Wireless Network Security

Unit-4 --- Part-2

Presentation by

Dr Capt Ravindra Babu Kallam

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 far more portable and mobile than wired devices. This mobility results in a number of risks.

Resources: Some wireless devices, such as smart phones 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 locations. This greatly increases their vulnerability to physical attacks.

Figure 18.1 Wireless Networking Components

wireless environment consists of three components that provide point of attack :

The wireless client can be a cell phone, a Wi-Fi–enabled laptop or tablet, a wireless sensor, a Bluetooth device, and so on.

The wireless access point provides a connection to the network or service. Examples: Cell towers, Wi-Fi hotspots, and wireless access points to wired local or wide area networks.

The transmission medium, which carries the radio waves for data transfer, is also a source of vulnerability.

Wireless Network Threats

Accidental association: A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network. Although the security breach is accidental, it however exposes resources of LAN to the accidental user.

Malicious association: In this situation, a wireless device is configured to appear to be a genuine 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 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 attack involves 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): In the context of a wireless network, a DoS attack occurs when an attacker repeatedly bombards a wireless access point with various protocol messages designed to consume system resources.

Network injection: A network injection attack targets wireless access points that are exposed to *no filtered network traffic*, such as routing protocol messages or network management messages to degrade network performance.

Wireless Security Measurers

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 (service set identifier) 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

Securing Wireless Networks (Wireless routers and end points)

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. This capability can be disabled, so as to thwart attackers.

4. Change the identifier on your router from the default. 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 practical 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

- 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

•Growing use of new devices: Organizations are experiencing significant growth in employee use of mobile devices. In many cases, employees are allowed to use a combination of endpoint devices as part of their day-to-day activities.

•Cloud-based applications: Applications no longer run exclusively on physical servers in corporate data centers. Applications can run anywhere—on traditional physical servers, or in the cloud. Additionally, end users can now take advantage of a wide variety of cloud-based applications and IT services for personal and professional use. Employees depend upon Skype to speak for legitimate business video conferencing.

- De - parameterization: Given new device explosion, application mobility, and cloud-based consumer and corporate services, the notion of a static network perimeter is all but gone. Now there are a huge number of network perimeters around devices, applications, users, and data.

- External business requirements: The enterprise must also provide guests, third-party contractors, and business partners network access using various devices from a huge number of locations.

Security Threats

Major security concerns for mobile devices:

- **Lack of Physical Security Controls :** Mobile devices are typically under the complete control of the user. Even if a device is required to remain on premises, the user may move the device within the organization between secure and no secured 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.

- **Use of Untrusted Mobile Devices :** In addition to company-issued / controlled mobile devices, virtually all employees will have personal smart phones / 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, etc.

- **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, 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 should have several options for dealing with this threat.

- **Interaction with Other Systems :** A common feature found on smart phones 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.

