

# **Appunti di Sistemi e Servizi di Telecomunicazione**

**A cura di:**

Francesco Refolli

Matricola 865955

**Fonte Immagini:**

Slide di M. Savi

**Anno Accademico 2023-2024**

# Chapter 1

## Teoria della Comunicazione, Multiplexing e Mezzi di Transmissione

### 1.1 Teoria della Comunicazione

Shannon e Weaver hanno proposto un modello che puo' essere adottato per le comunicazioni. Essenzialmente c'e' una sorgente che emette dei messaggi, che vengono codificati da un Trasmettitore (codifica + modulazione). Il Segnale e' trasmesso sul canale ed e' sogetto al rumore, quindi arriva al Ricevitore che lo decodifica (demodulazione + decodifica) e lo invia alla destinazione.

Il rumore e' modellato come additivo.

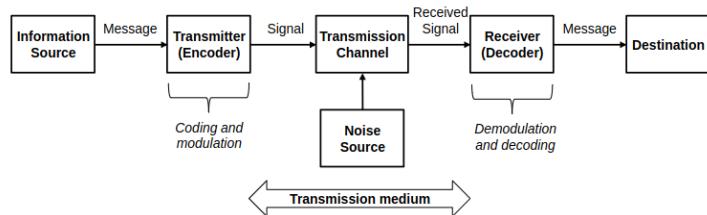


Figure 1.1: Schema di Shannon e Weaver (1948)

#### 1.1.1 Canale

Ci interessiamo principalmente di comunicazioni digitali, ma e' importante conoscere come le informazioni sono ecodificate nel segnale per essere propagate nel mezzo fisico.

Il canale di comunicazione e' un'astrazione che modella il mezzo e le fonti di rumore, distorsione e attenuazione.

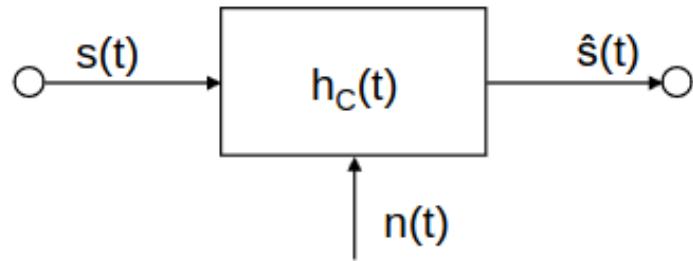


Figure 1.2: Canale di Trasmissione

L'attenuazione e la distorsione sono modellate come "modifica" della forma del segnale, mentre il rumore è additivo al segnale già distorto e attenuato. Esistono altri modi per modellare il rumore in modo più realistico.

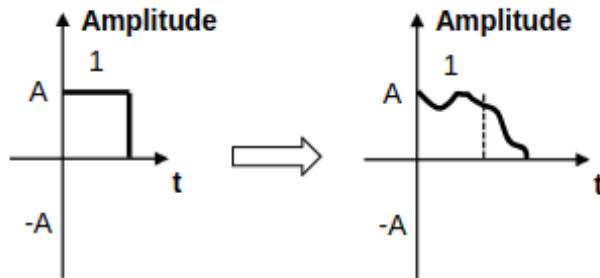


Figure 1.3: Distorsione e Attenuazione

### 1.1.2 Trasformata di Fourier

Il segnale può essere visto come una combinazione di infinite sinusoidi di diversa frequenza, ampiezza e fase (un po' come la serie di Taylor), la Trasformata di Fourier indica i valori di queste sinusoidi nelle varie frequenze.

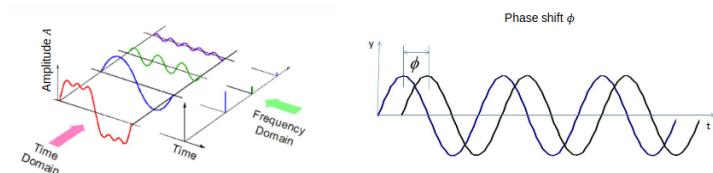


Figure 1.4: Trasformata di Fourier

Il risultato è una funzione nel dominio delle frequenze che indica quanto è "forte" il segnale in una certa frequenza. La larghezza di questo grafico è chiamato anche **bandwidth** (bandwidth).

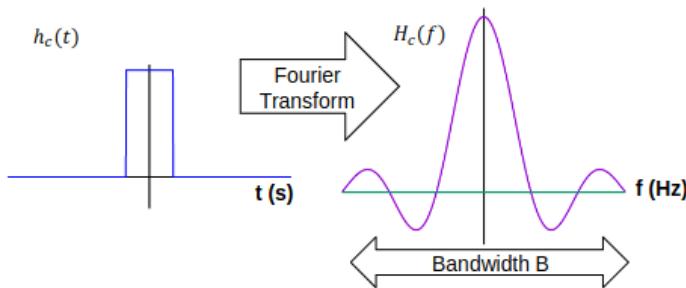


Figure 1.5: Banda

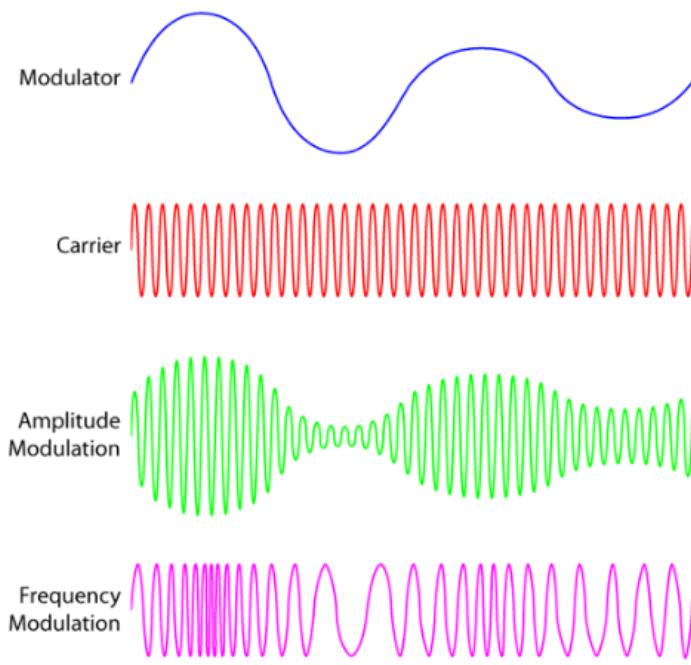
### 1.1.3 Capacita' del Canale

La capacita' e' definita come il massimo bit rate in cui le informazioni possono essere trasmesse in modo affidabile (ovvero con bit error trascurabile). Shannon ha dimostrato che essa per un canale rumoroso e'  $C = B \cdot \log_2(1 + \frac{S}{N})$  bit/s. Dove  $B$  e' la banda e  $\frac{S}{N}$  e' il rapporto segnale/rumore. Quest'ultimo e' il vero e proprio limite di capacita' del canale a parita' di banda (con modulazione e codifica appropriate e' possibile avere prestazioni vicine al limite).

### 1.1.4 Modulazione

#### Modulazione Analogica

E' la conversione in alte frequenze di un segnale da modulare. E' eseguita cambiando l'ampiezza, la frequenza o la fase di una portante sinusoidale per accomodare l'informazione.



M. Savi – Telecommunication Systems and Services

Figure 1.6: Esempi di Modulazione

## Modulazione Digitale

E' l'assegnamento di forme d'onda a gruppi di bit che devono essere trasmessi per ottenere segnali robusti a distorsione e rumore. Ogni unita' e' chiamato "simbolo" ed e' trasmesso per un quanto di tempo. La quantita' di simboli che e' possibile trasmettere in un secondo e' detta "baud rate".

Schemi di modulazione che trasmettono piu' bit per simboli necessitano anche di rapporti segnale/rumore migliori.

Come al solito la distinzione tra simboli diversi implifica avere livelli ( $A$ ,  $A/2$ ,  $-A/2$ ,  $-A$ ) che permettano di separare nettamente il segnale. Piu' livelli implicano la necessita' di un rapporto segnale/rumore migliore.

Inoltre sarebbe meglio che due livelli consecutivi non abbiano associati due simboli con distanza di hamming superiore ad 1 per evitare che un errore di un livello porti a errori sui bit maggiori. (si veda esempio nella modulazione a 4 livelli "10" e "01").

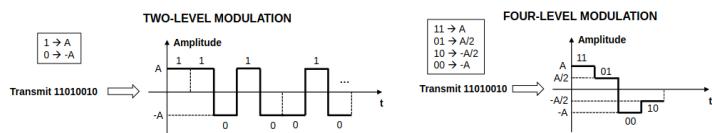


Figure 1.7: Esempi di Modulazione

Un'altra possibilita' e' quella proprio di avere simboli che siano tagli di un'onda in fasi diverse. Un esempio e' QPSK che permette di avere 2 bit per simbolo.

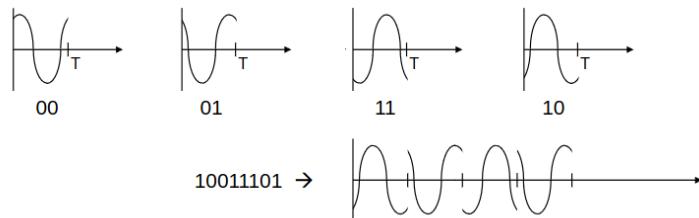


Figure 1.8: Quadrature Phase Shift Keying

## 1.2 Multiplexing e Accesso Multiplo

Il multiplexing e' l'insieme di tutte quelle tecniche atte a condividere la capacita' di un canale per combinare piu' segnali in uno solo. Questa puo' esse ottenuta partizionando risorse come frequenze, tempo e codici. Il demultiplexing, ca va sans dire, e' l'operazione inversa al multiplexing.

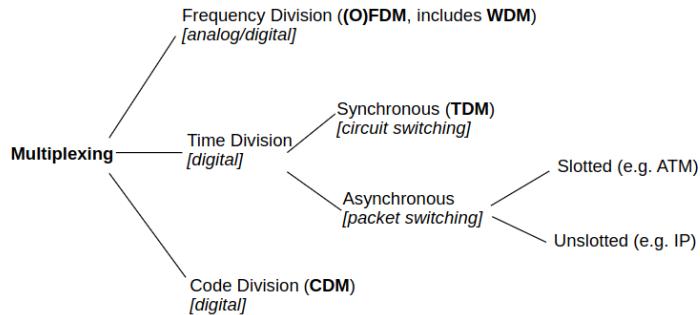


Figure 1.9: Tassonomia del Multiplexing

### 1.2.1 Frequency Division Multiplexing

La banda del canale e' divisa per il numero di segnali da trasportare e un frammento e' assegnato a ciascuno. Il risultato e' una portante che trasporta piu' segnali contemporaneamente su frequenze diverse. Il Wavelength Division Multiplexing e' una forma di FDM utilizzata per la fibra ottica.

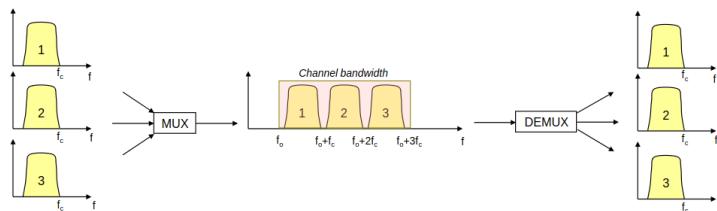


Figure 1.10: Schema

### 1.2.2 Orthogonal Frequency Division Multiplexing

Anche qui la banda e' divisa ma stavolta in una quantita' grande di piccole bande che poi possono essere assegnate ai segnali da trasmettere. E' importante afferrare che questi assegnamenti possono essere discontinui in modo da non penalizzare troppo alcuni segnali se una parte della banda e' in un certo momento soggetta ad interferenza. Tipico di sistemi in cui la qualita' del segnale cambia molto dinamicamente (Wireless domain per esempio).

E' conosciuta anche come Discrete Multitone (DMT).

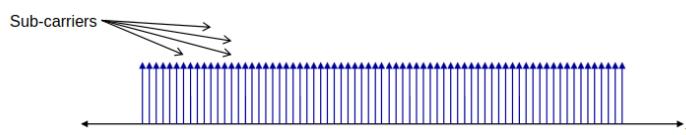


Figure 1.11: Schema

### 1.2.3 Synchronous Time Division Multiplexing

Qui e' il tempo di trasmissione ad essere suddiviso in time slots e in ognuno di essi viene trasmesso un frame di uno dei segnali piu' o meno ciclicamente. I frame contengono

l'informazione per la sincronizzazione (quando un nuovo frame inizia. Come nota, e' possibile ma complicato trasmettere piu' sorgenti con differenti bit rate. Synchronous Digital Hierarchy e' una infrastruttura di trasmissione ad alta velocita' basata su TDM per trasportare segnale (inclusa la banda larga).

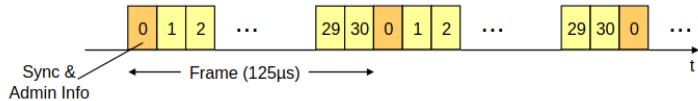


Figure 1.12: Schema

### 1.2.4 Asynchronous Time Division Multiplexing

Anche piu' si divide il tempo ma non e' costante (posso avere dei buchi). Questa variante e' piu' performante nelle comunicazioni a commutazione di pacchetto che di circuito. I frame possono essere slotted (Asynchronous Transfer Mode) o unslotted (IP). Come nota, e' piu' semplice trasmettere piu' sorgenti con differenti bit rate rispetto a STDM.

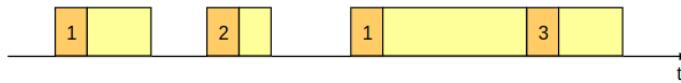


Figure 1.13: Schema

### 1.2.5 Statistical Multiplexing

ATDM da la possibilita' di adottare tecniche di adattamento della condivisione del segnale per ottimizzare l'uso di esso con traffico con picchi generato da varie sorgenti. Utile quando la quantita' di traffico oscilla nel tempo.

In base allo stato del canale posso decidere se trasmettere  $N$  o  $2N$  sorgenti per esempio, per garantire maggior uso possibile ma anche meno perdite possibili.

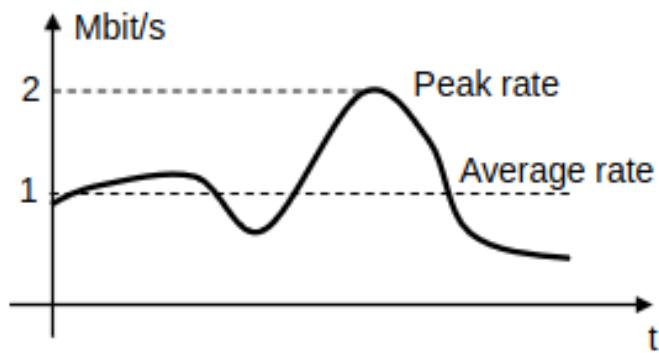


Figure 1.14: Schema

### 1.2.6 Code Division Multiplexing

Ogni segnale  $S_i$  e' moltiplicato per un codice  $C_i$  e viene inviato. Quando piu' segnali codificati si sommano, il ricevitore e' in grado di distinguere i piu' segnali. Questo grazie

al fatto che i codici sono ortogonali ( $C_i C_j = 0 \forall i \neq j$ ).

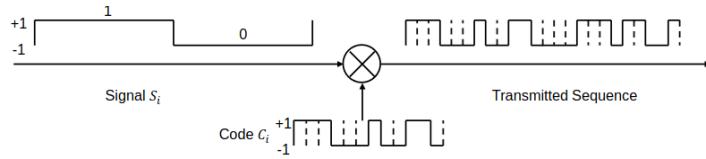


Figure 1.15: Schema

Per esempio se ho una stazione che deve trasmettere piu' segnali a 4 ricevitori distinti, puo' effettuare gli invii in questo modo per evitare che i segnali si sovrappongano e i ricevitori fraintendano.

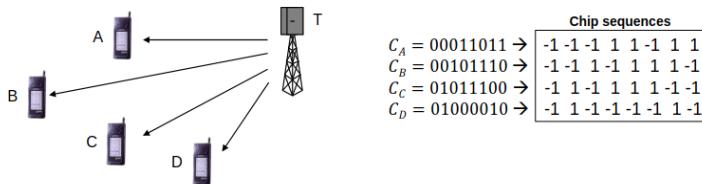


Figure 1.16: Esempio - Situazione

- Signal sums up on the air
  - Transmitted sequence to A ( $-1 \cdot C_A$ ):  $1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ -1$
  - Transmitted sequence to B ( $1 \cdot C_B$ ):  $-1 \ -1 \ 1 \ -1 \ 1 \ 1 \ 1 \ -1$
  - Transmitted sequence to C ( $1 \cdot C_C$ ):  $-1 \ 1 \ -1 \ 1 \ 1 \ 1 \ -1 \ -1$
  - Sum up to:  $\underline{-1 \ 1 \ 1 \ -1 \ 1 \ 3 \ -1 \ -3}$

Figure 1.17: Esempio - Trasmissione

- Demultiplexing at the stations
  - Signal at C  $\rightarrow C_C \cdot R = (-1 \ 1 \ -1 \ 1 \ 1 \ 1 \ -1) \cdot$   
 $(-1 \ 1 \ 1 \ -1 \ 1 \ 3 \ -1 \ -3) =$   
 $\underline{+1 \ +1 \ -1 \ -1 \ +1 \ +3 \ +1 \ +3} = 8 \leftarrow 1 \text{ received}$
  - Signal at A  $\rightarrow C_A \cdot R = (-1 \ -1 \ -1 \ 1 \ 1 \ -1 \ 1) \cdot$   
 $(-1 \ 1 \ 1 \ -1 \ 1 \ 3 \ -1 \ -3) =$   
 $\underline{+1 \ -1 \ -1 \ -1 \ +1 \ -3 \ -1 \ -3} = -8 \leftarrow 0 \text{ received}$
  - Signal at D  $\rightarrow C_D \cdot R = (-1 \ 1 \ -1 \ -1 \ -1 \ 1 \ -1) \cdot$   
 $(-1 \ 1 \ 1 \ -1 \ 1 \ 3 \ -1 \ -3) =$   
 $\underline{+1 \ +1 \ -1 \ -1 \ -3 \ -1 \ +3} = 0 \leftarrow \text{No transmission}$

Figure 1.18: Esempio - Ricezione

### 1.3 Accesso Multiplo

E' un concetto simile al multiplexing: consente di condividere la capacita' di un canale concorrentemente tra sorgenti differenti. Utilizzati di frequente negli schemi wireless e in generale anche radio che sono "shared" per la loro natura.

La differenza fondamentale rispetto al multiplexing e' che in questo caso abbiamo proprio sorgenti diverse che vogliono trasmettere ognuna un segnale, al contrario di esso dove avevamo una sorgente che doveva trasmettere piu' segnali contemporaneamente.

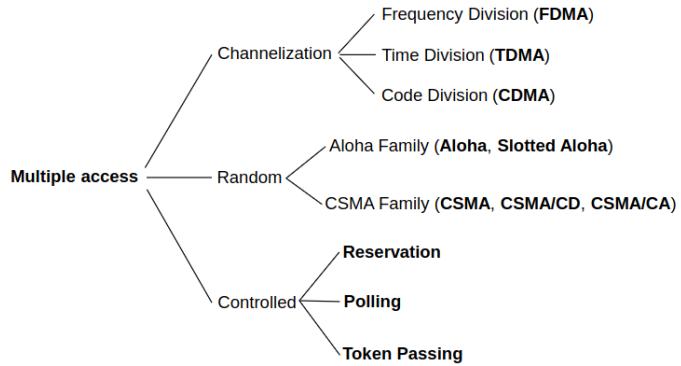


Figure 1.19: Tassonomia di Accesso Multiplo

## 1.4 Mezzi di Trasmissione

Ci sono sia mezzi di trasmissione guidati (doppini e fibra ottica) che trasmissioni non guidate (onde radio).

## 1.5 Mezzi Guidati

### 1.5.1 Doppini

Sono composti di fili di rame isolati avvitati tra loro per evitare le interferenze. Una coppia di cavi paralleli agirebbe come un'antenna, mentre avvitandoli si genera interferenza distruttiva che aiuta la propagazione affidabile di segnale. Spesso nello stesso cavo sono presenti piu' coppie avvitate: queste usano passi diversi di avvitamento per evitare il piu' possibile le interferenze.

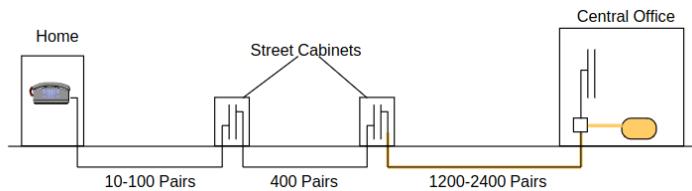


Figure 1.20: I Doppini Telefonici sono la base dell'infrastruttura che permette la telefonia e l'ADSL/VDSL

### 1.5.2 Fibra Ottica

I cavi in fibra ottica sono cavi molto fini di fibra di vetro che possono propagare luce quasi infrarossa con bassissima attenuazione. Il principio alla loro base e' la **total internal reflection**. Un sottile filo di vetro centrale e' rivestito da uno strato di vetro con basso indice refrattivo. La banda limite e' alta quindi dominano le infrastrutture di dorsale.



Figure 1.21: Fibra Ottica

Principalmente dobbiamo distinguere:

### Fibre Multi Modali

Accomodano la propagazione di segnale con velocità differenti ma questa dispersione limita il prodotto banda-distanza. Sono più facili da ottenere rispetto alle altre, ma si preferiscono comunque quelle più sottili perché trasportano meglio il segnale.

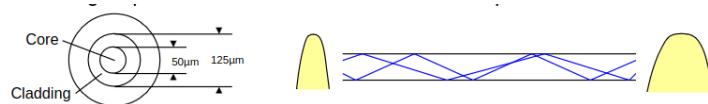


Figure 1.22: Fibra Ottica Multi Modale

### Fibre Mono Modali

Evitano la dispersione di segnale e possono trasportare molta più banda a parità di distanza, ma costano un po' in relazione a quanto devono essere sottili.

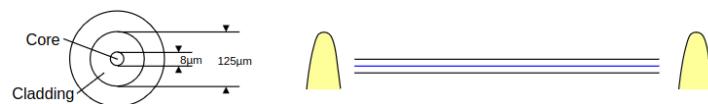


Figure 1.23: Fibra Ottica Mono Modale

## 1.6 Radio

- Radio wave
  - Wavelength:  $\lambda = \frac{c}{f}$  (m)
  - Frequency:  $f$  (hz)
  - Light speed:  $c = 3 \cdot 10^8 \frac{m}{s}$

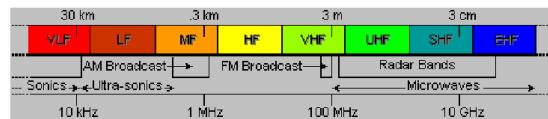
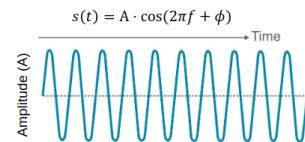


Figure 1.24: Spettro delle Onde Radio

Radio spectrum	ELF	<3 KHz	Remote control, Voice, analog phone
	VLF	3-30 KHz	Submarine, long-range
	LF	30-300 KHz	Long-range, marine beacon
	MF	300 KHz – 3 MHz	AM radio, marine radio
	HF	3-30 MHz	Amateur radio, military, long-distance aircraft/ships
	VHF	30-300 MHZ	TV VHF, FM radio, AM x aircraft commun.
	UHF	300 MHz - 3 GHz	Cellular, TV UHF, radar
	SHF	3-30 GHz	Satellite, radar, terrestrial wireless links, WLL
	EHF	30-300 GHz	Experimental, WLL
	IR	300 GHz – 400 THz	LAN infrared, consumer electronics
	Light	400-900 THz	Optical communications

Figure 1.25: Quello che ci interessa

Una frettolosa catalogazione delle comunicazioni radio di nostro interesse:

- Wireless Local Area Networks (WLANs) and Fixed Wireless Access (FWA): utilizzano una banda 2.4 GHz – 5 GHz unlicensed (se vuoi evitare interferenze, ovvero che qualcuno trasmetta devi pagare); verso 5 GHz si iniziano ad avere problemi con pioggia e nebbia.
- Mobile radio networks (2G, 3G, 4G, 5G): utilizzano la banda 800 MHz – 2.6 GHz; con poca energia e' possibile trasmettere un segnale decente a grandi distanze.
- Satellite networks and 5G mobile radio network: utilizzano la banda 3 – 30 GHz: la banda disponibile e' ampia ma si risente come prima di pioggia e nebbia.

### 1.6.1 Antenne

Le antenne possono irradiare energia nello spazio (trasmissione) e catturare energia dallo spazio (ricezione). In generale possono irradiare in modo uniforme in tutte le direzioni, oppure concentrato in alcune direzioni.

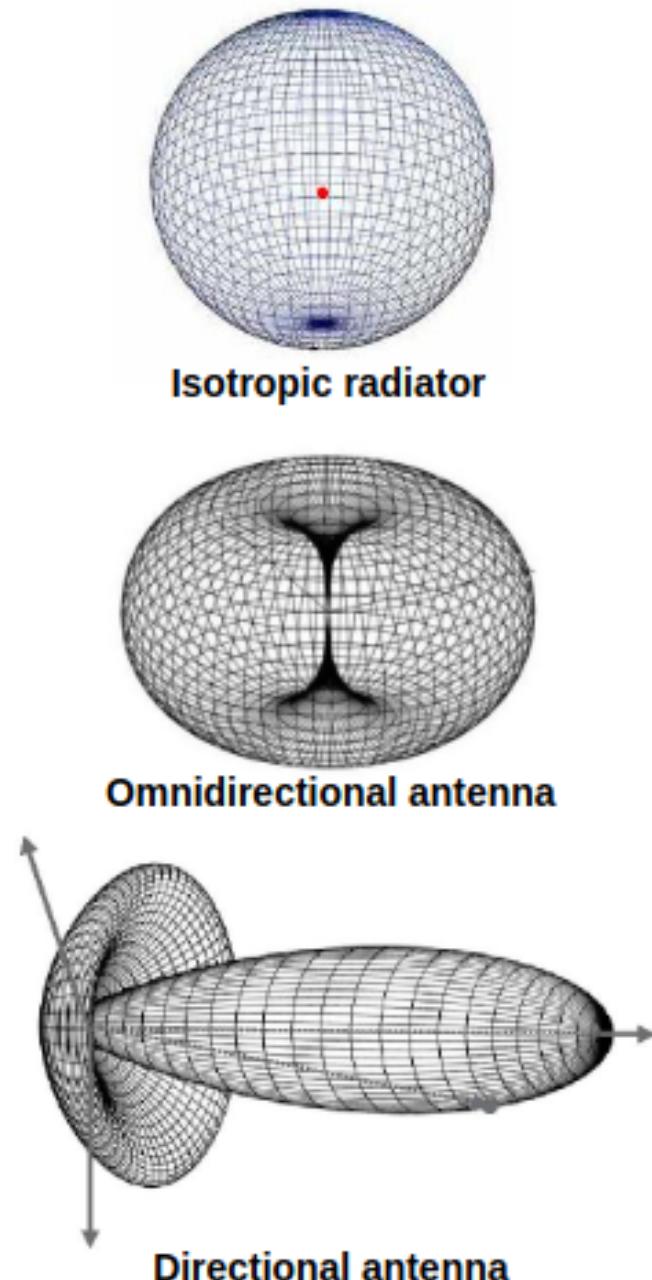


Figure 1.26: Propagazione del Segnale con le Antenne

### 1.6.2 Antenne Direzionali

I terminali mobili solitamente utilizzano antenne omnidirezionali, per poter trasmettere indipendentemente dalla posizione della stazione più vicina. Invece le stazioni impiegano delle antenne direzionali, ovvero antenne che ricevono/trasmettono per un angolo variabile del piano (settore, sono chiamate anche antenne settoriali). I collegamenti punto-a-punto e le stazioni satellitari utilizzano antenne paraboliche che possono concentrare il segnale in una direzione.

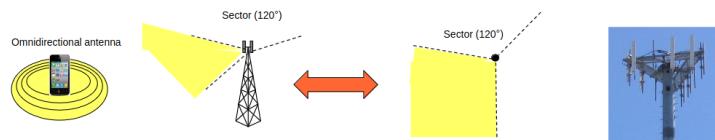


Figure 1.27: Antenne Direzionali

### 1.6.3 Caratteristiche del Canale

Le comunicazioni radio sono "broadcast" per loro natura, di solito si impiega una architettura centralizzata per coordinare le trasmissioni. Usualmente i terminali possono parlare solo con la stazione.



Figure 1.28: Architettura Stazione

### 1.6.4 Impedimenti di Trasmissione Radio

Il segnale radio si attenua con il quadrato della distanza ed e' soggetto a variazioni di caratteristiche se incontra degli ostacoli.

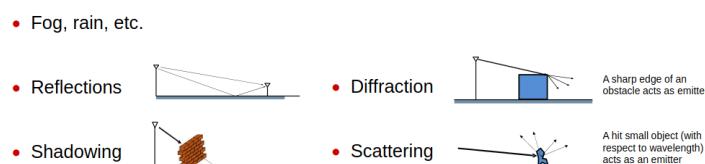


Figure 1.29: Ostacoli

Approfondiamo due fenomeni di interferenza, generati data la natura di onde:

- multi-path fading: un segnale, in seguito alla riflessione parziale o totale, giunge al ricevitore piu' volte con percorsi diversi.
- shadow fading: il contatto con un oggetto grosso puo' ostacolare la ricezione del segnale.

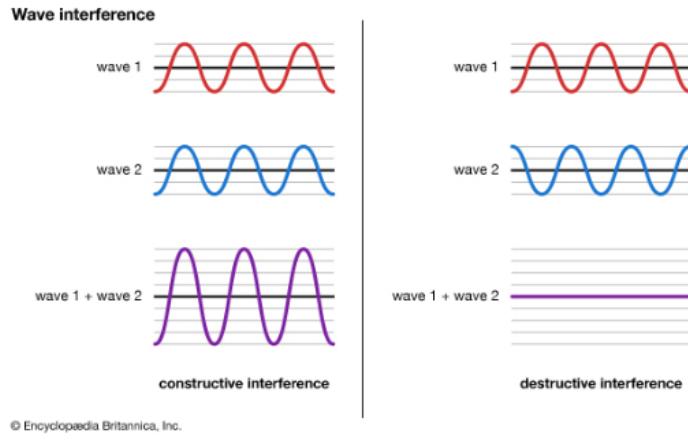


Figure 1.30: Interferenze

Per ovviare a questi problemi si agisce con il controllo di potenza (piu' energia per irradiare, drena la batteria dei cellulari) o tecniche di modulazione/coding viste precedentemente.

Frequenze piu' alte soffrono di attenuazione maggiore in relazione alla distanza, quindi per coprire una vasta area sono necessarie piu' antenne.

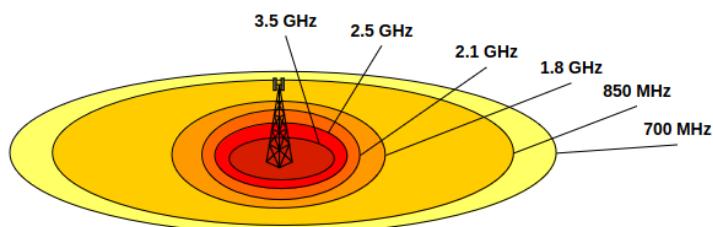


Figure 1.31: Copertura

Per quanto riguarda l'interazione della stazione con i terminali nei collegamenti Uplink e Downlink si nota che viene usato il Multiplexing nel caso di Downlink e Accesso Multiplo nel caso di Uplink.

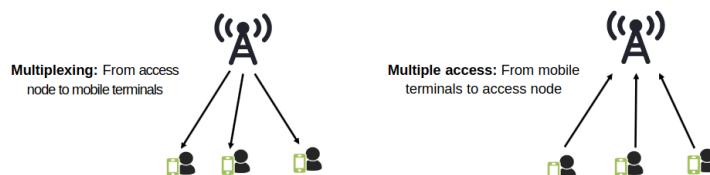


Figure 1.32: Uplink / Downlink

Esiste anche la possibilita' di effettuare il cosiddetto Duplexing, ovvero l'uso di tecniche di multiplexing per accomodare entrambi uplink e donwlink. Un esempio sono il TDM (suddidido gli slot tra i due versi) e il FDM (suddivido le frequenze tra i due versi).

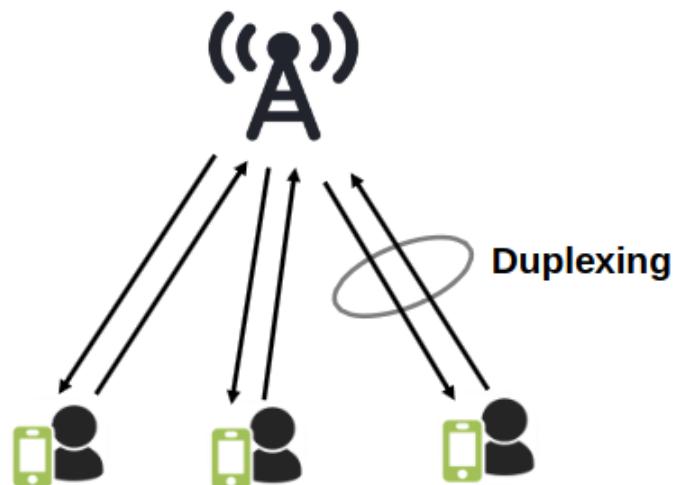


Figure 1.33: Duplexing

### 1.6.5 Multiple Input Multiple Output

I sistemi MIMO sfruttano la coesistenza di piu' antenne trasmetttrici per trasmettere lo stesso segnale a piu' antenne ricevitrici in modo da ridondare il segnale. Il Massive MIMO e' una tecnologia adottata nelle reti 5G basato sul MIMO.

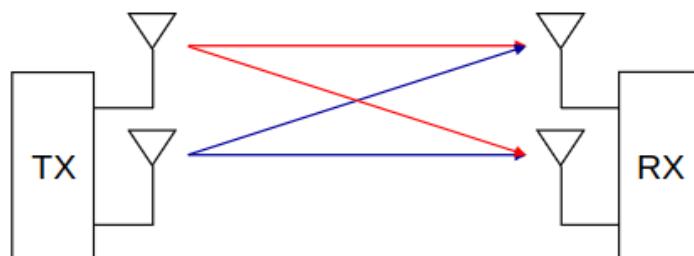


Figure 1.34: MIMO

# Chapter 2

## Reti di Accesso a Banda Larga

Ci concentriamo sulle reti a banda larga, one small issue, "broadband" e' un termine ambiguo perche' una definizione univoca non esiste. Alcuni utilizzano anche "ultra-broadband" come gadgetbahn ma fondamentalmente non si sa cosa voglia dire di preciso.

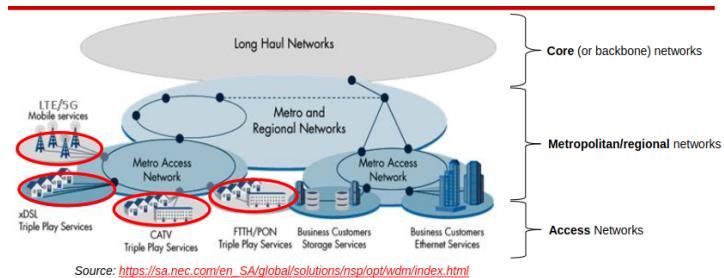


Figure 2.1: Dominio

### Tipologie

- Fixed Access Network: cablaggio fino alla casa dell'utente con varie soluzioni di rame, fibra o ibridi.
- Fixed Wireless Access Network: cablaggio in fibra fino ad un Point of Presence e poi comunicazione radio fino alla casa dell'utente.
- Satellite Access Network: cablaggio in fibra fino ad una stazione di terra e poi comunicazione radio satellitare fino alla stazione dell'utente.
- Mobile Radio Access Network: cablaggio o collegamento radio fino alla stazione di prossimita' e poi comunicazione radio con un terminale mobile (accomoda la mobilita' dell'utente).

### 2.1 Fixed Access Network

#### 2.1.1 Copper Access Network Infrastructure

Abbiamo un **distribution box** nell'edificio dell'utenza che evita la necessita' di cablare ogni singolo utente con le altre stazioni.

Quindi un **distribution point**: un permutatore che colleziona i collegamenti con i distribution box e li indirizza in un unico collegamento fisico (piu' doppini comunque). Tipicamente ci sono solo al massimo due distribution point tra l'utenza e la centrale, ma e' possibile che ce ne siano di piu' cosi' come e' possibile (ma molto raro) che non ce ne siano.

I collegamenti quindi terminano nel **Main Distribution Frame** che li allaccia alla rete a banda larga.

Quindi il DSL Access Multiplexer (DSLAM) seleziona la porzione di banda dedicata alla commutazione di pacchetti e invia il traffico nell'IP router. Il DSLAM modula e demodula il segnale tramite un array di **Modulator&Demodulator** (Modem) quindi e' necessario che anche l'utenza disponga di Modem.

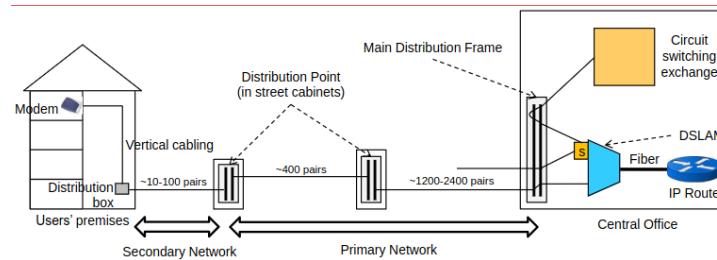


Figure 2.2: Architettura

Quando le basse frequenze sono utilizzate per la commutazione di circuito per la telefonia e' necessario un Plain Old Telephone Service (POTS) Splitter (S), ovvero un filtro che permette di separare le bande dedicate. Oggi giorno la telefonia puo' avvenire o tramite il POTS (sempre piu' raro) o sempre piu' spesso tramite il VoIP. Chiaramente se si usa uno Splitter e' necessario che anche l'utente ne usi uno.

La qualita' di una infrastruttura del genere dipende dalla distanza dei collegamenti (l'italia ha uno delle reti di accesso piu' corte, bene per la banda larga) e dalla qualita' di mezzi fisici e infrastruttura. Soluzioni a basso costo sfruttano l'infrastruttura di rame stesa per la telefonia per evitare di dover sprecare ulteriore materiale, ma chiaramente ha prestazioni peggiori (soluzione simile a quella della TV via Cavo di altri paesi).

Questa soluzione viene utilizzata parzialmente per alcune forme di Digital Subscriber Line (xDSL).

## 2.1.2 xDSL

L'idea e' avere la maggior parte della banda possibile gia' posizionata sui doppini telefonici. C'e' pero' un tradeoff tra la banda disponibile e la lunghezza dei collegamenti: soluzioni piu' aggressive soffrono di piu' di attenuazione e interferenza sulle distanze medie e lunghe, quindi sono utilizzabili solo per distanze corte.

Technology	Standard	Band	Capacity (down/up or aggregate)	Maximum distance (indicative)
ADSL2+	G.992.5	2.2 MHz	24/1.4 Mbit/s	A few km (approx. 3/5 km)
VDSL2	G.993.2 17a	17.6 MHz	70 Mbit/s	A few hundred meters (approx. 500m)
VDSL2	G.993.2 30a	30 MHz	100+ Mbit/s	A few hundred meters (approx. 500m)
VDSL2	G.993.2 35b	35 MHz	200+ Mbit/s	A few hundred meters (approx. 500m)
G.fast	G.9700/9701	106/212 MHz	700 Mbit/s	A few tens of meters (less than 100m)

Meaning of the letter preceding "DSL":  
 • ADSL: Asymmetric  
 • VDSL: Very-high-bit-rate

Possibility of distributing bandwidth with different degrees of symmetry

Figure 2.3: xDSL

**VDSL2** usa uno schema FDD per frammentare in bande alternate i collegamenti uplink e downlink nella fascia 138 kHz - 35 MHz.

**G.fast** utilizza invece tutta la fascia 35 MHz - 212 MHz con il TDD similmente a VDSL2 con la differenza che puo' sfruttare anche la fascia 138 kHz - 35 MHz se non e' utilizzata da ADSL2+ o VDSL2 (altrimenti con TDD si possono creare problemi di interferenze).

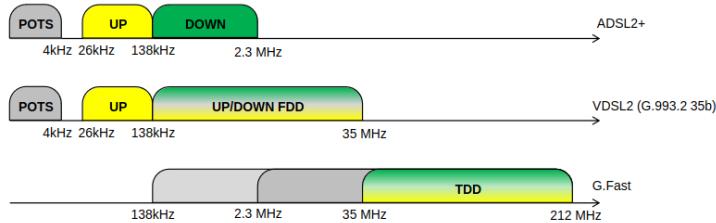


Figure 2.4: Esempi

### 2.1.3 Vectoring

E' una tecnica utilizzata per eliminare il **crosstalk**, ovvero la mutua interferenza tra due doppini adiacenti, per migliorare la qualita' del segnale. Consiste nello stimare la quantita'  $k_i$  di interferenza che il segnale  $s_i$  ha sul segnale trasmesso  $s_j$  e applicare una trasformazione lineare ai segnali trasmessi per eliminare il "rumore" dei singoli segnali.

$$\begin{aligned}
 s_1^* &= (1 - k_1 k_2)^{-1} (s_1 - k_2 s_2) & r_1 &= s_1 \\
 s_2^* &= (1 - k_1 k_2)^{-1} (s_2 - k_1 s_1) & r_2 &= s_2
 \end{aligned}$$

- By transmitting  $\vec{s}^* = T^{-1}\vec{s}$  the desired signal  $\vec{s}$  is received
  - $\vec{r} = T\vec{s}^* = T(T^{-1}\vec{s}) = (TT^{-1})\vec{s} = \vec{s}$
- In the example:  $T^{-1} = \frac{1}{1-k_1k_2} \begin{bmatrix} 1 & -k_2 \\ -k_1 & 1 \end{bmatrix}$

Figure 2.5: Esempio di Vectoring

Il problema e' che questi valori devono essere stimati in fretta (abbiamo cambi repentinamente su un grande numero di dati e quindi richiede grandi capacita' di processamento dei segnali). Spesso ha benefici limitati se coesistono sulla stessa rete di accesso piu' Internet Service Provider (ISP) che gestiscono le comunicazioni ("interferenze" involontarie?).

### 2.1.4 Fiber-Copper Access Network

Come detto precedentemente l'uso dei doppini e' limitato nella distanza rispetto alla banda a cui possono trasmettere. Per offrire prestazioni migliori e' necessario integrare soluzioni in fibra ottica per ridurre i doppini ed aumentare la qualita' del segnale. Ci sono diversi schemi per questo "Fiber-to-the-X" (FTTE, FTTC, FTTB) che hanno costi e vantaggi diversi (in termini di installazione).

### 2.1.5 Fiber to the Exchange

La fibra raggiunge il centro di sismistamento centrale della rete di accesso.

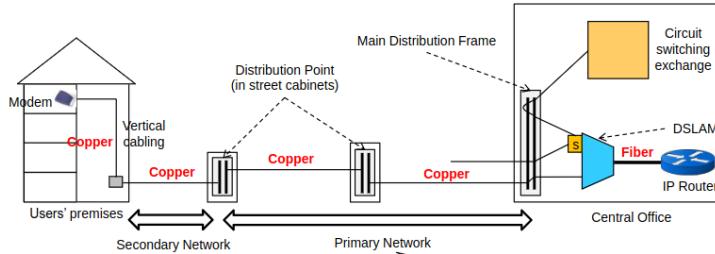


Figure 2.6: FTTE

### 2.1.6 Fiber to the Cabinet

La fibra raggiunge il distribution point (nel Multi-Service Access Node (MSAN) deve essere installato un Mini DSLAM). Il Mini DSLAM deve essere alimentato in qualche modo dalla corrente elettrica: questo e' fatto con il Reverse Power Feeding (ovvero le porte del dopping alimentano il Mini DSLAM, come con i cavi USB ...).

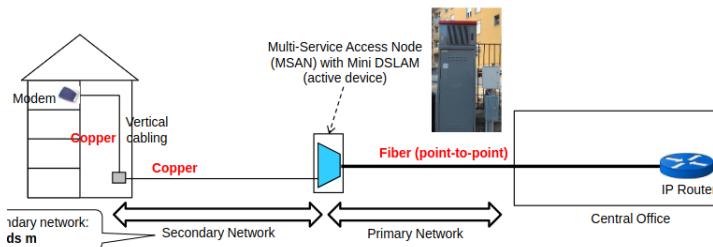


Figure 2.7: FTTC

### 2.1.7 Fiber to the Building

La fibra raggiunge il distribution box (anche qui e' necessario un MSAN). Di solito questo non si fa: si collega la rete direttamente alla casa dell'utente (FTTH).

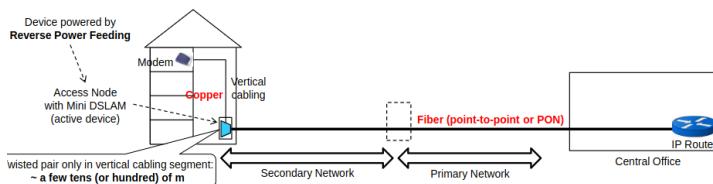


Figure 2.8: FTTB

### 2.1.8 xDSL + Fibra

L'integrazione della fibra permette di raggiungere prestazioni migliori a parita' di distanza (uso di FTTB/FTTC per migliorare le xDSL piu' aggressive).

### 2.1.9 Fiber to the Home

Due possilita': Fibra punto a punto, Passive Optical Network.

- P2P: A partire dalla centrale si porta una fibra singola a casa dell'utente per ognuno di essi. Soluzione tipica degli utenti business (perche' pagano ...). Linea dedicata a 1 Gbit/s per direzione. Mux/Demux avviene al Metropolitan Point of Presence per il traffico che arriva da piu' fibre.
- PON: Una singola fibra fino a una catena di splitter che diramano in fibre ad albero. Ogni utente ha una fibra dal suo Optical Network Unit allo splitter piu' vicino. Dalla centrale (Optical Line Termination) al primo splitter passa un solo cavo in fibra. Si usa molto meno cavo che nella prima soluzione, ma la banda e' condivisa con gli altri utenti (non dedicata). Soluzione tipica degli utenti residenziali.

Tecnologia FTTH GPON: downstream avviene in broadcast, mentre l'upstream e' un TDMA governato dall'OLT.

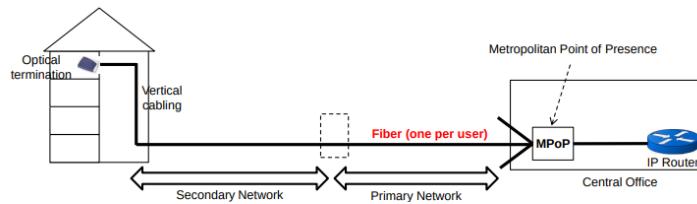


Figure 2.9: FTTH P2P

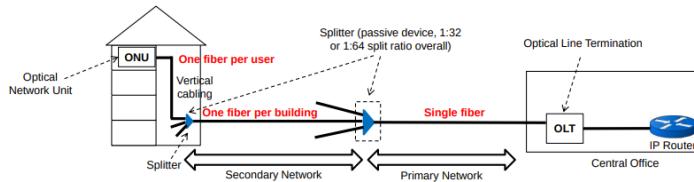


Figure 2.10: FTTH PON

### Monopoli

Si riporta l'architettura della rete di accesso installata da Open Fiber.

Gli alberi passivi dei singoli operatori sono collegati ad un cabinet che poi e' collegato in ultima istanza alla casa. Questo ha il vantaggio di dover installare solo una volta l'infrastruttura di prossimita' e poter collegare tutti gli OLT che voglio al cabinet con costi inferiori.

Si installa un PTE a casa dell'utente per cablare l'edificio alla sua costruzione e completare il collegamento solo quando l'utente decide di installare la fibra in casa.

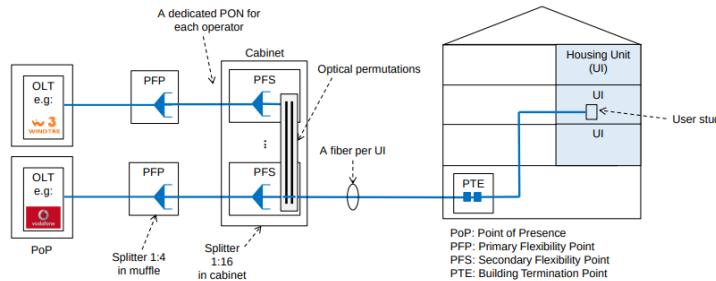


Figure 2.11: Esempio di Open Fiber, monopolista di quartiere

La rete PON puo' essere utilizzata anche per semplificare l'installazione di una rete di accesso FTTB (meno costi, piu' modularita' se vuoi ...):

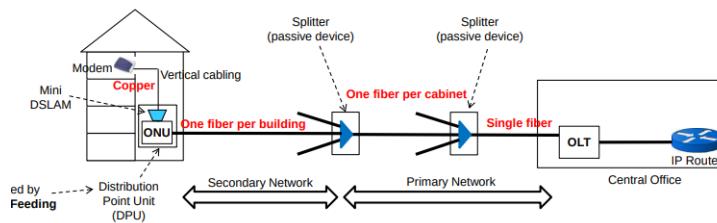


Figure 2.12: FTTB con PON

### 2.1.10 Ok ma perche' non soluzioni di sola fibra?

Perche' costa, e i cablaggi in fibra sulle reti di accesso secondario (prossimita') costano generalmente molto rispetto alla rete primaria (vicina alla centrale), probabilmente per il contesto urbano.

## 2.2 Fixed Wireless Access Network

Fondamentalmente abbiamo il cablaggio in fibra fino ad una stazione radio e poi si usano le onde radio per trasmettere agli utenti finali. E' una soluzione tipica di ambienti montani o collinari stile Castell'Arquato dove e' oggettivamente difficile portare un altro genere di infrastruttura. Usata anche in zone con bassa densita' di urbanizzazione per questione di costi (sarebbe troppo costoso avere un'infrastruttura capillare per due utenti in croce). "Utile per ridurre le diseguaglianze tecnologiche", ovvero con un giro di parole connettere anche chi vive isolato dalla rete digitale.

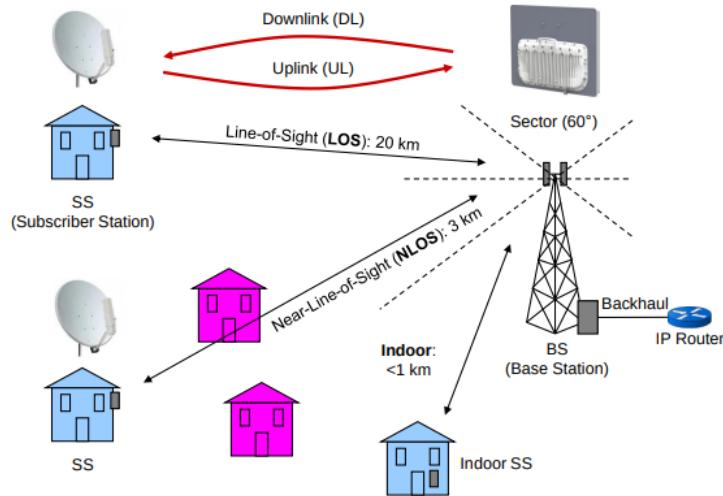


Figure 2.13: Architettur FWA

Chiaramente gli utenti possono soffrire di interferenze date da ostacoli lungo la "linea" del segnale, oppure da un'estrema vicinanza/lontananza dalla stazione. In base a dove sono posizionati gli utenti e' necessario scegliere un tipo di antenna che trasmetta in linea retta, omnidirezionale o settoriale. E' possibile nel caso di distanze ravvicinate di dotare l'utente di router indoor con costi di installazione bassissimi rispetto a quelli outdoor. La velocita' e' considerevole ma sicuramente inferiore a quelle a mezzo guidato moderne ( $> 30$  Mbit/s).

## 2.3 Satellite Access Network

Anche questa e' "un'ottima" soluzione per connettere le zone disabitate o isolate. La fibra arriva fino alla stazione di trasmissione satellitare. Il segnale e' trasmesso ai satelliti che lo fanno rimbalzare sulle antenne degli utenti a terra. C'e' la possibilita' di avere anche stazioni satellitari di terra in ricezione che poi inviano il segnale o tramite onde radio o tramite cablaggio nell'area servita.

La latenza e' purtroppo un problema, e in certe condizioni puo' impedire la comunicazione real-time.



Figure 2.14: Architettura SAN

I satelliti possono essere:

- Geostazionari (GEO): non utilizzati per comunicazioni real-time per via dell'alta latenza ( $> 500\text{ms}$ ), ma e' comunque adatta alle trasmissioni TV, la velocita' orbitale e' uguale a quella di rotazione della terra quindi sono "a posizione fissa". Il problema e' che non si possono servire i poli perche' essi orbinano lungo il piano equatoriale.
- Orbita Media (MEO): non e' utilizzato per le comunicazioni internet.
- Orbita Bassa (LEO): hanno latenza piu' bassa ( $< 50\text{ms}$ ) ma si muovono molto piu' velocemente di quelli Geostazionari quindi sono piu' difficili da gestire.

### 2.3.1 GEO

Le trasmissioni satellitari (GEO, ndr) hanno un grande range di copertura per via della posizione elevata. La copertura puo' essere **Single Beam** (un'area e' servita da un singolo segnale) o **Multi Beam** (un'area e' servita da tante irradiazioni nelle sotto aree con frequenze diverse), quest'ultima permette di aumentare la larghezza di banda (?).

Il downstream e' gestito con TDM e l'upstream con TDMA o CDMA.

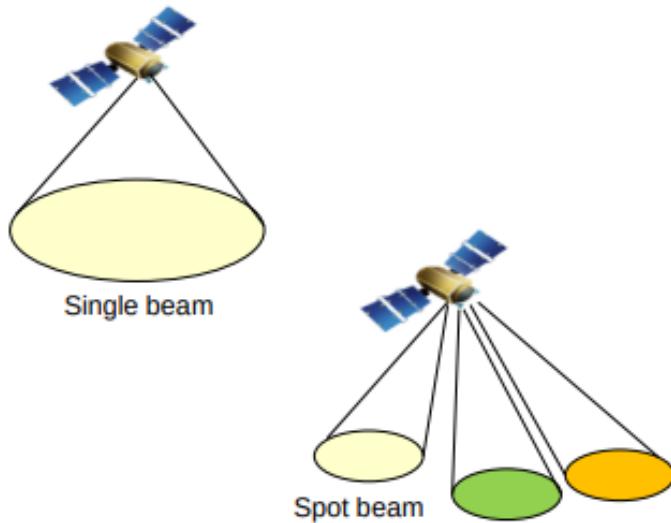


Figure 2.15: Single/Multi Beam

### 2.3.2 LEO

I satelliti sono piu' leggeri e necessitano di una rete fitta di stazioni di terra sul globo (ad oggi nonostante vari claims, nessuno lo ha fatto, forse per fortuna aggiungerei). Per servire tutte le zone e' necessaria anche una grandissima quantita' di satelliti in orbita che ad oggi nessun operatore garantisce (ancora, nonostante vari claims), ma hanno comunque riempito l'orbita di spazzatura. Il terminal dell'utente tenta di connettersi al satellite piu' vicino e si risintonizza con un altro quando quello finisce fuori dal campo visibile. In futuro si potrebbe fare *satellite routing*.

# Chapter 3

## Wireless Area Network

E' una soluzione di rete dedicata piu' costosa di una generalizzata, utilizzata per collegare entita' di tipo business. Si chiama *wide* perche' e' generalmente geograficamente estesa.

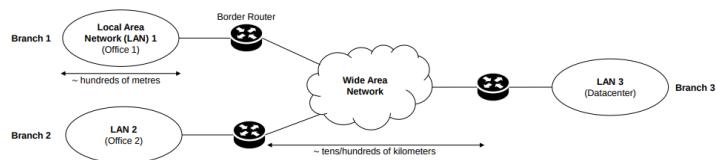


Figure 3.1: WAN

### 3.0.1 Physical WAN

L'organizzazione che deve far uso di una rete dedicata possiede e gestisce fisicamente un'infrastruttura che collega piu' entita' o sottoentita'. E' la soluzione piu' costosa in termini di risorse e denaro, ma da cui si ottiene in ritorno una larga banda e buonissime prestazioni. E' possibile noleggiare pezzi di infrastruttura di ISP che non sono utilizzati (dark fibers).

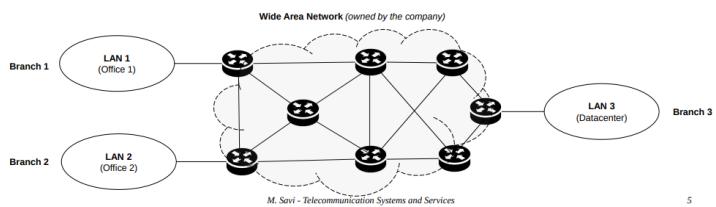


Figure 3.2: P. WAN

### 3.0.2 Leased WAN

L'organizzazione acquista con un contratto il servizio di circuito al gestore della rete con alcuni tipi di garanzie. Costa meno ma si ha meno controllo sull'infrastruttura.

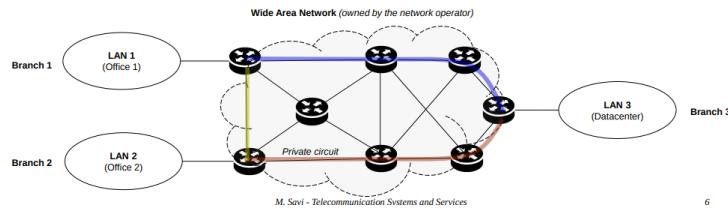


Figure 3.3: L. WAN

### 3.0.3 Multiprotocol Label Switching WAN

E' una soluzione meno costosa che permette ad un'organizzazione di acquistare con un contratto un servizio di mesh tra alcune entita'.

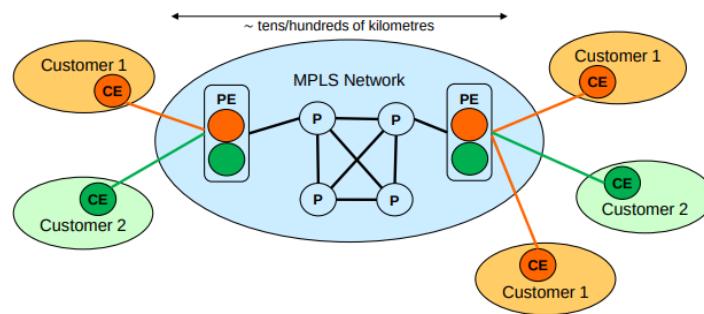


Figure 3.4: M.L.S. WAN

## 3.1 Multiprotocol Label Switching

MPLS da la possibilita' di creare delle linee virtuali tra Provider Edge Router per connettere le sottoreti mesh. Le linee possono essere dinamicamente gestite ed ottimizzate (flessibilita').

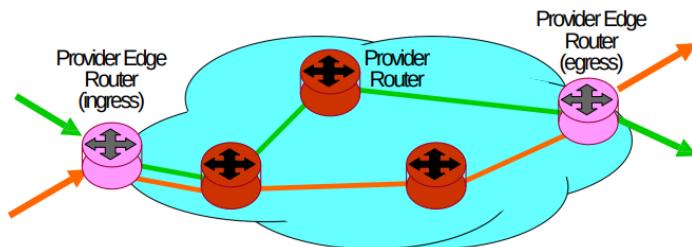


Figure 3.5: MPLS

### 3.1.1 Label Swapping Forwarding

Un pacchetto IP viene incapsulato in un pacchetto MPLS, e questo header (*label*) viene utilizzata per fare il routing virtuale all'interno del circuito. Gli indirizzi MPLS sono locali alla rete MPLS, e i pacchetti possono essere incapsulati piu' volte.

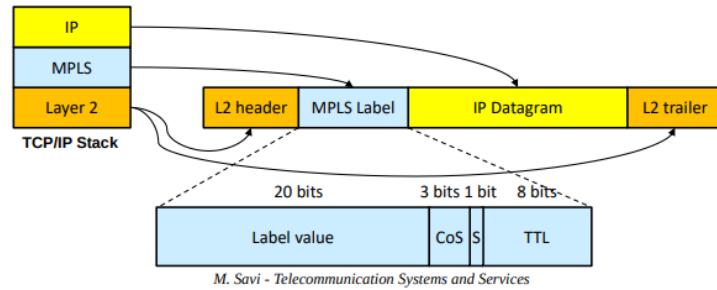


Figure 3.6: MPLS Packet

Durante il routing le label vengono sostituite al transito per accomodare il flusso di dati.

- Population of the MPLS Forwarding Tables of involved routers

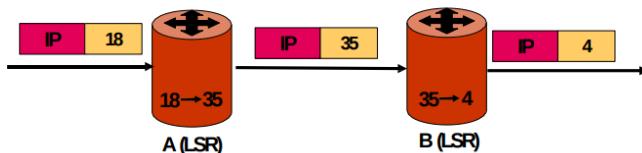


Figure 3.7: MPLS Routing

Il Label Edge Router aggancia o disaggancia l'header MPLS rilasciando il pacchettato IP nella destinazione.

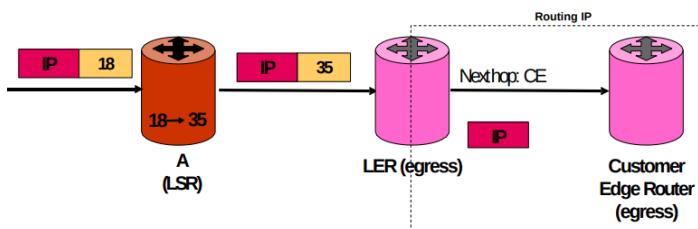


Figure 3.8: Label Edge Router

### 3.1.2 Confronto rispetto a Destination-Oriented

In IP il forwarding non dipende dalla sorgente del flusso ma solo dalla destinazione, mentre in MPLS il focus è il circuito dedicato ad una certa sorgente che viaggia per una certa destinazione.

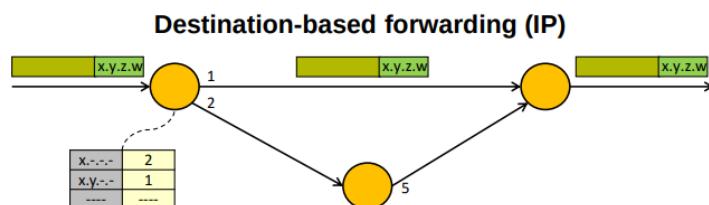


Figure 3.9: IP

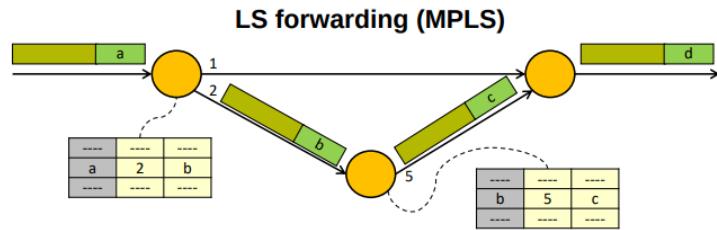


Figure 3.10: MPLS

### 3.1.3 Creazione delle Rotte

La creazione delle rotte in MPLS puo' avvenire o manualmente o in modo automatico tramite un layer di controllo simile per certi versi a quello del livello di Rete dello stack ISO/OSI.

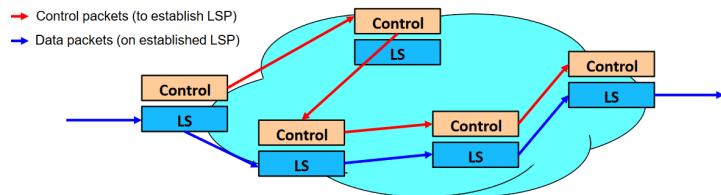


Figure 3.11: MPLS Control Plane

Il routing dei pacchetti di controllo avviene normalmente come in IP.

### 3.1.4 Traffic Engineering Database

E' un database che contiene informazioni circa la topologia dell'infrastruttura, i dati di carico, le limitazioni di banda ... etc e i dati amministrativi con le configurazioni dei clienti. E' utilizzato in MPLS per stabilire le rotte in maniera statica ("offline") o dinamica ("online").

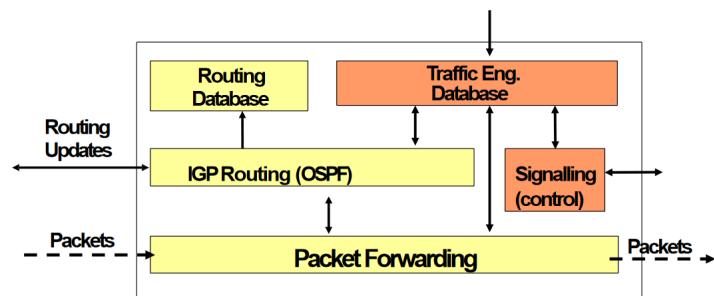


Figure 3.12: MPLS + TED

### 3.1.5 Protocolli di Segnalazione

Un meccanismo di segnalazione e stabilimento delle rotte e' necessario per coordinare i nodi nella distribuzione delle label, riservare/liberare risorse e prevenire i loop.

### Label Distribution Protocol

Questo e' un protocollo molto basilare che segue il routing dettato dai protocolli IGP. Non e' possibile specificare le rotte da seguire (ne' fa uso del TED) e funziona "hop-by-hop" ovvero ogni nodo del percorso agisce autonomamente nella distribuzione delle label. Ogni nodo invia la richiesta al nodo successivo, il quale risponde con la label da utilizzare per l'instradamento nel percorso "riservato".

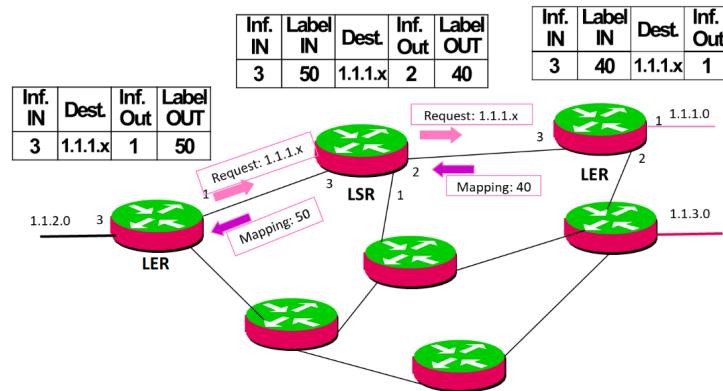


Figure 3.13: LDP /1

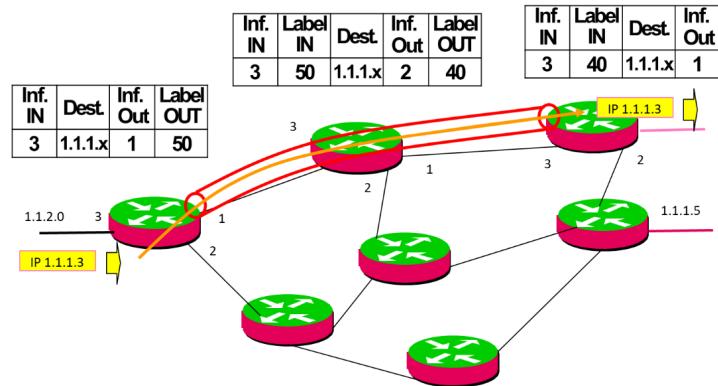


Figure 3.14: LDP /2

### Constrained LDP Routing

In questa variante di LDP abbiamo la possibilita' di specificare esplicitamente le rotte da instaurare nodo per nodo. Anche qua pero' il funzionamento e' "hop-by-hop".

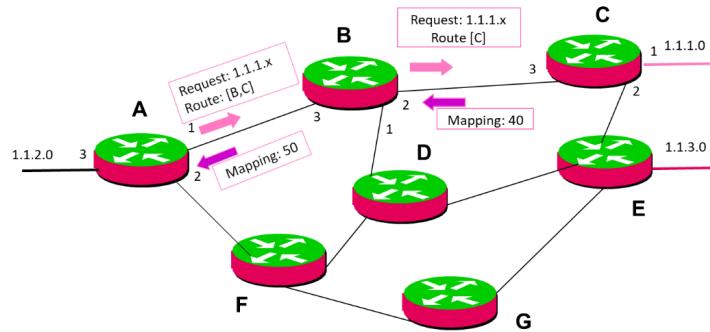


Figure 3.15: C. LDP R.

### Resource Reservation Protocol

La differenza fondamentale rispetto agli altri due e' che in questo caso non sono i singoli nodi a stabilire le label: Il nodo sorgente invia una richiesta di path (con percorso esplicito) al destinatario, il quale procede lui a calcolare le label da distribuire e poi le assegna tramite una risposta che fluisce fino al mittente.

Un'altra particolarita' di questo protocollo e' che puo' fare uso del TED (in questo caso si parla di RSVP-TE). In questo modo si puo' distribuire il carico del flusso in modo equo o intelligente lungo la topologia della rete.

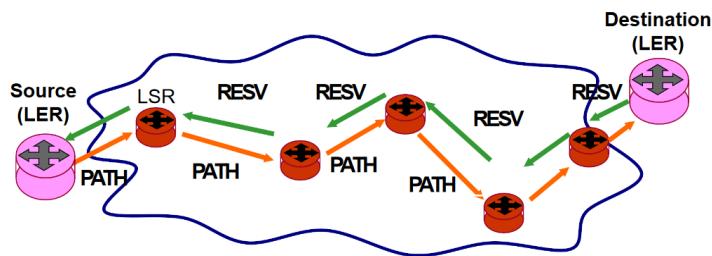


Figure 3.16: RSVP

Nel caso di esempio IP avrebbe mandato tutti i flussi nel percorso piu' veloce, con evidente overload rispetto alla capacita' del canale (quindi avremmo avuto perdite o rallentamenti). Invece RSVP-TE divide il flusso in base allo stato della rete.

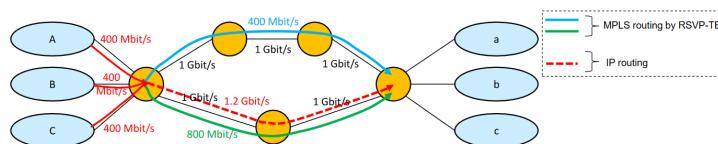


Figure 3.17: RSVP-TE /1

RSVP-TE puo' anche decidere di fare *Protection Switching*, ovvero riservare una porzione di rete alle emergenze, in modo da essere pronto a switchare l'assegnamento delle rotte per perdere meno dati possibile. Il problema di questo schema e' che occorre bilanciare la quantita' di risorse riservate nella rete per evitare di avere un throughput troppo basso oppure una bassa capacita' di recupero (esistono schemi 1-N cosi' come 1-1).

Questo tipo di recovery e' molto piu' veloce rispetto a quello dei protocolli IP perche' coinvolge solo una ristretta cerchia di nodi che devono cambiare una label in modo dinamico, non e' richiesta la riconfigurazione di tutta la rete ...

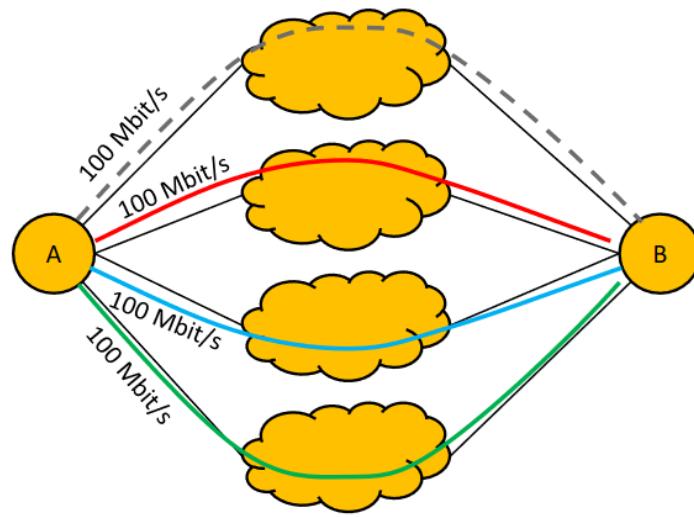


Figure 3.18: RSVP-TE /2

# Chapter 4

## Virtual Private Network

Le VPN sono reti private virtuali estese dal punto di vista geografico ma che si implementano su un'infrastruttura pubblica anziché privata.

In alternativa è possibile che siano implementate come livello aggiuntivo al MPLS di un ISP.

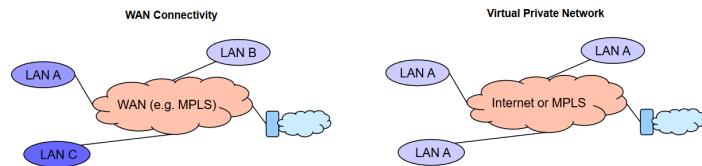


Figure 4.1: VPN /1

- **Trusted VPN:** sono tipicamente gestite dagli ISP, i quali garantiscono eventualmente requisiti di servizio (quality of service) ma non si occupano di nessun meccanismo di sicurezza particolare.
- **Secure VPN:** offerte dai VPN providers o configurate da aziende e istituzioni, le quali implementano protocolli di cifratura per la sicurezza delle trasmissioni (ma non garantiscono livelli di servizio).
- **Hybrid VPN:** una soluzione ibrida gestita dagli ISP.

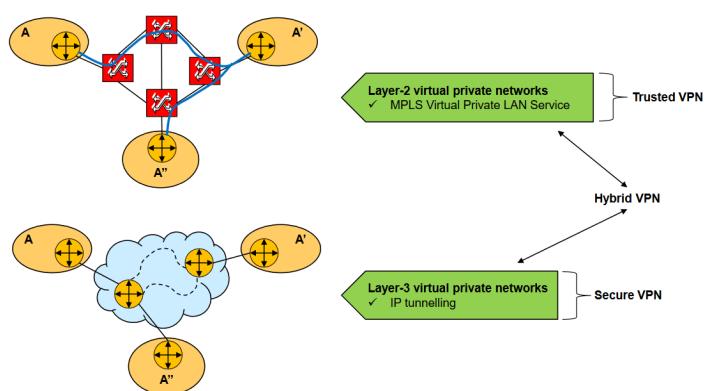


Figure 4.2: VPN /2

## 4.1 MPLS VPN

La rete MPLS si comporta come un'infrastruttura di Switch, pertanto trasporta direttamente i frame Ethernet. I cavi tra gli switch virtuali sono detti "pseudowires". Si adotta un meccanismo *L2 learning & forwarding* per instradare i pacchetti come nel livello collegamento.

E' vantaggioso per connettere i Datacenter.

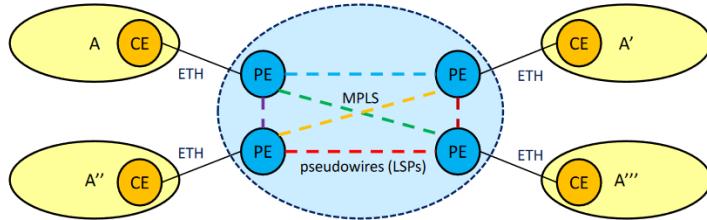


Figure 4.3: VPN on top of MPLS

## 4.2 IP Tunneling

I pacchetti sono incapsulati (ed eventualmente cifrati) all'interno di ulteriori pacchetti IP e viaggiano in maniera trasparente sulla rete.

Questa modalita' di esercizio e' compatibile con la creazione di reti virtuali (per esempio quella usata durante le gare della cyberchallenge) per fornire accesso "simil-locale" a nodi geograficamente separati.

Chiaramente rispetto ad MPLS questo schema e' meno efficiente e flessibile ma e' un tradeoff col fatto che non richiede infrastrutture particolari e puo' essere implementato direttamente sul il livello di rete IP.

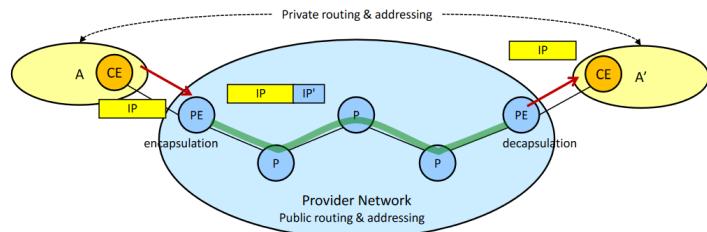


Figure 4.4: VPN by IP T.

## 4.3 Virtual Local Area Networks

Sono reti virtuali create per dividere logicamente porzioni di una rete come se fossero "stanze". E' il meccanismo tipico di aziende, istituzioni ed edifici sensibili che richiedono separazione netta del traffico tra terminali per evitare problemi di sicurezza. Sono facili da riconfigurare.

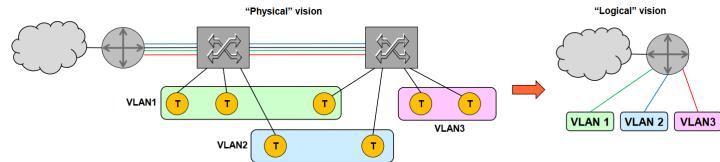


Figure 4.5: VLAN

Questa e' implementata in Ethernet tramite l'aggiunta di 4 byte per segnalare priorita' del traffico e VLAN di appartenenza.

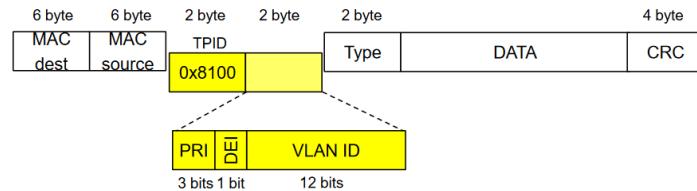


Figure 4.6: Ethernet VLAN

Dal punto di vista dell'infrastruttura e' richiesto che gli switch siano VLAN-Aware, mentre i terminali possono non esserlo e in quel caso gli switch appenderanno i famosi 4 byte per loro nelle trame ethernet.

# Chapter 5

## Dispositivi di Rete

In questa parte si vedono i dispositivi elementari della rete che concernono sia il forwarding/routing (Hub, Switch ... etc) sia altre funzioni importanti di sicurezza e bilanciamento della rete (Firewall, IDS ... etc).

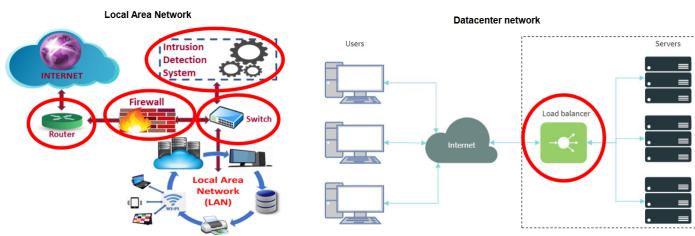


Figure 5.1: Dispositivi di Rete in contesti diversi (non necessariamente distinti)

Tutti i device tradizionali includono un piano dati (che si occupa del movimento da dove, per dove e quali dati nella rete) e un piano di controllo (che amministra gli invii di materiale, stabilendo policy e rotte per esempio).

Il primo tipo di operazioni deve essere velocissimo per favorire il flusso di dati, mentre il secondo puo' essere piu' lento ma comunque in tempi ragionevoli per garantire una risposta adeguata del sistema (di solito sono operazioni complesse che richiedono coordinamento tra nodi).

Entrambi i piani prevedono lo scambio di messaggi, ma nel primo caso sono pacchetti dati, nel secondo di pacchetti di controllo.

### 5.1 Forwarding/Routing Devices

#### 5.1.1 Router

Il piano di controllo del router aggiorna la tabella di routing ( $IP \rightarrow$  Interfaccia di uscita) eseguendo protocolli di instradamento distribuiti (BGP, OSPF ...), e calcolando il percorso migliore per raggiungere ogni destinazione.

Quando un pacchetto dati arriva nel piano dati, si cerca una regola nella tabella di routing (longest prefix wins) e si instrada il pacchetto sulla interfaccia di uscita corrispondente. Se nessuna regola e' trovata, il pacchetto viene scartato.

In piu' possono essere effettuate anche operazioni sui metadati (decremento del TTL).

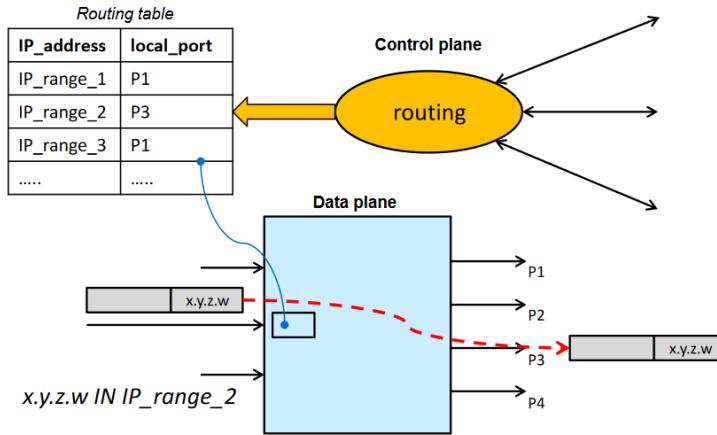


Figure 5.2: Control/Data Plane

Nel dettaglio l'architettura del Router si compone anche di un'infrastruttura di instradamento ad alte prestazioni (*Switching Fabric*) e di algoritmi di scheduling e code per inviare i pacchetti nelle interfacce.

