Capitolo 1

Livello collegamento e LAN

1.1 Il livello collegamento

I dispositivi che supportano un protocollo link-layer sono detti *nodi*. I canali di comunicazione che connettono nodi adiacenti sono detti *collegamenti*. Un nodo incapsula il datagramma ricevuto dal network layer sovrastante in un *link-layer frame* e lo trasmettono sul collegamento.

1.1.1 I servizi forniti dal livello collegamento

Incapsulazione

Quasi tutti i protocolli link-layer incapsulano i datagrammi ricevuti dal network layer prima di trasmetterli sul collegamento. Il frame è composto da un campo dati, dove viene inseito il datagramma, e degli header.

Accesso al collegamento

Un protocollo di medium access control (MAC) specifica come il frame deve essere trasmesso sul collegamento.

Trasporto affidabile

Un protocollo di trasferimento affidabile garantisce che ogni frame raggiunga la sua destinazione senza errori.

Individuazione e correzione degli errori

Il nodo mittente fornisce un meccanismo per individuare gli errori, che verranno poi corretti dal destinatario.

1.1.2 Implementazione del livello collegamento

Le funzionalità Ethernet sono integrate nella scheda madre o in un chip Ethernet. Il livello collegamento è implementato su un chip detto *network adapter* o *NIC*.

1.2 Individuazione e correzione degli errori

1.2.1 Controlli di parità

La forma più semplice di error detection è l'utilizzo di un bit di parità. Gli schemi di parità possono essere pari o dispari. Con uno schema di parità *bidimensionale*, dove i bit sono disposti a matrice, è

possibile identificare il bit corrotto e correggerlo. Questo schema non può correggere due errori in un singolo pacchetto, ma li può individuare.

1.2.2 CRC

I codici CRC (*cyclic redundancy check*) sono anche detti codici polinomiali in quanto è possibile considerare la stringa da inviare come un polinomio i quali coefficienti sono i valori 0 e 1 della stringa di bit. I CRC possono individuare $resto \leq$ bit errati consecutivi.

1.3 Multiple access link

Esistono due tipi di collegamento. Il collegamento *point to point* consiste in un solo mittente e un solo destinatario. Il collegamento *broadcast* può avere più nodi mittenti e destinatari connessi allo stesso canale di broadcast. Per coordinare la trasmissione di pacchetti all'interno di una rete broadcast, si utilizzano *protcolli di accesso multiplo*. Quando due o più nodi trasmettono frame allo stesso momento, i frame *collidono* e vengono persi. Esistono tre tipi di protocolli ad accesso multiplo.

1.3.1 Protocolli a partizionamento di canale

- *TDMA*: l'accesso al canale avviene in "round", e ogni nodo ha uno slot di tempo in cui può trasmettere in ognuno di questi round. Il tasso di trasmissione è R/N, e i canali inutilizzati vengono sprecati.
- *FDMA*: divide il canale da R bps in multiple frequenze e assegna ciascuna di queste frequenze ai nodi.
- *CDMA*: assegna un codice a ogni nodo, e ogni nodo usa quel codice per codificare i bit da inviare.

1.3.2 Protocolli ad accesso casuale

Con questi protocolli, il nodo mittente trasmette alla velocità concessa dal canale. Quando avviene una collisione, i nodi affetti ritrasmettono il pacchetto finchè non viene ricevuto, attendendo prima di ritrasmettere il pacchetto. Ogni nodo sceglie indipendentemente l'intervallo di ritrasmissione.

Slotted ALOHA

Assumiamo che i frame abbiano tutti la stessa dimensione L, il tempo sul canale sia diviso in slot di dimensione L/R, i nodi siano sincronizzati e se due frame collidono in un slot, tutti i nodi rilevano la collisione in quello slot. Sia p una probabilità tra 0 e 1.

