የሥራና ክህሎት ሚኒስቴር
Ministry of Labor and Skills

HARDWARE AND NETWORKING SERVICE LEVEL-IV

Based on November, 2023 Version-II

Wi Fi
Wireless Network
Wireless Access Point
DSL/Cable
Local Network

Module Title: Build a small wireless LAN

Module Code: EIS HNS4 M03 1123

Nominal duration: 40 **hours**

Prepared By: Ministry of Lobar and Skill

November, 2023
Addis Ababa, Ethiopia

Table of Contents

Acknowledgement

Ministry of Labor and Skills wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM)

Acronyms

WLAN	Wireless Local Area Network
2FA	Two-Factor Authentication
CMD	Command Prompt
CRC	Cyclic Redundancy Checking
IoC	Inversion of Control
LAN	Local Area Network
MLS	Managed LAN Services
SSID	Service Set Identifier
UPnP	Universal Plug and Play
VoD	video on Demand
VPN	Virtual Private Network
WAP2	Wi-Fi Protected Access 2
WEP	Wired Equivalent Privacy

Introduction to module

This module describes the performance outcomes, skills and knowledge required to build and arrange connectivity to basic wireless local area network (WLAN).

Module units

- Confirm client and equipment requirements
- Select, install and configure wireless access point
- Configure network
- Train users
- Monitor and administer wireless network

Learning objectives of the Module

At the end of this session, the students will able to:

- Install, configure and test at least two wireless access points
- Identify and resolve wireless network issues on at least two wireless local area networks
- develop and document user training material

Module Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below.
3. Read the information written in the information Sheets
4. Accomplish the Self-checks
5. Perform Operation Sheets
6. Do the "LAP test"

Unit One: Confirm client and equipment requirements

This learning unit is developed to provide the trainees the necessary information regarding the following content coverage and topics:

- Client and organizational requirements
- wireless device technical requirements
- Identifying components
- Selecting position for access point
- Cabling and power requirements

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand client and organizational requirements
- Identify wireless device technical requirements
- Identify components
- Select position for access point
- Understand cable and power requirements

1.1. Client and organizational requirements

As the organization's network grows, so does the organization's dependency on the network and the applications that use it. Network-accessible organizational data and mission-critical applications that are essential to the organization's operations depend on network availability.

To design a network that meets customers' needs, the organizational goals, organizational constraints, technical goals, and technical constraints must be identified. This section describes the process of determining which applications, network services already exist, and which ones are planned, along with associated organizational and technical goals and constraints. We begin by explaining how to assess the scope of the design project. After gathering all customer requirements, the designer must identify and obtain any missing information and reassess the scope of the design project to develop a comprehensive understanding of the customer's needs.

Assessing the Scope of a Network Design Project

When assessing the scope of a network design, consider the following:

- Whether the design is for a new network or is a modification of an existing network.
- Whether the design is for an entire enterprise network, a subset of the network, or a single segment or module..
- Whether the design addresses a single function or the network's entire functionality.

Table 1. 1 Network Design Scope Assessment

Scope of Design	Comments
Entire network	The backbone at the central office needs to be redesigned. All branch offices' LANs will be upgraded to Fast Ethernet technology.
Network layer	Introduction of private IP addresses requires a new addressing plan. Certain LANs must also be segmented. Routing must be redesigned to support the new addressing plan and to provide greater reliability and redundancy.
Data link layer	The central office backbone and some branch offices require redundant equipment and redundant links are needed. The organization also requires a campus wireless radio frequency (RF) site survey to determine mobility deployment options and equipment scope.
Scope of Design	Comments

1.1.1. Identify Required Information

Determining requirements includes extracting initial requirements from the customer and then refining these with other data that has been collected from the organization.

Extracting Initial Requirements

Initial design requirements are typically extracted from the Request for Proposal (RFP) or Request for Information (RFI) documents that the customer issues. An RFP is a formal request to vendors for proposals that meet the requirements that the document identifies. An RFI is typically a less formal document an organization issues to solicit ideas and information from vendors about a specific project.

The first step in the design process should be pre-documenting (sifting, processing, reordering, translating, and so forth) the design requirements and reviewing them with the customer for verification and approval, obtaining direct customer input, in either oral or written form. Figure 1-1 illustrates an iterative approach to developing the design requirements document.

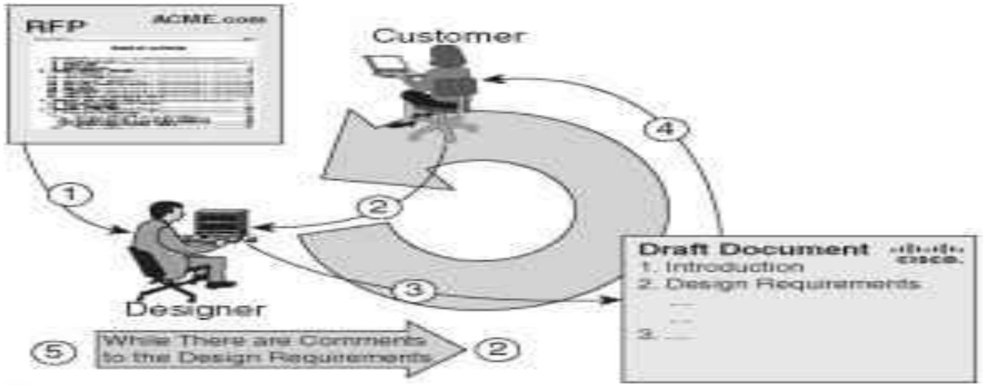


Figure 1. 1 Iterative Approach to Identifying Customer Requirements

Figure 0 illustrates the following ways:

1. Extract the initial customer requirements (from the RFP or RFI).
2. Query the customer for a verbal description of the initial requirements.
3. Produce a draft document that describes the design requirements.
4. Verify the design requirements with the customer, and obtain customer approval.

5 Revise the document as necessary to eliminate errors and omissions. 2 to 5 are repeated if the customer has additional comments about the draft document.

1.1.2. Gathering Network Requirements

As illustrated in Figure1the process of gathering requirements can be broken down into five steps. During these steps (which are sometimes called milestones), the designer discusses the project with the customer's staff to determine and gather the necessary data, including appropriate documentation.

Figure 2 Gathering Data for Design Requirements

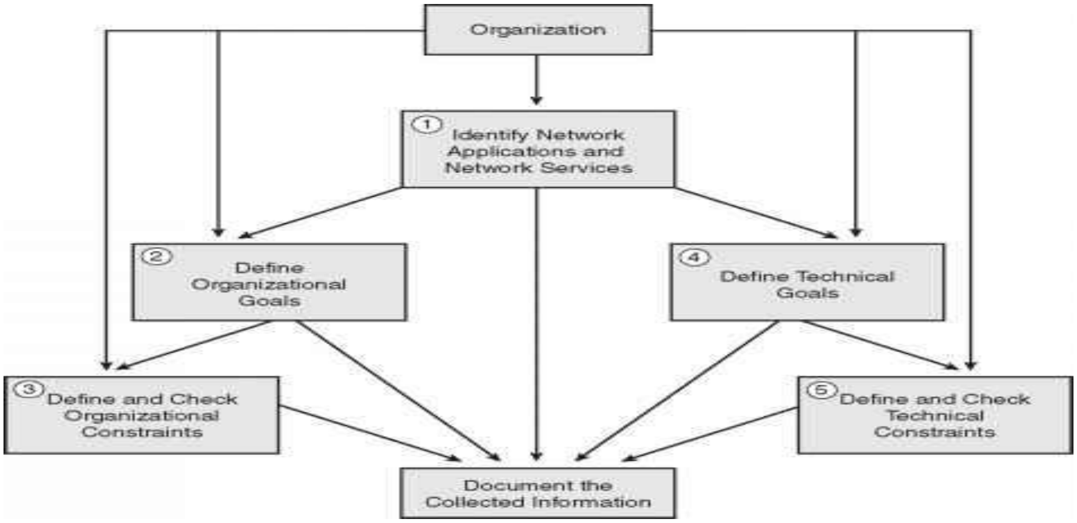

Organization
1 Identify Network Applications and Network Services
2 Define Organizational Goals
4 Define Technical Goals
3 Define and Check Organizational Constraints
5 Define and Check Technical Constraints
Document the Collected Information

Figure 1. 2 Gathering Data for Design Requirements

As shown in Figure 1.2, the steps are as follows

Step	1	Identify the planned network applications and network services.
Step	2	Determine1 the organizational goals.
Step	3	Determine the possible organizational constraints.
Step	4	Determine the technical goals.
Step	5	Determine the technical constraints that must be taken into account.

The process is not unidirectional; the designer might return to a step and make additional inquiries about issues as they arise during the design process. The next five sections detail these steps.

Planned Applications and Network Services

The designer must determine which applications the customer is planning to use and the importance of each of these applications. Using a table helps organize and categorize the applications and services planned; the table should contain the following information:

- **Planned application types:** Include e-mail, groupware (tools that aid group work), voice networking, web browsing, video on demand (VoD), databases, file sharing and transfer, computer-aided manufacturing, and so forth.
- **Applications**: Specific applications that will be used, such as Microsoft Internet Explorer, Cisco Unified Meeting Place, and so forth.
- **Level of importance**: The importance of the applications—whether critical, important, or not important is noted.
- **Comments:** Additional notes taken during the data-gathering process.

Table 1. 2 shows an example of data gathered about the planned applications for the sample company

Application Type	Application	Level of Importance (Critical, Important, Not Important)	Comments
E-mail	Microsoft Office Outlook	Important	
Groupware	Cisco Unified Meeting Place	Important	Need to be able to share presentations and applications during remote meetings
Web browsing	Microsoft Internet Explorer, Netscape Navigator, Opera	Important	
Video on demand	Cisco Digital Media System	Critical	
Database	Oracle	Critical	All data storage is based on Oracle
Customer support applications	Custom applications	Critical	

Recall that infrastructure services include security, QoS, network management, high availability, and IP multicast. Software distribution, backup, directory services, host naming, and user authentication and authorization are examples of other services and solutions that are deployed to support a typical organization's many applications. Table 1-3 shows sample data that was gathered about the infrastructure services planned for the sample company, Corporation X.

Table 1. 3 Shows an example of data gathered about the planned applications for the sample company

Service	Comments
Security	Deploy security systematically: Firewall technology to protect the internal network; virus-scanning application to check incoming traffic for viruses; intrusion detection and prevention systems to protect from and inform about possible outside intrusions. Consider the use of authentication, authorization, and accounting systems to ensure that only authenticated and authorized users have access to specific services.
QoS	Implementation of QoS to prioritize more important and more delay-sensitive traffic over less important traffic (higher priority for voice and database traffic; lower priority for HTTP traffic).
Network management	Introduction and installation of centralized network management tools (such as HP Open View with Cisco Works applications) for easier and more efficient network management.
High availability	Use redundant paths and terminate connections on different network devices to eliminate single points of failure.
IP multicast	Introduction of IP multicast services needed for the introduction of videoconferencing and e-learning solutions.
Voice	Company wants to migrate to IP telephony.
Mobility	Need mobility for employees and guest access for clients.
Service	Comments

Organizational Goals

Every design project should begin by determining the organizational goals that are to be achieved. The criteria for success must be determined, and the consequences of a failure understood.

Network designers are often eager to start by analyzing the technical goals before considering the organizational goals and constraints. However, detailed attention to organizational goals and constraints is important for a project's success. In discussions about organizational goals, the designer obtains knowledge about the customer's expectations of the design's positive outcomes for the organization. Both short- and long-term goals should be identified.

This is an opportunity to determine what is important to the customer. Some sample questions a designer might ask to help determine organizational goals include the following:

- What are you trying to accomplish with this project

- What business challenges are you currently facing?
- What are the consequences of not resolving these issues?
- What is the major objective of this project?
- What is driving the change?
- What other technology projects and business initiatives will affect your group in the next two to five years?
- What skill sets does your technical staff currently have?
- What is your goal for return on investment?

