Università di Roma Tor Vergata
Corso di Laurea triennale in Informatica

# Sistemi operativi e reti

A.A. 2017-18

Pietro Frasca

## Parte II: Reti di calcolatori

## Lezione 24

Giovedì 7-06-2018

# Wi-Fi 802.11

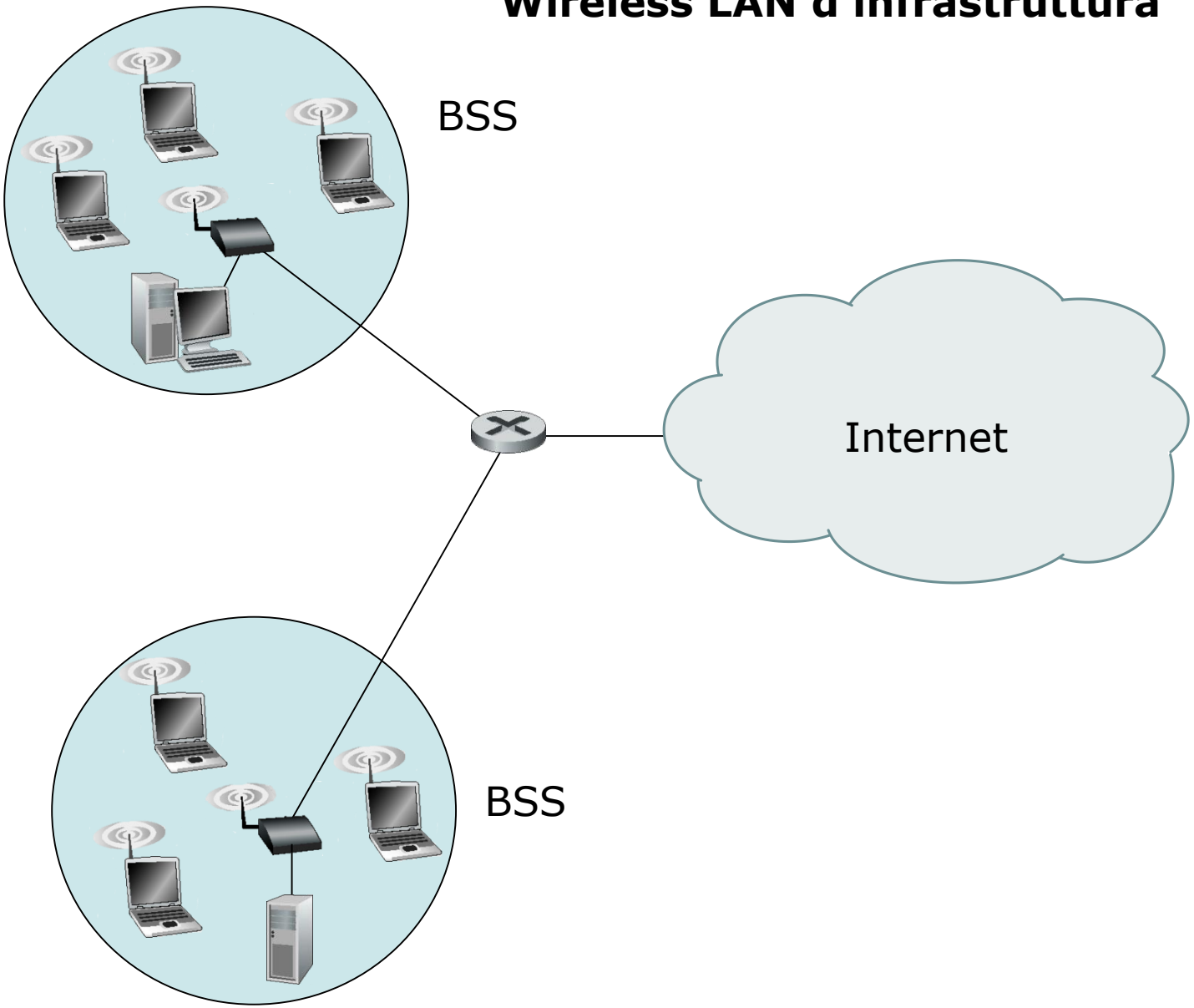
- Tra i vari standard delle reti wireless, lo standard **802.11** wireless LAN, detto anche **Wi-Fi** è lo standard più diffuso.
- Lo standard 802.11, nato negli anni '90, ha diverse varianti, tra cui 802.11 a, b, g e n. Attualmente sono disponibili adattatori wireless con tripla *(802.11 b/g/n)* modalità.
- I tre 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, i tre 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. Il più recente 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 oltre 200 Mbps.
- Tutti questi standard usano onde elettromagnetiche con portanti aventi frequenze comprese tra 2,4 e 2,485 GHz, che sono utilizzate anche dai telefoni senza fili.

# Architettura 802.11

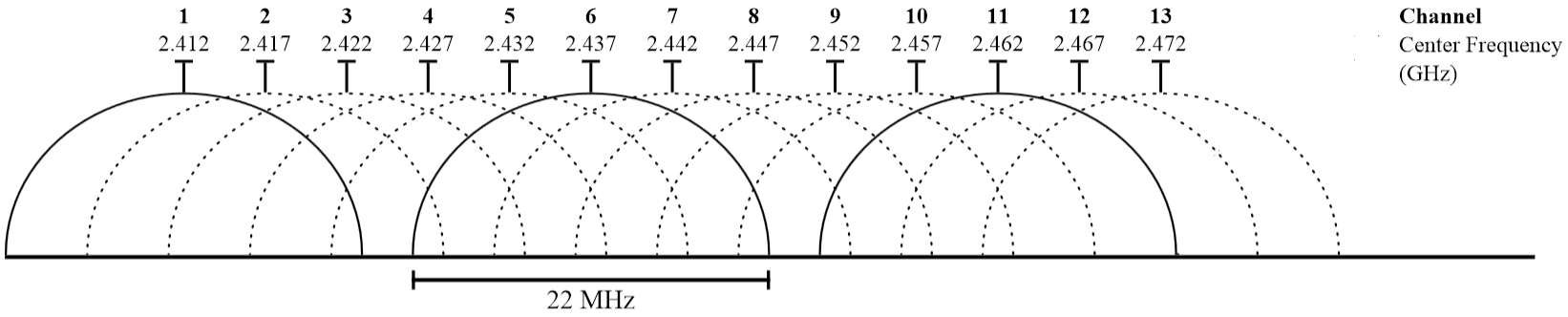
- L'architettura dello standard 802.11, è basata sul **BSS (*basic service set,* set di servizio base***),*** costituito da uno o più host wireless e un **AP *(Access point, punto di accesso)***.
- Una tipica rete residenziale, è costituita da un AP uno switch e un router NAT, assemblati nello stesso 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

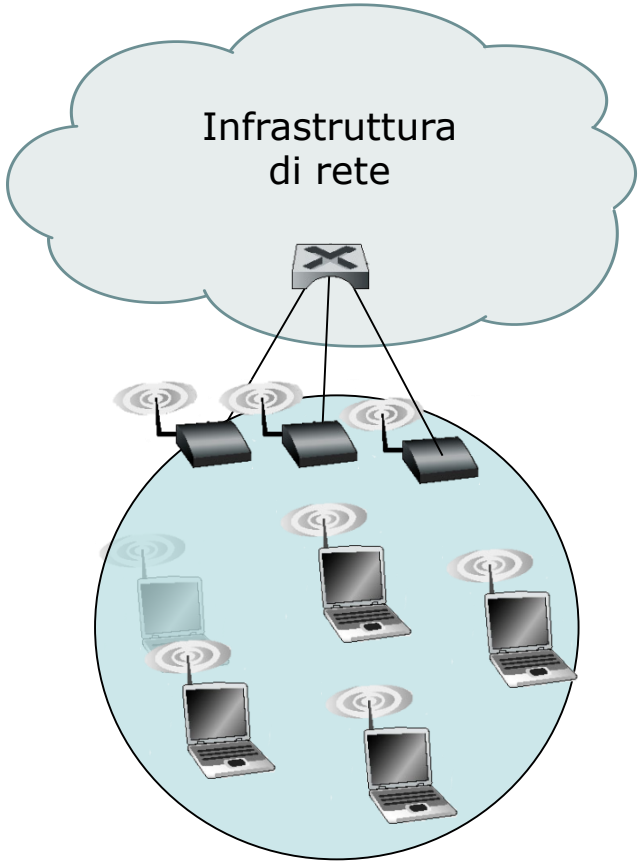


# Canali e associazioni

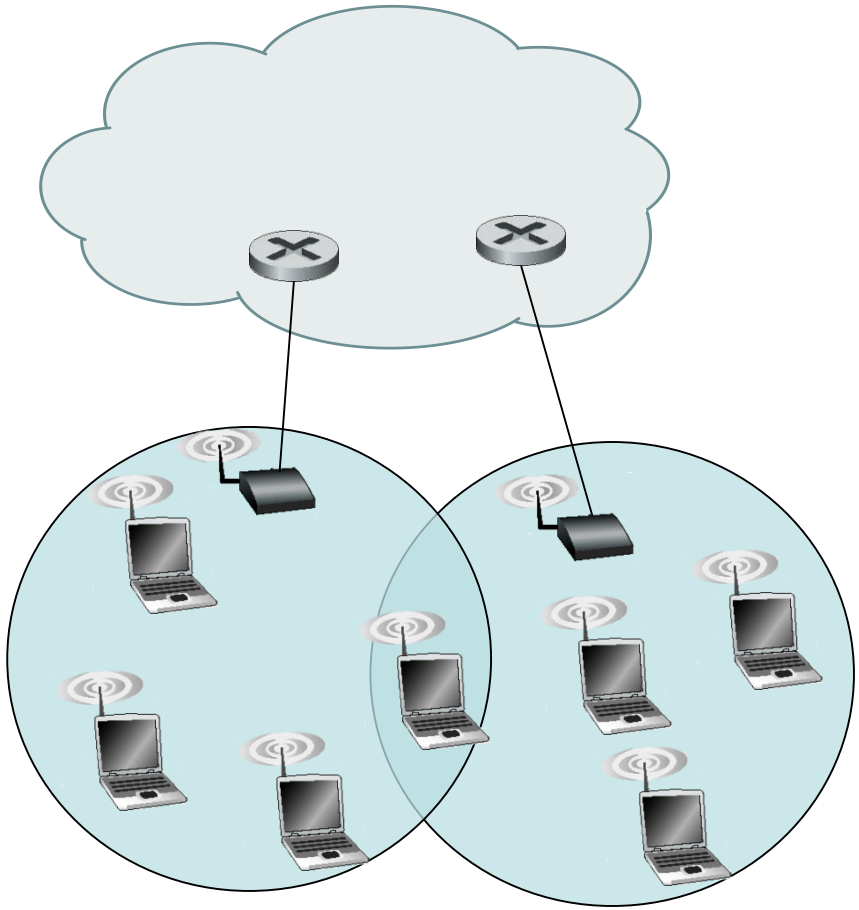
- Per poter comunicare, gli host devono prima associarsi a un AP.
- Quando si installa un AP, generalmente si assegna ad esso un identificativo detto **SSID *(service set identifier).***
- Oltre al SSID è necessario scegliere per l'AP un **numero di canale**. Un numero di canale corrisponde, per 802.11 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.


1 2 3 4 5 6 7 8 9 10 11 12 13
2.412 2.417 2.422 2.427 2.432 2.437 2.442 2.447 2.452 2.457 2.462 2.467 2.472
Channel
Center Frequency
(GHz)
22 MHz

- 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*200=600 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.



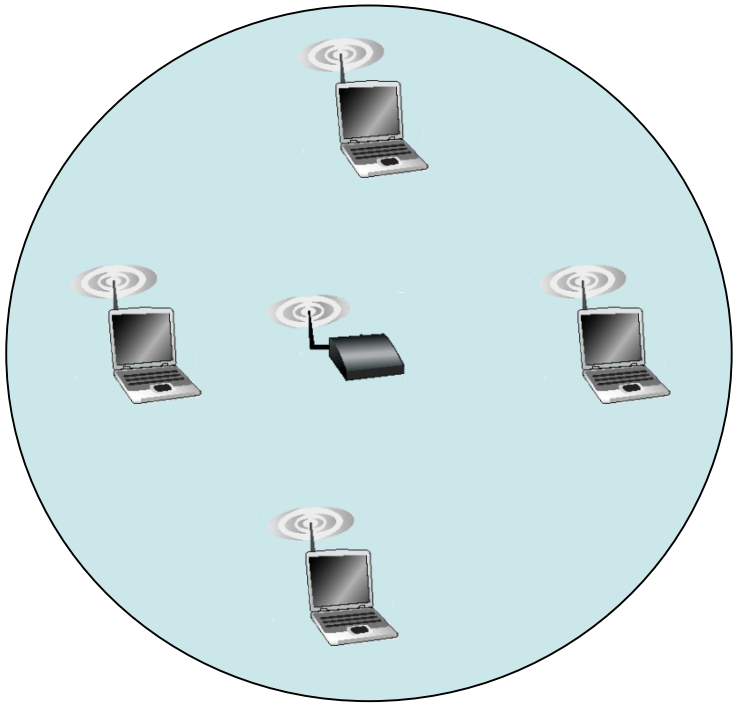
- Supponiamo che un host si trovi in una zona coperta da più AP.
- Per connettersi ad Internet, l'host deve associarsi a un unico AP e quindi accedere ad una subnet.
- L'host wireless può associarsi a un AP in due modalità dette ***scansione passiva*** e **scansione attiva**.
- La ***scansione passiva*** funziona nel seguente modo:
  - L'AP invia periodicamente dei piccoli frame detti frame **beacon**, che contengono il proprio **SSID** e il proprio **indirizzo MAC**. 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 connetterà 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 wireless generalmente è richiesto di autenticarsi. Le reti 802.11 forniscono diverse soluzioni per l'autenticazione (WPA-PSK, WPA2-PSK, 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.

