



VERSION 1

JULI , 2022

# [PRAKTIKUM JARINGAN KOMPUTER]

## CONFIGURE A WIRELESS NETWORK – MODUL 6

TIM PENYUSUN :

MAHAR FAIQURAHMAN, S.KOM, M.T

ALIF SYIFA ARSYILA

ARIEL BAGUS AR – RASYIID

PRESENTED BY: LAB - INFORMATIKA

UNIVERSITAS MUHAMMADIYAH MALANG

---

### PERSIAPAN MATERI

- Konfigurasi WLAN
- Konfigurasi Wireless Network

---

### TUJUAN

- Mahasiswa mampu memahami dan mengimplementasi Konfigurasi WLAN
- Mahasiswa mampu memahami dan mengimplementasi Konfigurasi Wireless Network

---

### PERSIAPAN SOFTWARE/APLIKASI

- Komputer/Laptop
- Sistem operasi Windows/ Linux/ Mac OS
- Simulator Packet Tracer

---

### MATERI POKOK

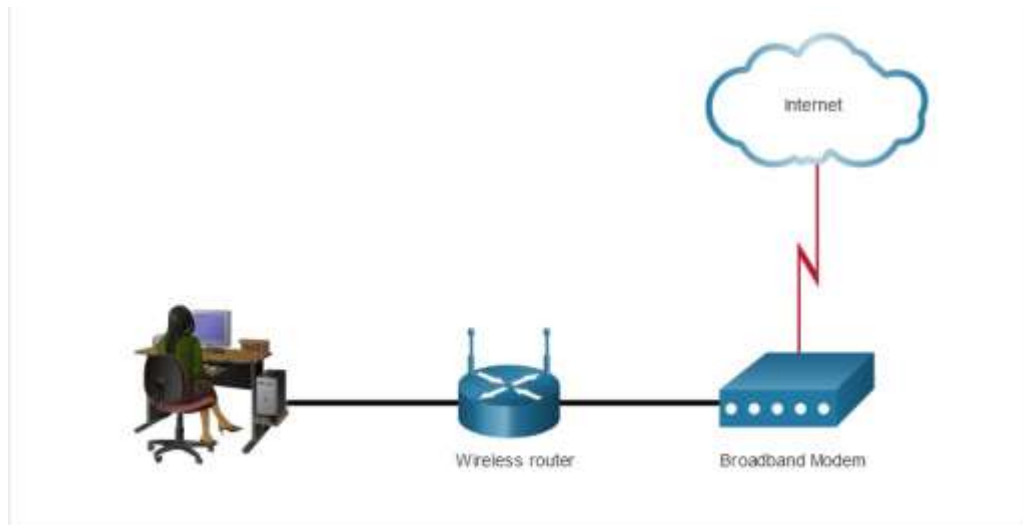
#### WLAN Configuration

##### 1. The Wireless Router

Remote workers, kantor cabang kecil, dan jaringan rumah sering menggunakan kantor kecil dan router rumah. Router ini kadang-kadang disebut router terintegrasi karena biasanya termasuk switch untuk klien kabel, port untuk koneksi internet (kadang-kadang berlabel "WAN"), dan komponen nirkabel untuk akses klien nirkabel, seperti yang ditunjukkan untuk Cisco Meraki MX64W dalam gambar. Cisco Meraki MX64W



Gambar berikutnya menunjukkan topologi yang menggambarkan koneksi fisik laptop kabel ke router nirkabel, yang kemudian terhubung ke kabel atau modem DSL untuk konektivitas internet.



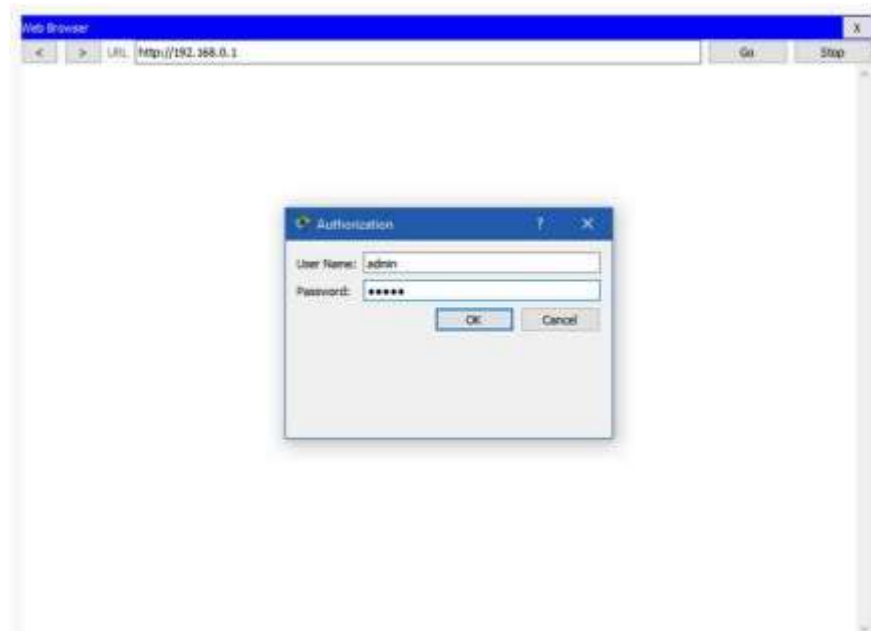
Router nirkabel ini biasanya menyediakan keamanan WLAN, layanan DHCP, Terjemahan Name Address Translation (NAT), quality of service (QoS), serta berbagai fitur lainnya. Set fitur akan bervariasi berdasarkan model router.

**Catatan:** Konfigurasi modem kabel atau DSL biasanya dilakukan oleh service provider baik di tempat atau dari jarak jauh melalui penelusuran dengan Anda di telepon. Kemungkinan besar akan dihubungi service provider Anda untuk informasi lebih lanjut.

## 2. Log in to the Wireless Router

Sebagian besar router nirkabel siap untuk layanan di luar kotak. Mereka telah dikonfigurasi untuk terhubung ke jaringan dan menyediakan layanan. Misalnya, router nirkabel menggunakan DHCP untuk secara otomatis menyediakan informasi yang menangani ke perangkat yang terhubung. Namun, alamat IP default router nirkabel, username, dan kata sandi dapat dengan mudah ditemukan di internet. Cukup masukkan frasa pencarian "alamat IP router nirkabel default" atau "kata sandi router nirkabel default" untuk melihat daftar banyak situs web yang menyediakan informasi ini. Misalnya, nama pengguna dan kata sandi untuk router nirkabel dalam gambar adalah "admin". Oleh karena itu, prioritas pertama Anda adalah mengubah default ini karena alasan keamanan.

Untuk mendapatkan akses ke GUI konfigurasi router nirkabel, buka browser web. Di bidang alamat, masukkan alamat IP default untuk router nirkabel Anda. Alamat IP default dapat ditemukan dalam dokumentasi yang disertakan dengan router nirkabel atau Anda dapat mencari di internet. Angka tersebut menunjukkan alamat IPv4 192.168.0.1, yang merupakan default umum bagi banyak produsen. Jendela keamanan meminta otorisasi untuk mengakses GUI router. Kata admin umumnya digunakan sebagai nama pengguna dan kata sandi default. Sekali lagi, periksa dokumentasi router nirkabel Anda atau cari di internet.

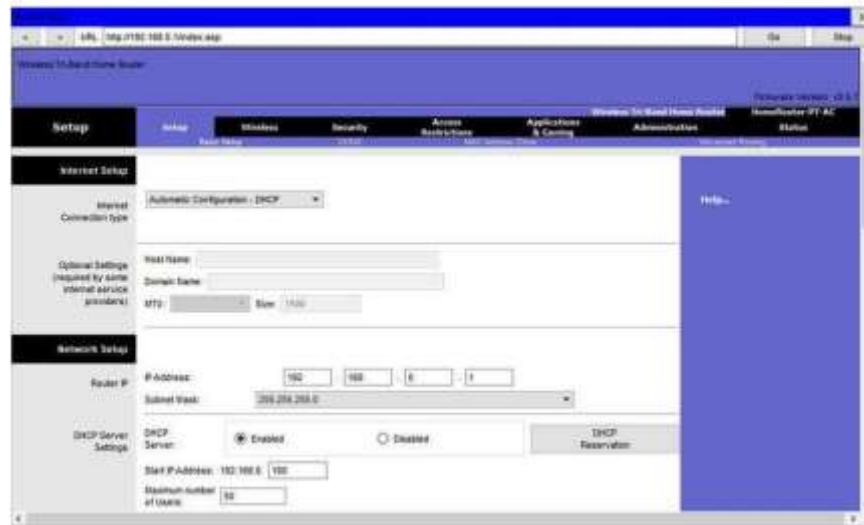


### 3. Basic Network Setup

Basic network setup includes the following steps:

- Log in to the router from a web browser.

