

📍 Avenue V. Maistriau 8a  
B-7000 Mons  
📞 +32 (0)65 33 81 54  
✉️ scitech-mons@heh.be

[WWW.HEH.BE](http://WWW.HEH.BE)

## UE : Networks : Connected and secure

- AA : Connecting networks  
Denis Mandoux

Bachelier en Informatique  
Orientation réseaux et télécommunications

## Table des matières

1. Monitoring réseau.....	(slide 2)	1
2. AAA .....	(slide 80)	40
3. Port mirroring .....	(slide 136)	68
4. Virtual Routing and Forwarding .....	(slide 149)	75
5. Analyse spectrale .....	(slide 171)	86
6. Modulations .....	(slide 188)	94
7. Lignes de transmission .....	(slide 216)	108
8. Les antennes .....	(slide 247)	124
9. Introduction au Pentesting (phases 1 et 2) .....	(slide 301)	151
10. Introduction à Nmap.....	(slide 323)	168
10. Pentesting Phases 3 à 7 .....	(slide 371)	186
11. Bibliographie.....		248

## UE : Networks : Connected and secure

- AA : Connecting networks

Denis Mandoux

Bachelier en Informatique  
Orientation réseaux et télécommunications



1

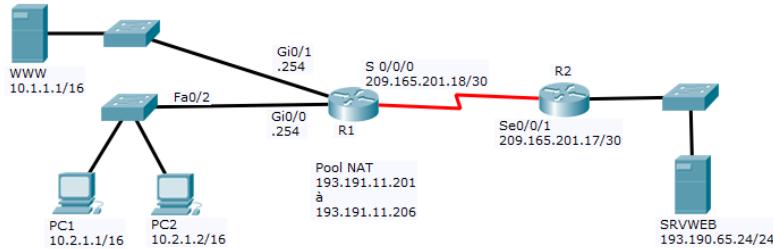
Chapitre 1

# Monitoring réseau



2

- Surveillance du réseau



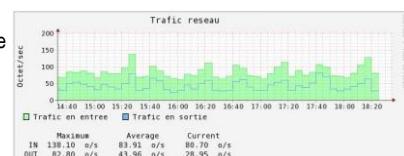
- Monitoring

- Désigne le fait de surveiller un équipement.
- La surveillance consiste à connaître l'état actuel d'un système ainsi que son historique.

- Métrie

- Ensemble des méthodes et techniques pour effectuer des mesures.
- Au niveau du monitoring, la métrologie consiste principalement à :

- Obtenir des mesures d'une charge.
  - Par ex. le % de charge CPU, le nombre de personnes connectées, le trafic entrant/sortant d'un commutateur, ...
- Tracer des graphiques de l'évolution d'une charge dans le temps.



## Introduction

- **Supervision**

- Consiste à récupérer un état à un instant T (état up ou down p.ex.)
- Permet de remonter des alertes en fonction des états.

- **Pourquoi superviser?**

Le serveur Web fournit-il les pages Web demandées ?

Qui consomme la bande passante?

Quel est l'état des circuits virtuels?

Les ventilateurs sont-ils fonctionnels?

## Introduction

- **Pourquoi superviser? (suite)**

- Disposer de données sur le fonctionnement du réseau
  - Parties plus utilisées que d'autres? Goulots? Qui consomme la BP?
  - Création d'une ligne de base réseau (Network baseline).
- Disposer d'un historique sur le comportement normal du réseau
  - Croissance du trafic réseau?
  - Vérifier l'évolution par rapport à la ligne de base.
- Être alerté rapidement en cas de problème
  - Vue en temps réel de l'état du réseau.
  - Facilite le dépannage.

Le serveur Web est inaccessible

Une alarme renseigne "interface down"

- **Superviser quoi?**

- "Tout" ce qui peut être utile

- Pour anticiper l'évolution du réseau.
- Planifier l'introduction de nouvelles applications.
- Être averti rapidement d'un problème.
- ...

→ Plus il y a d'indicateurs plus il y a de chance qu'un indicateur soit utile pour la détection d'un problème.

- Tout mais pas trop

- Surveiller trop d'éléments consomme des ressources sur les périphériques.
- Surveiller trop d'éléments consomme de la bande passante.
- Surveiller trop d'éléments pollue la visibilité des incidents importants.
- Surveiller trop d'éléments demande beaucoup de travail pour peu de résultats.

→ Analyse à réaliser

- En fonction des besoins et des ressources critiques.
- En fonction des ressources disponibles (CPU, BP, monitoring distribué, ...).

- **Exemples d'éléments à superviser**

- Sur les périphériques réseaux :

- le % de bande passante utilisée,
- le % de paquets en erreur,
- le % de paquets de diffusion,
- la température,
- les ports en erreur,
- la mémoire utilisée,
- le CPU utilisé,
- les authentifications incorrectes,
- l'état des services,
- ...

- **Comment superviser?**

- **Méthode active : polling (sondage)**

- Requête de la station de gestion – réponse du périphérique.
    - Induit un délai entre l'occurrence d'un événement et l'heure de journalisation.
    - Consomme des ressources alors qu'il n'y a peut-être pas d'informations utiles à récupérer.

- **Méthode passive : trap (déroutement)**

- L'équipement prend l'initiative de prévenir qu'un événement particulier s'est produit.
    - Sur base d'états ou de seuils configurés par l'administrateur.

- **Comment superviser? (suite)**

- **Exemple pour le service HTTPS**

- **Pinguer le périphérique**

- Le périphérique est joignable sur le réseau, mais cela ne garantit pas que le service HTTPS est démarré.

- **Vérifier que le processus HTTPS est démarré**

- Le service est démarré mais cela ne garantit pas que le serveur puisse fournir les pages Web.

- **Vérifier que le service est capable d'accéder aux pages Web**

- Le système de monitoring doit pouvoir aller "lire" une page Web.

- **Exemple pour l'état des ports**

- **Vérifier le statut up/down des interfaces**

- Mais pas sur les ports "utilisateur"!

## Introduction

- Comment superviser? (suite)

- Gestion des alarmes

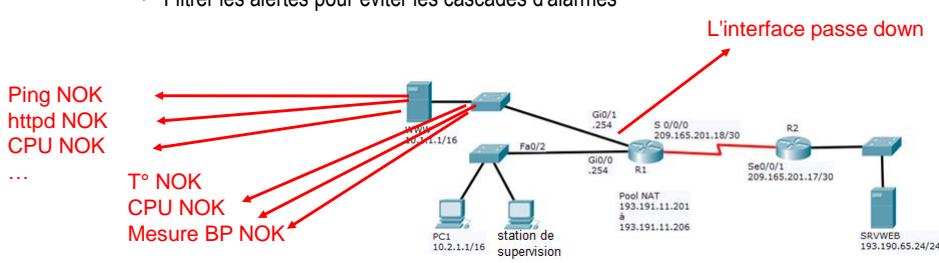
- Déterminer si et quand il faut générer une alarme
      - Chaque fois que le périphérique reçoit un paquet en erreur?
      - En cas de pourcentage trop élevé de paquets en erreur?
    - Limiter au maximum les alertes
      - Commencer la journée avec 50 mails d'alarmes c'est déprimant...
    - Clarté du niveau d'importance de l'alarme
      - Le sujet et la criticité du message doivent être visible au premier coup d'œil.
    - Seules les bonnes personnes doivent être alertées
      - Autre contact possible si le premier ne "répond" pas.
    - Choix du type d'alarme
      - Affichage sur une console de monitoring, alerte par mail (le temps de réaction peut être long) ou alerte par SMS.
    - Temporisateur
      - Interface up/down/up/down... → pas une alarme à chaque changement d'état.

## Introduction

- Comment superviser? (suite)

- Gestion des alarmes (suite)

- Filtrer les alertes pour éviter les cascades d'alarmes



- **Comment superviser? (suite)**

- **Gestion des actions de correction**

- **Il est possible d'automatiser une action sur base des données récoltées.**

- Par exemple le HTTPd est arrêté → exécuter un script de démarrage du service.

- **Attention**

- Il peut y avoir des effets néfastes à une automatisation mal pensée.

- Lors d'un arrêt pour maintenance un service pourrait être redémarré automatiquement.

- **Conservation des données récoltées**

- **Déterminer quelles données doivent être conservées**

- Par exemple celles donnant des indications sur l'évolution du réseau.

- **Déterminer avec quel niveau de détail conserver les données**

- A long terme, seules les tendances, les évolutions générales sont intéressantes.

- **Comment superviser? (suite)**

- **Documentation**

- Lister les éléments à superviser.
    - Classer les éléments par criticité.
    - Rédiger/compléter la base de connaissances.
      - Nomenclature des éléments supervisés.
      - Descriptifs des erreurs rencontrées + correctifs appliqués.
    - Conserver l'historique des alertes
      - Permet de remonter à la source d'un incident.

## Introduction

- **Superviser avec quels outils?**

- Protocoles

- Syslog, SNMP et NetFlow/IPfix

- Exemples d'outils

- Centreon
- PRTG network monitor
- SolarWinds Network Performance Monitor
- Nagios
- Zabbix
- Kiwi syslog
- Serveur Syslog Tftpd32
- Solawinds NetFlow Traffic Analyzer
- ...

## Comparer plusieurs outils informatiques

- **Analyser vos besoins**

- Pourquoi avez-vous besoin d'un tel outil?

- Identifiez ce que vous en attendez.
- Identifiez les principaux problèmes que vous espérez résoudre.
  - Vous en avez besoin car vous n'en avez pas? Vous souhaitez une solution offrant une meilleure performance? Vous souhaitez une solution offrant une interface plus ergonomique pour vos clients?
  - En comprenant le "pourquoi", il vous sera plus facile d'identifier l'outil dont vous avez besoin.

- Déterminer qui est concerné

- Des autorisations sont-elles nécessaires pour commencer ? Lesquelles ?
- Qui participera/dirigera le processus d'évaluation ?
- Quel est le budget alloué ?
- Quel est le délai donné pour mener à bien l'évaluation ?

## Comparer plusieurs outils informatiques

- **Déterminer les critères d'évaluation du logiciel informatique**

- Dresser une liste des fonctionnalités qui pourraient répondre à vos besoins
  - Vous devez prendre en compte les processus et les exigences propres à votre organisation/projet.
- **Must have – Best to have**
  - Définissez les critères incontournables (Must have)
    - Ces fonctionnalités sont indispensables, si l'outil ne les propose pas, il ne fera pas partie de la comparaison.
  - Définissez les critères optionnels (Best to have)
    - Ces fonctionnalités pourraient être utiles ou pratiques mais ne sont pas nécessaires.
- **Présélectionner une liste de solutions/outils**
  - Une fois les critères de qualité et fonctionnalités (must have) dont vous avez besoin clairement définis, présélectionner une liste d'outils qui répondent à ces exigences.

## Comparer plusieurs outils informatiques

- **Elaborer une grille d'évaluation ou une carte de score**

- **Quantifier vos critères (ou pas)**
  - Reprenez votre liste des fonctionnalités incontournables et optionnelles et assignez une valeur numérique ou un poids en fonction de leur utilité.
  - Plus la fonctionnalité est pertinente et plus son poids/valeur sera élevé.
    - Par exemple, la valeur totale de l'ensemble des fonctions = 100.
- **Tester et quantifier vos résultats**
  - Evaluatez individuellement chaque fonctionnalité des outils sélectionnés, par exemple via un score de 1 à 5 ou une appréciation telle que --, -, +, ++.

## Comparer plusieurs outils informatiques

- Exemple

Must-Have	Nice-To-Have
Auto Discovery du réseau	Prédicibilité de pannes
Interface web	Analyse des comportements inhabituels
Interface de gestion simple et intuitive	Gestion des alertes (corrélation, escalation,...)
Utilisateur viewer (read-only)	Serveur de centralisation des logs
Monitoring réseau	Système de ticket interne
Budget de xx € HTVA	
Windows Server 2016 et 2022	Imprimantes
Ubuntu 20.04 et 22.04	Access point de marque XX
Hyperviseur XX	Bancontact
Serveurs web (MySQL, Apache, PHP, requêtes HTTP)	Caisses
Contrôleur de domaine (Active Directory, DHCP, DNS)	Caméras
Switches XX	Antivirus XX
Microsoft Exchange (Backup, envoi de mail)	Solution de Backup XX
Firewall FortiGate	
UPS	
Pointeuses	
Badge	

## Comparer plusieurs outils informatiques

- Exemple

	Zabbix	Nagios XI	PRTG	NetCrunch
Utilisation de l'Auto Discovery	+	++	+	++
Performance de l'Auto Discovery	---	+	+++	=
Interface web	+	++	+++	--
Facilité de gestion	---	-	++	NE
Facilité de lisibilité des éléments et alertes	NE	+	+++	-
Interface intuitive	---	-	+++	-
Gestion des utilisateurs	NE	=	+	NE
Gestion des alertes (corrélation, escalation,...)	NE	---	+	NE
Gestion des alertes (downtime, acknowledge,...)	NE	++	=	NE
Fonctionnalités supplémentaires (xFlow, maps,...)	NE	NE	+	++
Performance (Interface, lenteur, scans,...)	+	++	--	---
Communauté et assistance	--	++	++	--
Durée d'implémentation (estimation)	NE	-	++	NE
Ressenti personnel	--	-	++	---

Légende : de --- à ++, +++ étant le meilleur, NE : fonctionnalité Non Expérimentée

- Analyser l'éditeur de la solution

- Quelles sont les qualités/défauts des éditeurs ?

- Quelles options de déploiement propose l'éditeur?

- Disposent-ils d'une solution cloud?
    - Si oui, où sont stockées les données?
    - Comment gère-t-il les mises à jour

- Quelles options de support technique sont disponibles ?

- Via email, téléphone, messagerie, système de tickets ?
    - Inclus dans le prix ou payant?

- Apprentissage de la solution

- Si l'outil est complexe à prendre en main, propose-t-il des formations, des guides pratiques, didacticiels vidéo ?

- Sécurité de la solution

- Vérifiez si le fournisseur ou la solution est régulièrement impliquée dans des failles de sécurité.

- Evaluer le coût de la solution

- TCO : Total cost of ownership

- Le TCO comprend toutes les dépenses liées à l'achat et l'utilisation de la solution.

- Exemples de frais à prendre en compte

- Achat du matériel.
    - Achat de licences.
    - Coût de formation des utilisateurs,
    - Coût d'implémentation de la solution (downtime nécessaire?)
    - Coût du support technique.
    - Coût d'entretien du matériel (serveur, ...).

- **Messages systèmes**

- **Les périphériques peuvent envoyer des messages système**

- Lors de l'occurrence de certains événements comme le changement d'état d'une interface.

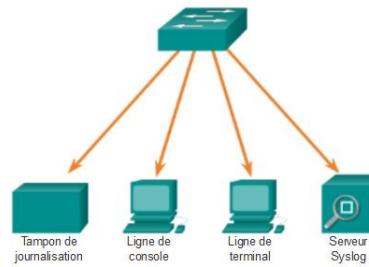
```
R1(config-if)#
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface
FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up
```

- **Syslog**

- Nom d'un protocole de journalisation d'événements d'un système informatique.
    - Nom de la norme décrivant le format des messages syslog.
    - Utilise le port UDP 514.
    - Disponible sur de nombreux périphériques (R, SW, SRV, FW, ...)

- **Destination des messages syslog**

- Dans une mémoire tampon sur le périphérique
    - Les données ne sont accessibles que par la CLI.
    - Les messages de niveau débogage ne sont transférés que vers le tampon interne.
  - Dans la console (console 0).
  - Dans un terminal (pty).
  - Vers un serveur syslog sur le réseau.



- **Niveau de gravité Syslog**

- Chaque message Syslog contient un niveau de gravité et une capacité.
- Plus le numéro du niveau est petit, plus l'alarme est critique.

Gravité Cisco	Niveau	Syslog	Descriptif
Emergencies (Urgence)	0	LOG_EMERG	Système instable
Alerts (Alerte)	1	LOG_ALERT	Action immédiate requise
Critical (Critique)	2	LOG_CRIT	Conditions critique
Errors (Erreur)	3	LOG_ERR	Conditions d'erreur
Warnings (Avertissement)	4	LOG_WARNING	Condition d'avertissement
Notifications (Notification)	5	LOG_NOTICE	Événement normal mais important
Informational (Informatif)	6	LOG_INFO	Message informatif
Debugging (Débogage)	7	LOG_DEBUG	Message de débogage

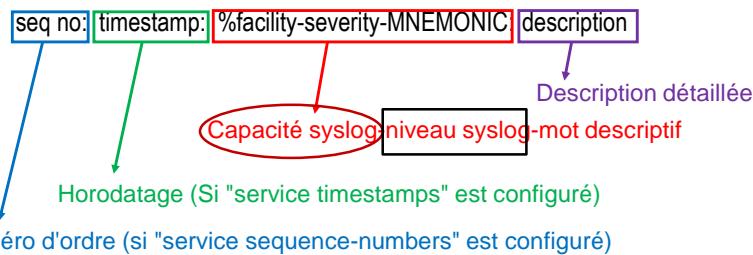
P. ex. Interface change state to up

- **Capacité syslog (facility)**

- **Les capacités Syslog sont des identificateurs**
  - **Elles spécifient l'appareil, le protocole ou le module qui logue le message.**
    - Cela facilite la gestion ultérieure des messages (classement).
  - **Les options de capacité de journalisation disponibles sont spécifiques au périphérique.**
    - Par exemple, les Sw 2960 (IOS 15.0(2)) prennent en charge 24 options de capacité classées en 12 types de capacité.
    - Les valeurs de capacités utilisées par Cisco sont différentes de celles utilisées par le protocole syslog lui-même.
- **Exemple de capacités**
  - Protocole "IP"
  - Protocole "OSPF"
  - Système d'exploitation "SYS"

## Syslog

- Format des messages Syslog



- Exemple

```
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

## Syslog

- Horodatage des messages

- Nécessite de configurer l'horloge

- Configuration manuelle de l'horloge

```
Sw# clock set
```

- Configuration automatique de l'horloge avec NTP

```
Sw(config)# ntp server adresse-ip
```

- Configuration en tant que serveur NTP

```
Sw(config)# ntp master number
```

- Horodatage des messages de log

- En affichant le temps écoulé depuis le dernier démarrage du périphérique.

```
R(config)# service timestamps log uptime
```

- En affichant la date et l'heure de l'événement.

```
R(config)# service timestamps log datetime [msec]
[localtime] [show-timezone]
```

- **Journalisation syslog**

- Les messages syslog peuvent être envoyés à la console

- Par défaut, tous les messages syslog sont envoyés à la console.

```
Sw(config)# logging console
```

- Les messages syslog peuvent être envoyés en mémoire tampon

```
Sw(config)# logging buffered
```

- Les messages syslog peuvent être envoyés sur les terminaux

```
Sw(config)# logging terminal
```

```
C:\>telnet 10.2.1.100
Trying 10.2.1.100 ...Open
Password:
S1>en
Password:
S1#conf t
S1(config)#inteface fastethernet 0/2
S1(config-if)#shutdown
S1(config-if)#|
```

Par défaut, pas de logs envoyés sur les terminaux vty



29

- **Journalisation syslog**

- Afficher les paramètres de journalisation

```
Sw# show logging
```

```
Si#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 12 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 12 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled, filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

Log des niveaux debug et inférieurs  
12 messages ont été logués



30

- Journalisation syslog

- Afficher les paramètres de journalisation

```
Sw# show logging
```

```
S1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                  0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 44 messages logged, xml disabled,
                  filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
                  filtering disabled
Buffer logging: level debugging, 44 messages logged, xml disabled,
                  filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
File logging: disabled
Persistent logging: disabled
```

Log des niveaux debug et inférieurs  
44 messages ont été logués

- Journalisation syslog

- Afficher les paramètres de journalisation

```
Sw# show logging
```

```
*Mar  1 10:25:19.080: %SYS-5-CONFIG_I: Configured from console by console
*Mar  2 00:18:49.241: %SYS-5-CONFIG_I: Configured from console by console
*Mar  2 02:44:18.477: %SYS-5-CONFIG_I: Configured from console by console
*Feb 11 13:59:10.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
04:14:41 UTC Tue Mar 2 1993 to 13:59:10 UTC Thu Feb 11 2021, configured from
console by console.
Feb 11 14:02:39.891: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:02:39 UTC Thu Feb 11 2021 to 15:02:39 gmt Thu Feb 11 2021, configured from
console by console.
```

Configuration de l'heure système.

- Journalisation vers un serveur syslog externe
  - Enregistrement des messages syslog reçus.
  - Affichage ergonomique des messages Syslog.
  - Recherches facilitées dans les données syslog.
  - Facilité pour supprimer rapidement des messages Syslog non importants.

Kiwi Syslog Service Manager (Registered - Version 8.2.17)					
	Date	Time	Priority	Hostname	Message
!	06-05-2007	15:49:30	Daemon.Notic	192.168.10.100	Test user c
!	06-05-2007	15:49:25	Local4.Warning	192.168.10.241	Test user c
!	06-05-2007	15:49:21	Local5.Debug	192.168.10.92	Test user c
!	06-05-2007	15:49:20	User.Debug	192.168.10.115	Test user c
!	06-05-2007	15:49:17	System1.Info	192.168.10.197	Test user c
!	06-05-2007	15:48:53	Local5.Info	192.168.10.7	Test user c
!	06-05-2007	15:48:50	Local0.Notice	192.168.10.223	Test user c
!	06-05-2007	15:48:49	System5.Notice	192.168.10.60	Test user c

Source : [http://www.computerperformance.co.uk/images/solarwinds/kiwi\\_server\\_sm.jpg](http://www.computerperformance.co.uk/images/solarwinds/kiwi_server_sm.jpg)



33

- Configuration de la journalisation vers un serveur syslog

- Configurez l'adresse IP(ou le nom) du serveur Syslog

```
Sw(config)# logging IP-address
Sw(config)# logging host IP-address
```

- Exemple

```
Sw(config)# logging host 192.168.1.3
```

- Configurez les messages qui seront envoyés au serveur Syslog

```
Sw(config)# logging trap level
```

- Exemple

```
Sw(config)# logging trap 4
Sw(config)# logging trap warning
```



34

- Journaliser des commandes entrées par les administrateurs

- Activer la journalisation des commandes de configuration

```
Sw(config)# archive
```

```
Sw(config-archive)# log config
```

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

- Limiter le nombre de commandes sauvegardées

```
Sw(config-archive-log-cfg)# logging size <1-1000>
```

- Empêcher de journaliser les mots de passe

```
Sw(config-archive-log-cfg)# hidekeys
```

- Envoyer les événements journalisés au serveur syslog

```
Sw(config)# notify syslog
```

- Journaliser des commandes entrées par les administrateurs (suite)

- Limiter le nombre d'événements de journalisation affichés sur la console du commutateur

```
Sw(config)# logging rate-limit console X except severity
```

- Limite les événements affichés sur la console à X événements par seconde , sauf si le niveau de gravité est supérieur ou égal à severity

- Afficher les événements journalisés

```
Sw(config)# show archive log config all
```

- Journaliser des commandes entrées par les administrateurs (suite)

- Définir l'origine des logs

```
Sw(config)# logging origin-ID ?
hostname Use origin hostname as ID
ip        Use origin IP address as ID
ipv6     Use origin IPv6 address as ID
string    Define a unique text string as ID
```

- Définir l'interface « source » des logs

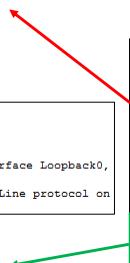
- L'adresse de l'interface source sera reprise dans le message syslog, quelle que soit l'interface utilisée par le paquet pour quitter le périphérique.

```
R1(config)# logging source-interface interface-name
R1(config)# logging source-interface gi0/0
```

- Exemple avec P.T.

- Remarque : dans P.T, il faut sortir puis revenir dans l'écran du serveur syslog pour mettre à jour les entrées.

Sans la commande "service timestamps log datetime msec"



Time	HostName	Message
1 janv. 01:00:00:00.000	10.1.1.254	%LINK-5-CHANGED: Interfa...
2 janv. 01:00:00:00.000	10.1.1.254	%LINEPROTO-5-UPDOWN: ...
3 janv. 01:00:00:00.000	10.1.1.254	%LINK-5-CHANGED: Interfa...
4 janv. 01:00:00:00.000	10.1.1.254	%LINEPROTO-5-UPDOWN: ...
5 oct. 13 13:19:51.148	10.1.1.254	%LINK-5-CHANGED: Interfa...
6 oct. 13 13:19:51.148	10.1.1.254	%LINEPROTO-5-UPDOWN: ...

Avec la commande "service timestamps log datetime msec"

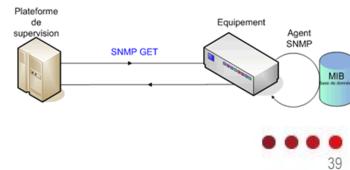
- **SNMP**

- **Simple Network Management Protocol**

- Protocole qui définit le format des messages échangés entre les gestionnaires et les agents SNMP.
    - SNMP utilise le port UDP 162.
    - SNMP permet de
      - gérer les équipements du réseau (modification de la configuration),
      - superviser les équipements du réseau (récolte, vérification de données, de config.),
      - diagnostiquer des problèmes réseaux (via l'analyse des données récoltées).

- **Le système SNMP se compose de trois éléments**

- Le gestionnaires SNMP (SNMP manager, NMS (Network Management Server)).
    - Les agents SNMP (SNMP agent).
    - Les bases d'informations de gestion (MIB).



- **MIB**

- **Management Information base**

- Base de données contenant les informations sur le matériel.
    - Les éléments de la MIB sont appelés "objets".
    - Un fichier MIB est un document texte écrit en langage ASN.1

- **Les objets peuvent être**

- **Statiques**
      - Type de matériel, constructeur, version d'un équipement.
    - **Dynamiques**
      - État à un instant donné (up, down, ...).
    - **Statistiques**
      - Minuteurs, compteurs, ... (uptime, nombre d'octets reçus sur un port, etc.).

- **MIB (suite)**

- La MIB a une structure arborescente

- Les informations des MIB sont nommées de manière unique suivant une notation hiérarchisée (SMI).
    - Chaque information est identifiée
      - par un nombre (OID : Object Identifier).
      - ou par un nom normalisé et hiérarchique (plus lisible).

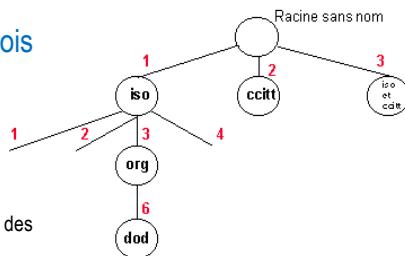
- La racine de l'arbre comprend trois branches

- **iso.org.dod**

- Le séparateur est un point.

- **.1.3.6**

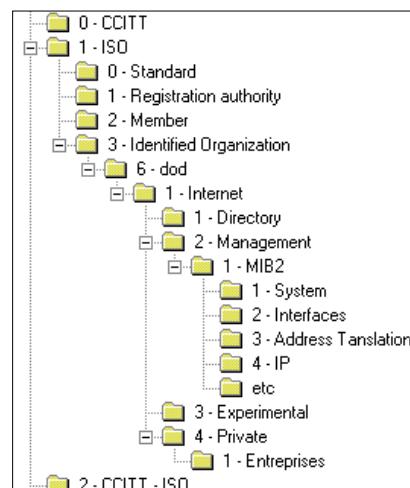
- Suite d'entier correspondants aux n° des feuilles de l'arborescence.



• • • 41

- **MIB Browser**

- Logiciel permettant d'explorer une arborescence MIB



• • • 42

**HEHbe** Sciences et technologies **SNMP**

- **SNMP Object Navigator**
  - Nécessite un compte CCO

Source : <http://snmp.cloudapps.cisco.com/Support/SNMP/doBrowseOID.do?local=en>

• • • 43

**HEHbe** Sciences et technologies **SNMP**

- **Versions SNMP**
  - Seules certaines versions sont supportées par le matériel.
  - **SNMPv1 : 1987 (RFC 1157)**
    - Sécurité basée uniquement sur une chaîne de caractère nommée "community" fonctionnant comme un mot de passe et envoyé en texte clair.
  - **SNMPv2c : 1993 (RFC 1901 à 1908)**
    - Propose diverses améliorations : utilise des compteurs sur 64 bits, requête "getbulk", gestion des erreurs améliorée ...
    - La version 2c est compatible avec SNMPv1.
    - « Community » envoyé en texte clair.
    - Risque faible si utilisé en lecture seule.
  - **SNMPv3**
    - Version plus sécurisée intégrant l'authentification, l'intégrité, la prévention du rejet ainsi que la confidentialité.
    - Permet d'introduire le protocole SNMP dans des réseaux étendus géographiquement.
    - RFC 2273 à 2275 et RFC 3410 à 3415

• • • 44

- Configuration de SNMP

- Configurer l'identifiant de communauté et le niveau d'accès

```
R(config)# snmp-server community string ro | rw
```

- Documenter l'emplacement du périphérique

```
R(config)# snmp-server location text
```

- Documenter la personne de contact

```
R(config)# snmp-server contact text
```

- Limiter l'accès avec une ACL

```
R(config)# ip access-list standard ACL-FOR-SNMP
```

```
R(config-std-acl)# permit 192.168.0.1
```

```
R(config-std-acl)# exit
```

```
R(config)# snmp-server community string ACL-name
```

- Configuration de SNMP (suite)

- Activez les déroutements (traps) sur un agent SNMP

```
R(config)# snmp-server enable traps notification-types
```

– Si aucun type n'est spécifié, tous les types de déroutements sont envoyés.

```
Sw(config)#snmp-server enable traps ?
cpu                  Allow cpu related traps
dot1x                Enable SNMP dot1x traps
errdisable           Enable SNMP errdisable notifications
flash                Enable SNMP FLASH notifications
hsrp                 Enable SNMP HSRP traps
...
```

- Configurer le destinataire des traps

```
R(config)# snmp-server host host-id [version{1| 2c | 3
[auth | noauth | priv}}] community-string
```

- 3 niveaux de sécurité

- noAuthNoPriv (noauth)

- Authentification : le nom d'utilisateur remplace la communauté SNMP
    - Pas de chiffrement.

- AuthNoPriv (auth)

- Authentication via HMAC-MD5 ou HMAC-SHA.
    - Pas de chiffrement.

- AuthPriv (priv)

- Authentication via HMAC-MD5 ou HMAC-SHA.
    - Chiffrement (DES, 3DES ou AES).

- Étapes de configuration

1. Définir quelles IP pourront envoyer des paquets SNMP

- Pour cela, on configure une liste de contrôle d'accès standard reprenant les IP des gestionnaires SNMP autorisés.
  - Appliquer l'ACL aux interfaces concernées.

```
R(config)# ip access-list standard acl-Name
R(config-std-acl)# permit source source-wildcard

R(config)#fa 0/0
R(config-if)#ip access-group acl-name in
```

## Configuration de SNMPv3

### 2. Spécifier les OID des objets auxquels un gestionnaire SNMP aura accès

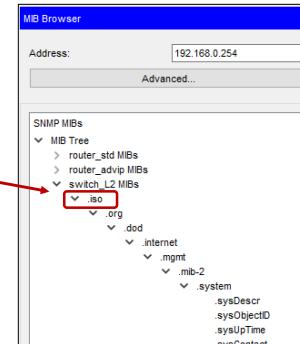
- Pour cela, on définit une ou plusieurs « view » SNMP.

```
R(config)# snmp-view view view-name oid-tree {included | excluded}
```

```
R(config)# snmp-view view MyViewALL iso included
```

Nom ou notation décimale  
(Par exemple : internet ou 1.3.6.1)

Vous pouvez référencer des objets individuels  
ou un sous-ensemble d'objets de l'arborescence MIB.



49

## Configuration de SNMPv3

### 3. Configurer des groupes SNMP

- Permet d'associer une ou plusieurs « views » aux utilisateurs SNMP.
- Permet de définir le type d'accès autorisé à une « view ».

```
R(config)# snmp-server group [groupname {v1 | v2c | v3 [auth |  
noauth | priv]}] [read readview] [write writeview] [ access [acl-  
number | acl-name] ]
```

```
R(config)#snmp-server group MySNMPGroup v3 priv read MyViewALL
```

#### 4. Configurer les utilisateurs SNMP

- Associer les utilisateurs aux groupes SNMP
- Définir les paramètres de sécurité associé aux utilisateurs SNMP.

```
R(config)# snmp-server user username groupname [remote host [udp-port port] v3 auth {md5 | sha} UserAuthPassword [priv {des | 3des | aes {128|192|256} UserPrivPaswword }] [access access-list]
```

```
R(config)# snmp-server user MyUser MySNMPGroup v3 auth sha MyPasswd priv aes 128
```

#### 5. Configurer les notifications SNMP (traps)

- Les niveaux de sécurité noauth, auth et priv s'appliquent aussi aux traps.
- Inform = trap avec ACK.

```
R(config)# snmp-server enable traps [notification-type [notification-options]]
```

```
R(config)# snmp-server host host [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [notification-type]
```

```
R(config)# snmp-server enable traps [notification-type [notification-options]]
```

```
R(config)# snmp-server host IPaddress traps version 3 priv MyUser
```

- Conseils d'implémentation

- Versions SNMP

- Utiliser la version 3 si elle est supportée par les périphériques.
    - Si une version 1 ou 2c doit être utilisée, il ainsi que les mots de passe convient de modifier régulièrement les noms de communauté.

- Désactiver la communauté "public"

- Pour des raisons de sécurité.

– R(config)# no snmp-server community public [ RO | RW ]

- Surveillance seule

- Si le protocole SNMP est utilisé uniquement pour surveiller des périphériques, il faut utiliser des communautés en lecture seule.

- Utiliser des ACL

- Pour empêcher les messages SNMP d'être propagés ailleurs que vers les systèmes de gestion (NMS).
    - Pour autoriser l'accès uniquement aux systèmes de gestion (NMS).

- Vérification

```
Sw# show snmp ?
chassis      show snmp chassis
community    show snmp communities
contact      show snmp contacts
context      show snmp contexts
engineID     show local and remote SNMP engine IDs
group        show SNMPv3 groups
host         show snmp hosts
location     show snmp location
mib          show mib objects
pending      snmp manager pending requests
sessions     snmp manager sessions
user         show SNMPv3 users
view         show snmp views
|
<cr>
```

- Vérification (suite)

```
Sw# show snmp group
groupname: public
readview : v1default
notifyview: <no notifyview specified>
row status: active

groupname: public
readview : v1default
notifyview: <no notifyview specified>
row status: active

groupname: MySNMPgroup
readview : MyViewALL
notifyview: <no notifyview specified>
row status: active
```

	security model:v1 writeview: <no writeview specified>
	security model:v2c writeview: <no writeview specified>
	security model:v3 priv writeview: <no writeview specified>

- Vérification (suite)

- Par défaut, plusieurs Views sont déjà configurées

```
Sw# show snmp view
MyViewALL iso - included nonvolatile active
v1default iso - included permanent active
v1default internet - included permanent active
v1default snmpUsmMIB - excluded permanent active
v1default snmpVacmMIB - excluded permanent active
v1default snmpCommunityMIB - excluded permanent active
v1default ciscoMgmt.252 - excluded permanent active
```

- Vérification (suite)

- Syntaxe snmpwalk

```
# snmpwalk -v3 -l <noAuthNoPriv|authNoPriv|authPriv> -u
<username> [-a <MD5|SHA>] [-A <authphrase>]
[-x <DES|AES>] [-X <privaphrase>]
<ipaddress>[:<dest_port>] [oid]
```

- Exemple

```
$ snmpwalk -v3 -l noauth -u MyUser 10.1.1.1:161 1.3.6.1
# snmpwalk -v3 -l noauth -u mel 192.168.0.240:161 1.3.6.1
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C3560C Software (C3560c405-
UNIVERSALK9-M), Version 12.2(55)EX3, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Wed 10-Aug-11 07:37 by prod_rel_team"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.1466
iso.3.6.1.2.1.1.3.0 = Timeticks: (2411078) 6:41:50.78
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "$1"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 6
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
```

- SNMP Object Navigator

- Recherche de l'objet sysName

Tools & Resources

### SNMP Object Navigator

HOME SUPPORT TOOLS & RESOURCES SNMP Object Navigator

TRANSLATE/BROWSE SEARCH DOWNLOAD MIBS MIB SUPPORT - SW

Translate | Browse The Object Tree

Translate OID into object name or object name into OID to receive object details

Enter OID or object name:  examples -  
 OID: 1.3.6.1.4.1.9.9.27  
Object Name: ifIndex

Object Information

Specific Object Information

Object	sysName
OID	1.3.6.1.2.1.1.5

- Vérification (suite)

- Syntaxe snmpget

```
$ snmpget -v3 -l [noauth|auth|authPriv] -u [User name] -  
a [MD5|SHA] -A [User password] -x [des|aes] -X [aes  
password] [AdresseIPcible] [OID]
```

- Exemples

```
$ snmpget -v3 -l noauth -u MyUser 10.1.1.1:161 1.3.6.1.2.1.1.5.0  
Iso.3.6.1.2.1.1.5.0 = STRING: « S1 »  
  
$snmpget -v3 -l auth -u MyUSER -a sha -A mypasswd 10.1.1.1:161  
1.3.6.1.2.1.1.5.0  
Iso.3.6.1.2.1.1.5.0 = STRING: « S1 »  
  
$snmpget -v3 -l auth -u MyUSER -a sha -A mypasswd -x aes -X  
Myprivpasswd 10.1.1.1:161 1.3.6.1.2.1.1.5.0  
Iso.3.6.1.2.1.1.5.0 = STRING: « S1 »
```

- Vérification (suite)

```
Sw# show snmp user  
  
User name: denis  
Engine ID: 8000000903000CD996568A01  
storage-type: nonvolatile active  
Authentication Protocol: SHA  
Privacy Protocol: AES256  
Group-name: MySNMPgroup
```

- **Protocole Netflow**

- **Technologie Cisco**

- Protocole réseau pour la collecte de trafic IP et la surveillance de trafic réseau.

