Esame di Stato

In questo capitolo vengono riportati i testi e le soluzioni (proposte) delle seconde prove scritte per la materia di “Sistemi di elaborazione e trasmissione delle informazioni” del corso Sperimentale - progetto "ABACUS" che sono stati somministrati dal Ministero della Pubblica Istruzione come prove per l’Esame di Stato a partire dal 2004.
Le soluzioni sono le stesse che ho formulato allora, quindi risentono, talora, di notazioni, assunzioni e impostazioni in vigore in quegli anni. Con gli stessi criteri vanno valutate le parti di Informatica contenute nelle soluzioni (es. database e esempi di script Web) proposte dal collega prof. Alberto Ferrari.
La qualità delle soluzioni che sono riportate, quando possibile, sono state tarate sulle competenze degli studenti e non degli insegnanti. Lo scopo delle soluzioni è quello di fornire un esempio metodologico dell’applicazione delle nozioni acquisite dal corso di Sistemi e Informatica, anche se, in qualche caso i testi del Ministero non sono del tutto coerenti con il programma del corso: si veda ad esempio la prova del 2006 che si incentra su un servizio di rete troppo peculiare e di fatto non trattato dal corso; oppure dalle prove degli anni 2011 e 2012 che si concentrano eccessivamente su argomenti di Elettronica applicata ripetto ai contenuti del corso di Sistemi.
A questo proposito va fatto notare che le parti di Elettronica (es. acquisizione di I/O), presenti soprattutto nelle ultime versioni delle prove ministeriali, non sono state particolarmente approfondite, pena una improbabile estensione del contenuto della soluzione che, nel caso pratico dell’Esame, lo studente non avrebbe potuto svolgere.

Naturalmente ad oggi (2012) non sono disponibili casi di prove scritte relativamente alla materia di “Sistemi e Reti”.

Tra le risorse OnLine *sono disponibili i testi di tutte le seconde prove ministeriali per Informatica e Informatica Abacus a partire dal 1974.*

A.S. 2003-2004

Testo Esame di Stato 2003-2004

YABC - ESAME DI STATO DI ISTITUTO TECNICO INDUSTRIALE

CORSO SPERIMENTALE - PROGETTO "ABACUS"

Indirizzo: INFORMATICA

Tema di: SISTEMI DI ELABORAZIONE E TRASMISSIONE DELLE INFORMAZIONI

Un istituto scolastico deve partecipare ad un progetto transnazionale che prevede lo scambio di informazioni (materiali didattici, materiali amministrativi, ecc.) via internet e via posta elettronica tra scuole di diversi paesi europei. Prendendo spunto da questa iniziativa, viene pianificata la realizzazione di una rete scolastica che consenta di:
a) collegare ad internet:
• i due laboratori a cui accedono le classi coinvolte nel progetto transnazionale;
• i computer degli uffici, per lo scambio di materiali amministrativi nell'ambito del progetto;
• i computer della presidenza, della vicepresidenza e della biblioteca;
b) creare un archivio centralizzato dei materiali didattici e amministrativi prodotti nell'ambito del _progetto europeo, rendendolo disponibile in rete locale. Si dovrà consentire a tutto il personale della scuola ed a tutti gli studenti la consultazione dei materiali dai computer della rete locale;
c) condividere, solo tra il personale degli uffici e la presidenza, gli archivi amministrativi poiché tali archivi contengono dati riservati.

La dislocazione dei computer è la seguente:
a) due in ciascun ufficio (segreteria didattica, segreteria amministrativa, ufficio personale, ufficio magazzino, ufficio tecnico);
b) quattro nella biblioteca;
c) cinque in ciascuno dei due laboratori;
d) uno sia in presidenza che in vicepresidenza.

Il candidato, dopo aver formulato le necessarie ipotesi aggiuntive, in particolare in merito:
- alla topologia della scuola,
- alla presenza di eventuali reti preesistenti,
- al tipo di accesso alla rete,
- alla tipologia dei computer presenti nella scuola,
- al numero di stampanti da installare,
- alla sicurezza dei dati sensibili,

1. fornisca una soluzione di massima per il progetto della rete scolastica;
2. illustri, in dettaglio, tipologia, struttura e architettura della rete con riferimento ai livelli del modello ISO/OSI.

Durata massima della prova: 6 ore.
E' consentito soltanto l'uso di manuali tecnici e di calcolatrici tascabili non programmabili- Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE

Premessa e ipotesi aggiuntive

L'analisi del testo contiene qualche ambiguità che deve essere ben specificata.
La piu' evidente e' che non è stato specificato quali servizi tale rete deve fornire pubblicamente, pur richiedendo scambio di informazioni pubbliche (dalla frase "progetto transnazionale").
Date le richieste del testo, si decide di rendere i seguenti servizi pubblici tramite la rete:
1. Scambio di documenti del progetto 'transnazionale', documenti in gestione ai due laboratori
2. Sito Web del progetto 'transnazionale', in carico ai due laboratori
3. Scambio di documenti amministrativi del progetto 'transnazionale' a cura degli uffici amministrativi.

Nulla e' specificato per il servizio di posta elettronica, anch'esso necessario per lo scambio di informazioni pubbliche circa il progetto 'transnazionale', pertanto si decide di utilizzare un servizio di posta elettronica gestito dall'esterno e non internamente come i suddetti.

Infine l'accenno ad una eventuale rete preesistente, nella sua vaghezza, è una indicazione che si decide di escludere dallo svolgimento.

Per sufficiente genericità si decide di riferirsi al progetto prescindendo dal sistema operativo server adottato, ovvero dal sistema operativo che gestisce utenti, routing e servizi. Per quanto possibile si daranno indicazioni circa entrambi i sistemi operativi piu' diffusi, Microsoft Windows Server (2000/2003) e Linux.

Per quanto assunto sia dal testo che dalle ipotesi aggiuntive, verrà adottato un modello di rete comprendente una rete locale isolata (TRUST), una rete locale perimetrale (DMZ) e una porzione di rete pubblica (INTERNET) servita da un collegamento DSL flat a 2Mbit/s in ingresso e in uscita.

Progettazione Livelli 1 e 2 OSI

Per quanto riguarda la rete TRUST, vengono immessi in questa rete gli elaboratori degli uffici (in tutto 10, come dal testo), gli elaboratori della Presidenza e Vicepresidenza (2), della Biblioteca (4) e dei due laboratori (10). In tutto 26 calcolatori, ovvero 26 host.
Il livello Fisico e Dati (OSI 1 e 2) delle connessioni viene realizzato in tecnologia Ethernet 802.3u (FastEthernet 10/100/1Gb/s) secondo il modello di rete 'switched'.
Nessun dato prevede tratte superiori ai 90m classici per la portata del mezzo 100BaseT, quindi nessuna assunzione particolare viene fatta in merito.

Vengono considerati i seguenti domini di collisione da mantenere separati tramite switch:
a. Uffici + Presidenza-Vicepresidenza
b. Biblioteca
c. Laboratori
La scelta e' stata fatta in base alla qualita' del traffico circolante sui relativi segmenti di rete locale.

Il dominio a. sarà connesso con 2 switch (in cascata) a 8 porte per i 10 host
Il dominio b. sarà connesso con 1 switch a otto porte per i 4 host
Il dominio c. sarà connesso con 2 switch (in cascata) a 8 porte per i 10 host

Le tre porte di upload dei tre domini convergeranno su uno switch 'stella' (a 8 porte) per ottenere la completa interconnessione delle macchine. Tale switch sara' contenuto in adeguato armadio di commutazione dotato di gruppo di continuità e quanto necessario.

Per quanto riguarda la rete DMZ, la scelta ricade di nuovo su Ethernet 802.3u, con un solo switch a 8 porte. Su questa rete, accessibile pubblicamente, saranno disposte le macchine server di servizi pubblici, come descritto nella premessa.

La porzione di rete pubblica INTERNET invece è costituita dal modem/router DSL che riceve in ingresso dalla rete pubblica geografica il segnale DSL con le caratteristiche offerte dal provider (ISP) e si affaccia sulla rete scolastica tramite una connessione Ethernet 802.3u

Progettazione Livello 3 OSI e Servizi di rete

Le interconnessioni delle tre reti previste dal progetto, TRUST, DMZ e INTERNET, avviene con un router opportunamente dislocato. Per semplicità consideriamo un router costituito da un elaboratore PC con tre interfacce di rete: una sulla rete TRUST, una sulla rete DMZ, una verso la rete INTERNET (cioe' verso il modem DSL).
Il modello di riferimento per il livello 3 e' IP dello stack TCP/IP della rete omonima.

I servizi di Rete necessari per tale progetto sono:
- Servizio di Dominio per consentire l'accesso con autenticazione agli utenti sulla rete
- Servizio DHCP per permettere la configurazione automatica degli host della rete TRUST.
- Servizio di Firewall, per impedire accessi dall'esterno sulla rete TRUST e accessi indesiderati sulla rete DMZ
- Servizio di NAT, in particolare sNAT per consentire agli host della rete TRUST di accedere ai servizi pubblici standard (HTTP, POP3, SMTP, FTP, NNTP)
- Servizio di NAT, in particolare dNAT, per rendere raggiungibili dall'esterno gli host sulla rete DMZ.
- Servizio DNS privato per consentire la risoluzione dei nomi interna alla rete TRUST e DMZ
- Servizio di Condivisione disco e stampanti (NBT) per consentire la condivisione di spazi disco e stampanti all'interno delle reti TRUST e DMZ
- Servizio FTP pubblico (come da premessa)
- Servizio HTTP pubblico (come da premessa)
- Servizio di DNS pubblico per risolvere i nomi pubblici della rete Internet mondiale

Tutti questi servizi saranno dislocati su macchine server individuate sulla rete.

Schema di indirizzamento (livello 3 OSI)

Dati i presupposti, si vengono a determinare due sottoreti isolate (TRUST e DMZ) su cui distribuire un pool di indirizzi.
Viene deciso di usare la classe di indirizzi dedicata alle reti isolate e previste dal modello IP 192.168.0.0 e un subnetting con 4 bit per le sottoreti, sui 16 a disposizione dal modello.
In questo caso la notazione e' 192.168.0.0/20 o netmask 255.255.240.0
Questo modello consente 2^4 subnet differenti, ognuna con 2^12 host indirizzabili (in realtà sarebbero 2^12-2 host indirizzabili, dato che il primo e l'ultimo indirizzo della subnet sono riservati alla subnet stessa e al broadcast).
Lo schema scelto e' ridondante, dato che le subnet reali sono solo 2 (TRUST e DMZ): 14 subnet rimangono inutilizzate.
Assegniamo quindi la subnet 192.168.0.0 alla rete TRUST
Assegniamo poi la subnet 192.168.16.0 alla rete DMZ

La rete TRUST avra' a disposizione quindi gli indirizzi 192.168.0.1 - 192.168.0.254; 192.168.1.1 - 192.168.1.254; 192.168.2.1 - 192.168.2.254; ecc. fino a 192.168.15.1 - 192.168.15.254
In totale: 254*16=4064 indirizzi utilizzabili

La rete DMZ avra' a disposizione quindi gli indirizzi 192.168.16.1 - 192.168.16.254; 192.168.17.1 - 192.168.17.254; 192.168.18.1 - 192.168.18.254; ecc. fino a 192.168.31.1 - 192.168.31.254
In totale: 254*16=4064 indirizzi utilizzabili

(per conferma, verificare che tutti gli indirizzi possibili della rete TRUST in AND con la netmask danno sempre 192.168.0.0, mentre tutti gli indirizzi possibili per la rete DMZ in AND con la netmask danno come risultato 192.168.16.0)

Dislocazione dei servizi e routing (livello 7 e 3 OSI)

Per una corretta e bilanciata dislocazione dei servizi è necessario aggiungere al progetto almeno tre macchine server:
a. un server router (SR) con interfacce sulle reti TRUST, DMZ e INTERNET
b. un server locale di sistema (PDC) con interfaccia sulla rete TRUST
c. un server pubblico di servizio (SP) con interfaccia sulla rete DMZ

A questo punto si possono dislocare i servizi elencati precedentemente.

Sul server SR saranno collocati: Routing, Firewall, NAT, eventuale Proxy
Questo server deve:
1. fare sNAT per tutte le macchine in TRUST e in DMZ
2. fare dNAT per le macchine su DMZ
3. bloccare il traffico proveniente dall'esterno e verso la TRUST
4. controllare il traffico proveniente dall'esterno e verso DMZ
5. consentire il traffico tra TRUST e DMZ
6. DNS

Sul server PDC sono collocati i servizi:
1. DHCP per la distribuzione delle configurazioni livello 3 degli host sulla rete TRUST
2. Dominio, per l'autenticazione degli utenti e delle macchine

3. DNS privato, per risolvere i nomi delle reti TRUST e DMZ

Sul server SP devono essere collocati i servizi:
1. FTP, per consentire lo scambio pubblico dei documenti del progetto 'transnazionale"
2. HTTP, per gestire un sito a servizio del progetto 'transnazionale'

I servizi NBT (NetBios) per spazio disco e condivisioni stampanti è disponibile su tutte le macchine con opportuna impostazione dei diritti di accesso forniti dal Dominio.

Si osserva che i tre server dovrebbero essere duplicati, per questioni di fault tolerance (i loro servizi devono sempre essere disponibili). Inoltre i loro indirizzi locali dovranno essere impostati manualmente (statici).

Configurazioni di rete (livello 3 OSI)

Gli host della rete TRUST avranno la seguente configurazione, ottenuta via DHCP:
Indirizzo IP: come da schema
Default Gateway: indirizzo IP della macchina SR (sulla sua interfaccia in TRUST)
DNS: indirizzo IP della macchina PDC

Gli host della rete DMZ avranno la seguente configurazione (statica):
Indirizzo IP: come da schema
Default Gateway: indirizzo IP della macchina SR (sulla sua interfaccia in DMZ)
DNS: indirizzo IP della macchina SR (sulla sua interfaccia in DMZ)

Consultare lo schema per un esempio numerico, compresi gli indirizzi pubblici ottenuti dall'ISP e opportunamente distribuiti con dNAT sugli host della rete DMZ.

