

Cognome:	Nome:	N° candidato:	Data:

<b>90 Minuti</b>	<b>25 Compiti</b>	<b>27 Pagine</b>	<b>87 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**

6	5,5	5	4,5	4	3,5	3	2,5	2	1,5	1
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

**Esperti**

Pagina	2	3	4	5	6	7	8	9	10	11	12	13
Punti:	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....

**Esperti**

Pagina	14	15	16	17	18	19	20	21	22	23	24	25
Punti:	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....

**Esperti**

Pagina	26	27
Punti:	.....	.....

**Firma  
esperta / esperto 1**

**Firma  
esperta / esperto 2**

**Punti**

**Nota**

**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</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?	1
b)	Descrivere un modo per migliorare l'immagine senza sostituire la rete.	1
c)	Come migliorare la ripresa video con misure ambientali (senza adeguamenti alla rete o IT)? Indicare due possibilità.	1
		<b>Punti per pagina:</b>

Punti

**2. SIP Trace**

**5**

- 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.

- Source MAC Address: ca:13:d3:a2:03:34
- Destination MAC Address: \_\_\_\_ : \_\_\_\_ : \_\_\_\_ : \_\_\_\_ : \_\_\_\_ : \_\_\_\_
- Source Port: \_\_\_\_
- Destination Port: \_\_\_\_
- Source IP Address: \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_
- Destination IP Address: 255.255.255.255

Punti  
per  
pagina:

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

2

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:

- 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.

Punti

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,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.

### 3. Trasmissione senza fili

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)			
LoRa			
Bluetooth-Versione 2			

1

1

1

### 4. Trasmissione dati

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.

## 5. Sistemi esterni

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

b) Quali condizioni deve soddisfare il collegamento della telecamera?

1

## 6. Interfacce

5

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

Vero	Falso	Affermazione	
		I moduli SFP sono utilizzati esclusivamente per collegare cavi dati singlemode e multimode.	0,5
		I moduli SFP possono essere installati durante il funzionamento.	0,5
		I moduli SFP+ possono essere installati in uno slot SFP.	0,5
		Direct Attached Cable (DAC) possono essere usati solo per SFP+.	0,5
		Già all'acquisto di un modulo SFP+ occorre decidere se il modulo sarà usato in SM o MM.	0,5
		Solo con i moduli QSFP si può raggiungere una velocità di trasmissione di 40 Gbps.	0,5

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

Vero	Falso	Affermazione	
		Il balun è un dispositivo per l'adattamento tra una linea bilanciata e una linea sbilanciata.	0,5
		Con un balun si possono adattare le impedenze.	0,5
		I balun sono spesso utilizzati con connettori BNC o IEC.	0,5
		I balun aumentano la sicurezza della rete, in quanto possono trasmettere solo unidirezionalmente.	0,5

Punti  
per  
pagina:



		Punti
<b>7. Ethernet</b>		<b>2</b>
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
b) Quale standard di trasmissione regola l'IEEE 802.3bz?		0,5
c) Qual è il vantaggio dello standard IEEE 802.3bz in termini di cablaggio LAN?		1
		<b>Punti per pagina:</b>

## 8. Tipi di Hypervisor

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 type="checkbox"/>
Impiego in ambienti produttivi.	<input type="checkbox"/>	<input type="checkbox"/>
L'Hypervisor è eseguito come applicazione in un sistema operativo.	<input type="checkbox"/>	<input type="checkbox"/>
L'Hypervisor è eseguito direttamente sull'hardware dell'host.	<input type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

## 9. Mobilità in sede

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

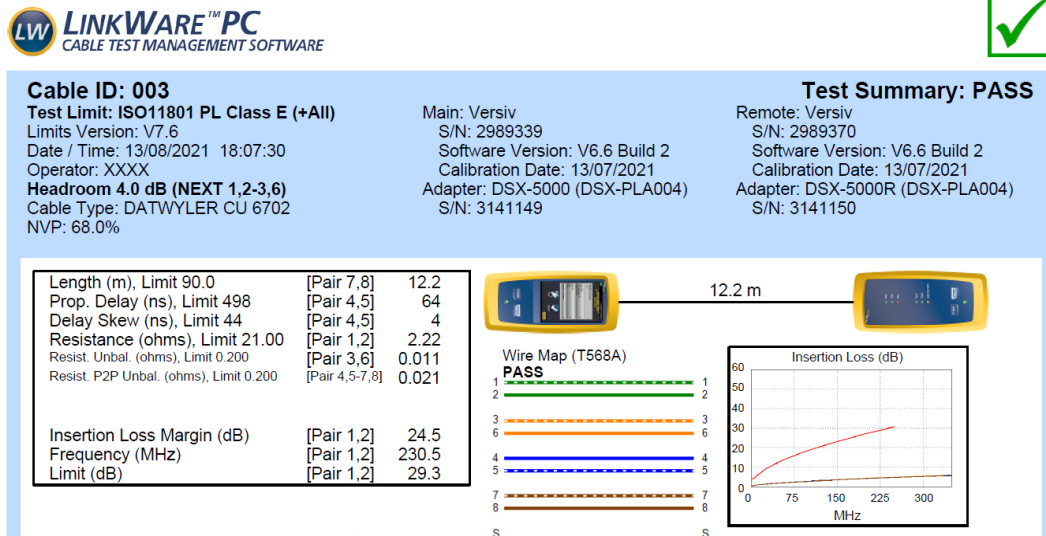
b) Indicare due vantaggi di questa tecnologia.

