

Università di Roma Tor Vergata  
Corso di Laurea triennale in Informatica  
**Sistemi operativi e reti**  
A.A. 2021-2022

Pietro Frasca

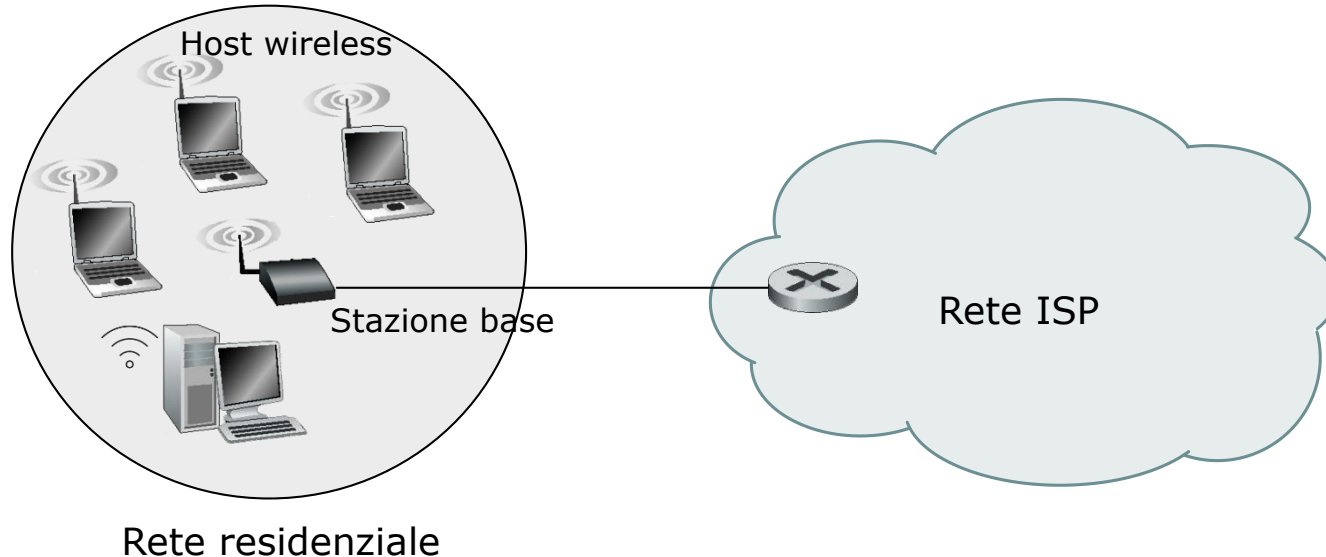
Parte II: Reti di calcolatori  
Lezione 24 (48)

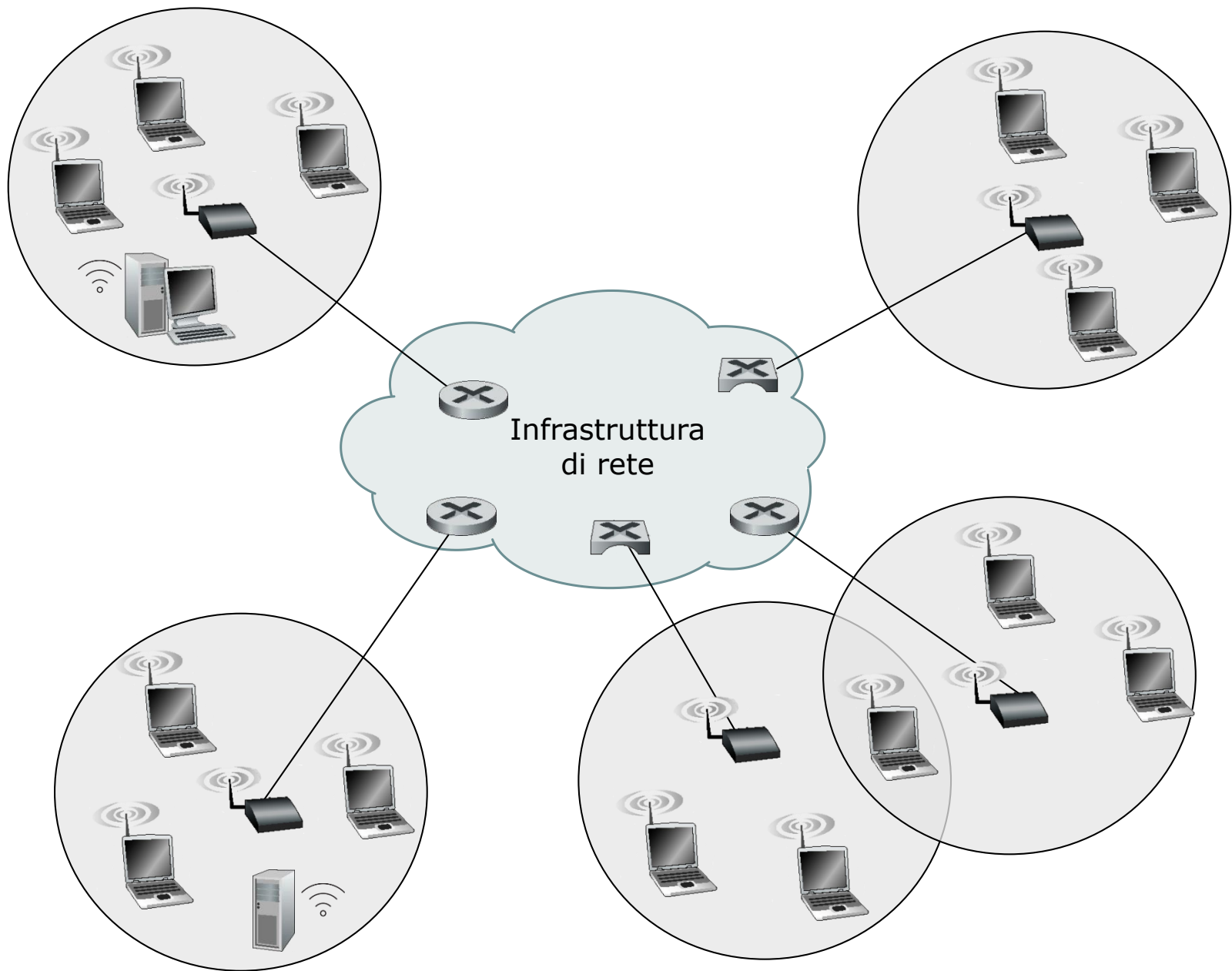
Martedì 31-05-2022

# Reti wireless

- Le reti wireless sono oggi una delle tecnologie più diffuse per l'accesso a Internet. Si trovano in vari tipi di ambiente come nelle case, posti pubblici, nelle università, in posti di lavoro, etc.
- Una rete wireless è costituita dai seguenti componenti:
  - **Host wireless.** Possono essere dispositivi di vario tipo come ad esempio PC, notebook, tablet, smartphone, smart TV. Gli host possono essere fissi o mobili.
  - **Collegamenti wireless.** Un host si connette alla stazione base o a un altro host attraverso un canale wireless. Attualmente, ci sono varie tecnologie wireless ciascuna caratterizzata da una diversa velocità di trasmissione e una massima distanza di copertura.
  - **Stazione base (access point).** Una stazione base provvede alla trasmissione e alla ricezione dei pacchetti che gli host ad essa associati trasmettono e ricevono. Un host per trasmettere in una rete wireless deve essere "**associato**" a una stazione base.

- La stazione base è connessa a una rete, per esempio ad una rete residenziale o a una rete ethernet cablata aziendale e funziona quindi come ripetitore tra gli host wireless ad essa associati e la rete fissa. Nelle reti domestiche gli access point (AP), gli switch e la tecnologia NAT sono inclusi nel modem DSL.
- Gli host associati a un AP, funzionano come gli host connessi con cavi a una rete ethernet cablata, in quanto tutti i servizi di rete come l'assegnazione degli indirizzi e l'instradamento, sono forniti dalla rete cui lo AP è connesso.

