

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL - INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE TELECOMUNICAZIONI

Tema di: TELECOMUNICAZIONI e SISTEMI E RETI

Il candidato svolga la prima parte della prova e risponda a due dei quesiti tra quelli proposti.

PRIMA PARTE

Un'emittente radiofonica vuole ampliare il network di broadcasting, costruendo un nuovo ripetitore su un noto hub locale, situato in montagna. Il nuovo ripetitore sarà connesso allo studio radiofonico mediante un ponte radio che provvederà a trasmettere il flusso della trasmissione radiofonica al trasmettitore DAB posizionato nell'hub in montagna.

Il trasmettitore DAB dispone di un'interfaccia G703 PCM/TDM 2,048 Mbit/s per lo stream DAB e di un'interfaccia ETH (Ethernet IP) per il controllo remoto e la supervisione.

Il nuovo ponte radio provvederà inoltre a collegare su interfaccia Ethernet il trasmettitore per la supervisione, un apparato IP che riporterà gli allarmi della stazione verso lo studio per controllo remoto e due telecamere di un sistema di videosorveglianza per il controllo di sicurezza. Il ponte radio è caratterizzato da due apparati TX/RX, operanti in modulazione digitale, installati nelle rispettive stazioni di monte e di valle e da due antenne paraboliche, le cui caratteristiche sono riassunte di seguito:

Porte di ingresso:	4xG703 (2,048 Mbit/s PCM cadauna) e 1 Ethernet/LAN layer 2 sia lato TX che lato RX.
Distanza tratta radio:	18 Km in LOS
Antenne entrambe i lati:	parabole diametro 90 cm, efficienza 0,65;
Attenuazione guida d'onda di antenna entrambe i lati:	1,4 dB
Frequenza trasmissione:	10168MHz
Frequenza ricezione:	10518MHz
Max potenza trasmissione:	26 dBm (regolabile da 4 a 26 dBm)

- sensibilità ricezione e modulazioni/capacità (canale da 14 MHz):

Modulation	Sensitivity	Payload
QPSK	-88 dBm	18,332 Mbit/s
8PSK	-82 dBm	27,499 Mbit/s
16QAM	-81 dBm	36,665 Mbit/s
32QAM	-78 dBm	45,832 Mbit/s
64QAM	-74 dBm	61,692 Mbit/s
128QAM	-71 dBm	74,204 Mbit/s
256QAM	-68 dBm	86,863 Mbit/s

Il ponte radio utilizzerà un flusso da 2,048 Mbit/s per il trasporto dello stream radio DAB, 3 flussi per utilizzi futuri ed una porta Ethernet per la video sorveglianza e la telemetria, a cui saranno collegate due telecamere IP, un apparato IP di telemetria per allarmi e l'interfaccia Ethernet di supervisione del trasmettitore DAB.

Il segnale di videosorveglianza, inviato tramite protocollo IP sull'interfaccia Ethernet, dovrà poi essere inoltrato tramite rete internet ad un centro di security per il servizio di sicurezza che si trova in luogo distante dallo studio radiofonico.

Il candidato, sulla base delle specifiche fornite e fatte le eventuali ipotesi aggiuntive ritenute necessarie:

- a) predisponga lo schema a blocchi del ponte radio e uno schema di rete di tutti gli apparati connessi sulla porta Ethernet, separando la telemetria dalla videosorveglianza, definendo apparati, indirizzamento e cablaggi della rete nella stazione di monte;
- b) dopo aver fatto un'ipotesi sul data rate necessario per la videosorveglianza, con o senza compressione video, ed aggiungendo 4 flussi da 2,048 Mbit/s per il DAB stream e 3Mbit/s complessivi per coprire le esigenze dell'apparato di telemetria allarmi e della porta di supervisione del trasmettitore, dimensioni la tratta radio con un margine di fading di almeno 30dB, scegliendo l'opportuna modulazione;
- c) realizzi una connessione sicura attraverso la rete internet per il collegamento tra lo studio radiofonico e il centro di sorveglianza e controllo, tramite opportuni apparati e protocolli;
- d) definisca un socket IP, con un linguaggio a scelta, tra l'HUB di telemetria e lo studio, per visualizzare su un PC di supervisione i dati di allarme e la condizione della stazione di monte.

SECONDA PARTE

1. Due reti LAN di due edifici separati fisicamente, la prima chiamata *rete1* con 12 host e la seconda chiamata *rete2* con 5 host compreso un server dati, sono connessi tra loro attraverso un router, che a sua volta ha una porta verso la rete internet. Definire il piano di indirizzamento delle due reti LAN e individuare una Access Control List da configurare sul router per impedire il traffico FTP dalla *rete1* verso il server dati della *rete2*.
2. Una fibra ottica monomodale ha una lunghezza di 70km e un coefficiente di dispersione cromatica @ 1550nm pari a $D_0=18 \text{ ps}/(\text{nm}*\text{km})$. Descrivere la dispersione modale e la dispersione cromatica di una fibra ottica e determinare la banda e la capacità della fibra, considerando una sorgente VCSEL con $\Delta\lambda = 0,5 \text{ nm}$.
3. Un computer Linux ospita un sito web utilizzato per la consultazione dei dati di rilevazione ambientale dell'inquinamento atmosferico, rilevato da appositi sensori. Sul lato client la pagina web, tramite un form, consente all'utente di generare una richiesta al server; il server risponde su interfaccia web, fornendo le informazioni in base ai dati rilevati. Proporre una soluzione software per la realizzazione del servizio indicato.
4. Un sistema FSK è utilizzato per trasmettere un flusso dati da 600bit/s su un cavo coassiale, impiegando le frequenze $f_1=1,3 \text{ kHz}$ e $f_2=1,7 \text{ kHz}$. Descrivere brevemente il principio della modulazione, anche tramite disegni e/o schemi, determinare la deviazione di frequenza, la frequenza della portante, l'indice di modulazione e la banda occupata dal segnale modulato.

Durata massima della prova: 7 ore.

È consentito l'uso di manuali tecnici e di calcolatrice non programmabile.

È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.

SOLUZIONE

a) Predisponga lo schema a blocchi del ponte radio e uno schema di rete di tutti gli apparati connessi sulla porta Ethernet, separando la telemetria dalla videosorveglianza, definendo apparati, indirizzamento e cablaggi della rete nella stazione di monte;

Lo **schema blocchi di riferimento** per il problema proposto può essere il seguente (si faccia riferimento al libro di testo per la spiegazione dettagliata):

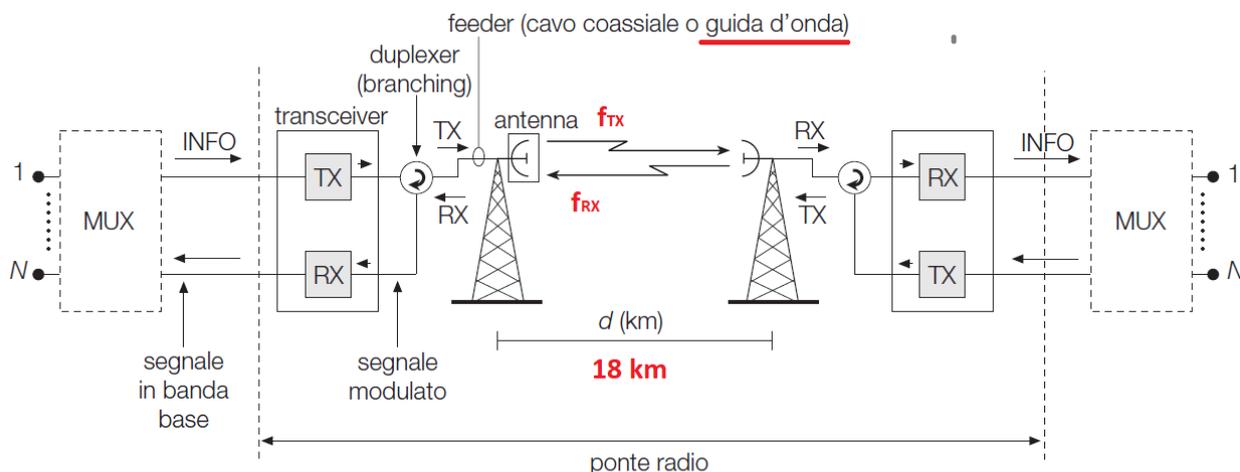


FIGURA 13 Schema elementare di un collegamento in ponte radio.

