



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 24 juin 2016

N° DAT-NT-25/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 75

NOTE TECHNIQUE

RECOMMANDATIONS POUR LA SÉCURISATION D'UN COMMUTATEUR DE DESSERTE



Public visé :

Développeur	<input type="checkbox"/>
Administrateur	<input checked="" type="checkbox"/>
RSSI	<input checked="" type="checkbox"/>
DSI	<input checked="" type="checkbox"/>
Utilisateur	<input type="checkbox"/>

INFORMATIONS

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations pour la sécurisation d'un commutateur de desserte** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
BAI, BAS, BRT, BSC, LRP	BSS	SDE	24 juin 2016

Évolutions du document :

Version	Date	Nature des modifications
1.0	24 juin 2016	Version initiale

Pour toute question :

Contact	Adresse	@mél
Division Assistance Technique de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	conseil.technique@ssi.gouv.fr

Table des matières

1	Préambule	5
1.1	Documents de référence	5
1.2	Acronymes et terminologie	6
2	Les commutateurs dans le système d'information	8
3	Interface en ligne de commande	9
4	Administration	10
4.1	Réseau d'administration <i>out-of-band</i>	10
4.1.1	Port physique dédié	10
4.1.2	Réseau dédié	11
4.2	Accès à l'administration du commutateur	11
4.2.1	Port console (CTY - ligne console)	11
4.2.2	Port Ethernet (VTY - ligne virtuelle)	12
4.2.2.1	SSH	12
4.2.2.2	HTTP/HTTPS	15
4.2.2.3	Telnet	16
4.2.2.4	Limitation de l'accès à l'interface d'administration	16
4.2.3	Journalisation des authentifications	17
4.2.4	Protection contre l'attaque par force brute	17
4.3	Gestion des comptes utilisateur	18
4.3.1	Niveau de privilège	18
4.3.2	Accès <i>enable</i> ou <i>system-view</i>	19
4.3.3	Comptes locaux et comptes centralisés	20
4.3.3.1	Gestion des comptes locaux	20
4.3.4	Désactivation/suppression des comptes par défaut	22
4.4	Contrôle d'accès	22
4.4.1	RADIUS	24
4.4.2	TACACS+	25
4.5	Politique de sécurité des mots de passe	26
4.6	Bannière de connexion	26
5	Cloisonnement des réseaux et VLAN	27
5.1	Configuration automatique des VLAN	27
5.2	Configuration des VLAN	28
5.2.1	Ports en mode <i>access</i>	28
5.2.2	Ports en mode <i>trunk</i>	29
5.3	DTP	30
5.4	VLAN de quarantaine	30
5.5	VLAN par défaut et VLAN natif	31
5.6	<i>Private VLAN</i> (ou PVLAN)	33
5.7	<i>Protected Port</i> et <i>Port Isolation</i>	38

6	Routage	38
6.1	Routage interVLAN	38
6.2	Mandataire ARP	39
6.3	Source routing	39
7	Sécurisation des ports	40
7.1	Port security	41
7.2	Contrôle d'accès par port 802.1X avec authentification par RADIUS	42
8	Mécanismes liés à la disponibilité	44
8.1	DHCP snooping et IP Source Guard	44
8.2	Inspection ARP	46
8.3	Spanning Tree	46
8.4	Storm control	48
8.5	Small-frame arrival rate	49
8.6	Protocol storm protection	50
8.7	Protection contre les trames indésirables (port blocking)	51
9	Synchronisation horaire et horodatage	51
9.1	Synchronisation horaire	51
9.2	Horodatage des événements journalisés	52
10	Journalisation	53
10.1	Niveau de journalisation	53
10.2	Centralisation des journaux	53
10.3	Journalisation des commandes de configuration	54
10.4	Cache	55
10.5	Stockage des journaux	55
10.6	Console et terminal	56
10.7	Particularité de la console	57
11	Supervision : SNMP	57
11.1	SNMPv3	59
11.1.1	Mode get	59
11.1.2	Mode trap	60
11.2	SNMPv2c	61
11.2.1	Mode get	61
11.2.2	Mode trap	61
12	Agrégation des liens	62
13	Gestion du parc et MCO/MCS	65
13.1	Homogénéité des équipements et des versions de système d'exploitation	65

13.2	Système d'exploitation à jour	65
13.3	Gestion du changement	67
13.4	Centralisation de la gestion des commutateurs	67
13.5	Sauvegarde et restauration des configurations	67
13.6	Outil de vérification de configuration	68
13.7	Les macros	68
14	Autres fonctionnalités	68
14.1	Fonctionnalités à activer	68
14.2	Fonctionnalités à désactiver	69
15	Disponibilité du système	70
15.1	Gestion du CPU	70
15.2	Gestion de la mémoire	71
15.3	Gestion des connexions TCP	71
15.4	Interface Null0	72
Annexes	72
A	Les macros	72
A.1	Exemples de macros Cisco	72
A.1.1	Création de la macro : désactivation d'un port inutilisé	72
A.1.2	Création de la macro : port <i>access</i>	73
A.1.3	Création de la macro : port <i>trunk</i>	73
A.2	Utilisation des macros	74

1 Préambule

Les commutateurs sont des équipements réseau très répandus au sein des systèmes d'information. Ils distribuent une grande partie des données qui y transitent. S'ils ne doivent pas être considérés comme des équipements de sécurité, leur rôle est souvent trop négligé dans la mise en place des mesures de sécurisation du SI. Étant donné leur positionnement et leur rôle dans le SI de l'entité (entreprise, administration, association, etc.), à la fois physiquement proche des utilisateurs pour certains et véhiculant beaucoup d'informations, ils ont potentiellement un impact important sur la sécurité et le fonctionnement du SI (déni de service, écoute du trafic réseau, intrusion dans le SI, etc.). Il convient donc de veiller à les sécuriser du mieux possible afin de renforcer leur robustesse face à des actions malveillantes (venant du SI interne ou de l'extérieur) ou à des erreurs de configuration.

Le but de cette note est d'améliorer le niveau de sécurité des SI en accompagnant les administrateurs réseau dans leurs tâches de configuration de ces équipements. Elle n'a pas vocation à être un guide technique de configuration des commutateurs.



Chaque SI étant unique, il est nécessaire d'adapter les configurations données en exemple dans ce document aux particularités du SI considéré et aux modèles d'équipements utilisés. Une copie telles quelles des lignes de commande, sans compréhension préalable de leur impact sur le fonctionnement des équipements, peut conduire à des indisponibilités du SI.

Les hypothèses suivantes ont été faites lors de la rédaction de cette note :

- seules les personnes autorisées disposent d'un accès physique aux commutateurs ;
- les problématiques de câblage physique entre les commutateurs et les équipements ou prises réseau ne sont pas abordées ;
- les commandes données en exemple sont adaptées aux commutateurs des marques Cisco (modèle Catalyst 2960, système d'exploitation IOS Version 15.0(2)SE9 LAN Base) et HP (modèle A5500 JD377A, système d'exploitation Comware version 5.20.99, release 2221P08).

À noter que les recommandations faites dans ce document ciblent uniquement les commutateurs de desserte¹.

1.1 Documents de référence

Référence	Titre
[Admin SI]	Recommandations relatives à l'administration sécurisée des systèmes d'information http://www.ssi.gouv.fr/securisation-admin-si/
[NT LOG]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation http://www.ssi.gouv.fr/journalisation/
[NT MdP]	Recommandations de sécurité relatives aux mots de passe http://www.ssi.gouv.fr/mots-de-passe/
[NT SSH]	Recommandations pour un usage sécurisé d'(Open)SSH http://www.ssi.gouv.fr/nt-ssh/
[RFC 5517]	Cisco Systems' Private VLANs : Scalable Security in a Multi-Client Environment

1. Voir détails dans la section 2.

Référence	Titre
	https://tools.ietf.org/html/rfc5517

TABLE 1 – Documents de référence

1.2 Acronymes et terminologie

Nom ou sigle	Autre nom d'usage	Définition
802.1Q	802.1Q	Standard IEEE qui définit le support des VLAN sur un réseau Ethernet
802.1X	802.1X	Standard IEEE définissant une méthode de contrôle d'accès au niveau des équipements permettant d'accéder à l'infrastructure réseau
AAA	Authentication Authorization Accounting	Protocole gérant l'authentification, les autorisations et la traçabilité
ACL	Access Control List	Mécanisme de contrôle d'accès basé sur un filtrage généralement effectué au niveau des adresses IP
AppleTalk Remote Access	AppleTalk Remote Access	Protocole propriétaire Apple d'accès à distance
ARP	Address Resolution Protocol	Protocole de résolution d'adresse permettant de faire le lien entre les adresses de niveau 3 (IP) et de niveau 2 (MAC)
AUX	Auxiliary line	Ligne console auxiliaire (ligne physique) correspondant à un port physique asynchrone
BPDU	Bridge Protocol Data Unit	Trames Spanning Tree échangées entre les commutateurs afin de définir un arbre réseau sans boucle
CDP	Cisco Discovery Protocol	Protocole propriétaire Cisco de découverte du voisinage réseau
CLI	Command Line Interface	Interface en ligne de commande
CTY	Console line	Ligne console (ligne physique)
DHCP	Dynamic Host Configuration Protocol	Protocole réseau configurant notamment les paramètres IP d'une machine
DNS	Domain Name System	Système de résolution de noms
DTP	Dynamic Trunking Protocol	Protocole propriétaire Cisco permettant de négocier dynamiquement le mode (<i>trunk</i> ou <i>access</i>) d'un lien reliant un port du commutateur à l'équipement situé à l'autre bout du câble
GVRP	GARP VLAN Registration Protocol	Protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur un parc de commutateurs de manière dynamique
HTTP	Hypertext Transfer Protocol	Protocole de communication client-serveur utilisé pour l'affichage des pages web

Nom ou sigle	Autre nom d'usage	Définition
HTTPS	Hypertext Transfer Protocol Secure	Version sécurisée avec TLS du protocole HTTP
IEEE	Institute of Electrical and Electronics Engineers	Association professionnelle qui établit et publie des standards
IGC	Infrastructure de gestion de clés	Ensemble des moyens matériels, organisationnels et humains permettant de gérer des certificats électroniques durant tout leur cycle de vie
IGMP	Internet Group Management Protocol	Protocole permettant la gestion des groupes multicast
LACP	Link Aggregation Control Protocol	Protocole de niveau 2 permettant d'agréger plusieurs liens physiques sous la forme d'un lien logique
MCO	Maintien en condition opérationnelle	Ensemble des mesures prises pour garantir un certain niveau de service du système d'information en cas de dégradation de l'environnement
MCS	Maintien en condition de sécurité	Ensemble des mesures prises pour garantir la gestion maîtrisée des risques liés à la sécurité du système d'information
MIB-2	MIB-2	Branche de la MIB (Management Information Base) utilisée par la majorité des équipements réseau
MSTP	Multiple Spanning Tree Protocol	Evolution du protocole STP
MVRP	Multiple VLAN Registration Protocol	Protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur un parc de commutateurs de manière dynamique
NTP	Network Time Protocol	Protocole permettant de synchroniser l'horloge d'une machine sur une autre
PSSI	Politique de sécurité du système d'information	Plan d'action définissant les conditions à respecter pour le maintien en conditions de sécurité du SI
PPP	Point-to-Point Protocol	Protocole de transmission de niveau 2 permettant d'établir des liaisons de type point à point
PVST	Per VLAN Spanning Tree	Évolution (propriété Cisco) du protocole STP
RADIUS	Remote Authentication Dial-In User Service	Protocole permettant de mettre en place des mécanismes d'authentification centralisés
RGS	Référentiel général de sécurité	Recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information destiné principalement aux autorités administratives qui proposent des services en ligne aux usagers
RPVST	Rapid PVST	Évolution du protocole PVST

Nom ou sigle	Autre nom d'usage	Définition
SI	Système d'information	Ensemble des moyens matériels et logiciels permettant de gérer et traiter de l'information dans un périmètre donné
SLIP	Serial Line Internet Protocol	Protocole de liaison en série qui encapsule le protocole IP
SNMP	Simple Network Management Protocol	Protocole de gestion et de supervision d'équipements
STP	Spanning Tree Protocol	Protocole permettant de déterminer une topologie réseau de niveau 2 sans boucle
SSH	Secure Shell	Protocole sécurisé d'accès à distance à l'interface en ligne de commande d'équipements
syslog	syslog	Protocole de journalisation
TACACS+	Terminal Access Controller Access-Control System	Protocole permettant de mettre en place des mécanismes d'authentification centralisés
TTL	Time To Live	Compteur placé dans l'entête des datagrammes IP indiquant le nombre maximal de routeurs de transit avant que le paquet ne soit défaussé
TTY	Teletype	Ligne console (ligne physique) semblable à la ligne auxiliaire
VLAN	Virtual Local Area Network	LAN virtuel
VTP	VLAN Trunking Protocol	Protocole propriétaire Cisco de niveau 2 utilisé pour configurer et administrer les VLAN sur un parc de commutateurs de manière dynamique
VTY	Virtual Teletype	Ligne virtuelle accessible par les ports synchrones
XRemote	XRemote	Protocole permettant le support de l'environnement graphique X sur un lien de communication en série

TABLE 2 – Acronymes et terminologie

2 Les commutateurs dans le système d'information

Comme mentionné en préambule, les commutateurs sont des équipements de transit pour une quantité importante d'informations. Il convient donc de porter une attention toute particulière à leur niveau de robustesse face à des attaques venant du réseau. Ces équipements n'ont pas tous le même rôle dans un SI. Afin de bien appréhender les menaces auxquelles ceux-ci sont exposés, il est utile de distinguer les différents types de commutateurs d'un SI selon trois catégories :

- **les commutateurs de desserte ou d'accès** : ce sont les équipements directement reliés aux prises réseau auxquelles se connectent les terminaux du SI (postes bureautique, téléphones IP, etc.) ;
- **les commutateurs de distribution** : ils regroupent le trafic venant des commutateurs de desserte afin de transmettre les données vers les équipements du cœur de réseau comme les commutateurs de cœur de réseau ou les routeurs ;
- **les commutateurs de cœur de réseau** : ils sont directement reliés aux serveurs, aux commutateurs de distribution ou aux routeurs. Ils sont situés généralement au cœur du réseau

ou à l'intérieur des centres de données.

Ces trois types se différencient principalement par leur contexte d'utilisation, leurs caractéristiques techniques en matière de capacité de traitement et de débit, les types de ports (Ethernet, fibre, etc.) et leur nombre, etc.

Le schéma ci-dessous représente un exemple de répartition de ces différents types de commutateurs au sein d'un SI :

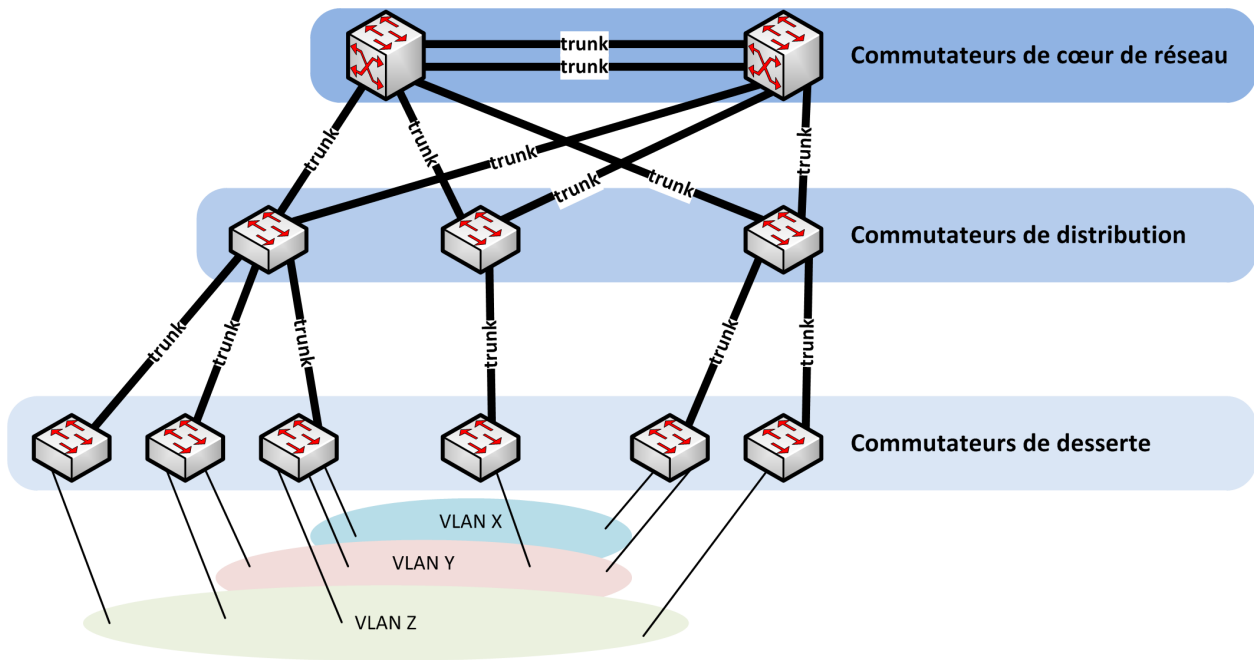


FIGURE 1 – Différents types de commutateurs au sein d'un SI

Dans la suite de ce document, seules les bonnes pratiques de sécurisation relatives aux commutateurs de desserte sont détaillées. Il est cependant possible de prendre en exemple certaines de ces pratiques et de les adapter aux autres types de commutateurs.

3 Interface en ligne de commande

L'administration des commutateurs se fait généralement via une interface de configuration appelée **CLI**. Celle-ci présente un affichage semblable aux interfaces en ligne de commande intégrées aux systèmes d'exploitation Microsoft, Unix ou dérivés. L'invite de commande, affichée en début de chaque ligne de commande, indique à l'administrateur de l'équipement dans quel mode de commande celui-ci se trouve. Pour rappel, voici les principaux modes de commande d'un commutateur Cisco :

Invite de commande	Signification
Switch>	Mode utilisateur
Switch#	Mode privilégié
Switch(config)#	Mode de configuration global
Switch(config-if)#	Mode de configuration d'une interface
Switch(config-vlan)#	Mode de configuration d'un VLAN

TABLE 3 – Modes de commande d'un commutateur Cisco

Chaque bloc de lignes de commande destiné à configurer un équipement Cisco est présenté dans ce document de la manière suivante :

Exemple Cisco IOS

```
! Commentaire  
Switch(config)# commande de configuration <variable-à-renseigner>
```

Pour un commutateur HP, les principaux modes de commande sont :

Invite de commande	Signification
<Switch>	Mode utilisateur
[Switch]	Mode privilégié et de configuration global
[Switch-GigabitEthernetX/X/X]	Mode de configuration d'une interface
[Switch-vlanXXXX]	Mode de configuration d'un VLAN

TABLE 4 – Modes de commande d'un commutateur HP

Chaque bloc de lignes de commande destiné à configurer un équipement HP est présenté dans ce document de la manière suivante :

Exemple HP Comware 5

```
# Commentaire  
[Switch] commande de configuration <variable-à-renseigner>
```

Les exemples illustrant ce document sont donnés, dans la mesure du possible, pour les commutateurs de type Cisco IOS et HP Comware.

4 Administration

Comme tout équipement réseau déployé dans un SI, l'administration des commutateurs doit se faire en respectant un certain nombre de recommandations de sécurité détaillées dans la note technique [\[Admin SI\]](#) de l'ANSSI relative à l'administration sécurisée des SI.

4.1 Réseau d'administration *out-of-band*

Pour des questions de sécurité, il est conseillé de mettre en place un réseau dédié aux flux d'administration des équipements du SI (hors terminaux), distinct des réseaux de données utilisés par les services métier.

4.1.1 Port physique dédié

Il est préférable d'utiliser un port physique dédié à l'administration d'un commutateur lorsque cela est possible afin de ne pas mélanger les flux de gestion et les flux métier. Cette pratique paraît d'autant plus aisée à réaliser que les commutateurs disposent en général d'un nombre important de ports physiques.

R1

Dédier une interface physique du commutateur à son administration.

4.1.2 Réseau dédié

Afin de procéder à une séparation entre le réseau d'administration du commutateur et les autres réseaux, plusieurs techniques peuvent être mises en œuvre. La méthode idéale consiste à utiliser un réseau physique dédié. Cependant, si cela n'est pas possible, l'utilisation d'un VLAN dédié à l'administration peut être une solution acceptable, mais elle dégrade le niveau de sécurité en comparaison de la première solution.

R2

Mettre en place une séparation physique entre les réseaux d'administration et les réseaux métier.

R2-

Au minimum, prévoir un cloisonnement logique utilisant des VLAN pour appliquer cette séparation. On pourra se reporter à la note technique [\[Admin SI\]](#) sur ce point.

Pour des explications plus approfondies sur les VLAN, se référer à la section 5.