- Quando un nodo ha un frame da inviare, attende fino al prossimo slot e lo trasmette.
- Se non si verifica una collisione, il nodo non ritrasmette.
- Altrimenti, il nodo rileva una collisione e ritrasmette il suo frame negli slot successivi con probabilità p finchè non riesce a ritrasmettere senza collisione

La probabilità introduce casualità, che rende più efficiente il protocollo. Slotted ALOHA permette a ogni nodo di trasmettere a full rate ed è decentralizzato, ma nelle collisioni gli slot vengono persi, possono esserci slot inutilizzati ed è necessario un meccanismo di sincronizzazione. Inoltre, non è molto efficiente: con un gran numero di nodi, solo il 37% degli slot viene effettivamente utilizzato.

CSMA

I protocolli CSMA e CSMA/CD seguono due regole:

- *carrier sensing*: un nodo ascolta sul suo canale prima di trasmettere; se il canale è occupato, attende
- *collision detection*: se un nodo rileva un altro nodo che sta trasmettendo sul canale, annulla la trasmissione

Nonostante il carrier sensing, le collisioni possono comunque avvenire a causa del ritardo di propagazione. Quando avviene una collisione, tutto il tempo impiegato a inviare un pacchetto viene sprecato. Il CSMA semplice non effettua collision detection.

CSMA/CD

CSMA/CD effettua collision detection, annullando una trasmissione se nota che il canale è occupato. Prima di ritrasmettere, il nodo attende una quantità di tempo casuale. Algoritmo CSMA/CD di Ethernet:

1. Ethernet riceve il datagramma dal livello rete e lo incapsula in un frame.
2. Se il canale è libero, trasmette, altrimenti attende.
3. Se non vengono rilevate collisioni, la trasmissione è andata a buon fine.
4. Altrimenti, la trasmissione viene annullata e viene inviato un segnale.
5. Ethernet entra in fase di *binary exponential backoff*: dopo la m-esima collisione, sceglie un numero K con $0 \leq 2^{m-1}$. Attende $512K$ bit volte e ritorna al punto 2, ripetendo fino al completamento della trasmissione.

1.3.3 Protocolli a turni

I protocolli a turni permettono di ottenere buone prestazioni sia con carichi leggeri che con carichi pesanti.

- *Polling protocol*. Un nodo viene scelto come nodo master. Questo interpella ognuno dei nodi con metodo round-robin. In questo modo, vengono eliminate le collisioni e non ci sono tempi morti. I principali svantaggi sono l'introduzione di un ritardo di polling, la latenza e il potenziale fallimento del nodo master.
- *Token-passing protocol*. Un frame apposito, detto token, viene passato in ordine tra i nodi. Quando un nodo riceve un token, lo tiene finchè ha dei frame da trasmettere. I principali svantaggi sono l'overhead introdotto dal token, la latenza e il fatto che il token rappresenta un potenziale punto di rottura.

1.4 Switched Local Area Networks

Gli switch utilizzano indirizzi propri al livello collegamento per inoltrare frame.

1.4.1 Indirizzamento nel livello collegamento e ARP

Indirizzi MAC

Le interfacce di rete degli host e dei router hanno indirizzi livello collegamento, ma non gli switch. Un indirizzo livello collegamento viene chiamato *indirizzo MAC*. Gli indirizzi MAC sono di solito lunghi 6 bytes (48 bit) e sono espressi in motazione esadecimale. Ogni interfaccia nella LAN ha un unico indirizzo

MAC e un (localmente) unico indirizzo IP. Ogni interfaccia possiede un unico indirizzo MAC perché questi sono controllati dalla IEEE.

Quando un'interfaccia vuole inviare un frame, inserisce l'indirizzo MAC di destinazione nel frame e lo inoltra sulla LAN. Se un mittente vuole inviare un frame a tutte le interfacce presenti sulla LAN, questo inserisce un indirizzo speciale, l'*indirizzo broadcast* nel frame.

ARP

ARP è il protocollo che si occupa della traduzione tra indirizzi IP e MAC, ma solo per interfacce sulla stessa sottorete.

