

**SIMULAZIONE**  
**ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE**

**Indirizzo:** ITTL - INFORMATICA E TELECOMUNICAZIONI  
ARTICOLAZIONE TELECOMUNICAZIONI

**Tema di:** TELECOMUNICAZIONI e SISTEMI E RETI

**PRIMA PARTE**

L'azienda che fornisce servizi di pubblica utilità XYZ è attualmente dislocata su due edifici, distanti circa 200 metri e collocati entro una propria area industriale, adibiti rispettivamente a sede principale, in cui è presente l'amministrazione e un CED (Centro Elaborazione Dati), e sede operativa. Per un ampliamento delle proprie attività l'azienda ha appena acquisito un terzo edificio, posto a circa 500 metri di distanza dai primi due, che sarà adibito a ufficio in cui si riceve il pubblico.

L'azienda intende ammodernare la propria infrastruttura di rete realizzando una propria intranet. A tale scopo l'azienda pubblica un bando di gara in cui vi sono, tra le altre, le seguenti richieste.

- **SOSTITUZIONE DEL CABLAGGIO IN MODO CONFORME AGLI STANDARD IN VIGORE E INTERCONNESSIONE DEGLI EDIFICI**
  - va sostituito il cablaggio verticale di edificio, attualmente realizzato con cavi in cat. 5e con un cablaggio moderno in grado di supportare velocità fino a 10 Gbit/s
  - va sostituito il cablaggio orizzontale di piano, attualmente realizzato con cavi in cat. 5 con un cablaggio in rame più moderno in grado di supportare velocità di 1 Gbit/s;
  - va sostituita la dorsale di campus che collega i due edifici, attualmente realizzata con un cablaggio in rame in cat. 5e e due ripetitori intermedi, sostituendola con un cablaggio in fibra ottica multimodale;
  - il terzo edificio, appena acquisito, va connesso in rete con gli altri due edifici in modalità wireless, attraverso due distinte connessioni radio punto-punto in quanto la connettività tra gli edifici è ritenuta di fondamentale importanza (mission critical);
- **AMPLIAMENTO E RICONFIGURAZIONE DELLA RETE AZIENDALE**
  - va definito un nuovo piano di indirizzamento per tutte le sottoreti che compongono l'intranet;
  - vanno acquistati e configurati:
    - apparati di rete di livello 2 che consentano una segmentazione logica, a livello 2, della rete;
    - apparati di rete con funzioni di livello 3, da porre in ciascun edificio, per realizzare una rete intranet ad alta affidabilità, tale per cui anche nel caso in cui la connessione tra un edificio e l'altro cada sia possibile comunque accedere alle risorse informatiche interne e ad Internet.
- **ULTERIORI SPECIFICHE:**
  - per motivi di sicurezza deve esserci un unico accesso a Internet, posto nella sede principale;
  - il personale che opera nei diversi edifici deve poter comunicare in rete e avere accesso alle risorse informatiche interne, ma solo con computer connessi in modo cablato;

- Nella sede principale deve essere disponibile una connessione Wi-Fi tramite cui si può solamente accedere a Internet, ma non accedere alle risorse informatiche interne.
- Nella sede principale è presente un sistema di videosorveglianza con telecamere IP, i cui flussi video devono essere inviati a un server video e a un PC di monitoraggio posti in una apposita sala della sede principale.

#### DATI DI PROGETTO

- Dispositivi informatici collegati in rete nella sede principale:
  - N. 2 stampanti di rete multifunzione;
  - N. 2 computer server per il CED;
  - N. 1 server video + 1 PC di monitoraggio
  - N. 15 computer per il personale
  - N. 4 telecamere IP con alimentazione PoE
- Dispositivi di utente collegati in rete nella sede operativa:
  - N. 8 computer
  - N. 1 stampante di rete multifunzione
- Dispositivi di utente collegati in rete nell'ufficio aperto al pubblico:
  - N. 6 computer
  - N. 1 stampante di rete multifunzione
- tutti i dispositivi di rete che si propongono devono essere di tipo amministrabile (manageable).

Il candidato, formulata ogni ipotesi aggiuntiva che ritiene opportuna, produca quanto segue.

- a) Proponga e discuta un progetto per l'ammmodernamento dell'infrastruttura di rete, illustrandone con un disegno la topologia fisica, specificando quale cablaggio conforme agli standard intende proporre, quali apparati di rete intende utilizzare all'interno di ciascuno dei tre edifici e a quali tecnologie/standard essi devono essere conformi; indichi infine quali apparati aggiuntivi (o funzioni di rete integrate) sono necessari per interconnettere le reti dei tre edifici a livello 3;
- b) con adeguate motivazioni proponga una descrizione operativa di massima della configurazione degli apparati di rete di livello 2 che consentano la segmentazione logica della rete della sede principale;
- c) identifichi il numero di sottoreti di livello 3 (subnet IP) che devono far parte della rete aziendale (intranet), evidenziandone le dimensioni in termini di indirizzi IPv4 totali che ciascuna di esse deve rendere disponibili. Quindi proponga un piano di indirizzamento IPv4 ottimizzato che, partendo da un unico blocco di indirizzi IPv4 privati, opportunamente scelto e suddiviso, consenta di assegnare gli indirizzi IPv4 a tutte le sottoreti e a tutti i dispositivi ed apparati che fanno parte dell'intranet.
- d) Proponga una configurazione delle scelte di instradamento (routing) effettuabili dagli apparati di rete di livello 3 che interconnettono le reti degli edifici in modo da soddisfare i requisiti di progetto con particolare riferimento alla tolleranza della eventuale caduta di uno dei collegamenti.

Discuta almeno due dei seguenti punti.

1. calcoli la latenza da server FTP a client che si ha con la vecchia infrastruttura quando un dispositivo di utente (client) posto nella sede operativa richiede al server FTP, posto nella sede principale, un blocco di dati di applicazione (o MSS, maximum segment size) avente dimensione pari a 1460 Byte, sapendo che:

- la connettività a livello 2 è Ethernet 100BASE-TX,
  - la distanza totale è di 280 metri
  - ognuno dei due ripetitori introduce un ritardo di 5  $\mu$ s.
2. sapendo che per la nuova dorsale, lunga complessivamente 280 m, si impiega un sistema su fibra ottica (f.o.) multimodale avente le caratteristiche riportate in figura, in cui i connettori alle estremità della f.o. introducono ciascuno un'attenuazione massima di 0,75 dB e vi sono due giunti, ciascuno dei quali introduce un'attenuazione massima di 0,2 dB, calcolare
- il livello di potenza che si ha in ricezione e il margine rispetto alla sensibilità del rivelatore ottico;
  - la banda utile della fibra ottica e la sua capacità trasmissiva massima teorica

Sorgente ottica			
VCSEL Parameters	Typ.	Max.	Units
Fiber coupled optical power	600		$\mu$ W
RMS Spectral Bandwidth		0.4	nm
Rise/Fall Time		40	ps

Fibra ottica multimodale	
Standards Compliance	
ISO/IEC 11801	Type OM4 fiber
<b>Optical Specifications</b>	
<b>Bandwidth</b> (MHz·km)	
4700	
<b>Attenuation</b>	
Wavelength (nm)	Maximum Value (dB/km)
850	$\leq 2.3$

Rivelatore ottico			
Parameter	Symbol	Typ.	Unit
<b>PIN Diode</b>			
Detection wavelength	$\lambda_0$	850	nm
Responsivity	R	0.6	A/W
Sensitivity	S	-20	dBm
Rise/Fall time <sup>1</sup>	$t_r$	100	ps

3. Valuti l'affidabilità a livello trasmissivo di un sistema di interconnessione wireless fra il sito principale e l'ufficio aperto al pubblico avente le seguenti caratteristiche:
- opera nella banda non licenziata (ISM) dei 17 GHz, con frequenza portante pari a 17,1 GHz e banda di canale pari a 80 MHz;
  - opera in trasmissione con un valore di EIRP pari a 20 dBm;
  - gli apparati posti nelle due sedi sono dotati ciascuno di antenna integrata con diametro pari a 60 cm.

La valutazione deve essere fatta calcolando il livello di potenza che si ha in ingresso al ricevitore e verificando che esso non sia inferiore a -75 dBm, anche in presenza di un'attenuazione dovuta al fading di 18 dB.

4. Proponga una modalità di implementazione e una configurazione per il servizio di rete che consente la configurazione automatica dei dispositivi utente (client) collegati in modo cablato di una sottorete IP a sua scelta, facendo però in modo che gli indirizzi IPv4 assegnati siano statici e illustri le fasi con cui avviene l'assegnazione degli indirizzi stessi all'accessione dei client.

## SECONDA PARTE

Il candidato scelga due tra i seguenti quesiti e per ciascun quesito scelto formuli una risposta della lunghezza massima di 20 righe (esclusi disegni e grafici).

