Table of Contents

12.

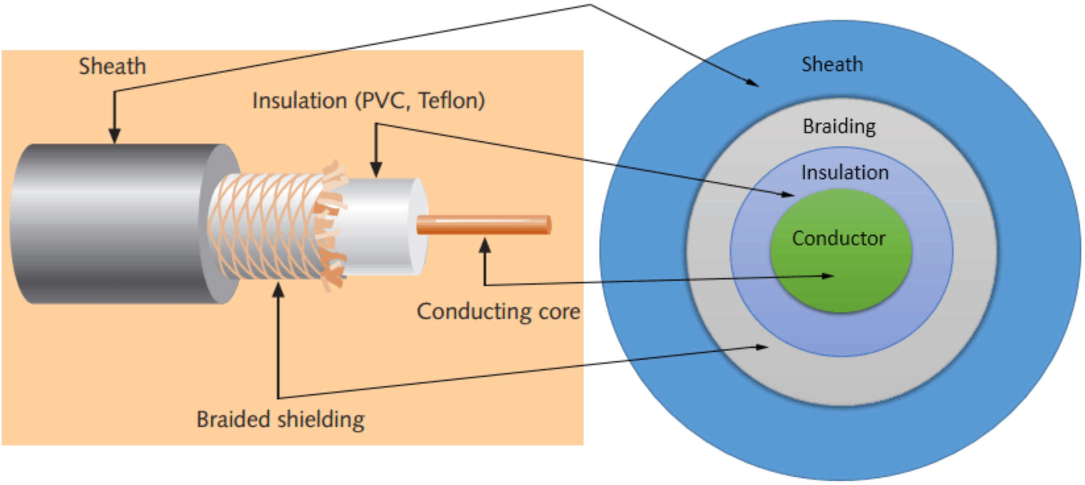
Introduction

I was hired as a network administrator by regional Institute of Technology, to plan and create a network between the company offices in different countries the headquarter is in Amman, and the other offices are in Dubai, Cairo, Beirut, Kuwait, and Jeddah.

Networking Principles

cable types

Coaxial cable



This cable contains conductor, insulator, braid and sheath. The sheath makes the braid, the braid covers the insulator, the insulator covers the conductor. The following picture shows these components

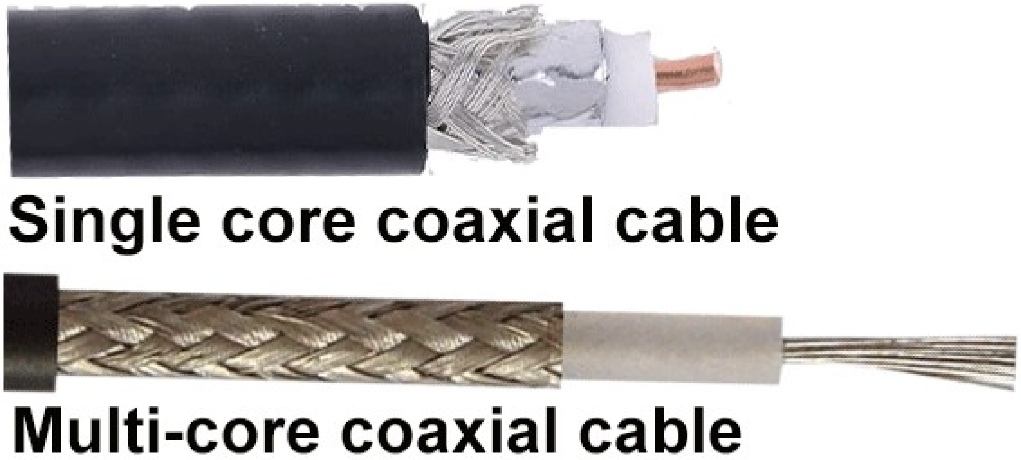
Sheath
This is the coaxial cable's outer layer. It safeguards the wire against physical harm.

Shield braided

Signals are protected from external interference and noise by this shield. The same metal that was utilized to construct the core is utilised to construct this shield.

Insulation

The core is protected by insulation. It also separates the braided shield from the core. Because both the core and the braided shield are made of the same metal, they will contact and cause a short-circuit in the wire if this layer is not there.



Conductor
Electromagnetic signals travel down the conductor. Single-core coaxial cable and multi-core coaxial cable are the two varieties of coaxial cable based on conductor.

A single-core coaxial cable has a single central metal conductor (often copper), whereas a multi-core coaxial cable has many thin strands of metal wires. Both types of cable are seen in the accompanying illustration.

Specifications of coaxial cables

Type	**Ohms**	**AWG**	**Conductor**	**Description**
RG-6	75	18	Solid copper	Used in cable network to provide cable Internet service and cable TV over long distances.
RG-8	50	10	Solid copper	Used in the earliest computer networks. This cable was used as the backbone cable in the bus topology. In Ethernet standards, this cable is documented as the 10base5 Thicknet cable.
RG-58	50	24	Several thin strands of copper	This cable is thinner, easier to handle and install than the RG-8 cable. This cable was used to connect a system with the backbone cable. In Ethernet standards, this cable is documented as the 10base2 Thinnet cable.
RG-59	75	20 - 22	Solid copper	Used in cable networks to provide short-distance service.

1. Twisted-pair cables

   Twisted-pair cable was designed particularly for computer networks. Ethernet cable is another name for this cable. This cable is used in almost all current LAN computer networks.

   Color-coded pairs of insulated copper wires make up this cable. To make a pair, every two wires are twisted around each other. There are usually four pairings. One solid color and one stripped color wire are included in each pair. Blue, brown, green, and orange are solid hues. The solid color is blended with the white color in stripped color.

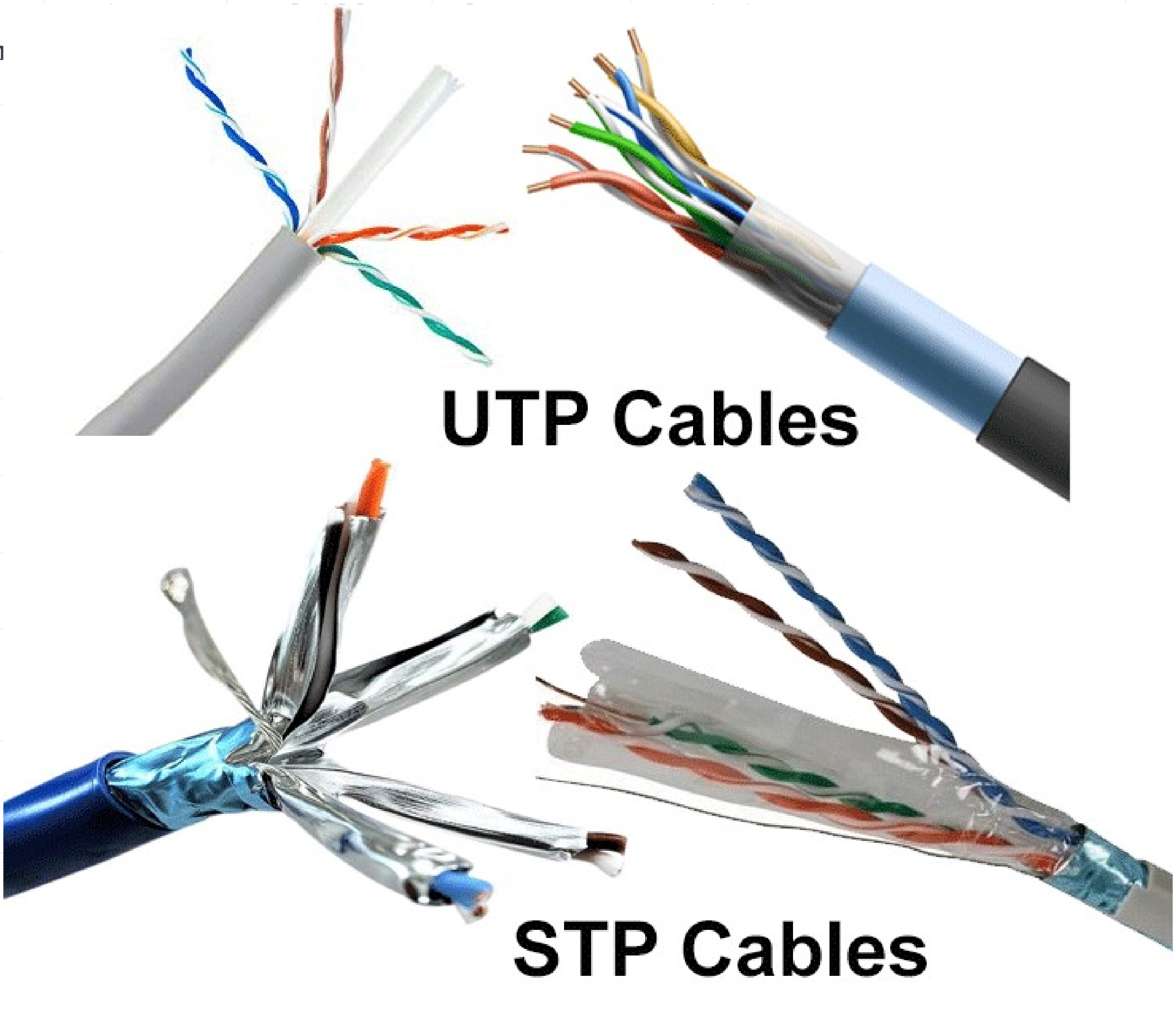
   Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

   In the UTP (Unshielded twisted-pair) cable, all pairs are wrapped in a single plastic sheath.

   In the STP (Shielded twisted-pair) cable, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

   STP and UTP cables have similarities and differences.
   STP and UTP may transfer data at speeds of 10Mbps, 100Mbps, 1Gbps, and 10Gbps, respectively.
   The STP cable is more costly than the UTP cable because it contains more materials.
   The RJ-45 (registered jack) modular connectors are used on both wires.

STP cables are more noisy and EMI resistant than UTP cables.
Both cables have a maximum segment length of 100 meters (328 ft).
Each section of both cables may have a maximum of 1024 nodes.
Both types of twisted-pair cables are shown in the figure below.



Category/ name of th cable				
Cat 1				
Cat 2				
Cat 3				
Cat 4				
Cat 5				
Cat 5e				
Cat 6				
Cat 6a				Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pair and shields each pair by its plastic sheath.

2. Fiber optic cable

A core, cladding, buffer, and jacket make up this cable. The core is made up of tiny glass or plastic strands that can transmit data over great distances. The cladding wraps around the core, the cladding wraps around the buffer, and the buffer wraps around the jacket.

The data signals are carried in the form of light by the core.

Light is reflected back to the core by the cladding.

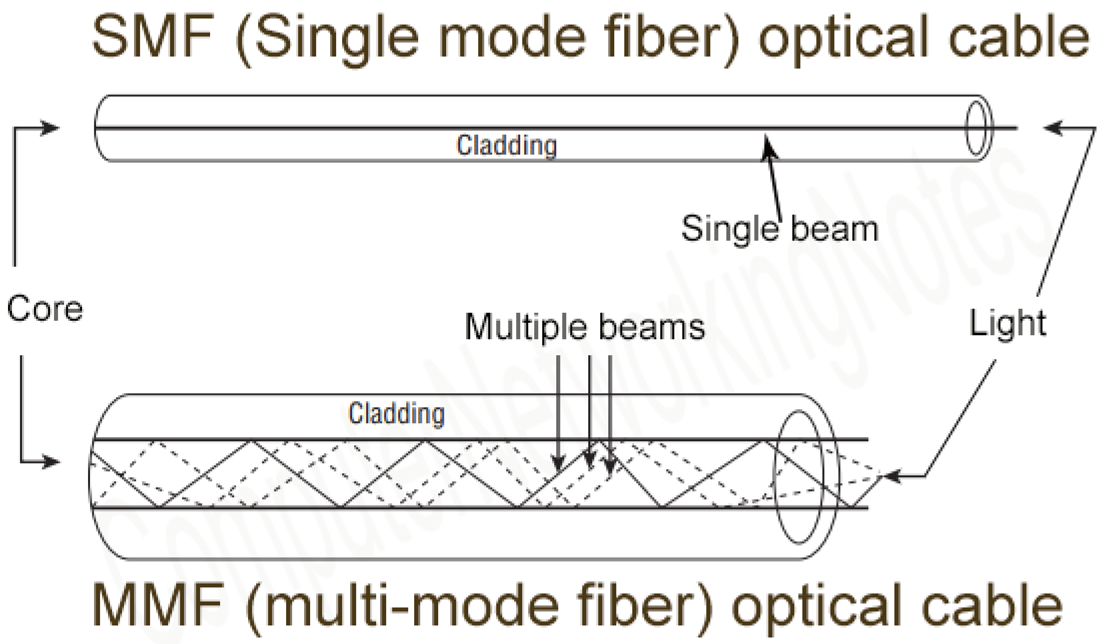
Buffer is a device that prevents light from leaking.

