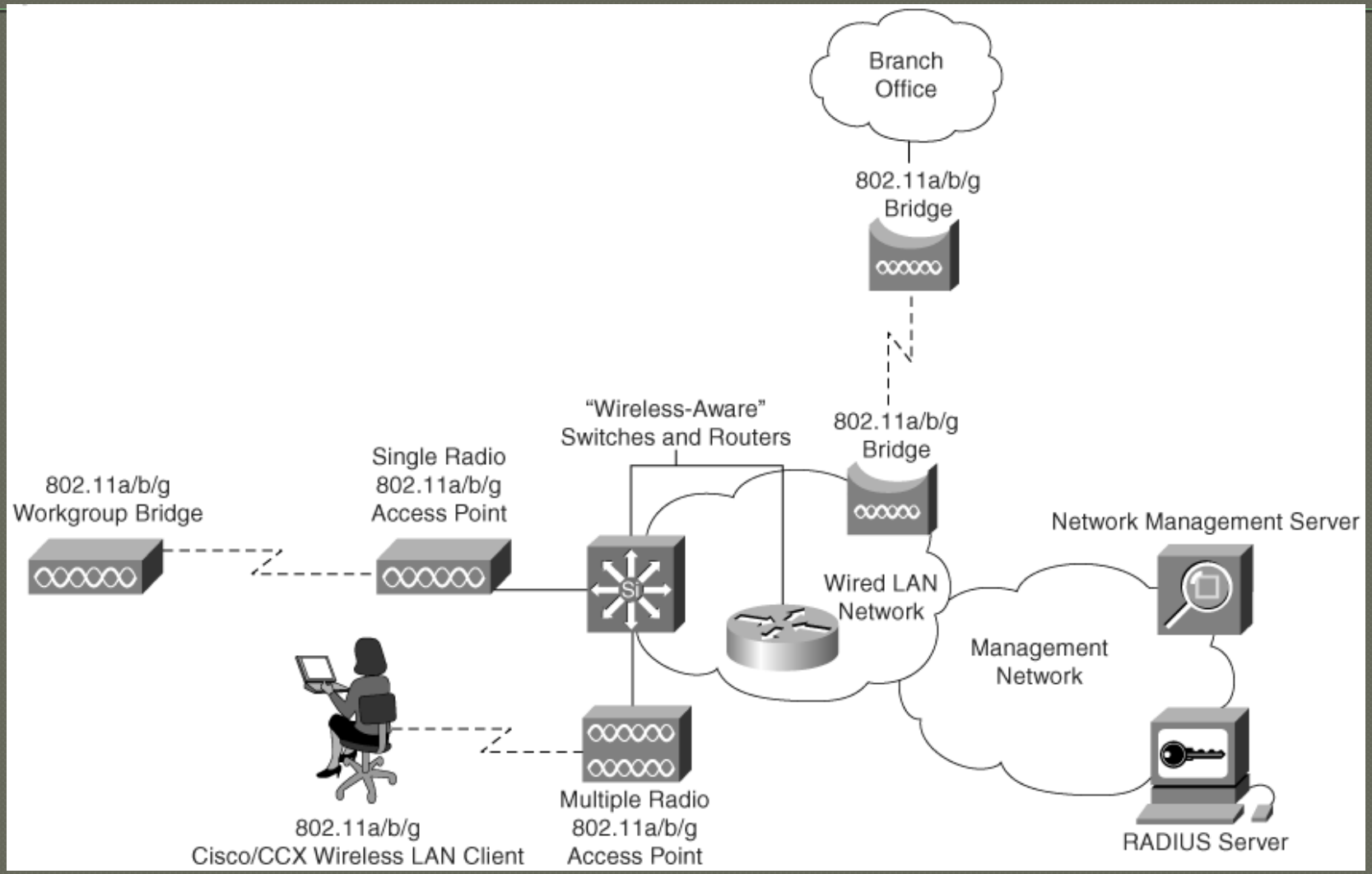
WIRELESS LAN SECURITY

01 – WIRELESS LAN OVERVIEW

01 – Wireless LAN Overview

- WLAN Components
- WLAN Standards
- WLAN Fundamentals
- WLAN Security Domain Conceptual Model

Wireless LAN Components



Components of WLAN System

- Access Point (AP)
- NIC or Client Adapter
- Wireless Bridge
- AAA Server
- Network Management Server (NMS)
- Wireless-aware Switches and Routers

Access Point

- informs the wireless clients of its availability
- authenticates and associates wireless clients to the wireless network
- coordinates the wireless clients' use of wired resources

NIC or Client Adapter

- A PC or workstation uses a wireless NIC to connect to the wireless network.
- The NIC scans the available frequency spectrum for connectivity and associates it to an AP or another wireless client.

Wireless Bridge

- used to connect multiple LANs, both wired and wireless.
- used in building-to-building wireless connections
- can cover longer distances than APs

AAA Server

- needed to secure a WLAN network
- used for both user and administrator authentication in a WLAN network
- to pass policy such as virtual LAN (VLAN) and SSID for clients
- to grant different levels of authorization rights to administrative users
- to generate dynamic encryption keys for WLAN users

Network Management Server

- to ease the complexity of deployment and management of large WLAN networks
- support firmware/software management, configuration management, performance trending and reporting, and client association reporting capabilities in a WLAN network

Note

- The client adapter is also called "STA" (station) or "supplicant" or "peer”
- The access point is also known as an "authenticator" or "network access server”
- The AAA server is also known as an "authentication server," "RADIUS server," or even "access control server (ACS)."

01 – Wireless LAN Overview

- WLAN Components
- WLAN Standards
- WLAN Fundamentals
- WLAN Security Domain Conceptual Model

WLAN Standards

- The fundamental standard is the IEEE 802.11, which specifies the WLAN protocols, data frames, various layers, and frequencies
- The IETF standards are in the security protocols and methods domain
- ETSI specifies the frequencies and other radio regulatory matters

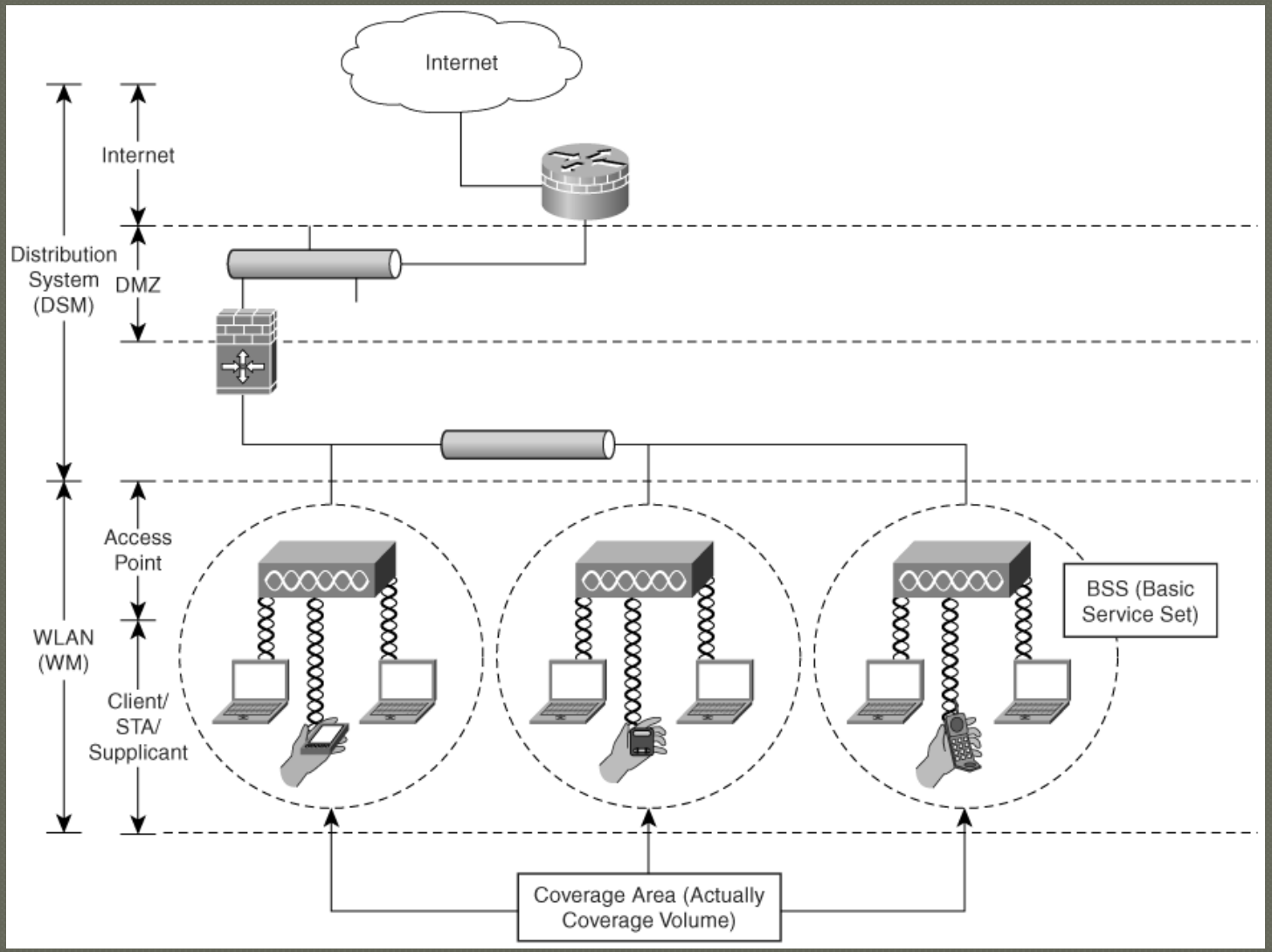
01 – Wireless LAN Overview

- WLAN Components
- WLAN Standards
- WLAN Fundamentals
- WLAN Security Domain Conceptual Model

WLAN Fundamentals

- WLAN Elements and Characteristics
- WLAN Basic Topology
- WLAN Building Blocks
- WLAN State Diagram
- WLAN Choreography

WLAN Elements and Characteristics



The Wireless Client

- known as the STA (station) or supplicant, is usually a card or embedded chip in a device.
- include PCs, PDAs, tablets, or smart phones.
- communicate over a radio link.

