School of Computing, Engineering & Digital Technologies

Course: System Administration and Security

Course Title: (Cryptography Basics, Security Analysis, Design and Implementation)

Student name: **Adefisoye, Toluwani Oyebamijo**

Student number: B1107803

Module Tutors: **Chunyan Mu**

Naumar Israr

Adi El-Dalahmeh

PART I

CRYPTOGRAPHY QUESTION

1. **Asymmetric Encryption and Symmetric Encryption**
   One secret key is required in symmetric to decipher or cypher information. It is regarded as an old and best technique where the key can either be a number, word or random letters. Asymmetric involves the use of two keys to decrypt a plain text. It is a new method that has two keys, the public key that is shared over a large network for encryption and a private key that is kept a secret for decryption.

Key Differences	Symmetric Encryption	Asymmetric Encryption
Size of Data	Large data are transmitted	Small data are being transmitted
Level of security	Security is less secured because it requires one single key	Private and public keys are required for encryption and decryption, makes it more secure
Technique	Old Technique	Modern technique
Encryption Speed	Faster	Slower

ASYMMETRIC ENCRYPTION VULNERABILITIES

Asymmetric encryption uses longer keys in order to ensure better security than symmetric encryption, but the process of decrypting causes a slower encryption speed. Also, keys in asymmetric are more vulnerable to brute force attacks.

2. **Decrypting OHW PHR XWC CC**

   Using a Caesar cypher of shift 3

   OHW PHR XWC CC
   LET MEO UTZ ZZ

3. Public key is (143,11)
   e = 11, P = 13, q = 11 n 143
   N = 13 x 11 = 143
   Ø(n) = (P-1) x (q-1) = (13 – 1) x (11-1)
   Ø(n) = 12 x 10 = 120
   D = 11MOD 120 = 11
   The private key is 11 143 and 11 are the public key

4. Let the encrypted message be represented by M. Also,

N = 143 and D = 11.

M = C MOD N

Therefore M1 = 111 mod 143 = 67

M2 = 4 mod 143 = 114

M3 = 88 mod 143 = 121

M4 = 57 mod 143 = 112

M5 = 116 mod 143 = 116

M6 = 67 mod 143 = 111

0	0	000	NUL	(null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH	(start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX	(start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX	(end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT	(end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ	(enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK	(acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL	(bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS	(backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB	(horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT	(vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF	(NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR	(carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO	(shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI	(shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE	(data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1	(device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2	(device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3	(device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4	(device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK	(negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN	(synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB	(end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN	(cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM	(end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB	(substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC	(escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS	(file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS	(group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS	(record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US	(unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

ASCII values, M1 = C, M2 = R, M3 = Y, M4 = P, M5 = T, M6 = O

5. Assigning Alice (X), Bob (Y) and Carol Z

Sent Messages (Round 1)

- Alice sends Bob $x = g^x$ MOD n
- Bob sends Carol $y = g^y$ MOD n
- Carol sends Alice $z = g^z$ MOD N

Sent Messages (Round 2)

- Alice sends Bob $Z^{1=} Z^{x}$ MOD n= g^{zx} MOD n
- Bob sends Carol $X^{1}= X^{y}$ MOD n= g^{xy} MOD n
- Carol sends Alice $Y^{1=} Y^{z}$ MOD n= g^{yz} MOD n

Computation:

- Alice computes K1= Y^{11x}MOD n= g^{xyz} MOD n
- Bob computes K2= Z^{11y} MOD n= g^{yzx} MOD n
- Carol computes K3= X^{11z} MOD n= g^{xyz} MOD n

$K_1=K_2=K_3$ the secret key Alice, Bob, Carol will share

PART II

CASE 1

MODEL DESCRIPTION

The main scheme of the BLP is to ensure confidentiality and availability of objects and information meant for a specific level only, this means the machine makes sure objects meant for higher-level security are not accessed by low-level security level. This is achieved by preventing information flow from higher-level security to low-security levels. These security levels can be classified into confidential, classified, secret, etc.

Ordering of the Model

Security property is required to maintain the BLP model.

Simple Protection: This security feature only enables "read" access to the file chevalier, which can only be used to read its contents.

To put it another way, the subject's level of security must be greater than or equal to the object's level of security. (s >= o).

*Asterix Characteristics: This attribute permits only 'write' access and is used for writing up. The subject's level of protection must be lower than or equal to the object's. (s=o).

This attribute encompasses both the ideas of reading and 'writing.' It makes certain that all other security elements are followed. Furthermore, a subject's level of security must match that of the object before the subject can read it. (s = = o).

These access privileges are read(r), append(a), and write(w) functions/operations (w).

Where r= read-only

A= write access only

W=read and write access (this makes it discretional)

Levels of security are low and high (low < high)

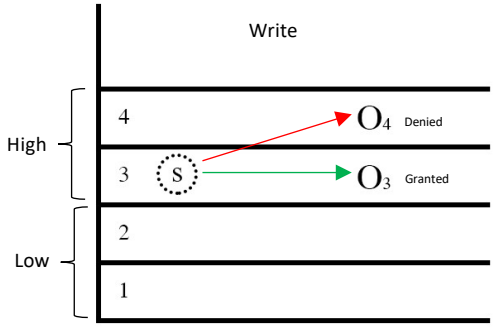
Security set are (army, navy, air force and marines)

Subject	**Objects**
Army S_4	top secret O_4
Air force S_3	secret O_3
Navy S_2	classified O_2
Marines S_1	unclassified O_1

