Administration d'un Intranet

- Déterminer un plan d'adressage
- Configuration des tables de routages
- Utilisation d'un NAT (Network Adressing Translation)
- Mise en place d'un pare-feux (Firewall)

Rappel: Le routage dans Internet

- **La décision dans IP du routage:**
  - Table de routage:
    - Adresse destination (partie réseau), netmask, adresse routeur voisin
  - Consultation de la table de routage à l'arrivée d'un paquet:
    - Pour chaque ligne de la table de routage (***Adr, netmask, AdrRouteur***) faire
      - ★Si (***adresse destination du paquet*** AND ***netmask***) = ***Adr*** alors
        - envoyer le paquet au routeur voisin d'adresse ***AdrRouteur***
          - Pour cela faire appel à ARP pour connaître son adresse Ethernet
      - ★Sinon passer à la ligne suivante
    - Si l'adresse n'est pas dans la table alors renvoyer un paquet ICMP: "*destination inaccessible*" à la machine source

Environnement et contraintes

- Intranet d'une entreprise
- 3 types d'utilisateurs
  - 25 cadres
  - 25 administratifs
  - 10 ateliers
  - 2 machines spécialisées (SF1 et SF2) pour être des serveurs de fichiers
- Application NFS (Network File System) permettant de « voir » sur une machine locale, les fichiers sur le disque dur distant du serveur de fichier

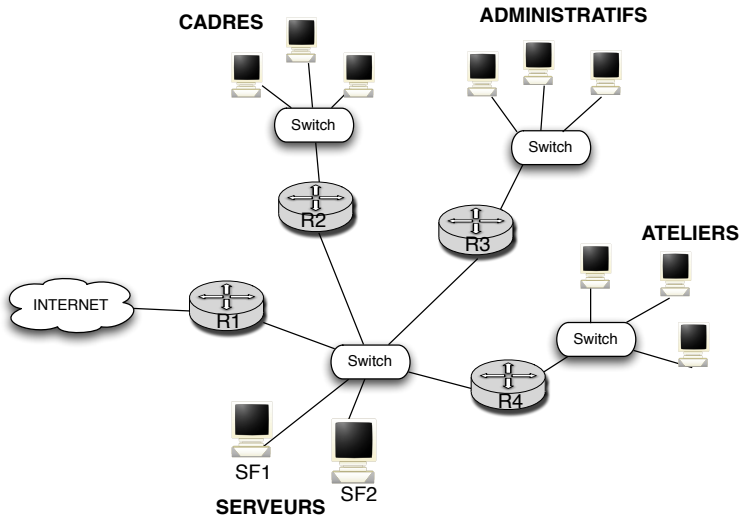
Contraintes

- Cadres : accès à toutes les machines de l'Intranet, SF1, SF2 et à l'Internet
- Administratifs : Accès à toutes les machines « administratifs » et SF1
- Ateliers : Accès à toutes les machines « Ateliers » et SF2
- Réseaux Ethernet
- Routeurs à 2 ports Ethernet

Choix de l'infrastructure réseau

- Découpage en plusieurs réseaux pour "isoler" les communications
- Diminue la charge des switchs
- Commutateurs (switch) Ethernet
  - Possibilité de les cascader si le nombre de ports est insuffisant
- Choix de la place des serveurs de fichier à discuter
- Un seul routeur en sortie:
  - sécurité, possibilités de filtrage…
  - Un port particulier vers Internet : ligne spécialisée avec un autre protocole: ADSL(PPP), ATM...
- Possibilités d'un seul routeur à 6 pattes (problème prix/ performances)

Topologie

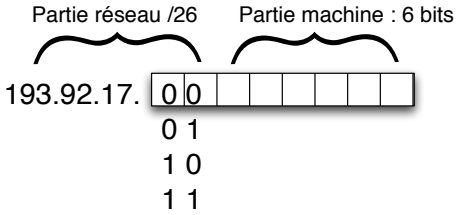


Choix des adresses

- **Adresse publique :** donnée par un organisme international de gestion des adresses (A chercher sur le web *Inter NIC* (Internet Network Information Center)
- **Supposons :** 193.92.17 / 24 (classe C)
- **Pour machines ne communiquant pas avec l'extérieur possibilité d'adresses privées:**
  - Trois plages d'adresses privées:
    - **10.0.0.0/8**: 10.0.0.1 à 10.255.255.254
    - **172.16.0.0/12**: 172.16.0.1 à 172.31.255.254
    - **192.168.0.0/16**: 192.168.0.1 à 192.168.255.254
  - Economie d'adresse mais si on veut changer de contraintes, il faut tout reconfigurer
  - Possibilités de faire de la translation d'adresses (NAT)

Découpage en "sous-réseaux" (Subnetting)

- On choisit d'affecter des adresses publiques à l'ensemble de l'Intranet
- 4 réseaux, 1 seule adresse publique
- Changement des netmasks
  - 2 bits de la partie machine sont attribués à la partie réseau de l'adresse
  - 2 bits de poids fort du dernier octet
  - On transforme un /24 en quatre /26



Sous-réseaux

- La partie réseau est appelé **Prefixe**
- **Netmask : 255.255.255.192**
- **4 réseaux:**
  - 193.92.17.**0 /26**
  - 193.92.17.**64 /26**
  - 193.92.17.**128 /26**
  - 193.92.17.**192 /26**
- **Nombre de machines par réseau : 64 -2 = 62**
  - Adresse partie machine
    - à 0 interdit (désigne un réseau)
    - à 11..111 interdit (broadcast)

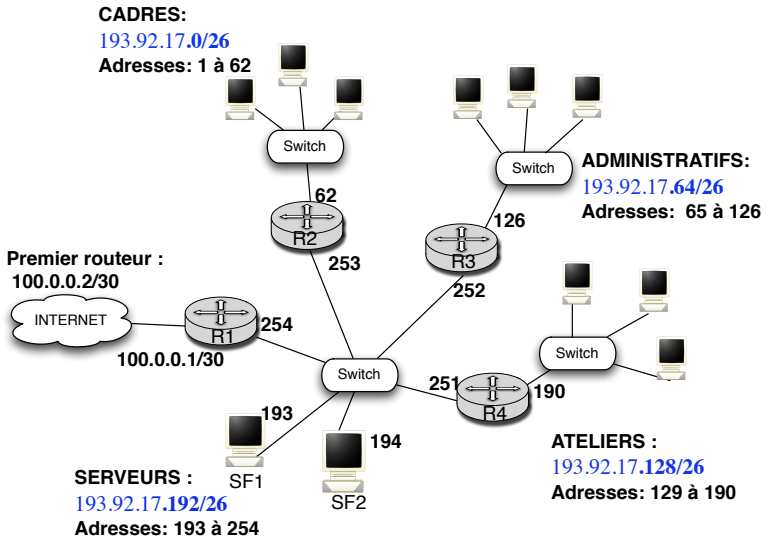
Sous-réseaux

- **Exemple pour le réseau** 193.92.17.**128 /26**
  - 1ère adresse machine: 10 000001=129 (en binaire)
  - dernière adresse: 10 111110=190
- **Plages d'adresses /26:**
  - 193.92.17.**1** à 193.92.17.**62**
  - 193.92.17.**65** à 193.92.17.**126**
  - 193.92.17.**129** à 193.92.17.**190**
  - 193.92.17.**193** à 193.92.17.**254**

Sous réseaux de tailles variables

- Supposons que le nombre de machine cadre est de 100
- Au lieu de quatre /26: un /25, un /26 et deux /27
  - 0 : 0 /25
  - 111: 224 /27
  - 110 : 192 /27
  - 10 : 128 / 26
- Plages d'adresses ?
- Nombre de machines sur chaque sous réseau ?

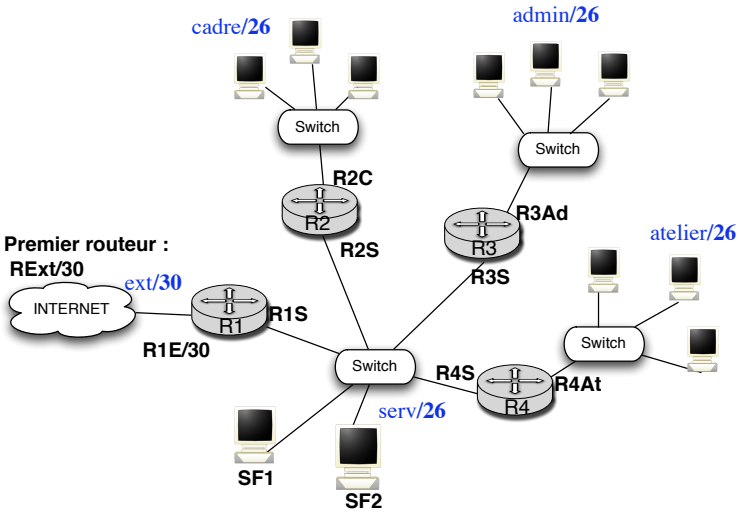
Plan d'adressage



Configuration routage

- Donner les tables de routage des machines et des routeurs en respectant les contraintes
- Mettre des noms à la place des adresses
  - /etc/hosts et /etc/networks
  - Réseaux:
    - cadre 193.92.17.0/26
    - admin 193.92.17.64/26
    - atelier 193.92.17.128/26
    - serveurs 193.92.17.192/26
- Format d'une table de routage :
  Adresse réseau destination / Netmask / Adresse du routeur voisin
  - Le Netmask est donné en décimal ou en notation ***/nombre de bits de la partie réseau*** (taille du préfixe)

Plan d'adressage avec des noms



Tables de routage

- **Les netmasks ne sont pas donnés: tous /26 : 255.255.255.192**
- **Machines "cadre" :**
  - **A l'origine:** *cadre direct*
    - **Connexion directe sur le réseau cadre après la configuration de l'interface**
  - **Une ligne par défaut:**
    - *Default R2C*
    - Quelle que soit l'adresse destination envoyer à R2C
    - **Defaut : adresse 0.0.0.0 Netmask 0.0.0.0**
- **Routeur 2 :**
  - *cadre direct*
  - *serv direct*
  - *admin R3S*
  - *atelier R4S*
  - *default R1S*
    - *Defaut pour l'accès à Internet*
- **Ping sur Internet ? ping sur machine atelier ?**

Tables de routage

- **Machines atelier :**
  - *atelier direct*
  - *Default R4At*
- **Machines atelier :**
  - Accède aussi à SF2 avec le ***default***
  - Les paquets à destination de l'Internet sont aussi envoyés sur le réseau (charge inutile)
- Il vaut donc mieux préciser les réseaux auxquels l'atelier peut accéder
  - De plus possibilité de mettre une adresse de machine dans la table de routage:
    - *SF2 /32 R4At*
    - *Attention Netmask change: /32 c'est à dire 255.255.255.255*

Tables de routage

- *ping* depuis cadre sur machine atelier ?
- Contrainte unidirectionnelle impossible au niveau routage
  - Si *cadre* accède à l'atelier alors l'atelier accède au cadre
- donc possibilité pour l'atelier avec contraintes seulement sur le serveur de fichier et cadre
  - *atelier direct*
  - *SF2 R4At (netmask 255.255.255.255)*
  - *cadre R4At*
- **Table de routage de R4:**
  - *serv direct*
  - *atelier direct*
  - *cadre R2S*

Tables de routage

- **Routeur 3 :**
  - *admin direct*
  - *serv direct*
  - *cadre R2S*
- **Machines admin**
  - *admin direct*
  - *SF1 R3Ad (netmask 255.255.255.255)*
  - *cadre R3Ad*
- **SF1:**
  - *serv direct*
  - *cadre R2S*
  - *admin R3S*

Tables de routage

- **SF2:**
  - *serv direct*
  - *cadre R2S*
  - *atelier R4S*
- **Routeur 1 :**
  - *serv direct*
  - *100.0.0.0 direct*
  - *cadre R2S*
  - *default RExt*

Problème de boucle

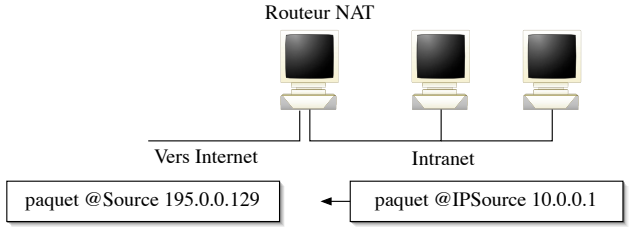
- Que se passe t-il si un paquet arrivant sur R1 depuis l'extérieur est à destination d'une adresse de Admin ?

Routage automatique

- Par exemple RIP
- Quel intérêt ?
- Que faire pour palier à une défaillance de R2 ?
- Contenu des paquets RIP ?

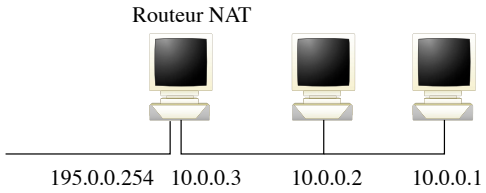
La translation d'adresse (NAT)

- Le routeur de sortie va modifier l'entête IP de tout paquet provenant d'une machine interne en remplaçant l'adresse source IP privée par une adresse publique
- Vue de l'extérieur, le routeur se fait passer pour la machine source
- **Deux types de NAT : statique et dynamique**
  - **Statique la correspondance @ Privée / @ publique est fixe**
  - **Dynamique : elle peut changer dans le temps**



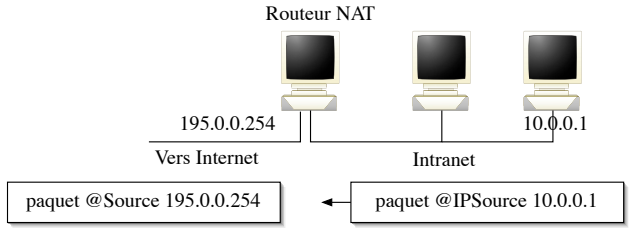
NAT STATIQUE: principe

- **Une adresse publique associée à chaque adresse privée**
- **Plage d'adresse publique 195.0.0.248/29**
- **Exemple d'associations Nat:**
  - **10.0.0.1 195.0.0.249**
  - **10.0.0.2 195.0.0.250**



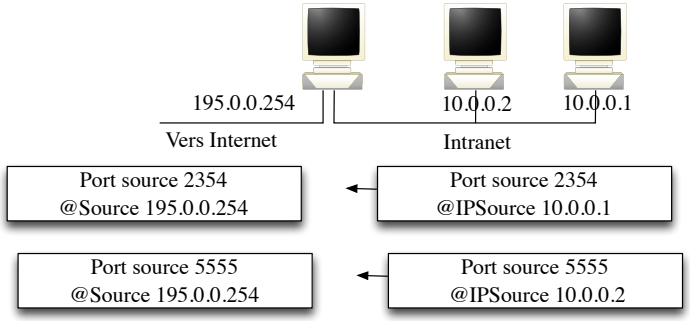
NAT dynamique ou IP masquerading : principe

- Permet d'attribuer dynamiquement lors des connexions des adresses IP publiques aux adresses privées
- L'adresse source des paquets devient l'adresse externe du routeur
- Problème : En cas de plusieurs connexions en parallèle comment le routeur peut il diriger les paquets vers la bonne machine ?



L'association connexion/@privée

- Se fait au moment du premier paquet qui sort en se rappelant le numéro de port source (mémorisation dans une table)

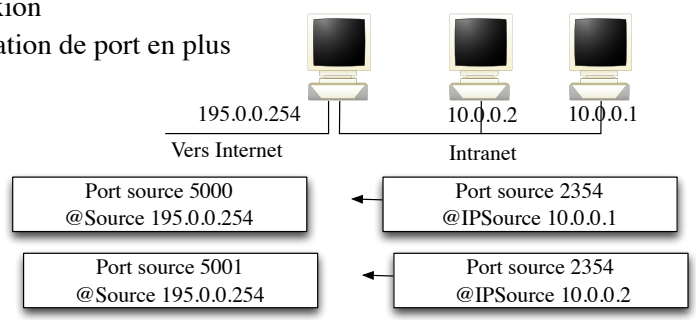


Mémorisation dans la table NAT:

2354 10.0.0.1
5555 10.0.0.2

L'association connexion/@privée

- Problème : si plusieurs connexions avec le même port source en même temps ?
- Attribution d'un port source virtuel unique à chaque connexion
- Translation de port en plus



Mémorisation dans la table NAT:

2354 10.0.0.1 5000
2354 10.0.0.2 5001

Nat Dynamique

- Une seule adresse publique suffit pour un nombre quelconque de machines dans l'Intranet
- On ne peut pas initier une connexion depuis l'extérieur
- Comment avoir un serveur WEB par exemple dans l'Intranet ?

Le *port forwarding*

- **Utiliser dans la NAT dynamique pour rendre une machine accessible depuis l'extérieur**
- **On mets en dur dans la table NAT du routeur**
  - port fixe: port privée/ adresse privée
  - Par exemple **21: 21/10.0.0.1** (port d'un serveur FTP)
  - Les paquets arrivant de l'extérieur vers (**195.0.0.254, 21**) seront redirigés vers (**10.0.0.1, 21**)
  - Problème si deux serveurs FTP sur 2 machines différentes ?
- **Le "*port mapping*" consiste à changer de port sur la machine interne**
  - Par exemple : **80: 8080/10.0.0.1**
  - Un serveur http est lancé sur 10.0.0.1 sur le port 8080

Sécurité

- **Pare-feux: filtrage à mettre en place sur le routeur 1**
- **Acces List**

- Liste d'interdictions ou d'autorisations suivant les adresses ou numéro de port, source et destination
    - Filtrage par machines (adresse IP source ou destination)
    - Filtrage par applications (numéro de port source ou destination)
    - Deux hypothèses possibles : tout ce qui n'est pas spécifié est soit interdit, soit autorisé

- **Une *Acces list* est associée à une interface (valable pour les paquets arrivant ou sortant par cette interface)**

Exemple d'*Acces list*

- *** veut dire «pour tout»**
- **Exemple sur l'interface extérieure de R1 pour les paquet sortants:**

Adr source / Adr Destination / Port source / Port destination

cadre/ * / * / * autorisé

* / * / * / * interdit

Règle 1 : on laisse passer tous les paquets provenant des machines cadres

Règle 2: Tous les autres paquets sont détruits

- Cela résout le problème du bouclage sur R1 pour les destinations différentes des machines cadres

Sécurité

- **Autre exemple d'Acces List pour autoriser les cadres seulement à naviguer sur les serveurs WEB d'Internet**

cadre/ * / * / 80 autorisé

* / * / * / * interdit

- Il existe d'autres types de filtres, par exemple sur le flag ACK de l'entête TCP (seul le paquet de demande de connexion porte le flag ACK à 0)

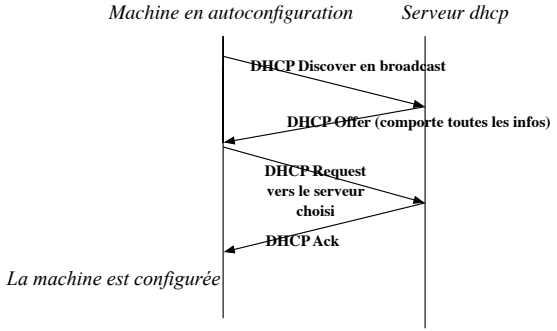
  Utile par exemple pour interdire un client extérieur d'initier une connexion dans l'Intranet

Aide à l'Administration
Le protocole DHCP (Dynamic Host Configuration Protocol)

- Intérêt:
    - Limiter le travail de l'administrateur système/réseau
    - Aucune action nécessaire sur une machine pour sa configuration réseau
    - Permet à une machine d'obtenir automatiquement son adresse IP afin de configurer son accès au réseau
    - Permet d'attribuer les adresses IP de façon dynamique
    - Utiliser par exemple par les fournisseurs d'accès pour attribuer des adresses aux clients
    - Le serveur DHCP connaît la plage d'adresses disponible et les affecte au fur et à mesure des demandes

Le protocole DHCP

- **Possibilité de plusieurs serveur DHCP sur le réseau**



Exemple de capture

- **Contenu du DHCP Ack**
  - Client IP address: 0.0.0.0 (0.0.0.0)
  - Your (client) IP address: 10.53.17.163 (10.53.17.163)
  - Next server IP address: 10.53.17.1 (10.53.17.1)
  - Relay agent IP address: 0.0.0.0 (0.0.0.0)
  - Client hardware address: 00:03:93:ed:b5:eb
  - Server host name not given
  - Boot file name not given
  - Magic cookie: (OK)
  - Option 53: DHCP Message Type = DHCP ACK
  - Option 54: Server Identifier = 10.53.17.1
  - Option 51: IP Address Lease Time = 10 minutes
  - Option 1: Subnet Mask = 255.255.255.0
  - Option 3: Router = 10.53.17.1
  - Option 6: Domain Name Server = 10.53.17.1
  - Option 15: Domain Name = "cybertable.com"
  - End Option

Configuration d'un serveur DHCP

- **Paramètres du serveur DHCP (démon dhcpd sous les Unix)**
  - Plage d'adresse IP à attribuer (souvent on donne la première et la dernière)
  - Adresses IP fixes (listes des adresses IP/Ethernet)
  - Un masque de sous-réseau pour ces adresses
  - Durée du bail DHCP
  - Adresse du serveur DNS
  - Nom du Domain