# **Project Documentation**

# **Addressing table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Subnet | Network Address | IP Range | Subnet mask | Broadcast | Allowed host number |
| 1 | 192.168.1.0 | 192.168.1.1-192.168.1.14 | 255.255.255.240 | 192.168.1.15 | 14 |
| 2 | 192.168.1.16 | 192.168.1.17-192.168.1.22 | 255.255.255.248 | 192.168.1.23 | 6 |
| 3 | 192.168.1.24 | 192.168.1.25-192.168.1.30 | 255.255.255.248 | 192.168.1.31 | 6 |
| 4 | 192.168.1.32 | 192.168.1.33-192.168.1.38 | 255.255.255.248 | 192.168.1.39 | 6 |
| 5 | 192.168.1.40 | 192.168.1.41-192.168.1.46 | 255.255.255.248 | 192.168.1.47 | 6 |
| 6 | 192.168.1.48 | 192.168.1.49-192.168.1.54 | 255.255.255.248 | 192.168.1.55 | 6 |
| 7 | 192.168.1.56 | 192.168.1.57-192.168.1.62 | 255.255.255.248 | 192.168.1.63 | 6 |
| 8 | 192.168.1.64 | 192.168.1.65-192.168.1.70 | 255.255.255.248 | 192.168.1.71 | 6 |
| 9 | 192.168.1.72 | 192.168.1.73-192.168.1.78 | 255.255.255.248 | 192.168.1.79 | 6 |
| 10 | 192.168.1.80 | 192.168.1.81-192.168.1.86 | 255.255.255.248 | 192.168.1.87 | 6 |
| 11 | 192.168.1.88 | 192.168.1.89-192.168.1.90 | 255.255.255.252 | 192.168.1.91 | 6 |
| 12 | 192.168.1.92 | 192.168.1.93-192.168.1.94 | 255.255.255.252 | 192.168.1.95 | 2 |
| 13 | 192.168.1.96 | 192.168.1.97-192.168.1.98 | 255.255.255.252 | 192.168.1.99 | 2 |
| 14 | 192.168.1.100 | 192.168.1.101-192.168.1.102 | 255.255.255.252 | 192.168.1.103 | 2 |
| 15 | 192.168.1.104 | 192.168.1.105-192.168.1.106 | 255.255.255.252 | 192.168.1.107 | 2 |
| 16 | 192.168.1.108 | 192.168.1.109-192.168.1.110 | 255.255.255.252 | 192.168.1.111 | 2 |
| 17 | 192.168.1.112 | 192.168.1.113-192.168.1.114 | 255.255.255.252 | 192.168.1.115 | 2 |
| 18 | 192.168.1.116 | 192.168.1.117-192.168.1.118 | 255.255.255.252 | 192.168.1.119 | 2 |

# **Assigning Ips**

1. We will start assigning Ips in the subnet with 14 hosts at Router 6.
   * Starting with the router we will configure the interface gig0/0/0
   * Assigned with IP 192.168.1.1 and no shutdown on the interface.
   * A computer screen shot of a computer code

     Description automatically generatedThen configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.
2. We will start assigning Ips in the subnet with 6 hosts at Router 5.
   * Starting with the router we will configure the interface gig0/0/0
   * Assigned with IP 192.168.1.17 and no shutdown on the interface.
   * A white background with black text

     Description automatically generatedThen configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.

A screen shot of a computer

Description automatically generated

1. We will start assigning Ips in the subnet with 6 hosts at Router 8.
   * Starting with the router we will configure the interface gig0/0/0
   * Assigned with IP 192.168.1.25 and no shutdown on the interface.
   * A screenshot of a computer screen

     Description automatically generatedThen configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.
2. We will start assigning Ips in the subnet with 6 hosts at Router 3(gig0/0/0).
   * Starting with the router we will configure the interface gig0/0/0
   * Assigned with IP 192.168.1.33 and no shutdown on the interface.
   * Then configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.

A screenshot of a computer

Description automatically generated

6. We will start assigning Ips in the subnet with 6 hosts at Router 3(gig0/0/1).

* + Starting by the router we will configure the interface gig0/0/1
  + Assigned with IP 192.168.1.41 and no shutdown on the interface.
  + A screenshot of a computer

    Description automatically generatedThen configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.

