

Dossier des expertes et experts

90	Minutes	25	Exercices	27	Pages	87	Points
----	---------	----	-----------	----	-------	----	--------

Moyens auxiliaires autorisés:

- Règle, équerre, chablon
- Calculatrice de poche indépendante du réseau (tablettes, smartphones etc. ne sont pas autorisés)

Cotation – Les critères suivants permettent l'obtention de la totalité des points:

- Les formules et les calculs doivent figurer dans la solution.
- Les résultats sont donnés avec leur unité.
- Le cheminement vers la solution doit être clair.
- Les réponses et leurs unités doivent être soulignées deux fois.
- Le nombre de points maximum est donné pour chaque exercice.
- Les réponses sont évaluées dans l'ordre.
- Les réponses données en plus ne sont pas évaluées.
- Le verso est à utiliser si la place manque. Par exercice, un commentaire adéquat tel que par exemple « voir la solution au dos » doit être noté.
- **Toute erreur induite par une précédente erreur n'entraîne aucune déduction.**

Barème

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

Délai d'attente:

Cette épreuve d'examen ne peut pas être utilisée librement comme exercice avant le 1^{er} septembre 2024.

Créé par:

Groupe de travail PQ d'EIT.swiss pour la profession de télématicienne CFC / télématicien CFC

Editeur:

CSFO, département procédures de qualification, Berne

1. Conférence vidéo N° d'objectif d'évaluation 5.1.1 B2

Le Home-Office et le Mobile-Office nécessitent une plateforme unique pour collaborer efficacement qui intègre la visioconférence. Dans ce contexte, les applications d'entreprise sont souvent exploitées via des réseaux privés et publics, ce qui nuit souvent à la qualité et à la disponibilité.

3

- a) Citez les deux sources de perturbation les plus fréquentes qui engendrent une détérioration de la qualité du son et de l'image dans un réseau domestique ?

1

- **Le WiFi (bande passante fluctuante et trop faible)**
- **La connexion à Internet (bande passante ascendante trop faible)**

**Indication pour experts:
D'autres réponses sont possibles.**

- b) Décrivez un moyen qui permet de rendre la vidéo plus fluide sans modifier le réseau.

1

- **Choisir une résolution vidéo plus basse, ce qui réduit les besoins en bande passante.**
- **Codec**
- **Mouvements, fonds d'écran**

**Indication pour experts:
D'autres réponses sont possibles.**

- c) Citez deux mesures externes (pas d'adaptation du réseau ou de l'informatique) qui peuvent être prises pour améliorer la qualité de la vidéo ?

1

- **Pas de sources lumineuses claires dans la zone de la caméra**
- **Le visage doit être éclairé de face**
- **Position de la caméra surélevée, au centre de l'écran, pour que la personne en face ait l'impression d'être regardée.**
- **Fonds d'écran, image de fond**

**Indication pour experts:
D'autres réponses sont possibles.**

Points

2. SIP Trace N° d'objectif d'évaluation 5.2.2 B2

5

- a) Vous connectez pour la première fois un appareil téléphonique Yealink SIP (LLDP désactivé) à un réseau IP. Quelles sont les valeurs qui peuvent être identifiées à l'aide de l'analyseur Wireshark-Trace ?

2

Complétez le contenu du premier message envoyé :

- Adresse MAC source: ca:13:d3:a2:03:34
- Adresse MAC destination: **FF:FF:FF:FF:FF:FF**
- Port source: **68**
- Port destination : **67**
- Adresse IP source: **0.0.0.0**
- Adresse IP destination: 255.255.255.255

**Points
par
page:**

- b) Lorsque vous lancez Wireshark-Trace, vous obtenez les requêtes DNS suivantes dans l'ordre chronologique :

2

1^{ère} requête :

2^{ème} requête :

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	172.16.52.30	DNS	80 Standard query 0xd20b A rpscloud.yealink.com
172.16.52.106	172.16.52.30	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	TCP	124 Destination unreachable (Port unreachable)
172.16.52.106	172.16.52.30	TCP	124 Destination unreachable (Port unreachable)

Expliquez ces deux requêtes DNS :

Le téléphone demande l'adresse IP du serveur de temps.

La première demande concerne une requête au serveur DNS afin de trouver l'adresse IP du serveur NTP configuré dans le téléphone.

Le téléphone demande l'adresse IP du serveur RPS.

La deuxième requête concerne une demande au serveur DNS afin de trouver l'adresse IP du serveur RPS Yealink, également configuré dans le téléphone.

Cela permettrait au téléphone d'obtenir l'URL de son serveur de communication final.

Points
par
page:

c) Dans le reste de la trace chronologique de Wireshark-Trace, vous appliquez un filtre pour identifier les paquets HTTP et découvrir cet échange entre le téléphone IP et l'IPPBX.

1

Source	Destination	Protocol	Length	Info
172.16.52.250	172.16.52.106	HTTP	213	GET /provisioning/z3a0e2c12t1/885ec04e57fd.boot HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	175	HTTP/1.1 404 Not Found
172.16.52.250	172.16.52.106	HTTP	214	GET /provisioning/z3a0e2c12t1/y00000000000000000000.boot HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	175	HTTP/1.1 404 Not Found
172.16.52.250	172.16.52.106	HTTP	213	GET /provisioning/z3a0e2c12t1/y0000000000000096.cfg HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	677	HTTP/1.1 200 OK
172.16.52.250	172.16.52.106	HTTP	212	GET /provisioning/z3a0e2c12t1/885ec04e57fd.cfg HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	356	HTTP/1.1 200 OK
172.16.52.250	172.16.52.106	HTTP	215	GET /provisioning/z3a0e2c12t1/logo/yealinkt46.png HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	1452	HTTP/1.1 200 OK (PNG)
172.16.52.250	172.16.52.106	HTTP	215	GET /provisioning/z3a0e2c12t1/logo/yealinkt46.png HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	1452	HTTP/1.1 200 OK (PNG)
172.16.52.250	172.16.52.106	HTTP	217	GET /provisioning/z3a0e2c12t1/directory_setting.xml HTTP/1.1
172.16.52.250	172.16.52.106	HTTP/XML	1413	HTTP/1.1 200 OK [Malformed Packet]
172.16.52.250	172.16.52.106	HTTP	265	GET /provisioning/z3a0e2c12t1/firmware/yealink_patchT54M(T57M,T53M,T53,T54,T57)-96.86.0.23.rom HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	1267	GET /provisioning/z3a0e2c12t1/yealink_phonebook.xml HTTP/1.1
172.16.52.250	172.16.52.106	HTTP	217	GET /provisioning/z3a0e2c12t1/yealink_phonebook.xml HTTP/1.1
172.16.52.250	172.16.52.106	HTTP/XML	1267	HTTP/1.1 200 OK

Décrivez le déroulement des échanges sur le réseau.

Il s'agit du premier enregistrement du téléphone IP sur l'IPPBX ainsi que de la demande par le téléphone de différents fichiers (fichier de configuration du téléphone, firmware, annuaire, logo du téléphone, ...). Le PBX lui fournit donc ces fichiers afin que le téléphone IP puisse démarrer et se configurer correctement.

Indication pour experts:
D'autres réponses sont possibles.

**Points
par
page:**

3. Transmission radio N° d'objectif d'évaluation 5.3.2 B2

3

Attribuez les caractéristiques suivantes à chaque technologie :
(Pas de réponses multiples possibles)

Fréquence	Débit maximal	Portée sans obstacles
A) 863 MHz à 870 MHz	a) env. 50 kbit/s	1) 10 m
B) 1.8 GHz	b) env. 2 Mbit/s	2) 50 m
C) 2.40 GHz à 2.48 GHz	c) env. 1 Gbit/s	3) Plusieurs km
D) 5 GHz	d) env. 10 Gbit/s	4) 80 km

Insérez les lettres et les chiffres correspondants dans le tableau.

Technologie	Fréquence	Débit maximal	Portée
Wi-Fi 6 (WLAN 802.11ax)	D	d	2
LoRa	A	a	3
Bluetooth-Version 2	C	b	1

1

1

1

Indication pour experts:
1 point par ligne complète.
0,5 point si 2 des 3 réponses sont justes par ligne.

4. Transmission de données N° d'objectif d'évaluation 5.1.1 B2

2

Votre client dispose d'une connexion Internet avec un débit download maximal de 300 Mbit/s et un upload maximal de 100 Mbit/s. Ce client effectue chaque nuit une sauvegarde (taille du fichier : 150 Go). Cette sauvegarde doit être terminée à 06h00 du matin.

A quelle heure faut-il démarrer la sauvegarde au plus tard ?

Remarque :

On ne tient pas compte du débit supplémentaire induit par les entêtes des paquets.

Le Backup doit démarrer au plus tard à 02h40 du matin.

Solution:

Temps de transmission = Taille du fichier / Débit upload

Taille du fichier en bit:

150 Go = 150 • 10⁹ octets = 150 • 10⁹ • 8 bits = 1,2 • 10¹² bits

Débit upload:

100 Mbit/s = 1 • 10⁸ bit/s

Temps de transmission = 1,2 • 10¹² bits / 1 • 10⁸ bit/s = 12'000 Secondes

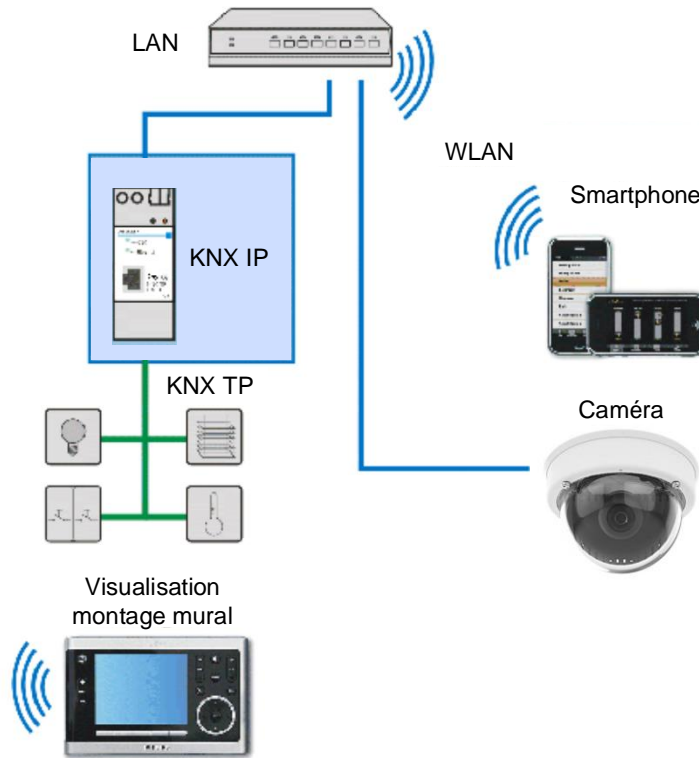
12'000 Secondes = 200 Minutes

Points
par
page:

5. Systèmes externes N° d'objectif d'évaluation 5.4.4 B2

3

En raison de perturbations fréquentes sur le 230 V, ce système de commande d'automatisation du bâtiment doit devenir indépendant du réseau électrique. Le système doit pouvoir être exploité sans interruption et les images de la caméra doivent continuer à être transmises au smartphone et aux unités de contrôle de l'automatisation du bâtiment.



a) Quels sont les quatre composants qui doivent être connectés à un onduleur ?

2

- Le switch LAN
- La console fixe
- Le gateway KNX IP
- L'alimentation du bus KNX
- Caméra

b) Quel est le meilleur mode d'alimentation pour la caméra ?

1

- La caméra et le switch PoE
- Injecteur PoE
- L'alimentation de la caméra

Indication pour experts:
D'autres réponses sont possibles.

Points

6. Interfaces N° d'objectif d'évaluation 5.6.1 B2

5

- a) Cochez les cases vrai / faux pour toutes les affirmations ci-dessous concernant les modules SFP dans l'interconnexion de switch.

vrai	faux	Affirmation	
	X	Les modules SFP sont exclusivement utilisés pour connecter des systèmes monomodes et multimodes.	0,5
X		Les modules SFP peuvent être installés sans arrêter les appareils sur lesquels ils sont mis en place.	0,5
	X	Les modules SFP+ peuvent être installés dans un slot SFP.	0,5
	X	Un Direct Attach Cable (DAC) ne peut être utilisé qu'avec du SFP+.	0,5
X		Lors de l'achat d'un module SFP+, il faut décider si le module sera utilisé en monomode ou multimode.	0,5
X		Ce n'est qu'avec des modules QSFP que le débit de données de 40 Gbit/s peut être atteint.	0,5

- b) Cochez les cases vrai / faux pour toutes les affirmations ci-dessous concernant les balun.

vrai	faux	Affirmation	
X		Le balun est un composant qui permet la conversion entre un système de lignes symétriques et un système de lignes asymétriques.	0,5
X		Un balun permet d'adapter les impédances.	0,5
X		Les balun sont souvent utilisés en combinaison avec des connecteurs BNC ou IEC.	0,5
	X	Les balun augmentent la sécurité du réseau car ils communiquent uniquement de manière unidirectionnelle.	0,5

**Points
par
page:**

Points

7. Ethernet N° d'objectif d'évaluation 5.6.2 B2

2

Vous devez équiper les bureaux d'une entreprise avec un système WiFi moderne. Pour garantir une transmission optimale des données et de la voix, il convient d'utiliser des points d'accès de la dernière génération Wi-Fi 6 Wave 2.

- a) Quelle technologie de réseau local doit être utilisée pour obtenir les meilleures performances ?

0,5

Multigigabit Ethernet

- b) Quels sont les standards définis par la norme Ethernet IEEE 802.3bz?

0,5

2.5 GBase-T

5 GBase-T (IEEE 802.3bz)

- c) Au niveau du câblage LAN, quel est l'avantage de la norme IEEE 802.3bz en ce qui concerne les liens LAN ?

1

Les câbles Cat 5e ou Cat 6 existants peuvent être réutilisés, aucun nouveau câblage n'est donc nécessaire.

**Points
par
page:**

8. Types d'Hyperviseurs N° d'objectif d'évaluation 5.5.2 B2

2

Quelles caractéristiques correspondent à quel type d'hyperviseur ?

Caractéristiques	Type 1	Type 2
De préférence pour le développement et les tests.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Utilisation pour des environnements de production.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
L'hyperviseur est une application qui tourne sur un système d'exploitation.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L'hyperviseur tourne directement sur le matériel hôte.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

9. Mobilité sur un site N° d'objectif d'évaluation 5.3.1 B2

2

Une entreprise de logistique a migré il y a quelques années l'ensemble de sa communication vocale sur un système Voice over Wi-Fi. Ceci permettait de couvrir la vaste zone de l'entreprise au moyen du réseau IP et a permis de démonter l'ensemble du câblage téléphonique. Malheureusement, de nombreux problèmes de transmission liés au déplacement de gros objets métalliques empêchent une bonne qualité audio. Pour augmenter la stabilité des communications, votre client souhaite installer une technologie radio dédiée à la communication vocale interne (pas de 4G / 5G) sans avoir à réajuster l'ensemble du câblage.

a) Quelle technologie pouvez-vous lui proposer ?

1

- IP-DECT ou SIP-DECT

b) Citez deux avantages de cette technologie.

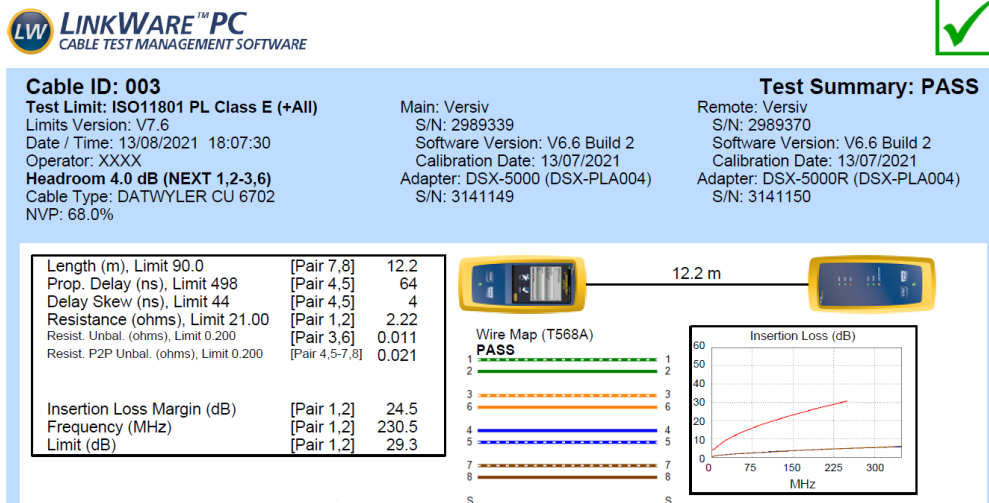
1

- Réseau radio résistant aux perturbations sur une fréquence réservée
- Itinérance (roaming) sans interruption entre les stations de base
- Sécurité par cryptage du lien radio
- Haute densité de conversations sans perte de qualité
- Les émetteurs peuvent se connecter au serveur de téléphonie via Ethernet
- Alimentation des émetteurs via un Switch PoE
- Le câblage LAN des points d'accès WI-FI peut être réutilisé

10. Câblage universel N° d'objectif d'évaluation 5.1.6 B1

5

Lors d'une certification d'un lien de câblage universel, votre appareil de mesure vous donne le résultat suivant:



a) Bien que le test de certification soit validé, citez quatre éléments essentiels pour la qualité du résultat du test.

2

- Date de calibration de l'appareil
- Version de logiciel
- Limite de test utilisée
- Choix du protocole de test
- Type de câble utilisé
- Valeur du NVP du câble

Indication pour experts:
D'autres solutions sont possibles.

b) Indiquez la signification des termes "Prop. Delay (ns)" et "Delay Skew (ns)" et expliquez-les en lien avec la mesure ci-dessus.

2

- Prop. Delay: Vitesse de propagation du signal dans une paire, ici la paire la plus lente est 4-5. Cela représente le délai de transmission du signal proprement dit.

- Delay Skew: Différence de vitesse de propagation entre la paire la plus rapide et la paire la plus lente.

c) Pourquoi l'écart entre les paires de signaux est-il important pour un réseau à haut débit ?

1

L'écart temporel de transmission entre les paires est important, car les technologies de réseau à haut débit, y compris Gigabit Ethernet, utilisent les quatre paires du câble pour la transmission de signaux. Si la vitesse de propagation varie fortement d'une paire à l'autre, les signaux envoyés simultanément à une extrémité du câble peuvent arriver au récepteur à des moments différents. Bien que les récepteurs soient conçus pour accepter de légers retards, un décalage trop important rend la recombinaison du signal initial impossible.

Indication pour experts:
D'autres solutions sont possibles.

11. Communication mobile 5G N° d'objectif d'évaluation 5.3.2 B2

3

La norme de communication mobile 5G est une évolution de la 4G. Lors de son développement, l'accent a été mis sur les exigences des futures applications mobiles telles que le jeu en ligne, les lunettes à réalité augmentée et les voitures à conduite autonome.

a) Citez quatre différences entre les technologies de réseau mobile 4G et 5G?

2

- **Temps de latence**
- **Débit binaire**
- **Nombre de terminaux connectés simultanément**
- **Codage (OFDM)**
- **Nombre de stations de base par unité de surface (densité)**
- **Beamforming (Formation de faisceaux)**

**Indication pour experts:
D'autres solutions sont possibles.**

b) Quelle est la caractéristique de performance la plus importante pour la mise en œuvre des applications en temps réel mentionnées ci-dessus?

1

Le temps de latence

**Indication pour experts:
La 5G a un temps de latence de l'ordre de la milliseconde alors que celui de la 4G est de 60 – 98 ms.**

Points

12. Éléments de réseau N° d'objectif d'évaluation 5.4.1 B2

4

- a) Expliquer l'utilité (effet) des composants cités ci-dessous.

SBC:

1

Le SBC sert d'élément de sécurité entre le fournisseur SIP et l'équipement du client. (Il peut aussi exécuter d'autres fonctions comme la conversion de codecs ou la modification de la signalisation SIP par exemple).

Passerelle WebRTC:

1

Le WebRTC Gateway fonctionne comme une interface entre les clients de téléphonie basés sur le protocole WebRTC et le système téléphonie. Cette passerelle fait la traduction de WebRTC au protocole SIP.

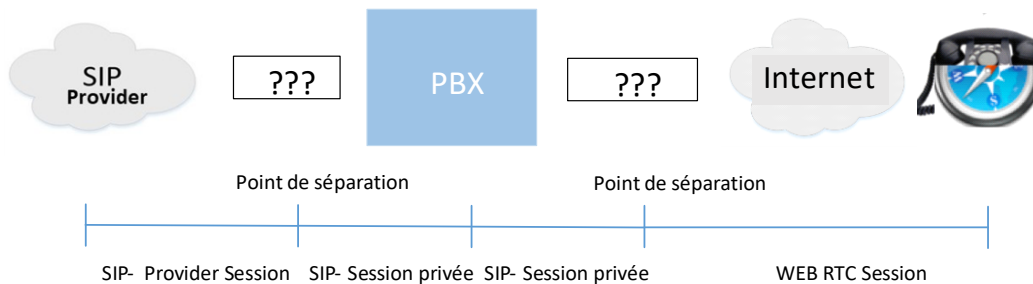
DSLAM:

1

Le DSLAM („Digital Subscriber Line Access Multiplexer“ ou „multiplexeur d'accès à la ligne d'abonné numérique“) fait partie de l'infrastructure nécessaire à l'exploitation du DSL. Les DSLAM sont situés à un point de convergence des lignes d'abonnés.

- b) Quels sont les deux composants mentionnés ci-dessus qui sont utilisés dans le schéma représenté ci-dessous ?

1



SBC

WebRTC Gateway

Points
par
page:

13. SNMP N° d'objectif d'évaluation 5.5.4 B2

4

- a) Expliquer ce que sont les paquets de données Trap SNMP.

1

Ce sont des messages envoyés spontanément par un agent SNMP à un manager SNMP sans requête de celui-ci. (Leur envoi est souvent généré par un dépassement d'une valeur cible)

- b) Qu'est-ce qu'un fichier MIB ?

1

Les MIB (Management Information Base) sont les fichiers descriptifs des objets utilisés par le protocole SNMP et implémentés dans les agents SNMP. Il contiennent les paramètres variables d'appareils (Données techniques) ainsi que les alertes qui peuvent être déclenchées. Le gestionnaire SNMP utilise les informations de la MIB pour les traduire les interpréter et les visualiser.

- c) SNMP V3 est utilisé pour surveiller les composants d'un réseau.
Cochez les cases vrai / faux pour les affirmations ci-dessous.

Affirmations	vrai	faux
Un agent SNMP logiciel ou matériel doit être actif sur tous les composants surveillés.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
En plus de la surveillance, SNMP peut être utilisé pour configurer ou contrôler des appareils distants.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP prend en charge le cryptage des données entre les agents et le gestionnaire.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP s'appuie sur TCP pour établir des connexions fiables entre l'agent SNMP et le gestionnaire SNMP.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

0,5

0,5

0,5

0,5

14. Transmissions N° d'objectif d'évaluation 5.5.4 B2

5

2

- a) Vous installez un nouveau PBX IP. La sauvegarde des données de ce nouveau système doit être sécurisée, automatisée et externalisée. Décrivez brièvement deux solutions possibles.

- IPPBX sauvegarde directement sur le Cloud (SFTP)
- IPPBX sauvegarde sur le stockage local (NAS, serveur), qui est synchronisé via le cloud (S3).
- Envoi de la sauvegarde par e-mail

Indication pour experts:
La liste est non exhaustive.

- b) Analysez les deux captures d'écran Wireshark de la page 16 :
Indication : L'adresse IP 172.16.52.250 est l'adresse d'un PBX IP.

Quel est le type d'équipement informatique qui a l'adresse IP 172.16.52.63 ?

1

Il s'agit d'un serveur FTP qui utilise le protocole SFTP.

Quel est l'échange représenté dans la Capture d'écran 1 et quels sont les ports utilisés à cet effet ?

1

Port du PBX IP aléatoire: 46660 (TCP)

Port du serveur SFTP: 22 (TCP)

Il s'agit de l'initialisation d'une communication via les protocoles TCP et SSH entre le PBX IP et un serveur SFTP.

Quel est l'échange représenté dans la Capture d'écran 2 et quels sont les ports utilisés à cet effet ?

1

Port du PBX IP aléatoire: 35370 (TCP)

Port du serveur SFTP: 61322 (TCP)

Il s'agit de la transmission de paquets cryptés entre le PBX IP et un serveur SFTP.

Indication pour experts:
0,5 Point pour les ports corrects.
0,5 point pour la description correcte.

b) Capture d'écran 1:

Capture d'écran 2:

Points

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=9
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=9
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.SshClient.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=3848272678
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=3848272678 TSecr=978622881
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=3848272678 TSecr=978622881
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=3848272713
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=3848272721 TSecr=3848272721

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=9
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=9
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=0 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=0 TSval=978685695 TSecr=3848335493
9028	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
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=978686496 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=978686496 TSecr=978686496
9032	152.158183	172.16.52.250	172.16.52.63	TCP	1122	61322 → 35370 [PSH, ACK] Seq=22 Ack=39 Win=13184 Len=1056 TSval=3848336296 TSecr=978686496

15. Backup N° d'objectif d'évaluation 5.5.4 B2

5

- a) Un concept de sauvegarde est établi sur la base d'une stratégie de sauvegarde 3-2-1. Expliquez la signification de ces trois chiffres.

3: Trois copies distinctes des données à protéger sont créées.

0,5

2: Les copies sont stockées sur deux types de supports différents.

0,5

1: Une des copies des données est sauvegardée sur un site externe.

0,5

- b) Expliquez le principe de génération (grand-père - père - fils) dans le cadre des sauvegardes.

1

La méthode de base est de définir trois ensembles de sauvegardes, telles que journalière, hebdomadaire et mensuelle.

Indication pour experts:

Les journalières, ou « fils », sont exécutées chaque jour avec l'un d'entre eux élevé au rang de « père » chaque semaine. Les hebdomadaires, ou pères, sont exécutées chaque semaine avec l'une d'entre elles élevée au rang de « grand-père » chaque mois.

- c) Expliquez la notion de déduplication dans le cadre des sauvegardes?

1

La déduplication des données, aussi appelée « compression intelligente » réduit les besoins de stockage en supprimant les données redondantes.

Le support de stockage, disque ou bande, conserve donc une seule instance des données. Les données redondantes sont remplacées par un pointeur vers l'unique copie.

- d) Un serveur effectue une sauvegarde complète chaque vendredi soir à 20h00. Du lundi au jeudi, il fait une sauvegarde incrémentale à la même heure. Chaque sauvegarde est effectuée sur une bande différente et malheureusement ce serveur tombe en panne un mercredi à 14h00.
Combien de bandes sont nécessaires pour le restaurer ?

Nombre de bandes: 3 (Full + Lu + Ma)

0,5

Le jeudi à 8h00, vous commencez la restauration et la terminez à 11h00 le même jour. Quelle est la durée du RPO et du RTO ?

RPO: 18h

0,5

RTO: 21h

0,5

**Points
par
page:**

16. PBX installé dans centre de calcul IT N° d'objectif d'évaluation 5.4.1 B2

4

Votre client souhaite installer son nouveau central téléphonique directement au centre informatique de son fournisseur. Ce centre informatique est entièrement virtualisé, de sorte qu'aucun composant matériel ne peut y être installé.

- a) Le SIP Trunk doit être relié au serveur d'appel en toute sécurité, les données doivent rester dans le réseau du fournisseur d'accès sans qu'elles ne circulent sur Internet. Quel est l'élément de réseau particulièrement important dans ce type de structure d'installation téléphonique ?

1

Le Session Border Controller (SBC), pour coupler des réseaux de données externes (non sécurisés) avec des structures informatiques internes (sécurisées) pour mettre en œuvre des sessions.

- b) Quels sont les technologies qui permettront de connecter des téléphones mobiles en interne à ce nouveau central téléphonique de l'entreprise ?

Cocher les cases oui ou non pour indiquer si les technologies sont compatibles.

Technologie	oui	non
Point d'accès WiFi	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Station de base IP-DECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Station de base DECT (TDM), 2 fils	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Réseau public 4G / 5G par VPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>

0,5

0,5

0,5

0,5

- c) Quels sont les deux aspects à prendre en compte dans la communication entre le site de l'entreprise et le site du centre de calcul IT ?

1

- **Sécurité (par cryptage, soit par un VPN, soit par l'utilisation de TLS / SRTP)**
- **Qualité (bande passante suffisante pour l'upload sur le site de l'entreprise)**

**Indication pour experts:
D'autres solutions sont également possibles.**

17. Protection des données N° d'objectif d'évaluation 5.5.5 B1

4

- a) Quelles sont les données personnelles qui doivent être protégées et quelles sont celles qu'il n'est pas nécessaire de protéger. Cochez les cases pour chacune des affirmations.

Données relatives à :	A protéger	Pas nécessaire de protéger	
Les opinions ou les activités religieuses, philosophiques, politiques ou syndicales.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5
La santé, l'intimité ou l'appartenance raciale.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5
Les mesures de l'aide sociale.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5
Poursuites et sanctions administratives ou pénales.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0,5

Un client vous informe que certains e-mails ne sont pas parvenus à plusieurs collaborateurs. Afin de mieux cerner l'erreur vous décidez de consulter les Log files du firewall.

- b) Expliquez pourquoi ceci n'est pas permis par la loi sans prendre des mesures particulières ?

1

Dans les fichiers Log, il est possible de tracer les faits et gestes des utilisateurs. Des informations personnelles comme par exemple les destinataires de mails ou les données des sites WEB visités sont visibles. La consultation de données personnelles ne peut être effectuée qu'en cas de suspicion d'abus.

- c) Comment pouvez-vous vous protéger ?

1

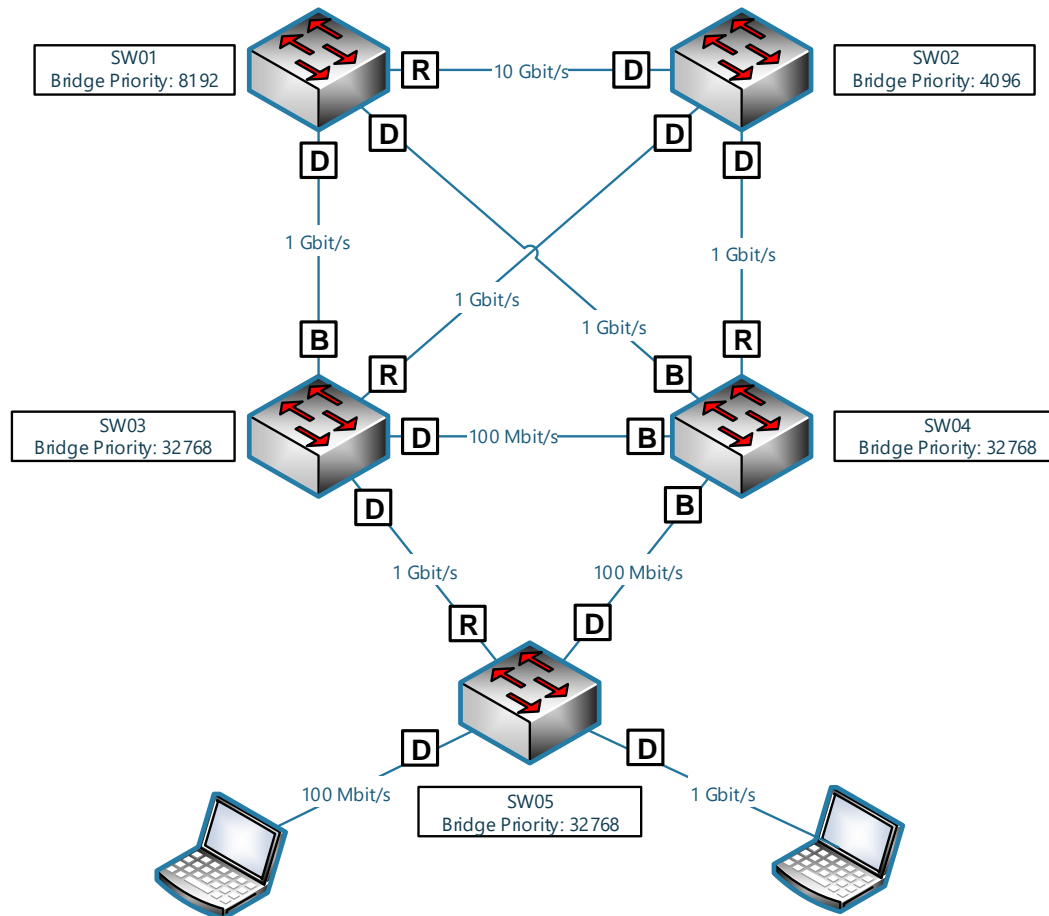
Dans un pareil cas, conformément à la loi sur la protection des données, chaque collaborateur doit être informé sur le traitement des données. Cela doit être confirmé au préalable par écrit.

18. Spanning Tree N° d'objectif d'évaluation 5.2.1 B3

5

- a) Dans le dessin, désignez chaque interface (dans le carré) par :
D (Designated Port) B (Blocked Port) R (Root Port)

4



- b) Pourquoi les ports correspondants doivent-ils être réglés sur " Blocked " ?

1

Cela permet de supprimer la formation de boucles.

Indication pour experts:

Pour les liaisons SW03 au SW04 et SW04 au SW05, les lettres (D - B) peuvent également être inversées.

Répartition des points:

Root Switch identifié → SW02 (1P)

Root Ports correctement placés (1P)

Blocked Ports correctement placés (1P)

Designated Ports correctement placés (1P)

Points

19. Zero Trust N° d'objectif d'évaluation 5.5.5 B2

3

- a) Quel est le principe le plus important dans un concept « Zero Trust » ?

1

Que ce soit de l'intérieur ou de l'extérieur du réseau, le système ne fait confiance à personne. Tout ce qui n'a pas été explicitement autorisé est bloqué. Tout accès est d'abord considéré comme non fiable, c'est le principe de base du concept « Zero Trust ».

- b) Citez deux exigences qui doivent être remplies dans un réseau « Zero Trust » ?

1

- **Toutes les applications et tous les utilisateurs doivent s'authentifier.**
- **Toutes les données doivent être transmises sous forme cryptée.**

- c) Expliquez brièvement comment un concept « Zero Trust » peut être mis en place dans une entreprise.

1

Pour toute communication venant de l'intérieur ou de l'extérieur du réseau, il faut prévoir des systèmes qui analysent, autorisent ou interdisent le trafic. Ceux-ci enregistrent également toutes les actions dans des fichiers journaux.

Indication pour experts:

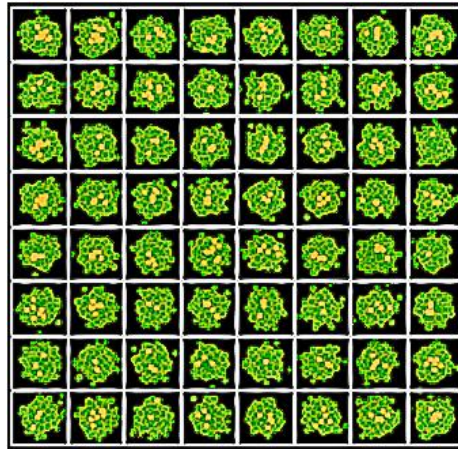
Il existe plusieurs produits qui remplissent ces fonctions, comme par exemple un bastion (Jump Host). L'accès aux ressources de l'entreprise (serveurs) n'est possible que via le bastion (Jump host). Aucun accès direct aux ressources n'est accordé. Les ressources peuvent se trouver dans un réseau virtuel (VLAN) spécifique pour lequel les utilisateurs ne connaissent pas les informations de connexion (nom d'utilisateur et mot de passe). L'accès aux appareils critiques peut être contrôlé, voire autorisé, par certaines personnes de l'entreprise.

Points
par
page:

20. Modulation N° d'objectif d'évaluation 5.1.6 B2

4

Dans les réseaux câblés, on utilise souvent des diagrammes de constellation pour évaluer la qualité de la transmission.



- a) En plus du diagramme de constellation, les valeurs mesurées "BER" et "MER" servent également à donner une indication sur la qualité de la transmission. Expliquez la signification de ces deux termes et citez l'unité de cette valeur mesurée.

2

BER (Bit-Error-Rate)

C'est le rapport entre le nombre de bits erronés et le nombre de bits reçus avant la correction d'erreurs (FEC). Il n'a pas d'unité de mesure, il est exprimé en nombre absolu.

MER (Modulations-Error-Rate)

Le MER représente une évaluation mathématique du taux de diffusion des points sur le diagramme de constellation. Le MER s'exprime en dB.

- b) Quelle est le type de modulation représenté sur le diagramme de constellation ci-dessus ?

1

QAM64 ou CAP64

- c) Quelle est votre évaluation de la qualité de la transmission représentée par le diagramme de constellation ci-dessus? Justifiez votre réponse.

1

La qualité de transmission n'est pas très bonne.

Les points de mesure sont très distribués dans les différents carrés et débordent parfois presque sur les carrés adjacents. Ceci ne permet pas une identification unique des signaux et ceci augmente le taux d'erreur dans la transmission.

21. Interférences sur les signaux N° d'objectif d'évaluation 5.1.6 B2

3

a)



L'illustration ci-dessus représente la transmission d'un signal. Ce signal subit une perturbation entre la source et le récepteur. Comment nomme-t-on cette perturbation et comment est-elle induite dans la transmission ?

Désignation :

Diaphonie (Crosstalk)

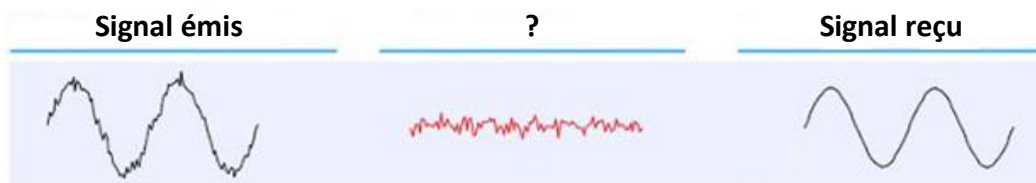
0,5

Origine :

Lors de la transmission, si plusieurs câbles se côtoient ils peuvent se perturber mutuellement. (Plus le nombre de câbles en cuivre regroupés dans un seul faisceau augmente, plus le problème s'aggrave. Ceci est aussi vrai si la fréquence de transmission augmente).

1

b)



Dans la représentation de la transmission de signal ci-dessus, il y a également une modification entre le signal émis et le signal reçu. Quel est le nom de la modulation utilisée dans ce cas et expliquez l'avantage de ce mode de modulation.

Désignation de la modulation :

Vectoring

0,5

Expliquez l'avantage de ce mode de modulation :

Si l'émetteur connaît les différentes perturbations qui agissent sur une ligne donnée, il peut envoyer un signal opposé qui compense les influences perturbatrices.

(L'amélioration du rapport signal bruit permet une vitesse de transmission de données plus élevée, cette technologie fonctionne sur le même principe que le contrôle actif du bruit utilisé dans les casques antibruit actifs).

1

22. Téléphonie IP N° d'objectif d'évaluation. 5.4.4 B3

3

Une caméra IP été installée dans l'entrée principale d'un bâtiment, elle est équipée d'un client SIP et connectée à un réseau LAN. Elle communique avec un PBX IP via le protocole SIP. Lorsqu'une personne passe devant la caméra, celle-ci déclenche automatiquement un appel SIP en direction du vidéophone (audio et vidéo) de la réception. La personne responsable de l'accueil peut alors voir la personne et communiquer avec elle.

- a) Citez un codec pour chaque type de communication (audio et vidéo) qui peut être utilisé pendant cet appel ?

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

0,5

Vidéo: **H.264**

0,5

Indication pour experts:

Un codec juste par type de communication pour obtenir tous les points.

- b) Si cet appel devait passer par un pare-feu, quelles sont les restrictions que vous pourriez rencontrer et quel paramètre devriez-vous modifier ?

2

Des problèmes de transmission audio pourraient intervenir, car le son est bidirectionnel et le firewall pourrait bloquer un des sens de communication.

Ces problèmes d'audio à sens unique peuvent souvent être résolus en configurant les paramètres ALG (Application Layer Gateway) du pare-feu.

Indication pour experts:

D'autres solutions sont possibles.

23. Localisation en intérieur N° d'objectif d'évaluation 5.5.3 B2

3

Un musée souhaite introduire une application qui permette de déterminer la position des visiteurs. Dès qu'un visiteur se trouve devant un objet exposé, un fichier audio contenant des informations sur l'objet est automatiquement lu sur l'application. Un positionnement rapide et précis est très important pour assurer aux visiteurs une expérience immersive de haute qualité.

a) Quelle technologie proposez-vous pour ce type d'application ?

1

Les balises BLE (Bluetooth Low Energy) qui ont été spécialement conçues pour le positionnement à l'intérieur des bâtiments.

b) Citez une solution de positionnement qui serait moins adaptée, voire qui ne fonctionnerait pas du tout pour ce genre d'application. Justifiez votre réponse.

1

- **WiFi : Trop lent et peu précis pour le positionnement.**
- **GPS : pas assez précis et ne fonctionne pas dans les bâtiments.**

c) Quelles sont les autres caractéristiques nécessaires pour qu'une telle solution soit utilisable en termes d'installation et d'exploitation ?
Citez deux de ces caractéristiques.

1

- **Fonctionnement sur batterie : pour réduire les frais d'installation**
- **Pas de câblage pour expositions modulaires**
- **Compatible avec les appareils mobiles courants**
- **Technologie basse consommation : pour une longue durée de vie de la batterie**
- **Configuration et dépannage faciles : pour une grande disponibilité**

**Indication pour experts:
D'autres solutions sont également possibles.**

24. VPN et cryptage N° d'objectif d'évaluation 5.2.1 B3

2

Cocher les cases oui ou non pour indiquer si les affirmations ci-dessous correspondent à la technologie VPN.

Affirmations	oui	non
Les fichiers sont obligatoirement cryptés pour être ensuite transférés via VPN.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Le cryptage DES est plus rapide que l'AES-256, c'est pourquoi DES est aujourd'hui utilisé comme cryptage standard dans le VPN.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Si un pirate informatique connaît la clé d'une connexion VPN, il peut décrypter le trafic HTTPS transmis dans le tunnel.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Une connexion VPN protège contre tout accès abusif aux données non sécurisées de l'entreprise.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

0,5

0,5

0,5

0,5

**Points
par
page:**

25. Routing N° d'objectif d'évaluation 5.5.9 B3

3

La table de routage suivante est affichée sur un périphérique réseau :

Réseau cible	Masque de sous réseau	Next Hop	Interface (IP)	Métrique
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

La passerelle pour l'accès à internet est :192.168.54.1

- a) Expliquez pourquoi l'hôte 192.168.78.43 ne peut pas être atteint par ce périphérique réseau ?

1

Il n'y a pas de destination cible 192.168.78.43 dans le tableau, sauf la route par défaut vers Internet. L'adresse 192.168.78.43 est cependant une adresse privée qui n'est pas routée sur Internet et qui est donc rejetée.

Il manque une entrée pour le réseau 192.168.78.40/28 dans lequel l'adresse 192.168.78.43 serait contenue.

- b) Quelle serait l'interface utilisée pour une connexion à 192.168.88.243 lorsque toutes les passerelles sont en service.

1

La connexion est établie via l'interface 192.16.2.12, car cette route présente la métrique la plus petite et donc le "coût" le plus bas.

- c) Quelle est l'adresse IP visible par un serveur web sur Internet lorsqu'un périphérique réseau se connecte à ce dernier par l'intermédiaire de cette table de routage ?

1

Du point de vue du serveur web seul l'adresse IP publique côté WAN du routeur qui fait office de passerelle Internet (192.168.54.1) sera visible. (L'adresse 192.168.54.1 est une adresse IP privée et n'est donc pas visible depuis Internet).