Ogni host e router possiedono una *tabella ARP*, che contiene mappature tra indirizzi IP e MAC, e un valore di time-to-live che indica la durata di quella voce nella tabella.

Per ottenere l'indirizzo MAC del destinatario, un mittente invia sull'indirizzo MAC di broadcast un *pacchetto ARP*, attendendo la risposta del nodo con l'indirizzo IP corrispondente. Una volta ricevuta la risposta, il mittente aggiorna la sua tabella ARP.

Inviare datagrammi in un'altra sottorete

Come inviare un datagramma da un host A a un host B? Supponiamo A conosca l'indirizzo IP di B, l'indirizzo IP del router e l'indirizzo MAC del router (via ARP). Allora:

- A crea un datagramma con destinazione l'indirizzo IP B (non può conoscere il suo MAC)
- A incapsula il datagramma in un frame indirizzato al router
- il frame è ricevuto dal router e passato a IP
- il router determina la giusta interfaccia sulla quale inoltrare il datagramma
- il router incapsula il datagramma con destinazione indirizzo MAC di B

1.4.2 Ethernet

La LAN Ethernet originalmente utilizzava un bus coassiale per connettere i nodi, e i frame erano trasmessi in broadcast. Successivamente, il bus è stato rimpiazzato con uno switch, che a differenza dei router opera esclusivamente sul livello collegamento.

Struttura di un frame Ethernet

- *Preambolo.* Serve a sincronizzare le interfacce.
- *Indirizzo di destinazione.* Contiene l'indirizzo MAC di destinazione.
- *Indirizzo di provenienza.* Contiene l'indirizzo MAC di provenienza.
- *Tipo.* Serve all'interfaccia di destinazione per indirizzare il frame al giusto protocollo di livello rete.
- *Campo dati.* Contiene il datagramma IP.
- *CRC.*

Ethernet è connectionless e non affidabile.

1.4.3 Switch

Gli switch sono dispositivi operanti nel livello collegamento. Sono trasparenti gli host e ai router nella sottorete. Gli switch, come i router, hanno dei buffer per contenere i frame in eccesso.

Forwarding e filtering

Il *filtering* è la funzionalità degli switch che determina se un frame deve essere inoltrato o scartato. Il *forwarding* è la funzionalità che determina le interfacce alle quali il frame va inoltrato. Queste funzioni sono svolte tramite una *tabella di switching*. Questa tabella contiene informazioni su alcuni dispositivi presenti in LAN. Ogni voce contiene un indirizzo MAC, il numero di interfaccia dello switch che porta a quell'indirizzo, e quando quell'indirizzo è stato aggiunto alla tabella.

Supponiamo che un frame con indirizzo di destinazione DD-DD-DD-DD-DD-DD giunga a uno switch sull'interfaccia x. Lo switch consulta la sua tabella. Si possono verificare tre casi.

- Nessuna voce nella tabella corrisponde all'indirizzo DD-DD-DD-DD-DD-DD. Lo switch inoltra copie del frame a tutte le interfacce eccetto l'interfaccia x.
- È presente una voce corrispondente nella tabella, che associa l'indirizzo DD-DD-DD-DD-DD-DD con l'interfaccia x. Non serve imoltrare il frame ad altre interfacce, quindi viene scartato (filtering).
- È presente una voce corrispondente nella tabella, che associa l'indirizzo DD-DD-DD-DD-DD-DD con l'interfaccia $y \neq x$. Il frame viene inoltrato sul segmento della LAN corrispondente all'interfaccia y (forwarding).

Self-Learning

La tabella di uno switch viene riempita automaticamente, dinamicamente e autonomamente.

1. La tabella è inizialmente vuota.
2. Per ogni frame in arrivo, lo switch memorizza nella sua tabella l'indirizzo MAC del mittente del frame, l'interfaccia dal quale è arrivato e quando.
3. Lo switch elimina dalla tabella un indirizzo se nessun frame con quell'indirizzo viene ricevuto in un certo lasso di tempo.