- **NetFlow est devenu une norme pour la surveillance de réseaux IP**

- Netflow (v5) → Flexible Netflow (v9) → IPFIX

- Les matériels de nombreux constructeurs prennent en charge NetFlow.

- Jflow ou cflowd chez Juniper Networks
    - NetStream chez 3Com/HP
    - AppFlow chez Citrix
    - ...

- **Protocole Netflow (suite)**

- **Netflow collecte des informations sur les flux IP traversant un R ou Sw L3**

- **L'analyse de ces données collectées peut permettre de :**

- Comprendre l'utilisation de la bande passante par les applications.
      - Déterminer qui génère le plus de trafic ?
      - Déterminer quels sont les sites Web visités régulièrement et quel est le contenu téléchargé ?
      - Comptabiliser et facturer en fonction du niveau d'utilisation des ressources.
      - Servir de source d'informations pour l'identification et le dépannage de goulets d'étranglement, de lenteur, ...
      - Vérifier les performances des règles de QoS.
      - ...

- **Netflow / SNMP / analyseur réseau**

- **NetFlow ne fait que collecter des statistiques de trafic**
  - SNMP peut collecter de nombreuses autres informations (erreurs d'interface, utilisation du processeur, ...).
  - SNMP permet de modifier les configurations.
  - SNMP ne permet pas de collecter des informations aussi précises que Netflow concernant le trafic réseau.
  - Un analyseur de protocole enregistre toutes les informations possibles à la sortie ou à l'entrée d'un port, Netflow cible des données spécifiques directement sur les périphériques réseau.
- Des collecteurs Netflow peuvent utiliser ces données pour agir sur les périphériques.

- **Terminologie**

- **Collecteur NetFlow**
  - Nom du serveur externe où sont envoyées les statistiques Netflow.
- **Flexible NetFlow**
  - Nom donné à la version la plus récente du protocole NetFlow de Cisco.
- **IPFIX**
  - Version standardisées IETF basée sur flexible Netflow.
- **Format d'exportation**
  - Format sous lequel les données sont envoyées au collecteur.  
→ Défini aussi quelles données peuvent être envoyées.

- Principe de Netflow

- Flux TCP/IP

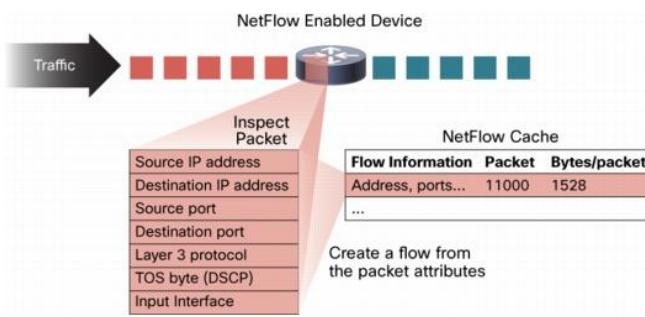
- Un flux est un déplacement unidirectionnel de paquets entre une source et une destination.
    - Netflow répartit les communications TCP/IP selon différents flux.
    - Avec Netflow (v5), les flux se distinguent par
      - Adresse IP source
      - Adresse IP de destination
      - Numéro du port source
      - Numéro du port de destination
      - Type de protocole de couche 3
      - Marquage TOS (type de service)
      - Interface logique d'entrée

→ Deux paquets appartiennent au même flux si ces sept champs sont identiques.

- Principe de Netflow (suite)

- Table des flux

- Le périphérique construit une table des flux qu'il stocke en cache.



Source : [http://www.cisco.com/c/dam/en/us/products/collateral/ios-xr-software/ios-netflow/prod\\_white\\_paper0900aecd80406232.doc\\_jcr\\_content/renditions/prod\\_white\\_paper0900aecd80406232-1.jpg](http://www.cisco.com/c/dam/en/us/products/collateral/ios-xr-software/ios-netflow/prod_white_paper0900aecd80406232.doc_jcr_content/renditions/prod_white_paper0900aecd80406232-1.jpg)

- Principe de Netflow (suite)

- Minutiers (flow aging timer)

- Le flux s'arrête

- Lorsque le flux est inactif (inactive timer de 15s. par défaut).
      - Lorsque le flux est trop long (30 min. par défaut).
      - Lorsque la session s'arrête (TCP flag RST, FIN).

- Une fois le flux arrêté

- Netflow l'exporte vers un collecteur Netflow.
      - Les données sont envoyées au collecteur dans le format d'exportation configuré.

- Un collecteur Netflow

- Écoute le trafic NetFlow envoyé par les périphériques.
      - N'envoie jamais de requêtes netflow aux périphériques.

- Peut implémenter des fonctionnalités afin d'agir sur les périphériques selon l'analyse des données Netflow.

- Principe de Netflow (suite)

- Netflow (V5)

- Collecte toujours les mêmes données.
    - Or, on n'a pas nécessairement toujours besoin des mêmes données.

- Flexible NetFlow et IPFIX

- Permettent de définir les champs pour distinguer un flux d'un autre.
    - Permettent de spécifier quelles données doivent être envoyées au collecteur.
    - Plus flexible que Netflow.
    - La configuration peut être plus compliquée.
    - Moins de données inutiles à stocker sur le collecteur Netflow.

- Configuration de Netflow

- Capture des données entrantes et sortantes

```
R(config)# interface fa 0/1
R(config-if)# ip flow ingress
R(config-if)# ip flow egress
```

- Exportation des données

- Spécifier le destinataire et le port UDP sur lequel le collecteur NetFlow écoute

```
R(config)# ip flow-export destination ip-address udp-port
R(config)# ip flow-export destination 192.168.0.1 9996
– Les ports UDP généralement attribués sont 99, 2055 et 9996.
```

- Spécifier la version de Netflow (version 1, 5, 7, 8 ou 9)

```
R(config)# ip flow-export version version
R(config)# ip flow-export version 5
– Le choix de la version dépend de la compatibilité des systèmes avec les versions plus récentes.
```

- [Optionnel] Spécifier l'interface à utiliser en tant que source des paquets envoyés au collecteur

```
R(config)# ip flow-export source typenumber
```

- Vérification de Netflow

- Via une application

- SolarWinds NetFlow Traffic Analyzer, Plixer Scrutinizer, Cisco NetFlow Collector (NFC), Ntop sous Linux, ...
    - Ces applications peuvent nécessiter pas mal de ressources pour fonctionner.
      - Par exemple 4Go RAM et 50Go d'espace disque.

- Via les commandes show

- R# show ip cache flow
        - Permet de voir notamment quel protocole utilise le plus grand volume du trafic ainsi que les hôtes entre lesquels ce trafic s'écoule.
      - R# show ip flow interface
        - Permet de vérifier que NetFlow est configuré sur les interfaces correctes et dans les directions appropriées.
      - R# show ip flow export
        - Permet de contrôler la configuration des paramètres d'exportation.

- Vérification de Netflow

- Via les commandes show

```
R# show ip cache flow
```

- Permet de voir notamment quel protocole utilise le plus grand volume du trafic ainsi que les hôtes entre lesquels ce trafic s'écoule.

```
R1#show ip cache flow
IP packet size distribution (0 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
   512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
 0 active, 0 inactive, 0 added
 1 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
 last clearing of statistics never
Protocol      Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
-----       Flows     /Sec   /Flow /Pkt   /Sec   /Flow   /Flow
Total:        0       0.0     0       0       0.0     0.0     0.0
SrcIf      SrcIpAddress      DstIf      DstIpAddress      Pr SrcP DstP Pkts
```

Aucun flux

- Vérification de Netflow

```
R# show ip cache flow
```

- Après envoi de pings via le routeur R1.

```
R1#show ip cache flow
IP packet size distribution (10 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
   512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
 2 active, 4034 inactive, 6 added
 4 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
 0 active, 1024 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never
Protocol      Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
-----       Flows     /Sec   /Flow /Pkt   /Sec   /Flow   /Flow
ICMP          4       0.0     1     28       0.0     0.0     916.0
Total:        4       0.0     1     28       0.0     0.0     916.0

SrcIf      SrcIpAddress      DstIf      DstIpAddress      Pr SrcP DstP Pkts
Gig0/0    10.2.1.1      Se0/0/0    193.190.65.24  01 0000 0000      2
Se0/0/0  193.190.65.24  Gig0/+    10.2.1.1      01 0000 0000      2
```

Mémoire utilisée par le cache

Trafic ICMP entre ces deux adresses

- Vérification de Netflow

```
R# show ip cache flow
```

```
R1#show ip cache flow
IP packet size distribution (46 total packets):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .304 .696 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

 512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache: 438541 bytes
 6 active, 4059 inactive, 18 added
 11.49% Total U-L2MV based structures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
 IP Sub Flow Cache, 34056 bytes
 0 active, 1024 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunks added
 last clearing of statistics never
Protocol  Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-----  -----
ICMP      10    0.0     1    28    0.0     0.6    1516.0
TCP-HTTP   1    0.0     5    41    0.0     0.0    2416.0
TCP-other   1    0.0     3    41    0.0     0.0    2416.0
Total:    12    0.0     1    32    0.0     0.5    1666.0

SrcIf  SrcIPAddress  DstIf  DstIPAddress  Pr SrcP  DstP  PktA
Gig0/0  10.2.1.2    Se0/0/0  193.190.65.24  06 0402 0050  5
Se0/0/0  193.190.65.24  Gig0/0*  10.2.1.2    06 0050 0050  3
Gig0/0  10.2.1.2    Se0/0/0  193.190.65.24  06 0403 0050  5
Se0/0/0  193.190.65.24  Gig0/0*  10.2.1.2    06 0050 0403  3
Gig0/0  10.2.1.2    Se0/0/0  193.190.65.24  06 0404 0050  5
Se0/0/0  193.190.65.24  Gig0/0*  10.2.1.2    06 0050 0404  3
```

Nombre de flux actifs/inactifs

Statistiques

Port destination  
0x0050 = port 80

• • • 73

- Vérification de Netflow

– Via une application : onglet desktop dans P.T.



• • • 74

**HEH.be** Sciences et technologies

## Netflow

- Vérification de Netflow
  - Dans P.T., via l'onglet desktop, port de capture 9996

The screenshot shows the Netflow Collector application window. On the left, there's a pie chart divided into four segments, each labeled 'IPV4 SOURCE ADDRESS...'. A red arrow points from the top-left segment to the text 'Pas de N° de port car ICMP' (No port number because ICMP). Another red arrow points from the right side of the pie chart to the text 'Echo Reply'. On the right, a detailed table of flow information is displayed, with several fields highlighted by red boxes. The highlighted fields include:

Traffic Contribution: 25% (1/4)	
Flow information:	
IPV4 SOURCE ADDRESS:	193.190.65.24
IPV4 DESTINATION ADDRESS:	10.2.1.2
INTERFACE INPUT:	Se0/0/0
TRNS SOURCE PORT:	0
TRNS DESTINATION PORT:	0
IP TOS:	0x00
IP PROTOCOL:	1
FLOW SAMPLER ID:	0
FLOW DIRECTION:	Output
ip4 source mask:	/24
ip4 destination mask:	/16
ip4 source bytes:	28
ip4 next hop address:	10.2.1.2
tcp flags:	0x00
interface output:	Gig0/0
counter packets:	1
timestamp first:	15:13:02.863
timestamp last:	15:13:02.863
ip source as:	0
ip destination as:	0

75

**HEH.be** Sciences et technologies

## Netflow

- Vérification de Netflow

The screenshot shows the Netflow Collector application window. On the left, there's a pie chart divided into four segments, with one segment labeled 'HTTP'. A red arrow points from this segment to the text 'HTTP'. Another red arrow points from the right side of the pie chart to the text 'Horodatage' (Timestamping). On the right, a detailed table of flow information is displayed, with several fields highlighted by red boxes. The highlighted fields include:

Traffic Contribution: 25% (1/4)	
Flow information:	
IPV4 SOURCE ADDRESS:	10.2.1.2
IPV4 DESTINATION ADDRESS:	193.190.65.24
INTERFACE INPUT:	Gig0/0
TRNS SOURCE PORT:	1025
TRNS DESTINATION PORT:	80
IP TOS:	0x00
IP PROTOCOL:	6
FLOW SAMPLER ID:	0
FLOW DIRECTION:	Input
ip4 source mask:	/16
ip4 destination mask:	/24
ip4 source bytes:	205
ip4 next hop address:	0.0.0.0
tcp flags:	0x02
interface output:	Se0/0/0
counter packets:	5
timestamp first:	15:13:42.730
timestamp last:	15:13:42.741
ip source as:	0
ip destination as:	0

76

- Configuration de Flexible Netflow

- Configurer où envoyer les données

```
R(config)# flow exporter Exporter-name
R(config-flow-exporter)# destination ip-address
R(config-flow-exporter)# export-protocol netflow-v9
R(config-flow-exporter)# transport udp 9996
```

- Configurer quelles données doivent être collectées

```
R(config)# flow record myrecord
R(config-flow-record)# match ipv4 destination address
R(config-flow-record)# match ipv4 source address
R(config-flow-record)#collect counter bytes
```

- Relier le flow exporter au flow record

```
R(config)# flow monitor mymonitor
R(config-flow-monitor)# exporter Exporter-name
R(config-flow-monitor)# record myrecord
```

- Appliquer la configuration à une interface

```
R(config)# interface interface-name
R(config-if)#ip flow monitor mymonitor [input|output]
```

- Exemple de Flexible Netflow

1. Configurer où envoyer les données

```
R2(config)#flow exporter ExporterSRVWEB
R2(config-flow-exporter)#destination 193.190.65.24
R2(config-flow-exporter)#export-protocol netflow-v9
R2(config-flow-exporter)#transport udp 9996
```

2. Définir les données qui doivent être collectées

```
R2(config)#flow record myrecord
R2(config-flow-record)#match ipv4 destination address
R2(config-flow-record)#match ipv4 source address
R2(config-flow-record)#collect counter bytes
```

3. Relier le flow exporter au flow record

```
R2(config)#flow monitor mymonitor
R2(config-flow-monitor)#exporter ExporterSRVWEB
R2(config-flow-monitor)#record myrecord
```

4. Appliquer la configuration à une interface

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip flow monitor mymonitor input
```

**HEH.be** Sciences et technologies Netflow

- Vérification de Flexible Netflow

Netflow Collector

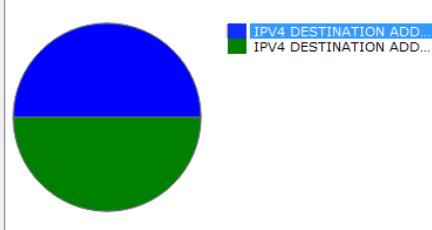
Service

On  off

Traffic Contribution: 50% (1/2)

Flow information:  
IPV4 DESTINATION ADDRESS: 193.190.65.24  
IPV4 SOURCE ADDRESS: 193.191.11.203  
counter bytes: 28

IPV4 DESTINATION ADD...  
IPV4 DESTINATION ADD...



WALLONIE-BRUXELLES ENSEIGNEMENT

UCLouvain

• • • 79

**HEH.be** Sciences et technologies

## Chapitre 2

### AAA (Authentication, Authorization and Accounting)

WALLONIE-BRUXELLES ENSEIGNEMENT

UCLouvain

• • • 80

## Introduction

- **Authentification locale**

- **Local authentication**

- Uniquement via un mot de passe
  - Protection des accès console et terminaux uniquement par un mot de passe.
  - Ne permet pas de savoir quel utilisateur s'est connecté.
- Via un couple username/password
  - Implique de créer des comptes utilisateurs locaux.
  - Un éventuel attaquant doit aussi connaître le username.
  - Permet de savoir quel utilisateur/compte s'est connecté.

- **Base de données locale**

- Chaque périphérique doit être configuré séparément.
- Lourdeur administrative dans les grands réseaux.
- N'offre pas de méthode d'authentification de secours (fallback).

- **Local AAA authentication**

- Idem DB locale, mais autorise des méthodes d'authentification de secours.

## Introduction

- **Authentification centralisée**

- **Server-Based AAA Authentication**

- Les couples username/password sont stockés sur un serveur distant.

- **Protocoles d'authentification**

- Protocoles utilisés pour la communication entre le routeur et le serveur d'authentification (serveur AAA).
- RADIUS : Remote Authentication Dial-In User Service.
- TACACS+ : Terminal Access Controller Access-Control System Plus.

- **Authentifier, mais pas seulement**

- **Un réseau doit être configuré de manière à :**

- Contrôler quels utilisateurs sont autorisés à s'y connecter (Authentication).
- Contrôler ce que les utilisateurs sont autorisés à faire (Authorization).
- A garder une trace des actions réalisées à des fins de traçabilité ou de comptabilisation (Accounting/Auditing).

- Fonctions AAA

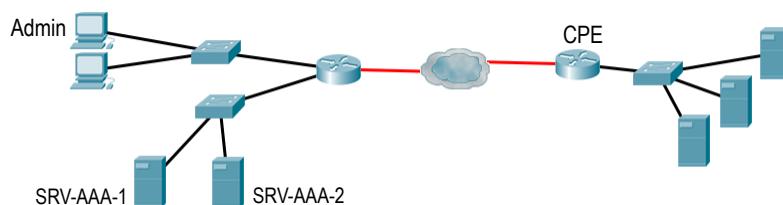
1. Authentication

- Impose à l'utilisateur de fournir une preuve de son identité. Par exemple:
  - Via ce qu'il sait : un mot de passe.
  - Via ce qu'il a : un badge ou un token.
  - Via ce qu'il est : son empreinte digitale, son œil (scan rétinien).
- L'authentification forte consiste à utiliser au moins deux facteurs différents.  
Par exemple,
  - Un mot de passe et un badge.
  - Un badge et un scan facial.

- Fonctions AAA

- Exemple d'authentification

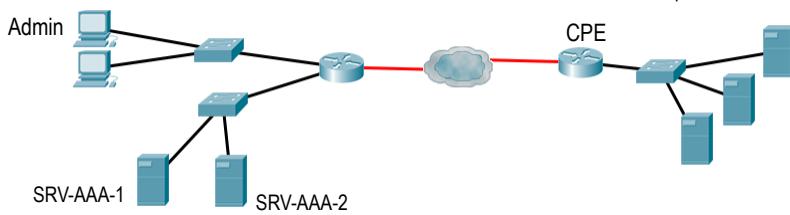
- 1) Un administrateur essaie de se connecter au routeur CPE.
- 2) Le routeur CPE envoie une requête d'authentification demandant au serveur AAA si l'utilisateur « admin » peut se connecter.
- 3) Le serveur répond au routeur en demandant une authentification : "Demande son mot de passe" ou « demande son token ».
- 4) L'utilisateur entre son mot de passe et le routeur CPE le transmet au serveur qui répond si l'authentification est réussie ou non.



- Fonctions AAA (suite)

### 2. Authorization

- Les autorisations décrivent les accès/droits dont les utilisateurs disposent une fois authentifiés.
  - Pour chaque action de l'utilisateur, une requête est envoyée au serveur AAA.
- Sur un grand parc de machines, cette fonction peut générer un très grand nombre de requêtes
  - Nécessite de dimensionner le serveur AAA et le réseau en conséquence.



- Fonctions AAA (suite)

### 3. Accounting/Auditing

- Fonction de comptabilisation ou de traçabilité
  - Elle permet d'enregistrer des données sur l'utilisation des systèmes : compte utilisateur, temps de connexion, commandes exécutées, etc.
  - Ces données sont utilisées à des fins de facturation, d'audit et/ou de dépannage.
  - L'enregistrement se fait dans des fichiers ou des bases de données.
- Quand comptabiliser ou garder une trace des événements?
  - L'utilisation de la comptabilisation est optionnelle.
  - Les requêtes de comptabilisation peuvent être lancées suite à différents événements :
    - » Par ex. au début de connexion d'un utilisateur pour pourvoir facturer l'accès.
    - » Par ex. suite à l'exécution d'une commande pour garder un historique des commandes exécutées.

## Introduction

- Fonctions AAA (suite)

3. Accounting/Auditing (suite)

- Pourquoi comptabiliser?

- Pour facturer l'utilisation de ressources.
- Les utilisateurs étant "surveillés", ils font plus attention.
- Pour détecter des actions suspectes voir interdites.
- Pour mieux cibler la source d'un problème et intervenir.
- Pour avoir une trace légale des actions effectuées sur un système de l'entreprise.

- Comptabiliser quoi?

- Les commandes exécutées.
- Les temps de connexion.
- Le volume de données (nombres d'octets transmis).
- Les informations sur les connexions Telnet ou SSH (qui, quand, ...).
- Les événements systèmes (lorsque le système redémarre par exemple).

## Authentification locale AAA

- Configurer l'authentification locale AAA

- Ajouter les noms d'utilisateurs et les mots de passe à la DB locale

```
R(config)#username nomducompte algorithm-type scrypt secret mdp
```

- Activer AAA au niveau du routeur

```
R(config)# aaa new-model
```

- Appliquer l'authentification AAA

```
R(config)#line [aux |console |tty |vty] lineNumber [end-line-N°]
R(config-line)# login authentication {default | list-name}
```

- Configurer l'authentification locale AAA (suite)

- Configurer les paramètres AAA

```
R(config)# aaa authentication login { default | list-name }
method1 ...[method4]
```

- **default** : indique qu'il s'agit du type d'authentification par défaut à appliquer sur toutes les lignes.
- **list-name** : nom donné à la liste des méthodes en train d'être créée. La création d'une liste est prioritaire par rapport à l'authentification par défaut.
- **method** : il est possible de définir jusqu'à 4 méthodes d'authentification (fallback).

- Méthodes d'authentification supportées

- **enable** : utilise le mdp défini par "enable password" (et pas en secret?).
- **krb5** : utilise Kerberos 5 pour l'authentification.
- **krb5-telnet** : utilise Kerberos 5 pour authentifier une connexion telnet.
- **line** : utilise le mdp défini dans la configuration "line".
- **local** : utilise le couple login/password, seul le mdp étant sensible à la casse.
- **local-case** : utilise le couple login/password sensible à la casse.
- **none** : pas d'authentification, toutes les demandes sont acceptées.
- **groupe radius** : utilise la liste des serveurs RADIUS pour l'authentification.
- **groupe tacacs+** : utilise la liste des serveurs TACACS+ pour l'authentification.
- **group groupe-name** : utilise un sous-ensemble de serveurs défini par une commande "aaa group server radius" or "aaa group server tacacs+".

- Exemple de configuration de l'authentification locale AAA

```
R(config)# aaa authentication login default local enable
R(config)# aaa authentication login SSH-LOGIN local-case
R(config)# line vty 0 4
R(config-line)# login authentication SSH-LOGIN
```

- **Default** : indique qu'il s'agit du type d'authentification par défaut à appliquer sur toutes les lignes.
- **Local** : utilise la DB locale.
- **Enable** : utilisation du mdp enable si "local" n'est pas possible.
- **SSH-LOGIN** : nom de la liste d'authentification à utiliser avec les lignes vty. Elle est prioritaire sur la méthode par défaut.
- **Local-case** : utilise la DB locale et les noms d'utilisateurs sont aussi sensibles à la casse.

- Remarques

- La commande "aaa new-model"

- Applique immédiatement l'authentification locale à toutes les lignes et interfaces (excepté la console).
      - Il est donc conseillé de définir un nom d'utilisateur et un mot de passe *avant* de commencer la configuration AAA.
      - Sinon, une connexion distante peut être perdue avec impossibilité de se reconnecter à distance.
    - Sauvegardez vos configurations avant de configurer vos commandes AAA.
      - Ceci vous permet de pouvoir récupérer un accès en cas de verrouillage imprévu.

- La commande "no authentication login"

- Permet de revenir à la méthode d'authentification par défaut

- Autres configurations AAA

- Verrouiller l'accès à un compte après un certain nombre de tentatives de connexion échouées.

```
R(config)# aaa local authentication attempts max-fail number
```

- Configurer un délai entre deux tentatives de connexion

```
R(config)# login seconds
```

- Lister les comptes verrouillés

```
R(config)# show aaa local user lockout
```

- Déverrouiller les comptes bloqués.

```
R(config)# clear aaa local user lockout [all | username]
```

- Session AAA

- Unique ID

- Si un utilisateur se connecte en utilisant AAA, une session est établie et est associée à un numéro de session unique (Unique ID).

- Les attributs de la session AAA sont enregistré dans la DB AAA.

- Afficher l'identifiant d'une sessions AAA

```
R# show aaa sessions
```

R1# sho aaa sessions
Total sessions since last reload: 1
Session Id:1
Unique Id:1
User Name:admin
IP Address:10.2.1.2
Idle Time: 0
CT Call Handle: 0

## Authentification locale AAA

## • Session AAA

## – Afficher les attributs des sessions AAA

R# show aaa user unique-ID

```
R1#show aaa user 1
-----
Unique id 1 is currently in use.
< Lignes omises >
Interface:
TTY Num = 194
Stop Received = 0
Byte/Packet Counts till Call Start:
      Start Bytes In = 0           Start Bytes Out = 0
      Start Paks In = 0          Start Paks Out = 0
< Lignes omises >
StartTime = 13:51:47 UTC oct. 29 2016
Component = EXEC
Authen: service=LOGIN type=ASCII method=LOCAL
Kerb: No data available
< Lignes omises >
General:
Unique Id = 000001
Session Id = 000001
Attribute List:
        47B2AC48 0 00000009 interface(174) 4 tty194
        47B2AC58 0 00000001 port-type(178) 4 Virtual Terminal
        47B2AC68 0 00000009 clid(28) 5 10.2.1.2
```

## Authentification locale AAA

## • Dépanner un problème de connexion

R# debug aaa ?

```
R1# debug aaa ?
accounting          Accounting
administrative       Administrative
api                 AAA api events
attr                AAA Attr Manager
authentication      Authentication
authorization       Authorization
cache               Cache activities
coa                AAA CoA processing
db                  AAA DB Manager
dead-criteria      AAA Dead-Criteria Info
id                 AAA Unique Id
ipc                AAA IPC
mlist-ref-count    Method list reference counts
mlist-state         Information about AAA method
list state change and notification
per-user           Per-user attributes
pod                AAA POD processing
protocol           AAA protocol processing
server-ref-count   Server handle reference counts
sg-ref-count        Server group handle reference counts
sg-server-selection Server Group Server Selection
subsys             AAA Subsystem
testing            Info. about AAA generated test packets
```

- Dépanner un problème de connexion

```
R# debug aaa authentication
```

```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user='ruser='
      ports='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
      action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
      (user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
      (user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

- Dépanner un problème de connexion

```
R# debug aaa authentication
```

- Rien d'intéressant sous P.T.!

```
R1#debug aaa authentication
AAA Authentication debugging is on
R1#
*oct. 29 14:04:44.614: AAA/BIND(2): Bind i/f
*oct. 29 14:04:44.614: AAA/AUTHEN/LOGIN(2): Pick method list
'default'
*oct. 29 14:05:17.747: AAA/BIND(3): Bind i/f
*oct. 29 14:05:17.747: AAA/AUTHEN/LOGIN(3): Pick method list
'default'
```

Authentification réussie

Authentification échouée

- Protocoles de communication
  - RADIUS, TACACS+
- Exemples de serveurs utilisables
  - Cisco Identity Services Engine (ISE)
    - Supporte RADIUS et TACACS+
    - Peut être intégré à l'AD Microsoft Windows.
  - AD
    - Microsoft Windows Server peut être configuré en tant que serveur AAA.
  - LDAP
    - Lightweight Directory Access Protocol.
  - FreeRADIUS
    - Serveur RADIUS open source
  - Remarque
    - Plusieurs serveurs peuvent être configurés pour offrir de la redondance.

- Caractéristiques de TACACS+
  - Processus d'authentification et d'autorisation séparés
    - Cela offre plus de modularité que RADIUS.
    - Par ex. il est possible d'utiliser TACACS+ pour l'autorisation et la comptabilisation et une autre méthode pour l'authentification.
  - Confidentialité
    - L'entièreté de chaque paquet TACACS+ est chiffré.
  - Protocole de couche transport
    - Utilisation de TCP.
  - CHAP
    - Bidirectionnel.
  - Comptabilisation/traçabilité
    - Possibilités sont plus limitées qu'avec RADIUS.
  - Protocole propriétaire Cisco
    - TACACS+ est incompatible avec les anciennes versions TACACS.

- **Caractéristiques de RADIUS**

- **Fonctionnalités**

- Authentification et autorisation RADIUS associées dans un seul processus.
    - Il n'est pas possible de séparer les deux.

- **Confidentialité**

- Chiffrement du mot de passe uniquement (même avec PAP).
    - RADIUS ne permet pas de chiffrer les noms d'utilisateur, les informations de comptabilité ou toute autre information transmise dans un message RADIUS.

- **Protocole de couche transport**

- Utilisation d'UDP port 1812 et 1813.

- **CHAP**

- Unidirectionnel, (Challenge du serveur, réponse du client).

- **Comptabilisation/traçabilité**

- Possibilités étendues.

- **Standard ouvert**

- **Configuration pour un serveur RADIUS**

- **Activer AAA**

- Permet d'avoir accès à toutes les commandes AAA

```
R(config)# aaa new-model
```

- **Renseigner le serveur RADIUS**

```
R(config)# radius-server host 192.168.0.1 auth-port 1812 acct-port 1813
```

- Si plusieurs serveurs Radius, une commande par serveur.
    - Auth-port : N° du port utilisé pour l'authentification.
    - acct-port : N° du port utilisé pour la comptabilisation.
    - Les ports sont 1645 et 1646 par défaut. L'IANA a réservé les ports 1812 (authentication) et 1813 ( accounting).

- **Configurer la clé privée pour l'encryption**

```
R(config-radius-server)# key r@dius-sh@red-key
```

- **Variante**

```
R(config)#radius host 192.168.0.230 key r@dius-sh@red-key
```

- Configuration pour un serveur TACACS+

- Activer AAA

```
R(config) #aaa new-model
```

- Renseigner le serveur TACACS

```
Router(config) # tacacs-server host IPorNAME [single-connection] [port integer] [timeout integer] [key string]
```

- Exemple

```
R(config) #tacacs-server host 192.168.0.1 single-connection  
key tacacs-P@ssw0rd
```

Configuration de l'adresse du serveur (le port d'authentification et autorisation utilisé est celui par défaut : 49)

Maintient une seule connexion TCP pour toute la durée de la session.

Configuration du secret partagé



103

- Configurer la liste des méthodes d'authentification

- Définir les méthodes d'authentification

- Une fois le serveur AAA identifié, il faut l'inclure dans la liste des méthodes d'authentification.

```
R1(config) #aaa authentication login default ?  
enable Use enable password for authentication.  
group Use Server-group.  
local Use local username authentication.  
none NO authentication.
```

- Exemple

```
R(config) # aaa authentication login default group tacacs+  
group radius local-case
```

- Tentative d'authentification avec un serveur TACACS+, ensuite avec un serveur RADIUS, ensuite en utilisant la base de données locale.
    - Attention :
      - Tentative avec radius uniquement si le serveur TACACS+ ne répond pas.
      - Tentative avec DB locale uniquement si aucun des serveurs ne répond.



104

- Méthodes d'authentification

```
R1(config)# aaa authentication login default ?
cache      Use Cached-group
enable     Use enable password for authentication.
group      Use Server-group
krb5       Use Kerberos 5 authentication.
krb5-telnet Allow logins only if already authenticated via Kerberos V
              Telnet.
line       Use line password for authentication.
local      Use local username authentication.
local-case  Use case-sensitive local username authentication.
none       NO authentication.
passwd-expiry enable the login list to provide password aging support

R1(config)# aaa authentication login default group ?
WORD      Server-group name
ldap      Use list of all LDAP hosts.
radius    Use list of all Radius hosts.
tacacs+   Use list of all Tacacs+ hosts.
```

Source : Cisco System Inc., Networking academy, CCNA security, page 3.4.1.4 figure 1

- Commandes Debug

- En cas de problème, il est intéressant d'utiliser les commandes debug pour disposer d'informations concernant la phase d'authentification.

```
R1# debug radius ?
accounting  RADIUS accounting packets only
authentication RADIUS authentication packets only
brief        Only I/O transactions are recorded
elog         RADIUS event logging
failover     Packets sent upon fail-over
local-server Local RADIUS server
retransmit   Retransmission of packets
verbose     Include non essential RADIUS debugs
<cr>
```

Source : Cisco System Inc., Networking academy, CCNA security, page 3.4.2.2 figure 1

```
R1# debug tacacs ?
accounting  TACACS+ protocol accounting
authentication TACACS+ protocol authentication
authorization TACACS+ protocol authorization
events       TACACS+ protocol events
packet      TACACS+ packets
<cr>
```

Source : Cisco System Inc., Networking academy, CCNA security, page 3.4.2.2 figure 2

```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

Source : Cisco System Inc., Networking academy, CCNA security, page 3.4.2.1

- Commandes Debug

```
R1# debug tacacs
TACACS access control debugging is on
R1#

14:00:09: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.1.101 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.1.101 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.1.101 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Source : Cisco System Inc., Networking academy, CCNA security, page 3.4.2.2 figure 3

- Commandes Debug

```
R1# debug tacacs
TACACS access control debugging is on
R1#

13:53:35: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.1.101 (AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.1.101 (AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.1.101 (AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Source : Cisco System Inc., Networking academy, CCNA security, page 3.4.2.2 figure 4

- **Les autorisations**

- **Autorisation**

- Une fois authentifié, il faut s'assurer que les utilisateurs ont uniquement accès à certaines fonctions, programmes ou parties du réseau.

- **Exemple avec une connexion à un périphérique réseau**

- Une fois authentifié, un utilisateur est connecté à un périphérique réseau.
    - Cet utilisateur ne doit pas nécessairement pouvoir exécuter toutes les commandes disponibles sur le périphérique .
    - Un contrôle des autorisations associées à son compte utilisateur est nécessaire.
    - Ainsi, dès qu'une commande est entrée, un appel est fait au serveur AAA pour vérifier que l'utilisateur a bien l'autorisation d'exécuter cette commande.
    - Sur un grand parc de machines, ce la peut générer un grand nombre de requêtes.

- **Méthodes d'autorisations supportées**

- **TACACS+**

- Échange d'informations avec un serveur TACACS+ pour vérifier les autorisations attribuées à un utilisateur.

- **RADIUS**

- Échange d'informations avec un serveur TACACS+ pour vérifier les autorisations attribuées à un utilisateur.

- **If-Authenticated**

- Si l'utilisateur a été authentifié avec succès, il est d'office autorisé à accéder à la fonction demandée.

- **None**

- L'autorisation n'est pas active sur cette ligne / interface.

- **Local**

- Vérification de la base de données locale pour autoriser des droits spécifiques aux utilisateurs.
    - Seul un nombre limité de fonctions peuvent être contrôlées via la DB locale.

- Configuration des autorisations

```
R(config)# aaa authorization { network | exec | commands
level } { default | liste-name} method1 ...[ method4]
```

- **network** : permet d'autoriser des services réseau (par exemple PPP).
- **exec** : permet d'autoriser l'exécution d'un shell.
- **command** : permet d'autoriser l'exécution de commandes shell.

- Remarques

- Par défaut, aaa authorization n'est pas activé  
→ tous les utilisateurs ont accès à tout.
- Une fois aaa authorization activé, par défaut plus aucun accès n'est autorisé.
  - ATTENTION : il faut donc créer un utilisateur avec tous les droits, sans cela, l'admin sera automatiquement déconnecté.
  - R# username admin algorithm-type scrypt secret P@ssphr@se

- Server-based AAA accounting

- Facturation

- La comptabilisation permet de suivre et donc comptabiliser l'usage des ressources.
- Souvent, la comptabilisation est liée à la gestion financière qui l'utilise pour la facturation.

- Au niveau sécurité, la comptabilisation est intéressante pour

- Créer une liste des personnes qui se connectent et de quand ils se connectent.
  - Cela facilite la détection de connexion "étranges", à des moments inhabituels.
- Créer une liste horodatée des modifications qui sont effectuées par chaque administrateur.
  - Connaître les opérations effectuées facilite le dépannage.
- Ces enregistrements fournissent des renseignements utiles dans le cadre d'audits de sécurité.
- On parle plutôt de traçabilité que de comptabilisation.

- Configuration de la comptabilisation

```
R(config)# aaa accounting { network | exec | command
| connection } { default | liste-name } {start-stop |stop-
only |none } [broadcast] method1 ...[ method4]
```

- Types de comptabilisation

- **network** : active la comptabilisation sur les services réseau.
  - Par exemple comptabilise le nombre de paquets transmis lors d'une session PPP.
- **exec** : active la comptabilisation sur les sessions shell.
  - Comptabilise "le nom d'utilisateur, la date, les dates (start et stop), et l'adresse IP d'une session shell.
- **command** : active la comptabilisation sur les commandes du mode EXEC.
  - Enregistre la liste des commandes exécutées pour un niveau de privilège déterminé, la date d'exécution et l'utilisateur qui a exécuté la commande.
- **connection** : active la comptabilisation sur les connexions sortantes (ssh).

- Configuration de la comptabilisation

- Méthode : default | list-name :

- Comptabilisation par défaut ou utilisation d'une liste de méthodes de comptabilisation.
- Une fois la comptabilisation activée, la méthode de comptabilisation par défaut s'applique à toutes les interfaces (sauf celle où une list-name est déjà appliquée).

- Déclenchement de la comptabilisation (= record types or trigger)

- Indique quand la comptabilisation doit commencer/arrêter les enregistrements.
- Start-stop :
  - » Fourni des enregistrement "start" une fois la phase d'authentification réussie et "stop" à la fin du processus.
- Stop-only :
  - » Envoie une notification "stop" à la fin du processus utilisateur.
- None :
  - » désactive la comptabilisation sur une ligne ou une interface.

- Broadcast :

- Permet d'envoyer les informations de comptabilisation vers plusieurs serveurs AAA.

## Server-based AAA example

- Exemple de configuration AAA