The cable is protected from physical harm by the jacket.
EMI and RFI are not a problem with fiber optic cable. This cable can carry data at the greatest speed over a long distance. It can transfer data at 100Gbps over a distance of 40 kilometers.

Light is used to convey data using fiber optics. Light is reflected from one terminal to the other. There are two varieties of fiber optical cable: SMF and MMF, which differ in the number of light beams transferred at any one moment.

Optical cable with SMF (single-mode fiber)
This wire only transmits a single light beam. Compared to the MMF connection, this is more stable and enables significantly higher bandwidth and longer distances. This cable emits light with wavelengths of 1300 or 1550 nanometers and is powered by a laser.

Optical cable using MMF (multi-mode fiber)
This wire contains several light beams. This cable carries a lot more data than the SMF cable since it has many beams. For shorter distances, this cable is utilized. This cable transmits 850 or 1300 nanometer wavelengths of light using an LED as the light source.


SMF (Single mode fiber) optical cable
Cladding
Single beam
Core
Multiple beams
Light
Cladding
MMF (multi-mode fiber) optical cable

2. network types
    1. Local Area Network (LAN)

       You may have heard of these types of networks. Local networks are one of the most talked about networks, one of the most common, and one of the most important and simplest types of networks. A local network connects a group of computers and low-voltage devices that are located over a short distance (within a building or between groups of two or three buildings) to exchange information and resources. Businesses typically operate and maintain local networks.

    2. Wireless Local Area Network (WLAN)

       A WLAN works like a LAN and uses wireless networking technologies like Wi-Fi. These types of networks are typically used in LAN applications of the same type and do not require equipment that relies on physical cables to connect to the network.

    3. Wide Area Network (WAN)

       A WAN, slightly more complex than a LAN, connects computers that are physically separated. This allows low-voltage computers and devices to communicate remotely over large networks that are miles apart.

    4. Virtual Private Network (VPN)

       With the proliferation of private networks on the Internet, VPNs allow devices to send and receive data even when they are not connected to a private network as if they were connected. Virtual point-to-point connections allow users to remotely access private networks. If you have questions about which type of network is best for your business, or want to learn more about network solutions that improve working hours, ensure security and improve user access.

Protocols

1. DHCP: Dynamic Host Configuration Protocol

   DHCP is a communication protocol that allows network administrators to automatically determine the IP address of a network. An IP network requires a unique IP address for each device connected to the Internet. DHCP allows network administrators to distribute IP addresses from a central point and automatically send new IP addresses when devices connect to other locations on the network. DHCP works in a client/client model.

2. DNS: Domain Name System protocol

   The DNS protocol is used to translate or assign hostnames to IP addresses. DNS works in a client/client model and uses a distributed database at the name server layer. Hosts are selected based on complex and difficult-to-manage IP addresses. IP addresses are also dynamic, so you need to map domain names to IP addresses. DNS helps solve this problem by translating your website's domain name into a numeric IP address.

3. FTP: File Transfer Protocol

   FTP allows you to share files locally and remotely between hosts and works over TCP. To transfer files, FTP creates two TCP connections: a control connection and a data connection. Control connections are used to transfer control information such as passwords, file recovery, command history, etc. It then uses the data connection to transfer the actual file. Both connections work in parallel during the file transfer process.

4. HTTP: Hyper Text Transfer Protocol

   HTTP is an application-layer protocol used in distributed, collaborative, and cloud multimedia systems. It works with a client-client model in which the web browser acts as a client. Data such as text, images, and other multimedia files are exchanged on the World Wide Web via HTTP. As a request-and-response protocol, a client sends a request to a server. The server processes the response before sending it back to the client. HTTP is a stateless protocol. This means that the client and server know each other as long as there is no error in communication between the client and server. So the client and server forget each other. This behavior prevents the client and server from storing information between requests.

5. IMAP and IMAP4: Internet Message Access Protocol (version 4)

   IMAP is an email protocol that allows email clients to access messages stored on an email server and treat them as if they were on a remote device. IMAP follows a client-client model, allowing multiple clients to simultaneously access messages on a shared mail server. IMAP involves the process of creating, deleting, and renaming mailboxes. Check for new messages. Permanently delete messages. Inserts and removes flags. etc. The current version of IMAP is version 4 version 1.

6. POP and POP3: Post Office Protocol (version 3)

   The postal protocol is also a messaging protocol. This protocol allows end users to download e-mail from an e-mail server to an e-mail client. If you download your email locally, you can read it even without an internet connection. When an email is delivered locally, it is also removed from the mail server to free up storage space. Unlike IMAP4, POP3 is not designed for large-scale message manipulation on mail servers. POP3 is the latest version of the postal protocol.

7. SMTP: Simple Mail Transfer Protocol

   SMTP is a protocol for sending email safely and efficiently. SMTP is a push protocol used to send email while POP and IMAP are used to receive email from end users. SMTP sends e-mail messages between systems and advertises incoming e-mail messages. SMTP allows a client to send e-mail to another client on the same network through a logon relay or gateway on both networks.

Devices

1. Hub

   A hub connects various devices to a computer's network. Hubs also act as repeaters because they amplify signals that are split over long distances by jumper cables. A hub is the simplest device in a family of networking devices because it connects LAN components with a similar protocol and allows the hub to be used for digital and analog data as long as the data format is configured. 'Enrollment. For example, if the input data is digital, the distributor must package it. However, if the input data is analog, the hub signals it. The hub does not perform any packet filtering or addressing functions. It simply sends a data packet to all connected devices. Hubs operate at the physical layer of the Open Systems Interconnection (OSI) model. There are two types of hubs: single-part and multi-part.

2. Switch

   Switches are usually smarter than hubs. A switch is a multi-port device that improves network performance. Switches handle limited routing information through internal network nodes and allow connections to systems such as hubs and routers. LAN chains are usually connected through switches. In general, a key can direct the hardware address of an incoming packet to the appropriate destination. Switches allow virtual connections to improve network performance between hubs or routers. The switch also improves network security because Network Monitor is more difficult to monitor virtual connections. A switch can be thought of as a device that combines some of the great features of a router and a hub. Switches can operate at either the data link layer or the OSI network layer. A multilayer switch is a switch that can operate at both levels. In other words, it acts as both a switch and a router. Multilayer switches are powerful devices that support the same routing protocols as routers, and switches can be vulnerable to distributed denial of service (DDoS) attacks. Flood protection switches are used to prevent harmful traffic. It is important to protect the switch ports. So make sure the switch is secure. Disable all unused ports and enable DHCP snooping, ARP discovery, and MAC address filtering.

3. Router

   Routers help route packets to their destinations by tracing routes from the ocean to interconnected network devices with different network topologies. A router is a smart device that stores information about connected networks. Most routers can be configured to act as a firewall that filters packets and uses access control lists (ACLs). Routers are also used by Channel Service Units/Data Service Units (CSU/DSU) to convert the LAN format to the WAN architecture. This is necessary because local area networks and wide area networks use different network protocols. These routers are called border routers. This is a remote LAN-to-WAN connection that operates within a network and uses a router to divide the internal network into two or more subnets. A router can also internally connect to other routers to create zones that operate independently. The router communicates with the destination via local communication while maintaining a schedule. A router contains information about the systems it is connected to and where to query if the destination is unknown. Routers typically pass routing and other information using one of three standard protocols: Routing Information Protocol (RIP), Border Gateway Protocol (BGP), or Open Shortest Path First (OSPF).
   Your router is at the forefront and should be configured to only allow network traffic from your network administrator. The path itself can be configured either statically or dynamically. If it

has changed, you can only configure it manually and it will not change until you change it. As it travels, it finds other routers in the area and uses that router's information to create its own routing table. A router is a public device that connects two or more heterogeneous networks. They are typically used for specific computers and have a separate network I/O interface for each connected network. Because routers and gateways are the backbone of large computer networks such as the Internet, breaking large packets into smaller elements provides flexibility and the ability to handle different network addressing schemes and frame sizes. Each router interface has a unique Address Resolution Address (ARP), LAN address (NIC address), and Internet Protocol (IP). A router can use a routing table to know the path a packet can take from its source to its destination. As with bridges and switches, routing tables grow dynamically. When a packet is received, the router strips the header and trailer from the packet and parses the IP header on arrival using the source and destination addresses and datatype details. It also updates the router table with new addresses that are not already in the table. The IP header and access time information are entered into the routing table. Routers typically operate at the OSI network layer.

4. Bridge

   A bridge is used to connect two or more hosts or networks. The main role of a bridge in a storage network architecture is to redirect frames between different parts of the bridge. Sends frames using a Media Access Control (MAC) address. Bridges can transmit data or prevent data from passing through by marking the MAC addresses of devices connected to each segment. A bridge can also be used to connect two physical LANs to a larger logical LAN. Bridges only work on the physical layer and data connections of the OSI model. Bridges are used to divide large networks into smaller sections by placing them between two physical parts of a network and controlling the flow of data between them.
   Bridges are similar to hubs in many ways, including the fact that they use similar protocols to connect LAN components. However, bridging filters incoming data packets, called frames, before sending them. When filtering data packets, the bridge does not change the format or content of the input data. Bridge uses a dynamic bridge table to filter and forward frames in the grid. The initially empty bridge table contains the LAN address of each computer on the LAN and the address of each bridge interface that connects the LAN to another LAN. Like hubs, bridges are single-part and multi-part bridges that have mostly been dismantled in recent years and replaced with more powerful keys. In fact, switches are sometimes referred to as "multiport bridges" because of the way they work.

5. Gateway

   Gates generally work with transport layer and OSI models. There are many protocols and standards from different vendors at the shipping level. Portals are used to interact with portals. Gates provides translation between networking technologies such as Open Systems Communication (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). For this reason, a gateway connects two or more independent networks, each using its own routing algorithms, protocols, topologies, domain name services, and network management methods and guidelines. A gateway does everything like a router. In fact, a router with additional translation capabilities is a gateway. The ability to translate between different network technologies is called a protocol converter.

6. Modem

   Modems (modulator-demodulators) are used to carry digital signals over analog telephone lines. For example, a digital signal is converted by the modem to an analog signal of a different frequency and transmitted from the receiving point to the modem. The receiving modem performs the inverse conversion and provides a digital output to the device connected to the modem (typically a computer). Digital data is typically sent to the modem over a serial line or a standard RS-232 interface. Many operators offer DSL services, and many cable operators use modems as an end-to-end device to identify and identify home and home users. Modems operate at both the physical and data link level.

7. Repeater

   A repeater is an electronic device that amplifies a received signal. A repeater can be thought of as a device that receives a signal and sends it to a higher level or power. This allows the signal to travel over 100 meters using standard LAN cables. Repeaters operate on a physical level.

Server Types

1. Web server

   Open source web servers are used to access the World Wide Web through public domain software. This server connects information stored on websites on the Internet to your computer. Web servers use "HTTP" codes to store received Internet information and send it to your web browser. This is one of the most common server types.

2. Proxy server

   A proxy server acts as a bridge between the host server and the client server. After going through the proxy server, the proxy sends data from the website to the IP address of your computer. An added layer of security is added because information is requested and then sent from the source to the proxy server instead of being sent directly from one client to another. A proxy server can rule out many malicious organisms on the Internet.

3. Virtual machine (VM)

   As the name suggests, virtual machines regularly store and connect data to cyberspace. IT teams create virtual machines using a hypervisor, also known as a virtual machine monitor (VMM). It is software that can run thousands of virtual machines on a single physical hardware. This method of server virtualization is widely used for data transfer and storage because it is the cheapest type of server.

4. File transfer protocol (FTP) server

   An FTP server is used to transfer files from one computer to another. Files downloaded from your computer are transferred to the server, and files downloaded from the server are extracted to your device. File transfer protocol also refers to the use of servers to connect one computer to another for secure data exchange.

5. Application server

   These servers connect virtual servers to connect clients to the software. This allows the user to log into the app by bypassing downloading data to the device. Application servers are ideal for businesses because they can efficiently host large amounts of application data for multiple users at the same time.

6. File server

   A file server stores data files for multiple users. Allows for fast data retrieval and file storage or computer writing. It is a common type of server that is popular in organizations because many users need to access files stored on their computer more easily and securely than the server.

7. Database server

   A database server serves as a large storage area accessed and used by an organization because it needs to run multiple applications. A database server can operate independently of any database architecture.

8. Mail server

   The mail server stores the mail and delivers it to the customer through the email service platform. The mail server is configured for a persistent network connection so that all users can access their mail through their device without a system.

9. Print server

   A remote print server connects to a local computer and prints over the network. These servers allow companies to serve their entire sector using a single printer. Some printers have their own internal servers that you can install in your office to connect to your network.

10. Domain name system (DNS) server

    This server translates computer-readable domain names into computer language IP addresses. The DNS server finds the address it needs to retrieve the user's search information and forward it to the client computer.

