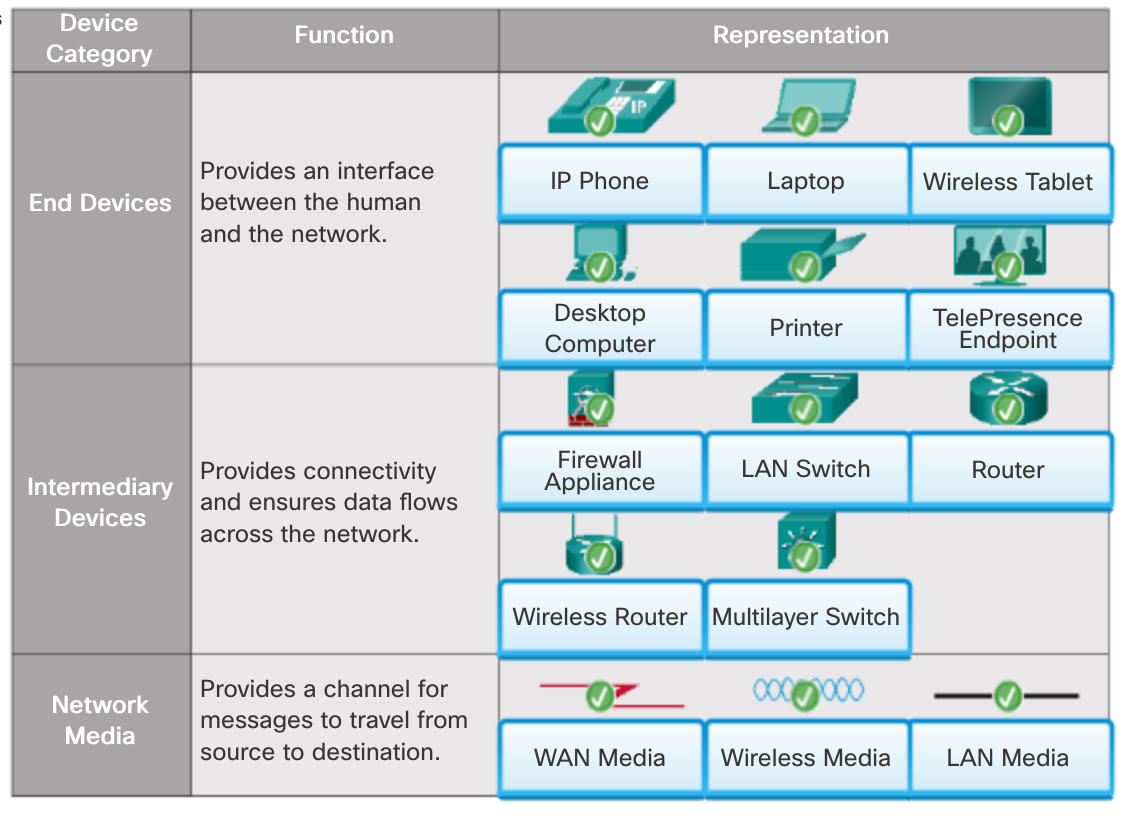
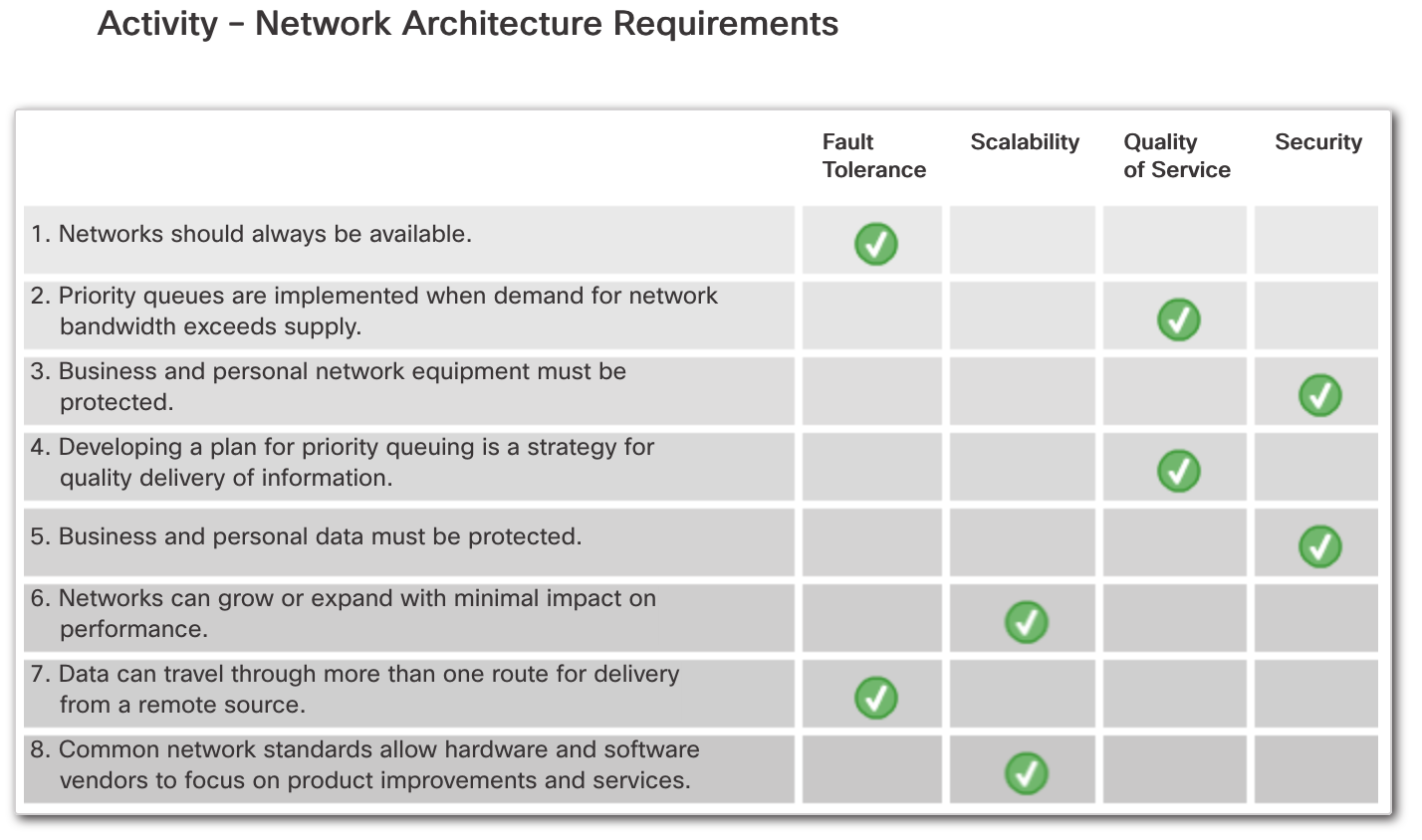
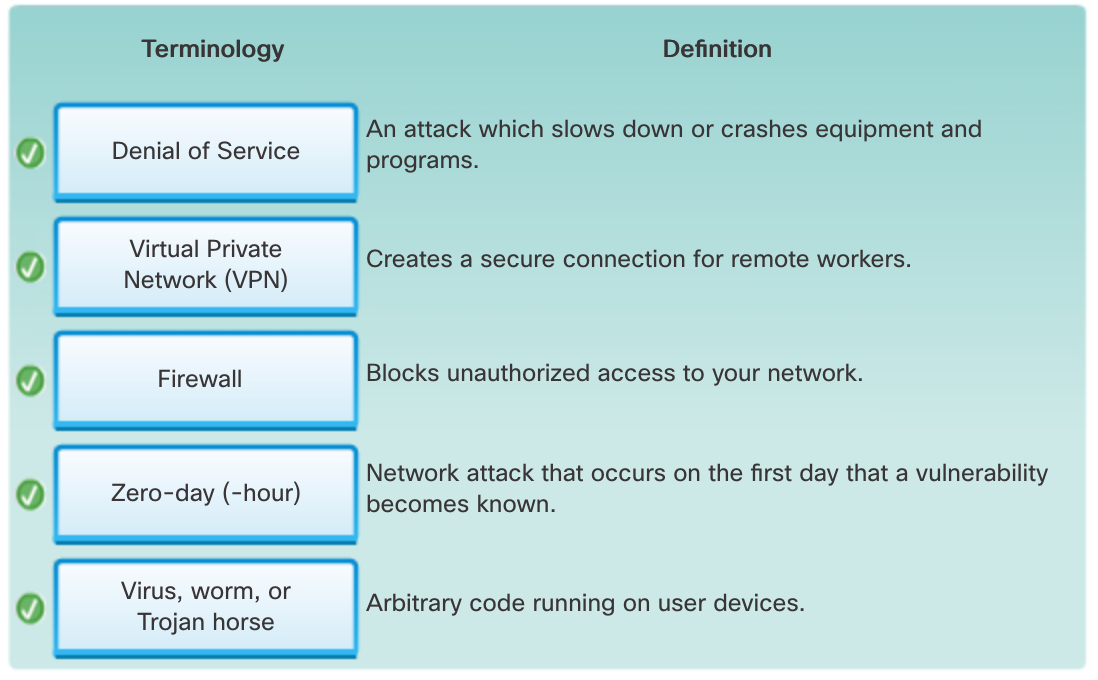
**Introduction to Networks**

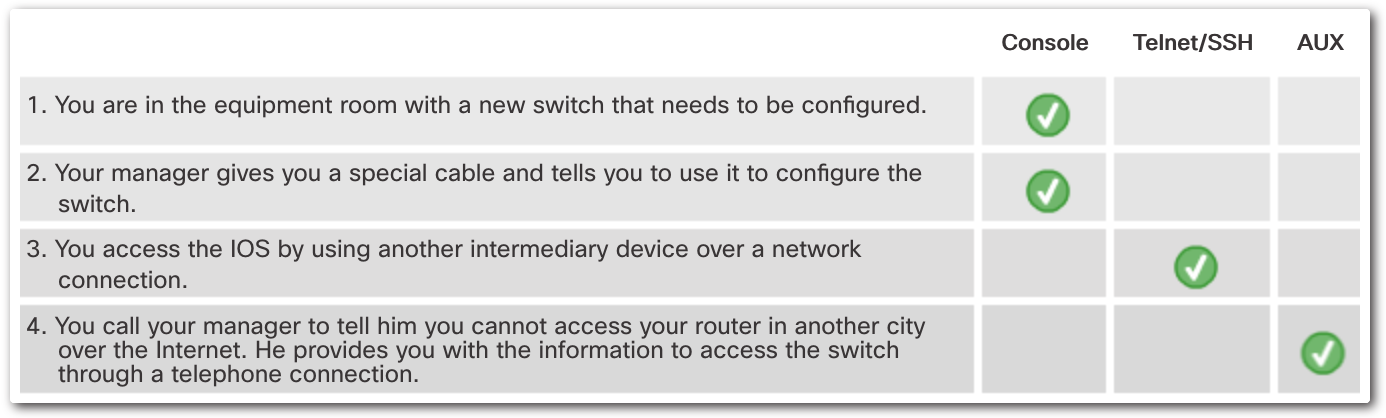


|  |  |  |
| --- | --- | --- |
| Local Area Networks  LANs are a network infrastructure that spans a small geographical area. Specific features of LANs include:  LANs interconnect end devices in a limited area such as a home, school, office building, or campus.  A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies are enforced on the network level.  LANs provide high speed bandwidth to internal end devices and intermediary devices.    Wide Area Networks  WANs are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SP) or Internet Service Providers (ISP).  Specific features of WANs include:  WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.  WANs are usually administered by multiple service providers.  WANs typically provide slower speed links between LANs. | | Types of Networks Network infrastructures can vary greatly in terms of:   * Size of the area covered * Number of users connected * Number and types of services available * Area of responsibility   The figure illustrates the two most common types of network infrastructures:   * **Local Area Network (LAN)** - A network infrastructure that provides access to users and end devices in a small geographical area, which is typically an enterprise, home, or small business network owned and managed by an individual or IT department. * **Wide Area Network (WAN)** - A network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a telecommunications service provider.   Other types of networks include:   * **Metropolitan Area Network (MAN)** - A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity such as a large organization. * **Wireless LAN** **(WLAN)** - Similar to a LAN but wirelessly interconnects users and end points in a small geographical area. * **Storage Area Network (SAN)** - A network infrastructure designed to support file servers and provide data storage, retrieval, and replication. |
|  | **Home and Small Office Internet Connections**  The figure illustrates common connection options for small office and home office users:  **Cable** - Typically offered by cable television service providers, the Internet data signal is carried on the same cable that delivers cable television. It provides a high bandwidth, always on, connection to the Internet.  **DSL** - Digital Subscriber Lines provide a high bandwidth, always on, connection to the Internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.  **Cellular** - Cellular Internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular Internet access. Performance will be limited by the capabilities of the phone and the cell tower to which it is connected.  **Satellite** - The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.  **Dial-up Telephone** - An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling.  Many homes and small offices are more commonly being connected directly with fiber optic cables. This enables an ISP to provide higher bandwidth speeds and support more services such as Internet, phone, and TV | |
|  | | Businesses Internet Connections Corporate connection options differ from home user options. Businesses may require higher bandwidth, dedicated bandwidth, and managed services. Connection options available differ depending on the type of service providers located nearby:  **Dedicated Leased Line** - Leased lines are actually reserved circuits within the service provider’s network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate. They can be expensive.  **Ethernet WAN** - Ethernet WANs extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later chapter. The benefits of Ethernet are now being extended into the WAN.  **DSL** - Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL) which is similar to the consumer version of DSL, but provides uploads and downloads at the same speeds.  **Satellite** - Similar to small office and home office users, satellite service can provide a connection when a wired solution is not available.  The choice of connection varies depending on geographical location and service provider availability. |