Setelah masuk, GUI terbuka. GUI akan memiliki tab atau menu untuk membantu Anda menavigasi ke berbagai tugas konfigurasi router. Seringkali perlu untuk menyimpan pengaturan yang diubah dalam satu jendela sebelum melanjutkan ke jendela lain. Pada titik ini, ini adalah praktik terbaik untuk membuat perubahan pada pengaturan default.



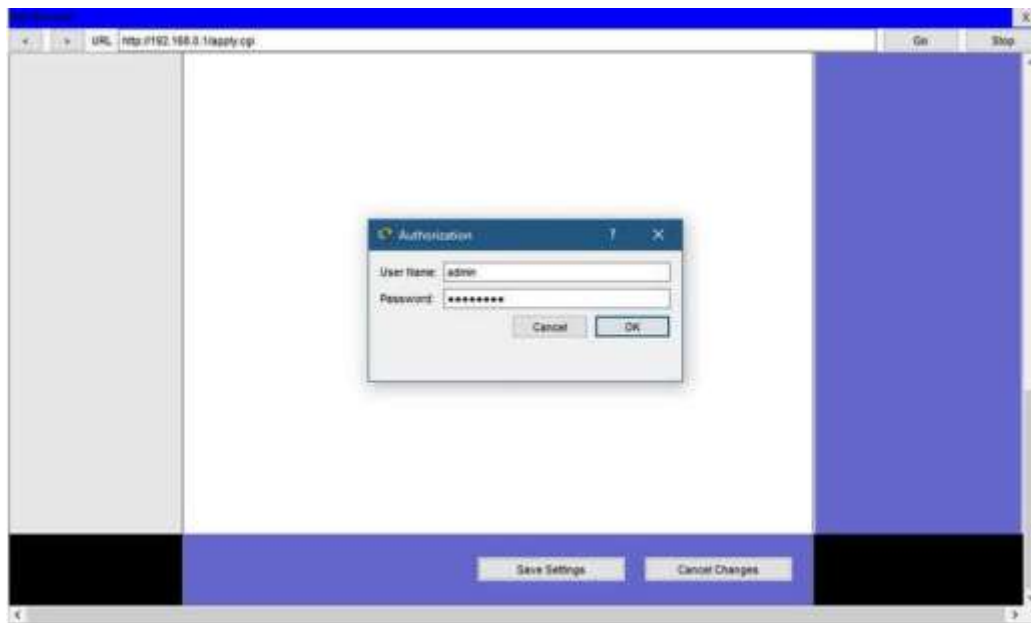
- Change the default administrative password.

Untuk mengubah kata sandi masuk default, temukan bagian administrasi GUI router. Dalam contoh ini, tab Administrasi dipilih. Di sinilah kata sandi router dapat diubah. Di beberapa perangkat, seperti yang ada di contoh, Anda hanya dapat mengubah kata sandi. Nama pengguna tetap admin atau apa pun nama pengguna default untuk router yang Anda konfigurasi.



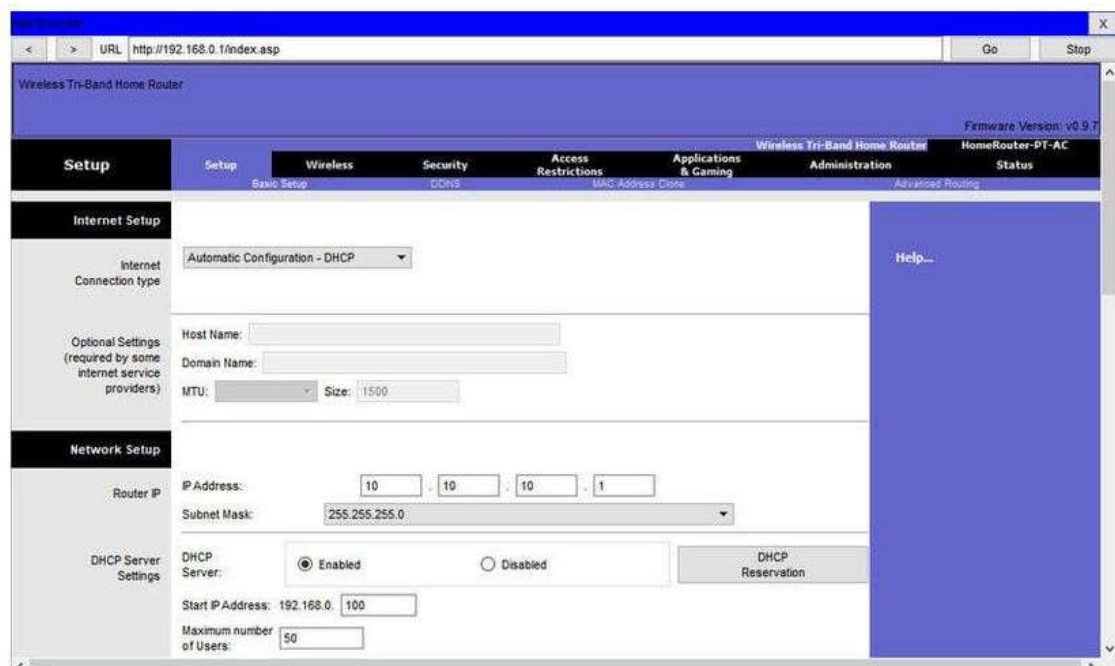
- Log in with the new administrative password.

Setelah Anda menyimpan kata sandi baru, router nirkabel akan meminta otorisasi lagi. Masukkan nama pengguna dan kata sandi baru, seperti yang ditunjukkan dalam contoh.



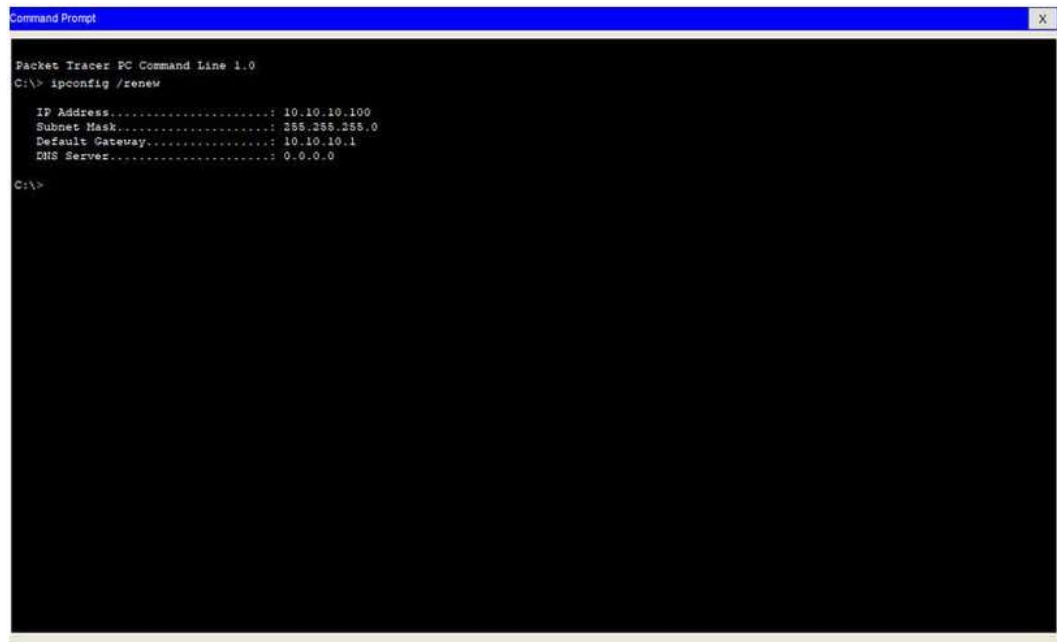
- Change the default DHCP IPv4 addresses.