1

10. CUC

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
- b) Indicare il significato dei termini “Prop. Delay (ns)” e “Delay Skew (ns)” e spiegarli in relazione a questa misura. 2
- c) Perché la differenza tra coppie di segnali è importante per le reti ad alta velocità? 1

Punti

**11. Telefonia mobile 5G**

**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.

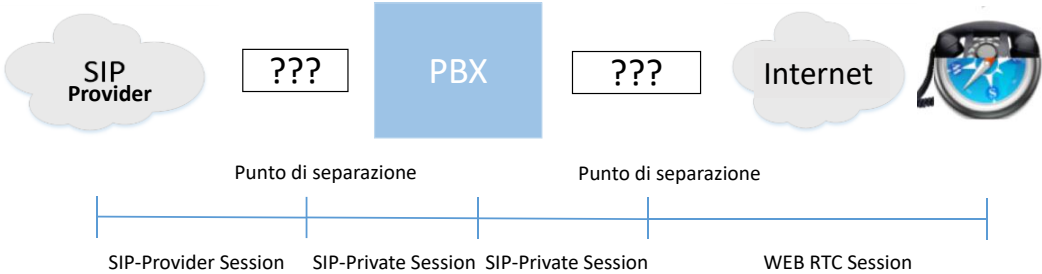
a) Indicare quattro differenze tra le tecnologie di rete 4G e 5G.

**2**

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

**1**

Punti  
per  
pagina:

	Punti
<b>12. Struttura Telematica</b>	<b>4</b>
a) Spiegare le funzioni (compiti) dei seguenti componenti. SBC:	1
WebRTC Gateway:	1
DSLAM:	1
b) Quali due dei suddetti componenti sono utilizzati nello scenario seguente?	1
	
	Punti per pagina:

**13. SNMP**

**4**

a) Spiegare cosa sono i pacchetti dati Trap SNMP.

1

b) Cos'è un file MIB?

1

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 type="checkbox"/>	<input type="checkbox"/>
Oltre al monitoraggio, SNMP può essere usato anche per configurare o controllare da remoto i dispositivi.	<input type="checkbox"/>	<input type="checkbox"/>
SNMP consente la crittografia dei dati tra gli agenti e il gestore.	<input type="checkbox"/>	<input type="checkbox"/>
SNMP si basa su TCP per stabilire connessioni sicure tra l'agente e il gestore.	<input type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

		Punti
<b>14. Connessione</b>		<b>5</b>
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.		2
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
Che sequenza mostra la figura 1 e quali sono le porte utilizzate?		1
Che sequenza mostra la figura 2 e quali sono le porte utilizzate?		1
		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</b>		<b>5</b>
a) Una delle strategie di backup si basa sulla regola 3-2-1. Cosa sta dietro ogni singolo numero?		
3:		0,5
2:		0,5
1:		0,5
b) Spiegare il principio di generazione (nonno-padre-figlio) nei backup.		1
c) Cos'è la deduplicazione?		1
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'RTO?		
Numero di nastri:		0,5
RPO:		0,5
RTO:		0,5
		<b>Punti per pagina:</b>

**16. PBX in un centro di calcolo esterno**

**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**

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 type="checkbox"/>	<input type="checkbox"/>
IP-DECT Basis Station	<input type="checkbox"/>	<input type="checkbox"/>
DECT Basis Station (TDM), due fili	<input type="checkbox"/>	<input type="checkbox"/>
Rete pubblica 4G / 5G attraverso VPN	<input 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**

**17. Protezione dei dati**

**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 type="checkbox"/>	<input type="checkbox"/>
Salute, sfera personale o appartenenza razziale.	<input type="checkbox"/>	<input type="checkbox"/>
Misure dell'aiuto sociale.	<input type="checkbox"/>	<input type="checkbox"/>
Procedimenti o sanzioni amministrative o penali.	<input 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

- c) Come ci si può tutelare?