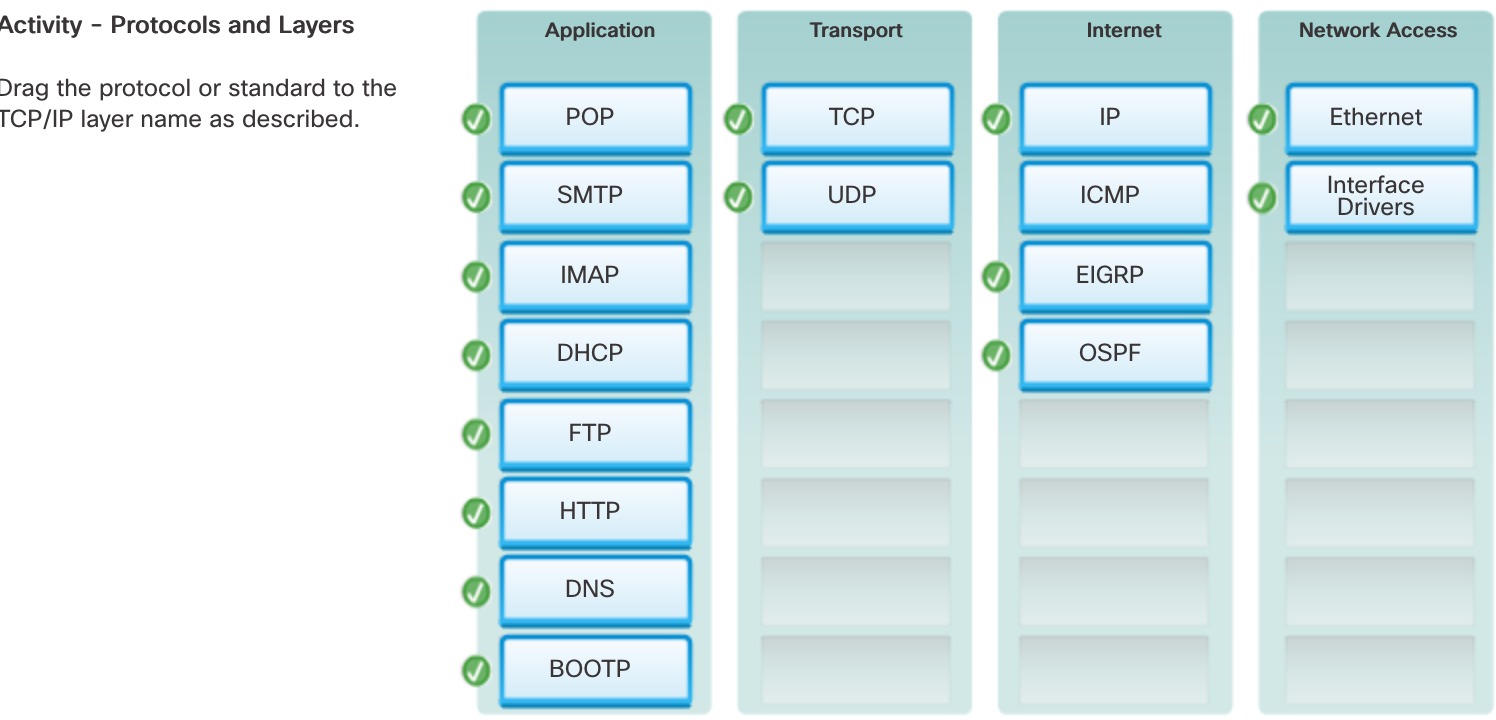


|  |  |
| --- | --- |
|  | **Security Threats**  The most common external threats to networks include:  **Viruses, worms, and Trojan horses** - malicious software and arbitrary code running on a user device  **Spyware and adware** - software installed on a user device that secretly collects information about the user  **Zero-day attacks, also called zero-hour attacks** - an attack that occurs on the first day that a vulnerability becomes known  **Hacker attacks** - an attack by a knowledgeable person to user devices or network resources  **Denial of service attacks** - attacks designed to slow or crash applications and processes on a network device  **Data interception and theft** - an attack to capture private information from an organization’s network  **Identity theft** - an attack to steal the login credentials of a user in order to access private data  It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats. |
| Security Solutions No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others still stand.  A home network security implementation is usually rather basic. It is generally implemented on the connecting end devices, as well as at the point of connection to the Internet, and can even rely on contracted services from the ISP.  In contrast, the network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security.  Network security components for a home or small office network should include, at a minimum:   * **Antivirus and antispyware** – These are used to protect end devices from becoming infected with malicious software. * **Firewall filtering** – This is used to block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.   In addition to the above, larger networks and corporate networks often have other security requirements:   * **Dedicated firewall systems** – These are used to provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity. * **Access control lists (ACL)** – These are used to further filter access and traffic forwarding. * **Intrusion prevention systems (IPS)** – These are used to identify fast-spreading threats, such as zero-day or zero-hour attacks. * **Virtual private networks (VPN)** – These are used to provide secure access to remote workers.   Network security requirements must take into account the network environment, as well as the various applications, and computing requirements. Both home environments and businesses must be able to secure their data while still allowing for the quality of service that is expected of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.  The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services. | |

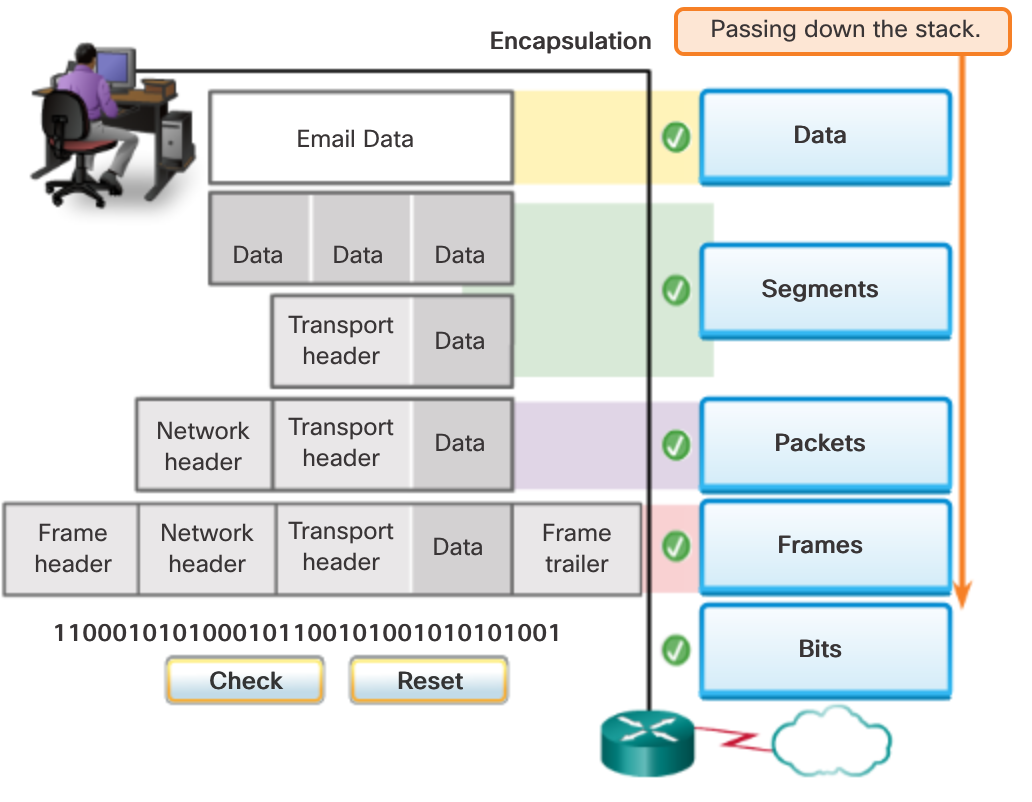




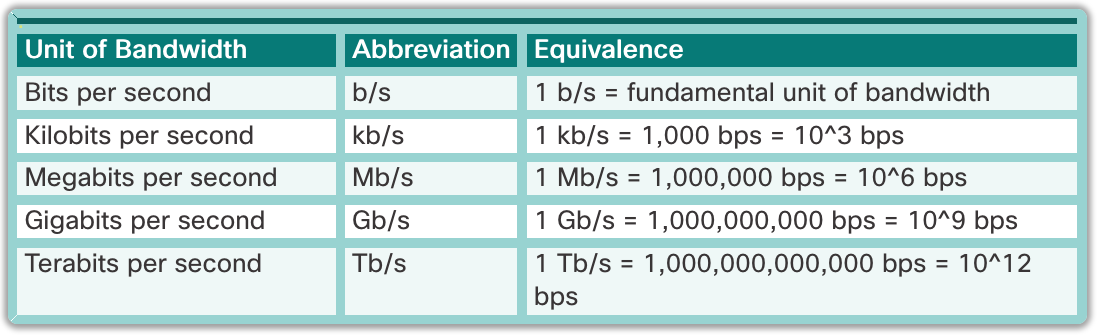
|  |  |
| --- | --- |
|  | **Protocol Interaction**  Communication between a web server and web client is an example of an interaction between several protocols. The protocols shown in the figure include:  **HTTP -** is an application protocol that governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server. Both the client and the web server software implement HTTP as part of the application. HTTP relies on other protocols to govern how the messages are transported between the client and server.  **TCP** - is the transport protocol that manages the individual conversations. TCP divides the HTTP messages into smaller pieces, called segments. These segments are sent between the web server and client processes running at the destination host. TCP is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.  **IP -** is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them to the destination host.  **Ethernet** - is a network access protocol that describes two primary functions: communication over a data link and the physical transmission of data on the network media. Network access protocols are responsible for taking the packets from IP and formatting them to be transmitted over the media. |

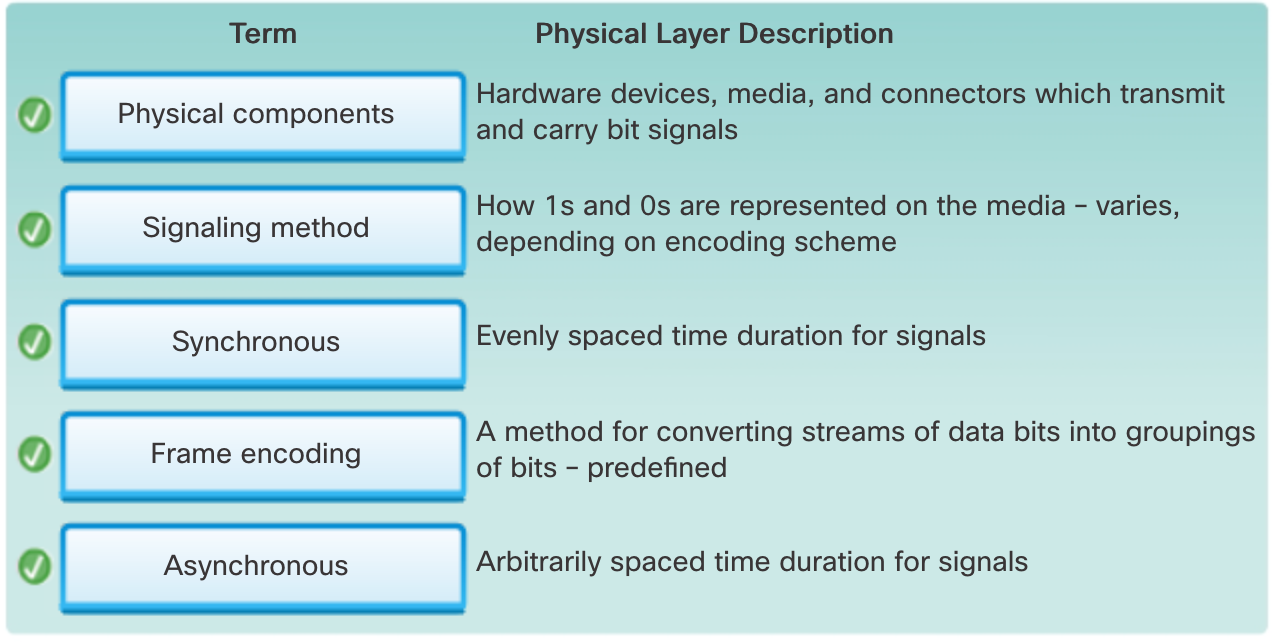


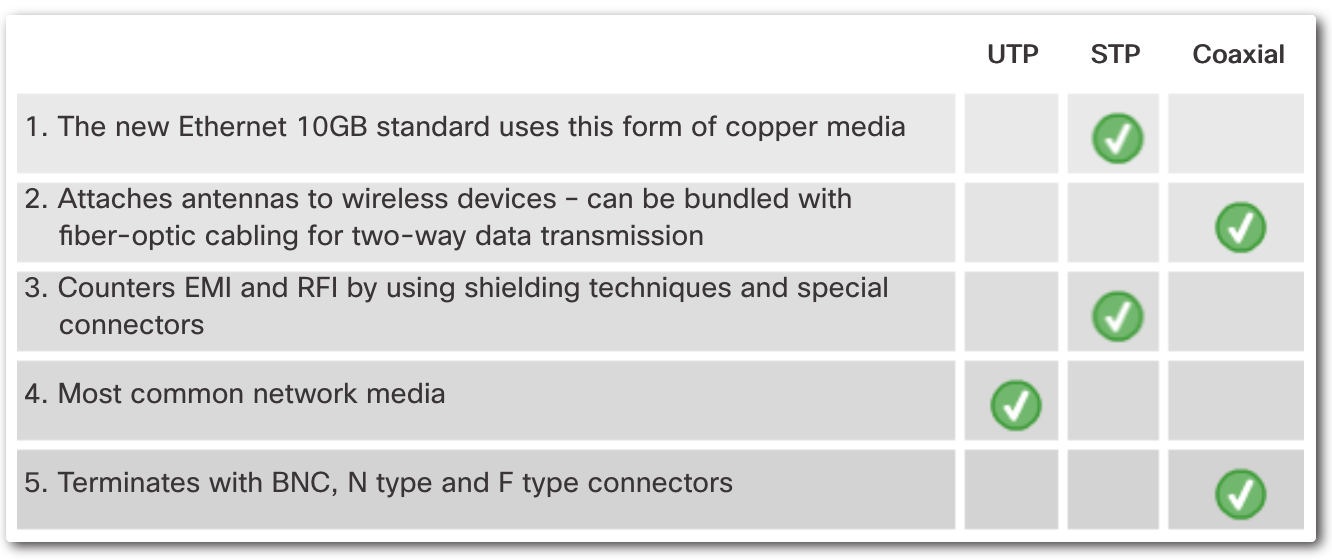
|  |  |
| --- | --- |
|  | **Protocol model** - This type of model closely matches the structure of a particular protocol suite. The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite. TCP/IP is also used as a reference model.  **Reference model** - This type of model provides consistency within all types of network protocols and services by describing what has to be done at a particular layer, but not prescribing how it should be accomplished. The OSI model is a widely known internetwork reference model, but is also a protocol model for the OSI protocol suite. |



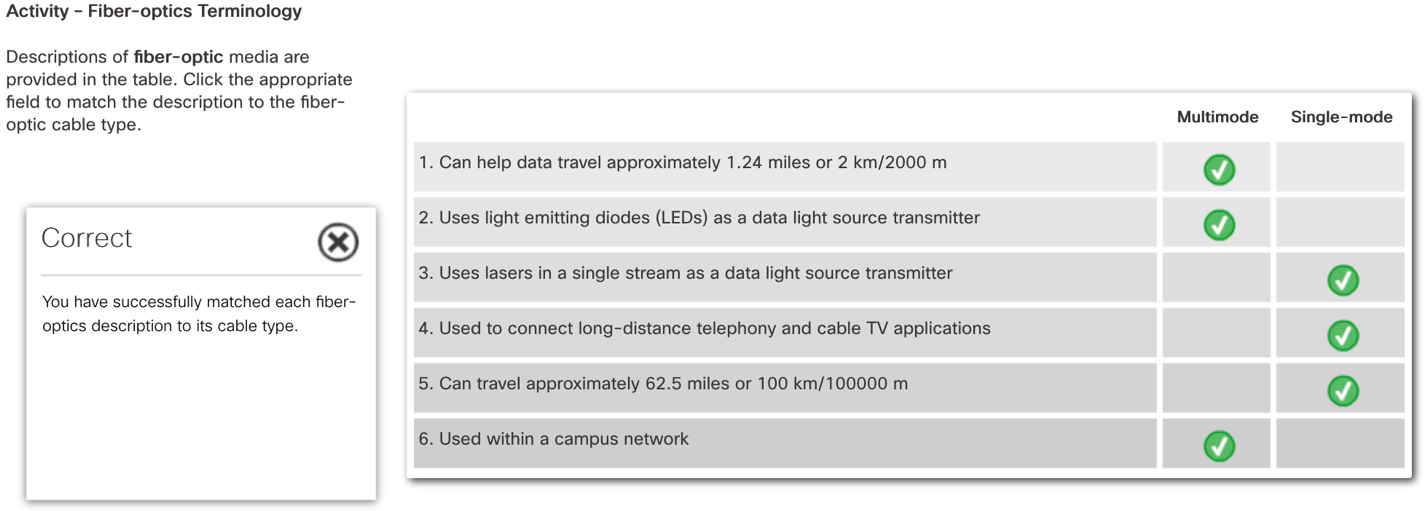
|  |
| --- |
| Physical Layer Standards  The protocols and operations of the upper OSI layers are performed in software designed by software engineers and computer scientists. The services and protocols in the TCP/IP suite are defined by the Internet Engineering Task Force (IETF).  The physical layer consists of electronic circuitry, media, and connectors developed by engineers. Therefore, it is appropriate that the standards governing this hardware are defined by the relevant electrical and communications engineering organizations.  There are many different international and national organizations, regulatory government organizations, and private companies involved in establishing and maintaining physical layer standards. For instance, the physical layer hardware, media, encoding, and signaling standards are defined and governed by the:  International Organization for Standardization (ISO)  Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)  International Telecommunication Union (ITU)  American National Standards Institute (ANSI)  Institute of Electrical and Electronics Engineers (IEEE)  National telecommunications regulatory authorities including the Federal Communication Commission (FCC) in the USA and the European Telecommunications Standards Institute (ETSI) |

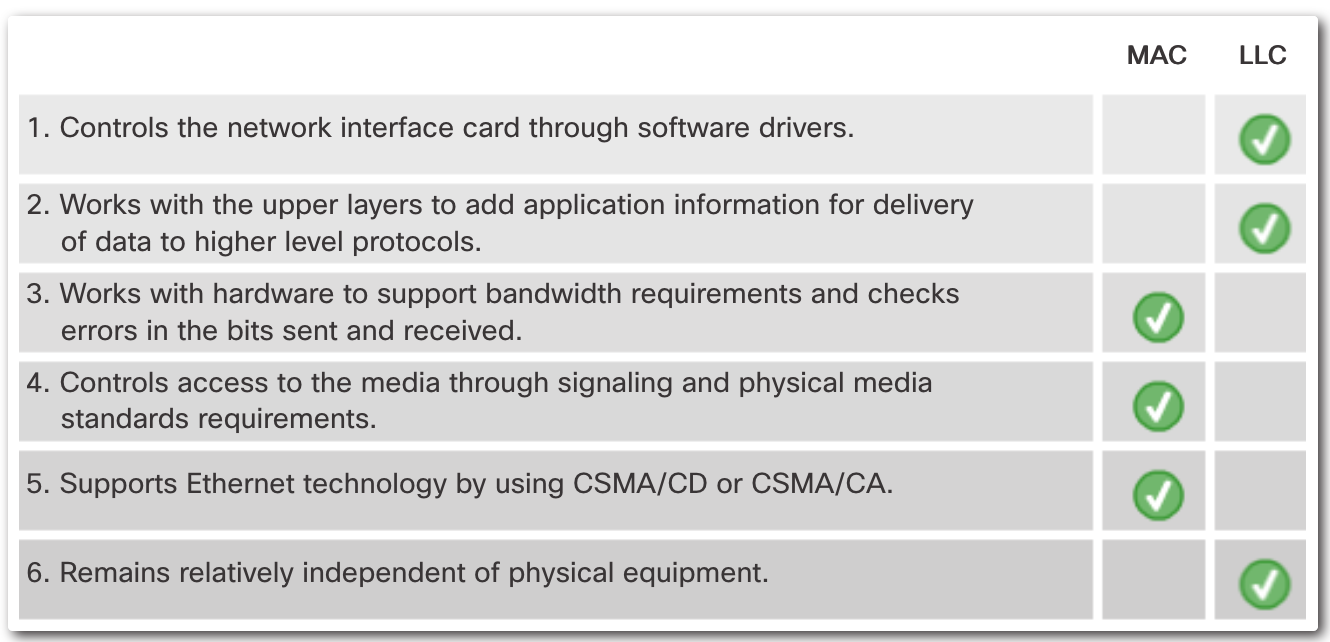






|  |  |
| --- | --- |
|  |  |







|  |  |
| --- | --- |
| <https://www.packettracernetwork.com/labs/packettracerlabs.html>  <https://itexamanswers.net/ccna-2-activities-lab-manuals-packet-tracer-instructions-answers>  lab1-basicswitchconfig.pka | #2 -> Switch -> Host Name  Switch> enable  Switch# configure terminal  Switch(config)# hostname LOCAL-SWITCH  #3 -> Switch -> Banner MOTD (not working)  (config)# banner motd “  Unauthorized access is forbidden”  #4 -> Switch -> Enable Secret  (config)# enable secret cisco  #5 -> Switch -> Service Password Encryption  (config)#service password-encryption  #6 -> Switch -> Console Line -> Password  (config)# line console 0  (config-line)# password ciscoconsole  #6 -> Switch -> Console Line -> Login  (config-line)# login  #6 -> Switch -> Console Line -> History Size  (config-line)# history size 15  #6 -> Switch -> Console Line -> Terminal Line timed out  (config-line)# exec-timeout 6 45  #6 -> Switch -> Console Line -> Logging Synch  (config-line)# logging synchronous  (config-line)# exit  **TELNET**  (config)# line vty 0 15  #6 -> VTY Lines -> VTY Line(x) -> Password  (config-line)# password ciscoconsole  #6 -> VTY Lines -> VTY Line(x) -> Login  (config-line)# login  #6 -> VTY Lines -> VTY Line(x) -> History Size  (config-line)# history size 15  #6 -> VTY Lines -> VTY Line(x) Terminal Line timed out  (config-line)# exec-timeout 8 20  #6 -> VTY Lines -> VTY Line(x) -> Logging Synch  (config-line)# logging synchronous  (config-line)# exit  #7 -> Switch -> Default Gateway  (config)# ip default-gateway 192.168.1.1  #7 -> Switch -> Ports -> Vlan 1 -> IP & Subnet  (config)# interface vlan 1  (config-if)# ip address 192.168.1.2 255.255.255.0  #7 -> Switch -> Ports -> Vlan 1 -> Port Status  (config-if)# show interface switchport |