A subject s, and four object O1, O2, O3, O4

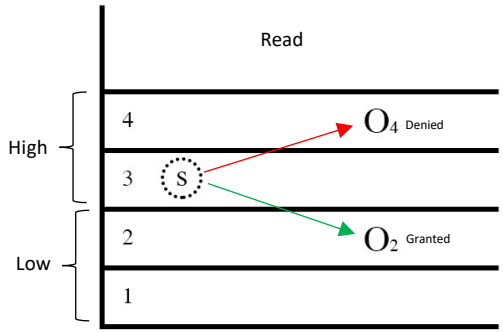
$\lambda(s) = 3, \lambda(O1) = 1, \lambda(O2) = 2, \lambda(O3) = 3, \lambda(O4) = 4$

$B = \emptyset$



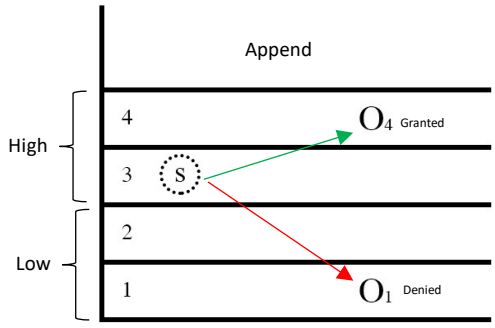
S 'write' access to O_3: granted; B = {(s, O_1, r), (s, O_2, r), **{s, O_3, w}**} (s == o).

S 'read' access to O_4: denied



S 'read' access to O_2: granted; B = {(s, O_1, r), **{s, O_2, r}**} (s > o).

S 'read' access to O_4: denied



S 'append' access to O_4: granted; B = {(s, O_1, r), (s, O_2, r), **{s, O_4, a}**} (s < o).

S 'append' access to O_1: denied

SCENARIO 2

CONFERENCE MANAGEMENT SYSTEM HIGHLIGHTS

I. CHAIR

Obtaining and installing management software

The user can download the relevant software via the Chair Function. this means only the user with the chair function have permission to download software,

The user with the Chair Role is in charge of installing the necessary software.

I. manage Grade
II. This individual is responsible for planning and executing events. (Events can include various conferences)
III. Review Documents
IV. Paper Grading o Reviews

Assigns Papers to Reviewer Users

Provides on-paper comments or discussions

Releases Paper Decisions (Accept/Reject)

REVIEWER

Manage score

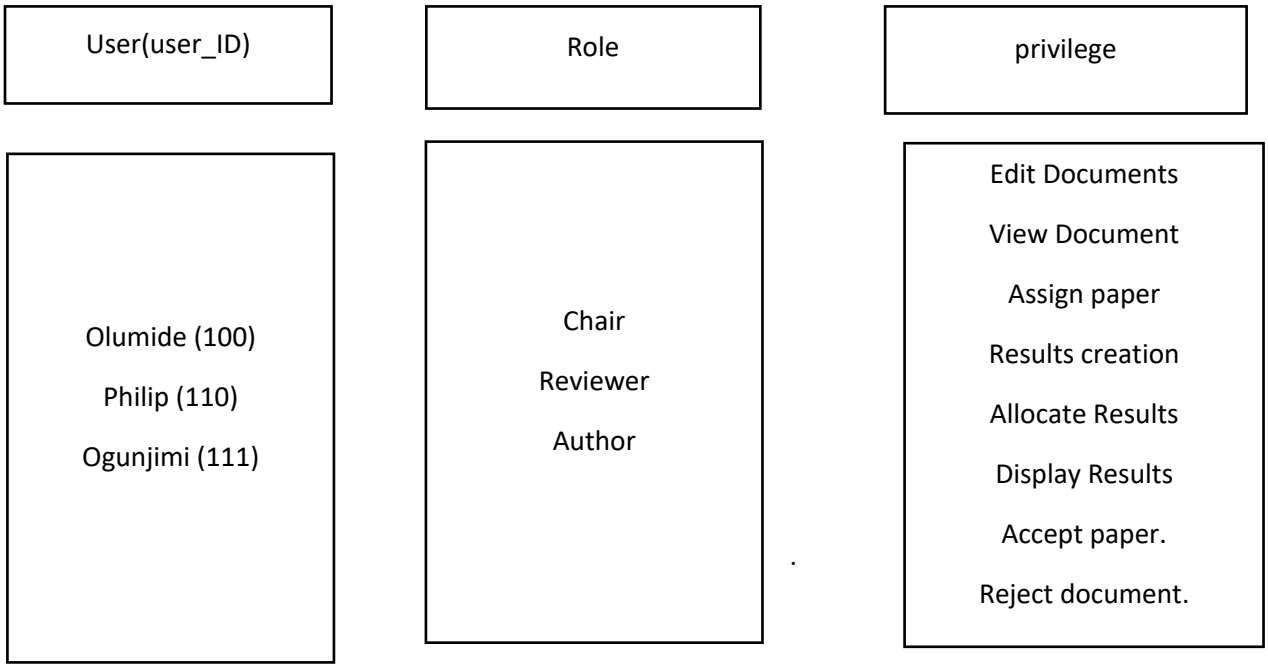
Can contribute to a paper discussion or remark
Can Grade Paper/Assign Grade
can have access to the paper for review.
Can Assign score
Can release decision on paper (Accept/Reject)

AUTHOR

Submit documents.

Analysis

a. Paper review, discussions and conclusion
b. Examine the decision-making process (Accept/Reject)
c. Analyze the evaluation document's result.



A. Communication channel (The capacity of software to interface with clients should be protected.)
B. User IDs - These unique identities are associated with certain positions and should be protected.
C. Results Management - Individual results, and the process should be safeguarded.

In order to safeguard the objects, the system can utilize security models to assure compliance with confidentiality, honesty, and availability. A formal security approach for guaranteeing confidentiality is the Bell-Lapadula model. This model uses mandatory access control to carry out the Department of Defense's (DoD) multilevel security policy A subject must have a clear need to know and satisfy or surpass the classification level of the data in order to gain access to it. It also allows for discretionary access control by using an access matrix to check access rights (Module II Security policies and models: confidentiality policies, Bell-LaPadula model, Integrity policies, Biba model, Clark-Wilson models, Chinese wall model, waterfall model GOALS OF CONFIDENTIALITY POLICIES BLP Model: Multi-level Security Using a MAC Model (n.d.), In an information system, the components of this formal model are separated into two categories: items and topics. By transitioning from a safe to a safe state, every state transition has been proved to protect security. As a result, the system inductively demonstrates that it meets the model's safety objectives. There are various possible states in a Bell–Lapadula state machine when it is implemented in a computer device. Transient functions are defined as functions that characterize the transition from one state to another. A security policy for a system must specify the one and only forms of access that are permitted for subjects to objects. "Secure" will be used to describe the status. The clearance level is compared to the classified level to determine whether a topic is approved for access mode. The clearance or categorization scheme is given in further depth in tertiary form. Information flow is controlled primarily in the BL system.

The following are included:

i. An access control matrix,
ii. A set of subjects, and a set of items

In addition, there are several layers of protection that must be fulfilled in the proper order, and each individual has a clearance level, as well as a classification that allocates each object to a level of security. Each subject has a maximum clearance level that can be reached and is not permitted to receive data that is higher than that level. Consequently, a subject is limited to changing to a clearance level that is lower than the one that was originally assigned to them.

The Biba Integrity Paradigm is a hierarchical security architecture for protecting system assets (or objects) from unauthorized alteration and thereby maintaining system integrity. Subjects can only alter objects to a degree equal to or lower than their own integrity level in this model, which is based on ordinal integrity levels (Naccache et al., 2011). The Biba model can be described by the phrase "read up, write down. " It is more concerned with data integrity than with confidentiality, in the Biba paradigm, subjects can only provide material that is equal to or lower than their own personal honesty level. Subjects, on the other hand, can only understand the material that is on par with or better than their own personal standards of honesty.

According to the Stride Model for Stable Software Creation, the following software qualities must also be enforced when developing software.

Tamper-proof: Tamper-proof devices should prevent unauthenticated individuals from accessing or manipulating data. (integrity),

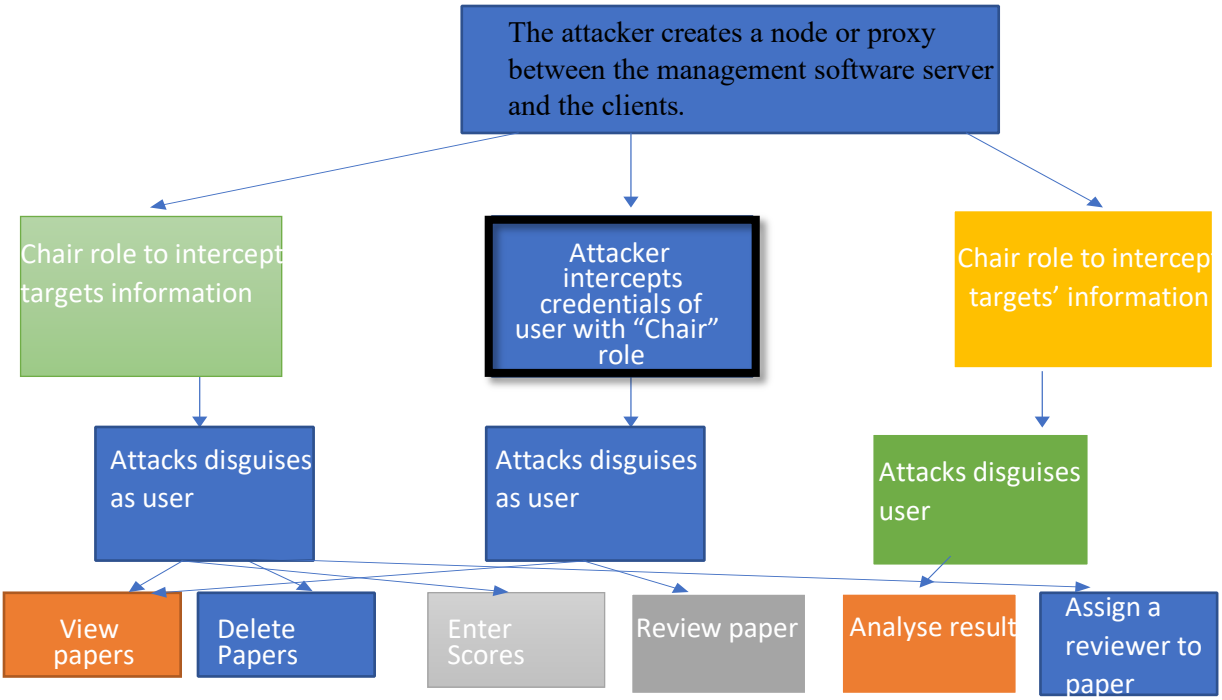
Non-bypass: Getting into the system shouldn't necessitate circumventing security measures like control and authorization checks. (Integrity, confidentiality).

Spoof-Spoof: To get an unfair edge, someone or something impersonates someone else by manipulating facts in order to look like them. According to the design, other users should be unable to assume other users' identities (CT Comm, 2020). (Integrity, confidentiality).

Should be impervious to Denial-of-Service attacks: The system should have controls in place to ensure that it does not refuse service to its clients by accident or deliberately. (availability).

Vulnerability in the systems are

1. In addition, users in the "chair" position are not held to a high standard of transparency under the framework. This means that an account with that position can be compromised and be used to participate in activities that other role users are unable to alter (author, reviewers).
2. The chair's management software seems to include an exploitable software issue. As a result, an adversary gains access to it. Additionally, the user’s identity that includes their responsibilities is managed and created in the management software, therefore having access to it can enable arbitrary profile creation.
3. Another loophole is the intermediary existing between the base station/server where the management application communicates with the client, the attacker can deploy the adversary profile that acts as the link/bridge that in turn intercepts data that is being transmitted between the client and the server. These data can be in any form that holds sensitive contents.



Phishing is a technique that involves sending phony emails to consumers that contain links to counterfeit websites that appear to be identical to the legitimate online conferencing system. The hacker can steal a user's login credentials when they enter them on the bogus website. To intercept server-client communication, a man-in-the-middle attack can be deployed. To carry out a MITM attack on both clients and servers, the attacker must be able to steer packets between both clients and servers using a device under his or her direct control. The attacker can convince the victim to open risky content/email containing malware by launching the attachment in the phishing email, and the target may unintentionally download malware on their PC. After that, the malware takes control of the browser and installs itself without the user's knowledge. The software collects and sends information between the user and particular target websites to the attacker, who then utilizes it to conduct fraud.

SCENARIO 3
PROPOSED LOGICAL DESIGN FOR SMITH LOGISTICS

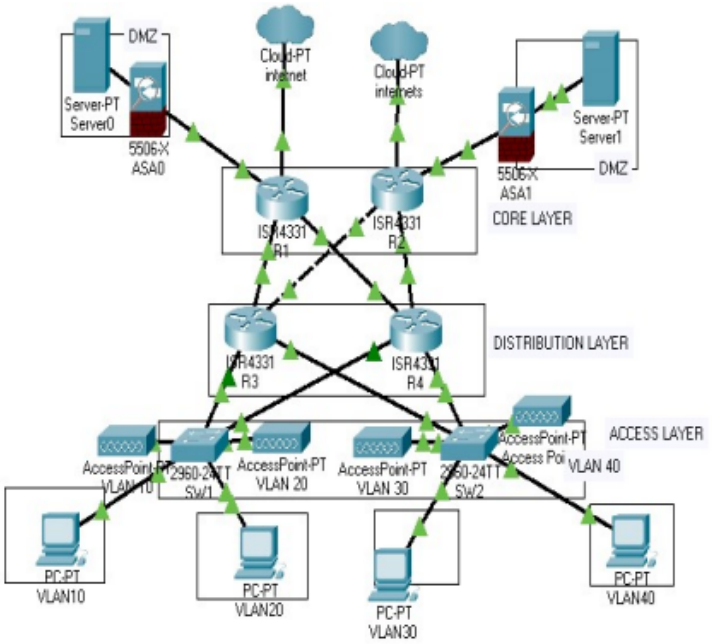


FIGURE 1.1

Figure 1.1 is my proposed network design for smith logistics. This design comprises two routers at the core layer, two routers at the distribution layers, twenty-one layers two switches at the access layer, four access-point (APS) at the access layer, two firewalls at the core layer, and two servers at the core layer.

PROPOSED IP ADDRESS TABLE FOR SMITH LOGISTICS

INTERFACES	IP ADDRESS	SUBNET MASK	NUMBER OF USABLE HOST PER SUBNET	Broadcast
R1G0/0/0	192. 168.1. 1/ 30	255.255.255.252	2	192.168.1.3
R1 G0/0/1	192.168.2.1/30	255.255.255.252	2	192.168.2.3
R1 g0/0/2	192.168.0.1/30	255.255.255.252	2	192.168.0.3
R2 g0/0/0	192.168.3.1/30	255.255.255.252	2	192.168.3.3
R2 g0/0/1	192.168.4.1/30	255.255.255.252	2	192.168.4.3
R2 g0/0/2	192.168.0.2/30	255.255.255.252	2	192.168.0.3
R3 g0/0/1	192.168.4.2/30	255.255.255.252	2	192.168.4.3
R3 g0/0/2	192.168.1.2/30	255.255.255.252	2	192.168.1.3
R4 g0/0/1	192.168.2.2/30	255.255.255.252	2	192.168.2.3
R4 g0/0/2	192.168.3.2/30	255.255.255.252	2	192.168.3.3
VLAN 10	192.168.5.1/25	255.255.255.0	254	192.168.5.127
VLAN 20	192.168.6.1/25	255.255.255.0	254	192.168.6.127
VLAN30	192.168.7.1/25	255.255.255.0	254	192.168.7.127
VLAN40	192.168.8.1/25	255.255.255.0	254	192.168.8.127

Figure 1.2. Ip address table

Figure 1.2 is the proposed IP address table for smith logistics, I used /30 subnet masks at each point-to-point link which gives room for just two valid hosts, and this was used in others to avoid wasting IP addresses. According to the smith logistics requirements, 500 machines are required for the network, There are four VLANs in my proposed design model with .25 subnets, therefore every VLAN contain 126 valid hosts making a total of 506, four wireless APS are also present in the design in the network design, and they are meant for backup at the access layer in case if any user of a company connected using an ethernet cable and if the cable is damaged, the user can connect using wireless and also the wireless is for mobile devices or any other non-ethernet port devices. This network design concept separates a single network into smaller, more manageable networks using hierarchical network architecture. Depending on the hierarchy, each level or tier is responsible for a specific set of tasks. Network designers had a lot of alternatives when it came to optimising and selecting the finest network hardware, applications, and features for various network levels using this design technique. It also made network administrators' troubleshooting considerably easier by eliminating a single point of failure in the network design. This means that if one side of the network fails, the rest of the network will remain operational since a backup device will immediately turn on. In a hierarchical network model for smith logistics, the access layer, the distribution layer, and the core layer, as well as additional sublayers, are provided.

SECURITY MODEL

This model primarily provides a new line of defence for the company, allowing them to detect and mitigate safety violations before they reach the internal network, which holds important properties. (Fortinet, 2021).

WAN protocol proposed for smith logistic design

In order to provide SMITH LOGISTIC with fast Internet connectivity, they received a proposal for broadband Internet access. Broadband Internet connection was chosen since it is a common WAN protocol with a high data transfer rate, implying quick Internet connectivity. Because Very High Digital Subscriber Line (VHDSL) achieves rates up to 52 MBit/s downstream and 16 MBit/s upstream using a single untwisted or twisted pair of copper cable with a 25 kHz to 12 MHz frequency ribbon, new technologies such as high bandwidth DSL (VDSL) will be used for broadband. (WAN Redundancy.org, n.d.).