7. We will start assigning IPs in the subnet with 6 hosts at Router 0(gig0/0/0).

* + Starting with the router we will configure the interface gig0/0/0
  + Sub-interfaces will be applied on this router gig0/0/0.10 and   
    gig 0/0/0.20
  + Assigned with IPs 192.168.1.49 and 192.168.1.57 (static) and no shutdown on the interface gig0/0/0 itself.

A screenshot of a computer program

Description automatically generated

A close-up of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

8. We will start assigning Ips in the subnet with 6 hosts at Router 4(gig0/0/0).

* Starting with the router we will configure the interface gig0/0/0
* Assigned with IP 192.168.1.65 and no shutdown on the interface.
* Then configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.

A computer screen shot of a computer

Description automatically generated

9. We will start assigning Ips in the subnet with 6 hosts at Router 4(gig0/0/1).

* + Starting by the router we will configure the interface gig0/0/1
  + Assigned with IP 192.168.1.73 and no shutdown on the interface.
  + Then configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.

A screenshot of a computer

Description automatically generated

10. We will start assigning Ips in the subnet with 6 hosts at Router 2(gig0/0/0).

* Starting by the router we will configure the interface gig0/0/0
* Assigned with IP 192.168.1.81 and no shutdown on the interface.
* Then configuring a DHCP pool on the router to assign the machines in the subnet IPs automatically as shown in the following screenshot.

A screenshot of a computer program

AI-generated content may be incorrect.

10. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

11. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A white background with black text

Description automatically generatedA screen shot of a computer

Description automatically generated

12. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A number on a white background

Description automatically generated

A screen shot of a computer

Description automatically generated

13. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A close up of numbers

Description automatically generated

A close-up of numbers

Description automatically generated

14. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A screen shot of a computer

Description automatically generated

A white background with black numbers and letters

Description automatically generated

15. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A number on a white background

Description automatically generated

A close-up of numbers

Description automatically generated

16. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A close-up of numbers

Description automatically generated

A white background with black text

Description automatically generated

17. Configuring and assigning routers that are directly connected together, and these subnets will only require 2 IPs, so our mask will be /30 (255.255.255.252)

A close up of numbers

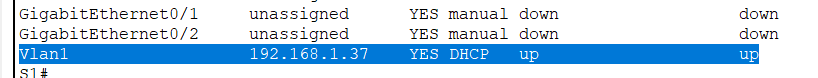
Description automatically generated

A white background with black numbers and letters

Description automatically generated

**Enabling the DHCP service on every switch**

Example on S1

A black text on a white background

AI-generated content may be incorrect.

# **Basic configuration**

**Routers**

* Setting a host name for each router
* Configuring enable password for each router EBHAM (it’s the first letter of our names)
* Securing console line with the password EBHAMcon
* Securing vty lines with the password EBHAMvty
* Encrypt the passwords & setting min-length for more security
* Adding the logging synchronous command to synchronize system messages (like debug or syslog outputs) with the command line, so that those messages don’t interrupt or overwrite the commands we’re typing.
* Saving the configuration

Example at router1

A screenshot of a computer program

AI-generated content may be incorrect.

A black text on a white background

AI-generated content may be incorrect.

A white background with black text

AI-generated content may be incorrect.

**Switches**

* Setting a host name for each router
* Configuring enable password for each router EBHAM (it’s the first letter of our names)
* Securing console line with the password EBHAMcon
* Securing vty lines with the password EBHAMvty
* Encrypt the passwords
* Adding the logging synchronous command to synchronize system messages (like debug or syslog outputs) with the command line, so that those messages don’t interrupt or overwrite the commands we’re typing.
* Saving the configuration

A screenshot of a computer program

AI-generated content may be incorrect.Example at switch1

A screenshot of a computer program

AI-generated content may be incorrect.