Mobile Device Security Elements

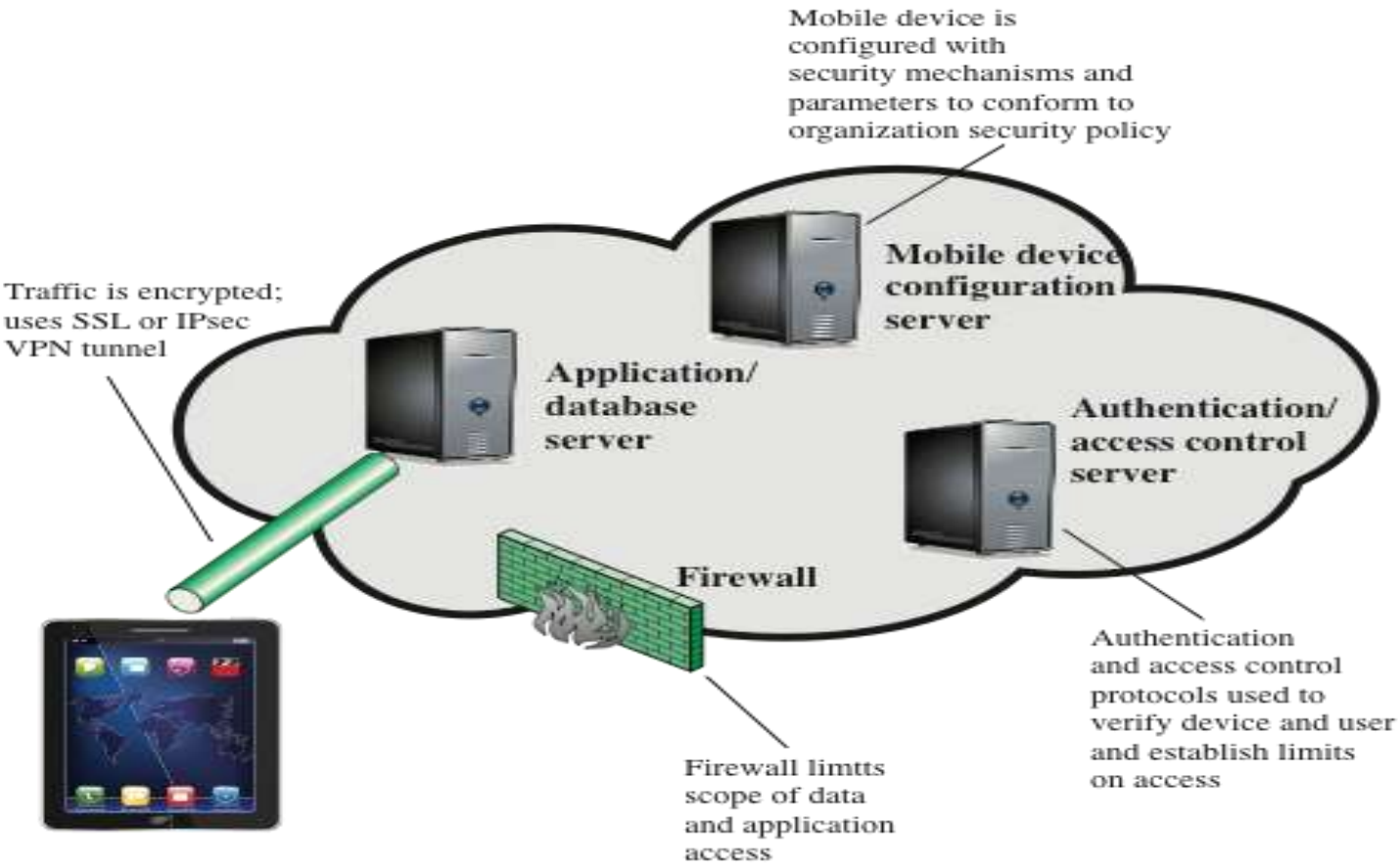


Figure 18.2 Mobile Device Security Elements

Mobile Device Security

Mobile device security fall into three categories: device security, client/server traffic security, and barrier security

Device Security : A number of organizations will supply mobile devices for employee use and preconfigured those devices to conform to the enterprise security policy.

- However, many organizations will find it convenient or even necessary to adopt a bring-your-own-device (BYOD) policy that allows the personal mobile devices of employees to have access to corporate resources.
- IT managers should be able to inspect each device before allowing network access.

The organization should configure the device with security controls, including the following:

- Enable auto-lock, which causes the device to lock if it has not been used for a given amount of time, requiring the user to re-enter a four-digit PIN or a password to re-activate the device.

- Enable password or PIN protection. The PIN or password is needed to unlock the device. In addition, it can be configured so that e-mail and other data on the device are encrypted using the PIN or password and can only be retrieved with the PIN or password.

- Avoid using auto-complete features that remember user names or passwords.
- Enable remote wipe It is a security future that allows a network admin or **device owner to send a command to computing device to delete data from remote location**.

- Ensure that SSL protection is enabled, if available.
- Make sure that software, including operating systems and applications, is up to date.
- Install antivirus software as it becomes available.
- Either sensitive data should be prohibited from storage on the mobile device or it should be encrypted.

