CCNA 200-301, Volume I

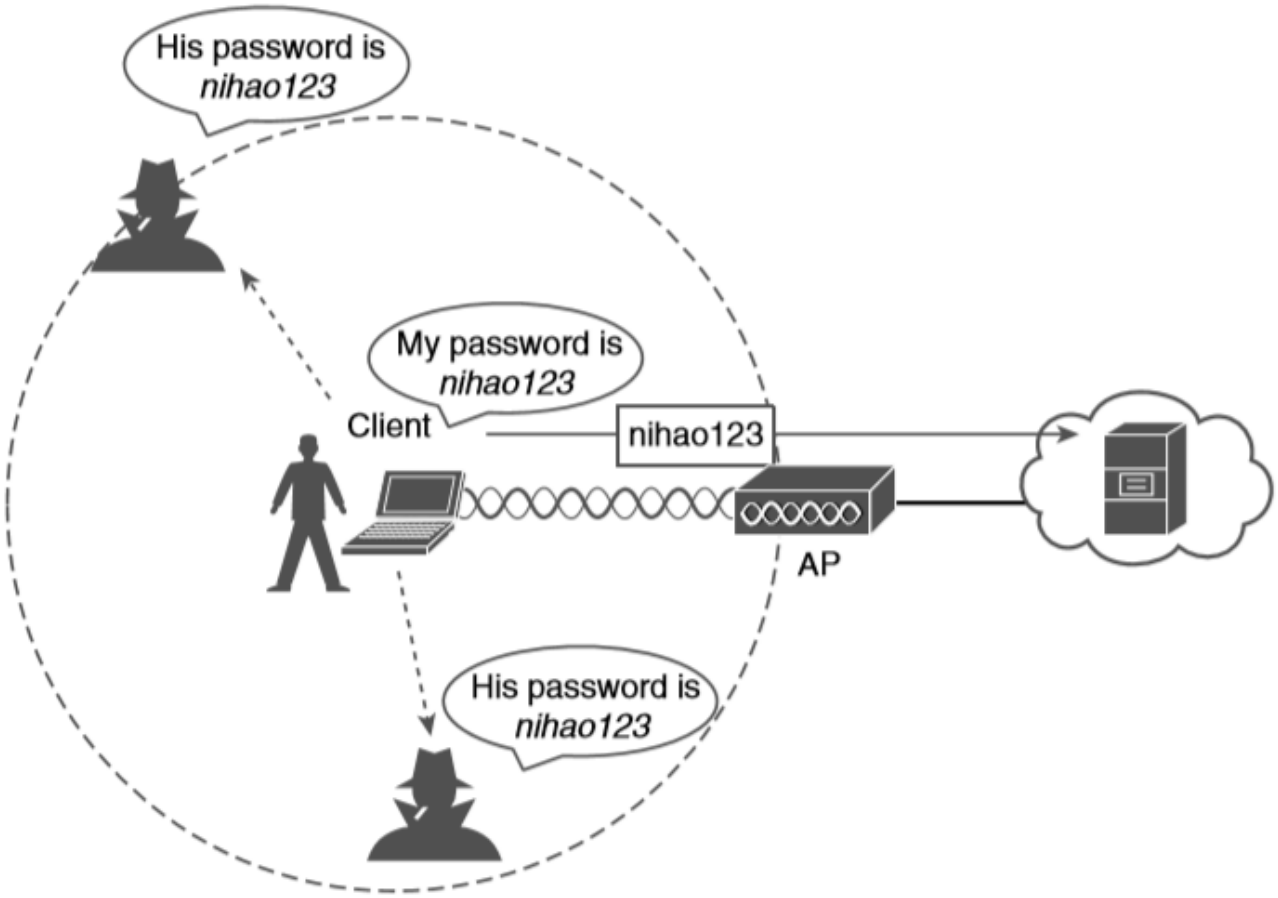
Chapter 28

Securing Wireless Networks

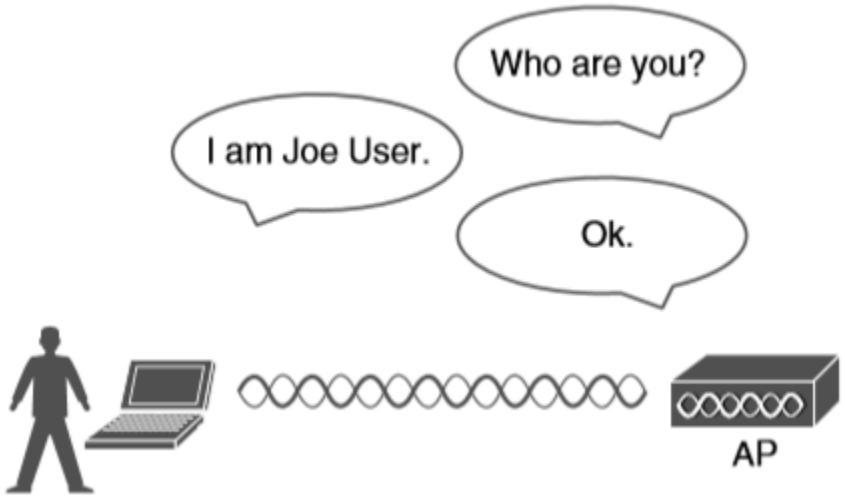
Objectives

- Anatomy of a Secure Connection
