

Reti di Telecomunicazioni

Fondamenti e Tecnologie Internet

Romano Fantacci



ISBN 978-88-7488-771-2

Prima edizione: Luglio 2014

Responsabile produzione: Alessandro Parenti

Redazione: Giancarla Panigali e Carlotta Lenzi

Fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, comma 4 della legge 22 aprile 1941, n. 633 ovvero dall'accordo stipulato tra SIAE, AIE, SNS e CNA, CONFARTIGIANATO, CASA, CLAAI, confcommercio, confesercenti il 18 dicembre 2000.

Le riproduzioni ad uso differente da quello personale potranno avvenire, per un numero di pagine non superiore al 15% del presente volume, solo a seguito di specifica autorizzazione rilasciata da AIDRO, via delle Erbe, n. 2, 20121 Milano, Telefax 02-80.95.06, e-mail: aidro@iol.it



40131 Bologna - Via U. Terracini, 30 - Tel. 051-63.40.113 - Fax 051-63.41.136
www.editrice-esculapio.it

Ai miei studenti

Indice

Romano Fantacci

Reti di Telecomunicazioni *Fondamenti e Tecnologie Internet*

Prefazione	xi
1 Introduzione	1
1.1 Modalità di Comunicazione	3
1.2 Caratteristiche di una Rete di Telecomunicazioni	3
1.3 Topologia	4
1.3.1 Topologia a maglia (Mesh)	4
1.3.2 Topologia a stella (Star)	5
1.3.3 Topologia lineare (Bus)	5
1.3.4 Topologia ad anello (Ring)	6
1.4 Tecniche di commutazione	7
1.4.1 Tecnica a commutazione di circuito	7
1.4.2 Tecnica a commutazione di messaggio	8
1.4.3 Tecnica a commutazione di pacchetto	9
1.4.4 Confronto tra le varie tecniche	11
1.5 Letture Consigliate	12
2 La rete telefonica	13
2.1 Telefonia	14
2.1.1 Telefonia analogica	14
2.1.2 Telefonia numerica	15
2.2 Tecniche di multiplexing	16
2.2.1 Multiplexing a divisione di frequenza	17
2.2.2 Multiplexing a divisione di tempo	18
2.2.3 Multiplexing a divisione di lunghezza d'onda	19
2.2.4 Servizio dati in rete telefonica: tecnologie xDSL	19
2.3 Letture Consigliate	21
3 I commutatori	23
3.1 Strutture a divisione di spazio	25
3.2 Strutture a divisione di tempo	26
3.3 Strutture multistadio	28
3.3.1 Struttura S-S	28
3.3.2 Struttura T-S	31
3.3.3 Struttura S-T	32
3.3.4 Struttura S-S-S	33
3.3.5 Struttura T-S-T	36

3.3.6	Analisi di Lee	38
3.4	Commutatori Veloci a Pacchetto	39
3.5	Letture Consigliate	40
4	Reti per trasmissione di dati	41
4.1	Architettura a livelli	42
4.2	Modello ISO/OSI	46
4.3	Architetture Proprietarie	50
4.4	Modello TCP/IP	51
4.5	Suite Protocollare TCP/IP	52
4.5.1	Livello Host to Network	52
4.5.2	Livello Internet	53
4.5.3	Internet Protocol version 4	53
4.5.4	Internet Protocol versione 6	60
4.5.5	Livello Trasporto	67
4.5.6	Livello Applicativo	72
4.6	Confronto tra architettura TCP/IP e ISO/OSI	73
4.7	Modello IEEE 802	73
4.7.1	Sottolivello Logical Link Control	75
4.7.2	Sottolivello Medium Access Control	77
4.7.3	Livello Fisico	79
4.8	Rete Distribuited Queue Double Bus (DQDB)	80
4.8.1	Struttura di un nodo DQDB	81
4.9	Rete Fiber Distributed Data Interface (FDDI)	83
4.9.1	Livello MAC	84
4.10	Letture Consigliate	86
5	Accesso Multiplo	87
5.1	Tecniche ad accesso ordinato	87
5.1.1	Tecniche Polling	88
5.1.2	Token Passing	90
5.2	Tecniche ad accesso casuale	90
5.2.1	Aloha	91
5.2.2	CSMA	93
5.3	Letture consigliate	97
6	Rete Ethernet	99
6.1	Livello MAC	99
6.2	Livello fisico	101
6.2.1	Ethernet standard	101
6.2.2	Ethernet veloce	102
6.2.3	Ethernet gigabit	103
6.2.4	Ethernet 10-gigabit	104
6.3	Dispositivi di connessione	105
6.3.1	Hub passivi	105
6.3.2	Ripetitori e Hub attivi	105

6.3.3	Bridge	106
6.3.4	Switch	106
6.3.5	Router	108
6.3.6	Gateway	109
6.4	Un caso pratico : Il Proxy	109
6.5	Letture Consigliate	110
7	Reti wireless	111
7.1	IEEE 802.11	112
7.1.1	Architettura di rete	112
7.1.2	Livello fisico	113
7.1.3	Livello MAC	115
7.2	IEEE 802.16	125
7.2.1	Livello Fisico	126
7.2.2	Gestione della QoS	126
7.3	IEEE 802.15.1	127
7.3.1	Architettura	128
7.3.2	Architettura Protocollare Bluetooth	128
7.4	Tecnologia RFID	132
7.5	Letture Consigliate	134
8	Reti di sensori	135
8.1	Generalità	135
8.2	Accesso Multiplo	138
8.3	Ultra WideBand	139
8.4	IEEE 802.15.4	141
8.5	IEEE 802.15.3	144
8.6	Il protocollo 6LoWPAN	146
8.7	Data Centric Forwarding	148
8.7.1	Direct Diffusion	149
8.7.2	Sensor Protocols for Information via Negotiation (SPIN)	150
8.8	In-Network Processing	151
8.8.1	Clustering	151
8.8.2	Low-Energy Adaptive Clustering Hierarchy (LEACH)	151
8.8.3	Hybrid Energy-Efficient Distributed Clustering (HEED)	152
8.9	Uno Sguardo Verso il Futuro : Internet of Things e sue evoluzioni .	153
8.10	Le Body Area Network	154
8.11	Letture Consigliate	156
9	Rete ISDN	159
9.1	Raccomandazione X.25	159
9.1.1	Multiplexing	161
9.2	Frame Relay	162
9.3	Principi di ISDN	164
9.4	Canali ISDN	166

9.5 Accesso alla Rete	168
9.6 Architettura protocollore	170
9.7 Letture consigliate	171
10 Sistema di segnalazione SS7	173
10.1 Sistemi di segnalazione	173
10.2 Segnalazione inter-nodo a canale comune	175
10.3 Sistema di Segnalazione No. 7 (SS7)	176
10.3.1 Architettura Protocollare	176
10.4 <i>Letture consigliate</i>	178
11 Rete SDH	181
11.1 SDH: Principi Base	181
11.2 Dispositivi di Rete	184
11.3 Architettura a Strati	186
11.4 <i>Letture consigliate</i>	187
12 Rete ATM	189
12.1 Generalità	189
12.1.1 Cella ATM	192
12.2 Architettura protocollore ATM	193
12.3 Architettura ATM	196
12.4 Letture consigliate	198
13 Algoritmi di routing	199
13.1 Generalità	199
13.2 Algoritmi senza tabella	203
13.3 Algoritmi con tabella	205
13.3.1 Distance vector	205
13.3.2 Link state	209
13.3.3 Distance vector e link state a confronto	211
13.4 Dalla teoria alla pratica: Architettura di un router Link State	211
13.5 Algoritmi gerarchici	212
13.6 Routing su base etichetta: Multiprotocol Label Switching	214
13.7 Routing Broadcast e Multicast	217
13.7.1 Broadcast	217
13.7.2 Multicast	218
13.8 Un caso di studio: Il protocollo di routing RPL	220
13.8.1 Messaggi di controllo RPL	223
13.8.2 Funzionamento del protocollo RPL	224
13.8.3 Inserimento in un DODAG e gestione delle rotte	225
13.9 Letture Consigliate	227

14 Controllo della congestione	229
14.1 Generalità	229
14.2 Controllo Proattivo	231
14.2.1 Leaky Bucket	231
14.2.2 Token Bucket	232
14.3 Controllo reattivo	234
14.3.1 Sliding Window	234
14.3.2 Un caso pratico: Controllo della congestione in TCP	236
14.4 Letture Consigliate	237
15 Sicurezza delle reti	239
15.1 Introduzione	239
15.2 Elementi di crittografia	240
15.3 Crittografia a chiave simmetrica	241
15.4 Crittografia a chiave pubblica (asimmetrica)	242
15.4.1 Algoritmo RSA	242
15.5 Un caso pratico: Firewall	244
15.6 Letture Consigliate	245
Sigle	247
Glossario	251
Indice analitico	253

Prefazione

Le reti telecomunicazioni e le tecnologie Internet, in particolare, hanno registrato un crescita tecnologica che difficilmente trova paragoni in altri settori e sono divenuti un elemento pervasivo ed irrinunciabile della nostra vita quotidiana. Conseguenza di tutto questo è che una profonda conoscenza delle metodologie e dei principi base delle reti di telecomunicazioni è divenuta di fondamentale importanza per molte professioni. Per questi motivi, un corso di Fondamenti di Reti di Telecomunicazioni ricopre un ruolo importante nel percorso formativo degli studenti universitari e non deve essere considerato limitato al solo settore dell'Ingegneria dell'Informazione. Il volume si propone come supporto didattico per gli studenti dei corsi universitari di primo livello inerenti le Reti di Telecomunicazioni e le loro applicazioni. Il testo è stato concepito in accordo con il recente riordino degli studi con l'obiettivo principale di fornire uno strumento per acquisire conoscenze di base nel settore delle Reti di Telecomunicazioni con specifico riferimento alle Tecnologie Internet in relazione a differenti contesti applicativi. Nella stesura del volume si è cercato di stabilire un filo conduttore tra la trattazione di argomenti classici e la discussione di tematiche più recenti ed innovative come le reti wireless, le reti di sensori ed i nuovi paradigmi di comunicazioni autonomiche e Internet of Things.

Organizzazione e contenuti del testo

L'organizzazione dei contenuti del testo ha avuto come obiettivo principale quello di facilitarne la lettura e di favorire in questo modo una rapida e completa comprensione dei concetti e dei principi esposti. In particolare, pur cercando di mantenere un rigore concettuale nella presentazione e discussione delle varie tematiche esaminate nel testo, si è evitato una presentazione troppo rigorosa cercando di privilegiare, ovunque possibile, gli aspetti applicativi delle metodologie considerate.

Il testo ha un carattere prettamente introduttivo ed è per questo motivo che non necessita, per la comprensione dei concetti esposti, di nozioni di base specifiche ed è rivolto, principalmente, agli studenti dei corsi di Laurea del settore dell'Ingegneria dell'Informazione ma è di facile comprensione anche per studenti di altre Classi di Laurea.

Il volume prevede complessivamente quindici capitoli attraverso i quali si è cercato di trattare in maniera esaurente i principi base e gli argomenti principali riguardanti la tecnologia Internet e, più in generale, il settore delle reti di telecomunicazioni fornendo, inoltre, una descrizione dettagliata delle nuove tematiche emergenti nel settore. Al termine di ogni capitolo viene poi proposta una lista di testi, articoli scientifici e documentazione tecnica per permettere ad ogni lettore interessato di reperire approfondimenti e complementi a quanto esposto nel testo. I contenuti di ogni capitolo sono brevemente indicati di seguito.

Nel capitolo 1 vengono introdotti i concetti di base del settore delle reti di telecomunicazioni e sono, inoltre, delineate le evoluzioni più recenti verso i nuovi paradigmi delle comunicazioni autonomiche tra macchine e dispositivi e al riguardo della nuova realtà di una rete Internet di oggetti intelligenti.

Nel capitolo 2 viene presentata la rete telefonica sia nella sua versione analogica sia nella più recente versione numerica. Per facilitare lo studente nella comprensione dei concetti esposti vengono inoltre richiamati i principi base della trasmissione e multiplazione sia di segnali analogici che numerici. Il capitolo propone anche una descrizione della tecnologia xDSL soffermandosi in particolare sulle sue più recenti evoluzioni.

Il capitolo 3 illustra i principi base della commutazione e discute le relative strutture identificando i criteri di progetto più adeguati in relazione a specifici requisiti di servizio. Nel capitolo vengono anche trattate le più recenti strutture di commutazione veloce di pacchetto.

Il capitolo 4 affronta il vasto argomento delle reti per trasmissione dati. Nella sua parte iniziale vengono definiti i concetti base di una architettura a livelli. Successivamente vengono discussi i principi architettonici ed i meccanismi per il trasferimento dell'informazione in reti di calcolatori. Viene inoltre considerato anche il caso di reti che si estendono lungo distanze brevi. La maggior parte del materiale presentato in questo capitolo è comunque inerente la suite protocollare TCP/IP.

Il capitolo 5 si occupa nello specifico delle problematiche proprie dell'accesso multiplo cioè delle metodologie di condivisione di uno stesso canale di comunicazione da parte di più utenti. Vengono presentate e discusse criticamente sia tecniche di accesso senza contesa che con contesa.

Il capitolo 6 è dedicato alla descrizione della tecnologia Ethernet in relazione sia ad implementazioni base sia alle sue recenti evoluzioni tecnologiche verso reti più complesse e veloci. Nello stesso capitolo vengono inoltre presentati gli apparati e le principali metodologie utilizzate per realizzare l'interconnessione di reti.

Il capitolo 7 si concentra sulle reti wireless per comunicazioni dati. Vengono considerate diverse tecnologie in relazione alle velocità di accesso, all'estensione e alla tipologia dei servizi offerti agli utenti. Per ciascuna tipologia di rete considerata vengono discussi i principi architettonici e le metodologie previste per il trasferimento dei dati.

Il capitolo 8 si occupa del settore emergente delle reti di sensori. In particolare viene presentata l'architettura di un nodo sensore e vengono descritti i principali standard ad oggi utilizzati. Il capitolo fornisce anche una presentazione di metodologie avanzate relative all'elaborazione dell'informazione acquisita dai dispositivi sensoriali ed alle modalità di distribuzione della stessa verso gli

utilizzatori. Il capitolo si conclude con la presentazione delle body area network per le quali vengono individuati i settori di impiego considerati, ad oggi, di maggiore interesse.

Il capitolo 9 inizia con la presentazione della raccomandazione X.25 e continua con la descrizione della tecnologia Frame Relay in relazione a reti di generazioni successiva. Il capitolo tratta inoltre le reti ISDN concentrandosi, in particolare, sugli aspetti architetturali e sulle metodologie previste per l'accesso di utente.

Il capitolo 10 tratta un argomento decisamente importante, ma anche molto complesso, quello della segnalazione di rete. Dopo l'introduzione dei concetti di base, il capitolo si concentra sulla descrizione del sistema di segnalazione SS7 che è, ad oggi, il sistema di segnalazione più evoluto disponibile per le reti di telecomunicazione.

Il capitolo 11 presenta la tecnologia SDH (Synchronous Digital Hierarchy) intesa come metodologia per il trasporto dell'informazione in forma digitale in reti estese ad alta velocità.

Il capitolo 12 è dedicato alla descrizione dei principi base della tecnologia ATM (Asynchronous Transfret Mode) la cui funzionalità primaria è quella di essere in grado di gestire il trasporto ad alto data rate di diverse tipologie di traffico (voce, dati, multimediale). Il capitolo inizialmente propone una descrizione generale della tecnologia ATM ed illustra il suo inquadramento temporale nel percorso evolutivo delle reti di telecomunicazioni. Successivamente viene descritto il funzionamento delle reti ATM partendo da una sintetica introduzione della sua struttura protocollare e delle modalità previste per la gestione dei diversi servizi a cui la rete si rivolge.

Il capitolo 13 si concentra sui principi alla base degli algoritmi di instradamento intesi come procedure che coinvolgano più dispositivi di una stessa rete per consentire il collegamento tra una dispositivo sorgente con il dispositivo destinazione. Il capitolo illustra ed analizza i principali algoritmi utilizzati nelle attuali reti di calcolatori con particolare riferimento alle reti in tecnologia TCP/IP.

Il capitolo 14 affronta il problema del controllo della congestione in una rete a commutazione di pacchetto considerando le principali metodologie utilizzate sia per prevenirla sia per contenerla o, addirittura, risolverla quando questa si manifesta. Come nel caso del capitolo precedente, la trattazione si focalizza principalmente sulle tecniche utilizzate in reti TCP/IP.

Il capitolo 15 conclude il testo occupandosi di problematiche, oggi molto attuali, relative alla sicurezza e confidenzialità delle informazioni scambiate attraverso una rete di calcolatori, o più in generale di dispositivi intelligenti ed autonomi. In particolare, argomento di questo capitolo è la descrizione di due tecniche

di crittografia che consentono di rendere riservato e confidenziale lo scambio dei messaggi.

Come utilizzare il testo

La struttura del testo è stata pensata per lasciare al docente la libertà di affrontare gli argomenti trattati nei vari capitoli in qualsiasi ordine. La raccomandazione è comunque che, dopo il capitolo introduttivo, i docenti trattino i capitoli dal 2 al 8 in sequenza, presentando gli argomenti in maniera da stabilire un filo conduttore tra la trattazione di argomenti classici e la discussione di tematiche più recenti ed innovative.

Ringraziamenti

L'autore desidera ringraziare David per aver proposto e curato la grafica della copertina e, in particolare, Francesca per la competenza, l'entusiasmo e la pazienza con cui ha contribuito alla stesura del testo. Un profondo e affettuoso ringraziamento va inoltre a tutte quelle persone che, a diverso titolo, con ruoli ed in momenti diversi, hanno consentito di portare a compimento questo lavoro.

Firenze, Giugno 2014

*Romano Fantacci
Università degli Studi di Firenze*

Introduzione

Con il termine telecomunicazione si intende la capacità di due o più individui, ed oggi anche dispositivi, generalmente non vicini tra loro, di condividere informazioni di vario genere attraverso collegamenti in aria (wireless) o cablati (wired). In termini generali, come delineato in *Kurose'2013* (vedi paragrafo 1.5), si può affermare che così come il diciottesimo secolo è stato caratterizzato dalla rivoluzione dall'era industriale, conseguenza dell'affermarsi della tecnologia dei grandi sistemi meccanici, ed il secolo seguente dell'invenzione ed uso del motore a vapore che ha permesso il superamento di lunghe distanze in tempi più ragionevoli, il ventesimo secolo ha visto come tecnologia caratterizzante l'elaborazione, la raccolta e la distribuzione dell'informazione. Senza dubbio possiamo considerare la capacità di inviare a distanza messaggi scritti, suoni e immagini come una delle grandi conquiste tecnologiche dell'uomo da cui poi è derivato il profondo cambiamento che la nostra società ha vissuto e sta tuttora vivendo. Le reti di telecomunicazioni sono l'elemento pervasivo che sta caratterizzando, sia direttamente che indirettamente, tramite le sue innumerevoli applicazioni, il ventunesimo secolo. Oggi abbiamo reti di telecomunicazioni sempre più veloci capaci di condividere grosse quantità di informazioni in tempi estremamente bassi e di permettere, oltre alla comunicazione tra persone, anche collegamenti tra soli dispositivi (Device-to-Device (D2D)) e macchine (Machine-to-Machine (M2M)) in modalità automatica cioè senza bisogno di interventi diretti dell'uomo. Come avremo modo di vedere nei prossimi capitoli, esiste una moltitudine di sistemi, tra loro anche profondamente diversi, per trasmettere a distanza informazioni, ma tutti hanno in comune il fatto di usare una struttura a rete, in cui cioè il segnale, quando deve essere inviato da una stessa sorgente ad una stessa destinazione, non segue necessariamente un percorso obbligato, ma può essere indirizzato, di volta in volta, verso percorsi differenti. In questo senso, ogni rete di telecomunicazioni è definita da un mezzo fisico usato per trasmettere il segnale e da un sistema che permette, a partire da un punto della rete, di entrare in collegamento con un altro punto scelto come destinatario della comunicazione, generalmente su una base temporale finita. Una rete di telecomunicazioni può quindi essere considerata come un insieme di dispositivi e dei loro collegamenti (fisici o logici) che consentono la trasmissione e la ricezione di informazioni tra due o più utenti situati in posti distinti. Una volta che la connessione tra



Figura 1.1: Rappresentazione di un sistema di telecomunicazioni

due utenti (o dispositivi) della rete è stata resa disponibile, il sistema di telecomunicazioni si riconduce allo schema classico end-to-end illustrato nella figura 1.1.

Le reti di telecomunicazioni sono strutture tecnologiche di grande complessità, che mettono in collegamento i loro utenti (persone, dispositivi) senza che vi siano, almeno virtualmente, limiti al loro numero. La prima rete moderna è stata quella telegrafica, che ha costituito il modello per la successiva rete telefonica, da cui poi si sono sviluppate le moderne reti telematiche e Internet. In particolare la rete Internet è da molti considerata come il più grande sistema complesso realizzato dall'uomo. Questa rete consente connessioni pervasive ed ubiquie tra milioni di elaboratori, tablet, sensori, webcam, smartphone, console di gioco, ed, ad oggi, anche oggetti e dispositivi che sempre di più diventano i protagonisti della nostra vita quotidiana. La rete internet deve poi essere considerata come una *infrastruttura che fornisce servizi alle applicazioni*. Genericamente possiamo identificare come applicazioni Internet la posta elettronica, la navigazione sul WEB, le social networks, telefonia su Internet (VoIP), televisione su internet, streaming video, giochi distribuiti, condivisione di file in modalità Peer-to-Peer (P2P) e molto altro ancora.

Nonostante i notevoli ed inimmaginabili progressi conseguiti, il settore delle reti di telecomunicazioni è in continua evoluzione ed è, ad oggi, l'elemento principale dell'Information Communication Technology (ICT). Nuove prospettive applicative si presentano oggi per le reti di telecomunicazioni nella sanità, nel controllo dell'ambiente e della qualità della vita, per la tutela del patrimonio artistico e a supporto della sicurezza del cittadino. Esse costituiscono la principale tecnologia abilitante per la domotica, cioè l'integrazione funzionale delle risorse impiantistiche ed oggetti nell'ambito di un edificio, per il nuovo paradigma di città intelligente e sostenibile (Smart City) e per una più efficiente gestione delle reti di distribuzione dell'energia elettrica (Smart Grid). Alle applicazioni in ambienti classici si sono poi recentemente aggiunte applicazioni specifiche in ambienti ritenuti fino a qualche anno fa improponibili come l'ambiente sottomarino, avionico, spaziale e perfino molecolare. Da ricordare, infine, come la necessità di rispondere efficacemente alle esigenze di applicazioni sempre più sfidanti ed estreme abbia richiesto terminali e dispositivi di rete sempre più tecnologicamente complessi ed evoluti, in grado perfino di comunicare direttamente tra loro in maniera autonoma, di interpretare le esigenze di contesto e prendere decisioni in accordo con l'emergente nuovo paradigma delle Self-Aware Internet-of-Things e più in generale con le metodologie proprie dei sistemi autonomici (Autonomic Systems).

1.1 Modalità di Comunicazione

In generale si hanno tre possibili modalità di trasmissione e ricezione di informazioni su un canale di comunicazione:

- **simplex**: in questa modalità la comunicazione è unidirezionale, ovvero soltanto un dispositivo trasmette e l'altro può solo ricevere;
- **half-duplex**: in questa modalità i due dispositivi possono sia trasmettere sia ricevere, ma non nello stesso istante; la comunicazione si dice che è bidirezionale alternata. Un esempio sono i walkie-talkie, quando un walkie-talkie è abilitato alla trasmissione gli altri rimangono in ricezione;
- **full-duplex**: in questa modalità i dispositivi possono inviare e ricevere dati contemporaneamente; la comunicazione quindi è bidirezionale.

Le tre modalità sono illustrate in figura 1.2.

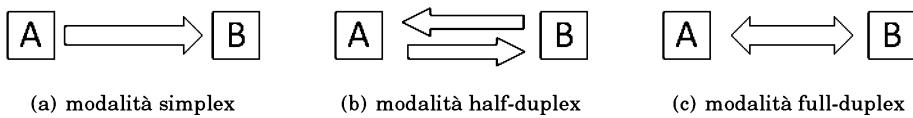


Figura 1.2: modalità di trasmissione e ricezione

1.2 Caratteristiche di una Rete di Telecomunicazioni

Una rete di telecomunicazione in generale viene classificata sulla base dei tre seguenti indicatori:

- *Prestazioni* (performance): il modo più efficiente per valutare le prestazioni di una rete di telecomunicazioni è fare uso delle metriche di throughput e delay. Il throughput di una rete è di solito riferito alla quantità di dati trasmessi in una unità di tempo nel collegamento da e verso gli utenti della rete. Questo parametro indica l'effettivo utilizzo di un collegamento nei confronti della sua massima capacità (sempre espressa in bit/s), cioè la frequenza massima (rate) di trasmissione dei bit nel collegamento. Il delay è invece riferito al tempo che trascorre da quando un flusso informativo ha completato la trasmissione nel canale di comunicazione (lato sorgente) a quando questo viene ricevuto dal suo destinatario. Questo parametro, in genere, dipende dalla modalità con cui l'inoltro del flusso è gestito dalla rete e dalle tecnologie utilizzate. Il caso ideale sarebbe avere un elevato throughput e un basso delay;
- *Affidabilità* (reliability): è legata alla confidenza relativa alla continuità di esercizio della rete;

- **Sicurezza (security)**: indica il livello di protezione dei dati e degli apparati di rete nei confronti di intrusioni esterne.

Il vantaggio principale offerto da una rete di telecomunicazioni è la possibilità di condivisione delle sue risorse (nodi, collegamenti) per consentire le comunicazioni tra dispositivi (utenti) differenti. In generale questa funzionalità diventa indispensabile quando il numero dei dispositivi da connettere è elevato. In questo caso, la soluzione di solito adottata è una suddivisione gerarchica dei dispositivi di rete in più reti elementari che, combinate tra loro, concorrono a definire una struttura di rete più complessa. Un esempio tipico di questa metodologia lo si incontra nella Rete Telefonica pubblica che verrà trattato nel capitolo seguente.

Esistono due modalità principali di comunicazione tra i dispositivi di una rete:

- *punto-punto*: si riferisce ad una comunicazione limitata a due soli dispositivi di rete. Uno ha il ruolo di sorgente del flusso e l'altro di destinatario dello stesso;
- *multi-punto*: in questo caso il flusso informativo di una sorgente ha destinati multipli (multicast) nella rete. Quando tutti i destinati sono tutti gli altri dispositivi di rete si parla di comunicazione broadcast.

Le reti di telecomunicazioni sono infine caratterizzate sulla base della loro **topologia**, riferita al modo con cui i nodi della rete sono collegati tra loro nello spazio (fisica) oppure alla modalità di comunicazione degli stessi (logica); tipo del **servizio offerto** ed infine **area di copertura geografica** cioè l'area entro la quale la rete opera e rende i suoi servizi fruibili agli utenti.

1.3 Topologia

In questa sezione ci riferiremo alla topologia fisica di una rete, cioè alla rappresentazione geometrica dei collegamenti tra i suoi nodi nello spazio. Esistono a questo riguardo 4 topologie di base: **mesh**, **stella**, **bus**, **ring**. È bene inoltre ricordare che le varie topologie base possono essere combinate tra loro, dando origine a topologie di rete ibride più complesse ed articolate.

1.3.1 Topologia a maglia (Mesh)

In una topologia mesh ogni dispositivo ha una connessione dedicata punto-punto. Quindi in una rete di n nodi, si ha $n(n - 1)$ possibili collegamenti. Se i link sono duplex, il numero di collegamenti si dimezza:

$$\frac{n(n - 1)}{2} \simeq n^2$$

Per poter essere connesso a $n - 1$ nodi, un singolo dispositivo deve essere equipaggiato con $n - 1$ porte I/O. Gli ovvi vantaggi che offre questa soluzione riguardano principalmente la possibilità di disporre di collegamenti dedicati ed esclusivi con tutti gli altri nodi della rete. Lo svantaggio evidente è conseguente

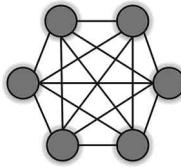


Figura 1.3: Topologia mesh

a questa particolarità, cioè una bassa utilizzazione dei singoli collegamenti ed alla impossibilità di realizzare questa topologia quando il numero di nodi è elevato. Infine, occorre evidenziare che questa topologia di rete è particolarmente resiliente nei confronti di guasti in quanto questi interesseranno soltanto collegamenti fisici specifici e non influiranno sul corretto funzionamento dell'intera rete. Conseguente a questa sua funzionalità è il suo utilizzo frequente quando la continuità di servizio e la velocità nel comunicare sono requisiti predominanti rispetto ad un costo contenuto ed ad un'alta utilizzazione delle infrastrutture di rete. La topologia mesh è mostrata in figura 1.3.

1.3.2 Topologia a stella (Star)

In questo caso i diversi dispositivi (nodi) hanno un collegamento dedicato verso un controllore centrale, chiamato spesso hub (o centro stella), in modo da creare una configurazione che ricorda una stella (star). Si deve notare che i nodi della rete non sono direttamente collegati tra loro. Se due diversi nodi vogliono comunicare tra loro, devono necessariamente passare prima dal centro stella: il nodo sorgente invia i dati al controllore centrale che a sua volta lo indirizza al nodo di destinazione. A differenza della topologia mesh la topologia a stella consente la modalità multicast/broadcast. La topologia a stella prevede poi un numero di cablaggi molto minore rispetto alla topologia mesh e questo si riflette anche sul numero di porte I/O presenti su ciascun dispositivo. In generale, è sufficiente una sola porta per un dispositivo e questo permette quindi di avere un minore costo di installazione e riconfigurazione. Una configurazione a stella ha una buona resilienza nei confronti di guasti di nodi o dei collegamenti individuali verso il centro stella ed è in questo confrontabile con la topologia mesh. Tuttavia in questo caso, rispetto ad una rete mesh, è presente lo svantaggio che se il nodo centrale si guasta questo implica il blocco di tutta la rete. La topologia a stella è mostrata in figura 1.4.

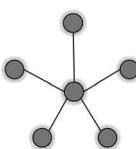


Figura 1.4: topologia stella

1.3.3 Topologia lineare (Bus)

La topologia a bus supporta indifferentemente sia la modalità punto-punto che multi-punto. In una topologia a bus ogni dispositivo (nodo) della rete è fisicamente connesso al bus tramite un connettore. La propagazione del segnale nel bus avviene nelle due direzioni possibili rendendo semplice l'implementazione della modalità broadcast di comunicazione tra i nodi della rete. Il vantaggio di questa topologia è legata alla facile implementazione. Non è invece garantita la robustezza della rete in caso di guasto: se il bus si rompe, tutta la rete non funziona più. Risulta inoltre difficile aggiungere nuovi nodi alla rete, dato che l'attenuazione del segnale nel bus è direttamente proporzionale alla sua lunghezza e al numero dei nodi connessi. La topologia bus è mostrata in figura 1.5.

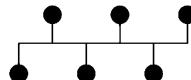


Figura 1.5: Topologia bus

1.3.4 Topologia ad anello (Ring)

In questa topologia ogni dispositivo della rete possiede due connessioni punto-punto con i dispositivi adiacenti. È una topologia attiva: il messaggio viene trasmesso da uno nodo al successivo seguendo un senso di ordinamento orario fino ad arrivare di nuovo al nodo sorgente che lo elimina dalla rete. Ciascuno dei nodi concorre al corretto trasferimento dell'informazione svolgendo il doppio ruolo di ricevitore/ripetitore. La rigenerazione dei segnali nei nodi di passaggio permette alle reti ad anello di coprire distanze maggiori di quelle consentite da altre topologie di rete. Le reti ad anello sono abbastanza semplici da installare e configurare: aggiungere o eliminare un dispositivo richiede la modifica di due soli collegamenti. Il limite è ancora una volta rappresentato dal numero dei dispositivi connessi e dalla lunghezza dell'anello. La modalità cooperativa adottata per il trasferimento dell'informazione nella rete può rendere la rete inutilizzabile nel caso di guasto di un nodo, tuttavia esistono semplici metodologie che consentono sia di individuare il nodo guasto sia di riconfigurare la rete in maniera che ne venga garantita la continuità di esercizio. In alcuni casi per aumentare la resilienza nei confronti di guasti accidentali si ricorre ad una topologia a doppio anello dove uno dei due anelli è di solito inattivo e viene utilizzato solo quando si manifestano guasti nell'altro.

La topologia ring è mostrata in figura 1.6.

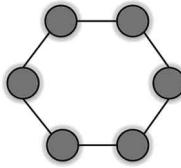


Figura 1.6: Topologia ring

1.4 Tecniche di commutazione

Una rete è un insieme di vari dispositivi (terminali) con possibilità di connessione reciproca, tipicamente a richiesta e non in maniera permanente. Questa funzionalità viene implementata mediante una particolare operazione detta commutazione (switching) da elementi interni alla rete (nodi). Mediante operazioni di switching in nodi diversi della rete, opportunamente definite e coordinate, è possibile definire, su base temporale limitata, un percorso interno alla rete che mette in comunicazione due o più terminali che ne hanno necessità. Le modalità secondo le quali la rete realizza il trasferimento dei flussi informativi dalle sorgenti alle loro destinazioni finali sono le seguenti:

- commutazione di circuito (CC);
- commutazione di messaggio (CM);
- commutazione di pacchetto (CP).

Le reti a commutazione di circuito e di pacchetto sono attualmente le reti a più larga diffusione ed uso.

1.4.1 Tecnica a commutazione di circuito

In una rete a commutazione di circuito il percorso fisico del flusso informativo viene determinato prima del trasferimento dati ed è utilizzato esclusivamente dai due utenti (sorgente, destinazione) per tutta la durata del trasferimento dati. Questa metodologia si articola nelle tre fasi seguenti da eseguire in sequenza:

- **set-up:** viene costruito all'interno della rete un cammino che individua in maniera univoca un percorso ottimo (es.: minore ritardo di trasferimento dell'informazione) che collega il nodo S (sorgente) e il nodo D (destinazione);
- **utilizzo (usage)** del collegamento: una volta stabilito, il cammino è esclusivo tra S e D, non può essere cioè utilizzato da altri dispositivi connessi alla rete. Si ha quindi un'allocazione permanente ed esclusiva del cammino per tutto il periodo di attività;
- **abbattimento (reset)** del collegamento: una volta terminata la trasmissione tra S e D, il collegamento viene abbattuto per rendere disponibili tutte le risorse di rete impegnate per altri collegamenti.

La tecnica a commutazione di circuito rende quindi disponibile, una volta instaurato, un collegamento fisico tra una sorgente ed una destinazione senza ritardi di accesso. Il grosso svantaggio della commutazione a circuito è che, nella sua versione classica, non è prevista nessuna forma di memorizzazione e elaborazione dei dati nei nodi intermedi della rete. Questo comporta la necessità di una compatibilità fisica completa lungo tutto il cammino (es.: non potranno coesistere tratti in cavo coassiale e fibra ottica). Questa tecnica è molto vantaggiosa usarla quando si necessita di connessioni veloci (es.: comunicazioni di emergenza) e quando il tempo di utilizzo è molto maggiore rispetto al tempo di set-up e di reset della linea stessa. La commutazione di circuito è tipica della rete telefonica: il sistema telefonico stabilisce tra chiamante e chiamato un circuito che essi utilizzano in modo esclusivo per tutta la durata del colloquio. Il diagramma di temporizzazione degli eventi per la commutazione di circuito è mostrato in figura 1.7.

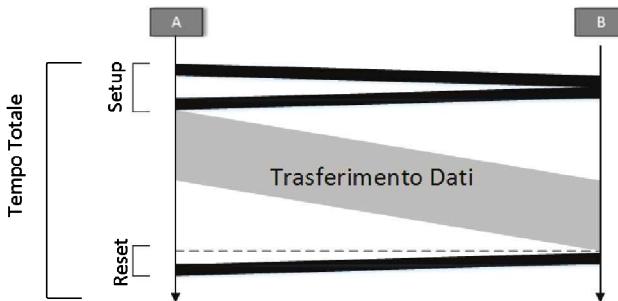


Figura 1.7: Diagramma di temporizzazione degli eventi per la commutazione di circuito.

1.4.2 Tecnica a commutazione di messaggio

In una rete a commutazione di messaggio gli utenti comunicano scambiandosi messaggi. Il messaggio è costituito da un insieme aleatorio di byte che nel loro complesso ne definiscono la lunghezza. Indipendentemente poi dalla sua lunghezza (in byte), il messaggio viene trasferito in blocco, ovvero non viene in alcun modo frammentato. Nell'intestazione di ogni messaggio vi è l'identificativo (generalmente in formato indirizzo) del destinatario. Ogni nodo della rete, in base alla conoscenza della destinazione finale del messaggio, individua tra i propri vicini il nodo più adatto per il trasferimento successivo. I link tra nodi adiacenti sono impegnati solo per il tempo di trasmissione del messaggio e mai su base permanente o in forma esclusiva.

Con questa tecnica la costruzione del cammino tra sorgente e destinatario, viene eseguita a passi successivi, in maniera indipendente da nodo a nodo ma comunque sempre coerente con un adeguato criterio di ottimizzazione. Ogni volta che un nodo riceve un messaggio, esegue due operazioni:

- memorizzazione (store);
- inoltro (forward).

Per questo motivo i nodi di una rete sono detti *store-and-forward*. Una volta ricevuto un messaggio il nodo, se previsto dal tipo di servizio, ne controlla l'integrità prima di accettarlo e memorizzarlo nel proprio buffer in attesa della successiva elaborazione (scelta del nodo di inoltro e successiva trasmissione nel canale di collegamento). La presenza del buffer consente al nodo di accettare messaggi anche se non può elaborarli immediatamente e quindi di limitare la probabilità di rifiuto degli stessi. Inoltre è possibile far coesistere nell'ambito di uno stesso collegamento end-to-end tecnologie trasmissive differenti (es.: elettromagnetiche, ottiche). Il diagramma di temporizzazione degli eventi relativo a questa tecnica è mostrato in figura 1.8.

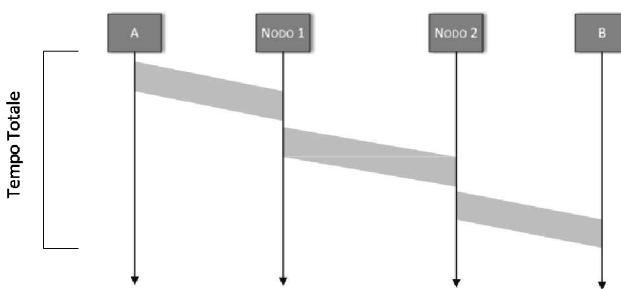


Figura 1.8: Diagramma di temporizzazione degli eventi per la commutazione di messaggio.

1.4.3 Tecnica a commutazione di pacchetto

In una rete a commutazione di pacchetto i dati da inviare sono organizzati in pacchetti formati da un numero massimo (lunghezza) di byte. Questo evita che la rete sia monopolizzata da pochi utenti e si presta, quindi, ad impieghi in reti dove il traffico è marcatamente interattivo. I pacchetti vengono inoltrati nella rete appena sono resi disponibili alla sorgente ed ognuno di essi viene gestito come un'unità indivisibile (non può essere frammentato).

Diversamente dalla commutazione di circuito, in questo caso le risorse di rete non vengono mai destinate esclusivamente ad una connessione ma sono, con modalità spesso diverse, condivise con altri collegamenti. Come nella commutazione di messaggio i nodi hanno la disponibilità di buffer che permettono di accettare pacchetti anche quando il nodo non li può processare immediatamente. Anche in questo caso possono coesistere tecnologie di trasmissione differenti (elettromagnetica, ottica) nell'ambito di uno stesso collegamento. La possibilità di operare su entità più compatte rispetto alla commutazione di messaggio rende poi le singole trasmissioni tra nodi adiacenti maggiormente immuni da errori.

Nell'ambito della commutazione di pacchetto (packet switching) sono state proposte due tecniche alternative: la tecnica a circuito virtuale e la tecnica a datagramma.

Tecnica a circuito virtuale

La tecnica di commutazione di pacchetto a circuito virtuale è una tecnica dove al trasferimento del flusso di pacchetti deve precedere una fase iniziale di set-up concettualmente analoga a quella della tecnica a commutazione di circuito, anche se, tipicamente, di durata inferiore. Una volta individuato il percorso sorgente-destinazione tutti i pacchetti di uno stesso flusso lo dovranno seguire. Questa tecnica si adatta quindi perfettamente ad impieghi dove è richiesto di preservare l'ordinamento di generazione dei pacchetti nell'ambito di uno stesso flusso (servizi connection oriented, vedi capitolo 4). Lo svantaggio maggiore della tecnica a circuito virtuale è legato a brusche ed impreviste variazioni dello stato della rete che determinano la necessità di ripetere la fase di set-up. Il diagramma di temporizzazione degli eventi è mostrato in figura 1.9.

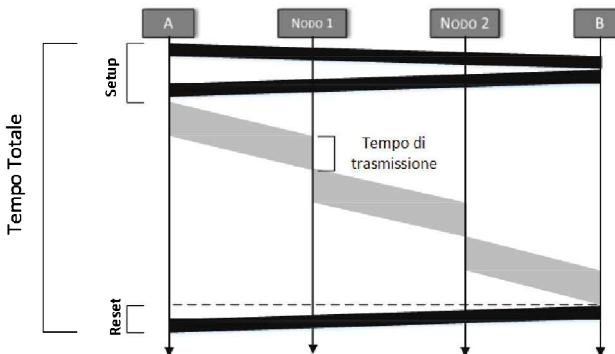


Figura 1.9: Diagramma di temporizzazione degli eventi per la commutazione a pacchetto (circuito virtuale).

Tecnica a datagramma

La tecnica a commutazione di pacchetto a datagramma è una tecnica in cui viene meno la necessità di individuare preventivamente un percorso fisico e di mantenere questa scelta fissa per l'intera durata del collegamento. Ogni nodo, in maniera autonoma ed indipendente da pacchetto a pacchetto, individua, in accordo ad un opportuno criterio, tra i suoi vicini il nodo a cui inoltrare il pacchetto. Questa metodologia comporta che nel pacchetto siano inserite delle informazioni di supporto (es.: indirizzo del destinatario, indirizzo del mittente e numero d'ordine di generazione del pacchetto). Il poter eseguire la decisione riguardo l'inoltro successivo pacchetto per pacchetto consente una forte flessibilità di uso permettendo, in particolare, di reagire prontamente a qualsiasi anomalia la rete.

possa manifestare. La conseguenza naturale della modalità a datagramma è che i pacchetti appartenenti ad uno stesso flusso possono arrivare alla destinazione finale con un ordine diverso rispetto a quello di generazione. Questo comportamento è congruente con servizi connectionless ma non con servizi connection oriented. Se quindi si vuole rendere compatibile la modalità a datagramma con servizi connection oriented occorre demandare al nodo di destinazione il compito di ripristinare il corretto ordine di generazione del flusso prima della sua utilizzazione.

Il diagramma di temporizzazione degli eventi relativo alla modalità a datagramma è mostrato in figura 1.10.

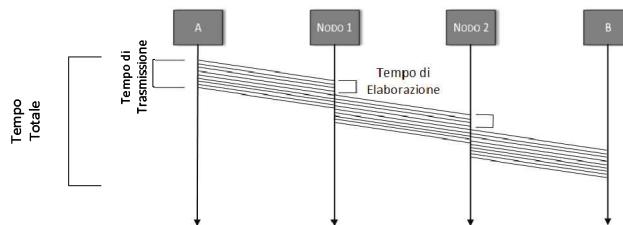


Figura 1.10: Diagramma di temporizzazione degli eventi per la commutazione a pacchetto (datagramma).

1.4.4 Confronto tra le varie tecniche

In figura 1.11 è mostrato un diagramma logico che racchiude le tre tecniche di commutazione.



Figura 1.11: Tecniche di commutazione

Come detto in precedenza, la commutazione di circuito è una tecnica che prima di trasmettere un flusso informativo deve definire preventivamente un cammino interno alla rete destinando in maniera esclusiva a questo scopo risorse di rete (nodi, collegamenti). Questa modalità si adatta alle esigenze di servizi critici con necessità di una disponibilità garantita di accesso ma, in genere, si presenta come poco conveniente dal punto di vista di utilizzazione delle risorse di

rete per le note caratteristiche del traffico dati (vedi capitolo 4). Dall'altra parte, si ha che la tecnica a commutazione di pacchetto consente decisamente un migliore utilizzo delle risorse di rete (linee) ma, a causa dei ritardi non predicibili di accodamento nei nodi di transito, non può garantire un ritardo fisso per la consegna dei pacchetti al destinatario e quindi risulta poco adatto a servizi in tempo reale come video o voce. Infine è importante notare che la commutazione di pacchetto presenta in generale una maggiore flessibilità di utilizzo ed una implementazione più semplice, più efficiente e meno costosa rispetto alle altre tecniche alternative (vedi Kurose'2013 in 1.5).

1.5 Letture Consigliate

Per approfondire le tematiche di base delle reti di telecomunicazioni e le loro più recenti applicazioni si consigliano i seguenti testi:

- M. Schwartz, Broadband Integrated Networks, Prentice Hall, 1996.
- F. Halsall, Reti di Calcolatori e Sistemi Aperti, Addison-Wesley, 1996.
- D. Wright, Broadband: Business Services, Technologies, and Strategic Impact, Artech House, 1993.
- A. Acampora, An Introduction to Broadband Networks, Plenum Press, 1994.
- W. Stalling, High Speed Networks, Prentice Hall, 1998.
- B.A. Forouzan, Reti di Calcolatori ed Internet, McGraw-Hill, 2007.
- A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.
- J.F. Kurose, K. W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.

Si consiglia inoltre di consultare i seguenti siti Web:

ieeexplore.ieee.org

<https://www.wikipedia.org>

2

La rete telefonica

La rete telefonica è stata introdotta, in una versione compiuta, alla fine del XIX° secolo, per fornire un servizio di comunicazione vocale ai propri utenti. Con l'avvento delle reti di calcolatori, all'inizio degli anni '80 del secolo scorso, la rete tradizionale ha subito notevoli cambiamenti conseguenti al suo nuovo utilizzo per collegamenti dati. Nell'ultimo decennio la rete telefonica ha migrato da una tecnologia di trasmissione analogica ad una tecnologia di trasmissione numerica. Dal punto di vista normativo, la rete telefonica è regolata dagli standard emanati dal ITU-T (International Telecommunication Union – Telecommunication Standardization Bureau).

Le reti telefoniche attuali si suddividono in:

- *reti pubbliche*: sono reti il cui utilizzo è offerto a chiunque sia interessato. L'utilizzo della rete telefonica pubblica normalmente è a pagamento e può avvenire attraverso o una singola utenza telefonica privata oppure una utenza pubblica;
- *reti private* : sono reti il cui utilizzo è riservato solo ad utenti autorizzati. Di solito riguardano applicazioni professionali di interesse per Pubblica Sicurezza, Istituti Finanziari, Gruppi Industriali, Enti Pubblici in generale.

Argomento di questo capitolo sono le reti telefoniche pubbliche.

La rete telefonica pubblica usa la commutazione di circuito e comunemente viene chiamata Public Switched Telephone Network (PSTN). E' un sistema complesso organizzato secondo un'architettura a piani gerarchici come illustrato nella figura 2.1 con riferimento alla rete telefonica pubblica italiana.

Dalla figura si può notare come gli elementi appartenenti ai due piani gerarchici più elevati (centrali nazionali, centrali di compartimento) siano collegati a maglia (ovvero formano una rete mesh 1.3.1). Questa soluzione è stata adottata per garantire una elevata affidabilità di esercizio della rete in quanto guasti occidentali (es.: interruzione di un collegamento) localizzati in questi due piani gerarchici pregiudicherebbero il corretto funzionamento di gran parte della rete. Il collegamento a maglia può essere esteso anche a collegamenti tra centrali di distretto in situazioni specifiche (es: alta concentrazione di utenti/traffico). In generale comunque, a partire dal piano delle centrali di compartimento, i collegamenti tra gli elementi del piano superiore, con quelli appartenenti al piano immediatamente inferiore, è realizzato a stella.

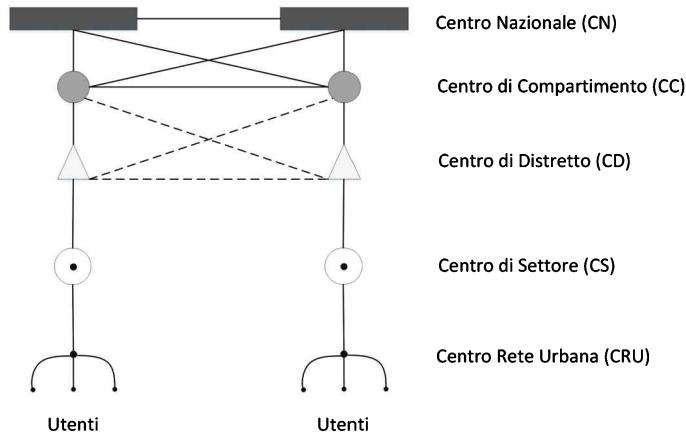


Figura 2.1: Struttura della rete telefonica

2.1 Telefonia

La telefonia è la metodologia di comunicazione adottata in una rete telefonica per consentire la trasmissione a distanza in tempo reale di segnali fonici tra due o più utenti. In relazione al formato dei segnali vocali trasmessi essa si suddivide in:

- Telefonia analogica;
- Telefonia numerica.

2.1.1 Telefonia analogica

Ad un canale telefonico analogico viene associata la banda nominale di 4 KHz nell'intervallo $[0 \div 4]\text{ KHz}$. In relazione alla fisiologia dell'apparato uditivo dell'uomo, si considera come banda utile (entro la quale il segnale non deve essere alterato per non pregiudicarne l'intereleggibilità) una banda di $3,1\text{ KHz}$ nell'intervallo $[300 \div 3400]\text{ Hz}$. Il processo di modulazione analogica consente di traslare la banda utile del segnale in un intervallo di frequenze più conveniente in relazione ad un particolare mezzo fisico (cioè si cerca di individuare la porzione di frequenza entro la quale il mezzo fisico è meno ostile al passaggio del segnale). I segnali analogici hanno necessità di essere ricostruiti fedelmente in ricezione affinché siano interpretabili correttamente. Questo vincolo li rende quindi particolarmente sensibili ai disturbi e alle distorsioni introdotte dal canale di comunicazione e dal sistema di ricezione.

2.1.2 Telefonia numerica

L'avvento dell'era digitale la si deve principalmente all'intuizione di C.E. Shannon che con il *Teorema del Campionamento*, (si veda Schwartz'1986, Fou�ozan'2007, Proakis'1994 in 2.3), dimostrò come fosse possibile conoscere esattamente un segnale analogico, di banda limitata, unicamente partendo dalla conoscenza dei valori assunti in corrispondenza di istanti di tempo specifici (istanti di campionamento).

In particolare, con campionamento di un segnale continuo nel tempo $s(t)$ a banda limitata, si intende l'operazione mediante la quale si definiscono i valori che il segnale originario assume in corrispondenza di istanti temporali presi con passo T_s (periodo di campionamento). Affinché da questo insieme discreto di valori sia possibile ricostruire il segnale continuo originale occorre che il passo di campionamento risulti maggiore, o uguale, a due volte l'occupazione di banda unilaterale B del segnale (solo frequenze positive):

$$f_s \geq 2B$$

Il valore minimo della frequenza di campionamento necessaria affinché sia possibile ricostruire esattamente il segnale originario, è uguale al doppio della banda del segnale stesso ($f_s = 2B$), e prende il nome di frequenza di Nyquist. Analogamente, per il passo (periodo) di campionamento T_s , si ha:

$$T_s \leq \frac{1}{2B}$$

Si deve notare che i campioni del segnale continuo ottenuti con la procedura del suo campionamento sono grandezze continue. Mediante l'operazione di quantizzazione si trasformano i valori continui dei campioni in valori interi confrontandone l'ampiezza con una unità di riferimento (il numero intero indica quante volte l'unità di riferimento è contenuta nell'ampiezza del campione). Inevitabilmente, in questo modo, si introduce un errore di rappresentazione che è detto errore di quantizzazione. Il passo finale per chiudere tutto il processo consiste nel rappresentare il valore intero quantizzato di ogni singolo campione in forma binaria. La lunghezza della stringa di bit associata ad ogni campione definisce l'accuratezza dell'operazione nel suo complesso (maggiore è il numero di bit minore sarà l'errore di quantizzazione).

Nel caso di un segnale fonico, lo standard della telefonia numerica prevede, per ogni campione, una rappresentazione mediante sequenze binarie lunghe 8 bit. Considerando un valore di B convenzionale uguale a 4 KHz , secondo il Teorema del Campionamento, si ha che il passo di campionamento massimo è:

$$T_s = \frac{1}{2 \cdot 4 \cdot 10^3} = 125 \quad \mu s$$

Nel tempo che separa l'acquisizione del campione del segnale fonico dal successivo si deve essere in grado di trasmettere per intero il gruppo di 8 bit ad esso associato. Questo comporta che il tempo di trasmissione del singolo bit dovrà essere ($\tau = \frac{T_s}{8}$) e quindi la banda minima necessaria per la trasmissione senza

distorsione di un segnale fonico, in forma numerica, quantizzato a 8 bit risulta essere pari a:

$$B = \frac{1}{\tau} = 64 \text{ KHz}$$

A cui corrisponde un bit rate convenzionale (velocità di trasmissione dei singoli bit) pari a:

$$R = \frac{8}{T_s} = 64 \text{ Kbit/s}$$

La modalità di trasmissione di un segnale fonico in formato numerico è nota come tecnica PCM (Pulse Code Modulation). Inizialmente la telefonia numerico, soprattutto a causa del suo elevato costo, fu impiegata limitatamente a collegamenti a lunga distanza dove i disturbi presenti rappresentavano l'ostacolo maggiore al suo trasferimento affidabile. La decisione su di un segnale numerico tipicamente comporta solo decidere quale tra due forme d'onda di riferito è stata ricevuta e non necessita, a differenza di decisioni su segnali analogici, di una ricostruzione esatta della stessa. In questo modo, ipotizzando decisioni corrette, per comunicazioni multi tratta (a lunga distanza), si riusciva a disaccoppiare gli effetti dei disturbi facendo in modo che la ricezione finale, indipendentemente dal numero di tratte previste, fosse solo dipendente dalla qualità della trasmissione nell'ultima tratta.

A fronte di una indubbia penalizzazione per quanto riguarda la richiesta minima di banda per un singolo collegamento (si passa dai 4 KHz del caso analogico ai 64 KHz del caso numerico), oltre alla migliore immunità ai disturbi di canale di particolare interesse per comunicazioni a lunga distanza, la telefonia numerica consente di avere:

- costi realizzativi contenuti;
- migliore capacità di impiego di tecniche di protezione dell'informazione nei confronti di errori di trasmissione;
- livello di sicurezza (riservatezza) maggiore;
- maggiore flessibilità di utilizzo: segnali informativi differenti (Voce, Video, multimediali) possono essere gestiti nello stesso modo;
- maggiore flessibilità di gestione: i segnali di controllo sono trattati dalla rete nello stesso modo dei segnali informativi.

Sulla base di questi vantaggi e tenendo conto che la richiesta di banda nominale maggiore di 64 KHz può essere attenuata mediante l'impiego di opportune tecniche di modulazione numerica, si può giustificare a pieno il successo e l'affermarsi della telefonia numerica a scapito della telefonia analogica.

2.2 Tecniche di multiplexing

Il multiplexing (si veda Schwartz'1986, Fou�an'2007 in 2.3) è una tecnica che permette la condivisione di uno stesso canale fisico tra più segnali (utenti) distinti. In generale, quando le esigenze di trasmissione aumentano è più conveniente

disporre di un mezzo fisico capace di trasportare più segnali anziché aumentare il numero di linee. Le principali metodologie di multiplexing sono legate alla natura dei segnali da trasmettere, si parla quindi di multiplazione a divisione di frequenza quando i segnali da trasmettere sono in genere segnali analogici, multiplazioni a divisione di tempo quando i segnali da trasmettere sono in formato numerico (bit) oppure, infine, di multiplazione a divisione di lunghezza d'onda, o a diffusione, quando i segnali sono in formato ottico.

2.2.1 Multiplexing a divisione di frequenza

La tecnica multiplexing a divisione di frequenza, (si veda Schwartz'1986, Fouoran'2007 in 2.3), (FDM) è una tecnica di condivisione di un canale di trasmissione tra più sorgenti di informazione (utenti), che prevede la suddivisione della banda di frequenza disponibile (canale di trasmissione) in un pari numero di sottobande (sottocanali). Ogni sottocanale è assegnato in maniera esclusiva ad uno solo utente (collegamento). Un esempio rappresentativo di sistema FDM lo si ha nelle trasmissioni radiofoniche dove la banda totale per il servizio è suddivisa in sottocanali tra loro opportunamente distanziati dove le singole stazioni irridiano i propri programmi.

L'operazione di multiplexing FDM consiste nel fare in modo, attraverso il processo di modulazione, che il segnale proprio di un utente, si vada a posizionare nella banda di frequenza assegnata. In ricezione, un'opportuna sequenza di filtri passabanda, permetterà di selezionare il segnale d'interesse dal gruppo FDM che, successivamente processato (demodulazione), verrà reso fruibile al suo destinatario finale.

Il sistema FDM è rappresentato in figura 2.2 considerando un numero N di utenti.

La tecnica FDM prevede la presenza contemporanea di tutti i segnali di utente nella banda assegnata. Questo comporta una maggiore vulnerabilità nei confronti di interferenze tra segnali diversi e la necessità (evidenziata anche in precedenza) di assegnare ad ogni utente un intervallo di frequenza maggiore del minimo indispensabile, prevedendo in testa ed in coda alle bande di frequenza utili, degli intervalli detti di guardia, per evitare interferenze tra trasmissioni su sottocanali contigui.

Nella struttura gerarchica di figura 2.1, si ha che ogni elemento di un certo piano provvede ad aggregare in un unico flusso tutti i flussi generati da elementi appartenenti al piano gerarchico immediatamente inferiore con cui è connesso. Il flusso aggregato viene poi trasferito all'elemento del piano gerarchico superiore con cui, l'elemento considerato è, a sua volta, connesso. Le modalità secondo la quale i canali fonici di banda 4 KHz sono aggregati tra di loro sono standardizzate nell'ambito prima del CCITT poi del ITU-T. Il gruppo base comprende 12 canali (gruppo), si hanno poi i super gruppi formati da 60 canali ed i gruppi master formati da 300 canali fonici di base. Il gruppo di dimensioni maggiori (10800 canali), previsto dallo standard, è di regola riservato a collegamenti a grande capacità (es. collegamento tra centrali nazionali).

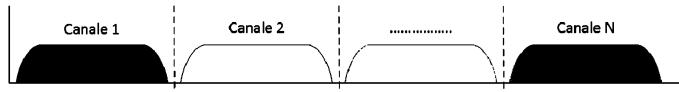


Figura 2.2: Multiplazione FDM

2.2.2 Multiplexing a divisione di tempo

La multiplazione a divisione di tempo (TDM), è una tecnica di condivisione del canale di comunicazione, (si veda Schwartz'1986, Fourozan'2007, Proakis'1994, Hykin'2010 in 2.3) secondo la quale ogni utente ottiene a turno, per un tempo prefissato, l'uso esclusivo dello stesso. L'accesso al canale da parte di tutti gli utenti viene completato in un tempo detto *tempo di trama* (frame). Ogni frame è, a sua volta, suddiviso in sottointervalli uguali detti *slot*. Ogni slot è assegnato in maniera esclusiva ad un solo utente. Conseguente alla presenza individuale ed alternata delle comunicazioni nel canale, il sistema TDM non necessita di bande di guardia per separare collegamenti contigui e limitare le interferenze. Tuttavia, la necessità di sincronizzazione tra i vari utenti necessita di tempi di guardia tra slot contigui che rendono il tempo effettivo di accesso al canale minore di quello nominale (tempo di slot).

Il sistema TDM è rappresentato in figura 2.3.

Come nel caso della tecnica FDM le regole con cui si aggregano i flussi numerici sono definite a livello di standard internazionale ITU-T. In questo caso per identificare la modalità di aggregazione dei flussi base PCM si parla di gerarchia PDH (Plesiochronous Digital Hierarchy). A livello mondiale non esiste però uniformità: il sistema nord-americano differisce ad esempio da quello europeo. Nel sistema europeo il raggruppamento di primo livello prevede 32 canali PCM di cui 30 dedicati al trasporto dell'informazione e 2 dedicati alla segnalazione di supporto. Complessivamente il bit-rate aggregato è di 2,048 Mbit/s e la struttura viene indicata con la sigla E1. In Nord-America l'equivalente struttura di primo livello, denominata T1, è formata da 24 canali dedicati al trasporto dell'informazione ed un bit per trama per la segnalazione. In questo caso il bit-rate aggregato è pari a 1,544 MBit/s. Sono previsti nel sistema europeo quattro successivi livelli di aggregazione ciascuno dei quali è ottenuto dalla multiplazione di 4 flussi indipendenti del livello immediatamente precedente (es.: 4 flussi primari E1 aggregati tra loro formano un flusso di secondo livello E2).

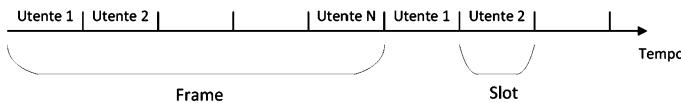


Figura 2.3: Multiplazione TDM

2.2.3 Multiplexing a divisione di lunghezza d'onda

Il multiplexing a divisione di lunghezza d'onda (WDM) è una tecnologia utilizzata per sfruttare di più la capacità di trasporto delle fibre ottiche (Fourozan'2007 in 2.3). Questa tecnica è concettualmente simile al metodo FDM con ovviamente la differenza che in questo caso si aggregano fasci di luce con lunghezza d'onda differente nell'ambito di una stessa fibra ottica. Si arriva a raggiungere valori di banda aggregata dell'ordine dei Teraherz (10^{12} Hz). Così come nei sistemi FDM trasmissioni in bande adiacenti possono disturbarsi a vicenda, nei sistemi WDM trasmissioni di flussi informativi su lunghezze d'onda contigue possono interferire tra di loro (crosstalk). Più larga è la spaziatura tra le lunghezze d'onda utilizzate migliore è l'immunità dai disturbi di crosstalk. Di conseguenza diventa meno critica e complessa l'operazione di multiplexing/demultiplexing, permettendo quindi di utilizzare dispositivi ottici meno costosi. L'evoluzione tecnologica nel campo dei multipliatori a divisione di lunghezza d'onda ha recentemente portato alla definizione di Dense WDM (DWDM) dove la spaziature tra le lunghezze d'onda è ridotta rispetto ai sistemi tradizionali WDM. In genere un sistema DWDM convenzionale prevede fino a 40 canali nella terza finestra di trasmissione (la banda C) delle fibre in silicio, intorno alla lunghezza d'onda di 1550 nm, con una separazione tra i canali di 100 GHz. Diminuendo la spaziatura tra lunghezze d'onda è oggi possibile usare la stessa finestra di trasmissione arrivando a 80/96 canali a intervalli di 50 GHz o addirittura fino a 160 canali e intervalli di 25 GHz (in questo caso si parla di WDM ultra densi).

2.2.4 Servizio dati in rete telefonica: tecnologie xDSL

Le linee telefoniche tradizionali possono essere utilizzate per la trasmissione di dati, (si veda Fourozan'2007, Stalling'2000, Tanembaum'2011 in 2.3), verso le postazioni utente inviando dati su un collegamento telefonico tradizionale (*dial-up*). Inizialmente questa possibilità è stata sfruttata grazie ad apparati di trasmissione/ricezione denominati *modem*. Le velocità di accesso alla rete, seppure significative per le applicazioni iniziali, rapidamente divennero insoddisfacenti. Per poter rispondere quindi a richieste di velocità di accesso più elevate, i gestori del servizio di connessione (NSP) svilupparono una nuova tecnologia, denominata *DSL* (Digital Subscriber Line), per meglio sfruttare le capacità di trasporto delle linee in doppino di rame (la banda utile è di circa 1,1 MHz contro i 4 KHz nominali per comunicazioni foniche). Ad oggi la tecnologia *DSL* prevede quattro diverse varianti: *ADSL*, *VDSL*, *HDSL* e *SDSL* che complessivamente vengono indicate come tecnologie *xDSL*.

DSL asimmetrico

La tecnologia *ADSL* si basa su l'uso di una linea DSL in modalità asimmetrica cioè fornisce servizi di connessione a diversa capacità di trasferimento dati nelle due direzioni del collegamento: si assegna una velocità maggiore per il trasferimento dati dalla rete Internet alla postazione di utente *download*. La caratteristica funzionale dei dispositivi di accesso *ADSL* è una sorta di capacità cognitiva

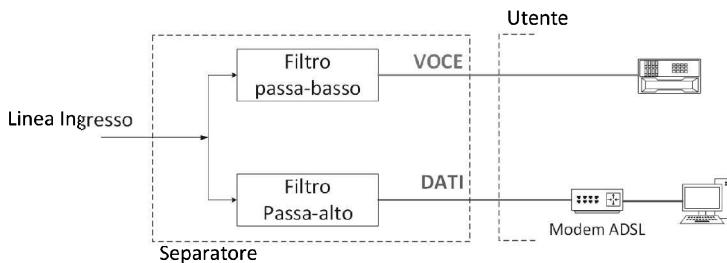


Figura 2.4: ADSL lato utente

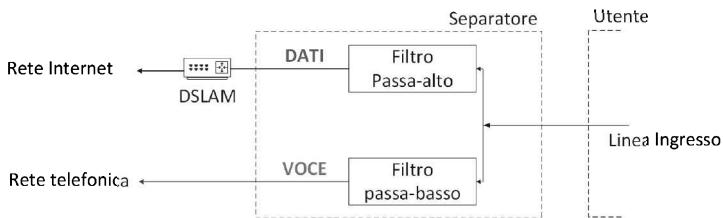


Figura 2.5: ADSL lato centrale

che li consente di interpretare il contesto in cui operano (condizione del collegamento) e di conseguenza adattare la tecnica di trasmissione dei dati ad esso per ottenerne una migliore utilizzazione. Conseguenza di questo è che la trasmissione *ADSL* non ha un rate fisso in quanto cambia in relazione alle condizioni del collegamento. La tecnologia trasmissiva utilizzata per permettere una efficace adattività al contesto (si veda Fourozan'2007 in 2.3), viene indicata come tecnica *DMT* (Discrete Multitone Technique).

La figura 2.4 illustra una tipica installazione *ADSL* alla postazione utente. La componente fondamentale di tale sistema è un dispositivo chiamato separatore (*splitter*), composto da due filtri, passa-basso e passa-alto, in maniera da separare in ingresso le comunicazioni vocali da quelle dati.

In figura 2.5 è mostrato invece come una connessione *ADSL* viene gestita dal NSP (centrale). In questo caso la situazione operativa è differente. Anche in questo caso è presente lo splitter che serve per separare il segnale vocale da quello dati. Il segnale vocale è filtrato e inviato verso la rete telefonica tradizionale. Il segnale dati, invece, viene inoltrato verso un dispositivo denominato *DSLAM* che implementa sia le stesse funzionalità di un modem *ADSL* (trasmissione in modalità *DSL* su doppino in rame verso l'utente finale) sia la funzionalità di multiplavazione, aggregando in un unico flusso più flussi provenienti dai singoli utenti ed inoltrandoli in forma di pacchetti su una linea di collegamento di maggiore capacità verso la rete dati.

DSL simmetrico

La tecnologia DSL simmetrico,(si veda Fourozan'2007 in 2.3), prevede di allocare bande uguali (quindi stesse velocità di trasmissione) per un collegamento dati bilanciato upstream (dall'utente ad internet) e downstream. Queste tecniche sono:

- *HDSL* (High-bit-rate Digital Subscriber Line) : Diversamente da *ADSL*, prevede un doppino in rame dedicato per ogni utente, consentendo quindi di avere una connessione sempre disponibile. Ha costi di accesso, dovuti alle apparecchiature modem da utilizzare, superiori ad *ADSL*. Deve utilizzare delle tecniche in grado di eliminare il fenomeno dell'eco. Per superare distanze maggiori di 1 Km occorre utilizzare dei ripetitori che aumentano ancora di più il costo del sistema;
- *SDSL* (Symmetric Digital Subscribe Line) : Questa tecnologia consente di disporre di un collegamento bidirezionale veloce con uguale capacità di trasmissione dati (upload e download).

Infine, come caso particolare, possiamo citare la tecnologia *VDSL* (Very high-bit-rate Digital Subcriber Line) la quale si trova disponibile sia nella versione simmetrica che asimmetrica. Solitamente vengono utilizzati mezzi di buona qualità come fibre ottiche e cavi coassiali, tuttavia, quando le distanza da coprire sono limitate a qualche centinaia di metri, si possono utilizzare anche i doppini in rame. Ovviamente, l'impiego del doppino per supportare velocità di accesso elevate (da 25 a 55 Mbps in download) richiede l'uso di tecniche di trasmissione specifiche e complesse.

2.3 Letture Consigliate

Per approfondimenti inerenti gli argomenti trattati in questo capitolo si suggerisco i seguenti testi:

M. Schwartz, Telecommunication Networks, Addison Wesley, 1986.

W. Stalling, Trasmissione Dati e Reti di Computer, Jackson, 2000.

J.G. Proakis, M. Salehi, Communication Systems Enginering, Prentice Hall, 1994.

S. Haykin, M. Moher, Communication Systems, John Wiley, 2010.

B.A. Forouzan, Reti di calcolatori ed Internet, McGraw-Hill, 2007.

A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.

3

I commutatori

Il commutatore in una rete di telecomunicazioni è una struttura fisica preposta alla funzione di commutazione (inoltro). È una struttura *intelligente* in quanto deve decidere a quale delle sue uscite collegare un certo ingresso in relazione all'interpretazione della richiesta di connessione ed, in questo modo, concorre insieme ad altre strutture simili a rendere disponibile i collegamenti tra gli utenti, o dispositivi, della rete. Il commutatore deve essere in grado di costruire, mantenere e abbattere specifici collegamenti tra i suoi ingressi e le sue uscite. La rete di connessione è la parte funzionale del commutatore che consente di attuare i collegamenti richiesti ingresso/uscita. La trattazione dei commutatori fatta in questo capitolo si concentrerà sulla descrizione, l'analisi e il progetto di diverse alternative realizzative possibili per le reti di connessione in relazione a modalità a commutazione di circuito (rete telefonica) e a commutazione di pacchetto (reti di calcolatori).

Un po' di storia

Agli inizi del diffondersi della telefonia, le poche linee attive venivano attestate in uno stesso edificio. La commutazione veniva realizzata manualmente creando, su richiesta, la connessione elettrica tra l'utente chiamante e l'utente chiamato. Il primo sistema di commutazione automatico venne sviluppato agli inizi del Novecento dall'americano A. B. Strowger il quale oggi potrebbe essere considerato come un sostenitore convinto della "privacy". Egli infatti riteneva giusto che dovesse essere possibile chiamare chiunque si volesse senza condividere questo desiderio, o necessità, con altri. In realtà, si racconta che una spinta decisa verso l'invenzione del primo commutatore automatico fosse derivata dal fatto che la moglie di un suo concorrente, che lavorava presso il centralino di smistamento delle chiamate, quando riceveva una richiesta di connessione verso l'azienda di proprietà di Strowger, la dirigesse verso l'azienda del marito causando quindi consistenti perdite di affari.

La struttura di un commutatore automatico (autocommutatore) dei nostri tempi (figura 3.1) è formata da una *rete di connessione*; da due blocchi di *terminazione* per le linee di ingresso e di uscita e da un'*unità di controllo* (vedi Schwartz'1987, Hammond'1986, Pearce'1981 in 3.5). La terminazione di rete in ingresso ha il compito di separare il flusso delle informazioni di utente dal flusso

di segnalazione (demultiplexing). Una volta separati i flussi, invia il primo alla rete di connessione e il secondo all'unità di controllo. La terminazione di uscita ha il compito di riunificare i due flussi secondo le regole di inoltro dettate dall'unità centrale (multiplexing). L'unità di controllo è la parte principale del commutatore. Essa è in pratica un sistema per l'elaborazione dell'informazione vero e proprio in grado di interpretare il flusso di segnalazione in ingresso e operare di conseguenza. La rete di connessione, comandata dall'unità di controllo, ha il compito di stabilire l'interconnessione tra le linee di ingresso e le linee di uscita in modo da commutare un flusso informativo di utente, che arriva ad una precisa linea di ingresso, su una particolare linea di uscita. Le connessioni sono realizzate attraverso appositi dispositivi che, per semplicità, chiameremo "interruttori". Le modalità realizzative di questi interruttori ha caratterizzato l'evoluzione tecnologica degli autocommutatori inizialmente di tipo elettromeccanica oggi, completamente in tecnologia elettronica. Parallelamente si è avuto un incremento delle prestazioni degli autocommutatori in termini di velocità di esecuzione dell'operazione di commutazione e di riconfigurazione in maniera da essere allineati ai sempre più stringenti requisiti della moderna telefonia numerica.

A seconda del numero di linee di ingresso e di uscita, i commutatori si possono classificare come:

- *Concentratori*. Quando il numero delle linee in ingresso, n_{IN} , è maggiore del numero delle linee in uscita, n_{OUT} ($n_{IN} > n_{OUT}$), si ha un concentratore. Questi dispositivi aggregano flussi di informazione elementari in ingresso convogliandole su linee di uscita di maggiore capacità (banda). Operano tipicamente, nella rete telefonica pubblica, nel percorso verso l'alto del piano gerarchico;
- *Espansori*. Quando il numero di linee in ingresso è minore del numero di linee di uscita ($n_{IN} < n_{OUT}$), allora si ha un espansore. Questi commutatori separano le informazioni in ingresso distribuendole su linee di uscita con minore capacità (banda) e si trovano tipicamente nella linea telefonica pubblica nel percorso verso il basso del piano gerarchico;
- *Distributori*. Quando il numero delle linee di ingresso è uguale al numero di linee in uscita ($n_{IN} = n_{OUT}$) si ha un distributore.

Le reti di connessioni possono essere divise in due categorie, a seconda della loro tecnologia realizzativa:

- reti a *divisione di spazio*, o strutture S;
- reti a *divisione di tempo*, o strutture T.

Le strutture S e T possono essere combinate tra di loro per creare strutture multi-stadio (si arriva ad avere strutture fino a cinque stadi). L'architettura delle reti di connessione utilizzate nella pratica è generalmente di tipo combinato poiché si riesce in questo modo ad aumentare la flessibilità dell'operazione di commutazione e a ridurre il costo della struttura risultante senza pregiudicarne i requisiti di servizio. Le reti di connessione multi-stadio, a loro volta, si dividono in

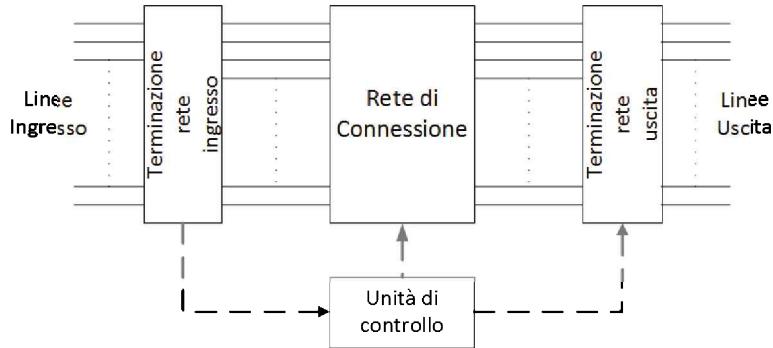


Figura 3.1: Autocommutatore

omogenee e non omogenee. Le prime sono reti di connessione formate da componenti omogenei per tecnologia realizzativa, mentre le seconde sono strutture nelle quali coesistono blocchi basati su tecnologie a divisione di spazio e tempo con l'obiettivo di sfruttare le caratteristiche funzionali di entrambe.

Il *fattore di costo* è un parametro qualitativo che indica il costo della rete di connessione ed è legato alla tecnologia con cui è realizzata la struttura. Congiuntamente al suo costo, una rete di connessione viene anche identificata come struttura bloccante o non bloccante in relazione alla sua capacità funzionale di gestire le richieste di connessione ingresso/uscita. Una rete di connessione viene definita *non bloccante* quando è sempre possibile connettere una linea di ingresso ad una qualsiasi linea di uscita libera. Di conseguenza, una struttura bloccante è una struttura in cui una linea di ingresso non può essere collegata con una linea di uscita libera. Le strutture a singolo stadio S e T sono intrinsecamente non bloccanti, mentre le strutture a due stadi S-S, S-T, T-S sono bloccanti (da notare che nel caso di strutture S-S è possibile ridurre il costo rispetto ad una equivalente struttura monostadio S). Le strutture a tre stadi S-S-S e T-S-T, opportunamente progettate, consentono invece di abbinare i requisiti funzionali propri di strutture diverse (nel caso di reti di connessione non omogenee T-S-T), di mantenere una funzionalità non bloccante e di ridurre i costi rispetto alle equivalenti strutture monostadio.

3.1 Strutture a divisione di spazio

Le strutture S si basano concettualmente su una struttura a matrice dove le righe rappresentano le linee di ingresso e le colonne rappresentano le linee di uscita. Nel punto di intersezione fra linee di ingresso e linee di uscita sono disposti degli interruttori che stabiliscono il mapping tra ingressi e uscite. Sarà poi l'unità di controllo a stabilire, sulla base delle informazioni di segnalazione, quali connessioni devono essere attivate (chiusura degli interruttori nei punti di intersezione fra linee ingresso/uscita). Questa struttura effettua solo un cambio di

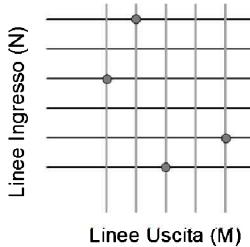


Figura 3.2: Struttura S

linea, ad esempio se l'ingresso si trova sulla linea X , potrà poi trovarsi in uscita sulla linea Y . Nel caso di telefonia digitale il cambio di linea mantiene inalterato il numero di canale nell'ambito della trama PDH in ingresso : il canale 1 della trama PDH associata alla linea X in ingresso potrà diventare il canale 1 della trama PDH relativa all'uscita Y .

Inizialmente, la chiusura automatica (senza l'interventi esterni) dei collegamenti è stata prima realizzata con tecnologia elettromeccanica (relè automatici) e, successivamente, con tecnologia completamente elettronica tramite porte logiche (realizzate con BJT), per rispondere alle nuove esigenze di servizio della telefonia numerica (elevata frequenza di riconfigurazione delle connessioni). Si deve notare che, mentre con la telefonia analogica l'utente chiamante è sempre una continuità elettrica (collegamento) con l'utente chiamato, con la telefonia numerica gli utenti, sebbene in maniera per loro non percettibile, sono fisicamente collegati tra loro per il solo tempo di canale. La struttura a divisione di spazio S è mostrata in figura 3.2.

Il fattore di costo per una struttura S è legato al numero di connessioni complessivamente possibili. Nel caso in cui le linee di ingresso sono N e le linee di uscita sono M , il fattore di costo C è pari a:

$$C = N \cdot M$$

Nel caso particolare di una matrice quadrata, ovvero numero di linee di ingresso uguale al numero di linee di uscita ($N = M$), si ottiene un costo pari a:

$$C = N^2$$

3.2 Strutture a divisione di tempo

Le strutture T sono reti di commutazione usate solo nella telefonia numerica, poiché possono effettuare solo l'operazione di permutazione di canale, cioè modificano solo la posizione di uno canale nell'ambito di una trama PDH. Ad esempio, se un utente è stato associato al canale X all'interno di una trama, in uscita lo stesso utente potrà ritrovare il proprio canale permutato in una posizione Y diversa della stessa trama. Dal punto di vista strutturale, le reti di connessione a divisione di tempo sono caratterizzate da una architettura completamente

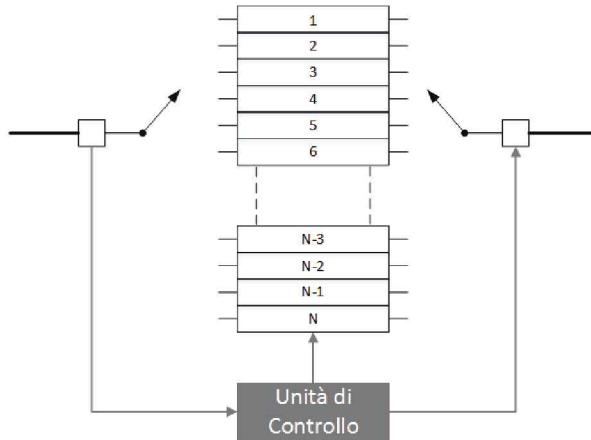


Figura 3.3: Struttura T

elettronica. In pratica sono memorie che mediante le operazioni di lettura e scrittura svolgono l'operazione di permutazione di canale, quando richiesta. La memoria dovrà avere un numero di celle pari al numero massimo di canali in ingresso/uscita con capacità di ogni cella pari 8 bit (byte di fonia). La struttura T è mostrata in figura 3.3.

