M2 informatique
Année universitaire 2018-2019 - Session 1

Consignes : Les documents sont interdits. Les calculatrices et téléphones portables sont interdits.

Examen d'administration réseau

Partie 1 – Couches basses (14 points)

Exercice 1.1 – Le protocole du *spanning tree* (4 points)

Considérez le réseau de la figure 1, où les ronds représentent des commutateurs, et les croisements de câbles représentent des concentrateurs.

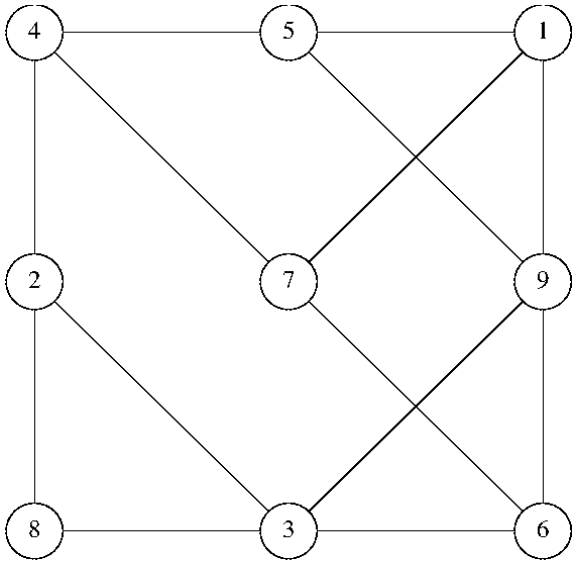

Figure 1 : Un de réseau avec 9 commutateurs et 2 concentrateurs.

Question 1.1.1 (1 point) : Dessinez le résultat du protocole du *spanning tree* sur ce réseau.

Question 1.1.2 (1 point) : Est-ce que cet arbre est adapté si les communications majoritaires ont lieu entre les commutateurs 2 et 4 ? Comment gérer cette situation ? Dessinez le nouveau résultat du protocole.

Le protocole RSTP *(Rapid Spanning Tree Protocol)* est un protocole permettant d'accélérer la convergence du protocole du *spanning tree* en cas de détection de la panne d'un lien. Le protocole RSTP définit quatre types de ports par concentrateur : le port racine (qui est celui sur le plus court chemin au commutateur racine), les ports désignés (qui sont les ports actifs, c'est-à-dire ceux qui reçoivent ou transmettent des trames), et le port alternatif (qui est le port conduisant au meilleur chemin alternatif vers le commutateur racine). Le protocole définit plusieurs règles en cas de détection d'une panne, et notamment les deux règles suivantes :

- Un port qui n'est pas connecté à un autre commutateur peut devenir immédiatement actif.
- Le port alternatif peut être utilisé immédiatement si la panne est identifiée sur le port racine.

Question 1.1.3 (1 point) : Considérez la première règle. Pourquoi un tel port n'était-il pas sélectionné avant la panne ? Qu'est-ce qui garantit qu'il n'y aura pas de boucle ? Comment le protocole peut-il détecter qu'il n'y a pas d'autre commutateur connecté à ce port ?

Question 1.1.4 (1 point) : Quelles sont les règles qui permettent d'établir le port alternatif ? Par exemple, est-ce qu'il y a des contraintes sur le port, sur le lien, sur le chemin, etc. ? Détaillez l'algorithme qui calcule ce port. Est-ce que cet algorithme trouve toujours une solution ? Que faire s'il n'en trouve pas ?

Exercice 1.2 – Configuration de VLAN (4 points)

Vous êtes l'administrateur réseau d'une PME. Vous avez configuré trois VLAN : un VLAN 1 pour l'équipe de développeurs, un VLAN 2 pour l'équipe de commerciaux et pour les gestionnaires, et un VLAN 3 pour l'administration réseau.

Question 1.2.1 (1 point) : Pourquoi avoir créé un VLAN spécifique pour l'administration réseau ? Contre quelles attaques est-ce que cette solution vous protège ?

Question 1.2.2 (1 point) : Contre quelles attaques cette solution ne vous protège pas ?

Question 1.2.3 (1 point) : Vous détectez un problème de routage : les paquets transmis du VLAN 1 ne sont pas routés au VLAN 2, et vice-versa. Citez deux causes possibles du problème.

Question 1.2.4 (1 point) : Vous avez établi un tunnel entre deux switchs en mode *trunk*. Cependant, les utilisateurs connectés sur le premier switch n'arrivent pas à interagir avec les utilisateurs connectés sur le deuxième switch. Citez deux causes possibles du problème.

Exercice 1.3 – L'attaque WannaCry (6 points)

WannaCry est le nom d'un virus informatique datant de mai 2017 et ayant infecté plus de 200 000 machines. WannaCry se base sur une vulnérabilité du protocole de partage de fichiers de Windows, nommé SMB, pour exécuter du code arbitraire avec les droits de l'utilisateur sur la machine distante, en utilisant un dépassement de buffer. Une fois la machine infectée, l'ensemble des fichiers de l'utilisateur est crypté et le virus demande à l'utilisateur de payer une rançon en *bitcoins* (monnaie virtuelle). Puis, le virus cherche à infecter d'autres machines. La faille avait été corrigée le 14 mars 2017.

Question 1.3.1 (1 point) : En tant qu'administrateur réseau, indiquez deux moyens qui auraient pu permettre à votre entreprise de ne pas subir cette attaque.

Question 1.3.2 (1 point) : Indiquez deux moyens qui auraient pu permettre à votre entreprise de limiter les dégats liés à cette attaque (en faisant l'hypothèse que certaines machines ont été infectées).

Question 1.3.3 (1 point) : À votre avis, pourquoi beaucoup d'entreprises ont malheureusement été victimes de ce virus ?

Question 1.3.4 (1 point) : En pratique, qu'est-ce qui peut empêcher un administrateur réseau d'installer des mises à jour ?

Question 1.3.5 (1 point) : Vous venez d'apprendre que l'attaque WannaCry est en train de sévir. Comment déterminer si les machines de votre entreprise sont attaquées, ou susceptibles de l'être ?

Question 1.3.6 (1 point) : Vous découvrez qu'au moins une machine du réseau de votre entreprise est attaquée. Comment réagissez-vous ?

Partie 2 – Couches hautes (6 points)

Exercice 2.1 : Questions de cours (3 points)

Question 2.1.1 (0.5 point) : Expliquez la différence entre une socket en mode connecté et une socket en mode non connecté. Donnez des exemples de protocoles utilisant les deux modes.

Question 2.1.2 (1 point) : Quelle est l'utilité du mécanisme de NAT ? Quelle est la différence entre le NAT statique et le NAT dynamique ? Quel est l'intérêt d'un firewall ?

Question 2.1.3 (1 point) : Comment fonctionne le protocole DHCP ?

Question 2.1.4 (0.5 point) : Qu'est-ce que le routage ?

Exercice 2.2 : Lecture de trames (3 points)

Question 2.2 (3 points) : On récupère la trame suivante sur le réseau via le sniffer Wireshark. Quelles informations contient-elle ? Analysez la trame afin de récupérer les différents protocoles encapsulés et les données des émetteurs et destinataires.

```
40 b9 3c bf aa 6f 98 90  96 a2 69 0d 08 00 45 00
00 38 27 66 00 00 80 11  02 49 ac 10 40 03 c0 a8
64 4a f0 01 00 35 00 24  4f 62 99 4f 01 00 00 01
00 00 00 00 00 00 06 65  63 6f 73 69 61 03 6f 72
67 00 00 01 00 01
```

Pour rappel :

Format d'une trame PDU-Ethernet II ou PDU-802.3 :

Destination (6)	Source (6)	Type/longueur (2)	Données (<1500)	Bourrage (<46)

Champ type/longueur :

- 0000 à 05DC = longueur IEEE 802.3
- 0800 = IP
- 0806 = ARP
- 0808 = Frame Relay ARP

Format d'une trape IP :

Version (4 bits)	Longueur entête sur 4 (4 bits)	Service QoS (1)	Longueur totale (2)	
Identifiant du fragment (2)			Drapeau (3 bits)	Position du fragment (13 bits)

TTL (1)	Protocole encapsulé (1)	Checksum (2)
Adresse IP source (4)		
Adresse IP destination (4)		
Données (variable)		

Drapeaux : 010 = autorisation de fragmentation, 001 = dernier fragment
Protocole encapsulé : 1 = ICMP, 6 = TCP, 17 = UDP

Format d'une trame TCP :

Port source (2)		Port destination (2)
Numéro de séquence (4)		
Numéro d'acquittement (4)		
Longueur entête (3 bits)	Flags TCP (13 bits)	Fenêtre TCP (2)
Checksum TCP (2)		Pointeur urgent (2)
Options TCP (variable)		
Données (variable)		

Flags TCP :

- 0000000100000 = URG
- 0000000010000 = ACK
- 0000000001000 = PSH
- 0000000000100 = RST
- 0000000000010 = SYN
- 0000000000001 = FIN

Format d'une trame UDP :

Port source (2)	Port destination (2)
Taille des données (2)	Checksum UDP (2)
Données (variable)	

Format d'une trame DNS :

Transaction ID (2)	Flags (2)	Nombre questions (2)	Nombre réponses RR (2)
Nombre d'autority RR (2)	Nombre d'additional RR (2)	Nom de l'hôte - zone 2 (variable)	
Type zone 2 (2)	Classe zone 2 (2)	Réponse - zone 3 (variable)	
Type zone 3 (2)	Classe zone 3 (2)	TTL réponse (4)	
Longueur adresse réponse (2)	Adresse recherchée (variable)	Nom des serveurs faisant autorité – zone 4 (variable)	
Options zone 4 (variable)		Enregistrements additionnels – zone 5 (variable)	
Options zone 5 (variable)			