



Protocolli PH e DL nelle LAN

Luca Veltri

(mail.to: luca.veltri@unipr.it)

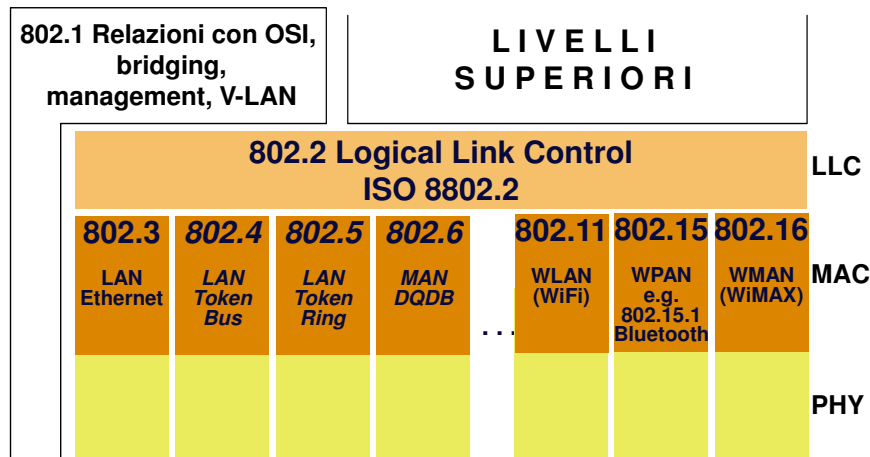
Corso di Reti di Telecomunicazione, a.a. 2016/2017

<http://www.tlc.unipr.it/veltri>

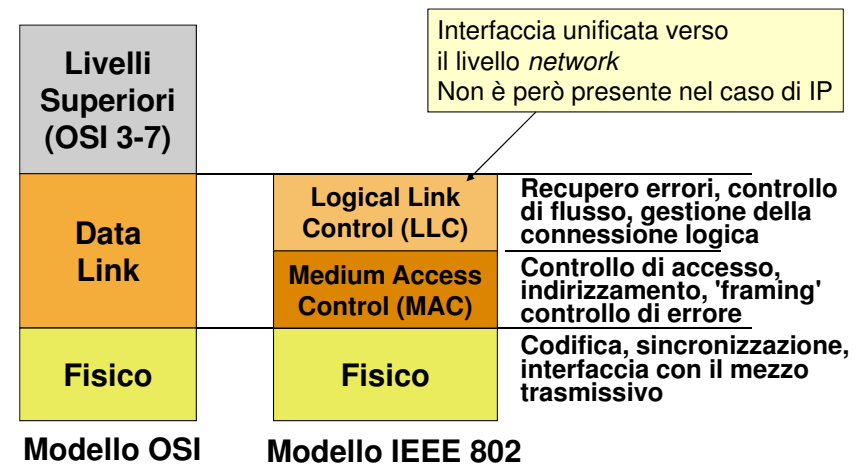
Reti in area locale (LAN)

- Una LAN è un sistema di comunicazione che permette di interconnettere apparecchiature indipendenti in un'area limitata
- Sono spesso caratterizzate da
 - Estensione geografica limitata (edificio, gruppo di edifici)
 - Velocità trasmissiva elevata
 - Basso tasso di errore
 - Mezzi trasmissivi condivisi (solo in origine nel caso di connettività con cavi)
 - Utilizzo di particolari protocolli di accesso al mezzo
 - Facilità di installazione e gestione
 - HW plug&play
 - assenza di configurazione (indirizzi, routing, etc)
 - Sotto la proprietà di una singola organizzazione e gestita da questa

Il modello IEEE 802



IEEE 802 vs OSI



Standard IEEE 802.3 (Ethernet)

Ethernet: Storia

- Il protocollo Ethernet è uno degli standard per reti in area locale più diffuso e implementato a livello mondiale
- Nacque agli inizi degli anni 70 presso il laboratorio di ricerca Xeros californiano
- Nel 1982 lo standard divenne Ethernet II (Digital, Intel, Xeros)
- Nel 1983 lo standard fu posto sotto il controllo dell'IEEE (nel gruppo 802)

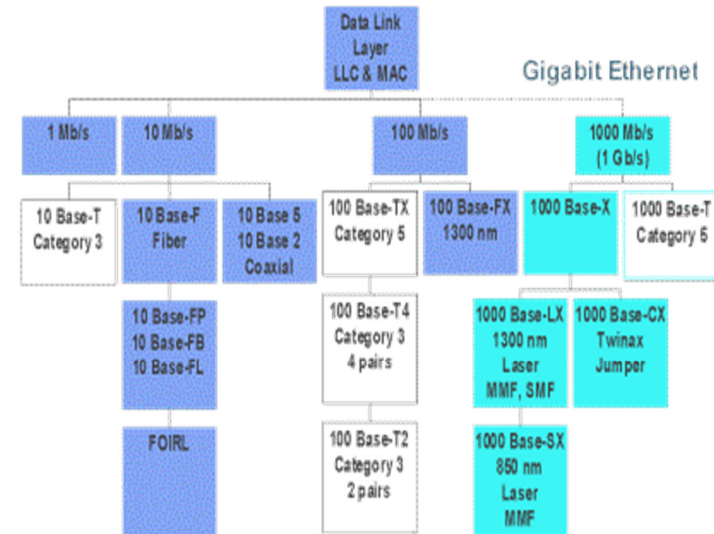
Ethernet: Caratteristiche principali

- La topologia logica di una rete Ethernet (cioè il percorso logico che le informazioni seguono) è a BUS
- La velocità di trasmissione nella versione originale era di 10 Mbit/s in banda base con codifica di tipo Manchester; attualmente sono utilizzate le versioni a 100 Mb/s e a 1 Gb/s
- Utilizza un protocollo di accesso al mezzo denominato CSMA/CD
- Dimensione minima di un pacchetto 64 byte (tale valore corrisponde al tempo necessario per assicurare che tutte le stazioni siano in grado di rilevare una avvenuta collisione)

Ethernet: Funzioni implementate

- Obiettivi degli strati PH e MAC Ethernet e relative funzioni:
 - **indirizzamento dei nodi (stazioni) sorgente e destinazione, identificando anche il protocollo utente (di strato superiore)**
 - funzione di indirizzamento, tramite indirizzi dei SSAP e DSAP
 - **invio di UI a datagramma tra stazioni terminali, con o senza nodi intermedi**
 - funzione di invio/ricezione, routing
 - **utilizzo di un mezzo broadcast condiviso**
 - funzione MAC
 - **rivelazione di errore e scarto delle UI errate (non recupero)**
 - funzione di controllo di errore

802.3: Standard di livello fisico



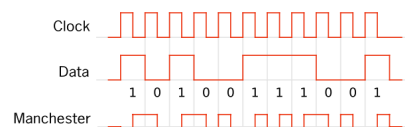
Reti di telecomunicazione - Luca Veltri

10

IEEE 802.3 - Strato PH

IEEE 802.3 di livello fisico: Coassiale

- IEEE 802.3 (Ethernet) 10Base5 e 10Base2
 - dominante sino al '90, usato solo in Ethernet a 10Mb/s
- Topologia base di strato fisico: BUS
 - tutte le stazioni collegate direttamente ad un unico bus (coassiale)
 - il bus e le stazioni collegate formano un singolo segmento di rete
 - non sono necessari nodi intermedi
- Opzionalmente, più segmenti di rete possono essere interconnessi tramite nodi intermedi di livello PH (repeater)
 - si ottiene così una topologia ad ALBERO
 - con instradamento broadcast



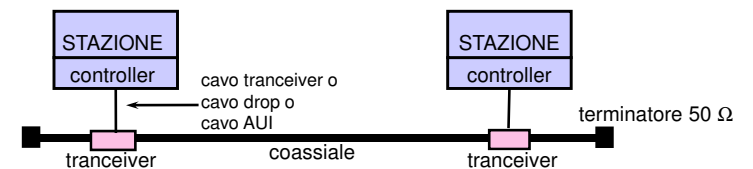
- Codifica utilizzata: Manchester
- Tipi di cavi coassiali usati:
 - Cavo grosso (Thick-RG213)
 - Cavo sottile (Thin-RG58)

Reti di telecomunicazione - Luca Veltri

11

Coassiale Thick (10Base5)

- Cavo coassiale grosso (Thick-RG213)
 - unico cavo coassiale 50 Ω, senza giunture
 - stazioni collegate tramite dispositivi detti "transceiver"
 - transceiver connessi direttamente al coassiale con prese "a vampiro"
 - min distanza tra i transceiver: 2.5 m
 - max lunghezza del singolo segmento: 500m
 - max numero di transceiver su singolo segmento: 100



