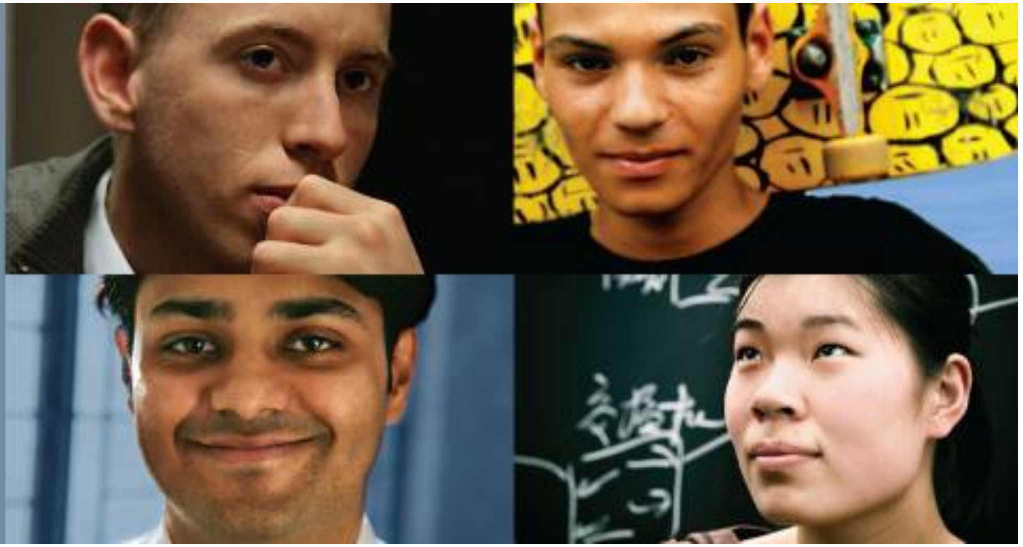
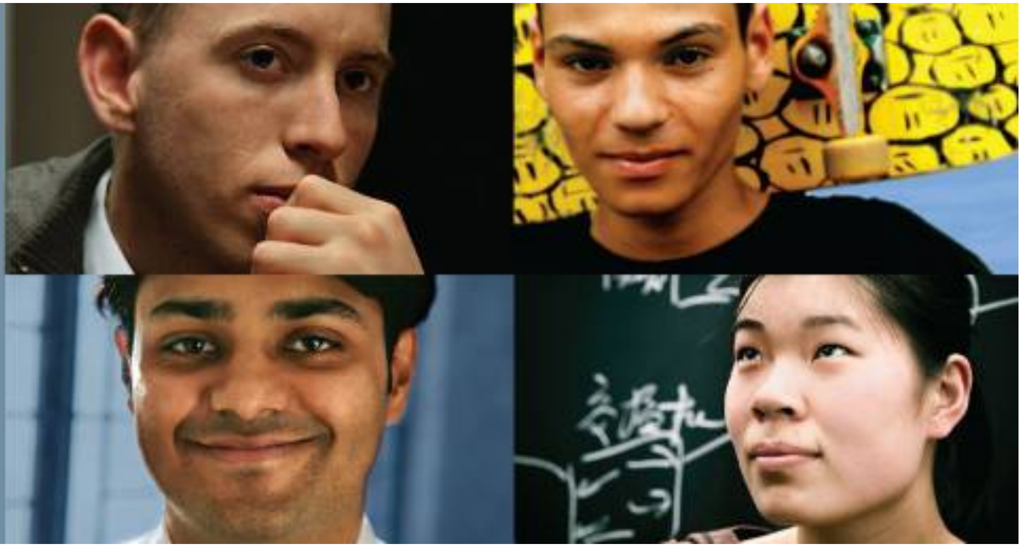
# Instructor Materials
# Chapter 6
# Building a Home Network



## Networking Essentials

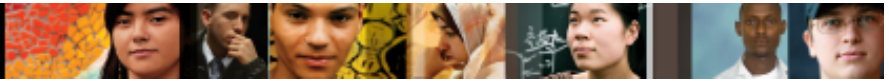
Cisco | Networking Academy®
Mind Wide Open™

# Chapter 6: Building a Home Network



## Networking Essentials

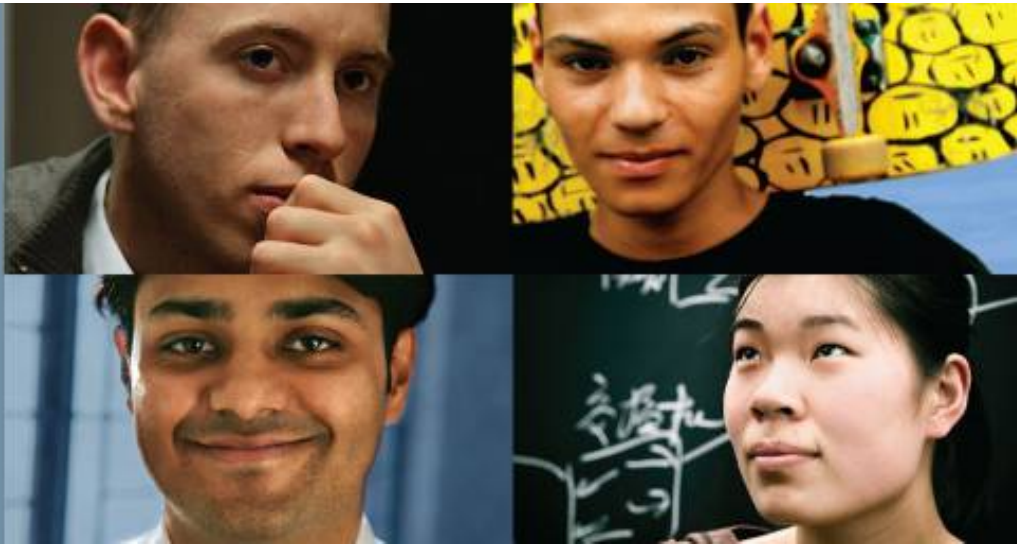
Cisco | Networking Academy®
Mind Wide Open™



# Chapter 6 - Sections & Objectives

- 6.1 What Does a Home Network Look Like?
  - Compare different types of network connections.
- 6.2 How Does Wi-Fi Work?
  - Explain how Wi-Fi functions.
- 6.3 Setting Up Your Wireless Network
  - Connect wireless PC clients to a wireless router.
- 6.4 Choosing ISP Services
  - Compare the options available for connecting to an ISP.
- 6.5 Security Considerations in a Home Network
  - Configure a wireless LAN device to protect data and the network.
- 6.6 Mobile Devices in the Network
  - Explain how to configure mobile devices to use various wireless technologies.

