process of selecting the best path using some predetermined rules.

**Why is routing important?**

Routing creates efficiency in network communication. Network communication failures result in long wait times for website pages to load for users. It can also cause website servers to crash because they can't handle a large number of users. Routing helps minimize network failure by managing data traffic so that a network can use as much of its capacity as possible without creating congestion.

**What is a router?**

A router is a networking device that connects computing devices and networks to other networks. Routers primarily serve three main functions.

**Path determination**

A router determines the path data takes when it moves from a source to a destination. It tries to find the best path by analyzing network metrics such as delay, capacity, and speed.

**Data forwarding**

A router forwards data to the next device on the selected path to eventually reach its destination. The device and router may be on the same network or on different networks.

**Load balancing**

Sometimes the router may send copies of the same data packet by using multiple different paths. It does this to reduce errors due to data losses, create redundancy, and manage traffic volume.

**How does routing work?**

Data moves along any network in the form of data packets. Each data packet has a header that contains information about the packet’s intended destination. As a packet travels to its destination, several routers might route it multiple times. Routers perform this process millions of times each second with millions of packets.

When a data packet arrives, the router first looks up its address in a routing table. This is similar to a passenger consulting a bus timetable to find the best bus route to their destination. Then the router forwards or moves the packet onward to the next point in the network.

For example, when you visit a website from a computer in your office network, data packets first go to the office network router. The router looks up the header packet and determines the packet destination. It then looks up its internal table and forwards the packet—either to the next router or to another device, such as a printer—within the network itself.

**What are the types of routing?**

There are two different types of routing, which are based on how the router creates its routing tables:

1-Static routing

In static routing, a network administrator uses static tables to manually configure and select network routes. Static routing is helpful in situations where the network design or parameters are expected to remain constant.

The static nature of this routing technique comes with expected drawbacks, such as network congestion. While administrators can configure fallback paths in case a link fails, static routing generally decreases the adaptability and flexibility of networks, resulting in limited network performance.

**2-Dynamic routing**

In dynamic routing, routers create and update routing tables at runtime based on actual network conditions. They attempt to find the fastest path from the source to the destination by using a dynamic routing protocol, which is a set of rules that create, maintain, and update the dynamic routing table.

The biggest advantage of dynamic routing is that it adapts to changing network conditions, including traffic volume, bandwidth, and network failure.

**What are the main routing protocols?**

A routing protocol is a set of rules that specify how routers identify and forward packets along a network path. Routing protocols are grouped into two distinct categories: interior gateway protocols and exterior gateway protocols.

Interior gateway protocols work best within an autonomous system—a network administratively controlled by a single organization. External gateway protocols better manage the transfer of information between two autonomous systems.

Interior gateway protocols

These protocols assess the autonomous system and make routing decisions based on different metrics, such as the following:

Hop counts, or the number of routers between the source and the destination

Delay, or the time taken to send the data from the source to the destination

Bandwidth, or the link capacity between the source and the destination

The following are some examples of interior gateway protocols.

Routing Information Protocol

The Routing Information Protocol (RIP) relies on hop counts to determine the shortest path between networks. RIP is a legacy protocol that no one uses today because it does not scale well for larger network implementation.

Open Shortest Path First protocol

The Open Shortest Path First protocol (OSPF) collects information from all other routers in the autonomous system to identify the shortest and fastest route to a data packet’s destination. You can implement OSPF using various routing algorithms or computer processes.

External gateway protocols

The Border Gateway Protocol (BGP) is the only external gateway protocol.

Border Gateway Protocol

BGP defines communication over the internet. The internet is a large collection of autonomous systems all connected together. Every autonomous system has autonomous system number (ASN) that it obtains by registering with the Internet Assigned Numbers Authority.

BGP works by keeping track of the closest ASNs and mapping destination addresses to their respective ASNs.

**What are routing algorithms?**

Routing algorithms are software programs that implement different routing protocols. They work by assigning a cost number to each link; the cost number is calculated using various network metrics. Every router tries to forward the data packet to the next best link with the lowest cost.

The following are some example algorithms.

Distance Vector Routing

The Distance Vector Routing algorithm requires all routers to periodically update each other about the best path information they have found. Each router sends information about the current assessment of the total cost to all known destinations.

Eventually, every router in the network discovers the best path information for all possible destinations.

Link State Routing

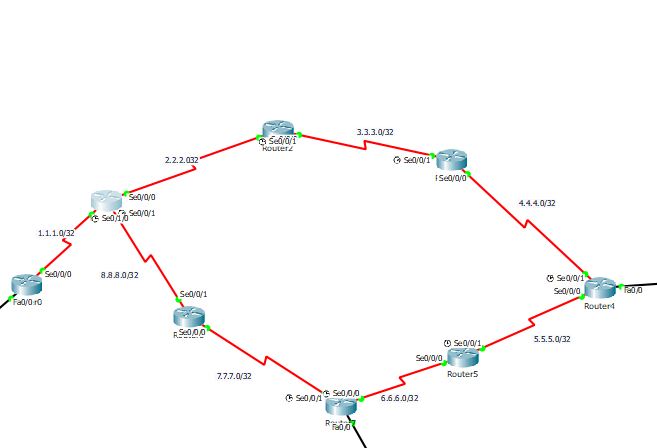
In Link State Routing, every router discovers all other routers in the network. Using this information, a router creates a map of the complete network and then calculates the shortest path for any data packet.

How has routing evolved?

Routing has evolved to meet the requirements of advances in network technology. Routing is no longer just about switching data packets between autonomous systems and the internet.

We now have cloud infrastructure with computing resources and hardware hosted by third-party cloud providers. These cloud resources are connected virtually to create a virtual network of resources that businesses can use to host and run applications. Many organizations now have hybrid networks that consist of both on-premises networks with internal hardware and cloud networks. Routers must route traffic between these internal networks, the internet, and the cloud

## 3.2:  routing configuration



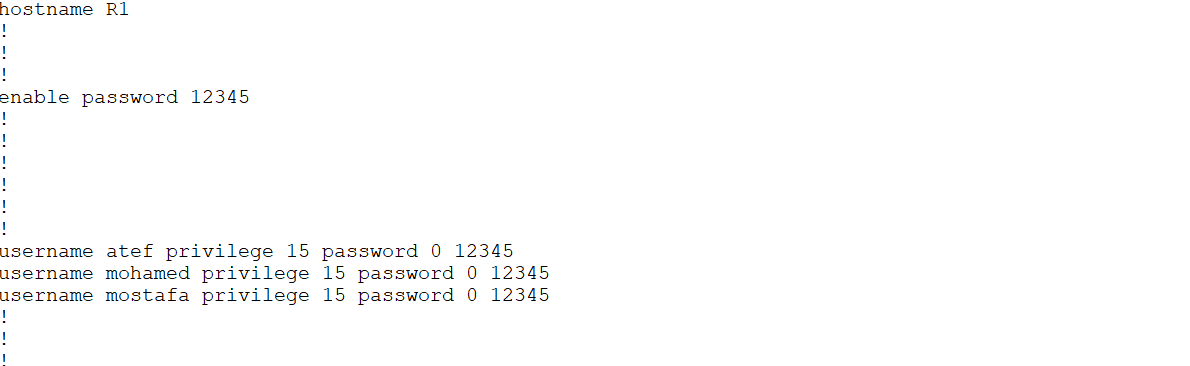
**Router 1**

**Interface configuration**

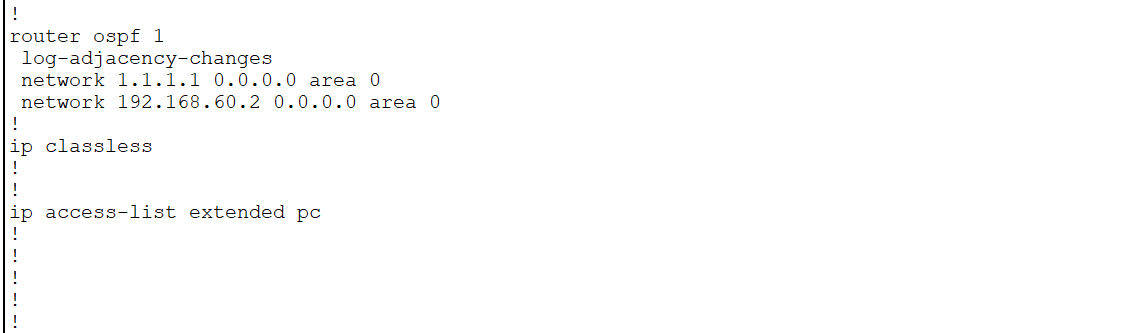
## interface conf

**Remote login**



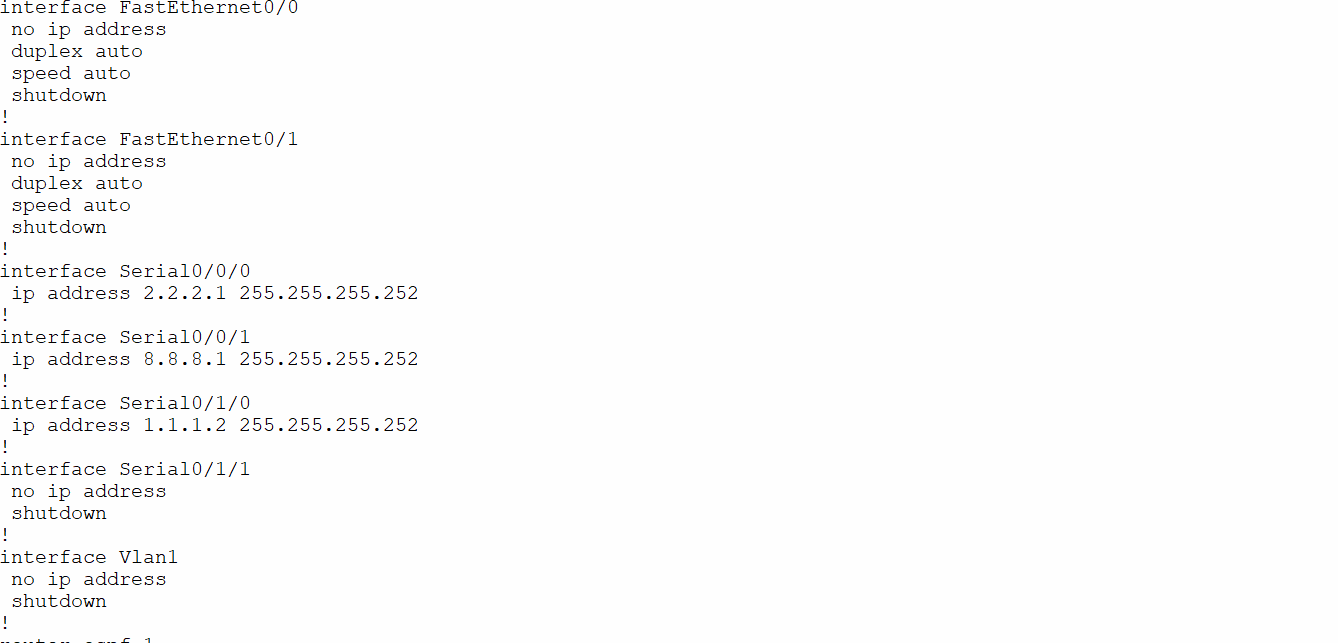


**ospf configuration**

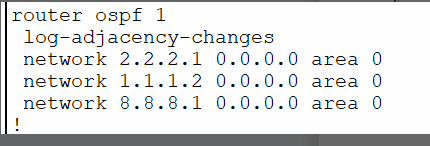


**Router 2**

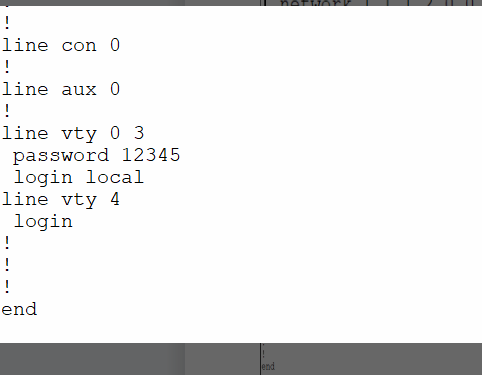
**Interface configuration**

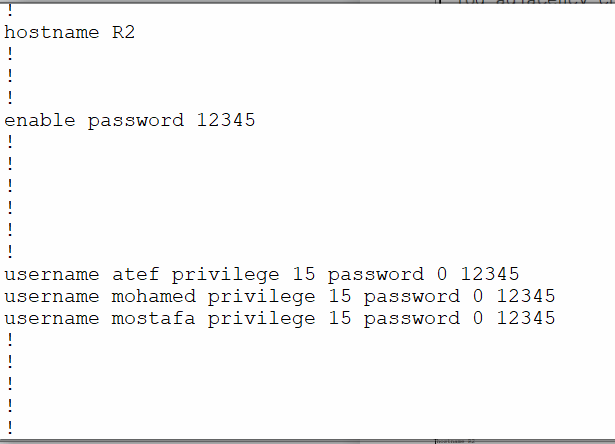


**ospf configuration**



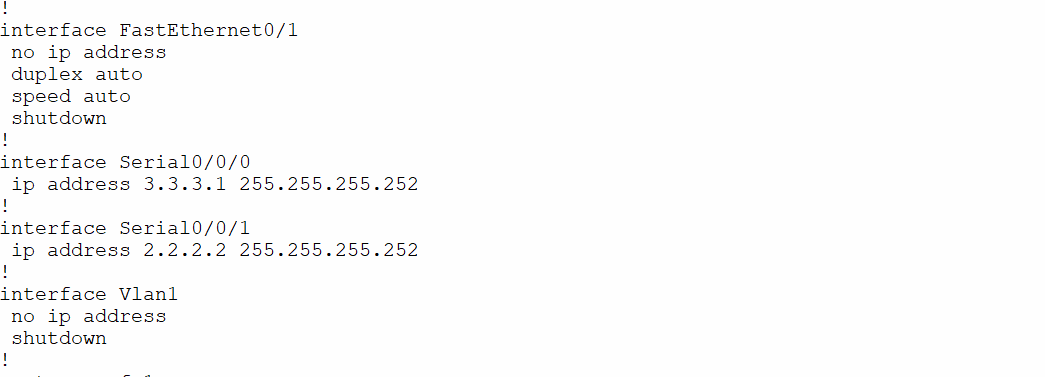
**Remote login**



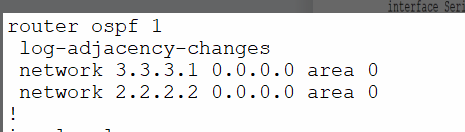


**Router 3**

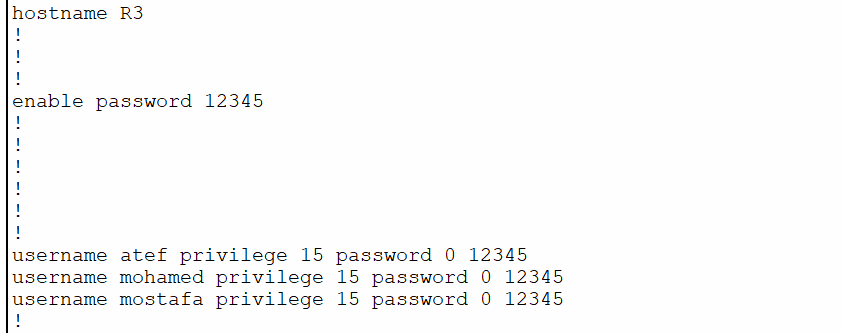
**Interface configuration**



**ospf configuration**

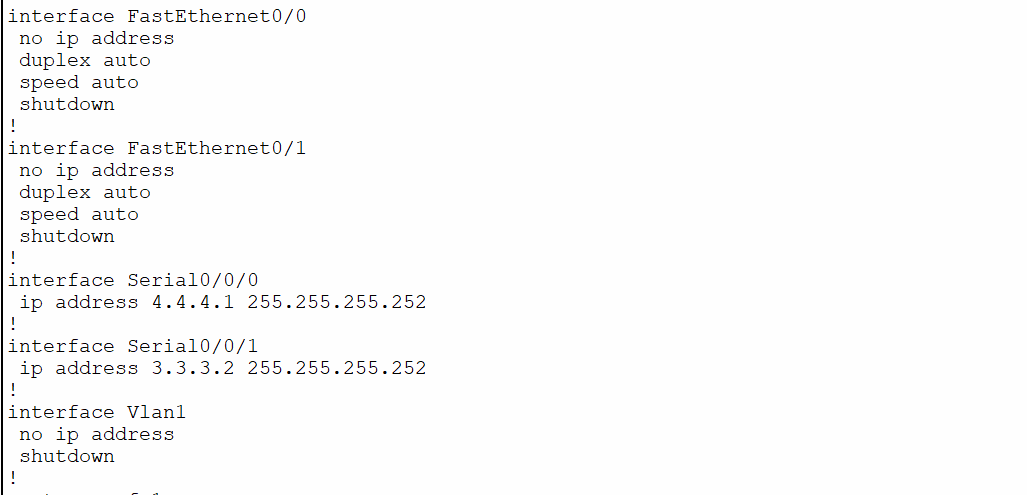


**Remote login**

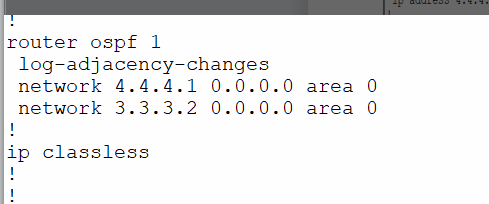


**Router 4**

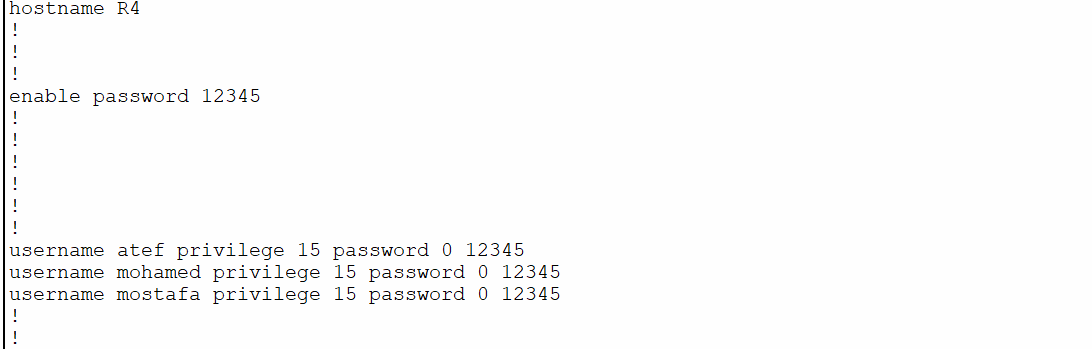
**Interface configuration**



**ospf configuration**

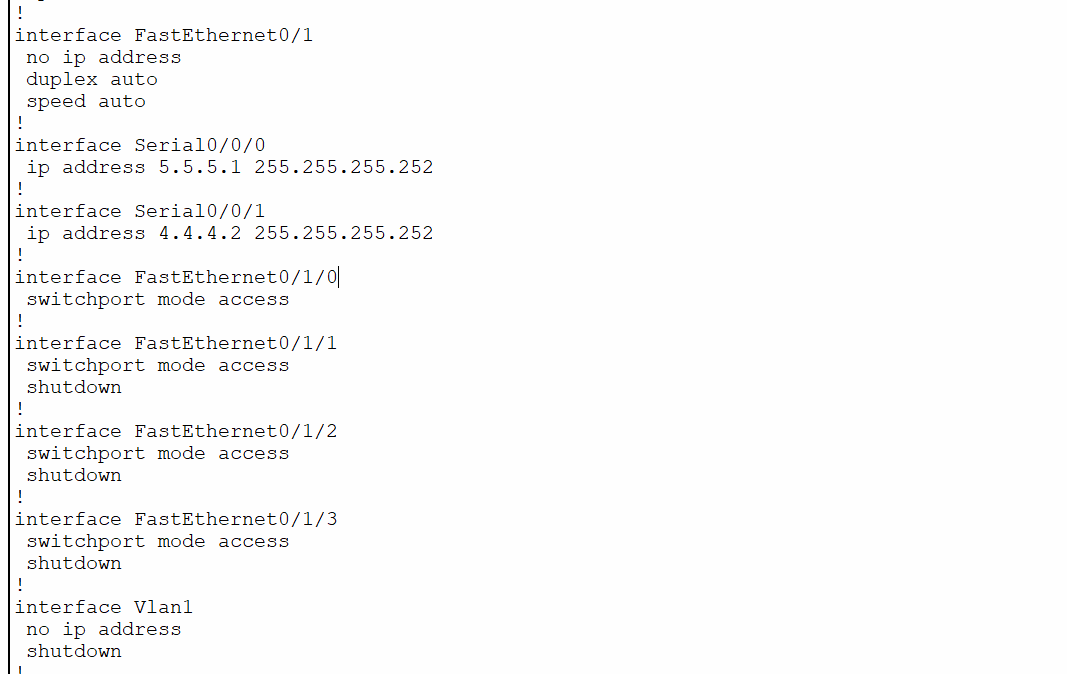


**Remote login**

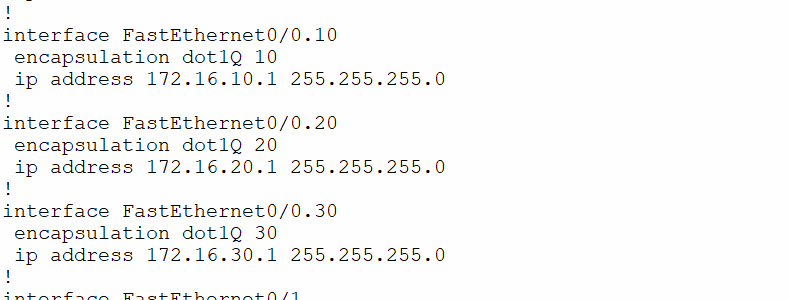