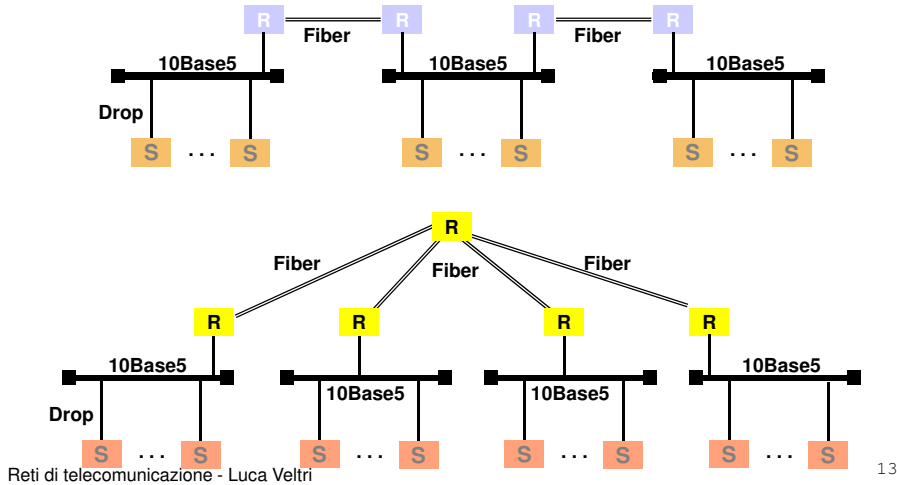
- Eventualmente, utilizzo di ripetitori per interconnettere più segmenti

Reti di telecomunicazione - Luca Veltri

12

Coassiale Thick (10Base5) (cont.)

- Esempi di configurazione 10Base5

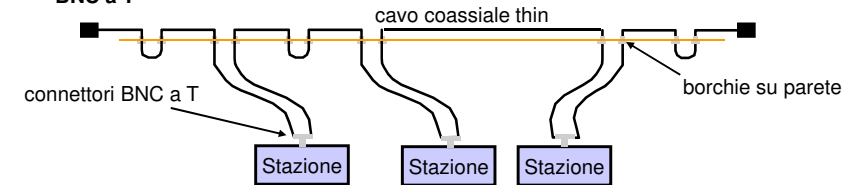
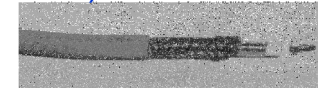


13

Coassiale Thin (10Base2)

- Cavo coassiale sottile (Thin-RG58)

- più spezzoni di coassiale interconnessi tramite connettori BNC "crimpati" al cavo
- max lunghezza del cavo (maggiore attenuazione): 185 m
- max numero di stazioni: 30
- min distanza tra le stazioni: 0.5 m
- schede di rete in genere connesse direttamente al cavo, tramite connettori BNC a T



- Altre caratteristiche

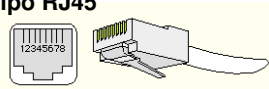
- costo inferiore del cavo
- maggiore facilità e minor costo di posa
- scarsa affidabilità (il cavo è accessibile all'utente)

Reti di telecomunicazione - Luca Veltri

14

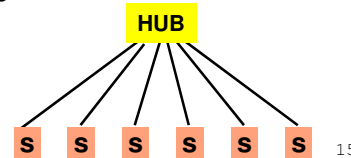
IEEE 802.3 di livello fisico: Coppia simmetrica (Twisted Pair)

- IEEE 802.3 (Ethernet) 10/100/1000 Base T
- Cavi con 4 coppie simmetriche e intrecciate
 - trasmissione bilanciata
 - i due conduttori trasportano lo stesso segnale, ma in contofase
 - l'intreccio mira a far subire ad entrambi i conduttori le stesse interferenze elettromagnetiche
 - utilizzo di connettori di tipo RJ45



- Realizza solo collegamenti punto-punto

- richiede l'adozione di apparati di rete per collegare più stazioni
 - a livello PH: ripetitori multiporta (hub)
 - a livello DL: switch



Reti di telecomunicazione - Luca Veltri

15

Coppia simmetrica (cont.)

- Caratteristiche:

- lunghezza massima consigliata 100 m
 - 90 m di cablaggio strutturato
 - 10 m di cavetti di patch
- prestazioni inferiori al cavo coassiale (su lunghe distanze)
- basso costo e facilità di posa e connessione (connettori RJ45)
- adatto a cablaggi strutturati
- enorme diffusione a partire dal '90

- Tipi di collegamenti

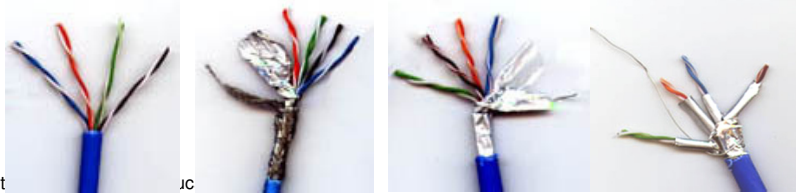
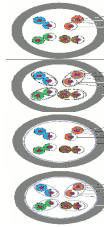
- tra stazione e stazione
- tra stazione e apparato
- tra apparati

Reti di telecomunicazione - Luca Veltri

16

Coppia simmetrica (cont.)

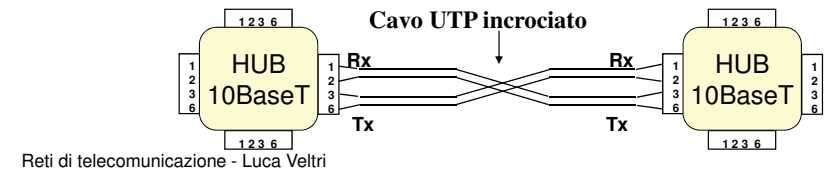
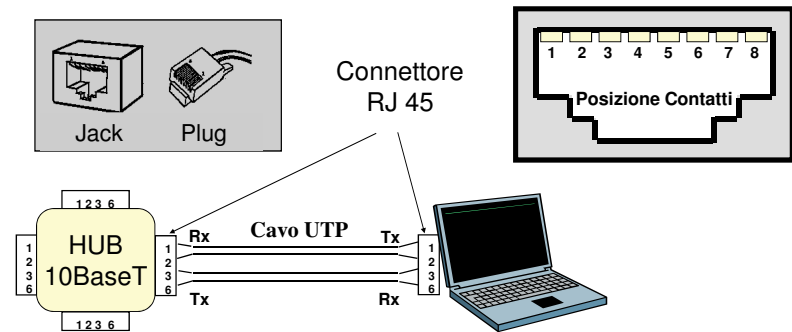
- Tipologie di cavi
 - UTP (Unshielded): non schermato
 - STP (Shielded): schermato coppia per coppia
 - FTP (Foiled): uno solo schermo per tutto il cavetto
 - S/FTP, S/UTP, SSTP
- Categorie dei cavi
 - 1 - telefonia analogica
 - 2 - telefonia numerica (ISDN) e dati a bassa velocità
 - 3 - dati sino a 16 MHz di banda
 - 4 - dati sino a 20 MHz di banda
 - 5 - dati sino a 100 MHz di banda
 - 6 - dati sino a 250 MHz di banda
 - 7 - dati sino a 600 MHz di banda



Reti di t

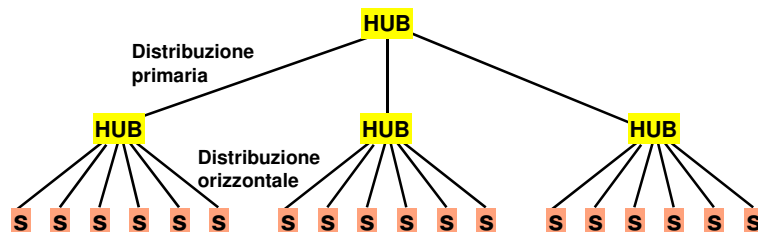
ic

Connettori per Base-T



Cablaggio in coppia simmetrica (o in fibra)

- Esempio di topologia stellare gerarchica

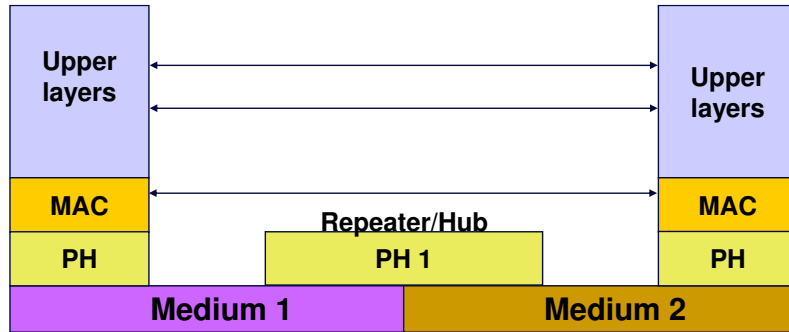


Reti di telecomunicazione - Luca Veltri

Fibra ottica

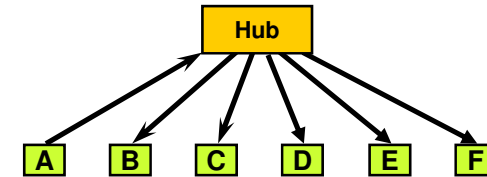
- Cavi con doppia fibra ottica
 - una fibra per ogni verso di trasmissione
 - elevate velocità di trasmissione
 - adatti a lunghe distanze di interconnessione
 - adatti ad ambienti con problemi di compatibilità elettromagnetica
 - Caratteristiche:
 - insensibilità al rumore elettromagnetico
 - mancanza di emissioni
 - bassa attenuazione
 - banda passante molto elevata
 - costo della fibra relativamente basso
 - alto costo per interfacce e giunzioni
 - Tipologie di fibre
 - Fibre multimodali
 - Fibre monomodali
- Reti di telecomunicazione - Luca Veltri

Repeater/Hub



Repeater/Hub

- Serve per ripetere e rigenerare una sequenza di bit ricevuti da una porta sulle altre porte
- Assume il nome di:
 - **repeater** quando è costituito da 2 porte
 - **multiport repeater** quando è costituito da più di 2 porte
 - **hub** equivale a multiport repeater per cablaggi a coppie simmetriche con connettori RJ45

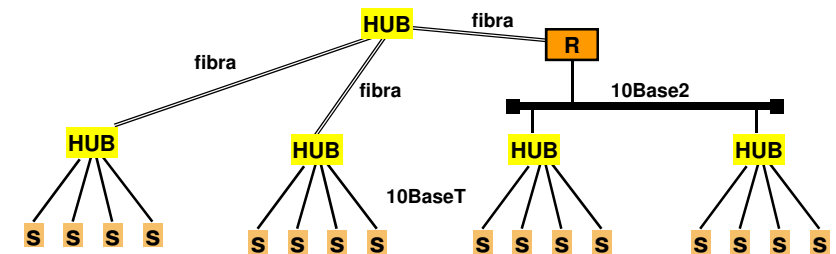


Repeater/Hub: funzioni

- Un pacchetto ricevuto su una porta va ripetuto su tutte le altre porte (Retiming)
- Se su un porta viene rilevata una collisione deve interrompere la ripetizione del pacchetto su tutte le porte e trasmettere una sequenza di Jamming
 - l'hub deve poter anche rilevare una collisione che avviene al suo interno invece che su un segmento
- In caso di collisioni consecutive deve "partizionare" la porta interessata
 - rilevamento di guasti/malfunzionamenti

Cablaggio misto

- Esempio di cablaggio misto a 10Mb/s

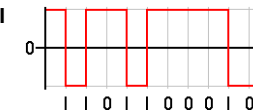
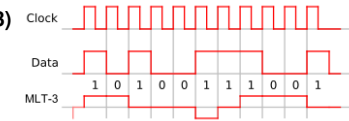


Ethernet a 100 Mb/s (IEEE 802.3u)

- 802.3u detto anche 100BASE-T o Fast-Ethernet
- Stesso protocollo CSMA/CD dello standard originale a 10Mb/s
- Velocità dieci volte superiore rispetto al 10 Mb/s
 - 100 Mb/s
 - bit time 10 ns
 - slot time 512 bit (5.12 μs)
- Distanze dieci volte inferiori
 - Stessa lunghezza del pacchetto
 - 'Round trip delay' ridotto di 10 volte
 - dimensioni max. della rete ridotte di 10 volte
 - stazioni connesse a max. 100 mt dall'HUB
- Compatibilità a livello di scheda con 10BaseT
- Tre sotto-standard per tre tipi di mezzi fisici:
 - 100BASE-TX (doppino, su 2 coppie)
 - 100BASE-4 (doppino, su 4 coppie)
 - 100BASE-FX (fibra ottica)

IEEE802.3u: 100Base-TX e 100Base-FX

- 100BASE-TX utilizza con pochissime modifiche lo standard TP-PMD (Twisted-Pair Physical Medium Dependent) per FDDI:
 - Codifica 4B/5B
 - Scrambling
 - Codifica MLT-3 (Multilevel threshold-3)
- 100BASE-FX utilizza con pochissime modifiche lo standard PMD per FDDI su fibra ottica multimodale (ISO 9314-3)
 - Codifica 4B/5B
 - Scrambling
 - Codifica NRZI



Gigabit Ethernet

- Come lo standard IEEE 802.3u, rappresenta una evoluzione di Ethernet
 - formato e dimensione del pacchetto uguali a Ethernet 10/100Mb/s (IEEE 802.3)
 - bitrate di 1 Gb/s
- Come anche Fast-Ethernet, supporta le seguenti modalità operative:
 - Half-Duplex
 - CSMA/CD
 - nella pratica NON è implementato nella versione Gigabit
 - Full-Duplex (con controllo di flusso)
 - senza collisioni
 - non ci sono limiti al diametro della rete dovuti al protocollo di accesso
 - è la modalità di Gigabit Ethernet effettivamente implementata

Gigabit Ethernet (cont.)

- Gigabit Ethernet offre i vantaggi tipici di Ethernet:
 - semplicità del metodo di accesso CSMA/CD
 - alta scalabilità tra le diverse velocità di trasmissione
- Facile evoluzione (e costi contenuti) a partire da LAN Ethernet già esistenti:
 - sostituzione degli apparati di rete (hub, switch, schede, etc.)
- Nella modalità half-duplex per mantenere lo stesso slot time previsto per Fast Ethernet (e quindi stesso diametro max) è previsto:
 - estensione dei pacchetti corti
 - sino a raggiungere lunghezza di 4096 bit
 - trasmissione consecutiva di più pacchetti senza rilasciare il mezzo trasmissivo
 - fino al burst limit che è di 65536 bit (8192 ottetti)

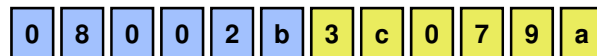
IEEE 802.3: Livello DL

- Funzioni realizzate da IEEE 802.3 livello DL:
 - controllo di accesso multiplo al mezzo (MAC)
 - rivelazione di errore
 - indirizzamento e instradamento delle UI
- Nodi a livello DL:
 - stazioni terminali
 - nodi intermedi: BRIDGE e SWITCH

IEEE 802.3 - Strato MAC/DL

Indirizzi Ethernet

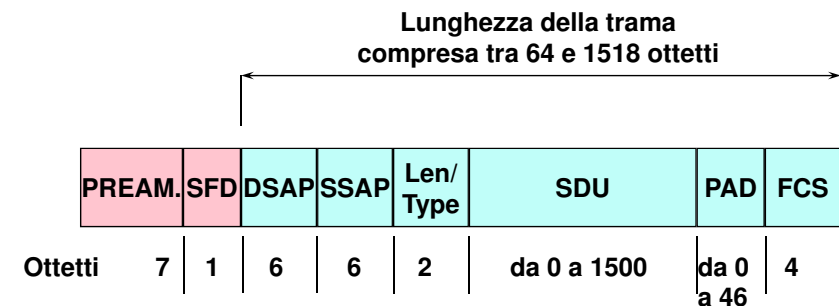
- A livello PH le le UI vengono inviate a tutte le stazioni; a livello DL le UI vengono ricevute sulla base dell'indirizzo di destinazione presente nelle UI (DL-PDU)
 - indirizzi Ethernet (IEEE 802.3) o Indirizzi MAC
- L' indirizzo MAC è una stringa di 48 bit (6 Bytes)



Assegnato dall'IEEE Assegnato dal costruttore

- L' indirizzo MAC può essere:
 - Individuale (Es. 08-00-20-34-11-30)
 - Di gruppo (Es. 01-00-5e-12-34-56)
 - Broadcast (ff-ff-ff-ff-ff-ff)

IEEE 802.3: Formato della trama



IEEE 802.3: Formato della trama (cont.)