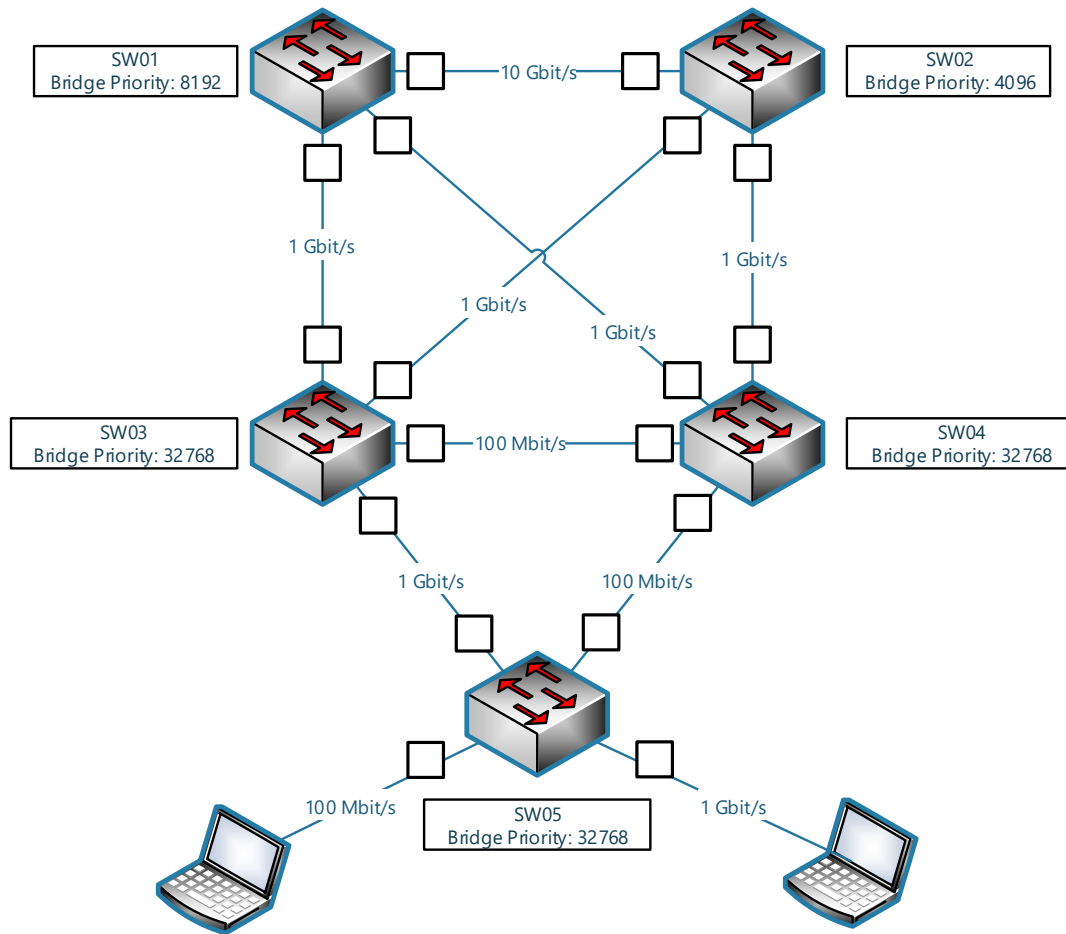
1

## 18. Spanning Tree

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?

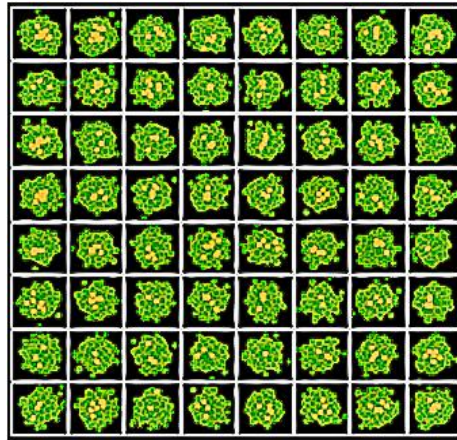
1

	Punti
<b>19. Zero Trust</b>	<b>3</b>
a) Qual è il principio più importante del modello Zero Trust?	1
b) Quali requisiti di rete devono essere soddisfatti?	1
c) Come implementare un sistema Zero Trust in azienda? Spiegare il principio per sommi capi.	1
	Punti per pagina:

**20. Modulazione**

**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**

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

**1**

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

**1**

**21. Influssi sul segnale**

**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

Descrivere la causa:

1

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

Spiegazione del vantaggio:

1

## 22. Telefonia IP

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:

0,5

Video:

0,5

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

2



Punti

**23. Posizionamento indoor**

**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

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

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

1

Punti  
per  
pagina:

**24. VPN e crittografia**

**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 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 type="checkbox"/>
Se un hacker conosce la chiave di una connessione VPN, può decifrare il traffico HTTPS trasmesso nel tunnel.	<input type="checkbox"/>	<input type="checkbox"/>
Una connessione VPN protegge dall'accesso non autorizzato ai dati aziendali.	<input type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

## 25. Routing

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

1

1