La permutazione viene implementata gestendo opportunamente le operazioni di memorizzazione della trama in ingresso nella memoria e della sua rilettura (ripetizione) per formare la trama di uscita. Esistono due modalità base per realizzare la permutazione di canale:

- **scrittura sequenziale e lettura casuale:** i byte di fonia (uno per ogni canale in ingresso) vengono trasferiti nelle celle di memoria rispettando l'ordinamento di arrivo (es.: il byte di fonia relativo al canale di ingresso X verrà trasferito nella cella della memoria di posizione X). L'operazione di lettura (trasferimento dei byte di fonia dalla memoria ai canali della trama di uscita) non rispetta una regola fissa (casuale) : i byte di fonia verranno letti e trasferiti nei canali della trama di uscita in relazione a richieste di permutazione specifiche;
- **scrittura casuale e lettura sequenziale:** questa modalità è simmetrica rispetto alla precedente. In questo caso quindi i byte di fonia relativi ai canali della trama in ingresso verranno trasferiti nelle celle di memoria in relazione alle esigenze di permutazione. Conseguentemente, il trasferimento dei byte di fonia dalle celle della memoria ai canali della trama in uscita avviene in maniera ordinata e sequenziale: il byte di fonia nella cella di memoria X verrà trasferito in uscita nel canale di posizione X .

La struttura T deve consentire in un tempo di trama ($125 \mu s$) due accessi completi alla memoria, uno in scrittura e uno in lettura per ogni canale. In-

dicando con N il numero dei canali (uguali in ingresso e uscita) ed assumendo come costo della struttura T legato al tempo di accesso (supposto uguale per scrittura/lettura) t_a , si ha:

$$C = t_a \leq \frac{\text{Tempo Trama}}{2N}$$

Ricordiamo che il tempo di trama nella telefonia digitale è una costante fissa, derivante dai vincoli imposti dal Teorema del Campionamento di un segnale fonico, con valore $125 \mu s$, si nota facilmente che maggiore è il numero dei canali da gestire, minore deve essere il tempo di accesso alla memoria e quindi maggiore sarà il costo della relativa struttura T. Il numero massimo di canali gestiti per singola struttura T sarà di conseguenza limitato superiormente dai vincoli (tempi di accesso) imposti dalla tecnologia attuale.

3.3 Strutture multistadio

Le strutture multistadio si dividono in due grosse famiglie:

- strutture multistadio omogenee:
 - due stadi: S-S;
 - tre stadi: S-S-S;
- strutture multistadio non omogenee:
 - due stadi: T-S, S-T;
 - tre stadi: T-S-T, S-T-S;

Lo scopo delle strutture multistadio omogenee è quello di ridurre il costo totale della struttura risultante, mantenendo inalterati i requisiti funzionali e le prestazioni rispetto ad una realizzazione a singolo stadio mentre, per le strutture multistadio non omogenee, l'obiettivo primario è quello di aumentare i gradi di libertà delle operazioni di commutazione combinando le funzionalità delle strutture S (cambio di linea) con quelle di strutture T (permutazione di canale). L'esame delle strutture a tre stadi non omogenee sarà limitato a strutture T-S-T essendo queste largamente più diffuse dell'alternativa S-T-S.

3.3.1 Struttura S-S

In questo tipo di struttura è previsto l'uso di più elementi S organizzati in gruppi rispettivamente indicati come *primo stadio* e *secondo stadio* della struttura. L'insieme delle linee in ingresso viene partizionato in gruppi uguali (con lo stesso numero di linee). Il numero dei gruppi creati definisce il numero degli elementi S che costituiranno il primo stadio della struttura. La stessa operazione viene effettuata con le linee di uscita arrivando, anche in questo caso, a definire il numero di elementi S che costituiranno il secondo stadio della struttura di commutazione. Un'uscita di un elemento S del primo stadio è connessa, in ingresso,

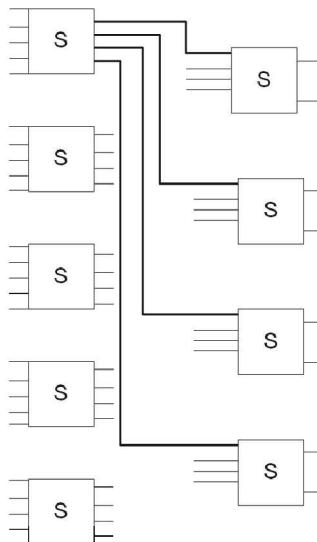


Figura 3.4: Struttura S-S

con uno ed uno solo degli elementi S del secondo stadio. La regola utilizzata per realizzare le connessione tra elementi S del primo e secondo stadio, supposti numerati con ordine crescente dall'alto verso il basso, può essere sintetizzata come segue:

L'uscita j dell'elemento i del primo stadio viene connessa all'ingresso i dell'elemento j del secondo stadio

In particolare la prima uscita del blocco uno del primo stadio è connesso al primo ingresso del blocco uno del secondo stadio; l'ultima uscita del blocco uno del primo stadio è connessa al primo ingresso dell'ultimo blocco del secondo stadio, continuando la prima uscita dell'ultimo blocco del primo stadio è connessa all'ultimo ingresso del blocco uno del secondo stadio; l'ultima uscita dell'ultimo blocco del primo stadio è connessa all'ultimo ingresso dell'ultimo blocco del secondo stadio. La struttura è mostrata in figura 3.4.

Come verificheremo al termine di questo paragrafo, il costo complessivo di una struttura S-S risulta minore del costo dell'equivalente struttura monostadio S, purtroppo però la struttura S-S non associa a questo vantaggio realizzativo il rispetto della condizione di non blocco. La struttura S-S è infatti bloccante perché un'altra linea in ingresso ad un elemento del primo stadio non può essere connessa in uscita con una linea appartenente ad un qualsiasi elemento del secondo stadio per il quale è già presente in uscita una richiesta gestita dallo stesso elemento del primo stadio in quanto la modalità di connessione tra elementi di stadi differenti prevede, per ogni coppia, uno solo collegamento. Per ripristinare il rispetto della condizione di non blocco sarebbe necessario prevedere un numero di connessione tra ogni elemento del primo stadio verso ogni elemento del secondo stadio uguale al numero delle sue possibili uscite. Questo, come verrà verificato ricorrendo ad

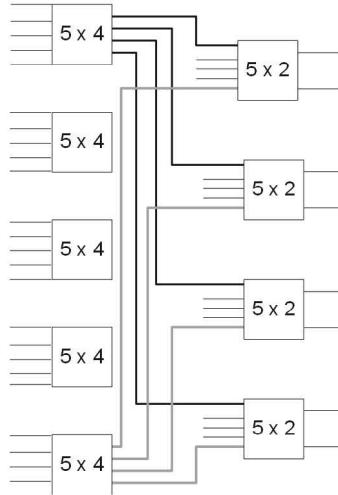


Figura 3.5: Esempio di struttura S-S

un esempio numerico, comporta la perdita del vantaggio in termini di costo della struttura S-S rispetto all'equivalente struttura S.

Come verifica di quanto affermato ci possiamo riferire al seguente caso pratico:

Si consideri un concentratore (numero linee in ingresso (L_{in}) > numero linee in uscita (L_{out})) caratterizzato da 25 linee di ingresso connesse con 8 linee di uscita. Si supponga di avere 5 blocchi di tipo S per la definizione del primo stadio, con 5 linee di ingresso e 4 linee di uscita e 4 blocchi di tipo S per la definizione del secondo stadio, con 2 linee in uscita e 5 linee in ingresso, come mostrato in figura 3.5.

Il costo di ciascun elemento al primo stadio è pari a:

$$C_I = 5 \cdot 4 = 20$$

Dunque il costo totale del primo stadio è:

$$C_{\text{tot}_I} = 5 \cdot C_I = 5 \cdot 20 = 100$$

Il costo di ciascun elemento del secondo stadio è:

$$C_{II} = 5 \cdot 2 = 10$$

Il costo totale del secondo stadio è:

$$C_{\text{tot}_{II}} = 4 \cdot C_{II} = 4 \cdot 10 = 40$$

Segue quindi che il costo totale della struttura S-S è:

$$C_{\text{tot}} = C_{\text{tot}_I} + C_{\text{tot}_{II}} = 100 + 40 = 140$$

Se lo stesso concentratore fosse stato realizzato con un'unica struttura S, il costo sarebbe stato di:

$$C_S = 25 \cdot 8 = 200$$

Questa struttura, come detto in precedenza, risulta bloccante. Per far sì che risulti non bloccante bisogna porre il numero di linee in uscita da ogni elemento del primo stadio connesse come ingressi al secondo stadio uguali al numero di linee in uscita dal secondo stadio. Il costo di ciascun elemento del primo stadio è pari a:

$$C_I = 5 \cdot 8 = 40$$

Quindi si ottiene un costo totale per il primo stadio pari a:

$$C_{\text{tot}_I} = 5 \cdot C_I = 5 \cdot 40 = 200$$

Analogamente il costo di ciascun elemento del secondo stadio è:

$$C_{II} = 10 \cdot 2 = 20$$

Ottenendo un costo totale per il secondo stadio di:

$$C_{\text{tot}_{II}} = 4 \cdot C_{II} = 4 \cdot 10 = 80$$

Il costo totale della struttura S-S non bloccante è quindi:

$$C_{\text{tot}} = C_{\text{tot}_I} + C_{\text{tot}_{II}} = 200 + 80 = 280$$

Come si può notare da questo semplice esempio, la condizione di non blocco fa aumentare il costo della struttura e non la rende più competitiva nei confronti dell'equivalente struttura S monostadio.

3.3.2 Struttura T-S

In questo tipo di struttura si interconnettono un primo stadio composto da elementi di tipo T e un secondo stadio costituito da un solo elemento di tipo S, come mostrato in figura 3.6. La struttura T-S ha lo scopo di combinare le funzionalità tipiche delle singole strutture T e S, consentendo la permutazione di canale (tramite lo stadio T) e il cambio di linea (tramite lo stadio S). Una struttura T-S a due stadi è bloccante: ad esempio non si riesce a gestire il caso di due richieste di connessione relative a due canali di una stessa trama in ingresso che vogliono essere trasferiti nello stesso stesso canale di trame su uscite differenti. Pur non essendo queste due richieste in conflitto tra loro la struttura T-S non riesce ad espletarle entrambe in quanto la struttura S riesce solo a trasferire nella posizione di uscita voluta una sola delle due. Le strutture ibride non consentono una riduzione del costo.

A titolo di esempio si faccia riferimento al seguente caso. Si ha una richiesta in ingresso sulla linea 1, canale 7 ($L1, Ch7$), la quale deve essere commutata sulla posizione di canale 3 della linea di uscita 8 ($L1, Ch3$). All'ingresso della struttura T la richiesta entra nella linea di competenza e in uscita viene permutato nella

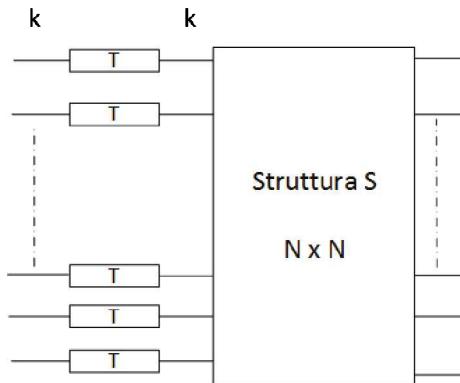


Figura 3.6: Struttura T-S

posizione di canale voluta. La richiesta adesso si trova sulla linea 1 canale 3 ($L1, Ch3$). Infine la richiesta entra nella struttura S la quale realizza il cambio di linea. In uscita, dunque, la richiesta si trova, come voluto, sulla linea 8 canale 3 ($L8, Ch3$).

3.3.3 Struttura S-T

Le strutture S-T hanno un'architettura simmetrica rispetto alle T-S. In questo caso abbiamo una struttura S come primo stadio che si connette con un secondo stadio formato da strutture T, come mostrato in figura 3.7. Anche in questo caso si riesce ad abbinare le funzionalità proprie delle singole strutture S e T : è possibile cambiare linea (tramite lo stadio S) mantenendo inalterata la posizione del canale e successivamente permutare la posizione di canale (tramite lo stadio T).

È facile prevedere che anche la struttura S-T, come la sua simmetrica T-S, risulterà bloccante. In questo caso non si riesce a soddisfare contemporaneamente due richieste, non in conflitto tra di loro, riferite alla connessione di due canali con lo stesso numero d'ordine nell'ambito di trame di ingresso su linee diverse che vogliono andare ad occupare posizioni diverse nella trama relativa ad una stessa linea di uscita.

A titolo di esempio, si faccia riferimento al caso trattato in precedenza. Si ha una richiesta in ingresso sulla linea 1, canale 7 ($L1, Ch7$), la quale deve essere trasferita sulla linea di uscita 8 con posizione di canale 3 ($L1, Ch3$). All'ingresso della struttura S la richiesta viene trasferita sulla linea richiesta mantenendo però inalterato il canale di origine. La richiesta adesso si trova sulla linea di uscita 8 canale 7 ($L8, Ch8$). Infine, la struttura T che gestisce l'uscita 8 della struttura S opera la permutazione di canale completando l'operazione di commutazione. Adesso quindi, come desiderato, la richiesta si trova nel canale 3 della linea di uscita 8 ($8, Ch3$).

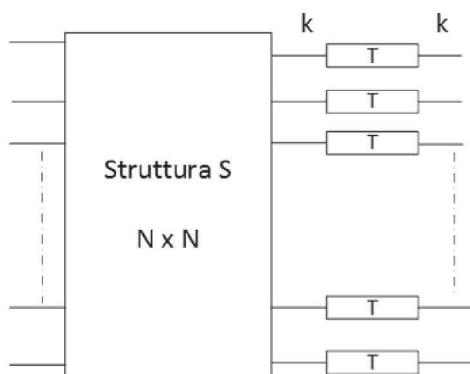


Figura 3.7: Struttura S-T

3.3.4 Struttura S-S-S

In questo tipo di struttura si interconnettono tre commutatori di tipo S. Anche in questo caso l'insieme delle linee in ingresso e di uscita sono partizionati in gruppi uguali (con lo stesso numero di linee) arrivando così a definire il numero di elementi S che costituiranno il primo e terzo stadio. In accordo con il vincolo che impone che una uscita di un elemento S del primo stadio debba essere connessa in ingresso con uno ed uno solo degli elementi S del secondo stadio (lo stesso vale per le uscite degli elementi del secondo stadio verso gli ingressi degli elementi del terzo stadio) si ha che il numero di elementi costituenti il secondo stadio deve essere uguale al numero di uscite/ingressi degli elementi del primo/terzo stadio.

La regola con cui si realizzano i collegamenti tra gli elementi di stadi differenti è analoga a quella utilizzata per strutture S-S con l'unica differenza che è adesso estesa al caso tre stadi. Potremo riformularla come segue :

L'uscita j dell'elemento i di uno stadio viene connessa all'ingresso i dell'elemento j dello stadio successivo

La struttura S-S-S è mostrata in figura 3.8.

Si ipotizzi, per semplicità di trattazione, di avere per il nostro commutatore N linee in ingresso e N linee in uscita. Chiaramente, se esso fosse realizzato con una singola struttura S il costo risultante sarebbe stato N^2 . Si assuma che ogni elemento del primo stadio della struttura S-S-S abbia n linee in ingresso, lo stesso vale per le linee di uscita degli elementi del terzo stadio e k linee di uscita (che saranno gli ingressi ai singoli elementi del terzo stadio). Di conseguenza si avranno k elementi del secondo stadio ciascuno di ordine $\frac{N}{n} \cdot \frac{N}{n}$. In generale si avrà poi $k >> n$, cioè il numero dell'uscita del secondo stadio è più grande del numero di ingressi al primo stadio. In accordo con questa impostazione si avranno al primo e al terzo stadio $\frac{N}{n}$ elementi S di ordine $n \cdot k$. Ricapitolando si ha:

- primo stadio: $\frac{N}{n}$ blocchi con n linee di ingresso e k linee di uscita;

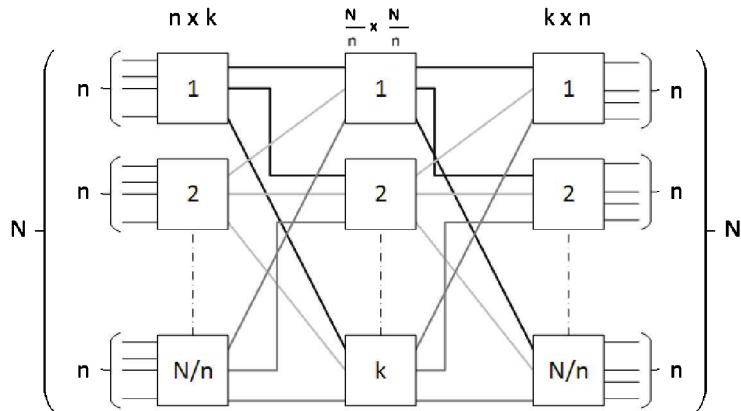


Figura 3.8: Struttura S-S-S

- secondo stadio: k blocchi con $\frac{N}{n}$ linee di ingresso e $\frac{N}{n}$ linee di uscita;
- terzo stadio: $\frac{N}{n}$ blocchi con k linee di ingresso e n linee di uscita.

Il costo complessivo della struttura S-S-S sarà quindi dato dalla somma dei costi dei singoli stadi:

$$\begin{aligned} C_{\text{TOT}} &= \frac{N}{n}(n \cdot k) + k\left(\frac{N}{n} \cdot \frac{N}{n}\right) + \frac{N}{n}(k \cdot n) = N \cdot k + k \cdot \frac{N^2}{n^2} + N \cdot k = \\ &= k \cdot N\left(2 + \frac{N}{n^2}\right) \end{aligned} \quad (3.1)$$

L'obiettivo dell'analisi che segue è quello di definire i valori ottimi dei parametri incogniti n e k in maniera da avere una struttura risultante con costo inferiore all'equivalente monostadio S e non bloccante.

Riportiamo il problema di ottimizzazione a due variabili ad una sola andando a definire il minimo valore del parametro k , dato come funzione di n , che permette di garantire la condizione di non blocco. Questa analisi fu per primo proposta da C. Clos ed il risultato finale è noto in letteratura come *risultato di Clos*. L'analisi di Clos si basa sulla individuazione del caso operativo peggiore e nella conseguente definizione del valore minimo di k , dato come funzione di n , che permette di garantire la condizione di non blocco (worst case analysis). Le ipotesi su cui si basa l'analisi di Clos, fissato un particolare elemento del primo stadio e uno del terzo stadio, sono:

- delle n linee di ingresso ad un elemento fissato del primo stadio, una è libera e $n - 1$ sono occupate (vi sono delle richieste in ingresso);
- delle n linee di uscita di un elemento fissato del terzo stadio, una è libera e $n - 1$ sono occupate (vi sono delle richieste in uscita);

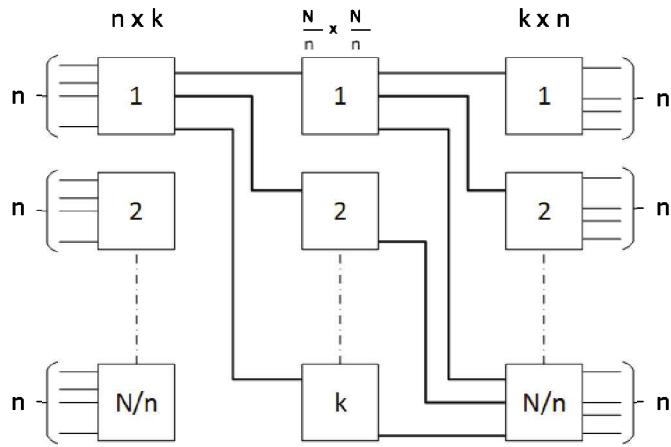


Figura 3.9: Analisi di Clos

- nessuna delle richieste presenti in ingresso all'elemento del primo stadio considerato è una di quelle presenti in uscita all'elemento del terzo stadio d'interesse: le richieste presenti in ingresso e uscita ai due elementi considerati (primo e terzo stadio) siano insiemi disgiunti;
- le $n - 1$ richieste in ingresso all'elemento del primo stadio sono connesse ad elementi del secondo stadio differenti da quelli che hanno un'uscita connessa con un ingresso dell'elemento del terzo stadio considerato: l'insieme degli elementi del secondo stadio impegnati dagli ingressi dell'elemento del primo stadio considerato è disgiunto rispetto all'insieme degli elementi del secondo stadio che hanno l'uscita connessa con un ingresso dell'elemento del terzo stadio di interesse;
- si vuole collegare l'unico ingresso disponibile dell'elemento del primo stadio considerato con l'unica uscita disponibile dell'elemento del terzo stadio di interesse.

La situazione è mostrata in figura 3.9.

È semplice notare che affinché sia possibile realizzare senza conflitto la richiesta di connessione si dovranno avere al secondo stadio un numero di elementi S almeno uguale a:

$$k = (n - 1) + (n - 1) + 2 = 2 \cdot n - 1 \quad (3.2)$$

Sostituendo la 3.2 nella 3.1 si ottiene il costo della struttura S-S-S non bloccante come funzione della sola incognita n :

$$C_{\text{TOT}} = 2 \cdot N(2 \cdot n - 1) + (2 \cdot n - 1) \left(\frac{N}{n} \right)^2$$

Supponendo $n >> 1$ si ottiene:

$$C_{\text{TOT}} = 4Nn + \frac{2N^2}{n} \quad (3.3)$$

Adesso rimane da determinare n ottimo tale che C assuma il valore minimo. Per prima cosa si effettua la derivata della 3.3 rispetto a n e la si pone uguale a 0:

$$\frac{dC}{dn} = 0 \quad \Rightarrow \quad \frac{dC}{dn} = 4N - \frac{2N^2}{n^2} = 0 \quad (3.4)$$

ottenendo un valore di n pari a:

$$n = \sqrt{\frac{N}{2}} \quad (3.5)$$

Sostituendo questo risultato nella 3.3 si ottiene, per il caso peggiore:

$$C_{\text{ottimo}} = 4\sqrt{2}N^{\frac{3}{2}} \quad (3.6)$$

e si può facilmente verificare che questo valore è minore rispetto al costo ($C = N^2$) di una equivalente struttura S monostadio. Nell'attuazione del dimensionamento ottimo prima descritto occorre però tenere di conto di alcuni vincoli per rispettare la realizzabilità fisica della struttura:

- 1) n deve essere un numero intero, in quanto rappresenta il numero di linee di ingresso del primo stadio;
- 2) $\frac{N}{n}$ deve essere un numero intero (N multiplo intero di n), in quanto rappresenta il numero di blocchi del primo stadio.

Quando non è possibile soddisfare questi vincoli si deve considerare un dimensionamento sub-ottimo considerando i valori di n che rispettano i vincoli della realizzabilità fisica in difetto ($n_1 < n_{\text{ott}}$) e in eccesso ($n_2 > n_{\text{ott}}$) e valutare i costi risultanti dalle strutture S-S-S non bloccanti. La soluzione da adottare sarà ovviamente quella che consentirà il costo minore.

3.3.5 Struttura T-S-T

L'obiettivo principale di una struttura T-S-T è realizzare un'operazione di commutazione che combini le capacità funzionali proprie di strutture S e T, che consenta di ridurre i costi realizzativi e che garantisca la condizione di non blocco. In questo contesto la riduzione dei costi è limitata alla realizzazione delle strutture T e può avere una importanza marginale rispetto agli altri requisiti. L'integrazione delle funzionalità di strutture S e T la si può ottenere anche con strutture non omogenee a due stadi (T-S, S-T) ma, come abbiamo visto, senza garanzia del rispetto della condizione di non blocco. La struttura T-S-T riesce invece a soddisfare entrambi i requisiti. La struttura di una rete di connessione T-S-T è mostrata in figura 3.10, dove, in particolare,abbiamo un primo stadio composto

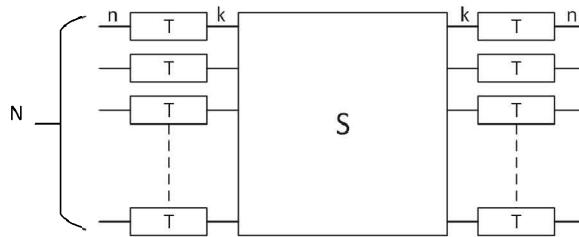


Figura 3.10: Struttura T-S-T

da elementi T (uno per ogni linea di ingresso) con trame in ingresso formate da n canali e trame in uscita di k canali con in genere $k \gg n$. Un secondo stadio formato da una struttura S ed un terzo stadio speculare al primo.

Poiché la complessità delle strutture T è funzione del parametro k , il dimensionamento ottimo di questa struttura consiste nel definire il minimo valore di k che sia in grado di garantire il rispetto della condizione di non blocco. Anche in questo caso lo studio di questo problema fu affrontato per la prima volta da C. Clos ed il risultato ottenuto è noto oggi in letteratura come *risultato di Clos* per strutture T-S-T. Analogamente al caso S-S-S Clos arrivò a definire il valore ottimo di k considerando il caso operativo peggiore (worst case analysis). Le ipotesi che assunse, considerando di dover trasferire il byte di un canale fonico di una trama relativa ad una fissata linea in ingresso in un canale disponibile di una trama su di una fissata linea di uscita, furono:

- degli n canali disponibili nella trama di ingresso di interesse (primo stadio), uno solo è libero mentre i rimanenti $n - 1$ sono occupati (vi sono richieste in ingresso);
- degli n canali disponibile nella trama relativa alla linea di uscita desiderata (terzo stadio), un solo è libero mentre gli altri $n - 1$ sono occupati (vi sono richieste in uscita);
- nessuna delle richieste presenti in ingresso all'elemento T del primo stadio considerato è una di quelle presenti in uscita all'elemento T del terzo stadio d'interesse: le richieste presenti in ingresso e uscita ai due elementi T considerati (primo e terzo stadio) siano insiemi disgiunti;
- nell'ambito della trama con k canali disponibili in uscita dall'elemento T del primo stadio ed in ingresso all'elemento T del terzo stadio di interesse occupano posizioni di canale diverse : ovvero l'insieme degli $n - 1$ canali occupati in uscita della struttura T del primo stadio è disgiunto dall'insieme dei canali occupati nella trama in ingresso alla struttura T del terzo stadio considerata;
- si vuole collegare l'unico canale libero dell'elemento T del primo stadio con l'unico libero in uscita all'elemento T del terzo stadio desiderato.

Affinché tale richiesta sia gestibile, senza blocco occorre, quindi che venga rispettata la seguente condizione:

$$k = (n - 1) + (n - 1) + 2 = 2 \cdot n - 1 \quad (3.7)$$

In questo caso una eventuale riduzione di costo è applicabile alle solo strutture T che assumerà, come conseguenza della (3.7), il minimo valore congruente con il rispetto della condizione di non blocco.

3.3.6 Analisi di Lee

Il risultato di Clos è focalizzato sulla garanzia assoluta del rispetto della condizione di blocco ed in particolare non tiene conto che un traffico dati è in generale un processo aleatorio e non deterministico. La Teoria di Lee è un approccio alternativo a quello di Clos che si basa su un modello statistico del traffico (cioè l'arrivo delle richieste alla rete di connessione è considerato come evento casuale e non certo). Si applica in particolar modo alle strutture multi-stadio a tre o più stadi. La sua particolarità è che in questa analisi si considera l'evento di blocco su base statistica. L'analisi di Lee si indirizza verso un dimensionamento di reti di connessione che non rispetta la garanzia assoluta dell'assenza di blocco ma che altresì ne tollera l'eventualità quando questo avviene con una probabilità piccola a sufficienza (outage). Quindi l'obiettivo dell'analisi di Lee è quello di definire strutture di commutazione per le quali l'evento probabilità di blocco sia estremamente raro e allo stesso tempo abbiano un costo inferiore rispetto alle equivalenti strutture basate sulla teoria di Clos.

L'analisi di Lee si applica indifferentemente alle strutture a tre stadi omogenee e non omogenee, per semplicità di trattazione considereremo di seguito solo strutture S-S-S. Volendo definire con quale probabilità la struttura S-S-S risulta bloccante si ammette di conoscere con quale probabilità una linea di ingresso è occupata. Detta a tale probabilità, si assume che la destinazione di uscita di una richiesta in ingresso ad un elemento del primo stadio sia uniforme su tutte le alternative possibili. Quindi con probabilità uniforme $\frac{1}{k}$ è richiesta una delle linee disponibili. Da qui ne segue che la probabilità di avere una linea di uscita di un elemento del primo stadio occupata è:

$$p = \frac{n \cdot a}{k} \quad (3.8)$$

dove n sono le linee complessivamente presenti in ingresso all'elemento S considerato.

Tenendo presente che gli elementi del secondo stadio hanno un numero di ingressi uguale alle uscite, si può definire la probabilità di avere un cammino libero che permetta la connessione di una linea in ingresso ad un elemento del primo stadio con una uscita libera di un elemento del terzo stadio così:

$$p\{\text{cammino libero}\} = (1 - p)^2$$

da qui è immediato notare che la probabilità di avere un cammino ingresso/uscita non disponibile è:

$$p\{\text{cammino occupato}\} = 1 - (1 - p)^2$$

Ne segue che la probabilità di blocco, cioè la probabilità che non sia possibile connettere un ingresso ad una uscita desiderata libera della struttura S-S-S, risulta essere data da:

$$p\{\text{blocco}\} = [1 - (1 - p)^2]^k \quad (3.9)$$

L'equazione 3.9 è la formula di Lee. Questa analisi non è esatta, la causa è da ricercarsi nell'ipotesi iniziale di indipendenza che ha portato a definire la (3.8). La verifica di questo la si ottiene facilmente sostituendo nella (3.9) il risultato di Clos e notando che la probabilità di blocco risultate non è zero (evento impossibile). Nonostante questi limiti, il risultato di Lee è largamente utilizzato nel definire il dimensionamento di strutture a tre stadi, fissati determinati requisiti di servizio (valori accettabili per la probabilità di blocco (outage) in relazione a condizioni di carico (paramento a) predefinite).

3.4 Commutatori Veloci a Pacchetto

Le attuali reti a commutazione di pacchetto dovendo garantire elevate velocità per il trasferimento dell'informazioni hanno richiesto uno sviluppo tecnologico specifico per gli autocommutatori (Hui'1990, Tobagi'1990, Iyer'2008, Turner'1998 in 2.3). In particolare, per evitare che l'operazione di commutazione sia il collo di bottiglia di un collegamento, viene tipicamente richiesto che essa sia eseguita in un tempo piccolo rapportato al tempo di trasmissione dei pacchetti nella rete. Per questo motivo le strutture di autocommutazione di questo tipo sono chiamate strutture a commutazione veloce di pacchetto (Fast Packet Switch). Per fissare questo concetto ci si può riferire alla analogia con una corsa automobilistica di Formula 1. Come gli appassionati di questo sport sanno, molto spesso un tempo eccessivo speso nella sosta ai box per il cambio gomme (switch) può pregiudicare il buon esito della gara e vanificare l'elevate prestazioni in termini di velocità della autovettura. Quindi nel nostro caso sarebbe poco redditizio investire su mezzi di trasmissione di elevata qualità (es. fibra ottica) e metodologie di trasmissione/ricezione avanzate se poi il ritardo di trasferimento E2E viene ad essere polarizzato dai tempi di switch nei nodi di transito.

Tipicamente per rendere veloce l'operazione di commutazione questa viene implementata il più possibile su base hardware. Le tecnologie di base sono:

- **Crossbar** : è la tecnologia a divisione di spazio precedentemente discussa che trova, con qualche modifica, applicazione anche nel caso di commutatori veloci di pacchetto;
- **Banyan** : In questo caso il pacchetto viene indirizzato verso la porta di uscita desiderata in base alla processazione sequenziale dei bit che indicano in forma binaria l'indirizzo della porta di uscita. La struttura dello switch è a più livelli, con ogni livello formato da semplici switch (vedi fig.3.11). In generale se si devono collegare N linee in ingresso con altrettante uscite la struttura ha $\log_2 N$ livelli ciascuno con $N/2$ switch elementari;
- **Batcher-Banyan**: questa soluzione consente di evitare che all'interno della struttura Banyan pacchetti destinati a porte di uscita differenti collidano

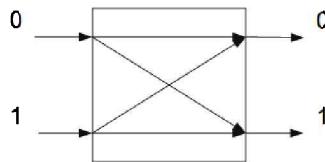


Figura 3.11: Switch Banyan (2x2)

(cioè entrano in competizione per una stessa uscita di uno switch elementare). L'idea alla base di questa struttura è quella di anteporre allo switch Banyan una struttura di commutazione che porta il nome del suo inventore (Batcher) che opera un opportuno ordinamento dei pacchetti in ingresso.

3.5 Letture Consigliate

Le tecnologie e le strutture di commutazione sono discusse nei seguenti testi:

- M.Schwarz, Telecommunication Networks, Addison Wesley, 1987.
- J.L.Hammond, P.J.P.O'Reilly, Local Computer Networks, Addison Wesley, 1986.
- F. Halsall, Reti di Calcolatori e Sistemi Aperti, Addison-Wesley, 1996.
- J.C. McDonald, Fundamentals of Digital Switching, Plenum, 1983.
- J.Y. Hui, Switching and Traffic Theory for Integrated Broadband Networks, Kluver, 1990.
- J.G. Pearce, Telecommunications Switching, Plenum, 1981.
- B.A. Forouzan, Reti di Calcolatori ed Internet, McGraw-Hill, 2007.
- J.F. Kurose, K.W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.

Si suggerisce inoltre di consultare i seguenti articoli scientifici:

- F. Tobagi, "Fast Packet Switching Architectures for Broadband Integrated Networks", Proc. IEEE INFOCOM, 1990.
- S. Iyer, R.R. Komella, N. McKeown, "Design Packet Buffers for Router Line Cards", IEEE Trans. on Networking, giugno 2008.
- J.S. Turner, "Design of Broadcast Packet Switching Networks", IEEE Trans. on Communications, giugno 1998.

4

Reti per trasmissione di dati

Le reti per trasmissione di dati (Data Network) servono per collegare tra loro sistemi per l'elaborazione dell'informazione (Computer Network), dispositivi o oggetti (Internet of Things), sensori e attuatori (Sensor and Actor Network) principalmente per lo scambio di informazioni in formato numerico (bit) ed oggi perfino in modalità autonoma cioè, senza l'intervento diretto dell'uomo. Per il tipo di informazione scambiata è quindi adatta una rete numerica anche se è possibile connettere calcolatori e dispositivi tramite una rete non specifica per la trasmissione dati come la rete telefonica. In particolare, questo è reso possibile utilizzando degli apparati chiamati modem e tecnologie xDSL che grazie ad opportune tecniche consentono la coesistenza tra flussi dati e comunicazioni foniche in uno stesso supporto fisico (es.: doppino telefonico). Un flusso dati è un flusso di bit che grazie a metodologie proprie della trasmissione dati (modulazione, codifica, ecc.) viene reso in grado di attraversare il canale di comunicazione, opportunamente individuato nella rete, per connettere la sorgente dell'informazione con l'utilizzatore che ne ha fatto richiesta. Le caratteristiche principali di un traffico dati sono :

- *intermittenza temporale*: il flusso informativo che passa in un collegamento non è continuo rispetto al tempo di osservazione. Sono in genere evidenti intervalli temporali in corrispondenza dei quali la scambio di informazioni non è attivo. Conseguenza di questo è che l'utilizzazione effettiva del collegamento risulta una frazione di tempo ridotta rispetto al tempo totale durante il quale il collegamento rimane attivo. Per ottimizzare l'uso delle risorse di rete si devono quindi individuare metodologie in grado di fare condividere stesse risorse di rete (nodi, linee) da più coppie sorgente/utilizzatore (connessioni) senza ovviamente pregiudicare la qualità del servizio offerto dalla rete (es.: ritardi di trasferimento eccessivi);
- *asimmetria*: le linee vengono impegnate diversamente a seconda della direzione del flusso, es.: in una connessione tra un utente (client) ed un data base, l'interrogazione del client rivolta al data base richiede un trasferimento di bit generalmente inferiore alla risposta fornita dal data base all'interrogazione (download);
- *integrità dell'informazione*: generalmente l'integrità dell'informazione trasferita, cioè l'assenza di errori nel flusso dati ricevuto, è meno tollerata



Figura 4.1: Traffico dati

rispetto a comunicazioni analogiche (es.: voce). In particolare, in relazione ad applicazioni specifiche, se non garantita a sufficienza, essa può diventare un fattore di notevole criticità. In generale, a titolo di esempio, si può dire che la probabilità di errore tollerata è dell'ordine di $10^{-4} \div 10^{-6}$.

La figura 4.1 mostra un tipico traffico dati con le sue principali caratteristiche. Una ulteriore classificazione di un traffico dati può essere fatta con riferimento alle sue caratteristiche temporali:

- sincrono: è un traffico dati quasi continuo, come ad esempio nel trasferimento di file di dimensioni notevoli;
- asincrono: è un traffico dati intermittente;
- isocrono: ha bisogno di un riferimento temporale preciso, come accade nella trasmissione numerica del segnale vocale o video.

4.1 Architettura a livelli

L'architettura di una rete risponde alla necessità di razionalizzare l'uso della rete stessa secondo un modello strutturale a cui tutti i dispositivi si devono uniformare al fine di comunicare tra loro (Forouzan'2007, Kurose'2013, Tanenbaum'2011 in 4.10). In generale, l'architettura di una rete comprende un insieme di protocolli, cioè una raccolta di regole che i dispositivi di rete devono rispettare per poter essere in grado di comunicare. Data la complessità di una rete, l'insieme dei protocolli propri della sua architettura sono organizzati secondo un criterio di raggruppamento e stratificazione. In particolare, i protocolli di rete sono organizzati in una struttura logica, gerarchica (protocol stack), rappresentabile mediante un modello a strati (ogni strato viene indicato con il nome di *livello* (layer)). Questi livelli possono essere visti come dei contenitori virtuali di tutte le operazioni preposte allo svolgimento di un servizio che tipicamente viene fornito dal livello stesso a quello immediatamente superiore secondo l'ordinamento gerarchico. Le modalità con cui il servizio è implementato sono trasparenti al livello superiore (information hiding) per il quale lo strato inferiore si configura come una sorta di macchina virtuale (Tanenbaum'2011 in 4.10). Ne consegue che le specifiche di una architettura di rete non riguarderanno i dettagli implementativi relativi alle funzioni espletate ma si rivolgeranno invece alle specifiche delle interfacce con i livelli contigui. L'architettura gerarchica di una rete è mostrata

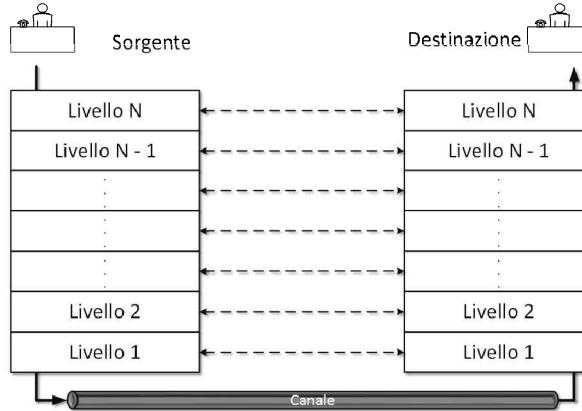


Figura 4.2: Architettura protocollare a livelli

in figura 4.2 considerando l'esempio di una comunicazione tra due terminali A (sorgente) e B (destinazione).

Come si può vedere dalla figura per poter conseguire una cooperazione tra i vari livelli occorre che siano rese disponibili modalità di interfaccia funzionali di ogni livello con lo strato immediatamente superiore ed inferiore. Fanno eccezione a questa modalità, (figura 4.2), il livello più alto, che si interfacerà con il solo livello sottostante e il livello più basso, che si interfacerà con il livello superiore e che dovrà preoccuparsi di predisporre le adeguate modalità per la trasmissione effettiva dell'informazione nel canale di comunicazione verso la sua destinazione. Lo scambio di informazioni viene poi gestito in accordo con il paradigma della comunicazione multilivello. Ogni livello della pila protocollare propria del dispositivo A è in comunicazione con il pari livello della pila protocollare propria di B. Livelli uguali appartenenti alle rispettive pile protocollari A, B sono detti pari (peer) e la modalità di comunicazione prima descritta si indica come comunicazione tra pari (peer-to-peer). Da notare che le comunicazioni tra livelli sono di tipo virtuale (tratteggiate in figura 4.2). La comunicazione effettiva tra i due dispositivi A,B è realizzata solo attraverso il canale di comunicazione.

Il concetto di una comunicazione multilivello trova analogie in molti casi della nostra vita comune. Si pensi ad esempio allo scambio di un documento relativo ad un accordo commerciale (figura 4.3) tra due gruppi industriali di nazioni differenti es.: italiano e cinese.

Immaginiamo il consiglio di amministrazione (livello superiore in figura 4.3) del gruppo italiano voglia sottoporre al consiglio di amministrazione del gruppo cinese (peer) l'atto dell'accordo. I due consigli si avvalgano del supporto dei rispettivi uffici affari legali (livello intermedio in figura 4.3). Il protocollo di comunicazione tra i rispettivi uffici legali (peer di livello intermedio) prevede che l'atto sia scritto in lingua inglese. L'ufficio legale del gruppo italiano provvederà quindi a produrre l'atto legale in lingua inglese secondo quanto concordato con il corrispondente ufficio legale del gruppo cinese. L'ufficio legale del gruppo italiano

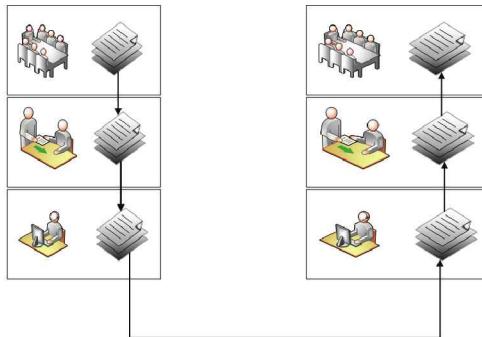


Figura 4.3: Architettura: consiglio di amministrazione, ufficio affari legali, ufficio comunicazioni.

trasferisce l'atto all'ufficio comunicazioni (livello inferiore in figura 4.3) che, a sua volta, lo inoltra all'ufficio comunicazioni (peer) di destinazione secondo una modalità concordata (es.: posta elettronica). Una volta ricevuto il messaggio l'ufficio comunicazioni del gruppo cinese provvederà a trasferirlo al proprio ufficio legale secondo modalità definite. L'ufficio legale a suo volta ne verificherà la congruenza con quanto stabilito con il corrispondente ufficio legale del gruppo italiano e, una volta tradotto in cinese, lo passerà al Consiglio di amministrazione per la sua ratifica finale.

Un altro concetto che è importante introdurre per comprendere meglio l'architettura di una rete è quello di *servizio* che, come specificato in precedenza, è ciò che un livello inferiore fornisce al livello superiore tramite le modalità di interfaccia. Un *servizio* è un'insieme di primitive (ovvero di operazioni base) che un livello offre a quello immediatamente superiore. Un servizio definisce quindi quali operazioni il livello è in grado di fornire. Un qualsiasi servizio è implementato in un livello attraverso operazioni specifiche che lo caratterizzano. Queste operazioni prendono il nome di *primitive*. Si possono distinguere quattro tipologie fondamentali di *primitive* (Kurose'2013, Tanenbaum'2011 in 4.10):

- *request*: un livello superiore richiede un servizio al livello sottostante;
- *indication*: un livello invia informazioni al livello superiore;
- *response*: un livello risponde alla richiesta di un servizio remoto utilizzando un servizio reso dal livello a lui sottostante;
- *confirm*: un livello informa il livello superiore di una risposta pervenuta da un sistema remoto.

Un servizio si può poi definire come orientato alla connessione (connection oriented) o senza connessione (connectionless):

- *connection oriented*: questa modalità viene attivata quando è strettamente necessario che la sequenza dei dati in arrivo rispetti lo stesso ordine di

generazione. Questo requisito implica che si debba individuare preventivamente all'interno della rete un percorso, che tutti i pacchetti appartenenti ad uno stesso flusso informativo (servizio) dovranno seguire. Questo necessita, se da un lato preserva, in ricezione, l'ordinamento dei pacchetti dall'altro comporta l'espletamento di una fase iniziale di scoperta e instaurazione del percorso all'interno della rete, detta fase di set-up (precedentemente definita), che, a sua volta, introduce un ritardo sull'inizio della comunicazione;

- **connectionless:** in questa modalità non è previsto la creazione di un percorso fisso tra mittente e destinatario. I pacchetti all'interno della rete possono seguire percorsi differenti che ogni nodo della rete può selezionare in maniera autonoma avendo comunque presente il raggiungimento della destinazione finale. Questo può portare, a destinazione, ad avere arrivi di pacchetti non coerenti con il loro ordine di generazione. Questa modalità rende comunque il trasferimento dell'informazione più reattivo nei riguardi di variazioni di stato della rete (congestioni, guasti, ecc.) e non necessita della fase di set-up.

Un servizio può poi essere ulteriormente caratterizzato sulla base della sua affidabilità. A questo riguardo si identificano i due casi seguenti:

- **affidabile:** in questa modalità si richiede una notifica esplicita dell'avvenuto invio del messaggio. Anche se il trasferimento della notifica di corretta ricezione (riscontro) è tipicamente più veloce che non il trasferimento dell'informazione, il meccanismo di conferma può introdurre ritardi che spesso non sono tollerabili. Un esempio tipico sono le comunicazioni voce su rete IP (VoIP) per le quali è preferibile tollerare un po' di rumore sul segnale informativo (dovuto in genere alla perdita di pacchetti) che un ritardo dovuto alle conferme;
- **non affidabile:** in questa modalità non è previsto l'inoltro di un messaggio di riscontro a fine comunicazione. Il mittente quindi non ha la certezza che la comunicazione sia andata a buon fine. Questa modalità è in genere utilizzata quando siamo di fronte ad inoltri verso più destinazioni di uno stesso flusso informativo (multicast).

In relazione alle comunicazioni multilivello si sono venute a formare due scuole di pensiero:

- **architettura aperta:** permette l'interscambiabilità di apparecchiature provenienti da costruttori differenti e l'ottimizzazione solo di singole parti della rete. Le sole interfacce di comunicazione tra i livelli adiacenti sono standardizzate. È di difficile realizzazione nella pratica, anche se accettata universalmente;
- **architettura proprietaria:** è caratterizzata dall'impiego esclusivo di dispositivi forniti da un'unica casa produttrice e la rete viene ottimizzata globalmente e non nei singoli livelli. Questo vincola l'utente ad utilizzare esclusivamente dispositivi certificati dalla casa proprietaria della rete.

Una caratteristica importante comune alle due declinazioni del concetto di architettura di rete è che la modalità di funzionamento di un livello non dipende da quello proprio degli altri. Questo requisito permette di avere una elevata flessibilità in quanto per ogni strato, una volta definite le regole con cui può comunicare con i livelli adiacenti, può essere aggiornato con un impatto minimo sull'intera architettura. Il servizio è correlato all'interfaccia tra i due livelli dove quello inferiore ha il ruolo di *provider* mentre quello superiore è l'*utente*.

4.2 Modello ISO/OSI

L'Open System Interconnection (OSI) è una proposta formulata da ISO (International Organization for Standardization) con la finalità di definire dei modelli (standard) per ogni livello. Il modello, adottato nel 1978, è internazionalmente conosciuto come architettura ISO/OSI. È un modello di rete aperta, quindi all'interno di una stessa rete possono coesistere e cooperare apparecchiature di produttori differenti. Il modello ISO/OSI prevede sette livelli, come mostrato in figura 4.4, organizzati in forma gerarchica, a ciascuno strato è poi associato un nome che ne caratterizza le funzionalità. A questo riguardo è necessario puntualizzare che il modello ISO/OSI non è propriamente una specifica di una architettura di rete in quanto non definisce i servizi ed i protocolli propri di ogni strato ma si limita ad indicarne le funzionalità base di competenza. I livelli sono, dall'alto verso il basso: livello di applicazione (*Application Layer*), livello di presentazione (*Presentation Layer*), livello di sessione (*Session Layer*), livello di trasporto (*Transport Layer*), livello di rete (*Network Layer*), livello di collegamento (*Data Link Layer*) e livello fisico (*Physical Layer*). I primi tre livelli (fisico, collegamento e rete) sono detti *livelli di rete*, mentre gli ultimi quattro (trasporto, sessione, presentazione e applicazione) sono detti *livelli di utente o applicativi*.

I livelli trasporto, sessione, presentazione e applicazione operano su base end-to-end (E2E), ciò vuol dire che questi livelli, lato sorgente, hanno una comunicazione virtuale solo con i pari livello della destinazione finale (le loro funzionalità

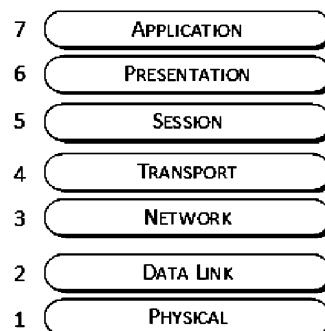


Figura 4.4: Architettura protocollare ISO/OSI

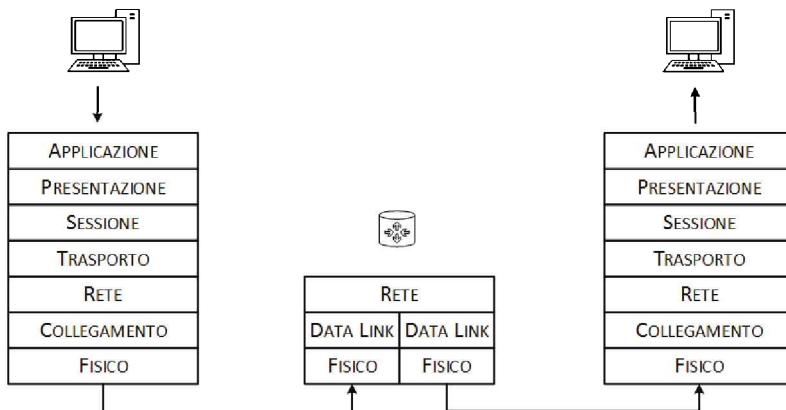


Figura 4.5: Architettura protocollare nodo sorgente, nodo di transito e nodo destinazione

non sono attivate negli apparati di rete di transito). Viceversa, i livelli inferiori sono attivati in tutti gli apparati di rete interessati al collegamento ed operano nella modalità detta link-to-link (L2L). Anche in questo caso i pari livello di apparati connessi sono in comunicazione virtuale tra loro. Il collegamento fisico effettivo è realizzato solo attraverso il supporto del canale di comunicazione.

Come anticipato, non tutti i livelli sono implementati in tutti i nodi. Nei nodi di transito, come è mostrato in figura 4.5, sono attivi solo i livelli di rete poiché le funzionalità proprie dei livelli di utente non sono necessarie. Dunque nei nodi di transito risultano attivi:

- *livello fisico* : i nodi di transito svolgono la funzione di ripetitore (amplificano/rigenerano il segnale ricevuto per disaccoppiare o limitare gli effetti dei disturbi di canale sull'integrità dell'informazione) e consentono anche l'interconnessione di segmenti di linea non omogenei (trasduzione del formato dei segnali trasmessi es. da elettrico ad ottico);
- *livello collegamento* : per effettuare controlli di affidabilità sull'informazione ricevuta evitando di ripetere flussi informativi affetti in maniera irrimediabile da errori;
- *livello rete*: per gestire l'inoltro del flusso informativo nella rete (routing) consentendo, inoltre, di individuare percorsi alternativi nel caso di guasti di linea o fuori servizio di apparati.

In figura 4.6 è mostrato come avviene il passaggio dell'informazione tra livelli. La tecnica utilizzata è quella dell'incapsulamento successivo: ogni livello, ad iniziare dal livello 6 (presentazione), inserisce in testa al messaggio ricevuto dal livello sovrastante un *header*. Gli header sono informazioni di controllo che un livello include nel messaggio, per consentire la comunicare con il suo pari livello nella pila di destinazione. L'unica eccezione viene effettuata a livello 2 (data link)

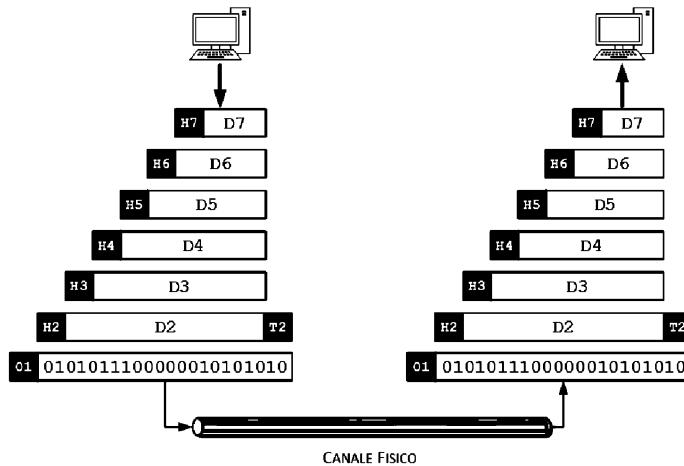


Figura 4.6: Tecnica dell'incapsulamento successivo secondo ISO/OSI

layer) in cui l'informazione di controllo viene posta sia in testa al messaggio (H2) che in coda (T2). Appena il messaggio arriva al destinatario, ogni livello interpreta le informazioni contenute nell'header di sua competenza che contengono le specifiche delle operazioni richieste dal pari livello con cui è in comunicazione logica. Successivamente si provvede ad eliminare la parte di header già utilizzata e a trasferire il pacchetto così creato al livello superiore che opererà con le stesse modalità.

Livello Fisico

(Physical Layer) È il livello più basso nell'architettura protocollare ISO/OSI. Si occupa della trasmissione (e ricezione) dei bit nel (dal) canale di comunicazione (mezzo fisico) con cui si interfaccia direttamente. Deve gestire la connessione e la trasmissione nel canale dell'informazione, ovvero gestisce l'inoltro dei dati intesi come singoli simboli, usando la tecnica di modulazione-demodulazione più adatta per migliorare la trasmissione.

Livello Collegamento

(Data Link) Questo livello svolge la funzione di trasferimento dati tra due nodi adiacenti. Le unità informative che vengono trasferite a questo livello si chiamano *trame*. I compiti principali del data link layer sono:

- sovrintendere ad un corretto trasferimento di dati fra il mittente e il destinatario mascherando al livello superiore l'eventuale presenza di errori nel trasferimento dell'informazione;

- gestire l'accesso al mezzo fisico condiviso quando questa funzionalità è richiesta;
- gestire il framing, ovvero suddividere il flusso dati in pacchetti;
- gestire l'invio di messaggi di riscontro (acknowledgement) quanto il flusso informativo è relativo ad un servizio affidabile.

Livello di Rete

(Network Layer) Il compito principale del livello di rete è quello di sovrintendere al trasferimento di informazioni lungo il percorso tra mittente e destinatario instaurando e rilasciando le connessioni logiche. L'instradamento dei pacchetti (routing) di uno stesso flusso verso il destinatario finale avviene tipicamente mediante l'interpretazione degli indirizzi logici in accordo a metodologie che possono essere statiche (cioè una volta definite rimangono valide su intervalli di tempo ragionevolmente lunghi) o dinamiche (cioè in gradi di aggiornarsi con una adeguata frequenza temporale). Compiti del livello rete sono anche:

- controllare il numero di pacchetti che va ad interessare uno stesso collegamento (link) o nodo al fine di prevenirne la congestione (colli di bottiglia);
- consentire l'interconnessione (internetworking) tra reti eterogenee.

Infine, si deve sottolineare che questo livello trova una implementazione semplificata quando l'inoltro dell'informazione avviene in modalità broadcast (cioè verso tutti gli utenti).

Livello di Trasporto

(Transport Layer) Questo livello si interfaccia direttamente con il pari livello di destinazione e quindi gestisce il trasferimento dati su base E2E. Permette di rendere compatibile la modalità connection oriented in reti che non lo supportano (livelli inferiori). Questo livello è il responsabile della segmentazione dell'informazione, cioè divide il flusso informativo ricevuto dal livello superiore in unità più piccole ogniqualvolta è necessario per garantire la compatibilità con i livelli sottostanti. Il livello di trasporto, al nodo sorgente, marca i pacchetti secondo il loro ordine di generazione. Conseguentemente, il livello di trasporto del nodo destinazione ricostruisce la giusta sequenza del flusso generato mediante l'uso di buffer e ripristina quindi il formato originale del flusso informativo prima di trasferirlo al livello superiore.

Livello di Sessione

(Session Layer) Consente a utenti diversi di realizzare una sessione di colloquio, fornendo i servizi necessari per organizzare e sincronizzare il dialogo, instaurando, mantenendo e abbattendo il collegamento. Ha il compito di:

- aprire un collegamento, effettuando l'operazione di LOGIN con un server remoto;
- sovrintendere al trasferimento dell'informazione, cioè controllare che il flusso informativo sia corretto;
- chiudere il collegamento, effettuando l'operazione di LOGOUT con il server remoto.

Livello di Presentazione

(Presentation Layer) Il livello di presentazione consente di far lavorare applicazioni che utilizzano i dati secondo formati differenti in termini sia di sintassi che di semantica. Le sue funzioni base sono la compressione dei dati per aumentare l'efficienza della rete (*compression*), la traduzione della sintassi (*translation*), la codifica dei dati per rendere il messaggio più sicuro (*encryption*) e la sicurezza dei dati mediante l'uso di password (*security*).

Livello Applicazione

(Application Layer) Consente la cooperazione tra utenti dell'ambiente OSI, sia-no essi processi applicativi o utenti finali fornendo le funzioni che caratterizzano un qualsiasi servizio che richiede un supporto di rete per essere implementato. Il livello Applicazione ha il compito di identificare e autenticare gli utenti che richiedono di colloquiare e di fornire le risorse richieste dall'utente. Esempi tipici di servizi offerti dal livello applicazione sono : HTTP (Hypertext Transfer Protocol) che è alla base del World Wide Web (Tanembaum'2011 in 4.10), posta elettronica, notizie, ecc..

4.3 Architetture Proprietarie

Prima dello standard ISO/OSI erano in vigore diverse architetture proprietarie, le due più famose sono la System Network Architecture (SNA) dell'IBM e la Digital Network Architecture (DNA) della Digital (Gai'1995, Halsall'1996 in 4.10). Essendo costruite specificatamente per poter operare con dispositivi di uno stesso costruttore presentano una struttura semplificata rispetto al modello ISO/OSI. Questa semplificazione si evidenzia soprattutto ai livelli superiori.

La rete SNA fu creata nel 1974. È uno stack protocollare completo per l'interconnessione di computer e le loro risorse ed è ancora largamente utilizzata per gestire transazioni finanziarie ed in molte agenzie governative (USA). Per questo motivo l'IBM sta ancora fornendo supporto al suo mantenimento ed adeguamento.

La DNA è basata sull'impiego di prodotti hardware e software complessivamente indicati come famiglia DECnet. La tecnologia DECnet è nata nel 1975 come mezzo per far comunicare tra loro calcolatori di tipo PDP-11 e si è evoluta attraverso versioni successive dette fasi. La rete DECnet è stata sviluppata avendo come obiettivo principale quello di realizzare una rete di calcolatori paritetici

(peer) in maniera che possano comunicare direttamente tra di loro. Esistono versioni (fasi) di DECnet che la rendono compatibile con apparati in standard OSI e con i più diffusi apparati in standard TCP/IP.

4.4 Modello TCP/IP

La suite protocollare TCP/IP (*Transmission Control Protocol / Internet Protocol*) è la base di Internet cioè della rete di comunicazione al giorno d'oggi più pervasiva, utilizzata e conosciuta. Internet è la contrazione della locuzione inglese interconnected networks, ovvero "reti interconnesse" (o rete di reti).

Un po' di storia

Internet prende forma da una rete di computer costituita nel settembre del 1969 negli USA dall'agenzia ARPA (Advanced Research Projects Agency), ARPANET. Nel 1957 l'Unione Sovietica prese il sopravvento nella corsa alla conquista dello spazio dopo il lancio in orbita del primo satellite Sputnik. In conseguenza di questo, il Dipartimento della Difesa degli Stati Uniti, per dare un grosso impulso alla ricerca scientifica e tecnologica, fondò nel 1958 l'agenzia ARPA. Quando la NASA subentrò all'ARPA nella gestione dei programmi spaziali, essa assunse il controllo di tutte le ricerche scientifiche a lungo termine in campo militare. Verso il 1965 l'ARPA aveva diversi computer sparsi in varie sedi e scambiare file fra loro era quasi impossibile, per questo, l'anno successivo l'ARPA ottenne uno consistente stanziamento per lo sviluppo del progetto ARPANET. ARPANET venne pianificato e realizzato dall'IPTO (Information Processing Techniques Office), un dipartimento gestito dal MIT (Massachusetts Institute of Technology) di Boston. ARPANET si basò su una tecnologia rivoluzionaria: la commutazione di pacchetto. La terza guerra mondiale incombeva sul mondo e, quindi, i ricercatori e gli ingegneri puntavano alla realizzazione di una rete efficiente, veloce ed affidabile e con l'obiettivo di essere il più possibile resiliente nei confronti di attacchi esterni. Nell'ottobre 1969 Leonard Kleinrock, fu incaricato di creare il primo collegamento telefonico fra l'University of California, Los Angeles (UCLA) e lo Stanford Research Institute, che furono così i primi due nodi di Internet (la prima applicazione fu una sessione Telnet). In seguito furono collegati le università di Santa Barbara e dello Utah, la BBN (Bolt, Beranek e Newman, una società di ingegneria acustica di Boston), il MIT, la Rand Corporation, la System Development Corporation e Harvard. Un ulteriore passo nello sviluppo di ARPANET fu quello di collegarla ad altre reti pre-esistenti, PRNET e SATNET, reti gestite sempre dall'agenzia ARPA. Alla fine del 1972 ARPANET aveva 37 nodi connessi. Nell'anno successivo fu definita la suite protocollare su cui si sarebbe basata ARPANET. Fu da prima definito un programma di ricerca finalizzato alla definizione di un Protocollo di Controllo Trasmissione (TCP) a cui fece seguito un ulteriore programma di ricerca rivolto alla definizione di un protocollo di rete che consentisse di interfacciare reti diverse (IP), definendo quindi la suite protocollare su cui ancora oggi opera Internet, la suite TCP/IP. Agli inizi degli anni

'80 il Dipartimento della Difesa statunitense, preoccupato per possibili vulnerabilità della rete di reti, creò MILNET, per scopi unicamente militari. ARPANET divenne così una rete esclusivamente dedicata alla ricerca. Parallelamente in Europa, sempre agli inizi degli anni '80, fu attivata la migrazione verso il protocollo TCP/IP. La Cisco Systems, venne incaricata dal CERN (Centre Européen pour la Recherche Nucléaire, Centro Europeo per la Ricerca Nucleare) di sviluppare la parte europea di Internet. La diffusione popolare di Internet avvenne solo però agli inizi degli anni '90 con lo sviluppo del World Wide Web, un sistema per la condivisione di informazioni in ipertesto. L'organismo internazionale che si occupa dello sviluppo di Internet è la Internet Engineering Task Force (IETF): un organismo aperto al quale chiunque può aderire.

4.5 Suite Protocollare TCP/IP

Come l'architettura ISO/OSI, Internet si basa sulla stratificazione della pila protocolle ma, a differenza della pila ISO/OSI, prevede solo quattro livelli: livello applicativo (*application layer*), livello di trasporto (*transport layer*), livello internet (*internet layer*) e il livello di accesso alla rete (*host to network layer*). La suite di protocolli TCP/IP, essendo stata sviluppata quando il modello OSI non era ancora stato individuato come standard di riferimento ed è quindi ragionevole attendersi delle differenze funzionali tra le due architetture. Si nota, ad esempio, la mancanza dei livelli fisico e collegamento nella suite protocolle TCP/IP, dove le funzioni di competenza sono gestite attraverso uno strato di accesso alla rete (Host-To-Network) che, in accordo con il paradigma proprio della rete Internet che la classifica come una rete di reti (Forouzan'2007, Kurose'2013, Tanenbaum'2011, Comer'2006 in 4.10), deve poter operare con realizzazione di questi livelli diverse tra loro. In figura 4.7 viene mostrata la suite protocolle TPI/IP nel suo dettaglio.



Figura 4.7: Suite protocollare TCP/IP

4.5.1 Livello Host to Network

Il livello più basso nella pila TCP/IP è il livello Host to Network (Accesso alla Rete). Questo livello ha il solo scopo di mascherare ai livelli superiori le caratte-

ristiche fisiche del mezzo trasmittivo utilizzato per trasferire l'informazione e di rendere compatibile la pila protocollare TCP/IP con differenti tipologie di rete.

4.5.2 Livello Internet

Abbreviato anche come livello IP, ha il compito di consentire lo scambio di pacchetti dati tra nodi di rete connessi attraverso diverse tipologie di rete. Consente, dunque, di far cooperare reti remote tra di loro. Sostanzialmente ha le funzionalità tipiche di un livello di rete di ISO/OSI. Questo livello ha pertanto il compito del controllo della congestione della rete e di definire le politiche d'instradamento più adeguate (routing) secondo la modalità connectionless. Il protocollo IP trasporta i dati in pacchetti chiamati *datagram*, in maniera indipendente tra di loro e senza controllo riguardo la loro possibile perdita o duplicazione. Al momento della stesura di questo testo è diffusa la versione 4 del protocollo IP, detta IPv4, anche se è in fase di completamento (e sperimentazione) la versione 6. Le motivazioni che hanno spinto alla realizzazione della versione 6 sono principalmente dovute all'esaurimento degli indirizzi logici di rete e a una più stringente necessità di garantire la riservatezza delle comunicazioni. In questa fase di transizione si è venuto a creare un problema di migrazione dai vecchi apparati di rete che usano IPv4 ai nuovi che usano IPv6: i nuovi sistemi sono retrocompatibili, ossia sono in grado d'inviare, instradare e ricevere datagrammi IPv4 mentre i sistemi IPv4 preesistenti non sono compatibili con più recenti apparati IPv6. Per risolvere questo problema sono stati proposti, come illustrato in RFC 2893, due approcci:

- *Dual Stack*: tale tecnica vede l'implementazione in un nodo sia del protocollo IPv4 sia IPv6. In questo modo il nodo è quindi capace di inviare e ricevere i datagrammi in entrambi i formati. Un tale nodo, inoltre, deve disporre di indirizzi sia IPv4 che IPv6;
- *Tunneling*: questa tecnica viene adoperata quando due nodi IPv6 si devono scambiare un datagramma e tale messaggio deve attraversare una porzione di rete costituita da dei nodi che supportano solo il protocollo IPv4. Il nodo di ingresso del tunnel IPv4 aggiunge in testa al datagramma l'header IPv4. In questo modo il datagramma risulta in un formato comprensibile per i nodi intermedi che sono quindi in grado di gestirne l'instradamento fino all'uscita della porzione di rete IPv4. Il nodo di uscita del tunnel elimina l'header IPv4 e gestisce l'instradamento successivo del datagramma sulla base del suo indirizzo IPv6 fino alla destinazione finale. Il tunneling è una tecnica frequentemente utilizzata nella presente fase di transizione da IPv4 a IPv6. La realizzazione di un tunnel IPv4 è illustrata in figura 4.8.

4.5.3 Internet Protocol version 4

L'Internet Protocol version 4 è specificato in RFC 791 e rappresenta la quarta revisione dell'Internet Protocol pubblicata da IETF nel settembre 1981.

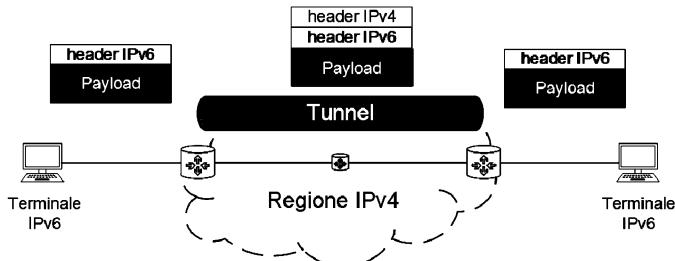


Figura 4.8: Tunneling

Prima di trattare IPv4 è bene specificare che il livello IP comprende, oltre al protocollo IP , da cui prende il nome, anche altri protocolli con finalità specifiche come l'Internet Control Message Protocol (ICMP) per informare riguardo l'indisponibilità di un servizio o la raggiungibilità di un nodo (Halsall'2005 in 4.10).

L'header IPv4 è formato da 13 campi, come mostrato in figura 4.9 ed è lungo 20 byte (160 bit) campo opzioni escluso. I vari campi, per i quali la lunghezza in bit è indicata in figura 4.9, indicano:

- *version*: indica la versione del protocollo IP (in questo caso avrà valore quattro);
- *IHL*: indica la lunghezza in byte della testata e quindi 'inizio dei dati nel datagramma';
- *type of service*: indica il tipo di dati che trasporta il relativo datagramma. A tipi di servizi differenti corrispondono trattamenti differenti all'interno della rete;
- *total length*: indica la lunghezza totale, espressa in byte, del datagramma (comprensivo dell'header, degli eventuali campi opzioni e del payload). Poiché questo campo è lungo 16 bit, si ha che il datagramma può essere al massimo $2^{16} - 1 = 65535$ byte (comprensivi della testata);
- *identification*: è un identificativo inserito dal mittente nei frammenti (vedi di seguito) di un datagramma di dimensioni superiori a quelle consentite. Questa etichetta (uguale per tutti i frammenti di uno stesso datagramma) viene utilizzata al nodo destinazione per ripristinare (assemblaggio) il formato originale datagramma;
- *flags*: usati come controllo per annunciare e gestire la frammentazione di un datagramma;
- *fragment offset*: anche questo campo è riferito ad indicazioni funzionali relative alla fase di ripristino di un datagramma frammentato nel suo formato originale;

Version (4 bit)	TTL (4 bit)	Type of Service (8 bit)	Total Length (16 bit)	
Identification (16 bit)		Flags (3 bit)	Fragment Offset (13 bit)	
Time To Live (8 bit)	Protocol (8 bit)	Header Checksum (16 bit)		
Source Address (32 bit)				
Destination Address (32 bit)				
Options ...			Padding	

Figura 4.9: Header IPv4

- *time to live*: È un contatore a decremento, quando raggiunge lo zero il corrispondente datagramma non viene più ripetuto e quindi viene eliminato dalla rete. Ogni volta che il datagramma effettua un hop (ovvero un salto da un router ad un altro) nella rete il valore di questo campo viene decrementato di uno. L'utilizzo di questo contatore consente di evitare che i datagrammi siano ripetuti permanentemente dai nodi della rete anche quando sono giunti alla loro destinazione finale;
- *protocol*: indica il tipo di protocollo usato a livello di trasporto;
- *header checksum*: serve ai router per verificare che nell'header non vi siano errori;
- *source address*: indirizzo IP del mittente del messaggio;
- *destination address*: indirizzo IP del destinatario;
- *options*: eventuali opzioni aggiuntive che riguardano particolari datagrammi (comunicazioni riservate, rotta da seguire verso la destinazione finale, ecc.).

IPv4 introduce la cosiddetta **frammentazione** del datagramma. Ogni livello data link ha una massima quantità di dati che può trasportare, chiamata *unità massima di trasmissione* (MTU). Può quindi accadere che un datagramma IP non possa essere trasportato per intero lungo un collegamento poiché eccede in lunghezza quanto previsto dal livello collegamento. Per ovviare a questo problema il datagramma originario IP viene frammentato in due o più datagrammi IP i quali poi saranno ricombinati per ripristinare il formato originale dal destinatario mediante i tre campi dell'header visti in precedenza (identification, flag, fragment offset).

Il protocollo IP richiede che tutte le interfacce di rete abbiano un proprio indirizzo IP, questo vuol dire che un indirizzo IP non identifica in maniera univoca il dispositivo ma solo la sua interfaccia con il collegamento fisico vero e proprio. Gli indirizzi IPv4 sono lunghi 32 bit (4 byte), in totale sono quindi oltre 4 miliardi. Tali indirizzi sono espressi nella notazione *decimale puntata*, in cui ciascun byte

	valore decimale primo Byte	valore binario primo Byte	uso
Classe A	0-127	0	Unicast
Classe B	128-191	10	Unicast
Classe C	192-223	110	Unicast
Classe D	224-239	1110	Multicast
Classe E	240-255	1111	Usi futuri

Tabella 4.1: Classi di Indirizzi IPv4

dell'indirizzo viene espresso in forma decimale e separato, con un punto, dagli altri byte dell'indirizzo, come ad esempio 182.45.136.1. Ogni interfaccia ha un indirizzo univoco all'interno della rete che non può essere scelto in modo arbitrario. Inizialmente era diviso in due parti: i primi 3 byte (quelli più significativi) identificavano la rete mentre i restanti identificavano l'interfaccia. È facile notare che in una rete generica era possibile indirizzare solo 256 terminali e questo risultò ben presto inefficiente. Per ovviare a questo problema fu introdotto la cosiddetta *classful networking*, un sistema di definizione degli indirizzi basato inizialmente su tre classi, successivamente estese a cinque. Le classi A,B,C usano lunghezze differenti di byte per identificare la rete (netid) e il dispositivo connesso (hostid), la classe D identifica gli indirizzi multicast mentre la classe E è stata riservata per usi futuri. Ad esempio, nella classe A era previsto che il primo bit fosse sempre 0, i sette bit successivi identificavano la rete e i rimanenti tre byte erano usati per identificare le interfacce. Quindi era possibile avere 128 reti univoche e in ognuna delle reti era possibile indirizzare oltre 16 milioni di interfacce. Le classi sono mostrate in dettaglio nella tabella 4.1. L'indirizzamento con classi è stato rapidamente abbandonato poiché comportava un grosso spreco di indirizzi IPv4 (Kurose'2013, Halsall'2005, Tanenbaum'2011 in 4.10) quando, ad esempio, ad uno stesso router facevano capo più reti locali (LAN) distinte. Nel 1993, con la pubblicazione del RFC 1517, questo sistema fu sostituito con una nuova notazione, la Classless Inter-Domain Routing (CIDR). La notazione adoperata è del tipo a.b.c.d/y. Il numero y è chiamato **prefisso di rete** (*network prefix*) e può assumere valore intero compreso fra 1 e 31 ed indica che i primi y bit costituiscono l'identificativo della rete IP; inoltre la notazione /y definisce la lunghezza della cosiddetta **maschera di sottorete** (*subnet mask*). La subnet mask consiste in una sequenza di 32 bit dove i primi y bit sono settati tutti a 1 e i rimanenti 32-y bit sono posti tutti a zero. Ad esempio, con l'indirizzo 185.165.204.96 /16 avremmo la maschera di sottorete 255.255.0.0. In conclusione la maschera indica quanti bit sono stati riservati per l'indirizzo di rete (y) e quanti bit sono usati per identificare l'host all'interno della rete (32 - y).

Per capire meglio come avviene l'indirizzamento nelle reti IPv4, si faccia riferimento alla figura 4.10. La figura mostra un router con tre interfacce attraverso le quali connette complessivamente otto differenti terminali. Come si nota, i terminali connessi a una interfaccia del router hanno un indirizzo IP che coincide

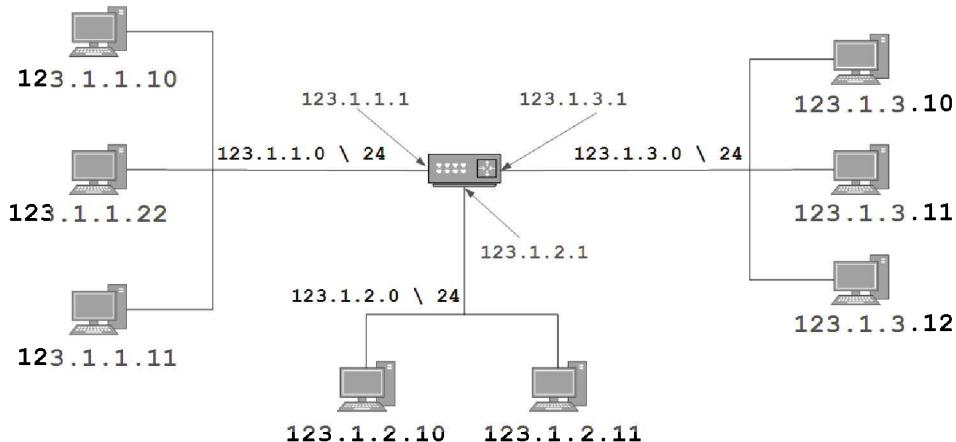


Figura 4.10: Rete IPv4

per i primi 24 bit (secondo la terminologia TCP/IP questa è una **sottorete** come indicato in RFC 950). Per semplificare i termini, le sottoreti vengono generalmente chiamate reti IP. Ritornando all'esempio, i primi 24 bit di ogni indirizzo identificano la rete IP mentre i rimanenti 8 bit identificano in maniera univoca l'host all'interno della rete. Ogni host dunque ha una maschera di sottorete formata da 24 bit posti a uno e 8 bit posti a zero, in particolare nella notazione decimale puntata: 255.255.255.0

Vi sono alcuni indirizzi IPv4 che hanno particolari usi, tra questi citiamo:

- indirizzi che hanno visibilità solo all'interno di una rete privata. Questi indirizzi sono utilizzati privatamente all'interno di una sotto-rete e pertanto non sono visibili (e raggiungibili) dalla rete esterna IP. La particolarità di questi indirizzi è che sono unici solo all'interno della sotto-rete che li adopera, ma due sotto-reti distinte possono tranquillamente adoperare gli stessi indirizzi privati. Sono divisi in tre classi e sono 10.0.0.0 /8, 172.16.0.0 /20, 192.168.0.0 /16;
- indirizzo dell'interfaccia di loopback: identifica il localhost, ovvero la macchina locale. I programmi possono utilizzare questo indirizzo per stabilire connessioni tra di loro sulla stessa macchina anche quando questa ha delle interfacce attive. L'utilizzo dell'interfaccia di loopback permette di testare il funzionamento dei programmi senza utilizzare realmente la rete. I pacchetti in uscita da questa interfaccia non vengono inoltrati nella rete ma rientrano nell'host che li ha generati. L'indirizzo è 127.0.0.0 /8, generalmente viene usato 127.0.0.1;
- indirizzo di broadcast: tutti i bit che identificano l'host sono posti a 1. Tale indirizzo rappresenta tutti i nodi della rete. Ad esempio, inviare un pacchetto all'indirizzo 142.108.5.255 equivale a mandare un pacchetto a tutti

gli host presenti nella rete 142.108.5. Esiste anche un indirizzo di broadcast di rete globale: ed è identificato dall'avere tutti i 32 bit dell'indirizzo IPv4 settati a 1, in notazione decimale puntata 255.255.255.255. Inviare un pacchetto a questo indirizzo vuol dire inoltrarlo verso tutti gli host della rete corrente.

Esiste un'autorità a livello mondiale che ha la responsabilità di gestire l'assegnazione degli indirizzi: l'Internet Corporation for Assigned Names and Numbers (ICANN). L'ICANN non assegna direttamente gli indirizzi alle singole organizzazioni, ma riserva grandi blocchi agli Internet Service Provider (ISP), i quali poi a loro volta dividono i blocchi in sotto-blocchi in maniera che i propri clienti li possano assegnare ai propri dispositivi. Esistono due metodi per assegnare un indirizzo IP ad un host:

- configurazione manuale: l'amministratore della rete assegna manualmente e permanentemente ad ogni host della rete un indirizzo IP univoco;
- configurazione dinamica: avviene tramite il **Dynamic Host Configuration Protocol**. Il server DHCP, vedi RFC 2131, permette ad un'host di ottenere, oltre che un indirizzo IP temporaneo, anche altre informazioni quali la sua maschera di sottorete, e l'indirizzo IP del router di primo hop (generalmente chiamato gateway di default). Il DHCP, appena un terminale entra nella rete, gli assegna un indirizzo IP temporaneo disponibile, ovvero alloca per l'host un indirizzo non utilizzato da nessun altro dispositivo della rete. Non appena un terminale si disconnette dalla rete, il suo indirizzo IP torna disponibile ed eventualmente viene ri-assegnato ad un altro host che ha effettuato l'accesso in quell'istante.

