Reti di Calcolatori

Appunti delle Lezioni di Reti di Calcolatori

Anno Accademico: 2024/25

Giacomo Sturm

Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche
Università degli Studi "Roma Tre"

Sorgente del file LaTeX disponibile al seguente link:
https://github.com/00Darxk/Reti-di-Calcolatori/

Indice

1 Introduzione

Una qualsiasi interconnessione di calcolatori può rappresentare una rete di calcolatori, ma in base alla distanza reciproca tra questi componenti si tratta di reti differenti. Convenzionalmente si considerano reti di calcolatori, sistemi di calcolatori interconnessi ad una distanza superiore ai 50 cm. Una distanza minore, fino ai 5 cm, generalmente interessa componenti dello stesso computer, sulla stessa scheda madre, connesse tra di loro; mentre una distanza inferiore ai 5 cm rappresenta componenti sullo stesso chip. Inoltre le reti considerate possono essere ulteriormente divise in base alla distanza dei loro elementi:

- Se hanno una distanza minore di 5 km, si tratta di risorse connesse sulla stessa rete o edificio, o su edifici vicini. Questo tipo di rete si chiama Local Area Network (LAN);
- Se hanno una distanza superiore ai 5 km, si tratta di risorse connesse su una vasta area geografica. Questo tipo di rete si chiama Wide Area Network (WAN).

Tra questi due livelli possono essere presenti anche tecnologie molto diverse tra di loro, queste tecnologie vengono identificate da acronimi da cui è possibile ricavare lo scopo della tecnologia, senza tuttavia conoscere il suo funzionamento.

Una connessione tra componenti di una rete coinvolge sempre uno scambio di informazioni, tramite uno scambio di messaggi in serie. Gli elementi della rete effettuano degli accessi ad essa apparentemente in parallelo e simultanei, per poter comunicare tra di loro. Mentre su componenti sulla stessa macchina o sullo stesso chip avvengono tramite accessi ad una memoria condivisa.

Le connessioni tra componenti di una rete avvengono su uno strato fisico, quindi attraverso diversi mezzi trasmissivi, i quali non verranno analizzati approfonditamente a questo livello di astrazione. Tra i più comuni mezzi trasmissivi abbiamo cavi in fibra ottica, o in rame, ed onde radio.

1.1 Commutazione

Una rete di calcolatori può essere rappresentata come un grafo composto da vari nodi, per realizzare tutte le possibili coppie di calcolatori che potrebbero comunicare tra di loro attraverso la rete. Ma se venissero collegati individualmente tutte le possibili coppie di calcolatori necessiterebbe di infrastrutture massicce, poiché il numero dei possibili percorsi aumenta quadraticamente rispetto all'aumento dei calcolatori della rete. Infatti avendo n, tutte le possibili combinazioni tra questi calcolatori sono $n(n-2)/2$, nel caso ognuna di queste coppie corrisponda ad una connessione differente, il costo di costruzione e gestione della rete sarebbe eccessivo.

Per risolvere questo problema e diminuire il numero totale di connessioni nella rete si utilizza il meccanismo della commutazione. Questo termine risale alla telefonia, dove ai sorse lo stesso problema, risolto introducendo centralini intermedi dove si potevano collegare diverse area telefoniche contenenti i telefoni che tentavano di comunicare. In questo modo si può drasticamente diminuire il numero di connessioni individuali nella rete, e non bisogna integrare un numero elevato di connessioni all'aggiunta di un singolo elemento. Si indica quindi con commutazione di circuito questo meccanismo di creare una connessione fisica tra due calcolatori, connettendo diverse zone della rete attraverso nodi intermedi. L'interazione tra computer consiste intrinsecamente da grandi

quantità di dati trasmessi velocemente a grandi distanze, per cui hanno bisogno di infrastrutture dedicate massicce, si preferisce quindi questo sistema di nodi intermedi, nonostante non consenta di soddisfare contemporaneamente tutte le coppie di calcolatori.

Poiché questa grande quantità di dati deve attraversare la rete velocemente, si utilizza una diversa tecnica di comunicazione a livello dei singoli messaggi, dividendoli in pacchetti da spedire separatamene. Nella commutazione a datagramma questi pacchetti vengono spediti su linee anche diverse e si mescolano a tutti i pacchetti che attraversano quel percorso. Le linee non sono quindi ad uso esclusivo di una singola connessione. Ma per ricomporre il messaggio originale bisogna combinare questi pacchetti nello stesso ordine in cui sono stati separati, sono necessari dati aggiuntivi per poter riconoscere il loro ordine, perso durante la trasmissione. La distanza attraversata da ciascun pacchetto infatti non è garantito sia uguale.

Esiste inoltre un altro tipo di commutazione a circuito virtuale, dove i pacchetti vengono inviati sullo stesso percorso sequenzialmente, ed ogni linea può essere condivisa da un altro circuito virtuale, quindi non sono ad uso esclusivo. In questo caso invece è necessario un meccanismo per poter distinguere tra di loro questi circuiti virtuali sulla stessa linea fisica.

Si è risolto tramite la commutazione di pacchetto l'esclusività delle linee della rete, introdotta dal modello a commutazione di circuito.

La rete internet moderna utilizza la commutazione a datagramma, per motivi economici e gestionali. Altrimenti sarebbe necessario un gestore della rete che deve trovare un percorso ed attribuirlo ad una coppia ad ogni tentativo di connessione. Data la complessità della rete moderna, lasciare che i pacchetti trovino il percorso autonomamente è la scelta più efficiente. Per realizzare una commutazione a datagramma, piccole aree geografiche diverse vengono coperte da "Internet Service Provider" (ISP) differenti che possono comunicare solamente con altri ISP adiacenti. Quindi all'invio di un pacchetto, se il destinatario non è nella stessa zona dell'ISP corrente, questo lo invia ad un ISP adiacente che crede possa contenere il destinatario, così anche per la ricezione da un altro ISP. In caso il destinatario sia nella zona dell'ISP corrente, questo lo trasmette a lui. Accordi possono essere stipulati da chiunque a chiunque, un ISP ha sempre la necessità di trasmettere i pacchetti attraverso la rete.

In certi casi l'ISP può gestire la rete a circuito virtuale, se sia il destinatario che il mittente siano coperti dal singolo ISP.

1.2 Velocità

Nelle reti LAN e WAN si possono trasmettere dati a velocità diverse:

- LAN: velocità tra 10 ai 100 Mb/s;
- WAN: velocità tra 64 Kb/s ai 200-400 Mb/s.

Le reti WAN presentano hanno molti livelli di retrocompatibilità mantenuti, per cui si possono trasmettere dati a velocità minori di una rete LAN. In generale sono sempre richieste reti a velocità di trasmissione elevata, e connessioni ad alta velocità.

Data una rete si può definire la velocità in due modi differenti. Se si considera il tempo in cui il primo bit del messaggio arriva a destinazione. Le connessioni ad alta velocità vengono realizzate in

linee a fibra ottica, per cui i bit vengono inviati come impulsi di luce, e viaggiano ad una velocità costante, quindi per ogni rete la velocità di trasmissione di un singolo bit è la stessa. Si definisce quindi il tempo di ritardo o delay, il tempo per trasmettere un singolo bit, alla velocità della luce, sulla rete e dipende interamente dalla distanza.

Un pacchetto non viene rappresentato da un singolo bit, per cui non possono essere trasmessi alla stessa velocità, si definisce banda la quantità di bit trasmessi contemporaneamente sulla linea. Questa si chiama banda, e generalmente è sempre possibile comprare più banda in modo relativamente facile, ma è molto difficile comprare meno delay.

1.3 Gestione delle Risorse

La rete è essenzialmente un insieme di risorse interconnesse tra di loro e dalla teoria dei sistemi operativi, il loro controllo può essere descritto da varie attività:

- Verifica dei diritti d'accesso;
- Sequenziamento degli accessi alla risorsa;
- Esecuzione delle operazioni disponibili.

Ad ogni risorsa vengono assegnato almeno un gestore, di numero variabile in base al tipo di gestione. Le modalità di gestione delle risorse sono varie, si dividono in gestione autocratica e multilaterale. Nella gestione autocratica ogni risorsa ha un unico gestore associato ed univoco. Nella gestione multilaterale per ogni risorsa può esserci più di un gestore, si possono identificare quindi tre sottotipi di questa gestione:

- Gestione partizionata, dove attività di gestione viene effettuata da un singolo processo;
- Gestione successiva, dove tutte le attività di gestione vengono effettuate a turni da più processi;
- Gestione replicata, dove tutti i gestori partecipano a ciascuna attività, se ogni gestore ha peso decisionale uguale allora si tratta di gestione democratica.

La gestione replicata fornisce una forte resistenza ai guasti per un numero elevato di gestori che partecipano a ciascuna istanza di una attività, con alto grado di uguaglianza nella responsabilità di gestione. Sono abbastanza diffusi meccanismi di elezione per la scelta dei gestori.

2 Kathará

Le reti di calcolatori sono complicate, comprendono vari dispositivi, tra cui computer e router. Tante interfacce e protocolli diversi, collegati attraverso interconnessioni fisiche. Realizzano delle strutture topologiche molto vaste e complesse.

Si vuole sperimentare con reti anche molto complesse, senza utilizzare dispositivi fisici. Anche se si ha a disposizione una rete reale, sarebbe difficile convincere un provider a fornire a costi non eccessivi la loro rete per effettuare esperimenti su di essa. Realizzare una rete esclusivamente per effettuare questi esperimenti allo stesso modo si rivelerebbe estremamente costoso.

2.1 Introduzione

Kathará è un framework basato su container per effettuare esperimenti su reti di calcolatori, è un progetto open-source su github, per cui ognuno è in grado di contribuire allo sviluppo. Permette di effettuare emulazione di rete, differente da simulazione di rete. Negli strumenti di simulazione di un sistema si vogliono riprodurre le prestazioni di un sistema reale, la sua latenza, il ritardo, gli errori, la perdita di pacchetti, etc. Non si considerano le sue funzionalità, vengono analizzati solamente le prestazioni ed i parametri specifici della rete. Invece l'emulazione mira a riprodurre accuratamente le funzionalità offerte dal sistema, senza limitazioni di prestazioni. In questo caso le prestazioni rappresentano aspetti marginali della rete.

Per emulare una rete si utilizza una macchina in funzione da host, all'interno della quale vengono eseguiti container autonomi. Essenzialmente macchine isolate, queste vengono poi collegate da fili virtuali, in modo da simulare la presenza di una rete fisica, nonostante sia effettuata su una singola macchina. In Kathará i container sono collegati tra di loro in domini di collisione virtuali, non fili virtuali, per motivi di praticità. Questo consente di collegare l'host ad ogni dominio di collisione, per poter analizzare il comportamento su tutta la rete. Utilizzando fili virtuali invece non sarebbe stato così semplice da implementare.

Ciascuno dei container viene configurato come un dispositivo, in principio sono tutti uguali, ma possono rappresentare computer, router, switch, etc. Per rappresentare tutti gli elementi di una rete realisticamente.

I container rappresentano una virtualizzazione leggera, non sono macchine virtuali, quindi viene emulato un altro sistema operativo al loro interno, ma solamente un'applicazione o una piccola parte di un sistema operativo. Sono quindi molto leggeri, con un tempo di avvio ridotto rispetto alle macchine virtuali, utilizzate generalmente per realizzare micro-servizi che godono di vita autonoma.

