

MULTIMEDIA UNIVERSITY

ASSIGNMENT

**TRIMESTER 1, 2022/2023**

**TCS2351**

**NETWORK SECURITY**

| **No.** | **NAME** | **STUDENT ID** |
| --- | --- | --- |
| **1.** | **Nur Irdina Binti Hassan** | **1191202351** |
| **2.** | **Mohammad Harez Bin Hafez** | **1191202413** |
| **3.** | **Syafiq Zachery Bin Sharizal** | **1201303535** |

[**1. Introduction**](#_abkb7vopb3ss) **2**

[**2. Secure Network Requirements**](#_wdzi07xrfalt) **2**

[**3. Proposed Design**](#_rkx8be2tsr97) **7**

[**4. Implementation**](#_4v34amj9dzkm) **11**

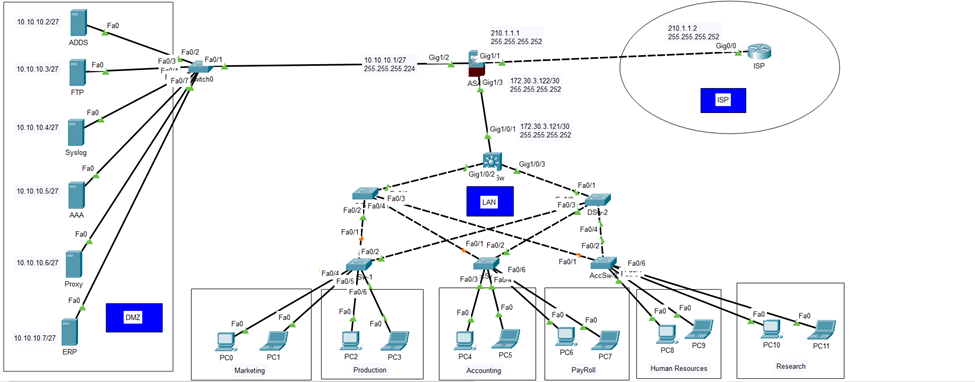
[**5. Conclusion**](#_zvjeerl1k1r) **13**

[**6. References**](#_2tdh8tijotyb)

**7. Working Device Configuration 13**

## Introduction

In this assignment, we have designed a complete network infrastructure for an enterprise that is secure. We divided our network into 3 main zones. One is OUTSIDE which is connected to the ISP and the other is INSIDE which is our LAN in which we have connected with endpoints and the last one is DMZ in which we have placed our servers which is accessible from the outside. Servers and resources in the DMZ are accessible from the internet, but the rest of the internal LAN remains unreachable. This approach provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data from the internet. The picture below shows the network topology that we have designed accordingly with the requirements given.



## Secure Network Requirements

A network without security is vulnerable to breaches, so various companies adopt different security measures. One common approach is the use of firewalls, like the Cisco ASA 5506, to secure the network. Our network has been divided into three zones: the INSIDE zone, which is our LAN and can easily communicate with the WAN; the OUTSIDE zone, which is our WAN connectivity with the ISP; and the DMZ zone, which is a secured zone for public servers. This separation prevents unauthorised access to our LAN from the public and secures our network from potential threats and attacks. To secure the company's network, we have implemented several important measures that provide adequate protection against possible cyber attacks. The following are the key security measures we have established:

**ADDS Server**

Active Directory Domain Services (ADDS) is a network Services Provider which provides different services and manages computers and allows system admin to organise the Data in logical Hierarchies.

**How it Works**

• We can customise our data to be organised to meet company needs.

• We can manage network services centralised from any computer or remotely as well.

• We configured DC as a backup server if our primary ADDS goes down then DC takes a primary rule.

• We can manage and create user data and credentials centralised.

• All the access of network resources are managed by ADDS and allow system admin to organise the data in hierarchical form.

**AAA Server (Authentication, Authorization and Accountability)**

• AAA stands for Authentication, Authorization and Accounting.

• AAA is a centralised management of users to access the network devices.

• AAA services allow setting up access control on Cisco Routers & Switches.

• When users attempt to login the network devices are verified by AAA.

• User management done on AAA without need to reconfigure each device.

• AAA provides flexibility and scalability, using privilege levels

• AAA servers can be RADIUS protocol or TACACS+ where the database is located.

**How It Works:**

• Cisco provides a number of ways to implement AAA.