```
R(config) # aaa new-model
R(config) # aaa authentication login default group radius local
R(config) # aaa authentication enable default group radius enable
R(config) # aaa authorization config-commands
R(config) # aaa authorization exec default group radius local if-
authenticated
R(config) # aaa authorization commands 1 default group radius if-
authenticated
R(config) # aaa authorization commands 15 default group radius
local if-authenticated
R(config) # aaa accounting exec default start-stop group radius
R(config) # aaa accounting commands 0 default start-stop group
radius
R(config) # aaa accounting commands 1 default start-stop group
radius
R(config) # aaa accounting commands 15 default start-stop group
radius
```

## 802.1X

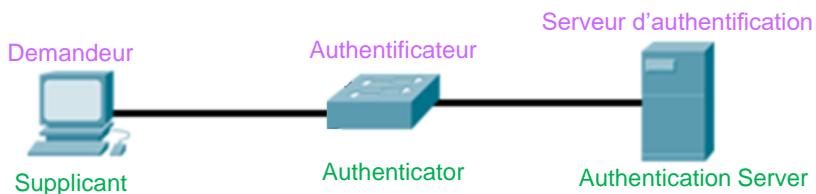
- Norme IEEE 802.1X

- Port-based Network Access Control

- Protocole de contrôle d'accès basé sur les ports.
    - L'accès au réseau est refusé tant que l'utilisateur ne s'est pas authentifié.

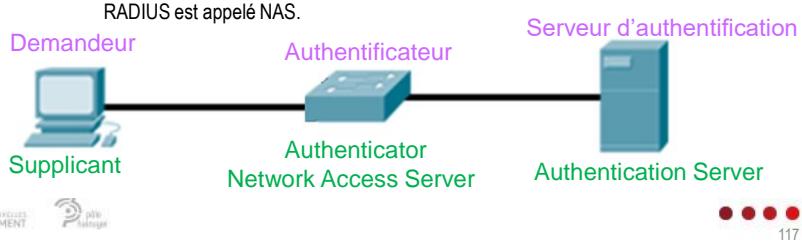
- Supplicant

- Le poste de travail doit exécuter un logiciel client compatible 802.1X (supplicant).
    - L'authentification est réalisée sans communication directe entre le poste de travail et le serveur. Le client ne connaît ni le nom ni l'IP du serveur.



– **Authenticator**

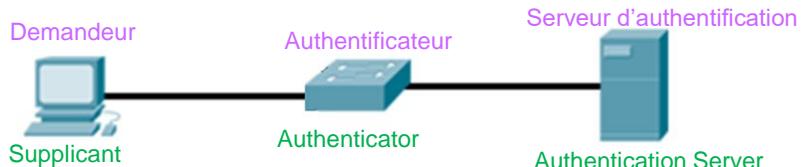
- Il contrôle l'accès physique au réseau, sur base du résultat de l'authentification
  - Il demande des informations d'identification au client et les transfèrent au serveur pour vérification.
  - Il relaie les réponses du serveur vers le client.
- Un agent RADIUS est présent sur l'authentificateur
  - Il communique avec le serveur RADIUS via des trames EAP (encapsulation EAP Over RADIUS).
- **NAS : Network Access Server**
  - Dans la terminologie RADIUS, le commutateur ou le point d'accès client du serveur RADIUS est appelé NAS.



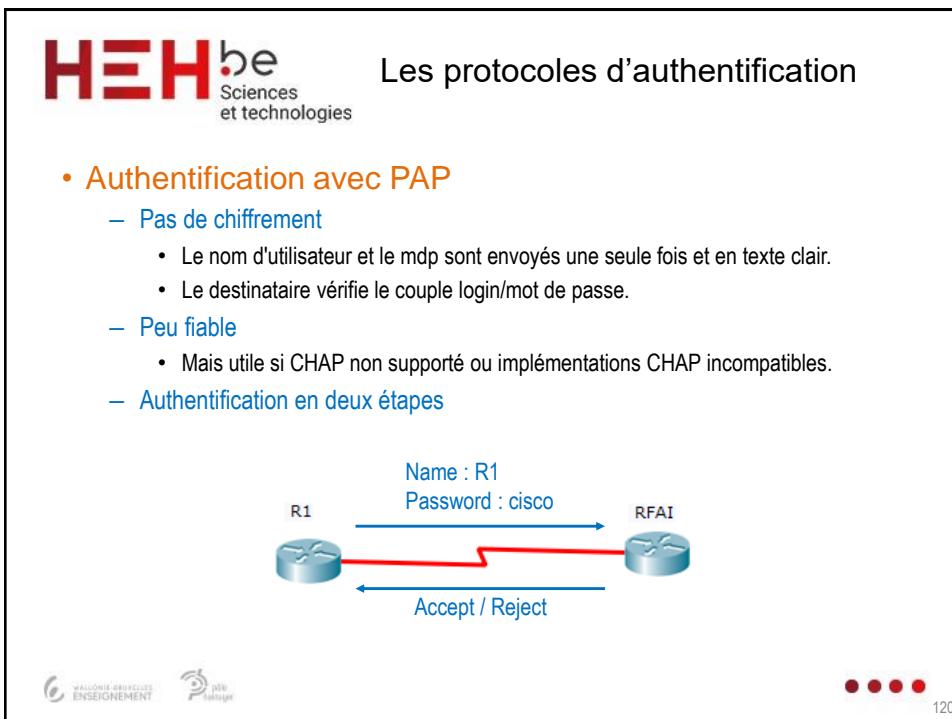
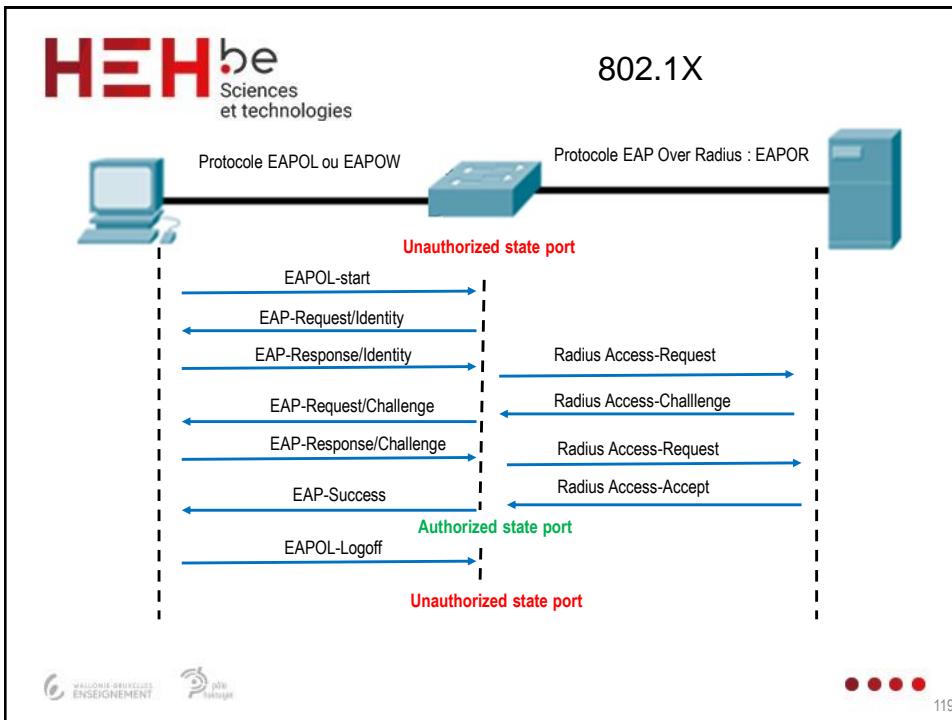
• • •  
117

– **Authentication Server**

- Equipment qui réalise l'authentification et informe l'authentificateur.
- **EAP : Extensible Authentication Protocol**
  - « Protocole de transport » de protocoles d'authentification.
    - Il définit des mécanismes d'échanges de données d'authentification entre équipements.
  - Permet l'indépendance entre le transport et la méthode d'authentification.
  - Seuls le supplicant et le serveur doivent connaître le protocole d'authentification



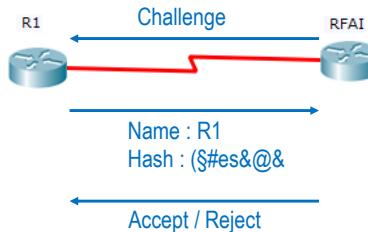
• • •  
118



## Les protocoles d'authentification

- Authentification avec CHAP

  - Authentification en trois étapes

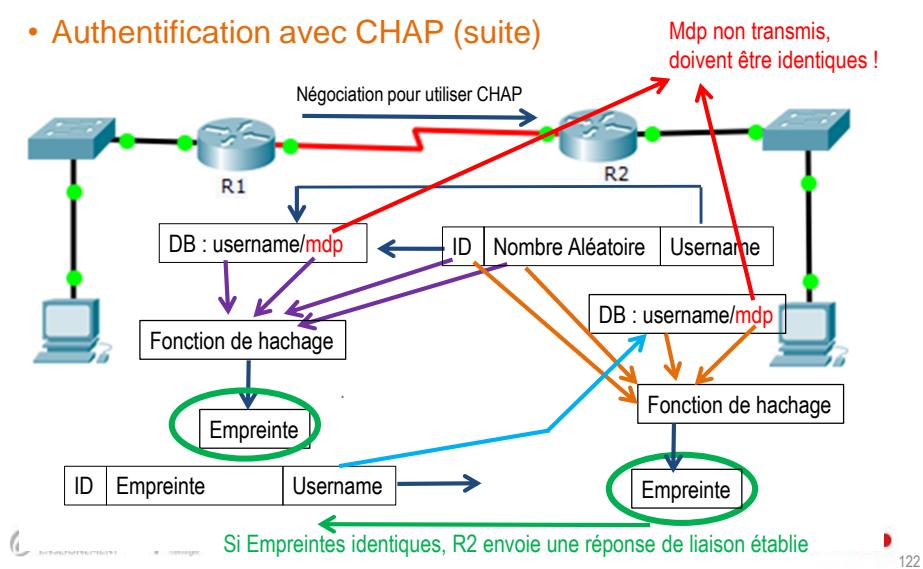




  - Le mot de passe n'est pas transmis.
  - Des challenges sont transmis régulièrement afin d'authentifier régulièrement connexion.

## Les protocoles d'authentification

- Authentification avec CHAP (suite)



- **Authentification avec MS-CHAP**

- Microsoft a développé une variante qui ajoute une authentification mutuelle
  - Il y a authentification du serveur et authentification du client.
  - MSCHAP-Version1, puis MSCHAP-V2.

- **Authentification avec EAP/TLS**

- **Authentification via des certificats**

- Client et serveur doivent posséder un certificat.
- Ces certificats sont échangés et vérifiés
- TLS permet aussi d'obtenir un tunnel chiffré mais qui n'est pas utilisé ici.

- Nécessite de distribuer des certificats à tous les utilisateurs

- **Authentification avec EAP/TTLS**

- **Tunneled Transport Layer Security**

- Comme EAP/TLS, création d'un tunnel chiffré, mais permet de pallier la nécessité de distribuer des certificats à tous les utilisateurs. Similaire à PEAP

- **Authentification EAP/PEAP**

- **Protected EAP**

- Protocole qui a été développé par Microsoft, Cisco et RSA security.
- Comme EAP/TLS, création d'un tunnel chiffré, mais permet de pallier la nécessité de distribuer des certificats à tous les utilisateurs.

- **Authentification mutuelle asymétrique**

- **Le serveur est authentifié par son certificat auprès du client**

- Le client doit uniquement posséder le certificat de l'autorité qui a émis le certificat du serveur.

- **Le client est authentifié via un mot de passe**

- Le serveur d'authentification devra avoir une base de données des mots de passe (AD, LDAP, ...).
- Le mot de passe est généralement vérifié via des échanges MSCHAP-V2 au travers du tunnel chiffré.

### • États d'un port 802.1X

- L'état d'un port 802.1X détermine si le client est autorisé à accéder au réseau

```
Sw(config)# authentication port-control { auto | forced-authorized | forced-unauthorized }
```

- Auto

- Active l'authentification 802.1X.
- Le port est placé dans un état "unauthorized" : seules les trames EAP sont autorisées.
- Si l'authentification réussie, le port passe en état "authorized".
  - » Le serveur envoie l'ordre d'ouvrir le port et sur un VLAN donné.
- Si un port 802.1X change d'état (up -> down) ou s'il reçoit un message de déconnexion (logoff), il repasse dans l'état unauthorized.

- Force-authorized

- Tout trafic est autorisé, aucune authentification 802.1X n'est requise. C'est l'état par défaut.

- Force-unauthorized

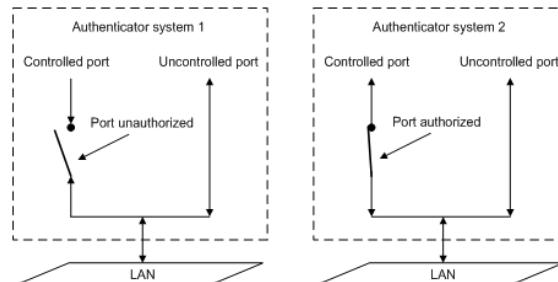
- Tout trafic est refusé. Aucune authentification n'est possible pour autoriser le trafic.

### • PAE : Port Access Entity

- 802.1X définit deux entités de port logique (PAE) pour un port authentifié :

- Tout se passe comme si chaque port était divisé en deux ports :

1. Un port contrôlé dont l'état dépend du résultat de l'authentication.
2. Un port non contrôlé qui laisse passer uniquement des trames EAP.



Source : [http://www.h3c.com.hk/res/201211/14/20121114\\_1453982\\_image002\\_761930\\_1285\\_0.png](http://www.h3c.com.hk/res/201211/14/20121114_1453982_image002_761930_1285_0.png)

- Exemple de configuration 802.1X

- Activer globalement l'authentification 802.1X

```
S(config)# dot1x system-auth-control
```

- Activer AAA

```
S(config)# aaa new-model
```

- Spécifier l'utilisation de la méthode d'authentification 802.1X

```
S(config)# aaa authentication dot1x {default} method1 ...
```

```
S(config)# aaa authentication dot1x default group radius
```

- Activer l'authentification au niveau de l'interface

```
S(config)# interface fa 0/1
```

```
S(config-if)# dot1x port-control auto
```

- Activer l'authentification 802.1X avec les paramètres par défaut

```
S(config-if)# dot1x pae authenticator
```

- Port Access Entity Authenticator : indique que l'interface du commutateur doit jouer le rôle de l'authentificateur.

- Serveur d'authentification RADIUS

- Serveur RADIUS open source

- Peut être utilisé avec plusieurs sources d'identités (LDAP, AD, SQL, ...).

- Supporte plusieurs méthodes d'authentification (EAP/TLS, PEAP, ...).

- Multi-plateforme (Linux, FreeBSD, macOS, ...)

- Exemples d'utilisation de FreeRADIUS

- Par les FAI pour authentifier des utilisateurs lors de connexions DSL.

- Par les entreprises pour l'authentification d'utilisateurs réseau filaire ou sans fil.

- Par Eduroam.

- Installation de FreeRADIUS

- Installer, vérifier et démarrer FreeRADIUS sur Ubuntu

```
$ sudo apt-get install freeradius
$ freeradius -v
$ sudo /etc/init.d/freeradius start
$ sudo ls /etc/freeradius/3.0
```

```
denis@vmubuntu:~$ freeradius -v
radiusd: FreeRADIUS Version 3.0.20, for host x86_64-pc-linux-gnu, built on Jan 25 2020 at 06:11:13
FreeRADIUS Version 3.0.20
```

```
denis@vmubuntu:~$ sudo ls /etc/freeradius/
(sudo) password for denis:
3.0 clients.conf
denis@vmubuntu:~$ sudo rm /etc/freeradius/clients.conf
denis@vmubuntu:~$ sudo ls /etc/freeradius/
3.0
denis@vmubuntu:~$ sudo ls /etc/freeradius/3.0
clients.conf experimental.conf mods-available panic.gdb radiusd.conf sites-enabled users
clients.conf hints mods-config polity.d README.rst templates.conf
dictionary huntgroups mods-enabled proxy.conf sites-available trigger.conf
```

- Le fichier radius.conf

- Contient les paramètres de bases et la définition des fonctions souhaitées

- Contient les paramètres de base
      - Chemins d'accès, port d'écoute, ...
    - Contient la déclaration des modules utilisés
      - Par exemple les modules correspondant aux méthodes d'authentification.
    - Configuration par défaut
      - Est déjà opérationnelle pour un fonctionnement avec « authentification système » (Auth-Type = System). Le serveur cherchera les utilisateurs dans le fichier /etc/passwd.

- Le fichier clients.conf

- Contient la description des équipements autorisés à interroger le serveur RADIUS
  - Seuls les périphériques définis dans ce fichier pourront demander au serveur des authentifications.

```
$ sudo nano clients.conf

client router.exemple {
    ipaddr = 192.168.0.1
    secret = r@dius-sh@red-key
    nastype = cisco
}
```

R(config)#radius host 192.168.0.230 key r@dius-sh@red-key

- Le fichier clients.conf (suite)

- Possibilité de spécifier un seul secret partagé pour un ensemble de clients
  - Lorsqu'une demande d'un client arrive, la meilleure correspondance est choisie.

```
$ sudo nano clients.conf

client 192.168.0.0/24 {
    secret = r@dius-sh@red-key
}
```

R1(config)#radius host 192.168.0.230 key r@dius-sh@red-key  
 R2(config)#radius host 192.168.0.231 key r@dius-sh@red-key  
 Sw(config)#radius host 192.168.0.232 key r@dius-sh@red-key

- Le fichier eap.conf

- Permet de définir les méthodes d'authentification supportées

```
$ sudo nano eap.conf
eap {
    default_eap_type = tls
    timer_expire      = 60
    max_sessions     = 4096
    ... < lignes omises>
    tls {
        certdir = ${confdir}/ssl
        cadir = ${confdir}/ssl
        private_key_password = RadiusKey2013
        private_key_file = ${certdir}/private/radiuskey.pem
        certificate_file = ${certdir}/certs/radiuscert.pem
        ... < lignes omises>
```

- Le fichier users

- Ce fichier est la base de données locale

- Simple fichier texte qui peut être utilisé soit comme base d'autorisations, soit comme base d'authentification ou les deux à la fois.

```
$ sudo nano users
adminrad Cleartext-Password := "motDePass"
          Service-Type = NAS-Prompt-User,
          Cisco-AVPair = "shell:priv-lvl=15"
```

Identifiant de l'utilisateur

Les reply-items, écrits un par ligne.  
 Chaque ligne se termine par une virgule sauf la dernière.

Contient les config-items puis check-items, écrits sur une seule ligne, séparés par des virgules.  
 Pas de point ni virgule à la fin

- Finaliser la configuration

- Redémarrer le service afin que les modifications soient prises en compte.

```
# sudo /etc/init.d/freeradius restart
```

- Démarrer FreRadius en mode debug

```
$ sudo /etc/init.d/freeradius stop
$ sudo freeradius -X
```

- Test de connexion

```
$ radtest {username} {password} {hostname} 10
{radius_secret}
```

## Chapitre 3

# Port Mirroring

## Port mirroring

- Mise en miroir de ports

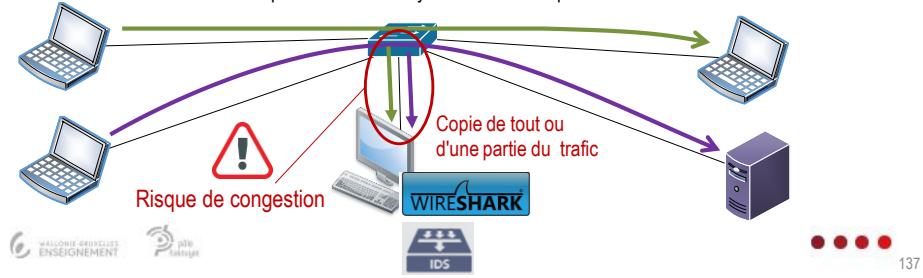
- Principe

- Fonction de surveillance

- Permet à un commutateur de copier le trafic Ethernet entrant par un ou plusieurs ports et l'envoyer vers un autre port.
      - Le port de sortie est généralement connecté à un dispositif d'analyse (analyseur de paquets, IDS, ...).

- La trame d'origine est transmise normalement

- Le SPAN permet ainsi d'analyser le trafic sans perturber le fonctionnement du réseau.



## Port mirroring

- Mise en miroir de ports

- Terminologie

- SPAN, miroir de port, port d'écoute, *port mirroring* ou encore *port monitoring*.

- **SPAN (Switched Port ANalyzer)**

- Terminologie Cisco.

- **VSPAN**

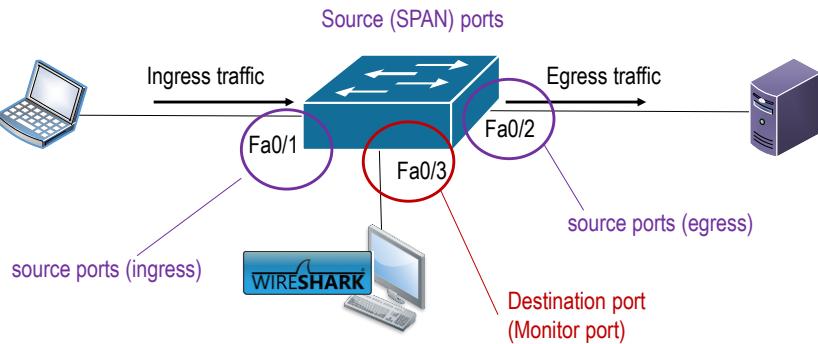
- VLAN-based SPAN : Permet de surveiller tous les ports qui appartiennent à un VLAN particulier en une seule commande.

- **RSPAN (Remote SPAN)**

- On parle de SPAN distant lorsque les ports sources ne sont pas sur le même commutateur que le port destination.

## Port mirroring

### – Terminologie (suite)



## Port mirroring

### • SPAN Session

#### – Session SPAN

- Une session SPAN est l'association entre un ou des ports source (ou VLAN source) et un ou des ports de destination.
- Le commutateur reproduit le trafic entrant ou sortant du port source (ou des ports associés à un VLAN) sur le port de destination.
  - Sur certains modèles de commutateur, il est possible de copier le trafic d'une session SPAN vers plusieurs ports de destination.

#### – Identification d'une session SPAN

- Un numéro de session permet d'identifier une session SPAN locale.

#### – Surveillance du trafic

- Dans une session SPAN ou RSPAN, vous pouvez surveiller tout le trafic d'un port source : le trafic reçu (Rx), transmis (Tx) ou les deux (bidirectionnel).

- Caractéristiques d'un port source SPAN

- Un port source est un port qui est surveillé avec la fonction SPAN
  - N'importe quel type de port (EtherChannel, Fast Ethernet, Gigabit Ethernet, ...)
  - Il peut être surveillé dans plusieurs sessions SPAN.
  - Il ne peut pas être un port de destination.
- Les ports sources peuvent
  - Être configurés pour surveiller le trafic en entrée, en sortie ou les deux.
  - Se trouver dans le même VLAN ou dans des VLAN différents.
  - Être des ports de couche 2 ou de couche 3.
- Port et VLAN source
  - Un commutateur peut prendre en charge un nombre quelconque de ports source et un nombre quelconque de VLAN source.
  - Les sources d'une session SPAN peuvent être des ports ou des VLAN mais pas les deux à la fois.

- Caractéristiques d'un port destination SPAN

- Port de destination
  - Port qui reçoit une copie du trafic des ports source et/ou des VLAN source.
  - Également appelé port de surveillance.
  - Chaque session *local SPAN* ou *Remote SPAN* doit avoir un port de destination.
  - Le nombre de ports de destination supporté dépend de la plate-forme utilisée.
  - Un port de destination ne peut pas être un port source
- Un port de destination n'est plus un port de commutation normal
  - Seul le trafic surveillé transite par ce port.
  - L'état d'un port de destination SPAN est up/down par conception.
  - Il ne participe pas à l'arborescence STP lorsque la session SPAN est active.
  - Il ne participe pas non plus aux protocoles de couche 2 (VTP, CDP, DTP, PAgP).
- Un port de destination ne peut participer qu'à une seule session SPAN à la fois
  - Excepté sur certains modèles de commutateurs.

## Configuration du SPAN local

- Associer une session SPAN avec un port source

```
Sw(config)# monitor session number source [ interface interface-id |  
vlan vlan ] [both | rx | tx]
```

numéro d'identification de la session SPAN

- Associez une session SPAN avec un port de destination

```
Sw(config)# monitor session number destination [ interface interface-  
id | vlan vlan ]
```

- Supprimer les configurations SPAN pour une ou toutes

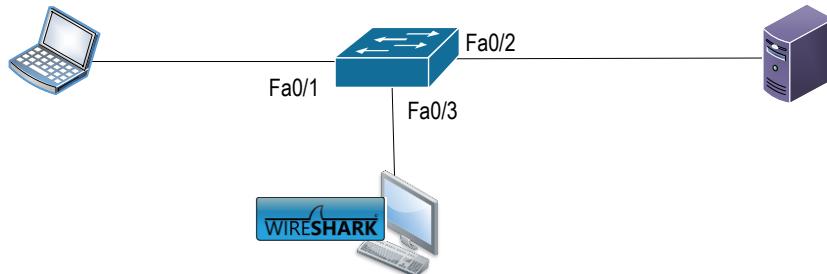
```
Sw(config)# no monitor session {session_number | all |  
local | remote}
```

## Configuration du SPAN local

- Exemple

- Une copie de tout le trafic envoyé et reçu sur le port source Fa0/2 sera transmis au port de destination Fa0/3.

```
Sw(config)# monitor session 1 source interface fa0/2 both  
Sw(config)# monitor session 1 destination interface fa0/3
```



## Configuration du SPAN local

- Vérification du SPAN

```
Sw# show monitor [session session_number]
```

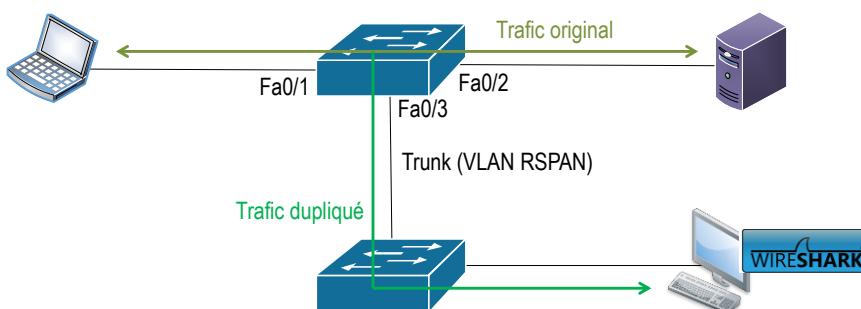
```
SWLANA1#show monitor
Session 1
-----
Type : Local Session
Description : -
Source Ports :
    Both : Fa0/2
Destination Ports : Fa0/3
Encapsulation : Native
    Ingress : Disabled
```

La session SPAN d'entrée est désactivée sur le port de destination.  
Seul le trafic qui quitte le port de destination est copié vers ce port.

## Remote Port mirroring

- RSPAN

- La fonction RSPAN est utile lorsque l'analyseur de paquets ou la sonde IPS se trouve sur un commutateur différent de celui du trafic surveillé.



- Session RSPAN

- RSPAN utilise deux sessions

- Une des sessions est utilisée comme source.
    - L'autre session sert à copier ou à recevoir le trafic d'un VLAN.

- VLAN RSPAN

- Le trafic de chaque session RSPAN est transporté sur des liaisons trunk dans un VLAN RSPAN dédié.
    - Le VLAN RSPAN est configuré par l'administrateur et dédié à la session RSPAN.
    - Le VLAN RSPAN doit être configuré dans tous les commutateurs participants.

- Volume de trafic

- Chaque paquet surveillé est transmis deux fois (trafic normal + une copie).
    - La surveillance d'un grand nombre de ports ou de VLAN peut générer de grandes quantités de trafic réseau.

- Créer le VLAN RSPAN

```
Sw1(config)# vlan vlan-id
Sw1(config-vlan)# remote-span
```

- Créer la session RSPAN source

```
Sw1(config)# monitor session number source [ interface interface-id |
  vlan vlan ]
Sw1(config)# monitor session number destination remote vlan-id ]
```

- Créer la session RSPAN destination

```
Sw2(config)# vlan vlan-id
Sw2(config-vlan)# remote-span
Sw2(config-vlan)# exit
Sw2(config)# monitor session number source remote vlan vlan-id
Sw2(config)# monitor session session_number destination interface
  interface-id
```

## Chapitre 4

# Virtual routing and forwarding

VRF lite

VRF

- **Virtual Routing and Forwarding**

- **Isolation du trafic**

- Certaines organisations peuvent avoir besoin de séparer diverses classes de trafic ou d'isoler des groupes spécifiques d'utilisateurs les uns des autres.
    - Par exemple
      - Une société pourrait vouloir séparer le trafic « invité », le trafic de sous-traitant ou encore le trafic de vidéosurveillance IP du reste du réseau.
      - Un fournisseur doit interconnecter de nombreux sites et services de sociétés distinctes au travers d'un même réseau fédérateur et souhaite les isoler les uns des autres.

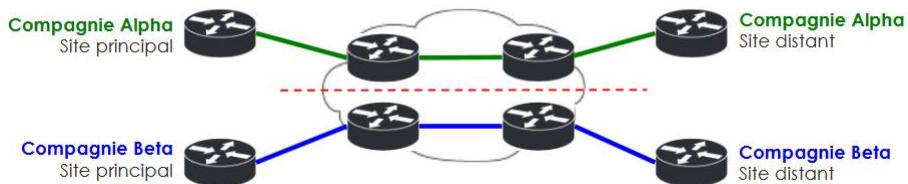


## VRF

- Virtual Routing and Forwarding (suite)

- Isolation physique des ressources ?

- Utilise une infrastructure dédiée pour chaque compagnie.
- Engendre des coûts d'infrastructure importants.

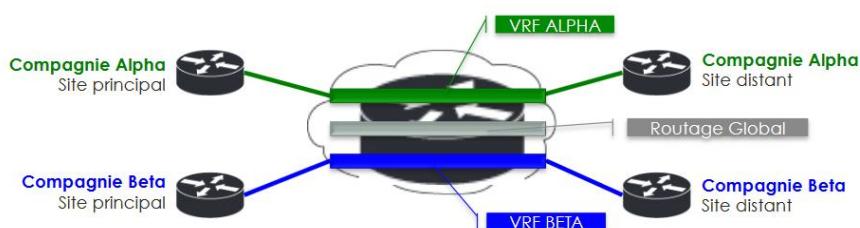


## VRF

- Virtual Routing and Forwarding (suite)

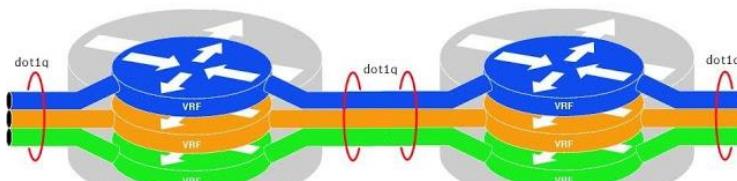
- Isolation virtuelle des ressources

- Les VRF permettent de créer plusieurs routeurs logiques au sein d'un même routeur physique.
  - Chaque VRF dispose de sa propre table de routage.
  - Chaque VRF est indépendante des autres.
  - Les VRF isolent les trafics utilisateurs dans «leur» VRF.
  - Peuvent être utilisées avec des VPN et des protocoles de routage dynamiques.



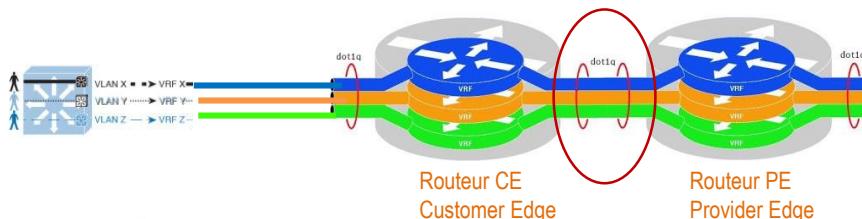
- Virtual Routing and Forwarding (suite)

- Les différents trafics sont isolés de manière virtuelle
  - La table de routage dite « globale » est celle utilisée par défaut, avec ou sans VRF.
  - La table globale (GRF) contient toutes les interfaces IP qui ne font pas partie d'un réseau virtuel spécifique.
- Une interface peut appartenir à une et une seule VRF
  - Interface physique ou sous-interface (subinterface).



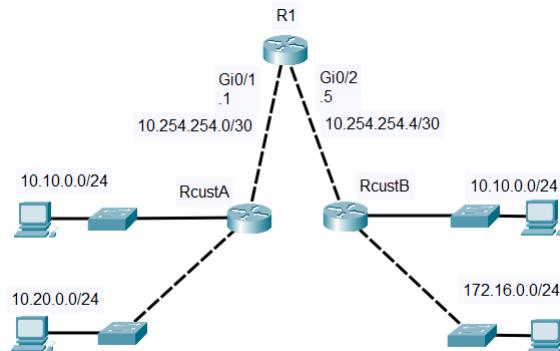
- Virtual Routing and Forwarding (suite)

- Les paquets ne sont routés qu'en fonction des routes de la VRF dans laquelle ils circulent
  - Les paquets arrivant sur une interface sont uniquement transmis aux autres interfaces du même réseau virtuel.
  - Il est donc possible d'utiliser des adresses IP identiques ou qui se chevauchent dans les différents réseaux virtuels.
- Isolation possible jusqu'aux routeurs CE et même aux VLAN



## Configuration de VRF

- Exemple de configuration VRF-Lite



## Configuration de VRF

- Exemple de configuration VRF-Lite (suite)

- Créer les VRF

```
Core1(config)#ip vrf VRF-Name
Core1(config)#ip vrf CustA
Core1(config-vrf)#description VRF Client A
Core1(config-vrf)#exit
```

- Activer IPv4 au sein de la VRF

```
Core1(config)#ip vrf CustA
Core1(config-vrf)#address-family ipv4
Core1(config-vrf)#exit
```

## Configuration de VRF

- Exemple de configuration VRF-Lite (suite)
  - Assigner des interfaces aux VRF

```
Syntaxe:  
Core1(config-if)# ip vrf forwarding VRF-Name  
  
Exemple:  
Core1(config)#interface Gi0/1  
Core1(config-subif)#ip vrf forwarding CustA  
% Interface Gi0/1 IPv4 disabled and address(es) removed due to  
disabling VRF CustA  
  
Core1(config-subif)#ip address 10.254.254.1 255.255.255.252  
% Interface Gi0/1 is linked to a VRF. Enable IPv4 on that VRF  
first.  
Core1(config-subif)#exit
```

## Configuration de VRF

- Vérifier la configuration
  - Afficher les informations sur les VRF

- «Route Distinguisher».
  - Un RD est un identifiant unique permettant d'identifier les routes associées à un VRF lors de la propagation des routes.
  - Il est nécessaire pour garantir l'unicité des routes en cas de chevauchement des adresses IP entre les VRF.

```
Core1#show ip vrf
Name      Default RD      Interfaces
CustA    <not set>      Gi0/1
                  Fa0.12
                  Fa0.11
CustB    <not set>      Gi0/2
```

- Exemple de configuration VRF-Lite (suite)

- Créer des routes statiques

```
Core1# ip route vrf VRF-Name DestNetID DestMask NextHopAddress
Core1# ip route vrf CustA 10.10.0.0 255.255.255.0 10.254.254.2
```

```
Core1(config)#ip route vrf CustA 10.10.0.0 255.255.255.0 10.254.254.2
Core1(config)#ip route vrf CustA 10.20.0.0 255.255.255.0 10.254.254.2
Core1(config)#
Core1(config)#ip route vrf CustB 10.10.0.0 255.255.255.0 10.254.254.6
Core1(config)#ip route vrf CustB 172.16.10.0 255.255.255.0 10.254.254.6
```

- Vérifier la configuration

- Afficher les tables de routage

- La table de routage globale est vide.

```
Core1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from Pfr

Gateway of last resort is not set
```

- Vérifier la configuration

- Afficher les tables de routage

- La table de routage globale est vide.

```
Core1#show ip route vrf CustA

Routing Table: CustA
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
S        10.10.0.0/24 [1/0] via 10.254.254.2
S        10.20.0.0/24 [1/0] via 10.254.254.2
C        10.254.254.0/30 is directly connected, GigabitEthernet0/1
L        10.254.254.1/32 is directly connected, GigabitEthernet0/1
```

161

- Vérifier la configuration

```
Core1#show ip route vrf CustB
```

```
Routing Table: CustB
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
S        10.10.0.0/24 [1/0] via 10.254.254.6
C        10.254.254.4/30 is directly connected, GigabitEthernet0/2
L        10.254.254.5/32 is directly connected, GigabitEthernet0/2
      172.16.0.0/24 is subnetted, 1 subnets
S        172.16.10.0 [1/0] via 10.254.254.6
```

162

- Exemple de configuration VRF-Lite (suite)

- Créer des routes statiques entre VRF et/ou avec la GRF

- Le mot clé **global** indique que le saut suivant (next-hop) est joignable via la table de routage globale et pas la VRF.
    - La table globale doit évidemment avoir une route vers chaque next-hop requis dans chaque VRF.

ATTENTION : on peut alors perdre l'isolation entre ces réseaux !