Per Kathará viene utilizzato il sistema Docker, il più ampiamente utilizzato a livello globale per realizzare virtualizzazioni leggere. Per realizzare un container è necessaria un'immagine, ovvero un'insieme di software e le loro librerie e binari, necessari alla loro esecuzione, statici. Sono disponibili diverse immagini per realizzare dispositivi diversi, ma in questo corso verrà utilizzata solamente l'immagine di base presente in Kathará. Tramite quest'immagine è possibile realizzare un computer, un router, un bridge ed è possibile inserire al suo interno applicazioni di tipo server, servizi web, etc. Tutti gli elementi necessari per effettuare esperimenti di rete in questo corso. Ogni container poiché rappresenta un'esecuzione isolata di un'immagine, può essere costruiro su

un'immagine diverse, oppure di versione diversa dagli altri container in esecuzione, senza influire sul funzionamento di Kathará.

Un dispositivo si presenta con un terminale, su cui possono essere eseguiti comandi specifici a quel dispositivo, una memoria dedicata, un filesystem e zero o più interfacce di rete. Ogni interfaccia di rete è connessa ad un unico dominio di collisione. Tutte le interfacce trattate rispetteranno il protocollo 4.3 per comunicare tra di loro.

Kathará dispone di tre tipi di comandi:

- "v-commands": utilizzano il carattere `v` come prefisso, e sono comandi di basso livello per configurare ed avviare un singolo dispositivo;
- "l-commands": utilizzano il carattere `l` come prefisso, e permettono di gestire un intero "lab", configurandolo ed avviandolo;
- "Global commands": sono comandi principalmente di gestione.

I v-commands sono:

- `vstart`: comando di avvio di un dispositivo;
- `vconfig`: aggiunge un file di configurazione ad un dispositivo attualmente in esecuzione;
- `vclean`: termina l'esecuzione di un dispositivo.

Gli l-commands sono:

- `lstart`: comando di avvio di un lab;
- `lconfig`: permette di effettuare operazioni di configurazione su un dispositivo di un lab già attivo;
- `lclean`: termina l'esecuzione del lab;
- `lrestart`: termina e riavvia tutti i dispositivi del lab;
- `linfo`: fornisce informazioni sul lab.

I global commands sono:

- `check`: controlla l'ambiente del sistema, per controllare che l'installazione è andata a buon fine;
- `connect`: permette di collegarsi ad una macchina di Kathará già attiva;
- `list`: mostra tutti le macchine di Kathará in esecuzione per l'utente corrente;
- `settings`: mostra e configura le opzioni di Kathará;
- `wipe`: elimina tutte le macchine di Kathará, le loro connessioni ed eventuali opzioni.

Per testare il funzionamento di Kathará dopo l'installazione è consigliabile utilizzare i seguenti comandi:

```
> kathara check
```

Per controllare il suo corretto funzionamento si può testare la creazione di una singola macchina:

```
> kathara vstart -n pc1 --eth 0:A
```

Si crea una macchina di nome `pc1`, tramite l'opzione `-n` e si connette al dominio di collisione `A` con l'opzione `--eth 0:A`, che specifica anche il tipo di connessione virtuale, in questo caso ethernet. Se non vengono sollevati errori dopo questi comandi, si può interrompere la sua esecuzione con:

```
> kathara vclean -n pc1
```

Un lab di Kathará è un insieme di dispositivi che possono essere avviati e terminati contemporaneamente. La loro struttura consiste in una directory principale del lab, sempre contenente il file `lab.conf`, dove viene descritta la topologia della rete. Se sono è necessario, sono presenti subdirectories dove vengono specificate le configurazioni per i singoli dispositivi. Inoltre per ciascun dispositivo è ipotizzabile la presenza di un file chiamato con il nome del dispositivo di tipo `.startup` dove vengono descritte le operazioni da effettuare dal dispositivo all'avvio.

Negli esercizi ed in sede d'esame non sarà richiesto di realizzare un lab, ma si dovrà analizzare il comportamento di lab preesistenti, agendo sulle reti ed in caso correggendo eventuali errori o bug.

Il file `lab.conf` descrive la topologia della rete ed i dispositivi che devono essere avviati all'avvio del lab. Contiene istruzioni di sintassi:

```
<machine>[<arg>]=<value>
```

Dove `<machine>` è il nome della macchina su cui si vuole effettuare una certa operazione, `<arg>` è il tipo di operazione da effettuare su quella macchina. Se questo argomento è un numero indica a quale interfaccia della macchina si riferisce l'assegnazione, ovvero connessione ad un certo dominio di collisione, di valore specificato dal termine `value`.

Per avere un dispositivo nel lab, questo deve essere citato nel file di configurazione. Non è possibile riferirsi ad un'interfaccia successiva, se non si è già assegnata la sua precedente. Gli unici caratteri consentiti per definire il nome di una macchina o il nome di un dominio di collisione sono caratteri alfanumerici, dove lettere maiuscole e minuscole vengono considerate uguali.

I filesystem di tutte le macchine sono indipendenti ed isolati dal filesystem della macchina host, ma sarebbe conveniente il alcuni casi poter accedere e scrivere su file nella macchina host, per salvare una serie di dati, da analizzare dopo la terminazione delle macchine. Esistono due diverse modalità per permette un'interfaccia tra i filesystem della macchina host e dei vari dispositivi. Si possono condividere file tra i due filesystem direttamente, in modo che ogni cambiamento su uno dei due sia riflesso anche nell'altro. Oppure è possibile condividere una copia del file, in modo da avere due file indipendenti contenenti le stesse informazioni, quest'ultima è certamente la più semplice, ma la meno funzionale. Su Kathará sono presenti entrambi questi approcci. Utilizza una cartella `/shared` all'interno del lab, contenuta nei filesystem di ogni dispositivo in esecuzione in quel lab per condividere direttamente un file. Questa condivisione è abilitata di default, ma è possibile

modificarlo nelle impostazioni. Invece per condividere una copia di un file si possono utilizzare le subdirectories di un dispositivo, direttamente collegate alle subdirectories del lab di quello specifico dispositivo. In queste stesse subdirectories sono contenuti i file di avvio `.startup` delle singole macchine. Contengono comandi shell da essere eseguiti all'avvio, per configurare le interfacce di rete o avviare certi servizi di rete.

Per avviare un lab di Kathará bisogna aprire una Powershell, su Windows, e navigare alla directory del lab. In questa directory vanno eseguiti i vari l-commands, per avviare o terminare l'esecuzione di un lab.

Per evitare eventuali complicazioni, in questi laboratori si disabilita l'opzione per il protocollo IPv6, poiché genera complicazioni di semantica di difficile interpretazione.

2.2 Laboratorio del 16 Ottobre

In questa esercitazione si vuole emulare la una connessione tra due calcolatori `PC1` e `PC2`. Vengono specificate le ultime due cifre del MAC address: `0:1` e `0:2`. Viene consigliato di rappresentare la topologia della rete, descritta nel file `lab.conf`, i file di estensione `.startup` sono i comandi eseguiti dalle ciascuna macchine all'accensione. In questo laboratorio, non ci sono comandi da eseguire all'avvio. Non sono presenti neanche cartelle, per cui la configurazione di queste macchine è estremamente basilare

Il file `lab.conf` contiene all'inizio i meta dati del file:

Seguono le dichiarazioni ed assegnazioni dei computer nel laboratorio. Dove si specifica il nome della macchina, e tra parentesi quadre l'opzione da assegnare. Si indica con 0 l'interfaccia `eth0`. La stringa assegnata consiste nel dominio di collisione specificato `A`.

Senza specificare l'indirizzo, Kathará utilizza un indirizzo casuale, per cui in molti di questi laboratori gli indirizzi MAC di queste macchine verranno assegnati per renderli facilmente leggibili:

```
pc1[0]="A/00:00:00:00:00:01"
```

Con `image` viene specificata l'immagine di docker utilizzata dal calcolatore, contiene tutti gli strumenti necessari per mandare, ricevere e analizzare i pacchetti:

```
pc1[image]="kathara/base"
```

La terza riga di assegnazione consiste nella configurazione del protocollo IPv6, protocollo molto invasivo, per cui si vederebbero dati non di interesse in questo esercizio in particolare:

```
pc1[ipv6]="false"
```

Quindi si disattiva questo protocollo. Analogamente si configura la macchina 2:

```
pc2[0]="A/00:00:00:00:00:02"
pc2[image]="kathara/base"
pc2[ipv6]="false"
```

Inoltre è possibile modificare l'indirizzo IP di un calcolatore nella rete tramite il comando `ip` si accedono a tutti i comandi sulle reti. Il termine `link` indica a quale livello appartiene il comando, in questo caso il livello due di link. Si specifica quale protocollo deve essere modificato con `set dev eth0`, e si specifica cosa viene modificato, in questo caso l'indirizzo `address`:

```
prompt> ip link set dev eth0 address 00:00:00:00:01
```

Per avviare Kathará si apre una powershell all'interno della cartella del laboratorio, dopo aver avviato docker, e si avvia con il comando:

```
prompt> kathara lstart
```

Se viene modificato il file in `lab.conf` bisogna riavviare Kathará con il comando `lrestart`. Si chiude invece con il comando `lclean`.

All'avvio apre due terminali per entrambe le macchine, e vengono specificati i domini di collisioni e le connessioni definite nel file `.conf`. Per determinare la configurazione di un certo livello si utilizza sempre il comando `ip`, seguito dal livello che s vuole analizzare:

```
prompt> ip link
```

Al'interno di ciascuna delle macchine viene installato uno strumento chiamato `scapy`, una libreria in python utilizzata per creare pacchetti, ed in particolare gestire e modificare pacchetti. In questo modo si avvia il prompt di `scapy`, e si esce con il comando `exit`.

Questo terminale permette di creare un pacchetto ed inviarlo. Si crea una variabile `p` a cui assegnare il pacchetto. Si indica che si tratta di un pacchetto ethernet con `Ethernet()`, dove bisogna specificare gli indirizzi MAC del mittente e del destinatario:

```
prompt> p=Ethernet(dst:'00:00:00:00:00:01', src='00:00:00:00:00:02')
```

In questo modo è possibile specificare indirizzi MAC arbitrari, anche non presenti nella rete, e Kathará permette di analizzare questi comportamenti anomali. Il resto dei campi non specificati vengono inizializzati ad informazioni di default.

Per inviare un pacchetto si utilizza la funzione `send()`, che prende come argomenti il nome della variabile a cui è stato assegnato il pacchetto `p` ed il protocollo a cui viene inviato assegnato ad `iface`:

```
prompt> send(p, iface='eth0')
```

Esistono delle tecnologie chiamate "packet sniffer", come Wireshark, per controllare il traffico di rete. Questo viene specificato nelle ultime righe del file di configurazione, questa macchina tuttavia non è collegata, si dice fluttuante e sarà utile per analizzare il traffico su queste reti emulate.

```
wireshark[bridged]=true
wireshark[port]="3000:3000"
wireshark[image]="lscr.io/linuxserver/wireshark"
wireshark[num_terms]=0
```

L'ultima configurazione determina quanti terminali di Wireshark aprire all'avvio di Kathará. Si specifica 0, poiché si vuole utilizzare l'interfaccia grafica, e poiché in questi laboratori non si utilizzeranno comandi sul terminale i Wireshark.

