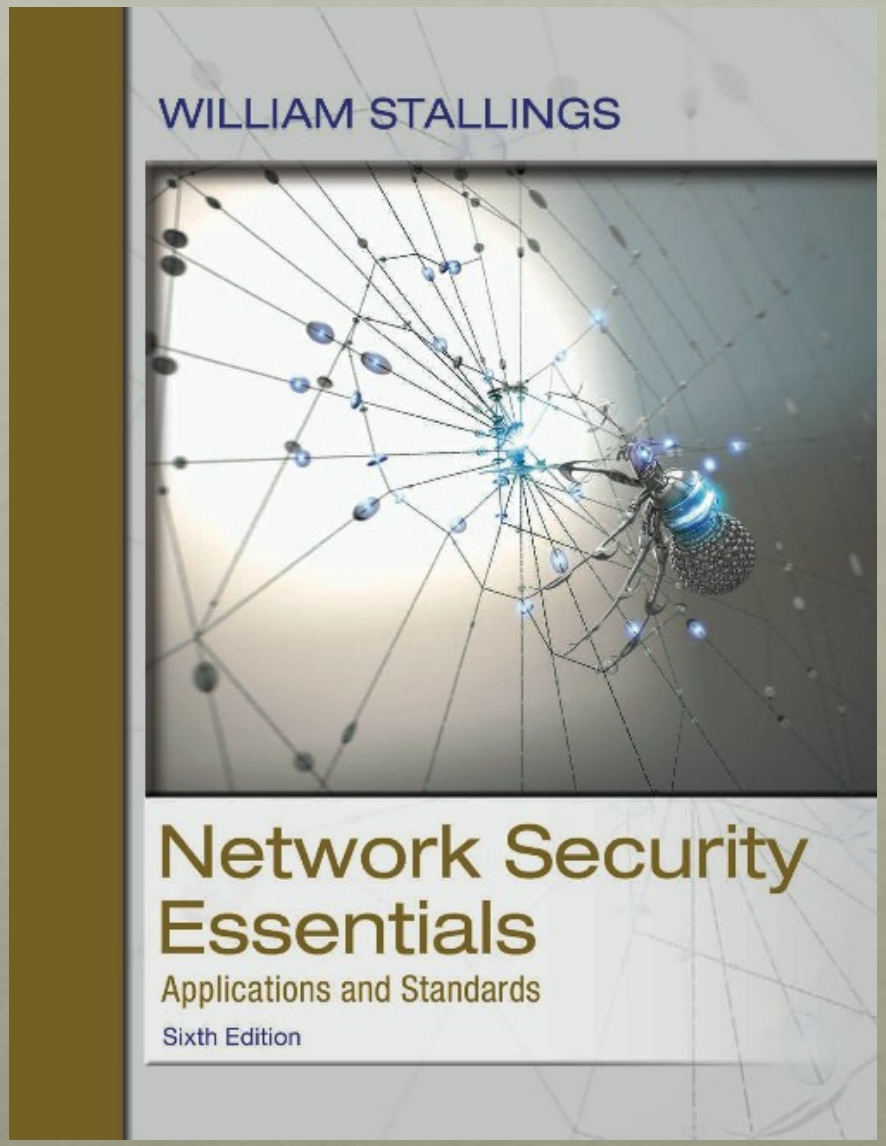
Network Security Essentials

Sixth Edition

by William Stallings



Chapter 7

Wireless Network Security

Wireless Security

Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include:

• Channel: Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks. Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols.

• Mobility: Wireless devices are, in principal and usually in practice, far more portable and mobile than wired devices. This mobility results in a number of risks, described subsequently.

• Resources: Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware.

• Accessibility: Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks

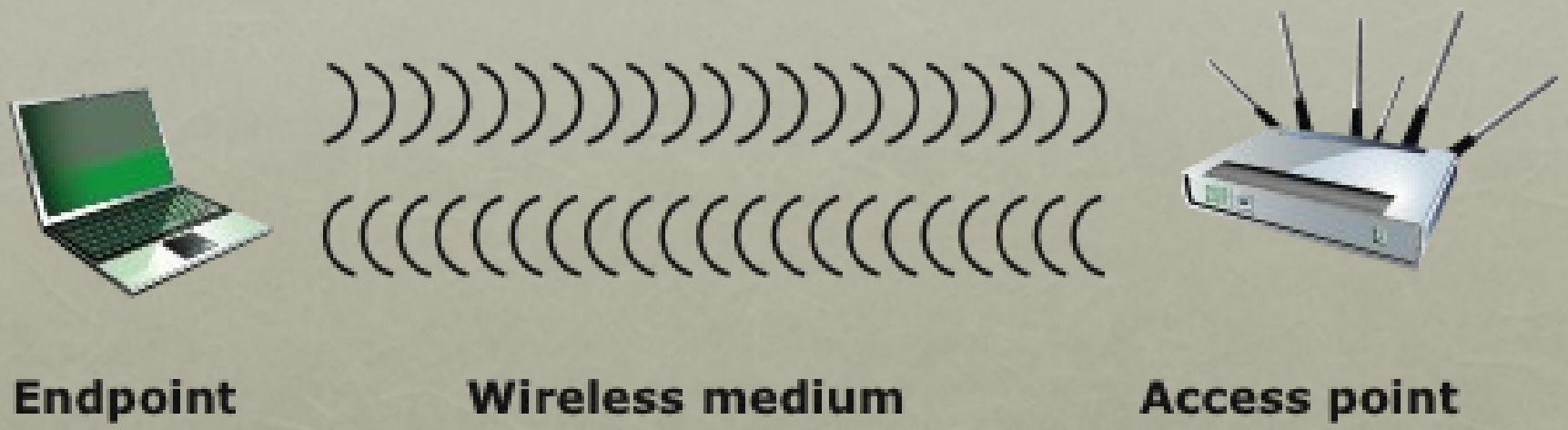


Figure 7.1 Wireless Networking Components

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Wireless Network Threats

• Accidental association: Company wireless LANs or wireless access points to wired LANs in close proximity (e.g., in the same or neighboring buildings) may create overlapping transmission ranges.

• Malicious association: In this situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.

• Ad hoc networks: These are peer-to-peer networks between wireless computers with no access point between them. Such networks can pose a security threat due to a lack of a central point of control.

• Nontraditional networks: Nontraditional networks and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs, pose a security risk in terms of both eavesdropping and spoofing.

• Identity theft (MAC spoofing): This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.

• Man-in-the middle attacks: This type of attack is described in Chapter 3 in the context of the Diffie-Hellman key exchange protocol. In a broader sense, this attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device. Wireless networks are particularly vulnerable to such attacks.

• Denial of service (DoS): This type of attack is discussed in detail in Chapter 10. In the context of a wireless network, a DoS attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources.

• Network injection: A network injection attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages.