Ubah alamat IPv4 router default. Ini adalah praktik terbaik untuk menggunakan alamat IPv4 pribadi di dalam jaringan Anda. Alamat IPv4 10.10.10.1 digunakan dalam contoh tetapi bisa jadi alamat IPv4 pribadi yang Anda pilih.



- Renew the IP address.

Ketika Anda mengklik simpan, Anda akan kehilangan akses sementara ke router nirkabel. Buka jendela perintah dan perbarui alamat IP Anda dengan perintah `ipconfig /renew`, seperti yang ditunjukkan dalam contoh.



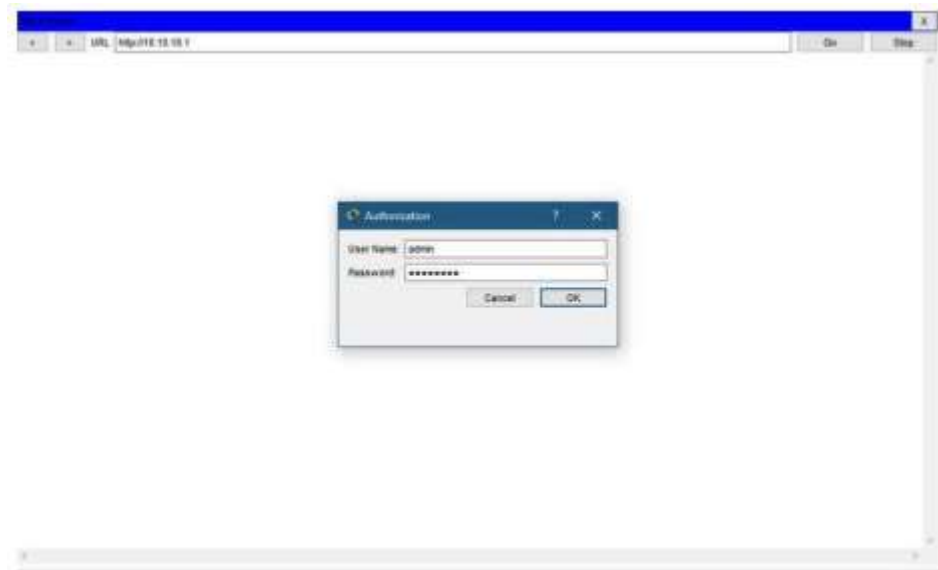
```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\> ipconfig /renew

IP Address. . . . .: 10.10.10.100
Subnet Mask. . . . .: 255.255.255.0
Default Gateway. . . . .: 10.10.10.1
DNS Server. . . . .: 0.0.0.0

C:\>
```

- Log in to the router with the new IP address.

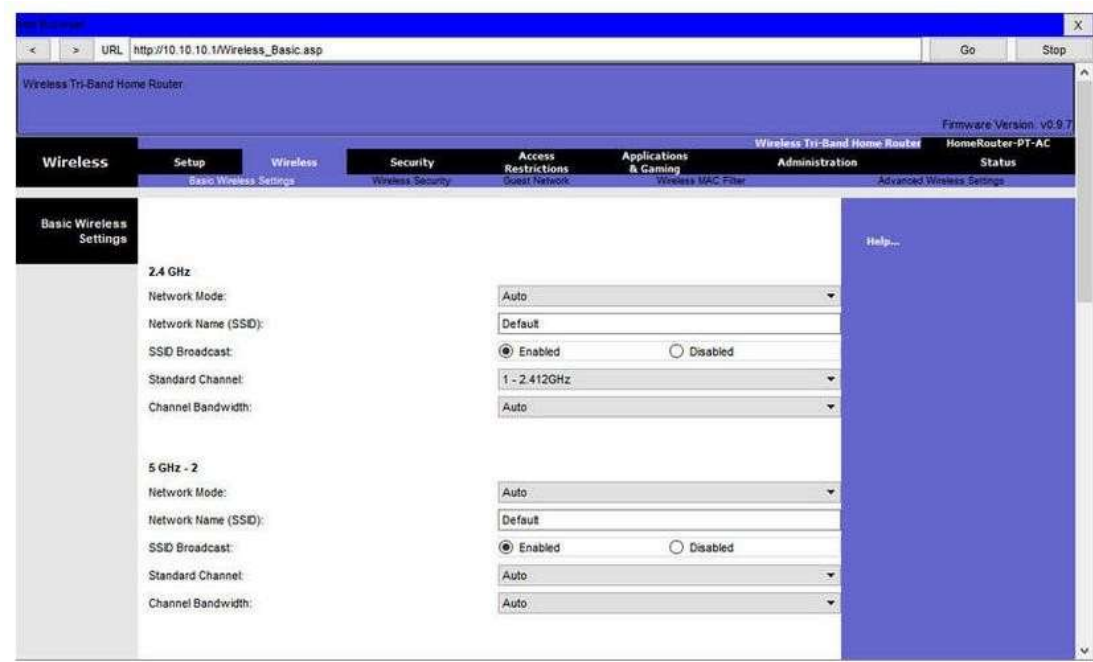
Masukkan alamat IP baru router untuk mendapatkan kembali akses ke GUI konfigurasi router, seperti yang ditunjukkan dalam contoh. Anda sekarang siap untuk terus mengonfigurasi router untuk akses nirkabel.



#### 4. BASIC WIRELESS SETUP

- View the WLAN defaults.

Di luar itu, router nirkabel menyediakan akses nirkabel ke perangkat menggunakan nama jaringan dan kata sandi nirkabel default. Nama jaringan disebut Service Set Identified (SSID). Temukan setelan nirkabel dasar untuk router Anda agar dapat mengubah setelan default ini, seperti yang ditunjukkan dalam contoh.





- Change the network mode.

Beberapa router nirkabel memungkinkan Anda memilih standar 802.11 mana yang akan diterapkan. Contoh menunjukkan bahwa "Warisan" telah dipilih. Ini berarti perangkat nirkabel yang terhubung ke router nirkabel dapat memiliki berbagai NIC nirkabel yang terinstal. Router nirkabel saat ini dikonfigurasi untuk mode warisan atau campuran kemungkinan besar mendukung 802.11a, 802.11n, dan 802.11ac NIC.



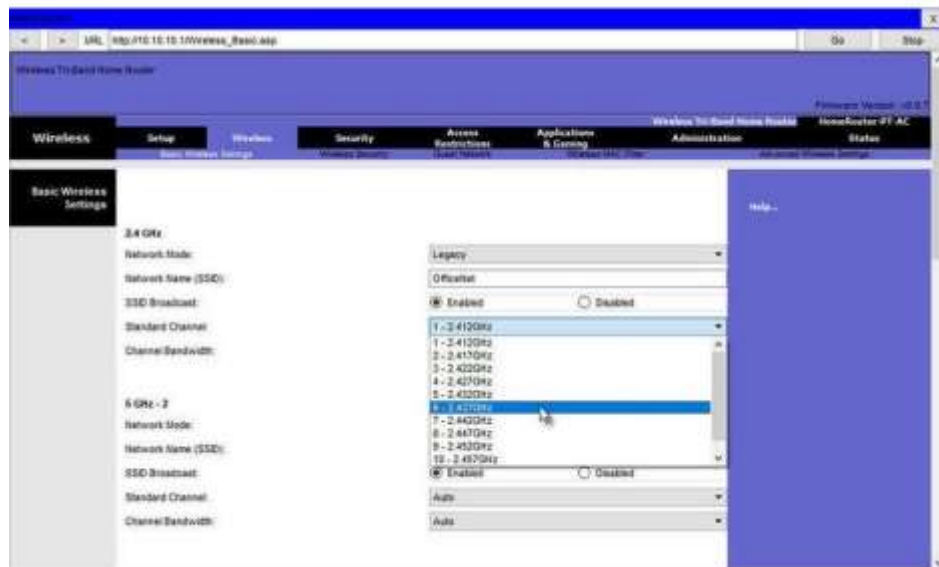
- Configure the SSID.

