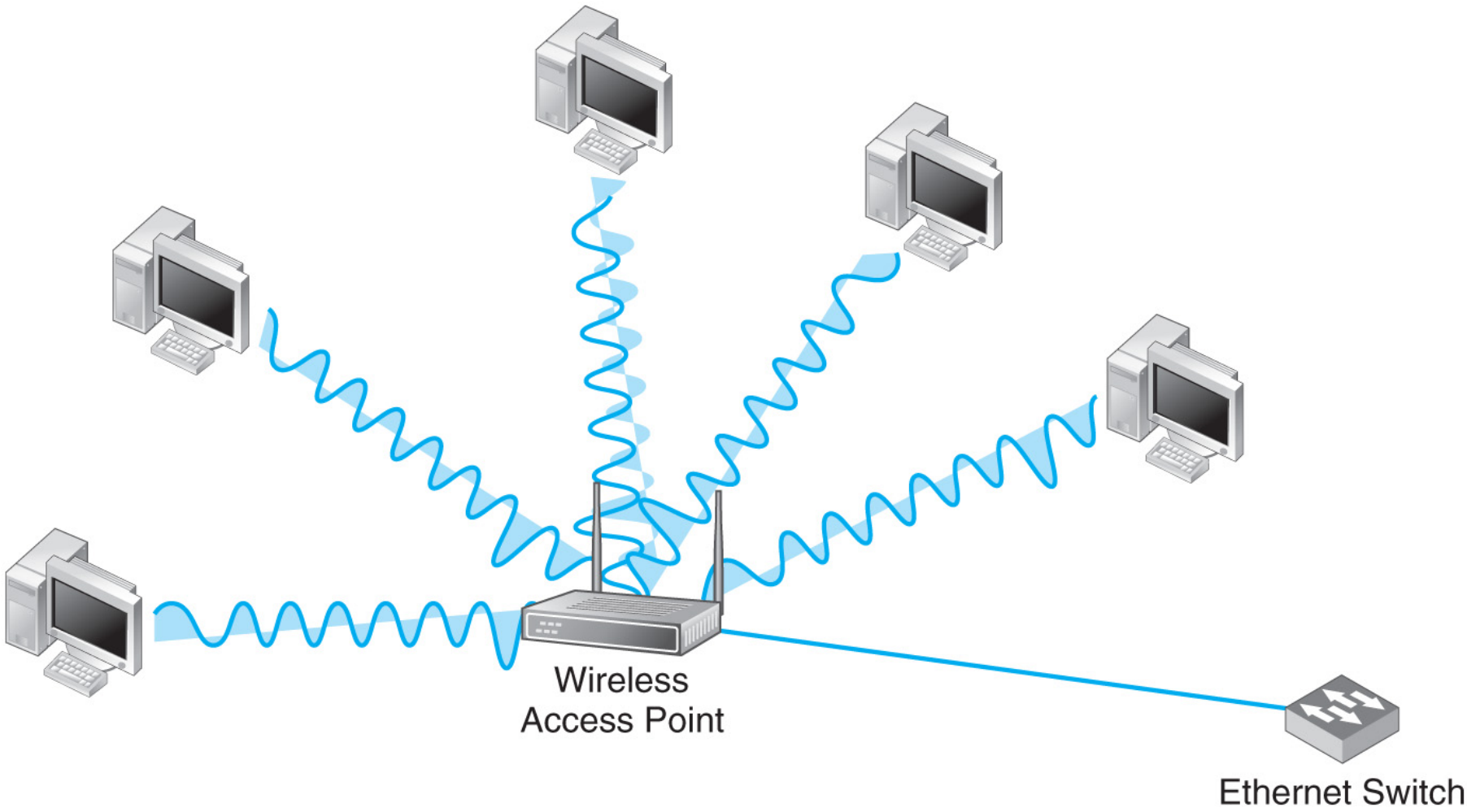
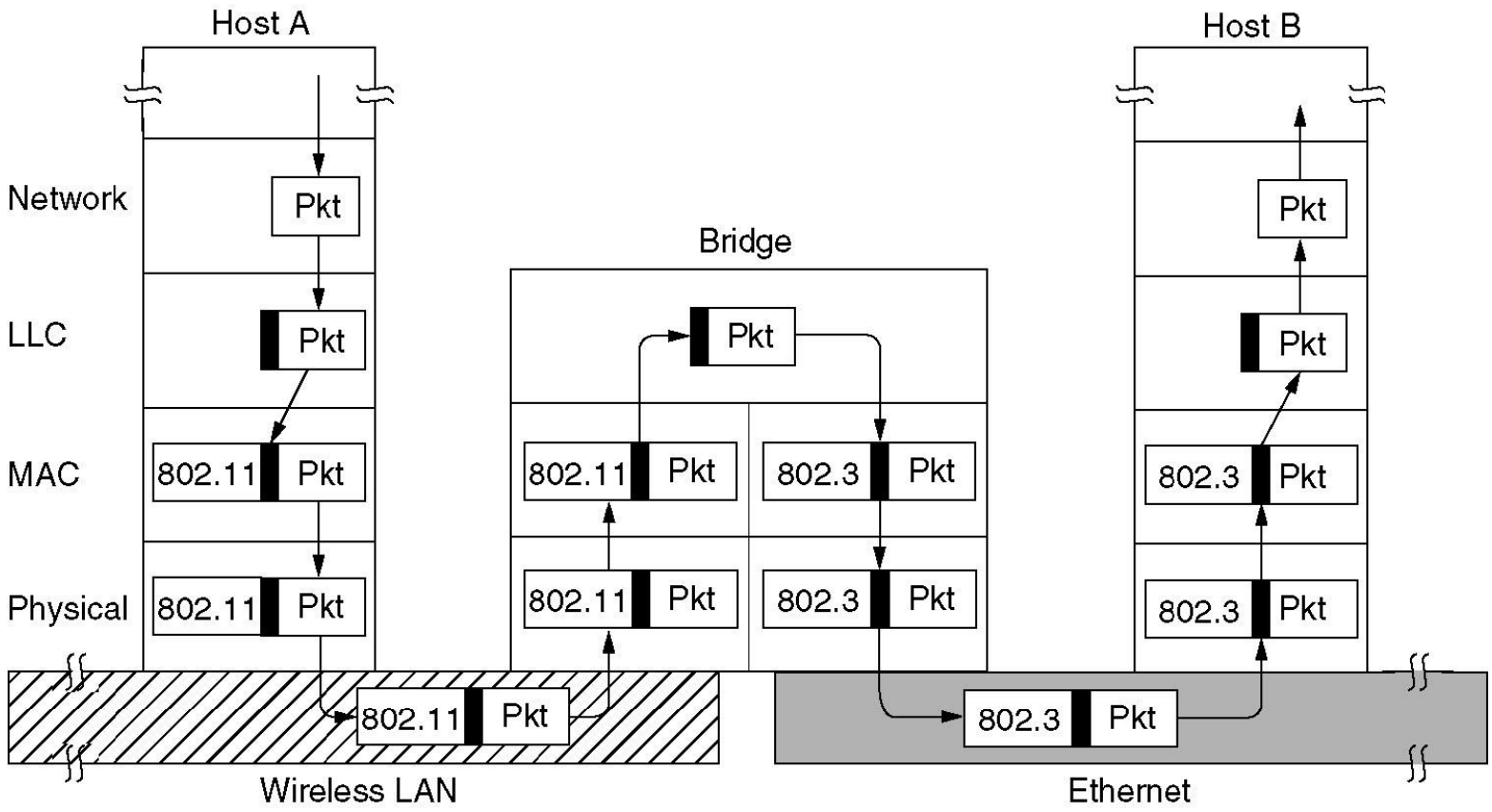
Typical Wireless Topology



Bridges from 802.11 to 802.3



Operation of a LAN bridge from 802.11 to 802.3.

Wireless Standards

802.11 (legacy):
- Originally used for infrared such as TV remote controls

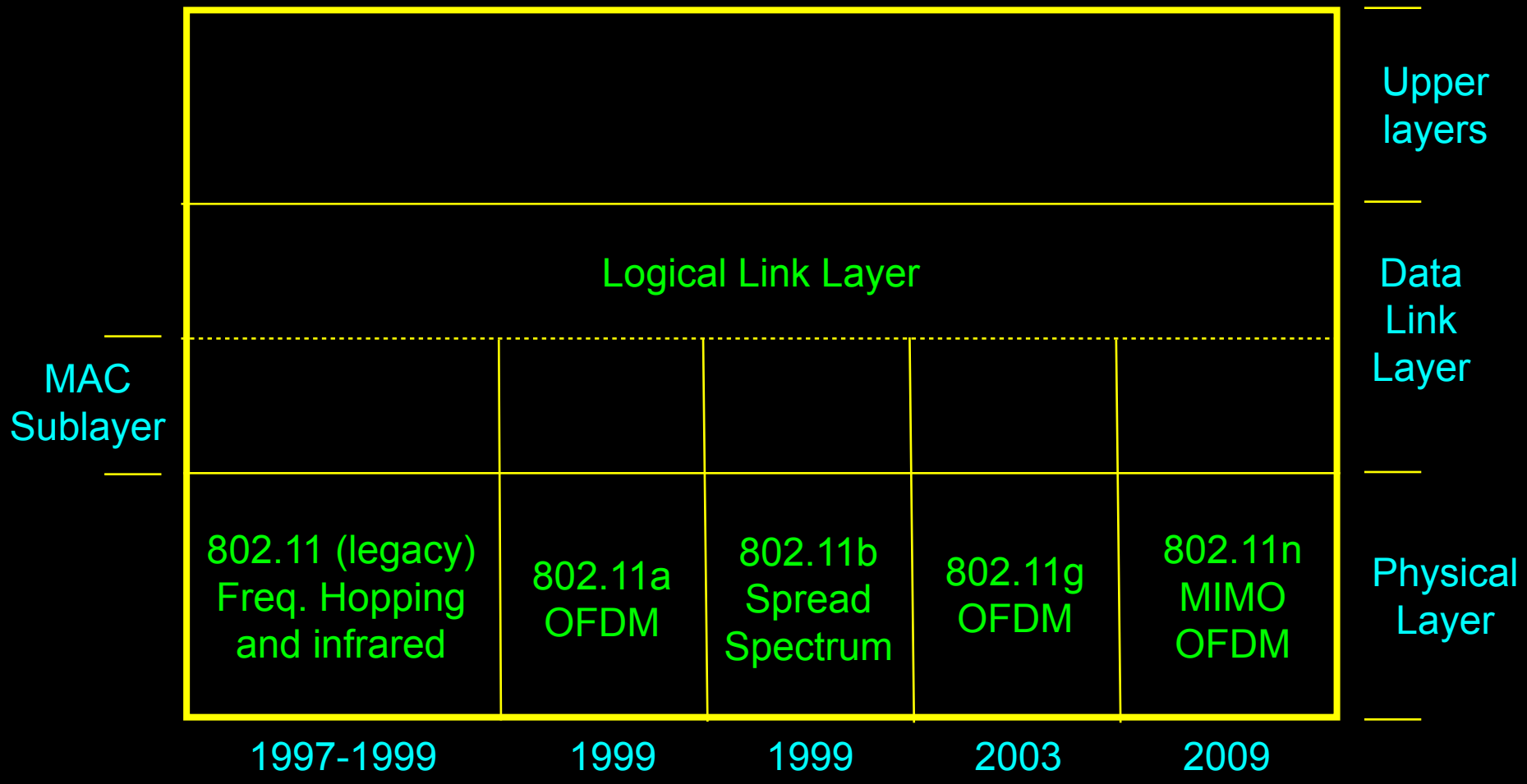
802.11a:
- OFDM (Orthogonal Frequency Division Multiplexing)
- 5ghz range
- ~ 54Mbps