```
Core1# ip route vrf VRF-Name DestNetID DestMask NextHopAddress global
```

```
Core1# ip route vrf CustA 172.16.10.0 255.255.255.0 10.254.254.2
global
```

- Virtual Routing and Forwarding (suite)

- Partager les routes entre VRF

- Plusieurs FAI pourraient avoir le même VRF en interne et leurs clients les mêmes adresses IP.
      - Comment propager les routes de manière sélective ?
      - Comment identifier les VRF au niveau de la table de routage globale unique et commune de BGP par exemple ?

- La communication entre routeurs de VRF (identiques ou distinctes), peut être implémentée de deux façons

- Routes statiques et table de routage globale.
    - Importation et exportation des route-targets.

- Virtual Routing and Forwarding (suite)

- Route Distinguisher (RD)

- Un RD est un identifiant unique permettant d'identifier les routes associées à un VRF.
    - Il est nécessaire pour garantir l'unicité des routes en cas de chevauchement des adresses IP entre les VRF.
    - Définir les Route Distinguisher :

```
Core1(config)#ip vrf VRF-A
Core1(config-vrf)#rd 100.1
```

- Virtual Routing and Forwarding (suite)

- Route Target (RT)

- C'est une information supplémentaire associée à tout préfixe d'une VRF lors de son export vers BGP.
    - Cette valeur est utilisée pour distinguer et filtrer les préfixes reçus en MP-BGP afin de déterminer vers quelles VRF locales ils doivent être importés.

- Isolation

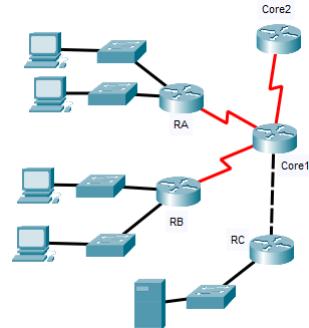
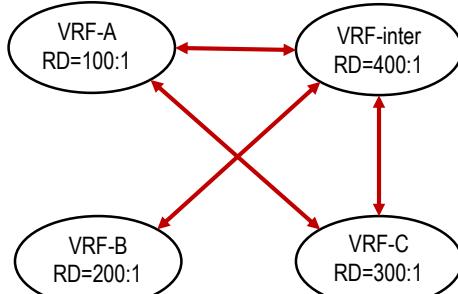
- Classiquement une VRF importera et exporterá un route-target similaire à son route-distinguisher.

- Communication entre VRF

- Pour faire communiquer des VRF différentes entre elles, il faut utiliser des valeurs de RT différentes des RD pour permettre les import/export de préfixes provenant de VRF distinctes.

## VRF

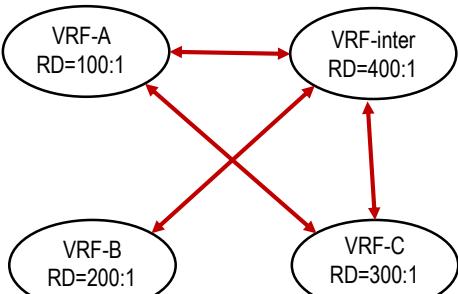
- Virtual Routing and Forwarding (suite)
  - Route Target (suite)



• • • 167

## VRF

- Virtual Routing and Forwarding (suite)
  - Route Target (RT)



```
R(config)# ip vrf VRF-A
R(config-vrf)# route-target export 100:1
R(config-vrf)# route-target import 300:1
R(config-vrf)# route-target import 400:1
```

```
R(config)# ip vrf VRF-B
R(config-vrf)# route-target export 200:1
R(config-vrf)# route-target import 400:1
```

```
R(config)# ip vrf VRF-C
R(config-vrf)# route-target export 300:1
R(config-vrf)# route-target import 100:1
R(config-vrf)# route-target import 200:1
R(config-vrf)# route-target import 400:1
```

```
R(config)# ip vrf VRF-inter
R(config-vrf)# route-target export 400:1
R(config-vrf)# route-target import 100:1
R(config-vrf)# route-target import 200:1
R(config-vrf)# route-target import 300:1
```

• • • 168

- Virtual Routing and Forwarding (suite)

- Routage

- MP-BGP est capable de transporter des informations sur divers protocoles routés dans la même session.
      - IPv4 Unicast, IPv4 Multicast, IPv6 Unicast, IPv6 Multicast, VPNv4, CLNP.
    - Dès lors, il faut pouvoir indiquer à BGP quelles familles d'adresses doivent être échangées avec un voisin particulier.

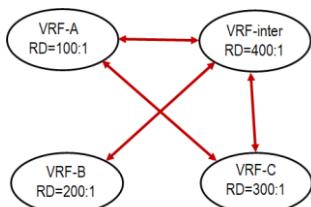
- « address-family »

- Définir un voisin sous une « famille d'adresses » particulière signifie que nous voulons échanger des itinéraires de cette famille d'adresses particulière avec ce voisin.
    - Si elle n'est pas configurée, une famille d'adresse par défaut (invisible) est automatiquement assignée pour la rétrocompatibilité avec les anciennes versions de BGP non compatibles avec le multiprotocole.

- Virtual Routing and Forwarding (suite)

- Redistribution de route