- Wireless Client Authentication Methods
- Wireless Privacy and Integrity Methods
- WPA, WPA2, and WPA3

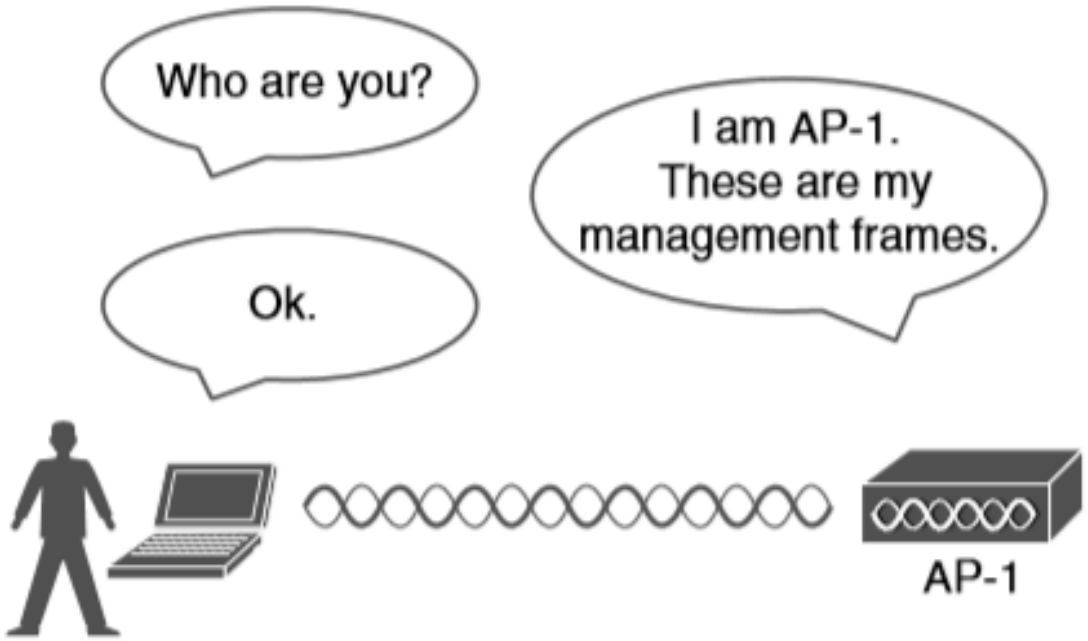
Wireless Transmissions Reaching Unintended Recipients



