

IEEE 802.11

Wireless LAN

(wLAN)

IEEE 802.11

Specified by IEEE 802 Committee for LAN/MAN

Standards for Infrastructure Layers (OSI 1 and 2)

Extends Ethernet for wireless physical layer

Data rates

802.11 (1997) specified 1 or 2 Mbps (legacy)

802.11a (1999) specifies 6 to 54 Mbps

802.11b (1999) 5.5 Mbps and 11 Mbps (WiFi)

802.11g (2003) 54 Mbps (WiFi)

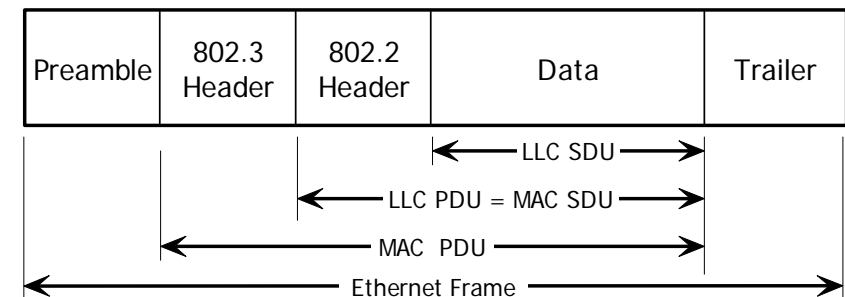
802.11n (2009) specifies up to 300 Mbps

IEEE 802 LAN Model

OSI Layer	IEEE 802 Layer	Function
Data Link Layer	Logical Link Control (LLC)	Transmission reliability
	Bridging	LAN-to-LAN frame forwarding
	MAC Sublayer	Medium access, frame structure, physical addresses
Physical Layer	Convergence Sublayer	PHY-specific header
	PHY	Bits: Electricity, Optics, Radio

Ethernet in IEEE 802 Model

LLC	802.2 LLC frame for SEQ/ACK/Control
Bridging	Ethernet bridge protocols (spanning tree, promiscuous, etc.)
MAC	Ethernet header/trailer fields and CSMA/CD access
Convergence	64 bit preamble for transceiver training
PHY	10/100/1000/10,000 Mbps Baseband, wire cable or optical fiber



Wireless Issues in LANs

Mobility

- Addressable unit is a mobile station (STA)
- Dynamic topologies
- Medium boundaries are neither absolute nor visible
- Lack full connectivity — STAs may be "hidden"

Reliability

- Medium less reliable than wired PHY
- Time-varying and asymmetric propagation

Power management

IEEE 802.11 wLAN Architectures

Ad Hoc Mode

- Simple Peer-To-Peer Mode (STA-to-STA)
- Limited to local communication
 - No WAN access or hand-off
- Authentication and Registration
 - Permitted but not required

Infrastructure Mode

- Basic topology
 - Permits forwarding to wired LANs and WANs
 - All communication via central Access Point (AP)
 - Permits Authentication
 - Requires Registration
- Extended topology
 - Permits hand-off among WLAN segments

Ad Hoc Mode (Peer-To-Peer Mode)

Independent Basic Service Set (IBSS)

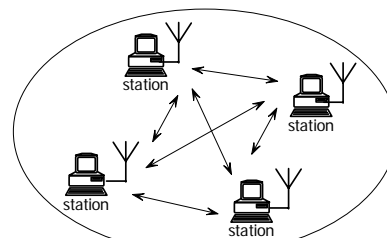
- Any set of 802.11 STAs (wireless stations)
- No connection to a wired network

Simple unmediated communication

- STAs communicate directly with one another
- Useful for quick set up
- Authentication or Registration not required

Multiple IBSSs are independent

- No bridging
- No hand-off



Independent Basic Service Set

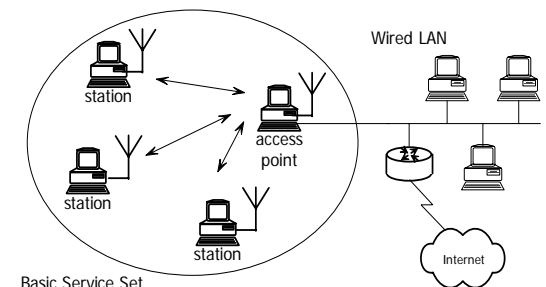
Infrastructure Mode

Basic Service Set (BSS)

- A set of wireless end stations (STA)
- An Access Point (AP)
 - Connected to the wired network infrastructure
 - Acts as base station for the wireless network
 - All traffic flows through AP by Contention or Polling (CFP)

Stations must Associate with AP

- Authentication
- Registration



Basic Service Set

Infrastructure Mode

Extended Service Set (ESS)

Two or more BSSs

Form single subnetwork (broadcast domain)

Looks like one large BSS to LLC layer

One Access Point (AP) in each BSS

BSSs connected via Distribution System (DS)

DS is backbone network

DS performs MAC-level transport of MAC SDUs

DS implementation not specified in 802.11

Portal

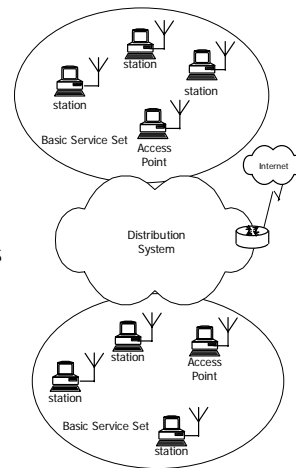
Software gateway function in AP

Bridges BSS to any non-802.11 DS protocol

DS services permit handoff

Station moving from one BSS to another

Requires coordination between APs



Defined Services in IEEE 802.11

Station Services (SS)

Privacy

Authentication

Deauthentication

MAC Service Data Unit (MSDU) Delivery

Distribution System Services (DSS)

Association

Reassociation

Disassociation

Distribution

Integration

802.11 Protocol Layers

PHY Dependent Sublayer

Transmission type

Modulation scheme

Data transmission rates

Physical Layer Convergence Sublayer

PHY medium dependent

Specifies header for PHY Dependent Sublayer

MAC layer

Medium access

Addressing

Procedures

Data Link Layer	LLC	802.2	LLC frame for SEQ/ACK/Control
	Bridging		Exchange of 802.2 PDUs
	MAC		CSMA/CA, MACA, CFP
Physical Layer	Convergence	802.11	PHY-Dependent Convergence Sublayer
	PHY		FHSS, DSSS, IR, Data rates

Station Services (SS) — 1

Privacy in wired LAN

Design assumes physical closure

Illegal access requires physical connection

Privacy in wLAN

Any 802.11 receiver in range can receive all frames

Wired Equivalent Privacy (WEP) algorithm

Shared key encryption

Not secure

No worse than wire

Station Services (SS) — 2

Authentication

Station provides proof of identity to AP or STA
 Method not specified in 802.11
 Required before Association

Deauthentication

Terminate authentication of another station
 Deauthentication invokes Disassociation

MAC Service Data Unit (MSDU) Delivery

End-to-end delivery of LLC packets
 LLC packets (PDUs) are the SDUs of the MAC

Distribution System Services (DSS) — 1

Association

Station associates with one AP
 Association provides STA/AP mapping to the DS
 DS forwards to STA via unique AP association

Reassociation

Station moves from BSS to New BSS
 Station associates with New AP in New BSS

Disassociation

New AP informs Old AP of Reassociation
 Old AP terminates old association
 APs may also disassociate all STAs (for maintenance)

Distribution System Services (DSS) — 2

Distribution

Delivery of packets to stations through DS
 STA sends to source AP
 Logically invokes DSS Distribution Service
 DS passes frame to Destination AP
 Destination AP passes frame to Destination STA

Integration

Portal services provided by DS
 Source AP sends frame to Portal
 Portal forwards to foreign (not 802.11) network

Synchronization

All STAs in BSS are synchronized to common clock

Timing Synchronization Function (TSF)

Synchronizes timers for all STAs in same BSS
 STAs maintain a local TSF timer

Infrastructure networks

AP initializes its TSF timer independently
 AP periodically transmits beacon frames with its TSF
 Receiving STA accepts TSF timing

Independent BSS (IBSS)

Distributed algorithm among BSS members
 Each STA in BSS transmits a beacon
 Each STA adopts latest (largest) TSF

