

Sessione ordinaria 2024 - Seconda prova scritta

Ministero dell'istruzione e del merito

A038 – ESAME DI STATO CONCLUSIVO DE SECONDO CICLO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITIA - INFORMATICA E TELECOMUNICAZIONI ARTICOLAZIONE "INFORMATICA"

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 garantire 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.

Premessa

La prova si basa su una rete WAN regionale in fibra ottica e sul progetto di ampliamento necessario per implementare un nuovo servizio territoriale. I quesiti della prima parte e i primi due quesiti della seconda fanno riferimento specifico al tema descritto nella traccia e richiedono la conoscenza delle configurazioni e dei dispositivi di rete, del routing e del subnetting, delle misure di sicurezza informatica.

Gli ultimi due quesiti della seconda parte coinvolgono maggiormente l'aspetto del saper fare e riguardano le azioni da mettere in atto per rendere un web server locale accessibile da Internet e per affrontare il problema dell'impossibilità di "navigare su Internet" in una postazione di una rete locale.

Soluzione prima parte

La Regione X, attraverso una società appositamente creata, ha sviluppato un'infrastruttura 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". Verosimilmente ha realizzato una rete a banda ultra larga (BUL) imperniata sulla tecnologia FTTH (Fiber To The Home) che consente di ottenere una connettività Internet ad altissima velocità. In ambito sanitario, i dati dei pazienti, raccolti nelle strutture pubbliche e archiviati in un fascicolo sanitario elettronico, sono gestiti da un data-center regionale. Come si evince dalla traccia, sono in larga parte immagini e video ad alta risoluzione e la loro digitalizzazione richiede una larghezza di banda molto elevata.

La Regione intende ora realizzare un nuovo progetto che permetta di "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 altre parole, nell'ottica del miglioramento dei servizi, vuole estendere il fascicolo sanitario elettronico a tutti i cittadini, anche a quelli che si servono di strutture sanitarie private convenzionate.

Quesito 1

Il candidato 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

"La società regionale che gestisce l'infrastruttura in fibra ha adottato un piano d'indirizzamento utilizzando sottoreti della rete 10.0.0.0/8". 10.0.0.0/8 è un blocco di indirizzi IP privati di classe A e realizza dunque una WAN privata, ovvero una rete geografica di grandi dimensioni, gestita e di proprietà della Regione X, che interconnette le reti locali (LAN) delle varie strutture territoriali e il data-center regionale tramite router installati a ogni estremità della rete.

Una WAN privata offre un'infrastruttura molto sicura, non esposta ad Internet e per questo meno soggetta ad attacchi esterni. La banda è sempre garantita e la qualità del servizio (QoS) assicura l'ottimizzazione del traffico dati.

Generalmente una WAN privata viene realizzata con linee dedicate prese in leasing dai Service Provider e utilizzando le tecnologie più recenti quali MPLS (Multiprotocol Label Switching) e SD-WAN (Software Defined WAN)

Non approfondiamo questi argomenti, ci limitiamo a dire che SD-WAN è una tecnologia, basata sul cloud, molto innovativa, performante e diffusa e a ricordare che in passato si utilizzavano altre tecnologie, che tanto spazio avevano nei libri di testo di Sistemi e Reti di alcuni anni fa, quali ATM, X.25 e Frame Relay.

La rete 10.0.0.0/8, con subnet mask 255.0.0.0, mette a disposizione 2^{24} indirizzi IP (circa 16,8 milioni) nell'intervallo 10.0.0.0 - 10.255.255.255 e viene divisa in gruppi più piccoli di sottoreti, che indicano la tipologia della struttura (scuola, ente pubblico ecc.), che vengono a loro volta suddivisi in gruppi di sottoreti ancora più piccoli che individuano le singole strutture. Queste sottoreti private si trovano solitamente dietro router o firewall che eseguono l'operazione di NAT (Network Address Translation), necessaria perché gli indirizzi IP privati siano instradabili sull'Internet pubblica.

La traccia richiede di estendere la rete 10.0.0.0/8 alle strutture sanitarie private convenzionate:

- utilizzando gli indirizzi consentiti dalla sottorete 10.100.0.0/16
- tenendo conto che le strutture interessate sono circa 2000 e che per ciascuna di esse devono essere disponibili almeno 8 indirizzi IP

Poiché non fornisce informazioni su com'è stata sviluppata l'infrastruttura di rete già in funzione, ipotizziamo che le sottoreti delle tipologie pre-esistenti, enti locali, scuole e strutture sanitarie pubbliche, e la nuova sottorete, assegnata alle strutture sanitarie private convenzionate, abbiano lo stesso piano di indirizzamento IP.

Il piano si basa su indirizzi IP e subnet mask. L'indirizzo IP nella versione IPv4 è formato da 32 bit suddivisi in 4 byte: la subnet mask indica quale parte dell'indirizzo IP è l'indirizzo di rete e quale parte è l'intervallo di indirizzi IP disponibili (campo host).

Utilizzando la notazione binaria, analizziamo la sottorete 10.100.0.0/16 con subnet mask 255.255.0.0

Indirizzo di rete binario	10	100	0	0
	00001010.	01100100.	00000000.	00000000
Subnet mask binaria	255	255	0	0
	11111111.	11111111.	00000000.	00000000

Il primo byte dell'indirizzo individua la classe (10), il secondo individua la tipologia di rete (100 "strutture sanitarie private convenzionate"), gli altri due byte individuano il campo host, ovvero gli indirizzi disponibili pari a $2^{16} = 65536$. Per progettare un piano di indirizzamento che permetta di connettere circa 2000 strutture (con possibili incrementi futuri) e assegnare a ciascuna un minimo di 8 indirizzi, occorre realizzare il subnetting della rete.

Ragionando in termini di numerazione binaria e di potenze di 2, prendiamo in considerazione il numero 2048, pari a 2^{11} : 11 bit sono idonei per connettere le circa 2000 strutture presenti allo stato attuale ma potrebbero diventare presto insufficienti per far fronte al possibile e probabile incremento futuro del numero delle strutture. Scegliamo dunque il numero successivo delle potenze di 2, cioè 4096, pari a 2^{12} : i 12 bit necessari li prendiamo in prestito dal campo host originale, ovvero dagli ultimi 2 byte dell'indirizzo IP, utilizzando la subnet mask 255.255.255.240

Indirizzo di rete binario	10	100	x	x	
	00001010.	01100100.	bbbbbbbb.	bbbb0000	$240 = 2^7 + 2^6 + 2^5 + 2^4 = 128 + 64 + 32 + 16$
Subnet mask binaria	255	255	255	240	
	11111111.	11111111.	11111111.	11110000	

I primi 16 bit in viola individuano la classe e la tipologia della struttura, degli altri 16 bit, i primi 12 in rosso individuano la sottorete relativa alla struttura e i restanti 4 in blu individuano gli indirizzi IP disponibili (campo host).

Utilizzando la subnet mask 255.255.255.240 e in linea con quanto richiesto dalla traccia, otteniamo una subnet 10.100.0.0/28 (28 è la dimensione della subnet in quanto i bit di sottorete sono 16+12).

Possiamo connettere in tal modo **4096 sottoreti** e assegnare a ciascuna di esse la disponibilità di 16 (2^4) indirizzi. Tenendo conto dell'indirizzo di rete e di quello di broadcast, **gli indirizzi di rete utilizzabili per ciascuna sottorete sono 14.**

Sul web sono presenti diversi strumenti online per la progettazione di una rete di computer. Dal sito calculator.net, per fare una verifica di quanto sviluppato, utilizziamo IP Subnet Calculator, un software che, partendo dall'indirizzo IP e dalla maschera di rete, calcola: il broadcast, la classe, la rete, la wildcard mask di Cisco, e il range di host utilizzabili.

IPv4 Subnet Calculator

Result

IP Address:	10.100.0.0
Network Address:	10.100.0.0
Usable Host IP Range:	10.100.0.1 - 10.100.0.14
Broadcast Address:	10.100.0.15
Total Number of Hosts:	16
Number of Usable Hosts:	14
Subnet Mask:	255.255.255.240
Wildcard Mask:	0.0.0.15
Binary Subnet Mask:	11111111.11111111.11111111.11110000
IP Class:	C
CIDR Notation:	/28
IP Type:	Private
Short:	10.100.0.0 /28
Binary ID:	00001010011001000000000000000000
Integer ID:	174325760
Hex ID:	0xa640000
in-addr.arpa:	0.0.100.10.in-addr.arpa
IPv4 Mapped Address:	::ffff:0a64.00
6to4 Prefix:	2002:0a64.00::/48

All 16 of the Possible /28 Networks for 10.100.0.*

Network Address	Usable Host Range	Broadcast Address:
10.100.0.0	10.100.0.1 - 10.100.0.14	10.100.0.15
10.100.0.16	10.100.0.17 - 10.100.0.30	10.100.0.31
10.100.0.32	10.100.0.33 - 10.100.0.46	10.100.0.47
10.100.0.48	10.100.0.49 - 10.100.0.62	10.100.0.63
10.100.0.64	10.100.0.65 - 10.100.0.78	10.100.0.79
10.100.0.80	10.100.0.81 - 10.100.0.94	10.100.0.95
10.100.0.96	10.100.0.97 - 10.100.0.110	10.100.0.111
10.100.0.112	10.100.0.113 - 10.100.0.126	10.100.0.127
10.100.0.128	10.100.0.129 - 10.100.0.142	10.100.0.143
10.100.0.144	10.100.0.145 - 10.100.0.158	10.100.0.159
10.100.0.160	10.100.0.161 - 10.100.0.174	10.100.0.175
10.100.0.176	10.100.0.177 - 10.100.0.190	10.100.0.191
10.100.0.192	10.100.0.193 - 10.100.0.206	10.100.0.207
10.100.0.208	10.100.0.209 - 10.100.0.222	10.100.0.223
10.100.0.224	10.100.0.225 - 10.100.0.238	10.100.0.239
10.100.0.240	10.100.0.241 - 10.100.0.254	10.100.0.255

tabella 1

Sono 16 sottoreti/28 per 10.100.0.*
 16 sottoreti/28 per 10.100.1.*
 ...
 16 sottoreti/28 per 10.100.255.*
Totale sottoreti/28=16*256=4096

Un piano d'indirizzamento dell'infrastruttura di rete, limitato alle tipologie delle strutture, potrebbe essere il seguente:

Struttura	Sottorete	Subnet Mask	N. Sottoreti	N. Ip disponibili (host)
Enti locali	10.8.0.0/28 *	255.255.255.240	$2^{12} = 4096$	$2^4 - 2 = 14$
Scuole	10.16.0.0/28	255.255.255.240	$2^{12} = 4096$	$2^4 - 2 = 14$
Strutture sanitarie pubbliche	10.32.0.0/28	255.255.255.240	$2^{12} = 4096$	$2^4 - 2 = 14$
Strutture sanitarie private convenzionate	10.100.0.0/28	255.255.255.240	$2^{12} = 4096$	$2^4 - 2 = 14$

* per facilitare, quando serve, la rappresentazione binaria si consiglia di utilizzare le potenze di 2 (8, 16, 32, 128, ...)

Il data-center che raccoglie i dati sanitari dei cittadini della Regione, e si ipotizza, anche i dati relativi alle altre tipologie di strutture, utilizza ad esempio la sottorete 10.128.0.0/16 con subnet mask 255.255.0.0; tale rete può essere eventualmente segmentata per esigenze specifiche.

Una web application consentirà ai cittadini e ai medici chiamati a curarli, di accedere in maniera selettiva e riservata e in modalità di consultazione, al fascicolo sanitario di loro interesse.

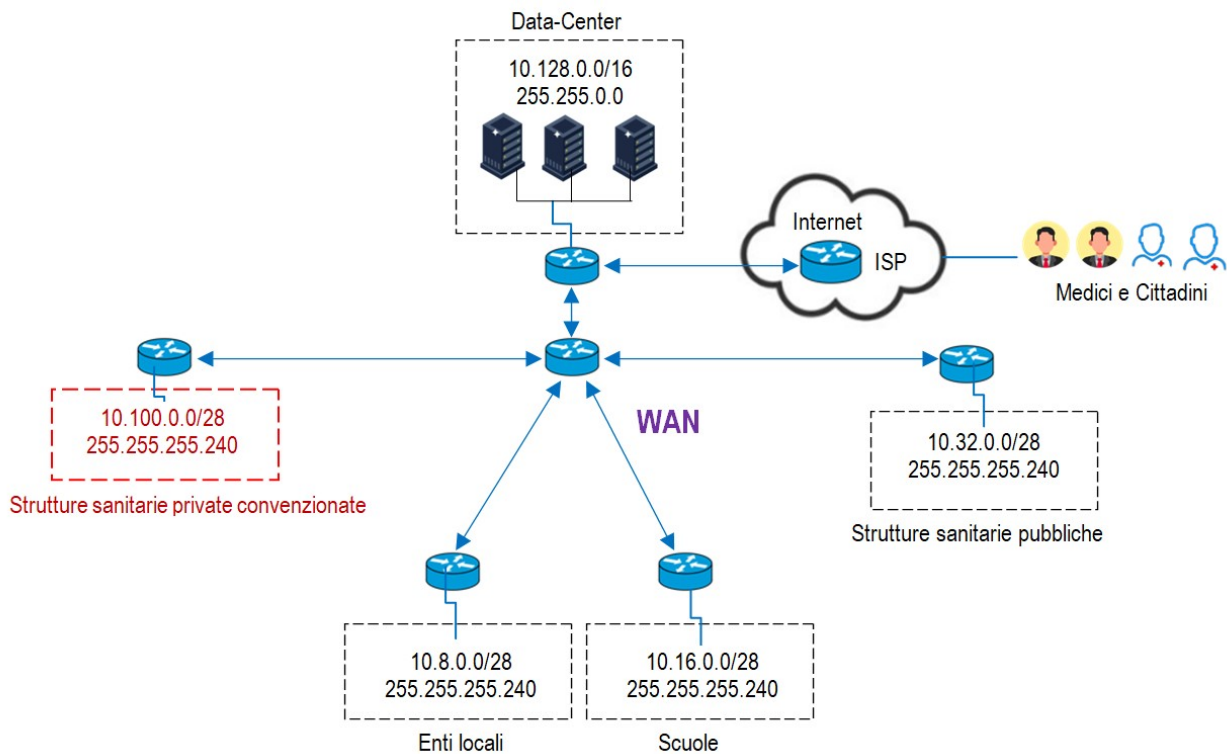


figura 1

Ciascuna struttura collegata non può accedere direttamente alle reti di tutte le altre strutture connesse alla rete in fibra regionale in quanto l'inoltro diretto di un pacchetto dati da una subnet ad un'altra non è permesso. Ad esempio, facendo riferimento alla tabella 1, dalla rete 10.100.0.0/28 non si può accedere alla rete 10.100.0.16/28, poiché le due subnet sono diverse e la comunicazione è possibile solo utilizzando un router o uno switch layer 3.

Il subnetting rappresenta una prima misura di sicurezza perché riduce la possibilità che il traffico non autorizzato o dannoso possa propagarsi liberamente attraverso l'intera rete. Per garantire che non si possano verificare intrusioni tra le reti delle varie strutture, occorre configurare le ACL opportune sui router della WAN, indicando quali indirizzi IP possono comunicare tra di loro e consentendo o bloccando, di conseguenza, il traffico tra le subnet. Le ACL (Access Control Lists) sono una lista di istruzioni applicate alle interfacce del router che indicano quali sono i pacchetti dati da accettare e quali sono quelli da rifiutare.

Quesito 2

Il candidato 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

Il dispositivo che sarà fornito ad ogni struttura sanitaria privata convenzionata è sicuramente un router idoneo a:

- connettere la LAN interna di ogni struttura con la WAN regionale
- essere configurato e controllato da remoto dalla società regionale che gestisce l'infrastruttura di rete

Facendo riferimento a un'ipotetica struttura sanitaria privata convenzionata, ipotizziamo che il nuovo router si inserisca in un contesto di rete LAN pre-esistente in cui sono presenti un modem-router per l'accesso ad Internet e un firewall che protegge la rete interna e realizza una DMZ. Una situazione classica di questo tipo di rete è la seguente:

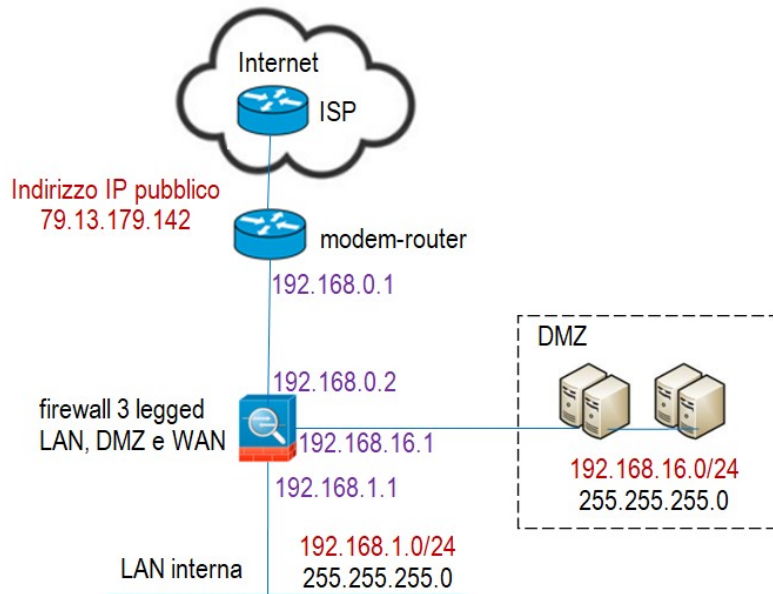


figura 2 – Rete pre-esistente

Poiché l'accesso ad Internet non è consentito dalla sottorete 10.100.0.0/28 ma è comunque assolutamente indispensabile per ciascuna LAN, si possono adottare due soluzioni progettuali.

Soluzione 1

La società regionale fornisce un router di connessione alla WAN regionale che viene collegato in cascata al modem-router esistente dedicato alla connettività Internet

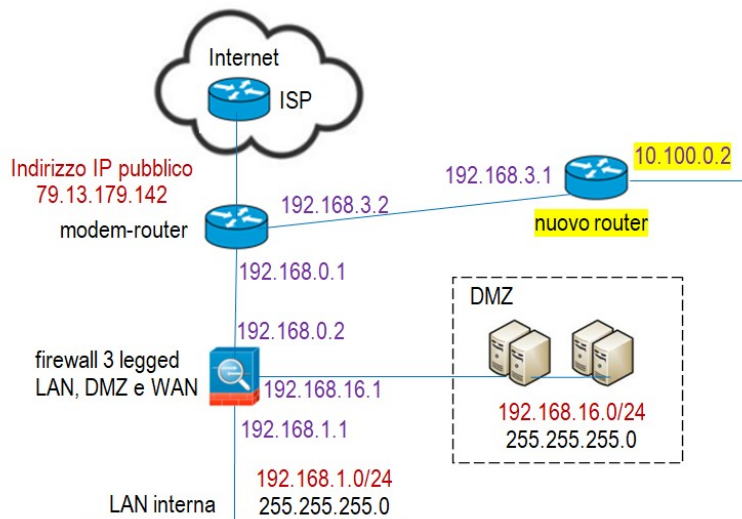


figura 3 – nuovo router in cascata al modem-router pre-esistente

Soluzione 2

La società regionale, in sostituzione del modem-router esistente, fornisce un router con funzionalità Dual WAN che collega la LAN alla WAN regionale in fibra ottica e dispone di un'interfaccia Ethernet e di una sezione modem per accedere a Internet.

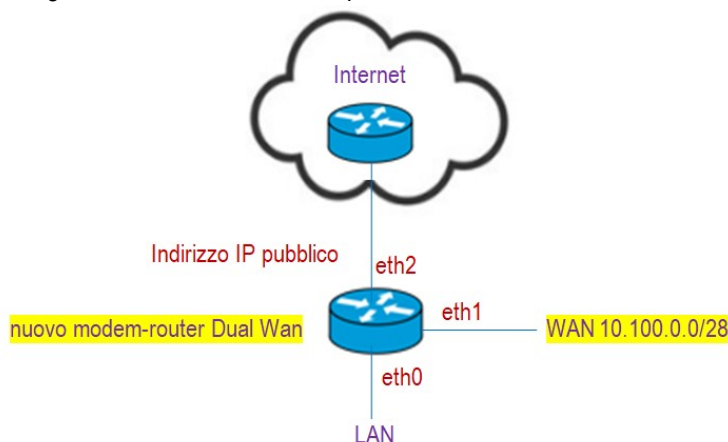


figura 4 - modem-router Dual Wan al posto del modem-router pre-esistente

Il modem-router Dual WAN viene inserito al posto del modem-router esistente, a valle del firewall 3 legged (vedi figura 2)

Delle due soluzioni, si sceglie di adottare e approfondire la seconda

Configurazione del modem-router Dual Wan

Interfaccia LAN (eth0 in rame Gigabit)

Indirizzo IP: 192.168.0.1
Subnet Mask: 255.255.255.0

Interfaccia WAN (eth1 in fibra ottica) per la rete 10.100.0.0/28

Tipo di Connessione: IP Statico
Indirizzo IP: 10.100.0.2 (o qualsiasi altro indirizzo interno alla subnet 10.100.0.0/28)
Subnet Mask: 255.255.255.240
Gateway: 10.100.0.1 (il next-hop ovvero l'indirizzo IP del router successivo nella rete 10.100.0.0/28, ad esempio l'indirizzo 10.100.0.1)
DNS: 8.8.8.8 8.8.4.4 (Google Public DNS)

Interfaccia WAN (eth2 in rame o fibra ottica) per Internet

La configurazione di una connessione WAN Internet varia in base al tipo di connessione fornita dall'ISP (il Provider dei Servizi Internet). I tipi di connessione più comuni sono:

1. DHCP (Dynamic Host Configuration Protocol)
2. Indirizzo IP Statico
3. PPPoE (Point-to-Point Protocol over Ethernet)

Ipotizzando che l'ISP fornisca un indirizzo IP statico 200.10.100.2/24 con gateway 200.10.100.1, la configurazione è la seguente:

Tipo di Connessione: Indirizzo IP statico
Indirizzo IP: 200.10.100.2
Subnet Mask: 255.255.255.0
Gateway: 200.10.100.1
DNS: 8.8.8.8 8.8.4.4 (Google Public DNS)

Servizi che devono essere configurati sul router

1. routing per instradare il traffico tra la LAN 192.168.0.0/24 e la WAN privata 10.100.0.0/28. Ipotizziamo che il routing della WAN venga configurato tramite rotte statiche implementate manualmente dall'amministratore di rete della società regionale. In alternativa, utilizzando un protocollo di routing dinamico come OSPF, le rotte possono essere "imparate" e impostate automaticamente dal router
2. abilitazione del NAT per consentire ai dispositivi della LAN di connettersi a Internet utilizzando l'indirizzo IP pubblico del router fornito dall'ISP
3. abilitazione del protocollo di rete crittografico SSH (Secure Shell) per consentire di accedere al router da una posizione remota. Occorre impostare le credenziali di un utente per l'accesso SSH e le regole di sicurezza ACL per compilare la lista di indirizzi IP che possono accedere al servizio.
Una soluzione alternativa per controllare il router da remoto, consigliata soprattutto quando si accede da reti poco sicure o da Internet, è quella di configurare e attivare una VPN (Virtual Private Network) che crea una connessione crittografata tra il dispositivo remoto e il router
4. configurazione delle regole di sicurezza (firewall) per proteggere la LAN e la WAN privata da accessi non autorizzati. Ad esempio:
 - a. permettere il traffico HTTP/HTTPS dalla LAN a Internet
 - b. bloccare tutto il traffico non autorizzato dall'esterno

....

La configurazione di un router varia in base al produttore e al modello e può essere eseguita tramite l'interfaccia grafica utente (GUI) o attraverso le sessioni SSH e l'uso delle CLI (Command Line Interface). Le CLI consumano meno risorse rispetto alle applicazioni grafiche e sono generalmente utilizzate dagli amministratori di rete per la gestione remota dei dispositivi.

Quesito 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

La soluzione adottata nel quesito precedente è quella di utilizzare un modem-router equipaggiato con due interfacce WAN, una per Internet e l'altra per la subnet 10.100.0.0/28. Il nuovo router fornito dalla società regionale si inserisce in un contesto di rete LAN pre-esistente (così come l'abbiamo ipotizzata in *figura 2*) e viene installato a valle di un firewall 3 legged che protegge la rete interna e realizza una DMZ. Tenendo conto che ciascuna struttura si connette alla rete regionale e accede ai server del data-center per trasmettere i dati dei propri pazienti, occorre integrare e/o modificare le regole impostate sul firewall. In particolare occorre che le regole del firewall non blocchino il traffico interno alla subnet e consentano l'accesso solo agli utenti autorizzati.

Quesito 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

Le principali misure di sicurezza per garantire un trattamento sicuro dei dati sensibili sia durante l'archiviazione che durante i trasferimenti da e per il data center, sono le seguenti:

Archiviazione dei dati nei server del data-center

- Crittografia dei dati: utilizzo di algoritmi di crittografia robusti, come ad esempio l'AES-256
- Controlli di accesso: autenticazione multifattoriale per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili
- Backup sicuri: backup regolari dei dati crittografati e sistemi di disaster recovery

Trasferimento dei dati da e per il data-center

- Crittografia dei dati: utilizzo di protocolli sicuri come TLS/SSL
- Controlli di accesso: procedure sicure per garantire che solo gli utenti e i sistemi autorizzati possano avviare il trasferimento dei dati

Altre misure di sicurezza

- Formazione: buone pratiche sulla sicurezza e il trattamento dei dati sensibili
- GDPR: conformità alle normative sulla sicurezza e la protezione dei dati

La traccia non fornisce indicazioni esplicite riguardo la modalità di trasferimento dei dati dalle strutture sanitarie al data-center regionale. Considerando il notevole numero di strutture sanitarie coinvolte e la qualità dei dati contenuti nei fascicoli elettronici (informazioni testuali ma anche molte immagini e video), si prevede che la quantità di dati da trasferire sia molto elevata. Per questo motivo si ipotizza che i dati vengano trasferiti al data-center in modalità batch: man mano che vengono acquisiti, sono archiviati in un server locale e periodicamente trasferiti a lotti al data-center. Rispetto al trasferimento real time, che prevede che i dati vengano trasmessi al data-center nel momento in cui sono stati generati, la modalità batch garantisce un utilizzo più efficiente della banda di comunicazione.

La schedulazione temporale può dipendere dalle esigenze operative della struttura sanitaria ma anche dalle indicazioni dell'Assessorato regionale: una schedulazione di 60 minuti potrebbe essere un buon compromesso tra l'esigenza di aggiornare i dati e renderli disponibili a cittadini e medici curanti in un tempo accettabile e l'esigenza di effettuare trasferimenti batch sicuri e stabili.

Soluzione seconda parte

Quesito 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

Malfunzionamenti sui sistemi di archiviazione

I malfunzionamenti possono essere hardware (rotture dei server o dei dischi) o software (corruzione dei dati). Principali strategie da adottare:

- server fault tolerant
- sistemi di archiviazione ridondanti RAID
- backup regolari dei dati e sistemi di disaster recovery

Malfunzionamenti della connessione

Il trasferimento dei dati in modalità batch ipotizzato nel quesito 4, prevede che i dati man mano acquisiti vengano archiviati in un server locale e ogni 60 minuti trasferiti a lotti al data-center. Principali strategie da adottare:

- connessione di backup (rete di failover): una rete alternativa, una VPN o un diverso percorso di rete, che si attiva automaticamente se la connessione principale fallisce
- ripristino della connessione: il sistema prova automaticamente a riconnettersi e a riprendere il trasferimento
- ripresa del trasferimento: utilizzo di protocolli quali SFTP, FTPS e Rsync che in caso di interruzione sono in grado di riprendere il trasferimento esattamente dal punto in cui è stato interrotto
- verifica del trasferimento: controllo dell'integrità e della correttezza dei dati trasferiti. Solo a seguito della verifica positiva del trasferimento, i dati del lotto vengono eliminati dal server locale

Quesito 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)

L'autenticazione qualificata a più fattori (MFA - Multi-Factor Authentication) è un metodo di verifica dell'identità che richiede agli utenti di fornire almeno un fattore di autenticazione in aggiunta alla password, o almeno due fattori di autenticazione senza password, prima di consentire l'accesso a un sistema o a un servizio.

Tra le molteplici forme di autenticazione che si possono adottare, è molto diffusa l'autenticazione OTP, utilizzata anche dal Sistema Pubblico di Identità Digitale (SPID) che attualmente è il sistema più semplice e veloce per accedere ai servizi online della Pubblica Amministrazione.

Autenticazione OTP via SMS

Questo metodo richiede all'utente di inserire il proprio numero telefonico durante la registrazione dell'account. Quando l'utente accede con user-name e password, gli viene chiesto di inserire il codice OTP (One-Time Password) inviategli sul suo cellulare tramite SMS. Inserendo il codice può accedere al sistema o al servizio richiesto. L'OTP serve come forma di autenticazione per verificare che l'utente è chi dice di essere perché è in possesso del suo dispositivo.

Questo metodo è comodo da usare ma poco sicuro in quanto i cybercriminali sono in grado di trovare online i numeri di telefono delle persone e di intercettare i messaggi SMS.

Autenticazione TOTP

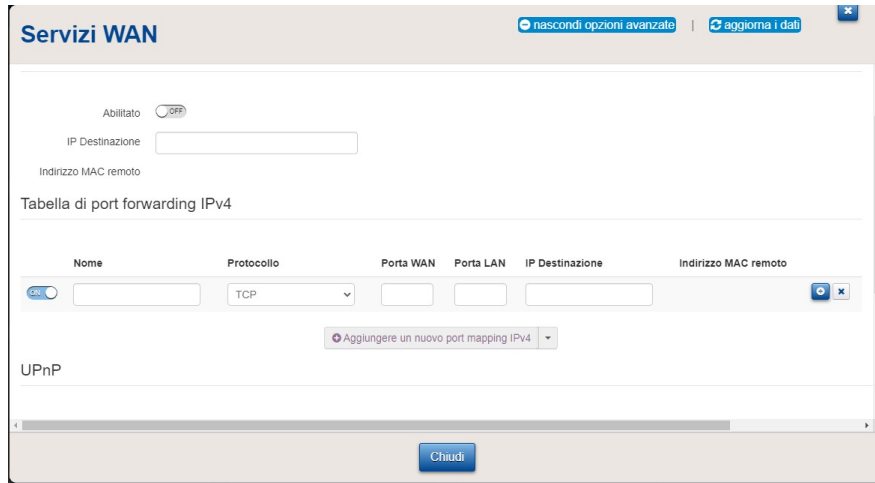
Dopo aver inserito le credenziali, all'utente viene richiesto di verificare la propria identità inserendo il codice TOPT (Time-Based One-Time Password) generato da un'app disponibile sul suo smartphone. L'utente ha tempo 30 o 60 secondi per inserire il TOPT ed essere autenticato e autorizzato ad accedere al sistema o al servizio richiesto.

Questa è una delle forme di autenticazione multifattoriale più sicure, perché i codici hanno durata breve e sono difficili da intercettare.

Token hardware

Un dispositivo elettronico, di piccole dimensioni e dotato di display, visualizza un OPT che l'utente, una volta fornite le proprie credenziali, deve inserire per essere autorizzato ad eseguire le operazioni previste dall'app o dal sito web a cui vuole accedere. Anche questa forma di autenticazione è molto sicura perché il dispositivo non può essere rubato tramite Internet.

Step 3 Entrare nella sezione "Servizi WAN"



Step 4 Aggiungere alla "Tabella di port forwarding IPv4" le seguenti regole:

HTTP (Porta 80)

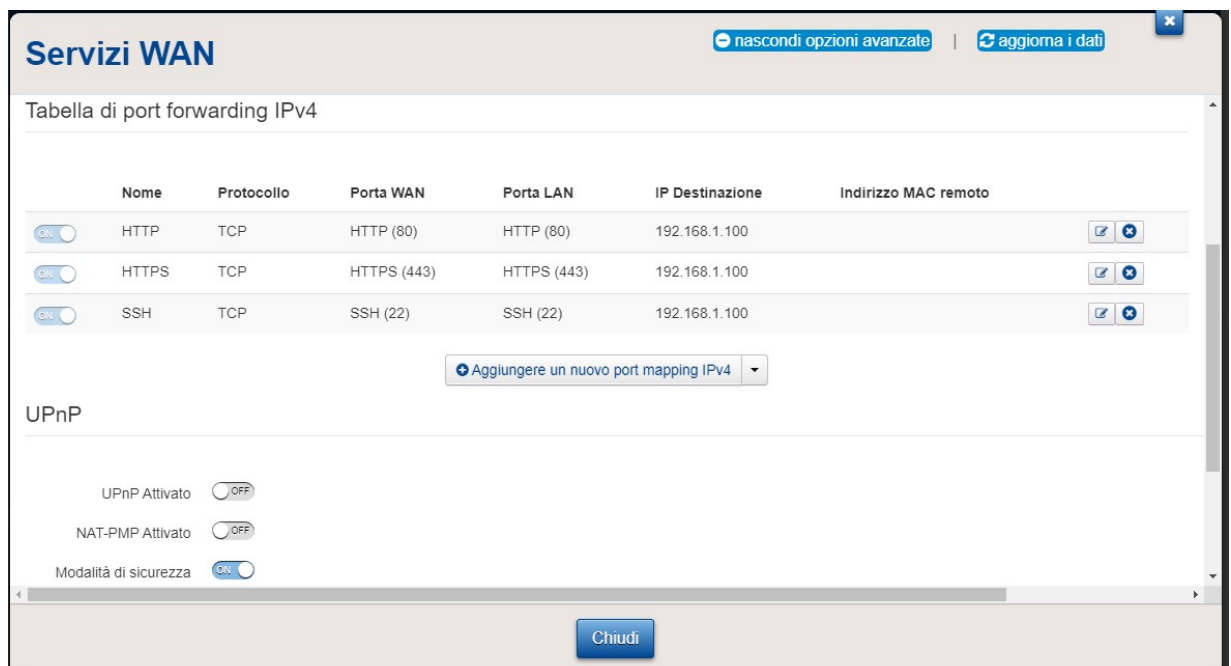
- Nome HTTP
- Protocollo TCP
- Porta WAN 80
- Porta LAN 80
- IP destinazione 192.168.1.100

HTTPS (Porta 443)

- Nome HTTPS
- Protocollo TCP
- Porta WAN 443
- Porta LAN 443
- IP destinazione 192.168.1.100

SSH (Porta 22)

- Nome SSH
- Protocollo TCP
- Porta WAN 22
- Porta LAN 22
- IP destinazione 192.168.1.100



Step 5 Assicurarsi che il firewall del router e il firewall del web server consentano l'accesso alle porte 80, 443 e 22

La configurazione di modelli di router diversi da quello preso a riferimento, ma comunque accessibili tramite un browser web, non presenta particolari difficoltà quantunque i menù, la grafica e i nomi dei campi nei form di inserimento possono essere differenti (ad esempio può essere richiesto "IP Server" al posto di "IP Destinazione" oppure "Porta esterna" al posto di "Porta WAN", ecc).

Si tenga conto inoltre, come già sottolineato nel quesito 2 della prima parte, che molti router professionali vengono configurati tramite la linea di comando (linguaggio CLI)

Quesito IV

All'interno di un'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

Supponendo, come suggerisce il testo del quesito, che la segnalazione provenga da un solo utente della LAN aziendale, escludiamo tra le cause del problema la mancanza generalizzata di connessione a Internet (quindi guasti o malfunzionamenti del modem-router, problemi del Provider, ecc.) e ci concentriamo sulle cause di natura hardware o software che riguardano esclusivamente la postazione di lavoro dell'utente impossibilitato a "navigare su Internet".

Per semplicità ipotizziamo che il tecnico di help-desk, dopo aver raccolto e registrato la segnalazione, intervenga direttamente sul computer dell'utente (dotato di SO Windows 10) attraverso i seguenti passi di diagnosi ed eventuale risoluzione dei problemi riscontrati:

1. verifica se l'utente è connesso alla LAN aziendale attraverso un ping verso l'indirizzo IP del router (il gateway), che abbiamo ipotizzato è 192.168.1.1; sul prompt dei comandi (Start->Esegui->cmd) digita "ping 192.168.1.1"
2. se il ping fallisce:
 - a. controlla che il cavo di rete non sia danneggiato e risulti stabilmente collegato al computer e allo switch di rete. Eventualmente sostituisce il cavo o ripristina i collegamenti
 - b. sull'app "Gestione dispositivi" (Start->Gestione dispositivi) verifica il buon funzionamento della scheda di rete. Eventualmente reinstalla la scheda o la sostituisce
 - c. se non si tratta di un problema di cavi o di scheda di rete, controlla che le impostazioni IP siano corrette (Start->Connessioni di rete->Ethernet). Eventualmente reimposta l'indirizzo IP della scheda di rete o l'indirizzo IP del gateway (il router)
3. se il ping ha esito positivo, ovvero se l'utente è connesso alla LAN aziendale ma non naviga:
 - d. controlla che la risoluzione dei nomi di un dominio, il DNS (Domain Name System), funzioni correttamente. A tal fine sul prompt dei comandi (Start->Esegui->cmd) digita "nslookup www.google.com" oppure "nslookup www.maurodeberardis.it" :-)
Se la risoluzione DNS fallisce, controlla che il server DNS sia correttamente configurato e regolarmente in funzione.
Eventualmente modifica le impostazioni IP (Start->Connessioni di rete->Ethernet) inserendo gli indirizzi di un server DNS sicuramente affidabile (ad esempio 8.8.8.8 e 8.8.4.4)