Contiene un'immagine di Wireshark, chiamata analogamente per semplicità. Quest'applicazione viene avviata all'avvio del laboratorio. Questa macchina ha un'interfaccia grafica disponibile. Con il comando `lconfig` è possibile aggiungere un'interfaccia ad una macchina ad uno specifico link. Si specifica il nome della macchina con `-n` e si può specificare di aggiungere o rimuovere l'interfaccia con `--add` o `--rm`:

```
prompt> kathara lconfig -n wireshark --add A
```

Questo comando viene eseguito all'interno dell'hub del laboratorio, si utilizza per collegare questa macchina al dominio di collisione A. Nello stesso terminale dove è stato eseguito il laboratorio.

Il comando `bridged` connette la macchina all'host, con il comando `port` si specifica la porta dove la macchina condivide l'interfaccia grafica. Si accede tramite l'indirizzo `localhost:xxxx` dove viene specificata la porta inserita nella configurazione. Cliccando due volte sul nome dell'interfaccia, si possono analizzare i pacchetti inviati su quella connessione. Bisogna analizzare la connessione `eth1`, poiché la `eth0` viene inizializzata all'avvio di Kathará ed è connessa all'host. Il protocollo su vengono spediti i pacchetti creati, non essendo specificato.

Si può utilizzare la cartella `shared` costruita ogni volta che viene costruito il laboratorio, condivisa tra la macchina dispositivo e la macchina host. In questo modo è possibile utilizzare uno sniffer diverso da Wireshark per catturare i pacchetti. Si può effettuare quest'operazione tramite i comandi Linux `tcpdump`, con l'opzione `-tenny`, una composizione di tutte le flag necessarie per configurare il comando. Quando si manda un pacchetto, si può vedere il pacchetto sul terminale, direttamente. Aggiungendo l'opzione `-w` si può creare un file della cattura, di estensione `.pcap` "Packet Capture". Per salvare questo file nella cartella `shared`, condivisa, bisogna effettuare il comando in questa cartella. Ed è possibile aprirlo tramite Wireshark nella macchina host, per analizzare i pacchetti offline rispetto alla cattura.

2.3 Laboratorio del 25 Ottobre

In questo laboratorio si utilizza un bridge che collega quattro macchine su quattro domini di collisione differenti:

```
pc1[0]="A/00:00:00:00:00:01"
pc1[image]="kathara/base"
pc1[ipv6]="false"
pc2[0]="B/00:00:00:00:00:02"
pc2[image]="kathara/base"
pc2[ipv6]="false"
pc3[0]="C/00:00:00:00:00:03"
pc3[image]="kathara/base"
pc3[ipv6]="false"
pc4[0]="D/00:00:00:00:00:04"
pc4[image]="kathara/base"
pc4[ipv6]="false"
```

Ed una macchina che si comporta come bridge b1:

```
b1[0]="A/00:00:00:00:00:b1"
b1[1]="B/00:00:00:00:00:b2"
b1[2]="C/00:00:00:00:00:b3"
b1[3]="D/00:00:00:00:00:b4"
b1[image]="kathara/base"
b1[ipv6]="false"
```

Per permettere questo comportamento bisogna aggiungere un'interfaccia bridge con il seguente comando, che utilizza software per realizzare bridge, già presenti nei sistemi Linux. Si utilizza il software `ip link`, già utilizzato precedentemente:

```
root@b1:~$ ip link add name mainbridge type bridge
```

In questo modo si crea l'interfaccia di nome `mainbridge`, e di tipo `bridge`, all'interno della macchina b1.

Dopo aver creato il bridge bisogna connettere le diverse interfacce della macchina al bridge appena creato. Questo processo prende il nome di "enslaving", si realizza impostando il bridge come il master di quell'interfaccia, tramite il seguente comando:

```
root@b1:~$ ip link set dev eth0 master mainbridge
```

Questo va effettuato su ogni dominio di collisione a cui è connesso il bridge.

Quando viene realizzato il bridge, di default è spento e per attivarlo, o per fermarlo `set down`, si utilizza un ulteriore comando:

```
root@b1:~$ ip link set up dev mainbridge
```

Per controllare i bridge si utilizza un'altra serie di comandi già presenti in Linux, chiamata `brctl`, per "Bridge Control". Quando un bridge riceve un pacchetto, il MAC address del mittente viene salvato per un certo periodo di tempo nel suo filtering database. Dato che questo database è dinamico, il MAC address viene rimosso dopo un tempo di invecchiamento, di default di 5 minuti, o 300 secondi. Per modificare questo tempo si inserisce nel seguente comando come parametro, in secondi:

```
root@b1:~$ brctl setageing mainbridge 600
```

Bisogna specificare il nome del bridge precedentemente creato `mainbridge` ed il tipo di operazione da effettuare `setageing`.

Considerando questi comandi, il file `b1.startup`, permette di avere un bridge funzionate ed attivo ad avvio del lab:

```
ip link add name mainbridge type bridge
ip link set dev eth0 master mainbridge
ip link set dev eth1 master mainbridge
ip link set dev eth2 master mainbridge
ip link set dev eth3 master mainbridge
ip link set up dev mainbridge
brctl setageing mainbridge 600
```

Durante il lab per osservare il filtering database del bridge si può utilizzare il comando `showmacs`, che restituisce una tabella, contenente la porta, l'indirizzo MAC corrispondente. Inoltre contiene un'indicazione se quell'indirizzo MAC è locale, all'avvio infatti conosce automaticamente gli indirizzi MAC delle sue interfacce locali; ed il tempo di invecchiamento. Se un MAC è locale, il suo tempo non viene aumentato:

```
root@b1:~$ brctl showmacs mainbridge
port no mac addr            is local?   ageing timer
 1      00:00:00:00:00:b1   yes             0.00
 1      00:00:00:00:00:b1   yes             0.00
 2      00:00:00:00:00:b2   yes             0.00
 2      00:00:00:00:00:b2   yes             0.00
 3      00:00:00:00:00:b3   yes             0.00
 3      00:00:00:00:00:b3   yes             0.00
 4      00:00:00:00:00:b4   yes             0.00
 4      00:00:00:00:00:b4   yes             0.00
```

Il primo parametro indica il numero di porta del bridge, su un kernel Linux, il massimo numero di porte disponibili è di 1024, queste vengono assegnate sequenzialmente a partire da 1, nell'ordine in cui sono state connesse.

Se viene inviato un pacchetto da una delle stazioni, il bridge è in grado di imparare il suo MAC address:

```
root@pc1:~$ scapy
>>> p=Ether(dst='00:00:00:00:00:02', src='00:00:00:00:00:01')
>>> sendp(p, iface='eth0')
Sent 1 packets.
>>>
```

Dopo l'invio di questo pacchetto, il bridge conosce la posizione nella rete della stazione `pc1`:

```
root@b1:~$ brctl showmacs mainbridge
port no mac addr            is local?   ageing timer
    1      00:00:00:00:00:01   no             18.54
    1      00:00:00:00:00:b1   yes             0.00
    1      00:00:00:00:00:b1   yes             0.00
    2      00:00:00:00:00:b2   yes             0.00
    2      00:00:00:00:00:b2   yes             0.00
    3      00:00:00:00:00:b3   yes             0.00
    3      00:00:00:00:00:b3   yes             0.00
    4      00:00:00:00:00:b4   yes             0.00
    4      00:00:00:00:00:b4   yes             0.00
```

Se si invia un pacchetto con l'indirizzo MAC sorgente errato, allora il bridge non è in grado di imparare la posizione delle stazioni e quindi invierà pacchetti nei domini errati, impedendo ai pacchetti di arrivare a destinazione.

3 Modello ISO-OSI

Per il funzionamento della rete gli standard sono strettamente necessari, altrimenti non sarebbe possibile una comunicazione tra un mittente ed un destinatario qualsiasi, alcuni di questi standard vengono imposti dalla case costruttrici, altri vengono definiti da organizzazioni internazionali, nell'ambito informatico o delle telecomunicazioni. Alcune di queste associazioni come IETF sono indipendenti da stati nazionali, dove varie aziende o istituzioni propongono modifiche di vecchi standard o introduzione e definizione di nuovi.

Il modello ISO-OSI rappresenta un importante strumento di classificazione nel modo delle reti. Venne realizzato in parte e sostanzialmente dismesso, ma nonostante questo viene utilizzato a livello globale.

Questo modello si basa sull'architettura stratificata di hardware o software, dove partendo da un nucleo centrale il sistema viene diviso in livelli o strati indipendenti dal livello inferiore, ed uno strato fornisce servizi solamente allo strato immediatamente superiore. Avanzando da uno strato al superiore i servizi vengono mostrati in modo sempre più astratto ed il sistema aumenta progressivamente di utilità. Per la sua utilità questo tipo di architettura stratificata permane molti campi dell'informatica.

La rete viene divisa in 7 livelli numerati dal basso verso l'alto, il livello indica la funzione delle tecnologie che vi appartengono e questo fornisce uno strumento di classificazione per analizzarle senza dover conoscere i loro meccanismi interni.

Ogni strato rappresenta un diverso livello di astrazione ed offrono funzioni ben definite. Poiché ognuno di questi strati è indipendente dal livello inferiore, viene minimizzato lo scambio di informazioni tra strati. Il numero dei livelli venne scelto in base alle funzioni distinte di una rete da descrivere e dalla realizzabilità.

All'interno di ogni strato si possono individuare diverse "entità", hardware o software dove sono contenuti i protocolli di quel livello. Per offrire servizi allo strato superiore, è presente un punto logico chiamato "Service Access Point" (SAP) al quale può accedere il livello superiore. L'unico punto di contatto tra livelli e quello inferiore è la loro interfaccia. Un protocollo è un linguaggio utilizzato da entità dello stesso livello, quindi entità di uno stesso strato possono comunicare con le adiacenti tramite protocolli e con superiori tramite SAP, ed inferiori tramite interfaccia.

Secondo questo modello i pacchetti sono contenuti in altri pacchetti, destinati a livelli inferiori, per cui quando vengono ricevuti da un livello $n-1$, viene letto il pacchetto di livello $n-1$ ed estratto il pacchetto di livello n contenuto ed inviato all'entità di livello n. I protocolli su uno stesso strato possono comunicare con altre entità dello stesso livello, e possono inviare indicazioni o conferme a richieste di entità utenti del servizio del livello superiore.

I dati generati da un protocollo di livello n sono detti n-pdu, "Protocol Data Unit", composti da un header indirizzato all'entità di livello n ed una payload, contente un $n+1$-pdu, destinata al livello superiore. Per cui all'aumento dei livelli aumenta l'overhead.

3.1 Livelli

I diversi livelli di questo modello presentano le seguenti funzioni:

1. Il primo strato della pila ISO-OSI rappresenta lo strato fisico, che si interfaccia direttamente con il mezzo trasmissivo della rete e quindi rappresenta il livello di natura fisica della trasmissione. Offre al livello superiore una comunicazione indipendente dal mezzo trasmissivo. Fornisce allo strato di collegamento servizi di trasmissione di bit a tra sistemi adiacenti, consegna in sequenza di bit o notifiche di malfunzionamenti.

2. Il secondo livello rappresenta lo strato data-link per risolvere eventuali malfunzionamenti dello strato fisico, rilevando e correggendo errori, tramite algoritmi di correzione, come i bit di parità. Offre allo strato superiore la possibilità di trasmettere pdu a sistemi adiacenti utilizzando due code nelle due direzioni.

