Sécurité dans les réseaux informatiques

Exercices+ Solutions

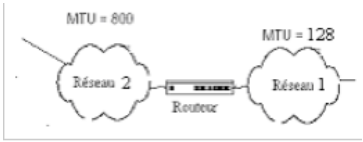
Vos ennemies connaissent les failles de sécurité de vos systèmes, les connaissez-vous?

Mohamed Mejri

October 2, 2016

Exercice 1

Soit le réseau suivant :



On suppose que le router a reçu un paquet dont l'en-tête (en hexadécimal est le suivent :

```
4500 012e 9d06 138a 2006 d11f 84d0 87bb 84c7 6633
```

Exercice 1 (suite)

Répondre aux questions suivantes (en décimal) :

1. Quelle est la taille totale du datagramme (en octets)?

   302 octets

2. Quelle est la durée de vie de ce datagramme?

   32

3. Quelle aurait été la réaction du routeur si la durée de vie est égale à 1?

   Détruit le datagramme et envoie un message ICMP à la machine 132.208.135.187 pour lui rendre compte de la situation.

4. Quel est le réseau qui a envoyé ce datagramme (Réseau 1 ou Réseau 2)? Justifier.

   Le réseau 2, car tous les datagrammes du réseau 1 auront comme longueur totale inférieure ou égale à 128 octets (MTU=128)

5. Est-ce un fragment ou un datagramme original?

   Il s'agit d'un fragment, car le champ "offset" est différent de zéro. En plus, il s'agit du dernier fragment, car le bit MF=0

Exercice 1 (suite)

6. Donner l'adresse source et l'adresse destination ?

   @source=132.208.135.187 @destination=132.199.102.51

7. Quelles seront les valeurs des champs (excepté «Header Checksum») des en-têtes de tous les fragments générés par le routeur?

Segment 1

4	5	0	124
40198		0 0 1	5002
31	06	Checksum	
132.208.135.187			
132.199.102.51			

Segment 2

4	5	0	124
40198		0 0 1	5015
31	06	Checksum	
132.208.135.187			
132.199.102.51			

Segment 3

4	5	0	94
40198		0 0 0	5028
31	06	Checksum	
132.208.135.187			
132.199.102.51			

Exercice 2

Soit le réseau 216.122.44.0

1. Quels sont la classe et le masque par défaut de ce réseau?

   La classe est "C" et le masque par défaut est 255.255.255.0

2. Si l'on veut brancher 12 segments physiques à ce réseau, quel sera le nouveau masque?

   La partie désignant le réseau dans le nouveau masque doit être à "1"; pour permettre 12 segments, 4 bits à "1" seront requis. D'où le nouveau masque : 255.255.255.240

3. Quel sera le maximal de machines à brancher à chaque sous-réseau?

   $2^4 - 2 = 14$ machines par segment

4. Énumérez les 12 sous-réseaux.

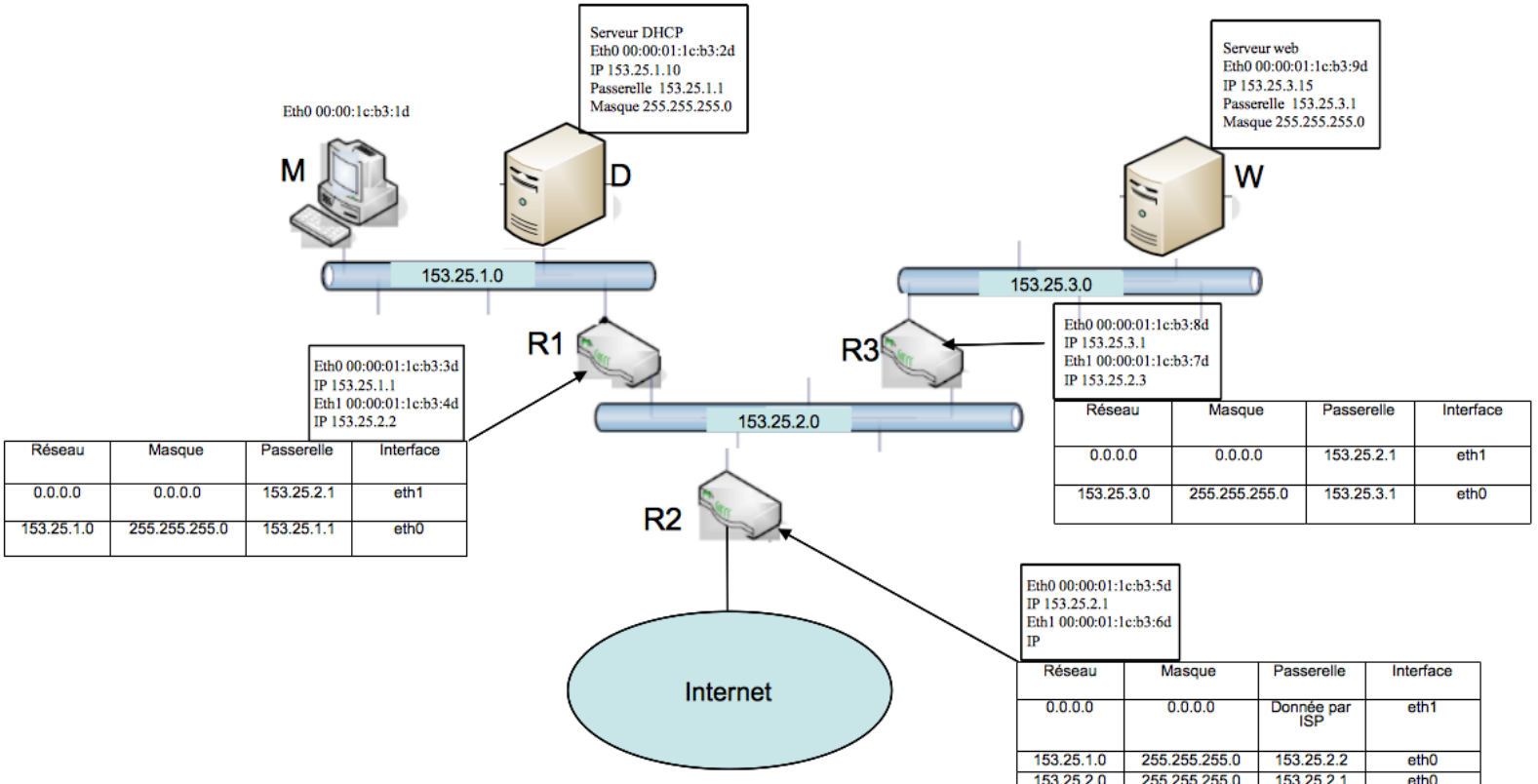
   216.122.44.16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 (14 sous-réseaux au total)

5. Énumérez la plage de toutes les machines qu'on pourrait brancher à un de ces sous-réseaux

   Pour le segment 216.122.44.16, les machines auront pour adresses la plage 216.122.44.17 à 216.122.44.30 (216.122.44.31 est une adresse de diffusion et elle ne peut pas être attribuée)

Exercice 3

- Nous considérons le réseau ayant la configuration suivante.



Réseau	Masque	Passerelle	Interface
0.0.0.0	0.0.0.0	153.25.2.1	eth1
153.25.1.0	255.255.255.0	153.25.1.1	eth0

Réseau	Masque	Passerelle	Interface
0.0.0.0	0.0.0.0	153.25.2.1	eth1
153.25.3.0	255.255.255.0	153.25.3.1	eth0

Réseau	Masque	Passerelle	Interface
0.0.0.0	0.0.0.0	Donnée par ISP	eth1
153.25.1.0	255.255.255.0	153.25.2.2	eth0
153.25.2.0	255.255.255.0	153.25.2.1	eth0
153.25.3.0	255.255.255.0	153.25.2.3	eth0

Exercice 3 (suite)

- Chaque routeur a une table de routage lui permettant d'acheminer les datagrammes à la bonne destination.
- Par exemple la table de routage de R1 indique qu'un datagramme ayant une destination dans le réseau 153.25.1.0 sera envoyé sur l'interface eth0. Tous les autres datagrammes seront envoyés via l'interface eth1 à la passerelle 152.25.2.1.
- L'entrée par défaut marquée par l'@ 0.0.0.0 est celle qui sera utilisée si aucune autre entrée dans le tableau ne correspond au datagramme en question.
- Les autres tables de routage se lisent de la même manière.
- L'adresse IP de l'interface eth1 du routeur R2 est donnée par le fournisseur de service Internet (ISP) et sa valeur n'est pas pertinente pour cet exercice.

Exercice 3 (suite)

- Le serveur DHCP (Dynamic Host Configuration Protocol) permet d'attribuer dynamiquement des adresses IP à des machines. On suppose que le protocole DHCP fonctionne comme suit :
  - Un ordinateur (un client) qui n'a pas d'adresse IP, utilise 0.0.0.0 comme adresse et fait un "broadcast général (255.255.255.255)". C'est un **DHCP Discover** à travers lequel le client regarde qui peut lui offrir une adresse IP. À noter que ce "broadcast général" ne quitte pas le réseau local et qu'il est généralement bloqué par le routeur.
  - Les serveurs DHCP qui interceptent la demande font une offre, via un message **DHCP Offer**, contenant l'@IP proposée, un masque de sous-réseau, la durée du contrat et potentiellement d'autres informations utiles telles que l'@IP de la passerelle par défaut et du serveur DNS
  - Le client choisit une parmi les propositions et envoie un **DHCP Request** pour demander la réservation de l'@IP
  - Le serveur DHCP confirme la réservation par un **DHCP Ack** et donne potentiellement toutes les informations utiles

Exercice 3 (suite)

- Nous supposons que la machine M vient de démarrer, elle ne connait pas encore son @IP et elle veut se connecter au serveur Web (noté par W) dont elle connait son @IP.
- Remplir le tableau suivant en donnant dans l'ordre chronologique toutes les étapes permettant à M d'atteindre son objectif
- Dans le champ commentaires donner une brève idée sur le contenu ou la description de la trame Vous pouvez utiliser des abréviations à partir du moment où la version intégrale apparait au moins une fois. Exemple ff:ff:ff:ff:ff:ff=broadcas 255.255.255.255=broadcast; 00:00:01:1c:b3:8d=@Mac0 (R3, eth0); 153.25.1.10 = @IP D; etc.
- La dernière trame à indiquée est celle contenant la confirmation de l'établissement de la connexion TCP entre M et W

Exercice 3 (suite)

No	@Mac Src.	@Mac Dest.	@IP Src.	@IP Dest.	Prot.
Commentaire					
1	00:00:01:1c:b3:1d	ff:ff:ff:ff:ff	0.0.0.0	255.255.255.255	DHCP
DHCP Discover 68 $\longrightarrow$ 67 : à la recherche d'une @IP					
2	00:00:01:1c:b3:2d	@MAC M	153.25.1.10	153.25.1.15	DHCP
DHCP Offer 67 $\longrightarrow$ 68; masque=255.255.255.0; passerelle=153.25.1.1 (R1, eth0) Nous supposons que 153.25.1.15 est une des adresses libres de D					
3	@MAC M	@MAC D	0.0.0.0	@IP D	DHCP
DHCP Request 68 $\longrightarrow$ 67					
4	@MAC D	@MAC M	@IP D	153.25.1.15	DHCP
DHCP Ack 67 $\longrightarrow$ 68; masque=255.255.255.0; passerelle = 153.25.1.1 (R1, eth0)					
5	@MAC M	Broadcast	@IP M	@IP (R1, eth0)	ARP
ARP Request : chercher l'@MAC de (R1, eth0)					
6	00:00:01:1c:b3:3d	@MAC M	@IP (R1, eth0)	@IP M	ARP
ARP Replay					
7	@MAC M	@MAC (R1, eth0)	@IP M	@IP 153.25.3.15	HTTP
TCP SYN : demande d'ouverture de connexion avec W sur le port 80					

Exercice 3 (suite)

No	@Mac Src.	@Mac Dest.	@IP Src.	@IP Dest.	Prot.
Commentaire					
8	00:00:01:1c:b3:4d	broadcast	153.25.2.2	153.25.2.1	ARP
ARP Request : rechercher @MAC de 153.25.2.1					
9	00:00:01:1c:b3:5d	@MAC (R1, eth1)	@IP (R2 ,eth0)	@IP (R1, eth1)	ARP
ARP Replay					
10	@MAC (R1, eth1)	@MAC (R2, eth0)	@IP M	@IP W	HTTP
TCP SYN : demande d'ouverture de connexion avec W sur le port 80					
11	@MAC (R2, eth0))	broadcast	@IP (R2, eth0)	153.25.2.3	ARP
ARP Request : rechercher @MAC de 153.25.2.3					
12	00:00:01:1c:b3:7d	@MAC (R2 eth0)	@IP (R3, eth1)	@IP (R2, eth0)	ARP
ARP Replay					
13	@MAC (R2, Eth0))	@MAC (R3, eth1))	@IP M	@IP W	HTTP
TCP SYN : demande d'ouverture de connexion avec W sur le port 80					
14	00:00:01:1c:b3:8d	broadcast	153.25.3.1	@IP W	ARP
ARP Request : rechercher @MAC de W					

Exercice 3 (suite)

No	@Mac Src.	@Mac Dest.	@IP Src.	@IP Dest.	Prot.
Commentaire					
15	00:00:01:1c:b3:9d	@MAC (R3, eth0)	@IP W	@IP (R3, eth0)	ARP
ARP Replay					
16	@MAC (R3, eth0)	@MAC W	@IP M	@IP W	HTTP
TCP SYN : demande d'ouverture de connexion avec W sur le port 80					
17	@MAC W	@MAC (R3, eth0)	@IP W	@IP M	HTTP
TCP SYN/ACK					
18	@MAC (R3, eth1))	@MAC (R2, eth0)	@IP W	@IP M	HTTP
TCP SYN/ACK					
19	@MAC (R2, eth0))	@MAC (R1, eth1)	@IP W	@IP M	HTTP
TCP SYN/ACK					
20	@MAC (R1, eth0)	@MAC M	@IP W	@IP M	HTTP
TCP SYN/ACK					
21	@MAC M	@MAC (R1, eth0)	@IP M	@IP W	HTTP
TCP ACK					

Exercice 3 (suite)

No	@Mac Src.	@Mac Dest.	@IP Src.	@IP Dest.	Prot.
Commentaire					
22	@MAC (R1,eth1)	@MAC (R2, eth0)	@IP M	@IP W	HTTP
TCP ACK					
23	@MAC (R2,eth0)	@MAC (R3, eth1)	@IP M	@IP W	HTTP
TCP ACK					
24	@MAC (R3,eth0)	@MAC W	@IP M	@IP W	HTTP
TCP ACK					