Proposed Network layer for smith logistics

Using class c IP addresses at Smith logistics' proposed network layer, two subnets that belong to class C was used with the addresses .25 and .30 respectively at the network layer. In each interface of the layer three devices, the /25 allowed 126 eligible hosts to connect, and there are four interfaces of the layer three devices with the /25. RIPV2 is a layer three device that allows communication between the interfaces of the layer three devices. It is found within layer three devices. The most efficient channel to transport data in the network is determined by layer 3 devices

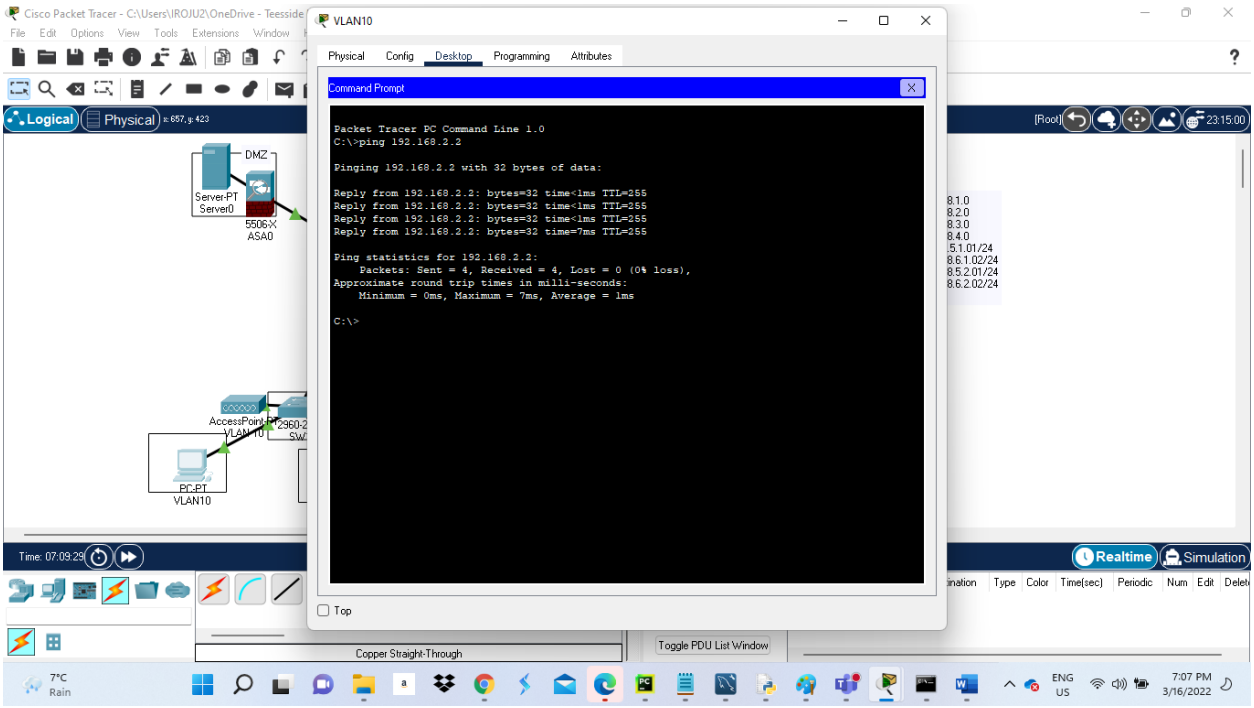
Layer three devices are responsible for determining the most efficient data delivery channel throughout the network.

IEEE PROTOCOL PROPOSED FOR THE DESIGN

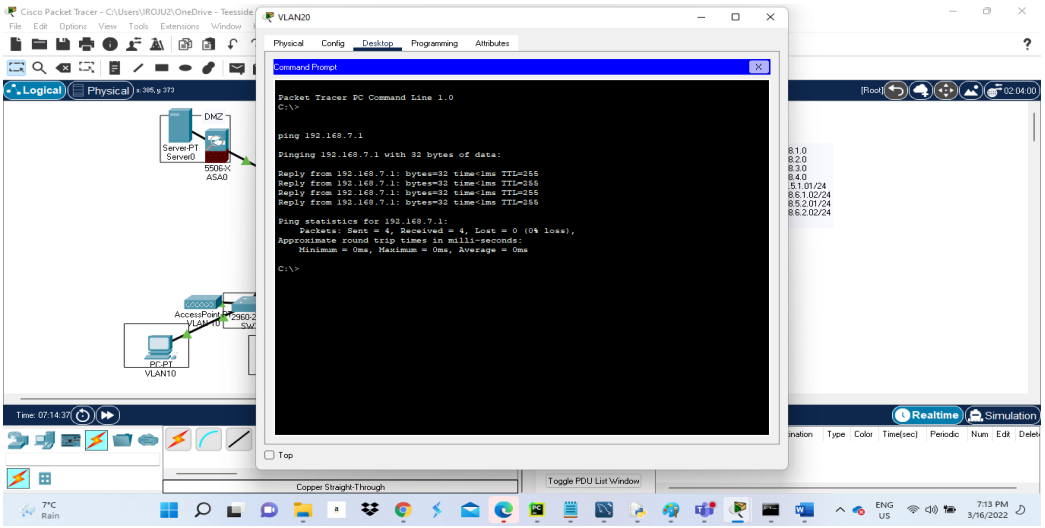
This design incorporates IEEE 802.11, also known as WLAN, which is a network infrastructure access standard for wireless and mobile networks. Wi-Fi 802.11AC MIMO technology has been suggested as an IEEE 802.11 standard, with Wi-Fi speeds of up to 1200Mbps (300Mbps + 867Mbps) and data rates of up to 1200Mbps. The purpose of using a wireless access point was to allow users to connect to the network wirelessly.