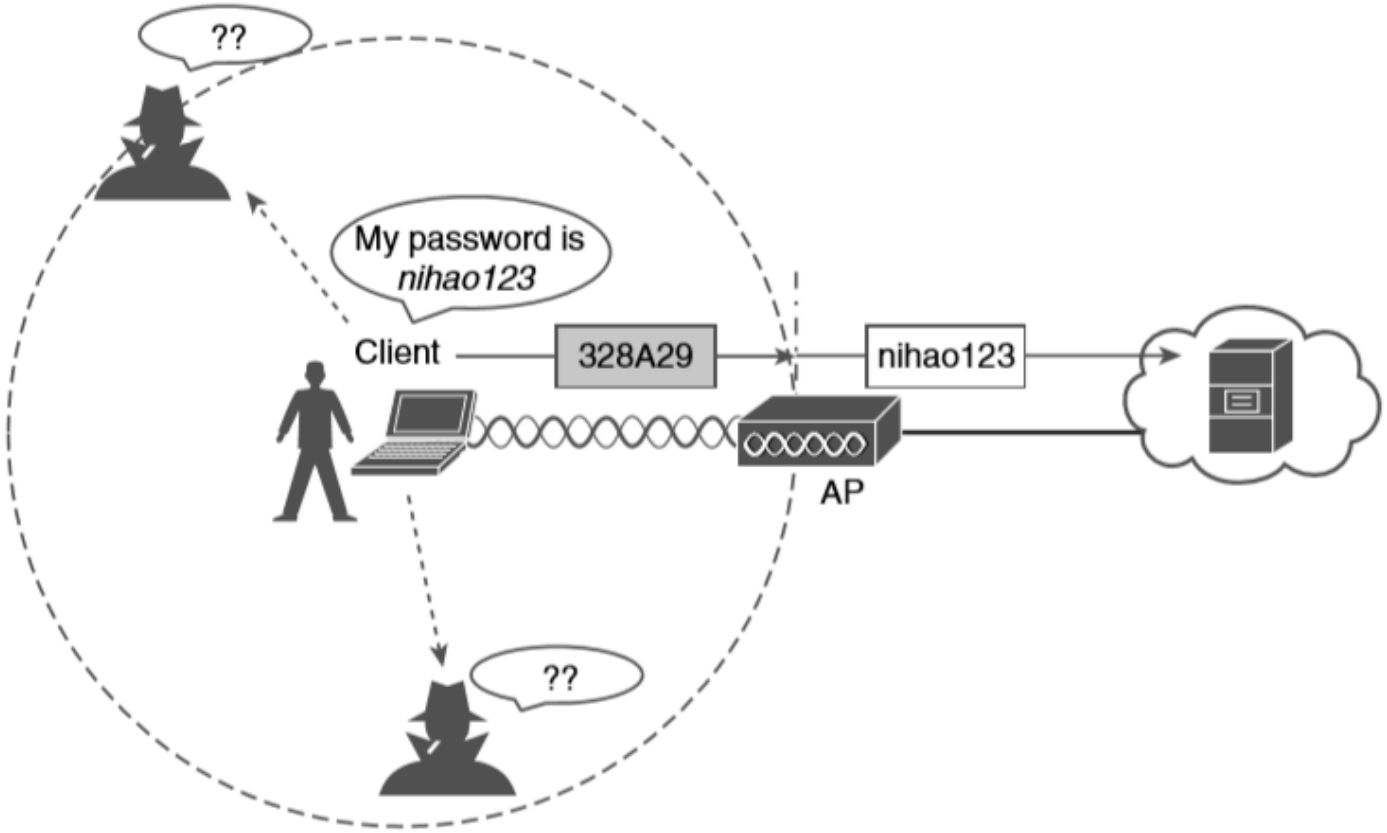
Authenticating a Wireless Client



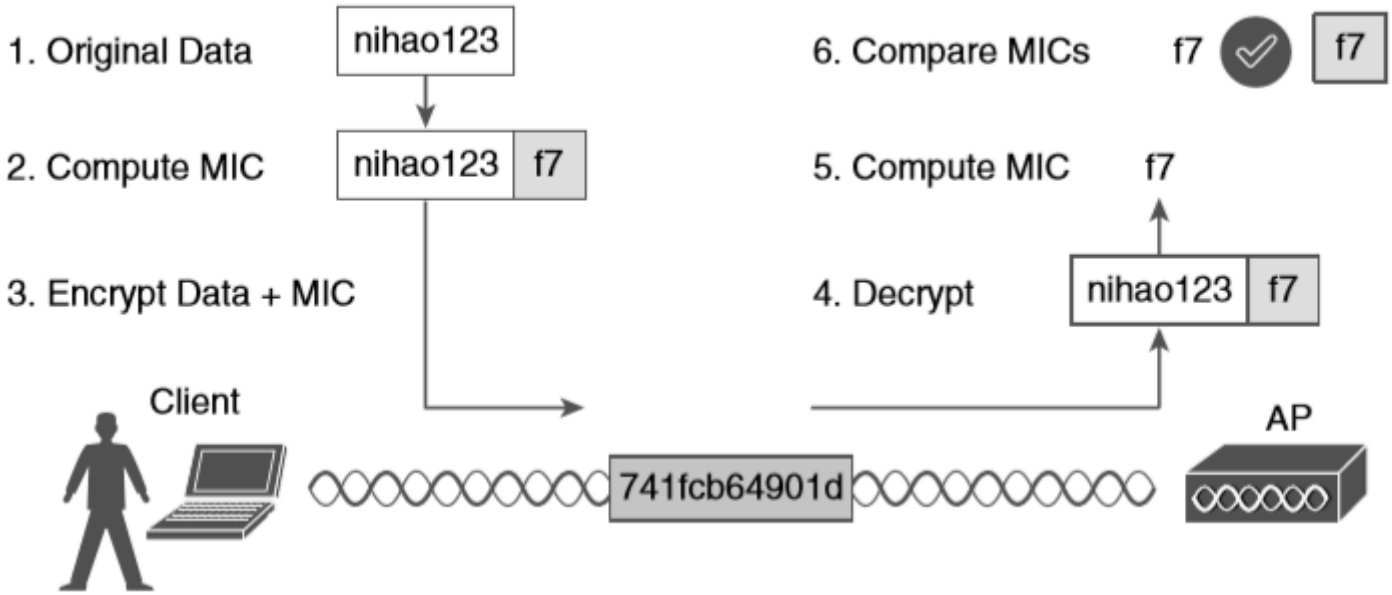
Authenticating a Wireless AP



Encrypting Wireless Data to Protect Data Privacy



Checking Message Integrity over a Wireless Network



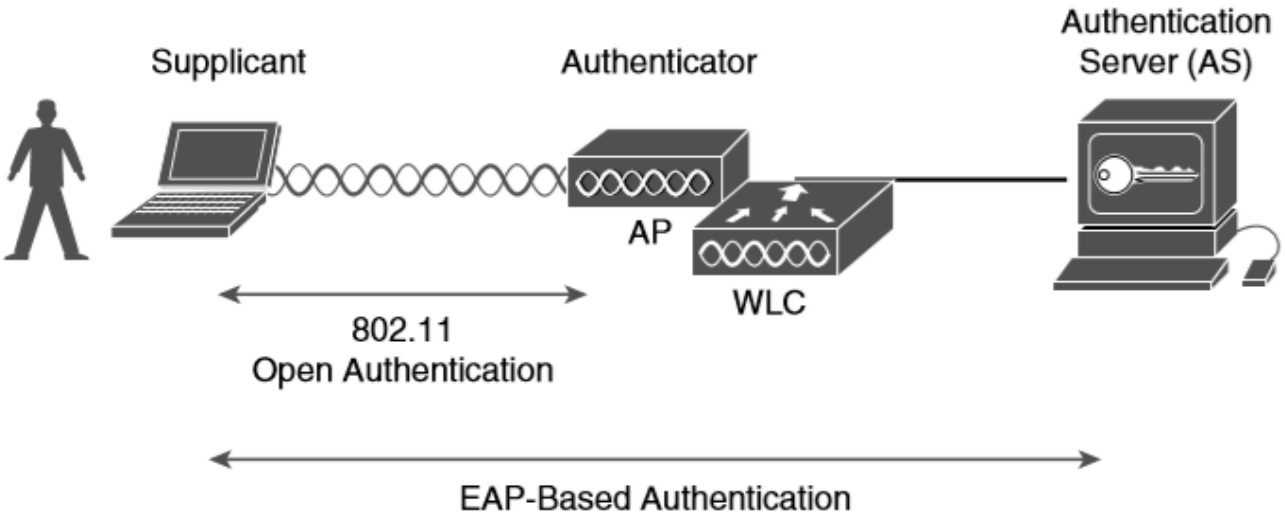
Open Authentication

- Open authentication is true to its name; it offers open access to a WLAN.
- The only requirement is that a client must use an 802.11 authentication request before it attempts to associate with an AP. No other credentials are needed.

WEP

- WEP uses the RC4 cipher algorithm to make every wireless data frame private and hidden from eavesdroppers.
- The algorithm uses a string of bits as a key, commonly called a WEP key, to derive other encryption keys—one per wireless frame.
- WEP is known as a shared-key security method.

802.1x Client Authentication Roles



EAP-FAST

The PAC is a form of shared secret that is generated by the AS and used for mutual authentication. EAP-FAST is a sequence of three phases:

- Phase 0: The PAC is generated or provisioned and installed on the client.
- Phase 1: After the supplicant and AS have authenticated each other, they negotiate a Transport Layer Security (TLS) tunnel.
- Phase 2: The end user can then be authenticated through the TLS tunnel for additional security.

TKIP

TKIP adds the following security features using legacy hardware and the underlying WEP encryption:

- MIC: This efficient algorithm adds a hash value to each frame as a message integrity check to prevent tampering; commonly called “Michael” as an informal reference to MIC.
- Time stamp: A time stamp is added into the MIC to prevent replay attacks that attempt to reuse or replay frames that have already been sent.
- Sender’s MAC address: The MIC also includes the sender’s MAC address as evidence of the frame source.
- TKIP sequence counter: This feature provides a record of frames sent by a unique MAC address, to prevent frames from being replayed as an attack.
- Key mixing algorithm: This algorithm computes a unique 128-bit WEP key for each frame.
- Longer initialization vector (IV): The IV size is doubled from 24 to 48 bits, making it virtually impossible to exhaust all WEP keys by brute-force calculation.

CCMP

The Counter/CBC-MAC Protocol (CCMP) is considered to be more secure than TKIP. CCMP consists of two algorithms:

- AES counter mode encryption
- Cipher Block Chaining Message Authentication Code (CBC-MAC) used as a message integrity check (MIC)

GCMP

The Galois/Counter Mode Protocol (GCMP) is a robust authenticated encryption suite that is more secure and more efficient than CCMP. GCMP consists of two algorithms:

- AES counter mode encryption
- Galois Message Authentication Code (GMAC) used as a message integrity check (MIC

GCMP is used in WPA3, which is described in the following section.

Comparing WPA, WPA2, and WPA3

Authentication and Encryption Feature Support	WPA	WPA2	WPA3*
Authentication with Pre-Shared Keys?	Yes	Yes	Yes
Authentication with 802.1x?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	Yes	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes