



Ministero dell'Istruzione e del Merito

A038 - ESAME DI STATO CONCLUSIVO DEL SECONDO CICLO DI ISTRUZIONE

Indirizzo: ITIA - INFORMATICA E TELECOMUNICAZIONI ARTICOLAZIONE "INFORMATICA"

(Testo valevole anche per gli indirizzi quadriennali IT32)

Disciplina: SISTEMI E RETI

Il candidato svolga la prima parte della prova e due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

L'amministrazione di una Regione italiana, attraverso una società appositamente creata, ha recentemente sviluppato una infrastruttura di comunicazione in fibra ottica, allo scopo di fornire connettività a banda larga ad Enti locali, scuole e strutture sanitarie pubbliche presenti in tutto il suo territorio. In particolare, in ambito sanitario, la società gestisce anche un *data-center* che raccoglie tutti i dati sanitari dei cittadini residenti in regione, relativi alle prestazioni sanitarie erogate dalle strutture pubbliche (fascicolo sanitario elettronico).

I dati raccolti nel fascicolo sanitario elettronico di ciascun paziente possono essere di vari formati e dimensioni in quanto riguardano, ad esempio, gli accertamenti diagnostici (es. ecografia), le visite specialistiche (es. visita cardiologica) e la relativa documentazione (referto, immagini diagnostiche, video ...).

All'interno della componente M6C2 "Innovazione, ricerca e digitalizzazione del Servizio Sanitario Nazionale", prevista dalla Missione 6 del PNRR, la Regione intende estendere la rete in fibra già esistente, per offrire il servizio di connettività a banda larga a tutte le strutture sanitarie private convenzionate, in modo che anche i dati da loro prodotti possano direttamente confluire nel *data-center* regionale.

In tal modo, tutti i cittadini ed i medici chiamati a curarli, sia presso strutture sanitarie pubbliche che presso quelle private convenzionate, avranno a disposizione in un unico luogo virtuale (il fascicolo sanitario elettronico) tutte le informazioni sanitarie di loro interesse.

Per differenziare le diverse tipologie di strutture connesse alla rete (Enti locali, scuole e strutture sanitarie pubbliche e private), la società regionale che gestisce l'infrastruttura in fibra ha adottato un piano di indirizzamento utilizzando sottoreti della rete 10.0.0.0/8; in particolare, a questo nuovo servizio di connettività verso le strutture sanitarie private convenzionate è stata assegnata la sottorete 10.100.0.0/16. Questa sottorete sarà finalizzata esclusivamente all'interazione con il *data-center* delle strutture sanitarie private convenzionate, ma non offrirà loro servizi di accesso generalizzato ad Internet.

Utilizzando gli indirizzi consentiti da questa sottorete, il progetto dovrà pertanto dettagliare un piano di indirizzamento che permetta di connettere un numero di strutture sanitarie private convenzionate che si stima essere intorno alle 2000 in regione (con possibili incrementi futuri), assegnando a ciascuna di esse la disponibilità di un minimo di 8 indirizzi complessivi.

Ogni struttura sanitaria privata convenzionata ovviamente dispone già di una propria infrastruttura di rete locale interna. La società regionale di gestione fornirà a tali strutture private convenzionate un dispositivo per la connessione alla rete regionale, configurato e controllato da remoto dalla società regionale stessa. Il progetto dovrà garantire che ciascuna struttura collegata non possa accedere alle reti di tutte le altre strutture connesse alla rete in fibra regionale.

Il candidato analizzi la realtà di riferimento e, formulate le opportune ipotesi aggiuntive, contribuisca alla stesura del progetto svolgendo i seguenti punti:

