

Simulazione n. 1 della prova scritta di Telecomunicazioni per l'Esame di Stato (a cura del prof. Onelio Bertazioli)

Tema n° 1

La condivisione delle informazioni e lo sviluppo delle risorse informatiche tramite cui esse possono venire memorizzate e scambiate è diventata una assoluta priorità nella società attuale, tanto che per essa è stato coniato il termine “società dell'informazione”.

Le tecnologie impiegate per l'interconnessione di apparati informatici sia in ambito locale sia geografico hanno subito un forte sviluppo in questi ultimi anni e le infrastrutture di telecomunicazioni sono diventate risorse strategiche per lo sviluppo dell'economia di una nazione. Oltre alle innovazioni in ambito hardware, un ruolo fondamentale è ricoperto dall'impiego di protocolli standardizzati riconosciuti a livello mondiale. Il mondo della scuola può trarre grandi vantaggi dall'utilizzo delle tecnologie di rete sia in termini di organizzazione sia per la memorizzazione, la condivisione e il reperimento di informazioni.

Il candidato, formulando di volta in volta le ipotesi aggiuntive che ritiene necessarie:

1. Proponga un progetto per l'interconnessione in ambito locale dei computer di una scuola dotata di:
 - 5 laboratori attrezzati ciascuno con 15 computer;
 - un'aula con 10 computer a disposizione dei docenti;
 - 15 computer a disposizione della segreteria (uno dei quali funge da server per la segreteria);
 - 3 server, dei quali uno gestisce gli ordini e le giacenze a magazzino, uno funge da controllore di dominio, server DHCP e server DNS interno e uno da server WEB ed FTP.

Il progetto è costituito dallo schema della rete locale (LAN, Local Area Network) e da una relazione che dettagli le scelte fatte, evidenziandone i pregi, nei seguenti aspetti:

- standard tecnologico con cui si intende realizzare la rete; si illustrino le caratteristiche salienti dello standard prescelto in termini di tecnologia trasmissiva, metodo di accesso multiplo, architettura dei protocolli impiegati;
 - tipo di cablaggio da adottare e topologia scelta per la rete;
 - tipi di apparati impiegati;
 - architettura dei protocolli scelta per consentire la condivisione in rete di applicazioni e risorse.
2. Proponga un piano di indirizzamento IP per la rete e definisca quale deve essere la configurazione IP dei computer e degli apparati di rete su cui essa va configurata sapendo che l'ISP (Internet Service Provider) ha fornito i seguenti indirizzi IP di server DNS: 208.67.222.222 (primario); 208.67.220.220 (secondario).
 3. Proponga un progetto per dotare la scuola di un accesso a Internet di sufficiente capacità, integrandolo nel progetto di cui al punto 1. In particolare il candidato svolga almeno due dei seguenti punti:
 - a) illustri le problematiche sia trasmissive sia relative alla sicurezza della rete nel caso in cui si voglia inserire un ulteriore server WEB/FTP accessibile da Internet per fornire servizi usufruibili via Internet;
 - b) scelga il tipo di mezzo trasmissivo e il tipo di apparato da utilizzare per realizzare l'accesso a Internet;
 - c) illustri la tecnica di adattamento del segnale al mezzo trasmissivo impiegata dall'apparato scelto;

Durata della prova: 6 ore.

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

Non è consentito l'uso di libri di testo e appunti personali.

Non è consentito l'uso di telefoni cellulari, PDA, notebook e apparecchi simili, che devono essere spenti e posti in luogo adatto.

Soluzione tema n°1

Per la trattazione dettagliata delle tematiche inerenti la simulazione di tema d'esame proposta si rimanda al libro di testo

Onelio Bertazioli
Telecomunicazioni voll. A e B (2ª edizione)
Ed. Zanichelli

1. Per la trattazione generale delle LAN si rimanda all'Unità 11 del testo sopraccitato. Per la parte più pratica si rimanda anche all'esercitazione di laboratorio N. 6 contenuta nel testo. A titolo esemplificativo si riportano delle figure tratte dal testo citato.

La tecnologia che ormai costituisce lo standard di fatto per le LAN è l'Ethernet per cui si sceglie di realizzare una **LAN Ethernet 100BASE-TX**, o **FastEthernet** (si veda l'Unità 11 par. 11.7.1), le cui caratteristiche salienti sono le seguenti:

- opera a 100 Mbit/s;
- la trasmissione avviene in banda base con un opportuno **codice di linea** (denominato MLT-3, si veda l'Unità 7 par. 7.2.4);

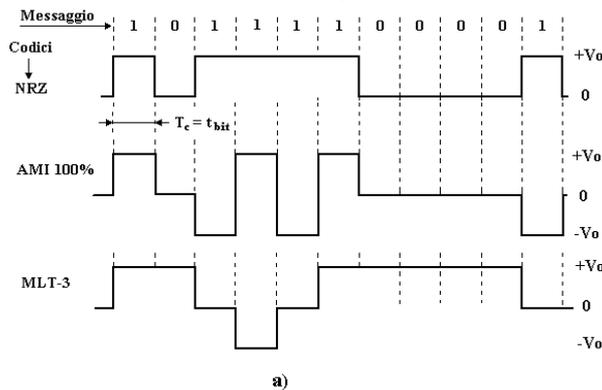


Figura 7.7 a) Codifica di linea MLT-3

- adotta il **metodo di accesso multiplo CSMA/CD**, descritto nel par. 11.5 (Unità 11), come specificato dallo standard IEEE 802.3u;

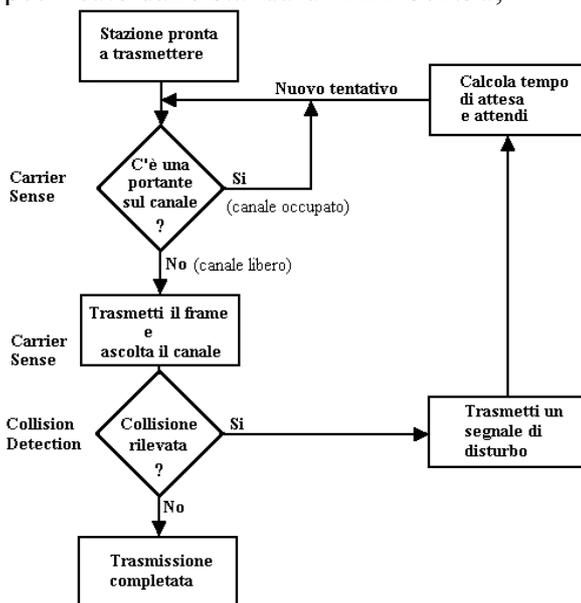


Fig. 11.2 Diagramma di flusso per il CSMA/CD

Metodo di accesso multiplo CSMA/CD

- l'architettura dei protocolli comprende i **primi due strati OSI**: lo strato fisico e lo strato 2, che nel modello generale comprende il **protocollo MAC (Medium Access Control)** e l'**LLC (Logical Link Control)**, si veda il par. 11.8 Unità 11. Per una descrizione più generale dell'architettura di una LAN si rimanda al par. 11.9 Unità 11;

