

# EXIGENCES LIÉES AU RÉSEAU ET COMMUTATEURS

(SE RÉFÈRE À LA NOTE TECHNIQUE N°DAT-NT-25/ANSSI/SDE/NP DU 24 JUIN 2016: RECOMMANDATIONS POUR LA SECURISATION D'UN COMMUTATEUR DE DESSERTE)

---

Ce document présente les principales « Recommandation pour la sécurisation d'un commutateur de desserte » que préconise le BSSI-SIC de l'ESID de Bordeaux.

**R1** : Dédier une interface physique du commutateur à son administration.

**R2** : Mettre en place une séparation physique ou un cloisonnement logique utilisant des VLAN pour appliquer cette séparation entre les réseaux d'administration et les réseaux métier.

**R3** : Ne pas désactiver le port console des commutateurs.

**R4** : Utiliser le protocole SSH en version 2 pour l'administration à distance des commutateurs.

**R6** : Désactiver le serveur web de gestion du commutateur, que ce soit en version sécurisée (HTTPS) ou non (HTTP).

**R7** : Supprimer les certificats créés par défaut sur le commutateur.

**R8** : Ne pas utiliser le protocole Telnet pour l'administration à distance des commutateurs lorsque des protocoles plus sécurisés sont supportés par l'équipement. 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.

**R9** : Un commutateur ne doit disposer que d'une seule adresse IP dédiée à son administration.

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

**R11** : Activer la journalisation des authentifications et tentatives d'authentification.

**R12** : Mettre en place des contre-mesures pour protéger le commutateur des attaques de type brute force. (Exemple commande CISCO : login block - for 300 attempts 3 within 120 / login delay 2)

**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.

**R18** : Supprimer les comptes par défaut - au minimum, les désactiver - tout en veillant à conserver au moins un compte administrateur local « de secours ».

**R22** : La politique de sécurité des mots de passe des comptes utilisateurs doit respecter la PSSI en vigueur.

**R25** : Désactiver les services de configuration automatique des VLAN, VTP, MVRP ou GVRP selon les commutateurs.

**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.

**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.

**R28** : Le VLAN par défaut ne doit jamais être utilisé.

**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.

**R31** : Le routage interVLAN doit être assuré par des équipements de niveau 3. Celui-ci doit donc être désactivé sur les commutateurs d'accès.

**R33** : Désactiver la fonctionnalité de Source routing.

**R37** : Activer les fonctions de DHCP snooping et d'IP Source Guard afin de pallier les faiblesses de sécurité du protocole DHCP.

**R38** : Activer les fonctions d'inspection ARP.

**R39** : Activer des protections contre la propagation des trames Spanning Tree sur les ports d'accès.

**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.

**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.

**R48** : Régler le niveau de journalisation des commutateurs pour l'adapter aux besoins de journalisation du SI et si possible activer l'envoi des journaux vers un serveur de collecte (exemple : syslog).

**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.

**R51** : Activer la journalisation des commandes entrées par les administrateurs.

**R57** : Utiliser SNMP en version 3 AuthPriv, si cela n'est pas possible techniquement, utiliser à défaut la version 2c. Ne pas utiliser le protocole SNMP en mode set pour administrer les commutateurs.

**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).

**R61** : Homogénéiser les configurations matérielles et logicielles des commutateurs de son système d'information afin de faciliter leur MCO/MCS.

**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.

**R64** : Centraliser l'administration des commutateurs au sein du système d'information.

**R65** : Mettre en place une procédure de sauvegarde, restauration de la configuration des commutateurs. Tester les procédures de façon régulière.

**R69** : Activer le chiffrement des mots de passe contenus dans le fichier de configuration.

# GLOSSAIRE

---

Nom ou sigle	Autre nom d'usage	Définition
ACL	Access Control List	Mécanisme de contrôle d'accès basé sur un filtrage généralement effectué au niveau des adresses IP
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)
DHCP	Dynamic Host Configuration Protocol	Protocole réseau configurant notamment les paramètres IP d'une machine
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
HTTPS	Hypertext Transfer Protocol Secure	Version sécurisée avec TLS du protocole HTTP
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
MVRP	Multiple VLAN Registration Protocol	Protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur un parc de commutateurs de manière dynamique
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
SI	Système d'information	Ensemble des moyens matériels et logiciels permettant de gérer et traiter de l'information dans un périmètre donné
SNMP	Simple Network Management Protocol	Protocole de gestion et de supervision d'équipements
SSH	Secure Shell	Protocole sécurisé d'accès à distance à l'interface en ligne de commande d'équipements
syslog	syslog	Protocole de journalisation
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