Wireless Protocols

Training materials for wireless trainers

The Abdus Salam
International Centre
for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

Goals

The goal of this lecture is to introduce:

- IEEE wireless protocols coverage
- 802.11 radio protocols terminology
- WiFi modes of operation details

IEEE Wireless Protocols
Coverage Scope

802.15	802.11	802.16	802.22
W. PAN	W. LAN	W. MAN	W. RAN
meters	**hundred m**	**kilometers**	**hundred km**

Terminology

- Station: Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system. Also called **Client**.

- Access Point (AP) :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

Beacons

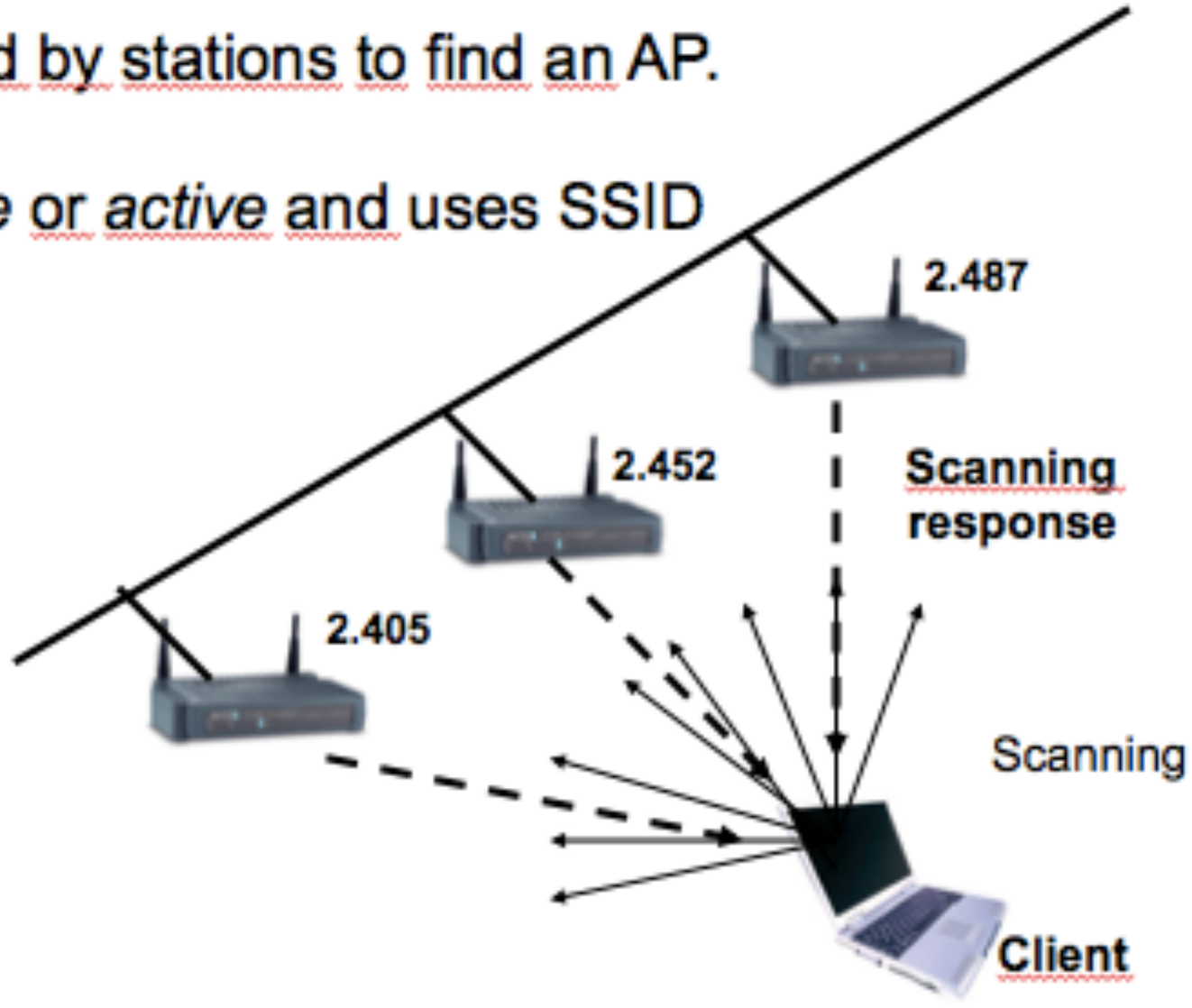
- Short frames sent from the access point to stations (infrastructure mode) or station-to-station (ad hoc mode) in order to organize and synchronize wireless communication on the wireless LAN.

Beacons functions

- Time Synchronization
- DSSS Parameter Sets Advertising
- SSID Information
- Supported Rates
- Traffic Indication Map

Scanning

- Scanning is used by stations to find an AP.
- It can be *passive* or *active* and uses SSID and *beacons*.



Passive Scanning

- Process of listening for beacons sent by and access point on each channel for a specific period of time after the station is initialized

Active Scanning

- Active scanning involves the sending of a probe request frame from a wireless station.