4.2 Accès à l'administration du commutateur

Il existe deux types de lignes de terminaux : les lignes physiques et les lignes virtuelles. Les lignes physiques sont rattachées à des interfaces physiques asynchrones, chaque ligne étant associée à une interface. Les lignes virtuelles ne sont quant à elles pas rattachées à une interface physique en particulier, plusieurs d'entre elles peuvent être utilisées simultanément sur une même interface physique. Ainsi, par exemple, plusieurs connexions [SSH](#) peuvent être établies au même moment sur une interface physique synchrone (par exemple Ethernet ou série).

Il existe 4 types de lignes de terminaux :

- **CTY** : la ligne console (ligne physique). C'est elle qui est utilisée lorsqu'un administrateur réseau se connecte au port console avec un câble console ;
- **VTY** : les lignes virtuelles (en général 16 lignes, de 0 à 15) accessibles par les ports synchrones (par exemple Ethernet ou série) ;
- **AUX** : une ligne physique correspondant à un port physique asynchrone. Lorsqu'elle est utilisée, c'est généralement pour accéder au commutateur à distance en utilisant un modem ;
- **TTY** : une ligne physique semblable à la ligne auxiliaire. Elle permet l'accès à distance par certains protocoles comme [SLIP](#), [PPP](#), [AppleTalk Remote Access](#) et [XRemote](#).

Dans cette sous-section, seules les lignes de terminaux du commutateur les plus utilisés (CTY et VTY) sont traitées. Dans le cas des lignes AUX et TTY, se référer à la documentation du constructeur en prenant en exemple les mesures de sécurité détaillées dans cette sous-section.

4.2.1 Port console (CTY - ligne console)

Le port console d'un commutateur ne doit jamais être désactivé car c'est l'unique moyen de reprendre la main sur l'équipement en cas de problème dans sa configuration sans avoir à le réinitialiser

en configuration usine.

R3

Ne pas désactiver le port console des commutateurs.

Lorsque l'affichage des événements système est activé sur le commutateur (comportement par défaut), ceux-ci peuvent gêner l'administrateur dans son travail en affichant les événements au milieu des commandes qu'il entre. La commande donnée en exemple ci-dessous permet d'éviter cela, les événements s'affichant alors sur une ligne différente de celle en cours d'écriture par l'administrateur :

Exemple Cisco IOS

```
! Configuration de la ligne console
Switch(config)# line console 0

! Affiche les événements système sur une ligne différente de la ligne de commande
! en cours de saisie
Switch(config-line)# logging synchronous

! Ferme automatiquement la session sur la ligne console après une période
! d'inactivité de 15 minutes
Switch(config-line)# exec-timeout 15
```

Exemple HP Comware 5

```
# Affiche les événements système sur une ligne différente de la ligne de commande
# en cours de saisie
[Switch]info-center synchronous

# Configuration de la ligne console
[Switch]user-interface aux 0

# Ferme automatiquement la session sur la ligne console après une période
# d'inactivité de 15 minutes
[Switch-ui-aux0]idle-timeout 15
```

4.2.2 Port Ethernet (VTY - ligne virtuelle)

Les lignes virtuelles sont généralement utilisées pour accéder à distance aux commutateurs en SSH. Le protocole Telnet est encore utilisé sur les équipements obsolètes, mais pour des raisons de sécurité détaillées plus loin, il est à proscrire dès qu'un commutateur supporte SSH.

4.2.2.1 SSH

SSH est un protocole sécurisé d'accès à distance à l'interface en ligne de commande d'équipements. C'est un protocole éprouvé d'administration à distance des équipements. Il existe deux versions du protocole, à savoir les versions 1 et 2. Seule la version 2 est recommandée, la version 1 étant sujette à une faille protocolaire connue et facilement exploitable par une personne malveillante.

R4

Utiliser le protocole SSH en version 2 pour l'administration à distance des commutateurs.

R5

La configuration doit respecter les recommandations cryptographiques détaillées dans l'annexe B du [RGS](#).

Concernant les recommandations de sécurité pour la mise en œuvre du protocole SSH, il est aussi possible de se référer à la note technique [\[NT SSH\]](#) de l'ANSSI traitant des recommandations pour un usage sécurisé d'(Open)SSH.

Ci-dessous est détaillée en exemple la configuration du serveur SSH d'un commutateur :

Exemple Cisco IOS

```
! Configure le nom d'hôte du commutateur (préalable nécessaire à l'activation de SSH)
Switch(config)# hostname <Switch>

! Génère une bi-clé RSA de 2048 bits nommée <ssh-rsa-keypair>
Switch(config)# crypto key generate rsa usage-keys label <ssh-rsa-keypair> modulus 2048

! Sélectionne la bi-clé devant être utilisée pour SSH
Switch(config)# ip ssh rsa keypair-name <ssh-rsa-keypair>

! Force le serveur SSH à utiliser la version 2 du protocole
Switch(config)# ip ssh version 2

! Définit le groupe Diffie-Hellman à utiliser lors de l'échange de clés (groupe 14)
Switch(config)# ip ssh dh min size 2048

! Active SCP pour la copie de fichiers sécurisée à travers SSH
Switch(config)# ip scp server enable

! Force l'utilisation du SSH et désactive le Telnet
Switch(config)# line vty 0 15
Switch(config-line)# transport input ssh

! Ferme automatiquement la session sur la ligne VTY après une période d'inactivité de
! 15 minutes
Switch(config-line)# exec-timeout 15
Switch(config-line)# exit

! Ferme automatiquement les connexions SSH entrantes dont la liaison est coupée
Switch(config)# service tcp-keepalives-in

! Active la journalisation des connexions SSH
Switch(config)# ip ssh logging events
```

Exemple HP Comware 5

```
# Configure le nom d'hôte du commutateur
[Switch]sysname Switch

# Génère une bi-clé RSA de 2048 bits
[Switch]public-key local create rsa
[Switch]2048

# Démarre le serveur SSH et le force à utiliser la version 2 du protocole
[Switch]ssh server enable
[Switch]undo ssh server compatible-ssh1x

# Active l'écoute sur le port TCP 22 pour le service SSH
[Switch]user-interface vty 0 15
[Switch-ui-vty0-15]authentication-mode scheme
[Switch-ui-vty0-15]protocol inbound ssh

# Telnet est désactivé par défaut
# Ferme automatiquement la session sur la ligne VTY après une période d'inactivité de
# 15 minutes
[Switch-ui-vty0-15]idle-timeout 15
```

Afin de répondre à certains besoins opérationnels, il est possible de mettre en place une authentification par clé publique. Cette méthode d'authentification ne peut cependant fonctionner que pour l'authentification avec un compte local. Pour plus d'informations concernant les types de comptes, se référer au paragraphe 4.3.3.



Pour que l'authentification par clé publique fonctionne, le compte pour lequel est renseignée la clé publique doit être créé parmi les comptes locaux du commutateur.

Ci-dessous est donné en exemple l'ajout de la clé publique d'un administrateur dans le magasin d'un commutateur afin qu'il puisse s'y authentifier par clé publique :

Exemple Cisco IOS

```
! Entre dans le menu de gestion des comptes avec authentification par clé publique
Switch(config)# ip ssh pubkey-chain

! Sélectionne le compte localaccount
Switch(conf-ssh-pubkey)# username <localaccount>

! Entre dans le menu de saisie de la clé publique associée au compte
Switch(conf-ssh-pubkey-user)# key-string
Switch(conf-ssh-pubkey-data)# <copier la clé publique par bloc de 254 caractères maximum
en validant chaque étape par Entrée>
Switch(conf-ssh-pubkey-data)# exit
Switch(conf-ssh-pubkey-user)# exit
Switch(conf-ssh-pubkey)# exit
```

Exemple HP Comware 5

```
# Copie la clé publique de l'utilisateur sur le commutateur
user@poste-admin:~$ scp <.ssh/localaccount-key.pub>
<localadmin>@<switch-ip-address>:/<localaccount-key.pub>

# Importe la clé publique de l'utilisateur
[Switch]public-key peer <localaccount-key> import sshkey flash:/<localaccount-key.pub>

# Associe l'utilisateur à la clé publique importée
[Switch]ssh user <localaccount> service-type scp authentication-type publickey assign
publickey <localaccount-key> work-directory flash:/

# Il est alors possible de télécharger un fichier présent sur le commutateur,
# mais il n'est pas possible de s'y connecter en SSH
# Pour pouvoir se connecter en SSH, remplacer scp par all.

# Commandes nécessaires :
## pour pouvoir téléverser des fichiers sur le commutateur
## pour que les administrateurs connectés en SSH puissent pouvoir acquérir les droits
priviliégiés
[Switch]user-interface vty 0 15
[Switch-ui-vty0-15]user privilege level 3
[Switch-ui-vty0-15]quit
```



Sur les commutateurs HP, la commande `user privilege level 3` dans le menu `local-user <localaccount>` ne s'applique qu'aux utilisateurs locaux qui se connectent par « login/password ». Ainsi, pour que des administrateurs puissent obtenir les droits privilégiés lors de la connexion au commutateur par clé publique, il est nécessaire d'appliquer la commande de configuration `user privilege level 3` aux lignes VTY ; cela définit le niveau de privilège par défaut des utilisateurs qui se connectent en utilisant ces lignes. Lors d'une connexion par « login/password », le niveau de privilège du menu `local-user <localaccount>` prend le dessus sur le menu `user-interface vty 0 15`.

4.2.2.2 HTTP/HTTPS

De nombreux modèles de commutateur embarquent un serveur [HTTP](#) offrant aux administrateurs réseau la possibilité de configurer ces équipements via une interface web. Même si cette fonctionnalité permet de configurer un commutateur sans avoir recours à l'interface en ligne de commandes, cette dernière se révèle plus adaptée à une gestion industrialisée des parcs de commutateurs. De plus, la présence d'un serveur web augmente la surface d'attaque de l'équipement et peut nuire à ses performances, il est donc recommandé de le désactiver.

R6

Désactiver le serveur web de gestion du commutateur, que ce soit en version sécurisée ([HTTPS](#)) ou non ([HTTP](#)).

Exemple de commandes de désactivation des serveurs HTTP et HTTPS :

Exemple Cisco IOS

```
! Désactive le serveur HTTP
Switch(config)# no ip http server

! Désactive le serveur HTTPS
Switch(config)# no ip http secure-server
```

Exemple HP Comware 5

```
# Désactive le serveur HTTP
[Switch]undo ip http enable

# Désactive le serveur HTTPS
[Switch]undo ip https enable
```

Les commutateurs créent généralement des certificats par défaut, notamment un certificat utilisé par le serveur HTTPS. Ce dernier doit être supprimé une fois que le serveur a été désactivé.

R7

Supprimer les certificats créés par défaut sur le commutateur.

Exemple de commande pour la suppression du certificat utilisé par le serveur HTTPS :

Exemple Cisco IOS

```
! Supprime le certificat créé par défaut pour le serveur HTTPS
Switch(config)# no crypto pki trustpoint <TP-self-signed-123456789>
```


4.2.2.3 Telnet

Telnet est un protocole non sécurisé permettant l'accès à distance à des équipements. Étant donné que toutes les informations sont envoyées en clair sur le réseau, notamment le mot de passe de l'administrateur (sauf si Telnet est couplé à d'autres mécanismes de sécurité), ce protocole est à proscrire sur les matériels supportant des protocoles d'administration sécurisés comme SSH.

R8

Ne pas utiliser le protocole Telnet pour l'administration à distance des commutateurs lorsque des protocoles plus sécurisés sont supportés par l'équipement.

R8-

Si Telnet doit être utilisé du fait de l'absence de protocoles sécurisés, mettre en place les moyens adéquats de sécurisation du réseau sur lequel vont transiter ces flux.



Dans le cas où il n'est pas possible de se passer de Telnet pour administrer les commutateurs, se référer à la note technique [\[Admin SI\]](#) de l'ANSSI relative à l'administration sécurisée des SI.

Le paragraphe [4.2.2.1](#) détaille comment désactiver le protocole Telnet.

4.2.2.4 Limitation de l'accès à l'interface d'administration

Il est possible d'attribuer plusieurs adresses IP à un commutateur. Néanmoins, ceci n'est pas nécessaire et peut causer des problèmes de sécurité, comme par exemple exposer l'interface d'administration du commutateur aux postes bureautiques. Il faut donc veiller à ne configurer qu'une seule adresse IP répondant aux seuls besoins d'administration de l'équipement, réduisant ainsi sa surface d'attaque.

R9

Un commutateur ne doit disposer que d'une seule adresse IP dédiée à son administration.

Enfin, il est commun de limiter au niveau d'un commutateur l'accès à son interface d'administration par l'utilisation des [ACL](#), mécanisme complexe à maintenir au sein d'un SI. La mesure à privilégier est donc d'opérer un filtrage des flux au niveau des pare-feux présents dans le SI et, quand cela n'est pas possible, d'utiliser des ACL.

R10

Prendre les mesures nécessaires au sein du SI afin de n'autoriser l'accès à l'interface d'administration des commutateurs qu'aux administrateurs, notamment par l'utilisation de filtrage au niveau des pare-feux.

R10-

Si cela n'est pas possible, la mise en place des ACL sur le commutateur peut être envisagée en tant que mesure palliative.

4.2.3 Journalisation des authentifications

Il est important de journaliser les accès et tentatives d'accès à l'administration des commutateurs, et ce dans une optique de détection d'intrusion et d'imputabilité.

R11

Activer la journalisation des authentifications et tentatives d'authentification.

Exemple de commandes pour activer la journalisation des authentifications :

Exemple Cisco IOS

```
! Active la journalisation des authentifications
Switch(config)# login on-failure log
Switch(config)# login on-success log
```



La description d'un protocole équivalent n'a pas été trouvée dans la documentation du commutateur HP.

4.2.4 Protection contre l'attaque par force brute

Afin de protéger un commutateur contre une attaque par force brute², il est possible de mettre en place des mécanismes de protection.

R12

Mettre en place des contre-mesures pour protéger le commutateur des attaques de type force brute.

Exemple de commandes servant à la protection contre l'attaque par force brute :

Exemple Cisco IOS

```
! Interdit les tentatives d'authentification pendant 5 minutes si 3 erreurs
! d'authentification ont lieu en 2 minutes
Switch(config)# login block-for 300 attempts 3 within 120

! Définit le temps d'attente minimum en secondes entre deux tentatives d'authentification
Switch(config)# login delay 2
```

Sur les commutateurs HP, *password control* est un ensemble de fonctions fournies par le service d'authentification local permettant d'améliorer la sécurité du système. Certaines fonctions deviennent actives directement lors de l'exécution de la commande générale d'activation du *password control*, comme le masquage des mots de passe lors de l'affichage de la commande *display current-configuration*, tandis que d'autres sont à configurer par la suite pour être actives.

2. Attaque consistant à tester l'exhaustivité des couples identifiant/mot de passe avec pour but la pénétration d'un système.

Exemple HP Comware 5

```
# Active le password control
[Switch]password-control enable

# Interdit les tentatives d'authentification pendant 5 minutes si 3 erreurs
# d'authentification ont lieu d'affilée
[Switch]password-control login-attempt 3 exceed lock-time 5
```

4.3 Gestion des comptes utilisateur

La gestion des comptes des personnes administrant les commutateurs fait partie des points d'attention les plus critiques pour la sécurité du SI. En effet, une gestion laxiste de ces comptes et des droits associés a généralement pour conséquence qu'il est impossible d'imputer des dysfonctionnements importants ou de graves lacunes de sécurité à quelque personne que ce soit.

Pour commencer, l'utilisation des comptes nominatifs doit être généralisée. En effet, l'utilisation de ce type de compte permet de tracer efficacement les actions du personnel qui administre les équipements tout en facilitant leur gestion, notamment pour les mots de passe.

R13

Généraliser l'utilisation des comptes nominatifs.



Une exception peut être faite pour le compte local d'administration « de secours » de l'équipement dont la nature est abordée au paragraphe 4.3.3.

R13-

Dans des cas d'administration très particuliers qui ne permettent pas de se passer des comptes non nominatifs, respecter des conditions d'emploi strictes et adaptées au contexte.

Pour parvenir à mettre en place une gestion cohérente des comptes utilisateur des commutateurs, il est nécessaire de commencer par comprendre les différents types de compte qui existent, puis de suivre les recommandations présentées ci-après.

4.3.1 Niveau de privilège

Les commutateurs permettent de restreindre les accès de comptes utilisateur cibles à certaines de leurs fonctionnalités. Dans le cas des commutateurs Cisco par exemple, il est possible d'avoir une granularité allant du niveau 1 (compte non privilégié) au niveau 15 (compte administrateur avec des droits privilégiés). Se limiter à ces deux types de compte suffit dans la majorité des cas et utiliser les niveaux intermédiaires³ complexifie la gestion des droits des utilisateurs. Néanmoins, certains besoins bien identifiés peuvent nécessiter l'usage des niveaux de privilège intermédiaires.

3. Comptes dont les droits sont définis sur mesure. Par exemple un compte utilisateur sans privilèges auquel le droit d'exécuter certaines commandes privilégiées a été attribué.

Le niveau 15 des commutateurs Cisco correspond au niveau 3 des commutateurs HP, le principe de fonctionnement restant le même.

R14

Se limiter à l'usage des niveaux de privilège « sans privilège » et « compte administrateur » est une bonne pratique tant que des besoins nécessitant l'usage d'autres niveaux de privilèges ne sont pas identifiés.

4.3.2 Accès *enable* ou *system-view*

La commande **enable** permet à un utilisateur de n'importe quel niveau (dans la configuration par défaut d'un commutateur) d'acquérir les droits administrateur (niveau 15 pour Cisco IOS et niveau 3 pour HP Comware) sous condition que cet utilisateur connaisse le mot de passe permettant cette action. Cette manière de fonctionner n'est pas très adaptée à la gestion des commutateurs car elle implique que tous les administrateurs réseau partagent le mot de passe *enable* (à retenir en plus de leur mot de passe personnel). La gestion d'un mot de passe partagé est de plus compliquée. Cette fonctionnalité est donc à proscrire dans le cadre de l'administration des commutateurs, contrairement à l'utilisation des comptes administrateurs (niveau 15 ou 3 selon l'équipement) nominatifs.

R15

La fonctionnalité *enable* doit être désactivée, l'utilisation de comptes administrateurs nominatifs rend cette fonctionnalité superflue.

La restriction de la commande *enable* se fait de la manière suivante pour un commutateur Cisco :

Exemple Cisco IOS

```
! Interdit l'utilisation de la commande enable
Switch(config)# privilege exec level 15 enable
```



Il est nécessaire de vérifier au préalable qu'il est effectivement possible de se connecter au commutateur avec un compte de niveau 15.



Sur les commutateurs HP, l'équivalent de la commande **enable** de Cisco est la commande **system-view**. Le fonctionnement est cependant légèrement différent. Si sur les commutateurs Cisco un administrateur qui se connecte est directement en mode privilégié, un administrateur qui se connecte sur un commutateur HP y accède dans un premier temps en mode non privilégié ; il doit alors exécuter la commande **system-view** pour obtenir les droits privilégiés. Cette commande ne nécessite toutefois pas de mot de passe.

4.3.3 Comptes locaux et comptes centralisés

Les comptes utilisateur sont de deux sortes :

- **les comptes locaux** : gérés dans la configuration locale du commutateur ;
- **les comptes centralisés** : gérés dans un annuaire du SI.

L'utilisation de comptes centralisés est la méthode d'administration à privilégier. En effet, la gestion des comptes locaux se révèle très lourde dès lors que le nombre d'administrateurs ou d'équipements du SI devient conséquent. Les services d'authentification utilisant des comptes centralisés permettent aussi une meilleure traçabilité des modifications apportées aux configurations des équipements.

Dans l'idéal, un compte utilisateur nominatif est créé dans l'annuaire central pour chaque personne physique ; ce sont ces comptes que vont utiliser les administrateurs pour effectuer leurs tâches d'administration quotidiennes. Puis, sur chaque commutateur, un compte administrateur local non nominatif, qui peut par exemple être nommé « localadmin », est créé. Celui-ci n'est utilisé qu'en cas d'opérations d'administration spécifiques et exceptionnelles, c'est un compte d'administration « de secours ». Le mot de passe de ce compte doit être inscrit dans un fichier stocké de manière sécurisée uniquement accessible des administrateurs ayant le besoin d'en connaître, potentiellement hors ligne. Étant donné qu'il s'agit d'un mot de passe à privilèges, il est fortement conseillé d'appliquer les recommandations issues de la note technique [NT MdP] de l'ANSSI relative à la sécurité des mots de passe, qui recommande notamment l'utilisation d'un mot de passe différent pour chaque équipement.

Comme évoqué précédemment, l'utilisation de comptes nominatifs permet facilement d'imputer des actions à des personnes physiques. La gestion de ces comptes de manière centralisée permet alors de gérer les comptes utilisateurs de façon optimale.

R16

Centraliser les comptes dans un ou plusieurs annuaires présents sur le système d'information (plutôt que de les gérer localement sur chaque commutateur) à l'exception d'un compte local d'administration « de secours ».