11. The servers that are going to be used are
    1. mail server
    2. print server
    3. DNS
    4. DHCP
    5. HTTP
    6. FTP

       HTTP is used for website hosting, FTP is used to transfer file, Mail services are used for communication, print server is used for sending data to the printer so it can print it, DHCP is used to giving IP address for devices on the network, DNS is used for translating the web address to IP address to get to the site that is required

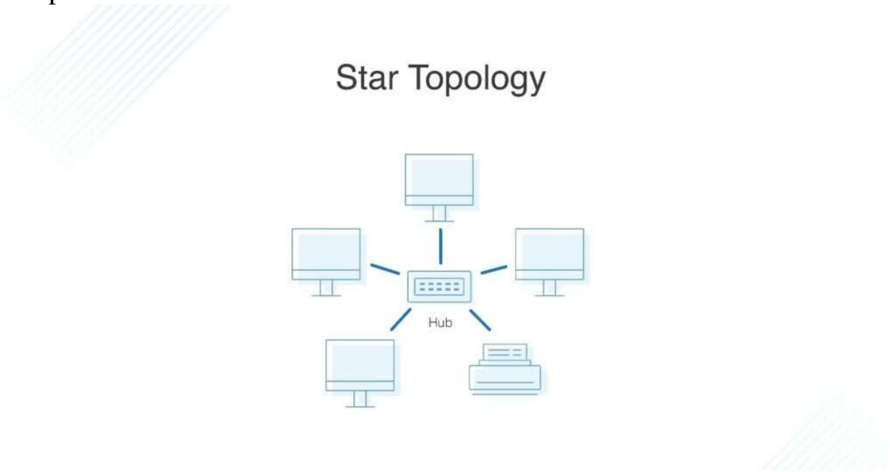
Network Topologies

1. Logical Topology
   Ethernet

   Ethernet padding is the most commonly used logical topology. There are two physical topologies for this topology: bus topology and star topology. The bus topology connects all devices on the network through the same medium, also known as physical channels. Examples of this physical channel are coaxial, twisted pair or optical fiber. With this topology all the other connected devices (Black Box, n.d.) can hear the communication in progress. Ethernet also uses CSMA / CD, which stands for Carrier Sense Multiple Access with collision detection. Carrier Sense prevents transmissions from other devices if one of them is transmitting (Black Box, n.d.). Multiple access refers to the ability of multiple devices to communicate using the same medium (black box, n.d.). Collision detection is a check that occurs to detect if multiple signal transmissions have occurred, mix the signals, wait a random amount of time, and then retransmit. (Black box, n.d.)

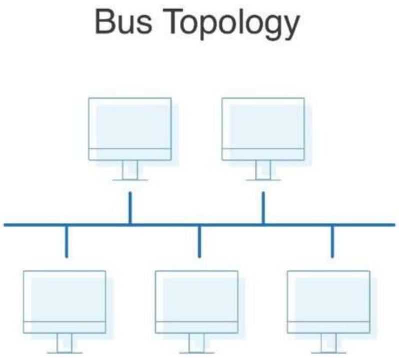
2. Star Topology

   The most common network topology, the star topology, is configured such that each node in the network is connected directly to a control center via coaxial cable, twisted pair, or optical fiber. As a server, this central node manages the transfer of data (information sent from each node in the network must pass through the central node to reach its destination). It works like a repeater and prevents data loss.



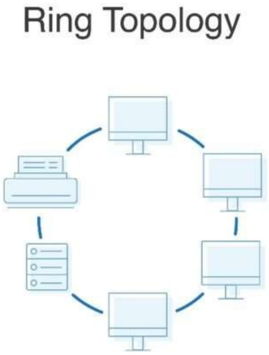
3. Bus Topology

   A bus topology routes all devices on a network through a single cable that extends from one side of the network to the other. This is why it is sometimes called "line topology" or "base topology". The data stream on the network also travels in one direction along the cable path.



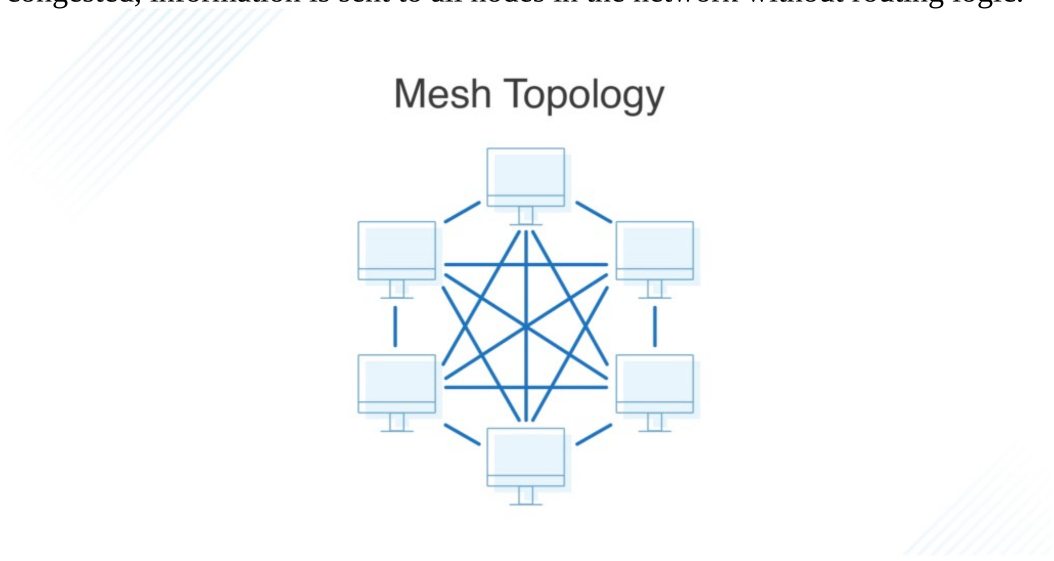
4. Ring Topology

   In a loop topology, nodes are arranged in a circle (or loop). A data loop can travel in one or both directions within a network, with each device having a neighbor.



5. Mesh Topology
   A network topology is a complex structure of point-to-point connections in which nodes are interconnected. Mesh networks can be fully or partially meshed. Partial retinal structures are often interconnected and some nodes have only two or three connections, but complete retinal structures stand out. - It is firmly attached. A network architecture, such as a network topology, provides two methods for transmitting data. Routing and unloading. When data is routed, nodes use logic to determine the minimum distance between source and destination, and when data is

congested, information is sent to all nodes in the network without routing logic.



My choice was ring star topology because of Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it’s easy to identify where errors or performance issues are occurring. Each device is only connected to both devices, so when data is transmitted, packets also travel along the line, passing through each intermediate node to reach their destination. If a large network is configured in a ring topology, you can use repeaters to ensure that packets arrive correctly without data loss. Because only one station can send data at a time, the risk of packet collisions is greatly reduced, creating a ring topology that sends data without errors. Ring structures are generally inexpensive and inexpensive to install, and the complex point-to-point connections of nodes make it relatively easy to identify problems and configurations in the network.

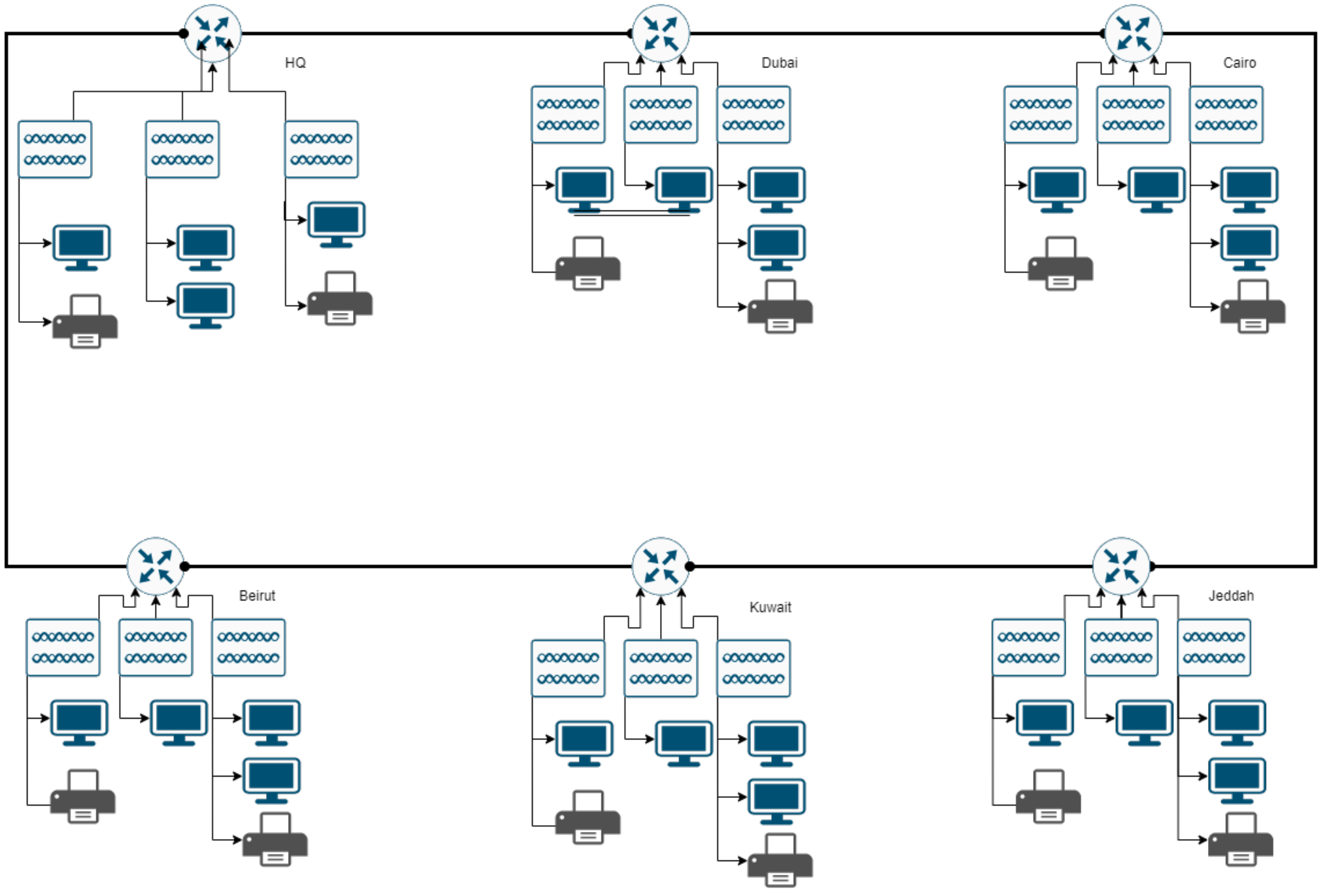
inter-dependencies of workstation hardware with relevant networking software

Diskless workstations have their own operating system on the server. To use a network component such as a printer on a workstation, the server must be connected to that network component. That is, the server must be connected to any workstation that does not have a hard drive. This can cause traffic jams and increase traffic volume. Diskless workstations have their own operating system on the server. If your workstation uses a network component such as a printer, you must connect the server to that network component. This means that the server must be connected to any workstation that does not have a hard drive. This can cause traffic jams and increase traffic volume. Also, every computer on the network uses a server: hard drives, processors, and memory. The workstation (client) hardware must wait for the server hardware to provide the requested information. Using workstations on a network without a network hard drive/computer greatly improves the connectivity between the workstation hardware. Therefore, it is very important to install reliable hardware and software components on the server and implement security and redundancy technology on the server.

Blueprint

the design I came up with is made for Institute of Technology, and it should be able to cover every thing they need and requirements.

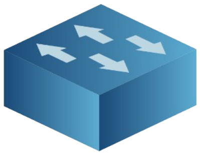
The unified network design was successful because it met all user needs with minimal cost and superior performance, and everything was tested to maintain the network integrity that users demanded.



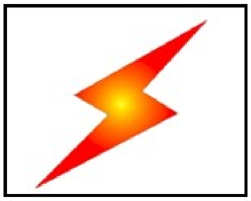
Devices Used

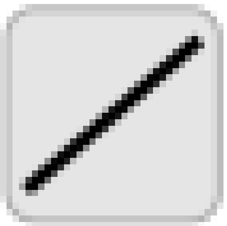
1. Router: Router: Many configurations are available to view routes to other networks and to connect to other networks for WAN use. This is the 1941 type I use for my grill.

2. switches: Switch: There are many different types of LANs that connect devices on the network, but the network uses the 2960-24TT.



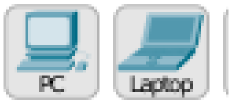
3. Cables: connect everything. The computer and the switch are connected by a straight copper cable. The router is connected with a DTE serial cable.





4. server: Server: Provides the necessary services for the network. I am using virtual servers for DHCP, HTTP, DNS, FTP and mail services.

5. Normal devices : pc, printers, smart devices laptops



Server:
For business servers, all protocols are used by installing a master server in the head office. Because what one server can do, it's cheaper and lower performance to set up with two or three servers. However, although we have shown how to improve the point of the relationship, the network retains only one strength. Here you can see the server IP address of the image and all the details. The servers

are located in the headquarters and control all other offices around the world. This server includes many services.