802.11 Physical Medium

Three Bit-Serial Transmission Bands

Infra Red (IR) Optical Transmission

- 2 km line-of-sight
- 20 meter omnidirectional

Point-to-Point Microwave Radio

Omnidirectional Radio

- Industrial/Scientific/Medical (ISM) band
- 2.4 — 2.483 GHz
- 10 to 100 mW

Data Coding Schemes for 802.11

Spread Spectrum techniques

- Use more capacity than required minimum
- Increases error control and security

Direct Sequence Spread Spectrum (DSSS)

- Transmit m bits for each data bit
- Data rate of n bps \Rightarrow transmission rate of $m \times n$ bps
- Similar to CDMA, but only one code is used

Frequency Hopping Spread Spectrum (FHSS)

- Radio transmit frequency jumps around
- Use m frequencies of bandwidth $B \Rightarrow$ bandwidth $m \times B$
- Stations must know how and when to jump

Convergence Layer Frames

Direct Sequence Spread Spectrum (DSSS)

DSSS Physical Layer Convergence Protocol (PLCP)

PLCP preamble		PLCP header				PSDU
synch	start frame delimiter	signal	service	length	CRC	
128	16	12	4	16	16	variable

Preamble	Receiver synchronization bits (like Ethernet)
Signal	Data transmission rate
PSDU	Physical-layer Service Data Unit (SDU) Protocol Data Unit (PDU) of MAC layer
Length	Length of PSDU

Convergence Layer Frames

Frequency Hopping Spread Spectrum (FHSS)

FHSS Physical Layer Convergence Protocol (PLCP)

PLCP preamble		PLCP header			whitened PSDU
Synch	start frame delimiter	PLW	PSF	HEC	
80	16	12	4	16	variable

PLW	PSDU Length Word
PSF	PLCP Signaling Field
HEC	Header Error Check
Whitened	Encoding scheme to smooth statistics of data

IEEE 802.11a-1999

Specifies new PHY entity in 5 GHz band

Orthogonal Frequency Division Multiplexing (OFDM)

Advanced data coding method

Permits higher transmission rates

Radio frequencies

5.15–5.25, 5.25–5.35 GHz

5.725–5.825 GHz

Data rates: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps

IEEE 802.11b-1999

Extends existing PHY in 2.4 GHz band (ISM)

Enhances 802.11 DSSS system

Provides 5.5 Mbps and 11 Mbps data rates

No change to PLCP frame structure

Both PHYs can operate simultaneously in same BSS

Basis for WiFi products

New Enhancements to PHY

IEEE 802.11g-2003

Extends existing PHY in 2.4 GHz band (ISM)

Enhances 802.11 DSSS system

Provides 6, 9, 12, 18, 24, 36, 48, and 54 Mbps data rates

Minor changes to PLCP frame structure

Both PHYs can operate simultaneously in same BSS

IEEE 802.11h-2003

Extends existing PHY in 5 GHz band

Provides Spectrum and Transmit Power management

MAC Layer Issues

Channel Allocation Method

Contention (distributed control)

Round Robin (deterministic)

Polling (centralized control)

Collision Detection and Error Detection

Fragmentation

Addressing

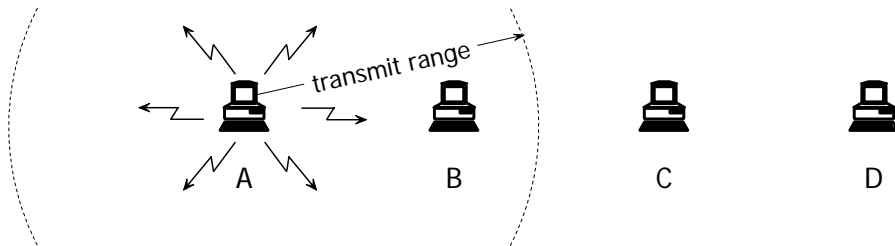
Control and Management Frames

Hidden Node Problem

A transmits to B

C cannot receive from A — out of range

C is may interfere with A's transmission

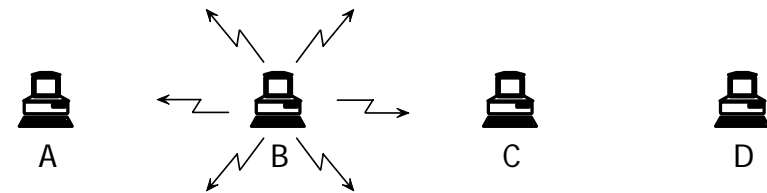


Exposed Node Problem

B transmits to A

C receives B's transmission and is not free to start

C delays its transmission to D unnecessarily



Older MAC Schemes for wLAN

Pure ALOHA protocol

Stations transmit at random

Collisions occur when transmissions overlap

Avoid collisions

Limit access to 18% duty cycle

Reach 36% duty cycle with slotted ALOHA

Carrier Sense Multiple Access (CSMA)

ALOHA with carrier sense

Stations do not transmit if radio medium is active

Polling

Access Point polls STAs

STAs only transmit after being polled

Channel Allocation Methods in IEEE 802.11

Distributed Control Function (DCF)

Contention-based multiple access methods

DCF based on CSMA/CA is mandatory

Carrier Sense Multiple Access with Collision Avoidance

DCF based on CSMA/CA with MACA is optional

Multiple Access with Collision Avoidance

Point Control Function (PCF)

Centralized Access Control (polling)

PCF polling is optional

CSMA with Collision Avoidance (CSMA/CA)

Carrier Sense Multiple Access (CSMA)

- Stations listen for transmissions
- Do not transmit if carrier is detected
- Collision detection not possible
 - Hidden node problem
 - Antenna cannot receive while transmitter active

Collision Avoidance (CA)

- Non-persistent access
- Random backoff

Multiple Access with Collision Avoidance (MACA)

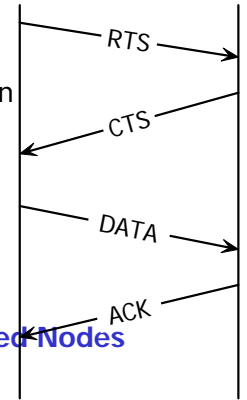
Channel set-up before data transmission

- RTS — Request To Send
- CTS — Clear To Send
- ACK — Acknowledgment of error-free transmission

Net Allocation Vector (NAV)

- Transmitted in RTS
- Predicted data transmission time

Improves behavior of Hidden Nodes and Exposed Nodes



Multiple Access with Collision Avoidance (MACA)

B sends 30-byte RTS (request to send) packet to C

- Includes a NAV for the data to be sent
- All stations in B's range hear RTS

C responds with CTS (clear to send) packet to B

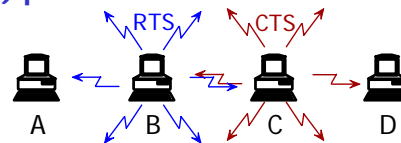
- Echoes NAV
- All stations in C's range hear CTS

B in range of A but not D

- A receives RTS but not CTS
- A can transmit without interfering with B's destination

C in range of B but not A

- D receives CTS but not RTS
- D waits data transmit time before transmitting



Priority Control in (DCF)

Interframe Space (IFS)

- Idle time between frames

Three defined IFS lengths

- Short IFS (SIFS)
- Point-coordination IFS (PIFS)
- DCF IFS (DIFS)

Each node has definite IFS

- Waiting time before attempt to transmit
- Node with short IFS transmits before node with long IFS
- Defines effective priority

Point Control Function (PCF) — Polling

Mobile Station

Does not initiate communication

Waits to be polled

Receives data from Access Point

Sends data for other stations to Access Point

Access Point

Polls stations according to schedule

Sets up connection oriented channel

Sends stored data from other Mobile Stations

Point Control Function (PCF) in IEEE 802.11

Polling by Point Controller (PC) in AP

Determines access for all stations

Scheduling is implementation dependent

Mixed Contention and PCF

Most transmission is contention-based

Periodic Contention-Free period (CFP)

AP begins Point Control (polling)

No contention/collision allowed

Contention-Free Period (CFP)

CFP repetition interval — frequency of CFP

AP initiates CFP with a beacon signal

PCF Sequence

Point Controller (PC)