Il est par ailleurs recommandé d'utiliser un ou plusieurs annuaires dédiés aux comptes d'administration du SI, comme expliqué dans la note technique [Admin SI] de l'ANSSI relative à l'administration sécurisée des SI.

4.3.3.1 Gestion des comptes locaux

Sur les commutateurs de la marque Cisco, plusieurs types⁴ de mots de passe peuvent être utilisés mais ils n'offrent pas la même robustesse, celui offrant la meilleure robustesse à ce jour étant le type 5 (hash md5 salé). Certains commutateurs utilisent par défaut le type 4 et ne peuvent pas générer le hash des mots de passe au format du type 5, mais ils acceptent cependant d'utiliser des hashes de type 5 générés par un équipement tiers.

Le type 5 stocke le hash MD5 du mot de passe du compte utilisateur. Il permet ainsi de masquer les mots de passe utilisateurs des comptes locaux (affichés dans le fichier de configuration du commutateur) aux personnes indiscreètes. Cela ne garantit cependant pas que ces mots de passe ne puissent être retrouvés par une personne malveillante utilisant des attaques de type force brute par dictionnaire sur

4. Le type indique la méthode de hashage du mot de passe utilisée pour le stocker.

un fichier de configuration qu'il aurait récupéré.

R17

Protéger les fichiers de configuration contenant des mots de passe, ceux-ci étant soit stockés en clair, soit retrouvables facilement par une personne malveillante. Supprimer les mots de passe des fichiers de configuration en cas de partage de ces fichiers avec d'autres personnes ou entités.

Exemple de procédure pour la configuration d'un compte local d'administration pour un commutateur utilisant le type 5 par défaut :

Exemple Cisco IOS

```
! Crée le compte "localadmin", compte d'administration local
Switch(config)# username localadmin privilege 15 secret <mot-de-passe-complexe>
```

Exemple de procédure pour la configuration d'un compte local d'administration pour un commutateur utilisant le type 4 par défaut :

- génération du hash du mot de passe (sur le poste d'administration) :

```
# Génère le hash du mot de passe de l'utilisateur créé dans l'étape suivante
user@poste-admin:~> openssl passwd -salt 'openssl rand -base64 3' -1
<mot-de-passe-complexe>
```

- création du compte local d'administration :

Exemple Cisco IOS

```
! Crée le compte "localadmin", compte d'administration local en utilisant le hash du mot
! de passe généré à l'étape précédente
Switch(config)# username localadmin privilege 15 secret 5 <hash-du-mot-de-passe-complexe>
```

Il est possible de vérifier le type utilisé pour stocker un mot de passe local en utilisant la commande suivante :

Exemple Cisco IOS

```
! Affiche les lignes commençant par username
Switch(config)# show running-config | include ^username
```

Dans le résultat de cette commande, le chiffre après l'attribut « secret » indique le type qui a été utilisé pour stocker le mot de passe.

Exemple HP Comware 5

```
# Crée le compte "localadmin", compte d'administration local
[Switch]local-user localadmin

# Active le password control
[Switch]password-control enable

# Définit le mot de passe de l'utilisateur
[Switch-luser-localadmin]password
(renseigner le mot de passe et le confirmer)

# Donne au compte les droits administrateur
[Switch-luser-localadmin]authorization-attribute level 3

# Autorise l'utilisateur à se connecter à son compte par la console
[Switch-luser-localadmin]service-type terminal

# Autorise l'utilisateur à se connecter à son compte à distance par SSH
[Switch-luser-localadmin]service-type ssh
```

4.3.4 Désactivation/suppression des comptes par défaut

Certains commutateurs sont préconfigurés en usine avec des comptes par défaut. Afin d'éviter leur utilisation par des personnes malintentionnées, il est nécessaire de les supprimer, ou à défaut, de les désactiver. Ne pas oublier toutefois de conserver un compte administrateur local « de secours » sur le commutateur afin de pouvoir l'administrer en dernier recours par la suite.

R18

Supprimer les comptes par défaut - au minimum, les désactiver - tout en veillant à conserver au moins un compte administrateur local « de secours ».

4.4 Contrôle d'accès

Il existe deux façons d'effectuer un contrôle d'accès sur les commutateurs :

- **le contrôle d'accès local** : le commutateur compare le couple nom d'utilisateur/mot de passe saisi avec le contenu de sa configuration afin d'autoriser ou non l'accès à son interface d'administration par ligne de commande avec les droits associés à ce compte ;
- **le contrôle d'accès distant** : le commutateur interroge un service d'authentification distant reposant sur un annuaire.

Le contrôle d'accès distant est de loin la méthode à privilégier pour les connexions sur toutes les lignes (y compris console), car elle permet non seulement de s'appuyer sur une gestion centralisée des comptes utilisateurs, mais aussi de conserver une traçabilité des demandes d'accès directement au niveau du service de contrôle d'accès.

R19

L'utilisation d'un moyen de contrôle d'accès distant reposant sur un annuaire présent sur le système d'information doit être mis en place pour les connexions au commutateur sur toutes les lignes (y compris console).

R20

L'authentification locale ne doit être autorisée que pour le compte local d'administration.

Il existe un certain nombre de protocoles de contrôle d'accès à distance reposant sur un annuaire, appelés protocoles AAA. Ces protocoles permettent, en plus de gérer l'authentification des utilisateurs et l'attribution de leurs droits (autorisations), de tracer les authentifications et les commandes entrées par les utilisateurs dans un but d'imputabilité.

Les bonnes pratiques de configuration des deux protocoles AAA les plus fréquemment retrouvés dans les commutateurs (à savoir RADIUS et TACACS+) sont décrites dans les paragraphes suivants. Il faut toutefois noter que le protocole TACACS+ est plus fiable et plus sécurisé que le protocole RADIUS, notamment sur les points suivants :

- il utilise TCP, alors que RADIUS repose sur UDP ;
- les paquets sont entièrement chiffrés entre le client et le serveur alors que concernant RADIUS, seul le mot de passe présenté par le client au serveur est chiffré⁵ ;

5. Les algorithmes employés dans les deux solutions ne sont cependant pas conformes au RGS.

- il est possible de n'autoriser l'exécution de certaines commandes qu'à certains utilisateurs de façon précise ;
- l'authentification et les autorisations peuvent être dissociées sur deux serveurs différents.

R21

Préférer l'utilisation de TACACS+ à RADIUS.

L'exemple ci-dessous détaille la configuration de base du contrôle d'accès tel que décrit dans ce paragraphe (les détails propres à RADIUS et TACACS+ sont donnés dans les paragraphes suivants) :

Exemple Cisco IOS

```
! Active AAA
Switch(config)# aaa new-model

! Configuration des méthodes d'authentification et d'autorisation utilisées par défaut

!! Crée la liste d'authentification par défaut (celle-ci détaille les méthodes
!! d'authentification utilisées successivement, ici tacacs+ puis local
!! dans le cas où le serveur tacacs+ n'est pas accessible)
Switch(config)# aaa authentication login default group tacacs+ local

!! Crée la liste d'autorisation par défaut (celle-ci détaille les méthodes
!! d'autorisation utilisées successivement, ici tacacs+ puis local
!! dans le cas où le serveur tacacs+ n'est pas accessible)
Switch(config)# aaa authorization exec default group tacacs+ local

! Configuration des méthodes d'authentification et d'autorisation pour le port console
Switch(config)# aaa authorization console
Switch(config)# line console 0
Switch(config-line)# login authentication default
Switch(config-line)# authorization exec default
```

Exemple HP Comware 5

```
# Active AAA
[Switch]user-interface vty 0 15
[Switch-ui-vty0-15]authentication-mode scheme

# Active journalisation des commandes
[Switch-ui-vty0-15]command accounting

# Donne l'autorisation d'être en system-view
[Switch-ui-vty0-15]command authorization
[Switch-ui-vty0-15]quit

# Création d'un domaine
[Switch]domain <my-domain>
[Switch-isp-my-domain]quit

# Définition du domaine par défaut
[Switch]domain default enable <my-domain>

# Configure la ligne console pour accepter uniquement les authentifications
# sur les comptes locaux
[Switch]user-interface aux 0
[Switch-ui-aux0]authentication-mode scheme
[Switch-ui-aux0]command authorization
[Switch-ui-aux0]command accounting
[Switch-ui-aux0]quit
```

Selon les contraintes d'exploitation, il est possible d'adapter la configuration du contrôle d'accès, notamment les méthodes d'authentification et d'autorisation, ainsi que leur ordre d'emploi.

Une partie de la sécurité des protocoles RADIUS et TACACS+ repose sur l'utilisation de mots de passe. Afin de respecter les bonnes pratiques quant au choix des mots de passe, se référer à la note technique [NT M&P] de l'ANSSI relative à la sécurité des mots de passe.

4.4.1 RADIUS

Le protocole RADIUS est un protocole d'authentification distante de type AAA très fréquemment utilisé.

Ci-dessous un exemple des commandes de configuration de ce mode d'authentification :

Exemple Cisco IOS

```
! Menu de configuration du serveur radius-server-1 (rentrer ces commandes pour chaque
! serveur RADIUS à déclarer)
Switch(config)# radius server <radius-server-1>

! Configure l'adresse IP du serveur radius
Switch(config-radius-server)# address ipv4 <radius-server-ip-address> auth-port 1812
acct-port 1813

! Renseigne la clé partagée entre le commutateur et le serveur RADIUS
Switch(config-radius-server)# key <radius-secret-key>
Switch(config-radius-server)# exit

! Active la journalisation pour toutes les sessions utilisateurs possédant
! les droits exec
Switch(config)# aaa accounting exec default start-stop group radius
```

Exemple HP Comware 5

```
# Configuration RADIUS

## Création d'un schéma AAA RADIUS
[Switch]radius scheme <radius>

## Prend en charge les extensions RADIUS (RFC 6929)
[Switch-radius-radius]server-type extended

## Configure l'adresse IP du serveur radius pour la partie authentification
[Switch-radius-radius]primary authentication <radius-server-ip-address> 1812

## Renseigne la clé partagée entre le commutateur et le serveur RADIUS pour la partie
## authentification
[Switch-radius-radius]key authentication <radius-secret-key>

## Configure l'adresse IP du serveur radius pour la partie traçabilité
[Switch-radius-radius]primary accounting <radius-server-ip-address> 1813

## Renseigne la clé partagée entre le commutateur et le serveur RADIUS pour la partie
## traçabilité
[Switch-radius-radius]key accounting <radius-secret-key>

## Exclut le nom de domaine du nom d'utilisateur
[Switch-radius-radius]user-name-format without-domain

## Active la traçabilité
[Switch-radius-radius]accounting-on enable

## Précise l'adresse IP source utilisée par le commutateur pour communiquer avec
## le serveur RADIUS
[Switch-radius-radius]nas-ip <source-ip-address>
[Switch-radius-radius]quit

# Configuration des méthodes d'authentification et d'autorisation utilisées par défaut

## Configuration du domaine
[Switch]domain <my-domain>
```

```

## Crée la liste d'authentification par défaut (celle-ci détaille les méthodes
## d'authentification utilisées successivement, ici RADIUS, puis local)
[Switch-isp-my-domain]authentication login radius-scheme radius local

## Crée la liste d'autorisation par défaut (celle-ci détaille les méthodes
## d'autorisation utilisées successivement, ici RADIUS, puis local)
[Switch-isp-my-domain]authorization login radius-scheme radius local

## Crée la liste de traçabilité par défaut (celle-ci détaille les méthodes
## d'autorisation utilisées successivement, ici RADIUS, puis local)
[Switch-isp-my-domain]accounting login radius-scheme radius local

```

4.4.2 TACACS+

Le protocole TACACS+ est un protocole d'authentification distante de type AAA. Il permet de réaliser séparément les fonctions d'authentification, d'autorisation et de traçabilité. De plus, les comptes utilisateurs sont gérables d'une manière plus fine qu'avec RADIUS, notamment grâce à un système de listes blanches et noires des commandes invoquées.

Ci-dessous un exemple des commandes de configuration de ce mode d'authentification :

Exemple Cisco IOS

```

! Menu de configuration du serveur tacacs-server-1 (rentrer ces commandes pour chaque
! serveur TACACS+ à déclarer)
Switch(config)# tacacs server <tacacs-server-1>

! Configure l'adresse IP du serveur tacacs
Switch(config-tacacs-server)# address ipv4 <tacacs-server-ip-address>

! Renseigne la clé partagée entre le commutateur et le serveur TACACS+
Switch(config-tacacs-server)# key <tacacs-secret-key>
Switch(config-tacacs-server)# exit

! Active la journalisation pour toutes les sessions utilisateurs possédant
! les droits exec
Switch(config)# aaa accounting exec default start-stop group tacacs+

```

Exemple HP Comware 5

```

# Configuration TACACS+

## Menu de configuration de TACACS+
[Switch]hwtacacs scheme <tacacs>

## Configure l'adresse IP du serveur tacacs pour la partie authentification
[Switch-hwtacacs-tacacs]primary authentication <tacacs-server-ip-address>

## Renseigne la clé partagée entre le commutateur et le serveur TACACS pour la partie
## authentification
[Switch-hwtacacs-tacacs]key authentication <tacacs-secret-key>

## Configure l'adresse IP du serveur tacacs pour la partie autorisation
[Switch-hwtacacs-tacacs]primary authorization <tacacs-server-ip-address>

## Renseigne la clé partagée entre le commutateur et le serveur TACACS pour la partie
## autorisation
[Switch-hwtacacs-tacacs]key authorization <tacacs-secret-key>

## Configure l'adresse IP du serveur tacacs pour la partie traçabilité
[Switch-hwtacacs-tacacs]primary accounting <tacacs-server-ip-address>

## Renseigne la clé partagée entre le commutateur et le serveur TACACS pour la partie
## traçabilité
[Switch-hwtacacs-tacacs]key accounting <tacacs-secret-key>

```

```

## Exclut le nom de domaine du nom d'utilisateur
[Switch-hwtacacs-tacacs]user-name-format without-domain

## Précise l'adresse IP source utilisée par le commutateur pour communiquer avec
## le serveur TACACS+
[Switch-hwtacacs-tacacs]nas-ip <source-ip-address>
[Switch-hwtacacs-tacacs]quit

# Configuration des méthodes d'authentification et d'autorisation utilisées par défaut

## Configuration du domaine
[Switch]domain <my-domain>

## Crée la liste d'authentification par défaut (celle-ci détaille les méthodes
## d'authentification utilisées successivement, ici TACACS+, puis local)
[Switch-isp-my-domain]authentication login hwtacacs-scheme tacacs local

## Crée la liste d'autorisation par défaut (celle-ci détaille les méthodes
## d'autorisation utilisées successivement, ici TACACS+, puis local)
[Switch-isp-my-domain]authorization login hwtacacs-scheme tacacs local

## Crée la liste de traçabilité par défaut (celle-ci détaille les méthodes
## d'autorisation utilisées successivement, ici TACACS+, puis local)
[Switch-isp-my-domain]accounting login hwtacacs-scheme tacacs local

```

4.5 Politique de sécurité des mots de passe

Les mots de passe associés aux comptes utilisateurs doivent respecter des critères de sécurité afin d'empêcher que des personnes non légitimes ne les trouvent et ne s'en servent pour porter atteinte au SI. Cette politique est généralement décrite dans la [PSSI](#) de l'entité.

R22

La politique de sécurité des mots de passe des comptes utilisateurs doit respecter la PSSI en vigueur.

Pour approfondir le sujet, consulter les recommandations mentionnées dans la note technique [\[NT MdP\]](#) de l'ANSSI relative à la sécurité des mots de passe.

4.6 Bannière de connexion

Lorsqu'une personne tente de se connecter à un commutateur, il est possible d'afficher une bannière de connexion à son écran avant l'apparition de l'invite de commande lui demandant de renseigner son identifiant et son mot de passe. Les informations contenues dans ce type de bannière sont très utiles aux personnes malveillantes en phase de reconnaissance du réseau car elles leur permettent de mieux cartographier le réseau cible. L'utilisation de ces bannières est donc à proscrire.

R23

Ne pas configurer de bannière de connexion.

Sur un commutateur, il est possible de désactiver l'affichage de la bannière de connexion :

Exemple Cisco IOS

```

! Supprime la bannière de connexion
Switch(config)# no motd-banner

```

```
# Supprime la bannière de connexion  
[Switch]undo copyright-info enable
```

5 Cloisonnement des réseaux et VLAN

Les SI ont développé une plus grande modularité au fil des évolutions technologiques successives. Les VLAN font partie des solutions techniques qui ont accru cette modularité au niveau du réseau en donnant aux commutateurs la capacité de simuler différents réseaux physiques sur un même équipement.

Il est tout de même important de noter que si la technologie est éprouvée, elle n'a pas été conçue dans le but d'améliorer la sécurité des SI. De plus, des réglementations imposent un cloisonnement physique des réseaux dans certains cas d'usage, le cloisonnement physique étant la méthode de cloisonnement la plus sécurisée.

Cette section a pour but d'exposer les bonnes pratiques de configuration des VLAN, puis d'expliquer les particularités de certains VLAN et enfin d'indiquer comment les configurer afin de se prémunir de certains problèmes de sécurité dans le SI.

Il est possible de segmenter son réseau en un nombre conséquent de VLAN, la plage utilisable définie par le standard 802.1Q allant du VLAN 1 au VLAN 4094 (hors VLAN 1002 à 1005)⁶. À noter que pour opérer cette séparation, le commutateur numérote l'entête des trames Ethernet avec le numéro de VLAN correspondant. Il est par exemple possible de cloisonner son réseau bureautique entre les différents services de son entité (service financier, service technique, service RH, etc.), mais il ne faut pas oublier que plus un réseau est complexe, plus sa gestion est difficile, plus le risque d'erreur humaine est grand, ce qui conduit mécaniquement à une diminution du niveau de sécurité. Il est donc important de limiter le nombre de VLAN au strict nécessaire.

R24

Lorsqu'il n'est pas possible de mettre en place une séparation physique, il est recommandé de cloisonner son système d'information de façon cohérente grâce à l'utilisation des VLAN tout en respectant une logique utilité/simplicité dans le choix de la segmentation.

5.1 Configuration automatique des VLAN

Le protocole VTP, de niveau 2, est utilisé pour administrer et configurer les VLAN sur les commutateurs Cisco de façon automatisée. Cette automatisation réduit la maîtrise de la configuration des VLAN ce qui peut créer des problèmes de sécurité, il est donc préférable de le désactiver.

Sur les commutateurs de marque HP, l'équivalent du protocole VTP se retrouve sous la dénomination de MVRP ou GVRP, ce dernier étant obsolète, remplacé par MVRP.

R25

Désactiver les services de configuration automatique des VLAN, VTP, MVRP ou GVRP selon les commutateurs.

6. Implémentation Cisco, cela peut varier selon les constructeurs.

L'exemple ci-dessous présente la commande permettant de désactiver le protocole VTP de manière globale sur le commutateur :

Exemple Cisco IOS

```
! Désactive VTP sur le commutateur
Switch(config)# vtp mode off
```

Exemple de commande de configuration par interface :

Exemple Cisco IOS

```
! Configure la plage d'interfaces FastEthernet 0/1 à 0/48
Switch(config)# interface range FastEthernet <0/1-48>

! Désactive le protocole VTP sur l'interface
Switch(config-if)# no vtp
```

Exemple HP Comware 5

```
# Désactive MVRP sur le commutateur
[Switch]undo mvrp global enable

# Désactive GVRP sur le commutateur
[Switch]undo gvrp
```

5.2 Configuration des VLAN

Un commutateur gère l'attribution des VLAN par port ; ces ports peuvent être configurés dans l'un des deux modes suivants :

- **mode *access*** : le port est directement connecté à un terminal (poste bureautique, imprimante, téléphone IP, etc.). Les trames Ethernet en provenance ou à destination de ces équipements ne sont pas marquées sur ce type de port ;
- **mode *trunk*** : le port est utilisé pour interconnecter le commutateur à tout autre équipement compatible avec la norme 802.1Q. Les trames Ethernet en provenance ou à destination de ces équipements sont marquées sur ce type de port ⁷

Chacun de ces deux modes a des particularités de configuration. Les paragraphes suivants détaillent les spécificités de ces modes et expliquent comment les configurer.

5.2.1 Ports en mode *access*

Par défaut, certains commutateurs basculent automatiquement un port du mode *access* au mode *trunk* lorsqu'un port en mode *trunk* est détecté de l'autre côté du câble. Même si cette fonction peut paraître utile, elle nuit à la sécurité du réseau. En effet, une attaque consistant à faire passer l'attaquant pour un commutateur (*Switch Spoofing*) en simulant un port en mode *trunk* peut permettre à celui-ci de capter tout le trafic passant par le commutateur. Le fait de forcer les ports à être en mode *access* protège le commutateur contre l'attaque du *Switch Spoofing*.