| lab2-configuringinterfaces.pka | PC: 192.168.1.1  #1 -> Switch0 -> Ports -> FastEthernet(x) -> Duplex  Switch> enable  Switch# configure terminal  Switch(config)# interface range FastEthernet0/1-4  (config-if-range)# duplex full  #1 -> Switch0 -> Ports -> FastEthernet -> Bandwidth  (config-if-range)#speed 100  #1 -> Switch0 -> Ports -> FastEthernet -> Access VLAN  (config-if-range)# switchport access vlan 1  #1 -> Switch0 -> Ports -> FastEthernet -> Port Status  (config-if-range)# no shutdown  (config-if-range)# exit  #3 -> Switch0 -> GigabitEthernet0/1 -> Port Mode  (config)# interface GigabitEthernet0/1  (config-if)# switchport mode trunk  #3 -> Switch0 -> GigabitEthernet0/1 -> Port Status  (config-if)# no shutdown  (config-if)# switchport nonegotiate. (optional)  (config-if)# exit  **Use Copper Cross-Over cable**  PC: 192.168.1.2. **(before set cable between S0->S1)**  Switch(config)# interface range GigabitEthernet0/1-2  (config-if-range)# switchport mode trunk  (config-if-range)# no shutdown  (config-if-range)# exit  **Use Copper Cross-Over cable**  PC: 192.168.1.4. **(before set cable between S1->S2)**  Switch(config)# interface GigabitEthernet0/2  (config-if)# switchport mode trunk  (config-if)# no shutdown  (config-if)# exit |
| lab3-vlan.pka | PC connect to VTP Server  #1 -> VTP SERVER -> VTP -> Domain / Password  VTP-SERVER>enable  VTP-SERVER# configure terminal  VTP-SERVER(config)# vtp mode server  VTP-SERVER(config)#vtp domain TESTDOMAIN  VTP-SERVER(config)#vtp password cisco  VTP-SERVER(config)#exit  (Optional info)  VTP-SERVER# show vlan brief  VTP-SERVER# show vtp status  VTP-SERVER# exit  #2  VTP-SERVER>telnet 192.168.1.2  VTP-CLIENT1>enable  (Optional info)  VTP-CLIENT1# show arp  VTP-CLIENT1# show mac-address-table  VTP-CLIENT1#configure terminal  #2 - > VTP CLIENT1 -> VTP -> VTP Mode  VTP-CLIENT1(config)# vtp mode client  #3 - > VTP CLIENT1 -> VTP -> Domain Name  VTP-CLIENT1(config)# vtp domain TESTDOMAIN  #3 - > VTP CLIENT1 -> VTP -> VTP Password  VTP-CLIENT1(config)# vtp password cisco  #2 (All links must be configured as trunk lines)  VTP-CLIENT1(config)# interface Gig0/1  VTP-CLIENT1(config-if)# switchport mode trunk  VTP-CLIENT1(config-if)# exit  VTP-CLIENT1(config)# exit  VTP-CLIENT1# exit  (Repeat step 2 for all other switches: telnet 192.168.1.3  telnet 192.168.1.4)  VTP-SERVER> enable  VTP-SERVER# configure terminal  #4 -> VTP SERVER -> VLANS ->VLAN10 -> VLAN Name  VTP-SERVER (config)# vlan 10  VTP-SERVER (config-vlan)# name STUDENTS  VTP-SERVER (config-vlan)# exit  #4 -> VTP SERVER -> VLANS ->VLAN50 -> VLAN Name  VTP-SERVER (config)# vlan 50  VTP-SERVER (config-vlan)# name SERVERS  VTP-SERVER (config-vlan)# exit  VTP-SERVER (config)# exit  (Optional Verify info)  VTP-SERVER #show vlan brief  VTP-SERVER #show vtp status |
| lab4-portsecurity.pka | #5 Attach the **Copper Straight-Through** cable between ROGUE (FastEthernet0) and Switch (FastEthernet0/4)  #2 -> Switch -> Host Name  Switch> enable  (Optional info)  Switch# show running-config  Switch# show port-security interface FastEthernet0/1  Switch# show port-security interface FastEthernet0/2  Switch# show port-security interface FastEthernet0/3  Switch0 -> Ports -> FastEthernet0/x -> Dynamic Mode  Switch# configure terminal  (config)# interface range FastEthernet0/1-4  (config-if-range)# switchport mode access  Switch0 -> Ports -> FastEthernet0/x -> Port Security -> Enabled  (config-if-range)# switchport port-security  Switch0 -> Ports -> FastEthernet0/1&2 -> Port Security -> Maximum Static MACs  (config-if-range)# switchport port-security maximum 3  Switch0 -> Ports -> FastEthernet0/1&2 -> Port Security -> Sticky Enabled  (config-if-range)# switchport port-security mac-address sticky  Switch0 -> Ports -> FastEthernet0/3 -> Port Status  (config)# interface range FastEthernet0/1-4  (config-if-range)# no shutdown  (config-if-range)# exit  Switch0 -> Ports -> FastEthernet0/1 -> Port Security -> Port Security Violation  (config)# interface FastEthernet0/1  (config-if)# switchport port-security violation restrict  (config-if)# exit  #3 Switch0 -> Ports -> FastEthernet0/3 -> Port Security -> Static MACs  (config)# interface FastEthernet0/3  (config-if)# switchport port-security mac-address 00E0.A3CE.3236  Switch0 -> Ports -> FastEthernet0/3 -> Port Security -> Port Security Violation  (config-if)# switchport port-security violation protect  Switch0 -> Ports -> FastEthernet0/3 -> Port Security -> Maximum Static MACs  (config-if)#no switchport port-security maximum  Switch0 -> Ports -> FastEthernet0/3 -> Port Security -> Sticky Enabled  (config-if-range)# no switchport port-security mac-address sticky  (config-if)# exit |
