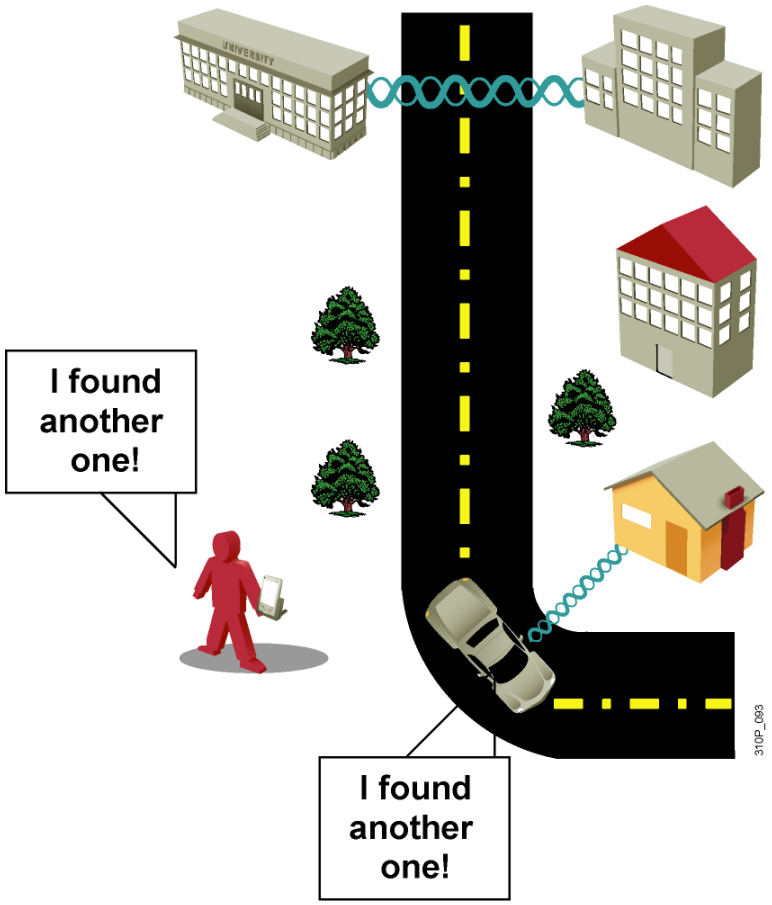
Wireless Security

Why WLAN Security?

- Wide availability and low cost of IEEE 802.11 wireless equipment
- 802.11 standard ease of use and deployment
- Availability of sniffers
- Statistics on WLAN security
- Media hype about hot spots, WLAN hacking, war driving
- Nonoptimal implementation of encryption in standard Wired Equivalent Privacy (WEP) encryption
- Authentication vulnerability



Wireless Security Overview

A WLAN is open to anyone within range of an AP and the appropriate credentials to associate to it.

Attacks can be generated by outsiders, disgruntled employees, and even unintentionally by employees. Wireless networks are specifically susceptible to several threats, including the following:

- Interception of data
- Wireless intruders
- Denial of Service (DoS) Attacks
- Rogue APs

DoS Attacks

Wireless DoS attacks can be the result of the following:

- Improperly configured devices
- A malicious user intentionally interfering with the wireless communication
- Accidental interference

To minimize the risk of a DoS attack due to improperly configured devices and malicious attacks, harden all devices, keep passwords secure, create backups, and ensure that all configuration changes are incorporated off-hours.

Rogue Access Points

- A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy.
- Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.
- A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP.
- To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies and use monitoring software to actively monitor the radio spectrum for unauthorized APs.

Man-in-the-Middle Attack

In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the “evil twin AP” attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

Defeating a MITM attack begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.

Wireless LAN Security Threats

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
	 THE WALL STREET JOURNAL. Hackers Can Penetrate Wireless Network *The weakness is another reminder of the difficulty in implementing effective network security.*	