Testing

The test was successful as shown in the results down below this design needs 1 server at minimum each user requires a PC/ laptop to connect to the server its a big network so you will need a lot of switches and some routers the design is the best friend for money, I tried to be as efficient as possible with taking in to consideration cost each user will cost other than the computer it self is around 30 jds a year, each user have 1000Mbps in his hands that are more than enough.

Test	Testing	Result
DHCP	IP Configuration	Successful
Connection	Ping	Successful
FTP/Mail	FTP Commands / Email	Successful
HTTP/DNS	Web Browsing	Successful

Elements of a Security Plan

Physical security: all data is place in the Headquarter building plus there are few security guard around it, with video feed.

Network security: on each computer there is a firewall plus each user need an username and a pass word, transferring anything also requires a password there are no wireless points what so ever connected to the same network as the server.

application data security: each application the user uses has it own security while communicating with the server, the only way the outsider can under stand it is through being physically in front of a computer in side the company with password for a computer plus the application username and password.

For future upgrade

you should make more than one server room around the glob and make the server room to server building , increase human security plus take a private network line from IPS.

Maintenance:

Because we need to keep the network running to monitor for incidents such as security breaches and bugs, we have a maintenance plan in place.

Devices	Time
Servers	Once a week 00:00
Router	5 days 06:00
Switches	5 days 06:00

PCs/Printers	2 days 10:00

Network future upgrades:

The first step in improving your network is to install multiple servers to protect them and download the primary server. Cables are expensive to use, so I want to connect to a wireless network as well. You can easily get more devices with better subnets, security for used devices and FTP users, and email and printers for people living in the same room. I would like to set up a firewall that is more advanced to protect my network from external attacks and malware that could cause this network to crash.

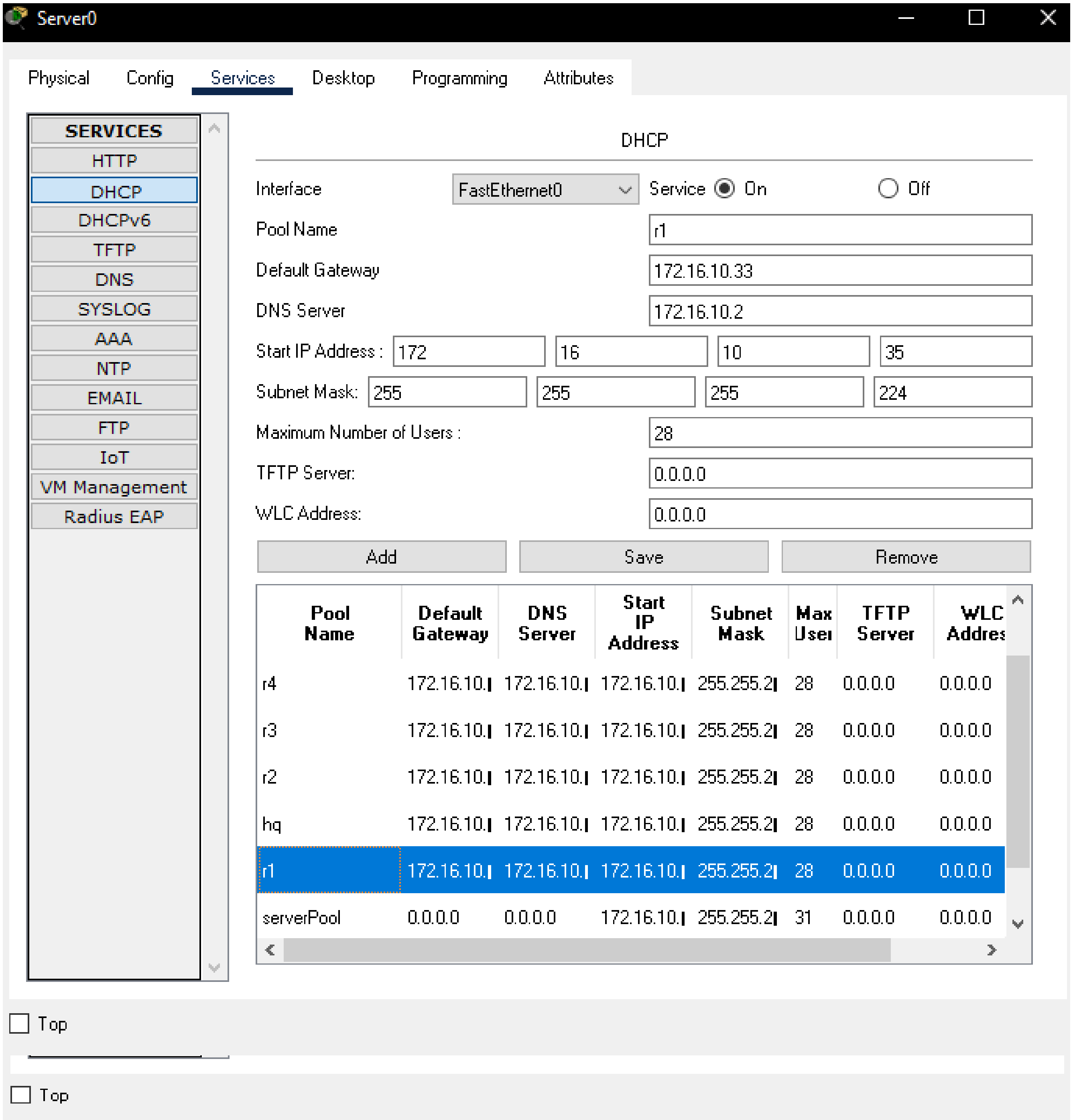
Growth support:
the network that I built is growth capability because:

1. it was built in consideration of cost which means there is a huge place for upgrades
2. the performance can be increased by upgrading the routers and switches
3. fiber optic wires can be used instead of copper based wires
4. systems can be upgrades and it also includes security
5. making backups for any risk of having the server to go down
6. adding vpn to enable secure connection from the employee’s house if required

network configurations

HQ

Dubai



DHCP

Interface: FastEthernet0 Service ● On ○ Off

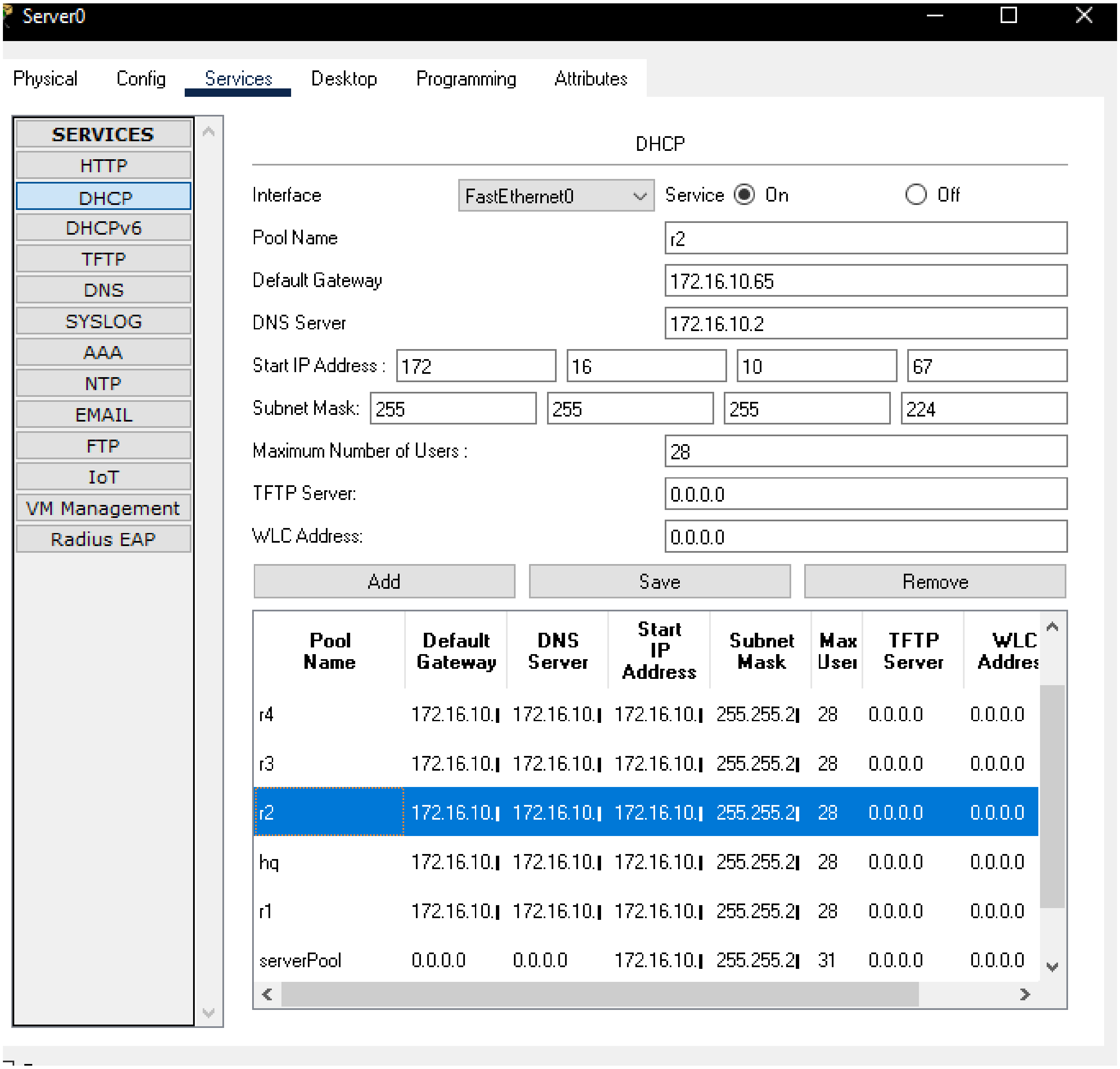
Pool Name	r1
Default Gateway	172.16.10.33
DNS Server	172.16.10.2
Start IP Address :	172 . 16 . 10 . 35
Subnet Mask:	255 . 255 . 255 . 224
Maximum Number of Users :	28
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Usei	TFTP Server	WLC Addres
r4	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r3	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r2	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
hq	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r1	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.10.	255.255.2	31	0.0.0.0	0.0.0.0

☐ Top

☐ Top

Cairo



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: r2

Default Gateway: 172.16.10.65

DNS Server: 172.16.10.2

Start IP Address : 172 . 16 . 10 . 67

Subnet Mask: 255 . 255 . 255 . 224

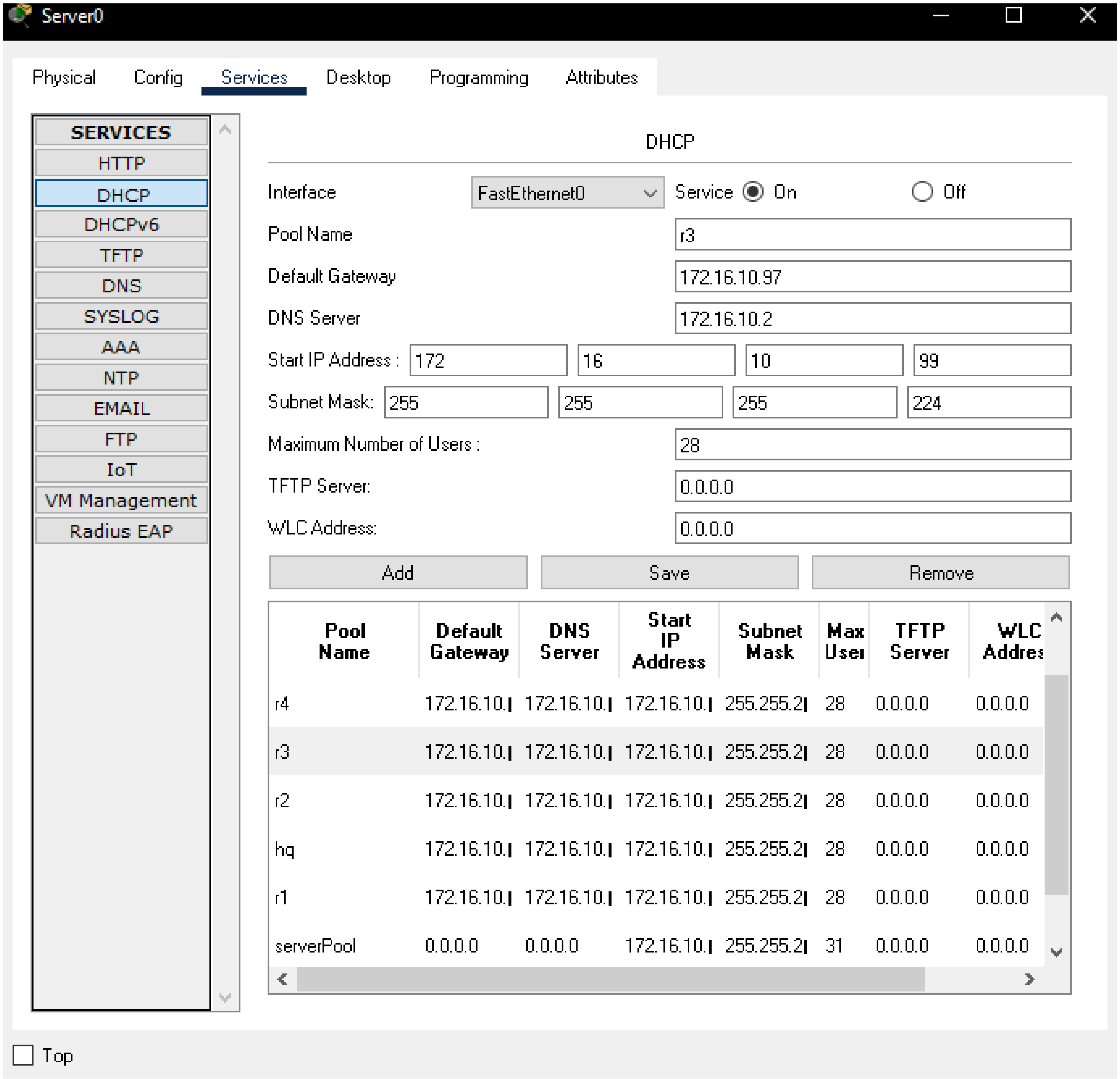
Maximum Number of Users : 28

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Addres
r4	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r3	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r2	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
hq	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r1	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.10.	255.255.2	31	0.0.0.0	0.0.0.0