3. Il terzo livello è lo strato di rete e conosce la topologia completa della rete, per effettuare operazioni di instradamento. Contiene i protocolli come IPv4, progressivamente sostituito da IPv6, e permette il trasferimento di pdu da estremo ad estremo. Inoltre permette la commutazione di circuito o di pacchetto a datagramma e a circuito virtuale.

4. Il quarto livello di trasporto, divide il messaggio in pacchetti, prova a colmare fluttuazioni della qualità del servizio dello strato di rete in modo trasparente rispetto agli strati superiori. In caso manchino dei pacchetti prova a recuperarli attraverso algoritmi di correzione, è il primo strato che risiede solamente nei terminali. Offre allo strato superiore la possibilità di instaurare una connessione e gestione della stessa, una trasmissione affidabile, ed il rilascio della connessione.

5. Il quinto livello di sessione sincronizza e struttura il dialogo tra due processi.

6. Il sesto livello di presentazione permette uno scambio di messaggi indipendentemente dalla sintassi della trasmissione.

7. Il settimo livello di applicazione offre un mezzo per accedere alla rete tramite un processo, interfacciando l'utente alla rete.

Per tutti i livelli superiori a quello fisico si possono definire due modalità operative ed associati servizi e protocolli, connessi e non connessi. Nei servizi o protocolli connessi, si instaura una connessione o dialogo tra le entità, e termina solamente dopo convenevoli finali. La modalità non connessa non ha bisogno di una connessione costante tra le due entità, viene instaurata senza un dialogo da una delle entità senza una terminazione.

Nella prima modalità l'entità non ha bisogno di ascoltare tutto il traffico per determinare quali pdu sono indirizzati alla stessa, ma necessita di una connessione continua anche se vengono trasmessi una piccola quantità di dati. Mentre nella seconda modalità possono essere inviate pdu indipendente dalla connessione e dalla distanza temporale tra le due, ma le entità che offrono questo servizio o protocollo devono costantemente analizzare il traffico per individuare le pdu a loro indirizzate. I protocolli non connessi sono quindi più efficienti, ma mancano di affidabilità, poiché manca una conferma di ricezione dei dati come nei protocolli connessi. quest'ultimi sono quindi più affidabili, ma meno efficienti, poiché dopo aver instaurato il dialogo non è possibile terminarlo preventivamente, e ciò può causare uno spreco di risorse.

In un servizio connesso sono presenti primitive per instaurare una connessione, inviare messaggi e una conferma di ricezione o ricevere messaggi, specificare l'indirizzo o nome della connessione ed abbattere la connessione. Mentre per servizi non connessi sono presenti solo primitive per inviare messaggi separatamene. Nelle reti LAN sono disponibili servizi connessi, solamente sul quarto strato, mentre nelle reti WAN è possibile siano offerti anche nel primo strato.

I primi tre livelli della pila ISO-OSI sono presenti su ogni nodo della rete non solo sui calcolatori, poiché rappresentano i livelli di trasmissione dei pacchetti, necessari anche nei nodi intermedi per poter trasmettere i pacchetti.

Nei protocolli di livello 2,3 e 4 si utilizzano meccanismi di riscontro o acknowledgment e tecniche di controllo a finestra, a riga indice e puntatore in avanti per correggere eventuali errori nei pacchetti.

Gli ultimi tre strati della pila si interfacciano con le applicazioni e lavorano generalmente in parallelo invece che in serie come il resto della pila.

Una singola connessione di livello n può essere sfruttata da più connessioni di livello $n+1$, interne in modo che gli n-pdu contengono entrambe le $n+1$-pdu delle due connessioni. Può essere il caso di connessioni tra più processi diversi sulle stesse due macchine, dove una singola connessione tra queste due macchine contenga numerose connessioni processo-processo tra le due.

Inoltre una singola connessione $n+1$ può utilizzare più di una connessione di livello n, per parallelizzare la trasmissione e velocizzarla partizionando i dati da inviare, oppure per implementare una resistenza ai guasti. La connessione $n+1$ utilizza più canali di comunicazione di livello n non in competizione.

Una singola connessione di livello $n+1$ nel tempo, può utilizzare più di una connessione di livello inferiore; è possibile che il terminale si sposta durante la trasmissione e si aggancia a reti diverse da quella iniziale, senza interrompere la connessione. Nello stesso caso, una stessa connessione di livello n continua nel tempo può essere utilizzata da diverse connessioni di livello $n+1$. La connessione originale dell'esempio precedente vede uscire il primo terminale e quindi la prima connessione $n+1$ per poi vedere accedere un altro terminale ed un'altra connessione $n+1$.

4 Livello 2: Standard IEEE 802

Lo standard IEEE 802 riguarda i primi due livelli del modello ISO-OSI, ovvero il livello fisico, ed il livello data link. Le tecnologie definite in base a questo standard quindi hanno come obiettivo la trasmissione e la rivelazione o correzione di bit attraverso un mezzo trasmissivo. Si occupano della connessione e quindi comunicazione tra macchine adiacenti, per una qualche definizione di adiacenza. Altri protocolli e standard noti sono l'IPv4 ed IPv6, protocolli di routing di livello tre, protocolli TCP ed UDP di livello quattro, ed il protocollo HTTP di livello sette, ma si occupa anche da solo delle funzioni dei livelli 5 e 6.

Questi standard vengono realizzati dall'organizzazione IEEE, Institute of Electrical and Electronics Engineers, organizzazione indipendente da stati sovrani. Il progetto IEEE 802 venne definito con l'obiettivo di realizzare una serie di standard di livello fisico e data-link per permettere la comunicazione di calcolatori sulla stessa rete locale, LAN, personale, PAN, o rete metropolitana, MAN, di grandezza intermedia tra le reti LAN e WAN. Ha avuto successo sopratutto per le reti LAN e MAN, ma per le reti personali si utilizza uno standard diverso basato sul bluetooth. Questi standard riguardano tecnologie con pacchetti di lunghezza variabile.

Le specifiche tecnologie vengono individuate tramite una notazione puntata, con $802.x$, dove x rappresenta un numero, ed identifica la tecnologia. I numeri precedenti al punto individuano lo standard dove è stata introdotta questa tecnologia. Ma le tecnologie non rimangono invariate nel tempo, per cui si possono assegnare delle lettere dopo il numero per specificare la versione o tipo di quella specifica tecnologia.

Lo standard IEEE 802.2 divide il livello due in due sottolivelli: "Logical Link Control" (LLC) e "Media Access Control" (MAC), questi gestiscono due tipologie diverse di pacchetti. Per le diverse tecnologie dello standard, il livello MAC è diverso, mentre il livello LLC è comune a tutti. Il sottolivello MAC è specifico per ogni tipo di LAN, si suppone che tutti i calcolatori che devono comunicare siano nella stessa LAN. Data questa ipotesi il sottolivello MAC risolve il problema di determinare il destinatario in ricezione, e di verificare la disponibilità della LAN in trasmissione, in caso la LAN sia a singolo canale condiviso. Quindi bisogna evitare che il canale sia utilizzato da più utenti.

4.1 802.2: Sottolivello MAC

Poiché il canale è condiviso, tutti gli utenti possono vedere i pacchetti inviati, sono quindi necessari protocolli di sicurezza e cifratura per impedira che sia possibile a chiunque connesso alla rete leggere il contenuto dei pacchetti. Tecniche che non verranno trattate in questo corso. Inoltre si utilizza un canale condiviso poiché se ci fosse un malfunzionamento fisico, una sola connessione verrebbe compromessa e non l'intera rete.

Per determinare il destinatario di un pacchetto nella MAC pdu è presente un campo per definire il tipo di trasmissione:

- Punto a Punto: da un calcolatore ad un altro nella LAN;
- Punto a Gruppo: da un calcolatore a diversi altri nella LAN;
- Broadcast: a tutti gli utenti connessi alla LAN.

Per permettere di identificare univocamente un unico elemento nella rete, gli indirizzi MAC devono essere univoci nella rete considerata. Dato che è possibile connettersi ad una LAN dall'esterno senza conoscere gli indirizzi MAC utilizzati, servirebbe un gestore di rete per assegnarli ad ogni nuova connessione, ma questo è un approccio inefficiente. Si utilizzano quindi indirizzi MAC univoci a livello mondiale, in questo modo nell'intera rete esisteranno solo indirizzi MAC differenti. Questa condizione vale anche su VPN o LPN, inoltre se su una stessa macchina vengono simulate diverse macchine virtuali, ognuna di esse dovrà avere un indirizzo MAC differente, all'interno della rete locale che utilizzano per comunicare tra di loro. Se due macchine avessero lo stesso MAC, riceverebbero gli stessi pacchetti, e verrebbero riconosciuti da entrambe le macchine come propri.

La MAC pdu è composta da diversi campi, che possono variare in base alla tecnologia con l'aggiunta di campi specifici. Ma per ogni tecnologia aderente allo standard IEEE 802 sono presenti sicuramente questi quattro campi per la MAC pdu:

- MAC-dsap (Destination Service Access Point): indirizzo di destinazione;
- MAC-ssap (Source/Send Service Access Point): indirizzo di partenza;
- Info: LLC pdu;
- FCS (Frame Check Sequence): per identificare e correggere eventuali errori.

Per ottenere l'indirizzo del destinatario, si utilizzano protocolli di acquisizione descritti in seguito.

Gli indirizzi MAC sono composti da 6 byte, in base allo standard EUI-48, "Extended Unique Identifier", per indirizzi a 48 bit, ma esiste anche uno standard a 64 bit non utilizzato. Questi byte vengono rappresentati in forma esadecimale, separati da due punti o trattini. I primi tre byte dell'indirizzo MAC vengono assegnati al costruttore e rappresentano gli OUI "Organization Unique Identifier", gli ultimi 3 byte vengono scelti dal costruttore. Per cui dato un indirizzo MAC, è sempre possibile determinare il costruttore della macchina a cui appartiene.

Esistono diversi tipi di indirizzi MAC, in base al valore di determinati bit:

- Unicast: indirizzi che individuano le singole schede di rete dei calcolatori; se l'ultimo bit del primo byte ha valore zero;
- Multicast: indirizzi che identificano gruppi di schede di rete; se l'ultimo bit del primo byte ha valore uno;
- Broadcast: identificano tutte le schede di rete; se l'indirizzo è `FF:FF:FF:FF:FF:FF`.

Inoltre è possibile assegnare indirizzi MAC non unici a livello mondiale, specificando il valore del penultimo bit del primo byte, in modo che abbia valore uno. In questo modo è possibile gestire localmente indirizzi MAC nella stessa LAN.

Per risolvere i conflitti in trasmissione si utilizzano nelle rete WiFi degli algoritmi distribuiti sulle singole macchine in contemporanea, che collaborano per determinare a chi abilitare gli accessi alla rete.

4.2 802.2: Sottolivello LLC

Il sottolivello LLC consegna al livello MAC un pacchetto da spedire, questo pacchetto è uguale per ogni tecnologia aderente allo standard e presenta campi analoghi al sottolivello MAC. I campi LLC-dsap/ssap individuano gli indirizzi LLC del mittente e destinatario, il campo info contiene il tipo di pdu per gestire diverse tipologie di pacchetto, e l'ultimo campo contiene la pdu di terzo livello. Gli indirizzi LLC non individuano macchine come gli indirizzi MAC, ma vengono utilizzati per identificare i protocolli di livello 3 a cui sono indirizzati i pacchetti. Consentono la convivenza di diversi protocolli di livello 3 sulla stessa macchina e sulla stessa LAN, dove sono presenti diverse pile protocollari con obiettivi e versionatura diversa.

