

SPPU-BE-COMP-CONTENT - KSKA Git

Q1> Describe the Process of Building a Wireless Network.

ANS. Building a Wireless Network involves referring / configuring a Wireless router to provide access to the Internet or a Private Network.

⇒ The Router acts as both a router and Wireless Access Point.

(1) Connecting the Router.

The Wireless Router is connected to a Modem (like xDSL, DOCSIS, or Fiber Optic modem) to get the Internet Access.

(2) Configuration

- You use a local login page to configure the Router's settings. This is where you ^{can} manage the security setting to permit prevent the Un-authorized Access.

(3) Security Measures

- To Enhance security, it is recommended to disable WPS mode to prevent the Brute Force attacks on the Networks SSID. You can also implement MAC Address Filtering by performing Address reservation to ensure only specific devices can connect.

(4) Network Monitoring.

- You can check the System Log Files on the Router's configuration pages to monitor network Activity and identify any suspicious events.

Q2> How to Ensure that WiFi is Blocking Hackers?

ANS. WiFi can block hackers by implementing certain security configurations on the Wireless router.

Following are the ways to do it:

SPPU-BE-COMP-CONTENT - KSKA Git

(1) Dis-abling WPS Mode:-

- Wi-Fi Protected Setup (WPS) can make the Network vulnerable to brute-force attacks on the SSID.
- Disabling such Feature, prevents such attacks.

(2) Performing Address Reservation via MAC Address:

- This method allows user to authorize specific device to connect to the network. By using a list approved MAC Address, the router can deny access to any Un-approved devices.

(3) Checking System Log Files:

- The Router's System logs can be used to monitor network Activity and detect any suspicious connection attempts helping to identify the potential Threats.
- Regularly checking these logs can help you to identify unusual or un-authorized connection Attempts.

Q3. Explain the Modes of Wireless Security in Brief.

ANS. The Modes of Wireless Security have evolved over the time to Address Vulnerabilities and provide stronger protection for Wifi Networks.

- The Primary modes in order to development are WEP, WPA, WPA2, and WPA3.

(1) WEP. (Wired Equivalent Privacy)

- WEP is the Oldest and least secure of the protocols.
- It was an initial attempt to provide the some level of security as a wired network, but it contains significant vulnerabilities that make it easy for hackers to Exploit.

SPPU-BE-COMP-CONTENT - KSKA Git

(2) WPA. (WiFi Protected Access)

- It is a temporary solution to WEP.
- It introduced Temporal Key Integrity Protocol (TKIP) which is more secure than the static key used by WEP.

(3) WPA 2

- WPA2 is currently the most widely used security protocol, it replaced the Temporal Key Integrity Protocol (TKIP) with the most robust Advanced Encryption Standard (AES)
- It provides much stronger Defence against the Attacks.

(4) WPA 3

- WPA3 is the latest standard offering several security enhancements over WPA2
- It provides stronger encryption, better protection against offline password guessing attacks. It also improves security ~~over~~ on public Network.

→ CONCLUSION:-

Hence, By configuring the basic settings on the WiFi console, we can prevent the un-authorized access and un-ethical use of Network (Internet)