- Formato di una MAC PDU IEEE 802.3
 - preambolo (7 ottetti), formato da alternanze di 1 e 0
 - Start Frame Delimiter (SFD) (1 ottetto), con valore 1010101, indica l'inizio trama
 - indirizzo di destinazione (2 o 6 ottetti)
 - indirizzo di sorgente (2 o 6 ottetti)
 - lunghezza del campo dati (IEEE 802.3) o Protocol Type (Ethernet) (2 ottetti)
 - SDU (nello standard 802.3 sono la PDU di strato LLC)
 - PAD (da 0 a 46 ottetti), inserito quando la parte dati è inferiore a 46 ottetti in modo da garantire che la trama abbia una lunghezza minima di 64 ottetti
 - Frame Check Sequence (FCS) (4 ottetti), di tipo CRC

Formato IEEE 802.3 vs Ethernet

IEEE 802.3



Ethernet



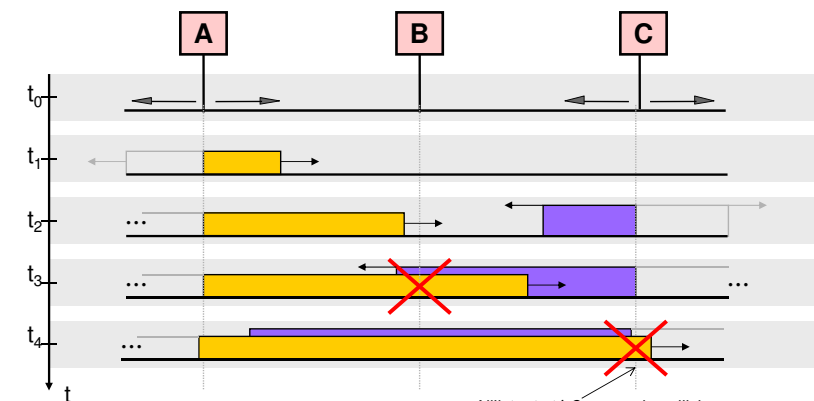
- Il campo 'Protocol Type' permette di moltiplicare più protocolli direttamente sullo stesso MAC
- e.g. PT=0x0800 (=2048) corrisponde al protocollo IP

Protocollo MAC IEEE 802.3

- E' funzione importante del IEEE 802.3 a livello DL
 - per questo lo strato viene indicato come strato MAC
- Carrier Sensing Multiple Access with Collision Detection (CSMA/CD)
 - meccanismo non deterministico (accesso casuale) con tempo di attesa non limitato superiormente
 - concepito per topologie a bus ma utilizzato anche con topologie di strato fisico a stella e albero
 - un singolo segmento di rete che interconnette stazioni con solo nodi di livello PH viene visto a livello logico dal MAC come unico mezzo condiviso (dominio di collisione)

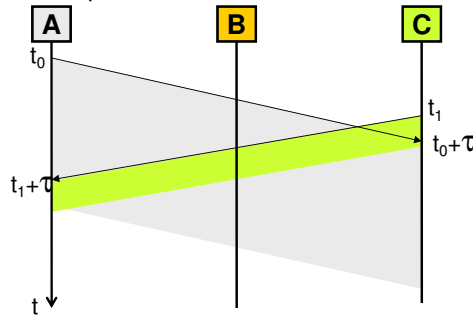
Collisioni

- Tra due stazioni (e.g. A e C) avviene una collisione se esse accedono al canale in istanti che distano tra loro un tempo inferiore a quello di propagazione tra le due stazioni



Intervallo di vulnerabilità

- L'intervallo di vulnerabilità è l'intervallo di tempo in cui una unità informativa emessa può subire collisione



- se t_0 e t_1 sono due istanti di tempo in cui due stazioni incominciano ad inviare una UI, il caso peggiore è quando $t_1 = t_0 + \tau - \epsilon$, con ϵ piccolo

- Intervallo di vulnerabilità: $\Delta T = t_1 + \tau - t_0 = t_0 + \tau - \epsilon + \tau - t_0 < 2\tau$

Reti di telecomunicazione - Luca Veltri

37

Intervallo di vulnerabilità (cont.)

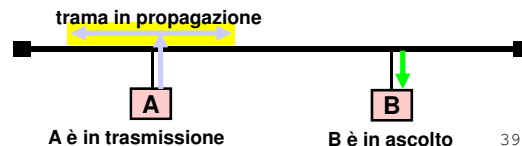
- Per definizione, lo strato MAC Ethernet (IEEE 802.3) NON deve terminare l'emissione completa di una trama prima che sia certo lo stato di NON collisione; in questo modo che:
 - a fine trasmissione la sorgente sa se la trama deve essere considerata inviata o deve essere ri-trasmessa
 - in caso di collisione chi trasmette può aggiungere alla trama in invio informazione che segnali l'evento (trama errata)
 - in questo modo si evita che alcune stazioni possano non accorgersi della collisione; tutte le stazioni capiscono che la trama deve essere scartata
- Poiché il tempo per trasmettere completamente una trama dipende dalla sua lunghezza e dal bit rate R, mentre il tempo di propagazione τ massimo dipende dalla lunghezza del mezzo, Ethernet definisce una lunghezza min di trama (MAC-PDU) di 64 byte e lunghezza massima del mezzo d_{max} così legati:
 - $L_{min} = 64 \text{ byte (512 bit)}$
 - $\tau \cong d_{max} / v_m$
 - tempo minimo di trama: $T_{min} = L_{min} / R$
 - imponendo: $T_{min} > 2\tau$
 - si ottiene: $d_{max} \cong v_m \tau < v_m L_{min} / 2R$
 - con v_m = velocità di propagazione nel mezzo

Reti di telecomunicazione - Luca Veltri

38

CSMA/CD

- Procedura di accesso al mezzo (CSMA):
 - Una stazione prima di tentare la trasmissione verifica lo stato del mezzo (Carrier Sensing)
 - Se il mezzo è occupato si ritarda l'emissione ad un istante successivo (si attende che diventi libero)
 - Quando il mezzo è libero si attende un tempo di deferring (distanziamento delle trame) e si effettua la trasmissione (due PDU consecutive devono essere separate da un intervallo di durata non inferiore a un valore specificato - tempo di intertrama)
 - se il canale era stato rilevato occupato, oltre ad attendere un tempo di intertrama, l'istante successivo di emissione può essere ulteriormente ritardato in accordo ad una PROCEDURA DI PERSISTENZA
 - e.g. con probabilità p si trasmette subito, e con probabilità 1-p si ritarda
- A causa del ritardo di propagazione non nullo il protocollo CSMA non evita completamente le collisioni



Reti di telecomunicazione - Luca Veltri

39

CSMA/CD (cont.)

- Durante l'emissione si ascolta il canale per verificare eventuali collisioni (Collision Detection)
- Se è rivelata una collisione
 - si interrompe l'emissione della trama e si "rinforza" la collisione con una sequenza di jamming (procedura di collision enforcement) per segnalare l'evento alle altre stazioni
 - si esegue poi l'algoritmo di subentro per decidere quando deve essere riemessa la PDU andata in collisione
 - l'accesso viene tentato nuovamente dopo un intervallo di tempo T scelto a caso tra 0 e un valore Tmax (algoritmo di subentro)
 - per ridurre la probabilità di collisione il valore di Tmax dovrebbe dipendere dal numero di stazioni che stanno provando contemporaneamente ad inviare PDU
 - non potendo sapere quante sono le stazioni contemporaneamente in trasmissione, Tmax viene aumentato esponenzialmente all'aumentare del numero di collisioni consecutive verificatesi (back-off esponenziale)

Reti di telecomunicazione - Luca Veltri

40

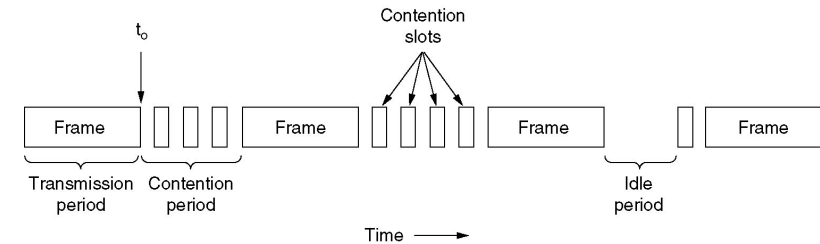
Back-off esponenziale

- Algoritmo che controlla le ritrasmissioni in caso di collisioni
- Parametri:
 - τ = tempo min. di trama = tempo necessario a trasmettere 512 bit
 - e.g. Ethernet 100Mb/s, $\tau = 5,12 \mu\text{s}$
 - n = numero di trasmissioni già tentate (e fallite per collisione)
- Algoritmo
 - tra due trasmissioni si deve attendere $T = r \cdot \tau$
 - al massimo 16 tentativi di trasmissione
 - r è scelto casualmente nell'intervallo

$$0 \leq r < 2^k \quad k = \min\{n, 10\}$$
 - ovvero,
 - T viene scelto casualmente tra 0 e $T_{\text{max}} = \min\{n \cdot \tau, 2^{10} \tau\}$

Protocollo CSMA/CD (cont.)