Ci-dessous, un exemple de configuration d'une plage de ports en mode *access* :

Exemple Cisco IOS

```
! Configure la plage d'interfaces FastEthernet 0/4 à 0/12
Switch(config)# interface range FastEthernet <0/4-12>
```

7. À l'exception du VLAN natif qui n'est généralement pas marqué, notamment car certains équipements ne le supportent pas. Se référer au paragraphe 5.5 pour plus d'informations sur le VLAN natif.

```
! Force le mode access
Switch(config-if)# switchport mode access

! Associe la plage d'interfaces au VLAN 33
Switch(config-if)# switchport access vlan <33>
```

Pour un commutateur HP, une des deux méthodes suivantes peut être utilisée :

Exemple HP Comware 5

```
# Configure la plage d'interfaces GigabitEthernet 1/0/4 à 1/0/12
[Switch-if-range]interface range GigabitEthernet 1/0/4 to GigabitEthernet 1/0/12

# Force le mode access
[Switch-if-range]port link-type access

# Associe la plage d'interfaces au VLAN 33
[Switch-if-range]port access vlan <33>
```

Ou alors :

Exemple HP Comware 5

```
# Entre dans le menu de configuration du VLAN 33
[Switch]vlan <33>

# Associe la plage d'interfaces GigabitEthernet 1/0/4 à 1/0/12 au VLAN 33
[Switch-vlan33]port GigabitEthernet <1/0/4> to GigabitEthernet <1/0/12>
```

5.2.2 Ports en mode *trunk*

De même que pour les ports en mode *access*, il est nécessaire de forcer les ports voulus à fonctionner en mode *trunk* afin d'éviter qu'ils ne basculent en mode *access* suite à une négociation avec un autre équipement. De plus, les ports en mode *trunk* laissent circuler par défaut tous les VLAN. Il convient donc de procéder à un filtrage pour ne laisser passer que les VLAN autorisés.

Les lignes de commandes données en exemple ci-dessous détaillent comment configurer un port en mode *trunk* :

Exemple Cisco IOS

```
! Configure l'interface FastEthernet 0/48
Switch(config)# interface FastEthernet <0/48>

! Force le mode trunk
Switch(config-if)# switchport mode trunk

! Interdit à tous les VLAN de passer par le port trunk
Switch(config-if)# switchport trunk allowed vlan none

! Autorise seulement certains VLAN à passer par le port trunk, ici les VLAN 39 et 99
Switch(config-if)# switchport trunk allowed vlan add <33,99>
```

Exemple HP Comware 5

```
# Configure l'interface FastEthernet 1/0/24
[Switch]interface GigabitEthernet <1/0/24>

# Force le mode trunk
[Switch-GigabitEthernet1/0/24]port link-type trunk

# Autorise seulement certains VLAN à passer par le port trunk, ici les VLAN 39 et 99
[Switch-GigabitEthernet1/0/24]port trunk permit vlan <33 99>
[Switch-GigabitEthernet1/0/24]undo port trunk permit vlan 1
```

R26

Interdire la configuration automatique des ports (en mode *trunk* ou *access*) et configurer ceux-ci de façon sécurisée, notamment :

- dans le cas des ports en mode *access* : ne configurer que le VLAN nécessaire sur un port donné ;
- dans le cas des ports en mode *trunk* : n'autoriser que les VLAN devant effectivement circuler sur le port *trunk*.

5.3 DTP

Le protocole **DTP** est un protocole propriétaire Cisco permettant de négocier dynamiquement le mode (*trunk* ou *access*) d'un lien reliant un port du commutateur à l'équipement situé à l'autre bout du câble. Cette fonctionnalité est activée par défaut, le commutateur émet donc régulièrement des trames DTP sur toutes ses interfaces.

Ce service étant inutile (les ports étant configurés statiquement en mode *trunk* ou *access* sur les équipements), il est nécessaire de le désactiver conformément à la recommandation **R26**. Les lignes de commandes données en exemple ci-dessous détaillent comment désactiver DTP sur tous les ports du commutateur :

Exemple Cisco IOS

```
! Configure la plage d'interfaces FastEthernet 0/1 à 0/48
Switch(config)# interface range FastEthernet <0/1-48>

! Désactive l'émission de trames DTP
Switch(config-if)# switchport nonegotiate
```



La description d'un protocole équivalent n'a pas été trouvée dans la documentation du commutateur HP.

5.4 VLAN de quarantaine

Le VLAN de quarantaine est un VLAN dans le lequel sont placés par défaut tous les ports qui sont censés ne pas être utilisés. Les ports placés dans ce VLAN doivent être isolés entre eux et du reste du SI. Ceci permet de rajouter une protection au cas où un port n'aurait pas été désactivé comme il aurait dû l'être. Il n'y a pas de contrainte particulière concernant le choix du numéro du VLAN si ce n'est qu'il doit être différent du VLAN par défaut⁸ de l'équipement.

R27

Tous les ports qui sont censés être inutilisés doivent être associés au VLAN de quarantaine. Les ports placés dans ce VLAN ne doivent donner accès à aucune ressource du système d'information et doivent interdire les communications avec toute autre machine, y compris les machines placées dans ce VLAN. Ces ports doivent aussi être désactivés, de même que le VLAN de quarantaine et l'interface associée.

Concernant l'interdiction des communications entre les machines présentes dans ce VLAN, se référer aux paragraphes **5.6** et **5.7** sur les mécanismes de *Private VLAN* et *Protected Port*.

8. Voir le paragraphe **5.5** pour plus d'informations sur le VLAN par défaut.

Exemple de configuration du VLAN de quarantaine :

Exemple Cisco IOS

```
! Configure le VLAN de quarantaine
Switch(config)# vlan <666>

! Nomme le VLAN
Switch(config-vlan)# name VLAN-QUARANTAINE

! Désactivation du VLAN
Switch(config-vlan)# shutdown
```

Exemple HP Comware 5

```
# Entre dans le menu de configuration du VLAN 666
[Switch]vlan <666>

# Nomme le VLAN
[Switch-vlan666]name VLAN-QUARANTAINE
[Switch-vlan666]quit

# Désactivation du VLAN
[Switch]interface Vlan-interface 666
[Switch-Vlan-interface666]shutdown
```

5.5 VLAN par défaut et VLAN natif

Ces deux VLAN sont particuliers, il est indispensable de bien comprendre leur rôle afin d'appréhender les risques associés à leur mauvaise configuration :

- le **VLAN par défaut** est celui dans lequel les interfaces sont placées par défaut tant qu'elles n'ont été attribuées à aucun VLAN. En configuration par défaut, c'est généralement le VLAN 1 ;
- le **VLAN natif** est utilisé par les commutateurs pour s'échanger des informations nécessaires au fonctionnement de certains services qu'ils offrent dont **STP**, **CDP** et **VTP**. Ce VLAN a pour particularité de circuler non marqué (au sens 802.1Q) sur les liens *trunk*. Ainsi, toute trame Ethernet entrante non marquée sur un port *trunk* du commutateur sera automatiquement associée par celui-ci au VLAN natif.

Une mauvaise configuration du VLAN natif sur les commutateurs peut avoir plusieurs impacts sur la sécurité du SI :

- en configuration par défaut de l'équipement, les ports non configurés sont associés au VLAN par défaut (VLAN 1). Or ce VLAN est également, en configuration par défaut, le VLAN natif. Ainsi, le terminal se connectant à l'un de ces ports a accès à tout le trafic circulant sur le VLAN natif et peut donc attaquer en disponibilité certains services utilisant le VLAN natif et *in fine* perturber le fonctionnement du commutateur ;
- si des commutateurs d'un même domaine de diffusion sont configurés avec comme VLAN natif des numéros de VLAN différents, un phénomène de saut de VLAN⁹ peut se produire de manière permanente au niveau d'un port *trunk* ;
- si un attaquant connecté à un port *trunk* du commutateur envoie une trame marquée deux fois avec comme premier marquage visible le numéro du VLAN natif et comme second marquage le VLAN de destination du paquet, un saut de VLAN peut se produire. Cependant, si cette attaque réussit, seul un sens de communication fonctionne, il n'y a pas de retour.

Ces particularités impliquent de mettre en œuvre les recommandations énoncées ci-dessous :

9. Trames qui transitent d'un VLAN à un autre par simple changement de marquage des trames dans leur entête au sens 802.1Q. Ce phénomène est aussi connu sous le nom anglais de *VLAN hopping*.

R28

Le VLAN par défaut ne doit jamais être utilisé.

Ci-dessous sont données en exemple les lignes de commandes de configuration du VLAN par défaut sur un commutateur :

Exemple Cisco IOS

```
! Sélection de l'interface du VLAN par défaut
Switch(config)# interface vlan 1

! Désactive l'interface du VLAN par défaut
Switch(config-if)# shutdown

! Supprime l'adresse IP du VLAN par défaut
Switch(config-if)# no ip address
```

Exemple HP Comware 5

```
# Sélection de l'interface du VLAN par défaut
[Switch]interface Vlan-interface 1

# Désactive l'interface du VLAN par défaut
[Switch-Vlan-interface1]shutdown

# Supprime l'adresse IP du VLAN par défaut
[Switch-Vlan-interface1]undo ip address
```

R29

Le VLAN natif :

- doit être configuré afin d'être différent du VLAN par défaut ;
- ne doit être attribué à aucun port en mode *access* (il ne doit pas être utilisé pour faire circuler du trafic métier ou d'administration ;
- doit être le même sur tous les commutateurs du même domaine de diffusion (et de préférence dans tout le système d'information par principe d'homogénéité) afin d'éviter les comportements inadéquats.

Ci-dessous sont données en exemple les lignes de commandes de configuration du VLAN natif sur un commutateur :

Exemple Cisco IOS

```
! Commande à saisir pour chaque lien trunk

! Sélectionne le port trunk préalablement configuré sur l'interface FastEthernet 0/48
Switch(config)# interface FastEthernet <0/48>

! Redéfinit le VLAN natif pour ce port trunk
Switch(config-if)# switchport trunk native vlan <999>
```

Exemple HP Comware 5

```
# Commande à saisir pour chaque lien trunk

# Sélectionne le port trunk préalablement configuré sur l'interface FastEthernet 1/0/24
[Switch]interface GigabitEthernet <1/0/24>

# Redéfinit le VLAN natif pour ce port trunk
[Switch-GigabitEthernet1/0/24]port trunk pvid vlan <999>
```

5.6 *Private VLAN* (ou PVLAN)

Le *Private VLAN*¹⁰ est une fonctionnalité qui permet de rajouter un niveau de compartimentation au sein même des VLAN. Son but premier est de permettre d'économiser des adresses IP mais elle a aussi introduit un concept à valeur ajoutée en matière de sécurité : le VLAN isolé (*isolated VLAN*). Grâce au VLAN isolé, il est possible d'interdire à des machines situées dans un même VLAN de dialoguer entre elles directement, c'est-à-dire sans passer par un équipement tiers, qui peut par exemple filtrer les connexions. Le résultat est semblable à celui du *Protected Port* (voir paragraphe 5.7), à la différence près que le mécanisme n'est pas seulement local au commutateur.

Le principe de fonctionnement des *Private VLAN* est le suivant : des VLAN secondaires sont inclus dans un VLAN primaire. Les VLAN secondaires peuvent être de deux sortes :

- communauté (*community*) : les ports placés dans ce type de VLAN peuvent communiquer entre eux comme s'ils se trouvaient dans un même VLAN « classique », mais ne peuvent pas communiquer avec les ports affectés à d'autres VLAN secondaires ;
- isolé (*isolated*) : les ports placés dans ce VLAN ne peuvent pas communiquer entre eux, mais uniquement avec les ports en mode *promiscuous* (généralement la passerelle par défaut).

Le mode *promiscuous* indique que le port appartient au VLAN primaire et ne comporte aucune restriction de communication avec les VLAN secondaires décrits ci-avant.

Le tableau suivant présente la matrice des flux autorisés ou non entre les différents types de ports :

Port en mode	<i>isolated</i>	<i>promiscuous</i>	<i>community 1</i>	<i>community 2</i>
<i>isolated</i>	✗	✓	✗	✗
<i>promiscuous</i>	✓	✓	✓	✓
<i>community 1</i>	✗	✓	✓	✗
<i>community 2</i>	✗	✓	✗	✓

TABLE 5 – Matrice des flux autorisés



À noter qu'il ne peut y avoir qu'un seul VLAN isolé par VLAN primaire, contrairement aux VLAN de communauté.

R30

Utiliser des *Private VLAN* en mode isolé dès lors que cela est possible techniquement, c'est-à-dire qu'aucun service indispensable au système d'information n'est affecté. En effet, les communications poste à poste ne sont plus possibles dans ce cas.

10. Pour plus d'informations sur les *Private VLAN*, se référer à la [\[RFC 5517\]](#).

L'exemple de configuration suivant détaille comment mettre en place le *private VLAN* :

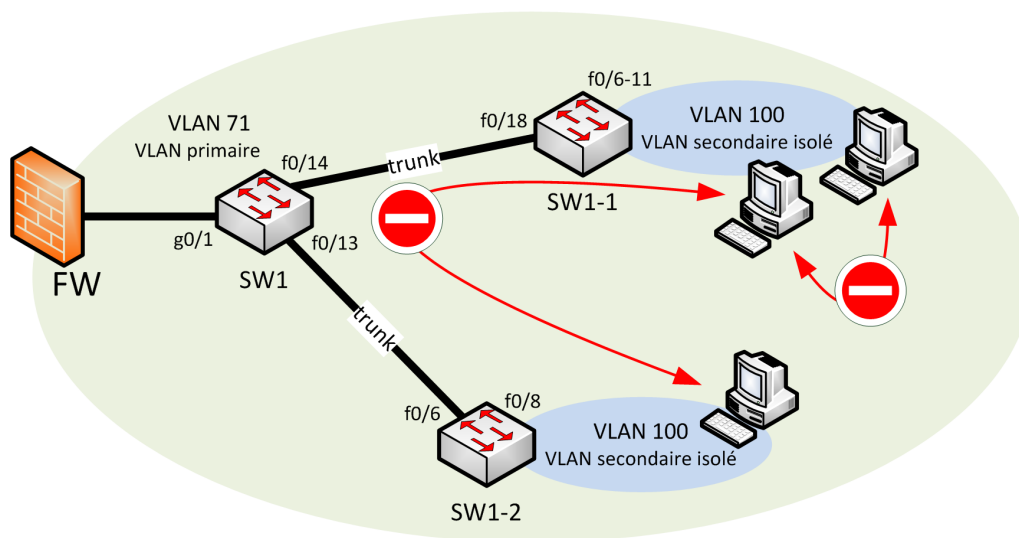



FIGURE 2 – Exemple de mise en place du *private VLAN*

Dans cet exemple, le commutateur SW1 est un commutateur de distribution tandis que SW1-1 et SW1-2 sont des commutateurs de desserte. Le VLAN 71 est le VLAN primaire et le VLAN 100 est un VLAN secondaire isolé associé au VLAN primaire 71. Le pare-feu FW est la passerelle de sortie des terminaux situés dans le VLAN 100. Ainsi, les terminaux situés dans le VLAN 100 peuvent communiquer avec leur passerelle de sortie mais ne peuvent ni se voir, ni communiquer entre eux.

 Le commutateur Cisco pris en exemple dans ce document ne supporte pas cette fonctionnalité. Ce n'en n'est pas moins une fonctionnalité très intéressante à mettre en œuvre sur un équipement qui la supporte car elle augmente la sécurité d'une manière significative tout en étant facile à configurer.

Les lignes de commande de configuration de cet exemple sont détaillées ci-dessous (cas d'un commutateur Cisco Catalyst 3560 avec IOS 12.2(52)SE) :

– Commutateur de distribution SW1 :

Exemple Cisco IOS

```
! Désactive VTP sur le commutateur
Switch(config)# vtp mode off

! Configuration du VLAN 71 (primaire)
Switch(config)# vlan <71>
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit

! Configuration du VLAN 100 (secondaire)
Switch(config)# vlan <100>
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit

! Configuration du VLAN 71 (primaire)
Switch(config)# vlan <71>
Switch(config-vlan)# private-vlan association <100>
Switch(config-vlan)# exit
```

```

! Configuration du port vers le pare-feu
Switch(config)# interface GigabitEthernet <0/1>
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping <71> <100>
Switch(config-if)# exit

! Configuration du port vers le commutateur SW1-1
Switch(config)# interface FastEthernet <0/14>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# switchport trunk allowed vlan add <71,100>
Switch(config-if)# switchport trunk native vlan <999>
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable
Switch(config-if)# exit

! Configuration du port vers le commutateur SW1-2
Switch(config)# interface FastEthernet <0/13>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# switchport trunk allowed vlan add <71,100>
Switch(config-if)# switchport trunk native vlan <999>
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable

```

– Commutateur de desserte SW1-1 :

Exemple Cisco IOS

```

! Désactive VTP sur le commutateur
Switch(config)# vtp mode off

! Configuration du VLAN 71 (primaire)
Switch(config)# vlan <71>
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit

! Configuration du VLAN 100 (secondaire)
Switch(config)# vlan <100>
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit

! Configuration du VLAN 71 (primaire)
Switch(config)# vlan <71>
Switch(config-vlan)# private-vlan association <100>
Switch(config-vlan)# exit

! Configuration du port trunk vers le commutateur SW1
Switch(config)# interface FastEthernet <0/18>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# switchport trunk allowed vlan add <71,100>
Switch(config-if)# switchport trunk native vlan <999>
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable

! Configuration de la plage de ports vers des machines du VLAN 100 (secondaire)
Switch(config)# interface range FastEthernet <0/6-11>
Switch(config-if-range)# switchport mode private-vlan host
Switch(config-if-range)# switchport private-vlan host-association <71> <100>
Switch(config-if-range)# exit

```

- Commutateur desserte SW1-2 :

Exemple Cisco IOS

```
! Désactive VTP sur le commutateur
Switch(config)# vtp mode off

! Configuration du VLAN 71 (primaire)
Switch(config)# vlan <71>
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit

! Configuration du VLAN 100 (secondaire)
Switch(config)# vlan <100>
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit

! Configuration du VLAN 71 (primaire)
Switch(config)# vlan <71>
Switch(config-vlan)# private-vlan association <100>
Switch(config-vlan)# exit

! Configuration du port trunk vers le commutateur SW1
Switch(config)# interface FastEthernet <0/6>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# switchport trunk allowed vlan add <71,100>
Switch(config-if)# switchport trunk native vlan <999>
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable

! Configuration du port vers une machine du VLAN 100 (secondaire)
Switch(config)# interface FastEthernet <0/8>
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association <71> <100>
Switch(config-if)# exit
```

Exemple pour un commutateur HP Comware :

- Commutateur de distribution SW1 :

Exemple HP Comware 5

```
# Configuration du VLAN 71 (primaire)
[Switch]vlan <71>
[Switch-vlan71]isolate-user-vlan enable
[Switch-vlan71]quit

# Configuration du VLAN 100 (secondaire)
[Switch]vlan <100>
[Switch-vlan100]isolated-vlan enable
[Switch-vlan100]quit

# Associe le VLAN secondaire 100 avec le VLAN primaire 71
[Switch]isolate-user-vlan <71> secondary <100>

# Configuration du port vers le pare-feu
[Switch]interface GigabitEthernet <1/0/1>
[Switch-GigabitEthernet1/0/1]port link-mode bridge
[Switch-GigabitEthernet1/0/1]port isolate-user-vlan <71> promiscuous
[Switch-GigabitEthernet1/0/1]port link-type hybrid
[Switch-GigabitEthernet1/0/1]port hybrid vlan <100> <71> tagged
[Switch-GigabitEthernet1/0/1]quit

# Configuration du port vers le commutateur SW1-1
[Switch]interface GigabitEthernet <1/0/14>
[Switch-GigabitEthernet1/0/14]port link-type trunk
[Switch-GigabitEthernet1/0/14]port trunk permit vlan <71> <100>
[Switch-GigabitEthernet1/0/14]port trunk pvid vlan <999>
```

```
[Switch-GigabitEthernet1/0/14]undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/14]quit

# Configuration du port vers le commutateur SW1-2
[Switch]interface GigabitEthernet <1/0/13>
[Switch-GigabitEthernet1/0/13]port link-type trunk
[Switch-GigabitEthernet1/0/13]port trunk permit vlan <71> <100>
[Switch-GigabitEthernet1/0/13]port trunk pvid vlan <999>
[Switch-GigabitEthernet1/0/13]undo port trunk permit vlan 1
```

– Commutateur de desserte SW1-1 :

Exemple HP Comware 5

```
# Configuration du VLAN 71 (primaire)
[Switch]vlan <71>
[Switch-vlan71]isolate-user-vlan enable
[Switch-vlan71]quit

# Configuration du VLAN 100 (secondaire)
[Switch]vlan <100>
[Switch-vlan100]isolated-vlan enable
[Switch-vlan100]quit

# Associe le VLAN secondaire 100 avec le VLAN primaire 71
[Switch]isolate-user-vlan <71> secondary <100>

# Configuration du port vers le commutateur SW1
[Switch]interface GigabitEthernet <1/0/18>
[Switch-GigabitEthernet1/0/18]port link-type trunk
[Switch-GigabitEthernet1/0/18]port trunk permit vlan <71> <100>
[Switch-GigabitEthernet1/0/18]port trunk pvid vlan <999>
[Switch-GigabitEthernet1/0/18]undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/18]quit

# Configuration de la plage de ports vers des machines du VLAN 100 (secondaire)
[Switch]interface range GigabitEthernet <1/0/6> to GigabitEthernet <1/0/11>
[Switch-if-range]port link-type access
[Switch-if-range]port access vlan <100>
[Switch-if-range]port isolate-user-vlan host
```

– Commutateur desserte SW1-2 :

Exemple HP Comware 5

```
# Configuration du VLAN 71 (primaire)
[Switch]vlan <71>
[Switch-vlan71]isolate-user-vlan enable
[Switch-vlan71]quit

# Configuration du VLAN 100 (secondaire)
[Switch]vlan <100>
[Switch-vlan100]isolated-vlan enable
[Switch-vlan100]quit

# Associe le VLAN secondaire 100 avec le VLAN primaire 71
[Switch]isolate-user-vlan <71> secondary <100>

# Configuration du port vers le commutateur SW1
[Switch]interface GigabitEthernet <1/0/6>
[Switch-GigabitEthernet1/0/6]port link-type trunk
[Switch-GigabitEthernet1/0/6]port trunk permit vlan <71> <100>
[Switch-GigabitEthernet1/0/6]port trunk pvid vlan <999>
[Switch-GigabitEthernet1/0/6]undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/6]quit

# Configuration du port vers une machine du VLAN 100 (secondaire)
[Switch]interface GigabitEthernet 1/0/8
[Switch-GigabitEthernet1/0/8]port link-type access
[Switch-GigabitEthernet1/0/8]port access vlan <100>
[Switch-GigabitEthernet1/0/8]port isolate-user-vlan host
```

5.7 Protected Port et Port Isolation

Protected Port est semblable au mécanisme de *Private VLAN isolated* au détail près qu'il n'agit qu'au niveau local d'un commutateur. Il permet d'interdire le trafic direct entre différents terminaux connectés au même commutateur, même si ceux-ci sont dans un même VLAN.