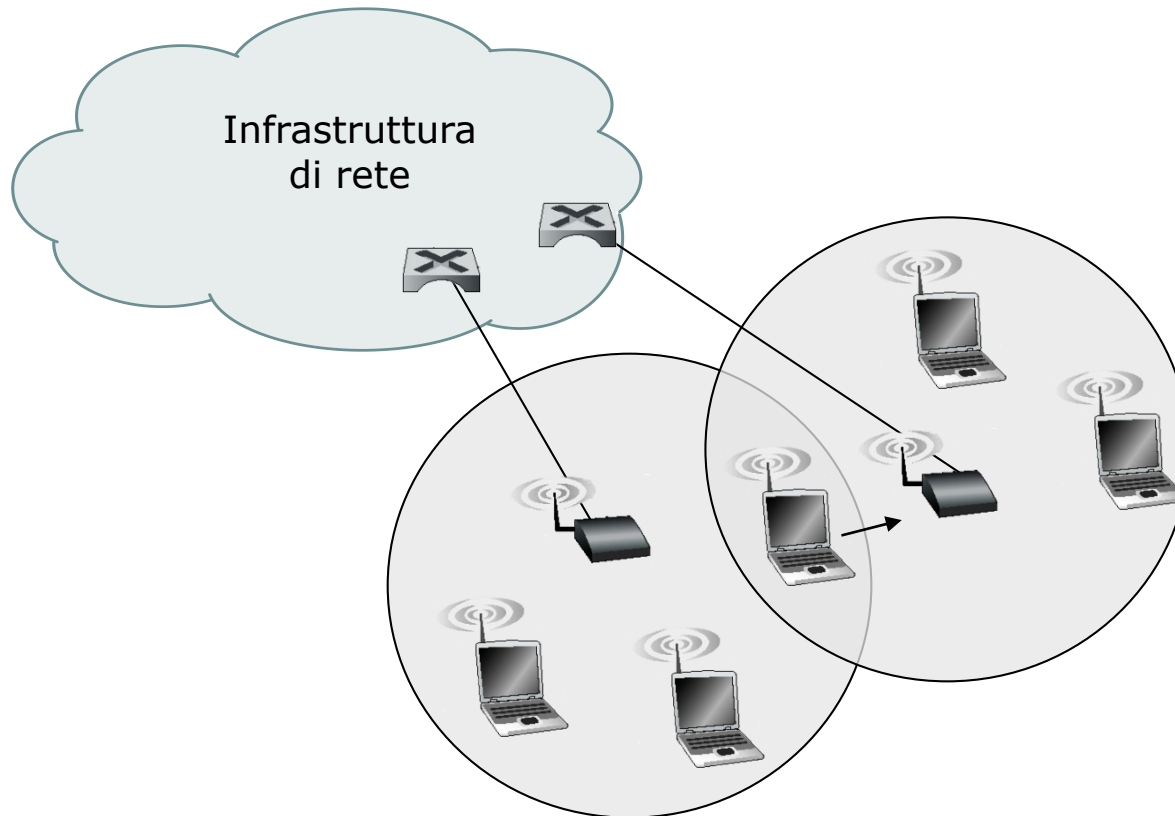




- Le **reti ad hoc**, sono reti wireless nelle quali gli host non hanno un'infrastruttura a cui connettersi. Pertanto, gli stessi host devono provvedere a tutti i servizi di rete necessari per la comunicazione, compresi i servizi d'instradamento e di assegnazione degli indirizzi.



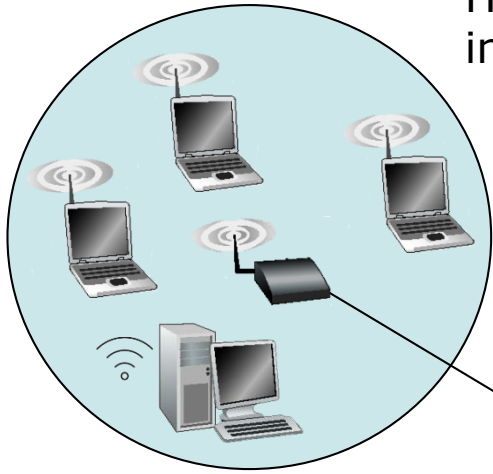
Quando un host si sposta dall'area di copertura di una stazione base a un'altra, cambierà il suo punto di collegamento con la rete globale. Questo processo è chiamato **handoff**.



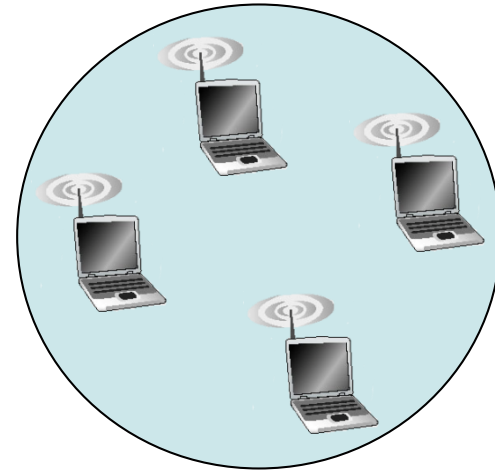
- **Infrastruttura di rete.** E' la rete più ampia con la quale l'host wireless potrebbe volersi connettere.

- Le componenti di una rete wireless, possono essere combinate in vari modi, formando diverse tipologie di rete.
  - **Hop singolo, con infrastruttura.** Queste reti hanno una stazione base che si collega a una rete cablata, ad esempio una LAN la quale è connessa a Internet. Inoltre, tutte le comunicazioni sono tra la stazione base e gli host su un singolo hop wireless. Un esempio è la rete 802.11 (wi-fi).
  - **Hop singolo, senza infrastruttura.** Manca la stazione base. Tuttavia, uno dei nodi di questa rete può coordinare la trasmissione degli altri nodi. Un esempio di questa classe sono le reti Bluetooth e 802.11 in modalità ad hoc.
  - **Hop multipli, con infrastruttura.** È presente una stazione base, collegata ad una LAN. Tuttavia, alcuni nodi potrebbero comunicare con altri nodi wireless, per raggiungere la stazione base.
  - **Reti a hop multipli e senza infrastruttura** non c'è un AP. I nodi possono dover ritrasmettere i messaggi a parecchi altri nodi per raggiungere la destinazione. I nodi possono anche essere mobili e la connettività tra loro può cambiare, come in una classe di reti nota come **rete mobile ad hoc**.

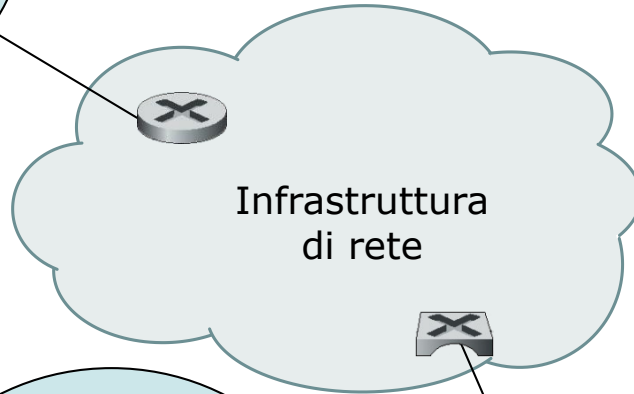
Hop singolo con  
infrastruttura



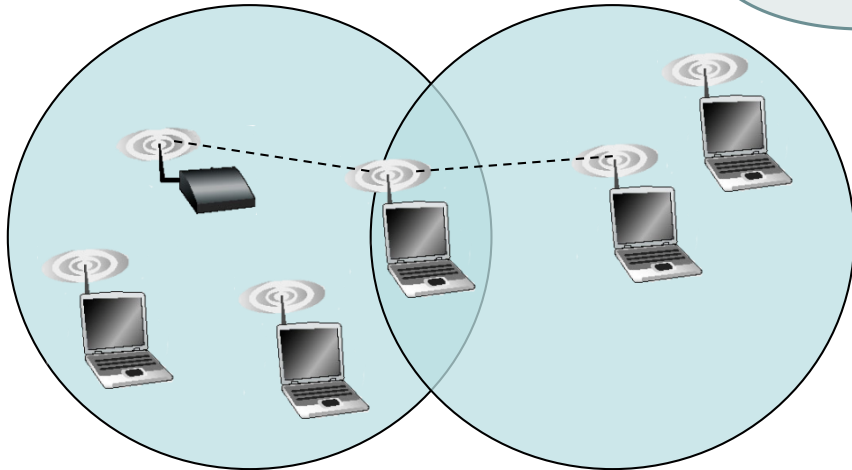
Rete ad hoc



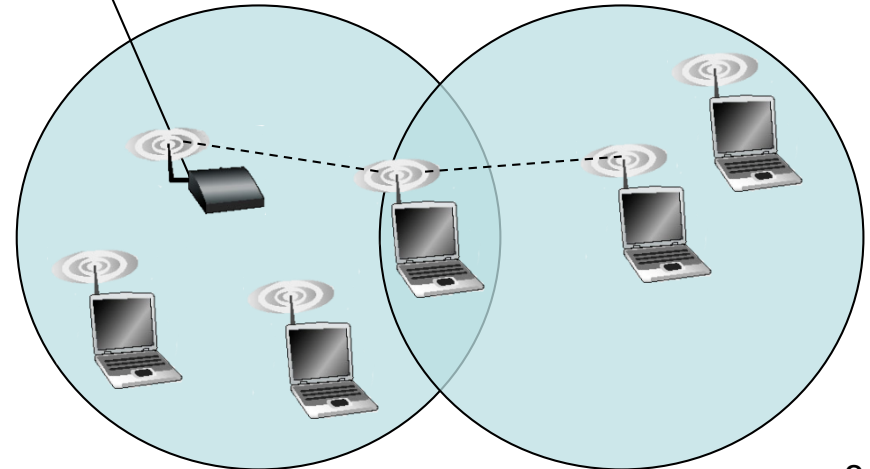
Infrastruttura  
di rete



Hop multipli senza  
infrastruttura



Hop multipli con  
infrastruttura





# Collegamenti wireless e caratteristiche di rete

- Descriviamo le più importanti caratteristiche delle reti wireless.
  - **Attenuazione del segnale.** Le onde elettromagnetiche si attenuano quando incontrano ostacoli come le pareti degli ambienti, oggetti di vario tipo e anche persone in movimento. Tuttavia, anche in mancanza di ostacoli, l'intensità del segnale diminuisce al crescere della distanza percorsa.
  - **Interferenze da parte di altre sorgenti.** Dispositivi elettronici di vario tipo che trasmettono nella stessa banda di frequenza interferiscono tra loro. Per esempio, i telefoni a 2,4 GHz e le LAN 802.11 (wi-fi) trasmettono nella stessa banda di frequenze e quindi, se usati contemporaneamente, possono interferire producendo errori nella trasmissione. Inoltre il rumore elettromagnetico ambientale, come ad esempio, le onde elettromagnetiche prodotte da un motore o di un forno a microonde, può generare interferenze.
  - **Propagazione su più cammini.** La propagazione su più cammini si verifica quando una parte delle onde elettromagnetiche trasmesse riflettendosi su oggetti, pareti,

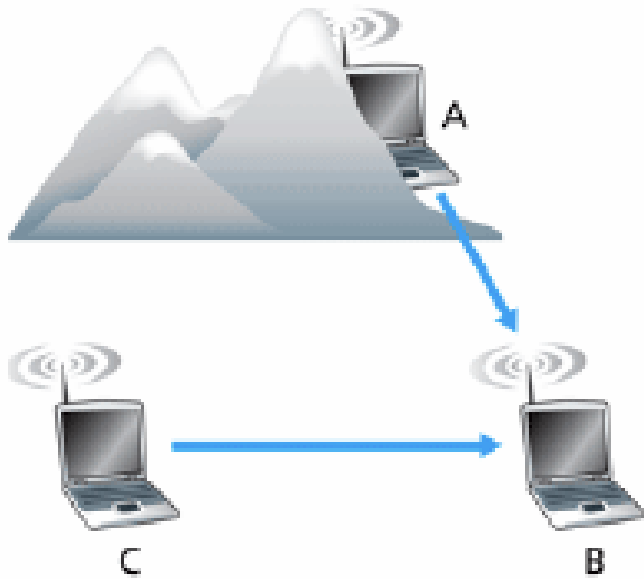
- pavimenti, persone in movimento, etc. seguono poi percorsi multipli di diversa distanza tra il trasmittente e il ricevitore. Questo fenomeno genera una miscelazione dei segnali multipli che fornisce un segnale risultante degradato che giunge al nodo ricevente.
- Da quanto descritto, è evidente che gli errori di trasmissione saranno più frequenti nelle reti wireless che nelle reti cablate.
- Pertanto, nelle reti wireless, a livello di collegamento, oltre alla rilevazione degli errori CRC, si utilizzano protocolli di **trasferimento affidabile**.
- In generale, i nodi wireless ricevono un segnale elettromagnetico distorto dovuto alla miscelazione del segnale trasmesso dal mittente e un rumore di fondo dell'ambiente. Il **rapporto segnale rumore (SNR, *signal to noise ratio*)** è una misura che esprime il rapporto tra l'ampiezza del segnale utile ricevuto e l'intensità del rumore.
- L'SNR si esprime in **Decibel (dB)**, che è definito come venti volte il logaritmo in base 10 del rapporto dell'ampiezza del

segnale ricevuto e l'ampiezza del rumore. Più è grande l'SNR migliore è la comunicazione.

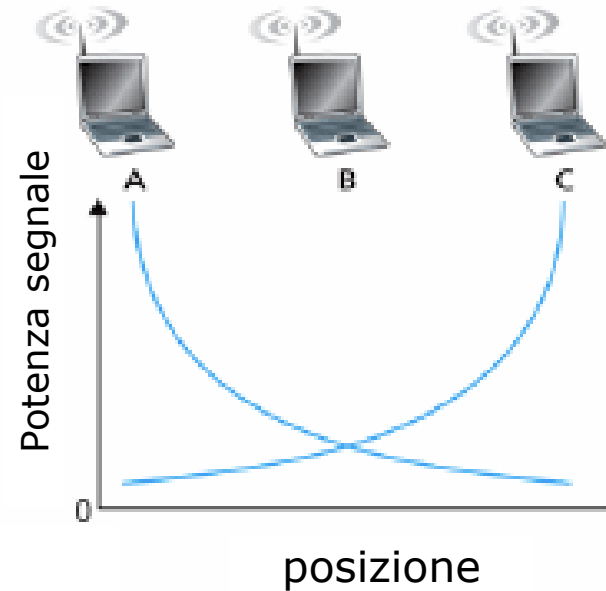
$$\mathbf{SNR = 20\log_{10}(S/N)}$$

- Un altro parametro, il **BER (bit error rate)** indica la probabilità che si verifichino errori di trasmissione.
- Il BER viene espresso in funzione dell'SNR, per diverse tecniche di modulazione, che vengono usate per codificare i dati per la trasmissione su un canale wireless ideale.
- Per un data tecnica di modulazione (ad esempio BSPK 1 Mbps, QAM16 4 Mbps, QAM256 8Mbps), **maggiore è SNR minore sarà il BER.**
- Poiché un host mittente può aumentare SNR aumentando la potenza di trasmissione, potrà anche diminuire, entro certi limiti, la probabilità che si verifichino errori nella trasmissione. Tuttavia aumentando la potenza di trasmissione, il mittente consuma più energia ed aumenta la probabilità che le trasmissioni possano interferire tra loro.

- SNR e BER possono cambiare a causa della mobilità o dei cambiamenti delle caratteristiche dell'ambiente.
- Modulazioni adattative sono usate nelle reti 802.11 (wi-fi), nelle reti 802.16 (Wi-Max) e nei sistemi dati cellulari. Questo consente di selezionare la tecnica di modulazione che fornisce la più alta velocità di trasmissione possibile senza superare una specifica soglia del BER.
- L'elevata quantità di errori non è l'unica differenza tra i collegamenti wireless e quelli cablati. Ricordiamo che, nel caso dei canali cablati condivisi, ciascun nodo riceve i frame trasmessi da tutti gli altri nodi. Nei collegamenti wireless, l'accesso multiplo è molto più complesso che nelle reti cablate a causa di problemi come il **terminale nascosto** e il **fading**.
- Per descrivere il problema del terminale nascosto consideriamo la figura seguente in cui supponiamo che gli host A e C stiano trasmettendo all'host C. Il **problema del terminale nascosto**, è dovuto alla presenza di ostacoli fisici nell'ambiente, come ad esempio, edifici, alberi, etc, che



- **Problema del terminale nascosto**
  - B, A possono comunicare
  - B, C possono comunicare
  - A, C non possono comunicare ma possono causare interferenza presso la destinazione B



- **Fading:**
  - B, A possono comunicare
  - B, C possono comunicare
  - A, C non possono comunicare ma causano interferenza presso B

potrebbero impedire ad A e a C di rilevare la trasmissione dell'altro, anche se le loro trasmissioni arrivano alla destinazione B. In questo caso si possono verificare collisioni non rilevate dai due host mittenti.

- Un'altra situazione nella quale si crea una collisione non rilevabile dalla stazione ricevente è quella in cui si verifica il **fading** (evanescenza) del segnale che si propaga nell'ambiente. La figura mostra il caso in cui A e C si trovano posizionati in modo tale che il loro segnale non è sufficientemente potente da essere rilevato a vicenda, ma le loro trasmissioni interferiscono con la stazione ricevente B.
- Questi problemi rendono l'accesso multiplo nelle reti wireless molto più complesso che nelle reti cablate.

# Wi-Fi (IEEE 802.11)

- Tra i vari standard delle reti LAN wireless, lo standard **IEEE 802.11** wireless LAN, detto anche **Wi-Fi** è uno degli standard più diffusi per l'accesso a Internet.
- Lo standard 802.11, nato negli anni '90, ha diverse varianti, tra cui 802.11 a, b, g, n e ac. Attualmente sono disponibili adattatori wireless con tripla (*802.11 b/g/n*) o *quadrupla* (*802.11 b/g/n/ac*) modalità.
- Tutti gli standard 802.11 hanno in comune diverse caratteristiche. Utilizzano lo stesso protocollo di accesso al mezzo, **CSMA/CA**, e la stessa struttura del frame a livello di collegamento.
- Ciascuno di questi standard può ridurre la velocità di trasmissione per raggiungere distanze maggiori e può funzionare sia in modalità infrastruttura sia in modalità ad hoc.
- Tuttavia, questi standard presentano considerevoli differenze a livello fisico.

- Lo standard 802.11b ha una velocità di trasferimento di 11 Mbps mentre 802.11g raggiunge i 54 Mbps. Lo standard l'802.11n usa antenne a più ingressi e più uscite (MIMO, *multiple-input multiple-output*) cioè più antenne sul lato di trasmissione e due o più antenne sul lato ricevente che trasmettono/ricevono segnali diversi. Tale standard può raggiungere un throughput di 450 Mbps. Il più recente standard 802,11ac (2014) può arrivare a un throughput di 1300 Mbps. Gli standard 802.11b/g usano onde elettromagnetiche con portanti aventi frequenze nello spettro dei 2,4 GHz; 802.11n opera nello spettro di frequenze dei 2.4 e 5 Ghz, mentre 802.11ac funziona solo nello spettro di frequenze di 5 GHz.

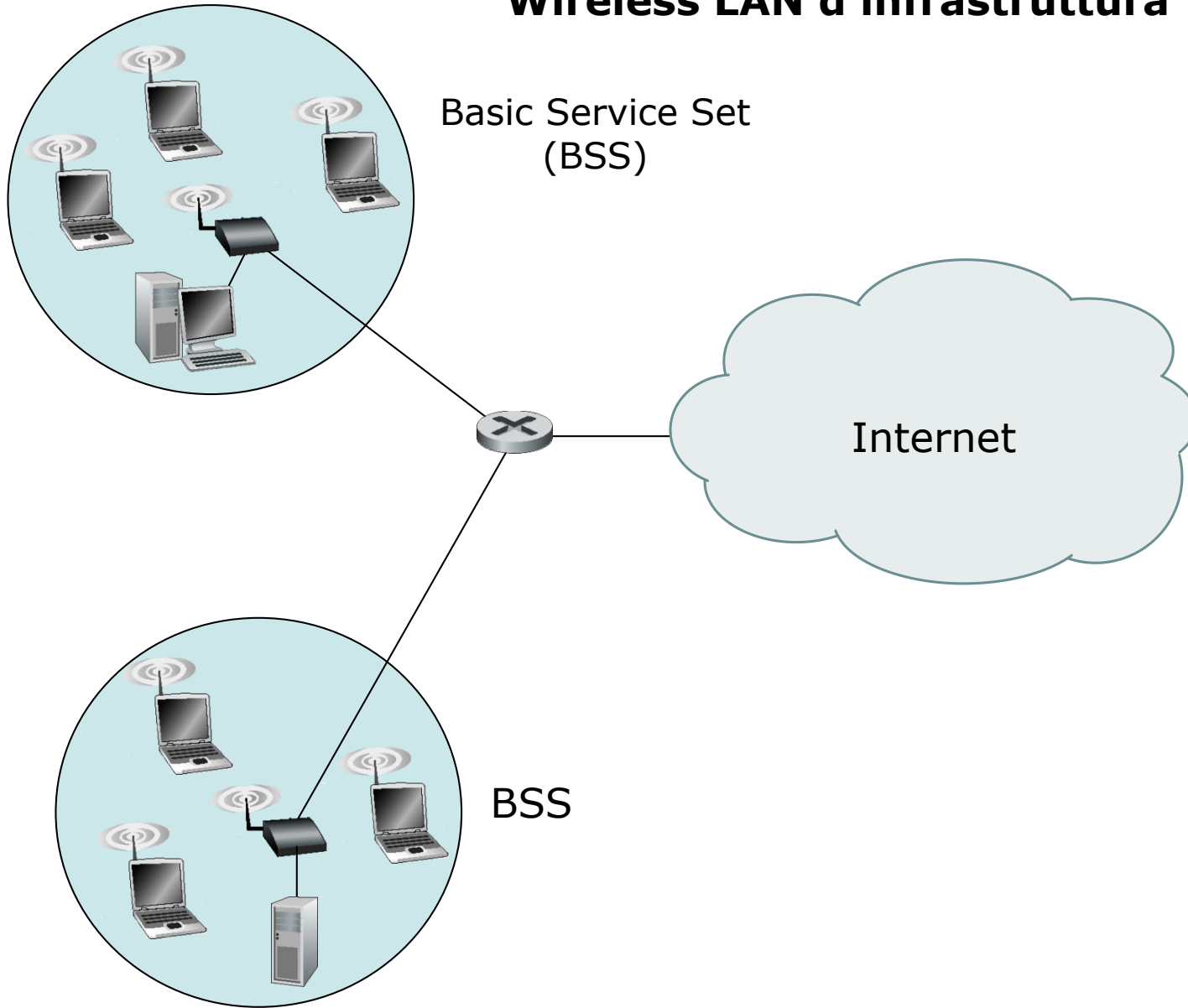
Standard	Portanti (GHz)	Velocità trasmissione max (Mbps)
802.11b	2,4	11
802.11g	2,4	54
802.11n	2,5 e 5	450
802.11ac	5	1300



# Architettura 802.11

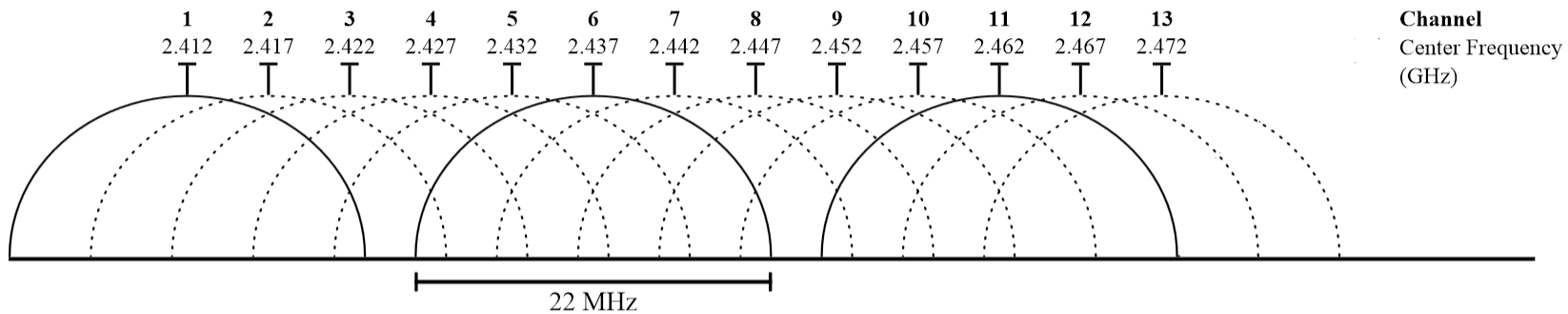
- L'architettura dello standard 802.11, è basata sul **BSS** (***basic service set, set di servizio base***), costituito da uno o più host wireless e un **AP** (***Access point, punto di accesso***).
- Una tipica rete residenziale, è costituita da un AP uno switch e un router NAT, assemblati nello stesso dispositivo, che connettono gli host a Internet.
- Come per Ethernet, anche le schede di rete wireless e gli AP hanno **indirizzi MAC di 6 byte**.
- Come già descritto, le reti wireless che utilizzano **AP** sono anche chiamate **wireless LAN d'infrastruttura**, dove "l'infrastruttura" è formata dagli AP, dalla rete Ethernet che li collega, e da un router.

# Wireless LAN d'infrastruttura

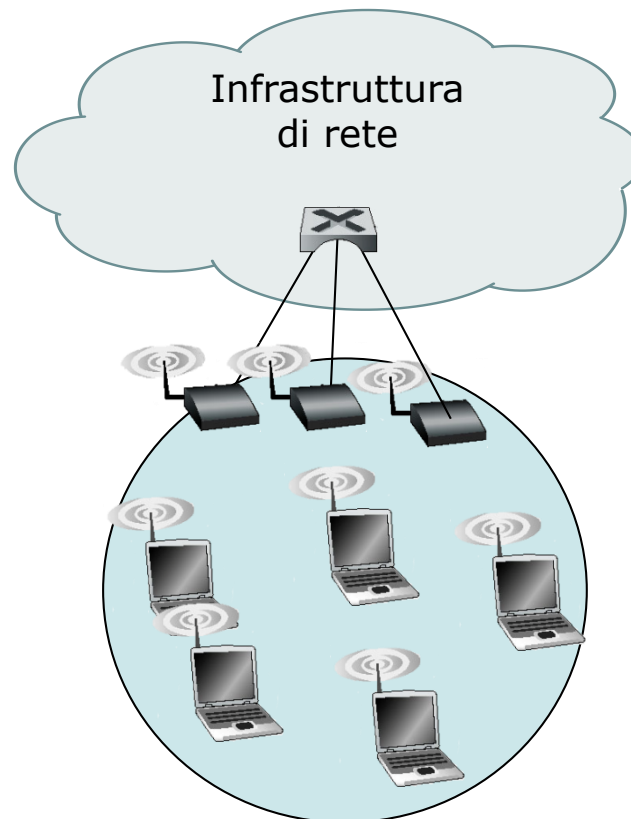


# Canali e associazioni

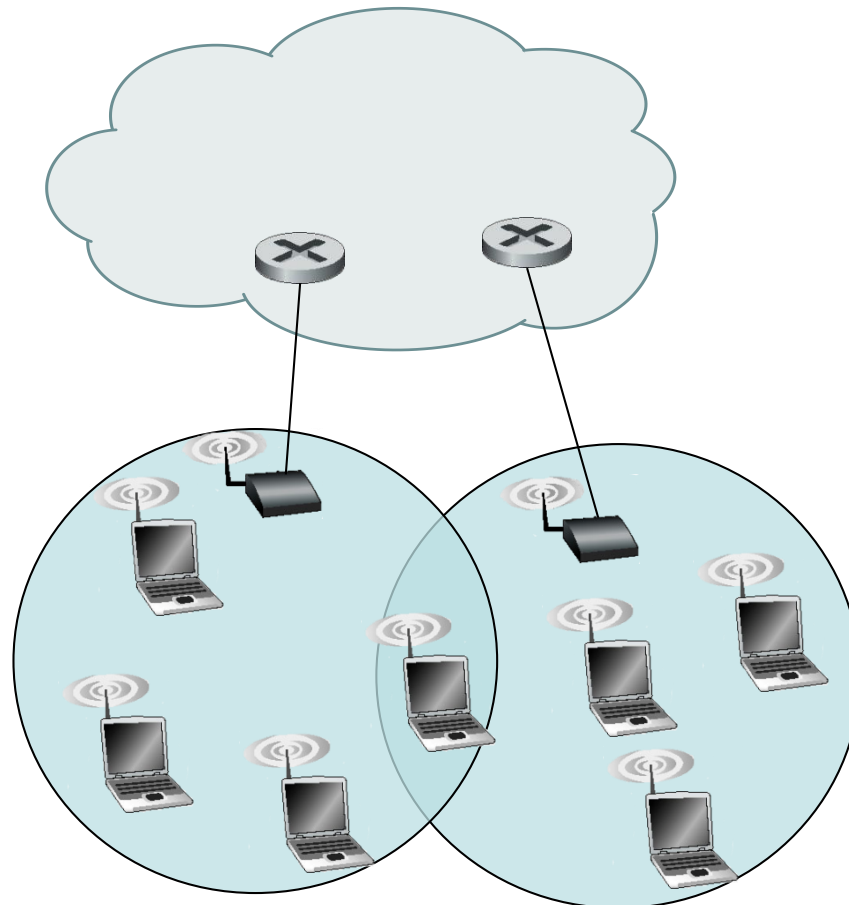
- Per poter comunicare, gli host devono prima associarsi a un AP.
- Quando si installa un AP, generalmente si assegna ad esso un identificativo detto **SSID** (*service set identifier*).
- Oltre al SSID è necessario scegliere per l'AP un **numero di canale**. Un numero di canale corrisponde, per 802.11 b/g/n, ad una specifica frequenza compresa nella banda compresa tra **2,4 GHz e 2,485 GHz**. In questa larghezza di banda di **85 MHz**, sono definiti, in Italia, **13 canali** (11 negli USA) parzialmente sovrapposti. Ciascun canale occupa una banda di 22 MHz.
- Generalmente l'AP seleziona automaticamente il canale che fornisce le migliori prestazioni.
- Due canali non si sovrappongono solo se sono separati da 4 o più canali. Pertanto, al massimo ci sono 3 canali che non si sovrappongono, ad esempio i canali 1, 6 e 11.



- Questo significa che è possibile creare una wireless LAN con un throughput trasmissivo totale di 3 volte la massima velocità di trasmissione consentita. Ad esempio installando tre AP 802.11n nello stesso luogo, e assegnando i canali 1, 6 e 11 agli AP e connettendoli con uno switch si ottiene un throughput trasmissivo totale di  $3 \times 450 = 1350$  Mbps (supponendo che il throughput di 802,11 n sia di 450 Mbps).



- A volte può capitare che in una zona un host mobile, come un portatile o uno smartphone, riceva un segnale sufficientemente intenso da due o più AP. Ciascuno di questi punti d'accesso potrebbe appartenere a una diversa sottorete.



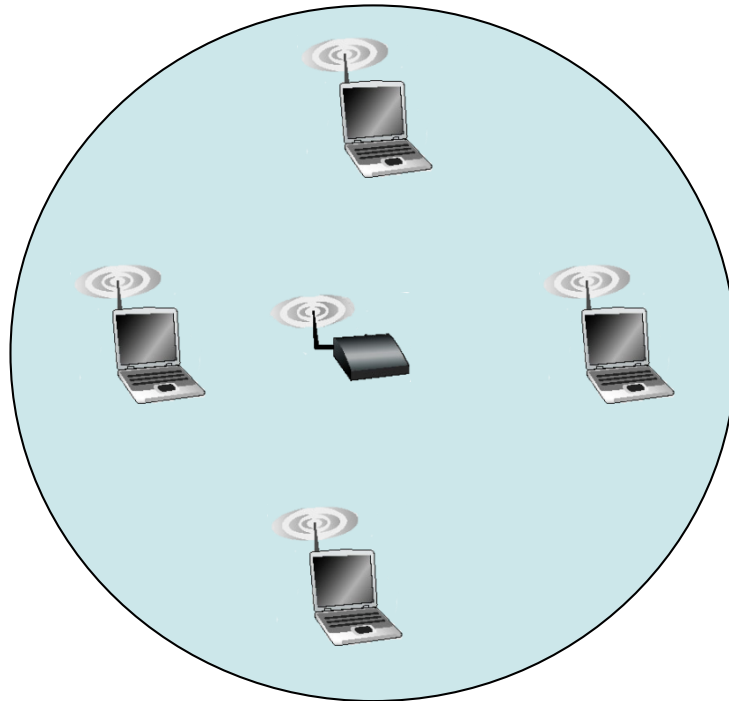
- Supponiamo che un host si trovi in una zona coperta da più AP.
- Per connettersi ad Internet, l'host deve associarsi a un unico AP e quindi accedere ad una subnet.
- L'host wireless può associarsi a un AP in due modalità dette **scansione passiva** e **scansione attiva**.
- La **scansione passiva** funziona nel seguente modo:
  - L'AP invia periodicamente dei piccoli frame detti frame **beacon**, che contengono il proprio **SSID** e il proprio **indirizzo MAC** e altre informazioni. L'host scansiona i 13 (o 11) canali in cerca di questi frame beacon provenienti dagli AP situati nelle vicinanze. Alcuni AP potrebbero trasmettere sullo stesso canale.
  - Ricevuti i beacon di vari AP l'host si associa ad uno di essi.
- Lo standard 802.11 non specifica un algoritmo per selezionare l'AP con il quale associarsi. L'algoritmo è scelto dai progettisti firmware e software della scheda di rete 802.11.

- Generalmente, si usa un algoritmo con il quale la scheda di rete sceglie l'AP i cui frame beacon sono ricevuti con la potenza di segnale più alta. Tuttavia, selezionare un AP solo in base alla potenza del segnale non sempre è la scelta migliore.
- Infatti, è possibile che l'AP selezionato abbia un segnale forte, ma che sia sovraccarico per via di molti host associati che dovranno condividere il canale di quell'AP, mentre un AP potrebbe avere associati pochi host perché non è selezionato a causa di un segnale leggermente più basso.
- Recentemente sono stati proposti parecchi metodi alternativi per selezionare gli AP.
- Con l'altra procedura, la **scansione attiva**, un host per associarsi ad un AP esegue le seguenti operazioni:
  - invia in broadcast un **frame sonda di richiesta** che sarà ricevuto da tutti gli AP raggiungibili dall'host. L'AP risponde al frame sonda di richiesta con un **frame sonda di risposta**. L'host può quindi scegliere l'AP con il quale associarsi tra quelli che hanno risposto.



- Dopo aver individuato l'AP con il quale associarsi, l'host invia un **frame di richiesta di associazione** all'AP, il quale risponde con un **frame di risposta di associazione**.
- Una volta associato con un AP, l'host si conetterà a una sottorete alla quale appartiene l'AP.
- In genere, quindi l'host utilizza DHCP per ottenere un indirizzo IP su quella sottorete.
- Per creare un'associazione con un particolare AP, all'host generalmente è richiesto di autenticarsi. Le reti 802.11 forniscono diverse soluzioni per l'autenticazione (WPA-PSK (Wifi Protected Access-Pre-Shared Key, WPA2-PSK (Wifi Protected Access 2-Pre-Shared Key), etc.).

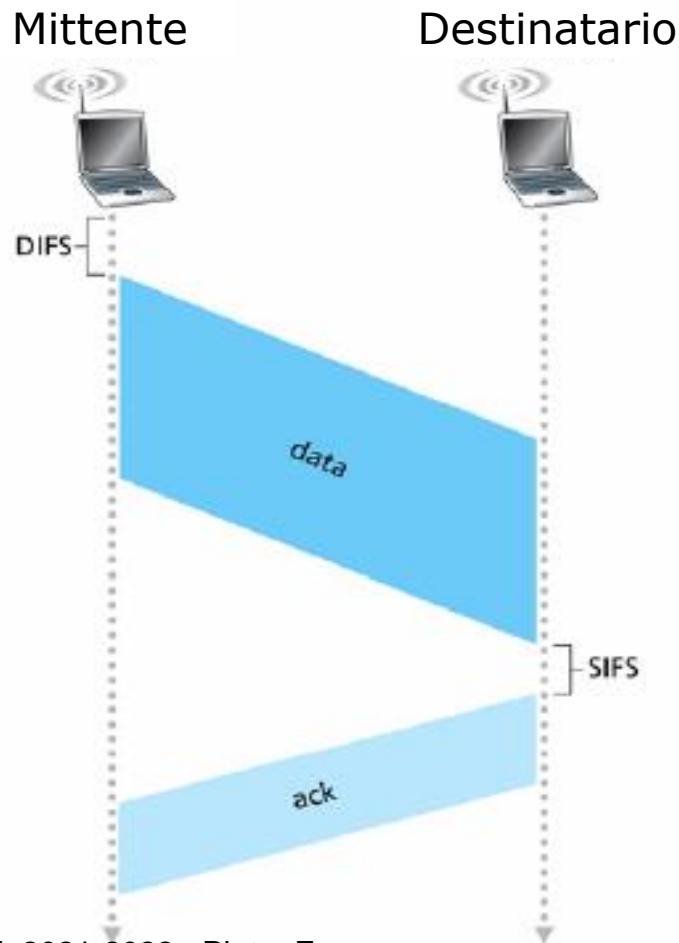
- Una volta che un host è associato a un AP, può iniziare a trasmettere. Ma, poiché più host potrebbero voler trasmettere frame nello stesso momento sullo stesso canale, è necessario un **protocollo ad accesso multiplo** per coordinare le trasmissioni.



- Il protocollo usato è il **CSMA/CA** (***Carrier Sense Multiple Access / Collision avoidance***, **accesso multiplo con rilevazione della portante/collisioni evitate**).
- Come il CSMA/CD di Ethernet anche il CSMA/CA richiede che ogni stazione ascolti prima di trasmettere e non trasmette se rileva che il canale è occupato. A differenza di Ethernet, wi-fi utilizza una variante del CSMA in grado di evitare quanto più possibile il verificarsi delle collisioni.
- Ricordiamo che un frame inviato da un host in una rete wireless potrebbe non raggiungere l'host destinatario per vari motivi. Pertanto, IEEE 802.11 fornisce un servizio di trasmissione affidabile a livello di collegamento.

- Col protocollo CSMA/CA, un host **mittente** quando vuole trasmettere un frame segue i seguenti passi:
  1. Se il canale è libero, allora trasmette il frame dopo un breve periodo di tempo casuale detto **DIFS** (***distributed inter-frame space, spazio distribuito di inter-frame***).
  2. Altrimenti, se il canale è occupato, attende un ritardo casuale prima di trasmettere. In particolare, per il calcolo di questo ritardo, usa una variabile di tipo contatore a cui assegna un valore casuale intero che esprime il numero di volte che il mittente deve trovare il canale libero prima di trasmettere. Il contatore è decrementato se il canale è trovato libero. Se il canale è occupato, il valore del contatore non varia.
  3. Quando il contatore giunge al valore zero, e questo può verificarsi soltanto quando il canale è libero, l'host mittente trasmette il frame e aspetta il **frame di riscontro (ACK)**.
  4. Se riceve l'**ACK**, il mittente se ha un altro frame da inviare, riattiverà il protocollo *CSMA/CA* dal passo 2.

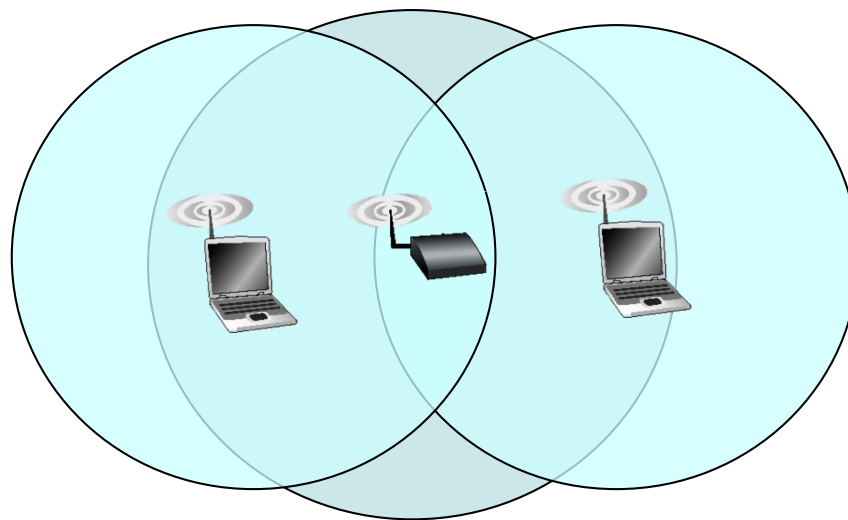
- Quando l'host **destinatario** riceve un frame esegue il controllo CRC e se corretto, attende per un breve periodo di tempo, detto **SIFS** (**short inter-frame space, breve spazio inter-frame**), dopo il quale invia al mittente un frame di riscontro di avvenuta ricezione.



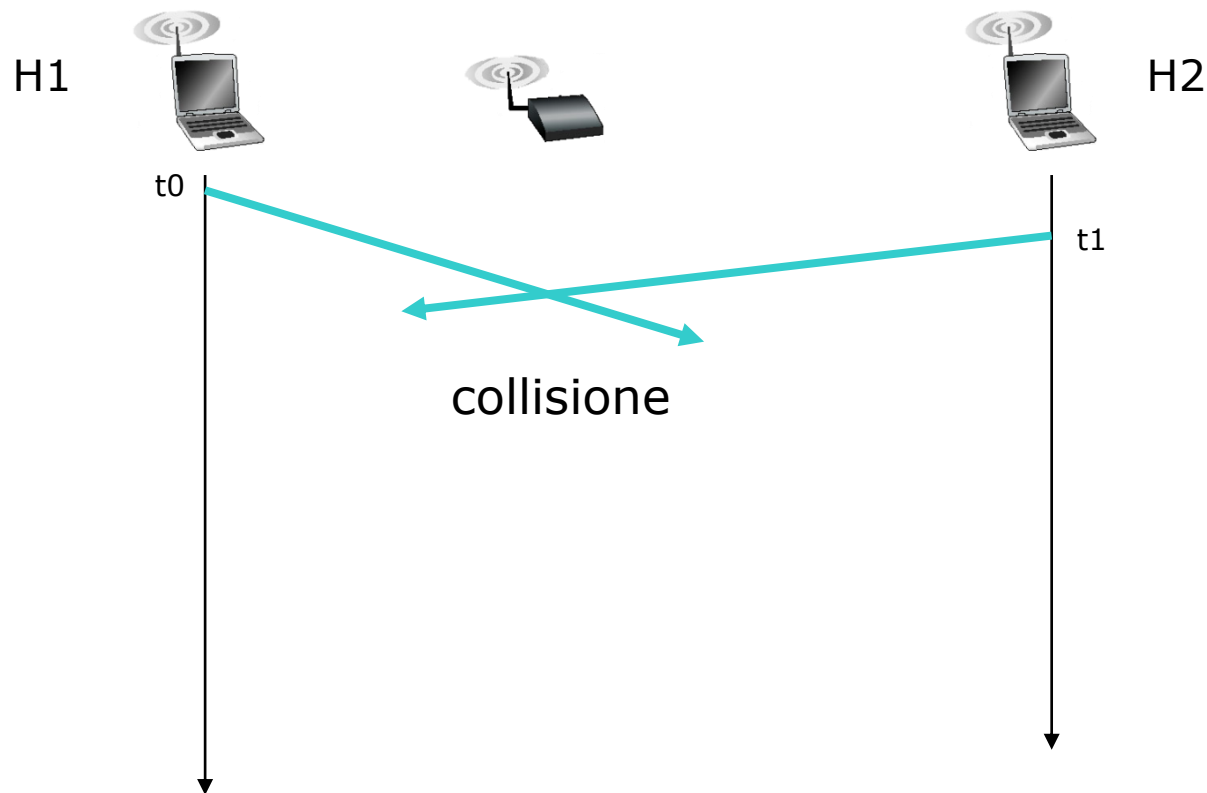
- Se l'host mittente non riceverà questo riscontro entro un intervallo di tempo stabilito (timeout), ritrasmetterà il frame. Il mittente ritorna al passo 2 incrementando il valore del ritardo.
- Se il frame di riscontro non sarà ricevuto dopo un numero prefissato di ritrasmissioni, l'host mittente scarperà il frame corrente e passerà alla trasmissione del frame successivo.
- Con il CSMA/CD un mittente inizia a trasmettere appena rileva che il canale è libero. Con **CSMA/CA** invece, il mittente trasmette dopo che **ha verificato più volte** che il canale è libero. Questo comportamento più prudente ha l'obiettivo di evitare quanto più possibile le collisioni.
- Tuttavia, le collisioni possono verificarsi. Ad esempio due host potrebbero essere **nascosti**, o potrebbero trasmettere in istanti molto vicini tra loro in modo tale che la trasmissione del host che ha iniziato per primo non abbia ancora raggiunto l'altro host.

# Host nascosti: RTS e CTS

- Il protocollo MAC 802.11 dispone anche di un'opzionale funzionalità di **prenotazione della trasmissione** che aumenta la probabilità di evitare le collisioni anche in presenza di host nascosti.
- Nella figura seguente, due host wireless si trovano nel raggio dell'AP al quale sono associati, ma ciascuno degli host è nascosto all'altro.