Wireless Security

No physical connection needed

Attacker can “tune into” your network just like tuning into a radio station

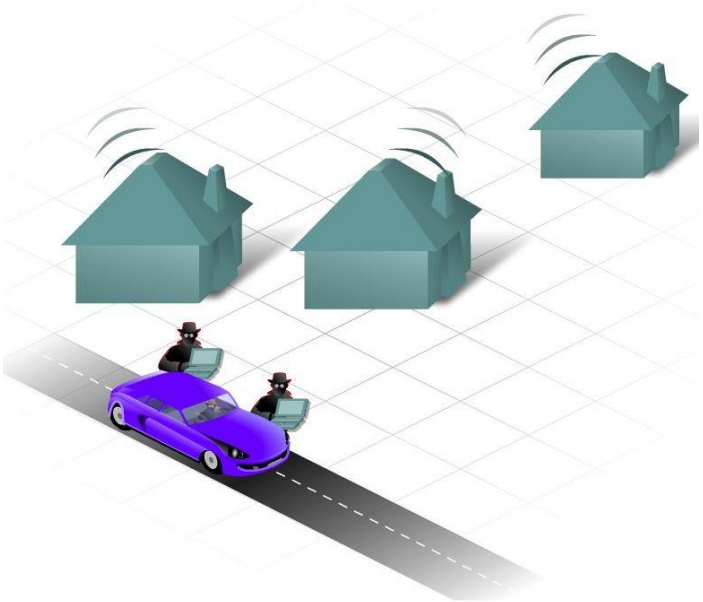
Easy access if all settings are set to default, so . . .

CHANGE THE SETTINGS

- disable SSID
- change default password
- change default IP

But . .

- SSID transmitted in clear text
- still possible to learn the SSID



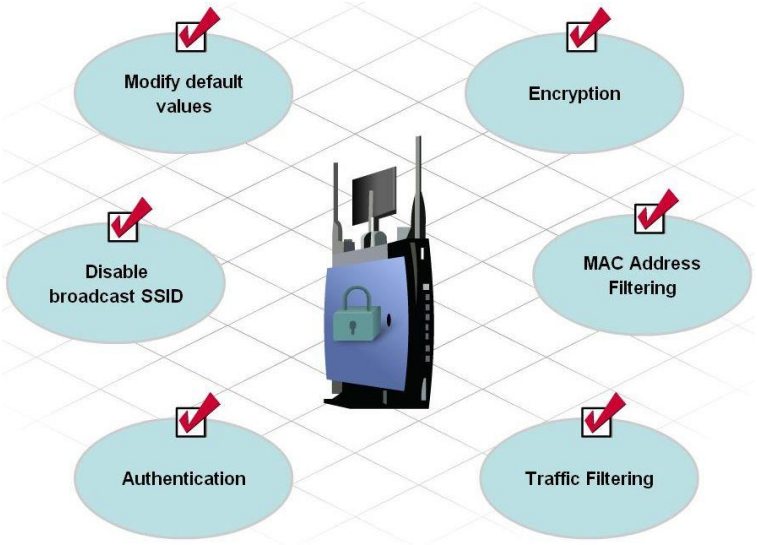
Securing the AP

Basic Security

- Changing values (SSID, usernames, passwords)
- Disable Broadcast SSID
- MAC Address filtering

Advanced Security

- Encryption
- Authentication
- Traffic Filtering

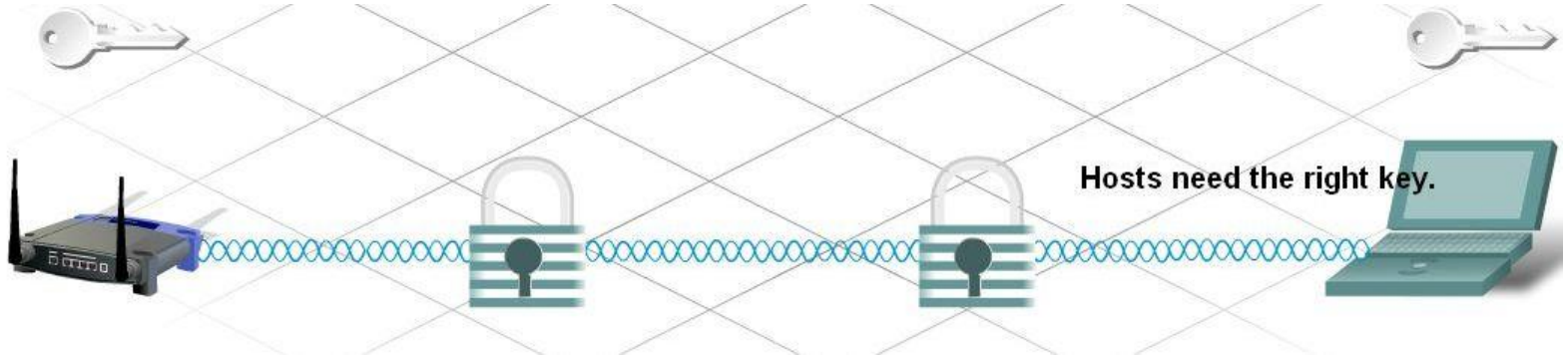


Encryption

Process of transforming data so if intercepted, will still be unusable

WEP (Wired Equivalency Protocol)