1. Illustri le possibili alternative che vi sono per dotare di un accesso a Internet a banda larga o (preferibilmente) ultralarga una rete aziendale; proponga quindi la soluzione che a suo motivato parere è più indicata per l'unico accesso Internet, condiviso dalle reti di tutti gli edifici, che l'azienda desidera avere e che va posto nella sede principale.
2. Descriva quali sono le principali misure di sicurezza da prendere a difesa della rete aziendale; illustri quindi, avvalendosi anche di disegni, in che modo il server FTP locale potrebbe essere esposto in modo sicuro su Internet e reso accessibile con comunicazioni protette solo dal personale dell'azienda che opera da remoto.
3. Illustri le caratteristiche generali delle modulazioni M-QAM, proponga lo schema di un modulatore 16-QAM e calcoli il bit rate (o velocità di informazione) e il symbol rate (o baud rate o velocità di modulazione) che tale modulatore consente di ottenere quando la banda a disposizione è pari a 350 kHz.
4. Descriva una possibile soluzione per interconnettere in modo protetto, sicuro e a costi non eccessivi una porzione della rete aziendale con una sottorete remota di un'azienda partner situata in un'altra regione italiana.

---

Durata massima della prova: 6 ore.

È consentito l'uso di manuali tecnici e di calcolatrici non programmabili.

---

Simulazione a cura del prof. Onelio Bertazioli Pagina 4

© Zanichelli Editore S.p.A., 2019

È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.  
Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

### SOLUZIONE<sup>1</sup>

- a) Proponga e discuta un progetto per l'ammodernamento dell'infrastruttura di rete, illustrandone con un disegno la topologia fisica, specificando quale cablaggio conforme agli standard intende proporre, quali apparati di rete intende utilizzare all'interno di ciascuno dei tre edifici e a quali tecnologie/standard essi devono essere conformi; indichi infine quali apparati aggiuntivi (o funzioni di rete integrate) sono necessari per interconnettere le reti dei tre edifici a livello 3;

Dal punto di vista fisico il progetto della nuova infrastruttura di rete potrebbe essere così definito.

- Cablaggio conforme agli standard del cablaggio strutturato, con le seguenti caratteristiche:
- cablaggio verticale con f.o. multimodale graded index a standard OM3 o OM4, oppure, in subordine, cablaggio in rame con cavi F/FTP in cat. 6a;
  - cablaggio orizzontale con cavi in rame F/UTP in cat. 6 o cat. 6a;
  - dorsale in f.o. multimodale graded index a standard OM4.

Lo schema di principio generale del cablaggio strutturato è il seguente (Cap. 2 Par. 4 vol. 2 del libro di testo)

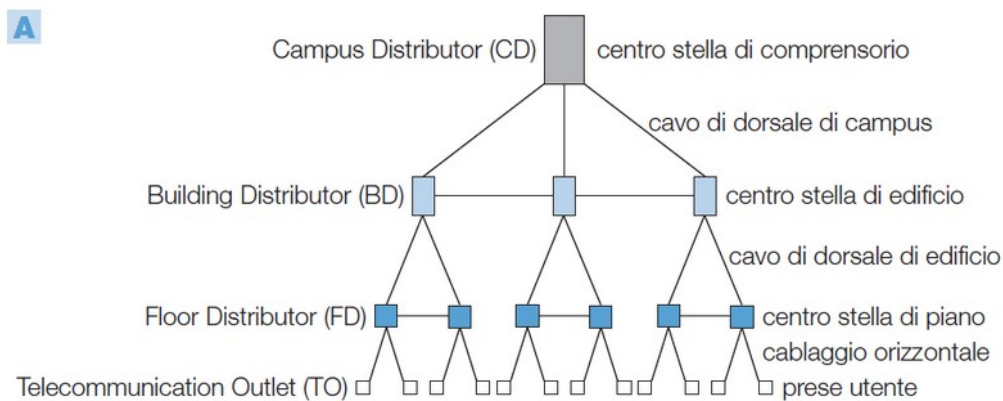


FIGURA 18 A) Schema di principio di un sistema di cablaggio strutturato.

Nel caso proposto può quindi essere rappresentato nel seguente modo:

<sup>1</sup> Le soluzioni proposte sono più dettagliate di quanto normalmente richiesto per la prova di un candidato.

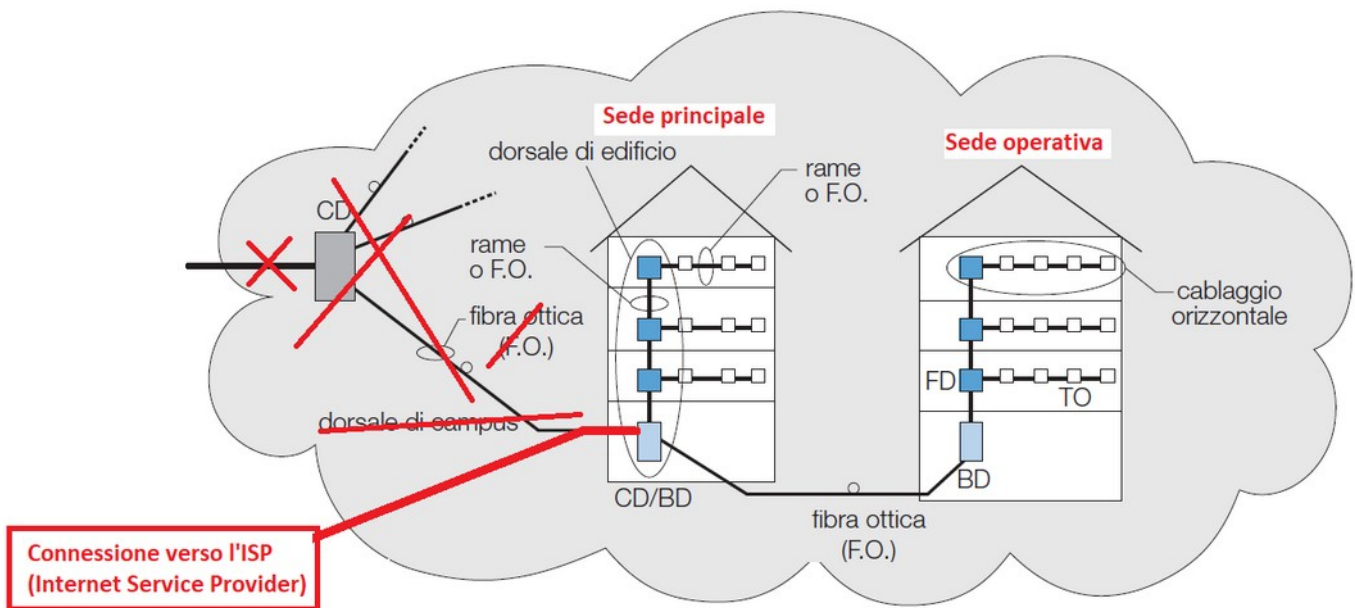


FIGURA 19 Schematizzazione del cablaggio di campus.

➤ Apparati di rete da impiegare

- **switch Layer 2 amministrabili** con porte a standard 100/1000BASE-T per la connessione con i dispositivi utente cablati e con porte a 10 Gbit/s per l'interconnessione diretta con altri eventuali switch;
- **router** (o **switch layer 3**) oppure funzionalità di router integrate nei sistemi wireless di interconnessione tra gli edifici con porte almeno a 1 Gbit/s;
- **Access point a standard 802.11ac/n** per l'accesso Wi-Fi, con funzionalità PoE (Power over Ethernet), con gestione centralizzata (preferibilmente in cloud) e controllo completo degli accessi.

Per l'interconnessione a livello 3 delle reti dei tre edifici è possibile impiegare dei router oppure degli switch Layer 3 o, per le connessioni wireless, degli apparati radio che integrino anche la funzione di router.

In modo semplificato l'infrastruttura di rete che si viene a realizzare può essere così rappresentata.



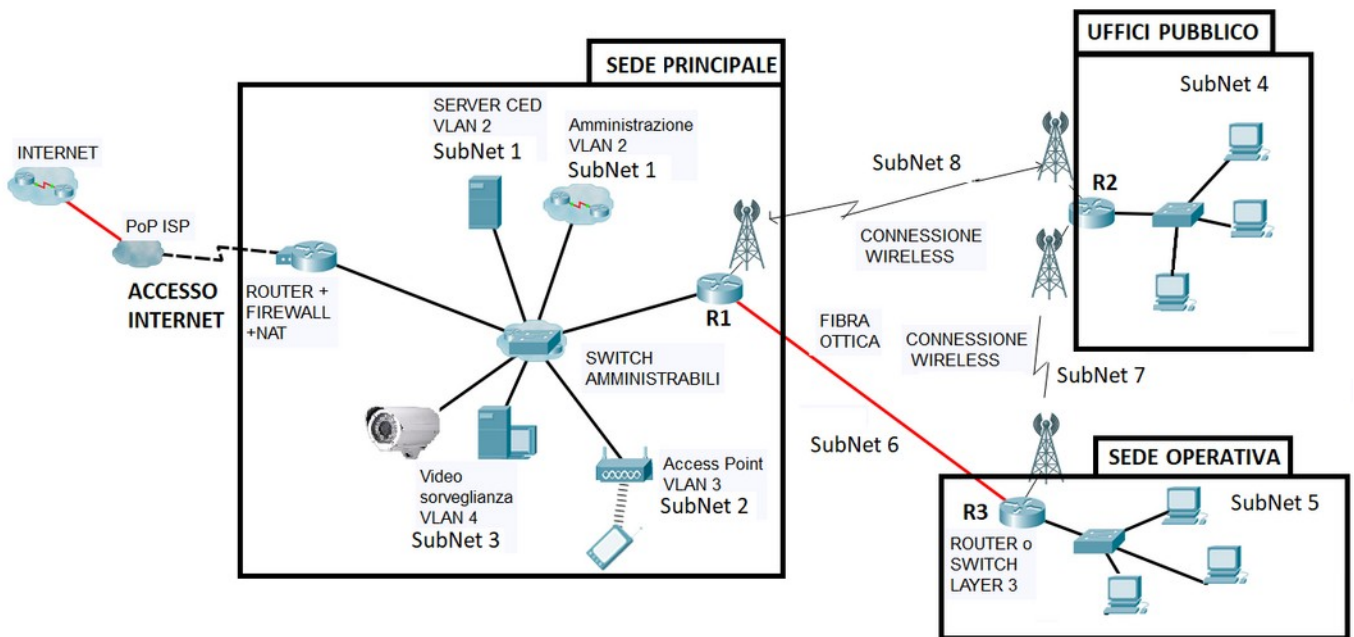


FIGURA 2 Schema semplificato dell'infrastruttura di rete

b) Con adeguate motivazioni proponga una descrizione operativa di massima della configurazione degli apparati di rete di livello 2 che consentano la segmentazione logica della rete della sede principale.