# **Routing using OSPF**

* Starting by activating OSPF service on the router
* Telling OSPF which interfaces/networks to advertise
* If there is an interface connected to end devices, we will make it passive interface to avoid unnecessary data exchange

A screenshot of a computer

AI-generated content may be incorrect.Example on R1

Example on R6

A screen shot of a computer error

AI-generated content may be incorrect.

* IP route OSPF on each router for verification

1. R0

A screen shot of a computer

Description automatically generated

1. A black text on a white background

   AI-generated content may be incorrect.R1
2. A white background with black numbers and letters

   AI-generated content may be incorrect.R2
3. R3

A screenshot of a computer screen

AI-generated content may be incorrect.

1. A white text with black numbers

   AI-generated content may be incorrect.R4
2. A screenshot of a computer code

   AI-generated content may be incorrect.R5
3. A white background with black numbers and letters

   AI-generated content may be incorrect.R6
4. A black text on a white background

   AI-generated content may be incorrect.R7
5. R8

A screenshot of a computer code

AI-generated content may be incorrect.

# **Routing Protocol Authentication**

* Now that we have configured the routing protocol there will be some risks we have to avoid

**Routing Protocol Spoofing:**

1. **Routing loops  Redirect traffic to create routing loops**.
2. **Sniffing  Redirect traffic through insecure links for monitoring.**
3. **Drop traffic  Redirect traffic to discard it**.
4. **Cause a Denial-of-Service (DoS)**  sending false routing information

**Routing Protocol Authentication**

* **Protect routing protocols from spoofing and unauthorized updates.**
* **OSPF supports two authentication types: MD5 and SHA.**
* **We will use the strongest between them (SHA)**

1. **Configuring a key-chain named OSPF-SECURE with a key-string (password) EBHAM**
2. **Choosing the encryption protocol SHA256**
3. **Apply the key-chain to every interface in the router**

A screenshot of a computer program

AI-generated content may be incorrect.**Example on R1**

* We can see the p2p connection between the interface we encrypted, and its neighbor went down. It will return to full once we encrypt the other interface

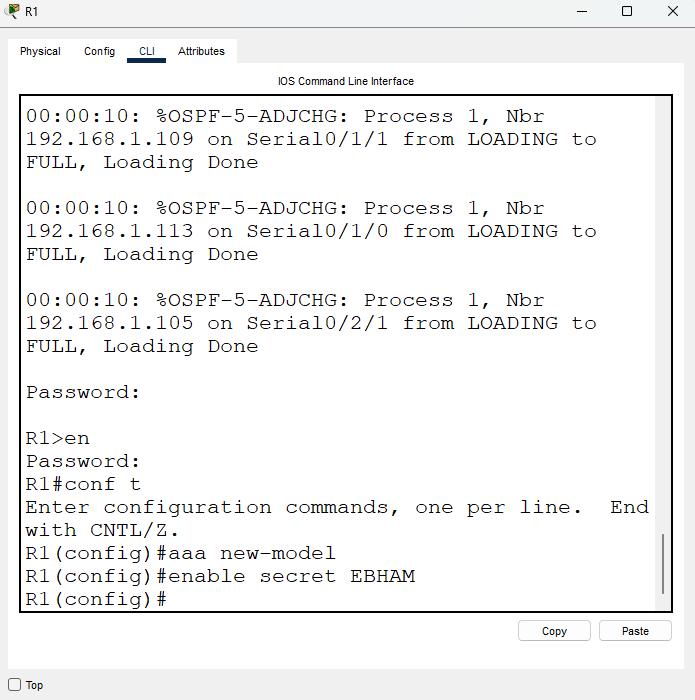
# **Views on Router**

I intend to create NTI and VIEWIT views, and every view has allowed commands

1-**create** **username and its password (EBHAM), create aaa-model and give a password (EBHAM):**

A screenshot of a computer

AI-generated content may be incorrect.