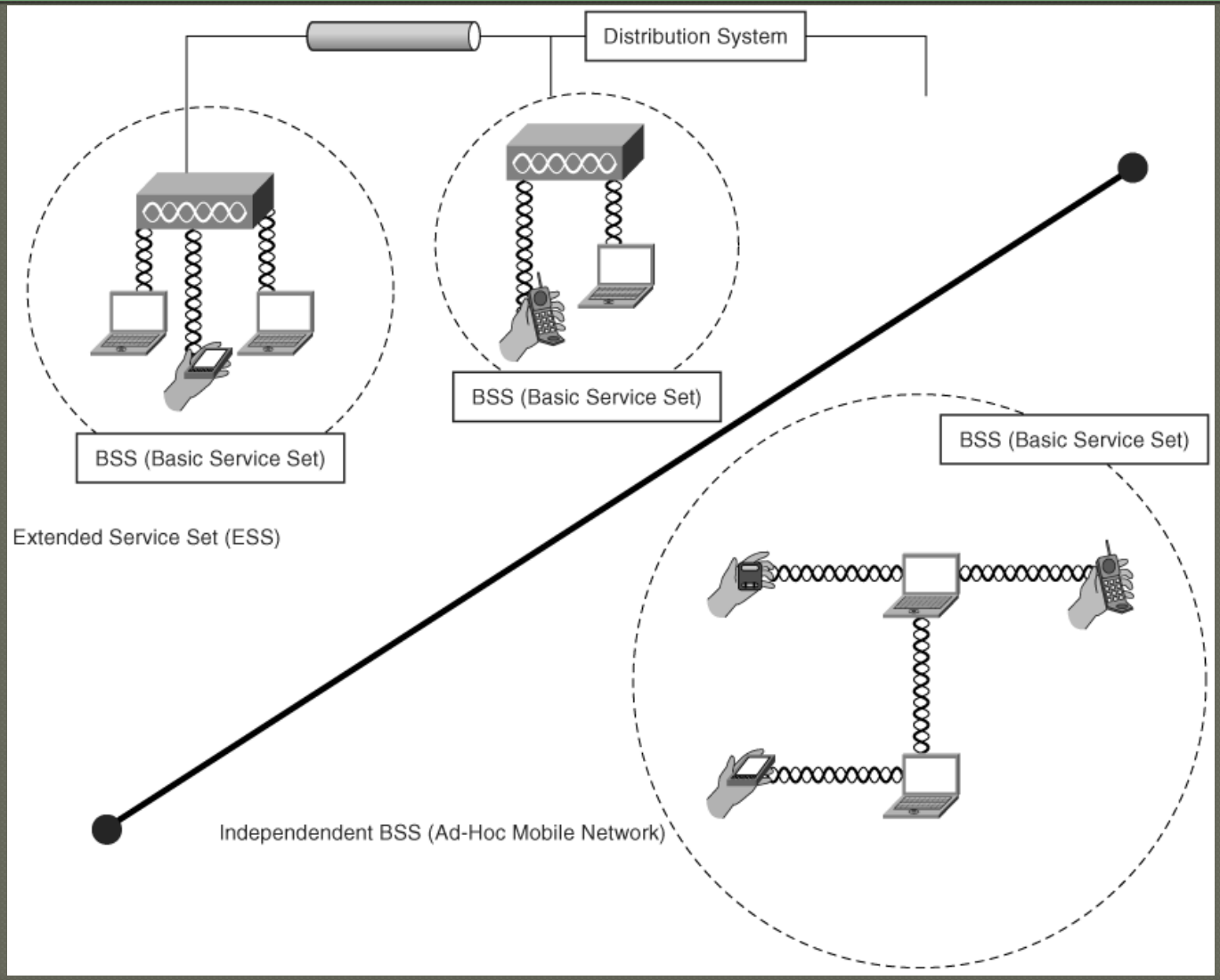
The Access Point

- the receiving (or sending) end of the radio link
- has the capability to reach back to the LAN
- has a range called the coverage area, which could overlap or be disjointed between the APs
- The coverage area is also essentially a Basic Service Set (BSS)

The Distribution Service

- the wired network that provides connectivity from the WLAN to the rest of the world.
- could be a corporate LAN, access provider, wireless service provider (WSP), or even the Internet.