La segmentazione logica della rete della sede principale, così come quella delle altre sedi, può essere realizzata a livello 2 OSI impiegando degli **switch amministrabili** in modo da poter creare diverse **VLAN** (Virtual LAN). In particolare possono essere create almeno le seguenti VLAN:

- una VLAN che permette la comunicazione tra i PC e i server connessi in modo cablato, configurata per esempio come **VLAN 2**;
- una VLAN che permette la comunicazione tra l'access point Wi-Fi e il router tramite cui si accede a Internet, per concedere solo l'accesso a Internet ai dispositivi mobili, configurata per esempio come **VLAN 3**;
- una VLAN che permette la comunicazione tra le telecamere IP, il server video e il PC di monitoraggio, configurata per esempio come **VLAN 4**.

Può poi essere definita un'ulteriore VLAN riservata all'amministratore di rete per la configurazione e il monitoraggio degli apparati di rete.

In linea di massima la configurazione degli switch Layer 2 che consente la segmentazione logica dell'infrastruttura di rete può essere fatta con i seguenti passaggi:

1. si creano le VLAN assegnando loro un identificativo numerico (VLAN 2 ecc.) e una denominazione che ne descriva sinteticamente lo scopo (es. VLAN 2 name cablata)
2. si configurano come porte di accesso le porte collegate ai dispositivi appartenenti a ciascuna VLAN (es. "Interface Gi 0/10 → switchport mode access") e si configurano le porte stesse come appartenenti alle rispettiva VLAN (es. "Interface Gi 0/10 → switchport access VLAN 2")
3. sui router connessi agli switch si configurano delle ACL (*Access Control List*) che non consentono al router di instradare i pacchetti tra subnet IP mappate su VLAN diverse;
4. nel caso vi siano più switch interconnessi si configurano come *trunk* le porte che interconnettono gli switch (es. "Interface Gi 0/24 → switchport mode trunk"), così

come va configurata come trunk l'interfaccia (su cui si possono creare delle sottointerfacce) del router tramite cui si accede a Internet.

- c) identifichi il numero di sottoreti di livello 3 (subnet IP) che devono far parte della rete aziendale (intranet), evidenziandone le dimensioni in termini di indirizzi IPv4 totali che ciascuna di esse deve rendere disponibili. Quindi proponga e discuta un piano di indirizzamento IPv4 ottimizzato che, partendo da un unico blocco di indirizzi IPv4 privati, opportunamente scelto e suddiviso, consenta di assegnare gli indirizzi IPv4 a tutte le sottoreti e a tutti i dispositivi ed apparati che fanno parte dell'intranet.

Tenendo conto della segmentazione logica della sede principale e del fatto che ogni interfaccia dei router deve appartenere a una subnet IP diversa, il numero di subnet IP che devono essere configurate può essere determinato nel seguente modo:

- 3 subnet IP nella sede principale, mappate sulle 3 VLAN;
- 1 subnet per la sede operativa e 1 subnet IP per l'ufficio aperto al pubblico;
- 3 subnet IP per le interconnessioni tra i router che collegano gli edifici.

Le dimensioni delle subnet, in termini di indirizzi IPv4 che mettono a disposizione sono le seguenti:

- **Subnet 1**, numero di dispositivi da collegare: 15 PC + 2 stampanti + 2 server a cui vanno aggiunti gli apparati di rete (switch, ecc.); sono quindi necessari almeno 5 bit per la parte host degli indirizzi IP, per cui la dimensione della subnet IP deve quindi essere di **32 indirizzi IPv4** totali (30 dei quali sono disponibili per la configurazione, uno è l'indirizzo di rete e uno quello di broadcast)
- **Subnet 2**, si ipotizza che la subnet 2 sia composta esclusivamente da dispositivi mobili e che il numero massimo di dispositivi che si possono collegare sia pari a 30, per cui la dimensione della subnet 2 è di **32 indirizzi IPv4** totali, dei quali 30 sono configurabili; l'indirizzo IP dell'Access Point non appartiene a questa subnet;
- **Subnet 3**, numero di dispositivi da collegare: 4 telecamere + 1 server video + 1 PC; sono quindi sufficienti 3 bit per la parte host degli indirizzi IP per cui la dimensione della subnet 3 è di **8 indirizzi IP** totali, dei quali 6 sono configurabili;
- **subnet 4**, numero di dispositivi da collegare: 7, a cui vanno aggiunti due indirizzi IP uno per lo switch e uno per l'interfaccia del router; sono quindi necessari 4 bit per la parte host degli indirizzi IP per cui la dimensione della subnet 4 è di **16 indirizzi IP** totali, dei quali 14 sono configurabili;
- **subnet 5**, numero di dispositivi da collegare: 9, a cui vanno aggiunti due indirizzi IP uno per lo switch e uno per l'interfaccia del router; sono quindi necessari 4 bit per la parte host degli indirizzi IP per cui la dimensione della subnet 4 è di **16 indirizzi IP** totali, dei quali 14 sono configurabili;
- **subnet 6, subnet 7, subnet 8**; ognuna di queste subnet IP è composta da 2 soli indirizzi IP configurabili, quelli delle interfacce dei router che sono direttamente connesse, a cui vanno aggiunti l'indirizzo di rete e quello di broadcast.

Poiché complessivamente si devono avere a disposizione almeno 116 indirizzi IP da ripartire tra le varie subnet IP è possibile scegliere come blocco di partenza un blocco di indirizzi IPv4 privati con associata la subnet mask /25 (255.255.255.128), composta da 25 "1" e 7 "0", per esempio è possibile scegliere il blocco di indirizzi IPv4 **10.0.0.0/25**.



## Suddivisione del blocco 10.0.0.0/25 per la creazione delle subnet IP

Si allunga la subnet mask di 2 bit (/27 → 255.255.255.224) per suddividere il blocco in 4 parti:

- Blocco N.1 → **10.0.0.0/27, subnet mask 255.255.255.224**; la parte host degli indirizzi IP è di 5 bit per cui la subnet mette a disposizione 30 indirizzi IP configurabili, dal 10.0.0.1 al 10.0.0.30; l'indirizzo di broadcast è 10.0.0.31; questo blocco può essere usato per la **subnet IP N. 1**;
- Blocco N.2 → **10.0.0.32/27, subnet mask 255.255.255.224**; la parte host degli indirizzi IP è di 5 bit per cui la subnet mette a disposizione 30 indirizzi IP configurabili, dal 10.0.0.33 al 10.0.0.62; l'indirizzo di broadcast è 10.0.0.63; questo blocco può essere usato per la **subnet IP N. 2**;
- Blocco N.3 → **10.0.0.64/27**; può essere suddiviso in 2 parti allungando la subnet mask di 1 bit (diventa /28):
  - **10.0.0.64/28, subnet mask 255.255.255.240**; ; la parte host degli indirizzi IP è di 4 bit per cui la subnet mette a disposizione 14 indirizzi IP configurabili, dal 10.0.0.65 al 10.0.0.78; l'indirizzo di broadcast è 10.0.0.79; questo blocco può essere usato per la **subnet IP N. 4**;
  - **10.0.0.80/28, subnet mask 255.255.255.240**; ; la parte host degli indirizzi IP è di 4 bit per cui la subnet mette a disposizione 14 indirizzi IP configurabili, dal 10.0.0.81 al 10.0.0.94; l'indirizzo di broadcast è 10.0.0.95; questo blocco può essere usato per la **subnet IP N. 5**;
- Blocco N.4 → **10.0.0.96/27**; può essere suddiviso in 2 parti allungando la subnet mask di 1 bit (diventa /28):
  - **10.0.0.96/28, subnet mask 255.255.255.240**; ; la parte host degli indirizzi IP è di 4 bit per cui la subnet mette a disposizione 14 indirizzi IP configurabili, dal 10.0.0.97 al 10.0.0.110; l'indirizzo di broadcast è 10.0.0.111; questo blocco può essere usato per la **subnet IP N. 3**;
  - l'altro blocco, **10.0.0.112/28**, può essere suddiviso in 4 parti allungando la subnet mask di 2 bit (diventa /30) per ottenere le subnet IP 6, 7 e 8:
    - **10.0.0.112/30, subnet mask 255.255.255.252**; ; la parte host degli indirizzi IP è di 2 bit per cui la subnet mette a disposizione 2 indirizzi IP configurabili, dal 10.0.0.113 al 10.0.0.114; l'indirizzo di broadcast è 10.0.0.115; questo blocco può essere usato per la **subnet IP N. 6**;
    - **10.0.0.116/30, subnet mask 255.255.255.252**; ; la parte host degli indirizzi IP è di 2 bit per cui la subnet mette a disposizione 2 indirizzi IP configurabili, dal 10.0.0.117 al 10.0.0.118; l'indirizzo di broadcast è 10.0.0.119; questo blocco può essere usato per la **subnet IP N. 7**;
    - **10.0.0.120/30, subnet mask 255.255.255.252**; ; la parte host degli indirizzi IP è di 2 bit per cui la subnet mette a disposizione 2 indirizzi IP configurabili, dal 10.0.0.121 al 10.0.0.122; l'indirizzo di broadcast è 10.0.0.123; questo blocco può essere usato per la **subnet IP N. 8**;
    - il blocco 10.0.0.124/30 non viene utilizzato.