Dunque il DHCP esenta l'utente più inesperto alla configurazione manuale di una rete privata.

Ben presto, con l'aumentare dei dispositivi connessi ad internet, gli indirizzi stavano rapidamente terminando, fu così che con la pubblicazione del RFC 1631 nel 1994 venne introdotto il Network Address Translation (NAT). Lo scopo principale del NAT era quello di arginare il problema della scarsità degli indirizzi IPv4 fin quando IPv6 non avesse preso piede come protocollo di rete di riferimento. Con questa tecnica, non ben vista dai puristi della rete TCP/IP poiché il NAT non è conforme ai dettami che prevedono che la connessione end-to-end debba essere trasparente ed i pacchetti non modificati, un'utente può utilizzare, nella propria sotto-rete, un numero estremamente grande di indirizzi privati e un numero molto ristretto di indirizzi IP visibili dalla rete globale. Nel 2000 l'IETF emana l'RFC 2776 con cui evolve il NAT nel Network Address Translation-Protocol Translation (NAT-PT).

L'interconnessione tra rete privata e rete IP è, come mostrato in figura 4.11, gestita attraverso un router che utilizza un software NAT.

Quando i pacchetti attraversano il router NAT, esso sostituisce l'indirizzo sorgente (che è un indirizzo privato) con il proprio indirizzo pubblico. Quando, invece, i pacchetti arrivano al router NAT, esso sostituisce l'indirizzo di destinazione

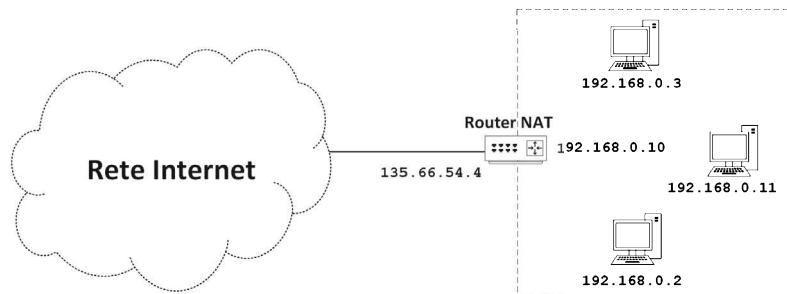


Figura 4.11: tecnica NAT

(che è il proprio indirizzo pubblico), con l'indirizzo privato del vero destinatario del messaggio. In ricezione, il NAT effettua il cambio di indirizzo di destinazione pubblico/privato grazie all'uso della tabella di traduzione: essa nella sua forma più semplice ha solo due colonne. In una viene memorizzato l'indirizzo privato del mittente e nell'altra l'indirizzo di destinazione. Quando un pacchetto passa dal router, esso, oltre a modificare l'indirizzo sorgente, inserisce nella tabella l'indirizzo privato mittente con l'indirizzo pubblico di destinazione, cosicché, non appena arriva un pacchetto, in base all'indirizzo mittente, sa a chi inoltrare il messaggio. Si nota subito che l'utilizzo di questa tecnica funziona solo se la comunicazione è iniziata da un host appartenente ad una rete privata: il NAT ha una corrispondenza biunivoca indirizzo privato/indirizzo pubblico solo se il primo pacchetto è stato inviato da un terminale all'interno della rete privata. Il tipo di comunicazione permessa è quindi di tipo client-server, dove l'utente all'interno della rete privata contatta un server esterno. Un host che si trova all'interno di una rete privata, dunque, non può offrire un servizio server, in quanto il suo indirizzo IP univoco non è visibile dall'esterno.

Il problema nella strategia precedente si verifica quando due host che si trovano all'interno della stessa rete vogliono comunicare con lo stesso server. In questo caso, nella tabella di traduzione del NAT si crea un'ambiguità, poiché due indirizzi interni hanno come uscita lo stesso indirizzo e al momento della ricezione del pacchetto, il router NAT non sa a chi consegnarlo. Un modo per risolvere questo problema è quello di utilizzare più indirizzi pubblici IP. In questo modo si possono gestire un numero di connessioni verso lo stesso server pari al numero di indirizzi pubblici che il router NAT dispone. Ma se da una parte questa soluzione risolve le connessioni multiple verso lo stesso server dall'altro lato non risolve il problema per cui il NAT è stato introdotto, ovvero la scarsità degli indirizzi IP disponibili.

Una soluzione più flessibile che è stata trovata è quella di utilizzare, insieme agli indirizzi IP, anche il **numero di porta**. Il numero di porta è un concetto del livello di trasporto e serve per identificare il processo di destinazione non appena il pacchetto arriva all'host destinatario. Quindi se l'indirizzo IP serve per identificare il mittente ed il destinatario di un pacchetto, il numero di porta di destinazione serve per identificare processo destinatario sul relativo host; da

Indirizzo locale	Porta locale	Indirizzo esterno	Porta esterna	Protocollo
192.168.0.11	1600	18.18.18.8	80	TCP
192.168.0.11	1601	5.6.1.2	88	UDP
192.168.0.3	1602	18.18.18.8	80	TCP
...

Tabella 4.2: Esempio di tabella NAT

notare che la porta sorgente viene assegnata in maniera casuale dal livello di trasporto: questa porta si chiama *effimero*, mentre le porte dei processi di destinazione, in quanto porte che devono essere conosciute a priori si chiamano *porte ben note*. I pacchetti appartenenti ad una connessione saranno quindi identificati dalla quadrupla { *indirizzo IP sorgente*, *indirizzo IP destinazione*, *porta sorgente*, *porta di destinazione* }. In TCP e UDP sono stati riservati 16 bit per identificare il numero di porta, quindi si hanno $2^{16} = 65536$ possibili porte. L'operazione di impegnare una porta TCP o UDP da parte di un processo è detta bind. Per maggiori informazioni sull'assegnazione delle porte si può fare riferimento al sito internet ufficiale della IANA e al documento RFC 1349.

L'insieme numero di porta del processo e indirizzo IP del terminale viene chiamata **socket**.

Tramite l'utilizzo congiunto delle porte e degli indirizzi IP è stata trovata una soluzione all'uso del NAT. Ovviamente adesso all'interno della tabella di traduzione devono essere aggiunte le porte sorgenti e le porte di destinazione e il protocollo di trasporto adoperato per quella sessione.

Anche in questo caso si rende necessario l'uso univoco delle porte interne alla rete privata: ogni quintupla porta, indirizzo e protocollo usato deve identificare in maniera univoca un host all'interno della rete. Un esempio di tabella NAT è riportata nella tabella 4.2.

Il 3 febbraio 2011 l'organismo internazionale preposto all'assegnazione degli indirizzi di rete ha assegnato definitivamente gli ultimi blocchi di indirizzi IPv4.

4.5.4 Internet Protocol versione 6

L'IPv6 (vedi RFC 2460), è stato proposto per risolvere alcune criticità della versione IPv4 e per introdurre nuove funzionalità. In particolare, IPv6 può essere considerato come un aggiornamento del protocollo IP che, nella versione IPv4, è divenuto il protocollo di rete più usato al mondo. IPv6 prevede un MTU minimo di 1280 byte. Ogni nodo deve implementare una procedura di MTU Path Discovery e se è richiesto di inviare pacchetti più grandi della massima MTU consentita a livello collegamento, si deve utilizzare i fragment header (header con il campo next-header di valore 44). IPv6 prevede un supporto nativo alla sicurezza, grazie all'implementazione di IPSec e alla presenza dell'Authentication Header, il quale permette di verificare l'identità del mittente e di evidenziare eventuali manomissioni del datagramma e l'Encapsulating Security Payload, mediante il quale solo

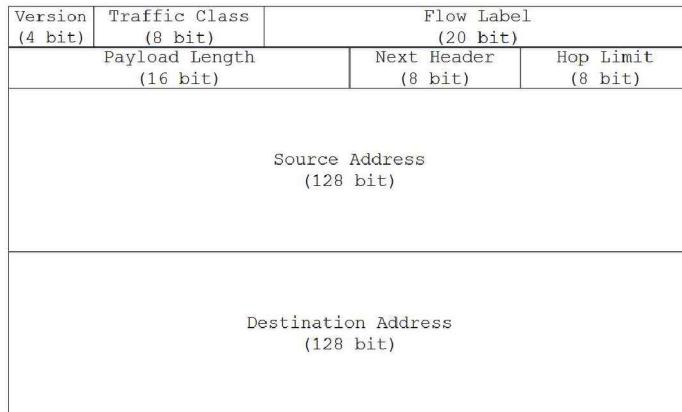


Figura 4.12: Header IPv6

il destinatario autorizzato è messo in grado di accedere al contenuto informativo del datagramma.

La differenza sostanziale con IPv4 sta nel campo destinato alla specifica del destinatario dei datagrammi (indirizzamento). IPv6 prevede un campo di 128 bit (16 byte) per gli indirizzi IP, per cui vi sono 2^{128} (circa 3.4×10^{38}) combinazioni diverse di indirizzi possibili, mentre IPv4 prevede un campo di soli 32 bit, per cui riesce a garantire soltanto 2^{32} (circa 4×10^9) indirizzi diversi. Gli indirizzi IPv6 sono solitamente rappresentati come 8 gruppi di 4 cifre esadecimale (ovvero 8 parole di 16 bit ciascuna), ad esempio:

2407:0:ABCD:0:3FFE:3112:FOOD:CAFE

Un'altra grossa differenza con IPv4 è nell'header dei datagrammi. IPv4 prevede 13 campi, diversamente IPv6 li limita a 8, aumentando così la velocità di elaborazione del pacchetto da parte dei router. Oltre all'header vero e proprio, in IPv6 è previsto un blocco opzionale chiamato Extension Headers (viene usato solo quando richiesto) e, ovviamente, il campo payload. Nel header sono solo presenti informazioni di controllo mentre il payload è un datagramma di livello superiore. L'header è costituito da 320 bit, ovvero 40 Byte come mostrato in figura 4.12.

I campi previsti, la cui consistenza (in bit) è indicata in figura 4.12, sono:

- *version*: questo campo indica la versione del datagramma IP (ha valore sei), serve per distinguere i datagrammi IPv4 da quelli IPv6;
- *traffic class*: indica i diversi tipi di traffico nelle reti Differentiated Service (Kurose'2011 in 4.10), ha una funzione simile al campo *typy of service* di IPv4;
- *flow label*: è un campo, correlato al campo precedente, che viene utilizzato dal mittente per etichettare una flusso di datagrammi. Consente di garantire la qualità del servizio ad una specifica connessione;

- *payload length*: indica la lunghezza del payload (espresso in byte) escluso l'header IPv6 di lunghezza fissa 4 byte. La lunghezza massima del payload è 65535 (2^{16}) byte;
- *next header*: indica il tipo di intestazione presente dopo l'header IPv6. Esso può essere un'intestazione del tipo di protocollo del livello TCP oppure un'Extension Header per implementare funzionalità aggiuntive come la frammentazione che è consentita solo al nodo sorgente (non ai nodi di transito);
- *hop limit*: indica il numero massimo di salti (hop) che il pacchetto può avere nella rete. Corrisponde al Time To Live (TTL) di IPv4. Viene decrementato ogni volta che un pacchetto viene instradato nella rete da un router. Quando un router trova questo campo a zero, il pacchetto viene rifiutato e quindi eliminato dalla rete;
- *source address*: indica l'indirizzo IPv6 del mittente del pacchetto;
- *destination address*: indica l'indirizzo IPv6 del destinatario del pacchetto.

IPv6 introduce tre tipi di indirizzi e di indirizzamento come specificato in RFC 4291 e descritto in Tanembaum'2011, Kurose'2013 (vedi 4.10):

- *Multicast*: un indirizzo multicast corrisponde a più interfacce nella rete. Il mittente invia una sola copia del pacchetto con indirizzo multicast (il suo prefisso è FF0M:: con M che identifica la visibilità), sarà compito del multicast router inviare una copia del pacchetto ad ogni singolo nodo. L'indirizzamento multicast prende il posto del broadcast. Un'interfaccia può avere un qualsiasi numero di indirizzi multicast. La loro struttura è mostrata in figura 4.13. Flag indica se l'indirizzo multicast è temporaneo (valore 1) oppure permanente (valore 0). La visibilità (scope) di un indirizzo IPv6 multicast viene determinata in base al valore della quarta cifra esadecimale del gruppo più significativo (primo gruppo partendo da sinistra):

- 0: Riservato
- 1: Scope Node-Local
- 2: Scope Link-Local
- 3 e 4: Non Assegnato
- 5: Scope Site-Local
- 6 e 7: Non Assegnato
- 8: Scope Organization-Local
- 9, A, B, C, D: Non Assegnato
- E: Scope Globale
- F: Riservato

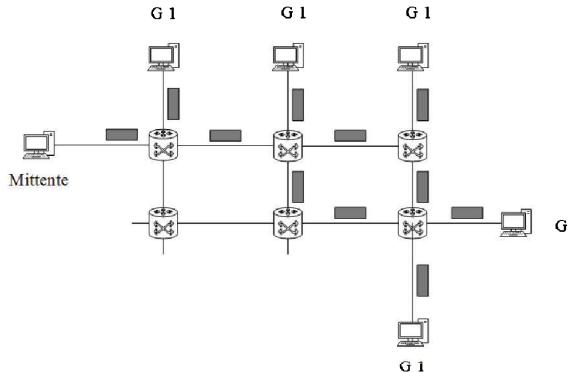


Figura 4.13: Indirizzamento Multicast

- *Unicast*: l'indirizzo unicast identifica una sola interfaccia nella rete, quindi è la modalità di instradamento per la quale un pacchetto è inviato ad un solo terminale della rete. L'indirizzo con visibilità globale è formato come mostrato in figura 4.14 ed è stato ratificato con l'RFC 3587. L'indirizzo unicast è stato pensato con una struttura gerarchica, in modo da permettere la massima aggregazione e di ridurre i problemi di scalabilità della rete. Il *Global Routing Prefix* è assegnato ad un Site (ovvero una rete amministrata da un unico gestore) ed è il suo spazio di indirizzamento, la *Subnet ID* identifica una sottorete all'interno del Site e, infine, *Interface ID* identifica un'interfaccia univoca di un'host. Tutti gli indirizzi unicast, ad eccezione di quelli che iniziano con il valore binario 000, devono avere Interface ID lunga 64 bit; essa viene ricavata o modificando l'indirizzo EUI-64 oppure modificando l'identificatore EUI-48 ovvero il MAC address di ogni scheda di rete. Nel primo caso basta invertire il settimo bit dell'identificatore (il cosiddetto bit Universal/Local) e quello che si ottiene inserirlo come Interface ID, nel secondo caso si deve inserire dopo i primi 24 bit del MAC address la sequenza 0xFFFF, inserire gli altri 24 bit e appena si ha la sequenza lunga 64 bit invertire il settimo bit, come nel caso precedente. Allo stato attuale sono stati previsti 48 bit per il Global Routing Prefix, 16 per la Subnet ID e 64 per la Interface ID. Gli indirizzi unicast con visibilità link-local, invece, sono indirizzi la cui visibilità è solo su collegamento link e la loro struttura è mostrata in figura 4.15. Questo tipo di indirizzo può essere usato solo per scambiare pacchetti fra nodi dello stesso link ed è il primo indirizzo fornito ad ogni nodo per iniziare le comunicazioni dato che viene automaticamente configurato su ogni interfaccia usando l'interface identifier. Il suo formato è: fe80:0:0:0:<interface identifier>

Gli indirizzi unicast con visibilità site-local sono usati soltanto fra nodi dello stesso sito e non possono essere usati fuori dal sito stesso. Questi indirizzi non vengono configurati di default. Questo è particolarmente utile quando abbiamo bisogno di indirizzamenti privati all'interno della stessa organiz-

Global Routing Prefix (n bit)	Subnet ID (64 - n bit)	Interface ID (64 bit)
----------------------------------	---------------------------	--------------------------

Figura 4.14: Indirizzo Global Unicast

1111111010 (10 bit)	000...000..0000...00 (54 bit)	Interface ID (64 bit)
------------------------	----------------------------------	--------------------------

Figura 4.15: Indirizzo Link-Local Unicast

zazione (es.: per indirizzare stampanti locali in rete). Il formato di questi indirizzi è: `fec0:0:0:<subnet id>:<interface identifier>`

- Anycast: è un indirizzo IP che corrisponde a più interfacce nella rete. Quando un pacchetto viene inviato ad un indirizzo anycast, la rete lo consegna al nodo (appartenente al gruppo anycast) più vicino al nodo mittente. È un tipo di indirizzamento utilizzato per distribuire il traffico ed aumentare l'affidabilità di specifici servizi.

Si noti che gli indirizzi vengono assegnati alle interfacce connesse alla rete, non ai singoli nodi. Poiché ciascuna interfaccia appartiene ad un singolo nodo, qualsiasi interfaccia di quel nodo con indirizzo unicast può essere utilizzato come un identificatore per il nodo. Ogni interfaccia deve avere almeno un indirizzo link-local unicast, ma può avere più indirizzi IPv6 di qualsiasi tipo (unicast, anycast, multicast) e visibilità. Gli indirizzi unicast con visibilità globale sono inutili per quelle interfacce che non vengono utilizzate come origine o destinazione nella rete. Il tipo specifico dell'indirizzo IPv6, dichiarato nei primi 8 bit del campo indirizzo stesso, ovvero dalle prime due cifre esadecimali del gruppo più significativo (es. FF corrisponde a 1111 1111 ed identifica un indirizzo multicast). Ci sono diverse forme per rappresentare un indirizzo IPv6, quello più usato è la rappresentazione CIDR. Come avviene in IPv4 si fa seguire un indirizzo dal simbolo / e dalla lunghezza del prefisso espressa in decimale. Questo rappresenta il numero di bit dell'indirizzo, a partire da quello più significativo, che compongono il prefisso. Esso è nella forma: `IPv6_Address / Prefix_Length`

In IPv6 il NAT non ha più senso di esistere, in quanto lo spazio di indirizzamento è praticamente illimitato e, in particolare, per quanto riguarda la funzione di mascheramento della rete privata, questa è sostituita dal *firewall* (vedi capitolo 15).

ICMPv6

Il protocollo ICMPv6, come specificato in RFC 4443, viene usato dai nodi per riportare errori riscontrati nel routing dei pacchetti nella rete, come diagnostica della rete stessa, risoluzione degli indirizzi di livello link, individuazione del router corretto oppure per autoconfigurare gli indirizzi IPv6. Il protocollo ICMPv6 è parte integrante del protocollo IPv6. Il suo pacchetto viene usato dal protocollo di

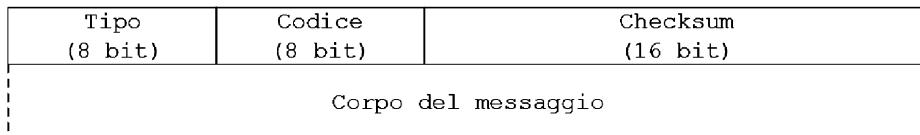


Figura 4.16: Pacchetto ICMPv6

Neighbor Discovery (vedi di seguito). L'header del protocollo ICMPv6 è preceduto da uno o più header IPv6 (con campo Next Header di valore 58). Il messaggio ICMPv6 ha la struttura mostrata in figura 4.16.

Il significato dei vari campi è:

- **Tipo:** indica che tipo di dati trasporta il messaggio. Per messaggi di errore assume valori da 0 a 127, per messaggi di informazione, invece, da 128 a 255.
- **Codice:** dipende dal campo precedente, e viene utilizzato come livello aggiuntivo di sicurezza.
- **Checksum:** viene usato per trovare errori nel pacchetto.

I messaggi ICMPv6 si dividono in due categorie: messaggi di errori e messaggi di informazione.

Di seguito sono riportati alcuni esempi:

- **Messaggi di errori:**
 - Tipo = 1: Destination Unreachable;
 - Tipo = 2: Packet Too Big;
 - Tipo = 3: Time Exceeded;
 - Tipo = 4: Parameter Problem;
 - Tipo = 100: Private Experimentation;
 - Tipo = 101: Private Experimentation;
 - Tipo = 127: Riservato per usi futuri.
- **Messaggi di informazioni:**
 - Tipo = 128: Echo Request;
 - Tipo = 129: Echo Reply;
 - Tipo = 200: Private Experimentation;
 - Tipo = 201: Private Experimentation;
 - Tipo = 255: Riservato per usi futuri.

I messaggi ICMPv6 per i protocolli di Neighbor Discovery

Il protocollo Neighbor Discovery, emanato nell'RFC 4861, è stato introdotto per risolvere alcuni problemi relativi all'interazione tra i nodi connessi allo stesso link. Definisce i meccanismi per risolvere i seguenti problemi:

- Router Discovery: serve per localizzare i router da parte degli host;
- Prefix Discovery: serve per trovare i prefissi degli indirizzi dei nodi connessi allo stesso link;
- Parameter Discovery : serve per conoscere i parametri (es. MTU o hop limit) della rete;
- Address Autoconfiguration: introduce il meccanismo di autoconfigurazione degli indirizzi delle interfacce in modo stateless;
- Address Resolution: serve a un nodo per determinare l'indirizzo link-layer di un nodo adiacente partendo solo dall'indirizzo IP;
- Next-Hop Determination: è un algoritmo che mappa l'indirizzo IP del destinatario, partendo dagli indirizzi dei vicini;
- Neighbor Unreachability Detection: serve per determinare quando un nodo non è più raggiungibile;
- Duplicate Address Detection: serve come controllo sugli indirizzi IPv6 già in uso;
- Redirect: i router possono informare i nodi della presenza di un router migliore per una specifica destinazione;
- Recursive DSN Server e DSN Search List: funzioni per la ricerca e l'assegnazione del DSN;

Il protocollo di ND, per propagare i suoi pacchetti, si basa sul protocollo ICMPv6 e sfrutta cinque tipi di pacchetti:

- Router Solicitation (RS): viene inviato quando un host (o un'interfaccia) si connette alla rete in modo da richiedere immediatamente un Router Advertise, senza aspettare l'intervallo successivo. Tali pacchetti vengono spediti all'indirizzo link-local multicast all-routers ($ff02::2$);
- Router Advertisement (RA): viene inviato periodicamente (oppure dopo una richiesta RS da parte di un nodo) dai router ai propri vicini. All'interno di questo pacchetto sono presenti i vari parametri della rete (come ad esempio gli indirizzi per i nodi, il valore dell'hop-limit, il valore dell' MTU ect.). I Router Advertisement sono spediti con visibilità link-local all'indirizzo multicast all-nodes ($ff02::1$);
- Neighbor Solicitation (NS): viene inviato dai nodi per determinare l'indirizzo link-layer dei vicini inviando contemporaneamente il proprio;

- Neighbor Advertisement (NA): viene inviato o come risposta a un NS oppure per avvisare i vicini del cambio del proprio indirizzo link-layer;
- Redicted: in questo caso i router possono informare i nodi della presenza di un router migliore per una specifica destinazione.

Gli indirizzi globali possono essere autoconfigurati una volta noto il prefisso dichiarato dai router e noto il proprio indirizzo fisico IEEE EUI-64.

4.5.5 Livello Trasporto

Questo livello ha il compito di rendere compatibile le esigenze di servizio con il livello Internet. Ha gli stessi scopi dell'analogo livello ISO/OSI. Il pacchetto generato da questo livello viene chiamato più propriamente **datagram**.

User Datagram Protocol

L'User Datagram Protocol (UDP) è stato standardizzato nell'agosto del 1980 con l'RFC 768 ed è il protocollo di trasporto senza connessione e inaffidabile. Tutti i pacchetti inviati con il protocollo UDP sono indipendenti gli uni dagli altri e ogni datagram (datagramma) potrebbe seguire un percorso diverso nella rete e giungere a destinazione in un ordine diverso rispetto a quello di generazione. È usato con servizi che non richiedono né il rispetto dell'ordinamento di generazione per i pacchetti, né la sicurezza della loro ricezione. UDP richiede poca interazione tra il mittente e il destinatario. In particolare, la fase di set-up della connessione viene eliminata e quindi viene limitato il tempo di latenza nell'iniziare il trasferimento dei dati verso il nodo destinazione. UDP viene adoperato con le applicazioni che non richiedono grosse iterazioni client-server e in cui sono tollerati possibili errori nel datagramma.

L'header UDP è mostrato in figura 4.17; esso ha una lunghezza fissa di 8 byte e i singoli campi hanno il seguente significato:

- *Numero porta sorgente*: 16 bit, specifica il numero di porta utilizzato dal processo mittente;
- *Numero porta destinatario*: 16 bit, specifica il numero di porta del processo di destinazione;
- *Lunghezza*: 16 bit, esprime in byte la lunghezza del campo dati che segue l'header UDP. Un datagram UDP può essere lungo al massimo $2^{16} = 65535$ byte;
- *Checksum*: 16 bit, viene adoperato come controllo degli errori del datagram.



Figura 4.17: Header UDP

Transmission Control Protocol

Il Transmission Control Protocol (TCP) è stato standardizzato nel gennaio del 1980 con l'RFC 761. È un protocollo di livello trasporto orientato alla connessione e affidabile. Prima di spedire i pacchetti, è compito del protocollo TCP creare una connessione virtuale tra mittente e destinatario che rimarrà attiva fino a che la connessione è in atto. È compito di TCP (al nodo destinazione) controllare l'integrità dei datagrammi ricevuti e il rispetto del loro ordine di generazione. Se un datagramma non viene ricevuto oppure è ricevuto con errori è compito di TCP provvedere alla richiesta di ritrasmissione del pacchetto. Poiché processi mittente e processo destinatario potrebbero non lavorare alla stessa velocità, TCP prevede l'uso di buffer per limitare la perdita di dati. Il buffer del processo mittente è diviso due aree, in una di queste sono memorizzati i datagrammi che sono stati spediti ma che ancora non hanno avuto riscontro di corretto invio mentre nell'altra vengono memorizzati i datagrammi che sono in attesa di essere spediti. Analogamente sul processo di destinazione è presente un secondo buffer dove verranno salvati i messaggi arrivati in attesa di essere prelevati ordinatamente dal processo.

TCP a differenza di UDP permette di trasferire grandi quantità di byte. Mentre UDP è limitato ad avere una dimensione massima confinata al datagramma IPv4 (per IPv6 questo non vale, poiché la versione 6 ha un limite minimo della dimensione del datagramma ma non un limite massimo), TCP permette la cosiddetta segmentazione dei dati: se i dati da spedire eccedono la capacità massima del pacchetto IPv4, TCP si preoccupa di spedire questo flusso di segmenti e di riassestarli appena giungono a destinazione. Per collegamenti interattivi, durante la configurazione del collegamento tra due dispositivi TCP viene definita la dimensione massima di un segmento. Questa viene stabilita in relazione alla necessità di evitare le ritrasmissioni e di non richiedere al livello IP la frammentazione dei datagrammi. La connessione virtuale che si viene a creare con il protocollo TCP è bidirezionale: si può spedire i dati in entrambe le direzioni secondo lo stesso percorso. Quando tutti i datagrammi sono stati trasferiti in entrambe le direzioni (vedi di seguito) la connessione (logica) viene chiusa. L'header TCP è mostrato in figura 4.18 ed è lungo 20 byte, ma può arrivare ad un massimo di 60 byte se sono presenti opzioni o byte di riempimento. I singoli campi, come indicato in Halsall'2005, Forouzan'2007 e Kurose'2013, (vedi paragrafo 4.10) hanno il seguente significato:

- *numero porta mittente*: campo da 16 bit, identifica il numero della porta del processo mittente;
- *numero porta destinatario*: campo da 16 bit, come significato analogo al precedente, solo che identifica il processo di destinazione;
- *numero di sequenza*: TCP numera i pacchetti generati, in modo che il destinatario possa controllare l'arrivo del flusso. Questo campo è lungo 32 bit e il mittente numera il primo pacchetto del flusso con un valore casuale compreso tra 0 e $2^{32} - 1$. I pacchetti che seguono avranno il numero di sequenza aumentato di uno rispetto al precedente. In accordo con quanto evidenziato in precedenza, la numerazione di un flusso è indipendente da quella relativa a flussi diversi.
- *numero di riscontro*: campo da 32 bit, serve per notificare al mittente l'avvenuta ricezione dei datagrammi. TCP utilizza la tecnica piggyback; ipotizziamo di avere due terminali A e B coinvolti in una comunicazione, A invia un messaggio a B che deve essere riscontrato. B inserisce il numero di riscontro nel prossimo datagramma, congiuntamente ad altri dati, da inviare ad A. Per essere valido questo campo, il bit ACK deve essere posto ad 1. Come valore di riscontro, l'host inserisce il numero di sequenza aumentato di uno: ad esempio se il terminale A ha inviato un pacchetto con numero di sequenza 23569, l'host B risponderà con numero di riscontro 23570. Questo perché l'host B attende il prossimo pacchetto da A con numero di sequenza 23570;
- *lunghezza header*: prevede 4 bit, indica in byte la lunghezza dell'header. Poiché l'header TCP ha una lunghezza variabile tra 20 e 60 byte, serve un campo per specificarne di volta in volta l'effettiva lunghezza;
- *riservati*: comprende 6 bit riservati per eventuali usi futuri;
- *flag*: 6 bit, ogni bit ha un significato ben preciso:
 - URG: bit che indica se il datagramma è urgente oppure no;
 - ACK: bit che indica che il numero di riscontro è il riscontro al messaggio;
 - PSH: bit che indica una richiesta di invio di dati immediata;
 - RST: bit che serve per indicare la richiesta di interruzione della comunicazione;
 - SYN: bit che indica la richiesta di instaurazione di una comunicazione;
 - FIN: bit che indica la chiusura della comunicazione in corso;
- *finestra*: prevede 16 bit, fa riferimento al meccanismo di controllo a finestra scorrevole (sliding window) descritto nel capitolo 13 ed indica quanti byte il mittente è in grado di accettare. Il valore di questo campo viene deciso dal destinatario del flusso;

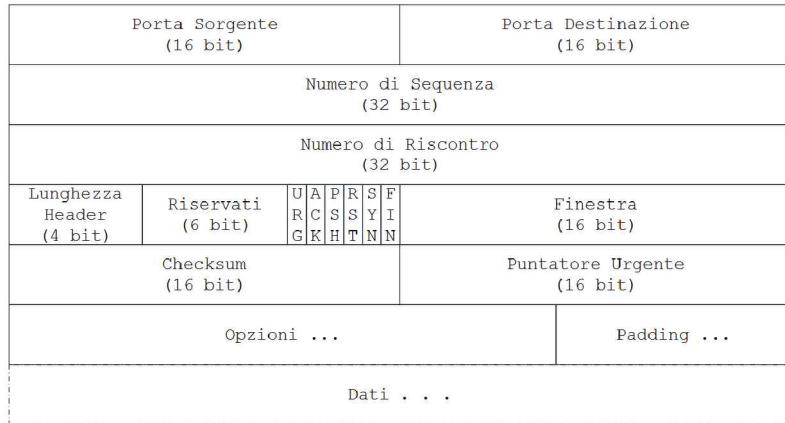


Figura 4.18: Header TCP

- *checksum*: campo di 16 bit e viene utilizzato come rilevatore di errori nell'header;
- *puntatore urgente*: campo da 16 bit ed è valido solo quando il bit di flag URG è posto a 1. Questo campo contiene il numero di byte di dati urgenti, dati che TCP deve trasferire immediatamente dopo avrei ricevuti al processo di destinazione. La lettura dei byte urgenti inizia dal primo byte del campo dati fino a quello indicato, meno uno, dal campo puntatore;
- *opzioni*: campo di lunghezza variabile, utilizzato per aggiungere funzionalità ulteriori a quelle già previste dai vari campi dell'header TCP (es.: per definire la dimensione massima dei segmenti in bit).

In precedenza è stato detto che TCP è il protocollo di livello di trasporto orientato alla connessione è quindi lecito chiedersi:

Come avviene l'apertura e la chiusura della connessione TCP?

La risposta è la seguente :

La fase di apertura di una connessione logica TCP avviene utilizzando una procedura di handshake a tre fasi (**three-way handshake**) illustrata in figura 4.19.

In particolare, come indicato in Halsall'2005 in 4.10, si ha:

1. un processo client per instaurare una connessione con un processo server per prima cosa invia un messaggio, chiamato *SYN*, dove ha posto il bit SYN uguale a 1 e ha scelto in modo casuale un numero di sequenza;
2. il processo server risponde con un secondo messaggio, chiamato *SYN + ACK*, dove ha posto i bit SYN e ACK uguali a 1 e nel campo numero di sequenza ha scelto un valore casuale indipendente dal primo e nel campo

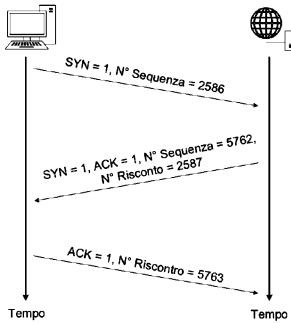


Figura 4.19: Three-way handshake TCP

numero riscontro ha scritto il valore del *numero di sequenza* del messaggio SYN aumentato di uno. Da notare che da questo momento in poi, la numerazione dei due datagrammi (dal client al server e viceversa) avrà come riferimento questi due valori;

3. il client risponde con un terzo messaggio, chiamato *ACK*, dove il flag ACK ha valore 1 e il numero riscontro ha il valore del numero di sequenza del precedente datagramma del server aumentato di uno. Questo datagramma è la risposta al messaggio SYN da parte del client.

Una volta finiti questi tre passaggi può iniziare lo scambio dati tra il client e il server.

Una volta instaurata la connessione, i due terminali procedono allo scambio dei datagrammi.

Quando una le due connessioni TCP attivate contemporaneamente (duplex) termina l'invio dei datagrammi, ciascun collegamento TCP viene chiuso separatamente. La chiusura di una connessione TCP può avvenire secondo due tecniche: la **three-way handshake** e la tecnica **four-way handshake**. La prima tecnica prevede le seguenti fasi:

1. il processo che vuole terminare la comunicazione invia un messaggio, che può contenere oppure no dati, con il bit FIN posto a 1. Per semplicità, questo messaggio è chiamato *FIN*;
2. il processo che riceve il pacchetto di FIN risponde con un secondo messaggio dove i bit FIN e ACK sono posti a 1. Questo messaggio può contenere gli ultimi dati da inviare. Per assonanza, questo messaggio è chiamato *FIN + ACK*;
3. infine, chi ha iniziato la richiesta di chiusura invia un messaggio che non contiene dati, ma che ha il bit ACK posto a 1. Questo messaggio è chiamato *ACK*.

La four-way handshake è simile alla procedura precedente, prevede soltanto un controllo preventivo, prima della sua attivazione, riguardo il completamento

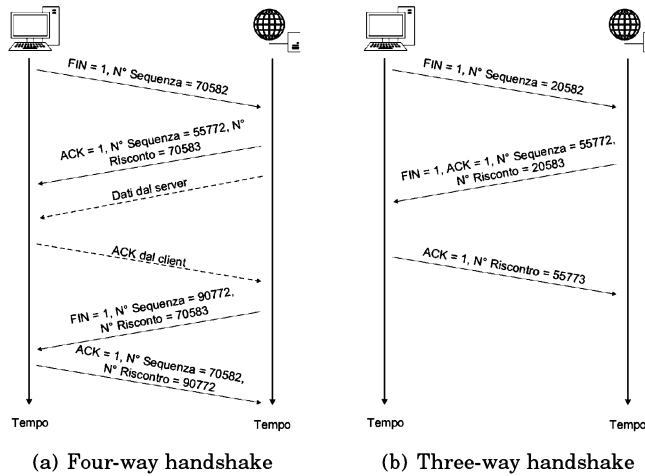


Figura 4.20: Chiusura della connessione TCP

congiunto della trasmissione dei datagrammi nella connessione (duplex) TCP. La procedura di chiusura non viene attivata se l'altro terminale non ha completato l'invio dei dati. Le fasi previste sono:

1. il processo che vuole terminare la comunicazione invia un messaggio, che può contenere gli ultimi dati, con il bit FIN posto a 1;
 2. il processo che riceve il pacchetto di FIN risponde con un messaggio dove il bit ACK è posto a 1. In questo modo avvisa il primo processo che ha ricevuto la richiesta di chiusura della connessione, ma che ha ancora necessità di inviare dati nel collegamento;
 3. una volta terminata la trasmissione dei dati, il secondo processo invia un messaggio dove i bit FIN e ACK sono posti a 1;
 4. il processo che ha iniziato la richiesta di chiusura del collegamento TCP invia un messaggio con il bit ACK posto a 1. Successivamente all'invio di questo messaggio la connessione TCP viene chiusa.

Le due procedure sono illustrate in figura 4.20.

4.5.6 Livello Applicativo

Questo è un livello generico che raggruppa i livelli superiori della pila ISO/OSI (sessione, presentazione e applicativo), contiene le applicazioni tipiche per cui è richiesta la connessione, alcuni esempi:

- TELNET: connessione di un terminale a un host remoto;

- FTP (File Transfer Protocol): protocollo per il trasferimento dati di grosse dimensioni;
- SMTP (Simple Mail Transfer Protocol): servizio di posta elettronica;
- HTTP (HyperText Transfer Protocol): navigazione siti, accessi a database, etc.

4.6 Confronto tra architettura TCP/IP e ISO/OSI

Come mostrato in figura 4.21 le pile architettoniche TCP/IP e ISO/OSI evidenziano molte similitudini. In particolare è banale sottolineare il fatto che entrambi si rifanno al paradigma di pila (stack) protocollare dove in ogni livello risiedono protocolli indipendenti. In aggiunta a questo, alcuni livelli hanno funzionalità simili (Kurose'2013, Tanembaum'2011, Forouzan'2007 in 4.10). In entrambe le architetture è presente il livello applicazione che, nell'architettura TCP/IP, include anche le funzionalità proprie dei livelli sessione e presentazione di ISO/OSI. Il livello trasporto è nuovamente presente in entrambe le architetture ed è principalmente preposto in entrambi i casi a fornire una modalità di comunicazioni peer-to-peer indipendente dalla rete. Il livello Internet di TCP/IP ha una implementazione semplificata rispetto al corrispondente livello di rete di ISO/OSI in quanto prevede solamente la modalità di comunicazione connectionless mentre in ISO/OSI è prevista anche la modalità connection oriented. I livelli collegamento e fisico non sono espressamente presenti nell'architettura TCP/IP dove invece il livello Host-to-Network, come descritto in precedenza, si preoccupa di rendere compatibile la pila TCP/IP con differenti tipologie di rete.

Come conclusione possiamo affermare che la suite protocollare TCP/IP è uno standard più semplice rispetto alla pila ISO/OSI e di più facile implementazione. Queste sono poi le motivazioni principali che giustificano l'enorme successo commerciale del protocollo TCP/IP le cui proporzioni fanno poi in modo che si possa considerare, senza dubbio, come il principale modello di rete ad oggi conosciuto ed utilizzato.

4.7 Modello IEEE 802

L'organizzazione IEEE (Institute of Electrical and Electronic Engineers) è un comitato internazionale con l'obiettivo di proporre e promuovere nuove metodologie ed applicazioni nel campo dell'elettrotecnica, dell'elettronica, dell'informatica, nell'ambito biomedico e delle telecomunicazioni. Nacque il 1º gennaio 1963 dalla fusione di due istituzioni precedenti: l'IRE (Institute of Radio Engineers) e l'AIEE (American Institute of Electric Engineers) nati un secolo prima.

L'IEEE 802 LAN/MAN Standards Committee (LMSC), vedi RFC 4443, è una commissione dell'IEEE preposta a sviluppare standard per le reti locali (LAN) e per le reti metropolitane (MAN). In generale si identifica con il termine LAN una rete dati adatta a connettere dispositivi di rete disposti entro un area limitata (non superiore a qualche chilometro) con topologie tipiche a Bus, Ring o a Stella,

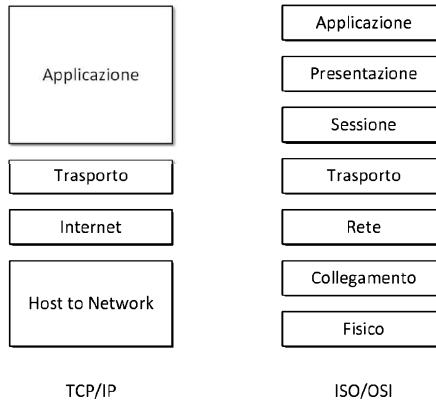


Figura 4.21: Architetture protocollari TCP/IP e ISO/OSI

funzionalità di base relativamente semplici, che presuppongono l'uso di mezzi trasmittivi di elevata qualità (fibra ottica, cavo coassiale) con un buon livello di immunità dai disturbi esterni (rumore). Una MAN è una rete dati con caratteristiche funzionali e topologiche simili alle LAN ma preposta a fornire connettività a dispositivi entro un area più ampia (decine di chilometri). Una caratteristica più specifica per le LAN, ma applicabile anche alle MAN, è conseguente alla loro semplicità topologica e funzionale che le rende particolarmente attraenti dal punto di vista del costo. Inoltre entrambe sono caratterizzate da una elevata affidabilità (spesso conseguente alla qualità del mezzo fisico), resilienza a guasti accidentali e flessibilità d'impiego (Tanembaum'2011, Kurose'2013, Frouzan'2007 in 4.10). In genere l'adeguamento tecnologico di una LAN o MAN (es.: per aumentare la velocità di accesso) si limita alla sostituzione degli apparati di rete e non coinvolge il mezzo fisico. Infine esse consentono di adeguarsi ad incrementi di esigenze di servizio (es.: numero di utenti) in maniera modulare e scalabile richiedendo quindi un investimento economico ridotto. Compito del comitato IEEE 802 LMSC è stato quello di definire un modello di riferimento a strati come illustrato nella figura 4.22. Questo modello si riferisce principalmente alla standardizzazione di tre livelli denominati *Logical Link Control* (LLC), che ha il compito di gestire i collegamenti logici del livello sottostante, *Medium Access Control* (MAC), con il compito primario di gestire l'accesso ad uno stesso mezzo fisico tra più dispositivi di rete ed il *Physical Layer* (PL) che infine ha la competenza di sovrintendere alle operazione di trasmissione/ricezione dell'informazione nel/dal mezzo fisico. Come illustrato nella figura 4.22 questi tre strati trovano una analogia funzionale con i due livelli più bassi della pila protocollare ISO/OSI, ovvero il livello fisico e il livello data link.

In tabella 4.3 sono mostrati alcuni standard licenziati dal comitato IEEE 802.

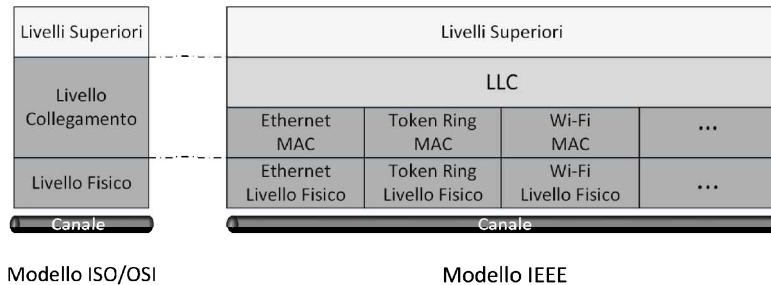


Figura 4.22: Architettura protocollare IEEE

4.7.1 Sottolivello Logical Link Control

La caratterizzazione del livello Logical Link Control (LLC) è competenza del comitato IEEE 802.2 (vedi <http://www.ieee802.org>), il quale ha la responsabilità di sviluppare un unico standard che si possa interfacciare, al livello inferiore, con tutti i livelli MAC e fisici standardizzati dal comitato IEEE 802 e, al livello superiore, con il protocollo di rete previsto (es.: nel caso di architettura TCP/IP si deve interfacciare con il protocollo IP). Il sottolivello LLC sovrintende al trasferimento dei pacchetti tra due nodi della rete. È il responsabile del controllo del flusso dati, della l'integrità dell'informazione ed in generale concorre a garantire un corretto collegamento tra i nodi. Il livello LLC è unico per tutte le reti in standard IEEE 802 (vedi tabella 4.8) ed è, di conseguenza, indipendente dai livelli MAC e Fisico.

Il sottolivello LLC fornisce al livello superiore tre distinte modalità di servizio (Tanembaum'2011, Kurose'2013, Forouzan'2007 in 4.10):

- **connectionless senza riscontro:** chiamato anche modalità di servizio logical data link; i singoli datagrammi sono trasmessi in modo indipendente l'uno dall'altro; una volta inviati non si richiede alcuna conferma della loro effettiva ricezione. Al nodo destinazione si può verificare che i singoli elementi arrivino senza rispettare la sequenza di trasmissione. Inoltre, prevede la possibilità di trasmettere verso una sola stazione (comunicazione unicast), più stazioni (comunicazioni multicast) o verso l'intera rete (comunicazione broadcast). Non è prevista alcuna forma di correzione degli errori e nemmeno sono previste funzioni di controllo di flusso; se queste funzioni sono richieste, devono essere implementati dai protocolli di livello superiore;
- **connectionless con riscontro:** è un servizio logical data link alternativo; pur essendo una modalità non orientata alla connessione prevede una conferma di ricezione (acknowledgement) per tutti i pacchetti inviati, questo garantisce la consegna ordinata dei dati trasmessi;

Nome	Descrizione	note
IEEE 802.1	Bridging e Network Management	
IEEE 802.2	Logical Link Control	inattivo
IEEE 802.3	Ethernet	
IEEE 802.4	Token Bus	dismesso
IEEE 802.5	Token Ring	inattivo
IEEE 802.6	Distributed Queue Dual Bus	dismesso
IEEE 802.7	Broadband LAN using Coaxial Cable	dismesso
IEEE 802.8	Fiber Optic TAG	dismesso
IEEE 802.9	Integrated Services LAN	dismesso
IEEE 802.10	Interoperable LAN Security	dismesso
IEEE 802.11	Wireless Local Area Network (WLAN)	
IEEE 802.12	100BaseVG	dismesso
IEEE 802.13	Non Utilizzato	
IEEE 802.14	Cable Modems	dismesso
IEEE 802.15	Wireless Personal Area Network (WPAN)	
IEEE 802.16	Broadband Wireless Access	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	
IEEE 802.25	Omni-Range Area Network	Non ancora ratificato

Tabella 4.3: Standard IEEE 802



Figura 4.23: Protocol Data Unit del sottolivello LLC

- **connection oriented:** chiamato anche modalità di servizio data link connection; è un servizio affidabile e orientato alla connessione, che si articola in tre fasi:
 - apertura di un canale di comunicazione tra sorgente e destinazione per consentire lo scambio dei dati (set-up);
 - controllo della comunicazione durante il trasferimento dei dati;
 - eliminazione (reset) del canale dedicato.

Inoltre questo strato prevede metodologie per garantire l'integrità dell'informazione trasferita.

I dati provenienti dal livello superiore vengono incapsulati secondo le modalità classiche e trasferiti al livello MAC e successivamente vengono passati al livello fisico che opera con la stessa modalità e conclude il processo con la trasmissione fisica di opportuni segnali associati ai bit del flusso informativo nel mezzo di comunicazione. Secondo la terminologia IEEE 802 il blocco informativo gestito da ogni livello prende il nome di *Protocol Data Unit* (PDU). Il PDU, riferito al sottolivello LLC, è illustrato in figura 4.23. In particolare, esso prevede i seguenti campi:

- indirizzo DSAP: è l'indirizzo del Service Access Point di destinazione;
- indirizzo SSAP: è l'indirizzo del Service Access Point di origine;
- controllo: è un campo che può essere di 8 bit per le modalità connectionless oppure 16 bit per la modalità connection oriented;
- informazione: è un campo di lunghezza variabile, è il pacchetto proveniente dai livelli superiori. Non è stabilito un limite massimo alla lunghezza in byte.

4.7.2 Sottolivello Medium Access Control

Il sottolivello MAC è di fatto la componente principale e caratterizzante l'architettura specifica. Il suo compito funzionale è la gestione dell'accesso al mezzo trasmisivo condiviso da tutti i dispositivi della rete. Conseguenza di questo è che la trasmissione dell'unità informativa nel mezzo stesso è generalmente realizzata in modalità broadcast (diffusione globale). Conseguenza di questo è che tutti i dispositivi connessi ricevono l'unità informativa anche se non ne sono i

destinatari. Le unità informative di livello MAC hanno comunque tutte specificato l'indirizzo della sorgente e della destinazione (MAC-SSAP e MAC-DSAP, rispettivamente) per cui solo il dispositivo che si riconosce come destinatario processa l'unità informativa che viene invece ignorata dagli altri. La modalità di trasmissione, nativamente broadcast, consente, definendo adeguatamente il campo indirizzo di destinazione, di implementare comunicazioni punto multipunto (Multicast o Broadcast). I protocolli ad accesso multiplo si dividono poi in base alla metodologia di riferimento in:

- **tecnica ordinate;**
- **tecnica casuali.**

Le varie tecniche di accesso al canale rivestano un grande interesse nel settore delle reti dati e per questo motivo si rimanda una loro discussione dettagliata al capitolo 5.

Indirizzi di livello MAC

Ogni host deve avere un identificativo univoco che identifichi le sue varie interfacce. A differenza degli indirizzi IP (che sono indirizzi logici), gli indirizzi di livello MAC (o di livello collegamento oppure indirizzi fisici) sono assegnati in modo univoco dal produttore ad ogni scheda di rete realizzata (al momento della sua produzione). L'indirizzo MAC è diverso dall'indirizzo IP poiché esso è l'indirizzo di livello rete necessario per interconnettere gli host di una sottorete locale con quelli di altre sottoreti garantendo interoperabilità tra di esse (si dice che avviene un instradamento indiretto tra le sottoreti). L'indirizzo MAC, invece, è utilizzato per l'instradamento diretto nelle reti locali. Esiste un protocollo che ha il compito di tradurre gli indirizzi di livello IP in quelli di livello MAC, in IPv4 è il protocollo ARP (Address Resolution Protocol), vedi RFC 0826, mentre in IPv6 è il protocollo NDP (Neighbor Discovery Protocol), vedi RFC 1971. A livello concettuale il funzionamento per i due standard è analogo: l'host che vuole conoscere il MAC address di un altro host, di cui conosce l'indirizzo IP, invia in broadcast una richiesta contenente l'indirizzo IP del terminale di cui vuole conoscere il MAC Address. Tutti i terminali della sottorete che ricevono la richiesta confrontano l'indirizzo IP inserito nel pacchetto con il proprio indirizzo IP. L'host che riconoscerà il proprio indirizzo IP nel pacchetto provvederà ad inviare una risposta, in unicast, quindi solo al mittente del primo pacchetto, contenente il proprio MAC address all'indirizzo MAC del richiedente.

Gli indirizzi di livello MAC, come indicato in Tanembaum'2011, Kurose'2013, Forouzan'2007, (vedi paragrafo 4.10), sono divisi in tre spazi di numerazione, tutti regolati dall'IEEE: MAC-48, EUI-48, EUI-64, i primi due usano 48 bit per l'indirizzo mentre l'ultimo di bit ne usa 64. Tutti i tre sistemi utilizzano lo stesso formato. La differenza tra indirizzo EUI-48 e indirizzo MAC-48 è puramente nominale: l'indirizzo MAC-48 identifica l'hardware di rete mentre l'indirizzo EUI-48 identifica gli altri device e i software; teoricamente le due classi di indirizzi identificano due apparati diversi ma a livello sintattico sono indistinguibili

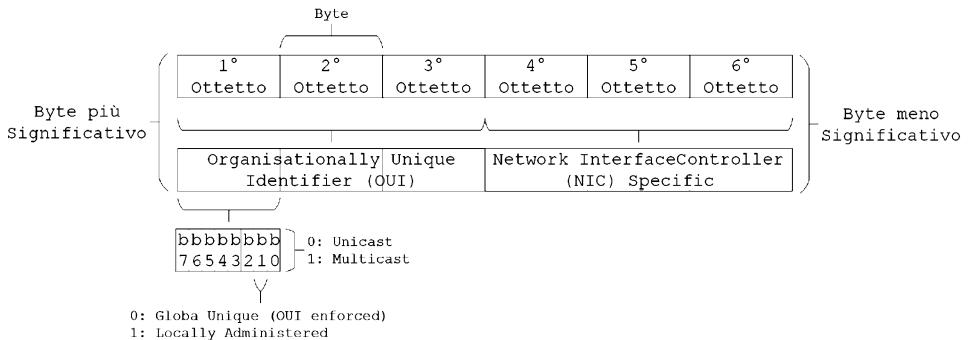


Figura 4.24: Indirizzo MAC-48

e questo ha portato l'IEEE a considerare obsoleta la nomenclatura MAC-48. In futuro con il termine EUI-48 si considerano tutti gli indirizzi MAC a 48 bit.

L'indirizzo MAC IEEE 802 deriva dalla specifica di Ethernet (capitolo 6). Chi inizialmente progettò Ethernet decise di usare 48 bit per gli indirizzi, quindi si hanno 2^{48} indirizzi MAC disponibili. I 48 bit dell'indirizzo MAC sono espressi in 12 cifre esadecimali, mentre i 64 bit dell'indirizzo EUI-64 sono espressi in 16 cifre esadecimali. Gli indirizzi MAC si differenziano in *universally administered addresses* o in *locally administered addresses*. Nel primo caso l'indirizzo è univocamente assegnato a livello mondiale. In entrambi i casi i primi tre ottetti (quindi i 24 bit più significativi) identificano l'organizzazione o il produttore proprietario della scheda di rete e sono anche chiamati *Organizationally Unique Identifier (OUI)*. I successivi tre byte, nel caso di indirizzo EUI-48, o cinque byte, nel caso di indirizzo EUI-64, sono assegnati dal produttore alla singola scheda di rete. Nel secondo caso invece l'indirizzo MAC è assegnato a un device dall'amministratore di rete, sovrascrivendo l'indirizzo univoco. Le due tipologie di indirizzi si distinguono in base al valore assunto dal secondo bit meno significativo del byte più significativo; se questo bit ha valore 0 allora siamo in presenza di un indirizzo universally administered mentre se il bit ha valore 1 siamo in presenza di un indirizzo locally administered.

L'indirizzo MAC si scrive normalmente in 6 ottetti, nel caso di indirizzo EUI-48, oppure in 8 ottetti nel caso si avesse un indirizzo EUI-64, separati da un o trattino oppure dai due punti, come ad esempio 0A-06-FC-AB-B7-2C. La figura 4.24 riassume tutto quanto detto in precedenza.

Per vedere la lista completa degli OUI assegnati dall'IEEE ai singoli produttori si può fare riferimento alla documentazione reperibile al sito:

<http://standards.ieee.org/develop/regauth/oui/oui.txt>

4.7.3 Livello Fisico

La specifica del livello fisico è conseguente il particolare tipo di rete ed il mezzo fisico di cui si dispone. Lo standard IEEE 802 prevede specifiche proprie di ogni

rete LAN. In alcuni casi, come nelle reti Ethernet (IEEE 802.3) per uno stesso sottolivello MAC esistono diverse alternative per il mezzo fisico e di conseguenza standard differenti.

4.8 Rete Distributed Queue Double Bus (DQDB)

La rete Distributed Queue Double Bus (DQDB) è uno standard rivolto a reti MAN. Sebbene non abbia ottenuto un grande successo rappresenta un modello di rete che è utile discutere per meglio cogliere gli aspetti metodologici e funzionali propri di reti più attuali, o di più larga diffusione, che esamineremo di seguito. La rete DQDB è una rete multi-accesso con protocollo ordinato che prevede una topologia fisica a doppio bus (ciascuno unidirezionale) e la distribuzione dell'accesso ai vari dispositivi (nodi) in accordo con l'ordinamento temporale delle loro richieste di accesso, secondo un modello di accodamento FIFO (First-In-First-Out) distribuito. Lo standard IEEE 802 relativo alla rete DQDB è lo standard IEEE 802.6. La rete DQDB è illustrata in figura 4.25. In accordo a quanto affermato in precedenza, la rete è formata da due bus unidirezionali, con senso di propagazione del segnale opposto, ognuno con velocità di accesso di 150 Mbps. Ogni nodo della rete ha la possibilità di effettuare un doppio accesso in lettura e scrittura (R/W) per ogni bus. La prenotazione per la trasmissione in un certo bus viene effettuata e notificata agli altri nodi accedendo all'altro bus. La scelta del ruolo di un bus (accesso/prenotazione) viene stabilita in base alla posizione del nodo con cui si vuole comunicare. Ad esempio, guardando la figura 4.25, se il nodo B vuole comunicare con il nodo C effettuerà la prenotazione di accesso accedendo al bus inferiore e completerà la trasmissione dell'informazione verso C accedendo al bus superiore. Da qui ne segue che il corretto funzionamento della rete necessita della conoscenza completa da parte di ogni nodo della posizione degli altri nodi.

L'accesso ai due bus è organizzata su base slot (tempo). In ogni slot si trasporta un solo pacchetto informativo per il quale si possono individuare due campi principali : Testata (Header) e Dati (Payload). La testata, a sua volta, prevede un campo di stato (S) e un campo di prenotazione (P), come mostrato (in forma semplificata) in figura 4.26. Il campo S assume il valore binario 1 se il seguente campo informativo (DATI) è occupato (cioè il pacchetto trasporta informazione), altrimenti il suo valore è 0. Analogamente, il campo P di valore 1 significa che un altro nodo ha notificato la necessità di accesso alla rete e quindi il nodo che legge questo valore deve attendere per rispettare l'ordinamento temporale delle

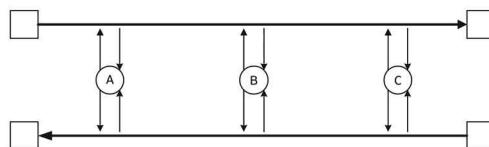


Figura 4.25: Rete DQDB

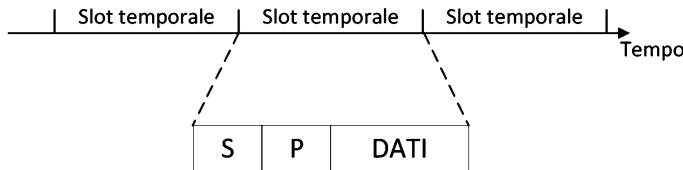


Figura 4.26: Divisione temporale degli slot

richieste di accesso, oppure, se ha valore 0, il nodo ha la possibilità di notificare la sua prenotazione e di entrare in attesa di trasmissione. Tutte le stazioni leggono l'intestazione degli slot temporali e, in base ai valori dei campi S e P, acquisiscono una conoscenza globale ed aggiornata della rete.

4.8.1 Struttura di un nodo DQDB

La gestione dell'accesso ai due bus è gestita da due strutture duali specifiche per ogni bus. L'architettura della struttura interna di un nodo DQDB preposta alla gestione dell'accesso al bus superiore è mostrata in figura 4.27. Si nota subito che essa è formata da tre macro blocchi:

- *contatore add/drop*: incrementa di uno il valore memorizzato tutte le volte che osserva nel bus inferiore uno slot con il campo P settato a uno. Decrementa di uno il suo valore ogni volta che osserva nel bus superiore uno slot con il campo S settato a zero;
- *contatore drop*: viene decrementato ogni volta che sul bus di trasmissione passa uno slot libero, ovvero con campo S di valore 0;
- *buffer*: memorizza i dati in attesa di trasmissione.

Il valore del contatore add/drop ad ogni istante (tempo di slot) rappresenta il numero di nodi che hanno già dichiarato la necessità di accesso senza ovviamente specificarne l'ordinamento temporale. Ogni nodo di una rete DQDB può gestire un solo accesso per uno stesso bus per cui non può procedere ad una nuova prenotazione fino a quando la fase di accesso iniziata non è stata completata. Quando un nodo ha necessità di accedere al bus per la trasmissione inizia l'osservazione del campo P degli slot che viaggiano nel bus opposto a quello desiderato. Non appena scopre uno slot con campo P con valore zero effettua la sua prenotazione. Contemporaneamente il valore del contatore ADD/DROP viene trasferito al contatore DROP. Il valore del contatore DROP rappresenta quindi il numero di nodi che, indipendentemente dal loro ordinamento temporale, hanno priorità nell'accesso al canale in accordo al modello di coda FIFO distribuita. Il valore del contatore DROP viene decremento di 1 ogni volta che nel bus di trasmissione viene individuato uno slot con campo S a 1. Quando il contatore DROP assume il valore 0, il primo slot con campo S a 0 viene utilizzato dal nodo per effettuare

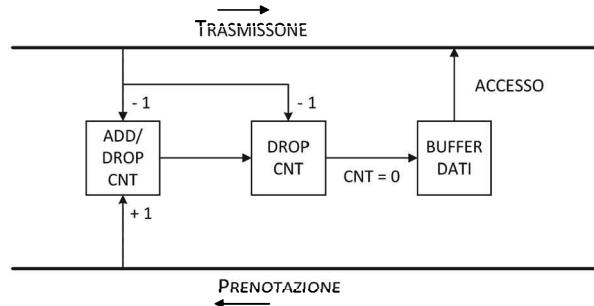


Figura 4.27: Struttura di un nodo DQDB

la trasmissione del proprio pacchetto e concludere la fase di accesso. Durante l'attesa per l'accesso il contatore ADD/DROP continua ad operare nella modalità base in maniera da seguire puntualmente l'evoluzione temporale delle richieste di accesso.

Mediante queste operazioni ogni stazione rispetta l'ordinamento temporale delle richieste effettuate dalle altre stazioni, cioè l'ordine di arrivo e le priorità di accesso, evitando quindi che si creano conflitti nella rete. La rete DQDB, per come è stata fino a qui descritta, appare quindi basata su di un protocollo per la distribuzione dell'accesso ad un mezzo condiviso con prestazioni prossime all'ideale.

Purtroppo la realtà operativa è diversa. Nel nostro modello infatti non abbiamo considerato i ritardi di propagazione che inevitabilmente il mezzo fisico introduce e che fanno perdere il rispetto stretto dell'ordinamento temporale delle richieste di accesso (può accadere che un nodo prenoti dopo un altro senza averne conoscenza). In aggiunta a questo, un importante difetto di queste reti è dovuto ad una non equa distribuzione della possibilità di accesso tra i nodi. In pratica i nodi che si trovano più vicini al punto di inizio del bus usato per le prenotazioni acquisiscono una priorità implicita per l'accesso fino ad arrivare a situazioni estreme in cui il nodo più vicino all'inizio del bus delle prenotazioni può monopolizzare l'accesso al bus superiore a scapito degli altri nodi. La modifica proposta per alleggerire questo inconveniente consiste nell'imporre una limitazione al numero di slot che ogni stazione può utilizzare in maniera consecutiva. La priorità di accesso per i nodi più vicini al punto di origine della trama utilizzata per le prenotazioni rispetto ad altri nodi non viene eliminata, ma i suoi effetti vengono limitati.

La rete DQDB è stata progettata per servizi non isocroni, tuttavia essa può essere resa compatibile anche con tali specifiche esigenze di servizio (trasmissione con cadenza regolare). La soluzione consiste nell'introdurre un meccanismo di prenotazione che consente di pre-allocare un certo numero di slot a quei nodi che hanno bisogno di trasmettere con cadenza temporale fissa (traffico isocrono).

4.9 Rete Fiber Distributed Data Interface (FDDI)

Questo protocollo è stato progettato per una rete che utilizza come mezzo trasmissivo condiviso la fibra ottica con una capacità di trasferimento dell'informazione di 100 Mbps. L'estensione massima è dell'ordine delle centinaia di chilometri e permette il collegamento di circa 500 stazioni. La rete FDDI è nata come standard ANSI ed ha rappresentato una evoluzione tecnologica dello standard IEEE 802.5 (Token Ring). Le principali innovazioni tecnologiche introdotte sono state:

- Utilizzo esclusivo di mezzi trasmissivi in fibra ottica;
- Area di lavoro più estesa (si parla più propriamente di FDDI come rete MAN);
- Resilienza ai guasti sia dei collegamenti che dei nodi di rete.

La topologia della rete è molto particolare e ne rappresenta una degli aspetti più caratterizzanti. Nello specifico, la rete FDDI ha una topologia logica (e spesso anche fisica) a doppio anello, come mostrato in figura 4.28.

La propagazione del segnale ottico nei due anelli ha senso opposto (controrotanti). Le comunicazioni tra i nodi della rete interessano uno solo dei due anelli. Tale anello, detto *primario*, è tipicamente l'anello esterno. L'altro anello (tipicamente quello interno), detto *secondario*, viene attivato quando nella rete si manifestano guasti ai nodi o interruzione del primario permettendo una rapida riconfigurazione della rete e quindi aumentandone l'affidabilità di esercizio. In condizioni particolari il secondario può anche essere utilizzato per aumentare la capacità di accesso fino a raggiungere il valore nominale di 200 Mbps. Entrambe queste caratteristiche rendono la rete FDDI adatta ad impieghi quali reti di backbone (dorsali per LAN) o per trasferimento di flussi informativi con alta affidabilità di esercizio (es.: applicazioni in ambienti ospedalieri).

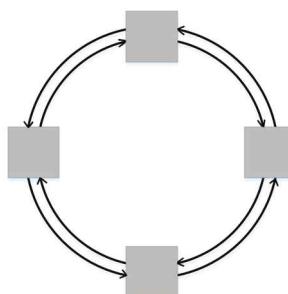


Figura 4.28: Rete FDDI

4.9.1 Livello MAC

L'accesso al canale da parte dei nodi avviene mediante tecnica ad accesso ordinato che si richiama ai principi base del metodo token ring (vedi Tanenbaum'2011, Kurose'2013, Forouzan'2007 in 4.10). Supporta la trasmissione di traffico sincrono e asincrono. Per la trasmissione di traffico isocrono è stato definito il protocollo FDDI-II, che tuttavia, essendo risultato di più complessa implementazione e gestione, non ha avuto una significativa diffusione applicativa.

Il traffico sincrono non prevede suddivisione in livelli di priorità a differenza invece del traffico asincrono per il quale lo standard ha previsto un'ulteriore classificazione dei flussi informativi in otto livelli di priorità. Al traffico sincrono viene sempre garantito il diritto di trasmissione mentre per il traffico asincrono la modalità adottata è di tipo best-effort (viene trasmesso solo quando possibile). Quando un nodo acquisisce il diritto di trasmissione per traffico asincrono, questa possibilità viene gestita coerentemente con la classificazione dello stesso in livelli di priorità: la priorità massima viene assegnata al traffico di livello 1 ed in successione ordinata agli altri. La gestione di traffico sincrono e asincrono da parte di un nodo, come meglio verrà chiarito di seguito, comporta la necessità di avere dei buffer dove i flussi informativi sono memorizzati in accordo alla loro tipologia (sincrono, asincrono) e livello di priorità, quando prevista.

La rete FDDI prevede due differenti tipologie di trame:

- *token frame* (segnalazione): ha una struttura predefinita e nota a tutti i nodi. Viene utilizzata per la condivisione dell'accesso. La stazione che ha il token frame è quella adibita alla trasmissione, una volta terminato l'invio dei dati rilascia nella rete il token frame, accodando la sua trasmissione a quella del flusso informativo;
- *data frame* (informazione): sono frame contenenti informazioni.

Il protocollo prevede un controllo di integrità dell'informazione trasmessa su base end to end (E2E). I nodi che non riconoscono il proprio indirizzo nel campo del destinatario dell'informazione ritrasmettono direttamente il frame senza interpretarlo. Viceversa, il nodo destinatario, interpretato il frame lo riscontra, accedendo ad un campo opportuno, come ricevuto al mittente. Tutti i nodi ripetono i frame di canale eccetto quelli generati da loro stessi correttamente riscontrati dai rispettivi destinatari (solo i nodi destinatari possono togliere l'informazione dalla rete non ripetendola in uscita).

L'implementazione dell'accesso viene fatta sulla base di un ordinamento temporale dell'accesso al mezzo condiviso. A tale scopo viene definito un parametro, denominato **Token Target Rotation Time (TTRT)**, come segue:

$$\text{TTRT} \geq \sum_{i=1}^{N_d} \alpha_i + \sum_{i=1}^{N_d} d_i \quad (4.1)$$

dove:

- α_i è il tempo necessario alla stazione i -esima per la trasmissione del traffico sincrono (in unità di tempo normalizzate);
- d_i è il tempo di passaggio del token da una stazione alla successiva indicato come tempo di cammino (*walking time*). Tale parametro è legato a: tempo di propagazione del segnale nel supporto ottico (propagazione nel mezzo fisico); tempo di trasmissione del token e tempo di elaborazione e gestione del token (latenza) in ogni nodo (inteso come interpretazione semantica del messaggio e attivazione della procedura di accesso al canale).

Il TTRT, per come è stato definito, indica il tempo di riferimento necessario al fine di assegnare a tutti i nodi della rete il diritto alla trasmissione congruente con le necessità di accesso (traffico sincrono) dichiarate.

Una volta determinato e condiviso il valore TTRT, la gestione dell'accesso è implementata in forma distribuita ed indipendente da ogni nodo. A questo fine, in ogni nodo è reso disponibile un contatore adibito alla misura del **Token Rotation Time** (TRT) inteso come il tempo effettivo che intercorre tra una ricezione del token e la successiva. Questo contatore misura quindi il tempo effettivo che il token impiega a distribuire l'accesso a tutti i nodi della rete secondo quanto previsto dal protocollo. Ogni nodo ha poi un altro contatore, a solo decremento, che definisce il tempo di accesso del nodo alla rete (o equivalentemente il tempo di tenuta del token da parte del nodo), indicato come **Token Holding Time** (THT). Il THT è così definito:

$$\text{THT} = \begin{cases} \alpha_i, & \text{se TTRT - TRT} \leq 0 \\ \text{TTRT} - \text{TRT}, & \text{altrimenti} \end{cases} \quad (4.2)$$

Questo vuol dire che se accade che il tempo di rotazione effettivo misurato per il token (TRT) è superiore al valore di riferimento (TTRT) la rete si è discostata dal funzionamento nominale dichiarato (qualche nodo ha trasmesso traffico sincrono per più di quanto dichiarato), conseguenza di questo è che al nodo non può essere riconosciuto il diritto di accesso per la sola trasmissione del traffico garantito (sincrono). Differentemente, se si verifica la condizione opposta, il valore del THT viene posto uguale alla differenza tra il valore TTRT e TRT. In questo modo, conclusa la fase di accesso per il traffico sincrono, il residuo, se presente, viene utilizzato per la trasmissione di traffico asincrono rispetto la classificazione dello stesso in livelli di priorità.

Conseguenza di come il protocollo FDDI opera si può dire che, detta B la banda nominale della rete, al nodo i -esimo viene in media garantita una banda B_i pari a:

$$B_i = \frac{\alpha_i}{\text{TTRT}} \cdot B \quad (4.3)$$

Per una rete FDDI si introduce poi un parametro η , denominato *efficienza d'uso*, così definito:

$$\eta = \frac{\text{TTRT} - \text{RL}}{\text{TTRT}} \leq 1 \quad (4.4)$$

dove RL indica la somma di tutti i walking time (tempi di latenza per i nodi). Dalla (4.4) si può facilmente notare che a valori più bassi di RL corrispondono valori più alti di η . La condizione ideale si ha quindi quando RL= 0.

4.10 Letture Consigliate

Per approfondire i vari argomenti trattati si consigliano i seguenti testi:

- F. Halsall, Reti di Calcolatori e Sistemi Aperti, Addison-Wesley, 1996.
- B.A. Forouzan, Reti di Calcolatori ed Internet, McGraw-Hill, 2007.
- A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.
- J.F. Kurose, K. W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.
- S.Gai, L. Montessoro, P. Nicoletti, Reti Locali, SSGRR, 1995.
- D.E. Comer, Internetworking con TCP/IP, Pearson, 2006.
- F. Halsall, Networking e Internet, Pearson, 2005.

Per informazioni più specifiche si consiglia inoltre di consultare le RFC citate nel capitolo.

5

Accesso Multiplo

Una caratteristica importante delle reti LAN è che l'accesso al mezzo fisico è condiviso. Questo, in generale, comporta dover gestire e risolvere problemi di conflitto derivanti da accessi contemporanei. Quando due o più utenti cercano di accedere simultaneamente al canale di comunicazione, senza un coordinamento preventivo, si viene a creare una situazione di mutua interferenza tra i rispettivi segnali che ne pregiudica irrimediabilmente l'integrità. Questo evento viene indicato come *collisione* e la sua conseguenza è la perdita dell'informazione trasmessa. È intuitivo notare che la probabilità di una collisione aumenta all'aumentare del numero di utenti che condivide uno stesso canale. Per questo motivo, al fine di limitarne gli effetti sull'efficienza della rete, di solito si pone un limite al numero massimo di possibili utenti e, se questo tende ad essere per ragioni di esercizio superato, si ricorre alla partizione degli utenti in singole LAN tra loro interconnesse.

Di seguito verranno descritte sinteticamente le tecniche di accesso al canale di tipo *ordinato*, senza contesa e *casuale* (random), con *contesa*, rimandando alle letture consigliate in 5.3 per un maggiore approfondimento delle stesse.

5.1 Tecniche ad accesso ordinato

Le tecniche ad *accesso ordinato* sono tecniche in cui l'accesso alla rete viene definito in accordo con una procedura fissata e nota a tutti gli utenti finalizzata ad evitare le situazioni di conflitto (collisioni) per l'accesso al canale condiviso.

La modalità tradizionale per condividere uno stesso canale tra più utenti senza contesa è quella di utilizzare le tecniche di multiplexing sia in frequenza (FDM) che nel tempo (TDM) descritte nel capitolo 2. Nel caso specifico di reti LAN le tecniche ad allocazione statica FDM o TDM si dimostrano tuttavia inefficienti in quanto, in generale, il singolo utente utilizza la propria risorsa di accesso (banda di frequenza o tempo di canale) senza continuità dando così luogo a spreco di capacità di accesso. Con l'obiettivo di limitare questo inconveniente, sono state proposte varianti alle tecniche base che prevedono una allocazione dinamica delle risorse di accesso pur preservando le caratteristiche proprie di un accesso ordinato (Tanembaum'2011, Schwartz'1987, Forouzan'2007, Hammond'1986 in 5.3). Un esempio a questo riguardo è la tecnica TDM asincrona, nota anche con il nome di multiplexer statistico, che rimuove il vincolo di una allocazione rigida

e fissa tra frazione di tempo (slot) di accesso e utente, prevedendo di assegnare ad uno stesso utente più frazioni di tempo di accesso consecutive. Il fine che si persegue in questo modo è quello di eliminare l'inefficienza derivante da risorse assegnate e non utilizzate. Altri esempi di tecniche ad accesso ordinato sono quelle basate sulla metodologia di multiplexer a divisione di codice (CDMA) e a divisione di frequenze ortogonali (OFDMA) brevemente descritte di seguito (per maggiori dettagli si veda Tanembaum'2011, Forouzan'2007 in 5.3):

- **CDMA** : si può ricorrere per comprendere il funzionamento di questa tecnica all'analogia con un caso comune di più persone in una stanza che si parlano a coppie in lingue differenti. Ciascuno interpreta solo ciò che viene detto nella propria lingua dal proprio partner ed ignora tutto il resto o, al più, lo percepisce come un fastidioso romore. Nel contesto di nostro interesse ogni utente trasmette la propria informazione occupando tutta la banda del canale condiviso, mediante l'uso di opportune sequenze binarie ortogonalni (Tanembaum'2011, Forouzan'2007 in 5.3). Il ricevitore, mediante una operazione, di correlazione estrarrà dall'aggregato del segnale ricevuto solo la componente relativa alla sequenza d'interesse ed ignorerà tutto il resto. Questa tecnica è utilizzata nei sistemi cellulari UMTS.
- **OFDMA** : realizza la condivisioni di un canale tra più utenti utilizzando il principio del multiplexing con frequenze ortogonali (OFDM). Questo metodo prevede la suddivisione della banda di canale in sottobande, ciascuna centrata su una frequenza ortogonale con tutte le altre. Un flusso dati che richiede una velocità (rate) di trasmissione elevato può essere suddiviso in flussi elementari trasmessi in parallelo, su canali diversi, a velocità più bassa. Il principio alla base della tecnica OFDM è noto da tempo (si veda Tanembaum'2011, Forouzan'2007, Marabissi'2008 in 5.3) ma solo recentemente ha ricevuto attenzione da parte degli sviluppatori di reti grazie alla possibilità di implementazione basata sulla trasformata veloce di Fourier (FFT). Questa tecnica è oggi impiegata nelle reti wireless IEEE 802.11, IEEE 802.16 e LTE (Long Term Evolution).

Altri esempi di tecniche ad accesso ordinato di tipo dinamico, adatte ad applicazioni in reti LAN, sono le tecniche polling e token passing, descritte di seguito.

5.1.1 Tecniche Polling

Le tecniche Polling (si veda Hammond'1986 per maggiori dettagli in 5.3) permettono di gestire, senza sovrapposizione, l'accesso di più nodi di rete ad un mezzo condiviso evitando le collisioni. La metodologia utilizzata è quella della chiamata diretta (o interrogazione). Il principio è simile alla procedura di appello nominale effettuato per verificare la presenza degli studenti ad una lezione o dei candidati ad una valutazione comparativa. In questo caso esiste una nodo principale (master) che gestisce l'accesso al canale condiviso di un certo numero di nodi secondari (client). Lo schema di principio della tecnica polling è illustrato in figura

5.1. Esistono poi due modalità per implementare praticamente la procedura di interrogazione:

- *Roll-Call*;
- *Hub-Polling*.

La modalità Roll-Call è completamente centralizzata: è il nodo master a gestire le fasi di autorizzazione e di rilascio del canale da parte dei nodi. Esso possiede la lista delle interrogazioni (Roll) e provvede ad interrogare (Call) i propri client secondo questa lista, dando ad ognuno la possibilità di accedere al canale condiviso attraverso l'invio di un messaggio di abilitazione. Il nodo client, una volta terminata la sua fase di accesso, invia in coda un messaggio predefinito per notificare al master il completamento del suo turno. Il master, ricevuto tale messaggio, provvederà ad interrogare un nuovo nodo client secondo la lista programmata delle interrogazioni.

La modalità Hub-Polling, diversamente, si basa su una metodologia di gestione dell'accesso che prevede la cooperazione dei nodi client. Tipicamente questa modalità si adatta ad essere utilizzata in reti LAN con topologia (logica) a bus ma viene anche utilizzata nel caso di topologia a ring. Il nodo master interroga per primo il nodo client più lontano. Questo, completata la sua fase di accesso, invierà in coda al flusso informativo trasmesso il pacchetto di rilascio. In questo modo il pacchetto di rilascio viene ricevuto per primo dal nodo client immediatamente successivo al nodo che ha completato la fase di accesso secondo la direzione che porta al nodo master. Il messaggio di rilascio viene interpretato come una autorizzazione implicita all'accesso al canale che viene quindi attivata e rilasciata con le stesse modalità. Alla conclusione del ciclo il pacchetto di rilascio ritorna al nodo master che inizializza una nuova fase di accesso interrogando nuovamente il nodo più lontano. Con questa modalità cooperativa si riesce a ridurre l'influenza dei tempi spesi per la gestione degli accessi al canale condiviso da parte di tutti i nodi client.

Indipendentemente dalle due modalità di interrogazione, una volta che un nodo client ha ricevuto l'autorizzazione all'accesso al canale, questa viene gestita secondo due procedure distinte:

- *gated*: si consente l'accesso al canale per un tempo massimo definito. Il nodo client è autorizzato a trasmettere soltanto i pacchetti arrivati nella frazione di tempo che intercorre tra due arrivi successivi dell'abilitazione al nodo. Quelli che arrivano durante l'espletamento della fase di accesso dovranno attendere (memorizzati in un buffer) per la loro trasmissione l'arrivo successivo dell'autorizzazione;
- *esaustivo*: non viene introdotta nessuna limitazione al tempo di accesso al canale. Di conseguenza, in questo caso, anche i pacchetti che arrivano durante l'espletamento di una fase di accesso vengono trasmessi. Il nodo termina la sua fase di accesso solo e soltanto quanto non ha più pacchetti da trasmettere.