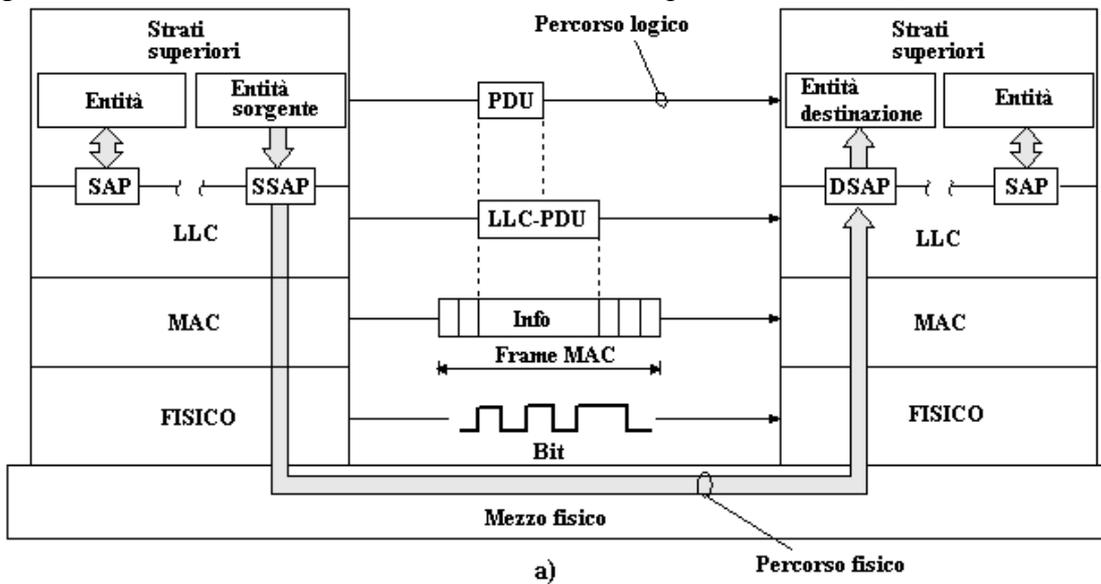


Fig. 11.10 a) Correlazione tra gli strati di una LAN;

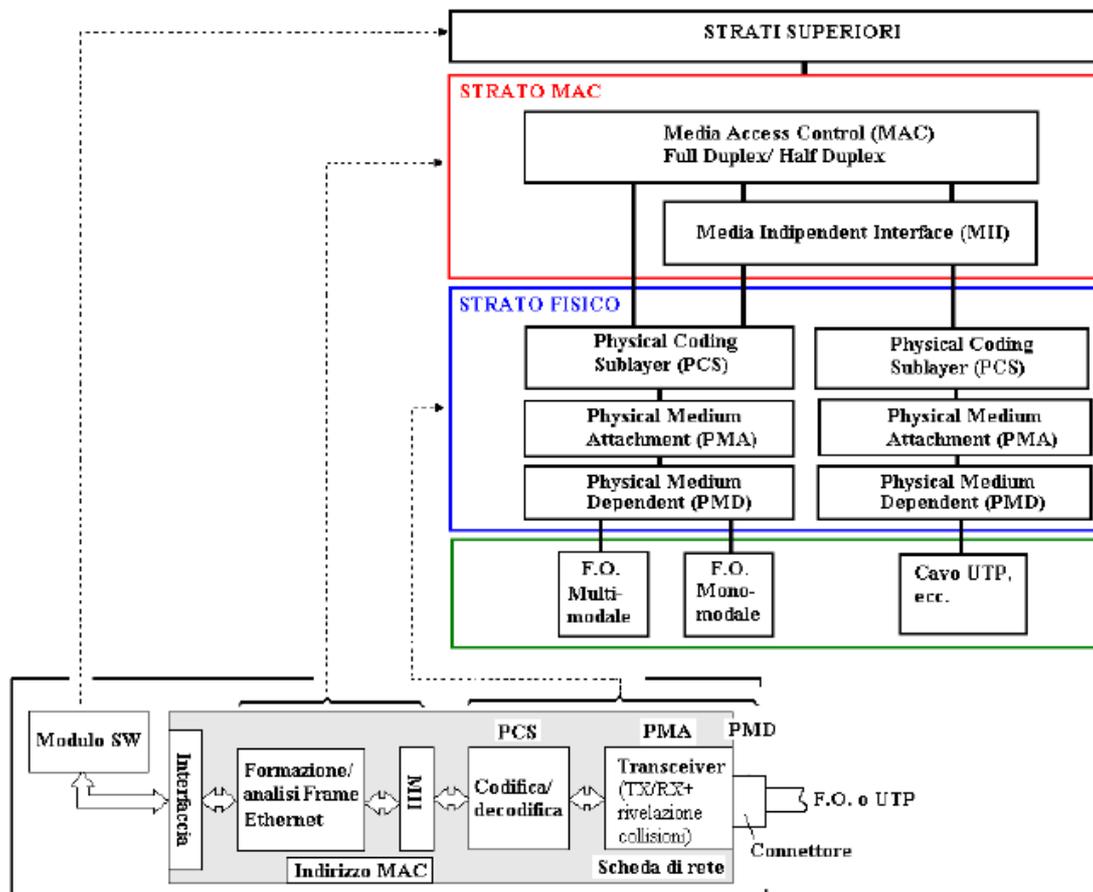


Fig. 11.7 Schema di principio di una scheda di rete posto in corrispondenza con l'architettura di rete Ethernet.

- si adotta la **suite di protocolli TCP/IP** per gli strati superiori al secondo (si veda l'Unità 9).

Per il cablaggio, da eseguire in modo conforme agli standard specificati dal cablaggio strutturato, si adottano **cavi a coppie simmetriche non schermati UTP** (Unshielded Twisted Pair) **in categoria 6** per collegare i computer alle prese di rete, mentre per la rimanente parte del cablaggio si scelgono **cavi schermati di tipo FTP**, sempre in categoria 6, meno sensibili ai disturbi. La scelta della categoria 6, invece della tradizionale categoria 5e, consente di realizzare un cablaggio che supporta meglio una transizione futura di almeno una parte della rete, per esempio quella che collega i server, verso la tecnologia Ethernet 1000BASE-T Unità 11 par. 11.7.2), operante a 1 Gbit/s.