- Esempio di accesso CSMA/CD:



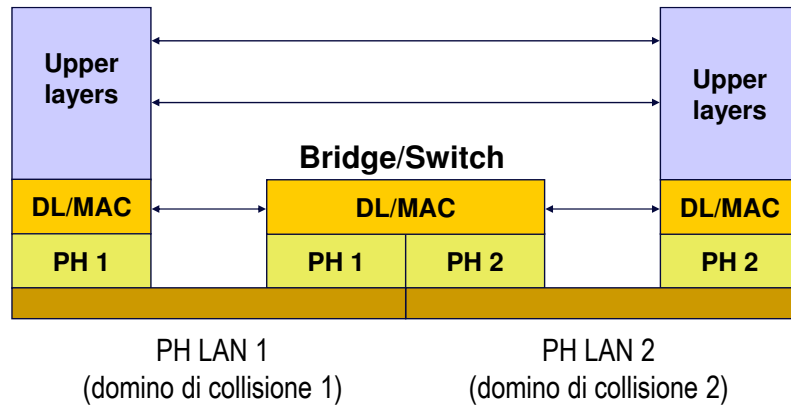
Procedura di emissione

- Procedura di emissione delle MAC PDU:
 - 1) accettare i dati dello strato superiore (e.g. LLC) e l'indirizzo di destinazione
 - 2) formare la PDU
 - indirizzamento
 - controllo della lunghezza minima (in caso sia inferiore si effettua il riempimento)
 - calcolo del CRC (campo controllo di errore)
 - 4) presentare un flusso di dati seriale allo strato fisico per la codifica e per la successiva emissione, in accordo al protocollo MAC CSMA/CD

Procedura di ricezione

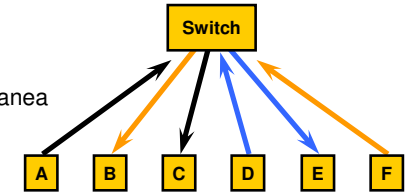
- Procedura di ricezione delle MAC PDU:
 - 1) ricevere un flusso seriale di dati dallo strato fisico
 - 2) elaborare la PDU
 - controllo dell'integrità della PDU (tramite il campo di rivelazione di errore)
 - controllo dell'indirizzo di destinazione della PDU
 - 3) presentare allo strato superiore le PDU indirizzate al terminale locale

Bridging/Switching



Bridge e Switch

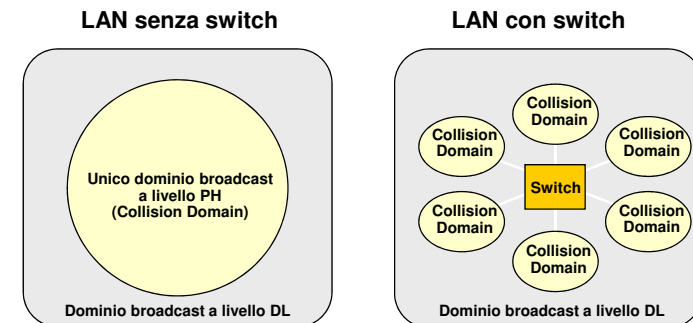
- I Bridge nascono per sezionare le LAN in differenti domini di broadcast a livello PH
 - per ragioni di traffico
 - traffico locale confinato su ciascun segmento
 - per ragioni di distanze fisiche
- Gli switch si comportano come i Bridge e nascono come apparati centro-stella in sostituzione degli Hub
 - traffico tra coppie di stazioni confinato su coppie di rami
 - banda aggregata molto superiore a quella della singola porta
 - molte trasmissioni in contemporanea tra segmenti



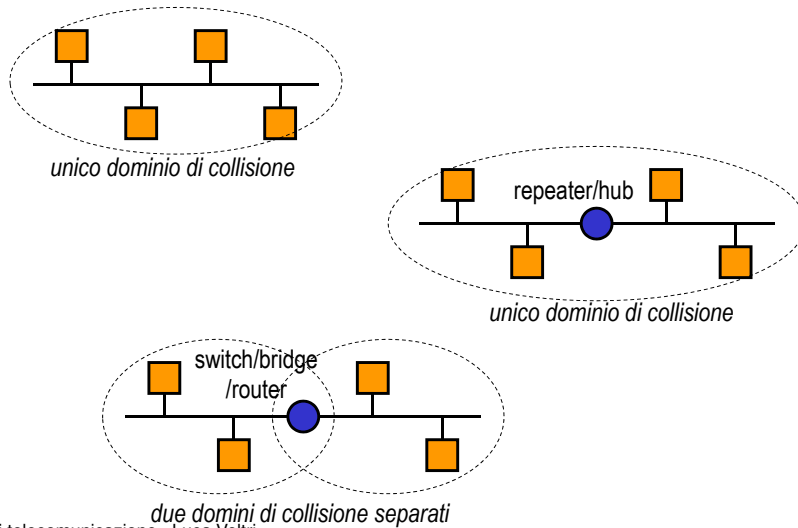
Domini di collisione: Hub vs Switch

- In una rete CSMA/CD al crescere del numero di stazioni e/o del traffico aumenta la probabilità di collisioni e quindi diminuisce l'efficienza della rete
- E' possibile suddividere la rete in più sottoreti in modo che la contesa del mezzo avvenga soltanto tra le stazioni appartenenti ad una singola sottorete, la quale rappresenta un singolo dominio di broadcast a livello fisico o dominio di collisione
- Le stazioni separate da repeater fanno parte dello stesso dominio di collisione (i repeater e gli hub sono nodi di relay che lavorano a livello PH)
- Appartengono a domini di collisione diversi le stazioni separate da apparecchiature di rete che lavorano a livelli superiori al fisico (bridge, switch)

Domini di collisione: Hub vs Switch



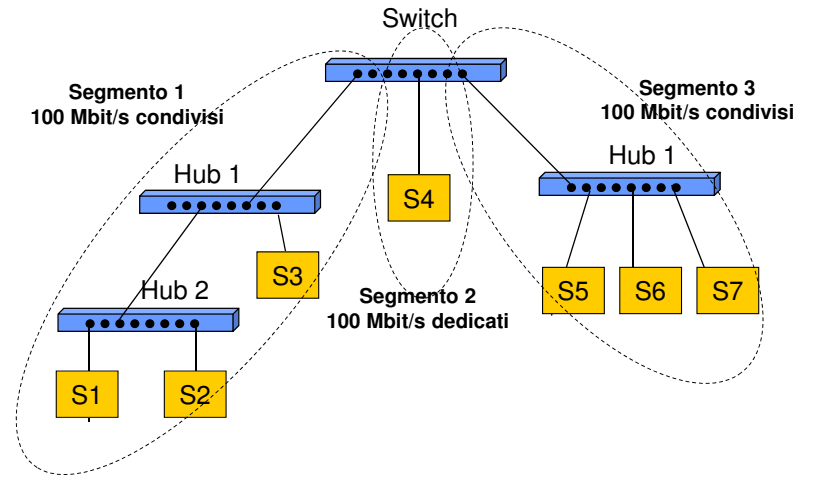
Domini di collisione: Hub vs Switch



Reti di telecomunicazione - Luca Veltri

49

Esempio di LAN con Hub e Switch



Reti di telecomunicazione - Luca Veltri

50

Ethernet Full-Duplex (1/2)

- Le LAN sono storicamente Half-duplex:
 - una sola stazione trasmette in un certo istante di tempo (mezzo trasmissivo condiviso)
- D'altra parte le connessioni tra due switch o tra switch e stazione Ethernet sono dedicate:
 - il mezzo trasmissivo diventa punto-punto
- Il mezzo trasmissivo punto-punto può allora essere usato in modalità Full-duplex (se supportata):
 - entrambe le stazioni possono trasmettere contemporaneamente
 - le trasmissioni avvengono su canali fisici diversi
 - due coppie separate del cavetto in rame
 - due fibre ottiche
 - assenza di collisioni, viene disattivato il CSMA-CD
 - la lunghezza di un link full-duplex dipende ora solo dalle caratteristiche del mezzo trasmissivo (non c'è dominio di collisione)
 - raddoppia la banda disponibile

Reti di telecomunicazione - Luca Veltri

51

Ethernet Full-Duplex (2/2)

- Per utilizzare Ethernet in modalità full-duplex:
 - il mezzo trasmissivo deve supportare trasmissioni full-duplex (twisted pair o fibra ottica)
 - connessione diretta tra due dispositivi "attivi" (link punto-punto)
 - connessione tra due switch
 - connessione stazione-switch o router-switch
 - connessione tra due stazioni
 - le schede di rete deve essere in grado di operare in full-duplex
 - nei transceiver deve essere disabilitata la rilevazione di collisioni
- Nota:
 - In modalità Half-duplex i transceiver inviano un segnale di collisione quando si ha la presenza di attività contemporanea su TX e RX
 - In modalità Full-duplex i transceiver non rilevano la collisione