Un possibile **schema a blocchi per il ponte radio** è il seguente (si faccia riferimento al libro di testo per la spiegazione dettagliata):

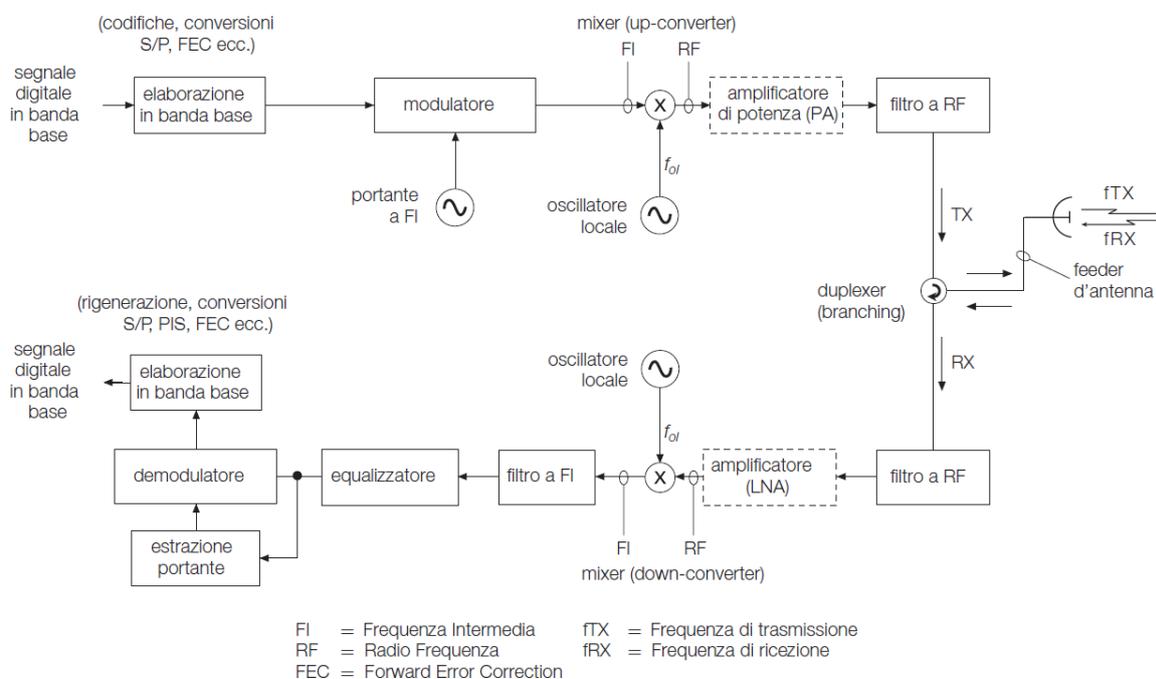
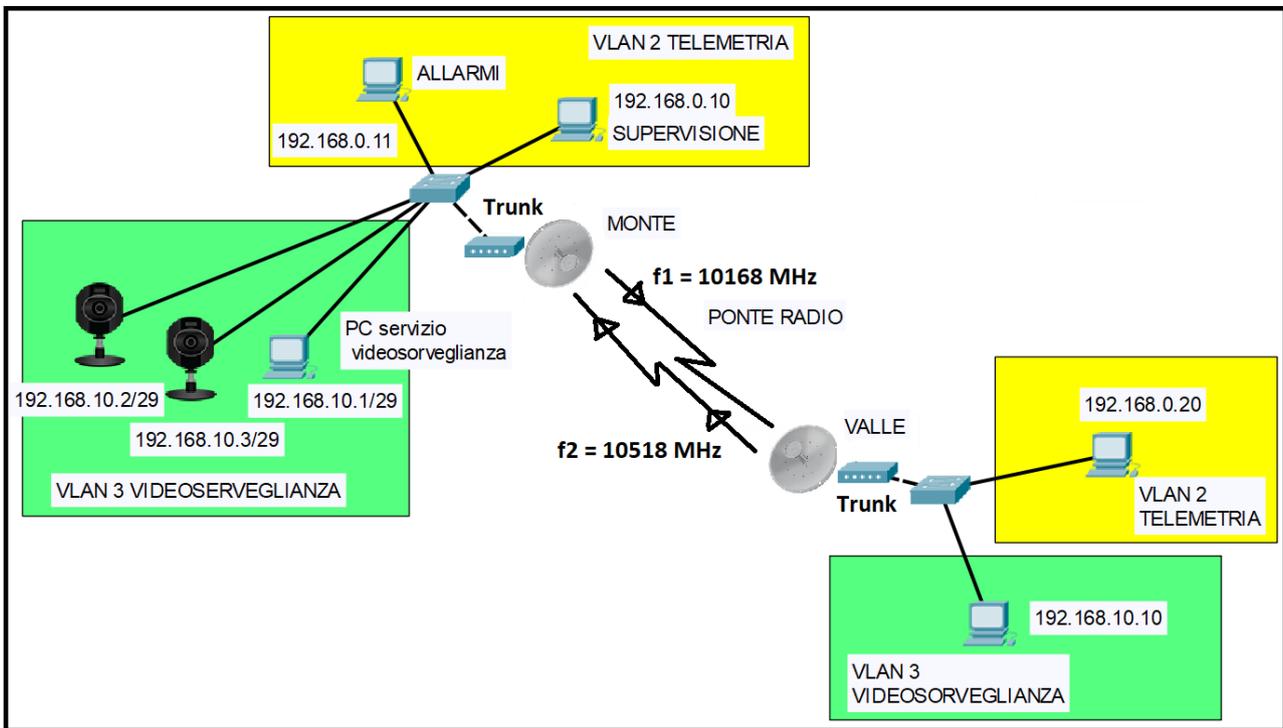


FIGURA 14 Schema a blocchi di un ponte radio digitale.

Schema della rete a monte

Per quanto concerne la rete a monte, un possibile schema può essere il seguente:



Le caratteristiche della rete a monte possono essere le seguenti:

- si impiega uno switch amministrabile su cui sono configurate due VLAN, per esempio
 - VLAN 2 per la Telemetria, che quindi connette in rete il trasmettitore per la supervisione, l'apparato IP per la segnalazione degli allarmi e un eventuale PC di servizio;
 - VLAN 3 per la videosorveglianza, che quindi connette in rete le due telecamere IP e un PC di servizio (opzionale);
 - la separazione del traffico di telemetria da quello della videosorveglianza è garantita dallo switch che impedisce la comunicazione fra porte appartenenti a VLAN differenti, mentre inoltre il traffico di tutte le VLAN, marcandolo con la VLAN ID di appartenenza, sulla porta configurata come trunk;
- la porta dello switch collegata alla porta Ethernet dell'apparato del ponte radio viene configurata come trunk;
- Si ipotizza che l'apparato del ponte radio operi come bridge trasparente e quindi consenta il trasporto senza alcuna modifica dei frame emessi dallo switch; quest'ultimo si può così ritenere collegato a uno switch amministrabile della stazione di valle dal canale fisico dedicato realizzato dal ponte radio;
- A livello IP vengono configurate due subnet IP, una per ciascuna VLAN, configurando gli indirizzi IP in modo statico, per esempio con le seguenti scelte
 - subnet IP 192.168.0.0/29 (subnet mask 255.255.255.248), che mette a disposizione 6 indirizzi IPv4 dei quali due sono assegnati agli apparati di telemetria, uno allo switch amministrabile, uno alla porta Ethernet del ponte radio e uno a un eventuale PC di servizio

- subnet IP 192.168.10.0/29 (subnet mask 255.255.255.248), che mette a disposizione 6 indirizzi IPv4 dei quali due sono assegnati alle telecamere e uno a un eventuale PC di servizio;
- Come cablaggio si utilizzano cavi in rame F/UTP in categoria 6 per collegare gli apparati e cavi U/UTP per collegare i PC di servizio.

b) dopo aver fatto un'ipotesi sul data rate necessario per la videosorveglianza, con o senza compressione video, ed aggiungendo 4 flussi da 2,048 Mbit/s per il DAB stream e 3Mbit/s complessivi per coprire le esigenze dell'apparato di telemetria allarmi e della porta di supervisione del trasmettitore, dimensioni la tratta radio con un margine di fading di almeno 30dB, scegliendo l'opportuna modulazione;

- **Data rate della videosorveglianza**

Per quanto concerne il data rate necessario per la videosorveglianza, si può far notare che un segnale video digitalizzato determina un bit rate molto elevato e quindi non è conveniente trasmetterlo senza compressione. Infatti se per semplicità si considera un segnale video analogico digitalizzato (vedi tabella 1 cap. 2 vol. 2) si ha un data rate che supera i 200 Mbit/s.

TABELLA 1
Banda, frequenza di campionamento, bit rate del segnale digitalizzati o digitali.

Per concludere, nella **TABELLA 1** sono poste a confronto le bande che normalmente vengono assegnate ai segnali che abbiamo esaminato e il bit rate che deriva dalla loro digitalizzazione.

Tipo di segnale	Banda (Hz)	Frequenza di campionamento	Codifica A/D (bit/campione)	Bit rate ⁸
Musica, registrazione professionale	20 ÷ 22 · 10 ³	48, 96, 192 kHz	20, 24, 32	960 o superiore
Musica alta fedeltà (qualità CD)	20 ÷ 20 · 10 ³	44,1 kHz	16	705,6 kbit/s, pari a ⁹ 88,2 kB/s
Musica (qualità radio FM o «quasi CD»)	20 ÷ 15 · 10 ³	32 kHz	16	512 kbit/s
Voce alta qualità	50 ÷ 7000	16 kHz	14	224 kbit/s ¹⁰
Telefonico analogico	300 ÷ 3400	8 kHz	8	64 kbit/s (PCM)
Video analogico	≈ 5 · 10 ⁶	13,5 MHz	8	216 Mbit/s ¹¹
Digitale	≈ $\frac{1}{t_{simb}}$	-	-	$\frac{1}{t_{simb}} \cdot \log_2 m$ ¹²

⁸ Si intende il bit rate derivato dalla pura conversione analogico-digitale (A/D), tale valore può essere ridotto tramite una opportuna compressione.

⁹ Per un segnale mono, per un segnale stereo tale valore raddoppia. Si ricorda inoltre che 1 byte = 8 bit.

¹⁰ Tale valore viene ridotto tramite opportuna compressione, per esempio a 64 kbit/s.

¹¹ Tale valore viene ridotto tramite opportuna compressione, per esempio a circa 2 Mbit/s.

¹² Il bit rate si ottiene moltiplicando il numero di simboli/s (pari a $x = 1/t_{simb}$) per il numero di bit associati a ciascun simbolo ($\log_2 m$); infatti il numero di bit associabili a una delle m ampiezze diverse che può assumere un segnale digitale è pari a $\log_2 m$. Se $m = 2$ si ha il segnale binario puro, in cui un simbolo è associato a un bit.

Il data rate prodotto da una telecamera digitale è invece dato dal prodotto della risoluzione impostata, che determina il numero di pixel, per il numero di frame/s (quadri/s trasmessi) per il numero di bit con cui si codifica un pixel. Il valore del bit rate è in ogni caso elevatissimo².

Poiché il data rate di un segnale video compresso dipende da svariati fattori (risoluzione, tipo di compressione: H.264, H.265, ecc.) a seconda della qualità desiderata e dell'algoritmo di compressione si può assumere indicativamente un valore compreso tra 384 kbit/s e 10 Mbit/s. Per avere una buona qualità consideriamo un data rate di 2 Mbit/s ottenuto con H.264. Complessivamente il data rate che deve essere supportato dal ponte radio è quindi pari a circa:

$$DR_{totale} \approx (2 \cdot 2 \cdot 10^6)_{videosorv.} + (4 \cdot 2 \cdot 10^6)_{flussi_DAB} + (3 \cdot 10^6)_{Telem+superv} = 15 \text{ Mbit/s}$$

- **Dimensionamento della tratta radio.**

Si schematizza il problema secondo lo schema di FIGURA 18 CAPITOLO 9, indicando anche i dati a disposizione.

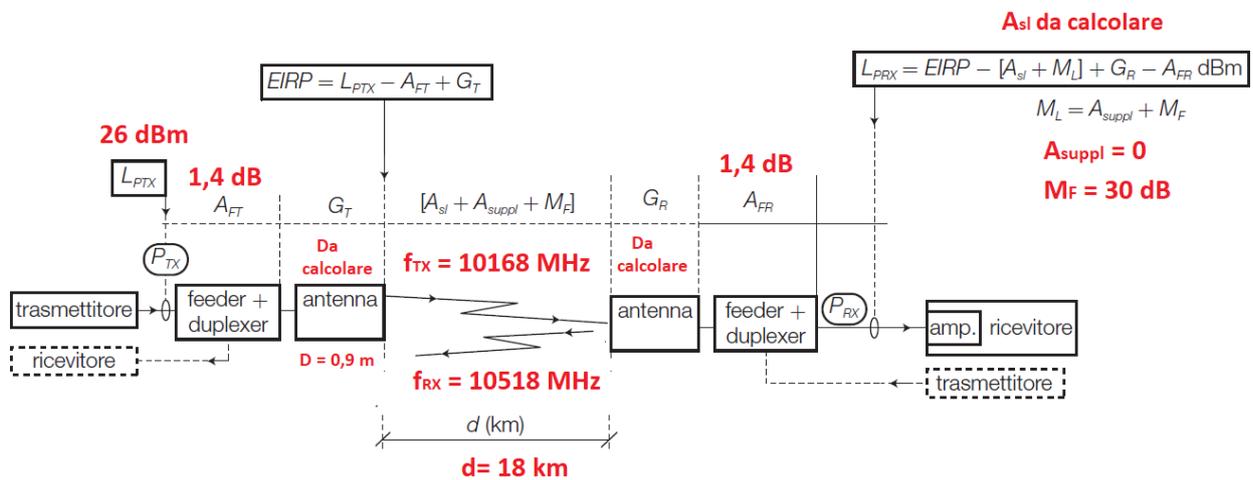


FIGURA 18 Bilancio di potenza di un collegamento in ponte radio.

Si ipotizza che la frequenza più bassa venga usata nella tratta da monte a valle (MV), perché è la frequenza meno attenuata, mentre la frequenza più alta venga usata nella tratta da valle a monte (VM).

In entrambe le direzioni si suppone di operare con il massimo livello di potenza in trasmissione ($L_{pTX} = 26 \text{ dBm}$).

Si calcola il guadagno delle antenne nelle due direzioni (il guadagno sarà diverso in quanto si utilizzano due frequenze per realizzare la comunicazione bidirezionale) con la formula:

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

² Per esempio con una risoluzione di 1280x720 (HD), con 24 frame/s (immagini in movimento sufficientemente fluide), con una codifica di 16 bit/pixel si ha un data rate (DR) pari a $DR = 1280 \times 720 \times 24 \times 16 = 353 \text{ Mbit/s}$

$$G_{ant_MV} = 18,5 + 20 \log(0,9) + 20 \log(10,168) = 37,8 \text{ dB}$$

$$G_{ant_VM} = 18,5 + 20 \log(0,9) + 20 \log(10,168) = 38,1 \text{ dB}$$

- **Dimensionamento della tratta da monte a valle (MV).**

Guadagno dell'antenna parabolica: $G_{ant_MV} = 37,8 \text{ dB}$

Attenuazione della guida d'onda (comprensiva anche del circolatore che separa i sensi di TX e RX, accoppiandoli alla stessa antenna): $A_F = 1,4 \text{ dB}$

Si calcola l'EIRP del sistema trasmittente da Monte a Valle con la formula:

$$EIRP = L_{PTX[dBm]} - A_{FT[dB]} + G_{T[dB]} \text{ [dBm]} \quad (9.6)$$

$$EIRP_{MV} = 26 - 1,4 + 37,8 = 62,4 \text{ dBm}$$

Si calcola l'attenuazione dello spazio libero con la formula:

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

$$A_{sl_MV} = 92,5 + 20 \log(18) + 20 \log(10,168) = 137,8 \text{ dB}$$

Si calcola il livello di potenza in ingresso al ricevitore con la formula:

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

dove M_L è il margine di fading richiesto, pari a 30 dB

$$L_{pRX_MV} = EIRP_{MV} - [137,8 + 30] + 37,8 - 1,4 = -69 \text{ dBm}$$

- **Dimensionamento della tratta da valle a monte (VM).**

Guadagno dell'antenna parabolica: $G_{ant_VM} = 38,1 \text{ dB}$

Attenuazione della guida d'onda, o feeder d'antenna, (comprensiva anche del circolatore):

$$A_F = 1,4 \text{ dB}$$

Si calcola l'EIRP del sistema trasmittente da Valle a Monte con la formula:

$$EIRP_{VM} = 26 - 1,4 + 38,1 = 62,7 \text{ dBm}$$

Si calcola l'attenuazione dello spazio libero con la formula:

$$A_{sL_{VM}} = 92,5 + 20 \log(18) + 20 \log(10,518) = \mathbf{138 \text{ dB}}$$

Si calcola il livello di potenza in ingresso al ricevitore con la formula:

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

dove M_L è il margine di fading richiesto, pari a 30 dB

$$L_{PRX_{VM}} = 26 - [138 + 30] + 38,1 - 1,4 = \mathbf{-68,6 \text{ dBm}}$$

Comparando il livello in ricezione con le diverse sensibilità riportate tra i dati del ponte radio si determina che **NON si può utilizzare la modulazione 256QAM.**

Sarebbe possibile, ma non consigliabile, utilizzare la modulazione 128 QAM, che richiede un livello di potenza in ricezione di almeno -71 dBm (sensibilità) e con cui si ottiene una capacità trasmissiva dei dati (payload) pari a circa 74 Mbit/s.