Organizational goals differ from organization to organization. The following are some typical goals that commercial organizations might have:

- Increase the operation's generated revenue and profitability. A new design should reduce costs in certain segments and propel growth in others. The network designer should discuss with the customer any expectations about how the new network will influence revenues and profits.
- Shorten development cycles and enhance productivity by improving internal data availability and interdepartmental communications.
- Improve customer support and offer additional customer services that can expedite reaction to customer needs and improve customer satisfaction.
- Open the organization's information infrastructure to all key stakeholders (prospects, investors, customers, partners, suppliers, and employees), and build relationships and information accessibility to a new level.

Table 1. 4 data gathered about the organizational goals of a sample company

Organizational Goal	Gathered Data (Current Situation)	Comments	Organizational Goal	Gathered Data (Current Situation)
Increase competitiveness	Corporation Y Corporation Z	Better products Reduced costs	Increase competitiveness	Corporation Y Corporation Z
Reduce cost	Repeating tasks—entering data multiple times, time-consuming tasks	Single data-entry point Easy-to-learn applications Simple data exchange	Reduce cost	Repeating tasks—entering data multiple times, time-consuming tasks
Improve customer	Order tracking and	Introduction of	Improve customer	Order tracking and

support	technical support is done by individuals	web-based order tracking and web-based tools for customer technical support	support	technical support is done by individuals

Organizational Constraints

When assessing organizational goals, it is important to analyze any organizational constraints that might affect the network design. Some sample questions the designer might ask to help determine organizational constraints include the following:

- What in your current processes works well?
- What in your current processes does not work well?
- Which processes are labor-intensive?
- What are the barriers for implementation in your organization?
- What are your major concerns with the implementation of a new solution?
- What projects already have budget approval?
- Are other planned technology projects and business initiatives compatible with your current infrastructure and technology solutions?
- Do you have a budget for technical development for your staff?
- Are there any policies in place that might affect the project?

Typical constraints include the following:

- **Budget:** Reduced budgets or limited resources often force network designers to implement an affordable solution rather than the best technical solution. This usually entails some compromises in availability, manageability, performance, and scalability.
- **Personnel**: The availability of trained personnel within the organization might be a design consideration. Organizations might not have enough trained personnel, or they might not have enough personnel.
- **Policies:** Organizations have different policies about protocols, standards, vendors, and applications; to design the network successfully, the designer must understand these policies.

- **Schedule:** The organization's executive management must discuss and approve the project schedule to avoid possible disagreements about deadlines.

Table 1-5 Corporation X's Organizational Constraints

Table 1.5 data gathered about the organizational goals of a sample company

Organizational Constraint	Gathered Data (Current Situation)	Comments
Budget	$650,000	Budget can be extended by a maximum of $78,000
Personnel	Two engineers with college degrees and Cisco Certified Network Associate (CCNA) certifications for network maintenance; one has Cisco Certified Network Professional (CCNP) certification Three engineers for various operating systems and applications maintenance	Plans to hire additional engineers for network maintenance; need technical development plan for staff
Policy	Prefers a single vendor and standardized protocols	Current equipment is Cisco; prefers to stay with Cisco
Schedule	Plans to introduce various new applications in the next nine months	New applications that will be introduced shortly are videoconferencing, groupware, and IP telephony

Technical Goals

The technical goals of the project must also be determined before the design starts. Some sample questions the designer might ask to help determine technical goals include the following:

- What infrastructure issues exist or will exist related to your applications rollouts?
- What skill sets does your technical staff need to acquire?
- Does your current network have any performance issues?
- Which portions of your network are considered mission-critical?

The following list describes some common technical goals:

- **Improve network performance**: An increase in the number of users and the introduction of new applications might degrade network performance, especially responsiveness and throughput.
- Note Performance is a general term that includes responsiveness, throughput, and resource utilization. The users of networked applications and their managers are usually most sensitive to responsiveness issues; speed is of the essence.
- **Decrease expected downtime and related expenses**: When a network failure occurs, downtime must be minimal, and the network must respond quickly to minimize related costs.
- **Modernize outdated technologies:** The emergence of new network technologies and applications demands regular updates to and replacement of outdated equipment and technologies.
- **Improve scalability of the network**: Networks must be designed to provide for upgrades and future growth.
- **Simplify network management**: Simplify network management functions so that they are easy to use and easily understood.

Table 1-6 depicts the desired technical goals that were gathered for the sample company, Corporation X, along with their importance rating and additional comments. In this example, the designer sees that the customer places great importance on availability, scalability, and performance; this suggests that the network design should include redundant equipment, redundant paths, use of high-speed links, and so forth.

Table 1. 6. Depicts the desired technical goals that were gathered for the sample company

Technical Goals	Importance	Comments
Performance	2O	Important in the central site, less important in branch offices
Security	15	The critical data transactions must be secure
Availability	25	Should be 99.9%
Adaptability (to new technologies)	1O	
Scalability	25	The network must be scalable
Manageability	5	

Technical Constraints

- Network designers might face various technical constraints during the design process. Some sample questions the designer might ask to help determine technical constraints include the following:
- How do you determine your technology priorities?
- Do you have a technology refresh process?
- What urgent technical problems require immediate resolution or mitigation?
- Do you have a plan for technical development for your staff in specific areas?
- Do any applications require special network features (protocols and so forth)?

Good network design addresses constraints by identifying possible trade-offs, such as the following:

- **Existing equipment:** The network design process is usually progressive; legacy equipment must coexist with new equipment.
- **Bandwidth availability:** Insufficient bandwidth in parts of the network where the bandwidth cannot be increased because of technical constraints must be resolved by other means.
- **Application compatibility**: If the new network is not being introduced at the same time as new applications, the design must provide compatibility with old applications.
- **Lack of qualified personnel:** Lack of qualified personnel suggests that the designer must consider the need for additional training; otherwise, certain features might have to be dropped. For example, if the network proposal includes the use of IP telephony but the network administrators are not proficient in IP telephony, it might be necessary to propose an alternative solution.

Table 1-7 presents sample technical constraints gathered for Corporation X. Under existing equipment, the designer notes that the coaxial cabling in the LAN's physical cabling plant still exists and comments that twisted pair and fiber optics should replace it. The bandwidth availability indicates that the WAN service provider does not have any other available links; the organization should consider changing to another service provider. Application compatibility suggests that the designer should take care when choosing equipment

Table 1.7.Technical Constraints for

Technical Constraints	Gathered Data (Current Situation)	Comments
Existing equipment	Coaxial cable	The cabling must be replaced with twisted pair to the desktop, and fiber optics for uplinks and in the core
Bandwidth availability	64-kbps WAN link	Upgrade bandwidth; change to another service provider because the current one does not have any other links to offer
Application compatibility	IP version 6 (IPv6)-based applications	New network equipment must support IPv6

1.1.3. Assigning appropriate authority

The importance of wireless network security cannot be understated. With the proliferation of mobile devices and the popularity of public Wi-Fi hotspots, the potential for data breaches and other cyber security threats has increased exponentially.

While there are many different steps that can be taken to secure a wireless network, these 12 best practices are essential for ensuring that your data and devices are safe from malicious actors

Enabling Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security to the login process. It requires users to enter both a username and password, as well as a code that is generated by an authenticator app. This makes it more difficult for someone to gain unauthorized access to the network.

Using A Strong Password

Using a strong password is one of the most important best practices for wireless network security. A strong password is at least eight characters long and includes a mix of upper- and lower-case letters, numbers, and symbols. Passwords should be changed regularly to ensure that they remain secure.

Encrypting Data

Encrypting data is another important best practice for wireless network security. Data encryption scrambles data so that it can only be decrypted and read by authorized users. This helps to protect sensitive information from being accessed by unauthorized individuals.

Disabling SSID Broadcast

Disabling SSID broadcast is another best practice for wireless network security. When SSID broadcast is enabled, it allows anyone within range of the wireless network to see the network's name. You can disable SSID broadcast by accessing the wireless router's configuration page and disabling the SSID broadcast feature.

Using MAC Filtering

Using MAC filtering is another best practice for wireless network security. MAC addresses are unique identifiers assigned to devices that connect to a network.

Enabling WPA3 Security

Enabling WPA3 security is another best practice for wireless network security. WPA3 is the most recent and most secure wireless security protocol. It provides stronger protection than WPA2 and should be used whenever possible.

Using A VPN

Using a VPN is another best practice for wireless network security. A VPN encrypts all traffic between a device and the VPN server, making it more difficult for someone to eavesdrop on the connection. This is especially important when using public Wi-Fi networks, as they are often less secure than private ones.

Disabling Remote Administration

Disabling remote administration is another best practice for wireless network security. When remote administration is enabled, it allows anyone with the proper credentials to access the router's configuration page and make changes to the network. This can be a security risk, as it allows unauthorized individuals to potentially gain access to the network.

Changing the default password

Changing the default password is another best practice for wireless network security. Many routers come with a default password that is easy to guess. This can be a security risk, as it allows unauthorized individuals to potentially gain access to the network..

Using a Firewall

Using a firewall is another best practice for wireless network security. A firewall helps to protect the network by blocking incoming traffic that is not authorized. This can be especially important in preventing attacks from malware and other malicious software.

Disabling UPnP

Universal Plug and Play (UPnP) is a protocol that allows devices to automatically discover and connect to each other. This can be a security risk, as it allows unauthorized devices to potentially gain access to the network. To disable UPnP, access the wireless router's configuration page and disable the feature. You can also disable UPnP on individual devices by accessing the settings menu.

Disabling Unnecessary Services

You often find that routers come with a number of unnecessary services enabled. These can be a security risk, as they can provide potential attackers with information about the network. To disable unnecessary services, access the wireless router's configuration page and disable any services that are not needed. This will help to reduce the attack surface of the network. Common unnecessary services include things like telnet, SSH, and HTTP.

1.2.Wireless device technical requirements

1.2.1 Define Wireless Network Requirements

Requirements define what the wireless network must do, which provides the foundation for the design. Requirements for a wireless network include needs, such as signal coverage in all elevators and support for voice telephony. Leave the technical details, such as specific technologies (such as 2.4GHz vs. 5GHz 802.11n), components, and configuration settings to the designers after all requirements are well-defined and agreed upon.

Requirements to consider

Before implementing a wireless network, consider the following types of requirements:

a. **Applications**.

Ultimately, the wireless network must support user applications, so be sure to fully define them in the requirements. This could be general office applications, such as web browsing, email, and file transfer, or it could be wireless patient monitoring in a hospital or voice telephony in a warehouse. Be as specific as possible. The application requirements enable designers to specify applicable throughput, technologies and products when designing the system.

b. **Environment**.

Provide a description of the environment where the wireless network will operate. For buildings, include the floor plan, type construction, and possible locations for mounting access points. For outdoor areas, include satellite images, aerial photographs, or drawings. Walk through the areas to verify accuracy of these items. Take lots of photos. In addition to a visible inspection, consider performing a RF site survey. All of this will capture the environment in a way that will help designers choose the right technical elements.

c. **Coverage areas**.

This describes where users will need access to the wireless network. They might only need connectivity in their offices and conferences rooms, but they may also need connectivity inside power utility rooms and the cafeteria. Also, carefully think about whether coverage is needed in stairwells, elevators, and parking garages. These are difficult-to-cover areas and can drive the cost of the wireless network very high. By properly specifying coverage area, you'll avoid the unnecessary expense of installing access points where they're not needed. Unless obvious, also identify the country where the wireless network will operate. This impacts channel planning and product availability.

d. **End users**.

Be sure to identify whether users are mobile or stationary, which provides a basis for including enhanced roaming in the design. Mobile users will move about the facility and possible roam across IP domains, creating a need to manage IP addresses dynamically. Some users, however, may be stationary, such as wireless desktops.

e. **Client devices**.

You should specify the client devices (and existing client radios) to ensure the solution accommodates them in the most effective manner. For example, you could specify that users will have laptops running Microsoft Vista operating system with integrated 802.11b/g radios. This provides a basis for deciding on the type of client radios to specify for other client devices during the design and whether there is a need to support legacy devices (i.e., 802.11b/g).

f. **Existing infrastructure**.

Be certain to describe all existing applicable infrastructure. Identify locations and availability of communications closets, switch types and available ports, PoE interfaces, fiber runs, conduit, authentication servers, VPN ports, and operational support systems.

g. **Security**.

Describe the sensitivity of the information that will traverse the wireless network. If possible, cite existing corporate wireless security policies. You will likely need to require encryption and authentication of all client devices. Be sure to give security requirements plenty of thought so that you design a solution that will protect the company's valuable resources.

h. **Funding**.

The requirements stage of a wireless network project is a good time to ask how much money is available. If funding limits are known, then you will know how much there is to work with when designing the system. In most cases, however, a company will ask how much the system will cost. You will then need to define the requirements and design the system before giving a cost estimate. In this situation, consider stating requirements with options, such as with and without signal coverage provided in parking garages. You can then provide two separate cost estimates based on optional signal coverage.

i. Schedules.

Of course, a company will generally want the wireless network installed "yesterday," but we all know that is impossible. You will need to nail down a realistic completion date, though, and plan accordingly. For example, you may be defining requirements in July, and a retail store will likely demand that a wireless price marking application be installed by the end of September.

After defining these elements, you should have enough information to design the solution. Before proceeding, though, ensure you have consensus from all stakeholders, such as executives, users, and the operational support organization. If requirements are not clear enough, you should do some prototyping or pilot testing to fully understand requirements before spending money on the design and installation.

1.3.Identify components to be installed to meet the technical requirements

Technical requirements are important because they describe how software should function and what its behavior should be. This helps developers and users to understand the best way to use the software. A document of clearly defined specifications helps to create a project or software that has a proper process for implementation. Developers and other technicians refer to this as technical requirement documentation.

Technical requirements vary depending on the product or industry. However, there is no all-encompassing list of technical requirements that apply to every project or development here is a sample list of technical requirement examples:

- Accessibility
- Authentication and authorization
- Availability
- Information security
- Maintainability
- Performance
- Privacy
- Reliability

1.4.Selecting appropriate position for access point

Wireless Access Point (WAP) placement is an important aspect of setting up and maintaining a wireless network. Proper placement of WAPs ensures good coverage, capacity, and performance. Here are some best practices for WAP placement:

A. **Conduct a site survey:** Before installing any WAPs, conduct a Wireless site survey to identify areas with poor coverage, high demand, and potential sources of interference. This will help you to determine the optimal location for each WAP.

B. **Use ceiling-mounted WAPs:** Ceiling-mounted WAPs provide better coverage than wall-mounted WAPs, as they can reach a wider area and provide more uniform coverage.

C. **Place WAPs in the center of the coverage area:** In general, WAPs should be placed in the center of the area they are supposed to cover, as this will ensure good coverage for the entire area.

D. **Avoid physical obstructions:** Physical obstructions such as walls, ceilings, and furniture can interfere with wireless signals, so it’s important to avoid placing WAPs near these types of obstructions.

E. **Use multiple WAPs:** In large areas, it’s important to use multiple WAPs to ensure good coverage and capacity. This will also help to reduce the risk of congestion and ensure that users have a good experience.

F. **Use Power over Ethernet (PoE):** PoE allows WAPs to receive power over the same cable that carries the network data, making it easy to install them in a variety of locations.

G. **Use wireless planning tools:** wireless planning tools can help to predict coverage, capacity, and performance of wireless networks, by simulating the environment and giving you an idea of how the wireless network will perform.

1.4.1 Access Point Placement Guidelines for Successful Installation

In order to build a wireless network infrastructure, a company needs to consider the placement of multiple access points around their campus. Access points connect to a wired network and allow devices to connect to that network via the access point wirelessly. They are the cornerstone of wireless networking; as such, knowing how to properly install them is essential. Physical access point placement plays a huge part in this installation process.

Access points must be placed in strategic locations in order to provide maximum coverage. Depending on the size, shape, and needs of every area of your infrastructure, your team will need to install access points at different locations. This is true for companies of any size, from SMBs to enterprises. To help your business learn the proper methods of access point placement, we have outlined five guidelines for you to follow when installing access points.

1. **Place access points where Wi-Fi will be used the most**

The first rule of proper access point placement is to determine the locations where Wi-Fi networks will be used the most. This seems like it should be obvious, but it makes a huge difference in determining the optimal placement of access points across an infrastructure. The closer a device is to an access point, the better its connection will be.

2. **Precise access point placement is key**

Access point placement is not just about picking the right general area to install a device. You also need to consider the precise physical placement for the access point in each room/location you need to service. Access points need to be built in optimal locations to provide the best signal strength to the areas it will cover.

3. **Avoid coverage overlap whenever possible**

When designing your wireless infrastructure, you need to select the best access point locations that will provide maximum coverage for your business. The simple answer to this problem is installing access points anywhere you can, but this is almost always a bad idea. Not only does this introduce unnecessary costs, but it also generates a lot of coverage overlap.

4. **Electronic devices**

Devices that emit electromagnetic signals, such as microwaves, are notorious for completely blocking wireless signals. Whenever possible, access points should be placed as far away from these devices as possible.

5. **Building materials**

The building materials of the structures your business operates in can cause varying degrees of wireless signal interference or blockage. Concrete, brick, and other dense materials are infamous for blocking Wi-Fi signals. Your team should place access points in areas that provide the best area of coverage when considering the building materials around it.

1.5.Cabling and power requirements

Wireless cabling, also known as wireless connectivity or wireless networking, refers to the transmission of data or information between devices without the need for physical cables or wires. Instead, wireless communication technologies such as Wi-Fi, Bluetooth, or cellular networks are used to establish connections.

When it comes to power requirements, wireless devices typically require a power source to operate. The specific power requirements can vary depending on the device and its intended use. Here are a few common examples:

1. **Wireless Routers:** Wireless routers, which provide Wi-Fi connectivity, are usually powered by connecting them to a standard electrical outlet. They require a continuous power source to function and transmit wireless signals.

2. **Wireless Access Points**: Similar to routers, wireless access points are devices that provide wireless connectivity in a specific area or location. They may be powered through an electrical outlet or, in some cases, through Power over Ethernet (PoE) technology, which allows both data and power to be transmitted over the same Ethernet cable.
3. **Wireless Cameras**: Wireless security cameras or other types of wireless cameras may be powered by batteries or by connecting them to an electrical outlet. Battery-powered wireless cameras are often designed for flexibility and portability, while those connected to an outlet can provide continuous power.

4. **Wireless Devices**: Various wireless devices, such as smartphones, tablets, and laptops, have built-in batteries that power their wireless capabilities. These devices need to be periodically recharged to maintain their wireless functionality.

Self-check 1

Part-I choose the best answer for the given alternative.

_______1. Which one are best practices for WAP placement:

A. Conduct a site survey C. Place WAPs in the center of the coverage area

B. Use ceiling-mounted WAPs D. All

_______2. __ is refers to a technical requirement that seeks to make a service, software or technology accessible to all users and parties

A. Authentication and authorization C. Availability

B. Accessibility D. Non

________3. Before implementing a wireless network you should consider______

A. End users. C. Coverage areas.

B. Environment. D. all

_______4. Which one is under Technical Constraints

A. Existing equipment B. Bandwidth availability C. Application compatibility D all

_______5. __________refers to the average time that a system or software operates between downtimes or failures

A. Privacy B. Accuracy C. Reliability D. Integrity

Part-II Give short answer

1. Describes some common technical goals that were gathered for the sample company
2. When assessing the scope of a network design, what you should be consider
3. List the step that are used to Gathering Network Requirements

Unit Two: Install and configure wireless access point

This learning unit is developed to provide the trainees the necessary information regarding the following content coverage and topics:

- Selecting access point device
- Installing and configure access points
- Configuring services
- Testing access point for connection and security
- Upgrading legacy equipment

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Select access point device
- Install and configure access point
- Configure services
- Testing access point for connection and security
- Upgrading legacy equipment

2.1. Selecting access point device

What is a wireless access point?

A wireless access point is a device used to create a WLAN. Businesses in large offices or buildings often use wireless access points. This device is connected to an internet hub, wired router, or switch using an Ethernet cable. Then project the Wi-Fi signal to the designated area. It is best to understand your business needs before you make a choice. Consider some of the above, or ask an expert for recommendations. Router-switch–your professional IT provider.

Things to Consider

As more and more enterprises upgrade their wireless network environment, people also have doubts about choosing a wireless access point. When choosing a wireless access point, keep the following points in mind.

1. **Range**

The range that an AP can cover is an important parameter, and a WAP with a larger coverage area is more beneficial. Because it means the number and cost of access points can be reduced. Purchasing WAPs with additional coverage areas can reduce costs for businesses. Most enterprise wireless access points are capable of covering an area of 5,000 to 10,000 square feet.

2. **Speed**

The rate at which information travels is also something we need to consider, usually measured in bps (bits per second), kilobits, megabits, or gigabits. In general, if the exact 802.11n protocol is supported, wireless AP speeds can reach 300Mbps or higher, six times faster than 802.11n. The WAP that supports the 802.11ac protocol can reach 1200Mbps.

3. **Gain Antenna**

The antenna of the wireless AP is basically built-in, it is not external like the antenna of the router. The antenna of the wireless AP is very important, it will directly affect the signal strength and transmission range of the wireless AP. When buying a wireless AP, it is best to choose one with a booster antenna.

4. **Guest Access**

Data breaches and other cyber security issues are happening every day now. When people use their phones and computers over the Internet, security issues are not expected. Modern systems have intelligent guest access systems that apply corporate security policies. This ensures that guests stay safe on the network. Also, there is no need to worry about access from unsecured devices.

5. **No Hardware Controllers**

In the past, access points also required IT technicians with specialized knowledge to operate from a computer. However, with the advancement of technology, these are no longer necessary. The latest Wi-Fi 6 access points, for example, use software control in the network and do not require an external controller. Software-based control has many benefits over previous hardware-dependent access points.

6. **Wi-Fi Technology**

Choose devices using MESH, MIMO and POE access point technologies based on your business needs. MESH technology can be used in home and commercial equipment. POE technology adopts low-power cabling technology and can transmit signals up to 100M.

7. **Price**

It is not that the higher the price, the better the AP. Sometimes the high price will not only increase the cost, but also cause waste of product function and performance. Too low a price can tempt people to buy inferior or counterfeit products.

2.2. Installing and configure access points

Wireless devices (also known as access points) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. When configured as an access point, the wireless device serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

Here we are providing an example of how to configure a wireless access point (a DLink access point, in this case). Please take the following technics:

1. Change the default admin password.

2. Change the default SSID to something of your choosing.

3. Enable encryption.

4. Disable the DHCP Server function, if your access point has this feature.

5. Register the hardware (MAC) address of your wireless card. With these steps taken, you should have no problem connecting securely to your wireless access point.

The Wireless Access Point (WAP) is a networking devices that enables the capability for wireless-capable devices to connect to a wired network. Introducing a WAP to your existing wired network is instrumental to accommodating those devices only capable of wireless connection. I have not come across a smartphone with an RJ45 port yet and so it is only appropriate that I consider the connectivity capability of the end user device. It is like creating or deploying another network purely for wireless devices but still an essential part of your existing wired network such as the diagram displayed below in this wireless access point setup diagram.

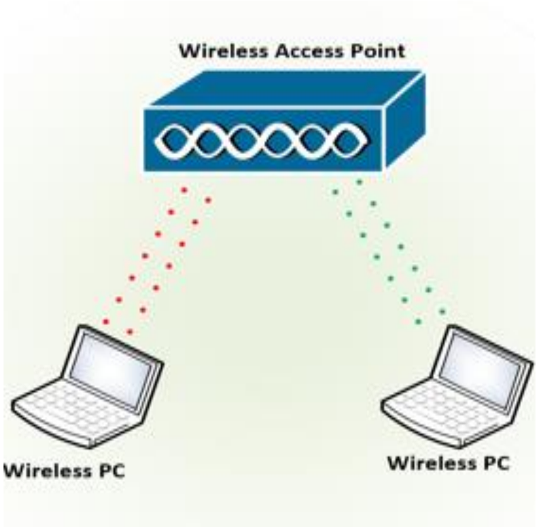


Figure 2. 1 Wireless Access Point

Wireless devices (also known as access points) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. When configured as an access point, the wireless device serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network

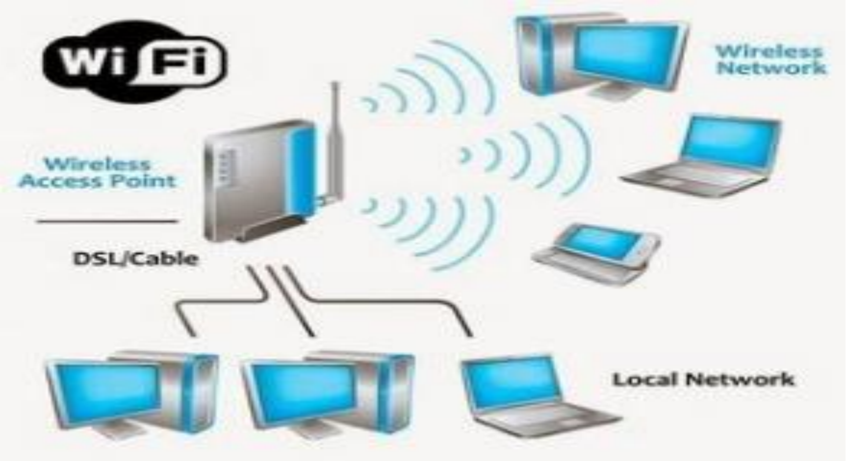


Figure 2.2. Wireless Access Point (WAP)

In the network, diagram displayed above Figure 2.2 how to connect a Wireless Access Point to a Wired Network; you can see clearly two portions of networks. One being a wired network and the other being a wireless network. The wired network consists of three wired computers to a switch, which is connected to a router. The wireless network in the right portion shows three wireless computers connected to a wireless access point (WAP). Since the objective of this post is to show you how to connect a wireless access point to a wired network.

2.3. Configure Services

The Configure Services method is a place where you can register your dependent classes with the built-in IoC container. After registering dependent class, it can be used anywhere in the application. You just need to include it in the parameter of the constructor of a class where you want to use it. The IoC container will inject it automatically.

ASP.NET Core refers dependent class as a Service. So, whenever you read "Service" then understand it as a class, which is going to be used in some other class.

2.1.1 What are Managed LAN Services?

Managed LAN Services (MLS) is a term used to describe a service provided by a third party service provider to manage a company’s local area network (LAN). This type of service provides remote monitoring and maintenance of the company’s network infrastructure.

This type of service allows companies to reduce their IT costs and increase productivity. The main advantage of MLS over other solutions is its ability to provide 24/7 support and proactive monitoring. It also offers an easy way to access your network remotely.

A Local Area Network (LAN) is a high-speed communication system. It allows users to share information and connect to other computers and peripherals. A LAN is usually connected to a server via a router. Some types of LANs are wireless while others are wired.

Your company may already have an existing LAN, or you might need to create one. You will need to buy equipment such as switches, routers, and hubs. Depending on the size and type of your network, you might also need to purchase servers, printers, fax machines, and modems.

If you want to use a managed LAN service, you should contact a local IT service provider who specializes in these kinds of services. They will be able to help you decide which kind of managed LAN service is right for you.

2.1.2. Benefits of Using Managed LAN Services?

- **Security:** A managed LAN services provider can secure your network by installing firewalls, intrusion detection/prevention systems, and other security products.
- **Network Monitoring:** A managed LAN services company can monitor your network 24 hours a day, seven days a week. It can alert you when there are problems with your network.
- **Improved Network Performance:** managed LAN service providers usually offer faster speeds than you could get from a public Internet access point. You won't have to wait as long to download large files.
- **Cost Savings:** Managed LAN service providers offer lower rates than you would pay for similar services.
- **Reliability:** Most managed LAN service providers guarantee 99% uptime. If they fail to deliver this level of reliability, they will reimburse you for the downtime.
- **24-Hour Availability:** Most managed LAN service providers offer 24-hour availability. If an issue arises, they will resolve it immediately.
- In conclusion, managed LAN services are beneficial because they help improve your business's productivity and save you money by reducing the cost of maintaining your network infrastructure.

2.4. Testing access point for connection and security

When planning the testing of a WLAN, consider the following forms of testing:

- **Signal coverage testing**: Signal coverage testing determines where client devices are able to satisfy coverage requirements. This testing may be part of performing a WLAN site survey or done after the network is installed to determine the as-installed signal coverage
- **Performance testing:** Performance testing determines whether the WLAN can satisfy user needs for using specific applications over the WLAN.
- **In-motion testing**: In-motion testing determines whether users can continue to make use of applications while roaming throughout the coverage areas, especially when the roaming requires handoffs between access points.

- **Security vulnerability testing**: Security vulnerability testing ensures that the WLAN implements required security mechanisms and offers sufficient protection to unauthorized access and passive monitoring.
- **Acceptance/verification testing**: After installing a WLAN, it is important to run a series of acceptance/verification tests to ensure that the WLAN satisfies all requirements. This is especially important if the organization is having a contractor install the WLAN.
- **Simulation testing**: In some cases, such as when implementing a very large WLAN, it may be beneficial to simulate the behavior of the WLAN before actually installing it. This can provide helpful feedback when designing the system, especially if the WLAN will have critical performance requirements.
- **Prototype testing:** Prototype testing involves implementing an individual function of the WLAN that is not well understood before deploying the complete system. For example, an organization may not be very familiar with 802.1X authentication systems and may benefit by implementing the 802.1X authentication in a lab environment with a limited number of test client devices.
- **Pilot testing:** Before installing the WLAN across the entire organization, which may include numerous buildings and different applications, it is strongly advisable to install the system in a limited number of facilities (ideally one) and make that one work effectively first. After you work out all the problems, you can install the WLAN at the remaining location without the need for extensive rework because the problems will likely have been solved during the pilot testing.

2.5. Upgrading legacy equipment

Our client, an iconic manufacturing company in Romania, faced challenges in managing traditional manufacturing equipment that was individually connected to dedicated hardware. In order to improve operations, it was necessary to integrate a modern and functional ICT system with optimized monitoring. We also needed to provide staff with the necessary training to operate the new system effectively.

Together with the client company, we defined the following ICT priorities:

- Networking of legacy production equipment
- Moving from a fragmented, sub-optimal network to an integrated management system;
- Upgrading the ICT system;

- Implementation of new work processes and communications;
- Training users on the new ICT system;
- Consultancy to executive management on ICT system optimizations;
- Infinilink full responsibility for the ICT system.

Networking of legacy production equipment running specific software from multiple third-party industry vendors:

Each vendor has its own communication protocols and standards, which can make it difficult to integrate equipment into a single system. This solution required detailed knowledge of industry protocols and communication standards, as well as the ability to develop custom software solutions to integrate legacy equipment into the new system.

The existing client-company network was sub-optimal and fragmented, making it difficult to effectively manage, design and implement new processes. The infinilink team designed and implemented an integrated management system that provides visibility and control over the entire network infrastructure, reducing complexity and fragmentation of the ICT system.

1. **Upgrading the ICT system:**

The modernization of the system required the replacement of multiple hardware and software elements, the integration of old equipment and the implementation of new systems and applications. Very important was that the entire process was carried out without interrupting ongoing operations, with minimal downtime.

Outcome: reduce downtime, improve data management and increase productivity.

2. **Implementation of new work processes and communications:**

Together with the client, we developed new processes that are compatible with the existing system and easy to adopt by the client's staff. The infinilink team worked closely with client staff to ensure that the new processes optimized efficiency and productivity of operations. **Outcome**: increase productivity, reduce errors and improve communication on operations between staff members.

3. **Training users on the new ICT system:**

The successful implementation of the new ICT system depended on the ability of the client's staff to use it. The infinilink team provided the client's employees with comprehensive training on the features and functionality of the new system, as well as on-site support to ensure staff could use the system confidently and effectively.

Outcome: increase staff confidence, reduce errors and increase productivity.

4. **Consultancy to executive management on ICT system optimizations:**

Team has identified ICT areas affecting the client's business processes that need optimization. We provide concrete recommendations to the executive management of the client company, leading to continuous improvement of system performance and efficiency.

Outcome: improve system performance, increase efficiency and reduce costs.

5. **Full ICT system responsibility for continuous support of business and production processes:**

To support business and production processes, we ensure that the system is always working optimally. We monitor system performance and take proactive measures to prevent outages and ensure continuity of operations

Outcome: reducing downtime, improving system performance and increasing productivity, with a positive effect on the quality of the client company's products.

Self-check 2

Part-II True or False

________1. The Wireless Access Point (WAP) is a networking devices that enables the capability for wireless-capable devices to connect to a wired network

________2. Improved Network Performance is one of the Benefits of Using Managed LAN Services?

________**3.** We monitor system performance and take proactive measures to prevent outages and ensure continuity of operations

________4. The Outcome of Implementation of new work processes and communications is not increase productivity, reduce errors and improve communication on operations between staff members

Part-I Multiple choose

________1. What is a wireless access point?

A. a device used to create a WLAN C. Used to generate signal
B. Is software resource D. all

________2. Why upgrading legacy equipment?

A. To improve performance C. A & B
B. To improve operations D. Non

________3. When planning the testing of a WLAN you should consider______

A. Signal coverage testing C. In-motion testing
B. Performance testing D. All

________4. Which one is not Benefits of Using Managed LAN Services?

A. Security C. Improved Network Performance
B. Increase Cost Savings D. Network Monitoring

________5. ____________is a term used to describe a service provided by a third party service provider to manage a company's local area network (LAN).

A. Managed LAN Services (MLS) C. A&B
B. Local Area Network (LAN) D. all

Operation Sheet 2.1

Operation title: Configuring a Wireless Access Point

Purpose: To **Configuring a Wireless Access Point**

Instruction: based on the given scenario perform the given step below appropriately. For this operation, you have given 40 minutes and you are expected to provide the answer.

Scenario: - The Linksys WRT300N includes an integrated 4-port switch, a router and a wireless Access Point (AP). In this lab, you will configure the AP component of the multi-function device to allow access for wireless clients. The basic wireless capabilities of the multi-function device will be configured but this will not be a secure wireless network

Tools and requirement:

- Windows 10 based computer that is cabled to the multi-function device
- Linksys WRT300N

Precautions: before starting check the resource needed

Procedures in doing the task

Step 1: Verify connectivity between the computer and the multi-function device

A. The computer used to configure the AP should be attached to one of the multi-function device's switch ports.

B. On the computer, click the Start button and select Run Type CMD and click OK or press Enter CMD and click OK or press Enter

C. At the command prompt, ping the multi-function device using the default IP address 192.168.1.1 or the IP that has been configured on the multi-function device's port. Do not proceed until the ping succeeds

D. Write down the command used to ping the multi-function device

NOTE: If the ping is not successful, try these troubleshooting steps:

- Check to make sure the IP address of the computer is on the 192.168.1.0 network. The computer must be on the same network as the multi-function device to be able to ping it. The DHCP service of the multi-function device is enabled by default. If the computer is configured as a DHCP client, it should have a valid IP address and subnet mask. If the computer has a static IP address, it must be in on the 192.168.1.0 network and the subnet mask must be 255.255.255.0.
- Make sure the cable is a known-good straight-through cable. Test to verify.
- Verify that the link light for the port where the computer is attached is lit.

- Check whether the multi-function device has power.

If none of these steps correct the problem, check with your instructor.