C'est une fonctionnalité très intéressante d'un point de vue sécurité, car elle permet de limiter les communications potentiellement malveillantes entre équipements terminaux (souvent vectrices d'attaques), tout en étant simple à mettre en œuvre.

Étant donné que *Protected Port* n'agit que localement sur un commutateur, cela n'empêche pas à deux machines connectées sur deux commutateurs différents du même domaine de diffusion de communiquer directement sans passer par un équipement de sécurité de niveau 3, comme par exemple un pare-feu. Ainsi, l'utilisation de *Private VLAN isolated* est bien plus efficace que l'utilisation de *Protected Port* qui reste cependant une option intéressante à activer par défaut.

R30-

S'il n'est pas possible de mettre en place le mécanisme de *Private VLAN isolated*, activer au minimum le mécanisme de *Protected Port* ou *Port Isolation* en fonction du modèle d'équipement.

Exemple de configuration de la fonctionnalité *Protected Port* :

Exemple Cisco IOS

```
! Active le Protected Port sur les ports 4 à 42
Switch(config)# interface range FastEthernet <0/4-42>
Switch(config-if-range)# switchport protected
```

Sur les commutateurs HP, le principe est le même, mais il se nomme isolation de port :

Exemple HP Comware 5

```
# Active l'isolation de port sur les ports 4 à 20
[Switch]interface range GigabitEthernet 1/0/4 to GigabitEthernet 1/0/20
[Switch-if-range]port-isolate enable
```

6 Routage

6.1 Routage interVLAN

Les commutateurs n'ont pas été conçus pour faire du routage de paquets, cette fonction doit exclusivement être remplie par des équipements de niveau 3. Or, de nombreux commutateurs permettent de faire du routage interVLAN, il faut donc veiller à ce que cette fonctionnalité soit effectivement désactivée. Celle-ci est d'ailleurs parfois activée de façon involontaire par les administrateurs réseau. En effet, sur certains commutateurs, le simple fait de leur attribuer deux adresses IP dans des VLAN différents active automatiquement cette fonctionnalité.

Le principal danger à activer le routage interVLAN sur un commutateur est de faire transiter les données directement d'un VLAN à l'autre sans aucun filtrage.

R31

Le routage interVLAN doit être assuré par des équipements de niveau 3. Celui-ci doit donc être désactivé sur les commutateurs d'accès.

Sur les commutateurs HP, il faut notamment s'assurer que la ligne de configuration `link-mode bridge` est présente au niveau de la configuration de chaque interface.

6.2 Mandataire ARP

Les commutateurs peuvent remplir le rôle de mandataire ARP (*proxy ARP*). Ceci permet à deux réseaux IP situés de part et d'autre du commutateur de communiquer ensemble sans que le routage IP ne soit activé. C'est une fonctionnalité qu'il est nécessaire de désactiver pour les mêmes raisons de sécurité que celles exposées dans le paragraphe 6.1 concernant le routage interVLAN.

R32

Le routage interVLAN doit être assuré par des équipements de niveau 3. La fonctionnalité de mandataire ARP doit donc être désactivée sur les commutateurs d'accès.

Exemple de commande de configuration pour la désactivation de la fonctionnalité ARP proxy :

Exemple Cisco IOS

```
! Désactive le proxy ARP du commutateur
Switch(config)# ip arp proxy disable
```

Sur un commutateur HP, le proxy ARP s'active/se désactive par VLAN :

Exemple HP Comware 5

```
# Désactive le proxy ARP du commutateur sur l'interface du VLAN 23
[Switch]interface Vlan-interface 23
[Switch-Vlan-interface23]undo local-proxy-arp enable
```

6.3 Source routing

Dans l'entête du protocole IP, l'option *source routing* permet à la machine émettrice d'un paquet de spécifier des informations de routage spécifiques à ce paquet. L'utilisation de ce mécanisme est déconseillée car il introduit des problèmes de sécurité, comme par exemple le risque d'un accès par une personne malveillante à un sous-réseau auquel les règles de routage des équipements sur cette route ne lui donneraient normalement pas accès.

R33

Désactiver la fonctionnalité de *Source routing*.

La commande de configuration donnée ci-dessous en exemple précise comment désactiver ce mécanisme :

Exemple Cisco IOS

```
! Défausse les datagrammes IP contenant l'option source-route dans leur entête
Switch(config)# no ip source-route
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

7 Sécurisation des ports

Dans une entité, les commutateurs de desserte sont la principale porte d'entrée du SI depuis l'intérieur. Les prises réseau disséminées dans les locaux sont en effet directement connectées à ces commutateurs et le personnel, voire les visiteurs, y ont physiquement accès. Leur sécurisation joue donc un rôle essentiel dans le contrôle d'accès au SI de l'entité.

Parmi les bonnes pratiques de contrôle d'accès, la plus efficace pour se protéger contre les intrusions est de désactiver tous les ports des commutateurs qui ne sont pas censés être utilisés. Ainsi, en prenant l'exemple des prises réseau des bureaux vacants, celles-ci ne pourront pas être utilisées par des personnes malveillantes.

R34

Désactiver les ports inutilisés sur les commutateurs.

Exemple de désactivation d'un port réseau :

Exemple Cisco IOS

```
! Désactive le port réseau 0/5
Switch(config)# interface GigabitEthernet <0/5>
Switch(config-if)# shutdown
```

Exemple HP Comware 5

```
# Désactive le port réseau 1/0/5
[Switch]interface GigabitEthernet <1/0/5>
[Switch-GigabitEthernet1/0/5]shutdown
```

Les ports qui ne sont pas désactivés doivent être protégés contre la connexion de matériel illégitime, car à ce stade, rien n'empêche une personne malintentionnée de remplacer une machine légitime par un équipement illégitime ou de brancher un autre commutateur afin de partager la connexion entre plusieurs machines.

Deux mécanismes permettent de rendre ces attaques moins évidentes : *port security* et [802.1X](#) (avec authentification par RADIUS avec certificat). Toutefois, le niveau de sécurité qu'ils apportent n'est pas le même. *Port security* permet seulement de limiter le nombre de machines connectées à une même interface d'accès, tandis que 802.1X apporte en plus un mécanisme de contrôle d'accès éprouvé, qui peut reposer sur des fonctions cryptographiques robustes. Chez certains constructeurs,

les deux solutions sont en partie redondantes et doivent donc être utilisées de façon exclusive, tout en privilégiant 802.1X.

R35

Sécuriser l'accès au ports des commutateurs en utilisant 802.1X.

R35-

S'il n'est pas possible de mettre en place 802.1X, utiliser *port security*.

7.1 *Port security*

Port security permet de limiter le nombre d'adresses MAC connectées à une même interface d'accès¹¹.

Les commandes suivantes données en exemple permettent de configurer *port security* :

Exemple Cisco IOS

```
! Configure la plage d'interfaces FastEthernet 0/4 à 0/12
Switch(config)# interface range FastEthernet <0/4-12>

! Active port security sur les interfaces
Switch(config-if-range)# switchport port-security

! Définit un maximum d'adresses MAC connectées simultanément par port (ici 1)
Switch(config-if-range)# switchport port-security maximum <1>

! Désactive l'interface s'il y a violation de la limite définie
Switch(config-if-range)# switchport port-security violation shutdown
Switch(config-if-range)# exit

! Indique qu'un port bloqué (état err-disabled) à cause du port security peut être
! débloqué automatiquement par le mécanisme de recovery
Switch(config)# errdisable recovery cause psecure-violation

! Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
Switch(config)# errdisable recovery interval <300>
```

Exemple HP Comware 5

```
# Active port security sur le commutateur
[Switch]port-security enable

# Définit la fréquence d'apprentissage des adresses MAC des machines connectées aux ports
# du commutateur (toutes les 5 minutes)
[Switch]port-security timer autolearn aging <5>

# Configure la plage d'interfaces FastEthernet 1/0/4 à 1/0/12
[Switch]interface range GigabitEthernet <1/0/4> GigabitEthernet <1/0/12>

# Configure le commutateur de sorte qu'il apprenne automatiquement les adresses MAC des
# machines qui lui sont connectées
[Switch-if-range]port-security port-mode autolearn

# Définit un maximum d'adresses MAC connectées simultanément par port (ici 1)
[Switch-if-range]port-security max-mac-count <1>
```

11. Il est également possible d'activer *port security* sur des interfaces en mode *trunk* pour le cas particulier des terminaux connectés à plusieurs VLAN.

```
# Désactive l'interface s'il y a violation de la limite définie
[Switch-if-range]port-security intrusion-mode disableport-temporarily
[Switch-if-range]quit

# Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
[Switch]port-security timer disableport <300>
```

7.2 Contrôle d'accès par port 802.1X avec authentification par RADIUS

Comme indiqué précédemment, la méthode la plus efficace pour sécuriser les ports des commutateurs est la mise en place d'un contrôle d'accès par 802.1X basé sur une authentification par RADIUS. Dans ce mode, la sécurité va reposer sur la présence d'un serveur RADIUS (au sein du SI de l'entité) qui va jouer le rôle de contrôleur d'accès lors de chaque connexion d'un équipement à l'un des ports du commutateur.

Le mode de fonctionnement est le suivant : tous les ports sont activés par défaut mais dans un état bloqué. Lorsqu'un terminal se branche, un processus d'authentification démarre. Si l'authentification réussit, le port est débloqué et la machine cliente accède au VLAN auquel le port a été rattaché. Dans le cas contraire, le port reste bloqué.

Exemple de configuration du 802.1X sur des ports connectés à des postes de bureautique :

Exemple Cisco IOS

```
! Configure le commutateur pour qu'il procède à une authentification RADIUS sur
! les ports 4 à 15

! Active le service AAA (authentification, autorisation et traçabilité)
Switch(config)# aaa new-model

! Active l'authentification 802.1X
Switch(config)# aaa authentication dot1x default group radius

! Active l'authentification 802.1X globalement sur le commutateur
Switch(config)# dot1x system-auth-control

! Menu de configuration du serveur radius-1
Switch(config)# radius server <radius-server-1>

! Configure l'adresse IP du serveur RADIUS
Switch(config-radius-server)# address ipv4 <radius-server-ip-address> auth-port 1812
acct-port 1813

! Renseigne la clé partagée entre le commutateur et le serveur RADIUS
Switch(config-radius-server)# key <radius-secret-key>
Switch(config-radius-server)# exit

! Configuration des interfaces bureautique
Switch(config)# interface range FastEthernet <0/4-15>

! Passage des interfaces en mode access
Switch(config-if-range)# switchport mode access

! Active l'authentification sur ces ports
Switch(config-if-range)# authentication port-control auto

! Active la réauthentification périodique des clients
Switch(config-if-range)# dot1x reauthentication

! Configure le commutateur pour qu'il utilise comme valeur de timeout celle du
! Session-Timeout du serveur RADIUS (sinon, renseigner un nombre de secondes à la
! place de l'argument "server")
Switch(config-if-range)# dot1x timeout reauth-period server
```

```
! Configure le commutateur pour que les ports défaussent les paquets de toute
! nouvelle machine connectée faisant dépasser le nombre maximum de machines
! acceptées sur le port
Switch(config-if-range)# dot1x violation-mode protect
```

Les commandes suivantes permettent de limiter l'accès à certains ports du commutateur à une machine unique par port :

Exemple Cisco IOS

```
! Configure le serveur d'accès pour reconnaître et utiliser les attributs spécifiques
! du vendeur
Switch(config)# radius-server vsa send authentication

! Configuration des interfaces bureautique
Switch(config)# interface range FastEthernet <0/4-15>

! Limite le nombre de machines connectées simultanément à un port à 1
Switch(config-if)# authentication host-mode single-host
```



Pour les commutateurs HP, le contrôle d'accès par port 802.1X est un sous-ensemble de la fonctionnalité *port-security*.

Exemple HP Comware 5

```
# Active port security sur le commutateur
[Switch]port-security enable

# Crée le plan RADIUS
[Switch]radius scheme <radius-scheme>

# Configure l'adresse IP du serveur RADIUS et renseigne la clé partagée entre le
# commutateur et le serveur RADIUS
[Switch-radius-radius-scheme]primary authentication <radius-server-ip-address> 1812 key
<radius-secret-key>
[Switch-radius-radius-scheme]primary accounting <radius-server-ip-address> 1813 key
<radius-secret-key>

# Enlève la partie domaine dans les noms d'utilisateurs à authentifier
[Switch-radius-radius-scheme]user-name-format without-domain

# Précise l'adresse IP utilisée par le commutateur comme adresse source pour les
# communications avec le serveur RADIUS
[Switch-radius-radius]nas-ip <switch-admin-ip-address>
[Switch-if-range]quit

# Crée le domaine RADIUS
[Switch]domain radius-domain

# Associe le plan RADIUS au domaine RADIUS pour l'authentification, les autorisations
# et la traçabilité
[Switch-isp-radius-domain]authentication default radius-scheme <radius-scheme>
[Switch-isp-radius-domain]authorization default radius-scheme <radius-scheme>
[Switch-isp-radius-domain]accounting default radius-scheme <radius-scheme>
[Switch-if-range]quit

# Active la méthode d'authentification EAP (Extensible Authentication Protocol)
[Switch]dot1x authentication-method eap

# Configure le commutateur pour qu'il procède à une authentification RADIUS sur
# les ports 1/0/4 à 1/0/15
[Switch]interface range GigabitEthernet <1/0/4> GigabitEthernet <1/0/15>

# Définit un maximum d'adresses MAC connectées simultanément par port (ici 1)
[Switch-if-range]port-security max-mac-count <1>
```

```
# Active le mode d'authentification par 802.1X avec vérification de l'adresse MAC
[Switch-if-range]port-security port-mode userlogin-secure

# Ne transmet les trames qu'aux ports dont les machines connectées sont autorisées,
# par comparaison de l'adresse MAC de destination avec celle de la machine
# authentifiée sur le port
[Switch-if-range]port-security ntk-mode ntkonly
[Switch-if-range]quit
```

Le contrôle d'accès effectué sur les ports du commutateur repose aussi grandement sur la configuration faite au niveau des machines clientes et du serveur RADIUS. Différentes méthodes existent, mais beaucoup n'offrent pas un niveau de sécurité suffisant. La méthode d'authentification à privilégier est celle reposant sur le standard EAP-TLS.

R36

Si le contrôle d'accès aux ports du commutateur par 802.1X est mis en œuvre, utiliser le standard reposant sur EAP-TLS.



La mise en place de EAP-TLS utilise des certificats et requiert donc la mise en place d'une IGC.

8 Mécanismes liés à la disponibilité

8.1 DHCP snooping et IP Source Guard

Le protocole DHCP permet d'attribuer et de configurer dynamiquement les adresses IP (et d'autres informations comme la passerelle par défaut, le serveur DNS, etc.) des terminaux se connectant au réseau. Le *DHCP snooping* et l'*IP Source Guard* sont des fonctionnalités qui protègent le commutateur contre diverses attaques portant sur ce protocole. En effet, le protocole présente, de par sa conception, des faiblesses utilisables par des attaquants pour perturber le trafic réseau ou usurper des adresses IP. La machine d'un attaquant se faisant passer pour un serveur DHCP ou encore générant du trafic en se faisant passer pour un autre terminal (*IP spoofing*) sont les deux méthodes d'attaque les plus courantes. Parmi les contre-mesures existantes, les plus éprouvées sont :

- le *DHCP snooping*, consistant à :
 - déclarer des ports de confiance identifiés comme les seuls par lesquels peuvent provenir des baux DHCP,
 - maintenir une table d'association DHCP au sein du commutateur (appelée table *DHCP snooping*) afin qu'il conserve en temps-réel l'état du bail DHCP de tous les terminaux qui lui sont connectés,
 - limiter le nombre de requêtes DHCP par seconde sur une interface,
- l'*IP Source Guard*, consistant à vérifier la cohérence entre les adresses IP utilisées par les terminaux connectés au commutateur et les données contenues dans la table *DHCP snooping*, afin d'empêcher l'*IP spoofing*.

R37

Activer les fonctions de *DHCP snooping* et d'*IP Source Guard* afin de pallier les faiblesses de sécurité du protocole DHCP.

Exemple de configuration de *DHCP snooping* et *IP Source Guard* :

Exemple Cisco IOS

```
! Active le DHCP snooping
Switch(config)# ip dhcp snooping

! Définit sur quels VLAN le DHCP snooping doit être activé (tous ici, sauf le
! VLAN 1 inutilisé)
Switch(config)# ip dhcp snooping vlan <2-4094>

! Définit l'interface par laquelle le commutateur dialogue avec le serveur ou relai DHCP
! de confiance
Switch(config)# interface FastEthernet <0/1>
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# exit

! Active la base de données de DHCP snooping (sert à suivre l'état des baux DHCP)
Switch(config)# ip dhcp snooping database <flash:snooping-database>

! Désactive l'insertion des champs de l'option 82 du protocole DHCP (action nécessaire
! pour que le DHCP snooping fonctionne)
Switch(config)# no ip dhcp snooping information option

! Limite le nombre de paquets DHCP à 10 par seconde sur les interfaces connectées
! aux clients
Switch(config)# interface range FastEthernet <0/4-15>
Switch(config-if)# ip dhcp snooping limit rate <10>
Switch(config-if)# exit

! Active l'IP Source Guard sur les interfaces connectées aux clients
Switch(config)# interface range FastEthernet <0/4-15>
Switch(config-if)# ip verify source
```

Exemple HP Comware 5

```
# Active le DHCP snooping
[Switch]dhcp-snooping

# Définit l'interface par laquelle le commutateur dialogue avec le serveur ou relai DHCP
# de confiance
[Switch]interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1]dhcp-snooping trust
[Switch-GigabitEthernet1/0/1]quit

# Définit le nombre maximum d'entrées dans la table IP Source Guard par port sur
# les interfaces connectées aux clients
[Switch]interface range GigabitEthernet 1/0/3 GigabitEthernet 1/0/12
[Switch-if-range]ip verify source max-entries <1>

# Active la vérification d'adresse MAC (compare l'adresse MAC source de la trame
# de la requête DHCP avec le champ chaddr contenu dans celle-ci)
[Switch-if-range]dhcp-snooping check mac-address

# Active la comparaison du contenu des requêtes DHCP avec les entrées de la base
# locale de DHCP snooping
[Switch-if-range]dhcp-snooping check request-message

# Limite le débit de paquets DHCP à 64 kbits par seconde sur les interfaces connectées
# aux clients
[Switch]interface range GigabitEthernet 1/0/3 GigabitEthernet 1/0/12
[Switch-if-range]dhcp-snooping rate-limit 64
[Switch-if-range]quit

# Active l'IP Source Guard sur les interfaces connectées aux clients
[Switch]interface range GigabitEthernet 1/0/3 GigabitEthernet 1/0/12
[Switch-if-range]ip verify source ip-address mac-address
[Switch-if-range]quit
```

8.2 Inspection ARP

Le protocole ARP permet à un équipement de faire les associations entre les adresses IP et les adresses MAC des machines situées dans son domaine de diffusion. Le modèle sur lequel il a été conçu présente des faiblesses qui permettent entre autres à un attaquant de se faire passer pour une autre machine, technique appelée *ARP spoofing* ou encore *ARP poisoning*.

La fonction d'inspection ARP permet de pallier ces faiblesses. Elle consiste à vérifier la cohérence entre le contenu des trames ARP (adresses source MAC/IP et adresses destination MAC/IP) et les données contenues dans la table *DHCP snooping*, afin de détecter et bloquer les tentatives d'*ARP spoofing*.

R38

Activer les fonctions d'inspection ARP.

Exemple de configuration des fonctions d'inspection ARP sur un commutateur :

Exemple Cisco IOS

```
! Active l'inspection des échanges ARP sur les VLAN 38 à 60 dans un environnement
! où le DHCP est activé
Switch(config)# ip arp inspection vlan <38-60>

! Active la validation des packets ARP en fonction de la cohérence retrouvée dans
! leurs champs ou de leur formatage
Switch(config)# ip arp inspection validate src-mac dst-mac ip

! Définit les interfaces connectées à d'autres commutateurs comme de confiance
Switch(config)# interface range FastEthernet <0/2-3>
Switch(config-if-range)# ip arp inspection trust
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

8.3 Spanning Tree

Pour améliorer la résilience des SI, il est fréquent de mettre en place une topologie réseau comprenant entre autres, des liens et des commutateurs redondés. Il en résulte l'apparition de boucles réseau génératrices d'instabilité, voire de coupures de connexion.