Polling function in AP

CF-Aware Node

Station which can respond to polling

Beacon Frame

Indicates beginning of Contention Free Period (CFP) for polling

CF-Poll

PC polls a node for data

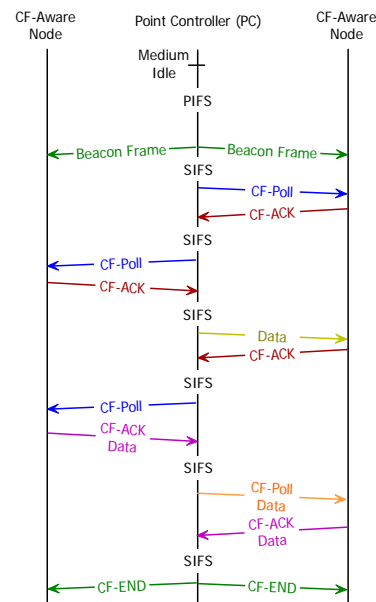
CF-ACK

Node indicates no more data to send

Data can be sent with a **Poll** or an **ACK**

CF-END

Indicates end of Contention Free Period (CFP) for polling



PCF Sequences

PC side

Senses idle medium, waits PIFS

Transmits beacon frame

Waits SIFS

Sends: CF-Poll (no data), data, or CF-Poll with data

CF-aware node side

Receives CF-Poll (no data)

Sends CF-ACK (no data), or CF-ACK (with data)

PC side can respond

Send CF-ACK (no data), or CF-ACK (with data), or CF-ACK (no data)+CF-Poll (ACK and poll new node)

PC may end CFP with CF-End frame

Fragmentation

LLC can create long MPDUs (packets)

Convergence Sublayer fragments long MPDU

Maximum length parameter

Fragments transmitted sequentially

Each fragment independently ACKed

Power Management States and Modes

Awake state: STA is fully powered

Doze state

STA not able to transmit or receive

Consumes very low power

Active mode (AM)

STA in the Awake state

STA may receive frames at any time

CFP-aware STA must be active for CFP

Power Save mode (PS)

STA listens for selected beacons

Sends PS-Poll frames to AP (requesting buffered data)

AP transmits response to PS-Poll (sends waiting frames)

State Transitions — 1

Power Save mode (PS)

STA in Doze state

STA enters Awake state

To receive selected beacons

To transmit

To send PS-Poll frames and wait for responses

For contention-free transmissions

State Transitions — 2

STAs changing Power Management mode

Inform AP using Power Management bits

In Frame Control field of transmitted frames

AP transmission to STAs in power-save (PS) mode

No arbitrary transmissions

AP buffers MSDUs

AP transmits them at designated times

STAs that have buffered MSDUs within AP

Identified in a Traffic Indication Map (TIM)

Are included as an element within all AP beacons

STAs in PS mode periodically listen for beacons

STA receives a TIM and knows AP has buffered data

STA sends PS-poll and waits for response

TIM identifies STAs with buffered traffic in AP

Information is coded in a partial virtual bitmap

MAC Sublayer Frame Structure

Frame Control	Control flags
Duration/ID	Timing control
Addresses	Various MAC entities
Sequence Control	Sequence/Fragment number for error/flow control
Frame Body	0 or more data bytes (SDU)

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0-2312 bytes	4 bytes

Frame Control

Type and Subtype	Data, Control, Management with subtypes
To DS/From DS	Access Point (AP) is destination/source
More Fragments	Part of fragmented LLC packet
Retry	Indicates re-transmission of bad packet
Power Management	STA alerts AP of its mode
	Value of 1 STA will be in power-save mode Value of 0 STA will be in active mode
More Data	AP alerts STA (in power-save mode) of buffered frames
WEP	Indicates WEP encrypted data
Order	Indicates Strictly Ordered service class

Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

MAC Layer Address Fields

4 Address Fields

5 possible MAC entities:

BSS Identification Number (BSSID)

Source Address (SA)

Station which initiated the message

Destination Address (DA)

Final destination for the message

Transmitting Station Address (TA)

Station sending the message on this hop

Receiving Station Address (RA)

Destination for the message on this hop

Address Field Definitions

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	—
0	1	DA	BSSID	SA	—
1	0	BSSID	SA	DA	—
1	1	RA	TA	DA	SA

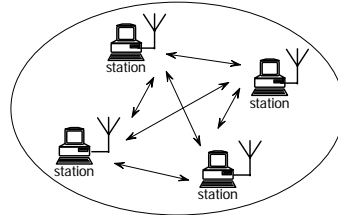
Address 1	Immediate destination address
Address 2	Immediate source address
Address 3	Final destination or source when DS performs distribution
Address 4	Source address for DS to DS messages (802.11 is also DS)

Addressing in an IBSS

To DS	From DS	Address 1	Address 2	Address 3
0	0	DA	SA	BSSID

Independent Basic Service Set (IBSS)

No Access Point (AP) and no DS
Fields To DS and From DS are 0



Independent Basic Service Set

Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	BSSID Identifies Ad Hoc network Prevents message from reaching outside IBSS

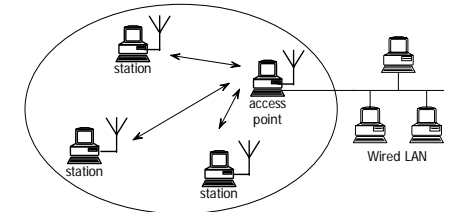
Data Addressing in a BSS

To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Basic Service Set (BSS)

All transmissions are sent To/From Access Point
To/From DS actually means To/From AP

Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	Final Destination or Source

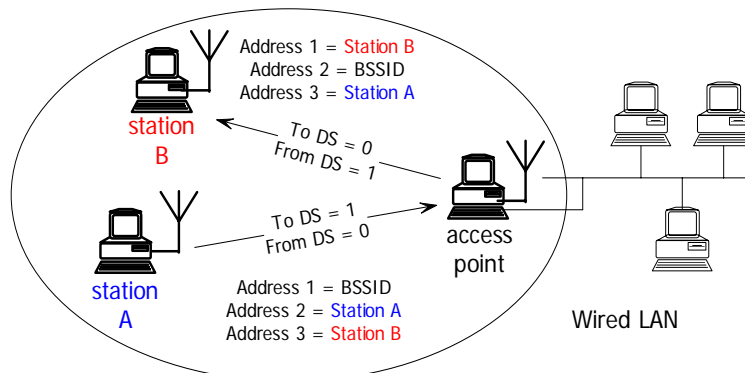


Basic Service Set

BSS Addressing Example

To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Station A sends message to Station B via AP (BSSID)



Basic Service Set

Control and Management Addressing in a BSS

To DS	From DS	Address 1	Address 2	Address 3
0	0	DA	SA	BSSID

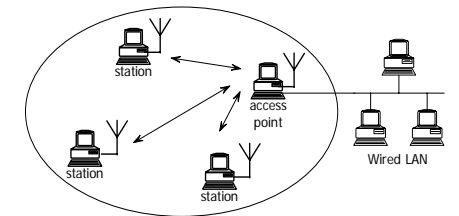
Control and Management messages in a BSS:

Only involve stations in the BSS and the AP

Are sent with To DS = From DS = 0

Either the Source or the Destination will be the AP (BSSID)

Address 3 is included as an error check



Basic Service Set

Addressing in an ESS

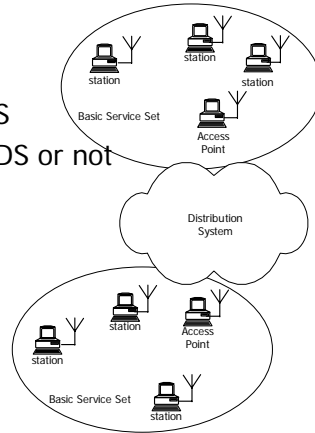
To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Extended Service Set (ESS)

All transmissions are sent via an AP

To the stations, entire ESS looks like one BSS

Stations do not know if message passes via DS or not



Address 1	Immediate destination address (DA)
Address 2	Immediate source address (SA)
Address 3	Final Destination or Source

ESS Addressing Example

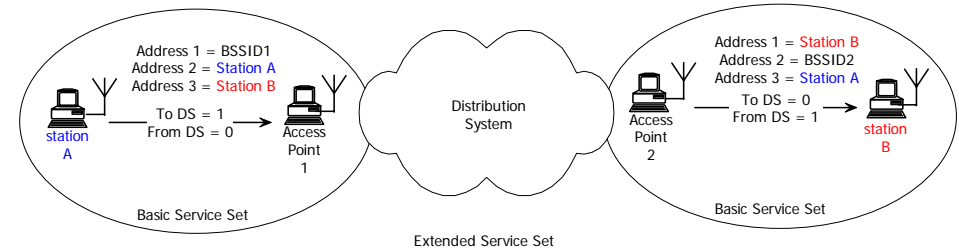
To DS	From DS	Address 1	Address 2	Address 3
0	1	DA	BSSID	SA
1	0	BSSID	SA	DA