Securing Wireless Transmissions

- The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption
- To deal with eavesdropping, two types of countermeasures are appropriate:
  - Signal-hiding techniques
    - Turn off SSID broadcasting by wireless access points
    - Assign cryptic names to SSIDs
    - Reduce signal strength to the lowest level that still provides requisite coverage
    - Locate wireless access points in the interior of the building, away from windows and exterior walls
  - Encryption
    - Is effective against eavesdropping to the extent that the encryption keys are secured

Securing Wireless Access Points

- The main threat involving wireless access points is unauthorized access to the network
- The principal approach for preventing such access is the IEEE 802.1x standard for port-based network access control
  - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
  - The use of 802.1x can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

Securing Wireless Networks

1. Use encryption. Wireless routers are typically equipped with built-in encryption mechanisms for router-to-router traffic.

2. Use antivirus and antispyware software, and a firewall. These facilities should be enabled on all wireless network endpoints.

3. Turn off identifier broadcasting. Wireless routers are typically configured to broadcast an identifying signal so that any device within range can learn of the router's existence. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.

4. Change the identifier on your router from the default. Again, this measure thwarts attackers who will attempt to gain access to a wireless network using default router identifiers.

5. Change your router's pre-set password for administration. This is another prudent step.

6. Allow only specific computers to access your wireless network. A router can be configured to only communicate with approved MAC addresses. Of course, MAC addresses can be spoofed, so this is just one element of a security strategy

Mobile Device Security

- Mobile devices have become an essential element for organizations as part of the overall network infrastructure
- Prior to the widespread use of smartphones, network security was based upon clearly defined perimeters that separated trusted internal networks from the untrusted Internet
- Due to massive changes, an organization's networks must now accommodate:
  - Growing use of new devices
  - Cloud-based applications
  - De-perimeterization
  - External business requirements

Security Threats

- Major security concerns for mobile devices:

Mobile devices need additional, specialized protection measures beyond those implemented for other client devices, such as desktop and laptop devices that are used only within the organization's facilities and on the organization's networks. SP 800-14 (Guidelines for Managing and Securing Mobile Devices in the Enterprise , July 2012) lists seven major security concerns for mobile devices. We examine each of these in turn.

Lack of Physical Security Controls

Mobile devices are typically under the complete control of the user, and are used and kept in a variety of locations outside the organization's control, including off premises. Even if a device is required to remain on premises, the user may move the device within the organization between secure and nonsecured locations. Thus, theft and tampering are realistic threats.

The security policy for mobile devices must be based on the assumption that any mobile device may be stolen or at least accessed by a malicious party. The threat is twofold: A malicious party may attempt to recover sensitive data from the device itself, or may use the device to gain access to the organization's resources.

Use of Untrusted Mobile Devices

In addition to company-issued and company controlled mobile devices, virtually all employees will have personal smartphones and/or tablets. The organization must assume that these devices are not trustworthy. That is, the devices may not employ encryption and either the user or a third party may have installed a bypass to the built-in restrictions on security, operating system use, and so on.

Use of Untrusted Networks

If a mobile device is used on premises, it can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from the Internet to the organization. Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks. Thus, the security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy.

Use of Applications Created by Unknown Parties

By design, it is easy to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software. An organization has several options for dealing with this threat, as described subsequently.

Interaction with Other Systems

A common feature found on smartphones and tablets is the ability to automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage. Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware.

Use of Untrusted Content

Mobile devices may access and use content that other computing devices do not encounter. An example is the Quick Response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. The QR code translates to a URL, so that a malicious QR code could direct the mobile device to malicious Web sites.

Use of Location Services

The GPS capability on mobile devices can be used to maintain a knowledge of the physical location of the device. While this feature might be useful to an organization as part of a presence service, it creates security risks. An attacker can use the location information to determine where the device and user are located, which may be of use to the attacker.

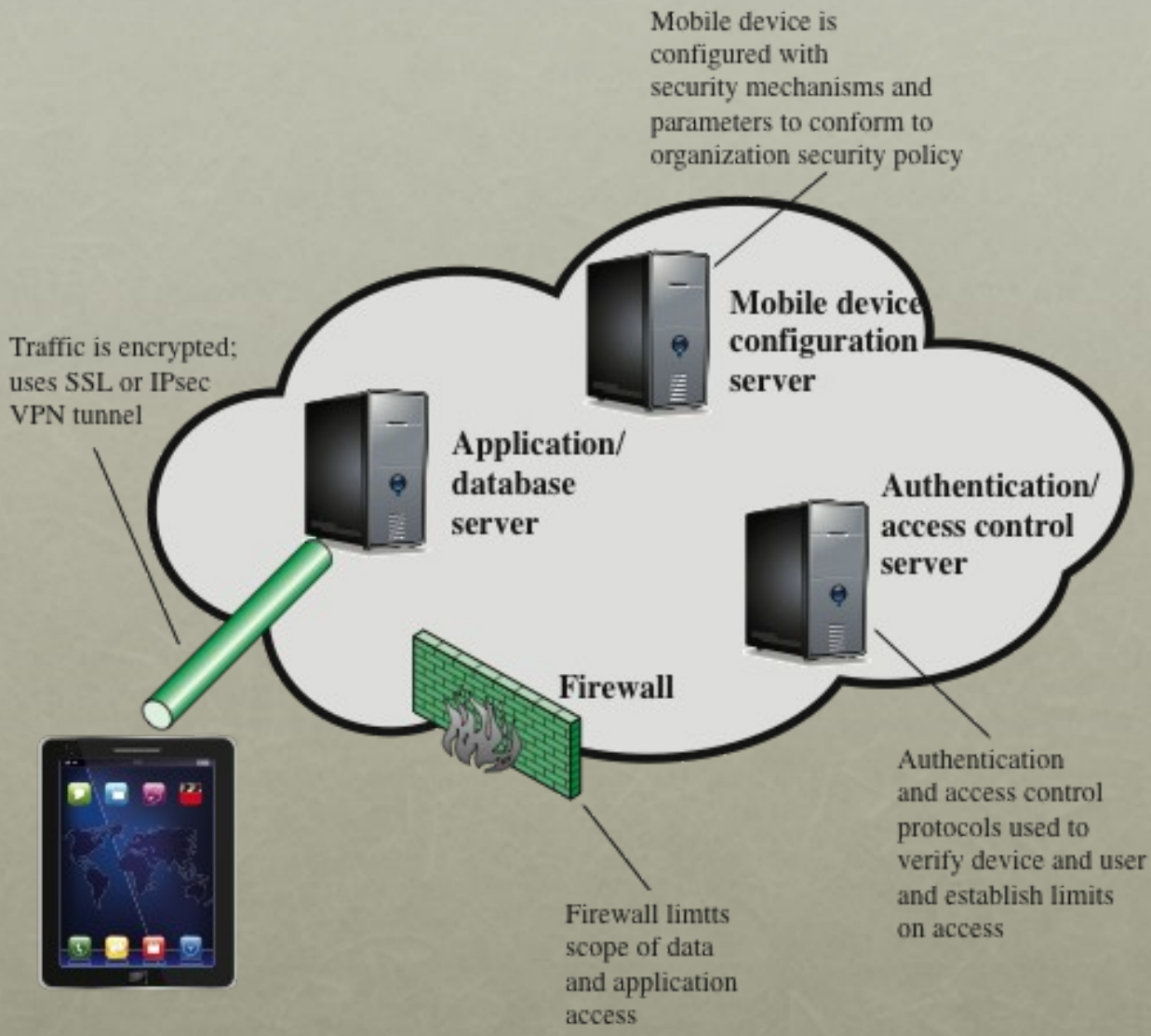


Figure 7.2 Mobile Device Security Elements

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

IEEE 802.11 Wireless LAN Overview

- IEEE 802 is a committee that has developed standards for a wide range of local area networks (LANs)
- In 1990 the IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs)
- Since that time, the demand for WLANs at different frequencies and data rates has exploded