Stations send this probe frame when they are actively seeking a network to join. The probe frame will contain either the SSID of the network they wish to join or a broadcast SSID

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

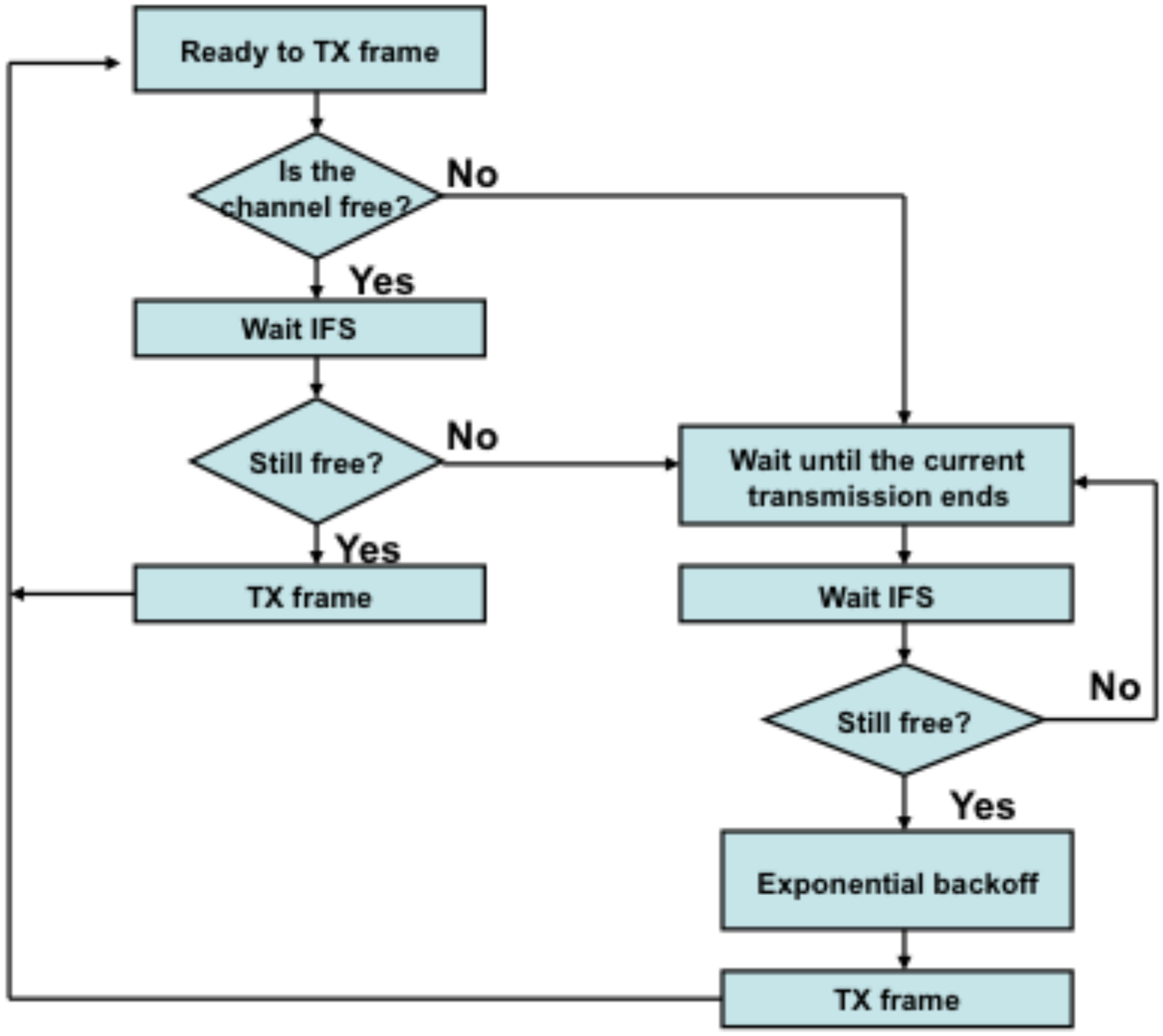
- Association Request
  Capability, Listen Interval, SSID, Supported Rates

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

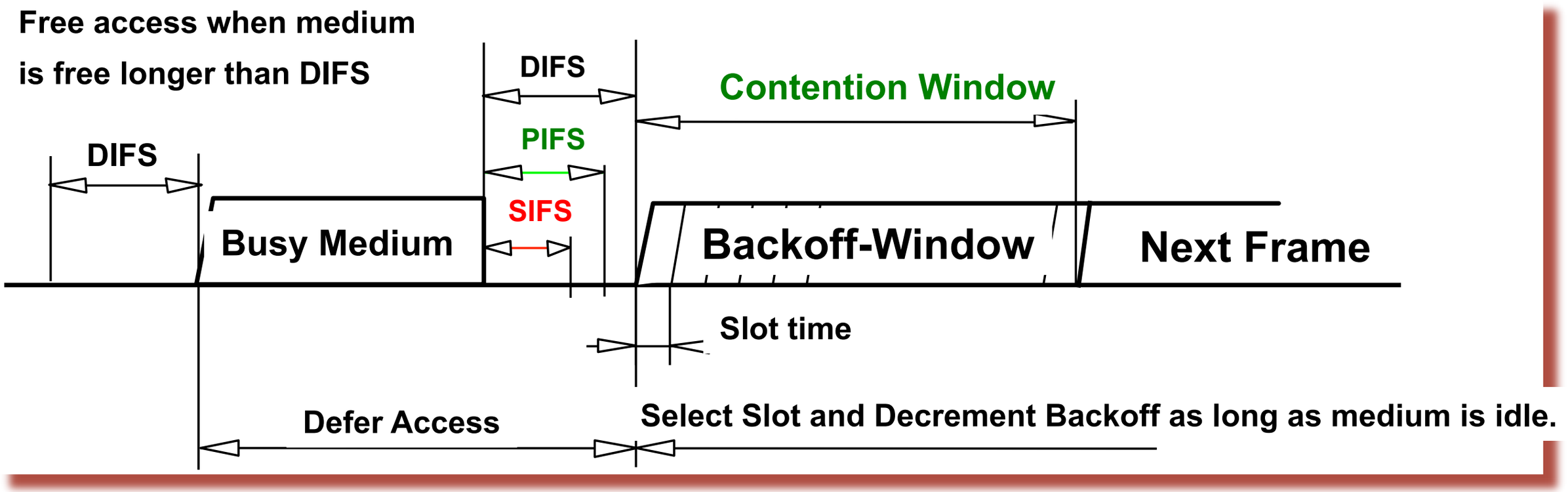
Re-association Request
  Capability, Listen Interval, SSID, Supported Rates, Current AP Address