Station A sends message to Station B via

AP1 (BSSID1) → DS → AP2 (BSSID2)

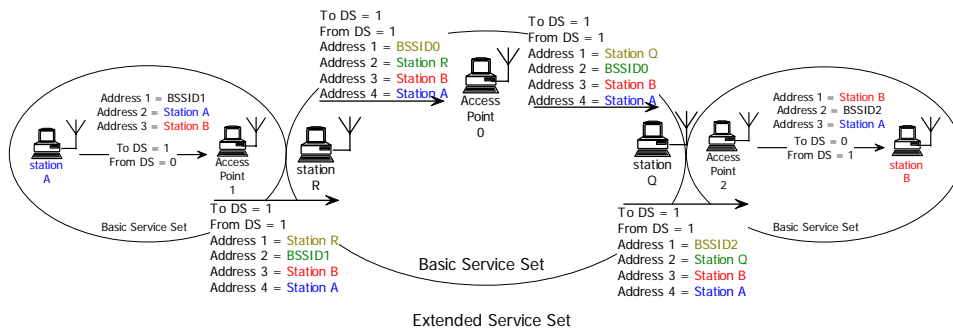
DS must forward Data, Sequence, SA, and DA

By some legal means



802.11 as Distribution System

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	DA	BSSID	SA	—
1	0	BSSID	SA	DA	—
1	1	RA	TA	DA	SA



Duration/ID

Bit 15	Bit 14	Bits 13–0	Usage
0		0–32,767	Duration — Set in NAV
1	0	0	Transmitted During CFP
1	0	1–16,383	Reserved
1	1	0	Reserved
1	1	1–2,007	Association ID (AID) in PC-Poll frames
1	1	2,008–16,383	Reserved

Duration	Estimated packet transmission time (as sent in RTS)
CFP	Used in Contention-Free Period
AID	ID assigned to STA by AP during Association

Data Frame Types

Type Data Frame includes these subtypes:

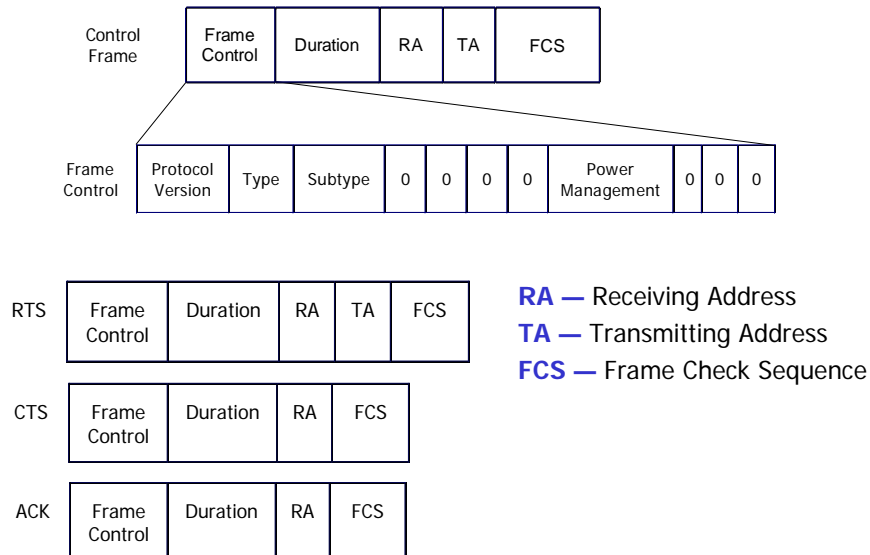
- Data
- Data + CF-ACK
- Data + CF-Poll
- Data + CF-ACK + CF-Poll
- Null function (no data)
- CF-ACK (no data)
- CF-Poll (no data)
- CF-ACK + CF-Poll (no data)

Control Frame Types

Type Control Frame includes these subtypes:

- Request To Send (RTS)
- Clear To Send (CTS)
- Acknowledgment (ACK)
- Power Save (PS)-Poll
- Contention-Free (CF)-End
- CF-End + CF-ACK

Control Frame Structure



Management Frame Types

Type Management Frame includes these subtypes:

- Authentication
- Deauthentication Association request
- Association response
- Disassociation
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon

Management Frame Fields

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS
---------------	----------	----	----	-------	------------------	------------	-----

SA — Source Address

DA — Destination Address

Frame Body contains Information Elements

Depend on management function

Parameters, identifications, status codes

Beacon Frame Body

Information Elements

Timestamp	Time at transmission
Beacon Interval	Time between beacons
Capability Information	System features
SSID	Service Set Identity (ESS or IBSS)
Supported Rates	Supported data rates
FH Parameter Set	When FHSS is used
DS Parameter Set	When DSSS is used
CF Parameter Set	When a PCF is used
IBSS Parameter Set	When Beacon is generated by a STA in an IBSS
TIM	Traffic Information Map — If the AP has buffered data for a group of STAs

Association Request Frame Body

Information Elements

Capability Information	
Listen Interval	How often STA wakes up to hear beacon
SSID	
Supported Rates	

Association Response Frame Body

Information Elements

Capability Information	
Status Code	
Association ID (AID)	Identifies Station to AP
Supported Rates	

Status Code	Meaning
0	Successful
1	Unspecified Failure
2–9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to inability to confirm that association exists
12	Association denied due to reason outside the scope of this standard
13	Responding station does not support the specified authentication algorithm
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence
15	Authentication rejected because of challenge failure
16	Authentication rejected due to timeout waiting for next frame in sequence
17	Association denied because AP is unable to handle additional associated stations
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter

Authentication Frame Body

Information Elements

Authentication Algorithm Number	Authentication algorithm number = 0: Open System Authentication algorithm number = 1: Shared Key All other values of authentication number are reserved.
Authentication Transaction Sequence Number	Indicates the current state of progress through a multistep transaction
Status Code	Authentication Status or Reserved
Challenge Text	Only present in certain Shared Key systems

Association Response Frame Body

Information Elements

Capability Information	
Status Code	
Association ID (AID)	Identifies Station to AP
Supported Rates	

Status Code	Meaning
0	Successful
1	Unspecified Failure
2-9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to inability to confirm that association exists
12	Association denied due to reason outside the scope of this standard
13	Responding station does not support the specified authentication algorithm
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence
15	Authentication rejected because of challenge failure
16	Authentication rejected due to timeout waiting for next frame in sequence
17	Association denied because AP is unable to handle additional associated stations
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter

Intel® PRO/Wireless 2011 LAN PC Card



Intel® PRO/Wireless 2011 LAN PC Card

SPECIFICATIONS	Intel® PRO/Wireless LAN PC Card
NOTEBOOK SLOT TYPE	Type II 16-bit PC card
SOFTWARE DRIVERS	Windows* 2000, 98, 95, NT*, Pocket PC and DOS; Linux*; Palm OS*
DEVICE DRIVERS	NDIS2, NDIS3, NDIS4, NDIS5 and ODI
SOFTWARE UTILITIES	Location profiles "My WLAN places"; Real-time signal strength/quality "NICutilities"; Diagnostic and Configuration "NIC Info"; Firmware upgrade "NIC Update"; Site Survey Tool
NETWORK ARCHITECTURE TYPES	Supports peer-to-peer networking and communication to wired networks via Access Points
RANGE AT 1MBPS (TYPICAL)	1500ft (460m) open environment; 300ft (90m) office environment
RANGE AT 11MBPS (TYPICAL)	400ft (120m) open environment; 100ft (30m) office environment
ANTENNA	Integrated internal diversity antenna
LED INDICATORS	Link status and link activity
RECEIVE SENSITIVITY	-87dBm @ 1Mbps; -85dBm @ 2Mbps; -84dBm @ 5.5Mbps - 81dBm @ 11Mbps
MAX OUTPUT POWER	Typical 18dBm; Minimum 14dBm
POWER CONSUMPTION	Transmit: 300mA typical (500mA max.); Receive: 170mA typical (300mA max.); Sleep: 10mA typical (25mA max.)
SAFETY COMPLIANCE	USA/Canada: UL1950/CSA 22.2; Europe: CE Marked
DIMENSIONS	Length: 111mm/4.37in; Width: 54mm/2.23in; Thickness: 5mm/.20in; Weight: 1.6oz/45.36g

Intel® PRO/Wireless 2010 LAN Access Point

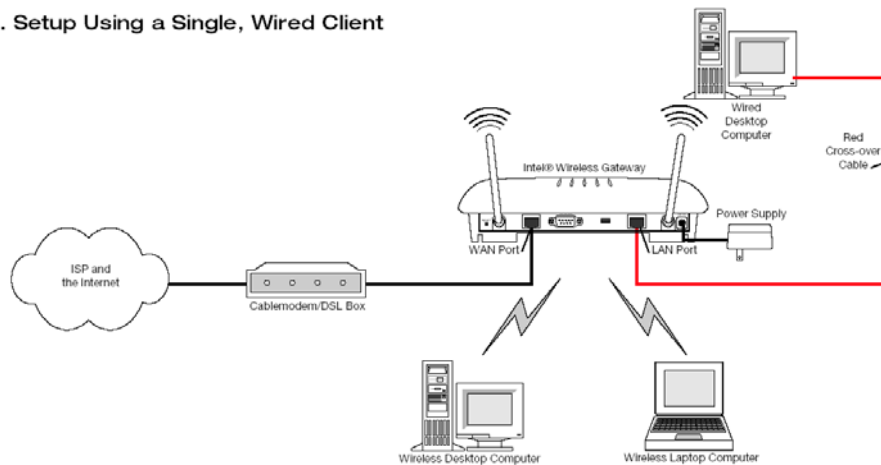


Intel® PRO/Wireless 2010 LAN Access Point

SPECIFICATIONS	Intel® PRO/Wireless LAN Access Point
STANDARDS CONFORMANCE	IEEE 802.11b High Rate, IEEE 802.3 (10BASE-T), 802.1H, 802.1d Spanning Tree, SNMP v2
LOCAL CONFIGURATION	Direct console port (serial EIA-232 DB-9 male)
REMOTE CONFIGURATION	HTTP, Telnet, SNMP, PPP, tFTP, and Intel feature to perform bulk configuration to many APs
AUTOMATIC CONFIGURATION	BOOTP and DHCP
MAXIMUM CLIENTS	256
MANAGEMENT FEATURES	Client Access Control via MAC address; Embedded HTTP Server SNMP traps; Multilevel passwords
DIAGNOSTIC CAPABILITIES	Event logging, data packet tracing, SNMP alarm generation, operating statistics; Protocol and bandwidth filters; Site Survey utility with signal strength logging
ROAMING SUPPORT	IEEE 802.11b High Rate compliant with Intel enhanced roaming features; Mobile IP
PERFORMANCE ENHANCEMENTS	Proxy ARP; Short preamble support; QoS Voice and Data Prioritization
SECURITY	64- or 128-bit Encryption; Access Control List; MD5 Member Authentication (Mobile IP)
RANGE AT 1MBPS (TYPICAL)	1500ft (460m) open environment; 300ft (90m) office environment
RANGE AT 11MBPS (TYPICAL)	400ft (120m) open environment; 100ft (30m) office environment
ANTENNA	Two 2.2dBi dipole antennas with diversity support; also supports specialty antennas
LED INDICATORS	Status, network activity, and RF activity
RECEIVE SENSITIVITY	-87dBm @ 1Mbps; -85dBm @ 2Mbps; -84dBm @ 5.5Mbps; -81dBm @ 11Mbps
MAX OUTPUT POWER	Typical 18dBm; Minimum 14dBm
POWER SUPPLY	Input: 85 to 270V AC; Output: 12V DC
POWER ENHANCEMENTS	Power over Ethernet option2 (eliminates need for AC power at AP location)
SAFETY COMPLIANCE	USA/Canada: UL1950/CSA 22.2; Europe: CE Marked
DIMENSIONS	Length: 15.24cm/6in; Width: 21.59mm/8.5in; Height: 4.45cm/1.75in; Weight (w/ power supply): 1lbs./0.454kg
HARDWARE SHIPPING CONFIGURATION	Access Point, two dipole antennas, one power supply, one country-specific power supply cord (three in "EU" SKU), mounting brackets, clips and screws

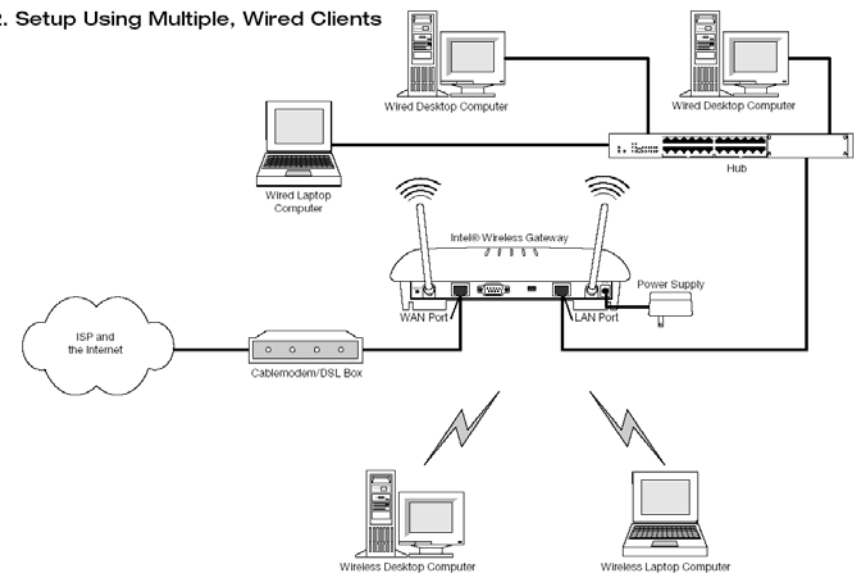
Infrastructure Network Configurations — 1

1. Setup Using a Single, Wired Client



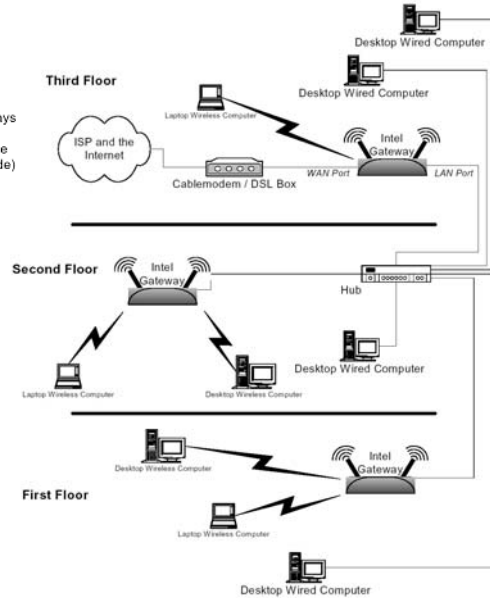
Infrastructure Network Configurations — 2

Figure 2. Setup Using Multiple, Wired Clients



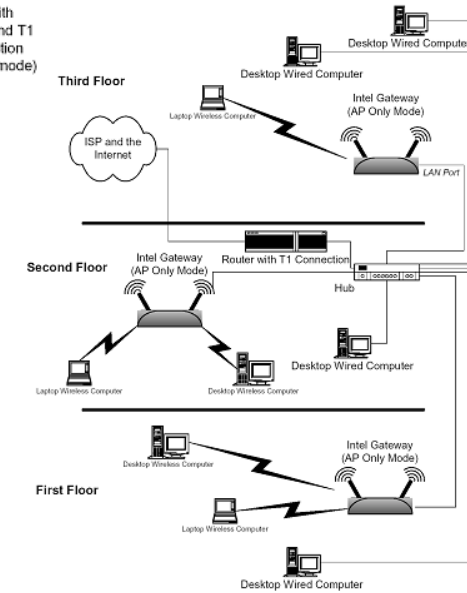
Infrastructure Network Configurations — 3

Installation example with multiple gateways
(one Intel Gateway in gateway/AP mode and other Intel Gateways in AP only mode)



Infrastructure Network Configurations — 4

Installation example with multiple Intel Gateways and T1 or other Internet connection (all Gateway's in AP only mode)



Wired Equivalent Privacy (WEP)

Protects users from casual eavesdropping

Implementation and use is optional in IEEE 802.11

WEP may be used without authentication

Key encryption algorithm

Short secret key

Longer public key

"Reasonably" strong

Requires effort to discover the secret key

Frequently changes public key

External key management service

Distributes secret keys

Not defined as part of WEP

May be implemented in either hardware or software

Definitions

Encryption (E)	Disguising data to hide information
Plaintext (P)	Data that is not enciphered (encrypted)
Ciphertext (C)	Data that is enciphered
Decryption (D)	Returning ciphertext to plaintext
Key Sequence (k)	Used in encryption operation

Encryption function E maps P to C

$$E_k(P) = C$$

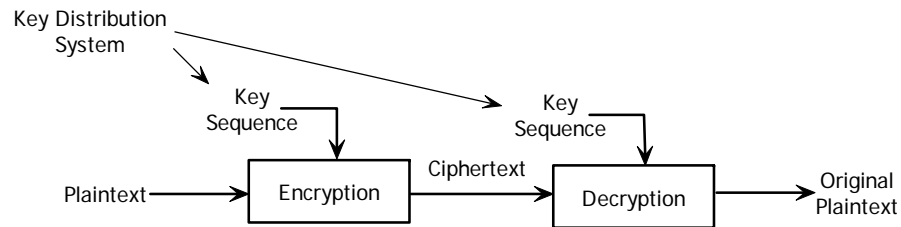
Decryption function D maps C to P

$$D_k(C) = P$$

Symmetry: Same key for encryption and decryption

$$D_k(E_k(P)) = P$$

Encryption and Decryption



WEP Encryption/Decryption Technique

Bitwise XOR of plaintext and pseudorandom key

$$C = E_k(P) = P \oplus k$$

$$P = D_k(C) = C \oplus k$$

example:

$$\begin{array}{r}
 P = \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \\
 k = \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \\
 \hline
 C = P \text{ XOR } k = \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \\
 \\
 C = \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \\
 k = \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \\
 \hline
 P = C \text{ XOR } k = \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1
 \end{array}$$

WEP Encryption and Decryption are Symmetric

$$\begin{aligned}
 (a \oplus b) \oplus c &= (\overline{ab} + \overline{ab}) \oplus c \\
 &= \overline{ab + ab} c + (\overline{ab} + \overline{ab}) \overline{c} \\
 &= (\overline{ab})(\overline{ab})c + (\overline{ab} + \overline{ab})\overline{c} \\
 &= (a + b)(\overline{a + b})c + (\overline{ab} + \overline{ab})\overline{c} \\
 &= abc + \overline{abc} + \overline{abc} + \overline{abc} \\
 &= \overline{abc} + \overline{abc} + abc + \overline{abc} \\
 &= (\overline{abc} + \overline{abc}) + a(b + \overline{c})(\overline{b} + c) \\
 &= (\overline{abc} + \overline{abc}) + a(\overline{bc})(\overline{bc}) \\
 &= a \oplus (\overline{bc} + \overline{bc}) a(\overline{bc} + \overline{bc}) \\
 &= a \oplus (b \oplus c)
 \end{aligned}$$

$$a \oplus a = (\overline{aa} + \overline{aa}) \equiv 0$$

$$a \oplus 0 = (\overline{a0} + \overline{a0}) \equiv a$$

$$C = E_k(P) = P \oplus k$$

$$P = D_k(C) = C \oplus k$$

$$= (P \oplus k) \oplus k$$

$$= P \oplus (k \oplus k)$$

$$= P \oplus 0$$

$$= P$$

WEP Encryption/Decryption Procedure

Plaintext

MAC Layer PDU (MPDU)

CRC-32 Frame Check Sequence (FCS) on MPDU

Key Sequence

Generated from Secret Key and Initialization Vector (IV)

Key length is MPDU length + 4

Transmission

Encrypted Plaintext

Unencrypted Initialization Vector (IV)

Receiver

Generates Key Sequence from Secret Key and IV

Deciphers Plaintext and checks FCS for errors

WEP Encryption Algorithm

Secret Key distributed by some background process

Initialization Vector (IV) 24-bit suffix generated by transmitter

IV may be changed as frequently as every MPDU

IV transmitted unencrypted with message to receiver

Receiver needs IV to decrypt

IV provides no information about secret key

Seed

64-bit concatenation: Secret Key ## IV

Seed input to Pseudo-Random Number Generator (PRNG)

Key Sequence k

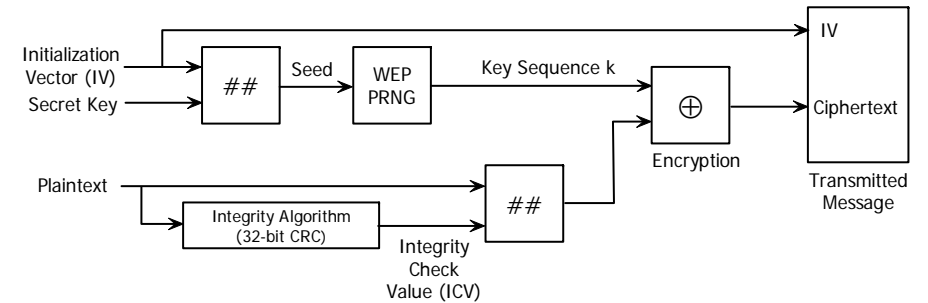
Pseudo-Random Number generated by PRNG using seed

Integrity Check Value (ICV)

32-bit CRC on MPDU

Plaintext (MPDU ## ICV) encrypted with Key Sequence

WEP Encryption Algorithm



WEP Decryption Algorithm

Key Sequence generated from IV and Secret Key

Decryption

Key Sequence applied to Ciphertext

Plaintext includes MPDU and ICV

Integrity check performed on Plaintext

On error in received MPDU

Error indication is sent to MAC management

Data not passed to LLC

Problems with WEP Algorithm

XOR encryption is not very strong

Secret Key is too easy to deduce

Part of MPDU may be easy to guess

Example: IP header fields

Can find k from P and C

Encryption strength

Depends on lifetime of Initialization Vector (IV)

Best privacy when IV is changed for every MPDU

More Problems with WEP

AP beacons

- Announce service availability
- Can be found by unauthorized listeners

WEP not always implemented

Weak encryption

- 40-bit secret key
- Simple XOR of key with plaintext

Weak authentication

- STA requests service
- AP sends random number
- STA returns number encrypted with key (password)

Authentication password is used as encryption key

- Eavesdropper can learn key from plaintext and encrypted number

WEP Encryption/Decryption Can Be Cracked

Authentication

- STA requests association
- AP sends Random Number R as challenge text
- STA encrypts R with Secret Key k as Ciphertext C
- Same key is used for Encryption of traffic

Eavesdropper

- Hears Random Number R
- Hears Ciphertext C
- Computes Secret Key k

$$\begin{aligned} C &= E_k(R) = R \oplus k \\ R &= D_k(C) = C \oplus k \\ R \oplus C &= R \oplus (R \oplus k) \\ &= (R \oplus R) \oplus k \\ &= k \end{aligned}$$

802.11i-2004 Improved wLAN Security

Recognizes problems with WEP

- Key protection vulnerability
- Weak authentication
- Weak encryption

802.11i Robust Security Network (RSN)

- Authentication and Encryption
 - Algorithms negotiated dynamically by APs and STAs
- Authentication
 - 802.1X and Extensible Authentication Protocol (EAP)
- Encryption
 - Advanced Encryption Standard (AES)

Wi-Fi Protected Access (WPA)

- Subset of 802.11i adopted by Wi-Fi Alliance
- Key Management — Temporal Key Integrity Protocol (TKIP)
- Authentication — Extensible Authentication Protocol (EAP)
- Encryption — Keeps WEP for hardware compatibility

802.11i Authentication

Implements 802.1X

Supplicant

- STA requesting access to network

Authenticator

- 802.1x capable AP

Authentication server

- Enterprise — RADIUS server
- Non-enterprise — privately distributed keys

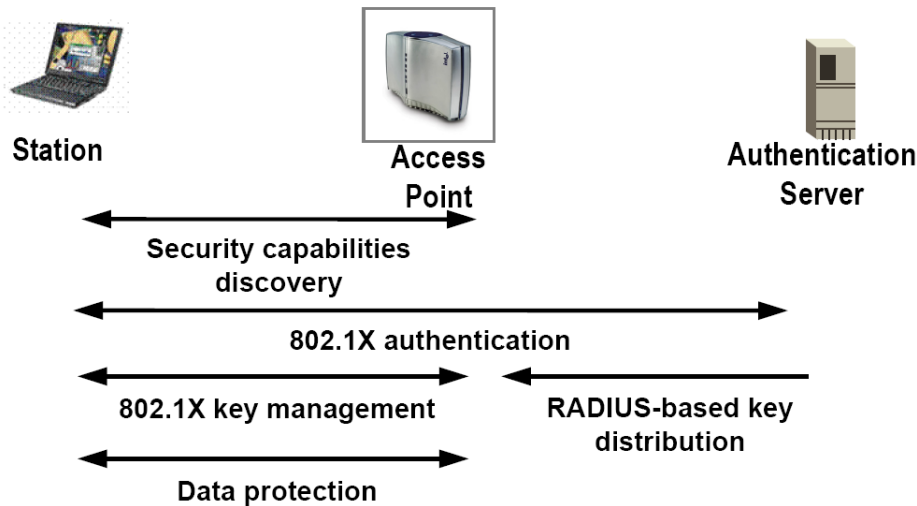
Controlled/Uncontrolled Ports

- Uncontrolled ports used for authentication exchange
- Controlled ports after authentication

Authentication Message Exchange

- IEEE 802.11i allows choice of authentication
- WPA recommends Extensible Authentication Protocol (EAP)

Security Operations



Problems in Extended Service Set (ESS)

ESS is a single broadcast domain

To STAs, entire ESS looks like one BSS

All transmissions are sent via an AP

Each STA must associate with one AP
STA may roam from BSS to BSS

802.11 does not specify mechanisms for:

Coordinating between APs
Forwarding 802.11 packets over DS

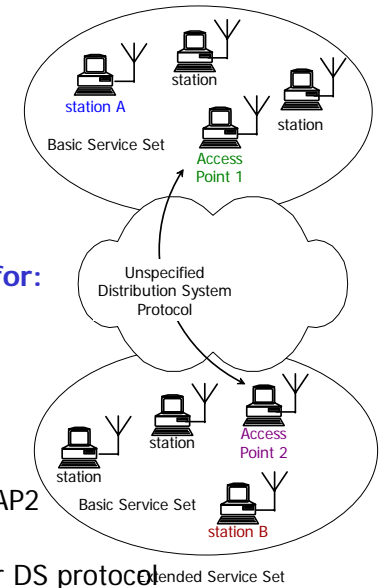
Example

STA A sends to STA B via AP1

AP1 must learn that STA B belongs to AP2

AP1 must locate AP2 via DS

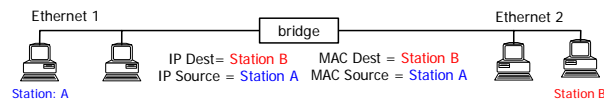
AP1 must send information to AP2 over DS protocol



802.3 Frame Forwarding Between Segments

Station A sends message to Station B via: STA_A → bridge → STA_B

Bridge forwards 802.3 MAC layer fields unchanged

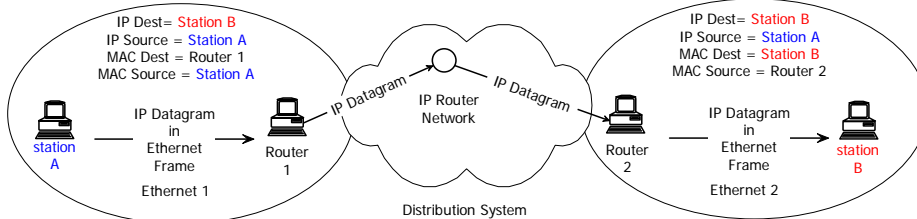


Station A sends message to Station B via:

STA_A → Router_1 → DS → Router_2 → STA_B

Routers do not forward 802.3 MAC layer fields

Routers use routing protocols and ARP to locate destination



802.11f Recommendation for DS in an ESS

No specification of DS implementation

802.11 frame forwarding not affected

Operates in parallel to DS

APs forward 802.11 frames via user-specified protocol

Specifies Inter-AP Access Protocol (IAPP)

AP-to-AP mobility management protocol

Integrates with existing AP management software

Provides Service API to AP

APs exchange information on associated STAs

Enables AP1 to locate AP2 as gateway for STA B

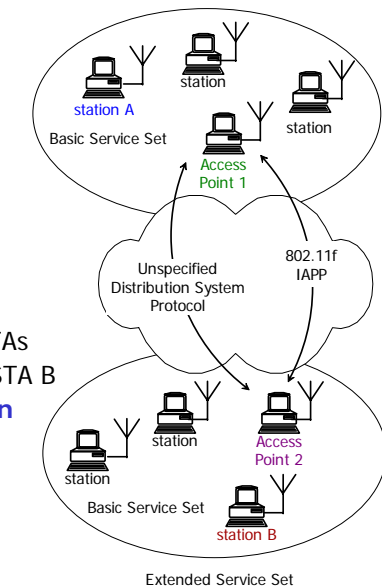
Specifies TCP/IP for AP-to-AP coordination

IAPP operates over TCP/IP stack

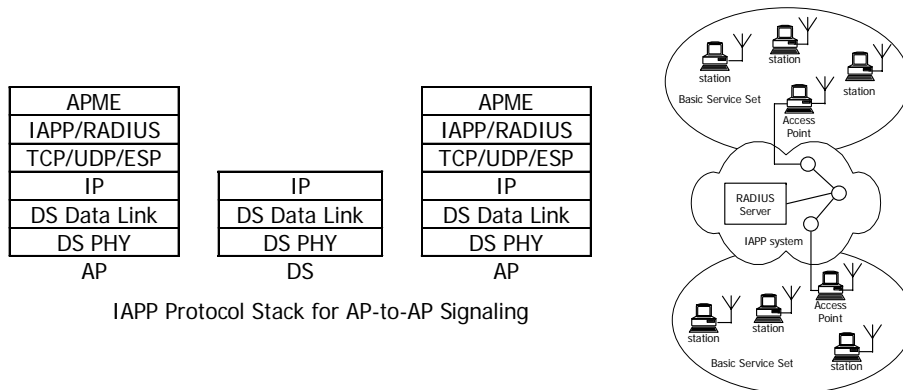
IAPP does not specify 802.11 DS behavior

DS implementation may not be TCP/IP

TCP/IP must be available in AP



Overview of IAPP Protocol Stack



APME	AP Management Entity	AP control program (manages the AP) Exchanges IAPP messages with other APs
IAPP	Inter-AP Protocol	Service Primitives for AP-to-AP coordination
RADIUS	Remote Authentication Dial-in User Service	IETF Authentication Database protocol Manages authentication and encryption for users
ESP	IP Encapsulating Security Payload	Provides security services (authentication/encryption) for IP data

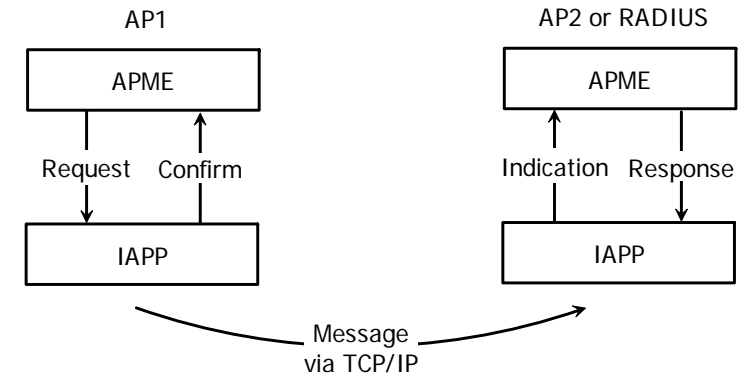
802.11f Definitions

802.11f defines transaction protocol between APs

Service primitives allow APME to invoke IAPP service functions

APP frame structure and transfer via TCP or UDP

Access to RADIUS for IP routing in DS



802.11f Address Mapping

AP Addresses

802.11 traffic in BSS

AP uses BSSID as MAC address

AP may have some network address in BSS (or not)

IAPP traffic between APs

AP uses IAPP IP address

AP have some MAC address on IAPP (or not)