- d) Proponga una configurazione delle scelte di instradamento (routing) effettuabili dagli apparati di rete di livello 3 che interconnettono le reti degli edifici in modo da soddisfare i requisiti di progetto con particolare riferimento alla tolleranza della eventuale caduta di uno dei collegamenti.

La configurazione del routing nei router R1, R2, R3 che interconnettono le reti dei tre edifici, cioè la compilazione delle tabelle di routing tramite le quali i router scelgono i percorsi su cui instradare i pacchetti IP affinché raggiungano le reti di destinazione, può essere fatta manualmente, configurando le *route* (percorsi o rotte) con opportuni comandi e definendo le priorità dei percorsi alternativi tramite *la distanza amministrativa*, oppure in modo più veloce optando per il *routing dinamico* e configurando un protocollo di routing come RIPv2, semplice da configurare e adatto a operare in piccole reti<sup>2</sup>.

Con il piano di indirizzamento definito a partire da un unico blocco di indirizzi IP la configurazione del protocollo RIPv2 è particolarmente semplice in quanto è sufficiente effettuare i seguenti passaggi<sup>3</sup> (dando i relativi comandi):

1. si seleziona il protocollo di routing RIP ("router RIP");
2. si seleziona la versione 2 (se non è quella di default, "version 2")
3. si configura la rete "major" a cui appartengono le subnet direttamente collegate che vanno annunciate agli altri router ("network 10.0.0.0"), la rete major è la rete in classe A, B o C a cui appartengono le subnet IP collegate al router, nel caso in esame è una rete in classe A;
4. si richiede di mantenere separate le subnet IP che appartengono alla rete major quando il router comunica agli altri router le reti che può raggiungere ("no-autosummary").

Nel caso cada un collegamento i router scelgono automaticamente il percorso alternativo scambiandosi le necessarie informazioni tramite il protocollo RIPv2.

---

<sup>2</sup> Un altro protocollo di routing che è possibile impiegare in questo caso è il protocollo OSPF.

<sup>3</sup> Per condividere l'accesso a Internet il router su cui è configurata la default route verso Internet (route 0.0.0.0 0.0.0.0 <ind\_IP\_router\_verso:Internet>) deve comunicare ciò agli altri router, opzione attivata con il comando `default-information originate`.

Discuta almeno due dei seguenti punti.

1. calcoli la latenza da server FTP a client che si ha con la vecchia infrastruttura quando un dispositivo di utente (client) posto nella sede operativa richiede al server FTP, posto nella sede principale, un blocco di dati di applicazione (o MSS, maximum segment size) avente dimensione pari a 1460 Byte, sapendo che:
  - la connettività a livello 2 è Ethernet 100BASE-TX,
  - la distanza totale è di 280 metriognuno dei due ripetitori introduce un ritardo di 5  $\mu$ s.

In una direzione di una *comunicazione in cui non interviene la correzione d'errore* la latenza può essere definita come il tempo che intercorre fra l'emissione di una PDU (Protocol Data Unit) da parte della sorgente e la ricezione della PDU stessa da parte del destinatario. Poiché lo strato 2 OSI controlla e gestisce la comunicazione su un canale fisico, organizzandola come trasmissione di *frame* (2-PDU), in generale la latenza (LT) può essere calcolata sommando la durata di un frame, i ritardi di propagazione dovuti ai mezzi trasmissivi, i ritardi dovuti all'attraversamento di apparati di rete (switch, ecc.):

$$LT = \Delta t_{Frame} + \Delta t_{Prop.} + \sum_1^N (\Delta t_{App.}_i + \Delta t_{Q}_i) \quad [s]$$

La durata di un frame, cioè il tempo necessario per la sua emissione da parte della sorgente, è calcolabile come rapporto tra la dimensione del frame espressa in bit ( $D_F$ ) e il bit rate (BR, o velocità di trasmissione espressa in bit/s) con cui si opera:

$$\Delta t_{Frame} = \frac{D_F \text{ [bit]}}{BR \text{ [bit/s]}} \quad [s]$$

Per determinare la dimensione di un frame Ethernet è quindi necessario determinare la dimensione del suo campo informativo (o *payload*), che contiene gli header dei protocolli degli strati superiori e il blocco di dati veri e propri.

Nel caso in esame ricordando che:

- il protocollo di applicazione FTP per il trasporto dei dati si appoggia sul protocollo TCP, le cui PDU (o segmenti) hanno un header di 20 Byte (B);
- l'MSS è la dimensione massima di un blocco di dati trasportato dal protocollo TCP (è il payload del segmento avente la dimensione massima, pari a 1460 B nel caso in esame);
- il protocollo TCP si appoggia sul protocollo di rete IPv4, le cui PDU (o pacchetti) hanno un header di 20 B;

si ha che il campo informativo (payload) di un frame Ethernet ha una dimensione pari a:

$$D_{info} = 1460 + 20 + 20 = 1500 \text{ Byte}$$

Il protocollo Ethernet aggiunge al campo informativo (payload) un proprio header di 22 Byte (8 B di preambolo+SFD, 12 B per ind. MAC destinazione e sorgente, 2 B per il Protocol Type) e un campo di coda per la rivelazione d'errore (FCS) di 4 B.

La dimensione totale di un frame Ethernet è quindi di **1526 Byte**. La velocità di trasmissione (bit rate lordo) della tecnologia Ethernet 100BASE-TX è pari a 100 Mbit/s, per cui la durata di un frame è pari a:

$$\Delta t_{Frame} = \frac{1526 \cdot 8}{100 \cdot 10^6} = 122,08 \mu s$$

Il ritardo introdotto dai cavi Ethernet impiegati per il collegamento può essere calcolato come rapporto tra la loro lunghezza complessiva e la velocità di propagazione, pari al prodotto tra il fattore di velocità e la velocità della luce. Assumendo come fattore di velocità di un cavo  $F_v = 0,7$  (indicativamente  $F_v$  varia tra 0,66 e 0,8) si ha quindi:

$$\Delta t_{Propagaz.} = \frac{280}{2,1 \cdot 10^8} = 1,33 \mu s$$

Conoscendo il ritardo introdotto dai due ripetitori interposti si può quindi determinare la latenza, che risulta pari a:

$$\zeta = 122,08 \cdot 10^{-6} + 1,33 \cdot 10^{-6} + 10 \cdot 10^{-6} = 133,41 \mu s$$

2. sapendo che per la nuova dorsale, lunga complessivamente 280 m, si impiega un sistema su fibra ottica (f.o.) multimodale avente le caratteristiche riportate in figura, in cui i connettori alle estremità della f.o. introducono ciascuno un'attenuazione massima di 0,75 dB e vi sono due giunti, ciascuno dei quali introduce un'attenuazione massima di 0,2 dB, calcolare
- il livello di potenza che si ha in ricezione e il margine rispetto alla sensibilità del rivelatore ottico;
  - la banda utile della fibra ottica e la sua capacità trasmissiva massima teorica

Sorgente ottica			
VCSEL Parameters	Typ.	Max.	Units
Fiber coupled optical power	600		$\mu W$
RMS Spectral Bandwidth		0.4	nm
Rise/Fall Time		40 40	ps

Fibra ottica multimodale	
Standards Compliance	
ISO/IEC 11801 Type OM4 fiber	
<b>Optical Specifications</b>	
<b>Bandwidth</b> (MHz·km)	
4700	
<b>Attenuation</b>	
Wavelength (nm)	Maximum Value (dB/km)
850	$\leq 2.3$

Rivelatore ottico			
Parameter	Symbol	Typ.	Unit
<b>PIN Diode</b>			
Detection wavelength	$\lambda_0$	850	nm
Responsivity	R	0.6	A/W
Sensitivity	S	-20	dBm
Rise/Fall time <sup>1</sup>	$t_r$	100	ps

Il livello di potenza che si ha in ricezione può essere calcolato con un bilancio di potenza (link budget, rif. Cap. 5 Par. 10.1 vol. 2 del testo):

► Facendo riferimento alla FIGURA 3 e operando con i decibel, il bilancio di potenza può essere espresso con la seguente relazione:

$$L_{PRX} = L_{PTX\_[\text{dBm}]} - A_{totale\_[\text{dB}]} - M_{[\text{dB}]} \quad [\text{dBm}] \quad (5.21)$$

dove:

- $L_{PRX}$ : livello di potenza, in dBm, in ingresso al ricevitore;
- $L_{PTX}$ : livello di potenza, in dBm, iniettata nella F.O. dalla sorgente ottica;
- $A_{totale}$ : attenuazione totale del collegamento;
- $M$ : margine di sistema, tiene conto delle possibili variazioni che possono intervenire dopo la posa del collegamento e di variazioni rispetto ai dati di targa dei dispositivi ecc.

Si calcola quindi il livello di potenza che si ha in ricezione senza margine.

Il margine può poi essere determinato come differenza tra il livello in ricezione calcolato e la sensibilità del ricevitore (che è il minimo livello di potenza in ricezione che consente al ricevitore ottico di operare correttamente).

Calcolo del livello di potenza in ricezione (con  $M=0$ ):

- si calcola il livello di potenza con cui opera la sorgente ottica sapendo dai dati forniti che la potenza di emissione tipica è 0,6 mW:

$$Lp_{TX} = 10 \log(0,6) = -2,22 \text{ dBm}$$

- si calcola l'attenuazione totale sapendo, dai dati forniti, che l'attenuazione massima della f.o. al km è 2,3 dB/km, che ogni connettore attenua di 0,75 dB e che ciascuno dei due giunti attenua di 0,2 dB:

L'attenuazione totale di un collegamento in F.O. lungo  $l$  km si può calcolare con la (5.17) :

$$A_{totale} = A_{F.O.} + A_c + A_g = \alpha_{F.O.\text{-dB/km}} \cdot l_{\text{km}} + \alpha_{c\text{-dB}} \cdot N_c + \alpha_{g\text{-dB}} \cdot N_g \text{ dB}$$

$$A_{totale} = 2,3 \cdot 0,28 + 0,75 \cdot 2 + 0,2 \cdot 2 = 2,54 \text{ dB}$$

- Il livello di potenza in ricezione è quindi pari a:

$$Lp_{RX} = -2,22 - 2,54 = -4,76 \text{ dB}$$

Nota la sensibilità (sensitivity,  $Lp_{RX\_min} = -20 \text{ dBm}$ ) del ricevitore ottico (fotodiode PIN) si può calcolare il margine di sistema, che risulta pari a:

$$M = Lp_{RX} - \text{Sensitivity} = -4,76 + 20 = 15,24 \text{ dB}$$

3. Valuti l'affidabilità a livello trasmissivo di un sistema di interconnessione wireless fra il sito principale e l'ufficio aperto al pubblico avente le seguenti caratteristiche:
- opera nella banda non licenziata (ISM) dei 17 GHz, con frequenza portante pari a 17,1 GHz e banda di canale pari a 80 MHz;
  - opera in trasmissione con un valore di EIRP pari a 20 dBm;
  - gli apparati posti nelle due sedi sono dotati ciascuno di antenna integrata con diametro pari a 60 cm.

La valutazione deve essere fatta calcolando il livello di potenza che si ha in ingresso al ricevitore e verificando che esso non sia inferiore a -75 dBm, anche in presenza di un'attenuazione dovuta al fading di 18 dB.

Il livello di potenza in ricezione si può calcolare con un bilancio di potenza (link budget, rif. Cap. 9 Par. 7.1 vol. 2 del testo)

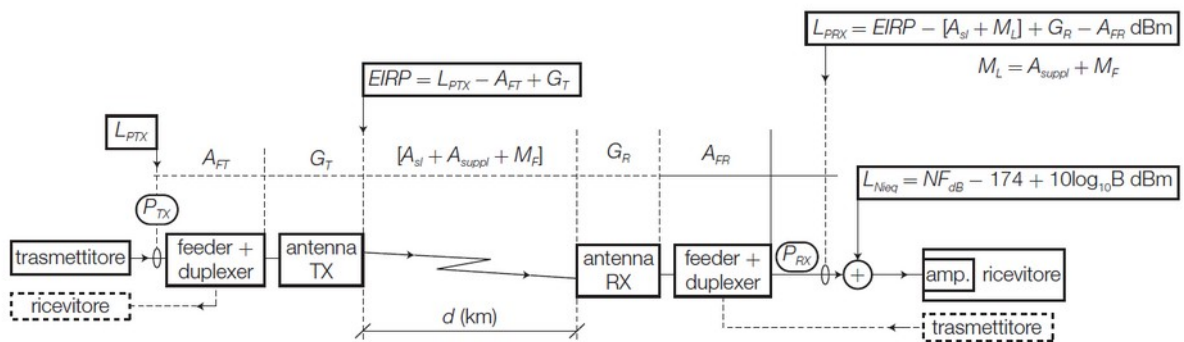


FIGURA 18 Bilancio di potenza di un collegamento in ponte radio.

Si può quindi procedere nel seguente modo.

- Si calcolano l'attenuazione dello spazio libero e l'attenuazione totale del collegamento radio (comprensiva del margine richiesto)

$$A_{sl} = 92,5 + 20 \log_{10} d_{[km]} + 20 \log_{10} f_{[GHz]} \quad \text{[dB]} \quad (9.9)$$

dove:

- $d$ : lunghezza del collegamento, in (km);
- $f$ : frequenza di trasmissione, in (GHz).

$$A_{sl} = 92,5 + 20 \log(0,5) + 20 \log(17,1) = 111,1 \text{ dB}$$

$$A_{tot.colleg.} = 111,1 + 18 = 129,1 \text{ dB}$$

- Si calcola il guadagno dell'antenna ricevente (considerando l'efficienza tipica di 0,65):



Le antenne utilizzate nei ponti radio sono usualmente antenne paraboliche, il cui guadagno può essere calcolato nel seguente modo<sup>24</sup>:

$$G = 18,5 + 20\log_{10}D_{a[m]} + 20\log_{10}f_{[GHz]} \quad [\text{dB}] \quad (9.7)$$

dove:

- $D_a$ : diametro dell'antenna, in (m);
- $f$ : frequenza di trasmissione, in (GHz).

$$G_{Ant_{RX}} = 18,5 + 20\log(0,6) + 20\log(17,1) = 38,8 \text{ dB}$$

- Noto il valore dell'EIRP (20 dBm), si calcola il livello di potenza in ingresso al ricevitore (l'antenna è integrata e quindi non vi è il cavo di interconnessione con il ricevitore):
- c) Si calcola il livello di potenza in ingresso al primo amplificatore in ricezione sottraendo all'EIRP tutte le attenuazioni del collegamento radio e dell'eventuale feeder lato ricezione e sommando il guadagno dell'antenna ricevente:

$$L_{PRX} = EIRP_{[\text{dBm}]} - [A_{sl[\text{dB}]} + M_{L[\text{dB}]}] + G_{R[\text{dB}]} - A_{FR[\text{dB}]} \quad [\text{dBm}] \quad (9.8)$$

$$L_{PRX} = 20 - 129,1 + 38,8 = -70,3 \text{ dBm}$$

Il livello di potenza in ricezione supera quanto richiesto dai dati di progetto e quindi il collegamento si può ritenere affidabile dal punto di vista trasmissivo.

4. Proponga una modalità di implementazione e una configurazione per il servizio di rete che consente la configurazione automatica degli indirizzi IPv4 sui dispositivi utente (client) collegati in modo cablato di una sottorete IP a sua scelta, facendo però in modo che gli indirizzi IPv4 assegnati siano statici e illustri le fasi con cui avviene l'assegnazione degli indirizzi stessi all'accessione dei client.

Il servizio per la configurazione automatica degli indirizzi IPv4 è il servizio DHCP. Il servizio DHCP è di tipo client server, per cui è necessario avere installato su una macchina collegata in rete un'applicazione server DHCP. Il server DHCP può essere installato su diversi tipi di macchine: su un PC, per esempio con sistema operativo LINUX, su un router, su un access point, ecc.

Gli indirizzi possono essere assegnati dal server DHCP:

- *in modo dinamico*, quando essi possono variare nel tempo;
- *in modo statico*, quando essi non variano nel tempo; l'assegnazione statica può essere ottenuta vincolando l'assegnazione di un indirizzo IPv4 a uno specifico indirizzo MAC (MAC address), il quale identifica univocamente (a livello 2) una scheda di rete (Ethernet o Wi-Fi), operazione nota anche come *binding IP-MAC*; configurando in questo modo il server DHCP si ottiene il risultato di assegnare sempre lo stesso indirizzo IP al client che ha la scheda di rete con l'indirizzo MAC a esso legato.

Nel caso di un server DHCP installato su un PC con sistema operativo LINUX, per esempio, la configurazione del server per la subnet N. 1 viene fatta editando un file di configurazione in modo analogo al seguente (rif. Cap. 5 Lab. 4 vol. 3 e corso di Sistemi e reti):

```
# Sample configuration file for ISC dhcpd for Debian
# If this DHCP server is the official DHCP server for the
local
# network, the authoritative directive should be uncommented.
authoritative;
```

```
# A slightly different configuration for an internal subnet.

subnet 10.0.0.0 netmask 255.255.255.224 {
  range 10.0.0.11 10.0.0.24;
  option domain-name-servers 208.67.220.220, 208.67.222.222;
  option domain-name "LAB-TELECOMUNICAZIONI";
  option routers 10.0.0.1;
  option broadcast-address 10.0.0.31;
  default-lease-time 6000;
  max-lease-time 72000;
}

# Fixed IP addresses can also be specified for hosts.

host PC-IP-FISSO {
  hardware ethernet e0:cb:4e:1e:83:84;
  fixed-address 10.0.0.10;
}
```

FIGURA 14 File di configurazione del server DHCP.

Si elimina il range di indirizzi dinamici e aggiungono tanti host con indirizzo fisso (statici) quanti sono i computer cablati, assegnando a ciascuno un indirizzo IP associato all'indirizzo MAC della sua scheda di rete.

All'accensione del client l'assegnazione dell'indirizzo IPv4, con i parametri associati (subnet mask, gateway predefinito o router, server DNS o domain-name server) avviene con i seguenti passaggi.

- a) **DHCP Discover**: all'accensione il PC client non possiede un indirizzo IPv4 per cui invia un pacchetto (incapsulato in un frame) in broadcast utilizzando come indirizzo IPv4 sorgente 0.0.0.0 (indirizzo non specificato) e come indirizzo IPv4 di destinazione il 255.255.255.255 (broadcast generico) per scoprire se in rete vi è un server DHCP attivo, indicando che di preferenza vorrebbe avere l'indirizzo IPv4 precedentemente assegnatogli;
- b) **DHCP offer**: il server DHCP conferma la sua presenza in rete offrendo tale indirizzo IPv4, se disponibile;
- c) **DHCP request**: il client richiede al server l'indirizzo IPv4 offerto e i parametri associati (indirizzo del router, server DNS ecc.);
- d) **DHCP ACK**: il server DHCP conferma l'indirizzo IPv4 assegnato e invia i parametri richiesti.

## SECONDA PARTE

1. Illustri le possibili alternative che vi sono per dotare di un accesso a Internet a banda larga o (preferibilmente) ultralarga una rete aziendale; proponga quindi la soluzione che a suo motivato parere è più indicata per l'unico accesso Internet, condiviso dalle reti di tutti gli edifici, che l'azienda desidera avere e che va posto nella sede principale.

Le tecnologie per gli accessi a banda larga che utilizzano il doppino telefonico come linea che giunge all'utente sono indicate come **xDSL**.

I sistemi xDSL si suddividono in

- **sistemi asimmetrici**, nei quali la velocità di ricezione lato utente (o *downstream*) è molto maggiore di quella di trasmissione (o *upstream*);
- **sistemi simmetrici**, nei quali la velocità di ricezione, lato utente, è uguale a quella di trasmissione.

Un tabella riassuntiva dei sistemi xDSL attualmente disponibili può essere la seguente (rif. Cap. 9 Par. 2 vol. 3 del libro di testo).

Tipo di sistema		Bit rate max downstream	Bit rate max upstream kbit/s	Lunghezza max linea	N. doppini
Asimmetrico	ADSL ( <i>Asymmetric DSL</i> )	32 ÷ 7936 kbit/s a passi di 32 kbit/s	32 ÷ 768 kbit/s a passi di 32 kbit/s	≈ 5,5 km	1
Asimmetrico	ADSL2+	≈ 25 Mbit/s	≈ 1,3 Mbit/s	≈ 1,5 km	1
Asimmetrico/ simmetrico	VDSL <sup>1</sup> ( <i>Very high speed DSL</i> )	≈ 52 Mbit/s ≈ 28 Mbit/s	≈ 30 Mbit/s ≈ 28 Mbit/s	≈ 300 m	1
Asimmetrico/ simmetrico	VDSL2	≈ 100 Mbit/s ≈ 100 Mbit/s	≈ 60 Mbit/s ≈ 100 Mbit/s	≈ 300 m	1
Simmetrico	HDSL ( <i>High bit rate DSL</i> )	≈ 2 Mbit/s	≈ 2 Mbit/s	≈ 6 km	2
Simmetrico	SHDSL ( <i>Single-pair High speed DSL</i> )	≈ 5,7 Mbit/s	≈ 5,7 Mbit/s	≈ 2,6 km	1

TABELLA 2 Caratteristiche salienti dei principali sistemi xDSL.

Note:  
DSL = *Digital Subscriber Line* (linea di utente/abbonato digitale)

Come si può evincere dalla tabella, nel caso di linea di utente completamente su doppino telefonico, da centrale a utente, e la cui lunghezza supera il km, possono essere impiegati sistemi asimmetrici ADSL o ADSL 2+, a seconda della lunghezza del doppino telefonico, con prestazioni che vengono definite "*banda larga*" (indicativamente inferiori a 30 Mbit/s). Questo può essere il caso di utenza posta in zone periferiche o rurali.

Nel caso in cui il collegamento tra la centrale dell'operatore di telecomunicazioni e l'utente sia parzialmente su fibra ottica e venga completato da un tratto su doppino telefonico (con lunghezza massima indicativamente attorno ai 300 m), allora è possibile impiegare i sistemi VDSL2 (più moderni), i quali consentono di fornire accessi definiti a "banda ultralarga" (velocità di ricezione superiore ai 30 Mbit/s). I sistemi di accesso a Internet che impiegano, del tutto o in parte, fibra ottica (f.o.) sono complessivamente indicati con l'acronimo **FTTx** (*Fiber To The x*, dove x indica il punto dove termina la f.o.), essi vengono comunemente suddivisi nel seguente modo (rif. Cap. 11 Par. 7 vol. 3).

► Nel contesto delle reti di accesso di nuova generazione (NGAN) e delle reti di distribuzione su F.O. (ODN) è stato creato l'acronimo **FTTx** (*Fiber To The...*) per indicare una famiglia di architetture che si distinguono per il punto in cui termina la fibra ottica e inizia l'eventuale collegamento su cavo in rame (doppino telefonico).

La famiglia di accessi FTTx è costituita essenzialmente dalle seguenti architetture<sup>38</sup> (FIGURA 21, a pagina seguente).

- **FTTE** (*Fiber To The Exchange*, fibra fino alla centrale): la fibra ottica termina nella centrale locale e il collegamento verso l'utenza avviene interamente tramite i doppini telefonici; è la situazione iniziale in cui la F.O. non è ancora stata posata nella rete di distribuzione; i collegamenti a banda larga sono forniti da sistemi ADSL/ADSL2+ (a seconda della lunghezza del doppino, che indicativamente può andare da circa 300 m a circa 3 km).
- **FTTC** (*Fiber To The Cabinet/curb*, fibra fino all'armadio o al marciapiede): l'ONU (*Optical Network Unit*) su cui termina la F.O. può essere posta in un armadio (*cabinet*), che sostituisce l'armadio ripartilinee tradizionale, posto a livello di marciapiede (*curb*); il collegamento viene prolungato verso l'utenza su doppino, che indicativamente può arrivare a una lunghezza massima di circa 700 m; i collegamenti a banda larga sono forniti da sistemi ADSL2+ e nei casi di linea corta (per esempio 300 m) tramite VDSL/VDSL2.
- **FTTD<sub>p</sub>** (*Fiber To The Distribution point*, fibra fino al punto di distribuzione<sup>39</sup>): la F.O. termina su un punto di distribuzione, che può essere posto ancora più vicino agli utenti; il prolungamento su doppino ha così una distanza che indicativamente non supera i 200 m; ciò permette di utilizzare sistemi VDSL2 o G.fast che consentono di offrire servizi a banda ultralarga.
- **FTTB** (*Fiber To The Building*, fibra fino all'edificio): l'ONU su cui termina la F.O. è posto all'interno dell'edificio dove risiede l'utenza da servire (per esempio un'azienda o un condominio), il collegamento verso i singoli utenti avviene tramite doppino e sistemi VDSL2 o G.FAST, supportando così i servizi a banda ultralarga.
- **FTTH** (*Fiber To The Home*, fibra fino all'abitazione): la F.O. giunge<sup>40</sup> fino alle singole abitazioni degli utenti; poiché il collegamento è completamente su F.O. possono essere offerti servizi avanzati a banda ultralarga.



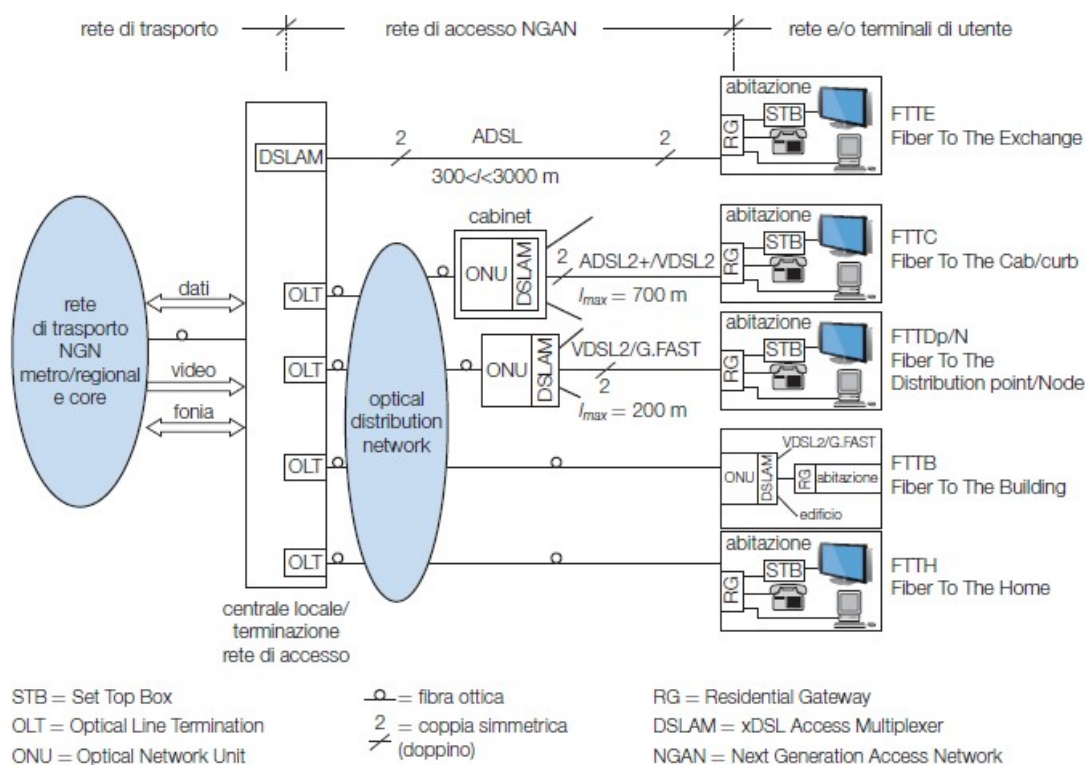


FIGURA 21 Esempi di architetture FTTx.

39 Oppure al nodo (N) di distribuzione, soluzione FTTN.

40 Le soluzioni FTTP/FTTH vengono anche denominate FTTP, *Fiber To The Premise*.

Per la connettività Internet dell'azienda è consigliabile optare per una connettività **FTTH** (preferibilmente di tipo dedicato) se disponibile, o in subordine con connettività **FTTC a banda ultralarga**. In entrambi i casi è importante richiedere una connettività con **banda minima garantita**. Nel caso in cui la connettività Internet sia una risorsa indispensabile, come nel caso in cui l'azienda utilizzi diversi *servizi cloud*, è utile avere una doppia connettività Internet, preferibilmente con due ISP (*Internet Service Provider*) diversi e con due mezzi trasmissivi diversi (tipicamente una connessione su f.o. e una connessione wireless), in modo da garantire la connettività anche nel caso in cui l'accesso a Internet principale subisca dei guasti.

2. Descriva quali sono le principali misure di sicurezza da prendere a difesa della rete aziendale; illustri quindi, avvalendosi anche di disegni, in che modo il server FTP locale potrebbe essere esposto in modo sicuro su Internet e reso accessibile con comunicazioni protette solo dal personale dell'azienda che opera da remoto.

Le principali misure di sicurezza a difesa della rete aziendale possono essere le seguenti (rif. Cap. 7 Par. 6 vol. 3 del testo e corso di Sistemi e reti).

## 6 Concetti generali sulla sicurezza delle reti

Uno dei problemi maggiormente sentiti nelle comunicazioni su reti IP, e in particolare su Internet, è quello della sicurezza sia contro accessi non autorizzati sia del trasferimento dati. In questo contesto si possono definire essenzialmente le seguenti problematiche: sicurezza dei luoghi fisici (accesso a edifici, locali ecc.); sicurezza perimetrale; identificazione degli utenti, verifica dei permessi loro attribuiti e controllo delle operazioni fatte; riservatezza e confidenzialità dei dati trasmessi.

### 6.1 Sicurezza perimetrale

La sicurezza perimetrale consiste nel proteggere la rete da attacchi esterni e da tentativi di accesso non autorizzati tramite l'impiego di *Access Control List* (liste di controllo degli accessi), *firewall* e *DMZ (DeMilitarized Zone)*.

A ciò si può aggiungere l'impiego di sistemi per il rilevamento e la prevenzione dei tentativi di intrusione (*IDPS, Intrusion Detection and Prevention System*).

Un firewall può poi effettuare l'analisi del traffico che entra e esce da una rete fino a livello 7, applicando anche regole per il filtraggio dei contenuti (*content filtering*) che per esempio impedisca l'accesso a determinate categorie di siti. Oltre a ciò è necessaria la presenza di antivirus e antispam.

A livello 2, poi, possono essere messa in atto una serie di interventi tesi a impedire accessi non autorizzati all'interno della rete aziendale, come i seguenti (rif. cap. 3 par. 6 del vol. 3)



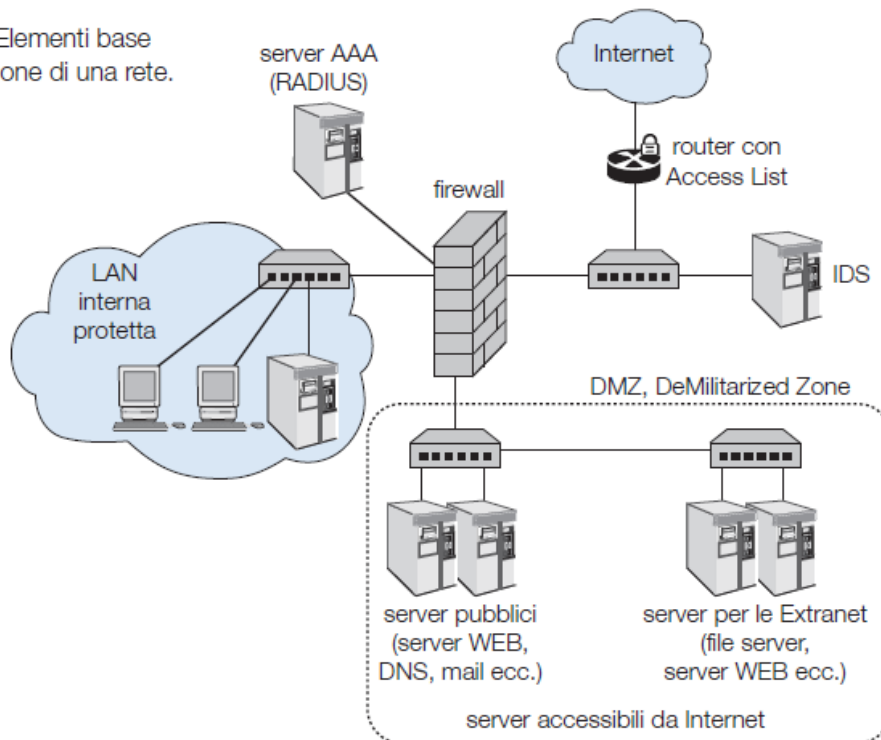
Esempi di misure di sicurezza che possono essere prese a protezione degli switch sono le seguenti.

- *Sicurezza fisica*: gli switch vanno posti in luoghi che non siano facilmente accessibili (locali chiusi a chiave ecc.).
- *Protezione degli accessi* (porta console, Telnet, GUI) per la configurazione dello switch con password forti.
- *Disabilitazione delle modalità di accesso alla configurazione non impiegate*: se si impiega solo la GUI è consigliabile disabilitare l'accesso via Telnet.
- *Impiego di protocolli sicuri* per l'accesso alla configurazione, se sono supportati dallo switch, come SSH in modalità CLI, e HTTPS in modalità GUI; essi sono definiti sicuri perché operano crittografando i dati inviati in rete.
- *Configurazione di un'apposita VLAN riservata all'amministrazione dello switch*, che può essere associata a una sola porta dello switch, quella a cui viene collegato solo il PC dell'amministratore di rete.
- *Configurazione del port security* sulla porta a cui viene collegato il PC dell'amministratore di rete, che consiste nel vincolare l'accesso in rete tramite quella porta solamente a un indirizzo MAC specificato (quello del PC dell'amministratore di rete); se non si prevedono cambiamenti nei PC collegati in rete si potrebbe anche applicare il port security a tutte le porte.
- *Disabilitazione delle porte* dello switch che non vengono mai utilizzate, in modo da prevenire accessi in rete non autorizzati.
- *Filtraggio del traffico* di flooding.

Il server FTP può essere esposto su Internet, rendendolo accessibile da una connessione Internet remota, collocandolo su una DMZ (si rimanda al Cap. 7 Par. 6.1 del testo e al corso di Sistemi e reti per i dettagli).

Il personale che opera da remoto può accedere al server FTP in modo sicuro tramite una *VPN ad accesso remoto* o una *mobile VPN* (si rimanda al Cap. 7 Par. 4.4 del testo e al corso di Sistemi e reti per i dettagli).

FIGURA 24 Elementi base per la protezione di una rete.



AAA = Authentication, Autorization, Accounting  
 RADIUS = Remote Authentication Dial-In User Service  
 IDS = Intrusion Detection System  
 DNS = Domain Name System

3. **Illustri le caratteristiche generali delle modulazioni M-QAM, proponga lo schema di un modulatore 16-QAM e calcoli il bit rate (o velocità di informazione) e il symbol rate (o baud rate o velocità di modulazione) che tale modulatore consente di ottenere quando la banda a disposizione è pari a 350 kHz.**

Le modulazioni M-QAM sono modulazioni digitali miste ampiezza-fase, cioè modulazioni in cui  $n$  bit alla volta sono mappati su  $M=2^n$  possibili combinazioni di ampiezza e fase del segnale modulato, generate a partire da portanti sinusoidali.

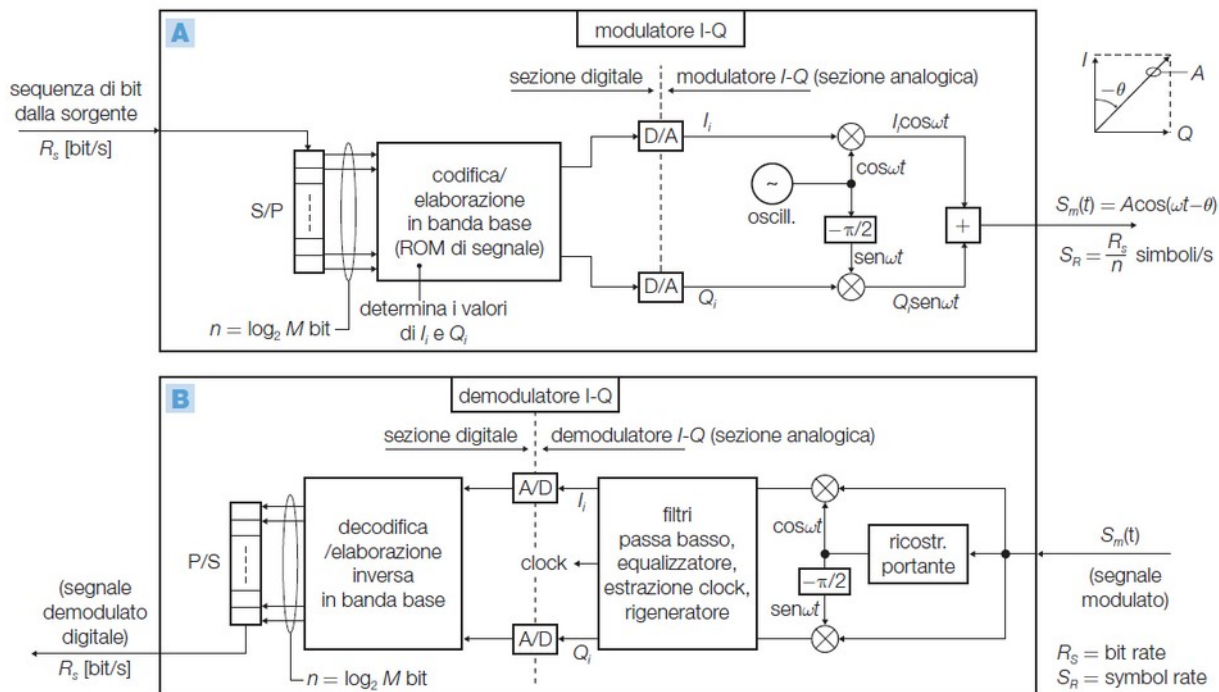
Le modulazioni M-QAM sono quindi modulazioni ad alta efficienza spettrale in quanto ottimizzano lo sfruttamento della banda di canale a disposizione, massimizzando la velocità di trasmissione (bit rate) su esso.

Una combinazione di ampiezza e fase costituisce uno stato di modulazione (o simbolo) che trasporta  $n$  bit. Il numero di stati di modulazione ( $M$ ) può essere molto elevato (per esempio si arriva a 1024 o 2048 stati), il che conferma l'elevata efficienza spettrale della modulazione (si rimanda al Cap. 8 Par. 5.7 per i dettagli).

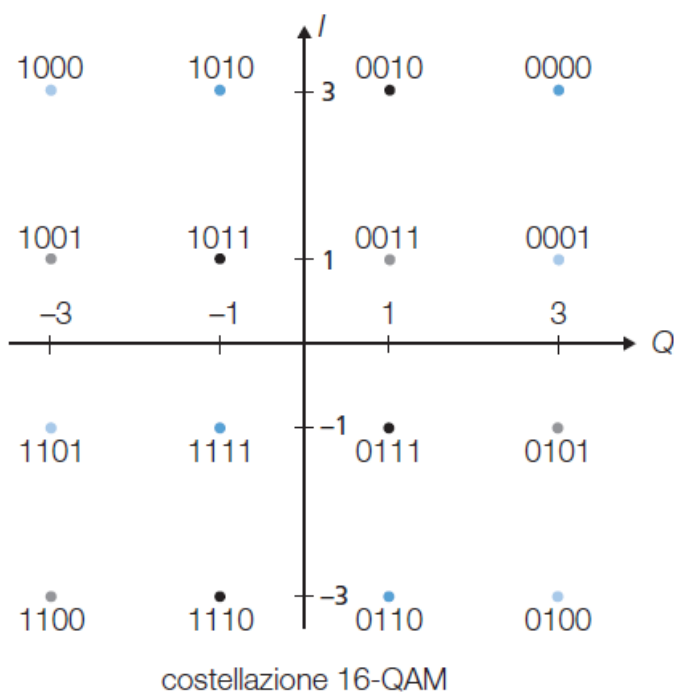
I modulatori M-QAM si basano sul modulatore I-Q (rif. cap. 8 par. 6), il cui schema di principio è il seguente.

**FIGURA 17**  
**A)** Generazione di un segnale modulato a  $M$  stati tramite un modulatore I-Q.  
**B)** Demodulazione.

In FIGURA 17 si illustra lo schema di principio di un modem (*modulatore-demodulatore*) in grado di operare con qualsiasi modulazione digitale multistato. In FIGURA 17A viene riportato lo schema di principio del modulatore, che è diviso in due parti: la sezione digitale, che opera in banda base, e la sezione analogica, costituita dal *modulatore I-Q*.



Per ottenere la modulazione 16-QAM si devono prelevare 4 bit alla volta dal flusso di bit seriale da trasmettere (convertitore Serie/Parallelo a 4 celle), bit che vengono mappati su una costellazione di 16 combinazioni di ampiezza e fase, come la seguente:



In prima approssimazione la velocità di modulazione massima (o *Symbol Rate*,  $S_R$ ) di un modulatore 16-QAM è numericamente uguale al valore della banda a disposizione, per cui ricordando che il legame tra Symbol Rate e Bit Rate ( $R_s$ , o velocità di informazione) è il seguente (cap. 8 Par. 5.1 vol. 3).

Il bit rate generato dalla sorgente,  $R_s$  (bit/s), può così essere maggiore del symbol rate (velocità di modulazione),  $S_R$  (simboli/s o baud), dato dal numero di simboli al secondo emessi dal modulatore.

Si ricorda che il legame tra bit rate ( $R_s$ ) e symbol rate ( $S_R$ ) è il seguente:

$$R_s = S_R \log_2 M \quad [\text{bit/s}] \quad (8.9)$$

## 8 Tecniche di trasmissione digitali

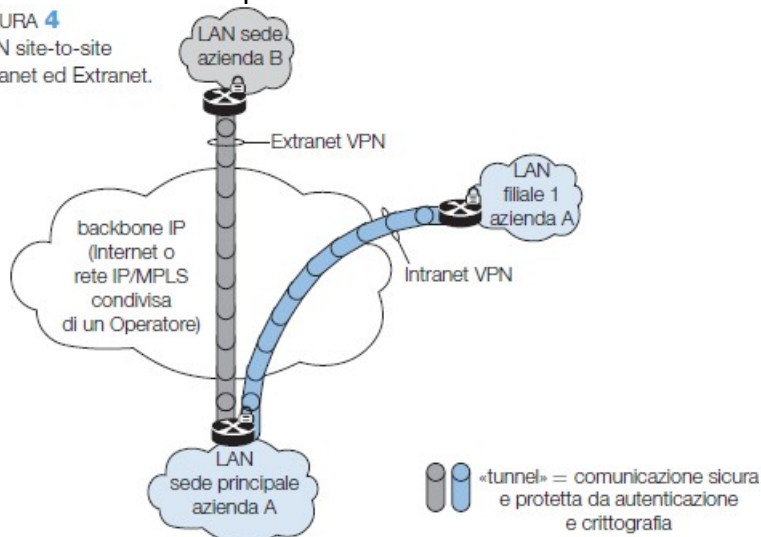
Nel caso in esame, quindi, assumendo come Symbol rate il valore  $S_R = 350 \text{ kSimboli/s}$  si ha che il bit rate risulta pari a:

$$R_s = S_R \cdot \log_2 16 = 350 \cdot 10^3 \cdot 4 = 1,4 \text{ Mbit/s}$$

4. Descriva una possibile soluzione per interconnettere in modo protetto, sicuro e a costi non eccessivi una porzione della rete aziendale con una sottorete remota di un'azienda partner situata in un'altra regione italiana.

Una possibile soluzione per realizzare una *Extranet* che interconnette porzioni di rete di aziende diverse è impiegare una *Extranet VPN*, realizzata per esempio con firewall VPN e connessioni Internet se si desidera minimizzare i costi o richiedendo una *Network based VPN* (VPN creata attraverso la rete IP/MPLS di un operatore di Telecomunicazioni) se si desidera massimizzare le prestazioni e l'affidabilità della VPN (si rimanda al Cap. 7 Par. 4.4 vol. 3 e al corso di Sistemi e reti per i dettagli)

FIGURA 4  
VPN site-to-site  
Intranet ed Extranet.



8 I server devono essere dotati di un opportuno sistema operativo di rete, che può svolgere anche la funzione di server RADIUS (*Remote Authentication Dial-In User Service*).

## 7 Sistemi di accesso remoto, reti WAN e protocolli di linea

Libri consigliati:

Onelio Bertazioli

Corso di Telecomunicazioni vol. 2 e vol. 3

ed. Zanichelli

Manuale Cremonese di Informatica e Telecomunicazioni