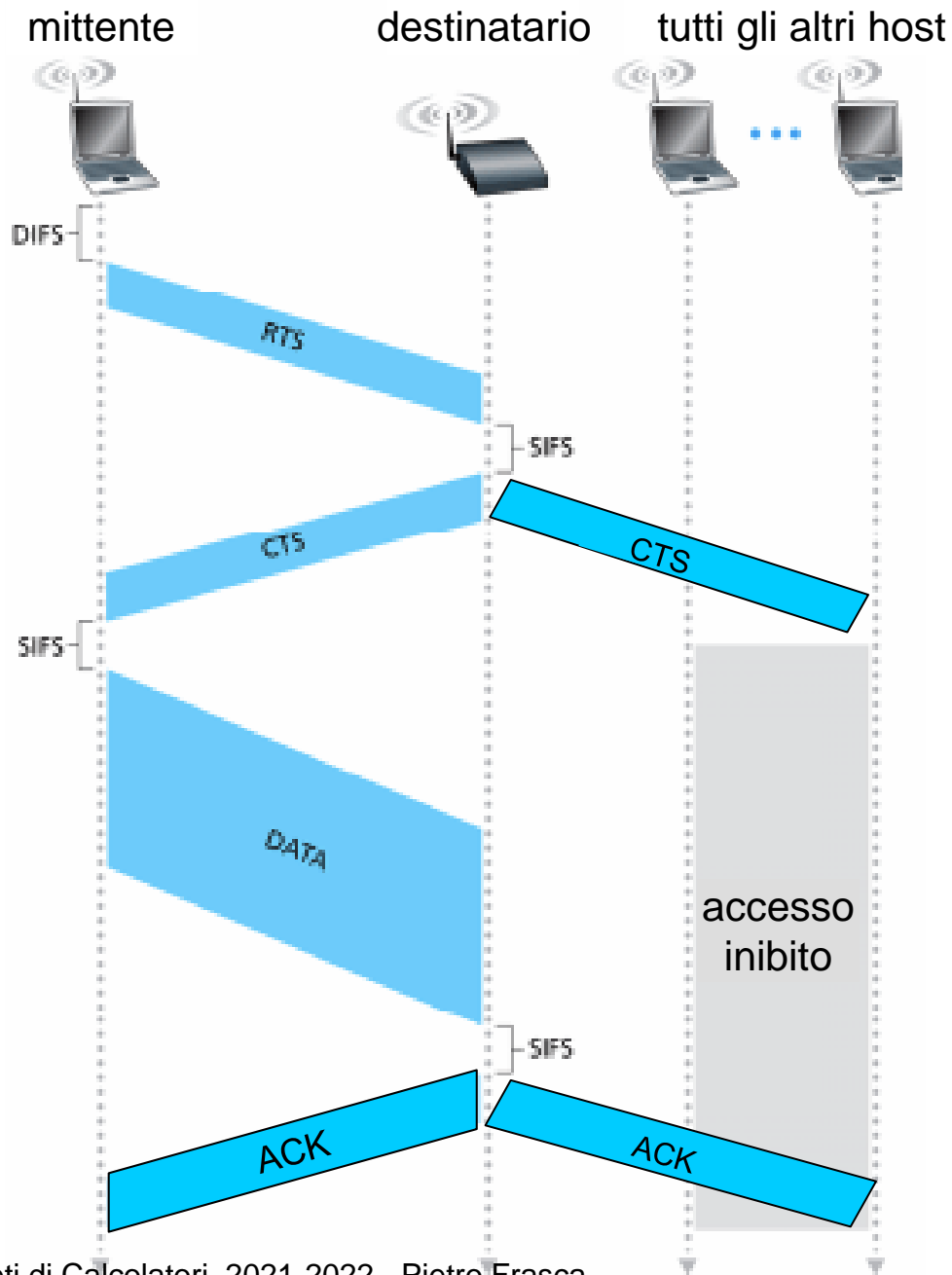


- Supponiamo che l'host H1, all'istante  $t_0$ , stia trasmettendo un frame e, subito dopo, all'istante  $t_1$ , H2 trasmetta un frame all'AP. H2, non rilevando la trasmissione di H1, attenderà un breve periodo di tempo casuale DIFS e poi trasmetterà il frame, causando la collisione.





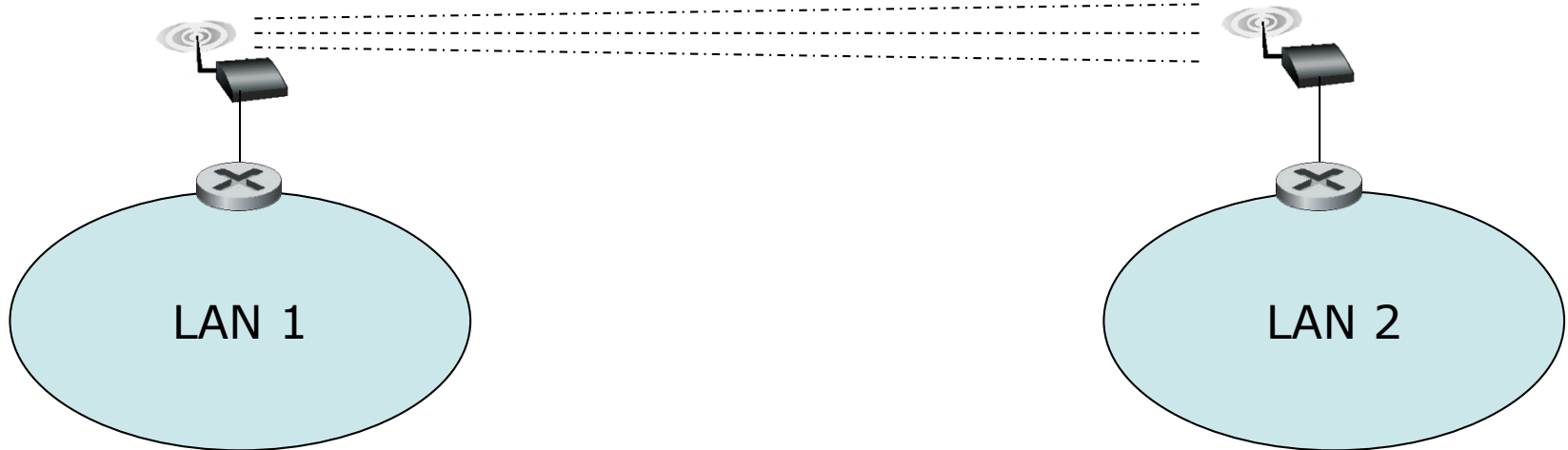
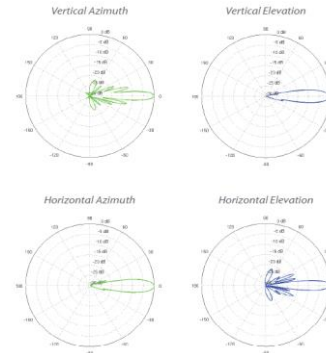
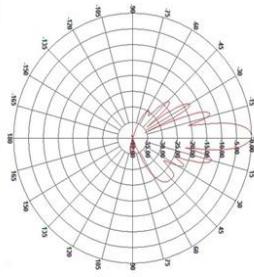
- Per evitare questo problema, il protocollo IEEE 802.11 utilizza due brevi frame di controllo:
  - **RTS** (*request to send, richiesta d'invio*) e
  - **CTS** (*clear to send, libero di spedire*) per riservare l'accesso al canale.
- Il mittente, quando vuole trasmettere, prima invia il frame **RTS** all'**AP**, indicando il **tempo totale** richiesto per trasmettere il **frame DATI** e il **frame ACK**.
- Quando l'**AP** riceve il frame **RTS** risponderà inviando in **broadcast** il frame **CTS**. Questo ha due scopi:
  - **abilitare il mittente alla trasmissione e**
  - **impedire alle altre stazioni la trasmissione durante il periodo di tempo prenotato.**



- L'uso dei frame RTS e CTS può incrementare le prestazioni per i seguenti motivi:
  - risolve il **problema dell'host nascosto**, in quanto il frame DATI viene trasmesso soltanto dopo che il canale è stato prenotato;
  - dato che i frame RTS e CTS sono piccoli, una eventuale collisione sarà di breve durata. Una volta che i frame di controllo sono stati trasmessi con successo, i successivi frame DATI e ACK dovrebbero essere trasmessi senza collisioni.
- Tuttavia, se da una parte lo scambio dei frame RTS e CTS riduce le collisioni, d'altra parte introduce ritardo e quindi diminuisce la larghezza di banda. Per questo motivo, questi frame sono utilizzati solamente per prenotare il canale per la trasmissione di **grandi frame**.
- In pratica, un host wireless può stabilire una **soglia RTS**, così che i frame di controllo RTS/CTS siano usati soltanto per i frame più grandi di questa soglia.

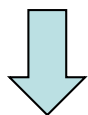
# Utilizzo di 802.11 per collegamenti punto-punto

- Usando AP con antenne direttive ad alto guadagno si potrebbe utilizzare il protocollo 802.11 per realizzare un collegamento wireless punto-punto economico, su distanze di decine di chilometri.



# Frame IEEE 802.11

- I frame 802.11 sono molto simili ai frame Ethernet, ma contengono campi specifici per l'utilizzo nei collegamenti wireless.



Intestazione del frame 802.11



Formato del campo **controllo frame**

## Campo dati (payload)

- Il campo dati, generalmente è un datagram o un messaggio ARP. Tipicamente ha una lunghezza inferiore ai 1500 byte ma può raggiungere i 2312 byte.

# Campo CRC

Il campo CRC di 32 bit permette al ricevente il rilevamento degli errori nei bit.

## Campi indirizzo

- Il frame 802.11 contiene quattro campi indirizzo MAC (invece di 2 di Ethernet).
- I primi tre campi indirizzo sono necessari a scopi d'interconnessione, il quarto campo indirizzo è usato nelle reti ad hoc, ma non in quelle d'infrastruttura. I campi sono definiti nel modo seguente:
  - **L'indirizzo MAC 1** è l'indirizzo MAC del **destinatario**. Se il mittente è un host wireless, questo campo conterrà il MAC dell'AP di destinazione. Se il mittente è l'AP che trasmette, questo campo conterrà l'indirizzo MAC dell'host wireless di destinazione.

- **L'indirizzo 2** è l'indirizzo MAC del **mittente**. Quindi, se l'host wireless trasmette il frame, viene inserito in questo campo il suo indirizzo. Se invece è l'AP a trasmettere, in questo campo si inserirà l'indirizzo MAC dell'AP.
- **L'indirizzo 3** contiene l'indirizzo MAC dell'interfaccia del router alla quale l'AP è connesso.

# Campi numero di sequenza, durata e controllo del pacchetto

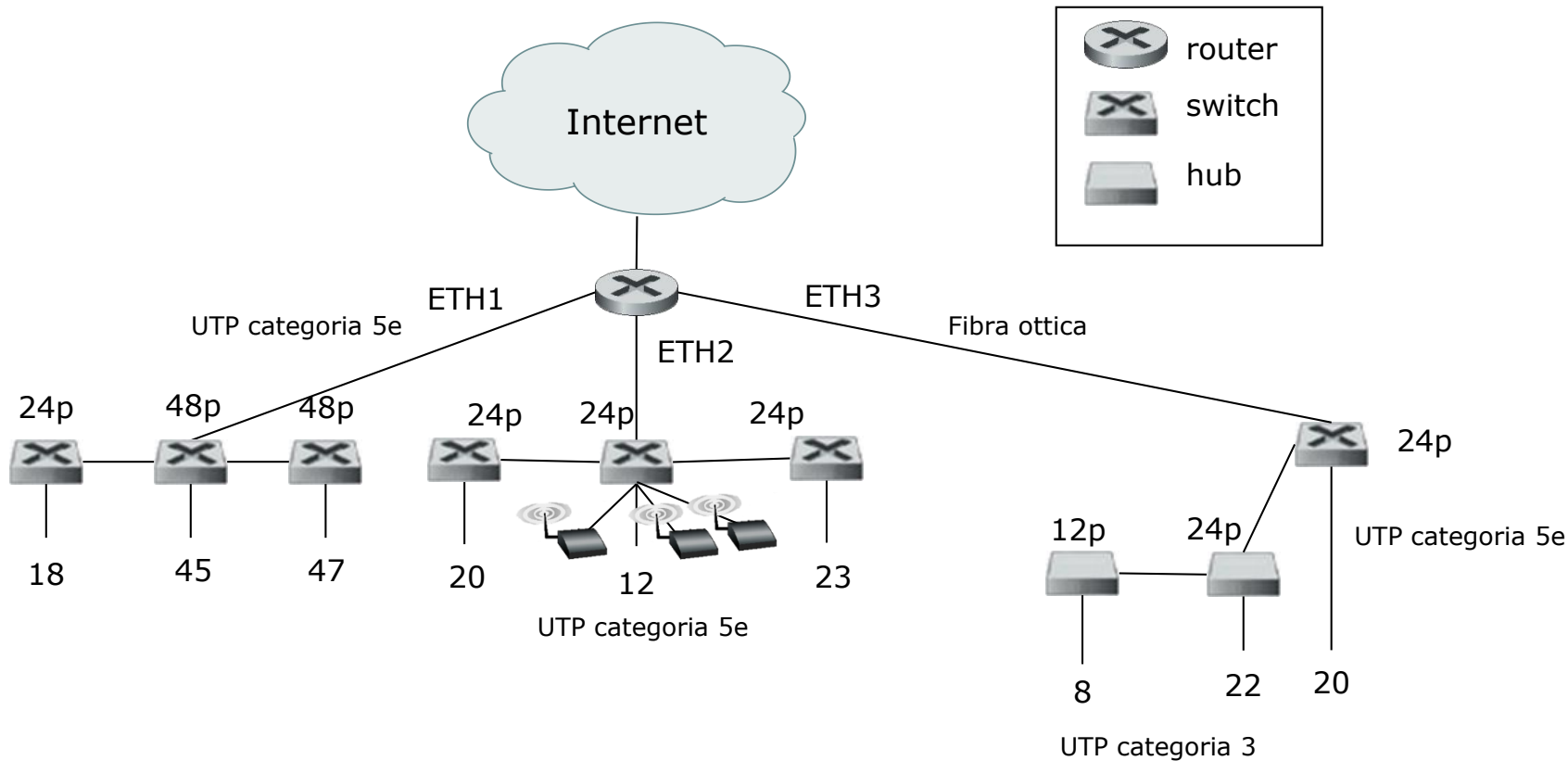
- Ricordiamo che ogni volta che una stazione wi-fi riceve correttamente un frame da un'altra stazione, invia al mittente un frame ACK per confermare l'avvenuta ricezione. Poiché, questo frame di conferma può perdersi, la stazione trasmittente potrebbe inviare più copie dello stesso frame. Come abbiamo già visto per il TCP, i numeri di sequenza consentono all'host ricevente di distinguere tra un frame appena trasmesso e la ritrasmissione di un frame. Il campo **numero di sequenza** nel frame 802.11 ha la stessa funzione di quello a livello di trasporto.
- Ricordiamo che 802.11 permette al nodo trasmittente di riservare il canale per un intervallo di tempo che comprende il tempo necessario per trasmissione del suo frame dati e quello del frame di riscontro. Questo valore è posto nel campo **durata** (per i frame dati, per RTS e per CFS).



- Il **campo di controllo** è costituito da vari campi. I campi **tipo e sottotipo** sono utilizzati per distinguere il tipo di frame, come ad esempio richiesta d'associazione, RTS, CTS, ACK e frame dati. I campi **to DS** (verso AP) e **from DS** (da AP) definiscono la funzione dei diversi campi indirizzo. Il significato di questi cambia a seconda che sia utilizzata una rete ad hoc o d'infrastruttura e, in quest'ultimo caso, è inviato da una stazione o da un punto d'accesso.
- Infine, il campo WEP specifica un' eventuale cifratura dei dati.

# Esempio di progettazione di una LAN

- In un'azienda privata deve essere installata una rete costituita da tre LAN Ethernet 100/1000baseT, indicate con i nomi ETH1, ETH2 e ETH3. Le prime due LAN ETH1 e ETH2 devono essere cablate all'interno di uno stesso edificio mentre la LAN ETH3 deve essere installata in un altro edificio, a distanza di 800 metri dal primo. All'azienda è stato assegnato il blocco di indirizzi 200.70.40.0/24 (formato CIDR). Le LAN devono essere strutturate in modo tale che a ETH1 siano connessi un massimo di 110 host, a ETH2 un massimo di 55 host e a ETH3 un massimo di 50 host di cui 30 devono avere adattatori a 10Mbps e appartenere ad uno stesso dominio di collisione, e gli altri 20 devono avere adattatori a 100Mbps e funzionare in full-duplex. Tutti i computer dell'azienda devono avere la connessione ad internet. Inoltre, a ETH2 deve essere connessa una rete wi-fi con throughput trasmissivo totale di almeno 1 Gbps.
- *A)* Disegnate uno schema della rete descritta, indicando i dispositivi di interconnessione e i tipi di mezzi trasmissivi utilizzati.
- *B)* Indicate l'indirizzo IP, la netmask e l'indirizzo di broadcast per ciascuna sottorete.
- *C)* assegnate gli indirizzi IP alle tre interfacce dei router (lato LAN) e a tutti gli host della rete.
- *D)* Scrivete le righe della tabella di instradamento del router, relativamente alle LAN di cui sopra.
- (NOTA: considerate di poter utilizzare HUB e SWITCH a 4, 8, 12, 24 o 48 porte, router a 2,3 o 4 interfacce).



## Piano di indirizzamento

LAN	IP SUBNET	NETMASK	BROADCAST	IP router e host
ETH1	200.70.40.0	255.255.255.128 (/25)	200.70.40.127	da 200.70.40.1 a 200.70.40.126
ETH2	200.70.40.128	255.255.255.192 (/26)	200.70.40.191	da 200.70.40.129 a 200.70.40.190
ETH3	200.70.40.192	255.255.255.192 (/26)	200.70.40.255	da 200.70.40.193 a 200.70.40.254

## Tabella Router.

LAN	IP SUBNET	NETMASK	IP Interfaccia router	
ETH1	200.70.40.0	255.255.255.128 (/25)	200.70.40.1	
ETH2	200.70.40.128	255.255.255.192 (/26)	200.70.40.129	
ETH3	200.70.40.192	255.255.255.192 (/26)	200.70.40.193	