

Computer and Information System Assignment Sample By Call Assignment Help

Table of Contents

Introduction.....	4
Client description.....	4
Requirements and constraints (Site-to-Site VPN, AAA, Frame Relay, Syslog, Firewall & PPP)5	
Justification of implementing these constraints.....	15
Technical description for implementing these constraints.....	16
Description of network topology.....	16
Addressing table.....	17
WAN security.....	18
Description of applying different components of WAN.....	18
Protection parameter.....	19
Assumption and limitation.....	19
Conclusion.....	19
Reference List.....	21
Appendices:.....	23
Appendix 1: Syslog configuration command.....	23
Appendix 2: PPP encapsulation.....	24
Appendix 3: Frame-relay configuration.....	25
Appendix 4: Firewall configuration commands.....	26
Appendix 5: Command used in configuring site-to-site VPN.....	27
Appendix 6: Addressing Table.....	28

List of Figures

Figure 1: Cisco networking design	5
Figure 2: Site-to-site VPN configuration	6
Figure 3: AAA configuration in server	7
Figure 4: AAA Configuration	8
Figure 5: Frame-relay configuration	9
Figure 6: Frame-relay authentication	10
Figure 7: Syslog output	11
Figure 8: Firewall configuration	12
Figure 9: Router0 PPP encapsulation configuration	13
Figure 10: Router1 PPP encapsulation configuration	14
Figure 11: Pinging response from PC0 to PC6 after PPP encapsulation	15
Figure 12: Network Topology	17

Computer and Information System Assignment Sample By Call Assignment Help

Introduction

Telecommunication and WAN security can be used by most of the organizations to safe and secure their organization sites. Telecommunications and network security domain includes the “*Structures, techniques, transport protocols, and security measures*” to give “*Integrity, availability, confidentiality and authentication*” for transmissions over the public and private communication networks. Moreover, WAN security is mainly used in most of the organization to protect “Branch Internet, connection from threats and many more”. This security encrypted the traffic over security “IPSec VPNs” into private and public DCs. On the other hand, it advances “Web traffic to Secure Web Gateway” suppliers and permits or denies traffic to go straightforwardly into the Internet. “WAN or Wide Area Network ” is one of the main parts of Telecommunication Networks. Here in this project we can implement WAN in “Cisco Packet Tracer” and create a full connectivity network infrastructure across different locations in the UAE or other cities or countries. Moreover, security techniques must be included in the design and implementation of the company network.

Client description

Tatweer is a UAE based company which provides network and security solutions and takes an approach to spread their company’s network in three different sites in other cities or countries. A client from UAE gave responsibility to design a network and security control system for safe and secure company network systems in these three different sites. The main motto of the project is to create a full connectivity network infrastructure across three different locations. The client from UAE, with help of the design of this network system and security control can use all or be used particularly according to the company size and requirements (Azeez & Chinazo, 2018). This network system and security control design helps to save and secure networks from three different sites in other cities or countries. Moreover, all the three network connections should be connected into one network and frame relay networking has to be done between the sites. “*Site-to-Site VPN, AAA, Frame Relay, Firewall & PPP*” networking has to be done between the sites which can help to save and secure their networks and cannot be hacked from others. The above-mentioned security techniques client must need to use in the design and implementation of company networks in at least three different sites. All companies require a high security level to be achieved for that the client also needs this high security level in three different sites to protect and secure their networks from unwanted threats.

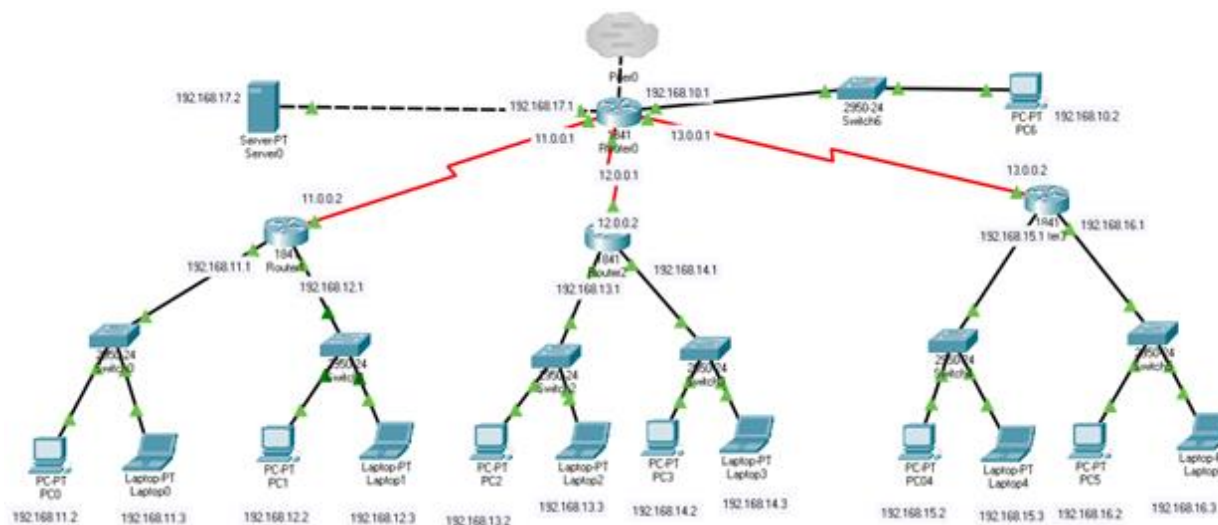


Figure 1: Cisco networking design

Requirements and constraints (Site-to-Site VPN, AAA, Frame Relay, Syslog, Firewall & PPP)

Site-to-Site VPN

This type of “*Site to site virtual private network*” security technology applied here is mainly used for connection between more than one network such as “*Corporate Networks, Branch office networks and many more*”. They use these security techniques in their network systems for high security control purposes (Refer to Appendix 5). This site-to-site VPN security technique helps to leverage an “Internet connection” for private traffic alternatively using “*Private MPLS circuits*”. Moreover, to connect site to site VPN are follows some steps such as

- “*Create a customer Gateway*”
- *Create a target Gateway*
- *Configure routing*
- *Update security Group*
- *Create a site-to-site VPN connection*
- *Download configuration file”.*