- IT staff should also have the ability to remotely access devices, wipe the device of all data, and then disable the device in the event of loss or theft.

- The organization may prohibit all installation of third-party applications.

- The organization can implement and enforce restrictions on what devices can synchronize and on the use of cloud-based storage.

- Disable camera use on corporate mobile devices.

- To counter the threat of malicious use of location services, the security policy can dictate that such service is disabled on all mobile devices.

Traffic Security : Traffic security is based on the usual mechanisms for encryption and authentication. All traffic should be encrypted and travel by secure means, such as SSL or IPv6.

Virtual private networks (VPNs) can be configured so that all traffic between the mobile device and the organization's network is via a VPN.

A strong authentication protocol should be used to limit the access from the device to the resources of the organization. A preferable strategy is to have a two-layer authentication mechanism, which involves authenticating the device and then authenticating the user of the device.

Barrier Security : The organization should have security mechanisms to protect the network from unauthorized access. The security strategy can also include **firewall policies** specific to mobile device traffic. Intrusion detection and intrusion prevention systems can be configured to have tighter rules for mobile device traffic.

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 license 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

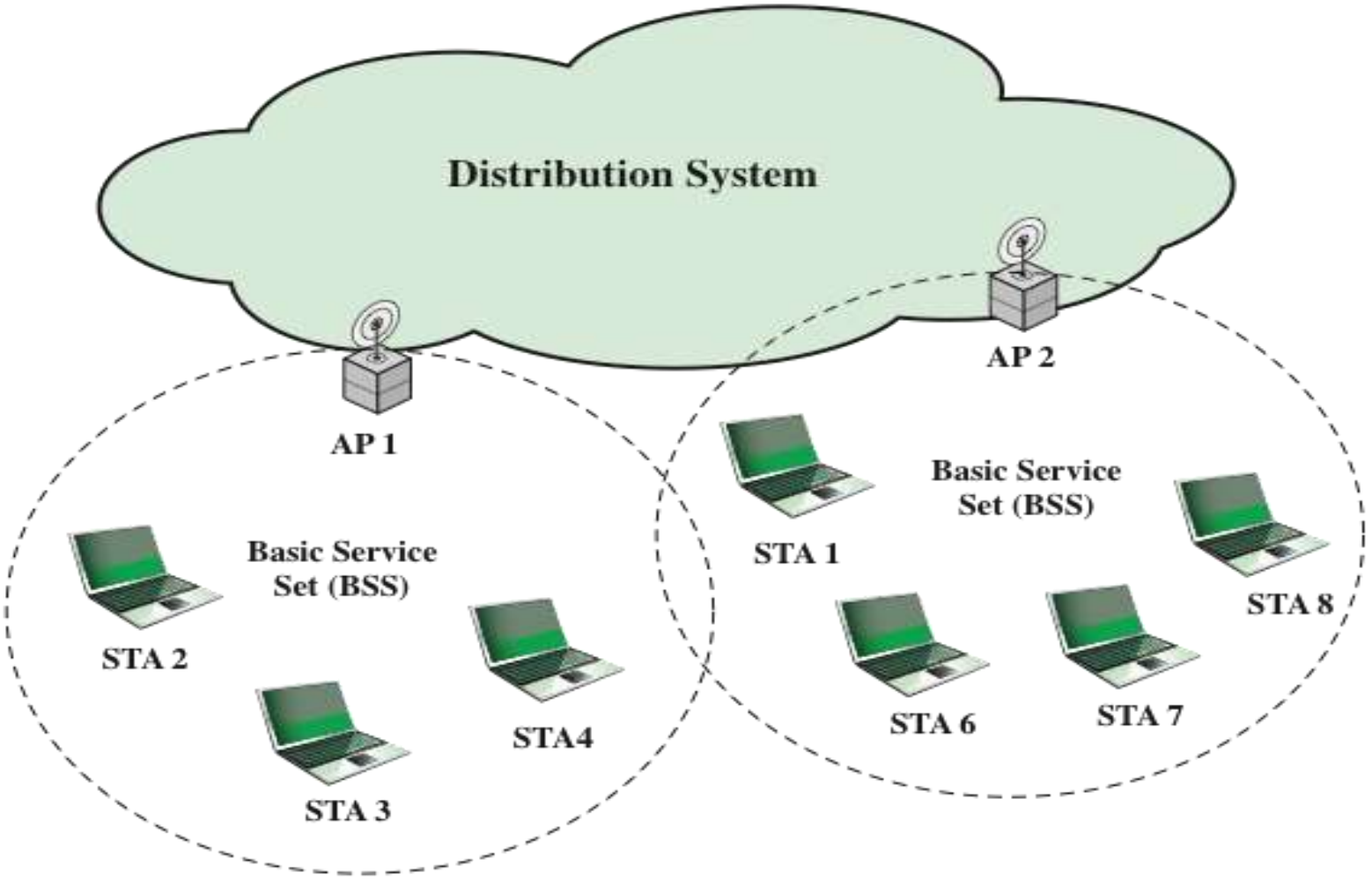


Figure 18.5 IEEE 802.11 Extended Service Set

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.

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)