Gli indirizzi LLC vengono attribuiti dall'IEEE solo a protocolli "ufficialmente" standard, ma questa è una classificazione che ignora molti dei protocolli più utilizzati a livello globale come TPC-IP, il protocollo più utilizzato al mondo. Vengono identificati da un byte in esadecimale, se non sono protocolli standard, il loro indirizzo è `AA`, ed il pacchetto subisce una variazione con la snap-pdu, "SubNet Access Point", dopo il campo control di 5 byte per identificare il protocollo. Questo rappresenta un ulteriore livello di overhead, già elevato per il modello ISO-OSI, per i pacchetti.

4.3 802.3: Ethernet

La prima tecnologia ethernet nacque nel 1970 dal consorzio DIX, dalle iniziali delle tre più grandi case produttrici informatiche dell'epoca: Digital, Intel e Xerox. In seguito venne revisionato negli anni '80 due volte, nel 1989 lo standard IEEE 802.3 diventa lo standard ISO 8802.3, e negli anni '90 ebbe talmente successo sulle reti LAN e WAN che divenne essenzialmente lo standard di tutte le trasmissioni su filo, completamente retrocompatibile. Nel tempo ha usato diversi mezzi trasmissivi, da cavi di rame intrecciati a coppie, alla fibra ottica moderna. I cavi di rame venivano avvolti da una isolante dielettrico ed una schermatura esterna, dove erano presenti quattro coppie di cavi di rame intrecciati. Questo permette connessioni punto-punto bidirezionali e contemporanee.

Dagli anni '90 in poi la banda massima possibile è aumentata fino ad un massimo di 100-400 Gb/s.

Il formato del pacchetto ethernet è rimasto sostanzialmente invariato nel tempo, nonostante le sue revisioni, nello standard IEEE 802.3 presenta i seguenti campi:

- Preambolo (56 bit): veniva utilizzato per sincronizzare in fase i pacchetti, modalità di trasmissione non più in uso;
- SFD "Start Frame Delimiter" (8 bit): indica l'inizio del pacchetto;
- Indirizzi MAC di sorgente e destinazione (96 bit);
- Lunghezza del campo dati (16 bit);
- Dati: di lunghezza variabile con un massimo di 1500 Byte, contiene una LLC-pdu;
- Pad: eventuale riempimento, da 0 a 46 Byte, la somma con il campo dati deve essere compresa tra 46 e 1500 Byte;

- FCS "Frame Check Sequence" (32 bit): contiene il valore del codice di ridondanza ciclica (CRC) calcolato.

Non è presente invece un delimitatore finale del pacchetto. I pacchetti hanno una lunghezza minima di 512 bit, mentre una lunghezza massima di 1512 Byte, esclusi il preambolo ed il SFD. Si definisce per rete ethernet l'"Inter-Frame Space" (ITR) o "Inter-Packet gap" (IPG) come il tempo minimo tra due pacchetti consecutivi. Questo viene definito indipendentemente dalla velocità della rete, come il tempo necessario per inviare 96 bit, è necessario per permettere di distinguere due pacchetti inviati consecutivi e determinare si tratti di spazio tra i due.

Agli albori di questa tecnologia si utilizzavano reti condivise, quindi bisogna effettuare una connessioni a turni, e per occupare la connessioni su reti di 5 km, si scelse la lunghezza minima di 512 bit. Analogamente se il pacchetto è troppo grande, occuperebbe il mezzo trasmissivo per troppo tempo, quindi si è imposta una lunghezza massima.

Nella trasmissione ethernet il livello MAC in trasmissione riceve la LLC-pdu, inserendolo nel pacchetto di livello MAC e convertendolo in bit da passare al livello fisico. In ricezione, converte i bit in un pacchetto MAC, se questo è indirizzato ad un altro oppure contiene errori, calcolando il CRC, viene scartato, altrimenti viene rimossa la parte MAC ed inviato al livello LLC. Scartando pacchetti in questo modo si perde di affidabilità del sistema, ma si guadagna efficienza, poiché si suppone queste informazioni perse vengano recuperate ad un livello superiore (livello di trasporto), senza che sia l'ethernet ad inviare una richiesta di ritrasmissione. Ogni terminale che riceve pacchetti deve quindi ricalcolare il CRC, quest'operazione potrebbe rappresentare il collo di bottiglia e deve essere il più veloce possibile. Questo livello garantisce una distanza minima tra pacchetti rispettando l'IPG e verifica la lunghezza minima del pacchetto. Se un pacchetto non rispetta la lunghezza minima, viene anch'esso buttato. Vengono inoltre generati, in trasmissione, e rimossi, in ricezione, il preambolo e lo SFD dal pacchetto.

In passato le reti ethernet erano formate da connessioni sullo stesso filo condiviso non era punto-punto e bidirezionale, chiamato dominio di collisione, tra varie stazioni ed usato a turno. I pacchetti inviati da due o più macchine potevano collidere e si poteva richiedere una ritrasmissione da queste. Questo mezzo condiviso era realizzato da un repeater o ripetitore o hub, questo ripete il segnale su tutti i canali connessi e li amplifica, a causa della lunghezza delle reti infatti, il segnale poteva perdere di potenza durante la trasmissione. A livello fisico si comporta come un filo, non memorizza infatti i pacchetti che riceve, ma li trasmette, non è una macchina "Store & Forward". Ripetitori del genere sono ancora diffusi in alcuni contesti. Si trova al livello fisico ed ha diverse porta su cui può ricevere dati e trasmetterli su tutte le altre.

Il mezzo trasmissivo per le connessioni ethernet viene realizzato in cavi di rame o fibra ottica, al massimo di 100 m di lunghezza, progettati senza amplificatori. Si usano coppie separate per trasmissione e ricezione per mantenere una connessione bidirezionale. Si usano connettori RJ-45. Reti a fibra ottica invece possono percorrere distanze molto significative rispetto a cavi in rame.

Ethernet II e ethernet IEEE 802 sono diversi tra di loro, lo standard ethernet II non ha uno sottolivello LLC ed è in generale molto più snello. Nelle reti locali convivono connessioni di entrambi gli standard, e sono tendenzialmente molti di più nella vecchia versione di ethernet. Sono necessari quindi meccanismi per mantenere la retrocompatibilità completa dei pacchetti. Non essendoci lo strato LLC, il pacchetto di terzo livello viene contenuto direttamente nel pacchetto MAC, poiché non esiste il livello LLC per questi pacchetti, si utilizza un altro campo type, per specificare a

quale protocollo di livello superiore inviare il pacchetto. Questo sostituisce il campo lunghezza di IEEE 802.3. Viene riconosciuto se il campo lunghezza ha un valore maggiore di 1500, lunghezza massima del campo data, e viene interpretato come un codice identificativo di un protocollo di livello superiore.

Poiché ethernet ha vissuto un enorme crescita tecnologia, sono presenti diversi sottolivelli dello standard per classificarle, da versioni 802.3u da 100 Mb/s alle ultime versioni 802.3ba/bg/bm dai 40 ai 100 Gb/s. Sono inoltre in corso di standardizzazione tecnologie ethernet nell'ordine dei terabit al secondo.

Generalmente se nel sottolivello dello standard è presente una lettera maiuscola, questo rappresenta un tecnologia estremamente importante.

Sono presenti inoltre molte versioni differenti per scopi diversi, esiste uno standard specifico per il mercato automobilistico, dove è presente poco spazio interno, e quindi si utilizzano cavi da una singola coppia di cavi intrecciati: 802.3bw e 802.3bp (2015/2016) permettono una banda nell'ordine dei gigabit sulla singola coppia. Esiste inoltre uno standard per inviare corrente elettrica su ethernet ed alimentare tramite ethernet telefoni IP a bassa tensione: 802.3af e 802.3at (2003/2009).

4.4 802.1D: Bridge-Switch

La connessione instaurata tramite ethernet è bidirezionale simultanea solamente su due calcolatori, ma su una stessa connessione può inviare i dati un solo calcolatore, quindi sono necessarie altre componenti. Un bridge è una componente che consente di connettere tra di loro più di un computer tramite ethernet, comportandosi come se fosse un calcolatore intermedio ai calcolatori della rete, connesso a ciascuno di questi tramite una connessione ethernet.

Inoltre connettendo tra di loro diversi bridge è possibile creare una struttura più articolata, creando una struttura simile ad un albero. La parte wired o cablata delle connessioni LAN vengono instaurate in questo modo.

I bridge svolgono una prima funzione di rendere possibili topologie articolate, effettuando un'operazione di "filtering", per separare tra di loro porzioni di rete che non devono dialogare tra di loro in modo diretto

I bridge sono delle macchine "store & forward", ovvero quando ricevono un pacchetto, prima di essere inviato su altre porte, viene memorizzato e trasmesso su altre porte, analogamente come se fosse un calcolatore, in caso le altre porte siano impegnate a trasmettere altri pacchetti, quindi in caso di traffico. Si può quindi immaginare una coda di pacchetti sulle porte del bridge per essere trasmesse.

Il bridge sono delle tecnologie di livello 2, ed utilizzano algoritmi di instradamento per inviarli ad un MAC address specifico, ma questo tipo di algoritmo viene effettuato a livello 3. Questo non sorge problemi, poiché quest'operazione di instradamento è interna alla LAN, e non coinvolge alcun'altra componente della rete. I bridge devono essere conformi allo standard IEEE 802.1D. Gli standard comprendenti il carattere "D", sono di grande importanza. I sistemi connessi a reti LAN ignorano i bridge, si dicono quindi trasparenti, poiché i calcolatori connessi alla rete non conoscono la loro posizione all'interno della rete.

Un calcolatore per inviare un messaggio ad un altro calcolatore su una rete LAN, invia il suo pacchetto ad un bridge attraverso il sul MAC address. Il bridge quindi utilizza in principio un

diverso MAC address, per spedire questo pacchetto al computer di destinazione tramite il suo MAC address. Tra questi due MAC è presenta un componente di relay, per trasmettere il pacchetto tra porte diverse del bridge.

Le porte di un bridge possono avere lo stesso MAC o MAC differenti. Poiché il pacchetto è specifico al MAC del bridge, deve ricostruire il pacchetto scartando i campi specifici al MAC address del bridge. Inoltre poiché i pacchetti non sono tutti conformi allo standard IEEE 802.3, deve ricostruire anche il campo LLC. I MAC address dei computer nella rete sono realizzati in modo da poter essere connessi a ciascun tipo di MAC.

Si vuole che il modello di rete sia "plug & play", ovvero non deve essere dipendente da un intervento umano. I bridge costruiscono la loro tabella di instradamento per identificare dove sono presenti i diversi MAC address, autonomamente attraverso un meccanismo di "learning", salvando questa tabella nel "filtering database". Ogni porta del bridge rappresenta una linea ethernet diversa, identificando un loro dominio di collisione, a cui possono essere connessi diversi calcolatori.

Si considera una rete dove ogni componente connesso è spento, ed una tabella vuota. Appena si accende un calcolatore ed invia un pacchetto da un dominio di collisione, allora il bridge capisce a quale porta corrisponde il MAC address del mittente. Ma ancora non conosce dove si trova il destinatario, quindi lo invia su tutte le sue porte disponibili, su tutta la rete. Invece se conosce la porta dov'è presente il destinatario lo invia solamente su quella porta.

