-
-

Table of Contents

•

•

-
-

Table of Figures

-
-

Introduction

Care Medical Hospital, a renown health services provider in the independent sector, is obligated to reenforce its network security infrastructure to stop the flow of secret data, maintain uninterrupted service delivery, and shield itself from growing variants of threats. Based on my initial appointment as a security analyst for Care Medical Hospital, this assignment is meant to delineate a meticulous architectural design that will boost the hospital's network security standards. First of all, accordance, strength, and priority lie at a heart of the design together with implementation of the networks contemporary security principles in order to provide a protection to the head office in Colombo and its remote branches as well. Prime concerns include implementation of Gigabit Ethernet, delivering firewall settings, utilizing AAA for authentication, portraying public resources, adhering to hierarchical network design principles, unlocking user authentication, restricting internet use, guaranteeing encryption of data transmitted from the branch, constructing backup, and catastrophe recovery strategies. This assignment elucidates the strategic framework for supplying the skills of Care Medical Hospital with droughts regarding cyber threats as well as preservation of confidentiality, integrity, and reliability of its health care resources.

Task 1

Network Security

Network security is a general word that points to the diverse technologies and tools that make networks secure. In a concise and clear statement, it implies to set of algorithms and settings developed to defend data and computer systems from unauthorized access, breaches of their confidentiality, and manipulations by using both software and hardware-based technologies.

Network Security Devices

The use of the right devices and solutions definitely can enhance the network security of ours. The most prevalent types of network security devices covering us from external attacks that I will list below are:

Intrusion detection system (IDS)

A network IDS effectively enhances cyber security by identifying hackers, virus or malware on a network before they are executed, consequently disallowed to occur, or a data breach allowing for reporting and further development of security measures to avoid future intrusions. Spending money on a properly reacted IDS is likely to be much cheaper than fixing losses and dealing with affected jurisdictions, their populations, and the legal issues associated with them.

-
-

Intrusion prevention system (IPS)

An intrusion prevention system (IPS) is a specific network security tool, which is responsible for identification as well as prevention of threats like viruses and worms. IDSs are mechanisms to monitor your network 24/7, filtering out whatever suspicious activity they find and log it. The IPS reports these events in real-time and reacts by closing the network access points or configuring the firewall to prevent future access from the outside. This is another benefit of IPS solutions as they can be used to detect problems with the corporate security policy, preventing employee or network guest abuses from infringements contained in the policy.

Firewall

The firewall is one of the basic tools of network defence that provides an isolation between two separate networks. Firewall systems can be standalone or they can also be hardened and made part of the other infrastructure devices like routers and servers. You can find the firewalls both of hardware and software categories; some firewalls are appliances that live at a location where the networks meet as the major device that separates two networks.

Network Security Software

A network security system is a must condition for the businesses. Among the most important and appropriate items are those businesses which use cloud-based applications and procedures - because there are more edge cases to deal with. Undisputedly, network security software is the most complex type of software, which however, enabling even small businesses, without the in-house IT team, to effectively utilize it.

Bitdefender

Bitdefender is a thriving, multi-national company committed to developing security software that secures homes and businesses all over the world. The fact is this particular technology is currently tracking and protecting in excess of 500 million devices in more than 170 countries.

Avast Cloud Care

Advantage of Avast is that it has never been present among the alternatives specified above. Introduced with the main aim to enhance and control the managed service providers to manage their client’s IT security more effectively. It not too much for a man, however, it is great on what it is supposed to do. Taking into account the number of ways they can be used (along with the fact that they help keep costs down, which is impressive), they continue to deliver the best in terms of endpoint protection as well as network security.

Firemon

Firemon is an innovative network security system, unlike others, it stands out in the multitude. A premier network security solution, Firemon does not only secure your network, but it accelerates and optimizes it too. The autonomy of firemon SingRouter from other using in that industry. Automation of many of the control functions network security. These can be customized to work perfectly under many different situations from strict environmental requirements and, all the way to differently designed infrastructure and very specific use cases. After these international policies are in effect, operators will feel relieved and safe through the network.

Watchguard

Watchguard is a multilevel shield offering cover for each and every private, government or business sector. They provide network security solutions, endpoint security solutions, cloud Wi-Fi security solutions, and multi-factor authentication-solutions which have been followed with awards. Through Watchguard's monitoring which occur in the real time you can get a glimpse at the whole picture and screen of the network. This enables the IT personnel to react swiftly, interpret, and decide whether the Network has any failure, or if there is any data protected.

Network Security protocols

Routing, e-mailing, chatting and communication protocols including many types of the protocols are existing. One might as well use a security mechanism that provides for data privacy and credibility over the network space as network security protocols. To give protection layer for the network that can exist data discreetly from unauthorized sniffing or rather the extraction of the real nature of the parameter, these protocols have employed numerous methodologies.

Secure transport of Hyper Text Transfer Protocol (HTTPS)

HTTPS is a secured protocol (used for the transfer of information among two or more systems) which provides information security during data communication. The founder used Secure Socket Layer (SSL) to set up an encrypted link as the first step of the present TLS security provision. With the transmission of data in this encoded form, Internet criminals are unable to understand and tamper of data during transmission from browser to web server. In such an event, even though the criminals might capture the data packets, they will be unable to read them because they are encrypted using the encryption techniques associated with data packets.

Kerberos

As the client-server applications authentication is desired to be secure, Kerberos is another network validation protocol that demonstrates the use of symmetric-key cryptography. As per encryption protocol of Kerberos network, all workplace and services should fit for insecure networks which responsible and ensures security for the whole system.

IPsec

IPsec is a system that includes four main protocols that establish trust between computers and other devices such as a router. Providing the security of data transmitted via the public is one of the responsibilities of cloud providers. IPsec is an encryption that enters IP packets and upon implementation of the source of authentication as well. It might be used for instance in order to establish VPNs. In the word "IPsec," IP and sec refers to an acronym for "Internet Protocol" and "secure". Issuance of a uniquely identifying IP address is based on the IP (Routing Protocol), which is all over the Internet, that determines where the Data to be transmitted should go. IPsec protocol enables the procedure to be more secure by introducing the encryption and authentication (encryption and authorized access).

Comparison between SSL and HTTPS

SSL	**HTTPS**
It is (Secure Sockets Layer) or TLS (Transport Layer Security) languages, which are abbreviated as.	It is short for Secure. Sockets. Layer encoded with a URL that contains the addition of the domain name and HTTPS at the end of the address to ensure security.
It is one of the three protocol tiers, in addition with HTTP, that are responsible for implementation of actual data transfer through the process of encrypting HTTP into HTTPS (Hypertext Transfer Protocol Secure).	This can be expressed as HTTPS being a result of combining HTTP protocol with Secure Sockets Layer (SSL).
They are SSL 1.0, SSL 2.0 and SSL 3.0 which are the most innovative and widely used standards in the world	There is no other version of HTTPS yet.
Meanwhile at this point it is becoming a relic which has been transferred to the archive. Today, the establishment of the TLS protocol, i.e. the open standard TC Transport Layer Security for data security in internet traffic is becoming more popular.	Most of the websites are switching to HTTPS rather than HTTP. If a website does not use HTTPS, browsers flag that site as "Not secure," which also affects the user experience.

Task 2

Secure Network

An adequately secure network can be defined as the home, business, school, or any other network where security precautions have been taken, thus protecting it from external aggressors. For sure, there is no perfect network existing in reality. Once one computer or another device that is within the same network is online, it becomes an instant easy victim of possible internet assaults. Nonetheless, following those procedures allows a network to be safe against cyber-attacks.

Purpose of a secure Network for Care Medical Hospital

The objective of a safe Care Medical Hospital IP network is to guarantee the privacy, the integrity, and the accessibility of sensitive patient data, the hospital critical functioning, and communication systems. A safe network is a crucial element which secures health of patients making them immune to unauthorized access, data breaches, malware and other cyber threats that could compromise patients' privacy and lead to disruption of services in the hospital or even financial losses. Also, a networked connection becomes enabler of information flow among various hospital sites, supports its workers within permitted areas, and is essential for keeping informed about regulations in medical practice.

Requirements for a secure Network for Care Medical Hospital

Network Design Overview:

1. **Hierarchical Network Design Model:**

- Core Layer: Responsible for high-speed backbone connectivity.
- Distribution Layer: Segregates traffic and implements security policies.
- Access Layer: Provides connectivity for end devices.

2. **Physical Connectivity:**

- Main hospital LAN: Gigabit Ethernet for maximum performance.
- Remote branches: Secure connectivity (e.g., VPN) to the main branch.

Security Measures:

1. **Firewall Configuration:**

- Implement a robust firewall at the main branch to filter and control incoming and outgoing traffic.
- Configure firewall rules to enforce strict access control policies.

2. **AAA (Authentication, Authorization, and Accounting):**

- Utilize AAA for network device login authentication whenever possible.
- Implement Syslog Server for recording and monitoring events.
- Deploy an NTP server for time synchronization across the network.

3. **Separation of Public Resources:**

- Place all publicly available resources, including public web servers, on a separate subnet.
- Enable only secure web access (HTTPS) for web servers.
- Implement access control lists (ACLs) to restrict access to these resources.

4. **Centralized Authentication and Policy Management:**

- Utilize Domain Controllers for centralized end-user authentication and security policy management.
- Implement group policies to enforce security settings across the network.

5. **Internet Usage Management and URL Filtering:**

- Deploy a robust web filtering solution to manage internet usage and enforce URL filtering policies.
- Regularly update and maintain the URL filtering database to block malicious or inappropriate websites.

6. **Secure Communication between Branches:**

- Use secure VPN tunnels to establish encrypted communication between the main branch and remote branches.
- Implement strong encryption protocols (e.g., IPSec) to ensure data confidentiality and integrity.

7. **Backup and Disaster Recovery Plan:**

- Implement regular backups of critical data and systems.
- Store backup data in secure offsite locations to mitigate the impact of disasters.
- Test and validate the backup and disaster recovery procedures periodically.

Network Device Compatibility and Performance:

Verify the compatibility of network devices so that there remains no hiccups for smooth functioning and reliability.

-
-

Periodically provide updates relating to both firmware and software that can be used to fix security risks and achieve the required adjustment.
Among which mentioned measures, Care Medical Hospital aims to shield its infrastructure from cyber-threats and at the same time ensure seamless optimum performance of its computer networks.

Network Hardware for Care Medical Hospital

Core Layer:

Router:

Cisco 9000 Series Integrated Services Router (ISR) - The Routers for Rendering High-end Routing.

Switch:

Cisco Catalyst 9000 Series Switch for scalable backbone connectivity and increased bandwidth.

Distribution Layer:

Firewall:

A Palo Alto Networks Next-Generation Firewall deployment for advanced threat protection and precise control policies.

Switch:

Cisco Catalyst 9000 Series switch is used for traffic segregation and VLAN protocol implementation.

Access Layer:

Switches:

Cisco Catalyst switches of 9000 series to make them available to device endpoint.

Wireless Access Points:

Cisco Catalyst 9100 Series Access Point offers secured WiFi connection to the hotel visitors the reception area and the guests area.

Domain Controllers:

Server Hardware:

Dell PowerEdge or HP ProLiant Server and Domain Controller Servers shall be the instances to provide for those respective role instances.

Operating System:

The Firm gets to use the Window Server to ensure authentication and policy controls are administered in a homogeneous way.

Web Servers:

Server Hardware:

Secondly, a choice server racks would either be a Dell PowerEdge Server Selector or HP ProLiant Server for web hosting.

Web Server Software:

Apache HTTP Server and Microsoft Internet Information Services (IIS) on the Internet, for example.

Security Measures:

Employ HTTPS schemes as well as SSL/TLS certificates for secure HTTP access.

Syslog Server:

Server Hardware:

On VM-ware vSphere or Microsoft Hyper-V.

Syslog Software:

Splunk Enterprise or SolarWinds Kiwi Syslog Server can be installed to detect and study events logs and monitoring.

NTP Server:

Server Hardware:

Running on VMware vSphere machine virtualization or Microsoft Hyper-V.

NTP Software:

It further extends the service of synchronizing time by integrating with Windows Time Service or NTPd.

VPN Hardware:

VPN Concentrator:

Cisco ASA Firewall with VPN features for on the protected lane between branches.

Encryption Protocols:

Use VPN tunnels with IPSec for data encryption over the air.

Backup and Disaster Recovery:

Backup Appliance:

As for backups, we will use either Barracuda Backup Appliance or Dell EMC Data Domain for automated jobs.

Offsite Storage:

The storage environment on cloud like AWS S3 or Azure Blob Storage should be used to prepare safe and secure offsite storage.

Network Software for care medical hospital

To complement the recommended network hardware for Care Medical Hospital, here are software solutions that align with the outlined security and operational requirements:To complement the recommended network hardware for Care Medical Hospital, here are software solutions that align with the outlined security and operational requirements:

Firewall Software:

Palo Alto Networks Next-Generation Firewall (NGFW):Palo Alto Networks Next-Generation Firewall (NGFW):

It provides the latest anti-virus software, the rapid identification of applications, and hands-on configuration of the network flow.

AAA and Syslog Software:

Cisco Identity Services Engine (ISE):Cisco Identity Services Engine (ISE):

AAA services provider for network device logins performs authentication, authorization and accounting purposes.

Splunk Enterprise or SolarWinds Kiwi Syslog Server:Splunk Enterprise or SolarWinds Kiwi Syslog Server:

Features event logging, analysis and reporting functions, assembled under centralized network security monitoring.

Web Server Software:

Apache HTTP Server:

A commonly utilized open-source, secure server software for being the website host.

Microsoft Internet Information Services (IIS):

Aimed to offer web hosting with coordinated environments on servers with version of Windows operating systems.

-
-

Domain Controller Software:

Windows Server Active Directory:

Prior to offering the described auditing, with centralized authentication, policy management, and directory services for Windows networks.

VPN Software:

Cisco AnyConnect Secure Mobility Client:Cisco AnyConnect Secure Mobility Client:

Provides SSL VPN or IPsec VPN for secure remote access to key locations, such as the hospital branches, where data can be relayed confidentially.

NTP Software:

Windows Time Service:

Windows Server handles the time synchronization service automatically, hence ensuring that all machines in the network are in line with the correct time.

Web Filtering Software:

Cisco Umbrella (formerly OpenDNS):

Web filtering cloud solutions that monitor and control use of the internet by defining and enforcing usage policies as well as blocking malicious and undesirable websites.

Backup and Disaster Recovery Software:

Veeam Backup & Replication:

To ensure the success of virtualized environment and business continues, it has full backup and disaster recovery solutions, and data protection.

Importance of Network Security for an organization

Network security, no matter how you big or small your company is, it is one of the most important aspects of the online work of your company and connected with LAN or other methods in use. It is fair to say that no network can withstand all the attacks but, efficient network security solution needs to be trusted as well as must be useful. Enterprises can dispel the danger of data theft and sabotage with the use of a resilient network security system vital to the security of the organization.

Firstly, the souring level of network security for AstraZeneca Campus either contributes to or stems from several factors. Security is also critical for our firm as all its employees will attain the tranquility and peace of mind that come with knowing their information is safe and not susceptible to malicious activities. Just as it is in the case of systems, security also means global security for everyone. The campus users' increase in confidence and the prevention of costs that come with conduct and legal consequences of the data breach are some of the benefits of our network. All the users consequently embark on the encryption since they might lose huge amounts of data to cyber-criminals thus making the system more secure that both individuals and organizational data. Network safeguarding denies unauthorized influence. They may also have too much sensitive data that may include the personal data of clients. With the enrollment to the network, such critical data are prone to risk even for an individual granted such access. Isolation scenario makes the implementation of the security network longer process.

IP table

Table 2: IP table

Department	VLAN	Number of Devices	Subnet mask	IP Range	Gateway
Hospital LAB Main	10	50	255.255.255.192	172.30.0.0-172.30.0.63	172.30.0.1
Hospital Administration	20	20	255.255.255.224	172.30.0.64-172.30.0.95	172.30.0.65
IT	30	12	255.255.255.240	172.30.0.96-172.30.0.111	172.30.0.97
HR	40	10	255.255.255.240	172.30.0.112-172.30.0.127	172.30.0.113
LAB Sub	50	10	255.255.255.240	172.30.0.128-172.30.0.143	172.30.0.129
Marketing	60	5	255.255.255.248	172.30.0.144-172.30.0.151	172.30.0.145

Network Diagram

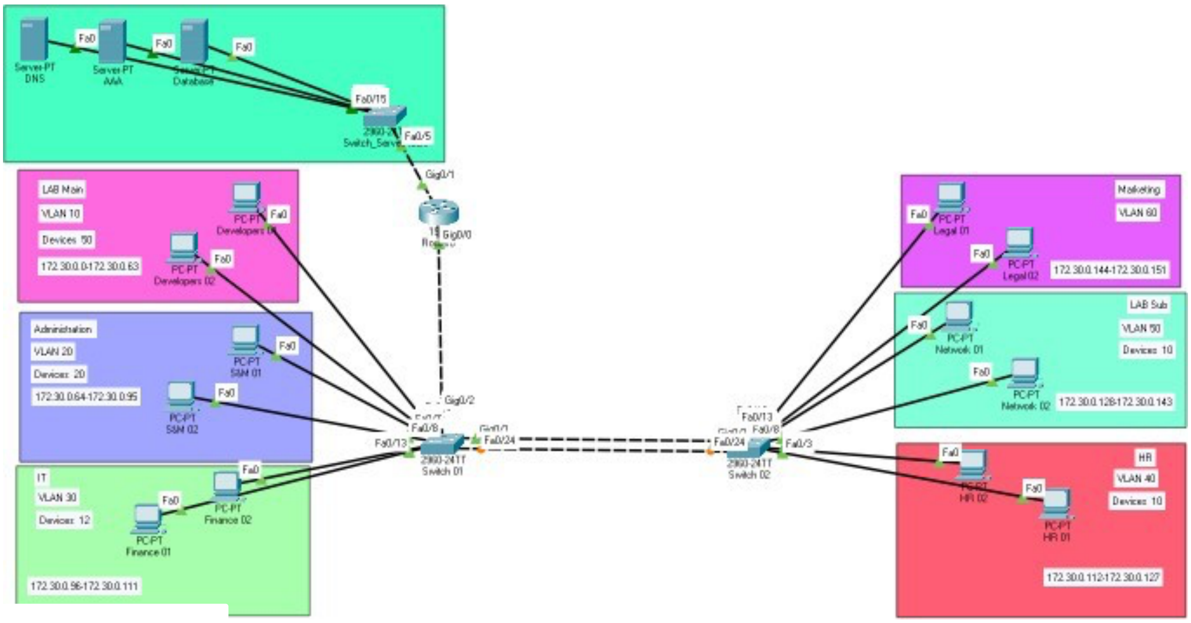


Figure 1 Network Diagram 1

Technical Diagram

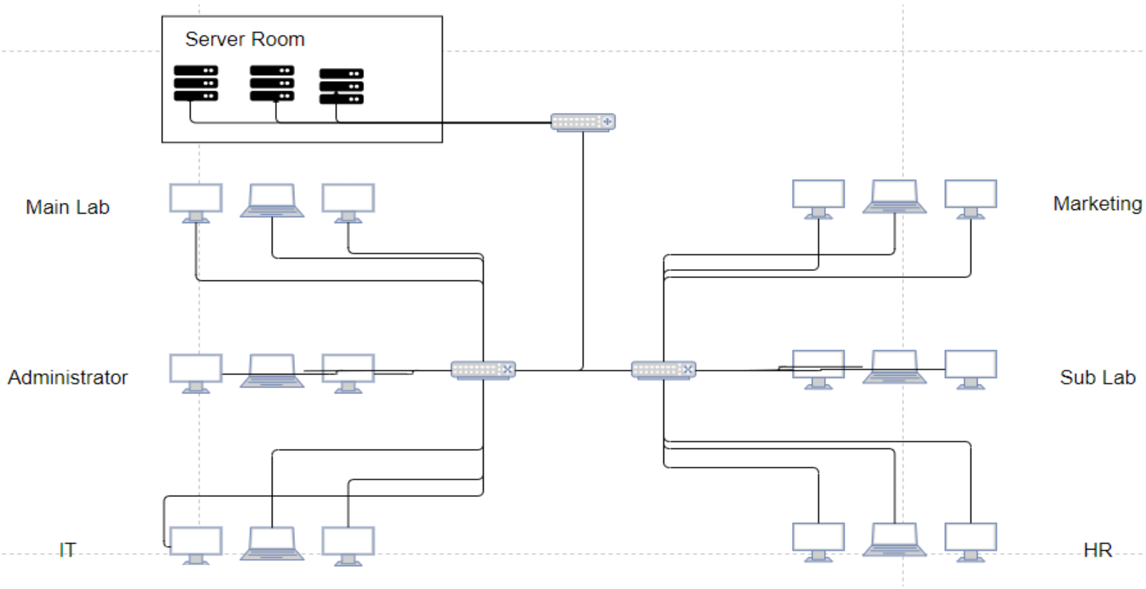
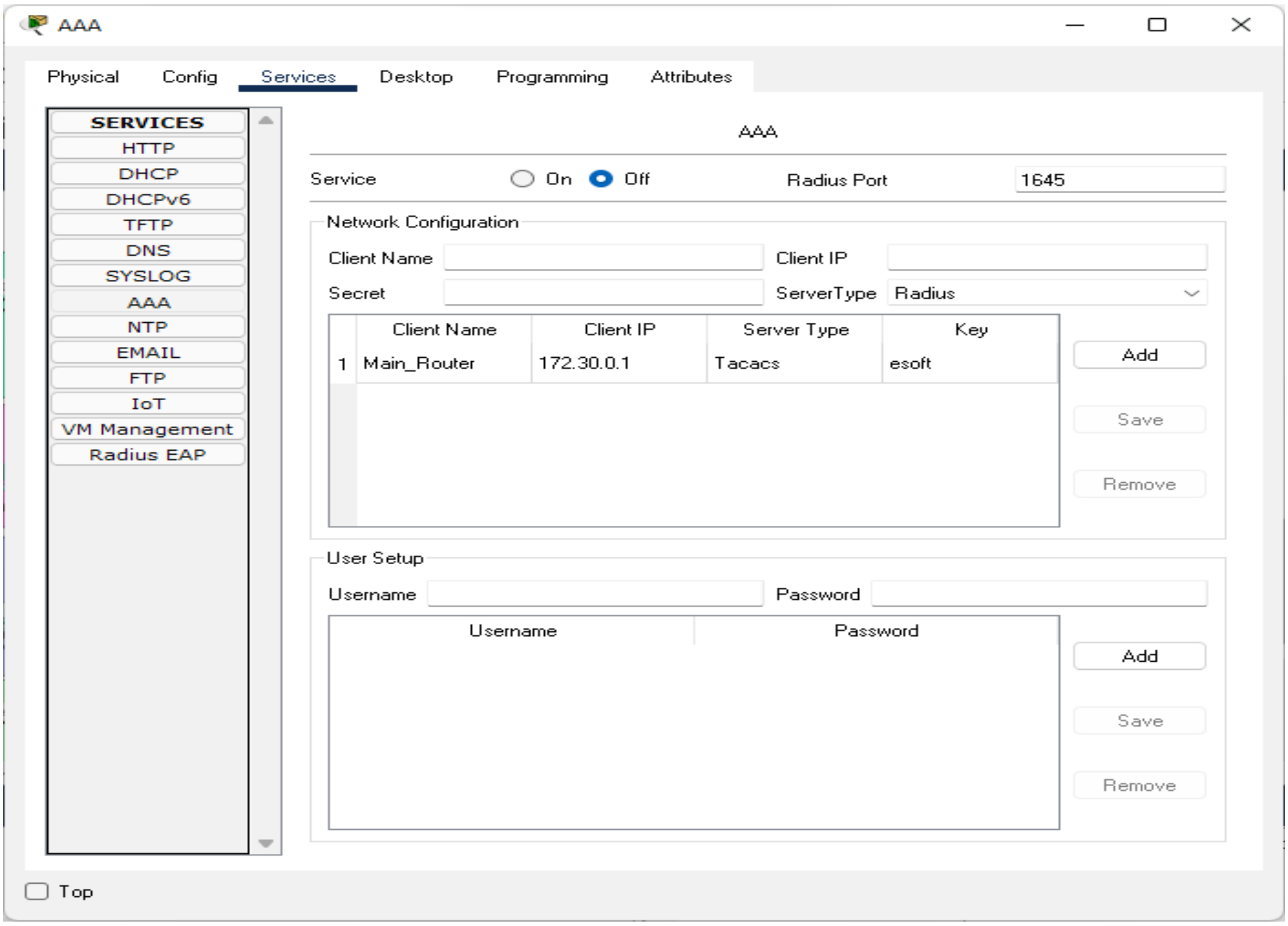


Figure 2: Technical Diagram 1 1Figure 2: Technical Diagram 1

-
-

TASK 3

AAA in server



AAA

Service ○ On ● Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	Main_Router	172.30.0.1	Tacacs	esoft

User Setup

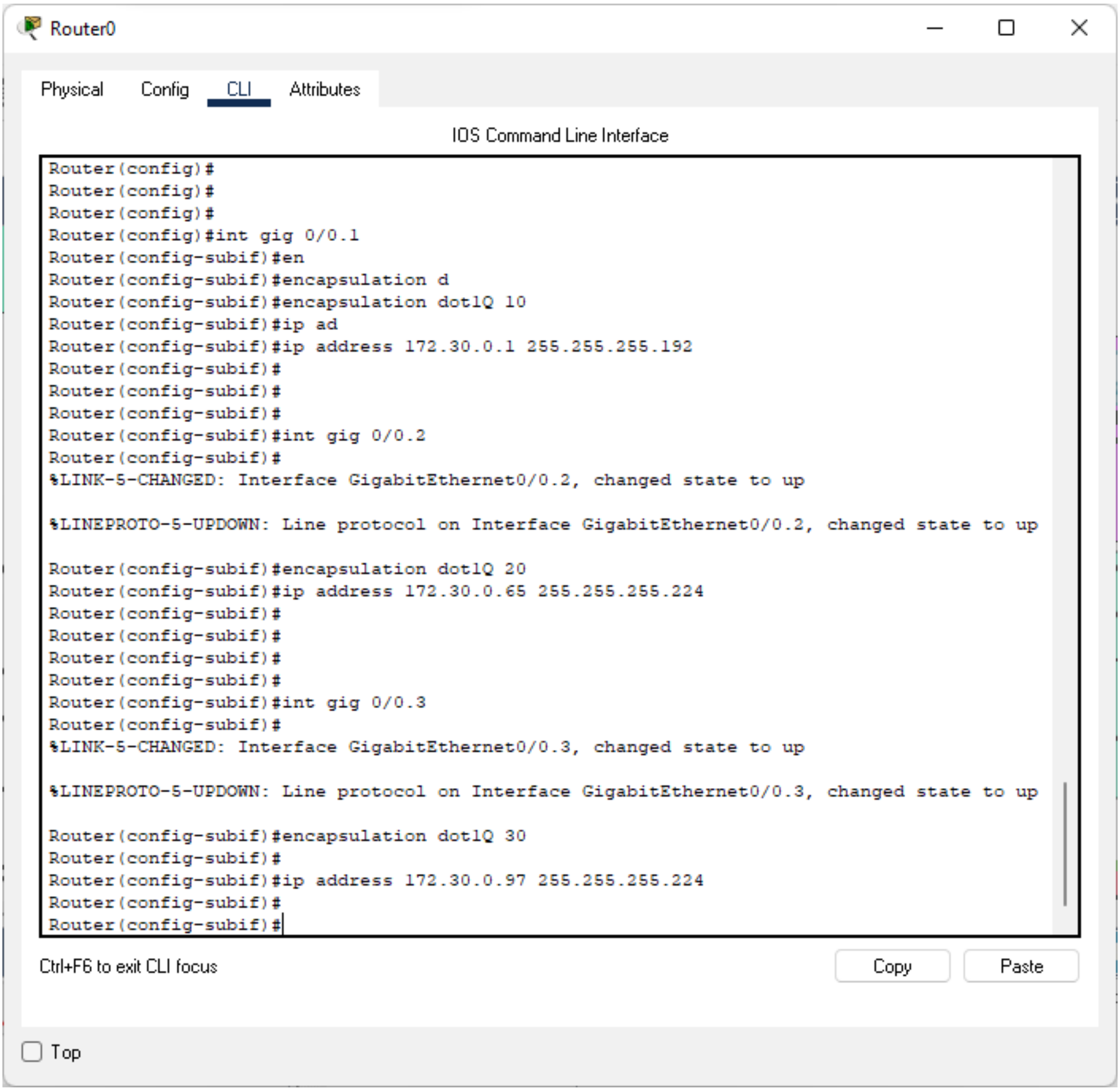
Username Password

Username	Password

Figure 3: AAA in server 1 1Figure 3: AAA in server 1

-
-

Creating sub interface

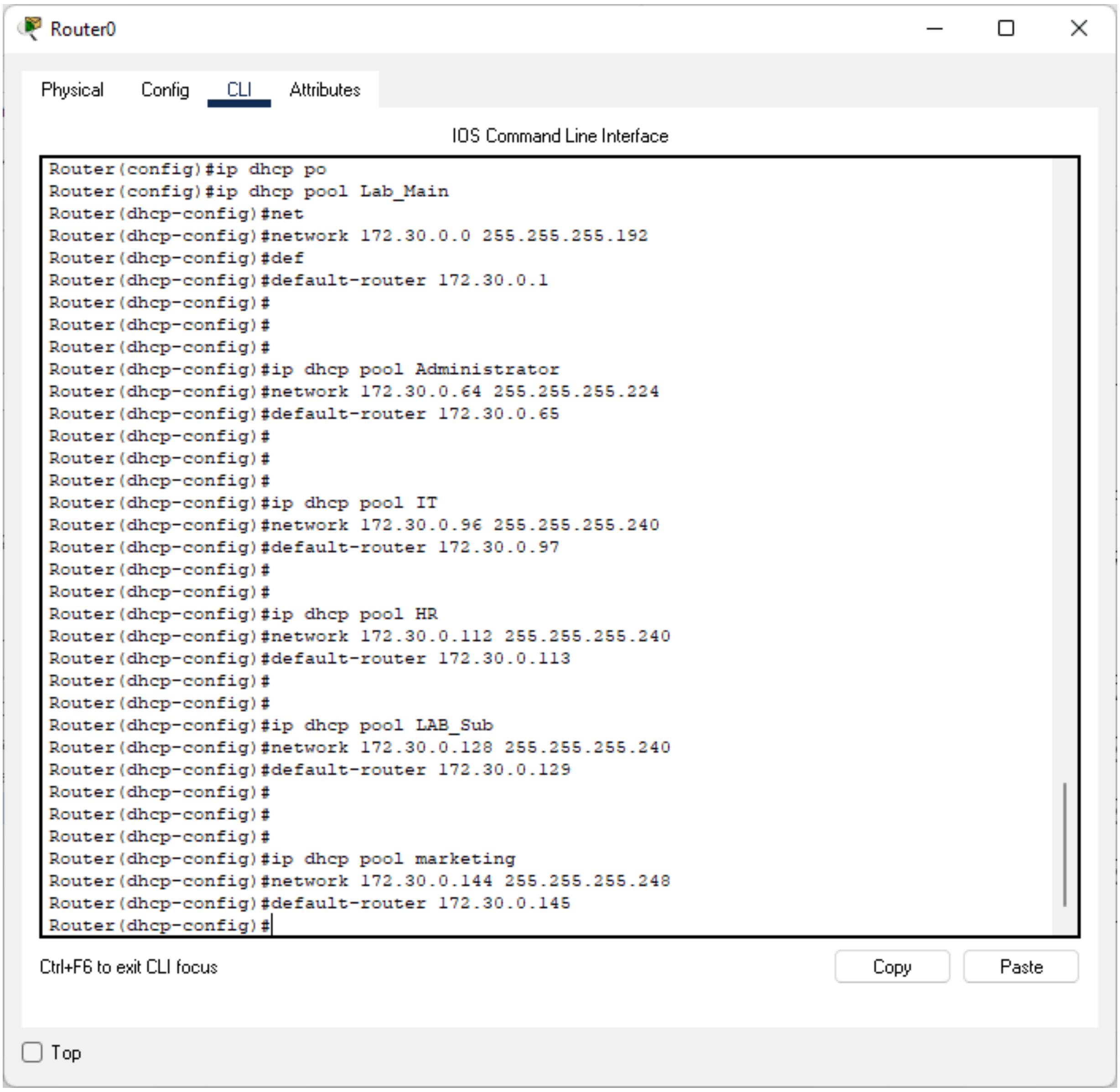


```
Router(config)#
Router(config)#
Router(config)#
Router(config)#int gig 0/0.1
Router(config-subif)#en
Router(config-subif)#encapsulation d
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip ad
Router(config-subif)#ip address 172.30.0.1 255.255.255.192
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#int gig 0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 172.30.0.65 255.255.255.224
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#int gig 0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.3, changed state to up

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#
Router(config-subif)#ip address 172.30.0.97 255.255.255.224
Router(config-subif)#
Router(config-subif)#
```

Figure 4: Creating sub interface 1

-
-

DHCP in Router

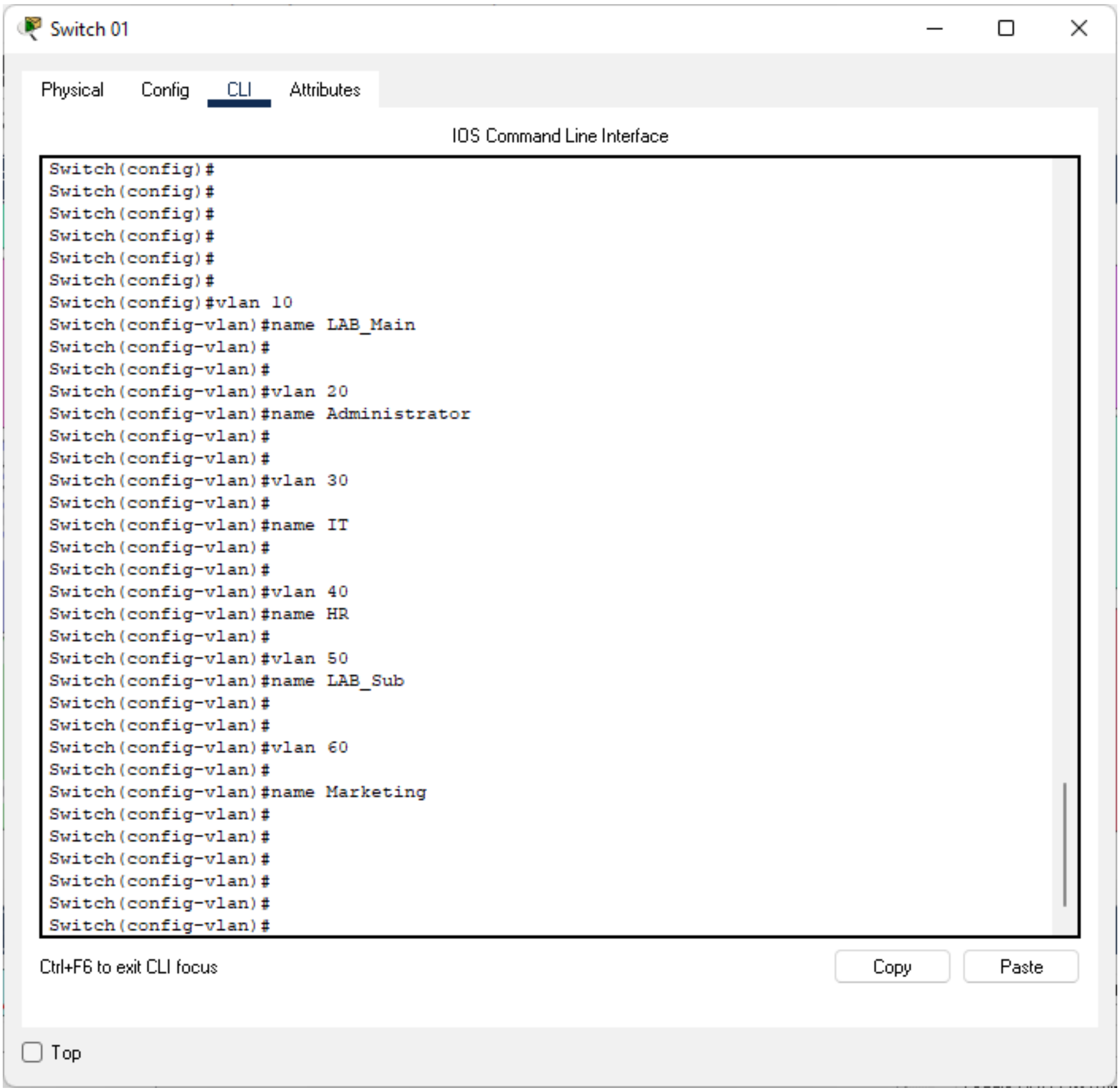


```
Router(config)#ip dhcp po
Router(config)#ip dhcp pool Lab_Main
Router(dhcp-config)#net
Router(dhcp-config)#network 172.30.0.0 255.255.255.192
Router(dhcp-config)#def
Router(dhcp-config)#default-router 172.30.0.1
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool Administrator
Router(dhcp-config)#network 172.30.0.64 255.255.255.224
Router(dhcp-config)#default-router 172.30.0.65
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool IT
Router(dhcp-config)#network 172.30.0.96 255.255.255.240
Router(dhcp-config)#default-router 172.30.0.97
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool HR
Router(dhcp-config)#network 172.30.0.112 255.255.255.240
Router(dhcp-config)#default-router 172.30.0.113
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool LAB_Sub
Router(dhcp-config)#network 172.30.0.128 255.255.255.240
Router(dhcp-config)#default-router 172.30.0.129
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#ip dhcp pool marketing
Router(dhcp-config)#network 172.30.0.144 255.255.255.248
Router(dhcp-config)#default-router 172.30.0.145
Router(dhcp-config)#
```

Figure 5: DHCP in Router 1

-
-

Create VLAN

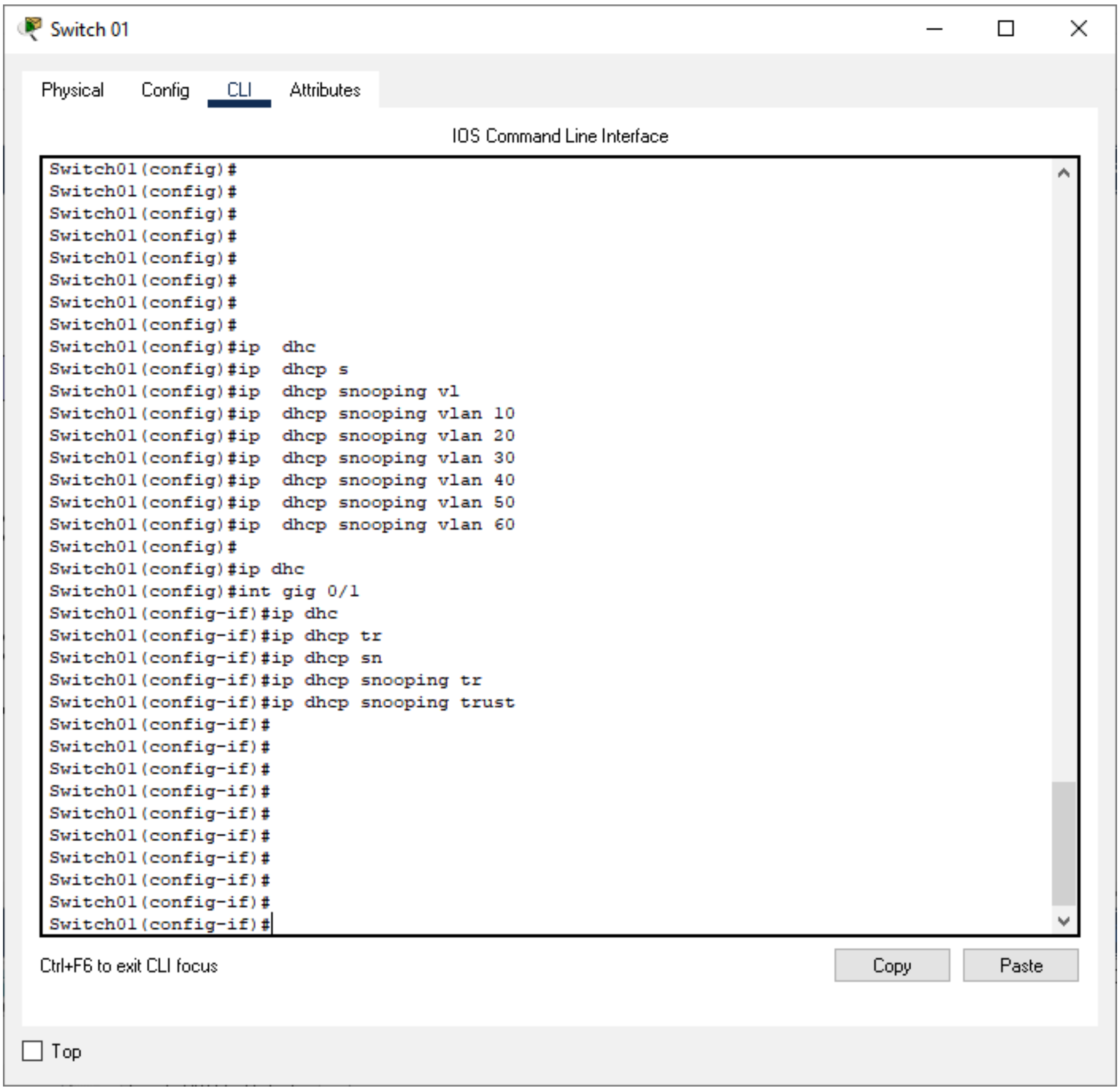


```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name LAB_Main
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Administrator
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#vlan 30
Switch(config-vlan)#
Switch(config-vlan)#name IT
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name HR
Switch(config-vlan)#
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name LAB_Sub
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#vlan 60
Switch(config-vlan)#
Switch(config-vlan)#name Marketing
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#
```

Figure 6: Create VLAN 1

-
-

DHCP Snooping

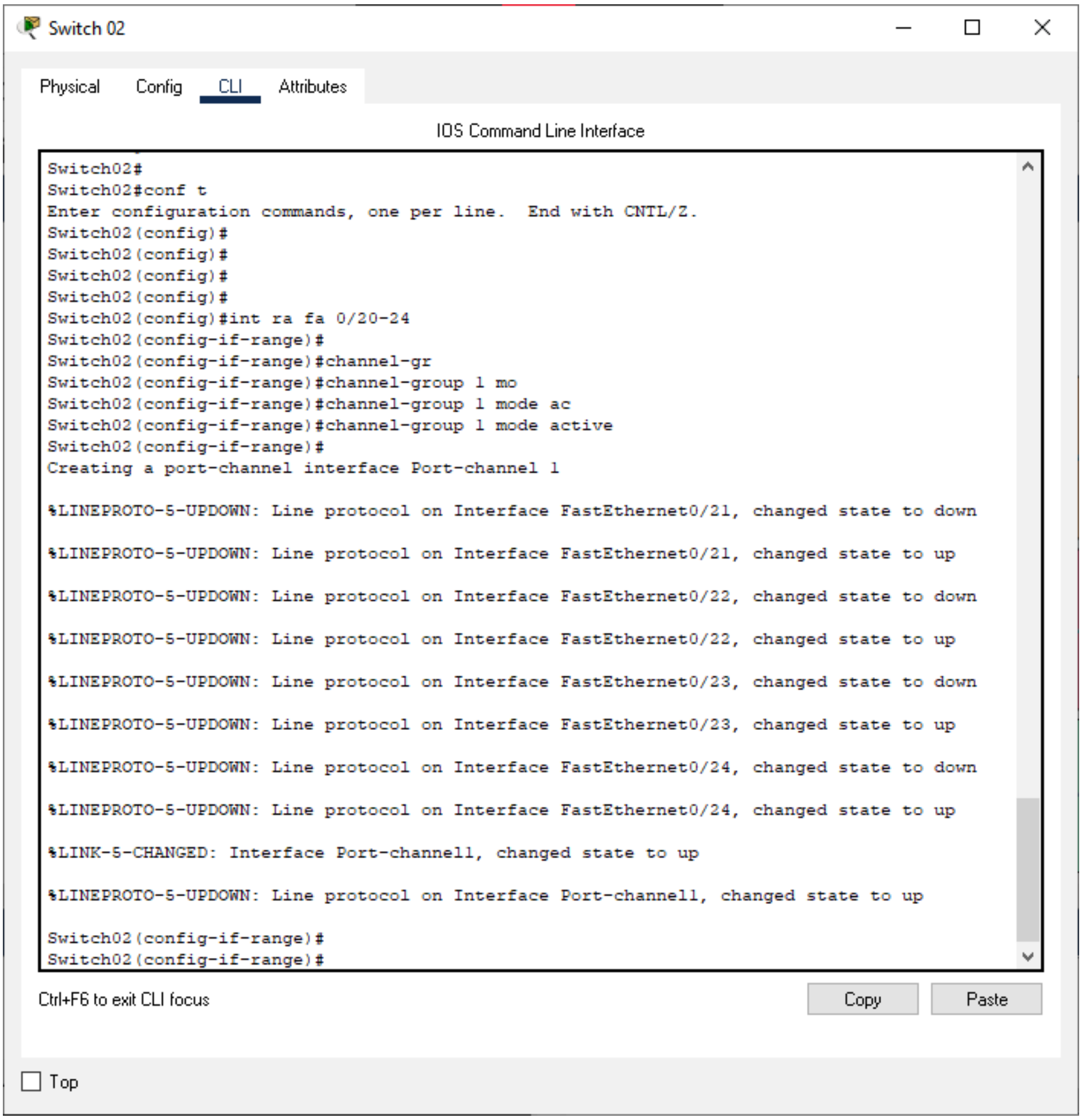


```
Switch01(config)#
Switch01(config)#
Switch01(config)#
Switch01(config)#
Switch01(config)#
Switch01(config)#
Switch01(config)#
Switch01(config)#
Switch01(config)#ip  dhc
Switch01(config)#ip  dhcp s
Switch01(config)#ip  dhcp snooping vl
Switch01(config)#ip  dhcp snooping vlan 10
Switch01(config)#ip  dhcp snooping vlan 20
Switch01(config)#ip  dhcp snooping vlan 30
Switch01(config)#ip  dhcp snooping vlan 40
Switch01(config)#ip  dhcp snooping vlan 50
Switch01(config)#ip  dhcp snooping vlan 60
Switch01(config)#
Switch01(config)#ip dhc
Switch01(config)#int gig 0/1
Switch01(config-if)#ip dhc
Switch01(config-if)#ip dhcp tr
Switch01(config-if)#ip dhcp sn
Switch01(config-if)#ip dhcp snooping tr
Switch01(config-if)#ip dhcp snooping trust
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
Switch01(config-if)#
```

Figure 7: DHCP Snooping 1

-
-

LACP

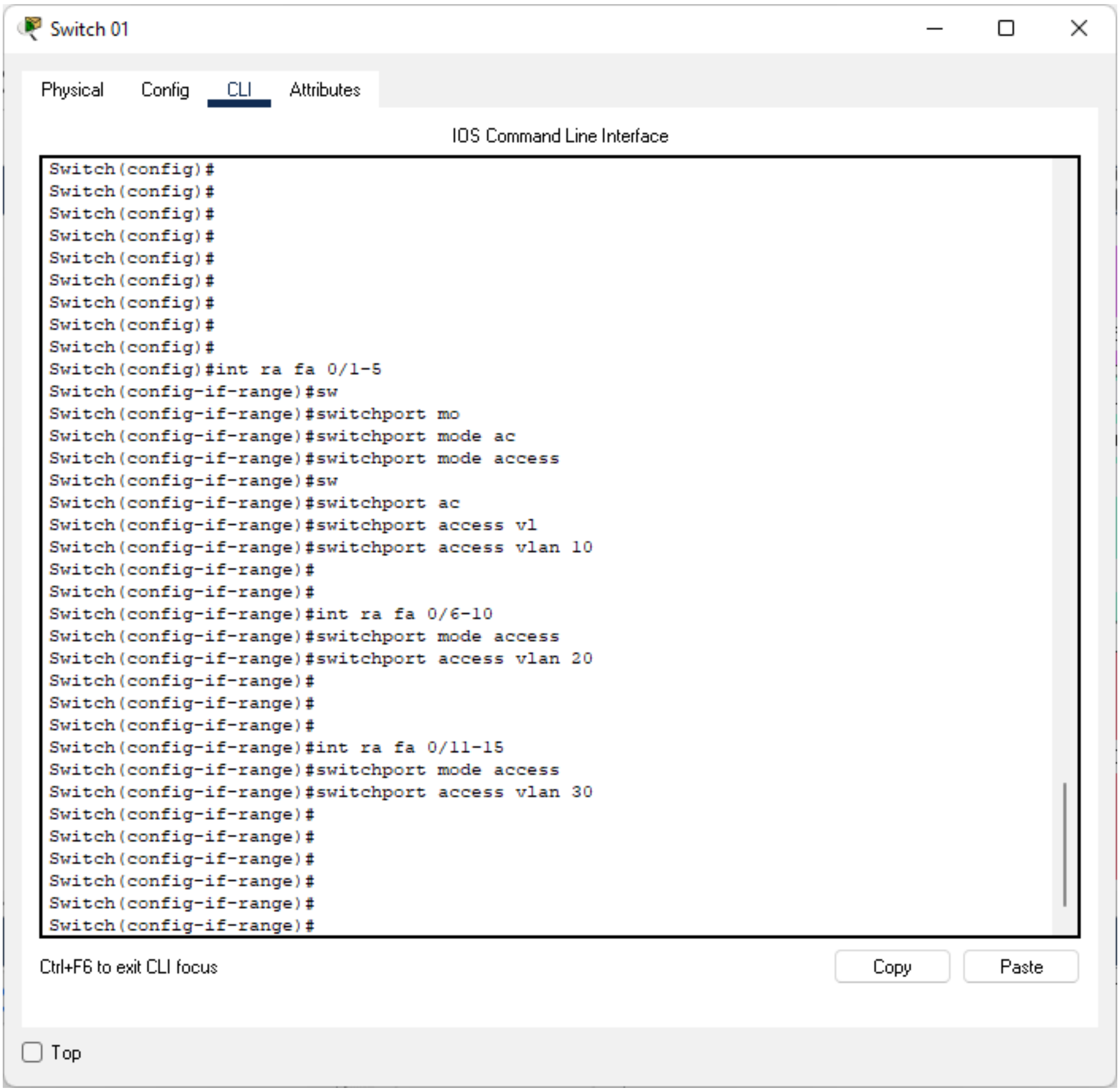


```
Switch02#
Switch02#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch02(config)#
Switch02(config)#
Switch02(config)#
Switch02(config)#
Switch02(config)#int ra fa 0/20-24
Switch02(config-if-range)#
Switch02(config-if-range)#channel-gr
Switch02(config-if-range)#channel-group 1 mo
Switch02(config-if-range)#channel-group 1 mode ac
Switch02(config-if-range)#channel-group 1 mode active
Switch02(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

Switch02(config-if-range)#
Switch02(config-if-range)#
```

Figure 8: LACP 1

-
-

Allocating ports to VLAN

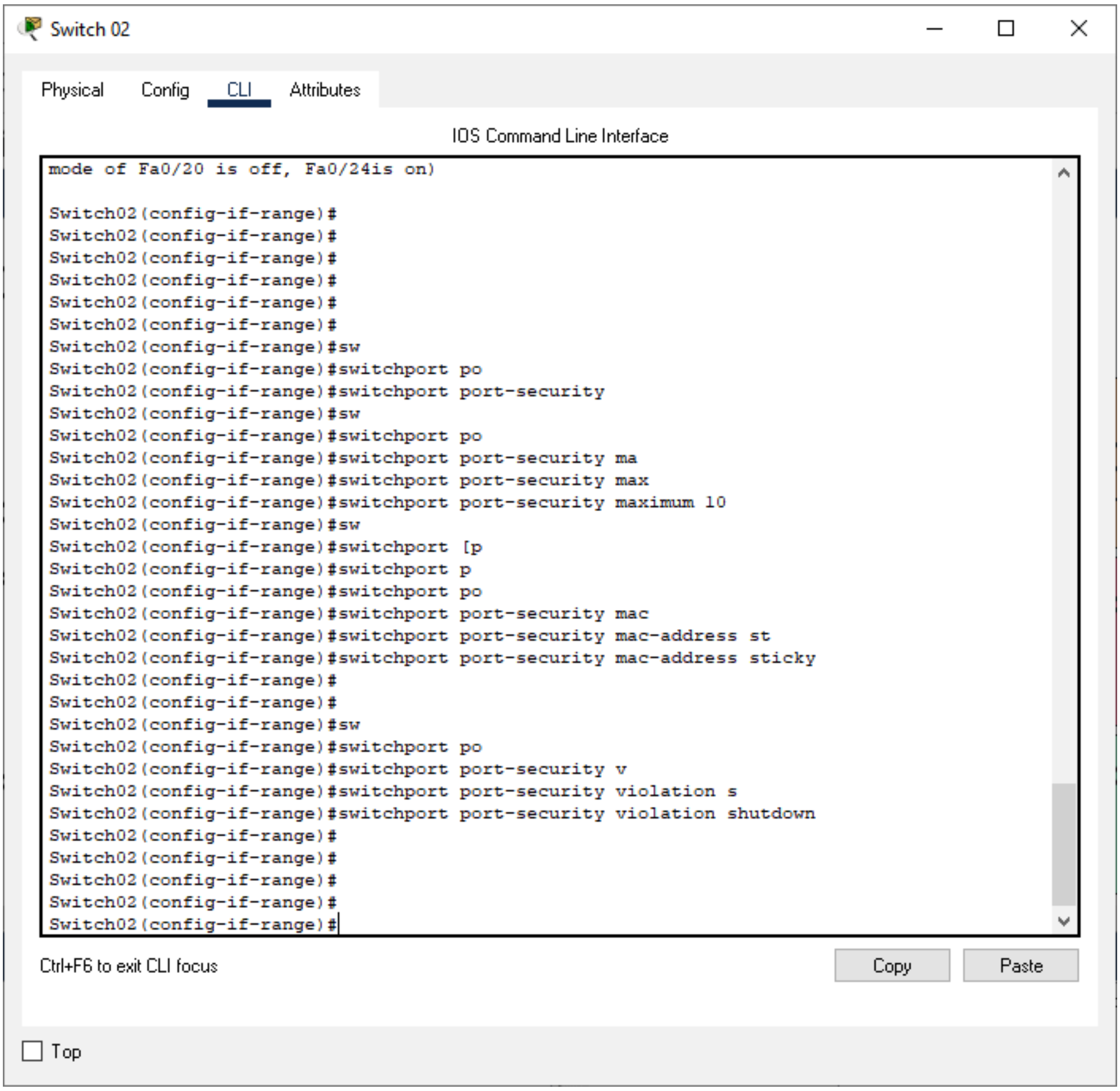


```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int ra fa 0/1-5
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mo
Switch(config-if-range)#switchport mode ac
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access vl
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#int ra fa 0/6-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#int ra fa 0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
```

Figure 9: Allocating ports to VLAN 1

-
-

Switch port security

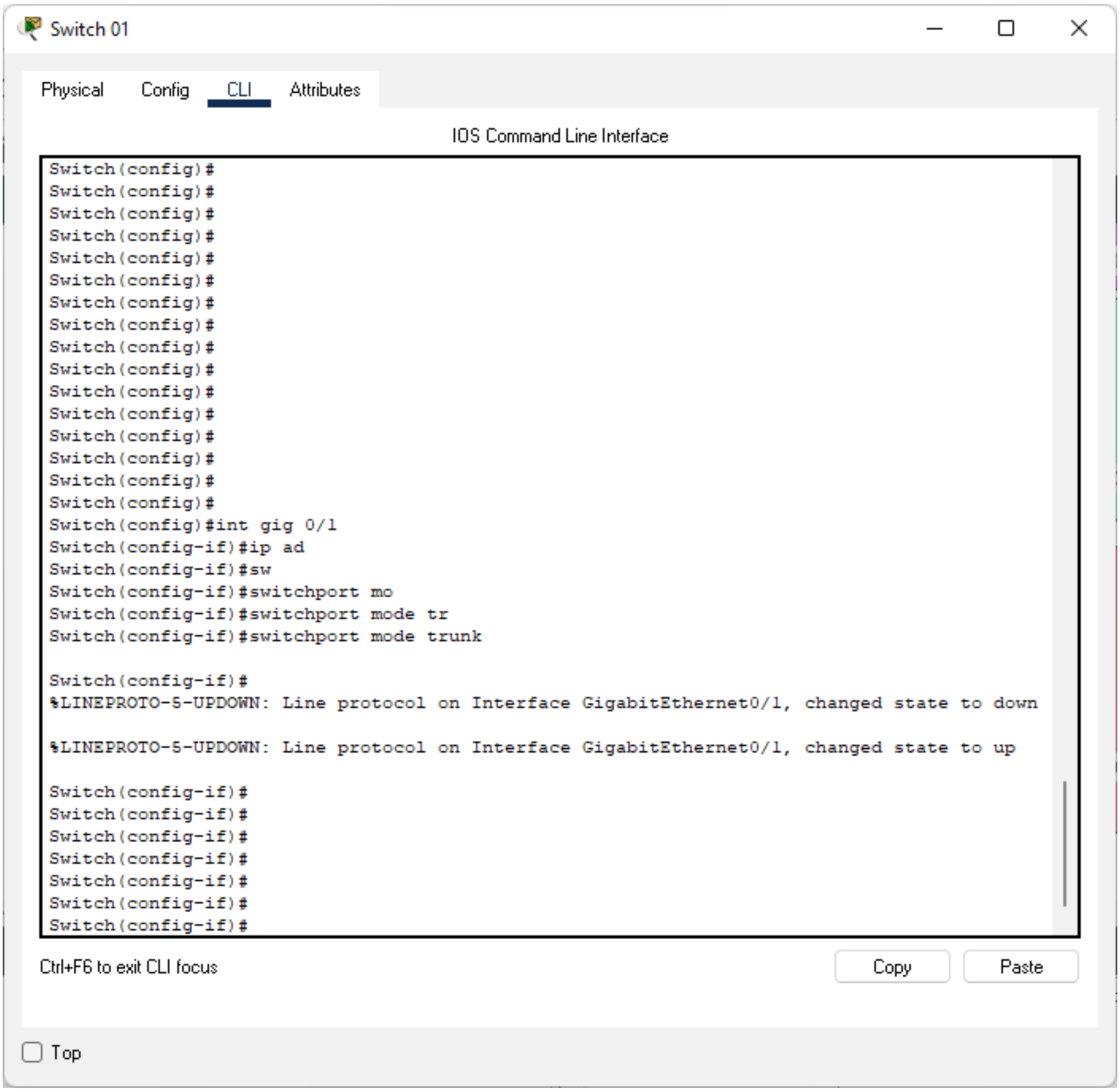


```
mode of Fa0/20 is off, Fa0/24is on)

Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#sw
Switch02(config-if-range)#switchport po
Switch02(config-if-range)#switchport port-security
Switch02(config-if-range)#sw
Switch02(config-if-range)#switchport po
Switch02(config-if-range)#switchport port-security ma
Switch02(config-if-range)#switchport port-security max
Switch02(config-if-range)#switchport port-security maximum 10
Switch02(config-if-range)#sw
Switch02(config-if-range)#switchport [p
Switch02(config-if-range)#switchport p
Switch02(config-if-range)#switchport po
Switch02(config-if-range)#switchport port-security mac
Switch02(config-if-range)#switchport port-security mac-address st
Switch02(config-if-range)#switchport port-security mac-address sticky
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#sw
Switch02(config-if-range)#switchport po
Switch02(config-if-range)#switchport port-security v
Switch02(config-if-range)#switchport port-security violation s
Switch02(config-if-range)#switchport port-security violation shutdown
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
Switch02(config-if-range)#
```

Figure 10: Switch port security 1

-
-

Switch port trunk



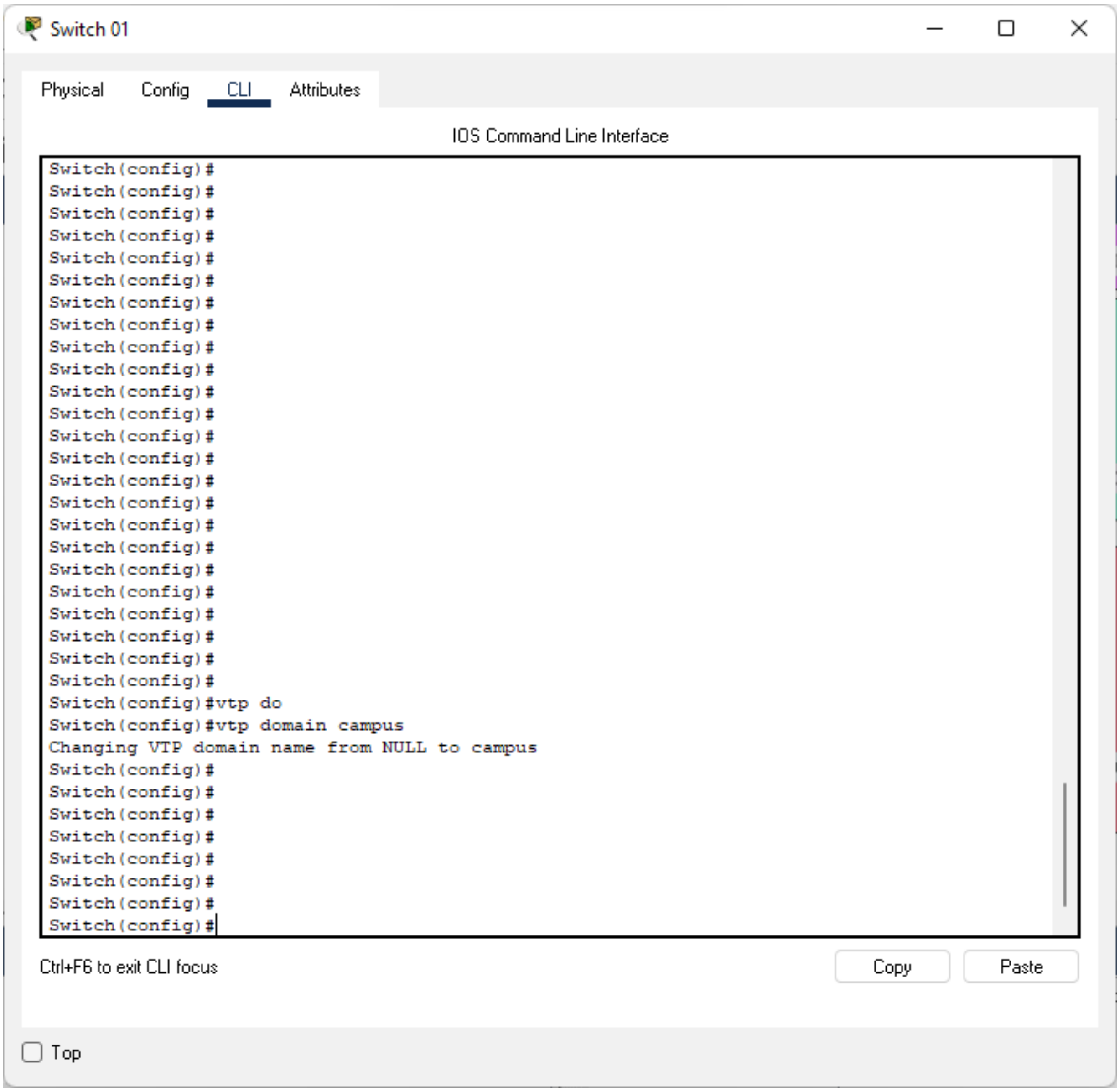
```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int gig 0/1
Switch(config-if)#ip ad
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
```

Figure 11: Switch port trunk 1

-

-

VTP Domain

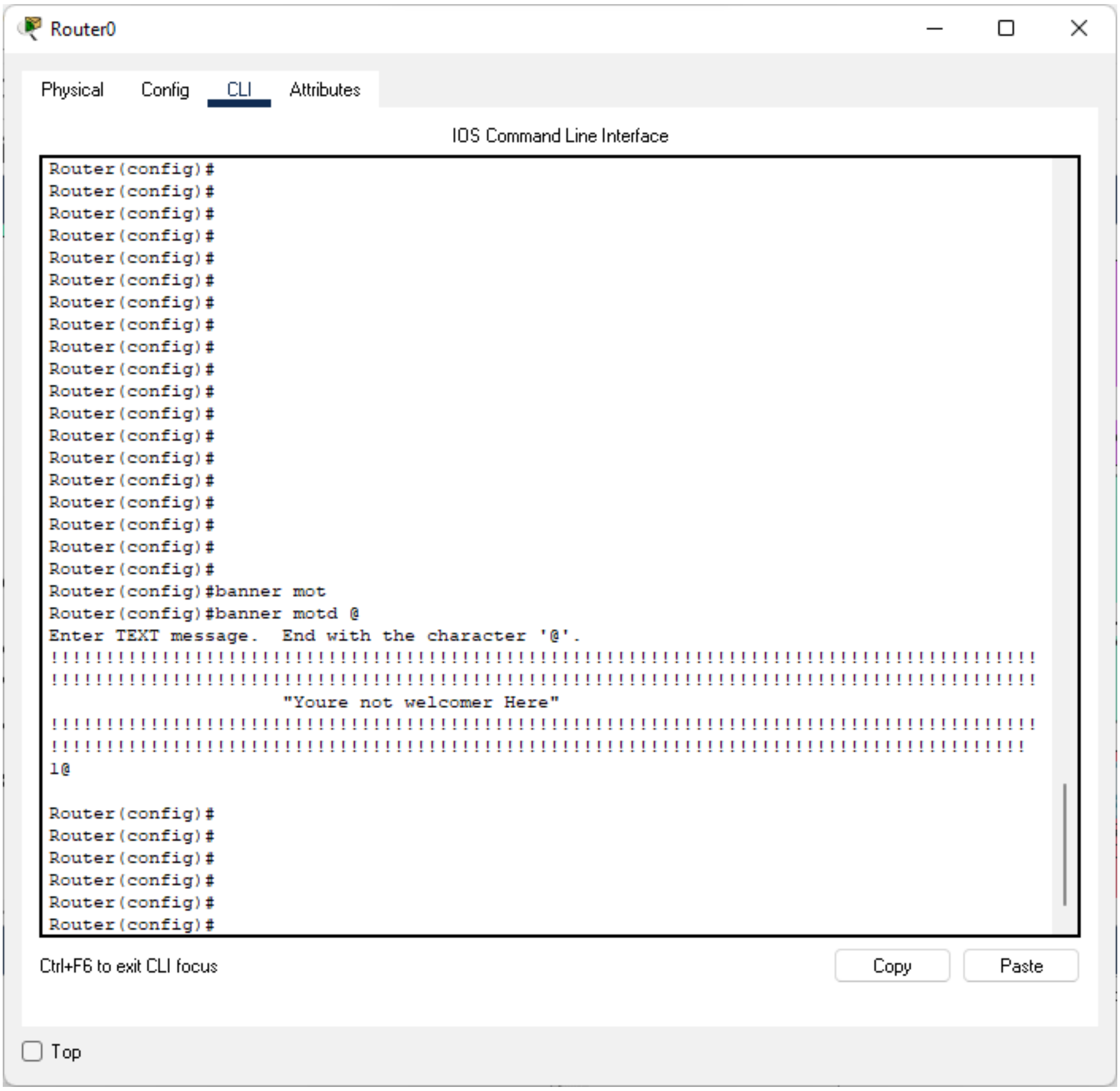


```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vtp do
Switch(config)#vtp domain campus
Changing VTP domain name from NULL to campus
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```

Figure 12: VTP Domain 1

-
-

Creating banner



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#banner mot
Router(config)#banner motd @
Enter TEXT message.  End with the character '@'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                     "Youre not welcomer Here"
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
1@

Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

Figure 13: Creating banner 1

pfSense Screenshot

Login

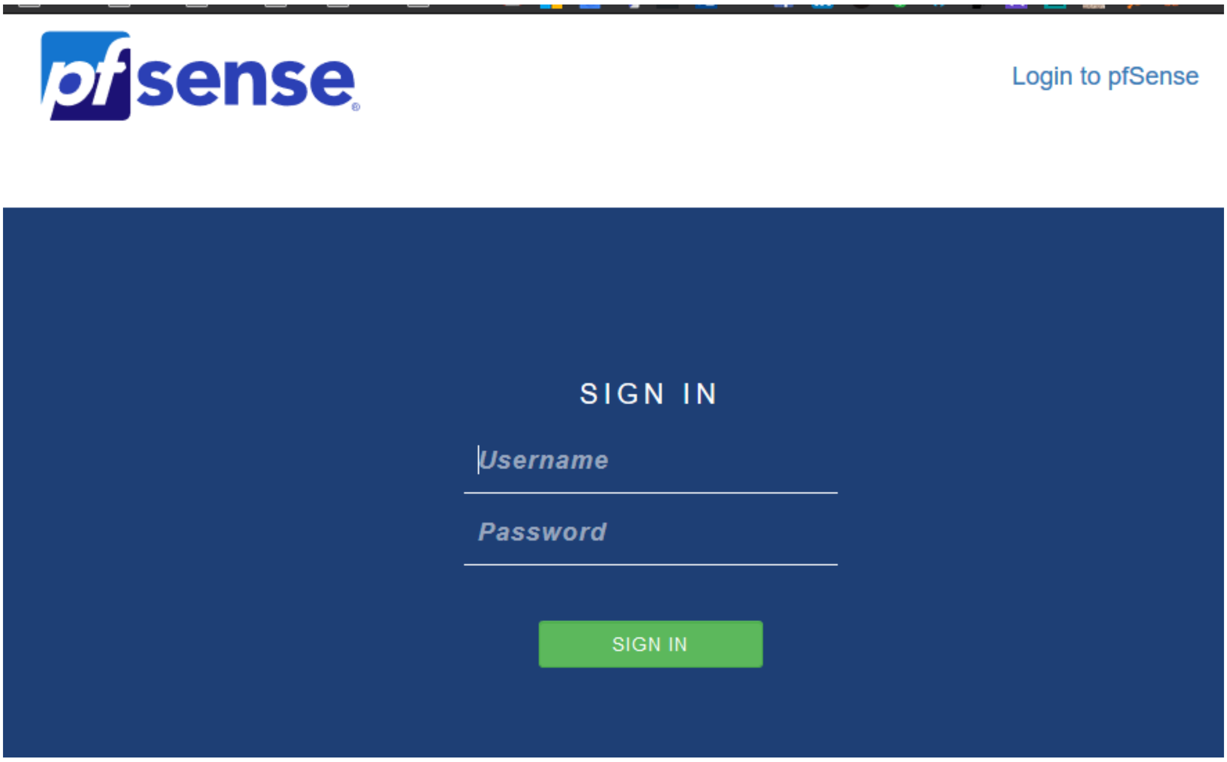
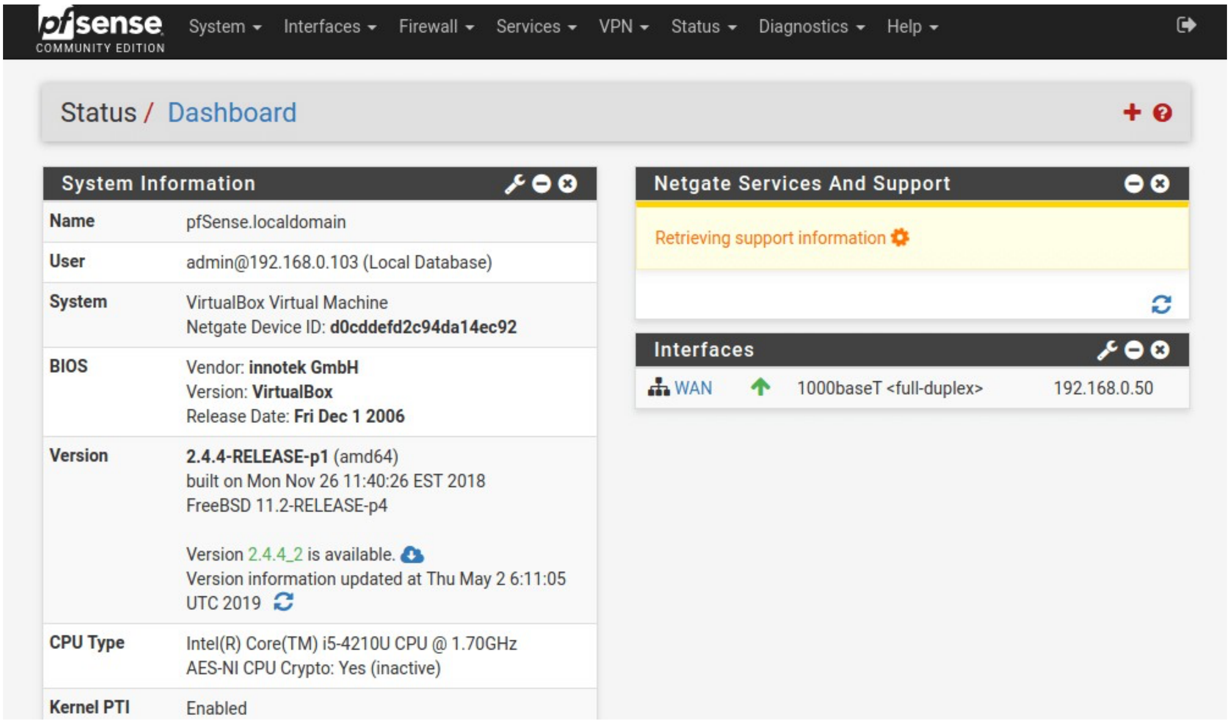


Figure 14: Login 1

-
-

Dashboard



Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.0.103 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: **d0cddefd2c94da14ec92**
BIOS	Vendor: **innotek GmbH** Version: **VirtualBox** Release Date: **Fri Dec 1 2006**
Version	**2.4.4-RELEASE-p1** (amd64) built on Mon Nov 26 11:40:26 EST 2018 FreeBSD 11.2-RELEASE-p4 Version 2.4.4_2 is available. Version information updated at Thu May 2 6:11:05 UTC 2019
CPU Type	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled

Netgate Services And Support

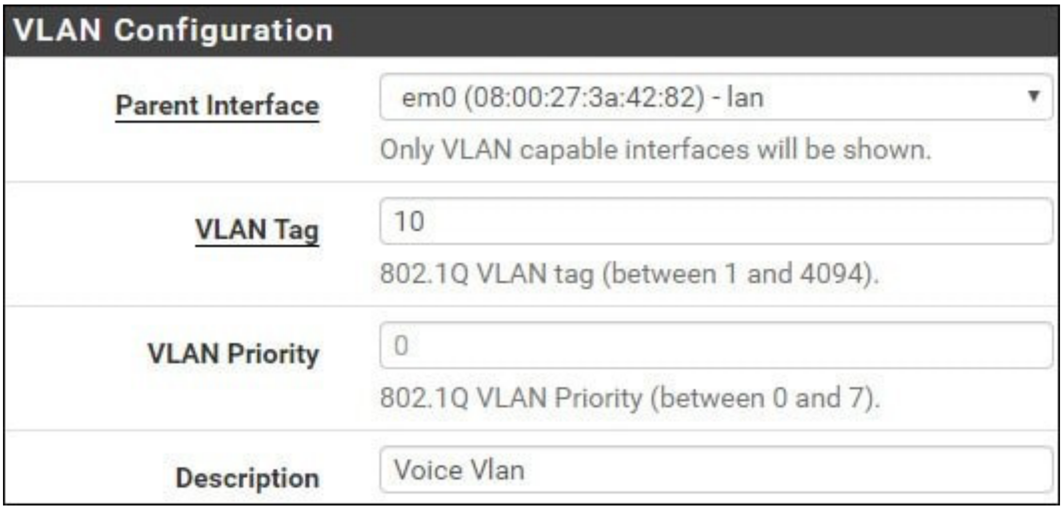
Retrieving support information

Interfaces

WAN	1000baseT <full-duplex>	192.168.0.50

Figure 15: Dashboard 1

Create VLAN



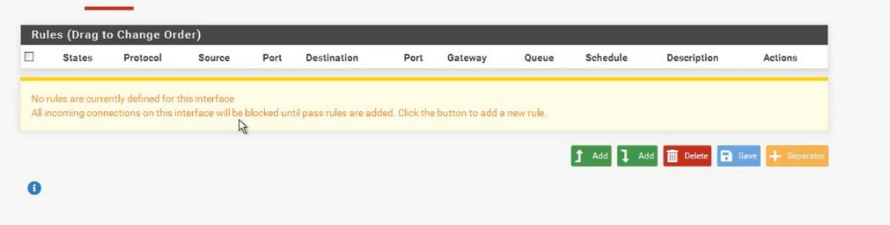
VLAN Configuration

Parent Interface	em0 (08:00:27:3a:42:82) - lan Only VLAN capable interfaces will be shown.
VLAN Tag	10 802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0 802.1Q VLAN Priority (between 0 and 7).
Description	Voice Vlan

Figure 16: Create VLAN 1

-
-

Basic Firewall configuration



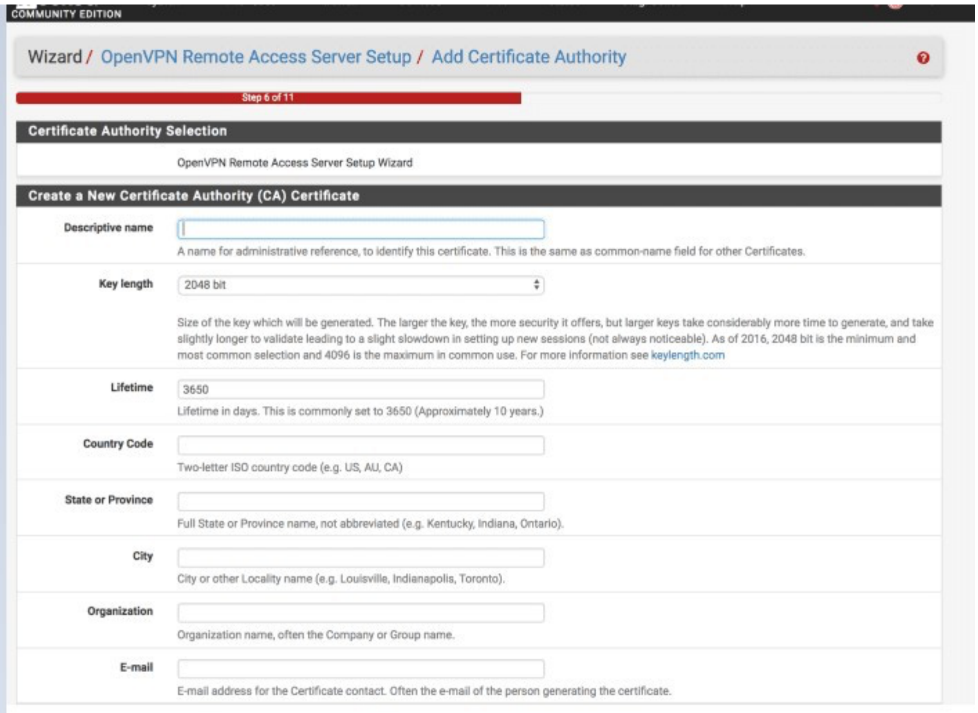
Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Figure 17: Basic Firewall configuration 1

VPN setup



COMMUNITY EDITION

Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority

Step 6 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length: 2048 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime: 3650
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

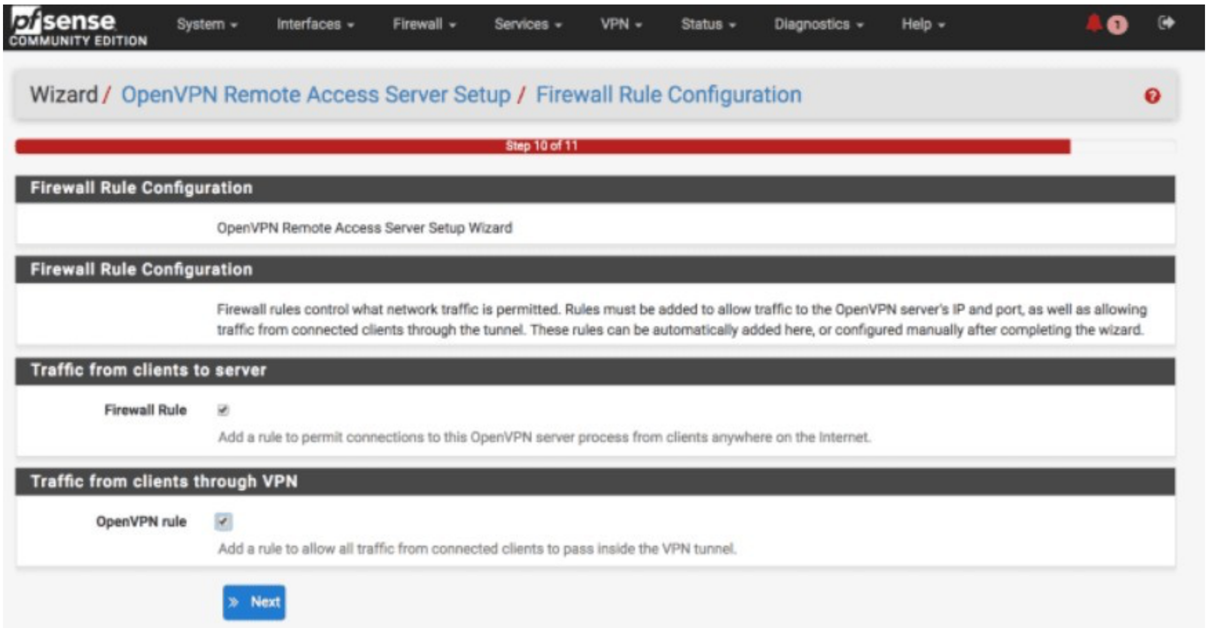
Organization
Organization name, often the Company or Group name.

E-mail
E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate.

Figure 18: VPN setup 1

-
-

Automated firewall



Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule ☑

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

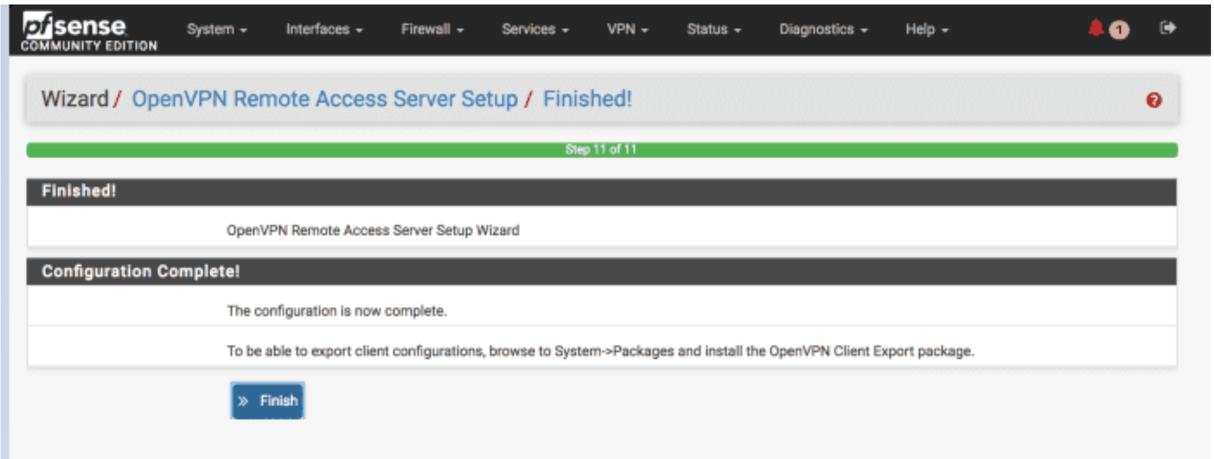
Traffic from clients through VPN

OpenVPN rule ☑