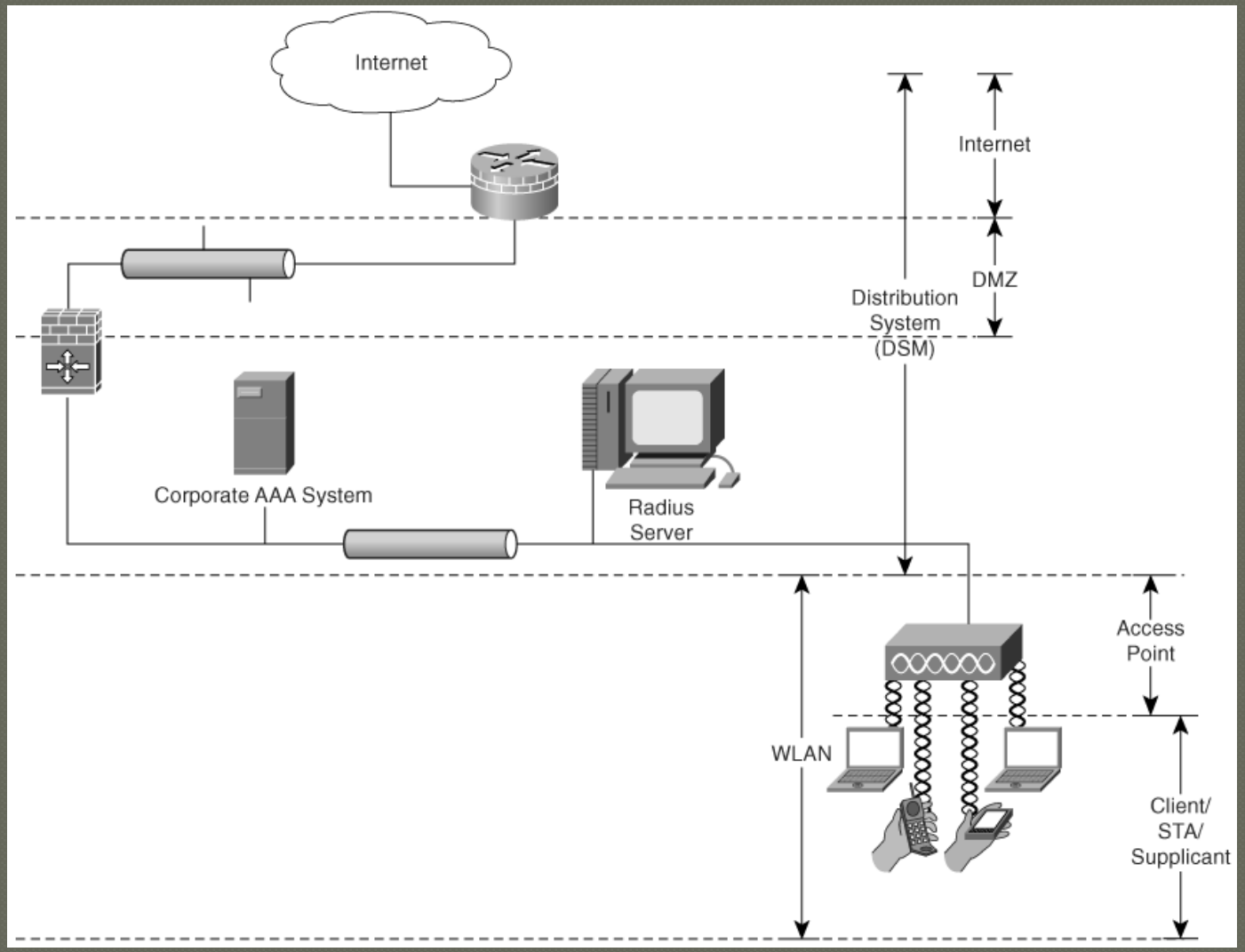
WLAN Operation Modes



WLAN Operation Modes

- There are two modes of WLAN operation: independent BSS (IBSS) and ESS.
- In the IBSS mode, the devices form ad-hoc connections with each other.
- The ESS consists of STAs connected to APs that, in turn, are connected to the DS. A client/STA can move from AP to AP connected to the same ESS and will not lose the connectivity context .

WLAN Basic Topology