Il learning permette di costruire autonomamente il filtering database di un bridge, questo meccanismo tuttavia non funziona quando al rete presenta una topologia diversa dalla topologia ad albero. Per esempio se è presente un ciclo all'interno della rete, il bridge si vede arrivare un pacchetto dallo stesso MAC address su porte diverse. Ma un albero è una topologia contenente solo "Single Points of Failures" (SPoF) e quindi fortemente sconsigliata, poiché un singolo malfunzionamento causerebbe la perdita di funzionalità dell'intera rete. Per cui data una topologia a grafo, un bridge è in grado di calcolare autonomamente un albero ricoprente della rete, ad ogni cambio di topologia della stessa. I bridge inoltre vengono collegati tra di loro per più di una connessione per evitare altri SPoF, ed evitare che a un singolo guasto la rete venga tagliata in due.

Tramite un meccanismo progressivo i bridge individuano la loro posizione nella struttura dell'albero ricoprente e sono in grado di staccare alcune porte e rimanere collegati sull'intera rete; quando questi bridge rilevano un guasto su una di queste connessioni, riattivano una delle porte disattivate per mantenere in funzione la rete, ottenendo una significativa resistenza ai gusti. Questo tipo di algoritmo di spanning tree verrà trattato in corsi più avanzati di reti di calcolatori.

Le prestazioni di un bridge influenzano le prestazioni dell'intera rete locale, vengono identificate da una serie di parametri. Il numero massimo di pacchetti al secondo processabili dal bridge, rappresentano un collo di bottiglia per i pacchetti che possono essere presenti sulla rete in ogni singolo momento, se vengono inviati un numero superiore ci pacchetti, alcuni pacchetti verranno scartati. Un altro parametro caratteristico è il tempo medio di latenza, ovvero il tempo in cui il bridge prende le sue decisioni ed invia il pacchetto alla porta giusta. Per cui è preferibile avere bridge full speed, ovvero con una velocità pari al massimo teorico. Più corti sono i pacchetti maggiore è il numero di decisioni effettuate nell'unità di tempo. Nello standard IEEE 802.3 a 10 Mb/s, un bridge si definisce full speed, se è in grado di processare 41880 pacchetti al secondo, per ogni porta. Questi esperimenti di verifica a parità di frequenza devono essere effettuati utilizzando pacchetti di lunghezza minima, così ad ogni porta è presente la massima frequenza di funzionamento del bridge.

Il pacchetto più piccolo che può essere inviato è da 512 bit, per cui il numero massimo di pacchetti al secondo ad una velocità di 10 Mb/s è di circa 19500 pacchetti, ma il pacchetto comprende anche il preambolo ed lo SFD, per cui vanno aggiunti altri 64 bit, numero di pacchetti al secondo scende quindi a 17300. Tuttavia tra un pacchetto ed il successivo in ethernet è presente l'"interpacket gap" di 96 bit. Per ciascuna tipologia di porta del bridge si effettua questa analisi e si verifica nel caso peggiore quanti pacchetti è in grado di gestire.

Il bridge è un calcolatore, con una CPU, RAM ed interfacce per le diverse LAN, in ROM le funzionalità dello standard Per bridge più potenti, le porte vengono realizzate tramite schede ASIC, per risolvere il problema dell'instradamento localmente. Le porte vengono realizzati tramite diversi slot che possono essere inseriti o rimossi in base al tipo di porta necessaria. Inoltre sono necessari massicci impianti di raffreddamento per riuscire a mantenere la temperatura del data center. A differenza di un server che può essere rallentano in caso di traffico allentato e quindi diminuire la temperature, le apparecchiature di bridge non possono spegnersi, e quindi comportano una temperatura costantemente elevata. Bridge di fascia alta sono in grado di effettuare bilanci sulle prese di corrente.

Logicamente sono presenti almeno due porte una "MAC relay entity", per trasmettere i pacchetti tra le varie porte, ed un'entità di livello superiore, per la gestione del bridge, degli algoritmi e dei protocolli. Queste entità di alto livello comunicano con altri bridge attraverso pacchetti per realizzare lo spanning tree.

Le porte del bridge possono essere abilitate o disattivate dall'amministratore di rete. Una porta attiva può essere in stato di "forwarding" o di "blocking", se sono bloccate lo spanning tree lo ha bloccate. Ogni porta ha un indirizzo MAC univoco, e sono numerate progressivamente a partire da uno. Convenzionalmente l'indirizzo MAc del bridge corrisponde all'indirizzo MAC della porta numero uno.

La tabella di instradamento contiene "entries" (righe) statiche o dinamiche. Le righe statiche vengono inserite dall'amministratore a causa di esigenze di sicurezza importanti, altrimenti la posizione del MAC address vengono mantenuti per un tempo finito, configurabile, e di default di 5 minuti. Infatti è possibile che il calcolatore venga spostato spazialmente attraverso la rete, è quindi possibile si colleghi ad una porta differente.

Lo sviluppo di ethernet ha portato alla creazione di meccanismi di controllo di flusso, soprattutto per gli switch. Una richiesta attraverso il bridge può essere di pochi byte verso un server, ma può provocare un trasferimento notevole di dati verso il client, quindi attraverso il bridge ad una porta ad alta velocità, ma questi pacchetti da ritrasmettere verso il cliente passano attraverso una porta di banda minore, quindi la porta più lente può andare facilmente in saturazione. Viene introdotto quindi tramite lo standard IEEE 802.3x e 802.3bd un controllo di flusso tramite dei "pause frame" un MAC control frame di 512 bit, per fermarsi prima di riprodurre traffico I pause frame non contengono dati ma contengono informazioni di controllo, e rappresentano una novità, viene quindi implementato attraverso un nuovo sottostato di MAC chiamato MAC control. Il supporto allo standard 802.3x è opzionale e viene negoziato tra le schede alle due estremità del filo.

Prima dello standard 802.3x poiché ethernet era una comunicazione a turni, per impedire la saturazione i bridge potevano inviare pacchetti senza dati prendendo il controllo della connessione.

4.5 802.11: WiFi

A differenza di ethernet, dove si ha una connessione punto a punto bidirezionale e simultanea, attraverso un bridge permette di comunicare a diversi computer con una singola connessione tra tutti i calcolatori ad un bridge. Per cui i MAC ethernet è molto semplice, ma questo non si può dire per la rete WiFi. Una rete locale è un ambiente dove tutti parlano contemporaneamente con tutti, e ciò non può avvenire su di un filo condiviso tra due calcolatori. Quindi le connessioni WiFi presentano un indirizzo MAC molto più complesso.

Ethernet è molto versatile, ma su alcuni edifici non è possibile effettuare un cablaggio economicamente, oppure sono presenti uffici nei quali gli impiegati sono presenti occasionalmente. Oppure nel caso di reti offerte pubblicamente, con utenti occasionali. Per questi motivi di praticità nei portatili moderni, sono presenti schede di rete WiFi e non ethernet.

Nonostante questi benefici, il mezzo trasmissivo non è affidabile, e comporta un costante consumo elettrico per connettersi alla rete. Comprende una zona di copertura limitata. Esistono diversi studi sull'uso delle frequenze o micro-frequenze sulla salute.

Il sistema WiFi nel venne definito nel comitato IEEE 802, dove forma il working group 902.11 dedicato alle LAN senza fili. Il primo standard ad affermarsi è 802.11b. Nel 1999 si forma il consorzio Wireless Ethernet Compatibilità Alliance, successivamente denominato Wi-Fi (Wireless Fidelity) Alliance per certificare i prodotti IEEE 802.11.

Una rete WiFi può presentare architetture di due tipi, ad hoc o strutturate. In una rete ad hoc le stazioni comunicano direttamente l'una con l'altra.

Quest'architettura è prevista dallo standard, ma le reti WiFi non funzionano in questo modo. Quest'architettura è stata progettata per permettere di comunicare dispositivi personali, ma su questo ambiente applicativo ha prevalso bluetooth.

Sono realizzate tramite architettura strutturata, tutte le stazioni, astrazione di calcolatore poiché funziona su tante tipologie di dispositivi, possono accedere solamente tramite punti di accesso (Access Point o AP). Questi punti di accesso sono interconnessi mediante fili, quindi non rappresenta una rete completamente senza fili. Questi collegamenti vengono effettuati tramite ethernet, rappresentato come un unico domino di collisione, nonostante sia presente una topologia più complessa. In queste reti non è presente un master, ma tutti gli AP sono allo stesso livello, in modo che non siano presenti SPoF.

Quest'architettura permette una semplice scalabilità, infatti è sufficiente connettere altri AP alla rete ethernet. L'informatica deve essere scalabile, con costi limitati deve poter aumentare le sue infrastrutture.

Ciascuno di questi AP ha un MAC di tipo IEEE 802.11, e si comporta come un bridge, presenta almeno due interfacce, una 802.11 per comunicare con i dispositivi wireless, ed un'altra porta 802.3 per comunicare sulla rete ethernet. Ma questi pacchetti inviati con due MAC differenti, necessitano di un'entità di relay per poter gestire questi diversi tipi di MAC. Ogni AP controlla un "Basic Service Set" (BSS), che estende la rete cablata. Ogni BSS ha un identificatore (BSSID), può essere utilizzato il MAC della scheda AP corrispondente. Ma è possibile modificare questo BSSID. La parte cablata si chiama "Distribution System" (DS) e rappresenta l'infrastruttura portante della rete.

Sono presenti delle eccezioni, infatti è possibile costruire dei collegamenti tra AP che estendono il DS tramite WiFi. Ma dal punto di vista dell'architettura si comporta come un filo, collegando solamente due AP.

Per gestire il sottolivello MAC, bisogna gestire il problema dell'accesso al mezzo trasmissivo condiviso. Inoltre bisogna avere una spedizione affidabile dei pacchetti su un mezzo trasmissivo poco affidabile. Livelli fisici differenti utilizzano frequenze e bande diverse. Il sottolivello MAC viene a sua volta diviso in due sottolivelli, questo viene effettuato per permettere di realizzare architetture modulari. Un sottolivello "Distributed Coordination Function" (DCF) e "Point Coordination Function" (PCF), questi due livelli indipendentemente sono connessi al LLC. L'accesso distribuito al mezzo trasmissivo viene realizzato nel DCF, questo è il modello effettivamente utilizzato. Rappresenta il MAC vero e proprio, e tramite questo le macchine tentano di accedere al mezzo trasmissivo, ma non è garantito questo accesso, e può comportare ritardi. In alcuni ambienti applicativi si vuole accedere al mezzo trasmissivo con garanzia di un tempo di ritardo massimo che non superi una certa soglia. In queste applicazioni si sceglie una stazione di riferimento che in ogni intervallo temporale indica chi può trasmettere con il mezzo trasmissivo. Ambienti "Mission Critical", dove una macchina deve necessariamente effettuare un azione in un certo intervallo di tempo.

La probabilità che il ritardo sia elevato in una rete WiFi è molto bassa, per cui questa tecnologia non viene quasi mai utilizzata. Poiché in questo caso bisognerebbe utilizzare un controllore unico che si cerca molto spesso di non utilizzare in una rete.