| lab6-basicroutersetup.pka | #1 -> Configure Terminal  Connect to the router using Terminal, be sure you are using 9600 bits per seconds.  #2 -> GATEWAY -> Host Name  Router>enable  Router# configure terminal  Router(config)#hostname GATEWAY  #3 -> GATEWAY -> Enable Password  GATEWAY(config)#enable password cisco  #3 -> GATEWAY -> Enable Secret  GATEWAY(config)#enable secret cisco  #4 -> GATEWAY -> Service Password Encryption  (config)# service password-encryption  #5 -> GATEWAY -> Console Line -> Password  (config)# line console 0  (config-line)#password cisco  #5 -> GATEWAY -> Console Line -> Login  (config-line)# login  #5 -> GATEWAY -> Console Line -> History Size  (config-line)# history size 10  #5 -> GATEWAY -> Console Line -> Login Sync  (config-line)# logging synchronous  #5 -> GATEWAY -> Console Line -> Login Sync  (config-line)# logging synchronous  #5 -> GATEWAY -> Console Line -> Line timed out  (config-line)# exec-timeout 2 45 |
| lab7-staticroutes.pka | Click on Atlanta router and select CLI tab  Atlanta>enable  (Optional info)  Atlanta# show running-config | include ip route  Atlanta# show ip interface brief  Atlanta# show interfaces Fa0/0 | include address  Atlanta# show running-config | include interface | ip address  #1 -> Atlanta -> Ports -> FastEthernet0/0 -> IP Address  Atlanta# configure terminal  Atlanta(config)# interface Fa0/0  <http://www.subnet-calculator.com/> - 30 Mask Bit (252)  (config-if)# ip address 10.112.8.1 255.255.255.252  #1 -> Atlanta -> Ports -> FastEthernet0/0 -> Post Status  (config-if)# no shutdown  (config-if)# exit  #3 -> Atlanta -> Routes -> Static Routes -> Route0  (route New York Fa0/0)  (config)# ip route 10.114.65.128 255.255.255.252 10.112.8.2  Click on Chicago router and select CLI tab  #1 -> Chicago -> Ports -> FastEthernet0/1 -> IP Address Chicago> en  Chicago# conf t  Chicago(config)# int Fa0/1  (config-if)# ip address 10.114.65.130 255.255.255.252  #1 -> Chicago -> Ports -> FastEthernet0/1 -> Post Status  (config-if)# no shutdown  (config-if)# exit  #2 -> Chicago -> Routes -> Static Routes -> Route0  (route New York Fa0/1)  (config)# ip route 10.112.8.0 255.255.255.252 10.114.65.129  Click on New-York router and select CLI tab  #1 -> New-York -> Ports -> FastEthernet0/0 -> IP Address  New-York> en  New-York# conf t  New-York (config)# int Fa0/0  (config-if)# ip address 10.112.8.2 255.255.255.252  #1 -> New-York -> Ports -> FastEthernet0/0 -> Post Status  (config-if)# no shutdown  #1 -> New-York -> Ports -> FastEthernet0/1 -> IP Address  New-York (config)# int Fa0/1  (config-if)# ip address 10.114.65.129 255.255.255.252  #1 -> New-York -> Ports -> FastEthernet0/1 -> Post Status  (config-if)# no shutdown  #4 Test  Internet Control Message Protocol - ICMP (ping command)  Click Simulation button  Click “Show All/None”  Click “Edit Filters”  IPv4 select ICMP checkbox  Close dialog  Click on the toolbar the “Closed envelope with plus icon”  And click on Atlanta router than on the Chicago router  Click on the Play Controls the Play button  To delete scenario click on the bottom right expand button with the black arrow, then click Delete button |
| lab11-hdlc.pka | Router-A>enable  (Optional info)  Router-A# show interfaces serial 0/0/0  Router-A#show running-config | include interface | ip address  #1 -> Router A -> Ports -> Serial0/0/0 -> IP Address  Router-A# configure terminal  Router-A(config)#interface serial 0/0/0  (config-if)# ip address 192.168.10.6 255.255.255.252  #1 -> Router A -> Ports -> Serial0/0/0 -> Port Status  (config-if)# no shutdown  #2 -> Router B -> Ports -> Serial0/0/0 -> IP Address  Router-B>enable  Router-B# configure terminal  Router-B(config)#interface serial 0/0/0  (config-if)# ip address 192.168.10.5 255.255.255.252  #2 -> Router B -> Ports -> Serial0/0/0 -> Port Status  (config-if)# no shutdown  #2 -> Router B -> Ports -> Serial0/0/0 -> Clock Rate  Router-B(config-if)# clock rate 250000  (Optional)  Router-B(config-if)# encapsulation hdlc  Testing:  Router-A>ping 192.168.10.5  Router-B>ping 192.168.10.6 |
