Mobile and Wireless Technology

CT090-3-2-MWT Version VD01

WLAN Security

Topic & Structure of The Lesson

Wireless LAN Threats and Intrusion
IEEE 802.11 Standards Security
- Open System Authentication
- Shared Key Authentication

Early WLAN Security Mechanisms
- Service Set Identifier (SSID)
- SSID Hiding
- Media Access Control (MAC) Address

Overview of other WLAN Security Standards and Technology

Learning Outcomes

ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION

At the end of this topic, You should be able to:

- Know 802.11 legacy security solutions
- Know the characteristics and features of security mechanisms, including Service Set Identifier (SSID), Media Access Control (MAC) filtering, and Wired Equivalent Privacy (WEP), and the weaknesses or vulnerabilities of each.

Key Terms You Must Be Able To Use

If you have mastered this topic, you should be able to use the following terms correctly in your assignments and exams:

- Authentication
- Encryption
- SSID
- MAC
- WEP

Wireless LAN Security - Introduction

In the early days of wireless networking, security was weak. This led to much vulnerability, which in turn made wireless networking not a very attractive solution for many enterprise deployments, especially those concerned about security.

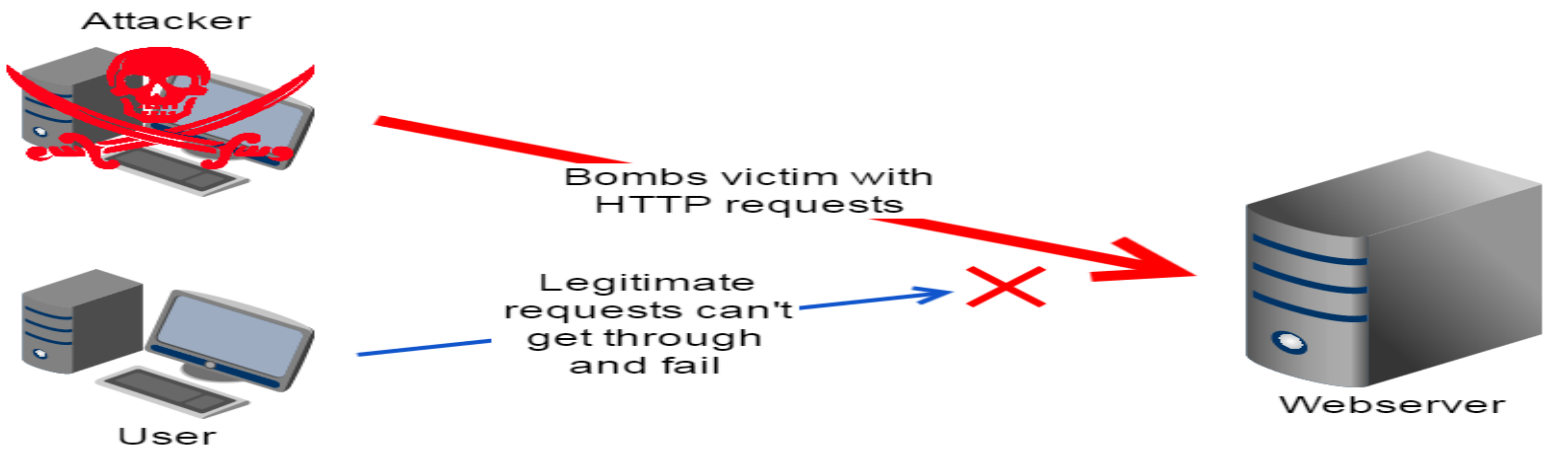
Wireless LAN Threats and Intrusion

There are many security concerns related to wireless networking. Some of these concerns and threats are as follows:

Eavesdropping - Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission.

Wireless LAN Threats and Intrusion

RF denial of service (DoS) - Denial-of-Service (DoS) attacks, which aim to prevent access to network resources, can be devastating and difficult to protect against. Typical DoS attacks involve flooding the network with traffic choking the transmission lines and preventing other legitimate users from accessing services on network.



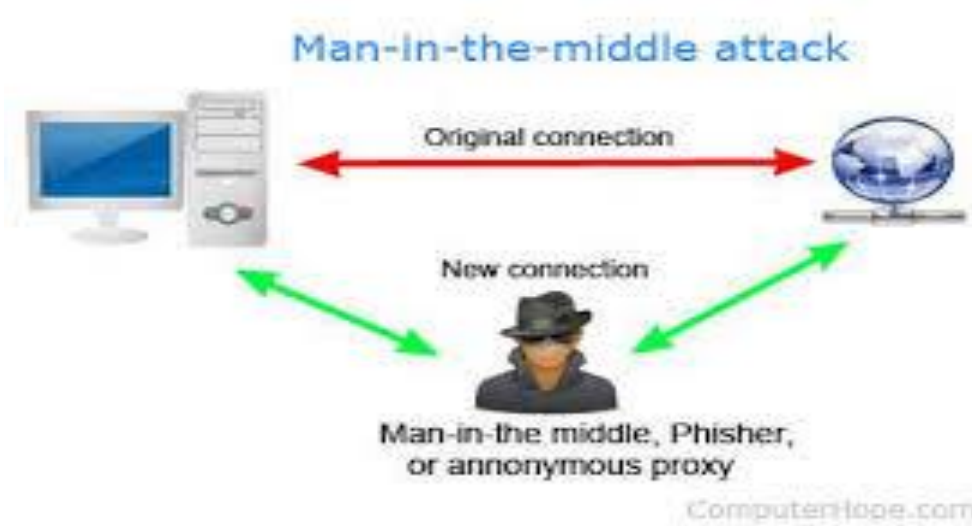
Wireless LAN Threats and Intrusion

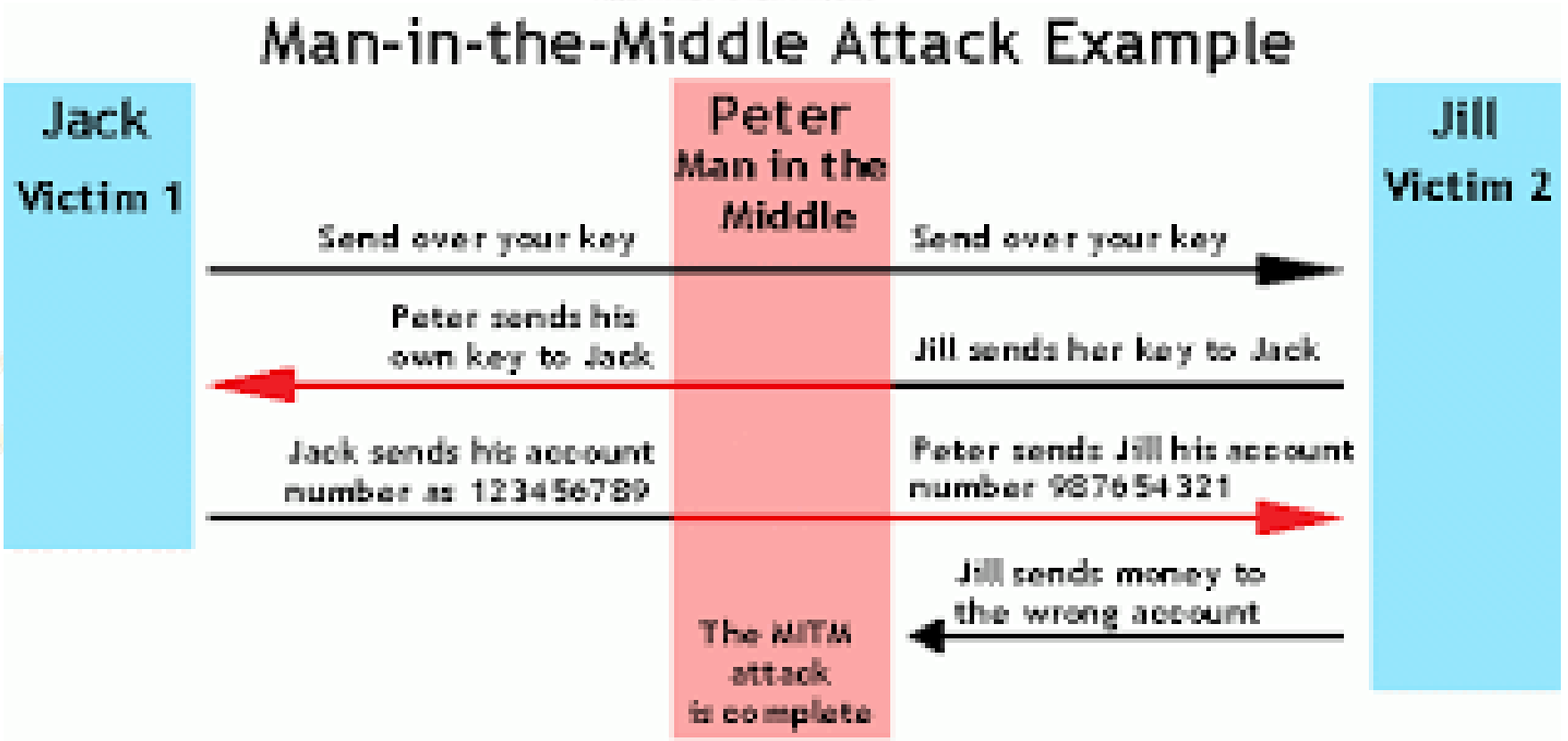
Man-in-the-middle attacks

is an **attack** where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Hijacking

is a form of **M**an **I**n **T**he **M**iddle (MITM) attack in which a malicious attacker has access to the transport layer and can eavesdrop on communications. When communications are not protected they can steal the unique session ID and impersonate the victim on the target site. This grants the attacker access to your account and data.


Man-in-the-middle attack
Original connection
New connection
Man-in-the middle, Phisher,
or annonymous proxy
ComputerHope.com


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the
Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his
own key to Jack
Jill sends her key to Jack
Jack sends his account
number as 123456789
Peter sends Jill his account
number 987654321
Jill sends money to
the wrong account
The MITM
attack
is complete

IEEE 802.11 Standards Security

Even though wireless LAN security has greatly increased over the past decade, it is important to look at the original IEEE 802.11 standard as it relates to security.

The original standard addressed two areas of security: authentication and privacy.

Authentication is defined as a way of confirming an identity; basically, it determines that you are who you say you are.

Two types of Authentication: Open System Authentication & Shared Key Authentication.

IEEE 802.11 Standards Security

Open System Authentication

This type of authentication is a two-step process, also known as a two-way handshake, and is one of the simplest ways to provide an authentication process. Open system authentication cannot fail. This authentication is what is known as a *null authentication*.

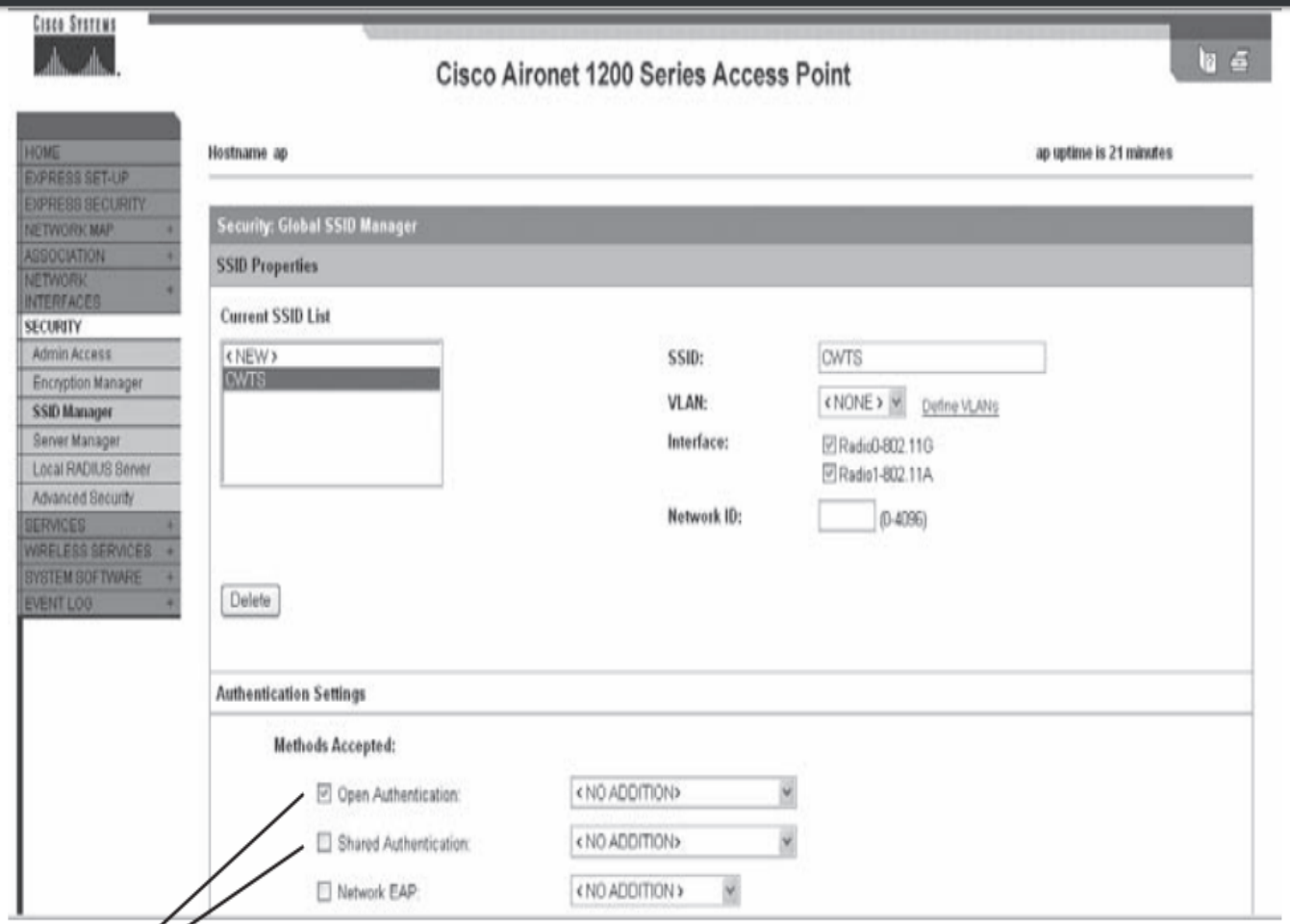
For example, if a wireless client device such as a notebook computer wants to join the wireless network, it will ask the access point if it can authenticate, and the access point will always accept.

IEEE 802.11 Standards Security

Shared Key Authentication

Shared Key Authentication (SKA) is a process by which a computer can gain access to a wireless network that uses the Wired Equipment protocol. With SKA, a computer equipped with a wireless modem can fully access any Wired Equivalent Privacy (WEP) network and exchange encrypted or unencrypted data.

Privacy - Privacy is ensuring that information or data is understandable only by the individuals or groups it is intended for, the sender and the intended receiver.



Select the authentication type

Early WLAN Security Mechanisms

Because of the way security was defined in the original IEEE 802.11 standard, manufacturers of wireless LAN equipment were able to design several ways a user could secure wireless LAN.

Some of these common WLAN security methods are:

- Service Set Identifier (SSID) hiding (closed network)
- Media Access Control (MAC) filtering
- Wired Equivalent Privacy (WEP)

Early WLAN Security Mechanisms – SSID (Service Set Identifier)

SSID is a name for the wireless network and was designed to be used for device segmentation.

The SSID will allow wireless devices such as notebook computers to identify and connect to a wireless LAN. There are a couple of ways this can be accomplished.

One is to specify the SSID of the wireless LAN to be joined in the wireless client utility of the connecting device. In this case, a wireless client sends a probe request frame with the intent of joining that particular network. The SSID is specified in a beacon frame.

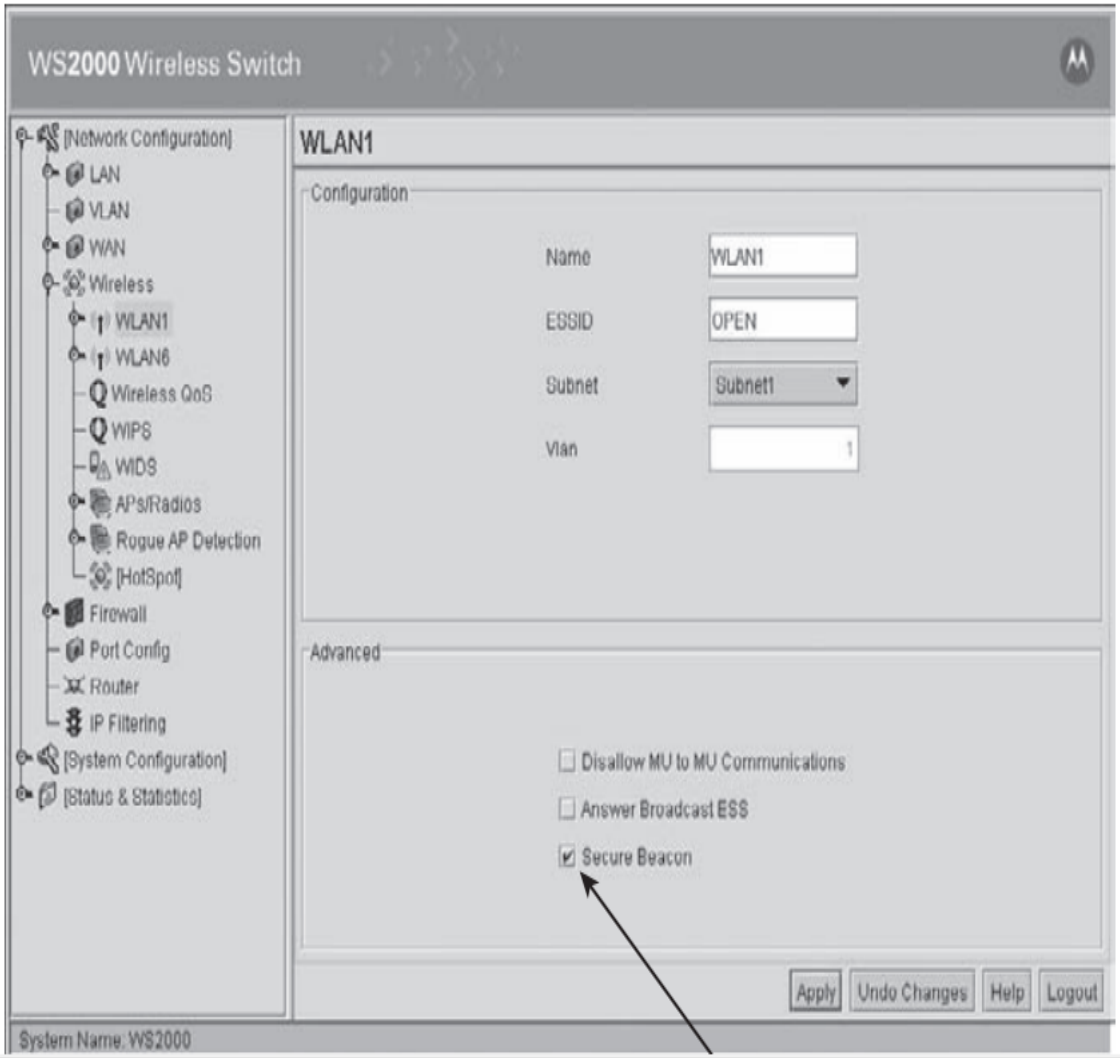
Early WLAN Security Mechanisms – SSID Hiding

Most manufacturers of wireless LAN equipment provide the capability to disable SSID broadcasting. Another term for this process is *SSID hiding*.

SSID hiding allows a user to remove the SSID that would normally appear in broadcast beacon frames. If the SSID is not being broadcast, the network is invisible to the client devices that do not have that network's SSID specified in their client utility.

If somebody knows the SSID, they would be able to enter it into their client device software and then be able to connect to the network.

broadcast


WS2000 Wireless Switch
[Network Configuration]
LAN
VLAN
WAN
Wireless
WLAN1
WLAN6
Wireless QoS
WIPS
WIDS
APs/Radios
Rogue AP Detection
[HotSpot]
Firewall
Port Config
Router
IP Filtering
[System Configuration]
[Status & Statistics]
WLAN1
Configuration
Name
WLAN1
ESSID
OPEN
Subnet
Subnet1
Vlan
1
Advanced
Disallow MU to MU Communications
Answer Broadcast ESS
Secure Beacon
Apply
Undo Changes
Help
Logout
System Name: WS2000

Early WLAN Security Mechanisms – Media Access Control (MAC) Address

MAC address is a unique hardware identifier of a network device.

This 6-byte address is the Layer 2 address that allows frames to be sent and received to and from a device. An important point here is that the MAC address is unique and no two devices should ever have the same MAC address.

In a wireless network, MAC addresses are easily visible using a packet analyzer. These addresses are required for a device to send and receive information; therefore, they cannot be encrypted and are visible to anyone with the knowledge to view them.

FIGURE 10.4 Microsoft Windows command-line utility ipconfig.exe will display MAC address

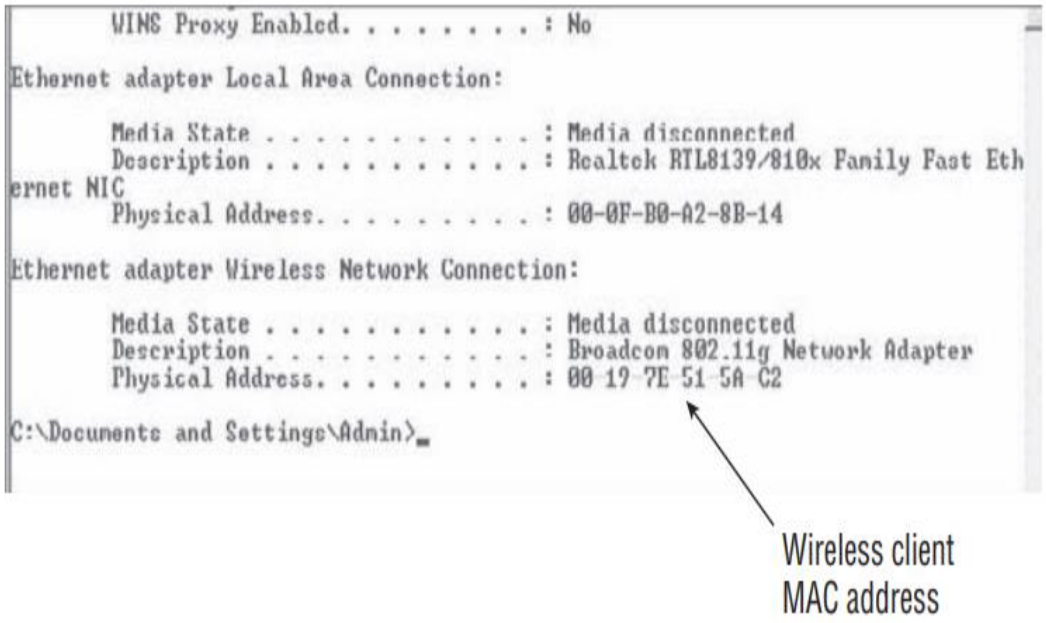
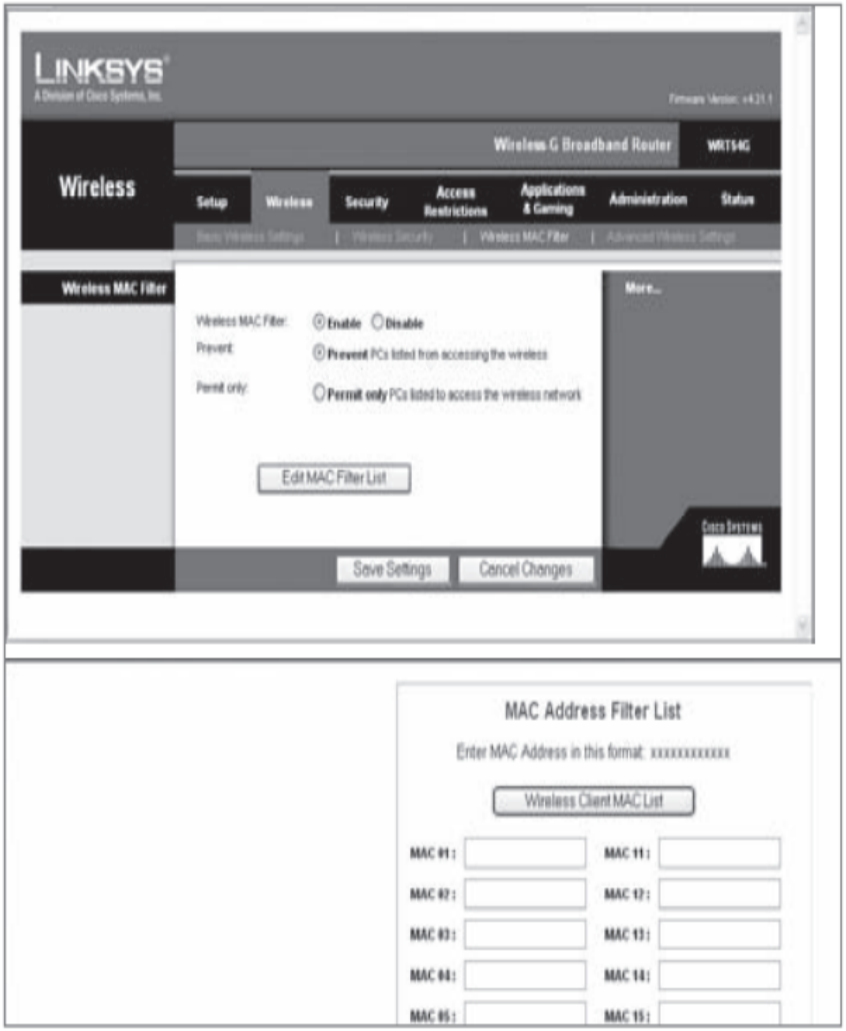


FIGURE 10.5 Linksys WRT54G MAC filter setup



Overview of other WLAN Security Standards and Technology

Wired Equivalent Privacy(WEP)

With open system authentication, all information is broadcast through the air in clear text. What this means is anyone with knowledge of how to use a packet analyzer or other software tool can easily see all the information that is passing between devices.

WEP was designed as a way to protect wireless networking from casual eavesdropping. WEP is fairly simple to implement. It requires all devices to have the same key.

Overview of other WLAN Security Standards and Technology

The WEP key can be either 64-bit or 128-bit; however, the standard required only 64-bit WEP. WEP is static, which means all wireless devices—access points, bridges, and client stations—must have the key manually entered into them.

PIN-Based Security

PIN-based security requires a unique PIN to be entered on all devices that will be part of the same secure wireless network.

When the device tries to join the network, the registrar will prompt the user to enter the unique PIN. Once the PIN is entered, the process authenticates the device and encrypts the network data sent to and from the device.

Overview of other WLAN Security Standards and Technology

Push – Button Security

Push-button security or push-button configuration (PBC) allows users to configure wireless LAN security with "the push of a button," making setting up wireless security a one-step process.

When a user pushes a hardware button on the wireless residential gateway (wireless router) and clicks a software button in the utility for the network adapter installed in the client device wanting to associate, push-button security creates a connection between the devices, configures the network's SSID, and turns on security. This allows a secure connection among all devices that are part of the wireless network.

Overview of other WLAN Security Standards and Technology

User-based security

User-based security allows an administrator to restrict access to a wireless network and its resources by creating users in a database. Anyone trying to join the network will be required to authenticate as one of the users by supplying a username and password. After successful authentication, the user will be able to gain access to resources for which they have permissions.

This type of mutual authentication is more secure than the previously mentioned security measures.

Quick Review Question

- Briefly explain WLAN security mechanisms.
- Compare shared key versus with open key authentication.

Summary of Main Teaching Points

In this chapter, we briefly discussed network intrusion and the impact it can have on a wireless LAN.

We also took a look at IEEE 802.11 security methods and a quick review of the authentication types defined in the standard, open system and shared key.

We explored some of the 802.11 WLAN security techniques, including:

- SSID hiding
- MAC address filtering
- Wired Equivalent Privacy (WEP)

Question and Answer Session

A · P · U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Q & A

What we will cover next

WLAN Site Survey

- Gathering Business Requirements
- Public Access, Hotspots, Hospitality, Interviewing Managers and Users
- Manufacturer Guidelines and Deployment Guides
- Defining Physical and Data Security Requirements
- Gathering Site-Specific Documentation
- Documenting Existing Network Characteristics
- Identifying Infrastructure Connectivity and Power Requirements
- Understanding RF Coverage and Capacity Requirements
- Client Connectivity Requirements