Proprietà

- *Eliminazione delle collisioni.* In una LAN gestita tramite switch non ci sono collisioni. Gli switch bufferizzano i frame e non trasmettono più di un frame su uno stesso segmento.
- *Collegamenti eterogenei.* Poiché uno switch isola segmenti di LAN l'uno dall'altro, questi possono avere velocità differenti o operare su architetture differenti.
- *Gestione.* Uno switch semplifica la gestione della rete. Se un'interfaccia di un dispositivo si guasta e continua a inviare frame in broadcast, uno switch può rilevare il problema e disconnettersi dall'interfaccia malfunzionante.

1.4.4 VLAN

Le reti LAN tradizionali non sono facilmente scalabili o portabili, ma le VLAN sì. Uno switch che supporta VLAN permette di definire LAN virtuali su una singola LAN fisica. Gli host su una VLAN possono comunicare tra loro come se fossero solo loro connessi a quello switch.

Nelle VLAN basate su porte, le porte dello switch sono divise in gruppi. Ogni gruppo costituisce una VLAN, e le porte in ogni VLAN formano un dominio di broadcast. Per connettere due VLAN bisogna utilizzare un router.

Una soluzione più scalabile per connettere due VLAN è detta *VLAN trunking*. Una porta dello switch è designata come porta per connettere due VLAN. Questa porta appartiene a tutte le VLAN, e i frame inviati a ogni VLAN sono inoltrati su quel collegamento a un altro switch. I frame che passano per il trunk sono in uno speciale formato, detto 802.1Q. Questi frame sono identici ai frame Ethernet standard, ma possiedono una *tag VLAN* nell'header che contiene informazioni circa la VLAN alla quale il frame appartiene.

1.5 Networking nei data center

1.5.1 Architetture dei data center

I data center non sono solamente connessi a Internet, ma a dei loro network interni che connettono gli host tra loro. Gli host nei data center sono chiamati *blades*, impilati in rack. In cima ad ogni rack c'è uno switch, detto *Top of Rack* (TOR), che connette gli host nel rack tra di loro e con gli altri switch nel data center. Ogni host nel rack ha un'interfaccia di rete che si connette al proprio TOR, e ogni TOR ha porte che possono essere connesse ad altri switch.

I data center supportano due tipi di traffico: il traffico tra client esterni e host interni e traffico tra host interni. Per gestire il primo, i data center utilizzano dei *border router*, che connettono il data center con Internet.

Load balancing

Le richieste ricevute da un data center sono innanzitutto dirette a un load balancer che si occupa di distribuire le richieste agli host. I grossi data center possiedono molti load balancer, ognuno dedicato a specifiche applicazioni cloud. Un tale load balancer è spesso chiamato "layer-4 switch" in quanto basa le sue decisioni sul numero di porta e sull'indirizzo IP del pacchetto. Al ricevimento di una richiesta, il load balancer la inoltra a uno degli host che gestisce l'applicazione. Il load balancer funziona anche come NAT, in quanto traduce l'IP pubblico della richiesta nell'IP interno e viceversa.

1.6 Il processamento di una richiesta

Capitolo 2

Livello fisico

Capitolo 3

Reti wireless e mobili

3.1 Elementi delle reti wireless

Nelle reti wireless si possono identificare i seguenti elementi:

- *Host wireless.*
- *Collegamenti wireless.* Un host si connette a una base statio o un altro host wireless tramite un collegamento wireless.
- *Base station.* Gestisce l'invio e la ricezione dei dati da e a un host wireless associato. Gli host associati con una base station operano in *modalità infrastruttura.* Nelle *reti ad hoc*, gli host non hanno un' infrstruttura a cui connettersi.