WLAN Basic Topology

- 2 infrastructures:
  - a wireless environment/infrastructure consisting of STAs/clients that is connected to
  - a wired environment/infrastructure through APs.

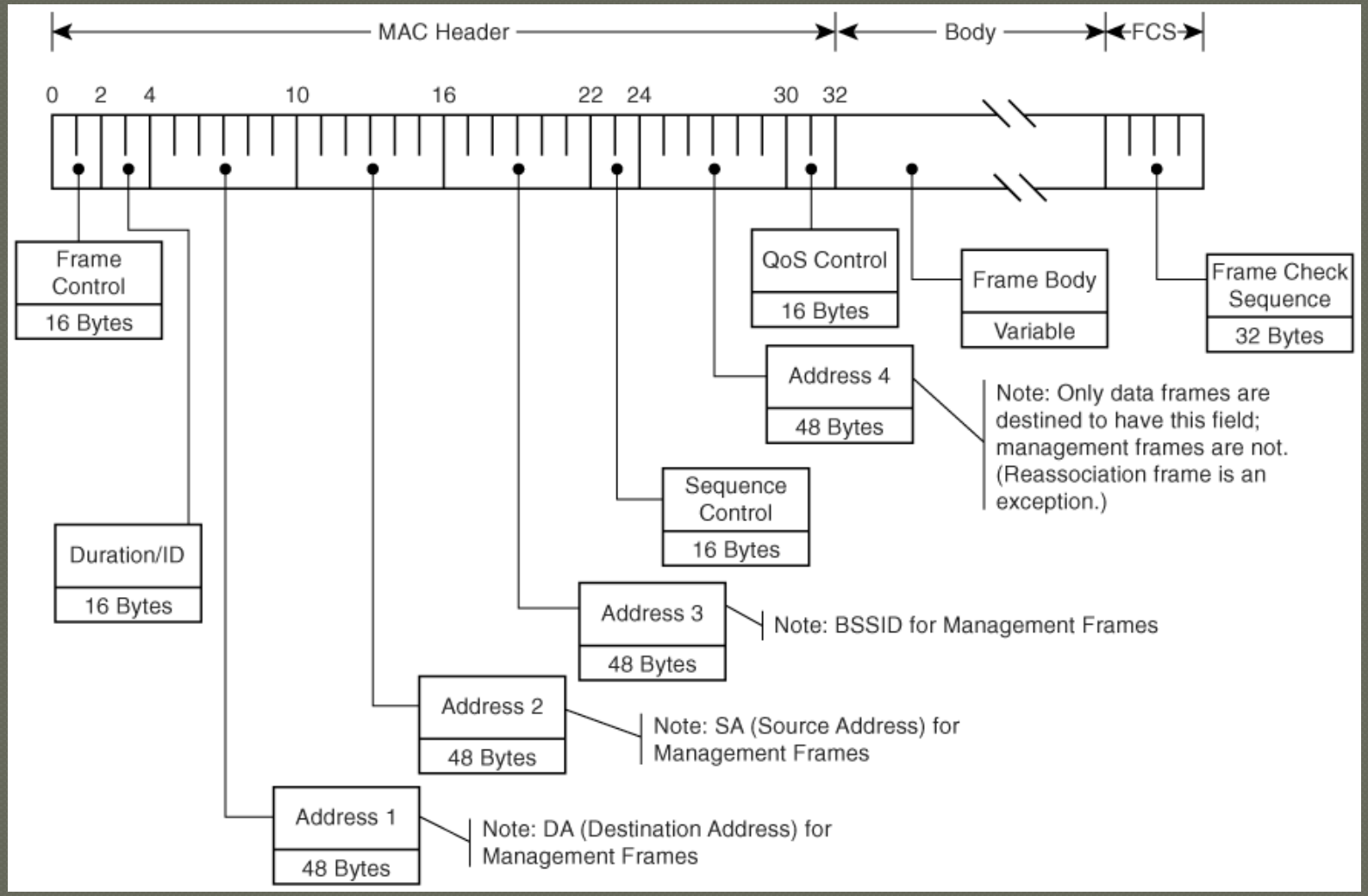
WLAN Building Blocks

- The 802.11 WLAN consists of a set of services.
- The services are achieved by messages between the entities, mainly the STA/client, the APs, and the distribution system.
- In turn, messages are composed of frames.