Step 2: Log in to the multi-function device and configure the wireless network

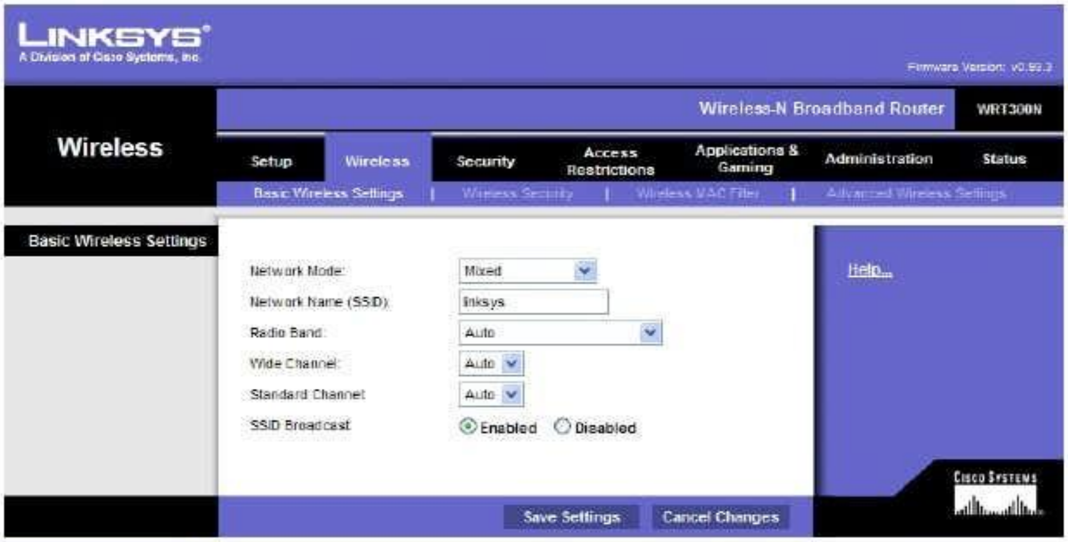
A. Open a web browser. In the address line:-

Type http: / / ip_address where IP address is the IP address of the wireless router.

Default is 192.168.1.1. At the prompt, leave the user name textbox empty, but type the password assigned to the router.

B. The default password is **Admin** Click OK

C. In the main menu, click on the Wireless option


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v0.93.3
Wireless-N Broadband Router
WRT300N
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Basic Wireless Settings
Help...
Save Settings
Cancel Changes
Cisco Systems

Network Mode: Mixed
Network Name (SSID): linksys
Radio Band: Auto
Wide Channel: Auto
Standard Channel: Auto
SSID Broadcast: ● Enabled ○ Disabled

D. In the Basic Wireless Settings window, the Network Mode Shows mixed by default, because the AP supports 802.11b, g, and n wireless devices. You can use any of these standards to connect to the AP. If the wireless portion of the multi-function device is not being used, the network mode would be set to Disabled .Leave the default of Mixed selected

E. Delete the default SSID (Linksys) in the Network Name (SSID) textbox. Enter a new SSID using your last name or name chosen by your instructor. SSIDs are case-sensitive.

F. Write down the exact SSID name that you are using.

G. Click on the Radio Band drop-down menu and write down the two options

Quality Criteria: admin client on the network

LAP Test

Instruction I: Given necessary network components or equipment’s, you are required to perform the following tasks within 40 minutes.

Task 1: Installing and configure access points

Tsk 2: Testing access point for connection and security

Unit Three: Configure network

This learning unit is developed to provide the trainees the necessary information regarding the following content coverage and topics:

- Introduction to Wireless Security Threats
- Configuring security and other key parameters
- Testing security and firewall arrangements
- Testing network compatibility and access

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Introduction to Wireless Security Threats
- Configuring security and other key parameters
- Testing security and firewall arrangements
- Testing network compatibility and access

3.1. Introduction to Wireless Security Threats

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by Internet users at home. Some of the basic technologies of wireless network systems are outlined below.

a. Wireless Local Area Network

A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices.

b. Access Point

A wireless access point (AP) is a hardware device that allows wireless communication devices, such as PDAs and mobile computers, to connect to a wireless network. Usually, an AP connects into to a wired network, and provides a bridge for data communication between wireless and wired devices.

c. Service Set Identifier

A Service Set Identifier (SSID) is a configurable identification that allows wireless clients to communicate with an appropriate access point. With proper configuration, only clients with correct SSID can communicate with the access points. In effect, the SSID acts as a single shared password between access points and clients.

d. Open System Authentication

Open System Authentication is the default authentication protocol for the 802.11 wireless standard. It consists of a simple authentication request containing the station ID and an authentication response containing success or failure data. Upon successful authentication, both stations are considered mutually authenticated.

e. Shared Key Authentication

Shared Key Authentication is a standard challenge and response mechanism that makes use of WEP and a shared secret key to provide authentication. Upon encrypting the challenge text with WEP using the shared secret key, the authenticating client will return the encrypted challenge text to the access point for verification.

f. Ad-Hoc Mode

Ad-hoc mode is one of the networking topologies provided in the 802.11 standard. It consists of at least two wireless stations where no access point is involved in their communication. Ad-hoc mode WLANs are normally less expensive to run, as no APs are needed for their communication.

g. Infrastructure Mode

Infrastructure mode is another networking topology in the 802.11 standard, in addition to ad-hoc mode. It consists of a number of wireless stations and access points. The access points usually connect to a larger wired network. This network topology can scale to form large-scale networks with arbitrary coverage and complexity.

h. Wired Equivalent Privacy Protocol

Wired Equivalent Privacy (WEP) Protocol is a basic security feature in the IEEE 802.11 standard, intended to provide confidentiality over a wireless network by encrypting information sent over the network. A key-scheduling flaw has been discovered in WEP, so it is now considered as unsecured because a WEP key can be cracked in a few minutes with the aid of automated tools. Therefore, WEP should not be used unless a more secure method is not available.

i. Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a wireless security protocol designed to address and fix the known security issues in WEP. WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption. 802.1x authentication has been introduced in this protocol to improve user authentication.

Wi-Fi Protected Access 2 (WPA2), based on IEEE 802.11i, is a new wireless security protocol in which only authorised users can access a wireless device, with features supporting stronger cryptography(e.g. Advanced Encryption Standard or AES), stronger authentication control (e.g. Extensible Authentication Protocol or EAP), key management, replay attack protection and data integrity.

TKIP was designed to use with WPA while the stronger algorithm AES was designed to use with WPA2. Some devices may allow WPA to work with AES while some others may allow WPA2 to work with TKIP. But since November 2008, vulnerability in TKIP was uncovered where attacker may be able to decrypt small packets and inject arbitrary data into wireless network. Thus, TKIP encryption is no longer considered as a secure implementation. New deployments should consider using the stronger combination of WPA2 with AES encryption.

Wi-Fi Protected Access 3 (WPA3) is a new wireless security standard built on WPA2 but brings new features to enhance Wi-Fi security for more robust authentication and enhanced cryptographic strength, while maintaining resiliency of mission critical networks. The WPA3-Personal mode utilizes the Simultaneous Authentication of Equals key establishment protocol as defined in IEEE 802.11-2016 to strengthen password-based authentication against brute-force attacks. It has a natural password selection feature to help users choose easy-to-remember and strong passwords. It also provides forward secrecy that prevents attackers who have compromised the network from decrypting data traffic already sent out before the compromise. The WPA3-Enterprise mode comes with an optional security suite that offers 192-bit level encryption instead of WPA2's 128-bit level encryption for enhanced protection of critical Wi-Fi networks handling sensitive information. WPA3 is compatible with WPA2 and more new Wi-Fi devices will support WPA3 in the years to come.

3.1.2. Security Threats and Risks Associated with Wireless Networks

Low deployment costs make wireless networks attractive to users. However, the easy availability of inexpensive equipment also gives attackers the tools to launch attacks on the network. The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions.

"Parking Lot" Attack

Access points emit radio signals in a circular pattern, and the signals usually extend beyond the physical boundaries of the area they intend to cover. Signals can be intercepted outside buildings, or even through the floors in multi-story buildings. As a result, attackers can implement a "parking lot" attack, where they actually sit in the organization's parking lot and try to access internal hosts via the wireless network.

Shared Key Authentication Flaw

Shared key authentication can easily be exploited through a passive attack by eavesdropping on both the challenge and the response between the access point and the authenticating client. Such an attack is possible because the attacker can capture both the plaintext (the challenge) and the cipher text (the response).

Service Set Identifier Flaw

Access points come with default SSIDs. If the default SSID is not changed, these units can easily be compromised. In addition, SSIDs are sent over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring network traffic. For some products, even when WEP is enabled, management messages containing the SSID will still be broadcasted in clear text by access points and clients, making it possible for an attacker to sniff SSIDs and gain access to the wireless LAN.

3.1.1. The Vulnerability of Wired Equivalent Privacy Protocol

Data passing through a wireless LAN with WEP disabled (which is the default setting for most products) is susceptible to eavesdropping and data modification attacks. However, even when WEP is enabled, the confidentiality and integrity of wireless traffic is still at risk because a number of flaws in WEP have been revealed which seriously undermine its claims to security. In particular, the following attacks on WEP are possible:

- Passive attacks to decrypt traffic based on known plaintext and chosen cipher text attacks;
- Passive attacks to decrypt traffic based on statistical analysis on cipher texts;
- Active attacks to inject new traffic from unauthorized mobile stations;
- Active attacks to modify data; or
- Active attacks to decrypt traffic, based on tricking the access point into redirecting wireless traffic to an attacker's machine.

3.1.2. The most wireless Network Threats

- Accidental Association: Overlapping networks ⇒ unintentionally connect to neighbors
- Malicious Association: Malicious access points (Free public Wi-Fi) can steal passwords.
- Ad-Hoc Networks: Two computers can exchange data
- Nontraditional Networks: Bluetooth can be used to eavesdrop
- MAC Spoofing: Change MAC address to match a privileged computer
- Man-In-The-Middle Attacks: Using rogue access point between the user and the real access point
- Denial of Service (DoS): Keep the media busy 8. Network Injection: Spoof routing/management messages

The below are a counter measurements that to reduce Wireless Network Threats

- Turn-off SSID broadcast

- Use Cryptic SSID names
- Reduce signal strength
- Locate APs away from boundary
- Use encryption
- Use IEEE 802.1x network access control
- Change the router's user ID from default
- Change the router's password from default
- MAC Filtering: Only specific MAC address connect

3.2. Configuring security and other key parameters

These sections describe the security settings that you configure, depending on your selection in the **Security** list on the Networks page.

None (Plain text)

If you select none as your security mode, no additional security settings are configurable on the WAP device. This mode means that any data transferred to and from the WAP device is not encrypted. This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key plus 24-bit initialization vector (IV)) or 128-bit (104-bit secret key plus 24-bit IV) Shared Key for data encryption.

Static WEP is not the most secure mode available, but it offers more protection than setting the security mode to None (Plain text), as it does prevent an outsider from easily sniffing out unencrypted wireless traffic.

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a stream cipher called RC4.)

These parameters configure Static WEP:

- **Transfer Key Index**—Enter a key index list. Key indexes 1 through 4 are available. The default is 1. The Transfer Key Index indicates which WEP key the WAP device uses to encrypt the data it transmits.

- **Key Length**— Choose either 64 bits or 128 bits as the length of the key.
- **Key Type**—Choose either ASCII or Hex as the key type.
- **WEP Keys**—You can specify up to four WEP keys. In each text box, enter a string of characters for each key. The keys you enter depend on the key type selected:
- **ASCII** — Includes uppercase and lowercase alphabetic letters, the numeric digits, and special symbols such as @ and #.
- **Hex** — Includes digits 0 to 9 and the letters A to F.

Shared Key authentication requires the client station to have the correct WEP key in order to associate with the WAP device. When the authentication algorithm is set to Shared Key, a station with an incorrect WEP key cannot associate with the WAP device.

