CWSP Guide to Wireless Security

Secure Wireless Authentication

Objectives

- Define wireless authentication
- List and describe the different types of authentication servers
- Explain the differences between various extended authentication protocols
- Describe IEEE 802.11i authentication and key management

Defining Authentication

- It is important to understand exactly what authentication is
  - And the types of credentials that are used to authenticate users

What is Wireless Authentication?

- Authentication
  - Users must give proof that they are authentic
  - Wired network devices are assumed to be authentic
- Wireless authentication
  - Requires device to be authenticated before being connected to the WLAN
- Types of wireless device authentication
  - Open system authentication
  - Shared key authentication

Authentication, Authorization, and Accounting (AAA)

- Triple “A” elements
  - Authentication determines who the user is
  - Authorization determines what the user can do
  - Accounting determines what the user did
- Authentication controls access by requiring valid user credentials
- Authorization is the process that determines whether the user has the authority to carry out certain tasks
- Accounting **measures** the resources a user consumes during each network session

Authentication, Authorization, and Accounting (AAA) (continued)

- Information can be used:
  - To find evidence of problems
  - For billing
  - For planning
- AAA servers
  - Servers dedicated to performing the AAA functions
  - Can provide significant advantages in a wireless LAN

Authentication Credentials

- Categories of credentials
  - Something the user knows
  - Something the user is
  - Something the user has
- Passwords
  - Fall into the category of something the user knows
  - Secret combinations of letters and numbers
- Biometrics
  - Uses unique human characteristics for authentication

Authentication Credentials (continued)

- Biometrics (continued)
  - Human characteristics commonly used
    - Fingerprints and unique characteristics of the face, hand, or voice
- Digital certificates
  - Asymmetric encryption or public key cryptography
    - Private key is used to encrypt messages
    - Public key is used to decrypt messages
  - Electronic files used to uniquely identify users and resources over networks
  - Issued by a trusted third party (certification authority (CA))

Authentication Credentials (continued)



Figure 8-1 Fingerprint scanner

Authentication Credentials (continued)

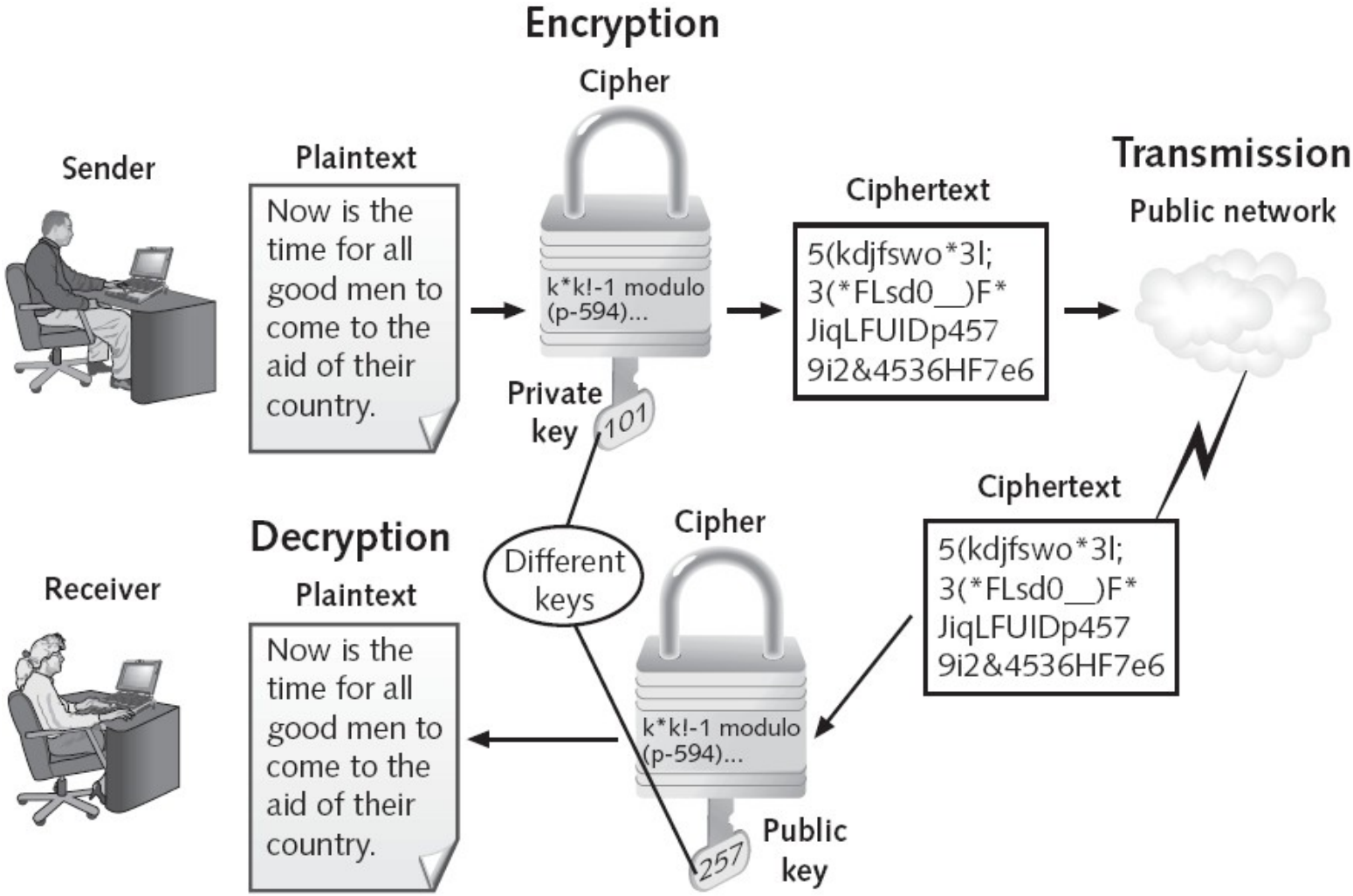


Figure 8-2 Asymmetric encryption

Authentication Credentials (continued)

- Digital certificates (continued)
  - Registration authority (RA)
    - Handles some CA tasks, such as processing certificate requests and authenticating users
  - Information in a certificate
    - A serial number
    - The holder's public key
    - The name of the certification authority
    - The name of the holder and other identification info
    - The start and stop date in which the certificate is valid

Authentication Credentials (continued)

- Digital certificates (continued)
  - Can be used for authentication in a wireless LAN
  - Can also be used to provide encryption between the wireless device and the AP
  - Public Key Infrastructure (PKI)
    - System of using digital certificates, CAs, and other registration authorities
      - That verify and authenticate the validity of each party involved in a transaction over a public network
    - There currently is no single standard for using a PKI