IMPLEMENTATTION TESTING

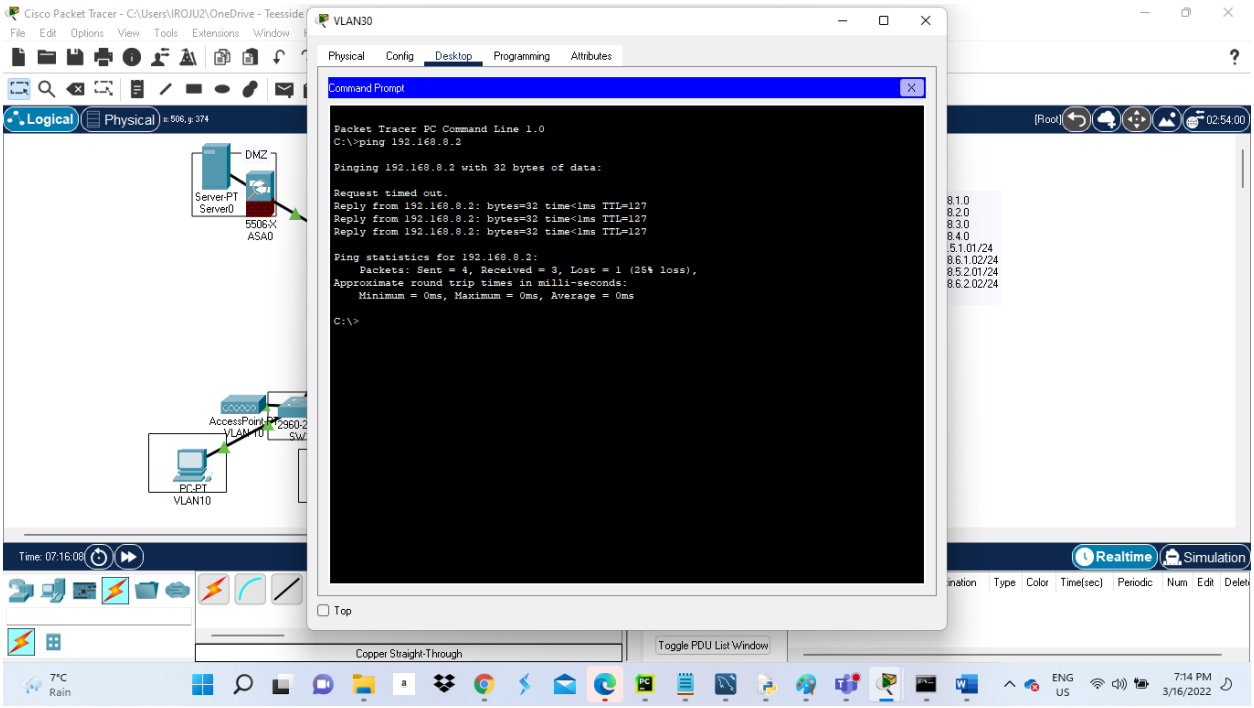
Pinging vlan20 from VLAN 10 to test connectivity, the output of the echo reply is less than 1ms, this proves that the design gives 99.9% availability and less than 1ms performance



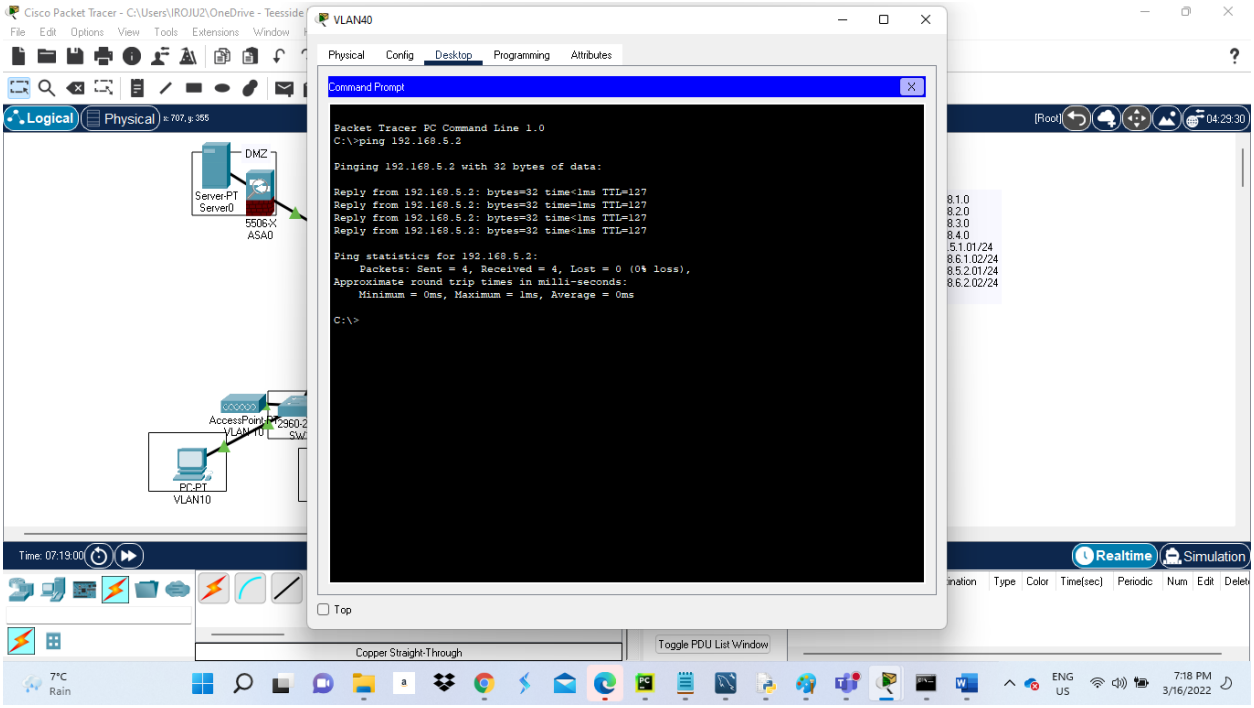
Pinging vlan30 from VLAN 20 to test connectivity, the output of the echo reply is less than 1ms, this proves that the design gives 99.9% availability and less than 1ms performance



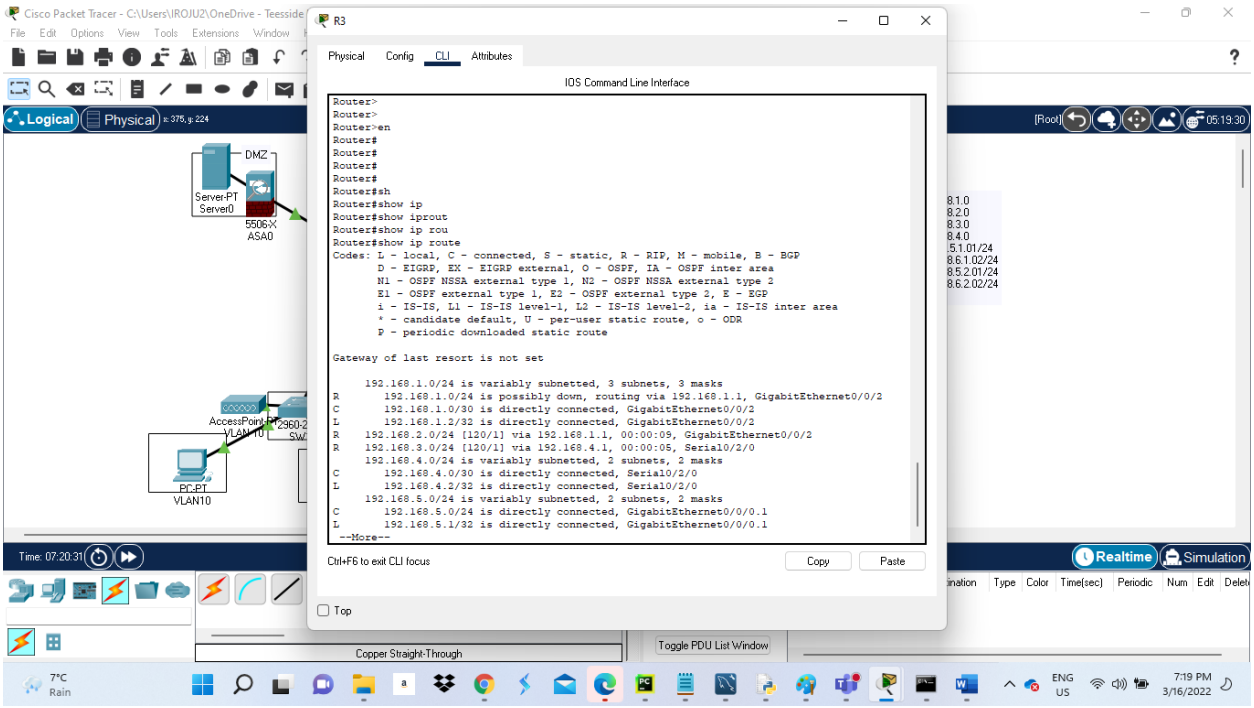
Pinging vlan40 from VLAN 30 to test connectivity, the output of the echo reply is less than 1ms, this proves that the design gives 99.9% availability and less than 1ms performance.



Pinging vlan10 from VLAN 40 to test connectivity, the output of the echo reply is less than 1ms, this proves that the design gives 99.9% availability and less than 1ms performance.



The routing table for my proposed network design



COST OF IMPLIMENTATION 1

ITEMS	DESCRIPTIONS	UNITs	AMOUNTs
router	Dual AC PSUs included, fully functional, factory defaults Cisco ISR4431/K9 router (eBay, n.d.).	2	3,800
Manageable switches	Unclaimed Cisco Meraki Cloud Managed Switch MS120-24P-HW, brand new in box (eBay, n.d.)	2	1,500
Switch Racks	Server Racks & CabinetsRackyRax 600mm x 1000mm Server Cabinet (www.cablemonkey.co.uk, n.d.)	2	999.12
Cable management	RS PRO Grey Slotted Panel Trunking - Open Slot, W25 mm x D25mm, L2m, PVC (uk.rs-online.com, n.d.)	24	1,262.88
server	Ebay Dell Server PowerEdge T140-3,4 GHz - E-2224-8 GB - DDR4-SDRAM - 1000 GB	2	5600
firewall	Cisco Firewall Edition Adaptive Security Appliance with 8 GE Copper Ports Ebay	2	5,600
Cisco POE switches	Cisco SG220-26P-K9 26-Port Gigabit PoE Smart	19	4,730

	Plus Switch New Sealed (eBay, n.d.)		
Network accessories	RJ45, copper cable, etc.	Pack per each	1,000
		Total amount	13,292

COST OF IMPLIMENTATION 2

ITEMS	DESCRIPTIONS	UNITs	AMOUNTs
router	Dual AC PSUs included, fully functional, factory defaults Cisco ISR4431/K9 router (eBay, n.d.).	2	3,800
Manageable switches	Unclaimed Cisco Meraki Cloud Managed Switch MS120-24P-HW, brand new in box (eBay, n.d.)	2	1,500
Switch Racks	Server Racks & CabinetsRackyRax 600mm x 1000mm Server Cabinet (www.cablemonkey.co.uk, n.d.)	2	999.12
Cable management	RS PRO Grey Slotted Panel Trunking - Open Slot, W25 mm x D25mm, L2m, PVC (uk.rs-online.com, n.d.)	24	1,262.88
D-Link switches	D-Link DES-1024D/B Unmanaged Metal Desktop Switch with 24-Port Fast Ethernet - UK Version (www.amazon.co.uk, n.d.)	19	760
Network accessories	RJ45, copper cable, etc.	Pack per each	1,000
		Total amount	13,292

CONCLUSION

Reference list

CT Comm. (2020). *Spoof Proof: Protect Yourself Against Fraudulent Calls*. [online] Available at: https://ctcomm.net/spoof-proof-protect-yourself-against-fraudulent-calls/ [Accessed 17 Mar. 2022].

eBay. (n.d.). *Cisco ISR4431/K9 router, dual AC PSUs included, fully working, factory defaulted*. [online] Available at: https://www.ebay.co.uk/itm/154935533344?hash=item2412e09f20:g:Tc4AAOSwKNliTWAZ [Accessed 8 Apr. 2022].

eBay. (n.d.). *MS120-24P-HW Cisco Meraki Cloud Managed Switch unclaimed, brand new in box.* [online] Available at: https://www.ebay.co.uk/itm/134068219604?hash=item1f3716aed4:g:F0MAAOSwxk5iQie- [Accessed 8 Apr. 2022].

Fortinet (2021). *What Is a DMZ and Why Would You Use It?* [online] Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/what-is-dmz [Accessed 20 Mar. 2022].

Module II Security policies and models: confidentiality policies, Bell-LaPadula model, Integrity policies, Biba model, Clark-Wilson models, Chinese wall model, waterfall model GOALS OF CONFIDENTIALITY POLICIES Bell-LaPadula Model: A MAC Model for Achieving Multi-level Security. (n.d.). [online] Available at: http://www.icet.ac.in/Uploads/Downloads/MOD2.pdf [Accessed 17 Mar. 2022].

Naccache, D., Bauer, F.L., Cankaya, E.C., Elliott Bell, D., Kaliski, B., Canteaut, A., Aaron Estes, C., Millen, J.K., Sunar, B., Möller, B., Kaliski, B., Subramanian, N., Cavoukian, A., Stoianov, A., Vijaya Kumar, B.V.K., Scotti, F., Cimato, S., Sassi, R., Kryszczuk, K. and Richiardi, J. (2011). Biba Integrity Model. *Encyclopedia of Cryptography and Security*, [online] pp.81–81. Available at: https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_774 [Accessed 29 Mar. 2020].

uk.rs-online.com. (n.d.). *RS PRO Grey Slotted Panel Trunking - Open Slot, W25 mm x D25mm, L2m, PVC | RS Components*. [online] Available at: https://uk.rs-online.com/web/p/cable-trunking/3011924?cm_mmc=UK-PLA-DS3A-_-google-_-PLA_UK_EN_Cables_%26_Wires_Whoop-_-Cable+Trunking_Whoop+(2)-_-3011924&matchtype=&pla-300917485362&gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X1MwJiohSzsDgwWsGe1Y-6KORrSTWruPkD2Rv0REyl7afC-V1EXEQ4aAngMEALw_wcB&gclsrc=aw.ds [Accessed 8 Apr. 2022].

www.amazon.co.uk. (n.d.). *Cisco ASA 5525-X Firewall Edition Adaptive Security Appliance with 8 GE Copper Ports : Amazon.co.uk: Computers & Accessories*. [online] Available at: https://www.amazon.co.uk/Cisco-Firewall-Adaptive-Security-Appliance/dp/B007J3BW8U/ref=sr_1_4?crid=3B2MWG60WOLQK&keywords=asa+firewall&qid=1649464706&s=computers&sprefix=asa+firewall%2Ccomputers%2C78&sr=1-4 [Accessed 9 Apr. 2022].

www.amazon.co.uk. (n.d.). *D-Link DES-1024D/B 24-Port Fast Ethernet Unmanaged Metal Desktop Switch - UK Version : Amazon.co.uk: Computers & Accessories*. [online] Available at: https://www.amazon.co.uk/D-Link-Ethernet-Unmanaged-Desktop-Rackmount/dp/B0001JZVDG/ref=sr_1_5?crid=QX4UDCN3PANM&keywords=24+port+dlink+switch&qid=164946529

6&s=computers&sprefix=24+portdlink+switch%2Ccomputers%2C69&sr=1-5 [Accessed 9 Apr. 2022].

www.amazon.co.uk. (n.d.). *Dell Server PowerEdge T140-3,4 GHz - E-2224-8 GB - DDR4-SDRAM - 1000 GB - Tower : Amazon.co.uk: Computers & Accessories*. [online] Available at: https://www.amazon.co.uk/Dell-EMC-PowerEdge-T140-2224/dp/B098LZTKXX/ref=sr_1_4?crid=2399OR8C4BW82&keywords=dell+server&qid=1649464308&s=computers&sprefix=dell+server%2Ccomputers%2C94&sr=1-4 [Accessed 9 Apr. 2022].

www.cablemonkey.co.uk. (n.d.). *RackyRax 600mm x 1000mm Server Cabinet | Server Cabinets from Cable Monkey*. [online] Available at: https://www.cablemonkey.co.uk/server-racks-cabinets/89936-rackyrax-600mm-x-1000mm-server-cabinet.html?ipa=827814&gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X3JSc8BSxENYUm_fM2T8UjrGSk9ZLd-JZm7WwkFY8OSXX7P5djNuf4aAvceEALw_wcB#/690-roof_fans-no_fan_unit/633-castors-none/2935-height-12u [Accessed 8 Apr. 2022].

www.softpanorama.org. (n.d.). *Bell LaPadula Security Model*. [online] Available at: http://www.softpanorama.org/Access_control/Security_models/bell_lapadula_security_model.shtml [Accessed 17 Mar. 2022].