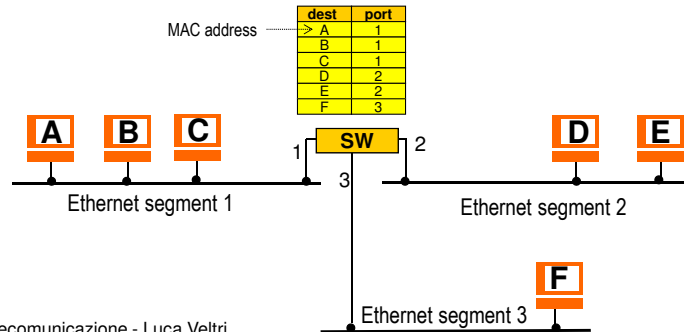
Reti di telecomunicazione - Luca Veltri

52

Switching

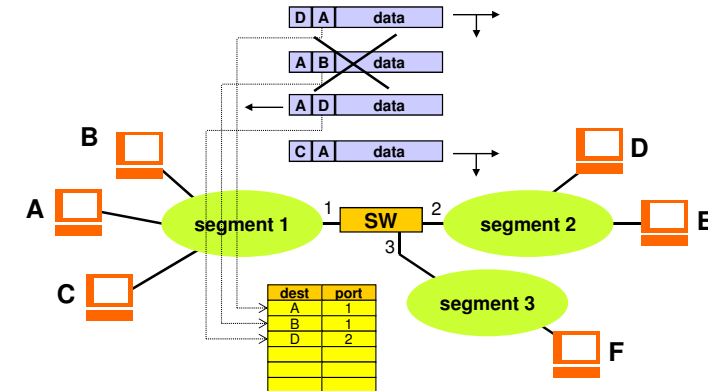
- I bridge/switch rilanciano le trame sulla base del loro indirizzo di destinazione
 - se è nota l'interfaccia attraverso la quale è raggiungibile la destinazione, la trama è rilanciata su questa interfaccia
 - altrimenti, la trama è rilanciata su tutte le interfacce tranne quella di provenienza

tabella di instradamento di SW



Switching (cont.)

- I bridge/switch "apprendono" la struttura di rete osservando il campo "Source Address" delle trame ricevute
 - le tabelle di instradamento vengono aggiornate in accordo a tali informazioni (backward learning)



Switching (cont.)

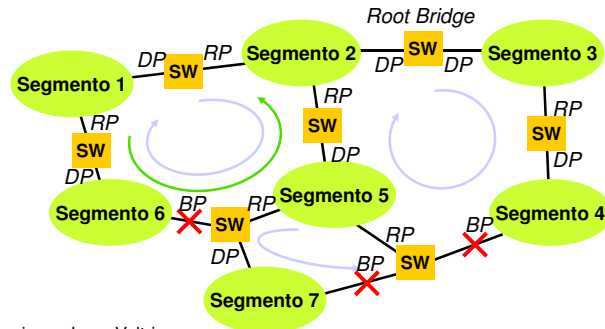
- Le tabelle di instradamento normalmente sono calcolate tramite apprendimento dinamico
 - **backward learning**
 - aggiornamento delle tabelle in base agli indirizzi di sorgente presenti nelle trame ricevute
- Il backward learning
 - funziona solo su reti con topologia ad albero
- In caso di rete magliata questa deve essere trasformata in albero
 - a questo scopo viene utilizzato un algoritmo/protocollo di spanning-tree (IEEE 802.1D)
 - gli instradamenti così ottenuti ("spegnendo" alcuni rami) non sono più quelli ottimali che sarebbero possibili nella rete magliata originale

Bridging e Switching

- Vantaggi
 - isolano il traffico aumentando la capacità trasmissiva totale e la sicurezza
 - Si configurano automaticamente
 - Permettono riconfigurazioni automatiche della rete in caso di guasti
- Svantaggi
 - Non adatti alla gestione di reti complesse
 - Non filtrano i pacchetti 'broadcast'
 - Non permettono il bilanciamento del traffico su link in parallelo o in generale su più percorsi

Spanning Tree Protocol (STP)

- Protocollo Spanning Tree
 - IEEE 802.1D (MAC Bridging and Spanning Tree), IEEE 802.1aq (Shortest Path Bridging), IEEE 802.1Q-2014 (virtual LAN)
 - ha lo scopo di trasformare una topologia magliata in albero
 - opera periodicamente
 - decide quali porte porre in stato di forwarding (RP e DP) e quali in stato di blocking (BP)



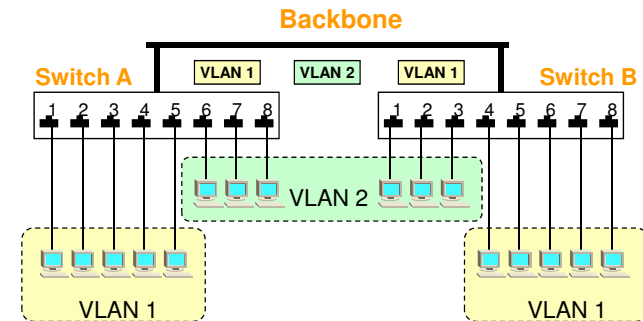
Spanning Tree Protocol (STP) (cont.)

- Bridge Protocol Data Unit (BPDU)
 - Invio in broadcast (all'indirizzo STP multicast 01:80:C2:00:00:00) di pacchetti BPDU
 - utilizzati per scambiare informazioni su bridge ID e costi dei "root path"
 - Configuration BPDU (CBPDU), per il calcolo dello Spanning Tree, sono inviate ogni 2sec
- Root bridge
 - il bridge con il più basso ID è il root bridge dello spanning tree
 - Bridge ID = priority ID + MAC address
- Cammini a costo minimo verso il root bridge
 - ad ogni segmento è associato un costo
 - il root bridge invia delle BPDU che vengono rilanciate dai bridge incrementando salto dopo salto il costo dal root bridge (ad ogni passo si somma il costo del segmento)
 - ogni bridge determina il cammino minimo verso il root bridge ("root path")
 - la porta utilizzata da questo cammino minimo diventa la "root port" (RP) del bridge
 - su ogni segmento i bridge determinano quello che ha il cammino minimo; la porta del bridge con cammino minimo che lo connette al segmento diventa la "designed port" (DP) del segmento
- Blocco delle porte
 - Ogni porta che non è né RP né DP viene bloccata, "blocked port" (BP)

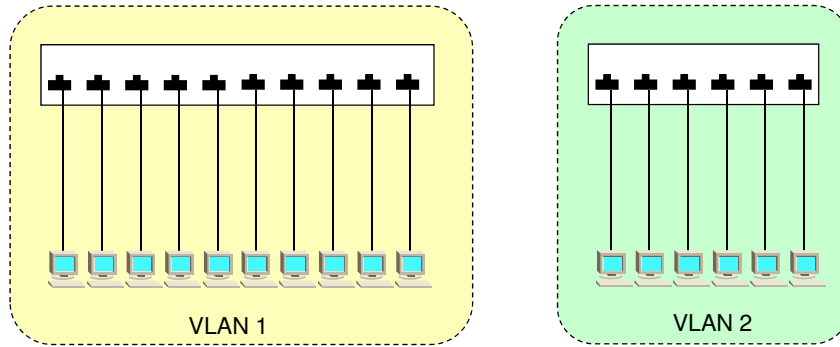
LAN virtuali (VLAN)

- Le LAN estese, quando crescono troppo di dimensione, sono fonte di problemi:
 - elevato traffico di multicast/broadcast
 - routing tra le sottoreti IP
 - sicurezza
- Si può introdurre il concetto di LAN virtuali:
 - unica infrastruttura fisica con apparati di rete
 - definizione di più sottoreti logiche separate tramite opportune configurazioni degli switch (domini Ethernet differenti)
 - Protocollo IEEE 802.1Q, utilizza meccanismo di tag (VLAN)
- Vantaggi
 - limitazione del traffico broadcast e multicast, impegnando banda trasmissiva e capacità elaborativa solo dove necessario
 - aumentare il livello di sicurezza limitando l'accesso a porzioni della rete fisica
- **allo stesso tempo, gestione dinamica di un'unica rete fisica**

Esempio di VLAN: struttura fisica



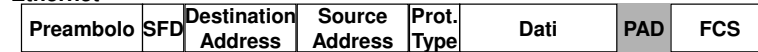
Esempio di VLAN: struttura logica equivalente