Tetapkan SSID ke WLAN. OfficeNet digunakan dalam contoh untuk ketiga WLAN (WLAN ketiga tidak diperlihatkan). Router nirkabel mengumumkan kemunculannya dengan mengirim broadcast yang menyebarkan SSID-nya. Ini memungkinkan host nirkabel menemukan nama jaringan nirkabel secara otomatis. Jika broadcast SSID dinonaktifkan, Anda harus memasukkan SSID secara manual pada setiap perangkat nirkabel yang terhubung ke WLAN.

- Configure the channel.

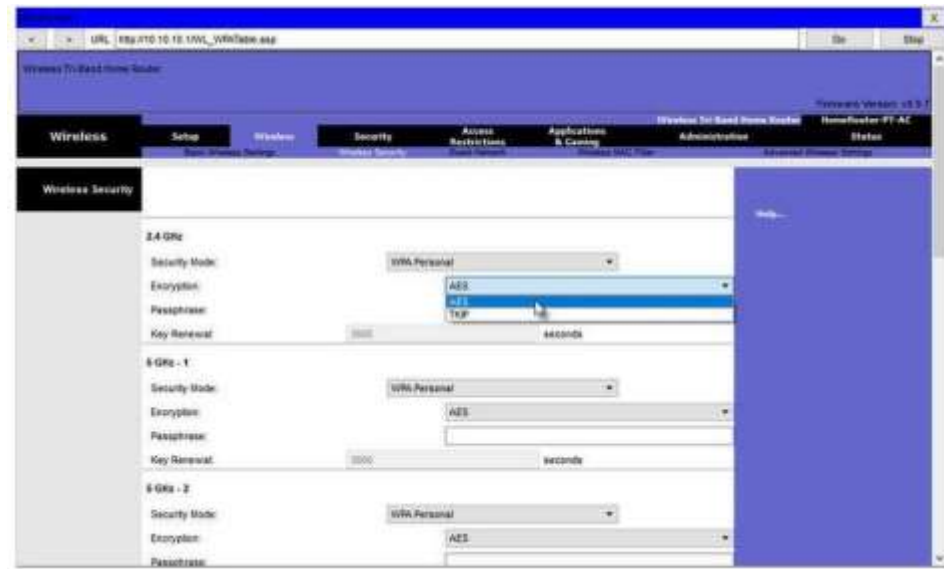


Perangkat yang dikonfigurasi dengan saluran yang sama dalam pita 2.4GHz dapat tumpang tindih dan menyebabkan distorsi, memperlambat kinerja nirkabel dan berpotensi merusak koneksi jaringan. Solusi untuk menghindari gangguan adalah dengan mengkonfigurasi saluran yang tidak tumpang tindih pada router nirkabel dan titik akses yang dekat satu sama lain. Secara khusus, saluran 1, 6, dan 11 tidak tumpang tindih. Dalam contoh, router nirkabel dikonfigurasi untuk menggunakan saluran 6.



- Configure the security mode.

Di luar itu, router nirkabel mungkin tidak memiliki keamanan WLAN yang dikonfigurasi. Dalam contoh, versi pribadi Wi-Fi Protected Access versi 2 (WPA2 Personal) dipilih untuk ketiga WLAN. WPA2 dengan enkripsi Advanced Encryption Standard (AES) saat ini merupakan mode keamanan terkuat.



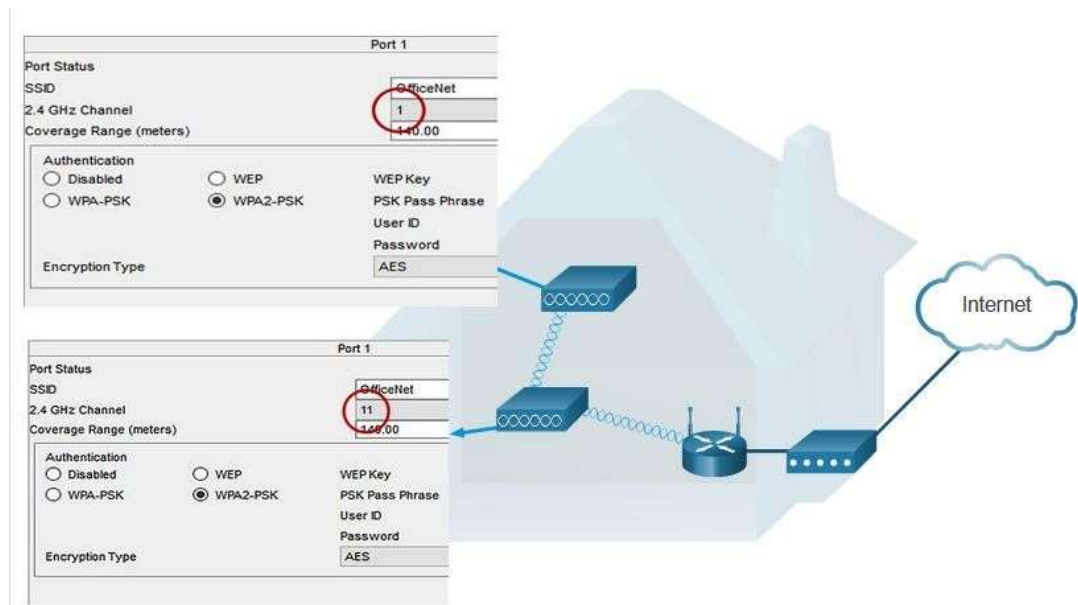
- Configure the passphrase.

WPA2 personal menggunakan frasa sandi untuk mengautentikasi klien nirkabel. WPA2 personal lebih mudah digunakan di lingkungan kantor atau rumah kecil karena tidak memerlukan server otentikasi. Organisasi yang lebih besar menerapkan WPA2 enterprise dan mengharuskan klien nirkabel untuk mengautentikasi dengan nama pengguna kata sandi.



## 5. CONFIGURE A WIRELESS MESH NETWORK

Dalam jaringan kantor atau rumah kecil, satu router nirkabel mungkin cukup untuk menyediakan akses nirkabel ke semua klien. Namun, jika Anda ingin memperluas jangkauan di luar sekitar 45 meter di dalam ruangan dan 90 meter di luar ruangan, Anda dapat menambahkan titik akses nirkabel. Seperti yang ditunjukkan dalam jaringan jala nirkabel dalam gambar, dua titik akses dikonfigurasi dengan pengaturan WLAN yang sama dari contoh kami sebelumnya. Perhatikan bahwa saluran yang dipilih adalah 1 dan 11 sehingga titik akses tidak mengganggu saluran 6 yang dikonfigurasi sebelumnya pada router nirkabel.



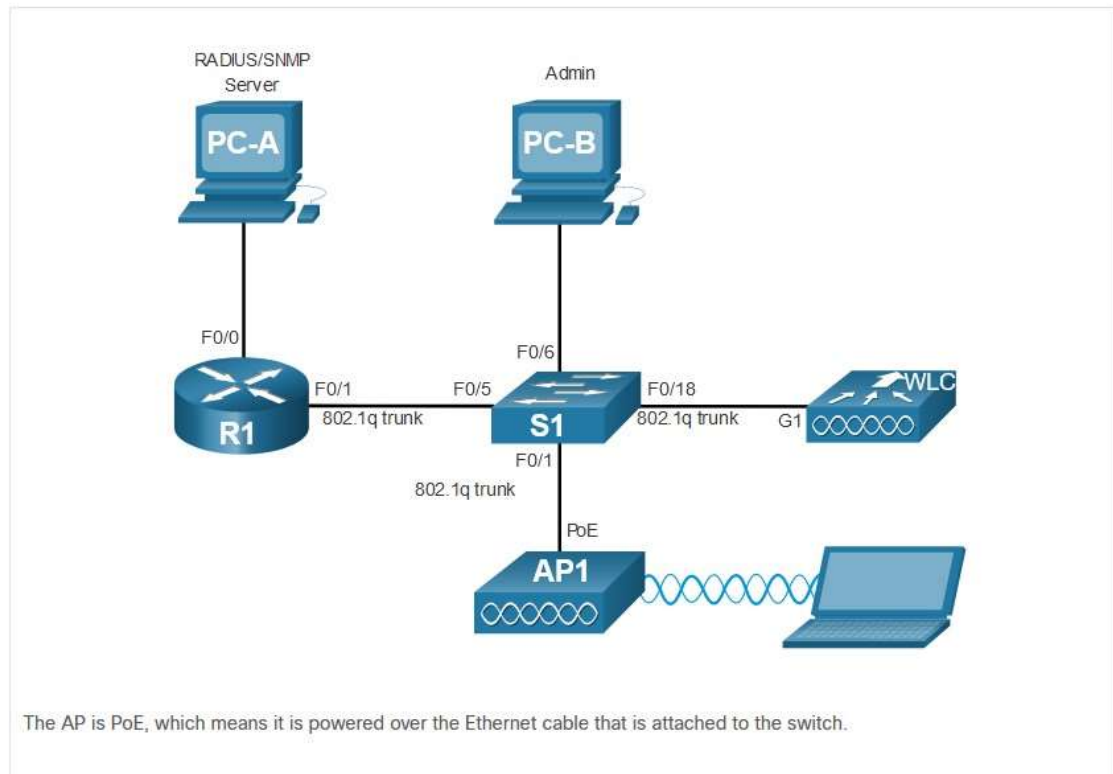
Memperpanjang WLAN di kantor kecil atau rumah menjadi semakin mudah. Produsen telah membuat pembuatan jaringan jaring nirkabel (WMN) sederhana melalui aplikasi smartphone. Anda membeli sistem, menyebarkan titik akses, menyambungkannya, mengunduh aplikasi, dan mengonfigurasi WMN Anda dalam beberapa langkah. Cari di internet untuk "best wi-fi mesh network system" untuk menemukan review tentang penawaran saat ini.