IAPP may operate on Ethernet, PPP, or other data link protocol

RADIUS server

Authentication of APs for IAPP traffic

Encryption keys for IAPP traffic between APs

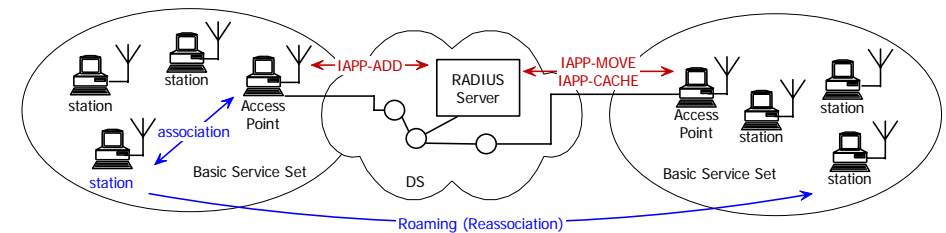
Database of BSSID (MAC addresses) to IP address for IAPP traffic

Allows APs to find IAPP address for a given BSSID

Without RADIUS server

BSSID to IP mapping performed by Inverse ARP server

802.11f Basic Operations



STA associates with AP (802.11 procedure)

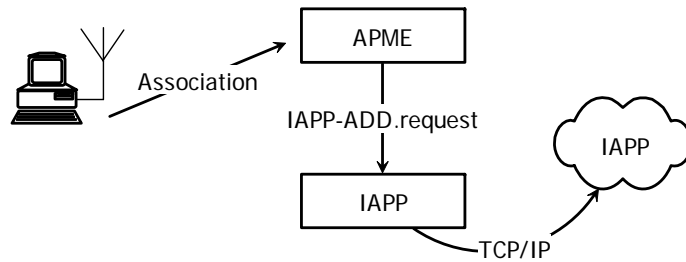
AP issues IAPP-ADD.request (802.11f procedure)

STA reassociates with new AP (802.11 procedure)

AP issues IAPP-MOVE.request (802.11f procedure)

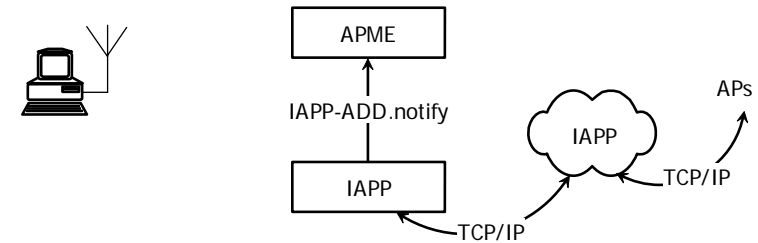
AP issues IAPP-CACHE.request (802.11f procedure)

IAPP ADD Request



STA requests association from AP
 AP Management Entity (APME) sends IAPP-ADD.request to IAPP layer
 IAPP layer sends association message to all APs

IAPP-ADD.notify



**All APs on IAPP network receive IAPP-ADD.notify message
 In each AP**

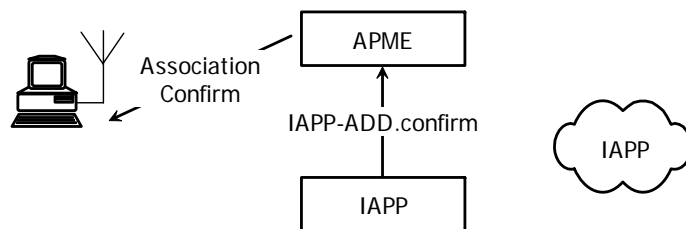
IAPP layer sends IAPP-ADD.notify message to APME
 Contains

- BSS MAC address of Associating STA
- SEQ of Association request on BSS

**All APs remove STA from location tables
 Associated AP sends broadcast message from Associating STA**

All DS nodes learn that STA is associated with AP

IAPP-ADD.confirm



In Associated AP, IAPP sends IAPP-ADD.confirm message to APME
 APME adds STA to its association list
 AP sends 802.11 Association Confirm message to STA

IAPP ADD Move

New APME		IAPP		Old IAPP
	→	IAPP-MOVE.request		
			→	IAPP-MOVE.notify
		IAPP-MOVE.response Security information	←	
IAPP-MOVE.confirm Security information	←			

Security information — keys for previous transfers between **STA** and **Old AP**

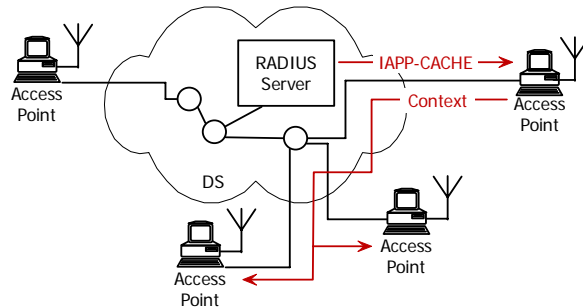
IAPP-CACHE.request

AP receives IAPP-cache.request

AP provides STA Context to all APs within one-hop

Used to speed up roaming and hand-off

Usually a STA will roam from a BSS to a neighbor BSS



802.11 Frame Forwarding Over DS

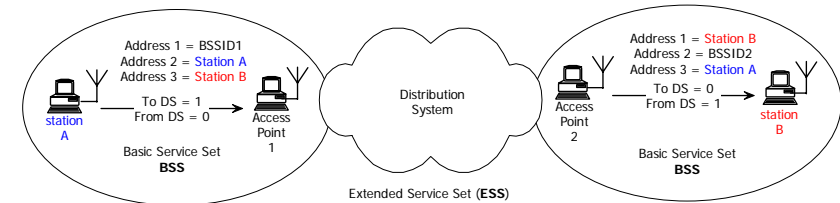
Station A sends message to Station B via:

STA_A → AP1 (BSSID1) → DS → AP2 (BSSID2) → STA_B

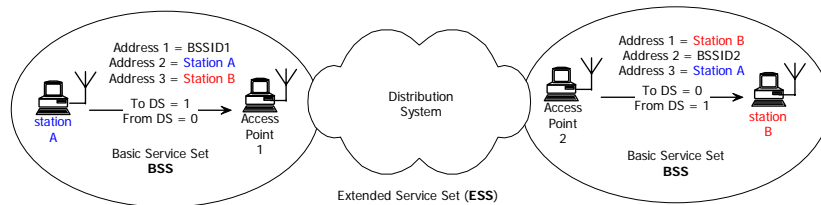
DS forwards Data, Sequence, SA, and DA fields

From AP1 to AP2

By some legal means (not specified in 802.11)



Choices for Implementing DS



Proprietary protocol

Some communications protocol runs between AP1 and AP2

AP1 accepts 802.11 frame from STA A

DS function in AP1 provides AP2 with information from the 802.11 frame

AP2 builds a 802.11 frame for STA B

Tunneling protocol

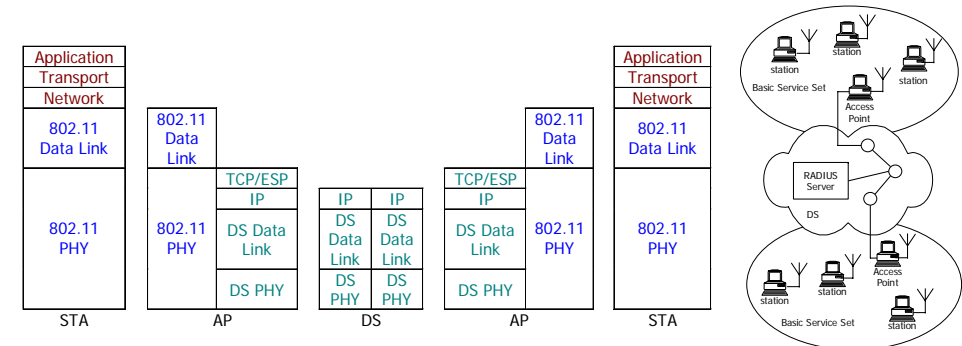
APs running 802.11f

Connected by TCP/IP network

Know BSSID and IP address of Associated AP for each STA MAC

AP can tunnel (encapsulate) complete 802.11 frames to AP2 as IP SDU

Possible STA-to-STA Forwarding Over DS



IEEE 802.11f IAPP requires TCP/IP functionality in DS

APs use TCP/IP or UDP/IP for IAPP signaling

TCP/IP protocols available in DS

Likely that APs will use TCP/IP to tunnel 802.11 STA frames

“Leverages” TCP/IP capability

Not the only possibility

Not discussed in 802.11f