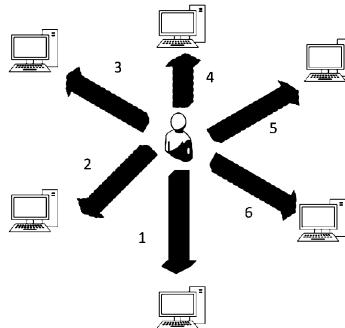


Figura 5.1: Tecnica polling

5.1.2 Token Passing

Questa tecnica di accesso multiplo ad un canale condiviso è di tipo ordinato e prevede una implementazione distribuita. Il principio base lo si potrebbe definire come "*passa parola*". La tecnica token passing prevede che tutti i nodi della rete si passino, secondo un ordine definito, un messaggio chiamato token (gettone). In generale i nodi sono ordinati logicamente (non sempre anche fisicamente) secondo un anello (ring) in modo che ogni nodo abbia sempre un nodo che lo precede ed uno che lo segue secondo il senso di propagazione del segnale nel mezzo fisico. La consegna del token ad un nodo rappresenta il riconoscimento al quel nodo del diritto di accesso esclusivo al canale condiviso. Completata la sua fase di accesso, il nodo consegna il token al nodo successivo rispettando l'ordine predefinito. Ovviamente, se un nodo che entra in possesso del token, non ha necessità di accesso, lo passa immediatamente al nodo successivo. I flussi informativi (frame) vengono trasmessi nel canale secondo la direzione e la modalità di passaggio del token tra i nodi. In questo modo è evidente che il destinatario del flusso verrà sempre raggiunto. Solo i nodi che hanno generato le informazioni possono toglierle dal canale. Per evitare che le informazioni circolino nell'anello senza limite, viene assegnato ai nodi mittente il compito di rimuoverli dall'anello (cioè una volta ricevuti di nuovo non vengono più ripetuti verso il nodo successivo).

5.2 Tecniche ad accesso casuale

Le tecniche ad *accesso casuale* non prevedono forme di coordinamento tra i nodi che condividono uno stesso canale. Non esiste nessuna gerarchia tra i nodi (assenza di nodi primari) ed ogni nodo gestisce l'accesso al canale condiviso esattamente nello stesso modo di tutti gli altri ed operando indipendentemente da essi. In particolare, ogni volta che un nodo ha informazione (dati) da trasmettere, appena possibile (in alcuni casi il nodo controlla preventivamente la presenza di trasmissioni in atto nel canale), effettua il tentativo di accesso al canale. Se più di un nodo prende contemporaneamente la stessa decisione di accesso al canale, si ha una collisione tra le singole trasmissioni e quindi la perdita dell'informa-

zione. Quando l'evento collisione accade, i vari protocolli, con funzionalità certe volte diverse, devono:

- Riconoscere quando una collisione è avvenuta;
- Risolvere la collisione portando a buon fine la trasmissione dell'informazione.

Il modo secondo cui le due funzioni precedenti vengono implementate caratterizzano le singole tecniche ad accesso casuale. In questo ambito le due tecniche più note ed utilizzate sono la tecnica Aloha e la tecnica CSMA (Carrier Sensing Multiple Access).

5.2.1 Aloha

La tecnica Aloha è stata il primo esempio di una metodologia pratica per far condividere un canale da più utenti senza coordinamento reciproco. Questa tecnica è stata, nella sua versione base, sviluppata all'Università delle Hawaii nei primi anni '70 principalmente per permettere la condivisione di un canale radio (wireless) tra più dispositivi (nodi) per accedere ad uno stesso host. La tecnica Aloha adotta una trasmissione dati a pacchetti (si inviano le informazioni strutturate in blocchi di bit di dimensioni fissate) e non è previsto nessun controllo dello stato del canale (libero/occupato) trasmisivo al momento del tentativo di accesso (Hammond'1986, Tanembaum'2011 in 5.3). Esistono due versioni di questa tecnica:

- i Aloha Puro;
- ii Aloha Slotted.

Aloha Puro

Questa versione della tecnica Aloha non prevede, in maniera assoluta, nessuna forma di coordinamento tra i nodi che condividono il canale. Ogni nodo quando ha necessità di accedere al canale effettua il suo tentativo in maniera del tutto indipendente dal comportamento degli altri nodi. Le collisioni vengono rivelate adottando un metodo di riscontro diretto. In generale i nodi della rete condividono uno stesso canale per comunicare con uno stesso nodo detto nodo centrale (sotto opportune condizioni questo vincolo può comunque essere rimosso). Le componenti di una rete di accesso basata sulla tecnica Aloha sono illustrate nella figura 5.2. Se la trasmissione di un pacchetto ha avuto successo (senza collisione) il nodo centrale è in grado di interpretare l'informazione ricevuta e di abilitare l'invio della conferma di corretta ricezione (messaggio di riscontro) in modalità broadcast (verso tutti i nodi della rete). Il ritardo che passa dal completamento di un tentativo di accesso da parte di un nodo e l'eventuale arrivo del messaggio di riscontro (timeout) è noto a priori e fa parte dei parametri di progetto della rete. Come conseguenza di questo abbiamo che solo il nodo interessato a conoscere

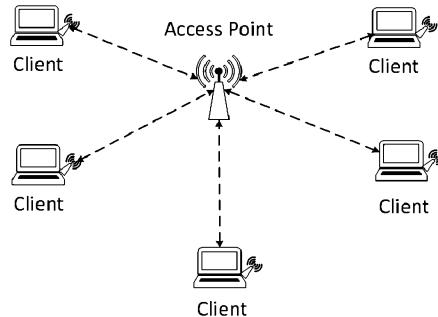


Figura 5.2: Componenti di una rete Aloha

l'esito del tentativo effettuato si metterà in ascolto sul canale broadcast (distinto da quello condiviso) per verificare la presenza del messaggio di riscontro. La mancata ricezione dello stesso rappresenta una notifica implicita del fallimento del tentativo di accesso ed attiva nei nodi interessati, almeno due, la modalità *risoluzione della collisione*. Ogni nodo della rete può gestire la trasmissione di un solo pacchetto: ogni nodo non può iniziare un nuovo tentativo di accesso, se ne ha un altro in corso, fino a quando questo non è stato completato con successo. La modalità di risoluzione di una collisione è ovviamente finalizzata ad evitare che se ne verifichino di nuove. Per questo motivo i nodi coinvolti non possono accedere immediatamente al canale appena dopo il termine del timeout altrimenti genererebbero una sequenza infinita di collisioni (loop). Per evitare questo, è quindi necessario prevedere, per i nodi interessati da una collisione, meccanismi di programmazione dei nuovi accessi che evitino o rendano minima la probabilità di una nuova collisione. La metodologia utilizzata a questo fine consiste nell'effettuare il nuovo accesso con un ritardo casuale che ogni nodo coinvolto seleziona in maniera indipendente dagli altri. Più precisamente nel caso di Aloha Puro viene individuato, per tutte le stazioni un tempo di ritardo massimo (tempo di back-off), contato dal termine del timeout, entro cui il nuovo tentativo deve essere effettuato. Entro questo intervallo la selezione dell'istante del nuovo accesso viene effettuato secondo un criterio statistico con probabilità uniforme. In alcune versioni della tecnica Aloha Puro l'ampiezza dell'intervallo di back-off non è costante ma può variare, (può essere aumentato o ridotto), entro un intervallo di variazione massimo predefinito in maniera da non penalizzare eccessivamente i tentativi di accesso successivi ad una collisione ed allo stesso tempo rendere meno probabile nuove collisioni.

Aloha Slotted

La versione slotted della tecnica Aloha è stata proposta come conseguenza della critica mossa alla versione Aloha Puro di un basso utilizzo della capacità del canale condiviso (pari al 18%). In particolare con la versione Slotted si riesce a raddoppiare l'utilizzazione del canale condiviso (36% della capacità nominale).

le) rimuovendo il vincolo di una assenza assoluta di coordinamento tra i nodi della rete. Nel caso dell'Aloha Slotted ogni nodo non può più accedere al canale ogniqualvolta decide di farlo (modalità asincrona) ma deve rispettare precisi vincoli temporali (modalità sincrona) che comportano una sincronizzazione temporale tra tutti i nodi della rete. In altre parole il tempo è pensato suddiviso in intervalli temporali regolari e costanti detti *slot* di durata uguale al tempo di trasmissione di un pacchetto. I nodi possono tentare l'accesso al canale solo in corrispondenza degli istanti di inizio slot. Con questo meccanismo, il *tempo di vulnerabilità*, cioè il tempo entro cui un qualsiasi altro tentativo di accesso da parte di altri nodi della rete provoca la collisione con un tentativo in corso che, nel caso dell'Aloha Puro, è due volte il tempo di pacchetto, si dimezza nel caso dell'Aloha Slotted (diviene uguale al tempo di pacchetto) come conseguenza del coordinamento temporale sugli accessi (diventano determinanti ai fini di una collisione solo le richieste di accesso dei nodi originate nel tempo di slot precedente quello su cui l'accesso viene tentato). Il meccanismo di riconoscimento di una collisione e la conseguente modalità di risoluzione delle collisione, una volta rilevata, è simile a quello utilizzato nella versione Aloha Puro con l'unica variante legata al vincolo temporale (sincronizzazione) sull'accesso al canale condiviso.

5.2.2 CSMA

La tecnica CSMA prevede che ogni nodo ascolti il canale prima di effettuare il tentativo di accesso. Si basa sul principio "*ascolta prima di parlare*" : quando più persone partecipano ad una discussione prima di esprimere il proprio punto di vista sull'argomento oggetto della discussione ognuno aspetta che chi ha la parola termini la sua esposizione. Mutuando questa modalità nel contesto di una comunicazione tra nodi di rete attraverso un canale condiviso, si può dire che ogni nodo prima di iniziare l'accesso al canale ne verifica preventivamente la disponibilità. Questo meccanismo in pratica consiste nell'effettuare la ricerca nel canale di un segnale alla frequenza della portante (Carrier Sensing). Quando, a seguito di un ascolto, un nodo rivela la presenza del segnale portante, non procede alla fase di accesso ed, in genere, interpreta questo evento come una *collisione virtuale*. Esistono diverse varianti della tecnica con rilevamento (sensing) della portante, di seguito discuteremo più nel dettaglio le metodologie:

- CSMA 1-persistent;
- CSMA non-persistent;
- CSMA p-persistent;
- CSMA con Collision Detection;

nel capitolo dedicato alle reti wireless analizzeremo poi nel suo contesto applicativo specifico una ulteriore variante denominata CSMA con Collision Avoidance. Tutte le varianti della tecnica CSMA elencate in precedenza hanno a comune la modalità con cui si tenta di risolvere una collisione dopo che questa è stata rilevata. Come nel caso della tecnica Aloha (anche in questo caso un nodo non

può gestire la trasmissione multipla di pacchetti diversi) si utilizza la riprogrammazione statistica dei nuovi tentativi entro l'intervallo di back-off il quale, a sua volta, può avere un valore variabile e dipendente dal contesto (es.: numero di collisioni successive rilevate).

Il meccanismo di ascoltare il canale prima di effettuare l'accesso potrebbe, a prima vista, apparire come una metodologia ideale per evitare le collisioni. Purtroppo, nonostante siano evidenti i vantaggi che comporta il suo uso, non si riesce ad evitare completamente che le collisioni avvengano. Questa perdita di idealità è principalmente dovuta ai ritardi di propagazione (in genere piccoli ma finiti) del segnale nel mezzo fisico. Questi, a loro volta, danno luogo ad un ritardo tra l'istante di inizio di una accesso e l'istante in cui tutti gli altri nodi della rete possono rivelarlo. Ad esempio, può capitare che due nodi tra loro separati da un tempo τ (propagazione del segnale) entrino in ascolto ad istanti che differiscono tra loro meno di τ . In questo caso, entrambi i nodi, trovando il canale libero, decideranno di accedere al canale dando così luogo ad una collisione. In pratica l'efficacia dell'ascolto del canale da parte di un nodo è considerata tanto maggiore quanto minore è il tempo di propagazione massimo (*tempo di vulnerabilità*) tra i due nodi fisicamente più distanti. In particolare, per migliorare le prestazioni delle tecniche CSMA, si richiede che il tempo massimo di propagazione nella rete sia molto piccolo nei confronti del tempo di trasmissione di un pacchetto. Questo requisito pone quindi dei limiti all'estensione massima (fisica) della rete e/o alla sua velocità di accesso.

CSMA 1-persistent

Quando un nodo ha un pacchetto da trasmettere ascolta preventivamente il canale per rilevare la presenza del segnale portante. Se il canale viene rilevato libero, il nodo completa il suo tentativo di accesso. Per rilevare una eventuale collisione (dovuta ai tempi di propagazione nella rete) il nodo, completata la trasmissione, resta in ascolto del canale per un tempo fissato (almeno uguale al massimo valore del tempo di propagazione). Se non viene rilevata nessuna attività nel canale la trasmissione si considera andata a buon fine ed il nodo può iniziare di nuovo la procedura di accesso per procedere ad una ulteriore trasmissione. Viceversa, se viene rilevata attività, significa che almeno un altro nodo, non rilevato nella fase di ascolto preventiva, ha deciso di accedere al canale provocando una collisione. Rilevata la collisone, i nodi interessati entrano nella modalità *risoluzione di collisione* attivando la procedura di back-off. Se invece la fase di ascolto preventivo rivela presenza di segnale nel canale, il nodo non completa il suo accesso e continua a controllare (ascolto) il canale. Non appena lo riconosce come libero, procede alla trasmissione del proprio pacchetto senza ritardi ulteriori. È evidente che questa modalità è efficace solo in presenza di un numero limitato di nodi (o limitate necessità di accesso) in quanto se accade che almeno un altro nodo si viene a trovare nelle stesse condizioni (ascolto continuo del canale) inevitabilmente si ha collisione.

CSMA non-persistent

Questa metodologia prevede che quando un nodo rileva il canale occupato considera questo evento come una *collisione virtuale* e riprogramma il nuovo tentativo di accesso in accordo alla modalità di risoluzione delle collisioni (in maniera casuale). In questo modo si risolve la situazione critica precedente ma, come è evidente, si introduce un ritardo, certe volte inutile, per ogni accesso successivo. Questo meccanismo può quindi essere efficiente in reti dense (con un elevato numero di nodi) ma non è adatto a reti con nodi e/o richieste di accesso, marcatamente sporadiche.

CSMA p-persistent

Questa tecnica cerca di unire i vantaggi delle due precedenti e di eliminarne gli svantaggi. Essa opera esclusivamente nella modalità slotted e, come ogni altra tecnica CSMA, prevede l'ascolto preventivo del canale prima di ogni accesso (prima trasmissione o trasmissioni conseguenti a collisioni) dopodiché si attiva la seguente procedura:

- se il canale è riconosciuto libero il nodo prende la decisione riguardo l'accesso su base statistica (distribuzione di Bernoulli): con probabilità p decide di trasmettere il proprio pacchetto mentre con probabilità complementare $q = 1 - p$ desiste dall'accesso e si mette in ascolto per decidere se accedere o meno al canale sullo slot successivo;
- se il nuovo tentativo di ascolto ha dato esito positivo (canale libero) si riattiva la procedura statistica di decisione riguardo l'accesso al canale;
- ogni volta che il canale è riconosciuto come occupato si considera questo evento come una *collisione virtuale* e di conseguenza il nodo attiva la modalità di risoluzione della stessa.

La predente procedura viene eseguita fino a quando la trasmissione del pacchetto non ha avuto buon fine. Questa tecnica si presta poi ad una ottimizzazione delle prestazioni finalizzata ad individuare il valore ottimo di p in relazione a specifiche condizioni di contesto (numero di nodi, necessità di accesso, ecc.).

La figura 5.3 mostra i diagrammi di flusso (flow chart) relative alle procedure di gestione dell'accesso per le tecniche CSMA descritte in precedenza.

CSMA con Collision Detection

In tutte le tecniche CSMA fino a qui esaminate un nodo che accede al canale condiviso non è in grado di rilevare eventuali collisioni durante il completamento della fase di accesso. Questo meccanismo prevede che i nodi controllino il canale anche durante la fase di accesso (e non solo al suo completamento) al fine di rilevare prontamente una collisione ed interrompere quindi immediatamente il tentativo di accesso in corso evitando il completamento di trasmissioni inutili (risparmio di potenza, tempo, banda). Il principio su cui si basa la tecnica

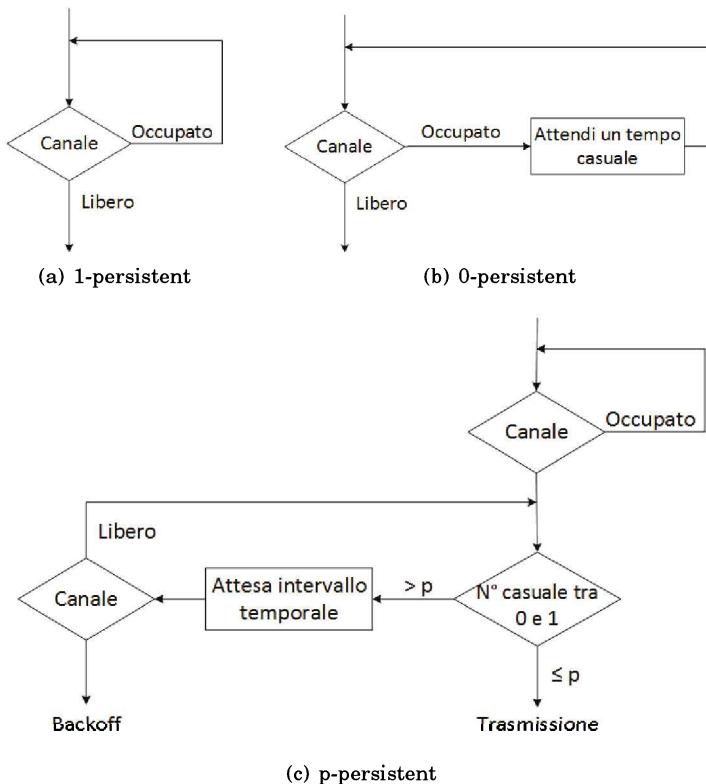


Figura 5.3: Procedure di accesso per le tecniche CSMA 1-persistente, non-persistente e p-persistente

CSMA/CD è "*ascolta prima di parlare e mentre parli*". Riprendendo l'analogia citata all'inizio di questo paragrafo si può dire che durante un colloquio tra più persone oltre che aspettare il proprio turno per esternare la propria opinione, siamo anche pronti ad interromperla se ci accorgiamo che la nostra voce è sovrapposta a quella di altri. Nel caso di nostro interesse un nodo che inizia una fase di accesso rimane in ascolto del canale durante la trasmissione del pacchetto. Se nel canale si rilevano variazioni di potenza durante la fase di accesso, il nodo si accorge che la sua trasmissione è interferita da altre (collisione) e quindi la interrompe istantaneamente. Prima di attivare la modalità di risoluzione della collisione, i nodi interessati dalla stessa inviano nel canale per un tempo limitato un segnale di disturbo (*jamming*) per fare in modo che tutti gli altri nodi si accorgano della collisione che potrebbe essere nascosta da fenomeni dovuti ad attenuazioni eccessive introdotte dal mezzo fisico di collegamento (si veda Tanembaum'2011, Forouzan'2007 in 5.3). Il tempo impiegato per rilevare una collisione con la modalità *collision detection* nel caso peggiore può essere assunto (con buona approssimazione) uguale al doppio del massimo valore del tempo di

propagazione e quindi significativamente inferiore tempo di trasmissione di un pacchetto.

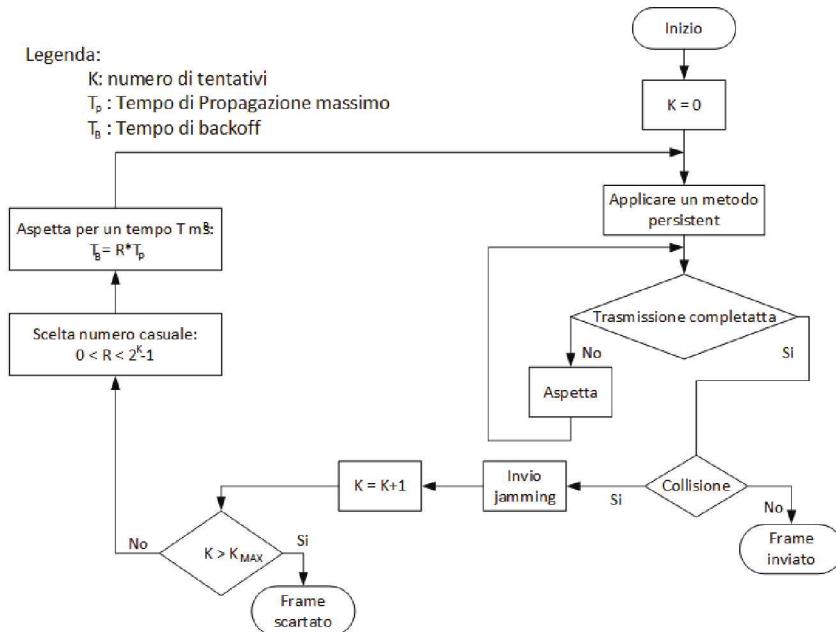


Figura 5.4: Procedura di accesso per la tecnica CDMA/CD

La figura 5.4 mostra il diagramma di flusso (flow chart) relativo alle procedure di gestione dell'accesso per le tecniche CSMA/CD descritte in precedenza.

5.3 Letture consigliate

Per approfondire le metodologie di accesso ad un canale condiviso si può fare riferimento a:

J.L. Hammond, P.J.P. O'Reilly, *Performance Analysis of Local Computer Networks*, Addison Wesley, 1986.

M. Schwartz, *Telecommunication Networks*, Addison Wesley, 1987.

B.A. Forouzan, *Reti di Calcolatori e Internet*, McGraw-Hill, 2007.

A.S. Tanenbaum, D.J. Wetherall, *Reti di Calcolatori*, Pearson, 2011.

D. Marabissi, D. Tarchi, R. Fantacci, *Adaptive OFDMA Systems*, River Publisher, 2008.

Si consiglia inoltre di consultare i documenti RFC citati nel teso ed il sito web: ieeexplore.ieee.org.

6

Rete Ethernet

La rete Ethernet è nata intorno alla metà degli anni settanta grazie a Robert Metcalfe e David Boggs ricercatori della Xerox. Dalla loro invenzione queste reti hanno continuato ad evolversi e a migliorarsi fino a diventare la tecnologia predominante per le reti LAN. L'evoluzione di queste reti è avvenuta tramite quattro generazioni: Ethernet standard (con una velocità di trasferimento di 10 Mbps), Ethernet veloce (con velocità di trasferimento di 100 Mbps), Ethernet gigabit (con velocità di trasferimento di 1 Gbps) e l'ultima Ethernet 10-gigabit (velocità di trasferimento 10 Gbps). Ethernet è stata standardizzata dall'IEEE con norme indicate con la sigla IEEE 802.3 per definire le sole specifiche tecniche del livello fisico e del livello MAC. Una rete Ethernet può avere una topologia a bus o a stella (per maggiori informazioni vedere il paragrafo 1.3) e può funzionare sia su cavo coassiale, doppino telefonico o fibra ottica. La tecnologia Ethernet è, ad oggi, la più utilizzata in reti LAN cablate. Le ragioni di questa posizione dominante sono molteplici, tra esse si cita la possibilità di trasferire flussi informativi con un rate elevato ed una migliore flessibilità di gestione e manutenzione rispetto ad altre alterative (es.: reti FDDI).

6.1 Livello MAC

Il livello MAC della rete Ethernet ha come compito primario la gestione dell'accesso al canale: la tecnica adoperata è la CSMA/CD con modalità 1-persistent. La tecnica di risoluzione delle collisioni è basata sull'algoritmo Binary Exponential Backoff descritto in precedenza. Tutte le tecnologie Ethernet (vedi testi elencati in 6.5) forniscono al livello di rete un servizio senza connessione: ovvero quando due host iniziano una comunicazione su una rete Ethernet, il mittente incapsula il datagramma in un frame Ethernet e lo invia al destinatario senza effettuare alcun collegamento preventivo (*handshake*) per concertare alcuni parametri della connessione con il destinatario. Inoltre, tutte le generazioni Ethernet forniscono un servizio inaffidabile al livello di rete. In particolare quando il destinatario riceve il pacchetto esso non invia nessun messaggio di riscontro al mittente, né in caso di esito positivo della ricezione né in caso negativo. Se il frame ricevuto non supera il controllo con il CRC, (Cyclic Redundancy Check), ovvero *codice di controllo di errore a ridondanza ciclica*, il destinatario semplicemente lo scarta. Questo implica che i livelli superiori, quando previsto e/o necessario, devono pre-

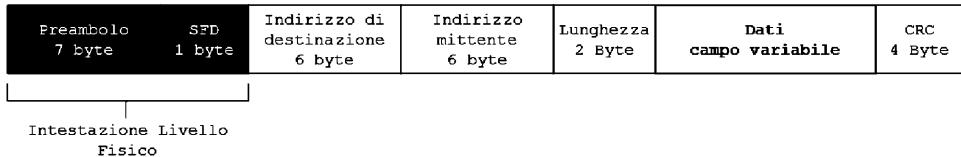


Figura 6.1: Formato del frame IEEE 802.3

vedere qualche tecnica per il controllo dell'integrità dell'informazione ricevuta (rilevazione e correzione degli errori) che consenta di sopportare alla mancanza di affidabilità della rete Ethernet.

Formato frame

La peculiarità di Ethernet è che in tutte le generazioni e per le diverse tecnologie trasmissive previste, il formato del frame è lo stesso. In particolare per il livello MAC è prevista una dimensione minima di 64 byte ed una massima di 1518 byte. *Curiosità:* il frame Ethernet viene chiamato DIX, dalle iniziali dei tre partner che hanno dato vita a Ethernet: DEC, Intel e Xerox. Il formato del frame 802.3 è mostrato in figura 6.1.

I significati dei vari campi sono i seguenti:

- *Preamble:* contiene sette byte, con i bit di valore 0 o 1 che si alternano per annunciare al destinatario l'arrivo del frame e per consentirne la sincronizzazione. La ripetizione delle sequenze serve per permettere la sincronizzazione del destinatario anche quando si perde la sua parte iniziale;
- *Start Frame Delimiter (SFD):* è un campo formato da un solo byte con struttura definita e fissa: 10101011. Questo byte segnala l'inizio del frame ed è l'ultima possibilità per il ricevitore di sincronizzarsi correttamente. Preamble e SFD fanno parte dell'intestazione del livello fisico;
- *Indirizzo di destinazione:* specifica l'indirizzo fisico del (o degli) host di destinazione. È un campo di 6 byte;
- *Indirizzo sorgente:* identifica l'indirizzo fisico dell'host mittente. È anche questo un campo di 6 byte;
- *Lunghezza:* è un campo di 2 byte. Si utilizza per specificare o la lunghezza del campo payload o il tipo di dati trasportati;
- *Payload:* è il campo che contiene i dati veri e propri, provenienti dai livelli superiori. Questo campo ha una lunghezza minima di 46 byte e una massima di 1500 byte. Il massimo valore trasportabile dal payload rappresenta l'MTU (Maximum Transmission Unit);

- **CRC:** è il campo che contiene il codice a ridondanza ciclica per il rilevamento degli errori.

La restrizione sulla lunghezza minima del payload è necessaria per avere un corretto funzionamento del metodo di accesso al canale. Nella rete Ethernet classica a 10 Mbps il tempo necessario affinché un nodo si accorga che ci sia stata una collisione è pari a $51,2 \mu s$ e questo vuol dire spedire 512 bit ovvero 64 byte. Dunque, se i livelli superiori inoltrano un datagramma con una dimensione minore di 46 byte, si rende necessario l'uso di byte di riempimento.

Molto simile è anche la motivazione alla base della definizione della dimensione massima del payload la quale è dovuta alla iniziale necessità di contenere i costi delle memorie (buffer) utilizzate per la gestione delle comunicazioni (vedi Tanembaum'2011 in 6.5): introducendo un limite massimo alla lunghezza di frame si riusciva a ridurre la capacità massima di memorizzazione dei buffer e quindi il loro costo.

La lunghezza della rete dipende dalla velocità di propagazione del segnale e dai requisiti temporali della tecnica CSMA/CD. Tipicamente, per una rete Ethernet con velocità nominale di 10Mbps si considera una lunghezza massima di 2500 m.

6.2 Livello fisico

Il livello fisico cambia in relazione alla generazione Ethernet considerata ed, in alcuni casi, perfino nell'ambito di una stessa generazione di rete.

6.2.1 Ethernet standard

Tutte le implementazioni utilizzano segnali digitali su un canale la cui velocità di trasmissione è 10 Mbps. Il mittente converte i bit ricevuti in un segnale digitale utilizzando la codifica Manchester (si veda Forouzan'2007, Tanembaum'2011 in 6.5), la quale permette una sincronizzazione automatica e consente di prevenire errori causati dalla perdita della sincronizzazione del clock. Nella codifica Manchester ogni bit codificato contiene una transizione a metà del periodo di bit e la direzione della transizione determina se il bit è uno 0 o un 1.

In figura 6.2 sono mostrate le principali implementazioni di un a rete Ethernet. Nella nomenclatura in uso, ci si riferisce a sigle formate da tre campi: il primo termine indica la velocità di trasmissione, il secondo indica la banda utilizzata (BASE si riferisce ad una rete Ethernet in banda base) ed infine il terzo si riferisce alla tipologia del mezzo fisico utilizzato per i collegamenti (es.: T si riferisce ai classici doppini di rame intrecciati (UTP)).

Nell'implementazione **10Base5** il cavo usato per la comunicazione è un cavo coassiale grosso, ovvero un cavo il cui diametro è sufficientemente grande da risultare un cavo rigido. Questa è stata la prima implementazione di Ethernet e si basa su un modulo di trasmissione/ricezione esterno che è responsabile della trasmissione, della ricezione e del rilevamento delle collisioni. È consentito avere una lunghezza massima del canale di 500m senza ripetitori; nel qual caso si

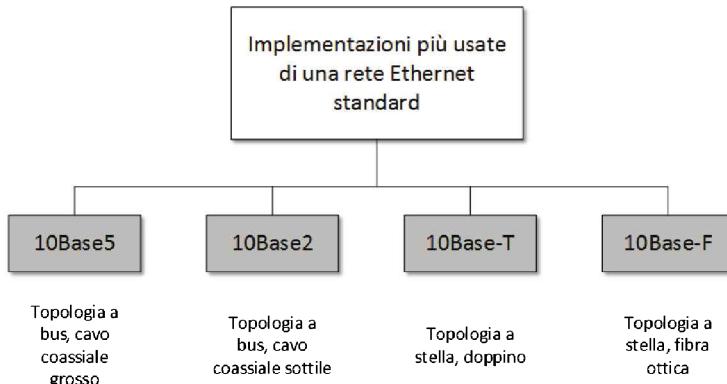


Figura 6.2: Reti Ethernet standard

volesse allungare la copertura è permesso l'uso dei ripetitori, fino ad un massimo di cinque segmenti collegati.

Nella rete **10Base2** il cavo adoperato è un cavo coassiale sottile e molto flessibile. In questo caso l'installazione è molto più semplice grazie alla flessibilità del cavo stesso, ma ciò introduce anche un limite notevole nella massima lunghezza tra due terminali: non deve superare i 185m.

Nella rete **10Base-T**, il mezzo utilizzato è un doppino. Ogni nodo viene collegato con un hub centrale dunque la topologia che si viene a creare è una stella. Per la trasmissione e la ricezione sono presenti due distinti doppini, quindi le collisioni, se avvengono, sono localizzate nell'hub centrale. La lunghezza massima ammessa per il doppino è di 100m.

Nella rete **10Base-F** il mezzo adoperato è la fibra ottica. Anche in questo caso sono presenti due collegamenti, uno per la ricezione e l'altro per la trasmissione e entrambi sono collegati ad un hub centrale.

6.2.2 Ethernet veloce

È una evoluzione di Ethernet standard (Tanembaum'2011, Forouzan'2007, Ku-rose'2013, Stallings'2000 in 6.5) nata per competere con le reti FDDI (vedere paragrafo 4.9); è stata standardizzata dall'IEEE con il nome 802.3u. Queste reti hanno una velocità di 100 Mbps e sono retrocompatibili con le pre-esistenti reti Ethernet standard, in particolare, esse prevedono lo stesso formato del frame e lo stesso spazio di indirizzamento (in pratica è stata aumentata la velocità di trasferimento e lasciato inalterato il sottolivello MAC). Per questa versione di rete Ethernet non è prevista la topologia a bus. Le reti Ethernet veloci ammettono solo una topologia a stella con collegamenti o half-duplex o full-duplex. Nel primo caso i nodi sono connessi attraverso gli hub (descritti di seguito) e il metodo di accesso al canale è di tipo CSMA/CD; nel secondo caso i nodi sono connessi attraverso degli switch (descritti di seguito) e, sebbene non sia necessario

nessun meccanismo di gestione dell' accesso al canale, per mantenere la compatibilità con le reti Ethernet standard, viene comunque implementata la tecnica CSMA/CD.

Ethernet veloce introduce il concetto di autonegoziazione, ovvero due nodi della rete possono negoziare tra di loro alcuni parametri come la velocità di trasmissione dei dati. Anche in Ethernet veloce (Tanembaum'2011, Forouzan'2007, Kurose'2013, Halsall'1996 in 6.5) esistono più implementazioni del livello fisico. In particolare, si ha:

- 100Base-TX: costituito da due doppini UTP di categoria 5 e con schema di codifica MLT-3. Poiché tale codifica non è autosincronizzante viene utilizzata anche la codifica 4B/5B.
- 100Base-FX: costituito da due cavi in fibra ottica ed utilizza come schema di codifica il NRZ-I. Anche in questo caso, per sequenze lunghe di uno stesso bit, la codifica non è autosincronizzante e quindi viene aggiunta la codifica 4B/5B.
- 100Base-T4: costituito da quattro doppini e la codifica adoperata è la 8B/6T

Per maggiori dettagli e approfondimenti riguardo le forme di codifica citate precedentemente si faccia riferimento ai testi indicati come letture consigliate al termine del capitolo.

6.2.3 Ethernet gigabit

Standardizzato dall'IEEE con il numero 802.3z, porta la velocità di trasferimento fino al gigabit e mantiene la retrocompatibilità con le versioni precedenti. L'aumento di velocità di trasferimento ha introdotto delle modifiche a livello MAC rispetto alle due versioni precedenti. In questa versione sono previste le due modalità seguenti:

- **half-duplex**: la topologia che si forma è o punto-punto, se siamo in presenza di due soli terminali, oppure una stella se si hanno più dispositivi; il centro stella è rappresentato da un hub (si veda paragrafo 6.3). La tecnica di accesso al canale è una CSMA/CD, quindi all'interno dell'hub si possono verificare delle collisioni quando sono presenti contemporaneamente almeno due segnali su ingressi diversi. Poiché viene utilizzata la metodologia CSMA/CD, la lunghezza massima dei collegamenti dipende dalla dimensione minima dei frame. Nella modalità half-duplex sono stati definiti tre tipi di frame:

- *frame tradizionale*: la lunghezza del frame è uguale a quella di Ethernet standard. Poiché il tempo di bit, in questa generazione, è un centesimo del tempo di bit di IEEE 802.3, l'intervallo temporale necessario per rilevare una collisione è di $0.512 \mu s$ e questo implica che la lunghezza massima della rete non debba superare i 25 m;

- *frame esteso*: per aumentare l'estensione fisica della rete si aumenta la lunghezza minima del frame, da 64 byte si passa a 512 byte, ricorrendo a bit di riempimento quando i frame sono più piccoli della dimensione minima. In questo modo la lunghezza massima della rete diventa 200 m;
- *frame a burst*: nel caso in cui si debbano trasmettere datagrammi di piccole dimensioni, l'uso del frame esteso risulta poco conveniente. Per migliorare l'efficienza si inviano, consecutivamente, più frame, in modo da limitare il ricorso ai bit di riempimento.
- **full-duplex**: la topologia che si forma è o punto-punto, se siamo in presenza di due soli terminali, oppure a stella se si hanno più dispositivi: tutti i nodi sono connessi ad uno switch centrale il quale ha al suo interno dei buffer, uno per ogni porta. I buffer servono per memorizzare i frame prima di essere inoltrati verso la loro destinazione finale. Nella rete full-duplex non vi sono collisioni e dunque la lunghezza massima del cavo dipende solo dall'attenuazione dello stesso (Kurose'2013 in 6.5).

Esistono quattro implementazioni diverse del livello fisico per Ethernet gigabit, esse sono:

- 1000Base-SX e 1000Base-LX: utilizzano due fibre ottiche ed una codifica NRZ insieme ad uno schema di codifica 8B/10B. Si differenziano a seconda della lunghezza massima della rete: SX permette una lunghezza massima di 550m mentre le reti che usano LX arrivano ad avere estensione fino a 5 Km;
- 1000Base-CX: utilizza due doppini STP ed utilizza una codifica NRZ insieme allo schema di codifica 8B/10B;
- 1000Base-T: utilizza quattro doppini UTP ed è stata progettata per quei casi in cui esiste già un cablaggio che utilizza gli stessi doppini. La codifica utilizzata è 4D-PAM5.

6.2.4 Ethernet 10-gigabit

Standardizzato con il nome IEEE 802.3ae; con questo standard si aumenta la velocità di trasferimento, cercando, per quanto possibile, di mantenere la retrocompatibilità con le precedenti generazioni. Tutte le versioni di una rete Ethernet a 10 Gbps ammettono solo la modalità full-duplex, di conseguenza il protocollo CSMA/CD non è previsto nello standard. Il livello fisico si differenzia in: 10GBase-E, 10GBase-L, 10GBase-S. Tutte e tre usano due cavi ottici, si differenziano a seconda della lunghezza massima della rete (la versione E è quella che permette un'estensione maggiore, intorno ai 40 Km mentre la versione S è quella che permette l'estensione minore, intorno ai 300 m).

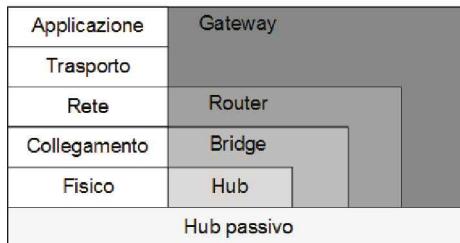


Figura 6.3: Dispositivi di connessione

6.3 Dispositivi di connessione

Per far comunicare tra loro LAN distinte o per connettere una LAN con la rete globale vengono utilizzati opportuni dispositivi di connessione. I dispositivi si distinguono a seconda del livello protocollare ISO/OSI in cui lavorano. Una visione grafica è mostrata in figura 6.3.

6.3.1 Hub passivi

Come si può notare dalla figura 6.3 questi dispositivi operano sotto il livello fisico direttamente a livello di canale di collegamento. In pratica essi sono dei connettori fisici che permettono la continuità di segnale tra cavi di rete distinti permettendo quindi di aumentare l'estensione della rete senza tuttavia attuare nessuna forma di elaborazione sul segnale trasmesso (l'estensione sarà quindi limitata dal livello di attenuazione del segnale).

6.3.2 Ripetitori e Hub attivi

Un ripetitore è un dispositivo che interconnette, a livello fisico, due segmenti di una sottorete. Esso è molto utile poiché permette di aumentare l'estensione di una rete. In reti cablate (wired), l'estensione fisica dipende dall'attenuazione che il segnale subisce nel mezzo fisico di collegamento, quando tale attenuazione risulta eccessiva si pregiudica pesantemente l'integrità dei frame ricevuti. I ripetitori devono essere disposti nella rete in modo che sia possibile ricevere un segnale prima che la sua attenuazione diventi eccessiva e non più controllabile. Il ripetitore ha il compito di rigenerare il segnale attenuato ricevuto e ripeterlo nuovamente nella rete. Il ripetitore quindi in pratica realizza una connessione fisica "attiva" tra due segmenti di una stessa LAN, permettendo di estenderne la lunghezza fisica. Un ripetitore, pur non essendo un amplificatore di tipo tradizionale (prende decisioni riguardo i bit ricevuti e li ripete sulla sua uscita nel loro formato originale), non ha, comunque, alcuna possibilità di selezionare i frame in ingresso (ripete quindi in uscita anche i frame non destinati al segmento di LAN successivo). In sintesi posiamo dire che l'hub non è altro che un ripetitore multi-porta. Quando un frame arriva a un'interfaccia, l'hub rigenera i suoi bit, amplifica la sua potenza e lo ripete su tutte le altre porte. La topologia di

connessione è tipicamente a stella e viene preservata la natura broadcast della rete Ethernet conseguenza della modalità operativa prima descritta. Quando più sezioni Ethernet sono interconnesse attraverso un hub si comportano come una unica LAN. In questo caso infatti quando sono presenti più frame in ingresso si ha collisione nell'espletare il processo di inoltro (ripetizione dei frame sulle uscite). Per contenere gli effetti negativi di questo fenomeno viene utilizzato il meccanismo CSMA/CD e quindi si introducono limitazioni sull'estensione massima della rete nel suo complesso.

6.3.3 Bridge

Il bridge opera fino al livello di collegamento (figura 6.3) e dunque può controllare gli indirizzi MAC. Controllando gli indirizzi, il bridge può prendere delle decisioni in base all'indirizzo sorgente e destinatario. La proprietà di filtrare i pacchetti (Kurose'2013, Tanembaum'2011,Halsall'1996 in 6.5) viene detto *filtering* mentre la capacità di inoltrare i frame è detta *forwarding*. Quando un pacchetto arriva al bridge, sulla base dell'indirizzo di destinazione e sorgente e di specifiche procedure, il bridge decide se il pacchetto deve essere scartato o ripetuto (inoltrato) sulle uscite. L'inoltro avviene consultando una tabella, chiamata *tavella del bridge*. Questa tabella è formata da due campi, in uno viene salvato l'indirizzo MAC di un dispositivo mentre nell'altro campo viene salvata la porta che collega il bridge allo stesso dispositivo. Il bridge interpreta l'indirizzo di destinazione del pacchetto e lo confronta con gli indirizzi presenti nella sua tabella. Se l'indirizzo del destinatario è stato precedentemente salvato, il bridge è in grado di inoltrare correttamente il pacchetto al destinatario. La configurazione della tabella avviene in modo dinamico: osservando il traffico in ingresso il bridge apprende la disposizione dei nodi a lui connessi.

Il punto debole di una interconnessione con bridge si manifesta nel caso di guasto dello stesso: se un bridge si rompe, tutta la sottorete si scollega dalla rete Internet. Per risolvere questo problema, si creano percorsi multipli ridondanti. In questo modo si risolve il problema del guasto, ma se ne genera un altro: i frame rischiano di seguire dei percorsi ciclici e di moltiplicarsi senza controllo. Per evitare questo il bridge definisce un albero ricoprente (*spanning tree*), cioè, i bridge si costruiscono una propria sottorete, con topologia ad albero, privo di anelli (cicli). Per la descrizione della procedura seguita per definire la struttura ad albero ricoprente si rimanda a Forouzan'2007 in 6.5. I bridge operano esclusivamente su base software per cui hanno bisogno di ricercare completamente un frame prima di elaborarlo. La modalità operativa classica è detta *store-and-forward* (si veda 6.3.5).

6.3.4 Switch

Con il termine switch si intende un dispositivo che opera fino al livello collegamento (figura 6.3). A differenza degli hub, gli switch di livello due, in maniera simile ai bridge, implementano le funzioni di memorizzazione ed inoltro. Lo switch è trasparente ai nodi della rete in quanto questi specificano solo l'indirizzo

del nodo destinazione. Lo switch riceve i frame sulle sue porte di ingresso e per poter gestire situazioni di conflitto legate a richieste contemporanee su ingressi diversi verso uno stesso uscita lo switch deve avere capacità di memorizzare i frame in buffer distinti, di solito tanti quante sono le uscite. La funzionalità base dello switch è detta *filtraggio*. Essa consiste nell'interpretazione della richiesta di ripetizione del frame sulle uscite e può comportare l'eliminazione del frame quando viene riscontrato un indirizzo di destinazione uguale a quello di arrivo (in questo modo si separano i domini di collisione). Se la fase di *filtraggio* ha esito positivo (cioè il frame non viene scartato) si attiva la fase di *inoltro* che consiste nell'indirizzare il frame verso l'interfaccia di uscita desiderata. Questa ultima operazione viene realizzata andando a leggere in una tabella interna gli abbinamenti interfaccia di uscita - destinazione finale del frame. Gli switch hanno una funzionalità molto utile quella dell'*autoapprendimento* per quanto riguarda la definizione delle tabelle di inoltro. Questa procedura viene realizzata attraverso i seguenti passi (Tanembaum'2011, Kurose'2013, Forouzan'2007 in 6.5):

- la tabella inizialmente non ha contenuti (vuota);
- Ogni volta che lo switch riceve un frame per la prima volta registra nella tabella l'indirizzo del mittente e lo associa alla porta attraverso la quale è stato ricevuto. In questo modo lo switch autoapprende che tutti i frame che avranno come indirizzo di destinazione quello del mittente registrato dovranno essere inoltrati sulla interfaccia di uscita abbinata. Quando tutti i nodi della rete avranno inviato per la prima volta un frame lo switch avrà completato il suo periodo di autoapprendimento;
- Se trascorso un tempo di riferimento (tempo di invecchiamento) lo switch non ha ricevuto frame da un dato indirizzo questo viene eliminato alla tabella di inoltro in quanto il nodo associato non è considerato attivo. Questa procedura è utile per gestire le fasi di aggiornamento degli apparati di rete.

Gli switch, possono operare, oltre che con la modalità descritta *store-and-forward*, che evita di inoltrare i frame difettosi (con errori) ma è più lenta, anche in modalità *cut-trough*, come i *router*, più veloce ma che può provocare la perdita di frame. Entrambe queste tecniche sono descritte con più dettaglio nel paragrafo 6.3.5 .

Confronto tra Bridge e Switch

I bridge e gli switch hanno funzionalità simili in quanto usano gli indirizzi MAC all'inizio di ogni frame di livello collegamento per svolgere le operazioni di inoltro (commutazione). Tuttavia, si possono evidenziare le seguenti differenze funzionali:

- *Numeri di porte*: il bridge ha un numero di porte inferiore ad uno switch. Questa particolarità consente di realizzare tramite uno switch collegamenti con singoli nodi di rete, riducendo il dominio di collisione a valore minimi. Ovviamente con questa soluzione il numero di cavi cresce proporzionalmente con il numero di nodi e può diventare un parametro critico.

- *inoltro con destinazione sconosciuta* : quando non è nota la porta di uscita richiesta il bridge ripete il frame su tutte le porte eccetto quella di arrivo mentre lo switch non opera nessuna distinzione e ripete in broadcast il frame su tutte le porte;
- *tipologia di collegamento* : lo switch è un dispositivo *full duplex* per cui non esiste contesa per l'accesso ad una stessa porta di uscita.

6.3.5 Router

Il router è un dispositivo che lavora fino al livello rete (livello tre di OSI o IP di TCP/IP), quindi può controllare gli indirizzi logici propri di tale livello (figura 6.3). Un router, a differenza dei bridge e switch, processa i pacchetti ricevuti dal livello collegamento e li memorizza in un buffer (quando previsto dalla modalità operativa) e successivamente li elabora sfruttando le informazioni di testata di livello rete per effettuare l'inoltro del pacchetto secondo un opportuno criterio. Anche in questo caso le decisioni riguardo l'inoltro dei pacchetti sono prese sulla base di opportune tabelle dette *tabelle di routing*, definite ed aggiornate dinamicamente secondo opportuni algoritmi di *routing* che saranno argomento del capitolo 13. Gli elementi della tabella di instradamento non corrispondono, in genere, a singoli dispositivi ma ad intere reti. Un router in generale opera in accordo alle due seguenti modalità (Tanembaum'2011, Kurose'2013 in 6.5):

- *cut-through*: il router si limita a leggere l'indirizzo IP del destinatario e quindi manda il contenuto del pacchetto (es. IP) contemporaneamente alla sua acquisizione. In questo caso, quindi, per l'inoltro dei pacchetti verso le uscite non è necessario che sia completata la loro ricezione. Per evitare perdite o congestioni al dispositivo ricevente è necessario che il router sorgente e quello ricevente operino alla stessa velocità;
- *store-and-forward* : in questo caso il router memorizza il pacchetto ricevuto in un opportuno buffer prima di inoltrarlo verso l'uscita desiderata. Questo meccanismo consente di gestire meglio eventuali situazioni di congestione della rete prevenendo la perdita dei pacchetti.

Dal punto di vista architettonico un router prevede le seguenti componenti principali:

- **Porte di Ingresso** : svolgono compiti di livello fisico, di collegamento (se necessario) e provvedono ad estrarre l'informazione relativa alle richieste di inoltro ed inviarle al processore di instradamento.
- **Struttura di Commutazione** : è la componente preposta a trasferire un pacchetto (o datagramma) arrivato ad una porta di ingresso verso la porta di uscita richiesta. Può essere realizzata con tecnologie differenti: cross-bar, bus, a memoria.
- **Porte di Uscita** : svolgono funzionalità di livello fisico e collegamento gestendo la connessione con il successivo router o con una LAN direttamente

connessa. Prevedono dei buffer dove i pacchetti possono essere memorizzati in attesa dell' inoltro verso le loro destinazioni finali.

- **Processore di Instradamento:** Interpreta ed attua le richieste di instradamento interagendo con la tabella di inoltro propria del router e con la struttura di commutazione.
- **Tabella di Instradamento :** contiene le informazioni necessarie per legare una richiesta di inoltro ad una delle possibili porte di uscite. Deve poter consentire tempi di ricerca contenuti comparativamente con i tassi di trasmissione delle LAN gestite (es. con tassi di trasmissione dell'ordine dei Gbps si devono sostenere tempi di ricerca dell'ordine dei ns (nanosecondi)).

Confronto Switch e Router

Da quanto esposto in precedenza appare chiara l'analogia funzionale tra questi due dispositivi, come evidente è anche la differenza attuativa della stessa. Gli switch operano infatti a livello 2 mentre i router a livello 3. Questo di conseguenza comporta un maggior carico di lavoro per i router rispetto agli switch. Inoltre possiamo dire che :

- gli switch sono dispositivi plug-and-play mentre i router necessitano di interventi per poter essere configurati adeguatamente;
- entrambi consentono di limitare i domini di collisioni;
- i router permettono di inoltrare i frame secondo algoritmi ottimi non vincolati dalle restrizioni imposte dalla topologia ad albero ricoprente (spanning tree) necessaria per evitare i cicli nella rete.

6.3.6 Gateway

Molto spesso si trova il termine gateway come sinonimo di router; nella realtà il gateway è un dispositivo che opera a livello di rete e a livelli superiori e ha il compito principale di trasportare i pacchetti all'esterno di una rete locale. Il gateway ha anche un compito importante nella sicurezza delle reti LAN. Per maggiori dettagli riguardo i gateway si suggerisce di consultare i testi indicati nel paragrafo 6.5.

6.4 Un caso pratico : Il Proxy

Il proxy è un programma installato su una macchina, che si interpone tra il client e il server. Quando un client effettua una richiesta ad un server, in realtà la sua richiesta viene gestita prima dal proxy e poi dal server: una volta che il proxy ha ricevuto la richiesta dal client, la interpreta e poi la inoltra al server; una volta che ha ricevuto la risposta dal server la interpreta e la inoltra al client. La differenza sostanziale con tutti gli altri dispositivi è che la maggior parte dei

proxy lavorano a livello applicativo dunque un programma proxy deve essere in grado di gestire la maggior parte dei protocolli applicativi.

Un proxy può essere configurato per permettere ad una LAN di accedere alla rete globale, in questo caso il proxy (in cui si trova anche il firewall, vedi capitolo 15) funge da unica porta di ingresso/uscita tra le due reti. Inserendo un proxy come unico punto di uscita si aumenta anche la sicurezza degli utenti stessi, in quanto il proxy modifica l'indirizzo IP del mittente e dunque il server non sa quale utente ha realmente effettuato la richiesta. Il proxy può essere utilizzato anche per salvare in una memoria temporanea (cache) le richieste con le relative risposte dei vari client a lui associati. In questo modo, se un altro utente effettua una richiesta già presente in cache, il proxy può rispondere immediatamente. I proxy possono essere utilizzati anche per monitorare e controllare i vari utenti della rete LAN in quanto può analizzare, ed eventualmente bloccare, richieste e/o risposte che violano determinate regole dell'amministratore di sistema. Ovviamente se il proxy non supporta determinati protocolli applicativi alcune applicazioni risultano inutilizzabili.

6.5 Letture Consigliate

Per approfondimenti e complementi riguardo gli argomenti trattati in questo capitolo si suggeriscono come letture consigliate i seguenti testi (e i riferimenti bibliografici specifici indicati negli stessi):

J.F. Kurose, K.W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.

K.C. Mansfield, J.L. Antonakos, An Introduction to Computer Networking, Prentice Hall, 2002.

F. Halshaw, Reti di Calcolatori e Sistemi Aperti, Addison-Wesley, 1996.

B.A. Forouzan, Reti di Calcolatori e Internet, McGraw-Hill, 2007.

A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.

W. Stallings, Trasmissione Dati e Reti di Computer, Jackson Libri, 2000.

7

Reti wireless

Le reti wireless sono reti in cui i terminali sono collegati tra loro attraverso un canale radio. Il principale vantaggio di una rete wireless è la possibilità di un accesso ubiquo e pervasivo che consente, in particolare, la mobilità degli utenti. In una rete wireless le difficoltà maggiori, che per buona parte ne limitano l'impiego, derivano dalle caratteristiche del canale radio stesso che si manifestano con una maggiore difficoltà a garantire l'integrità dell'informazione trasmessa. Questo effetto negativo è dovuto al fatto che, in un collegamento radio, a differenza di un classico collegamento cablato, il canale di comunicazione è particolarmente ostile alla trasmissione dei segnali e presenta spesso caratteristiche che cambiano con il tempo. Un altro importante problema, tipico delle reti wireless, è dovuto alla scarsa garanzia di confidenzialità riguardo le informazioni scambiate in quanto, per la natura stessa del canale radio, queste sono maggiormente soggette ad intrusioni esterne. Nel suo complesso la tecnologia di comunicazione wireless può essere esaminata mediante un'analisi *SWOT*. Questa metodologia è usata per valutare comparativamente i punti di forza (*Strengths*), di debolezza (*Weaknesses*), le opportunità (*Opportunities*) e le minacce (*Threats*), di una tecnologia. Nel caso delle reti wireless il risultato dell'analisi *SWOT* è illustrata nella tabella 7.1.

La figura 7.1 nostra invece un confronto fra le differente tecnologie ad oggi possibili per le comunicazioni wireless in termini di banda nominale di accesso e estensione dell'area di servizio.

Strengths	Weakness	Opportunities	Threats
connettività ubiqua	banda di accesso minore rispetto alle reti cablate	applicazioni innovative	sicurezza limitata
costi minori	canale condiviso	accesso mobile	riservatezza
tecnologia matura	sensibilità interferenze	convergenza	

Tabella 7.1: Analisi SWOT

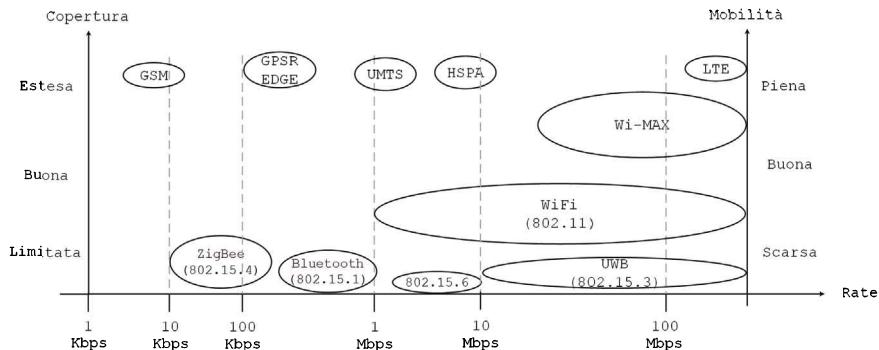


Figura 7.1: Reti wireless

7.1 IEEE 802.11

Lo standard IEEE 802.11, come ogni altro standard della famiglia IEEE 802, prende in considerazione solo specifiche proprie del livello fisico e del livello MAC. Comunemente questo standard è conosciuto con il nome di WiFi, dal nome *WiFi Alliance* dell'organizzazione internazionale che dal 1999, anno della sua nascita, ha come compito quello di standardizzare e certificare tutti gli apparati che possono essere utilizzati in reti a standard IEEE 802.11.

7.1.1 Architettura di rete

Una rete IEEE 802.11, è formata da una cella elementare, chiamata *set di servizio base* (in inglese **Basic Service Set**, BSS). Una BSS contiene uno o più terminali e una stazione base (*Base Station*, BS) che ha il compito di coordinare la rete. La BS nelle reti LAN wireless (WLAN) viene comunemente indicata con il nome di *Access Point* (AP). Una rete che prevede solo terminali (client) connessi unicamente all'AP viene detta *rete centralizzata* (o *rete infrastrutturata*): i terminali, possono essere sia fissi che mobili e possono comunicare tra di loro solo ed esclusivamente con il supporto dell'AP. A loro volta, gli AP possono essere collegati tra di loro mediante una sistema di distribuzione (*Distribution System*), spesso indicato con la sigla DS, solitamente costituito da una rete cablata (wired) Ethernet (descritta nel capitolo 6), per dar vita alla rete senza fili estesa (*Extended Service Set*), in sigla ESS.

L'architettura di rete centralizzata non è l'unica ammessa dallo standard. Una rete IEEE 802.11 ammette che i terminali, anche autonomamente, senza cioè interventi esterni diretti, si organizzino spontaneamente in una rete che può anche non prevedere collegamenti verso l'esterno (es.: connessioni con la rete Internet globale). Questa tipologia di architettura di rete è chiamata **rete ad hoc** ed ha, come particolarità, il fatto di non prevedere l'uso di un AP.

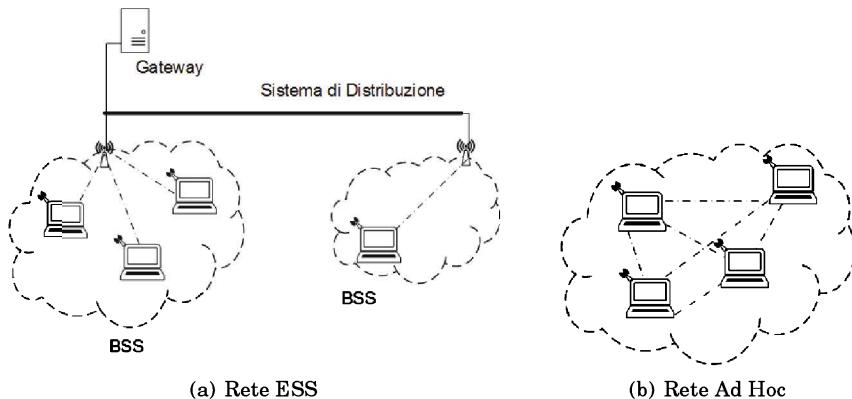


Figura 7.2: Reti WLAN

La figura 7.2 illustra le due alternative possibili per l'architettura di una rete IEEE 802.11.

7.1.2 Livello fisico

Non esiste un unico livello fisico dello standard: dal 1997, anno della prima ratificazione, ad oggi sono state introdotte varianti e nuovi livelli fisici che si differenziano tra loro in base alla modulazione adoperata, alla frequenza operativa e quindi al data rate raggiungibile. Una tabella riassuntiva è mostrata di seguito.

La prima versione dello standard, (Forouzan'2007 e Tanembaum'2011 in 7.5), è stata indicata con la sigla IEEE 802.11 Legacy. Essa prevedeva due alternative per il livello fisico: una in grado di operare alle frequenze degli Infrarossi (IR), mentre l'altra nella banda ISM (Industrial Scientific Medical), in particolare alla frequenza 2.4 GHz. La prima alternativa fu rapidamente abbandonata sia a causa dello scarso successo della trasmissione ad IR sia per il costo dei dispositivi di trasmissione/ricezione necessari. La modulazione adoperata con gli IR era una Pulse Position Modulation (PPM). Del secondo livello fisico esistono due versioni; entrambe hanno un trasferimento dati massimo di 2 Mbit/s ma si differenziano per la tecnica di allargamento della banda utilizzata: la Frequency Hopping Spread Spectrum (FHSS) e la Direct Sequence Spread Spectrum (DS-SS). La prima è una tecnica che consiste nel variare la frequenza di trasmissione a intervalli regolari attraverso un codice pseudocasuale e noto sia al trasmettitore che al ricevitore. In IEEE 802.11 si suddivide la banda in 75 sottocanali con una larghezza di banda di 1 MHz, inoltre le variazioni di frequenza hanno una cadenza di 2.5 salti/s mentre la tecnica di modulazione prevista è a spostamento di frequenza FSK (Forouzan'2007, Halsall'1996 in 7.5). Per la seconda alternativa era stata invece prevista una tecnica ad allargamento di spettro basata sull'impiego di un particolare sequenza binaria pseudocasuale, nota sia al trasmettitore che al ricevitore, detta *sequenza di Barker*. La modulazione usata

Versione	Release	Frequenza (GHz)	Banda (MHz)	Data rate (Mbit/s)	Tecnica
Legacy	06/1997	2.4	20	da 1 a 2	DSSS, FHSS
		IR		da 1 a 2	
a	09/1999	3.7, 5	20	da 6 a 54	OFDM
b	09/1999	2.4	20	da 1 a 11	DSSS
g	06/2003	2.4	20	da 6 a 54	OFDM, DSSS
n	10/2009	2.4, 5	20	da 7.2 a 72.2	OFDM
			40	da 15 a 150	
ad	12/2012	60	2, 160	> 6.75 Gb/s	SC, OFDM
ac	01/2014	5	20	> 87.6	OFDM
			40	> 200	
			80	> 433.3	
			160	> 866.7	

Tabella 7.2: Standard IEEE 802.11

in questo caso è una modulazione binaria a spostamento di fase (PSK : Phase Shift Keying).

Come evoluzioni successive sono state standardizzate due versioni: la IEEE 802.11a e la IEEE 802.11b. Lo standard IEEE 802.11a opera nella banda Unlicensed National Information Infrastructure (U-NII), ad una frequenza intorno ai 5 GHz. Lavorando a questa frequenza si limitano le interferenze esterne (nessun dispositivo wireless lavora a queste frequenze) e si riesce a offrire data rate elevati (fino a 54 Mbps). Lo svantaggio principale di questa soluzione è tuttavia dovuto ad una maggiore attenuazione del segnale trasmesso. Di conseguenza, per avere un'area di servizio adeguata, si ha necessità di maggiore potenza in trasmissione, il che può essere un aspetto particolarmente critico per terminali di utente mobili. La tecnica di accesso al canale è la OFDM mentre, come tecnologia trasmittiva, sono previste le modulazioni PSK e QAM (Quadrature Amplitude Modulation). Lo standard prevede 12 canali in frequenza non sovrapposti, 8 dedicati alle comunicazioni interne e 4 per le comunicazioni punto-punto. Questo standard non ha avuto molto successo. In particolare, in Europa, questo standard non fu inizialmente nemmeno autorizzato perché le frequenze di lavoro previste non erano disponibili. Solo nel 2002 tali frequenze vennero liberate e si iniziò allora la diffusione della versione a. Lo standard IEEE 802.11b lavora nella frequenza ISM a 2.4 GHz ed utilizza la tecnica DSSS ad alta velocità: è sempre una tecnica DSSS che però utilizza uno particolare schema di codifica (sequenze pseudocasuali) detto Complementary Code Keying (CCK). La modulazione utilizzata è una PSK e, a differenza dello standard IEEE 802.11a, è retrocompatibile con il la versione Legacy. L'evoluzione successiva è lo standard IEEE 802.11g. Questa versione utilizza, come frequenze di lavoro, quelle previste nella versione IEEE 802.11b, permettendo, tuttavia, un data rate massimo più elevato (si arriva a 54 Mbps grazie all'impiego della tecnologia di accesso al canale OFDMA).

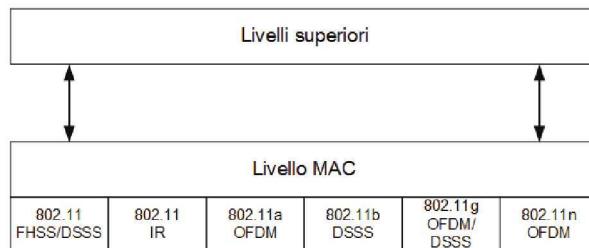


Figura 7.3: Livello MAC protocollo IEEE 802.11

prevista in IEEE 802.11a. Lo standard IEEE 802.11g è totalmente compatibile con lo standard IEEE 802.11b. La versione più recente (al momento di stesura di questo testo) è la IEEE 802.11n. Con questa versione dello standard si aumenta il data rate massimo fino a 300 Mbps e si è previsto di poter lavorare alle due frequenze 2.4 GHz e 5.4 GHz. Questa versione dello standard (Forouzan'2007, Tanembaum'2011 in 7.5) è particolarmente innovativa anche perché introduce la possibilità di gestire la qualità del servizio (QoS), consentendo, di conseguenza, una migliore efficienza nella gestione dei servizi delay-sensitive (come ad esempio multimedia streaming). Lo standard IEEE 802.11n prevede anche l'utilizzo della tecnologia MIMO (Multiple Input Multiple Output) che prevede di utilizzare più antenne, sia per trasmettere che per ricevere, separando spazialmente i singoli flussi ed incrementando così la banda disponibile. Questa versione è nata per realizzare reti wireless di dimensioni metropolitane (WMAN).

7.1.3 Livello MAC

Il livello MAC nello standard IEEE 802.11, come illustrato in figura 7.3, è comune a tutte le diverse alternative disponibili per il livello fisico. La tecnica di accesso al canale condiviso è basata sulla tecnica Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) che rappresenta una variante della tecnica base CSMA descritta in 5.2.2. La tecnica CSMA/CA è stata introdotta poiché nelle reti senza fili non è sempre possibile rilevare in maniera affidabile e conveniente una collisione. A differenza delle reti cablate (wired), un terminale dovrebbe poter trasmettere e ricevere contemporaneamente e questo renderebbe il suo costo più elevato. Inoltre, le particolarità del canale radio (es.: attenuazione in funzione della distanza) e la possibilità di avere terminali anche molto distanti tra loro rende poco efficace mutuare in un contesto radio le metodologie utilizzate in reti cablate per rivelare le collisioni.

Frame MAC

Il formato di un frame MAC per il protocollo IEEE 802.11 (vedi Forouzan'2007, Tanembaum'2011 in 7.5) è mostrato in figura 7.4. Esso comprende nove campi:

- *Frame Control*: è composto da undici sottocampi:

- Protocol Version: indica la versione del protocollo, attualmente ha valore 0;
 - Type: indica il tipo di informazione contenuta all'interno del frame, può assumere i seguenti valori:
 - * 00: gestione : per stabilire la comunicazione iniziale tra i terminali e l'AP;
 - * 01: controllo: per la procedura di handshake descritta di seguito;
 - * 10: dati;
 - Subtype: indica il tipo di messaggio di controllo inoltrato, può assumere i seguenti valori:
 - * 1011: RTS (Request-to-Send, Richiesta di collegamento);
 - * 1100: CTS (Clear-to-Send, Accettazione di una RTS);
 - * 1101: ACK (Acknowledgment, Riscontro);
 - To DS/From DS: il loro funzionamento verrà spiegato in seguito;
 - More Frag: se vale uno indica che sono presenti altri frammenti di uno stesso messaggio (vedi di seguito);
 - Retry: se vale uno indica una ritrasmissione;
 - Power MGMT: se vale uno indica che il nodo è in modalità risparmio energia;
 - More Data: se vale uno indica che ci sono altri dati da inviare;
 - WEP: se vale uno, il dato è cifrato;
 - Order: bit riservato;
- *Duration ID*: indica il tempo dichiarato per la trasmissione da un terminale. Questo valore è utilizzato nel contatore a decremento del vettore di allocazione NAV (Network Allocation Vector), descritto nel paragrafo seguente;
 - *Address 1 - Address 2 - Address 3 - Address 4*: il loro significato dipende dai valori assunti dai campi *To DS/From DS*;
 - *Sequence Control*: indica il numero di sequenza del pacchetto;
 - *Payload*: La sua grandezza può essere variabile, e contiene il datagramma di livello superiore;
 - *CRC*: contiene un codice CRC-32 per il rilevamento degli errori.

Per limitare gli effetti negativi delle condizioni di propagazione sull'integrità dei dati trasmessi, lo standard raccomanda l'utilizzo della tecnica della *frammentazione* che consiste nel suddividere un frame informativo in sottoparti con un numero di bit ragionevolmente minore. Oltre a ridurre la possibilità di avere errori nei singoli frammenti, questa tecnica rende più efficiente la gestione del meccanismo di ritrasmissione in quanto permettendo di localizzare gli errori si richiede la ritrasmissione solo dei frammenti difettosi (con errori). Non è quindi necessario chiedere la ritrasmissione dell'intero frame.

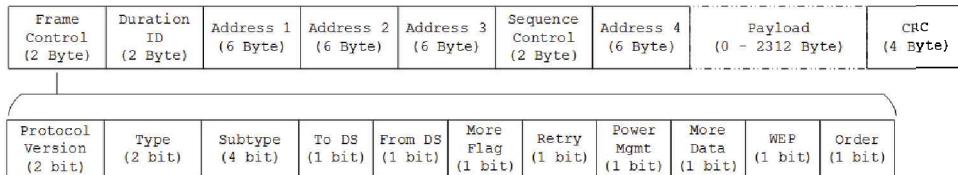


Figura 7.4: Livello MAC protocollo IEEE 802.11

Dai campi *To DS* e *From DS* del MAC frame si capisce che il protocollo IEEE 802.11 gestisce 4 tipi di indirizzi differenti. Questo perché un pacchetto, nel suo tragitto potrebbe dover essere gestito da uno o più AP (quindi potrebbe cambiare rete). Solitamente *Address 1* contiene l'indirizzo del prossimo nodo che riceve il pacchetto, *Address 2* contiene l'indirizzo del nodo da cui proviene il pacchetto, *Address 3* e *Address 4* vengono usati in casi particolari. In base al valore assunto dai due bit si hanno i seguenti casi:

- *To DS = 0, From DS = 0*: in questo caso, il pacchetto viaggia all'interno della stessa sottorete. Nel primo campo indirizzo viene posto l'indirizzo del destinatario, nel secondo campo viene posto l'indirizzo mittente;
- *To DS = 0, From DS = 1*: in questo caso si ha che il pacchetto arriva da una rete diversa, connessa a quella di riferimento grazie al sistema di distribuzione. In questo caso, l'identificativo del mittente originario del messaggio (nodo di un'altra rete) è specificato nel campo *Address 3*. *Address 4* è lasciato vuoto.
- *To DS= 1, From DS = 1*: in questo caso, il pacchetto sta entrando nel sistema di distribuzione per arrivare al destinatario posto in una rete diversa da quella del mittente. In questo caso, il destinatario finale del messaggio è salvato nel campo *Address 3*. *Address 4* è lasciato vuoto.
- *To DS =1, From DS=1*: è un caso molto particolare e vuol dire che il sistema di distribuzione è anch'esso una rete wireless (a differenza dei tre casi precedenti, dove il sistema di distribuzione è wired). A differenza dei casi precedenti, si ha la necessità di specificare gli indirizzi degli AP. Nei casi precedenti questo non era necessario in quanto, essendo gli AP connessi tra di loro in modalità wired (via cavo), la specifica dei loro indirizzi è prevista dal protocollo utilizzato per farli comunicare. In particolare, in questo caso, in *Address 3* viene indicato l'indirizzo del destinatario finale del pacchetto mentre in *Address 4* viene inserito l'indirizzo mittente originario.

Accesso al canale

La tecnica CSMA/CA si basa sulla tecnica a rilevazione di portante con l'aggiunta di una funzionalità finalizzata a prevenire le collisioni.

Con questa tecnica, l'accesso al canale per l'invio di un frame viene ritardato di un tempo prestabilito, anche se il canale risulta libero, per ridurre l'intervallo

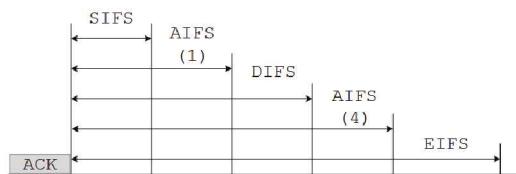


Figura 7.5: Ordinamento temporale dei sotto-intervalli in IEEE 802.11

di vulnerabilità della tecnica di accesso (un terminale è in grado di rivelare un accesso di un altro terminale con un ritardo che dipende dalla loro distanza fisica). Questo tempo è chiamato *Inter Frame Space* (IFS) e prevede, a sua volta, una suddivisione in sotto intervalli di durata differente: Short IFS (SIFS), Arbitration Interframe Space (AIFS), Distributed Coordination Function (DIFS), Extended IFS (EIFS). L'ordine di questi intervalli nell'ambito dell'IFS stabilisce una priorità nell'effettuare l'accesso al canale in relazione a diverse condizioni di trasmissione. L'ordinamento temporale dei sotto-intervalli previsti dallo standard è illustrato in figura 7.5.

Come si vede dalla figura il primo intervallo è SIFS che quindi assegna alle funzionalità di accesso ad esso associate che sono : a) trasmissione di messaggi di riscontro (ACK); b) trasmissione di frammenti successivi di un frame, la priorità maggiore. Ogni terminale deve attendere almeno un tempo pari a SIFS prima di accedere al canale.

Il secondo intervallo è l'intervallo indicato in figura come AIFS (1). È l'intervallo di tipo AIFS più piccolo utilizzato per dare priorità di accesso a traffici sensibili ai ritardi come il traffico voce. Sempre in figura è indicato anche un intervallo AIFS più lungo (anche dell'intervallo DIFS), AIFS(4), che di conseguenza viene utilizzato per traffico a priorità più bassa detto *traffico di background*. Nella figura sono anche mostrati gli intervalli DIFS, e EIFS che rappresentano rispettivamente il tempo che un terminale deve aspettare una volta trovato il canale libero prima di tentare la trasmissione di un pacchetto e il tempo di attesa prima che un terminale, che ha ricevuto un frame difettoso o non riconosciuto, possa notificarlo a tutti altri terminali. Come si vede dalla figura a quest'ultima funzionalità viene assegnata la priorità minore.

La procedura di accesso al canale da parte di un terminale in modalità casuale viene effettuata secondo la procedura illustrata in figura 7.6. Quando un terminale ha necessità di accedere al canale ne verifica preventivamente lo stato di libero o occupato. Se il canale viene rilevato libero, il terminale fa partire il contatore a decremento inizialmente impostato a valore DIFS. Terminato il tempo di attesa, se il canale risulta ancora libero, la stazione trasmette il pacchetto e rimane in attesa del riscontro per un tempo uguale a SIFS, se il riscontro non arriva entro questo intervallo si assume che il pacchetto abbia subito una collisione. Di conseguenza il terminale entra nello stato di contesa. Lo stesso accade se, trascorso DIFS, il canale viene rilevato occupato, quando un terminale si trova nello stato di contesa.

In entrambi i casi, il terminale aspetta un tempo DIFS (in generale questo tempo può essere diversificato in relazione alle differenti priorità dei pacchetti da inviare) ed imposta un contatore a decremento detto *backoff timer* ad un valore scelto con probabilità uniforme entro un intervallo temporale detto *finestra di contesa* (Contention Window (CW)) la cui ampiezza dipende dal numero di tentativi di accesso falliti per uno stesso pacchetto. Inizialmente la CW viene impostata al valore minimo previsto, che può, anche in questo caso, essere legato alla priorità del traffico. Valori di CW minori danno priorità nell'accesso. Successivamente, la CW viene definita così:

$$CW(n) = \min\{2CW(n - 1), CW_{Max}\} \quad (7.1)$$

dove CW_{Max} è il massimo valore ammesso per CW . Come si vede dalla (7.1) il valore di CW raddoppia ad ogni tentativo di accesso fallito. Raggiunto un numero massimo di riferimento per i tentativi di accesso falliti per uno stesso pacchetto, questo viene scartato dal terminale. Questa operazione indirettamente aiuta a contenere la congestione (numero eccessivo di accessi contemporanei) del canale condiviso. Durante il tempo di backoff il terminale ascolta il canale ad ogni slot. Ogni volta che il terminale rileva il canale occupato, il backoff timer viene fermato, il conto allo rovescio riprende da dove è stato interrotto dopo un tempo uguale a DIFS (quindi senza impostare un nuovo valore del tempo di backoff). Quando il backoff timer arriva a zero, il terminale trasmette e rimane in attesa dell'ACK. La tecnica CA ha quindi come scopo principale quello di prevenire le collisioni. Tale obiettivo è perseguito utilizzando il backoff timer il cui valore viene impostato su base statistica grazie all'estrazione casuale (ed indipendente terminale da terminale) con probabilità uniforme, entro la CW , del ritardo di backoff. In questo modo si riduce la possibilità che due o più terminali impostino il backoff timer allo stesso valore e quindi diano luogo ad una nuova collisione.

La procedura utilizzata dalla tecnica CSMA/CA è illustrata in figura 7.6.

La modalità CSMA/CA descritta in precedenza presenta una criticità operativa nota come **problema del terminale nascosto**. Per illustrare nel dettaglio di cosa si tratta si faccia riferimento alla figura 7.7 (a). La figura mostra tre terminali A , B e C e le loro aree di copertura (viene omessa per semplicità quella relativa al terminale B). Tutti i dispositivi entro una certa area di copertura di un terminale sono in grado di riceverne i messaggi. Dalla figura si nota che A e C sono esterni alle rispettive aree di copertura e quindi A e C non possono comunicare direttamente tra di loro. Viceversa il terminale B è interno ad entrambe le aree di copertura, quindi sia A che C possono comunicare con B . Supponiamo adesso che A sia in collegamento con B stia inviando frammenti di un frame più lungo. Se durante il tempo di accesso di A anche C decide di comunicare con B , non riscontrando il canale occupato da altri, concluso il tempo DIFS inizia ad inviare i propri frammenti di frame a B provocando (se A non ha completato l'accesso) una collisione.

Questo problema può essere risolto prevedendo una procedura di handshake (set-up del collegamento) tra terminale mittente e terminale destinatario. Questa procedura può essere descritta, riferendosi all'esempio precedente, come segue:

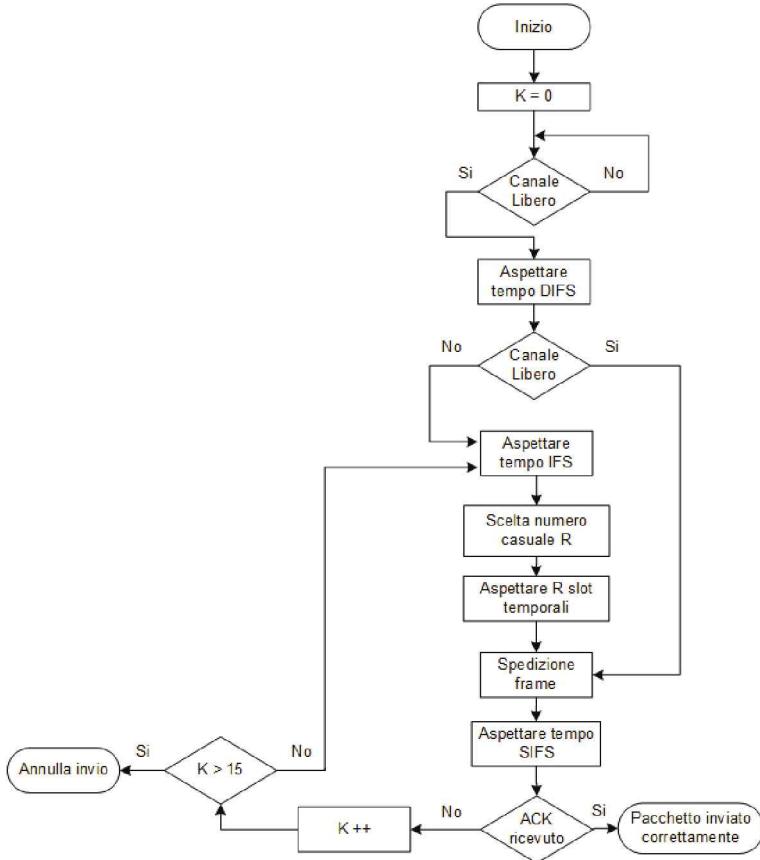


Figura 7.6: Procedura di accesso per la tecnica CSMA/CA

1. Conclusa la fase preliminare di ingresso al canale (DIFS) se questo è ancora libero, A invia un messaggio breve (RTS) di richiesta di collegamento a B ;
2. Se B riceve senza collisione il messaggio RTS, trascorso il tempo SIFS, risponde con un breve messaggio di conferma (CTS);
3. Ricevuto da B il messaggio CTS, trascorso il tempo SIFS, A procede all'invio dei frame verso B .

Conclusa la fase di handshake, la gestione della successiva fase di accesso avviene secondo le modalità base (ogni frammento ricevuto correttamente viene riscontrato ad A mediante l'invio di un ACK da parte di B). Una ulteriore riflessione su questa procedura consente di comprenderne l'efficacia riguardo il *problema del terminale nascosto*: l'invio del messaggio RTS viene interpretato da tutti i terminali nell'area di A come una prenotazione del canale ed un *invito a desistere* da eventuali accessi. Questo messaggio ovviamente non è noto a C che quindi ancora non conosce le intenzioni di A . Il messaggio CTS inviato da B

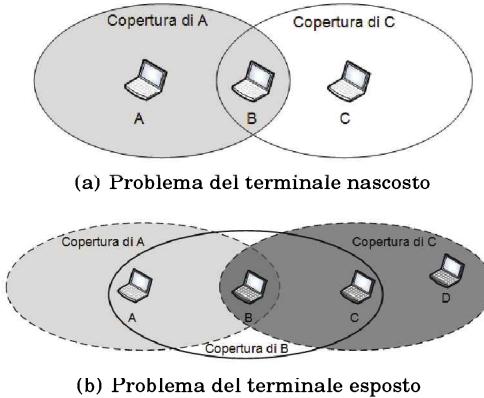


Figura 7.7: Problema del terminale nascosto ed esposto

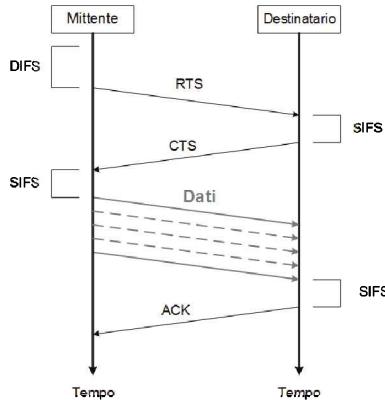


Figura 7.8: Procedura di handshake nel protocollo IEEE 802.11

come accettazione della richiesta di collegamento fatta da *A* viene però ricevuto anche da *C* che a questo punto lo interpreta come una prenotazione del canale ed un conseguente invito a desistere dall'accesso. In questo modo quindi si evita che un terminale nascosto acceda ad un canale occupato perché non è in grado di rivelarne lo stato. La procedura di handshake è mostrata in figura 7.8.

La procedura di handshake risolve il *problema del terminale nascosto* ma ne introduce una nuova criticità nota come **problema del terminale esposto** illustrata in figura 7.7 (b). In questo caso si hanno quattro terminali A,B,C e D. Supponiamo che B sia in collegamento con A, se durante questo tempo D avesse necessità di collegarsi con C, pur non avendo nessuna conseguenza sul collegamento in corso A-B (B sta trasmettendo, D non è nell'area di copertura di A) l'accesso al canale non viene consentito. La ragione di questo è dovuta al messaggio RTS inviato da B e ricevuto da C che ne inibisce le funzionalità di trasmissione e ricezione per il tempo dichiarato necessario per completare l'accesso (valore cam-

po *Duration ID*). È immediato notare che la procedura di handshake comporta una riduzione di efficienza della rete. Inoltre occorre notare che, se da un lato si riduce la probabilità di collisioni, dall'altro aumenta il tempo necessario a completare una fase di accesso al canale. Per limitare la perdita di efficienza occorre che i frame da trasmettere siano sufficientemente lunghi in maniera che il tempo necessario ad espletare la fase di handshake sia trascurabile nei confronti del tempo effettivo di accesso (trasmissione dei pacchetti).

Esaminiamo più nel dettaglio le modalità attraverso le quali i terminali vengono inibiti dall'accesso al canale quando questo è stato acquisito mediante la procedura di handshake da un determinato collegamento (es.: caso precedente B verso A). Per evitare poi che i terminali procedano ad attivare (inutilmente) una fase di accesso al canale quando questo è in uso per un collegamento (consumando quindi energia) è stato introdotto in ogni terminale un ulteriore contatore a decremeento chiamato **Network Allocation Vector** (NAV). Come mostrato nel paragrafo 7.1.3, il frame MAC contiene un campo che indica la durata della trasmissione (*Duration ID*); appena un terminale invia un messaggio RTS o CTS, tutti i nodi presenti nella sua area di copertura, leggono questo campo ed impostano il NAV a tale valore: i terminali non coinvolti in un collegamento attivato non tenteranno l'accesso fino a che il valore del NAV non è giunto a zero.

Un altro problema, conseguente alla priorità assegnata alle stazioni che conquistano il canale, è la possibilità di un accesso esclusivo per tempi troppo lunghi a scapito di tutti gli altri terminali. Per evitare questo, lo standard prevede di assegnare ad ogni terminale, anche eventualmente in relazioni a necessità (tipo di traffico) di accesso differenti, un valore massimo per il tempo di trasmissione. Questo valore è indicato come **Transmit Opportunity** (TXOP). Una procedura completa di accesso al canale è illustrata in figura 7.9.

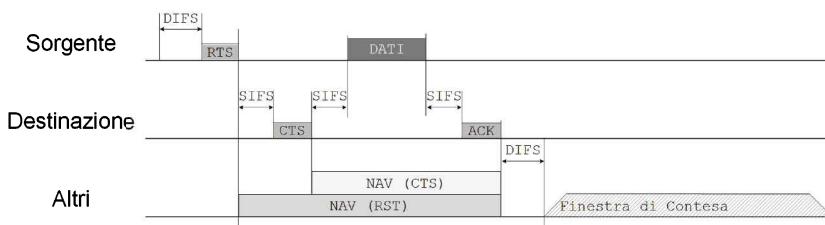


Figura 7.9: Accesso al canale secondo il modello IEEE 802.11

La metodologia di accesso al canale descritta in precedenza viene detta funzione di coordinamento distribuita (**distributed coordination function**, DCF). Lo standard prevede anche un metodo di accesso alternativo, senza contesa, implementato sfruttando la funzione di coordinamento centralizzata (**point coordination function**, PCF). Tale tecnica viene utilizzata nelle reti infrastrutturate (con AP). Si basa sul paradigma polling-response: a turno l'AP interroga i singoli terminali abilitati a tale modalità di accesso per permettere loro di trasmettere, senza contesa, i propri pacchetti. La funzione di coordinamento centralizzata ha priorità rispetto alla fase DCF e, quindi, quando prevista, è associata

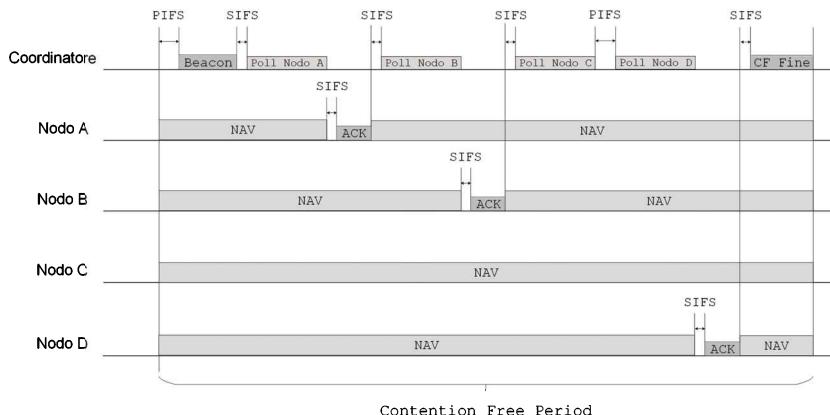


Figura 7.10: Accesso PCF

ad un tempo di ritardo PIFS (PCF Interframe Spacing) minore (nell'ordinamento temporale (figura 7.9) segue di solito il periodo SIFS). L'assegnare priorità superiore alla fase PCF rispetto alla DCF da luogo al seguente problema:

I nodi che utilizzano solo la tecnica DCF potrebbero non riuscire mai ad accedere al canale.

Questo inconveniente viene eliminato semplicemente prevedendo di dedicare un tempo massimo per la fase PCF. All'inizio di ogni trasmissione, l'AP aspetta un tempo PIFS, se il canale è libero, invia un Beacon Frame (messaggio di annuncio e controllo). All'interno di questo frame è presente un campo che indica la durata dichiarata per la fase PCF: tutti i terminali che non prevedano la modalità PCF imposteranno quindi il loro NAV al valore dichiarato ed eviteranno di accedere al canale fino a quando il contatore NAV non è a zero. La modalità operativa della funzione PCF è mostrata in figura 7.10.

Principali problematiche

Il meccanismo RTS/CTS apparentemente sembra un rimedio efficace almeno per risolvere il problema del *terminale nascosto*. In realtà nelle applicazioni pratiche viene attivato raramente e di solito viene preferita una versione semplificata del protocollo base. I motivi di questa scelta sono:

- Non è efficace con frame corti (il tempo di necessario a chiudere la procedura di accesso può essere dominante rispetto al tempo di accesso effettivo);
- Non è utile nel caso di rete infrastrutturale (presenza di un *access point* (AP));
- Rallenta comunque il trasferimento dei frame a causa della fase iniziale di set-up;

- Non risolve il problema del *terminale esposto*;
- I terminali nascosti sono in genere rari.

Importante sottolineare che nelle comunicazioni wireless, in generale, un problema critico è garantire un'adeguata integrità ai frame trasmessi causa le condizioni di esposizione del canale wireless al disturbi ambientali (es.: forni a microonde) e condizioni spesso severe di rumore. In questi casi utilizzare il meccanismo di riscontro non porta a benefici apprezzabili in quanto notifica l'evento "errata ricezione" ma non presuppone nessun meccanismo per risolvere il problema. Due soluzioni, che si dimostrano invece efficaci a questo riguardo, sono:

- a. Ridurre la velocità di trasmissione dei frame (trasmissioni più lente consentono di utilizzare tecniche di trasmissione maggiormente immuni ai disturbi esterni);
- b. Suddividere un frame in sottoparti (*frammentazione*): diminuendo il numero di bit che costituiscono il blocco trasmesso si riduce la possibilità di avere errori. In questo caso è necessario etichettare ciascun elemento di un frame per poter ripristinare in ricezione la versione originale non suddivisa del flusso informativo. In generale si adotta una strategia denominata *Stop-and-Wait* la quale implica che ogni segmento non può essere trasmesso se quello di ordine immediatamente inferiore non è stato riscontrato come correttamente ricevuto.

Nelle comunicazioni wireless di solito i terminali di utente sono terminali mobili per quali il *consumo energetico* è un aspetto prioritario al fine di preservare la loro autonomia di funzionamento. Per questo motivo si cerca di ridurre al minimo l'impegno di un terminale quando non ha necessità di accesso alla rete. Il meccanismo adottato a questo riguardo è quello del *beacon frame*. Esso prevede l'invio periodico da parte di un AP di messaggi opportunamente strutturati in modalità broadcast. Questi messaggi hanno lo scopo di rendere pubblica la presenza di un AP, di fornire informazioni circa il processo di invio dei messaggi di beacon e, quando necessario, le impostazioni di sicurezza. I terminali entro l'area di copertura dell'AP possono rispondere notificando una loro eventuale sofferenza in termini di consumo energetico. Una volta che l'AP riceve queste informazioni, interrompe l'eventuale comunicazione con detti utenti conservando i frame, a loro indirizzati, in un buffer per un inoltro successivo. I terminali diventano attivi (si svegliano) ad ogni ricezione di un messaggio di beacon. Leggendo la mappa del traffico contenuta nel messaggio, i terminali sono poi in grado di capire se vi è necessità di collegamento con l'AP. In caso affermativo rispondono con un messaggio di conferma che autorizza l'AP ad attivare la fase di trasferimento dell'informazione verso di essi. Conclusa questa fase i terminali tornano nello stato di *riposo* ed attendono l'arrivo del nuovo messaggio di beacon (la sua frequenza temporale deve essere nota). Un'altra alternativa è la tecnica *APSD* (Automatic Power Save Delivery) adatta ad essere implementata in reti infrastrutturate. L'AP conserva in un buffer i dati diretti ad un proprio utente fino a quando non riceve dati dallo stesso utente. In questo modo il terminale utente può rimanere inattivo fino a quando non avrà nuovamente dati da trasmettere.

Una ulteriore esigenza che il protocollo IEEE 802.11, in relazione alle nuove richieste di utilizzo, deve saper gestire è il controllo della *Qualità del Servizio* (QoS) offerto agli utenti. Come è stato illustrato, questo obiettivo si raggiunge mediante una distribuzione temporale delle diverse fasi di accesso ed associando alle procedure con livello di priorità superiore ad intervalli di attesa minore.

7.2 IEEE 802.16

Lo standard IEEE 802.16 anche noto come *WiMAX* (Worldwide Interoperability for Microwave Access) nasce per poter usufruire di velocità di accesso superiori a quelle tipiche di reti IEEE 802.11 e su distanze maggiori. Il WiMAX Forum, un'associazione formata da un gruppo di aziende di settore, è l'ente preposto a definire gli standard di riferimento per questa tecnologia wireless e per certificare i dispositivi proposti per operare con essa, attraverso il rilascio di una sorta di marchio di qualità (WiMAX Forum Certified) per i dispositivi approvati. Per le sue caratteristiche WiMAX fu proposto per risolvere le difficoltà di collegamento veloce ad internet specialmente in zone rurali o scarsamente abitate dove gli ISP non avevano giustificati interessi commerciali a predisporre collegamenti cablati veloci (digital divide). Rispetto alla più popolare tecnologia IEEE 802.11, WiMAX consente di avere:

- Gestione della qualità di servizio (QoS);
- Confidenzialità delle informazioni scambiate.

L'accesso al canale è regolato secondo la tecnica OFDMA con matrice tempo-frequenza di allocazione delle risorse di accesso. Il numero delle sottoportanti e la loro posizione può variare nel tempo in relazione ad uno stesso collegamento per migliorare le prestazioni della rete. L'allocatione delle sottoportanti rimane fissa entro un tempo detto *tempo di simbolo*. La possibilità di modificare le sottoportanti allocate agli utenti consente di fare in modo di individuare per ognuno di essi l'insieme di sottoportanti che consentono una migliore qualità della trasmissione.

WiMAX prevede (Tanembaum'2011, Fantacci'2011, Fantacci'2008 in 7.5) una stazione principale, detta *Base Station*, in grado di collegarsi con i propri utenti (Subscriber Station). Il ruolo principale svolto dalla Base Station è coordinare le comunicazioni da e verso le varie Subscriber Station che si trovano nella sua area di copertura. In particolare essa dovrà interpretare i messaggi ricevuti dalle proprie Sunscriber Station e inoltrarli verso le loro destinazioni finali. A questo riguardo essa disporrà di adeguate connessioni verso altre Base Station che gestiscono aree diverse (tipicamente con collegamenti a maglia). Le modalità di gestione dell'accesso sono:

- TDD (Time Division Duplex) : Vengono separate temporalmente le due fasi di trasmissione dalla Base Station verso le proprie Subsciber Station (downlink) e da queste verso la Base Station (uplink). In questa modalità il

tempo è organizzato in frame, a loro volta costituiti da sottointervalli temporali distinti destinati alle due fasi di comunicazioni downlink e uplink. Nella prima metà (downlink) la Base Station comunica in modalità broadcast verso le proprie Subscriber Station. Durante la fase di comunicazione uplink le varie Subscriber Station comunicano individualmente su risorse assegnate in maniera esclusiva con la Base Station. I due sottointervalli sono separati da un intervallo di guardia necessario per far commutare lo stato dei dispositivi lato Base Station e Subscriber Station da trasmissione (attivo) a ricezione (passivo);

- **FDD (Frequency Division Duplexing):** In questa modalità vengono assegnate bande distinte alle comunicazioni uplink e downlink. Vengono dunque separati in frequenza i flussi informativi che vanno in sensi opposti.

In generale la modalità TDD è più semplice da implementare ed offre un livello di flessibilità superiore. La Base Station gestisce le connessioni con le Subscriber Station inviando delle mappe cioè specificando come ha previsto di distribuire le sottoportanti potendo anche modificare da frame a frame le sue scelte.

Non è compito di questo testo fornire una descrizione esaurente dello standard IEEE 802.16, limitandoci quindi all'essenziale, descriveremo di seguito alcune delle funzionalità caratterizzanti questo standard per quanto riguarda la modalità di trasmissione delle informazioni (livello Fisico) e la gestione della QoS.

7.2.1 Livello Fisico

WiMAX prevede la possibilità di trasmettere l'informazione con tre differenti tecniche con lo scopo di aumentare, quando possibile, la velocità di trasferimento dei flussi informativi. Nel rendere più veloce il trasferimento dei dati occorre tuttavia tenere in conto che l'integrità dei dati trasmessi, a parità di potenza impiegata, è inversamente proporzionale al rate di trasmissione. In altri termini, la tecnica che consente il rate più alto sarà anche quella più vulnerabile nei conformi di errori di trasmissione (maggiore degradazione dell'integrità dell'informazione). Per questo motivo la scelta della tecnica di trasmissione viene fatta cercando di bilanciare queste due esigenze contrapposte in maniera adattiva alle condizioni di canale. Semplificando si può dire che le Subscriber Station più prossime alla Base Station, potendo usufruire di condizioni di propagazione più favorevoli, saranno quelle che potranno beneficiare di velocità di accesso più alte rispetto a Subscriber Station poste ai margini dell'area di copertura.

7.2.2 Gestione della QoS

WiMAX prevede le quattro classi di servizio seguenti (Tanembaum'2011, Forouzan'2007, Nauaymi'2007 in 7.5):

- **Bit-rate costante:** prioritariamente rivolto ai servizi voce non compressa. Ha bisogno di avere risorse di accesso riservate per un uso esclusivo ad intervalli di tempo regolari senza che sia necessario richiederle ogni volta.
- **Bit-rate variabile - tempo reale:** tipicamente rivolto ad un traffico multimediale compresso e applicazioni in tempo reale. La Base Station interroga con cadenza regolare le Subscriber Station interessati a questo profilo di servizio per conoscere le necessità di accesso e provvedere di conseguenza.
- **Bit-rate variabile - non tempo reale:** È rivolto a comunicazioni di stream di dati (consistenti) che non richiedono il tempo reale, per esempio il trasferimento di un file. La Base Station interroga, non con cadenza regolare, le Subscriber Station interessate dal servizio. Se accade che una particolare Subscriber Station non risponde ad una interrogazione, questa viene eliminata dalla lista di interrogazione individuale (perde il diritto al servizio) ed inserita in un gruppo di potenziali Subscriber Station interessate a cui viene rivolta un'interrogazione collettiva (il diritto al servizio si conquista superando una fase di contesa).
- **Best-effort:** È la modalità che riguarda tutto il traffico rimanente (es.: applicazioni e-mail). In questo caso non viene fatta nessuna interrogazione da parte della Base Station verso le proprie Subscriber Station. La Base Station comunica con la mappa quale risorse ha destinato a questo servizio trama per trama. Le Subscriber Station interessate si contendono le risorse disponibili. Ogni volta che una di esse ha successo, la risorsa "conquistata" viene specificata nella successiva mappa. Viceversa ogni volta il tentativo di accesso fallisce se ne deve programmare uno nuovo impiegando un meccanismo di risoluzione delle contese di tipo backoff esponenziale binario. Questo processo serve anche per acquisire l'identità di nuovi client che si accendono e, quindi, che si connettono alla Base Station.

Nonostante la tecnologia WiMAX abbia avuto una diffusione limitata e stia oggi soffrendo della concorrenza di nuove tecnologie wireless per la trasmissione a larga banda, sta comunque riscuotendo un notevole interesse in applicazioni specifiche come ad esempio la gestione delle comunicazioni in ambienti aeroportuali (AreoMax) per le quali si presenta come una soluzione molto attraente (Bartoli'2013 in 7.5).

7.3 IEEE 802.15.1

Lo standard IEEE 802.15.1 (vedi www.ieee802.org/15/pub/TG1.html), fa parte della famiglia Wireless Personal Area Network (WPAN) ed è conosciuto come standard **Bluetooth**. Questa tecnologia fu ideata da Ericsson nel 1994 e il suo nome deriva da Harald Blaatand, re di Danimarca vissuto nella seconda metà del 900 D.C. che unificò la Danimarca e la Norvegia sotto la stessa bandiera. Il cognome di questo re si traduce in inglese con il termine Bluetooth.

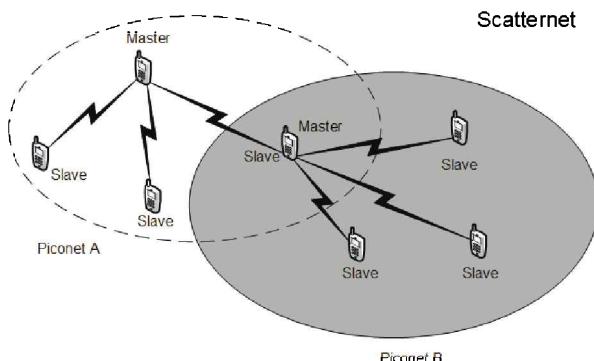


Figura 7.11: Rete Bluetooth

7.3.1 Architettura

Bluetooth prevede solo reti ad-hoc con pochi dispositivi attivi contemporaneamente. Una rete Bluetooth viene chiamata generalmente **Piconet** e può avere fino a otto nodi attivi. Di questi, uno ha il ruolo di coordinatore della rete (chiamato **Master**) mentre gli altri sette sono i cosiddetti **Slave**. Gli Slave, una volta che sono entrati nella rete, sincronizzano il loro clock con quello del Master. Alla Piconet possono appartenere più nodi, ma attivi contemporaneamente ne devono risultare solo sette, tutti gli altri nodi si troveranno in uno stato particolare di attesa (*parking*). Il nodo che si trova in questo stato è sincronizzato con il Master, ma non può comunicare fino a che un nodo attivo della Piconet non abbandona lo stato di attività per entrare in quello di parking.

Se più Piconet sono connesse tra di loro, si forma una **Scatternet**. In questa modalità saranno presenti dei nodi con funzionalità duale Master/Slave che funzionano da connettori tra le varie Piconet come illustrato in figura 7.11.

Le reti sono centralizzate, e gli Slave non possono comunicare direttamente tra di loro.

7.3.2 Architettura Protocollare Bluetooth

Lo stack protocollare Bluetooth è mostrato in figura 7.12.

Livello Radio (Radio Layer)

Bluetooth usa una bassa potenza di trasmissione (dell'ordine dei mW) e dunque le comunicazioni sono limitate a distanze brevi (area di copertura molto ristretta), dell'ordine dei 10 m. Il data rate previsto non è tanto elevato (≈ 1 Mbps) mentre la banda utilizzata è la banda ISM alla frequenza di 2.4 GHz. Lo standard prevede di dividere la banda in 79 canali, ciascuno di ampiezza (banda) di 1 MHz. Per ridurre le interferenze tra i vari dispositivi si usa la tecnica FHSS con 1600 salti al secondo. Ovviamente la scelta della sequenza di salto da un

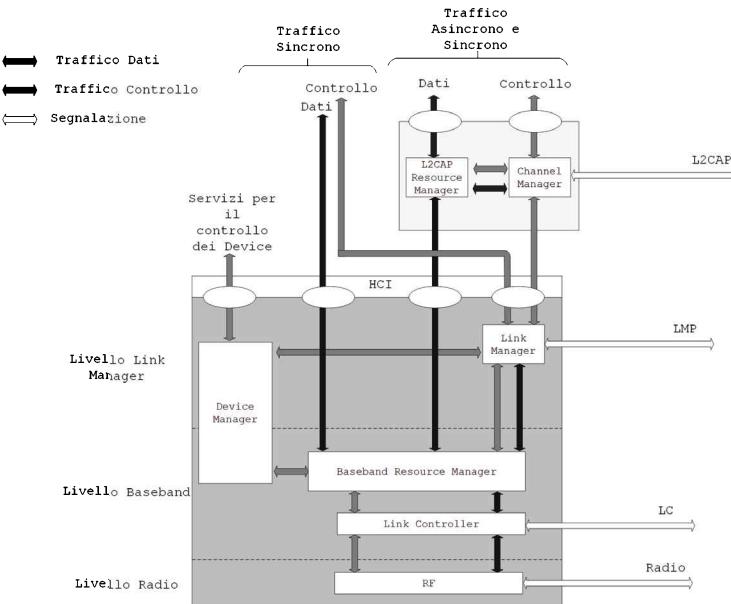


Figura 7.12: Architettura protocollare Bluetooth

canale all'altro avviene in modalità pseudocasuale. Le collisioni tra dispositivi di reti differenti sono molto rare. Per risolvere una collisione bastano tecniche a rilevazione d'errore (FEC) e ritrasmissione (ARQ). Un dispositivo Bluetooth ha a disposizione la bada di accesso per un tempo lordo $625 \mu s$ ($1/1600$) ed un tempo effettivo di 366 ms , la differenza tra tempo lordo di accesso e tempo effettivo viene utilizzata dai dispositivi per riconfigurarsi alla nuova frequenza di lavoro secondo lo schema FHSS. La modulazione adoperata è una Gaussian Frequency Shift Keying (GFSK), si veda Forouzan'2007 in 7.5 per maggiori dettagli.

Livello Baseband (Baseband Layer)

Questo livello ha le funzionalità del livello MAC previsto negli altri standard IEEE 802. Dunque è il responsabile dell'accesso al mezzo condiviso. L'accesso al canale avviene mediante la tecnica polling gestita dal Master ed estesa a tutti gli Slave appartenenti alla sua Piconet (Forouzan'2007, Tanembaum'2011 in 7.5). La trasmissione dei dati nel canale comune viene gestita sulla base della tecnica Time Division Duplex (TDD) con slot di durata $625 \mu s$ e modalità half-duplex (un dispositivo non può inviare e ricevere contemporaneamente i dati). Dato che l'accesso al canale avviene con tecnica polling e la comunicazione tra Master e Slave avviene mediante divisione temporale. Il Master della piconet comunica verso gli slave sempre negli slot temporali pari, mentre lo slave interpellato comunica nello slot successivo. Quindi, se il Master interella lo Slave A nello slot 0 esso gli risponderà nello slot 1 successivamente il Master interella lo Slave B nello

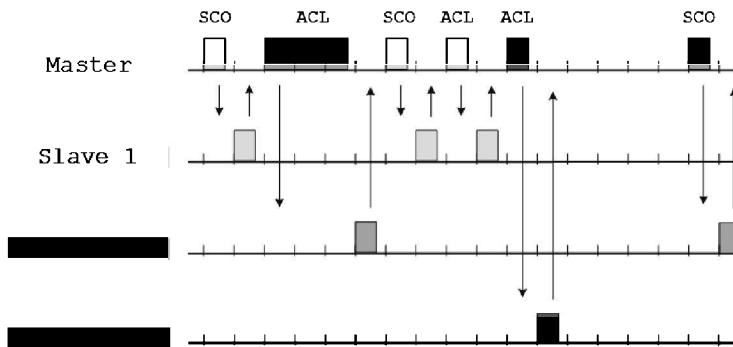


Figura 7.13: Comunicazione Bluetooth

slot 2 ed esso gli risponderà nello slot 3 e così via. Uno Slave può comunicare solo se nello slot precedente ha ricevuto il messaggio dal Master.

Bluetooth prevede, come indicato in Forouzan'2007 e Tanembaum'2011 (vedi 7.5), l'uso di due tipologie di canali tra Master e Slave:

- *Synchronous Connection Oriented* (SCO): è adatto a collegamenti orientati alla connessione, viene instaurato prenotando degli specifici intervalli temporali secondo uno schema prestabilito. Viene utilizzato per il trasferimento di dati audio real-time. Si cerca di minimizzare il ritardo temporale a discapito della qualità della comunicazione. Uno Slave può creare fino a tre canali SCO con lo stesso Master.
- *Asynchronous Connectionless Link* (ACL): in questa modalità di trasmissione (best effort) si cerca di salvaguardare l'integrità dei dati più che il ritardo con cui arrivano. In questa modalità si possono assegnare uno, tre o cinque intervalli temporali per la trasmissione dei dati. Se il Master decide di iniziare una comunicazione ACL, la tecnica FHSS viene bloccata, quindi non si effettuano salti di portante durante la trasmissione ACL.

Al termine di ogni trasmissione è sempre inviato un messaggio di ACK per l'avvenuta ricezione. Le due modalità di trasmissione sono mostrate in figura 7.13.

Il frame Bluetooth ha una particolarità, il campo dati dipende dalla modalità di trasferimento e nel caso ACL dipende da quanti slot temporali sono stati allocati per il trasferimento dati. Il frame Bluetooth è illustrato in figura 7.14. I significati dei campi sono (Forouzan'2007, Tanembaum'2011 in 7.5):

- *access code*: contiene i bit necessari per la sincronizzazione tra Master e Slave;
- *packet header*: contiene i seguenti campi ripetuti tre volte:
 - *address*: indica l'indirizzo dello Slave nella piconet, se questo campo è zero vuol dire che è un messaggio di broadcast dal Master verso tutti gli altri nodi;

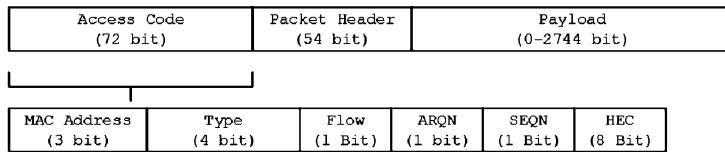


Figura 7.14: Frame Bluetooth

- type: indica il tipo di dati che vengono inviati;
- flow: usato per il controllo di flusso, se è pari a uno lo Slave non può ricevere ulteriori pacchetti
- ARQN: viene usato per i riscontri. Bluetooth adopera la tecnica Stop and Wait;
- SEQN: numero di sequenza del pacchetto;
- HEC (Header Error Correction): questo campo serve per rilevare gli errori nel frame;
- *payload*: come detto in precedenza la lunghezza è variabile e contiene i dati provenienti dai livelli superiori.

Livello Link Management Protocol (Link Management Protocol Layer)

Questo livello è il responsabile del collegamento, quindi deve controllare lo stato della connessione di un dispositivo all'interno della piconet e la sicurezza della comunicazione, quindi ha il compito di autenticare gli utenti e criptare le comunicazioni (vedi capitolo 15).

Livello Stack Logical Link Control and Adaptation Protocol (L2CAP)

Questo livello è chiamato anche con l'acronimo L2CAP ed è l'equivalente del livello LLC nelle reti IEEE 802. Riguarda solo le comunicazioni di tipo ACL in quanto quelle di tipo SCO non lo prevedano. Ha il compito di suddividere in frame i messaggi di lunghezza variabile (se richiesto) e fornire supporto per comunicazioni affidabili. In altre parole, questo livello ha il compito di provvedere al multiplexing dei protocolli di livello superiore, effettuare la segmentazione e il ri-assemblaggio dei pacchetti ed è anche il responsabile della gestione della QoS.

Altri Livelli

Per quanto riguardo i livelli superiori a L2CAP la tecnologia Bluetooth prevede varie alternative, ognuna con compiti e finalità ben precise. Una loro discussione dettagliata esula dallo scopo di questo testo. Per dettagli ed approfondimenti specifici si suggerisce di consultare i testi indicati in 7.5.

Modalità operative

Un dispositivo Bluetooth si può trovare in due stati: connessione o stand-by. Lo slave si trova nello stato di connessione se è connesso ad un Master ed è coinvolto con esso nello scambio dati. Se lo Slave non è connesso a nessuna piconet oppure è presente all'interno di una piconet ma non è coinvolto nello scambio dati, allora si trova nello stato di stand-by. Questo è lo stato che serve per far risparmiare energia ai dispositivi Bluetooth. Quando uno Slave si trova nello stato di stand-by ascolta il canale ogni 1,28 secondi per ricevere eventuali messaggi dal Master. Quando un dispositivo passa dallo stato di stand-by allo stato di connessione, esso si può trovare in uno dei seguenti sottostati:

- **active mode:** lo Slave partecipa attivamente allo scambio dati della piconet. Ha un indirizzo lungo tre bit;
- **hold mode:** lo Slave entra in questo stato solo su autorizzazione del Master. È un sottostato concepito per il risparmio di energia e la sua durata ha un tempo fissato da parte del Master. Lo Slave che si trova in questo stato non può ricevere messaggi e mantiene il suo indirizzo di bit;
- **sniff mode:** anche questo stato è stato concepito per risparmiare energia. Per entrare in questo stato, Master e Slave negoziano due parametri: lo "sniff interval", che fissa gli slot di sniff e lo "sniff offset", che indica il primo slot di sniff. In questa modalità lo Slave ascolta il canale in intervalli prefissati;
- **park mode:** lo Slave che si trova in questa modalità appartiene sempre alla piconet ma non è più attivo, dunque perde il suo indirizzo di tre bit e ne acquista uno nuovo di otto bit. Come spiegato nella sezione 7.3.1, questa modalità è stata progettata per poter creare piconet con più di sette Slave (esattamente $2^8 - 1$). Grazie al nuovo indirizzo da otto bit, il Master è in grado di ritrovare lo Slave e quindi lo può riportare in modalità attiva. Gli Slave che sono in modalità parking ascoltano regolarmente il canale per sentire se vi sono dei messaggi di broadcast da parte del Master: questi messaggi infatti sono gli unici che gli Slave in park mode possono ricevere. La richiesta di entrare in modalità attiva può partire anche dallo Slave stesso.

7.4 Tecnologia RFID

La tecnologia RFID (Radio Frequency Identification) consente ad oggetti di uso comune di poter essere parte di una rete di comunicazione. Nello specifico RFID è una tecnologia che consente il riconoscimento di oggetti o il recupero di dati in maniera automatica (AIDC: Automatic Identifying and Data Capture). Una caratteristica comune a molte realizzazioni di RFID è l'assenza di alimentazione. L'energia necessaria ad attivarsi per trasferire i dati memorizzati viene fornita sotto forma di onde elettromagnetiche dall'esterno da un dispositivo chiamato

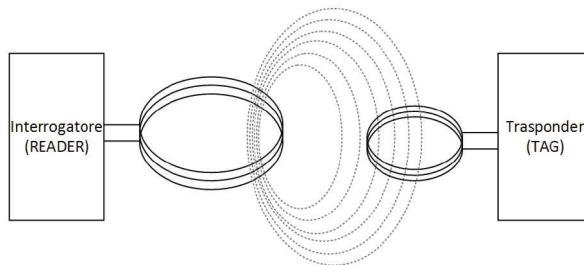


Figura 7.15: Sistema RFID

lettore. Questa tipologia di tecnologia RFID viene detta *passiva*. Sebbene di uso meno frequente, la tecnologia RFID si può trovare anche nella versione *attiva* che prevede la disponibilità di una sorgente di energia integrata nel dispositivo RFID.

Le applicazioni della tecnologia RFID sono molteplici e comprendono oltre al riconoscimento e tracciamento di oggetti, le smartcard, passaporti, ecc.. Un sistema RFID è composto da :

- Tag;
- Lettore.

Un sistema RFID è mostrato in figura 7.15.

I tag RFID sono dispositivi di dimensioni contenute e, tipicamente, a basso costo. A loro volta sono costituiti da:

- **un trasponder** che prevede una memoria di capacità limitate che ammette accessi sia in lettura che in scrittura (aggiornamento dei dati), circuiti per la trasmissione dei dati e un sistema (microchip) di controllo e supervisione;
- **una antenna** con funzioni di cattura del segnale elettromagnetico inviato verso la tag ed inviare indietro una parte adeguatamente modulato dai dati che si intende trasferire;
- **una batteria** (quando prevista).

I lettori sono la parte attiva del sistema, sono di solito alimentati da una sorgente propria, il loro compito è quello di interrogare tutti tag presenti nel loro raggio di azione, di identificarli e recuperare le informazioni di interesse. Un lettore che desidera interrogare un tag invia un segnale portante che, ricevuto attraverso l'antenna del tag, per il principio della induzione, viene trasformato in energia elettrica, successivamente impiegata per alimentare il microchip. A sua volta il microchip attiva le funzioni di lettura dei dati dalla memoria locale e provvede al loro invio verso il lettore pilotando la modulazione della frazione di segnale portante riflesso verso il lettore. Da notare che per permettere al tag di inviare i dati posseduti il lettore deve continuare a trasmettere il segnale di

interrogazione. Questa modalità è stata assimilata al principio su cui si basano i sensori radar e denominata *backscatter*.

Trattandosi di dispositivi con capacità di potenza limitate, le metodologie di trasmissione dei dati devono essere molto semplici (Tanenbaum'2011, Forouzan'2007 in 7.5). Infine, si deve notare che spesso un lettore che invia una interrogazione può ricevere risposte da più tag che si trovano nelle sue vicinanze. Questo può dare luogo a collisioni (questa situazione è simile alla condivisione di uno stesso canale radio tra più utenti (accesso multiplo). In questo caso i dispositivi interrogati non hanno possibilità di sentirsi reciprocamente (sensing) per cui una metodologia utilizzata per contenere le collisioni è la tecnica Aloha.

In questi ultimi anni si sta infine affermando un nuovo standard denominato NFC (Near Field Communication) che consente comunicazioni a distanze dell'ordine dei 10 cm con velocità di trasmissione dati fino a 424 kbps ed, in particolare, ammette lo scambio di informazioni anche direttamente tra lettori (bidirezionale).

7.5 Letture Consigliate

Per approfondire gli argomenti trattati in questo capitolo si consiglia:

Ieee standard for information technology – local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, IEEE Standard for Local and metropolitan area networks, Marzo 2012. Disponibile al sito: standards.ieee.org/about/get/802/802.11.html;

F. Halsall, Reti di Calcolatori e Sistemi Aperti, Addison-Wesley, 1996.

B.A. Forouzan, Reti di Calcolatori ed Internet, McGraw-Hill, 2007.

A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.

J.F. Kurose, K. W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.

R. Fantacci, D. Tarchi, A. Tassi, Wireless Communications Protocols for Distributed Computing Enviroments, Intech, 2011.

P.M. Shankar, Introduction to Wireless Systems, John Wiley, 2002.

L. Nauaymi, WiMAX, Technology for Broadband Wireless Access, John Wiley, 2007.

B.G. Lee, S. Choi, Broadband Wireless Access and Local Networks, Artech House, 2008.

R. Fantacci, Communication Infrastructure, Starrylink, 2008.

G. Bartoli, R. Fantacci, D. Marabissi, AeroMACS: A New Perspective for Mobile Airport Communications and Services, IEEE Wireless Commun., dic. 2013.

8

Reti di sensori

Le reti di sensori possono utilizzare come un supporto trasmissivo cablato (wired) oppure radio (wireless). La seconda alternativa è, ad oggi, quella più diffusa ed in questo caso si parla più propriamente di Wireless Sensor Networks (WSN). Le WSN si sono presentate come una naturale evoluzione tecnologica e funzionale delle reti wireless tradizionali. In particolare, le WSN si riferiscono ad una tipologia di rete con architettura distribuita comprendente dispositivi, anche eterogenei e con capacità differenti, ma comunque in grado di prelevare dati dall'ambiente in cui operano e di comunicare tra loro. Le WSN attuali hanno innumerevoli campi di applicazione che includono il monitoraggio ambientale, la sicurezza, la domotica, le applicazioni tattiche, la tutela e monitoraggio di beni culturali ed di infrastrutture (edifici, ponti, dighe, ecc.) e molto altro ancora. L'idea alla base delle WSN è quella di combinare in un modo funzionale la misura di una o più grandezze fisiche, come ad esempio temperatura, umidità o anche spostamenti in uno spazio o in un piano, con la trasmissione dei dati acquisiti verso un centro (detto comunemente sink) dove verranno elaborate in accordo a specifici processi applicativi o resi disponibili per accessi remoti. In generale quindi un sensore è chiamato ad implementare due funzione base :

- **sensing** : acquisire dall'ambiente in cui è inserito le misure delle grandezze fisiche di interesse;
- **comunicazione** : trasferire i dati raccolti, eventualmente elaborati e combinati, verso il centro di raccolta.

In generale un sensore è un dispositivo di dimensioni ridotte, fisso o mobile, con limitate capacità di calcolo e con stringenti limitazioni sul consumo energetico (legate al suo tempo di operatività). In generale le WSN sono reti con capacità autonomiche ed, in particolare, in grado di autoconfigurarsi dinamicamente secondo la migliore topologia in relazione a specifiche finalità applicative e restrizioni funzionali (es.: limitata autonomia).

8.1 Generalità

In generale una WSN può essere considerata come un insieme di sensori (nodi) i quali, nel loro insieme, definiscono una rete pervasiva per l'acquisizione e il

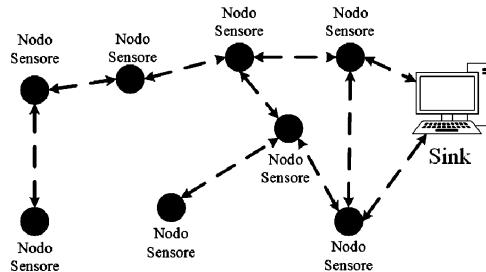


Figura 8.1: Rete di sensori

trasferimento di dati, utilizzando collegamenti radio. Un esempio di WSN è mostrata nella figura 8.1 dove ogni nodo della rete (sensore) è pensato equipaggiato con un modulo di trasmissione/ricezione che gli consente di partecipare al trasferimento dei dati (modalità ad-hoc) sia acquisiti direttamente tramite le proprie funzionalità di sensing sia ricevuti da altri sensori della rete. Nell'esempio illustrato nella figura tutti i dati acquisiti dai sensori vengono trasferiti ad un nodo principale (sink) che oltre ad avere il compito di elaborare le informazioni acquisite in relazione a specifiche applicazioni, in genere, (se richiesto), provvede anche al coordinamento delle funzionalità (sensing e comunicazione) degli elementi della rete. In generale quindi un nodo della rete può essere attivato per espletare la funzione di sensing, elaborazione e comunicazione o, eventualmente, solo quest'ultima quando viene chiamato unicamente a cooperare per il trasferimento dei dati acquisiti da altri nodi verso il sink. In generale quindi possiamo distinguere i nodi di una WSN in:

- **Sensori**: eseguano le misure (sensing) di una o più grandezze fisica che sono oggetto dell'applicazione specifica e provvedono al loro trasferimento verso un centro di raccolta (sink);
- **Sink** : sono nodi che hanno una funzionalità superiore al sensore. Possono a loro volta agire come sensori limitatamente all'operazione di sensing ma il loro ruolo principale è quello di provvedere alla raccolta dei dati provenienti dai nodi client (sensori) ed eventualmente elaborarli in accordo a definite metodologie e, infine, a trasferire l'informazione raccolta alle applicazioni (locali o remote);
- **Attuatori** : sono particolari elementi in grado di interpretare ed eseguire comandi conseguenti all'elaborazione delle informazioni acquisite secondo definite metodologie (applicazioni). Possono coincidere con i sink o essere degli elementi distinti della WSN;
- **Processori**: in una WSN alcuni sensori, oltre al sink, possono essere dotati di capacità di elaborazione delle informazioni acquisite o ricevute per ridurre la ridondanza dei dati da trasferire (quindi riducendo il consumo energetico o arricchire il loro contenuto informativo combinandoli con altri dati).

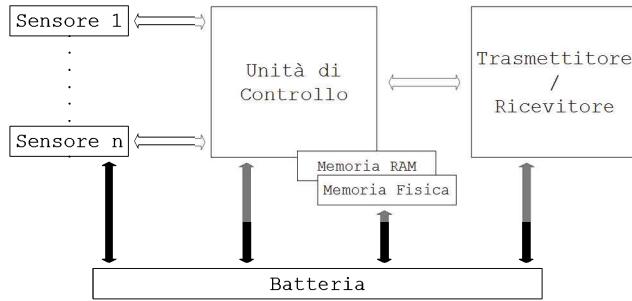


Figura 8.2: Struttura di un nodo sensore

All'inizio le WSN erano reti semplici, generalmente omogenee per quanto riguarda i nodi della rete che generalmente erano statici. Gli sviluppi tecnologici e la richiesta di sempre nuove applicazioni alle WSN hanno radicalmente modificato questa visione. Le WSN attuali sono costituite da elementi non omogenei che possano muoversi e, quindi, modificare dinamicamente nel tempo la topologia della WSN a cui appartengono. La struttura tipica di un sensore è mostrata in figura 8.2. Le sue componenti principali sono:

- **Unità di Controllo:** è un processore preposto alla gestione di tutte le funzioni (sensing, comunicazione, elaborazione) che un sensore deve poter espletare. Tipicamente è realizzato con tecnologia abbasso consumo energetico per prolungare il tempo di esercizio e non possiede, in genere, capacità di elaborazione troppo spinte;
- **Trasmettitore/Ricevitore :** costituisce l'interfaccia radio del sensore. Deve consentire di comunicare (ricevere o trasmettere informazione) con gli altri elementi della rete;
- **Batteria :** è la componente hardware più critica in quanto dalla sua efficienza e durata dipende la continuità (autonomia) di funzionamento del sensore;
- **Sensori:** rappresentano dei trasduttori che trasformano la misura di una specifica grandezza fisica in un adeguato segnale che può essere elaborato oppure trasmesso a distanza. Generalmente il processore riesce a gestire più trasduttori relativi a misure di grandezze fisiche differenti come temperatura, umidità, movimento, ecc..

Il trasferimento dell'informazione in una WSN può essere gestita in accordo alle due seguenti modalità base:

- **Address-based :** questa modalità necessita che ogni elemento della rete (nodo sensore, attuatore, processore, sink, ecc) abbia un indirizzo di rete che lo identifica in maniera univoca. L'informazione viene quindi trasferita avendo conoscenza della sua destinazione finale, generalmente attraverso

la cooperazione di altri elementi della WSN che svolgono solo il ruolo di inoltro dei dati ricevuti non essendone destinatari.

- **Data-centric** : in una WSN non è comune (a certe volte agevole) avere tutti gli elementi della rete associati ad un indirizzo univoco. Inoltre molte applicazioni richiedano la disponibilità di dati raccolti non da uno specifico sensore ma riferiti ad una determinata aerea di interesse. Questa modalità prevede che il trasferimento dell'informazione in una WSN sia legato al suo significato semantico ed indirizzata solo agli elementi della rete che in qualche modo sono interessati ad essa. Per questa sua particolarità spesso viene indicata anche come modalità *application-centric*.

La conoscenza della posizione dei nodi sensori o più in generale degli elementi della WSN, così come la possibilità di elaborare l'informazione (aggregazione, fusione) permette poi di migliorare la comunicazione tra i nodi di una WSN limitando l'area di inoltro dell'informazione e la ridondanza della stessa.

Infine, si possono individuare due diverse metodologie per attivare la comunicazione tra nodi sensori e il sink:

- **Push** : Viene di solito definita una procedura che autonomamente, senza sollecitazioni esterne, attiva il sensore (per le funzionalità di sensing e comunicazione) in corrispondenza di precisi istanti temporali;
- **Pull** : questa è una modalità di tipo reattivo cioè necessita di una sollecitazione esterna per l'attivazione delle funzionalità base (sensing, comunicazione).

Confrontando le due alternative, si può dire che la modalità *Push* non necessita di un controllo remoto del sensore (autonoma) ma ha lo svantaggio di attivare il sensore anche quando i dati raccolti possono non essere di interesse. Viceversa, la modalità *Pull* necessita di un controllo remoto del sensore ma in questo caso non accade mai che vengano inviati dati non richiesti.

8.2 Accesso Multiplo

In generale le metodologie utilizzate sono di tipo a contesa, tuttavia per applicazioni specifiche possono essere implementate tecniche ad accesso ordinato come ad esempio tecniche polling ad interrogazione diretta. Le tecniche ad accesso multiplo con contesa sono ispirate al protocollo CSMA/CA ed hanno come obiettivo primario quella di prevenire le collisioni. La tecnica nota da più tempo appartenente a questo gruppo è la MACA (Multiple Access with Collision Avoidance) che differisce dalla CSMA/CA nel fatto di non prevedere la rivelazione della portante. Questo protocollo riduce gli effetti negativi dovuti al problema del terminale nascosto senza, tuttavia, eliminarli completamente in quanto non si può prevenire la collisione di messaggi RTS/CLS generati da terminali non in visibilità radio oppure dovuti al movimento dei nodi attivi che accidentalmente entrano entro il raggio di attività di nodi diversi. Ogni volta che una collisione

avviene il protocollo MACA raddoppia la sua finestra di Back-off (intervallo di tempo entro cui si programma il tentativo di accesso successivo) fino a raggiungere un valore massimo prefissato. Viceversa, quanto un tentativo di accesso è andato a buon fine la finestra di back-off viene riportata al valore minimo previsto. Questo meccanismo non garantisce una sufficiente equità nella condivisione dell'accesso. Per giustificare questa affermazione, consideriamo il caso di due nodi N1 e N2 i quali hanno entrambi un flusso dati da trasmettere (es.: file video). Supponiamo che N1 riesca ad acquisire l'accesso al canale, durante il suo tempo di trasmissione N2 tenterà inutilmente di accedere al canale rivelando sempre collisioni virtuali. Conseguenza di questo è che al termine della trasmissione N1 avrà la sua finestra di back-off al valore minimo mentre per N2 sarà al valore massimo. Sotto queste condizioni, se entrambi tentano un nuovo accesso, è molto probabile che nuovamente N1 abbia la meglio. Questo problema nasce dalla mancanza di condivisione riguardo i valori della finestra di back-off. Un primo semplice rimedio è quello di inserire nella testata dei pacchetti il valore della finestra di back-off del nodo che ha avuto successo nell'accesso in maniera che tutti gli altri nodi possono uniformare il valore delle proprie finestre di back-off. Un secondo rimedio è quello di contenere le variazioni dei valori della finestra di back-off. In particolare nel protocollo MACAW (MACA for Wireless) viene adottato il meccanismo MILD (Multiplicative increase and Linear Decrease), questo meccanismo consiste nell'assumere un valore della finestra di back-off 1,5 volte superiore al precedente (fino a raggiungere un valore massimo) ogni volta che si rileva una collisione e a diminuire di 1 il valore della stessa finestra quando la trasmissione ha successo fino a raggiungere un valore minimo fissato. Il requisito di cercare di preservare l'operatività di un nodo in una WSN ha poi portato alla definizione di un protocollo di accesso multiplo specifico per i nodi sensori, indicato come S-MAC (Sensor - MAC), che prevede di mettere a riposo (stand-by) un nodo quando lo stesso non è partecipe alle attività della rete. Il principale problema che si incontra con il protocollo S-MAC è realizzare un efficace coordinamento tra nodi vicini in maniera che si trovino attivi (svegli) quando necessitano la loro cooperazione nel trasferimento dell'informazione.

Infine, un altro meccanismo utilizzato per cercare di preservare l'energia di un nodo, prevede il controllo di potenza dei segnali trasmessi. La scelta opportuna del livello di potenza da adottare per la trasmissione la si fa basandosi sulla stima della potenza del messaggio di risposta CLR del nodo destinatario. Essendo questo trasmesso con potenza convenzionale fissa, misurando il livello di potenza del segnale ricevuto si può ricavare il livello di potenza minima da adottare in trasmissione che garantisca l'integrità dei dati, al nodo destinazione, entro i requisiti fissati.

8.3 Ultra WideBand

La Federal Communication Commission (FCC) e l'International Telecommunication Union (ITU), con il termine Ultra WideBand, si riferiscono a una qualsiasi trasmissione che ha una elevata larghezza di banda: *ogni tecnologia radio la cui*

banda superi il 20% della frequenza centrale viene definita UWB. Quindi, ogni trasmissione radio che presenta una larghezza di banda che è almeno 1/5 della frequenza portante, è considerata trasmissione a banda ultra larga.

La banda operativa dei sistemi UWB è nel range [3,1 - 10,6] GHz. I sistemi UWB, prevedendo l'uso di impulsi di durata temporale molto ridotta (da qualche μs a pochi ns), richiedono un'occupazione spettrale ampia. La potenza di trasmissione di questi sistemi è dell'ordine dei mW ed si ha la possibilità di raggiungere elevati data rate entro brevi distanze. La larghezza di banda e le basse potenze di trasmissione fanno sì che la densità spettrale di potenza del segnale sia molto bassa. Questo implica che, per altre eventuali comunicazioni presenti nella stessa banda, i sistemi UWB siano percepiti come una sorgente di rumore.

Per comprendere la tecnologia UWB occorre richiamare il *Teorema di Shannon sulla Capacità di Canale*. Questo teorema afferma che la capacità C di un canale rumoroso, intesa come il valore massimo del data rate ammesso per avere un trasferimento affidabile (tasso di errore $\rightarrow 0$), fissata la potenza S del segnale utile e la potenza media di rumore N , è:

$$C = B \log_2 \left(1 + \frac{S}{N} \right) \quad \text{bit/s}$$

C aumenta quindi in modo lineare aumentando la banda del canale B mantenendo fissi gli altri parametri S e N oppure, a parità di condizioni di rumore e banda di canale B fissata, aumentando S in modo esponenziale. Poiché i sistemi UWB sono caratterizzati da valori di banda di canale elevati, da qui ne segue che essi sono in grado di sostenere trasmissioni affidabili con data rate elevati senza richiedere un eccessivo aumento della potenza impiegata in trasmissione.

La FCC ha imposto rigide finestre di emissione per i sistemi che utilizzano la tecnica di trasmissione UWB.

Grazie ai suoi pregi, UWB è stato proposto come livello fisico per molte famiglie dello standard IEEE 802.15.

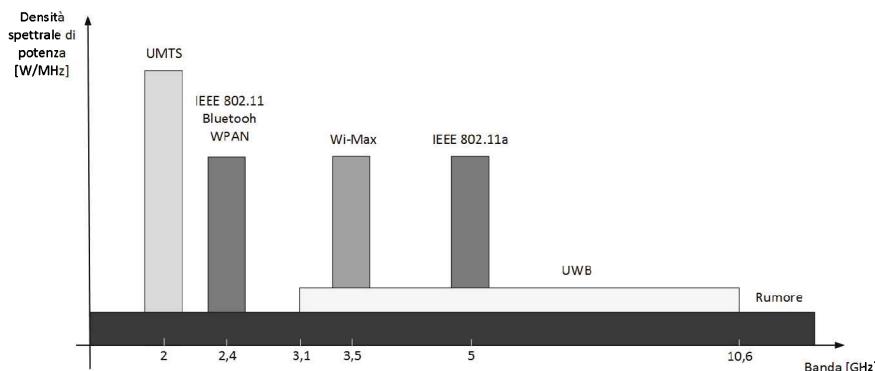


Figura 8.3: Confronto tra le densità spettrali di potenza di alcuni standard

8.4 IEEE 802.15.4

Lo standard IEEE 802.15.4 specifica, in riferimento al modello ISO/OSI, il livello fisico e il livello MAC per reti wireless personali, WPAN, a basso data rate. In queste reti le comunicazioni sono tipicamente limitate a distanze dell'ordine dei 10 m (corto raggio), con un data rate di 250 kbit/s. Le caratteristiche funzionali del protocollo IEEE 802.15.4 sono:

- basso data rate;
- basse potenze in trasmissione;
- indicazione della qualità del canale;
- limitati consumi energetici.

Il protocollo IEEE 802.15.4 è rivolto alla comunicazione tra dispositivi i quali sono classificati secondo due tipologie : dispositivi (o nodi) di tipo RFD oppure di tipo FFD. I nodi RFD sono estremamente semplici, hanno limitate capacità di calcolo e possono solo comunicare con i dispositivi FFD (non direttamente tra di loro). I nodi FFD sono più complessi, all'interno della rete possono svolgere la funzione di coordinatore e hanno la possibilità di comunicare con qualsiasi dispositivo in visibilità radio. La comunicazione a livello fisico e MAC è sempre di tipo link-to-link. Sono possibili le seguenti modalità di comunicazione:

- invio di dati da un nodo al coordinatore;
- invio di dati dal coordinatore a un nodo;
- comunicazione bidirezionale tra due nodi (usato nelle reti peer-to-peer, necessaria di sincronizzazione e può essere usato solo con dispositivi di tipo FFD)

Il Livello Fisico (PHY) offre agli strati superiori due tipi di servizio: il PHY *data service* per la trasmissione e la ricezione di pacchetti, denominati Packet Protocol Data Unit (PPDU) e il PHY *management service*, il cui compito è fornire servizi ai livelli superiori, dietro loro richiesta. I servizi offerti sono:

- ricezione e trasmissione dei pacchetti;
- attivazione e disattivazione del ricetrasmettitore;
- selezione del canale su cui trasmettere;
- Energy Detection sul canale selezionato;
- Link Quality Indication per i pacchetti ricevuti;
- Clear Channel Assessment per il CSMA/CA.

Le possibili bande di lavoro sono tre e tutte libere (non licenziate):

PHY	Banda (MHz)	Modulazione	Bit rate (Kbps)
868 / 915	868-868.6	BPSK	20
	902-928	BPSK	40
868 / 915	868-868.6	ASK	250
	902-928	ASK	250
868 / 915	868-868.6	O-QPSK	100
	902-928	O-QPSK	250
2450	2400-2483.5	O-QPSK	250

Tabella 8.1: Specifiche del livello fisico per lo standard IEEE 802.15.4.

- 868.0-868.6 MHz: presenta un unico canale di comunicazione, è utilizzata in Europa.
- 902-928 MHz: in questa banda sono previsti dieci canali, è usata in Nord America.
- 2.4-2.4835 GHz: è la banda più usata in tutto il mondo, prevede sedici canali.

La prima versione dello standard (2003) specificava due strati fisici sulla base della tecnica di trasmissione ad allargamento di spettro DSSS che prevede la trasmissione di un sequenza di simboli binari di durata limitata, detti chip (sequenza *pseudocasuale*) modulati in ampiezza da simboli binari bipolar. Una versione dello standard di livello fisico prevedeva di operare nella banda 868/915 MHz permettendo un data rate di 20 o 40 kbit/s mentre l'altra utilizzava la banda 2450 MHz e consentiva una data rate di 250 kbit/sec. La revisione del 2006 porta la velocità di trasferimento delle bande a 868 MHz e 915 MHz a 250 kbit/sec e definisce due strati fisici che si differenziano per la modulazione usata e la tecnologia di trasmissione:

- 868MHz, 915 MHz: utilizza la tecnica DSSS con modulazione di tipo BPSK;
- 868MHz, 915 MHz: utilizza la tecnica DSSS con la modulazione di tipo O-QPSK;
- 868MHz, 915 MHz: utilizza la tecnica PSSS con la modulazione di tipo BPSK e ASK;
- 2.450 GHz: utilizza la tecnica la DSSS con la modulazione di tipo O-QPSK.

Da notare che la terza specifica di livello fisico prevede di utilizzare la tecnica PSSS (Parallel Sequence Spread Spectrum) anziché la DSSS e l'uso combinato di due tecniche di modulazione. Le diverse specifiche per il livello fisico precedentemente introdotte sono richiamate nella 8.1.

Il livello MAC fornisce due tipi di servizi:

- *MAC Data Service*, permette la trasmissione e la ricezione dei pacchetti MPDU verso il livello fisico

- *MAC management service*, il quale fornisce servizi:
 - accesso al canale;
 - gestione dei tempi con suddivisione di slot temporali;
 - invio dei pacchetti di ACK;
 - associazione/dissociazione ad una rete WPAN;
 - servizi legati alla sicurezza e all'autenticazione.

Per garantire l'affidabilità della comunicazione, i dispositivi possono richiedere delle conferme di corretta ricezione ai nodi riceventi, tramite un pacchetto di riscontro (ACK). Il protocollo IEEE 802.15.4 supporta la gestione automatica delle ritrasmissioni dei pacchetti non riscontrati positivamente. In IEEE 802.15.4 un dispositivo che deve comunicare con un altro dispositivo, non ha a disposizione una via preferenziale per raggiungere la meta. Il canale di comunicazione è comune a tutti i dispositivi della rete e viene gestito secondo la modalità condivisa. Lo standard IEEE 802.15.4 prevede la condivisioni del canale su base accesso casuale secondo la tecnica CSMA/CA discussa nel capitolo 7.

Sono previste due modalità di trasmissione:

- *Beaconless* CSMA/CA: un nodo che utilizza questa tecnica nel momento in cui vuole trasmettere deve ascoltare il canale. Se il canale risulta libero, può iniziare la trasmissione, altrimenti attenderà un periodo aleatorio prima di ritentare la trasmissione con un nuovo ascolto;
- *Beacon-enabled* CSMA/CA: nella modalità beacon enabled, l'algoritmo prevede una più rigida ripartizione temporale gestita dal coordinatore della rete WPAN. In questo caso il coordinatore usa dei pacchetti di sincronismo (chiamati Beacon Frame) con lo scopo di suddividere l'asse temporale in intervalli detti *superframe*. Il superframe può ospitare solo una fase CAP oppure sia una fase CAP che una fase CFP durante la quale particolari dispositivi possono accedere al canale in modalità senza contesa su slot riservati (indicati come GTS). Nel primo caso il superframe è diviso in 16 slot temporali di durata uguale. Il primo slot è sempre dedicato all'invio del Beacon Frame, il quale serve per sincronizzare la comunicazione, identificare la WPAN e delimitare il superframe stesso. Un qualsiasi dispositivo della rete che voglia comunicare con un altro dispositivo, durante il CAP, entrerà in competizione con altri dispositivi con un uguale necessità e dovrà completare il suo accesso entro il tempo di arrivo del prossimo beacon frame. Nel caso in cui sia previsto anche un CFP il superframe viene diviso in 2 sotto-parti, che a loro volta sono divisi in 11 slot per la fase CAP, con il primo di questi dedicato alla trasmissione del beacon frame, e i rimanenti 5 slot destinati alla fase CFP. La modalità Beacon-enabled CSMA/CA è previsto anche che il superframe possa prevedere una sottoparte (Inactive Period) durante la quale tutte le interfacce radio sono messe a riposo per risparmiare energia. Ovviamente la scelta di dividere il superframe in due parti (attiva e inattiva) spetta sempre al coordinatore.

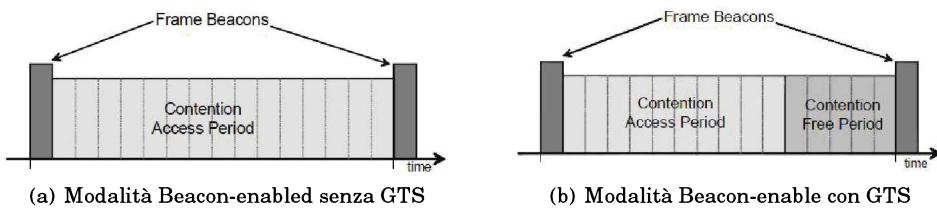


Figura 8.4: Modalità di trasmissione mediante beacon

Gli indirizzi a livello MAC supportati dallo standard IEEE 802.15.4 sono di due tipi:

- Indirizzo lungo (o esteso): sono indirizzi formati da 64 bit (conosciuti anche con l'acronimo EUI-64).
- Indirizzo corto (o unico): sono indirizzi formati da 16 bit, vengono usati dopo che un nodo è stato associato ad una WPAN.

Nel 2007 è stato presentato un aggiornamento di tale standard : IEEE 802.15.4a. Le modifiche apportate sono limitate, ma tutte importanti:

- sono previste due modalità di accesso al canale, modalità CSMA/CA e Aloha;
- non è prevista la modalità superframe senza GTS;
- al livello fisico sono state apportate alcune modifiche tra cui la possibilità di utilizzare il sistema UWB, utilizzare la tecnica Chirp Spread Spectrum (CSS) e utilizzare alcune nuove modulazioni tra cui la M-ary Phase Shift Keying (MPSK) operante nella banda a 780 MHz e la Gaussian Frequency Shift Keying (GFSK), operante nella banda a 950 MHz. Il livello fisico UWB lavora a tre differenti frequenze:
 - un singolo canale che occupa lo spettro da 249.6 a 749.6 MHz;
 - quattro canali che occupano lo spettro da 3.1 a 4.8 GHz (chiamata anche banda bassa);
 - undici canali che occupano lo spettro da 6.0 a 10.6 GHz (chiamata anche banda alta).

Le modulazioni usate sono la Burst Position Modulation (BPM) e la Binary Phase Shift Keying (BPSK).

8.5 IEEE 802.15.3

Lo standard IEEE 802.15.3 è stato proposto, in contrapposizione allo standard IEEE 802.15.4, per poter trasmettere ad alti data rate nelle reti personali (High

Rate - Wireless Personal Area Networks). Tale standard è in grado di offrire data rate da 11 fino a 55 Mbps per distanze superiori ai 70 m. Introduce poi il concetto di Qualità del Servizio (QoS) ed è adatto al trasferimento di dati multimediali. Prende spunto dal pre-esistente standard Bluetooth, ma con l'obiettivo dichiarato di non essere un'estensione dello stesso ma bensì definire modalità precise per una coesistenza funzionale con tutti gli altri standard già esistenti.

La rete realizzata da dispositivi IEEE 802.15.3 viene definita piconet ma, a differenza di Bluetooth, i dispositivi possono comunicare tra di loro. E' poi previsto che un dispositivo svolga le funzioni di coordinatore della piconet e che piconet distinte possano collegarsi tra di loro per formare delle reti estese.

Lavora nella banda ISM a 2,4 GHz, in particolare opera nell'intervallo 2,4 - 2,4835 GHz e prevede 5 canali. Questi canali sono stati divisi in due gruppi. Uno gruppo è utilizzato per le modalità ad alta densità mentre l'altro viene usato quanto è necessaria una coesistenza con il protocollo IEEE 802.11b. Il livello fisico supporta 5 data rate diversi in relazione ad altrettanti differenti profili di modulazione. Il data rate minimo è 11 Mbps mentre quello massimo è di 55 Mbps.

La sincronizzazione della comunicazione tra i dispositivi avviene mediante la definizione di un superframe. Il superframe prevede: l'invio del segnale di beacon per la sincronizzazione dei dispositivi e per inviare informazioni di servizio; il CAP dove i nodi tentano l'accesso al canale per trasferire dati in modo asincrono con modalità CSMA/CA; il channel time allocation period (CTAP), diviso a sua volta in due parti (channel time allocations (CTA) e il management CTAs (MCTA)) dove si accede con tecnica TDMA nel CTA oppure nel MCTA con tecnica Aloha (MCTA di tipo open o association) o TDMA (MCTA di tipo regular). Prevede la possibilità di frammentare i dati da trasmettere e inoltre prevede l'uso un messaggio di riscontro (ACK) dopo l'invio di un messaggio.

Il livello MAC è il responsabile della connessione dei dispositivi, deve garantire la QoS per i dati trasferiti ed è il responsabile della sicurezza. Il MAC frame è composto da 2 campi: il MAC header e il MAC body. La lunghezza massima del MAC frame è di 2058 byte (10 byte riservati al MAC header più 2048 byte (massimo) del MAC body).

Poiché punto focale di questo standard era riuscire ad avere elevati data rate nelle WPAN, la trasmissione UWB sembrava essere un'ottima candidata per lo scopo. Nacque così il Task Group 3a il cui unico obiettivo era standardizzare un livello fisico alternativo per 802.15.3: questa evoluzione fu chiamata IEEE 802.15.3a. Sfortunatamente, in fase di progettazione dello standard, i membri del TG 3a non furono in grado di scegliere tra due livelli fisici differenti: la Multi-band Orthogonal Frequency Division Multiplexing (MB-OFDM) voluta dal gruppo WiMedia Alliance e la Direct Sequence UWB (DS-UWB) proposta dall'UWB Forum. I tentativi di realizzare un livello fisico tutto UWB terminarono quando il gruppo si sciolse, nel gennaio del 2006. Nel 2005 fu stata standardizzata un'evoluzione del protocollo base indicata come standard IEEE 802.15.4b. Allo stato attuale è al lavoro il Task Group 3c che ha proposto un livello fisico alternativo: l'uso di onde millimetriche. L'intervallo di frequenza considerato è 57 - 64 GHz con la prospettiva di garantire un data rate di oltre 2 Gbps.

8.6 Il protocollo 6LoWPAN

Il protocollo 6LoWPAN (IPv6 over Low power PAN), come indicato in RFC 4919, è stato progettato per poter adeguare il protocollo IPv6 al livello fisico e MAC dello standard IEEE 802.15.4, come mostrato in figura 8.5. Il problema principale della trasmissione di un pacchetto IPv6 in una rete IEEE 802.15.4 sono le sue dimensioni. IPv6 ammette una dimensione minima di 1280 byte (di cui 40 sono riservati all'header), mentre IEEE 802.15.4 supporta una grandezza massima di 127 byte. La conseguenza di questo divario è stata l'introduzione di un livello di adattamento (adaptation layer) tra il livello L3 (rete) e il livello L2 (collegamento) che si occupi della compressione dell'header, della frammentazione del pacchetto IPv6 e l'ottimizzazione del protocollo di Neighbor-Discovery di IPv6 descritto in RFC 4861. Il protocollo 6LoWPAN presenta le seguenti specificità:

- **Compressione dell'Header:** i campi dell'header IPv6 vengono compressi o eliminati quando l'adaptation layer è in grado di ricavarli direttamente dalle informazioni del livello MAC o li conosce a priori.
- **Frammentazione:** i pacchetti IPv6 sono frammentati in più frame di livello MAC per adattarsi ai requisiti MTU IPv6 minimi.
- **Instradamento di livello 2:** per supportare l'instradamento di livello 2 dei datagrammi IPv6, l'adaptation layer è in grado di trasportare gli indirizzi di livello MAC.

Il datagramma che arriva al livello MAC è ottenuto incapsulando il pacchetto di livello applicativo, dentro il datagramma del livello di trasporto, che a sua volta è incapsulato dentro il pacchetto del livello di rete. Ogni header 6LoWPAN inizia con un gruppo di bit che identifica il tipo di header seguito dai campi del pacchetto. L'header 6LoWPAN presenta una sequenza analoga all'header IPv6.

La compressione dell'header definita in RFC 4944 prevede: Header Compression 1 (HC1) e Header Compression 2 (HC2). HC1 permette di comprimere i 40 byte di un header standard IPv6 in 2 byte, nel caso migliore. Allo stesso modo HC2 descrive i modi per comprimere l'header del livello di trasporto utilizzato. Per arrivare ad avere solo 2 byte di header IPv6, HC1 elimina il campo Version,

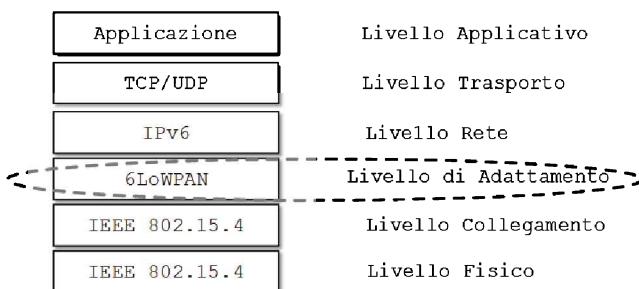


Figura 8.5: Compatibilità di 6LoWPAN con l'architettura protocollare ISO/OSI

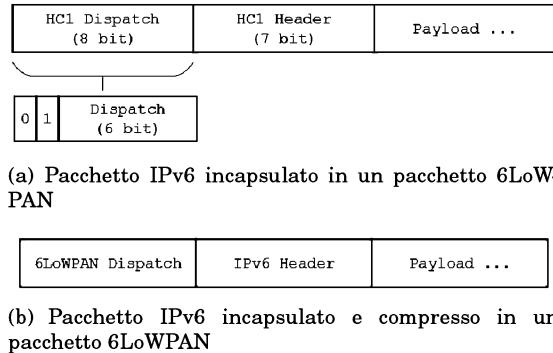


Figura 8.6: Struttura del pacchetto IPv6 incapsulato o incapsulato e compresso in un pacchetto IPv6

dato che esso vale sempre 6, gli indirizzi del mittente e del destinatario sono compressi (essi possono essere ricostruiti dagli indirizzi MAC 802.15.4), lo stesso avviene per la lunghezza dei pacchetti. Per quanto riguarda i campi Header Class e Flow Label, questi valgono sempre 0 e possono essere eliminati. Infine il Next Header può essere solo UDP, TCP o ICMP, mentre non c'è modo di comprimere il campo Hop Limit. Il primo byte è il dispatch, e definisce il formato HC1 dell'header mentre il secondo byte è detto byte di codifica e definisce i parametri della codifica stessa. 6LoWPAN permette di incapsulare l'header IPv6 in un pacchetto LoWPAN oppure di comprimerne e, in seguito, incapsularne il pacchetto proveniente dal livello superiore. In figura 8.6 sono mostrate le due modalità. Il campo dispatch è il primo byte di ogni pacchetto compresso e incapsulato ed indica il tipo di header che segue: i primi due bit identificano tale campo mentre i sei bit seguenti identificano l'header che segue; il campo HC1_header, nel caso di compressione dell'header IPv6 è formato da 7 bit. Ognuno di essi indica se il relativo campo dell'header IPv6 è stato compresso. HC2 si occupa della compressione dell'header del protocollo di trasporto. Allo stato attuale sia l'RFC 4944 che l'RFC 6282 definiscono il formato di compressione del solo protocollo UDP. Tramite compressioni simili ad HC1 si riesce a ridurre la lunghezza dell'header UDP da 8 Byte a 4 nel caso migliore.

I mesh header sono stati concepiti per le reti mesh dove le operazioni di routing sono effettuate a livello di collegamento. In tale configurazione ogni nodo responsabile dell'inoltro dei pacchetti cambia gli indirizzi del mittente e del destinatario nel pacchetto con il proprio indirizzo e quello del next-hop. Poiché il routing è effettuato a livello collegamento, gli indirizzi della vera sorgente e del destinatario finale devono essere salvati da qualche parte. Infine si deve ricordare che ogni volta che il campo payload è troppo grande, rispetto a quanto previsto per un singolo frame IEEE 802.15.4, esso deve essere frammentato in più pacchetti. La frammentazione introduce un'header aggiuntivo che deve essere presente in ogni pacchetto frammentato.

8.7 Data Centric Forwarding

La modalità di instradamento Data Centric (DC), come evidenziato in precedenza, è una metodologia di inoltro dei dati in una WSN alternativa alla tecnica Address-based su cui sono basati gli algoritmi di routing classici descritti in 13. In generale i metodi di inoltro DC consentono di evitare i principali problemi legati all'utilizzo pratico delle tecniche Address-based dovuti alla necessità di :

- associare ad ogni dispositivo di rete un indirizzo univoco con conseguenti difficoltà in termini di scalabilità della WSN;
- prevedere la mobilità dei dispositivi connessi in rete;
- prevedere un aggiornamento periodico riguardo i possibili cammini interni alle WSN.

Le tecniche DC sono basate su una metodologia di inoltro che, anziché considerare la destinazione finale di un pacchetto, ne analizza il contenuto semantico e decide la procedura di inoltro di conseguenza. In generale, la modalità DC consente le seguenti funzionalità:

- **Data Dissemination** : questa funzionalità prevede di diffondere nell'intera WSN l'informazione acquista dagli elementi delle reti (sensori);
- **Network-Centric Processing** : la possibilità di elaborare le informazioni è di fondamentale importanza per migliorare le prestazioni di una WSN. In generale ci si riferisce ad operazioni di aggregazione dei dati, essenzialmente per eliminare ridondanze o per aumentarne il contenuto informativo.

Al fine di limitare la diffusione di informazioni non necessarie sono utilizzati nelle applicazioni DC indicatori di posizione, atte ad identificare l'area di raccolta (o richiesta) delle informazioni o di interesse delle stesse e indicatori temporali in maniera che per ogni informazione se ne possa percepire l'attualità (informazioni non più attuali non hanno in generale interesse).

Flooding e Gossiping

La tecnica *Flooding* è basata su un principio molto semplice e di facile implementazione. Ogni nodo di una WSN che riceve o genera un messaggio lo inoltra a tutti i suoi vicini come illustrato nella figura 8.7. Ovviamente l'utilizzazione della tecnica Flooding, se da un lato garantisce che tutti i nodi della WSN riceveranno il messaggio, dall'altro pone seri problemi in termini di congestione e consumo di potenza : i nodi possono ripetere indefinitamente un stesso messaggio (broadcast storm). Per cercare di limitare questi effetti dannosi è stata introdotta una informazione aggiuntiva TTL (Time-to-Live) nella testata (header) del messaggio che ne specifica il tempo di vita espresso in numero di ripetizioni. Ogni volta che un messaggio visita un nodo, questo, prima di inoltrarlo ai suoi vicini controlla il campo TTL. Se questo ha valore zero, il nodo scarta il messaggio che quindi

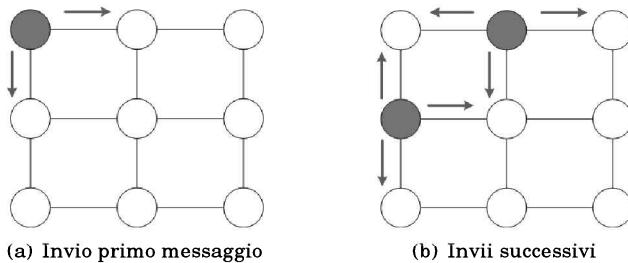


Figura 8.7: Tecnica Flooding

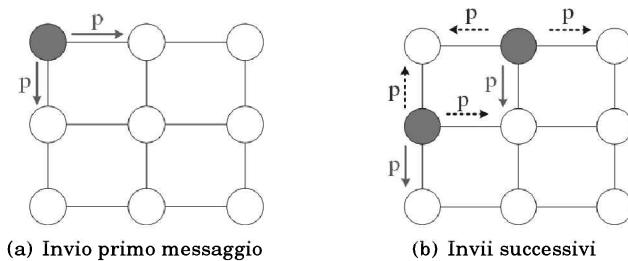


Figura 8.8: Tecnica Gossiping

termina la sua "vita" nella rete altrimenti, riduce di una unità il campo TTL e, successivamente, lo inoltra ai suoi vicini.

Questo meccanismo consente di limitare gli effetti legati al broadcast storm ma necessita di una appropriata definizione del valore TTL per non pregiudicare la pervasività dell'inoltro del messaggio stesso nella WSN.

La tecnica *Gossiping* è una variante della tecnica Flooding che prevede, al fine di limitare gli effetti del broadcast storm, di effettuare l'inoltro di un messaggio non indistintamente a tutti i vicini ma ad uno solo di questi sulla base di una decisione statistica. Il principio base della tecnica Gossiping è illustrato nella figura 8.8.

Varianti della tecnica Gossiping base consistono nell'ottimizzare la scelta statistica riguardo l'inoltro di un messaggio o di utilizzare informazioni aggiuntive come ad esempio la conoscenza del contesto dei nodi vicini (Smart Gossiping).

8.7.1 Direct Diffusion

Questa metodologia di inoltro delle informazioni in una WSN prevede di identificare i dati generati da un sensore mediante una coppia attributo-valore. Un qualsiasi altro elemento della rete può esprimere il proprio interesse a ricevere determinate informazioni inoltrando in modalità broadcast un opportuno

messaggio costituito da una lista di coppie attributo-valore (es.: area geografica, tempo, ecc.). In generale, la tecnica Direct Diffusion prevede le seguenti fasi:

- **Interest e Gradient** : Un elemento della WSN interessato a determinate informazioni (generalmente un sink), inoltra la sua richiesta di *interesse* (interest) in modalità flooding. Questo primo passaggio ha solo il fine di scoprire i nodi proprietari delle informazioni d'interesse. Viene associata ad ogni possibile rotta dal nodo proprietario dell'informazione al richiedente una misura (gradiente) relativa alla qualità (es: bit rate, ritardi), affidabilità (es.: livello di disturbo), ecc. e tra tutte le possibili alternative si sceglie la migliore (o un insieme ristretto di scelte migliori) da utilizzare per il trasferimento delle informazioni richieste;
- **Data Propagation** : Una volta ricevuta una dichiarazione di interesse e verificata la pertinenza con le funzionalità del nodo. Il nodo stesso diventa la sorgente dell'informazione che viene inoltrata verso il richiedente seguendo le rotte costruite con il criterio del gradiente. Se il messaggio arriva ad un nodo che non ha interesse a gestirlo, il messaggio viene eliminato dal nodo e non più inoltrato ai vicini;
- **Reinforcement** : Una volta attivata la procedura di raccolta delle informazioni dalla WSN, sulla base dell'invio della dichiarazione di interesse, il nodo richiedente (sink) può rinforzare la sua richiesta aggiungendo ulteriori specifiche che, ad esempio, consentano di eliminare percorsi poco affidabili o con bit rate basso a favore di alternative migliori.

La tecnica Direct Diffusion opera in modalità reattiva query-driven e quindi non si adatta ad applicazioni che richiedono un continuo invio di dati verso il sink.