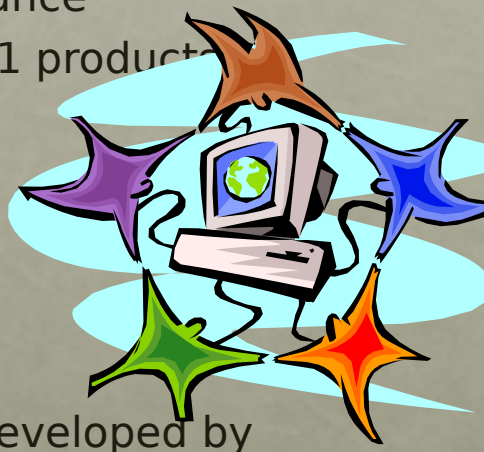
Table 7.1
IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

(Table is on page 215 in the textbook)

Wi-Fi Alliance

- The first 802.11 standard to gain broad industry acceptance was 802.11b
- Wireless Ethernet Compatibility Alliance (WECA)
  - An industry consortium formed in 1999
  - Subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance
  - Created a test suite to certify interoperability for 802.11 products
- Wi-Fi
  - The term used for certified 802.11b products
  - Has been extended to 802.11g products
- Wi-Fi5
  - A certification process for 802.11a products that was developed by the Wi-Fi Alliance
  - Recently the Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards
  - Referred to as Wi-Fi Protected Access (WPA)



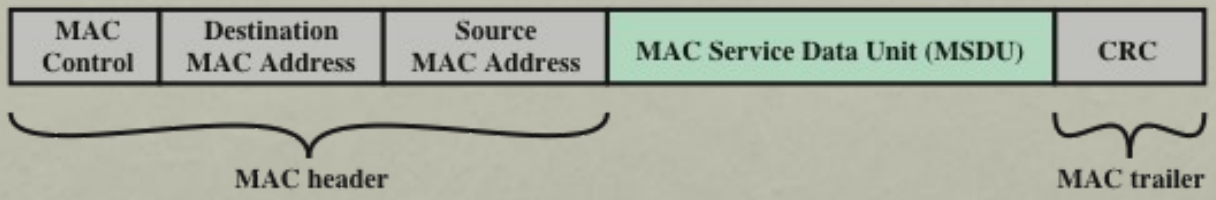


Figure 7.4 General IEEE 802 MPDU Format

• MAC Control: This field contains any protocol control information needed for the functioning of the MAC protocol. For example, a priority level could be indicated here.

• Destination MAC Address: The destination physical address on the LAN for this MPDU.

• Source MAC Address: The source physical address on the LAN for this MPDU.

• MAC Service Data Unit: The data from the next higher layer.

• CRC: The cyclic redundancy check field; also known as the Frame Check Sequence (FCS) field. This is an error-detecting code, such as that which is used in other data-link control protocols. The CRC is calculated based on the bits in the entire MPDU. The sender calculates the CRC and adds it to the frame. The receiver performs the same calculation on the incoming MPDU and compares that calculation to the CRC field in that incoming MPDU. If the two values don't match, then one or more bits have been altered in transit

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

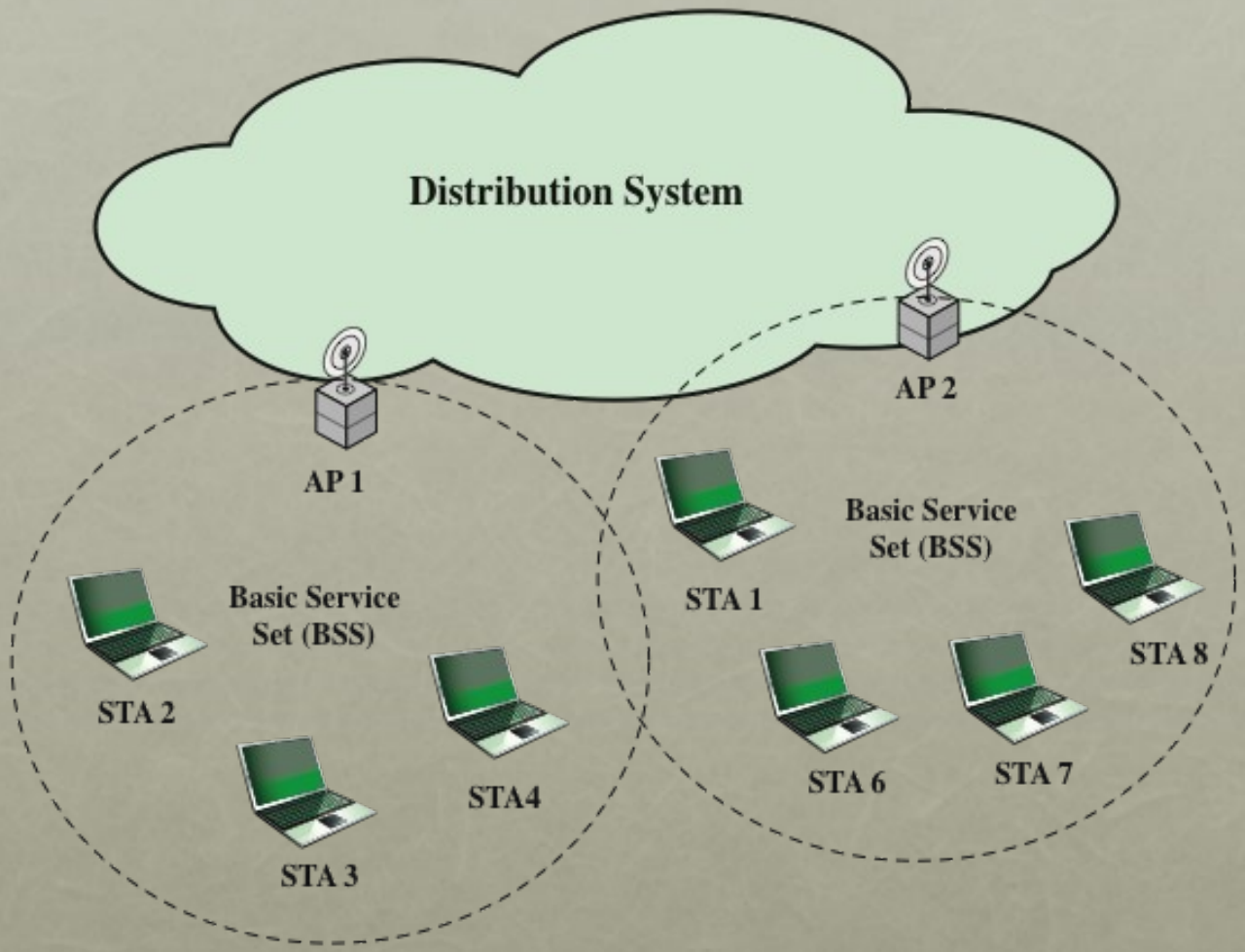


Figure 7.5 IEEE 802.11 Extended Service Set

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

Table 7.2 IEEE 802.11 Services

Association-Related Services

Transition types based on mobility:

The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service. For that service to function, it requires information about stations within the ESS that is provided by the association-related services. Before the distribution service can deliver data to or accept data from a station, that station must be associated. Before looking at the concept of association, we need to describe the concept of mobility. The standard defines three transition types, based on mobility:

- No transition: A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.