**2-go into root view and create the NTI view and give it a password (EBHAM):**

A white background with text

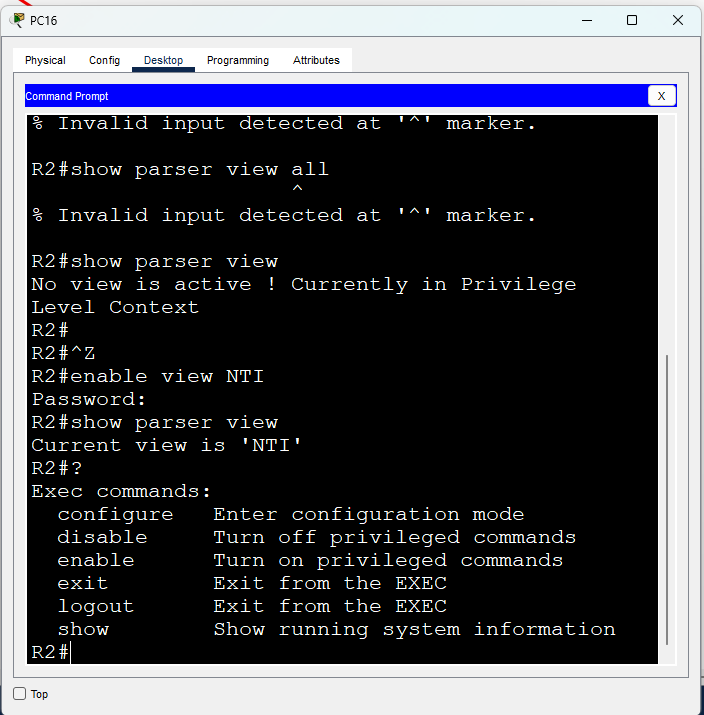
AI-generated content may be incorrect.

**3- give the allowed command that we need on NTI view:**

A screenshot of a computer

AI-generated content may be incorrect.

**To test it we will go to a pc in the same network and do “telnet 192.168.1.81” to test the view:**



**Now we will create VIEWIT view with telnet, ssh , ping , show ip route:**

**1- go to root view and create VIEWIT with It password(EBHAM):**

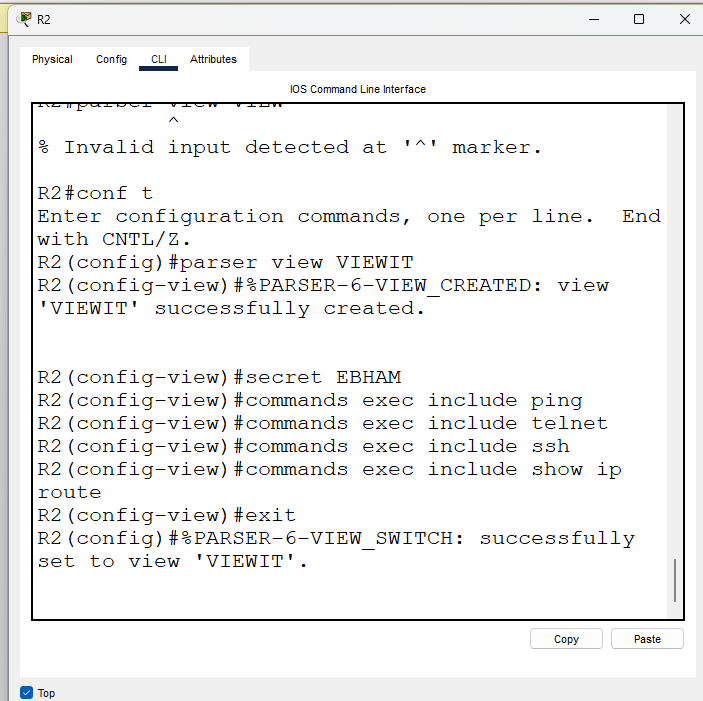
A black text on a white background

AI-generated content may be incorrect.

**A white background with black text

AI-generated content may be incorrect.**

**2-give the intended commands:**

****

**To test it we will go to any pc in the same network and “telnet 192.168.1.81” to test the view:**

A screenshot of a computer

AI-generated content may be incorrect.

# **ACL (Access Control List) on R6**

**Router 6**

**We need to create an ACL that allows only PC6, PC7, PC17 to establish ssh session on the router using the VTY lines**

* A close up of black text

  AI-generated content may be incorrect.Creating username (baraa) and password (EBHAM) for the remote login
* A white screen with black text

  AI-generated content may be incorrect. Enabling SSH protocol on the router so the PCs can establish the sessions
* Creating ACL that allows only the IPs of the PCs above

A black text on a white background

AI-generated content may be incorrect.