| lab12-ppp.pka | Router-A>enable  (Optional info)  Router-A# show interfaces serial 0/0/0  Router-A#show running-config | include interface | ip address  #1 -> Router A -> Ports -> Serial0/0/0 -> IP Address  Router-A# configure terminal  Router-A(config)#interface serial 0/0/0  (config-if)# ip address 192.168.10.6 255.255.255.252  #1 -> Router A -> Ports -> Serial0/0/0 -> Port Status  (config-if)# no shutdown  #1 -> Router A -> Ports -> Serial0/0/0 -> Encapsulation  Router-A(config-if)# encapsulation ppp  #2 -> Router B -> Ports -> Serial0/0/0 -> IP Address  Router-B>enable  Router-B# configure terminal  Router-B(config)#interface serial 0/0/0  (config-if)# ip address 192.168.10.5 255.255.255.252  #2 -> Router B -> Ports -> Serial0/0/0 -> Port Status  (config-if)# no shutdown  #2 -> Router B -> Ports -> Serial0/0/0 -> Clock Rate  Router-B(config-if)# clock rate 250000  #2 -> Router B -> Ports -> Serial0/0/0 -> Encapsulation  Router-B(config-if)# encapsulation ppp  Testing:  Router-A>ping 192.168.10.5  Router-B>ping 192.168.10.6 |
| lab13-framerelay.pka | NEW-YORK>enable  (EIGRP info):  NEW-YORK# show running-config | include router eigrp  NEW-YORK# show frame-relay map  NEW-YORK# show ip eigrp interfaces  NEW-YORK# show ip eigrp neighbors  #2 -> NEW\_YORK -> Ports -> Serial0/0/0 -> Encapsulation  NEW-YORK# configure terminal  NEW-YORK(config)# interface Serial0/0/0  NEW-YORK(config-if)# encapsulation frame-relay  #2 -> NEW\_YORK -> Ports -> Serial0/0/0.120 -> Port Status  NEW-YORK(config-if)#no ip address  (config-if)# interface Serial0/0/0.120 point-to-point  #2 -> NEW\_YORK -> Ports -> Serial0/0/0.120 -> IP Address & Subnet Mask  (config-subif)# ip address 10.6.0.1 255.255.255.252  #4 -> NEW\_YORK -> Ports -> Serial0/0/0.120 -> DLCI -> DLCI 120  (config-subif)# frame-relay interface-dlci 120  #2 -> NEW\_YORK -> Ports -> Serial0/0/0.130 -> Port Status  NEW-YORK(config-if)#no ip address  (config-if)# interface Serial0/0/0.130 point-to-point  #2 -> NEW\_YORK -> Ports -> Serial0/0/0.120 -> IP Address & Subnet Mask  (config-subif)# ip address 10.6.0.5 255.255.255.252  #4 -> NEW\_YORK -> Ports -> Serial0/0/0.130 -> DLCI -> DLCI 130  (config-subif)# frame-relay interface-dlci 130  (config-subif)# exit  2 -> NEW\_YORK -> EIGRP -> Networks -> Route0  NEW-YORK(config)#router eigrp 200  NEW-YORK(config-router)#network 10.6.0.0  2 -> NEW-YORK -> EIGRP -> Auto Summary  NEW-YORK (config-router)# no auto-summary  MEXICO>enable  #2 -> MEXICO -> Ports -> Serial0/0/0 -> Encapsulation  MEXICO # configure terminal  MEXICO (config)# interface Serial0/0/0  MEXICO (config-if)# encapsulation frame-relay  #2 -> MEXICO -> Ports -> Serial0/0/0.110 -> Port Status  MEXICO (config-if)#no ip address  (config-if)# interface Serial0/0/0.110 point-to-point  #2 -> MEXICO -> Ports -> Serial0/0/0.110 -> IP Address & Subnet Mask  (config-subif)# ip address 10.6.0.2 255.255.255.252  #4 -> MEXICO -> Ports -> Serial0/0/0.110 -> DLCI -> DLCI 110  (config-subif)# frame-relay interface-dlci 110  (config-subif)# exit  #1 -> MEXICO -> Ports -> Serial0/0/0.110 -> Frame Relay -> LMI Type  MEXICO(config)# interface Serial0/0/0  MEXICO(config-if)# frame-relay lmi-type q933a  (config-if)# exit  2 -> MEXICO -> EIGRP -> Networks -> Route0  MEXICO (config)#router eigrp 200  MEXICO (config-router)# network 10.6.0.0  2 -> MEXICO -> EIGRP -> Auto Summary  MEXICO (config-router)# no auto-summary  PARIS>enable  #2 -> PARIS -> Ports -> Serial0/0/0 -> Encapsulation  PARIS # configure terminal  PARIS (config)# interface Serial0/0/0  PARIS (config-if)# encapsulation frame-relay  #2 -> PARIS -> Ports -> Serial0/0/0.110 -> Port Status  PARIS (config-if)#no ip address  (config-if)# interface Serial0/0/0.110 point-to-point  #2 -> PARIS -> Ports -> Serial0/0/0.110 -> IP Address & Subnet Mask  (config-subif)# ip address 10.6.0.6 255.255.255.252  #4 -> PARIS -> Ports -> Serial0/0/0.110 -> DLCI -> DLCI 110  (config-subif)# frame-relay interface-dlci 110  (config-subif)# exit  2 -> PARIS -> EIGRP -> Networks -> Route0  PARIS (config)#router eigrp 200  PARIS (config-router)# network 10.6.0.0  2 -> PARIS -> EIGRP -> Auto Summary  PARIS(config-router)# no auto-summary |