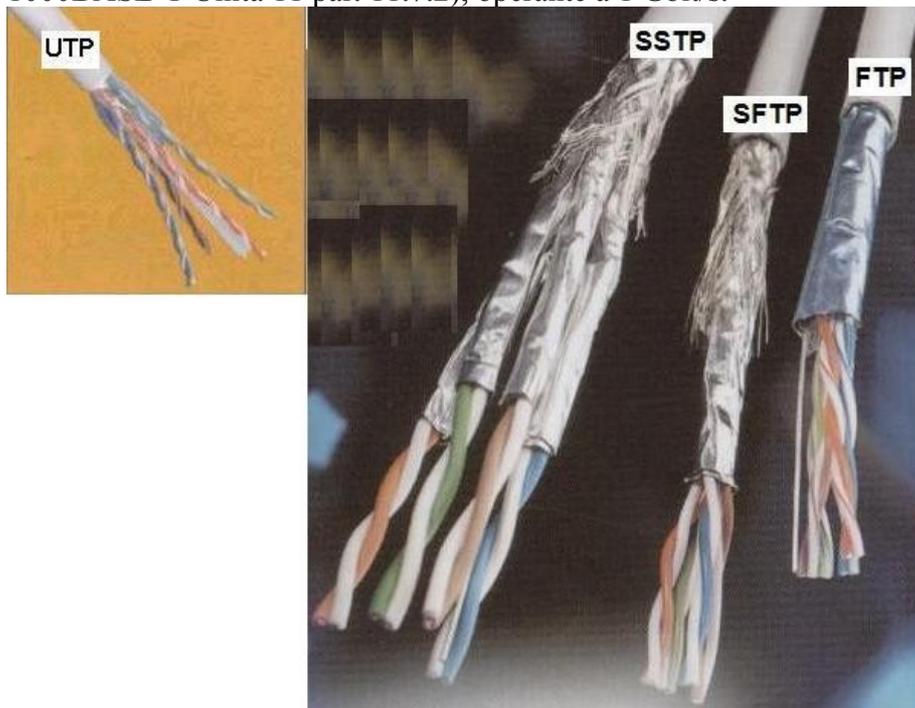


Figura 4.5 (vol. A)

Si adotta la **topologia a stella con l'impiego di switch** come apparati di rete.

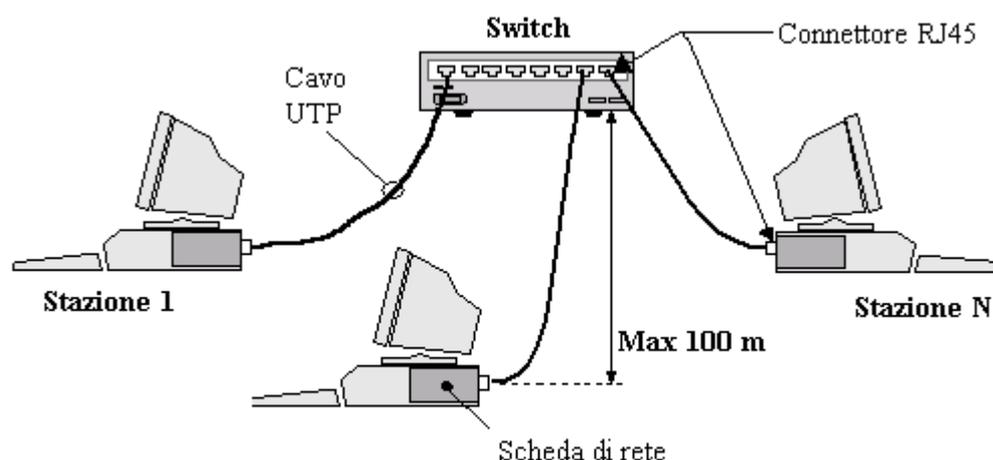


Fig. 11.1 c) topologia a stella

L'impiego degli switch aumenta le prestazioni della rete in quanto riduce il numero delle collisioni.

Si può quindi proporre di installare uno switch, per esempio a 24 porte¹, in ciascuno dei locali da cablare; gli switch possono poi essere collegati a uno switch principale, anch'esso a 24 porte, che deve avere caratteristiche tecniche più evolute.

Gli switch periferici (di accesso) possono anche essere non amministrabili, per risparmiare sui costi.

Lo switch centrale, invece, dovrebbe essere almeno uno **switch layer 2 amministrabile** in grado di suddividere la rete in un certo numero di **VLAN** (Virtual LAN, Unità 11 par. 11.7.3).

L'impiego delle VLAN consente di suddividere la rete, a livello 2, in segmenti distinti che non comunicano direttamente tra loro, aumentando così sia le prestazioni della rete (si riducono le dimensioni dei domini di broadcast) sia la sicurezza in quanto lo switch amministrabile non consente la comunicazione diretta tra PC che appartengono a VLAN diverse.

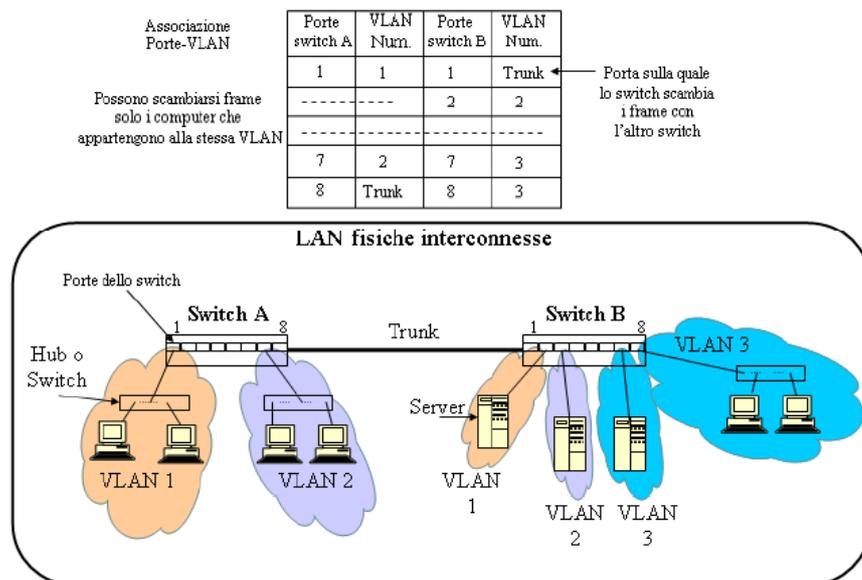


Fig. 11.5 Concetto di VLAN ed esempio di configurazione delle porte degli switch.

Per esempio si possono definire 3 VLAN: una comprende i PC dei laboratori, una i PC dei docenti e una i PC della segreteria. Ovviamente sono possibili anche altre scelte. Per quanto concerne i 3 server si può supporre che debbano essere visibili a tutti i PC, per cui essi possono fare capo a uno switch che viene collegato a una porta configurata come **Trunk (VLAN ALL)** sullo switch principale. Una porta configurata come trunk viene considerata appartenente a tutte le VLAN, per cui i server sono raggiungibili da un qualunque PC della rete. Ovviamente l'effettiva accessibilità ai server va consentita solo agli utenti autorizzati, definendo in maniera opportuna i diritti di accesso (username, password). Sono possibili anche altre scelte².

Per consentire la condivisione in rete di applicazioni e risorse si adotta la suite di protocolli TCP/IP (Unità 9), implementata da un sistema operativo in grado di operare in rete (Windows XP, LINUX, ecc.). E' quindi necessario configurare opportunamente le risorse di rete (protocolli TCP/IP) su ogni macchina.

¹ In modo da avere porte disponibili nel caso si vogliano inserire un numero maggiore di computer.

² Soluzioni più complesse possono prevedere l'utilizzo di un router interno o di uno switch layer 3, in modo tale da suddividere la rete in un certo numero di subnet IP. Per semplicità ci si limita a considerare il caso in cui si impiegano solo switch layer 2.

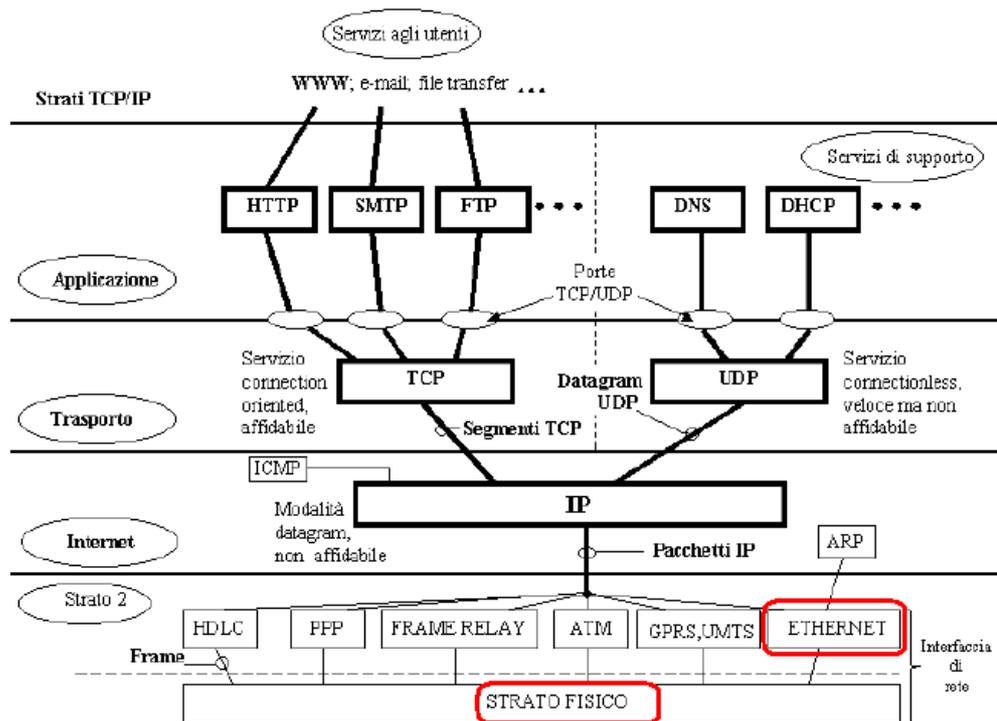
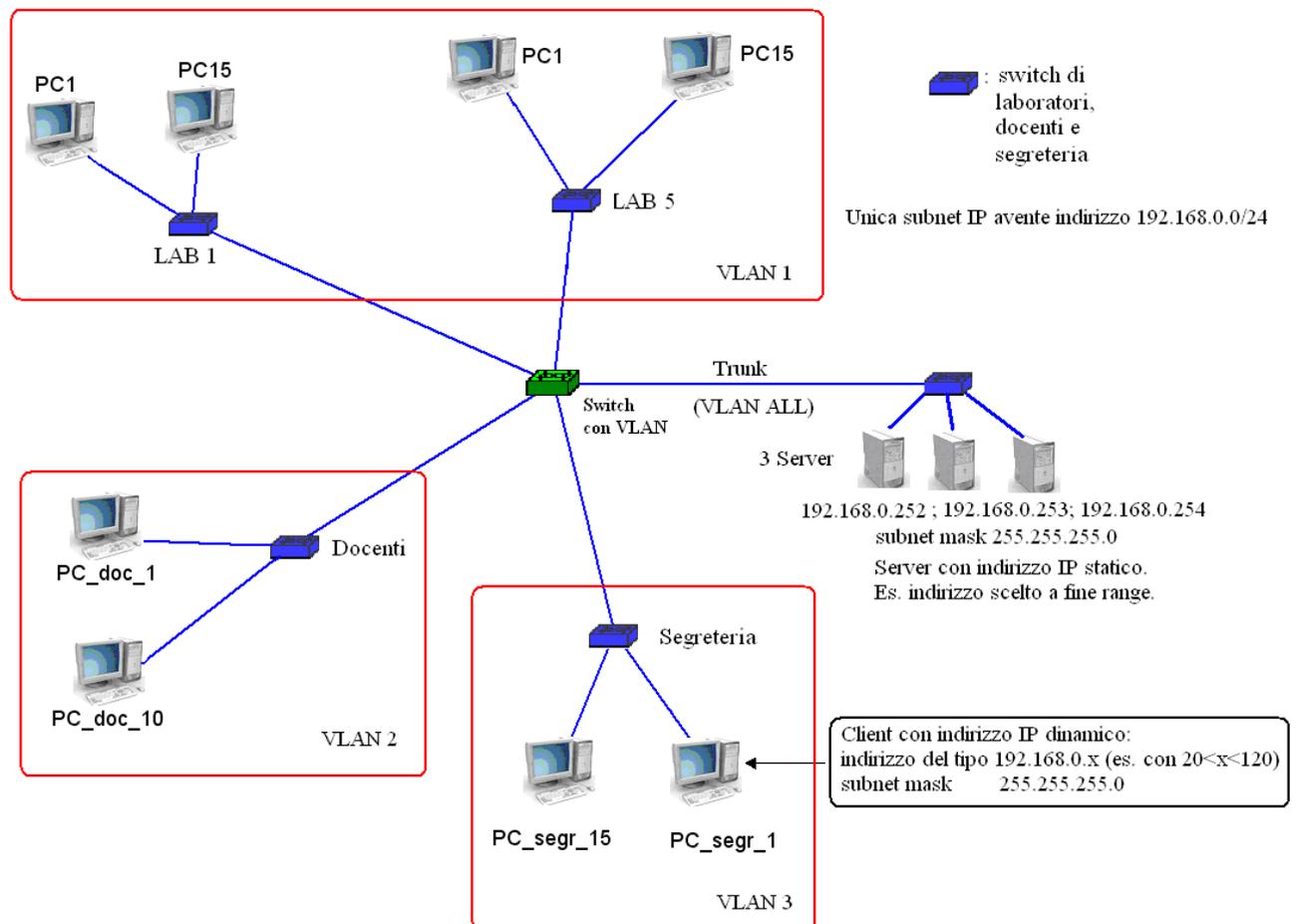


Fig. 9.5 Principali protocolli della suite TCP/IP

Lo schema della rete senza accesso a Internet è quindi il seguente:



2. La definizione del **piano di indirizzamento** consiste nella definizione dei parametri di configurazione dei protocolli TCP/IP da assegnare a ciascuna macchina (PC, switch, router) che deve essere vista in rete a livello IP (strato 3).

Per semplicità consideriamo il caso in cui non vi siano router interni, per cui è sufficiente definire un'unica subnet (rete) IP che comprende tutti i PC, i server e gli apparati di rete che necessitano di un indirizzo IP.

Per la rete di figura 1, che non ha ancora un accesso a Internet, è quindi necessario configurare su ogni computer **almeno un indirizzo IP e una subnet mask**.

Necessitano di un indirizzo IP e di una subnet mask anche gli switch amministrabili, in quanto essi vengono configurati da un PC collegato in rete per cui è necessario che essi abbiano un indirizzo IP per essere visti in rete.

Gli switch non amministrabili, invece, non necessitano di un indirizzo IP in quanto non sono configurabili.

Con le ipotesi fatte, la definizione del piano di indirizzamento IP può essere effettuata come qui di seguito indicato (per i dettagli si veda l'Unità 10 e l'esercitazione di laboratorio N. 6 sul testo).

Poiché tutti i PC appartengono a una stessa LAN (non sono presenti router interni) si sceglie un unico indirizzo IP di rete preso da uno dei tre blocchi di indirizzi IP privati a disposizione: 10.0.0.0/8; 172.16.0.0/12 e 192.168.0.0/16 (Unità 10, tab. 10.1).

Tab. 10.1 Blocchi di indirizzi IP privati

Blocco di indirizzi IP	Notazione decimale
10.0.0.0/8	da 10.0.0.0
	a 10.255.255.255
Subnet mask "/8"	255.0.0.0

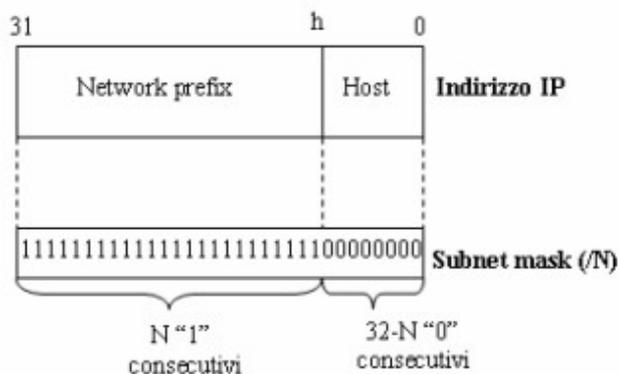
Blocco di indirizzi IP	Notazione decimale
172.16.0.0/12	da 172.16.0.0
	a 172.31.255.255
Subnet mask "/12"	255.240.0.0

Blocco di indirizzi IP	Notazione decimale
192.168.0.0/16	da 192.168.0.0
	a 192.168.255.255
Subnet mask "/16"	255.255.0.0

Scegliamo di utilizzare il blocco **192.168.0.0/24**. La subnet mask è costituita da 24 bit posti a "1" (/24) e da 8 bit posti a 0, per cui viene espressa in decimale come **255.255.255.0**.

Subnet mask "/24"

11111111	11111111	11111111	00000000	Notazione binaria
255	255	255	0	Notazione decimale



c)

Fig. 10.3 Metodi di identificazione del prefisso di rete (network prefix): c) classless.

Il prefisso di rete risulta così formato dai primi tre campi (24 bit) dell'indirizzo IP, mentre l'ultimo campo (8 bit) costituisce la parte host e consente di numerare fino a $2^8-2=254$ host; agli host non è possibile assegnare né il numero "0", che identifica la rete, né il 255 (tutti "1") che viene utilizzato come indirizzo IP di broadcast (pacchetto diretto a tutti gli host della subnet (rete) IP.

Come parte host del proprio indirizzo IP, a ciascuna interfaccia di PC, server, apparato visibile in rete va quindi assegnato un numero compreso tra 1 e 254, garantendone l'univocità.

	Notazione binaria			Notazione decimale		
Indirizzo IP di rete	11000000	10101000	00000000	00000000	192.168.0.0	/24
Ind. IP di broadcast	11000000	10101000	00000000	11111111	192.168.0.255	/24
Subnet mask "/24"	11111111	11111111	11111111	00000000	255.255.255.0	

Ind. IP host	
000001	192.168.0.1
.....
111110	192.168.0.254

Gli apparati di rete e i server necessitano di indirizzi IP statici, mentre i PC client sono di solito configurati in automatico tramite un server DHCP (Dynamic Host Configuration Protocol).

Per questo motivo molto spesso si assegnano gli indirizzi IP più bassi (per esempio 192.168.0.1, 192.168.0.2, ecc.) agli apparati di rete (router, switch amministrabili, ecc.), quelli più alti ai server (per esempio 192.168.0.252, 192.168.0.253, 192.168.0.254), mentre si definisce sul server DHCP un range intermedio di indirizzi IP (per esempio da 192.168.0.20 a 192.168.0.120) da assegnare ai PC client quando essi lo richiedono (all'accensione).

Avendo un'unica subnet IP, accanto all'indirizzo IP andrà configurata su tutte le macchine la seguente subnet mask: **255.255.255.0**, espressa come **/24** in notazione binaria concisa. Seguendo queste linee guida riserviamo la seguente configurazione IP al gateway della rete, cioè all'interfaccia ethernet (LAN) del router o del firewall tramite cui si accederà a Internet: **gateway 192.168.0.1**

Questo indirizzo IP costituirà il (futuro) gateway predefinito per tutti i PC della scuola, cioè l'indirizzo IP a cui vanno mandati i pacchetti che devono uscire dalla rete 192.168.0.0/24 per andare su Internet.

Allo switch amministrabile assegniamo l'indirizzo IP statico **192.168.0.2**

Ai tre server assegniamo rispettivamente gli indirizzi IP statici **192.168.0.252; 192.168.0.253; 192.168.0.254**

Avendo un elevato numero di PC è sconsigliabile l'assegnazione manuale degli indirizzi IP sui PC client.

Nel caso di configurazione automatica degli indirizzi IP nei PC client, selezionando la voce corrispondente nella configurazione delle risorse di rete, è necessario inserire in rete un **server DHCP**³ che distribuirà ai PC gli indirizzi IP, figura 2.

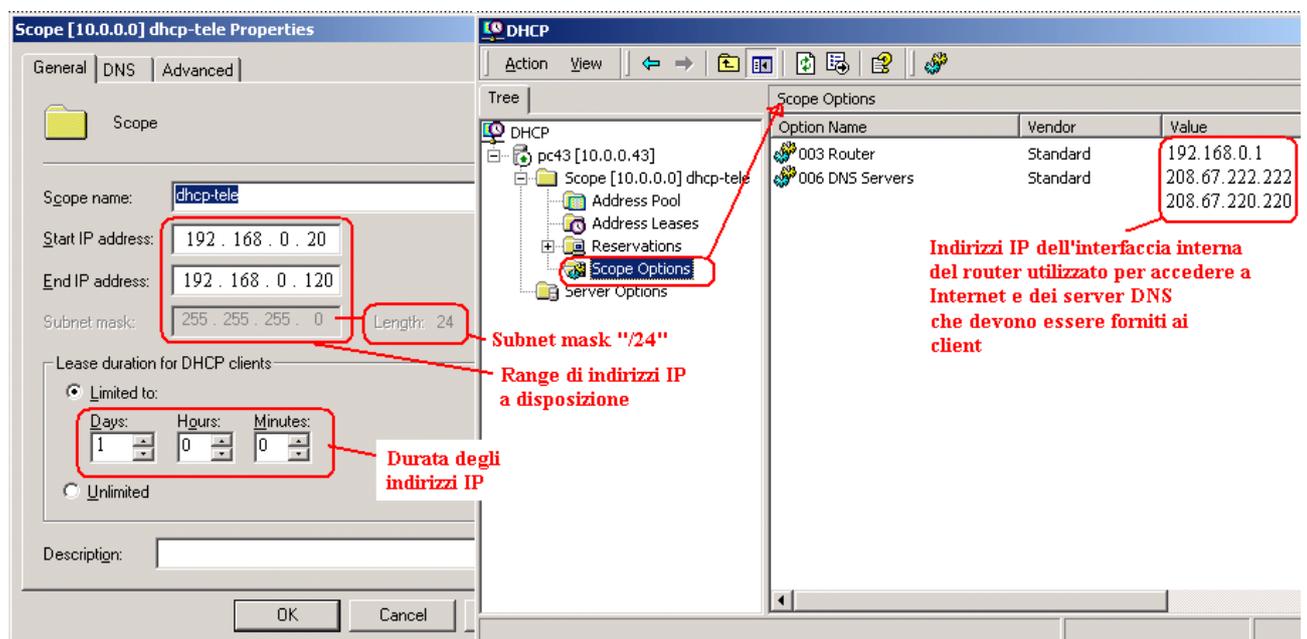
Si configura quindi il server DHCP in modo che assegni a ciascun PC client un indirizzo IP univoco compreso nel range

