The University Of Alabama in Huntsville Computer Science

cs570

Ad-hoc, DCF

The University Of Alabama in Huntsville Computer Science

Basics

cs570

- Ad-hoc mode AKA "Independent Basic Service Set" (IBSS)
- Senders/receivers can elect to use:
  - 2-frame exchange (Data – ACK)
  - 4-frame exchange (RTS – CTS – Data – ACK)
- All sends are done with a timeout – if no ACK before timeout, retransmit

The University Of Alabama in Huntsville Computer Science

802.11 Data frame format

cs570

2	2	6	6	6	2	6	0-2312	4
Cntl	Dur	Addr1	Addr2	Addr3	Seq	Addr4	Data	CRC

- Control:
  - Version
  - Type of frame (Data, CTS, RTS, re-transmit…)
  - “ToDistributionSystem” and “FromDistributionSystem” flags (used in addressing)
  - Fragmentation support
- Duration:
  - The sender’s calculation of the amount of time that the frame will take to transmit
  - Used by other nodes to estiomate when they can do an RTS
- Address 1,2,3,4:
  - Standard 802-series MAC addresses
- Seq:
  - Sequence number for fragments
- Data
- CRC

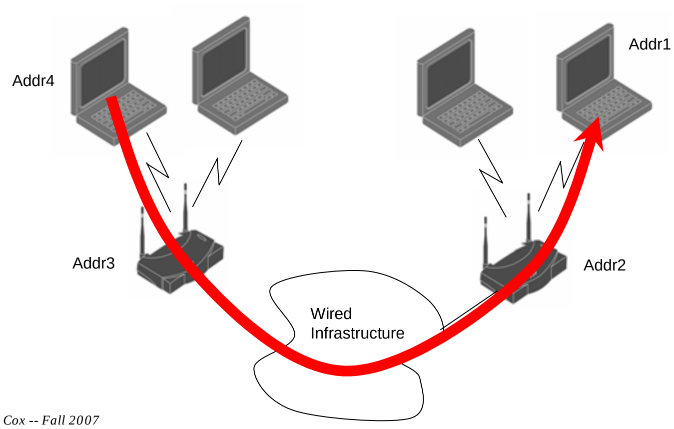
The University Of Alabama in Huntsville Computer Science

Why 4 addresses in a frame?

cs570

Needed to support a message from a wireless device, through the wired network to another wireless device

ToDistributionSystem = FromDistributionSystem = TRUE



The University Of Alabama in Huntsville Computer Science

Addressing variations

cs570

ToDS	FromDS	Addr1	Addr2	Addr3	Addr4
0	0	Dest (Wireless)	Source (Wireless)	Not used	Not used
0	1	Dest (Wireless)	Sending AP	Source (Wired)	Not used
1	0	Receiving AP	Source (Wired)	Dest (Wireless)	Not Used
1	1	Receiving AP	Sending AP	Dest (Wireless)	Source (Wireless)

G. W. Cox -- Fall 2007

The University Of Alabama in Huntsville Computer Science

802.11 Control frame formats

cs570

RTS/CTS

2	2	6	6	4
Cntl	Dur	Addr	Addr	CRC

ACK

2	2	6	4
Cntl	Dur	Addr	CRC

G. W. Cox -- Fall 2007

The University Of Alabama in Huntsville Computer Science

How duration is handled

cs570

- When a device hears an RTS/CTS sequence, it sets its “Network Allocation Vector” (NAV) according to the “duration” field of the RTS/CTS
- The time in the NAV is counted down.
- The device cannot do an RTS until the NAV=0 (and hears an ACK)

G. W. Cox -- Fall 2007

The University Of Alabama in Huntsville Computer Science

Frame fragmentation

cs570

- The fact that we have an inherently noisy medium introduces problems:
- Example:

Probability of frame being received correctly

Probability of a bit error	1,000 bit frame	10,000 bit frame
10-5	**99.9%**	**90%**
10-4	**99%**	**37%**
10-3	**90%**	**0.0045%**

- Senders have the option to break a frame that’s larger than a threshold value into smaller fragments.
- After the channel is acquired using RTS/CTS, the sender can send a stream of fragments (a “fragment burst”) using the stop-and-wait protocol