| lab14-radius.pka | #2 -> R1 -> Host Name  Router>enable  Router # configure terminal  Router(config)#hostname R1  #3(No Points)  R1(config)# interface F0/0  R1(config-if)#ip address 192.168.1.1 255.255.255.0  R1(config-if)#no shutdown  R1(config-if)# interface F0/1  R1(config-if)#ip address 192.168.2.1 255.255.255.0  R1(config-if)#no shutdown  R1(config-if)#exit  #4 -> R1 -> VTY Lines -> VTY Line 0 -> Login  R1(config)#line vty 0  R1(config-line)# login authentication default  #4 -> R1 -> VTY Lines -> VTY Line 15 -> Login  R1(config)#line vty 15  R1(config-line)# login authentication default  R1(config-line)# exit  #4 -> R1 -> AAA -> New-model  R1(config)#aaa new-model  #4 -> R1 -> RADIUS Client -> RADIUS Server Hosts  R1(config)# radius-server host 192.168.1.2 key p@ssword  R1(config)# exit  #6 Open Command Promt from the Server or Laptop  C:\> telnet 192.168.1.1  or  C:\> telnet 192.168.2.1 |
| lab15-etherchannel.pka | CENTRAL>enable  (Optional info)  CENTRAL#show running-config | include ip address  CENTRAL# show ip route  CENTRAL# show etherchannel  CENTRAL# show etherchannel summary  CENTRAL -> Routers -> IP Routing  CENTRAL# configure terminal  CENTRAL(config)# ip routing  CENTRAL -> RIP -> Networks -> Version  CENTRAL(config)# router rip  CENTRAL(config-router)# version 2  CENTRAL -> RIP -> Networks -> Route 0  CENTRAL(config-router)#network 10.0.0.0  CENTRAL -> RIP -> Networks -> Route 1  CENTRAL(config-router)#network 192.168.1.0  (Continue after setting a ROUTER)  ROUTER -> Routers -> IP Routing  ROUTER>enable  ROUTER # configure terminal  ROUTER (config)# ip routing  ROUTER -> RIP -> Networks -> Version  ROUTER (config)# router rip  ROUTER (config-router)# version 2  ROUTER -> RIP -> Networks -> Route 0  ROUTER (config-router)# network 10.0.0.0  …  #LAYER 3 EATHERCHANNEL -> 3 ROUTER(config)# interface range Fa0/23-24 ROUTER(config-if-range)# channel-group 1 mode on  # LAYER 3 EATHERCHANNEL -> 4 ROUTER(config-if)# interface port-channel 1 ROUTER(config-if)# no switchport ROUTER(config-if)#ip address 10.6.0.2 255.255.255.0  …  # LAYER 3 EATHERCHANNEL -> 1 CENTRAL(config)# interface range Fa0/23-24 CENTRAL(config-if-range)#channel-group 3 mode on  #LAYER 3 EATHERCHANNEL -> 2 CENTRAL(config-if)# interface port-channel 3 CENTRAL(config-if)# no switchport CENTRAL(config-if)# ip address 10.6.0.1 255.255.255.0  #LAYER 2 EATHERCHANNEL -> 1 CENTRAL(config-if-range)#interface range Fa0/1-2  CENTRAL(config-if-range)#channel-protocol pagp  CENTRAL(config-if-range)#channel-group 1 mode desirable  #LAYER 2 EATHERCHANNEL -> 1  CENTRAL(config-if-range)#interface range Fa0/3-4  CENTRAL(config-if-range)#channel-protocol lacp  CENTRAL(config-if-range)#channel-group 2 mode active  #LAYER 2 EATHERCHANNEL -> 2 SW1>enable SW1#configure terminal SW1(config)#interface range Fa0/1-2  SW1(config-if-range)#channel-protocol pagp  SW1(config-if-range)#channel-group 1 mode auto  #LAYER 2 EATHERCHANNEL -> 3 SW2>enable SW2#configure terminal SW2(config)#interface range Fa0/1-2  SW2(config-if-range)#channel-protocol lacp SW2(config-if-range)#channel-group 1 mode passive  #IP CONECTIVITY -> 2 (Laptop 0 -> Command Promt) C:\>ping 192.168.1.1 C:\>ping 10.6.0.1 C:\>ping 10.6.0.2 |
| lab16\_ssl\_vpn | Open on the laptop a browser and type: <http://192.168.2.3>  Open Firewall -> CLI tab  ciscoasa>enable  Password: (Press Enter)  (Optional info)  ciscoasa#show switch vlan  ciscoasa#show interface ip brief  ciscoasa#show running-config | include interface | nameif  ciscoasa#show running-config | include interface | security  ciscoasa# configure terminal  ciscoasa(config)#interface Vlan1  ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0  ciscoasa(config-if)# exit  (optional add DHCP for other devices in the network)  ciscoasa(config)# dhcpd address 192.168.2.2-192.168.2.33 inside  Open the Server IP (192.168.2.x) 🡪 Command Promt  C:\>ping 192.168.2.1  In case of failure, verify cable **not** injected to vlan2 port (0)  Or verify Server Gateway pointing to Gateway 192.168.2.1  ciscoasa(config)#interface Vlan2  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0  Open