Static WEP Rules

If you use Static WEP, these rules apply:

- All client stations must have the Wireless LAN (WLAN) security set to WEP, and all clients must have one of the WEP keys specified on the WAP device in order to decode AP-to-station data transmissions.
- The WAP device must have all keys used by clients for station-to-AP transmit so that it can decode the station transmissions.
- The client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but using the same key is less secure because it means one station can decrypt the data being sent by another.)
- On some wireless client software, you can configure multiple WEP keys and define a client station transfer key index, and then set the stations to encrypt the data that they transmit using different keys.
- You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Dynamic WEP

Dynamic WEP refers to the combination of 802.1x technology and the Extensible Authentication Protocol (EAP). With Dynamic WEP security, WEP keys are changed dynamically.

EAP messages are sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation over LANs (EAPOL). IEEE 802.1X provides dynamically generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

3.3. Testing security and firewall arrangements

A firewall is a vital component of an organization's security infrastructure, and it needs to be protected against exploitation. Firewalls serve as the first line of defense in network security, crucial in safeguarding your internal network from cyber threats. With hackers perpetually on the lookout for open ports and misconfigurations, the relevance of firewall testing becomes paramount. In this guide, we delve into the varied methods and tools to ensure your firewall is operating optimally.

Regular firewall testing ensures the integrity of your network, keeping malware, tunneling attempts, and hackers at bay. Always remember to check the permissions, access control list (ACL), DMZ settings, and file sharing formats to ensure that your firewall and network devices are protected.

Importance of Firewall testing

The essence of firewall testing lies in its ability to critically evaluate the functionality of your firewall. By identifying open ports, misconfigurations, or potential backdoors, you can thwart hackers. In essence, firewall testing is like auditing your network security.

Methods for Testing Firewall Security

The primary techniques for firewall security testing are penetration testing and port scanning. These methods, when executed appropriately, expose vulnerabilities, shedding light on the type of firewall's strengths and weaknesses.

Penetration Testing

Firewall penetration testing, usually undertaken by penetration testers, simulates cyber attacks on your network devices, similar to how a hacker would infiltrate systems. This form of security testing mimics actual threats, thus gauging the robustness of your firewall policy and other defenses.

Port Scanning

Port scanning is an indispensable tool in identifying open and closed ports within your internal network. Tools like Nmap, Netcat, and ShieldsUp play pivotal roles in this. Since open ports can be gateways for malware and cyber attacks, it's crucial to determine and seal any unnecessary ones.

Firewall Testing Tools

There is a plethora of tools to test firewalls. Prominent among them are Nmap, Netcat, and Shields Up. These not only assist in port scanning but also in conducting traceroute checks, creating reverse shell scenarios, and ICMP requests, crucial for advanced security testing.

How to Test Firewall Security on Windows

Windows, especially its operating system Windows 10, comes with robust built-in features for firewall testing. Microsoft’s firewall policy allows intricate customization, which can be audited using the Windows Defender Firewall with Advanced Security. Additionally, tools like Netcat can help in understanding routes, routers, and potential issues in routing.

Secure the Firewall

A firewall is a vital component of an organization’s security infrastructure, and it needs to be protected against exploitation. To secure your firewall, take the following steps:

- Disable insecure protocols like telnet and SNMP or use a secure SNMP configuration.
- Schedule periodic backups of the configuration and database.
- Enable auditing of system changes and send logs via secure syslog or another method to an external, secured, central SIEM server or firewall management solution for forensics and reporting.
- Add a stealth rule in the firewall policy to hide the firewall from network scans.
- Limit management access to specific hosts.

3.4. Testing network compatibility and access

What is Compatibility Testing?

Compatibility testing is a type of testing that examines and compares functionality over multiple browsers, devices, platforms, and OS to recognize potential discrepancies. Performing compatibility testing verifies that your product/software works efficiently in its intended environments.

What are the Benefits of Compatibility Testing?

- **Improves Software Development Process:** Compatibility test estimates the issues in the software in the SDLC itself. But, it becomes easier to verify the app’s usability, scalability, and stability across various platforms and deliver feedback.

- **Detects Bugs before Production:** A compatibility test is effective in the timely detection of bugs in web and mobile apps, even in tricky areas. Since errors are recognized before production.
- **Complete User Satisfaction:** By utilizing compatibility tests, you ensure that every portion of your product is up and performing as it should across all software, browsers, and devices.
- **Successful Launches:** One of the crucial advantages of compatibility testing, in conjunction with other testing, is that it gives an entirely successful

Self-check 3

Part I: Choose the best Answer

_______1. _________ can easily be exploited through a passive attack by eavesdropping on both the challenge and the response

A. Shared Key Authentication Flaw   C. all

B. Parking Lot" Attack   D. none

_______2. Which one is wireless Network Threats

A. Accidental Association: C. Ad-Hoc Networks

B. Malicious Association: D. All

_______3. From the following which one is a counter measurements that to reduce Wireless Network Threats

A. Turn-off SSID broadcast   C. Use encryption

B. Use Cryptic SSID names   D. All

_______4. .—is either 64 bits or 128 bits as the length of the key.

A. Key Type.   C. Key Length

B. WEP Keys   D. All

Part- II: Matching

	A	B
__1.	Service Set Identifier	A. hardware device that allows wireless communication devices,
__2.	.AD-hoc	B. identification that allows wireless clients to communicate with an appropriate access point
__3.	Wireless Local Area Network	C. a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices
__4.	Access Point	D. one of the networking topologies provided in the 802.11 standard

Part II: - Write short answer for the following question

1. List and explain basic technologies of wireless network systems?
2. What are the Benefits of Compatibility Testing?

Unit Four: Train users

This learning unit is developed to provide the trainees the necessary information regarding the following content coverage and topics:

- Devices to be connected to the network
- Demonstrating how pairing and log-on
- Traffic capacity issues
- Developing user documentation

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand devices to be connected to the network
- Demonstrate how pairing and log-on
- Understand traffic capacity issues
- Develop user documentation

4.1 Determine devices to be connected to the network

The internet and traditional mail are similar in many ways. We have a MAC address as a physical identifier rather than a home address. We have MAC addresses rather than names. Together they deliver the information to your door.

We require both, an IP address and a MAC address to establish communication between two networked devices. The TCP/IP protocol transfers data from one network to another using the IP address. The MAC address is used to route data to the correct network device.

IP Address

A device on the internet or a local network is identified by its specific IP address, which is different from other addresses. IP stands for "Internet Protocol".

Finding Out Your IP Address

You can discover your IP address in a variety of ways. The simplest method would be to enter "what is my IP address" into a search engine like Google.

For Windows users, navigate to **Start** > **Settings** > **Network & internet** and choose the Wi-Fi network you're connected to obtain your IP address. Locate your IP address next to "IPv4 address" under Properties.

MAC Address

In computer networking, the physical address that identifies each device on a given network is called the Media Access Control (MAC) address. It is also known as Physical address, hardware address, or BIA (Burned In Address). It is 12-digit and 64-bit long, the first 24 bits are utilized for the OUI (Organization Unique Identifier), and the remaining 24 bits are used for NIC/vendor-specific information. It operates on the OSI model's data link layer.

It is supplied by the device's manufacturer and included in its NIC, which is ideally fixed and cannot be modified.

Ping

Ping a computer network management tool is used to determine whether a host is accessible over an IP network. It is supported by almost all operating systems with networking capabilities, including the vast majority of embedded network administration software.

Ping calculates the time it takes for transmissions to travel from the source host to the destination computer and back.

Working of Ping

Ping transmits data with the help of Internet Control Message Protocol (ICMP) packets. An ICMP echo request is sent to the target host and waits for an ICMP echo response.

It reports errors, packet loss, and a statistical summary of the results, typically including the lowest and maximum round-trip timings, mean, and standard deviation of the mean.

The ping utility's command-line arguments and output differ among its several implementations. Options may include:

- The payload size.
- The number of tests.
- The number of network hops (TTL) a probe can travel.
- The gap between requests.
- The amount of time to wait for a response.

Several systems include the IPv6-compatible implementation of ping, and ping6 to test IPv6 network environments.

Address Resolution Protocol (ARP)

The Address Resolution Protocol is a layer 2 protocol used to translate MAC addresses to IP addresses.

All hosts on a network may be found using their IP address, although NICs use MAC addresses rather than IP addresses. ARP is the protocol that connects an IP address to a MAC address.

Working of ARP

Consider that a device wishes to interact with another device over the internet. ARP broadcasts a packet to all the devices on the source network.

The network devices remove the data link layer header from the protocol data unit (PDU) and send the packet to network layer 3 of OSI, where the network ID of the packet and the network ID of the destination IP are checked.

If it's equal, it responds to the source with the MAC address of the destination. Otherwise, the packet reaches the network's gateway which broadcasts the packet to the devices to which it is connected with an address.

The procedure continues until the second-to-last network device in the path arrives at the destination. At this point, it is verified, and ARP responds with the destination MAC address

How to Identify Devices Connected to your Wi-Fi?

There are many ways to check how many devices are connected to my wifi. It can be done manually or automatically with the help of network scanning tools. In the next section, we discuss some ways to identify devices connected to your network.

Manually Identify Devices on a Wireless Network

One way to find network devices on wireless networks is to manually log in to the router's web interface. In-depth information on your network equipment, such as data transfer rate and packet loss, isn't provided by this, though. Typically, routers use the dynamic host configuration (DHCP) protocol to assign each device in a wireless network a distinct local IP address and MAC address so they can be identified.

Automatically Identify Devices on a Wireless Network

To help users more readily discover network devices on Wi-Fi, **Network Scanning Tools** are designed to give extensive information from wireless access points, such as SSID, device type, signal strength, and connected devices.

To steal private data, they employ strategies like packet sniffing, password theft, and man-in-the-middle attacks.

- Network Scanning Tools is software that detects network flaws and protects the system from unusual or abnormal activities.
- The following are some of the most common network scanning tools.
- **Nexpose** Nexpose is a network scanning program that is used to do network scanning. To do the scan, it normally executes the Nmap scripts in the background.
- **Nessus** Nessus is another network scanning tool used to ensure application security by magnifying flaws. It, like nexpose, checks particular files and directories containing data relating to the device's security setup.
- **Nmap** Nmap is another command-line-based network scanning program that is included with several Linux distributions. It performs a scan to determine the condition of a port using either the TCP or UDP protocols. It is fast and powerful enough to scan all 65535 ports.
- **Zenmap** Zenmap is the graphical user interface (GUI) based version of the Nmap network security scanner. Its GUI helps easily map out a network environment.

4.2 Demonstrating how pairing and log-on

4.2.1. Identify the Devices in Your Network

There are many ways to check how many devices are connected to my network. You can quickly discover what is connected to your network, provided you should have internet access at home and a web browser.

The method below is straightforward and does not require any extra software. You need to follow a few easy way:

1. Log into the administrative IP address of your router. Typically, it is 192.168.0.1 or 192.168.1.1.
2. Launch a web browser on your PC or mobile device, enter your default gateway IP address, and press Enter.
3. Use the administrator username and password to log in. For the default credentials, consult the router's documentation.
4. You should be able to see the devices connected to your network on the router's home page or in the router's administrative panel (the interface may vary depending on the router's make and model).

In the administrative UI, you will get the details of a device's connection status, such as whether it is online or offline or how long it has been connected to the network.

It may sometimes list any wired or wireless devices linked to your router. Once you can identify which devices are connected, you can figure out which ones should be allowed to connect to your network and which ones are unknown.

Some routers also allow you to restrict devices from connecting to your network. If you find traces of unsolicited connections, immediately change your Wi-Fi SSID and password.

4.3 Traffic capacity issues

Wireless and mobile networks are essential for connecting people and devices in today's world. However, not all network traffic is the same. Different types of applications and services have different requirements and preferences for bandwidth, latency, reliability, and security. How do you optimize wireless and mobile networks for different types of traffic? Here are some tips and techniques to help you achieve the best performance and user experience

1. **Identify and classify traffic**

The first step to optimize wireless and mobile networks is to identify and classify the traffic that flows through them. You can use tools and protocols such as deep packet inspection (DPI), network analytics, and quality of service (QoS) to monitor and categorize the traffic according to its source, destination, content, and priority. For example, you can distinguish between voice, video, web, gaming, and IoT traffic, and assign different levels of service and resources to each.