Moreover, to set up all these steps requires the “Cisco adaptive security application” for both sites. Below picture shows the Site-to-site VPN Configuration.

```

Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router(config)#conf t
%Invalid hex value
Router(config)#
Router(config)#license boot module c1900 technology-package securityk9
^
% Invalid input detected at '^' marker.

Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exi
Router(config)#crypto isakmp key vpnpa55 address 10.2.2.2
Router(config)#
Router(config)#
Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#description VPN connection to Router3
Router(config-crypto-map)#set peer 10.2.2.2
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#match address 110
Router(config-crypto-map)#
Router(config-crypto-map)#exi
Router(config)#interface s0/0/0
Router(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
Router(config-if)#
Router(config-if)#ex
Router(config)#
Router(config)#exi

Ctrl+F6 to exit CLI focus
Copy Paste

```

Figure 2: Site-to-site VPN configuration

AAA

This AAA security technique is applied in Design Company networks in three different sites mainly used for “*Authentication, authorization and accounting*” networks in three different sites in other cities or countries. Moreover, these security techniques must be implemented and designed in the company network for safe and secure multiple sites (Sneps-Sneppe, 2021). AAA is the platform which can control “*Computer resources, enforcing policies, auditing usage, and providing the information*” for different types of services. On the other hand, in “*Cisco IOS*

device” performances this can be used as a line password and enable password level fifteen. Below pictures shows the “AAA Configuration” in the server.

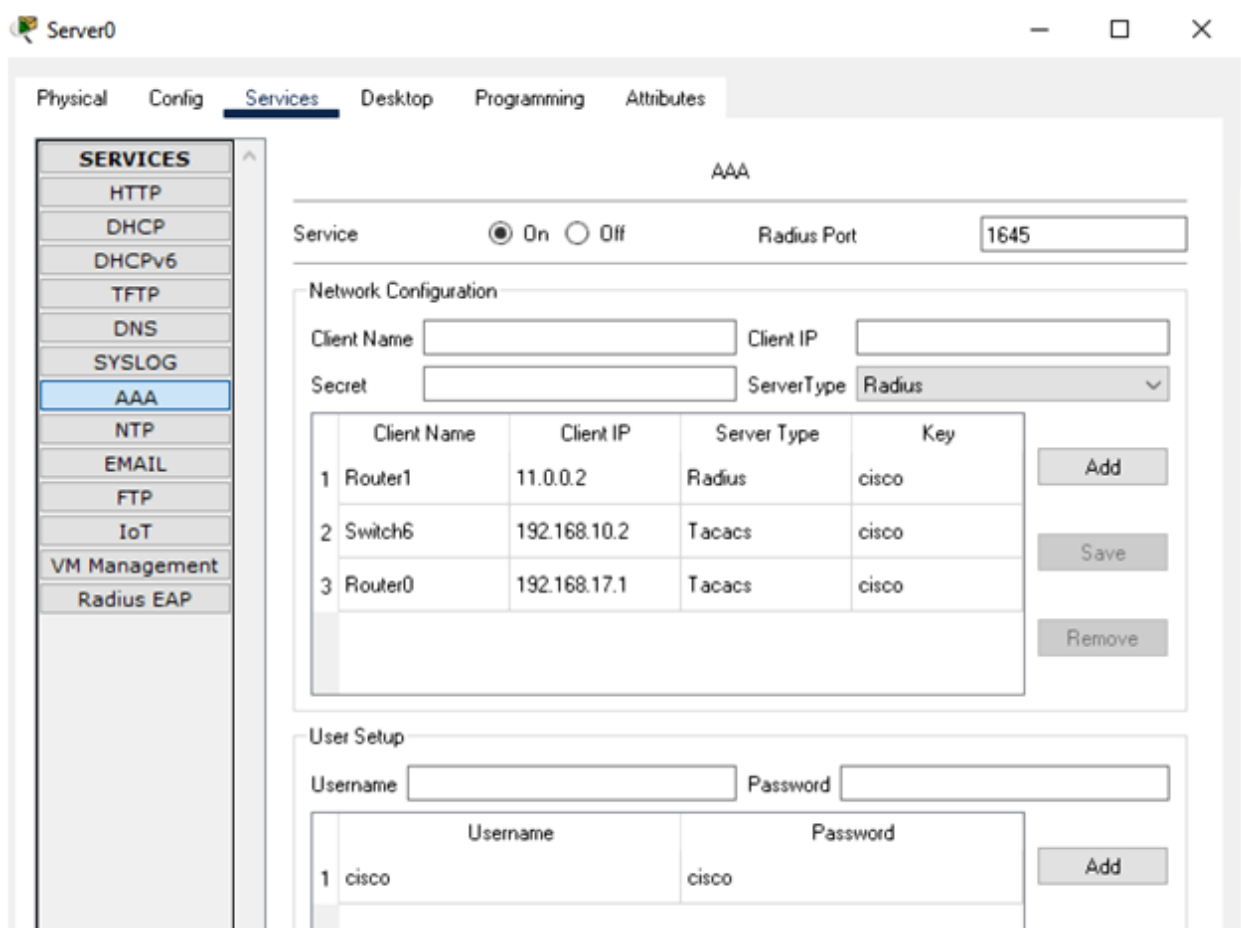


Figure 3: AAA configuration in server

Computer and Information S...