- advanced security feature
- encrypts network traffic as it travels
- 64 – 128 bits (letters and/or numbers)
- AP and every device on the network must have the same WEP key



Evolution of Wireless LAN Security

WEP	802.1x EAP	WPA	802.11i / WPA2
▪ Basic encryption ▪ No strong authentication ▪ Static, breakable keys ▪ Not scalable ▪ MAC filters and SSID-cloaking also used to complement WEP	▪ Dynamic keys ▪ Improved encryption ▪ User authentication ▪ 802.1X EAP (LEAP, PEAP) ▪ RADIUS	▪ Standardized ▪ Improved encryption ▪ Strong, user authentication (such as, LEAP, PEAP, EAP-FAST)	▪ AES strong encryption ▪ Authentication ▪ Dynamic key management

Security – Authentication

Controls who connects to the network

Permitted based on set of credentials

Helps to verify the “trustworthiness” of the device

- usernames
- passwords

Occurs before client is connected to WLAN

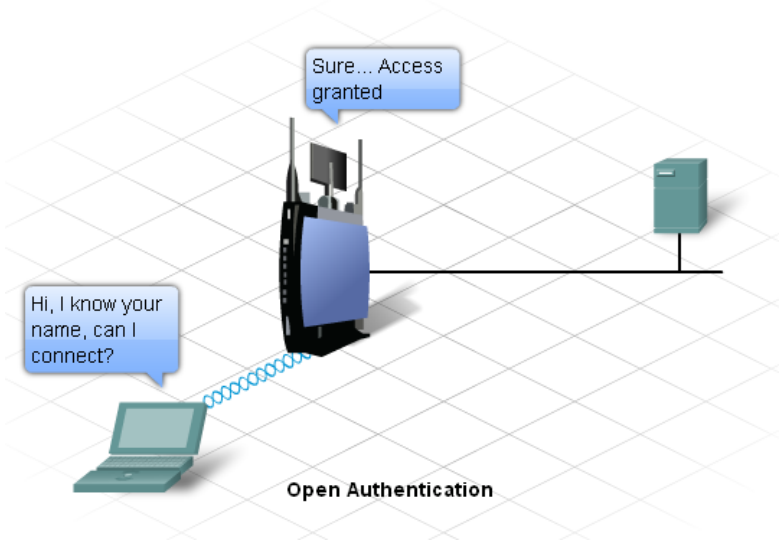
Open Authentication

On by default

Any and all clients can access AP

Should only be used on public wireless networks

- Schools
- Internet Café

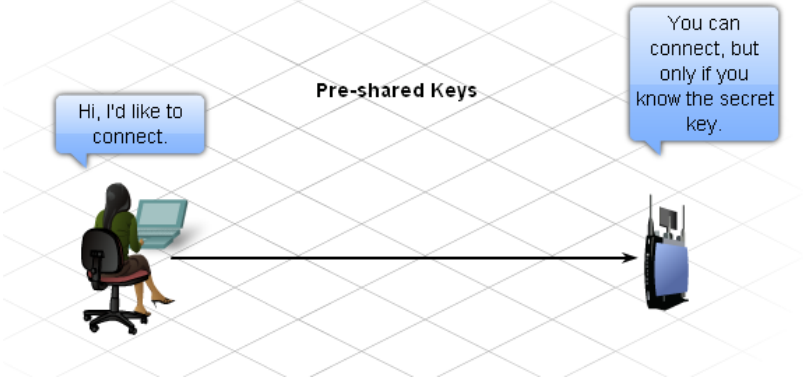


PSK (Pre-Shared Keys) Authentication

Both AP and client must have the same secret key or word

Here's how it works:

- AP sends random string of bytes to client
- Client accepts it, encrypts it, and sends it back to AP
- AP receives encrypted string, decrypts it
- if decrypted string = original string → client is added