- BSS transition: This is defined as a station movement from one BSS to another BSS within the same ESS. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.

- ESS transition: This is defined as a station movement from a BSS in one ESS to a BSS within another ESS. This case is supported only in the sense that the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. In fact, disruption of service is likely to occur.

Association-Related Services

- To deliver a message within a DS, the distribution service needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station
- Three services relate to a station maintaining an association with the AP within its current BSS:
  - Association
    - Establishes an initial association between a station and an AP
  - Reassociation
    - Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another
  - Disassociation
    - A notification from either a station or an AP that an existing association is terminated

IEEE 802.11I Wireless LAN Security

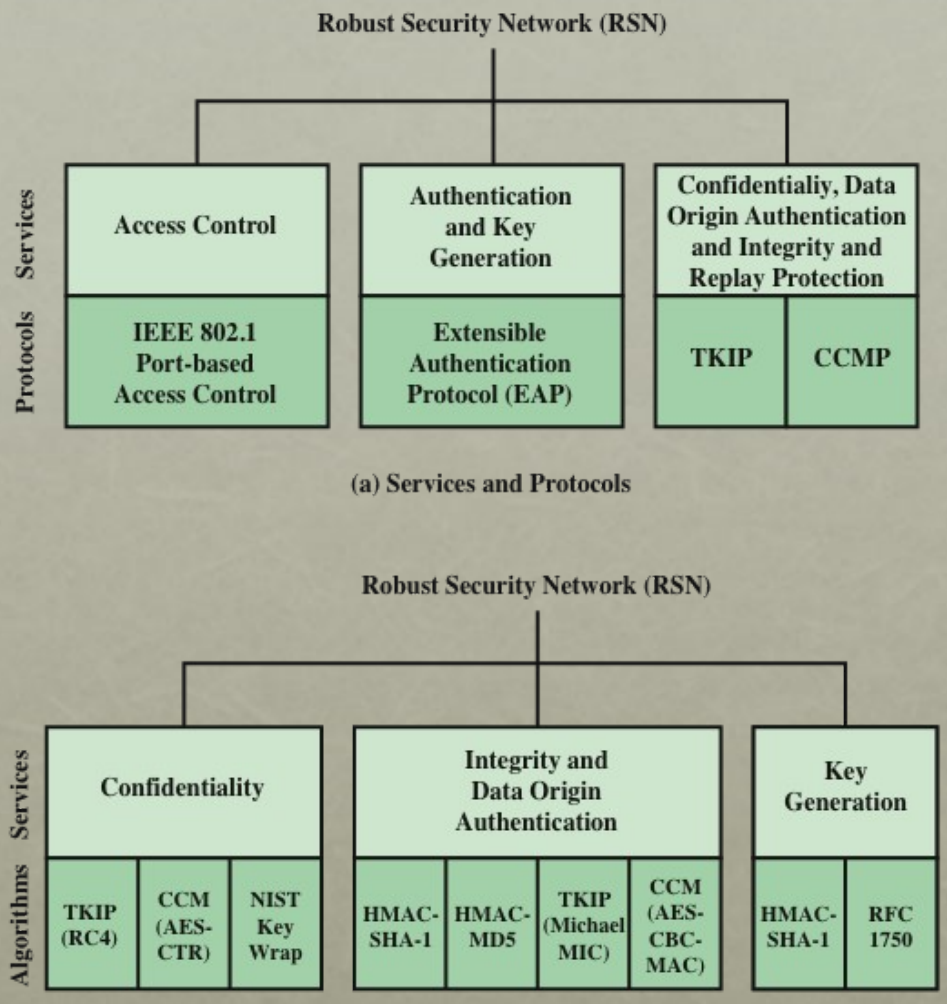
There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN in that it requires some positive and presumably observable action to connect a station to a wired LAN.

2. Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

These differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs. The original 802.11 specification included a set of security features for privacy and authentication that were quite weak. For privacy, 802.11 defined the Wired Equivalent Privacy (WEP) algorithm. The privacy portion of the 802.11 standard contained major weaknesses. Subsequent to the development of WEP, the 802.11i task group has developed a set of capabilities to address the WLAN security issues.

In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard. WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard. The final form of the 802.11i standard is referred to as Robust Security Network (RSN) . The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.



CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure 7.6 Elements of IEEE 802.11i