La technologie *Spanning Tree* (protocole de niveau 2) a été introduite pour résoudre cette problématique en supprimant les boucles réseau par domaine de diffusion. Dans chaque domaine de diffusion, un commutateur (généralement un commutateur de cœur de réseau) est déclaré racine (*root*) au sens *Spanning Tree*. Son rôle est de calculer une topologie réseau sans boucle et de garantir son maintien. L'élection de ce commutateur en tant que *root* est faite automatiquement et dynamiquement par l'ensemble des commutateurs du domaine de diffusion au moyen de trames spécifiques appelées [BPDU](#).

Les attaques sur ce protocole portent sur le mécanisme d'élection du commutateur *root*. Les deux attaques les plus fréquentes depuis une machine malveillante ¹² sont :

- l'écoute de trafic : s'autodéclarer en tant que commutateur *root* pour récupérer tout le trafic du domaine de diffusion ;

12. Celle-ci doit se trouver dans le domaine de diffusion cible.

- le déni de service : envoyer des messages BPDU pour provoquer de manière fréquente et aléatoire la réélection du commutateur *root*. Ceci crée un déni de service difficile à diagnostiquer.

Pour contrer ce type d'attaques au niveau des commutateurs de desserte, il est possible d'utiliser la fonction *BPDU Guard* de la configuration *Spanning Tree*. Celle-ci a pour rôle de bloquer toutes les trames BPDU arrivant sur les ports configurés avec cette option et de les désactiver temporairement si de telles trames sont détectées. Les informations de topologie *Spanning Tree* reçues sur ces ports seront ignorées par le commutateur et non propagées.

R39

Activer des protections contre la propagation des trames *Spanning Tree* sur les ports d'accès.

Configurer les ports d'accès en mode *portfast* pour Cisco IOS, ou *edge port* pour HP Comware, permet de faire qu'ils passent presque immédiatement en mode *forwarding* au sens *Spanning Tree* sans attendre la convergence du protocole. Ce mode est généralement conseillé pour les ports d'accès car il permet d'éviter des problèmes de réseau que l'on peut rencontrer avec certains protocoles si les ports prennent trop de temps à passer à l'état *forwarding*.

R40

Activer le mode *portfast* ou *edge port* (selon le constructeur) sur les ports connectés à des machines clientes. Ne pas activer ce mode sur les interfaces connectées à d'autres commutateurs.

Exemple de configuration pour la sécurisation de *Spanning Tree* :

Exemple Cisco IOS

```
! Sélectionne les interfaces d'accès
Switch(config)# interface range FastEthernet <0/1-20>

! Force les ports d'accès en mode forwarding (au sens Spanning Tree)
Switch(config-if-range)# spanning-tree portfast
Switch(config-if-range)# exit

! Désactive les ports en mode portfast s'ils reçoivent des trames BPDU en provenance
! des équipements qui y sont connectés
Switch(config)# spanning-tree portfast bpduguard default

! Indique qu'un port bloqué (état err-disabled) à cause du bpduguard peut être débloqué
! automatiquement par le recovery
Switch(config)# errdisable recovery cause bpduguard

! Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
Switch(config)# errdisable recovery interval <300>
```

Exemple HP Comware 5

```
# Sélectionne les interfaces d'accès
[Switch]interface range GigabitEthernet <1/0/1> to GigabitEthernet <1/0/20>

# Force les ports d'accès en mode forwarding (au sens Spanning Tree)
[Switch-if-range]stp edged-port enable
[Switch-if-range]quit

# Désactive les ports edge s'ils reçoivent des trames BPDU en provenance
# des équipements qui y sont connectés
[Switch]stp bpdu-protection
```



```
# Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
[Switch]shutdown-interval <300>
```



La commande `spanning-tree portfast bpduguard default` (respectivement `stp edged-port enable` pour HP) est globale et s'applique à tous les ports en mode *portfast* (respectivement *edge* pour HP). Pour appliquer la fonction *BPDU Guard* sur des ports du commutateur qui ne sont pas en mode *portfast*, il faut utiliser la commande `spanning-tree bpduguard enable` au niveau des interfaces concernées.



HP Comware et Cisco IOS n'utilisent pas la même version du protocole *Spanning Tree* par défaut. HP Comware utilise **MSTP** alors que Cisco IOS utilise **PVST**. D'un point de vue sécurité, les différentes versions de *Spanning Tree* ne présentent pas de différence : MSTP est la version standardisée du protocole qui fonctionnera avec le plus de matériels de différents constructeurs tandis que PVST, développé par Cisco, n'est pas forcément implémenté chez les concurrents, même si beaucoup de produits tiers sont compatibles.

Du point de vue du dimensionnement, PVST est plutôt adapté aux réseaux contenant peu de VLAN (de l'ordre de 20 maximum) tandis que **RPVST** et MSTP sont plutôt adaptés à de gros déploiements, mais sont un peu plus délicats à déployer. Il faut notamment configurer les ports connectés aux machines clientes en mode *portfast* afin d'éviter les blocages de port temporaires lors des reconvergences *Spanning Tree* sur le réseau.

8.4 Storm control

Le *Storm control* permet de maintenir le commutateur dans un état fonctionnel dans le cas où une « tempête » de trames *broadcast*, *multicast* ou *unicast* (qui peuvent dégrader sévèrement les performances du commutateur) se produirait. L'activer peut s'avérer utile pour améliorer la robustesse du réseau.

R41

Les mécanismes de protection contre les « tempêtes » de trames sont intéressants à mettre en œuvre pour renforcer la résistance des commutateurs face à ces agressions.



Le *Storm control* est à mettre en place avec précaution. La mise en place de seuils non adaptés aux caractéristiques du SI peut causer des indisponibilités réseau.

Exemple de commandes de configuration du *Storm control* :

Exemple Cisco IOS

```
! Sélectionne les interfaces d'accès
Switch(config)# interface range FastEthernet <0/1-20>
```

```

! Limite le trafic broadcast à X% de la bande passante
Switch(config-if-range)# storm-control broadcast level <X>

! Limite le trafic multicast à Y% de la bande passante
Switch(config-if-range)# storm-control multicast level <Y>

! Limite le trafic unicast à Z% de la bande passante
Switch(config-if-range)# storm-control unicast level <Z>

! Active les remontées d'alertes par SNMP (seulement si les traps SNMP sont activés)
Switch(config-if-range)# storm-control action trap

! Eteint un port s'il subit une tempête de trames
Switch(config-if-range)# storm-control action shutdown

! Indique qu'un port éteint à cause d'une tempête de trames peut être débloqué
! automatiquement par le recovery
Switch(config)# errdisable recovery cause storm-control

! Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
Switch(config)# errdisable recovery interval <300>

```

Pour les commutateurs HP, les ports bloqués par le *Storm control* ne peuvent pas être automatiquement débloqués. Une solution consiste donc à bloquer le trafic en excès par rapport aux règles établies :

Exemple HP Comware 5

```

# Sélectionne les interfaces d'accès
[Switch]interface range GigabitEthernet <1/0/2> GigabitEthernet <1/0/20>

# Limite le trafic broadcast à X% de la bande passante
[Switch-if-range]broadcast-suppression <X>

# Limite le trafic multicast à Y% de la bande passante
[Switch-if-range]multicast-suppression <Y>

# Limite le trafic unicast à Z% de la bande passante
[Switch-if-range]unicast-suppression <Z>

# Active les remontées d'alertes par SNMP (seulement si les traps SNMP sont activés)
[Switch-if-range]storm-constrain enable trap

# Eteint un port s'il subit une tempête de trames
[Switch-if-range]storm-constrain control shutdown

# Génère un événement de journalisation lorsque du trafic est bloqué
[Switch-if-range]storm-constrain enable log

# Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
[Switch]shutdown-interval <300>

```

8.5 *Small-frame arrival rate*

Les trames de petite taille (moins de 67 octets) ne sont pas pris en compte dans le *Storm control* et sont donc traitées séparément. Le *small-frame arrival rate* permet de limiter le nombre de trames de petite taille qu'une interface peut accepter en une seconde.

R42

Le mécanisme de contrôle du taux de petites trames est intéressant à mettre en œuvre pour renforcer la résistance des commutateurs face à des attaques utilisant ce type de trames.



Ce mécanisme peut potentiellement perturber la téléphonie sur IP avec l'utilisation de certains mécanismes d'encodage.

Exemple de commandes de configuration du *small-frame arrival rate* :

Exemple Cisco IOS

```
! Active le service de détection du taux de petites trames sur le commutateur
Switch(config)# errdisable detect cause small-frame

! Indique qu'un port bloqué (état err-disabled) à cause du compteur de petites trames
! peut être débloqué automatiquement par le recovery
Switch(config)# errdisable recovery cause small-frame

! Indique le temps (en secondes) au bout duquel l'interface sort de l'état d'erreur
Switch(config)# errdisable recovery interval <300>

! Sélection des interfaces connectées à des postes de travail
Switch(config)# interface range FastEthernet <0/6-42>

! Définition du taux (en paquets par seconde) maximum de trames de petite taille
Switch(config-if-range)# small-frame violation-rate <10000>
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

8.6 Protocol storm protection

Sur certains commutateurs, il est possible de limiter le nombre des paquets par seconde des protocoles ARP, DHCP et IGMP afin de se protéger contre des attaques en déni de service s'appuyant sur ces protocoles.

R43

Limiter le nombre de paquets par seconde des protocoles ARP, DHCP et IGMP.

Exemple de configuration de la protection contre les tempêtes de paquets ARP, DHCP et IGMP :

Exemple Cisco IOS

```
! Limitation du nombre de paquets DHCP à X par seconde
Switch(config)# psp dhcp pps <X>

! Limitation du nombre de paquets ARP à Y par seconde
Switch(config)# psp arp pps <Y>

! Limitation du nombre de paquets IGMP à Z par seconde
Switch(config)# psp igmp pps <Z>
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

8.7 Protection contre les trames indésirables (*port blocking*)

Les commutateurs offrent des mécanismes qui permettent de se protéger contre certains types de trame Ethernet qui peuvent être considérés comme nuisibles sur le réseau, comme par exemple les trames *multicast* et *unicast* à destination d'adresses MAC inconnues du commutateur (adresses absentes de la table MAC).



Ces mécanismes bloquent uniquement les trames qui ne contiennent pas de paquets IP, c'est-à-dire des trames purement de niveau 2. Dans certains contextes d'utilisation comme celui de réseaux n'utilisant que du niveau 2 mais pas de niveau 3, la mise en place de ces mécanismes peut se révéler incompatible et causer d'importants problèmes de connectivité réseau.

R44

Afin de limiter la pollution réseau de niveau 2 sur les commutateurs, il est utile d'activer la protection contre les trames indésirables.

Exemple de configuration de la protection :

Exemple Cisco IOS

```
! Blocage des trames unicast et multicast à destination d'adresses MAC inconnues du
! commutateur sur tous ses ports
Switch(config)# interface range FastEthernet <0/1-42>
Switch(config-if-range)# switchport block unicast
Switch(config-if-range)# switchport block multicast
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

9 Synchronisation horaire et horodatage

La mise en place d'une politique de journalisation nécessite de configurer au préalable les paramètres de synchronisation horaire, comme le précise la note technique [NT LOG] relative à la journalisation publiée par l'ANSSI.

9.1 Synchronisation horaire

Il est possible d'utiliser le protocole [NTP](#) pour la synchronisation horaire des commutateurs afin de garantir une cohérence de l'heure au sein du SI.

R45

Synchroniser l'heure des commutateurs de son système d'information de manière automatisée afin de garantir une cohérence de l'heure de ses équipements. Utiliser si possible plusieurs sources de temps situées au sein du système d'information.

Exemple de configuration des sources de synchronisation horaire :

Exemple Cisco IOS

```
! Active la synchronisation horaire et précise l'adresse IP du serveur de temps sur  
! lequel se synchroniser. Deux serveurs de temps sont configurés ici.  
Switch(config)# ntp server <ntp-server-ip-address-1>  
Switch(config)# ntp server <ntp-server-ip-address-2>
```

Exemple HP Comware 5

```
# Active la synchronisation horaire et précise l'adresse IP du serveur de temps sur  
# lequel se synchroniser. Deux serveurs de temps sont configurés ici.  
[Switch]ntp-service unicast-server <ntp-server-ip-address-1>  
[Switch]ntp-service unicast-server <ntp-server-ip-address-2>
```

Une bonne pratique est de ne pas faire circuler les flux de synchronisation horaire sur les réseaux métier. Une solution est de leur faire emprunter le réseau d'administration.

R46

Synchroniser l'heure des commutateurs en faisant transiter les flux de synchronisation horaire sur un réseau différent des réseaux métier, par exemple le réseau d'administration.

Pour configurer le commutateur ainsi, préciser dans sa configuration que le protocole NTP doit utiliser le VLAN d'administration.

Exemple de configuration de l'adresse source utilisée pour le service NTP :

Exemple Cisco IOS

```
! Définit l'adresse IP source utilisée par le protocole NTP. Est choisie ici l'adresse IP  
! située dans le VLAN d'administration.  
Switch(config)# ntp source vlan <admin-vlan-number>
```

Exemple HP Comware 5

```
# Définit l'adresse IP source utilisée par le protocole NTP. Est choisie ici l'adresse IP  
# située dans le VLAN d'administration.  
[Switch]ntp-service source-interface Vlan-interface <admin-vlan-number>
```

9.2 Horodatage des événements journalisés

Les commutateurs n'horodatent généralement pas les événements de journalisation par défaut mais supportent cette option. Activer cette fonctionnalité se révèle indispensable dans la mise en place d'une politique de journalisation globale et cohérente au sein d'un SI.

R47

Activer l'horodatage des événements journalisés sur les commutateurs. Cet horodatage doit contenir les informations nécessaires pour maintenir une cohérence temporelle entre ces événements quelle que soit la répartition géographique du système d'information.

Dans le cadre d'architectures réparties dans le monde entier, un horodatage avec l'heure locale en précisant le fuseau horaire permet de garder la cohérence nécessaire à l'exploitation des journaux. Cela implique que le fuseau horaire soit correctement configuré sur le commutateur.

Exemple de configuration :

Exemple Cisco IOS

```
! Active l'horodatage des événements journalisés en précisant l'heure locale  
! et le fuseau horaire.  
Switch(config)# service timestamps log datetime localtime show-timezone
```

Exemple HP Comware 5

```
# Active l'horodatage des événements journalisés en précisant l'heure locale  
[Switch]info-center timestamp log date
```

10 Journalisation

La journalisation fait partie intégrante de la SSI. C'est une fonctionnalité indispensable à la détection de comportements anormaux, ainsi qu'aux recherches de compromission a posteriori.

Les recommandations faites dans cette partie sont une déclinaison de celles mentionnées dans la note technique [NT LOG] publiée par l'ANSSI relative à la journalisation.

10.1 Niveau de journalisation

Les commutateurs permettent généralement de filtrer le niveau de gravité des événements à journaliser. Ceci limite la quantité d'événements à sauvegarder localement sur l'équipement, à envoyer à un serveur **syslog** centralisé ou à afficher dans la console ou dans le terminal.

R48

Régler le niveau de journalisation des commutateurs pour l'adapter aux besoins de journalisation du SI.



La configuration du niveau de journalisation se fait lors de la configuration des différents mécanismes de journalisation du commutateur.

10.2 Centralisation des journaux

La centralisation des journaux est une bonne pratique de sécurité des SI. En effet, elle rend plus aisée l'exploitation des informations qu'ils contiennent à des fins d'analyse ou de détection. Cela permet aussi de conserver une copie des journaux en cas d'effacement de ceux-ci sur la machine qui les a générés. L'envoi des événements journalisés au serveur de collecte se fait généralement sous la forme de messages au format syslog.

R49

Activer l'envoi des journaux du commutateur vers un serveur de collecte.

Exemple de configuration de la fonction d'envoi des journaux :

Exemple Cisco IOS

```
! Définit l'adresse du serveur syslog auquel envoyer les événements journalisés
Switch(config)# logging <172.16.1.1>

! Envoie les événements de journalisation au serveur syslog si le niveau de gravité
! est supérieur ou égal à notification
Switch(config)# logging trap notifications
```

Exemple HP Comware 5

```
# Définit l'adresse du serveur syslog auquel envoyer les événements journalisés
[Switch]info-center loghost <172.16.1.1>

# Envoie les événements de journalisation au serveur syslog si le niveau de gravité
# est supérieur ou égal à notification
[Switch]info-center source default channel loghost log level notifications
```

Une bonne pratique de SSI concernant la remontée des événements de journalisation est de les faire transiter par le réseau d'administration. En effet, ces flux contiennent souvent des informations sensibles, voire des informations à caractère personnel.

R50

Dans le cadre de la centralisation des journaux du commutateur, faire remonter les événements par le réseau d'administration afin d'éviter la fuite d'informations sensibles.

Exemple de configuration de l'adresse source utilisée pour le service syslog :

Exemple Cisco IOS

```
! Définit l'adresse source utilisée pour envoyer les événements au serveur syslog.
! Est choisie ici l'adresse IP correspondant au VLAN d'administration.
Switch(config)# logging source-interface vlan <admin-vlan-number>
```

Exemple HP Comware 5

```
# Définit l'adresse source utilisée pour envoyer les événements au serveur syslog.
# Est choisie ici l'adresse IP correspondant au VLAN d'administration.
[Switch]info-center loghost source Vlan-interface <admin-vlan-number>
```

10.3 Journalisation des commandes de configuration

Certains commutateurs peuvent journaliser les commandes entrées par les administrateurs réseau, informations importantes dans le cadre de la surveillance du SI.

R51

Activer la journalisation des commandes entrées par les administrateurs.

Exemple détaillant comment activer la journalisation des commandes entrées par les administrateurs :

Exemple Cisco IOS

```
! Active la journalisation des commandes de configuration
Switch(config)# archive
```

```
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable

! Limite à 1000 le nombre de commandes sauvegardées
Switch(config-archive-log-cfg)# logging size <1000>

! Empêche de journaliser les mots de passe
Switch(config-archive-log-cfg)# hidekeys

! Envoie les événements journalisés au serveur syslog
Switch(config-archive-log-cfg)# notify syslog
```



Pour les commutateurs HP, la commande se trouve dans l'exemple de configuration du paragraphe 4.4.

10.4 Cache

Sur certains commutateurs, il est possible de configurer la taille du cache alloué à la journalisation. Ceci permet d'augmenter la quantité d'événements que l'équipement peut garder en mémoire vive en cas de perte prolongée de la connectivité avec le collecteur de journaux, réduisant ainsi le risque de perte d'événements.

R52

Augmenter la taille du cache dédié à la journalisation tout en veillant à ne pas affecter les performances des commutateurs de manière notable.

La commande ci-dessous donnée en exemple permet de configurer un cache de 32 ko, ce qui permet de conserver environ 400 messages, contre 50 messages environ avec le cache par défaut d'un Cisco Catalyst 2960 :

Exemple Cisco IOS

```
! Limite la taille du cache pour les événements journalisés à 32 ko
Switch(config)# logging buffered <32000>
```

Exemple HP Comware 5

```
# Limite la taille du cache pour les événements journalisés à 400 messages
[Switch]info-center logbuffer size <400>

# Ne met en cache que les événements de niveau de gravité supérieur ou égal à
# notification
[Switch]info-center source default channel logbuffer log level notifications
```

10.5 Stockage des journaux

Les commutateurs peuvent stocker localement les événements de journalisation. Ceci permet de conserver une copie locale des journaux en cas de perte de la connectivité avec le serveur de collecte

des journaux.

R53

Activer le stockage local des événements journalisés. Adapter la taille du journal à la quantité d'événements qu'il est estimé nécessaire de conserver localement et à la quantité d'espace disque disponible sur l'équipement.

En configurant la taille du journal à 1 Mo, il est possible de stocker sur l'équipement un peu plus de 12 000 événements. Voir l'exemple ci-dessous :

Exemple Cisco IOS

```
! Active la journalisation locale dans le fichier flash:syslog avec une limite de taille
! à 1 Mo et en ne sauvegardant que les événements dont le niveau de gravité est supérieur
! ou égal à notifications
Switch(config)# logging file <flash:syslog> <1000000> notifications
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

10.6 Console et terminal

Il est possible d'afficher les événements de journalisation directement sur la console¹³ (connexion en port console) ou sur le terminal (connexion en SSH). Cela donne à l'administrateur réseau une vision en temps réel de la prise en compte des paramètres de configuration du commutateur et de son activité. Afin de n'afficher que les messages importants, il est utile de filtrer leur affichage.