802.11b:
- Spread spectrum
- 2.4ghz
- ~ 11Mbps

802.11g:
- OFDM in the 2.4gz range and backward compatible with 802.11b
- Global downgrade to 802.11b for compliancy with any single 802.11b client
- ~ 54Mbps

802.11n:
- MIMO (Multiple Input Multiple Output), up to four antennas
- Goal is to achieve 100Mbps

Wireless Protocol Stack



Wireless 802.11ac

https://en.wikipedia.org/wiki/IEEE_802.11ac

Approved in January 2014

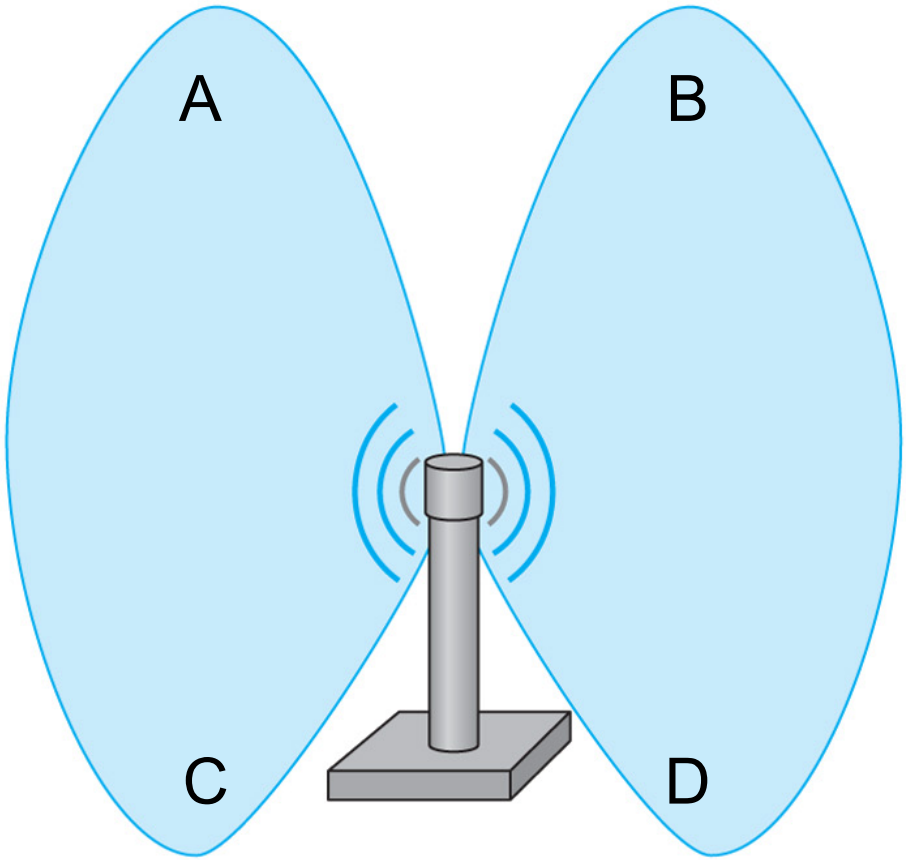
Multi-station WLAN throughput of at least 1Gbps