Infatti, poiché il ponte radio deve supportare un data rate complessivo di circa 15 Mbit/s, è preferibile optare per *una modulazione meno efficiente ma più robusta*, che necessiti di un livello di potenza in ricezione inferiore, aumentando così il margine di fading e l'affidabilità del ponte radio. Si può così optare per una modulazione 64QAM (sensibilità = -74 dBm, Payload di circa 61 Mbit/s) o volendo massimizzare il margine e l'affidabilità anche per una 16QAM (sensibilità -81 dBm, payload di circa 36 Mbit/s).

c) realizzi una connessione sicura attraverso la rete internet per il collegamento tra lo studio radiofonico e il centro di sorveglianza e controllo, tramite opportuni apparati e protocolli;

Si ipotizza che nello studio radiofonico sia presente una sottorete IP (*subnet VDS*, configurata con indirizzi IP privati) su cui transitano i flussi della videosorveglianza, così come nel centro di security remoto sia presente una subnet (*subnet CDS*, configurata con indirizzi IP privati) a cui sono diretti i flussi della videosorveglianza.

Per realizzare una connessione sicura attraverso Internet che colleghi la subnet VDS dello studio radiofonico alla subnet CDS del centro di security remoto è possibile impiegare una *VPN (Virtual Private Network) site-to-site*.

La VPN può essere realizzata impiegando nelle due sedi, per l'accesso a Internet, dei router che integrano un firewall³ con funzionalità VPN e la *suite di protocolli IPsec*, per la cui descrizione si rimanda al corso di Sistemi e reti. La VPN crea un *tunnel* che collega *in modo protetto* le due sedi e quindi ha come *endpoint* due indirizzi IPv4 pubblici, quelli dell'interfaccia WAN (esposta su Internet) di ciascuno dei due router/Firewall.

Nella VPN *site-to-site* che si viene a instaurare il traffico "interessante", costituito dai flussi video che devono transitare attraverso il "tunnel" VPN, è quello che ha come indirizzi IP sorgente quelli appartenenti alla subnet VDS.

³ Il firewall VPN può anche essere un dispositivo fisico distinto rispetto al router.

A titolo esemplificativo si delineano i passi con cui si può configurare una VPN sul router/firewall dello studio radiofonico.

L'interfaccia esterna (WAN) del router/firewall costituisce l'*endpoint* lato studio.

L'altro *endpoint*, lato centro di security, è l'indirizzo IP pubblico dell'interfaccia esterna (WAN) del router/firewall del centro di security.

Si può procedere quindi nel seguente modo⁴.

1. Sull'interfaccia di configurazione del router/firewall si seleziona: *VPN -> Site-to-Site VPN*
2. si sceglie l'interfaccia esterna che costituisce l'*endpoint* della VPN lato studio
3. si configura l'indirizzo IP dell'altro *endpoint*, lato centro security
4. si sceglie il metodo di autenticazione con chiave pre-condivisa (*Pre-Shared Key*) e si configura la relativa chiave (metodo più semplice rispetto a quello dei certificati)
4. si sceglie il tipo di crittografia (DES, 3DES, AES-128 ecc.) e di autenticazione (SHA, MD5) che si vogliono impiegare.
5. si crea e si seleziona un proprio *transform set*, il quale specifica gli algoritmi di crittografia e autenticazione che sono usati per proteggere i dati e che realizzano il tunnel VPN; il router/firewall remoto deve essere configurato con lo stesso *transform set* per poter comunicare
6. si configurano gli indirizzi IP della subnet VDS (sottorete dello studio) e della subnet CDS (sottorete remota del centro di sicurezza) che devono essere messe in comunicazione in modo protetto.

Si procede in modo analogo nel centro di security.

Una volta terminate le configurazioni si effettua il test dei tunnel. Se tutto è stato configurato correttamente la VPN diventa attiva (*Status: Up*) e la subnet VDS dello studio radiofonico è messa in comunicazione con la subnet CDS remota. Per confermare l'avvenuta connessione tra le due subnet IP si possono effettuare dei *ping* da un dispositivo della subnet VDS verso uno della subnet CDS, utilizzando il suo indirizzo IP *privato*.

- d) Definisca⁵ un socket IP, con un linguaggio a scelta, tra l'HUB di telemetria e lo studio, per visualizzare su un PC di supervisione i dati di allarme e la condizione della stazione di monte.

Data la natura privata della connessione tra lo studio radiofonico e lo HUB si ipotizza il ricorso al protocollo di trasporto UDP, la cui mancanza di affidabilità non è normalmente apprezzabile in un contesto come questo. Per la verifica delle condizioni si può implementare un semplice protocollo applicativo in cui il client (il PC posto nello studio radiofonico) invia al server collocato nello hub richieste come le seguenti:

“CHECK1”

“CHECK2”

“CHECK3”

...

per richiedere lo stato attuale di una condizione identificata numericamente. Il server risponde alle singole richieste con uno stato corrispondente ad uno dei tre caratteri “N” (stato *Normal*), “W” (stato *Warning*), o “A” (stato *Alarm*).

Per la definizione del socket si impiega il linguaggio di programmazione *Python*⁶.

⁴ I passi illustrati si riferiscono alla configurazione di una VPN site-to-site fatta su router/ firewall Cisco con il software di configurazione Cisco Configuration Professional

⁵ Soluzione a cura dei proff. Giorgio Meini e Giuseppe Di Palma

⁶ Python consente l'uso di socket UDP mediante una API (*Application Programming Interface*) che implementa il classico standard Berkley per le API di gestione dei socket.

Il seguente è il frammento di codice Python che realizza un semplice **server UDP** che implementa il protocollo applicativo sopra definito:

```
import socket
# definisce i possibili stati
possibiliStati = ('N','W','A')

IndirizzoIPLocale = "127.0.0.1"
PortaLocale       = 20001
DimensioneBuffer  = 1024

# crea un datagram socket (protocollo UDP)
UDPServerSocket = socket.socket(family=socket.AF_INET, type=socket.SOCK_DGRAM)

# associa al socket le informazioni su indirizzo IP e porta del server
UDPServerSocket.bind((IndirizzoIPLocale, PortaLocale))

print("Server in attesa di richieste...")
# ciclo di attesa delle richieste
while(True):
    Richiesta = UDPServerSocket.recvfrom(DimensioneBuffer)
    bytesMessaggio = Richiesta[0]
    strMessaggio = bytesMessaggio.decode()
    indirizzoClient = Richiesta[1]
    # visualizza informazioni sulla richiesta ricevuta
    print("Richiesta proveniente da: ", indirizzoClient)
    print("Richiesta per la condizione: ", strMessaggio[5])

    # genera la risposta per il client
    if strMessaggio=="CHECK1":
        ...
        risposta = ...
    elif strMessaggio=="CHECK2":
        ...
        risposta = ...
    elif strMessaggio=="CHECK3":
        ...
        risposta = ...

    # visualizza la risposta da inviare
    print("Stato: ", risposta)
    # codifica la risposta da inviare
    MessaggioDalServer = risposta
    BytesDaInviare = str.encode(MessaggioDalServer)
    # invia la risposta al client
    UDPServerSocket.sendto(BytesDaInviare, indirizzoClient)
```