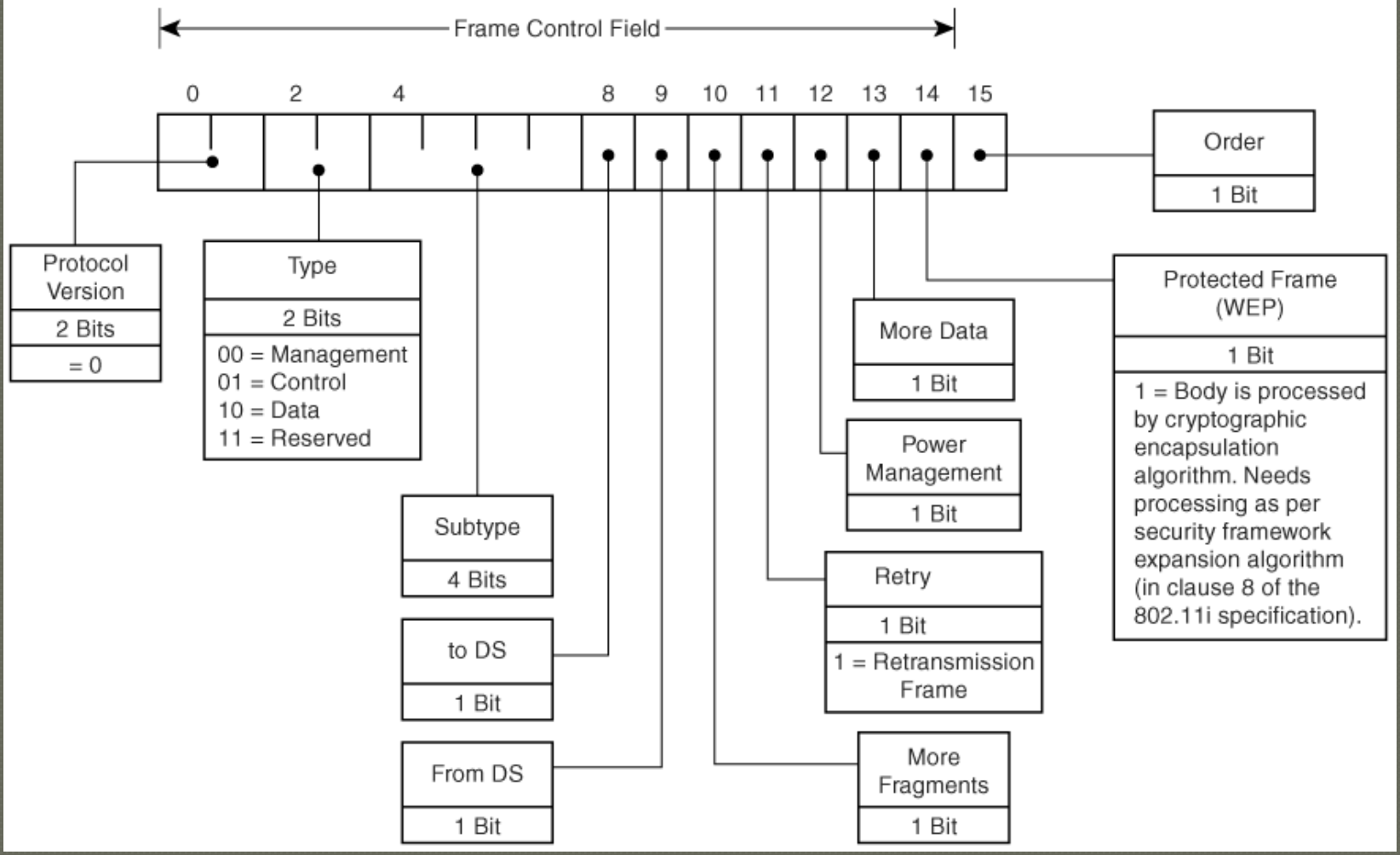
802.11 Services

Service	Type
Authentication	Request
Deauthentication	Notification
Association	Request
Disassociation	Notification
Reassociation	Request
Privacy (Confidentiality)	Request
Distribution	Request
Integration	Request
MSDU delivery	Request
Higher-layer timer synchronization	Request
QoS traffic scheduling	Request

802.11 MAC Frames



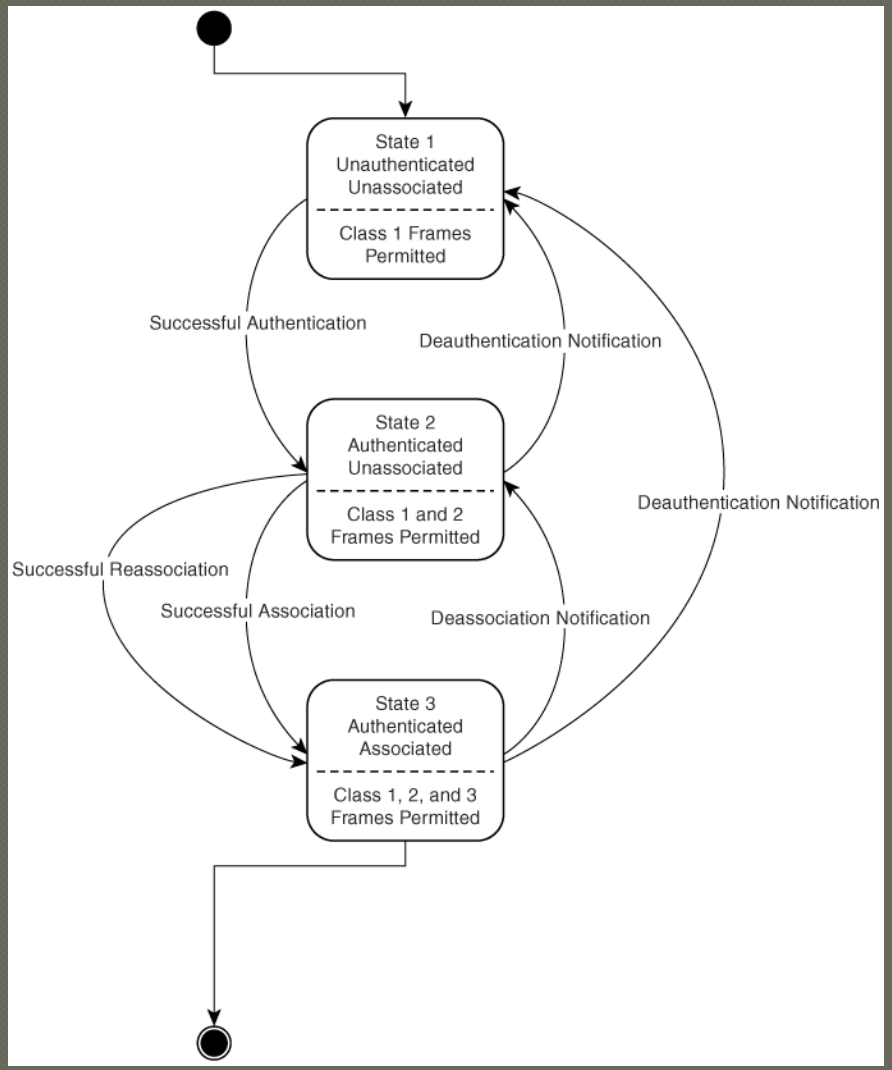
Frame Control Field Bits



Frame Control Field Bits

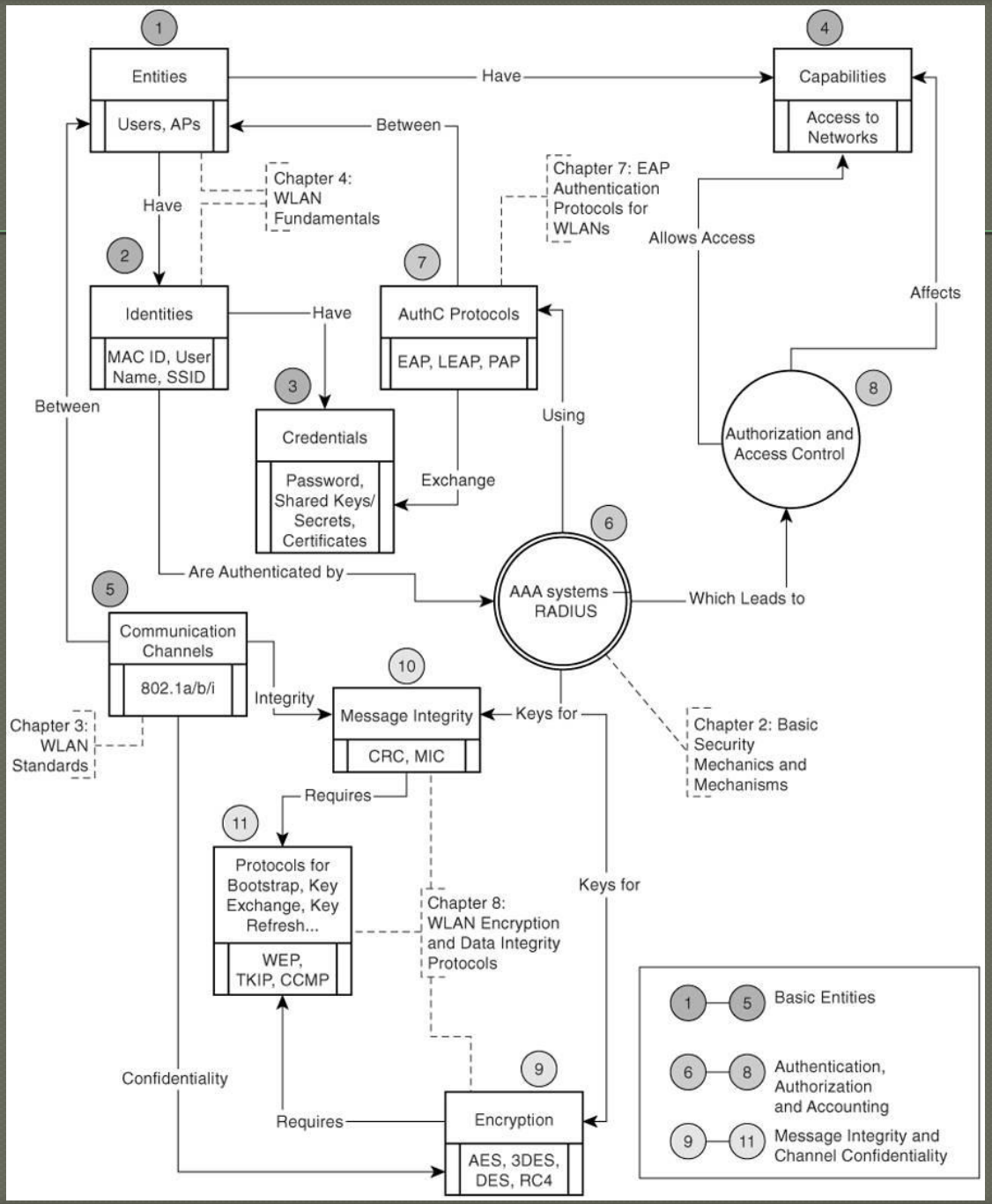
- The management frames include the request and response frames from the association/reassociation service, the authentication, beacon, and probe request/probe response.
- The control frames include Clear to Send (CTS), acknowledgement (ACK), and Request to Send (RTS) frames for controlling the transmission at the medium layer.
- The data frames include the actual data bits.

STA State Diagram



01 – Wireless LAN Overview

- WLAN Components
- WLAN Standards
- WLAN Fundamentals
- WLAN Security Domain Conceptual Model


1
Entities
Users, APs
Have
4
Capabilities
Access to Networks
Between
Have
Chapter 4: WLAN Fundamentals
Chapter 7: EAP Authentication Protocols for WLANs
Allows Access
Affects
2
Identities
MAC ID, User Name, SSID
Have
7
AuthC Protocols
EAP, LEAP, PAP
Between
3
Credentials
Password, Shared Keys/ Secrets, Certificates
Exchange
Using
8
Authorization and Access Control
6
AAA systems RADIUS
Are Authenticated by
Which Leads to
5
Communication Channels
802.1a/b/i
10
Message Integrity
CRC, MIC
Integrity
Keys for
Chapter 3: WLAN Standards
Chapter 2: Basic Security Mechanics and Mechanisms
Requires
11
Protocols for Bootstrap, Key Exchange, Key Refresh...
WEP, TKIP, CCMP
Keys for
Chapter 8: WLAN Encryption and Data Integrity Protocols
Confidentiality
Requires
9
Encryption
AES, 3DES, DES, RC4
1 5 Basic Entities
6 8 Authentication, Authorization and Accounting
9 11 Message Integrity and Channel Confidentiality

WLAN Security Domain Conceptual Model

- defines the entities, functionalities, and relationships between components
- Entities include users, wireless cards, APs, corporate networks, and service provider network access.