Single link throughput of 500Mbps

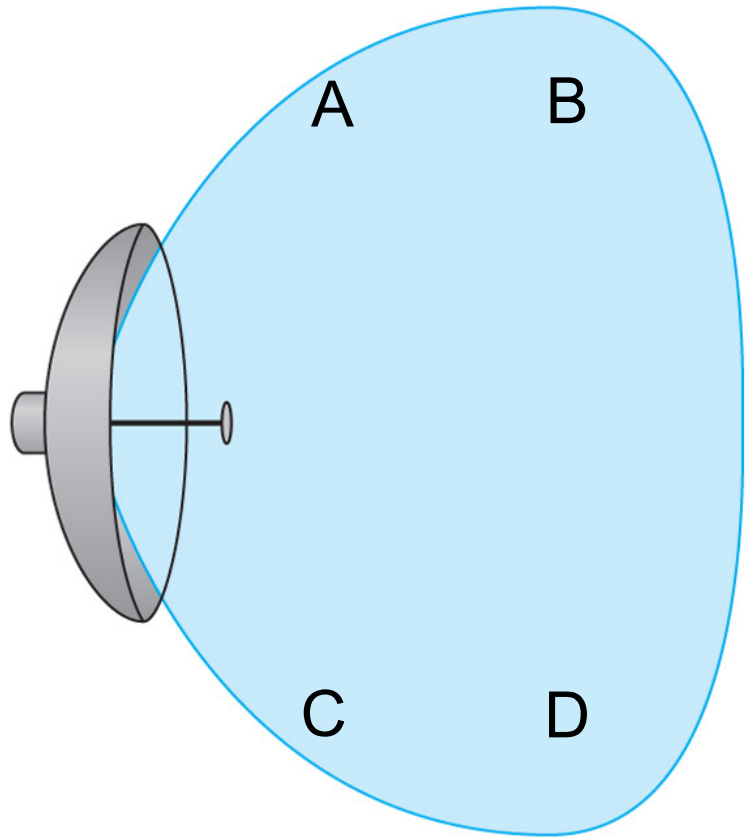
8 uplink MIMO streams

4 downlink MIMO streams

Antenna Types
and Hidden Station Problem



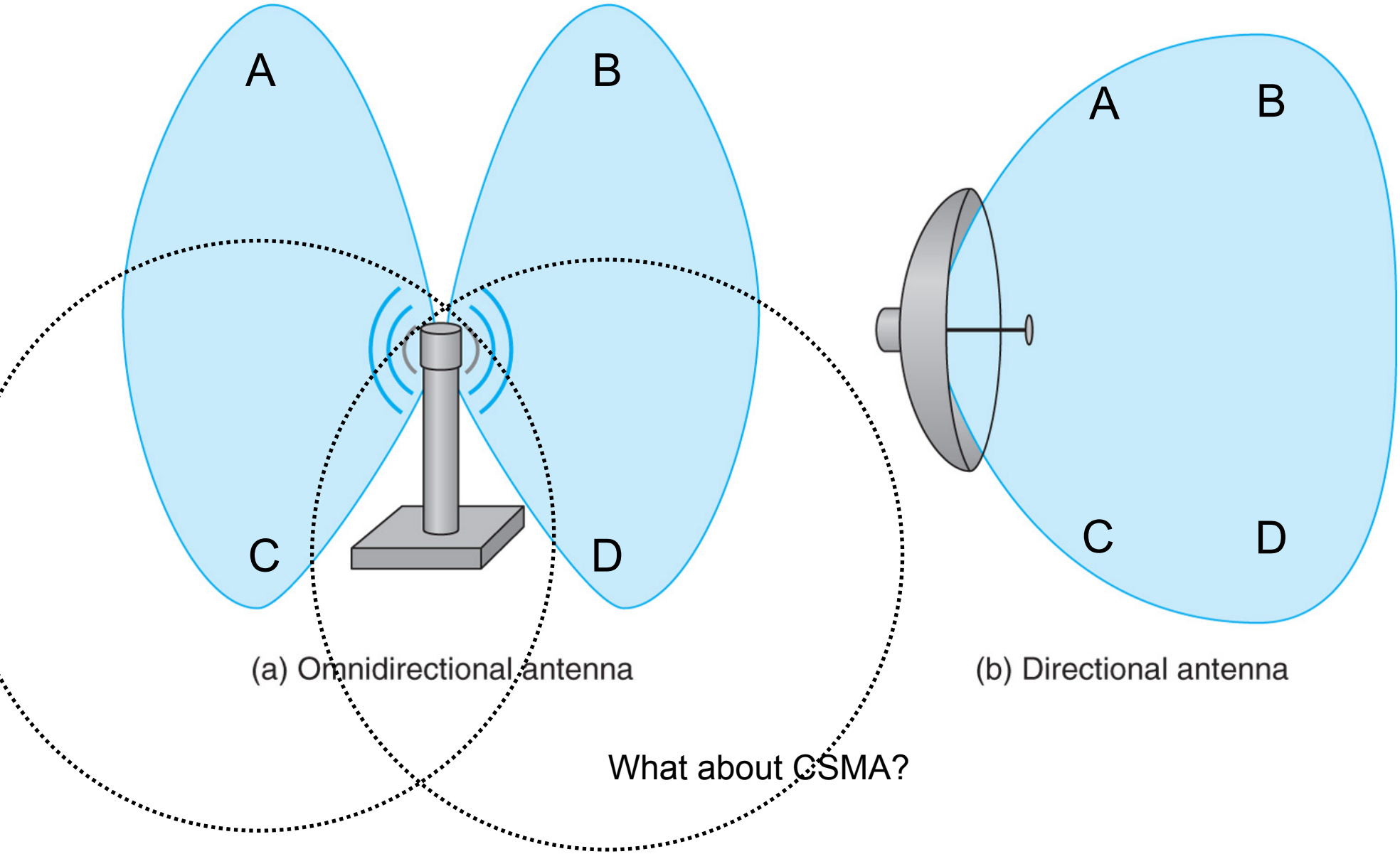
(a) Omnidirectional antenna



(b) Directional antenna

What about CSMA/Collision Detection?

Antenna Types and Hidden Station Problem

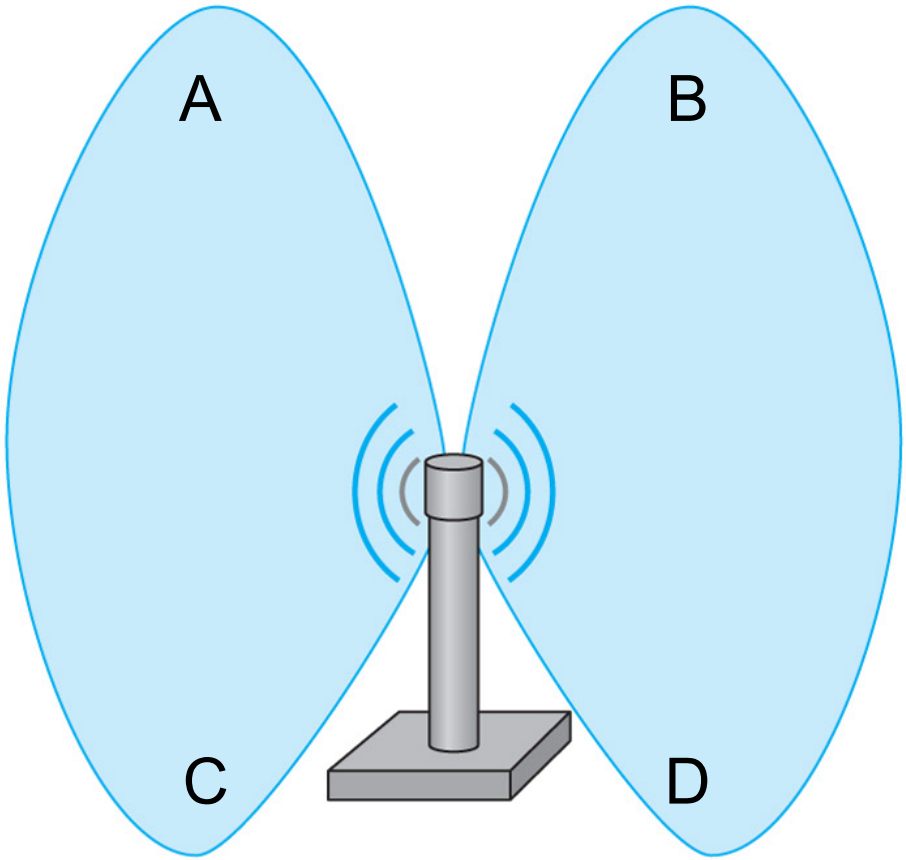


(a) Omnidirectional antenna

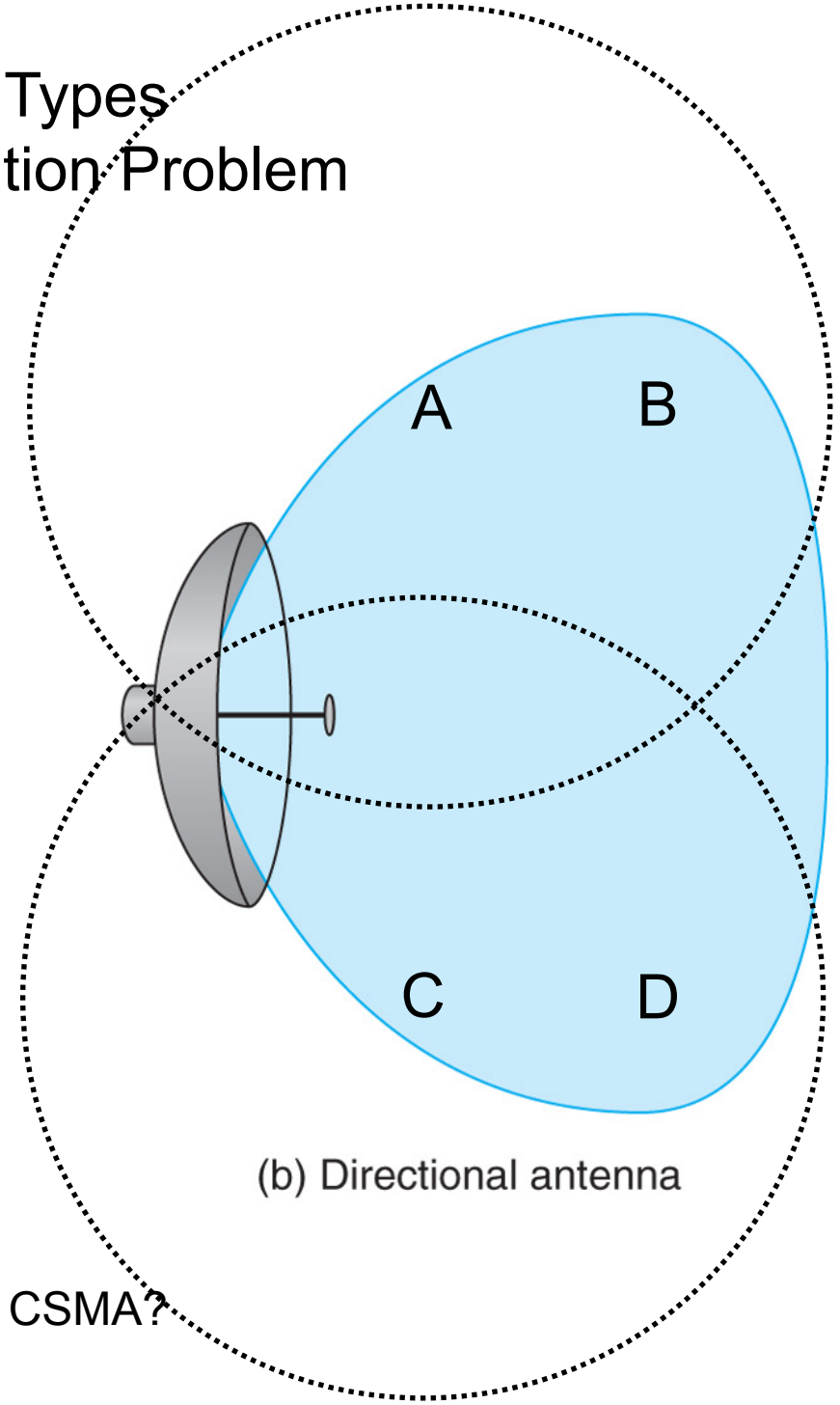
(b) Directional antenna

What about CSMA?