8.7.2 Sensor Protocols for Information via Negotiation (SPIN)

Il protocollo SPIN si basa sulla diffusione nella WSN non delle informazioni vere e proprie acquisite ma bensì di una loro descrizione (metadati). Prima che avvenga la trasmissione dell'informazione vera e propria, il nodo invia un pacchetto ADV che pubblicizza ai vicini il metadato corrispondente all'informazione di cui è proprietario. Ogni nodo vicino interessato all'informazione risponde al messaggio ADV con una messaggio di richiesta di invio (REQ) e successivamente riceve l'informazione (DATA). A questo punto il processo si ripete per i nuovi proprietari dell'informazione che in questo modo concorrono a distribuire la stessa a tutti i nodi interessati della WSN. È evidente che SPIN non garantisce il trasferimento dell'informazione a tutti in nodi interessati, si consideri come esempio il caso di un nodo interessato che però si trova distante dal proprietario dell'informazione, il quale a sua volta, ha tutti i vicini non interessati a riceverla. SPIN consente di migliorare le prestazioni rispetto alla tecnica Flooding evitando di inviare inutilmente le informazioni raccolte dai nodi ed eliminando la ridondanza nella diffusione delle stesse.

8.8 In-Network Processing

In una WSN i nodi sensori hanno la responsabilità di acquisire informazione dal contesto in cui sono collocati e di trasferirla ai centri di raccolta (sink). In generale in una WSN si hanno delle limitazioni, anche consistenti, per quanto riguarda il consumo di potenza ammissibile e la banda di canale (rate di trasmissione). Inoltre, molto spesso, le misure acquisite da sensori diversi, ma in prossimità tra loro, possono risultare correlate. Per queste ragioni spesso non è efficiente trasmettere direttamente l'informazioni raccolte dai sensori verso uno stesso sink. Le metodologie base impiegate per limitare la ridondanza dell'informazione trasferita al sink, contenere la congestione della rete e ridurre il consumo di potenza per le comunicazioni sono:

- **Data Aggregation:** Per *data aggregation* si intende la combinazione di informazioni (messaggi) generati da sensori diversi in un singolo messaggio. Esempi tipici di operazioni di data aggregation sono il calcolo di parametri statistici relativi ad una sequenza di misure (media, deviazione standard, mediana, ecc.);
- **Data Fusion:** In questo caso per *data fusion* si intende un processo di elaborazione delle informazioni acquisite individualmente da sensori diversi che permettono di rendere disponibili informazioni non rilevate direttamente (aumenta il contenuto semantico dei dati). Questo, riportato ad esperienze della nostra vita quotidiana, è paragonabile ad un medico che prima di diagnosticare una malattia pone più domande al paziente non limitandosi ad una sola.

8.8.1 Clustering

Il concetto di *clustering* è molto comune in computer science. In generale esso consiste nel partizione un insieme di oggetti, dispositivi in gruppi secondo un opportuno criterio (es.: distanza reciproca, possesso di una stessa caratteristica, ecc.). In una WSN i metodi di clustering sono particolarmente efficaci per migliorare l'inoltro dei messaggi dalla rete verso l'esterno e viceversa o per ridurre i domini di collisione (la WSN viene suddivisa in sottoreti). Due tecniche di clustering molto conosciute ad oggi sono:

- a. Low-Energy Adaptive Clustering Hierarchy (LEACH);
- b. Hybrid Energy-Efficient Distributed Clustering (HEED).

8.8.2 Low-Energy Adaptive Clustering Hierarchy (LEACH)

È una tecnica di clustering che consente di distribuire il dispendio di potenza in maniera equa tra tutti i nodi della WSN e di conseguenza massimizzare il tempo di operatività (life time) della rete stessa. Questa tecnica consente di integrare funzionalità di data aggregation cercando di limare la ridondanza nei dati trasmessi al sink. Lo scopo di questo protocollo è quello di scegliere in maniera

random alcuni nodi ed eleggerli a capo-cluster (clusterhead - punto di riferimento per un cluster). Gli altri nodi, invece, si associano ad un cluster in modo da minimizzare la dissipazione di energia. Il clusterhead ha il compito di gestire le comunicazioni con i nodi del proprio cluster e tra esso ed il sink. Questa funzionalità comporta una dispendio di potenza consistente ed è per questo motivo che il ruolo di clusterhead non è permanente. Periodicamente il clusterhead viene ridefinito in maniera da distribuire il consumo di potenza in maniera il più possibile equa tra i nodi della rete.

L'approccio sul quale si basa il protocollo è fondato sulle seguenti due assunzioni: (i) esiste un'unico sink con la quale tutti i nodi devono comunicare; (ii) tutti i nodi hanno la possibilità di comunicare direttamente con il sink.

la modalità di funzionamento della tecnica LEACH è la seguente :

1. Si definisce a priori il numero p di nodi che devono svolgere il ruolo di clusterhead;
2. Ogni nodo sceglie un numero n con probabilità uniforme entro l'intervallo $[0, 1]$;
3. Si definisce come valore di soglia di riferimento il termine $T(n)$ dato da :

$$T(n) = \begin{cases} \frac{p}{1-p} r \ mod(\frac{1}{p}) & \text{se } n \in G; \\ 0 & \text{altrimenti,} \end{cases} \quad (8.1)$$

dove r indica il numero del round di elezione e G indica il numero di nodi che negli ultimi $1/p$ round di elezione non sono stati selezionati come clusterhead. Da notare che al primo passo tutti i sensori hanno la stessa possibilità di essere eletti clusterhead.

4. I rimanenti nodi della WSN si associano ai p clusterhead tipicamente in accordo con un criterio di prossimità.

8.8.3 Hybrid Energy-Efficient Distributed Clustering (HEED)

Questa tecnica si può considerare come una evoluzione della LEACH. Supponiamo di avere una WSN composta da n nodi distribuiti in un determinato ambiente. Il problema che vogliamo risolvere è determinare il numero di clusterhead necessari per la nostra applicazione. Ogni nodo può essere connesso ad uno ed uno solo dei clusterhead e può comunicare direttamente (un hop) con esso. La metodologia HEED prevede l'espletamento di tre fasi in sequenza :

- a. inizializzazione;
- b. selezione dei clusterhead;
- c. set-up delle sottoreti (cluster).

L'importante differenza rispetto alla tecnica LEACH è l'utilizzo dell'informazione relativa all'energia residua per ogni nodo durante la procedura (ancora di tipo random) di elezione dei clusterhead. In particolare, ogni nodo definisce la probabilità CH_{prob} con cui può essere eletto clusterhead in questo modo:

$$CH_{\text{prob}} = C_{\text{prob}} \cdot \frac{E_{\text{res}}}{E_{\text{max}}} \quad (8.2)$$

dove:

- C_{prob} indica la probabilità iniziale che un nodo sia eletto clusterhead ottenuta come rapporto tra il numero di clusterhead fissato ed il numero totale dei sensori nella WSN;
- E_{res} è la stima della energia disponibile al nodo;
- E_{max} è il valore massimo di riferimento dell'energia assunto, nel nostro caso, uguale per tutti i nodi.

Il protocollo HEED è detto ibrido in quanto il clusterhead è individuato su base statistica in relazione al life time residuo (stimato) mentre i nodi si associano ad un clusterhead secondo il criterio di prossimità.

8.9 Uno Sguardo Verso il Futuro : Internet of Things e sue evoluzioni

Internet of Things (IoT) rappresenta un paradigma di comunicazione recentemente proposto che si sta imponendo come modello di riferimento per le comunicazioni sia wireless che wired tra dispositivi, processori e sensori. L'idea che ne sta alla base presuppone la presenza pervasiva di oggetti come i tag RFID, sensori, attuatori, smartphone, ecc., in quali in virtù di uno schema di indirizzamento globale sono capaci di interagire tra loro e di cooperare in maniera autonoma per conseguire obiettivi comuni. Il paradigma IoT oggi attrae un forte interesse per le sue prospettive di sviluppo tecnologico e le sue importanti ricadute sulla nostra società. L'obiettivo da raggiungere è quello di rendere completamente inter-operabili un insieme di dispositivi eterogenei sia per tecnologia realizzativa che per funzionalità e di conferire loro un elevato livello di intelligenza operazionale, in maniera da stimolare un comportamento autonomamente adattativo al contesto in cui operano, nel rispetto di specifici requisiti di affidabilità e sicurezza. Di conseguenza la visione che sottende l'evoluzione del paradigma IoT è quello di creare e rendere fruibile un contesto di comunicazione autonoma non solo tra dispositivi o oggetti intelligenti (*smart*) ma anche tra applicazioni che sostanziano le comunicazioni "*anytime, anywhere, anymedia, anything*". Le funzionalità principali di una IoT futura saranno quelle di consentire una piena mobilità delle sue componenti, di adattarsi opportunisticamente al contesto operativo consentendo la cooperazione tra tecnologie differenti, garantire una livello elevato di affidabilità e sicurezza delle comunicazioni ed, infine, attuare tutte

procedure tipiche dei sistemi automatici note come *self-properties*. La riconfigurazione autonoma di applicazioni su piattaforme eterogenee di comunicazione e calcolo sarà poi un'altra caratteristica funzionale di base delle future IoT.

Le metodologie di comunicazione saranno essenzialmente in modalità autonoma secondo l'emergente paradigma delle comunicazioni Machine-to-Machine (M2M) e Device-to-Device (D2D) in modo che si possano attivare collegamenti tra sensori, attuatori, processore per scambiare informazioni tra loro o direttamente con le applicazioni. Lo sviluppo della tecnologia IP ha decisamente favorito queste modalità di comunicazione permettendo di ridurre i tempi di ritardo e i consumi energici per i dispositivi coinvolti.

8.10 Le Body Area Network

Le Body Area Network (BAN) o Body Sensor Network (BSN), sono reti formate da dispositivi indossabili, il cui raggio di copertura è circa un metro. Nel dicembre del 2011 il gruppo di lavoro 6 facente parte della famiglia 802.15 approva lo standard per le Wireless Body Area Network denominato IEEE 802.15.6. Lo scopo primario di questo gruppo di lavoro è stato la realizzazione di uno standard compatibile con dispositivi che lavorano a stretto contatto con il corpo umano e le basse emissioni di potenza emanate dagli stessi. Le BAN trovano molte applicazioni soprattutto nel campo medico e dell'intrattenimento (personal entertainment)

Lo scopo del protocollo IEEE 802.15.6 è quello di fornire uno standard internazionale per comunicazioni a corto raggio, in prossimità (o addirittura all'interno) del corpo umano, a bassa potenza ed altamente affidabile. Una BAN generalmente lavora nelle bande ISM garantendo un data rate che può arrivare fino ad un massimo di 10 Mbps. Novità rispetto agli altri standard della famiglia 802.15 è quella di introdurre il concetto di Qualità del Servizio (QOS) nelle LLN. Grazie alla velocità di trasmissione dati, il protocollo è utilizzabile nel campo medico e più in generale nella fornitura di servizi sanitari. Le Wireless Personal Area Network (WPAN) non soddisfano le norme di comunicazione mediche (vicinanza al tessuto umano) e rilevanti per alcuni ambienti applicativi. Essi inoltre non supportano la QoS, sono a bassa potenza e bassa velocità di trasmissione dati. Prima dell'introduzione di questo standard, le reti personali non soddisfacevano le stringenti norme per poter introdurre tali dispositivi vicino al corpo umano. Inoltre non supportavano la QoS e potevano creare interferenze con altri dispositivi medici

La topologia di rete prevista dallo standard 802.15.6 è una topologia a stella, dove è presente un solo hub, ovvero il coordinatore della rete e, al massimo, 64 nodi. La comunicazione avviene, in modo bidirezionale, tra nodi e hub. E' comunque possibile creare una stella estesa ma, al massimo, dev'essere presente un solo nodo con funzionalità di relay per i nodi più lontani: in pratica la topologia permessa è o una comunicazione diretta tra noodi e hub oppure con un solo salto (hop) intermedio tra nodo e hub. Se due nodi vogliono comunicare tra di loro devono sempre inviare i loro messaggi al coordinatore della BAN.

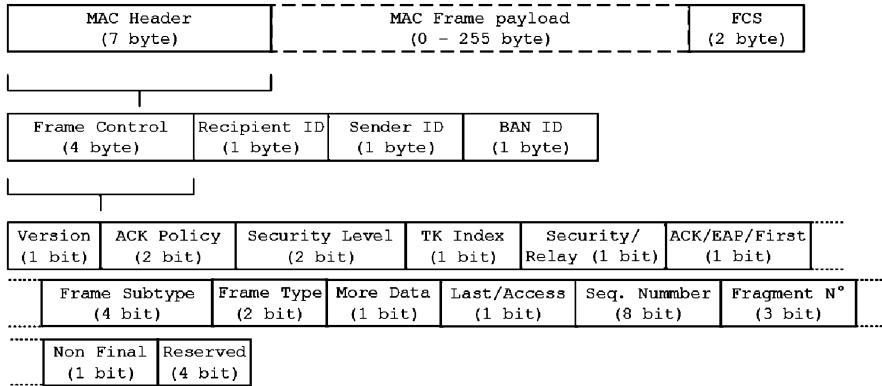


Figura 8.9: MAC frame per il protocollo IEEE 802.15.6

La comunicazione avviene dividendo l'asse temporale in superframe, tutti di durata temporale uguale; ogni superframe può essere suddiviso a sua volta in slot temporali della stessa durata. Il numero di slot temporali che compongono un superframe viene scelto dal coordinatore di rete (hub) al momento della creazione della BAN. Gli intervalli temporali vanno da un minimo di uno (quindi un superframe corrisponde a un intervallo temporale) ad un massimo di 256. Nella modalità beacon, l'hub comunica la durata di un intervallo temporale trasmettendo a tutti i nodi il beacon all'inizio (o in altri specifici intervalli) del superframe. Nella modalità senza beacon (beaconless), non viene trasmesso alcuna informazione all'inizio del superframe ma ovviamente è richiesta una sincronizzazione tra i dispositivi: l'hub comunica la durata del superframe trasmettendo particolari frame (T-Poll Frame). Quindi un hub può operare in uno dei seguenti tre modi:

- superframe con beacon;
- superframe senza beacon;
- Senza superframe senza beacon;

La tecnica di accesso al canale da parte dei nodi è scelta a discrezione dell'hub e può essere di tipo CSMA/CA oppure la Slotted Aloha. La tecnica Slotted Aloha viene, però usata solo se l'hub decide di adottare la tecnica superframe con beacon; negli altri due casi, hub e nodi, devono utilizzare la tecnica CSMA/CA.

La comunicazione tra nodo e hub può avvenire in modalità sicura o insicura. Per cambiare la modalità di comunicazione (quindi passare da insicura a sicura o viceversa) il nodo si deve disconnettere e iniziare una nuova connessione.

Il frame MAC è diviso in tre campi principali: un header di lunghezza fissa (7 byte), diviso a sua volta in quattro campi, un frame body di lunghezza variabile (la cui lunghezza è compresa tra zero e 255 Byte) e un frame check sequence (FCS) di lunghezza fissa (2 Byte). Il frame MAC è mostrato in figura 8.9.

Ogni rete BAN ha un identificativo lungo un byte (BAN_ID), l'identificativo viene scelto dall'hub al momento della formazione della rete. Ovviamente un hub deve scegliere una BAN_ID che non è stata scelta dagli hub vicini. Ogni hub e ogni nodo hanno un identificativo univoco di un byte che li distingue all'interno della rete. I valori che possono assumere tali identificativi vanno da 0x02 a 0xF5. Gli altri valori sono usati per particolari scopi (come ad esempio per l'invio in broadcast dei messaggi di connessione, oppure per l'invio in multicast). Questo identificativo non va confuso con l'indirizzo MAC del dispositivo: ogni dispositivo è in possesso del suo indirizzo EUI-48.

Il livello fisico è il responsabile dell'attivazione e della disattivazione del transceiver, deve offrire il Clear Channel Assessment per il canale adoperato e deve trasmettere e ricevere i dati. Questo protocollo prevede l'uso di tre diversi livelli fisici:

- *banda stretta*: opera in determinate bande, in particolar modo i dispositivi che usano il livello fisico a banda stretta devono lavorare nelle bande: 402 - 405 MHz, 420 - 450 MHz, 863 - 870 MHz, 902 - 928 MHz, 950 - 958 MHz, 2360 - 2400 MHz, 2400 - 2483.5 MHz. Le modulazioni usate sono una DPSK o una GMSK con fattore M=2. Con questo livello fisico si arriva ad un massimo di 971.4 Kbps di data rate;
- *Ultra WideBand*: questo livello fisico è stato progettato per offrire alte prestazioni, robustezza, bassa complessità e basse emissioni di potenza. Esistono due differenti tipi di tecnologia UWB: impulsi radio UWB (IR-UWB) e modulazione di frequenza UWB (FM-UWB). L'hub può avere un transceiver con tecnologia IR-UWB oppure può implementare entrambe le tecnologie. I nodi invece possono avere un transceiver IR-UWB o un transceiver FM-UWB oppure un transceiver che implementi entrambi;
- *Human Body Commuication*: questo livello fisico implementa la tecnologia Electric Field Communication (EFC) la quale permette di avere un raggio di copertura vicino ai 30 m. La banda è centrata a 21 MHz ed ha una maschera molto rigida per ridurre al minimo le interferenze con gli altri dispositivi. Il data rate raggiunto con questo livello fisico è di 1312.5 Kbps.

Recentemente, nel 2013, è stato presentato lo standard IEEE 802.15.4j. Questa evoluzione cerca di fondere le reti personali wireless a basso rate (LR-WPAN) con le BAN: presenta un livello fisico alternativo per supportare le Medical Body Area Network (MBAN) nella banda 2360 - 2400 GHz. La definizione di questo standard si è resa necessaria per attenersi alle normative imposte dalla FCC in materia di applicazione nel settore medico.

8.11 Letture Consigliate

Gli argomenti affrontati in questo capitolo sono trattati in molti testi e pubblicazioni scientifiche. Tra essi si segnalano per approfondimenti e complementi:

F. Dresler, "Self-Organization in Sensor and Actor Networks", J. Wiley, 2007.

I.F. Akyildiz, X. Wang, "A Survey on Sensor Networks", *IEEE Communications Magazine*, pagg.102, 116, agosto 2002.

R. Shorey, A. Ananda, M. Choon Chan, W. Tsang Ooi, Mobile, Wireless, and Sensors Networks : technology, Applications and Future Directions, John Wiley, 2006.

M. Ilyas, I. Maghoub, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004.

Gli standard IEEE sono disponibili, gratuitamente e in formato pdf, sul sito IEEE (<http://standards.ieee.org>). Si suggeriscono in particolare i seguenti documenti tecnici:

IEEE standard for information technology – local and metropolitan area networks– specific requirements – part 15.1: Wireless medium access control (mac) and physical layer (phy) specifications for wireless personal area networks (wpans), Giugno 2005.

<http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf>;

IEEE standard for information technology – local and metropolitan area networks– specific requirements – part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (wpans), IEEE Standard for Local and metropolitan area networks, Luglio 2006.

<http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>;

IEEE standard for information technology – local and metropolitan area networks – specific requirements – part 15.6: Wireless body area networks, Febbraio 2012.

<http://standards.ieee.org/getieee802/download/802.15.6-2012.pdf>.

Per maggiori informazioni sul funzionamento di 6LoWPAN si rimanda alla lettura degli RFC, oppure al testo:

Zach Shelby and Carsten Bormann, "6LoWPAN: The Embedded Internet", J.Wiley, 2009.

N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," Agosto 2007.

<http://www.ietf.org/rfc/rfc4919.txt>;

Infine una presentazione dettagliata degli standard IEEE 802.15 è disponibile al sito web:

<http://www.wikipedia.org/>

Materiale tutoriale e di approfondimento è inoltre reperibile al sito:

<http://ieeexplore.ieee.org/Xplore/home.jsp>

9

Rete ISDN

Gli sviluppi tecnologici nel settore dei sistemi per l'elaborazione delle informazioni, insieme ad una crescente necessità di comunicazioni fra dispositivi, oltre che tra persone, ha determinato la necessità di una più stretta integrazione funzionale tra metodologie di comunicazione differenti (voce, video, dati). Questo percorso è stato poi decisamente facilitato dal fatto che la tecnologia trasmittiva di tipo numerico era ormai diventata lo standard di riferimento rendendo così disponibile una modalità unificata per la gestione di flussi informativi diversi. Le prime reti pubbliche, concepite espressamente per collegamenti dati, furono basate sulla raccomandazione X.25 e prendevano una gestione separata dei collegamenti dati e delle comunicazioni voce classiche. Con il crescere delle esigenze di accesso dati divenne pressante la necessità di definire per l'utente una fornitura integrata di servizi facilitandone l'accesso mediante la definizione di un terminale multifunzione e multiservizio in grado cioè di gestire in modo indifferenziato connessioni voce, dati, o multimediali. Nasceva quindi quella che è stata definita la rete ISDN, che sintetizza in questa sigla la denominazione *Integrated Services Digital Network* (rete integrata nelle tecniche e nei servizi). Questa rete ha consentito l'integrazione funzionale di metodologie differenti, proprie di reti monoservizio, per il trasporto dell'informazione sfruttando la flessibilità derivante dall'impiego di una tecnologia trasmittiva completamente numerica e definendo una interfaccia standard per l'accesso ai servizi offerti in modo integrato.

Nel seguito si descriveranno le caratteristiche generali della raccomandazione X.25 che, sebbene ad oggi rappresenti una tecnologia di rete non più adatta per molte delle attuali applicazioni richieste dall'utente, ci consentirà di affrontare per la prima volta le problematiche base di una rete pensata per la trasmissione dati. Successivamente, verranno descritte la rete Frame Relay e la rete ISDN dove la raccomandazione X.25 trova applicazione, in termini di architettura protocollare e differenti alternative di interfaccia utente-rete.

9.1 Raccomandazione X.25

La raccomandazione X.25 si rivolge principalmente alla definizione delle modalità di interfaccia utente-rete. Per meglio acquisire questo concetto possiamo riferirci al caso pratico di una spedizione di un plico illustrata in figura 9.1.

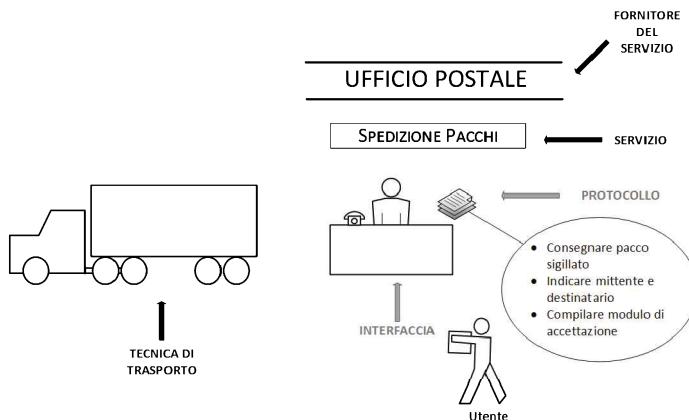


Figura 9.1: Servizio spedizioni

La persona interessata accede al servizio "spedizione" mediante un'interfaccia di accesso (ad esempio compila la lettera di vettura). Il plico viene poi consegnato all'incaricato per il suo ritiro o ad un ufficio apposito. La compagnia che gestisce il processo di spedizione provvederà poi con una tecnica non percettibile all'utente a recapitare il plico al suo destinatario.

La raccomandazione X.25 prevede una architettura protocollare a livelli. In particolare sono stati previsti tre livelli che hanno funzionalità corrispondenti ai primi tre livelli (Fisico, Collegamento e Rete) di OSI:

- *Livello Fisico*: definisce le modalità di accesso al mezzo trasmissivo;
- *Livello Collegamento*: si preoccupa di garantire su base link-to-link l'integrità della trasmissione. Questa funzionalità è particolarmente importante in questo contesto per la vulnerabilità del mezzo fisico previsto (bassa qualità) per collegamenti;
- *Livello Pacchetto*: definisce le procedure di utilizzo dei circuiti virtuali per realizzare la multiplazione dei flussi dati.

Sono poi previsti due servizi base :

- *Chiamata Virtuale* (VC): necessita di una fase di set-up per ogni richiesta di collegamento;
- *Chiamata Virtuale Permanente* (PVC): prevede che il cammino virtuale tra due utenti sia preventivamente definito e reso disponibile senza ritardi di accesso (non richiede la fase di set-up) ad ogni necessità di collegamento.

Lo standard identifica gli apparati di utente come *Data Terminal Equipment* (DTE) e il nodo della rete a cui il DTE è connesso come *Data Circuit Equipment* (DCE). In particolare la raccomandazione X.25 si preoccupa solo di definire le

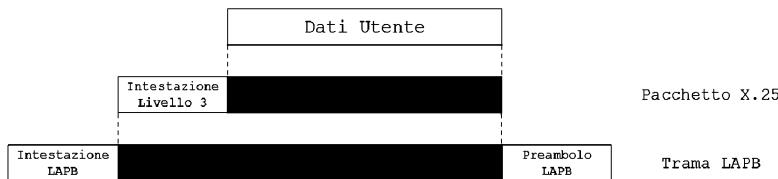


Figura 9.2: Incapsulamento della raccomandazione X.25

modalità di interfaccia tra DTE e DCE. Anche per X.25 vale l'analogia dell'incapsulamento sequenziale, proprio della modalità di gestione delle interfacce tra livelli contigui di OSI, illustrato nella figura 9.2.

I dati dell'utente arrivano al livello 3 che aggiunge le proprie informazioni di controllo definendo quello che viene indicato come pacchetto X.25. Queste informazioni sono utilizzate per:

- Identificare con una etichetta (numero) un circuito virtuale specifico a cui i dati devono essere associati;
- Introdurre la numerazione di sequenza per identificare ogni pacchetto di uno stesso flusso (controllo errore).

Il pacchetto X.25 viene poi passato al livello 2 che provvede a creare la trama LAPB illustrata in figura 9.3.

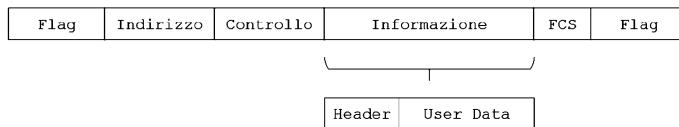


Figura 9.3: Link Access Procedure Balanced

Il *Flag* è costituito da una sequenza nota di 8 bit (01111110) che serve per delimitare le trame LAPB (inizio e fine). Poiché il contenuto del campo dati non è predicibile potrebbe capitare che la sequenza di *Flag* sia accidentalmente presente nel campo dati facendo erroneamente interpretare questo come una indicazione di fine trama. Per evitare questo inconveniente viene utilizzata la tecnica del *bit stuffing* che consiste nell'inserire in fase di trasmissione fittiziamente un bit 0 quando viene riscontrata nel campo dati una sequenza di cinque 1 che segue un bit 0. In ricezione si eseguirà l'operazione opposta: si scarterà ogni bit 0 che segue una sequenza 011111.

9.1.1 Multiplexing

Il multiplexing è la funzionalità che caratterizza maggiormente X.25 e che permette ad uno stesso DTE di avere fino a 4095 circuiti virtuali simultanei con altrettanti DTE della rete con una sola connessione fisica DTE-DCE. Il DTE può,

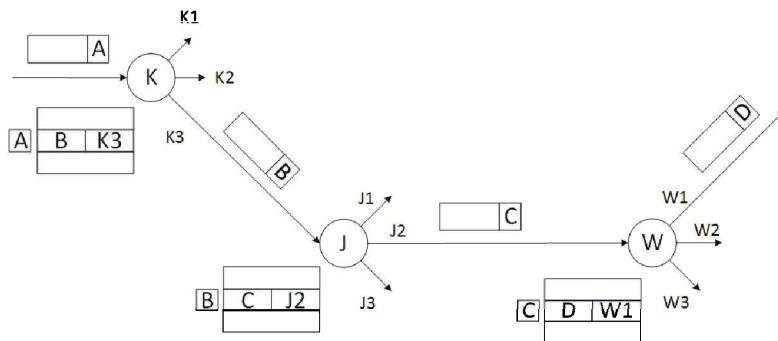


Figura 9.4: Commutazione in X.25

a sua descrizione, assegnare le etichette dei circuiti virtuali possibili ai vari collegamenti attivati, a loro volta associati ad applicazioni specifiche. La modalità di gestione di un circuito virtuale è full duplex. Per associare i pacchetti ai circuiti virtuali appropriati ogni pacchetto prevede un campo nella testata (header) di 12 bit. L'identificativo del circuito ha valore solo locale ed è riferito al collegamento fisico che lo ospita. Questa procedura trova un riscontro anche nel modo di gestire la commutazione nei nodi di transito di una rete X.25. Questa consiste di due fasi :

- associare l'identificativo di canale logico (circuito virtuale) relativo ad una linea in ingresso con un nuovo identificativo di canale logico relativo alla linea di uscita richiesta;
- inoltrare il pacchetto verso la stessa linea.

La procedura di commutazione è mostrata nella figura 9.4.

9.2 Frame Relay

Le reti basate sulla tecnologia Frame Relay utilizzano la modalità di inoltro dei flussi informativi a circuito virtuale e sono state pensate per realizzare in forma efficiente e flessibile l'interconnessione di apparati in una rete WAN (Wide Area Network). Il predecessore della tecnologia Frame Relay è stata la raccomandazione X.25 discussa nel paragrafo precedente dalla quale è stata mutuata la modalità a circuito virtuale. La raccomandazione X.25 prevede di realizzare la commutazione a livello 3 (rete) e presenta le seguenti principali criticità riguardo una crescente esigenza di collegamenti dati veloci ed affidabili:

- La velocità di accesso di riferimento è 64Kbps (lenta rispetto alle nuove esigenze);
- Il mezzo fisico è pensato di bassa qualità per cui sono previsti dei meccanismi onerosi in termini di complessità e tempi di esecuzione al livello 3 (con-

trollo del flusso) ma soprattutto a livello 2, per garantire un livello adeguato di integrità dell'informazione trasmessa;

- Necessita che i pacchetti scambiati tra utenti di reti TCP/IP siano resi compatibili (livello 3) con il formato previsto e questo comporta l'incapsulamento dei datagrammi IP in pacchetti di livello 3 di X.25 con conseguente aumento dei tempi di elaborazione.

Le reti Frame Relay hanno permesso di superare queste criticità e si sono proposte come una tecnologia di collegamento particolarmente attraente per organizzazioni con più sedi decentrati soprattutto in confronto con quanto le reti pubbliche potevano offrire.

Le principali caratteristiche di una rete Frame Relay sono:

- Permette velocità di accesso elevate che possono arrivare, partendo da una velocità di riferimento di 1,544 Mbps fino a 44,376 Mbps;
- Prevede un'architettura protocollare semplificata e limitata ai primi due livelli OSI, proponendosi quindi come soluzione efficiente per il collegamento veloce di reti TCP/IP;
- Consente un'allocazione di capacità di accesso variabile e scalabile in relazione alle esigenze dell'utente;
- Ha la possibilità di inoltrare pacchetti di dimensioni notevolmente superiori a X.25 (9 Kbyte) evitando l'aggravio computazione della frammentazione dei flussi;
- Ha un costo competitivo in confronto con altre tecnologie di collegamento veloce;
- Attua procedure per garantire l'integrità della trasmissione limitate alla sola rilevazione di errore e confinate nello strato collegamento in modalità non affidabile (i frame corrotti da errori vengono scartati).

La figura 9.5 illustra un esempio di utilizzo di una rete Frame Relay.

La caratteristica della tecnologia Frame Relay è quella di associare ad ogni circuito virtuale attivato un identificativo denominato *Data Link Connection Identifier* (DLCI). Questa metodologia è simile a quella impiegata in X.25 per identificare flussi informativi distinti nel multiplexer su uno stesso supporto trasmissivo. Anche Frame Relay come X.25 prevede due diverse tipologie di circuiti virtuali:

- *Circuito Virtuale Temporaneo* : è reso disponibile sulla base di una richiesta specifica di connessione. Necessitano della fase di set-up iniziale e sono terminati quanto la necessità di collegamento non sussiste più;
- *Circuito Virtuale Permanente*: è reso disponibili senza limitazioni di tempo e tra utenti che ne hanno fatto richiesta preventiva (saranno quindi

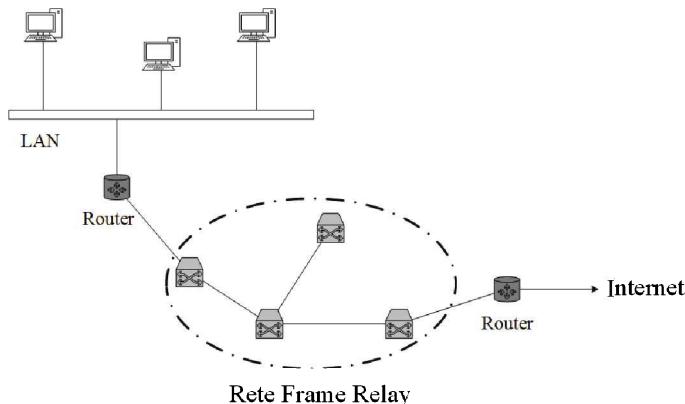


Figura 9.5: Rete Frame Relay

programmati di conseguenza tutti gli apparati di rete preposti ad attuarli). Non necessita della fase di set-up ed essendo sempre disponibile non soffre di ritardi di accesso. Gli svantaggi tipici di questa soluzione sono principalmente un costo levato giustificato dalla disponibilità immediata ed esclusiva del collegamento e la limitazione a una sola coppia di utenti.

La commutazione in una rete Frame Relay viene realizzata sulla base di una tabella che associa il DLCI di un flusso su una certa linea di ingresso ad una nuova coppia DLCI, linea di uscita desiderata.

La figura seguente illustra la struttura protocollare a strati per reti Frame Relay.

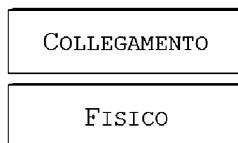


Figura 9.6: Architettura protocollare Frame Relay

Come precedente anticipato l'architettura Frame Relay è di tipo semplificato e prevede, in particolare, solo la specifica del livello fisico e del livello collegamento.

9.3 Principi di ISDN

Le reti ISDN furono inizialmente sviluppate sulla base della prospettiva di diventare il modello di riferimento per le reti di telecomunicazioni per integrare tecnologie di trasporto diverse ed offrire un'ampia gamma di servizi agli utenti. La rete ISDN è stata definita mediante la standardizzazione di una interfaccia

di utente ed ha avuto come obiettivo quello di un utilizzo ottimizzato delle infrastrutture di rete preesistenti, pretendono comunque un aggiornamento tecnologico nelle loro componenti fondamentali ed unificando le procedure di accesso. Una rete ISDN consente a diverse tipologie di apparato di utente di accedere alla rete mediante una unica interfaccia con modalità a commutazione di circuito, a commutazione di pacchetto o anche di tipo esclusivo (dedicata). Gli obiettivi funzionali e di servizio che ISDN si è posta hanno richiesto un adeguamento di tutte le procedure a supporto della rete stessa come ad esempio la segnalazione la quale, in particolare, è realizzata secondo un sistema di segnalazione a canale comune in accordo con il protocollo SSN7 descritto nel capitolo 10.3.

Gli standard ISDN sono stati definiti da ITU-T e raccolti in documenti (raccomandazioni) indicati come *Serie-I*. I principi propri di ISDN sono:

- Supporto di un'ampia gamma di servizi per collegamenti fonici e dati con un numero limitato di interfacce e con adeguate funzionalità (dati);
- Capacità di supportare sia la commutazione di circuito sia quella a pacchetto con la possibilità di definire anche collegamenti dedicati (non commutati);
- Connessioni a commutazione di circuito o pacchetto a 64 Kbps. Questo tasso di trasmissione fu selezionata per argini di compatibilità con le reti *numeriche integrate* (Integrated Digital Network - IDN) che sono state le prime reti a consentire non solo trasmissione dati, ma anche trasmissioni vocali, testuali e video, utilizzando come elemento comune un'unica tecnica numerica capace di supportare, almeno nei collegamenti punto-punto, capacità dell'ordine di 64 kbps;
- Intelligenza di rete in grado di poter implementare servizi più evoluti rispetto alla solo instaurazione di un collegamento a commutazione di circuito;
- Architettura della rete a livelli riconducibile al modello OSI. Questa caratteristica consente di utilizzare standard sviluppati per applicazioni OSI come ad esempio il livello 3 della raccomandazione X.25 per gestire l'accesso ai servizi a commutazione di pacchetto di ISDN;
- Varietà di configurazioni fisiche per implementare la rete ISDN in maniera che sia rese compatibili con differenze tecnologiche degli apparati di rete sviluppati da costruttori diversi e di richiesta di servizi da parte degli utenti.

La figura 9.7 offre una visione concettuale di una rete ISDN ponendosi dal lato utente. Un utente di tipo residenziale si prevede abbia necessità diverse di accesso alla rete da quelle di tipiche di comunità di utenti professionali che generalmente richiederà di connettersi alla rete tramite un centralino locale (PBX).

L'architettura tipica di una rete ISDN è mostrata in figura 9.8 dove si può notare che tra il nodo della rete (commutatore ISDN) che gestisce direttamente

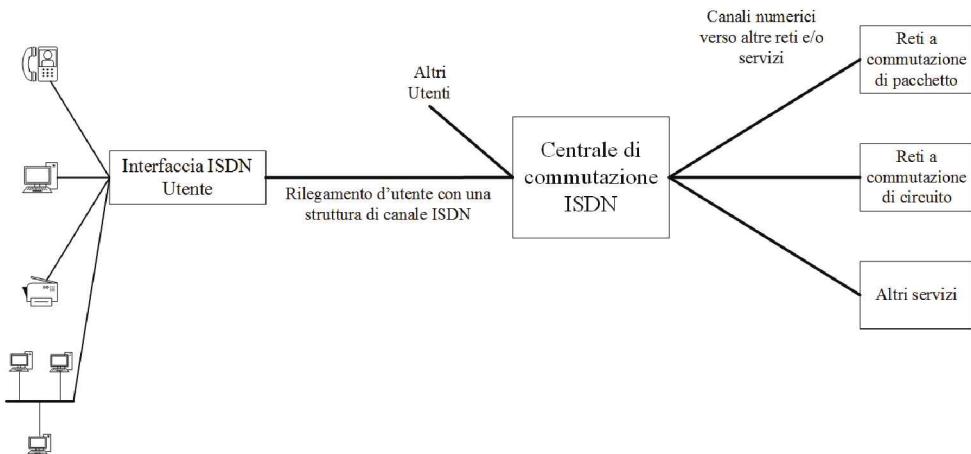


Figura 9.7: Esempio di connessione ISDN

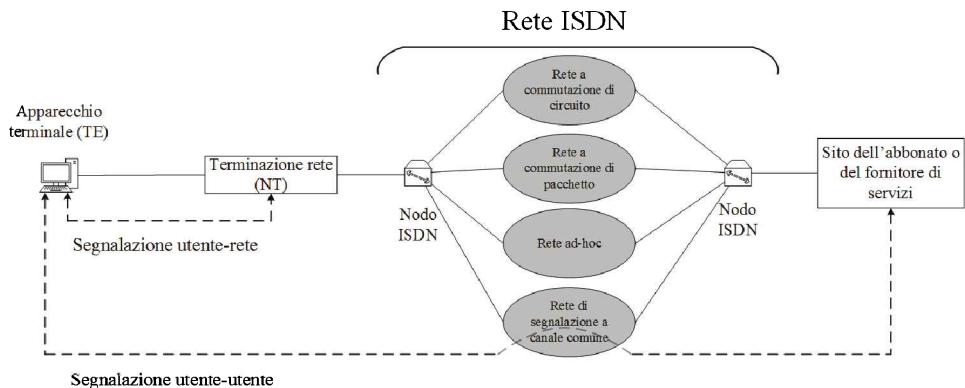


Figura 9.8: Architettura ISDN

la connessione dell'utente sorgente e il nodo di rete a cui è connesso il terminale utente di destinazione può esserci o una rete a commutazione di pacchetto, o una rete a commutazione di circuito o perfino reti specifiche (altri tipi di rete nella figura). Infine ISDN rende disponibile l'accesso ad una rete di segnalazione a canale comune, implementata sulla base del protocollo SSN7, per rendere fruibili tutti i servizi previsti dalla rete.

9.4 Canali ISDN

L'interfaccia ISDN, dal punto di vista fisico, è basata su classico doppino telefonico, mentre dal punto di vista logico, il trasporto delle informazioni è strutturato sulla base dei seguenti tipi di canale:

- *Canale B* a 64 Kbps;
- *Canale D* a 16 o 64 Kbps;
- *Canale H* a 384 Kbps (H0), 1536 Kbps (H11) o 1920 Kbps (H12)

Il *canale B* è il canale base di un utente ISDN. esso può essere dedicato ad un collegamento telefonico (numerico) o per la trasmissione dati. Esso ammette quattro diverse modalità di connessione:

- Comutazione di circuito: è la modalità classica per la gestione di chiamate telefoniche. Rispetto a reti tradizionali, in questo caso la segnalazione di rete viene veicolata su un canale diverso (Canale D);
- Comutazione di pacchetto: la connessione di utente è verso un nodo di rete in grado di gestire comunicazioni dati a pacchetto in accordo con la raccomandazione X.25;
- A trama: in questo caso il terminale di utente è connesso da un nodo che opera in accordo con il protocollo Frame Relay;
- Dedicata: è una connessione permanente (o semipermanente) attivata precedentemente (quindi disponibile immediatamente) tra due utenti.

Il *canale D* ha due finalità. la prima è quella di trasferire le informazioni di segnalazione per controllare le chiamate foniche relative a *canali B* relative ad una stessa interfaccia di utente. La seconda prevede l'uso di questi canali per veicolare dati a basso bit rate (telemetria, allarmi).

I *canali H* sono canali in grado di supportare trasferimento di flussi informativi a tassi superiori rispetto ai *canali B*. Questi canali possono essere utilizzati per trasportare flussi aggregati in modalità TDM. Le applicazioni specifiche verso le quali questa tipologia di canali si rivolge includono la trasmissione veloce di testi ed immagini, collegamenti video, dati ad alta velocità, multiplazione di flussi dati a basso rate ad esempi relativi a sistemi di monitoraggio e controllo.

I canali prima descritti sono organizzati in maniera ordinata in strutture di trasmissione che costituiscono le interfacce ISDN o tipologie di accesso. In particolare si ha:

- *Accesso Base*: prevede l'aggregazione (full duplex) di due canali di tipo B e un canale di tipo D a 16 Kbps per un accesso (utile) ad un rate di riferimento di 144 Kbps. la necessità di prevedere di bit aggiuntivi per la sincronizzazione, la gestione della struttura a trama ed informazione di overhead porta il rate totale sul collegamento a 192 Kbps. La trama è formata da 48 bit ed include 16 bit per ciascuno dei canali B e 4 bit per il canale D. Questa tipologia di accesso è stata pensata per soddisfare le esigenze di utenti residenziali permettendo la possibilità simultanea di due collegamenti voce o di far coesistere un collegamento voce con servizi differenti a commutazione di pacchetto.;

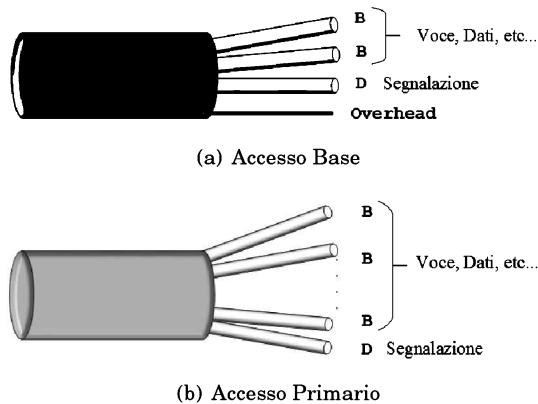


Figura 9.9: Accessi ISDN

- **Accesso Primario:** è stato pensato per utenti con esigenze più specifiche (professionali). Questa tipologia prevede un capacità aggregata di trasferimento pari a 2048 Kbps. In questo ambito possono essere previsti canali 30 canali tipo B e un canale di tipo D a 64 Kbps oppure come alternativa canali tipo H per un accesso a velocità più elevata.

La figura 9.9 mostra schematicamente la topologia di accesso base e di accesso primario basato su canali di tipo B e D.

9.5 Accesso alla Rete

Per arrivare alla definizione dell'accesso di utente alla rete lo standard prevede la definizione di :

- **Gruppi Funzionali:** si riferiscono ad un numero finito di configurazioni di apparati o aggregazioni di essi;
- **Punti di Riferimento:** si riferiscono ad una separazione logica dei gruppi funzionali.

Riassumendo, possiamo dire che l'architettura del sito di utente è strutturata in gruppi funzionali, separati da punti di riferimento, a loro volta relativi a specifiche modalità di interfaccia. Le ragioni alla base di questa filosofia si possono ricondurre a quelle che hanno dato origine all'architettura a livelli di una rete di telecomunicazioni. Anche in questo caso una volta definite le modalità di interfaccia i gruppi funzionali potevano essere individualmente aggiornati o sostituiti senza influenzare l'intera struttura.

I gruppi funzionali previsti sono:

- **Network Termination 1 (NT1):** prevede le funzionalità associate alla terminazione ISDN al sito utente. Corrisponde al livello fisico di OSI e definisce

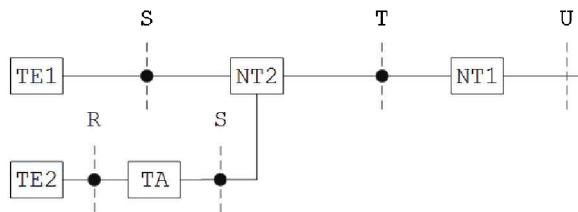


Figura 9.10: Modello di riferimento delle interfacce ISDN

una separazione tra le metodologie tecnologiche proprie della rete e gli apparati di utente. Fornisce supporto alle operazioni di manutenzione della rete. NT1 prevede la gestione di canali multipli (es.: 2B+D) mediante una tecnica di multiplexing sincrono a livello fisico. Permette la modalità *multi-drop* che consiste nella possibilità di gestire tramite l'unica interfaccia NT1 contemporaneamente un telefono, un accesso dati (computer) e due accessi relativi a sensistica di controllo.

- *Network Termination 2 (NT2)*: è riferito ad un dispositivo più complesso ed precedente in grado di operare fino al livello rete di OSI. Implementa funzionalità di commutazione e concentrazione. Un esempio tipico di NT2 è un PBX capace di gestire sia traffico telefonico che accesso a rete LAN. Come applicazione si può considerare un accesso ad ISDN in modalità semipermanente che collega due siti di una stessa istituzione. Localmente NT2 opera in ingresso lo smistamento del traffico in ingresso verso le rispettive destinazioni mentre in uscita implementa la funzione di concertazione del traffico generato da dispositi differenti.
- *Network Terminator 1,2 (NT1)* : prevede le funzionalità combinate di NT1 e NT2.
- *Terminal Equipment (TE)* : si riferisce all'apparato di proprietà dell'utente che necessita di accesso alla rete ISDN. Si distinguono due tipi di TE :
 - *Terminal Equipment type 1 (TE1)* : si riferisce a dispositivi nativi ISDN che possono accedere direttamente alla rete;
 - *Terminal Equipment type 2 (TE2)* : si riferisce a tutti i dispositivi preesistenti non direttamente compatibile con un accesso ISDN. Questi dispositivi necessitano di un ulteriore apparato denominato *Terminal Adapter (TA)* per poter essere collegati alla rete ISDN.

La figura 9.10 illustra il modello di riferimento per le interfacce ISDN.

Nell'ambito della standardizzazione ISDN, non si fa riferimento all'interfaccia utente-rete in senso globale, ma, all'interno della stessa interfaccia, si fa riferimento a *punti di riferimento* che si articolano in :

- *Punto di Riferimento T* : corrisponde al punto di separazione tra gli apparati di rete e gli apparati di utente;

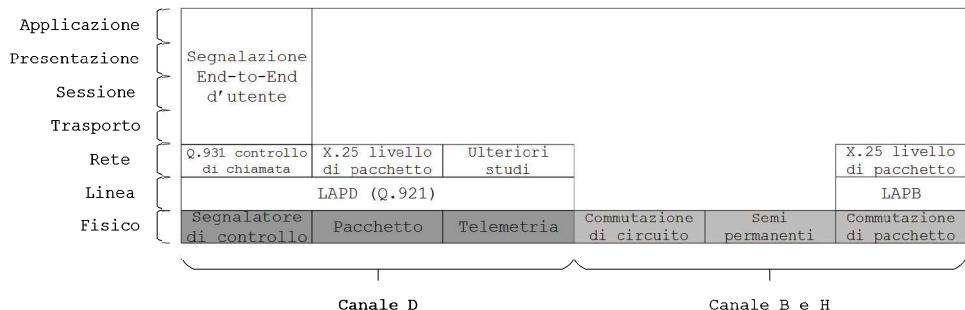


Figura 9.11: Protocolli ISDN

- *Punto di Riferimento S:* si riferisce all'interfaccia dei terminali ISDN standard individuai
- *Punto di Riferimento R:* si riferisce ai punti di interconnessione di apparati non a standard ISDN;
- *Punto di Riferimento U:* individua la connessione tra la centrale ISDN e NT1, può essere realizzata con un doppino di rame o (in futuro) con la fibra ottica.

9.6 Architettura protocollare

L'architettura protocollare di ISDN è mostrata nella figura 9.11 in riferimento alla gestione dell'accesso a canali di tipo B e tipo D. Nel caso di ISDN sono considerati solo i livelli 1-3 in quanto deputati a gestire l'accesso alla rete mentre non si hanno specifiche per il livelli 4-7 in quali sono di pertinenza dell'utente e quindi implementati su base end-to-end.

Il livello 1 è univoco per i due canali B e D e prevede due specifiche differenti per l'accesso base (I.430) e per l'accesso primario (I.431). Questo è conseguente al fatto che sia i canali di tipo B che di tipo D sono multiplati sulla stessa interfaccia fisica. La gestione dell'accesso si differenzia invece per quanto riguarda i due livelli superiori.

Per il canale di tipo D il livello 2 è indipendente dalla applicazione supportata ed è basato sul protocollo *Link Access Protocol, D Channel* (LAPD), una versione semplificata del protocollo *High Data Link Control* (HDLC) previsto nel livello 2 (collegamento) di OSI. Le applicazioni previste sono: *segnalazione di controllo, commutazione dati a pacchetto, telemetria*. In particolare il livello 3 per le applicazioni di *telemetria* non è stato specificato in maniera univoca mentre per le restanti due applicazioni esso prevede:

- *Segnalazione di controllo:* un protocollo per il controllo delle chiamate (I.451/Q.931) attivate tramite canali B;

- *Commutazione a pacchetto* : l'uso del protocollo di livello 3 di X.25 con pacchetti trasmessi in trame LAPD per gestire modalità di collegamento a circuito virtuale con dati a pacchetto.

Il canale di tipo B prevede tre applicazioni di riferimento:

- *Commutazione di circuito* : il collegamento viene attivato su canale B a richiesta tramite il protocollo di controllo di chinata previsto per il canale D;
- *Circuito semipermanente* : il collegamento è stabilito su canale B sulla base di una procedura di attivazione preventiva e concordata;
- *Commutazione a pacchetto* : la connessione commutata su canale B è stabilita mediante il protocollo di controllo del canale D. Conclusa la fase di set-up il collegamento viene gestito attivando funzionalità di livello 2, 3 di X.25 (modalità a circuito virtuale).

9.7 Letture consigliate

Per approfondimenti sulle reti X.25, Frame Relay e ISDN si consigliano i seguenti testi:

- M. Schwartz, "Broadband Integrated Networks", Prentice Hall, 1996.
- F. Halsall, "Reti di Calcolatori e Sistemi Aperti", Addison-Wesley, 1996.
- W. Stalling, "Trasmissione Dati e Reti di Computer", Jackson, 2000.
- B.A. Forouzan, "Reti di Calcolatori ed Internet", McGraw-Hill, 2008.
- A.S. Tanenbaum, D.J. Wetherall, "Reti di Calcolatori", Pearson, 2011.
- U. Black, "ISDN and SS7: Architectures for Digital Signalling Networks", Prentice Hall, 1997.
- G. Kessler, P. Southwick, "ISDN: Concepts, Facilities, and Services", McGraw Hill, 1999.
- W. Stalling, "ISDN and Broadband ISDN, with Frame Relay and ATM", Prentice Hall, 1999.

Si consiglia inoltre di consultare i siti Web:

<http://ieeexplore.ieee.org/Xplore/home.jsp>

<https://www.wikipedia.org>

10

Sistema di segnalazione

SS7

Affinché una rete di telecomunicazioni per comunicazioni foniche basata sulla commutazione di circuito possa attivare i propri servizi è necessario consentire uno scambio di messaggi tra le apparecchiature della rete per attivare specifiche funzionalità sia nei nodi interessati sia al sito utente. Nel suo insieme l'aggregato di questi messaggi viene indicato come *segnalazione* ed il sistema che li utilizza e li genera viene indicato come *sistema di segnalazione*.

Lo scopo di questo capitolo è quello di fornire una descrizione sintetica delle principali caratteristiche e funzionalità di un sistema di segnalazione e di illustrare le principali caratteristiche e prerogative del sistema di segnalazione SS No.7 come esempio concreto di applicazione ed uso delle più recenti tecnologie della segnalazione.

10.1 Sistemi di segnalazione

In generale la segnalazione di rete viene identificata in :

- *segnalazione di utente*: riguarda tutte le procedure necessarie per attivare la connessione di un utente e la rete intesa come sistema per veicolare le informazioni verso la loro destinazione finale;
- *segnalazione inter-nodo*: riguarda l'attivazione e il coordinamento di funzionalità specifiche nei nodi interni alla rete affinché sia realizzato il trasferimento dell'informazione richiesto tra sorgente e destinazione.

La segnalazione di utente è gestita da procedure consolidate che non hanno registrato significativi aggiornamenti funzionali. Aspetti specifici riguardanti la segnalazione di utente non saranno trattati nel seguito e si rimanda per un loro approfondimento alle letture consigliate al termine di questo capitolo.

Le tecniche di segnalazione inter-nodo (tra nodi interni alla rete) sono implementate seguendo due approcci base:

- **segnalazione associata al canale:** le informazioni di segnalazione specifiche per un canale fonico (collegamento) vengono veicolate utilizzando lo stesso supporto fisico impiegato per il flusso informativo con collocazione fissa dipendente dal canale interessato;
- **segnalazione a canale comune:** le informazioni di segnalazione relative ad un aggregato di canali informativi sono veicolate su un canale specifico e distinto (anche come supporto fisico) da quello utilizzato per l'informazione detto *canale comune*.

In particolare per la modalità associata si possono ulteriormente distinguere le due seguenti metodologie:

- **in banda:** la segnalazione è veicolata entro la risorsa di accesso (banda o slot) destinata al trasporto del segnale informativo in relazione al suo formato (analogico o numerico). Nel caso ad esempio di segnale analogico l'informazione di segnalazione è essa stessa in formato analogico e viene allocata nell'ambito della banda di canale al di fuori dell'intervallo utile, tipicamente nella frazione di banda residua a frequenza maggiore (3400-4000Hz). Nel caso invece di telefonia numerica, l'informazione di segnalazione deve sostituirsi a quella relativa al segnale fonico ogni volta che è necessario inviarla;
- **fuori banda:** le informazioni di segnalazione non condividono la stessa risorsa di accesso utilizzata per veicolare il flusso informativo. Nel caso di telefonia numerica, ad esempio, la segnalazione viene realizzata utilizzando i due canali nel blocco di 32 che costituiscono la struttura della trama base. In particolare si utilizza il canale 16 utilizzando 4 bit di segnalazione per ogni canale informativo e quindi distribuendo la segnalazione su più trame consecutive, definendo, in questo modo, una struttura composta detta *multitrama*.

La figura seguente riassume tutte le possibili metodologie di implementazione della segnalazione inter-nodo.

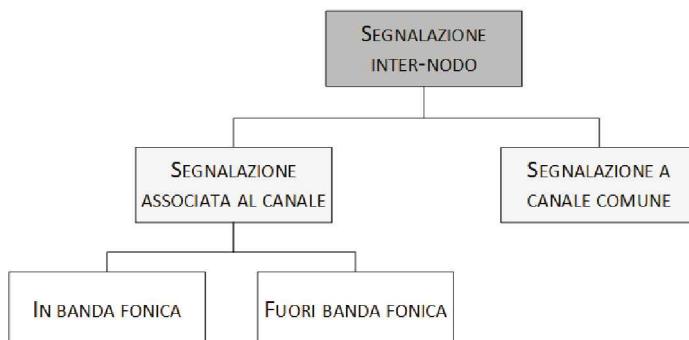


Figura 10.1: Tecniche di segnalazione inter-nodo

La segnalazione a canale comune è una metodologia più recente, prevista, ed in parte già utilizzata, nelle reti a commutazione di circuito di nuova concezione e che progressivamente sta sostituendo alla tecnologia di segnalazione associata al canale largamente utilizzata nelle reti preesistenti.

10.2 Segnalazione inter-nodo a canale comune

La segnalazione inter-nodo a canale comune rappresenta ad oggi la tecnologia di riferimento per l'implementazione dei sistemi di segnalazione. Essa presuppone che venga resa disponibile una specifica infrastruttura di rete da destinarsi esclusivamente allo scambio di informazioni di segnalazioni tra i nodi della rete primaria a commutazione di circuito. Questa rete è indicata come *rete di segnalazione*, utilizza la commutazione di pacchetto e prevede oltre alle linee di connessione fisica due tipologie di dispositivi:

- *Signal Point (SP)*: ha il compito di aggregare le informazioni di segnalazione ed inoltrarle nella rete di segnalazione (origine) e di ricevere e trasferire agli attuatori (destinazione);
- *Signal Transfert Point (STP)*: È un vero e proprio commutatore (router) per la rete di segnalazione che può indirizzare l'informazione di segnalazione o verso un successivo STP o verso il SP di destinazione.

L'informazione di segnalazione inter-nodo riguarda i nodi stessi della rete primaria per cui i SP dovranno essere associati ad essi. Questo vincolo è rilassato nel caso dei STP che possono tuttavia essere localizzati in corrispondenza dei nodi della rete primaria svolgendo in questo modo la funzione duale di STP/SP cioè sorgente/destinazione dell'informazione di segnalazione o semplicemente nodo di transito della stessa.

In generale si identificano tre tipologie di riferimento per la rete di segnalazione :

- *Associata*: questa soluzione prevede l'utilizzo di soli SP. Dovendo questi essere disposti in corrispondenza dei nodi della rete primaria si avrà di conseguenza che le linee di collegamento tra essi, (dette *signal link*), risulteranno parallele con le linee di giunzione della rete primaria. Di fatto si realizza una rete di segnalazione con topologia identica a quella della rete primaria. Questa soluzione riduce i costi degli apparati utilizzati nella rete di segnalazione e, di solito, consente anche di ridurne i costi di messa in opera (es.: si utilizzano le stesse opere infrastrutturali della rete primaria) ma ha lo svantaggio di prevedere collegamenti con (in genere) basso fattore di utilizzo ed è vincolata dalla topologia della rete primaria.
- *Non Associata*: questa soluzione prevede l'impiego sia di STP che di SP e di conseguenza un costo maggiore in termini di apparati necessari per la rete di segnalazione. Nonostante questa penalizzazione la realizzazione con modalità non associata consente di mettere in opera un numero di collegamenti (*signal link*) inferiore veicolando su un unico mezzo fisico la segnalazione

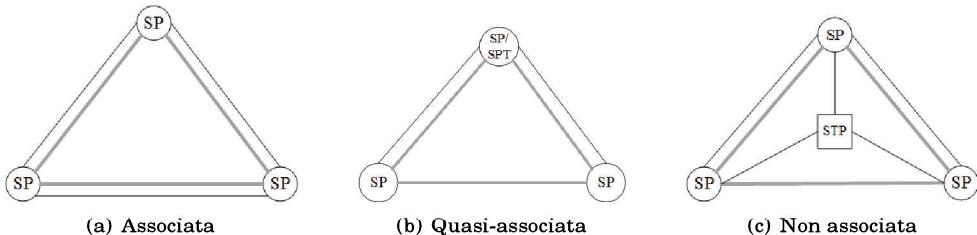


Figura 10.2: Metodologie di segnalazione

relativa a più linee di giunzione. Questa soluzione presenta poi un livello di flessibilità superiore rispetto alla soluzione associata in quanto permette di effettuare il progetto e la realizzazione della rete di segnalazione in maniera completamente indipendente dalla rete primaria.

- *Quasi Associata*: con questa soluzione tecnologica si fanno coesistere le due modalità precedenti. In questo caso è previsto l'impiego, in sostituzione degli STP classici, dispositivi duali con funzionalità integrate STP/SP. Conseguenza di questo è che nel complesso della rete di segnalazione esisteranno sia sezioni di rete primaria controllate e gestite da una segnalazione veicolata in modalità associata sia parti controllate da segnalazione inoltrata con modalità non associata.

Le diverse alternative possibili per la topologia della rete di segnalazione sono illustrate nella figura 10.2.

10.3 Sistema di Segnalazione No. 7 (SS7)

Il sistema di segnalazione SS7 è il sistema di segnalazione più attuale e più diffuso. Questo sistema è completamente basato su tecnologia numerica ed ha capacità di segnalazione significativamente superiori a quella dei preesistenti sistemi di segnalazione. La rete che veicola i messaggi di segnalazione è una rete a commutazione di pacchetto basata su tecnologia a datagramma. L'affidabilità del trasferimento dell'informazione è in genere molto elevata. I nodi previsti dalla rete di segnalazione sono tecnologicamente evoluti, hanno elevate capacità di gestire velocemente grosse quantità di informazione e sono in genere basate su architetture di rete specifiche ed ottimizzate in relazione alle operazioni che devono eseguire.

10.3.1 Architettura Protocollare

Il Sistema di segnalazione SS7 ha mutuato il principio dell'architettura a strati proprio delle reti preposte al trasferimento dell'informazione e standardizzato da ISO (modello ISO/OSI). La configurazione della pila protocollare è illustrata in

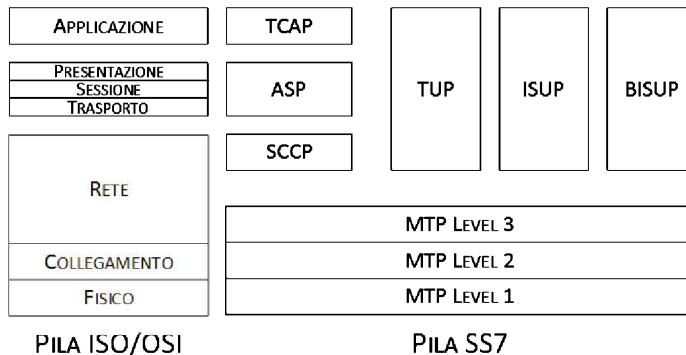


Figura 10.3: Architettura protocollare SS7

figura 10.3. Anche in questo caso esiste una organizzazione gerarchica delle funzionalità dei vari livelli che operano e si interfacciano con le stesse modalità previste nel modello ISO/OSI. Nella stessa figura 10.3 è riportata, per facilitare un confronto funzionale, l'architettura protocollare ISO/OSI. Guardando la figura si può notare che l'architettura protocollare SS7 prevede quattro livelli. I primi tre livelli costituiscono nel loro insieme la parte di trasferimento dei messaggi *Message Transfert Part* (MTP) preposti ad attivare tutte le funzionalità necessarie alla gestione delle comunicazioni nella rete primaria unitamente, quanto richiesto, a servizi aggiuntivi così detti *a valore aggiunto*. Nello specifico la sottoparte MTP prevede i seguenti tre livelli:

- *MTP - Livello 1*: Ha funzionalità proprie del livello fisico di OSI e quindi di interfacciamento diretto con il mezzo fisico. Gestisce trasmissioni ad un rate di 64 Kbit/s ed è responsabile della protezione dei dati nei riguardi di errori di trasmissione, ecc.;
- *MTP - Livello 2*: implementa funzioni tipiche del livello collegamento (Data Link) di OSI occupandosi quindi nello specifico di strutturare l'informazione scambiata in opportune unità informative, della sequenzializzazione e il controllo e recupero di errori di linea;
- *MTP - Livello 3*: svolge funzioni tipiche del livello rete di OSI. In generale vengono distinti funzioni di trattamento dei messaggi, che riguardano l'instradamento in modalità connectionless e funzionalità proprie di procedure di gestione della rete in grado di garantire un'adeguata reattività al verificarsi di condizioni anomale di funzionamento come guasti accidentali o temporanei sovraccarichi.

Il livello 4 dell'architettura protocollare SS7 comprende funzioni essenzialmente riconducibile a funzionalità tipiche dei livelli trasporto, sessione, presentazione ed applicazioni di OSI come mostrato nella figura 10.3. Nel loro complesso formano quella che viene chiamata *User Part* (UP) del sistema SS7.

Nel livello 4 (UP) si possono poi distinguere:

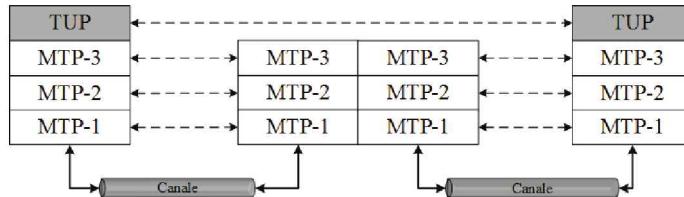


Figura 10.4: Iterazione tra i vari livelli nella rete di segnalazione: nodo sorgente, nodo di transito e nodo destinazione

- *Signalling Connection Control Part (SCCP)*: È preposta al controllo della connessione di segnalazione permettendo il controllo delle connessioni logiche nella rete di segnalazione. In particolare consente di adattare il servizio connectionless di MTP per quelle applicazioni (UP) che richiedono un servizio orientato alla connessione (esercizio e manutenzione, controllo di specifiche transazioni);
- *Transaction Capability Application Part (TCAP)*: si occupa della gestione dell’interazione tra i nodi della rete primaria a commutazione di circuito nell’ambito di specifiche applicazioni e nuovi servizi come numero verde, servizi a costo aggiuntivo, ecc..

Altre componenti lo strato UP che utilizzano i servizi forniti da MTP o direttamente o tramite SCCP sono definite sia per il controllo di specifiche connessioni sia per consentire l’attivazione di funzionalità legate a garantire un corretto esercizio della rete primaria e alla sua supervisione e manutenzione. In particolare abbiamo:

- *Telephony User Part (TUP)*: preposta a gestire lo scambio di segnalazione rivolta al controllo delle chiamate telefoniche. Implementa una modalità di selezione di instradamento step-by-step (o link by link);
- *ISDN User Part (ISUP)*: svolge funzioni di controllo delle connessione in una rete ISDN;
- *B-ISDN User Part (BISUP)*: svolge funzioni di controllo delle connessione in una rete ISDN a larga banda.

La figura 10.4 mostra le modalità di interazione e comunicazione tra due SP tramite un STP intermedio. Si noti che le funzionalità di livello 4 sono attivate solo su base end-to-end in quanto gli STP attivano funzioni fino al livello 3 (MTP) dell’architettura protocollare SS7.

10.4 Letture consigliate

Una descrizione dettagliata del sistema SS7 si può trovare in:

- W. Stalling, Trasmissione Dati e Reti di Computer, Jackson, 2000.
- B.A. Forouzan, Reti di Calcolatori ed Internet, McGraw-Hill, 2007.
- R. Russel, Signaling System 7, McGraw Hill, 1995.
- U. Black, ISDN and SS7: Architectures for Digital Signalling Networks, Prentice Hall, 1997.
- G. Kessler, P. Southwick, ISDN: Concepts, Facilities, and Services, McGraw Hill, 1999.
- W. Stalling, ISDN and Broadband ISDN, with Frame Relay and ATM, Prentice Hall, 1999.

Si consiglia inoltre di consultare il sito Web:

<https://www.wikipedia.org>

Rete SDH

In questo capitolo esamineremo la tecnologia SDH (Synchronous Digital Hierachy) intesa come metodologia per il trasporto dell'informazione in forma digitale in reti estese (WAN) ad alta velocità. Il mezzo trasmittivo di riferimento è la fibra ottica. SDH consente di poter gestire in maniera efficiente flussi informativi con rate anche molto diverso tra loro prevedendo quindi connessioni sia a larga banda sia di tipo tradizionale. Una rete SDH è basata sulla multiplazione a divisione di tempo (TDM) sincrona che richiede la sincronizzazione di tutti gli apparati della rete.

11.1 SDH: Principi Base

Con il diffondersi delle richieste di accesso a larga banda e con l'ampliamento dei servizi offerti a bit rate nominale diverso si sono manifestati i limiti prestazionali della tecnologia PDH evidenziando quindi la necessità di definire un nuovo standard in grado di trarre beneficio dalle nuove tecnologie elettroniche ed ottiche. Questo standard fu denominato SONET (Synchronous Optical NEtwork) negli USA e successivamente fu affiancato da una versione standardizzata da ITU denominata SDH.

La gerarchia PDH esaminata nel capitolo 2.2.2 permette di aggregare diversi flussi di uguale ordine gerarchico (es. base) in flussi di ordine superiore. Nella figura seguente è illustrata la modalità con cui 5 flussi base (detti tributari) vengono aggregati in flusso di ordine superiore (gruppo).

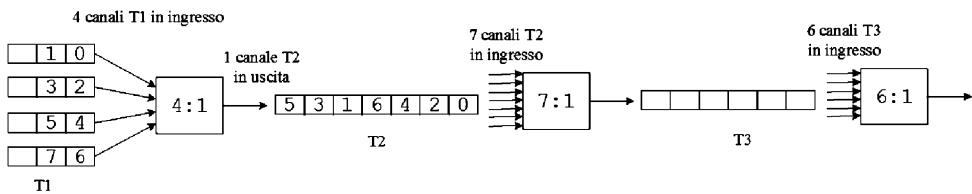


Figura 11.1: Multiplazione PDH

Come si può notare la multiplazione viene eseguita bit per bit e non byte per byte. Questo rende complesso il processo di inserimento o estrazione diret-

ta di un singolo traffico tributario senza dover effettuare la demultiplazione (e, successivamente, la moltiplicazione) completa dell'intero flusso. Per superare i limiti presenti in PDH è stata quindi proposta la tecnologia SDH i cui vantaggi principali sono:

- impiego di una moltiplicazione sincrona che permette di aggregare flussi a rate più basso (es.: 2Mbps) con flussi a velocità più elevate (es.: 2.4 Gbps) senza richiedere una demultiplazione e una moltiplicazione successiva completa. Allo stesso modo si riesce più facilmente ad estrarre direttamente un flusso tributario a bassa velocità dal flusso aggregato a velocità superiore;
- retro-compatibilità con la tecnologia PDH avendo la possibilità di trasportare direttamente trame PDH all'interno di trame SDH;
- topologia di rete ad anello con facilità di interconnessione degli apparati di rete;
- facilità di gestione: SDH prevede l'uso di un supporto applicativo specifico che elimina le carenze prestazionali delle precedenti soluzioni. In particolare è possibile un controllo continuo del tasso di errore e l'integrazione di canali ausiliari specifici nelle trame;
- ambiente di tipo aperto (Multivendor): è possibile far cooperare apparati di rete di costruttori differenti;
- superamento delle problematiche conseguenti la non uniformità della gerarchia PDH a livello mondiale.

Il protocollo SDH è un protocollo di tipo sincrono, controllato da un generatore primario (master) di clock con precisione pari a $1 \text{ su } 10^9$, che prevede modalità specifiche per aggregare (o moltiplicare), ai vari livelli di gerarchia possibili, flussi dati a bit-rate diversi e ritrasmetterli tutti insieme su grandi distanze con tecniche di tipo TDM a interallacciamento di byte (byte interleaving).

L'elemento caratterizzante SDH è una speciale struttura di trama che con l'aggiunta di un numero significativo di informazioni di servizio (overhead) permette non solo l'estrazione diretta di un singolo traffico tributario senza dover effettuare la demultiplazione completa dell'intero flusso, rendendo così la rete molto più flessibile ed efficiente, ma anche il trasferimento di informazioni essenziali per la corretta gestione della rete e per la sua auto-protezione a fronte di guasti o di condizioni di funzionamento anomale. Il risultato finale è che il protocollo SDH consente di raggiungere elevatissimi livelli di qualità di servizio e mette a disposizione strumenti efficaci per il controllo e monitoraggio in tempo reale dell'intera rete di trasmissione.

La trama SDH ha un periodo fondamentale di ripetizione pari a $125 \mu\text{s}$ (lo stesso della trama PDH e richiesto dalla tecnologia PCM) per motivi di compatibilità. Conseguenza del fatto che SDH ha una struttura sincrona le trame vengono emesse anche se non trasportano informazione. La trama base in SDH viene indicata come *Synchronous Transport Module* (STM-1). Come illustrato nella figura 11.2 viene tipicamente rappresentata sotto forma di matrice di byte

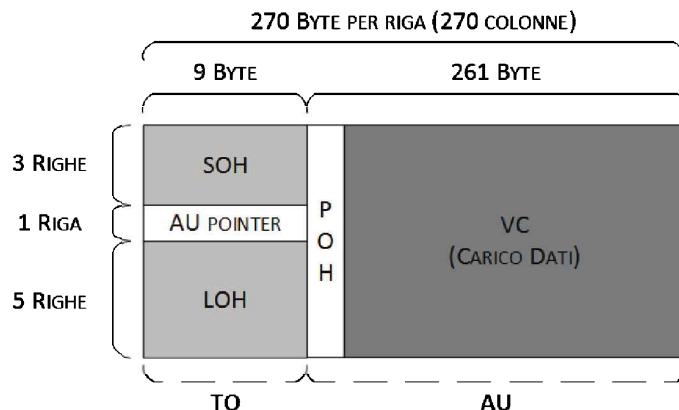


Figura 11.2: Frame STM-1

disposti su 9 righe e 270 colonne per un totale di 2430 byte, trasmessi ad una velocità aggregata di 155.52 Mbps. Questi parametri furono scelti per garantire la compatibilità di SDH con lo standard simile SONET adottato negli USA. In particolare la trama STM-1 corrisponde alla trama di livello 3 di SONET definita come *Synchronous Transport Signal STS-3*.

Ogni elemento della struttura a matrice corrisponde ad un byte e individua un canale a 64 Kbit/s, equivalente a un singolo canale di telefonia numerica: da questo discende il vincolo di trasmissione di ogni trama elementare di tipo STM-1 in $125 \mu s$. Il protocollo prevede poi aggregazioni di più moduli STM-1 in gerarchie via via superiori definite STM-N, dove "N" indica il numero di moduli STM-1 aggregati insieme.

La trama SDH è suddivisa in due parti fondamentali:

- Parte dedicata alle informazioni di servizio globali denominata *Transport Overhead* (TO) comprendente gli elementi appartenenti alle prime 9 righe e 9 colonne della trama ($9 \times 9 = 81$ byte) destinata al trasporto delle informazioni di gestione della rete. Questa parte è ulteriormente suddivisa in :
 - *Section Overhead* (SOH): comprende le informazioni trasportate negli elementi della trama corrispondenti alle prime 3 righe e 9 colonne. Questa parte della trama contiene informazioni di servizio relative alla trama nel suo complesso ed essenziali per il riconoscimento della trama stessa e per l'accesso ai singoli flussi tributari, nonché un insieme di informazioni di controllo per la gestione, il monitoraggio e la protezione dell'intero modulo;
 - *AU Pointer*: campo formato dai primi nove elementi della quarta riga e riservate per specificare la posizione dei dati nel frame e per l'allineamento;

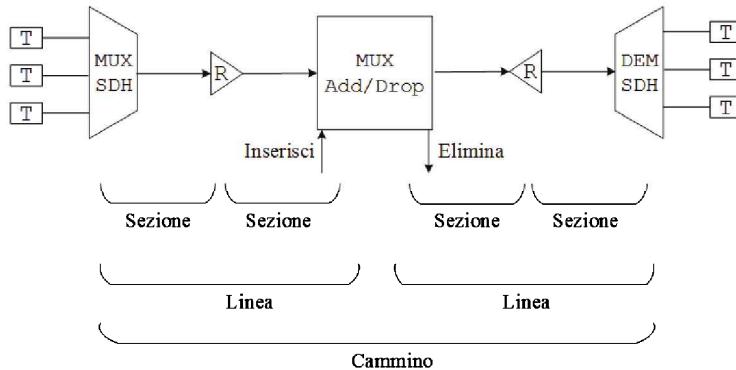


Figura 11.3: Rete SDH

- *Line Overhead (LOH)* : comprende le informazioni trasportate negli elementi della trama corrispondenti ai primi nove elementi delle ultime cinque righe della trama. È dedicata a funzioni di recupero di errori e gestione di operazioni di multiplexing (add) o demultiplexing (drop).
- Parte destinata al trasporto dei dati e della segnalazione di cammino denominata *Administrative Unit (AU)* a sua volta suddivisa in :
 - *Virtual Container*: È devoluto al trasporto dei singoli flussi tributari organizzati come sequenze di strutture omogenee. Questa denominazione è conseguente al fatto che SDH è retro-compatibile con tutte le modalità di multiplazione preesistenti.
 - *Path Overhead(POH)*: informazioni di servizio aggiuntive, su base end-to-end, necessarie per operazioni di gestione, monitoraggio e protezione, oltre che dal flusso informativo vero e proprio costituito dal tributario adattato alla trama SDH.

La trasmissione della trama SDH avviene sequenzialmente per righe.

11.2 Dispositivi di Rete

Lo schema generale relativo ad una connessione SDH tra due terminali di rete (T) è mostrato nella figura 11.3. Gli elementi caratterizzanti questa struttura, oltre ai terminali di rete, sono il Multiplexer/Demultiplexer STM che delimita il collegamento fisico tramite la rete SDH tra due terminali di rete detto *path* (cammino), gli Add/Drop Multiplexer che suddividono il path in sottoparti ciascuna denominata *linea* ed infine i repeater che suddividono una linea in una o più sottoparti denominate *sezioni*.

Multiplexer/Demultiplexer STM

Questi dispositivi rappresentano il punto di accesso della rete SDH da parte dei terminali di utente. Questi elementi ricevono/trasmettono il segnale cliente (PDH, Ethernet, ecc.) e lo inseriscono (multiplexing) in una struttura di trama SDH, tipicamente di bassa gerarchia (es.: STM-1), per poi interfacciarsi con il resto della rete tipicamente tramite un collegamento lineare. Lato destinazione finale l'operazione effettuata (demultiplexing) è inversa alla precedente cioè si provvede ad estrarre i vari flussi tributari dalla trama SDH ricevuta e a distribuirli verso gli utilizzatori finali. Definiscono una trama SDH completa anche parti devolute alla segnalazione (TO, POH).

Ripetitore

Questi sono dispositivi intermedi in grado di gestire la sola informazione del campo SOH. La funzione di questi dispositivi è quella di rigenerare il segnale al fine di poter coprire lunghe distanze. Nel caso si trasmetta su fibra ottica eseguono una trasduzione di formato del segnale da ottico ad elettrico e viceversa: demodulano il segnale ricevuto in formato ottico, lo rigenerano in formato elettrico ed infine lo trasformano di nuovo in formato ottico per la ritrasmissione. In questo modo è possibile eliminare o correggere gli effetti negativi legati alla tratta percorsa (es. attenuazione, distorsione, sfasamenti, rumore indotto ecc.).

Add/Drop Multiplexer

Questi dispositivi hanno il compito di inserire ed estrarre i flussi tributari a bit rate inferiore rispetto al bit rate della trama SDH ricevuta. Sono in genere apparati di transito ma possono essere utilizzati anche come apparati di accesso alla rete SDH. Tipicamente vengono utilizzati in configurazione ad anello (in alcuni casi anche a stella) con il compito primario di creare in modo gerarchico i vari livelli di aggregazione e distribuzione del traffico (es.: anelli metropolitani caratterizzati da bassa-media capacità interconnessi ad infrastrutture SDH di capacità superiore). Questi dispositivi utilizzano ed aggiornano (quando necessario) le informazioni contenute nelle sottoparti AU Pointer e LOH della sezione TO.

Terminali

In termini generali un terminale è il dispositivo interconnesso alla rete SDH proprietario delle informazioni da trasmettere (sorgente) o utilizzatore designato delle stesse (destinazione). Come esempio si può pensare a due dispositivi di gestione di due reti distinte (es.: LAN) che si scambiano le informazioni attraverso una supporto SDH.

11.3 Architettura a Strati

L'architettura a strati di una rete SDH è mostrata in figura 11.4 dove viene anche fornito un suo confronto con il modello ISO/OSI.