## 6. CONFIGURE A BASIC WLAN ON THE WLC

### 1. WLC Topology

Skema topologi dan alamat yang digunakan untuk video dan topik ini ditampilkan dalam gambar dan tabel. Titik akses (AP) adalah AP berbasis pengontrol dibandingkan dengan AP otonom. Ingat bahwa APs berbasis pengontrol tidak memerlukan konfigurasi awal dan sering disebut APs (LAP) ringan. LAP menggunakan Lightweight Access Point Protocol (LWAPP) untuk berkomunikasi dengan pengontrol WLAN (WLC). APs berbasis pengontrol berguna dalam situasi di mana banyak APs diperlukan dalam jaringan. Karena lebih banyak APs ditambahkan, setiap AP secara otomatis dikonfigurasi dan dikelola oleh WLC.

#### Topology



#### Addressing Table

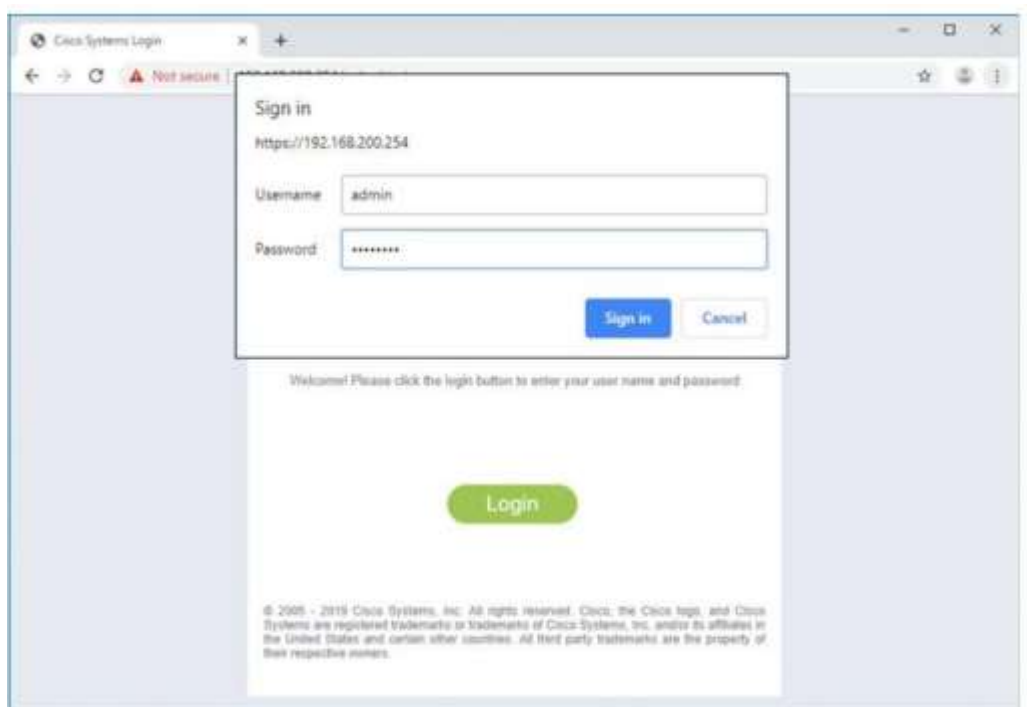
Device	Interface	IP Address	Subnet Mask
R1	F0/0	172.16.1.1	255.255.255.0
R1	F0/1.1	192.168.200.1	255.255.255.0
S1	VLAN 1	DHCP	
WLC	Management	192.168.200.254	255.255.255.0
AP1	Wired 0	192.168.200.3	255.255.255.0
PC-A	NIC	172.16.1.254	255.255.255.0
PC-B	NIC	DHCP	
Wireless Laptop	NIC	DHCP	

## 2. LOG IN TO THE WLC

Mengonfigurasi kontroler LAN nirkabel (WLC) tidak jauh berbeda dengan mengonfigurasi router nirkabel. Perbedaan besarnya adalah bahwa WLC mengontrol APs dan menyediakan lebih banyak layanan dan kemampuan manajemen, banyak di antaranya berada di luar lingkup modul ini.

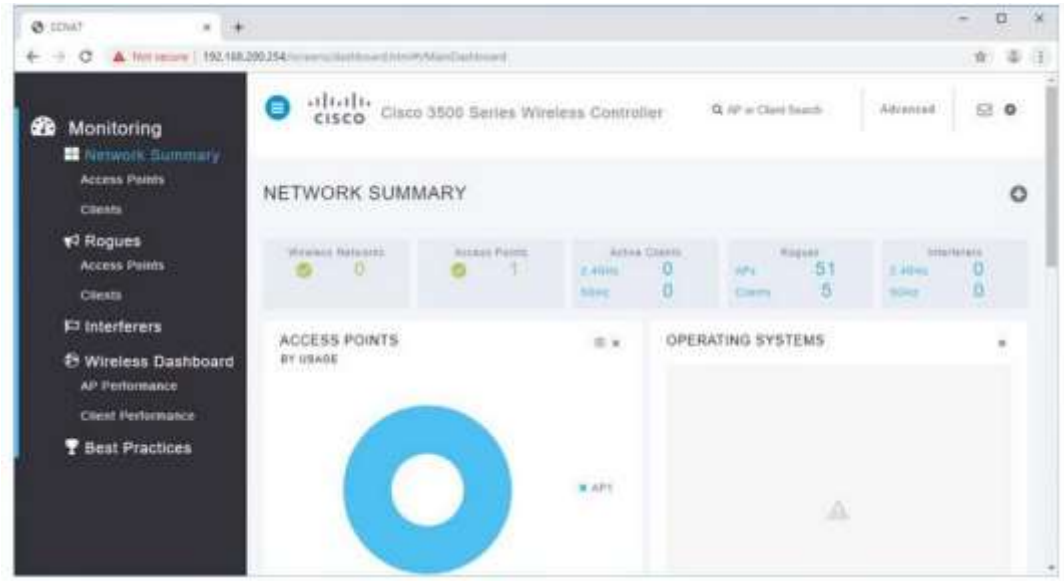
**Catatan:** Angka-angka dalam topik ini yang menunjukkan interface pengguna grafis (GUI) dan menu berasal dari Pengontrol Nirkabel Cisco 3504. Namun, model WLC lainnya akan memiliki menu dan fitur serupa.

Gambar menunjukkan pengguna masuk ke WLC dengan kredensial yang dikonfigurasi selama pengaturan awal.



**Network Summary** adalah halaman dasbor yang menyediakan gambaran umum singkat tentang jumlah jaringan nirkabel yang dikonfigurasi, titik akses terkait (APs), dan klien

aktif. Anda juga dapat melihat jumlah titik akses nakh dan klien, seperti yang ditunjukkan pada gambar.