Risposte ai quesiti

I punti 1. e 2. contenuti nel testo sono stati affrontati nello svolgimento.
Dei punti esplicitamente ricordati, invece, rimangono esclusi:
- presenza di eventuali reti preesistenti
- numero di stampanti da installare
- sicurezza dati sensibili

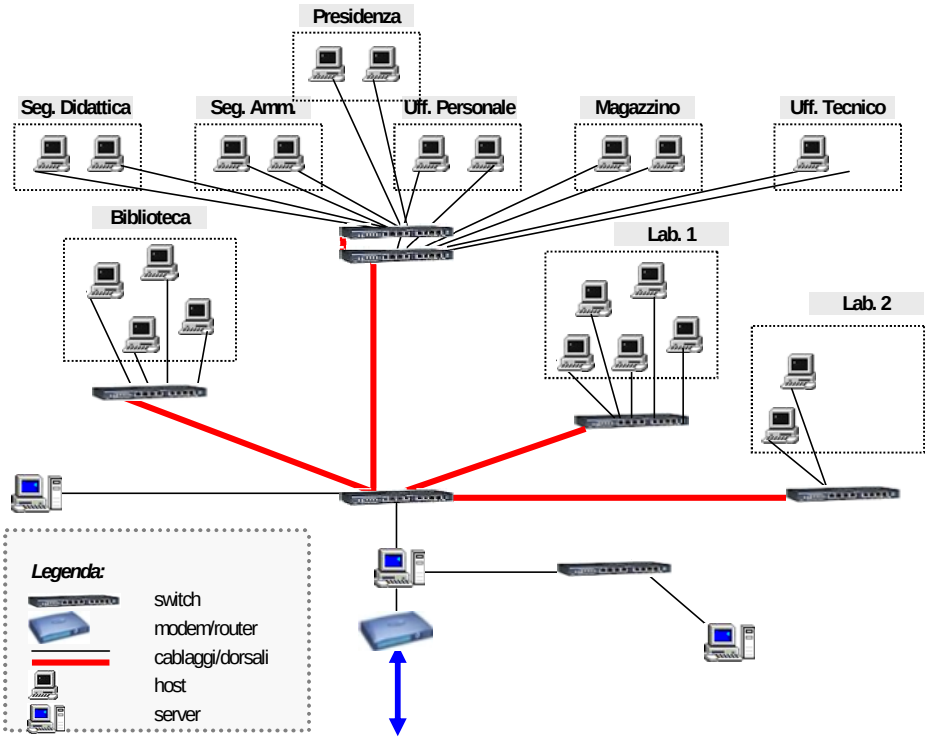
Per quanto riguarda la "presenza di eventuali reti preesistenti", data la vaghezza, non è possibile una risposta esauriente.
Nello schema proposto si potrebbe considerare una serie di host generici presenti nella scuola, magari distribuiti sui vari laboratori. Essi farebbero parte della rete TRUST e ne condividerebbero le scelte, sempre considerando di separare i domini di collisione opportunamente (magari tra i vari laboratori).
Lo schema degli indirizzi non cambierebbe (con piu' di 4000 indirizzi a disposizione il problema non sussiste). Eventualmente si potrebbero individuare macchine Server di servizi interni, come ad esempio server Dati (SQL Server o analoghi) presso i quali accedere dasi vari client per esigenze didattiche o altro ancora.

Per quanto riguarda il "numero di stampanti da installare" si puo' affermare che il quesito è debole: tante quante ne servono, con opportune condivisioni NBT.

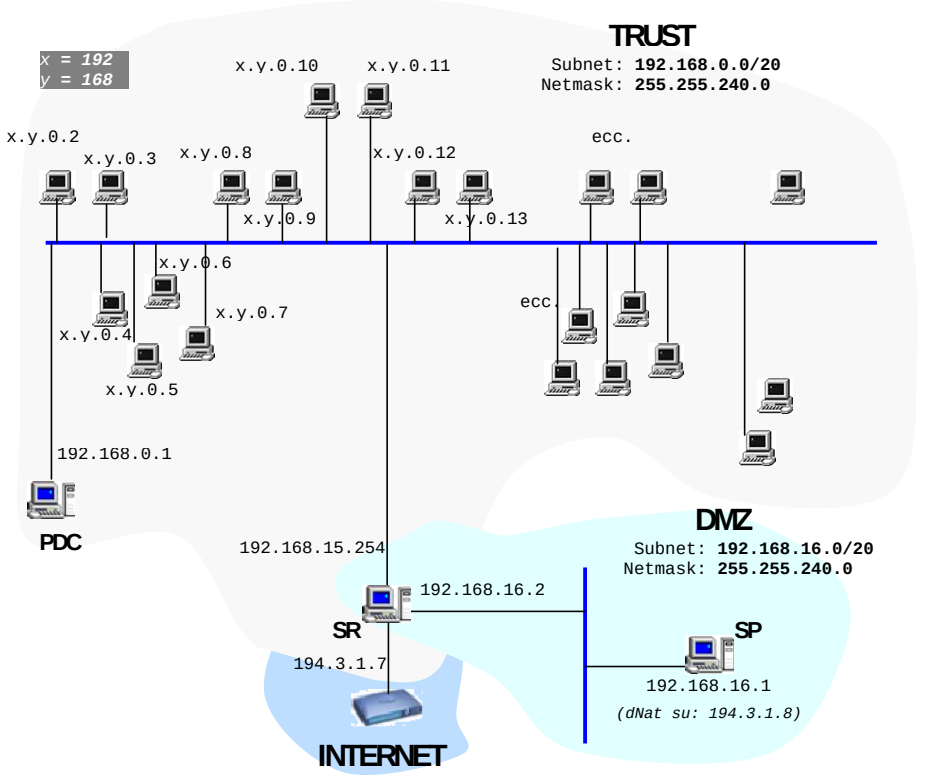
Infine per quanto riguarda i "dati sensibili" è necessario che i documenti che li contengono siano protetti all'accesso e consultabili solo dagli utenti del dominio autorizzati. Sarà cura dell'Amministratore della rete (e del Dominio) concedere i diritti d'accesso opportuni per la protezioni di tali informazioni, utilizzando i servizi già presenti nel Sistema Operativo adottato.

Schemi

Schema cablaggio strutturato



Schema topologia e indirizzamento



A.S. 2005-2006

Testo Esame di Stato 2005-2006

YABC - ESAME DI STATO DI ISTITUTO TECNICO INDUSTRIALE

CORSO SPERIMENTALE - PROGETTO "ABACUS"

Indirizzo: INFORMATICA

Tema di: SISTEMI DI ELABORAZIONE E TRASMISSIONE DELLE INFORMAZIONI

II candidato svolga, a sua scelta, uno dei due temi proposti ([NB]).

Tema n. 1

L'editore di un quotidiano locale che insiste sul territorio di una piccola provincia, decide di offrire ai suoi lettori alcuni nuovi servizi on-line.
In particolare:

1. vuole pubblicare su un sito appositamente registrato la versione on-line del giornale, inserendo gli articoli piu importanti dell' edizione cartacea del giorno, con una eventuale fotografia inerente alla notizia;
2. vuole realizzare una web-radio attiva a partire dallo stesso sito, per la diffusione di notizie, approfondimenti, musica, eventi on-line.

Il candidato, formulate le ipotesi aggiuntive e/o semplificative che ritiene necessarie:

a) proponga e illustri un primo progetto di massima del sistema hardware/software che comporti la installazione del server web presso la redazione;

b) proponga e illustri un secondo progetto di massima del sistema che comporti l'utilizzo di apparecchiature in hosting presso un provider ISP;

c) illustri i pro e i contro di ciascuna delle due soluzioni proposte al punto a) e b);

d) proponga e motivi la soluzione eventualmente mista che a suo parere meglio si adatta alle richieste dell'editore;

e) illustri il progetto organizzativo necessario al mantenimento del sistema proposto al punto d).

Durata massima della prova: 6 ore.

E' consentito soltanto l'uso di manuali tecnici e di calcolatrici tascabili non programmabili-

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

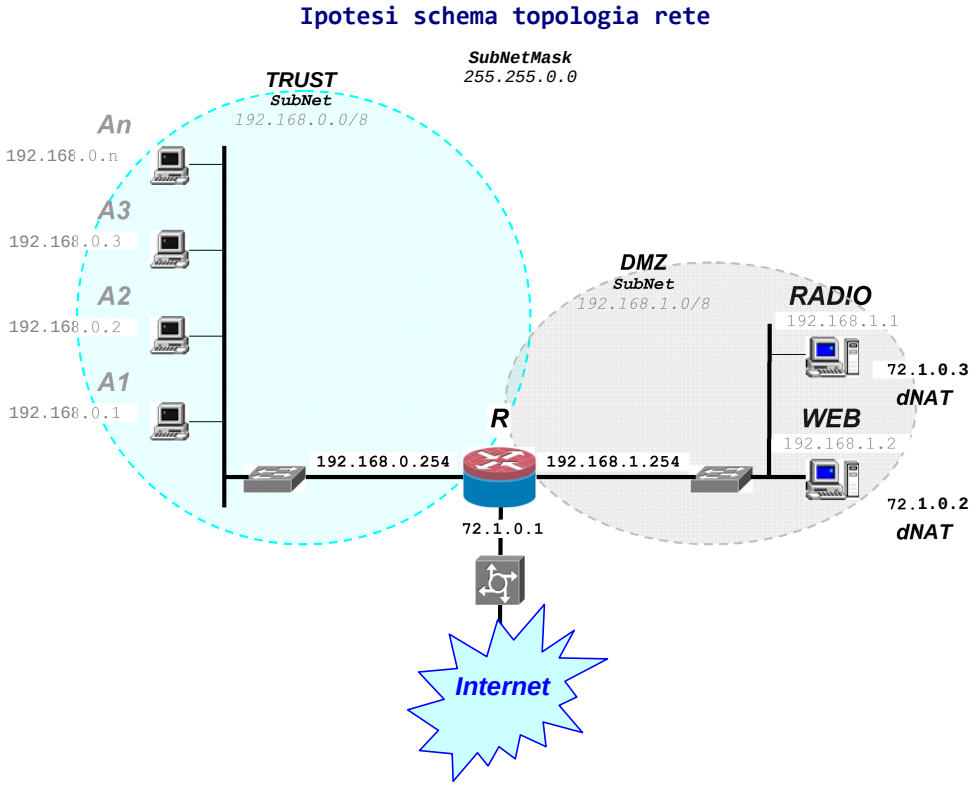
(***NB***) *Il secondo tema proposto è di carattere Elettronico e quindi viene tralasciato*

SOLUZIONE

Premessa e ipotesi aggiuntive

L'analisi del testo sembra richiedere soprattutto valutazioni: sulla realizzazione di un server Web (per la versione on-line del quotidiano) e di un server streaming audio (per la radio del quotidiano). Non vengono fatte assunzioni sulla rete che dovrà ospitare i due servizi, quindi in proposito va fatta una ipotesi di lavoro.

Si assume perciò che la rete del quotidiano sia una classica TRUST/DMZ; nel segmento DMZ andranno posti i due server (Web e Radio):



Si nota la collocazione di un firewall/routing R che potrebbe anche ospitare praticamente tutti i server di base per la rete: DHCP su TRUST, DNS privato, NAT o proxy per l'http dei client su TRUST, ecc...
In particolare andranno configurati i due server sulla DMZ con un DNAT per fare in modo che i rispettivi servizi (Web e radio) siano accessibili dalla rete pubblica.
Si suppone inoltre che la rete abbia un hostname pubblico (es. *www.quotidianoXYZ.it*) in modo, ad esempio, da consentire l'accesso diretto al server Web del Quotidiano xyz.
Per quanto riguarda il server Radio, bisogna prevedere che il tipo di connessione alla rete pubblica tramite ISP abbia una larghezza di banda sufficiente per 'servire' varie connessioni streaming che, di per se', sono abbastanza onerose rispetto alle connessioni Web, dato che devono sopportare flussi di dati in tempo reale. Per esempio, l'audio di tipo mp3 occupa una banda sull'ordine delle decine di kbit/s, anche centinaia di kbit/s.
Queste considerazioni saranno importanti per valutare se collocare il server Radio all'interno della rete della radio locale o su server esterni.

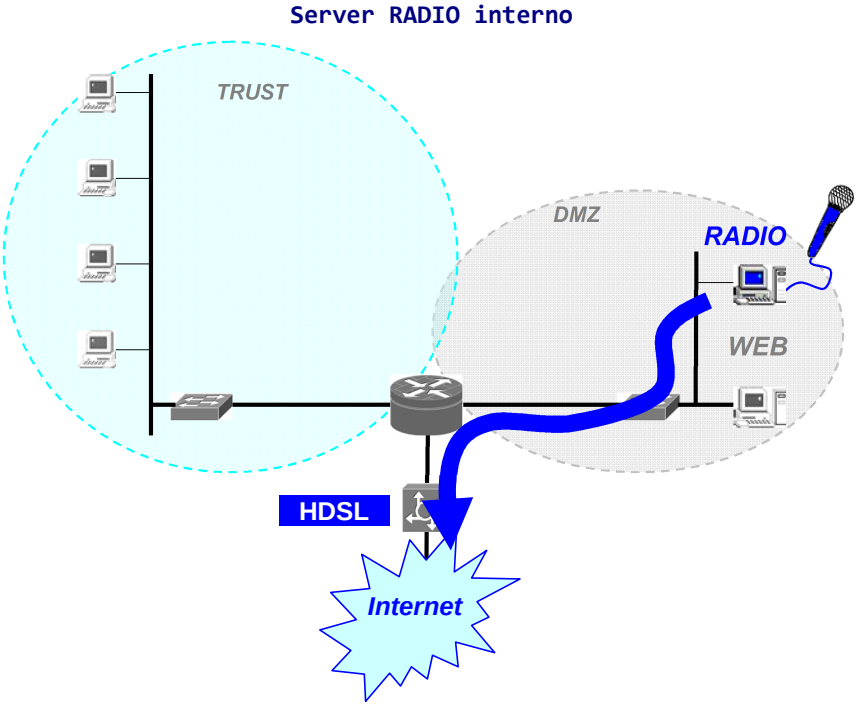
Server Web

La progettazione del server Web che fornisca i contenuti del quotidiano tramite un sito interno da far accedere pubblicamente si baserà sull'installazione e la configurazione di un server Web classico, quindi o Microsoft IIS o Apache Web Server (in questo secondo caso, multipiattaforma). In questo caso è abbastanza interessante valutare l'uso del recente pacchetto XAMPP, che riunisce in sé vari applicativi satelliti di Apache Web Server (compreso un modulo per l'accesso a database) e che è multipiattaforma.
Il server Web fornirà il suo servizio agli utenti tramite la porta TCP 80 e quindi il firewall dovrà essere configurato per lasciar correre il traffico esterno verso la DMZ.
I contenuti del sito, in continuo aggiornamento (almeno una volta al giorno) saranno modificati da qualche macchina client della rete, anche della rete TRUST. A questo proposito potrebbe essere interessante sperimentare un sistema CMS per realizzare il sito Web del quotidiano, affinchè la gestione dei contenuti risulti accessibile e gestibile anche da personale non specificatamente tecnico.

Server Radio

In effetti la realizzazione di un server di streaming non è un tipico argomento del corso del quinto anno, pertanto si può provare a riportare qualche valutazione sulla base delle nozioni di programmazione TCP/IP e realizzazione di programmi client/server.

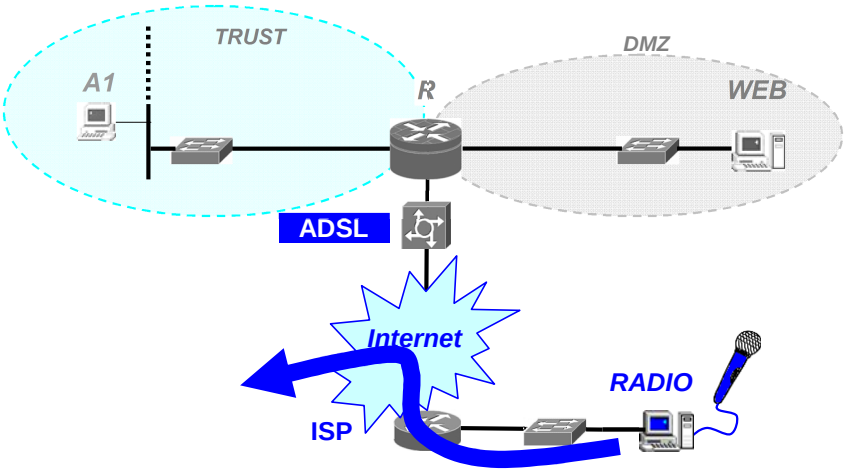
Allo stato attuale, ad esempio, tra i client più diffusi per accedere a server che trasmettono streaming audio come radio o canali musicali, bisogna ricordare il software WinAmp come software multipiattaforma, o Windows Media Player come software proprietario. In particolare, dal menù di WinAmp si desume che ne esista una versione o un pacchetto integrativo in grado di realizzare anche un server Audio WinAmp (e quindi anche utilizzabile come server 'radio').
In ogni caso un server Radio dovrebbe essere, presumibilmente, basato su UDP e, come già indicato nelle premesse, dovrebbe essere supportato da una connessione alla rete pubblica abbastanza veloce, almeno tale da supportare una sufficiente quantità di utenti connessi contemporaneamente.
Inoltre un server radio dovrebbe essere dotato di un hardware di periferica specializzato, come una scheda audio professionale dotata di mixer e multicanale, per esempio per acquisire contemporaneamente da più fonti come un flusso audio musicale e vari flussi audio vocale contemporaneamente.
Potrebbe essere interessante proporre qualche ipotesi sul carico dei flussi di dati in upload verso la rete pubblica (gli utenti connessi alla web radio), direzione normalmente meno considerata dai fornitori di servizio di transito.
Per esempio, una linea ADSL classica fornisce, ad oggi, una banda di upload tipica che si aggira sui 256 Kbit/s (nella migliore delle ipotesi). Ipotizzando un singolo flusso audio a 32 Kbit/s (come un mp3 di media qualità), gli utenti connessi contemporaneamente al server Radio risulterebbero 256/32=8, sempre che la banda di upload sia sempre disponibile sul suo valore massimo, cosa non sempre vera con le tipologie di contratto ADSL. E' evidente che 8 utenti contemporanei non sarebbero sufficienti per un servizio accettabile, pertanto la soluzione ADSL risulta impraticabile per un server Radio interno alla rete del Quotidiano xyz. In questo caso si dovrà optare per una connessione di tipo HDSL con banda upload garantita. Ad esempio, se la banda HDSL fosse 1 Mbit/s, si potrebbero avere una trentina di utenti contemporanei. In ogni caso la soluzione 'interna' del server Radio appare abbastanza improbabile.



Hosting

La soluzione accennata nel testo consiste nel collocare il servizio radio online presso un server esterno, magari collocato sulla rete dell'ISP che fornisce la connessione alla rete del Quotidiano xyz.
L'ipotesi risolverebbe, presumibilmente, il problema della larghezza di banda necessaria al servizio e, magari, anche una certa scalabilità nell'investimento dell'hardware necessario al server Radio. Di contro il Quotidiano xyz dovrebbe corrispondere un canone supplementare per il servizio di hosting. Logisticamente, però, la soluzione presenta un problema piuttosto complesso: una parte della redazione del Quotidiano xyz dovrebbe stabilirsi presso un'altra sede, praticamente nei locali in cui il server Radio verrebbe ospitato dall'ISP. I contenuti del servizio, infatti, essendo in tempo reale, non consentono una produzione remota accettabile.
Per quanto riguarda l'hosting del sito Web, invece, non sussistono particolari controindicazioni. L'unica valutazione rimane se dotare il personale di conoscenza tecnica necessaria per sviluppare il sito internamente e dotare la rete del Quotidiano xyz delle strutture informatiche già discusse, oppure risparmiare l'investimento interno e pagare un canone per l'hosting del sito. In questo secondo caso dovrà essere gestito un sistema di aggiornamento dei contenuti dalla sede del quotidiano all'ISP basato su FTP (in modo economico) o su pacchetti dedicati forniti dall'ISP (modo meno economico).

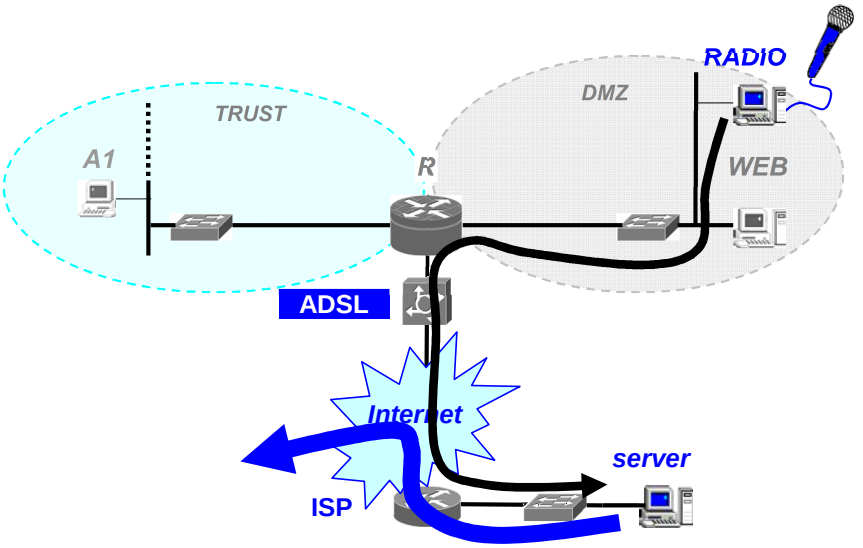
Server RADIO in hosting



Soluzione mista

In effetti la soluzione mista riguarda il servizio critico del server Radio, dato che l'hosting del sito Web o la sua gestione interna sono questioni relativamente semplici da attuare e sostanzialmente equivalenti.
Come soluzione mista per il server Radio si potrebbe optare per la gestione dei contenuti streaming interna, con la produzione del flusso radio attraverso un server interno come descritto in precedenza, ma con la diffusione del servizio tramite ISP specializzato. La presenza di numerose radio online, infatti, ha prodotto vari server pubblici disposti a diffondere un segnale audio ricevuto da una sorgente che, in questo caso, sarebbe la sede del Quotidiano xyx. In questo modo verrebbe superato il problema della larghezza di banda pubblica necessaria alla rete del Quotidiano xyz, dato che si tratterebbe dell'invio in tempo reale di un unico flusso audio verso il server esterno. Contemporaneamente si avrebbe che la redazione del Quotidiano xyz rimarebbe compatta su una unica sede, cosa che è auspicabile anche da un punto di vista dei costi.

Server RADIO misto



A.S. 2007-2008

Testo Esame di Stato 2007-2008

YABC - ESAME DI STATO DI ISTITUTO TECNICO INDUSTRIALE

Indirizzo: INFORMATICA

CORSO SPERIMENTALE - PROGETTO "ABACUS"

Tema di: SISTEMI DI ELABORAZIONE E TRASMISSIONE DELLE INFORMAZIONI

Il proprietario di una catena di supermercati intende aprire dieci nuovi punti di vendita.
La sede centrale comprende uffici e due magazzini collegati mediante una rete locale.
Ciascun punto di vendita dovrà disporre di un magazzino attiguo per lo stoccaggio delle merci; l'approvvigionamento verrà effettuato con richieste dirette alla sede centrale.
Gli uffici si occupano dei rapporti con i punti vendita e con i magazzini (verifica delle giacenze, evasione degli ordini, ...). La base di dati deve consentire la memorizzazione delle informazioni relative alle vendite e agli ordini dei prodotti dei vari punti vendita, che devono potersi interfacciare con la sede centrale; allo stesso modo i clienti devono poter visualizzare i cataloghi dei prodotti i corrispondenti listini per poter eventualmente acquistare via web.

Il candidato, fatte le opportune ipotesi aggiuntive,

1. proponga uno schema generale del sistema che metta in evidenza le diverse funzioni
2. scelga la tipologia di rete che ritiene più idonea, ne indichi le sue caratteristiche e progetti in dettaglio alcune sue parti
3. analizzi e progetti uno schema concettuale e il corrispondente schema logico del data base della sede centrale
4. proponga una soluzione per la gestione via web dell'interfaccia con i punti vendita al dettaglio, oppure, a scelta, con i clienti
5. illustri le metodologie di collaudo
6. effettui un'analisi massima dei costi

Durata massima della prova: 6 ore.

E' consentito soltanto l'uso di manuali tecnici e di calcolatrici tascabili non programmabili-

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE

Premessa e ipotesi aggiuntive

L'analisi del testo contiene una richiesta implicita che aggiunge una caratteristica ad una tipica organizzazione di rete isolata privata con interfaccia pubblica: la connessione di host remoti alla LAN isolata, i "dieci punti vendita". Questi dieci host, per come sono descritti, devono usufruire dei servizi standard della rete isolata privata, ma non si trovano all'interno della rete privata. La soluzione obbligata è la gestione di una **VPN** (Virtual Private Network) che consenta ai dieci punti vendita di accedere alla LAN privata attraverso la rete pubblica.

Un'altra parte del testo che non è del tutto implementabile in questa sede riguarda la richiesta 6. A questo quesito sarà risposto in termine meno generici possibile, dato che l'analisi dei costi non è un argomento specificatamente trattato nel programma scolastico.

Siccome poi non sono richiesti specifici servizi di rete relativi all'organizzazione descritta, saranno indicati solo quelli ritenuti necessari (scartando, ad esempio, un servizio di posta elettronica gestito internamente).

Per sufficiente genericità si decide di riferirsi al progetto prescindendo dal sistema operativo server adottato, ovvero dal sistema operativo che gestisce utenti, routing e servizi. Per quanto possibile si daranno indicazioni circa entrambi i sistemi operativi piu' diffusi, Microsoft Windows Server (2000/2003 e successivi) e Linux.

Per quanto assunto sia dal testo che dalle ipotesi aggiuntive, nella sede centrale verrà adottato un modello di rete comprendente una rete locale isolata (TRUST), una rete locale perimetrale (DMZ) e una porzione di rete pubblica (INTERNET) servita da un collegamento HDSL flat a 1Mbit/s in ingresso e in uscita, con tre indirizzi pubblici rilasciati dall'ISP (es. 82.13.0.1, 82.13.0.2, 82.13.0.3).
Si ipotizzano presenti sulla rete TRUST gli uffici (es. 5) e i due magazzini.
Si ipotizzano sulla rete DMZ un server WEB e, su tutte tre le reti un server router R che ospiterà il server VPN.

Su ogni punto vendita si prevede una LAN con una interfaccia su rete pubblica di tipo ADSL (con IP su rete pubblica dinamico), un router con client VPN, Internet e LAN (collocato nel punto vendita) e un host collocato sulla LAN (magazzino del punto vendita).

Progettazione Livelli 1 e 2 OSI

Sede centrale

Per quanto riguarda la rete TRUST, vengono immessi in questa rete un totale di 5+2=7 host (uffici e magazzini).
Il livello Fisico e Dati (OSI 1 e 2) delle connessioni viene realizzato in tecnologia Ethernet 802.3u (FastEthernet 10/100/1Gb/s) secondo il modello di rete a stella 'switched'.
Nessun dato prevede tratte superiori ai 90m classici per la portata del mezzo 100BaseT, quindi nessuna assunzione particolare viene fatta in merito.
E' sufficiente un dominio di collisione e quindi un solo switch a 16 o 24 porte (considerando che ad esso dovrà connettersi anche il router R ed eventuali macchine temporanee come portatili o eventuali access point per WI-FI in questo caso non considerati come necessari).

Per quanto riguarda la rete DMZ, la scelta ricade di nuovo su Ethernet 802.3u, con un solo switch a 8 porte. Su questa rete, accessibile pubblicamente, saranno disposte la macchina router e la macchina server WEB.

La porzione di rete pubblica INTERNET invece è costituita da uno switch/router HDSL a 8 porte, che riceve in ingresso dalla rete pubblica geografica il segnale DSL con le caratteristiche offerte dal provider (ISP) e sul quale si collocheranno il Router R e il server WEB.

Tutti questi apparati di livello 1-2 (due switch e il router) potrebbero essere installati in uno stesso armadio di commutazione dotato di gruppo di continuità e quanto necessario, se le distanze materiali tra la sezione TRUST sono inferiori ai classici 90m supportati da Ethernet XBaseT.

Lan remota (un Ufficio vendite qualsiasi)

In questo caso è sufficiente un solo switch (es. a 8 porte), sempre su tecnologia Ethernet 802.3u su cui collocare il Server VPN (punto vendita), l'host (magazzino) e il modem ADSL.
Come prima, il tutto potrebbe essere inglobato in apposito armadio dotato di gruppo di continuità e quant'altro.

Progettazione Livello 3 OSI e Servizi di rete

Le interconnessioni delle tre reti previste dal progetto, TRUST, DMZ e INTERNET, compresa la VPN, avviene con un router R opportunamente dislocato.
Per semplicità consideriamo un router costituito da un elaboratore PC con tre interfacce fisiche di rete: una sulla rete TRUST, una sulla rete DMZ, una verso la rete INTERNET.
Il modello di riferimento per il livello 3 e' IP dello stack TCP/IP della rete omonima.

I servizi di Rete necessari per tale progetto sono:
- Servizio di Dominio per consentire l'accesso con autenticazione agli utenti sulla rete
- Servizio DHCP per permettere la configurazione automatica degli host della rete TRUST.
- Servizio di Firewall, per impedire accessi dall'esterno sulla rete TRUST e accessi indesiderati sulla rete DMZ
- Servizio di NAT, in particolare sNAT per consentire agli host della rete TRUST di accedere ai servizi pubblici standard (HTTP, POP3, SMTP, FTP, NNTP)
- Servizio di NAT, in particolare dNAT, per rendere raggiungibili dall'esterno host pubblici sulla rete DMZ.
- Servizio DNS privato per consentire la risoluzione dei nomi interna alla rete TRUST e DMZ
- Servizio di Condivisione disco e stampanti (NBT) per consentire la condivisione di spazi disco e stampanti all'interno delle reti TRUST e DMZ

• Servizio HTTP pubblico (come da premessa)
• Servizio di DNS pubblico per risolvere i nomi pubblici della rete Internet mondiale
• Servizio **VPN** pubblico per consentire agli host remoti di diventare host sulla rete TRUST

Tutti questi servizi saranno dislocati su macchine server individuate sulla rete.

Schema di indirizzamento (livello 3 OSI)

Dati i presupposti, si vengono a determinare due sottoreti isolate (TRUST e DMZ) su cui distribuire un pool di indirizzi. Viene deciso di usare la classe di indirizzi dedicata alle reti isolate e previste dal modello IP 192.168.0.0 e un subnetting con 4 bit per le sottoreti, sui 16 a disposizione dal modello.
In questo caso la notazione e' 192.168.0.0/20 o subnetmask 255.255.240.0
Questo modello consente 2^4 subnet differenti, ognuna con 2^12 host indirizzabili (in realtà sarebbero 2^12-2 host indirizzabili, dato che il primo e l'ultimo indirizzo della subnet sono riservati alla subnet stessa e al broadcast).
Lo schema scelto e' ridondante, dato che le subnet reali sono solo 2 (TRUST e DMZ): 14 subnet rimangono inutilizzate.
Assegniamo quindi la subnet 192.168.0.0 alla rete TRUST
Assegniamo poi la subnet 192.168.16.0 alla rete DMZ

La rete **TRUST** avra' a disposizione quindi gli indirizzi 192.168.0.1 - 192.168.0.255; 192.168.1.0 - 192.168.1.255; 192.168.2.0 - 192.168.2.255; ecc. fino a 192.168.15.0 - 192.168.15.254
In totale: 254*16=4064 indirizzi utilizzabili

Nome di rete: 192.168.0.0
Nome del broadcast: 192.168.15.255
Subnetmask: 255.255.240.0

La rete **DMZ** avra' a disposizione quindi gli indirizzi 192.168.16.1 - 192.168.16.255; 192.168.17.0 - 192.168.17.255; 192.168.18.0 - 192.168.18.255; ecc. fino a 192.168.31.0 - 192.168.31.254
In totale: 254*16=4064 indirizzi utilizzabili
Nome di rete: 192.168.16.0
Nome del broadcast: 192.168.31.255
Subnetmask: 255.255.240.0

Per quanto riguarda la VPN lato server, si decide di assegnare ad ogni connessione entrante un indirizzo IP appartenente alla rete TRUST, cosicchè anche gli host client adotteranno indirizzi locali appartenenti alla rete TRUST (cioè 192.168.0.0).
Anche in questo caso lo schema è ridondante, avendo a disposizione più di 4000 indirizzi utili).

Sulla **LAN remota** (punti vendita) si decide di assegnare un indirizzamento sempre appartenente al gruppo 192.168.0.0/20 con identica subnetmask ma id di sottorete 240, ovvero la rete 192.168.240.0.
Essa avrà a disposizione 4064 indirizzi, da 192.168.240.1 - 192.168.240.255; 192.168.241.0 - 192.168.241.255; ecc. fino a 192.168.255.0 - 192.168.255.254
In totale: 254*16=4064 indirizzi utilizzabili
Nome di rete: 192.168.240.0
Nome del broadcast: 192.168.255.255
Subnetmask: 255.255.240.0

Dislocazione dei servizi e routing (livello 7 e 3 OSI)

Per una corretta e bilanciata dislocazione dei servizi è necessario aggiungere al progetto almeno una macchina server che faccia da PDC (Domain Controller); nel caso, prevedere il servizio anche duplicato su una seconda macchina della rete.
A questo punto si possono dislocare i servizi elencati precedentemente.

Sul server **R** saranno collocati: Routing, Firewall, NAT, eventuale Proxy e server VPN. Questo server deve:
1. fare sNAT per tutte le macchine in TRUST
2. bloccare il traffico proveniente dall'esterno e verso la TRUST
3. controllare il traffico proveniente dall'esterno e verso DMZ
4. consentire il traffico tra TRUST e DMZ
5. DNS pubblico
6. Server VPN, accettando le connessioni client VPN

Sul server **PDC** sono collocati i servizi:

1. DHCP per la distribuzione delle configurazioni livello 3 degli host sulla rete TRUST
2. Dominio, per l'autenticazione degli utenti e delle macchine
3. DNS privato, per risolvere i nomi delle reti TRUST e DMZ

Sul server **WEB** devono essere collocati i servizi:
1. HTTP, per gestire il sito a servizio delle vendite su Web
2. Server SQL
3. Eventuale DC secondario e DNS pubblico e privato

I servizi NBT (NetBios) per spazio disco e condivisioni stampanti è disponibile su tutte le macchine con opportuna impostazione dei diritti di accesso forniti dal Dominio.
Gli indirizzi IP delle interfacce delle macchine R e WEB dovranno essere esclusi dal DHCP e impostati manualmente.

Sulla **LAN remota** possiamo adottare uno schema di rete WORKGROUP e non a dominio.
La macchina Gateway, che effettua la connessione ADSL, dovrà ospitare il server VPN e consentire l'aggregamento alla LAN centrale.
Data la scarsa numerosità degli host (due soli) si può optare per configurazioni TCP/IP statiche senza usare DHCP.
Come sopra, i servizi NBT (NetBios) per spazio disco e condivisioni stampanti è disponibile su tutte le macchine con opportuna impostazione dei diritti di accesso forniti dal modello Workgroup.

Si noti come l'host di magazzino non possa associarsi alla LAN centrale. I dati in esso presenti saranno gestiti dalla Macchina Gateway che si connette con la VPN.

Configurazioni di rete (livello 3 OSI)

Gli host della rete **TRUST** avranno la seguente configurazione, ottenuta via DHCP:
Indirizzo IP: come da schema
Subnet Mask: come da schema
Default Gateway: indirizzo IP della macchina R (sulla sua interfaccia in TRUST)
DNS: indirizzo IP della macchina PDC

Gli host della rete **DMZ** avranno la seguente configurazione (statica):
Indirizzo IP: come da schema
Subnet Mask: come da schema
Default Gateway: indirizzo IP della macchina R (sulla sua interfaccia in DMZ)
DNS: indirizzo IP della macchina R (sulla sua interfaccia in DMZ)

Consultare lo schema per un esempio numerico, compresi gli indirizzi pubblici ottenuti dall'ISP e opportunamente distribuiti con dNAT sugli host della rete DMZ.

Per la **Rete remota** invece, avremo:
- Gateway **VPN**:
Indirizzo IP: statico, come da schema
Subnet Mask: come da schema
Default Gateway: fornito dall'ISP in fase di connessione
DNS: fornito dall'ISP in fase di connessione

Indirizzo IP su interfaccia **VPN**: acquisito come da schema LAN centrale, così come gli altri parametri (Gateway e DNS).

- **Host** (magazzino):
Indirizzo IP: statico, come da schema
Subnet Mask: come da schema
Default Gateway: Indirizzo IP del Router
DNS: Indirizzo IP del Router

Configurazione Tcp/Ip, Routing e Firewalling

Come esemplificazione, si riporta la configurazione e la tabella di routing di un host su Trust e del Router R nella rete della Sede:

Host **U1**

```
Indirizzo IP:  192.168.0.1
Subnet Mask:  255.255.240.0
Gateway predefinito: 192.168.15.254
```

Indirizzo	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	192.168.15.254	192.168.0.1	1 (pacchetti stranieri)
192.168.0.0	255.255.240.0	(192.168.0.1)	192.168.0.1	1 (sulla rete di provenienza)
192.168.15.255	255.255.255.255	(192.168.0.1)	192.168.0.1	1 (broadcast di rete)

(si tralasciano il loopback e gli altri broadcast)

Router **R**

```
Indirizzo IP:  192.168.15.254    (TRUST)
Subnet Mask:  255.255.240.0
Gateway predefinito: -

Indirizzo IP:  192.168.31.254    (DMZ)
Subnet Mask:  255.255.240.0
Gateway predefinito: -

Indirizzo IP:  82.13.0.1       (Internet)
Net Mask:  255.0.0.0
Gateway predefinito: 82.13.0.254     (ricevuto dall'ISP)
```

Indirizzo	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	82.13.0.254	82.13.0.1	1 (pacchetti stranieri)
192.168.0.0	255.255.240.0	-	192.168.15.254	1 (sulla rete di provenienza)
192.168.16.0	255.255.240.0	-	192.168.31.254	1 (sulla rete di provenienza)
192.168.15.255	255.255.255.255	-	192.168.15.254	1 (broadcast su Trust)
192.168.31.255	255.255.255.255	-	192.168.31.254	1 (broadcast su DMZ)

(si tralasciano il loopback e gli altri broadcast)

Sul router R possiamo implementare le seguenti ACL per il Firewall:

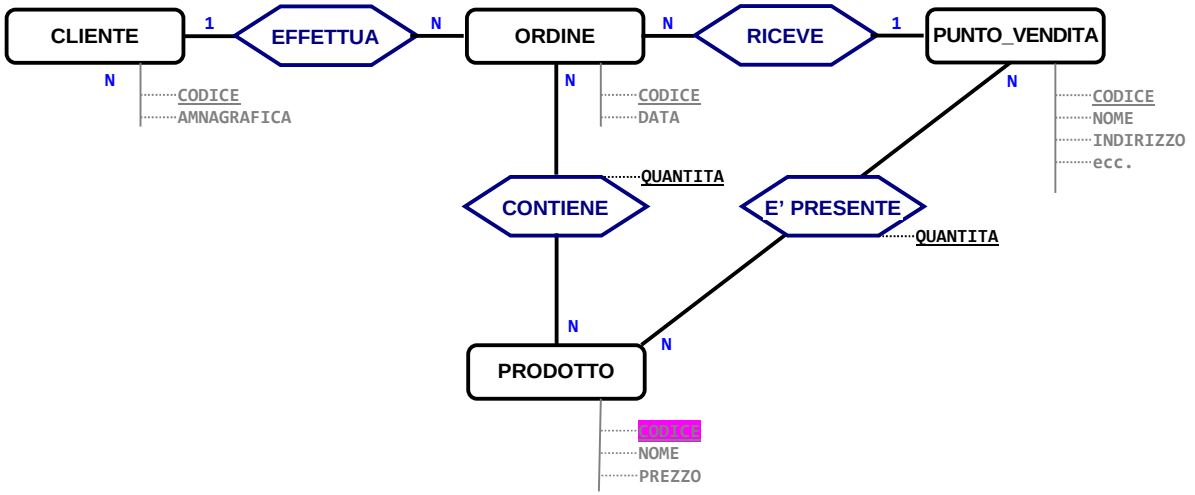
regola	permit/deny	liv 3-4	Interfaccia1	Interfaccia2	liv 5-6-7	direzione
ACL1	permit	any	192.168.15.254	192.168.31.254	eq any	in/out
ACL2	permit	tcp	192.168.15.254	82.13.0.1	eq HTTP	out
ACL3	permit	tcp	192.168.15.254	82.13.0.1	eq DNS	out
ACL4	permit	tcp	82.13.0.1	192.168.15.254	eq HTTP	out
ACL5	permit	tcp	82.13.0.1	192.168.15.254	eq DNS	out

Tutto ciò che non è permesso (permit), viene automaticamente negato (deny).
Si considera Interfaccia1 come soggetto di in/out, cioe' una direzione in significa che Interfaccia1 è server (se TCP).
Commento:
ACL1 consente tutto il traffico Tcp/Ip tra Trust e DMZ
ACL2 consente tutto il traffico client HTTP da Trust a Internet (richieste dei client Trust)
ACL3 consente tutto il traffico client DNS da Trust a Internet (richieste dei client Trust)
ACL4 consente tutto il traffico server HTTP da Internet a Trust (risposte ai client Trust)
ACL5 consente tutto il traffico server DNS da Internet a Trust (risposte ai client Trust)

Interfaccia WEB per vendita al dettaglio

Si è deciso di implementare la vendita al dettaglio tramite server Web e relativo codice HTML/ASP (o Php) sulla macchina WEB della sede centrale.
Un utente di rete pubblica, accedendo a tale sito, avrà a disposizione una serie di pagine web che lo guideranno alla consultazione dei listini e alla fase di ordine e pagamento.
La gestione della vendita effettiva, una volta ricevuto l'ordine dalla sede centrale, sarà distribuito tramite la VPN sulla sede più appropriata.

La base di dati in appoggio alla richiesta sarà sviluppata tramite server SQL installato sulla macchina WEB.
Lo schema di soluzione concettuale della base di dati da gestire è il seguente:



La proposta è un diagramma entità/associazioni (E/R) che realizza appunto lo schema concettuale.
Lettura dello schema:

- Un cliente effettua uno o più ordini – Un ordine è effettuato da un solo cliente (associazione 1:N)
- Un punto vendita riceve uno o più ordini – Un ordine è ricevuto in un solo punto vendita (associazione 1:N)
- Un prodotto è presente in uno o più punti vendita – In un punto vendita sono presenti uno o più prodotti (associazione N:N)
- Un ordine contiene uno o più prodotti – Un prodotto è presente in uno o più ordini (associazione N:N)

Non vengono definite parzialità o totalità delle associazioni per non appesantire il tutto.
Viene poi richiesto di passare allo schema logico equivalente (schema relazionale):

Cliente (**Codice**, anagrafica)
Ordine (**Codice**, data, evaso, ***codice_cliente***, ***codice_punto_vendita***)
Punto_Vendita (**Codice**, nome, indirizzo)
Prodotto (**Codice**, nome, prezzo)
Contiene(***Codice_ordine***, ***codice_prodotto***, quantità) [rappresenta le righe d'ordine]
E'Presente(***Codice_punto_vendita***, ***codice_prodotto***, quantità)

In grassetto le chiavi primarie, in grassetto corsivo le chiavi esterne.

Codice SQL e PHP

Creazione delle tabelle (script SQL):

```
CREATE TABLE 'Cliente' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Anagrafica' varchar(100) NOT NULL,
  PRIMARY KEY ('Codice')
) ;
CREATE TABLE 'Contiene' (
  'Codice_ordine' bigint(20) NOT NULL,
  'Codice_prodotto' bigint(20) NOT NULL,
  'Quantità' decimal(10,0) NOT NULL,
  KEY 'Codice_ordine' ('Codice_ordine','Codice_prodotto')
);
CREATE TABLE 'E_presente' (
  'Codice_punto_vendita' bigint(20) NOT NULL,
  'Codice_prodotto' bigint(20) NOT NULL,
  'Quantità' decimal(10,0) NOT NULL,
  KEY 'Codice_punto_vendita' ('Codice_punto_vendita','Codice_prodotto'),
  KEY 'Codice_prodotto' ('Codice_prodotto')
);
CREATE TABLE 'Ordine' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Data' date NOT NULL,
  'Evaso' char(1) NOT NULL,
  'Codice_cliente' bigint(20) NOT NULL,
```

```
  'Codice_punto_vendita' bigint(20) NOT NULL,
  PRIMARY KEY ('Codice'),
  KEY 'Codice_cliente' ('Codice_cliente','Codice_punto_vendita'),
  KEY 'Codice_punto_vendita' ('Codice_punto_vendita')
);
CREATE TABLE 'Prodotto' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Nome' varchar(50) NOT NULL,
  'Prezzo' decimal(10,0) NOT NULL,
  PRIMARY KEY ('Codice')
);
CREATE TABLE 'Punto_Vendita' (
  'Codice' bigint(20) NOT NULL AUTO_INCREMENT,
  'Nome' varchar(30) NOT NULL,
  'Indirizzo' varchar(100) NOT NULL,
  PRIMARY KEY ('Codice')
);
```

Codice Associazioni tra le tabelle (script SQL)

```
ALTER TABLE ‘Contiene’
  ADD CONSTRAINT ‘Contiene_Ordine’ FOREIGN KEY (‘Codice_ordine’) REFERENCES ‘Ordine’ (‘Codice’);

ALTER TABLE ‘E_presente’
  ADD CONSTRAINT ‘E_presente_prodotto’ FOREIGN KEY (‘Codice_prodotto’) REFERENCES ‘Prodotto’ (‘Codice’),
  ADD CONSTRAINT ‘E_presente_punto_vendita’ FOREIGN KEY (‘Codice_punto_vendita’) REFERENCES ‘Punto_Vendita’ (‘Codice’);

ALTER TABLE ‘Ordine’
  ADD CONSTRAINT ‘Ordine_punto_vendita’ FOREIGN KEY (‘Codice_punto_vendita’) REFERENCES ‘Punto_Vendita’ (‘Codice’),
  ADD CONSTRAINT ‘Ordine_cliente’ FOREIGN KEY (‘Codice_cliente’) REFERENCES ‘Cliente’ (‘Codice’);
```

Per la gestione via web dell’interfaccia con i punti vendita si realizza un sito web di consultazione dei prodotti e per l’effettuazione degli ordini da parte dei clienti.
Per semplificare la trattazione presentiamo qui il codice di una pagina PHP che recupera le informazioni dal database (si ipotizza un database MySQL) e visualizza l’elenco dei prodotti.

```
<html>
<head>
<title>Visualizzazione Prodotti</title>
</head>
<body>
<?php
$host = "localhost";
$user="esame";
$password="stato";
$connect = mysql_connect($host,$user,$password) or die("Impossibile connettersi all'host");
if(mysql_select_db("supermercati",$connect)==0)
{
 echo("Il database non esiste");
 exit;
}
$sql="SELECT * FROM Prodotto";
$result = mysql_query($sql);
if(mysql_num_rows($result)!=0)
{
 echo "<table border='1'>
 <tr> <th>Codice</th>
 <th>Nome del Prodotto</th>
 <th>Prezzo</th>
 </tr>";
 while($row = mysql_fetch_array($result))
 {
  echo "<tr>";
```

```
  echo "<td>" . $row["Codice"] . "</td>";
  echo "<td>" . $row["Nome"] . "</td>";
  echo "<td>" . $row["Prezzo"] . "</td>";
  echo "</tr>";
 }
 echo "</table>";
}
else
 echo("Nessun Prodotto disponibile ...");
?>
</body>
</html>
```

Risposte ai quesiti

I punti 1. 2. 3. e 4. presenti nel testo sono stati affrontati nello svolgimento.
Dei punti esplicitamente ricordati, invece, rimangono esclusi:
- Metodologie di collaudo
- Analisi dei costi

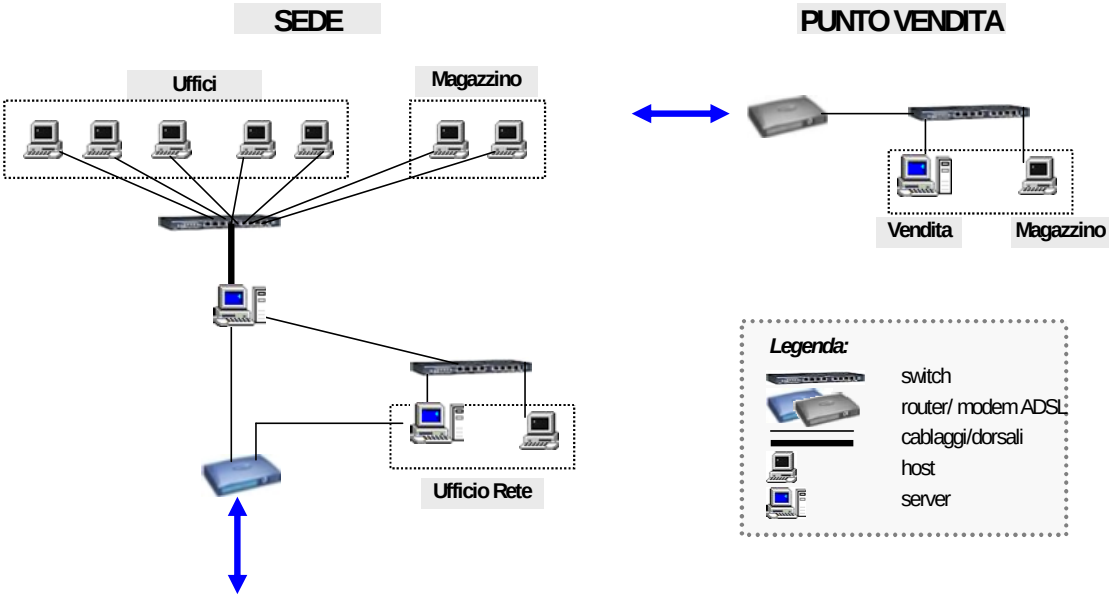
Si sorvola sul collaudo dei sistemi operativi adottati, che si suppongono installati a dovere (in particolare la versione Server sulle due macchine della rete principale che ospitano i Domain Controller).
Il collaudo si concentrera' soprattutto sulla correttezza dell'impostazione della rete, sia locale sia pubblica, sia nella sede centrale che nelle sedi periferiche.
In caso di piattaforma Microsoft, il funzionamento del livello fisico è possibile anche senza aver installato applicativi e pianificato indirizzi IP, tramite i protocolli di default forniti di livello 1 e 2 dal sistema operativo.
Una volta pianificati gli indirizzi IP, si collauderà la raggiungibilità delle stazioni (comando ping) utilizzando i semplici indirizzi IP ed effettuando il collaudo da tutte le macchine significative verso tutte le macchine significative.
Quindi si verificherà la risoluzione degli indirizzi tramite DNS, prima interno poi pubblico, sempre utilizzando il comando ping (stavolta con i nomi stringa delle macchine locali e poi con url noti di rete pubblica).
Infine, con il comando tracert (o equivalente) si verificheranno i percorsi dei pacchetti per verificare gli instradamenti.
Le tabelle di routing degli host possono essere verificate con il comando route print, mentre possono essere gestite sui router (inserimento e cancellazione di regole) con le opzioni del comando route.

Per verificare il funzionamento della VPN si usa un modo analogo (comando ping) una volta che un client VPN ha accettato una connessione entrante. In questo caso il test si presenta meno agevole; sarebbe opportuno effettuarlo tramite una macchina pubblica a cui accedere, dalla rete principale, tramite un applicativo di controllo di desktop remoto.

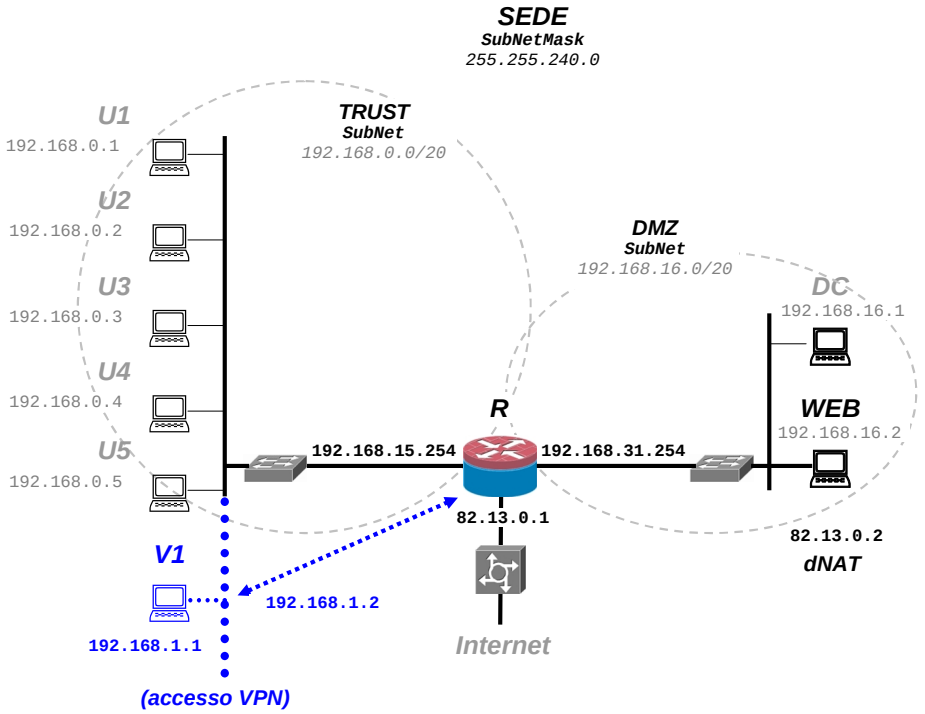
L'analisi dei costi viene esplicitamente tralasciata, dato che non si tratta di una competenza acquisibile in sede scolastica, ne' prevista dai programmi curricolari.

Schemi

Schema cablaggio strutturato



Schema topologia e indirizzamento



A.S. 2010-2011

Testo Esame di Stato 2010-2011

YABC - ESAME DI STATO DI ISTITUTO TECNICO INDUSTRIALE

Indirizzo: INFORMATICA

CORSO SPERIMENTALE - PROGETTO "ABACUS"

Tema di: SISTEMI DI ELABORAZIONE E TRASMISSIONE DELLE INFORMAZIONI

I recenti eventi sismici e le conseguenze catastrofiche spingono gli Enti e le Amministrazioni Locali alla ricerca di ulteriori soluzioni in grado di diffondere nel modo più rapido possibile le informazioni raccolte dai vari punti di rilevamento (PR) presenti sul territorio.
Ciascun punto di rilevamento acquisisce i segnali provenienti dalle centraline provviste di sismografi, li elabora, li converte in formato digitale e li invia al centro elaborazione dati della Protezione Civile.

In particolare

- La rilevazione è continua, ad intervalli di 1 minuto, per tutti i giorni dell'anno
- Il segnale digitalizzato (onda sismica in scala Richter) viene integrato con le seguenti informazioni: identificativo della centralina (dal quale sarà possibile risalire al luogo di rilevazione), identificativo del sismografo, data e ora
- Il sistema informativo centrale acquisisce e memorizza, ogni 5 minuti, i dati relativi da tutte le centraline dislocate sull'intero territorio, quindi invia sulle Protezione Civile i rapportisulla valutazione di rischio di sisma nelle diverse regioni monitorate ed eventuali messaggi di allerta

.
Il candidato, fatte le opportune ipotesi aggiuntive,

1. analizzi il problema e proponga uno schema generale del sistema
2. scelga la tipologia di rete che ritiene più idonea, ne indichi le sue caratteristiche e progetti in dettaglio alcune sue parti
3. analizzi e progetti uno schema concettuale e il corrispondente schema logico del data base della sede centrale
4. proponga una soluzione per la gestione via web dell'interfaccia con i punti di rilevazione.

Durata massima della prova: 6 ore.

E' consentito soltanto l'uso di manuali tecnici e di calcolatrici tascabili non programmabili-

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE

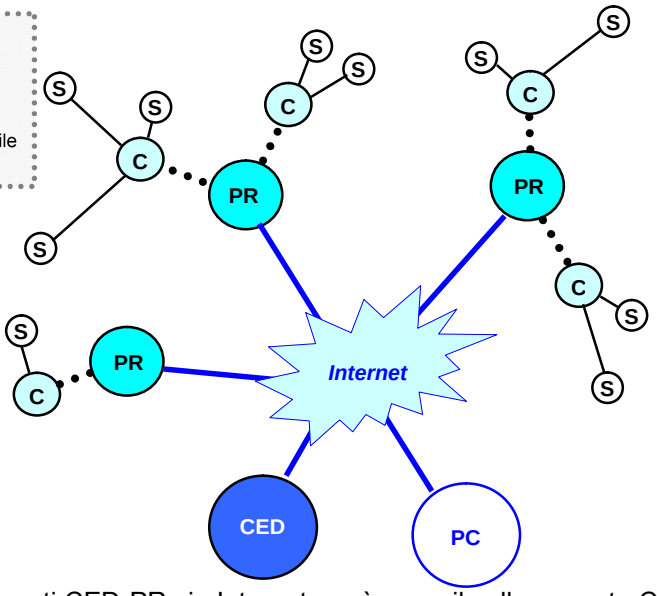
Premessa e ipotesi aggiuntive

L'analisi del testo comporta uno schema progettuale piuttosto complesso.
Gli elementi descritti nella traccia sono i seguenti: sismografi (S), centraline (C), punti di rilevamento (PR), centro elaborazione dati della Protezione Civile (CED). Viene inoltre citata la Protezione Civile (PC), come entità di sola consultazione dati.

Usando la seguente simbologia, lo schema che lega questi elementi risulta il seguente (tratteggiati i collegamenti wireless):

legenda:

S = sismografo
C = centralina
PR = punto di rilevamento
CED = centro elaborazione dati della Protezione Civile
PC = Protezione Civile



Risulta evidente che la rete coinvolta nei collegamenti CED-PR sia Internet, così come il collegamento CED-PC. Si deduce che o i collegamenti PR-C o i collegamenti C-S devono essere wireless, altrimenti avremmo sismografi poco significativi perche' troppo ravvicinati geograficamente.
Ipotizziamo quindi che i collegamenti PR-C siano wireless, mentre i collegamenti C-S cablati.

Nota: *In ogni caso più sismografi cablati su una centralina non hanno molto senso (troppo ravvicinati), cosicche' sarebbe meglio ipotizzare un sismografo per centralina. Lasciamo comunque l'ipotesi del testo, che prevede piu' sismografi per centralina*

• **Per le centraline C**
si ipotizza di utilizzare un modulo di acquisizione di I/O analogico/digitale per acquisire i dati dai sismografi S, integrato con un modulo Modem Dati GPRS per superare la tratta wireless verso il punto di rilevamento PR.
Il firmware/software sul modulo si occuperà di rilevare in tempo reale i dati dei sismografi, preparare il pacchetto e inviarlo tramite il modem dati GPRS al punto di rilevamento PR.

• **Per il punto di rilevamento PR**
si prevede un Personal Computer dotato di **n** moduli Modem Dati GPRS (per n centraline C) e una connessione a Internet. Un programma dedicato server Tcp/Ip che, oltre a gestire le n connessioni sui modem dati (via protocollo seriale con memorizza in locale dei dati), stia in attesa delle richieste Tcp/Ip sulla connessione Internet da parte del CED.
Non si prevede un server Web a bordo di queste stazioni PR, contrariamente a quanto alluso nel testo, per la eccessiva difficoltà di gestione di numerosi server http sparsi sul territorio nelle macchine PR, potendo centralizzare, con programma dedicato, tutte le informazioni sul centro di elaborazione dati CED.

• **Per il centro di elaborazione dati CED**
si prevede un Server connesso ad Internet, dotato di un programma dedicato Client Tcp/Ip che gestisce le **m** connessioni verso i punti di rilevamento PR, richiedendo i dati. Tali dati saranno memorizzati in un database server del CED stesso. Inoltre deve ospitare un Server http per rispondere alle richieste dei browser della protezione civile PC.

Progettazione Livelli OSI

Centralina C

• Livello 1 Fisico
Connessione wireless realizzata con modem Dati GPRS, larghezza di banda 64kbit/s equivalente ad un modem analogico tradizionale, piu' che sufficiente per la larghezza di banda dei dati da gestire.
Considerando di cifrare un valore della scala Richter con 4 byte (codici Ascii di formato XX.X), e di registrare un valore al secondo per un massimo di 10 sismografi per centralina, abbiamo la seguente ampiezza di banda dati:
10 x 4 byte al secondo, ovvero 40 x 8 bit al secondo, ovvero 320 b/s, del tutto compatibile con la larghezza di banda scelta.

- Livello 2 DataLink
  Normalmente realizzato su interfaccia seriale Rs232 e relativo protocollo, con comandi AT per il modem
- Livello 3 Network
  Nulla, essendo una connessione punto-punto.
- Livello 4 Trasporto
  Nulla, essendo una connessione punto-punto e prevedendo un protocollo dedicato a livello 7
- Livello 7 Applicazione
  Pacchetto dati da 246 byte, generato automaticamente ogni minuto per ogni sismografo S, di formato:
  IDS (1 byte), identificativo numerico del sismografo (da 0 a 255)
  DATAORA (5 byte, AAMMGGOOMM)
  RICTHER (240 byte), valore scala Richter (da 00.0 a 99.0) rilevato dai sensori ogni secondo.

Punto di rilevazione PR

Sulla rete verso le centraline C:
- n livelli 1,2 e 7 simmetrici a quelli della centralina C

Sulla rete Internet verso il CED:
- Livello 1 Fisico
  Modem Adsl
- Livello 2 datalink
  PPPOE
- Livello 3 Network
  Ip, con indirizzo IP dinamico
- Livello 4 Trasporto
  Tcp Server, su porta dedicata (es. 8221).
- Livello 7 Applicazione
  Programma dedicato Server Tcp/Ip in attesa di connessione da parte del CED, con pacchetto dati da inviare su richiesta (e memorizzato localmente in un database, es. MsAccess):
  IDPR (2 byte), id. del Punto di Rilevamento
  IDC (10 byte), id. della centralina C (es. numero SIM)
  IDS come sopra
  DATAORA come sopra
  RICTHER come sopra

Centro elaborazione Dati CED

- Livello 1 Fisico
  Modem Hdsl, per poter gestire una buona larghezza di banda proveniente dai PR
- Livello 2 datalink
  PPPOE (o PPPOA)
- Livello 3 Network
  Ip, con indirizzo IP statico
- Livello 4 Trasporto
  Tcp, su porta dedicata (vedi Livello 4 di PR) e http su porta 80
- Livello 7 Applicazione
  Programma dedicato Client Tcp/Ip che si connette alla parte Server Tcp/Ip sui punti di rilevamento PR sulle porte impostate, e che richiede pacchetti uguali a quelli descritti. Salvataggio su database server (es. MySQL o SQL Server)
  Server http (IIS o Apache) per rispondere alle richieste dei browser della Protezione Civile PC, prelevando dati dal database server

Dettaglio livelli 7 (Applicazione)

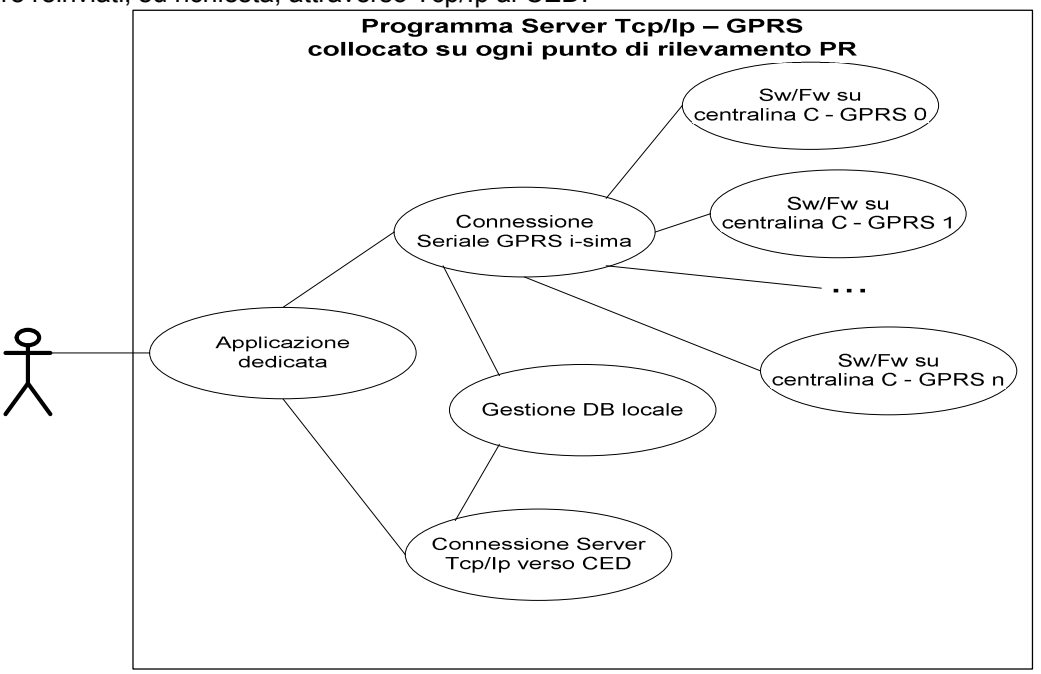
I livelli 7 qualificanti del progetto sono:
a. Programma Server Tcp/Ip collocato su ogni punto di rilevamento PR
b. Programma Client Tcp/Ip collocato sul centro di elaborazione dati CED
c. Server Web collocato sul centro di elaborazione dati CED

Viene esclusa l'analisi del software/firmware a bordo delle centraline C, che ipotizziamo essere in grado di trasmettere su modem GPRS wireless le informazioni descritte tratte dai sismografi S attraverso opportuni canali di acquisizione analogico/digitali di I/O.

Questo flusso viene generalmente gestito tramite protocollo Rs232 implementato sul modem GPRS.

a. Programma Server Tcp/Ip collocato su ogni punto di rilevamento PR

Questo software deve ricevere i dati dei sismografi S - raccolti a loro volta dalle centraline C – implementando una connessione remota su modem GPRS, presumibilmente realizzata su protocollo seriale Rs232. Dovrà quindi essere in grado di connettersi via GPRS a n centraline C (con n numeri di telefono su SIM dati).
Contemporaneamente deve essere in grado di programmare un socket Tcp/Ip in modalità server, in attesa di connessione (da parte del centro di elaborazione dati CED) e fornire i dati dei sismografi S su richiesta. Per questo motivo si prevede un database locale su cui memorizzare temporaneamente i dati ricevuti dai modem GPRS in attesa di essere reinviati, su richiesta, attraverso Tcp/Ip al CED.



Pseudocodice Connessione seriale GPRS (i-sima)

Impostazione
- Impostazione porta seriale con protocollo (es. 115200,N,8,1)
- Comandi AT per il Modem (compresa composizione numero della SIM i-sima)
- Impostazione routine Send (su porta seriale)
- Impostazione routine Receive (su porta seriale)

Routine Send
- Richiesta dati (con un pacchetto di un solo byte, es. ‘S’)

Routine Receive
- Salvataggio sul DB Locale del pacchetto ricevuto

Pseudocodice Connessione Server Tcp/Ip

Impostazione
- Nuovo socket server
- EndPoint del socket server (IP: any; TCP: 8221)
- Associazione dell’EndPoint sul socket (Bind)
- Avvio metodo Listen sul socket
- Impostazione routine Accept

Routine Accept
- Impostazione routine Receive

Routine Receive
- Lettura DB locale
- Avvio routine Send

Routine Send
- Trasmissione dei pacchetti descritti, a partire dai record letti sul Db Locale

Pseudocodice Gestione DB Locale

Scrittura di un record (ricevuto via GPRS)

- Connessione al DB, es. `New SqlConnection("data source = DBSISMOGRAFI.MDF”)`
- Stringa SQL di inserimento record, es. `insert into dbsismografi(IDPR, IDC, IDS, DATAORA, RICHTER) values (1, 0, 0, “1101011200”, “00.010.010.10…1”)`
- Esecuzione comando SQL, es. ExecuteQuery()

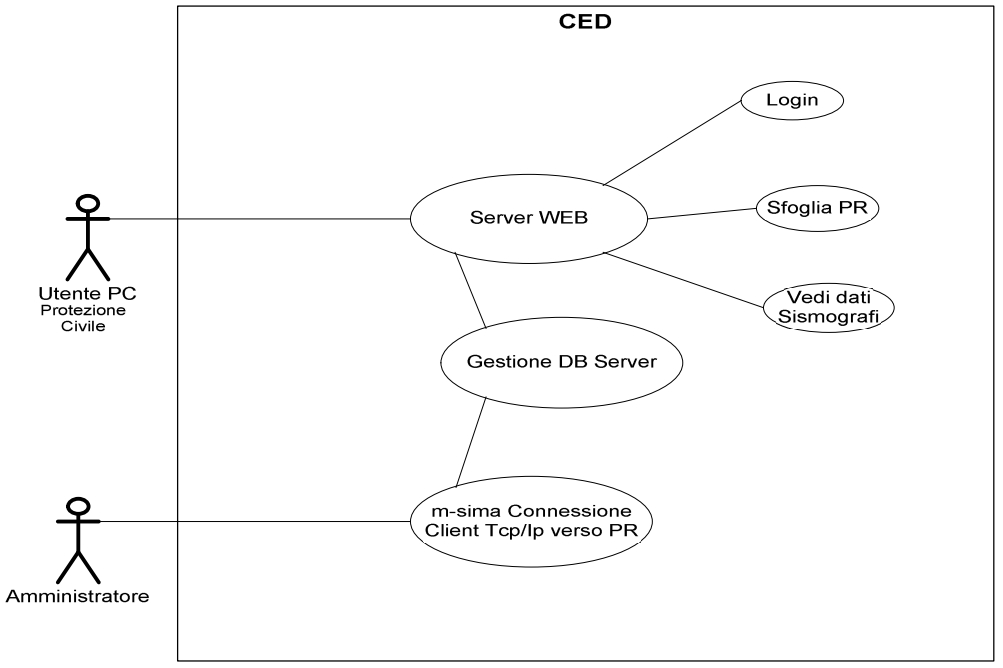
Lettura dei record (da spedire via Tcp/Ip)
- Connessione al DB, es. `New SqlConnection("data source = DBSISMOGRAFI.MDF”)`
- Stringa SQL per leggere tutti i record, es. `select * from dbsismografi order by dataora`
- Esecuzione comando SQL, es. `ExecuteQuery()`
- Eliminazione dei record trasferiti, es. `delete from dbsismografi`

• Esecuzione comando SQL, es. `ExecuteQuery()`

Per gli altri livelli Applicazione, esponiamo solo i casi d’uso:

b. Programma Client Tcp/Ip collocato sul centro di elaborazione dati CED

c. Server Web collocato sul centro di elaborazione dati CED



NB. La m-sima Connessione Client Tcp/Ip verso PR potrebbe agire ogni 5 minuti, come richiesto dal testo, tramite un timer dedicato.