* Applying the ACL to VTY lines. Adding In the VTY lines login local command to use the username and password we created, and also enabling the SSH connection

A screen shot of a computer code

AI-generated content may be incorrect.

* A white screen with black text

  AI-generated content may be incorrect.Show command to make sure of everything
* A screenshot of a computer screen

  AI-generated content may be incorrect.Testing from the PCs

# **ACL (access control list) on R8**

* Our goal here is to make an ACL on Router 8 to permit PCs 14 and 19 to be able to access the WEB server on the following services (HTTP, HTTPS, FTP), also we will add a rule for ICMP requests.
* First thing to be done is to give the PCs that will be in the ACL static IPs as the DHCP server assign IPs automatically and they are changed frequently, and we don’t the IP to be changed.



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Also, we will give the WEB server a static IP.



A screenshot of a computer

Description automatically generated

* Now we will start adding the rules for the HTTP/HTTPS, FTP connections to the WEB server and the ICMP requests to only permit the connection from PC9 and PC14.

A screenshot of a computer

Description automatically generated

# **NTP**

1. **Giving the DNS server a static IP and excluding it from the DHCP range so it doesn’t change.**

**A black text on a white background

AI-generated content may be incorrect.**

1. **Manually setting the time on the NTP server and enabling the service (NTP master)**

**A screenshot of a calendar

AI-generated content may be incorrect.**

1. A screenshot of a computer error

   AI-generated content may be incorrect.**Making S10 (closest switch to the server) a NTP server (server/client mode)**
2. A screenshot of a computer program

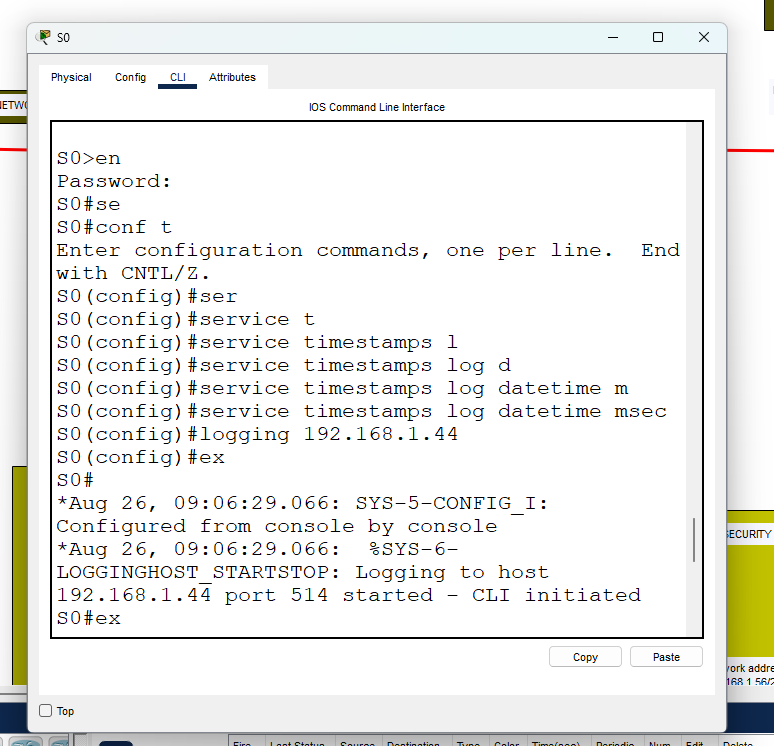
   AI-generated content may be incorrect.**Making R3 a NTP server (server/client mode)**

Now we keep going until the stratum (hops) reaches its limit (15), witch is not in our case

# **SYSlog**

**1- give service to get logs with msec**

**And configure the server’s IP which will get the logs:**



**2-after that you will get this output to tell that server is ready to get logs:**

A number with black text

AI-generated content may be incorrect.

**3-we will use these codes again on every router and switch to make sure everything is connected to the server**

# **Layer 2 Security**

**1. Network Setup**

* **PC12** assigned static IP 192.168.1.50 /29 with default gateway 192.168.1.49.
* **PC13** assigned static IP 192.168.1.58 /29 with default gateway 192.168.1.57.
* PC12 connected to **S2 Fa0/1** (access port in VLAN 10).
* PC13 connected to **S7 Fa0/1** (access port in VLAN 20).
* **S2 Fa0/2** connected to **S8 Fa0/1** (trunk).
* **S7 Fa0/2** connected to **S8 Fa0/2** (trunk).
* **Router0 Gi0/0/0** connected to **S8 Fa0/3** (trunk).

**2. VLAN Configuration**

* Created **VLAN10** and **VLAN20** on S2, S7, and S8.
* Assigned **PC12’s port (S2 Fa0/1)** to VLAN10.
* Assigned **PC13’s port (S7 Fa0/1)** to VLAN20.
* Configured trunk links between switches (S2–S8, S7–S8) and between S8–Router0.

### **3. Router Subinterface Configuration On** Router0 **under Gi0/0/0:**

* Created subinterface for VLAN10:
* interface g0/0/0.10
* encapsulation dot1Q 10
* ip address 192.168.1.49 255.255.255.248
* Created subinterface for VLAN20:
* interface g0/0/0.20
* encapsulation dot1Q 20
* ip address 192.168.1.57 255.255.255.248

1. A white screen with black text

   AI-generated content may be incorrect.**Allowing the Computers and Switch on VLAN 10,20**
2. **Testing Computers with CMD and pinging each other and their gateways**

**A screenshot of a computer

AI-generated content may be incorrect.A computer screen shot of a black screen

AI-generated content may be incorrect.**

1. **Assigning STP Portfast and Bpduguard on the network (Globally)**

* **Switch S2 (PC12 on VLAN10):**

spanning-tree portfast default

spanning-tree portfast bpduguard default

* **Switch S7 (PC13 on VLAN20):**

spanning-tree portfast default

spanning-tree portfast bpduguard default

### A screenshot of a computer AI-generated content may be incorrect.**Verification**

### A screenshot of a computer AI-generated content may be incorrect.

1. **Aaa authentication:**

the security settings of three routers (R1, R7, and R3) based on the provided images. All routers utilize a standard AAA (Authentication, Authorization, and Accounting) system for enhanced access control and monitoring.

1. AAA Settings (Authentication, Authorization, Accounting)

1. System Type: aaa new-model (enabled on all routers).

Authentication: aaa authentication login default group radius local

User identity is first verified with a RADIUS server. If that fails, the router's local database is used as a fallback.

1. Authorization: aaa authorization exec default group radius local

User privileges (what they can do after logging in) are determined by the RADIUS server first, then by local settings.

1. Accounting: aaa accounting exec default start-stop group radius

The start and end of each user session are logged on the RADIUS server for auditing purposes.

2. Access and User Accounts

R1 and R7:

1. Enable Secret Password: enable secret 5 [encrypted]
2. User Account: username admin privilege 15 secret 5 [encrypted]
3. Security Level: High. Passwords are encrypted using a strong algorithm.

R3:

1. User Account: username admin privilege 15 secret Admin@123
2. Security Level: Medium. The password is in plain text, which is a security vulnerability.

3. Remote Connection Methods

R7 and R3:

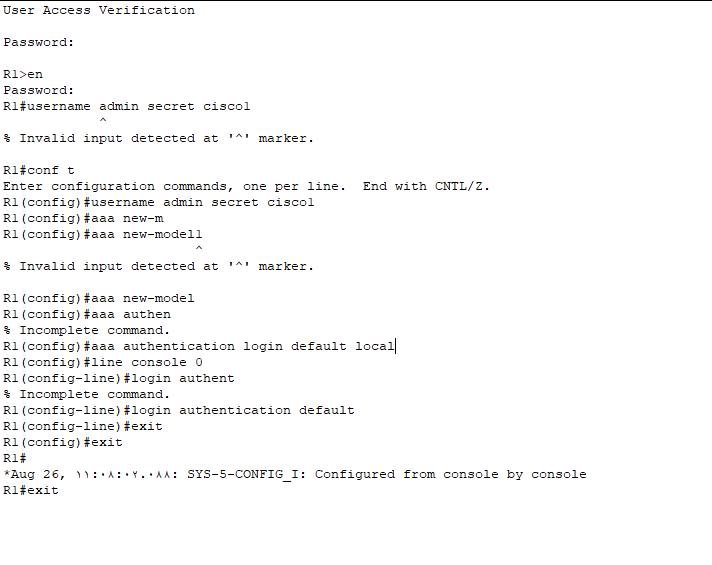
1. Console Access: line console 0

* Requires authentication based on AAA settings.

1. Remote Access (VTY): line vty 0 4

* Configured to accept connections only via SSH (transport input ssh), which is more secure than Telnet.
* Requires authentication based on AAA settings.

**1.Aaa authentication on routers 1**

****

**A screenshot of a computer

AI-generated content may be incorrect.**

Router R1 🔒

This router has the strongest security settings. Everything is protected and monitored:

Passwords: Both the administrator password and the password for entering privileged mode are strongly encrypted, making them very secure against brute-force attacks.

Security System (AAA): It implements a comprehensive system for authentication, authorization, and accounting. This means anyone attempting to access the device must have their identity and privileges verified, and every action they take is logged

**2.aaa authentication on routers 7**

**A screenshot of a computer

AI-generated content may be incorrect.**

1: Title

Securing User Access with Local Authentication

2: Creating a User Account

* The first step is to create a local user account with a password.
* We use the username command to define the account.
* We use the secret keyword to encrypt the password, making it more secure.

Example: username admin secret cisco

This creates a user named admin with an encrypted password of cisco.

3: Enabling Local Authentication

* We need to enable the AAA (Authentication, Authorization, and Accounting) framework on the device.
* This is the foundation for applying all security policies.

Command: aaa new-model

4: Applying the Policy to the Console Port

* Now, we define how users will be authenticated upon login.

We apply this authentication policy to the Console port, which is used for direct physical access to the device.

Commands:

line console 0

login authentication default

5: Conclusion

* These simple steps ensure that anyone attempting to access the router via the Console port will be prompted for a username and password.

Router R7 🔐

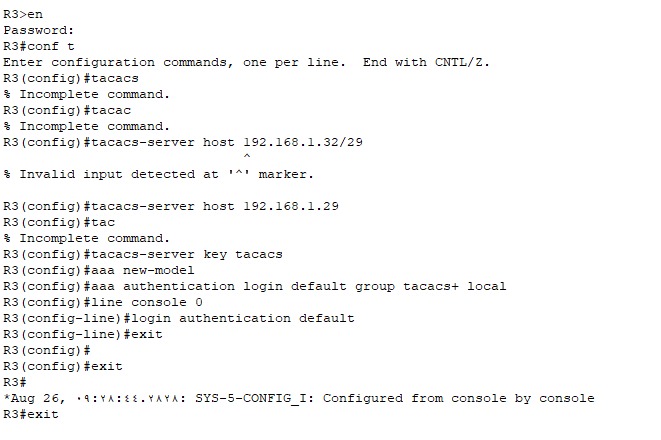
This router is similar to R1 in its security settings but specifies the connection methods more clearly:

Passwords: Just like R1, its passwords are strongly encrypted.

Remote Access: It only allows connections via the SSH protocol, which securely encrypts all transferred data. This is a significant security improvement over the older, unsecure Telnet protocol.

Security System (AAA): It applies the same robust security system for authentication, authorization, and accounting as R1.

**3.aaa authentication on router 3 & tacacs/radius server**



A screenshot of a computer

AI-generated content may be incorrect.

Title

Configuring Authentication using TACACS+

2: Introduction to TACACS+

What is TACACS+?

* A security protocol that controls access to network devices.
* It separates the three main functions: Authentication, Authorization, and Accounting.

Why do we use it?

* Centralized Security: All user data is stored on a central server, not on each individual device.
* Simplified Management: It's easier to manage accounts, especially in large networks.
* Greater Flexibility: It allows you to grant different levels of privileges to different users.