```
R(config) # router bgp <ASN>
R(config-router) # address-family ipv4 vrf <VRFname>
R(config-router-af) # redistribute connected
R(config-router-af) # redistribute static
R(config-router-af) # neighbor <remote_addr> remote <remote_as>
R(config-router-af) # network <address> mask <netmask>
```



- La table de routage de la VRF-A contiendra maintenant des routes vers tous les réseaux sauf ceux du clients B.
- La table de routage de la VRF-A contiendra maintenant des routes vers tous les réseaux sauf ceux des clients A et C .

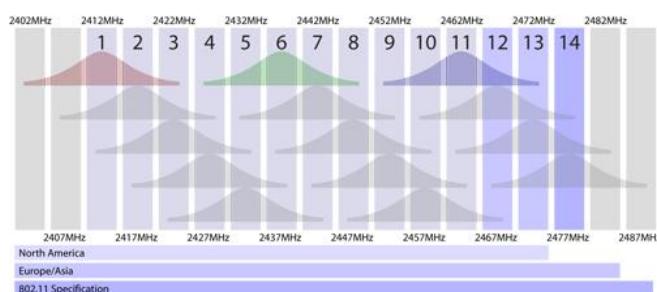
## Chapitre 5

# Analyse spectrale

## Analyse spectrale

### • Analyse spectrale

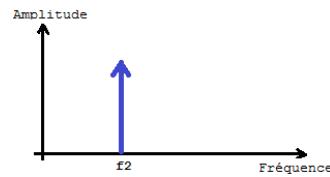
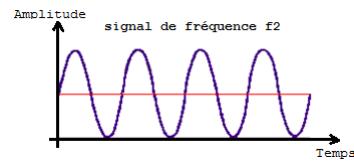
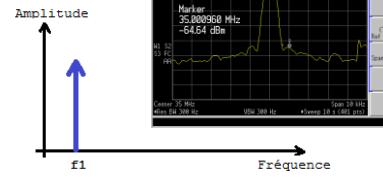
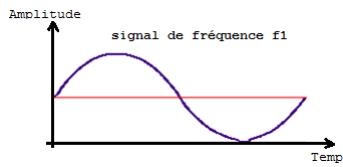
- Quelle place occupe un signal dans le spectre électromagnétique?
- Nombre de canaux utilisables? Nombre de communications simultanées?
  - La bande passante disponible étant limitée, on cherche à concentrer l'énergie et à minimiser l'encombrement spectral.



Source : [http://blog.serverfault.com/files/2012/01/WiFi\\_Channel\\_Overlap.png](http://blog.serverfault.com/files/2012/01/WiFi_Channel_Overlap.png)

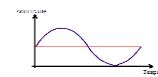
## Analyse spectrale

- Analyse temporelle et analyse spectrale



## Analyse spectrale

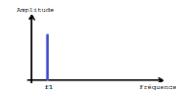
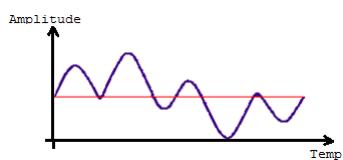
- Analyse temporelle et analyse spectrale



+



=



+

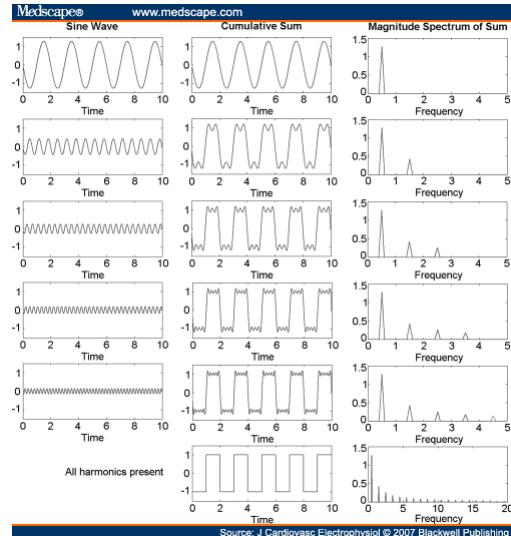


=



## Analyse spectrale

- Simulation



• • •  
175

## Analyse spectrale

- Série de Fourier

- Toute onde périodique peut être décomposée en une somme de sinusoïdes et cosinusoïdes d'amplitudes et de positions de phase appropriées.

$$x(t) = a_0 + \sum_{n=1}^{\infty} (a_n \cos n\omega t + b_n \sin n\omega t)$$

- Exemple du signal carré :

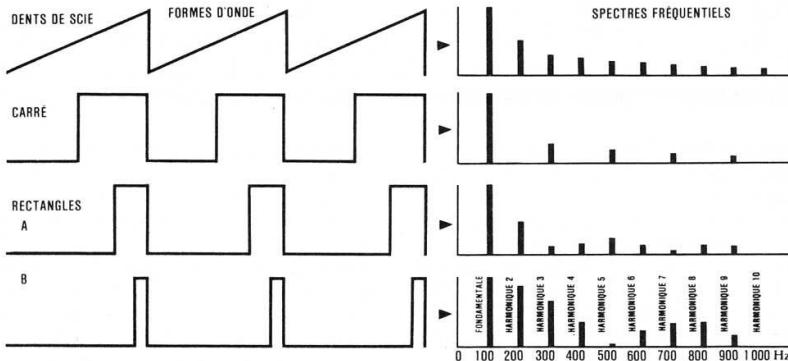
$$x_{\text{carré}}(t) = \frac{4A}{\pi} [ \sin(\omega t) + \frac{1}{3} \sin(3\omega t) + \frac{1}{5} \sin(5\omega t) + \frac{1}{7} \sin(7\omega t) + \dots ]$$

• • •  
176

## Analyse spectrale

- Analyse spectrale

- Fréquence fondamentale et harmoniques

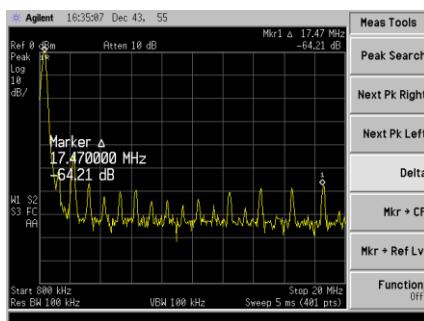


Source : <http://www.pianoweb.fr/synthese/constitutionduonde-etcration-4-agrandi.jpg>

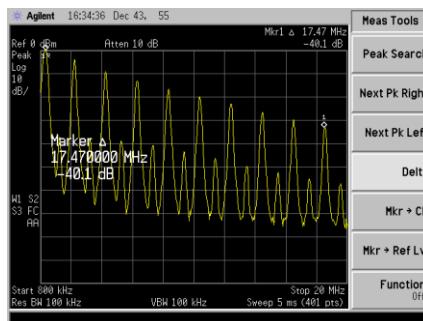
## Analyse spectrale

- Exemple de spectres réels

Signal sinusoïdal

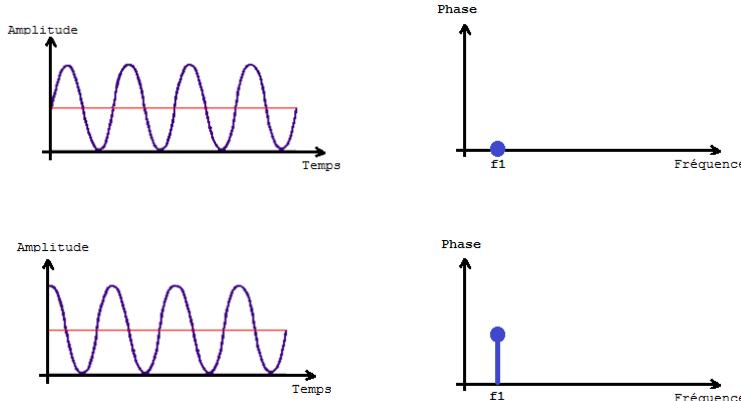


Signal carré



## Analyse spectrale

- Remarque



## Analyse spectrale

- Les décibels

$$dB = 10 \log \frac{P_1}{P_2}$$

Puissance reçue

Puissance émise

- Valeurs courantes

- 3dB = facteur 2
- 10 dB = facteur 10

Décibel	Correspond à une puissance ...
Diminution de 3 dB	Divisée par 2
Augmentation de 3 dB	Multipliée par 2
Diminution de - 10 dB	Divisée par 10
Augmentation de + 10 dB	Multipliée par 10
Diminution de - 20 dB	Divisée par 100
Augmentation de + 20 dB	Multipliée par 100

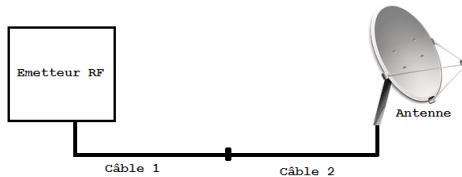
- Facilité d'utilisation

- Au niveau des graphiques

- Des valeurs dont l'écart est important peuvent être facilement représentées sur un graphique.

- Au niveau des calculs

- Exprimés en dB, les gains ou pertes de puissances s'additionnent.
      - Si chacun des câbles jusqu'à l'antenne occasionne -1,5dB de pertes.
      - L'atténuation résultante est de 50% :  $-1,5 - 1,5 = -3\text{dB}$



- Les décibels

- La sensibilité d'un récepteur RF peut lui permettre de détecter un signal de 0,000000001Watts (graduation des axes difficile).

- Les dBm

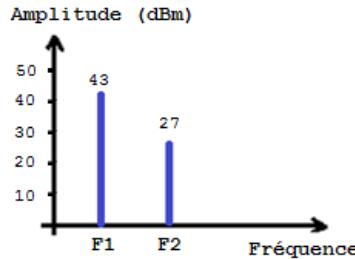
- Les dB fournissent des rapports, pas des valeurs absolues.
  - Formules :

- $\text{dBm} = 10 \log \frac{P_1}{P_{\text{réf}}} = 10 \log \frac{P_1}{1\text{mW}} = 10 \log P_1$  (exprimé en mW)
      - $\log_a(x \cdot y) = \log_a(x) + \log_a(y)$
      - $\log_a(x^n) = n \log_a(x)$
      - $P_1 = 10^{(\text{dBm}/10)}$  (La valeur dBm est exprimée en mW)

## Analyse spectrale

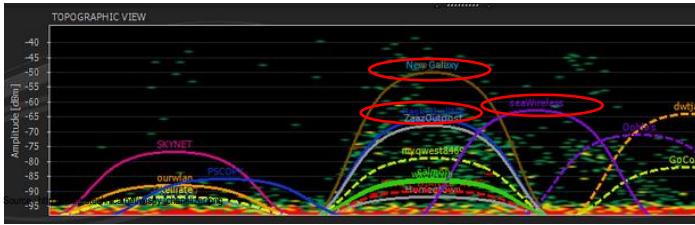
## • Attention : axe logarithmique !

- $43 - 27 = 16$  dB de différence
  - $16 = 10 + 3 + 3$
  - 16 dB correspond à un facteur 40.
- Le signal F1 est 40 fois plus puissant que le signal F2



## Analyse spectrale

## • Attention : axe logarithmique !



- New Galaxy (-50dBm) est 20 fois plus puissant que Sea Wireless (-63dBm).
- Sea Wireless (-63dBm) est 2 fois plus puissant que BasketballNet (-66dBm).

SSID	CH	dBm
bellon54g	1	-92
wireless	1	-93
ounwan	1	-88
Kellilate	1	-92
SKYNET	1	-77
PSCOPY	2	-86
zp_wifi	6	-50
New Galaxy	6	-50
Homegrown	6	-100
salmon	6	-86
mywest8469	6	-79
wxguywa	6	-87
ZazzOutpost	6	-88
KOREY_DIANNE	6	-90
BasketballNet	6	-66
seaWireless	8	-63
Oohla's	10	-71
dwtjain	11	-64
GoCougla	11	-82

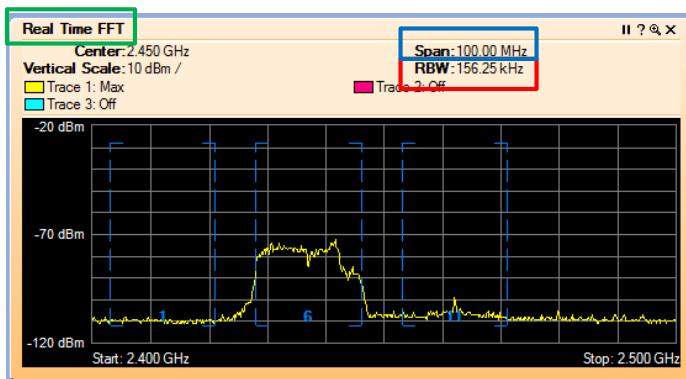
## Analyse spectrale

## • Tableau de conversion dBm-Watt

dBm - Volts - Watts Power Conversion Chart (into 50 ohms)							
dBm	V <sub>pp</sub>	V <sub>p</sub>	Watts	dBm	V <sub>pp</sub>	V <sub>p</sub>	Watts
+40 dBm	22.5 V	63.5 V	1.0 W	-30 dBm	7.1 mV	20 mV	1 μW
+38 dBm	19.0 V	50.9 V	6.4 W	-35 dBm	4.0 mV	11 mV	0.3 μW
+37 dBm	16.0 V	45.3 V	5.0 W	-40 dBm	2.25 mV	6.36 mV	
+36 dBm	14.1 V	39.9 V	4.0 W	-45 dBm	1.25 mV	3.54 mV	
+34 dBm	11.5 V	32.5 V	2.5 W	-50 dBm	.71 mV	2.0 mV	
+32 dBm	9.0 V	25.5 V	1.6 W	-55 dBm	.40 mV	1.1 mV	
+30 dBm	7.1 V	20.1 V	1.0 W	-60 dBm	.22 mV	.62 mV	
+28 dBm	5.8 V	16.4 V	.640 mW	-65 dBm	.128 mV	.362 μV	
+26 dBm	4.7 V	12.8 V	.400 mW	-70 dBm	.070 mV	.200 μV	
+24 dBm	3.6 V	10.2 V	.250 mW	-75 dBm	.040 μV	.113 μV	
+22 dBm	2.8 V	7.9 V	.160 mW	-80 dBm	.022 μV	.062 μV	
+20 dBm	2.2 V	6.2 V	.100 mW	-85 dBm	.013 μV	.037 μV	
+18 dBm	1.8 V	5.1 V	.064 mW	-90 dBm	.007 μV	.020 μV	
+16 dBm	1.4 V	4.0 V	.040 mW	-95 dBm	.004 μV		
+14 dBm	1.1 V	3.1 V	.025 mW	-100 dBm	.0025 μV	.0083 μV	
+12 dBm	0.9 V	2.5 V	.016 mW	-102 dBm	.0018 μV		
+10 dBm	0.7 V	2.0 V	.010 mW	-104 dBm	.0014 μV	.0040 μV	
+8 dBm	589 mV	1.8 V	.004 mW	-108 dBm	.0018 μV	.0033 μV	
+6 dBm	445 mV	1.3 V	.004 mW	-108 dBm	.00090 μV	.0025 μV	
+4 dBm	355 mV	1.0 V	.0025 mW	-110 dBm	.00071 μV	.0020 μV	
+2 dBm	280 mV	0.8 V	.0018 mW	-112 dBm	.00054 μV	.0016 μV	
-2 dBm	229 mV	0.6 V	.0010 mW	-114 dBm	.00045 μV	.0013 μV	
-4 dBm	180 mV	0.51 mV	.00064 μW	-116 dBm	.00036 μV	.0010 μV	
-6 dBm	141 mV	399 mV	.000388 μW	-118 dBm	.00029 μV	.00082 μV	
-8 dBm	115 mV	325 mV	.000265 μW	-120 dBm	.00023 μV	.00065 μV	
-10 dBm	90 mV	255 mV	.000162 μW	-122 dBm	.00018 μV	.00051 μV	
-12 dBm	71 mV	201 mV	.000100 μW	-124 dBm	.00014 μV	.00040 μV	
-15 dBm	40 mV	113 mV	.00030 μW	-126 dBm	.00012 μV	.00034 μV	
-20 dBm	22 mV	62 mV	.00010 μW	-128 dBm	.00009 μV	.00025 μV	
-25 dBm	13 mV	37 mV	.00003 μW	-130 dBm	.00007 μV	.00020 μV	

## Analyse spectrale

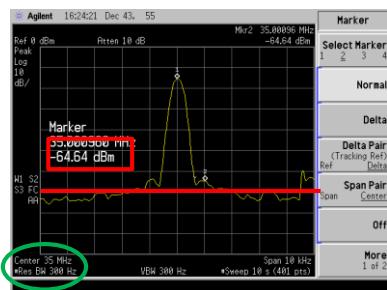
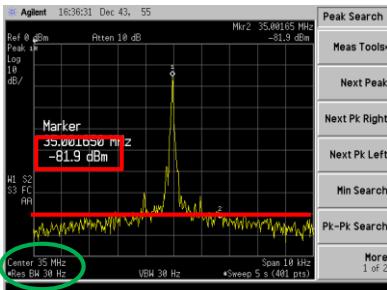
## • Terminologie



## Analyse spectrale

- Terminologie

- FFT : Fast Fourier Transform
- Span : excursion de fréquences
- RBW : Resolution Bandwidth



## Chapitre 6

# Modulations

## Les modulations analogiques

- **Rôle de la modulation**

- Faire subir des modifications au signal à transmettre afin de déplacer son spectre vers des fréquences élevées plus facilement transportables.

- **Avantages de la modulation**

- Adaptation des fréquences utilisées selon les besoins.
  - Bandes de fréquences utilisables sur le support de transmission.
  - Dimensions des antennes.
- Meilleure protection contre le bruit et les interférences.
- Utilisation du multiplexage fréquentiel.

## Les modulations analogiques

- **Dimension des antennes**

- La longueur d'une antenne filaire doit être de l'ordre de grandeur de la longueur d'onde du signal à transmettre.
- Les sons audibles : environs de 20Hz à 20kHz.

- Prenons  $v = c = 300\ 000\ km/s$  et signal = 300Hz

$$\lambda = \frac{v}{f} = \frac{300\ 000\ 000}{300} = 1\ 000\ km$$

- Prenons  $v = c = 300\ 000\ km/s$  et signal = 100MHz (Radio FM)

$$\lambda = \frac{v}{f} = \frac{300\ 000\ 000}{100\ 000\ 000} = 3\ m$$

## Les modulations analogiques

- Analyse spectrale du son "O"

Un son est composé d'un ensemble de fréquences

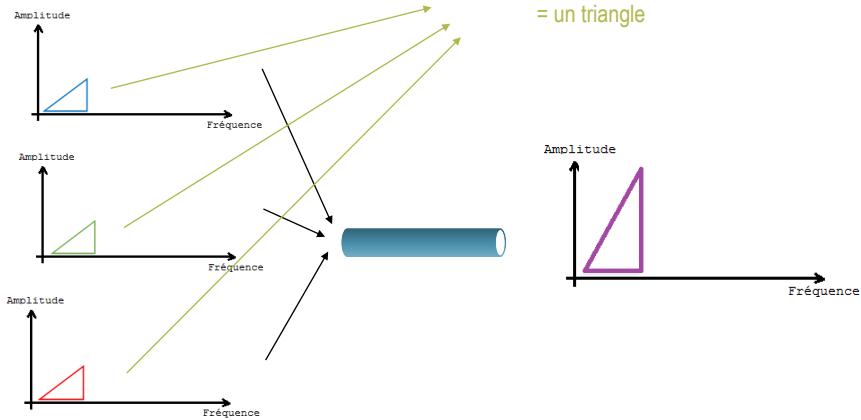


Source : <http://www.exo.net/~pauld/workshops/atomicoperaworkshop/vowelsospectrumpd600.jpeg>

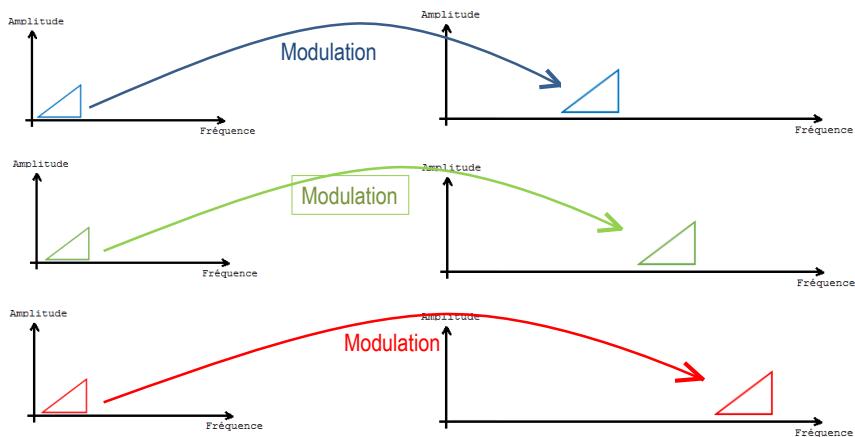
## Les modulations analogiques

- Multiplexage fréquentiel

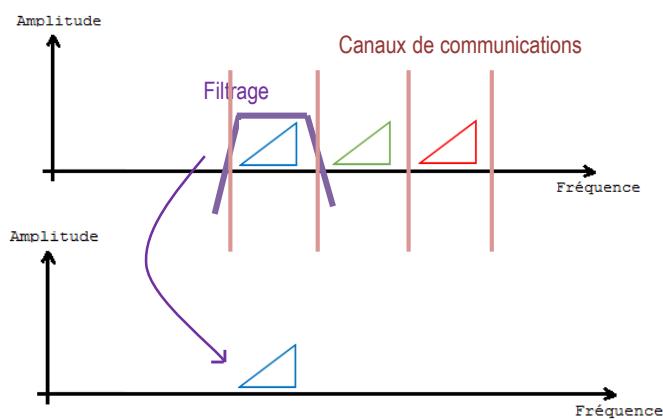
Représentation simplifiée du spectre  
= un triangle



- Multiplexage fréquentiel : modulation

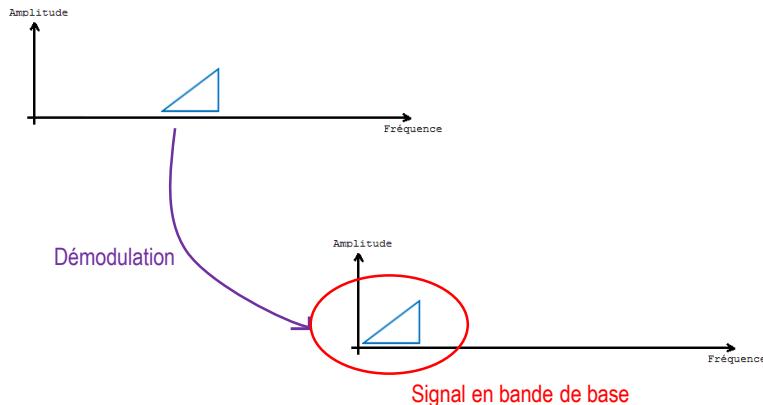


- Multiplexage fréquentiel : filtrage



## Les modulations analogiques

- Multiplexage fréquentiel : démodulation



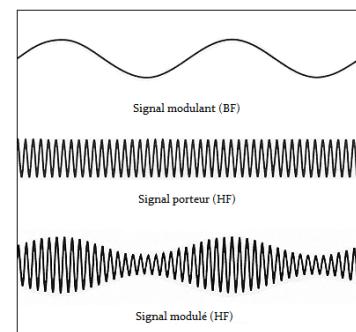
## Les modulations analogiques

- Modulation d'amplitude
  - Modulation par multiplication

$$v(t) = v_0 + v_m \cos(\omega_m t)$$

$$p(t) = p_m \cos(\omega_p t)$$

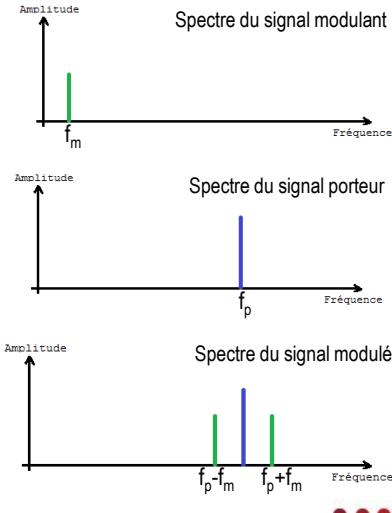
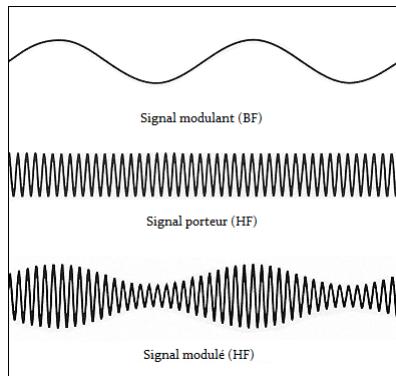
$$x_{AM}(t) = (v_0 + v_m \cos(\omega_m t)) \cdot p_m \cos(\omega_p t)$$

Source : <http://tutoworld.com/uploads/tuto-479/file-3.png>

$$x_{AM}(t) = v_0 p_m \cos(\omega_p t) + \frac{1}{2} v_m p_m \cos(\omega_p + \omega_m)t + \frac{1}{2} v_m p_m \cos(\omega_p - \omega_m)t$$

## Les modulations analogiques

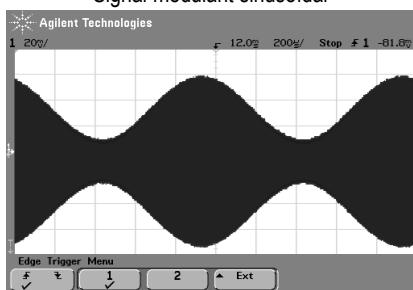
- Modulation d'amplitude



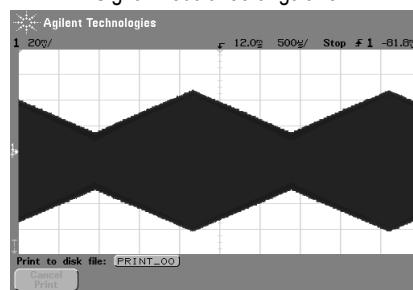
## Les modulations analogiques

- Exemples d'oscillogramme

Signal modulant sinusoïdal

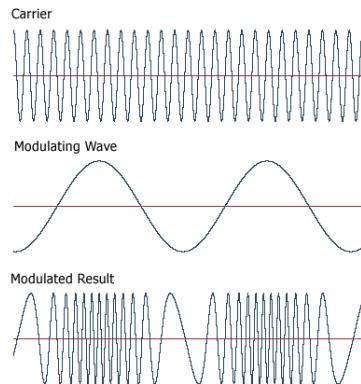


Signal modulant triangulaire



## Les modulations analogiques

- Modulation de fréquence

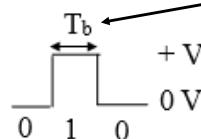
Source : [http://cf.ydcdn.net/1.0.1.44/images/computer/\\_FMMOD.GIF](http://cf.ydcdn.net/1.0.1.44/images/computer/_FMMOD.GIF)

## Les modulations analogiques

- Source de données

- Les données à transmettre sont numérisées.

$$\text{Débit binaire} = D = \frac{1}{T_b}$$



- Signal porteuse et modulant

- La porteuse est un signal analogique sinusoïdal haute fréquence.
- Le signal modulant est un signal numérique basse fréquence.

- Objectifs de la modulation numérique

- Identiques aux modulations analogiques.

## Les modulations analogiques

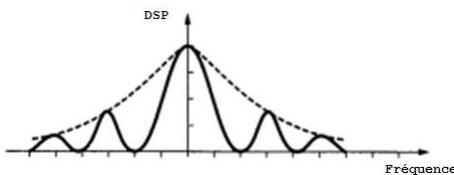
- Efficacité spectrale

- Modulation analogique

- On parle largeur de bande occupée autour de la porteuse.

- Modulations numériques

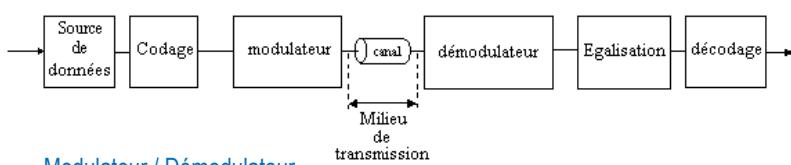
- On parle d'efficacité spectrale qui correspond au rapport du débit sur la largeur de bande occupée autour de la porteuse.
    - L'efficacité spectrale peut s'exprimer en bit/s/Hz.



DSP = La limite quand  $T$  tend vers l'infini de l'espérance mathématique du carré du module de la transformée de Fourier du signal.

## Les modulations analogiques

- Transmissions numériques



- Modulateur / Démodulateur

- Modulation d'amplitude
      - ASK : Amplitude Shift Keying
    - Modulation de fréquence
      - FSK : Frequency Shift Keying
    - Modulation de phase
      - PSK : Phase Shift Keying

- Égalisation

- Consiste à faire subir au signal reçu des modifications inverses à celles subies lors de sa transmission.

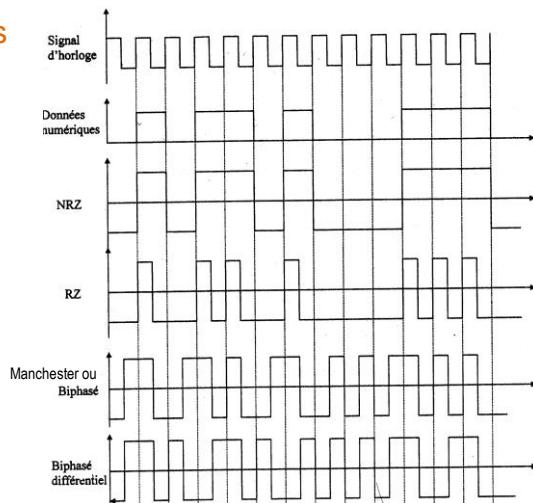
- **Codage de canal**

- Substituer au signal numérique un signal mieux adapté à la transmission.

- **Avantages**

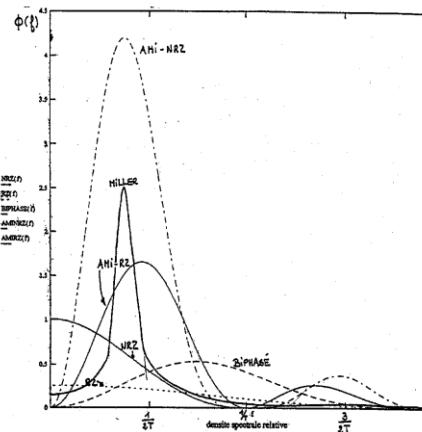
- Peut introduire des redondances pour réaliser une correction d'erreur.
- Peut introduire une séquence de bits qui sera utilisée par l'égalisation pour évaluer les perturbations introduite par le canal de transmission.
- Peut compresser les données.
- Peut modifier le spectre du signal.
  - Pour éviter de devoir transmettre et donc régénérer une composante continue.
  - Pour limiter le spectre du signal dans les BF, là où les distorsions linéaires sont les plus importantes.
  - Pour limiter le spectre du signal dans les HF, là où l'affaiblissement et la diaphonie sont les plus importants (Cela réduit aussi la largeur de bande).
  - Pour garantir une teneur en informations d'horloge suffisante pour assurer la synchronisation des récepteurs.

- **Exemples de codages**



## Les modulations analogiques

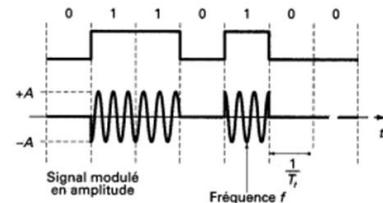
- Densité spectrale de puissance



## Les modulations analogiques

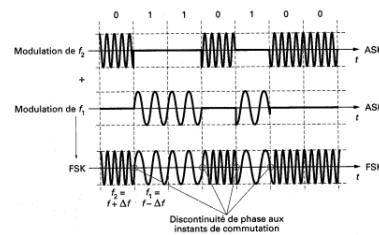
- Modulation d'amplitude

- Amplitude Shift Keying.
- Simple et faible coût.
- Seule modulation utilisable en optique.



- Modulation de fréquence

- Frequency Shift Keying.
- Moins sensible aux interférences.

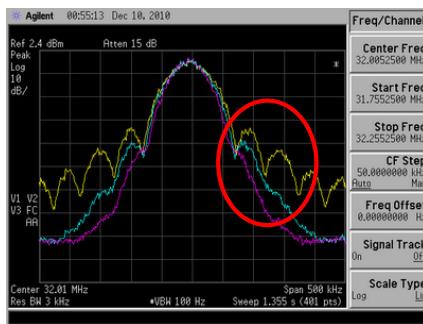


## Les modulations analogiques

- Densité spectrale de puissance

- MSK (Minimum Shift Keying)

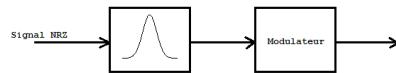
- La modulation de fréquence FSK offre la meilleure concentration de l'énergie autour de la porteuse lorsque  $x = 0,5$ .



$$x = \frac{f_2 - f_1}{D}$$

La MSK présente des lobes secondaires non négligeables.

Avant modulation, on applique un filtre Gaussien sur le signal NRZ → GMSK.

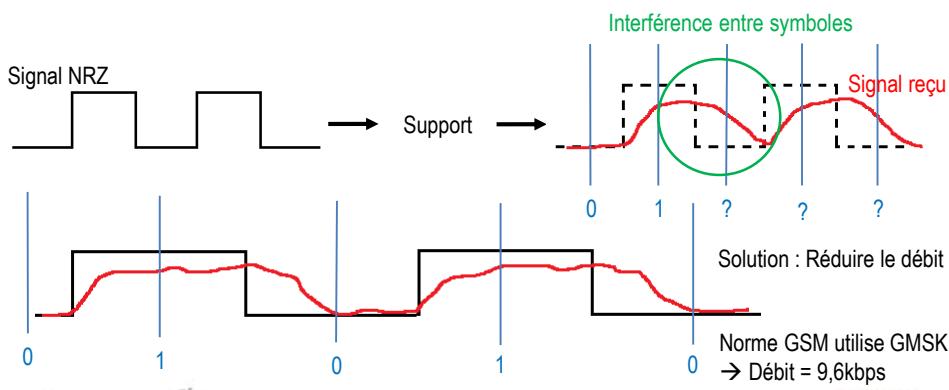


• • • 207

## Les modulations analogiques

- Effet d'un filtre gaussien

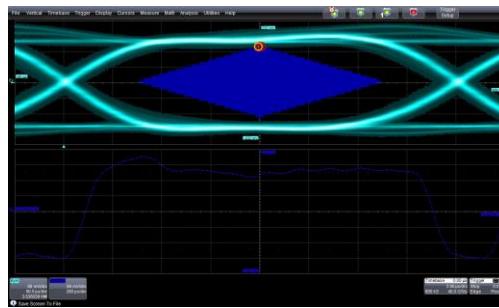
- Filtrage → suppression de certaines harmoniques.
  - Le signal est déformé : atténuation et élargissement des impulsions.



## Les modulations analogiques

- **Diagramme de l'œil**

- Il permet de juger la qualité d'une transmission numérique.
- On le compare à un gabarit normalisé (un masque, ici le losange bleu) ce qui permet de vérifier la qualité du signal.

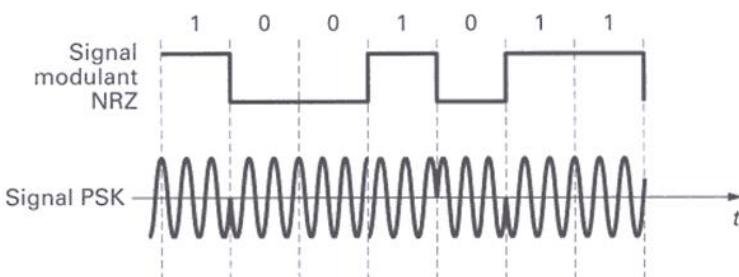


Source : <http://teledynelecroy.com/serialdata/serialdatastandard.aspx?standardid=227>

## Les modulations analogiques

- **Modulation de phase (PSK)**

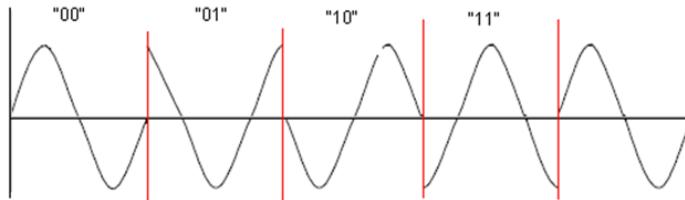
- Binary Phase Shift Keying (BPSK)
- 1 symbole représente 1 bit.



## Les modulations analogiques

- **Modulation de phase (QPSK)**

- Quadrature Phase Shift Keying.
- 1 symbole représente 2 bits → débit doublé par rapport à la BPSK.

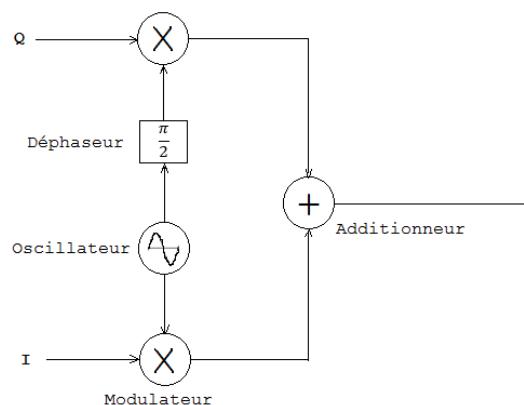


Source : <http://onlydot.net/cnt/wp-content/uploads/2008/07/QPSK.bmp>

## Les modulations analogiques

- **Quadrature phase-shift keying (QPSK)**

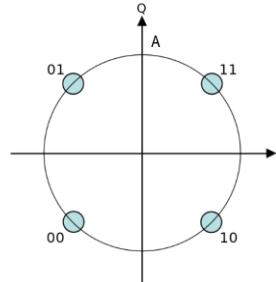
- Lorsque le nombre d'états est supérieur à 2, on utilise un modulateur IQ.



## Les modulations analogiques

- Constellation

Bits	I	Q	Phase
11	$A \frac{\sqrt{2}}{2}$	$A \frac{\sqrt{2}}{2}$	$\frac{\pi}{4}$
10	$A \frac{\sqrt{2}}{2}$	$-A \frac{\sqrt{2}}{2}$	$\frac{3\pi}{4}$
00	$-A \frac{\sqrt{2}}{2}$	$-A \frac{\sqrt{2}}{2}$	$\frac{5\pi}{4}$
01	$-A \frac{\sqrt{2}}{2}$	$A \frac{\sqrt{2}}{2}$	$\frac{7\pi}{4}$



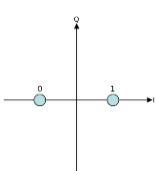
CC BY-SA 3.0

Source : [https://upload.wikimedia.org/wikipedia/commons/thumb/B/8f/QPSK\\_Gray\\_Coded.svg/618px-QPSK\\_Gray\\_Coded.svg.png](https://upload.wikimedia.org/wikipedia/commons/thumb/B/8f/QPSK_Gray_Coded.svg/618px-QPSK_Gray_Coded.svg.png) copié à l'identique

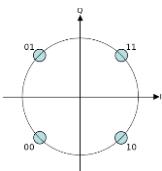
## Les modulations analogiques

- Constellation

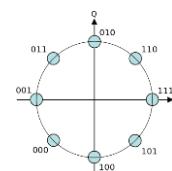
BPSK



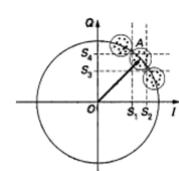
QPSK



8-PSK



Présence de bruits



Source : [https://en.wikipedia.org/wiki/Quadrature\\_amplitude\\_modulation](https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation)

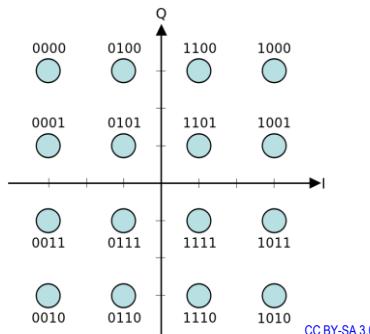
CC BY-SA 3.0

## Les modulations analogiques

## • Modulation QAM

## – Quadrature amplitude modulation.

- Exemple d'une constellation 16 QAM.



CC BY-SA 3.0

Source : [https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/16QAM\\_Gray\\_Coded.svg/200px-16QAM\\_Gray\\_Coded.svg.png](https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/16QAM_Gray_Coded.svg/200px-16QAM_Gray_Coded.svg.png)

## Chapitre 7

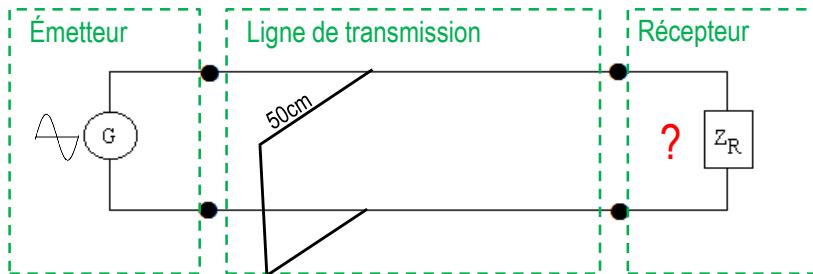
## Lignes de transmission

## Théorie des lignes

- Étude de la propagation en haute fréquence

- But :

- Déterminer les valeurs de la tension et du courant en chaque point d'une ligne de transmission.

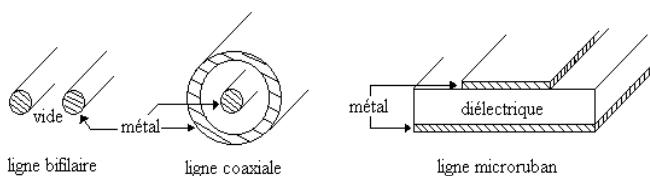


## Théorie des lignes

- Domaine de validité de l'étude

- Lignes bifilaires et coaxiales

- Les lignes de transmissions considérées sont constituées de deux conducteurs métalliques isolés l'un de l'autre par du vide ou par des diélectriques.



- Hautes fréquences :  $\pm$  entre 1MHz et 1GHz

- T.E.M. : Mode transverse électromagnétique.
    - Les champs électriques et magnétiques sont perpendiculaires aux conducteurs qui les constituent et par conséquent à la direction de propagation.

- Pertes dans les lignes

- Pertes par fuites entre les conducteurs

- Le champ électrique produit par une tension entre deux conducteurs, peut faire passer des électrons d'un conducteur à l'autre (l'isolant n'est pas parfait).

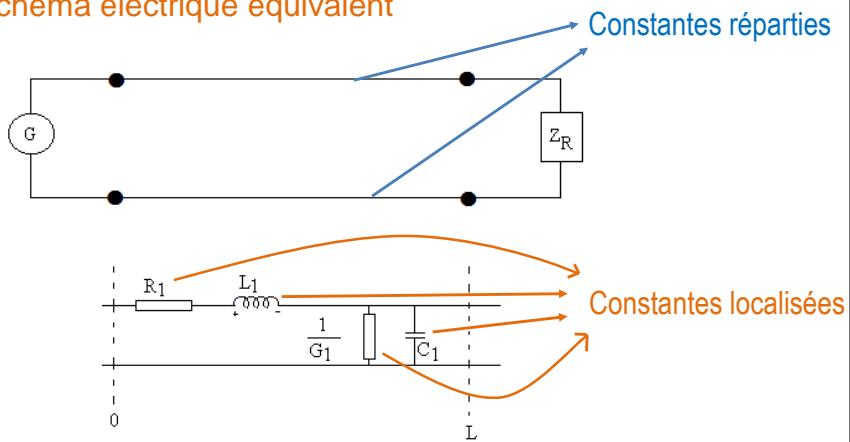
- Chute de tension dans les conducteurs

- Les conducteurs formant la ligne de transmission possèdent une certaine résistance qui occasionne une perte d'énergie par effet joule.

- Pertes par rayonnement

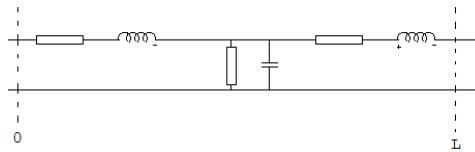
- Une ligne de transmission peut, par induction, transmettre une certaine quantité d'énergie aux conducteurs et milieu environnants.

- Schéma électrique équivalent

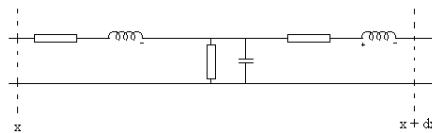


### • Schéma électrique équivalent

- Un seul quadripôle n'est pas suffisant pour modéliser correctement le fonctionnement d'une ligne de transmission.

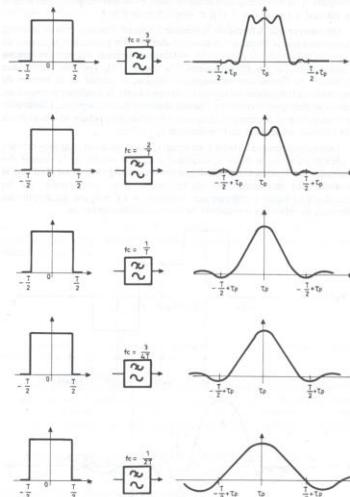


- Une modélisation correcte se base sur la mise en série d'un ensemble de quadripôle, chacun de ceux-ci représentant une petite portion de ligne par rapport à la longueur d'onde.



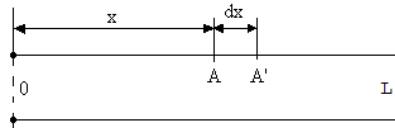
### • Circuit RLC

- Une ligne de transmission agit comme un filtre.



- **Équations de propagation**

- Soient  $v$  et  $i$  respectivement la tension et l'intensité du courant en A.
- Soient  $dv$  et  $di$  les variations de tension et de courant entre A et A'.



- En divisant  $dv$  et  $di$  par  $dx$ , nous obtenons des dérivées partielles

$$\frac{\partial v}{\partial x} = R_1 \cdot i + L_1 \frac{\partial i}{\partial t} \quad \frac{\partial i}{\partial x} = G_1 \cdot v + C_1 \frac{\partial v}{\partial t}$$

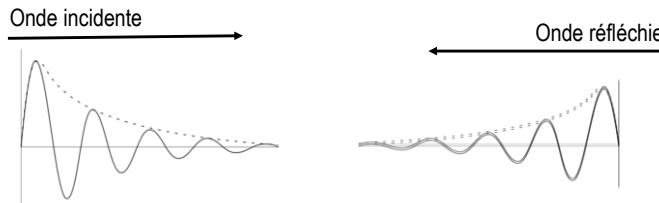
- **Équations de propagation**

- En dérivant les équations respectivement par rapport à x et par rapport au temps, on obtient finalement des équations différentielles dont la solution générale pour l'onde de tension est :

$$V = A_r e^{\gamma x} + B_i e^{-\gamma x}$$

- Ou encore

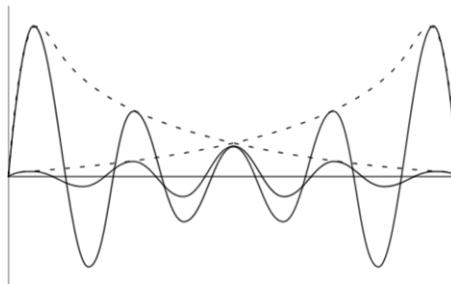
$$V = A_r e^{\alpha x} e^{j\beta x} + B_i e^{-\alpha x} e^{-j\beta x}$$



## Théorie des lignes

- Analyse de la solution générale

- L'onde résultante est la combinaison d'une onde incidente et d'une onde réfléchie.
- Interférence? Pertes? Rendement? Quantité d'onde réfléchie?



CC BY-SA 3.0

Source : [https://upload.wikimedia.org/wikipedia/commons/thumb/a/a2/Damped\\_sinewave.svg/524px-Damped\\_sinewave.svg.png](https://upload.wikimedia.org/wikipedia/commons/thumb/a/a2/Damped_sinewave.svg/524px-Damped_sinewave.svg.png)

## Théorie des lignes

- Caractéristiques de ces ondes

- Périodicité dans le temps

$$T = \frac{2\pi}{\omega}$$

- Périodicité dans l'espace

$$\lambda = \frac{2\pi}{\beta}$$

- Vitesse de propagation

$$V_p = \frac{\omega}{\beta}$$

- Équations de propagation

$$\boxed{\begin{aligned} V_x &= V_0 \operatorname{ch}(\gamma x) - I_0 Z_c \operatorname{sh}(\gamma x) \\ I_x &= I_0 \operatorname{ch}(\gamma x) - \frac{V_0}{Z_c} \operatorname{sh}(\gamma x) \end{aligned}}$$

– Où

$$Z_c = \sqrt{\frac{R_1 + j\omega L_1}{G_1 + j\omega C_1}}$$

$$\gamma = \sqrt{(R_1 + j\omega L_1)(G_1 + j\omega C_1)}$$

- Équations de propagation pour une ligne "sans pertes"

– Ligne sans pertes = sans pertes résistives

$$\left\{ \begin{array}{l} V_x = V_0 \cos(\beta x) - j I_0 Z_c \sin(\beta x) \\ I_x = I_0 \cos(\beta x) - j \frac{V_0}{Z_c} \sin(\beta x) \end{array} \right.$$

– Expression des équations en fonction des données du récepteur

$$\left\{ \begin{array}{l} V_x = V_r \cos(\beta x) + j I_r Z_c \sin(\beta x) \\ I_x = I_r \cos(\beta x) + j \frac{V_r}{Z_c} \sin(\beta x) \end{array} \right.$$

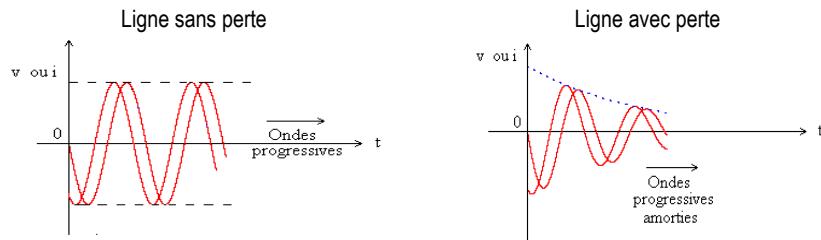
– où

$$Z_c = \sqrt{\frac{L_1}{C_1}} = \text{constante}$$

## Théorie des lignes

- Ondes progressives

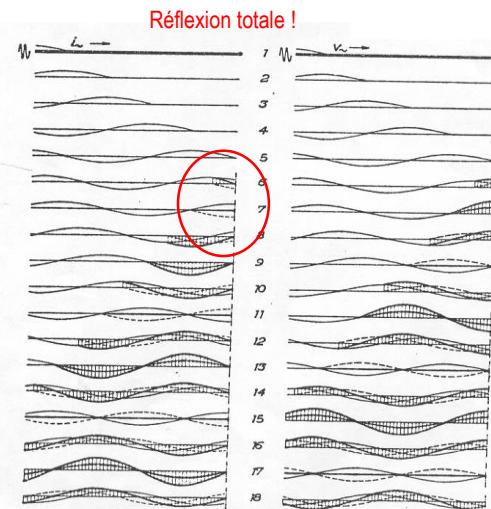
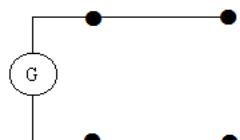
- Représentations d'ondes progressives sur des lignes de longueurs infinies.



## Théorie des lignes

- Ondes stationnaires

- Exemple de propagation sur une ligne ouverte.

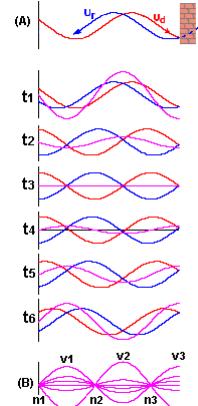
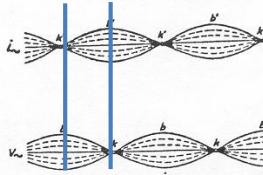


## Théorie des lignes

### • Ondes stationnaires

- La combinaison des ondes incidentes et réfléchies forme des nœuds et des ventres qui sont toujours aux mêmes endroits.
- Les endroits où sont positionnés ces nœuds et ces ventres sont déterminés par l'extrémité de la ligne ainsi que par la fréquence de l'onde.

Déphasage entre les nœuds de l'onde de courant et de l'onde de tension.



Source : <http://f5zv.pagesperso-orange.fr/RADIO/RM/RM07/RM07104d.gif>

## Théorie des lignes

### • Ligne sans perte en court-circuit

- Calcul de l'impédance à l'entrée de la ligne.
- Extrémité en court-circuit  $\rightarrow V_r = 0$ . Si  $x = L$ ,  $V_x = V_0$

$$V_x = V_r \cos(\beta x) + j I_r Z_c \sin(\beta x) \quad \text{et} \quad I_x = I_r \cos(\beta x) + j \frac{V_r}{Z_c} \sin(\beta x)$$

$$V_0 = 0 + j Z_c I_r \sin(\beta L) \quad \text{et} \quad I_0 = I_r \cos(\beta L) + 0$$

$$Z_0 = \frac{V_0}{I_0} = \frac{j Z_c I_r \sin(\beta L)}{I_r \cos(\beta L)} = j Z_c \operatorname{tg}(\beta L)$$

## Théorie des lignes

- Analyse de l'impédance d'entrée

– L'impédance d'entrée varie avec la longueur de la ligne

$$Z_0 = j Z_c \operatorname{tg}(\beta L)$$

– Exemple 1

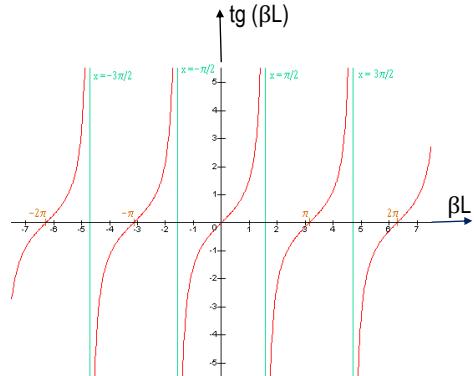
- Si  $\beta L = k\pi$  alors  $\operatorname{tg}(\beta L) = 0$

$$\rightarrow Z_0 = 0$$

$$\bullet \lambda = \frac{2\pi}{\beta} \rightarrow \beta = \frac{2\pi}{\lambda}$$

$$\bullet \frac{2\pi}{\lambda} L = k\pi$$

$$\bullet \text{Si } L = k \frac{\lambda}{2}, \text{ alors } Z_0 = 0$$



Source : <http://tanopah.jo.free.fr/seconde/ftang407.gif>

## Théorie des lignes

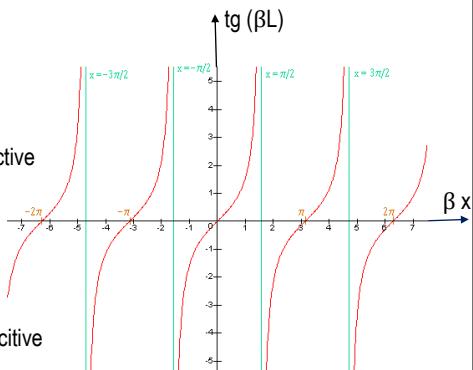
- Exemple 2

– Si  $\beta L = (2k+1) \frac{\pi}{2}$  alors  $\operatorname{tg}(\beta L) = \infty$

$$– \beta L = \frac{2\pi}{\lambda} L = (2k+1) \frac{\pi}{2}$$

$$– \text{Si } L = (2k+1) \frac{\lambda}{4} \text{ alors } Z_0 = \infty$$

(+) Impédance inductive



(-) Impédance capacitive

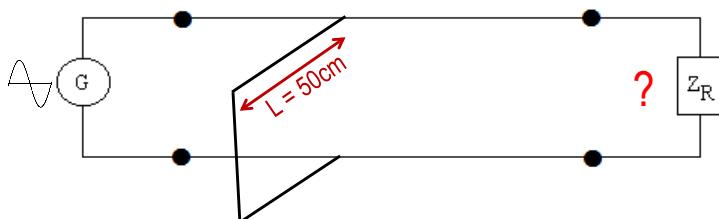
## Théorie des lignes

- Variation de la nature de l'impédance d'entrée d'une ligne en court-circuit

$\ell$	Nature de $Z_0$	$Z_0$	$I_0$
de 0 à $\lambda/4$			
$\lambda/4$		$\infty$	0
de $\lambda/4$ à $\lambda/2$			
$\lambda/2$		0	Max

## Théorie des lignes

- Étude de la propagation en haute fréquence



- Générateur délivre deux fréquences :  $f_1 = 150\text{MHz}$  et  $f_2 = 300\text{MHz}$
- $\lambda_1 = 300000000/150000000=2\text{m} \rightarrow$  Pour  $f_1$ ,  $L=\lambda/4$  ( $50\text{cm} = 1/4$  de  $2\text{m}$ )
  - Ligne en court-circuit de longueur  $\lambda/4$  :  $Z_0 = \infty$
- $\lambda_1 = 300000000/300000000=1\text{m} \rightarrow$  Pour  $f_2$ ,  $L=\lambda/2$  ( $50\text{cm} = 1/2$  de  $2\text{m}$ )
  - Ligne en court-circuit de longueur  $\lambda/2$  :  $Z_0 = 0$

## Théorie des lignes

- **Ligne sans perte ouverte à son extrémité**

- Calcul de l'impédance à l'entrée de la ligne.
- Extrémité ouverte  $\Rightarrow I_r = 0$ . Si  $x = L$ ,  $I_x = I_0$

$$V_x = V_r \cos(\beta x) + j I_r Z_c \sin(\beta x) \quad \text{et} \quad I_x = I_r \cos(\beta x) + j \frac{V_r}{Z_c} \sin(\beta x)$$

$$V_0 = V_r \cos(\beta L) + 0 \quad \text{et} \quad I_0 = 0 + j \frac{V_r}{Z_c} \sin(\beta L) \rightarrow V_r = \frac{I_0 Z_c}{j \sin(\beta L)}$$

$$Z_0 = \frac{V_0}{I_0} = \frac{V_r \cos(\beta L)}{j \frac{V_r}{Z_c} \sin(\beta L)} = j Z_c \cotg(\beta L)$$

## Théorie des lignes

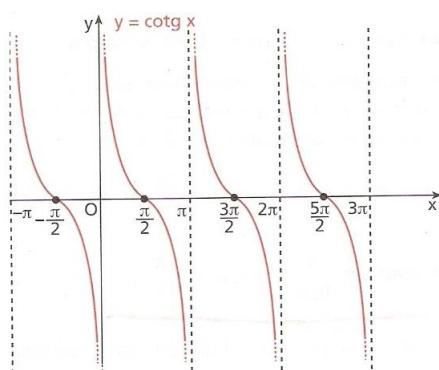
- **Analyse de l'impédance d'entrée**

- L'impédance d'entrée varie avec la longueur de la ligne

$$Z_0 = j Z_c \cotg(\beta L)$$

- **Exemple 1**

- Si  $L = (2k+1) \frac{\lambda}{4}$
- Alors  $\beta L = \frac{2\pi}{\lambda} (2k+1) \frac{\lambda}{4}$
- $\beta L = (2k+1) \frac{\pi}{2}$
- $\cotg((2k+1) \cdot \frac{\pi}{2}) = 0$



## Théorie des lignes

- Analyse de l'impédance d'entrée

– L'impédance d'entrée varie avec la longueur de la ligne

$$Z_0 = j Z_c \cotg (\beta L)$$

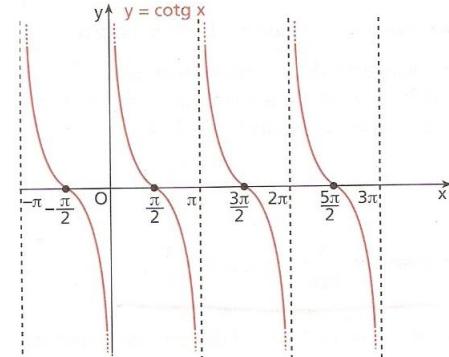
- Exemple 2

- Si  $L = k \frac{\lambda}{2}$

- Alors  $\beta L = \frac{2\pi}{\lambda} k \frac{\lambda}{2}$

- $\beta L = k \pi$

- $\cotg (k \pi) = \infty$



Source : [http://olrelascuola.altervista.org/goniometria/secante1\\_file/scansione0009.jpg](http://olrelascuola.altervista.org/goniometria/secante1_file/scansione0009.jpg)

## Théorie des lignes

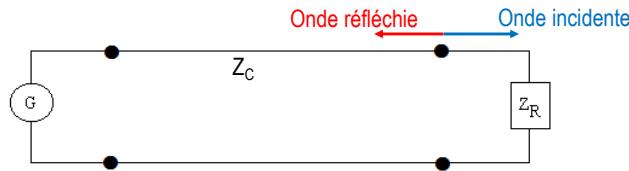
- Variation de la nature de l'impédance d'entrée d'une ligne ouverte

$\ell$	Nature de $Z_o$	$Z_o$	$I_o$
de 0 à $\lambda/4$			
$\lambda/4$		0	Max
de $\lambda/4$ à $\lambda/2$			
$\lambda/2$		$\infty$	0

## Théorie des lignes

- Coefficient de réflexion

- Lorsque la ligne est ouverte ou en court-circuit, il y a réflexion totale



- Dans les autres cas, quelle est la quantité d'onde réfléchie et quelle est la quantité d'onde allant vers la charge?

$$\Gamma_R = \frac{Z_R - Z_C}{Z_R + Z_C}$$

## Théorie des lignes

- Coefficient de réflexion

- Ligne ouverte

- Si  $Z_R = \infty$  alors  $\Gamma_R = \frac{\infty}{\infty} = 1 \rightarrow 100\% \text{ de réflexion, désadaptation totale.}$

- Ligne en court-circuit

- Si  $Z_R = 0$  alors  $\Gamma_R = \frac{Z_R - Z_C}{Z_R + Z_C} = -1 \rightarrow 100\% \text{ de réflexion, désadaptation totale.}$

- Adaptation d'impédance

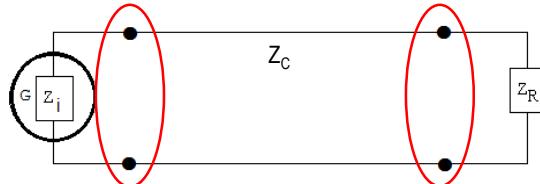
- Si  $Z_R = Z_C$  alors  $\Gamma_R = \frac{Z_R - Z_C}{Z_R + Z_C} = 0 \rightarrow \text{il n'y a pas de réflexion entre la ligne et la charge.}$

- Désadaptation partielle

- Si  $Z_R = 2 Z_C$  alors  $\Gamma_R = \frac{Z_R - Z_C}{Z_R + Z_C} = \frac{2Z_C - Z_C}{Z_C + Z_C} = 0,5 \rightarrow 50\% \text{ de l'onde est réfléchie.}$

- Coefficient de réflexion

- La réflexion n'intervient pas uniquement à l'extrémité d'une ligne, mais chaque fois que l'on se trouve en présence d'une variation d'impédance.



- Adaptation d'impédance

- Pour assurer un transfert maximum de puissance de l'émetteur à la charge, il faut donc qu'il n'y ait pas de variation d'impédance sur le trajet de l'onde incidente.

$$Z_i = Z_C = Z_R$$

- Adaptation d'impédance

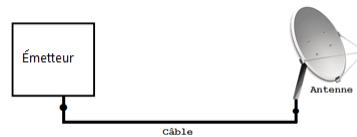
- Nécessaire pour obtenir un meilleure rendement

- Transfert maximum de puissance

- Nécessaire pour éviter les ondes réfléchies

- Celles-ci peuvent revenir vers l'émetteur qui ne pourra peut-être pas dissiper cette énergie supplémentaire, il y a donc des risques de détérioration.
- Celles-ci peuvent éventuellement être radiées par une antenne de réception ou peuvent occasionner des parasites dans le récepteur.

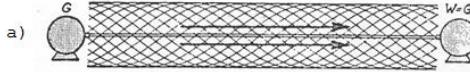
- En pratique, les impédances sont souvent réelles



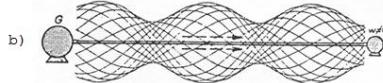
## Théorie des lignes

- **Coefficient de réflexion**

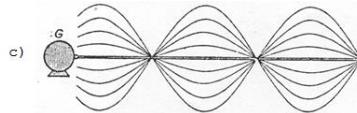
- Adaptation parfaite : un flux d'énergie régulier dans la ligne (ondes progressives).



- Défaut partiel d'adaptation. L'onde d'énergie utile qui parcourt la ligne est plus faible que dans le cas a)



- Défaut total d'adaptation, on observe une onde stationnaire qui ne transporte pas d'énergie vers le récepteur.



## Théorie des lignes

- **Standing Wave Ratio (SWR)**

- Rapport d'ondes stationnaires (R.O.S.)

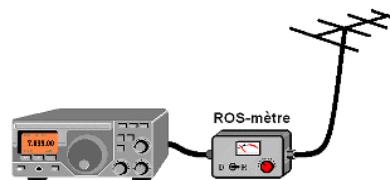
- Correspond au rapport entre un ventre et un nœud :  $\text{SWR} = \frac{|V_{max}|}{|V_{min}|}$

- Le SWR peut être mesuré ou calculé.

$$\text{SWR} = \frac{1+|\Gamma|}{1-|\Gamma|}$$

- Si  $\Gamma = 1$ ,  $\text{SWR} = \infty$

- Si  $\Gamma = 0$ ,  $\text{SWR} = 1$



Source : <http://f5zv.pagesperso-orange.fr/RADIO/RM/RM07/RM07g/RM07g03d.gif>

## Chapitre 8

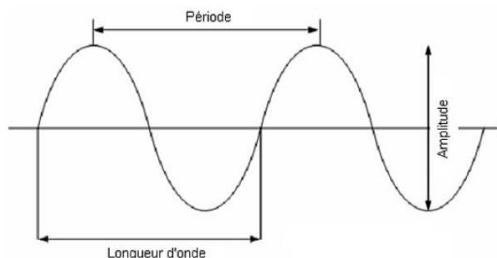
# Les antennes

## Les ondes électromagnétiques

### • L'onde radio (Radio Wave)

- La technologie Wi-Fi utilise les ondes radios.
- L'onde radio fait partie de la famille des ondes électromagnétiques.
- Une onde électromagnétique est constituée d'oscillations générées par un courant alternatif.

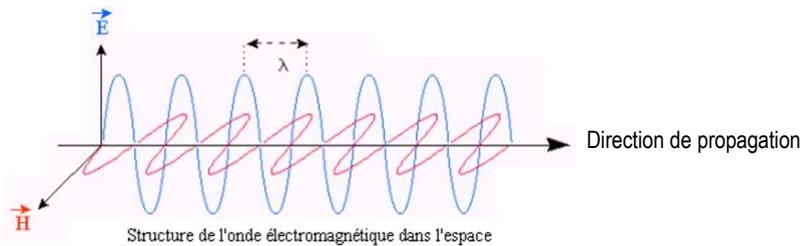
Période :  $T$   
 Fréquence :  $f$   
 Longueur d'onde :  $\lambda$   
 Phase :  $\phi$   
 Vitesse de propagation :  $v$



## Les ondes électromagnétiques

### • L'onde radio (Radio Wave)

- Plus précisément, les ondes électromagnétiques sont constituées par deux champs : l'un électrique, l'autre magnétique, tous deux en phase et perpendiculaires l'un à l'autre.



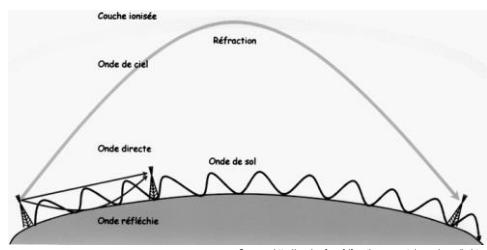
## Propagation des ondes radios

### • Types d'ondes

- Une onde électromagnétique se propage de façon différente selon sa fréquence et son environnement.

#### – Onde de sol (ou de surface)

- Elle se déplace le long du sol en suivant la surface terrestre.
- Elle est indépendante des conditions atmosphériques.
- Elle n'est utilisable que sur des fréquences relativement basses (quelques kilohertz à 1 MHz).
- On les utilise notamment en radiodiffusion AM.

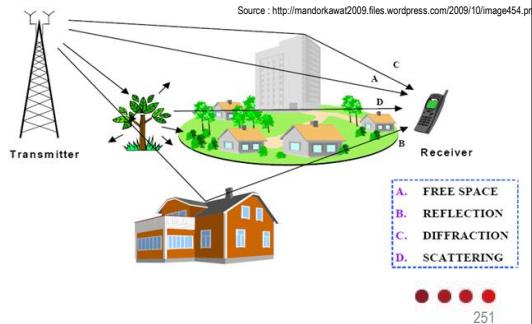


## Propagation des ondes radios

### • Types d'ondes

#### – Onde d'espace (onde directe et onde réfléchie)

- Ce mode de propagation est surtout valable pour les fréquences supérieures à 30MHz.
- Aux fréquences UHF notamment, (300MHz à 3GHz) l'onde d'espace reçue est la résultante de plusieurs composantes : une onde directe et des ondes réfléchies.
- Ces ondes sont sensibles aux obstacles.
- Les objets de dimensions supérieures à la longueur d'onde constituent des obstacles.

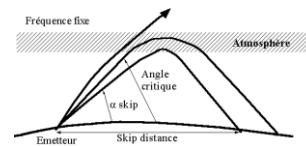
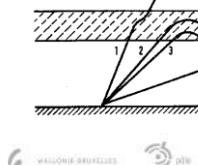


## Propagation des ondes radios

### • Types d'ondes

#### – Onde de ciel

- L'atmosphère se divise en différentes zones parmi lesquelles l'ionosphère.
  - L'ionosphère吸 absorbe une quantité importante de l'énergie émise par le soleil.
  - En fonction du cycle saisonnier et journalier, cette énergie va ioniser différemment les couches de l'ionosphère.
- Lorsqu'une onde de ciel atteint l'ionosphère, elle peut être "absorbée", réfractée ou réfléchie.
  - En fonction de l'angle "d'attaque".
  - En fonction des indices de réfraction des milieux.

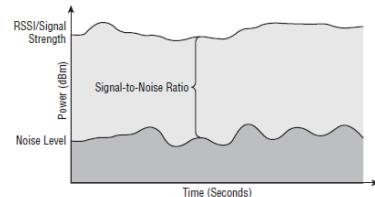


## Les incidents de propagation

### • Rapport signal/bruit

#### – SNR, Signal to Noise Ratio

- Rapport qui permet de comparer le niveau des ondes utiles avec celui des interférences.
- Plus le SNR est important, meilleures sont la qualité et les performances d'une communication sans fil.
- Si le niveau de bruit (bruit de fond, interférences) est trop proche du niveau du signal reçu, celui-ci ne pourra pas être différencié du bruit.



Source : Lammle T., CCNA Wireless Study Guide, Wiley Publishing, Inc., 2010

#### – Sources de bruit

- Tout équipement qui émet des ondes dans les mêmes fréquences que celles d'émission.
- Pour le Wi-Fi : un autre réseau Wi-Fi, bluetooth, les fours micro-onde, les équipements industriels, ...

## Les incidents de propagation

### • Atténuation de l'onde en espace libre

- En se propageant dans l'air, l'intensité d'une onde électromagnétique diminue.
- Plus on s'éloigne de l'émetteur, plus l'intensité de l'onde diminue jusqu'à se confondre avec le bruit.
- La sensibilité d'un récepteur définit sa capacité à recevoir des signaux faibles.
  - Plus il sera sensible, plus il sera capable de recevoir des signaux de faible amplitude.

### • Réflexion de l'onde

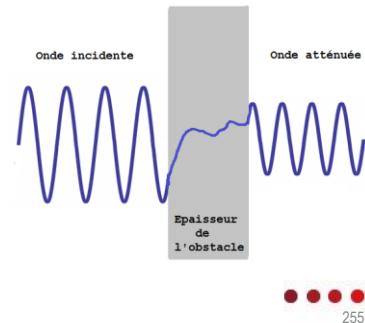
- Lorsqu'elle rencontre un obstacle, l'onde peut s'y réfléchir (totalement ou partiellement) et/ou subir une réfraction dépendant de l'épaisseur et de la nature de l'obstacle.
- Le plastique et le verre sont des matériaux qui vont plutôt réfléchir les ondes Wi-Fi.



## Les incidents de propagation

### • Absorption de l'onde

- Lorsqu'elle rencontre un obstacle, l'onde incidente peut y pénétrer plus ou moins facilement en fonction du type de matériau, de la fréquence du signal et de l'angle d'incidence.
- Bien que l'onde puisse ainsi traverser la plupart des obstacles, une partie de son énergie est y absorbée et l'onde est atténuée plus ou moins fortement.
- Le papier (livres, bibliothèques, meubles en carton, ...), le béton (mur, plancher, ...) et le verre blindé offrent un taux élevé d'absorption des ondes.
- Le métal offre un taux très élevé d'absorption des ondes.



## Les incidents de propagation

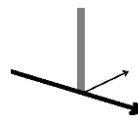
### • Réfraction de l'onde

- Lorsqu'elle rencontre certains matériaux (verre, eau, ...) l'onde peut être réfractée, c'est-à-dire traverser le matériau et ressortir (ou pas) avec un angle différent.



### • Diffraction de l'onde

- Lorsqu'elle rencontre certains obstacles ou ouvertures, une zone d'interférence est créée ce qui modifie tout ou partie de la trajectoire de l'onde.



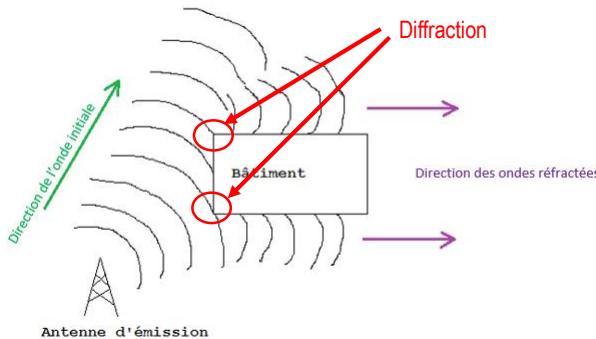
### • Diffusion de l'onde

- Lorsque l'onde atteint un obstacle de dimension comparable à sa  $\lambda$  ou ayant une surface contenant des aspérités, elle subit une diffusion.



## Les incidents de propagation

- Autre exemple de diffraction



## Les incidents de propagation

- Chemins multiples

- Combinaison d'ondes

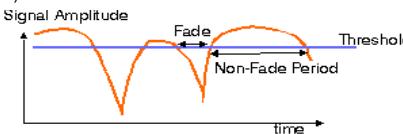
- En subissant divers incidents de propagation, l'onde reçue est la résultante de plusieurs composantes : une onde directe et des ondes réfléchies.

- Résultante variable

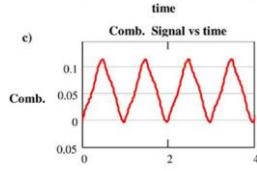
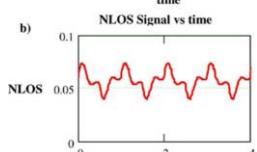
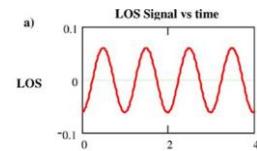
- La résultante n'est pas "constante" car les incidents peuvent varier au cours du temps.

- Affaiblissement

- A certains moments, il se peut que le niveau du signal résultant soit trop faible pour être reçu (opposition de phase).



Source : <http://www.wirelesscommunication.nl/reference/images/fld.gif>

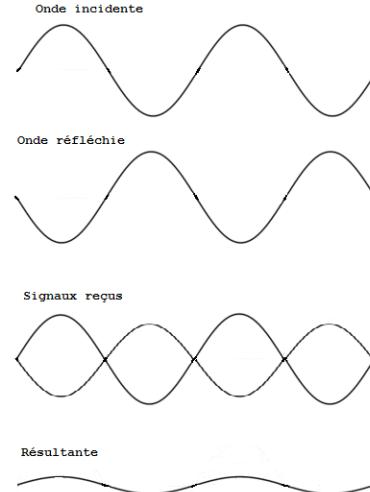
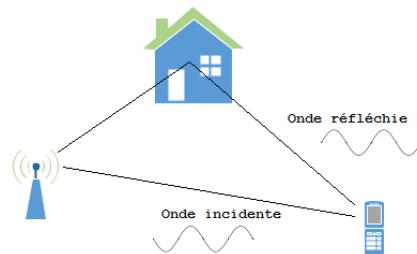


Source : [http://spie.org/Images/Graphics/Newsroom/Imported/269/269\\_fq4.jpg](http://spie.org/Images/Graphics/Newsroom/Imported/269/269_fq4.jpg)

## Les incidents de propagation

- **Fading**

- Effet d'évanouissement du signal



## Les incidents de propagation

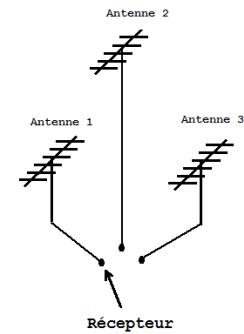
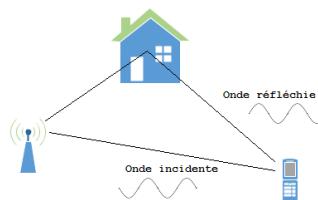
- **Fading**

- Types de fading

- Fading général
- Fading sélectif

- Exemples de Protection

- Antennes très directives diminuent le nombre de chemins
- Contrôle automatique de gain
- Diversity



## Les incidents de propagation

### • Zone de Fresnel

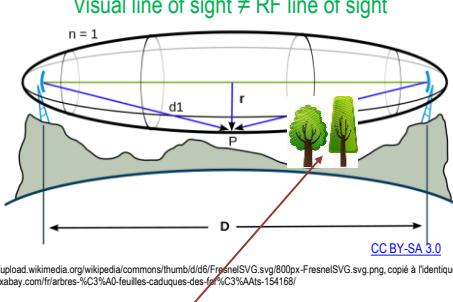
- La meilleure transmission correspond toujours à une portée en vision directe (LoS : Line of Sight), c'est un élément crucial en transmission point à point.
- L'Ellipsoïde de Fresnel délimite la région de l'espace où est véhiculée la plus grande partie de l'énergie du signal.
- Si les obstacles de cette zone ne bloquent pas plus de 40% du signal (20% avec marge), la propagation se passe comme dans les conditions de la propagation en espace libre.

$$r = \frac{1}{2} \sqrt{\lambda \cdot D}$$

Sources :  
 Fresnel : <https://upload.wikimedia.org/wikipedia/commons/thumb/d/d6/FresnelSVG.svg/800px-FresnelSVG.svg.png>, copié à l'identique

Arbre : <https://pixabay.com/fr/arbres-%C3%A0-feuilles-caduques-des-bois-%C3%A0-fleurs-154168/>

Visual line of sight  $\neq$  RF line of sight



CC BY-SA 3.0

Les arbres poussent ?  $\rightarrow$  marge à 0%

## Les incidents de propagation

### • Pertes de transmission

#### – Free Space Path Loss (FSPL)

- Sans obstacles, la puissance du signal est inversement proportionnelle au carré de la distance parcourue.  
 $\rightarrow$  Distance doublée, réception d'un quart de la puissance du signal.

#### – Variable rate shifting

- Plus le débit est important, plus la distance de réception sera faible.  
 $\rightarrow$  voir sensibilité du récepteur

#### – Fréquence

- Plus la fréquence est élevée, plus l'onde s'atténue rapidement.

#### – Conclusion

- Meilleur débit = plus haute fréquence et plus haut "débit".
- Meilleure portée = plus faible fréquence et plus faible "débit".

## Les incidents de propagation

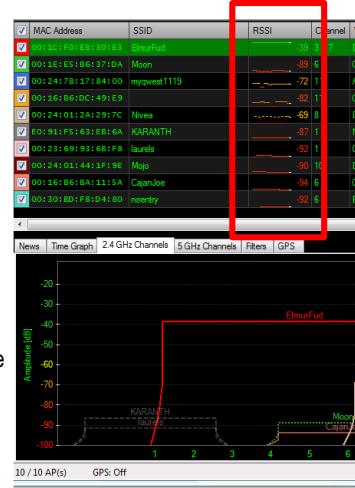
### • RSSI et SNR

#### – Received Signal Strength Indicator.

- Mesure qui décrit la quantité de puissance du signal qui arrive au niveau du récepteur.

#### – Valeur du RSSI

- Peut être exprimée en une échelle décimale (par exemple) entre 0 et 255. Chaque valeur correspondant à une valeur en dBm.
- Le RSSI peut également être directement exprimé en dBm.
- En Wi-Fi les valeurs usuelles de RSSI pour une station varient de -30 à -90 dBm.



Source : <http://magumataishi.cocolog-nifty.com/photos/uncategorized/2010/12/12/snag0007.jpg>

## Les incidents de propagation

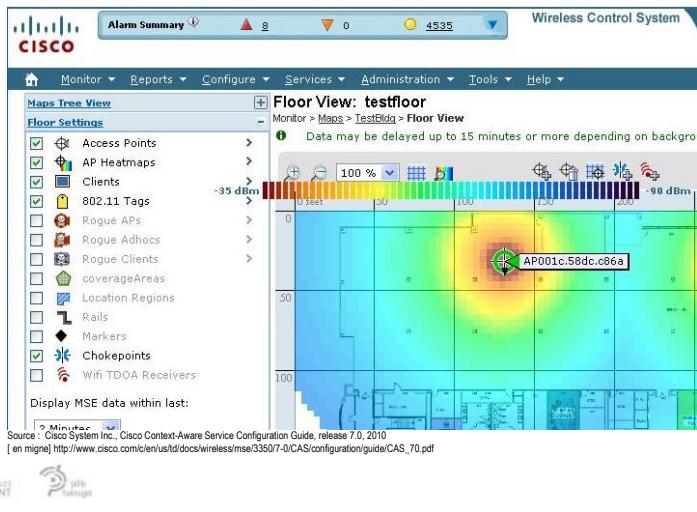
### • RSSI et SNR

#### – Utilisations par les appareils

- Pour sélectionner une antenne de réception parmi plusieurs.
- Pour préparer et décider les handovers en comparant les niveaux des signaux reçus de l'ancienne et de la nouvelle cellule radio.
- Pour la géolocalisation en intérieur, notamment la détection de points d'accès pirates (rogues AP).
- Dans l'algorithme CSMA/CA pour vérifier, avant d'émettre, que le canal radio est libre en mesurant le RSSI sur ce canal.

## Les incidents de propagation

- Exemple de monitoring avec Cisco WCS



## Les antennes

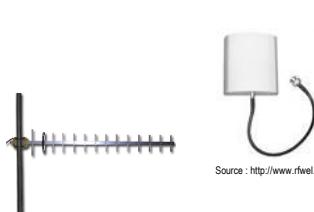
- Antenne

- Rôle

- Une antenne converti l'énergie électrique fournie en ondes électromagnétiques et vice versa.

- Types d'antenne

- La manière dont une antenne va rayonner l'énergie dépend de sa forme ainsi que des matériaux qui la compose.



Source des images : <http://www.andersontec.com/upload/700-2700MHz-Antenna-pdf/AI698-2700V1160A.pdf>



Source : <http://www.cosmtec.com/images/upload/DIPOLE.jpg>



Source : [http://www.comfortsurf.com/images/antenna/Wifi\\_Grid\\_24dBi/Grid\\_Antenna\\_1.jpg](http://www.comfortsurf.com/images/antenna/Wifi_Grid_24dBi/Grid_Antenna_1.jpg)

## Caractéristiques des antennes

### 1. Résistance de rayonnement

- La résistance de rayonnement est une résistance fictive qui, mise à la place de l'antenne, dissiperaient en chaleur la même puissance que celle qui est rayonnée par l'antenne.  
→ Valeur utilisée pour l'adaptation d'impédance.

### 2. Bande passante (Bande fréquentielle)

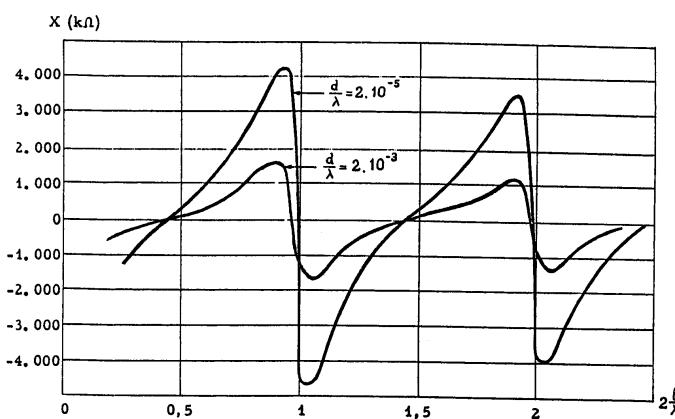
- Bandes de fréquences dans laquelle une antenne peut émettre et recevoir.

Feature	AIR-ANT2451V-R=	AIR-ANT5145V-R	AIR-ANT5160V-R	AIR-ANT5170P-R	AIR-ANT5195P-R
Frequency***	2.4 and 5 GHz	5 GHz	5 GHz	5 GHz	5 GHz

Fait référence à la bande des 2,4GHz

## Caractéristiques des antennes

### • Exemple pour antenne filaire



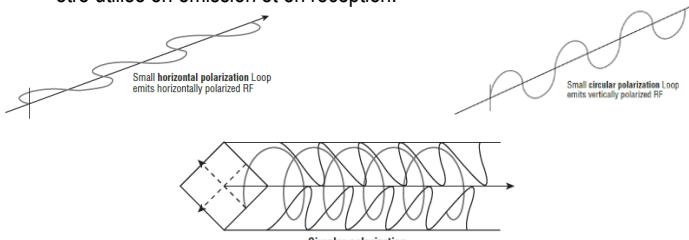
### 3. Polarisation

#### – Définition

- La polarisation d'une antenne décrit l'orientation des lignes de force du champ électrique par rapport à la terre.

#### – Polarisation horizontale, verticale ou circulaire

- Généralement, pour une meilleure performance, le même type de polarisation doit être utilisé en émission et en réception.



Source des images : Lammlie T., CCNA Wireless Study Guide, Wiley Publishing, Inc., 2010

### 4. Gain d'une antenne

#### – Définition

- Rapport entre la puissance qu'il faudrait fournir à une antenne de référence et celle qu'il suffit de fournir à l'antenne considérée placée au même endroit pour produire la même intensité de rayonnement dans une direction donnée.

#### – Mesure du gain

##### • Le décibel isotropique (dBi)

- Pour renseigner le gain d'une antenne, on utilise plutôt les dBi prenant comme référence le rayonnement d'une antenne isotropique.

##### • Le décibel dipôle (dBd)

- Plutôt que de se référer à une antenne théorique, il est possible de renseigner le gain par rapport au gain d'une antenne réelle (antenne  $\frac{\lambda}{2}$  ou dipôle).
- $0 \text{ dBd} = 2,14 \text{ dBi}$

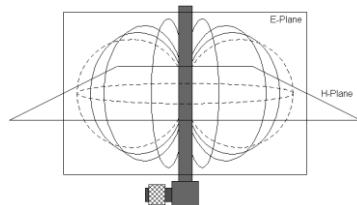
## 5. Diagramme de rayonnement

### – Définition

- La directivité d'une antenne caractérise la manière dont cette antenne concentre son rayonnement dans certaines directions de l'espace.

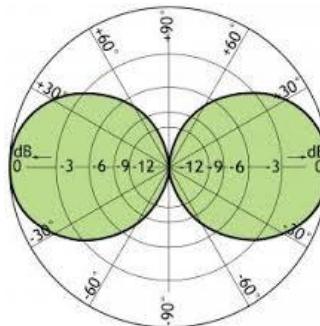
### – 3D difficile à dessiner → deux plans

- H-plane (Horizontal plane, Azimut)
  - Montre comment l'antenne rayonne vers la gauche et vers la droite.
- E-plane (Vertical Plane, Elevation )
  - Montre comment l'antenne rayonne vers le haut et vers le bas.



### • Graduation des diagrammes

- Les vendeurs assignent généralement un point de référence (valeur de 0 dB) au point de rayonnement maximum du diagramme.
- Les autres points (-x dB) indiquent la perte de puissance dans les autres directions

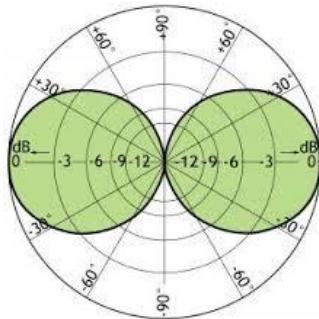


Source : <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTORSDAhINrzNHQHTWdZ9Am3wKwqJ0KAh3syjlyOF5o7yA>

## Caractéristiques des antennes

### • Mesure de la directivité

- La directivité est souvent exprimée par l'angle dont la bissectrice est la direction de rayonnement maximum et à l'intérieur duquel le gain en puissance ne descend pas en dessous de la moitié du gain maximal.



Source : [https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcT\\_ORSDahNnzvNHOTWdZ9Aam3ivKwqU0KAh3ysjlyOF5o7yA](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcT_ORSDahNnzvNHOTWdZ9Aam3ivKwqU0KAh3ysjlyOF5o7yA)

## Caractéristiques des antennes

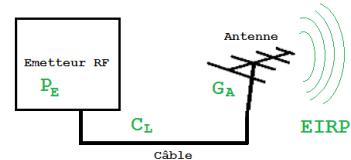
### 6. EIRP

#### – Effective Isotropic Radiated Power

- Puissance Isotrope Rayonnée Équivalente (PIRE)
- Puissance du signal réellement rayonnée par l'antenne d'émission dans la direction du rayonnement maximal.

#### – Calcul de l'EIRP

- $EIRP = P_E \text{ (dBm)} - C_L \text{ (dB)} + G_A \text{ (dBi)}$ 
  - $P_E$  = puissance de sortie de l'émetteur (dBm)
  - $C_L$  = atténuation due au câble d'émission (dB)
  - $G_A$  = gain de l'antenne d'émission (dBi)



#### – Réglementation

- ETSI (Europe) : 20 dBm  $\rightarrow$  100mW
- FCC (USA) : 36 dBm  $\rightarrow$  4W

## Réception des ondes

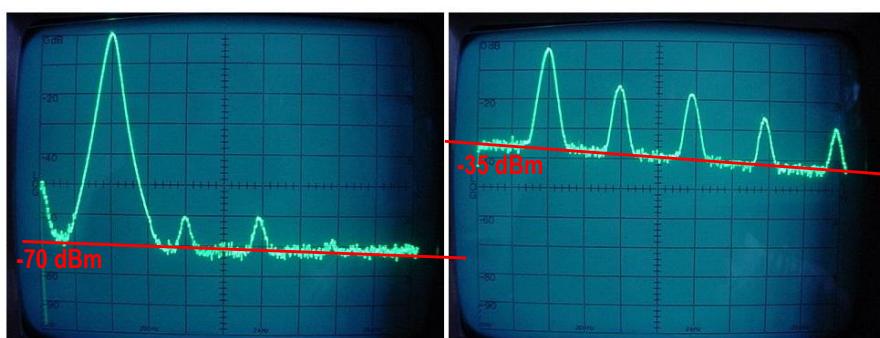
- Sensibilité du récepteur

– Le signal reçu doit être plus puissant que la sensibilité du récepteur.

Receive Sensitivity (Typical)	802.11a	802.11g
	• 6 Mbps: -88 dBm	• 1 Mbps: -96 dBm
	• 9 Mbps: -87 dBm	• 2 Mbps: -93 dBm
	• 12 Mbps: -86 dBm	• 5.5 Mbps: -91 dBm
	• 18 Mbps: -85 dBm	• 6 Mbps: -91 dBm
	• 24 Mbps: -82 dBm	• 9 Mbps: -85 dBm
	• 36 Mbps: -79 dBm	• 11 Mbps: -88 dBm
	• 48 Mbps: -74 dBm	• 12 Mbps: -83 dBm
	• 54 Mbps: -73 dBm	• 18 Mbps: -81 dBm
		• 24 Mbps: -78 dBm
		• 36 Mbps: -74 dBm
		• 48 Mbps: -73 dBm
		• 54 Mbps: -73 dBm

## Réception des ondes

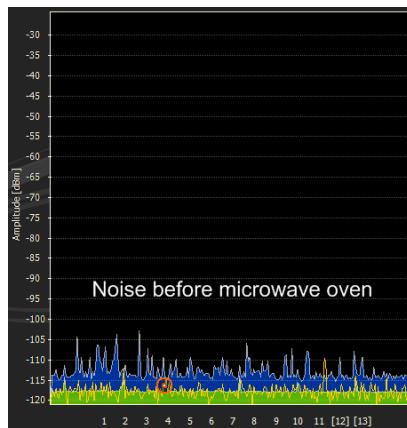
- Background noise (Bruit de fond)



Source : <http://ham-radio.com/k8sti/mn45.jpg>

## Réception des ondes

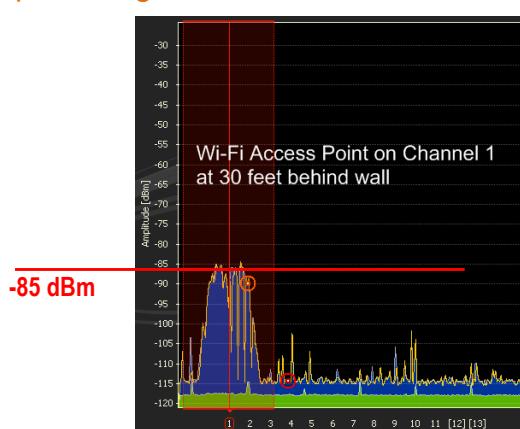
- Background noise (Bruit de fond)



Source : <http://www.zdnet.com/story/60/03/000578/pre-microwave-noise.png>

## Réception des ondes

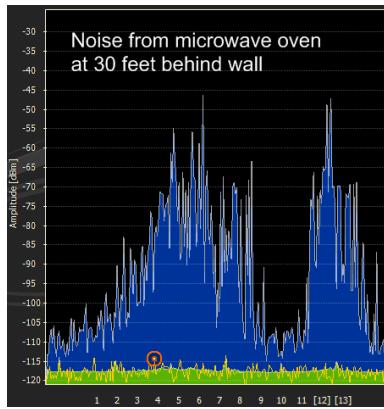
- Exemple de signal dans le canal 1



Source : <http://zdnet3.cbsstatic.com/hub/i/r/2014/10/04/1560c8e4-4ab1-11e4-b6a0-d4ae52e95e57/resize/270xauto/94da3bd8e6cb1a34fbca92c75e94020/ap-signal-s.png>

## Réception des ondes

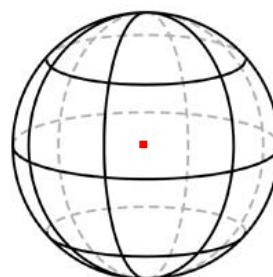
- Exemple d'interférences générées par un four micro-onde



• • •  
279

## Types d'antennes

- Antenne isotropique
  - Antenne théorique omnidirectionnelle.
  - Gain : 0dBi.

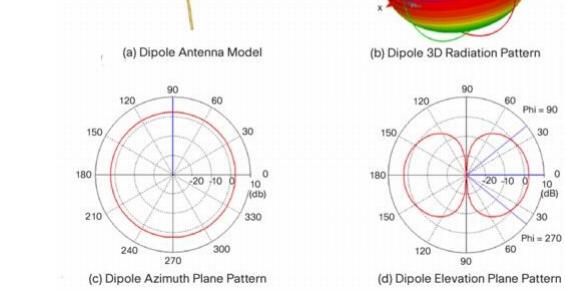
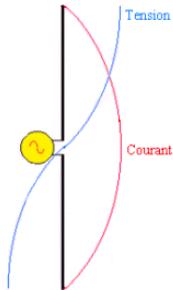


• • •  
280

## Types d'antennes

- Antenne dipôle

- Antenne omnidirectionnelle.
- Gain : environ 2,14dBi.
- R rayonnement :  $75\Omega$ .



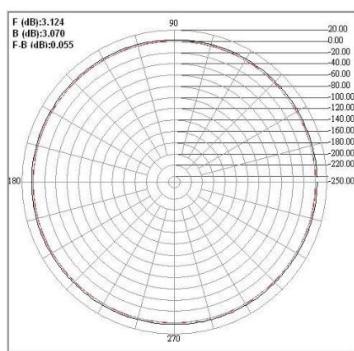
Source : Cisco Systems, Inc, Antenna Patterns and Their Meaning, 1992-2007

## Types d'antennes

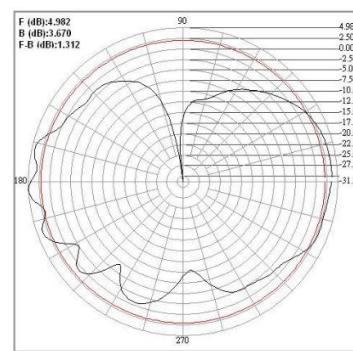
- Antenne dipôle

- Exemple de diagramme de rayonnement

Pattern H-Plane



Pattern E-Plane



Source : <http://www.wimo.com/download/17012.pdf>

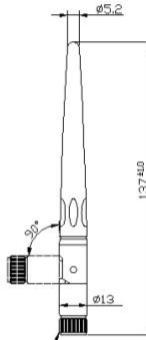
## Types d'antennes

- Antenne dipôle

- Exemple de spécifications d'une Antenne dipôle (Wimo articulée 17012.xxx)

### Specifications

Frequency Range	2.4 ~ 2.4835GHz
VSWR	2.0
Impedance	50Ω ± 5Ω
Gain	3dBi
Polarization	Vertical
Power Handling	> 1 Watt
Beam Width	H: 360° / E: 32.2°
Connector	RP SMA or RP TNC
Operation Temp.	-30° ~ +60°
Material	ABS (UL-94HB)
Dimension (L*W*H)	137*130 mm
Weight	22g ± 2g
Color	Black
part no.	RP SMA: 17012.RSMA RP TNC: 17012.RTNC



Source : <http://www.wimo.com/download/17012.pdf>

## Types d'antennes

- Antenne patch

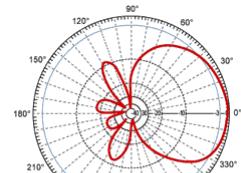
- Antenne semidirectionnelle.
- Exemple de spécifications d'une antenne "flat patch".



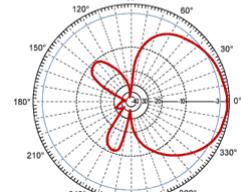
Source : <http://www.rfel.com/images/antennas/82-5906.jpg>

Frequency	2400-2500 MHz
Gain	8 dBi
Horizontal Beam Width	75 degrees
Vertical Beam Width	65 degrees
Impedance	50 Ohm
VSWR	< 1.5:1 avg.
Lightning Protection	DC Short

Source : [http://www.i-com.com/multimedia/datasheets/DS\\_RE09P-XX.PDF](http://www.i-com.com/multimedia/datasheets/DS_RE09P-XX.PDF)



Vertical



Horizontal

Source : [http://www.i-com.com/multimedia/datasheets/DS\\_RE09P-XX.PDF](http://www.i-com.com/multimedia/datasheets/DS_RE09P-XX.PDF)

## Types d'antennes

- Antenne Yagi

- Antenne directionnelle.
- Exemple de spécifications d'une antenne Yagi large bande



### Electrical Specifications

Item No.	AI698-2700V11i60A	
Frequency Range	MHz	698-960/1710-2700
Gain	dBi	10/11
Polarization		Vertical/Horizontal
Beam width	Horizontal	60/65
	Vertical	90/75
VSWR		≤1.6/1.5
Front-to-back ratio	dB	≥10
Maximum input power	w	50
Lightning protection		DC Ground
Impedance	Ω	50

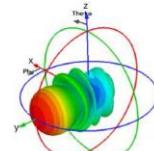
Source des images : <http://www.andersontec.com/upfile/700-2700MHz-Antenna-pdf/AI698-2700V11i60A.pdf>

## Types d'antennes

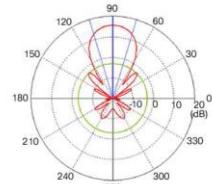
- Antenne Yagi



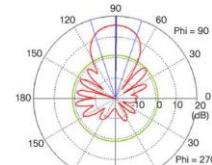
(a) Yagi Antenna Model



(b) Yagi Antenna 3D Radiation Pattern



(c) Yagi Antenna Azimuth Plane Pattern



(d) Yagi Antenna Elevation Plane Pattern

Source : Cisco Systems, Inc, Antenna Patterns and Their Meaning, 1992-2007

## Types d'antennes

- Antenne parabolique

  - Antenne directionnelle

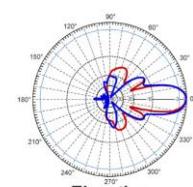
    - Parabolic dish antenna, parabolic grid antenna.

  - Exemple de spécifications d'une antenne parabolique

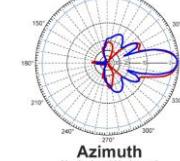


<b>Frequency Range</b>	2400 – 2500 MHz
<b>Gain</b>	18 dBi
<b>Polarization</b>	Vertical and Horizontal
<b>Horizontal Beam Width</b>	18°
<b>Vertical Beam Width</b>	19°
<b>VSWR</b>	< 1.5 typical
<b>F/B Ratio</b>	> 25 dB
<b>Cross-Pol Isolation</b>	> 28 dB
<b>Max Input Power</b>	100W
<b>Input Impedance</b>	50 Ohm
<b>Lightning Protection</b>	DC Ground

Source : [http://www.comfortsurf.com/images/antenna/Wifi\\_Grid\\_24dBi/Grid\\_Antenna\\_1.jpg](http://www.comfortsurf.com/images/antenna/Wifi_Grid_24dBi/Grid_Antenna_1.jpg)



Elevation  
Vertical and Horizontal



Azimuth  
Vertical and Horizontal

Source des images : [http://www.l-com.com/multimedia/datasheets/DS\\_HG2418DPD.PDF](http://www.l-com.com/multimedia/datasheets/DS_HG2418DPD.PDF)

## Accessoires des antennes

- Amplificateurs

  - A connecter au câble menant à l'antenne.

    - A placer le plus près possible de l'antenne.
    - Amplification active, nécessite une alimentation.

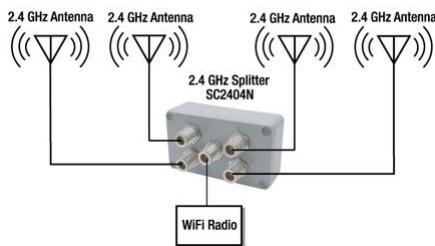


Source : <https://www.radiolabs.com/images/products/indoor-wifi-booster-zoom.png>

- **Splitters**

- Permettent de répartir le signal vers plusieurs antennes.
- Inconvénients.
  - Introduction d'une perte pouvant aller jusqu'à 4dB.
  - Débit divisé.

### Typical RF Splitter Application



Source : <http://www.i-com.com/images/typical-rf-splitter-application.jpg>

## Exemple de calcul d'une liaison sans fil

- Atténuation
  - En dB
- Puissance
  - S'exprime en Watt
  - En radio elle s'exprime souvent en dBm
    - $P(\text{en dBm}) = 10 \log P(\text{en mW})$
    - $1\text{W}=1000\text{mW}=10 \log 1000=30\text{dBm}$
- Rappel
  - $-3\text{dB} = \text{Puissance divisée par 2}$

- Atténuation dans le vide
  - $32,4 + 20 \log F + 20 \log R$
  - F = fréquence en MHz
  - R = distance émetteur/récepteur en km
- Atténuation à 2,4GHz
  - Atténuation =  $100 + 20 \log R$
- Réception
  - La puissance reçue (= puissance à l'émission – atténuation) doit être supérieure à la sensibilité en réception.

- **PIRE (EIRP)**
  - Puissance réellement émise par l'antenne
- **Calcul de l'EIRP**
  - $EIRP = Pout - Ct + Gt$ 
    - Pout = puissance de sortie de l'émetteur (dBm)
    - Ct = atténuation due au câble d'émission (dB)
    - Gt = gain de l'antenne d'émission (dBi)

- **Puissance reçue au récepteur**
  - $Pr = Pout - Ct + Gt - Pl + Gr - Cr$ 
    - Si = Puissance reçue à l'entrée du récepteur
    - Pl = Pertes de liaison, Path Loss (dB)
    - Gr = Gain de l'antenne de réception (dBi)
    - Cr = Atténuation du câble de réception (dB)
- **Sensibilité du récepteur**
  - Sr : fournie par le fabricant.
  - $Pr > Sr$

## Exercice

- **Calculer la distance maximale entre deux points d'accès**
  - Norme 802.11g à son débit maximum
  - Point d'accès Cisco Aironet 1100
  - Câble d'émission et de réception
    - Type de câble RG214
    - Longueur du câble d'émission : 2m
    - Longueur du câble de réception : 3m
  - Antennes émission et réception
    - Cisco AIR-ANT2455V-N

## Exemple de data sheet

### AP Aironet 100

<b>Antenne AIR-ANT2455V-N</b>	
Feature	AIR-ANT2455V-N
Description	Omnidirectional
Application	Outdoor, direct mount on unit
Gain	5.5 dBi
Frequency	2.4 GHz
Beam width	25° V
Cable Length	None
Dimensions	12.5 in (31.75 cm) x 1 in. (2.54 cm)
Weight	5 oz. (14 kg)
Operating Temperature	-30° to 70°C

### Câble RG214

RG214-50f ATTENUATION		
Frequency MHz	Attenuation dB/100 m	Attenuation dB/100 ft
300	12.0	3.66
600	19.0	5.79
900	24.0	7.31
1200	29.0	8.84
1500	33.0	10.1
1800	37.0	11.3
2100	41.0	12.5
2400	45.0	13.7
2700	49.0	14.9
3000	52.0	15.8
3300	56.0	17.1
3600	60.0	18.3
3900	63.0	19.2
4200	66.0	20.1
4500	70.0	21.3

Receive Sensitivity	802.11b:
	<ul style="list-style-type: none"> <li>• 1 Mbps: -94 dBm</li> <li>• 2 Mbps: -91 dBm</li> <li>• 5.5 Mbps: -89 dBm</li> <li>• 11 Mbps: -85 dBm</li> </ul>
	802.11g:
	<ul style="list-style-type: none"> <li>• 1 Mbps: -95 dBm</li> <li>• 2 Mbps: -91 dBm</li> <li>• 5.5 Mbps: -89 dBm</li> <li>• 6 Mbps: -90 dBm</li> <li>• 9 Mbps: -84 dBm</li> <li>• 11 Mbps: -80 dBm</li> <li>• 12 Mbps: -82 dBm</li> <li>• 18 Mbps: -80 dBm</li> <li>• 24 Mbps: -77 dBm</li> <li>• 36 Mbps: -73 dBm</li> <li>• 48 Mbps: -72 dBm</li> <li>• 54 Mbps: -72 dBm</li> </ul>

Available Transmit Power Settings	802.11g:
	<ul style="list-style-type: none"> <li>• CCK:</li> </ul>
	<ul style="list-style-type: none"> <li>• 100 mW (20 dBm)</li> <li>• 50 mW (17 dBm)</li> <li>• 30 mW (15 dBm)</li> <li>• 20 mW (13 dBm)</li> <li>• 10 mW (10 dBm)</li> <li>• 5 mW (7 dBm)</li> <li>• 1 mW (0 dBm)</li> </ul>
	<ul style="list-style-type: none"> <li>• OFDM:</li> </ul>
	<ul style="list-style-type: none"> <li>• 30 mW (15 dBm)</li> <li>• 20 mW (13 dBm)</li> <li>• 10 mW (10 dBm)</li> <li>• 5 mW (7 dBm)</li> <li>• 1 mW (0 dBm)</li> </ul>

## Exemple de data sheet

Air Interface Standard	IEEE 802.11b or IEEE 802.11g Note: Autonomous bridge mode has enhancements to the standard to allow longer-range bridging communications.
Frequency Band	<ul style="list-style-type: none"> <li>2.412 to 2.462 GHz (FCC)</li> <li>2.412 to 2.472 GHz (ETSI)</li> <li>2.412 to 2.472 GHz (TELEC)</li> </ul>
Wireless Modulation	<p>802.11b</p> <ul style="list-style-type: none"> <li>Direct Sequence Spread Spectrum (DSSS): <ul style="list-style-type: none"> <li>Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps</li> <li>Differential Quadrature Phase Shift Keying (QPSK) at 2 Mbps</li> <li>Complementary Code Keying (CCK) at 5.5 and 11 Mbps</li> </ul> </li> </ul> <p>802.11g</p> <ul style="list-style-type: none"> <li>Orthogonal Frequency Divisional Multiplexing (OFDM): <ul style="list-style-type: none"> <li>BPSK at 6 and 9 Mbps</li> <li>QPSK at 12 and 18 Mbps</li> <li>16-quadrature amplitude modulation (QAM) at 24 and 36 Mbps</li> <li>64-QAM at 48 and 54 Mbps</li> </ul> </li> </ul>
Media Access Protocol	Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
Lightweight Access Point Protocol	A network protocol for lightweight access points that also provides for centralized management.
Operating Channels	802.11b/g <ul style="list-style-type: none"> <li>ETSI: 13</li> <li>Americas: 11</li> <li>TELEC (Japan): 13</li> </ul>
Nonoverlapping Channels	3

Source : Cisco System Inc., Data sheet : Cisco Aironet 1300 Series Outdoor Access Point or Bridge

## Exemple de data sheet

Power Injector LR2	The power injector converts the standard 10/100BASE-T Ethernet Cat5 RJ-45 interface that is suitable for weather-protected areas to a dual F-Type connector interface for dual coaxial cables that are more suitable for harsh outdoor environments. While providing a 100BASE-T interface to the Cisco Aironet 1300 Series, the power injector also provides power to the unit over the same cables with a power discovery feature that protects other appliances from damage should they accidentally be connected. As an added benefit to the installer, the automatic medium-dependent interface crossover (Auto-MDI/IX) feature is built in, allowing the dual cables to be swapped while maintaining the same capability. To support longer cable runs from your network switch or router, the power injector is designed to accommodate up to a 100 meter coaxial cable run plus 100 meters of indoor Cat5 cable—enabling total cable runs up to 200 meters. Lightning and surge protection is also included at the F-Type connector interface to provide added protection to your network devices. The power injector requires a 48V DC source supplied by Cisco.
Power Injector LR2T	The Power Injector LR2T supports all the capabilities of LR2. It is designed for use in transportation applications and operates with an input voltage range of +12 to +40V DC. The DC source is provided by the user. The LR2T can therefore be vehicle- or solar-powered.
Power Supply	<ul style="list-style-type: none"> <li>48V DC supply for AIR-PWRINJ-BLR2=</li> <li>User-supplied 12 to 40V DC source for AIR-PWRINJ_BLR2T=. Could require an external load-dump-module for automotive and bus installations.</li> </ul>
AIR-BR1310G-x-K9 or AIR-LAP1310G-x-K9 Integrated Antenna	<ul style="list-style-type: none"> <li>Vertical polarization</li> <li>13-dBi gain</li> <li>36° E-plane by 38° H-plane (3-dB beam width)</li> </ul>

Source : Cisco system inc., Data sheet : Cisco Aironet 1300 Series Outdoor Access Point or Bridge

## Exemple de data sheet

### Descriptif : Antenne wifi interne 7dBi

[Haut de page ^](#)

Antenne wifi interne 7dBi - Spécifications techniques Gain d'antenne: 7dBi Angle d'ouverture horizontal: 360° Angle d'ouverture vertical: 40° Fréquence d'utilisation: 2.4 - 2... Voir la présentation

\* Prix renseigné par le vendeur

#### Informations générales sur le produit

Marque	<u>LINDY</u>
Nom du produit	Antenne wifi interne 7dBi
Catégorie	CLE WIFI - 3G

#### Informations générales

Poids net en kg	0 g
-----------------	-----

Découvrez aussi : [Guide Achat Réseau WiFi - Bluetooth - Choix par marque - Adaptateur USB WiFi - Carte WiFi - Routeur - Modem - Point d'accès - Répéteur de signal WiFi - Adaptateur USB Bluetooth](#)

### Présentation produit : Antenne wifi interne 7dBi

[Haut de page ^](#)

Antenne wifi interne 7dBi - Spécifications techniques Gain d'antenne: 7dBi Angle d'ouverture horizontal: 360° Angle d'ouverture vertical: 40° Fréquence d'utilisation: 2.4 - 2.5GHz Spécifications réseau supportées IEEE 802.11b/g/n VSWR (taux d'ondes stationnaires): <2.0 Polarisation: verticale (linéaire) Impédance d'entrée: 50 ohms Prise: RP SMA (RG178). 1m Température d'utilisation: -10°C - 55°C Humidité: 95% maxi, non condensée Dimensions: 300 x Ø 12mm (sans pied) - Utilisez cette antenne pour émettre le signal wifi dans toutes les directions, avec un gain d'antenne de 7dBi.



[www.heh.be](http://www.heh.be)



299

## Exemple de data sheet

Feature	AIR-ANT2455V-H
Description	Omnidirectional
Application	Outdoor, direct mount on unit
Gain	5.5 dBi
Frequency	2.4 GHz
Beam width	25° V
Cable Length	None
Dimensions	12.5 in (31.75 cm) x 1 in. (2.54 cm)
Weight	5 oz. (14 kg)
Operating Temperature	-30° to 70°C

RG214-50/Fe ATTENUATION		
Frequency	Attenuation dB/100 m	Attenuation dB/100 ft
300	12.0	3.66
600	19.0	5.79
900	24.0	7.31
1200	29.0	8.84
1500	33.0	10.1
1800	37.0	11.3
2100	41.0	12.5
2400	45.0	13.7
2700	49.0	14.9
3000	53.0	15.8
3300	56.0	17.1
3600	60.0	18.3
3900	63.0	19.2
4200	66.0	20.1
4500	70.0	21.3

Receive Sensitivity	802.11b: • 1 Mbps: -94 dBm • 2 Mbps: -91 dBm • 5.5 Mbps: -89 dBm • 11 Mbps: -85 dBm
802.11g:	• 1 Mbps: -95 dBm • 2 Mbps: -91 dBm • 5.5 Mbps: -89 dBm • 6 Mbps: -90 dBm 9 Mbps: -84 dBm • 11 Mbps: -86 dBm • 12 Mbps: -82 dBm • 18 Mbps: -80 dBm • 24 Mbps: -77 dBm • 36 Mbps: -73 dBm • 48 Mbps: -72 dBm • 54 Mbps: -72 dBm

Available Transmit Power Settings	802.11g: • CCK: + 100 mW (20 dBm) + 50 mW (17 dBm) + 30 mW (15 dBm) + 20 mW (13 dBm) + 10 mW (10 dBm) + 5 mW (7 dBm) + 1 mW (0 dBm) • OFDM: + 30 mW (15 dBm) + 20 mW (13 dBm) + 10 mW (10 dBm) + 5 mW (7 dBm) + 1 mW (0 dBm)
-----------------------------------	--



300

## Chapitre 9

# Introduction au pentesting

Pentesting Phases 1 et 2

## Introduction pentesting

### • Pентest et audit de sécurité

#### – Tests d'intrusion, tests de pénétration ou pentest

- Technique de piratage consistant à tester la vulnérabilité d'un système informatique
  - Système = une IP, un réseau, un serveur, une application, un site web...
  - Piratage éthique et légal s'il est commandité par un client (Posture du hacker).
  - Se base sur la recherche et l'identification des points de vulnérabilité et sur une tentative d'intrusion afin de vérifier que des failles sont exploitables.
  - Le pentest doit aussi vérifier ce que l'attaquant pourrait gagner après l'exploitation d'une faille afin de définir et classifier les risques encourus.
  - Souvent, le pentest propose un plan de contre-mesures permettant d'améliorer la sécurité.

- Conclusions valables uniquement à un instant T

- Le test ne fournit pas une surveillance continue du système informatique.
- Le système d'information (SI) de l'entreprise va évoluer, de nouvelles brèches peuvent donc apparaître.

- **Pentest et audit de sécurité (suite)**

- **Audit de sécurité**

- Dans un audit, on réalise une étude approfondie du SI du client, avec l'aide de celui-ci.
      - Vérification de la sécurité organisationnelle, le PRA/PCA, le DLP, la conformité à une norme (PCI DSS, HIPAA), contrôle des configurations, des codes, effectuer une analyse des risques (EBIOS, MEHARI,...).
    - L'audit peut inclure un pentest ou simplement déterminer des failles potentielles sans vérifier si celles-ci sont réellement exploitables.

- **Stratégies d'audit**

- En aveugle (l'auditeur est en env. non connu, le service info est prévenu).
    - En double aveugle (auditeur en env. non connu, service info non prévenu).
    - En tandem (auditeur en environnement connu, tout le monde collabore).
    - En boîte grise, en double boîte grise, inversée.

- **Quand faire un pentest ?**

- **Lors de la conception**

- Pour tester un projet avant de le mettre en production.

- **Lors du fonctionnement (à réaliser à intervalles réguliers)**

- Car de nouvelles failles sont découvertes régulièrement.
    - Car le Système d'information de l'entreprise évolue, de nouvelles brèches peuvent donc apparaître.

- **Après une cyberattaque**

- Pour en éviter une autre.

- **Quand vous en avez l'obligation réglementaire**

- Par exemple, c'est une obligation pour les organisations impliquées dans le stockage, le traitement ou la transmission des transactions par carte de crédit et de débit (PCI DSS : Payment Card Industry Data Security Standard)

- **Bénéfices d'un Pentest**

- Un pentest peut viser plusieurs objectifs (à définir avec le client)
  - Démontrer qu'un attaquant potentiel est en capacité de trouver des vulnérabilités et de les exploiter pour s'introduire dans le système d'information.
  - Dresser une liste des vulnérabilités ou faiblesses du système de sécurité pouvant être exploitées.
  - Lister les informations sensibles ou critiques qu'un hacker pourrait se procurer.
  - Tester l'efficacité des systèmes de détections d'intrusion.
  - Tester la réactivité des équipes de sécurité (SOC) et des utilisateurs (ingénierie sociale)

- **Phases d'un pentest**

- Un pentest se réalise en plusieurs phases ou étapes
  - Les phases à réaliser dépendent de la méthodologie de pentesting choisie
    - PTES : Penetration Testing Methodologies and Standards
    - OSSTMM : Open Source Security Testing Methodology Manual.
    - OWASP : Open Web Application Security Project.
    - ...
  - 7 étapes du pentest selon la méthodologie "PTES"
    1. Pre-engagement Interactions
    2. Intelligence Gathering
    3. Threat Modeling
    4. Vulnerability Analysis
    5. Exploitation
    6. Post Exploitation
    7. Reporting

### 1. Pre-engagement Interactions

- Phase de définition des accords contractuels et financiers

- L'objectif est d'établir un cadre légal, technique et organisationnel, validé par le client et le prestataire (clauses de confidentialités, ...).

- Les règles d'engagement doivent être claires

- Le prestataire et le client doivent avoir une compréhension claire de ce qui se passera pendant le test d'intrusion

- Quels systèmes, données, processus et activités entrent dans le cadre du test ?
- Quel type de pentest (white/grey/black box) ?
- Quelles informations sur la cible le pentester a-t-il à sa disposition ?
- Etablissement de canaux de communication sécurisés.
- Le budget.

- Le client doit donner son autorisation au testeur (contrat)

- Si le pentesteur s'écarte des termes du contrat, il est dans l'illégalité : ce n'est plus du pentesting mais du piratage.

### 2. Intelligence Gathering (La collecte d'informations)

- Rassembler un maximum d'informations sur les cibles

- On parle de *reconnaissance*, *footprinting* ou *information gathering*
- Informations sur l'entreprise (sites, agences), les employés (qui fait quoi), le FAI, les adresses IP des serveurs publics, ...
  - Afin de pouvoir identifier les différents systèmes de la cible et leurs caractéristiques.
  - Ces informations permettront de dresser une liste de cibles classées par ordre de priorité.

- Via de la reconnaissance passive (ou semi-passive)

- En collectant des données accessibles publiquement (par exemple WHOIS, les réseaux sociaux).
- En collectant des données accessibles via une utilisation normale (par exemple en naviguant sur l'application du client).

- Via de la reconnaissance active

- En utilisant des outils dédiés (Par exemples, des scanners de ports).
- Risque plus élevé de se faire repérer.

### 3. Threat Modeling (Modélisation des menaces)

– L'objectif de cette phase est d'identifier

- **Les principales cibles au sein d'une entreprise**

- Les brevets et R&D, les outils industriels de production, les informations financières, le site vitrine, la base de données des clients, ...
- Analyse de la valeur de chaque cible découverte et de l'impact si celle-ci est compromise.

- **Les sources de menaces les plus probables**

- Le crime organisé, hacktivistes, un employé interne mécontent, ...

– Pour mieux préparer la phase d'attaque

- Les conclusions de cette phase seront les plus pertinentes lorsque le pentest est conduit en "boîte blanche".
- Déterminer les cibles et les attaquants les plus probables permet de mettre en place un pentest plus proche de la réalité.

### 4. Vulnerability Analysis (Analyse des vulnérabilités)

– Identifier des vulnérabilités exploitables des cibles

- Analyse des informations récoltées précédemment pour identifier des vulnérabilités.

- Par exemple via les numéros de version des OS, des applications, ...

- Recherche actives de vulnérabilités.

- A l'aide d'un scanner de vulnérabilités.
- En analysant le code source de programmes (si white box pentesting).
- En essayant des identifiants par défaut des périphériques.
- ...

– Lister les attaques possibles

- Toutes ces informations vont permettre la création d'une liste d'attaques possibles dont certaines seront mises en application lors de la phase d'exploitation.

## 5. Exploitation

- Consiste à tenter d'exploiter les vulnérabilités
  - Développer un plan d'action et mettre en place les méthodes d'attaque.
  - Essayer d'exploiter les vulnérabilités découvertes et de pénétrer le SI.
- Grande variété de scénario d'attaque
  - Attaques sur les acteurs humains (phishing, usurpation d'identité).
  - Injections SQL.
  - Brute forcing.
  - Man in the middle.
  - Crochetage de serrure.
  - ...

## 6. Post Exploitation

- Elle a pour objectifs
  - D'entrer aussi profondément que possible dans le SI
    - ATTENTION : en restant dans les limites établies par les règles d'engagement.
    - La récupération des accès et comptes utilisateurs supplémentaires, permettant de compromettre d'autres éléments du SI (Pivoting).
  - L'identification des informations sensibles accessibles.
  - La mise en place de canaux d'accès malveillants et permanents (backdoor, ...).
  - La récupération des preuves du succès du pentest.
    - Par exemple des captures d'écran pour étayer le rapport final.
- Applicable uniquement si l'étape l'exploitation a réussi

## 7. Reporting

### – Fournir les résultats des tests de pénétration au client

- Doit fournir des informations utiles au client sur la sécurité de son environnement informatique
  - La liste et la sévérité des vulnérabilités découvertes.
  - La complexité des corrections à apporter.
  - ...
- Doit fournir des recommandations claires et exploitables
  - Sur les méthodes de résolution et de correction des vulnérabilités découvertes.
  - Pour la mise en œuvre de nouveaux contrôles de sécurité.
  - Pour l'amélioration des contrôles existants.

### – Une présentation orale

- Plus ou moins technique en fonction des interlocuteurs présents.

## 7. Reporting (suite)

### – Un rapport pour le management

- Présente notamment les résultats sous la forme d'indicateurs chiffrés ou graphiques, l'analyse des risques et d'impact des différentes vulnérabilités identifiées avec les remédiations associées ainsi qu'une suggestion de planning pour leur application en fonction de leur priorité.

### – Un rapport technique détaillé

- Présente notamment les références CWE, une explication détaillée de la vulnérabilité et du chemin d'exploitation, des outils utilisés, des conseils pour la remédiation, les preuves associées.

## Pentesting Phase 1 : Pre-engagement Interactions

## Pre-engagement Interactions

- **Pre-engagement Interactions**
  - **Phase de définition des accords contractuels et financiers**
    - L'objectif est d'établir un cadre légal, technique et organisationnel, validé par le client et le prestataire (clauses de confidentialités, ...).
  - **Les règles d'engagement doivent être claires**
    - **Le prestataire et le client doivent avoir une compréhension claire de ce qui se passera pendant le test d'intrusion**
      - Quels systèmes, données, processus et activités entrent dans le cadre du test ?
      - Quel type de pentest (white/grey/black box) ?
      - Quelles informations sur la cible le pentester a-t-il à sa disposition ?
      - Etablissement de canaux de communication sécurisés.
      - Le budget.
  - **Le client doit donner son autorisation au testeur (contrat)**
    - Si le pentesteur s'écarte des termes du contrat, il est dans l'illégalité : ce n'est plus du pentesting mais du piratage.

- Déterminer pourquoi réaliser le pentest

- Le pentest basé sur un objectif précis (goal-based)

- Par exemple, tester une nouvelle application avant sa mise en production ou évaluer la sécurité d'une organisation récemment acquise.

- Le pentest de conformité (compliance-based)

- Servent à vérifier la conformité à une loi ou une norme.
  - Pour être conforme à certaines normes, l'entreprise a l'obligation de réaliser des pentests réguliers.
- Il peut nécessiter l'engagement d'un prestataire spécifique certifié pour effectuer l'évaluation.

- Le pentest en mode red team.

- Elle permet de confronter l'entreprise à des scénarios d'attaques crédibles en testant les réactions des équipes internes (Blue team).
- Généralement plus ciblé que les autres tests de pénétration.
  - Ne sont pas destinés à fournir des détails sur toutes les failles de sécurité d'une cible.

- ...

- Déterminer ce qui doit être testé et ce qui est interdit

- Définir ce qui doit être testé (scope, scoping)

- Quels systèmes, réseaux ou services doivent être testés ?
- Quand ces systèmes peuvent-ils être testés et combien de temps durera le pentest ?
- Quelles techniques sont autorisées ou interdites ?
  - Les équipes défensives peuvent-elles réagir (block-listing) ?
  - Les attaques destructives (effacement de mdp, DoS, ...) sont-elles autorisées ?
  - Les attaques contre les membres du personnel (phishing, ...) sont-elles autorisées ?
- Quelles autorisations le pentester doit-il avoir ?
- Comment réagir en cas de problème (notification immédiate, quel média, ...) ?
- Existe-t-il des informations/systèmes auxquelles le prestataire ne peut pas accéder ?
- Etc.

- Le prestataire doit comprendre tous les éléments du pentest

- C'est en fonction de ces éléments qu'il peut établir un plan d'action pour son pentest.

### • Législation

#### – Le pentesteur doit tenir compte des lois et restrictions locales

- Vous devez toujours disposer d'une documentation claire de votre client indiquant que vous avez l'autorisation d'effectuer les tests.
- Vous devez être au courant des lois qui s'appliquent sur le lieu du pentest.
  - Les outils de sécurité spécifiques peuvent être considérés comme des "armes" et peuvent être contrôlés et limités par certaines lois nationales dans différents pays.

#### – Confidentialité

- Il faut rédiger un **accord de non-divulgation** indiquant quelles informations sont confidentielles et ne doivent pas être divulguées.
- Il faut définir comment seront traitées des données confidentielles (vulnérabilités, mots de passe trouvés, ...).
  - Qui y aura accès? Comment les communiquer? ...
- Une fois la mission achevée, il faut supprimer tous les enregistrements de vos systèmes (preuve de pénétration, liste des failles, ...).

### • Législation (suite)

#### – Autres concepts juridiques importants

- **SLA (Service Level Agreement)**
  - Document reprenant les attentes du client concernant les performances (qualité, délais, coût) du service de test de pénétration.
- **Statement of work (SOW)**
  - Cahier des charges qui spécifie les activités à réaliser lors d'une mission de test de pénétration.
- **Le contrat**
  - Il précise les termes de l'accord, la manière dont vous serez payé, et il fournit une documentation claire des services qui seront exécutés.
  - Le cas échéant, vous devez obtenir l'autorisation écrite de tout fournisseur tiers ou partenaire commercial impliqué.
- **Clauses de non-responsabilité**
  - Clause qui limite la responsabilité notamment dans le cas où l'entreprise perd des données suite à l'utilisation des applications ou des systèmes lors du pentest.

- Exemples de réglementations auxquelles certaines entreprises doivent se conformer
  - Protection des données
    - RGPD : Règlement général sur la protection des données (Europe).
  - Réglementation dans le secteur financier
    - GLBA : Gramm-Leach-Bliley Act (États-Unis).
  - Réglementation dans le secteur des soins de santé
    - HIPAA : Health Insurance Portability and Accountability Act (États-Unis).
  - Réglementation relative aux cartes de paiement.
    - PCI-DSS : Payment Card Industry Data Security Standard

- Types de pentest en fonction des connaissances du prestataire
  - Unknown-environment testing (anciennement Black box)
    - L'attaquant ne dispose d'aucune ou de très peu d'informations sur la cible.
      - Il est dans la peau d'une personne externe à l'entreprise.
      - Le champ d'application peut se limiter à identifier un chemin d'accès et s'arrêter là.
    - Ces tests à l'aveugle ont pour principaux avantages
      - D'être réalistes et plus rapides (cela coutent donc moins cher au client).
      - L'équipe défensive peut ne pas être au courant (du moment exact) de l'attaque, l'empêchant de se préparer et offrant ainsi une vision plus réelle de la manière dont les dispositifs de sécurité réagissent.
    - Les inconvénients sont qu'ils sont moins exhaustifs et ne testent pas la qualité de la configuration des systèmes.

- **Types de pentest en fonction des connaissances du prestataire**
  - Known-environment testing (Anciennement White box)
  - **Le pentester dispose d'un maximum d'informations**
    - Les schémas topologiques.
    - Des identifiants de compte utilisateur.
    - Les configurations des systèmes.
    - Le code source des applications.
    - Etc.
  - **Permet au pentester d'aller beaucoup plus loin dans l'analyse des cibles**
    - L'objectif est d'identifier autant de failles de sécurité que possible.
    - Le pentester est dans la peau d'un « administrateur système et réseau » de l'entreprise cible.
    - Nécessite plus de connaissances de la part du pentester.

- **Types de pentest en fonction des connaissances du prestataire**
  - Partially known environment testing (anciennement Grey box)
  - **Le pentester ne possède qu'une quantité limitée d'informations**
    - Approche hybride entre les tests dans un environnement inconnu et les tests dans un environnement connu.
    - Comme beaucoup de compromissions commencent par un client et se propagent à travers le réseau, le pentester commence à l'intérieur du réseau.
      - » Il a accès à une machine cliente et dispose d'un couple identifiant/mot de passe valide.
    - Permet notamment de savoir à quoi un « utilisateur normal » de l'entreprise cible pourrait avoir accès (collaborateur malveillant ou collaborateur dont l'ordinateur a été piraté par exemple).

## Pentesting Phase 2 : Intelligence Gathering (collecte d'informations)

## Phases d'un pentest

- **Intelligence Gathering (La collecte d'informations)**
  - Consiste à rassembler un maximum d'informations sur les cibles
    - Recherche d'informations sur l'entreprise :
      - Les sites/agences, les employés (qui fait quoi), le FAI, les adresses IP des serveurs publics, les logiciels utilisés, ...
    - Afin de pouvoir identifier les différents systèmes de la cible et leurs caractéristiques.
    - Ces informations permettront de dresser une liste de cibles classées par ordre de priorité.
  - **Terminologie**
    - On parle de *reconnaissance*, *footprinting* ou *information gathering*.
  - **Trois manières de collecter des informations**
    - Via de la reconnaissance passive.
    - Via de la reconnaissance semi-passive.
    - Via de la reconnaissance active.

- Reconnaissances par des méthodes passives

- Reconnaissance passive

- Méthode de collecte d'informations dans laquelle les outils n'interagissent pas directement avec l'appareil ou le réseau cible.
    - Par exemple, en collectant des données accessibles publiquement (via les réseaux sociaux, WHOIS, DNS, ...).
    - Plus difficile d'obtenir des informations utiles sans jamais envoyer de trafic vers l'organisation cible mais idéal pour ne pas être détecté par les systèmes de défense.

- Reconnaissance semi-passive

- Collecte avec interaction avec la cible mais via des méthodes qui ressemblent à un trafic et à un comportement normaux.
      - Par exemple en naviguant sur l'application ou le site web du client.
    - Pas de recherches inversées approfondies ou de requêtes DNS par force brute, pas de scan de ports, ...

- Reconnaissance active

- Collecte en interagissant avec la cible, par exemple via l'utilisation de scanners de ports ou de scanner de vulnérabilité.
    - Dans l'idéal, ces interactions devraient être détectées par les systèmes/équipes défensives comme étant un comportement suspect ou malveillant.

- Reconnaissances par des méthodes passives ou semi-passives

- Open-Source INTeelligence (OSINT)

- Renseignement d'Origine Source Ouverte (ROSO).
    - Ensemble de techniques, méthodes et activités visant à collecter et analyser des informations extraites de sources librement accessibles.
      - Sites web, conférences, médias sociaux, Registres DNS, ...
      - Déclarations fiscales des entreprises, ...
    - Les informations collectées peuvent notamment contribuer à rendre plus crédibles des attaques de type ingénierie sociale.

– Exemples d'informations à rechercher

- **Mesures de sécurité physique du site**
  - Emplacement des caméras, capteurs, clôtures, entrée des fournisseurs, ...
  - Existence de sites secondaires (agence souvent moins sécurisée que le site central).
- **Relations de l'entreprise**
  - Partenaires commerciaux, fournisseurs, clients, ...
  - Ces informations peuvent être utilisées pour mieux comprendre l'entreprise afin de créer des scénarios d'ingénierie sociale réussis.
  - Il est parfois plus facile de pour un hacker de pirater un petit partenaire commercial qui dispose de certains accès privilégiés à l'entreprise cible.
- **Dates importantes de la société**
  - Réunions du conseil d'administration, jours fériés, anniversaires, JPO, ...
  - » Une attaque peut être plus difficilement contrée en été lorsqu'une partie du personnel est en vacances.
- **Offres d'emplois**
  - Permet de déterminer les types de technologies utilisées au sein de l'organisation.

– Exemples d'informations à rechercher (suite)

- **Listes des employés (énumération)**
  - Organigramme et identifications des postes.
  - Cartographier les interactions possibles entre les personnes dans l'organisation et à savoir comment y accéder depuis l'extérieur.
  - Noms d'utilisateur, adresses email, numéro de téléphone, ...
- **Média sociaux**
  - Localisation des employés.
- **Métadonnées des documents**
  - Fournissent des informations sur les documents et les logiciels.
  - » Par exemple : nom de l'auteur/du créateur, l'heure et la date, l'emplacement dans un réseau informatique, la géolocalisation, le logiciel utilisé, ...
- **Informations sur les réseaux**
  - Adresses IP, fréquences Wi-Fi, normes de sécurité, ...
- **Existence de contre-mesures**
  - FW, A-V, WAF, proxy, ...
- ...

### – Exemples d'outils de collecte passifs ou semi-passifs

- **Outils de recherche de domaines**
  - DNSdumpster, Dnsrecon, ...
- **Outils pour trouver des métadonnées dans les documents (Office, PDF, ...).**
  - FOCA, Exiftool, meta-extractor.
- **Outils pour trouver des localisations**
  - Média sociaux, applications Bing Map, Foursquare, Google Latitude , Yelp, Gowalla.
- **Pour trouver les adresses mail**
  - Sites web, groupes, blogs, forums, portails de réseaux sociaux, ...
- **Outils divers**
  - host, dig, nslookup, traceroute.
  - WHOIS Lookups.
  - Spiderfoot.
  - Recon-neg.
- ...

### – Exemples d'outils de collecte passifs ou semi-passifs (suite)

- **Shodan**
  - Moteur de recherche qui scanne le web 24h/24 à la recherche d'objets connectés à Internet.
    - » Caméras Web, éoliennes, yachts, appareils médicaux, feux de circulation,, lecteurs de plaques d'immatriculation, téléviseurs intelligents, ...
  - Permet de rechercher des périphériques vulnérables à des exploits spécifiques.
  - En utilisation défensive, il permet de garder une vue complète de tous nos services exposés sur le Net.
- **Censys**
  - Moteur de recherche qui collecte les données sur les appareils connectés en IPv4 sur le net.
    - » Recherches par mots clés, par IP, par nom de domaine, par protocole utilisé, par certificat, ...etc.
    - » Fournit des informations géographiques si elles sont disponibles, un résumé complet des services exposés par l'hôte.

- Exemple avec shodan
  - Liste de machines accessibles en RDP

- Reconnaissances par des méthodes actives
  - Le pentester interagit avec le système cible pour collecter des informations
    - Par exemple en utilisant un scanner (de ports, de vulnérabilités)
      - Découverte des hôtes et des ports ouverts.
      - Identification des services, de leur version, de leurs vulnérabilités.
      - Identification du système d'exploitation (OS fingerprinting).
    - Si pentest en whitebox, voir aussi :
      - A exploiter les systèmes de gestion centraux (SCCM, Jamf Pro, GLPI, ...)
      - Les fichiers journaux de réseau ou de serveurs DHCP.
      - Les fichiers de configuration.
      - Le code source des programmes.
      - ...
  - Footprinting
    - Nom donné à la technique consistant à récolter des informations afin de pouvoir identifier les différents systèmes de la cible.
    - Ces informations permettront de dresser une liste de cibles classées par ordre de priorité.

- Exemple d'outils de reconnaissance active
  - Scanner de ports
    - Nmap, masscan.
  - Scanner de vulnérabilités
    - Nessus, OpenVAS, Qualys, ...
    - Dans PTES, l'utilisation d'un scanner de vulnérabilité peut aussi être reprise dans la phase 3 : vulnerability analysis.
  - Scanner de services Web
    - Nikto.
    - Burp Suite.
      - Composé de : serveur proxy (Burp Proxy), robot d'indexation (Burp Spider), un outil d'intrusion (Burp Intruder), un scanner de vulnérabilités (Burp Scanner) et un répéteur HTTP (Burp Repeater).

## Chapitre 9

# Introduction à Nmap

- Network scanning

- Qu'est-ce qu'un scan du réseau?

- Processus permettant de découvrir les périphériques actifs d'un réseau ainsi que fournir des informations sur ces périphériques.

- Exemple d'informations pouvant être récoltées

- **Cartographie du réseau** (Network mapping) : Envoi de messages sur l'ensemble du réseau afin d'obtenir une réponse et ainsi découvrir des hôtes actifs.
- **Port/services actifs** (Port scanning) : Envoi de messages à des ports TCP/UDP afin de déterminer s'ils sont actifs.
- **Détection de service** : Envoi de messages à un port afin de générer des réponses qui permettront de déterminer le type et la version du service en cours d'exécution.
- **Détection du système d'exploitation** : Envoi de messages à un hôte afin de générer des réponses qui permettront de déterminer le système d'exploitation.
- **Détection des vulnérabilités connues** : Nmap comprend une suite de scripts (Nmap Scripting Engine, NSE) comparant les versions des services découverts avec la base de données CVE.
- ...

- Principe

- Principe d'un scan

- Envoi d'une requête et analyse de la réponse.

- Exemple d'un scan de type Connect (-sT)

- Ce scan réalise une connexion TCP complète.
- Scan utilisé lorsque la commande nmap n'a pas les priviléges administrateur.

Réponse de la cible	Status bmap du port	Analyse
TCP SYN/ACK	Open	Le service écoute sur ce port
TCP RST	Closed	Le service n'écoute pas sur ce port
Pas de réponse	Filtered	Le port est filtré (pare-feu)

- Compte admin/root

- Il est probable que nombreux scans nécessitent d'être exécutés avec un compte administrateur.