R54

Si la fonction d'affichage des événements de journalisation sur la console et/ou sur le terminal est activée, filtrer les événements affichés afin de réduire la pollution visuelle due à des événements d'importance mineure. Si elle n'est pas jugée utile, la désactiver pour préserver les ressources du commutateur.

Les commandes données ci-dessous en exemple limitent l'affichage aux seuls événements dont le niveau de gravité est supérieur ou égal à **notifications** :

Exemple Cisco IOS

```
! Affiche les événements sur la console si le niveau de gravité est supérieur
! ou égal à notification
Switch(config)# logging console notifications

! Affiche les événements sur le terminal si le niveau de gravité est supérieur
! ou égal à notification
Switch(config)# logging monitor notifications
```

Exemple HP Comware 5

```
# Affiche les événements sur la console si le niveau de gravité est supérieur
# ou égal à notification
[Switch]info-center source default channel console log level notifications state on
```

13. Cette fonctionnalité est en général activée par défaut.

```
# Affiche les événements sur le terminal si le niveau de gravité est supérieur
# ou égal à notification
[Switch]info-center source default channel monitor log level notifications state on
```

Les commandes ci-dessous désactivent l'affichage des événements :

Exemple Cisco IOS

```
! Désactive l'affichage des événements sur la console
Switch(config)# no logging console

! Désactive l'affichage des événements sur le terminal
Switch(config)# no logging monitor
```

Exemple HP Comware 5

```
# Désactive l'affichage des événements sur la console
[Switch]info-center source default channel console log level notifications state off

# Désactive l'affichage des événements sur le terminal
[Switch]info-center source default channel monitor log level notifications state off
```

10.7 Particularité de la console

La survenue d'un grand nombre d'événements système ou réseau au niveau du commutateur peut entraîner la génération de nombreux événements en peu de temps. Sachant que tous les messages écrits sur la console causent des interruptions de CPU, une grande quantité d'événements à afficher sur la console en peu de temps peut affecter de façon notable le fonctionnement du commutateur. Il est donc important de limiter le nombre d'événements journalisés affichés sur la console.

R55

Limiter le nombre d'événements de journalisation affichés sur la console du commutateur afin d'éviter de perturber son fonctionnement.

Exemple de commande pour limiter le taux d'événements affichés sur la console :

Exemple Cisco IOS

```
! Limite les événements affichés sur la console à 2 événements par seconde, sauf si
! le niveau de gravité est supérieur ou égal à warning
Switch(config)# logging rate-limit console <2> except warnings
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

11 Supervision : SNMP

SNMP est un protocole qui permet de transmettre des informations concernant l'état d'un équipement à un équipement de supervision (mode *get* ou mode *trap*), ou de configurer un équipement client depuis un serveur de gestion (mode *set*). Sachant que le protocole SNMP est par nature moins

sécurisé que les protocoles d'administration de type SSH ou HTTPS, l'utilisation du mode *set* est à proscrire¹⁴.

R56

Ne pas utiliser le protocole SNMP en mode *set* pour administrer les commutateurs.

En plus d'interdire l'utilisation du mode *set*, il est possible de journaliser les tentatives d'utilisation.

Exemple de journalisation des commandes *set* :

Exemple HP Comware 5

```
# Journalise les opération de type set
[Switch]snmp-agent log set-operation
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur Cisco.

Il existe plusieurs versions du protocole SNMP qui ont chacune apporté leurs améliorations. Les deux versions de SNMP principalement utilisées sont SNMPv2c et SNMPv3, elles sont donc traitées dans cette section. Il faut toutefois noter que la version 3 est à privilégier car elle apporte, en plus de l'authentification des équipements entre eux, la protection en confidentialité des flux SNMP (mode SNMPv3 AuthPriv).

R57

Utiliser SNMP en version 3 AuthPriv.

R57-

Si cela n'est pas possible techniquement, utiliser à défaut la version 2c.

Il existe deux méthodes pour communiquer des informations par SNMP :

- le **mode *get*** : le serveur SNMP va initier la connexion vers l'agent de la machine cible (ici, le commutateur) pour récupérer des informations sur son état ;
- le **mode *trap*** : la machine cliente (ici, le commutateur) va notifier le serveur SNMP au moyen de messages SNMP appelés *traps* (paquets UDP spécifiques) lors de la survenue d'événements significatifs.

Le mot *trap*, utilisé au sens large, comprend en réalité deux types de *trap* : les *trap* et les *inform*. À la différence du *trap*, le *inform* déclenche l'envoi par le serveur SNMP d'une confirmation de réception. Le mode *inform* est ainsi plus fiable que le mode *trap* et est donc à privilégier¹⁵.

R58

Lorsqu'il existe, il est recommandé d'utiliser le service *trap* en mode *inform*.

14. Il est possible d'empêcher l'utilisation du mode *set* en ne donnant que des autorisations d'accès en lecture seule.

15. Les configurations données en exemple dans les paragraphes suivants respectent cette préférence.

De plus, afin de garantir un réel niveau de sécurité, la cryptographie employée par le service SNMP doit respecter certaines contraintes en matière de protocoles et tailles de clés employés.

R59

La configuration du service SNMP doit, sauf contrainte très particulière, respecter les recommandations cryptographiques détaillées dans l'annexe B du RGS.

Une partie de la sécurité du protocole SNMP repose sur l'utilisation de mots de passe. Afin de respecter les bonnes pratiques quant au choix des mots de passe, se référer à la note technique [NT MdP] relative à la sécurité des mots de passe publiée par l'ANSSI.

11.1 SNMPv3

Ce paragraphe décrit comment configurer SNMPv3.

11.1.1 Mode *get*

Exemple de configuration de SNMP en mode *get* :

Exemple Cisco IOS

```
! Renseigne l'identifiant SNMP de la machine émettrice des gets
Switch(config)# snmp-server engineID remote <snmp-server-ip-address>
<snmp-server-engineID>

! Déclare la MIB nommée MIB-2
Switch(config)# snmp-server view <mib-2> mib-2 included

! Définit le groupe et le niveau de sécurisation
Switch(config)# snmp-server group <snmp-group> v3 priv read <mib-2>

! Définit l'utilisateur SNMP et les paramètres de sécurité associés
Switch(config)# snmp-server user <snmp-user> <snmp-group> v3 auth sha <auth-password>
priv aes 256 <priv-key>

! Active la persistance des index des interfaces
Switch(config)# snmp ifmib ifindex persist
```

Exemple pour un commutateur HP :

Exemple HP Comware 5

```
# Déclare la MIB nommée MIB-2
[Switch]snmp-agent mib-view included <mib-2> <1.3.6.1.2.1>

# Supprime la MIB par défaut
[Switch]undo snmp-agent mib-view ViewDefault

# Définit le groupe et le niveau de sécurisation
[Switch]snmp-agent sys-info version v3
[Switch]snmp-agent group v3 <snmp-group> privacy read-view <mib-2>

# Définit l'utilisateur SNMP et les paramètres de sécurité associés
[Switch]snmp-agent usm-user v3 <snmp-user> <snmp-group> authentication-mode sha
<auth-password> privacy-mode aes128 <priv-key>
```

11.1.2 Mode *trap*

Exemple de configuration de SNMP en mode *trap* :

Exemple Cisco IOS

```
! Renseigne l'identifiant SNMP de la machine destination des traps
Switch(config)# snmp-server engineID remote <snmp-server-ip-address>
<snmp-server-engineID>

! Déclare la MIB nommée MIB-2
Switch(config)# snmp-server view <mib-2> mib-2 included

! Définit le groupe et le niveau de sécurisation
Switch(config)# snmp-server group <snmp-group> v3 priv read <mib-2>

! Définit l'utilisateur SNMP et les paramètres de sécurité associés
Switch(config)# snmp-server user <snmp-user> <snmp-group> v3 auth sha <auth-password>
priv aes 256 <priv-key>

! Définit le serveur destination des traps, précise le mode inform, la version, le niveau
! de sécurisation et le nom d'utilisateur
Switch(config)# snmp-server host <snmp-server-ip-address> informs version 3 priv
<snmp-user>

! Active l'envoi des traps
Switch(config)# snmp-server enable traps

! Limite le nombre d'envois de messages informs
Switch(config)# snmp-server inform retries <0>

! Les paquets seront envoyés depuis l'adresse IP du vlan d'administration
Switch(config)# snmp-server trap-source vlan <admin-vlan>

! Active la persistance des index des interfaces
Switch(config)# snmp ifmib ifindex persist
```

Exemple HP Comware 5

```
# Déclare la MIB nommée MIB-2
[Switch]snmp-agent mib-view included <mib-2> <1.3.6.1.2.1>

# Supprime la MIB par défaut
[Switch]undo snmp-agent mib-view ViewDefault

# Définit le groupe et le niveau de sécurisation
[Switch]snmp-agent sys-info version v3
[Switch]snmp-agent group v3 <snmp-group> privacy read-view <mib-2>

# Définit l'utilisateur SNMP et les paramètres de sécurité associés
[Switch]snmp-agent usm-user v3 <snmp-user> <snmp-group> authentication-mode sha
<auth-password> privacy-mode aes128 <priv-key>

# Définit le serveur destination des traps, la version, le niveau de sécurisation
# et le nom d'utilisateur
[Switch]snmp-agent target-host trap address udp-domain <snmp-server-ip-address> params
securityname <snmp-user> v3 privacy

# Active l'envoi des traps
[Switch]snmp-agent trap enable

# Les paquets seront envoyés depuis l'adresse IP du vlan d'administration
[Switch]snmp-agent trap source Vlan-interface <admin-vlan>
```



La description d'une fonction équivalente aux *inform* n'a pas été trouvée dans la documentation du commutateur HP.

11.2 SNMPv2c

Ce paragraphe décrit comment configurer SNMPv2c.

11.2.1 Mode *get*

Exemple de configuration de SNMP en mode *get* :

Exemple Cisco IOS

```
! Renseigne l'identifiant SNMP de la machine émettrice des gets
Switch(config)# snmp-server engineID remote <snmp-server-ip-address>
<snmp-server-engineID>

! Déclare la MIB nommée MIB-2
Switch(config)# snmp-server view <mib-2> mib-2 included

! Définit le groupe et le niveau de sécurisation
Switch(config)# snmp-server group <snmp-group> v2c read <mib-2>

! Définit l'utilisateur SNMP et les paramètres de sécurité associés
Switch(config)# snmp-server user <snmp-user> <snmp-group> v2c auth sha <auth-password>

! Active la persistance des index des interfaces
Switch(config)# snmp ifmib ifindex persist
```

Exemple HP Comware 5

```
# Déclare la MIB nommée MIB-2
[Switch]snmp-agent mib-view included <mib-2> <1.3.6.1.2.1>

# Supprime la MIB par défaut
[Switch]undo snmp-agent mib-view ViewDefault

# Définit le groupe et le niveau de sécurisation
[Switch]snmp-agent sys-info version v2c
[Switch]snmp-agent group v2c <snmp-group> read-view <mib-2>

# Définit l'utilisateur SNMP et les paramètres de sécurité associés
[Switch]snmp-agent usm-user v2c <snmp-user> <snmp-group>
```

11.2.2 Mode *trap*

Exemple de configuration de SNMP en mode *trap* :

Exemple Cisco IOS

```
! Renseigne l'identifiant SNMP de la machine destination des traps
Switch(config)# snmp-server engineID remote <snmp-server-ip-address>
<snmp-server-engineID>

! Déclare la MIB nommée MIB-2
Switch(config)# snmp-server view <mib-2> mib-2 included

! Définit le groupe et le niveau de sécurisation
Switch(config)# snmp-server group <snmp-group> v2c read <mib-2>

! Définit l'utilisateur SNMP et les paramètres de sécurité associés
Switch(config)# snmp-server user <snmp-user> <snmp-group> v2c auth sha <auth-password>

! Définit le serveur destination des traps, précise le mode informs, la version,
! le niveau de sécurisation et le nom d'utilisateur
Switch(config)# snmp-server host <snmp-server-ip-address> informs version 2c
<snmp-community>
```

```

! Active l'envoi des traps
Switch(config)# snmp-server enable traps

! Limite le nombre d'envois de messages informs
Switch(config)# snmp-server inform retries <0>

! Les paquets seront envoyés depuis l'adresse IP du vlan d'administration
Switch(config)# snmp-server trap-source vlan <admin-vlan>

! Active la persistance des index des interfaces
Switch(config)# snmp ifmib ifindex persist

```

Exemple HP Comware 5

```

# Déclare la MIB nommée MIB-2
[Switch]snmp-agent mib-view included <mib-2> <1.3.6.1.2.1>

# Supprime la MIB par défaut
[Switch]undo snmp-agent mib-view ViewDefault

# Définit le groupe et le niveau de sécurisation
[Switch]snmp-agent sys-info version v2c
[Switch]snmp-agent group v2c <snmp-group> read-view <mib-2>

# Définit l'utilisateur SNMP et les paramètres de sécurité associés
[Switch]snmp-agent usm-user v2c <snmp-user> <snmp-group>

# Définit le serveur destination des traps, la version, le niveau de sécurisation
# et le nom d'utilisateur
[Switch]snmp-agent target-host trap address udp-domain <snmp-server-ip-address> params
securityname <snmp-user> v2c

# Active l'envoi des traps
[Switch]snmp-agent trap enable

# Les paquets seront envoyés depuis l'adresse IP du vlan d'administration
[Switch]snmp-agent trap source Vlan-interface <admin-vlan>

```

12 Agrégation des liens

Il est possible de mettre en place une agrégation de liens afin de répartir le trafic entre un commutateur de desserte et un commutateur de distribution sur l'ensemble des liens agrégés ou de redonder ce lien pour pallier une éventuelle perte de connectivité réseau. Ceci consiste à regrouper plusieurs interfaces physiques sous une unique interface logique. Il existe plusieurs protocoles permettant de mettre en place cette fonctionnalité, parmi lesquels le protocole [LACP](#) dont la mise en place est détaillée ci-après.

Le schéma ci-dessous représente un exemple d'agrégation de liens entre un commutateur de distribution (SW1) et deux commutateurs de desserte (SW1-1 et SW1-2) :

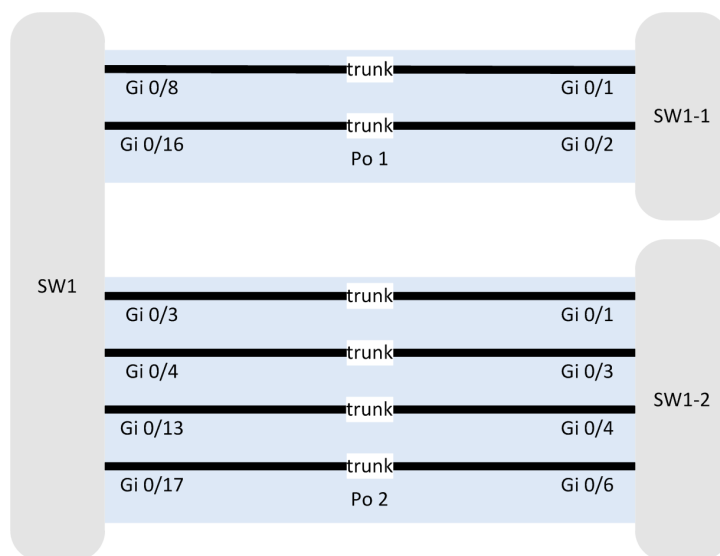


FIGURE 3 – Exemple d'*EtherChannel*

Po 1 et Po 2 sont deux interfaces logiques regroupant respectivement, en considérant le commutateur SW1 :

- pour l'interface logique Po 1, les interfaces physiques Gi 0/8 et Gi 0/16 ;
- pour l'interface logique Po 2, les interfaces physiques Gi 0/3, Gi 0/4, Gi 0/13 et Gi 0/17.

Il faut garder à l'esprit que ces protocoles ne permettent pas de garantir une répartition idéale des flux entre les interfaces physiques regroupées sous la même interface logique de par la nature des algorithmes qu'ils utilisent. Un flux réseau ne sera pas réparti entre plusieurs interfaces physiques même s'il occupe une part importante de la bande passante.

De plus, une attention toute particulière doit être portée sur le choix des interfaces lors des modifications de configuration. En effet, les paramètres saisis au niveau de l'interface logique sont pris en compte par toutes les interfaces physiques qui lui sont liées alors que des modifications de configuration apportées au niveau d'une interface physique n'affectent que celle-ci. Ainsi, certains services ou protocoles utilisés par le commutateur seront à configurer en considérant l'interface logique et non les interfaces physiques qui la composent au risque de causer des erreurs et instabilités.



LACP agit notamment sur les fonctionnalités CDP et DTP. Il est recommandé de lire la documentation constructeur afin d'éviter les instabilités réseau.

R60

Afin d'augmenter la bande passante ou d'assurer une redondance sur les liens réseau entre les commutateurs de desserte et de distribution, il est recommandé de mettre en place l'agrégation de lien (aussi appelée *EtherChannel* ou *Bridge Aggregation*).

Sur les commutateurs Cisco, LACP propose différentes méthodes de configuration des ports. Il est recommandé de procéder à la configuration manuelle des ports en mode *passive* ou *active*.



Lorsqu'un port est configuré en mode *passive* ou *active*, le port du commutateur situé à l'extrémité du câble doit être configuré dans le mode inverse.

L'exemple présenté ci-dessous¹⁶ est dans le cas d'un commutateur de desserte relié à un commutateur de distribution par deux liens physiques :

Exemple Cisco IOS

```
! Sélectionne les interfaces qui font partie du EtherChannel
Switch(config)# interface range FastEthernet <0/7-8>

! Configure les deux interfaces comme un port trunk
Switch(config-if-range)# switchport mode trunk

! Assigne les ports au channel group X en mode passif (il faut que le commutateur de
! l'autre côté soit en mode actif ; si ce n'est pas le cas, configurer celui-ci en
! mode actif)
Switch(config-if-range)# channel-group <X> mode passive
```

Une fois qu'un *EtherChannel* a été créé, cette interface est configurable avec la commande donnée en exemple ci-dessous :

Exemple Cisco IOS

```
! Sélectionne l'EtherChannel 3
Switch(config)# interface port-channel 3
```



Par défaut, LACP répartit le trafic selon les adresses MAC source des machines. Ce comportement peut être modifié si nécessaire afin, par exemple, d'utiliser les ports TCP ou UDP comme discriminants en combinaison, ou à la place, des adresses MAC source. Il est alors nécessaire de connaître le type de services fournis aux utilisateurs du SI afin de mieux paramétrer les liens de type *EtherChannel*.

Concernant les commutateurs HP, le terme *Bridge Aggregation* remplace le terme *EtherChannel* de Cisco. Ci-dessous l'équivalent de la configuration précédente pour un commutateur HP :

Exemple HP Comware 5

```
# Sélectionne les interfaces qui font partie du EtherChannel
[Switch]interface Bridge-Aggregation X
[Switch]quit
[Switch-Bridge-AggregationX]interface range GigabitEthernet 1/0/7 GigabitEthernet 1/0/8
[Switch-if-range]port link-aggregation group X
[Switch]quit

# Configure les deux interfaces comme un port trunk
[Switch]interface Bridge-Aggregation X
[Switch-Bridge-AggregationX]port link-type trunk

# Assigne les ports au channel group X en mode dynamique
[Switch-Bridge-AggregationX]link-aggregation mode dynamic
```

16. Pour des cas plus complexes comme la mise en place d'un *EtherChannel* de plus de 8 ports ou l'utilisation du *Stacking* ou du *Link-State Tracking*, se référer à la documentation constructeur.

Une fois qu'un *Bridge Aggregation* a été créé, cette interface est configurable avec la commande donnée en exemple ci-dessous :

Exemple HP Comware 5

```
# Sélectionne le Bridge Aggregation 3  
[Switch]interface Bridge-Aggregation 3
```

13 Gestion du parc et MCO/MCS

Afin de garantir des conditions de **MCO** et de **MCS** correctes, les administrateurs réseau doivent respecter les règles d'administration et de maintenance traitées dans cette section.

