COMPUTER SYSTEMS SERVICING

Software – 4RTH

Configure Client Device Setting

Pre Test 3.1

Direction: Check the procedures on how to configure client device settings. Use separate sheet of paper.

1. Set up Time and Date
2. Install Operating System
3. Set up Computer Name
4. Install and Configure Network Driver
5. Uninstall unnecessary files
6. Install MS Office
7. Back up and restore
8. Defragmentation
9. Install Antivirus
10. Set up Bluetooth Connection

Self-Check 3.1

Direction: Write True if the statement is correct and FALSE if it is not correct. Use a separate sheet of paper.

1. Client Device Settings is a way of configuring your client device by which you cannot specify client settings at a collection level.
2. On Windows 10 OS, to set up the Time and Date go to the upper left of your taskbar. 3. Setting up your Computer Name is important. This will serve as the Identity of your computer.
4. In every personal computer, it is necessary to install a network driver.
5. Assigning an IP Address must be unique.
6. The default subnet mask is, 255.255.0.0
7. In setting up Time, you cannot set time automatically.
8. In setting up the Time Zone, you could use "Philippines" for the setting.
9. Client setting on different OS are just the same.

10. In installing a network drivers, it compatibility on PC must be consider.

Configure Local Area Network

Pre–Test 3.2

Direction: Choose the letter of the correct answer and write it on separate paper.

1. Networking hardware used to connect one network device to other network devices or to connect two or more computers to share devices.

a. PC b. Ethernet Cable c. Router d. Modem

2. Type of ethernet cable used to connect two devices of the same type

a. Straight through b. Cross-over c. A and B d. None

3. Type of ethernet cable used in local area networks to connect a computer to a network hub such as a router.

a. Straight through b. Cross-over c. A and B d. None

4. A multipurpose electronic computer whose size, capabilities, and price make it feasible for individual use.

a. PC b. Ethernet Cable c. Router d. Modem

5. A group of computers and associated devices that share a common communications line or wireless link to a server.

a. PAN b. LAN c. CAN d. MAN

Self-Check 3.2

Direction: Identify what is being asked and write the answer on separate sheet of paper.

1. A multi-purpose electronic computer whose size, capabilities, and price make it feasible for individual use.
2. Networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc.
3. A group of computers and associated devices that share a common communications line or wireless link to a server.
4. Type of ethernet cable used to connect two devices of the same type
5. Type of ethernet cable used in local area networks to connect a computer to a network hub such as a router.
6. The option that you will choose to enter the assigned IP Address.
7. Encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.
8. The first thing to do if you will configure Local Area Network
9. The settings that you have to turn on before setting up the network connections.
10. How will you if you successfully configured a workgroup?

Activity Sheet 3.3

Direction: Locate the given words in the grid, running in one of eight possible directions horizontally, vertically, or diagonally. Copy and the answer on separate sheet of paper.

N	N	W	H	E	L	I	P	R	J	W	V	L	F	P
H	M	D	L	Z	D	V	P	C	E	C	B	Y	Y	A
V	E	B	E	U	Y	H	A	A	C	T	V	D	G	G
U	A	N	T	K	C	W	C	O	D	Y	U	O	Q	E
C	I	X	H	L	U	Q	M	P	R	D	H	O	X	U
A	C	C	E	S	S	P	O	I	N	T	R	M	R	C
P	S	H	R	W	U	W	I	F	I	X	G	E	Q	L
Q	S	I	N	T	I	E	R	B	Q	A	D	D	S	Z
X	H	E	E	L	F	S	J	U	K	I	Z	O	R	S
W	A	R	T	D	R	O	W	S	S	A	P	M	C	F

- access point
- cable
- computer
- WIFI
- modem
- ethernet
- IP address
- router
- DHCP
- password

Self-Check 3.4

Direction: Rearrange the given steps on how to configure WAN. Write the correct sequence of steps by using numbers 1-10 in separate sheet of paper.

1. Change the default user name and password
2. Set up a security key (password) for your network
3. Select Set up a new connection or network.
4. Securing your wireless network
5. Select the Start button, look for Control Panel and click Network and Internet.
6. Look for Network and Sharing Center.
7. Positioning the wireless router
8. Select Set up a new network, and then choose Next.
9. Setting up the modem and Internet connection.
10. We Need To Check Whether You Have A Wireless Adapter

Activity Sheet 3.4

Materials:

Bond Paper : Coloring Materials :
Pencil : Ruler :

Instruction:
1. Draw your desired one-story house plan. Then, put your wireless router somewhere where you think it will receive the strongest signal with the least amount of interference.
2. Write a short explanation below the house plan why did you place the router in that position.