Re-association Response
  Capability, Status Code, Station ID, Supported Rates

Medium Access Control

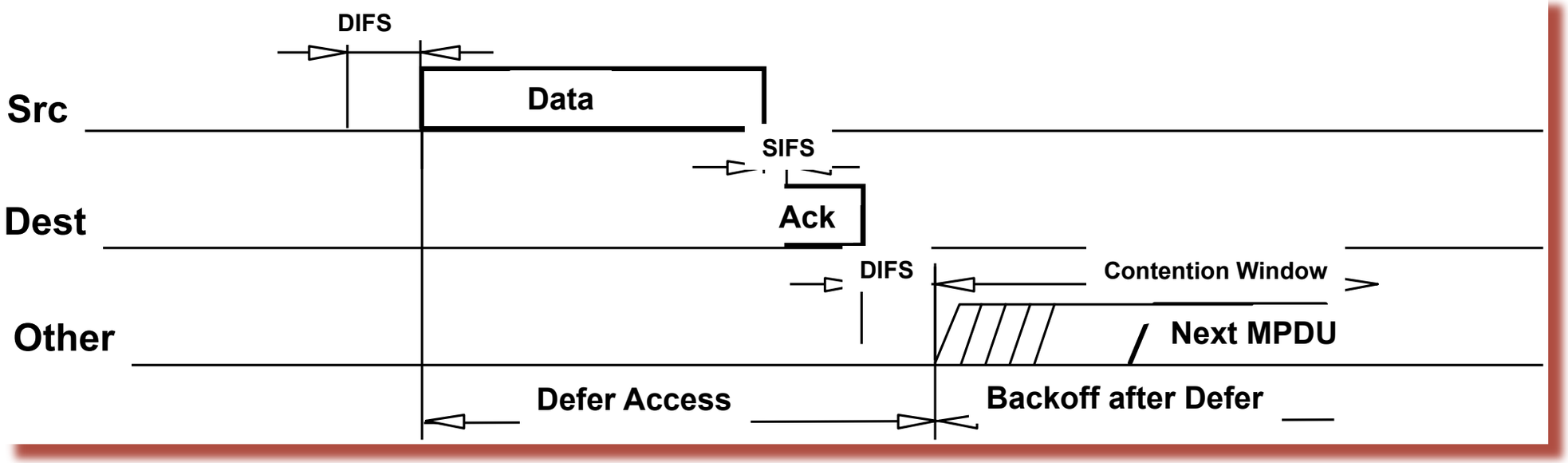


Inter-Frame Spacing



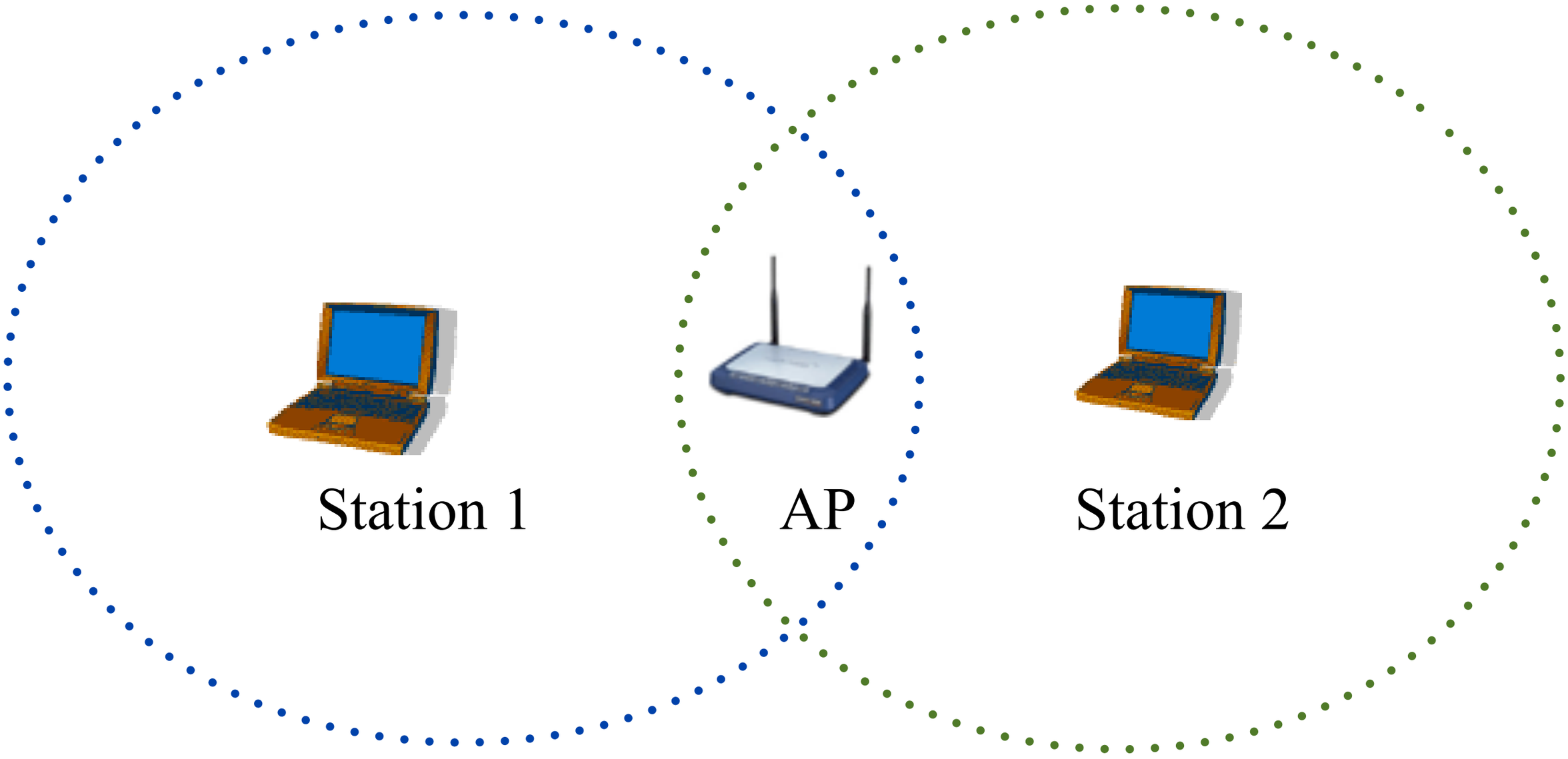
SIFS = Short interframe space
PIFS = PCF interframe space
DIFS = DCF interframe space
Back-off timer expressed in terms of number of time slots