Il seguente è il frammento di codice Python che realizza un semplice **client UDP** che implementa il protocollo applicativo sopra definito per la condizione 1

```
import socket

IndirizzoServer      = ("...", 20001)
DimensioneBuffer     = 1024
AttesaMax            = 1 # attesa massima per la risposta (s)

MessaggioDalClient   = "CHECK1"

# codifica la richiesta per il server
bytesDaInviare = str.encode(MessaggioDalClient)

# Crea datagram socket (protocollo UDP)
UDPClientSocket = socket.socket(family=socket.AF_INET, type=socket.SOCK_DGRAM)

# imposta il timeout
UDPClientSocket.settimeout(AttesaMax)

# invia la richiesta al server
UDPClientSocket.sendto(bytesDaInviare, IndirizzoServer)

# attende di ricevere la risposta dal server
try:
    # ricezione della risposta dal server
    Risposta = UDPClientSocket.recvfrom(DimensioneBuffer)
    # decodifica la risposta
    Risposta = Risposta[0].decode()
    # gestisce il messaggio all'utente
    if Risposta=="N":
        ...
    elif Risposta=="W":
        ...
    elif Risposta=="A":
        ...
except:
    # mancata risposta entro il timeout impostato
    ...
```

SECONDA PARTE

1. Due reti LAN di due edifici separati fisicamente, la prima chiamata *rete1* con 12 host e la seconda chiamata *rete2* con 5 host compreso un server dati, sono connessi tra loro attraverso un router, che a sua volta ha una porta verso la rete internet. Definire il **piano di indirizzamento delle due reti LAN** e individuare una Access Control List da configurare sul router per **impedire il traffico FTP** dalla *rete1* verso il server dati della *rete2*.

- **Piano di indirizzamento**

RETE 1, con 12 HOST

Si opta per un piano di indirizzamento ottimizzato.

Si ipotizza che oltre agli host intesi come dispositivi impiegati dagli utenti (PC), che necessitano di 12 indirizzi IP, e all'interfaccia Ethernet del router, che costituisce il gateway predefinito, si impieghi uno switch amministrabile, che può essere gestito e monitorato da remoto, per cui sono necessari 14 indirizzi IPv4, a cui vanno aggiunti l'indirizzo IP di rete (subnet) e l'indirizzo di broadcast, per un totale di 16 indirizzi IPv4.

Si sceglie quindi di usare la subnet mask /28 (255.255.255.240) che mette a disposizione 4 bit per la porzione host degli indirizzi IP a cui viene associata e quindi consente di avere $2^4 - 2 = 14$ indirizzi IP per la configurazione di tutti i dispositivi. In questo modo non vi sono ulteriori indirizzi IP disponibili e ciò può aumentare la sicurezza della rete in quanto non sono possibili inserimenti abusivi senza determinare conflitti con gli indirizzi IP assegnati.

Per la configurazione si sceglie un blocco di indirizzi IPv4 privato, per esempio il **10.0.0.0/28**, con subnet mask in notazione decimale puntata **255.255.255.240**.

Il piano di indirizzamento per la **RETE 1** può quindi essere il seguente.

Indirizzo IPv4	Subnet mask	Assegnato a
10.0.0.0	255.255.255.240	Indirizzo di rete (subnet IP)
10.0.0.1	255.255.255.240	Interfaccia Ethernet del router (gateway predefinito)
10.0.0.2	255.255.255.240	Switch amministrabile
10.0.0.3	255.255.255.240	HOST 1
.....	
10.0.0.14	255.255.255.240	HOST 12
10.0.0.15	255.255.255.240	Indirizzo di broadcast

Se invece si desidera avere una ridondanza negli indirizzi IP, allora è necessario scegliere la subnet mask /27 (255.255.255.224), che mette a disposizione 5 bit per la parte host degli indirizzi IP associati e quindi un massimo di $2^5 - 2 = 30$ indirizzi IP per la configurazione dei dispositivi.

RETE 2, con 5 HOST

Oltre ai 5 host è necessario assegnare un indirizzo IP all'interfaccia del router, che fa da gateway predefinito per la rete 2. Inoltre anche in questa rete si ritiene necessario impiegare uno *switch amministrabile*, a cui va assegnato un indirizzo IP. Il numero di indirizzi IP necessari risulta pari a 7, a cui vanno aggiunti l'indirizzo di rete (subnet) e l'indirizzo di broadcast, per un totale di 9 indirizzi IPv4.

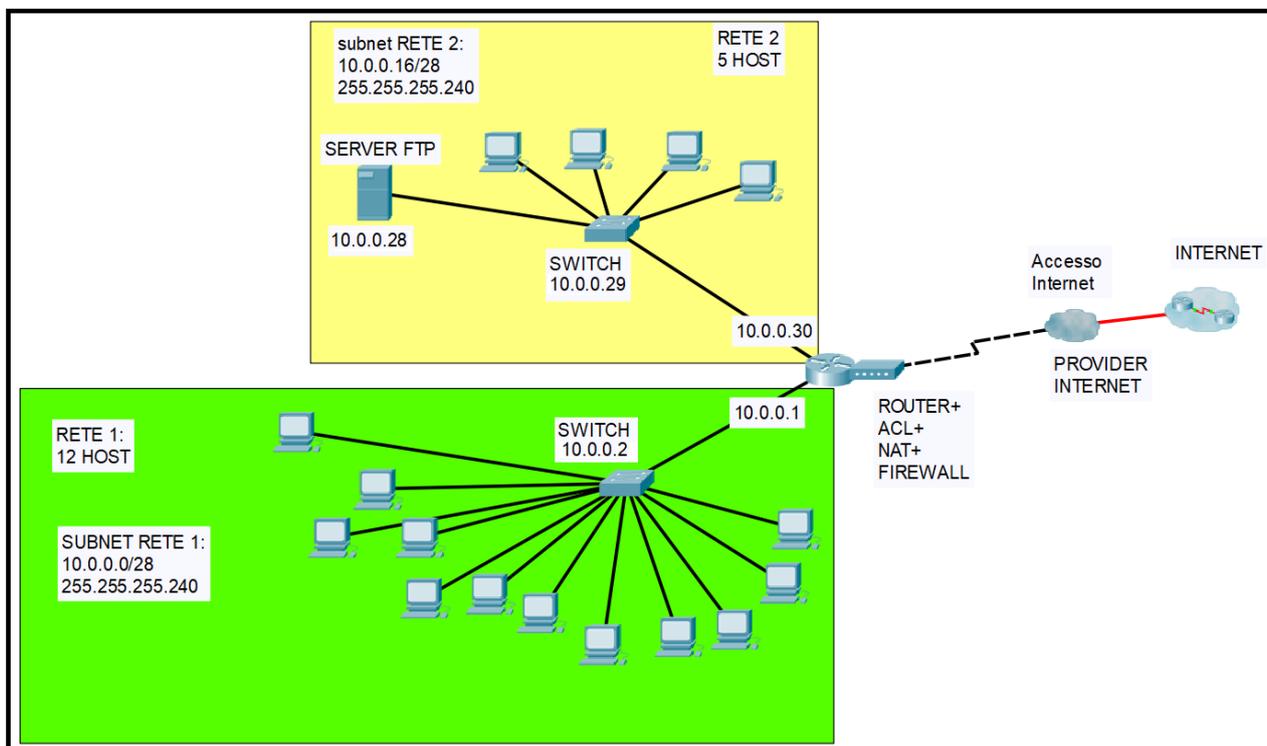
Gli indirizzi IP devono quindi avere la porzione host di almeno 4 bit per cui si sceglie di usare la subnet mask /28 (255.255.255.240). In questo modo si hanno a disposizione $2^4 - 2 = 14$ indirizzi IPv4 per gli host, con una ridondanza di 7 indirizzi IP per usi futuri.

Si sceglie poi il blocco di indirizzi IPv4 privato contiguo a quello della rete 1 (10.0.0.0/28): **10.0.0.16/28**, la cui subnet mask espressa in notazione decimale puntata è **255.255.255.240**.

Il piano di indirizzamento per la rete 2 può quindi essere il seguente.

Indirizzo IPv4	Subnet mask	Assegnato a
10.0.0.16	255.255.255.240	Indirizzo di rete
10.0.0.17	255.255.255.240	HOST 1
10.0.0.18	255.255.255.240	HOST 2
10.0.0.19	255.255.255.240	HOST 3
10.0.0.20	255.255.255.240	HOST 4
10.0.0.28	255.255.255.240	SERVER FTP
10.0.0.29	255.255.255.240	Switch amministrabile
10.0.0.30	255.255.255.240	Interfaccia Ethernet del router (Gateway predefinito)
10.0.0.31	255.255.255.240	Indirizzo di Broadcast

L'infrastruttura di rete si può quindi schematizzare come in figura.