# 6.1 What Does a Home Network Look Like?

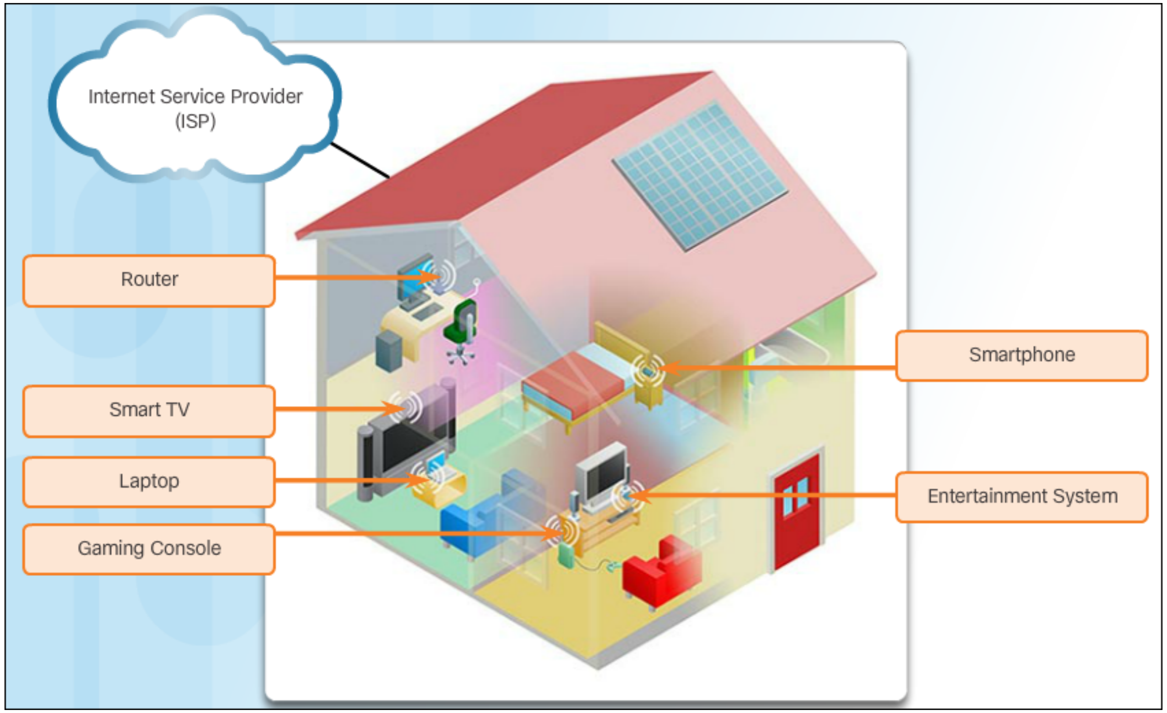


Cisco | Networking Academy®
Mind Wide Open™

### What Does a Home Network Look Like?

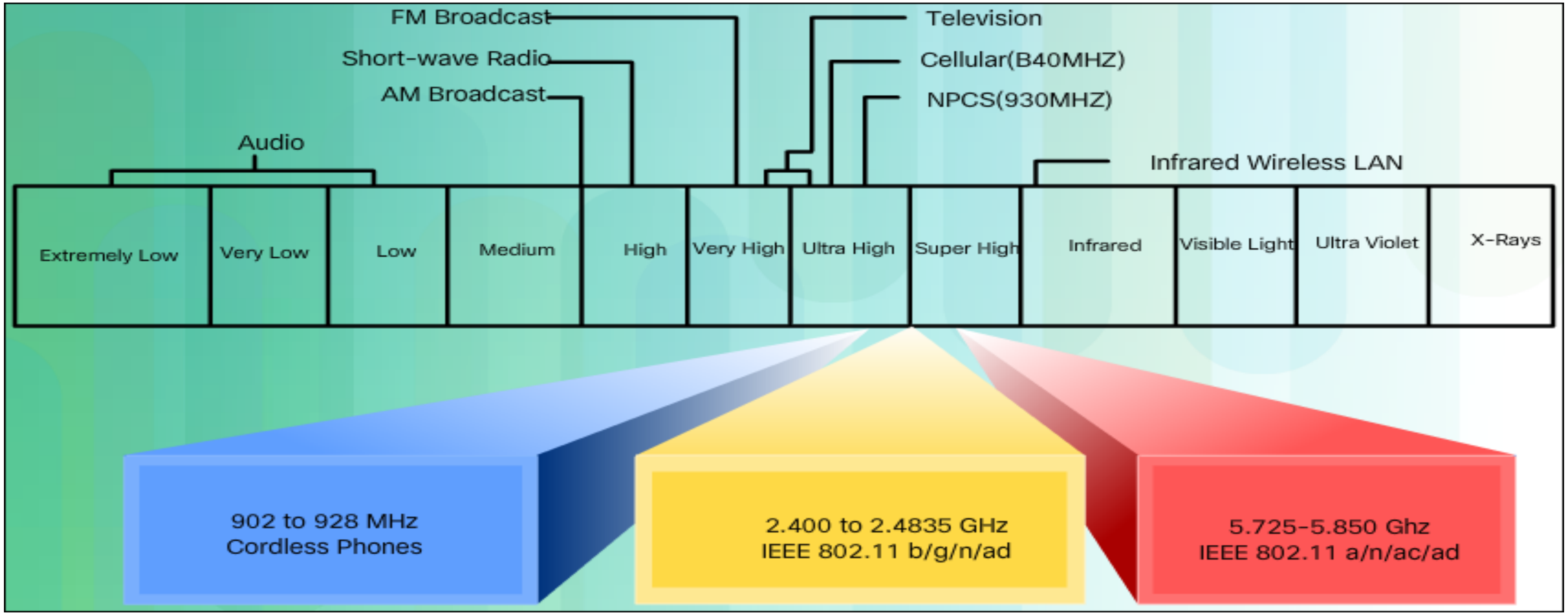
# Home Network Basics

- A home network is a small LAN with devices that connect to an integrated router. The router is connected to the Internet. Most likely, the home router is equipped with both wired and wireless capabilities.
- As new technologies come on the market, more and more household functions will rely on the network to provide connectivity and control.
- Small business and home routers typically have two primary types of ports: Ethernet ports and an Internet port.



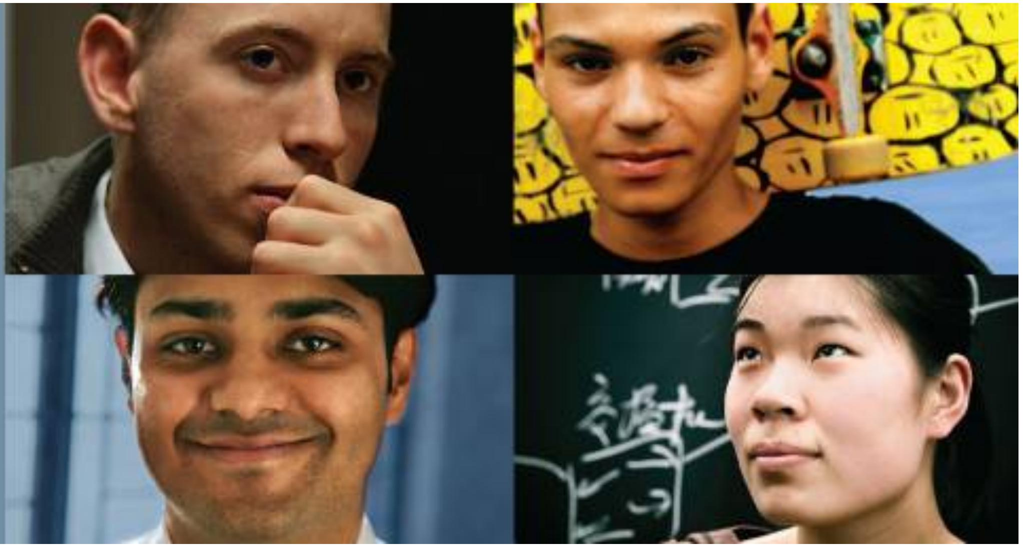
## What Does a Home Network Look Like?

# Network Technologies in the Home



- Wireless technologies use electromagnetic waves to carry information between devices.
- The wireless technologies most frequently used in home networks are in the unlicensed 2.4 GHz and 5 GHz frequency ranges.
- The most commonly implemented wired protocol is the Ethernet protocol. Ethernet uses a suite of protocols that allow network devices to communicate over a wired LAN connection.

# 6.2 How Does Wi-Fi Work?



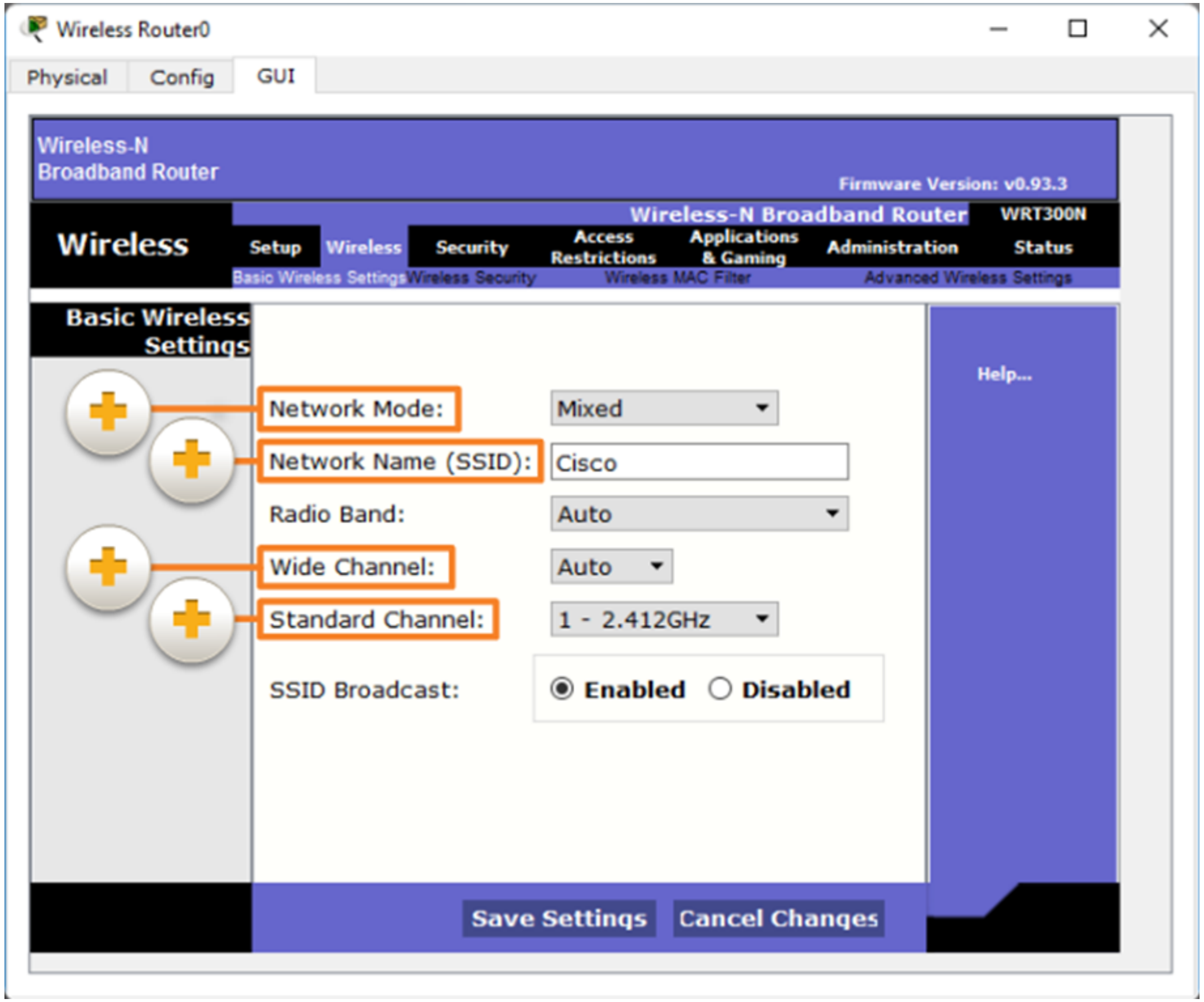
Cisco | Networking Academy®
Mind Wide Open™

## How Does Wi-Fi Work?

# Wireless Standards

- Many standards have been developed to ensure that wireless devices can communicate. The IEEE 802.11 standard governs the WLAN environment.
- Wireless routers using the 802.11 standards have many settings that have to be configured, including:
  - Network mode
  - Network Name (SSID)
  - Standard Channel
  - SSID Broadcast

Note: SSID stands for Service Set Identifier.



Network Mode: Mixed

Network Name (SSID): Cisco

Radio Band: Auto

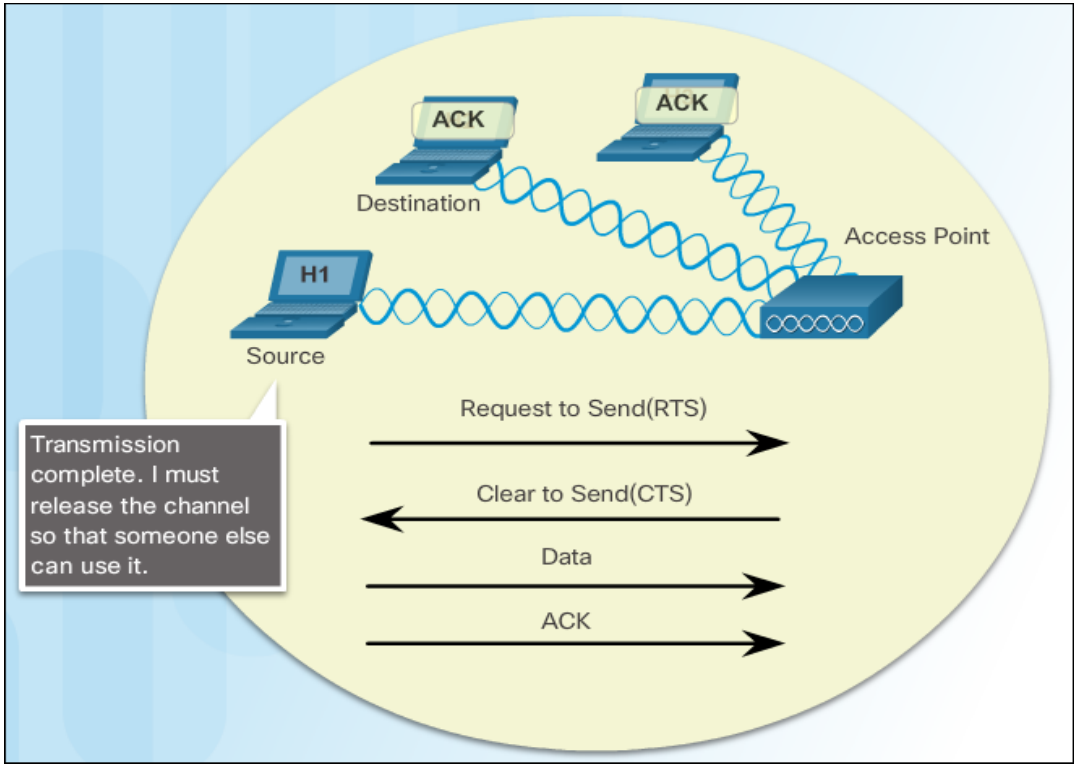
Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ● Enabled ○ Disabled

## How Does Wi-Fi Work?

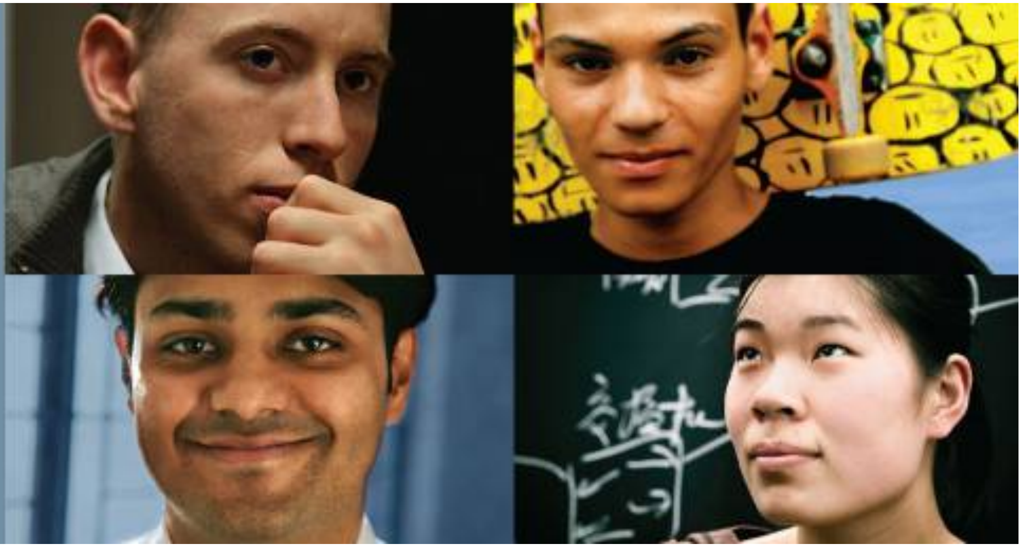
# Controlling Wireless Traffic



Transmission complete. I must release the channel so that someone else can use it.

- Wireless devices that transmit over the same frequency range create interference in a Wi-Fi network. Channels are created by dividing up the available RF spectrum. Each channel is capable of carrying a different conversation.
- Wireless technology uses an access method called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA creates a reservation on the channel for a specific conversation between devices.

# 6.3 Setting Up Your Wireless Network

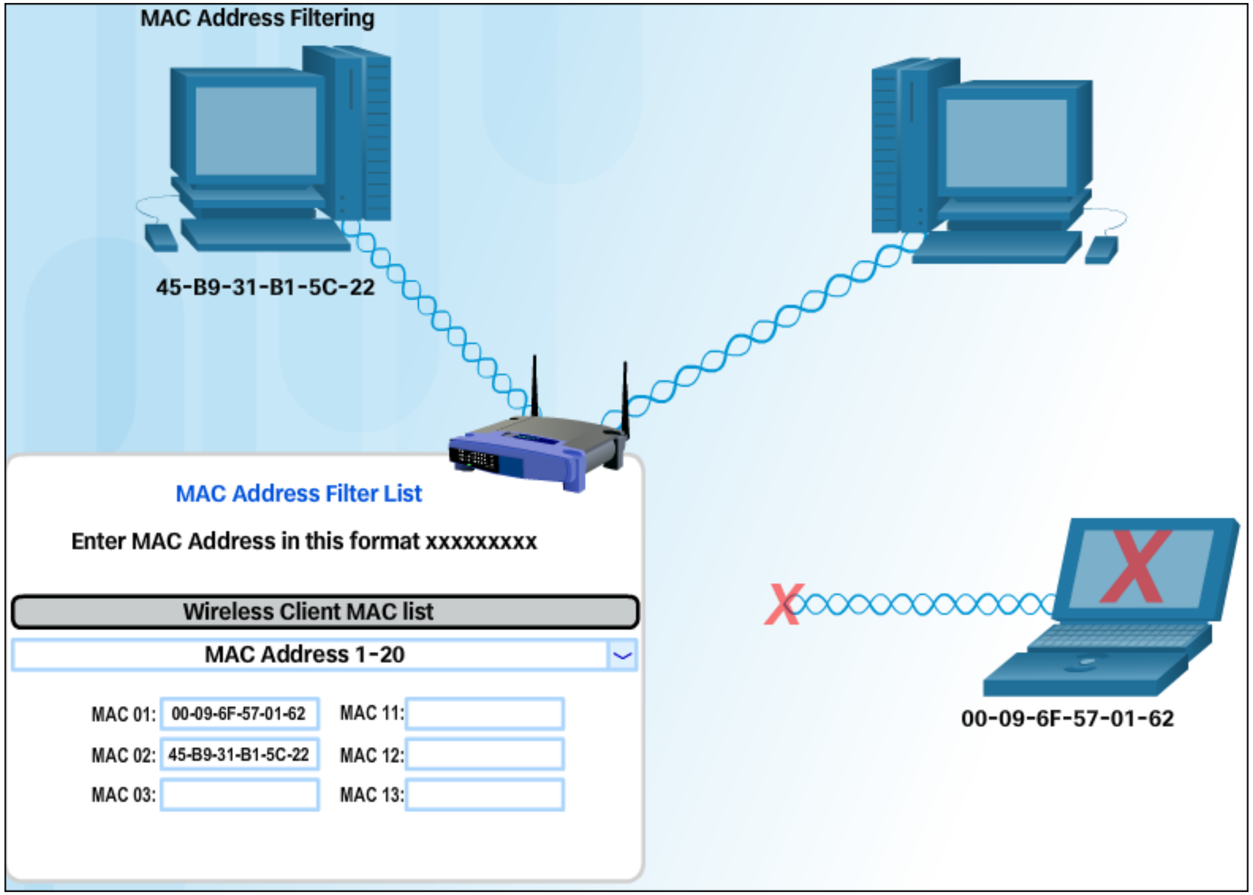


Cisco Networking Academy®
Mind Wide Open™

## Setting Up Your Wireless Network

# Accessing the Wireless Router

- Many wireless routers designed for home use have an automatic setup utility that can be used to configure the basic settings on the router.
- If SSID broadcasting is on, the SSID name will be seen by all wireless clients within your signal range.
- The decision regarding who can access your home network should be determined by how you plan to use the network. Many routers support MAC address filtering.



MAC Address Filter List

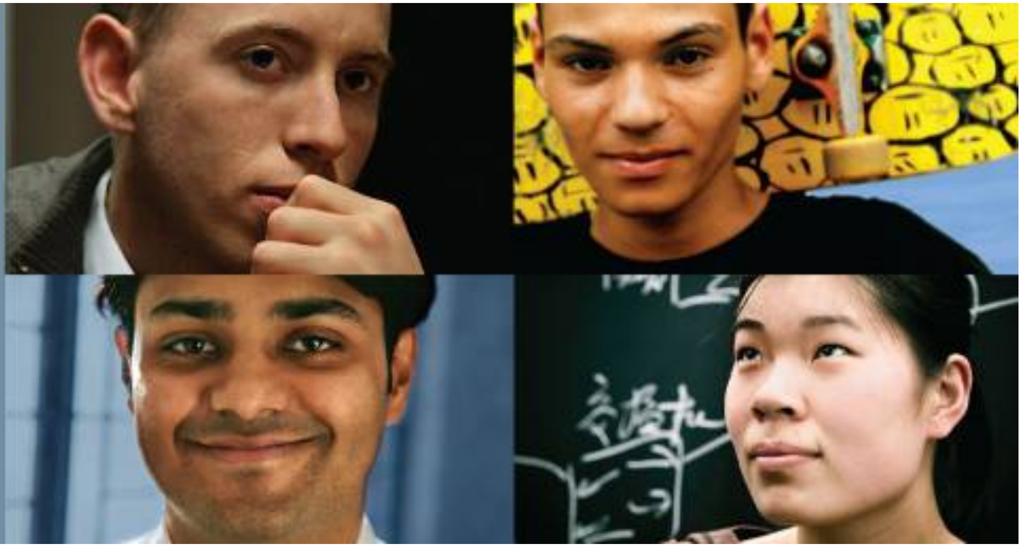
Enter MAC Address in this format xxxxxxxxx

