MINISTÈRE
DE LA DÉFENSE

Rappels réseaux TCP/IP

Premier Maître Jean Baptiste FAVRE
DCSIM / SDE / SIC / Audit SSI
jean-baptiste.favre@marine.defense.gouv.fr

sersim

MINISTÈRE
DE LA DÉFENSE

Au menu

- Modèle OSI, modèle TCP
- Principe d'encapsulation
- Structure des paquets et champs importants
- Établissement d'une connexion TCP
- Et au-dessus ?
- En théorie:
  - Adresses IP et sous-réseaux
- En pratique:
  - Quelques exemples de trafic réseau
- Les dangers du réseau

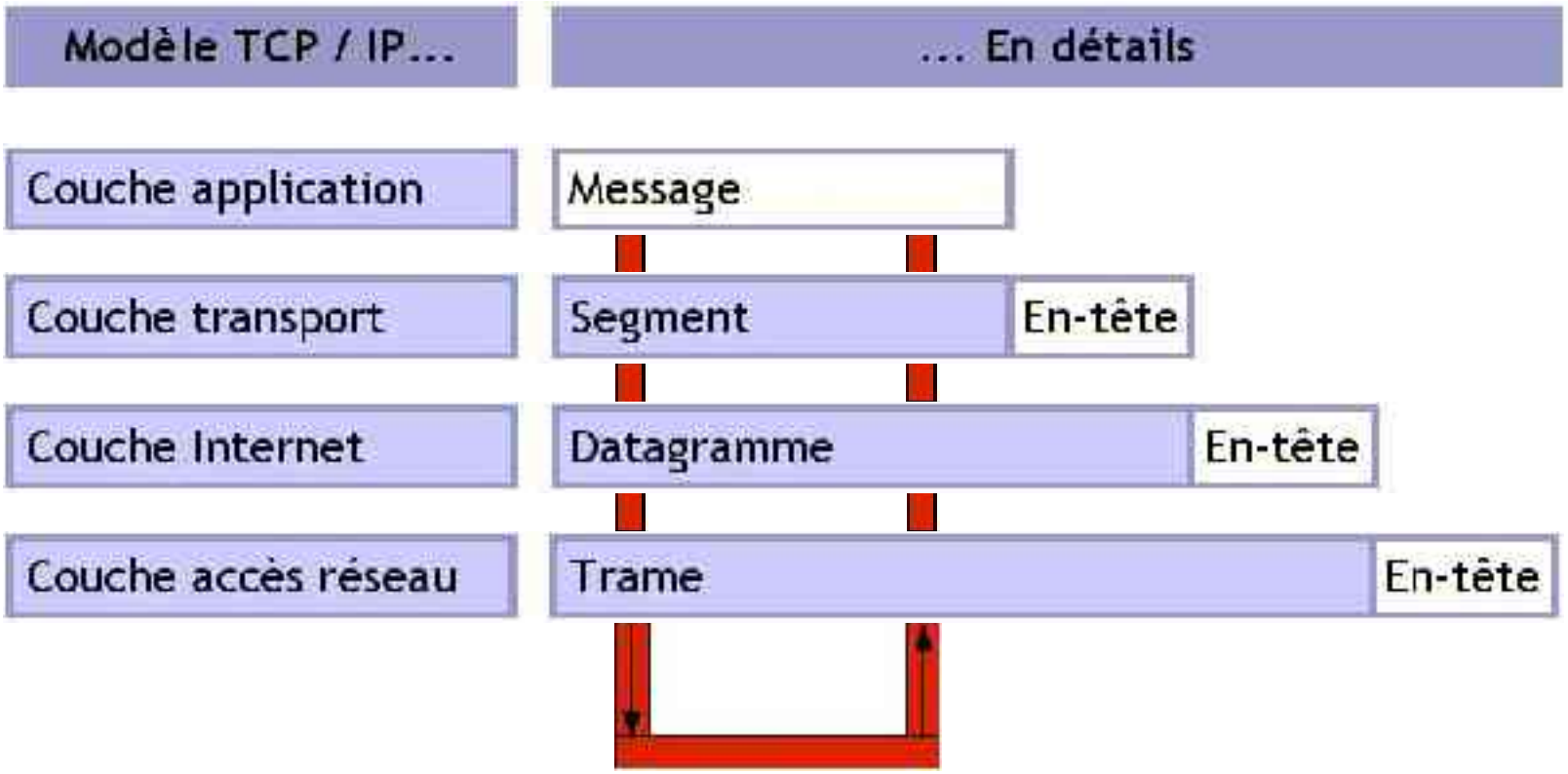
sersim

Modèle OSI, modèle TCP

Modèle TCP / IP	Modèle OSI	Protocoles
Couche application	Couche application	HTTP FTP POP SMTP
	Couche présentation	
	Couche session	
Couche transport	Couche transport	TCP / UDP
Couche Internet	Couche réseau	IP, ARP
Couche accès réseau	Couche liaison physique	Ethernet
	Couche physique	

MINISTÈRE
DE LA DÉFENSE

Principe d'encapsulation:



Structure: Datagramme IP

- Champs principaux:
  - Version: 4 ou 6
  - Protocole: 1 (ICMP), 6 (TCP), 17 (UDP), 50 (AH), 51 (ESP)
  - IP source et destination
  - Durée de vie (TTL)
  - Type de service (QOS)

Structure: Segment TCP

- Champs principaux:
  - Port source et destination
  - Drapeaux:
    - ACK: accuser réception des données,
    - PSH: transmettre les données au client,
    - RST: réinitialiser la connexion,
    - SYN: synchroniser la connexion,
    - FIN: clore la connexion

Structure: Segment UDP et ICMP

- Champs principaux:
  - Port source
  - Port destination

1		32
Port Source		Port destination
Longueur		Somme de contrôle
Donnees (Taille variable)		

- Champs principaux:
  - Type: 0 (echo response), 3(destination unreachable), 4(source quench), 5(redirection), 8 (echo request), 11(timeout), 13(timestamp), 14 (timestamp response)

1		32
Type	Code	Checksum
Message (Taille variable)		

Et au-dessus ?

- Couches applicatives
  - DNS: UDP/53
  - HTTP: TCP/80
  - POP: TCP/110
  - SMTP: TCP/25
  - FTP: TCP/20 (data) et 21 (control)
    - + les variantes SSL
  - SSH: TCP/22
  - Telnet: TCP/23
  - Netbios: TCP-UDP/137, UDP/138 et TCP/139
  - Etc, etc...

MINISTÈRE
DE LA DÉFENSE

En théorie: adresses IP

- 4 octets (32 bits)
  - Chaque octets peut aller de 0 à 255
  - En théorie 4 294 967 295 adresses IP disponibles
- Notation de l'adresse IP:
  - « Quadruplets pointés »: 192.168.0.1
  - Binaire: 11000000 10101000 00000000 00000001
  - Décimale: 3 232 235 521
- De moins en moins d'adresses disponibles
  - Création d'adresses « privées » (RFC 1918) et de la translation d'adresses

sersim

En théorie: Réseaux

- Les adresses IP sont réparties en réseaux
- 3 types de réseaux « publics »
  - Classe A: seul le premier octet est utilisé pour définir le réseau
  - Classe B: les 2 premiers octets
  - Classe C: les 3 premiers octets
- Répartition « arbitraire »
  - Classe A: de 1 à 126
  - Classe B: de 128 à 191
  - Classe C: de 192 à 254

MINISTÈRE
DE LA DÉFENSE

En théorie: Réseaux

- 3 classes de réseaux « privés »
  - Classe A: 10.0.0.0
  - Classe B: de 172.16.0.0 à 172.31.0.0
  - Classe C: de 192.168.0.0 à 192.168.255.0
- Exemple de réseau:
  - Adresse de réseau: 192.168.0.0
  - Masque de réseau: 255.255.255.0
  - Adresse de diffusion (broadcast): 192.168.0.255
    - Il y a donc 254 machines possibles dans un réseau de classe C (256 – adresse de réseau et adresse de broadcast)

sersim

MINISTÈRE
DE LA DÉFENSE

En théorie: Masques de sous-réseaux

- Utilisé pour « partager » une tranche d'adresses IP qui vous est allouée
- Permet de faire plusieurs sous-réseaux
- Ne permet pas de réutiliser plusieurs fois la même adresse IP
- Notation:
  - 192.168.0.0/255.255.255.0
  - 192.168.0.0/24
- Défini le nombre de bits de l'adresse IP identifiant le réseau

sersim

En théorie: Masques de sous-réseaux

- Calcul de sous-réseau
  - Adresse IP: 192.168.0.42
  - Masque de sous-réseau: 255.255.254.0
    - Adresse de réseau: 192.168.0.0
    - Adresse de diffusion: 192.168.1.255
- Comment ça marche ?

En théorie: Masques de sous-réseaux

- Transformons tout en binaire:
  - 192.168.0.42 = 11000000 10101000 00000000 00101011
  - 255.255.254.0 = 11111111 11111111 11111110 00000000
- Le réseau correspond aux bits à 1 du masque:

  11000000 10101000 00000000 00101011 (IP)
  11111111 11111111 11111110 00000000 (Mask)
  =
  11000000 10101000 00000000 00000000

  Soit ici 192.168.0.x auquel on accole la valeur minimale des adresses hôte (ici, x = 0)

MINISTÈRE
DE LA DÉFENSE

En théorie: Masques de sous-réseaux

- La plage d'adresse IP correspond aux valeurs mini et maxi du « reste » (bits à 0 du masque)

  11000000 10101000 00000000 ~~00000000~~ (Mask)
  11000000 10101000 00000000 00000000 (Mini)
  11000000 10101000 00000001 11111111 (Maxi)
  Soit de 192.168.0.0 à 192.168.1.255

  - Le mini est l'adresse de réseau
  - Le maxi est l'adresse de diffusion

- Dans cet exemple, on peut avoir 510 adresses IP (512 – adresse de réseau et adresse de diffusion)

En théorie: Masques de sous-réseaux

- Le choix du masque de réseau dépend du nombre d'IP à assigner.

Masque	Nb d'IP	Nb de sous-réseaux
255.255.255.0	254 (256-2)	1
255.255.255.128	126 ((256/2)-2)	2
255.255.255.192	62 ((256/4)-2)	4
255.255.255.224	30 ((256/8)-2)	8
255.255.255.240	14 ((256/16)-2)	16
255.255.255.248	6 ((256/32)-2)	32
255.255.255.252	2 ((256/64)-2)	64

MINISTÈRE
DE LA DÉFENSE

En théorie: Routage

- Nous avons partagé notre plage d'adresses en sous-réseau.
- Comment faire communiquer ces sous-réseaux ?

  => Il faut « router » le trafic
- Principe:
  - Disposer d'un élément réseau commun à plusieurs sous-réseau qui se chargera d'aiguiller le trafic
  - Il disposera donc d'une adresse IP par sous-réseau « géré »
  - Pour les machines de chaque sous-réseau, il agira comme passerelle

sersim

MINISTÈRE
DE LA DÉFENSE

En théorie: Routage

- La configuration réseau d'une machine doit donc comporter:
  - L'adresse IP
  - Le masque de sous-réseau
  - L'adresse IP de la passerelle (pour pouvoir « sortir » du sous-réseau de départ)
- Lors d'une connexion, la machine émettrice regarde si l'adresse IP de destination se trouve dans son sous-réseau
  - OUI: connexion directe
  - NON: connexion via la passerelle

sersim

En pratique: Trafic réseau

- Connexion directe d'une machine A vers B
  - Requête ARP:
    - MAC Source: MAC_A
    - MAC Destination: ff:ff:ff:ff:ff:ff
    - Données: « Who has IP_B? Tell IP_A »
  - Réponse ARP:
    - MAC Source: MAC_B
    - MAC Destination: MAC_A
    - Données: « IP_B is at MAC_B »

```
C0:08:74:4c:cc:0c ff:ff:ff:ff:ff:ff ARP who has 100.75.71.210? Tell 100.75.70.200
C0:30:6d:db:c4:45 00:08:74:4c:aa:0c ARP 100.75.71.210 is at 00:30:6d:db:c4:45
```

En pratique: Trafic réseau direct

- Connexion d'une machine A vers B (Suite)
  - Puis, requête IP:
    - MAC Source: MAC_A
    - MAC Destination: MAC_B
    - IP Source: IP_A
    - IP Destination: IP_B
    - Données TCP-UDP-ICMP-...

En pratique: Trafic réseau via routeur

- Connexion d'une machine A vers B hors sous-réseau
  - Requête IP:
    - MAC Source: MAC_A
    - MAC Destination: $MAC_{passerelle}$
    - IP Source: IP_A
    - IP Destination: IP_B
    - Données TCP-UDP-ICMP-...

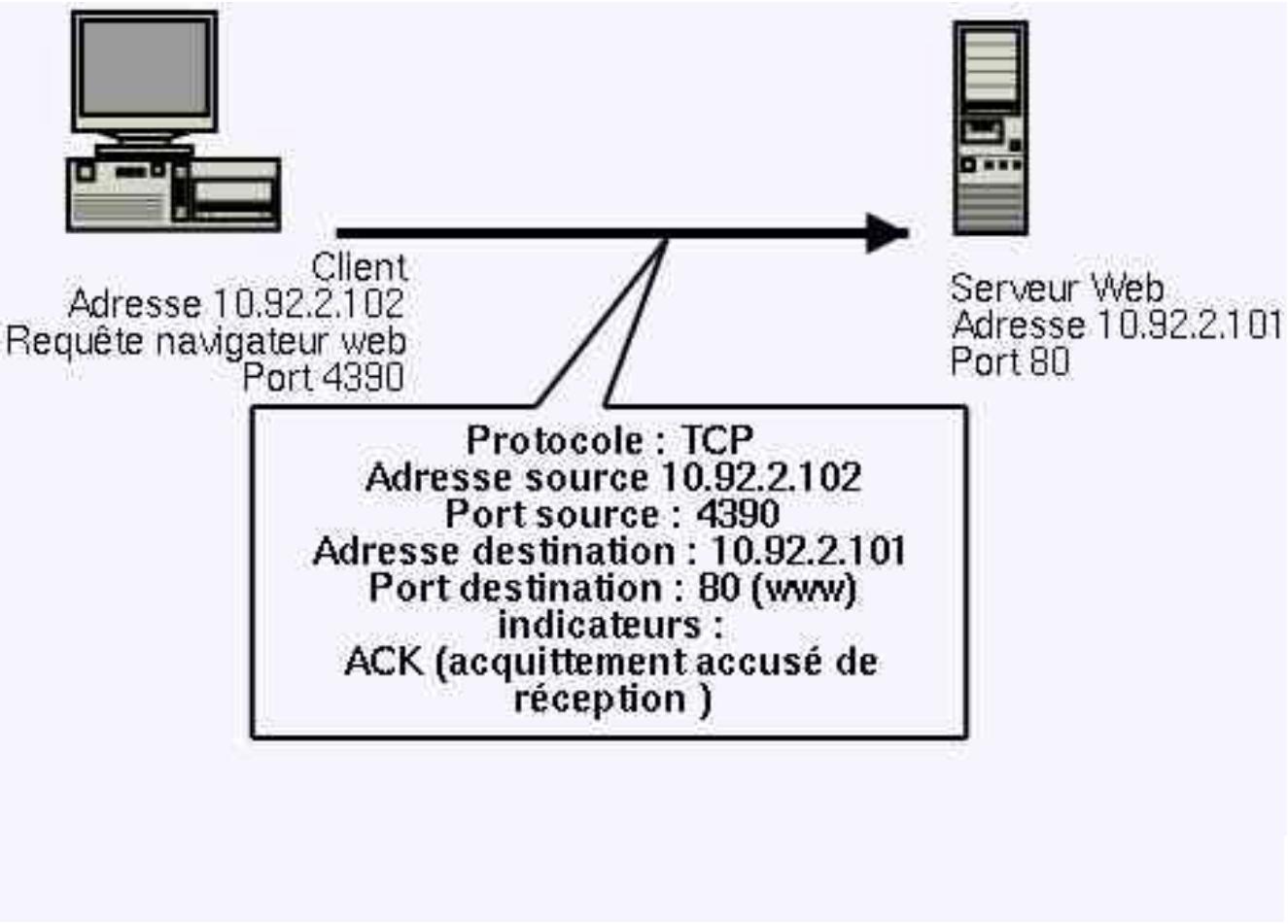
En pratique: Trafic réseau via routeur

Connexion d'une machine A vers B (Suite)

Le routeur reçoit la requête, voit qu'elle ne lui est pas directement destinée et la renvoie vers la machine B en fonction des routes programmées.

- Requête IP:
  - MAC Source: $MAC_{passerelle}$
  - MAC Destination: MAC_B
  - IP Source: IP_A ou $IP_{passerelle}$ si NAT
  - IP Destination: IP_B
  - TTL décrémenté de 1
  - Données TCP – UDP – ICMP - ...

Établissement d'une connexion TCP



Les dangers du réseau

- ARP Spoofing:
  - Saturer la cible de requêtes ARP
    - Détourner le trafic de la cible par notre machine.
- ARP Poisonning
  - Saturer 1 ou plusieurs machines de requêtes ARP
    - Isoler une ou plusieurs machines du reste du réseau

Les dangers

- IP Spoofing:
  - Modifier l'IP Source d'un paquet
    - Masquer la provenance d'une attaque
    - Contourner un dispositif d'authentification
    - Provoquer une attaque.
- TCP/UDP Flood
  - Saturer la cible de paquets TCP avec le drapeau SYN activé (ou de paquets UDP) pour mobiliser toutes ses ressources mémoire.
- TCP HighJacking
  - Prédiction des numéros de séquence
    - « perturber » une connexion établie

Les dangers

Attaques applicatives:

- Man-in-the-Middle (DNS ou éventuellement ARP)
- DOS (Exploitation d'un BOF)
- DDOS (Pareil mais à plusieurs)
- SQL Injection
- Cross-Site Scripting

Avez-vous de l'imagination ?

Rappels Réseau

Questions ?