ACL da configurare sul router

Poiché si desidera impedire solo il traffico FTP dalla RETE 1 verso il server della RETE 2 è necessario impiegare una ACL estesa che impedisca solo il traffico verso la porta TCP di controllo associata all'applicazione server FTP (porta 21) residente sul computer server (con indirizzo IP 10.0.0.28 nel piano di indirizzamento proposto).

L'ACL comprende quindi le seguenti due regole esplicite:

- I. Nega (**deny**) l'inoltro a Indirizzi IP sorgente appartenenti alla rete 1 (**10.0.0.0**), con la relativa **wildcard mask** (subnet mask con i bit invertiti: 255.255.255.240 diventa 0.0.0.15), verso la porta **tcp 21** (o **ftp**) dell'**host** server (**10.0.0.28**)

- II. Permetti (**permit**) il traffico IP a indirizzi IP sorgente appartenenti alla rete 1 (**10.0.0.0**), con la relativa wildcard mask (**0.0.0.15**), verso qualsiasi indirizzo IP di destinazione (**any**).

L'ACL viene applicata in uscita (*out*) sull'interfaccia del router appartenente alla rete 2 (10.0.0.30), a cui appartiene anche il server FTP.

A titolo esemplificativo si riportano i comandi che possono essere dati a un router Cisco System:

```
router_internet(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.15 host 10.0.0.28 eq ftp
router_internet(config)#access-list 110 permit ip 10.0.0.0 0.0.0.15 any
```

L'ACL è applicata in uscita all'interfaccia ethernet (es. Gi 0/0, 10.0.0.30) della rete a cui appartiene il server FTP.

```
router_internet(config)#interface Gi 0/0
router_internet(config-if)#ip access-group 110 out
```

2. Una fibra ottica monomodale ha una lunghezza di **70km** e un coefficiente di dispersione cromatica @ 1550nm pari a **$D_0=18 \text{ ps}/(\text{nm} \cdot \text{km})$** . Descrivere la **dispersione modale** e la **dispersione cromatica** di una fibra ottica e determinare **la banda** e la **capacità della fibra**, considerando una sorgente **VCSEL con $\Delta\lambda = 0,5 \text{ nm}$** .

In una fibra ottica (f.o.) la dispersione è una forma di distorsione degli impulsi ottici che determina un allargamento temporale dell'impulso di uscita rispetto all'impulso in ingresso: l'impulso in uscita ha una durata maggiore dell'impulso lanciato in ingresso alla f.o. Quando si trasmette un segnale digitale associando l'1 e lo 0 (detti *simboli*) alla presenza o assenza di impulsi ottici (codifica di linea NRZ) ciò determina una interferenza tra i simboli, detta interferenza intersimbolica o ISI (*InterSymbol Interference*), che può determinare l'impossibilità di riconoscere correttamente il flusso di bit logici associato al segnale trasmesso (non si riconosce correttamente la presenza o l'assenza di impulsi ottici). In presenza di dispersione consistente, per rendere trascurabile l'ISI è necessario aumentare il tempo di bit e quindi diminuire la velocità di trasmissione. In sostanza quindi la dispersione pone un limite alla banda utile della fibra ottica e alla sua capacità trasmissiva.

► In presenza di dispersione, per mantenere l'ISI entro limiti accettabili è necessario limitare il numero di bit/s che si trasmettono, il che corrisponde ad avere un limite sulla banda trasmissiva disponibile.

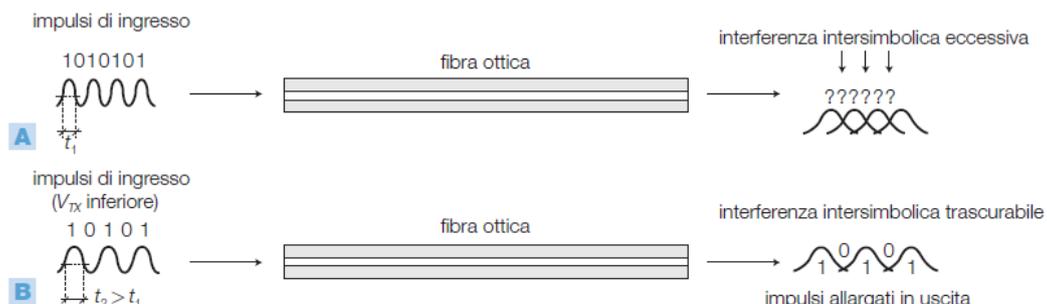
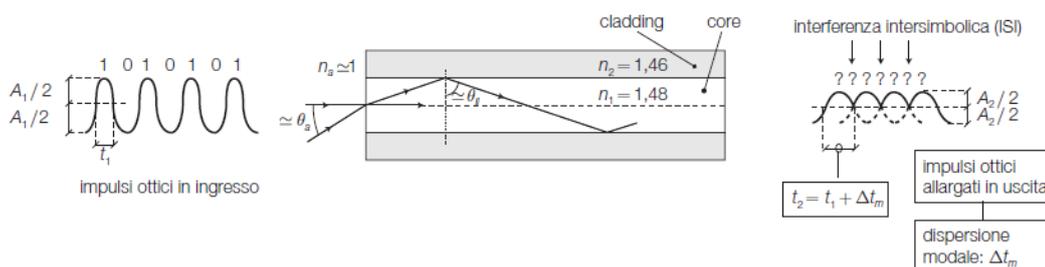


FIGURA 7 **A)** La dispersione causa interferenza intersimbolica (ISI) a velocità elevate. **B)** Riducendo la velocità si riduce l'ISI.

La **dispersione modale** è presente solo nelle **f.o. multimodali** ed è dovuta al fatto che un impulso ottico lanciato nella f.o. può essere considerato come la somma di tanti raggi ottici che entrano nella f.o. con angoli diversi (compresi nell'angolo di accettazione) e quindi subiscono una rifrazione diversa, il che comporta dei percorsi diversi nella propagazione lungo la f.o. Considerando una f.o. multimodale step index, in prima approssimazione la velocità di propagazione è data dal rapporto tra la velocità della luce e l'indice di rifrazione del *core* ($V_{propag.} = c/n_{core}$), per cui raggi ottici che compiono percorsi diversi viaggiando alla stessa velocità arrivano in tempi diversi all'uscita e ciò comporta un allargamento dell'impulso ottico di uscita.

Questo fenomeno provoca una distorsione in quanto l'energia associata ai diversi modi giunge all'uscita in tempi diversi facendo sì che la forma dell'impulso in uscita risulta allargata rispetto a quella di ingresso. Essendo determinata dalla presenza di più modi questa forma di distorsione viene denominata **dispersione modale** (FIGURA 8).

FIGURA 8 Dispersione modale in una F.O. multimodale step index.



Per ridurre la dispersione modale si deve impiegare una f.o. multimodale *graded index*: l'indice di rifrazione del core è maggiore al centro e diminuisce gradualmente andando verso il cladding. In questo modo anche la velocità di propagazione di un raggio ottico cambia:

- se viaggia al centro della f.o. il raggio fa un percorso più breve ma a una velocità minore
- se subisce delle riflessioni nelle vicinanze del cladding il raggio compie dei percorsi più lunghi ma a una velocità media maggiore.

Un aumento della lunghezza del percorso viene compensato da una velocità di propagazione maggiore, per cui le differenze di ritardo tra i raggi e quindi la dispersione modale viene ridotta in modo consistente, con conseguente aumento della banda e della capacità trasmissiva.

Nelle f.o. multimodali la dispersione cromatica (che si esprime in ps) è normalmente trascurabile in quanto molto minore della dispersione modale (che si esprime in ns).

Nelle f.o. monomodali non vi è dispersione modale, in quanto i raggi ottici seguono tutti lo stesso percorso.

Nelle **f.o. monomodali** va però considerata la **dispersione cromatica**, che è la causa principale di limitazione della banda e della capacità trasmissiva di una f.o. monomodale.