Classificazione dei network wireless:

- *Single-hop, con infrastruttura.* Queste reti hanno una base station connessa a una rete più grande, e tutte le comunicazioni avvengono in uno solo wireless hop (4G LTE).
- *Single-hop, senza infrastruttura.* Non hanno base station connessa a una rete wireless (Bluetooth).
- *Multi-hop, con infrastruttura.* I nodi comunicano tra di loro prima di connettersi alla base station (wireless mesh networks).
- *Multi-hop,senza infrastruttura.*

3.2 Collegamenti wireless e caratteristiche

Problematiche dei collegamenti wireless:

- *Diminuzione della potenza di segnale.*
- *Interferenza da altre sorgenti.*
- *Propagazione multipath.*

Il *signal-to-noise ratio* (SNR) è la misura relativa della potenza del segnale ricevuto e del suo rumore. È misurata in decibel. Maggiore è il SNR, più facile diventa estrarre il segnale dal rumore di sottofondo.

Per un dato sistema di modulazione, maggiore è il SNR, minore sarà il bit error rate (BER). Un mittente può incrementare il SNR incrementando la potenza di trasmissione, ma ciò richiede più energia.

Per un dato SNR, una tecnica di modulazione con un bit transmission rate maggiore avrà un BER maggiore.

CDMA

In un protocollo CDMA, ogni bit inviato viene codificato moltiplicandolo per un segnale (il codice) che varia molto più velocemente (chipping rate) della sequenza di bit originale. Supponiamo che ogni bit trasmesso richieda uno slot di tempo da un bit. Sia d_i il valore del bit per lo slot $i-$esimo. Ogni slot è diviso in M mini-slot. Il codice CDMA utilizzato dal mittente consiste in una sequenza di M valori.

Per il $m-$esimo mini-slot del tempo di trasmissione del bit d_i, l'output del codificatore CDMA, $Z_{i,m}$, è pari a:

$$Z_{i,m} = d_i \cdot c_m$$

Il destinatario può recuperare la sequenza di bit originale calcolando:

$$d_i = \frac{1}{M} \sum_{m=1}^{M} Z_{i,m} \cdot c_m$$

Con più mittenti, il valore ricevuto dal destinatario è la somma dei bit trasmessi dagli N mittenti in quel mini-slot:

$$Z^*_{i,m} = \sum_{s=1}^{N} Z^s_{i,m}$$

Se i codici sono scelti in maniera opportuna, ogni destinatario può utilizzare la seconda equazione per recuperare i dati ricevuti.

3.3 Reti WLAN 802.11

Lo standard IEEE 802.11 wireless LAN, detto anche WiFi, è lo standard più utilizzato.

3.3.1 Architettura

Il blocco fondamentale dell'architettura 802.11 è il *basic service set* (BSS). Un BSS contiene una o più stazioni wireless e una base station centrale, detto *access point* (AP). Ogni wireless station possiede un indirizzo MAC.

Canali e associazioni

Quando un amministratore installa un AP, gli assegna un *service set identifier* (SSID) e un numero di canale. 802.11 definisce 11 canali parzialmente sovrapposti. Due canali non si sovrappongono solo se sono separati da 4 o più canali.

Per ottenere accesso a Internet, un dispositivo wireless deve associarsi con un AP. Un AP invia periodicamente dei *beacon frame* contenenti il proprio SSID e indirizzo MAC. Il dispositivo wireless scandisce gli 11 canali per individuare i beacon frame.

Il processo di scnadire i canali è detto *passive scanning*. Un dispositivo wireless può anche condurre *active scanning* inviando in broadcast un frame che viene ricevuto da tutti gli AP in range.

Una volta scelto l'AP al quale collegarsi, il dispositivo invia un frame di richiesta di associazione all'AP, e questo risponde con un frame di risposta. Una volta associato con un AP, il dispositivo invia un messaggio DHCP nella sottorete tramite l'AP per ottenere un indirizzo IP.

Per associarsi con un AP, il dispositivo potrebbe doversi autenticare. L'autenticazione può avvenire tramite indirizzo MAC o username e password. In entrambi i casi, l'AP comunica con un server d'autenticazione.

3.3.2 Il protocollo MAC 802.11