IEEE 802.11 Protocol Stack

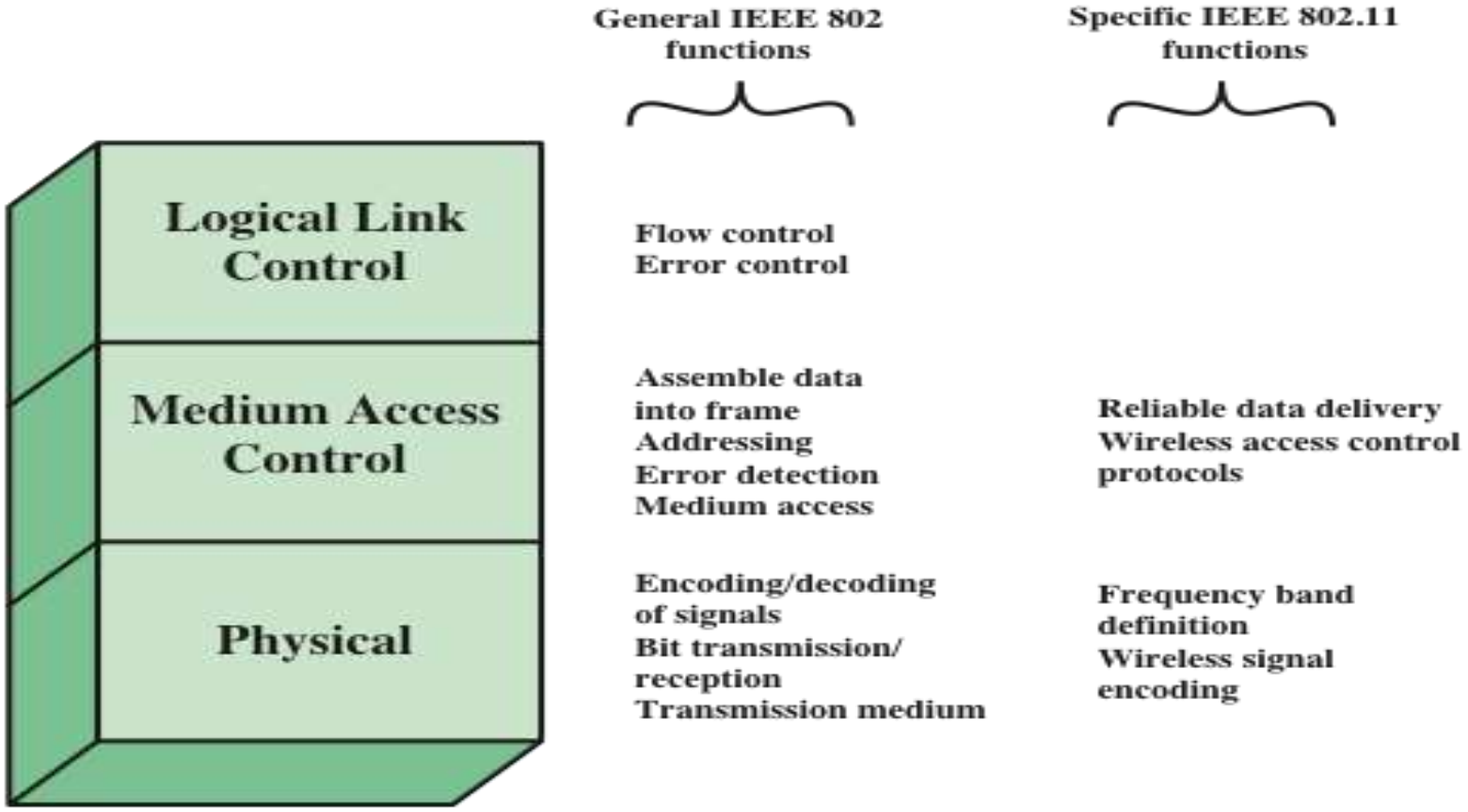


Figure 18.3 IEEE 802.11 Protocol Stack

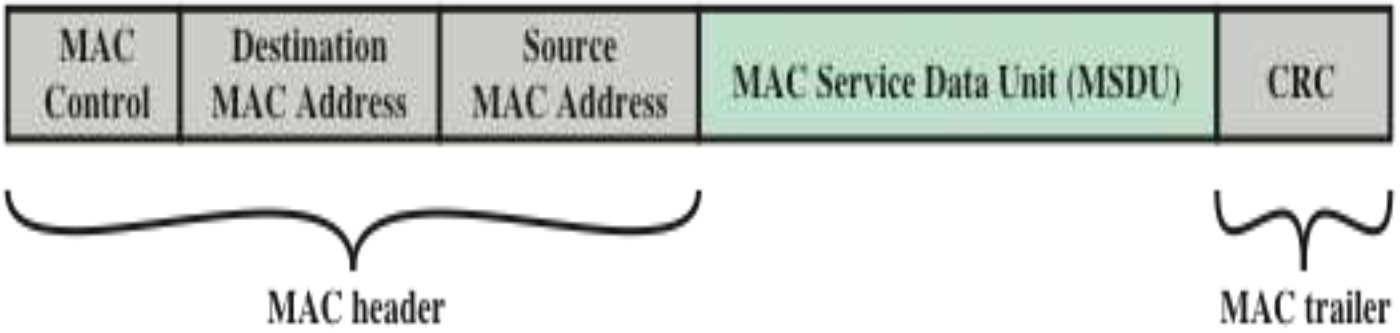


Figure 18.4 General IEEE 802 MPDU Format

- The exact format of the MPDU differs somewhat for the various MAC protocols in use. In general, all of the MPDUs have a format similar to that of Figure 18.4.
- The fields of this frame are as follows.

- 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 fields preceding the MSDU field are referred to as the MAC header, and the field following the MSDU field is referred to as the MAC trailer. The header and trailer contain control information that accompany the data field and that are used by the MAC protocol.

IEEE 802.11 Services

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

Distribution of Messages Within a DS

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 through the DS to get from a station in one BSS to a station in another 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.