Wireless Client MAC list

MAC Address 1-20

|  |  |  |  |
|---|---|---|---|
| MAC 01: | 00-09-6F-57-01-62 | MAC 11: |  |
| MAC 02: | 45-B9-31-B1-5C-22 | MAC 12: |  |
| MAC 03: |  | MAC 13: |  |

# 6.4 Choosing ISP Services

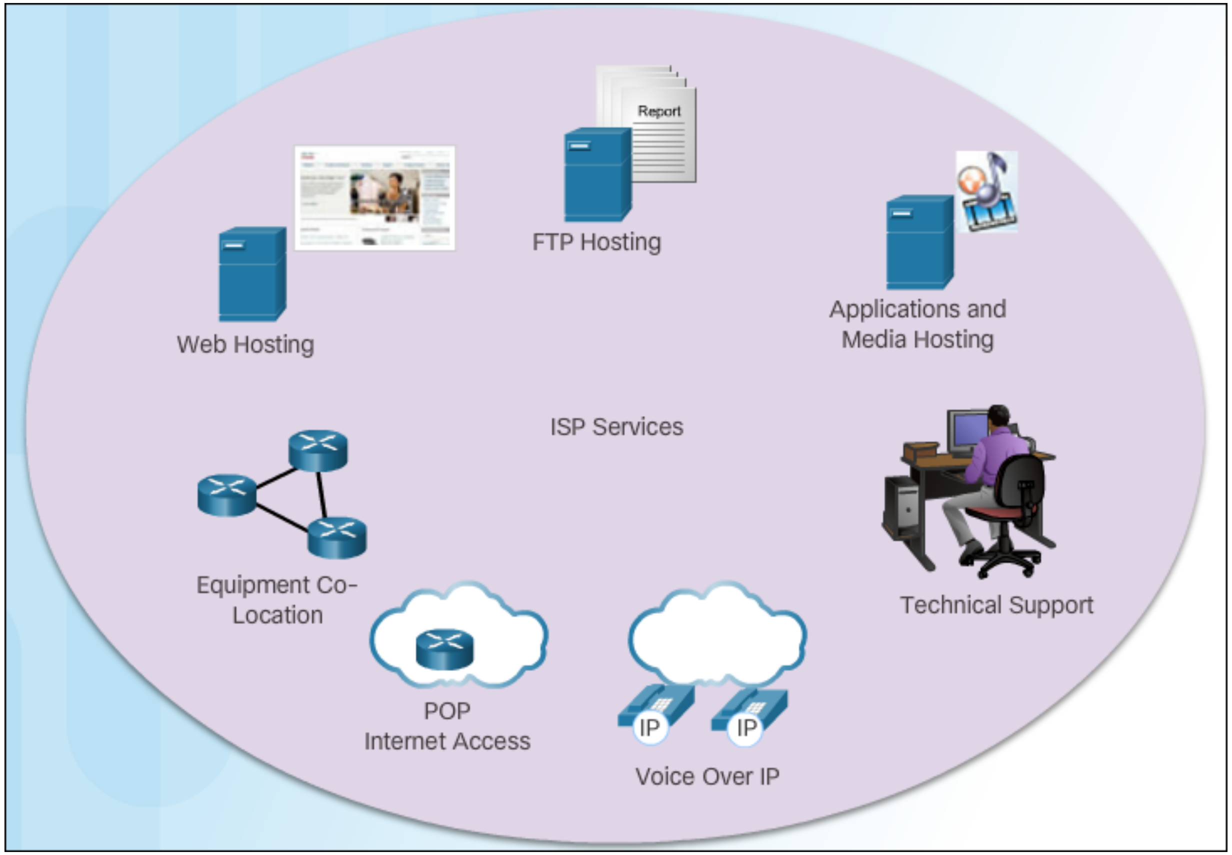


Cisco | Networking Academy®
Mind Wide Open™

### Choosing ISP Services

# Internet Service Providers

- An Internet Service Provider (ISP) provides the link between the home network and the global Internet. ISPs are critical to communications across the Internet. Each ISP connects to other ISPs to form a network of links that interconnect users all over the world.

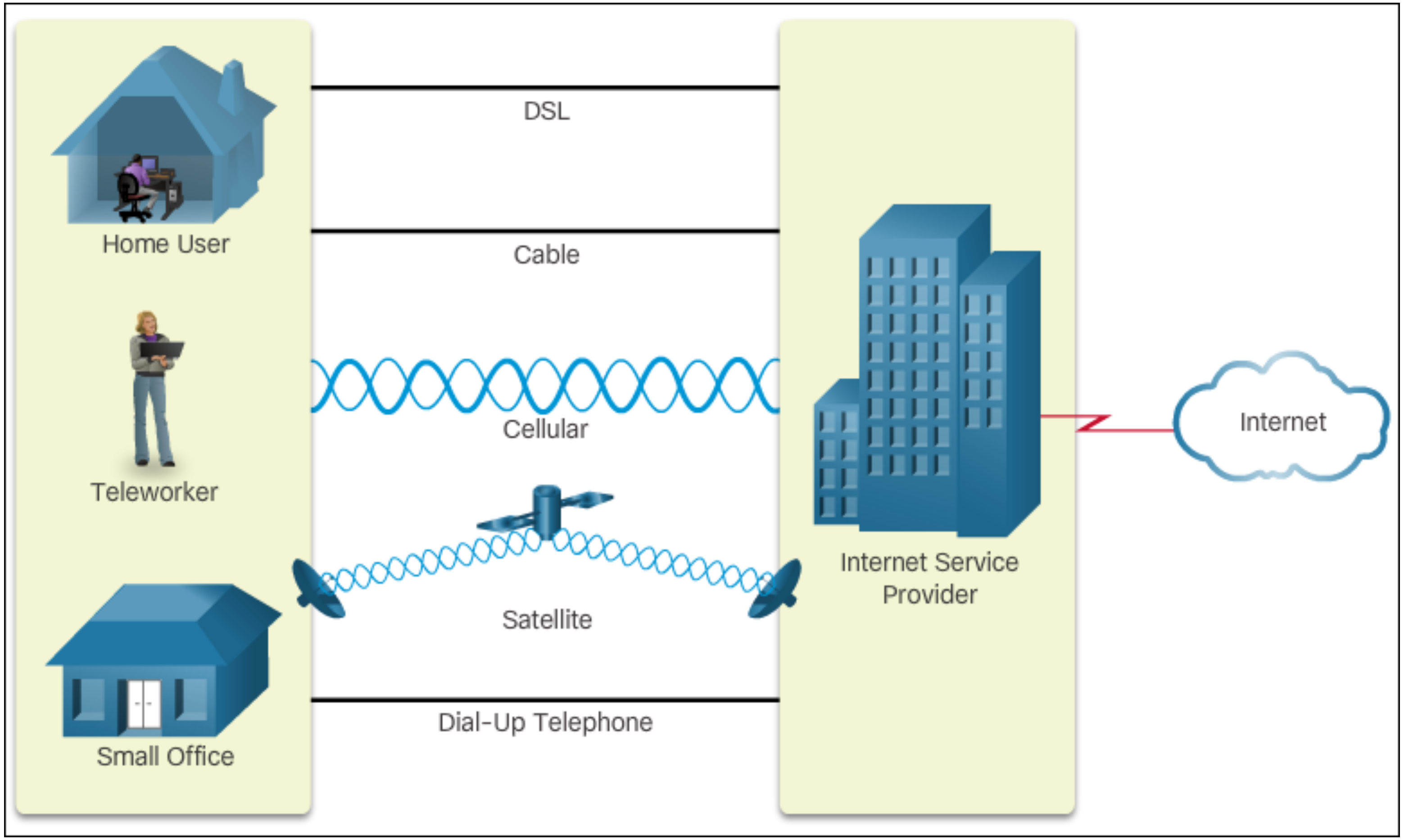


- A router is required to securely connect a computer to an ISP. The router includes a switch to connect wired hosts and a wireless AP to connect wireless hosts. The router also provides client addresses and security for inside hosts.

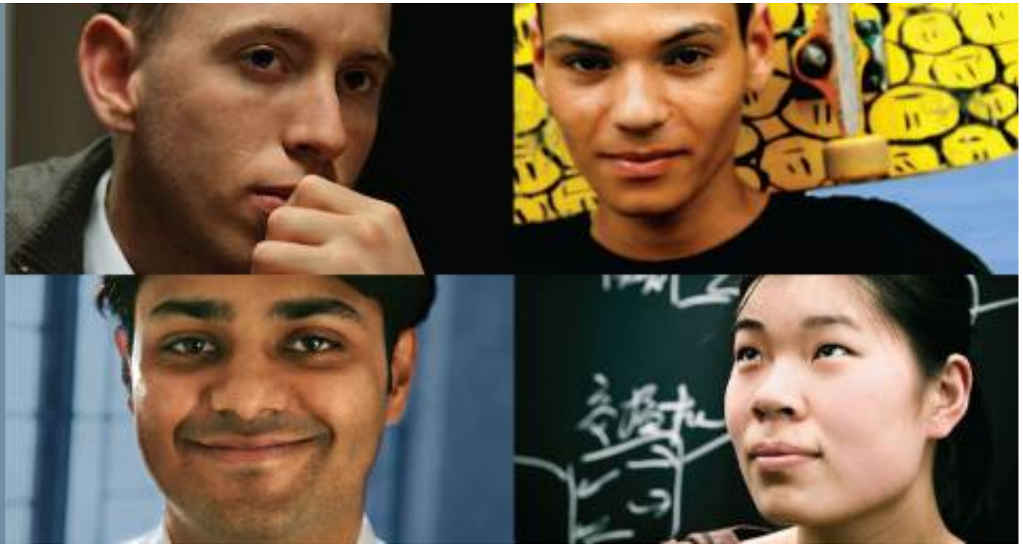
## Choosing ISP Services

# ISP Connectivity Options

- The two most common methods to connect to an ISP are Cable and Digital Subscriber Line (DSL).
- Other ISP connectivity options are Satellite, Cellular, and Dial-up Telephone.



# 6.5 Security Considerations in a Home Network

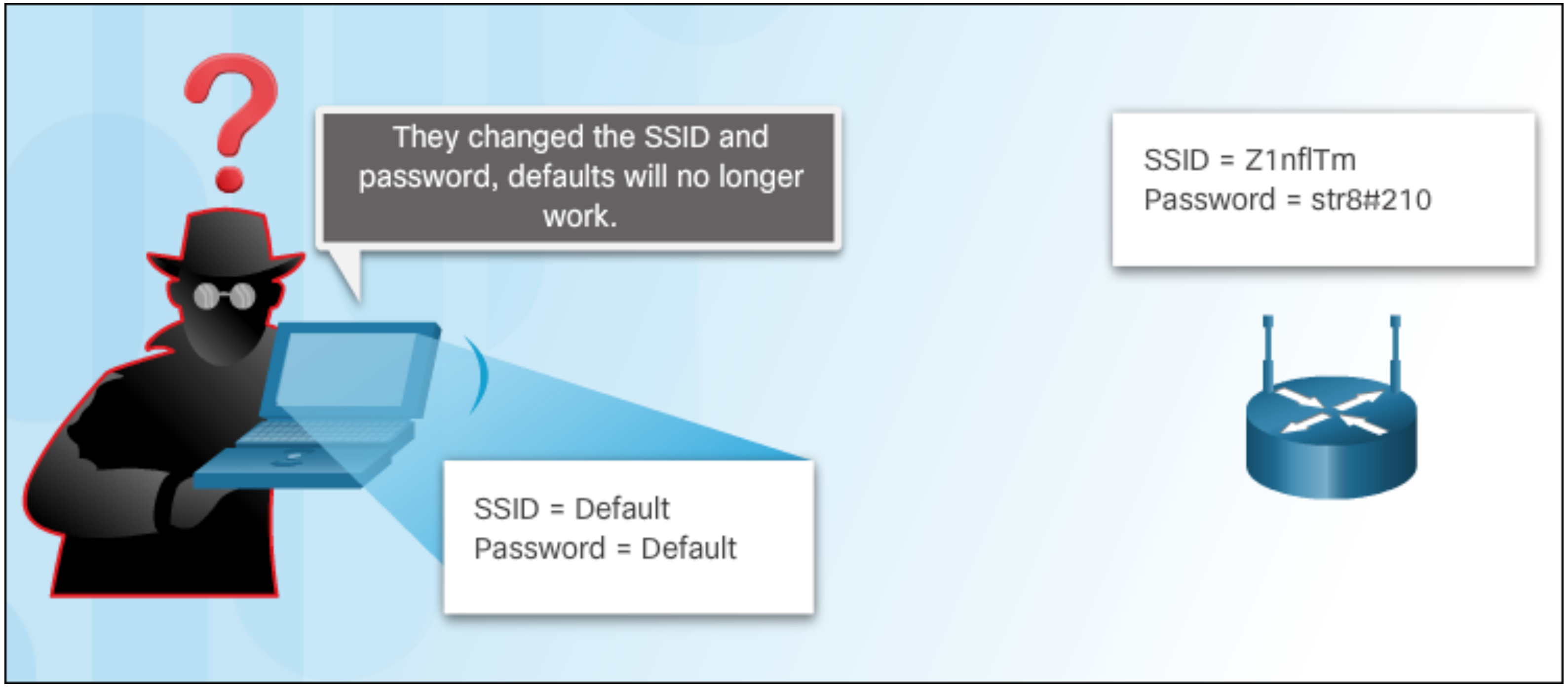


Cisco Networking Academy®
Mind Wide Open™

## Security Considerations in a Home Network

# Is My Network Safe?

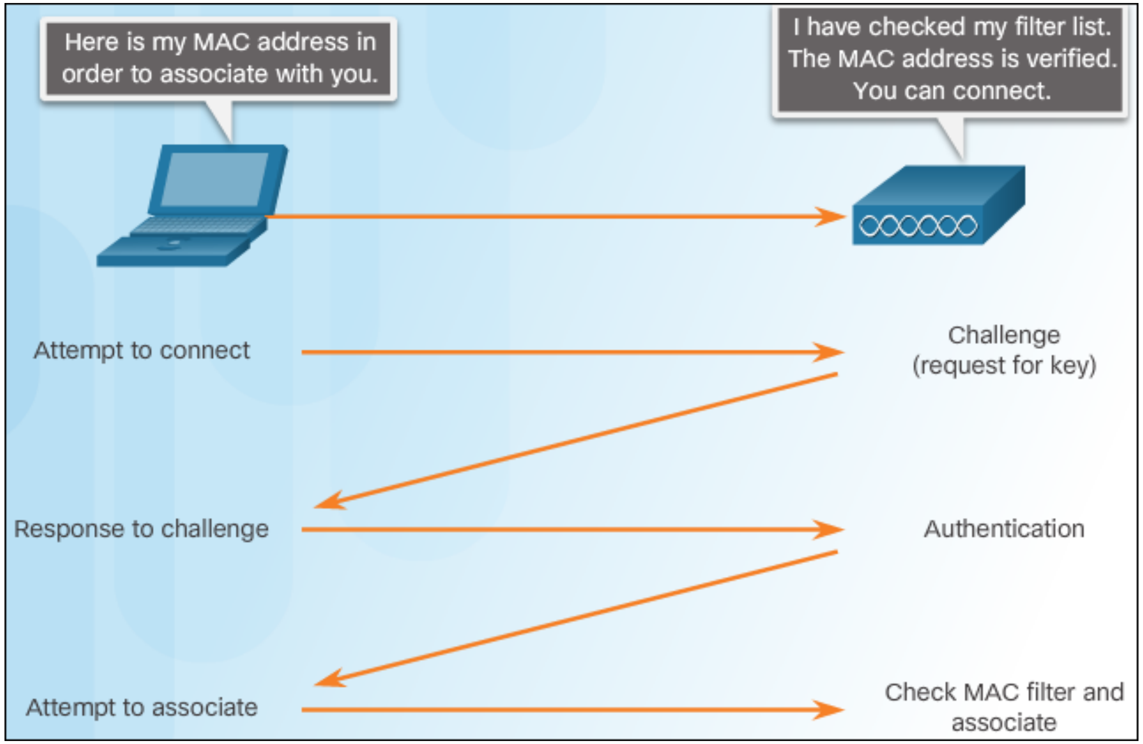
- It is possible for an attacker to tune into signals from your wireless network, much like tuning into a radio station.
- The SSID broadcast feature can be turned off. Any computer trying to connect to the network must already know the SSID. Turning off SSID broadcast alone does not protect the wireless network from experienced hackers.
- Changing the default settings on a wireless router will not protect your network by itself. It takes a combination of several methods to protect your WLAN.
- MAC address filtering uses the MAC address to identify which devices are allowed to connect to the wireless network.


They changed the SSID and password, defaults will no longer work.
SSID = Z1nflTm
Password = str8#210
SSID = Default
Password = Default

## Security Considerations in a Home Network

# Authenticating Users

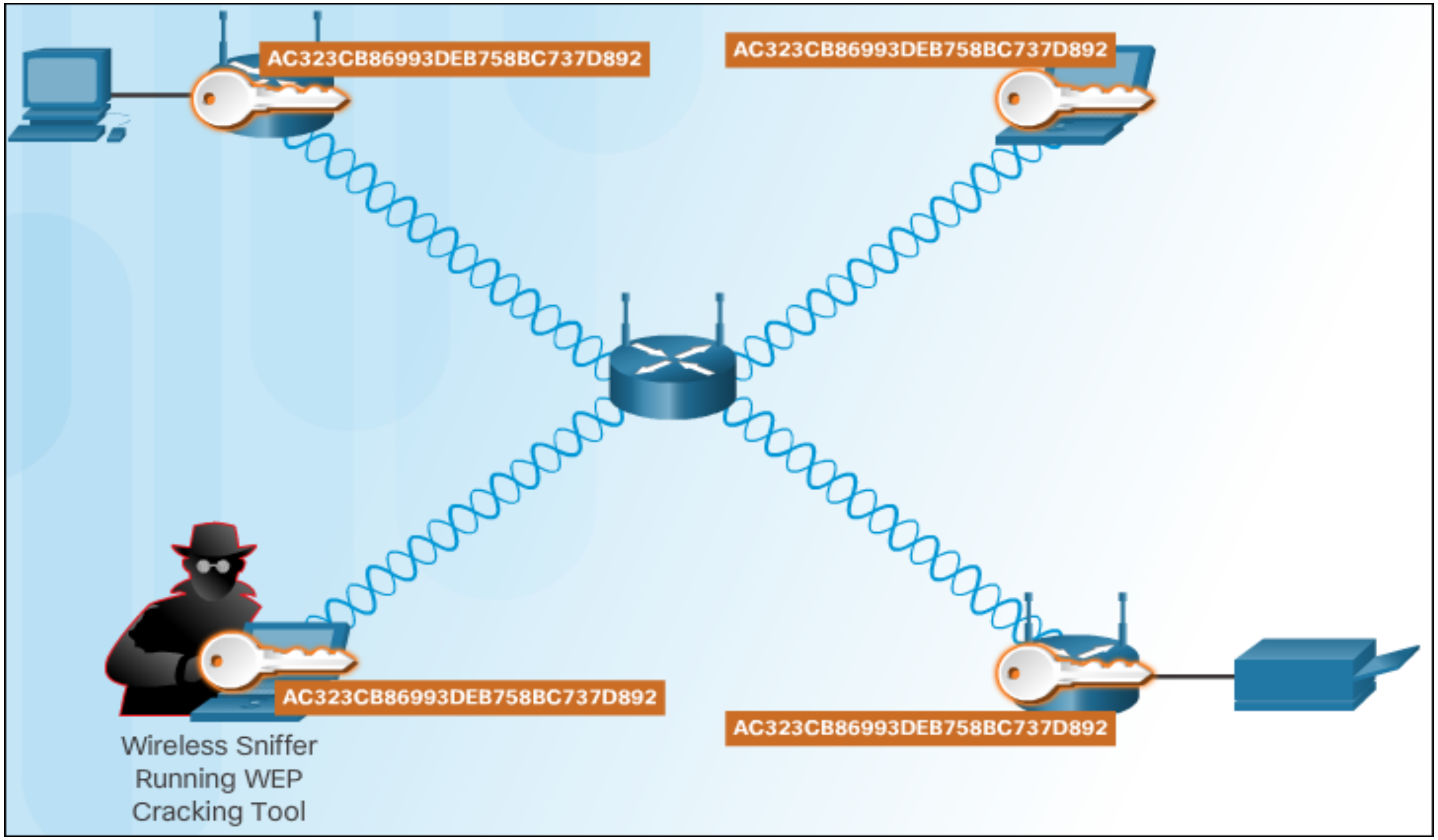
- Authentication is the process of permitting entry to a network based on a set of credentials. It is used to verify that the device attempting to connect to the network is trusted.
- After authentication is enabled, the client must successfully pass authentication before it can associate with the AP and join the network. When authentication is successful, the AP will then check the MAC address against the MAC address table. When verified, the AP adds the host MAC address into its host table.


Here is my MAC address in order to associate with you.
I have checked my filter list. The MAC address is verified. You can connect.
Attempt to connect
Challenge (request for key)
Response to challenge
Authentication
Attempt to associate
Check MAC filter and associate

Security Considerations in a Home Network

# Encrypting Data So It Cannot Be Read

- An advanced and secure form of encryption is Wi-Fi Protected Access (WPA). WPA2 uses encryption keys from 64 bits up to 256 bits. However, WPA2, unlike WEP, generates new, dynamic keys each time a client establishes a connection with the AP.

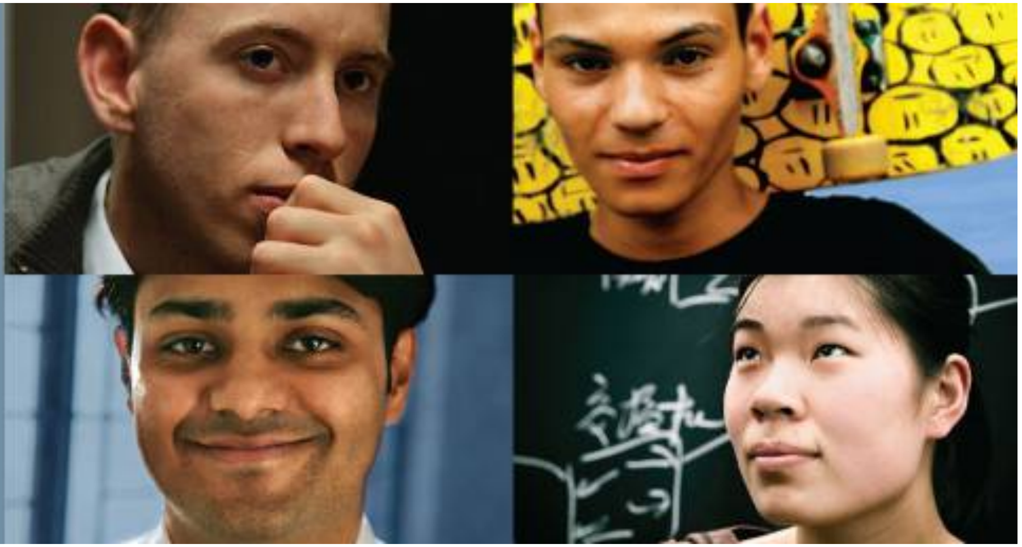

AC323CB86993DEB758BC737D892
AC323CB86993DEB758BC737D892
AC323CB86993DEB758BC737D892
AC323CB86993DEB758BC737D892
Wireless Sniffer Running WEP Cracking Tool

## Security Considerations in a Home Network

# Security Planning

- Security measures should be planned and configured before connecting the AP to the network or ISP.
- Some of the more basic security measures include:
  - Change default values for the SSID, usernames and passwords
  - Disable broadcast SSID
  - Configure MAC Address Filtering
- Some of the more advanced security measures include:
  - Configure encryption using WPA2
  - Configure authentication
  - Configure traffic filtering
- No single security measure will keep your wireless network completely secure. Combining multiple techniques will strengthen the integrity of your security plan.

# 6.6 Mobile Devices in the Network

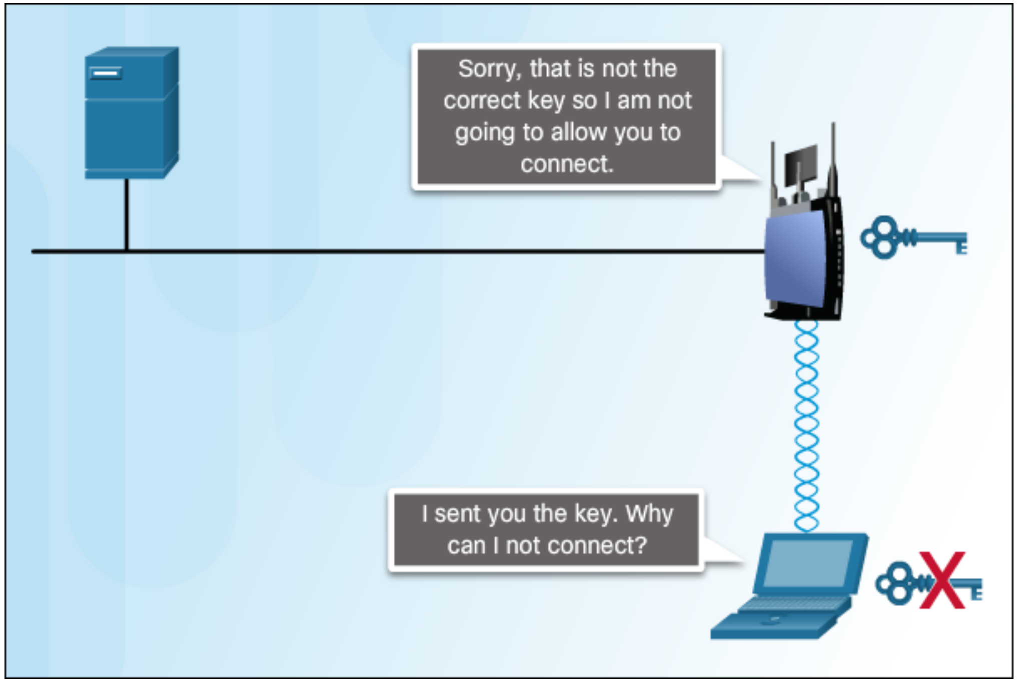


Cisco | Networking Academy®
Mind Wide Open™

## Mobile Devices in the  Network

# Network Connectivity

- These precautions should be taken to protect Wi-Fi communications on mobile devices:
  - Never send login or password information using unencrypted text (plaintext).
  - Use a VPN connection when possible if you are sending sensitive data.
  - Enable security on home networks.
  - Use WPA2 encryption for security.
- When a mobile device is out of the range of the Wi-Fi network, it attempts to connect to another Wi-Fi network in range. If no Wi-Fi networks are in range, the mobile device connects to the cellular data network.


Sorry, that is not the correct key so I am not going to allow you to connect.
I sent you the key. Why can I not connect?

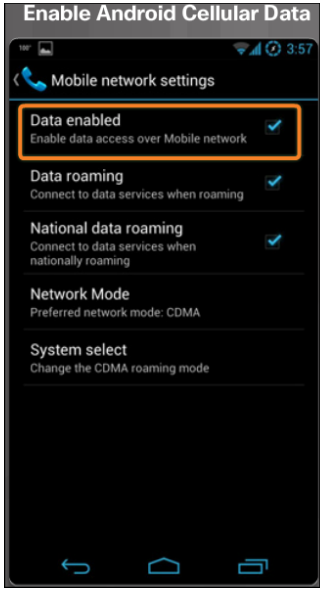
## Mobile Devices in the  Network

# Cellular Data and Bluetooth

- Mobile devices are preprogrammed to use a Wi-Fi network for Internet if one is available and the device can connect to the access point and receive an IP address. If no Wi-Fi network is available, the device uses the cellular data capability if it is configured.

- Bluetooth is wireless, automatic, and uses very little power, which helps conserve battery life. Up to eight Bluetooth devices can be connected together at any one time.

Enable Android Cellular Data



3:57

Mobile network settings

Data enabled ☑
Enable data access over Mobile network

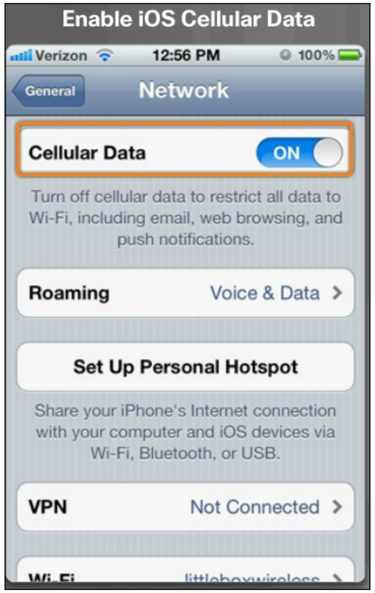
Data roaming ☑
Connect to data services when roaming

National data roaming ☑
Connect to data services when nationally roaming

Network Mode
Preferred network mode: CDMA

System select
Change the CDMA roaming mode

Enable iOS Cellular Data



Verizon 12:56 PM 100%

General | Network

Cellular Data: ON

Turn off cellular data to restrict all data to Wi-Fi, including email, web browsing, and push notifications.

Roaming: Voice & Data >

Set Up Personal Hotspot

Share your iPhone's Internet connection with your computer and iOS devices via Wi-Fi, Bluetooth, or USB.

VPN: Not Connected >

Wi-Fi: littleboxwireless >

Bluetooth Headset

Cisco | Networking Academy®

Mind Wide Open™