Per qualunque MAC IEEE 802.2 deve essere presente l'indirizzo del destinatario, del mittente, il campo dati e l'FCS. Esiste un altro campo "Frame Control" nello standard 802.11 che indica il tipo di pacchetto, di controllo o contenente dati, e fornisce anche informazioni sul mittente ed il destinatario del DS, sulla frammentazione e sulla riservatezza. Contiene un campo per indicare di durate che indica il tempo necessario in cui deve essere effettuata la trasmissione. Sono presenti fino a quattro indirizzi MAC. Il "Sequence Control" contiene informazioni utili per la frammentazione o il riassemblaggio dei pacchetti.

Si parla quindi di indirizzamento per spiegare il motivo per cui sono presenti fino a quattro indirizzi MAC in un unico pacchetto. Ogni scheda di rete wireless contiene un suo indirizzo MAC, e questa raccoglie i pacchetti e verifica che sia diretto alla stessa macchina dal suo indirizzo MAC. Nel pacchetto di livello MAC sono presenti quattro indirizzi numerati da 1 a 4, più due bit. Questi bit sono ToDS e FromDS, se il primo bit vale 1, questo pacchetto è spedito all'AP per essere smistato dal DS, il secondo vale uno quando il pacchetto proviene dal DS. In funzione di questi valori i quattro indirizzi hanno significati diversi.

Quando due computer comunicano direttamente, un una rete ad hoc, il primo indirizzo del pacchetto corrisponde all'indirizzo del destinatario ed il seguente all'indirizzo del mittente. Il terzo campo di indirizzo corrisponde al BSSID, ma questo si riferisce solamente alle reti strutturate. In questo modello le macchine comunicano tra di loro in gruppi chiusi, quindi condividano un identificatore chiamato BSSID. La connessione è quindi lecita solamente se il BSSID è lo stesso. Poiché si tratta di una comunicazione diretta, i suoi bit hanno valore nullo.

In una trasmissione da una stazione ad un AP, il primo indirizzo è l'indirizzo dell'access point, il secondo è quello del mittente vero. Il terzo indirizzo è quello del pacchetto vero. Questi AP sono

comunque trasparenti rispetto alle macchine, poiché alla prima connessione il calcolatore memorizza l'indirizzo del BSSID a cui può richiedere accesso per inviare e ricevere pacchetti.

Quando un pacchetto viene inviato dal DS, il primo indirizzo è il MAC del destinatario vero, il secondo è l'indirizzo dell'AP che lo invia, ed il terzo è l'indirizzo del vero mittente.

NNell'ultimo caso, il pacchetto è inviato e ricevuto dal DS, è il caso di due AP che comunicano tra di loro tramite WiFi. Sono necessari i due indirizzi degli AP e gli indirizzi del destinatario e del mittente vero.

Per realizzare dei turni senza una stazione di coordinamento centralizzata si utilizza il sottolivello DCF. Il DCF ha come requisiti principali di evitare interferenze di trasmissioni simultanee, contendo il maggior numero possibile di connessione e gestendo il canale trasmissivo in modo equo. Non si vuole utilizzare un controllore centralizzato, senza un clock. Si utilizza un algoritmo csma/ca, "Carrier Senza Multiple Access/Collision Avoidance". Questo meccanismo determina se il mezzo trasmissivo è disponibile, in caso una stazione ha un pacchetto da spedire "Carrier Sense". Se il mezzo è occupato aspetta che la stazione sia libera prima di trasmettere. È possibile che due stazioni provino a trasmettere contemporaneamente, in questo caso si verifica una collisione edi pacchetti diventano intellegibili per i destinatari, e dovranno essere ritrasmessi. Per evitare le collisioni si utilizzano degli strumenti per evitarle il quanto possibile. Gli algoritmi backoff, acknowledgment,

DCF per effettuare il suo lavoro utilizza gli intervalli tra due pacchetti consecutivi per gestire delle priorità. Questo tempo è l'interpacket gap, che in ethernet è lungo 96 bit-time. Ci sono due tipi principali di IFS, "Inter-Frame Space", di tempo variabile tra i vari pacchetti: DIFS, "DCF IFS", in generale quello standard, e SIFS, "Short IFS" di lunghezza minore. Se un pacchetto consecutivo può essere trasmesso immediatamente, allora si utilizza il SIFS, altrimenti si utilizza il tempo di standard DIFS.

Per ora si considera il DCF senza il RTS/CTS, "Request To Send"/"Clear To Send" per evitare collisioni. Quando una stazione vuole trasmettere, ed il canale è occupato, capisce che è presente traffico nel canale, e si autolimita scegliendo un numero random, di backoff, nell'intervallo $[0, cw]$, ed incrementa il timer quando il timer solo quando è libero. La trasmissione può essere effettuata solamente quando il timer raggiunge il termine.

Quando una stazione rileva una collisione, utilizzando vari meccanismi, duplica il cw in modo che l'intervallo di casualità sia duplicato, in modo da rendere più improbabile collisioni future. Limitato superiormente al valore $cw_{\max}$. Se è un pacchetto viene inviato con successo, il valore di cw viene posto al valore minimo $cw_{\min}$. Valori ragionevoli per questo intervallo $[cw_{\min}, cw_{\max}]$ sono $[7, 31]$ e $[255, 1023]$.

Per determinare se il canale trasmissivo è libero, si utilizza un'altro meccanismo. In ogni pacchetto viene specificata la sua durata, nel campo "duration". Poiché il messo trasmissivo è condiviso, tutte le stazioni connesse ascoltano questo campo e si segnano la durata della trasmissione corrente nel vettore NAV, "Network Allocation Vector". Rappresenta un contatore per sincronizzare le stazioni. Ogni stazione lo decrementa con il passare del tempo, ed ogni stazioni può trasmettere solamente se questo campo vale zero. Questo campo deve essere presente come primo campo del pacchetto, per essere letto.

Ogni pacchetto spedito da una stazione deve essere riscontrato dalla stazione destinataria tramite un acknowledgment. Quindi una macchina quando calcola la durata della trasmissione, calcola il tempo di trasmissione, nota la banda ed il numero di bit del pacchetto, una durata SIFS, più corta

di DIFS, prima dell'invio dell'acknowledgment, e la durata di questo piccolo pacchetto. Il SIFS è l'interpacket space che separa un pacchetto dal suo acknowledgment. -

La verifica della disponibilità della rete può essere effettuata anche a livello fisico, controllando se nel canale trasmissivo è presente del segnale attivo. Se rileva un segnale attivo aspetta di trasmettere, quindi solo quando entrambe le condizioni fisiche e logiche sono verificate. Una trasmissione non si interrompe fino alla fine, e termina quando viene ricevuto il pacchetto ack. Se non viene ricevuto, oppure è intelligibile, allora si è verificata una collisione, e deve essere ritrasmesso il pacchetto. La stazione mittente si calcola quando dovrebbe ricevere l'acknowledgment. Di tutte le stazioni nella rete, solo la stazione trasmittente è in grado di accorgersi che si è verificata una collisione. In questo caso duplica il valore di *cw* ed aspetta prima di inviare nuovamente il pacchetto.

Se una stazione trasmettesse senza interruzioni, allora il mezzo trasmissivo non sarebbe mai libero. Questo rappresenta un attacco di tipo DOS "Denial Of Service".

Se il pacchetto che viene trasmesso è molto lungo, e si effettua una collisione, la stazione mittente se ne può accorgere solamente dopo il periodo di trasmissione di questo lungo pacchetto. Si perde molto tempo prima dell'identificazione della collisione. Per risolvere questo problema la dimensione massima dei pacchetti WiFi è di 1500 byte come in ethernet. Inoltre è possible che tra le stazioni ci sia visibilità parziale, ovvero può vedere solo una parte della rete.

Quando una stazione vuole trasmettere, invia un frame al destinatario, di breve lunghezza, chiedendo l'autorizzazione alla trasmissione. Se il destinatario è disponibile emette un breve frame di conferma. Alle stazioni vicine è richiesto di non interferire per l'intera durata della trasmissione che sta per avvenire. Questo meccanismo di prenotazione del canale tra due stazioni permette di evitare le collisioni. Se il canale è libero, a stazione mittente invia un pacchetto RTS per richiedere l'autorizzazione, e viene concessa alla stazione con un pacchetto CTS, e tutte le altre stazioni aspettano per il tempo presente nel campo duration dei pacchetti RTS e CTS, invece che nel pacchetto da trasmettere.

Una collisione si verifica quando all'invio del RTS, non viene inviato il CTS. Analogamente alle condizioni precedenti, dove al pacchetto non viene seguito l'ack.

Il valore di *cw* viene decrementato solamente se il canale è libero, quando NAV è pari a zero. L'algoritmo di backoff rappresenta un algoritmo distribuito su molte macchine.

Su ogni stazione WiFi è presente un parametro ch indica quale pacchetti da utilizzare. Viene utilizzato RTS/CTS per pacchetti di lunghezza maggiore a questo parametro s. In queste reti senza fili l'insieme delle stazioni appartenenti ad uno stesso BSS cambia continuamente. Per poter accedere ad un BSS si possono utilizzare protocollo di handshake in due modalità.

Si utilizza un protocollo di handshake per scambiare informazioni tra l'AP ed il BSS. Ogni stazione AP presente il proprio indirizzo MAC, potrebbe inviare un messaggio al BSS per indicare la sua presenza alla rete, tramite un pacchetto broadcast chiamato "beacon frame". Altrimenti la stazione potrebbe inviare pacchetti sonda di "probe", trasmettendo pacchetti "probe request", per esplorare la rete, ed attende un pacchetto di "probe response. "

Un amministratore può definire varie reti logiche sulla stessa rete fisiche, ciascuna identificata a un suo SSID. Solo chi ha gli opportuni permessi può accedere ad una carta rete logica. Si definisce ESS, "Extended Service Set" l'insieme delle stazioni appartenenti ai BSS di una rete e con lo stesso SSID.

Le stazioni nello stesso ESS, possono muoversi cambiando BSS.

Il livello MAC può decidere se frammentare un pacchetto e si occupa anche del riassemblaggio. In queste reti è consigliabile diminuire l'overhead di un pacchetto e ridurre la probabilità di collisione, diminuendo la dimensione dei singoli pacchetti. Ogni frammento del "MAC service data unit" viene frammentato e ciascuno di questi frammenti viene trattato come un pacchetto e viene riscontrato singolarmente. La dimensione dei frammenti può essere modificata dall'utente per guadagnare un vantaggio in trasmissione sulle altre stazioni. In ricezione il livello MAC ricompone questi frammenti in modo che gli strati superiori non si accorgono della frammentazione, né gli enti MAC che non sono coinvolti nella trasmissione.

In questo momento storico i riscontri di LLC non vengono utilizzati, quindi anche se nello standard è possibile che l'invio e ricezione di pacchetti ack sia effettuata a livello LLC.

Per inviare pacchetti di tipo broadcast, dove ToDS sia pari a zero, non si utilizzano ack e RTS/CTS, le eventuali collisioni non vengono quindi rilevate. Quando ToDS è pari ad uno, si utilizzano pacchetti di ack, ed in caso RTS/CTS, per i pacchetti diretti verso gli AP. Si può configurare l'AP in modo che ogni pacchetto broadcast ricevuto venga inviato o meno a tutto il BSS.

5 Livello 3: Il Livello di Rete

Il livello di rete sceglie un percorso per i pacchetti, conoscendo la topologia della rete, attraverso passaggi intermedi chiamati salti o hop tra varie stazioni.