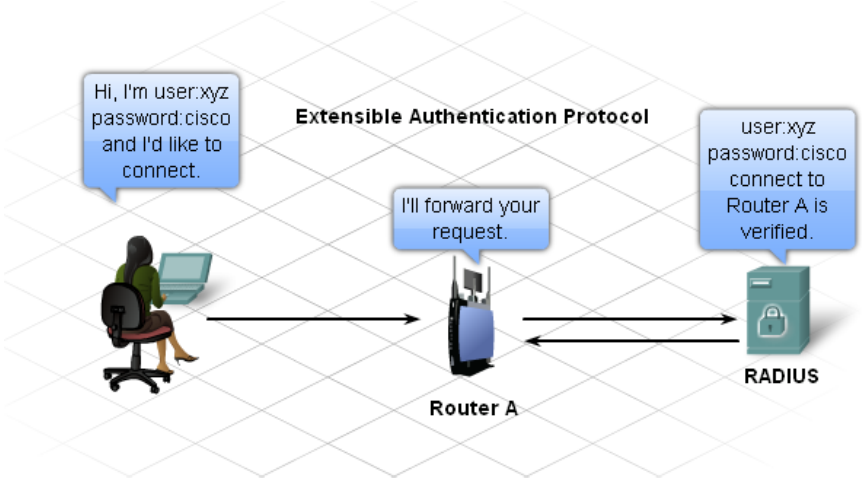


EAP (Extensible Authentication Protocol)

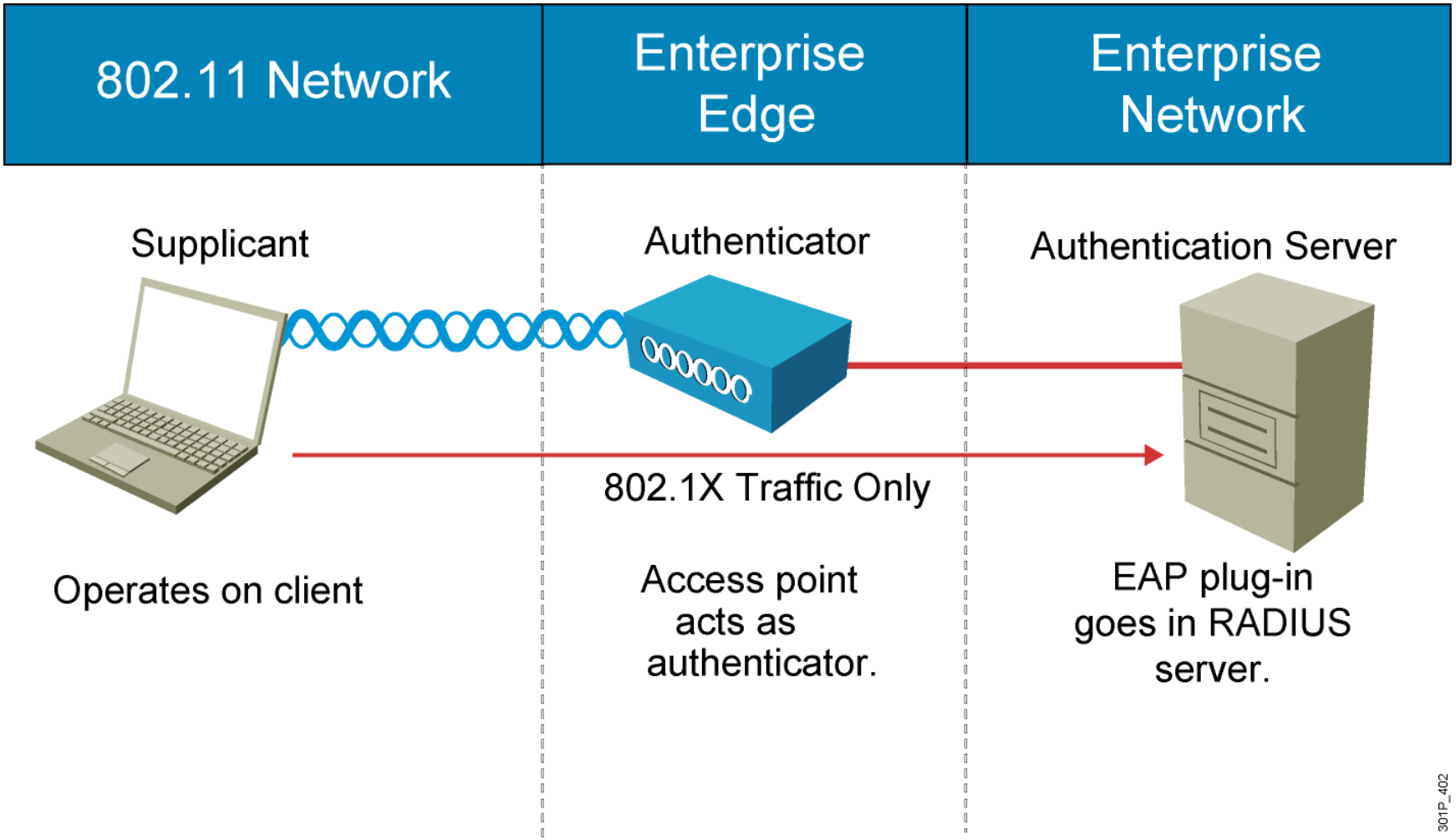
EAP software must be installed on the client device

