Machine	OS	Distribution	Version	C/S	IP
			1.0		

SÉCURISATION D'UN COMMUTATEUR ET AGRÉGATION DE LIENS LACP

Machine	OS	Distribution	Version	C/S	IP
			1.0		

Table des matières

Machine	OS	Distribution	Version	C/S	IP
			1.0		

Objectif :

L'objectif de cette procédure est de sécuriser les accès d'un commutateur et de mettre en place une agrégation de liens entre deux commutateurs.

Prérequis :

- Switch Cisco.
- Sécurisation de commutateurs.
- Agrégation de liens LACP.

Légende :

Les textes surlignés en jaune correspondent à des commandes ou à des indications qui permet de justifier les résultats obtenus ou de montrer des informations qu'elles doivent être respectées.

Mise en place de l'agrégation de liens LACP:

Afin de mettre en place l'agrégation de liens LACP, on va utiliser les ports en gigabitEthernet :

```
Switch(config)#interface range gigabitEthernet 0/1-2
```

On crée ensuite un groupe qui englobera les deux ports qui utiliseront l'agrégation de liens :

```
Switch(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
```

On applique ensuite au groupe le protocole LACP qui va permettre de faire l'agrégation de liens :

```
Switch(config-if-range)#channel-protocol lacp
```

On active les ports :

```
Switch(config-if-range)#no shutdown
```

Ensuite, on configure l'interface port-channel afin que chaque vlan puisse communiquer avec un autre vlan :

```
Switch(config)#interface port-channel 1
```

```
Switch(config-if)#switchport mode trunk
```

On active le port :

```
Switch(config-if)#no shutdown
```

On doit effectuer ces commandes sur les deux switchs.

Machine	OS	Distribution	Version	C/S	IP
			1.0		

On commence par observer si nos ports sont bien configurés dans le bon groupe avec la commande suivante :

```
Switch#show etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi0/1(P)    Gi0/2(P)
```

Nous regardons ensuite si la bande passante obtenue correspond bien à nos attentes :

```
Switch#show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001b.53f4.8319 (bia 001b.53f4.8319)
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Gi0/1 Gi0/2
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:09:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     705 packets input, 62204 bytes, 0 no buffer
     Received 705 broadcasts (705 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 705 multicast, 0 pause input
     0 input packets with dribble condition detected
     123 packets output, 24214 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Machine	OS	Distribution	Version	C/S	IP
			1.0		

On regarde les informations etherchannel :

```
Switch#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:00h:19m:38s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active             0
  0     00     Gi0/2    Active             0

Time since last port bundled:    0d:00h:19m:28s    Gi0/2
```

On peut utiliser la commande iperf pour mesurer la bande passante pour tester la mise en place du protocole LACP :

```
root@debian:~# iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.1.136 port 5001 connected with 192.168.1.25 port 36598
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.1 sec   113 MBytes  94.1 Mbits/sec
```

Machine	OS	Distribution	Version	C/S	IP
			1.0		

Sécurisation du switch :

Pour commencer, on renomme le switch :

```
Switch(config)#hostname SWITCH
```

On crypte ensuite le mot de passe :

```
SWITCH(config)#enable secret 12345
```

On crée un utilisateur en local :

```
SWITCH(config)#username antoine password 12345
```

Ensuite, on donne un nom de domaine au switch :

```
SWITCH(config)#ip domain-name gbs.local
```

On génère les certificats SSH grâce aux commandes *crypto key generate rsa*. On active le SSH avec *ip ssh version 2*, *line vty 0 4*, *transport input ssh*, *login local*, *username antoine password* 12345.

On peut ajouter une auto-logout de session qui permet de nous déconnecter au bout de x minutes et une déconnexion automatique en cas d'inactivité d'une durée de y minutes grâce aux commandes suivantes :

ip ssh version 2

line vty 0 4

exec-timeout x 0

line con 0

exec-timeout y 0

On va ensuite désactiver services inutiles.

On désactive le protocole VTP qui permet de gérer de manière centralisé les VLANS d'un réseau :

```
SWITCH(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

On désactive également le service source-routing qui permet à l'émetteur d'un paquet IP de spécifier le chemin que doit prendre le paquet pour accéder à sa destination :

```
SWITCH(config)#no ip source-route
```

On désactive le service CDP qui permet de savoir s'il agit d'un matériel Cisco, de récupérer le numéro du modèle et la version de l'OS :

```
SWITCH(config)#no cdp run
```

On désactive le service HTTP qui est non sécurisé :

```
SWITCH(config)#no ip http server
```

On désactive le service finger qui permet de découvrir les utilisateurs enregistrés sur le dispositif d'un réseau :

```
SWITCH(config)#no service finger
```

Enfin, on désactive les services « small servers » qui sont des services de transmission de données :

```
SWITCH(config)#no service tcp-small-servers
```

```
SWITCH(config)#no service udp-small-servers
```

On active ensuite des services de sécurité.

On active le service password encryption qui permet de chiffrer certains mots de passe :

```
SWITCH(config)#service password-encryption
```

On active le service tcp-keepalives-in qui permet de réduire les effets d'une attaque DoS :

```
SWITCH(config)#service tcp-keepalives-in
```

On active le service scheduler qui permet de tuer les processus plantés ou bloqués :

```
SWITCH(config)#scheduler max-task-time 5000
```

On active le DHCP snooping pour éviter le DHCP spoofing :

```
SWITCH(config)#ip dhcp snooping
```

Machine	OS	Distribution	Version	C/S	IP
			1.0		

On configure un port de confiance. Il sera le seul à émettre des requêtes de type OFFER et ACK :

```
SWITCH(config)#interface GigabitEthernet 0/47
SWITCH(config-if)#ip dhcp snooping trust
SWITCH(config-if)#ip dhcp snooping limit rate 100
```

Enfin, on va sécuriser les ports avec port-security. Il existe deux manières : une version manuelle et une version automatique :

Voici la version manuelle :

```
SWITCH(config)#interface gigabitEthernet 0/47
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security mac-address 74d4.35e2.01a7
```