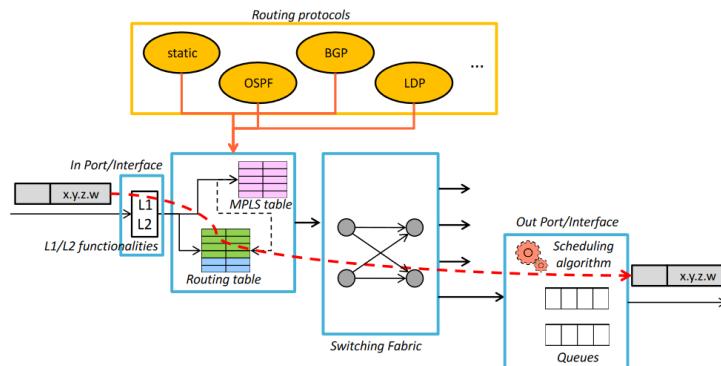


Figure 5.3: Architettura del Router

La scelta della regola corretta nella tabella di routing si basa sul Longest Prefix, come detto prima, ma anche su preferenze rispetto al protocollo che le ha generate, così come le metriche sulla distanza e un algoritmo di distribuzione del carico sulle interfacce.

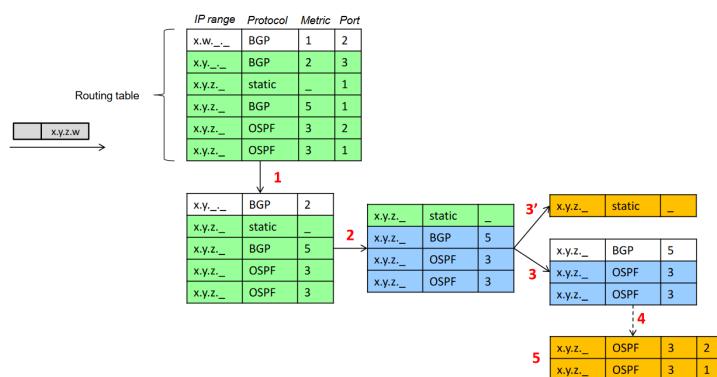


Figure 5.4: Forwarding Process

### 5.1.2 Switch

Quando un pacchetto arriva nel piano dati, si cerca una regola nella tabella di forwarding (MAC → Interfaccia di uscita). Se esiste si invia il pacchetto in quella uscita, altrimenti si esegue il *Flooding*, ovvero si invia il pacchetto in broadcast, in tutte le uscite.

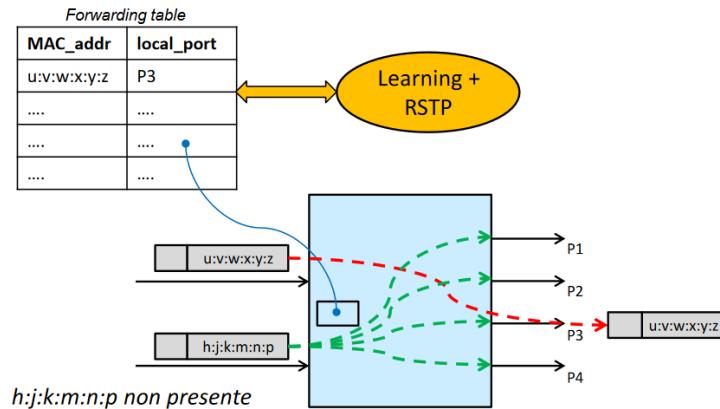


Figure 5.5: Control/Data Plane

Il Flooding e' pericoloso perche' si rischia di incorrere in cicli lungo la rete di invio dei suddetti pacchetti. Per risolvere questo problema il piano di controllo fa uso del RSTP, che riduce la topologia logica della rete ad un albero di switch (chiudendo alcune porte nei collegamenti tra switch al flooding).

Oltre a RSTP come visto in precedenza, il piano di controllo fa uso di algoritmi L2 Learning & Forwarding per riempire la tabella di forwarding.

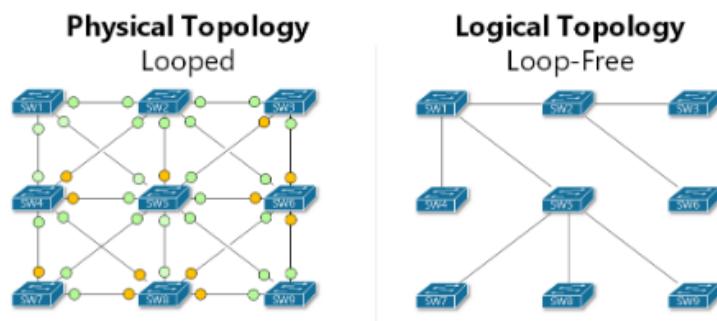


Figure 5.6: Rapid Spanning Tree Protocol

Anche qui l'architettura ha uno Switching Fabric e algoritmi di scheduling. Le similitarita' con il router non sono casuale, sono le basi per il SDN.

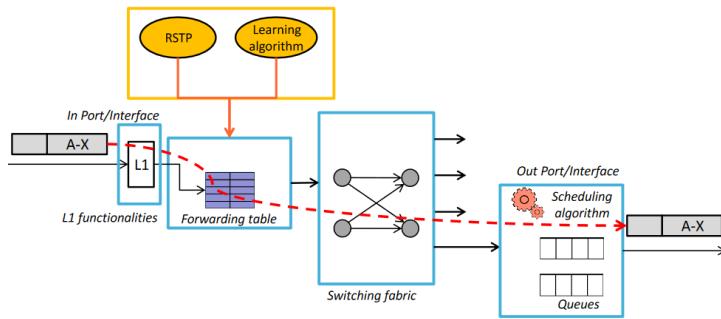


Figure 5.7: Architettura dello Switch

## 5.2 Middleboxes

### 5.2.1 Firewall

Il firewall e' un dispositivo in linea, ovvero riceve ogni pacchetto e lo inoltra lui stesso nella sottorete di destinazione (e pertanto richiede hardware dedicato ad alte prestazioni). Di default scarta i pacchetti, ma puo' essere istruito con regole (o *policy*) per accettare, scartare (notificando il mittente), rigettare (non notificandolo), loggare le informazioni sul pacchetto.

Una regola tipo e' qualcosa del genere: *set policy id <#> from <zonein> to <zoneout> <addin> <addout> <protocol/port> <action>*.

Il firewall e' anche un dispositivo stateful, ovvero tiene traccia delle richieste e delle connessioni, quindi per esempio accetta SYNACK solo da porte TCP per cui si e' inviato SYN.

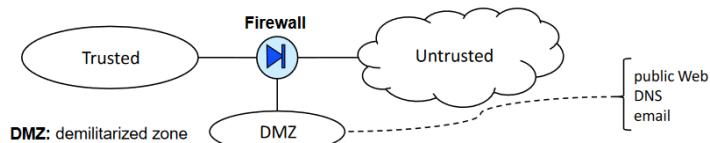


Figure 5.8: Firewall

### 5.2.2 Intrusion Detection System

L'IDS e' un dispositivo non in linea che riceve una copia di tutti i pacchetti che arrivano nella sottorete ed effettua operazioni di controllo complesse (anche molto costose) che permettono di individuare efficacemente le intrusioni. Se ne rileva una notifica allo switch le azioni da eseguire per determinati pacchetti successivi a quelli che ha letto (non ha controllo su quanto passato prima).

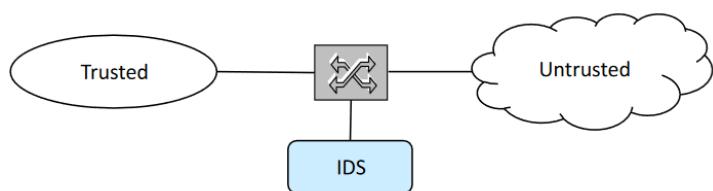


Figure 5.9: IDS

Spesso e' configurabile a regole come il Firewall.

```
Syntax of a rule (Snort)
• <action> <protocol> <IP> <port> -> <IP> <port> <options>
  o <action>: pass, alert, log, drop, reject
  o <protocol>: TCP, UDP, ICMP, IP
  o <IP> and <port>: IP and port ranges
  o <options>: general, payload detection, non-payload detection, post-detection
    □ general: generate/send specific messages to the admin
    □ payload detection: options related to the payload of the packet
    □ non-payload detection: options related to the headers of the packet - IP (TTL, fragment, options, length), TCP (flags, ack), ...
    □ post-detection: logging, user data extraction, ...

Example: alert TCP any 21 -> 10.199.12.8 any (msg: "FTP Traffic Detected");
```

Figure 5.10: Regole di Snort

### 5.2.3 Anti-DDOS

Questi sistemi cercano di filtrare le richieste in modo da scartare eventuali flussi malevoli che cercano di effettuare DDOS. Puo' essere implementato come meccanismo dall'ISP (di fronte pagamento) o applicato da una rete cloud dedicata che analizza e pulisce il traffico.

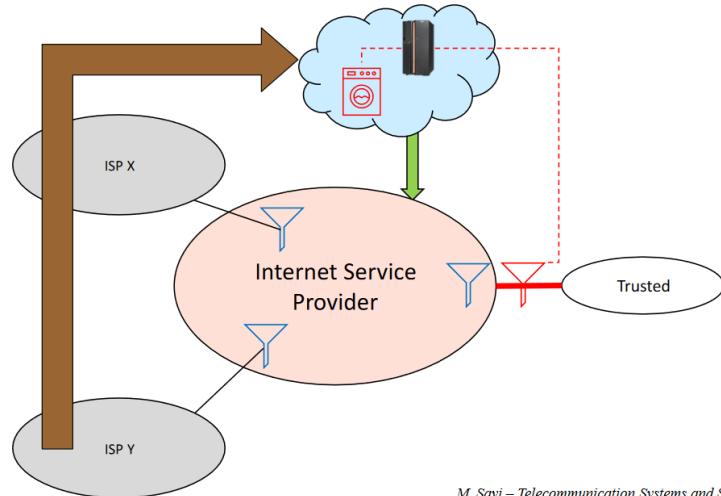


Figure 5.11: Anti-DDOS

### 5.2.4 Load Balancer

Il Load Balancer risolve un problema tipico di chi distribuisce contenuti a milioni di utenti: bilanciare le richieste sui server che provvedono ad esse per evitare overload.

Esistono soluzioni:

- Network based: CDN, Caching, DNS load balancing
- Application-based: reverse proxy
- **Hardware-based:** Load balance middleboxes

In quest'ultimo troviamo un hardware dedicato che divide le richieste sui server disponibili con algoritmi di bilanciamento rigidi (Round Robin) o adattivi in base ai tempi di risposta o ai livelli di carico dei server.

Inoltre si deve anche preoccupare di mantenere le sessioni, ovvero fare in modo che le richieste di una sessione vadano tutte allo stesso server. La cosa non e' banale e

discriminare solo in base all'IP spesso non basta (posso avere tanti nodi che inviano traffico sotto lo stesso indirizzo pubblico), si ricorre quindi per esempio ai cookie.

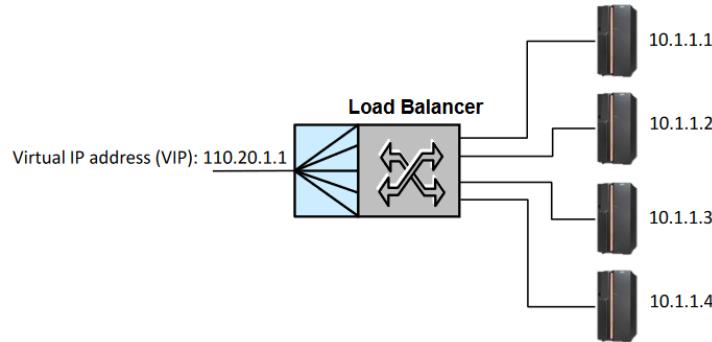


Figure 5.12: Load Balancer

### 5.3 Software Defined Networking

Molti dispositivi di rete visti in questa sezione avevano la medesima struttura: un piano di controllo che esegue algoritmi per aggiornare una serie di regole, un piano dati che esegue le suddette regole ed instrada i pacchetti con uno Switching Fabric.

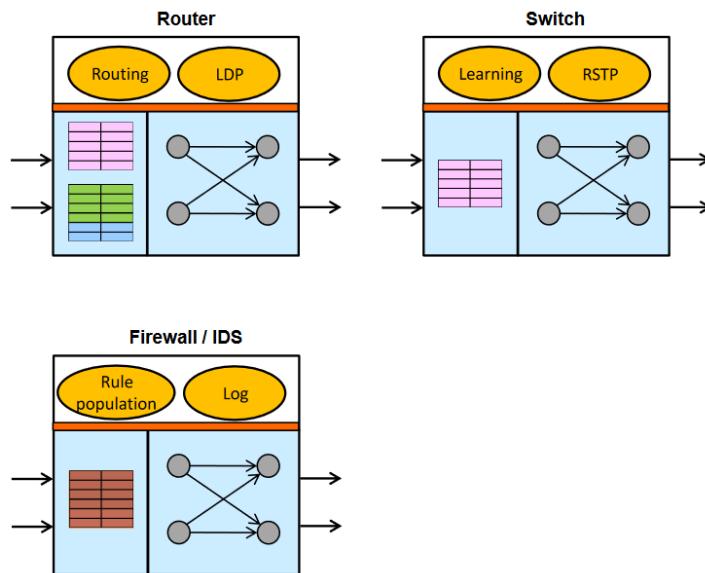


Figure 5.13: Coupled

L'idea quindi e' di generalizzare questo modello disaccoppiando fisicamente, quindi non solo logicamente, questi due piani. L'infrastruttura di rete quindi diventa "programmabile", con un **SDN controller** centrale che applica gli algoritmi necessari e conosce la topologia della rete, con delle Southbound Interfaces (SBI) che implementano i collegamenti tra gli "switch" del SDN e il controller, delle Northbound Interfaces (NBI) che implementano il collegamento tra il controller e i servizi di rete. Infine abbiamo gli switch che applicano le regole suddette con paradigma *match + action*.

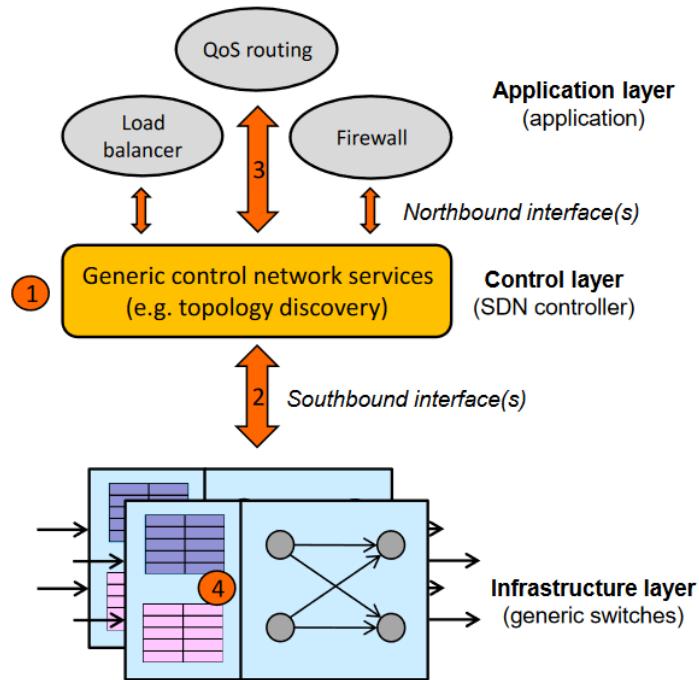


Figure 5.14: Decoupled

### 5.3.1 Protocollo OpenFlow

OpenFlow è un protocollo per realizzare SDN.

Abbiamo degli "Switch" (termine strano visto che operano dal livello 2 al 4, per la gioia degli inventori dello stack ISO/OSI e dei relativi studenti), che possiedono una *pipeline* di **Flow Table** (almeno una, le quali definiscono le regole di azione), una Group Table (gestisce le comunicazioni multicast, comprese le istruzioni di flooding) e una Meter Table (mantiene delle statistiche sullo switch).

I **Channel** permettono ai Controller di aggiornare le Flow Table.

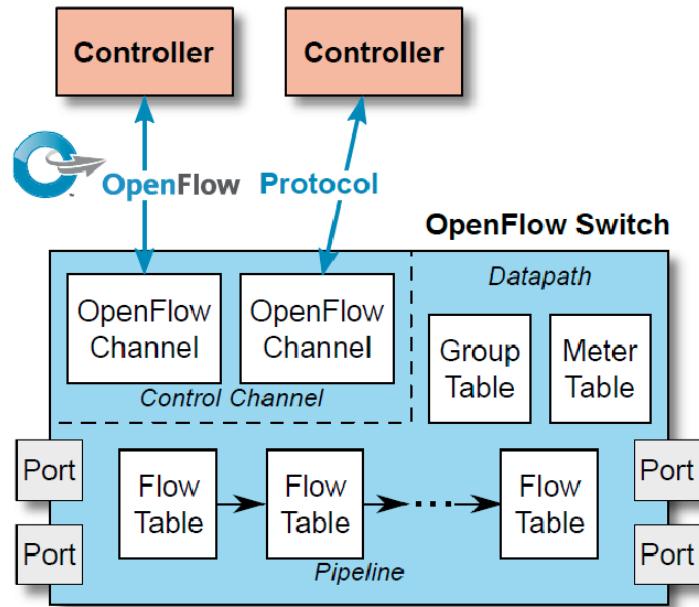


Figure 5.15: Architettura OpenFlow

### Flow Table

Le Flow Table sono attraversate in ordine crescente e possono eseguire azioni condizionate da **metadata** (compreso l'aggiornamento dei suddetti metadati).

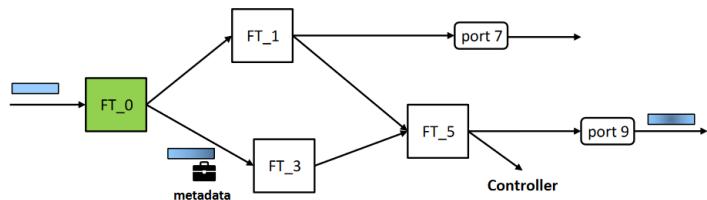


Figure 5.16: Pipeline delle Flow Table

Un esempio di Flow Table:

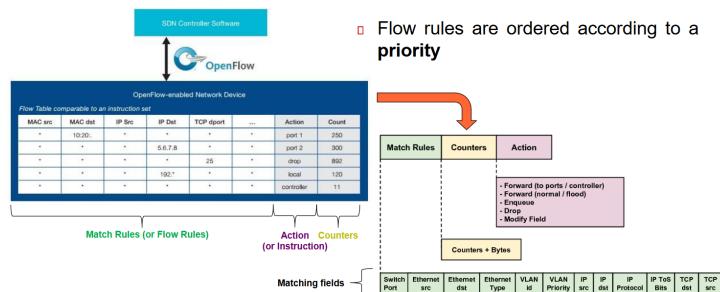


Figure 5.17: Regole delle Flow Table

Si riportano solo alcuni campi, ma quelli disponibili (in base alla versione della specifica) sono veramente tanti.

IN_PORT	TCP_SRC
IN_PHY_PORT	TCP_DST
ETH_DST	UDP_SRC
ETH_SRC	UDP_DST
ETH_TYPE	ICMPV4_TYPE
VLAN_VID	ICMPV4_CODE
VLAN_PCP	IPV6_SRC
IP_DSCP	IPV6_DST
IP_ECN	IPV6_FLABEL
IP_PROTO	MPLS_LABEL
IPV4_SRC	TCP_FLAGS
IPV4_DST	ACTSET_OUTPUT

Figure 5.18: Altri campi delle Flow Table

Lo stesso si puo' dire con le azioni e le istruzioni che possono essere accoppiate nel campo *Action* delle Flow Table.

- Instructions
  - APPLY ACTIONS 
  - CLEAR ACTIONS 
  - WRITE ACTIONS 
  - GO TO TABLE
  
- Actions
  - OUTPUT → Forward to a port or to the controller
  - DROP → Drop the packet
  - SET-QUEUE → Set the output queue
  - PUSH-TAG/POP-TAG (VLAN, MPLS, ...) → Set/remove specific tags
  - SET-FIELD → Set the value of a specific header field
  - COPY\_FIELD → Copy the header field
  - CHANGE-TTL → Change the TTL
  - ...

Figure 5.19: Azioni/Istruzioni delle Flow Table

## Configurazione

Le Flow Table possono essere istanziate dal Controller quando si accendono gli switch e poi piu' modificare (**Proactive Conf.**) oppure l'opposto, venire popolate durante l'esecuzione della rete partendo da vuote (**Reactive Conf.**).

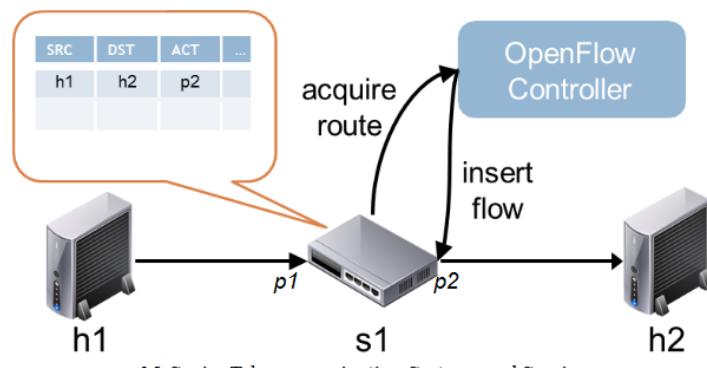


Figure 5.20: Configurazione Reattiva

Tipicamente quello che accade e' una situazione mista.

### 5.3.2 SDN + SWAN

Quello che posso ottenere applicando i principi di SDN alle reti WAN e' che posso pagare per avere piu' servizi in parallelo e poi utilizzare un controller che modula i collegamenti tra Customer Premises Equipment (*CPE*) in base alle prestazioni o all'uso che voglio fare di suddette reti (per esempio minimizzare l'uso di MPLS che costa un pacco).

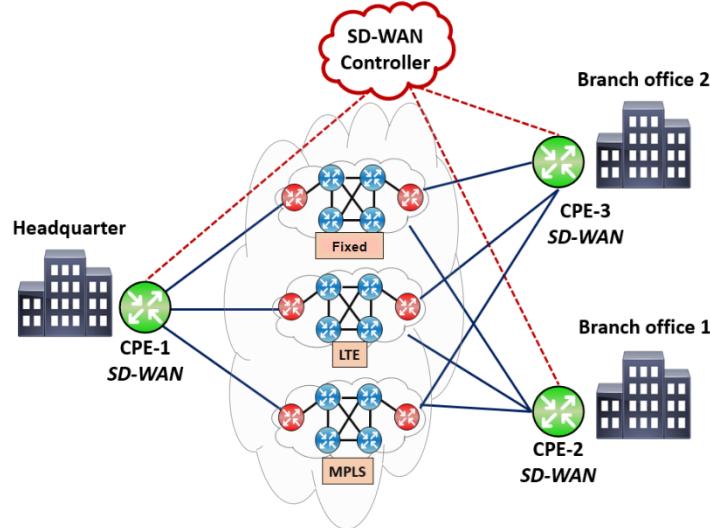


Figure 5.21: SD-WAN

### 5.3.3 Data Plane Programming

Il problema di OpenFlow e di tutte le soluzioni hardware based e' che se devo cambiare, aggiungere o togliere cambi devo modificare anche il pezzo di hardware che lo esegue. Si puo' fare un passo avanti a SDN per ottenere un'interfaccia completamente programmabile graize ai protocolli **PSA** e **PISA**.

Chiaro che soluzioni con hardware dedicato sono piu' performanti, ma non e' il punto del discorso.



Figure 5.22: Si, PISA

Fondamentalmente posso personalizzare il parser di pacchetti tramite un domain specific language (P4) e un compilatore per ottenere un parser programmato ad hoc molto flessibile.

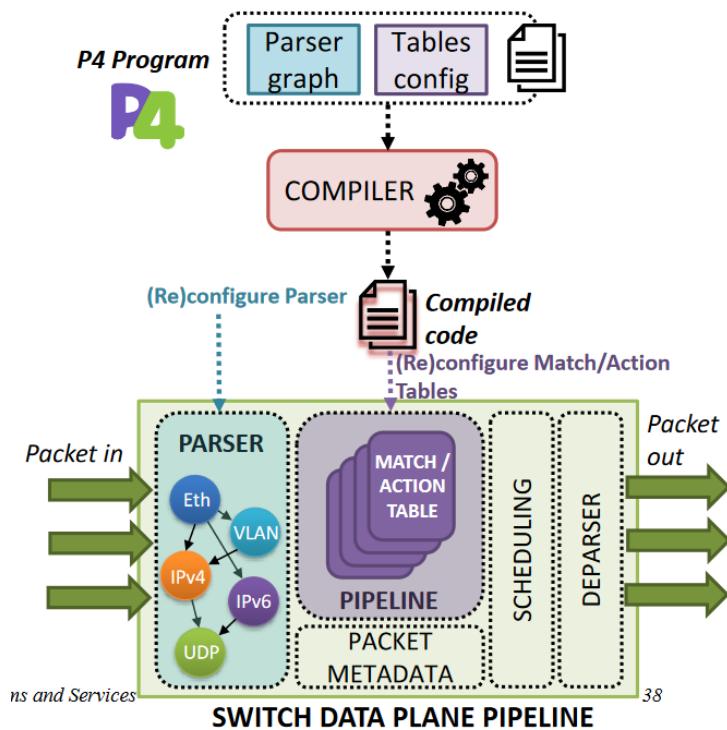


Figure 5.23: P4

### 5.3.4 In-Band Network Telemetry

Un'esempio di applicazione di DPP e' proprio questo. Fondamentalmente durante le operazioni di rete tengo traccia programmaticamente le operazioni svolte per tracciare delle metriche sull'uso degli switch e dei dispositivi di rete.

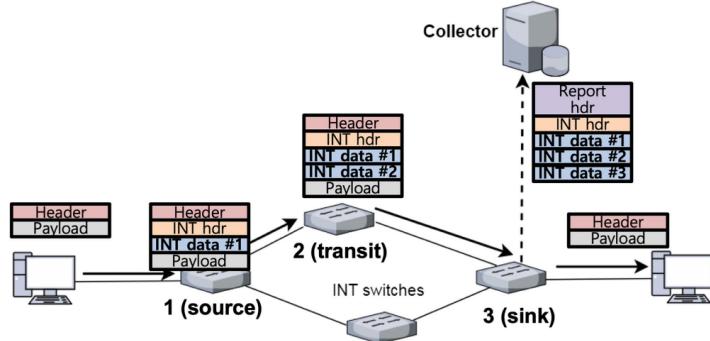


Figure 5.24: IBNT

## 5.4 Network Function Virtualization

TODO: