MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA RICERCA

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE TELECOMUNICAZIONI
Tema di: SISTEMI E RETI E TELECOMUNICAZIONI
ESEMPIO PROVA 1

* Durata massima della prova: 6 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.

Il candidato (che potrà eventualmente avvalersi delle conoscenze e competenze maturate attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda) svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte. *

PRIMA PARTE

Si vuole realizzare una LAN in un edificio scolastico di tre piani che deve essere collegata a Internet tramite un ISP (fornitore di accesso Internet), con il quale è stato stipulato un contratto di tipo aziendale per la fornitura di una linea HDSL a 4 Mbit/s su doppino telefonico.

Il router HDSL è fornito dall'ISP in comodato d'uso (noleggio).

La LAN deve avere un proprio server Web che ospita il sito Internet scolastico e un server interno di posta elettronica.

Le postazioni client sono 120, disposte in modo non uniforme sui tre piani.

La LAN deve soddisfare i seguenti requisiti:

1) il server web su Internet deve essere pubblicato in maniera sicura e visibile a tutti;
2) i server web e di posta elettronica devono risiedere in una DMZ (essendo a rischio attacchi);
3) la LAN deve essere adeguatamente protetta da attacchi esterni;
4) deve essere previsto un access point per fornire la possibilità di accesso alla rete fissa tramite postazioni di lavoro wireless;
5) si vuole evitare quanto più possibile il problema dello Spam (posta indesiderata);
6) deve essere possibile bloccare la navigazione su alcuni siti Web non autorizzati;
7) si deve configurare un dominio Active Directory del tipo "nomescuola.it";
8) si deve creare un File Server con Backup di tutti i dati sia amministrativi che didattici.

Il candidato, formulate le opportune ipotesi aggiuntive, sviluppi i seguenti punti:

1) Proponga un progetto grafico dell'infrastruttura di rete, indicando le necessarie risorse hardware e software, esaminandone in particolare l'architettura, gli apparati e le caratteristiche dei collegamenti;
2) definisca un piano di indirizzamento IPv4 statico per l'infrastruttura di rete proposta al punto 1;
3) illustri le procedure di configurazione degli indirizzi IP statici (in Windows);
4) predisponga il Dominio Active Directory e DNS.

SECONDA PARTE

Il candidato scelga due fra i seguenti quesiti e per ciascun quesito scelto formuli una risposta.

1) Illustri il funzionamento e i principali vantaggi dell'implementazione di un servizio DHCP.
2) Proponga e descriva un possibile servizio di autenticazione per gli utenti della rete.
3) Una fibra multimodo di lunghezza $L = 4$ km presenta una banda modale per unità di lunghezza $B_{m0} = 1550$ MHz · km. Nel caso la fibra sia pilotata da un laser avente larghezza spettrale $\Delta_\lambda = 3$ nm che lavora in prima finestra con coefficiente di disper-

sione cromatica $\mu = -90$ ps/nm · km, determini la banda modale, la banda cromatica e la banda complessiva della fibra.

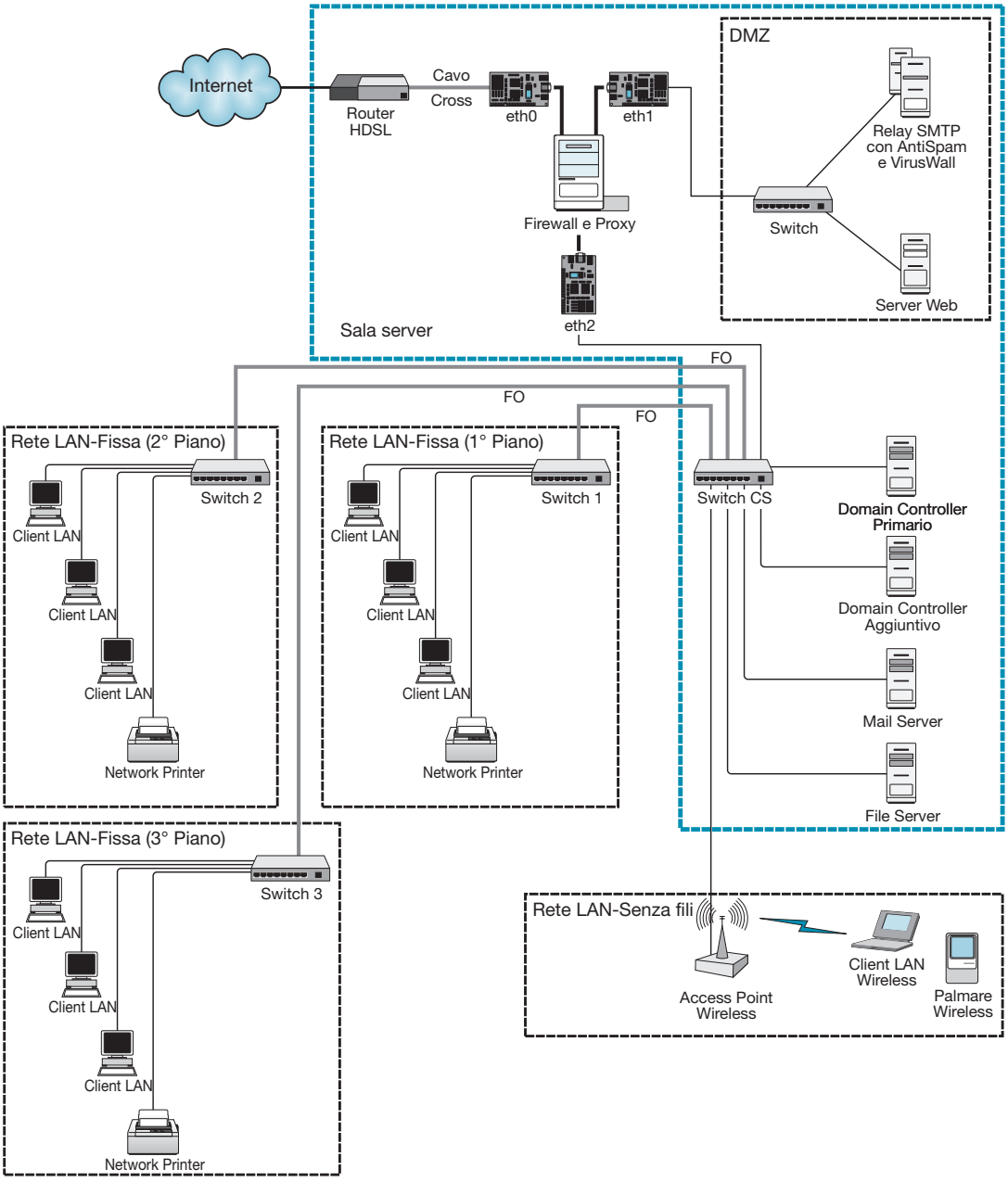
4) Una portante sinusoidale avente ampiezza $A_M = 0{,}2$ V è modulata con tecnica FSK incoerente da una sequenza modulante binaria. Sapendo che le frequenze di manipolazione sono $f_1 = 2100$ Hz e $f_2 = 1200$ Hz e che l'indice di modulazione è $m_f = 0{,}70$, determini la velocità di trasmissione dell'informazione e la potenza del segnale FSK riferita a un carico normalizzato (1 Ω).

SOLUZIONE PRIMA PARTE

Punto **1)** Il candidato proponga un progetto grafico dell'infrastruttura di rete, indicando le necessarie risorse hardware e software esaminandone, in particolare, l'architettura, gli apparati e le caratteristiche dei collegamenti.

La seguente figura mostra la struttura della LAN proposta, da analizzare approfonditamente in ogni sua parte.

Struttura della LAN da realizzare.

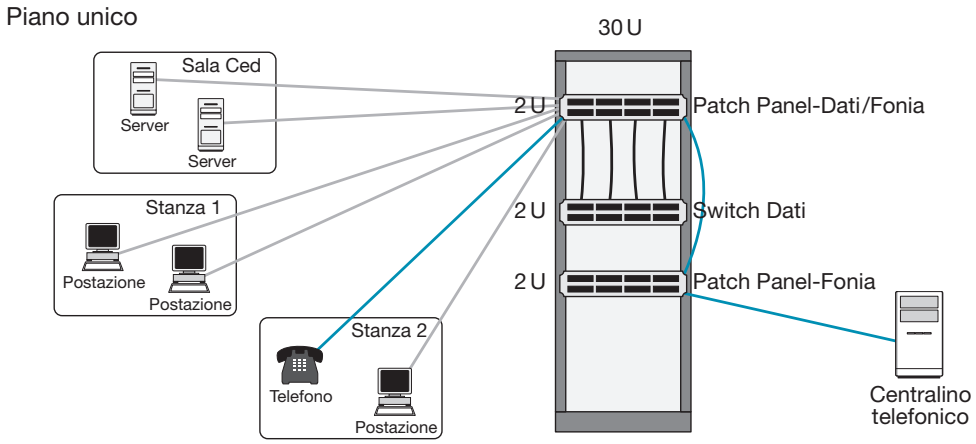


Realizzazione del cablaggio dell'edificio

Essendo l'edificio da cablare formato da tre piani, per ciascuno di essi occorre realizzare un cablaggio orizzontale.

Tutte le estremità dei cavi che partono dalle prese a muro devono essere convogliate in un armadio a rack, denominato **Centro Stella di piano**, come mostrato nella figura che segue.

Cablaggio orizzontale.



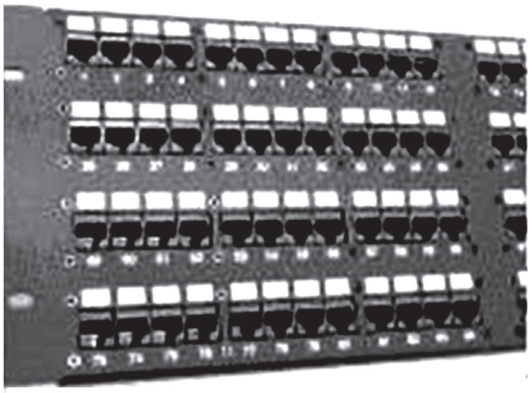
Cablaggio orizzontale

È importante sottolineare che ogni cavo ha limiti di lunghezza e pertanto, nel caso di superamento di tali limiti è necessario aggiungere dei ripetitori di segnale.

Ogni cavo proveniente da una presa a muro deve essere cablato sulla corrispondente terminazione RJ45 posta sul retro del **Patch Panel** (figura seguente), installato nell'armadio rack.

Sulla presa a muro e sul corrispondente attacco RJ45 del patch panel, viene posta un'etichetta con uno stesso numero, il quale consente di individuare univocamente il cavo interessato.

Patch panel.



Per collegare un PC al centro stella di piano, tramite una bretella di cavo viene connessa la relativa scheda di rete alla presa a muro più vicina, annotando il numero identificativo della presa stessa; sul patch panel, tramite un'altra bretella di cavo, la presa identificata dallo stesso numero è collegata allo switch di piano installato nel rack.

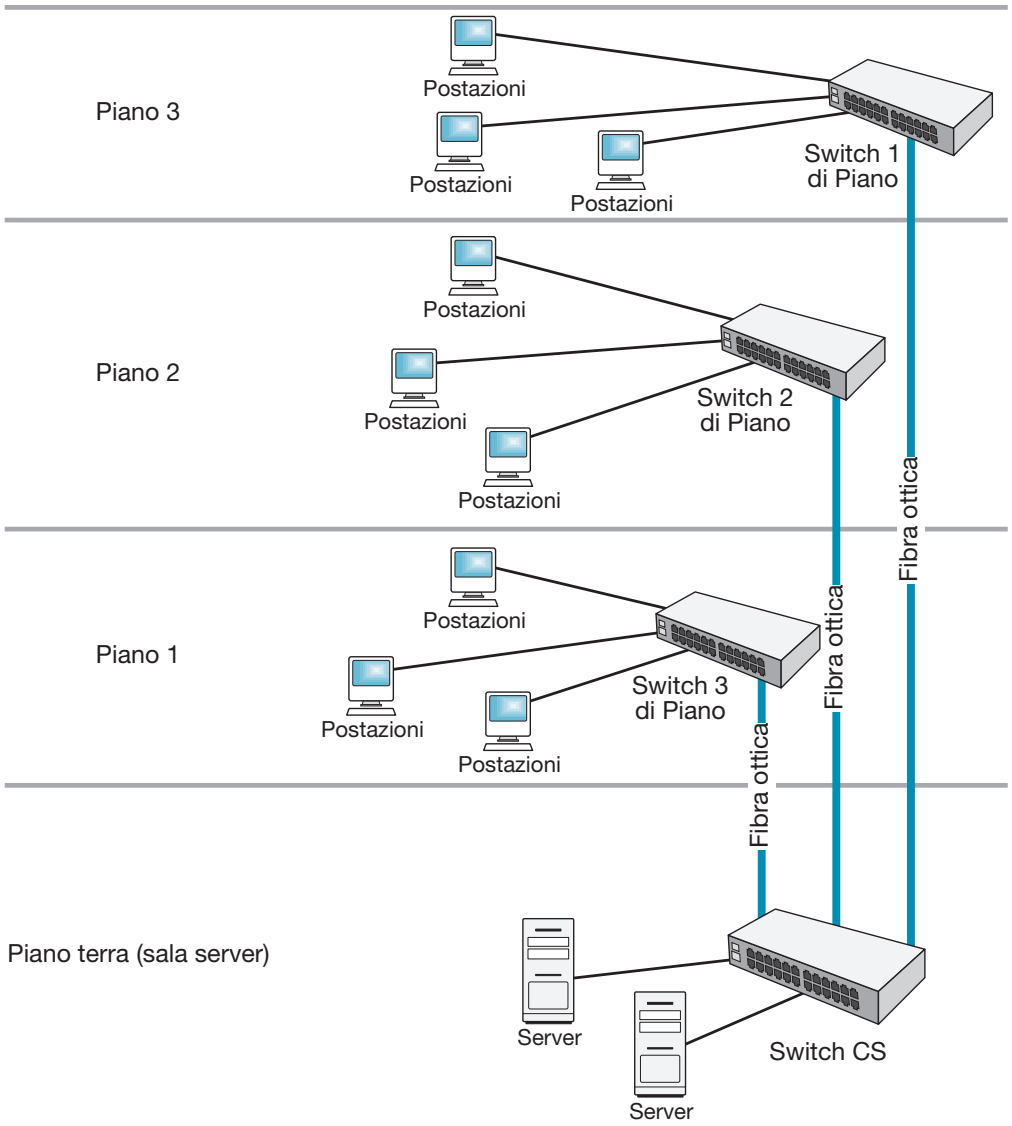
Questa tipologia di cablaggio, detto strutturato, consente di utilizzare automaticamente i cavi per trasportare indifferentemente dati e fonia.

Infatti, se al posto di un PC si vuole collegare un telefono, quest'ultimo può essere connesso alla presa a muro più vicina tramite una bretella telefonica a 4 fili (RJ11), annotandone il numero identificativo; tramite un'altra bretella telefonica viene colle-

gata la porta del patch panel identificata dallo stesso numero al centralino telefonico, anziché allo switch di piano.

Cablaggio verticale

Tramite tre dorsali (cablaggio verticale), ogni switch di piano viene collegato allo switch centrale (centro stella di edificio), ubicato a piano terra nella sala server, come indicato nella seguente figura.



Cablaggio verticale.

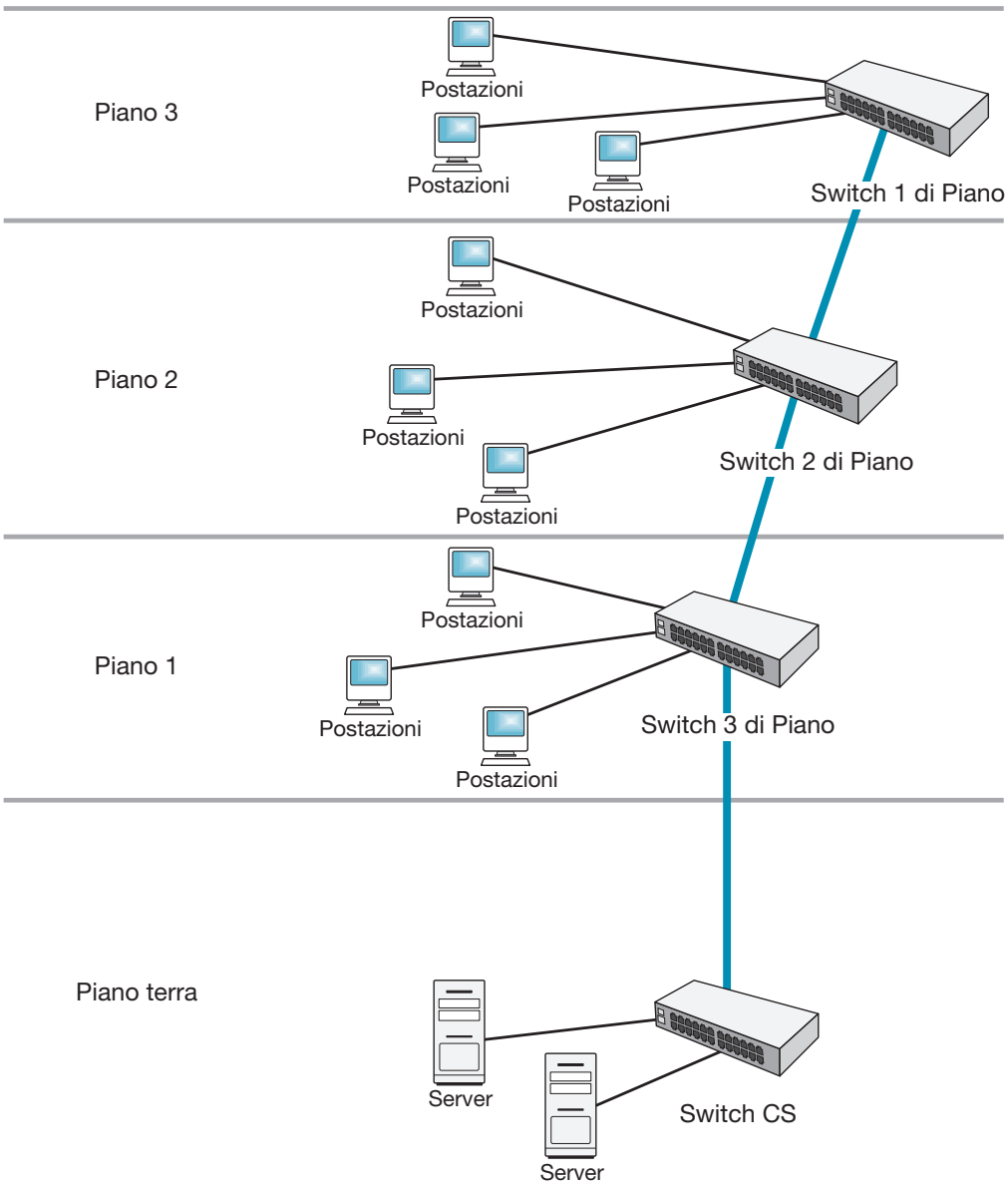
Le dorsali (evidenziate in blu) sono realizzate con cavi ottici monomodali, ciascuno dei quali formato da un numero di fibre tale da garantire tutti i collegamenti previsti dall'architettura di rete proposta, tenendo anche conto di possibili sviluppi futuri e delle eventuali fibre di scorta per ogni singola tratta posata.

Nella figura seguente è indicato un collegamento in cascata di più switch, fattibile ma sconsigliato, in quanto nel caso di guasto di uno di essi la comunicazione verrebbe interrotta.

La posa dei cavi e l'installazione delle prese a muro (o colonnine da pavimento) deve essere effettuata da elettricisti specializzati, i quali, tramite adeguati strumenti, possono "certificare" il corretto funzionamento di ogni tratto di rete (attenuazione, rumore, interferenze ecc.).

Tale certificazione, solitamente rilasciata all'utente in formato file TXT, ha lo scopo di formalizzare la corretta installazione del cablaggio effettuato e quindi rappresenta garanzia di qualità.

Cablaggio verticale sconsigliato.



Di seguito sono descritti in dettaglio i componenti sopra menzionati.

- *Distribuzione orizzontale*
  - cavi in rame;
  - postazioni di lavoro;
  - pannelli di permutazione;
  - bretelle in rame (patch cord).
- *Distribuzione di dorsale*
  - dorsale in fibra ottica;
  - pannelli di permutazione ottica;
  - bretelle ottiche monomodali.

Cavi in rame

I cavi in rame proposti, utilizzati per realizzare la connessione tra il pannello di permutazione e la postazione lavoro (cablaggio orizzontale), sono di tipo non schermato **UTP Cat. 6 Classe E**.

Sono formati da 4 coppie intrecciate con conduttori a filo solido temprati a sezione circolare 23 AWG divise da un setto separatore a croce, e hanno impedenza caratteristica 100 Ohm +/–3%.

Sono conformi alle normative EN50288-6-1 e ISO/IEC 61156-5.

Le guaine dei cavi sono di tipo LSZH/FR (HF1) e risultano adatte per installazioni all'interno degli edifici; supportano applicazioni a elevata velocità di trasferimento dei dati, in quanto assicurano una larghezza di banda fino a 250 MHz, in accordo con gli standard di riferimento.

Possiedono le caratteristiche di auto-estinguenza in caso d'incendio, di bassa emissione di fumi opachi e gas tossici corrosivi nel pieno rispetto delle normative vigenti (CEI 20-37, IEC 61034, NES 713, IEC 60754, EN 50265, EN 50267) e di ritardo di propagazione della fiamma (Flame Retardant) conformemente alle normative IEC 60332-1-2 (CEI 20-35, EN 50265).

Postazioni di lavoro

Ciascuna postazione di lavoro è collegata connettendo il cavo di distribuzione orizzontale alla presa; durante la fase di installazione deve essere rispettata la condizione che la distanza tra il pannello di permutazione all'interno dell'armadio a rack di piano e la presa della postazione di lavoro sia al massimo di 90 metri.

La presa è formata da tre elementi:

- scatola esterna di tipo ritardante la fiamma secondo UL 94V-0, UL listed;
- placca autoportante da 2 posizioni;
- prese modulari tipo U/UTP cat. 6.

Ciascuna presa è realizzata con un connettore a innesto rapido tool free conformemente alle normative internazionali recanti disposizioni in materia di prestazioni elettriche e meccaniche **ISO\IEC 11801 – 2nd Edition**, **EIA/TIA-568-B.2-1**, **EN 50173-1 2nd Edition** e testate in conformità alle **IEC 60603-7**.

Presa utente.

Patch panel

I patch panel (pannelli di permutazione) sono utilizzati negli armadi a rack per l'attestazione dei cavi in rame UTP che distribuiscono il cablaggio orizzontale.

Sono formati da un pannello dotato di una struttura metallica modulare a 24 fori che contiene prese modulari RJ45.

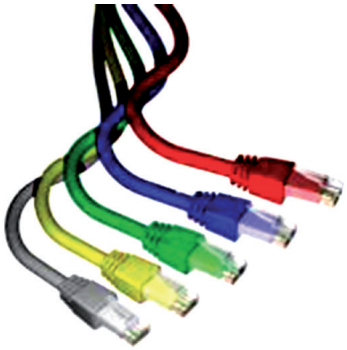
In genere hanno una struttura in acciaio satinato nero, con la parte frontale provvista di asole per montaggio su rack a 19", con 24 slot per prese RJ45 conformi alla normativa di riferimento **ISO\IEC 11801 – 2nd Edition**, **EIA/TIA 568-B.2-1** (per la Cat. 6), **EIA/TIA 568B.2-10** (per la cat. 6A) e testate in conformità alle **IEC 60603-7**.

Patch panel.

Bretelle in rame (patch cord e work area cable)

La connessione dei pannelli di permutazione agli apparati attivi e delle postazioni di lavoro alle relative prese, è effettuata mediante bretelle in rame, denominate **patch cord** o **work area cable**, realizzate con un cavo a 4 coppie U/UTP; sono disponibili in diverse lunghezze, tagli e colori e sono conformi alla norma ISO\IEC 61935-2; hanno una protezione anti-annodamento sul plug.

Bretelle in rame.



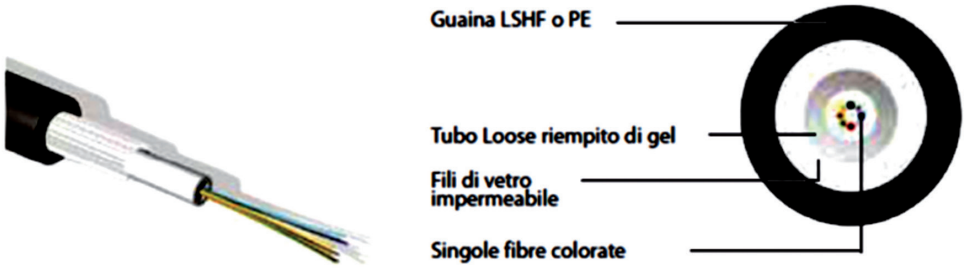
Cavi in fibra ottica

Al fine di aumentare le qualità tecnico-prestazionali della LAN, le dorsali sono realizzate con cavi in fibra ottica monomodale.

I cavi ottici proposti sono di tipo loose in configurazione unitubo, rinforzati da fibre di vetro conformi agli standard ISO/CENELEC o ITU-T G651 (MM) e ITU-T G652 (SM); hanno una guaina LSZH HF1 e una protezione antiroditore garantita da filati vetrosi. Sono disponibili con 4, 8 e 12 fibre e resistono alle prove di penetrazione dei fluidi previste dalle normative internazionali IEC 60794-1-2-F5.

Le temperature di esercizio del cavo sono comprese tra – 40 °C a + 70 °C.

Cavo in fibra ottica di tipo loose.



Pannelli di permutazione ottica

I cavi ottici di dorsale sono attestati su pannelli di permutazione ottica, che rappresentano il punto di interfaccia verso gli apparati attivi, sono idonei al montaggio su rack a 19”(483 mm).

Tali pannelli sono dotati di un vassoio porta bussole a scorrimento orizzontale, recrinabile a 45°, completo di fissaggi a sblocco rapido e a ingombro ridotto.

Il pannello è internamente provvisto di tutti gli accessori per la gestione delle fibre, ovvero di rotelle plastiche per la gestione del cavo, di pressacavi e di supporti per giunti a fusione (fusion spliceholder) in materiale plastico; è in grado alloggiare fino a 48 uscite fibra.

Pannello di permutazione ottica.

Bretelle ottiche monomodali

Ogni dorsale in fibra ottica viene permutata, attraverso il pannello di permutazione ottica, verso gli apparati attivi tramite bretelle ottiche.

Le bretelle ottiche proposte (fiber patch cord e fiber work area cable) sono tratti di cavo ottico in fibra monomodale (9/125), di lunghezza compresa tra 1 m e 10 m, attestati con connettori SC.

Bretella ottica monodale.

Sala server

Nella sala server sono installati, in uno o più rack, i server che gestiscono l'intera LAN, nonché l'apparato che interfaccia quest'ultima a Internet (router).

Occorre scegliere i rack più idonei in termini di spazio, compatibilità dei server ed espansibilità futura.

I parametri da tener presente nell'acquistare un rack sono i seguenti:

- profondità dei server da installare;
- larghezza dei server;
- "unità" disponibili.

Per i server è opportuno scegliere un rack da pavimento, per i patch panel di piano sono in genere sufficienti mini-rack a parete.

Gli armadi rack devono essere climatizzati, in quanto la temperatura deve essere compresa tra 10 °C e 28 °C: il valore ottimale è 19÷20 °C.

Occorre quindi dotare la sala server di un adeguato impianto di climatizzazione controllato da un software dedicato, che si avvale delle misurazioni effettuate dai diversi sensori di temperatura installati nella sala.

Nella sala server sono installati i seguenti server:

- il **Primary Domain Controller** (**PDC**), server che in una LAN Windows gestisce il dominio sul quale viene eseguita la Active Directory;
- il **Backup Domain Controller** (**BDC**), sistema di backup che conserva una copia a sola lettura del PDC, allo scopo di superare eventuali guasti di quest'ultimo;
- il **Mail server**, dove risiede il software che gestisce la ricezione e lo smistamento da un computer all'altro dei messaggi di posta elettronica;
- il **File server**, macchina progettata per mettere a disposizione degli utilizzatori della LAN un adeguato spazio su disco (singolo o composto da più dischi) nel quale sia possibile memorizzare, leggere, modificare, creare file e cartelle centralizzate, condivise da tutti oppure accessibili secondo regole o autorizzazioni generalmente assegnate dal gestore della rete. Tale macchina può essere un Network Attached Storage (NAS), cioè un apparecchio specificatamente studiato e costruito per tale scopo;
- il **Firewall**, che consente di filtrare ed eventualmente bloccare il traffico anomalo da e verso qualsiasi rete; il firewall agisce come una dogana che controlla il traffico proveniente dall'interno e dall'esterno di una rete, lasciando passare soltanto quello che rispetta regole definite; per motivi di sicurezza il firewall viene ospitato in un'apposita macchina dotata di tre schede di rete, eth0, eth1 e eth2 mediante le quali interfaccia rispettivamente il router, la DMZ e la LAN;
- il **router**, che collega la LAN a Internet, il quale è fornito dall'ISP in comodato d'uso (noleggio);
- la **DMZ** (DeMilitarized Zone, zona demilitarizzata), ovvero la zona isolata che ospita le applicazioni a disposizione del pubblico, utilizzata per consentire ai server in essa ospitati di fornire servizi all'esterno senza compromettere la sicurezza della rete aziendale interna: per le connessioni esterne la DMZ appare infatti una sorta di "**vicolo cieco**".
  La politica di sicurezza attuata sulla DMZ è la seguente:
  – traffico esterno verso la DMZ **autorizzato**;
  – traffico esterno verso la rete interna **vietato**;

– traffico della rete interna verso la DMZ **autorizzato**;
– traffico della rete interna verso l'esterno **autorizzato**;
– traffico della DMZ verso la rete interna **vietato**;
– traffico della DMZ verso la rete esterna **vietato**.

La DMZ contiene gli elementi di seguito indicati.

- Il **Web server**, macchina contenente un insieme di applicazioni software accessibile da parte dei client, che interpreta il linguaggio html (browser) utilizzando il protocollo di comunicazione HTTP.
- Il **relay SMTP**, server SMTP dove vengono utilizzati software di protezione per il traffico in/out (non solo email), ovvero:
  – Antispam (SpamAssassin, DSPAM);
  – Antivirus (ClamAV, OpenAntivirus).
- Uno **switch** a 8 porte al quale sono connessi il web server e il relay SMTP.

Materiale hardware attivo

Access Point

Le prestazioni dell'Access Point devono essere conformi agli standard IEEE 802.112. A seconda della richiesta, l'Access Point può essere alimentato sia autonomamente mediante adattatore di corrente, sia in modalità Power-over- Ethernet (PoE).

Viene proposto un Access Point TP-Link TL-WA901ND V5.0 Access Point Wireless, 450 Mbps, 3 Antenne Esterne, WPS, PoE.

Switch

Nella configurazione di rete proposta è necessario utilizzare cinque switch, dei quali uno a 8 porte (per la DMZ) e quattro a 48 porte: uno per ogni armadio di piano (switch1, switch2, switch3), uno per la sala server (switchCS).

Gli switch 1, 2 e 3 devono avere almeno due porte SPH in fibra ottica, lo switchCS almeno quattro porte SPH in fibra ottica.

Tutti gli switch devono inoltre presentare le seguenti caratteristiche:

- tecnologia Ethernet su cavi in rame: 1000BASE-T, 100BASE-T, 10BASE-T;
- standard di rete: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3x.

Punto **2)** Il candidato definisca un piano di indirizzamento IPv4 per l'infrastruttura di rete proposta al punto 1.

Per motivi di sicurezza è necessario suddividere la rete in tre sezioni, ciascuna delle quali indirizzata con un blocco di indirizzi di classe C (in totale occorrono quindi 3 blocchi di classe C).

La prima sezione è la rete interna, costituita dai 120 client più il PDC, il BDC, il mail server e il file server, indirizzabile, per esempio, con il blocco 192.168.3.0/24; la seconda sezione è costituita dalla DMZ, indirizzabile, per esempio, con il blocco 192.168.2.0/24; la terza sezione è costituita dal firewall e dal router, indirizzabile, per esempio, con il blocco 192.168.1.0/24.

Rete interna

Si può ipotizzare di riservare gli indirizzi compresi tra 192.168.3.1/24 e 192.168.3.229/24 ai client (più che sufficienti per indirizzare i 120 client e per gli eventuali sviluppi futuri) e gli indirizzi compresi tra 192.168.3.230/24 e 192.168.3.254/24 alle macchine installate nella sala server; così facendo si ottiene il piano di indirizzamento seguente:

- 192.168.3.1 all'interfaccia eth2 del firewall (quella verso la rete interna);
- 192.168.3.2/24 al PC1(primo piano);
- 192.168.3.3/24 al PC2(primo piano);

- 192.168.3.4/24 al PC3(primo piano);
- 192.168.3.5/24 al PC4(primo piano);
- 192.168.3.6/24 al PC5(primo piano);
- .....
- 192.168.3.46/24 al PC 45 (secondo piano);
- .....
- 192.168.3.121/24 al PC 120 (terzo piano);
- 192.168.3.122/24 all'access point;
- .....
- 192.168.3.230/24 al PDC;
- 192.168.3.231/24 al BDC;
- 192.168.3.232 al mail server;
- 192.168.3.233 al file server.

DMZ

- 192.168.2.1 alla scheda eth1 del firewall (quella verso la DMZ);
- 192.168.2.2 al web service;
- 192.168.2.3 al STMP relay.

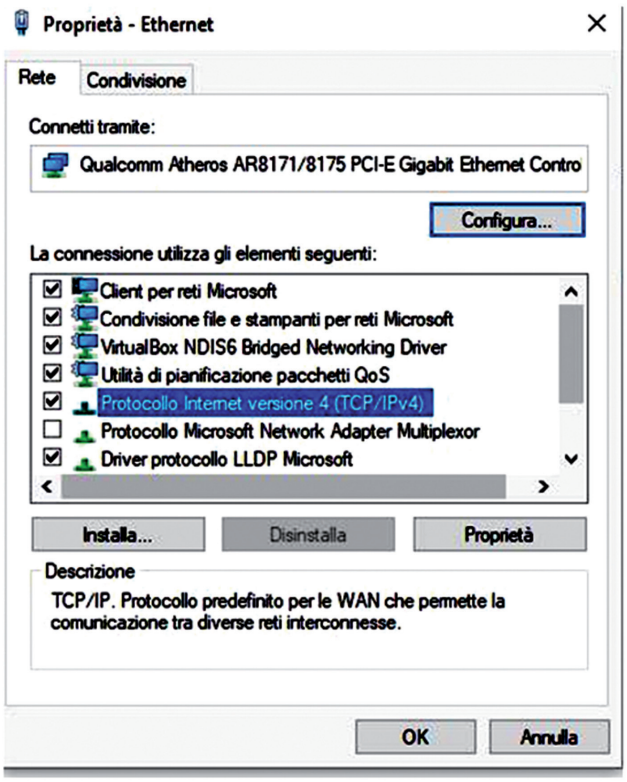
Firewall

- 192.168.1.1 alla scheda eth0 del firewall (quella verso il router);
- 192.168.1.254 all'interfaccia interna del router (quella, verso il firewall, che funge da gateway).

Punto **3)** Il candidato illustri le procedure di configurazione degli indirizzi IP statici (in Windows).

Considerando, per esempio, il client PC1, si seleziona "Pannello di controllo" → "Rete e Internet" → "Connessioni di rete".

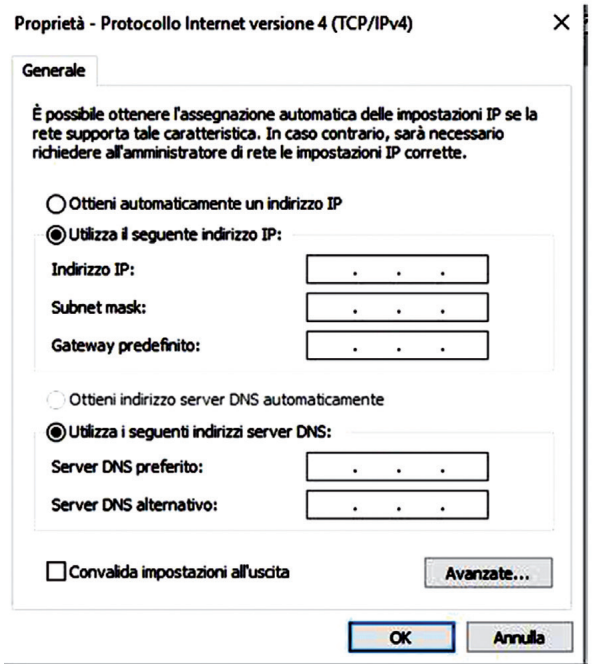
Cliccando con il tasto destro sull'icona che rappresenta la scheda di rete del PC e selezionando la voce "Proprietà", compare la finestra che segue.



Maschera Proprietà-Ethernet.

Si seleziona poi “Protocollo Internet versione 4 (TCP/IPv4)” e quindi “Proprietà” (figura seguente).

Configurazione degli indirizzi IP.



In tale finestra è specificata la configurazione della scheda di rete nella quale occorre impostare i seguenti valori (per il PC1).

- Indirizzo IP: 192.168.3;
- Subnetmask: 255.255.255.0;
- Gateway predefinito: 192.168.1.254.

Si può osservare che l’indirizzo del gateway coincide con quello del router: in questo modo tutti i pacchetti diretti a destinatari non appartenenti alla rete vengono inviati al router che provvede al loro instradamento.

Occorre infine configurare le impostazioni del DNS; al riguardo si utilizzano i seguenti indirizzi.

- Server DNS preferito: 192.168.3.230/24 (PDC); essendo i client in un dominio, come DNS preferito viene utilizzato il PDC. In questo modo i client si collegano al PDC, il quale, in base alle policy impostate, risolve i DNS dei client consentendo loro di navigare.
- Server DNS alternativo: 192.168.3.231/24; il DNS alternativo è facoltativo ma è consigliabile impostarlo con la stessa configurazione del BDC.

Per completare la configurazione della LAN si procede allo stesso modo per tutti gli altri PC e i server.

Punto **4)** Il candidato predisponga il Dominio Active Directory e DNS.

Il primo passo è la preparazione del Primary Domain Controller (PDC) e poi di Active Directory: si assegni al server PDC il nome **DC1**.

Dopo aver installato Windows 2016 Server da **Server Manager**, selezionando l’opzione “Aggiungi ruoli e funzionalità” si esegue la procedura guidata tramite la quale si configura il PDC.

I parametri essenziali che devono essere configurati in questo passaggio sono: il nome del dominio (per esempio nomescuola.it) e i percorsi dove verranno archiviati i file di database di AD.

A questo punto si configura il servizio DNS Server sullo stesso server, creando così una nuova zona primaria (diretta) integrata in AD, con nome per esempio "azienda-scuola.it" e successivamente una zona di ricerca inversa con gli IP della rete.

La zona diretta consente ai client di risolvere i nomi degli host nell'indirizzo IP corrispondente; la zona inversa, dato un IP, restituisce il corrispondente nome host.

Creazione degli utenti

A questo punto occorre definire uno standard per la creazione dei login e una politica delle password rigida.

I login (o username) possono essere creati anteponendo l'iniziale del nome al cognome per esteso dell'utente (per esempio, il login di Mario Rossi è mrossi) e la password definita da almeno 8 caratteri tra numeri e lettere.

Per creare un utente si apre "Utenti e Computer di Active Directory" nel menu "Strumenti di Amministrazione" sul server PDC (DC1).

Si inserisce poi una password provvisoria (per esempio mariorossi12345) e si clicca sulla voce "L'utente deve cambiare password al prossimo login": così facendo il signor Mario Rossi, quando entra per la prima volta nel suo PC come mrossi con password mariorossi12345, può modificarla.

Aggiunta (Join) dei client al dominio

Un dominio Windows è un contesto di sicurezza dove "girano" i client (e i server). Tutti gli host che appartengono a un dominio possono essere controllati centralmente attraverso le impostazioni gestite sul domain controller: Group Policy, gruppi di utenti, permessi NTFS.

Dal PDC è possibile impostare qualsiasi limite o configurazione sui client che ne fanno parte (che quindi hanno fatto "Joint al Dominio"); per Join si intende l'operazione di inserimento di un client al dominio (in tal caso nomescuola.it).

Per effettuare questa operazione occorre entrare come "Administrator Locale" sul PDC e cliccare con il tasto destro su"Risorse del Computer → Nome Computer e cambiare la configurazione da "Gruppo di lavoro" a "Dominio", specificandone il nome (nomescuola.it).

A questo punto si inserisce il login e la password dell'amministratore del dominio (l'utente Administrator creato sul server PDC) che ha il permesso di aggiungere i client nel dominio.

Si riavvia quindi il client e si entra in rete con il nome dell'utente e la sua password, selezionando dalla lista dei domini quello prescelto (nomescuola.it).

Con questa procedura possono essere inseriti tutti i client nel dominio.

Al termine dell'operazione è possibile configurare sul server PDC eventuali impostazioni di restrizione e applicarle a tutti i computer che fanno parte del dominio, senza agire sul singolo client.

SOLUZIONE SECONDA PARTE

Punto **1)** Il candidato illustri il funzionamento e i principali vantaggi dell'implementazione di un servizio DHCP.

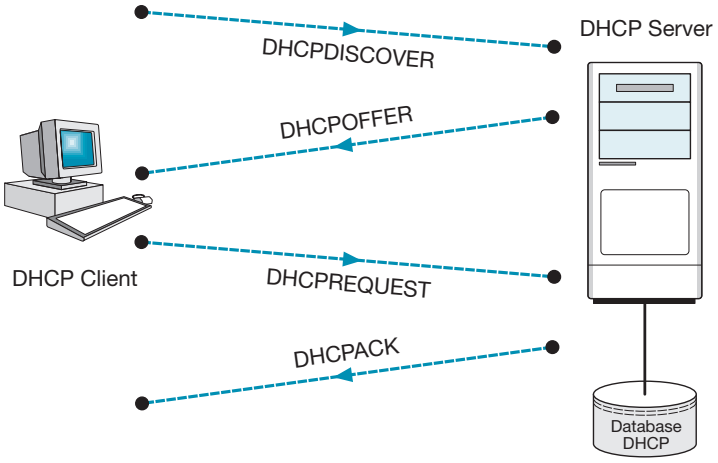
Il DHCP (acronimo di Dynamic Host Configuration Protocol), definito dai documenti RFC 2131 e 2132, è un protocollo che consente l'assegnazione automatica degli indirizzi IP. È basato sul modello client-server: un client, inizialmente non configurato, invia ai server DHCP presenti in rete un messaggio in broadcast (contenente il proprio MAC ADDRESS), denominato **DHCPDISCOVER**, mediante il quale richiede un indirizzo IP valido.

I server rispondono inviando un messaggio, denominato **DHCPOFFER**, nel quale propongono un indirizzo IP al client.

Allo scopo di ricevere le offerte da tutti i server DHCP presenti in rete, il client aspetta un certo tempo, terminato il quale ne seleziona una inviando un messaggio di

DHCPREQUEST al server che ha scelto; quest'ultimo conferma l'assegnazione con un messaggio di acknowledgement denominato **DHCPACK**.

Sequenza di messaggi DHCP per l'acquisizione di un indirizzo IP da parte di un client.



Per default tutti gli host (indipendentemente dal sistema operativo di rete utilizzato) possono agire come client DHCP, ma nel caso di configurazione di un host come server DHCP, è necessaria l'installazione manuale del relativo software da parte dell'amministratore. Tramite DHCP è inoltre possibile assegnare, oltre all'indirizzo IP, anche gli altri parametri addizionali (DHCP Options) necessari al completamento della configurazione dello stack TCP/IP, come per esempio il Dominio DNS, l'WINS Server, il gateway di default, in funzione delle necessità e del contesto operativo.

Punto **2)** Il candidato proponga e descriva un possibile servizio di autenticazione per gli utenti della rete.

Kerberos è un protocollo di autenticazione distribuito che consente a un utente di provare la sua identità. Il nome Kerberos deriva dal personaggio mitologico Cerbero, il cane a tre teste che sorveglia le porte dell'Ade; la scelta di questo nome esprime la presenza di tre importanti obiettivi di seguito indicati.

- **Autorizzazione**, riferita alla capacità del sistema di determinare se un soggetto è autorizzato a eseguire una certa operazione.
- **Autenticazione**, riferita alla capacità del sistema di determinare se un soggetto è veramente chi dichiara di essere.
- **Cifratura**, riferita alla capacità del sistema di prevenire un'intrusione per ascoltare i contenuti delle comunicazioni e di apportare modifiche.

Kerberos è basato su un'architettura client-server in cui le informazioni scambiate tra client e server sono cifrate: affinché questa modalità sia possibile, il client deve condividere una chiave crittografica segreta con il server con il quale scambia informazioni.

Gli algoritmi di cifratura sono simmetrici e pertanto la chiave della cifratura e quella della decifratura sono identiche.

L'assegnazione delle chiavi segrete alle due entità coinvolte nella transazione (client e server) è garantita dall'Authentication Server (AS), nel quale sono conservate le chiavi degli utenti e dei server che esso gestisce.

Punto **3)** Una fibra multimodo di lunghezza $L = 4$ km presenta una banda modale per unità di lunghezza $B_{m0} = 1550$ MHz · km.
Nel caso la fibra sia pilotata da un laser avente larghezza spettrale $\Delta_\lambda = 3$ nm che lavora in prima finestra con coefficiente di dispersione cromatica $\mu = -90$ ps/nm · km, il candidato determini la banda modale, la banda cromatica e la banda complessiva della fibra.

Considerando un parametro di mescolamento dei modi $\gamma = 0{,}85$, la banda modale risulta:

$$B_m = \frac{B_{m0}}{L^{\gamma}} = \frac{1550}{4^{0{,}85}} = 477 \text{ MHz}$$

La banda cromatica vale:

$$B_c = \frac{0{,}44 \cdot 10^6}{\mu \cdot \Delta\lambda \cdot L} = \frac{0{,}44 \cdot 10^6}{90 \cdot 3 \cdot 4} = 407{,}4 \text{ MHz}$$

La banda complessiva risulta:

$$B = \frac{1}{\sqrt{\frac{1}{B_m^2} + \frac{1}{B_c^2}}} = \frac{1}{\sqrt{\frac{1}{477^2} + \frac{1}{407{,}4^2}}} = 309{,}78 \text{ MHz}$$

Punto **4)** Una portante sinusoidale avente ampiezza $A_M = 0{,}2$ V è modulata con tecnica FSK incoerente da una sequenza modulante binaria. Sapendo che le frequenze di manipolazione sono $f_1 = 2100$ Hz e $f_2 = 1200$ Hz e che l'indice di modulazione è $m_f = 0{,}70$, il candidato determini la velocità di trasmissione dell'informazione e la potenza del segnale FSK riferita a un carico normalizzato (1 Ω).

Poiché l'indice di modulazione è:

$$m_f = \frac{f_1 - f_2}{V_f} = \frac{2\Delta f}{V_m}$$

Si può ricavare la velocità di modulazione V_m:

$$V_m = \frac{f_1 - f_2}{m_f} = \frac{2100 - 1200}{0{,}7} = 1285{,}7 \text{ baud}$$

Essendo la sequenza modulante binaria, la velocità di trasmissione coincide con quella di modulazione e quindi $V_T = V_m = 1285{,}7$ bit/s.

Poiché l'ampiezza della portante non varia dopo la modulazione, la potenza del segnale FSK su un carico normalizzato pari a 1 Ω vale:

$$S = \frac{A_M^2}{2} = \frac{0{,}2^2}{2} = 20 \text{ mW}$$

MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA RICERCA

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE TELECOMUNICAZIONI
Tema di: SISTEMI E RETI E TELECOMUNICAZIONI
ESEMPIO PROVA 2

* Durata massima della prova: 6 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.

Il candidato (che può avvalersi delle conoscenze e competenze maturate anche attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda) svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte. *

PRIMA PARTE

Un'azienda, che dispone di una LAN con 120 host, deve aprire una succursale ubicata a 4 km di distanza dalla prima, nella quale vuole realizzare una LAN comprendente 55 host.

Le due reti, che sono in visibilità ottica, devono comunicare tra loro in modo sicuro attraverso un collegamento in fibra ottica realizzato con due tronchi di fibra aventi le seguenti caratteristiche:

primo tronco

- indice di rifrazione del core $n_x = 1{,}3$;
- apertura numerica $NA_x = 0{,}20$;
- diametro del core $d_x = 50$ μm;
- lunghezza del tronco $l_x = 2{,}5$ km;
- attenuazione per unità di lunghezza 0,35 dB/km.

secondo tronco

- indice di rifrazione del core $n_y = 1{,}2$;
- apertura numerica $NA_y = 0{,}19$;
- diametro del core $d_y = 47$ μm;
- lunghezza del tronco $l_y = 1{,}5$ km;
- attenuazione per unità di lunghezza 0,40 dB/km.

Il collegamento è caratterizzato dai seguenti parametri:

- banda totale del collegamento $B_T = 66$ MHz;
- frequenza di cifra $f_C = 68{,}7$ MHz;
- potenza massima del trasmettitore $P_{TX\text{MAX}} = 1$ dBm;
- potenza minima del trasmettitore $P_{TX\text{MIN}} = -2$ dBm;
- potenza massima del ricevitore $P_{RX\text{MAX}} = -25{,}6$ dBm;
- potenza minima del ricevitore $P_{RX\text{MIN}} = -32$ dBm.

Nell'ipotesi di disporre del blocco di indirizzi IP 192.168.20.0, il candidato, formulate le opportune ipotesi aggiuntive, sviluppi i seguenti punti:

1) dopo aver disegnato un possibile schema a blocchi del sistema, definisca il piano di indirizzamento IPv4 per l'intera infrastruttura di rete;
2) determini l'attenuazione complessiva del collegamento in fibra ottica;
3) determini i margini inferiore e superiore del collegamento tenendo anche conto della penalità di banda η così definita:

$$\eta = 1{,}5\left(\frac{f_C}{B_T}\right)^2$$

4) verifichi se il collegamento soddisfa i requisiti di progettazione e consideri l'eventuale introduzione di adeguati attenuatori;

5) individui una Access Control List per impedire il traffico FTP dalla LAN della succursale verso la LAN della sede centrale;
6) evidenzi eventuali punti di debolezza del sistema e proponga, con opportune motivazioni, interventi aggiuntivi per ridurre la vulnerabilità ai guasti.

SECONDA PARTE

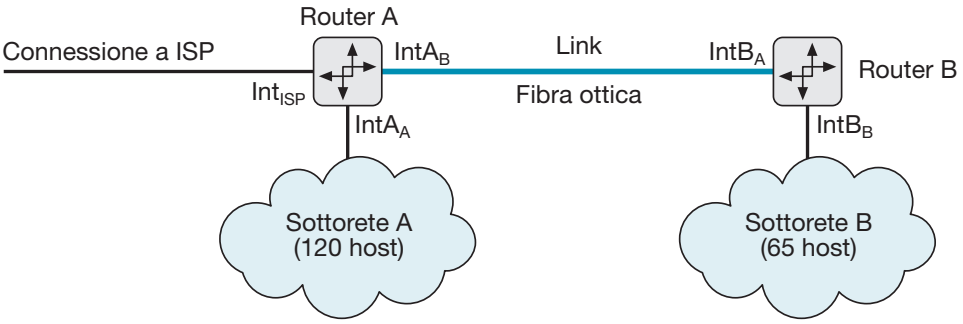
Il candidato scelga due fra i seguenti quesiti e per ogni scelta formuli una risposta:

1) illustri le differenze tra trasmissione analogica e numerica, evidenziando i vantaggi della seconda rispetto alla prima;
2) descriva il funzionamento del DNS e la divisione logica dell'insieme di tutti gli indirizzi simbolici di Internet;
3) due stazioni radio sono distanti tra loro 20 km. La stazione trasmittente, dotata di un'antenna a paraboloide avente diametro $d_T = 2$ m ed efficienza superficiale ha $\eta_{aT} = 0{,}73$, è collegata al trasmettitore tramite una guida d'onda di lunghezza pari a 25 m, avente un'attenuazione di 0,15 dB/m.
La stazione ricevente, dotata di un'antenna a paraboloide di diametro $d_R = 1{,}5$ m ed efficienza superficiale ha $\eta_{aT} = 0{,}71$, è collegata al ricevitore tramite un tratto di guida d'onda avente lunghezza pari a 15 m e attenuazione di 0, 12 dB/m. Nel caso la potenza in trasmissione sia $P_T = 1$ kW e la frequenza di lavoro $f = 3$ GHz, determini la potenza in ricezione.
4) Illustri le caratteristiche peculiari dei modelli di reti distribuiti Windows.

SOLUZIONE PRIMA PARTE

Punto **1)** Il candidato, dopo aver disegnato un possibile schema a blocchi del sistema, definisca un piano di indirizzamento IPv4 per l'intera infrastruttura di rete.

L'infrastruttura di rete proposta in base a quanto contenuto nel testo è la seguente:



Infrastruttura di rete proposta.

Il sistema è formato da tre sottoreti: la sottorete della sede centrale (A) con 120 host, la sottorete della succursale (B) con 65 host, e il link che collega i router A e B, il quale deve essere considerato a tutti gli effetti una sottorete.

È importare ricordare che è necessario assegnare un indirizzo IP a ciascuna interfaccia di ogni router: alle interfacce verso le sottoreti può essere assegnato un indirizzo della sottorete alla quale esso è interfacciato (per esempio l'ultimo indirizzo utile), alle interfacce verso il link uno degli indirizzi disponibili della relativa sottorete.

Con riferimento alla figura precedente, essendo il numero totale degli host della rete 120 + 55 = 175, è sufficiente utilizzare il solo blocco di indirizzi C assegnato per indirizzare gli host (si ricordi che un blocco C comprende 254 indirizzi IP).

Al riguardo conviene adottare la modalità di subnetting VLSM/CIDR, che consente di assegnare alle sottoreti netmask di lunghezza variabile costituite da un numero di bit tale da evitare indirizzi non utilizzati.

Occorre innanzitutto determinare il numero di bit necessari a indirizzare gli host della sottorete più grande (A).

Per indirizzare 120 host e l'interfaccia verso il router sono necessari 7 zeri nell'ultimo ottetto della netmask (il numero dei terminali per ciascuna sottorete si ottiene elevando la cifra 2 al numero di 0 presenti nella netmask diminuito di due unità); per la rete A la netmask risulta pertanto:

$$11111111.1111111.11111111.10000000 \rightarrow 255.255.255.128$$

Si ha infatti: $2^7 - 2 = 128 - 2 = 126$ host, sufficienti per le necessità della rete più grande (120 host più un indirizzo dell'interfaccia interna $IntA_A$ del router A, cioè 121).

Essendo il numero delle sottoreti in cui è suddivisa la rete principale pari a 2 elevato al numero di bit 1 presenti nel byte che contiene la separazione tra la serie di 1 e di 0 (in questo caso 1), possono essere definite $2^1 = 2$ sottoreti.

Per determinare gli indirizzi IP delle due sottoreti occorre calcolare l'incremento.

Al riguardo, considerata la netmask precedente in formato binario (11111111.1111 1111.11111111.10000000), si individua l'ultimo bit 1 della serie partendo da sinistra e si converte in base 10: l'incremento risulta $1 \times 2^7 = 128$.

Gli indirizzi IP delle due sottoreti si ricavano a partire dall'indirizzo della rete principale 192.168.20.0 incrementando di 128 l'ultimo byte, che pertanto risultano 192.168.20.0 e 192.168.20.128.

Si può quindi assegnare il primo indirizzo (192.168.20.0) alla sottorete A: gli indirizzi 192.168.20.1÷192.168.20.126 agli host e l'indirizzo 192.168.20.127 all'interfaccia interna $IntA_A$.

La netmask della seconda sottorete (255.255.255.128) è:

$$(255.255.255.128) \rightarrow 11111111.11111111.11111111.10000000$$

e pertanto, essendo 55 gli host di B, la netmask deve contenere 6 bit 0 ($2^6 - 2 = 64 - 2 = 62$), come di seguito indicato:

$$11111111.1111111.11111111.11000000 \rightarrow 255.255.255.192$$

Si può osservare che rispetto alla precedente netmask è stato aggiunto un bit 1, per cui si ottengono $2^1 = 2$ sottoreti da 62 host, più che sufficienti per indirizzare i 55 host della sottorete B.

Convertendo in decimale il byte della netmask in cui si ha la separazione dei bit 1 dai bit 0 (il quarto), si ottiene:

$$11000000 \rightarrow 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 192$$

e pertanto l'incremento vale:

$$k = 256 - 192 = 64$$

Gli indirizzi IP delle due sottoreti definite si ricavano a partire dall'indirizzo della rete 192.168.20.128 incrementando di 64 il quarto byte: l'indirizzo della prima sottorete è quindi 192.168.20.128, quello della seconda 192.168.20.192.

Si può quindi assegnare il primo indirizzo (192.168.20.128) alla sottorete B: gli indirizzi 192.168.20.129÷192.168.20.190 agli host e l'indirizzo 192.168.20.191 all'interfaccia interna $IntA_B$.

Assegnando il secondo indirizzo (192.168.20.192) al link, gli indirizzi disponibili risultano compresi tra 192.168.20.193 e 192.168.20.256: si può quindi assegnare all'interfaccia $IntA_B$ l'indirizzo 192.168.20.194 e all'interfaccia $IntB_A$ l'indirizzo 192.168.20.195.

Nella tabella che segue sono indicati gli indirizzi disponibili per le sottoreti e le interfacce dei router.

Sottorete	Indirizzi disponibili
A (192.168.20.0/25)	192.168.20.1/25 → 192.168.20.126/25
B (192.168.20.128/26)	192.168.20.129/26 → 192.168.20.190/26
$IntA_A$	192.168.20.127/25
$IntA_B$	192.168.20.194/26
$IntB_A$	192.168.20.195/26
$IntB_B$	192.168.20.191/26
Int_{ISP}	IP e netmask forniti dall'ISP

Indirizzi IP delle sottoreti.

Punto **2)** Il candidato determini l'attenuazione complessiva del collegamento in fibra ottica.

L'attenuazione complessiva A_T del collegamento è la somma dei seguenti contributi:

- attenuazione dovuta alla lunghezza del collegamento, il cui valore è dato da:
  - l'attenuazione del primo tronco = $0{,}35 \cdot l_x = 0{,}35 \cdot 2{,}5 = 0{,}875$ dB
  - l'attenuazione del secondo tronco = $0{,}40 \cdot l_y = 0{,}40 \cdot 1{,}5 = 0{,}6$ dB
- attenuazione dovuta ai diversi indici di rifrazione:

$$A_{(n)} = 10 \log \frac{1}{\tau}$$

in cui la trasmittenza τ risulta:

$$\tau = \frac{4}{2 + \frac{n_x}{n_y} + \frac{n_y}{n_x}} = \frac{4}{2 + \frac{1{,}3}{1{,}2} + \frac{1{,}2}{1{,}3}} = 0{,}998 \text{ dB}$$

Si ha quindi:

$$A_{(n)} = 10 \log \frac{1}{\tau} = 10 \log \frac{1}{0{,}998} = 0{,}0087 \text{ dB}$$

- attenuazione dovuta al diverso diametro del core dei due tronchi; il primo (fibra sorgente) ha il diametro del core superiore al secondo (fibra ricevente) e pertanto la relativa attenuazione vale:

$$A_d = 20 \log \frac{d_x}{d_y} = 20 \log \frac{50}{47} = 0{,}537 \text{ dB}$$

- attenuazione dovuta al diverso valore dell'apertura numerica dei due tronchi; il primo (fibra sorgente) ha infatti un'apertura numerica superiore a quella del secondo (fibra ricevente) e pertanto la relativa attenuazione vale:

$$A_{NA} = 20 \log \frac{NA_x}{NA_y} = 20 \log \frac{0{,}2}{0{,}19} = 0{,}445 \text{ dB}$$

L'attenuazione complessiva risulta quindi:

$$A_T = 0{,}875 + 0{,}6 + 0{,}0087 + 0{,}537 + 0{,}445 \approx 2{,}46 \text{ dB}$$

Punto **3)** Il candidato determini i margini inferiore e superiore del collegamento tenendo anche conto della penalità di banda η:

$$\eta = 1{,}5 \cdot \left(\frac{f_c}{B_T} \right)^2$$

La penalità di banda risulta:

$$\eta = 1{,}5 \cdot \left(\frac{f_c}{B_T} \right)^2 = 1{,}5 \cdot \left(\frac{68{,}7 \cdot 10^6}{66 \cdot 10^6} \right)^2 = 1{,}62 \equiv 2{,}09 \text{ dB}$$

Essendo l'attenuazione totale $A_T = 2{,}46$ dB e la penalità di banda $\eta = 2{,}09$ dB, poiché la potenza in trasmissione varia tra 1 e –2 dB, i livelli massimo e minimo del segnale in ricezione risultano:

$$P_{R\max} = P_{TXMAX} - A_T - \eta = 1 - 2{,}46 - 2{,}09 = -3{,}56 \text{ dB}$$
$$P_{R\max} = P_{TXMIN} - A_T - \eta = -2 - 2{,}46 - 2{,}09 = -6{,}55 \text{ dB}$$

Punto **4)** Il candidato verifichi se il collegamento soddisfa i requisiti di progettazione e consideri l'eventuale necessità di introdurre adeguati attenuatori.

Per garantire il corretto funzionamento del collegamento la potenza P_R del segnale in ricezione deve essere compresa nel range di accettabilità del ricevitore, cioè:

$$P_{RXMIN}\ (-32 \text{ dB}) < P_R < P_{RXMAX}\ (-25{,}6 \text{ dB})$$

Considerando allora il livello massimo di potenza che giunge al ricevitore calcolato al punto 3 ($P_{R\max} = -3{,}56$ dB) e la soglia di potenza massima accettabile dallo stesso ($P_{RXMAX} = -25{,}6$ dB), è immediato dedurre che $P_{R\max} > P_{RXMAX}$; si ha infatti:

$$P_{R\max} - P_{RXMAX} = -3{,}56 - (-25{,}6) = 22{,}04 \text{ dB}$$

e pertanto è necessario introdurre un attenuatore da 22,04 dB.

Infatti, con un tale valore di attenuazione, in corrispondenza del livello minimo del segnale che giunge in ricezione calcolato al punto 3 ($P_{R\min} = -6{,}55$ dB), il livello del segnale all'ingresso del ricevitore vale:

$$P_{R\min} - 22{,}04 = -6{,}55 - 22{,}04 = -28{,}59 \text{ dB}$$

che essendo maggiore di $P_{RXMIN} = -32$ dB garantisce il corretto funzionamento del sistema.

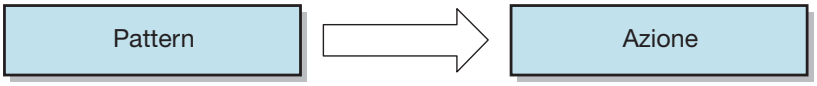
Punto **5)** Individui una Access Control List per impedire il traffico FTP dalla LAN della succursale verso la LAN della sede centrale.

Le **Access Control List** (**ACL**) sono liste nelle quali vengono disposte le regole di filtraggio dei pacchetti IP. In sostanza sono istruzioni di controllo sui pacchetti, ciascuna delle quali comprende una parte descrittiva e una decisionale.

L'ACL analizza sequenzialmente, istruzione per istruzione, ciascun pacchetto; appena un pacchetto soddisfa una delle regole la ricerca è interrotta e viene eseguita l'azione descritta nella parte decisionale della regola: il pacchetto è inoltrato o eliminato secondo l'istruzione eseguita.

Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (alla fine di un ACL c'è sempre l'istruzione deny any, ovvero nega tutto). Ogni regola ha la forma del tipo:

Forma della regola.



in cui

- il **pattern** specifica quali sono i pacchetti a cui si deve applicare la regola (per esempio tutto il traffico di un determinato indirizzo IP):
- l'**azione** indica se il pacchetto deve essere accettato o rifiutato (permit o deny).

Ogni ACL è composta da più regole, ciascuna delle quali viene valutata con il criterio "**first match**": si cerca la riga che soddisfa il pattern e una volta trovata si intraprende l'azione specificata (**permit o deny**), terminando la valutazione della ACL.

Se nessuna regola soddisfa il pattern si applica la policy di default; al riguardo si hanno due filosofie opposte:

- **open security policy**: tutto è permesso per default e nella lista ACL è presente l'elenco dei divieti;
- **closed security policy**: tutto è vietato per default e nella lista ACL sono elencati i pochi accessi che vengono permessi (è la politica maggiormente adottata).

Una volta definite, le regole devono essere memorizzate nel router, specificando se devono essere applicate al traffico in ingresso (inbound) oppure in uscita (outbound).

Sui router Cisco le ACL si possono categorizzare in due gruppi fondamentali:

- **ACL standard** – Sono utilizzate per filtrare il traffico basandosi solo sull'indirizzo IP sorgente del pacchetto IP e sono identificate da un numero che va da 1 a 99 e da 1300 a 1999;
- **ACL extended** – Oltre all'indirizzo IP sorgente basano le proprie decisioni anche su altri campi, quali l'indirizzo IP di destinazione, il protocollo utilizzato (TCP, UDP, …), le porte sorgente e destinazione ecc; sono identificate da un numero che va da 100 a 199 e da 2000 a 2699.

Un altro aspetto molto importante delle ACL è il loro posizionamento:

- **Posizionamento di ACL estese** – Devono essere posizionate il più vicino possibile alla sorgente da filtrare. Infatti, posizionarle lontano dalla sorgente sarebbe inefficiente, poiché i pacchetti attraverserebbero troppe zone prima di essere bloccati o filtrati.
- **Posizionamento di ACL standard** – Devono essere posizionate il più vicino possibile alla destinazione. Infatti, poiché le ACL standard filtrano i pacchetti solo in base all'indirizzo sorgente, il posizionamento nei pressi dell'interfaccia sorgente potrebbe bloccare il traffico ritenuto valido. Per esempio, se si volesse bloccare l'accesso a un server da una determinata rete, se la negazione fosse vicina alla rete sorgente, verrebbero bloccate anche altre destinazioni ritenute valide o addirittura negato tutto il traffico in uscita.

Nella richiesta del presente punto, la soluzione migliore è quella di utilizzare la filosofia "open security policy" sfruttando le ACL estese, che consentono di effettuare il controllo su più parametri.

La ACL estesa deve essere implementata più possibile vicino alla sorgente da filtrare (LAN succursale, rete B) e quindi nel router B.

Pertanto nell'interfaccia dei comandi CLI del router B va implementata l'ACL utilizzando i seguenti comandi:

Router(config)# **access-list 110 deny tcp 192.168.20.0 0.0.0.255 192.168.20.125 0.0.0.255 eq 21** (*blocco porta 21 ftp*)

Router(config)# **access-list 110 deny tcp 192.168.20.0 0.0.0.255 192.168.20.125 0.0.0.255 eq 20** (*blocco porta 20 ftp*)

Router(config)# **access-list 110 permitany** (*permesso a tutti gli altri protocolli*)

Router(config)# **interface Fa0/1** (*assumendo Fa0/1 la porta di ingresso al router B*)

Router(config-if)# **ipaccess-group 110 in** (*specifica che la regola va applicata in input*)

Punto 6. Il candidato metta in evidenza eventuali punti di debolezza del sistema e proponga, motivandola opportunamente, una modifica alla struttura dello stesso in modo da ridurre la vulnerabilità ai guasti.

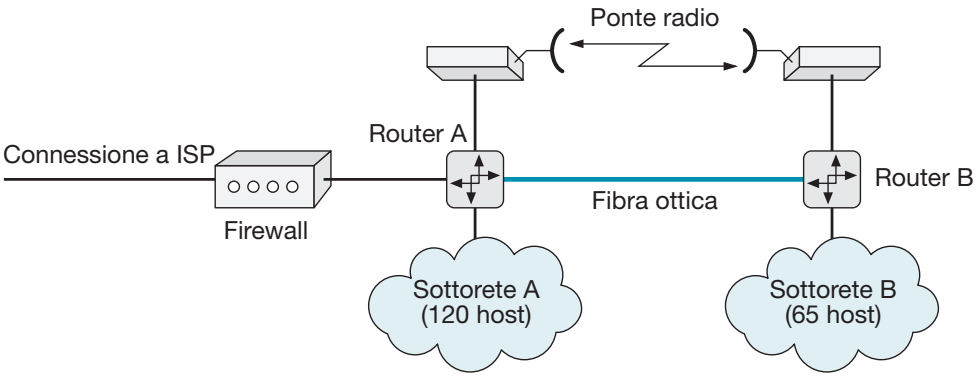
Dall'analisi dello schema del sistema indicato nel punto 1 si evince quanto segue:

- fra i due edifici esiste un solo collegamento in fibra ottica, e pertanto in caso di interruzione/guasto della fibra, la sottorete B non accederebbe più a Internet;
- assenza di almeno un firewall a protezione della rete nel collegamento verso l'ISP.

Le possibili azioni da intraprendere per migliorare le prestazioni del sistema possono quelle indicate di seguito.

- Proteggere la rete da attacchi esterni che potrebbero sia porre fuori servizio la rete sia consentire furti di dati, come per esempio progetti e documenti sensibili, tramite almeno un firewall hardware ad alte prestazioni.
- Essendo le due sedi in visibilità ottica, è possibile realizzare tra loro un secondo collegamento, di tipo radio, tramite una coppia di switch Wi-Fi o HIPERLAN (HIghPErformance Radio Local Area Network), in modo da avere velocità di trasmissione elevate e operare nella banda dei 5 GHz, meno congestionata di quella a 2,4 GHz, realizzando così una rete con topologia a maglia, come mostrato nella figura che segue.

Modifica alla struttura del sistema in modo da ridurre la vulnerabilità ai guasti.



SOLUZIONE SECONDA PARTE

Punto **1)** Il candidato illustri le differenze tra la trasmissione analogica e quella numerica, evidenziando i vantaggi delle seconde rispetto alle prime.

Il concetto di analogico è basato sulla somiglianza e continuità: una rappresentazione analogica riproduce le caratteristiche del fenomeno in ogni loro minima variazione (riproduzione fedele), stabilendo quindi un rapporto continuo tra il fenomeno rappresentato e il vettore di trasporto (segnale elettrico): per ogni variazione di stato della sorgente si ha una corrispondente variazione di stato del vettore.

Per esempio, in un collegamento telefonico, le vibrazioni generate nell'aria dalla voce umana arrivano al microfono della cornetta del telefono, sono convertite in variazioni di corrente elettrica e vengono inviate sulla linea di collegamento con l'altro apparecchio, dove avviene il processo inverso.

Nella trasmissione digitale, invece, le informazioni della sorgente, che possono essere già in formato digitale, oppure digitalizzate al momento della trasmissione, sono veicolate in un segnale che può assumere solo due stati, ai quali viene associata una cifra binaria: il bit, che può assumere soltanto i valori "0" o "1".

Ogni bit può essere rappresentato mediante vari tipi di segnali: per esempio, due livelli di tensione elettrica, due frequenze, o ancora due impulsi luminosi emessi da un laser (dipende dal sistema di trasmissione utilizzato). La codifica dei bit può essere effettuata in diversi modi.

Nel caso più semplice, a ogni bit corrisponde un livello del segnale: per esempio, allo 0 un livello di tensione basso, all'1 un livello alto.

Con questa tipologia di codifica sono però possibili errori dovuti, per esempio, a eventuali interferenze che possono trasformare gli "1" in "0" e viceversa: per questa ra-

gione nei sistemi di telecomunicazione digitale sono utilizzate codifiche più complesse, che consentono una corretta ricostruzione del segnale in quanto dotate di processi di individuazione e correzione degli errori di trasmissione.

I sistemi di trasmissione digitale hanno sostituito completamente quelli analogici per varie ragioni, le più importanti delle quali sono:

- maggiore efficienza e qualità nella comunicazione, in quanto meno soggetti ai disturbi che possono essere introdotti durante trasmissione, e possibilità di utilizzare tecniche per la correzione automatica degli errori di trasmissione;
- notevole sicurezza della comunicazione, perché consentono di implementare processi di cifratura che tutelano dalle intercettazioni;
- i costi delle tecnologie digitali sono diminuiti con un ritmo vertiginoso, rendendole economicamente convenienti;
- l'enorme diffusione dei computer, prima nelle tradizionali aree commerciali e scientifiche e poi nel mercato di massa, ha portato all'integrazione di tutte le tecnologie in un'unica piattaforma numerica, in grado di offrire servizi interattivi digitali.

Punto **2)** Il candidato descriva il funzionamento del DNS e la suddivisione logica dell'insieme di tutti gli indirizzi simbolici di Internet.

L'idea alla base del funzionamento del DNS è la suddivisione logica dell'insieme degli indirizzi simbolici di Internet, detto **spazio dei nomi**, in settori più o meno grandi, detti **domini**, per ciascuno dei quali è definita una struttura di gestione denominata **autorità di dominio**.

Le autorità di dominio, coordinate da un'**autorità centrale**, sono delegate a gestire l'assegnazione dei nomi nell'area di propria competenza.

Ogni dominio può essere diviso in domini più piccoli, detti **sottodomini**, la cui gestione è affidata ad **autorità di sottodominio**.

Un **nome di dominio** o **indirizzo Internet** (o anche **F**ully **Q**ualified **D**omain **N**ame, **FQDN**) è una notazione simbolica di tipo letterale formata da vari campi, detti **etichette**, separati da punti, ognuno dei quali è assegnato dall'autorità di dominio competente che ne garantisce l'unicità.

L'etichetta più a sinistra indica il nome del computer, che solitamente coincide con quello della persona fisica proprietaria del computer stesso (o al quale è affidato, nel caso di dipendente di un'azienda o ente), i successivi nomi indicano i domini, ciascuno dei quali è contenuto in quello che segue.

Un nome di dominio completo termina sempre con un punto, che rappresenta la radice della gerarchia (autorità centrale).

Per esempio nel nome di dominio:

mrossi.redazione.hoepli.it.

- il "**.**"rappresenta il livello più alto gestito dall'autorità centrale (ICANN, Internet Corporation for Assigned Names and Numbers);
- "**it**" è il dominio di primo livello (unico a livello mondiale) che comprende tutti i domini italiani; l'autorità centrale delega i responsabili della gestione dei nomi sotto il dominio "it" (It-NIC, Italian Network Information Center, presso l'Istituto per le applicazioni telematiche del CNR di Pisa);
- "**hoepli**" è il dominio di secondo livello che gestisce i nomi per la casa editrice HOEPLI ed è unico a livello del dominio "it"; l'autorità del dominio "it" delega ai responsabili la gestione dei nomi sotto il dominio hoepli.it;
- "**redazione**" è il dominio di terzo livello che gestisce i nomi per il reparto "redazione" della casa editrice HOEPLI ed è unico a livello del dominio "hoepli.it"; l'autorità del dominio "hoepli.it" delega ai responsabili la gestione dei nomi sotto il dominio "redazione.hoepli.it";
- "**mrossi**" è il nome di un computer stabilito dall'autorità del domino redazione. hoepli.it ed è unico a livello di tale dominio.

Si può osservare che l'ordine gerarchico va da destra verso sinistra: il nome più a destra rappresenta infatti il dominio di più alto livello, e procedendo a sinistra si entra nei dettagli.

Essendo le notazioni letterali soltanto artifici introdotti per ricordare più facilmente gli indirizzi IP, sui domini non esiste alcun vincolo geografico e pertanto, anche se in Italia la maggior parte dei computer appartengono al dominio "it", ne esistono alcuni con le altre denominazione (com, net, org e altri).

Normalmente un computer ha un solo nome, ma per lo stesso computer è possibile definire più nomi, allo scopo di indicare con notazione diversa i servizi che svolge.

Nell'ambito di ogni dominio di primo livello può essere definito qualsiasi numero di domini di livello inferiore.

Punto **3)** Due stazioni radio sono distanti tra loro 20 km. La stazione trasmittente, dotata di un'antenna a paraboloide avente diametro $d_T = 1$ m ed efficienza superficiale $\eta_{aT} = 0{,}77$, è collegata al trasmettitore tramite un tratto di guida d'onda di lunghezza pari a 15 m, avente un'attenuazione di 0,15 dB/m. La stazione ricevente, dotata di un'antenna a paraboloide di diametro $d_R = 1{,}2$ m ed efficienza superficiale $\eta_{aT} = 0{,}78$, è collegata al ricevitore tramite un tratto di guida d'onda avente lunghezza pari a 10 m e attenuazione di 0, 13 dB/m. Nel caso la potenza in trasmissione sia $P_T = 1{,}5$ kW e la frequenza di lavoro $f = 5$ GHz, il candidato determini la potenza in ricezione.

La lunghezza d'onda di lavoro vale:

$$\lambda = \frac{c}{f} = \frac{3 \cdot 10^8}{5 \cdot 10^9} = 6 \text{ cm}$$

Stazione trasmittente

- attenuazione della guida d'onda:

$$A_T = 15 \cdot 0{,}15 = 2{,}25 \text{ dB}$$

- guadagno del paraboloide:

$$G_T = \frac{\pi^2 d^2}{\lambda^2}\eta_{aT} = \frac{\pi^2 \cdot 1^2}{0{,}06^2} = 2338{,}77 \equiv 33{,}68 \text{ dB}$$

Stazione ricevente

- attenuazione della guida d'onda:

$$A_R = 10 \cdot 0{,}13 = 1{,}3 \text{ dB}$$

- guadagno del paraboloide:

$$G_T = \frac{\pi^2 d_R^2}{\lambda^2}\eta_{aT} = \frac{\pi^2 \cdot 1{,}3^2}{0{,}06^2} = 4628{,}53 \equiv 36{,}65 \text{ dB}$$

L'attenuazione dello spazio libero risulta:

$$A_L \left(\frac{4\pi R}{\lambda}\right)^2 = \left(\frac{4\pi \cdot 20 \cdot 10^3}{0{,}06}\right)^2 \cong 1{,}75 \cdot 10^{13} \equiv 132{,}43 \text{ dB}$$

Ricordando che il riferimento assoluto di potenza è $P_0 = 1$ mW, la potenza P_T espressa in dB vale:

$$P_T = 10\log\left(\frac{P_T}{P_0}\right) = 10\log\left(\frac{1{,}5 \cdot 10^3}{10^{-3}}\right) = 61{,}76 \text{ dB}$$

La potenza ricevuta risulta pertanto:

$$P_R(\text{dB}) = P_T(\text{dB}) + G_R(\text{dB}) + G_T(\text{dB}) - A_L(\text{dB}) - A_T(\text{dB}) - A_R(\text{dB}) =$$
$$= 61{,}76 + 36{,}65 + 33{,}68 - 132{,}43 - 2{,}25 - 1{,}3 = -3{,}89 \text{ dB}$$

Punto **4)** Il candidato illustri le caratteristiche peculiari dei modelli distribuiti di reti Windows.

Per la gestione delle reti di calcolatori, Windows propone due modelli distribuiti:

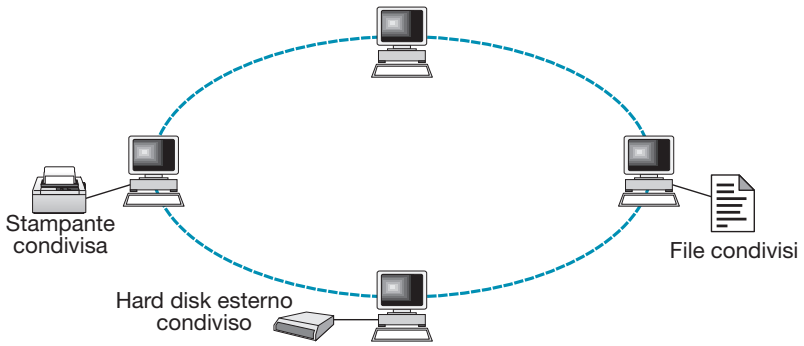
- **modello a Workgroup (Gruppo di lavoro)**;
- **modello a Dominio**.

Un gruppo di lavoro (figura che segue) è un insieme di computer connessi in rete, in genere una piccola LAN domestica o aziendale, che condividono una o più risorse (file, stampanti, modem, …).

In una LAN possono coesistere più gruppi di lavoro, ma ogni computer può accedere solo alle risorse condivise del gruppo al quale appartiene.

Il gruppo di lavoro non è protetto da password d'accesso: ogni computer opera come server stand-alone (indipendentemente dagli altri).

L'amministratore del computer (il proprietario) decide quali risorse condividere e con quali utenti.



Gruppo di lavoro.

Un dominio è un insieme di computer, tipicamente una LAN di un'organizzazione, come per esempio un'azienda o un ente pubblico, che condividono una politica di sicurezza e un database (database di directory) dove sono contenuti i dati di tutti i componenti del dominio stesso.

I computer sono amministrati tramite regole comuni di tipo autorizzativo (policy di sicurezza): un client deve rispettare le procedure di autenticazione definite dai servizi che risiedono sul server.

Tali procedure definiscono una gerarchia di profili (in termini di permessi e accessi alle risorse o ai sistemi) e stabiliscono l'appartenenza al dominio.

In un dominio sono sempre presenti un **PDC server** (Primary Domain Controller) e un **BDC server** (Backup Domain Controller).

Il primo (PDC server) gestisce il database di directory con le informazioni di account per il dominio: è il server primario che gestisce l'autenticazione degli utenti.

Il secondo (BDC server) è il backup del PDC server: contiene una copia della configurazione del PDC e interviene nel caso di malfunzionamento del PDC stesso.

Normalmente il modello a dominio viene applicato nelle grandi organizzazioni, il modello a gruppi di lavoro in ambiti domestici o piccole aziende.

MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA RICERCA

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

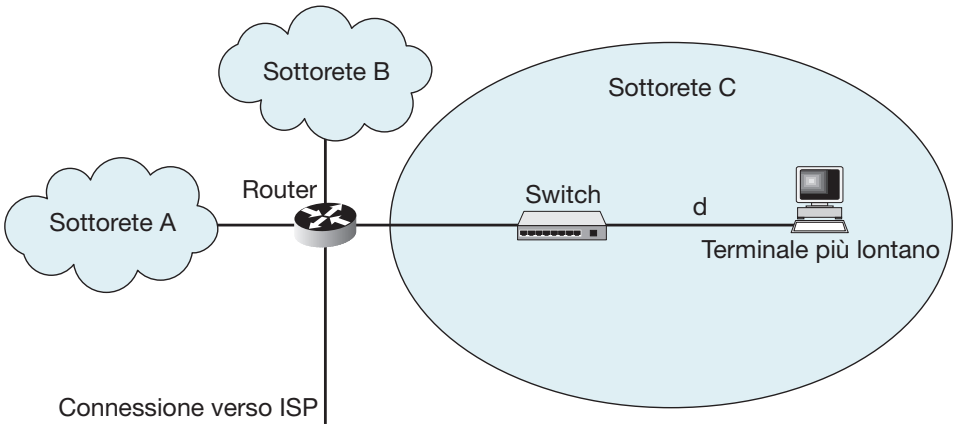
Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE TELECOMUNICAZIONI
Tema di: SISTEMI E RETI E TELECOMUNICAZIONI
ESEMPIO PROVA 3

* Durata massima della prova: 6 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.

Il candidato (che può avvalersi delle conoscenze e competenze maturate anche attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda) svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte. *

PRIMA PARTE

Una LAN aziendale è divisa in tre sottoreti, come indicato nella figura seguente.



Rete aziendale suddivisa in tre sottoreti.

La sottorete A è formata da 200 host, la sottorete B comprende 80 host, la sottorete C, che funziona secondo lo standard 802.3 alla velocità di 100 Mbps, comprende 25 host collegati allo switch ed ha una velocità v di propagazione dei segnali sulle linee pari a $1{,}5 \cdot 10^8$ m/s.

Sapendo che il ritardo di propagazione introdotto dallo switch è $t_{switch} = 2$ μs e che le trame trasmesse hanno una lunghezza minima di 64 byte, il candidato, formulata ogni ipotesi aggiuntiva che ritiene opportuna, produca quanto segue.

1) Descriva gli aspetti fondamentali dello standard di funzionamento della sottorete C.
2) Determini il massimo valore che può assumere la distanza d tra il terminale più lontano e lo switch nella sottorete C.
3) Proponga un piano di indirizzamento che minimizzi il numero di indirizzi da richiedere all'ISP e lasci il minor numero di indirizzi inutilizzati in ciascuna delle sottoreti, sapendo che l'ISP può assegnare indirizzi IP di classe C contigui a partire da 192.220.15.0.
4) Proponga e descriva un possibile servizio di autenticazione per gli utenti della rete.

SECONDA PARTE

Il candidato scelga due fra i seguenti quesiti e per ogni scelta formuli la risposta che ritiene più opportuna:

1) descriva e illustri l'architettura dei sistemi crittografici a chiave pubblica;
2) descriva il funzionamento della firma elettronica mediante crittografia a chiave pubblica;

3) una sorgente elettromagnetica puntiforme irradia nello spazio circostante uniformemente in tutte le direzioni. Determini i valori delle ampiezze E_M e H_M del campo elettromagnetico a una distanza $r = 2$ km dalla sorgente, supponendo che la potenza emessa sia $P_0 = 2$ kW e le perdite trascurabili;

4) supponendo di trascurare l'effetto del rumore, è possibile trasmettere una sequenza binaria a 24 000 bit/s su un mezzo trasmissivo avente banda $B = 6$ kHz?

SOLUZIONE PRIMA PARTE

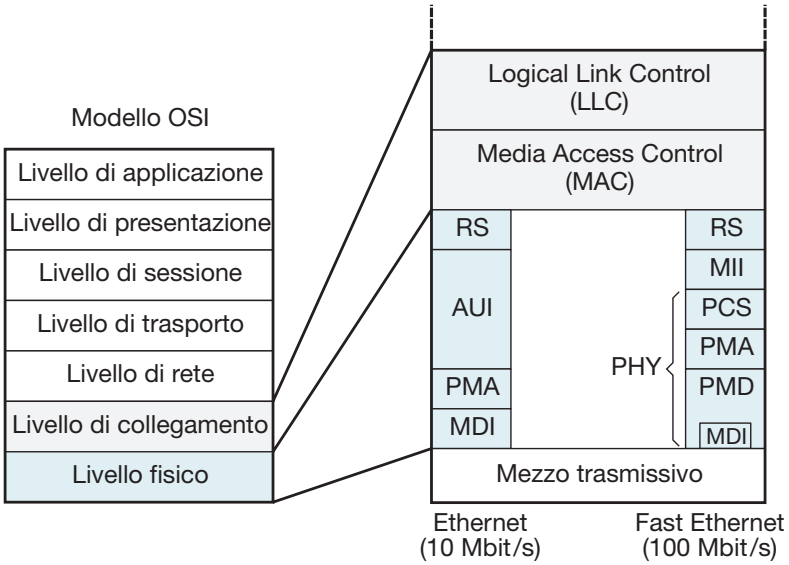
Punto **1)** Il candidato descriva gli aspetti fondamentali dello standard di funzionamento della sottorete C.

Lo standard indicato dal testo è lo IEEE 802.3u o 100baseT, noto come Fast Ethernet.

L'IEEE 802.3, evoluzione della rete Ethernet, utilizza un protocollo MAC di tipo CSMA/CD in cui la gestione del canale trasmissivo avviene tramite una procedura di contesa non deterministica, che non garantisce un tempo massimo di attesa predefinito; la topologia logica a bus può essere sia a bus sia a stella ed è caratterizzatao da una velocità di trasmissione di 100 Mbit/s.

Il MAC si interfaccia con il livello fisico (PHY) mediante un livello denominato Media Indipendent Interface (MII), in grado di funzionare sia a 10 che a 100 Mbit/s; dal punto di vista logico il MII equivale all'AUI (Attachement Unit Interface) di Ethernet.

In realtà tra l'MII e il MAC è posto il Reconciliation Sublayer (RS), avente la funzione di tradurre i segnali MII in formato di tipo PLS (Physical Layer Signaling) cioè il livello che realizza la codifica e decodifica dei bit rispettivamente in fase di trasmissione e ricezione (nel 10baseT è collocato tra AUI e MAC), le cui funzionalità sono inglobate nell'RS.



Architettura del 100baseT.

Il livello fisico PHY comprende i sottolivelli Physical Coding Sublayer (PCS), Physical Medium Attachment (PMA) e Physical Medium Dependent (PMD).

Nel PCS sono contenute le specifiche per ottenere le tre varianti del 100baseT rappresentate dagli standard 100baseTX, 100baseT4 e il 100baseFX (la coppia 100baseTX/FX è anche denominata 100baseX).

Il sottolivello PMA espleta le funzioni per la trasmissione e la ricezione del segnale informativo consentendo al PCS di supportare diversi mezzi trasmissivi; il PMD costituisce l'interfaccia vera e propria con i vari mezzi trasmissivi, nel quale sono definite le codifiche dei segnali utilizzate in ciascuno di essi; quest'ultimo contiene l'MDI,

cioè l'effettiva interfaccia meccanica ed elettrica con il mezzo trasmissivo, nella quale sono definite le modalità di connessione, come per esempio i connettori per i mezzi trasmissivi.

Essendo previsto il funzionamento sia a 10 che a 100 Mbit/s, lo standard 100baseT definisce un processo, detto di autonegoziazione, che consente a due schede di rete di scambiarsi automaticamente le informazioni sulle loro caratteristiche, in modo da poter realizzare la configurazione necessaria affinché entrambi funzionino alla massima velocità comune.

Per esempio, tramite l'autonegoziazione una scheda di rete 10/100 (cioè con possibilità di funzionamento sia a 10 sia a 100 Mbit/s) può funzionare in modalità 10baseT se connessa a un hub o switch 10baseT, e in modalità 100baseT se connessa a un hub o switch 100baseT.

Il mezzo di comunicazione più utilizzato è il cavo FTP (Foiled Twisted Pair), formato da doppini intrecciati, schermati con un unico schermo realizzato con un foglio di materiale conduttore (in genere alluminio).

Punto **2)** Il candidato determini il massimo valore che può assumere la distanza d tra il terminale più lontano e lo switch nella sottorete C.

Per la sottorete C il testo ipotizza una trama (PDU) minima di 64 byte e il protocollo CSMA/CD; indicando allora con τ il tempo di propagazione dei bit nella rete, il Round Trip Collision Delay (t_r), ovvero il massimo tempo di ritardo che può intercorrere dalla trasmissione del primo bit di una PDU all'individuazione di una collisione (ovvero l'ultimo bit della relativa sequenza di jamming), vale:

$$t_r = 2\pi$$

il quale deve essere inferiore al tempo di trasmissione $t_{tx\min}$ della trama di lunghezza minima, cioè:

$$t_r \leq t_{tx\,\min}$$

che vale:

$$t_{tx\,\min} = \frac{L_{trama}}{f_{bit}} = \frac{64 \cdot 8}{100 \cdot 10^6} = 5{,}12\ \mu\,\text{sec}$$

Considerando che il ritardo di propagazione introdotto dallo switch è $t_{switch} = 2$ µs, il tempo di propagazione τ risulta:

$$\tau = t_{switch} + \frac{d}{v} = 2 \cdot 10^{-6} + \frac{d}{1{,}5 \cdot 10^8}$$

Il Round Trip Collision Delay vale allora:

$$t_r = 2\tau = 2\left(2 \cdot 10^{-6} + \frac{d}{1{,}5 \cdot 10^8}\right) = 4 \cdot 10^{-6} + 1{,}33\frac{d}{10^8}$$

Dovendo essere $t_r \leq t_{tx\min}$, si ha:

$$4 \cdot 10^{-6} + 1{,}33\frac{d}{10^8} \leq 5{,}12 \cdot 10^{-6} \rightarrow 400 + 1{,}33d \leq 512$$

da cui si ottiene:

$$d \leq \frac{512 - 400}{1{,}33} \leq 84\ \text{m}$$

Punto **3)** Il candidato proponga un piano di indirizzamento che minimizzi il numero di indirizzi da richiedere all'ISP e lasci il minor numero di indirizzi inutilizzati in ciascuna delle sottoreti, sapendo che l'ISP può assegnare indirizzi IP di classe C contigui a partire da 192.220.15.0.

Essendo il numero totale degli host della rete 200 + 80 + 25 = 305, non è possibile utilizzare un solo blocco di indirizzi C (si ricordi che un blocco C comprende 254 indirizzi IP), e quindi occorre utilizzarne due: per esempio, per la sottorete A (200 host) si può utilizzare il blocco 192.220.15.0, e per le reti B e C il blocco 192.220.16.0.

Considerando per la sottorete A la netmask 255.255.255.0, gli host avranno indirizzi IP compresi tra 192.220.15.1 e 192.220.15.200; all'interfaccia del router verso la rete A è assegnato l'indirizzo 192.220.15.201.

Il blocco 192.220.16.00 viene suddiviso tra le sottoreti B e C e la connessione verso l'ISP; occorre quindi definire l'indirizzamento per tre sottoreti: B con 80 host (più l'interfaccia con il router), C con 25 host (più l'interfaccia con il router) e l'interfaccia verso l'ISP.

Al riguardo conviene utilizzare la modalità di subnetting VLSM/CIDR (Variable Lengh Subnetting Mask/Classless Inter Domain Routing), che consente di assegnare alle tre sottoreti netmask di lunghezza variabile, associando a ciascuna di esse un numero di bit tale da evitare indirizzi non utilizzati; a tal proposito occorre innanzitutto determinare il numero di bit necessari a indirizzare gli host della sottorete più grande (B).

Per indirizzare gli 80 host (più l'interfaccia verso il router) sono necessari 7 zeri nell'ultimo ottetto della netmask (il numero dei terminali per ciascuna sottorete si ottiene elevando la cifra 2 al numero di 0 presenti nella netmask diminuito di due unità); per la rete B la netmask risulta pertanto:

$$11111111.1111111.11111111.10000000 \rightarrow 255.255.255.128$$

Così facendo, infatti, si ottengono $2^7 - 2 = 126$ terminali, più che sufficienti per indirizzare gli 80 host più l'indirizzo l'interfaccia verso il router.

Ricordando che il numero delle sottoreti in cui è suddivisa la rete principale è pari a 2 elevato al numero di bit 1 presenti nel byte che contiene la separazione tra la serie di 1 e di 0 (in questo caso uno), le sottoreti che si possono definire sono $2^1 = 2$.

Per determinare gli indirizzi IP di ciascuna delle due sottoreti occorre calcolare l'incremento.

Al riguardo, considerata la netmask precedente in formato binario (11111111.111 11111.11111111.**1**0000000), si individua l'ultimo bit 1 della serie partendo da sinistra (in grassetto) e si converte in base 10: il valore dell'incremento risulta $1 \times 2^7 = 128$.

Gli indirizzi IP delle due sottoreti da 128 host si ricavano a partire dall'indirizzo della rete principale 192.220.16.0 incrementando di 128 l'ultimo byte e quindi risultano: 192.220.16.0 e 192.192.192.128.

Il primo dei due indirizzi (192.220.16.0) viene assegnato alla sottorete B, e si prosegue con il ripartizionamento della seconda sottorete (192.192.192.128) per ricavare gli indirizzi di C. Gli indirizzi della sottorete B sono pertanto compresi tra 192.220.16.1 e 192.220.16.80 e all'interfaccia con il router è assegnato l'indirizzo 192.220.16.81 (netmask 255.255.255.128).

La sottorete C ha 25 host e quindi sono necessari 5 zeri nell'ultimo ottetto della netmask:

$$11111111.1111111.11111111.11100000 \rightarrow 255.255.255.224$$

Così facendo si ottengono infatti $2^5 - 2 = 30$ terminali; nell'ottetto che contiene la separazione tra la serie di 1 e di 0 della netmask, il primo dei due bit 1 è riservato per la sottorete B (192.220.16.0) e quindi rimangono due bit 1 disponibili per la sottorete C, con i quali si possono definire $2^2 = 4$ reti da 30 terminali.

Considerata la netmask in formato binario (11111111.11111111.11111111.111**1**000 00), si individua l'ultimo bit 1 della serie partendo da sinistra (in grassetto) e si converte in base 10; poiché il valore risultante è pari a $1 \cdot 2^5 = 32$, l'incremento vale 32.

Gli indirizzi IP delle quattro sottoreti si ricavano a partire dall'indirizzo 192.220.16.128 incrementando di 32 l'ultimo ottetto. L'indirizzo della prima sottorete è quindi 192.220.16.128, quello della seconda 192.220.16.160, quella della terza 192.220.16.192 e quello della quarta 192.220.16.224.

Scegliendo per la sottorete C il primo indirizzo utile (192.220.16.128), rimangono disponibili altre tre sottoreti da 30 host ciascuna (la192.220.16.160, la 192.220.16.192 e la 192.220.16.224).

Gli indirizzi disponibili per la sottorete C, sono pertanto compresi tra 192.220.16.129 e 192.220.16.153, e all'interfaccia con il router è assegnato l'indirizzo 192.220.16.154.

L'IP verso l'ISP del router si intende fornito dall'ISP.

Nella tabella che segue è riassunta la configurazione degli indirizzi IP determinata.

Piano di indirizzamento della rete data.

Sottorete	Indirizzo di sottorete	Netmask	Indirizzi utilizzati	Indirizzi Interfaccia Router
A	192.220.15.0	255.255.255.0	192.220.15.1 → 192.220.15.200	192.220.15.201
B	192.220.16.0	255.255.255.128	192.220.16.1 → 192.220.16.80	192.220.16.81
C	192.220.16.128	255.255.255.224	192.220.16.129 → 192.220.16.153	192.220.16.154
ISP	192.220.16.160			

Punto **4)** Il candidato descriva e illustri un possibile servizio di autenticazione per gli utenti della rete.

La crittografia, cioè il procedimento che consente di modificare le informazioni in modo da renderle comprensibili soltanto ai legittimi destinatari, è fondamentale per l'integrità e la riservatezza dei dati; tuttavia, se non è affiancata da una procedura di autenticazione, non garantisce un livello di protezione adeguato agli utenti che operano online.

In una comunicazione sicura, infatti, oltre alla cifratura è necessaria una procedura di autenticazione che provi le identità degli interlocutori.

L'autenticazione dei messaggi è una procedura che consente di verificare se i messaggi ricevuti provengono dalla sorgente indicata e che non sia stata introdotta alcuna modifica durante la trasmissione.

Spesso l'autenticazione è considerata come una firma digitale: i due concetti sono simili ma non rappresentano la stessa operazione.

Infatti, la firma digitale è una tecnica di autenticazione che include misure per impedire al mittente di negare di aver trasmesso il messaggio.

Tutte le tecniche di autenticazione (e di firma digitale) possono essere considerate formate da due livelli funzionali:

- un **livello inferiore**, comprendente una funzione che genera un output, denominato autenticatore, utilizzato dal livello superiore per autenticare il messaggio;
- un **livello superiore**, comprendente un algoritmo il quale, sulla base dell'autenticatore, consente al destinatario del messaggio di verificarne l'autenticità.

La crittografia, sia simmetrica sia a chiave pubblica, può essere utilizzata come forma di autenticazione di un messaggio.

Nel caso della crittografia simmetrica, il messaggio inviato dalla sorgente A alla destinazione B viene crittografato utilizzando una chiave segreta K_s.

Essendo tale chiave conosciuta soltanto da A e B, nessuno può risalire al messaggio e ciò garantisce a B che il messaggio proviene da A: la crittografia simmetrica garantisce pertanto sia l'autenticazione sia la segretezza.

Il processo di decrittografia di B deve produrre un testo in chiaro uguale a quello inviato da A, e se quest'ultimo ha un senso compiuto, per B è semplice verificare se il messaggio che ha ricevuto è corretto.

Se invece il testo in chiaro trasmesso da A (previa crittografia) è una sequenza intelligibile di bit, per esempio il prodotto di una digitalizzazione di un fotogramma, per B risulta molto difficile stabilire se il testo in chiaro ottenuto dopo il processo di decrittografia è corretto e quindi autentico.

Un estraneo potrebbe infatti disturbare la comunicazione tra A e B semplicemente emettendo messaggi con contenuti privi di significato (per esempio una sequenza casuale di bit) senza che B se ne possa accorgere.

Una soluzione a tale problema è l'aggiunta al messaggio in chiaro di un codice di rilevamento degli errori, ottenuto inviando il messaggio all'input di una funzione F che fornisce in output un codice di errore in funzione del contenuto del messaggio stesso.

Il codice di errore è successivamente aggiunto al messaggio e il blocco così ottenuto (messaggio + codice di errore) viene crittografato.

Eseguita la decrittografia del blocco ricevuto, B separa il codice di errore dal messaggio e invia quest'ultimo all'input della stessa funzione F: se il codice di errore calcolato da F è uguale a quello ricevuto, il messaggio è sicuramente autentico.

L'autenticazione può essere ottenuta anche tramite la crittografia pubblica, codificando il messaggio tramite la chiave privata del mittente, anzichè con la chiave pubblica del destinatario, il quale può decrittografare il messaggio utilizzando la chiave pubblica del mittente. Poiché il messaggio è stato crittografato utilizzando la chiave privata del mittente, solo quest'ultimo può averlo trasmesso: è pertanto garantita l'autenticazione del mittente (l'intero messaggio crittografato funge in sostanza da autenticazione).

Questo metodo, sebbene convalidi sia l'autore sia il contenuto, richiede una grande area di memoria, in quanto deve essere mantenuta una copia in chiaro per l'utilizzo di ogni messaggio, e una copia in testo cifrato per poterne verificare l'origine in caso di disputa. Non è inoltre garantita la segretezza, in quanto, nel caso un terzo riuscisse a intercettare il messaggio potrebbe decrittografarlo utilizzando la chiave pubblica del mittente.

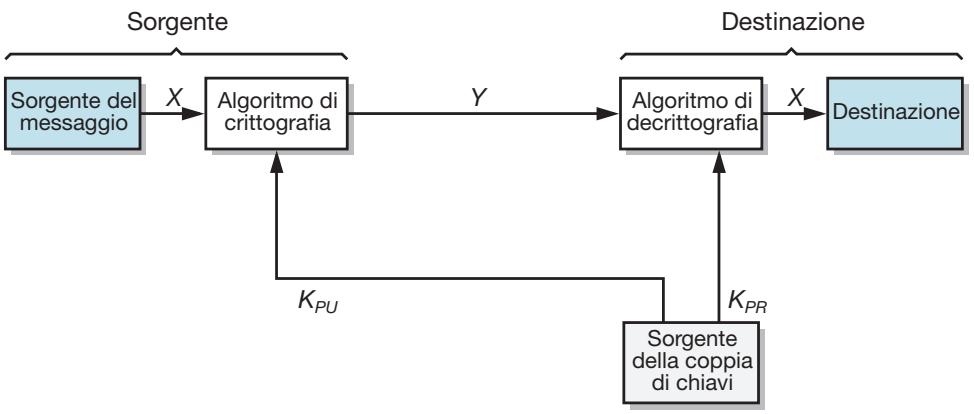
È però possibile garantire sia la funzione di autenticazione sia la segretezza tramite una doppia applicazione a chiave pubblica: prima viene crittografato il messaggio utilizzando la chiave privata del mittente, garantendo così l'autenticazione, e successivamente viene crittografato quello ottenuto utilizzando la chiave pubblica del destinatario, in modo che il testo cifrato prodotto possa essere decrittografato solo utilizzando la chiave privata del destinatario, garantendo così la segretezza.

Lo svantaggio di questo approccio è l'applicazione per due volte dell'algoritmo a chiave pubblica: questo inconveniente può essere superato mediante i codici MAC.

SOLUZIONE SECONDA PARTE

Punto **1)** Il candidato descriva e illustri l'architettura dei sistemi crittografici a chiave pubblica.

Nella figura che segue è indicato lo schema con i blocchi essenziali di un sistema di crittografia a chiave pubblica.



Schema di principio di un sistema crittografico a chiave pubblica.

Il messaggio in chiaro (indicato con X) prodotto dal mittente è un insieme di simboli di un alfabeto finito $[X_1, X_2, X_3, \ldots, X_N]$.

Il destinatario del messaggio genera una coppia di chiavi correlate: una chiave privata K_{PR} nota solo a lui e una chiave pubblica K_{PU} accessibile al mittente.

Utilizzando come input il messaggio in chiaro X e la chiave di crittogratia K_{PU}, mediante l'algoritmo di crittografia (indicato con E) il mittente genera il testo cifrato:

$$Y = [Y_1, Y_2, Y_3, \ldots, Y_N]$$

l'operazione può essere così rappresentata:

$$Y = E_{K_{PU}}(X)$$

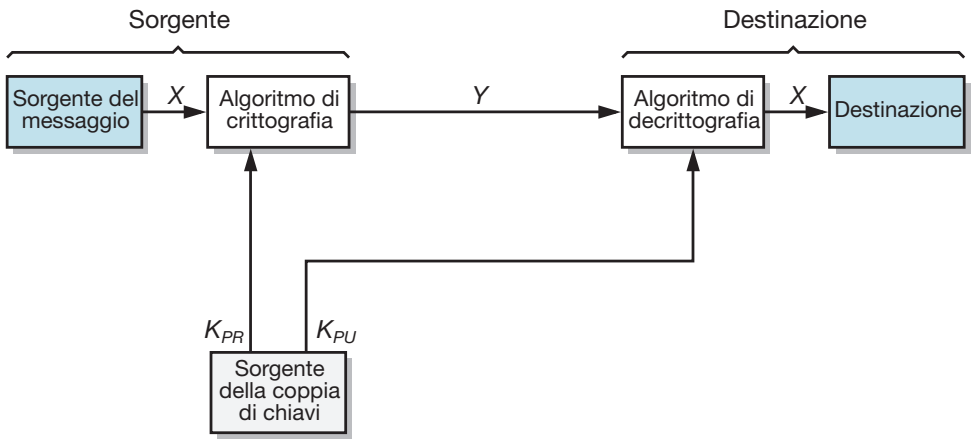
Il destinatario, in possesso della sua chiave privata (K_{PR}), applicando l'algoritmo di decrittografia (indicato con D) può invertire la trasformazione rigenerando il testo in chiaro:

$$X = E_{K_{PR}}(Y)$$

È importante sottolineare che può essere utilizzata una qualsiasi delle due chiavi correlate, utilizzando l'altra per la decrittografia.

Nel caso il mittente codifichi un messaggio per il destinatario utilizzando la propria chiave privata, anziché la chiave pubblica del destinatario, quest'ultimo può decrittografare il messaggio utilizzando la chiave pubblica del mittente.

Sistema crittografico o a chiave pubblica utilizzato per l'autenticazione.



Poiché il messaggio è stato crittografato utilizzando la chiave privata del mittente, solo quest'ultimo può aver trasmesso il messaggio: questo esempio mostra che l'algoritmo di crittografia a chiave pubblica può essere utilizzato per garantire l'autenticazione del mittente (l'intero messaggio crittografato funge da firma digitale).

Le operazioni possono essere così rappresentate:

$$Y = E_{K_{PR}}(X)$$

$$X = D_{K_{PU}}(Y)$$

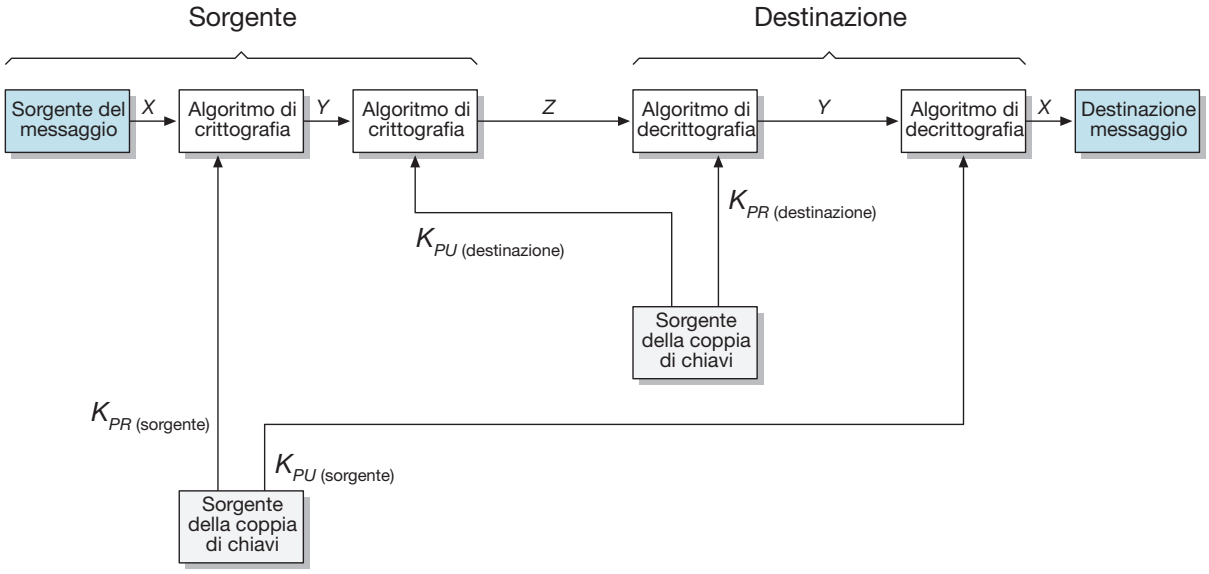
Questa metodologia, sebbene convalidi sia l'autore che il contenuto, richiede una grande area di memoria, perché deve essere mantenuta una copia in chiaro di ogni messaggio per essere utilizzato e una copia in testo cifrato per verificare l'origine in caso di disputa.

Lo stesso risultato può essere ottenuto mediante la crittografia di un piccolo blocco di bit, denominato **autenticatore**, che rende impossibile la modifica del documento senza modificare il blocco stesso, trasmettendo il messaggio in chiaro.

Così facendo non è però garantita la segretezza del messaggio in quanto viene trasmesso in chiaro: il messaggio è sicuro nei riguardi delle alterazioni ma non è protetto dalle intercettazioni.

È da osservare che anche nel caso di crittografia completa (crittografia dell'intero messaggio) non è garantita la segretezza, in quanto il messaggio può essere decrittografato utilizzando la chiave pubblica del mittente. È però possibile garantire sia la funzione di autenticazione sia la segretezza tramite una doppia applicazione a chiave pubblica, come mostrato nella figura seguente.

Segretezza e autenticazione.



In questo caso, prima viene crittografato il messaggio utilizzando la chiave privata del mittente, garantendo così la firma digitale, e poi è eseguita di nuovo la crittografia mediante la chiave pubblica del destinatario, in modo che il testo cifrato possa essere decrittografato solo utilizzando la chiave privata del destinatario, garantendo così la segretezza.

Questo approccio ha però uno svantaggio: l'algoritmo a chiave pubblica, già complesso, deve essere applicato per due volte invece di una.

Pertanto, a seconda dell'applicazione (crittografia o autenticazione), il mittente utilizza la propria chiave privata, la chiave pubblica del destinatario o entrambe.

In generale è possibile classificare i sistemi crittografici a chiave pubblica in due categorie.

- **Crittografia/decrittografia** – Il mittente esegue la crittografia di un messaggio con la chiave pubblica del destinatario.
- **Firma digitale** – Il mittente "firma" un messaggio con la propria chiave privata; la firma è ottenuta applicando un algoritmo crittografico al messaggio o a un piccolo blocco di dati.

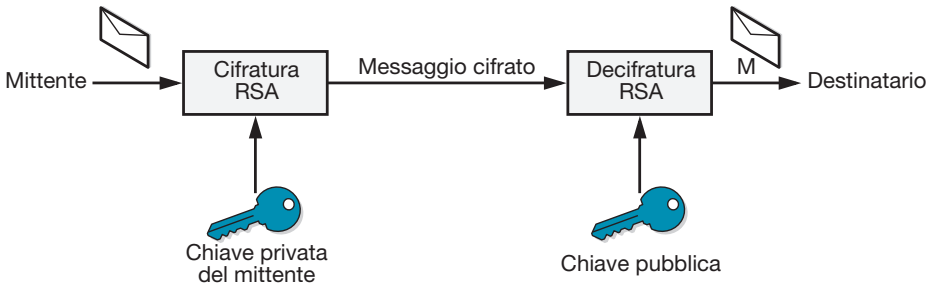
Punto **2)** Il candidato descriva il funzionamento della firma elettronica mediante crittografia a chiave pubblica.

La firma digitale può essere realizzata mediante la crittografia a chiave pubblica, per esempio tramite l'algoritmo RSA, crittografando l'intero messaggio con la chiave privata del mittente, anziché con la chiave pubblica del destinatario (figura seguente).

Il destinatario può decrittografare il messaggio utilizzando la chiave pubblica del mittente: poiché il messaggio è stato crittografato utilizzando la chiave privata del mittente, solo quest'ultimo può aver trasmesso il messaggio (l'intero messaggio crittografato funge pertanto da firma digitale).

In tal caso viene garantita sia la segretezza sia l'autenticazione del messaggio.

Firma elettronica mediante crittografia a chiave pubblica.



Questa metodologia convalida sia l'autore sia il contenuto, ma è molto lenta perché gli algoritmi a chiave pubblica (incluso l'RSA) richiedono lunghi tempi di elaborazione e la firma digitale è realizzata sull'intero messaggio.

Punto **3)** Una sorgente elettromagnetica puntiforme irradia nello spazio circostante uniformemente in tutte le direzioni. Il candidato determini i valori delle ampiezze E_M e H_M del campo elettromagnetico a una distanza $r = 2$ km dalla sorgente, supponendo che la potenza emessa sia $P_0 = 2$ kW e le perdite trascurabili.

Poiché la sorgente elettromagnetica irradia uniformemente in tutte le direzioni, le onde emesse sono di tipo sferico, per cui i relativi fronti d'onda sono formati da superfici sferiche.

La potenza P_0 trasmessa dal radiatore è allora uguale alla densità di potenza S estesa al fronte d'onda a distanza r dalla sorgente, cioè:

$$P_0 = S \cdot 4\pi r^2$$

essendo $4\pi r^2$ l'area del fronte d'onda considerato.

Essendo:

$$S = \frac{1}{2} E_M \cdot H_M$$

in cui:

$$H_M = \frac{E_M}{\eta}$$

si ha:

$$S = \frac{1}{2} \frac{E_M^2}{\eta}$$

Sostituendo tale espressione in quella di P_0 si ottiene:

$$P_0 = 2 \frac{E_M^2}{\eta} \pi r^2$$

dalla quale è possibile ricavare:

$$E_M = \frac{1}{r} \sqrt{\frac{P_0 \cdot \eta}{2\pi}} = \frac{1}{2 \cdot 10^3} \sqrt{\frac{2 \cdot 10^3 \cdot 377}{2\pi}} \cong 0{,}173 \text{ V/m}$$

L'ampiezza del campo magnetico risulta allora:

$$H_M = \frac{E_M}{\eta} = \frac{0{,}173}{377} \cong 4{,}59 \cdot 10^{-4} \text{ A/m}$$