Module contents

★ IEEE 802.11 Terminology
★ IEEE 802.11 MAC Frames
★ Basic processes in IEEE802.11 networks
★ Configuration parameters
Station (STA) Architecture:

- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system.
- Most often end-stations available in terminals (work-stations, laptops etc.)
- Implemented in Avaya Wireless IEEE 802.11 PC-Card
IEEE 802.11 Terminology

Station (STA) Architecture (cont’d):

★ Ethernet-like driver interface
  ★ supports virtually all protocol stacks

★ Frame translation according to IEEE Std 802.1H
  ★ IEEE 802.3 frames: translated to 802.11
  ★ Ethernet Types 8137 (Novell IPX) and 80F3 (AARP) encapsulated via the Bridge Tunnel encapsulation scheme
  ★ All other Ethernet Types: encapsulated via the RFC 1042 (Standard for the Transmission of IP Datagrams over IEEE 802 Networks) encapsulation scheme
  ★ Maximum Data limited to 1500 octets

★ Transparent bridging to Ethernet
IEEE 802.11 Terminology

Access-Point (AP) Architecture:

- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provide access to a distribution system for associated stations
- Most often infra-structure products that connect to wired backbones
- Implemented in Avaya Wireless IEEE 802.11 PC-Card when it is inserted in an AP-500 or AP-1000
IEEE 802.11 Terminology

Access-Point (AP) Architecture (cont’d):

★ Stations select an Access-Point and “associate with it

★ Access-Points:
  ★ Support roaming
  ★ Provide time synchronization functions (beaconing)
  ★ Provide Power Management support

★ Traffic typically flows through Access-Point
  ★ in IBSS direct Station-to-Station communication takes place
IEEE 802.11 Terminology

Basic Service Set (BSS):

★ A set of stations controlled by a single “Coordination Function”
   (=the logical function that determines when a station can transmit
   or receive)

★ Similar to a “cell” in pre IEEE terminology

★ A BSS can have an Access-Point (both in standalone networks
   and in building-wide configurations), or can run without and
   Access-Point (in standalone networks only)

★ Diameter of the cell is app. twice the coverage-distance between
   two wireless stations
Basic Service Set (BSS)
**IEEE 802.11 Terminology**

**Independent Basic Service Set (IBSS):**

- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
- A BSS without an Access-Point
- One of the stations in the IBSS can be configured to “initiate” the network and assume the Coordination Function
- Diameter of the cell determined by coverage distance between two wireless stations
Independent Basic Service Set (IBSS)
IEEE 802.11 Terminology

Extended Service Set (ESS):
★ A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
★ Traffic always flows via Access-Point
★ Diameter of the cell is double the coverage distance between two wireless stations

Distribution System (DS):
★ A system to interconnect a set of Basic Service Sets
  ★ Integrated; A single Access-Point in a standalone network
  ★ Wired; Using cable to interconnect the Access-Points
  ★ Wireless; Using wireless to interconnect the Access-Points
Extended Service Set (ESS)

single BSS (with integrated DS)
Extended Service Set (ESS)

BSS’s with wired Distribution System (DS)
Extended Service Set (ESS)
BSS’s and wireless Distribution System (DS)
**IEEE 802.11 Terminology**

Service Set Identifier (SSID):

- “Network name”
- 32 octets long
- Similar to “Domain-ID” in the pre-IEEE WaveLAN systems
- One network (ESS or IBSS) has one SSID
IEEE 802.11 Terminology

Basic Service Set Identifier (BSSID)

★ “cell identifier”

★ 6 octets long (MAC address format)

★ Similar to NWID in pre-IEEE WaveLAN systems

★ One BSS has one SSID

★ Value of BSSID is the same as the MAC address of the radio in the Access-Point
Module contents

- IEEE 802.11 Terminology
- IEEE 802.11 MAC Frames
- Basic processes in IEEE 802.11 networks
- Configuration parameters
### Frame Formats

**MAC Header format differs per Type:**

- **Control Frames** (several fields are omitted)
- **Management Frames**
- **Data Frames**
### Address Field Description

<table>
<thead>
<tr>
<th>Bits: 2</th>
<th>2</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Version</td>
<td>Type</td>
<td>SubType</td>
<td>To DS</td>
<td>From DS</td>
<td>More Frag</td>
<td>Retry</td>
<td>Pwr Mgt</td>
<td>More Data</td>
<td>WEP</td>
<td>Rsvd</td>
<td></td>
</tr>
</tbody>
</table>

#### Frame Control Field

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

- **Addr. 1** = All stations filter on this address.
- **Addr. 2** = Transmitter Address (TA), Identifies transmitter to address the ACK frame to.
- **Addr. 3** = Dependent on *To* and *From DS* bits.
- **Addr. 4** = Only needed to identify the original source of WDS (*Wireless Distribution System*) frames.
Type field descriptions

Type and subtype identify the function of the frame:

- **Type=00 Management Frame**
  - Beacon
  - (Re)Association
  - Probe
  - (De)Authentication
  - Power Management

- **Type=01 Control Frame**
  - RTS/CTS
  - ACK

- **Type=10 Data Frame**
MAC Management Frames

★ Beacon
  ★ Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  ★ Traffic Indication Map

★ Probe
  ★ SSID, Capabilities, Supported Rates

★ Probe Response
  ★ Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  ★ same for Beacon except for TIM
MAC Management Frames (cont’d)

★ Association Request
  ★ Capability, Listen Interval, SSID, Supported Rates

★ Association Response
  ★ Capability, Status Code, Station ID, Supported Rates

★ Re-association Request
  ★ Capability, Listen Interval, SSID, Supported Rates, Current AP Address

★ Re-association Response
  ★ Capability, Status Code, Station ID, Supported Rates
MAC Management Frames (cont’d)

- Dis-association
  - Reason code

- Authentication
  - Algorithm, Sequence, Status, Challenge Text

- De-authentication
  - Reason