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) .**

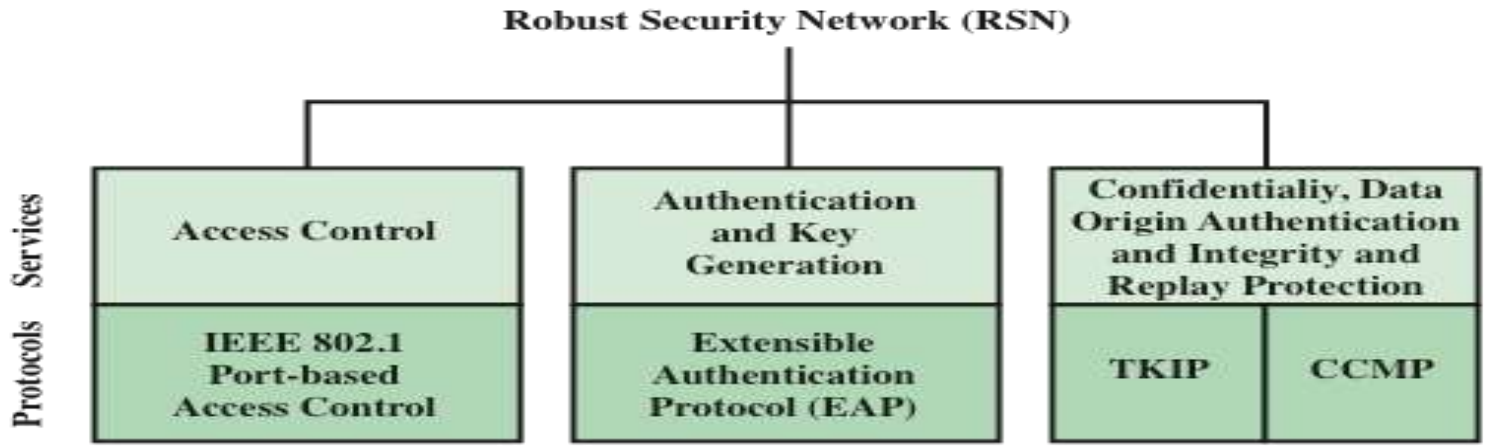
The 802.11i RSN security specification defines the following services.

- Authentication: A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.

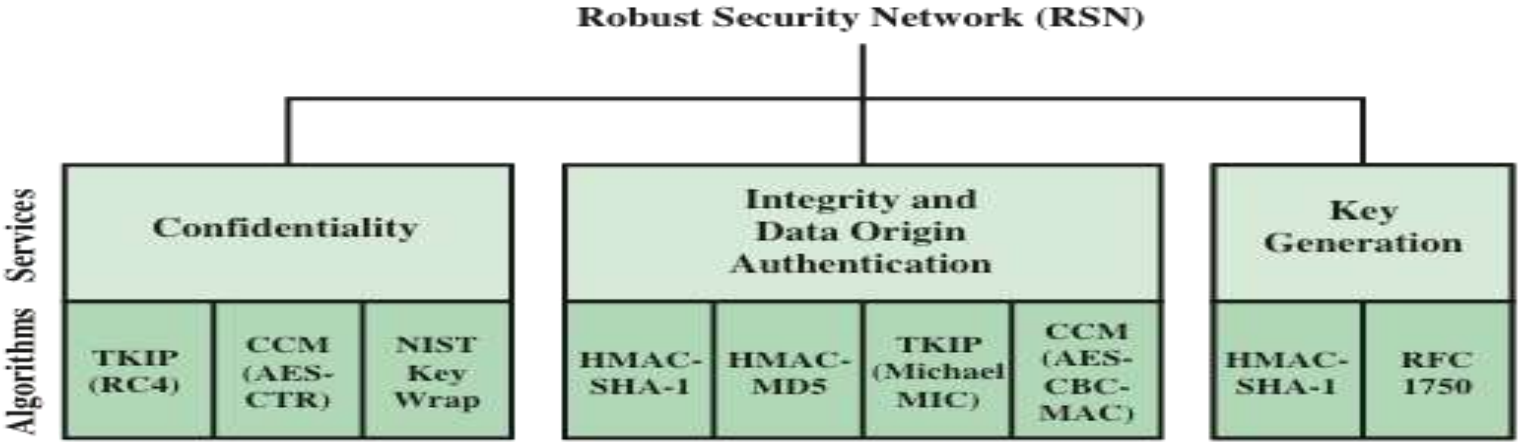
- Access control: This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange.

- Privacy with message integrity: MAC-level data are encrypted along with a message integrity code that ensures that the data have not been altered.

- Figure 18.6a indicates the security protocols used to support these services, while Figure 18.6b lists the cryptographic algorithms used for these services.