2. **Apply traffic shaping and management**

The next step is to apply traffic shaping and management techniques to control and optimize the flow of traffic. Traffic shaping is the process of manipulating the rate, volume, and direction of traffic to meet the network's capacity and objectives. Traffic management is the process of enforcing policies and rules to ensure the quality and security of traffic. For example, you can use traffic shaping to limit or prioritize certain types of traffic, and use traffic management to block or filter unwanted or malicious traffic.

3. **Optimize network protocols and parameters**

Another step is to optimize the network protocols and parameters that govern the communication and transmission of traffic. Network protocols are the rules and standards that enable different devices and systems to exchange data and information. Network parameters are the settings and values that affect the performance and behavior of network protocols. For example, you can optimize the network protocols and parameters to reduce overhead, improve efficiency, enhance security, and adapt to changing conditions.

4. **Leverage network slicing and virtualization**

A further step is to leverage network slicing and virtualization technologies to create and manage multiple logical networks within a single physical network. Network slicing is the process of dividing a network into multiple segments or slices, each with its own characteristics and capabilities. Network virtualization is the process of abstracting and decoupling the network resources and functions from the underlying hardware and software. For example, you can use network slicing and virtualization to isolate and customize different types of traffic, and to increase flexibility and scalability.

5. **Implement edge computing and caching**

A final step is to implement edge computing and caching solutions to reduce the latency and congestion of traffic. Edge computing is the process of moving the computation and processing of data closer to the source or destination of traffic, rather than relying on centralized servers or cloud platforms. Caching is the process of storing copies of frequently accessed or requested data in local or nearby locations, rather than retrieving them from distant or remote sources. For example, you can use edge computing and caching to improve the speed and responsiveness of traffic, and to save bandwidth and energy.

4.4 Developing user documentation

4.1.1. Determine documentation standards

Computer users need documentation so that they can make the best use of their computers as work tools. A computer system can assist them to do their work efficiently and effectively but they need to be able to do three things: • learn how to use the system and its applications • know how to get help when they need to learn more • know what to do when they experience problems. Users will be working across all parts and levels of an organization carrying out different functions such as data entry, financial administration, executive and middle management. However, user documentation is for anyone in an organization who needs assistance with these three tasks

4.1.2. User documentation and appropriate media

Books, manuals, computer-based tutorials and online help are all media for user documentation. Traditionally user documentation has consisted of a range of paper based documents. However, we are no longer limited to these, and organizations are shifting their paper-based user documentation to an online form. There are very good reasons for this:

- **Increased productivity** :- users have up-to-date, comprehensive information that they can access quickly and easily.
- **Increased corporate intelligence**:- information is stored centrally but distributed universally
- **consistency and quality**:- documentation appears in the same format and is easily updateable

What to include in user documentation

It's a good idea at this stage to think about the content that you will include in the user documentation. This is so you can estimate the number of pages, the complexity of the content and what the graphic and text components will be. The content will have some influence on:

- Design of the documentation, including layout, use of text and graphics
- Medium, eg paper-based or online
- The time and resources needed to develop the documentation.

You can consider paper-based documentation, online documentation or a combination of both. The media type you choose will be influenced by the:

- Purpose of the documentation
- User needs and characteristics
- Content (subject matter). Always keep in mind that you need to include a range of items that allow users to access the required information quickly and easily. There are advantages and disadvantages to online and paper media.

Always keep in mind that you need to include a range of items that allow users to access the required information quickly and easily. There are advantages and disadvantages to online and paper media.

Media	Advantages	Disadvantages
Paper	• conventional, most people are used to paper products • easy and fast to prepare • inexpensive to produce • requires readily available software	• hard to maintain control of different versions • costly to update
Online	• convenient Advantages • easy to reach many people geographically dispersed • can be colorful and fun • can link to other related documents • easy to maintain version control • not costly to update	• can be expensive • requires specialized software

Once you have determined the documentation requirements, you can develop a template that meets those requirements and makes the job easier. A template is a file that contains a standard layout, styles and fonts that are used in the production of the documentation. When you want to create a file for user documentation, you open the standard template, usually in Word, and the layout, fonts and styles are already set up in the document. All you need to do is start writing. Everyone uses the same template, so there is a consistent look and feel to all of the user documentation.

The template may be:

- A Word template
- An HTML template
- An online help template.

Self-check 4

Part-I: Say True or False

1. Books, manuals, computer-based tutorials and online help are all media for user documentation.
2. Wireless and mobile networks are essential for connecting people and devices in today's world
3. The Address Resolution Protocol is a layer 3 protocol used to translate MAC addresses to IP addresses.
4. Ping transmits data with the help of Internet Control Message Protocol (ICMP) packets

Part -II: Choose the best Answer

_______**2.** It is 12-digit and 64-bit long, the first 24 bits are utilized for the OUI (Organization Unique Identifier), and the remaining 24 bits are used for NIC/vendor-specific information

A. MAC Address C. Address Resolution Protocol
B. IP Address D. All

_______**3.** ____is network scanning tool used to ensure application security by magnifying flaws.?

A. Nessus C. Ping
B. Nmap D. all

_______**4.** One of the following is software that detects network flaws and protects the system from unusual or abnormal activities.

A. Network Scanning Tools C. Zenmap
B. Formatting D. All

_______**5.** You can consider paper-based documentation, online documentation or a combination of both. The media type you choose will be influenced by the:

A. Purpose of the documentation C. Content (subject matter).
B. User needs and characteristics D. All

_______**6.** Which one is the Advantages online documentation?

A. convenient
B. easy to reach many people geographically dispersed
C. can be colorful and fun
D. All

Part III: - Give short answer

1. List and explain techniques to help you achieve the best performance traffic capacity issue?
2. How to identify the Devices in Your Network?

Unit Five: Monitor and administer wireless network

This learning unit is developed to provide the trainees the necessary information regarding the following content coverage and topics:

- Monitoring wireless network performance
- Debugging networking issues
- Documenting and storing securely current settings.

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Monitor wireless network performance
- Debug networking issues
- Document and store securely current settings.

5.1. Monitoring wireless network performance

Wireless network monitoring is the process of monitoring key aspects of an environment's wireless network to have the insight you need to maintain network performance more easily. Using a wireless network monitor, you can collect and analyze wireless NW health and performance data, including wireless coverage, signal strength, connected clients, and performance statistics for wireless access points

Wireless network monitoring is typically a part of a broader network monitoring strategy, which involves tracking key metrics tied to a network's performance to prevent downtime or slowdowns that can affect end users. While general network monitoring focuses on all aspects of your network (including wired elements), WLAN monitoring specifically focuses on the wireless elements, including access points, controllers, and more.

The need for monitoring wireless networks

- Since wireless networks do not involve the presence of physical interfaces, monitoring them is essential to ensure that they do not suffer from outages / downtime.
- Most employees in organizations these days use wireless networks (such as Wifi, VPN etc) to perform their day to day activities. Hence, ensuring that the wireless networks do not suffer from downtime is a key to business continuity.
- The number of wireless devices in a network is usually more than the number of wired devices. Hence, it is important for a Wireless Network Monitor to ensure that the network does not slip into unplanned downtime.

Wireless network strength

The strength of your wireless network plays a crucial role in ensuring network stability and business continuity. A weak network can result in slow connection and sometimes even in termination of connectivity to a few devices in your wireless network.

- **Keep track of the total number of access points :**
  - ➢ An access point is a station that transmits and receives data. Various devices in a wireless network connect via the access point for interaction with one another.
  - ➢ The number of access points affects the range of connectivity of the wireless network and the connection strength of the network.
  - ➢ Op Manager allows you to keep track of the total number of access points in your wireless network. You can also view the statistics pertaining to the devices connected to a particular access point

The utilization of your wireless network effectively

One other factor that concerns network administrators greatly is the utilization of their wireless network. Op Manager allows you to continuously track the usage of your wireless network by facilitating you to monitor critical network usage metrics.

- You can track factors like CPU utilization, memory utilization, disk utilization, total bytes transmitted by the client etc.. These factors allow you to gain an in-depth understanding of the utilization of your wireless networks.
- What is more? Each of these monitors are backed up by powerful reports that can help you analyze the utilization of your wireless network over a particular period of time
- You can leverage the option to set multiple thresholds to get alerts when your network utilization crosses pre-defined values. This will help you to prevent any form of outages that may occur due to over utilization of your wireless network.
- Apart from the factors specified above, Op manager being a powerful wireless network monitoring tool, has a few additional key features that can simplify the process of monitoring and maintaining your wireless network:

5.2. Debugging networking issues

How do I debug network connectivity issues?

Network connectivity problems can occur at different layers or locations of the network. This article will start at the lowest layer and help you go through the different checks. In addition, most of the methods are not just specific to Firewall.

- **Physical Layer Checks**
  - ➢ Make sure you are using the right cables. CAT 5E or better cables are recommended. Please make sure all the cables are connected firmly.
  - ➢ Check the link lights on your switch/router, and make sure they display the right speed. Firewall link lights.
  - ➢ Check your physical connections, and make sure they are connected correctly. If you are using a switch, make sure there are no switching loops.
  - ➢ If you are having issues with Wi-Fi, try to plug in a device (PC/MAC) via ethernet and see if they are working or not.
  - ➢ Double-check that your access points are configured correctly. Reboot your wifi or AP if needed.

- ➢ If you have a modem, look at its link lights and reboot it.
- ➢ If you are having issues with VLAN, makes sure your none VLAN is working, then double-check your VLAN devices and make sure they are configured correctly.

- **WAN/ISP Connectivity**

We all know how frustrating it feels when experiencing internet outages. To enhance the troubleshooting process, we provided you with a network diagnostics tool that can get detailed network information when the internet is down.

If you need any help from our support team, you can just take a screenshot, or tap on the "Share" button in the top-right corner to send the information to our team for more support.

- **Local Network Connectivity**

LAN connectivity issues can happen if you have a bad cable or problems with the WiFi access point. In this test, you will need to ping the intermediate networks and make sure they are up.

- **DNS Connectivity**

Not all network issues are related to network traffic; sometimes, a bad DNS server configuration may cause issues. To test, you can ping a public IP address, say, 1.1.1.1 to check if the internet is accessible, and 'nslookup' will help you validate if the DNS server is doing a good job to find the public IP mapping to the domain.

5.3. Documenting and storing securely current settings.

How to Secure Your Documents?

The ability to share documents in multiple ways among members of your organization makes everyone’s jobs easier. Unless your job is managing the organization’s security, that is. Then your job becomes much harder.

With so many ways to share items, document security is a challenging undertaking, but it is possible to succeed by following the right steps.

What is Document Security Anyway?

Securing documents in an organization involves protecting them from a wide range of perils. Some of these perils include:

- Hackers stealing document data
- Loss of documents
- Revealing personal information
- Unwanted copies of sensitive documents

How Document Security Works

When trying to secure your documents, it involves thinking about the security of both paper and digital copies of documents. Team members should undertake steps that allow them to protect documents at all times.

Individually, team members will need to follow the policies, ensuring they are doing everything they can to guard sensitive information and documents. Here are eight reliable practices for securing your documents**.**

1. Digitize Your Documents

For the majority of organizations, paper documents become a greater security risk than digital documents. A team member could lose a hard copy of a document, or someone could carry it out of the building without anyone's knowledge.