da **192.168.0.20 a 192.168.0.120**;
con subnet mask **255.255.255.0**

configuriamo anche gli indirizzi IP che il server DHCP deve fornire ai client per consentire loro la navigazione su Internet, una volta inserita la connessione a Internet stessa:

gateway predefinito 192.168.0.1 (uguale per tutti)

server DNS 208.67.222.222; 208.67.220.220 (uguale per tutti)



Esempio di configurazione di un server DHCP (sistema operativo Windows 2000 server) (Fig. 10.6 adattata)

Va poi notato che poiché vi è un elevato numero di computer in rete è necessario impiegare un computer con installato un sistema operativo di rete (per esempio Windows 2003 server). In questo modo si inserisce in rete un server che consente di implementare un dominio; tale server prende il nome di controllore di dominio e consente una gestione centralizzata degli utenti (username e password), dei permessi per l'accesso alle risorse di rete, ecc.. Il sistema operativo di rete comprende anche **un server DHCP e un server DNS (Domain Name System)**, in grado di effettuare la risoluzione dei nomi host configurati sulle macchine in indirizzi IP.

Se si volesse operare senza controllore di dominio sarebbe necessario configurare un elevato numero di gruppi di lavoro (workgroup), per esempio uno per ogni laboratorio, uno per i docenti e uno per la segreteria (Microsoft sconsiglia l'utilizzo dei workgroup se si hanno più di 10 PC in rete).

³ Il server DHCP va considerato come una applicazione software che può sia far parte di un sistema operativo di rete, come Windows 2003 server, sia essere caricata su un apparato di rete (router, firewall, ecc).

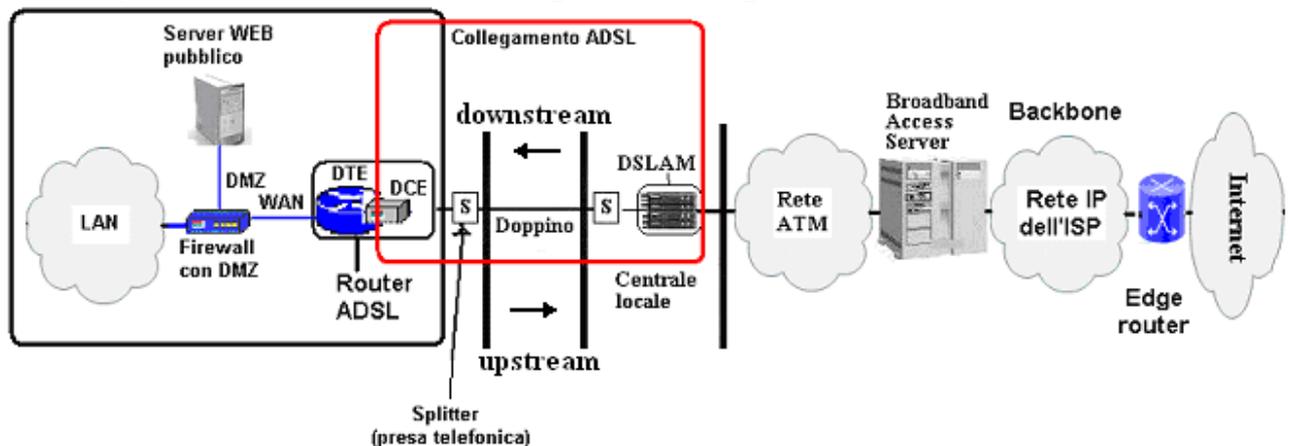
A questo punto i computer della LAN possono comunicare tra loro, ma non possono ancora accedere a Internet perché manca fisicamente l'accesso.

3. L'accesso a Internet ad alta velocità può essere realizzato inserendo nella LAN un router (si veda l'Unità 10 par. 10.7), il quale in generale accede tramite un **DCE** (Data Communication Equipment, Unità 13 par. 13.4) al canale trasmissivo che porta verso il router dell'Internet Service Provider (ISP), tramite cui si accedere effettivamente a Internet.

Per motivi di sicurezza il router è seguito da (o comprende se realizzato in modo software) un **firewall** (Unità 13 par. 13.3), che è un elemento in grado di proteggere la rete interna da attacchi provenienti da Internet.

- a) Facendo l'ipotesi che il traffico diretto verso il server web della scuola accessibile da Internet non sia molto elevato, si può orientare la scelta del tipo di accesso a Internet verso una **connessione ADSL** (meglio se ADSL 2+) avendo cura di definire nel contratto con l'ISP (Internet Service Provider) una velocità sufficientemente elevata sia in downstream (ricezione) sia in upstream (trasmissione), per esempio 8÷12 Mbit/s downstream, 1 Mbit/s upstream⁴.

Per una descrizione generale della struttura di un accesso ADSL si veda la figura 12.7 pag. 375, che permette di schematizzare il collegamento nel seguente modo:



L'inserimento del server WEB accessibile da Internet, noto anche come server HTTP dal nome del protocollo HTTP (Hyper Text Transfer Protocol) utilizzato per il trasferimento delle pagine HTML, comporta la necessità di utilizzare una struttura di rete in grado di proteggere adeguatamente la LAN interna.

Per quanto concerne le problematiche relative alla sicurezza, come illustrato nell'Unità 13 par. 13.3, è necessario impiegare un firewall che oltre alle porte ethernet LAN e WAN presenti anche una porta **DMZ (DeMilitarized Zone)**.

In questo modo il firewall consente a un client collegato a Internet di accedere solamente agli specifici servizi offerti dal server pubblico (server WEB ed FTP), inoltrando le relative richieste alla porta DMZ, mentre impedisce l'accesso dall'esterno alla LAN.

⁴ In alternativa si potrebbe anche richiedere un accesso a Internet di tipo simmetrico (stessa velocità in TX e RX) di sufficiente capacità, per esempio 2 Mbit/s, realizzabile attraverso una linea dedicata (CDN o HDSL o SHDSL), Unità 13 par. 13.2

Il principio di funzionamento del firewall si può così riassumere:

- direzione **LAN -> WAN** e **LAN -> DMZ**: le richieste di servizio provenienti dai client della LAN vengono inoltrate ai server esterni, su Internet attraverso la porta WAN o sulla DMZ se si deve raggiungere il server web della scuola;
- direzione **WAN -> DMZ**: le richieste di servizio provenienti da Internet vengono inoltrate solo se dirette al server pubblico posto sulla porta DMZ e solo per i servizi abilitati sul tale server;
- direzione **WAN -> LAN**: nessuna richiesta di servizio proveniente da Internet viene inoltrata sulla porta LAN, per cui su tale porta possono transitare **solo le risposte** alle richieste di servizio effettuate dai client della LAN stessa (per esempio le pagine web);

Come mostrato in figura, si effettuano le seguenti interconnessioni tramite cavi ethernet (UTP o FTP):

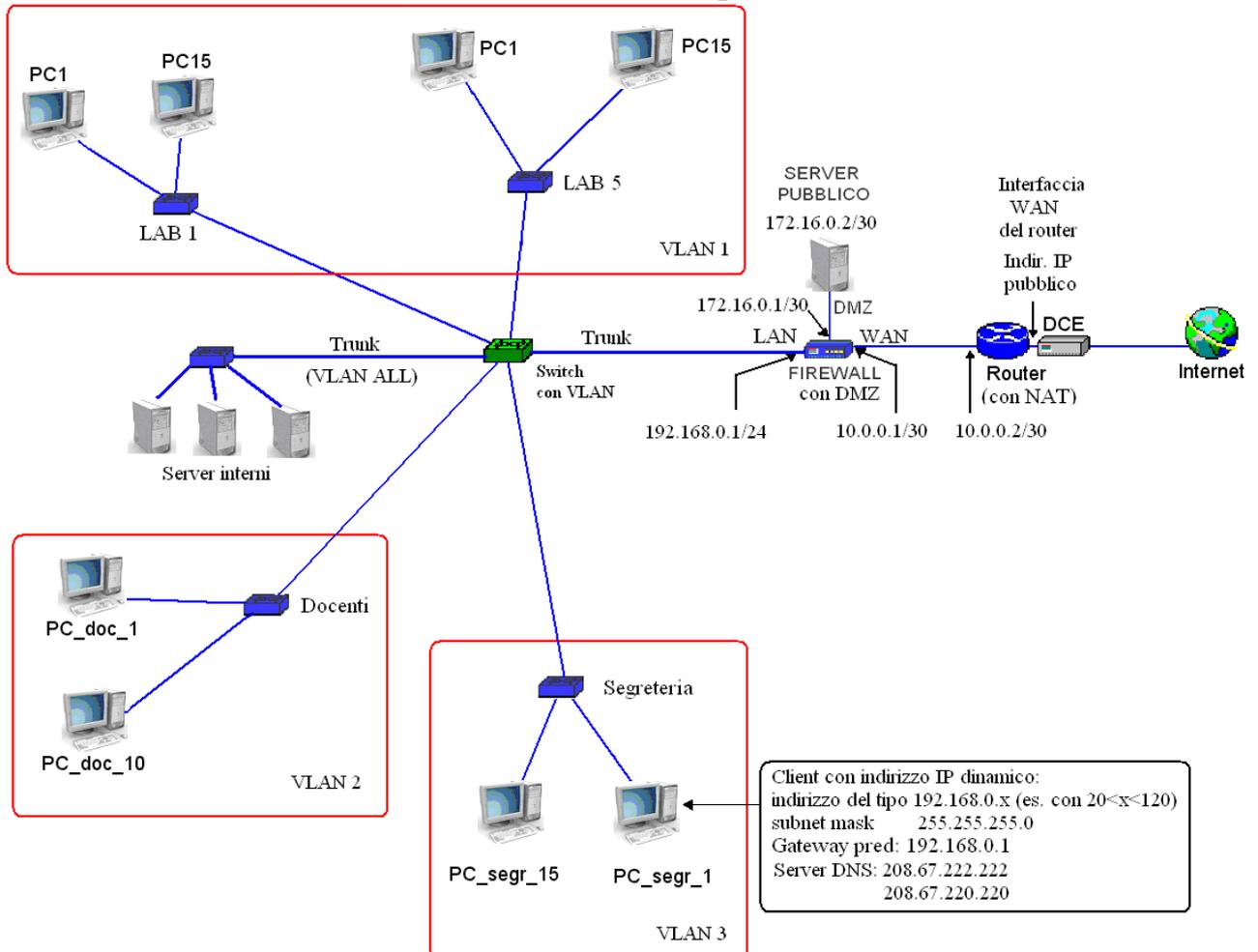
la **porta LAN** del firewall viene collegata a una porta dello switch principale configurata come **trunk**, in modo tale da renderla visibile a tutte le VLAN;

la **porta WAN** viene collegata al router tramite cui si accede a Internet;

la **porta DMZ** viene collegata al server che deve essere accessibile da Internet.

A livello di apparati è possibile utilizzare un firewall esterno, un router e un DCE (come in figura), oppure acquistare un router che abbia integrata la funzione di Firewall, realizzata in software, e abbia due porte Ethernet di cui una possa essere configurata come DMZ, oltre alla porta seriale da collegare al DCE.

Nel caso di router ADSL, infine, anche il DCE viene integrato nel router.



Rete con accesso a Internet e server ad accesso pubblico.

Per quanto concerne il piano di indirizzamento si ha che le porte LAN, DMZ e WAN devono appartenere a 3 subnet IP diverse, in modo da consentire il corretto instradamento dei pacchetti IP da parte del firewall.

Il piano di indirizzamento va completato per esempio nel seguente modo (sono ovviamente possibili scelte diverse):

- si assegna l'indirizzo IP **192.168.0.1/24** (cioè con subnet mask 255.255.255.0) all'interfaccia LAN del firewall, che costituisce il **gateway predefinito** (punto di uscita di default) per tutti i PC della LAN;
- si assegna l'indirizzo IP 172.16.0.1/30 (subnet mask 255.255.255.252) alla porta DMZ e l'indirizzo IP 172.16.0.2/30 al server pubblico; in questo modo sulla DMZ si configura una subnet che può avere solo due indirizzi IP, quelli che sono necessari per operare;
- si assegna l'indirizzo IP 10.0.0.1/30 all'interfaccia WAN del firewall e l'indirizzo IP 10.0.0.2/30 all'interfaccia ethernet (LAN) del router; anche qui si sceglie una subnet mask (/30 -> 255.255.255.252) che consente l'assegnazione di due soli indirizzi IP, quelli che servono;
- si assegna all'interfaccia WAN (seriale) del router l'indirizzo IP pubblico fornito dal provider; in questo caso l'indirizzo IP dovrebbe essere statico e noto in modo da rendere visibile su Internet il router e tramite esso anche il server WEB; se non vi fosse il server web pubblico il router può acquisire in automatico, da un server DHCP del provider, l'indirizzo IP pubblico;

Per consentire la navigazione su Internet dei PC della LAN è anche necessario abilitare nel router la funzione NAT (Network Address Translation, Unità 10 par. 10.5.3), che mappa gli indirizzi IP privati⁵ in uno o più indirizzi IP pubblici, assegnati (dietro richiesta se più di uno) dal Provider, quando i PC della LAN accedono a Internet.

Il router sostituisce così nei pacchetti in uscita verso Internet agli indirizzi IP privati un indirizzo IP pubblico ed esegue l'operazione inversa per i pacchetti ricevuti da Internet e diretti ai PC della LAN.

La presenza della DMZ complica ulteriormente la configurazione della rete e per semplicità viene solo accennata: è necessario configurare la funzione NAT in modo che anche l'indirizzo IP privato del server WEB venga convertito in un indirizzo IP pubblico visibile su Internet, è necessario aprire delle porte in ingresso al firewall per consentire l'accesso ai servizi offerti tramite il server collocato sulla DMZ, ecc.

b) Il mezzo trasmissivo utilizzato è il **doppino telefonico**⁶.

Nel caso di ADSL l'apparato tramite cui si accede al canale, o DCE, è costituito da un **modem ADSL** (Unità 13 par. 13.6) che può essere anche integrato nel router, formando così un router ADSL. Lo schema a blocchi di un modem ADSL è riportato in figura 13.12.

⁵ Si ricorda che gli indirizzi IP visibili su Internet sono denominati indirizzi IP pubblici e vengono assegnati da apposite organizzazioni (si veda il sito www.ripe.net) agli Internet Service Provider, i quali a loro volta li assegnano ai propri clienti. Tali indirizzi non possono perciò essere liberamente utilizzati da persone, enti o società private. Al contrario, i tre blocchi di indirizzi IP privati (10.0.0.0/8; 172.16.0.0/12 e 192.168.0.0/16) sono liberamente utilizzabili per le LAN, ma non sono utilizzabili per accedere a Internet.

⁶ E' necessario un solo doppino telefonico per i collegamenti ADSL (asimmetrico) e SHDSL (simmetrico), mentre sono richiesti due doppi telefonici (uno per trasmettere e uno per ricevere) nel caso di linea dedicata CDN o di collegamento HDSL. Infatti i DCE per CDN, così come i modem HDSL, operano con full duplex a 4 fili (Unità 6 par. 6.6.2) per cui richiedono due doppi telefonici, uno per la trasmissione e uno per la ricezione. Il router funge da DTE e va collegato al DCE per CDN tramite una porta seriale con di solito interfaccia V.35, ad alta velocità (Unità 13 par 13.7).

- c) I modem ADSL utilizzano una forma di **modulazione** denominata **DMT (Discrete Multitone)**, Unità 13 par. 13.6.1; essa è considerabile come una combinazione delle tecniche FDM (Frequency Division Multiplexing) e QAM/TCM (Quadrature Amplitude Modulation/Trellis Coded Modulation), Unità 8 par. 8.6 e 8.7. In sintesi, infatti, la modulazione DTM consiste nel suddividere la banda utile di canale (per esempio 1,1 MHz) in un numero elevato di sottobande da circa 4,3 kHz, realizzando così una sorta di FDM; su ciascuna sottobanda si modula una portante con la tecnica QAM/TCM.

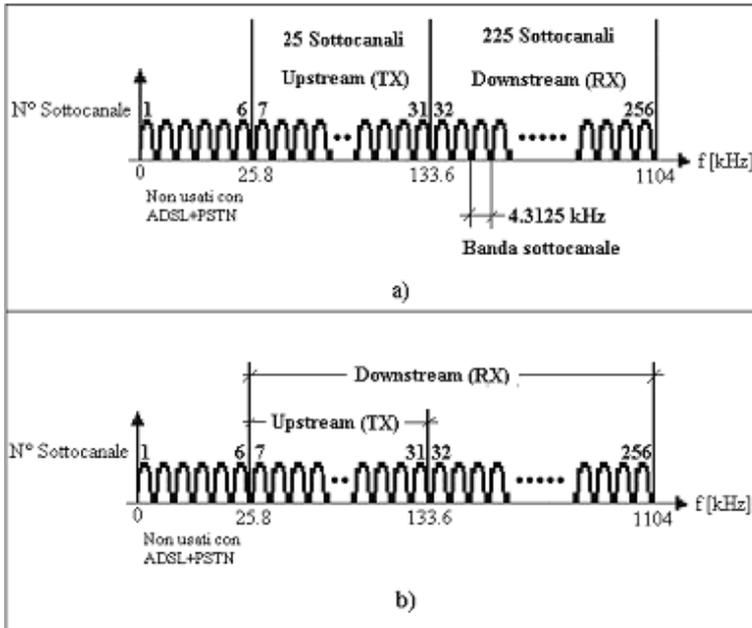


Fig. 13.10 a) e b)

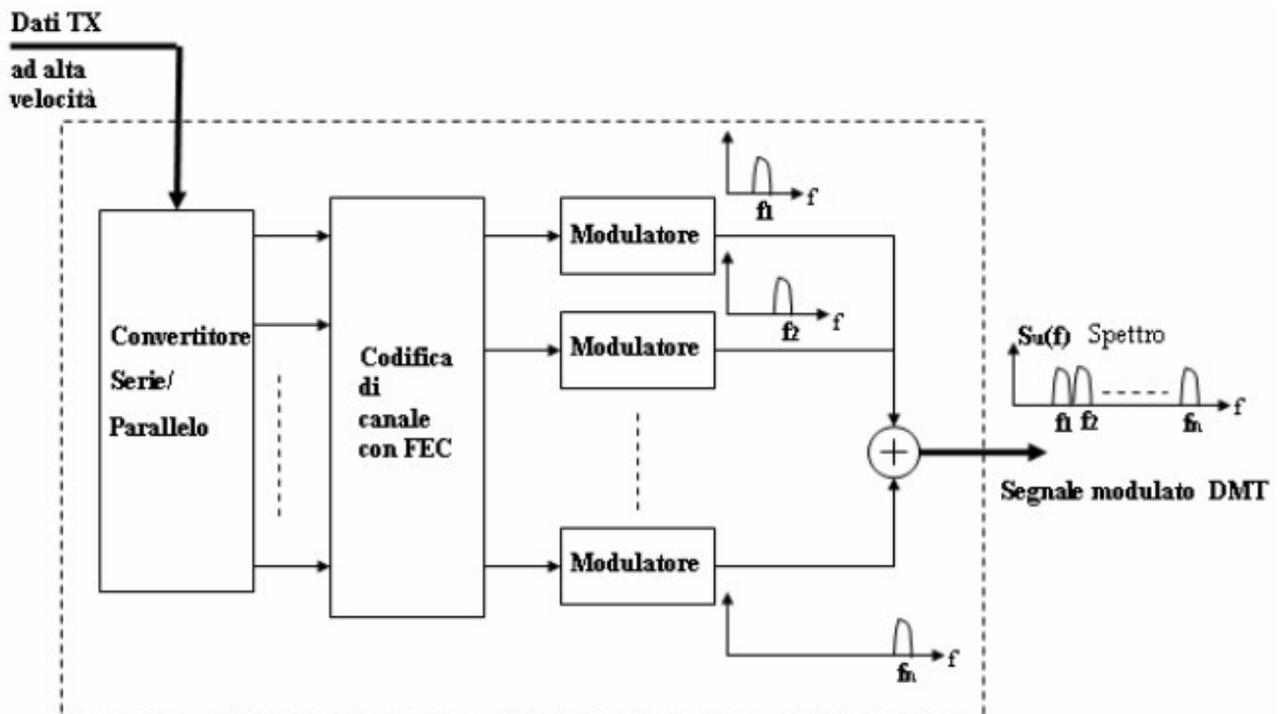


Fig. 13.11. Schema equivalente di un modulatore DMT.