Beirut

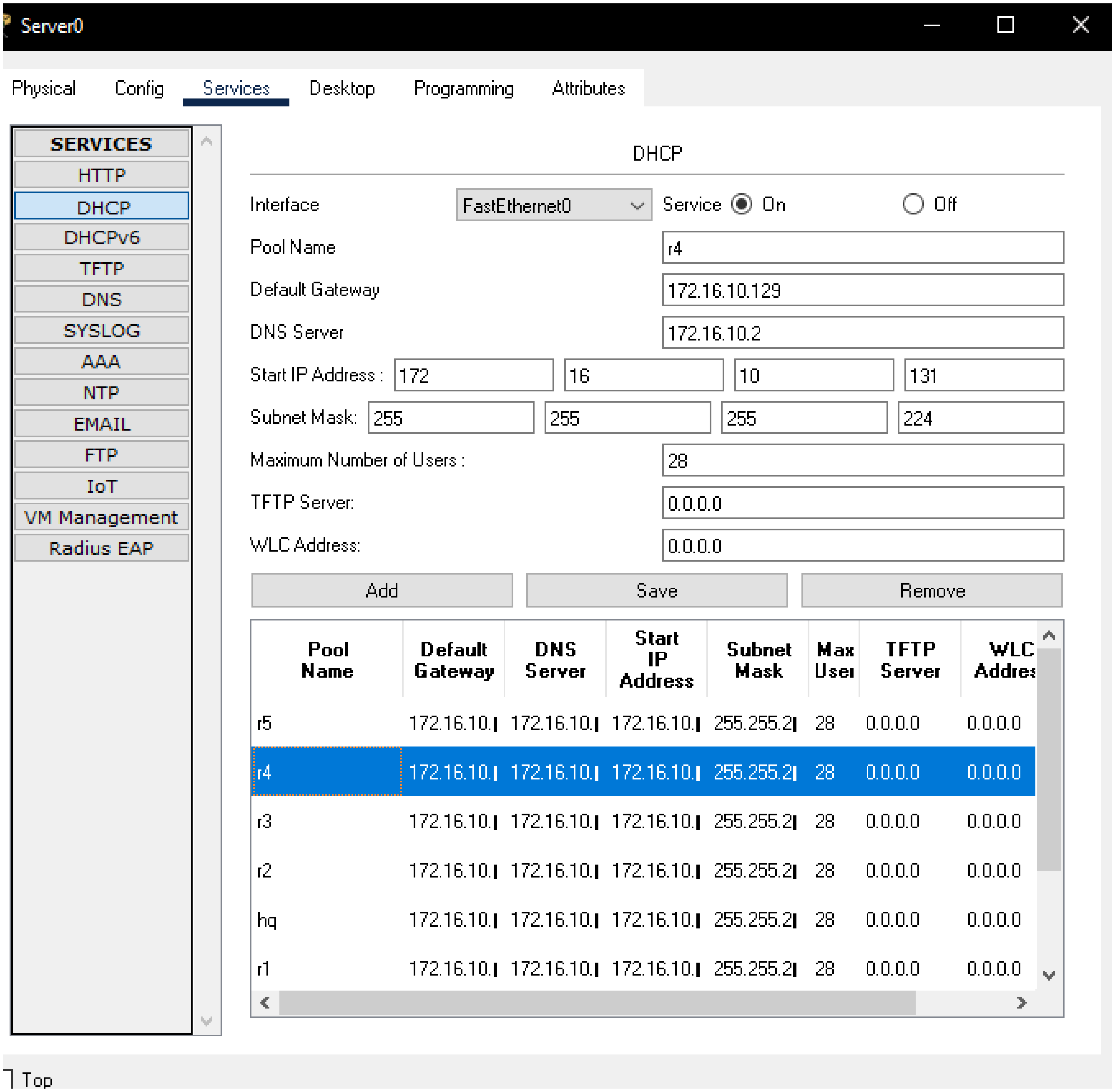


DHCP

Interface	FastEthernet0
Service	● On ○ Off
Pool Name	r3
Default Gateway	172.16.10.97
DNS Server	172.16.10.2
Start IP Address :	172 . 16 . 10 . 99
Subnet Mask:	255 . 255 . 255 . 224
Maximum Number of Users :	28
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Usei	TFTP Server	WLC Addres
r4	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r3	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r2	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
hq	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
r1	172.16.10.	172.16.10.	172.16.10.	255.255.2	28	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.10.	255.255.2	31	0.0.0.0	0.0.0.0

kuwait



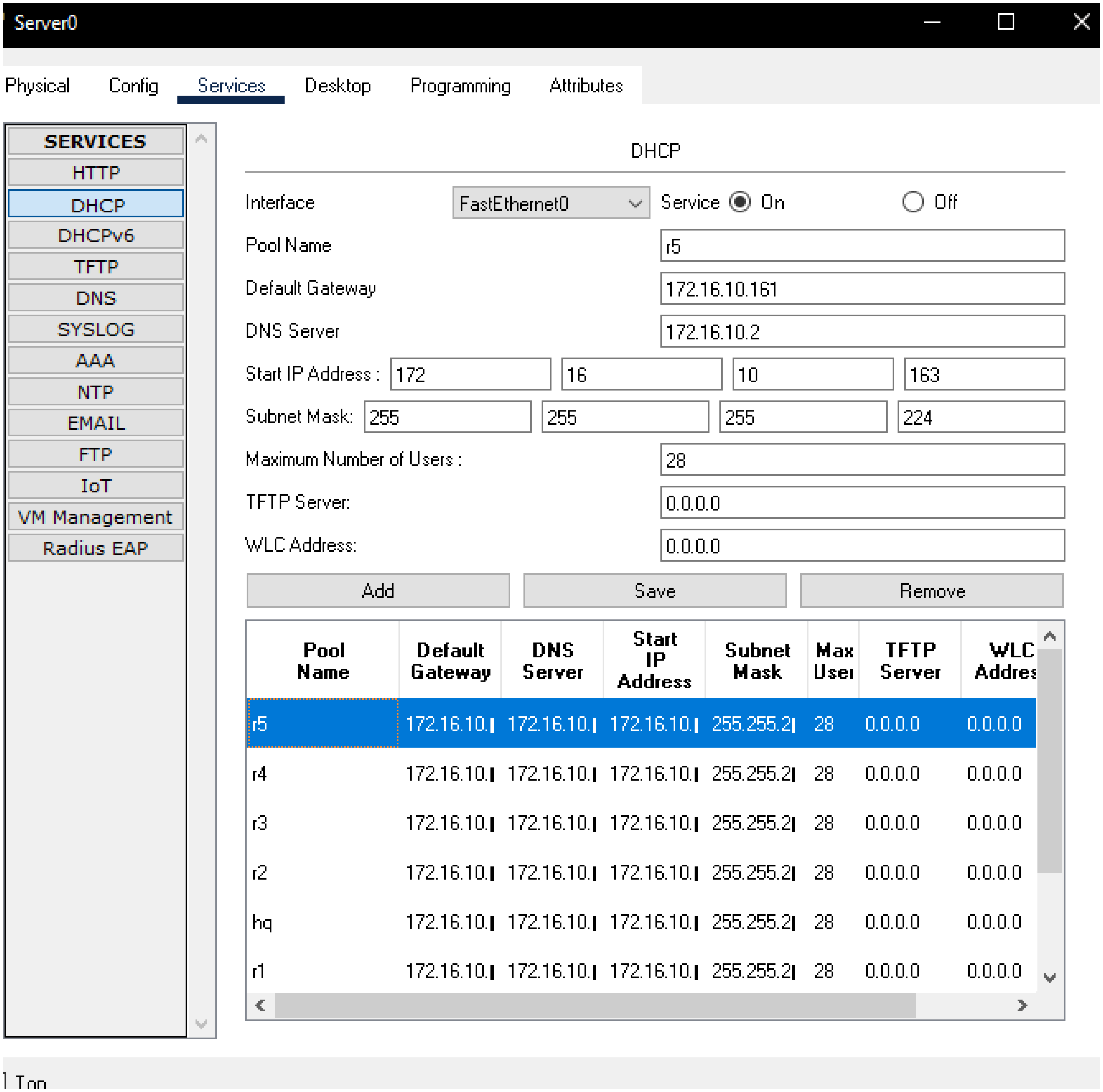
DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name	r4
Default Gateway	172.16.10.129
DNS Server	172.16.10.2
Start IP Address :	172 . 16 . 10 . 131
Subnet Mask:	255 . 255 . 255 . 224
Maximum Number of Users :	28
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Addres
r5	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r4	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r3	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r2	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
hq	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r1	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0

jeddah



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name r5

Default Gateway 172.16.10.161

DNS Server 172.16.10.2

Start IP Address : 172 16 10 163

Subnet Mask: 255 255 255 224

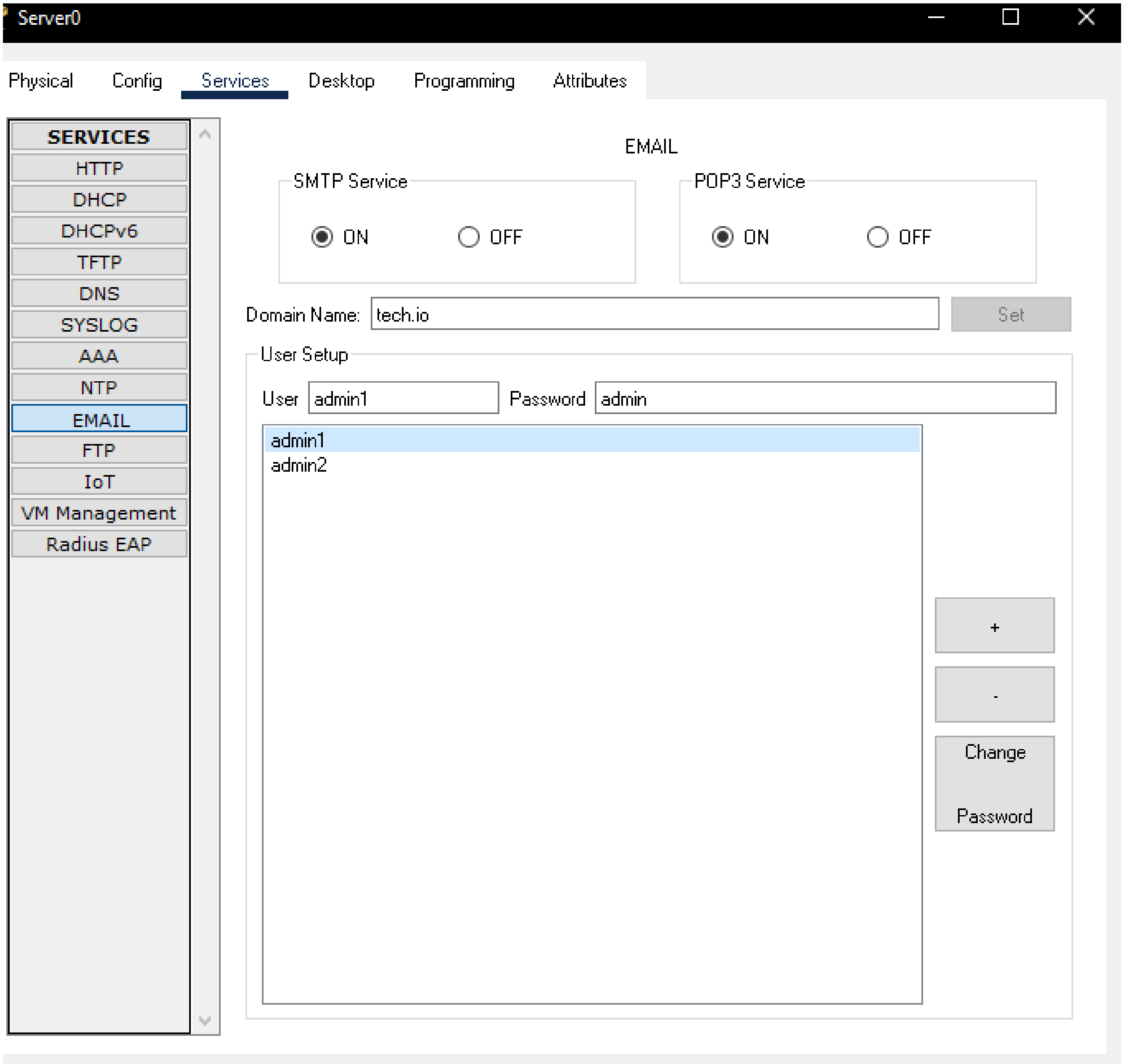
Maximum Number of Users : 28

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Usei	TFTP Server	WLC Addres
r5	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r4	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r3	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r2	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
hq	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0
r1	172.16.10.|	172.16.10.|	172.16.10.|	255.255.2|	28	0.0.0.0	0.0.0.0

mail configurations



EMAIL

SMTP Service
● ON ○ OFF

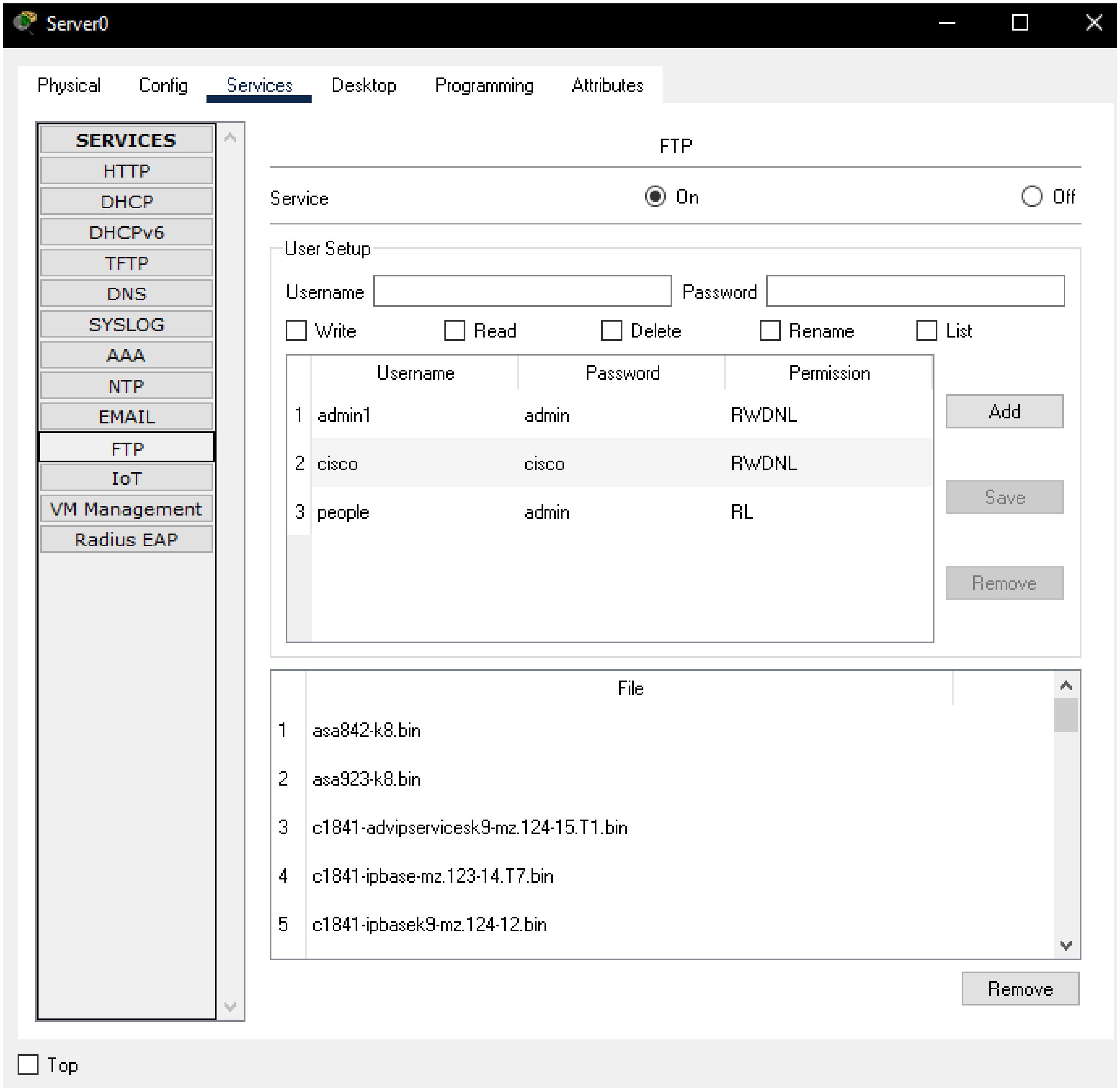
POP3 Service
● ON ○ OFF

Domain Name: tech.io

User admin1 Password admin

admin1
admin2

FTP configurations



FTP

Service ● On ○ Off

User Setup

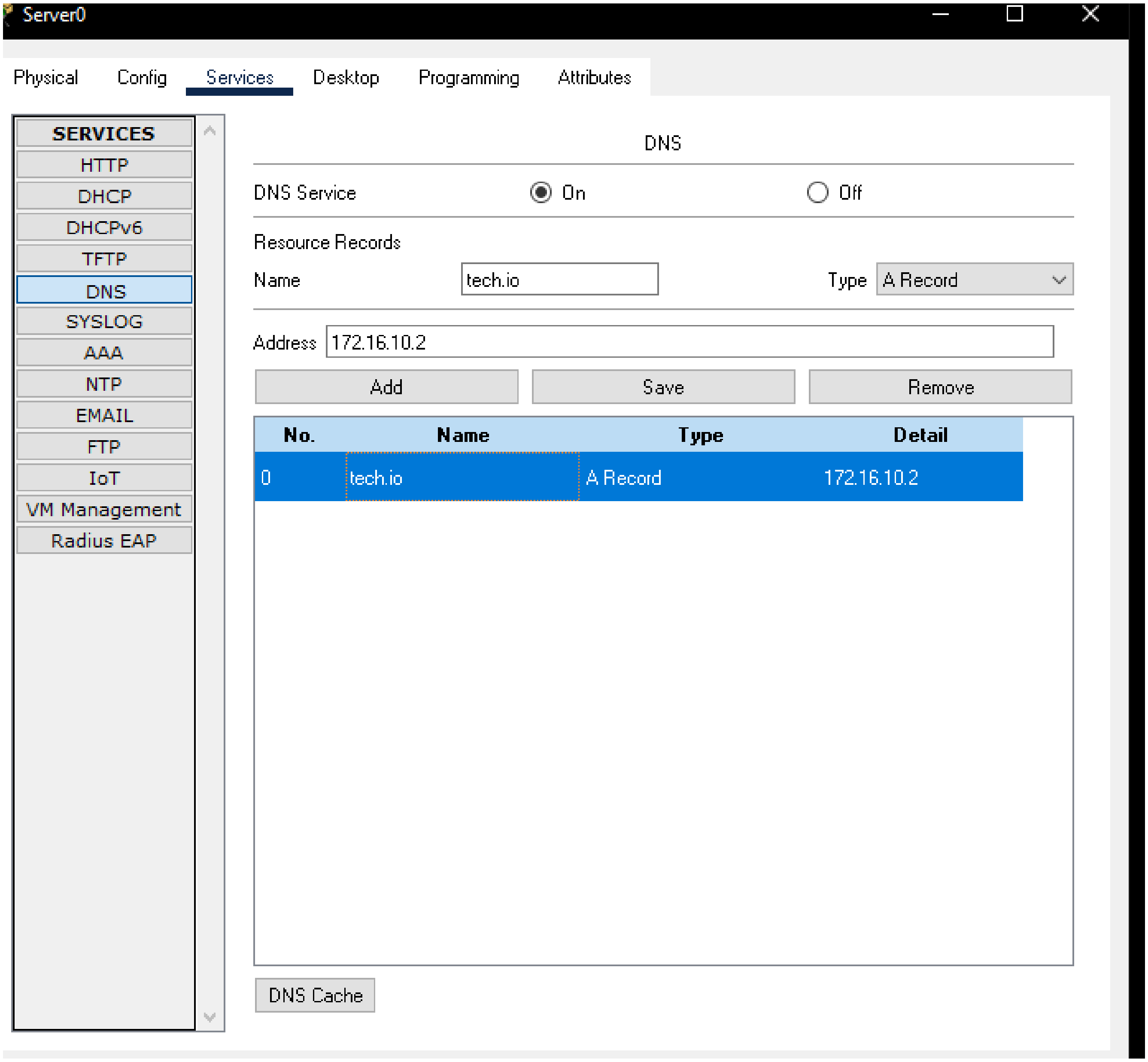
Username
Password

□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	admin1	admin	RWDNL
2	cisco	cisco	RWDNL
3	people	admin	RL

	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin

DNS configurations



DNS

DNS Service ● On ○ Off

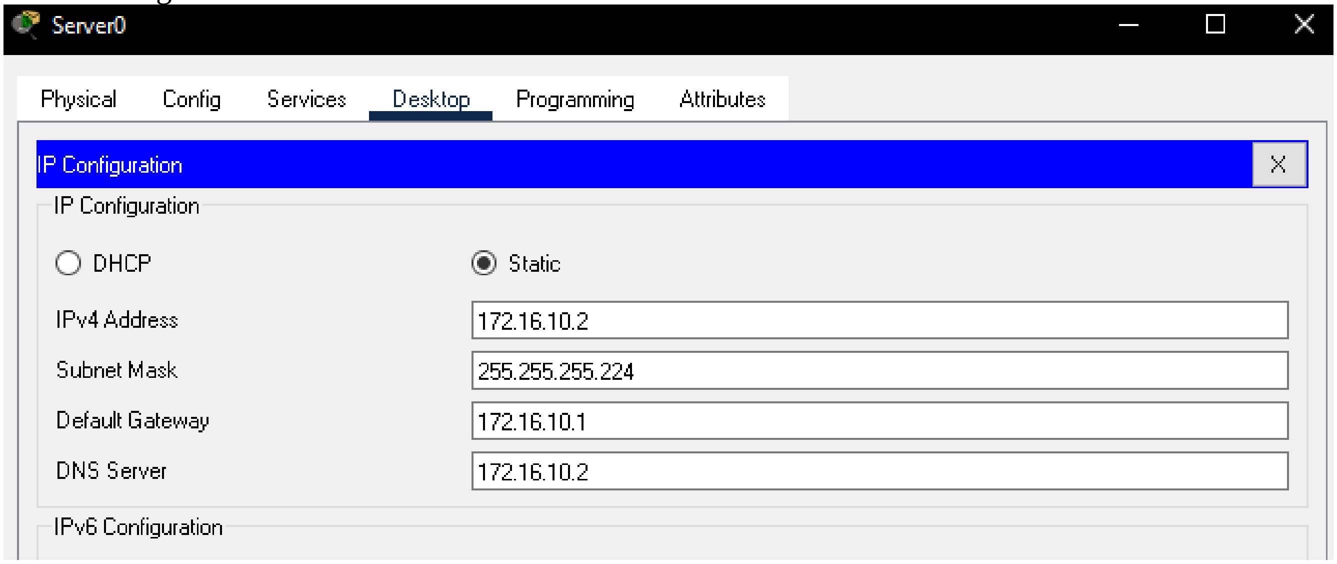
Resource Records

Name tech.io Type A Record

Address 172.16.10.2

No.	Name	Type	Detail
0	tech.io	A Record	172.16.10.2

server configurations



IP Configuration

○ DHCP ● Static

IPv4 Address 172.16.10.2

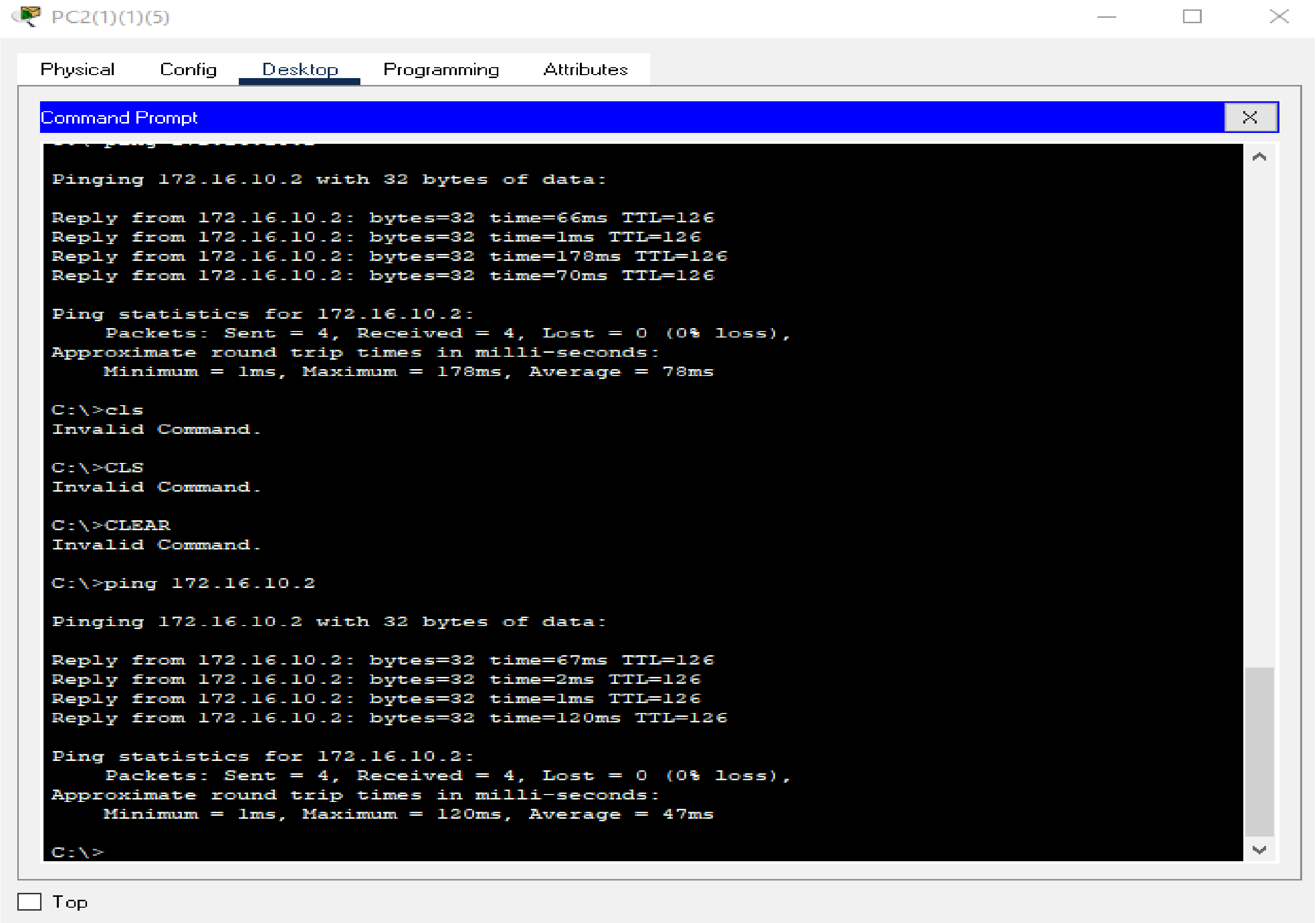
Subnet Mask 255.255.255.224

Default Gateway 172.16.10.1

DNS Server 172.16.10.2

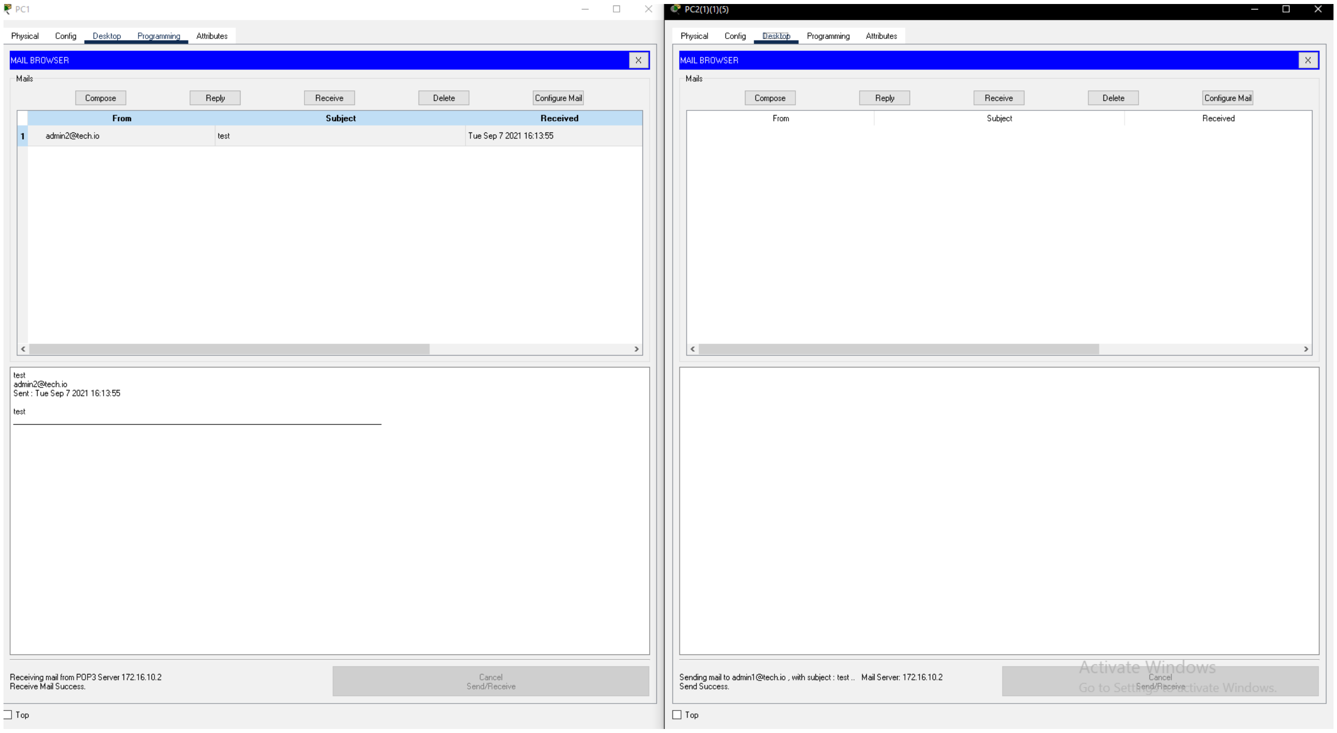
IPv6 Configuration

ping



```
Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time=66ms TTL=126
Reply from 172.16.10.2: bytes=32 time=1ms TTL=126
Reply from 172.16.10.2: bytes=32 time=178ms TTL=126
Reply from 172.16.10.2: bytes=32 time=70ms TTL=126

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 178ms, Average = 78ms

C:\>cls
Invalid Command.

C:\>CLS
Invalid Command.

C:\>CLEAR
Invalid Command.

C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time=67ms TTL=126
Reply from 172.16.10.2: bytes=32 time=2ms TTL=126
Reply from 172.16.10.2: bytes=32 time=1ms TTL=126
Reply from 172.16.10.2: bytes=32 time=120ms TTL=126

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 120ms, Average = 47ms

C:\>
```

email test



PC1:

	From	Subject	Received
1	admin2@tech.io	test	Tue Sep 7 2021 16:13:55

test
admin2@tech.io
Sent : Tue Sep 7 2021 16:13:55

test

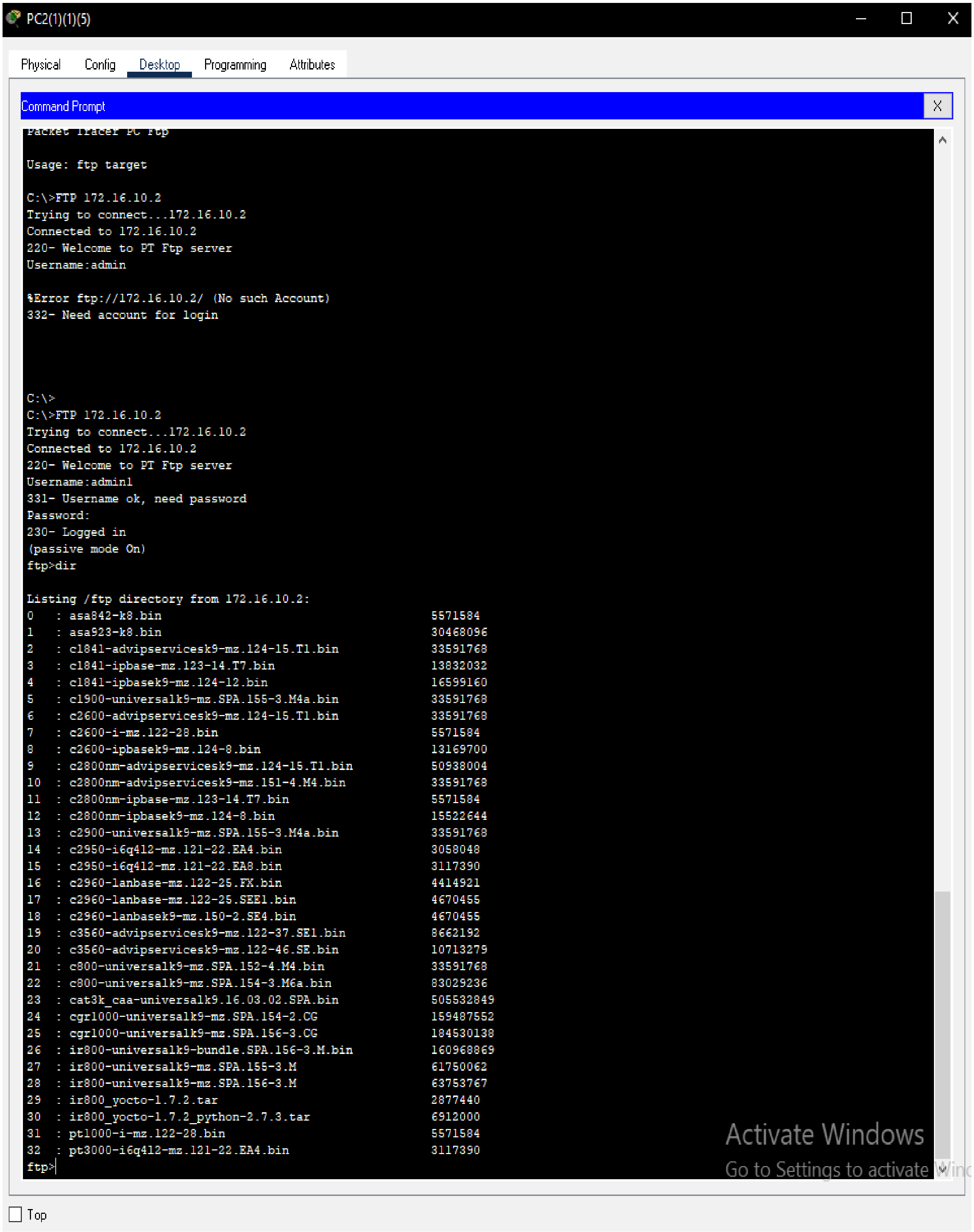
Receiving mail from POP3 Server 172.16.10.2
Receive Mail Success.

PC2(1)(1)(5):

From	Subject	Received

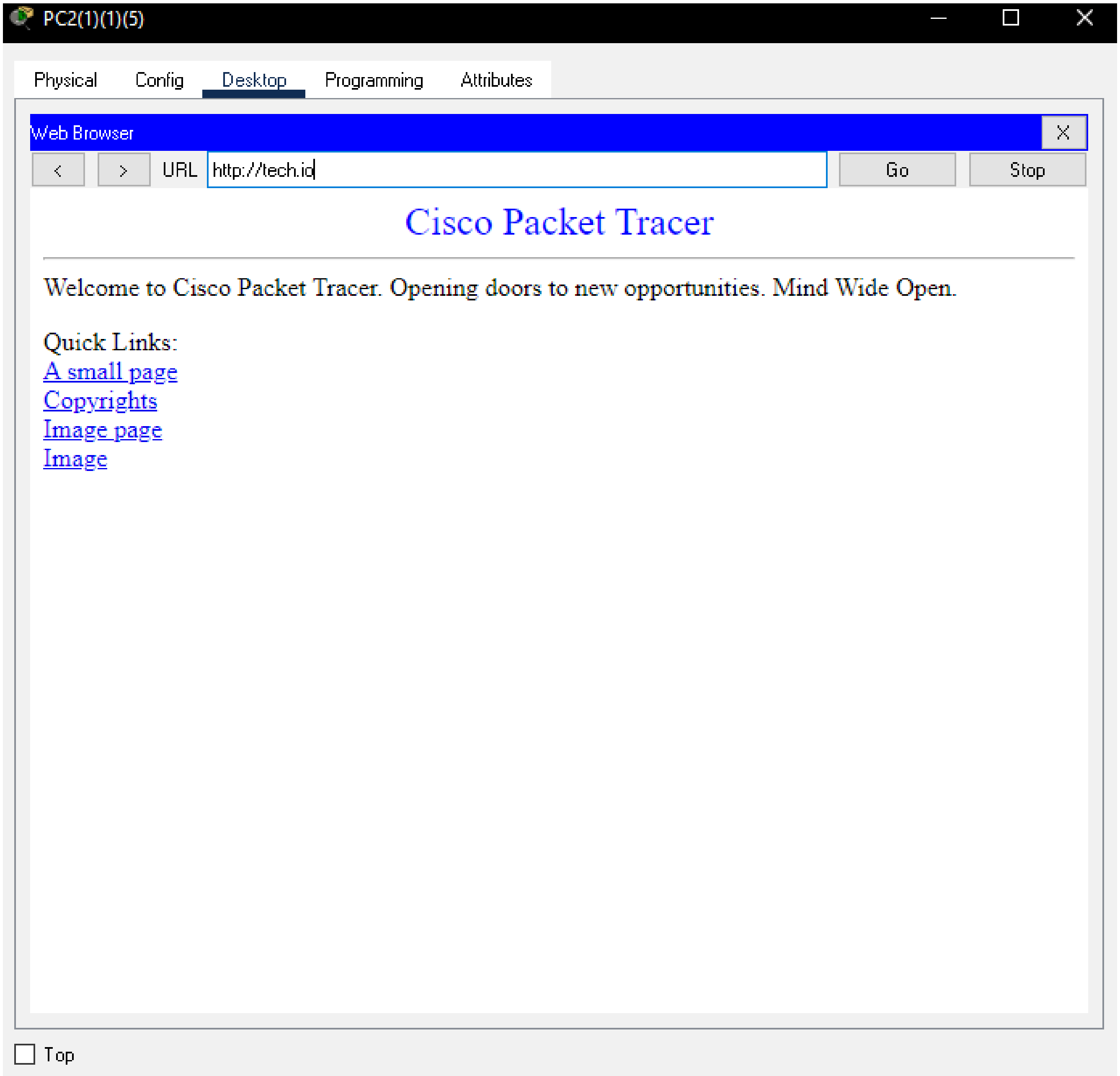
Sending mail to admin1@tech.io , with subject : test .. Mail Server: 172.16.10.2
Send Success.

FTP test



```
Packet Tracer PC Ftp

Usage: ftp target

C:\>FTP 172.16.10.2
Trying to connect...172.16.10.2
Connected to 172.16.10.2
220- Welcome to PT Ftp server
Username:admin

%Error ftp://172.16.10.2/ (No such Account)
332- Need account for login




C:\>
C:\>FTP 172.16.10.2
Trying to connect...172.16.10.2
Connected to 172.16.10.2
220- Welcome to PT Ftp server
Username:admin1
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 172.16.10.2:
0   : asa842-k8.bin                                      5571584
1   : asa923-k8.bin                                      30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin             33591768
3   : c1841-ipbase-mz.123-14.T7.bin                      13832032
4   : c1841-ipbasek9-mz.124-12.bin                       16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin             33591768
6   : c2600-advipservicesk9-mz.124-15.T1.bin             33591768
7   : c2600-i-mz.122-28.bin                              5571584
8   : c2600-ipbasek9-mz.124-8.bin                        13169700
9   : c2800nm-advipservicesk9-mz.124-15.T1.bin           50938004
10  : c2800nm-advipservicesk9-mz.151-4.M4.bin            33591768
11  : c2800nm-ipbase-mz.123-14.T7.bin                    5571584
12  : c2800nm-ipbasek9-mz.124-8.bin                      15522644
13  : c2900-universalk9-mz.SPA.155-3.M4a.bin             33591768
14  : c2950-i6q4l2-mz.121-22.EA4.bin                     3058048
15  : c2950-i6q4l2-mz.121-22.EA8.bin                     3117390
16  : c2960-lanbase-mz.122-25.FX.bin                     4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin                   4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin                   4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin            8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin             10713279
21  : c800-universalk9-mz.SPA.152-4.M4.bin               33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin              83029236
23  : cat3k_caa-universalk9.16.03.02.SPA.bin             505532849
24  : cgr1000-universalk9-mz.SPA.154-2.CG                159487552
25  : cgr1000-universalk9-mz.SPA.156-3.CG                184530138
26  : ir800-universalk9-bundle.SPA.156-3.M.bin           160968869
27  : ir800-universalk9-mz.SPA.155-3.M                   61750062
28  : ir800-universalk9-mz.SPA.156-3.M                   63753767
29  : ir800_yocto-1.7.2.tar                              2877440
30  : ir800_yocto-1.7.2_python-2.7.3.tar                 6912000
31  : pt1000-i-mz.122-28.bin                             5571584
32  : pt3000-i6q4l2-mz.121-22.EA4.bin                    3117390
ftp>
```

web site test



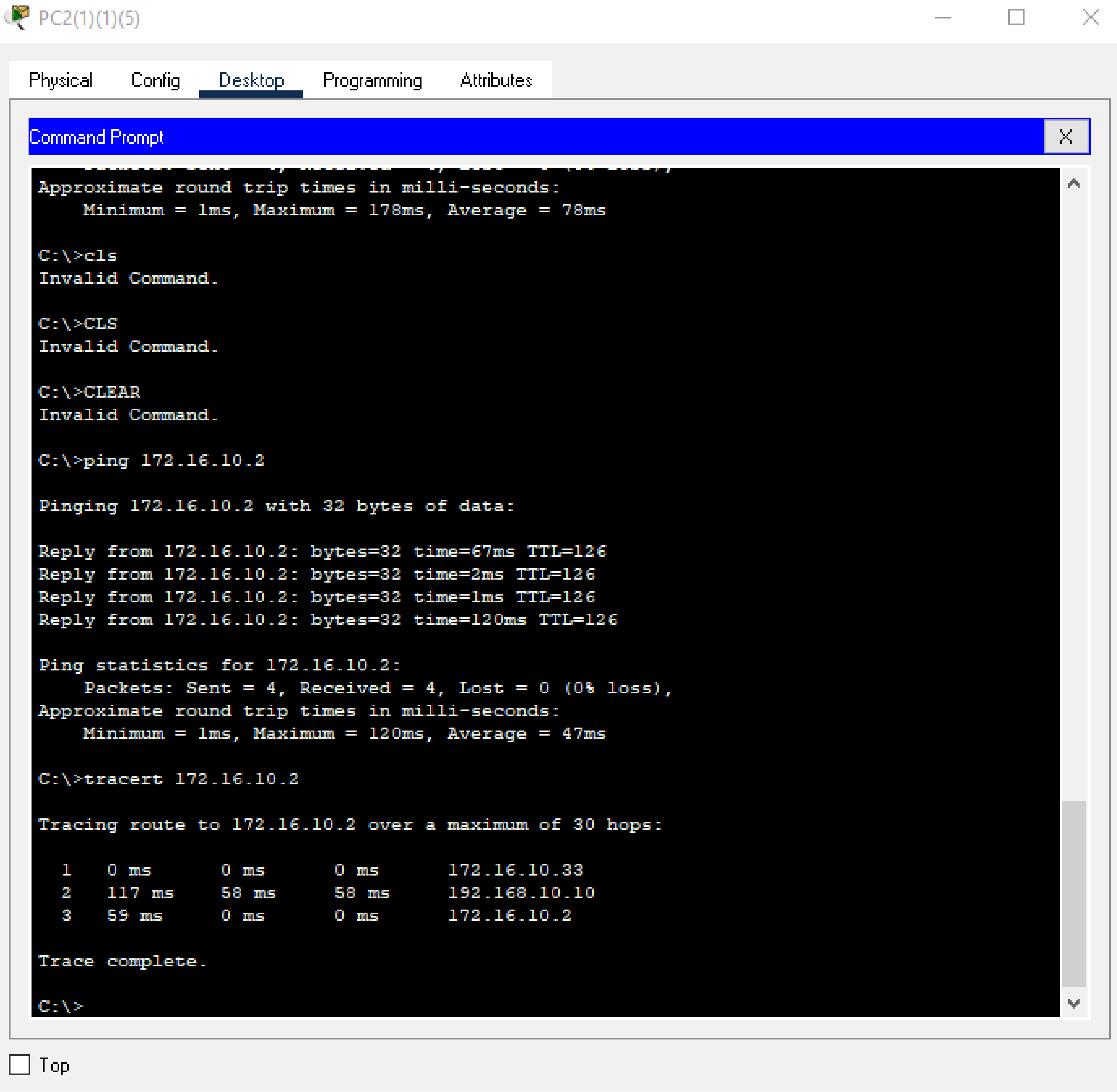
URL http://tech.io

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

trace route test



```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 178ms, Average = 78ms

C:\>cls
Invalid Command.

C:\>CLS
Invalid Command.

C:\>CLEAR
Invalid Command.

C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time=67ms TTL=126
Reply from 172.16.10.2: bytes=32 time=2ms TTL=126
Reply from 172.16.10.2: bytes=32 time=1ms TTL=126
Reply from 172.16.10.2: bytes=32 time=120ms TTL=126

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 120ms, Average = 47ms

C:\>tracert 172.16.10.2

Tracing route to 172.16.10.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      172.16.10.33
  2   117 ms    58 ms     58 ms     192.168.10.10
  3   59 ms     0 ms      0 ms      172.16.10.2

Trace complete.

C:\>
```

□ Top

references

Anonym (2015). *Network Server Types Explained*. [online] Pittsburgh. Available at: https://www.nhpittsburgh.com/solutions/resources/upcoming-events-and-webinars/network-server-types-explained.

beta.computer-networking.info. (n.d.). *Computer Networking : Principles, Protocols and Practice, third edition — Computer Networking : Principles, Protocols and Practice*. [online] Available at: https://beta.computer-networking.info/syllabus/default/index.html.

Bourgeois, S. (2016). *Network-types*. [online] belden.com. Available at: https://www.belden.com/blogs/network-types.

Cabinet Office (2016). *Network principles*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/network-principles/network-principles.

Circuit by Unify. (n.d.). *Support FAQs: Circuit by Unify.* [online] Available at: https://www.circuit.com/unifyportalfaqdetail?articleId=36901.

Cisco. (2019). *Using the Extended ping and Extended traceroute Commands*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html.

communications@manageengine.com, M. (n.d.). *Network Monitoring Software by ManageEngine OpManager*. [online] ManageEngine OpManager. Available at: https://www.manageengine.com.au/network-monitoring/network-protocols.html.

ComputerNetworkingNotes (2018). *Network Cable Types and Specifications*. [online] ComputerNetworkingNotes. Available at: https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html.

Contributor, S. (2019). *What is network topology? Best guide to types & diagrams - dnsstuff*. [online] DNSstuff. Available at: https://www.dnsstuff.com/what-is-network-topology.

Default. (2019). *Network Protocol Definition | Computer Protocol | CompTIA*. [online] Available at: https://www.comptia.org/content/guides/what-is-a-network-protocol.

docs.cxengage.net. (n.d.). *Bandwidth Availability and Requirements*. [online] Available at: https://docs.cxengage.net/Help/Content/Configuration/SystemRequirements/Bandwidth_availability_requirements.htm [Accessed 8 Sep. 2021].

docs.oracle.com. (n.d.). *Quality of Service Requirements (Sun Java Enterprise System Deployment Planning Guide)*. [online] Available at: https://docs.oracle.com/cd/E19636-01/819-2326/gaxqg/index.html.

Indeed Career Guide. (n.d.). *Types of Computer Servers and How They Function*. [online] Available at: https://www.indeed.com/career-advice/career-development/types-of-servers.

Information Technology at Sonoma State University. (2018). *Workstation Hardware & Software*. [online] Available at: https://it.sonoma.edu/kb/computers-software-devices/workstation-hardware-software.

Melnick, J. (2019). *Network Devices Explained*. [online] Netwrix.com. Available at: https://blog.netwrix.com/2019/01/08/network-devices-explained/.

Networks Training. (2020). *8 Different Types of Servers in Computer Networks*. [online] Available at: https://www.networkstraining.com/different-types-of-servers/.

Sciencedirect.com. (2009). *Bandwidth Requirement - an overview | ScienceDirect Topics*. [online] Available at: https://www.sciencedirect.com/topics/computer-science/bandwidth-requirement.

Siegler, M. (2018). *4 Types of Bandwidth: Advantages and Disadvantages - Ecessa*. [online] Ecessa. Available at: https://www.ecessa.com/blog/4-types-of-bandwidth-advantages-and-disadvantages/.

Warren, P. (2005). *Ten steps to secure networking*. [online] Computerworld. Available at: https://www.computerworld.com/article/2559866/ten-steps-to-secure-networking.html.

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

Student name: ABDELKAREEM YOUSEF MAMDOH SOUBAR 19110022		**Assessor name:** Dr. Huthaifa Al-Omari
Issue date: 18/08/2021	**Submission date:** 8/09/2021	**Submitted on: 8/09/2021**
Programme: Computing		
HTU Course Name: Networking **HTU Course Code:** 30201110	**BTEC Course name:** Networking **BTEC Course Code:** H/615/1619	
Assignment number and title: Assignment 1 [Computer Network of Institute of Technology]		

Plagiarism

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

Student declaration
I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student signature: *abdelkareem soubar* **Date: 8/09/2021**