```
Connect scan : # nmap -sT 192.168.0.1
```

- Principe (suite)

- Scan

- Les scanner font du « bruit »

- Comme ils envoient des requêtes sur le réseau, ces requêtes peuvent être détectées, analysées et/ou loguées par les dispositifs de sécurité.

- Le scan peut donc être détecté

- Les outils de sécurité et les systèmes de détection d'intrusion (IDS) sont plus susceptibles de déclencher des alarmes lors d'une connexion TCP complète et d'autant plus si sur plusieurs connexions TCP proviennent du même hôte.

- Certains scan laissent plus de traces que d'autres

- La cible peut loguer les connexions TCP mais pas les simples SYN.

- Scan furtif (Stealth Scans)

- Type de scan utilisant des options moins « bruyante » dans le but de ne pas se faire repérer par les systèmes de sécurité.
      - Par exemple, un *SYN scan* est moins bruyant qu'un *Connect scan*.

- Network scanning (suite)

- Utilisations principales

- Audit de sécurité, test de pénétration

- Auditer les pare-feu en vérifiant que le filtrage fonctionne correctement.
      - Rechercher des ports ouverts sur les appareils périphériques.
      - Effectuer une reconnaissance de certaines versions de services.
      - Rechercher des services et OS obsolètes ou non autorisés.
      - Détection des portes dérobées
      - Détection des vulnérabilités.
      - ...

- Test de conformité

- Tester les ports ouverts sur les interfaces d'un pare-feu.
      - Analyser les plages d'adresses IP pour déterminer si des applications réseau non autorisées sont installées.
      - Déterminer si la bonne version d'un service est installée.
      - Localiser les systèmes dont les ports de partage de fichiers sont ouverts.
      - Localiser les périphériques utilisant des systèmes d'exploitation non autorisés.
      - ...

- Réglementation

- Un scan de ports non approuvé peut entraîner :
  - Une poursuite pénale.
  - Un licenciement.
  - Une disqualification.
  - Une interdiction par votre fournisseur d'accès internet.
- Vous ne devez donc l'utiliser que lorsque vous en avez l'autorisation expresse
  - Par exemple, lorsque c'est décrit la description de votre job
    - Attention que cela ne vous donne pas le droit de scanner n'importe quelle cible.

- Exemples de scanner

- Nmap, Zenmap, Superscan, Angry IP scanner, Masscan, ...

- Techniques de découverte d'hôtes avec Nmap

- ICMP ECHO Request (icmp type 8)
  - Permet de découvrir les hôtes actifs lorsque ceux-ci envoient une réponse ICMP ECHO reply (ICMP type 0).
  - L'envoi de message ICMP ECHO requests à de multiples hôtes est appelé un "ping sweep".
  - Remarque : toutes les machines ne répondent pas au ping.
- ICMP Timestamp (icmp type 13)
  - L'hôte répond en fournit l'heure actuelle.
- ICMP Address Mask Request (icmp type 17)
  - L'hôte répond en fournit son masque de sous-réseau.

```
ICMP type 8 : # nmap -PE 192.168.0.1
ICMP type 13 : # nmap -PP 192.168.0.1
ICMP type 17 : # nmap -PM 192.168.0.1
```

- Techniques de découverte d'hôtes

- TCP SYN scan (half open scan)

- Envoie un message TCP SYN (vide) à un port TCP (port 80 par défaut) de la machine cible qui répond par un SYN/ACK ou un RST.
    - Avantages
      - Relativement discret et furtif.
      - Rapide.
    - Nmap ne complète pas la connexion TCP, contrairement à un TCP connect (-sT)
      - -PS : P=par quelle méthode découvrir des hôtes. S = via un SYN
      - -sS : s=quel type de scan de ports réaliser. S= un SYN scan.

```
TCP SYN : # nmap -PS 192.168.0.1
TCP SYN : # nmap -sS 192.168.0.1
```

- Techniques de découverte d'hôtes

- TCP FIN Scan (-sF)

- Un paquet FIN est envoyé à un port cible.
      - Si le port est fermé, le système cible renvoie un paquet RST.
      - Si rien n'est reçu, le port est probablement ouvert car le comportement normal serait d'ignorer le paquet FIN.
      - Plus furtif qu'un scan SYN.
    - Pas pour les machines Windows
      - Les systèmes basés sur Windows, répondent par des RST, quel que soit l'état du port.

- “Ping scan”

- Envoie un ICMP ECHO request et un TCP (ACK) à la cible (vers le port 80 par défaut).

```
Ping scan : # nmap -sP 192.168.0.1
Ping scan : # nmap -sP 192.168.0.0/24
```

- Techniques de découverte d'hôtes (suite)

- TCP ACK ping

- Envoi d'un paquet dont seul le drapeau ACK est activé vers un port TCP spécifié.
- S'il n'y a pas de filtrage les ports ouverts et fermés renverront un paquet RST.
  - Nmap les répertorie alors comme non filtrés (unfiltered), les cibles sont joignables.
  - Ne permet pas de déterminer les ports sont ouverts ou fermés.
- S'il y a un filtrage, soit le scanner ne recevra rien, soit il recevra un message d'erreur ICMP (Type 3 : Destination unreachable, code 1, 2, 3, 9, 10, ou 13).
  - Nmap les répertorie alors comme filtrés (filtered).

Type	Code	Description
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation needed and DF flag set
	5	Source route failed
	...	...