1. sviluppi una descrizione di massima, anche supportata da uno schema grafico, dell'infrastruttura di rete in fibra pre-esistente (che connette Enti locali, scuole e strutture sanitarie pubbliche) e di come questa si evolverà per implementare il nuovo servizio per le strutture sanitarie private convenzionate, con opportune esemplificazioni degli indirizzamenti IP adottati;
2. indichi la tipologia e le caratteristiche hardware (es: numero e tipologia delle singole porte) del dispositivo che sarà fornito ad ogni struttura sanitaria privata convenzionata, nonché i dettagli relativi alla eventuale configurazione di rete delle sue porte; espliciti anche i servizi che ritiene debbano essere configurati su tale dispositivo;
3. considerando le caratteristiche della LAN pre-esistente in una ipotetica struttura sanitaria privata convenzionata, specifichi con quali eventuali apparati aggiuntivi o riconfigurazioni degli apparati già esistenti tale rete verrà connessa con la rete in fibra regionale, esemplificando opportunamente;
4. data la natura sensibile dei dati trattati, espliciti le principali misure che è opportuno adottare per garantirne un trattamento con adeguata sicurezza, sia per la loro archiviazione che per i trasferimenti da e per il *data-center*; in particolare il candidato specifichi le modalità e la schedulazione temporale con cui le strutture sanitarie trasferiscono al *data-center* regionale i dati delle prestazioni sanitarie da loro effettuate.

SECONDA PARTE

- I. In relazione al tema proposto nella prima parte, si prevedano le strategie da adottare in caso di malfunzionamenti della connessione in fase di trasferimento dati e sui sistemi di archiviazione, allo scopo di evitare possibili perdite di dati.
- II. In relazione al tema proposto nella prima parte, il candidato descriva le possibili forme di autenticazione qualificata (a più fattori) per consentire al singolo cittadino di consultare via web tutti i dati del proprio fascicolo sanitario elettronico (accertamenti e visite specialistiche).
- III. Una piccola azienda dispone di un normale collegamento ad Internet a banda larga, con un router a cui è assegnato un solo indirizzo IP pubblico statico. Nella rete interna alla piccola azienda esiste un web server locale che si vuole rendere accessibile da Internet sia tramite protocollo HTTP che HTTPS, e si vuole rendere gestibile da remoto tramite protocollo SSH. Il candidato descriva la configurazione del router necessaria per raggiungere lo scopo, motivando nel dettaglio le scelte fatte ed elencando i comandi utilizzabili.
- IV. All'interno di una azienda con una propria LAN, un tecnico di *help-desk* riceve la segnalazione di un utente circa l'impossibilità di "navigare su Internet". Si descrivano i passi e gli opportuni strumenti da utilizzare per individuare tre possibili cause del problema.

Durata massima della prova: 6 ore.

È consentito l'uso di manuali tecnici e di calcolatrici scientifiche o grafiche purché non siano dotate della capacità di elaborazione simbolica algebrica e non abbiano la disponibilità di connessione a Internet.

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

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla consegna della traccia.

SOLUZIONE

Il testo mostra una realtà di riferimento che descrive una infrastruttura di rete regionale, ovvero di tipo geografico (WAN), ma fruibile tramite una rete privata (LAN) realizzata in fibra ottica da una **Società**. La **Società** gestisce anche un **data-center** presente all'interno della LAN e già fornisce servizi agli **Enti Locali** della Regione, che chiameremo **EL₁, EL₂, ..., EL_m**

A questi **EL_i** si devono aggiungere delle **Strutture Sanitarie Private**, che chiameremo **SSP₁, SSP₂, ..., SSP_n**

In definitiva al **data-center** devono accedere tutti gli **EL** e tutti gli **SSP** tramite utenti amministrativi (es., contabili) e sanitari (es. medici) con un applicativo gestionale che opera su un database.

Inoltre al **data-center** devono poter accedere anche **singoli cittadini**, stavolta con un client web che acceda al medesimo database.

PRIMA PARTE Quesito 1

In base al testo, è necessario produrre un piano di indirizzamento idoneo alla LAN della **Società** affinché si possano gestire opportunamente sia gli **EL** già in gestione (ma anche eventuali nuove affiliazioni), sia le **SSP** che devono essere aggiunte all'infrastruttura.

Un dato del testo sembra prevedere una parte dell'indirizzo alla *tipologia* di struttura gestita, infatti indica il secondo byte dell'indirizzo privato di classe A 10.0.0.0/8 con **100** per le **SSP**: 10.**100**.0.0/16. Seguendo questa logica, si può ipotizzare che una *Scuola* possa avere 1 (10.1.0.0/16), un *Comune* 2 (10.2.0.0/16), una *ASL* 3 (10.3.0.0/16), e così via.

A questo punto i **16** bit rimanenti possono essere scomposti in:

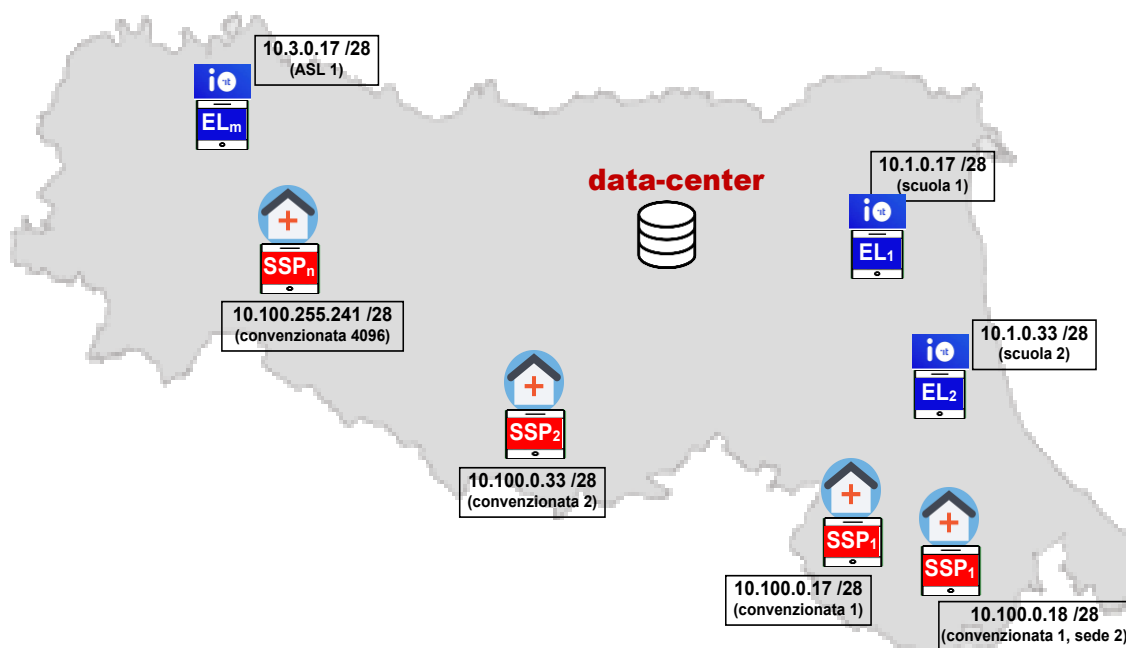
- **12** bit per la parte **subnetid** e
- **4** bit per la parte **hostid**

In questo modo ogni tipologia di Struttura può descrivere $2^{12} = 4096$ strutture diverse (ma dello stesso tipo) e, ognuna, possedere $2^4 = 16$ indirizzi a disposizione (per eventuali sedi distaccate). In definitiva la **LAN** offerta dalla **Società** possiede una subnetmask /28, ovvero **255.255.255.240**

Il piano rispetta le dimensionalità della richiesta del testo, infatti:

- a. Le **SSP** ipotizzate dal testo sono circa 2000 (<4096)
- b. Ogni **Struttura** possiede almeno 8 indirizzi IP (<16).
- c. Ogni **tipologia** di Struttura conta circa 4000 strutture diverse (es., in una regione italiana difficilmente sono presenti più di 4000 scuole(*)

Schema realtà di riferimento



Esempi:

EL1, 10.1.0.17/28 ovvero:	10.	1.	00000000.0001	0001
		scuola	-----	----
			subnetId	hostId
SSP1, 10.100.0.17/28 ovvero:	10.	100.	00000000.0001	0001
		SSP	-----	----
			subnetId	hostId
SSP1, sede 2, 10.100.0.18/28:	10.	100.	00000000.0001	0010
		SSP	-----	----
			subnetId	hostId

PRIMA PARTE Quesito 2

Il **Dispositivo** fornito dalla **Società** alle **SSP** è un **router**, infatti deve mettere in collegamento almeno due reti differenti, la **LAN** della **Società** (che usa FO a livello 1 OSI) e la **LAN** preesistente della **SSP** (tipicamente Ethernet a livello 1 OSI).

Questo router deve quindi avere almeno una porta ETH (rame) e tipicamente due porte fisiche FO, dato che le MAN in FO di questo tipo sono tipicamente ad anello.

Commercialmente sono diffusi router con 8/16/24 porte ETH (rame) da 1Gbps a 10Gbps e 2/4/8 porte FO SFP/SFP+Slots fino a 10Gbps. I router di alta fascia sono modulari, e quindi l'utente può decidere la configurazione dell'apparato in base alle proprie esigenze.

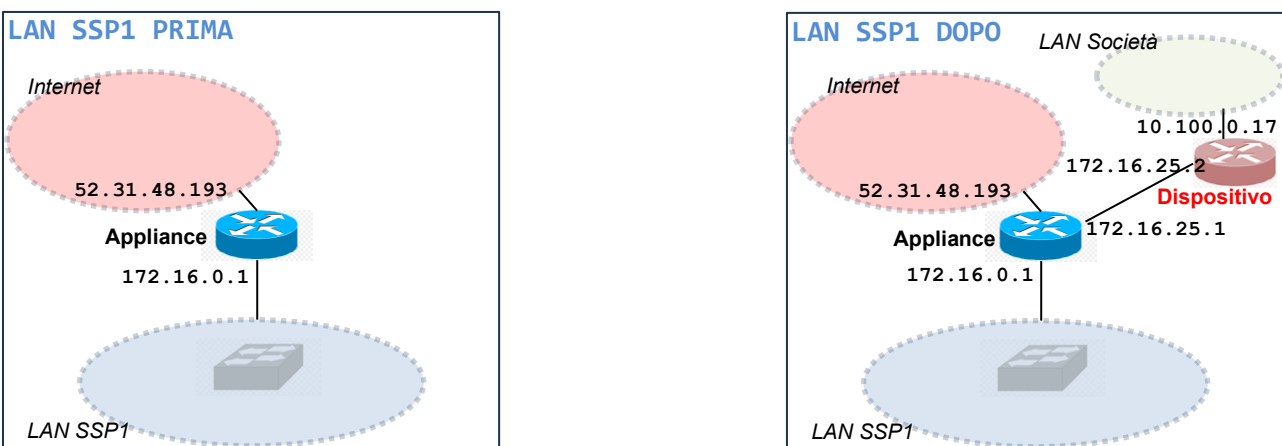
Su questi router è sempre possibile configurare un **Firewall**, un supporto **VPN** e ovviamente **STP** (o RSTP) e **VLAN** tramite la configurazione dei rispettivi protocolli.

Il servizio essenziale sul dispositivo è il **routing**, ovvero una **Tabella di Instradamento** configurata in modo da veicolare il traffico diretto e/o proveniente verso/dalla **LAN** della **Società** sulla porta FO. Per una possibile Tabella di Instradamento, vedi Quesito 3

PRIMA PARTE Quesito 3

Se la **LAN** della **Società** non offre connettività sulla rete pubblica, come ipotizzato nel testo, il **Dispositivo** (router, vedi Quesito 2) potrebbe essere installato a valle dell'**Appliance** preesistente nella **LAN SSP**: ovviamente la SSP ancora non connessa dalla Società possiede un provider Internet per dare il servizio alla LAN aziendale. Ipotizziamo che questa LAN preesistente sia una **172.16.0.0/24** alla quale il provider offre una supernet **52.31.48.192/29** (8 indirizzi tra cui nome della rete e broadcast).

Un dettaglio della **LAN** della **SSP prima e dopo** l'affiliazione alla **Società**:



Si nota la presenza di una **subnet di link** tra l'**Appliance** preesistente e il **Dispositivo**

Il router nell'**Appliance** preesistente deve essere riconfigurato per impostare la route sulla **subnet di link** (e relative regole sul Firewall).