Antenna Types and Hidden Station Problem



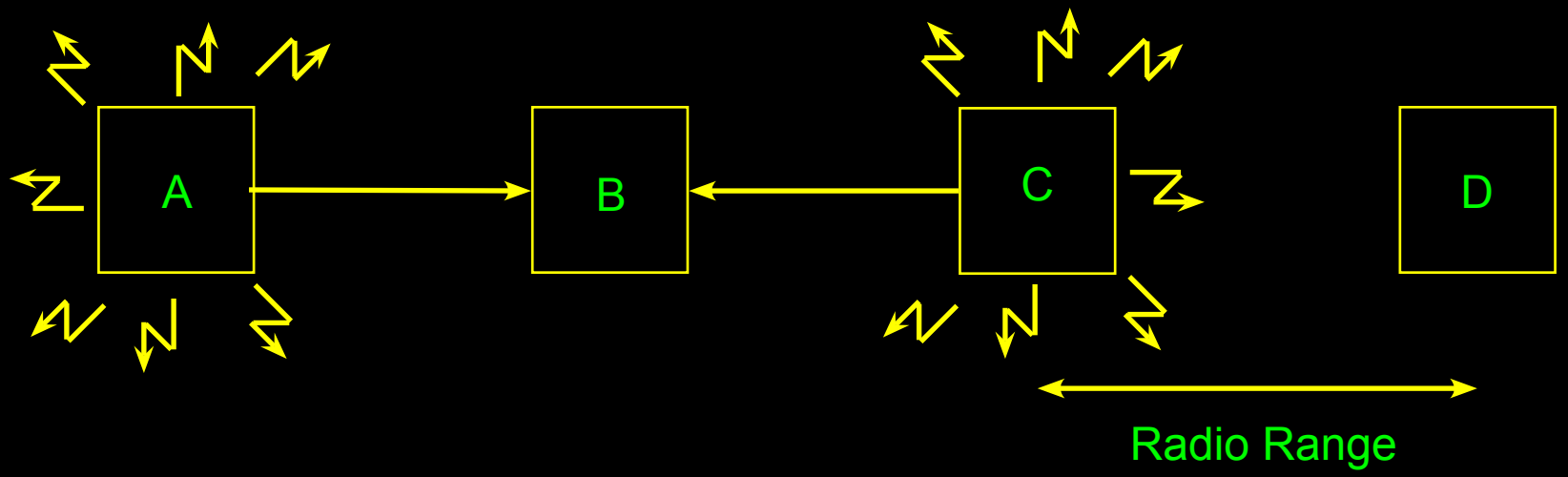
(a) Omnidirectional antenna



(b) Directional antenna

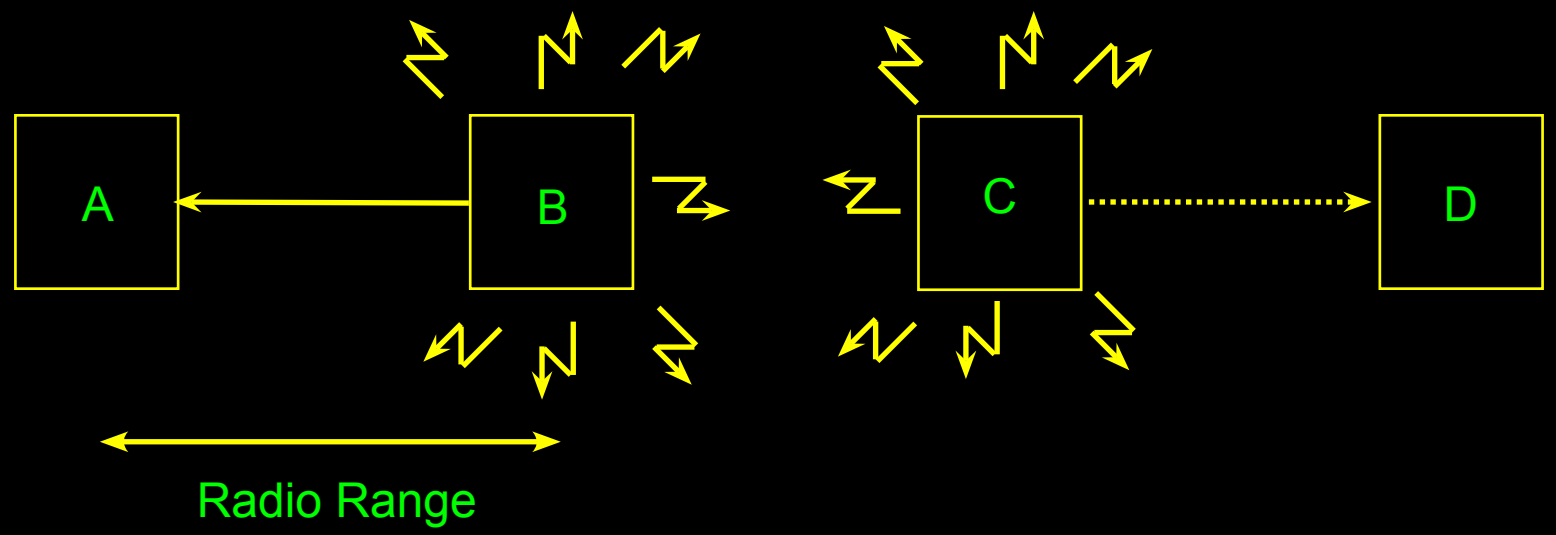
What about CSMA?