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

Figure 19: Automated firewall 1

Installation wizard is complete



Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

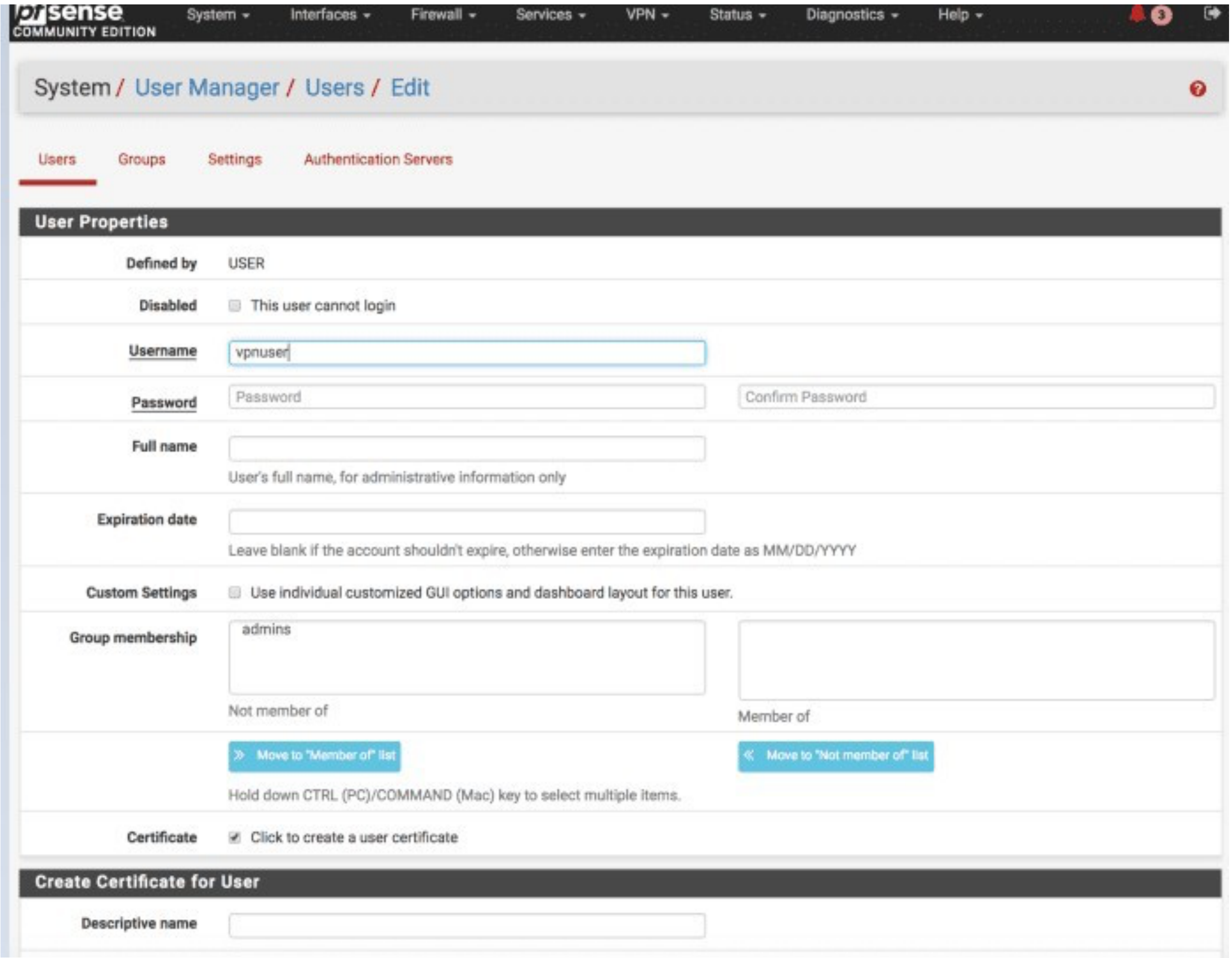
The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

Figure 20: Installation wizard is comple 1

-
-

Opening VPN



System / User Manager / Users / Edit

User Properties

Defined by	USER
Disabled	□ This user cannot login
Username	vpnuser
Password	Password / Confirm Password
Full name	User's full name, for administrative information only
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	□ Use individual customized GUI options and dashboard layout for this user.
Group membership	Not member of: admins Member of: Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate	☑ Click to create a user certificate

Create Certificate for User

Descriptive name	

Figure 21: Opening VPN 1

Quality of Service (QoS)

With QoS being a group of technologies which help networks to guarantee their capability to run both time-critical and low-priority applications and traffic traffic on networks that on limited capacity. QoS are technology that deals with having the network traffic into different categories, the flows with specific differentiation in handling and capacity are given different allocation. This will aid the network administrator to place the packets in the order which the packets are being processed and the amount of the bandwidth which is allocated to that application or traffic flow

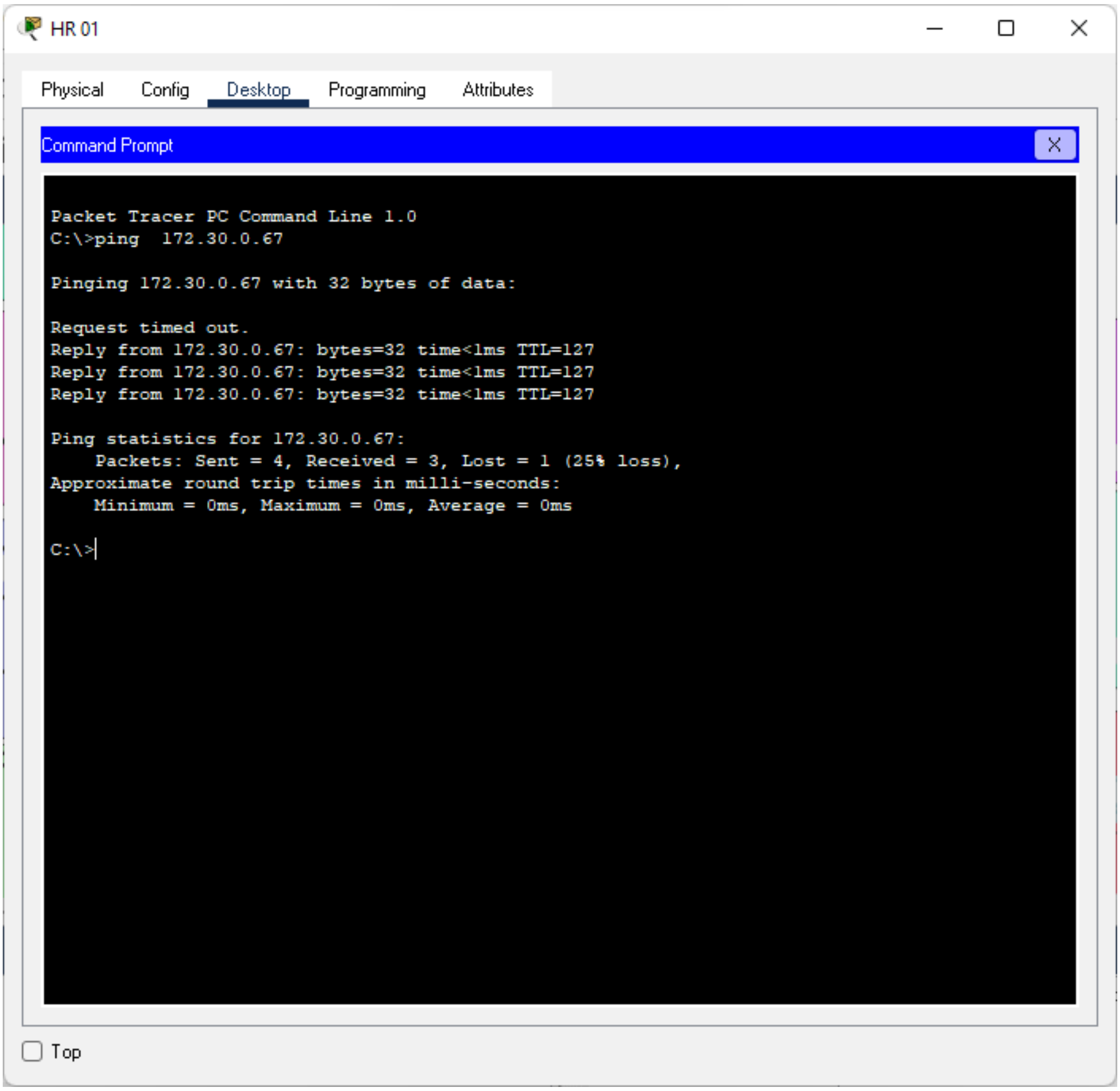
Implementing QoS for Care Medical Hospital

It is undeniable that security is one of the most important components of networking. And that has been a discussed topic by the senior experts. Security is an essential component of every secure network. However, there is more to that network family that stands out; it is a sophisticated way that this novel technique that brings it out clearly. Now, we are going to watch the film titled "Network Quality of Service". The categories are made that can be used to organize the information. We have recently finished with the delivery of a security system at AstraZeneca Campus. What has been definitely manifested is the fact that the quality of service is improved as well as the simulation and numeric equation results are the same. The AstraZeneca jobs of tomorrow would show which of the features mentioned is the most essential; hence, work in the AstraZenca Campus will determine it. Necessity of achievable level of Quality-of-Service (QoS) parameters and then optimal security level for the quality, in order to achieve the desired quality level.

Task 4

Test Plan

Ping HR to Administrator

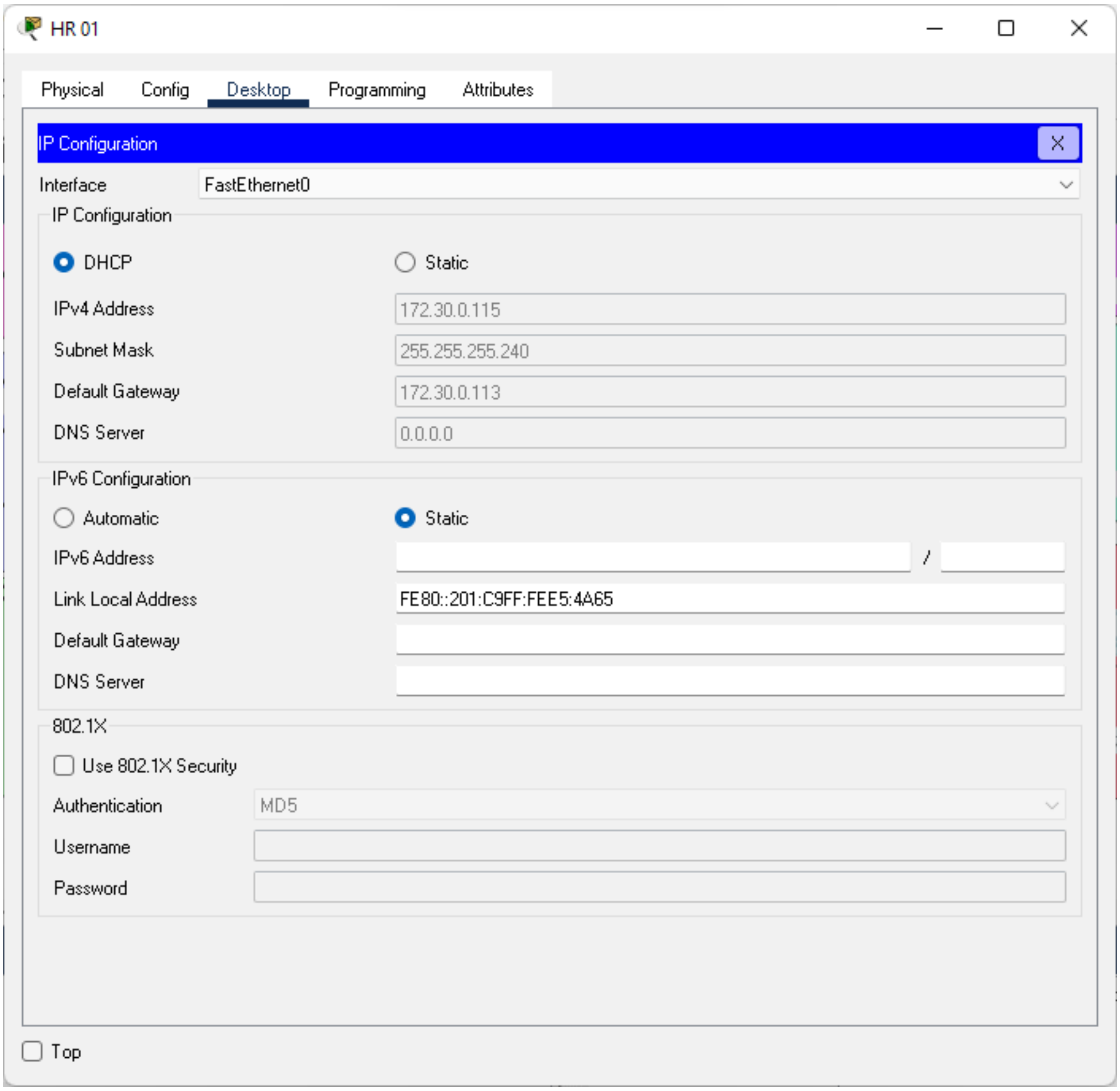


```
Packet Tracer PC Command Line 1.0
C:\>ping  172.30.0.67

Pinging 172.30.0.67 with 32 bytes of data:

Request timed out.
Reply from 172.30.0.67: bytes=32 time<1ms TTL=127
Reply from 172.30.0.67: bytes=32 time<1ms TTL=127
Reply from 172.30.0.67: bytes=32 time<1ms TTL=127

Ping statistics for 172.30.0.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 22: Ping HR to Administrator 1

-
-

Dynamic Ip to HR



Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 172.30.0.115

Subnet Mask 255.255.255.240

Default Gateway 172.30.0.113

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FEE5:4A65

Default Gateway

DNS Server

802.1X

□ Use 802.1X Security

Authentication MD5

Username

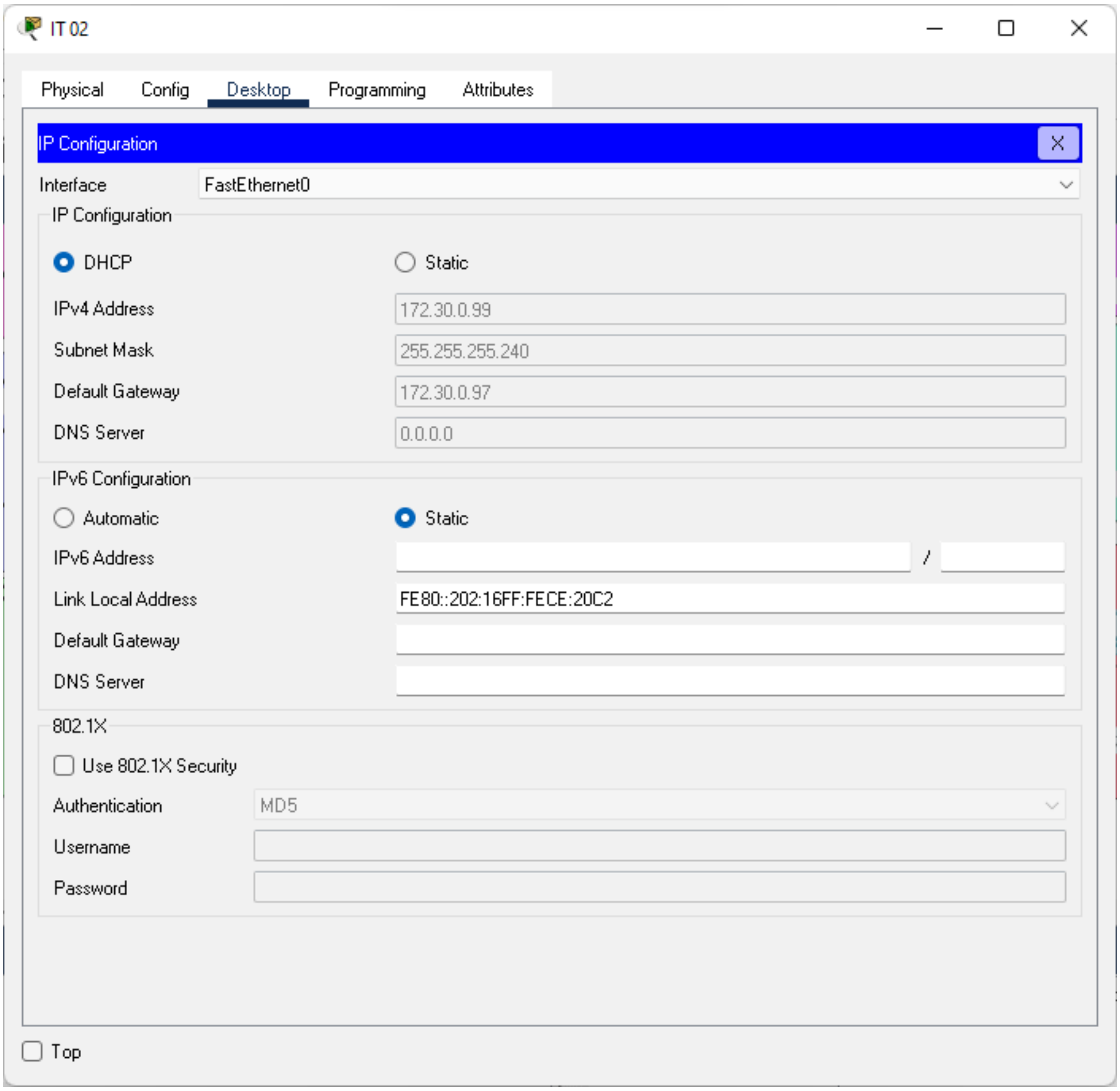
Password

□ Top

Figure 23: Dynamic Ip to HR 1

-
-

Dynamic Ip to IT



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 172.30.0.99

Subnet Mask: 255.255.255.240

Default Gateway: 172.30.0.97

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:16FF:FECE:20C2

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

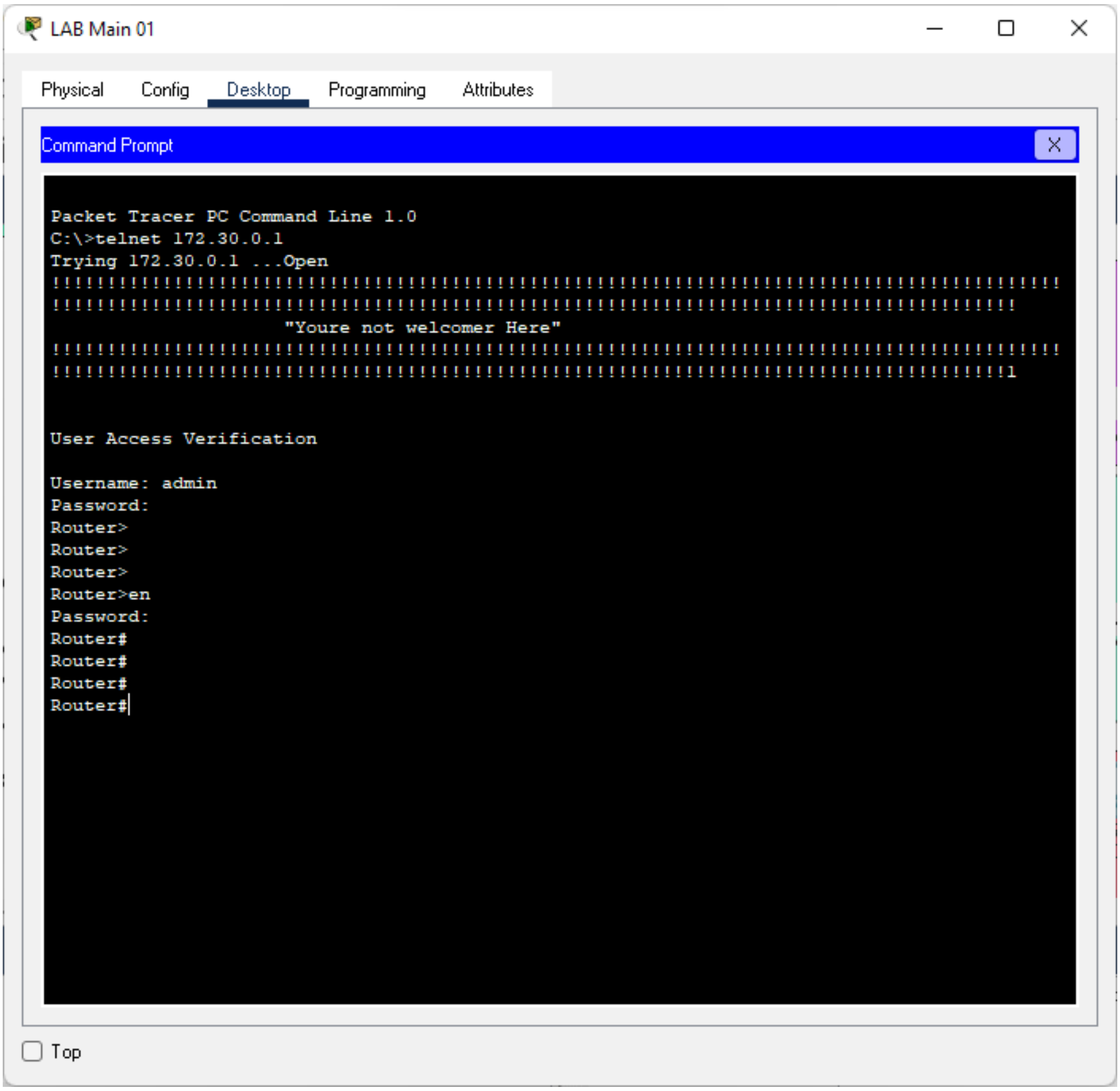
Username:

Password:

Figure 24: Dynamic Ip to IT 1

-
-

Check enable secret

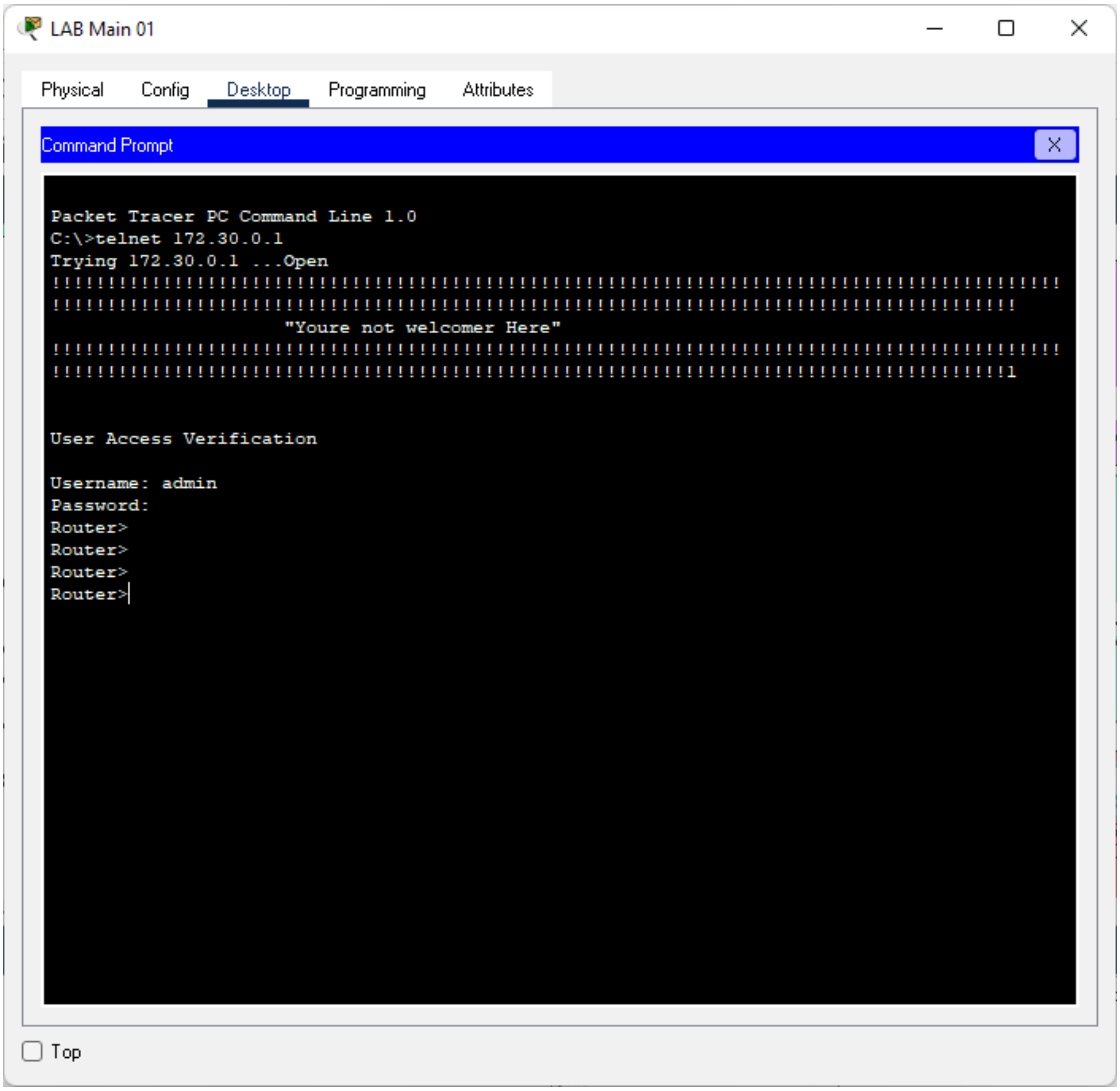


```
Packet Tracer PC Command Line 1.0
C:\>telnet 172.30.0.1
Trying 172.30.0.1 ...Open
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                     "Youre not welcomer Here"
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!1


User Access Verification

Username: admin
Password:
Router>
Router>
Router>
Router>en
Password:
Router#
Router#
Router#
Router#
```

Figure 25: Check enable secret 1

-
-

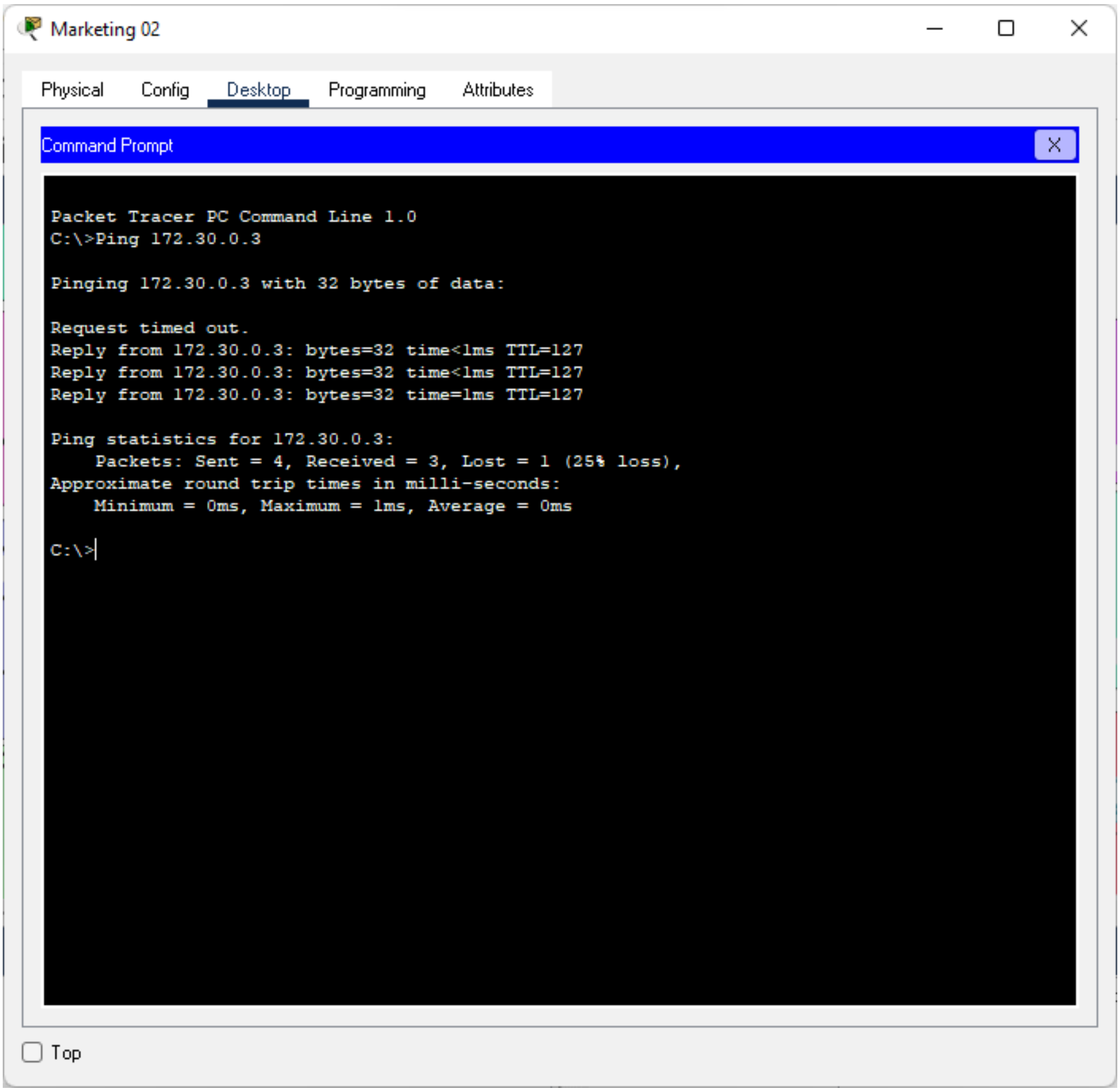
Check Banner



```
Packet Tracer PC Command Line 1.0
C:\>telnet 172.30.0.1
Trying 172.30.0.1 ...Open
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                     "Youre not welcomer Here"
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!1


User Access Verification

Username: admin
Password:
Router>
Router>
Router>
Router>
```

Figure 26: Check Banner 1

Ping Marketing to Main Lab



```
Packet Tracer PC Command Line 1.0
C:\>Ping 172.30.0.3

Pinging 172.30.0.3 with 32 bytes of data:

Request timed out.
Reply from 172.30.0.3: bytes=32 time<1ms TTL=127
Reply from 172.30.0.3: bytes=32 time<1ms TTL=127
Reply from 172.30.0.3: bytes=32 time=1ms TTL=127

Ping statistics for 172.30.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 27: Ping Marketing to Main Lab 1

Ping Marketing to Main Lab

Future improvements

For other pending developments on our networks, security, wires, and many other elements are key issues we should factor in. The expedient and effective technique that is applied in order to achieve customer comments and come up with a solution is by making use of the feedback form. In the future, as the startup bonus plan expands around the globe, we will have room to connect and upgrade in the following areas:

Cables

This network employs the use of Cat6 cables in its design as they have the capacity for delivering less load as compared to previous versions. This could work for now but may need to change as things progress. Also, however ,in case there is a growth in employees, traffic will as well increase, consequently network capacity will increase. It's going to be hard decision but perhaps it will serve us good. It will be the use of the fiber cable in case. As fibre cabling has great load capacity thus bandwidth limit can be increased to 10G.

IPv6

We incorporate IPv4 into our network since it is capable to hold more than four billion IP addresses. The rather limited quantity of IP addresses, although an excessive number to us is just a fraction of the really huge total number. IPv6 as an add might prove to be a highly useful option for our networks when the time comes. IPv6 can accommodate 2 to the 34th addresses, that is, 340 trillion IP addresses, compared to IPv4 that has a lesser security level. IPv6 supports IPsec in ensuring secrecy, authenticity as well as data integrity. Their ability to run malware programs typically sends ICMP traffic at IPv4 into lots of companies' firewalls, which are usually configurated to block them. Then it was identified that IPsec might be included in the ICMPv6 packets which is the Internet Control Message Protocol for IPv6 implementation. On the one hand, IPv4 has been used for years and IPv6 is new. Therefore, the use of IPv6 will bring the benefit of upgrade and extension to our network.

Backup

Secondly, AstraZeneca Campus must address one of the crucial data backup issues: the rising number of remote files located on clients' laptops, distributed desktops, and mobile devices. Most of data storage, management, and backup software applications recognize only the basic mechanisms required for the single protection of the stored information on the machines.

References

[1]Keary, T. (2019, February 28). Ultimate guide to Packet Tracer. Retrieved April 26, 2024, from ITPRC website: https://www.itprc.com/packet-tracers/

[2]kmbh Follow, K. (2021, November 22). Types of network protocols and their uses. Retrieved April 26, 2024, from GeeksforGeeks website: https://www.geeksforgeeks.org/types-of-network-protocols-and-their-uses/

[3]What is SSL, TLS, and HTTPS? (n.d.). Retrieved April 26, 2024, from Goanywhere.com website: https://www.goanywhere.com/blog/what-is-ssl-tls-and-https

[4](2022). *Cisco Tech Talk: Why network security is important.*

[5](N.d.). Retrieved April 26, 2024, from Cisco.com website: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/vlan/b_1610_vlan_9500_cg/configuring_layer_3_subinterfaces.pdf