Client talks with RADIUS Server

- Remote Authentication Dial-in User Services
- server functions separately from the AP
- server keeps a database of valid users
- username and password checked by the server



How 802.1X Works on the WLAN



Traffic Filtering

Controls the type of traffic allowed across a WLAN

Able to block traffic based on:

- IP Address
- MAC Address
- Port Numbers

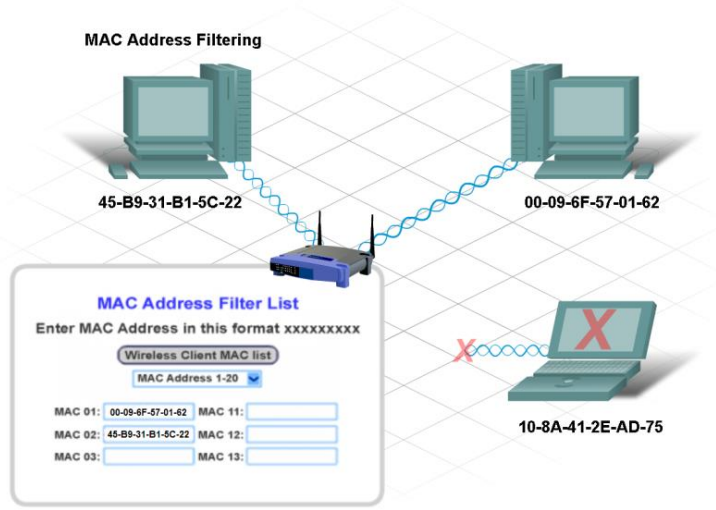
MAC Address Filtering

Another security feature

Will limit access to your network

MAC address used to identify which device can connect to the wireless network

- wireless AP looks up MAC in a list (database)
- only those addresses listed will gain access



Planning the WLAN

Determine the type of wireless standard

- 802.11b, g, n operates at 2.4 GHz
- travels farther than 5 GHz
- Less equipment = lower cost

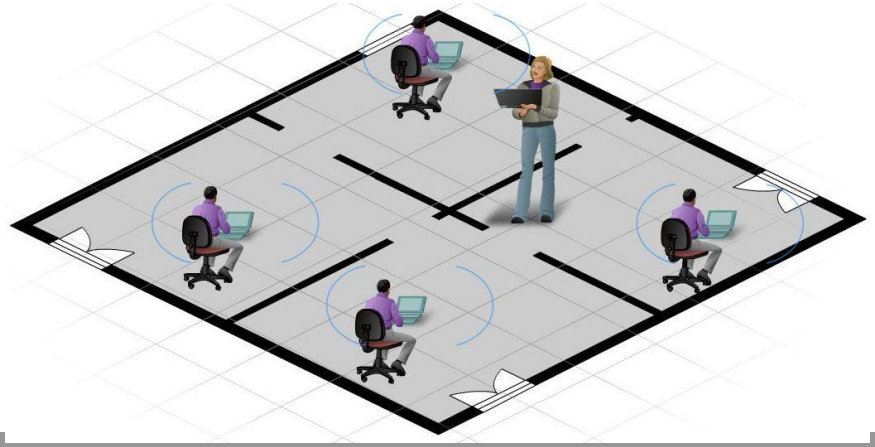
Determine layout

- look at existing infrastructure
- if using 802.11a, will it work with the newest standards??

Installation/Security

- Total Cost of Ownership (TCO)
- Site Survey
  - signal strength
  - possible interference

Backup/Updating Devices




CISCO