PRIMA PARTE Quesito 4

In merito a questo Quesito si nota che il GDPR non usa più il la locuzione "*dato sensibile*", sostituito da "*dato particolare*".

Inoltre la richiesta implica che i dati generati dagli affiliati alla Società (**EL** e **SSP**) posseggano un flusso di trasferimento schedato, ovvero una memorizzazione temporanea. *In base a questa progettazione questa memorizzazione temporanea e quindi questo flusso non esiste.*

La sicurezza sui dati particolari (dati sanitari delle persone) va affrontata a due livelli:

- Protezione del **protocollo** di livello 7 utilizzato dall'applicativo gestionale operante nella **LAN** della **Società**
- Protezione degli **archivi del data-center**

Nel primo caso potrebbe essere sufficiente utilizzare un protocollo di livello 7 con autenticazione tramite **Certificato Digitale** (anche autoprodotta), distribuito dalla **Società** ad ogni **SSP**. In questo caso si otterrebbero anche la cifratura e l'integrità dei trasferimenti (TLS/SSL) che, uniti alla connettività proprietaria (l'infrastruttura in FO) danno sufficienti garanzie.

Per la **continuità del servizio**, invece, è necessario prevedere una duplicazione della connessione, con tecnologia differente, ovvero su linea pubblica.

Si potrebbe optare per un servizio **VPN** sulla connessione pubblica della **SSP** (fornito dal **data-center**), dotando le **SSP** di un *client* VPN con relativo Certificato Digitale, magari con distribuzione di indirizzi IP privati identici a quelli utilizzati in condizioni standard.

Nel secondo caso il **data-center** deve dotarsi di un sistema di **backup 3-2-1**, ovvero:

- Si creano **tre** copie degli archivi: i dati originali sul dispositivo principale e almeno altre due copie.
- Si usano **due** dispositivi di storage diversi: PC, disco esterno, unità flash, DVD, NAS, cloud storage, ecc..
- **Una** delle copie di backup viene conservata offline.

SECONDA PARTE Quesito I

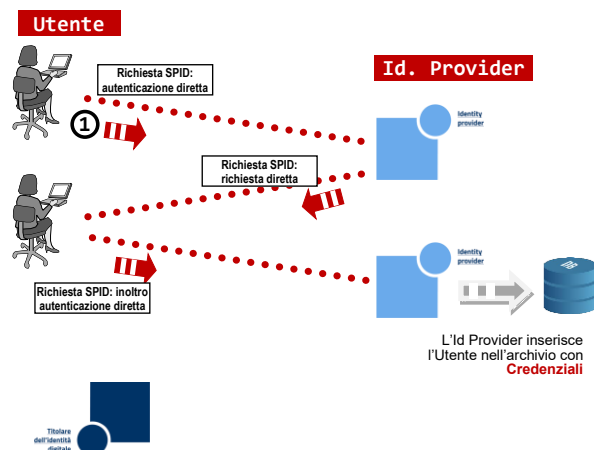
Quesito già affrontato in PRIMA PARTE Quesito 4.

SECONDA PARTE Quesito II

Il singolo cittadino italiano attualmente utilizza **SPID** come modalità di autenticazione a più fattori (Livello 2 e Livello 3 di SPID).

In questo caso il **cittadino** è detto **User** (possiede una identità digitale fornita da SPID), che ha depositato la sua identità presso un **Identity Provider** (es., Poste Italiane) mentre la **Società** che fornisce il servizio autenticato è detta **Service Provider**.

Fasi di SPID: richiesta servizio



Tipicamente i due fattori con cui il cittadino dimostra la propria identità sono il “*possesso di qualcosa*” (un cellulare) e la “*propria essenza*” (impronta digitale da fornire all'App) oppure la “*conoscenza di qualcosa*” (una credenziale, da fornire all'App).

Testi di:

prof. Paolo Ollari
prof. Ramon Ugolotti
prof.ssa Debora Marchesini
prof. Piero Radice
prof. Gabriele Martino

2024 - ITIS “L. Da Vinci”, Parma