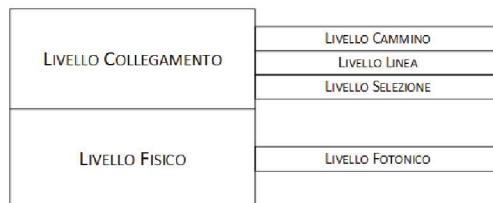


Figura 11.4: Architettura protocollare SDH

In particolare si può notare che essa prevede quattro livelli per i quali la corrispondenza funzionale con il modello ISO/OSI evidenzia una perfetta congruenza tra il primo livello di SDH (Fotonico) ed il livello Fisico di ISO/OSI mentre nel loro complesso i rimanenti tre livelli (Sezione, Linea, Cammino) possono essere assimilati al livello Collegamento di ISO/OSI. Nello specifico abbiamo:

Livello Fotonico

Si occupa della trasmissione delle trame nel canale ottico di collegamento e di conseguenza riguarderà tutte le metodologie specifiche adatte ad implementare queste funzionalità. È un livello attivo in tutti gli apparati della rete SDH.

Livello Sezione

Competenza di questo livello è garantire l'integrità e la gestione (framing) del trasporto del segnale in una sezione. Le funzionalità di questo livello sono attive in tutti gli apparati della rete SDH.

Livello Linea

Ha responsabilità della gestione del trasferimento delle trame SDH su base linea. Dovrà, oltre alle funzioni tipiche di controllo dell'integrità dell'informazione, implementare anche operazioni di inserimento o estrazione di flussi tributari nella struttura di trama gestita. Una linea fisica delimita il tratto di rete che interconnette due multiplexer consecutivi e, quindi, le funzionalità di questo livello sono attivate solo nei Multiplexer STM (sorgente, destinazione) o negli Add/Drop Multiplexer di transito.

Livello Cammino

Le funzionalità di questo livello consistono nel garantire il corretto trasferimento di un flusso informativo da un terminale di rete sorgente al terminale destinazione. Dovrà quindi anche sovraintendere ad operazioni di aggregazione ed estra-

zione dei flussi tributari. Le funzionalità di questo livello sono implementate su base end-to-end cioè solo al Multiplexer STM sorgente ed al multiplexer STM destinazione.

È importante notare che in SDH non è riconoscibile nella definizione della struttura di trama la procedura tipica dell'*incapsulamento* successivo di ISO/OSI avendo tutte le informazioni di overhead relative ai singoli livelli una collocazione specifica nella struttura della trama SDH.

La figura 11.5 mostra la relazione tra gerarchia logica e fisica in una rete SDH. In particolare si può riconoscere in questa figura, coerentemente con quanto esposto in precedenza, che gli unici dispositivi che operano a tutti e quattro i livelli dell'architettura di rete sono il Multiplexer SDH sorgente e destinazione. Anche in questo caso i collegamenti tra i livelli di dispositivi connessi è solo logica. Un collegamento effettivo viene realizzato solo attraverso il canale ottico di comunicazione tra gli apparati.

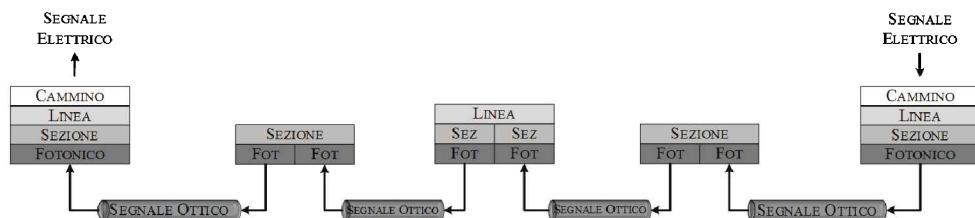


Figura 11.5: Interazione tra livelli SDH

11.4 *Letture consigliate*

La tecnologia relativa a reti SDH è un argomento non semplice da affrontare per chi per la prima volta si avvicina alle problematiche delle reti di telecomunicazioni. Per approfondimenti relativi agli argomenti trattati in questo capitolo si suggerisce di consultare i libri di testo:

Andrew S. Tanenbaum, David J. Wetherall, "Reti di Calcolatori", Pearson, 2011.

B.A. Forouzan, "Reti Di Calcolatori e Internet", McGraw-Hill, 2007.

Inoltre un'utile lettura può risultare essere l'articolo:

C.G. Omidyar, A. Aldridge, "Introduction to SDH/SONET", IEEE Communications Magazine, settembre 1993.

12

Rete ATM

In questo capitolo verranno presentati i principi base della tecnologia ATM (Asynchronous Transfret Mode) la cui funzionalità primaria è quella di essere in grado di gestire il trasporto ad alto data rate di diverse tipologie di traffico (voce, dati, multimediale). Un'altra importante caratteristica tecnologica di ATM è quella di prevedere l'uso della commutazione veloce di pacchetto descritta nel capitolo 3.

Il capitolo inizialmente propone una descrizione generale della tecnologia ATM ed il suo inquadramento temporale nel percorso evolutivo delle reti di telecomunicazioni. Successivamente viene descritto il funzionamento delle reti ATM partendo da una sintetica introduzione della sua struttura protocollare e delle modalità previste per la gestione dei diversi servizi a cui la rete si rivolge.

12.1 Generalità

Agli inizi degli anni '80 esistevano solo due tipologie di reti: le reti telefoniche per comunicazioni voce e le reti dati sempre di più chiamate a gestire traffici consistenti. Fu quindi percepita come opportuna e necessaria l'esigenza di definire un'unica modalità di trasporto dell'informazione che potesse adattarsi indistintamente al trasferimento di traffici differenti (grossi file, e-mail, voce, stream video e audio real-time) e di essere in grado di rispettare requisiti di servizio (QoS) diversi. Fu così che due comitati (ATM forum e ITU) standardizzarono l'Asynchronous Transfert Mode (ATM). ATM nasce con una genesi in controtendenza rispetto a quella tipica per tutte le altre tecnologie: prima viene standardizzata e poi vengono realizzati i servizi. ATM fu sviluppata con grossi investimenti delle maggiori società del settore delle telecomunicazioni che decisero di puntare decisamente sulla realizzazione della rete ATM. Questi grossi finanziamenti però non hanno evitato un sostanziale insuccesso della tecnologia ATM intesa come soluzione funzionale per l'interconnessione nelle reti di calcolatori. La tecnologia Internet (veloce e gigabit) rappresentò presto un'alternativa efficace, commercialmente più attraente e più famigliare agli utilizzatori.

ATM prevede l'uso della fibra ottica come mezzo fisico fino all'utente finale. Questo permette un data rate di accesso alla rete elevato ed un'ottima affidabilità dei collegamenti nei confronti degli errori di trasmissione, soprattutto su base link to link. Anche se non ha avuto il successo sperato, ATM è oggi ancora

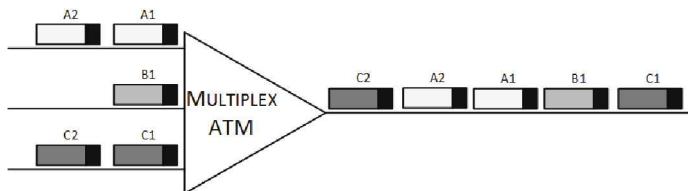


Figura 12.1: Multiplazione ATM

utilizzata per linee di accesso a larga banda in tecnologia DSL e come protocollo di trasporto in dorsali per il collegamento ad alta velocità di reti TCP/IP.

Va specificato che ATM non trova un riscontro preciso nella pila ISO/OSI. Forzandone il confronto, si può pensare di collocarlo a cavallo tra il livello fisico e il livello collegamento.

ATM funziona con la tecnica a commutazione di pacchetto a circuito virtuale ma, a differenza delle reti classiche come ad esempio le reti TCP/IP, non incapsula i dati in pacchetti di lunghezza variabile ma prevede un'unità fondamentale, di lunghezza fissa, chiamata **cella** comprendente 53 byte, di cui 5 byte riservati per la testata (header) e 48 byte di carico utile (payload). Avere messaggi di lunghezza fissa facilita ai dispositivi di rete l'interpretazione degli stessi e quindi aumenta la velocità di commutazione. Il circuito virtuale, nel gergo ATM, viene definito **canale virtuale**. La caratteristica funzionale caratterizzante ATM è la multiplazione asincrona veloce resa possibile dalla suddivisione dei flussi informativi in celle di dimensioni fisse offre. Da notare che, per non perdere la sincronizzazione, un canale di comunicazione in ATM non risulta mai inattivo: se un nodo della rete non ha celle da inviare, provvede a generare celle fittizie, con payload senza significato (vuote) al solo scopo di mantenere la sincronizzazione di rete. Il multiplex ATM è mostrato in figura 12.1. Va specificato che la tecnica di accesso al mezzo fisico è di tipo TDMA sincrono, cioè la trasmissione dell'informazione avviene in precisi istanti temporali. Questa visione asincrona nel trasferire le celle, ma sincrona nell'accedere al mezzo fisico è facilitato dall'uso delle celle: ogni pacchetto ha una durata temporale nota a priori, quindi l'accesso avviene in istanti temporali ben precisi; ovviamente gli slot temporali devono essere tali da essere compatibili con la durata (tempo di trasmissione) di una singola cella. Inoltre, come conseguenza del principio di intermittenza del traffico dati, non è prevista un'assegnazione rigida delle risorse, ogni stazione non avrà allocato un numero fisso di slot ma l'allocazione della risorsa può variare nel tempo in relazione alle richieste di servizio attive.

Come accennato in precedenza, ATM deve essere in grado di gestire diversi servizi e quindi diverse qualità del servizio. In particolare ATM identifica il traffico secondo le seguenti classi (Schwartz'1996, Halsall'1996, Acampora'1994, Forouzan'2007 in 12.4):

- **Constant Bit Rate (CBR):** la rete ATM garantisce al collegamento per tutta la sua durata della capacità dichiarata un data rate costante ed il rispetto di

vincoli, spesso stringenti, riguardo il massimo ritardo tollerato, il massimo tasso di perdita delle celle, ecc.;

- *Variable Bit Rate (VBR) - Real Time*: riguarda un traffico di tipo interattivo (video compresso) che richiede il rispetto di precisi vincoli sul ritardo di trasporto;
- *Variable Bit Rate (VBR) - Non Real Time*: riguarda un traffico di tipo interattivo. Vengono specificati gli stessi requisiti di servizio della classe precedente con la sola eccezione che in questo caso la rete non dà garanzia riguardo il ritardo di trasferimento. È rivolto ad un supporto di reti Frame Relay o applicazioni dipo *mission critical* come transazioni bancarie e sistemi di prenotazione;
- *Available Bit Rate (ABR)*: ha forti analogie con la classe precedente in quanto non richiede né un trasferimento in tempo reale né un data rate costante. Prevede l'uso di celle opportune per effettuare un controllo del flusso (utilizzazione) nei collegamenti ABR ed adattare dinamicamente il data rate per ogni collegamento alle condizioni di disponibilità attuali (si inizia con il minimo valore garantito e poi si cerca di incrementarlo fino a quando la rete lo consente);
- *Unspecified Bit Rate (UBR)*: è simile alla classe precedente con la differenza che in questo caso non sono offerte garanzie, nemmeno minime, di trasferimento delle celle. È spesso indicato come servizio *Best Effort* ed è rivolto ad applicazioni non *mission critical* come ad esempio pagamenti on-line tramite carta di credito (se non va a buon fine l'utente ritenterà).

Una caratteristica di ATM è quella di non prevedere il controllo dell'integrità dell'informazione trasmessa su base link to link. Questa decisione deriva dalla constatazione che il mezzo fisico di collegamento, in pratica, è immune da errori di trasmissione e dalla necessità, imprescindibile, di assicurare un inoltro veloce dei flussi informativi nella rete. Un controllo sull'integrità dell'informazione ricevuta su base link to link appesantirebbe l'elaborazione nei nodi di transito (per lo più inutilmente in questo caso) vanificando l'opportunità di un trasferimento dati veloce grazie all'uso della tecnologia trasmissiva di tipo ottico. Per comprendere questa situazione con una analogia si può fare riferimento ad un collegamento autostradale potenzialmente veloce, per il quale sono stati però previsti stazioni di pagamento del pedaggio troppo frequenti. La soluzione utilizzata, in questo caso, per non penalizzare una viabilità veloce, è quella di spostare le stazioni di pagamento dei pedaggi all'uscite. Questo è anche l'approccio applicato nelle reti ATM per le quali le funzionalità dei nodi di transito sono ridotte all'essenziale e gli eventuali controlli dell'integrità dell'informazione ricevuta sono demandati alla destinazione finale (end-to-end).

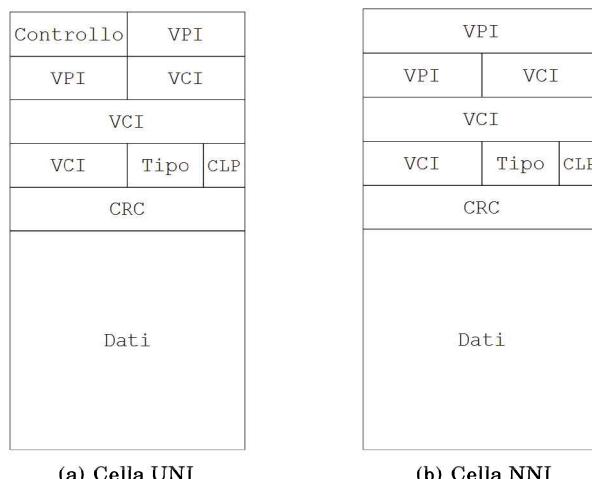
12.1.1 Cella ATM

ATM prevede, come evidenziato nel precedente paragrafo, lo scambio di informazioni strutturate in unità elementari chiamate celle. Una cella ha una dimensione fissa di 53 Byte di cui 5 sono riservati all'header e 48 per i dati. Se il flusso dati di utente è più grande di 48 byte, viene attivata la suddivisione del flusso stesso (frammentazione) in più celle. L'invio dei frammenti (celle) è sequenziale e, una volta arrivati a destinazione, i singoli frammenti vengono aggregati in maniera ordinata (ri-assemblati) in modo da ripristinare il formato originale dell'informazione.

Esistono due diversi formati per le celle: uno riferito ai messaggi scambiati tra i terminali di utente e i nodi della rete (interfaccia UNI, User Network Interface) e l'altro utilizzato per lo scambio di messaggi tra due nodi interni alla rete ATM (interfaccia NNI, Newtork Network Interface). Il formato relativo alle due differenti tipologie di celle è illustrato in figura 12.2.

I vari campi hanno i seguenti significati:

- **controllo:** campo da 4 bit, utilizzato per il controllo del flusso. Questo campo è presente solo nella cella UNI, mentre nella cella NNI questi quattro bit sono usati per incrementare il numero dei bit per l'identificativo del canale virtuale (VCI, vedi di seguito). Di conseguenza questo campo può essere utilizzato solo per il controllo del flusso sull'interfaccia utente-rete. E' utile (Stalling'1998 in 2.3) nel caso di coesistenza di servizi attivi con differenti requisiti (es.: rate di accesso garantito);
- **VPI (Virtual Path Identifier):** è un campo da 8 bit nel caso della cella UNI mentre è lungo 16 bit nel caso della cella NNI. Identifica il percorso virtuale di uno specifico flusso;



(a) Cella UNI

(b) Cella NNI

Figura 12.2: Formato celle in ATM

- **VCI** (Virtual Circuit Identifier): è un campo da 16 bit, sia nella cella UNI che nella cella NNI. Identifica il canale virtuale associato;
- **Tipo**: è un campo di 3 bit in entrambe le celle e identifica la tipologia di dati trasportati dalla cella;
- **CLP** (Cell Loss Priority): campo di un solo bit e indica la priorità di eliminazione delle celle nel caso in cui la rete sia congestionata. Se una cella ha questo campo posto a 1 verrà eliminata prima di una cella con il campo CLP posto a 0.
- **CRC** (Cyclic Redundant Check): campo da 8 bit ed è il codice che serve per rilevare, ed eventualmente correggere, errori introdotti nell'informazione di testata (header) della cella dal canale di comunicazione.

12.2 Architettura protocollare ATM

Lo standard ATM prevede una struttura protocollare con tre piani distinti. L'architettura di riferimento è illustrata in figura 12.3.

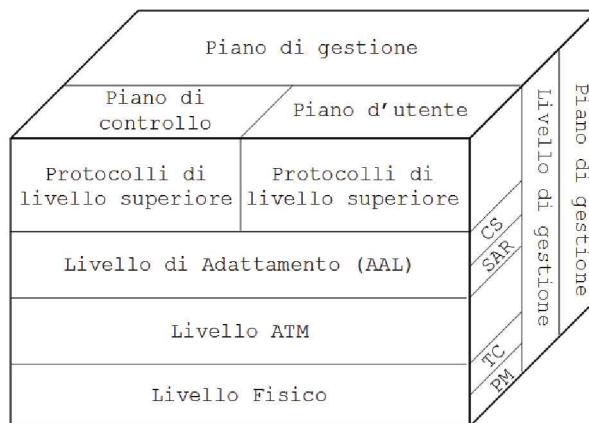


Figura 12.3: Architettura protocollare ATM

Il **piano d'utente** (o User Plane) è il responsabile dei servizi richiesti dall'utente, il **piano di controllo** (o Control Plane) è il responsabile del controllo e della segnalazione nella rete ATM mentre il **piano di gestione** (o Management Plane) ha lo scopo di sovrintendere ad una corretta cooperazione tra i piani utente e controllo. Il piano d'utente e il piano di controllo sono a loro volta strutturati a livelli.

I livelli sono:

- **livello fisico**: è un livello in comune ad entrambi i piani (utente e controllo) ed è il responsabile del trasferimento delle informazioni dalla sorgente alla destinazione. Grazie agli alti data rate consentiti e alla facilità con cui

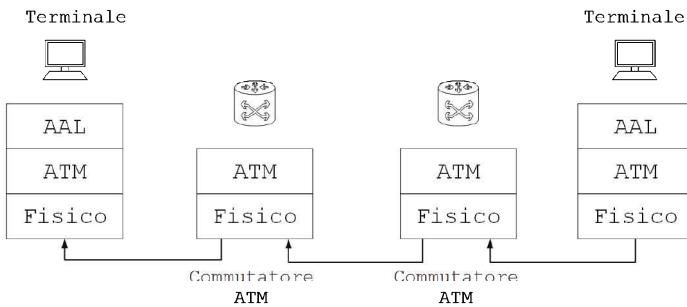


Figura 12.4: Metodologia Core & Edge

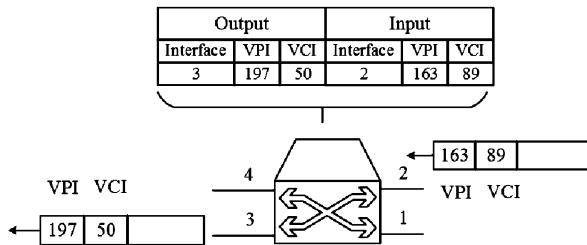


Figura 12.5: Commutazione in reti ATM

vengono delimitate le celle, il livello fisico originale per le reti ATM era SONET/SDH. Il livello fisico ATM a sua volta è diviso in due sottolivelli:

- *Physical Medium (PM)*: è l'interfaccia con il mezzo fisico vero e proprio e dipende dal mezzo fisico adoperato. Il suo compito principale è eseguire la codifica di linea ed inviare e recuperare le informazioni di sincronizzazione;
- *Transmission Convergence (TC)*: è responsabile, lato mittente, di trasformare un flusso di celle in un flusso di bit da trasmettere nel mezzo di collegamento e, lato destinatario, di ripristinare dal flusso dati ricevuto il flusso originale di celle. Inoltre è responsabile della verifica dell'integrità dell'header della cella tramite il campo CRC.
- **livello ATM**: anche questo livello è in comune tra il piano utente e il piano di controllo. Il livello ATM è indipendente dal livello fisico adoperato dalla rete ATM. Questo livello è il responsabile della consegna delle celle tra mittente e destinatario. ATM si basa sul principio *Core & Edge*, un principio dove le funzionalità superiori al livello ATM risiedono solo nel terminale sorgente e destinazione della comunicazione, come mostrato in figura 12.4. Nei commutatori di transito della rete, il livello ATM è il livello più alto e il suo compito è quello di instradare le celle nella rete lungo il percorso verso la loro destinazione. L'instradamento in ATM avviene leggendo i valori dei campi VPI e VCI contenuti nell'header della cella. Non appena una

cella arriva a un commutatore (nodo di transito), vengono letti i valori dei due campi VPI/VCI e quindi si effettua una ricerca nella sua routing table per individuare la nuova coppia di valori VCI/VPI di uscita (con relativa interfaccia) ad essi associata. Il commutatore effettua quindi la traslazione di etichetta, impostando i campi VPI/VCI con i loro nuovi valori (questa modalità è simile a quella incontrata in X.25 e Frame Relay). La fase di commutazione è mostrata in figura 12.5. Per quanto detto in precedenza, ATM non offre un servizio affidabile su base link to link in quanto non è in grado di rilevare perdita di cella dovute ad errori nella loro sezione di header oppure per congestione. Per controllare gli effetti negativi di eventuali perdite sulla qualità dei servizi offerte si introduce un controllo (Cell Loss Ratio) su base end to end e si verifica che non superi il valore di soglia prestabilito per ogni specifico servizio.

- **livello di adattamento (AAL):** Il livello AAL, ATM Adaptation Layer, è l'ultimo livello a comune tra piano d'utente e piano di gestione. Il suo scopo principale è quello di rendere compatibile il flusso informativo con il formato delle celle ATM. Le funzionalità del livello AAL non sono implementate nei nodi di transito ma solo nel nodo mittente e di destinazione, come illustrato in figura 12.4. Il livello AAL ha il compito di rendere compatibili i servizi richiesti dagli strati superiori (come ad esempio un collegamento di dorsale tra due o più LAN) e quelli disponibili tramite il livello ATM. In pratica lo strato AAL, in trasmissione, converte l'informazione ricevuta in segmenti di 48 byte che costituiranno il payload delle celle definite dal livello sottostante ATM. In ricezione viene effettuata l'operazione opposta: lo strato AAL riceve la parte di payload dal livello ATM e provvede a convertirlo nel formato utilizzabile dai livelli superiori. La suddivisione e la conseguente ricostruzione avviene con modalità differenti in base al servizio del livello superiore. In fase di definizione dei protocolli del livello AAL, l'ITU propose una suddivisione di tali protocolli in base alle classi di servizio definite per ATM, cercando di fare in modo che ogni classe di servizio definita avesse il suo specifico protocollo AAL. I tre parametri fondamentali utilizzati per la definizione dei protocolli sono stati: controllo sul jitter (Forouzan'2007 in 2.3), l'emissione del bit rate da parte di una sorgente e la modalità di trasferimento dei dati richiesto. Conseguentemente, sono stati definiti i quattro protocolli seguenti:

- **AAL 1:** questo protocollo viene usato quando il mittente invia dati con un bit rate costante; risulta la scelta migliore quando si adopera servizi isocroni come voce o video. Si riferisce a servizi orientati alla connessione;
- **AAL 2:** inizialmente questo protocollo era stato progettato per servizi isocroni con bit rate variabile orientati alla connessione, adesso viene adoperato per trasferire traffico aggregato a basso bit rate come ad esempio il traffico di reti cellulari;
- **AAL 3/4:** originariamente erano due protocolli distinti e supportavano, servizi connection oriented, il primo e servizi connectionless, il se-

	protocolli AAL			
	AAL 1	AAL 2	AAL 3/4	AAL 5
controllo jitter	richiesto	richiesto	non richiesto	non richiesto
Bit rate	CBR	VBR	VBR	VBR
modalità trasferimento	Connection oriented		non specificato	

Tabella 12.1: Protocolli AAL e relative classi di servizio

condo. Lo studio individuale dei due protocolli fecero emergere ben presto una profonda analogia tra i problemi riscontrati. Di conseguenza, fu deciso di unificarli in un unico protocollo. Allo stato attuale, questo protocollo viene adoperato per servizi non isocroni (non in tempo reale), sia orientati alla connessione che non (connectionless);

- **AAL 5:** questo protocollo offre il minimo indispensabile supporto al trasferimento delle celle. Non effettua nessun controllo dell'errore e nessuna verifica sull'effettivo ordine di arrivo delle celle. Si assume che le celle appartenenti ad una stessa sessione siano inviate in sequenza e che il controllo degli errori venga eseguito al livello superiore. AAL 5 è utilizzato per servizi best-effort.

La tabella 12.1 mostra le relazioni tra i parametri e i protocolli definiti. Il livello AAL è diviso in due sottolivelli:

- *Segmenting And Reassembling* (SAR): Il sottolivello SAR è il responsabile della segmentazione e del riassemblaggio;
- *Convergence Sublayer* (CS): il sottolivello CS invece controlla che in fase di segmentazione o ricostruzione non vi siano errori. Questo sottolivello è a sua volta diviso in due livelli distinti: il *Common Part Convergence Sublayer* (CPCS) e il *Service Specific Convergence Sublayer* (SSCS).

12.3 Architettura ATM

ATM prevede l'uso di due sole interfacce: la *User Network Interface* (UNI) che definisce le procedure con cui terminale finale ATM e nodo di accesso alla rete "parlano" tra di loro e la *Network Network Interface* (NNI), utilizzata per far comunicare tra di loro i commutatori della rete ATM.

ATM prevede, come già anticipato, il trasporto delle informazioni in modalità connection-oriented, dunque tra due utenti (mittente-destinazione) viene creato un collegamento virtuale seguito da tutte le celle che costituiscono il flusso informativo da trasferire. La connessione fisica è identificata con il canale di trasmissione (*Transmission Path*, TP), a sua volta la capacità di trasporto (banda) di un canale di trasmissione è suddivisa in più cammini virtuali (*Virtual Path*, VP). La banda allocata ai cammini virtuali viene ulteriormente suddivisa dinamicamente

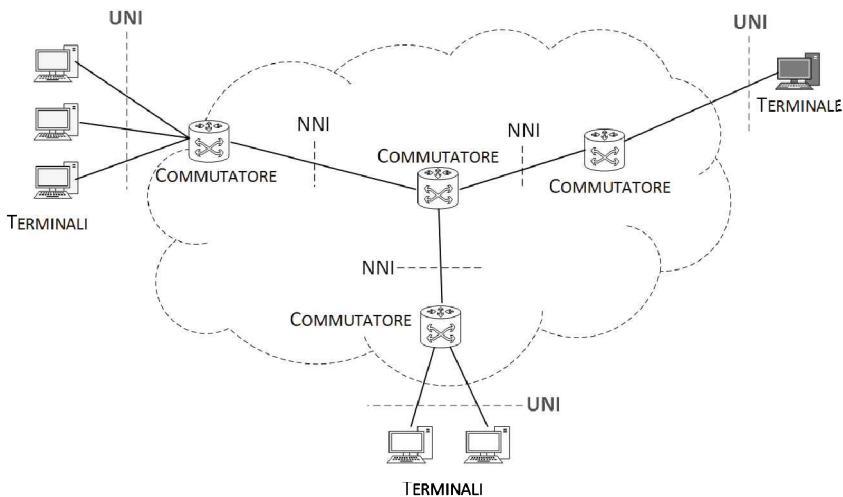


Figura 12.6: Architettura di una rete ATM

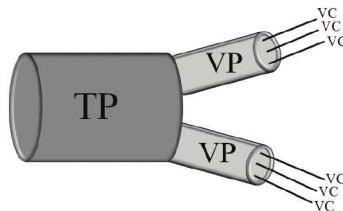


Figura 12.7: Tipologia delle connessioni in reti ATM

in relazione a specifiche necessità di accesso, in collegamenti virtuali individuati detti circuiti virtuali (*Virtual Channels*, VC). Come evidenziato in precedenza, ATM è rivolto a comunicazioni basate sulla commutazione di pacchetto ed orientate alla connessione (circuito virtuale). La conseguenza di questo è che è quindi necessario definire un collegamento virtuale tra sorgente e destinazione fisso che verrà seguito da tutte le celle appartenenti al flusso informativo da trasferire. Le varie connessioni virtuali tra coppie sorgente/destinazione dovranno poi essere identificate in maniera univoca e non ambigua. A questo riguardo in ATM l'identificazione delle connessioni virtuali viene ottenuta seguendo uno schema gerarchico a due livelli : identificatore di cammino virtuale (VPI) (principale) e identificatore di circuito virtuale (VCI) (secondario). In figura 12.7 viene mostrata la relazione tra i due indicatori.

I valori dei campi VPI/VCI sono locali e possono essere ridefiniti dai commutatori (nodi) di una rete ATM in relazione alle specifiche esigenze di switching. Questa operazione è indicata come *label swapping*. Frequentemente però i percorsi virtuali su base end to end sono predefiniti. In questo modo l'operazione di commutazione risulta più veloce in quanto viene limitata alla sola lettura e modifi-

fica del campo VPI (tutti i VC associati vengono trasferiti in blocco senza modifica del valore del campo VCI). La suddivisione del VP nelle sue componenti elementari VC individuali è demandata al nodo finale che si interfaccia direttamente con i terminali destinazione di servizi specifici.

12.4 Letture consigliate

Approfondimenti relativi alla tecnologia ATM sono disponibili nei seguenti testi:

- M. Schwartz, *Broadband Integrated Networks*, Prentice Hall, 1996.
- F. Halsall, *Reti di Calcolatori e Sistemi Aperti*, Addison-Wesley, 1996.
- D. Wright, *Bussiness Services, Technologies, and Strategic Impact*, Artech House, 1993.
- A. Acampora, *An Introduction to Broadband Networks*, Plemum Press, 1994.
- W. Stalling, *High Speed Networks*, Prentice Hall, 1998.
- B.A. Forouzan, *Reti di Calcolatori ed Internet*, McGraw-Hill, 2008.
- A.S. Tanenbaum, D.J. Wetherall, *Reti di Calcolatori*, Pearson, 2011.

13

Algoritmi di routing

Il compito di instradare un pacchetto dalla sorgente alla destinazione spetta ai protocolli di routing. Essi trovano collocazione nel livello di rete della pila ISO/OSI e IP per reti TCP/IP. Più propriamente un algoritmo di routing (alcune volte indicato anche come *algoritmo di instradamento*) è una funzionalità (software) propria del livello rete che decide, sulla base di un criterio specifico, verso quale interfaccia di uscita andranno inoltrati i pacchetti in ingresso relativi ad uno determinato collegamento. Per raggiungere questo obiettivo può essere necessario avere una conoscenza di tutta la rete per individuare i percorsi end-to-end migliori. Questa conoscenza può essere pre-acquisita ed aggiornata periodicamente oppure ottenuta in modalità reattiva sulla base di specifiche necessità.

Nel corso del capitolo saranno illustrati i principi alla base degli algoritmi di instradamento e verranno infine descritti i principali algoritmi utilizzati nelle attuali reti di calcolatori (dati).

13.1 Generalità

Il dispositivo che attua gli algoritmi di instradamento è di solito indicato come router, più in generale, esso può essere un qualsiasi dispositivo che possa attuare tutte le funzionalità proprie del livello rete di ISO/OSI (o livello IP della rete Internet (TCP/IP)). L'instradamento può essere attuato mediante l'ausilio di informazioni già disponibili al router, tipicamente in forma di tabelle (dette *tabelle di routing*), definite ed aggiornate periodicamente secondo specifiche metodologie oppure acquisite in modalità reattiva sulla base di determinate richieste di collegamento. Le funzionalità di instradamento e le informazioni necessarie per attuarle non sono disponibili né al dispositivo sorgente né a quello di destinazione ma solo nei router (nodi) che concorrono a definire il collegamento (Forouzan'2007, Kurose'2011, Tanembaum'2013 in 13.9).

I criteri per valutare e confrontare tra di loro algoritmi di routing differenti sono:

- **Semplicità:** un algoritmo, oltre ad essere affidabile, deve essere anche facilmente implementabile e non richiedere risorse computazionali eccessive per contenerne i tempi di esecuzione;

- **Robustezza:** l'algoritmo di routing deve funzionare per qualsiasi topologia di rete e condizioni di traffico. L'algoritmo di routing deve poi essere in grado di adeguarsi ai cambiamenti imprevisti sia della topologia della rete sia delle condizioni di traffico, garantendo sempre la continuità di esercizio;
- **Stabilità:** rappresenta un requisito irrinunciabile per un qualsiasi algoritmo di routing. La convergenza sulla soluzione ottima di equilibrio deve poi essere la più veloce possibile e comunque deve avvenire prima che le comunicazioni sia terminata;
- **Ottimalità:** l'algoritmo di routing deve scegliere il percorso ottimo secondo determinate metriche e criteri. Un metodo generale utilizzato è quello di minimizzare la distanza da percorrere (misurata in numero di salti, cioè di link, che il pacchetto deve seguire per raggiungere la sua destinazione). In questo modo, in generale, si migliora il tempo di ritardo su base end-to-end, si riduce la banda complessivamente utilizzata e, in ultima analisi, si riduce l'energia necessaria al trasferimento del pacchetto.

Il routing può essere *diretto*, quando mittente e destinatario fanno parte di una stessa rete oppure *indiretto*, quando mittente e destinatario fanno parte di reti differenti. Si noti che un routing indiretto (quando il destinatario non è connesso allo stesso router del mittente) prevede una sequenza di routing diretti relativi al passaggio dei pacchetti d'interesse tra router necessariamente connessi direttamente tra di loro (quindi appartenenti ad una stessa rete).

In generale un router (o nodo di transito) dovrà avere oltre alla funzionalità di routing anche quella di **forwarding**. La differenza tra le due funzioni è che il routing si riferisce ad una operazione che coinvolge tutti i router (nodi) di una rete che, interagendo tra di loro secondo opportune modalità (algoritmi di instradamento), concorrono ad individuare i percorsi ottimi (path o route) tra le diverse coppie di sorgente destinazione. Il routing prevede quindi che siano prese delle decisioni per individuare la scelta migliore. La funzionalità di forwarding (inoltro) invece si riferisce specificatamente al trasferimento di un pacchetto che arriva ad una interfaccia di ingresso del router all'interfaccia di uscita desiderata (e alla conseguente trasmissione sul collegamento relativo verso una nuova destinazione). Il forwarding (o switching) non prevede siano prese decisioni ma solo sia fatta una ricerca dell'uscita desiderata sulla base di informazioni già disponibili.

Gli algoritmi di routing possono essere implementati in modalità *non adattiva* (o statica) o *adattiva* (o dinamica). Gli algoritmi di routing statici si basano su decisioni predefinite e non attuali. Gli algoritmi di tipo statico non sono reattivi a variazioni di contesto relative a modifiche della topologia della rete, dovute a guasti accidentali (link, router), o variazioni di condizioni di traffico. Viceversa, gli algoritmi di routing dinamici prevedono delle procedure di aggiornamento periodico delle decisioni oppure attivate come reazione a variazioni percepite del contesto (guasti, traffico, ecc.).

Da un punto di vista metodologico, gli algoritmi di routing possono essere classificati come illustrato in figura 13.1.

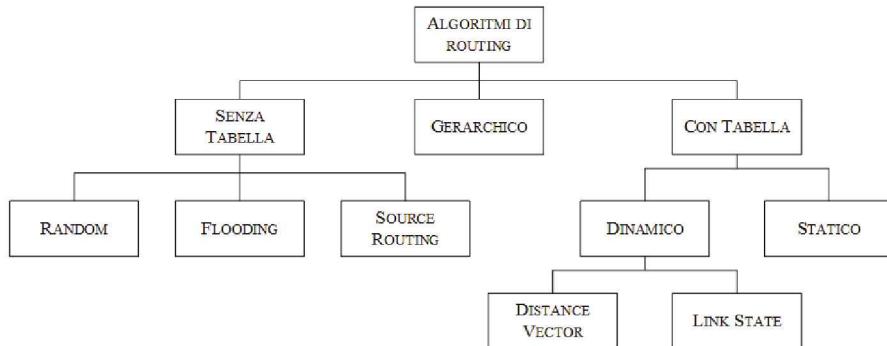


Figura 13.1: Classificazione algoritmi di Routing

Come si vede dalla figura il primo livello di classificazione degli algoritmi di routing prevede *algoritmi senza tabella*, *algoritmi con tabella* e *algoritmi gerarchici*. Gli algoritmi di routing con tabella sono algoritmi che permettono ad un nodo di associare le linee di uscita disponibili alle specifiche richieste di instradamento. Analogamente, gli algoritmi di routing senza tabella non prevedono nessun tipo di abbinamento tra linee di ingresso e uscita. Sono algoritmi di tipo reattivo, ovvero vengono attivati solo su richiesta. Gli algoritmi gerarchici sono invece riferiti al caso di reti molto estese per le quali non è praticamente possibile eseguire un instradamento diretto e si rende quindi necessario partizionare gli utenti in sottoreti, secondo uno schema gerarchico. Ciascuna delle sottoreti può attuare un instradamento con metodologie proprie ed indipendenti da quelle utilizzate nelle altre sottoreti. Un esempio pratico dove questo approccio è implementato è la rete Internet la quale prevede una organizzazione a livelli gerarchici che permettono di semplificare la definizione e gestione delle tabelle di routing. Un ulteriore vantaggio deriva dal fatto che l'organismo internazionale per l'assegnazione degli indirizzi IP, assegna gli indirizzi in base alla posizione geografica del provider ed è quindi possibile definire più facilmente la struttura gerarchica.

E' infine possibile la seguente classificazione degli algoritmi di routing:

- **Centralizzato:** prevedono esclusivamente tabelle e una unità di elaborazione centralizzata per la definizione dalla procedura di routing;
- **Distribuito:** prevede una esecuzione dell'algoritmo di routing in forma distribuita, detta anche cooperativa. Si prevede l'uso di tabelle;
- **Isolato:** tipicamente rivolta a realizzazioni senza tabella. Prevede l'esecuzione in locale (stand-alone) dell'algoritmo di routing.

Un esempio pratico

Gli algoritmi di routing con tabella dinamici prevedevano di rendere disponibili ed aggiornate in ogni router (nodo) della rete le tabelle di routing. Questa tabella

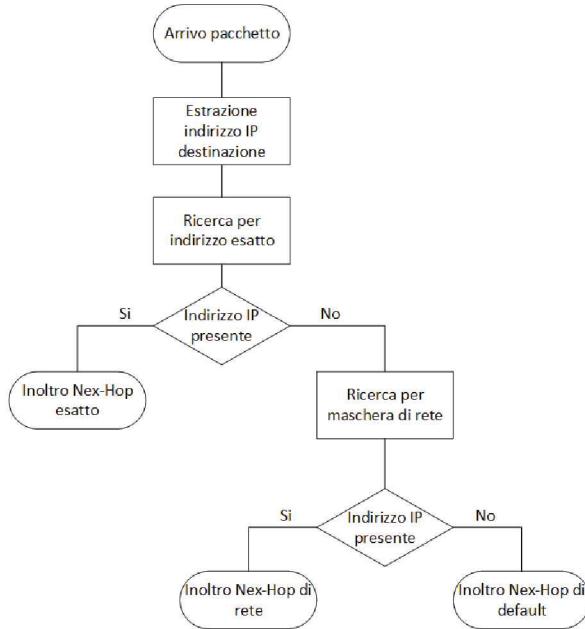


Figura 13.2: Procedura per la ricerca del Next Hop

per ogni router serve per attuare l'operazione di forwarding cioè individuare tra i router direttamente collegati (vicini) quello a cui spedire il pacchetto in maniera che l'instradamento nella rete sia realizzato secondo la scelta del cammino ottimo. Per cercare di semplificare la composizione di questa tabella, si hanno solo informazioni necessarie ad inoltrare il pacchetto al router successivo (*Next Hop*). E' evidente che non è praticamente possibile definire tabelle di routing che specifichino il *Next Hop* per tutte le possibili destinazioni. Questo problema è stato risolto limitando il numero di possibili destinazioni note ed associando ad una destinazione fittizia (default) tutte le destinazioni non riconosciute. Di conseguenza tutti i pacchetti che avranno un indirizzo di destinazione non riconosciuto saranno inoltrati verso il *Next Hop* router associato detto *router di default*.

Esaminiamo adesso più nel dettaglio la procedura attuata per implementare il forwarding di un pacchetto in un router.

Quando un pacchetto arriva ad un router viene per prima cosa estratto l'indirizzo di destinazione in modo da essere confrontato con gli indirizzi presenti nella sua tabella per poter quindi individuare il *Next Hop*. Per prima cosa viene effettuata una ricerca direttamente basata sull'indirizzo del destinatario, se non è presente viene effettuata una ricerca tramite l'identificativo della rete e, infine, se non è riconosciuto nemmeno l'identificativo della rete, il pacchetto viene associato alla destinazione di default e quindi inoltrato verso il router di default.

La procedura di ricerca del *Next Hop* è illustrata dal diagramma di flusso mostrato nella figura 13.2.

13.2 Algoritmi senza tabella

Gli algoritmi di routing senza tabella (Forouzan'2008, Tanenbaum'2011, Kurose'2013, in 13.9) operano in modalità reattiva, non hanno cioè disponibili le informazioni necessarie per definire la politica di instradamento dei flussi che invece viene stabilita su richiesta (on-demand) ogni volta che se ne pone la necessità. Di seguito esamineremo brevemente le principali tecniche appartenenti a questa classe.

Random

La prima tecnica che andiamo ad analizzare è la tecnica *random*. Questa tecnica è caratterizzata da un'implementazione molto semplice in quanto prevede l'inoltro del pacchetto su uno dei collegamenti disponibili, eccetto quello da cui il pacchetto è arrivato, selezionandolo secondo un criterio statistico opportuno. Le probabilità di ogni scelta possono, a loro volta, essere legate ad un procedimento di controllo ed ottimizzazione delle prestazioni dell'intera rete. La soluzione più elementare è quella di dare a ciascuna scelta un uguale probabilità di selezione (*distribuzione uniforme*). La semplicità di questa soluzione viene tuttavia bilanciata dalla mancanza di garanzia riguardo un utilizzo ottimo delle risorse di rete e può essere critica per la congestione dei collegamenti. Per come sono stati pensati, gli algoritmi di routing di tipo random sono robusti in quanto si possono adattare bene a variazioni di contesto, sia dovuti a guasti nei collegamenti sia a variazioni (aumento) di traffico, quindi si può avere un eccessivo affollamento (congestione) di pacchetti in certi collegamenti.

Flooding

La tecnica *flooding*, già descritta insieme ad alcune sue varianti nel capitolo 8, non prevede sia presa nessuna decisione sull'interfaccia di uscita: appena arriva un pacchetto si replica su tutte le interfacce del router, ad eccezione di quella su cui è arrivato il pacchetto. Questa procedura può ammettere un'eccezione quando viene rilevato che la destinazione del pacchetto è direttamente connessa al router su una sua interfaccia. In questo caso il pacchetto viene inoltrato solo e soltanto in quel collegamento. La tecnica flooding riduce al minimo l'elaborazione richiesta per implementarla (non esiste decisione) e rende molto sicura la consegna del pacchetto al suo destinatario (in genere riceverà più copie del pacchetto attraverso percorsi differenti). Un altro pregio di questa tecnica è sicuramente la sua robustezza, giustificata dalla sua modalità operativa. In particolare la sua notevole robustezza al riguardo di variazioni di contesto rendono questa metodologia particolarmente indicata in applicazioni militari e safety-critical (in cui è a rischio l'incolumità delle persone). Lo svantaggio principale di questa tecnica, come discusso nel capitolo 8, è dovuto all'eccessivo numero di copie di uno stesso pacchetto che si trova a circolare nella rete e che ne può provocare il collasso.

Oltre ai rimedi esaminati nel capitolo 8 due metodologie utilizzate sono:

- a. Introdurre un campo nella intestazione dei pacchetti contenente il numero massimo di ripetizioni che il pacchetto può ancora avere. Ogni router, prima di replicare il pacchetto sulle proprie uscite, controlla questo campo, se non è zero, lo ridefinisce, decrementando di uno il valore iniziale. Se invece il valore del campo è zero, il router semplicemente lo scarta. Questo rimedio è relativamente semplice ma, se non utilizzato adeguatamente, può pregiudicare la consegna dei pacchetti alle loro destinazioni (a priori non si conosce esattamente il numero minimo di Next-Hop che il pacchetto deve visitare (ripetizioni) prima di arrivare alla sua destinazione finale);
- b. Ogni router tiene copia di ogni pacchetto ripetuto. In questo modo quando un pacchetto arriva su di un ingresso, per prima cosa il router verifica se è presente una sua copia in memoria (in generale si memorizzano solo le etichette associate ai pacchetti ricevuti). Se viene trovata una copia del pacchetto questo viene scartato altrimenti viene registrato come già pervenuto e successivamente inoltrato. Questa seconda soluzione è decisamente più onerosa dal punto di vista computazione ed impegno di memoria ma, a differenza dell'altra procedura, permette di garantire una consegna sicura del pacchetto dal suo destinatario.

Source routing

La terza tecnica appartenente agli algoritmi senza tabella è l'algoritmo *source routing*. Secondo questa tecnica è direttamente il nodo sorgente che specifica il percorso del pacchetto nella rete fino al nodo di destinazione. Questa informazione è contenuta della intestazione (header) del pacchetto. Per rendere disponibile al nodo sorgente questa informazione ci sono sostanzialmente due modalità:

- **path server** (centralizzato): il percorso sorgente → destinazione è inviato al nodo sorgente da un server centrale. L'affidabilità di questa soluzione è legata all'affidabilità di esercizio del server centrale e dei collegamenti che permettono di raggiungerlo. Questo, in generale, è un aspetto particolarmente critico così come l'influenza di variazioni di stato della rete (guasti, aumento di traffico) sulla definizione dei percorsi sorgente-destinazione;
- **path discovery** (distribuito): secondo questa modalità tutti i nodi della rete cooperano a definire il percorso da seguire. Il nodo sorgente invia in flooding un pacchetto nella rete dove è specificato l'indirizzo del nodo sorgente e del nodo di destinazione. Il numero di ripetizioni del pacchetto per ogni nodo visitato è limitato ad una. Ogni volta che il pacchetto, che possiamo definire *esploratore*, visita un nodo, il nodo inserisce il proprio indirizzo nella testata del pacchetto. In questo modo si ha che, in accordo con la modalità flooding, più copie del pacchetto esploratore raggiungeranno la destinazione finale richiesta. Di queste, il nodo destinazione ne sceglierà una, di solito la prima arrivata (che rivela il percorso più veloce). Successivamente comunicherà al nodo sorgente (richiedente), con un pacchetto di riscontro, questa scelta. Tutti i pacchetti relativi al flusso informativo per il quale la

procedura di scoperta è stata attivata seguiranno il cammino selezionato. Anche in questo caso, la scelta del cammino può risentire, durante il tempo di utilizzo, di variazioni di stato della rete e, quindi, non rappresentare più la soluzione migliore.

13.3 Algoritmi con tabella

Questi algoritmi possono essere sia di tipo centralizzato che distribuito. Possono, inoltre, prevedere procedure di aggiornamento delle informazioni contenute nelle tabelle per meglio adattarsi a variazioni di contesto, in questo caso vengono definiti *dinamici*. Sono invece indicati come *statici*, quando le informazioni delle tabelle, una volta definite, rimangano inalterate rispetto a variazioni di contesto e costanti per lunghi intervalli temporali. Nel seguito ci riferiremo a due realizzazioni di algoritmi con tabella, distribuiti e dinamici in quanto questa è la tipologia di soluzione più diffusamente utilizzata nelle attuali reti di calcolatori soprattutto quando l'utilizzo ottimale delle risorse di rete con qualsiasi condizione di lavoro è un obiettivo primario.

Il *principio di ottimalità* per questi algoritmi consiste nell'individuare il percorso a metrica (costo) minima (*shortest path*) che collega la sorgente alla destinazione. A questo riguardo dobbiamo precisare che la metrica sulla base della quale viene individuato il cammino migliore può avere diverse definizioni; la lunghezza fisica dei collegamenti (quindi il ritardo di propagazione), la banda o l'affidabilità dei collegamenti sono alcune delle molte alternative possibili. Di seguito verranno descritti gli algoritmi denominati *distance vector* e *link state* senza specificare il tipo di metrica utilizzata.

13.3.1 Distance vector

L'algoritmo **distance vector** (Forouzan'2007, Tanenbaum'2011, Kurose'2013, in 13.9) è un algoritmo con tabella, dinamico e distribuito. La tabella mette a disposizione di ogni nodo (router) le informazioni relative alla distanza con ogni possibile destinazione ed il Next-Hop router a cui inoltrare i pacchetti. Queste informazioni sono mantenute aggiornate attraverso uno scambio periodico delle tabelle di routing tra i nodi vicini (direttamente connessi). La configurazione ottima della tabella di routing per l'algoritmo distance vector e la selezione dei cammini a costo minimo (migliori) per collegare un nodo ad ogni altra possibile destinazione, viene determinata mediante l'uso dell'algoritmo di *Bellman-Ford*. Questo algoritmo può essere enunciato come segue:

Trovare i percorsi a costo minore a partire da un nodo sorgente selezionandoli progressivamente.

All'inizio ogni nodo conosce solo il costo degli collegamenti verso i propri vicini. Per implementare tale algoritmo ogni router dispone della tabella di routing e di una struttura dati detta *distance vector* per ogni collegamento (link). Il distance vector associato ad un link contiene informazioni ricavate dalla tabella di

routing del router collegato tramite quel link. Il calcolo delle tabelle di routing avviene tramite un processo di fusione di tutti i distance vector associati ai link gestiti dal router. Ogni volta che un router aggiorna o calcola per la prima volta la propria tabella di routing la condivide con i router vicini. Il distance vector, in forma semplificata, lo si può pensare formato da coppie di valori: *indirizzo nodo di destinazione, costo del collegamento*. Quando un router riceve un distance vector da un router vicino, prima di memorizzarlo, ne aggiorna i valori sommando al costo di ogni collegamento previsto il costo del collegamento da cui ha ricevuto il distance vector. In questo modo il router ricevente rende propria la visione della rete percepita dal router mittente. Completata l'operazione di aggiornamento il distance vector è memorizzato nella struttura dati locale. Nell'eseguire questa operazione si confronta il distance vector ottenuto con quello già posseduto e precedentemente memorizzato per verificare se ci sono variazioni. Se questo accade, la tabella di routing viene ricalcolata fondendo tutti i distance vector dei collegamenti attivi. Questa operazione viene eseguita in accordo al criterio della maggiore convenienza di costo e, nel caso di partita di costo si privilegia l'alternativa con numero minore di hop (router presenti nel cammino) e, infine a parità di costo e di hop si effettua una scelta casuale (lancio moneta). Se ovviamente la nuova tabella di routing è differente dalla precedente questa viene condivisa con tutti gli altri router vicini. La frequenza di invio del distance vector ai router vicini è, in genere, un parametro caratterizzante lo specifico algoritmo. Un valore tipico utilizzato dall'algoritmo RIP (Routing Information Protocol, descritto di seguito) è di 30s.

Il vantaggio evidente di questa soluzione è la sua facilità di implementazione, mentre le sue criticità sono:

- Complessità computazione elevata;
- Lenta convergenza ad un instradamento stabile;
- Difficoltà di utilizzo in reti complesse.

In particolare, le prime due criticità rendono l'algoritmo di Belman-Ford poco adatto a contesti dove sia presente un elevato livello di dinamicità (mutamenti di topologia o condizioni di lavoro) che potrebbero pregiudicare la sua convergenza ad una soluzione stabile.

La lenta convergenza dell'algoritmo di Belman-Ford rende anche lungo il tempo necessario perché un guasto di un collegamento, o di un nodo, sia percepito da tutta la rete. Questo problema è noto come *conteggio all'infinito* ed è particolarmente evidente in una configurazione in cui tre router A,B,C sono collegati in cascata A→B→C. In condizioni normali A sa che può raggiungere C passando da B. Se ad un certo istante il collegamento B→C si guasta, B riesce ad accorgersi tempestivamente di questa situazione e, di conseguenza, ad aggiornare il distance vector e a condividerlo con A. Se però A invia prima che questo accada a B il suo distance vector il protocollo diventa instabile. B, sulla base della conoscenza del distance vector ricevuto da A, aggiorna la propria tabella di routing considerando come costo del collegamento verso C quello indicato da A aumentato del costo del collegamento B→A. Al periodico scambio dei distance vector,

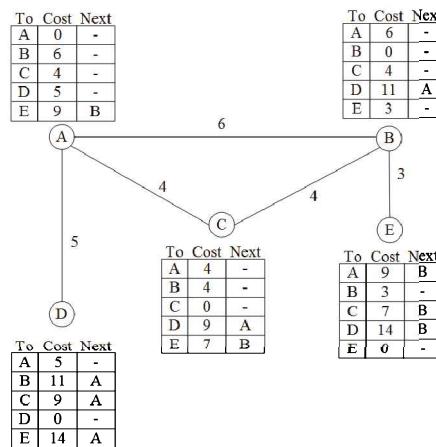


Figura 13.3: Distance vector

seguirà un progressivo incremento del costo del collegamento (ipotetico) di B verso C passando da A. Pur aumentando senza controllo questo collegamento viene comunque ritenuto possibile quando nella realtà non lo è.

Per risolvere questa situazione di instabilità dell'algoritmo si può assumere che quando il costo di un collegamento supera un valore massimo di riferimento il collegamento non è in pratica possibile (metodo dell'*infinito finito*). Questa soluzione permette di evitare che si ritenga da un certo istante in poi raggiungibile un router quando in pratica non lo è ma presenta, comunque, dei tempi di latenza che possono essere eccessivi. Una soluzione alternativa è la cosiddetta *split horizon* (orizzonte spaccato). Questa prevede l'invio di aggiornamenti solo per i cammini verso nodi non connessi direttamente con il nodo di destinazione degli aggiornamenti. In questo modo è facile convincersi che il problema della instabilità è subito risolto. Tuttavia la soluzione split horizon da luogo ad una nuova criticità: nell'algoritmo distance vector quando un'informazione non viene aggiornata per troppo tempo viene ritenuta non più attuale (o utile) e di conseguenza viene eliminata dalla tabella di routing. Per risolvere questo nuovo problema è stato proposto il metodo detto *poisoned reverse* (inversione avvelenata). In questo caso viene assegnato un valore convenzionale elevato al costo dei collegamenti che coinvolgono il router di destinazione del distance vector. In questo modo il nodo destinazione non aggiorna le scelte riguardati i collegamenti relativi e, allo stesso tempo, rinfresca le informazioni della tabella evitando che vengano eliminate. Nel nostro esempio quando A comunica a B il distance vector indicherà per il collegamento verso C un costo molto alto (superiore al valore convenzionale sopra il quale un nodo viene dichiarato irraggiungibile) in maniera che B sappia che tale nodo non è raggiungibile tramite A.

Un esempio pratico: Routing Information Protocol

Il Routing Information Protocol (RIP), è un protocollo basato sul distance vector che utilizza il numero di salti tra sorgente e destinazione come metrica di costo ed assume, di conseguenza, il costo di ogni collegamento unitario. Questo algoritmo è stato uno dei primi protocolli previsti da Internet per l'instradamento dei datagrammi in una rete ed è, ad oggi, ancora utilizzato. Il protocollo RIP evita l'instabilità dei metodi distance vector impostando come valore di irraggiungibilità di un nodo il valore 15. Questa scelta limita l'uso del protocollo RIP in reti in cui la distanza massima tra coppie sorgente-destinazione (misurata in hop, cioè numero di router (o sottoreti) interessati dal collegamento) non supera 15. Se un nodo ha come metrica 16 è quindi considerato irraggiungibile e non verrà quindi inserito nella tabella di routing. In RIP i router vicini si scambiano le informazioni di aggiornamento delle tabelle di routing ogni (circa) 30s in modalità normale oppure non appena vengono evidenziate delle variazioni di contesto. Viene utilizzato un messaggio detto *RIP response* che può comprendere informazioni (indirizzo, costo del collegamento) riferite ad massimo di 25 destinazioni. Questi messaggi sono spesso anche indicati come *RIP advertisement* (annunci RIP). Se un router non riceve aggiornamenti da un suo vicino entro un tempo massimo di 180s, quel router viene considerato non più raggiungibile presupponendo che sia stato spento o che il collegamento verso di esso non sia utilizzabile. Questo evento genera un aggiornamento della tabella di routing e conseguentemente forza il router a comunicarla tramite un RIP advertisement a tutti i router vicini. Questo protocollo prevede anche un altro tipo di messaggi detti di richiesta generati da un router, presentemente inattivo, che diventa attivo, oppure per aggiornare delle informazioni scadute della tabella di routing.

I messaggi di richiesta e risposta in una rete Internet utilizzando il protocollo UDP. Questo a prima vista appare come una situazione anomala in quanto si utilizza un protocollo di livello TCP per attivare funzionalità proprie del livello IP. In realtà questa è una incongruenza solamente apparente in quanto il RIP è implementato a livello applicazione da un processo *demone* (sempre in esecuzione) indicato come *route daemon* che offre servizi di routing. In particolare, questo processo definisce le tabelle di routing di livello IP e gestisce i processi di aggiornamento delle stesse mediante la loro condivisione con i router vicini. Esiste una versione recente di RIP, indicata come RIPng specificata in RFC 2080, che è una estensione del protocollo originale resa specifica per reti IPv6.

Le caratteristiche principali dell'algoritmo RIP sono:

- I RIP advertisement hanno una struttura semplice, vengono scambiati solo con i router vicini e, tipicamente, ne viene evitato l'invio contemporaneo da parte di più router;
- La convergenza è relativamente veloce conseguenza della limitazione del costo dei collegamenti che, a sua volta, esclude router *tropppo distanti*. Non viene evitata l'instabilità dovuta al problema del conteggio all'infinito che, tuttavia, può essere contenuta utilizzando i metodi split horizon e poissoned reverse;

- La robustezza dell'algoritmo è garantita dalla modalità di aggiornamento prevista che consente di diffondere nella rete ogni variazione di contesto che genera cambiamenti nelle decisioni di instradamento.

13.3.2 Link state

Questo algoritmo di routing prevede che ogni nodo acquisisce la conoscenza globale della rete partendo dalla conoscenza (metrica o costo) dello stato dei collegamenti verso i nodi vicini. Una volta acquisite queste informazioni, il nodo proprietario le condivide con i suoi vicini inviando dei pacchetti detti *Link State Packet*(LSP) in modalità flooding. In questo modo ogni nodo della rete riceve le informazioni relative allo stato dei collegamenti e alle distanze stimate degli altri nodi verso i loro vicini ed è quindi in grado di individuare i cammini migliori verso tutte le possibili destinazioni. Di conseguenza l'algoritmo link state assume che ogni router (nodo) della rete disponga della conoscenza (mappa) completa della rete su cui definire gli instradamenti ottimi. L'algoritmo utilizzato per la creazione della tabella ottima di routing è l'algoritmo di *Dijkstra* (Forouzan'2007, Tanenbaum'2011, Kurose'2013, in 13.9). Questo algoritmo può essere enunciato come segue :

Trovare i percorsi migliori da un nodo sorgente verso tutti gli altri nodi, definendoli per costi crescenti.

È importante sottolineare che la mappa completa della rete non è predefinita in ogni router ma viene acquisita in maniera cooperativa con gli altri router, tramite lo scambio dei pacchetti LSP come evidenziato in precedenza. I pacchetti LSP sono trasmessi secondo la modalità flooding detta selettiva che, a differenza della tecnica flooding classica, seleziona i collegamenti sui quali ripetere un pacchetto sulla base della stima della direzione di arrivo (es.: non si inoltra il pacchetto su tutti i collegamenti che sono ritenuti andare in direzione opposta da quella di arrivo). Ogni router possiede un LSP database che contiene tutte le versioni più recenti dei messaggi LSP ricevuti dai router vicini. Gli LSP database rappresentano, in pratica, la mappa della rete in quanto contengono tutte le informazioni necessarie (es.: costo dei collegamenti su base link-to-link) per permettere la definizione della tabella di routing ottima secondo l'algoritmo di Dijkstra. A questo punto è importante evidenziare una prima differenza con l'algoritmo distance vector dove tutti i router della rete cooperano attivamente e direttamente per definire le tabelle ottime di routing. Nel caso dell'algoritmo link state, i router cooperano ed interagiscono tra di loro solo per diffondere nella rete le informazioni necessarie per aggiornare lo stato dei collegamenti con i propri router vicini. Conseguentemente, ogni router in modalità autonoma, provvederà a ridefinire, aggiornandola, la propria tabella di routing secondo l'algoritmo di Dijkstra. La complessità di calcolo dell'algoritmo di Dijkstra la si può ritenere, per una rete con N router (nodi), dell'ordine $N \log(N)$. Questo algoritmo consente poi di gestire reti di grandi dimensioni, ha una convergenza rapida, difficilmente genera dei cicli che comunque possono essere riconosciuti e risolti ed è, infine, di facile

interpretazione. Il suo svantaggio principale è legato alla complessità di implementazione nei router per i quali sono richieste buone capacità di elaborazione e di memoria.

Un esempio pratico: Open Shortest Path First

L'Open Shortest Path First (OSPF) è un protocollo di routing che si basa sull'algoritmo link state standardizzato nel 1989 con l'RFC 1131. Esiste anche una versione per IPv6 uscita nel 1999 e specificata in RFC 2740 (vedi paragrafo 13.9). Come intuibile dall'acronimo *open* presente nella sua definizione, OSPF è di tipo aperto cioè le sue specifiche sono pubbliche. Questo algoritmo è stato concepito come un successore, e quindi come evoluzione, del protocollo RIP. OSPF utilizza la modalità flooding per diffondere le informazioni relative allo stato dei collegamenti e l'algoritmo di Dijkstra per la definizione dei percorsi a costo minimo verso tutte le possibili destinazioni (albero a costo minimo). I costi, quindi le metriche, su cui si basa l'algoritmo di Dijkstra possono essere differenti e non omogenei tra loro. Si può ad esempio decidere di impostare il costo di tutti i collegamenti ad uno e quindi, come per RIP, considerare come metrica solo il numero di salti (hop), oppure definire dei costi inversamente proporzionali alla massima velocità di trasmissione possibile nei collegamenti scoraggiando in questo modo scelte che coinvolgano collegamenti lenti. In sintesi OSPF non si occupa della metrica utilizzata ma definisce una procedura ad essa trasparente per definire un albero con percorsi a costo minimo. In OSPF ogni volta che un router rivela una variazione dello stato di un collegamento verso un router vicino o il cambiamento di disponibilità dello stesso, provvede a diffondere nella rete in modalità flooding il nuovo stato dei collegamenti con i suoi vicini. Se il contesto rimane stazionario, il router provvede comunque a diffondere nella rete, periodicamente, lo stato dei suoi collegamenti ogni 30 minuti (circa). Questa modalità assicura all'algoritmo OSPF un notevole livello di robustezza. I pacchetti di aggiornamento (LSP) vengono trasportati direttamente da IP come se fossero provenienti dal livello TCP. OSPF deve inoltre permettere un trasferimento affidabile delle informazioni, consentire la modalità broadcast e controllare che i collegamenti siano attivi (mediante messaggi opportuni detti HELLO).

Le caratteristiche principali dell'algoritmo OSPF sono:

- Lo scambio di informazioni tra i router OSPF può essere autenticati evitando intrusioni esterne finalizzate a mettere a rischio l'operatività della rete (vedi capitolo 15);
- Quando sono presenti percorsi con lo stesso costo OSPF consente di utilizzarli indistintamente senza necessità di usarne uno soltanto (bilanciamento del carico);
- permette di supportare in forma unificata instradamento unicast, multicast e broadcast (vedi paragrafo 13.7);
- Possibilità di gestire strutture gerarchiche (vedi paragrafo 13.5);

- La tabella di routing viene creata autonomamente da ogni router questo da un lato rende più veloce il processo di convergenza dell'algoritmo di Dijkstra attivato in locale dall'altro richiede sufficienti capacità di calcolo al router.

13.3.3 Distance vector e link state a confronto

I due algoritmi utilizzano approcci diversi per definire la tabella di routing: nell'algoritmo distance vector ogni nodo comunica solo con i nodi a lui connessi per scambiarsi informazioni inerenti al costo del percorso tra di loro mentre nell'algoritmo link state ogni nodo comunica con tutti i nodi della rete per acquisire una visione globale della rete stessa. In caso di variazione di costo per un collegamento tra due nodi, con l'algoritmo link state tutta la rete viene inondata con un messaggio che informa di tale variazione, indipendentemente dalla sua effettiva utilità al riguardo dell'aggiornamento della tabella di routing che ogni nodo valuta localmente. Invece nell'algoritmo distance vector, il cambio del costo verrà notificato a tutti i nodi della rete solo se esso introduce un cambio del percorso a minor costo per uno dei nodi collegati a quel link. L'algoritmo link state è più robusto rispetto al distance vector, poiché ogni nodo, in modo indipendente rispetto agli altri, calcola la propria tabella di routing. Invece nell'algoritmo distance vector, ogni calcolo (sbagliato) dei costi dei collegamenti viene poi passata ai nodi adiacenti, favorendo il propagarsi dell'errore nell'intera rete.

13.4 Dalla teoria alla pratica: Architettura di un router Link State

Vediamo di seguito come un router implementa nella pratica l'algoritmo link state descritto nel paragrafo 13.3.2. Riferendosi alla seguente figura 13.4 si ha che ogni volta che il *receive processor* ha un pacchetto in ingresso, questo ne verifica il tipo. In generale si possono avere queste alternative:

- *Pacchetto dati di transito*: il receive processor lo trasferisce al forwarding processor (entità che sovrintende all'operazione di forwarding descritta nel paragrafo 13.1) che, interrogato il forwarding database locale usando come chiave l'indirizzo di destinazione del pacchetto, ne determina l'instradamento cioè identifica il collegamento verso un nodo vicino su cui trasmettere il pacchetto;
- *Pacchetto dati destinato al router*: Il pacchetto viene passato ai livelli superiori.
- *Pacchetto di Hello*: questi pacchetti sono detti anche *neighbor greetings* (saliuti dai vicini) vengono utilizzati per segnalare la presenza di un nodo vicino. In questo caso, il router ricevente, come primo passo, verifica se già conosce il nodo vicino. Se è così, ignora il pacchetto altrimenti lo inserisce nella lista dei suoi vicini e notifica questa variazione a tutti i nodi adiacenti noti mediante un messaggio LSP in modo che il nuovo nodo possa essere raggiunto da tutti i nodi della rete;

- **Pacchetto LSP:** Questo pacchetto, oltre alle informazioni relative alle adiacenze del nodo che l'ha generato, contiene anche un'informazione sulla sua attualità (numero di sequenza). Il router sorgente trasmette i pacchetti LSP in flooding su tutti i collegamenti mentre un router ricevente lo ripete sui suoi collegamenti (eccetto quello di arrivo) solo se l'informazione ha generato un aggiornamento del proprio LSP data base (flooding selettivo). La procedura attivata dal router, a seguito della ricezione di un LSP, prevede i seguenti passi:

1. Se non ha mai ricevuto pacchetti LSP da quella sorgente o se il numero di sequenza rilevato è maggiore di quello associato all'ultimo pacchetto LSP ricevuto della stessa sorgente (contenuto nel LSP database), il router aggiorna il suo LSP database con le nuove informazioni e lo ripete in flooding su tutti i collegamenti, eccetto quello da cui è arrivato;
2. se il pacchetto LSP ricevuto ha un numero di sequenza uguale a quello disponibile nel LSP database locale non viene attivata nessuna ulteriore procedura;
3. se il pacchetto LSP ricevuto ha un numero di sequenza inferiore a quello relativo alla copia contenuta nel LSP database locale, il nodo trasmette sulla stesso collegamento di arrivo al nodo mittente (che non è il nodo sorgente dei messaggi LSP) il proprio pacchetto LSP per l'aggiornamento del LSP database del mittente.

La procedura descritta in precedenza è necessaria affinché nella rete non siano inoltrate informazioni obsolete ed allo stesso tempo per fare in modo che tutti i LSP database dei router si mantengano aggiornati e sincronizzati, condizione irrinunciabile per perseguire un instradamento ottimo nella rete.

13.5 Algoritmi gerarchici

Questi algoritmi nascono da specifiche necessità pratiche. La dimensione delle tabelle di routing cresce proporzionalmente alle dimensioni della rete. E' quindi ragionevole ritenere che con un qualsiasi algoritmo a tabella sia possibile gestire qualsiasi tipo di rete (si pensi ad esempio alla rete Internet nella sua completa globalità). L'aumento di dimensione delle tabelle non solo implica una maggiore richiesta di memoria ai router della rete ma determina anche un consistente (a volte non sostenibile) aumento del tempo di calcolo necessario per elaborare le informazioni e per diffondere gli aggiornamenti nella rete. Inoltre, un ulteriore problema, non secondario, è che l'aumento del numero di router rende molto complesso il processo di convergenza degli algoritmi di routing alla soluzione ottima.

Per queste ragioni, in reti complesse, il routing viene organizzato in modo gerarchico, cioè si partiziona la rete in regioni, tra loro interconnesse secondo uno schema gerarchico. Tutti i router appartenenti ad una stessa regione operano con le modalità fino a qui descritte (routing intra-regione): ogni router conosce tutte

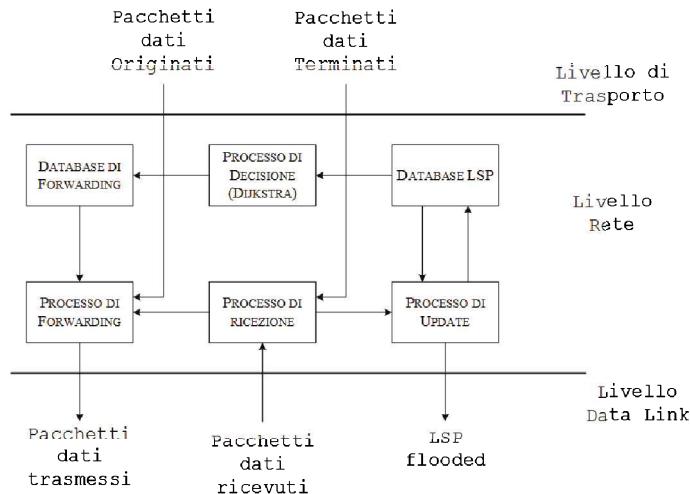


Figura 13.4: Architettura di un router link state

le informazioni necessarie per attivare l'instradamento dei pacchetti con destinazioni appartenenti alla stessa regione ma non ha informazioni sulle reti delle altre regioni. Secondo questa metodologia è logico considerare la rete propria di una certa regione come un sistema autonomo per il quale possono essere usate tecnologie specifiche, non necessariamente uguali a quelle utilizzate in altri contesti. Per questo motivo, le reti riferite a regioni specifiche vengono indicate come **Autonomous System (AS)**. Il concetto di AS (Forouzan'2007, Tanenbaum'2011, Kurose'2013, in 13.9) è essenzialmente di tipo amministrativo e si riflette principalmente sulle operazioni di routing. Il gestore dell'AS ha completa autonomia sulla rete e gestisce i blocchi di indirizzi a lui assegnati come meglio crede. Di conseguenza, un gestore di AS può scegliere la politica di routing che ritiene più conveniente ed adatta alle sue necessità in maniera completamente indipendente dalle soluzioni adottate in altri AS.

Tutti i router appartenenti ad un AS funzioneranno con lo stesso protocollo di routing. Questo algoritmo viene chiamato *intra-autonomous system routing protocol* e può essere basato su algoritmi con tabella o senza tabella; ovviamente la scelta è a discrezione del gestore. Questo approccio pone però il problema di come far comunicare AS che adottano politiche di gestione differenti. Questo obiettivo viene raggiunto utilizzando specifici dispositivi denominati *router/gateway di frontiera*, i quali devono comunicare tra loro sulla base di un protocollo comune. Ad oggi l'algoritmo più utilizzato per questo scopo è conosciuto come Border Gateway Protocol (BGP). E' un algoritmo basato sul vettore delle distanze le cui principali finalità sono:

- Ottenere informazioni sulla raggiungibilità delle reti delle varie regioni da parte dei sistemi confinanti;

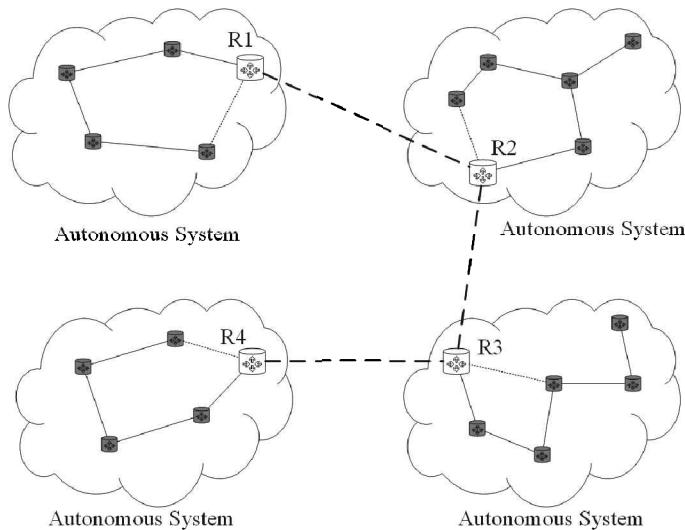


Figura 13.5: Autonomous System

- Diffondere le informazioni di raggiungibilità a tutti i router interni ad un AS;
- Identificare i percorsi migliori sulla base di criteri opportuni (vedi Tanenbaum'2013 in 13.9) verso le reti delle varie regioni.

Una discussione più approfondita dell'instradamento tra AS mediante il protocollo BGP non rientra negli scopi attuali di questo testo. Per un suo approfondimento si rimanda ai testi suggeriti come letture consigliate al termine di questo capitolo.

Come conclusione di questo paragrafo possiamo dire che con la divisione della rete internet in AS si è risolto il problema della gestione di milioni di router limitando le funzionalità di un router intra-AS alla solo conoscenza dei router appartenenti al suo stesso AS (compreso del/dei router di frontiera).

Da notare infine che un AS che ha una sola connessione verso un altro AS è chiamato *AS terminale* mentre un AS che ha più connessioni verso altri AS e permette il transito di messaggi al suo interno viene detto *AS di transito*. Mentre un AS che ha più connessioni ma non permette il transito di messaggi viene indicato semplicemente come *AS con più connessioni*.

13.6 Routing su base etichetta: Multiprotocol Label Switching

Il Multiprotocol Label Switching, o abbreviato MPLS, fu sviluppato intorno alla seconda metà degli anni novanta al fine di migliorare la velocità di commutazione dei classici router IP. Il principio base su cui MPLS si fonda è mutuato dalla

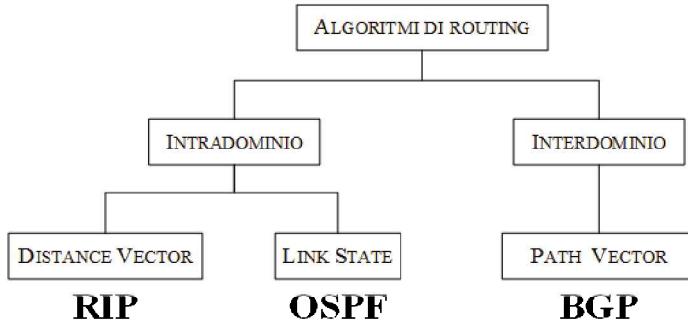


Figura 13.6: Classificazione degli algoritmi di routing

modalità con cui nelle reti Frame Relay e ATM viene gestita la commutazione nei nodi di transito. La commutazione su base etichetta di lunghezza fissa risultava decisamente più veloce della classica commutazione IP per questo motivo IETF ratificò la nascita di MPLS con la RFC 3031 e RFC 3032 nel 2001.

MPLS altro non fa che aggiungere un'etichetta di 32 bit tra l'header IP e l'header di livello 2, come mostrato in figura 13.7. Il significato dei vari campi è:

- *label*: è un campo di 20 bit ed è il valore dell'etichetta. Ha significato link to link. I valori dell'etichetta vengono decisi autonomamente dai commutatori;
- *Exp*: campo di 3 ed è un campo inizialmente definito come sperimentale, un suo possibile utilizzo è l'indicazione della classe di servizio;
- *S*: campo di un bit. Se è posto a 1 indica che l'etichetta è l'ultima dello stack, se è 0 ne esistono altre successive. Un router del dominio MPLS può assegnare una label a un gruppo di messaggi in ingresso "affasciandoli" in un singolo path di uscita. Questo è ottenuto aggiungendo una label alla label già presente. Le label vengono processate in ordine LIFO, *Last In, First Out* (ultimo ad entrare, primo ad uscire);
- *TTL*: campo da 4 bit e corrisponde all'omonimo campo dell'header IP. Il valore del campo TTL dell'header IPv4 (oppure il valore del campo Hop Limit in IPv6), viene ricopiatato in questi 4 bit. L'ultimo router del mondo MPLS cambierà il valore nell'header IP con quello presente nell'etichetta.

Da notare che MPLS può instradare qualsiasi protocollo di livello rete, da qui il nome multiprotocollo.

I router che operano secondo MPLS vengono chiamati *Label Switching Routers* (LSR) e un flusso con una prestabilita etichetta viene definito *Forward Equivalence Class* (FEC): per ogni FEC viene stabilito un percorso all'interno della rete che opera con MPLS. Inoltre una FEC è caratterizzata, oltre che dalla label, anche dalla Qualità del Servizio (QoS) richiesta.

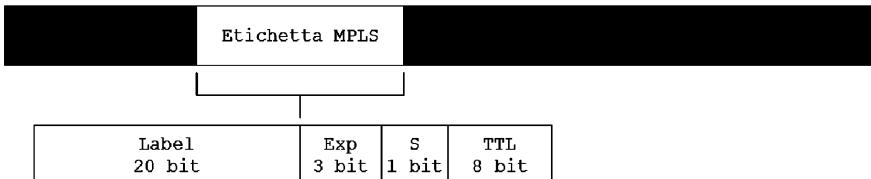


Figura 13.7: Etichetta MPLS

Le label hanno valore locale, ogni LSR deve sapere i valori associati dai vicini e può accadere che due router inviano allo stesso router pacchetti diversi con la stessa etichetta. Ogni LSR deve conoscere come i propri vicini hanno associato le label alle FEC (label binding). Esistono diversi protocolli di distribuzione delle label, i più noti sono il Label Distribution Protocol (LDP) specificato in RFC 3036 e l'RSVP-TE, descritto in RFC 3209 (Tanenbaum'2011 in 13.9). Il router di ingresso (Edge-LSR) al dominio MPLS abbina ad ogni pacchetto una label interpretando la testata IP del pacchetto IP per individuare la sua destinazione e associarlo ad una particolare FEC. I flussi che devono seguire uno stesso percorso, *Label Switched Path* (LSP), vengono associati ad una stessa etichetta. Una volta associata l'etichetta ad ogni pacchetto (label pushing), il router inoltra il messaggio sull'interfaccia di uscita che corrisponde al next hop del percorso identificato. I router intermedi ricevono i messaggi ed effettuano la sostituzione della label di arrivo con la corrispondente label di uscita (label swapping) secondo quanto definito nella Label Switching Table e lo inoltra verso il next hop. Il router di uscita (Edge-LSR) dal dominio MPLS rimuove l'etichetta (label popping) ed effettua il routing in base alla propria tabella sulla base dell'indirizzo IP del pacchetto ricevuto. Il funzionamento di MPLS è illustrato nella figura 13.8.

MPLS può poi operare su più livelli aggiungendo più di una etichetta ad uno stesso pacchetto (campo S) e creando quella che viene detta *pila di etichette*. Questo, ad esempio, si verifica quando pacchetti con etichette differenti devono seguire un tratto di percorso comune. In questo caso in vece che definire percorsi multipli su base etichetta si possono associare i flussi assegnandoli una stessa etichetta che li caratterizzerà nel tratto comune. L'LSR alla fine del percorso comune controllerà il campo S e di conseguenza rimuoverà l'etichetta più esterna ed i pacchetti verranno inoltrati sulla base delle etichette rimanenti.

MPLS permette di effettuare anche il cosiddetto **traffic engineering**. A differenza di IP che opera su base pacchetto (la scelta del percorso viene presa sul pacchetto singolo in ingresso al router sulla base del percorso più breve verso la destinazione finale) e non prevede cammini multipli, MPLS opera su base flusso, quindi si possono usare percorsi differenti per lo stesso flusso. Ogni percorso può essere soggetto a QoS diversa e la scelta di smistare il flusso su più percorsi è dettata dall'ottimizzazione delle prestazioni, motivi implementativi o per altre ragioni (Kurose'2013 in 13.9).