Authentication Servers

- Most common types
  - RADIUS
  - Kerberos
  - TACACS+
  - Lightweight Directory Access Protocol (LDAP)

RADIUS

- RADIUS: Remote Authentication Dial-In User Service
  - Developed in 1992
- For “high volume service control applications”
  - Such as dial-in access to a corporate network
- RADIUS client
  - Dial-up server or wireless access point
  - Responsible for sending user credentials and connection parameters to a RADIUS server
- RADIUS server
  - Authenticates and authorizes RADIUS client request

RADIUS (continued)

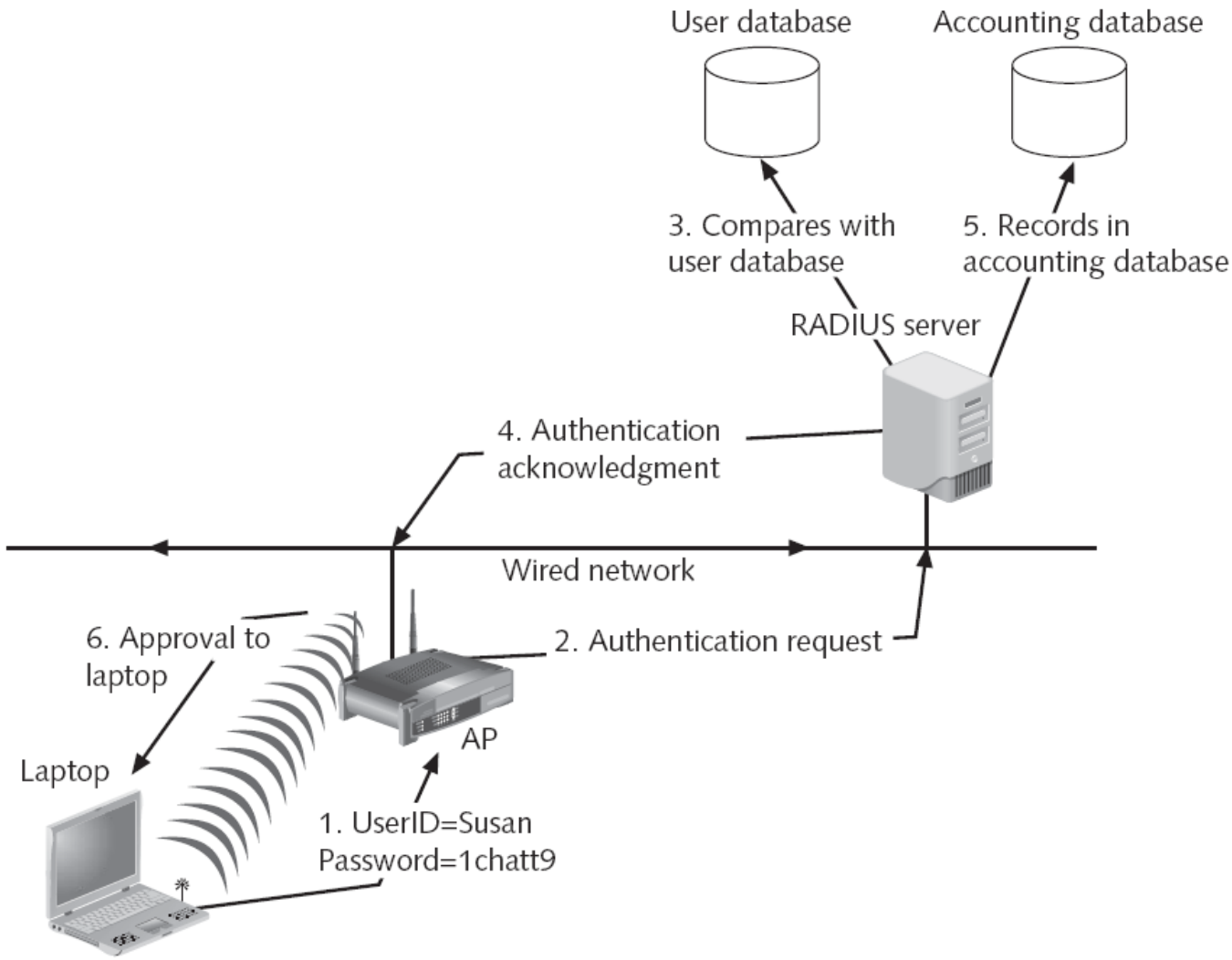


Figure 8-3 RADIUS authentication

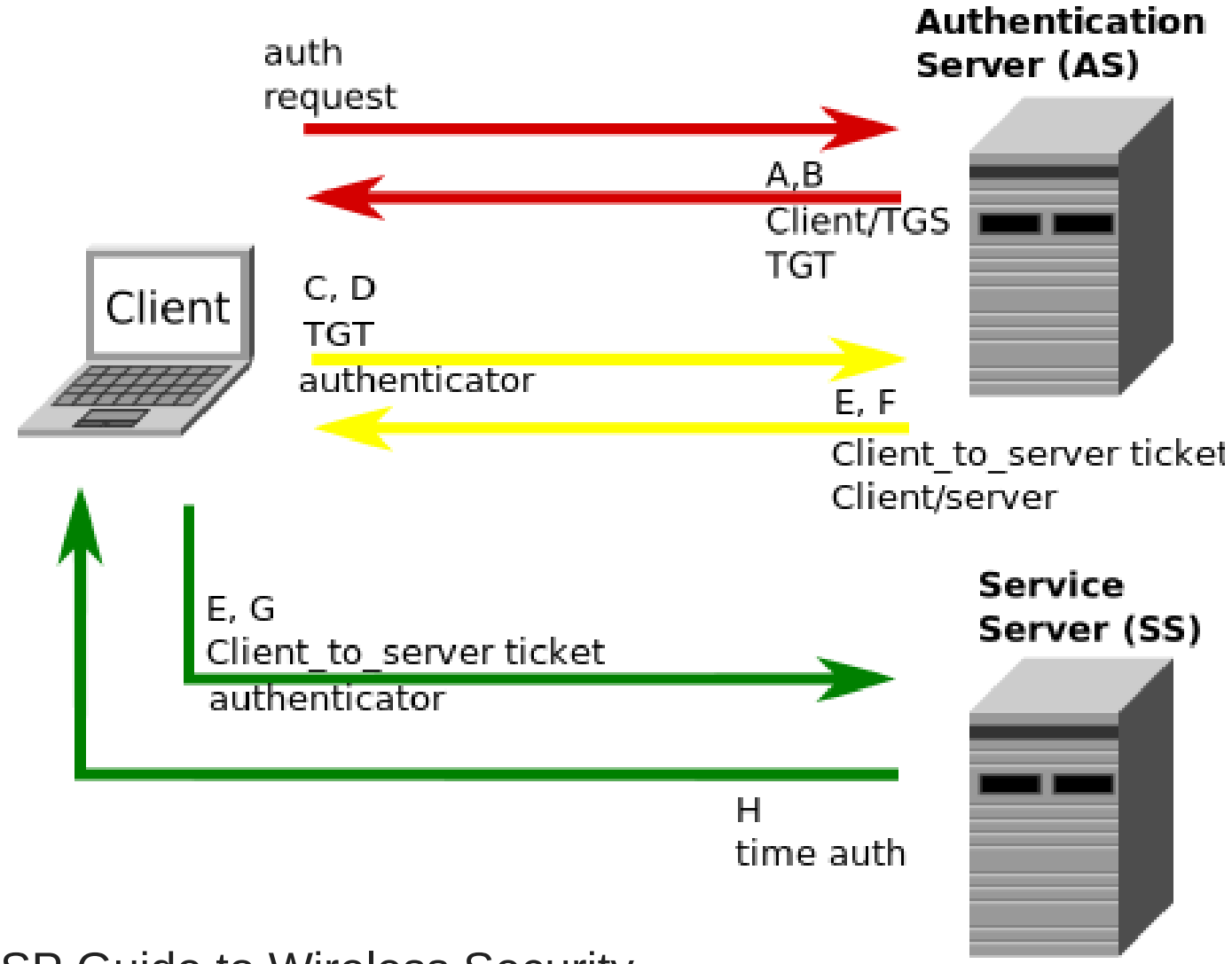
RADIUS (continued)

- RADIUS servers (continued)
  - Can be used in conjunction with VLAN tagging for additional security
- RADIUS allows a company to maintain user profiles in a central database
  - That all remote servers can share

Kerberos

- Authentication system
  - Developed by the Massachusetts Institute of Technology (MIT)
- Used to verify the identity of networked users
- Kerberos authentication server
  - Provides a ticket to the user
  - Ticket contains information linking it to the user
- User presents this ticket to the network for a service
- Service examines ticket to verify user identity

Kerberos


Authentication Server (AS)
auth request
A,B
Client/TGS TGT
Client
C, D
TGT
authenticator
E, F
Client_to_server ticket
Client/server
E, G
Client_to_server ticket
authenticator
Service Server (SS)
H
time auth

Terminal Access Control Access Control System (TACACS+)

- TACACS+
  - Industry standard protocol specification
  - Forwards username and password information to a centralized server
  - Designed to support thousands of remote connections
  - Supports authentication, authorization, and auditing

Lightweight Directory Access Protocol (LDAP)

- Directory service
  - Database stored on the network
  - Contains information about users and network devices
- X.500
  - International Organization for Standardization (ISO) standard for directory services
  - White-page service
    - Looks up information by name
  - Yellow-pages service
    - Searches for information by category

Lightweight Directory Access Protocol (LDAP) (continued)

- Information is in a directory information base (DIB)
- Entries in the DIB are arranged in a tree structure called the directory information tree (DIT)
  - Each entry is a named object and a set of attributes
- X.500 standard does not define any representation for the data stored
- Directory Access Protocol (DAP)
  - Protocol for a client application to access an X.500 directory

Lightweight Directory Access Protocol (LDAP) (continued)

- Lightweight Directory Access Protocol (LDAP)
  - Sometimes called X.500 Lite
  - Simpler subset of X.500
- Primary differences
  - LDAP was designed to run over TCP/IP
  - LDAP has simpler functions
  - LDAP encodes its protocol elements in a less complex way than X.500
- LDAP makes it possible for almost any application in any platform to obtain directory information

Lightweight Directory Access Protocol (LDAP) (continued)

- LDAP is often used in a WLAN in two different ways
  - Authentication server can use LDAP for retrieving user information
  - Many RADIUS servers support interfacing with an LDAP database

An entry can look like this when represented in LDAP Data Interchange Format (LDIF) (LDAP itself is a binary protocol):

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Authentication Design Models

- Single site deployment
  - Simplest type of authentication model
  - Consists of one or more RADIUS servers accessing a centralized authentication database
  - Used when all WLAN users are located at a single site
  - Advantages
    - Only one authentication database to support
    - Fairly easy to increase the capacity of the single site
  - Disadvantages
    - Can be more difficult to scale as more users are added

Authentication Design Models (continued)

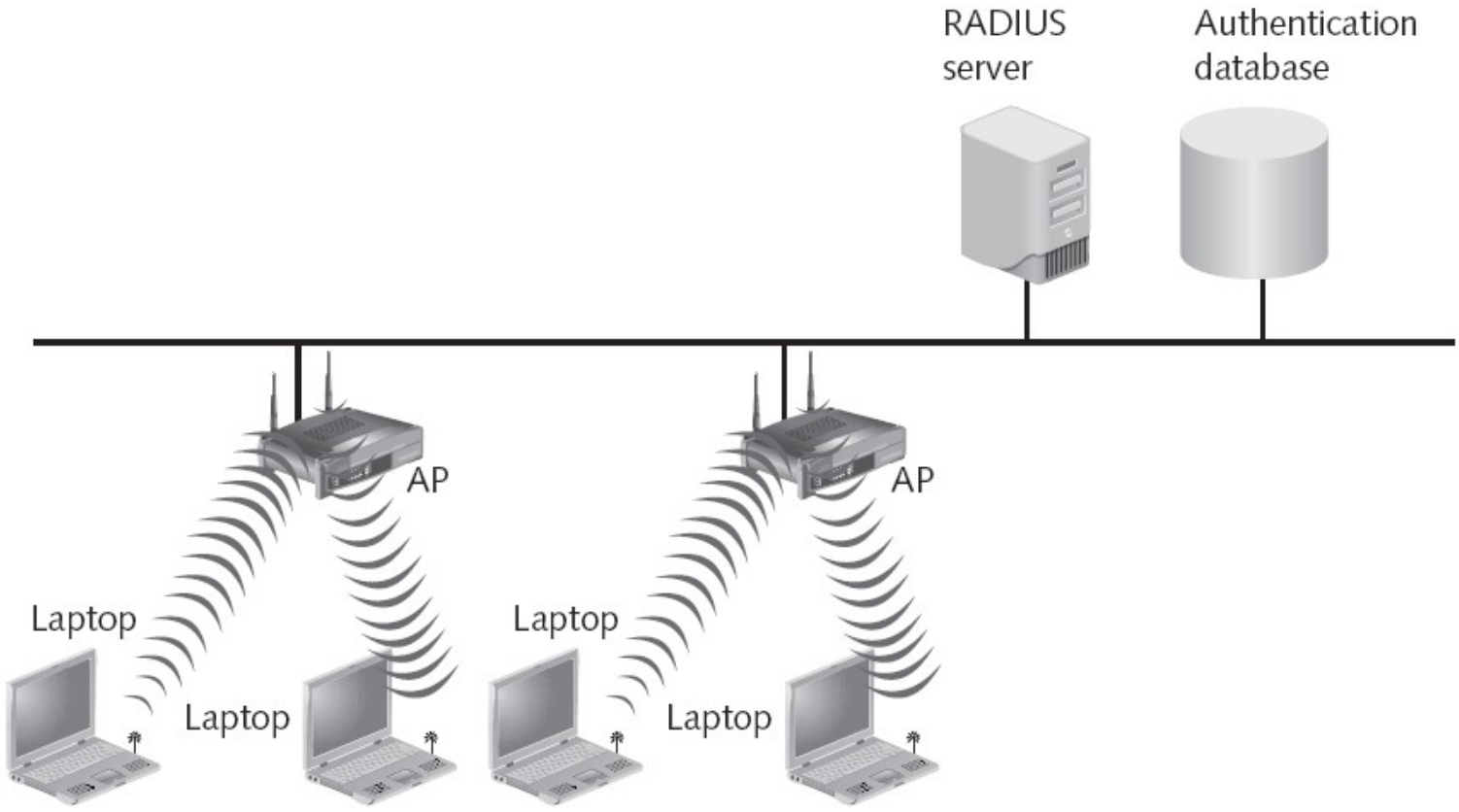


Figure 8-4 Single site deployment

Authentication Design Models (continued)

- Distributed autonomous site deployment
  - Uses local authentication with one or more RADIUS servers at each site
  - Authentication **database is replicated** from one central site to each local site
  - RADIUS servers actually perform the authentication and any accounting activity
  - Advantages
    - Does not rely on a remote network connection
    - Additional RADIUS servers can be added to remote site

Authentication Design Models (continued)

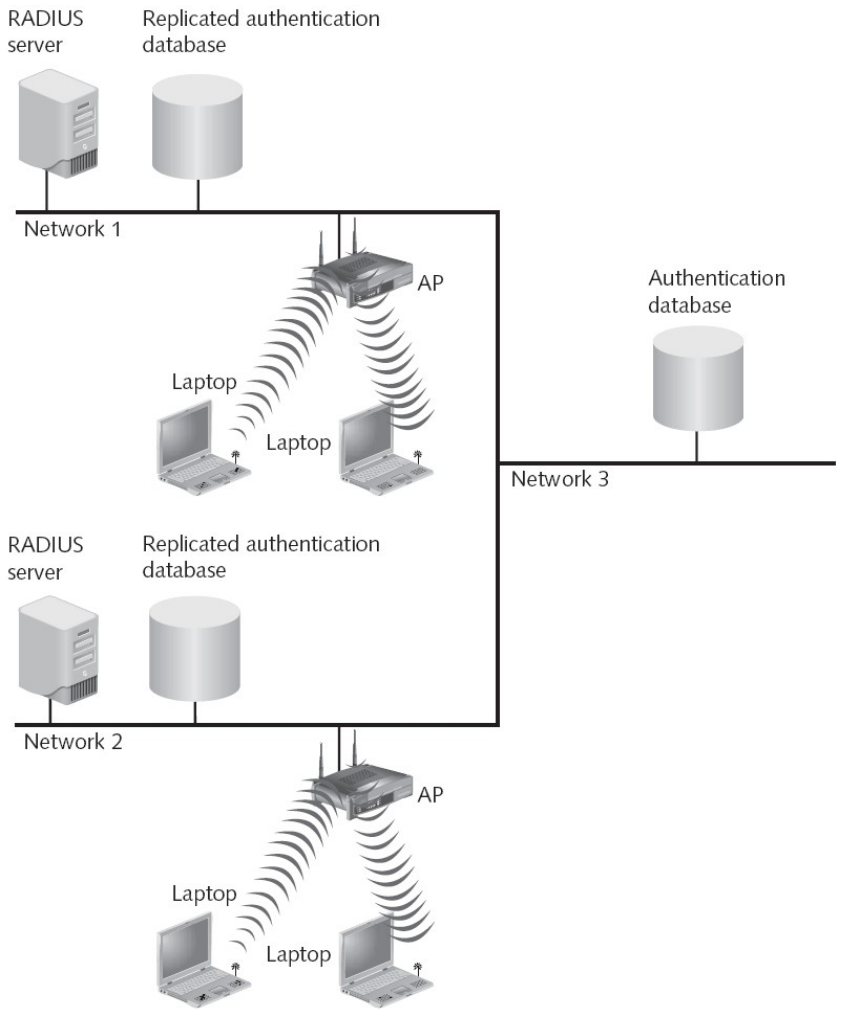


Figure 8-5 Distributed autonomous site deployment

Authentication Design Models (continued)

- Distributed sites with centralized authentication and security deployment
  - Rely on remote RADIUS servers for authentication
  - Management advantage
    - RADIUS servers and authentication database are all centrally located
  - Disadvantages
    - Depends on the reliability of the network connection
    - Bottleneck can occur if a large number of wireless users are supported

Authentication Design Models (continued)

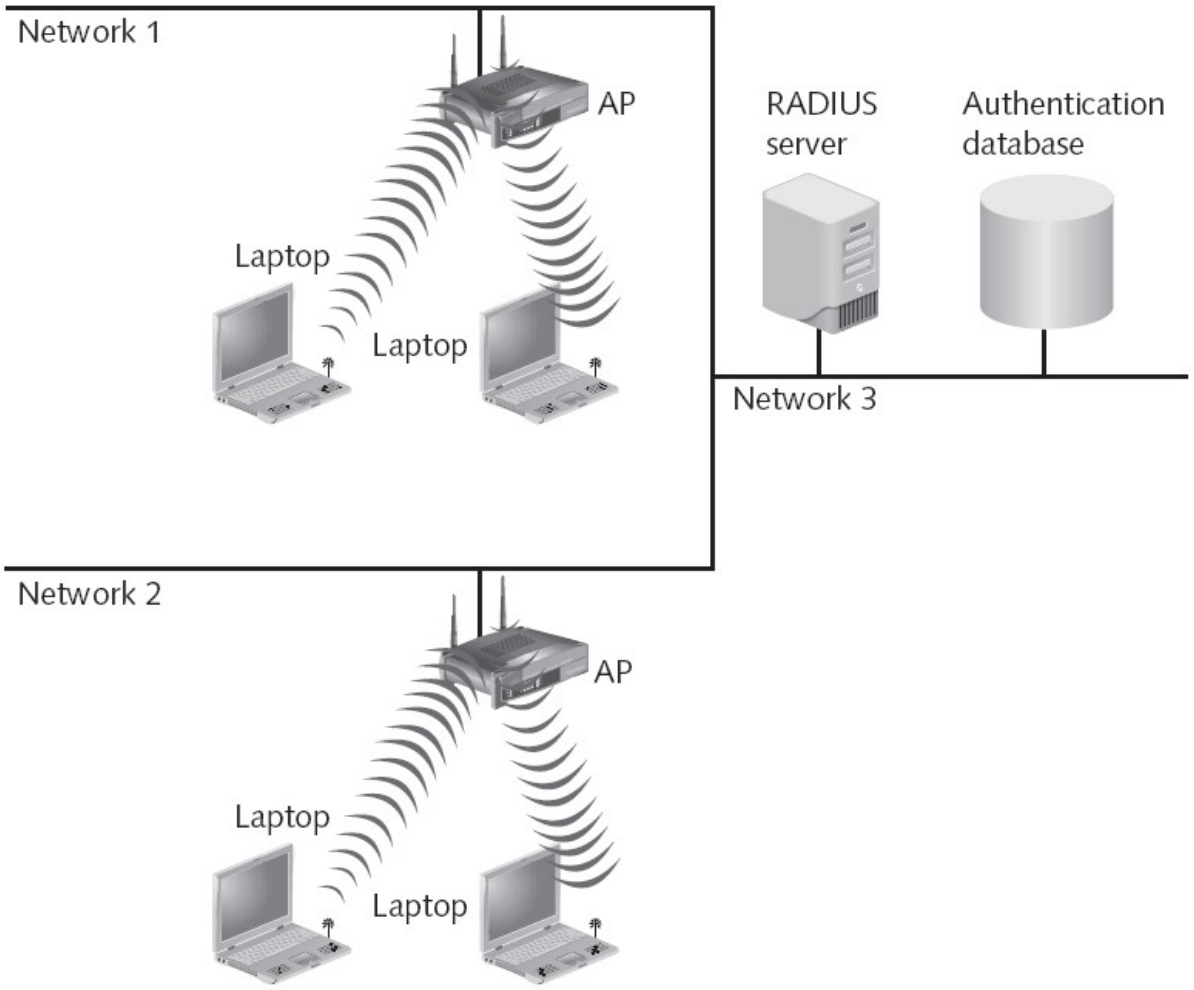


Figure 8-6 Distributed sites with centralized authentication and security deployment

Authentication Design Models (continued)

- Distributed sites and security with centralized authentication deployment
  - RADIUS servers are located at each site to perform authentication
  - Authentication database is centrally located
  - Advantage
    - Mitigates the bottleneck problem
  - Disadvantage
    - Depends on the reliability of the network connection

Authentication Design Models (continued)

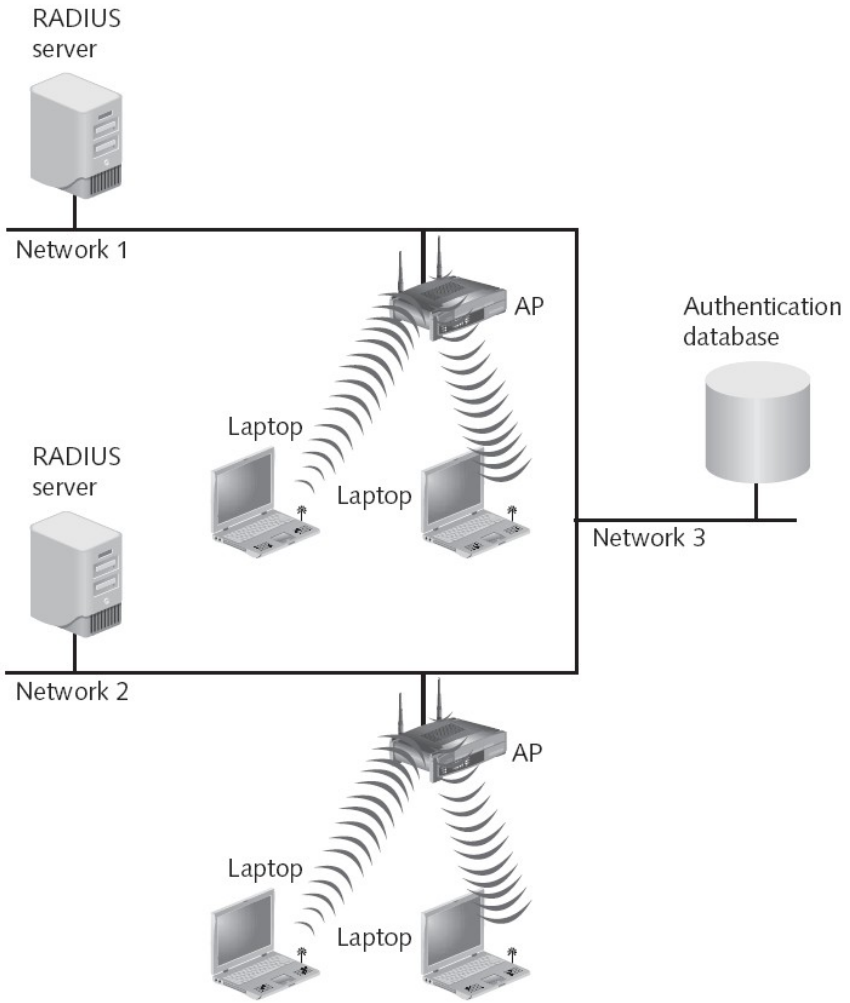


Figure 8-7 Distributed sites and security with centralized authentication deployment

Authentication Design Models (continued)

Table 8-1 Authentication design deployment models

Model	Location of RADIUS servers	Location of authentication database	Advantages	Disadvantages
Single site	Local	Local	Only one authentication database to support	May be difficult to scale if large number of users added
Distributed autonomous sites	Local	Remote	Does not rely on remote network connection	Not all authentication databases can be easily replicated
Distributed sites with centralized authentication and security	Remote	Remote	Authentication database more secure because not replicated	Dependent on reliable network link
Distributed sites and security with centralized authentication	Local	Remote	Reduces "bottleneck" processing	Dependent on reliable network link

Extended Authentication Protocols (EAP)

- Extensible Authentication Protocol (EAP)
  - Management protocol of IEEE 802.1x
  - Governs the interaction between the wireless device, access point, and RADIUS server
- EAP was designed with flexibility in mind
  - Different protocols can be used to support different authentication methods
    - And associated network security policies

Extended Authentication Protocols (EAP) (continued)

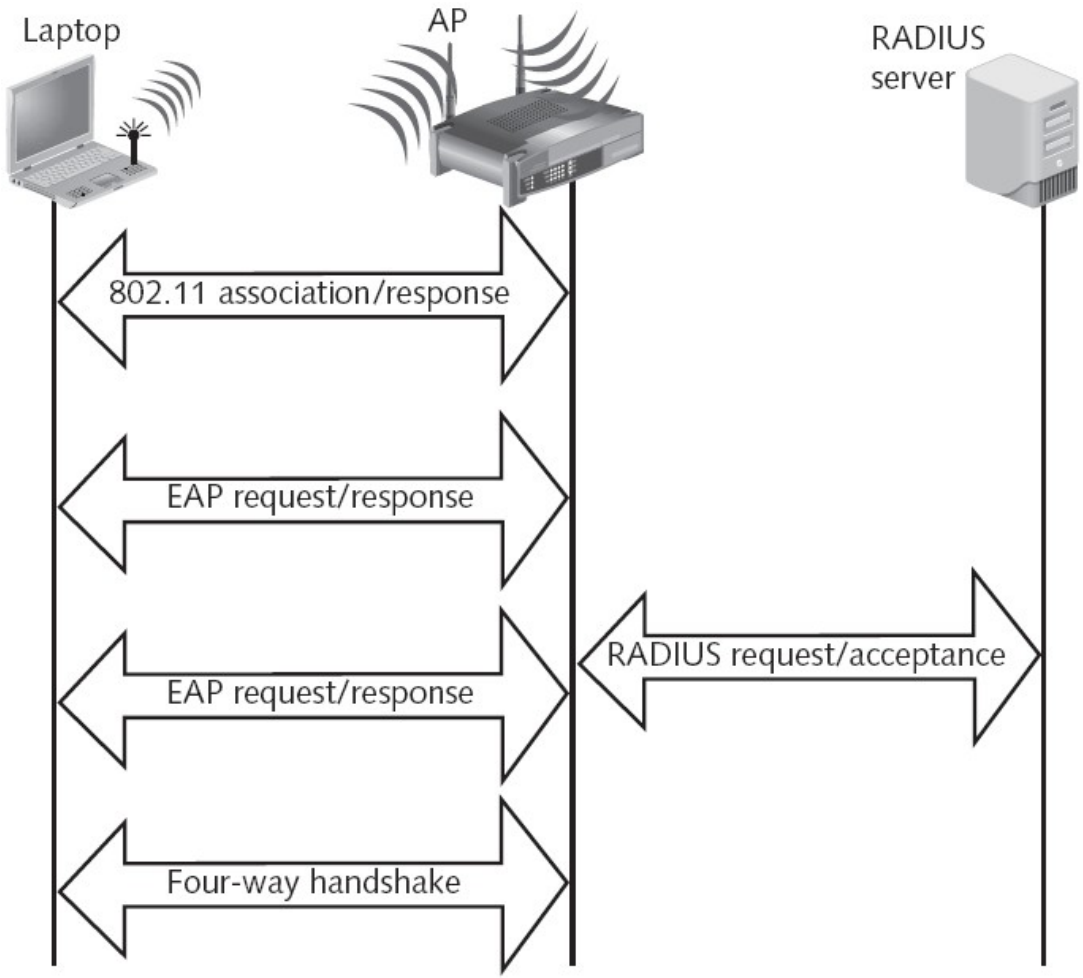


Figure 8-8 EAP in IEEE 802.1x

IEEE 802.11 Authentication and Key Management

- Once a user's device is authenticated, the next step is to enable encryption
- Encryption is based on a series of interrelated keys

IEEE 802.11 Authentication and Key Management

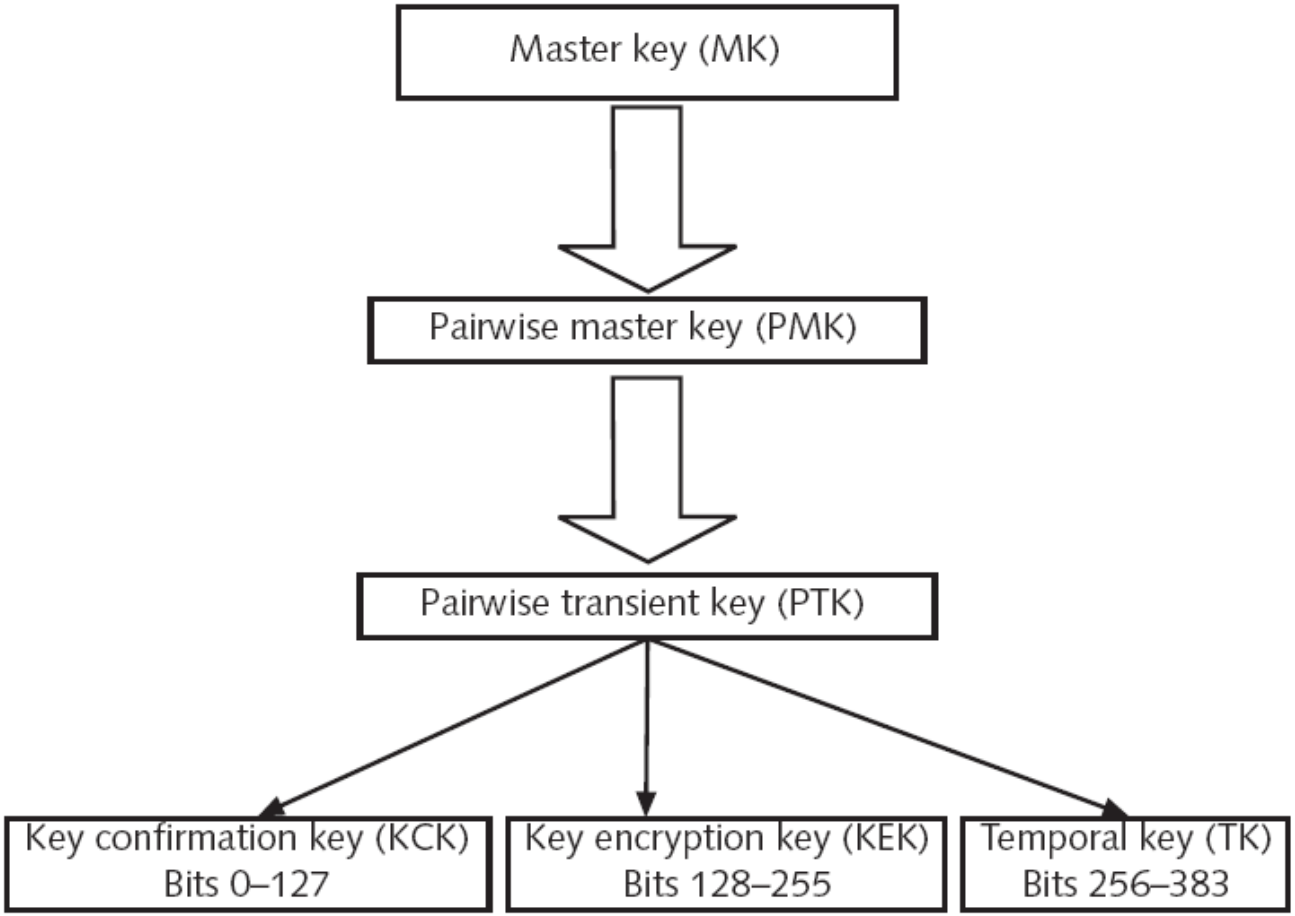


Figure 8-9 Key hierarchy

Master Key (MK)

- All other keys are formed from the master key
- When using IEEE 802.1x:
  - MK is sent from the authentication server (usually a RADIUS server) to the authenticator (access point)
    - As part of an acceptance packet
  - MK is encrypted within an EAP packet
  - AP forwards this packet directly to the wireless device
    - Without seeing its contents

Pairwise Master Key (PMK)

- Two ways for retrieving a PMK
  - In WPA or WPA2 Personal security model
    - Preshared key (PSK) is entered by a user into both the access point and the wireless device
    - PSK is used in conjunction with the SSID to form the mathematical basis of the PMK
  - In WPA or WPA2 Enterprise security model
    - PMK is generated by the RADIUS server and sent to the access point
    - Wireless device generates its own PMK

Pairwise Transient Key (PTK)

- PTK is generated by combining the PMK with four pieces of data
  - The supplicant's (wireless device) MAC address
  - The authenticator's (access point) MAC address
  - A nonce created by supplicant
  - A nonce created by the authenticator
- PTK is itself divided into three keys
  - Key confirmation key (KCK)
  - Key encryption key (KEK)
  - Temporal key

Pairwise Transient Key (PTK) (continued)

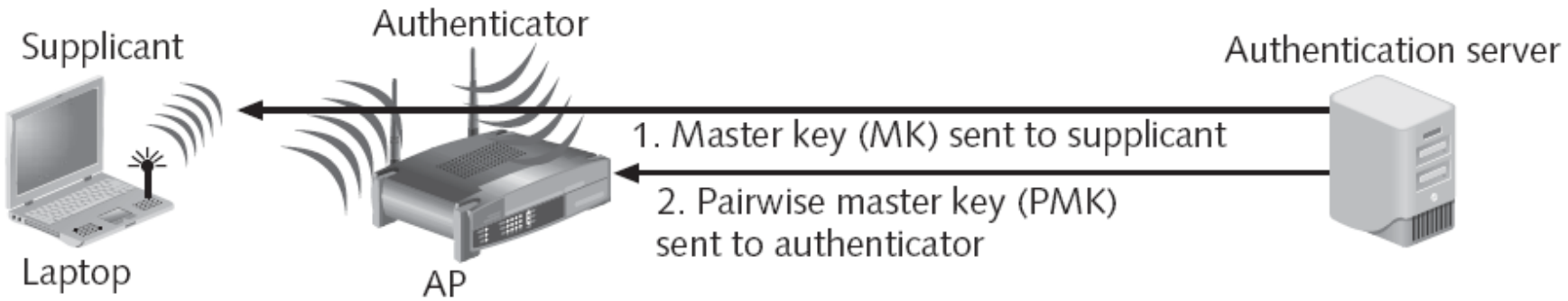


Figure 8-10 Key creation in WPA or WPA2 Enterprise security model

Pairwise Transient Key (PTK) (continued)

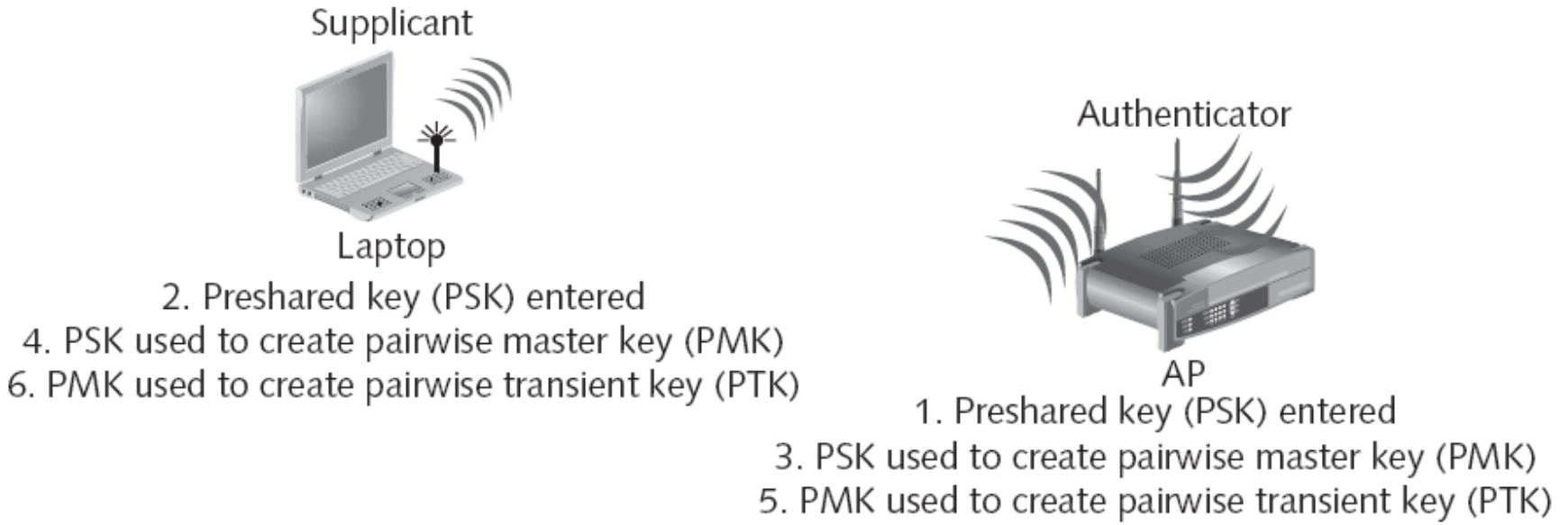


Figure 8-11 Key creation in WPA or WPA2 Personal security model

Group Keys (continued)

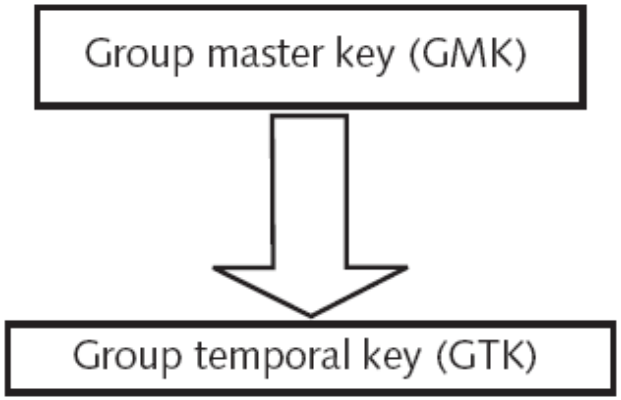


Figure 8-12 Group key hierarchy

Group Keys

- MKs are used for unicast transmissions
- Group keys (GK)
  - Used for broadcast transmissions
- Group master key (GMK)
  - Starting point of the group key hierarchy
  - Simply a random number
- Group temporal key (GTK)
  - Created using the GMK, authenticator's MAC address, and a nonce from the authenticator
  - Used to decrypt broadcast messages from APs

Handshakes (continued)

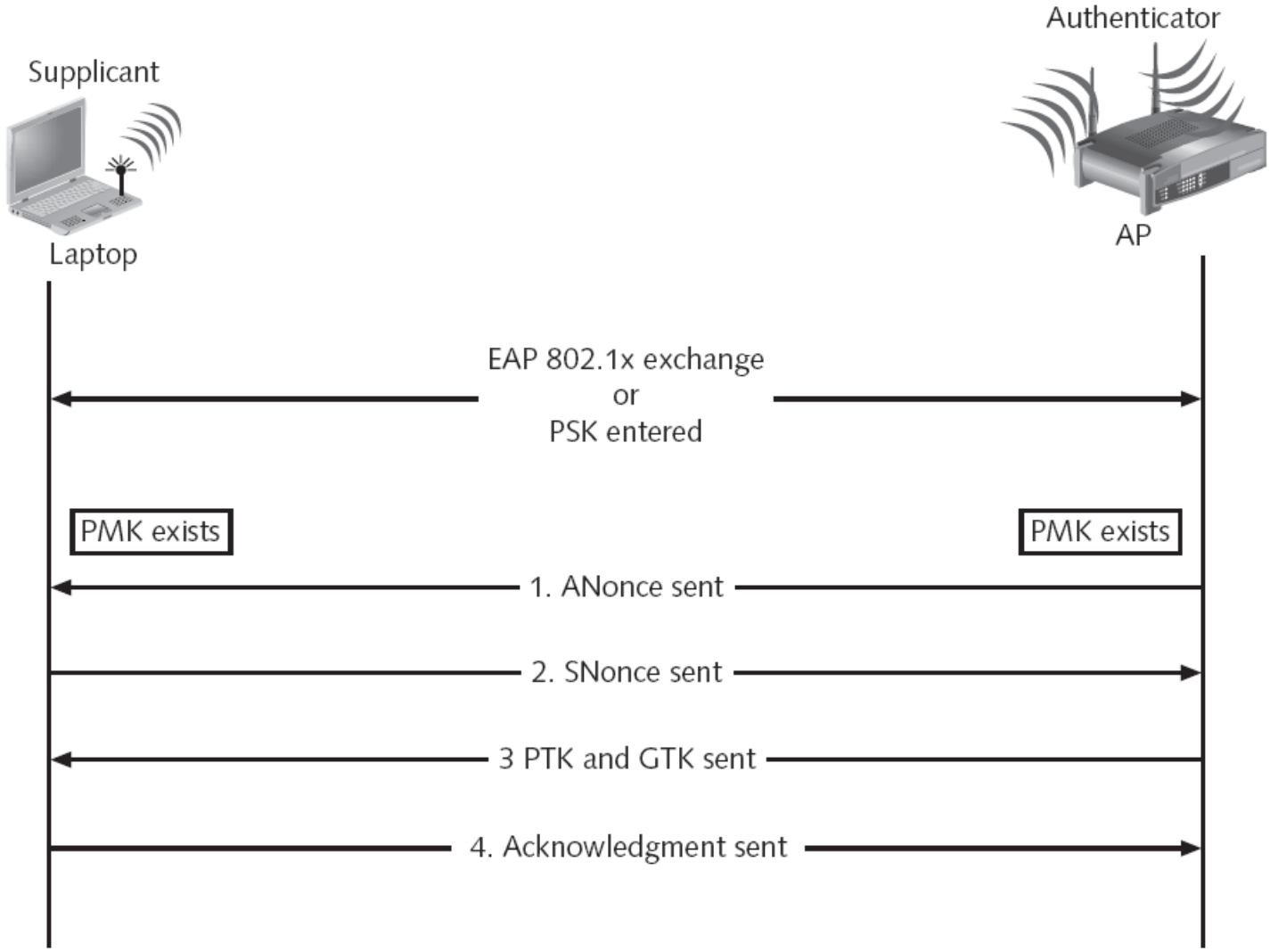


Figure 8-13 Four-way handshake

Handshakes

- Handshake
  - Exchange of info between APs and wireless devices
- Four-way handshake
  - Exchange of information for the MK
  - Accomplishes the following tasks:
    - Authenticates the security parameters that were negotiated
    - Confirms PMK between supplicant and authenticator
    - Establishes the temporal keys to be used by the data-confidentiality protocol

Handshakes (continued)

- Four-way handshake (continued)
  - Accomplishes the following tasks (continued):
    - Performs the first group key handshake
    - Provides keying material to implement the group key handshake
- Group-key handshake
  - Authenticates the GTK
  - Preceded by the four-way handshake

Wireless Authentication and Encryption Summary

- Based on the IEEE 802.11i security protocol
  - WPA Enterprise and WPA2 Enterprise security models utilize IEEE 802.1x port-based authentication
  - Credentials used can be passwords, biometrics, and digital certificates
  - EAP manages port-based authentication
  - EAP-TLS, PEAP, and others are used for encryption
- IEEE 802.1x
  - Provides the wireless device a unique encryption key called the MK
    - Used to create other encryption keys

Summary

- Wireless authentication is the process of a device proving that it is “genuine” and not an imposter
- Authentication servers are used to authenticate users in a WLAN
  - Most common type is a RADIUS server
- EAP
  - Management protocol of IEEE 802.1x that governs the interaction between the wireless device, access point, and RADIUS server

Summary (continued)

- IEEE 802.11 authentication and key management is based on a key hierarchy
- When an AP sends a broadcast packet to all wireless devices, GKs are used
  - Starting point of the group key hierarchy is the GMK