**Router 5**

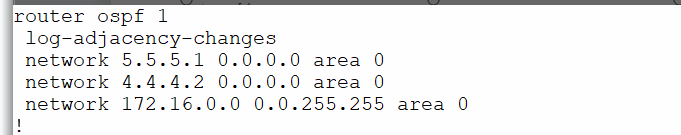
**Interface configuration**



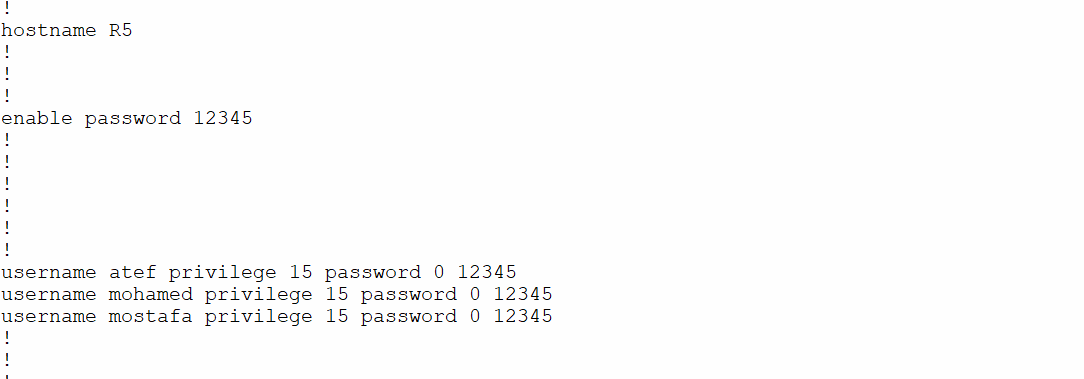
**Interface vlan configuration**



**ospf configuration**



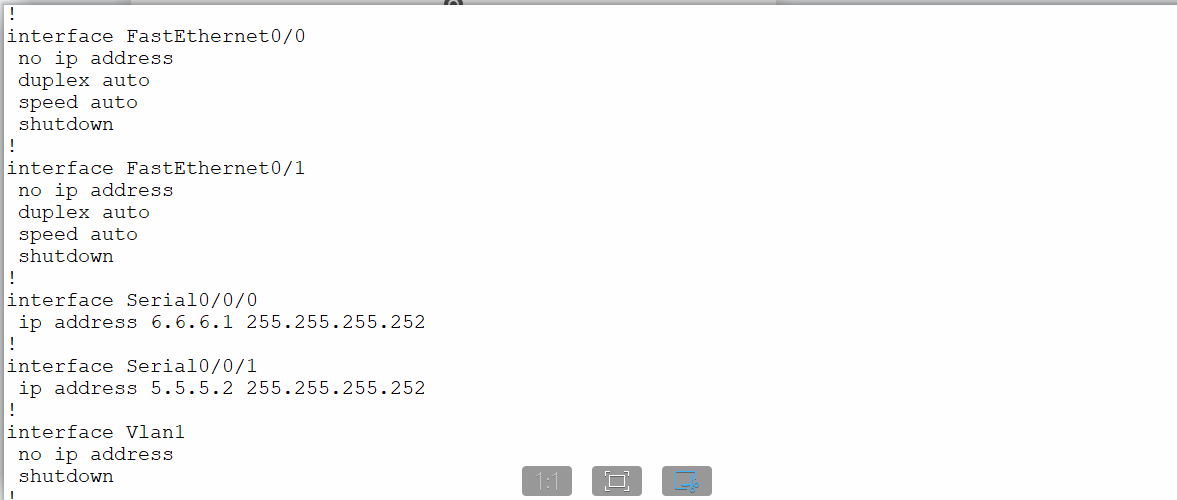
**Remote login**



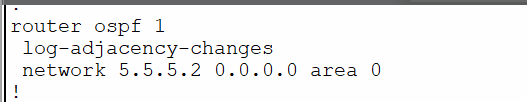


**Router6**

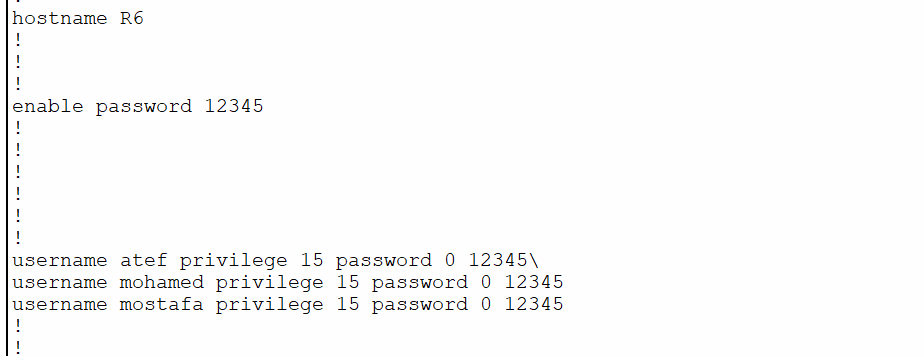
**Interface configuration**



**ospf configuration**



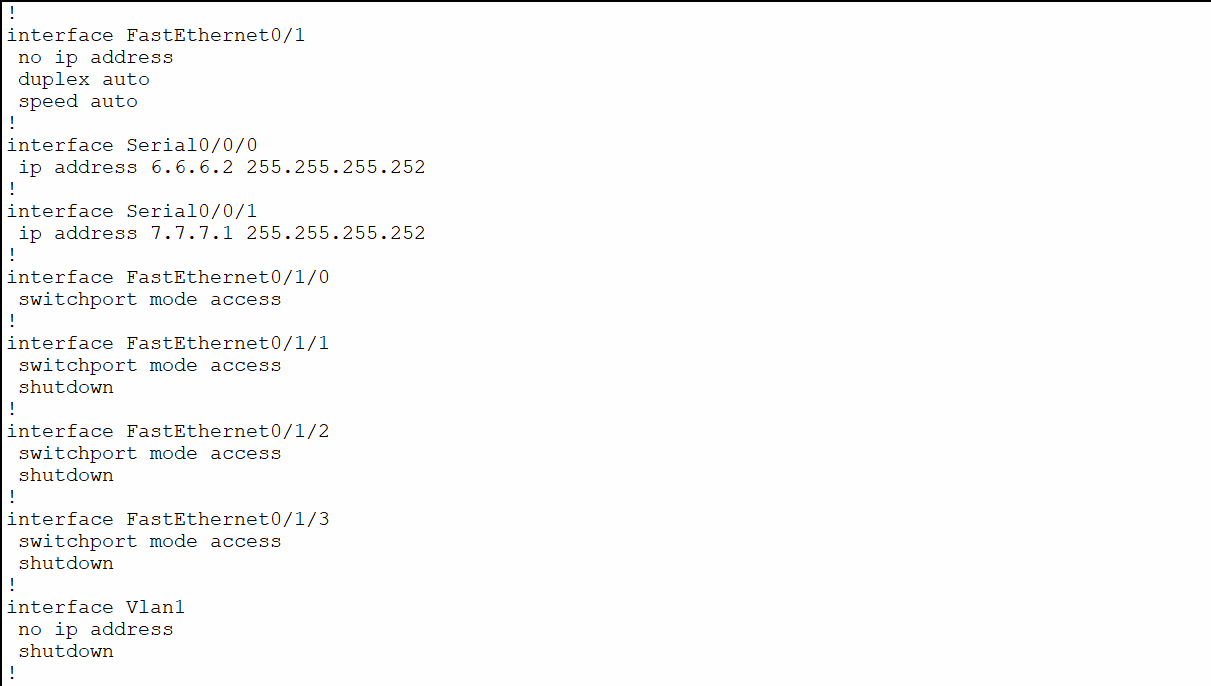
**Remote login**



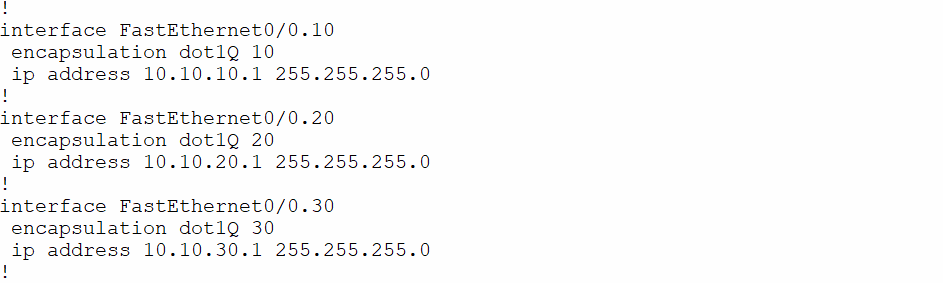


**Router 7**

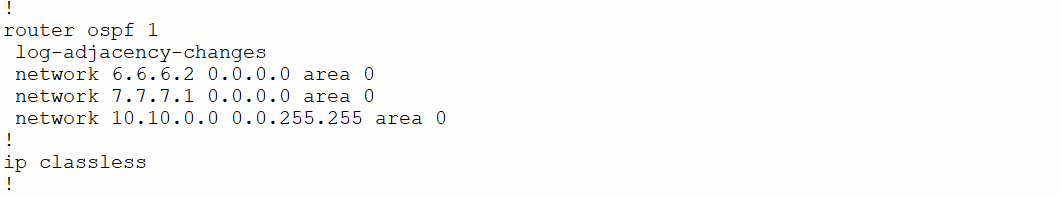
**Interface configuration**



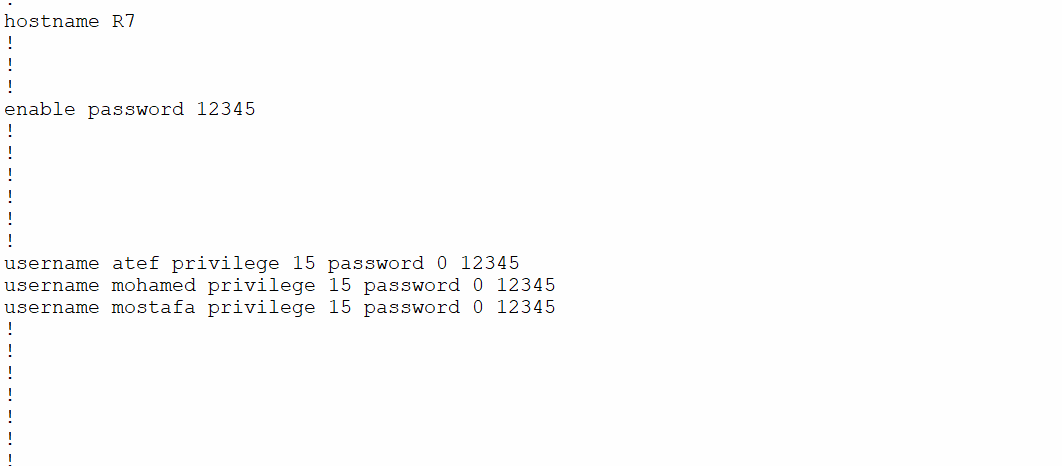
**Interface vlan configuration**



**ospf configuration**

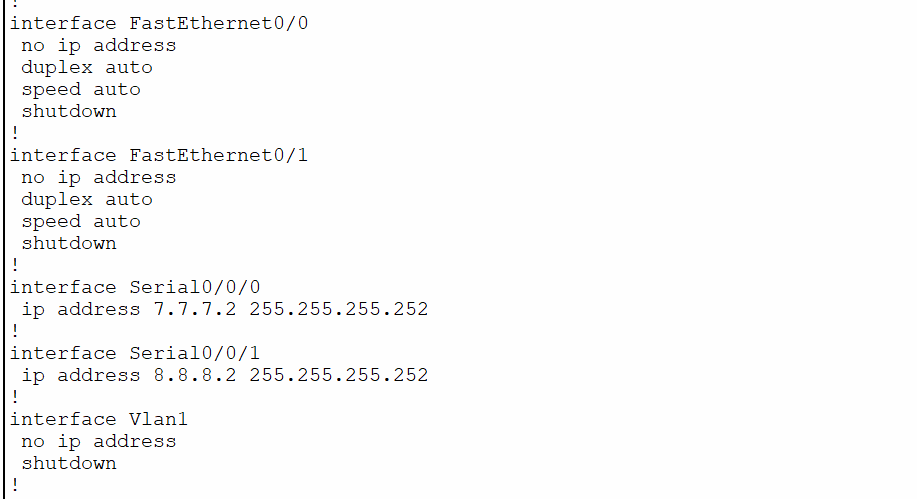


**Remote login**



**Router 8**

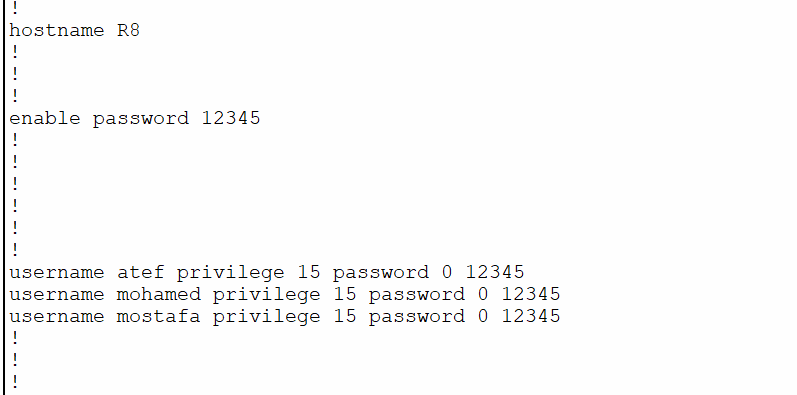
**Interface configuration**



**ospf configuration**



**Remote login**





# Chapter : ACL

4.1 : introduction

**What is an access control list (ACL)?**

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

Each system resource has a security attribute that identifies its access control list. The list includes an entry for every user who can access the system. The most common privileges for a file system ACL include the ability to read a file or all the files in a directory, to write to the file or files, and to execute the file if it is an executable file or program. ACL are also built into network interfaces and operating systems (OSes), including Linux and Windows. On a computer network, access control lists are used to prohibit or allow certain types of traffic to the network. They commonly filter traffic based on its source and destination.