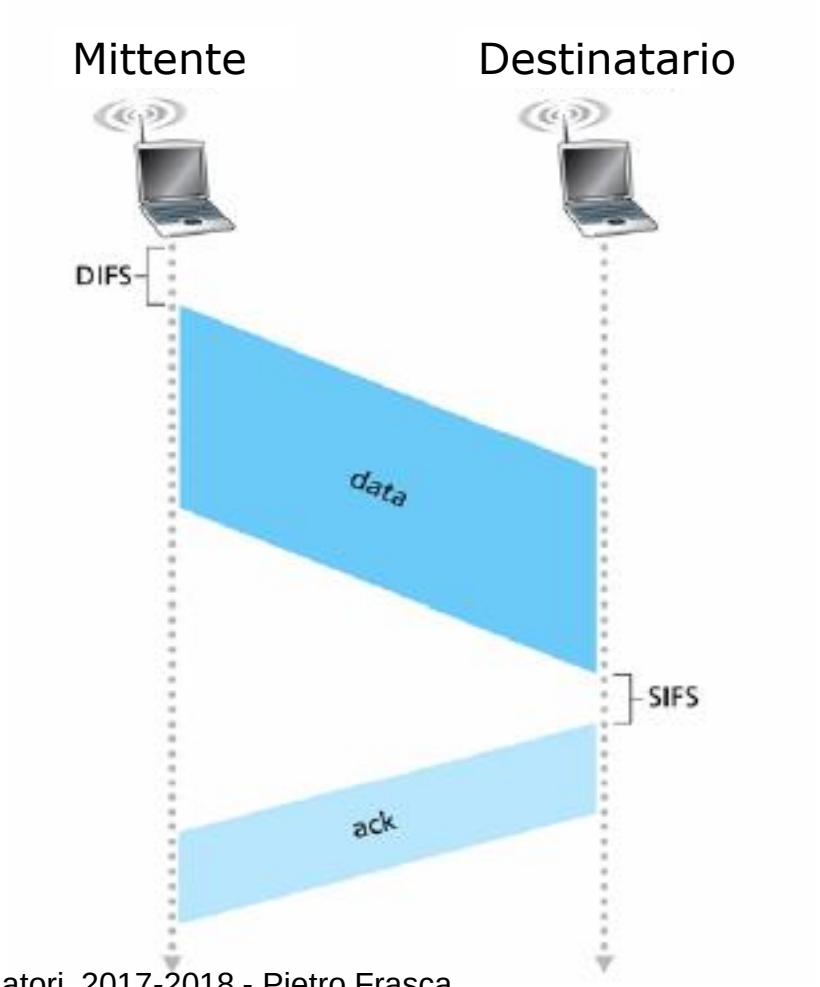


- Il protocollo usato è il **CSMA/CA** *(**Carrier Sense Multiple Access / Collision avoidance,*** **accesso multiplo con rilevazione della portante/collisioni evitate***).*
- Come in Ethernet il CSMA/CA richiede che ogni stazione ascolti prima di trasmettere e non trasmette se rileva che il canale è 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.

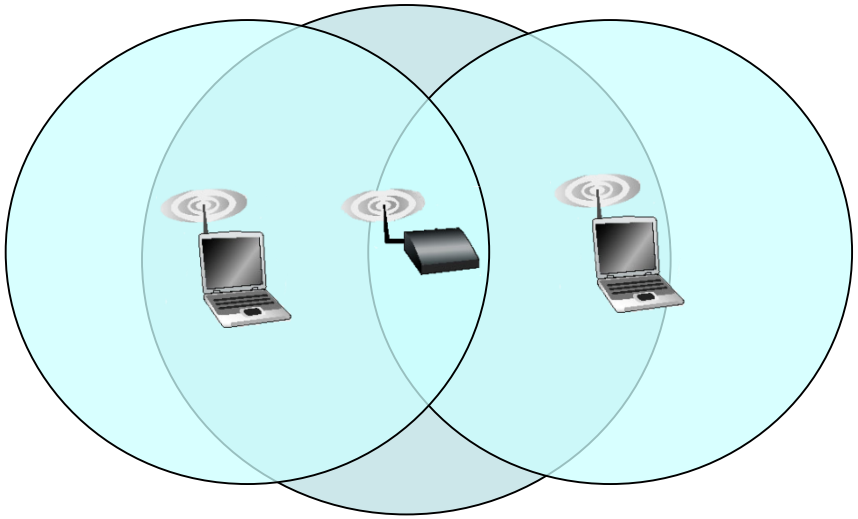
- Quando l'host **destinatario** riceve un frame esegue il controllo CRC e se corretto, attende per un breve periodo di tem*po,* detto **SIFS (*short inter-frame space,* breve spazio inter-fame*)***,** dopo il quale invia al mittente un frame di riscontro di avvenuta ricezione.



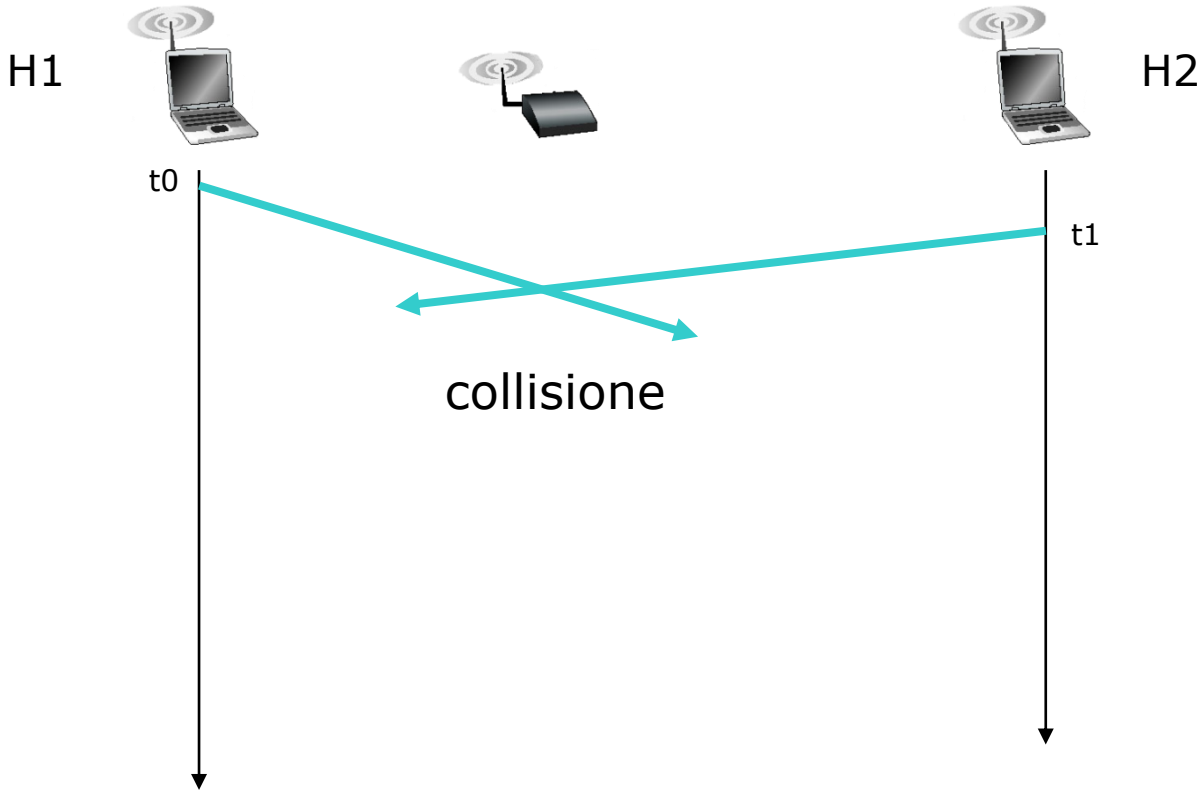
- Se l’host mittente non riceverà questo riscontro entro un intervallo di tempo stabilito (timeout), ritrasmetterà il frame. Il mittente ritorna al passo 2 incrementando il valore del ritardo.
- Se il frame di riscontro non sarà ricevuto dopo un numero prefissato di ritrasmissioni, l’host mittente scarterà 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.



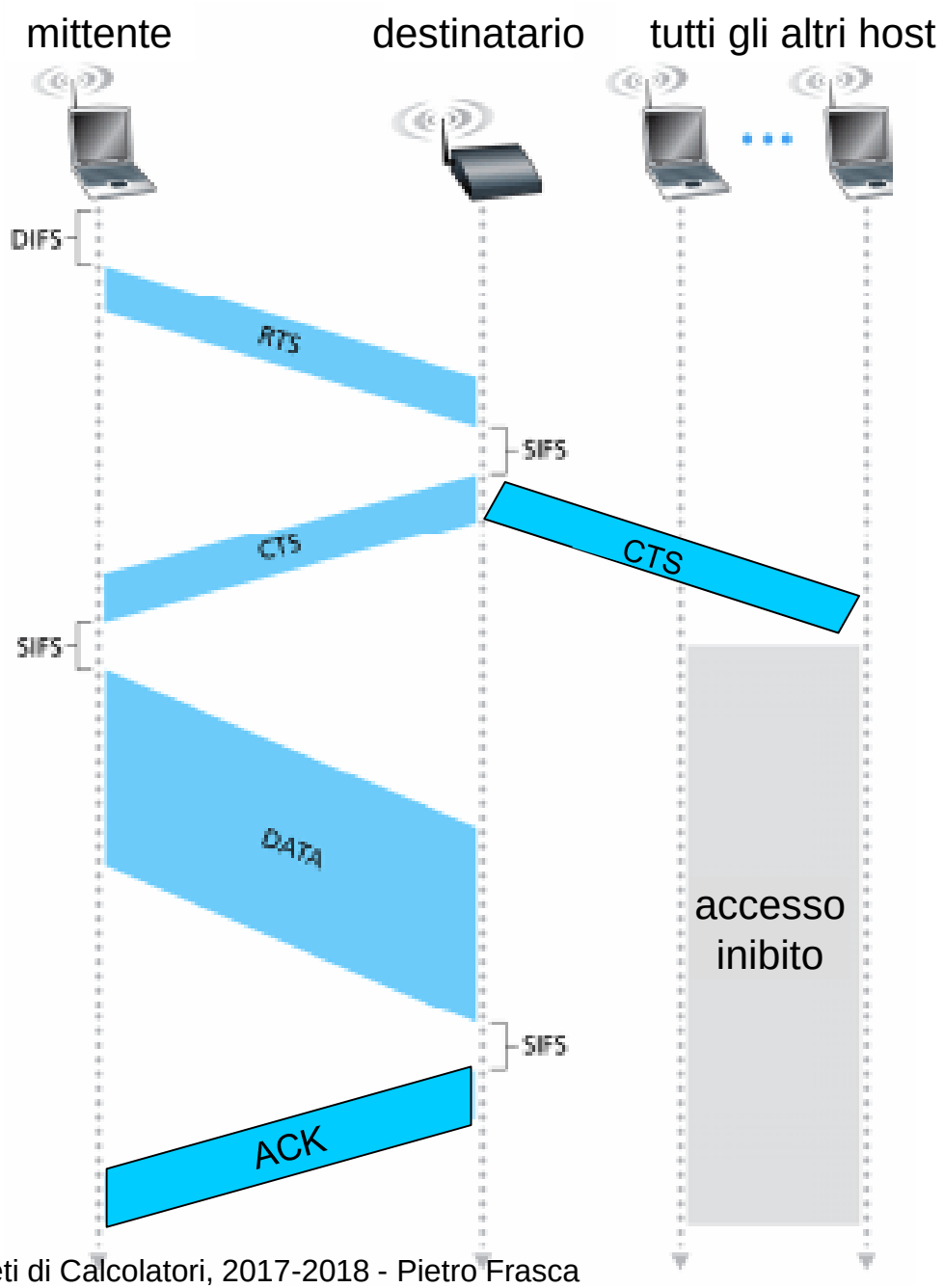
- Supponiamo che l'host H1, all'istante $t_0$, stia trasmettendo un frame e, subito dopo, all'istante $t_1$, H2 trasmetta un frame all'AP. H2, non rilevando la trasmissione di H1, attenderà un breve periodo di tempo casuale DIFS e poi trasmetterà il frame, causando la collisione.



- 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:

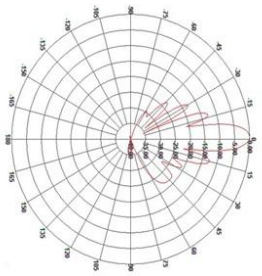
  - **abilitare il mittente alla trasmissione e**
  - **impedire alle altre stazioni la trasmissione durante il periodo di tempo prenotato.**

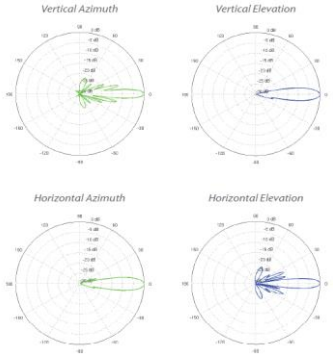

mittente
destinatario
tutti gli altri host
DIFS
RTS
SIFS
CTS
CTS
SIFS
DATA
accesso
inibito
SIFS
ACK

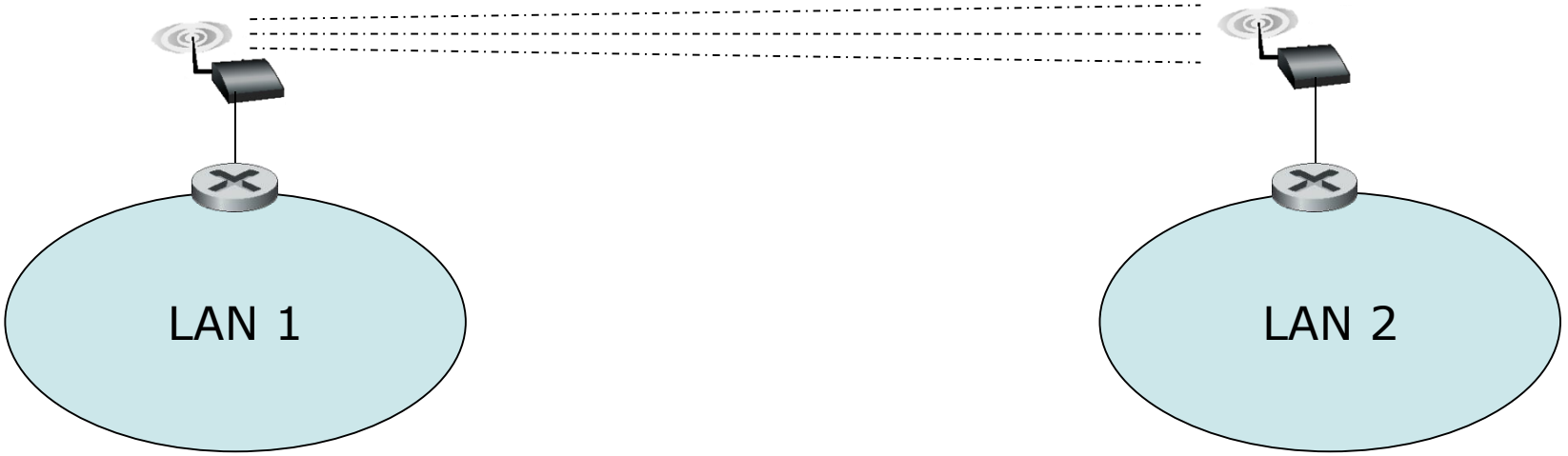
- L’uso dei frame RTS e CTS può incrementare le prestazioni per i seguenti motivi:
  - risolve il **problema dell’host nascosto**, in quanto il frame DATI viene trasmesso soltanto dopo che il canale è stato prenotato;
  - dato che i frame RTS e CTS sono piccoli, una eventuale collisione sarà di breve 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**, cosi 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.

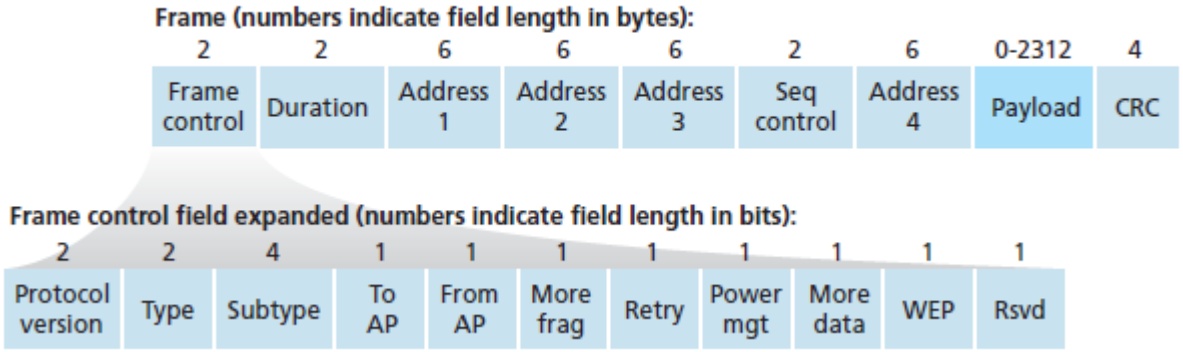




# Frame IEEE 802.11

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




## 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.

## Campo indirizzo

- Il frame 802.11 contiene quattro campi indirizzo MAC (invece di 2 di Ethernet).
- I tre campi indirizzo sono necessari a scopi d'interconnessione, il quarto campo indirizzo è impiegato 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.
- **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

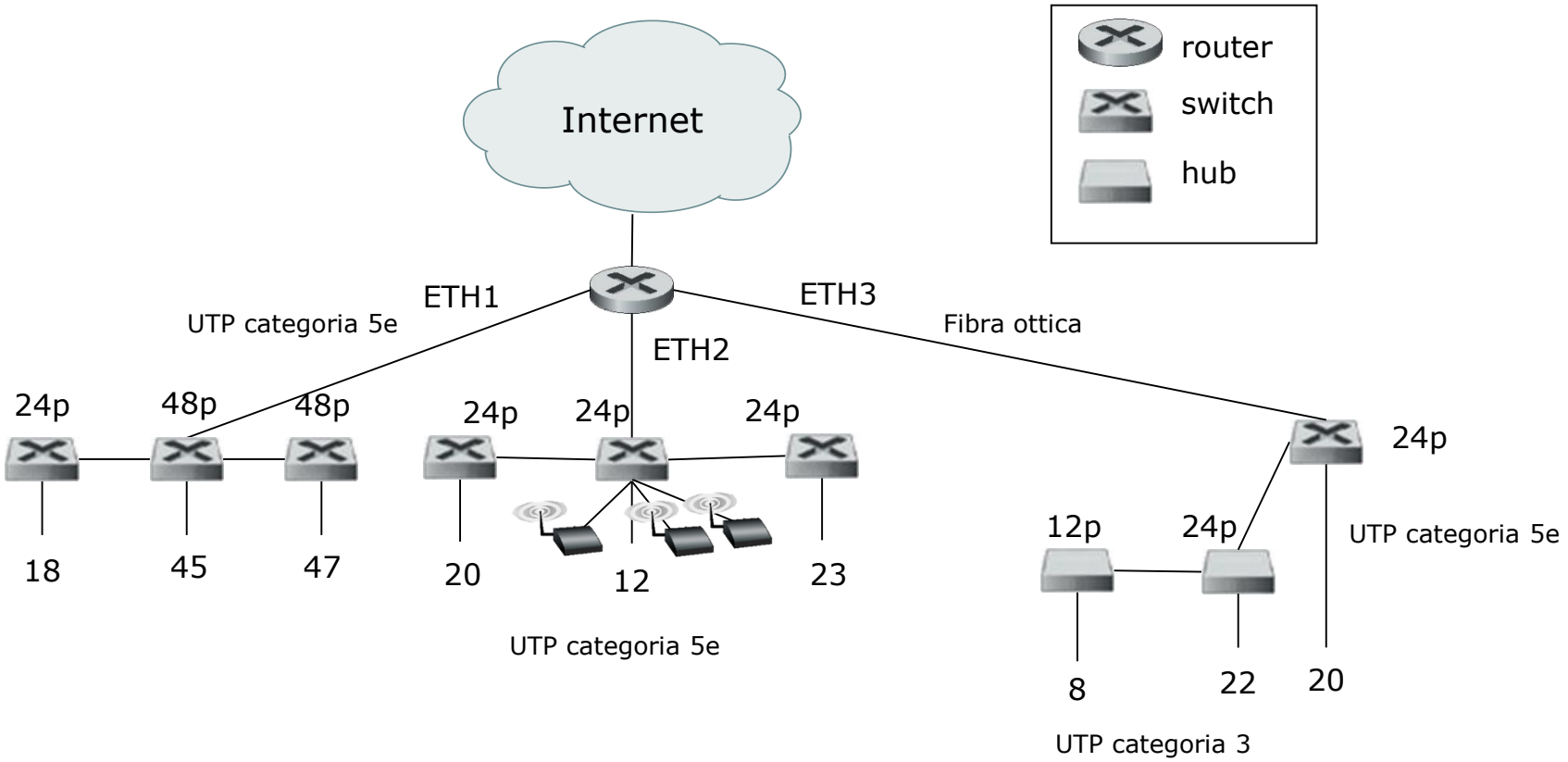
- Ricordiamo che ogni volta che una stazione wi-fi riceve correttamente un frame da un'altra stazione, invia al mittente un frame ACK che confermare l'avvenuta ricezione.

  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.
- Teniamo presente che 802.11 permette al nodo trasmittente di riservare il canale per un intervallo di tempo che comprende i tempo necessario per trasmissione del suo frame dati e quello del frame di conferma. 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 100baseT, 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 stata 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 circa 600 Mbps.
- *A)* Disegnate uno schema della rete descritta, indicando i dispositivi di interconnessione e i tipi di mezzi trasmessivi 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.
- E) Indicate il protocollo necessario per assegnare automaticamente i numeri IP agli host, specificando anche quale altri importanti parametri tale protocollo assegna automaticamente agli host.
- (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<br>a 200.70.40.126 |
| ETH2 | 200.70.40.128 | 255.255.255.192 (/26) | 200.70.40.191 | da 200.70.40.129<br>a 200.70.40.190 |
| ETH3 | 200.70.40.192 | 255.255.255.192 (/26) | 200.70.40.255 | da 200.70.40.193<br>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 | |