Data frames and ACK



Acknowledgment must be received within the SIFS
The DCF inter-frame space is observed before medium is considered free for use

Hidden Node



RTS/CTS Handshaking

Sending Station

AP

Receiving Station

Request to Send (RTS)

Request to Send (RTS)

Clear to Send (CTS)

Clear to Send (CTS)

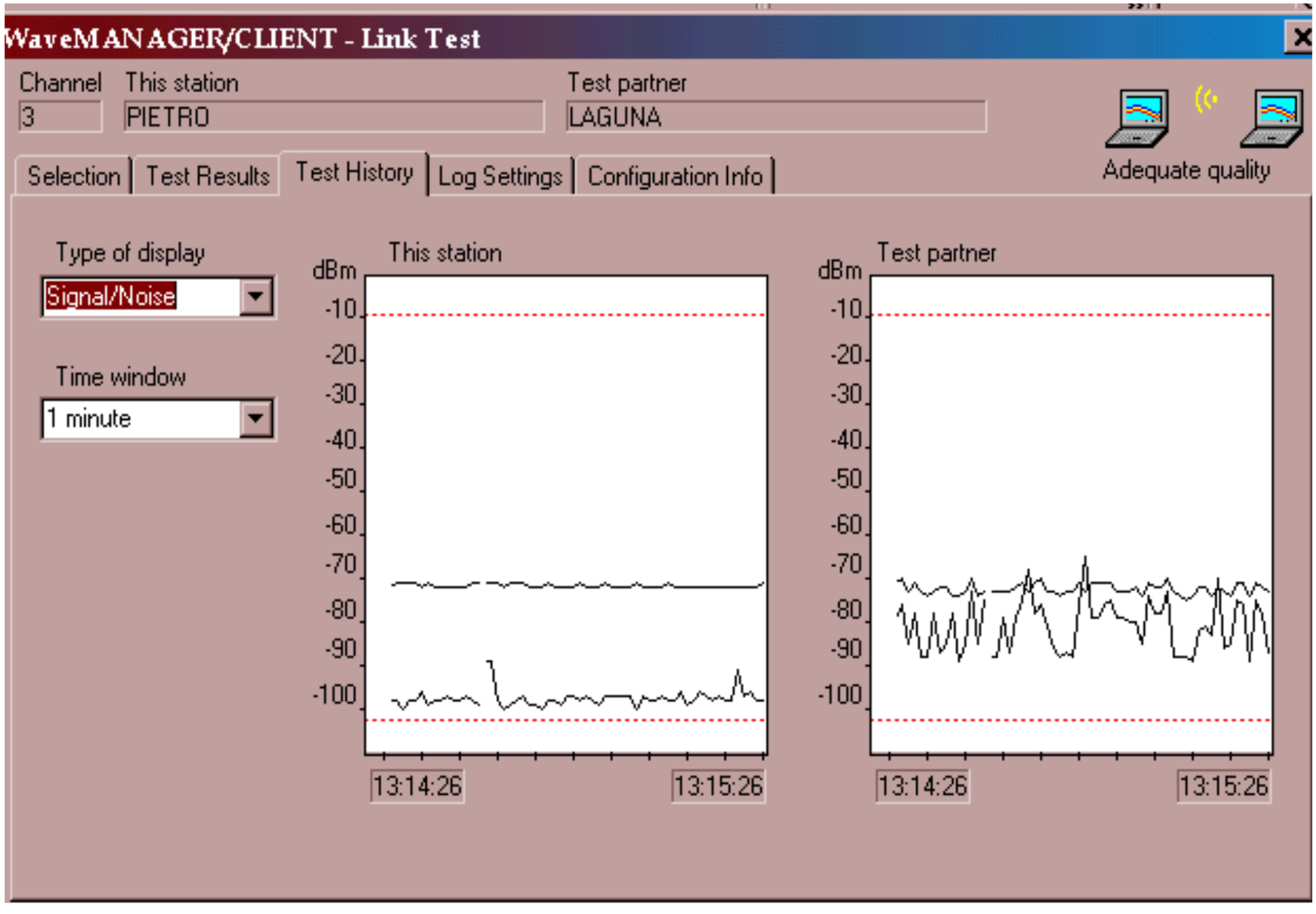
Data

Data

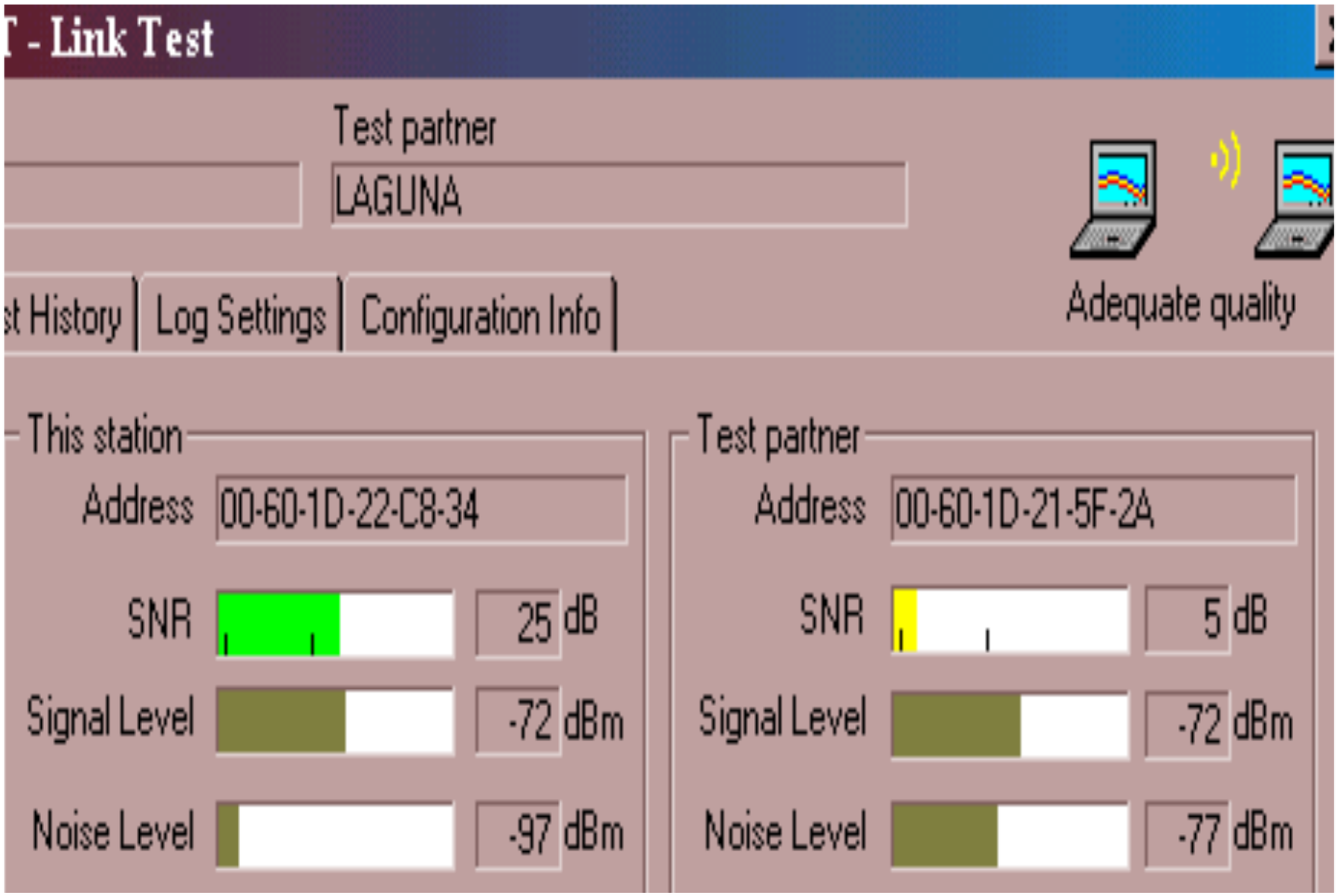
ACK

ACK

Interference



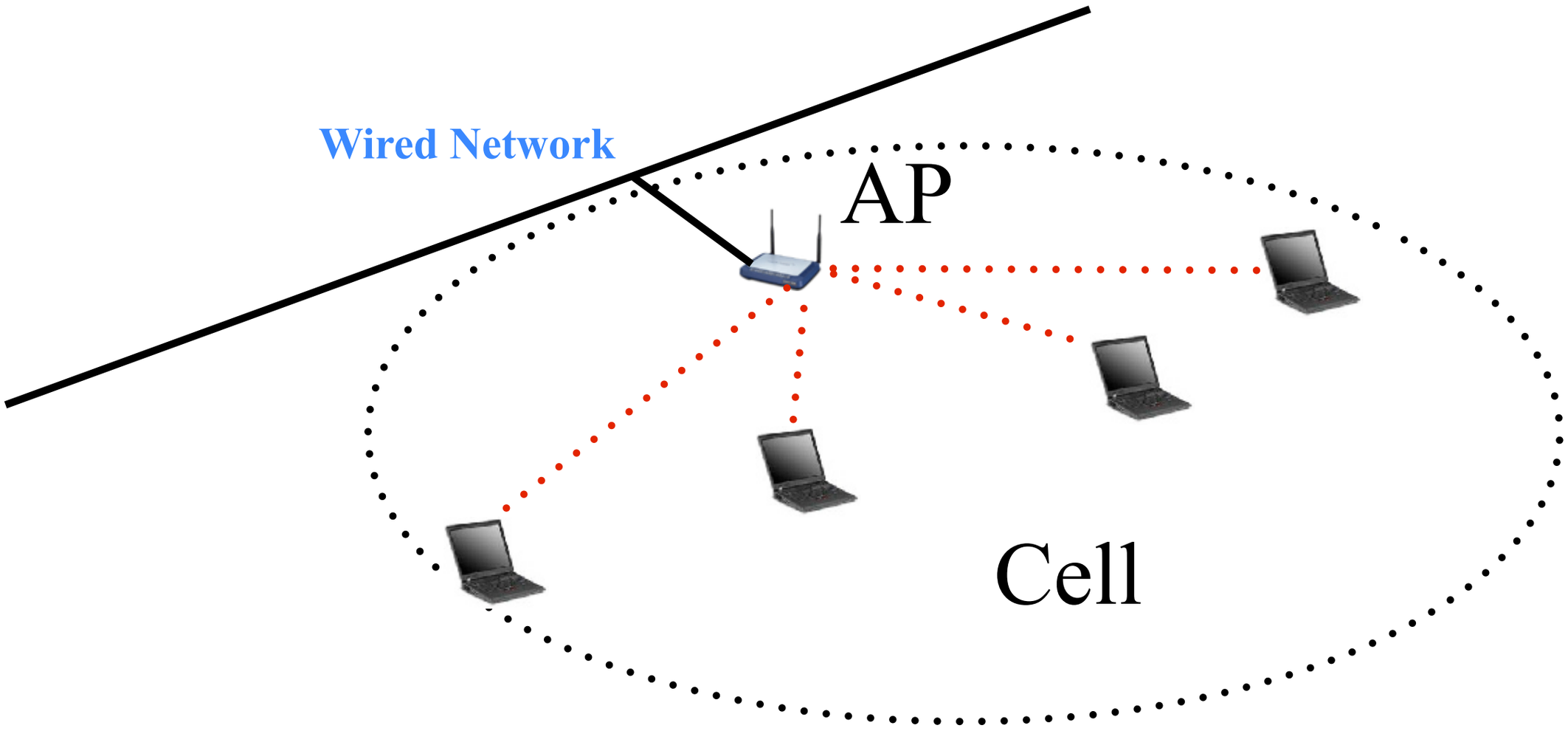
Interference



Service Sets

- Basic Service Set (BSS)
- Extended Service Set (ESS)
- Independent Basic Service set (IBSS)

Basic Service Set



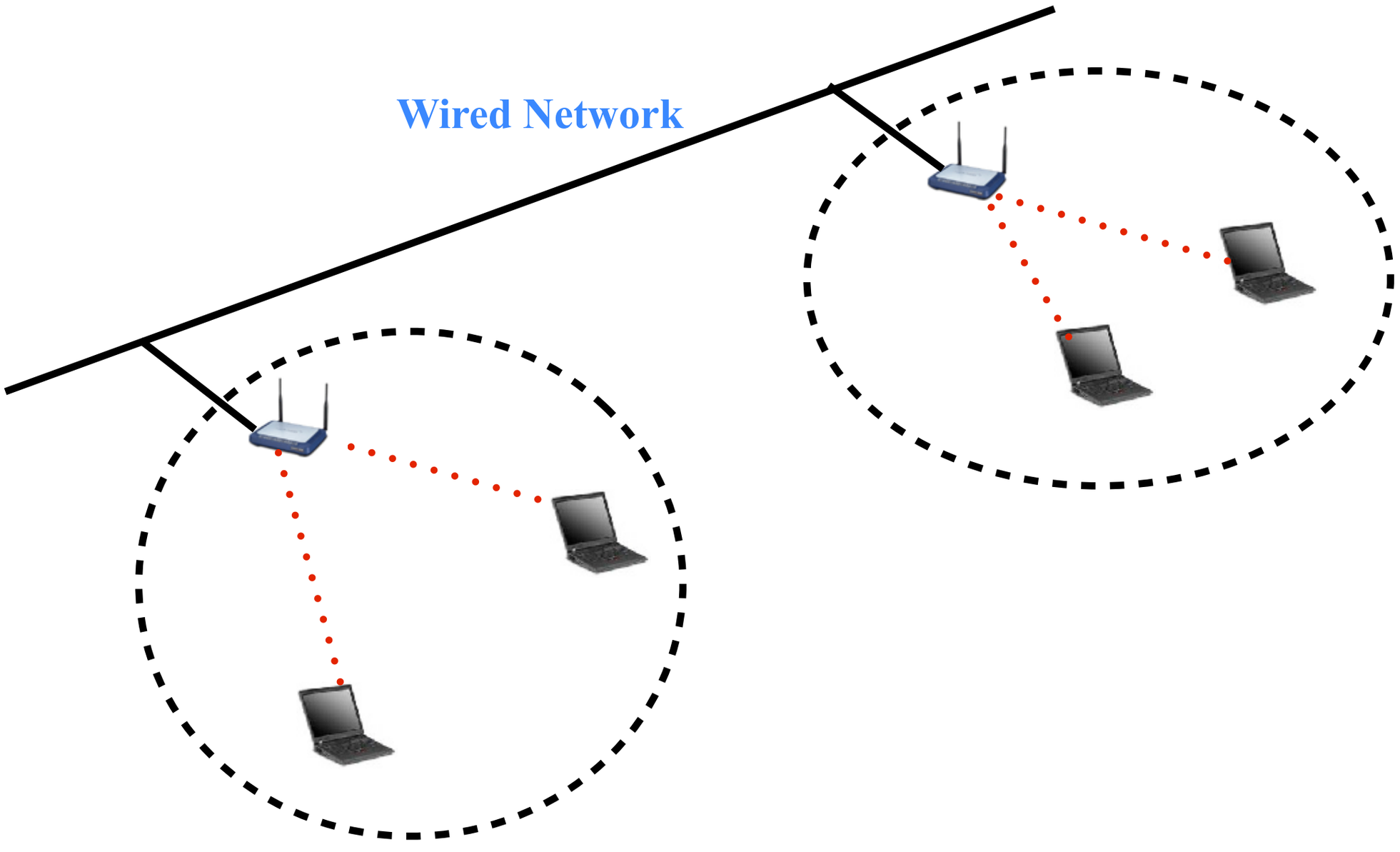
Distribution System

A system to interconnect several Basic Service Sets.

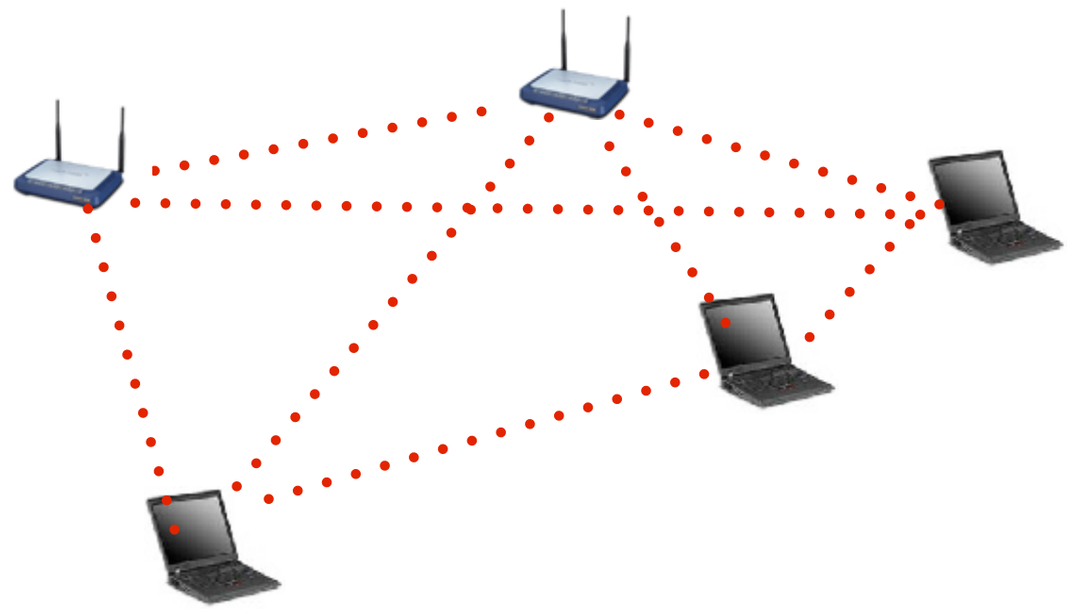
Can be:

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



Independent Basic Service Set



Service Set Identifier

- “Network name”

32 bytes long

One network (ESS or IBSS) has one SSID

Basic Service Set Identifier

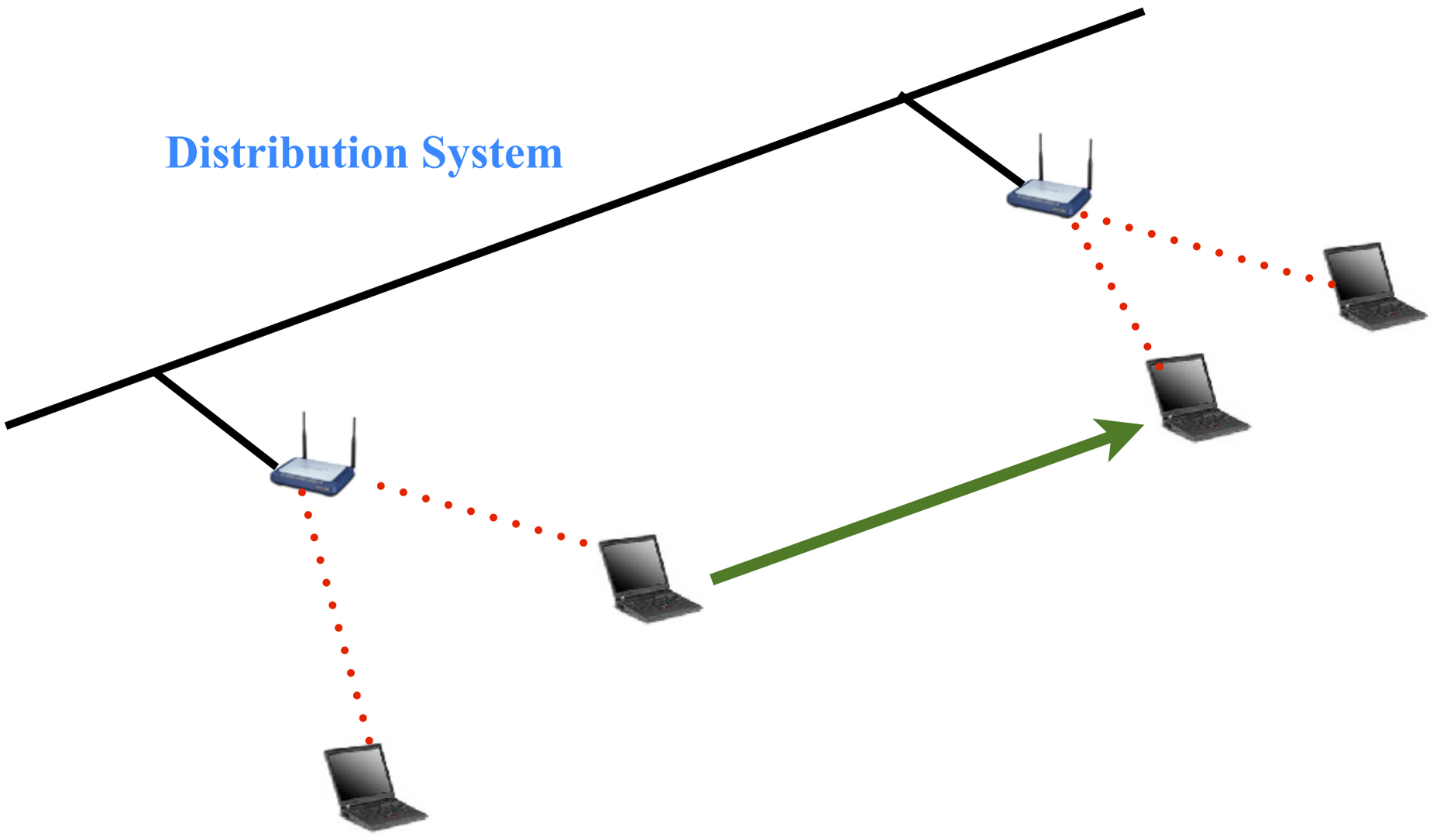
- “cell identifier”

6 bytes long (MAC address format)

One BSS has one SSID

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

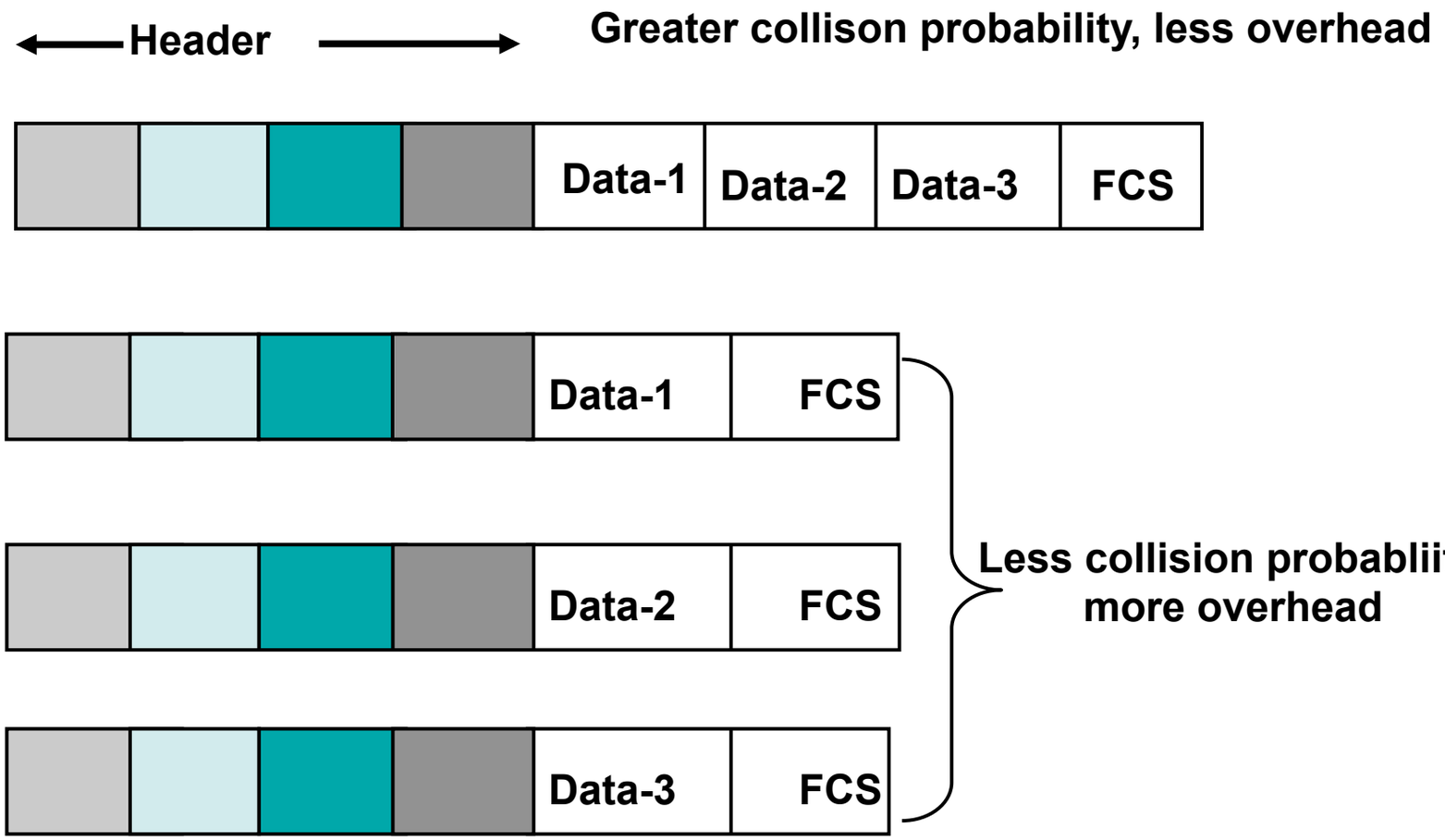
Roaming



Joining the Wireless Network

- Scanning
- Authentication
- Association
- Data Transfer

Fragmentation



802.1X Authentication

Request

ID request

AP blocks all requests until authentication is completed

Identification

Identification

The RADIUS server authenticates the client

Thank you for your attention

For more details about the topics presented in this lecture, please see the book ***Wireless Networking in the Developing World***, available as free download in many languages at:

http://wndw.net/