### 3.VIEW AP INFORMATION

Klik **Access Point** dari menu kiri untuk menampilkan gambaran keseluruhan informasi dan kinerja sistem AP, seperti yang diperlihatkan pada gambar berikutnya. AP menggunakan alamat IP 192.168.200.3. Karena Cisco Discovery Protocol (CDP) aktif di jaringan ini, WLC tahu bahwa AP terhubung ke port FastEthernet 0/1 pada switch.



AP dalam topologi ini adalah Cisco Aironet 1815i yang berarti Anda dapat menggunakan baris perintah dan sekumpulan perintah IOS yang akrab. Dalam contoh, administrator jaringan melakukan ping gateway default, ping WLC, dan memverifikasi antarmuka berkabel.

```

AP1# ping 192.168.200.1
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1069812.242/1071814.785/1073817.215 ms
AP1# ping 192.168.200.254
Sending 5, 100-byte ICMP Echos to 192.168.200.254, timeout is 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1055820.953/1057820.738/1059819.928 ms
AP1# show interface wired 0
wired0    Link encap:Ethernet  HWaddr 2C:4F:52:60:37:E8
          inet addr:192.168.200.3  Bcast:192.168.200.255  Mask:255.255.255.255
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:2478 errors:0 dropped:3 overruns:0 frame:0
          TX packets:1494 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:80
          RX bytes:207632 (202.7 KiB)  TX bytes:300872 (293.8 KiB)

AP1#

```

#### 4.ADVANCED SETTINGS

Sebagian besar WLC akan datang dengan beberapa pengaturan dasar dan menu yang dapat diakses pengguna dengan cepat untuk mengimplementasikan berbagai konfigurasi umum. Namun, sebagai administrator jaringan, Anda biasanya akan mengakses pengaturan tingkat lanjut. Untuk Pengontrol Nirkabel Cisco 3504, klik Tingkat Lanjut di sudut kanan atas untuk mengakses halaman Ringkasan tingkat lanjut, seperti yang ditunjukkan pada gambar. Dari sini, Anda dapat mengakses semua fitur WLC.



#### 5.CONFIGURE A WLAN

Pengontrol LAN Nirkabel memiliki porta dan interface. Port adalah soket untuk koneksi fisik ke jaringan kabel. Mereka menyerupai port switch. Interfacenya virtual. Mereka dibuat dalam perangkat lunak dan sangat mirip dengan interface VLAN. Bahkan, setiap interface yang akan membawa lalu lintas dari WLAN dikonfigurasi pada WLC sebagai VLAN yang berbeda. Cisco 3504 WLC dapat mendukung 150 titik akses dan 4096 VLAN, namun hanya memiliki lima port fisik, seperti yang ditunjukkan pada angka tersebut. Ini berarti bahwa setiap port fisik dapat mendukung banyak APs dan WLAN. Port pada WLC pada dasarnya adalah port bagasi yang dapat membawa lalu lintas dari beberapa VLAN ke switch untuk distribusi ke beberapa APs. Setiap AP dapat mendukung beberapa WLAN.





Basic WLAN configuration on the WLC includes the following steps:

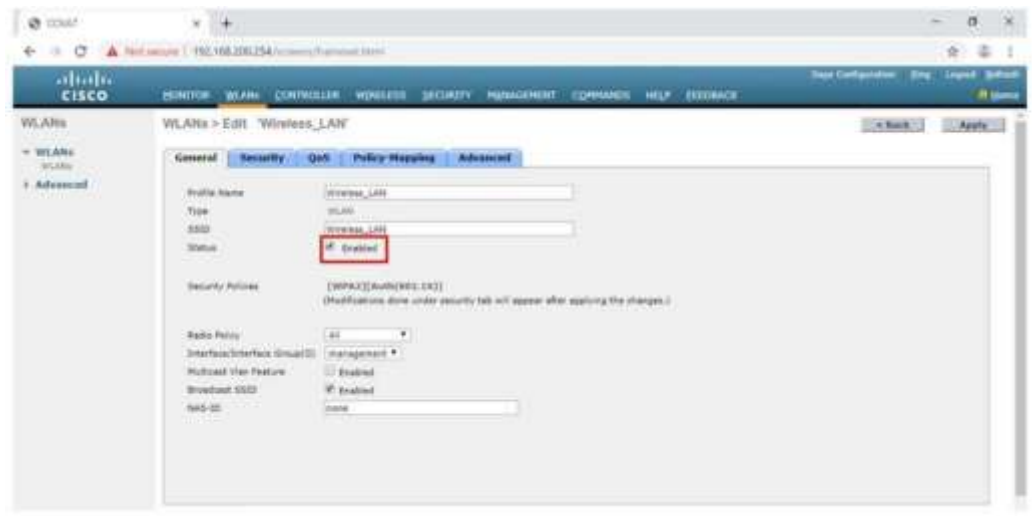
## 1. CREATE THE WLAN

Dalam gambar tersebut, administrator membuat WLAN baru yang akan menggunakan Wireless\_LAN nama dan service set identifier (SSID). ID adalah nilai sewenang-wenang yang digunakan untuk mengidentifikasi WLAN dalam output tampilan pada WLC.



## 2. APPLY AND ENABLE THE WLAN

Setelah mengklik Terapkan, administrator jaringan harus mengaktifkan WLAN sebelum dapat diakses oleh pengguna, seperti yang ditunjukkan pada gambar. Kotak centang Aktifkan memungkinkan administrator jaringan untuk mengonfigurasi berbagai fitur untuk WLAN, serta WLAN tambahan, sebelum mengaktifkannya untuk akses klien nirkabel. Dari sini, administrator jaringan dapat mengonfigurasi berbagai pengaturan untuk WLAN termasuk keamanan, QoS, kebijakan, dan pengaturan lanjutan lainnya.



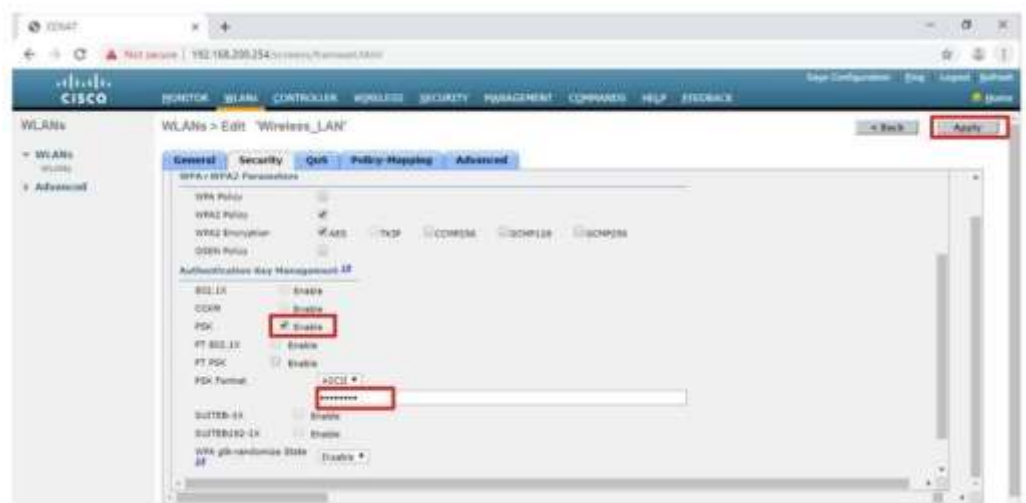
### 3. SELECT THE INTERFACE

Ketika Anda membuat WLAN, Anda harus memilih interface yang akan membawa lalu lintas WLAN. Gambar berikutnya menunjukkan pemilihan interface yang telah dibuat di WLC. Kami akan mempelajari cara membuat interface nanti dalam modul ini.



### 4. SECURE THE WLAN

Klik tab Keamanan untuk mengakses semua opsi yang tersedia untuk mengamankan LAN. Administrator jaringan ingin mengamankan Layer 2 dengan WPA2-PSK. WPA2 dan 802.1X ditetapkan secara default. Dalam kotak turun bawah Keamanan Lapisan 2, verifikasi bahwa WPA+WPA2 dipilih (tidak ditampilkan). Klik PSK dan masukkan kunci yang telah dibagikan, seperti yang ditunjukkan pada gambar. Lalu klik Terapkan. Ini akan memungkinkan WLAN dengan otentikasi WPA2-PSK. Klien nirkabel yang mengetahui kunci pre-shared mengautentikasi dengan AP.