• Two main protocols are TACACS Server and Radius Server. AAA with TACACS+:

• TACACS+ stands for Terminal Access Controller Access Control System Plus.

• TACACS+ is a Cisco proprietary protocol that is used to deliver AAA security services.

• TACACS+ uses TCP

• TACACS+ uses TCP port 49

• TACACS+ encrypts the entire communication

• TACACS+ treats Authentication, Authorization, and Accountability differently

• TACACS+ is Cisco proprietary protocol

• TACACS+ is a heavy-weight protocol consuming more resources

• TACACS+ supports 15 privilege levels

• Mainly used for Device Administration

AAA with RADIUS:

• RADIUS stands for Remote Authentication Dial in User Service.

• RADIUS is a security protocol that secures the network against unauthorised access.

• RADIUS uses UDP

• Uses ports 1812/1645 for authentication

• Uses ports 1813/1646 for accounting

• RADIUS encrypts passwords only

• RADIUS combines authentication and Authorization

• RADIUS is an open protocol

• RADIUS is a light-weight protocol consuming less resources

• RADIUS is limited to privilege mode

• Mainly used for Network Access

**Enterprise Resource Planning (ERP)**

Enterprise resource planning (ERP) is a platform which is use to manage and integrate the essential parts of their businesses. Many ERP software applications are critical to companies because they help them implement resource planning by integrating all the processes needed to run their companies with a single system.

**KEY POINTS**

• ERP software can integrate all of the processes needed to run a company.

• ERP solutions have evolved over the years, and many are now typically web-based applications that users can access remotely.

• Some benefits of ERP include the free flow of communication between business areas, a single source of information, and accurate, real-time data reporting.

• There are hundreds of ERP applications a company can choose from, and most can be customised.

• An ERP system can be ineffective if a company doesn't implement it carefully.

**How Does It Work**

ERP has evolved over the years from traditional software models that made use of physical client servers and manual entry systems to cloud-based software with remote, web-based access. The platform is generally maintained by the company that created it, with client companies renting services provided by the platform.

**Proxy Server**

A Proxy Server provides security services to secure network traffic and act like a network security gateway and it relies on Client and server environment. It helps and prevents a hacker from accessing a private network and then a different policy applied on traffic to allow or deny the users and traffic as a Firewall. It’s an intermediary server separating end users from the websites they browse

**How it Works:**

The Word Proxy Means “to act on behalf of another” as well as a “behalf of the users” all the users traffic goes and pass out from proxy server the proxy server evaluates the traffic shape and status then forward it to internet and when the response comes back then it check it with the same traffic as per user and application ID.

• Control and monitor internet usage of employees

• Bandwidth savings and improved speeds

• Added privacy benefits by obscuring your IP address and other personally-identifying information

• Improved security by encrypting web requests

• Gain access to blocked resources, circumventing restrictions imposed by companies or governments

**Use of Proxy Server**

• To control internet usage of employees and children

• Bandwidth savings and improved speeds

• Privacy benefits

• Improved security

• Get access to blocked resources

• Address Translation and Caching

• Application Level and Circuit Level

• Forward and Reverse Proxies

**FTP (File Transfer Protocol)**

• FTP stands for File Transfer Protocol.

• FTP is used to send & receive files from the remote device.

• FTP is a complete, session-oriented file transfer protocol.

• FTP depends on TCP, is connection oriented, and provides reliable control.

• FTP provides user authentication.

• FTP uses usernames and passwords for setup.

• Devices are required to have a username and password setup for FTP.

• FTP is faster when compared to TFTP.

• FTP uses two TCP ports 20 for sending data & 21 for sending control commands

**How it Works**

FTP is a File transfer protocol which we deploy on server and store any date then we will easily access from anywhere as well as remotely.

All companies use FTP services for data Store and transfer of multiple file as per Client or Company needs.

File transfer protocol (FTP) is a way to download, upload, and transfer files from one location to another on the Internet and between computer systems.

FTP enables the transfer of files back and forth between computers or through the cloud.

Users require an Internet connection in order to execute FTP transfers.

FTP is an essential tool for those who build and maintain websites.

Many FTP clients are free to download, although most websites already have the FTP built-in.

**VPN**

• VPN is a network term, which stands for Virtual Private Network.

• VPN allows creating secure connections to another network over the Internet.

• VPNs create tunnels that allow users and systems to connect securely.

• Virtual Private Network (VPN) is a secure private tunnel over an insecure path.