La dispersione cromatica è dovuta alle imperfezioni delle sorgenti ottiche (diodi LASER) che non emettono un segnale monocromatico puro, avente cioè una sola lunghezza d'onda, ma generano delle componenti spettrali indesiderate e quindi un segnale ottico caratterizzato da componenti distribuite su una certa larghezza spettrale $\Delta\lambda$. Poiché il materiale che compone la f.o. si comporta in maniera diversa al variare della lunghezza d'onda, determinando una modifica del valore dell'indice di rifrazione e quindi della velocità di propagazione dei raggi ottici, si ha che l'impulso ottico lanciato nella f.o. si può considerare come fatto da raggi ottici che compiono lo stesso percorso, ma sono caratterizzati da λ diverse e quindi da velocità di propagazione diverse, per cui subiscono ritardi diversi dando così origine a un allargamento temporale degli impulsi che si hanno in uscita dalla f.o., fenomeno denominato **dispersione cromatica**.

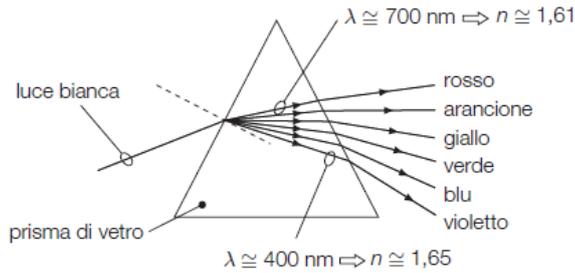


FIGURA 9 Esempio di variazione dell'indice di rifrazione con la lunghezza d'onda⁶.

► Il parametro che viene utilizzato per definire le caratteristiche di una F.O. monomodale, relativamente alla dispersione cromatica, viene denominato **coefficiente di dispersione cromatica, D_c (ps/nm · km)**.

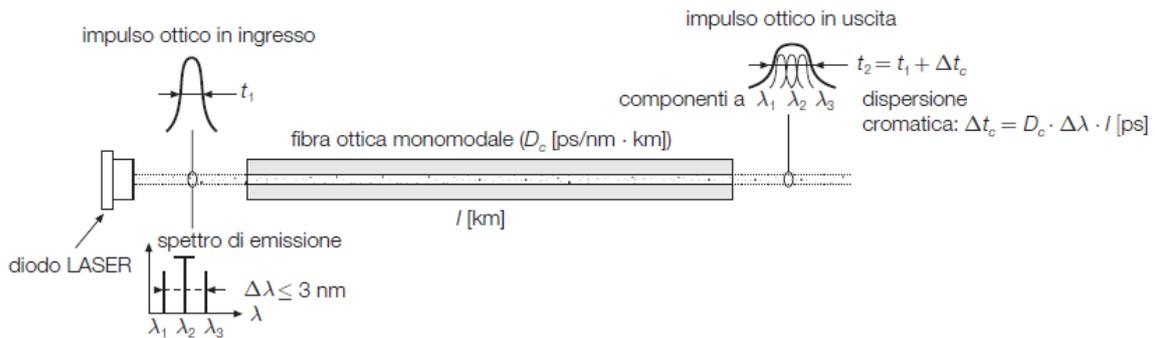


FIGURA 10 Dispersione cromatica.

La dispersione cromatica si calcola con la seguente relazione:

► La dispersione cromatica introdotta da una F.O. lunga l (km) si calcola come:

$$\Delta t_c = \Delta t_{c0[\text{ps/km}]} \cdot l_{[\text{km}]} = D_{c[\text{ps/nm}\cdot\text{km}]} \cdot \Delta \lambda_{[\text{nm}]} \cdot l_{[\text{km}]} \quad (5.8)$$

dove:

- D_c (ps/nm·km): coefficiente di dispersione cromatica; dipende dalle caratteristiche proprie della fibra;
- $\Delta \lambda$ (nm): larghezza dello spettro⁹ del segnale emesso dalla sorgente ottica (diodo LASER);
- l (km): lunghezza della F.O. espressa in km.

La banda della f.o. monomodale, detta anche banda cromatica, si può valutare con la seguente relazione

► La **banda cromatica, B_c** , di una F.O. monomodale lunga l km può essere stimata con la seguente relazione:

$$B_c = \frac{440}{(\Delta t_{c0[\text{ps/km}]} \cdot l_{[\text{km}]})} = \frac{440}{(D_{c-[\text{ps/nm}\cdot\text{km}]} \cdot \Delta \lambda_{[\text{nm}]} \cdot l_{[\text{km}]})} \text{ GHz} \quad (5.13)$$

dove:

- D_c (ps/nm · km): coefficiente di dispersione cromatica; dipende dalle caratteristiche proprie della fibra;
- $\Delta \lambda$ (nm): larghezza dello spettro del segnale emesso dalla sorgente ottica (diodo LASER);
- l (km): lunghezza della F.O.

per cui nel caso in esame si ha:

Dispersione cromatica $\rightarrow \Delta t_c = 18 \cdot 0,5 \cdot 70 = 630 \text{ ps}$

Banda cromatica $\rightarrow B_c = \frac{440}{\Delta t_c} = 700 \text{ MHz}$

In prima approssimazione la capacità (teorica) della f.o. si può calcolare come $C = 2B$, per cui il suo limite teorico è pari a $C = 1400 \text{ Mbit/s}$.

3. Un computer Linux ospita un sito web utilizzato per la consultazione dei dati di rilevazione ambientale dell'inquinamento atmosferico, rilevato da appositi sensori. Sul lato client la pagina web, tramite un form, consente all'utente di generare una richiesta al server; il server risponde su interfaccia web, fornendo le informazioni in base ai dati rilevati. Proporre una soluzione⁷ software per la realizzazione del servizio indicato.

La possibilità da parte di un server – nel caso specifico dotato di sistema operativo Linux – di fornire pagine web a richiesta di un client, che è normalmente un browser, è determinata dal fatto che esso esegue come servizio un web-server, ad esempio Apache HTTP server: è infatti il protocollo applicativo HTTP, basato a sua volta sul protocollo di trasporto TCP, che regola lo scambio di pagine web tra client e server.

La componente statica di una pagina web è codificata in linguaggio HTML con l'eventuale ricorso a regole CSS e codice JavaScript per la definizione degli aspetti grafici, di layout e di interazione con l'utente elaborati, visualizzati e gestiti dal browser. La componente dinamica – che in questo caso è data dallo stato dei sensori e dai valori da questi acquisiti – è normalmente generata lato server utilizzando linguaggi come PHP, Java, Python, Un'architettura software realistica, anziché una interazione diretta del codice di generazione della pagina web dinamica con i sensori, prevede la memorizzazione periodica da parte di un processo separato dello stato dei sensori e dei valori acquisiti in un database relazionale: in fase di generazione della pagina web dinamica il codice recupererà stato e valori dei sensori dal database.

Caratteristica comune a tutti i linguaggi di programmazione utilizzati per la generazione di pagine web dinamiche lato server è quello di produrre come output il codice

HTML/CSS/JavaScript che costituisce le pagine che sono restituite dal web-server in seguito alle richieste del browser.

⁷ Soluzione a cura del prof. Giorgio Meini

4. Un sistema FSK è utilizzato per trasmettere un flusso dati da 600bit/s su un cavo coassiale, impiegando le frequenze $f_1=1,3$ kHz e $f_2=1,7$ kHz. Descrivere brevemente il principio della modulazione, anche tramite disegni e/o schemi, determinare la deviazione di frequenza, la frequenza della portante, l'indice di modulazione e la banda occupata dal segnale modulato.

La modulazione FSK (*Frequency Shift Keying*) consiste nell'impiegare la modulazione di frequenza per trasmettere sequenze di bit associando due valori di frequenza ai due stati logici che può assumere un bit (rif. CAPITOLO 8 PAR. 5.5).

In ingresso al VCO si invia un segnale digitale avente escursione ΔV , tale da causare una variazione di frequenza totale (pari al doppio della deviazione di frequenza) pari a $2\Delta f = k_{1[\text{Hz/V}]} \cdot \Delta V$, che consente di generare le due frequenze da trasmettere, per esempio secondo la seguente associazione:

$$0 \Rightarrow f_0 = f_p - \Delta f; 1 \Rightarrow f_1 = f_p + \Delta f \quad (8.11)$$

dove:

- f_p : frequenza della portante;
- Δf : deviazione di frequenza.