### 5. VERIFY THE WLAN IS OPERATIONAL

Klik WLAN di menu sebelah kiri untuk melihat WLAN yang baru dikonfigurasi. Dalam gambar, Anda dapat memverifikasi bahwa WLAN ID 1 dikonfigurasi dengan Wireless\_LAN sebagai nama dan SSID, itu diaktifkan, dan menggunakan keamanan PSK WPA2.



## 6. MONITOR THE WLAN

Klik lagi tab Monitor di bagian atas untuk mengakses halaman Ringkasan tingkat lanjut. Di sini Anda dapat melihat bahwa Wireless\_LAN sekarang memiliki satu klien menggunakan layanannya, seperti yang ditunjukkan pada gambar.



## 7. VIEW WIRELESS CLIENT INFORMATION

Klik Klien di menu kiri untuk melihat informasi selengkapnya tentang klien yang terhubung ke WLAN, seperti yang ditunjukkan pada gambar. Satu klien dilampirkan ke Wireless\_LAN melalui AP1 dan diberi alamat IP 192.168.5.2. Layanan DHCP dalam topologi ini disediakan oleh router.



## PRE-PRAKTIKUM

Download file Packet Tracer pada link di bawah ini :

<https://bit.ly/jarkom2022UMM>

Praktikum dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah dibawah. Pengerjaan praktikum diselesaikan sebelum berlangsungnya kegiatan praktikum. Ketika jam praktikum berlangsung praktikan menyiapkan hasil pengerjaannya yang kemudian di demokan ke asisten.

## CONFIGURE A WIRELESS NETWORK

### OBJECTIVES

- Connect to a wireless router
- Configure the wireless router
- Connect a wired device to the wireless router
- Connect a wireless device to the wireless router
- Add an AP to the network to extend wireless coverage
- Update default router settings

In this activity, you will configure a wireless router and an access point to accept wireless clients and route IP packets. Furthermore, you will also update some of the default settings.

### Instructions

## PART 1: CONNECT TO A WIRELESS ROUTER

### STEP 1: CONNECT ADMIN TO WR.

- Connect **Admin** to **WR** using a straight-through Ethernet cable through the Ethernet ports. Select **Connections**, represented by a lightning bolt, from the bottom-left side of Packet Tracer. Click **Copper Straight-Through**, represented by a solid black line.
- When the cursor changes to connection mode, click **Admin** and choose **FastEthernet0**. Click **WR** and choose an available Ethernet port to connect the other end of the cable.

**WR** will act as a switch to the devices connected to the LAN and as a router to the internet. **Admin** is now connected to the LAN (**GigabitEthernet 1**). When Packet Tracer displays green triangles on both sides of the connection between **Admin** and **WR**, continue to the next step.

**Note:** If no green triangles are shown, make sure to enable **Show Link Lights** under **Options > Preferences**. You may also click **Fast Forward Time** just above the **Connections** selection box in the yellow bar.

### STEP 2: CONFIGURE ADMIN TO USE DHCP.

To reach the **WR** management page, **Admin** must communicate on the network. A wireless router usually includes a DHCP server, and the DHCP server is usually enabled by default on the LAN. **Admin** will receive IP address information from the DHCP server on **WR**.

- Click **Admin**, and select the **Desktop** tab.
- Click **IP Configuration** and select **DHCP**.

What is the IP address of the computer?

What is the subnet mask of the computer?

What is the default gateway of the computer?

- c. Close the **IP Configuration** window.

**Note:** Values can vary within the network range due to normal DHCP operation.

### STEP 3: CONNECT TO THE WR WEB INTERFACE.

- a. In the **Desktop** tab on **Admin**, choose **Web Browser**.
- b. Enter **192.168.0.1** in the URL field to open the web configuration page of the wireless router.
- c. Use **admin** for both the username and password.
- d. Under the Network Setup heading on the **Basic Setup** page, notice the IP address range for the DHCP server.

Is the IP address for **Admin** within this range? Is it expected? Explain your answer.

### STEP 4: CONFIGURE THE INTERNET PORT OF WR.

In this step, **WR** is configured to route the packets from the wireless clients to internet. You will configure the **Internet** port on **WR** to connect to the internet.

- a. Under the **Internet Setup** at the top of the **Basic Setup** page, change the Internet IP address method from **Automatic Configuration – DHCP** to **Static IP**.
- b. Type the IP address to be assigned to the Internet interface as follows:

**Internet IP Address:** 209.165.200.225

**Subnet Mask:** 255.255.255.252

**Default Gateway:** 209.165.200.226

**DNS Server:** 209.165.201.1

- c. Scroll down the page and click **Save Settings**.

**Note:** If you get a **Request Timeout** message, close the Admin window and wait for the orange lights to turn into green triangles. Click the fast forward button to make this happen faster. Then reconnect to **WR** from **Admin's** browser using the process explained in Step 3.

- d. To verify connectivity, open a new web browser and navigate to **www.cisco.pka** server.

**Note** It may take a few seconds for the network to converge. Click **Fast Forward Time** or **Alt+D** to speed up the process.

---

## PART 2: CONFIGURE THE WIRELESS SETTINGS

In this activity, you will only configure the wireless settings for 2.4 GHz.

### STEP 1: CONFIGURE THE WR SSID.

- a. Navigate to the **WR** GUI interface at **192.168.0.1** in a web browser on **Admin**.
- b. Navigate to **Wireless > Basic Wireless Settings**.
- c. Change **Network Name (SSID)** to **aCompany** for only 2.4 GHz. Notice that SSIDs are case-sensitive.
- d. Change the **Standard Channel** to **6 - 2.437GHz**.

- e. For this activity, disable both 5 GHz frequencies. Leave the rest of the settings unchanged.
- f. Scroll to the bottom of the window and click **Save Settings**.

## STEP 2: CONFIGURE WIRELESS SECURITY SETTINGS.

In this step, you configure the wireless security settings using WPA2 security mode with encryption and passphrase.

- a. Navigate to **Wireless > Wireless Security**.
- b. Under the 2.4 GHz heading, select **WPA2 Personal** for the Security Mode.
- c. For the Encryption field, keep the default **AES** setting.
- d. In the Passphrase field, enter **Cisco123!** as the passphrase.
- e. Click **Save Settings**.
- f. Verify that the settings in the **Basic Wireless Settings** and **Wireless Security** pages are correct and saved.

## STEP 3: CONNECT THE WIRELESS CLIENTS.

- a. Open **Laptop1**. Select **Desktop** tab. Click **PC Wireless**.
- b. Select the **Connect** tab. Click **Refresh** as necessary. Select the Wireless Network Name **aCompany**.
- c. Enter the passphrase configured in the previous step. Enter **Cisco123!** In the pre-shared key field and click **Connect**. Close the PC Wireless window.
- d. Open a web browser and verify that you can navigate to **www.cisco.pka** server.
- e. Repeat the above steps to connect **Laptop2** to the wireless network.

---

## PART 3: CONNECT WIRELESS CLIENTS TO AN ACCESS POINT

An access point (AP) is a device that extends the wireless local area network. An access point is connected to a wired router using an Ethernet cable to project the signal to a desired location.

### STEP 1: CONFIGURE THE ACCESS POINT.

- a. Connect **Port 0** of **AP** to an available Ethernet port of **WR** using a straight-through Ethernet cable.
- b. Click **AP**. Select the **Config** tab.
- c. Under the INTERFACE heading, select **Port 1**.
- d. In the SSID field, enter **aCompany**.
- e. Select **WPA2-PSK**. Enter the passphrase **Cisco123!** In the Pass Phrase field.
- f. Keep **AES** as the default Encryption Type.

### STEP 2: CONNECT THE WIRELESS CLIENTS.

- a. Open **Laptop3**. Select **Desktop** tab. Click **PC Wireless**.
- b. Select the **Connect** tab. Click **Refresh** as necessary. Select the Wireless Network Name **aCompany** with the stronger signal (Channel 1) and click **Connect**.
- c. Open a web browser and verify that you can navigate to **www.cisco.pka** server.

## PART 4: OTHER ADMINISTRATIVE TASKS

### STEP 1: CHANGE THE WR ACCESS PASSWORD.

- On **Admin**, navigate to WR GUI interface at **192.168.0.1**.
- Navigate to **Administration > Management** and change the current **Router Password** to **cisco**.
- Scroll to the bottom of the window and click **Save Settings**.
- Use the username **admin** and the new password **cisco** when prompted to log in to the wireless router. Click **OK** to continue.
- Click **Continue** and move on to the next step.

### STEP 2: CHANGE THE DHCP ADDRESS RANGE IN WR.

In this step, you will change the internal network address from 192.168.0.0/24 to 192.168.50.0/24. When the LAN network address changes, the IP addresses on the devices in the LAN and WLAN must be renewed to receive new IP addresses before the lease is timed out.

- Navigate to **Setup > Basic Setup**.
- Scroll down the page to **Network Setup**.
- The IP address assigned to **Router IP** is 192.168.0.1. Change it to 192.168.50.1. Verify that IP address still start at .100, and there are 50 available IP addresses in the DHCP pool.
- Add **209.165.201.1** as the DNS server with the DHCP settings.
- Scroll to the bottom of the window and click **Save Settings**.
- Note that the DHCP range of addresses has been automatically updated to reflect the interface IP address change. The Web Browser will display a **Request Timeout** after a short time.  
Why?
- Close the **Admin** web browser.
- In **Admin Desktop** tab, click **Command Prompt**.
- Type **ipconfig /renew** to force **Admin** re-acquire its IP information via DHCP.  
What is the new IP address information for **Admin**?
- Verify that you can still navigate to **www.cisco.pka** server.
- Renew the IP address on other laptops to verify that you can still navigate to **www.cisco.pka** server.
- Notice that **Laptop1** connected to the **AP** instead of **WR**.

Why?



## PRAKTIKUM

Download file Packet Tracer pada link di bawah ini :

<https://bit.ly/jarkom2022UMM>

Implementasi harus dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah dibawah. Setelah selesai melakukan konfigurasi pada File Packet Tracer, simpan hasil konfigurasi tersebut, kemudian ganti nama file Packet Tracer tersebut mengikuti format Tugas-nama-nim.pka. Tugas dikumpulkan di infotech.umm.ac.id pada bagian attachment **sebelum** berlangsungnya kegiatan praktikum.

## CONFIGURE A BASIC WLAN ON THE WLC

### ADDRESSING TABLE

Device	Interface	IP Address
R-1	G0/0	172.31.1.1/24
	G0/0/1.5	192.168.5.1/24
	G0/0/1.200	192.168.200.1/24
SW-1	VLAN 200	192.168.200.100/24
LAP-1	G0	DHCP
WLC-1	Management	192.168.200.254/24
Server	NIC	172.31.1.254/24
Admin PC	NIC	192.168.200.200/24
Wireless Host	Wireless NIC	DHCP

### Objectives

In this lab, you will explore some of the features of a wireless LAN controller. You will create a new WLAN on the controller and implement security on that LAN. Then you will configure a wireless host to connect to the new WLAN through an AP that is under the control of the WLC. Finally, you will verify connectivity.

- Connect to a wireless LAN controller GUI.
- Explain some of the information that is available on the WLC Monitor screen.
- Configure a WLAN on a wireless LAN controller.
- Implement security on a WLAN.
- Configure a wireless host to connect to a wireless LAN.

### Background / Scenario

An organization is centralizing control of their wireless LAN by replacing their standalone access points with lightweight access points (LAP) and a wireless LAN controller (WLC). You will be leading this project and you want to become familiar with the WLC and any potential challenges that may occur during the project. You will configure a WLC by adding a new wireless network and securing it with WPA-2 PSK security. To test the configuration, you will connect a laptop to the WLAN and ping devices on the network.



## INSTRUCTIONS

### PART 1: MONITOR THE WLC

Wait until STP has converged on the network. You can click the Packet Tracer Fast Forward Time button to speed up the process. Continue when all link lights are green.

- Go to the desktop of **Admin PC** and open a browser. Enter the management IP address of **WLC-1** from the addressing table into the address bar. You must specify the **HTTPS** protocol.
- Click **Login** and enter these credentials: User Name: **admin**, Password: **Cisco123**. After a short delay, you will see the WLC Monitor Summary screen.

**Note:** Packet Tracer does not support the initial dashboard that has been demonstrated in this module.

- Scroll through the Monitor Summary screen.

What can be learned from this screen?

Is the WLC connected to an AP?

- Click **Detail** next to the All APs entry in the Access Point Summary section of the page. What information can you find about APs on the All APs screen?

### PART 2: CREATE A WIRELESS LAN

Now you will create a new wireless LAN on the WLC. You will configure the settings that are required for hosts to join the WLAN.

#### STEP 1: CREATE AND ENABLE THE WLAN.

- Click **WLANs** in the WLC menu bar. Locate the dropdown box in the upper right hand corner of the WLANs screen. It will say **Create New**. Click **Go** to create a new WLAN.
- Enter the **Profile Name** of the new WLAN. Use the profile name **Floor 2 Employees**. Assign an SSID of **SSID-5** to the WLAN. Hosts will need to use this SSID to join the network.
- Select the **ID** for the WLAN. This value is a label that will be used to identify the WLAN in other displays. Select a value of **5** to keep it consistent with the VLAN number and SSID. This is not a requirement but it helps with understanding the topology.
- Click **Apply** so that the settings go into effect.
- Now that the WLAN has been created, you can configure features of the network. Click **Enabled** to make the WLAN functional. It is a common mistake to accidentally skip this step.
- Choose the VLAN interface that will be used for the WLAN. The WLC will use this interface for user traffic on the network. Click the drop-down box for Interface/Interface Group (G). Select the **WLAN-5** interface. This interface was previously configured on the WLC for this activity.
- Click the **Advanced** tab.
- Scroll down to the FlexConnect portion of the page. Click to enable **FlexConnect Local Switching** and **FlexConnect Local Auth**.
- Click **Apply** to enable the new WLAN. If you forget to do this, the WLAN will not operate.

#### STEP 2: SECURE THE WLAN.

The new WLAN currently has no security in place. This WLAN will initially use WPA2-PSK security. In another activity, you will configure the WLAN to use WPA2-Enterprise, a much better solution for larger wireless networks.

- In the WLANs Edit screen for the Floor 2 Employees WLAN, click the **Security** tab. Under the **Layer 2** tab, select **WPA+WPA2** from the **Layer 2 Security** drop down box. This will reveal the WPA parameters.
- Click the checkbox next to **WPA2 Policy**. This will reveal additional security settings. Under **Authentication Key Management**, enable **PSK**.
- Now you can enter the pre-shared key that will be used by hosts to join the WLAN. Use **Cisco123** as the passphrase.
- Click **Apply** to save these settings.

**Note:** It is not a good practice to reuse passwords when configuring security. We have reused passwords in this activity to simplify configuration.

### STEP 3: VERIFY THE SETTINGS

- After Applying the configuration, click **Back**. This will take you back to the WLANs screen.  
What information about the new WLAN is available on this screen?
- If you click the WLAN ID, you will be taken to the WLANs Edit screen. Use this to verify and change the details of the settings.

---

## PART 3: CONNECT A HOST TO THE WLAN

### STEP 1: CONNECT TO THE NETWORK AND VERIFY CONNECTIVITY.

- Go to the desktop of **Wireless Host** and click the **PC Wireless** tile.
- Click the **Connect** tab. After a brief delay you should see the SSID for the WLAN appear in the table of wireless network names. Select the **SSID-5** network and click the **Connect** button.
- Enter the pre-shared key that you configured for the WLAN and click **Connect**.
- Click the **Link Information** tab. You should see a message that confirms that you have successfully connected to the access point. You should also see a wireless wave in the topology showing the connection to LAP-1.
- Click the **More Information** button to see details about the connection.
- Close the PC Wireless app and open the IP Configuration app. Verify that Wireless Host has received a non-APIPA IP address over DHCP. If not, click the Fast Forward Time button a few times.
- From Wireless Host, ping the WLAN default gateway and the Server to verify that the laptop has full connectivity.

---

### RUBRIK PENILAIAN

Pemahaman Materi	10%
Pre-praktikum	20%
Praktikum	70%