• There are different technologies available for Wide Area Network (WAN) connectivity.

• Main drawback of many Wide Area Network (WAN) connectivity solutions is "Cost".

• VPN is a Network Security Technology, to secure private network traffic over a public.

• VPN ensures Privacy for network data from the source device to the destination device.

• VPN ensures Data Integrity for network data from the source device to destination device.

• VPN using network security protocols like IPSec to provide Privacy and Data Integrity.

• IPSec VPN provides Data Confidentiality by encrypting the data at the sending device.

• IPSec VPN provides Data Confidentiality by decrypting the data at receiving end.

• IPSec VPN also provides Data Integrity by using Hashing Algorithms like MD5 and SHA.

• Cisco supports several types of VPN implementations on the ASA IPSec & SSL based.

• Virtual Private Network (VPN) technology relies on the concept of tunnelling.

• VPN tunnelling involves establishing and maintaining a logical network association.

• Public network is a network to which anyone can connect and anyone can use.

• Private network is any network to which access is restricted and not for public use.

**Cloud Computing**

Cloud Computing is a cloud based service over the internet all cloud based solutions are internet based and we access all cloud based services from anywhere. All network and system services are able to deploy on cloud. We have mainly two types of clouds: Private and Public Cloud. Private cloud is accessible internally not on the internet but Public cloud is accessible externally over the internet.

Private Cloud - Private cloud is used for On-Prem Services which is accessible internally like a Data Center Services.

Public Cloud – Public Cloud is used for Public services over the internet which is accessible from anywhere.

Cloud Models:

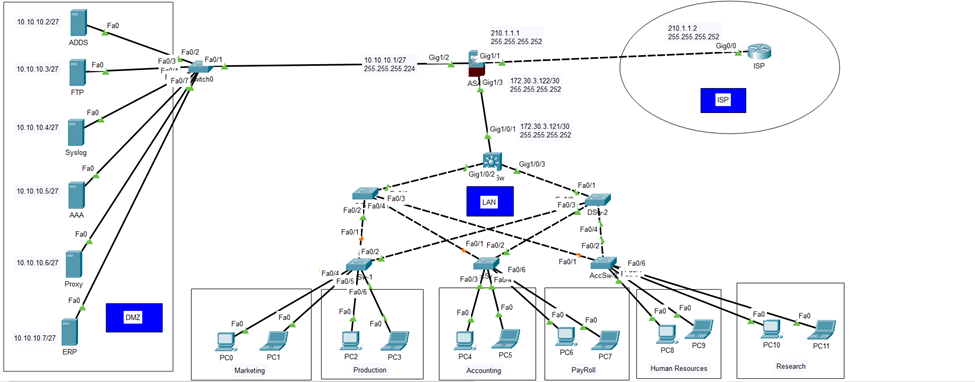
1 – IaaS – Infrastructure as a Service

2 – PaaS – Platform as a Service

3 – SaaS - Software as a Service

## 3. Proposed Design

The proposed design is for general network enterprises which need a secure network to operate. To create a secure network we proposed the network to have AD DS server, AAA, ERP, FTP, Syslog, Proxy, and VPN.



**IP Scheme**

We use IPv4 addressing scheme with submitted Networks using VLSM for each VLANs, P2P, and DMZ.

| **For DMZ (25 User Only)** | **WAN Connection with ISP** |
| --- | --- |
| IP Address------------------------10.10.10.1/27 (Class C)  Network Address----------------10.10.10.0  Usable Host IP Range------------10.10.10.1 - 10.10.10.30  Broadcast Address ---------------10.10.10.31  Total Number of Hosts------------32  Number of Usable Hosts-----------30  Subnet Mask---------------------------255.255.255.224  IP Type----------------------------------Private | IP Address-------------------------210.1.1.0  Network Address-----------------210.1.1.0  Usable Host IP Range-----------210.1.1.1 - 210.1.1.2  Broadcast Address---------------210.1.1.3  Total Number of Hosts----------4  Number of Usable Hosts--------2  Subnet Mask----------------255.255.255.252  IP Class-------------------------C  CIDR Notation----------------30  IP Type-------------------------Public |