the Laptop (192.168.1.x) 🡪 Command Promt  C:\>ping 192.168.1.1  In case of failure, verify cable injected to vlan2 port (0)  Or verify Laptop Gateway pointing to Gateway 192.168.1.1  ----  Optional Laptop Client(s)  Open the Server IP (192.168.1.x) 🡪 Command Promt  C:\>ping 192.168.2.3 (block by Firewall)  ciscoasa(config)# access-list access\_rule extended permit icmp any any echo  ciscoasa(config)# access-group access\_rule out interface inside  C:\>ping 192.168.2.3 (Now should work)  ----  ----  Optional Server ping Client(s)  Open the Server IP (192.168.2.x) 🡪 Command Promt  C:\>ping 192.168.1.2 (block by Firewall)  ciscoasa(config)# access-list access\_rule extended permit icmp any any echo-reply  (Optional – if not defined before)  ciscoasa(config)# access-group access\_rule out interface inside  C:\>ping 192.168.1.2 (Now should work)  ----  Create user:  ciscoasa(config)# username test password test.test  Create group policy (can be done from UI-Config)  ciscoasa(config)#group-policy **user\_group** internal  ciscoasa(config)#group-policy **user\_group** attributes  ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-clientless  ciscoasa(config-group-policy)#webvpn  ciscoasa(config-group-webvpn)#url-list value **site1**  ciscoasa(config-group-webvpn)#tunnel-group **user\_profile** type remote-access  ciscoasa(config)#tunnel-group **user\_profile** general-attributes  ciscoasa(config-tunnel-general)#default-group-policy **user\_group**  ciscoasa(config-tunnel-general)#username **test** attributes  ciscoasa(config-username)#vpn-group-policy **user\_group**  ciscoasa(config-username)#exit  Enable webvpn  ciscoasa(config)#webvpn  ciscoasa(config-webvpn)#enable outside  Open Web Browser on the Laptop and enter HTTPS connection to the outside Gateway:  <https://192.168.1.1>  Username: test  Password: test.test  ----  Optional enable http connection to Web Server  <http://192.168.2.3> - Request Timeout  ciscoasa(config)# access-list access\_rule extended permit tcp any any  (Optional – if not defined before)  ciscoasa(config)# access-group access\_rule out interface inside  --- |
| lab19-asa-5505-dpi.pka | class-map HTTP  match default-inspection-traffic  policy-map TestPolicy  class HTTP  inspect http  service-policy TestPolicy interface inside |
| lab20-CBAC.pka | #2 -> Router 1 -> DHCP Server -> Exclude Addresses Router>enable  Router#configure terminal  Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9  #2 -> Router 1 -> DHCP Server -> Pools -> Pool LAN ->  DNS server IP  Domain Name Name TFTP Server WLC Address:  Router(config)# ip dhcp pool LAN  #2 -> Router 1 -> DHCP Server -> Pools -> Pool LAN ->  Max User  Start IP address  Subnet mask:  Router(dhcp-config)# network 192.168.1.0 255.255.255.0  #2 -> Router 1 -> DHCP Server -> Pools -> Pool LAN ->  Default Gateway  Pool IPs  Router(dhcp-config)#default-router 192.168.1.1  #2 -> Router 1 -> ACL -> 1  Router(config-if)# access-list 1 permit 192.168.1.0 0.0.0.255  #4 -> Router 1 -> ACL -> DENY\_ANY  Router(config)#ip access-list extended DENY\_ANY  Router(config-ext-nacl)#deny ip any any  Router(config-ext-nacl)#exit  #3 -> Router 1 -> NAT -> Inside Source List  Router(config)#ip nat inside source list 1 interface GigabitEthernet0/2 overload  #3 -> Router 1 -> Ports -> GigabitEthernet0/0 -> NAT Mode  Router(dhcp-config)#interface GigabitEthernet0/0  Router(config-if)#ip address 192.168.1.1 255.255.255.0  Router(config-if)#ip nat inside  #3 -> Router 1 -> Ports -> GigabitEthernet0/2 -> NAT Mode  Router(config-if)#interface GigabitEthernet0/2  Router(config-if)#ip address 46.20.146.1 255.255.255.252  Router(config-if)#ip nat outside  #4 -> Router 1 -> Ports -> GigabitEthernet0/2 -> Access-group in  Router(config)# interface GigabitEthernet0/2  Router(config-if)#ip access-group DENY\_ANY in  Router(config-if)#exit  #5 -> Router 1 -> Firewall -> IP Inspect Name …  Router(config)#ip inspect name ALLOWED\_TRAFIC http audit-trail on  #6->Router 1-> Ports -> GigabitEthernet0/2 -> IP Inspect Out  Router(config)#interface GigabitEthernet0/2  Router(config-if)#ip inspect ALLOWED\_TRAFIC out  #6 Verify:  Router# show ip inspect all |