13.1 Homogénéité des équipements et des versions de système d'exploitation

De manière générale, il est plus facile d'administrer un parc de commutateurs dont les configurations matérielles et logicielles sont proches, voire identiques. Cela facilite le travail des équipes techniques, réduisant les erreurs de configuration et améliorant mécaniquement le MCO/MCS des équipements. À noter que des équipements qui doivent supporter des charges de trafic différentes ne sont pas nécessairement les mêmes, mais homogénéiser les versions des systèmes d'exploitation embarqués sur ceux-ci facilite tout de même leur exploitation car ils proposeront vraisemblablement les mêmes fonctionnalités et ils utiliseront les mêmes lignes de commande.

R61

Homogénéiser les configurations matérielles et logicielles des commutateurs de son système d'information afin de faciliter leur MCO/MCS.

13.2 Système d'exploitation à jour

La mise à jour régulière du système d'exploitation des commutateurs est une première étape dans la prévention des attaques informatiques car des correctifs de sécurité sont intégrés à beaucoup de mises à jour. Cependant, la mise à jour d'un commutateur entraîne son indisponibilité temporaire, le temps que la mise à jour soit effectuée et que les problèmes éventuellement engendrés par cette mise à jour soient résolus. Il faut donc veiller à perturber le moins possible les utilisateurs et les services durant ces mises à jour en procédant par zone ou à des créneaux horaires adaptés. De même, il est déconseillé d'appliquer les mises à jour sans les avoir testées¹⁷ au préalable ou de le faire de manière trop fréquente si celles-ci n'apportent pas de gain significatif en matière de sécurité.

R62

Mettre à jour régulièrement le système d'exploitation des commutateurs afin de les protéger contre les failles de sécurité corrigées par ces mises à jour.

17. Opérer ces tests sur une plateforme de pré-production.

La procédure suivante est conseillée pour la mise à jour des commutateurs :

- sauvegarder la configuration courante du commutateur (sur le poste d'administration) :

```
# Sauvegarde le fichier de configuration du commutateur
user@poste-admin:~> scp <login>@switch-33:flash:config.text ../switch-33/.

# Sauvegarde le fichier de configuration des VLAN du commutateur
user@poste-admin:~> scp <login>@switch-33:flash:vlan.dat ../switch-33/.
```

- créer le répertoire du même nom que la nouvelle image IOS dans la mémoire flash du commutateur (sur le commutateur) :

Exemple Cisco IOS

```
! Crée le répertoire dans lequel va être copiée l'image du nouvel IOS
Switch# mkdir flash:c2960-lanbasek9-mz.150-2.SE9
```

- copier le binaire de la nouvelle image d'IOS vers ce répertoire (depuis le poste d'administration) :

```
# Copie la nouvelle image d'IOS dans le répertoire créée précédemment sur le commutateur
user@poste-admin:~> scp c2960-lanbasek9-mz.150-2.SE9.bin
<login>@switch-33:flash:c2960-lanbasek9-mz.150-2.SE9/c2960-lanbasek9-mz.150-2.SE9.bin
```

- vérifier l'intégrité de l'image du nouvel IOS copié sur le commutateur. Il est préférable de vérifier l'empreinte sha512 de l'image téléchargée en la comparant avec celle fournie par le constructeur sur son site Internet ¹⁸ (sur le commutateur) :

Exemple Cisco IOS

```
! Génère le hash sha512 de l'image du nouvel IOS afin de comparer sa valeur avec celle
! affichée sur le site du constructeur
Switch# verify /sha-512
flash:c2960-lanbasek9-mz.150-2.SE9/c2960-lanbasek9-mz.150-2.SE9.bin
```

- déclarer le nouvel IOS comme système à lancer au démarrage (sur le commutateur) :

Exemple Cisco IOS

```
! Définit l'image d'IOS sur laquelle le commutateur doit démarrer
Switch(config)# boot system
flash:c2960-lanbasek9-mz.150-2.SE9/c2960-lanbasek9-mz.150-2.SE9.bin
```

- vérifier la justesse des paramètres de démarrage, puis redémarrer le commutateur (sur le commutateur) :

Exemple Cisco IOS

```
! Affiche les paramètres de démarrage du commutateur
Switch# show boot

! Redémarre le commutateur (à noter que cela occasionne une interruption de service)
Switch# reload
```

Pour un commutateur HP, la procédure à suivre est la suivante :

- sauvegarder la configuration courante du commutateur (sur le poste d'administration) :

```
# Sauvegarde le fichier de configuration du commutateur
user@poste-admin:~> scp login@switch-33:startup.cfg ../switch-33/.
```

- copier le binaire de la nouvelle image de Comware à la racine de la mémoire flash du commutateur (sur le poste d'administration) :

```
# Copie la nouvelle image Comware dans le répertoire créée précédemment sur le
# commutateur
user@poste-admin:~> scp A5500EI-CMW520-R2221P15.bin
login@switch-33:A5500EI-CMW520-R2221P15.bin
```

18. Historiquement, seules les empreintes md5 des images IOS étaient fournis par Cisco sur le site de téléchargement officiel. Depuis peu, les empreintes au format sha512 sont également fournies.

- déclarer le nouveau Comware comme système à lancer au démarrage (sur le commutateur) :

Exemple HP Comware 5

```
# Définit l'ancienne image de Comware comme image de démarrage de secours
<Switch>boot-loader file flash:/a5500ei-cmw520-r2221p08.bin slot 1 backup

# Définit l'image de Comware sur laquelle le commutateur doit démarrer
<Switch>boot-loader file flash:/a5500ei-cmw520-r2221p15.bin slot 1 main
```

- vérifier la justesse des paramètres de démarrage, puis redémarrer le commutateur (sur le commutateur) :

Exemple HP Comware 5

```
# Affiche les paramètres de démarrage du commutateur
<Switch>display boot-loader

# Redémarre commutateur (à noter que cela occasionne une interruption de service)
<Switch>reboot
```

13.3 Gestion du changement

Il est très important de mettre à jour les configurations des commutateurs lorsque des changements interviennent sur le SI. Par exemple, ne pas désactiver les ports des commutateurs qui ne sont plus utilisés permet à une machine malveillante d'accéder plus facilement au SI.

R63

Veiller à ce que les configurations des commutateurs soient cohérentes avec les modifications effectuées sur le système d'information.

13.4 Centralisation de la gestion des commutateurs

Une gestion centralisée des commutateurs du SI permet de faciliter la gestion du parc d'équipements ainsi que la cohérence des configurations en donnant la possibilité aux administrateurs réseau de connaître et modifier la configuration de chaque commutateur rapidement.

R64

Centraliser l'administration des commutateurs au sein du système d'information.

13.5 Sauvegarde et restauration des configurations

En cas d'erreur de configuration grave ou de défaillance matérielle nécessitant le remplacement d'un commutateur, le retour à l'état précédent cet événement doit pouvoir se faire très rapidement afin de rétablir l'accès au réseau. Ceci nécessite d'avoir une sauvegarde récente de la configuration de l'équipement, mais aussi d'avoir une bonne maîtrise des procédures de restauration (cette maîtrise passe généralement par des tests réguliers de ces procédures).

R65

Mettre en place des sauvegardes distantes, automatiques et régulières des configurations des commutateurs du système d'information.

R66

Tester de façon régulière les procédures de restauration des configurations des équipements.

13.6 Outil de vérification de configuration

Certains outils permettent de vérifier la configuration des commutateurs en effectuant un différentiel entre la configuration actuelle des équipements et leur configuration de référence connue de l'outil. Ceci permet de repérer facilement des modifications de configuration opérées sur des commutateurs afin de retrouver plus facilement les erreurs à l'origine de dysfonctionnements qui peuvent parfois être le signe d'une intrusion sur le SI.

R67

Mettre en place un système de vérification de configuration des commutateurs dans son système d'information.

13.7 Les macros

Les macros sont des séquences de commandes prédéfinies qui peuvent être exécutées à la demande pour automatiser les tâches d'administration les plus fréquentes. Ces objets, présents sur certains commutateurs, peuvent s'avérer très pratiques pour les administrateurs.

R68

Définir des macros pour les opérations récurrentes d'exploitation si le matériel le permet.

Certaines macros sont données en exemple dans l'annexe [A](#) pour les commutateurs Cisco.



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

14 Autres fonctionnalités

14.1 Fonctionnalités à activer

La fonctionnalité de chiffrement des mots de passe contenus dans le fichier de configuration du commutateur permet de les masquer aux personnes indiscrettes.

Pour les commutateurs Cisco, cette fonctionnalité ne concerne pas la commande **username** (utilisée pour créer des comptes locaux) si l'attribut **secret** (qui offre une meilleure robustesse¹⁹) est utilisé, mais s'applique aux autres secrets stockés (par exemple RADIUS ou TACACS+) dans le fichier de configuration. Cependant, étant donné que cette fonction utilise un chiffrement faible, elle ne protège pas efficacement les mots de passe contre des personnes malintentionnées qui possèderaient ces fichiers

19. Le mot de passe étant haché, il est toujours possible pour un attaquant de tenter de retrouver le mot de passe en procédant à une attaque par dictionnaire.

et souhaiteraient retrouver les mots de passe contenus. En effet, le chiffrement est facilement réversible et de nombreux outils disponibles sur Internet permettent de déchiffrer ces mots de passe quasi-instantanément.

Pour les commutateurs HP, le mécanisme équivalent consiste à masquer les mots de passe lors de leur affichage sur l'écran de l'administrateur ainsi que dans le fichier de configuration du commutateur.

R69

Activer le chiffrement des mots de passe contenus dans le fichier de configuration.

Exemple de commande de configuration globale :

Exemple Cisco IOS

```
! Active le chiffrement des mots de passe dans le fichier de configuration
Switch(config)# service password-encryption
```

Pour les commutateurs HP, se référer au paragraphe 4.2.4 qui aborde la notion de *password control*.



Compte-tenu de ce qui est écrit ci-dessus, il est impératif de traiter les fichiers de configuration des commutateurs en tant que fichiers sensibles. Se référer au paragraphe 4.3.3 contenant une recommandation sur le sujet.

14.2 Fonctionnalités à désactiver

Les fonctionnalités suivantes sont généralement activées de base sur un commutateur et doivent être désactivées afin de réduire sa surface d'attaque :

- **la résolution de nom (DNS)** : un commutateur ne requiert pas de service de résolution de nom pour fonctionner, le service DNS doit donc être désactivé ;
- **le protocole CDP** : protocole propriétaire Cisco de découverte réseau. Ce protocole transporte de nombreuses informations intéressantes pour un attaquant (type d'équipement, adresses des agents SNMP, TTL, etc.) sans protection cryptographique ;
- **les serveur et relai DHCP** : un commutateur n'a pas vocation à faire office de serveur DHCP. Cette fonctionnalité proposée par de nombreux commutateurs est donc à proscrire.

R70

En plus des fonctionnalités désactivées dans les autres sections de ce document, il est recommandé de désactiver les fonctionnalités suivantes dans la configuration d'un commutateur de desserte : la résolution de nom, le serveur DHCP, le protocole CDP.

Cependant, si une de ces fonctionnalités est nécessaire au fonctionnement de certains services offerts par le SI, il se peut que cette recommandation ne soit pas applicable dans sa totalité.

Exemple de commandes de configuration globales :

Exemple Cisco IOS

```
! Désactive la résolution de nom
Switch(config)# no ip domain-lookup
```

```
! Désactive le protocole CDP
Switch(config)# no cdp run

! Désactive les serveur et relai DHCP
Switch(config)# no service dhcp
```

Exemple HP Comware 5

```
# Désactive les serveur et relai DHCP
[Switch]undo dhcp enable
```

Exemple de commande de configuration par interface :

Exemple Cisco IOS

```
! Désactive le protocole CDP sur l'interface
Switch(config-if)# no cdp enable
```

15 Disponibilité du système

Outre l'amélioration du niveau de sécurité du commutateur, il est nécessaire de s'assurer que l'équipement a une disponibilité maximale. Ainsi, certaines mesures prises en avance de phase permettent de garantir une meilleure disponibilité du système.

R71

Prendre des mesures préventives contre les problèmes de disponibilité du commutateur en agissant au niveau des ressources mémoire et processeur.

15.1 Gestion du CPU

Il est possible, par le biais de certains paramètres de configuration, de mettre en place une supervision de l'utilisation du processeur du commutateur afin de détecter un possible dysfonctionnement, mais aussi de s'assurer qu'il résistera mieux à des tentatives de déni de service. Les paramètres donnés en exemple ci-dessous configurent un commutateur Cisco de manière à ce qu'il remonte des informations de sur-utilisation du processeur au serveur SNMP sous forme de *traps* :

Exemple Cisco IOS

```
! Génère un trap SNMP quand l'utilisation du processeur dépasse un certain seuil
Switch(config)# snmp-server enable traps cpu threshold

! Définition du seuil de déclenchement de l'envoi d'un trap
Switch(config)# process cpu threshold type total rising <pourcentage> interval
<temps (s)>

! Déclaration du serveur SNMP à utiliser pour envoyer les traps en rapport avec
! l'utilisation du processeur
Switch(config)# snmp-server host <snmp-server-ip-address> <nom d'utilisateur SNMPv3> cpu
```

Les paramètres de configuration donnés en exemple ci-dessous permettent de protéger un commutateur Cisco des attaques en déni de service de type *flooding* en réservant un minimum de temps processeur aux processus de faible priorité :

Exemple Cisco IOS

```
! Définit un temps de 500 ms maximum avant d'exécuter le processus de
! plus faible priorité
Switch(config)# scheduler interval 500
```



Le fonctionnement est sensiblement le même sur les commutateurs de la marque HP, à la différence près que ces paramètres sont déterminés par le système et ne sont pas paramétrables.

15.2 Gestion de la mémoire

De même que pour le CPU, il est possible de superviser la mémoire du commutateur afin de détecter l'apparition de problèmes de disponibilité liés à la mémoire. De plus, une partie de la mémoire peut être réservée afin d'assurer l'envoi des événements de journalisation au serveur syslog.

Génération d'un événement journalisé quand un certain seuil bas est atteint sur un commutateur Cisco :

Exemple Cisco IOS

```
! Définit le seuil bas de mémoire processeur disponible qui déclenche une notification
! syslog
Switch(config)# memory free low-watermark processor <seuil bas de mémoire (Ko)>

! Définit le seuil bas de mémoire I/O disponible qui déclenche une notification syslog
Switch(config)# memory free low-watermark io <seuil bas de mémoire (Ko)>
```

Réserve une partie de la mémoire pour assurer la génération des événements de journalisation critiques :

Exemple Cisco IOS

```
! Réserve 1 Mo de mémoire pour l'envoi des notifications
Switch(config)# memory reserve critical <1000>
```



Le fonctionnement est sensiblement le même sur les commutateurs de la marque HP, à la différence près que ces paramètres sont déterminés par le système et ne sont pas configurables.

15.3 Gestion des connexions TCP

Sur un commutateur, seule l'interface d'administration doit disposer de services en écoute sur le réseau. Malgré cela, le commutateur est potentiellement exposé à des attaques de type *SYN Flood*²⁰, il est possible d'augmenter sa résilience face à des attaques de ce type. L'exemple ci-dessous permet de se protéger contre les attaques de types *SYN Flood* en définissant un temps maximum d'attente lors de l'établissement d'une connexion TCP :

Exemple Cisco IOS

```
! Définit le temps d'attente maximum lors de l'établissement d'une connexion TCP
Switch(config)# ip tcp synwait-time 10
```

Exemple HP Comware 5

```
# Définit le temps d'attente maximum lors de l'établissement d'une connexion TCP
[Switch]tcp timer syn-timeout 10
```

20. *SYN Flood* : Attaque consistant à initier un très grand nombre de connexions TCP sans les fermer afin de provoquer un déni de service par saturation du nombre de connexions TCP ouvertes.


```
# Active la protection SYN cookie
[Switch]tcp syn-cookie enable
```

15.4 Interface Null0

L'interface Null0 est une interface particulière créée par défaut sur le commutateur, toujours active, qui ne peut ni recevoir ni transmettre du trafic. Elle est utilisée en tant que destination du trafic à défausser par les mécanismes de filtrage intégrés au commutateur. Par défaut, une trame envoyée sur cette interface déclenche l'envoi par le commutateur d'un message ICMP de type 3 (destinataire inaccessible) à la source de la trame. Il est possible de désactiver l'envoi de cette réponse ICMP afin d'économiser les ressources du commutateur. La trame sera alors défaussée de manière silencieuse, la machine à l'origine de la trame défaussée n'aura pas d'information sur la cause de cette défausse.

L'exemple ci-dessous désactive l'envoi de messages ICMP de type 3 par un commutateur Cisco en réponse aux trames envoyées sur l'interface Null0, ceci afin d'économiser de la ressource CPU :

Exemple Cisco IOS

```
! Désactive l'envoi de messages ICMP unreachable par le commutateur pour l'interface
Null0
Switch(config)# interface Null0
Switch(config-if)# no ip unreachable
```



La description d'une fonction équivalente n'a pas été trouvée dans la documentation du commutateur HP.

Annexes

A Les macros

A.1 Exemples de macros Cisco

A.1.1 Création de la macro : désactivation d'un port inutilisé

C'est une macro à exécuter lors de la libération d'un port du commutateur. Cette macro va éteindre le port, supprimer son adresse IP s'il en a une, puis le placer dans le VLAN de quarantaine.

Exemple de création d'une macro de désactivation d'un port inutilisé :

Exemple Cisco IOS

```
! Création de la macro nommée port_inutilise
Switch(config)# macro name <port_inutilise>

! Description de la macro
macro description <Port inutilise>

! Eteint l'interface
shutdown

! Désactive le protocole VTP sur l'interface
no vtp

! Désactive le protocole CDP sur l'interface
no cdp enable
```

```

! Limite le nombre de paquets DHCP à 10 par seconde sur l'interface
ip dhcp snooping limit rate <10>

! Active l'IP Source Guard sur l'interface
ip verify source

! Force le mode access
switchport mode access

! Désactive l'émission de trames DTP
switchport nonegotiate

! Placement de l'interfaces dans le VLAN de quarantaine (ici 666)
switchport access vlan <666>

! Supprime la description de la macro exécutée dans la configuration de l'interface
no macro description
@

```

A.1.2 Création de la macro : port *access*

Cette macro regroupe les commandes communes à la configuration de tous les ports de type *access*.

Exemple de création d'une macro à exécuter lors de la création d'un port *access* :

Exemple Cisco IOS

```

! Création de la macro nommée port_access
Switch(config)# macro name <port_access>

! Description de la macro
macro description <Port Access>

! Désactive le protocole VTP sur l'interface
no vtp

! Désactive le protocole CDP sur l'interface
no cdp enable

! Force le mode access
switchport mode access

! Désactive l'émission de trames DTP
switchport nonegotiate

! Active le Protected Port
switchport protected

! Force le port d'accès en mode forwarding (au sens Spanning Tree)
spanning-tree portfast

! Blocage des trafics unicast et multicast sur l'interface
switchport block unicast
switchport block multicast

! Supprime la description de la macro exécutée dans la configuration de l'interface
no macro description
@

```

A.1.3 Création de la macro : port *trunk*

Cette macro regroupe les commandes communes à la configuration de tous les ports de type *trunk*.

Exemple de création d'une macro à exécuter lors de la création d'un port *trunk* :

Exemple Cisco IOS

```

! Création de la macro nommée port_trunk
Switch(config)# macro name <port_trunk>

! Description de la macro
macro description <Port Trunk>

! Désactive le protocole VTP sur l'interface
no vtp

! Désactive le protocole CDP sur l'interface
no cdp enable

! Force le mode trunk
switchport mode trunk

! Désactive l'émission de trames DTP
switchport nonegotiate

! Interdit à tous les VLAN de passer par le port trunk
switchport trunk allowed vlan none

! Redéfinit le VLAN natif pour ce port trunk
switchport trunk native vlan <999>

! Supprime la description de la macro exécutée dans la configuration de l'interface
no macro description
@

```

A.2 Utilisation des macros

Sachant que les macros exécutées sur des interfaces s'appliquent en surcouche de la configuration déjà présente, il peut être utile de remettre les interfaces cibles en configuration par défaut avant de les reconfigurer.

Exemple de mise en configuration par défaut d'une plage d'interfaces :

Exemple Cisco IOS

```

! Reconfigure les interfaces 11 à 17 en configuration par défaut
Switch(config)# default interface range fa0/11-17

```

Pour utiliser une macro préalablement créée, il suffit de sélectionner les interfaces sur lesquelles l'exécuter, puis de saisir la commande d'application de la macro.

Exemple d'utilisation d'une macro :

Exemple Cisco IOS

```

! Sélection des interfaces sur lesquelles appliquer la macro
Switch(config)# interface range FastEthernet <0/11-17>

! Application de la macro
Switch(config-if-range)# macro apply <port_inutilise>

```