CSMA Wireless Hidden Node Problem



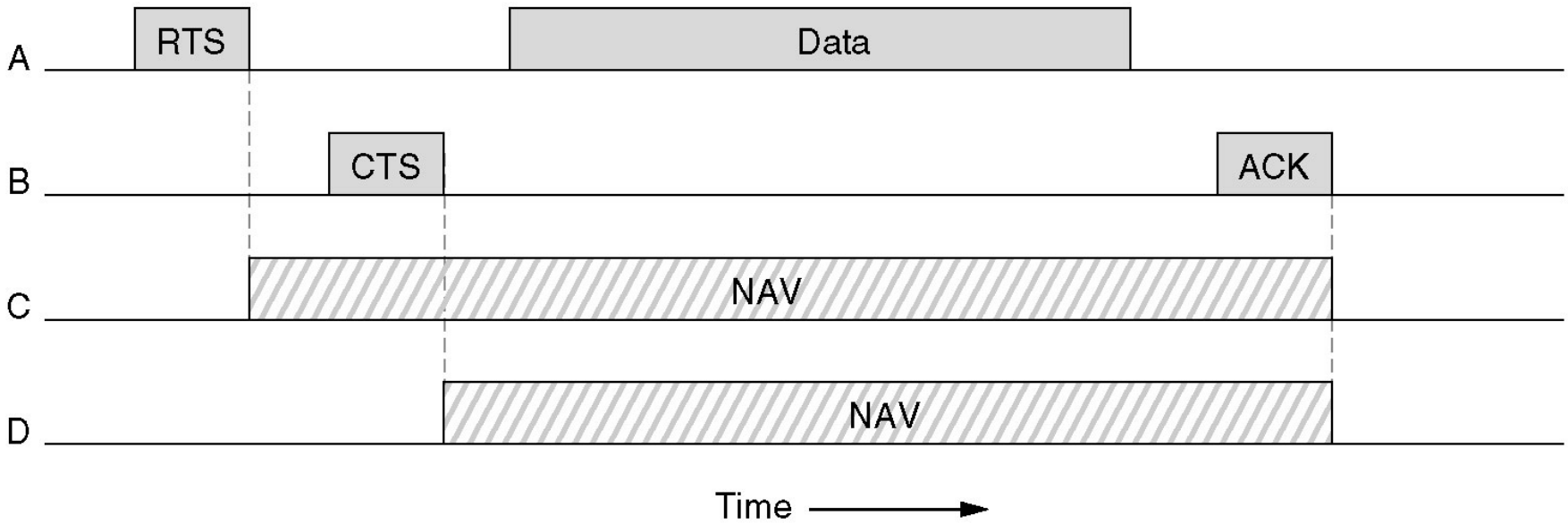
If A sends to B and then C immediately senses the medium, it will not hear A because A is out of range. Thus C will falsely conclude that it can transmit to B. If C does start transmitting, it will interfere at B, wiping out the frame from A.

CSMA Wireless Exposed Node Problem



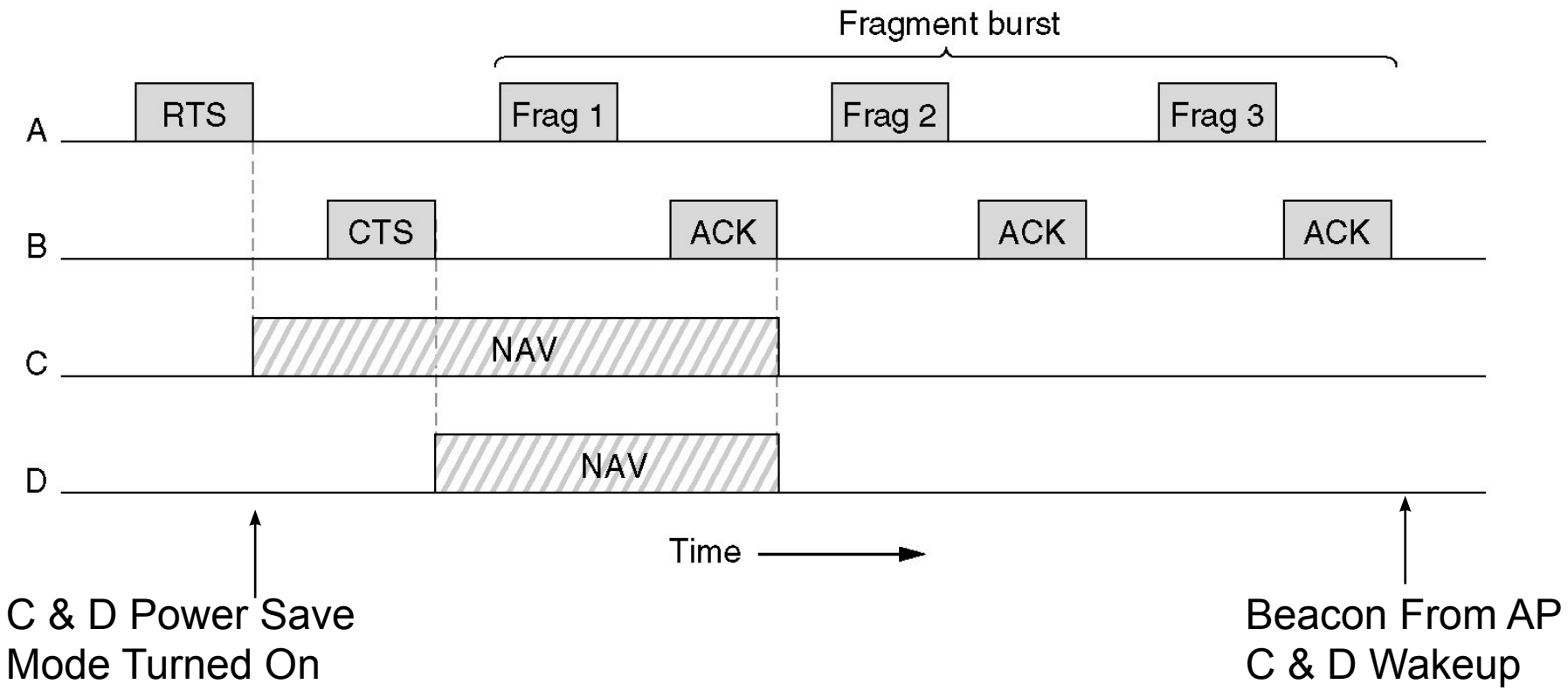
Assume B is transmitting to A at the same time that C wants to transmit to D. If C senses the medium, it will hear a transmission and falsely conclude that it may not send to D (shown as dashed line)

