


جامعة عبد المالك السعدي
Université Abdelmalek Essaadi

Université Abdelmalek Essaadi
Faculté des Sciences et Techniques de
Tanger



FST
Tanger

Administration Réseaux (services sous Linux)

Pr. Abdelhamid ZOUHAIR


Intitulé du module	Administration Réseaux
Etablissement dont relève le module	Faculté des Sciences et Techniques de Tanger
Filière	Cycle Ingénieur LSI
Semestre d'appartenance du module	S 4

A. U: 2024/2025

Objectif du Module

L'objectif de ce cours est de préparer les étudiants à l'administration d'un réseau d'ordinateurs. L'accent sera mis sur les aspects pratiques et concrets de l'administration d'un réseau d'entreprise pour les systèmes UNIX et Windows /Présenter les différentes services :

- ✂ Serveur FTP, Telnet et SSH
- ✂ Serveur DHCP, Serveur HTTP Apache
- ✂ VPN & OpenVPN
- ✂ Serveur NFS et Serveur de fichiers Samba
- ✂ Configuration VLAN, VTP et STP
- ✂ Configuration des ACLs
- ✂ Configuration SNMP
- ✂ Serveur d'impression
- ✂ ...



Plan

- Serveur FTP, Telnet et SSH
- Serveur HTTP Apache
- VPN & OpenVPN
- Configuration VLAN, VTP et STP

▪ACL (Listes de Contrôle d'Accès)

- Le protocole de supervision SNMP
- Serveur NFS et Serveur de fichiers Samba
- Serveur DNS (BIND9)
- Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)
- Serveur d'impression

3



ACL (Listes de Contrôle d'Accès)

ACL (Listes de Contrôle d'Accès)

Introduction à la liste de contrôle d'accès

Une **liste de contrôle d'accès (ACL - Access Control List)** fait référence à deux concepts distincts:

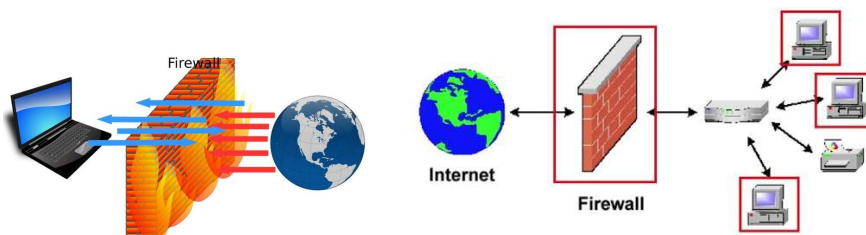
1. En système Linux: les ACL permettent de définir des permissions supplémentaires pour un ou plusieurs utilisateurs / groupes sur un fichier / répertoire.
2. En **réseau**, une liste des **adresses** et **ports** autorisés ou interdits par un **pare-feu**.

ACL (Listes de Contrôle d'Accès)

Introduction à la liste de contrôle d'accès (suite)

Une **ACL (Access Control List) réseau** est un **outil essentiel pour contrôler et sécuriser le trafic** en appliquant des règles de filtrage adaptées aux besoins de l'infrastructure informatique.

But : Gérer le trafic + sécuriser l'accès d'un réseau en entrée comme en sortie;



ACL (Listes de Contrôle d'Accès)

Introduction à la liste de contrôle d'accès (suite)

Dans un réseaux sans ACL (Listes de Contrôle d'Accès), plusieurs **problèmes** de sécurité et de performance peuvent survenir :

☐ **Accès non contrôlé aux ressources réseau**

- Tous les utilisateurs et périphériques peuvent accéder librement aux ressources du réseau, y compris les données sensibles.
- Cela peut entraîner des violations de confidentialité et des fuites d'informations critiques.

☐ **Risque accru de cyberattaques**

- Sans ACL, les attaquants peuvent facilement pénétrer le réseau et exécuter des attaques comme le **scanning**, le **brute force**, ou encore l'**exfiltration de données**.

☐ **Propagation des logiciels malveillants**

- Les virus, ransomwares et autres logiciels malveillants peuvent se propager rapidement sur un réseau non sécurisé.

☐ **Exposition aux attaques internes**

- Un employé malveillant peut facilement accéder à des ressources sensibles s'il n'y a pas d'ACL pour restreindre son trafic.
- Les ACL permettent de limiter les accès en fonction des adresses IP, des ports ou des services autorisés.

ACL (Listes de Contrôle d'Accès)

Introduction à la liste de contrôle d'accès (suite)

Dans un réseaux sans ACL (Listes de Contrôle d'Accès), plusieurs **problèmes** de sécurité et de performance peuvent survenir :

☐ **Utilisation abusive des ressources réseau**

- Sans ACL, n'importe qui peut consommer de la bande passante, ce qui peut ralentir le réseau.

☐ **Impossibilité de segmenter le réseau**

- Un réseau sans ACL est un réseau totalement ouvert où toutes les machines peuvent interagir entre elles.
- Avec des ACL, on peut isoler certains départements, serveurs ou zones critiques pour améliorer la sécurité.

☐ **Difficulté à appliquer les politiques de sécurité**

- Sans ACL, il est difficile d'imposer des règles de sécurité sur qui peut accéder à quoi et comment.
- Cela complique la mise en conformité avec des normes comme **ISO 27001**, **RGPD**, etc.

ACL (Listes de Contrôle d'Accès)

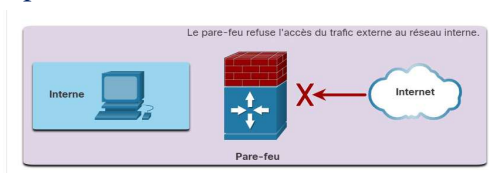
Définition des listes de contrôle d'accès

- ❑ Les **listes de contrôle d'accès** sont des **listes** de **conditions** qui sont appliquées au **trafic** circulant via une **interface** de **routeur**;
- ❑ Les listes indiquent au routeur (**pare-feu**) les types de paquets à **accepter** ou à **rejeter**;
- ❑ Certaines conditions dans une ACL sont des **adresses source** et de **destination**, des **protocoles** et des **numéros de port** de couche supérieure;

ACL (Listes de Contrôle d'Accès)

Définition des listes de contrôle d'accès (suite)

- ❑ Des ACL peuvent être créées pour tous les protocoles routés, tels qu'IP et IPX;
- ❑ Une ACL séparée doit être créée pour chaque direction : une pour le trafic entrant et une pour le trafic sortant;
- ❑ **Exemple** : Si le routeur a deux interfaces configurées pour IP, AppleTalk et IPX, 12 listes d'accès distinctes sont nécessaires : une liste pour chaque protocole, fois deux pour la direction (entrée et sortie), fois deux pour le nombre d'interfaces;



ACL (Listes de Contrôle d'Accès)

Autres définitions des listes de contrôle d'accès

- ❑ Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet.
- ❑ Une fois configurées, les listes de contrôle d'accès assurent les tâches suivantes :
 - Elles fournissent un niveau de sécurité de base pour l'accès réseau. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'y avoir accès.
 - Elles filtrent le trafic en fonction de son type. Ainsi, une liste de contrôle d'accès peut autoriser le trafic des e-mails, mais bloquer tout le trafic Telnet.
 - Elles limitent le trafic réseau pour accroître les performances réseau.
 - Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau. Les listes de contrôle d'accès peuvent autoriser ou refuser à un utilisateur l'accès à certains types de fichier, tels que FTP ou HTTP.
 - Elles contrôlent le flux de trafic. Les listes de contrôle d'accès peuvent limiter l'arrivée des mises à jour de routage par exemple.

11

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès

- ❑ **Par défaut, aucune liste de contrôle d'accès n'est configurée** sur les routeurs. Par conséquent, les routeurs ne filtrent pas le trafic, par défaut. Le trafic qui entre dans le routeur est routé uniquement en fonction des informations de la table de routage.
- ❑ Toutefois, lorsqu'une liste de contrôle d'accès est appliquée à une interface, le routeur évalue en outre tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminés.
- ❑ En dehors de l'autorisation ou du blocage du trafic, les listes de contrôle d'accès peuvent être utilisées pour sélectionner les types de trafic à analyser, à acheminer et à traiter selon d'autres méthodes.
 - Par exemple, les listes de contrôle d'accès permettent de classer le trafic par ordre de priorité.

12

ACL (Listes de Contrôle d'Accès)

Utilisation de listes de contrôle d'accès pour sécuriser les réseaux

Fonctionnement des listes de contrôle d'accès

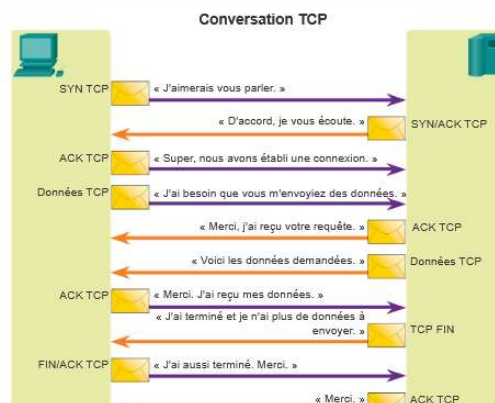
- ❑ L'ordre des instructions ACL est important;
- ❑ Le **Firewall** (Pare-feu) teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin;
- ❑ Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées;
- ❑ **Listes de contrôle d'accès entrantes** : les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet. Si le paquet est autorisé à l'issue des tests, il est soumis au routage;
- ❑ **Listes de contrôle d'accès sortantes** : les paquets sortants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante;

ACL (Listes de Contrôle d'Accès)

Fonctionnement des listes de contrôle d'accès IP

- ❑ Les listes de contrôle d'accès permettent aux administrateurs de contrôler le trafic entrant et sortant d'un réseau. Il peut tout simplement s'agir d'autoriser ou de refuser le trafic en fonction des adresses réseau ou bien d'atteindre des objectifs plus complexes, notamment contrôler le trafic réseau en fonction du **port TCP** demandé.

- ❑ Pour comprendre le principe de filtrage du trafic appliqué par une liste de contrôle d'accès, le plus simple est d'examiner le dialogue qui intervient dans une conversation TCP, notamment lorsque vous demandez une page Web.



ACL (Listes de Contrôle d'Accès)

Fonctionnement des listes de contrôle d'accès IP Ports TCP

Plage de numéros de port	Groupe de ports
0 à 1023	Ports réservés
De 1024 à 49151	Ports inscrits
49152 à 65535	Ports dynamiques et/ou privés

Légende

Ports TCP inscrits :

1863	MSN Messenger
2000	Cisco SCCP (VoIP)
8008	Alternate HTTP
8080	Alternate HTTP

Ports TCP réservés :

21	FTP
23	Telnet
25	SMTP
80	HTTP
143	IMAP
194	Internet Relay Chat (IRC)
443	Secure HTTP (HTTPS)

15

ACL (Listes de Contrôle d'Accès)

Fonctionnement des listes de contrôle d'accès IP Ports TCP

Définitions et différences entre les types de ports

1. Ports réservés

- Plage : **0 à 1023**
- Attribués par l'IANA (Internet Assigned Numbers Authority).
- Utilisés pour des services réseau connus (ex. : HTTP - 80, HTTPS - 443, FTP - 21, SSH - 22).

2. Ports inscrits (Registered Ports)

- Plage : **1024 à 49151**
- Également gérés par l'IANA.
- Utilisés par des applications spécifiques mais non standardisées (ex. : MySQL - 3306, Microsoft SQL Server - 1433).

3. Ports dynamiques/éphémères (Dynamic/Ephemeral Ports)

- Plage : **49152 à 65535**
- Assignés temporairement par le système d'exploitation pour les connexions client.
- Utilisés lors des communications temporaires (ex. : navigation web, messagerie instantanée).

Différence clé :

- **Ports réservés et inscrits** sont prédéfinis et souvent liés à des services spécifiques.
- **Ports dynamiques** sont attribués temporairement pour des sessions en cours.

16

ACL (Listes de Contrôle d'Accès)

Fonctionnement des listes de contrôle d'accès IP Ports UDP

Plages d'adresses des ports UDP

Les ports UDP suivent la même répartition que ceux de TCP :

❑ Ports réservés (Ports bien connus) : 0 – 1023

- Attributés par l'IANA pour les services connus (ex. : DNS - 53, DHCP - 67,68).

❑ Ports inscrits : 1024 – 49151

- Utilisé par des applications spécifiques (ex. : 3478/5349 pour VoIP, 1812 pour RADIUS).

❑ Ports dynamiques/éphémères : 49152 – 65535

- Assignés temporairement par le système pour les connexions client.

❑ **UDP vs TCP** : Les plages sont identiques, mais UDP est privilégié pour les communications rapides comme VoIP, streaming et jeux en ligne. Contrairement à TCP, UDP ne garantit pas la livraison des paquets ni leur ordre d'arrivée.

17

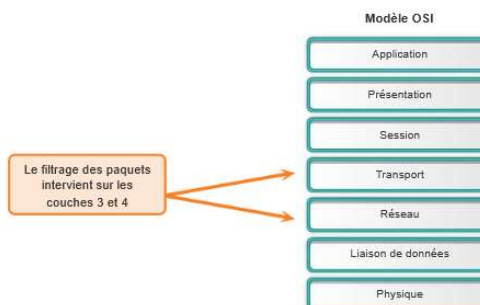
ACL (Listes de Contrôle d'Accès)

Fonctionnement des listes de contrôle d'accès IP

Comment les listes de contrôle d'accès utilisent-elles les informations transmises lors d'une conversation TCP/IP pour filtrer le trafic ?

- ❑ Le filtrage des paquets, parfois appelé filtrage statique des paquets, contrôle l'accès à un réseau en analysant les paquets entrants et sortants et en les transmettant ou en rejetant selon des critères spécifiques, tels que l'adresse IP source, les adresses IP de destination et le protocole transporté dans le paquet.

Un routeur filtre les paquets lors de leur transmission ou de leur refus conformément aux règles de filtrage. Lorsqu'un paquet arrive sur un routeur de filtrage des paquets, le routeur extrait certaines informations de l'en-tête de paquet. Celles-ci lui permettent de décider si le paquet peut être acheminé ou non en fonction des règles de filtre configurées. Comme le montre la figure, le filtrage des paquets peut fonctionner sur différentes couches du modèle OSI ou du modèle TCP/IP.



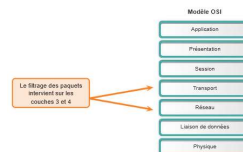
ACL (Listes de Contrôle d'Accès)

Fonctionnement des listes de contrôle d'accès IP

Filtrage des paquets

- ❑ Pour évaluer le trafic réseau, la liste de contrôle d'accès extrait les informations suivantes de l'en-tête de paquet de couche 3 :

- Adresse IP source
- Adresse IP de destination
- Type de message ICMP



- ❑ La liste de contrôle d'accès peut également extraire des informations de couche supérieure à partir de l'en-tête de couche 4, notamment :

- Port source TCP/UDP
- Port de destination TCP/UDP

19

ACL (Listes de Contrôle d'Accès)

Types de listes de contrôle d'accès

ACL (Listes de Contrôle d'Accès)

Types de listes de contrôle d'accès IPv4

- ❑ Les listes de contrôle d'accès (ACL) sont généralement divisées en trois grandes catégories : l'ACL **standard**, l'ACL **étendue** et l'ACL **nommée**. Ces dernières offrent des options plus flexibles de gestion du trafic réseau.
- ❑ ACL **standard** est une liste de contrôle d'accès qui filtre le trafic réseau en fonction de l'adresse **IP source uniquement**. Elle permet d'autoriser ou de bloquer l'accès à un réseau ou à un appareil sans tenir compte du protocole ou du port utilisé.
- ❑ ACL **étendue** est une liste de contrôle d'accès qui filtre le trafic réseau en fonction de **plusieurs critères**, notamment :
 - L'adresse IP source et destination
 - Le protocole (TCP, UDP, ICMP, etc.)
 - Les ports source et destination
 - Le type de service (ToS), les flags TCP, etc.

L'ACL étendue est idéale pour un filtrage avancé et un meilleur contrôle du trafic

- ❑ ACL **nommée** : C'est une version plus souple de l'ACL standard et étendue. Elle permet de créer des ACL avec des noms plutôt que des numéros, ce qui rend la gestion et l'organisation des ACL plus claires et pratiques. Elles peuvent être standard ou étendues, mais avec une syntaxe plus intuitive.

21

ACL (Listes de Contrôle d'Accès)

Types de listes de contrôle d'accès IPv4

L'ACL **nommée** peut être utilisée aussi bien pour les **ACL standards** que pour les **ACL étendues**.

- ❑ **ACL nommée** est une ACL standard à laquelle on a affecté un nom.
 - Filtre uniquement sur l'adresse IP source.
- Exemple
 - ip access-list standard MON_ACL_STANDARD
 - permit 192.168.1.0 0.0.0.255
 - deny any
- ❑ **ACL nommée étendue** : est une ACL étendue à laquelle on a affecté un nom.
 - Filtre sur plusieurs critères : adresse source/destination, protocole, ports, etc.
- Exemple:
 - ip access-list extended MON_ACL_ETENDUE
 - permit tcp 192.168.1.0 0.0.0.255 any eq 80
 - deny ip any any
- ❑ **Avantages des ACL nommés** :
 - Plus lisibles et faciles à gérer que les ACL numérotées.
 - Permettent d'ajouter/supprimer des règles sans tout reconfigurer.

22

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès standard

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès standard

Listes de contrôle d'accès standard

❑ Les listes de contrôle d'accès standard permettent d'autoriser et de refuser le trafic en provenance **d'adresses IP source**.

❑ Pour créer une liste ACL standard numérotée, utilisez la commande **access-list**.

Routeur(config)# access-list *numéro-liste-accès* deny /permit *ip-source* [*masque-générique-source*]

➤ ***numéro-liste-accès*** : Numéro de l'ACL standard (compris entre 1 et 99, ou 1300 et 1999).

➤ ***permit* | *deny*** : Indique si le trafic doit être autorisé (**permit**) ou bloqué (**deny**).

➤ ***ip-source*** : Adresse IP source des paquets concernés.

➤ ***masque-générique-source*** : c'est le **masque générique** utilisé pour spécifier une plage d'adresses.

❑ Exemple:

Router(config)# access-list 10 deny 192.168.1.0 0.0.0.255

Bloque tous les paquets venant du réseau 192.168.1.0/24.

Router(config)# access-list 10 permit any

Autorise tout autre trafic (important pour éviter un blocage total)

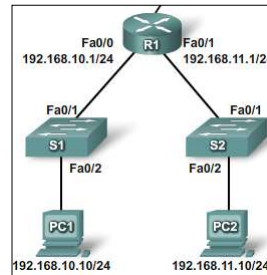
ACL (Listes de Contrôle d'Accès)

Syntaxe de la liste de contrôle d'accès standard

❑ Exemple :

R1(config)# access-list 10 permit 192.168.10.0

Cette liste autorise le trafic provenant du Réseau 192.168.10.0 et refuse tout autre trafic Provenant des autres réseau vue l'application Implicite de la commande **deny any** a la fin de chaque liste (access-list 2 permit 192.168.10.0 0.0.0.255 access-list deny any)



❑ Remarque: pour la suppression d'une ACL standard

Routeur(config)# **no access-list N°liste**

25

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès standard nommée

❑ Pour créer une ACL standard nommée, utilisez la commande :

Router(config)# ip access-list standard NOM_ACL

❑ Exemple d'ACL standard nommé :

Imaginons que nous voulons autoriser le trafic provenant du réseau **192.168.1.0/24** et bloquer tout le reste.

- Router(config)# ip access-list standard **LSI**
- Router(config-std-nacl)# permit 192.168.1.0 0.0.0.255
- Router(config-std-nacl)# deny any
- Router(config-std-nacl)# exit

❑ Puis, on applique l'ACL sur une interface :

- Router(config)# interface GigabitEthernet0/0
- Router(config-if)# ip access-group LSI in
- Router(config-if)# exit

26

ACL (Listes de Contrôle d'Accès)

Masques génériques dans les listes de contrôle d'accès

Masque générique

- ❑ Les listes de contrôle d'accès IPv4 incluent l'utilisation de masques génériques. Un masque générique est une chaîne de 32 chiffres binaires utilisés par le routeur pour déterminer quels bits de l'adresse examiner afin d'établir une correspondance.
- ❑ **Remarque** : à la différence des listes de contrôle d'accès IPv4, les listes de contrôle d'accès IPv6 n'utilisent pas de masques génériques.

Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0 :

Bit 0 de masque générique : permet de vérifier la valeur du bit correspondant dans l'adresse.

Bit 1 de masque générique : permet d'ignorer la valeur du bit correspondant dans l'adresse.

Masque générique									
Position de bit d'octet et valeur d'adresse du bit									
128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	Exemples	
0	0	0	0	0	0	0	0	Correspondance de tous les bits d'adresse (correspondance complète)	
0	0	1	1	1	1	1	1	Les 6 derniers bits d'adresse sont ignorés	
0	0	0	0	1	1	1	1	Les 4 derniers bits d'adresse sont ignorés	
1	1	1	1	1	1	0	0	Les 6 premiers bits d'adresse sont ignorés	
1	1	1	1	1	1	1	1	Tous les bits dans l'octet sont ignorés	

ACL (Listes de Contrôle d'Accès)

Masques génériques dans les listes de contrôle d'accès

Masque générique

- ❑ Utilisation d'un masque générique
- ❑ Le tableau suivant présente les résultats obtenus après l'application d'un masque générique 0.0.255.255 à une adresse IPv4 32 bits.
- ❑ Les masques génériques sont également utilisés lors de la configuration de certains protocoles de routage IPv4 tels que le protocole OSPF, pour les activer sur des interfaces spécifiques.

	Adresse décimale	Adresse binaire
Adresse IP à traiter	192.168.10.0	11000000.10101000.00001010.00000000
Masque générique	0.0.255.255	00000000.00000000.11111111.11111111
Adresse IP résultante	192.168.0.0	11000000.10101000.00000000.00000000

ACL (Listes de Contrôle d'Accès)

Etapes de configuration des listes de contrôle d'accès standard

1. Accéder au mode de configuration

Connectez-vous au routeur via la console ou SSH et entrez en mode de configuration :

```
enable
configure terminal
```

2. Créer une ACL

Utilisez la commande suivante pour créer une liste ACL standard:

```
access-list [numéro] [permit|deny] [adresse_source] [masque_wildcard]
```

Remarque : définir une norme ACL en spécifiant un numéro entre 1 et 99 ou entre 1300 à 1999

Exemples :

```
Autoriser tout le trafic : access-list 10 permit any
Bloquer une adresse IP spécifique (ex. 192.168.1.10) :
access-list 10 deny 192.168.1.10 0.0.0.0
access-list 10 permit any # Autoriser le reste du trafic
```

29

ACL (Listes de Contrôle d'Accès)

Etapes de configuration des listes de contrôle d'accès standard (suite)

3. Appliquer l'ACL à une interface

Une norme ACL est appliquée en entrée ou en sortie sur une interface :

```
interface [nom_interface]
ip access-group [numéro_ACL] [in|out]
```

Exemple pour appliquer l'ACL 10 en entrée sur une interface :

```
interface FastEthernet0/0
ip access-group 10 in
```

4. Vérifier la configuration

Utilisez les commandes suivantes pour afficher les ACL configurées :

```
show access-lists
show running-config | include access-list
show ip interface FastEthernet0/0
```

5. Supprimer une ACL

Pour supprimer une ACL, utilisez :

```
no access-list [numéro]
```

Pour des contrôles plus avancés, utilisez les étendues ACL (numéros 100-199 ou 2000 à 2699).

30

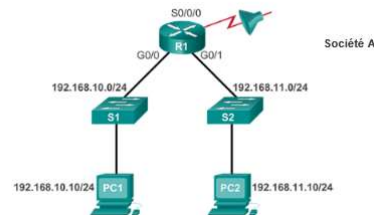
ACL (Listes de Contrôle d'Accès)

Application de listes de contrôle d'accès standard aux interfaces Exemple

La Figure suivante présente un exemple de liste de contrôle d'accès permettant une exception pour un hôte spécifique d'un sous-réseau.

- La première commande supprime la version précédente de l'ACL 1.
- La prochaine instruction de la liste de contrôle d'accès refuse l'hôte PC1 sur le réseau 192.168.10.10. Un hôte sur deux du réseau 192.168.10.0/24 est autorisé. L'instruction de refus implicite fait correspondre un réseau sur deux.
- La liste de contrôle d'accès est réappliquée à l'interface S0/0/0 dans la direction sortante.

Refuser un certain hôte et autoriser un sous-réseau spécifique



```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 1 out
```

31

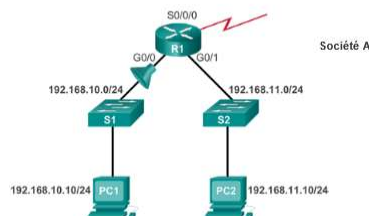
ACL (Listes de Contrôle d'Accès)

Application de listes de contrôle d'accès standard aux interfaces Exemple

La Figure suivante montre un exemple de liste de contrôle d'accès refusant un hôte spécifique. Cette liste de contrôle d'accès remplace l'exemple précédent. Cet exemple bloque toujours le trafic provenant de l'hôte PC1, mais autorise le reste du trafic.

- La première commande supprime la version précédente de l'ACL 1.
- La prochaine instruction de la liste de contrôle d'accès refuse l'hôte PC1 situé sur le réseau 192.168.10.10.
- La troisième ligne est nouvelle et autorise tous les autres hôtes. Cela signifie que tous les hôtes du réseau 192.168.10.0/24 seront autorisés sauf PC1 qui a été refusé dans l'instruction précédente.
- Cette liste de contrôle d'accès est appliquée à l'interface G0/0 dans la direction entrante.

Refuser un certain hôte



```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

Étant donné que le filtre affecte uniquement le réseau local 192.168.10.0/24 sur l'interface G0/0, il est plus judicieux d'appliquer la liste de contrôle d'accès à l'interface d'entrée.

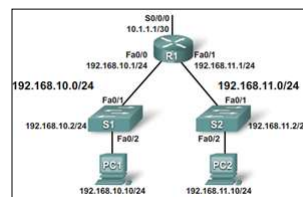
32

ACL (Listes de Contrôle d'Accès)

Application de listes de contrôle d'accès standard aux interfaces

- ❑ la commande **ip access-group**
 - Routeur(config-if)#ip access-group {numéro-liste-accès | nom-liste-accès} {in | out}
- ❑ **Supprimer une liste de contrôle d'accès d'une interface;**
 - Routeur(config-if)# no ip access-group
 - Routeur(config-if)# no access-list pour la supprimer dans son intégralité.
- ❑ **Exemple:**

```
R1(config)#no access-list 1
R1(config)#access-list 1 deny 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface S0/0/0
R1(config-if)#ip access-group 1 out
```

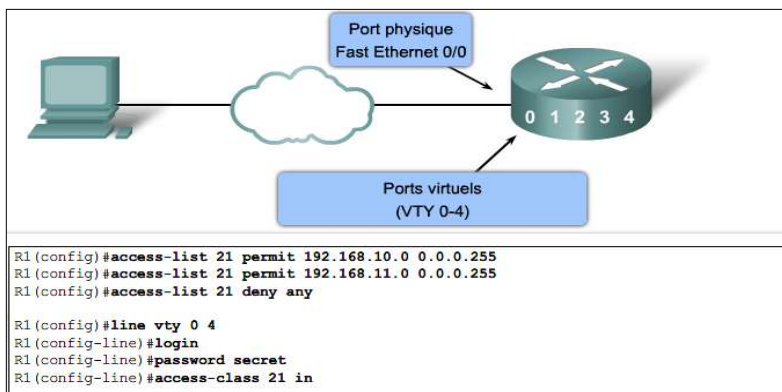


33

ACL (Listes de Contrôle d'Accès)

Utilisation d'une liste de contrôle d'accès pour contrôler l'accès VTY

- ❑ La commande **access-class**
 - Seules des listes de contrôle d'accès numérotées peuvent être appliquées aux lignes VTY.
 - Vous devez définir les mêmes restrictions sur toutes les lignes VTY car un utilisateur peut tenter de se connecter à n'importe laquelle.



34

ACL (Listes de Contrôle d'Accès)

Contrôle et vérification des ACL

- ❑ Afficher les ACL par nom ou par numéro;

```
R1# show access-lists { numéro-liste-accès|nom }
```

- ❑ Afficher toutes les listes d'accès;

```
R1# show access-lists
Standard IP access list SALES
 10 deny  10.1.1.0 0.0.0.255
 20 permit 10.3.3.1
 30 permit 10.4.4.1
 40 permit 10.5.5.1
Extended IP access list ENG
 10 permit tcp host 192.168.10.2 any eq telnet (25 matches)
 20 permit tcp host 192.168.10.2 any eq ftp
 30 permit tcp host 192.168.10.2 any eq ftp-data
```

35

ACL (Listes de Contrôle d'Accès)

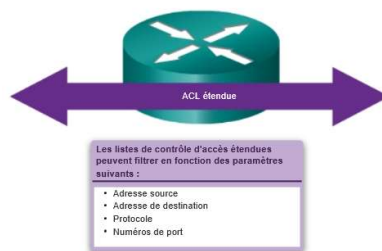
Ajout d'une ligne à une ACL nommée

```
R1# show access-lists
Standard IP access list WEBSEVER
 10 permit 192.168.10.11
 20 deny  192.168.10.0, wildcard bits 0.0.0.255
 30 deny  192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list standard WEBSEVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov  1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console
R1# sho access-lists
Standard IP access list WEBSEVER
 10 permit 192.168.10.11
 15 permit 192.168.11.10
 20 deny  192.168.10.0, wildcard bits 0.0.0.255
 30 deny  192.168.11.0, wildcard bits 0.0.0.255
R1#
```

36

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendue



ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

Listes de contrôle d'accès étendues

- ❑ Une liste de contrôle d'accès étendue est une collection d'instructions ayant comme objectif de permettre ou d'interdire la commutation des paquets en fonction d'un certain nombre de conditions ou de critères, tels que :
 - Type de protocole
 - Adresse IPv4 source
 - Adresse IPv4 de destination
 - Ports TCP ou UDP source
 - Ports TCP ou UDP de destination
 - Informations facultatives sur le type de protocole pour un contrôle plus précis
- ❑ Numérotées entre 100 et 199, 2000 et 2699;
- ❑ Les listes de contrôle d'accès étendues peuvent être nommées;
- ❑ Les paquets peuvent être filtré par les adresses sources /destination, les ports source /destination et les protocoles;

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

Syntaxe de l'ACL étendue

- ❑ Les ACL étendues utilisent une syntaxe plus détaillée qui permet de spécifier ces critères supplémentaires. Voici la syntaxe générale pour configurer une ACL étendue :

access-list extended n° de l'ACL (nom_de_l_acl) {permit|deny} <protocole> <adresse_source> < masque_source (masque générique)> <adresse_dest> < masque_dest (masque générique)> [opérateur <port_source|port_dest>] (opérande ou argument)

- **access-list extended <nom_de_l_acl>** : crée une ACL étendue avec un nom spécifique.
- **permit|deny** : Indique si le trafic doit être autorisé (permit) ou refusé (deny).
- **<protocole>** : Le protocole à filtrer (ex : ip, tcp, udp, icmp).
- **<adresse_source>** : L'adresse IP source du trafic. Cela peut être une adresse IP spécifique ou un sous-réseau.
- **<masque_source>** : Le masque générique de sous-réseau associé à l'adresse source pour définir la portée de l'adresse.
- **<adresse_dest>** : L'adresse IP de destination du trafic.
- **<masque_dest>** : Le masque générique de sous-réseau associé à l'adresse de destination.
- **[opérateur <port_source|port_dest>]** (facultatif) : Permet de spécifier un numéro de port spécifique pour filtrer le trafic à ce niveau. Il est utilisé pour les protocoles comme TCP ou UDP pour filtrer le trafic à un niveau plus fin. La liste des opérateurs est : Lt plus petit que, Gt plus grand que, Eq égal à, Neq différent de.

39

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

Syntaxe de l'ACL étendue (suite)

- ❑ La possibilité de filtrer en fonction des protocoles et des numéros de port permet aux administrateurs réseau de créer des listes de contrôle d'accès étendues très précises. Une application peut être spécifiée soit par le numéro de port soit par le nom d'un port réservé.
- ❑ L'administrateur réseau peut spécifier un numéro de port TCP ou UDP en le plaçant à la fin de l'instruction de la liste de contrôle d'accès étendue. Vous pouvez utiliser des opérateurs logiques, tels que égal (eq), non égal (neq), supérieur à (gt) et inférieur à (lt).
- ❑ R1(config)# access-list 101 permit tcp any any eq ?

Avec les numéros de port

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Avec des mots-clés

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

ACL (Listes de Contrôle d'Accès)

Configuration des listes de contrôle d'accès standard

Etapes de configuration des listes de contrôle d'accès standard

1. Accéder au mode de configuration

Connectez-vous au routeur via la console ou SSH et entrez en mode de configuration :

```
enable
configure terminal
```

2. Créer l'ACL Etendue

- Définir l'ACL avec un numéro (100-199 pour les ACLs IP étendues)
- Exemple pour bloquer HTTP de 192.168.1.0 vers 192.168.2.0 :
 - Router(config)# access-list 100 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80
- Ajouter une règle pour autoriser le reste du trafic :
 - Router(config)# access-list 100 permit ip any any

41

ACL (Listes de Contrôle d'Accès)

Configuration des listes de contrôle d'accès standard

Etapes de configuration des listes de contrôle d'accès standard

3. Appliquer l'ACL

- Aller sur l'interface concernée :
 - Router(config)# interface GigabitEthernet0/1
- Appliquer l'ACL en entrée ou en sortie :
 - Router(config-if)# ip access-group 100 in

4. Vérifier et sauvegarder

- Vérifier les ACLs configurées :
 - Router# show access-lists
- Vérifier les ACLs appliquées aux interfaces :
 - Router# show ip interface GigabitEthernet0/1
- Sauvegarder la configuration :
 - Router# write memory

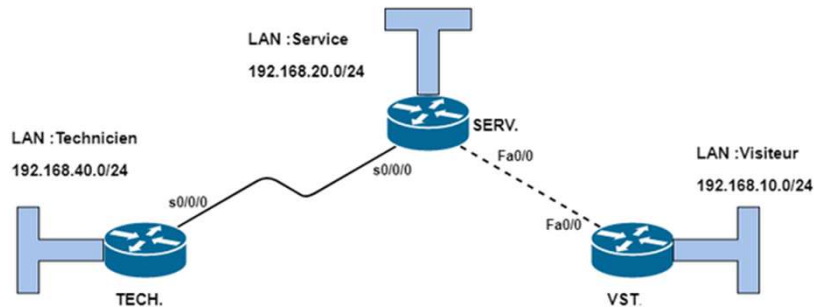
42

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

Exemple 1

- ❑ Soit la topologie ci-dessous :
- ❑ Objectif : Interdire l'accès web d'un terminal du LAN Visiteur au serveur http branché au LAN Service



source: <https://www.connecthostproject.com/acl.html>

43

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

Exemple 1 (suite)

On suppose l'adresse IP du serveur HTTP est 192.168.20.11 et celle du hôte qu'on veut lui interdire l'accès web est 192.168.10.10. La configuration de cette ACL est au routeur VST telle que :

```
VST(config)#access-list 110 deny tcp host 192.168.10.10 host 192.168.20.11 eq www
VST(config)#access-list 110 permit tcp any any
VST(config)#access-list 110 permit ip any any
```

La liste est appliquée à l'interface Fa0/1 de VST, c'est l'accès le plus près de la source des paquets HTTP. La syntaxe est :

```
SERV(config)#interface fa0/1
SERV(config-if)#ip access-group 110 in
```

44

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

Exemple 1 (suite)

On interdit les paquets entrants à cette interface en provenance du hôte 192.168.10.10 en allant vers le serveur HTTP ayant l'adresse 192.168.20.11. Les deux dernières lignes de VST(config)# permettent aux autres hôtes des 3 réseaux d'avoir l'accès HTTP et à tous les hôtes des réseaux de pouvoir communiquer en utilisant les protocoles TCP / IP. On peut appliquer la même liste mais à une interface différente, la fa0/0 de SERV.

On peut vérifier le fonctionnement des ACL en utilisant les commandes suivantes :

VST#show access-list 110

Extended IP access list 110

deny tcp host 192.168.10.10 host 192.168.20.11 eq www

permit tcp any any

permit ip any any

45

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

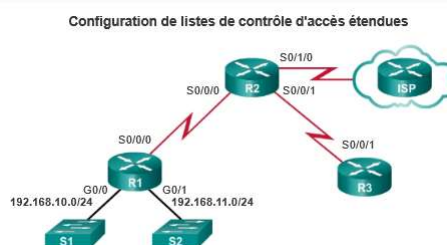
Exemple 2

La Figure suivante présente un exemple de liste de contrôle d'accès étendue. Dans cet exemple, l'administrateur réseau a configuré des listes de contrôle d'accès pour limiter l'accès au réseau.

- ❑ La navigation sur Internet est autorisée uniquement à partir du réseau local relié à l'interface G0/0. La liste de contrôle d'accès 103 autorise le trafic en provenance de toute adresse sur le réseau 192.168.10.0 à accéder à n'importe quelle destination, à condition que le trafic soit transféré via les ports 80 (HTTP) et 443 (HTTPS) uniquement.

```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255
established
```

- La liste de contrôle d'accès 103 autorise les requêtes vers les ports 80 et 443.
- La liste de contrôle d'accès 104 autorise les réponses HTTP et HTTPS établies.



46

ACL (Listes de Contrôle d'Accès)

Listes de contrôle d'accès étendues

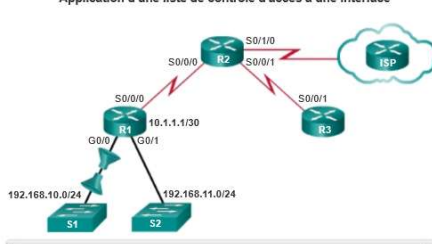
Exemple 2 : Application de listes de contrôle d'accès étendues aux interfaces

- Dans l'exemple précédent, l'administrateur réseau a configuré une liste de contrôle d'accès pour permettre aux utilisateurs du réseau 192.168.10.0/24 de naviguer sur les sites Web sécurisés et non sécurisés. Même si elle a été configurée, la liste de contrôle d'accès ne filtre pas le trafic tant qu'elle n'est pas appliquée à une interface. Pour appliquer une liste de contrôle d'accès à une interface, déterminez d'abord si le filtrage concerne le trafic **entrant** ou **sortant**. Lorsqu'un utilisateur du réseau local interne accède à un site Web sur Internet, le trafic est dans la direction **sortante** vers Internet. Lorsqu'un utilisateur interne reçoit un e-mail à partir d'Internet, le trafic entre dans le routeur local. Cependant, lorsque vous appliquez une liste de contrôle d'accès à une interface, les termes entrant et sortant prennent un sens différent. Dans le contexte d'une liste de contrôle d'accès, le référentiel est l'interface du routeur.

- Dans la topologie de la figure, R1 a trois interfaces : une interface série, S0/0/0, et deux interfaces Gigabit Ethernet, G0/0 et G0/1. Souvenez-vous que les listes de contrôle d'accès étendues doivent généralement être appliquées près de la source. Dans cette topologie, l'interface la plus proche de la source du trafic cible est l'interface G0/0.

```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

Application d'une liste de contrôle d'accès à une interface



47

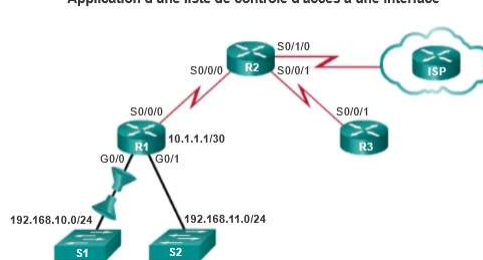
ACL (Listes de Contrôle d'Accès)

Configuration des listes de contrôle d'accès étendues

Exemple 2 : Application de listes de contrôle d'accès étendues aux interfaces

- Le trafic des requêtes Web émises par les utilisateurs du réseau local 192.168.10.0/24 entre dans l'interface G0/0. Le trafic de retour provenant des connexions établies avec les utilisateurs du réseau local sort de l'interface G0/0. Cet exemple applique la liste de contrôle d'accès à l'interface G0/0 dans les deux sens. La liste de contrôle d'accès entrante, 103, examine le type de trafic. La liste de contrôle d'accès sortante, 104, recherche le trafic de retour des connexions établies. L'accès internet de 192.168.10.0 sera donc limité à la navigation sur le Web.

Application d'une liste de contrôle d'accès à une interface



```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

48

ACL (Listes de Contrôle d'Accès)

Configuration des listes de contrôle d'accès étendues

Exemple 2 : Filtrage du trafic à l'aide de listes de contrôle d'accès étendues

L'exemple de la topologie suivante refuse le trafic FTP provenant du sous-réseau 192.168.11.0, mais autorise tout autre trafic.

Notez l'utilisation des masques génériques et de l'instruction de refus global explicite. Souvenez-vous que le protocole FTP utilise les ports TCP 20 et 21. Par conséquent, la liste de contrôle d'accès doit comporter les mots-clés `ftp` et `ftp-data`, ou `eq 20` et `eq 21` pour refuser le trafic FTP.

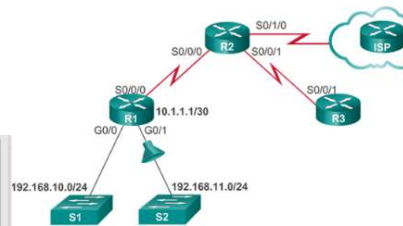
Si vous utilisez les numéros de port au lieu des noms de port, les commandes sont les suivantes :

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
```

Pour empêcher l'instruction de refus global implicite présente à la fin de la liste de contrôle d'accès de bloquer tout le trafic, l'instruction **permit ip any any** est ajoutée.

```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp-data
R1(config)# access-list 101 permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 101 in
```

Liste de contrôle d'accès étendue pour refuser le trafic FTP



49

ACL (Listes de Contrôle d'Accès)

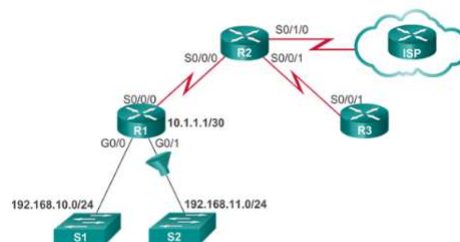
Configuration des listes de contrôle d'accès étendues

Exemple 2 : Filtrage du trafic à l'aide de listes de contrôle d'accès étendues

L'exemple de topologie suivante refuse le trafic Telnet provenant de n'importe quelle source vers le réseau local 192.168.11.0/24, mais autorise tout autre trafic IP. Étant donné que le trafic destiné au réseau local 192.168.11.0/24 est sortant sur l'interface G0/1, la liste de contrôle d'accès serait appliquée à l'interface G0/1 à l'aide du mot-clé **out**. Notez l'utilisation du mot-clé **any** dans l'instruction d'autorisation. Cette instruction est ajoutée pour garantir qu'aucun autre trafic n'est bloqué.

Remarque : les ACL traités utilisent tous l'instruction **permit ip any any** à la fin de la liste. Pour plus de sécurité, on peut utiliser la commande **permit 192.168.11.0 0.0.0.255 any**.

Liste de contrôle d'accès étendue pour refuser le trafic Telnet



```
R1(config)# access-list 102 deny tcp any 192.168.11.0 0.0.0.255
eq 23
R1(config)# access-list 102 permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 102 out
```

50

ACL (Listes de Contrôle d'Accès)

Création de listes de contrôle d'accès étendues nommées

- ❑ La création des listes de contrôle d'accès étendues nommées est similaire à la création des listes de contrôle d'accès standard nommées. Procédez comme suit pour créer une liste de contrôle d'accès étendue identifiée par un nom :
 1. **Étape 1.** En mode de configuration globale, utilisez la commande **ip access-list extended name** pour définir le nom de la liste de contrôle d'accès étendue.
 2. **Étape 2.** En mode de configuration de la liste de contrôle d'accès nommée, spécifiez les conditions **permit** ou **deny**.
 3. **Étape 3.** Repassez en mode d'exécution privilégié et vérifiez la liste à l'aide de la commande **show access-lists name**.
 4. **Étape 4.** Enregistrez les entrées dans le fichier de configuration en utilisant la commande **copy running-config startup-config**.
- ❑ Pour supprimer une liste de contrôle d'accès étendue nommée, utilisez la commande de configuration globale **no ip access-list extended name**.

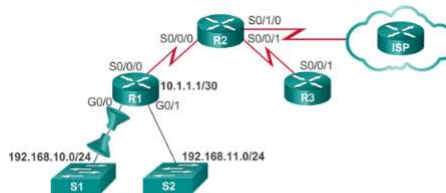
51

ACL (Listes de Contrôle d'Accès)

Création de listes de contrôle d'accès étendues nommées

Exemple

- ❑ La figure suivante montre les versions nommées des listes de contrôle d'accès créées dans les exemples précédents. La liste de contrôle d'accès nommée SURFING permet aux utilisateurs du réseau local 192.168.10.0/24 d'accéder aux sites Web. La liste de contrôle d'accès nommée BROWSING autorise le trafic de retour provenant des connexions établies. Les règles sont appliquées au trafic entrant et sortant de l'interface G0/0 à l'aide des noms des listes de contrôle d'accès.



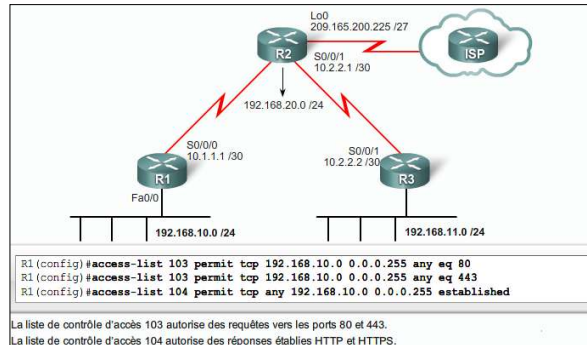
```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended BROWSING
R1(config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255
established
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group SURFING in
R1(config-if)#ip access-group BROWSING out
```

52

ACL (Listes de Contrôle d'Accès)

Configuration des listes de contrôle d'accès étendues

Autre Exemple de configuration



Application des LCA sur l'interface so/o/o de R1;

```

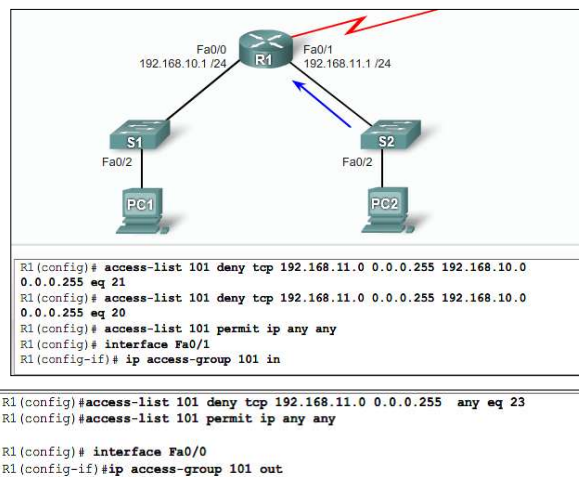
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 103 out
R1(config-if)# ip access-group 104 in
    
```

53

ACL (Listes de Contrôle d'Accès)

Configuration des listes de contrôle d'accès étendues

Autre Exemple de configuration : bloquer le trafic FTP et Telnet et autoriser tout autre trafic



54

ACL (Listes de Contrôle d'Accès)

Numérotation et attribution d'un nom aux listes de contrôle d'accès

ACL standard et étendues vs ACL nommée

- ❑ Les listes de contrôle d'accès standard et étendues et leur liste d'instructions peuvent être identifiées par un **numéro** ou par un **nom**.
- ❑ Les listes de contrôle d'accès numérotées sont pratiques pour déterminer le type de liste sur des réseaux de petite taille dont la définition du trafic est plus homogène. Toutefois, le numéro n'indique pas la fonction d'une liste de contrôle d'accès.
- ❑ Ci-après les règles à suivre pour attribuer des numéros ou des noms aux listes de contrôle d'accès.

Liste de contrôle d'accès numérotée :

Attribution d'un numéro en fonction du protocole à filtrer.

- Plages 1 à 99 et 1 300 à 1 999 : listes de contrôle d'accès IP standard
- Plages 100 à 199 et 2 000 à 2 699 : listes de contrôle d'accès IP étendue

Liste de contrôle d'accès nommée :

Attribution d'un nom à la liste de contrôle d'accès.

- Les noms doivent se composer de caractères alphanumériques.
- Il est conseillé d'écrire le nom en MAJUSCULES.
- Les noms ne doivent pas contenir d'espaces ni de signes de ponctuation.
- Il est possible d'ajouter et de supprimer des entrées de la liste de contrôle d'accès.

- ❑ Concernant les listes de contrôle d'accès numérotées, les numéros 200 à 1 299 ne sont disponibles, car ils sont utilisés par d'autres protocoles dont la plupart sont anciens ou obsolètes.

55





ACL (Listes de Contrôle d'Accès)



paloalto
NETWORKS





FORTINET
FortiGate 60E

ACL (Listes de Contrôle d'Accès)

Routeur Vs Pare-feu

1. Routeur

- ❑ **Rôle principal** : Il achemine les paquets de données entre différents réseaux (ex : entre un réseau local et Internet).
- ❑ **Fonctionnement** : Il analyse les adresses IP pour déterminer le meilleur chemin pour envoyer les données.
- ❑ **Sécurité** : Certains routeurs ont des fonctions de sécurité de base (ex : NAT, filtrage MAC), mais ce n'est pas leur fonction principale.

2. Pare-feu (Firewall)

- ❑ **Rôle principal** : Il protège un réseau en filtrant le trafic entrant et sortant selon des règles définies.
- ❑ **Fonctionnement** : Il bloque ou autorise les connexions en fonction de critères comme l'adresse IP, le port, ou le protocole.
- ❑ **Types** :
 - Pare-feu matériel (boîtier dédié)
 - Pare-feu logiciel (installé sur un PC ou serveur)
- ❑ **Sécurité** : Il empêche les attaques (ex : tentatives d'intrusion, malware).

57

ACL (Listes de Contrôle d'Accès)

Routeur Vs Pare-feu

Différence clé



- ❑ Le **routeur** dirige le trafic, tandis que le pare-feu contrôle et sécurise le trafic.
- ❑ Un **routeur** seul ne protège pas totalement contre les cyberattaques, alors qu'un **pare-feu** est conçu pour la sécurité.
- ❑ Dans les grandes infrastructures, un **pare-feu** est souvent placé derrière un routeur pour filtrer le trafic entrant.



Routeur
Pare-feu



Pare-feu
(Firewall)



58

ACL (Listes de Contrôle d'Accès)

Routeur Vs Pare-feu

Routeurs avec fonctionnalités de pare-feu

- ❑ Certains routeurs, surtout les modèles professionnels (Cisco, Fortinet, etc.), intègrent des fonctionnalités de pare-feu comme :
 - Filtrage des paquets (bloquer certains types de trafic)
 - NAT (Network Address Translation) pour masquer les IP internes
 - Filtrage d'adresses MAC/IP
 - Pare-feu SPI (Stateful Packet Inspection) qui analyse les connexions actives
 - Blocage des ports non sécurisés

Limites d'un routeur en tant que pare-feu

- ❑ Bien que certains routeurs aient des fonctions de sécurité, ils ne sont pas aussi **avancés** qu'un vrai pare-feu dédié :
 - Moins de contrôle sur le trafic (pas d'analyse approfondie des paquets)
 - Pas de détection des menaces avancées (DDoS, malwares)
 - Pas de gestion des VPN ou des règles complexes

59

ACL (Listes de Contrôle d'Accès)

Routeur Vs Pare-feu

Les pare-feu intégrés dans les routeurs avancés

- ❑ Certains équipements "tout-en-un", appelés UTM (Unified Threat Management) ou Next-Generation Firewalls (NGFW), combinent **routeur** + **pare-feu** + **antivirus** + **VPN** en un seul appareil.
- ❑ Exemples :
 - FortiGate (Fortinet)
 - Cisco ASA
 - pfSense (solution logicielle pare-feu/routeur)

Un **routeur** peut avoir des fonctions de pare-feu, mais pour une sécurité avancée, un **pare-feu dédié** est souvent nécessaire, surtout en entreprise.

60

Plan

- Serveur FTP, Telnet et SSH
- Serveur HTTP Apache
- VPN & OpenVPN
- Configuration VLAN, VTP et STP
- ACL (Listes de Contrôle d'Accès)

▪ **Le protocole de supervision SNMP**

- **Serveur NFS et Serveur de fichiers Samba**
- **Serveur DNS (BIND9)**
- **Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)**
- **Serveur d'impression**

61

Le protocole de supervision SNMP

62

Plan

- ❖ La supervision d'un réseau.
- ❖ Le Protocole SNMP
- ❖ Les composants du Protocole SNMP
- ❖ Principe de fonctionnement du protocole SNMP
- ❖ Les versions du protocoles SNMP.
- ❖ Les Avantages et les inconvénients de SNMPv1
- ❖ Protocole SNMPv2
- ❖ Protocole SNMPv3

La supervision

Définition :

- La supervision est la "surveillance du bon fonctionnement d'un système ou d'une activité".
Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques.
- La supervision réseau porte sur la surveillance de manière continue de la disponibilité des services en ligne - du fonctionnement, des débits, de la sécurité mais également du contrôle des flux.

Pour superviser un réseau il faut utiliser un protocole de supervision .

Qu'est ce que le protocole SNMP ?

- ❑ Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau (routeurs, ponts, etc...) , de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
- ❑ Il permet de contrôler un réseau à distance en interrogeant les stations qui en font partie sur leur état et modifier leur configuration, faire des tests de sécurité et observer différentes informations liées à l'émission de données. Il peut même être utilisé pour gérer des logiciels et bases de données à distance. Depuis qu'il est devenu un standard TCP/IP, son utilisation a beaucoup augmenté.

Les Composants du protocole SNMP

- 1. **Une station de gestion NMS** : C'est la station qui exécute un programme de gestion SNMP. Son but principal est de contrôler les stations du réseau et de les interroger sur différentes informations. Sa configuration matérielle doit posséder un processeur relativement rapide, beaucoup de mémoire et un espace disque suffisant (pour archiver les informations).
- 2. **Des éléments de réseaux avec des agents** : Ils sont les éléments à gérer sur le réseau (ex : logiciels, stations de travail, routeurs, concentrateurs, ponts, etc.). L'agent est un module résidant dans chaque nœud du réseau qui a pour fonction d'aller chercher les informations du système afin de tenir sa table MIB à jour.

Parfois , On trouve des vieux équipements administrables ne sont pas conformes à SNMP. Dans ce cas, il est possible d'utiliser un agent proxy sur un équipement SNMP, qui va servir d'intermédiaire avec celui non SNMP.

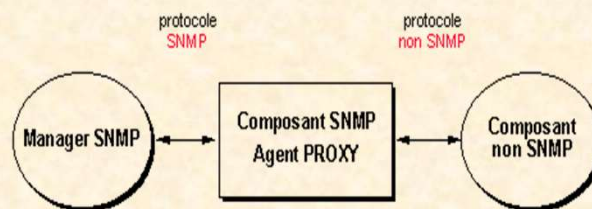


figure : un agent proxy pour communiquer avec les vieux équipements administrables ne sont pas conformes

Les Composants du protocole SNMP

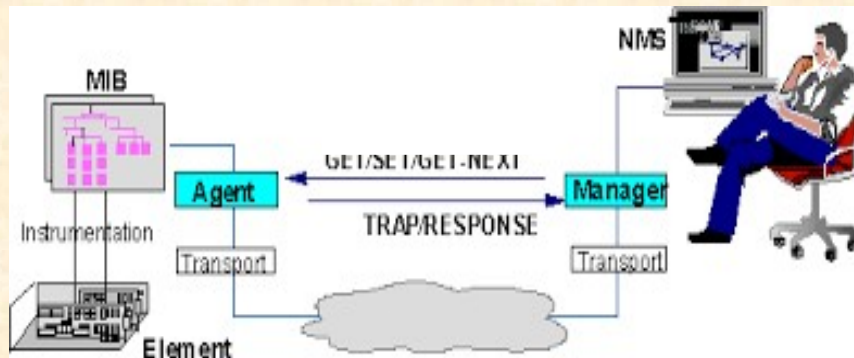
➤ 3. Les tables MIB (Management Information Base)

Les tables MIB : Elles représentent une base de données maintenue par l'agent qui contient les informations sur les transmissions de données et sur les composantes de la station ou du routeur, etc. (ex : *uptime*, configuration du routage, état du disque et du port série, nombre de paquets reçus et envoyés, combien de paquets erronés reçus, etc.).

➔ **uptime** est un terme **informatique** désignant le temps depuis lequel une **machine** , ou un logiciel informatique, tourne sans interruption

Principe de fonctionnement du protocole SNMP

- Les systèmes de gestion de réseau sont basés sur des éléments principaux : un superviseur (manager), des nœuds (nodes) et des agents.
- Le **superviseur** est la console qui permet à l'administrateur réseau d'exécuter des requêtes de gestion (management).
- Les **agents** c'est-à-dire les applications de gestion de réseau résidant dans un périphérique, sont chargés de transmettre les données locales de gestion du périphérique au format SNMP



La supervision par l'administrateur

Principe de fonctionnement du protocole SNMP

- Pour le protocole SNMP On trouve Deux situations sont possibles pour les échanges de données. Soit l'administrateur réseau demande une information à un agent et obtient une réponse, soit l'agent envoie de lui-même une alarme (**trap**) à l'administrateur lorsqu'un événement particulier arrive sur le réseau.

Principe de fonctionnement du protocole SNMP

- Le protocole SNMP définit un concept des alertes TRAPS . Une fois défini, si un certain événement se produit, comme par exemple le dépassement d'un seuil, l'agent envoie un paquet UDP à un serveur. Ce processus d'alerte est utilisé dans les cas où il est possible de définir simplement un seuil d'alerte. Les traps SNMP sont envoyés en UDP sur le port 162.

• Les alertes (traps)

Type de PDU (Protocol Data Units)	Nom
0	GetRequest
1	GetNextRequest
2	SetRequest
3	GetResponse
4	Trap

Principe de fonctionnement du protocole SNMP

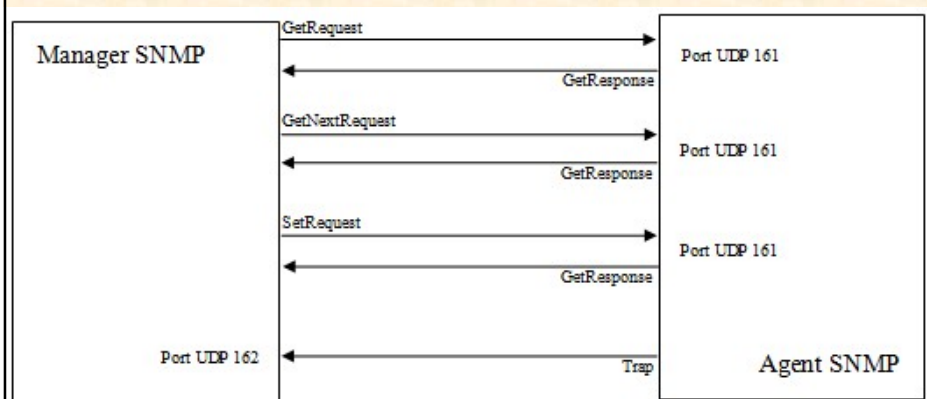
Il existe quatre types de requêtes :

- **GetRequest** : permet d'obtenir une variable.
- **GetNextRequest** : permet d'obtenir la variable suivante (si existante, sinon retour d'erreur).
- **GetBulk** : " permet la recherche d'un ensemble de variables regroupées. "
- **SetRequest** : permet de modifier la valeur d'une variable.

Puis, les réponses :

- **GetResponse** : permet à l'agent de retourner la réponse au NMS.
- **NoSuchObject** : informe le NMS que la variable n'est pas disponible.

Principe de fonctionnement du protocole SNMP



Les types de requêtes

LES DIFFÉRENTES VERSIONS DE SNMP

- SNMPv1 (ancien standard) : Première version apparue en 1989.
- SNMPv2p (historique) : Ajout de nouveau type de données.
- SNMPv2c (expérimental) : Amélioration des opérations du protocole
- SNMPv2u (expérimental) : Implémente la version 2c en ajoutant la sécurité utilisateurs.
- SNMPv2* (expérimental) : Combinaison des meilleures parties de v2u et v2p.
- SNMPv3 (nouveau standard) : La sécurité avant tout.

Les Avantages et les inconvénients de SNMPv1

Avantages :

- conception simple.
- Implémentation facile sur un réseau
- très répandu aujourd'hui.
- il ne nécessite pas une longue configuration
- simple à mettre à jour.
- nécessite moins de ressources et de connexions simultanées .

Inconvénients :

- la charge sur le réseau.
- n'est pas très pratique pour ramener une grosse quantité de données.
- L'authentification non sécurisée.
- SNMP ne permet pas de "commander" un agent, cette manipulation ne peut se faire qu'en modifiant une entrée de sa MIB.
- SNMP ne supporte pas la communication de station d'administration à station d'administration.

SNMPv2

- Devant le succès de SNMP, il a vite semblé nécessaire de développer un successeur qui corrigerait ses nombreuses faiblesses, notamment en terme de sécurité.
- Une version améliorée a été proposée sous le nom SNMPv2. Elle apporte des mécanismes d'authentification et de chiffrement ainsi que des méthodes de consultation des informations réseaux plus efficaces.
- Plus complexe que SNMP (v1), qui est par ailleurs bien implanté, SNMPv2 ne connaît pas de réel succès à ce jour.

SNMPv3

- Il est vrai que SNMPv3 introduit des notions de sécurité comme :
- Authentification / intégrité
- Confidentialité des données
- Contrôle d'accès par la MIB
- ...

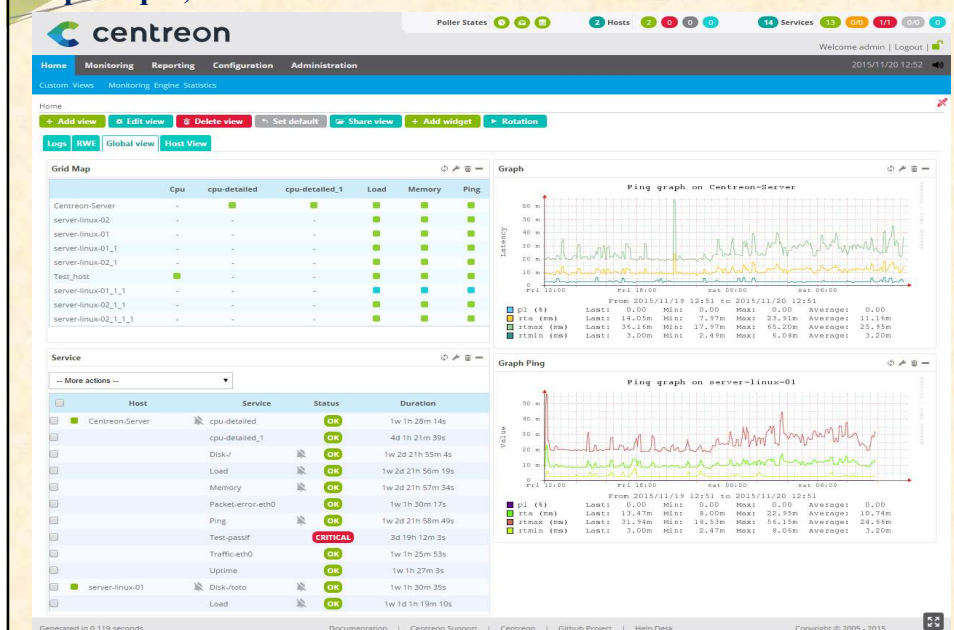
SNMP : Synthèse

En pratique; concrètement, dans le cadre d'un réseau, SNMP est utilisé :

- pour administrer les équipements ;
 - pour surveiller le comportement des équipements.
- Une requête SNMP est un datagramme **UDP** habituellement envoyé par le manager à destination du port 161 de l'agent. Les schémas de sécurité dépendent des versions de SNMP (v1, v2 ou v3). Les versions 1 et 2 du protocole SNMP comportent de nombreuses lacunes de sécurité. C'est pourquoi les bonnes pratiques recommandent de n'utiliser que la version 3. Cette dernière se base sur le chiffrement **DES** avec deux mots de passe ou clés sur 64 bits partagés entre l'agent et le manager :
- un pour l'authentification
 - un pour le chiffrement
- Un grand nombre de logiciels libres et propriétaires utilisent SNMP pour interroger régulièrement les équipements et produire des graphes rendant compte de l'évolution des réseaux ou des systèmes informatiques (Centreon, NetCrunch, MRTG, Cacti, Shinken, Nagios, RG System, Zabbix, PRTG).
- Le protocole SNMP définit aussi un concept d'interruptions (*traps* en anglais). Une fois défini, si un certain événement se produit, comme le dépassement d'un seuil, l'agent envoie un paquet **UDP** sur le port 162 du serveur de supervision.

SNMP : Synthèse

En pratique; Centreon





Plan

- Serveur FTP, Telnet et SSH
- Serveur HTTP Apache
- VPN & OpenVPN
- Configuration VLAN, VTP et STP
- ACL (Listes de Contrôle d'Accès)
- Le protocole de supervision SNMP

▪ Serveur NFS et Serveur de fichiers Samba

- Serveur DNS (BIND9)
- Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)
- Serveur d'impression

Network File System

- ❑ **Network File System** (ou **NFS**), en français *système de fichiers en réseau*, est à l'origine un protocole développé par Sun Microsystems en 1984 qui permet à un ordinateur d'accéder via un réseau à des fichiers distants. Il fait partie de la couche application du modèle OSI et utilise le protocole **RPC**.
- ❑ **Développé par** : Sun Microsystems (maintenant Oracle)
- ❑ **Principalement utilisé sur** : systèmes **Linux/Unix**
- ❑ **Fonction** : permet à des machines distantes de monter un système de fichiers comme s'il était local.
- ❑ **Protocoles** : utilise RPC (Remote Procedure Call)
- ❑ **Avantage** : rapide, bien intégré dans les environnements Linux/Unix
- ❑ **Inconvénient** : support limité sur Windows (pas natif, nécessite des outils supplémentaires). Des versions existent pour Macintosh ou Microsoft Windows.
- ❑ NFS est compatible avec IPv6.

Remarque:

NFS est un protocole historique de partage de fichiers entre machines UNIX (famille de systèmes d'exploitation dont Linux et macOS X font partie). Si vous souhaitez partager des fichiers avec des clients Windows, le partage par **Samba** est le plus adapté.

83

Network File System

NFS versions 1, 2 et 3

Les versions 1 et 2 sont non sécurisées, prévues pour fonctionner sur UDP.

La version 3 est étendue pour prendre en charge TCP.

Dans ces versions, la gestion de la sécurité reste élémentaire et souffre d'importantes lacunes. Le système est sans état (*stateless*) et ne permet pas la reprise sur incident.

84

Network File System : NFS Version 4

- ❑ **NFS 4** apporte beaucoup d'améliorations par rapport aux versions précédentes. Une des plus notables est l'utilisation d'un port TCP unique et configurable là où les versions précédentes utilisaient plusieurs ports TCP, parfois alloués dynamiquement, ce qui rendait difficile l'utilisation de NFS avec un pare-feu.
- ❑ Le serveur virtuel que vous avez monté n'a pas de pare-feu mais si c'était le cas, le port par défaut alloué à NFSv4 et qu'il faudrait ouvrir serait le **port TCP 2049 entrant**.
- ❑ Inspirée d'Andrew File System (AFS), la version 4 du protocole marque une rupture totale avec les versions précédentes. L'ensemble du protocole est repensé, et le code totalement réécrit. Il s'agit d'un système de fichiers objet.

85

Network File System : NFS Version 4

- ❑ **NFS 4** : Une gestion totale de la sécurité :
 - Négociation du niveau de sécurité entre le client et le serveur
 - Sécurisation simple, support de Kerberos5, certificats SPKM et LIPKEY4
 - Chiffrement des communications possible (kerberos 5p par exemple)
 - Compatibilité : NFSv4 peut être utilisé sous Unix et sous MS-Windows. Il est disponible sur Mac depuis Mac OS.
 - NFSv4 suppose l'utilisation d'UTF-8, pour les noms de fichiers, sans que ce soit obligatoire.
 - NFSv4.1 : La version 4.1 de NFS a été publiée dans le RFC 5661 en janvier 2010
 - NFSv4.2
 - La version 4.2 de NFS a été publiée dans le RFC 7862 en novembre 2016

86

Network File System : NFS Version 4

NFS est prévu pour fonctionner sur un réseau local. Vous ne devriez pas l'utiliser pour partager des fichiers sur internet sauf si vous passez par un VPN. Même dans ce cas, il y a souvent des solutions plus adaptées.

87

Principe de Fonctionnement du NFS

- ❑ Dans une communication entre un client compatible NFS et un serveur NFS. Tout d'abord, un client demande un fichier ou un répertoire au serveur à l'aide d'appels de procédure à distance (RPC). Le serveur vérifie ensuite si :
 - le fichier ou le répertoire est disponible ;
 - le client dispose des autorisations d'accès requises.
- ❑ Le serveur monte ensuite le fichier ou le répertoire à distance sur le client et partage l'accès via une connexion virtuelle. Pour le client, NFS permet d'utiliser le fichier du serveur distant de la même manière que l'accès à un fichier local pendant les opérations.
- ❑ NFS permet également aux clients de mettre en cache les fichiers pour améliorer la vitesse d'accès, de verrouiller les fichiers lorsque plusieurs ordinateurs tentent d'écrire simultanément sur le même fichier et de fournir des mises à jour synchronisées des attributs de fichiers.
- ❑ NFS reste populaire auprès des utilisateurs de Linux.

88

Serveur de fichiers Samba

- ❑ **Samba** est une suite de programmes libre qui tourne sous Linux et qui permet de créer un serveur de fichiers en s'appuyant sur l'implémentation du protocole **SMB**. Samba permet de partager des imprimantes et de créer un véritable contrôleur de domaine Active Directory, à partir de la version 4 (prise en charge DNS, etc.).
- ❑ Le logiciel **Samba** est un outil permettant de partager des dossiers et des imprimantes à travers un réseau local. Il permet de partager et d'accéder aux ressources d'autres ordinateurs fonctionnant avec des systèmes d'exploitation Microsoft® Windows® et Apple® Mac OS® X, ainsi que des systèmes GNU/Linux, *BSD et Solaris dans lesquels une implémentation de Samba est installée.
- ❑ Le protocole SMB (Server Message Block) est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.
- ❑ Remarque: Historiquement, les systèmes Windows utilisent leur propre protocole de partage de fichiers : SMB/CIFS. Le logiciel Samba a été développé pour permettre aux systèmes UNIX (dont Linux et Mac OS X) d'utiliser également ce protocole.

89

Serveur de fichiers Samba

- ❑ Il s'agit d'une réimplémentation des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix par ingénierie inverse. Samba a été initialement développée par l'Australien Andrew Tridgell et distribuée sous licence libre GNU GPL. Son nom provient du nom du protocole standard de Microsoft, SMB (Server Message Block), auquel ont été ajoutées les deux voyelles *a* : « SaMBa ».

Samba Active Directory

- ❑ Avec la sortie de la version 4.0 le 2 novembre 2012, Samba a désormais la capacité de servir de contrôleur de domaine Active Directory. Depuis cette version, le projet Samba a sorti une nouvelle version environ tous les 9 mois puis plus récemment tous les 6 mois.

90

Serveur de fichiers Samba

Serveur Samba → Solution pour un réseau multiplateforme

Pour configurer un protocole SMB(ou bien CIFS) il faut installer quelques modules de la suite du serveur Samba. Les quatre daemons (tâches de fond, ou processus qui s'exécute en arrière-plan) suivants forment le noyau de cette suite :

- ❑ **samba**: le daemon ajouté dans la version quatre, qui permet la gestion de l'Active Directory Domain Controllers.
- ❑ **smbd**: partage des données et imprimantes.
- ❑ **nmbd**: responsable de la résolution des noms NetBIOS(NETwork Basic Input Output System) dans les adresses IP, peut être configuré sur le fichier smb.conf
- ❑ **winbindd**: permet aux systèmes Linux de s'authentifier auprès d'un contrôleur de domaine Active Directory. Il est le composant effectuant le mapping entre les UID Linux et les SID (Security Identifier → Identifiant unique qui identifie chaque système, utilisateur ou objet (groupe) dans un réseau ou sur un PC) Windows.

91

Serveur de fichiers Samba : Installation

❑ Vous devez tout d'abord choisir entre agir directement sur votre serveur ou bien par accès à distance.

❑ Entrez la commande suivante pour installer le paquet Samba sur le serveur :

apt-get install samba

❑ Ajouter les comptes utilisateurs à la base de données Samba

Après avoir installé le serveur Samba, les comptes utilisateurs correspondants doivent être activés. Quelques distributions Linux synchronisent automatiquement les comptes d'utilisateurs de système disponibles dans le réseau et elles les ajoutent à la **base de données Samba**. Par exemple si le paquet libpam-smbpass est installé, les mots de passe Linux et SMB sont synchronisés. Dans d'autres cas, il est nécessaire de gérer manuellement les comptes utilisateurs pour que ces derniers puissent bénéficier des services de réseau correspondants.

92

Serveur de fichiers Samba : Installation

❑Ajouter les comptes utilisateurs à la base de données Samba

La première commande permet d'ajouter l'utilisateur respectif à la base de données du serveur Samba et activer le **partage de réseau**. Le mot de passe utilisateur (suivant le nom d'utilisateur) peut être attribué ou bien changé. Ce dernier peut être identique au mot de passe Linux ou bien s'en différencier. La deuxième commande (x) expulse l'utilisateur de la base de données tandis que la commande (d) le désactive. La commande (e) permet d'activer (ou de réactiver) un compte utilisateur.

sudo smbpasswd -a NOM UTILISATEUR (MOT DE PASSE)

sudo smbpasswd -x NOM UTILISATEUR

sudo smbpasswd -d NOM UTILISATEUR

sudo smbpasswd -e NOMU TILISATEUR

Le serveur peut charger et prendre en compte toutes les modifications effectuées grâce à la commande suivante :

sudo service smbd reload

93

Serveur de fichiers Samba : Installation

❑Configurer le partage de données Autorisations générales

Les autorisations générales peuvent être déterminées dans le fichier de configuration du serveur Samba. Ce fichier regroupe toutes les autorisations administratives et les propriétés générales du serveur. Ouvrez le fichier avec la commande suivante :

sudo gedit /etc/samba/smb.conf

Le fichier smb.conf contient de nombreux **exemples non commentés**, qui sont en règle générale inactifs et caractérisés par des losanges (#), ou point-virgules (;). Si vous souhaitez activer un tel exemple, il vous suffit de supprimer le caractère spécial. Vous pouvez insérer de nouvelles entrées selon les places disponibles sur le réseau à la fin du fichier en plaçant le nouveau nom entre crochets.

94

Serveur de fichiers Samba : Installation

❑ Configurer le partage de données Autorisations générales

`sudo gedit /etc/samba/smb.conf`

Par exemple pour partager un dossier avec des photos et autorisant des ajouts et modifications d'autres utilisateurs, vous pouvez configurer ces paramètres avec les commandes suivantes :

```
[Photos]
path= /documents/photos
writeable = yes
guest ok = yes
```

Pour prendre en compte ces modifications, vous devez à nouveau charger le serveur, grâce à la commande suivante :

`sudo service smbd reload`

Autres configurations Voir TP

95

Samba : versions principales

Samba 3.x

- ❑ Ancienne génération.
- ❑ Fonctionne comme un **contrôleur de domaine NT4**.
- ❑ Supporte le partage de fichiers, d'imprimantes et l'authentification Windows.
- ❑ Encore utilisé dans certains systèmes anciens, mais **obsolète aujourd'hui**.

Samba 4.x (version actuelle depuis 2012)

- ❑ Réécriture majeure avec **prise en charge d'Active Directory (AD)**.
- ❑ Peut fonctionner comme un **contrôleur de domaine AD**, compatible avec Windows Server.
- ❑ Inclut des fonctionnalités avancées comme :
 - Réplication AD
 - Gestion des GPO
 - DNS intégré

Bonnes pratiques à retenir :

- ❑ Toujours utiliser une version maintenue (ex : Samba 4.15 ou plus).
- ❑ Éviter SMBv1, désactivé par défaut dans Samba récent.
- ❑ Lire les notes de version pour suivre les nouveautés et les correctifs.

96

EternalBlue – Faille critique SMBv1

- ❑ EternalBlue est une vulnérabilité critique dans le protocole SMBv1 (Server Message Block version 1) de Microsoft Windows. Elle permet à un attaquant distant d'exécuter du code arbitraire sur un système vulnérable – sans authentification.
- ❑ Découverte par : la NSA (National Security Agency)
- ❑ Révélée publiquement par : le groupe de hackers Shadow Brokers en avril 2017
- ❑ Identifiant Microsoft : MS17-010
- ❑ Protocole concerné : SMBv1 (port TCP 445)
- ❑ Systèmes vulnérables : Windows XP, Vista, 7, 8, 10, Server 2003, 2008, 2012.
- ❑ Exécution de code à distance (RCE).
- ❑ Propagation automatique à d'autres machines sur le réseau.
- ❑ Permet l'exécution de code arbitraire à distance (accès total au système).

Comment se protéger ?

- **Installer le correctif MS17-010** (publié en mars 2017)
- **Désactiver SMBv1** (protocole obsolète et vulnérable)
- **Fermer le port 445** sur les pare-feu si non utilisé

97

Similitudes entre SMB et NFS

- ❑ Les protocoles Server Message Block (SMB) et Network File System (NFS) fonctionnent tous deux selon un modèle client-serveur, dans lequel les fichiers sont partagés sur le serveur distant et utilisés par le client local. Une fois les protocoles correctement configurés, lorsque vous accédez à des fichiers et à des répertoires réseau distants sur le serveur, cela fonctionne comme s'ils étaient locaux sur le système de fichiers de la machine client.
- ❑ Voici d'autres similitudes entre SMB et NFS :
 - Les deux permettent aux clients d'effectuer des opérations de création, de lecture, de mise à jour et de suppression sur les fichiers et les répertoires du serveur.
 - Vous pouvez les utiliser avec plusieurs systèmes d'exploitation. Cela inclut tous les systèmes d'exploitation courants, les environnements Windows et les environnements Linux.
 - SMB et NFS sont souvent utilisés dans les environnements réseau hérités, en particulier dans les infrastructures sur site.

98

Principales différences : NFS vs. SMB

❑ Network File System (NFS) et Server Message Block (SMB) présentent quelques différences en ce qui concerne leurs détails opérationnels.

Design original

- Bien que NFS et SMB puissent être utilisés sur tous les systèmes d'exploitation, le protocole SMB est le protocole Windows natif par défaut pour le partage de fichiers. Les fonctionnalités de Windows sont conçues autour de SMB. Vous avez besoin d'outils externes tels que Samba pour utiliser SMB sur des ordinateurs Linux et accéder à des fichiers Windows Server distants.
- En revanche, le protocole NFS a été conçu spécifiquement pour les systèmes Unix. Il s'agit d'un protocole de partage de fichiers natif, qui est le protocole de transfert de fichiers par défaut dans la plupart des distributions Linux.

Les ressources partagées

- SMB a été conçu pour vous permettre de partager un large éventail de ressources réseau, notamment des services de fichiers et d'impression, des périphériques de stockage et des machines virtuelles.
- Cela diffère de NFS, qui ne prend en charge que le partage de fichiers et de répertoires.

Communications de client à client

- SMB permet aux clients de communiquer et de partager des fichiers entre eux en utilisant le serveur comme médiateur.
- NFS autorise uniquement les opérations client-serveur.

99

Plan

- Serveur FTP, Telnet et SSH
- Serveur HTTP Apache
- VPN & OpenVPN
- Configuration VLAN, VTP et STP
- ACL (Listes de Contrôle d'Accès)
- Le protocole de supervision SNMP
- Serveur NFS et Serveur de fichiers Samba

▪ Serveur DNS (BIND9)

- Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)
- Serveur d'impression

100

Domain Name System

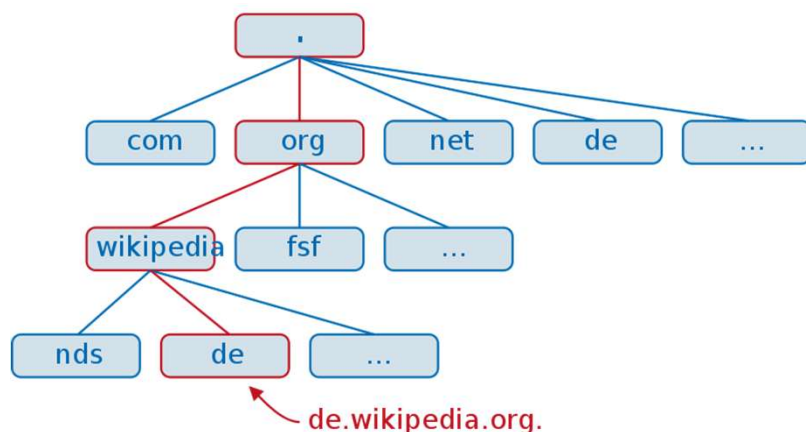
Domain Name System

- ❑ Le **Domain Name System** (Système de nom de domaine) ou DNS est un protocole de la couche 7 du modèle OSI. C'est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements. En fournissant dès les premières années d'Internet, autour de 1985, un service distribué de résolution de noms, le DNS est un composant essentiel du développement du réseau informatique.
- ❑ Le DNS est un protocole qui se charge d'effectuer la correspondance entre les adresses littérales et adresses IP. Plus précisément, il assoie un nom d'hôte à une adresse IP (et inversement). Cela permet donc de connaître l'adresse IP d'une adresse en lettre et inversement. Un serveur **DNS** (**Domain Name System**) est un serveur de noms qui gère les correspondances entre les noms de domaine et les adresses **IP**. Ce qui est fort utile pour naviguer sur internet, imaginez-vous mémoriser l'adresse **IP** de chaque site sur lequel vous souhaitez aller ? On peut penser que sans serveur **DNS** il n'y a plus d'internet.
- ❑ Le DNS fait correspondre un domaine à son adresse IP et inversement.
- ❑ Par défaut, la connexion internet utilise les serveurs de noms du fournisseur d'accès. Ces derniers sont attribués automatiquement par le protocole DHCP.

101

Domain Name System

Domain Name System : Hiérarchie du DNS



- ❑ Le système des noms de domaine consiste en une hiérarchie dont le sommet est appelé la racine. On représente cette dernière par un point. Dans un domaine, on peut créer un ou plusieurs sous-domaines ainsi qu'une délégation pour ceux-ci, c'est-à-dire une indication que les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur. Ces sous-domaines peuvent à leur tour déléguer des sous-domaines vers d'autres serveurs.

102

Domain Name System

Domain Name System : Serveurs DNS racine

- ❑ Les serveurs racine sont gérés par douze organisations différentes : deux sont européennes, une japonaise et les neuf autres sont américaines. Sept de ces serveurs sont en réalité distribués dans le monde grâce à la technique anycast et neuf disposent d'une adresse IPv6. Grâce à anycast, plus de 200 serveurs répartis dans 50 pays du monde assurent ce service.
- ❑ Il existe 13 autorités de nom appelées:
 - <https://a.root-servers.org/>
 - ...
 - <https://m.root-servers.org>
- ❑ Le serveur k reçoit par exemple de l'ordre de 70 000 à 100 000 requêtes par seconde en avril 2019.
- ❑ Le DNS ne fournit pas de mécanisme pour découvrir la liste des serveurs racine, chacun des serveurs doit donc connaître cette liste au démarrage grâce à un encodage explicite. Cette liste est ensuite mise à jour en consultant l'un des serveurs indiqués. La mise à jour de cette liste est peu fréquente de façon que les serveurs anciens continuent à fonctionner.

❑ Exemples d'adresses de serveurs DNS

Google Public DNS : 8.8.8.8

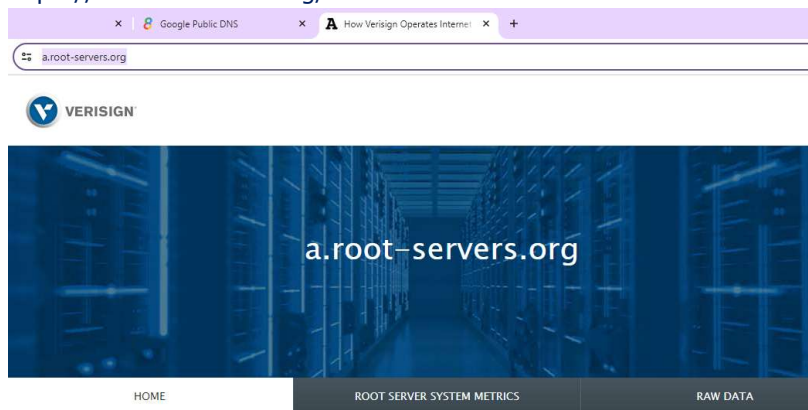
OpenDNS : 208.67.222.222

103

Domain Name System

Domain Name System : Serveurs DNS racine

- ❑ <https://a.root-servers.org/>



Verisign operates a.root-servers.net, one of the thirteen logical Internet Root name servers. Verisign cooperates with the eleven other [Root Server Operators](#) to provide authoritative data for the DNS Root Zone.

A-root receives DNS queries over IPv4 at [198.41.0.4](#) and over IPv6 at [2001:503:ba3e::2:30](#).

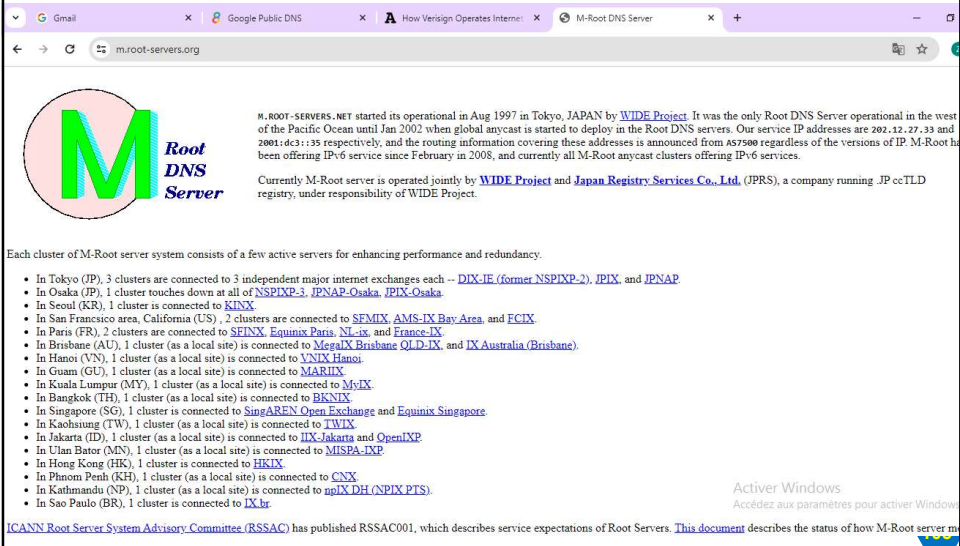
Activier Windows
Accédez aux paramètres

104

Domain Name System

Domain Name System : Serveurs DNS racine

□ m.root-servers.org



The screenshot shows the homepage of m.root-servers.org. It features a large green 'M' logo with 'Root DNS Server' text. The main text describes the history of the M-Root server, starting in 1997 in Tokyo, Japan, by the WIDE Project. It mentions that it was the only Root DNS Server operational in the west of the Pacific Ocean until Jan 2002. The text also states that the M-Root server is currently operated jointly by the WIDE Project and Japan Registry Services Co., Ltd. (JPRS). A list of active servers is provided, including Tokyo (JP), Osaka (JP), Seoul (KR), San Francisco (US), Paris (FR), Brisbane (AU), Hanoi (VN), Guam (GU), Kuala Lumpur (MY), Bangkok (TH), Singapore (SG), Kaohsiung (TW), Jakarta (ID), Ulan Bator (MN), Hong Kong (HK), Phnom Penh (KH), Kathmandu (NP), and Sao Paulo (BR). The page also mentions the ICANN Root Server System Advisory Committee (RSSAC) and provides a link to the RSSAC001 document.

Each cluster of M-Root server system consists of a few active servers for enhancing performance and redundancy.

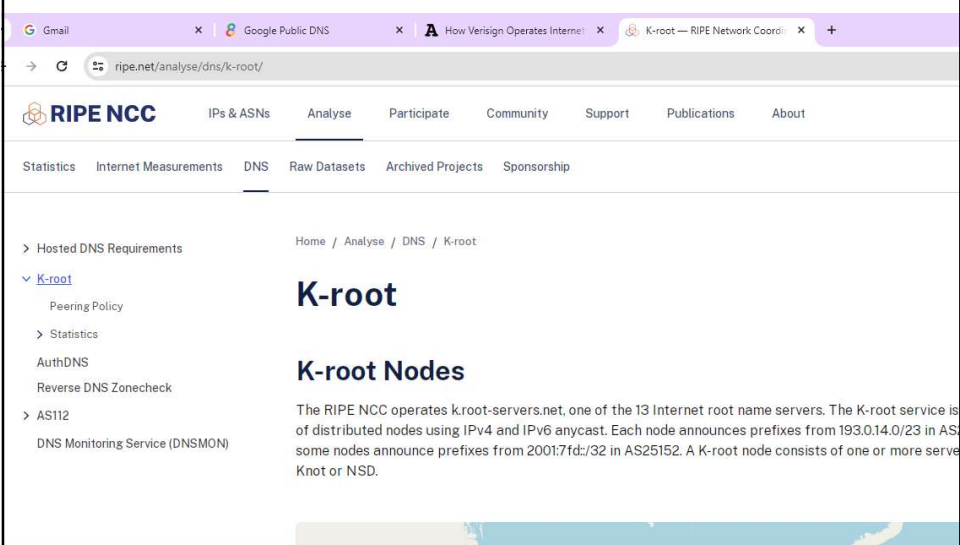
- In Tokyo (JP), 3 clusters are connected to 3 independent major internet exchanges each -- [DIX-IE](#) (former NSPIX-2), [JPIX](#), and [JPNAP](#).
- In Osaka (JP), 1 cluster touches down at all of [NSPIX-3](#), [JPNAP-Osaka](#), [JPIX-Osaka](#).
- In Seoul (KR), 1 cluster is connected to [KINX](#).
- In San Francisco area, California (US), 2 clusters are connected to [SFMIX](#), [AMS-IX Bay Area](#), and [ECIX](#).
- In Paris (FR), 2 clusters are connected to [SEINX](#), [Equinix Paris](#), [NL-ix](#), and [France-IX](#).
- In Brisbane (AU), 1 cluster (as a local site) is connected to [MegaIX Brisbane QLD-IX](#), and [IX Australia \(Brisbane\)](#).
- In Hanoi (VN), 1 cluster (as a local site) is connected to [VNIX Hanoi](#).
- In Guam (GU), 1 cluster (as a local site) is connected to [MARIX](#).
- In Kuala Lumpur (MY), 1 cluster (as a local site) is connected to [MfIX](#).
- In Bangkok (TH), 1 cluster (as a local site) is connected to [BKNIX](#).
- In Singapore (SG), 1 cluster is connected to [SingAREN Open Exchange](#) and [Equinix Singapore](#).
- In Kaohsiung (TW), 1 cluster (as a local site) is connected to [TWIX](#).
- In Jakarta (ID), 1 cluster (as a local site) is connected to [IX-Jakarta](#) and [OpenIXP](#).
- In Ulan Bator (MN), 1 cluster (as a local site) is connected to [MISPA-IXP](#).
- In Hong Kong (HK), 1 cluster is connected to [HKIX](#).
- In Phnom Penh (KH), 1 cluster (as a local site) is connected to [CNX](#).
- In Kathmandu (NP), 1 cluster (as a local site) is connected to [ngIX DH/NPIX PTS](#).
- In Sao Paulo (BR), 1 cluster is connected to [IX.br](#).

ICANN Root Server System Advisory Committee (RSSAC) has published RSSAC001, which describes service expectations of Root Servers. [This document](#) describes the status of how M-Root server m

Domain Name System

Domain Name System : Serveurs DNS racine

□ K.root-servers.org



The screenshot shows the homepage of K.root-servers.org. It features a navigation bar with links to Statistics, Internet Measurements, DNS, Raw Datasets, Archived Projects, and Sponsorship. The main content area is titled 'K-root' and 'K-root Nodes'. It describes the RIPE NCC's role in operating K.root-servers.net, one of the 13 Internet root name servers. The text mentions that the K-root service is distributed across nodes using IPv4 and IPv6 anycast, and that each node announces prefixes from 193.0.14.0/23 in AS some nodes announce prefixes from 2001:7fd::32 in AS25152. A K-root node consists of one or more servers Knot or NSD.

Home / Analyse / DNS / K-root

K-root

K-root Nodes

The RIPE NCC operates k.root-servers.net, one of the 13 Internet root name servers. The K-root service is of distributed nodes using IPv4 and IPv6 anycast. Each node announces prefixes from 193.0.14.0/23 in AS some nodes announce prefixes from 2001:7fd::32 in AS25152. A K-root node consists of one or more servers Knot or NSD.

DNS PRIVÉ (Réseau Local)

- ❑ Le DNS privé est un type de service DNS utilisé au sein d'un réseau privé, tel qu'un réseau d'entreprise ou domestique, pour résoudre des noms de domaine en adresses IP.
- ❑ De plus, dans le cas d'un **réseau local** si vous souhaitez faire de la résolution de noms c'est à dire que les hôtes du **LAN** puissent communiquer entre elles grâce à leur nom de domaine, le serveur **DNS** permet de donner un nom de domaine complet à une machine. Ainsi il y aura une correspondance entre l'adresse **IP** de l'hôte et le nom que vous lui donnez grâce au **DNS**.

107

Bind9 (Berkley Internet Naming Daemon)

Bind9 (Berkley InternetNaming Daemon)

- ❑ BIND ou BIND 9 est une implémentation open source du DNS, disponible pour presque toutes les distributions Linux. BIND est l'acronyme de Berkeley Internet Name Domain et permet de publier des informations DNS sur Internet ainsi que de résoudre les requêtes DNS des utilisateurs.
- ❑ Un serveur qui héberge le service DNS est appelé "serveur de noms". Ubuntu est livré par défaut avec BIND (Berkley InternetNaming Daemon), le serveur DNS le plus utilisé sur Internet.
- ❑ **BIND** (prononcé /baɪnd/ pour Berkeley Internet Name Daemon, parfois Berkeley Internet Name Domain) était le logiciel pour serveurs DNS le plus utilisé sur Internet (spécialement sur les systèmes de type UNIX et est devenu un standard. La première version de BIND a été conçue par quatre étudiants diplômés de Berkeley sur la base du système d'exploitation BSD 4.3. En 1988, Paul Vixie a repris la maintenance du projet. Depuis 1994 le logiciel est développé par l'Internet Systems Consortium.
- ❑ **BIND** : Dernière version 9.18.27 (15 mai 2024)

❑ **Installation & configuration ---- > Voir TP**

108

Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)

OpenLDAP est une implémentation libre du protocole LDAP maintenue par le projet OpenLDAP et distribuée selon les termes de la licence *OpenLDAP Public Licence*. Outre le code source, on trouve des versions compilées pour GNU/Linux, FreeBSD, NetBSD, OpenBSD, AIX, HP-UX, Mac OS X, Solaris, et Microsoft Windows.

- ❑ OpenLDAP est un annuaire informatique qui fonctionne sur le modèle client/serveur. Il contient des informations de n'importe quelle nature qui sont rangées de manière hiérarchique.
- ❑ Pour bien comprendre le concept, il est souvent comparé aux pages jaunes, où **le lecteur recherche un numéro de téléphone particulier : il va d'abord sélectionner la profession, puis la ville, puis le nom de l'entrée pour trouver finalement le numéro de téléphone.**
- ❑ En pratique, dans un réseau informatique, il est utilisé pour enregistrer une grande quantité d'utilisateurs ou de services, parfois des centaines de milliers. Il permet d'organiser hiérarchiquement les utilisateurs par département, par lieu géographique ou par n'importe quel autre critère. C'est une alternative libre à Microsoft **Active Directory**.

❑ Stockage

Le logiciel OpenLDAP ne stocke pas les données directement, il utilise une bibliothèque tierce pour le faire. Généralement, c'est la base de données Berkeley DB qui est utilisée sous GNU/Linux. Mais il est possible d'utiliser MySQL, LDBM, des fichiers à plat, etc.

109

Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)

Composants d'OpenLDAP

- ❑ OpenLDAP est constitué de 3 éléments principaux :
 1. **slapd** (Stand-alone LDAP Daemon) : démon LDAP autonome. Il écoute les connexions LDAP sur n'importe quel port (389 par défaut) et répond aux opérations LDAP qu'il reçoit via ces connexions. Typiquement, slapd est appelé au moment du boot.
 2. des **bibliothèques** implémentant le protocole LDAP.
 3. des **utilitaires**, des outils et des exemples de clients.
- ❑ Le projet OpenLDAP propose également des bibliothèques LDAP en Java :
 1. JLDAP : bibliothèque d'accès à LDAP en Java.
 2. JDBC-LDAP driver JDBC faisant office de pont JDBC-LDAP.

110

Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)

Principales versions

Les versions d'OpenLDAP :

- OpenLDAP Version 1 (1998) : première version publique
- OpenLDAP Version 2 (août 2000) : prise en charge de LDAPv3, d'IPv6, du TLS, ...
- OpenLDAP Version 2.1 (juin 2002) :
- OpenLDAP Version 2.2 (décembre 2003) :
- OpenLDAP Version 2.3 (juin 2005) : possibilité d'avoir la configuration accessible dans l'annuaire (*cn=config*)
- OpenLDAP Version 2.4 (octobre 2007) : réplication miroir et multi-maître; réplication Proxy Sync; extensions LDAP v3.
-
- OpenLDAP version 2.6.8 (21 mai 2024)

Remarque:

PhpLDAPAdmin

PhpLDAPAdmin est une interface en PHP qui facilite l'édition des données du serveur OpenLDAP. Son utilisation passe par un navigateur Web.

Apache Directory Studio

Apache Directory Studio est une interface en Java basé sur Eclipse. Permet de gérer l'architecture LDAP, les Schémas LDAP et les fichiers LDIF.

111

Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)

PhpLDAPAdmin

PhpLDAPAdmin est une interface en PHP qui facilite l'édition des données du serveur

The screenshot displays the PhpLDAPAdmin web interface. On the left, a tree view shows the LDAP directory structure under 'My LDAP Server'. The right pane is titled 'Create Object' and shows the 'New Posix Group (Step 1 of 1)' form. The form includes fields for 'Group' (with a yellow input box), 'GID Number' (set to 1004), and 'Users' (a list with checkboxes for 'ldap1 Asdasd (ldap1)' and 'Jack Wallen (jwall)'). A 'Create Object' button is at the bottom of the form.

Lightweight Directory Access Protocol (LDAP)

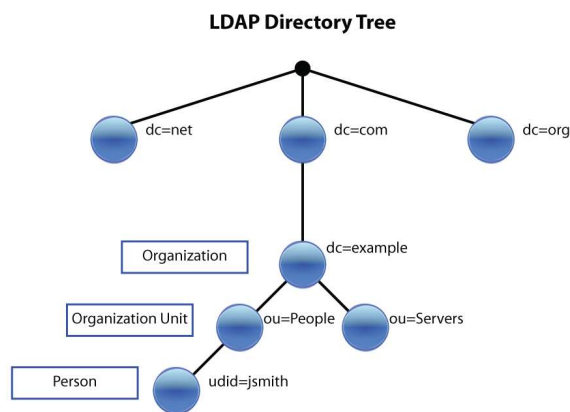
- ❑ LDAP est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire (il est une évolution du protocole DAP). C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.
- ❑ Le nommage des éléments constituant l'arbre (racine, branches, feuilles) reflète souvent le modèle politique, géographique ou d'organisation de la structure représentée. La tendance actuelle est d'utiliser le nommage DNS pour les éléments de base de l'annuaire (racine et premières branches, *domain components* ou **dc=...**). Les branches plus profondes de l'annuaire peuvent représenter des unités d'organisation ou des groupes (*organizational units* ou **ou=...**), des personnes (*common name* ou **cn=...** voire *user identifier* **uid=...**). L'assemblage de tous les composants (du plus précis au plus général) d'un nom forme son *distinguished name*, l

113

LDAP

les éléments de base de l'annuaire :

- racine et premières branches, *domain components* ou **dc=...**
- Les branches plus profondes de l'annuaire peuvent représenter des unités d'organisation ou des groupes (*organizational units* ou **ou=...**),
- des personnes (*common name* ou **cn=...** voire *user identifier* **uid=...**).



114

LDAP

```

graph TD
    A[dc=org] --> B[dc=example]
    B --> C[ou=people]
    B --> D[ou=groups]
    C --> E[uid=toto]
  
```

Lightweight Directory Access Protocol (LDAP)

Structure de l'annuaire

- Les annuaires LDAP suivent le modèle X.500 et son architecture nativement multi-tenant :
- Un annuaire est un **arbre** d'entrées.
- Une entrée est constituée d'un ensemble d'attributs.
- Un attribut possède un nom, un type et une ou plusieurs valeurs.
- Les attributs sont définis dans des *schémas*.
- Le fait que les attributs puissent être multi-valués est une différence majeure entre les annuaires LDAP et les SGBDR. De plus, si un attribut *n'a pas* de valeur, il est purement et simplement *absent* de l'entrée.
- Chaque entrée a un identifiant unique, le *Distinguished Name* (DN). Il est constitué à partir de son *Relative Distinguished Name* (RDN) suivi du DN de son parent. C'est une définition récursive. On peut faire l'analogie avec une autre structure arborescente, les systèmes de fichiers ; le DN étant le chemin absolu et le RDN le chemin relatif à un répertoire. En règle générale le RDN d'une entrée représentant une personne est l'attribut *uid* :

115

LDAP

Lightweight Directory Access Protocol (LDAP)

Structure de l'annuaire

En règle générale le RDN d'une entrée représentant une personne est l'attribut *uid* :

```

graph TD
    A[dc=org] --> B[dc=example]
    B --> C[ou=people]
    B --> D[ou=groups]
    C --> E[uid=toto]
  
```

Le RDN de toto est *rdn:uid=toto*, son DN est *dn:uid=toto, ou=people, dc=example, dc=org*.
 Une entrée peut ressembler à la représentation suivante lorsqu'elle est formatée en LDIF :

116

Serveur d'impression

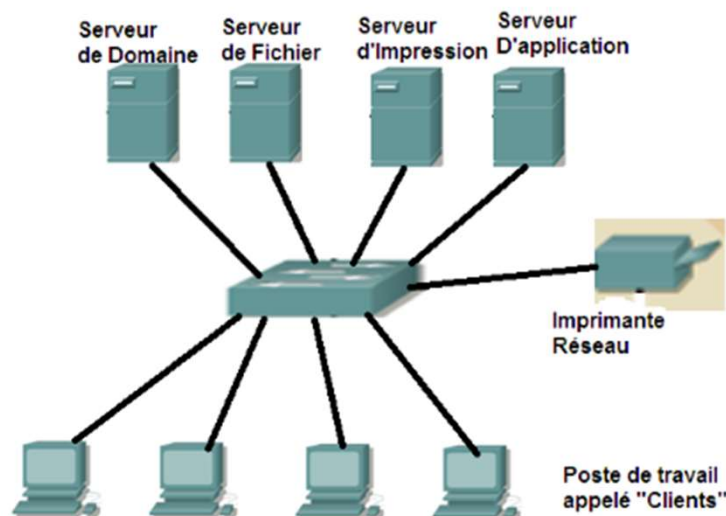
Serveur d'impression

- ❑ Un **serveur d'impression** est un serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs (ou ordinateurs) situés sur un même réseau informatique.
- ❑ Le serveur d'impression est un **périphérique réseau qui connecte les imprimantes et les ordinateurs de l'entreprise**. Ainsi, plusieurs collaborateurs peuvent utiliser la même imprimante.
- ❑ Agissant en tant qu'intermédiaire, ce serveur doit **gérer les requêtes d'impression** entre les ordinateurs et les imprimantes. Concrètement, lorsqu'un collaborateur souhaite imprimer un document, il envoie une requête via son ordinateur au serveur d'impression. Celui-ci va alors l'envoyer à la bonne imprimante afin de répondre favorablement à la demande d'impression du collaborateur.
- ❑ Le serveur dispose donc :
 - d'une connexion réseau (par exemple, un port RJ45 pour un réseau ethernet) gérant les protocoles réseaux (par exemple, TCP/IP, NetBEUI, AppleTalk) ;
 - d'une ou plusieurs connexions à des imprimantes. La plupart des serveurs d'impression disposent de connexions USB ; certains disposent également de ports parallèles. Certains serveurs d'impressions ne sont pas connectés directement par leur câble d'interface aux imprimantes. Ces dernières sont connectées via le réseau, en effet, les imprimantes professionnelles sont généralement connectées directement sur le réseau pour permettre une répartition au sein des locaux de l'entreprise.

117

Serveur d'impression

Serveur d'impression



118

Serveur d'impression

Serveur d'impression

- ❑ Le serveur d'impression peut être constitué d'un ordinateur qui partage une imprimante qui lui est directement connectée (ou à travers le réseau), ce peut également être un petit appareil spécialisé dédié. L'avantage de cette dernière solution est son faible prix. Un serveur d'impression doit toujours rester sous tension et il doit avoir une adresse IP fixe.
- ❑ Il peut être situé sur un poste client : à partir du moment où l'imprimante est connectée sur un ordinateur et que celle-ci est partagée, ce poste devient ce que l'on nomme un serveur d'impression.
- ❑ Les documents à imprimer sont placés sur des files d'attente (*spool*) puis envoyés petit à petit à l'imprimante.
- ❑ Le système d'impression qui est le plus utilisé aujourd'hui sous Linux et Unix est CUPS (Common Unix Printing System).
- ❑ Pour communiquer avec les imprimantes et les clients, les serveurs d'impressions utilisent une grande variété de protocoles tels LPD/LPR, IPP utilisé par CUPS, NetBIOS, AppSocket utilisé par les serveurs d'impression JetDirect ou encore IPX/SPX.

119

Bibliographie

1. https://cisco.ofppt.info/ccna2/course/module9/index.html?utm_source=chatgpt.com#9.3.2.7
2. <http://eventus-networks.blogspot.com/2013/11/les-topologies-physiques-et-logiques.html>
3. https://fr.wikipedia.org/wiki/IEEE_802.3
4. Hardware support : <http://www.cisco.com/public/support/tac/hardware.shtml>
5. <http://www.cisco.com/>
6. <https://fr.scribd.com/doc/142546820/PresentationVPN-ppt>
7. <http://cisco.ofppt.info/ccna4/course/module2/2.2.3.5/2.2.3.5.html>
8. http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours_secu_2_3_VPN.pdf
9. <http://cisco.ofppt.info/ccna4/course/module7/index.html#7.1.2.2>
10. <https://lazaarsaiida.wordpress.com/wp-content/uploads/2015/11/vpn1.pdf>
11. https://helios2.mi.parisdescartes.fr/~mea/cours/DU/IPsec_DUsec.pdf
12. <https://aws.amazon.com/fr/what-is/ipsec/>
13. <http://cisco.ofppt.info/ccna4/course/module7/7.3.2.6/7.3.2.6.html>
14. <https://fr.scribd.com/document/480077575/Expose-Open-VPN-pdf>
15. https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol
16. <https://aws.amazon.com/fr/compare/the-difference-between-nfs-smb/>
17. <https://openclassrooms.com/fr/courses/2356316-montez-un-serveur-de-fichiers-sous-linux/5173631-partagez-vos-fichiers-sur-un-reseau-linux-avec-nfs>
18. [https://fr.wikipedia.org/wiki/Samba_\(informatique\)](https://fr.wikipedia.org/wiki/Samba_(informatique))
19. https://fr.wikipedia.org/wiki/Server_Message_Block
20. <https://www.it-connect.fr/serveur-de-fichiers-debian-installer-et-configurer-samba-4/>
21. <https://doc.ubuntu-fr.org/samba>
22. <https://www.malekal.com/dns-serveurs-de-noms-fonctionnement/>
23. <https://www.it-connect.fr/dns-avec-bind-9%Ef%BB%BF/>
24. https://fr.wikipedia.org/wiki/Domain_Name_System
25. <https://fr.wikipedia.org/wiki/BIND>
26. <https://fr.wikipedia.org/wiki/OpenLDAP>

120