

## Esemplare per gli esperti

<b>90</b>	<b>Minuti</b>	<b>25</b>	<b>Compiti</b>	<b>27</b>	<b>Pagine</b>	<b>87</b>	<b>Punti</b>
-----------	---------------	-----------	----------------	-----------	---------------	-----------	--------------

### Mezzi ausiliari consentiti:

- Scalimetro, squadra geometrica e sciablona.
- Calcolatrice tascabile, indipendente dalla rete (tablet, smartphone, ecc. non sono ammessi)

### Valutazione – Per il punteggio pieno si richiede:

- La formula completa o l'equazione dimensionale.
- Le cifre esposte con l'unità di misura.
- La soluzione deve essere chiara e comprensibile.
- Il risultato finale marcato con una doppia sottolineatura e con l'unità di misura.
- Il numero delle risposte stabilito in un dato compito è vincolante.
- Le risposte sono valutate nell'ordine dato.
- Le risposte in esubero non vengono valutate.
- In mancanza di spazio, utilizzare il retro del foglio.  
Scrivere vicino al compito una nota, ad es. soluzione vedi retro.
- **Errori di riporto non portano a una detrazione.**

### Scala delle note

<b>6</b>	<b>5,5</b>	<b>5</b>	<b>4,5</b>	<b>4</b>	<b>3,5</b>	<b>3</b>	<b>2,5</b>	<b>2</b>	<b>1,5</b>	<b>1</b>
87,0-83,0	82,5-74,0	73,5-65,5	65,0-57,0	56,5-48,0	47,5-39,5	39,0-30,5	30,0-22,0	21,5-13,5	13,0-4,5	4,0-0,0

### Periodo di restrizione:

**Questa prova d'esame non può essere usata per scopi di esercizio prima del 1° settembre 2024.**

### Elaborato da:

Gruppo di lavoro PQ dell'EIT.swiss per la professione di telematica AFC e telematico AFC

### Editore:

CSFO, dipartimento per le procedure di qualificazione, Berna

		Punti
<b>1. Videoconferenza Obiettivo di valutazione n. 5.1.1 B2</b>		<b>3</b>
Home-Office e Mobile-Office richiedono applicativi per la collaborazione che permettano la videoconferenza. In più, le applicazioni aziendali, operando attraverso reti private e pubbliche, vedono spesso compromesse la qualità e la disponibilità.		
a) Quali sono due comuni cause per la scarsa qualità dell'immagine e del suono nelle reti domestiche?	<ul style="list-style-type: none"><li>- <b>WiFi, discontinuo e con larghezza di banda troppo bassa a causa di Access Points datati.</b></li><li>- <b>Connessione Internet, upload con banda passante troppo bassa.</b></li></ul> <div>Nota per gli esperti: Sono possibili anche altre soluzioni.</div>	1
b) Descrivere un modo per migliorare l'immagine senza sostituire la rete.	<ul style="list-style-type: none"><li>- <b>Scegliere una risoluzione più bassa, riducendo così anche il fabbisogno di banda passante.</b></li></ul> <div>Nota per gli esperti: Sono possibili anche altre soluzioni.</div>	1
c) Come migliorare la ripresa video con misure ambientali (senza adeguamenti alla rete o IT)? Indicare due possibilità.	<ul style="list-style-type: none"><li>- <b>Nessuna fonte di luce intensa nel campo della telecamera</b></li><li>- <b>Illuminare il volto dal davanti.</b></li><li>- <b>Posizionare la telecamera centralmente sullo schermo, in modo che l'altro abbia l'impressione di essere guardato.</b></li></ul> <div>Nota per gli esperti: Sono possibili anche altre soluzioni.</div>	1
		<b>Punti per pagina:</b>

		Punti
<b>2. SIP Trace</b>	<b>Obiettivo di valutazione n. 5.2.2 B2</b>	<b>5</b>
a)	Un telefono SIP Yealink (LLDP non attivo) è collegato per la prima volta a una rete IP. Quali valori possono essere identificati usando Wireshark-Trace?	2
Completare dove necessario.		
<ul style="list-style-type: none"><li>• Source MAC Address: ca:13:d3:a2:03:34</li><li>• Destination MAC Address: <b>FF:FF:FF:FF:FF:FF</b></li><li>• Source Port: <b>68</b></li><li>• Destination Port: <b>67</b></li><li>• Source IP Address: <b>0.0.0.0</b></li><li>• Destination IP Address: 255.255.255.255</li></ul>		

Punti  
per  
pagina:

- b) Avviando Wireshark-Trace si ottengono le seguenti richieste DNS in ordine cronologico:

1. richiesta:

2. richiesta:

172.16.52.106	10.240.2.30	DNS	75 Standard query 0x1716 A cn.pool.ntp.org
172.16.52.106	10.240.2.30	DNS	75 Standard query 0x1716 A cn.pool.ntp.org
172.16.52.106	172.16.52.30	DNS	75 Standard query 0x1716 A cn.pool.ntp.org
172.16.52.106	172.16.52.30	DNS	75 Standard query 0x1716 A cn.pool.ntp.org
172.16.52.30	172.16.52.106	DNS	139 Standard query response 0x1716 A cn.pool.ntp.org A 162.159.200.123 A 84.16.67.12 A 84.16.73.33 A 94.130.49.186
172.16.52.30	172.16.52.106	DNS	139 Standard query response 0x1716 A cn.pool.ntp.org A 162.159.200.123 A 84.16.67.12 A 84.16.73.33 A 94.130.49.186
10.240.2.30	172.16.52.106	DNS	139 Standard query response 0x1716 A cn.pool.ntp.org A 84.16.73.33 A 193.182.111.142 A 120.25.115.20 A 162.159.200.1
10.240.2.30	172.16.52.106	DNS	139 Standard query response 0x1716 A cn.pool.ntp.org A 84.16.73.33 A 193.182.111.142 A 120.25.115.20 A 162.159.200.1
172.16.52.106	10.240.2.30	DNS	80 Standard query 0xd20b A rpscloud.yealink.com
172.16.52.106	10.240.2.30	DNS	80 Standard query 0xd20b A rpscloud.yealink.com
172.16.52.106	10.240.2.30	DNS	80 Standard query 0xd20b A rpscloud.yealink.com
172.16.52.106	10.240.2.30	DNS	80 Standard query 0xd20b A rpscloud.yealink.com
10.240.2.30	172.16.52.106	DNS	96 Standard query response 0xd20b A rpscloud.yealink.com A 3.124.165.251
10.240.2.30	172.16.52.106	DNS	96 Standard query response 0xd20b A rpscloud.yealink.com A 3.124.165.251
172.16.52.30	172.16.52.106	DNS	96 Standard query response 0xd20b A rpscloud.yealink.com A 3.124.165.251
172.16.52.30	172.16.52.106	DNS	96 Standard query response 0xd20b A rpscloud.yealink.com A 3.124.165.251
172.16.52.106	172.16.52.30	ICMP	124 Destination unreachable (Port unreachable)

Spiegare le due richieste DNS:

**Il telefono chiede l'indirizzo IP del servizio NTP.**

La prima richiesta chiede al servizio DNS di risolvere l'indirizzo IP del servizio NTP configurato nel telefono.

**Il telefono chiede l'indirizzo IP del server per il provisioning.**

La seconda richiesta chiede al server DNS di risolvere l'indirizzo IP del servizio Yealink Redirection and Provisioning (RPS) anch'esso configurato nel telefono. Ciò permette al telefono di ottenere il suo URL di provisioning.

- c) Al resto della cronologia del Wireshark-Trace, è applicato un filtro per identificare i pacchetti HTTP e visualizzare il seguente scambio tra il telefono IP e l'IP PBX.

1

Source	Destination	Protocol	Length	Info
172.16.52.106	172.16.52.250	HTTP	213	GET /provisioning/z3aa0e2c12t1/805ec04e57fd.boot HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	175	HTTP/1.1 404 Not Found
172.16.52.106	172.16.52.250	HTTP	214	GET /provisioning/z3aa0e2c12t1/y00000000000000000000.boot HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	175	HTTP/1.1 404 Not Found
172.16.52.106	172.16.52.250	HTTP	213	GET /provisioning/z3aa0e2c12t1/y00000000000000000096.cfg HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	677	HTTP/1.1 200 OK
172.16.52.106	172.16.52.250	HTTP	212	GET /provisioning/z3aa0e2c12t1/805ec04e57fd.cfg HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	356	HTTP/1.1 200 OK
172.16.52.106	172.16.52.250	HTTP	215	GET /provisioning/z3aa0e2c12t1/logo/yealinkt46.png HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	1452	HTTP/1.1 200 OK (PNG)
172.16.52.106	172.16.52.250	HTTP	215	GET /provisioning/z3aa0e2c12t1/logo/yealinkt46.png HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	1452	HTTP/1.1 200 OK (PNG)
172.16.52.106	172.16.52.250	HTTP	217	GET /provisioning/z3aa0e2c12t1/Directory_setting.xml HTTP/1.1
172.16.52.250	172.16.52.106	HTTP/XML	1413	HTTP/1.1 200 OK [Malformed Packet]
172.16.52.106	172.16.52.250	HTTP	265	GET /provisioning/z3aa0e2c12t1/firmware/yealink/patcht54w(t57M, T53M, T53, T53C, T54, T57)-96.86.0.23.rom HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	217	GET /provisioning/z3aa0e2c12t1/yealink_phonebook.xml HTTP/1.1
172.16.52.106	172.16.52.250	HTTP/XML	1267	HTTP/1.1 200 OK
172.16.52.250	172.16.52.106	HTTP	217	GET /provisioning/z3aa0e2c12t1/yealink_phonebook.xml HTTP/1.1
172.16.52.106	172.16.52.250	HTTP/XML	1267	HTTP/1.1 200 OK

Dare una descrizione di questo scambio in rete.

**È la prima registrazione del telefono IP sull'IP PBX e la conseguente richiesta del telefono di vari file (file di configurazione del telefono, firmware, rubrica telefonica, logo, ...).**

**Il PBX fornisce questi file in modo che il telefono possa configurarsi correttamente.**

**Nota per gli esperti:  
Sono possibili anche altre soluzioni.**

**3. Trasmissione senza fili Obiettivo di valutazione n. 5.3.2 B2**

**3**

Assegnare le seguenti caratteristiche alla rispettiva tecnologia:  
(risposte multiple non possibili)

<u>Frequenza</u>	<u>Velocità dati max.</u>	<u>Portata in campo libero</u>
A) da 863 MHz a 870 MHz	a) ca. 50 kbit/s	1) 10 m
B) 1.8 GHz	b) ca. 2 Mbit/s	2) 50 m
C) da 2.40 GHz a 2.48 GHz	c) ca. 1 Gbit/s	3) qualche chilometro
D) 5 GHz	d) ca. 10 Gbit/s	4) 80 km

Inserire lettere e numeri nella tabella.

<b>Tecnologia</b>	<b>Frequenza</b>	<b>Velocità dati</b>	<b>Portata</b>
Wi-Fi 6 (WLAN 802.11ax)	<b>D</b>	<b>d</b>	<b>2</b>
LoRa	<b>A</b>	<b>a</b>	<b>3</b>
Bluetooth-Versione 2	<b>C</b>	<b>b</b>	<b>1</b>

1

1

1

**Nota per gli esperti:**  
**1 punto per ogni riga completa.**  
**0,5 punti per 2 risposte esatte su 3 per riga.**

**4. Trasmissione dati Obiettivo di valutazione n. 5.1.1 B2**

**2**

Un cliente ha una connessione Internet con download massimo di 300 Mbit/s e upload massimo di 100 Mbit/s. Il cliente attiva un backup (dimensione del file 150 GB) durante la notte che deve essere completato entro le 06h00.  
A che ora al più tardi deve essere avviato il backup?

Nota:

Il throughput aggiuntivo derivante dalle intestazioni dei pacchetti non viene preso in considerazione.

**Il backup deve essere avviato al più tardi alle 02:40.**

**Soluzione:**

**Tempo di trasmissione = Dimensione del file / Velocità di Upload**

**Dimensione del file:**

**$150 \text{ GB} = 150 \cdot 10^9 \text{ Byte} = 150 \cdot 10^9 \cdot 8 \text{ Bit} = 1,2 \cdot 10^{12} \text{ Bit}$**

**Velocità di Upload:**

**$100 \text{ Mbit/s} = 1 \cdot 10^8 \text{ Bit/s}$**

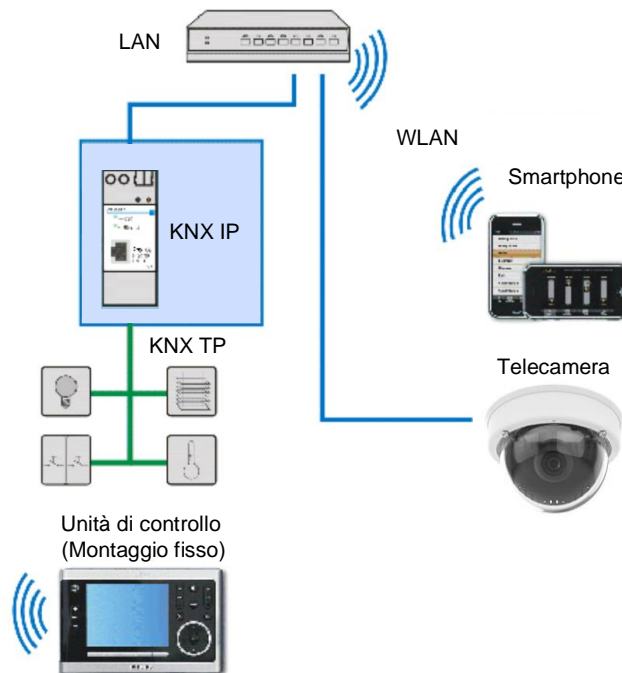
**$\text{Tempo di trasmissione} = 1,2 \cdot 10^{12} \text{ Bit} / 1 \cdot 10^8 \text{ Bit/s} = 12'000 \text{ secondi}$**

**$12'000 \text{ secondi} = 200 \text{ minuti}$**

**5. Sistemi esterni Obiettivo di valutazione n. 5.4.4 B2**

**3**

A causa dei cali di tensione, un sistema di gestione domotico deve essere reso indipendente dalla rete 230 V. L'impianto deve funzionare senza limitazioni e le immagini della telecamera devono sempre essere trasmesse allo smartphone e all'unità di controllo.



a) Quali quattro componenti devono essere collegati all'UPS?

**2**

- LAN Switch
- Unità di controllo
- KNX IP Gateway
- Alimentazione KNX
- Telecamera

b) Quali condizioni deve soddisfare il collegamento della telecamera?

**1**

- La telecamera e lo switch devono essere PoE
- Alimentazione telecamera
- Alimentazione iniettore PoE

**Nota per gli esperti:**  
Sono possibili anche altre soluzioni.

**Punti**

**6. Interfacce Obiettivo di valutazione n. 5.6.1 B2**

**5**

a) Spuntare vero o falso per ogni affermazione sui moduli SFP.

Vero	Falso	Affermazione
	<b>X</b>	I moduli SFP sono utilizzati esclusivamente per collegare cavi dati singlemode e multimode.
<b>X</b>		I moduli SFP possono essere installati durante il funzionamento.
	<b>X</b>	I moduli SFP+ possono essere installati in uno slot SFP.
	<b>X</b>	Direct Attached Cable (DAC) possono essere usati solo per SFP+.
<b>X</b>		Già all'acquisto di un modulo SFP+ occorre decidere se il modulo sarà usato in SM o MM.
<b>X</b>		Solo con i moduli QSFP si può raggiungere una velocità di trasmissione di 40 Gbps.

0,5

0,5

0,5

0,5

0,5

0,5

b) Spuntare vero o falso per ogni affermazione sui balun.

Vero	Falso	Affermazione
<b>X</b>		Il balun è un dispositivo per l'adattamento tra una linea bilanciata e una linea sbilanciata.
<b>X</b>		Con un balun si possono adattare le impedenze.
<b>X</b>		I balun sono spesso utilizzati con connettori BNC o IEC.
	<b>X</b>	I balun aumentano la sicurezza della rete, in quanto possono trasmettere solo unidirezionalmente.

0,5

0,5

0,5

0,5

**Punti  
per  
pagina:**



**Punti**

**7. Ethernet Obiettivo di valutazione n. 5.6.2 B2**

**2**

Si vuole equipaggiare un ufficio con un moderno impianto Wi-Fi. Per garantire una trasmissione ottimale di dati e voce si utilizzano Access Point dell'ultima generazione Wi-Fi 6 Wave 2.

- a) Quale tecnologia LAN dovrebbe essere utilizzata per ottenere le massime prestazioni?

0,5

**Multigigabit Ethernet**

- b) Quale standard di trasmissione regola l'IEEE 802.3bz?

0,5

**2.5 GBase-T**

**5 GBase-T (IEEE 802.3bz)**

- c) Qual è il vantaggio dello standard IEEE 802.3bz in termini di cablaggio LAN?

1

**I cavi Cat 5e o Cat 6 esistenti possono essere riutilizzati, non è quindi necessario un nuovo cablaggio.**

**Punti  
per  
pagina:**

**8. Tipi di Hypervisor Obiettivo di valutazione n. 5.5.2 B2**

2

A quale tipo di Hypervisor appartengono le seguenti proprietà?

Proprietà	Tipo 1	Tipo 2
Preferibile per lo sviluppo e i test.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Impiego in ambienti produttivi.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
L'Hypervisor è eseguito come applicazione in un sistema operativo.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L'Hypervisor è eseguito direttamente sull'hardware dell'host.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

**9. Mobilità in sede Obiettivo di valutazione n. 5.3.1 B2**

2

Alcuni anni fa, un'azienda industriale ha implementato l'intera comunicazione vocale con Voice over Wi-Fi, in modo da avere una sola rete IP su tutta l'area e smantellare l'intero cablaggio telefonico. Sfortunatamente, sono emersi ripetuti problemi di comunicazione causati da spostamenti di grandi oggetti metallici. Ora questa azienda vorrebbe utilizzare una tecnologia radio in-house vocale stabile (non 4G / 5G) senza dover adattare nuovamente il cablaggio.

a) Che tecnologia proporre?

1

**- IP-DECT o SIP-DECT**

b) Indicare due vantaggi di questa tecnologia.

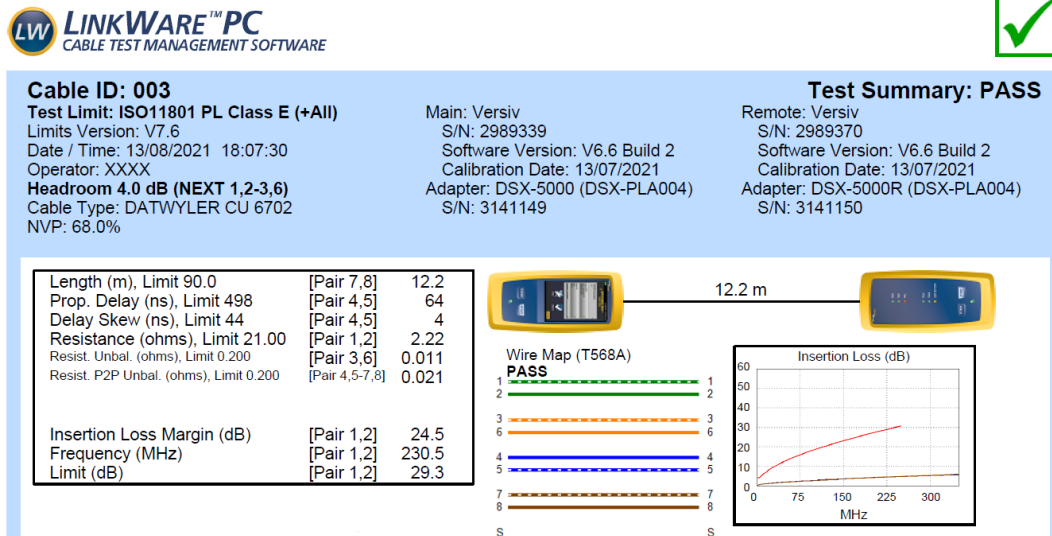
1

- Rete radio resistente alle interferenze in uno spettro di frequenza riservato
- Roaming senza interruzioni tra le stazioni di base
- Sicurezza attraverso la crittografia del collegamento radio
- Alta densità di chiamate senza perdita di qualità
- I trasmettitori possono essere collegati al server di telefonia tramite una rete IP
- Alimentazione dei trasmettitori tramite switch PoE
- Il cablaggio LAN degli AP WLAN può continuare ad essere utilizzato

**10. CUC Obiettivo di valutazione n. 5.1.6 B1**

5

Dalla misura di un collegamento CUC, lo strumento emette il seguente rapporto.



a) A cosa prestare attenzione anche se il test è stato superato? Indicare quattro aspetti essenziali per la qualità del risultato.

2

- **Data di calibrazione**
- **Versione del software**
- **Limits-Version**
- **Protocollo di test scelto**
- **tipo di cavo usato**
- **Valore NVP**

**Nota per gli esperti:**  
Sono possibili anche altre soluzioni.

b) Indicare il significato dei termini "Prop. Delay (ns)" e "Delay Skew (ns)" e spiegarli in relazione a questa misura.

2

- **Prop. Delay:** velocità di propagazione del segnale in una coppia di conduttori. Nel caso specifico la coppia più lenta è la 4-5. Determina la trasmissione effettiva del segnale.

- **Delay Skew:** differenza di velocità di propagazione tra la coppia di conduttori più veloce e quella più lenta.

c) Perché la differenza tra coppie di segnali è importante per le reti ad alta velocità?

1

La differenza è importante perché diverse tecnologie di rete ad alta velocità, tra cui Gigabit Ethernet, utilizzano tutte e quattro le coppie di conduttori. Se la differenza di una o più coppie di conduttori è molto diversa dalle altre, i segnali inviati simultaneamente da un'estremità del cavo possono giungere all'altro capo in tempi molto diversi e benché i ricevitori siano progettati per compensare piccoli ritardi, una variazione troppo grande rende impossibile la ricreazione del segnale originale.

**Nota per gli esperti:**  
Sono possibili anche altre soluzioni.

**Punti**

**11. Telefonia mobile 5G Obiettivo di valutazione n. 5.3.2 B2**

**3**

Lo standard di comunicazione 5G è un'evoluzione del 4G. Durante il suo sviluppo, l'attenzione è stata posta sui requisiti delle future applicazioni mobili come il gioco online, gli occhiali VR e le auto a guida autonoma.

a) Indicare quattro differenze tra le tecnologie di rete 4G e 5G.

**2**

- **Tempo di latenza**
- **Possibili velocità di download**
- **Stazioni di base multiple**
- **Modulazione OFDM**
- **Densità delle celle**
- **Beamforming**

**Nota per gli esperti:  
Sono possibili anche altre soluzioni.**

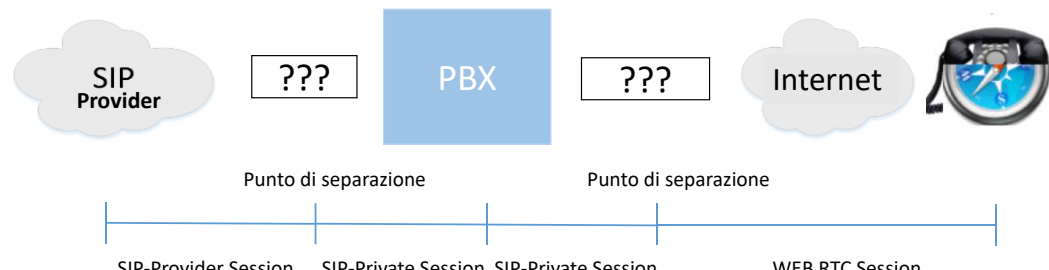
b) Qual è la caratteristica più importante per l'implementazione delle applicazioni menzionate sopra?

**1**

**Tempo di latenza**

**Nota per gli esperti:  
(tempo di risposta), 5G ha un tempo di latenza di 1 ms  
(4G si situa nell'intervallo tra 60 – 98 ms).**

**Punti  
per  
pagina:**

	Punti
<p><b>12. Struttura Telematica Obiettivo di valutazione n. 5.4.1 B2</b></p> <p>a) Spiegare le funzioni (compiti) dei seguenti componenti.</p> <p>SBC:</p> <p><b>L'SBC (Session Border Controller) agisce come elemento di sicurezza tra il provider SIP e l'infrastruttura del cliente. A tal scopo, può svolgere anche altre funzioni come le manipolazioni SIP o le conversioni Codec.</b></p> <p>WebRTC Gateway:</p> <p><b>Il gateway WebRTC funge da interfaccia tra i client di telefonia basati su WebRTC e il sistema telefonico. Questo gateway fa la traduzione da WebRTC al protocollo SIP.</b></p> <p>DSLAM:</p> <p><b>Il "Digital Subscriber Line Access Multiplexer"(abbreviato DSLAM) fa parte dell'infrastruttura necessaria al funzionamento della DSL. I DSLAM si trovano nel punto in cui convergono le linee d'abbonato.</b></p> <p>b) Quali due dei suddetti componenti sono utilizzati nello scenario seguente?</p>  <p><b>SBC</b></p> <p><b>WebRTC Gateway</b></p>	<p>4</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p>
Punti per pagina:	

Punti

**13. SNMP Obiettivo di valutazione n. 5.5.4 B2**

**4**

- a) Spiegare cosa sono i pacchetti dati Trap SNMP.

**1**

**Messaggi non richiesti inviati da un agente SNMP al gestore SNMP a causa del superamento di un valore nominale preimpostato.**

- b) Cos'è un file MIB?

**1**

**Un file MIB (Management Information Base) è una banca dati che descrive le informazioni sui dispositivi nel protocollo SNMP. Vi sono memorizzati i parametri variabili del dispositivo (dati tecnici, ecc.) e gli allarmi che può attivare. Il Browser MIB può quindi leggerli e visualizzarli.**

- c) SNMPv3 è utilizzato per monitorare i dispositivi di una rete.  
Spuntare per ogni affermazione ciò che fa al caso.

Affermazioni	Vero	Falso	
Un agente SNMP software o hardware deve essere attivo su tutti i dispositivi da monitorare.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5
Oltre al monitoraggio, SNMP può essere usato anche per configurare o controllare da remoto i dispositivi.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5
SNMP consente la crittografia dei dati tra gli agenti e il gestore.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5
SNMP si basa su TCP per stabilire connessioni sicure tra l'agente e il gestore.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0,5

Punti  
per  
pagina:

**Punti**

**14. Connessione Obiettivo di valutazione n. 5.5.4 B2**

**5**

**2**

- a) Un nuovo IP PBX è stato installato. La salvaguardia dei dati del nuovo sistema deve essere sicura, automatica ed esternalizzata.  
Descrivere brevemente due possibili soluzioni.

- **IP PBX memorizza direttamente nel cloud (SFTP)**
- **IP PBX memorizza su uno storage locale (NAS, Server), che sincronizza con il cloud (S3).**
- **Invio del backup per e-mail**

**Nota per gli esperti:  
Lista non esaustiva.**

- b) Analizzare le due immagini Wireshark a pagina 16.  
Nota: l'indirizzo IP 172.16.52.250 è l'indirizzo del IP PBX.

A cosa si riferisce l'indirizzo IP 172.16.52.63?

**1**

**È il Server FTP, che utilizza il protocollo SFTP.**

Che sequenza mostra la figura 1 e quali sono le porte utilizzate?

**1**

**Porta IP PBX casuale : 46660 (TCP)**

**Porta server SFTP: 22 (TCP)**

**Si tratta dell'inizializzazione di una comunicazione tramite protocolli TCP e SSH tra l'IP PBX e un server SFTP.**

Che sequenza mostra la figura 2 e quali sono le porte utilizzate?

**1**

**Porta IP PBX casuale: 35370 (TCP)**

**Porta server SFTP: 61322 (TCP)**

**È la trasmissione di pacchetti criptati tra il PBX e un server SFTP.**

**Nota per gli esperti:  
0,5 punti per le porte corrette.  
0,5 punti per la descrizione corretta.**

**Punti  
per  
pagina:**

Figura 1:

5574 88.535248	172.16.52.250	172.16.52.63	TCP	74 46660 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=978622874 TSecr=0 WS=128
5575 88.535248	172.16.52.250	172.16.52.63	TCP	74 [TCP Out-Of-Order] 46660 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=978622874 TSecr=0 WS=128
5576 88.535281	172.16.52.63	172.16.52.250	TCP	74 22 → 46660 [SYN, ACK] Seq=0 Ack=1 Win=13158 Len=0 MSS=1474 SACK_PERM=1 TSval=3848272672 TSecr=3848272672
5577 88.535281	172.16.52.63	172.16.52.250	TCP	74 [TCP Out-Of-Order] 22 → 46660 [SYN, ACK] Seq=0 Ack=1 Win=13158 Len=0 MSS=1474 SACK_PERM=1 TSval=3848272672 TSecr=3848272672
5578 88.535312	172.16.52.250	172.16.52.63	TCP	66 46660 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=978622875 TSecr=3848272672
5579 88.535312	172.16.52.250	172.16.52.63	TCP	66 [TCP Dup ACK 5578#1] 46660 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=978622875 TSecr=3848272672
5580 88.540821	172.16.52.250	172.16.52.63	SSHv2	104 Client: Protocol (SSH-2.0-Renci.SshNet.0.0.1)
5581 88.540821	172.16.52.250	172.16.52.63	TCP	104 [TCP Retransmission] 46660 → 22 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=38 TSval=978622881 TSecr=3848272672
5582 88.540887	172.16.52.63	172.16.52.250	TCP	66 22 → 46660 [ACK] Seq=1 Ack=39 Win=13184 Len=0 TSval=978622881 TSecr=3848272672
5583 88.540887	172.16.52.63	172.16.52.250	TCP	66 [TCP Dup ACK 5582#1] 22 → 46660 [ACK] Seq=1 Ack=39 Win=13184 Len=0 TSval=978622881 TSecr=3848272672
5587 88.576716	172.16.52.63	172.16.52.250	SSHv2	87 Server: Protocol (SSH-2.0-OpenSSH 8.2)
5588 88.576716	172.16.52.63	172.16.52.250	TCP	87 [TCP Retransmission] 22 → 46660 [PSH, ACK] Seq=1 Ack=39 Win=13184 Len=21 TSval=3848272713 TSecr=3848272672
5589 88.576780	172.16.52.250	172.16.52.63	TCP	66 46660 → 22 [ACK] Seq=39 Ack=22 Win=64256 Len=0 TSval=978622916 TSecr=3848272713
5590 88.576780	172.16.52.250	172.16.52.63	TCP	66 [TCP Dup ACK 5589#1] 46660 → 22 [ACK] Seq=39 Ack=22 Win=64256 Len=0 TSval=978622916 TSecr=3848272713
5591 88.577006	172.16.52.63	172.16.52.250	SSHv2	1122 Server: Key Exchange Init
5592 88.577006	172.16.52.63	172.16.52.250	TCP	1122 [TCP Retransmission] 22 → 46660 [PSH, ACK] Seq=22 Ack=39 Win=13184 Len=1056 TSval=3848272713 TSecr=3848272672

Figura 2:

9001 151.313459	172.16.52.250	172.16.52.63	TCP	74 35370 → 61322 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=978685653 TSecr=0 WS=128
9002 151.313459	172.16.52.250	172.16.52.63	TCP	74 [TCP Out-Of-Order] 35370 → 61322 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=978685653 TSecr=0 WS=128
9003 151.313838	172.16.52.63	172.16.52.250	TCP	74 61322 → 35370 [SYN, ACK] Seq=0 Ack=1 Win=13158 Len=0 MSS=1474 SACK_PERM=1 TSval=3848335452 TSecr=3848335452
9004 151.313838	172.16.52.63	172.16.52.250	TCP	74 [TCP Out-Of-Order] 61322 → 35370 [SYN, ACK] Seq=0 Ack=1 Win=13158 Len=0 MSS=1474 SACK_PERM=1 TSval=3848335452 TSecr=3848335452
9005 151.313993	172.16.52.250	172.16.52.63	TCP	66 35370 → 61322 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=978685654 TSecr=3848335452
9006 151.313993	172.16.52.250	172.16.52.63	TCP	66 [TCP Dup ACK 9005#1] 35370 → 61322 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=978685654 TSecr=3848335452
9011 151.355837	172.16.52.63	172.16.52.250	TCP	87 61322 → 35370 [PSH, ACK] Seq=1 Ack=1 Win=13184 Len=21 TSval=3848335493 TSecr=978685654
9012 151.355837	172.16.52.63	172.16.52.250	TCP	87 [TCP Retransmission] 61322 → 35370 [PSH, ACK] Seq=1 Ack=1 Win=13184 Len=21 TSval=3848335493 TSecr=978685654
9013 151.355900	172.16.52.250	172.16.52.63	TCP	66 35370 → 61322 [ACK] Seq=1 Ack=22 Win=64256 Len=38 TSval=978685695 TSecr=3848335493
9014 151.355900	172.16.52.250	172.16.52.63	TCP	66 [TCP Dup ACK 9013#1] 35370 → 61322 [ACK] Seq=1 Ack=22 Win=64256 Len=38 TSval=978685695 TSecr=3848335493
9028 152.157484	172.16.52.250	172.16.52.63	TCP	104 35370 → 61322 [PSH, ACK] Seq=1 Ack=22 Win=64256 Len=38 TSval=978686496 TSecr=3848335493
9029 152.157484	172.16.52.250	172.16.52.63	TCP	104 [TCP Retransmission] 35370 → 61322 [PSH, ACK] Seq=1 Ack=22 Win=64256 Len=38 TSval=978686496 TSecr=3848335493
9030 152.157543	172.16.52.63	172.16.52.250	TCP	66 61322 → 35370 [ACK] Seq=22 Ack=39 Win=13184 Len=0 TSval=3848336295 TSecr=978686496
9031 152.157543	172.16.52.63	172.16.52.250	TCP	66 [TCP Dup ACK 9030#1] 61322 → 35370 [ACK] Seq=22 Ack=39 Win=13184 Len=0 TSval=3848336295 TSecr=978686496
9032 152.158183	172.16.52.63	172.16.52.250	TCP	1122 61322 → 35370 [PSH, ACK] Seq=22 Ack=39 Win=13184 Len=1056 TSval=3848336296 TSecr=978686496



	Punti
<b>15. Backup Obiettivo di valutazione n. 5.5.4 B2</b>	<b>5</b>
a) Una delle strategie di backup si basa sulla regola 3-2-1. Cosa sta dietro ogni singolo numero?	
3: <b>possedere almeno tre copie dei dati da salvaguardare.</b>	0,5
2: <b>avere le copie su due supporti diversi.</b>	0,5
1: <b>conservare una copia del backup in un luogo esterno.</b>	0,5
b) Spiegare il principio di generazione (nonno-padre-figlio) nei backup.	1
<b>In concreto significa che per la settimana di cinque giorni, per i primi quattro giorni lavorativi si usano dei nastri-figlio, l'ultimo giorno lavorativo un nastro-padre.</b>	
<div style="border: 1px solid black; padding: 5px;"> <b>Nota per gli esperti:</b>  <b>Ogni venerdì, cioè quattro volte al mese, si usa il nastro-padre e l'ultimo giorno del mese viene utilizzato il nastro-nonno.</b> </div>	
c) Cos'è la deduplicazione?	1
<b>La deduplicazione descrive una procedura per analizzare i dati memorizzati più volte, che sono molto simili o identici, ed eliminare le ridondanze, risparmiando così spazio d'archiviazione visto che i dati multipli sono sostituiti da segnaposti costituiti da indirizzi di riferimento.</b>	
d) Un server registra un backup completo ogni venerdì alle 20:00 e un backup incrementale dal lunedì al giovedì alla stessa ora. Ogni backup è memorizzato su nastri separati. Il server subisce un guasto alle 14:00 di mercoledì. Quanti nastri sono necessari per il ripristino? Il ripristino inizia alle 08:00 di giovedì e termina alle 11:00 dello stesso giorno. Quanto durano l'RPO e l'RT0?	
Numero di nastri: <b>3 (Full + MO + DI)</b>	0,5
RPO: <b>18h</b>	0,5
RT0: <b>21h</b>	0,5
	<b>Punti per pagina:</b>

Punti

**16. PBX in un centro di calcolo esterno Obiettivo di valutazione n. 5.4.1 B2**

4

Un cliente desidera installare un nuovo centralino telefonico presso il centro di calcolo di un provider. Il centro di calcolo è completamente virtuale, non è perciò possibile installare componenti hardware.

- a) Quale componente di rete è particolarmente importante nell'installazione di questo centralino per collegare in modo sicuro il SIP trunk al Call server senza che i dati circolino su Internet ma restino nella rete del provider?

1

**Session Border Controller (SBC), per collegare reti di dati esterne (non sicure) con strutture IT interne (sicure) e implementare le cosiddette sessioni.**

- b) Quale tecnologia può essere utilizzata all'interno dell'azienda per collegare i telefoni cellulari al nuovo centralino?  
Spuntare ciò che fa al caso.

Tecnologia	Si	No
WiFi Access Point	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IP-DECT Basis Station	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DECT Basis Station (TDM), due fili	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Rete pubblica 4G / 5G attraverso VPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

- c) Quali sono due aspetti da considerare nella comunicazione tra l'azienda e il centro di calcolo?

1

- **Sicurezza (tramite crittografia o con una VPN o l'uso di TLS / SRTP)**
- **Qualità (sufficiente larghezza di banda in upload dalla sede aziendale)**

**Nota per gli esperti:  
Sono possibili anche altre soluzioni.**

Punti  
per  
pagina:

Punti

**17. Protezione dei dati Obiettivo di valutazione n. 5.5.5 B1**

**4**

- a) Spuntare quali dati personali sono da proteggere e quali no.

Dati su:	Da proteggere	Da non proteggere
Attività o convinzioni religiose, ideologiche, politiche o sindacali.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Salute, sfera personale o appartenenza razziale.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Misure dell'aiuto sociale.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Procedimenti o sanzioni amministrative o penali.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

Si riceve un messaggio d'errore da un'azienda che segnala che alcune e-mail non sono state ricevute da diversi dipendenti. Per circoscrivere l'errore, viene consultato il log-file del firewall.

- b) Spiegare perché quest'azione, senza un chiarimento preliminare, è penalmente perseguibile.

**1**

**Nel log-file i movimenti dell'utenza sono facilmente individuabili. Informazioni personali come scambi di mail o siti web visitati sono visibili. Analisi sui dati personali possono essere effettuate solo in caso di sospetto abuso.**

- c) Come ci si può tutelare?

**1**

**In conformità con la legge sulla protezione dei dati, i collaboratori dovrebbero confermare anticipatamente in forma scritta che sono stati informati sul trattamento dei loro dati.**

Punti  
per  
pagina:

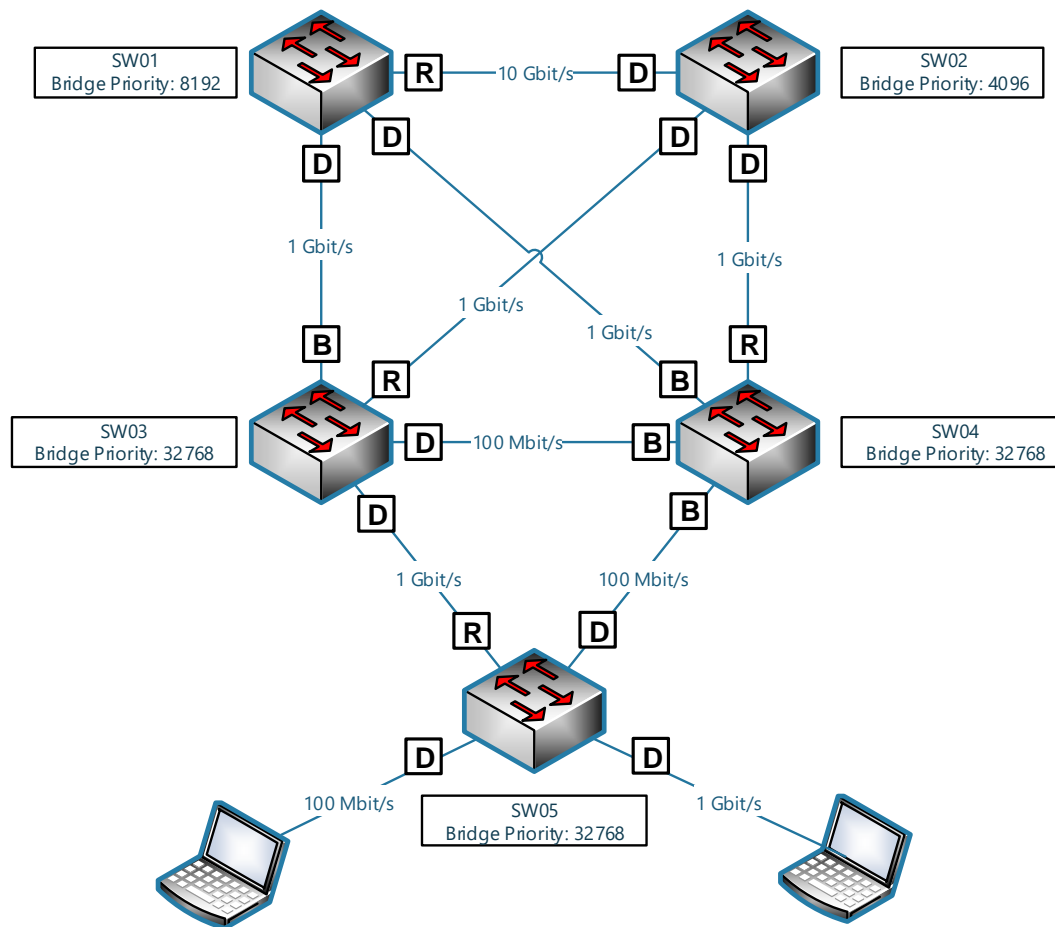
Punti

**18. Spanning Tree Obiettivo di valutazione n. 5.2.1 B3**

5

- a) Definire nel disegno le singole interfacce come:  
D (Designated Port) B (Blocked Port) R (Root Port)

4



- b) Perché certe porte devono essere impostate su Blocked?

1

**Per sopprimere la formazione di loop.**

**Nota per gli esperti:**

**Collegamenti da SW03 a SW04 e da SW04 a SW05 (da D a B), le impostazioni delle porte possono anche essere invertite.**

**Distribuzione punti:**

**Root Switch individuato → SW02 (1P)**

**Porte Root impostate correttamente (1P)**

**Porte Blocked impostate correttamente (1P)**

**Porte Designated impostate correttamente (1P)**

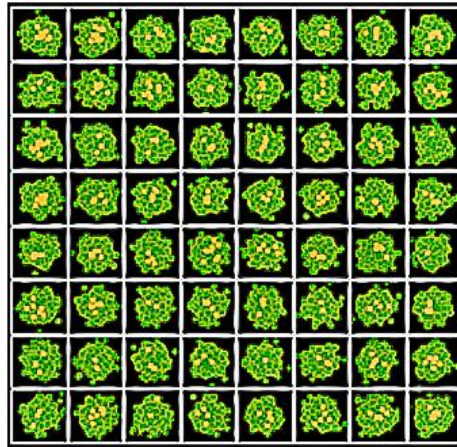
Punti  
per  
pagina:

		Punti
<b>19. Zero Trust</b>	<b>Obiettivo di valutazione n. 5.5.5 B2</b>	<b>3</b>
a)	Qual è il principio più importante del modello Zero Trust?  <b>Non fidarsi di nessuno né all'interno né all'esterno della rete. In pratica, è bloccato tutto ciò che non è stato esplicitamente permesso. Qualsiasi accesso è dapprima sempre considerato come non affidabile. È il principio fondamentale della sicurezza dei dati.</b>	1
b)	Quali requisiti di rete devono essere soddisfatti?  <ul style="list-style-type: none"><li>- <b>Tutte le applicazioni e gli utilizzatori si devono autenticare.</b></li><li>- <b>Tutti i dati possono essere trasmessi solo in forma criptata.</b></li></ul>	1
c)	Come implementare un sistema Zero Trust in azienda? Spiegare il principio per sommi capi.  <b>Sia sul perimetro che all'interno della rete, occorre prevedere sistemi che analizzino il traffico, che lo permettano o lo proibiscano e che registrino tutte le azioni in file di log.</b>  <b>Nota per gli esperti:</b> <b>Diversi prodotti svolgono questi compiti, ad es. un Bastion Server (Jump Host). Le risorse aziendali (server) sono accessibili solo tramite Jump Host. Non viene concesso alcun accesso diretto alle risorse. Queste possono trovarsi in una specifica rete virtuale (VLAN). Gli utilizzatori non conoscono le credenziali di connessione (nome utente, password) alle varie risorse. L'accesso a dispositivi critici può essere controllato o addirittura approvato da determinate persone in azienda.</b>	1
		Punti per pagina:

**20. Modulazione Obiettivo di valutazione n. 5.1.6 B2**

**4**

Nelle reti via cavo sono spesso utilizzati i diagrammi di costellazione per la valutazione della qualità.



- a) Oltre al diagramma di costellazione, anche i valori misurati “BER” und “MER” sono usati per una diagnosi qualitativa della trasmissione. Cosa significano questi due termini e qual è la loro unità di misura?

**2**

**BER (Bit-Error-Rate)**

È il rapporto tra i bit non ricevuti correttamente e i bit trasmessi. Il BER non ha unità di misura, ma è dato come valore assoluto.

**MER (Modulations-Error-Rate)**

Tutte le perturbazioni lineari sono raccolte nel MER. Il MER rappresenta una valutazione matematica del diagramma di costellazione. Il valore MER è misurato in dB.

- b) Quale modulazione si può vedere nel diagramma di costellazione qui sopra?

**1**

**QAM64 oppure CAP64**

- c) Come valutarne la qualità della trasmissione? Giustificare la risposta.

