CORRIGÉ TYPE sécurité et contrôle de flux :

PARTIE 1 : QCM (8 points)

1 point par réponse correcte.

1. **Réponse : C** (Le transfert de fichiers (FTP) et l'e-mail)
    - *Justification :* Le trafic élastique est tolérant aux délais, contrairement au trafic streaming (VoIP, vidéo) qui est sensible.
2. **Réponse : A** (Une ACL par protocole, par interface et par direction)
    - *Justification :* C'est la règle des trois P décrite dans le cours pour l'application des ACLs.
3. **Réponse : C** (Le paquet est refusé/éliminé - refus implicite)
    - *Justification :* Si un paquet ne satisfait aucune condition, il est éliminé par le refus implicite ("deny all") à la fin de la liste.

+1

4. **Réponse : C** (ip access-group NO_ACCESS [in|out])
    - *Justification :* La commande ip access-group est utilisée pour appliquer une ACL (nommée ou numérotée) à une interface.

+1

5. **Réponse : B** (1-99)
    - *Justification :* La plage 1-99 est réservée aux ACLs IP standard.
6. **Réponse : B** (Le Manager SNMP)
    - *Justification :* Dans l'architecture SNMP, c'est le Manager (serveur) qui envoie les requêtes aux agents.
7. **Réponse : C** (C'est la capacité actuellement consommée par les applications et les services)
    - *Justification :* Définition précise de la bande passante utilisée.
8. **Réponse : B** (0.0.0.255)
    - *Justification :* Pour un masque /24 (255.255.255.0), le masque générique inverse les bits (255-255=0, 255-0=255), soit 0.0.0.255.

PARTIE 2 : Questions Générales VLAN (4 Points)

1 point par question. Réponses attendues :

1. **Qu'est-ce qu'un VLAN et avantage sécurité ? (1 pt)**
    - Un VLAN (Réseau Local Virtuel) est une segmentation logique d'un réseau physique.
    - **Avantage sécurité :** Il segmente les domaines de diffusion et isole les groupes d'utilisateurs, empêchant l'accès direct aux ressources sensibles sans passer par un routeur/pare-feu.
2. **Communication directe inter-VLAN ? (1 pt)**
    - **Réponse :** Non.
    - **Justification :** Les VLANs sont des réseaux de couche 2 distincts. Pour communiquer entre eux, le trafic doit passer par un équipement de couche 3 (routeur ou switch L3) pour être routé.
3. **Protocole de tagging ? (1 pt)**
    - Le protocole standard est **IEEE 802.1Q** (ou dot1q).
4. **Pourquoi changer le VLAN natif ? (1 pt)**
    - Pour limiter les risques d'attaques par **saut de VLAN (VLAN Hopping)** ou "double tagging", où un attaquant peut accéder à un autre VLAN en exploitant la gestion du trafic non étiqueté sur le VLAN natif par défaut (VLAN 1).

PARTIE 3 : Scénario ACL (8 points)

Barème suggéré : 2 points par étape/commande correcte.

Objectif : Configurer une ACL Étendue nommée "SECURE_R1".

1. **Création de l'ACL (1 pt)**

R1(config)# ip access-list extended SECURE_R1

2. **Règle 1 : Autoriser Admin vers Web en Telnet (2 pts)**
    - *Syntaxe correcte : permit tcp + source host + dest host + eq 23*

R1(config-ext-nacl)# permit tcp host 192.168.10.50 host 172.16.1.10 eq 23

3. **Règle 2 : Autoriser LAN vers Web en HTTP (2 pts)**
    - *Syntaxe correcte : permit tcp + source réseau + wildcard + dest host + eq 80*

R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 host 172.16.1.10 eq 80

4. **Règle 3 : Interdire tout autre trafic LAN vers Web (1 pt)**

- *Note : Le refus implicite à la fin de l'ACL suffit théoriquement, mais une règle explicite est souvent demandée pour la clarté.*

R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 host 172.16.1.10

(Accepter aussi si l'étudiant compte sur le "deny ip any any" implicite à la fin, tant que la logique est comprise).

5. **Application sur l'interface (2 pts)**

R1(config)# interface FastEthernet 0/0

R1(config-if)# ip access-group SECURE_R1 in