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

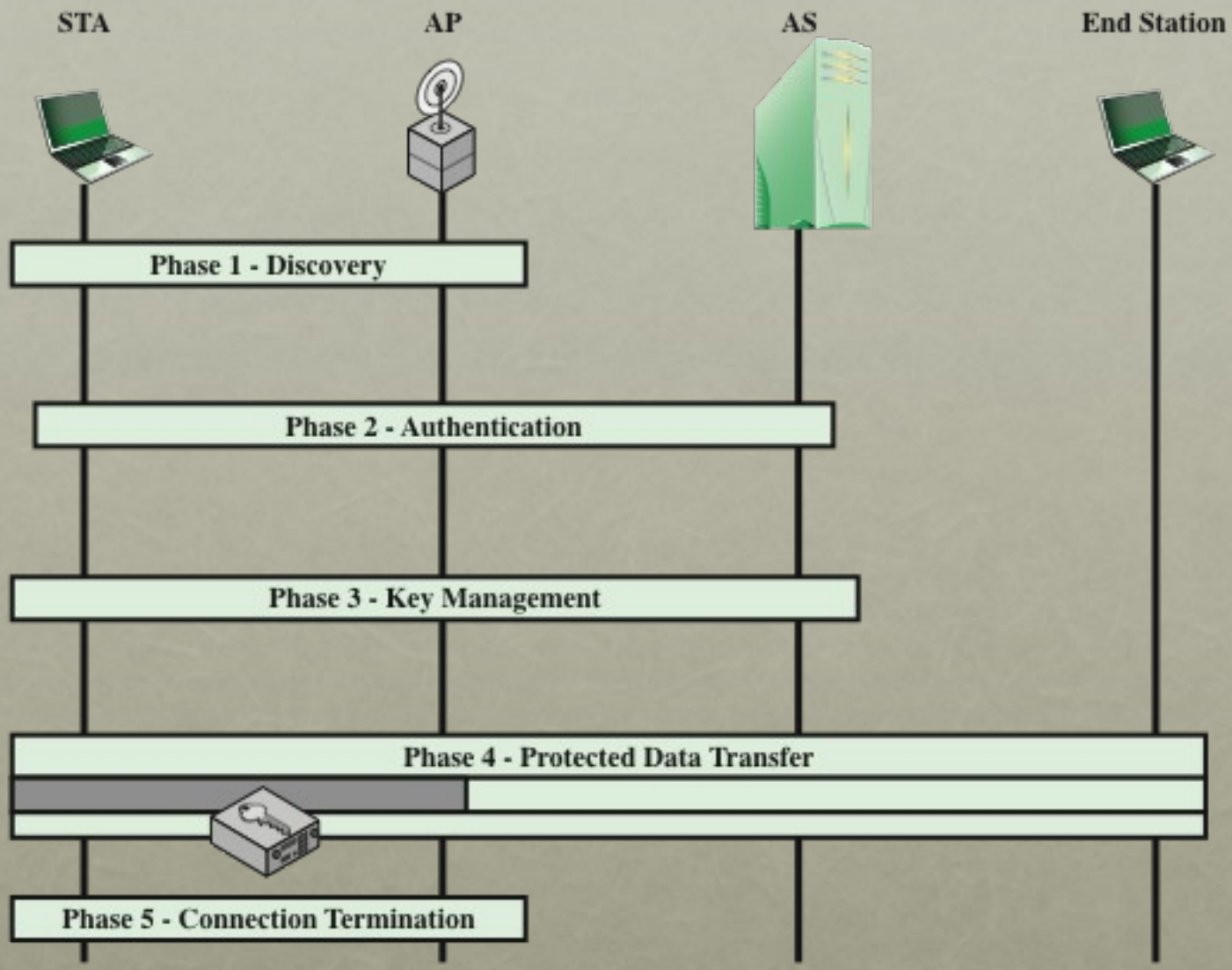


Figure 7.7 IEEE 802.11i Phases of Operation

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

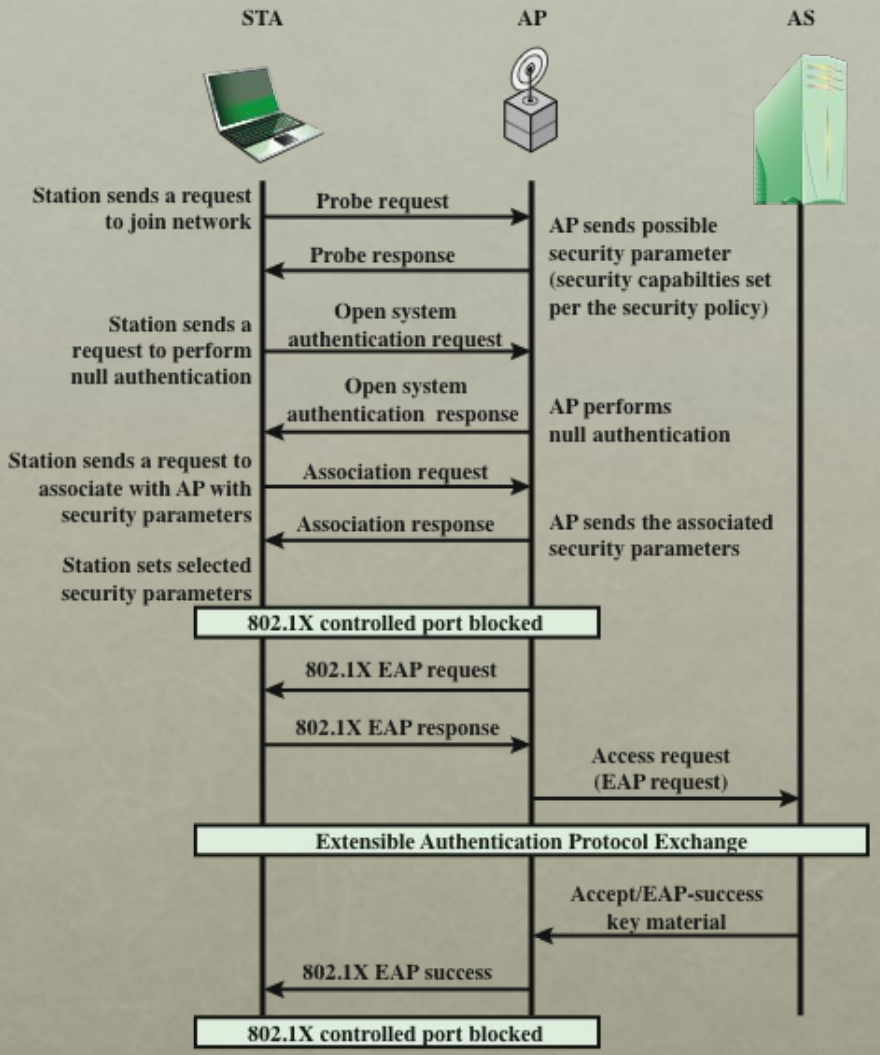


Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

IEEE 802.1X Access Control Approach

Port-Based Network Access Control
The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard

IEEE 802.11i makes use of another standard that was designed to provide access control functions for LANs. The standard is IEEE 802.1X, Port-Based Network Access Control. The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard. IEEE 802.1X uses the terms supplicant , authenticator , and authentication server (AS). In the context of an 802.11 WLAN, the first two terms correspond to the wireless station and the AP. The AS is typically a separate deviceon the wired side of the network (i.e., accessible over the DS) but could also reside directly on the authenticator.

Before a supplicant is authenticated by the AS using an authentication protocol, the authenticator only passes control or authentication messages between the
supplicant and the AS; the 802.1X control channel is unblocked, but the 802.11 data channel is blocked. Once a supplicant is authenticated and keys are provided, the authenticator can forward data from the supplicant, subject to predefined access control limitations for the supplicant to the network. Under these circumstances, the data channel is unblocked.

As indicated in Figure 5.5, 802.1X uses the concepts of controlled and uncontrolled ports. Ports are logical entities defined within the authenticator and refer to physical network connections. For a WLAN, the authenticator (the AP) may have only two physical ports: one connecting to the DS and one for wireless communication within its BSS. Each logical port is mapped to one of these two physical ports. An uncontrolled port allows the exchange of PDUs between the supplicant and the other AS, regardless of the authentication state of the supplicant. A controlled port allows the exchange of PDUs between a supplicant and other systems on the LAN only if the current state of the supplicant authorizes such an exchange. IEEE 802.1X is covered in more detail in Chapter 5.

The 802.1X framework, with an upper-layer authentication protocol, fits nicely with a BSS architecture that includes a number of wireless stations and an AP. However, for an IBSS, there is no AP. For an IBSS, 802.11i provides a more complex solution that, in essence, involves pairwise authentication between stationson the IBSS.