G. W. Cox -- Fall 2007

The University Of Alabama in Huntsville Computer Science

Timing and fairness

cs570

- 3 delay intervals govern timing:
  - SIFS (Short Interframe Space)
    - The shortest interval (supports DCF and PCF)
    - The interval generally used by sender and receiver between frames in an on-going exchange. Examples:
      - receipt of RTS to transmission of CTS
      - Receipt of CTS to transmission of Data
      - Receipt of Data to transmission of ACK
  - PIFS (PCF Interframe Space)
    - Next-shortest interval
    - Used by base station in PCS mode
  - DIFS (DCF Interframe Space)
    - Longest of the three
    - The interval generally used by sender when desiring to start a new exchange
- The IFS's form a de-facto priority structure:
  1. On-going exchanges (DCF or PCF)
  2. PCF Base station actions
  3. New DCF exchanges

G. W. Cox -- Fall 2007

The University Of Alabama in Huntsville Computer Science

cs570

Infrastructure Mode, PCF

G. W. Cox -- Fall 2007

Basics

The University Of Alabama in Huntsville Computer Science

- Infrastructure mode AKA “Basic Service Set” (BSS)

How a wireless device connects to an AP

The University Of Alabama in Huntsville Computer Science

A device may want to connect to a new AP:

- when it is not presently connected to an AP
- when it is connected, but wishes to connect to a new AP (due to signal loss, movement, etc)

Methods

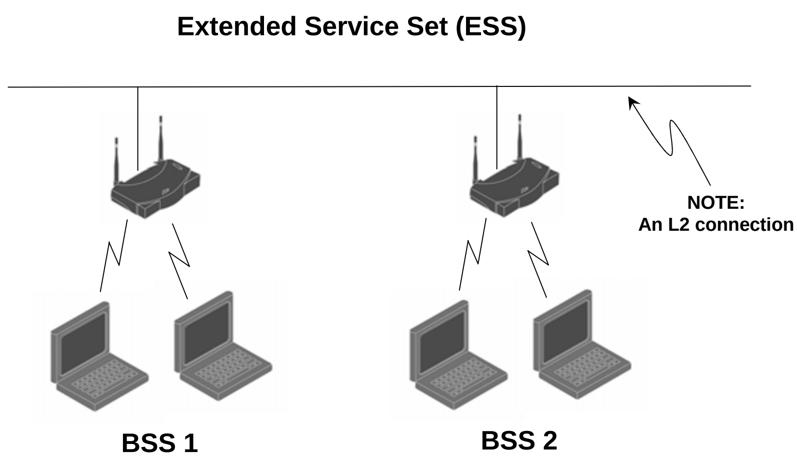
Active Scanning

1. Wireless device sends a **Probe** frame (“scanning”)
2. AP’s hearing the Probe frame (and willing to add devices), reply with a **Probe Response** frame
3. The device chooses one of the responding AP’s and sends an **Association Request** frame to it
4. The AP Sends an **Association Response** frame. If the device was previously associated with another AP, the new AP notifies the old one.

Passive scanning

1. AP’s broadcast advertisements periodically (**Beacon** frame).
2. A device hearing the beacon replies with an **Association Response** frame

Extending a net



PCF Control

The University Of Alabama in Huntsville Computer Science

cs570

- Base station periodically polls each device in its BSS to ask if the device has traffic to send
- No possibility for collision

Power saving

The University Of Alabama in Huntsville Computer Science

cs570

- Wireless nodes can enter a low-power “sleep” mode to save battery power
- Wireless device sets a flag in control field to inform AP that it is entering sleep mode.
- AP buffers traffic for the device until device reports it is awake again
- Device normally sets timeout to “wake up” to hear next beacon from AP

G. W. Cox -- Fall 2007

Security

The University Of Alabama in Huntsville Computer Science

cs570

- WEP
- WPA
- WPA2

G. W. Cox -- Fall 2007

WEP

The University Of Alabama in Huntsville Computer Science

cs570

- Wired Equivalent Privacy
- Original 802.11 security method (1999)
- Based on RC4 encryption algorithm (used in SSL)
- Originally, 40-bit keys. Later 104-bit.

- Cracked in 2001 – can now be broken in minutes
- Problem is not just key size – problem is inherent in the algorithm

- Replaced with WPA in 2003

G. W. Cox -- Fall 2007

WPA

The University Of Alabama in Huntsville Computer Science

cs570

- Based on early draft of 802.11i (security) standard

- Designed for compatibility with existing 802.11 NIC cards

- Method vs WEP
  - RC4 with 128-bit key
  - Dynamically changing keys
  - Improved Message Integrity method

- Far more secure than WEP, not perfect

G. W. Cox -- Fall 2007

The University Of Alabama in Huntsville   Computer Science

WPA-2

cs570

- 2005
- Implementation of IEEE 802.11i
- Method versus WPA
  - AES algorithm
  - Same dynamic key changing and message integrity
- Considered to be fully secure

G. W. Cox -- Fall 2007