Inoltre MPLS permette di facilitare la realizzazione delle Virtual Private Networks (VPN). MPLS può separare il flusso della VPN dal traffico normale e permettere un elevato grado di sicurezza. Non andando, né a controllare né a modi-

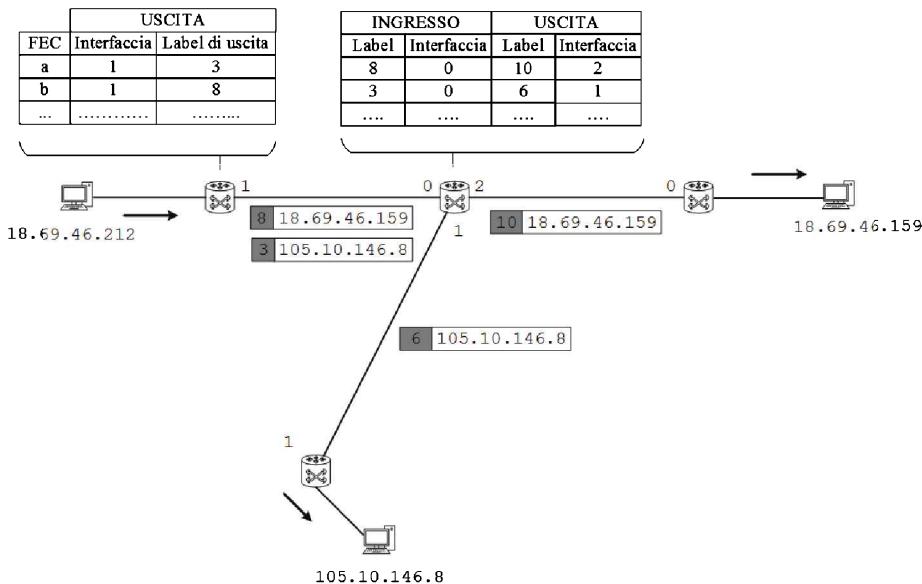


Figura 13.8: Routing MPLS

ficare, gli indirizzi IP del pacchetto MPLS rende semplice rendere segreto (vedi capitolo 15) il campo degli stessi header IP. Per maggiori informazioni su questo argomento si rimanda ai documenti RFC 4364 e RFC 4381.

13.7 Routing Broadcast e Multicast

Nei paragrafi precedenti abbiamo discusso la modalità di instradamento tra coppie isolate sorgente-destinazione. Questa modalità viene di solito indicata come *unicast*. Le moderne esigenze di servizio e le nuove applicazioni di una rete internet o, più in generale, di una rete di calcolatori ha reso necessario considerare con più attenzione le modalità di instradamento multiplo broadcast e multicast descritte di seguito.

13.7.1 Broadcast

In questo caso un pacchetto generato da una sorgente deve essere recapitato a tutti i dispositivi della rete secondo una relazione del tipo *da uno a tutti*. Le esigenze di comunicazioni broadcast nascono in reti dedicate a sistemi per l'elaborazione distribuita delle informazioni o in sistemi di informazione a diffusione pervasiva come quelli relativi a servizi meteo, di finanza, di intrattenimento, ecc.. E' immediato rendersi conto che le comunicazioni broadcast, in reti troppo estese, genererebbero seri problemi di traffico nei collegamenti ed è, quindi, per questo motivo che tipicamente il suo uso si indirizza principalmente verso reti

in aree limitate. Un metodo semplice per attuare una comunicazione broadcast che non necessita di modifiche funzionali è quello che prevede tanti collegamenti unicast quanti sono i dispositivi della rete. Gli svantaggi e le criticità di questa soluzione sono tuttavia ben evidenti (numero eccessivo di copie di uno stesso pacchetto inviato, necessità di definire cammini da una sorgente a tutte le possibili destinazioni del gruppo broadcast) ed è, quindi, facilmente intuibile perché non è di pratico interesse (si veda Forouzan'2007, Tanenbaum'2011, Kurose'2013, in 13.9). Una soluzione migliore è il *multidestination routing* che prevede l'invio da parte della sorgente di un solo pacchetto che però prevede nel suo campo di indirizzo la lista di tutte le destinazioni o ne specifica la tipologia broadcast. Quando il pacchetto arriva ad un router questo campo viene letto ed interpretato, di conseguenza viene attivato l'inoltro una copia del pacchetto su ogni linea di uscita inserendo nella testata delle singole copie inviate solo gli indirizzi delle destinazioni raggiungibili attraverso il collegamento a cui sono riferite. In questo modo, progressivamente, il campo di indirizzo si riduce di dimensioni fino ad arrivare a contenere l'indirizzo di un unico dispositivo destinazione e quindi riportando l'instradamento broadcast alla versione classica unicast. Questa soluzione riduce il numero di copie trasmesse e tutte le problematiche conseguenti ma non evita che il nodo sorgente debba conoscere l'indirizzo di tutte le destinazioni ed aumenta, rispetto alla modalità unicast, i tempi di elaborazione nei router di passaggio. Una tecnica che si presenta naturalmente adatta a gestire comunicazioni broadcast è la tecnica *flooding* descritta nel paragrafo 13.2. Una elegante ed efficiente variante della tecnica flooding è la tecnica Reverse Path Forwarding (RPF) (instradamento sul percorso inverso) che prevede l'inoltro di un pacchetto broadcast da parte di router su tutte le sue interfacce (eccetto quella da cui ha ricevuto il pacchetto) solo se è arrivato seguendo il cammino più breve tra il router stesso e il nodo sorgente. Se questo non è verificato il pacchetto viene scartato. Infine, un significativo miglioramento rispetto a quanto è possibile ottenere con la metodologia flooding o RPF è ottenuto ricorrendo alla tecnica dell'albero ricoprente (spanning tree) per il quale il nodo sorgente è la radice. Con questo metodo ogni volta che un pacchetto, per il quale è specificato l'inoltro broadcast, arriva ad un nodo questo viene replicato su tutti i rami di uscita (collegamenti) ad esso riferiti. Questa soluzione limita al minimo possibile il traffico nella rete (copie trasmesse di uno stesso pacchetto) ma pone il problema della conoscenza dell'albero ricoprente per ogni nodo verso ogni altro possibile nodo della rete. Questo requisito può essere rispettato senza aggravî solo se la rete implementa un algoritmo di routing unicast di tipo link state mentre diventa improponibile negli altri casi.

13.7.2 Multicast

In una collegamento *multicast* è presente una sola sorgente ed un insieme di destinazioni. In generale si identifica questo tipo di collegamento con il termine *da uno a molti*. Oggi sono molte le applicazioni che richiedono questo tipo di collegamento, come esempi si può pensare all'invio di informazioni di controllo a più centri di sorveglianza, la distribuzione di informazioni di interesse di una comunità specifica, il trasferimento di aggiornamenti software, intrattenimento

(video streaming, giochi condivisi, ecc.), formazione a distanza, servizi di teleconferenza e molto altro ancora. Si possono individuare due modalità attuative di un collegamento multicast (Forouzan'2007, Tanenbaum'2011, Kurose'2013, in 13.9):

- *Multicast base* : in questo caso è necessario che il gruppo di destinatari sia identificato in maniera univoca mediante un indirizzo comune. La sorgente invia un solo pacchetto nella rete con l'indirizzo del gruppo multicast. I router raggiunti dal pacchetto (o da una sua copia) provvedono a duplicarlo in tante copie quante sono le uscite su cui deve essere inoltrato per raggiungere i componenti del gruppo multicast. In questo caso il numero di copie di uno stesso pacchetto riferito ad uno stesso link è limitata ad una. Nel seguito, per semplicità, ci riferiremo questa metodologia indicandola semplicemente come *multicast*;
- *Unicast multiplo*: in questo caso non è necessario definire un indirizzo univoco per il gruppo. La sorgente invia nella rete un numero di copie di uno stesso pacchetto quante sono le destinazioni finali (nodi appartenenti al gruppo multicast). Ogni pacchetto ha l'indirizzo del suo destinatario. In questo caso è evidente che in ogni collegamento si possano trovare in sequenza più copie di uno stesso pacchetto.

La modalità *unicast multiplo* apparentemente potrebbe sembrare la più efficiente in realtà essa presenta delle criticità importanti che, di fatto, fanno preferire la modalità *multicast*. Nello specifico, esse sono:

- *Efficienza*: il *multicast* è più efficiente del *unicast multiplo* in quanto su ogni link viene inoltrata una sola copia del pacchetto d'interesse, si riduce, quindi, in questo modo sia l'occupazione di banda che il consumo di energia in trasmissione;
- *Ritardo*: la modalità *unicast multiplo*, prevedendo l'invio di più copie di uno stesso pacchetto in sequenza su uno stesso link, inevitabilmente introduce dei ritardi di trasmissione. Questo effetto negativo si riscontra anche nei router che, a loro volta, devono gestire più copie di uno stesso pacchetto (legate alle destinazioni raggiungibili tramite i propri collegamenti con i router adiacenti) invece di limitarsi ad una sola copia per interfaccia (quando richiesto ovviamente) indipendentemente dai destinatari raggiungibili attraverso il collegamento associato.

Le due modalità di gestione di un inoltro multicast sono illustrate nella seguente figura 13.9 e descritte di seguito.

Instradamento multcat con albero condiviso dal gruppo (Group-shared tree)

Come nel caso dell'albero ricoprente questo approccio si basa sulla costruzione di un albero a costo minimo per connettere tutti i nodi a cui fanno capo i dispositivi del gruppo multicast. E' un approccio centralizzato: si individua un nodo come

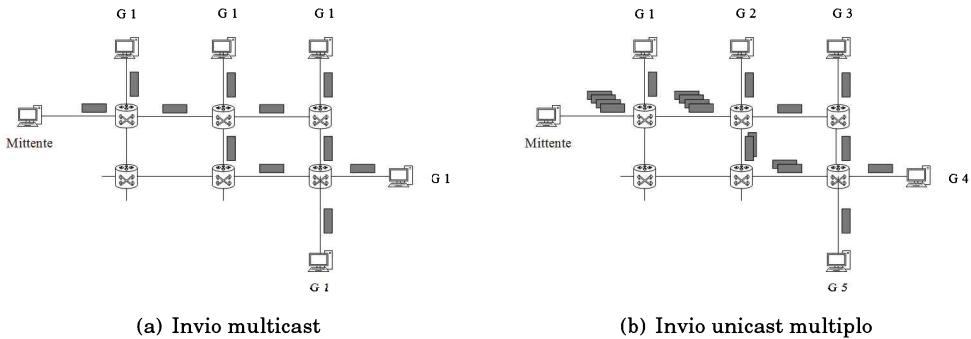


Figura 13.9: Modalità Multicast e Unicast Multiplo

coordinatore (core) del gruppo. Un qualsiasi nodo della rete che desideri inviare un flusso informativo al gruppo multicast lo indirizza in modalità unicast al *coordinatore* che si fa carico di inoltralo a tutti i membri del gruppo. L'albero ricoprente (spanning tree) viene formato inviando verso il *coordinatore* dei messaggi di adesione al gruppo. Questi messaggi potranno poi arrivare direttamente al *coordinatore* oppure si fermeranno in router che già appartengono all'albero ricoprente. I percorsi seguiti dai messaggi di adesione al gruppo costituiranno i rami dell'albero ricoprente, cioè i percorsi che i messaggi indirizzati al gruppo seguiranno per raggiungere tutti i membri del gruppo multicast.

Instradamento multicast con albero basato sull'origine (Source-based tree)

La differenza fondamentale con il primo metodo è che, in questo caso, l'albero ricoprente (spanning tree) non è unico ma viene definito per ogni possibile sorgente verso tutti i nodi della rete (gruppo multicast) interessati a riceverne le informazioni. L'albero ricoprente viene definito mediante la metodologia RPF descritta in precedenza. Viene inoltre introdotta una modifica detta *potatura* (pruning), attuata quando un router non ha collegamenti verso nessun nodo del gruppo multicast. In questo caso semplicemente il router notifica al router mittente che non è interessato all'inoltro dei pacchetti multicast e quindi ne richiede l'interruzione. Il *Multicast OSPF* (MOSPF) è un esempio di protocollo basato sul medito link state che opera in accordo con questa metodologia.

13.8 Un caso di studio: Il protocollo di routing RPL

Il protocollo RPL è un protocollo di routing per le Low-Power and Lossy Networks Low-Power and Lossy Networks (LLN), il quale gestisce l'instradamento nei dispositivi a bassa potenza (es.: reti di sensori) che supportino IPv6. In quanto protocollo di routing, esso si colloca nel livello 3 del modello ISO/OSI. RPL si

basa sul vettore delle distanze (distance vector), anche se nella realtà non forma dei veri e propri alberi, ma genera una particolare struttura a grafo. Nel protocollo non viene esplicitamente specificata la metrica associata ai cammini all'interno del grafo, questo poiché la sua definizione può variare a seconda delle applicazioni.

RPL si basa sulla formazione dei Directed Acyclic Graph (DAG), ovvero grafi in cui tutti i collegamenti sono orientati in modo tale che non esistano cicli. La radice del DAG è definita DAG Root. Poiché il grafo è aciclico, per definizione tutti i DAG devono avere almeno una radice e tutti i percorsi devono terminare alla radice. In RPL il grafo viene chiamato Destination Oriented Directed Acyclic Graph (DODAG): è un DAG orientato aciclico dove i cammini procedono verso i nodi radice, ove terminano. Per la definizione di DAG Root, non esistono collegamenti verso l'esterno del grafo. Ad ogni DODAG è associato unidentificatore (ID) detto DODAG ID, il quale è unico all'interno di una istanza. L'istanza è un insieme di uno o più DODAG identificata in modo univoco da un ID (RPL Instance ID); ogni istanza è indipendente dalle altre. Oltre al DODAG ID, RPL prevede di identificare la specifica configurazione di un DODAG, ovvero il DODAG Version. I nodi appartenenti ad un DODAG vengono identificati mediante un numero (Rank) che ne identifica la posizione nel grafo rispetto al nodo radice. Normalmente alla Root viene assegnato il valore uno. Il Rank cresce spostandosi verso le foglie dell'albero (ovvero verso l'esterno del grafo). Il suo valore è determinato da una funzione che dipende dalla distanza dalla radice, da metriche di link e da altri parametri. La funzione con cui viene calcolato il Rank (rango) di un nodo prende il nome di Objective Function (OF): definisce le metriche di routing e le funzioni per calcolare il Rank. Inoltre l'OF impone la selezione dei genitori e quindi come si forma il DODAG.

I percorsi RPL sono ottimizzati per il traffico da o verso una o più radici che agiscono come root per la topologia. Il risultato è un grafo orientato aciclico che è suddiviso in uno o più DAG orientati (DODAG), un DODAG per ogni root. Se il DAG ha radici multiple, allora avrà una dorsale comune. Ogni DODAG è univocamente identificato dalla coppia Instance ID e DODAG ID. RPL utilizza quattro valori per identificare e mantenere una topologia di DODAG, i quali sono RPL instance ID, DODAG ID, DODAG version, Rank. La versione di un DODAG viene stabilita dal nodo radice, e non può essere modificata da nessun nodo. I genitori, contenuti nel *parent set* di un nodo devono appartenere alla stessa versione di DODAG del nodo. Per scelta amministrativa, o periodicamente, il DODAG version viene aggiornato. Quando ciò avviene, la root invia un messaggio DODAG Information Object (DIO) con la versione aggiornata. Un nodo appartenente a quel DODAG, quando riceve il messaggio con la versione aggiornata può decidere se abbandonare quel grafo, oppure rimanere associato aggiornandone la versione. Nel caso in cui il nodo decide di rimanere associato, esso resetta il proprio parent set e la routing table. La scelta periodica di incrementare la versione viene fatta per mantenere aggiornate le informazioni sulle rotte possedute dai singoli nodi (nel caso di funzionamento in modalità non-storing) oppure per aggiornare le informazioni possedute dalla radice (nel caso di funzionamento in modalità storing). Le istanze di RPL (che sono indipendenti l'una dall'altra) sono

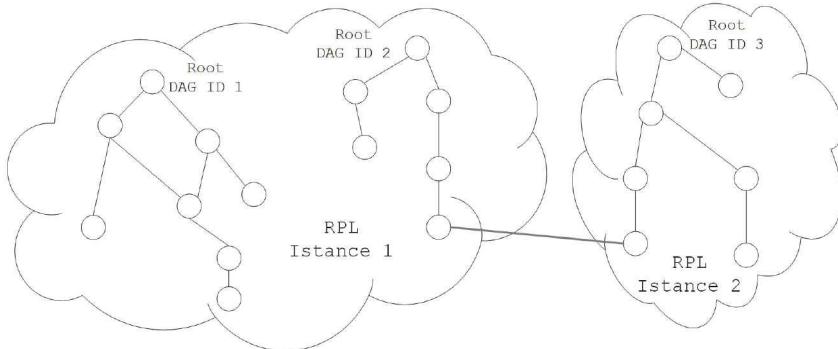


Figura 13.10: DODAG formati da RPL

un insieme di DODAG, indipendenti tra di loro. Ogni DODAG ha una propria versione e un proprio ID. Un nodo può appartenere a DODAG differenti se fanno parte di istanze diverse, ma deve appartenere a un solo DAG all'interno di ciascuna istanza come mostrato in figura 13.10. RPL supporta tre diversi tipi di traffico: multipoint-to-point (MP2P) da molti a uno; point-to-multipoint (P2MP) da uno a molti; point-to-point (P2P) da uno a uno.

Rank

Le scelte di un nodo si basano sul valore del proprio rango e da quello dei suoi vicini. In generale tutta la struttura topologica DODAG è mantenuta coerente sulla base di confronti fatti su tale parametro. Come è stato detto all'inizio del paragrafo il *Rank* è calcolato dalla OF e rappresenta la posizione del nodo all'interno di una versione del DODAG. Esso non va inteso come il costo del percorso anche se la OF può tenere conto di tali parametri. Il rank può essere pensato come un numero in virgola fissa, in cui la parte intera e la parte frazionaria sono determinati dal *MinHopRankIncrease*. Il parametro *MinHopRankIncrease* viene stabilito dalla DODAG root ed è definito nel campo *DODAG Configuration* e in sostanza stabilisce la differenza minima che ci deve essere tra il rango di un nodo ed il suo genitore. *MinHopRankIncrease* crea un compromesso tra il costo di un salto e il numero massimo di salti che una rete può supportare. Esso viene valutato secondo la formula:

$$DAGRank(rank) = \left\lfloor \frac{rank}{MinHopRankIncrease} \right\rfloor \quad (13.1)$$

Una OF calcola il rango di un nodo per confronto, aggiungendo al rango del candidato un valore che rappresenta la posizione relativa del nodo e del candidato. L'aumento del rango deve essere di almeno il valore *MinHopRankIncrease* ed ha la proprietà di essere strettamente monotono:

- crescente lungo le *Downward routes*;

- decrescente lungo le *Upward routes*.

Per ogni coppia di nodi M ed N si hanno le seguenti relazioni:

- $DAGRank(M) < DAGRank(N)$: il nodo M si trova più vicino alla DODAG root rispetto ad nodo N . Il nodo M può essere un genitore di N senza rischiare di creare cicli nel DODAG e mantenere coerente la struttura topologica;
- $DAGRank(M) = DAGRank(N)$: la posizione del nodo M ed N rispetto alla DODAG root sono da considerarsi simili o identiche. In questo caso l'instradamento verso un nodo con rango uguale può generare dei cicli;
- $DAGRank(M) > DAGRank(N)$: la posizione del nodo M è più lontana dalla DODAG root rispetto alla posizione del nodo N .

13.8.1 Messaggi di controllo RPL

RPL per creare e gestire i percorsi verso ogni nodo, sfrutta i pacchetti di controllo ICMPv6. Essi sono costituiti da un'header (suddiviso in 3 campi specifici), seguiti dal corpo del messaggio e da un campo di eventuali opzioni. Il formato del pacchetto è mostrato in figura 13.11. Il campo Type, nel messaggio di controllo RPL, assume il valore 155.

Il campo Code può assumere diversi valori, a seconda del tipo di messaggio trasportato ed identifica il tipo di Control Message RPL. Il campo Base avrà valori relativi ai parametri di informazione. I codici di controllo di RPL sono:

- 0x00: DIS
- 0x01: DIO
- 0x02: DAO
- 0x03: DAO Acknowledgment (DAO-ACK)
- 0x80: Secure DODAG Information Solicitation
- 0x81: Secure DODAG Information Object
- 0x82: Secure Destination Advertisement Object

Type (8 bit)	Code (8 bit)	Checksum (16 bit)
Base		
Option(s) ...		

Figura 13.11: Struttura del pacchetto di controllo RPL

- 0x83: Secure Destination Advertisement Object Acknowledgment
- 0x8A: Consistency Check

I messaggi di controllo hanno una visibilità link. L'indirizzo sorgente ha indirizzo unicast link-local, e l'indirizzo di destinazione o è un indirizzo multicast oppure è un indirizzo unicast link-local. L'unica eccezione è rappresentata dai messaggi DAO/DAO-ACK, i quali vengono scambiati usando indirizzi unicast su più hop. Ogni messaggio RPL ha una variante di sicurezza. Se essa è abilitata (campo Code settato a 0x8*), i messaggi RPL hanno un formato differente, ovvero hanno il campo aggiuntivo Security prima del campo Base. La riservatezza dei messaggi inizia dal primo byte dopo il campo di sicurezza e continua fino all'ultimo byte del pacchetto. Il messaggio di Consistency Check è utilizzato per controllare la consistenza delle chiavi di sicurezza dei messaggi in modalità sicura.

Per maggiori informazioni sui valori e i significati dei vari campi, si può fare riferimento al documento RFC 6550.

RPL prevede l'inoltro di tre tipi di messaggi:

- Messaggio DODAG Information Object (DIO): viene utilizzato per la formazione e il mantenimento dei cammini verso il nodo radice (Upward Route, ovvero rotte verso l'alto). Se il messaggio DIO viene usato per formare un cammino, le informazioni presenti nel campo Base permettono a un nodo di scoprire un'istanza e di apprenderne i corrispondenti parametri di configurazione. Se, invece, il messaggio viene usato per conservare un cammino, i parametri presenti nel campo Base permettono l'identificazione di un insieme di nodi nel DODAG tra i quali il nodo mittente può scegliere un genitore e mantenere la rotta.
- Messaggio di DODAG Information Solicitation (DIS): può essere utilizzato per sollecitare un l'invio di un pacchetto DIO da un altro nodo al fine di verificare l'esistenza di nodi vicini. Un nodo può utilizzare il messaggio DIS per sondare i DODAG nelle sue vicinanze.
- Messaggio Destination Advertisement Object (DAO): è utilizzato per costruire i cammini dal nodo radice verso gli altri nodi appartenenti al DODAG (Downward Route). Viene inviato in modalità unicast dal figlio a tutti i suoi genitori. Il messaggio DAO può essere optionalmente confermato dal genitore inviando in risposta un pacchetto DAO-ACK al suo figlio.

A seconda del messaggio inoltrato, il campo Base avrà uno specifico formato. Inoltre è previsto un messaggio di ACK che viene inviato da un destinatario di un messaggio DAO in risposta allo stesso: questo messaggio è chiamato DAO-ACK.

13.8.2 Funzionamento del protocollo RPL

RPL prevede quattro modi di funzionamento:

- Senza conservazione delle rotte;

- Modalità Non-Storing: tutti i pacchetti inviati vengono inviati alla radice che è l'unica a mantenere le rotte;
- Modalità Storing senza Multicast: ogni nodo mantiene le rotte, ma non gli è permesso utilizzare indirizzi multicast;
- Modalità Storing con Multicast: ogni nodo mantiene le rotte ed è permesso l'uso di indirizzi multicast.

Nella modalità non-storing la scoperta e il mantenimento delle rotte è tutta a carico della root. Questa modalità, infatti, è consigliata in reti dove sono presenti nodi con limitate capacità di memoria e di calcolo. Si deve comunque notare che, in questo caso, un messaggio, rispetto alla modalità storing, impiega più tempo per arrivare a destinazione. Nella modalità storing, sia senza sia con multicast, la gestione delle rotte è spostata molto sui nodi, riducendo così il traffico da e verso la root. I messaggi inviati in modalità storing seguono un percorso più breve all'interno del DODAG per raggiungere una certa destinazione.

13.8.3 Inserimento in un DODAG e gestione delle rotte

Inserimento

Un nodo, appena viene connesso alla rete, cerca di entrare a far parte di una versione di un DODAG. Quindi invia un messaggio DIS ai nodi adiacenti i quali risponderanno con un messaggio DIO specificando le informazioni del DODAG a cui appartengono (esse verranno specificate nell'opzione DODAG Configuration). La scelta del DODAG è fatta su base amministrativa in base al campo DODAG Preference dei messaggi DIO ricevuti. Una volta scelto il DODAG, il nodo calcolerà il suo rango (che aumenta mano a mano che ci si allontana dalla root) in base all' OF in uso nel DODAG scelto. Tra i nodi vicini (ovvero nodi raggiungibili direttamente) esso ne seleziona alcuni, e li elegge suoi nodi genitori (nodi parent). Tra questi nodi esso ne sceglie uno, il quale diventerà il suo parente preferito (prefered parent). La scelta viene fatta in base al rango posseduto dai nodi parent. Il rango viene calcolato in base alle OF, che a loro volta sono valutate in base alla metrica scelta, quindi, il parent preferito risulta quello con la metrica migliore. Se un nodo decide di entrare a far parte di un DODAG, ma non ne supporta le modalità di funzionamento, esso sarà inserito come una foglia. In questo caso particolare il rango sarà infinito (0xFFFF). Tale nodo non potrà inviare messaggi DIO, ma solo messaggi DAO. Un nodo può anche decidere di abbandonare il DODAG di cui faceva parte. La scelta può avvenire su base amministrativa oppure perché il nodo non rispetta il vincoli sul rango imposti nel DODAG. La dissociazione avviene inviando un messaggio DIO (con campo rank settato a 0xFFFF) ai suoi vicini e cancellando le tabelle di routing e il parents set. Una volta uscito dal DODAG, il nodo cercherà di rientrare in un altro grafo. L'inserimento è mostrato in figura 13.12.

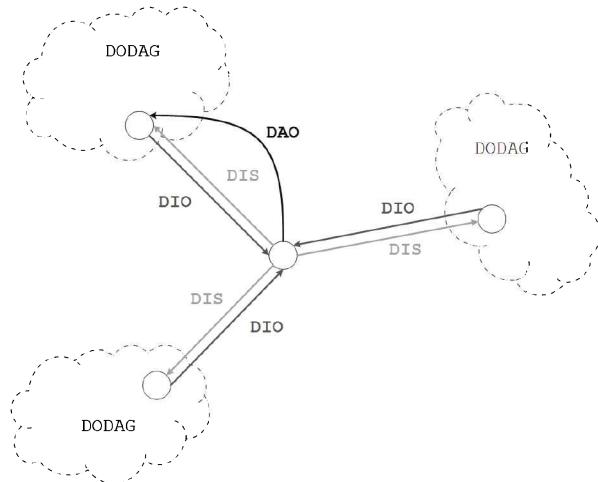


Figura 13.12: Ingresso di un nodo in un DODAG

Creazione e gestione dei cammini verso il nodo radice

I cammini possono essere creati (e mantenuti) verso il nodo radice (upward route) tramite l'invio dei pacchetti DIO tra i nodi. I campi del pacchetto G, MOP, prf, Version, RPL Instance ID, DODAGID sono definiti dal nodo radice e i nodi che ricevono il messaggio devono adottare una configurazione consona con i parametri inseriti nei campi e inoltrarli ai figli, inalterati. Ogni nodo che riceve un messaggio DIO può aggiornare solo i campi Rank e DSTN. Per creare e mantenere le upward route ogni nodo mantiene la *parents set*. In questa tabella sono presenti tutti i nodi genitori (ovvero nodi con rango minore rispetto al proprio, quindi più vicini alla radice). Per mantenere i percorsi, il nodo radice invia periodicamente i messaggi DIO a tutti i nodi direttamente collegati, i quali poi inoltreranno il messaggio ai loro figli. Il periodo di invio è variabile e regolato dal trickle time. Il trickle time è un algoritmo basato sulle consistenze e inconsistenze rilevate nel grafo. Le consistenze avvengono quando il rango è rispettato, ovvero quando un nodo parent ha rango minore del nodo figlio. Due nodi figli possono avere lo stesso rango, ma esso deve essere necessariamente maggiore del nodo genitore. Le inconsistenze avvengono quando questa condizione non viene rispettata. I messaggi DIO vengono inviati ogni qual volta le consistenze rilevate sono sotto una determinata soglia. Il funzionamento è mostrato in figura 13.13 (a).

Creazione e gestione dei cammini dal nodo radice

La creazione e la gestione dei percorsi dalla radice verso le foglie (downward route) avviene mediante l'uso dei pacchetti DAO che sono inviati verso il nodo radice con l'aggiunta di due opzioni: la Transit Information Option e una, o più, RPL Target Option. I messaggi DAO e le sue opzioni vengono inviati da ogni

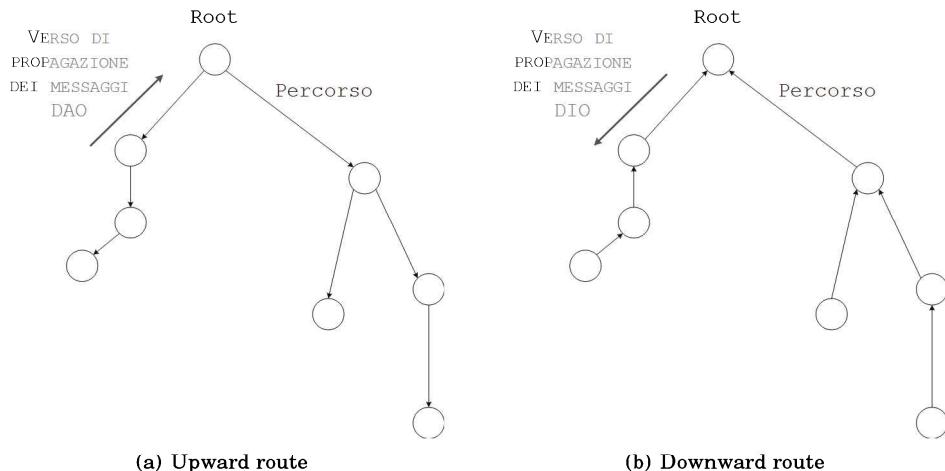


Figura 13.13: Creazione e gestione nelle due modalità

nodo alla radice specificando quali sono i suoi DAO parent (il next-hop per il pacchetto verso l'alto). Nella modalità non-storing la radice crea le downward route in base alle informazioni ricevute. I nodi intermedi (ovvero quelli che ricevono e ritrasmettono verso la radice il messaggio DAO), non tengono alcuna traccia delle informazioni presenti nel messaggio, ma aggiungono solo un'opzione RPL target. Nella modalità storing i messaggi DAO vengono inviati da ogni nodo a tutti i suoi DAO parents, specificando quali nodi sono presenti nei suoi sub-DODAG (è un sotto albero con radice il nodo in questione). In questa modalità i nodi costruiscono le downwardroute valutando le informazioni presenti nel messaggio DAO, scartando poi il messaggio. In questo modo, ogni nodo è a conoscenza dei nodi che lo seguono nel grafo (ovvero quei nodi con rango maggiore, quindi più lontani dalla radice, ma più vicini alle foglie dell'albero). I messaggi DAO vengono inviati o automaticamente, ogni qual volta un DAO parent viene aggiunto o rimosso dal parents set, oppure, su richiesta di un DAO parent. Per non sovraccaricare troppo la rete, RPL utilizza un timer per l'invio dei messaggi DAO. Quando si verifica un evento tale da richiedere l'inoltro di un messaggio DAO, il nodo aspetta un tempo delay-DAO prima di inviarlo. Prima della scadenza di questo tempo, il nodo non può inoltrare nessun messaggio DAO. Il funzionamento è mostrato in figura 13.13 (b).

13.9 Letture Consigliate

Per approfondire gli argomenti trattati in questo capitolo si consiglia:

Y. Dalal, R. Metcalf, Reverse Path Forwarding for Broadcast Packets, ACM Commun., 1978.

J. Moy, Multicast Routing Extetention for OSPF, ACM Commun., 1994.

M. Schwartz, Broadband Integrated Networks, Prentice Hall, 1996.

F. Halsall, Reti di Calcolatori e Sistemi Aperti, Addison-Wesley, 1996.

W. Stalling, High Speed Networks, Prentice Hall, 1998.

W. Stalling, "Trasmissione Dati e Reti di Computer", Jackson, 2000.

B.A. Forouzan, "Reti di Calcolatori ed Internet", McGraw-Hill, 2007.

A.S. Tanenbaum, D.J. Wetherall, "Reti di Calcolatori", Pearson, 2011.

J.F. Kurose, K. W. Ross, "Reti di Calcolatori e Internet", Pearson, 2013.

<http://en.wikipedia.org/wiki/Bellman-Ford>

http://en.wikipedia.org/wiki/Dijkstra's_algorithm

Si consiglia inoltre per approfondimenti e complementi specifici relativi alle tecniche, alle metodologie e alle metriche previste per i vari algoritmi di routing presentati di consultare i documenti RFC citati nel testo.

14

Controllo della congestione

Il controllo della congestione è una funzionalità propria delle reti di telecomunicazioni utilizzate per collegamenti dati (reti di calcolatori) che ha come obiettivo quello di prevenire, o limitare, perdite eccessive di prestazioni sia in termini di ritardo di trasferimento dei flussi informativi sia in utilizzo (throughput) dei collegamenti stessi. L'analogia comune che si cita per riportare il fenomeno della congestione di una rete ad una situazione propria della nostra vita comune è quello di un tratto autostradale che collega due grandi aree metropolitane. In condizioni normali, il traffico scorre veloce ed i tempi di percorrenza restano contenuti. Viceversa se sull'autostrada, ad esempio in certi periodi particolari (es.: esodo estivo), si immettono un numero eccessivo di auto, il traffico viene rallentato ed i tempi di percorrenza aumentano fino a rendere preferibile seguire precorsi alternativi. In una rete di calcolatori la congestione si manifesta quando il numero di pacchetti inviati è talmente elevato da saturare tutte le capacità di trasporto dei collegamenti e da sovraccaricare eccessivamente le operazioni nei nodi di transito. Sotto queste condizioni la rete non offre più un servizio adeguato ed i pacchetti, ammesso che sia possibile inviarli, vengono inoltrati molto lentamente. Attivare procedure per evitare o contenere la congestione di una rete non è compito esclusivo di uno solo livello dell'architettura della rete ma interessa può interessare più livelli (es.: livello collegamento, rete e trasporto), ovviamente con diverse modalità attuative. In questo capitolo affronteremo il problema del controllo della congestione in una rete a commutazione di pacchetto considerando le principali metodologie utilizzate a livello trasporto, per prevenirla, contenerla o, addirittura, risolverla quando questa si manifesta.

14.1 Generalità

In una rete a commutazione di pacchetto o, più in generale, in una rete di calcolatori la congestione si verifica quanto i collegamenti tra i dispositivi e i nodi della

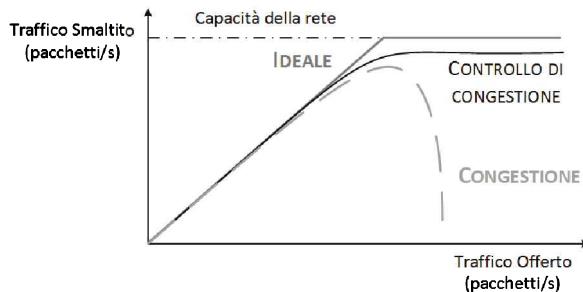


Figura 14.1: Congestione in una rete

rete sono sollecitati, in termini di pacchetti da trasmettere, in maniera eccessiva rispetto alle capacità nominali. La congestione può tuttavia anche avere origini interne alla rete ad esempio a causa di nodi che manifestano funzionamenti anomali. In generale, comunque, l'effetto della congestione è un progressivo decadimento delle prestazioni della rete. Quando la congestione si manifesta nei nodi della rete (router) questa viene individuata dal livello rete tuttavia, la situazione più frequente si ha quando la congestione è determinata da un eccessivo invio di pacchetti in un collegamento ed in questo caso il compito di controllarla è del livello trasporto. La modalità tipica che si adotta è quella di rallentare il tasso di inoltro dei pacchetti fino ad interromperlo quando i sintomi della congestione si manifestano. La figura 14.1 illustra come il traffico smaltito da un collegamento varia in funzione del traffico inviato. L'andamento *ideale* si riferisce ad una rete immaginaria per la quale ad un aumento del traffico offerto corrisponde un uguale aumento del traffico smaltito fino al raggiungimento della capacità massima del collegamento. La curva più in basso nella figura (*congestione*) si riferisce ad una rete per la quale non sono stati adottati meccanismi di controllo della congestione. In questo caso si può notare un andamento iniziale sovrapposto a quello *ideale* dopodiché, una volta che il traffico offerto supera un certo rate, l'aumento del traffico smaltito non segue più fedelmente l'aumento del traffico offerto. Lo scostamento per difetto è dovuto alla perdita dei pacchetti che, superando i limiti per il ritardo di consegna dovuti ad un loro eccessivo rallentamento, vengono scartati dai nodi che rilevano questa condizione oppure perché, arrivando ad un nodo congestionato, vengono rifiutati per mancanza di spazio di memoria nei buffer di attesa (code). Se non si attuata nessuna politica di controllo ai nodi finalizzata a limitare l'invio di nuovi pacchetti, la rete, come mostrato in figura, può collassare (il traffico smaltito tende ad annullarsi). La curva intermedia (con *controllo di congestione* evidenza invece l'efficacia dei meccanismi di controllo della congestione che tende a portare le prestazioni di una rete reale quanto più prossime ad un comportamento ideale.

In questo capitolo ci occuperemo di metodi per il controllo della congestione di tipo *proattivo* e *reattivo* che operano a livello trasporto (Kurose'2013, Stalling'2000, Forouzan'2007 in paragrafo 14.4).

14.2 Controllo Proattivo

I metodi per il controllo della cogestione di tipo *proattivo* hanno come finalità quella di prevenire la congestione evitando che si manifesti. Questo obiettivo può essere raggiunto con tecniche di :

- *Traffic Shaping* : controllano l'intensità e la frequenza di invio dei pacchetti in un collegamento;
- *Queue management* : si da possibilità ai nodi della rete (router) di eliminare i pacchetti ritenuti in eccesso;
- *Admission Control* : è più propriamente un meccanismo per garantire la qualità di un servizio ma è efficace anche come tecnica preventiva nei riguardi della congestione di una rete. Semplicemente, prima di accettare una connessione, se ne verifica la sostenibilità sia in termini di requisiti di servizio richiesti (es. : ritardo) sia in termini di influenza (variazione) su diritti di accesso già riconosciuti ad altri flussi. Questa metodologia può prevedere anche una fase di *negoziazione* nel caso in cui i requisiti di servizio richiesti non siano compatibili con le disponibilità della rete.

Di seguito descriveremo più nel dettaglio due tecniche afferenti alla classe dei metodi *Traffic Shaping*. Nello specifico saranno considerate le tecniche *leaky bucket* (secchio bucato) e *token buket* (secchio dei gettoni). Entrambi i metodi sono riferiti al principio *rate based* ed implementano un controllo di congestione mediante un meccanismo che agisce sulla frequenza (rate) di inoltro dei pacchetti nel collegamento d'interesse.

14.2.1 Leaky Bucket

Il metodo *leaky bucket* prende il nome dal principio ispiratore del *secchio bucato*.



Figura 14.2: Principio del secchio bucato

A tutti sarà capitato di utilizzare un imbuto per riempire di un liquido un altro recipiente come illustrato in figura 14.2. Indipendentemente dall'intensità del flusso in ingresso all'imbuto, ad esempio acqua proveniente da un rubinetto, il liquido esce dall'altra estremità con una intensità costante che non dipende

da quella in entrata (rubinetto). Ovviamente il liquido continua ad uscire fino a quanto l'imbuto non si vuota e può anche, se l'intensità in ingresso diventa eccessiva rispetto alla capacità di uscita, fuoriuscire dall'imbuto (tracimazione).

Questo principio, mutuato nel contesto di una rete a commutazione di pacchetto, presuppone di utilizzare un meccanismo opportuno per evitare che un afflusso eccessivo di pacchetti per un collegamento ne provochi la congestione (tracimazione) cioè renda tutti gli apparati di rete coinvolti non più in grado di rispettare fissati requisiti di servizio, sia per il traffico smaltito (throughput), sia per i valori del ritardo con cui i pacchetti arrivano alla loro distinzione finale. Lo schema di riferimento per il meccanismo *leaky bucket* è illustrato in figura 14.3.

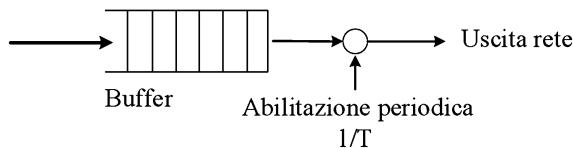


Figura 14.3: Tecnica Leaky Bucket

I pacchetti relativi al collegamento d'interesse non vengono trasmessi immediatamente ma sono invece inseriti in un buffer, rispettandone l'ordine di generazione (accodamento FIFO). I singoli pacchetti sono successivamente prelevati dal buffer secondo l'ordine di inserimento ed inviati nel collegamento con una cadenza fissata corrispondente alla frequenza di arrivo delle autorizzazioni (es.: possibilità di accesso 10 Mbit ogni 2 ms). In questo modo i pacchetti, conseguenti a picchi di traffico in ingresso (arrivo di un blocco di pacchetti molto numeroso), vengono distribuiti su un adeguato intervallo di tempo in modo che la frequenza di inoltro nel collegamento rimanga costante e congruente con il limite prefissato (eventualmente negoziato nella fase di richiesta del collegamento) in maniera da evitare la congestione.

Questo meccanismo consente di garantire che la frequenza massima di inoltro dei pacchetti in un collegamento non superi mai il valore di riferimento (controlla il rate di picco). Quando i pacchetti arrivati non trovano spazio nel buffer vengono scartati (è un controllo indiretto della congestione) così come se viene riconosciuto il diritto di trasmissione di un pacchetto ed il buffer è vuoto l'opportunità viene perduta (non è possibile garantire all'utente un rate medio di riferimento).

14.2.2 Token Bucket

Il meccanismo leaky bucket è penalizzante quando l'attività di accesso ha spiccate caratteristiche di intermittenza temporale. In questo caso si perdono le opportunità di accesso quando il buffer è vuoto e si rallenta lo smaltimento dei picchi di pacchetti in quanto l'inoltro nel collegamento deve sempre avvenire ad una frequenza costante (Kurose'2013, Comer'2006, Halsall'2005 in 14.4). Questo inconveniente viene eliminato con la tecnica *token bucket* che permette di conservare le autorizzazioni (token) all'inoltro di pacchetti non utilizzate che arrivano

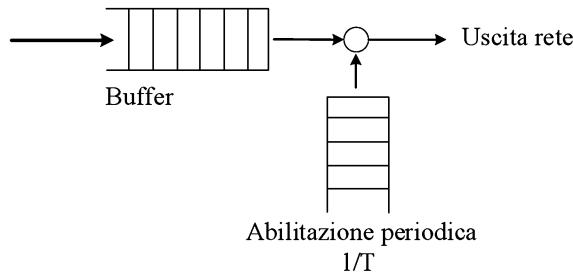


Figura 14.4: Tecnica Token Bucket

con una frequenza fissa e costante. Le autorizzazioni non usate vengono conservate in un buffer (bucket) che funge da deposito. La trasmissione di un pacchetto comporta l'utilizzo di una autorizzazione. I pacchetti arrivati a gruppi possono quindi essere inoltrati sequenzialmente rispettando il loro ordinamento fino a quando nel deposito sono presenti permessi. I pacchetti che arrivano e non hanno permessi di accesso disponibili, vengono inseriti nel buffer di arrivo secondo la disciplina FIFO. La figura 14.4 illustra schematicamente l'implementazione di questa modalità di funzionamento.

La capacità del buffer delle autorizzazioni (token), cioè il numero massimo di token che possono essere conservati come credito per accessi futuri, è in generale limitato per evitare una monopolizzazione eccessiva del collegamento da parte di un nodo. In questo caso se una autorizzazione arriva e trova il deposito pieno viene perduta.

Supponendo che il buffer (deposito) delle autorizzazioni abbia una capacità uguale a K (autorizzazioni), che sia esaurito (pieno) e che la frequenza di arrivo delle autorizzazioni sia ρ (autorizzazioni/s), il numero massimo Γ di pacchetti che possono essere inoltrati in queste condizioni è (Forouzan'2007 in 14.4) :

$$\Gamma = K + \rho t \quad (14.1)$$

a cui corrisponde una massima frequenza media di inoltro data da :

$$\nu = \frac{K + \rho t}{t} \quad (14.2)$$

Come si può facilmente dedurre dalle (14.1) e (14.2) in relazione alla capienza del deposito delle autorizzazioni (buffer) e alla frequenza di arrivo delle stesse il meccanismo *token bucket* controlla, limitandola superiormente, la velocità di inoltro dei pacchetti nel collegamento.

Gli obiettivi distinti di salvaguardare i nodi con sporadiche necessità di accesso e di limitare il traffico di picco inoltrato in un collegamento, perseguiti individualmente dalle due tecniche prima esaminate, possono essere considerati in un'ottica combinata mediante l'impiego congiunto di uno schema *leaky bucket* e uno schema *token bucket*. In questo caso il sistema *leaky bucket* deve essere collegato in cascata al un sistema *token bucket* e la frequenza di arrivo delle autorizzazioni per il sistema *leaky bucket* deve essere superiore a quella di arrivo delle autorizzazioni al sistema *token bucket*.

14.3 Controllo reattivo

I metodi per il controllo della congestione con modalità reattiva hanno come obiettivo di risolvere la congestione mediante determinate azioni non appena questa si è verificata ed è stata rilevata. Come per la famiglia delle tecniche di tipo proattivo, anche in questo caso, esistono diverse alternative. Nel seguito verrà fornita la descrizione funzionale di uno dei metodi più diffusi appartenenti a questa classe: il metodo *Sliding Window* (a finestra scorrevole) (Tanenbaum'2011 in 14.4).

14.3.1 Sliding Window

Questa tecnica serve per controllare l'inoltro di pacchetti in una rete che fornisce un collegamento end-to-end affidabile (con riscontro della ricezione, non necessariamente anche dell'integrità del pacchetto). Ogni pacchetto è etichettato con un numero univoco di sequenza che ne permette l'identificazione senza ambiguità sia per trasferirlo, rispettando l'ordine di generazione, alla destinazione finale sia per poterne notificare la corretta ricezione al nodo sorgente. Questo metodo richiede la definizione di un parametro WL detto *ampiezza della finestra* che rappresenta il numero di pacchetti che possono essere trasmessi in sequenza (senza interruzione) nel collegamento. Il parametro WL è definito in modo che prima della conclusione della trasmissione di tutti i pacchetti contenuti nella finestra

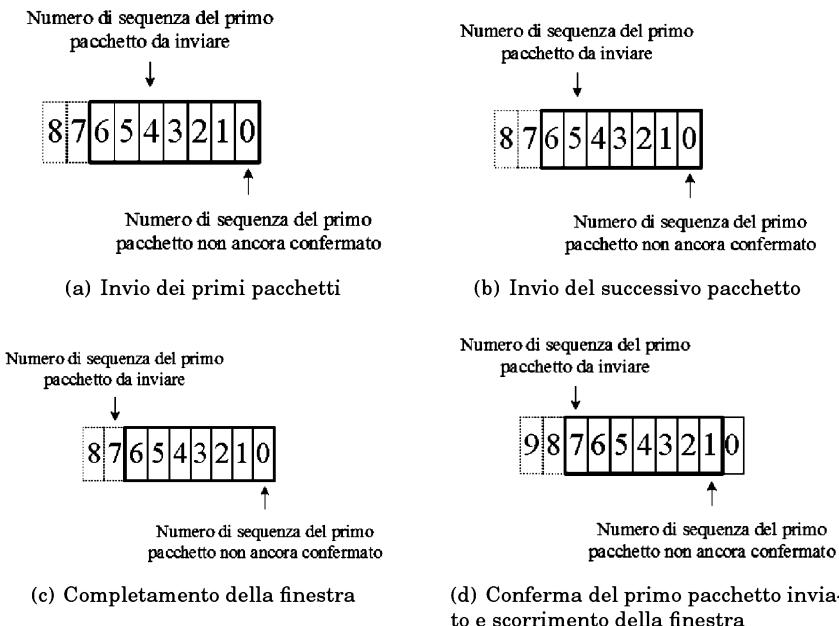


Figura 14.5: Meccanismo a finestra scorrevole

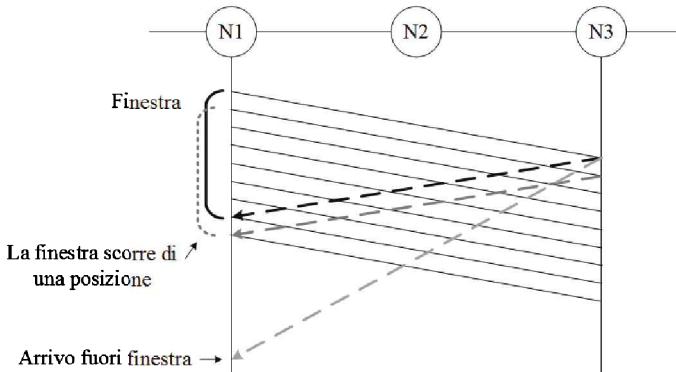


Figura 14.6: Arrivo dei riscontri

al nodo sorgente sia pervenuto il messaggio di notifica (riscontro) dell'avvenuta ricezione almeno del primo pacchetto della sequenza. Quando questo accade, il nodo sorgente fa scorrere la finestra in avanti di una posizione e procede alla trasmissione del pacchetto successivo all'ultimo compreso nella finestra. Allo stesso tempo si pone in attesa della ricezione del messaggio di riscontro relativo al nuovo capofila della sequenza.

La figura 14.5 illustra schematicamente il funzionamento del metodo *sliding window*.

Se la rete non presenta criticità riguardo la congestione, il processo di scorrimento della finestra e inoltro dei pacchetti evolve in maniera regolare, se, invece, questo non accade si attiva il meccanismo di risoluzione della congestione. Riprendendo l'analogia del rubinetto che versa acqua in un imbuto, questo si concretizza con una regolazione del rubinetto stesso, cioè, nel nostro caso, si limita la frequenza di invio di nuovi pacchetti in maniera da facilitare lo smaltimento dell'affollamento dei pacchetti già presenti nel collegamento e quindi consentire il ripristino di un funzionamento corretto. Nello specifico, la congestione viene riconosciuta perché il tempo di riscontro del primo pacchetto della finestra esce dall'ampiezza temporale della finestra stessa (figura 14.6).

Questo evento provoca la *chiusura della finestra*, in altri termini non si procede alla trasmissione di un nuovo pacchetto fino a quanto non arriva il riscontro del capofila. Ovviamente, più lungo è il tempo di attesa, maggiore è la riduzione della frequenza di invio. La figura 14.7 mostra la regolazione della frequenza di inoltro dei pacchetti in funzione del ritardo di riscontro (congestione).

Come si può vedere in figura 14.7 la frequenza di inoltro si mantiene uguale a quella nominale fino a quando il ritardo nel ricevere il riscontro rimane compreso nel tempo di finestra. Viceversa, quando il ritardo di riscontro esce dalla finestra, si ha un decadimento iperbolico che asintoticamente tende ad azzerare la frequenza di inoltro dei pacchetti.

Da questa figura se ne deduce che il meccanismo a finestra non garantisce all'utente una frequenza minima (rate) di inoltro dei pacchetti (questa può perfino, in condizioni particolarmente critiche, annullarsi).

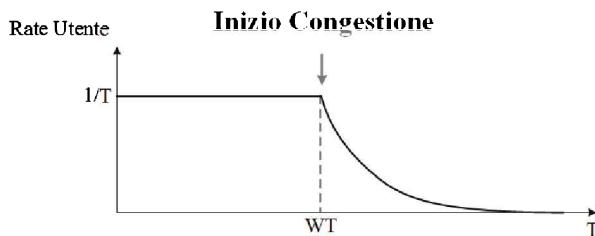


Figura 14.7: Regolazione della frequenza di inoltro dei pacchetti.

14.3.2 Un caso pratico: Controllo della congestione in TCP

Il protocollo TCP impone ad ogni nodo che invia pacchetti nella rete un limite alla frequenza di inoltro determinato in relazione al livello di congestione percepito della rete. Limitiamo la discussione presentata in questo paragrafo alla sola modalità adottata da TCP per implementare un controllo della congestione con il metodo della *finestra scorrevole* (Kurose'2013, Forouzan'2007, Tanembaum'2011 in 14.4). In generale, questa tecnica viene implementata dando al dispositivo sorgente la possibilità di modificare la frequenza di inoltro dei pacchetti sia in relazione al livello di congestione della rete e sia delle condizioni di ricezione (congestione al dispositivo di destinazione). Per il caso di nostro interesse, la sorgente può aumentare la frequenza di inoltro (aumentando le dimensioni della finestra) quando si accorge che la rete è interessata da un traffico scarso (rete scarica) oppure ridurla quando, viceversa, viene rilevata la presenza di congestione (riduzione della finestra). Il meccanismo di regolazione della frequenza di inoltro, agendo sulle dimensioni della finestra, viene attivato tramite i messaggi di riscontro ricevuti ed è detto *self-clocking* (auto-temporizzato). Le modalità di variazione delle dimensioni della finestra sono sostanzialmente tre:

- **Slow Start** : durante la fase di instaurazione del collegamento le dimensioni della finestra alla sorgente sono fissate ad un valore di riferimento convenzionale (es.: 1 pacchetto). Naturalmente si ha tutto l'interesse ad inoltrare i pacchetti nel collegamento secondo la massima frequenza di invio consentita senza provocare congestione. La sorgente non può, a priori, conoscere questo valore e quindi lo deve scoprire da sola attraverso un procedimento di autoapprendimento che consiste nell'aumentare di un'unità l'ampiezza della finestra per ogni pacchetto riscontrato entro il tempo di finestra (time-out) fino a quando questa condizione non viene violata per la prima volta (es: se i due pacchetti della finestra vengono entrambi riscontrati correttamente la finestra viene portata al valore 4). Non appena si rileva un riscontro fuori finestra, si fissa un valore target massimo delle dimensioni della finestra pari alla metà del valore raggiunto. Si inizia di nuovo la fase di *slow start* (impostando di nuovo la dimensione minima della finestra) per verificare che il valore limite della finestra sia compatibile con la congestione della rete (non si rilevano ricezioni di riscontri fuori della finestra). Si deve notare che contrariamente alla sua definizione di

"*partenza lenta*" con il meccanismo di *slow start* la frequenza di inoltro dei pacchetti viene raddoppiata se non ci sono problemi di congestione e quindi la finestra cresce in modo esponenziale.

- **Congestion avoidance** : terminata la fase di *slow start* il TCP entra nello stato di *congestion avoidance*. Le dimensioni della finestra sono di conseguenza fissate a metà del valore che ha fatto rilevare la congestione. Durante questa fase, al fine di prevenire l'insorgere della congestione, viene utilizzato un metodo più conservativo per modificare le dimensioni della finestra: ogni volta che tutti i pacchetti della finestra sono riscontrati correttamente, la dimensione della stessa viene incrementata di un pacchetto. In questo modo l'incremento delle dimensioni della finestra avviene in modo lineare. Se un riscontro di un pacchetto avviene fuori finestra la procedura di *congestion avoidance* si comporta come la *slow start* imposta cioè il valore massimo della finestra uguale a metà del valore assunto al verificarsi della congestione. In sintesi questa modalità presuppone un incremento lineare delle dimensioni della finestra quando la congestione non è rilevata ed un decremento esponenziale quando, viceversa, questa viene percepita.
- **Fast recovery** : è prevista nella versione TCP Reno e consente di distinguere la situazione di una congestione più lieve da una condizione più critica. Un pacchetto viene ritrasmesso o perché il suo time-out è scaduto o perché sono arrivati tre riscontri duplicati (cioè sono arrivati riscontri di pacchetti trasmessi successivamente al pacchetto di cui non si hanno notizie). Ovviamente la situazione di superamento del time-out è maggiormente indicativa di uno stato di congestione critico della rete (nel caso di una congestione effettiva i riscontri duplicati non possano arrivare). Di conseguenza la fase di *fast recovery* prevede l'inizio di una nuova fase di *slow start* con finestra di riferimento massima di valore metà rispetto a quello relativo alla rilevazione della congestione critica oppure, pur ridefinendo il valore di riferimento della finestra uguale alla metà di quello relativo alla rilevazione di una congestione lieve, si passa ad una nuova fase di *congestion avoidance*. Questa prevede una modalità temporanea relativa al tempo di attesa per ricevere il riscontro del pacchetto perduto durante la quale l'incremento lineare viene attivato sulla base della ricezione di riscontri duplicati. Appena viene ricevuto il riscontro del pacchetto perduto la procedura *fast recovery* viene abbandonata e si torna alla modalità base *congestion avoidance*.

In letteratura la procedura di controllo della congestione descritta in precedenza è nota come tecnica AIMD (Additive-Increment Multiplicative-Decrement).

14.4 Letture Consigliate

Il controllo della congestione è trattato in maniera semplice e di facile apprendimento nei testi:

- B.A. Forouzan, Reti di calcolatori ed Internet, McGraw-Hill, 2007.
- A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.
- J.F. Kurose, K. W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.
- W. Stallings, Trasmissione Dati e Reti di Computer, Jackson, 2000.
- M. Schwartz, Telecommunication Networks, Addison Wesley, 1987.
- D.E. Comer, Internetworking con TCP/IP, Pearson, 2006.
- F. Halsall, Networking e Internet, Pearson, 2005.

15

Sicurezza delle reti

La sicurezza in reti di telecomunicazioni riguarda tutte le procedure che, nel loro complesso, consentono un collegamento per lo scambio di informazioni tra persone o dispositivi. Numerose sono le tipologie di attacco e diversi sono i livelli dell'architettura della rete verso i quali possono essere diretti. In questo capitolo ci limiteremo a considerare due principali metodologie per consentire una comunicazione sicura, intendendo con questo termine la possibilità di conoscere con certezza, da parte di persone o dispositivi, che il collegamento è effettivamente quello richiesto, di proteggere le informazioni scambiate da intrusioni esterne e di potere rivelare immediatamente qualsiasi forma di intercettazione. Argomento di questo capitolo è la descrizione di due tecniche di crittografia (cioè di scrittura sicura), che consentono di rendere riservato e confidenziale uno scambio di messaggi tra due dispositivi di una rete. A questo scopo useremo l'analogia con due persone, che chiameremo Alice e Roberto, che vogliono scambiarsi messaggi segreti ed evitare che un ficcanaso, che chiameremo Bob, ne venga a conoscenza. Ovviamente nella realtà di una rete di telecomunicazioni Alice e Roberto possono essere due dispositivi qualsiasi della rete stessa, ad esempio due router che necessitano di condividere le tabelle di instradamento oppure anche applicazioni implementate in modalità distribuita su strutture di elaborazione dell'informazione distinte (grid computing).

15.1 Introduzione

Facciamo riferimento alla figura 15.1 per introdurre i concetti base della sicurezza di rete. Nel caso considerato Alice vuole comunicare solo con Roberto mantenendo riservato il contenuto delle loro conversazioni. I principali requisiti per una *comunicazione sicura* sono (Forouzan'2007, Kurose'2013 nel paragrafo 15.6):

- *Privacy* : Solo il mittente ed il destinatario possono conoscere il contenuto del messaggio scambiato. Per garantire questo requisito si applicano metodologie proprie della crittografia che consistono nel rendere il messaggio non comprensibile a chiunque non sia autorizzato a conoscerlo.
- *Integrità*: questo requisito è comune anche ad altri contesti e si riferisce alla necessità di evitare che il messaggio scambiato subisca alterazioni di contenuto durante la sua trasmissione.

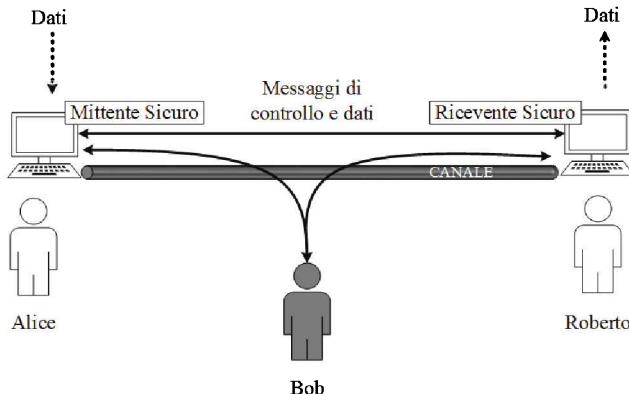


Figura 15.1: Schema di principio: mittente, ricevente e intruso

- *Autenticazione*: si richiede che il mittente e destinatario in un collegamento abbiano reciprocamente certezza della loro identità, cioè devono essere in grado di accertarsi che il corrispondente sia effettivamente chi dichiara di essere.
- *Sicurezza operativa e di apparati*: sia le applicazioni che gli apparati di rete devono avere adeguate protezioni contro intrusioni e manomissioni volte ad alterarne il corretto funzionamento.

15.2 Elementi di crittografia

La crittografia è una metodologia molto antica utilizzata per mascherare i messaggi che si trasmettono al fine di evitare che chiunque non sia autorizzato possa comprenderne il contenuto. Un semplice sistema crittografico è mostrato nella figura 15.2.

Il messaggio nella sua forma originale (per esempio *Ciao Roberto, sono Alice*) è detto **testo in chiaro**. L'operazione che trasforma il messaggio in un **testo cifrato** è detto algoritmo di cifratura. Per attivare la procedura di cifratura Alice deve conoscere un'informazione segreta detta *chiave*. Il messaggio cifrato viene quindi inviato a Roberto in modo sicuro in quanto anche se venisse intercettato da Bob, il suo contenuto sarebbe incomprensibile. In ricezione Roberto, per poter comprendere cosa Alice gli ha comunicato, deve attivare la procedura di decifratura per ripristinare il messaggio nel suo formato originale. Anche questa procedura è attivata sulla base di una informazione segreta detta anche in questo caso *chiave* che può essere un segreto condiviso (chiave simmetrica) oppure no (chiave pubblica). Più propriamente la crittografia si distingue in:

- *Crittografia simmetrica*: La chiave utilizzata dal mittente e dal destinatario è la stessa ed è nota ad entrambi (chiave segreta);

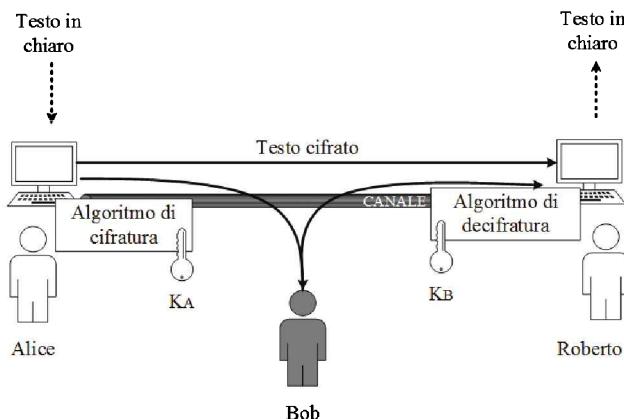


Figura 15.2: Componenti base di un sistema di crittografia

- **Crittografia asimmetrica:** In questo caso sono previste due diverse tipologie di chiave per ogni soggetto (utente):
 - *Chiave pubblica:* è una informazione nota a tutti;
 - *Chiave privata:* è una informazione segreta nota solo al possessore della chiave.

Nel nostro esempio (figura 15.2) Alice per spedire il suo messaggio a Roberto in modo sicuro usa per mascherarlo la chiave pubblica di Roberto. Il messaggio può essere reso comprensibile tramite l'operazione di decifratura attivabile solo sulla base della conoscenza della chiave privata di Roberto e, quindi, solo lui è in grado di comprenderne il significato.

15.3 Crittografia a chiave simmetrica

La cifratura di un messaggio comporta la trasformazione di un messaggio in chiaro (comprensibile) in un messaggio cifrato (incomprensibile). Questo procedimento ha origini molto antiche tanto che un primo esempio pratico di un algoritmo di cifratura a chiave simmetrica si fa risalire al tempo dell'Impero Romano. Si narra infatti che Cesare ne facesse uso per comunicare in modo sicuro con i suoi generali durante le guerre. Il metodo utilizzato è universalmente noto come *cifrario di Cesare*.

Il funzionamento del cifrario di Cesare è semplice ed al tempo stesso molto efficace. In pratica esso prevede la sostituzione di ogni lettera con un'altra sfasata rispetto all'originale di un numero fisso k di posizioni. Il valore di k costituisce l'informazione segreta condivisa tra mittente e destinatario (chiave simmetrica).

Esempio:

Alice vuole inviare il messaggio *Ti amo* a Roberto;

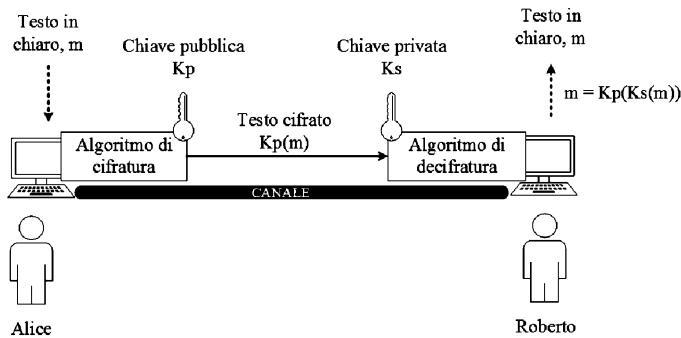


Figura 15.3: Crittografia a chiave pubblica

La chiave simmetrica k ha valore 3;

Il messaggio cifrato diventa :"Wl cpr".

15.4 Crittografia a chiave pubblica (asimmetrica)

Per molto tempo la crittografia è stata sviluppata sulla base di algoritmi a chiave simmetrica che tuttavia presupponeva che le due parti (mittente e destinatario) condividessero in qualche modo un segreto comune in un modo sicuro. La possibilità di inviare messaggi cifrati senza la conoscenza di una chiave condivisa sembrò per molto tempo non praticabile fino a quando fu definito nel 1976 il primo algoritmo di cifratura con scambio di chiavi che ha dato origine, successivamente, allo sviluppo degli attuali algoritmi a chiave pubblica di particolare interesse per procedure di autenticazione e per la firma digitale.

Un sistema di crittografia a chiave pubblica ha un funzionamento relativamente semplice. Riferendoci alla figura 15.3 supponiamo che Alice desideri inviare a Roberto un messaggio che deve rimanere segreto agli estranei. Alice per comunicare con Roberto deve possedere la chiave pubblica, K_p , di Roberto che usa per effettuare la cifratura del proprio messaggio (indicato con m) e quindi produrre il testo cifrato $K_p(m)$. Una volta che Roberto riceve il messaggio cifrato da Alice procede all'operazione di decifratura utilizzando la propria chiave segreta K_s , che solo lui conosce, in maniera da ripristinare il messaggio nel suo formato originale mediante l'operazione $K_s(K_p(m))$.

Il messaggio originale può essere reso comprensibile solo tramite la procedura di decifratura e quindi solo se la chiave segreta di Roberto è nota.

15.4.1 Algoritmo RSA

Questo algoritmo, il cui nome è l'acronimo delle iniziali dei cognomi dei suoi inventori (R. River, A. Shamir, L. Adleman), è l'esempio più comune di un algoritmo a chiave pubblica. L'algoritmo RSA viene impiegato per definire la coppia di chiavi

(pubblica e privata) da utilizzare nel procedimento di cifratura/decifratura. Vediamo più nel dettaglio come opera riferendoci al nostro esempio di scambio di messaggi segreti tra Alice e Roberto. Iniziamo con illustrare la procedura che permette a Roberto di definire la sua coppia di chiavi pubblica e segreta.

1. Roberto sceglie due numeri primi e molto grandi (più grande è il loro prodotto maggiore sarà la difficoltà nel violare la sicurezza RSA);
2. Si calcoli $n = pq$, chiamato *modulo* e $Z = (p - 1)(q - 1)$;
3. Si scelga un numero e , chiamato *esponente pubblico* minore di n , diverso da 1 e primo rispetto a Z ;
4. Si definisca un numero d , chiamato *esponente privato* tale per cui $(e \cdot d) - 1$ sia divisibile per Z . Questo implica $(e \cdot d) \bmod (Z) = 0$;
5. Risultato : la *chiave pubblica* di Roberto K_p è la coppia (n, e) mentre la sua chiave segreta K_s è la coppia (n, d) .

Di seguito descriveremo le operazioni di cifratura e decifratura relative all'algoritmo RSA.

Il testo di un messaggio viene trasformato in una sequenza di numeri associando ad ogni lettera il numero corrispondente alla sua posizione nell'alfabeto di riferimento. Consideriamo il caso di un numero (lettera) generico m minore di n (definito al passo 2 della precedente procedura). La cifratura di Alice si basa sulla conoscenza della chiave pubblica di Roberto (n, e) . Essa si articola nei seguenti passi:

- Si calcola il numero m^e ;
- Si associa ad m il numero c così definito : $c = m^e \bmod (n)$.
- Si associa alla lettera corrispondente al numero m la lettera associata al nuovo numero definito al passo precedente c .

Roberto riceve la lettera criptata che corrisponde nell'alfabeto di riferimento alla posizione di numero c . L'operazione di decifratura per associare alla lettera criptata la lettera originale viene implementata da Roberto sulla base della sua chiave segreta (n, d) che solo lui conosce. La procedura da eseguire consiste nel calcolare, sulla base della conoscenza di c , il numero m in questo modo:

$$m = c^d \bmod (n)$$

che come si può notare richiede la conoscenza della chiave segreta di Roberto.

Lettera in chiaro	valore di m	valore di c	lettera cifrata
l	12	17	q
o	15	15	o
v	22	22	v
e	5	10	j

Tabella 15.1: Codifica RSA della parola *love*, dove: $p = 7$, $q = 5$, $e = 5$ ed $n = 35$

Lettera cifrata	valore di m	lettere cifrate
q	12	l
o	15	o
v	22	v
j	5	e

Tabella 15.2: Decodifica RSA della parola *qovj*, dove: $d = 29$ ed $n = 35$

Esempio

Riportiamo di seguito l'esempio di applicazione della metodologia RSA proposto in nel testo Kurose'2013 suggerito come lettura consigliata al termine del capitolo.

Supponiamo che Roberto scelga: $p = 5$ e $q = 7$.

Di conseguenza si avrà: $n = pq = 35$ $z = (p - 1)(q - 1) = 24$; $e = 5$

Inoltre Roberto sceglie: $d = 29$ perché $(ed - 1) \bmod (z) = 144$

Roberto pubblica la chiave $(35, 5)$ e mantiene segreta la chiave $(35, 29)$. Come esempio di trasmissione di un messaggio supponiamo che Alice voglia inviare a Roberto la parola *love*. Alice è a conoscenza della chiave pubblica di Roberto $(35, 5)$ e procede quindi alla cifratura del messaggio come mostrato nella tabella 15.1.

Roberto, una volta ricevuto il messaggio cifrato da Alice, ne effettua la decifratura come mostrato in tabella 15.2.

Per un maggiore approfondimento della tecnica RSA si rimanda a Kurose'2013 e agli altri testi indicati in 15.6.

15.5 Un caso pratico: Firewall

Il *firewall* è una metodologia utilizzata per gestire uno aspetto diverso dalla sicurezza dei messaggi scambiati che come abbiamo visto è competenza della crittografia. L'effettuare l'operazione di firewall è una combinazione di hardware e software che permette di implementare il controllo dell'accesso ad un rete e ai suoi dispositivi.

Il firewall controlla tutto il traffico che entra ed esce dalla struttura controllata. Questa funzionalità generalmente viene attivata mediante una procedura di filtraggio di pacchetti. Questa prevede l'esame dell'informazione contenuta nella testata dei pacchetti e nella successiva verifica del rispetto dei criteri

di filtraggio definiti in maniera che si possa distinguere tra i pacchetti che possono passare e quelli che devono essere bloccati. Ovviamente affinché la protezione tramite firewall sia efficace occorre che esso stesso sia immune da penetrazioni esterne sia a livello software che hardware.

Il firewall prevede l'uso di un software configurato, in base a regole prestabilite per ammettere, abbattere o veicolare connessioni tra due aree di rete con differente livello di fiducia, ovvero si comporta, come ci suggerisce la sua denominazione, come un vero e proprio muro interposto tra la rete privata, che ha un elevato grado di fiducia e la rete pubblica, per la quale si assume invece un basso grado di fiducia. Il firewall agisce sui pacchetti in transito e può controllare, modificare oppure semplicemente monitorare il flusso. Si noti che per effettuare queste tre funzioni, il firewall apre il datagramma IP e legge le informazioni contenute nell'header e, in alcuni casi, anche i dati contenuti nel payload. Esistono tre tipi diversi di firewall:

- **packet filter:** è il firewall più semplice. Si limita a controllare gli header IP di ciascun pacchetto che transita e in base alle informazioni contenute nell'header e alle regole con cui è stato configurato decide quali pacchetti possono passare e quali vengono rifiutati. Tale firewall è detto anche stateless firewall poiché la decisione se far transitare o meno un pacchetto presa in un istante di tempo non è correlata con scelte precedenti.
- **stateful firewall:** questo tipo di firewall, al suo interno implementa macchine a stati per prendere decisioni più complesse.
- **application layer firewall:** questo tipo di firewall lavora a livello applicativo. Controlla il payload a livello applicativo e in base alle informazioni trasportate, decide quali applicazioni possono transitare e quali devono essere rifiutate.

15.6 Letture Consigliate

Approfondimenti riguardanti il tema della sicurezza delle reti trattato in questo capitolo possono essere trovati nei seguenti testi:

W. Stallings, Crittografia e Sicurezza delle Reti, McGraw Hill, 2007.

B.A. Forouzan, Reti di Calcolatori ed Internet, McGraw-Hill, 2007.

M. Bishop, Computer Security, Addison Wesley, 2003.

A.S. Tanenbaum, D.J. Wetherall, Reti di Calcolatori, Pearson, 2011.

P.J. Pieprzyk, T. Hardjono, J. Seberry, Fundamental of Computer Security, Springer, 2003.

J.F. Kurose, K. W. Ross, Reti di Calcolatori e Internet, Pearson, 2013.

D. Solomon, Data Privacy and Security, Springer, 2003.

Sigle

6LoWPAN IPv6 over Low-Power Wireless Personal Area Networks

ACK Acknowledgement

ADSL Asymmetric Digital Subscriber Line

ASK Amplitude Shift Keying

ATM Asynchronous Transfert Mode

BAN Body Area Network

BPSK Binary Phase-Shift Keying

BSS Basic Service Set

CAP Contention Access Period

CC Comutazione di Circuito

CDMA Code Division Multiple Access

CFP Contention Free Period

CM Comutazione di Messaggio

CP Comutazione di Pacchetto

DAO Destination Advertisement Object

DIFS Distribuited Inter Frame Space

DIO DODAG Information Object

DIS DODAG Information Solicitation

DNS Domain Name System

DPSK Differential Phase-Shift Keying

DQDB Distribuited Queue Double Bus

DSLAM Digital Subscriber Line Access Multiplexer

DSSS Direct Sequence Spread Spectrum

DSSS Direct Sequence Spread Spectrum

EUI Exdended Unique Identifier

FDM Frequency Division Multiplexing

FDMA Frequency Division Multiple Access

FFD Full-Function Device

FHSS Frequency Hopping Spread Spectrum

FIFO First In First Out

GMSK Gaussian Minimum Shift Keying

GTS Guaranteed Time Slot

HDSL High data rate Digital Subscriber Line

ICMPv6 Internet Control Message Protocol for IPv6

IID Interface Identifier

IoT Internet Of Things

ISDN Integrated Services Digital Network

LAN Local Area Network

LLC Logical Link Control

LLN Low-Power and Lossy Networks

MAC Medium Access Control

MPDU MAC Package Data Unit

MTU Maximum Transmission Unit

O-QPSK Offset Quadrature Phase-Shift Keying

OSPF Open Shortest Path First

PAN Personal Area Network

PBX Private Branch eXchange

PCM Pulse Code Modulation

PDH Plesiochronous Digital Hierarchy

PHY Livello Fisico

PPDU Packet Protocol Data Unit

PSSS Parallel Sequence Spread Spectrum

PSTN Public Switched Telephone Network

RFD Reduced-Function Device

RIP Routing Information Protocol

RPL IPv6 Routing Protocol for Low-Power and Lossy Networks

SAP Service Access Point

SDSL Symmetric Digital Subscriber Line

SIFS Short Inter Frame Space

TDM Time Division Multiplexing

TDMA Time Division Multiple Access

VDSL Very high bit-rate Digital Subscriber Line

WAN Wide Area Network

WDM Wavelength Division Multiplexing

WPAN Wireless Personal Area Networks

WSN Wireless Sensor Network

Glossario

Best-effort: classe di servizio che mira ad offrire una trasmissione al meglio delle possibilità attuali della rete

Bit-rate: quantità di dati digitali che possono essere trasferiti su un canale di comunicazione in un dato intervallo di tempo

Commutazione di circuito: rete in cui ogni singolo elemento è connesso agli altri con un collegamento fisico dedicato

Commutazione di pacchetto: rete in cui non vi è una prenotazione delle risorse. Il percorso dal mittente al destinatario è instaurato al momento dell'invio del pacchetto

Jitter: indica la variazione di una o più caratteristiche di un segnale come, ad esempio, l'ampiezza, la frequenza, la fase. Nelle reti, con questo termine si indica la variazione del ritardo di ricezione dei pacchetti trasmessi

Plesiochronous Digital Hierarchy: tecnologia e protocollo di rete (di livello fisico) usata per trasmettere dati multiplati su una rete di trasporto digitale

Pulse Code Modulation: modulazione che utilizza un campionamento del segnale analogico ad intervalli regolari; i valori campionati vengono successivamente quantizzati ed in seguito digitalizzati (generalmente in forma binaria)

Quantizzazione: processo di conversione di un segnale continuo in un segnale discreto

Service Access Point: punto di accesso ad un servizio che un livello offre al suo soprastante

Throughput: traffico smaltito, dato dal numero di pacchetti corretti che arrivano a destinazione

Wavelength Division Multiplexing: multiplazione utilizzata nei sistemi ottici. Si basa su una modulazione di tipo FDM dove però si usano le lunghezze d'onda del segnale anziché le usuali frequenze della portante.

Indice analitico

- ATM, 189
- Bluetooth, 127
- Body Area Network, 154
- Bridge, 106
 - Chiave Pubblica, 242
 - Algoritmo RSA, 242
 - Chiave Simmetrica, 241
 - Clos, 34
 - Commutatore, 23
 - Congestione
 - Leaky bucket, 231
 - Token bucket, 232
- DQDB, 80
- DSSS, 113
- Ethernet, 99
 - frame, 100
- FDDI, 83
- FHSS, 113
- Firewall, 244
- Gateway, 109
- Hub, 105
- IEEE 802, 73
- IPv4, 53
- IPv6, 60
- ISO/OSI, 46
- LCC, 74
- Lee, 38
- MAC, 74
- Modalità
 - connection oriented, 44
 - connectionless, 45
- MPLS, 214
- multiplexing, 16
 - FDM, 17
 - TDM, 18
- NAT, 58
- porta, 59
- Proxy, 109
- Rete di connessione, 23
 - struttura S, 25
 - struttura S-S, 28
 - struttura S-S-S, 33
 - struttura S-T, 32
 - struttura T, 26
 - struttura T-S, 31
 - struttura T-S-T, 36
- Rete telefonica, 13
 - Analogica, 14
 - Numerica, 15
- Router, 108
- Routing, 199
 - Algoritmi con tabella, 205
 - Distance Vector, 205
 - Link State, 209
 - Algoritmi gerarchici, 212
 - Algoritmi senza tabella, 203
 - Flooding, 203
 - Random, 203
 - Source Routing, 204
 - Diretto, 200
- Switch, 106
- TCP, 68
- TCP/IP, 51
- Tecniche di accesso
 - Casuale, 90
 - Aloha, 91
 - CSMA, 93
 - CSMA/CA, 115

CSMA/CD, 96	Commutazione di Pacchetto
Ordinato, 87	Datagramma, 10
tecniche di accesso	Teorema del Campionamento, 15
casuale	Topologia
CSMA/CA, 117	Bus, 5
Tecniche di Commutazione	Mesh, 4
Commutazione di Circuito, 7	Ring, 6
Commutazione di Messaggio, 8	Star, 5
Commutazione di Pacchetto, 9	UDP, 67
Circuito Virtuale, 10	Ultra Wideband, 139
Tecniche di commutazione	

Finito di stampare
nel Luglio 2014 da
Digital Print – Segrate (MI)