Un modulatore FSK può quindi essere ottenuto pilotando un oscillatore controllato in tensione (VCO) con un segnale a due livelli corrispondenti agli stati logici di un bit. La tensione a livello basso fa produrre al VCO un segnale avente frequenza f_1 mentre il livello alto fa produrre la frequenza f_2 (si veda anche la FIGURA 1)

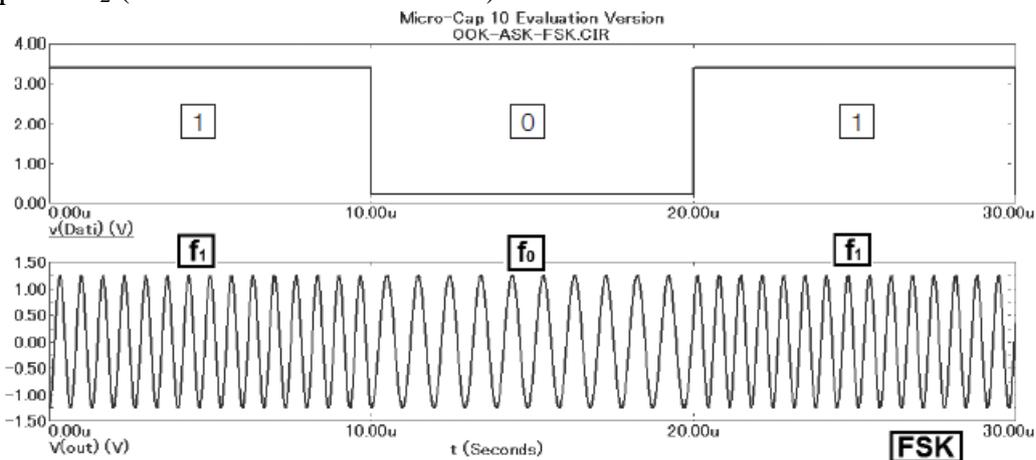


FIGURA 9 Segnale modulante e segnale modulato FSK.

La frequenza portante (f_p) e la deviazione di frequenza (Δf) risultano pari a:

$$f_p = \frac{f_1 + f_2}{2} = \frac{1300 + 1700}{2} = 1500 \text{ Hz}; \Delta f = \frac{f_2 - f_1}{2} = 200 \text{ Hz}$$

La frequenza massima del segnale modulante (f_{max}) si può ritenere all'incirca pari alla velocità di trasmissione (*bit rate*), pari a 600 bit/s nel caso in esame, per cui si ha $f_{\text{max}} = 600$ Hz (come evidenziato dalla FIGURA 2)

In prima approssimazione, l'indice di modulazione e la banda del segnale modulato si possono quindi calcolare come:

$$m_f = \frac{\Delta f}{f_{\max}} = \frac{200}{600} = 0,3 ; B_{FSK} = 2(\Delta f + f_{\max}) = 2(200 + 600) = 1600 \text{ Hz}$$

Una simulazione al computer evidenzia e conferma quanto sopra esposto.

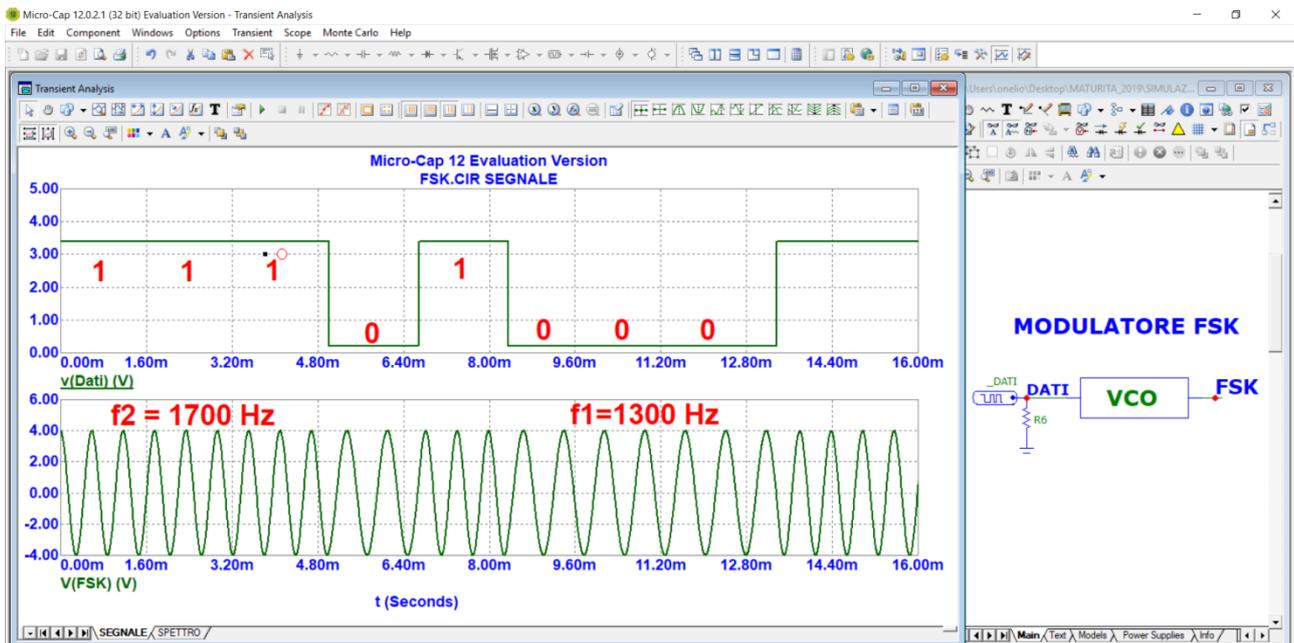


FIGURA 1 Segnale digitale (modulante) pseudocasuale e segnale modulato FSK.

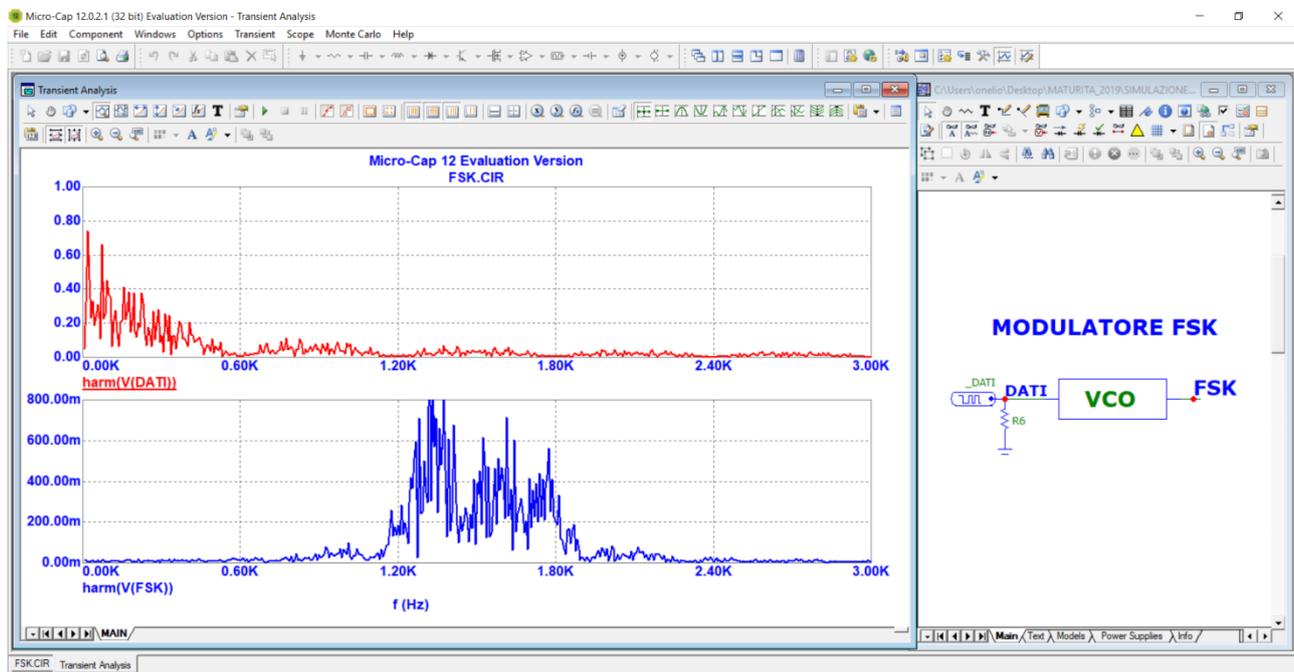


FIGURA 2 Spettri del segnale digitale (dati) e spettro del segnale modulato FSK.

Libri consigliati:

Onelio Bertazioli

Corso di Telecomunicazioni vol. 2 e vol. 3

ed. Zanichelli

Manuale Cremonese di Informatica e Telecomunicazioni