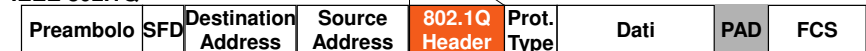
IEEE 802.1Q

- IEEE 802.1Q è lo standard per il supporto di LAN virtuali (VLAN) su reti Ethernet (IEEE 802.3)
- Lo standard definisce un meccanismo di etichettamento (VLAN tagging) delle trame Ethernet e le corrispondenti procedure che devono essere utilizzate nei Bridge/Switch
- Formato di una trama IEEE 802.1Q:

Ethernet



IEEE 802.1Q



- IEEE 802.1Q Header:
 - Tag protocol identifier (TPID): 16 bit, con valore 0x8100 per indicare una trama IEEE 802.1Q-tagged
 - Tag control information (TCI): 16 bit, che includono un VLAN ID di 12 bit

Standard per Wireless LAN

- 802.11 (1997)
 - prima versione dello standard IEEE 802.11 presentata nel 1997
 - velocità di trasmissione comprese tra 1 e 2 Mb/s
 - banda di frequenze IMS (Industrial Scientific & Medical) sui 2,4 GHz
 - differenti strati PH (FHSS, DSSS)
 - strato MAC di tipo CSMA/CA
- 802.11b (1999)
 - evoluzione dello standard per trasmissioni a 11 Mbit/s
 - banda di frequenze sui 2.4 GHz, modulazione CCK
 - in caso di cattiva copertura può lavorare a 5,5, 2 o 1 Mb/s
 - spettro diviso in 14 sottocanali da 22 MHz ciascuno
 - stesso MAC di tipo CSMA/CA
 - lo standard più diffuso
- IEEE 802.11i (2004)
 - miglioramento della sicurezza (WPA2)

Wireless LAN IEEE 802.11 (WiFi)

Standard per Wireless LAN (cont.)

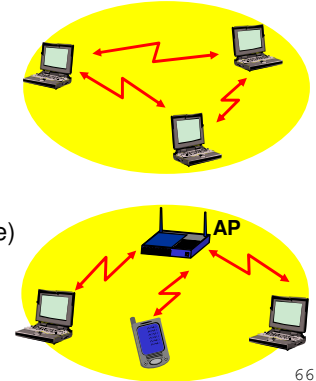
- 802.11a (2001)
 - velocità massima di 54 Mb/s sebbene la velocità reale disponibile all'utente sia di circa 20 Mb/s
 - la velocità massima può essere ridotta a 48, 36, 24, 18, 9 o 6
 - utilizza spazio di frequenze intorno ai 5 GHz, modulazione OFDM
 - poco utilizzato, anche perché in molti paesi l'uso delle frequenze a 5 GHz è riservato
- 802.11g (2003)
 - stesse frequenze dello standard 802.11b (banda di 2,4 GHz)
 - capacità teorica di 54 Mb/s con velocità reali di 24,7 Mb/s (simile a allo standard 802.11a)
 - totalmente compatibile con lo standard 802.11b
- 802.11n (2009)
 - velocità sino a 600 Mb/s
 - possibilità di operare sia intorno ai 2.4 GHz che 5 GHz

Reti di telecomunicazione include possibilità di utilizzare tecnologia MIMO

65

Basic Service Set (BSS)

- Basic Service Set (BSS)
 - gruppo di stazioni che sono sotto la stessa area di copertura (i.e. cella);
 - potenzialmente ogni stazione all'interno di una BSS potrebbe comunicare direttamente con un'altra
 - due modalità di funzionamento all'interno di un BSS
 - Ad-hoc mode
 - Infrastructure mode
- Modalità ad-hoc (Ad-hoc mode)
 - le stazioni si trovano in un unico BSS indipendente (IBSS)
 - solo stazioni all'interno del rispettivo raggio di copertura possono comunicare tra loro
- Modalità con infrastruttura (Infrastructure mode)
 - ogni stazione invia/riceve tutti i pacchetti ad/da un'unica stazione centrale chiamata AP (Access Point)

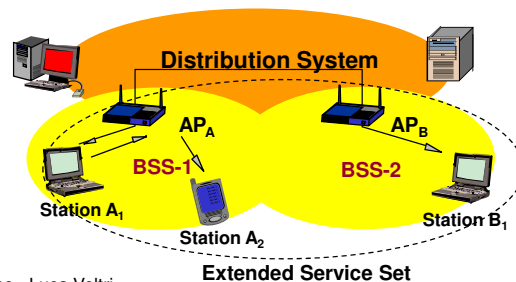


Reti di telecomunicazione - Luca Veltri

66

Extended Service Set (ESS)

- In una ESS, due o più reti senza fili (BSS) sono collegate tra loro tramite un "sistema di distribuzione" o Distribution System (DS), tipicamente una cablata
 - gli AP agiscono come bridge tra le BSS il DS
 - rilanciano tutti i pacchetti sul ramo di rete wireless o wired opportuno dove si trova la stazione di destinazione



Reti di telecomunicazione - Luca Veltri

67

802.11 MAC Layer

- Lo strato DL (MAC) del IEEE 802.11 implementa:
 - accesso al mezzo (MAC)
 - procedure di channel allocation
 - frame formatting
 - MAC-PDU addressing
 - error checking
 - fragmentation e reassembly
- Il MAC è basato su una tecnica di accesso denominata CSMA/CA (Carrier Sense Medium Access with Collision Avoidance)

Reti di telecomunicazione - Luca Veltri

68

802.11 MAC Layer

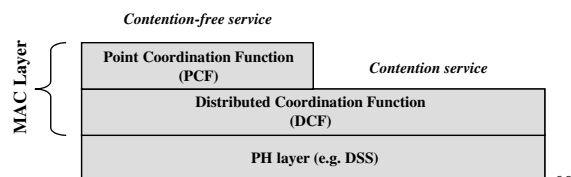
- Sono previste due differenti tipi di modalità di funzionamento per il MAC (spesso legate al fatto che si lavori in modalità ad-hoc o infrastructure):

- **Distributed Coordination Function (DCF)**

- sempre utilizzata nelle configurazioni di rete ad-hoc (IBSS), ma può essere usata anche in configurazione infrastructure (con AP)
- il mezzo lavora in Contention Period (CP)

- **Point Coordination Function (PCF)**

- può essere utilizzata solo se è presente un AP, cioè in ESS
- il mezzo lavora in Contention-Free Period (CFP)



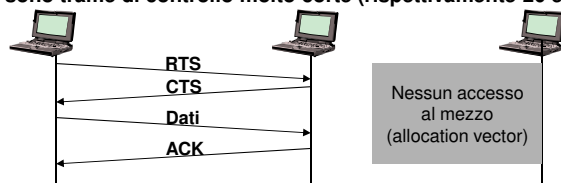
Distributed Coordination Function (DCF)

- E' il metodo di accesso fondamentale (deve essere sempre supportato) in grado di supportare modalità di trasferimento asincrono
 - **unico metodo di accesso possibile nel caso di modalità ad-hoc**
- DCF è una tecnica di accesso distribuita con collisioni e utilizza il CSMA/CA (Carrier Sense Multiple Access with collision Avoidance)
 - **collision detection (CSMA/CD) di Ethernet non può essere usato**
 - per l'impossibilità di trasmettere e contemporaneamente ascoltare lo stesso canale
 - le collisioni non potrebbero essere rilevate a causa del problema dei nodi nascosti
 - **carrier sense è realizzato sia a livello PH (PH carrier sensing) che MAC (virtual carrier sensing)**
 - **Il virtual carrier sensing è realizzato inviando informazioni sulla durata temporale di una trasmissione, all'interno dell'intestazione delle varie trame (MAC-PDU)**
 - **il collision avoidance è realizzato tramite trame di controllo Request To Send (RTS) e Clear To Send (CTS)**

DCF (cont.)

- Poiché in questa modalità possono accadere collisioni, prima di inviare una trama dati una stazione invia una trama di controllo di tipo Request To Send (RTS) che deve essere confermata dal ricevitore con una trama di Clear To Send (CTS)

- **RTS e CTS sono trame di controllo molto corte (rispettivamente 20 e 14 bytes)**

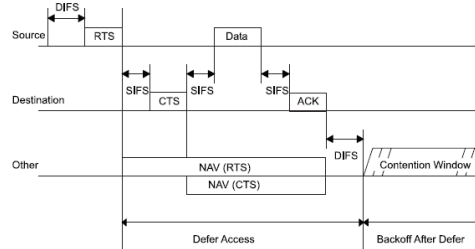
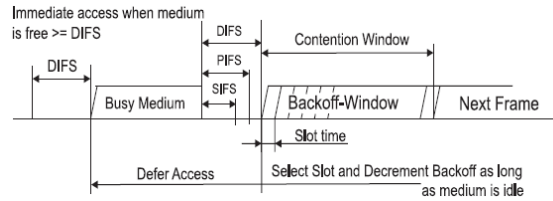


- Se avviene una collisione mentre si invia una trama RTS, il sender non riceve il corrispondente CTS, capisce che c'è stata una collisione e inizia una procedura di ritrasmissione del RTS ritardata con tempo di subentro incrementato esponenzialmente (exponential-backoff)
- L'algoritmo MAC risultante è equo, ma non garantisce un limite superiore al ritardo di trasmissione

DCF (cont.)