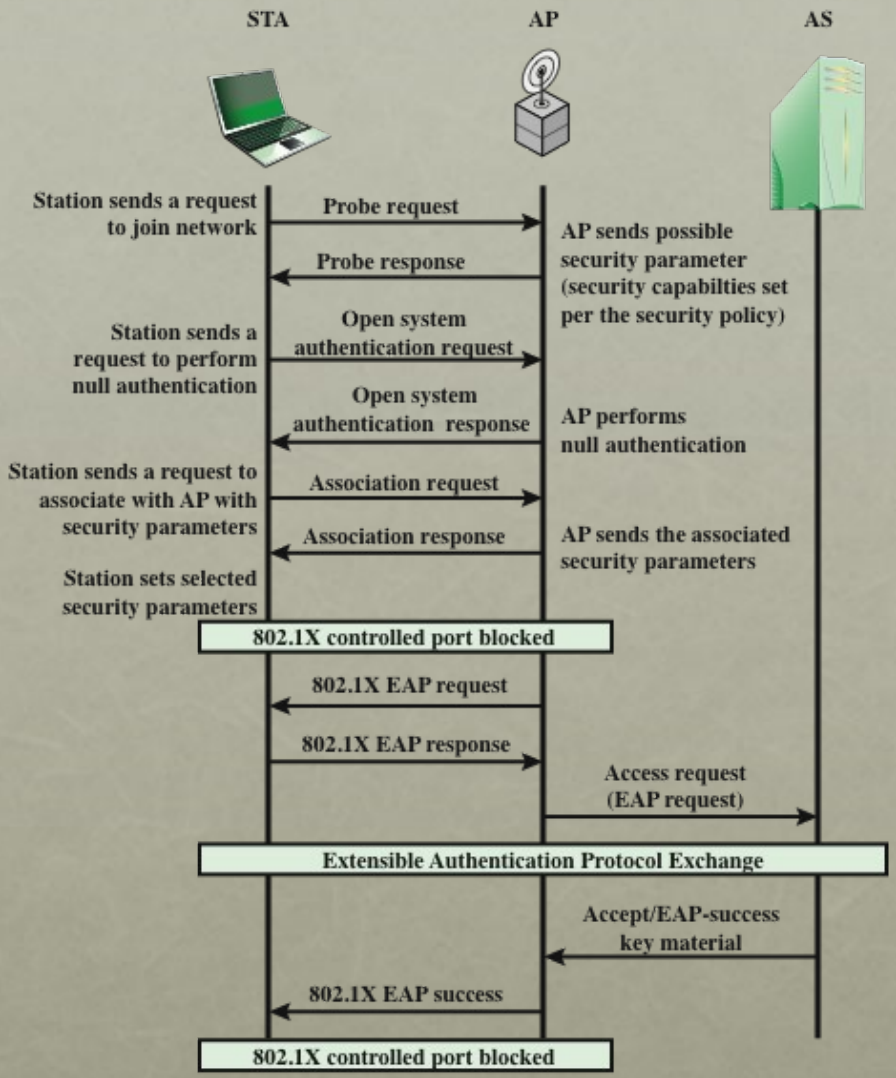
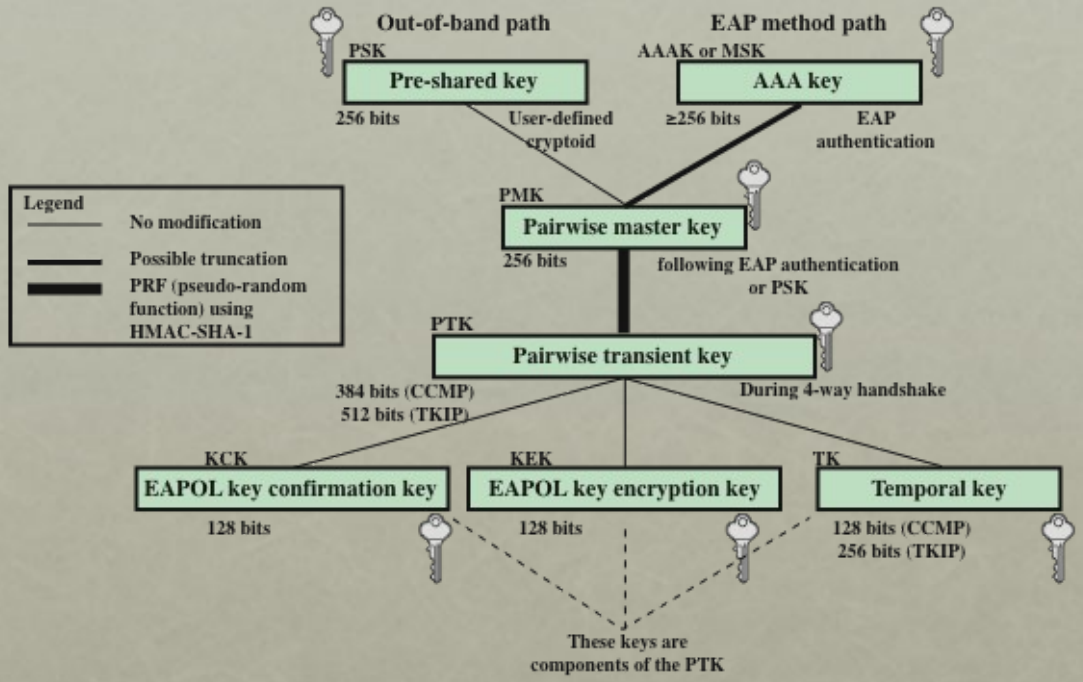
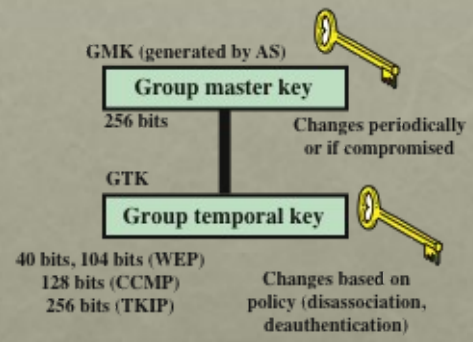


Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.



(a) Pairwise key hierarchy



(b) Group key hierarchy

Figure 7.9 IEEE 802.11i Key Hierarchies

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 7.3

IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

(Table can be found on page 229 in textbook)

Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

Pairwise Keys

- **Used for communication between a pair of devices, typically between a STA and an AP**
  - These keys form a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time
- **Pre-shared key (PSK)**
  - A secret key shared by the AP and a STA and installed in some fashion outside the scope of IEEE 802.11i
- **Master session key (MSK)**
  - Also known as the AAAK, and is generated using the IEEE 802.1X protocol during the authentication phase
- **Pairwise master key (PMK)**
  - Derived from the master key
  - If a PSK is used, then the PSK is used as the PMK; if a MSK is used, then the PMK is derived from the MSK by truncation
- **Pairwise transient key (PTK)**
  - Consists of three keys to be used for communication between a STA and AP after they have been mutually authenticated
  - Using the STA and AP addresses in the generation of the PTK provides protection against session hijacking and impersonation; using nonces provides additional random keying material

PTK Parts

The three parts of the PTK are as follows.

- EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK): Supports the integrity and data origin authenticity of STA-to-AP control frames during operational setup of an RSN. It also performs an access control function: proof-of-possession of the PMK. An entity that possesses the PMK is authorized to use the link.

- EAPOL Key Encryption Key (EAPOL-KEK): Protects the confidentiality of keys and other data during some RSN association procedures.

- Temporal Key (TK): Provides the actual protection for user traffic.

Group Keys

- Group keys are used for multicast communication in which one STA sends MPDUs to multiple STAs
  - Group master key (GMK)
    - Key-generating key used with other inputs to derive the GTK
  - Group temporal key (GTK)
    - Generated by the AP and transmitted to its associated STAs
    - IEEE 802.11i requires that its value is computationally indistinguishable from random
    - Distributed securely using the pairwise keys that are already established
    - Is changed every time a device leaves the network

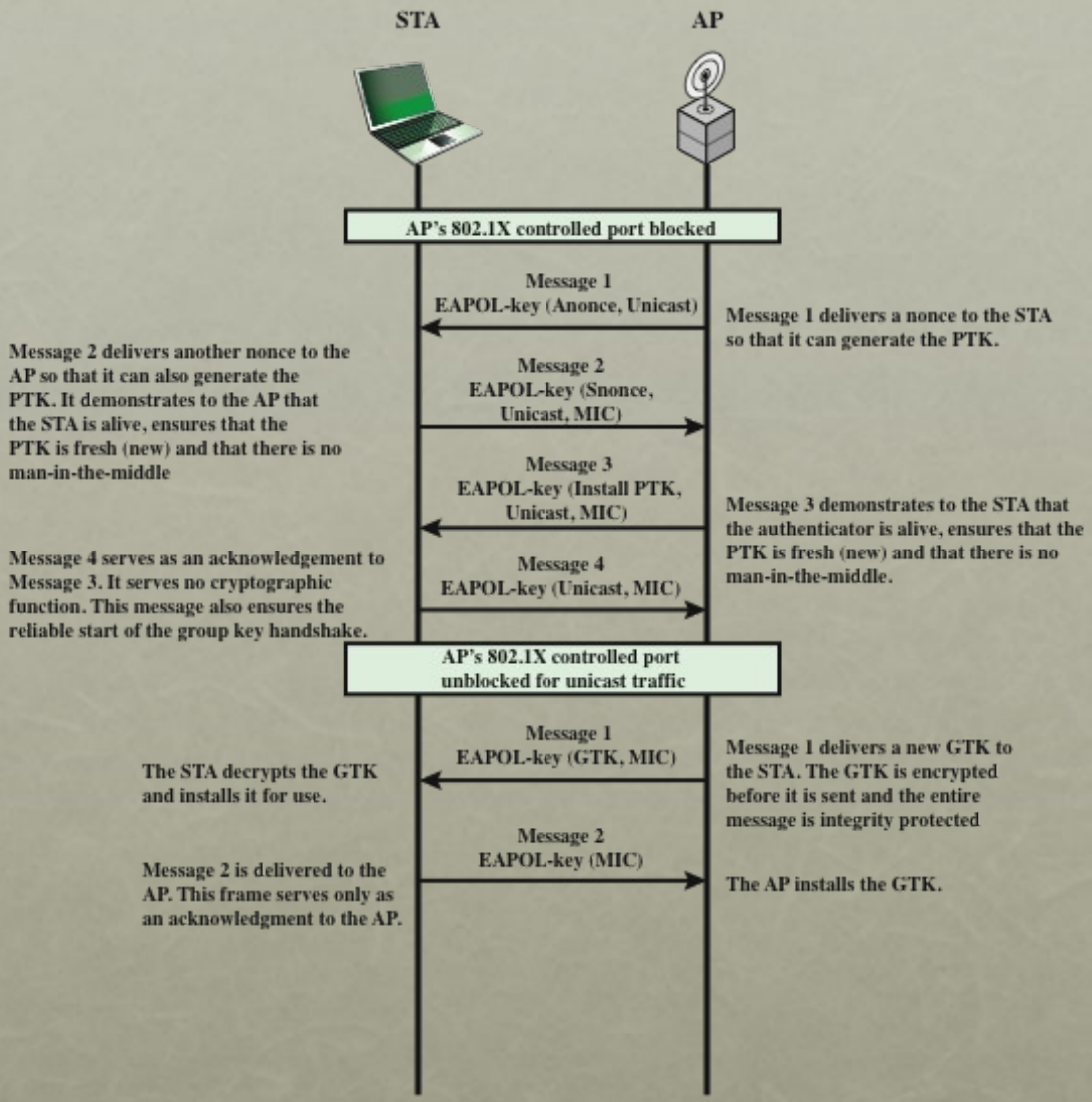


Figure 7.10 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Protected Data Transfer Phase

IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs: the Temporal Key Integrity Protocol (TKIP), and the Counter Mode-CBC MAC Protocol (CCMP).

TKIP is designed to require only software changes to devices that are implemented with the older wireless LAN security approach called Wired Equivalent Privacy (WEP). TKIP provides two services:

• Message integrity: TKIP adds a message integrity code (MIC) to the 802.11 MAC frame after the data field. The MIC is generated by an algorithm, called Michael, that computes a 64-bit value using as input the source and destination MAC address values and the Data field, plus key material.

• Data confidentiality: Data confidentiality is provided by encrypting the MPDU plus MIC value using RC4.

The 256-bit TK (Figure 7.9) is employed as follows. Two 64-bit keys are used with the Michael message digest algorithm to produce a message integrity code. One key is used to protect STA-to-AP messages, and the other key is used to protect AP-to-STA messages. The remaining 128 bits are truncated to generate the RC4 key used to encrypt the transmitted data.

For additional protection, a monotonically increasing TKIP sequence counter (TSC) is assigned to each frame. The TSC serves two purposes. First, the TSC is included with each MPDU and is protected by the MIC to protect against replay attacks. Second, the TSC is combined with the session TK to produce a dynamic encryption key that changes with each transmitted MPDU, thus making cryptanalysismore difficult.

CCMP is intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme. As with TKIP, CCMP provides two services:

• Message integrity: CCMP uses the cipher block chaining message authentication code (CBC-MAC), described in Chapter 3.

• Data confidentiality: CCMP uses the CTR block cipher mode of operation with AES for encryption. CTR is described in Chapter 2.

The same 128-bit AES key is used for both integrity and confidentiality.

The scheme uses a 48-bit packet number to construct a nonce to prevent replay attacks.

Summary

- Wireless network security
  - Network threats
  - Security measures
- Mobile device security
  - Security threats
  - Security strategy
- IEEE 802.11 wireless LAN overview
  - Wi-Fi Alliance
  - IEEE 802 protocol architecture
  - IEEE 802.11 network components and architectural model
  - IEEE 802.11 services
- IEEE 802.11i wireless LAN security
  - IEEE 802.11i services
  - IEEE 802.11i phases of operation
  - Discovery phase
  - Authentication phase
  - Key management phase
  - Protected data transfer phase
  - The IEEE 802.11i pseudorandom function

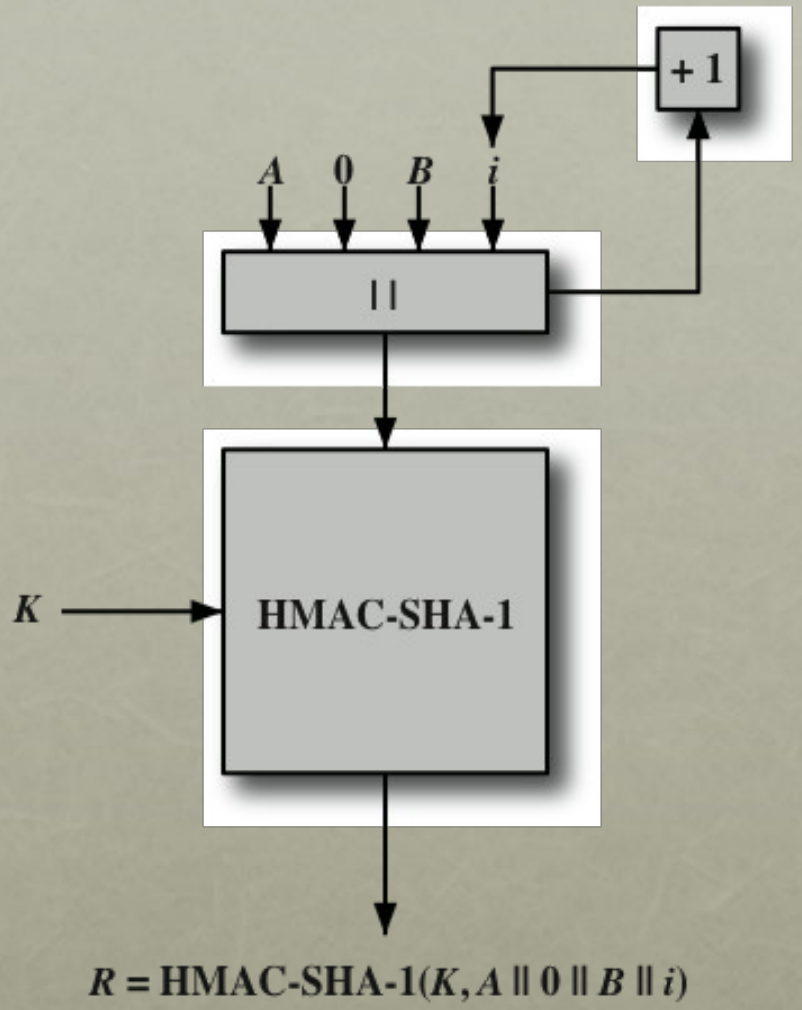


Figure 7.11 IEEE 802.11i Pseudorandom Function

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

IEEE 802.11i Pseudorandom Function (PRF)

- Used at a number of places in the IEEE 802.11i scheme (to generate nonces, to expand pairwise keys, to generate the GTK)
  - Best security practice dictates that different pseudorandom number streams be used for these different purposes
- Built on the use of HMAC-SHA-1 to generate a pseudorandom bit stream

Distribution of Messages Within a DS

- The two services involved with the distribution of messages within a DS are:

The two services involved with the distribution of messages within a DS are distribution and integration. Distribution is the primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS. For example, suppose a frame is to be sent from station 2 (STA 2) to station 7 (STA 7) in Figure 7.5. The frame is sent from STA 2 to AP 1, which is the AP for this BSS. The AP gives the frame to the DS, which has the job of directing the frame to the AP associated with STA 7 in the target BSS. AP 2 receives the frame and forwards it to STA 7. How the message is transported through the DS is beyond the scope of the IEEE 802.11 standard.

If the two stations that are communicating are within the same BSS, then the distribution service logically goes through the single AP of that BSS.

The integration service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN. The term integrated refers to a wired LAN that is physically connected to the DS and whose stations may be logically connected to an IEEE 802.11 LAN via the integration service. The integration service takes care of any address translation and media conversion logic required for the exchange of data.

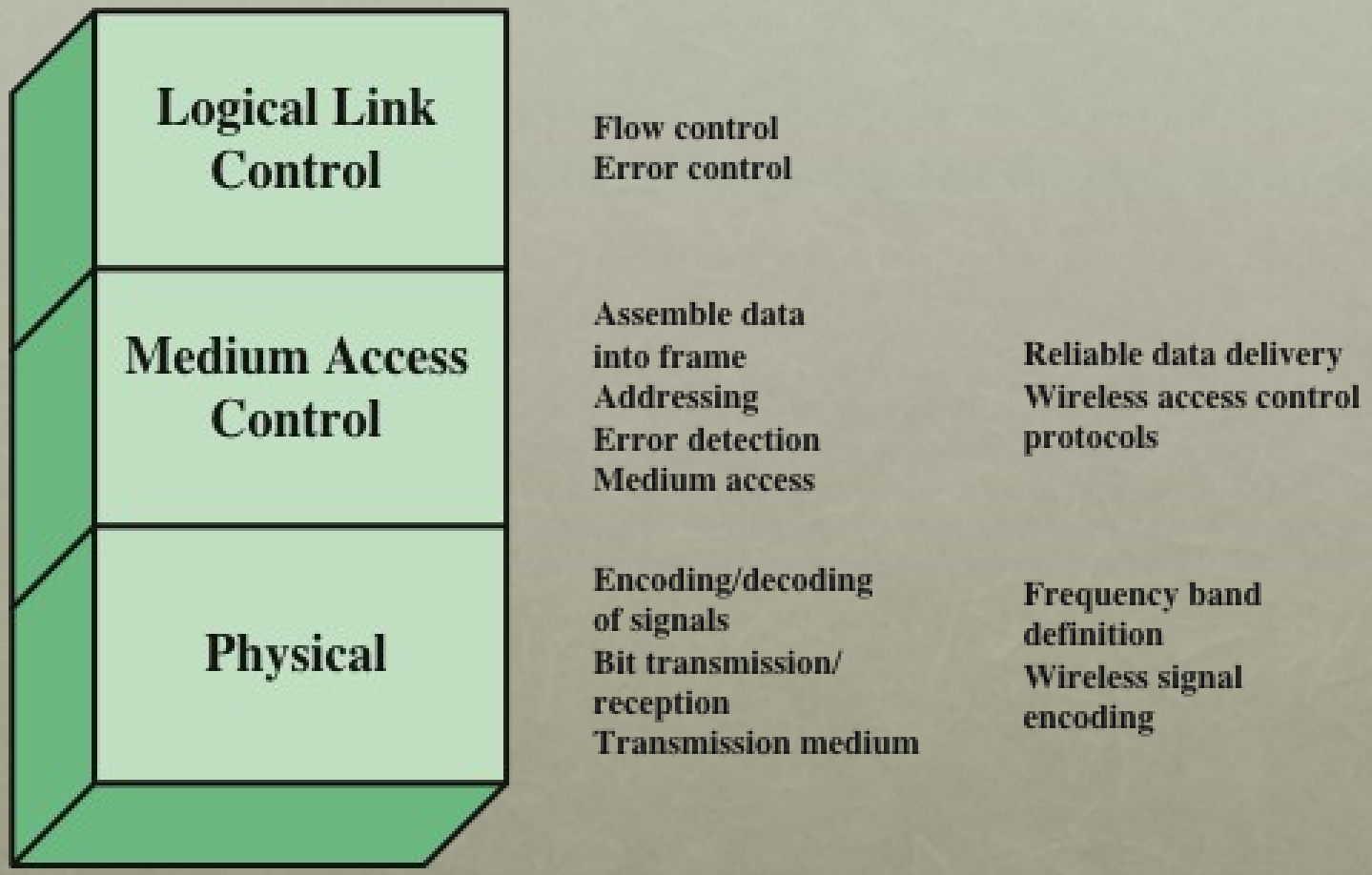


Figure 7.3 IEEE 802.11 Protocol Stack

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.