Performance Criteria

Criteria	4	3	2	1
House plan	The plan is completed with very good effort and attention to details.	The plan is done with good effort and less attention to details.	The plan is completed with minimal effort and no attention to details.	Unable to create a clear plan and the work is somewhat careless.
Following activity direction	All directions were followed	Most of the directions were followed	Some directions were followed	None of the directions were followed
Visual Clarity and Appeal	The project had an excellent design and layout. It was neat and easy to understand the content.	The project had a nice design. It was neat and easy to read.	The output needed improvement in design, layout and neatness.	The output needed a significant improvement in design, layout and neatness.
Explanation	A complete response with a detailed explanation	Good solid response with clear explanation	Explanation was unclear	Missed key point
Required Elements	All of the required elements were clearly visible, organized and well placed	Most of the required elements were clearly visible, organized and well placed.	Few of the required elements were clearly visible, organized and well placed	Missing most or all of the required elements

Self-Check 3.5

Direction: Write SECURITY if the statement is correct and VIRUS if it is not correct. Use a separate sheet of paper.
1. A firewall is hardware or software that can help protect your PC from unauthorized users or malicious software (malware).

2. Running a firewall on each PC on your network won't help control the spread of malicious software on your network.
3. In order to provide the security you need, the Windows Firewall has a standard set of inbound and outbound rules.
4. These rules can't be configured so that they are specific to: computers, users, programs, services, ports or protocols.
5. In the Windows Firewall with Advanced Security, you can access all rules and edit their properties.
6. Connection security rules are used to secure traffic between two computers while it crosses the network.
7. Monitoring section shows only the active rules for the current network location.
8. Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.
9. Windows Firewall with Advanced Security is a tool which gives you detailed control over the rules that are applied by the Windows Firewall.
10. Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device.

Activity Sheet 3.5

Direction: Complete the crossword by filling in a word that fits each clue below the puzzle. Use a separate sheet of paper for the answers.

Across

1. Data being transported on a network

3. Setting where you can find the Windows

Firewall

5. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured 6. Filter traffic passing from the local computer to the network based on the

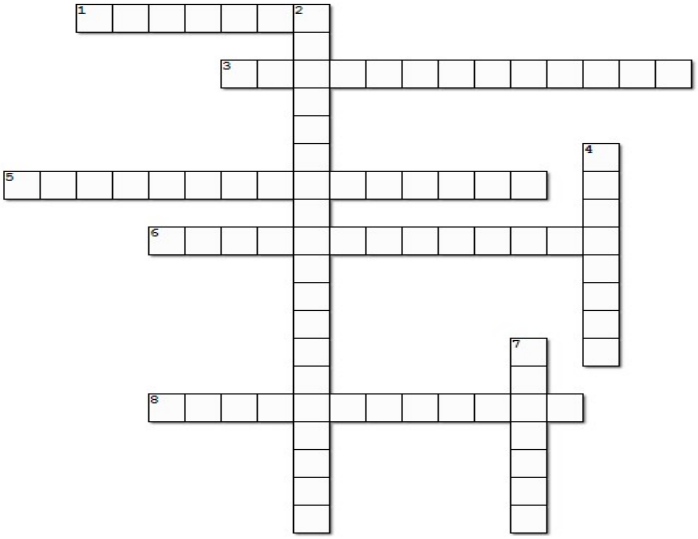
filtering conditions specified in the rule

8. Filter t raffic passing from the network to the local computer based on the filtering conditions specified in the rule.

Down

2. Used to secure traffic between two computers while it crosses the network.

4. Hardware or software that can help protect your PC from unauthorized users or malicious software 7. Any software intentionally designed to cause a damage to a computer,



Self-Check: 3.5

Direction: Identify what is being described in statement. Write the answer on separate sheet of paper.

1. It provides you with a complete product that is run and managed by the service provider.
2. Combine public and private clouds, bound together by technology that allows data and applications to be shared between them.
3. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space.
4. One in which the services and infrastructure are maintained on a private network.
5. All hardware, software, and other supporting infrastructure is owned and managed by the cloud provider.
6. Removes the need to manage underlying infrastructure (Usually hardware and operating systems), and allows you to focus on the deployment and management of your applications.

7 – 8 Give 2 characteristics of Cloud Computing

9 – 10 Give 2 benefits of using Cloud Computing

Pre-Test

I. TRUE or FALSE: Write **TRUE** if the statement is correct, and **FALSE** if not. Write your answer on a separate sheet of paper.