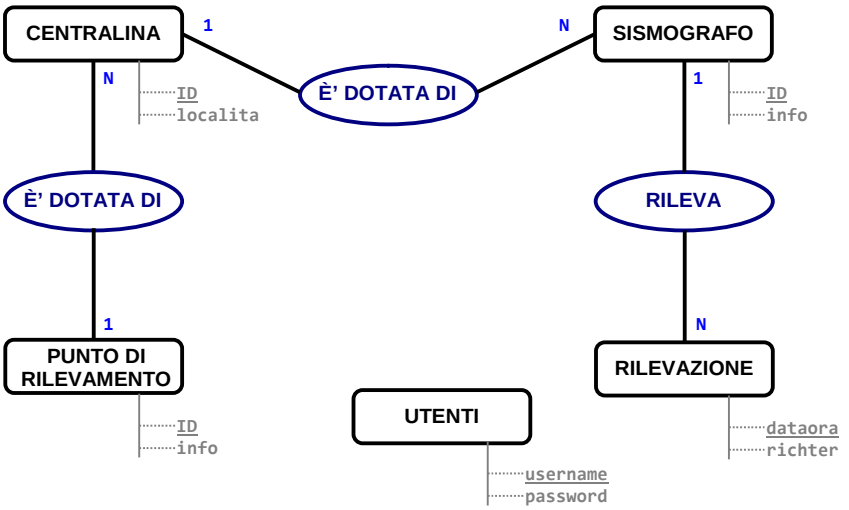
Schema concettuale e logico del DB sul Centro Elaborazione Dati (CED)

Le informazioni fondamentali che devono essere memorizzate nella base di dati sono le rilevazioni (onda sismica in scala Richter) che vengono effettuate dai sismografi associati a centraline distribuite nei luoghi di rilevazione.

Dall’analisi dei dati proponiamo quindi un’organizzazione in 4 entità:
• Rilevazione
• Sismografo
• Centralina
• Punto di rilevamento

Le entità sono in relazione fra loro facendo riferimento alle seguenti ipotesi:
• Ogni rilevazione è relativa ad un solo sismografo
• Ogni sismografo è collegato ad una sola centralina
• Ogni centralina è posizionata in un solo punto di rilevamento

Oltre ai dati relativi ai rilevamenti dei sismografi nel database devono essere memorizzate anche le informazioni che permetteranno l'accesso ai soli utenti autorizzati. Per questo motivo introduciamo l'entità utenti in cui memorizzare username e password di accesso.



Entità

- Punto di rilevamento con due attributi
  - ID chiave primaria
  - ulteriori informazioni (luogo ecc).
- Centralina con due attributi
  - ID della centralina come chiave primaria e la sua località.
- Sismografo con due attributi
  - ID del sismografo
  - ulteriori informazioni.
- Rilevazione con due attributi
  - Data e l'ora della rilevazione.
  - Grado in scala Richter del rilevamento.
- Utenti con due attributi
  - Nome utente.
  - Password.

Per semplificare la trattazione non abbiamo approfondito le "ulteriori informazioni" che potrebbero essere associate alle varie entità in quanto non sembrano particolarmente rilevanti per la proposta di soluzione.

Associazioni

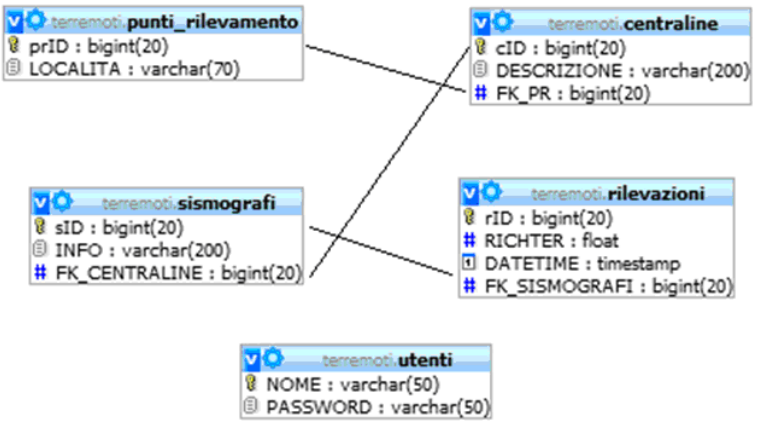
Abbiamo tre associazioni fra le entità:

- L'associazione 1:N tra le entità Punto di rilevamento e Centralina.
- L'associazione 1:N tra le entità Centralina e Sismografo.
- L'associazione 1:N tra le entità Sismografo e Rilevazione

L'entità Utente serve per registrare gli utenti che possono avere l'accesso alla pagina web per eseguire alcune operazioni.

Lettura dello schema:

- Un punto di rilevamento ha collegate di più centraline, mentre una centralina ha un solo punto di rilevamento.
- Una centralina è dotata di più sismografi, un sismografo invece è collegato a una sola centralina.
- Un sismografo effettua più rilevazioni, mentre una rilevazione viene effettuata da un solo sismografo.



Dal modello concettuale ricaviamo quello relazionale che è formato da 5 tabelle. Per implementare le 3 associazioni 1:N occorre inserire le chiavi esterne.

• Nella tabella Rilevazioni FK_SISMOGRAFI è un riferimento alla chiave sID della tabella Sismografi.
• Nella tabella Sismografi abbiamo la chiave esterna FK_CENTRALINE che è un riferimento alla chiave cID della tabella Centraline.
• Nella tabella Centraline è presente la chiave esterna FK_PR che si riferisce alla chiave prID della tabella Punti_rilevamento

Codice

Per la creazione del DB si propone il seguente script SQL:

```
CREATE DATABASE terremoti;
USE terremoti;
CREATE TABLE punti_rilevamento (
   prID bigint(20) NOT NULL AUTO_INCREMENT,
 LOCALITA varchar(70),
   PRIMARY KEY (prID)
);

CREATE TABLE centraline (
  cID bigint(20) NOT NULL AUTO_INCREMENT,
  DESCRIZIONE varchar(200) NOT NULL,
  FK_PR bigint(20) NOT NULL,
  FOREIGN KEY (FK_PR) REFERENCES punti_rilevamento(prID),
  PRIMARY KEY (cID)
);

CREATE TABLE rilevazioni (
  rID bigint(20) NOT NULL AUTO_INCREMENT,
  RICHTER float NOT NULL,
  DATETIME timestamp NOT NULL,
  FK_SISMOGRAFI bigint(20) NOT NULL,
  PRIMARY KEY (rID),
  FOREIGN KEY (FK_SISMOGRAFI) REFERENCES sismografi(sID)
);

CREATE TABLE sismografi (
  sID bigint(20) NOT NULL AUTO_INCREMENT,
  INFO varchar(200) NOT NULL,
  FK_CENTRALINE bigint(20) NOT NULL,
  PRIMARY KEY (sID),
  FOREIGN KEY (FK_CENTRALINE) REFERENCES centraline(sID)
);

CREATE TABLE  utenti (
```

```
  NOME varchar(50) NOT NULL,
  PASSWORD varchar(50) NOT NULL,
  PRIMARY KEY (NOME)
);
```

Gestione via Web (CED)

Per la gestione Web del database si propongono due pagine:
• Una pagina html in cui vengono richiesti all'utente i dati per l'interrogazione.
• Una pagina php che eseguirà effettivamente la query e visualizzerà i risultati.

Di seguito e' riportato il form di input:

```
<form id="formRichiesta" name="formRichiesta" method="post" action="query.php">
   <label>Punto di rilevamento:
     <input type="text" name="pr"  />
   </label>
   <label>Centralina:
     <input type="text" name="cent"/>
   </label>
   <label>Sismografo:
     <input type="text" name="sis" />
   </label>
   <p>
   <input type="submit" name="ok" />
   <label>
   <input type="reset" name="reset"/>
   </label>
   </p>
 </form>
```

Codice php per recuperare dati:

```
<?php
$host = "localhost";
$user="root";
$password="";

$connect = mysql_connect($host,$user,$password)or die("Impossibile connettersi all'host");

if(mysql_select_db("terremoti",$connect)==0)
{
 echo("Il database non esiste");
 exit;
}

$sql="SELECT * FROM ((sismografi INNER JOIN centraline ON sismografi.fk_centraline = centraline.cID)INNER
JOIN punti_rilevamento ON centraline.fk_pr = punti_rilevamento.prID)INNER JOIN rilevazioni ON
rilevazioni.fk_sismografi=sismografi.sID WHERE sismografi.sID=".$_POST['sis']." AND
centraline.cID=".$_POST['cent']." AND punti_rilevamento.prID=".$_POST['pr'];

if(!($result = mysql_query($sql)))echo "errore query 1";
if(mysql_num_rows($result)!=0)
{
echo "<table border='1'>
 <tr>
 <th>data</th>
 <th>grado</th>
 <th>localita</th>
 </tr>";

 while($row = mysql_fetch_array($result))
 {
  echo "<tr>";
  echo "<td>" . $row["DATETIME"] . "</td>";
```

```
  echo "<td>" . $row["RICHTER"] . "</td>";
       echo "<td>" . $row["LOCALITA"] . "</td>";
       echo "</tr>";
      }

    echo "</table>";
  }
  else
   echo("Nessun record selezionato.");
?>
```

Risposte ai quesiti

Per quanto riguarda il quesito n. 1, lo schema generale del sistema, con legenda, è stato riportato nella Premessa.
Per quanto riguarda il quesito n. 2, le tipologie di rete sono state individuate; non potendo tralasciare Internet Tcp/Ip per il collegamento geografico PR-CED (punti di rilevamento – centro di elaborazione dati), la proposta wireless con moduli GPRS potrebbe essere sostituita con altre soluzioni equivalenti (es. moduli di acquisizione dati dotati di stack Tcp/Ip e livello 1. WiFi), anche se la discriminante è la distanza a cui devono operare le centraline C dai punti di rilevamento PR.
Per quanto riguarda i punti 3. e 4., le soluzioni sono state riportate.

A.S. 2011-2012

Testo Esame di Stato 2011-2012

YABC - ESAME DI STATO DI ISTITUTO TECNICO INDUSTRIALE

CORSO SPERIMENTALE - PROGETTO "ABACUS"

Indirizzo: INFORMATICA

Tema di: SISTEMI DI ELABORAZIONE E TRASMISSIONE DELLE INFORMAZIONI

Un gruppo amatoriale di appassionati di gare automobilistiche, desidera organizzare una competizione di corsa su strada, suddivisa in 6 prove speciali. Su ciascuna tratta saranno posizionati 5 sensori di rilevazione dei tempi:

- FP: fotocellula alla partenza; si attiva e avvia il cronometro;
- FV1, FV2, FV3: fotocellule che si attivano al passaggio del mezzo e misurano la velocità istantanea e i tempi parziali in tre punti intermedi del percorso;
- FA: fotocellula all'arrivo; si attiva e ferma ii cronometro.

Un incaricato alla partenza determina l'inizio della prova di ciascun concorrente, mentre un altro, all'arrivo controlla i dati trasmessi dai sensori durante lo svolgimento della stessa e al termine li convalida per trasmetterli in tempo reale al sistema di gestione della competizione collocato presso la sede del gruppo. Al termine della competizione, un incaricato provvederà all'invio, sul sistema informativo della Federazione Italiana Automobilismo, della classifica, completa di tutte le informazioni richieste (nominativo concorrente, auto, targa, tempo di ogni prova, tempo totale, posizione in classifica, penalità).

Il candidato, fatte le opportune ipotesi aggiuntive:

- analizzi il problema, rappresenti lo schema della realtà proposta, descriva le possibili soluzioni per l'acquisizione dei dati che dovranno essere inviati in tempo reale al sistema informativo del gruppo e in seguito alla FIA e scelga quella che a suo motivato giudizio è la piü idonea a rispondere alle specifiche indicate;
- rappresenti graficamente l'architettura di rete del sistema fornendo gli elementi essenziali che caratterizzano le parti principali della stessa;
- progetti i sistemi di archiviazione e consultazione dati utilizzando il modello di rappresentazione Entità Relazioni;
- descriva la logica del software di controllo del sistema;
- indichi una soluzione per garantire la continuità del servizio nel caso in cui si interrompa il collegamento del sistema di trasmissione dati al sistema gestionale del gruppo.