**For LAN**

| **VLANs** | **Hosts Needed** | **Hosts Available** | **Network Address** | **Subnet Mask** | **Usable Range** |
| --- | --- | --- | --- | --- | --- |
| Production | 200 | 254 | 172.30.1.0/24 | 255.255.255.0 | 172.30.1.1 - 172.30.1.254 |
| Marketing | 150 | 254 | 172.30.2.0/24 | 255.255.255.0 | 172.30.2.1 - 172.30.2.254 |
| Accounting | 60 | 62 | 172.30.3.0/26 | 255.255.255.192 | 172.30.3.1 - 172.30.3.62 |
| Human Resources | 24 | 30 | 172.30.3.64/27 | 255.255.255.224 | 172.30.3.65 - 172.30.3.94 |
| Research | 12 | 14 | 172.30.3.96/28 | 255.255.255.240 | 172.30.3.97 - 172.30.3.110 |
| Payroll | 5 | 6 | 172.30.3.112/29 | 255.255.255.248 | 172.30.3.113 - 172.30.3.118 |
| P2P | 2 | 2 | 172.30.3.120/30 | 255.255.255.252 | 172.30.3.121 - 172.30.3.122 |

**Switching**

| **VLANs Names** | **VLAN ID** | **VLAN Network** | **Subnet Mask** | **VLAN Gateway** |
| --- | --- | --- | --- | --- |
| Dept-1 | 10 | 172.30.1.0/24 | 255.255.255.0 | 172.30.1.1 |
| Dept-2 | 20 | 172.30.2.0/24 | 255.255.255.0 | 172.30.2.1 |
| Dept-3 | 30 | 172.30.3.0/26 | 255.255.255.192 | 172.30.3.1 |
| Dept-4 | 40 | 172.30.3.64/27 | 255.255.255.224 | 172.30.3.65 |
| Dept-5 | 50 | 172.30.3.96/28 | 255.255.255.240 | 172.30.3.97 |
| Dept-6 | 60 | 172.30.3.112/29 | 255.255.255.248 | 172.30.3.113 |

**Interface Configuration**

| **Device** | **Interfaces** | **IP** | **Subnet Masks** | **Gateway** |
| --- | --- | --- | --- | --- |
| **Router - ISP** | Gi0/0 | 210.1.1.2/30 | 255.255.255.252 | NA |
| Loopback 1 | 8.8.8.8/32 | 255.255.255.255 | NA |
| **Cisco ASA** | Gig1/1 (OUTSIDE) | 210.1.1.1 | 255.255.255.252 | NA |
| Gig1/2 (DMZ) | 10.10.10.1/27 | 255.255.255.224 | NA |
| Gig1/3 (INSIDE) | 172.30.3.122/30 | 255.255.255.252 | NA |
| **L3 Switch** | Gig 1/0/1 | 172.30.3.121/30 | 255.255.255.252 | NA |
| Gig 1/0/2 | Trunk | NA | NA |
| Gig 1/0/3 | Trunk | NA | NA |
| **PC0 -** | NIC (VLAN- 10) | 172.30.1.2 | 255.255.255.0 | 172.30.1.1 |
| **PC1** | NIC (VLAN- 10 ) | 172.30.1.3 | 255.255.255.0 | 172.30.1.1 |
| **PC2** | NIC (VLAN- 20) | 172.30.2.2 | 255.255.255.0 | 172.30.2.1 |
| **PC3** | NIC (VLAN- 20 ) | 172.30.2.3 | 255.255.255.0 | 172.30.2.1 |
| **PC4** | NIC (VLAN- 30 ) | 172.30.3.2 | 255.255.255.192 | 172.30.3.1 |
| **PC5** | NIC (VLAN- 30 ) | 172.30.3.3 | 255.255.255.192 | 172.30.3.1 |
| **PC6** | NIC (VLAN- 40) | 172.30.3.66 | 255.255.255.224 | 172.30.3.65 |
| **PC7** | NIC (VLAN- 40) | 172.30.3.67 | 255.255.255.224 | 172.30.3.65 |
| **PC8** | NIC (VLAN- 50) | 172.30.3.98 | 255.255.255.240 | 172.30.3.97 |
| **PC9** | NIC (VLAN- 50 ) | 172.30.3.99 | 255.255.255.240 | 172.30.3.97 |
| **PC10** | NIC (VLAN- 60 ) | 172.30.3.114 | 255.255.255.248 | 172.30.3.113 |
| **PC11** | NIC (VLAN- 60 ) | 172.30.3.115 | 255.255.255.248 | 172.30.3.113 |

## 4. Implementation

The design of this network utilises a combination of tree and ring topology, which offers flexibility and scalability. The ring topology acts as the backbone and connects all branches of the tree topology, ensuring high availability and reliability. One router in the ring topology serves as the central hub, managing network traffic and acting as a single point of failure. Redundant routers are deployed to avoid this risk, and in case of a failure, provide automatic failover. The tree topology connects end devices, such as workstations, servers, and printers, and provides a hierarchical structure for easy management and maintenance. In summary, the design of the small business network combines the benefits of both tree and ring topologies to create a secure, robust, and scalable network infrastructure that meets the needs of the business and its end devices.

In the network topology, the following security prevention measures have been implemented:

1. VPN: To secure sensitive information transmitted between the DMZ and the internal network, a VPN is configured in the DMZ. The VPN acts as a secure intermediary and allows remote access for authorised users.
2. Firewall: An ASA firewall is implemented to filter incoming and outgoing network traffic based on rules set by network administrators.
3. IPS: The IPS is configured with security policies, placed inline with network traffic, and deployed to monitor all incoming and outgoing network traffic.
4. L2 Security: L2 security measures, such as ACLs, port security, and DAI, are chosen and deployed by configuring network switches and routers.
5. L3 Security: L3 security measures are deployed by configuring security policies and network routers.
6. Access Control: An access control system, such as RADIUS or TACACS+, is implemented to manage user authentication and authorization.
7. Encryption: Encryption technologies, such as SSL or TLS, are used to secure sensitive data transmitted over the network.
8. Antivirus and Anti-malware: Antivirus and anti-malware solutions are deployed on end devices and servers to protect against security threats.
9. Patch Management: Regular software and firmware updates are performed on all network devices to ensure network security by patching vulnerabilities.

## 5. Conclusion

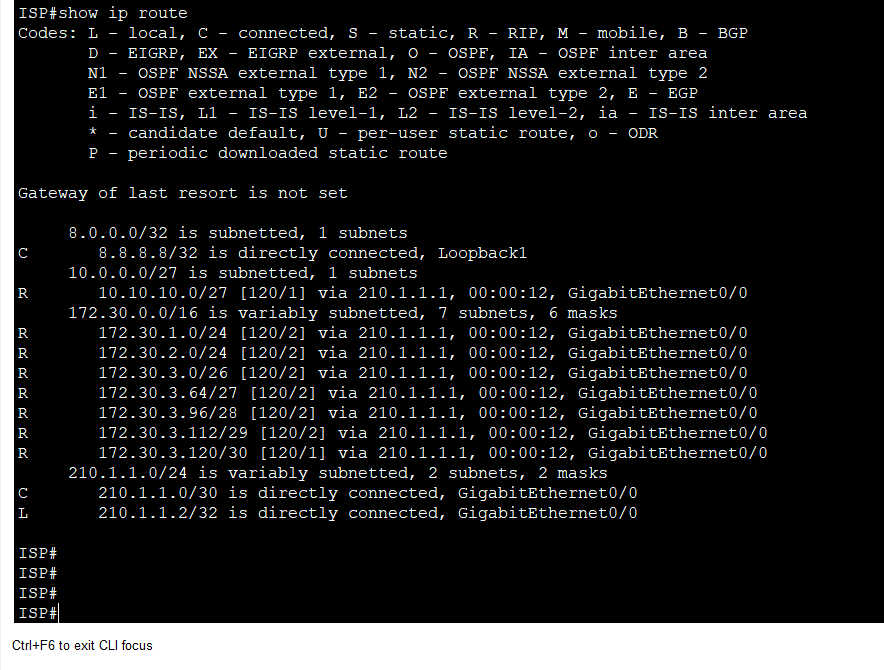
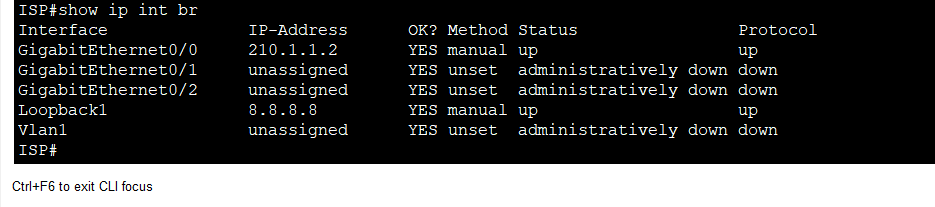
In this project, the network security is being updated by deploying various security solutions. ADDS server is used for user management and applying policies on users. Admin users are created on AAA server for management purposes. A syslog server is deployed for network analysis, and proxy servers are deployed to prevent harmful traffic and allow only authentic traffic. Firewall, FTP, and ERP solutions are also part of the security measures implemented in this project. All these services are managed centrally for ease of administration.

## 6. References

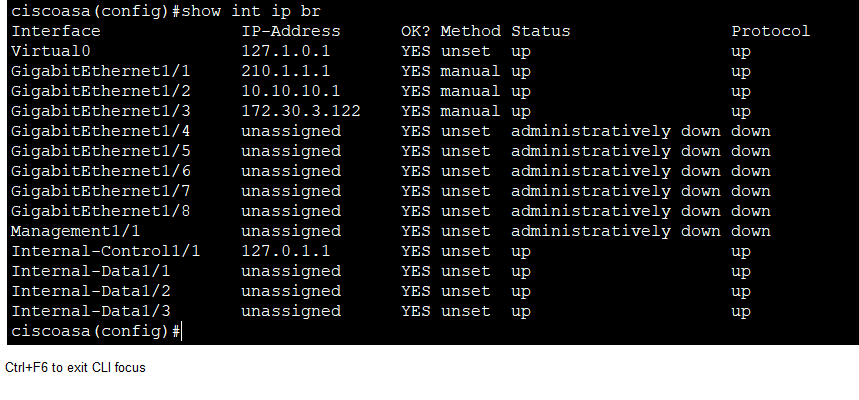
1. Corporation, M. (n.d.). What is ERP and why do you need it?| Microsoft Dynamics 365. Dynamics.microsoft.com. https://dynamics.microsoft.com/en-us/erp/what-is-erp/
2. Definition of proxy server. (n.d.). PCMAG. https://www.pcmag.com/encyclopedia/term/proxy-server
3. What is a Proxy Server and How Does it Work? (n.d.). Www.varonis.com. https://www.varonis.com/blog/what-is-a-proxy-server
4. Mitchell, C. (2020, June 23). File Transfer Protocol (FTP) Definition. Investopedia. https://www.investopedia.com/terms/f/ftp-file-transfer-protocol.asp
5. Chai, W. (2021). What is Cloud Computing? Everything You Need to Know. SearchCloudComputing. <https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing>

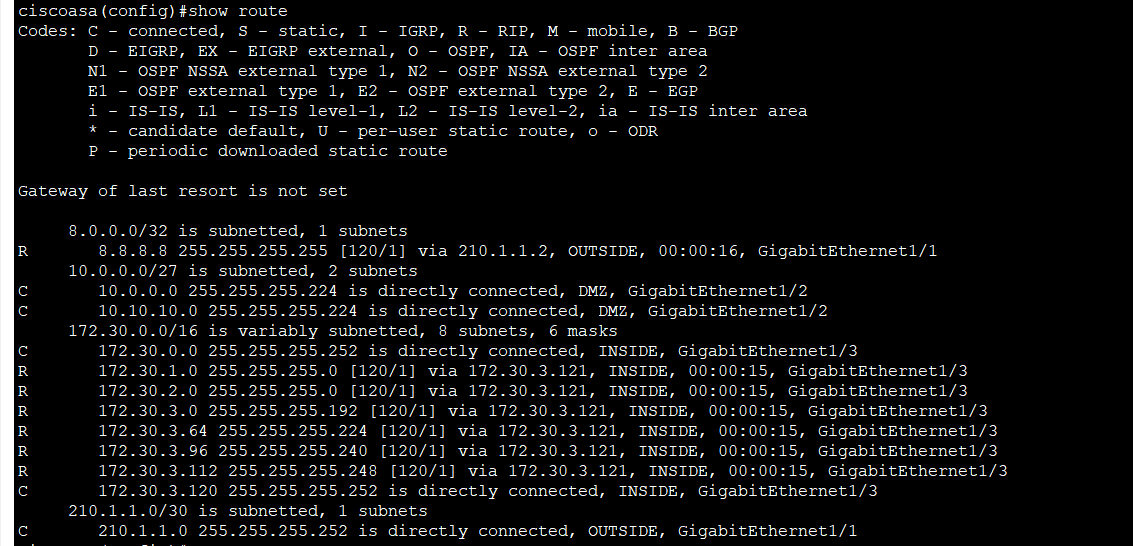
## 7. Working Device Configuration

**ISP Router**



**Cisco ASA**





**Core Switch**