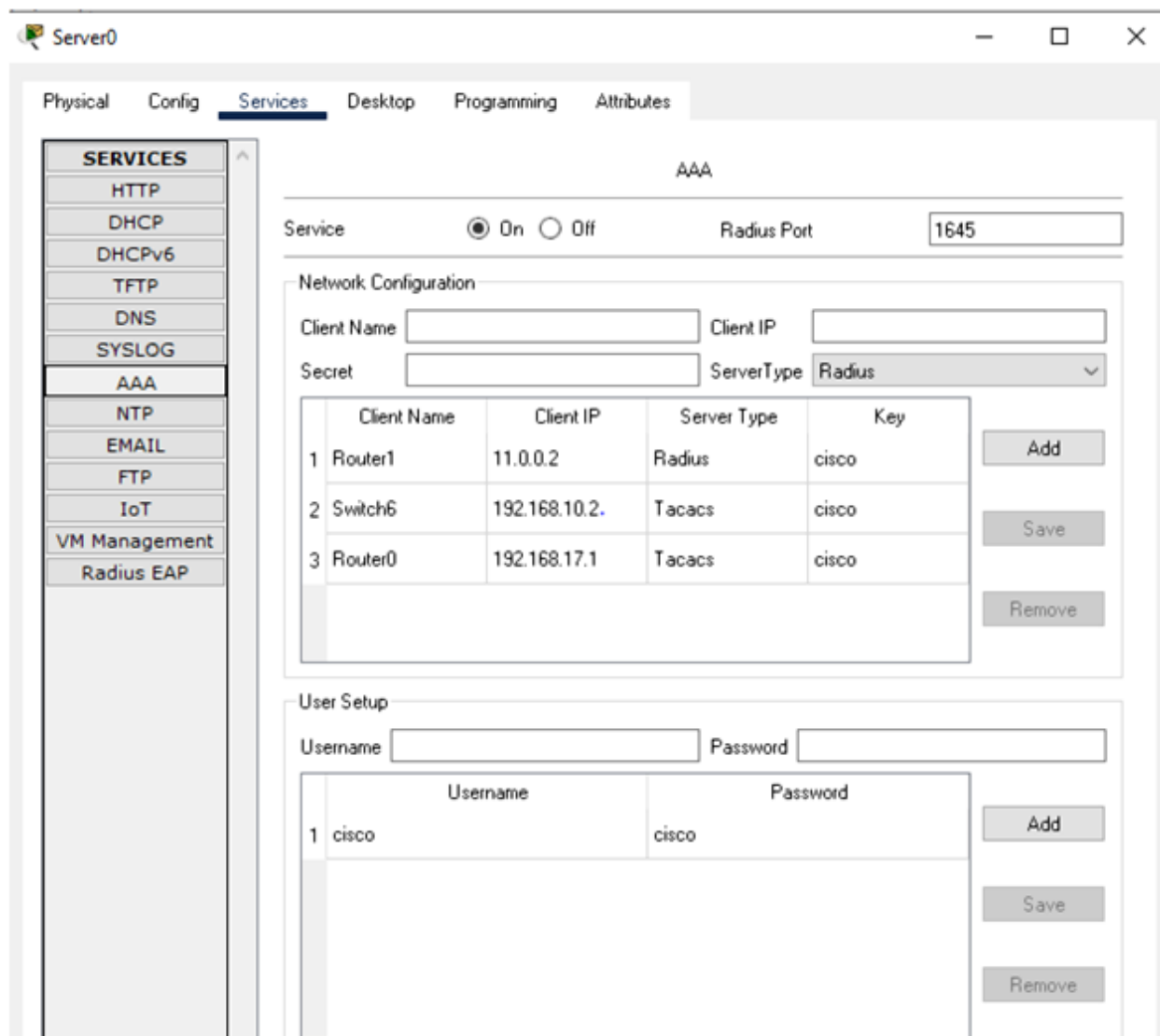


Figure 4: AAA Configuration

Frame Relay

This “*Frame Relay*” security technique helps in this design to define how the frames are routed into a “*Fast packet network*” depending on the address fields into the frame. This can take advantage of the reliability of “*Data communication network*” for minimizing the “*Error checking done*” through the Network nodes. This network technique helps in designing the network by connecting “*Local area network*” as well as WAN’s to the server into a private network environment over “*T 1*” lines. Framework Relay requires a dedicated connection into the “*Transmission period*” and it can send information in packets through “*Frame Relay Network*” (Refer to Appendix 3). This can contain all the required information to route it into the

correct or exact destination. Each of the end points can communicate with many destinations to access links into the network. Below picture shows the Frame Relay Configuration and Authentication.

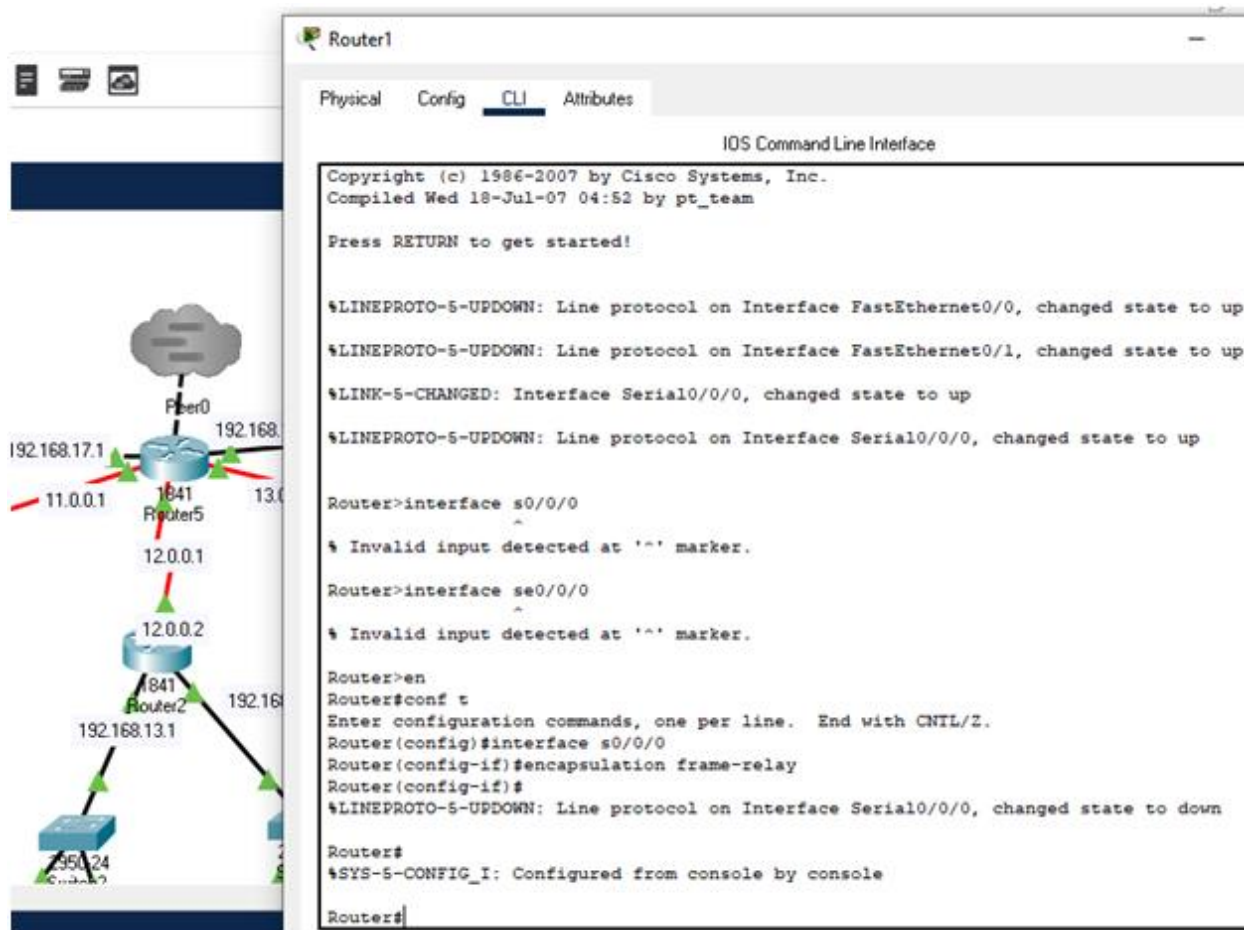


Figure 5: Frame-relay configuration

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface s0/0/0
Router(config-if)#frame-relay map ip 10.1.1.2 102 broadcast
Router(config-if)#frame-relay map ip 10.1.1.3 103 broadcast
Router(config-if)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#frame-relay lmi-type ansi
^
% Invalid input detected at '^' marker.

Router(config)#interface s0/0/0
Router(config-if)#frame-relay map ip 10.1.1.2 102 broadcast
%Address already in map
Router(config-if)#frame-relay lmi-type ansi
Router(config-if)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 6: Frame-relay authentication

Syslog

Here Syslog is mainly used to design the network system for informing the user to unauthorized assessors and immediately sending the system log messages to the specific server (Refer to Appendix 1). This is mainly used for collecting various “Device Logs” to the different machines into specific locations for monitoring (Avaniketh & Soumya, 2018). Moreover, this can reduce or decrease the downtime of servers and other devices and also helps to easily identify critical network related issues. Below picture shows the Syslog Output.

Syslog

Syslog

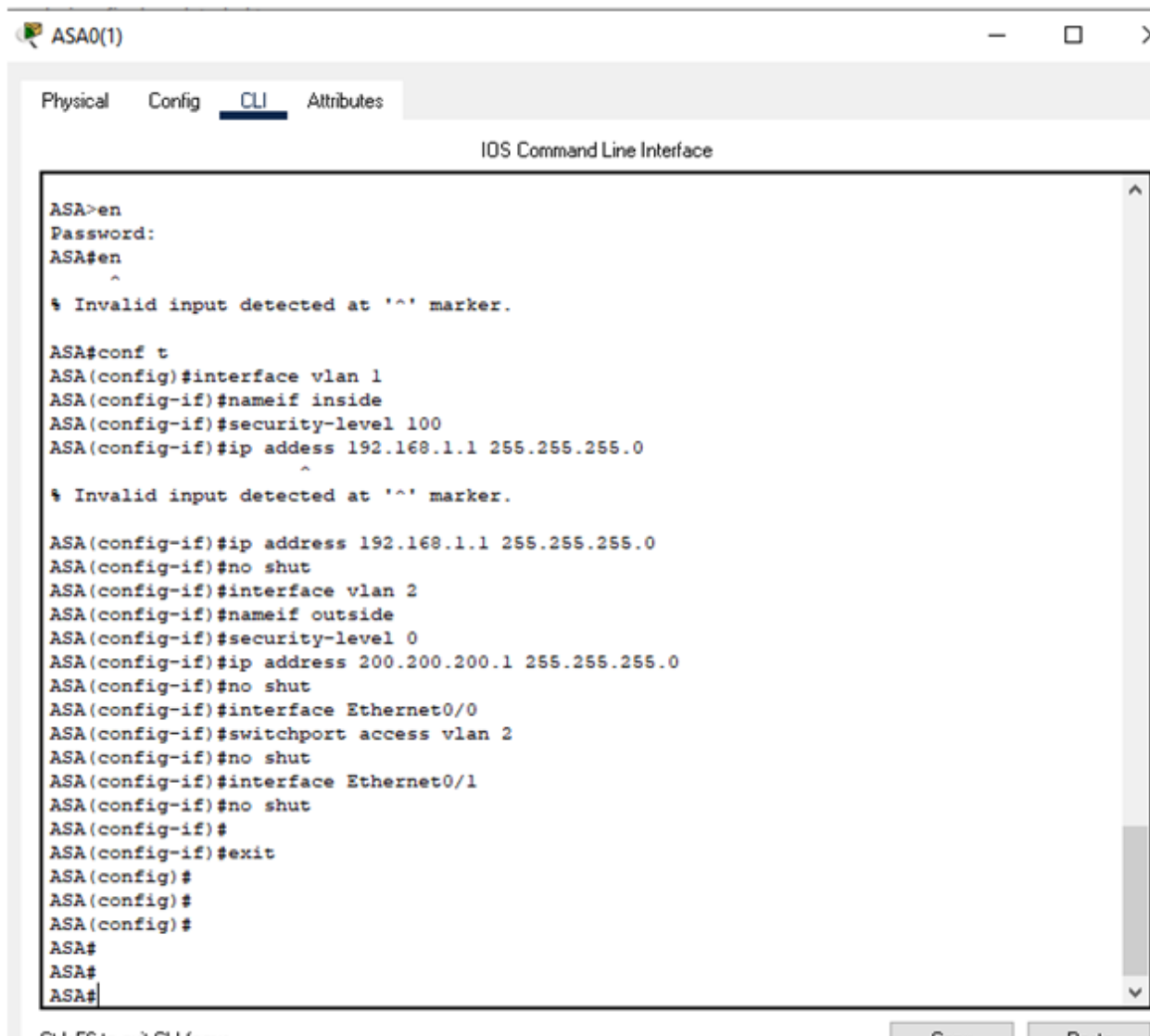
Service On Off

	Time	HostName	Message
1	-	192.168.17.1	%SYS-5-CONFIG_I: Configured I
2	-	192.168.17.1	%SYS-6-LOGGINGHOST_STARTSTOP: I
3	-	192.168.17.1	ICMP: echo reply rcvd, src I
4	-	192.168.17.1	ICMP: echo reply rcvd, src I
5	-	192.168.17.1	ICMP: echo reply rcvd, src I
6	-	192.168.17.1	ICMP: echo reply rcvd, src I
7	-	192.168.17.1	ICMP: echo reply rcvd, src I

Figure 7: Syslog output

Firewall

Firewall is basically used here for filters and monitors outgoing network traffics based on the organization's previous security policies. This is mainly put as a barrier between "Private and public internet networks" (Refer to Appendix 4). This can protect outside attacks such as "Cyber-attacks, hacking and many more" and safe and secure networks from unnecessary network traffic. Moreover, this can prevent or save malicious software's into accessing networks or computers through the internet. Below picture shows the Firewall Configuration.



```

ASA0(1)
Physical Config CLI Attributes
IOS Command Line Interface

ASA>en
Password:
ASA#en
^
% Invalid input detected at '^' marker.

ASA#conf t
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
^
% Invalid input detected at '^' marker.

ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config-if)#no shut
ASA(config-if)#interface vlan 2
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 200.200.200.1 255.255.255.0
ASA(config-if)#no shut
ASA(config-if)#interface Ethernet0/0
ASA(config-if)#switchport access vlan 2
ASA(config-if)#no shut
ASA(config-if)#interface Ethernet0/1
ASA(config-if)#no shut
ASA(config-if)#
ASA(config-if)#exit
ASA(config)#
ASA(config)#
ASA(config)#
ASA#
ASA#
ASA#

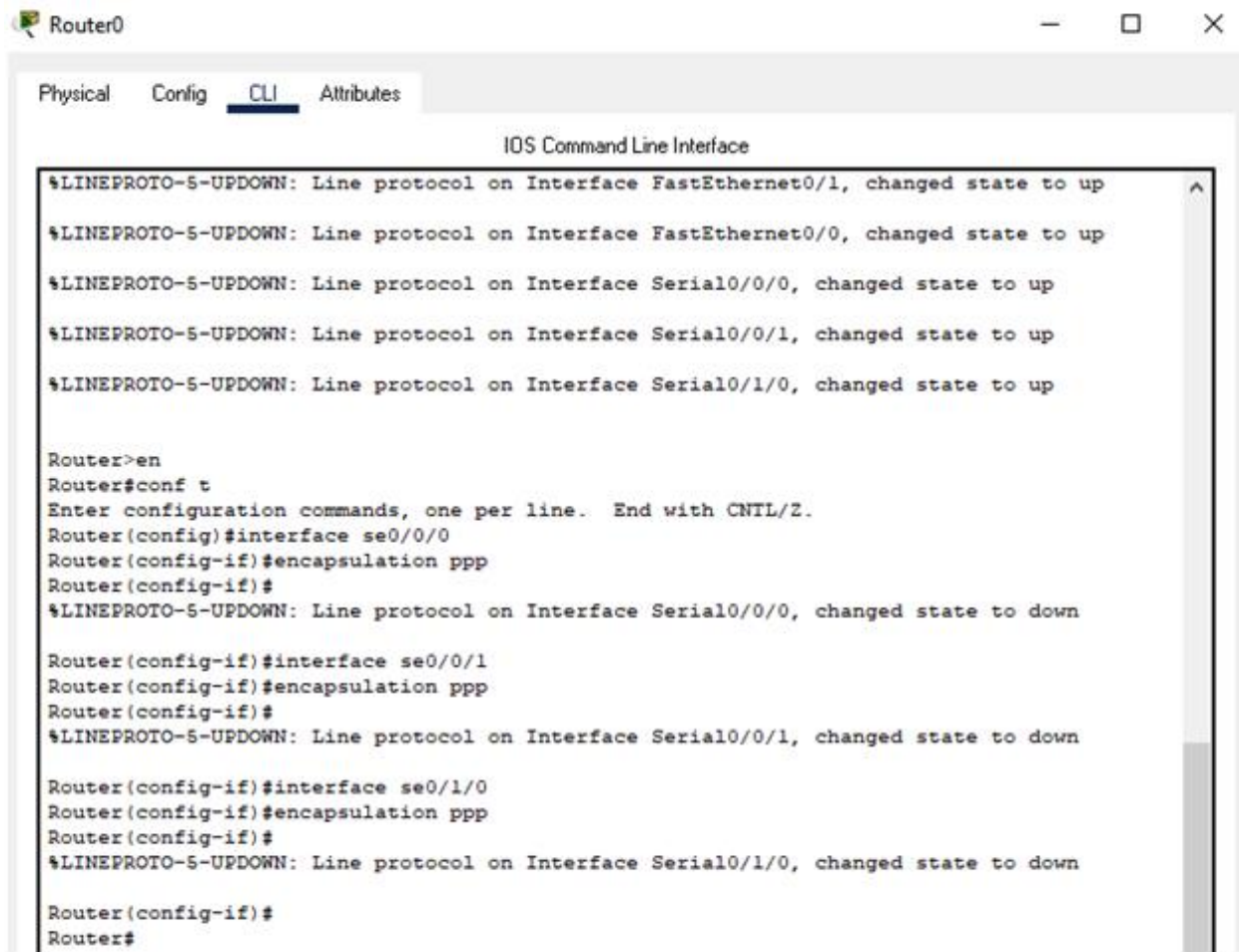
```

Figure 8: Firewall configuration

PPP (Point to Point Protocol)

This security technique is mainly used in the design and implementation of the company network in three different sites to connect one network device to another network device or computers. This security control is used by organizations for easily communicating over the internet (Rayjada & Parsania, 2020). Moreover, this connection exists while 2 systems are physically connected through a “*Telephone Line*”. PPP is a data link used for directly connected between 2 network nodes and eliminates the older “*Serial Line Internet Protocol or SLIP*” (Refer to Appendix 2). However, with the help of this protocol can give “*Connection authentication, transmission encryption, and compression*”. Below picture shows the Router0 to

Router1 PPP encapsulation configuration and pinging response from PC0 to PC6 after PPP encapsulation.



The screenshot shows the CLI of Router0. The window title is "Router0". The tabs are "Physical", "Config", "CLI", and "Attributes". The main content is the "IOS Command Line Interface". The output shows the following commands and responses:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface se0/0/0
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Router(config-if)#interface se0/0/1
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Router(config-if)#interface se0/1/0
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down

Router(config-if)#
Router#
```

Figure 9: Router0 PPP encapsulation configuration

The screenshot shows a Windows desktop environment for PC0. The 'Desktop' tab is selected in the top navigation bar. A Command Prompt window is open, displaying the results of three ping commands to the IP address 192.168.10.2. Each command shows four successful replies with 0% loss and various round-trip times. The statistics for each ping are as follows:

```

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=16ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 8ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=21ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 21ms, Average = 6ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=24ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 24ms, Average = 6ms

```

Figure 11: Pinging response from PC0 to PC6 after PPP encapsulation

Justification of implementing these constraints

Implementing “*Site-to-Site VPN, AAA, Frame Relay, Syslog, Firewall & PPP*” these constraints into design and implementation of company networks at least three different sites in other cities or countries will help to safe and secure the sites from unwanted threats, hackings, attacks and many more purposes. PPP helps in the design by, to directly connect between two networking nodes and reject old SLIP whereas firewall or network security helps to monitor and filter outgoing and incoming traffic networks based on the company’s previous security policy. Firewall is the barrier between private and public networks which can help to monitor and filter network traffic and safe and secure the company network. Moreover, Syslog is used in this

Tatweer company take an approach to spread their company's network in three different sites for protecting the networks and logging unwanted users or authorizations by giving messages into the server. This can help organizations to give more security when designing networks whereas Frame Relay is used for connecting LAN as well as WAN in "Private Network Environments" into the transmission period for reaching information into the exact or correct destination. AAA mainly used by designers to design a company's high security networks for "Controlling, authorizing, authentication, and accounting" computer resources. This can help to give actuarial information to bill for "Services" while site to site VPN helps to connect between more than one networks for private traffic alternatively used for "Private MPLS circuits". However, it has been shown that using these constraints in a company's network design and implementation at least three different sites in other cities or countries will help to connect the networks in one network and also safe and secure the different sites from unwanted threats, hackers, unwanted accesses. The following networking techniques that may be used all or be used partially according to the company size and requirements in three different sites in UAE.

Technical description for implementing these constraints

Implementing these constraints will help to safe and secure the networks and give high security support from the three different sites. These constraints will help to stop unwanted threats, hacking of data and information, attacks and many more. Implementing "Site-to-Site VPN, AAA, Frame Relay, Syslog, Firewall & PPP" will help to better the design structure and give all types of security to prevent unwanted accesses into the networks (Santamaria & Marchiori, 2019). Moreover, implementing WAN in "Cisco Packet Tracer" and creating a full connectivity network infrastructure will help to easily complete the design of the company network across three different locations in the UAE. Implementing these constraints in Cisco is by "Router, Firewall, VPN concentrator, Security appliance, IP connections and many more". The above design shows all of them are connected into three different sites into one network which help to build a high security company network in three different sites in other cities or countries.

Description of network topology

Network topology basically connects one device to other device nodes with each other into a computer network or flows data from one computer device to another computer device. There have been a total of five types of network topology such as "Star, Mesh, Bus, Ring and

Hybrid” (Krishna *et al.* 2019). Mesh topology is mainly connected to other device networks through PPP links where star topology is connected into a central device such as a hub. Bus topology connected with the device through main cables whereas ring topology connected with the two devices either side of it (de Carvalho Silva *et al.* 2017). Lastly hybrid topology is the combination of more than one topology and this is the combination of “*Bus and Mesh Topology*”. Here “*Hybrid topology*” is used to easily design the company network in three different places in other cities or countries.

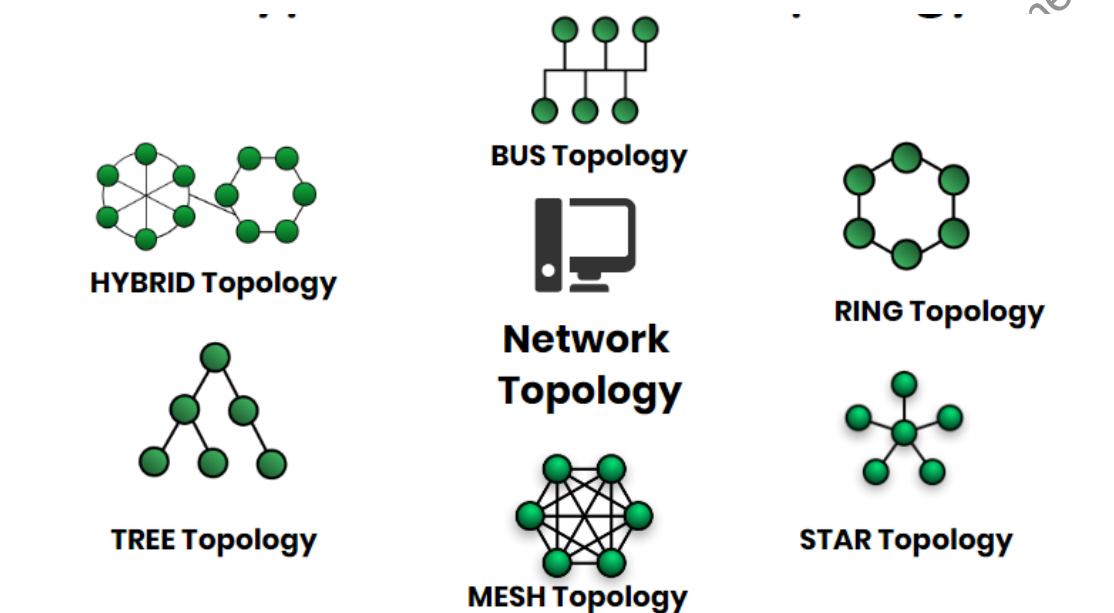


Figure 12: Network Topology

(Source: Kumar *et al.* 2020)

Addressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router0	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.17.1	255.255.255.0	N/A
	Se0/0/0	11.0.0.1	255.0.0.0	N/A
	Se0/0/1	12.0.0.1	255.0.0.0	N/A
	Se0/1/0	13.0.0.1	255.0.0.0	N/A
	Se0/1/1	192.168.1.1	255.255.255.0	N/A
Router1	Fa0/0	192.168.11.1	255.255.255.0	N/A
	Fa0/1	192.168.12.1	255.255.255.0	N/A
	Se0/0/0	11.0.0.2	255.0.0.0	N/A
Router2	Fa0/0	192.168.13.1	255.255.255.0	N/A
	Fa0/1	192.168.14.1	255.255.255.0	N/A
	Se0/0/0	12.0.0.2	255.0.0.0	N/A
Router3	Fa0/0	192.168.15.1	255.255.255.0	N/A
	Fa0/1	192.168.16.1	255.255.255.0	N/A
	Se0/0/0	13.0.0.2	255.0.0.0	N/A
PC0	IPv4	192.168.11.2	255.255.255.0	192.168.11.1
PC1	IPv4	192.168.12.2	255.255.255.0	192.168.12.1
PC2	IPv4	192.168.13.2	255.255.255.0	192.168.13.1
PC3	IPv4	192.168.14.2	255.255.255.0	192.168.14.1
PC4	IPv4	192.168.15.2	255.255.255.0	192.168.15.1
PC5	IPv4	192.168.16.2	255.255.255.0	192.168.16.1
LAPTO P0	IPv4	192.168.11.3	255.255.255.0	192.168.11.1
LAPTO P1	IPv4	192.168.12.3	255.255.255.0	192.168.12.1
LAPTO P2	IPv4	192.168.13.3	255.255.255.0	192.168.13.1
LAPTO P3	IPv4	192.168.14.3	255.255.255.0	192.168.14.1
LAPTO P4	IPv4	192.168.15.3	255.255.255.0	192.168.15.1
LAPTO P5	IPv4	192.168.16.3	255.255.255.0	192.168.16.1
SERVE R0	IPv4	192.168.17.2	255.255.255.0	192.168.17.1

WAN security

Description of applying different components of WAN

Applying different components of WAN which can help to easily make the sign and build a high security control network. Design a high security control network in three different places in WAN for reaching information into the exact location. This WAN security helps systems to easily connect one network to another network sites, nodes, constraints for safe and secure company networks. Design and implementation of the company network in three different places in UAE with different constraints and also applying these constraints of WAN will help to reach data and information, Control network and many more things into the exact location. WAN with different constraints or components connected to the sites through “ISDN, Frame Relay, Dial up internet, Cable modem and many more”. WANs with the help of different components are used in this design to connect LAN or other types of networks together so that networks are connected

in one location and communicate with other user networks more easily (Michael, 2017).

However, WAN here is mainly used for connecting the three different locations into one network and easily receiving the exact information into the exact location. Moreover, in any kind of communication or security or network privacy related issues such as attacks, hacking, and many more, WAN helps to track the location and give the information through different constraints.

Protection parameter

Moreover, using different types of constraints in WAN networks will help the company network design to give full security and support for any kinds of data or information hacking, attacks and many more purposes. The constraints with the help of WAN protect the networks from unwanted users and networks and safe and secure the networks (Rosolem & Roka, 2017). Design company networks in three different sites, WAN helps to connect the three different networks into one network and in any kind of issues it can inform the users and reach the exact location by using different constraints. WAN can protect the company's three different sites by using different components and reaching the exact location.

Assumption and limitation

Designing the company's network in three different places in other cities or countries by connecting to one network, it has been assured that companies with help of different contracts try their best to safe and secure their network from unwanted threats, unauthorized ones, hackers, attackers and many more. Moreover, with the help of this network design company can easily save and secure their data and information and network and easily connect with other network devices or systems through WAN. There has been some limitations or challenges facing to designing company network in three different places into one network connection such as *"Interference can occur, connection is not as stable as wired networks and can drop off"*, lose quality through walls or obstructions, more open to hacking, slower than wired networks, high set up cost, maintenance issues and many more".

Conclusion

This has been concluded that this project assignment can implement WAN in *"Cisco Packet Tracer"* and create a full connectivity network infrastructure in different locations in the UAE or other cities or countries. Moreover, security techniques must be included in the design and implementation of the company network. Different types of security technologies, network topologies help to design and implement a company's network through WAN security. Different

types of constraints of WAN help to reach exact information and give exact network related information about the location. Moreover, the Tatweer Company in UAE approaches to open a network in three different sites in other cities or countries. However, with the help of Cisco packet tracer can easily design a company's network with different constraints in three different sites in other cities or countries.

Computer and Information System Assignment Sample By Call Assignment Help

Reference List

- Avaniketh, P., & Soumya, A (2018). A Preliminary Study on Network Security Attacks & Preventive Measures. <http://shabdbooks.com/gallery/5-sep2019.pdf>
- Azeez, N. A., & Chinazo, O. J. (2018). Achieving Data Authentication with Hmac-Sha256 Algorithm. *Computer Science & Telecommunications*, 54(2).
https://www.researchgate.net/profile/Nureni_Azeez/publication/332182220_ACHIEVING_DATA_AUTHENTICATION_WITH_HMAC-SHA256_ALGORITHM/links/5ca4f16c299bf1b86d632692/ACHIEVING-DATA-AUTHENTICATION-WITH-HMAC-SHA256-ALGORITHM.pdf
- de Carvalho Silva, J., Rodrigues, J. J., Alberti, A. M., Solic, P., & Aquino, A. L. (2017, July). LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities. In *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)* (pp. 1-6). IEEE.
https://www.academia.edu/download/54035442/LoRaWAN_-_A_Low_Power_WAN_Protocol_for_Internet_of_Things-a_Review_and_Opportunities.pdf
- Krishna, T. S. S., Shiva Priya, N., & Rajabhushanam, C. (2019). Design and Implementation of a Secure Campus Network. *Eurasian Journal of Analytical Chemistry*, 13(4), 845-852.
<http://www.eurasianjournals.com/pdf-114794-44196?filename=Design%20and%20Implementation.pdf>
- Kumar, P. R., Wan, A. T., & Suhaili, W. S. H. (2020). Exploring Data Security and Privacy Issues in Internet of Things Based on Five-Layer Architecture. *International Journal of Communication Networks and Information Security*, 12(1), 108-121.
https://www.researchgate.net/profile/Ravi_Kumar415/publication/341201776_Exploring_Data_Security_and_Privacy_Issues_in_Internet_of_Things_Based_on_Five-Layer_Architecture/links/5eb373ca299bf152d6a1c72c/Exploring-Data-Security-and-Privacy-Issues-in-Internet-of-Things-Based-on-Five-Layer-Architecture.pdf
- Michael, G. (2017). Design and implementation of a secure campus network. *International Journal of Pure and Applied Mathematics*, 116(8), 303-307. <http://acadpubl.eu/jsi/2017-116-8/articles/8/51.pdf>

- Rayjada, H., & Parsania, V. (2020). Analytical Research of Data Center Security Implementations and Cyber Attacks. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(7), 14200-14210.
<https://archives.palarch.nl/index.php/jae/article/download/5362/5295>
- Rosolem, J. B., & Roka, R. (2017). Power-over-fiber applications for telecommunications and for electric utilities. *Optical fiber and wireless communications*, 255-278.
<https://www.intechopen.com/books/optical-fiber-and-wireless-communications/power-over-fiber-applications-for-telecommunications-and-for-electric-utilities>
- Santamaria, M., & Marchiori, A. (2019, November). Demystifying LoRa WAN Security and Capacity. In *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-7). IEEE.
<https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/1joXrzQVqpO/pdf>
- Sneps-Sneppe, M. (2021). On Telecommunications Thorn Path to the IP World: From Cybersecurity to Artificial Intelligence. In *Cybersecurity Threats with New Perspectives*. IntechOpen. <https://www.intechopen.com/online-first/on-telecommunications-thorn-path-to-the-ip-world-from-cybersecurity-to-artificial-intelligence>

Appendices:**Appendix 1: Syslog configuration command**

```
Router(config)#interface fa0/0
Router(config-if)#ip add 192.168.17.1 255.255.255.0
Router(config-if)#no shutdown
Router(config)#logging host 192.168.17.2
Router(config)#logging trap debugging
Router#debug ip icmp
Router#ping 192.168.17.2
```

Computer and Information System Assignment Sample By Call Assignment Help

Appendix 2: PPP encapsulation

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface se0/0/0
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Router(config-if)#interface se0/0/1
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Router(config-if)#interface se0/1/0
Router(config-if)#encapsulation ppp
```


Appendix 3: Frame-relay configuration

```
Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface s0/0/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface s0/0/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface s0/0/0

Router(config-if)#encapsulation frame-relay

Router(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
```

Appendix 4: Firewall configuration commands

```
ASA>en
Password:
ASA#conf t
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config-if)#no shut
ASA(config-if)#interface vlan 2
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 200.200.200.1
255.255.255.0
ASA(config-if)#no shut
ASA(config-if)#interface Ethernet0/0
ASA(config-if)#switchport access vlan 2
ASA(config-if)#no shut
ASA(config-if)#interface Ethernet0/1
ASA(config-if)#no shut
ASA(config-if)#exit
```

Appendix 5: Command used in configuring site-to-site VPN

```
Router>en
Router#conf t
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exi
Router(config)#crypto isakmp key vpnpa55 address 10.2.2.2
Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#description VPN connection to Router3
Router(config-crypto-map)#set peer 10.2.2.2
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#match address 110
Router(config-crypto-map)#
Router(config-crypto-map)#exi
Router(config)#interface s0/0/0
Router(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config)#exi
```

Appendix 6: Addressing Table

Computer and Information System Assignment Sample By Call Assignment Help

Telecommunications and Wan Security

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router0	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.17.1	255.255.255.0	N/A
	Se0/0/0	11.0.0.1	255.0.0.0	N/A
	Se0/0/1	12.0.0.1	255.0.0.0	N/A
	Se0/1/0	13.0.0.1	255.0.0.0	N/A
	Se0/1/1	192.168.1.1	255.255.255.0	N/A
Router1	Fa0/0	192.168.11.1	255.255.255.0	N/A
	Fa0/1	192.168.12.1	255.255.255.0	N/A
	Se0/0/0	11.0.0.2	255.0.0.0	N/A
Router2	Fa0/0	192.168.13.1	255.255.255.0	N/A
	Fa0/1	192.168.14.1	255.255.255.0	N/A
	Se0/0/0	12.0.0.2	255.0.0.0	N/A
Router3	Fa0/0	192.168.15.1	255.255.255.0	N/A
	Fa0/1	192.168.16.1	255.255.255.0	N/A
	Se0/0/0	13.0.0.2	255.0.0.0	N/A
PC0	IPV4	192.168.11.2	255.255.255.0	192.168.11.1
PC1	IPV4	192.168.12.2	255.255.255.0	192.168.12.1
PC2	IPV4	192.168.13.2	255.255.255.0	192.168.13.1
PC3	IPV4	192.168.14.2	255.255.255.0	192.168.14.1
PC4	IPV4	192.168.15.2	255.255.255.0	192.168.15.1
PC5	IPV4	192.168.16.2	255.255.255.0	192.168.16.1
LAPTO P0	IPV4	192.168.11.3	255.255.255.0	192.168.11.1
LAPTO P1	IPV4	192.168.12.3	255.255.255.0	192.168.12.1

Telecommunications and Wan Security

LAPTO P2	IPV4	192.168.13.3	255.255.255.0	192.168.13.1
LAPTO P3	IPV4	192.168.14.3	255.255.255.0	192.168.14.1
LAPTO P4	IPV4	192.168.15.3	255.255.255.0	192.168.15.1
LAPTO P5	IPV4	192.168.16.3	255.255.255.0	192.168.16.1
SERVE R0	IPV4	192.168.17.2	255.255.255.0	192.168.17.1

Computer and Information System Assignment Sample By Call Assignment Help