**1**

**La qualità della trasmissione non è ottimale.**

**I punti di misura si trovano spesso sul bordo dei singoli quadranti o addirittura nel quadrante adiacente, il che significa che i segnali non possono più essere correttamente classificati in modo univoco.**

**21. Influssi sul segnale Obiettivo di valutazione n. 5.1.6 B2**

3

a)



L'immagine qui sopra mostra la trasmissione di un segnale. Dal trasmettitore al ricevitore il segnale subisce una distorsione. Come si chiama questa interferenza e da cosa è causata?

Definizione:

0,5

**Diafonia (Crosstalk)**

Descrivere la causa:

1

**Alcune gamme di frequenza dei segnali trasmessi su conduttori che corrono adiacenti interferiscono tra loro. Il problema si accentua se più conduttori singoli in rame sono combinati in un fascio. Più alta è la frequenza di trasmissione maggiore è il disturbo sul segnale originale.**

b)



In questo tipo di trasmissione del segnale, il segnale ricevuto differisce da quello inviato. Come si chiama questo tipo di tecnica di trasmissione? Spiegarne il vantaggio.

Definizione:

0,5

**Vectoring**

Spiegazione del vantaggio:

1

**Se il trasmettitore è in grado di riconoscere le diverse interferenze che influenzano una particolare linea, può trasmettere un segnale contrario che riesca a compensare il disturbo; paragonabile alla soppressione del rumore esterno nelle cuffie. Il rapporto segnale-rumore così migliorato permette una maggiore velocità di trasmissione dei dati.**

**Punti**

**22. Telefonia IP Obiettivo di valutazione n. 5.4.4 B3**

**3**

Una telecamera IP, con SIP client integrato e collegata a una rete LAN, comunica tramite protocollo SIP con l'IP PBX. La telecamera è installata all'ingresso principale di un edificio aziendale. Un telefono SIP con funzionalità audio-video integrata è in funzione alla ricezione. Quando una persona passa davanti alla telecamera, viene automaticamente effettuata una chiamata SIP facendo squillare il telefono della ricezione. Il receptionist può così vedere la persona e comunicare con essa.

- a) Indicare almeno un codec per funzionalità che può essere utilizzato per questo tipo di chiamata.

Audio: **G.711a (G.711 PCMA), G.711u (G.711 PCMU), G.729, G.722**

0,5

Video: **H.264**

0,5

**Nota per gli esperti:  
Un codec per funzionalità per il punto completo.**

- b) Se questa chiamata dovesse transitare attraverso un firewall, quali restrizioni potrebbe incontrare e quali impostazioni dovrebbero essere adattate?

**2**

**Ci potrebbero essere problemi di audio a senso unico, visto che il suono è trasmesso solo in una direzione.**

**Questi problemi One-Way-Audio spesso possono essere risolti configurando le impostazioni ALG (Application Layer Gateway) del firewall.**

**Nota per gli esperti:  
sono possibili anche altre soluzioni.**

**Punti  
per  
pagina:**



Punti

**23. Posizionamento indoor Obiettivo di valutazione n. 5.5.3 B2**

**3**

Un museo vorrebbe introdurre un'applicazione per i visitatori che, determinandone la loro posizione, non appena questi si trovano di fronte a un oggetto esposto, riproduca automaticamente un file audio con le informazioni sull'oggetto. Per creare una buona esperienza utente, un posizionamento veloce e preciso è molto importante.

a) Quale tecnologia è preferibile per una tale soluzione?

**1**

**BLE Beacons (Bluetooth Low Energy) è stata sviluppata appositamente per il posizionamento indoor.**

b) Quali soluzioni per il posizionamento sono meno adatte per questo tipo d'applicazione o non funzionano affatto? Indicarne una e giustificare la risposta.

**1**

- **WiFi: è troppo lento e la potenza di trasmissione è troppo grande per un posizionamento preciso.**
- **GPS: non funziona al chiuso.**

c) Quali altre caratteristiche dovrebbe avere una tale soluzione in termini d'installazione ed esercizio? Indicarne due.

**1**

- **Funzionamento a batteria per una maggiore facilità d'installazione**
- **Facilmente adattabile: per esposizioni flessibili**
- **Compatibile: con i più diffusi cellulari**
- **Tecnologia Low Power: per una lunga durata della batteria**
- **Configurazione e ricerca guasti semplice: per un'alta disponibilità**

**Nota per gli esperti:  
Sono possibili anche altre soluzioni.**

Punti  
per  
pagina:

**Punti**

**24. VPN e crittografia Obiettivo di valutazione n. 5.2.1 B3**

**2**

Spuntare se le seguenti affermazioni sulle connessioni VPN sono vere o false.

Affermazioni	Vero	Falso
I file sono obbligatoriamente criptati per essere trasferiti via VPN.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
La crittografia DES è più veloce della AES-256 ed è per questo che è usata oggi come crittografia standard.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Se un hacker conosce la chiave di una connessione VPN, può decifrare il traffico HTTPS trasmesso nel tunnel.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Una connessione VPN protegge dall'accesso non autorizzato ai dati aziendali.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

0,5

0,5

0,5

0,5

**Punti  
per  
pagina:**

**25. Routing Obiettivo di valutazione n. 5.5.9 B3**

**3**

La seguente tabella di routing è visualizzata su un dispositivo di rete:

Rete di destinazione	Maschera di sottorete	Gateway	Interfaccia (IP)	Metrica
192.168.78.0	255.255.255.248	172.16.1.1	172.16.1.2	211
192.168.78.32	255.255.255.248	10.242.2.1	10.242.2.4	257
192.168.88.0	255.255.255.0	10.242.2.1	10.242.2.4	257
192.168.88.0	255.255.255.0	192.16.2.1	192.16.2.12	157
0.0.0.0	0.0.0.0	192.168.54.1	192.168.54.145	3

Il Gateway 192.168.54.1 porta a Internet.

- a) Perché l'host 192.168.78.43 non può essere raggiunto da questo dispositivo di rete?

**1**

**Per la destinazione 192.168.78.43, non c'è nessuna voce nella tabella tranne il percorso di default verso Internet. Tuttavia, l'indirizzo 192.168.78.43 è un indirizzo privato che non viene instradato su Internet e quindi eliminato.**

**Manca una voce per la rete 192.168.78.40/28 in cui 192.168.78.43 è incluso.**

- b) Quale interfaccia è usata per una connessione a 192.168.88.243 se tutti i gateway sono attivi?

**1**

**La connessione viene stabilita tramite 192.16.2.12, poiché questo percorso ha la metrica più piccola e quindi il "costo" più basso.**

- c) Quale indirizzo IP "vede" un server Web in Internet quando il dispositivo di rete con questa tabella di routing stabilisce una connessione con esso?

**1**

**Dal punto di vista del server Web, l'IP pubblico del router è visibile dietro 192.168.54.1, indirizzo che però è privato e quindi deve essere tradotto tramite NAT in un indirizzo pubblico (router). Ciò significa che non è visibile.**