3: Essential Configuration Steps

Objective: To configure the router to use a TACACS+ server for user authentication.

Identify the TACACS+ Server:

The first step is to tell the router where to find the server.

Command: tacacs-server host 192.168.1.29

Set the Shared Secret Key:

A secret key must be configured on both the router and the TACACS+ server for secure communication.

Command: tacacs-server key tacacs

Enable the AAA Model:

This command is crucial as it turns on the AAA framework on the router.

Command: aaa new-model

Configure the Authentication Policy:

We define the primary and fallback authentication methods.

We prioritize the TACACS+ server first, then fall back to the local database if the server is unreachable.

Command: aaa authentication login default group tacacs+ local

# 4: Applying the Policy

Apply the Policy to the Console Port:

We apply the created authentication policy to the console line, which ensures that anyone connecting directly to the device must authenticate.

Commands:

line console 0

login authentication default

Slide 5: Conclusion

By following these steps, we've successfully shifted our device's authentication from a local-only model to a centralized, server-based model.

This configuration provides a critical layer of security and management efficiency.

The local fallback (local keyword) is a key feature, ensuring that administrators can still access the device even if the TACACS+ server is down

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Router R3 ⚠

​This router has a clear security weakness:

​Password: The password for the admin user is not encrypted and appears as plain text. This makes it easy to discover and access, even though the other security settings may be correct.

​Security System (AAA): It applies the same security system as the other routers, but the exposed password significantly reduces the overall effectiveness of this system.

​Remote Access: Like R7, it enforces the use of the secure SSH protocol for remote connections.

**13.ZPF (Zone-Based policy firewall)**

In this scenario, we have two zones:  
 • INSIDE  
 • DMZ  
  
Goal: Allow only HTTPS and ICMP traffic between the two zones, and drop all other protocols.

Step 1: Create a Class-Map to Match the Protocols

class-map type inspect match-any MY\_CLASS  
 match protocol https  
 match protocol icmp

Step 2: Create a Policy-Map and Define the Action (Inspect or Drop)  
  
policy-map type inspect MY\_POLICY  
 class type inspect MY\_CLASS  
 inspect  
 class class-default  
 drop  
  
  
⸻  
  
Step 3: Define the Zones and Assign the Interfaces  
  
zone security INSIDE  
zone security DMZ  
  
interface g0/0/0  
 ip address 192.168.1.1 255.255.255.0  
 zone-member INSIDE  
  
interface g0/0/1  
 ip address 192.168.2.1 255.255.255.0  
 zone-member DMZ  
  
  
⸻  
  
Step 4: Create a Zone-Pair and Apply the Policy  
  
zone-pair security IN-DMZ source INSIDE destination DMZ  
 service-policy type inspect MY\_POLICY  
  
zone-pair security DMZ-IN source DMZ destination INSIDE  
 service-policy type inspect MY\_POLICY  
  
⸻

⸻  
  
✅ 1. show zone security  
  
Explanation:  
“This command shows the Zones we created. Here we have a Zone named INSIDE with interface G0/0/0, and another Zone named DMZ with interface G0/0/1. That means these networks are now protected by the Zone-Based Firewall.”  
  
⸻  
  
✅ 2. show policy-map type inspect  
  
  
  
Explanation:  
“This command displays the policies we created. For example, in the policy named POLICY\_INSIDE\_TO\_DMZ, any HTTPS or ICMP traffic is inspected (allowed and statefully monitored). Any other traffic falls under the class-default and is dropped. The same logic is applied in the opposite direction with POLICY\_DMZ\_TO\_INSIDE.”  
  
⸻  
  
✅ 3. show policy-map type inspect zone-pair sessions  
  
Possible Output after generating traffic (ping or https):  
  
Explanation:  
“This command shows the active sessions currently passing through the firewall and whether traffic is inspected or dropped. For example, it says 10 packets were inspected under the PROTOCOLS\_CLASS, and 0 packets were dropped. That confirms that my ping or HTTPS test from INSIDE to DMZ passed successfully through the firewall.”