The 802.11 MAC Sublayer Protocol



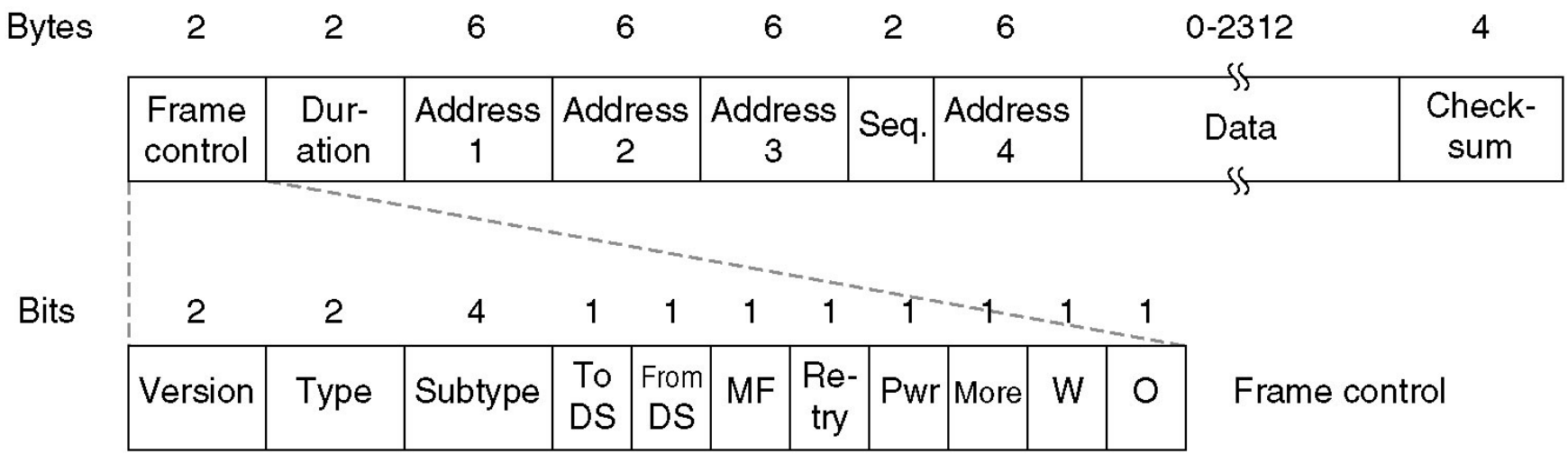
The use of virtual channel sensing using CSMA/CA.

The 802.11 MAC Sublayer Protocol



A fragment burst.

The 802.11 Frame Structure



The 802.11 data frame.

Frame Structure Detail

Frame Control:

Protocol Version

Type -> Data, Control, Management
Subtype -> e.g. RTS/CTS

To DS ->to Access Point

From DS -> from Access Point

More Frag. -> More fragments to follow

Retry -> Marks retransmission of a frame sent earlier

Pwr. Mgt.->sender going into power save mode

More data -> sender has more frames for the receiver

Protected -> frame body is encrypted

Order ->tells receiver sender that higher layers expects frames to be received in sequence

Frame Structure Detail

Duration:

> Microseconds of how long frame and its acknowledgment will occupy the channel. Used by stations to manage their NAV duration.

Address 1 -> Receiver

Address 2 -> Transmitter

Address 3 -> Distant endpoint

Sequence -> frame sequence number, used for error checking and recovery

Data -> Payload, The LLC PDU

Check Sequence -> 32-bit CRC

802.11 Services

802.11 Standard services that clients, APs and networks must conform to form a compliant wireless LAN:

Association:

Used by mobile stations to connect themselvs to APs

Reassociation:

Lets a station change its preferred AP

Disassociation:

Lets a station or AP orderly shutdown or leave the network

Authentication:

If network is open then anyone allowed to use it, otherwise credentials are needed to authenticate (next section)

Wireless Security

Why is Wireless security specifically more important than wired security?

Service Set IDentifier SSID:
- To advertise or not advertise?

Wired Equivalent Privacy (WEP):
- Uses a manually generated *key*
- 40-bit or 128-bit key
- Symentric key - dissemination

Extensible Authentication Protocol (EAP):
- Dynamic generatioin of WEP keys

Wireless Security

MAC Address Filtering:
- AP processes frames only from/to recognized MACs

Wi-Fi Protectred Access (WPA):
- Works like WEP or EAP
- Uses longer keys
- Key is altered for every frame to the client

IEEE 802.11i (aka WPA2):
- Uses EAP to obtain master key
- Client and AP use master key to obtain new key for duration of session