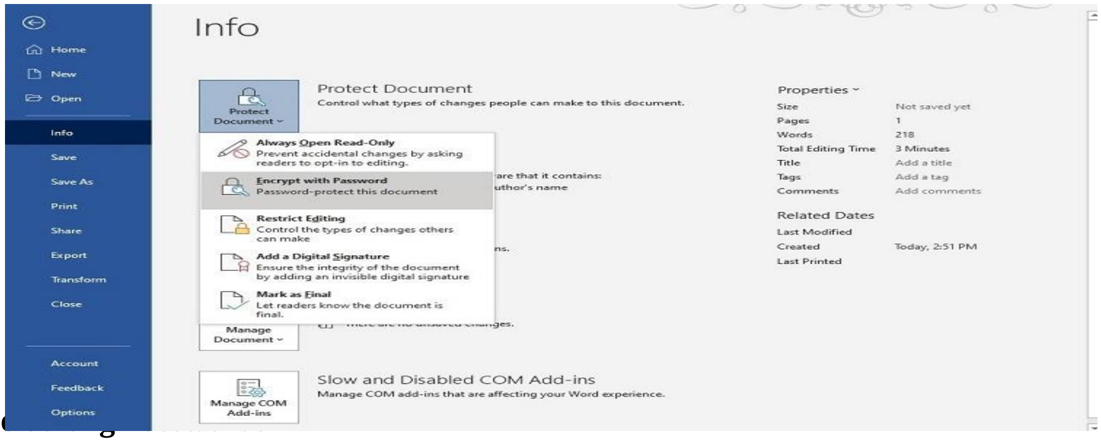
Create digital scans of any paper documents, and then apply security measures to the digital copies for maximum protection. Shred the paper documents to finish the job.

2. Use Password Protection

Using password protection on the most important files is a smart idea. If members of the organization are using laptops or smartphones to work on sensitive documents, someone could take the device. Without password protection on the files on the mobile device, the person who takes the device may access the sensitive files.

3. Password Protecting Microsoft 365 Documents

To protect a document you created in Microsoft 365 with a password, click the **File** menu and then Info. In the Info window, click the **Protect Document** button. In the popup menu, click Encrypt with Password.



Info

Protect Document
Control what types of changes people can make to this document.

Always Open Read-Only
Prevent accidental changes by asking readers to opt-in to editing.

Encrypt with Password
Password-protect this document

Restrict Editing
Control the types of changes others can make

Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature

Mark as Final
Let readers know the document is final.

Properties

Size	Not saved yet
Pages	1
Words	218
Total Editing Time	3 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	
Created	Today, 2:51 PM
Last Printed	

Slow and Disabled COM Add-ins
Manage COM add-ins that are affecting your Word experience.

4. Us

Creating passwords that are difficult to guess or decipher is as important as choosing to use passwords on your documents. The idea of creating strong passwords should be part of your network access and cloud storage accounts too.Some tips for creating strong passwords include:

- Don't use common words or phrases unless you're adding in numbers and special characters
- Don't use items that relate to your life or personality
- Use a mix of uppercase and lowercase letters
- Use multiple numbers and special characters
- Use at least eight characters, but 10 to 20 characters is even better

5. Encrypt Your Files

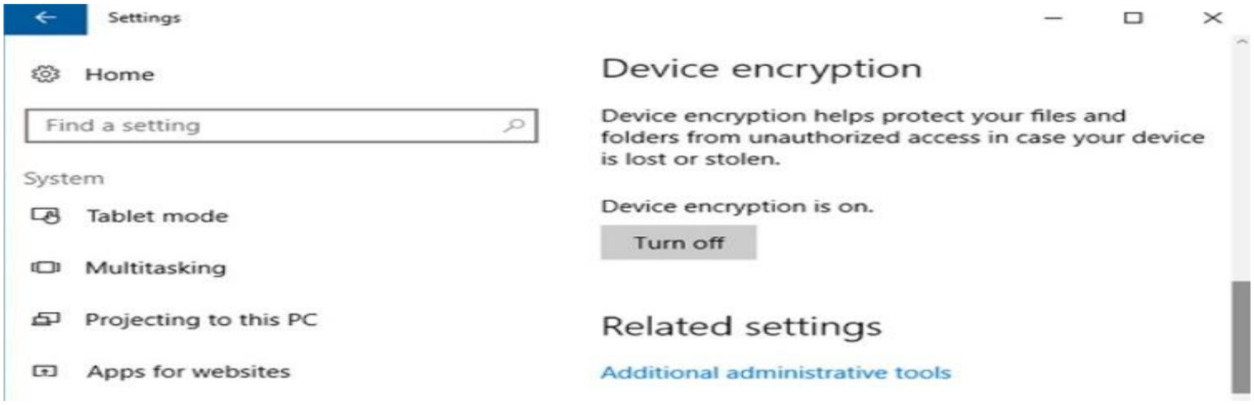
Encrypting the files on the computer provides another layer of security that's easy to use for your team members, but that thwarts would-be thieves effectively.

You have the option of using a free or subscription-based third-party encryption software. You also can use the encryption system built into the Windows or Macintosh operating systems.

Setting Up Encryption on Windows

With Windows 10 Pro, Education, or Enterprise versions, encryption is automatically available for your files. To turn on encryption on a Windows computer, sign in as an administrator.

Click the **Start** button. Then click **Settings, Update & Security,** and **Device Encryption**. If you do not see Device Encryption as an option, you are running Windows 10 Home, do not have administrator privileges, or your computer doesn't have the hardware to support encryption through Windows. **Click the button** to turn on (or turn off) encryption for the Windows computer.



Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen.

Device encryption is on.

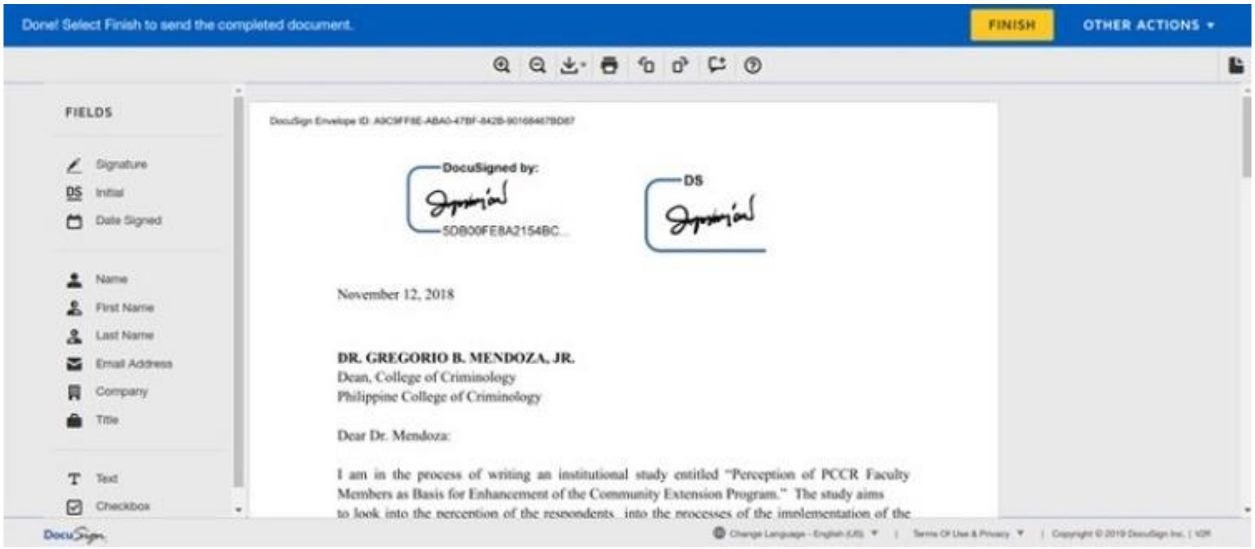
6. Avoid Emailing Documents

figure 5. 1 Setting Up Encryption on Windows

Rather than emailing documents to clients or coworkers, where recipients could make copies or printouts of sensitive data, organizations can use a few different options that do not involve sending attachments.

7. **Cloud Storage:** Many cloud storage providers give users the ability to share links to documents stored in the cloud. The document's creator can provide recipients with the ability to view it and make comments without copying or editing the document.

8. **Digital Signatures:** When an organization needs signatures on a document, rather than emailing the documents back and forth, use services that allow for digital signatures, such as DocuSign. The document remains protected, and you can send the recipient an uneditable copy after all parties sign it.


Done! Select Finish to send the completed document.
FINISH
OTHER ACTIONS ▾
FIELDS
Signature
DS Initial
Date Signed
Name
First Name
Last Name
Email Address
Company
Title
Text
Checkbox
DocuSign
Change Language - English (US) ▾ | Terms Of Use & Privacy ▾ | Copyright © 2019 DocuSign Inc. | V2R

DocuSign Envelope ID: A9C9FF8E-ABA0-47BF-842B-90168467BD87

DocuSigned by:

5DB00FE8A2154BC...

DS

November 12, 2018

DR. GREGORIO B. MENDOZA, JR.
Dean, College of Criminology
Philippine College of Criminology

Dear Dr. Mendoza:

I am in the process of writing an institutional study entitled "Perception of PCCR Faculty Members as Basis for Enhancement of the Community Extension Program." The study aims to look into the perception of the respondents, into the processes of the implementation of the

Figure 5. 2 Digital Signatures to protect file

Self-check-5

Part I:- Say True or False

________1. Wireless network strength can be improved by using signal boosters or range extenders.

________2. Encrypting your files before storing them in cloud storage provides an additional layer of security.

________3. Digital signatures are commonly used in wireless communication to verify the identity of the sender.

Part-II:- select the best answer from the given alternative

_______1. What is the process of monitoring key aspects of an environment's wireless network to have the insight you need to maintain network performance more easily?

A. Wireless network
B. Network monitoring
C. Wireless network monitoring
D. Monitoring websites

_______**2.** why we need for monitoring wireless networks

A. It is essential to ensure that they do not suffer from outages / downtime.
B. Ensuring that the wireless networks do not suffer from downtime is a key to business continuity
C. It is important for a Wireless Network Monitor to ensure that the network does not slip into unplanned downtime.
D. All of the above

_______3. How do we debug network connectivity issues?

A. Physical Layer Checks
B. WAN/ISP Connectivity
C. Local Network Connectivity
D. All of the above

_______4. What are the reliable practices for securing your documents?

A. Digitize Your Documents
B. Use Strong Passwords
C. Password Protecting Microsoft 365 Documents
D. All of the above

Part-III Short Answer all the questions listed below.

1. List some of the protecting and securing documents in an organization involves from perils or threat?
2. How do I debug network connectivity issues?

Reference

List of Book

1. Wi-Fi Home Networking Just the Steps For Dummies" by Danny Briere and Hurley
2. Building Wireless Community Networks" by Rob Flickenger
3. Computer Applications in Management Dahiya, U/ Nagpal, S. Taxman Allied Service
4. Wireless Networking Handbook" by Regis J. Bates and Donald W. Gregory:
5. Milestones in Computer Science and Information Technology by Edwin D. Reilly
6. Home Networking Do-It-Yourself For Dummies" by Lawrence C. Miller:
7. The Book of Wi-Fi: Install, Configure, and Use 802.11b Wireless Networking" by John
8. Deploying and Troubleshooting Cisco Wireless LAN Controllers" by Mark L. Gress
9. Building a Home Security System with Raspberry Pi" by Matthew Poole:

WEB Address

1. https://www.free-power-point-templates.com/articles/creating-business-cards-in-microsoft-publisher/
2. https://www.wikihow.com/Make-a-Certificate-Using-Microsoft-Publisher
3. https://purplesec.us/firewall-penetration-testing

Developers Profile

No	Name	Qualification (Level)	Field of Study	Organization/ Institution	Mobile number	E-mail
1	Zerihun Abate	MSc	ITM	Sebata PTC	0911858358	zedoabata2017@gmail.com
2	Abebe Mintefa	MSc	ITM	Ambo TVETC	0929362458	tolabula@gmail.com
3	Endale Berekat	Bsc	Computer Science	M/G/M/B/P/T/C	0915439694	zesaron1221@gmail.com
4	Yinebeb Tamiru	Bsc	Computer science	Akaki PTC	0936325182	yinebebtamiru07@gmail.com