**What are access control lists used for?**

Access control lists are used for controlling permissions to a computer system or computer network. They are used to filter traffic in and out of a specific device. Those devices can be network devices that act as network gateways or endpoint devices that users access directly.

On a computer system, certain users have different levels of privilege, depending on their role. For example, a user logged in as network administrator may have read, write and edit permissions for a sensitive file or other resource. By contrast, a user logged in as a guest may only have read permissions.

Access control lists can help organize traffic to improve network efficiency and to give network administrators granular control over users on their computer systems and networks. ACL can also be used to improve network security by keeping out malicious traffic.

**How do ACL work?**

Each ACL has one or more access control entries (ACE) consisting of the name of a user or group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups or roles, the access privileges are stated in a string of bits called an access mask. Generally, the system administrator or the object owner creates the access control list for an object.

**Types of access control lists :**

There are two basic types of ACL:

File system ACL manage access to files and directories. They give OSes the instructions that establish user access permissions for the system and their privileges once the system has been accessed.

Networking ACL manage network access by providing instructions to network switches and routers that specify the types of traffic that are allowed to interface with the network. These ACL also specify user permissions once inside the network. The network administrator predefines the networking ACL rules. In this way, they function similar to a firewall.

ACL can also be categorized by the way they identify traffic:

Standard ACL block or allow an entire protocol suite using source IP addresses.

Extended ACL block or allow network traffic based on a more differentiated set of characteristics that includes source and destination IP addresses and port numbers, as opposed to just source address.

Benefits of using an ACL

There are several benefits of using an ACL, including the following:

Simplified user identification. An access control list simplifies the way that users are identified. ACLs ensure that only approved users and traffic have access to a system.

Performance. ACL provide performance advantages over other technologies that perform the same function. They are configured directly on the routing device's forwarding hardware, so access control lists do not have a negative performance effect on routing devices. Compare this to a stateful inspection firewall, which is a separate piece of software that may cause performance degradation. Also, controlling network traffic enables networks to be more efficient.

Control. ACL can give administrators more granular control over user and traffic permissions on a network at many different points in the network. They help control access to network endpoints and traffic flowing between internal networks.

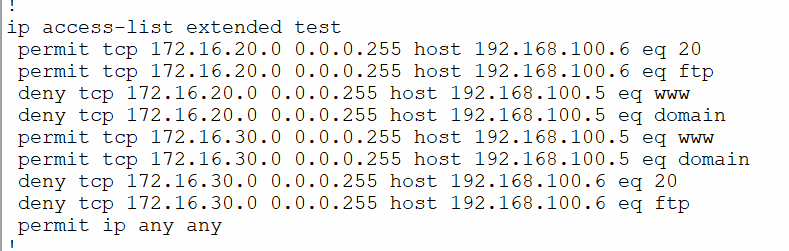
## 4.2:  ACL configuration

In this network, we have created an ACL on two routers

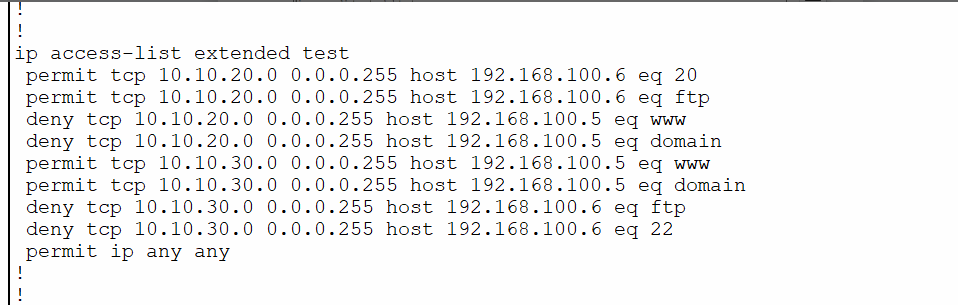
R5 and R7

R5





R7





**Conclusion**

In conclusion, a network is two or more computers connected together using atelecommunication system for the purpose of communicating and sharing resources. Without having anetwork, Companies would not be able to share resources and increase productivity more effectively.The WAN network allowed companies to use the Internet over large areas. This provided the company tohave meetings overseas by video conferencing and sharing data over the network. As you can see,Networks have many benefits to the end user. Weather your Network is Wired or Wireless, Networks arean important part of technology.

References:

Whit, Curt M.Data Communications and computer networks. 7th ed. N.p.: Cengage learning,2014. Web. 22 Sept. 2015

<https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL>

[What is routing? | IP routing | Cloudflare](https://www.cloudflare.com/learning/network-layer/what-is-routing/)