1. The use of cyber security cannot help prevents cyber-attacks, data breaches, and identity theft and can aid in risk management.
2. Cybersecurity is a set of techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access.
3. Every organization does not need to have a network security device (i.e. a firewall) to filter traffic.
4. The use of Infrastructure-as-a-Service (IaaS) allows companies to almost expand their computing resources instantly for a fraction of the cost of adding physical infrastructure internally.
5. A true SETA program is never a “one-and-done” solution.
6. Unauthorized Access, Unauthorized Deletion, and Unauthorized Modification are the three main aspects the cybersecurity is trying to control.
7. The components of the triad are considered to be the most important and fundamental components of security.
8. The CIA triad which stands for Confidentiality, Intelligence, and Availability is a design model to guide companies and organizations to form their security policies.
9. The first step is to recognize the problem that is causing the security issue, is to recognize whether there is a denial of service attack or a man in the middle attack.
10. When identifying, analyzing, and treating a cyber-attack, there are three principals that are kept in mind for various calculations. They are vulnerability, threat, and risk. **Cybercrime** is a global problem that has been dominating the news cycle. It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments. Today’s organized cybercrimes far out shadow lone hackers of the past now large organized crime rings function like start-ups and often employ highly trained developers who are constantly innovating online attacks. With so much data to exploit out there, Cybersecurity has become essential.

Self_Check:1.1

I. Identification: Identify the types of cyber-attacks by putting a ☑ the box beside the number and ☒ if it is not a type of cyber-attack. Write your answer on a separate sheet of paper.

1. Phishing
2. Networking
3. Malware
4. Rouge Software
5. Drive-By Downloads
6. Malverting
7. DDoS
8. Man in the Middle
9. Pyramiding
10. Password Attacks

Pre-Test

I. TRUE or FALSE: Write **TRUE** if the statement is correct, and **FALSE** if not. Write your answer on a separate sheet of paper.

1. Firewalls are a very basic component of any security architecture, and no business should be without them.
2. Incident and information management tools, such as security information and event management (SIEM) is not a crucial part of cybersecurity architecture.
3. Every organization does not need to have a network security device (i.e. a firewall) to filter traffic.
4. The use of Infrastructure-as-a-Service (IaaS) allows companies to almost expand their computing resources instantly for a fraction of the cost of adding physical infrastructure internally.
5. A true SETA program is never a “one-and-done” solution.

.

Self_Check: 4.2

I. TRUE or FALSE: Write **TRUE** if the statement is correct, and **FALSE** if not. Write your answer on a separate sheet of paper.

1. Every organization does not need to have a network security device to filter traffic.
2. It is important to be up to date with the latest cybersecurity information.
3. Today's attackers are fast, well-funded and organized, and they are using all the latest techniques to stay one step ahead of your security.
4. Firewalls are a very basic component of any security architecture, and no business should be without them.

5. Incident and information management tools, such as security information and event management (SIEM) is not a crucial part of cybersecurity architecture.
6. In any security architecture, there is no crucial security vulnerability.
7. A true SETA program is never a “one-and-done” solution.
8. Endpoint security agents help businesses protect individual assets on their network only when an attacker has breached external security measures.
9. The use of Infrastructure-as-a-Service (IaaS) allows companies to almost expand their computing resources instantly for a fraction of the cost of adding physical infrastructure internally.
10. Endpoint security can take many forms, including antivirus/antimalware programs and individual device firewalls.

Pre-Test

I. TRUE or FALSE: Write **TRUE** if the statement is correct, and **FALSE** if not. Write your answer on a separate sheet of paper.

1. Network inspection of outgoing data packets can help identify abnormal requests and prevent them from being completed.
2. Firewalls can never act as a final point of defense for keeping sensitive data from leaving the network by checking outgoing traffic.
3. The purpose of network inspection tools is to check all the data packets that are entering or leaving a network for signs of abnormal or malicious data.
4. Different types of firewalls do not have varying levels of impact on a network’s performance.
5. Packet Filtering Firewalls are the most basic forms of network inspection, and the oldest.
6. Next-Generation Firewalls are a catch-all term often used to describe newer network inspection devices that have specialized capabilities that may not be found in other firewall types.
7. Circuit-Level Gateways are network inspection devices that work by verifying the transmission control protocol (TCP) handshake to make certain the session is legitimate.
8. Stateful Inspection Firewalls provide a greater level of security than either of the previous two devices could alone but also have a larger impact on network performance.
9. Most network security devices now do not apply deep packet inspection and other next-gen security measures to prevent potentially malicious traffic requests from completing.
10. Application-Level Gateways are firewalls that act as a proxy between the network and the traffic source.