(a) Services and Protocols



(b) Cryptographic Algorithms

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 18.6 Elements of IEEE 802.11i

IEEE 802.11i Phases of Operation

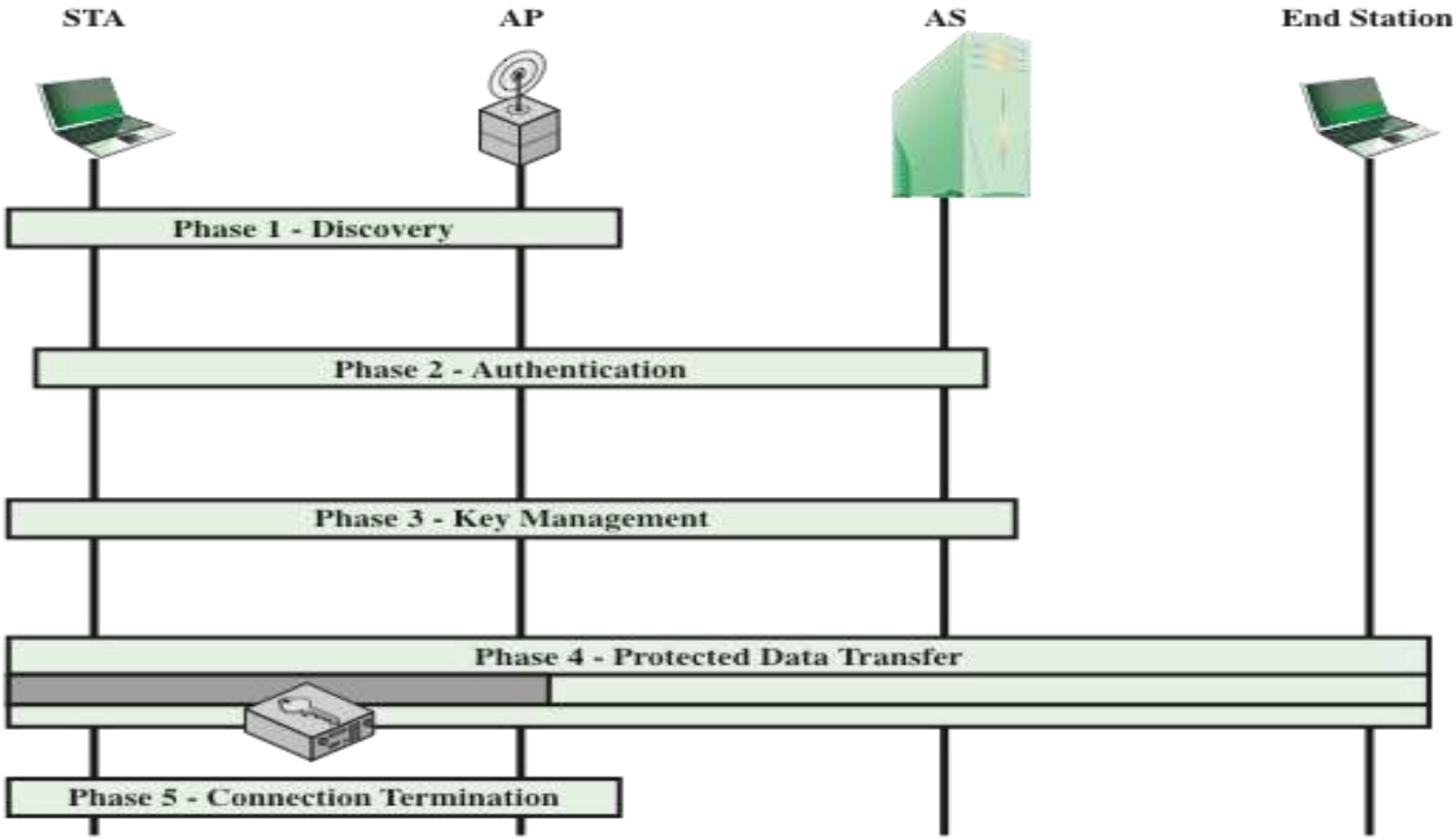


Figure 18.7 IEEE 802.11i Phases of Operation

The five phases are defined as follows.

Discovery: An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.

Authentication: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.

Key generation and distribution: The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only.

Protected data transfer: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.

Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.