NASSCOM® FOUNDATION

Directorate General of Training

Powered by Microsoft

Secure a Wi-Fi Network

Secure a Wi-Fi Network

Create a new W-LAN

Step 1: To create a new WLAN, expand the **Wi-Fi Networks** section and click **Create**.

Step 2: The **Create WLAN** pop-up window is displayed. Enter the following details.

1. Enter a suitable name for your WLAN.
2. Select the **Usage Type**.
3. Select the **Authentication Method**.
4. Select the **Encryption Method**.
5. Enable the **Web Authentication**.
6. Select the **Authentication Server**.

1. Name

Enter the name of your choice.

2. Usage Type

- **Standard:** Use this WLAN type for most regular wireless network usage.
- **Guest Access:** Use this WLAN type for a guest WLAN. Guest access policies and access controls will be applied.
- **Hotspot Service:** Use this WLAN type for a Hotspot (aka, WISPr) WLAN.
- **Social Media:** Social Media WLANs require the visitor to log in using a social media account before being granted Internet access.

3. Authentication Method

Open: No authentication method is used.

802.1X EAP: Authentication against either the internal database or an external RADIUS server.

MAC Address: Authentication using the client's MAC address against an external RADIUS server.

4. Encryption Method

WPA2: Encrypt traffic using the WPA2 standard.

None: No encryption; communications are sent in clear text.

5. Captive Portal

Choose whether a Captive Portal will be used for web-based authentication.

6. Authentication Server

If either 802.1X EAP, MAC Address or Web Auth (Captive Portal) options are chosen, select an **Authentication Server** from the list.

- If an external authentication server is to be used rather than the internal database, click **Create Service** to create an AAA server object to authenticate against.
- **Note**: Alternatively, you can create AAA servers on the Admin & Services > Services > AAA Servers page. For more information, see AAA Servers.

Step 3: After entering all the details click **OK** to save and deploy the new WLAN.

Configure a W-LAN

Steps to configure a WLAN

Step 1: Configure the interface and the security zone

1. On the **Navigation** pane, click **Configuration** > **Network** > **Network** to visit the Network page.

2. Select the **ethernet0/1** interface and then click **Edit**. In the pop-up window, configure the following settings.

- Binding zone - Layer 3 zone
- Zone - Select untrust from the drop-down menu
- Type - PPPoE
- Username - PPPoE-user
- Password - 123456
- Confirm password – 123456

3. Click **OK** to save the settings.

4. Select the **wlan1** interface and then click **Edit**. In the pop-up window, configure the following settings:

- Binding zone - Layer 3 zone
- Zone - Select trust from the drop-down menu
- Type - Static IP.
- IP address - 192.168.2.1
- Netmask - 255.255.255.0

5. Select the **Enable DNS** checkbox.

6. Click **DHCP**. In the pop-up window, configure the following settings:

- Type - DHCP server
- Gateway - 192.168.2.1
- Netmask - 255.255.255.0
- DNS1 - 192.168.2.1
- Start IP - 192.168.2.2
- End IP - 192.168.2.254

7. Click **Add**.

8. Click **OK** to save the configurations and return to the Interface Configuration page.

9. Click **OK** to save the configurations and return to the Network page.

Step 2: Configure the DNS Proxy

1.On the Navigation pane, click Configuration > Network > Network to visit the Network page.

2. Click DNS in the right Task pane. The DNS List dialog appears.

3. With the Server and Proxy tab active, click New in the DNS proxy section. The DNS Proxy Configuration pop-up appears.

4. Configure the following settings the pop-up window.

- Domain type - Any domain
- Domain server - Use system config

5. Click OK to save the configurations and close the dialog.

Step 3: Configure NAT rules

1. On the Navigation pane, click Configuration > Network > NAT to visit the NAT page.

2. With the SNAT tab active, click New. In the pop-up SNAT Configuration dialog, configure the following settings:

- VR - trust-vr
- Src address - Select Address entry and any.
- Dst address - Select Address entry and any.
- Egress - Select Egress interface and ethernet0/1.
- Sticky - Select Enable.

3. Click OK to save the configurations. The system will generate a SNAT rule whose ID is 1.

Step 4: Configure policy rules

1. On the Navigation pane, click Configuration > Security > Policy to visit the NAT page.

2. Click New. The Policy Configuration window appears.

3. Configure the following settings:

- Src zone - trust
- Dst zone - untrust
- Src address - Any
- Dst address - Any
- Service - Any
- Action - Permit

4. Click OK to save the configurations.

Step 5: Configure the AAA server

1. Select AAA Server from the Objects drop-down menu. The AAA Server dialog appears.

2. Click New and select Radius Server. In the pop-up Radius Server Configuration dialog, configure the following settings:

- Server name - radius1
- Server address - 202.10.1.2
- VR - trust-vr
- Port - 1812
- Password - 123456
- Confirm password - 123456

3. Click OK to save the modifications.

Step 6: Configure the WLAN settings

1. On the Navigation pane, click Configuration > Network > WLAN to visit the WLAN page.

2. Select the Enable checkbox and then click Apply.

3. Configure the following settings:

- SSID - test
- WLAN Interface - Select wlan0/1 from the drop-down menu.
- SSID broadcast - Select Enable.
- Security mode - Select WPA2-PSK/WPA2 from the drop-down menu.
- Data encryption - Select CCMP from the drop-down menu.
- Pre-shared key - abc123
- Maximum users – 64
- User isolation - Select Enable.

4. Click OK to save the configurations.

MAC address filtering

- MAC address filtering allows you to block traffic coming from certain known machines or devices.
- The router uses the MAC address of a computer or device on the network to identify it and block or permit the access.
- Traffic coming in from a specified MAC address will be filtered depending upon the policy.
- Most broadband routers and other wireless access points include an optional feature called MAC address filtering, or hardware address filtering.
- MAC address filtering adds an extra layer to this process.
- It improves security by limiting the devices that can join a network.
- Before letting any device join the network, the router checks the device's MAC address against a list of approved addresses. If the client's address matches one on the router's list, access is granted as usual; otherwise, it's blocked from joining.

Steps to enable the MAC address filtering

1. Choose Firewall > Advanced Settings > MAC Filtering.

2. Check the Enable box to enable MAC Address Filtering for this device. Uncheck the box to disable this feature.

3. If you enable MAC filtering, in the Policy for MAC Addresses Listed Below field, choose one of the following options:

    - Block and Allow the Rest—Choose this option to block the traffic from the specified MAC addresses and to allow traffic from all other addresses.
    - Allow and Block the Rest—Choose this option to allow the traffic from the specified MAC addresses and to block traffic from all other machines on the LAN side of the router.

4. In the MAC Addresses table, click Add.

5. Enter the MAC address and description to add to the table and click Save. Repeat for each address to allow or block.

6. Click Save.

Create User Accounts with Limited Rights

One can create user accounts with limited rights to restrict the access and can restrict users' access to Wi-Fi sessions with UserLock, using RADIUS Authentication and RADIUS Accounting

Steps to configure the Wifi access point to restrict user access to a Wi-Fi session.

Step 1: Install the NPS UserLock Agent to the NPS Server

1. From the UserLock console, right-click and click Install to deploy the NPS agent on the NPS server.

2. Under the NPS server, run CMD (or PowerShell) as administrator and run the following commands:

- net stop remoteaccess
- net stop ias
- net start ias
- net start remoteaccess

3. From the UserLock Console, check that the status of the NPS agent is "Installed".

Step 2: Test the protection restricting all users to 1 concurrent Wi-Fi Session maximum

1. Click **Protected accounts** > **Add group.** On the **Protected accounts** pop-up, create a protected account called "Everyone" to apply this new rule to all users and click **OK**.

2. Right-click on the group name and select **Properties**. Configure the "Everyone" protected account to restrict each user to 1 concurrent Wi-Fi session maximum.

Step 3: Testing the UserLock restrictions

1. Make a Wi-Fi connection with one account (in this example the account "Alice"). The connection is successful. You can see the session in the UserLock console.

2. Now try opening a second Wi-Fi connection with Alice, it will be denied.

Wi-Fi Authentication Mode

1. UserLock cannot monitor interactive sessions and Wi-Fi sessions for domain computers where the desktop agent is installed.
2. If the machine is a member of the domain, and the desktop agent is installed, the Wi-Fi must be configured with "computer authentication" for the desktop agent to function correctly.
3. For machines that are not part of the domain, the Wi-Fi authentication mode must be configured with "user authentication" to monitor Wi-Fi sessions.
4. Wi-Fi authentication mode can be changed in the properties of the Wi-Fi network adaptor or via GPO.

Recap:

- Configuring WLAN helps the user to secure the wifi.
- Unless using an external authentication server (i.e., RADIUS server), select Open authentication, and combine with WPA2 encryption for secure Wi-Fi access.
- MAC address filtering allows you to block traffic coming from certain known machines or devices.
- Most broadband routers and other wireless access points include an optional feature called MAC address filtering, or hardware address filtering.
- You can restrict users' access to Wi-Fi sessions with UserLock, using RADIUS Authentication and RADIUS Accounting