- Il campo *duration* di una MAC-PDU indica il tempo (μ s) che il canale sarà occupato dopo l'invio della trama corrente (compreso il relativo ACK)
- Le stazioni all'interno dello stesso BSS usano questa informazione per aggiornare il proprio "network allocation vector" (NAV) che indica la durata di tempo che il canale deve essere considerato occupato
- La priorità di accesso al canale dopo un periodo di occupato è controllato da un *interframe space* (IFS) variabile a seconda del tipo di trama che si vuole inviare
- Sono definiti tre tipi di IFS:
 - **short IFS (SIFS)**
 - **point coordination function IFS (PIFS)**
 - **distributed coordination function IFS (DIFS)**
- Stazioni che devono aspettare solo un SIFS hanno priorità di accesso rispetto a quelle che devono attendere un PIFS o DIFS
- Una stazione che riscontra il canale libero (fisicamente o virtualmente), aspetta un DIFS prima di controllare di nuovo il canale e trasmettere una MAC-PDU

DCF (cont.)



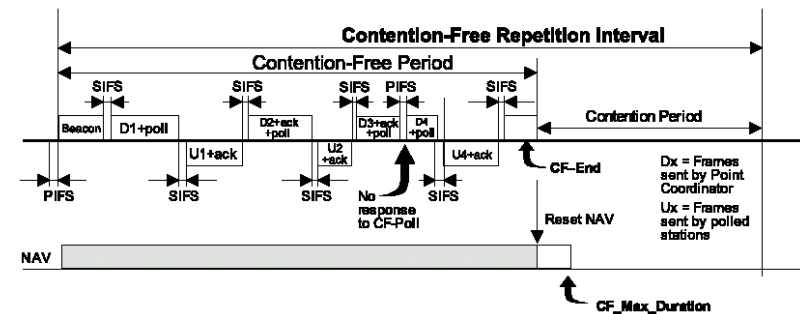
Point Coordination Function (PCF)

- PCF è una modalità di trasferimento opzionale (spesso non implementata) che garantisce un invio delle MAC-PDU senza collisioni
- PCF necessita di un AP (in ogni BSS), che periodicamente interroga le stazioni e le abilita alla trasmissione (senza competizione nell'accesso al mezzo)
- PCF deve poter coesistere con DCF
- L'asse dei tempi è diviso in intervalli di contention-free (CFP) alternati con intervalli di contention (CP)
- Durante un CFP non sono usate trame di RTS/CTS; è l'AP che indica alle singole stazioni (operazione di *poll*) quando possono iniziare a trasmettere

Point Coordination Function (PCF)

- All'istante di inizio nominale di un CFP l'AP ascolta il mezzo e, se libero, aspetta un PIFS e poi inizia il CFP con una trama di "beacon"
- Successivamente, possono essere inviate le seguenti trame:
 - CF-Poll (no data): usata dal AP per interrogare una stazione
 - Data: usata per trasmettere dei dati (dopo una CF-Poll)
 - Data+CF-Poll: usata dal AP per trasmettere dati e per interrogare una stazione
 - CF-ACK: usata da una stazione per confermare la ricezione di una trama dati (dopo un SIFS)
 - Data+CF-ACK: combinazione di Data e CF-ACK
 - Data+CF-ACK+CF-Pool: combinazione di CF-ACK + Data + CF-Poll
 - Null (no data): usata da una stazione come risposta a una CF-Poll se non ha dati da trasmettere
 - CF-End: usata dal AP per terminare un CFP

PCF (cont.)

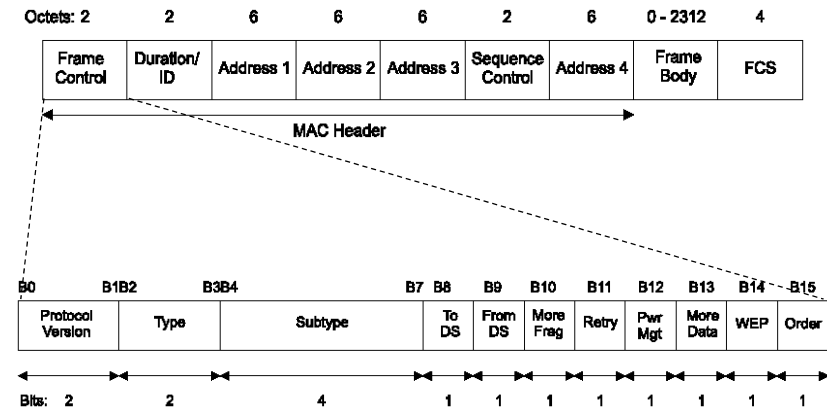


802.11 MAC Layer

Tre tipi di trame (frame):

- Trame di Management
 - usate per:
 - association/disassociation con un AP
 - timing e synchronization
 - authentication
- Trame di Controllo
 - usate per:
 - handshaking durante CP
 - acknowledgment positivi durante un CP
 - per chiudere un CFP
- Trame Data
 - usate per:
 - trasmettere dati durante un CP o un CFP, e possono essere combinate con trame di polling o acknowledgment

MAC-PDU format



Client-AP association

- Prima di iniziare a comunicare direttamente tra loro, due stazioni (e.g. un terminale e l'AP) devono stabilire una relazione denominata associazione
- Un terminale si riesce ad associare ad un AP nel seguente modo:
 - **tutti gli AP trasmettono periodicamente delle trame di management dette beacon**
 - **per associarsi ad un AP ed entrare così in un BSS, un terminale ascolta eventuali trame di beacon per identificare un eventuale AP**
 - **il terminale sceglie il BSS (tra vari possibili) in modi diversi, basati su pre-configurazione o su scelta dell'utente, ad esempio in base al nome della rete o SSID (Service Set ID) pubblicizzato**
 - **un terminale può anche inviare una trama di sollecitazione (trama di probe request management) specificando un particolare SSID richiesto**
 - **dopo aver identificato l'AP, il terminale inizia una procedura di mutua autenticazione utilizzando diverse trame di controllo**

Sicurezza nelle WLAN IEEE 802.11

- La protezione degli accessi e la sicurezza della comunicazione è un aspetto molto delicato nelle WLAN in quanto:
 - **la trasmissione avviene via radio esponendo i dati alla ricezione di utenti/stazioni non autorizzate**
 - è semplice ricevere il segnale delle WLAN
 - **poiché gli AP danno accesso alle stazioni wireless indipendentemente dalla loro posizione fisica, risulta molto più agevole introdursi all'interno di una rete**
- Lo standard originale IEEE 802.11 prevede alcuni meccanismi che possono essere utilizzati per tentare di proteggere la comunicazione
 - **Media Access Control (MAC) address filtering**
 - **Wired Equivalent Privacy (WEP)**
 - un protocollo di crittografia definito per lo standard originario IEEE 802.11, e in grado di garantire confidenzialità dei dati
 - ha come scopo quello di fornire una sicurezza simile a quella ottenibile tramite accesso wired
 - sfortunatamente è stato dimostrato essere assai debole e vulnerabile a vari tipi di attacchi

Tecnologie per la protezione delle WLAN

- Le debolezze dello standard originale vengono superate dai nuovi standard IEEE 802.1x e 802.11i, e altre tecnologie:
 - **Standard IEEE 802.1x, WPA**
 - filtraggio dei pacchetti non autorizzati, utilizzo di server di autenticazione, miglioramenti dell'algoritmo di cifratura
 - **Standard IEEE 802.11i, WPA2**
 - sostituzione del WEP con nuovo algoritmo di cifratura AES
 - **VPN IPSec**
 - sicurezza fornita a livello IP
 - **Captive portal**
 - autenticazione fornita a livello applicativo tramite browser, filtraggio a livello Ethernet
- La scelta della particolare tecnologia da usare dipende da vari fattori come
 - **scenario di utilizzo (accesso pubblico, aziendale, o residenziale)**
 - **tipologia dei terminale e applicativi**
 - **livello di sicurezza richiesto**