Durata massima della prova: 6 ore.

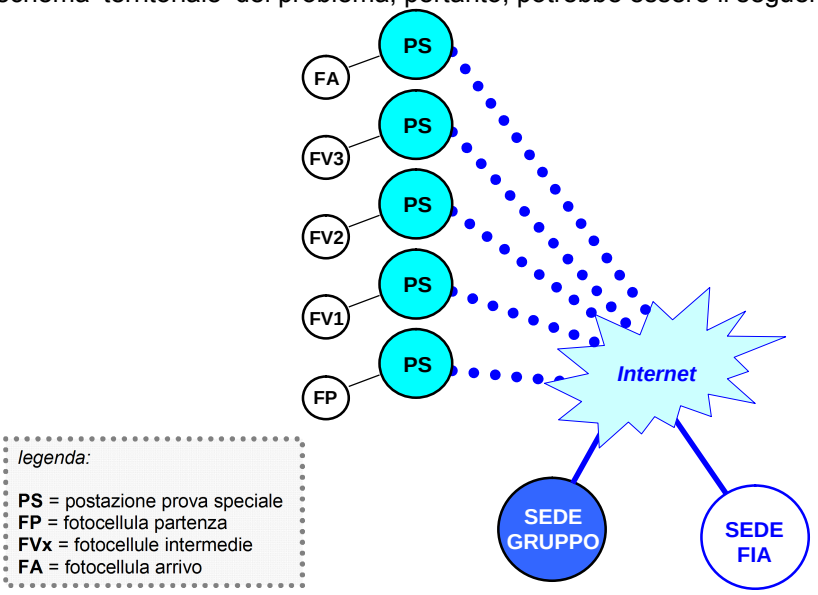
E' consentito soltanto l'uso di manuali tecnici e di calcolatrici tascabili non programmabili-

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE

Premessa e ipotesi aggiuntive

L'analisi del testo comporta uno schema progettuale piuttosto complesso.
Tra le varie perplessità che il testo solleva, il modo di condurre le prove speciali: la presenza di una fotocellula di arrivo, infatti, sembra presumere che le prove siano autonome e separate tra di loro nel tempo. Ciò però renderebbe la gara troppo lunga: organizzare sei "minigare" differenti in luoghi differenti con altrettanti arrivi e partenze di tutti i concorrenti in una sola giornata non è all'altezza di un gruppo amatoriale e comporta una organizzazione molto complessa.
Supporremo tuttavia che la prova speciale sia autonoma, considerando una prova speciale come il caso significativo delle altre (eventuali) cinque.
Gli elementi descritti nella traccia sono i seguenti: la prova speciale (una per tutte), la sede del gruppo amatoriale, la sede della FIA. Uno schema 'territoriale' del problema, pertanto, potrebbe essere il seguente:



Le connessioni tratteggiate sono wireless, dato che le fotocellule vengono disposte localmente al terreno di gara, presumibilmente in luoghi senza la possibilità di collegamenti cablati a Internet.
Siccome queste postazioni sono tutte previste "sul campo", è possibile sia necessario dotarsi di sistemi portatili di generatori di corrente autonoma.
Le postazioni PS, 5 per ogni prova speciale e una per fotocellula, possono essere PC portatili con connessione UMTS (GPRS, HSDPA o equivalente) a Internet e presidiate da un operatore. La fotocellula è connessa alla postazione PS con un mezzo cablato sufficientemente lungo (qualche metro), tale da garantire la sicurezza alla postazione oppure, preferibilmente, in modo wireless (es. Wi-Fi).

Il passaggio di una autovettura viene rilevato dalla fotocellula e segnalato alla postazione PS. La postazione PS ha l'orologio interno sincronizzato con un time server e registra la marca temporale del passaggio. Un applicativo TCP/IP Client operante sulla postazione spedisce la rilevazione ad un applicativo TCP/IP Server operante nella sede del gruppo. Le associazioni tra le marche temporali dei passaggi e il pilota vengono risolte 'a mano' dall'operatore della postazione PS, consultando il database che la postazione ha scaricato dalla sede del gruppo, magari facilitato dall'ordine di gara prestabilito.
Si decide di evitare di progettare dell' "intelligenza" sul sistema di rilevazione (es., tale che associ automaticamente il passaggio al pilota) per la complessità del progetto e i costi di manutenzione e realizzazione di un sistema a transponder.
La realizzazione di un applicativo Client/Server dedicato, invece, non rappresenta particolari difficoltà.

Sistema di rilevazione dell'I/O

Tralasciando i dettagli di progettazione, un sistema di rilevazione basato su fotocellula è abbastanza standard da poter essere acquistato sul mercato. L'interfaccia della periferica verso un personal computer può essere realizzato con un sistema a microcontrollore dedicato e con output su Bluetooth, o USB con emulazione seriale Rs232, oppure Wi-Fi.
Più complesso realizzare un sistema autonomo con gestione dell'I/O intelligente (con cambio stato della fotocellula ma anche rilevazione dell'identificativo del concorrente), memoria e modulo di trasmissione GSM/GPRS integrato

con SIM, per evitare la presenza di un personal computer presidiato. Tale soluzione, tra l'altro, prevederebbe un accurato sistema di sincronizzazione degli orologi dei vari moduli che esula dalle indicazioni del testo e dalle competenze degli studenti.

La proposta classica invece consiste nell'utilizzare una scheda Arduino 2009, programmabile in C e dotata di un modulo di conversione seriale-TCP/IP disponibile sul mercato (es. Lantronic WiPort, ma anche altri).
In questo caso il modulo mette a disposizione un piccolo Server TCP su connessione Wi-Fi a cui il client su un PC portatile in loco può connettersi: quando l'I/O della scheda Arduino ha qualcosa di pronto (es., il cambio di stato di un input digitale come quello rilevato dalla fotocellula) spedisce il dato sulla connessione TCP/IP e quindi al client della postazione PS. Ora la postazione PS rileva il tempo 'sincronizzato' e lo salva.
Naturalmente la scheda LAN Wi-Fi operante con il modulo Arduino va configurata per risiedere nella LAN TCP/IP costituita dalla postazione PS e dall'Access Point, per esempio una 192.168.0.x: va configurata l'interfaccia dell'AP, della postazione PS e del modulo stazione Wi-FI della scheda di I/O in modo coerente (in particolare, il modulo Wi-Fi della scheda di I/O possiede un suo indirizzo IP sul quale invocare un browser che darà accesso alle videate di configurazione del modulo wireless). Quindi si impostano sulle interfacce delel schede di rete tre indirizzi IP appartenenti a 192.168.0.x, una subnetmask 255.255.255.0, e gli indirizzi di gateway e DNS, ad esempio, sull'indirizzo IP della postazione PS.

Postazione PS

Per una singola prova speciale servono 5 postazioni PS (e relativo hardware di I/O per la fotocellula compreso di AP) del tutto equivalenti. Per 6 prove non necessariamente sono indispensabili 30 postazioni, dato che le prove speciali sono autonome e non contemporanee; probabilmente basterebbero due set di 5 postazioni mobili sul terreno di gara.
Il programma TCP/IP Client sulla postazione ha due compiti:

1. Rilevare il passaggio attraverso la fotocellula, per esempio con una connessione Client TCP al server TCP sul modulo di I/O che gestisce la fotocellula.
2. Scaricare l'elenco dei partecipanti alla prova dal Server TCP della sede del gruppo, registrare il tempo rilevato per il pilota e inviare i dati aggiornati al Server TCP della sede del gruppo. Potrebbe anche presentare il riepilogo dei risultati in tempo reale, scaricandoli dal Server TCP della sede del gruppo in su richiesta.
3. Possedere un comando di upload dei risultati di fine gara, da inviare al Server della sede del gruppo.

Sul sistema operativo del PC portatile della postazione PS deve essere avviato il servizio per la sincronizzazione ad un time server pubblico, affinchè le misurazioni temporali siano tutte coerenti.

Per la rilevazione della velocità istantanea (solo postazioni internedie), il calcolo potrebbe essere fatto aggiungendo a queste postazioni un secondo modulo di I/O Wi-Fi, anch'esso configurato sulla LAN locale e collocato sul campo ad una distanza predeterminata dal primo sensore: la differenza tra i tempi rilevati dai due passaggi ravvicinati consente di calcolare la velocità istantanea dell'auto. Agendo su una LAN Wi-Fi in campo aperto, i tre host possono essere collocati entro un raggio di almeno una cinquantina di metri, sufficienti per una distanza tra le fotocellule significativa.

Sede del gruppo

Nella sede del gruppo agisce il Server TCP sulla rete pubblica che accetta le connessioni dai client TCP delle postazioni PS. In esso deve essere presente un database che contiene tutte le informazioni di gara, compresi i nominativi dei partecipanti. Il database deve possedere le tabelle necessarie per creare le informazioni desunte dalle prove di una gara e quindi essere in grado di restituire in tempo reale l'andamento e i risultati della gara ai Client TCP sulle postazioni PS. Infine deve poter fare l'upload dei risultati della gara verso il server della FIA una volta ricevuto l'ok da una postazione PS.
Per facilitare la programmazione si assume che il server del gruppo possegga un indirizzo IP statico affinchè i client possano connettersi liberamente (in alternativa si può implementare un servizio DDNS tipo no-ip.com).

Sede FIA

Su un Server nella rete della FIA deve poter operare un server Web (IIS o Apache Web Server) in modo tale da poter realizzare un sito che, a partire dal database ricevuto in download dalla sede del gruppo, possa presentare i risultati delle gare tramite pagine Web.
Anche per il server Web della FIA si ipotizza sia disponibile un indirizzo IP statico.

Esempio: Client TCP della postazione PS verso sede del gruppo

A prescindere dal linguaggio utilizzato per scrivere l'applicazione TCP/IP Client sulla postazione PS, i passi da attuare quando un passaggio viene rilevato dall'I/O e letto dal programma che comunica con il modulo wireless della scheda di I/O, sono i seguenti:

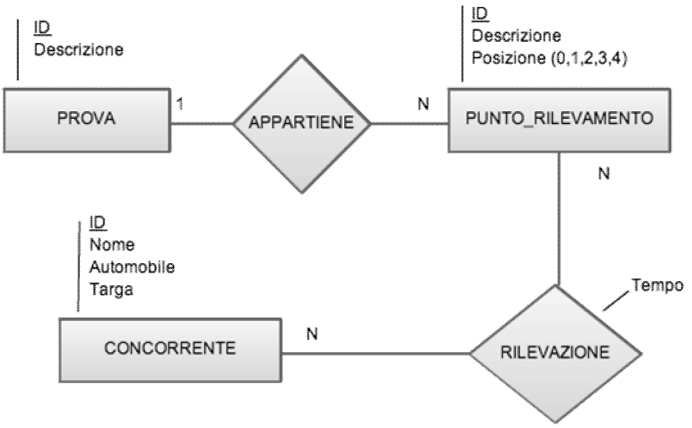
1. Creazione del socket client (verso il server TCP a bordo della sede del gruppo) e sua impostazione: primitiva *socket()*, con IP statico del server della sede del gruppo, porta TCP remota (es. 8221) su cui il Server della sede remota è in attesa di connessioni.
2. Connessione al server: primitiva *connect()*, con il socket client appena creato
3. Spedizione pacchetto di rilevazione passaggio (pkt Rilevazione): primitiva *send()*
4. Chiusura della connessione: primitiva *closesocket()*

Il formato del pacchetto rilevazione (pkt Rilevazione) deve contenere tutte le informazioni necessarie a ricostruire i dati della gara, pertanto un formato potrebbe essere:
`ID_concorrente, ID_provaspeciale, ID_tratta, temporilevato, velocita`

Immaginando tutti i dati espressi in codice Ascii, riservando agli `ID_` una dimensione opportuna (es. 10 caratteri per descrivere un intero senza segno su 32 bit), al tempo rilevato una sequenza Ascii di altri 10 caratteri (tipo `hhmmssMMMM`: ore, minuti, secondi, millisecondi) e per semplicità altri 10 caratteri per la velocità, si avrebbe un pacchetto di livello 7 di 50 byte.
Alla ricezione di un simile pacchetto il Server della sede del gruppo avrebbe tutte le informazioni per inserire nel database locale il dato della misurazione e, al termine, fornire i risultati della gara.

Modello E-R del sistema di archiviazione

Il testo richiede la realizzazione di un diagramma Entità Relazioni che permetta di rappresentare le informazioni inerenti il problema.
Si individuano 3 entità, per ognuna di queste si è indicata una chiave primaria artificiale (ID) per semplificare la trattazione:
• PROVA: oltre a ID l'attributo Descrizione per associare altre informazioni inerenti la prova
• PUNTO_RILEVAMENTO: rappresenta uno dei vari punti di rilevamento relativi alla prova; la posizione 0 indica la fotocellula di partenza, 1-2-3 le fotocellule intermedie e 4 quella d'arrivo)
• CONCORRENTE: ha come attributi i dati che saranno poi inviati alla Federazione Italiana Automobilismo
L'associazione APPARTIENE di tipo 1:N associa ogni PROVA con i propri PUNTO_RILEVAMENTO
L'associazione RILEVAZIONE di tipo N:N ha l'attributo tempo che rappresenta la rilevazione del passaggio di un CONCORRENTE in un PUNTO_RILEVAMENTO



Lo schema può essere letto nel modo seguente:
A una *Prova* appartengono più *Punti di rilevamento*; un *Punto di rilevamento* è relativo ad una singola *Prova.*
Un *Concorrente* ha una *Rilevazione* in più *Punti di rilevamento*; in un *Punto di rilevamento* si ha una *Rilevazione* per più *Concorrenti*.

Interruzione del collegamento alla sede del gruppo

In caso di malfunzionamento del collegamento verso la sede del gruppo il sistema di rilevazione non ha particolari problemi, potendo memorizzare localmente ad ogni postazione PS ogni dato rilevato.
Non appena il collegamento sarà ripristinato i PC portatili sulle postazioni PS potranno ricollegarsi al Server nella sede del gruppo e scaricare i dati locali consentendo il ripristino o il recupero del database.