Se il destinatario è nella stessa LAN del mittente, allora lo raggiunge direttamente, altrimenti deve percorrere diverse reti geografiche effettuano questi salti. Fino ad ora ci si è occupati di ogni salto separatamente tra la rete locale o la rete geografica attraverso un singolo filo, o mezzo trasmissivo. Per connettere tra di loro LAN e WAN si utilizzano reti di raccolta o di accesso.

5.1 Reti di Raccolta e Reti di Accesso

Nella LAN la trasmissione tar due stazioni, per quanto sia complessa la topologia della rete, è sempre diretta. Nelle reti geografiche (WAN), la trasmissione tra due stazioni a livello due avviene su un canale punto-punto. Viene realizzato solamente tramite un filo, non sono necessarie altre componenti della rete. Tipicamente questo filo viene realizzato da ethernet, anche se sviluppato principalmente per reti locali.

I collegamenti tra questi due tipi di rete vengono realizzati dall'ISP di cui si usufruiscono i servizi. Questa zona intermedia viene realizzata tramite reti di raccolta o di accesso. La rete di raccolta è la rete nella quale si raccoglie il traffico, mettendolo assieme, proveniente da tutte le stazioni coperte dal servizio dell'ISP. Le reti di accesso permettono, una volta raccolto il traffico, di accedere alla rete geografica vera e propria, composta da lunghi collegamenti punto-punto.

Per molti anni in quasi tutti i paesi del mondo, la rete di raccolta è stata la rete telefonica, due fili di rame, un doppino telefonico. Questa struttura molto pervasiva è stata il supporto delle comunicazioni di rete per molti anni. In seguito venne effettuata una progressiva sostituzione tra rame e fibra ottica, secondo una terminologia FTTx, "Fiber To The x", che distingue tra quanto vicino la stazione è vicina alla fibra ottica. La linea di tendenza punta a FTTH, "Fiber To The Home", dove la fibra ottica arriva direttamente alla stazione. Un altro metodo di raccolta simile è FTTB, che utilizza le esistenti strutture telefoniche per trasmettere i dati all'interno dell'edificio.

FTTN, "Fiber TO The Node", e FTTC, "Fiber To The Center", sono difficili da distinguere, questi rappresentano gli accessi xDSL o aDSL, quelli normalmente venduti, il caratteri prefisso di DSL descrive la trasmissione in termini di bilanciamento e traffico disponibile. In generale il cavo in fibra ottica raggiunge una stazione centrale che utilizza le preesistenti

Tipicamente gli accessi FTTH e FTTB sono a 1 Gb/s, recentemente si stanno vendendo accessi a velocità superiore. Queste strutture utilizzano la tecnologia GPON, "Gigabit-capable Passive Optical Network", il dispositivo vero e proprio di cui fanno uso è l'OLT, "Optical Line Termination", essenzialmente è uno switch. Permette di collegare fino a 64 clienti sullo stesso OLT. Al livello del cliente è presente un dispositivo router su cui si può connettere per accedere, questi sono collegati a vari livelli di splitting ottico, per connettere tutti i router dei clienti, connessi tutti su una porta di uno switch OLT. Questi dispositivi di splitting ottico non necessitano di alimentazione, ma unisce tra di loro il traffico proveniente da più clienti.

La banda di questi OLT arriva fino a 1 Gb/s, ma se più clienti vengono connessi alla stessa porta allora la banda effettiva per clienti diminuisce all'aumentare dei clienti, fino a 64 per porta. Questa è la rete con cui i provider attualmente raccolgono il traffico.

Per essere collegati alla WAN, si utilizza la rete di accesso, realizzata tramite switch OLT tutti collegati tra di loro, con un estensione geografica significativa. Ma è consigliabile non estendere troppo questa struttura, generalmente si indica come MAN. La maggior parte dei provider realizza la propria rete di accesso tramite un anello che connette le varie reti di raccolta e ciò che lo collega alla spina dorsale, la WAN, del provider è un nodo di aggregazione. Vengono realizzati in cicli per mantenere una certa resistenza ai guasti, e si utilizzano alberi ricoprenti di anello e loop-avoidance con tecnologie analoghe alle reti locali, per mantenere attivi solo i collegamenti strettamente necessari. Se si rompe un singolo switch, solo i clienti attestati a quello switch subiranno un disservizio. Generalmente vengono utilizzati più aggregation node, per mantenere un'importante resistenza ai guasti. Questo meccanismo di duplicare componenti può essere attuato a vari livelli per mantenere alta la resistenza del provider.

Molto spesso per aumentare la robustezza si utilizzano più anelli con doppi collegamenti, anche in fibra, che effettuano percorsi diversi. Si utilizza una nello poiché è la struttura contenente cicli più semplice possibile.

5.2 Indirizzo ed Instradamento

Il livello di rete fornisce servivi al livello di trasporto, che non è interessato della topologia delle varie reti attraversate per raggiungere una destinazione. Inoltre non conosce le tecnologie attraversate al livello due. Può offrire servizi connessi o non. Il protocollo di rete più diffuso IPv4 utilizza un protocollo di rete non connesso, utilizzano instradamento a datagramma, mentre un livello di rete connesso utilizza la commutazione a circuito virtuale. Ma questa distinzione non è strettamente mantenuta.

Il livello di trasporto deve conoscere degli indirizzi distribuiti in modo consistente su tutta la rete, in modo da poterle identificare univocamente tra rete locale e geografica. Una primitiva di servizio non connesso offerta al livello di trasporto indica l'indirizzo livello 3 del destinatario ed il suo payload, questo sarà ricevuto dal livello quattro corrispondente.

Dal punto di vista livello tre i sistemi possono essere "End System", ES, o "Intermediate System", IS. Ad ogni sistema viene associato un indirizzo numerico per poterlo identificare. Ad ogni sistema spesso viene associato un nome, la cui corrispondenza all'indirizzo viene gestita da server appositi presenti sulla rete.

Spesso queste apparecchiature intermedia si chiamano router o gateway, contengono almeno i primi tre strati della pila ISO-OSI, talvolta per motivi di gestione devono contenere anche livelli superiori. Alcuni casi di instradamento avvengono anche a livello due, anche se principalmente a livello 3.

L'indirizzo di livello due identifica un destinatario solamente all'interno di una LAN, mentre l'indirizzo di livello tre deve poter identificare il destinatario all'interno del'intera rete. Un sistema necessita di tanti indirizzi MAC quante sono le schede di rete al suo interno, ma è possibile associare una singola macchina ad un singolo indirizzo di livello tre, ma è possibile per alcuni protocolli, come IPv4 e IPv6, di essere associati ad indirizzi di livello tre differenti.

Esistono protocolli appositi per gestire e stabilire la corrispondenza tra gli indirizzi di livello due e livello tre. Ma gli indirizzi di livello due, i MAC address, sono univoci a livello globale, quindi si potrebbe utilizzare questi indirizzi. Il problema degli indirizzi MAC è che sono distribuiti

casualmente, ma sarebbe utile ai fini di individuare le stazioni se gli indirizzi associati a macchine vicine avessero caratteristiche simili. Poiché gli indirizzi MAC individuano univocamente la scheda di rete, mente gli indirizzi di livello tre possono cambiare, utilizzare solo i MAC comporterebbe problemi di privacy.

In linea di principio si possono individuare tre tipi di instradamento principali:

- Routing by Network Address: nel pacchetto c'è l'indirizzo del sistema destinatario, potrebbe non essere l'indirizzo dell'ES, ma di una sua interfaccia. Con commutazione a datagramma su questo indirizzo;
- Label Swapping: nel pacchetto non c'è l'indirizzo, ma un'etichetta che individua un cammino virtuale, con commutazione a circuito virtuale basata su queste etichette;
- Source Routing: nel pacchetto è indicata la lista ordinata di tutti gli IS da attraversare per raggiungere la destinazione.

5.2.1 Routing by Network Address

Quando il pacchetto raggiunge un IS, con varie linee di inoltro, questo guarda la sua tabella di instradamento locale e cerca come chiave di ricerca l'indirizzo del destinatario e restituisce la linea dove deve essere inoltrato il pacchetto. La commutazione è a datagramma poiché questa tabella può variare nel tempo. Questo rappresenta il modo più semplice di instradamento, operato dagli switch, dove la tabella di instradamento viene chiamata filtering database.

Se l'indirizzo non fosse presente nella sua tabella di instradamento, allora il pacchetto viene buttato, a differenza dei bridge, poiché su reti grandi l'inoltro di tutti i pacchetti sconosciuti su tutte le linee comporterebbero un aumento considerevole del traffico.

Sono necessari quindi dei protocolli per poter definire gli indirizzi e conoscere la topologia della rete, essendo dinamica. Questi meccanismi permettono di compilare automaticamente le tabelle di instradamento dell'intera rete. Ma è possibile che siano compilate manualmente, anche se non realistico. Ma questo processo di instradamento è indipendente dal chi ha compilato la tabella.

5.2.2 Label Swapping

Se due stazioni vogliono comunicare, in una rete a circuito virtuale, viene stabilito il percorso che deve attraversare il pacchetto. Le apparecchiature intermedie vengono quindi informate sul percorso che deve essere effettuato. Questo percorso viene identificato da un'etichetta in modo che all'arrivo del pacchetto presso un IS, si utilizza una tabella dove sono presenti le etichette ed i possibili percorsi, e quindi viene inviato su una certa linea. Questa tabella è locale e molto piccola, e determina la linea di ritrasmissione del pacchetto.

Deve essere stabilito il percorso tra le stazioni, analogamente alla tabella di instradamento per l'instradamento precedente. La differenza tra queste due tabelle è nelle loro dimensioni, infatti è necessaria una tabella che contenga tutti i destinatari per il meccanismo di instradamento precedente, mentre per una tabella delle etichette deve contenere solamente i possibili percorsi. Il numero di righe non è funzione del numero di stazioni globalmente presenti nella rete, ma dal numero di

circuiti virtuali che la attraversano in ogni dato istante. É irragionevole che in una rete tutte le stazioni trasmettano a tutte le altre stazioni.

Per evitare di dover generare etichette uniche in tutta la rete, e quindi verificarne la disponibilità, ad ogni tratto del percorso viene assegnata un'etichetta diversa localmente. In questo modo numero di etichette disponibili non è un limite superiore al numero dei circuiti virtuali attivabili. Queste etichette sono contenute in un campo nell'intestazione del pacchetto.

5.2.3 Source Routing

Nel pacchetto viene specificata la lista delle stazioni da attraversare per raggiungere la destinazione. Il ruolo dell'IS deve solo leggere questa lista e determinare la stazione successiva al quale inoltrare il pacchetto.

5.3 Router

L'architettura di un router è formato da un algoritmo per calcolare la tabella di instradamento, la tabella stessa ed il processo di inoltro dei pacchetti. In questo corso non si occupa dell'algoritmo di creazione automatica della tabella di instradamento.

Ciò che costituisce la tabella di instradamento ed il processo di ritrasmissione di un pacchetto rappresenta il "data plane", mentre l'algoritmo di costruzione della tabella di instradamento consiste nel "control plane".

In un router multiprocollo sono presenti diversi di queste pile di data e control plane per ogni protocollo, mantenendo le stesse interfacce. Un router può partecipare contemporaneamente a diverse tecnologie, senza che queste diverse tecnologie e protocolli conoscano la loro presenza. Se ad un router arriva un pacchetto destinato ad un protocollo che non può gestire, viene buttato.