```
# nmap -sA 192.168.0.1
```

• • • 345

- Techniques de découverte d'hôtes (suite)

- UDP scan

- Envie un message UDP à un port UDP de la machine cible
  - UDP n'envoie pas de réponses (par exemple SYN/ACK) comme TCP.
  - UDP utilise ICMP (port unreachable) pour répondre aux requêtes vers des ports fermés.
- Paquets UDP complets ou vides
  - Les ports UDP doivent être sondés par des requêtes UDP réelles au niveau de l'application. Or pour la plupart des ports, Nmap envoie un paquet UDP vide.
    - Considéré comme invalide et abandonné par la cible → pas de réponse.
  - Pour quelques-uns des ports les plus courants, une charge utile spécifique au protocole sera envoyée par Nmap.

```
# nmap -PU 192.168.0.1
# nmap -p 53 -sU 192.168.0.1
```

Pas de réponse car abandonné par la cible ou car filtré (FW) ?  
→ marqué comme open | filtered par Nmap

Probe Response	Assigned State
Any UDP response from target port (unusual)	open
No response received (even after retransmissions)	open filtered
ICMP port unreachable error (type 3, code 3)	closed
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	filtered

• • • 346

- Techniques de découverte d'hôtes (suite)

- IP protocol ping

- Envoie un paquet IP avec le N° de protocole ([PROTOLIST]) dans l'en-tête IP
      - Pour ICMP (protocole 1), ICMP (2), TCP (6) et UDP (17), les paquets sont envoyés avec les en-têtes de protocole appropriés.
      - Les autres protocoles sont envoyés sans données supplémentaires au-delà de l'en-tête IP (sauf si l'option --data-length est spécifiée).
      - Si une réponse est envoyée cela signifie que la machine est active.

```
# nmap -PO [PROTOLIST] 192.168.0.1
```

- Inverse mapping

- Le scan ne fonctionne pas toujours

- Par exemple, si l'hôte est configuré pour ne pas répondre aux messages ICMP ou si l'OS, un pare-feu ou un routeur filtre le trafic entre le scanner et la cible.

- Réponse du dispositif de filtrage?

- Selon la configuration, un pare-feu ou un routeur qui bloque les pings peut répondre par un paquet ICMP host unreachable si la cible n'est pas active, ce qui permet de déduire les hôtes actifs.

- Techniques de découverte d'hôtes (suite)

- ARP Scan (-PR)

- L'envoi de requêtes (ICMP ECHO) sur un réseau Ethernet nécessite de connaître les adresses MAC des cibles.
      - Envoy d'une requête ARP vers chaque cible du scan Nmap.
      - Dans un range IP, la grande majorité des adresses IP risquent d'être inutilisées.
      - Si ARP ne reçoit pas de réponse, il envoie une 2<sup>ème</sup> puis une 3<sup>ème</sup> requête ARP pour chaque cible. → Plusieurs secondes perdues pour chaque cible → Cela ralenti Nmap.

- Table ARP

- La table ARP du scanner va se remplir, même pour les IP non résolues (→ saturer?).

- Le scan ARP résout ces deux problèmes

- Nmap émet les requêtes ARP brutes et gère lui-même la retransmission et les délais d'attente et le cache ARP du système est contourné.

```
C:\>arp -av
Interface : 10.10.213.7 --- 0x18
  Adresse Internet      Adresse physique      Type
  10.10.213.1          00-00-00-00-00-00  non valide
  10.10.213.2          00-00-00-00-00-00  non valide
  10.10.213.3          00-00-00-00-00-00  non valide
  10.10.213.4          00-00-00-00-00-00  non valide
```

```
# nmap -PR 192.168.0.1
```

Remarque : si réponse ARP reçue, l'hôte est découvert → ICMP inutile.

- Techniques de découverte d'hôtes (suite)

- Discovery scan (-sn)

- Pour rechercher rapidement des hôtes actifs d'un réseau, vous pouvez effectuer en une opération un balayage qui enverra plusieurs types de requêtes.
    - Ainsi, avec l'option -sn, nmap envoie
      - une demande d'écho ICMP (ping),
      - un SYN TCP au port 443,
      - un ACK TCP au port 80
      - et une demande d'horodatage ICMP (icmp timestamp).

```
# nmap -sn 192.168.0.0/24
```

- Autres options courantes (suite)

- L'option -T[0-5]

- Permet de définir la politique de temporisation de Nmap, plus la valeur est élevée, plus le scan est rapide.
      - Un scan (beaucoup) plus lent peut permettre de ne pas être détecté.
    - Les options possibles :
      - -T0 (Paranoid) : Très lent, utilisé pour éviter les IDS
      - -T1 (Sneaky) : Assez lent, utilisé pour l'évasion IDS
      - -T2 (Polite) : Ralentit pour consommer moins de bande passante, fonctionne environ 10 fois plus lentement que la valeur par défaut.
      - -T3 (Normal) : Par défaut, modèle de synchronisation dynamique basé sur la réactivité de la cible
      - -T4 (Agressif) : Suppose un réseau rapide et fiable et peut submerger les cibles.
      - -T5 (fou) : Très agressif ; risque de submerger les cibles ou de manquer des ports ouverts.

- Autres options courantes (suite)

- L'option `-v` (`--verbose`)

- Le mode verbeux affiche aussi les hôtes inactifs, ainsi que des informations supplémentaires sur les hôtes actifs.
    - Plus il y a de « v » plus le mode est verbeux (`-vv`).

- L'option `--reason`

- Cette option affiche plus de détails sur la réponse des hôtes cibles.

- L'option `--data-length<Longueur>`

- Les systèmes de détection/prévention d'intrusion (IDPS), peuvent générer des alertes pour les paquets ping de zéro octet. Cette option permet d'éviter ces alertes en ajoutant `<Longueur>` octets aléatoires de données à chaque paquet.
    - Fonctionne avec les types de scan ping TCP, UDP et ICMP.
    - Une « Longueur » de 32 donne l'impression qu'une demande d'écho provient de Windows, tandis que 56 simule le ping par défaut de Linux.

- Autres options courantes (suite)

- Les options `--exclude` et `--excludefile`

- `--exclude <host1[,host2][,host3],...>` et `--excludefile <exclude_file>` permettent de spécifier une liste de cibles à exclure du scan.

- L'option `-n`

- La résolution DNS peut fortement allonger la durée d'un scan. L'option `-n` permet de désactiver les résolutions DNS.

- L'option `-6`

- Pour l'IPv6.

- **États des ports**

- **Open (ouvert)**

- Une application accepte des connexions TCP ou des paquets UDP sur ce port.
    - Il y a un service qui fonctionne derrière ces ports. Les attaques essaieront d'exploiter ces ports ouverts.

- **Closed (fermé)**

- Le port est accessible mais il n'y a pas d'application en écoute sur un port fermé.
    - La machine cible a répondu que le port était fermé ce qui est utile pour déterminer si un hôte est actif (découverte d'hôtes), ou pour la détection de l'OS.

- **Filtered (filtré)**

- Des dispositifs de filtrage (pare-feu) peuvent empêcher les paquets de tests Nmap (probes) d'atteindre leur cible.
      - Parfois ils répondent avec un message d'erreur ICMP « destination unreachable » (de type 3 code 13) mais souvent ils abandonnent les paquets sans rien répondre.
    - Dans ce cas, Nmap peut difficilement déterminer si un port est ouvert et le renseigne comme « filtré ».

- **États des ports (suite)**

- **Unfiltered (non-filtré)**

- L'état non-filtré signifie qu'un port est accessible, mais que Nmap est incapable de déterminer s'il est ouvert ou fermé.
    - Seul le scan ACK catégorise les ports dans cet état.

- **Open | filtered (ouvert | filtré)**

- Nmap met dans cet état les ports dont il est incapable de déterminer l'état entre ouvert et filtré.
    - Si des ports ouverts ne renvoient pas de réponse, Nmap est incapable de déterminer si le port est ouvert (mais n'a pas répondu car la requête est invalide (UDP ping)) ou si le port est filtré (un pare-feu a bloqué la réponse).

- **Closed | filtered (fermé | filtré)**

- Uniquement utilisé par le scan *Idle* basé sur les identifiants de paquets IP lorsque Nmap est incapable de déterminer si un port est fermé ou filtré.

- Exemple de scan

- <http://www.scanme.org/>

- Vous êtes autorisé à scanner cette machine (via Nmap ou d'autres scanners de ports).
- Essayez de ne pas trop solliciter le serveur.
  - Quelques scans par jour suffisent, n'utilisez pas ce site pour tester un brute force.

Commande: nmap -sS scanme.org

Hôtes	Services	Sortie de Nmap	Ports / hôtes	Topologie	Détails de l'hôte	Scans
OS	Hôte	nmap -sS scanme.org	Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-17 17:21 Paris, Madrid			
	scanme.org (45.33.32.156)		Nmap scan report for scanme.org (45.33.32.156)			
			Host is up (0.15s latency).			
			rDNS record for 45.33.32.156: scanme.nmap.org			
			Not shown: 966 filtered tcp ports (no-response), 31 closed tcp ports (reset)			
			PORt STATE SERVICE			
			21/tcp open  ftp			
			22/tcp open  ssh			
			80/tcp open  http			
						Nmap done: 1 IP address (1 host up) scanned in 13.90 seconds

- Détection d'OS (Appelé aussi OS fingerprinting)

- Active fingerprinting

- Les systèmes d'exploitation ont tous des caractéristiques permettant leur identification dans leurs piles et configurations TCP/IP.

- Par exemple des paramètres tels que la taille de la fenêtre TCP et les numéros de séquence initiaux de TCP peuvent être différents pour chaque OS.

- Active : le scanner réseau envoie plusieurs paquets à la cible avec différents paramètres.

- Les réponses sont analysées et comparées à une liste de valeurs de demande/réponse connues afin de trouver une correspondance avec un OS.

- Peut être utile pour détecter des OS non autorisés ou trop vieux

- Nmap tente d'identifier le fabricant, l'OS, la version de l'OS, le type de périphérique.

- Peut être utilisé pour inventorier le réseau (mais de meilleurs outils existent)

```
# nmap -O 192.168.0.1
```

- Exemples de détection d'OS

```
# nmap -O scanme.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 16:32 Paris, Madrid
< Lignes omises >
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (85%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:4.4 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 2.6.32 (85%), Linux 3.2 (85%), Linux 3.8 (85%),
Linux 4.4 (85%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).
```

```
# nmap -O this_machine
< Lignes omises >
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops
```

→ La machine est en réalité un Windows 11

- Détection des services

- Sans détection de service

- Nmap utilise le fichier « nmap-services » pour corrélérer les ports ouverts trouvés et les services affiché dans les résultats.
    - En réalité, il peut s'agir d'un service différent ou même d'une application de type cheval de Troie utilisant ce port ouvert trouvé.

- Principe de la détection de service

- Fonctionne sur le même principe que la détection d'OS : Nmap envoie plusieurs paquets à la cible avec différents paramètres afin de déterminer :
      - Le service (HTTP, FTP, ...)
      - Le nom de l'application (WU-FTPD, VSFTP, ...)
      - Le numéro de version
      - L'état du port
      - ...

- Exemples de détection de service

```
nmap -sV scanme.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 16:52 Paris, Madrid
N SOCK ERROR [0.0330s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.15s latency).
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 966 filtered tcp ports (no-response), 31 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  tcpwrapped
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Formats de sortie des résultats

- Interactive

- Par défaut, Nmap affiche les résultats sur la sortie standard (à l'écran.).

- Normal (-oN)

- Les résultats sont également envoyés à la sortie standard, mais avec moins d'informations.

- XML (-oX <fichier>)

- Les résultats sont rapportés au format XML et peuvent être analysés par d'autres logiciels.
- Informations sur le formatage XML de Nmap :  
<http://insecure.org/nmap/data/nmap.dtd>

- Grepable (-oG <fichier> )

- Format (déprécié) simple qui répertorie chaque hôte sur une ligne et qui peut être facilement analysé par des scripts et d'autres logiciels (Par exemple les outils Linux : grep, sed, awk, et cut )

- Formats de sortie des résultats (suite)

- Exemple avec XML

- Utiliser l'option --webxml afin de retrouver la dernière version de la feuille de style afin de lire le .xml dans votre navigateur

Scan Summary																									
Nmap 7.93 was initiated at Tue Mar 28 10:24:36 2023 with these arguments: C:\Program Files(x86)\Nmap\nmap.exe -oX D:\testxml --webxml scanme.org Verbosity: 0; Debug level 0 Nmap done at Tue Mar 28 10:24:44 2023; 1 IP address (1 host up) scanned in 8.31 seconds																									
<b>45.33.32.156 / scanme.nmap.org / scanme.org</b>																									
<b>Address</b>																									
• 45.33.32.156 (ipv4)																									
<b>Hostnames</b>																									
• scanme.org (user) • scanme.nmap.org (PTR)																									
<b>Ports</b>																									
The 966 ports scanned but not shown below are in state: <b>filtered</b>																									
• 966 ports replied with: <b>no-response</b>																									
The 31 ports scanned but not shown below are in state: <b>closed</b>																									
• 31 ports replied with: <b>reset</b>																									
<table border="1"> <thead> <tr> <th>Port</th> <th>State (toggle closed [0]   filtered [0])</th> <th>Service</th> <th>Reason</th> <th>P</th> </tr> </thead> <tbody> <tr> <td>21</td> <td>tcp open</td> <td>ftp</td> <td>syn-ack</td> <td></td> </tr> <tr> <td>22</td> <td>tcp open</td> <td>ssh</td> <td>syn-ack</td> <td></td> </tr> <tr> <td>80</td> <td>tcp open</td> <td>http</td> <td>syn-ack</td> <td></td> </tr> </tbody> </table>						Port	State (toggle closed [0]   filtered [0])	Service	Reason	P	21	tcp open	ftp	syn-ack		22	tcp open	ssh	syn-ack		80	tcp open	http	syn-ack	
Port	State (toggle closed [0]   filtered [0])	Service	Reason	P																					
21	tcp open	ftp	syn-ack																						
22	tcp open	ssh	syn-ack																						
80	tcp open	http	syn-ack																						

- Formats de sortie des résultats (suite)

- Différents niveaux de verbosité -v et -vv

- Affichent des informations supplémentaires sur les temps de scan, les messages d'avertissement, les hôtes inactifs, la détection d'OS, ...
    - Utiliser plus de 2 « v » est généralement peu intéressant.

- Différent niveaux de débogage (-d[level])

- Il y a 9 niveaux de débogage dans Nmap.
      - Le débogage donne un aperçu détaillé de ce que Nmap fait pendant le scan.
    - L'option --packet-trace.
      - Affichera chaque paquet envoyé et reçu pendant le scan de Nmap, comme le ferait un sniffer.
    - L'option --log-errors
      - Permet d'enregistrer les erreurs rencontrées dans un fichier de log.

- Le moteur de scripts de Nmap

- Nmap Scripting Engine (NSE)

- Fourni une infrastructure flexible afin d'étendre les capacités de Nmap, offrir une façon simple de créer ses propres tests personnalisés et de rapporter les résultats avec la sortie normale de Nmap.

- Documentation : <https://nmap.org/book/nse.html#nse-intro>

- Les scripts NSE (extension .nse) sont organisés en 14 catégories.

- Exemples d'applications des scripts NSE

- Détection de version évoluée (catégorie version)
    - Détection de malware (catégories malware et backdoor)
    - Détection de vulnérabilités (catégorie vulnerability)
    - Découverte du réseau évoluée (catégorie discovery)

- Commandes

- Plusieurs syntaxes sont possibles.

```
$ nmap --script filename|category|directory|expression,... [cible]
# nmap -script Script1,script2 [cible]
```



- Exemples de scripts NSE

- Afficher les bannières envoyées par les services en écoute

```
nmap -sV --script=banner 192.168.0.1
```

- Effectuer une attaque par force brute

```
nmap --script=mysql-brute 192.168.0.1
```

- Découvrir des vulnérabilités

```
nmap -Pn -sV -p80 --script=vulners 192.168.0.1
|http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
```

- **Enumération des utilisateurs et des groupes**

- Consiste à trouver des comptes et groupes utilisateurs valides

- La création d'une liste des comptes utilisateurs valides permettra ensuite de tenter d'obtenir les mots de passe des comptes, par exemple via une attaque par force brute.

- **Enumération à l'aide de SMB**

- Si vous avez obtenu l'accès à un réseau interne, vous pouvez réaliser l'énumération des utilisateurs via le protocole SMB.
    - Vous pouvez également rechercher des partages SMB.

```
$ nmap --script smb-enum-users.nse <host>
$ nmap --script smb-enum-groups.nse -p445 <host>
$ nmap --script smb-enum-shares.nse -p445 <host>
```

- **Quelques autres options de balayage de ports**

- Pas d'indicateur SYN, RST ni ACK

- La cible (qui respecte la RFC 793) recevant un paquet ne contenant pas d'indicateur SYN, RST ou ACK renverra un RST si le port est fermé et aucune réponse si le port est ouvert (rapporté comme open|filtered).
    - Probablement certains périphériques vont répondre un RST dans tous les cas.

- **TCP Null scan (-sN)**

- Aucun drapeau (flag) n'est activé.

- **TCP FIN scan (-sF)**

- Seul le flag FIN est activé.

- **Xmas scan (-sX)**

- Les flags FIN, PSH, URG sont activés.

- **Avantages**

- Pourrait passer à travers des filtrages non stateful qui bloquent uniquement les SYN.
    - Un peu plus furtif qu'un SYN scan mais les IDPS modernes peuvent facilement les détecter.

Probe Response	Assigned State
No response received (even after retransmissions)	open filtered
TCP RST packet	closed
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

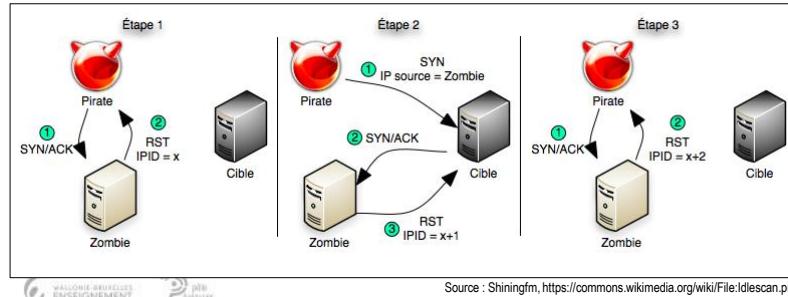
## Network scanning

- Quelques autres options de balayage de ports (suite)

- Idle scan

- Le champ « Identification » de l'en-tête IP (IP ID) peut être défini :

- Comme un compteur global (incrémenté d'une unité à chaque nouveau paquet),.
    - Comme un compteur local (compteurs distincts pour différentes destinations).
    - Comme la sortie d'un générateur de nombres pseudo-aléatoires.
    - Comme une constante (généralement de valeur nulle).



367

## Network scanning

- Idle scan (suite)

- Conditions

- Il faut trouver un « zombie » avec un port ouvert.
    - Il faut que les IP ID de ce voisin augmentent exactement de 1 à chaque envoi
      - » La plupart des systèmes modernes ont des IPID aléatoires et non incrémentaux.
    - Il faut qu'il y ait peu de trafic vers ce voisin, sinon l'IPID peut augmenter à cause d'autres requêtes.

- Le scanneur est-il indétectable?

- Non, il a fallu scanner la machine « zombie » pour trouver un port ouvert et celle-ci pourrait avoir logué nos scans.
    - Si le zombie est dans un autre réseau que le nôtre, les équipements du réseaux/fournisseurs d'accès pourraient avoir logué nos communications.

- Quelques autres options de balayage de ports (suite)

- TCP Window scan (-sW)

- Comme l'ACK scan, il envoie un paquet TCP avec le seul flag ACK. Nmap analyse la fenêtre TCP de la réponse pour déterminer si le port est ouvert ou fermé car certains systèmes utilisent une taille de fenêtre positive si le port est ouvert, et une taille de fenêtre nulle si le port est fermé.

- Gestion de Nmap

- Nmap doit être traité dans vos politiques et procédures (de sécurité)

- Respectez le principe du moindre privilège, le suivi des accès, l'établissement de rapports d'utilisation, ...
    - Qui peut utiliser Nmap?
    - Où/sur quel système Nmap doit-il être installé?
    - Nmap fait-il partie de votre dépôt de logiciels open source ?
    - ...

- Résultats des scans

- Doit-on sauvegarder les résultats ?
    - De manière chiffrées ou non ?
    - Combien de temps ces données doivent-elles être conservées ?
    - Quelle classification doit-on attribuer aux informations sur les résultats ?
    - ...

## Chapitre 10

# Pentesting Phases 3 à 7

Phase 3 : Threat Modeling (Modélisation des menaces)

- Threat Modeling

- Modélisation des menaces

- Son objectif consiste à comprendre quelles menaces et attaques pourraient être réalisées en profitant que quelles vulnérabilités

- Quelles sont les cibles qui pourraient intéresser les hackers?
- Quels types de hackers voudraient attaquer l'entreprise?
- Quelles menaces, si elles sont mises en œuvre, pourraient avoir un impact important ?
- Quels sont les points faible de telle application?
- Existe-t-il des angles mort aux caméras?
- ...

- Cette compréhension facilite la mise en œuvre de contre-mesures

- En tenant compte de la nature des actifs, des vecteurs d'attaque les plus probables et des actifs les plus recherchés par un attaquant.
- Outils, systèmes, contrôles et processus qui protègent et défendent l'entreprise.

- Exemple simple

- DB SQL → il existe attaque pas injection SQL → Web application Firewall

- Étapes d'un processus de modélisation des menaces

- Différentes structures, modèles et méthodologies existent

- Elles peuvent être centrée sur les actifs, sur les attaquants, sur les logiciels, sur la valeur et les parties prenantes ou hybride.
- STRIDE, DREAD, PASTA, VAST, Trike, ...

- Exemple : STRIDE

- Analyser les menaces potentielles suivant 6 catégories de menaces :
- **S**poofing (Usurpation d'identité)
- **T**ampering (Altération de données)
- **R**eputation (Réputation)
- **I**nformation disclosure (Divulgation d'informations)
- **D**enial of service (Déni de service)
- **E**levation of privilege (Élévation de priviléges)

- **Étapes d'un processus de modélisation des menaces**

- On y trouve généralement ces 5 étapes :

- **Définition de la portée**
      - Qu'est-ce qui est impliqué (applications, données, services, partenaires, processus, ...).
      - Comprendre ses systèmes et les flux de données.
    - **Identification des menaces**
      - Qu'est-ce qui peut mal tourner ? (scénarios d'attaque probables).
      - Identifier les menaces potentielles (par exemple, qui relèvent de chacune des six catégories de STRIDE) et les documenter.
    - **Évaluation des risques**
      - Évaluer l'impact et la probabilité d'occurrence de chaque menace, puis attribuer un niveau de risque basé sur une échelle pré définie (hiérarchiser les risques).
      - Déterminer les objectifs et les exigences de sécurité que vous souhaitez atteindre pour chaque menace.
    - **Prévention/mitigation**
      - Mise en œuvre de contrôles et protection contre les menaces afin d'atteindre ces objectifs.
    - **Validation/remédiation**
      - Tester et valider les contrôles de sécurité et les contre-mesures mis en place pour vérifier leur efficacité et leur efficience.
      - Réviser et améliorer le processus.

- **Modélisation des menaces et pentest**

- PTES

- PTES n'utilise pas de modèle spécifique de modélisation des menaces.
    - La norme se concentre sur deux éléments clés de la modélisation des menaces :
      - Les actifs (quels actifs sont plus importants que d'autres ?).
      - L'attaquant (quelles communautés de menaces sont plus pertinentes que d'autres ?).

- **Avantages de la modélisation des menaces pour le pentest**

- **Elle permet de déterminer quelles sont les cibles réelles au sein de l'organisation**
      - Ainsi, les contrôles, les processus et l'infrastructure les plus pertinents seront mis à l'épreuve plutôt que de suivre une liste généraliste d'éléments informatiques.
    - **Elle permet que le pentest imite étroitement les outils, les techniques, les capacités et l'accessibilité de l'attaquant**

- **Les actifs**

- **Le pentester doit**

- Identifier les actifs les plus susceptibles d'être ciblés.
    - Déterminer quelle est leur valeur et quel serait l'impact de leur perte (totale ou partielle).

- **Comment déterminer les actifs importants?**

- **En analyser la documentation**

- Les politiques, plans et procédures internes peuvent aider à identifier les rôles clés et les processus commerciaux critiques.

- **En interrogeant le personnel concerné**

- Direction, responsable informatique, ...

- **Les actifs**

- **Exemple d'actifs**

- Secrets commerciaux, données de R&D, brevets, propriété intellectuelle.
      - Informations financières (comptes bancaires, cartes de crédit, marketing).
      - Codes sources des programmes, configuration des systèmes, informations d'identification (compte admin).
      - Données des employés et des clients (Amendes RGPD, phishing).
        - Numéros d'identification nationaux, Informations personnelles identifiables (PII)
        - Informations de santé protégées (PHI), ...
      - Le personnel.
        - Personnes qui pourraient être exploitées pour divulguer des informations ou prendre des actions qui pourraient nuire à l'organisation (Direction générale, assistants de direction, ingénieurs, techniciens, ...).
      - Infrastructure informatique, chaîne de production, ...

- **Les menaces**

- **Acteurs de la menace**

- Identifier quels sont les acteurs de menaces (cybercriminels, hacktivistes, ...).
    - Déterminer si la menace est interne (dirigeants, développeurs, employés, ...) ou externe à l'organisation (sous-traitants, fournisseurs, ...) ou les deux.

- **Capacités de la menace**

- Une fois qu'une communauté de menace a été identifiée, ses capacités d'action doivent être analysées.
      - Capacité à obtenir ou à développer des exploits pour l'environnement de l'organisation, utilisation de sites de dépôt, utilisation de botnets, ...
        - » Des hackers sponsorisés par un état ont plus de moyens et de connaissances qu'un script kiddies.

- **Accessibilité à l'organisation**

- Avec quelle facilité l'acteur de menace peut-il accéder aux actifs ?
      - Par exemple, l'actif est-il interne ou exposé à Internet?

- **MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge)**

- **C'est une base de connaissances**

- Elle organise et catégorise divers types de tactiques, techniques et procédures (TTP) utilisées par les acteurs de la menace.
      - **Tactique** : Ce qu'ils essaient de faire (par ex. de la reconnaissance).
      - **Technique** : Comment y parvenir? (par exemple via un scan de ports)
      - **Procédure** : détaille la mise en œuvre de la technique.

- **Elle peut aider à**

- Simuler avec précision des cyberattaques pour tester les cybersécurités.
    - Choisir et configurer les technologies de sécurité pour mieux détecter, éviter et atténuer les cybermenaces.
    - Offrir un langage commun à utiliser pour partager des informations sur les cybermenaces et collaborer à la prévention des menaces.

**HEH.be** Sciences et technologies

## Threat Modeling

– La matrice MITRE ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾

Enterprise  
Mobile  
ICS

### ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs
	Compromise Accounts (3)	Exploit Public-		Boot or Logon Autostart

Source : <https://attack.mitre.org/>

381

**HEH.be** Sciences et technologies

### Phase 4 : Vulnerability Analysis (Analyse des vulnérabilités)

382

- Identifier des vulnérabilités exploitables

- Analyse des informations récoltées dans la phase de collecte pour identifier des vulnérabilités
  - En mettant en corrélation les numéros de version des OS ou des applications avec les vulnérabilités connues (VCE).
  - En analysant le code source de programmes (white box).
  - En analysant les métadonnées de fichiers récoltés.
  - En analysant les fichiers de configuration.
  - En réalisant de l'ingénierie inverse (reverse engineering).
  - En utilisant des scanners de vulnérabilité sur les systèmes découverts.
  - ...
- S'assurer qu'il n'y a pas de doublon
  - Différents outils peuvent mettre en évidence la même vulnérabilité → ne pas la comptabiliser deux fois au risque de créer un faux profil de risque accru.

- Vérifier l'exactitude des vulnérabilités

- Recherche d'informations
  - Lisez la documentation associée à chaque vulnérabilité (CVE) pour comprendre la nature de la vulnérabilité, les conditions requises pour l'exploiter, et les scénarios d'attaque potentiels.
- Cross-validation
  - Comparez les résultats avec d'autres scanners ou avec un outil différent.
- Test manuel
  - Essayez de reproduire manuellement la vulnérabilité sur le système affecté.
    - Par exemple, si le scanner indique une vulnérabilité SQL injection, essayez d'injecter des commandes SQL pour voir si vous pouvez obtenir des résultats inattendus.

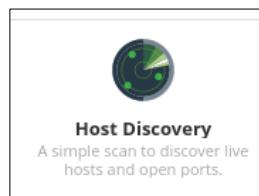
- **Lister les attaques possibles**

– Toutes ces informations vont permettre la création d'une liste d'attaques possibles dont certaines seront mises en application lors de la phase d'exploitation.

- Phishing.
- Tailgating.
- Brute force.
- Keylogger.
- Buffer overflow
- Evil twin.
- Injection SQL.
- DoS.
- Badge cloning.
- ...

## Configuration de Nessus

### Host Discovery Scan



**HEH.be Sciences et technologies**

## Host Discovery Template

- Découverte d'hôtes
  - Scan
    - Avant de pouvoir créer votre premier scan, vous devez attendre la fin de la compilation des plugins.
  - Scan template
    - Lorsque vous créez une analyse (New scan) ou une politique (Policies) pour la première fois, la section *scan template* apparaît.

387

**HEH.be Sciences et technologies**

## Host Discovery Template

- Découverte d'hôtes (suite)
  - Affichage des modèles (*scan templates*)

**Trois types de modèles**

- Discovery
- Vulnérabilités
- Compliance

Certains ne sont pas disponibles dans la version « Essentials » de Nessus

388

**HEH.be Sciences et technologies**

## Host Discovery Template

- Découverte d'hôtes (suite)

New Scan / Host Discovery

Back to Scan Templates

Settings Plugins

BASIC

- General (highlighted)
- Schedule
- Notifications

DISCOVERY

REPORT

ADVANCED

Name: Host-Discovering

Description:

Folder: My Scans

Targets: 192.168.0.0/24

Upload Targets Add File

Save or launch

Save Cancel

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle de l'enseignement

389

**HEH.be Sciences et technologies**

## Host Discovery Template

- Programmation des scans
  - Choisir des horaires pendant lesquels le réseau/hôtes ne sont pas déjà surchargés.

BASIC

- General
- Schedule (highlighted)
- Notifications

DISCOVERY

REPORT

ADVANCED

Enabled:

NOTE: Only one schedule can be enabled. Any other scheduled scans will be disabled. Upgrade to Nessus Professional

Frequency: Once

Starts: 14:00 2023-10-09

Timezone: Europe/Brussels

Summary: Once on Monday, October 9th, 2023 at 2:00 PM

Once

Daily

Weekly

Monthly

Yearly

Save Cancel

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle de l'enseignement

390

**HEH.be Sciences et technologies**

## Host Discovery Template

- Notification des scans
  - Un serveur SMTP doit être configuré

Filtres les informations notifiées par mail

391

**HEH.be Sciences et technologies**

## Host Discovery Template

- Configuration du serveur SMTP

392

**HEH.be Sciences et technologies**

## Host Discovery Template

- Discovery

Settings Plugins

BASIC

**DISCOVERY**

REPORT ADVANCED

Scan Type: Host enumeration

General Settings:

Always test the local Nessus host

Use fast network discovery

Ping hosts using:

TCP  
ARP  
ICMP (2 retries)

Host enumeration  
Host enumeration  
OS Identification  
Port scan (common ports)  
Port scan (all ports)  
**Custom**

Si désactivé, Nessus tente d'éviter les faux positifs en effectuant des tests supplémentaires pour vérifier que la réponse ne provient pas d'un proxy ou d'un équilibreur de charge.

WALLONIE-BRUXELLES ENSEIGNEMENT

393

**HEH.be Sciences et technologies**

## Host Discovery Template

- Host Discovery

BASIC

**DISCOVERY**

Host Discovery

Port Scanning

REPORT ADVANCED

Remote Host Ping

Ping the remote host

General Settings

Test the local Nessus host

Use fast network discovery

Ping Methods

ARP → Ne fonctionne que sur le réseau local

TCP

Destination ports: **built-in**

ICMP

Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries: 2

UDP

TCP built-in ports	
139	1029
135	79
445	497
80	548
22	5000
515	1917
23	53
21	161
6000	9001
1025	49000
25	443
111	993
1028	8080
9100	2869

394

**HEH.be** Sciences et technologies

## Host Discovery Template

- Port scanning

**BASIC**

**DISCOVERY**

- Host Discovery
- Port Scanning**
- REPORT
- ADVANCED

**Ports**

Consider unscanned ports as closed  
Port scan range: default

**Network Port Scanners**

TCP → Full TCP 3-way handshake  
 Override automatic firewall detection  
 Use soft detection  
 Use aggressive detection  
 Disable detection

SYN → TCP SYN scan  
 Override automatic firewall detection  
 Use soft detection  
 Use aggressive detection  
 Disable detection

UDP  
Due to the nature of the protocol, it is generally not possible for a port scanner to use the netstat or SNMP port enumeration options instead if possible.

• • • 395

**HEH.be** Sciences et technologies

## Host Discovery Template

- Host Discovery (suite)
  - Fragile devices

- Le balayage des ports est connu pour provoquer le dysfonctionnement de certains dispositifs dit « fragiles ».
- Par exemple, le balayage des ports d'une imprimante peut causer l'impression d'une grande quantité d'informations (probablement dénuée de sens) provenant de chaque port au fur et à mesure du balayage.

**Fragile Devices**

Scan Network Printers  
 Scan Novell Netware hosts  
 Scan Operational Technology devices

**Wake-on-LAN**

List of MAC addresses

Boot time wait (in minutes)

Indique à quelles adresses envoyer un paquet magique afin d'allumer le périphérique.

• • • 396

## Host Discovery Template

- Report

The screenshot shows the 'Output' section of the 'REPORT' settings. It includes three checkboxes:

- Allow users to edit scan results
- Designate hosts by their DNS name
- Display hosts that respond to ping
- Display unreachable hosts
- Display Unicode characters

A warning at the bottom states: "WARNING: This feature may cause issues with some..."

Permet de supprimer des éléments du rapport. Doit être désactivé en cas de scan de conformité.

Les hôtes qui n'ont pas répondu à la requête ping sont inclus dans le rapport de sécurité en tant qu'hôtes morts. A ne pas activer pour de larges étendues d'IP à scanner.

Les caractères Unicode apparaissent dans la sortie du plugin

- Par exemple, les noms d'utilisateur et les noms des applications installées.

## Host Discovery Template

- Advanced

The screenshot shows the 'ADVANCED' section with the following configuration:

- Performance Options:
  - Slow down the scan when network congestion is detected
  - Network timeout (in seconds): 5
  - Max simultaneous checks per host: 5
  - Max simultaneous hosts per scan: 256
  - Max number of concurrent TCP sessions per host: [empty]
  - Max number of concurrent TCP sessions per scan: [empty]
- Unix find command Options:
  - Exclude Filepath: Add File (Filepaths to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.)
  - Exclude Filesystem: Add File (Filesystems to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -fs-type argument.)
  - Include Filepath: Add File (Filepaths to include from any use of the find on Unix systems. One entry per line.)

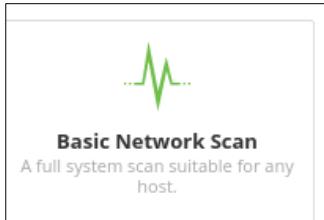
### Windows file search Options

Windows Exclude Filepath	Add File
	Filepaths to exclude from the thorough test
Windows Include Filepath	Add File
	Filepaths to include from the thorough test

**HEH.be**  
Sciences  
et technologies

## Configuration de Nessus

### Vulnerabilities Scan



Basic Network Scan  
A full system scan suitable for any host.

WALLONIE-BRUXELLES  
ENSEIGNEMENT

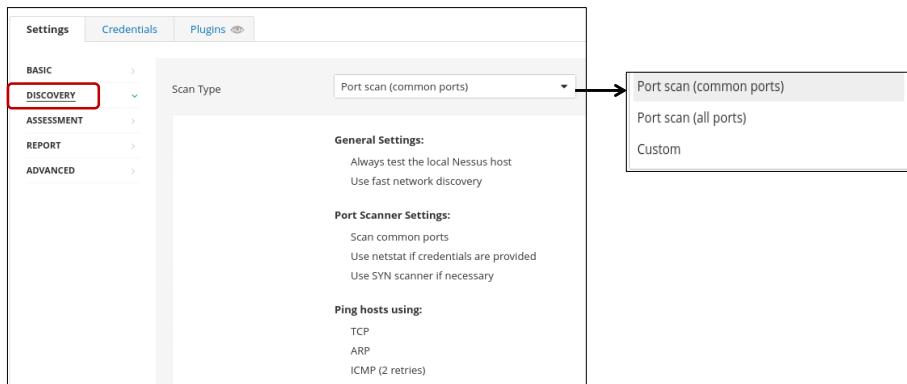
WIL

399

**HEH.be**  
Sciences  
et technologies

### Basic Network Scan Template

- Scan de vulnérabilités (Onglet « Settings »)
  - Basic Network Scan > Discovery
    - Effectue un scan de vulnérabilités avec « tous » les plugins de Nessus activés.



Settings    Credentials    Plugins

BASIC >  
**DISCOVERY** >  
ASSESSMENT >  
REPORT >  
ADVANCED >

Scan Type: Port scan (common ports)

General Settings:  
Always test the local Nessus host  
Use fast network discovery

Port Scanner Settings:  
Scan common ports  
Use netstat if credentials are provided  
Use SYN scanner if necessary

Ping hosts using:  
TCP  
ARP  
ICMP (2 retries)

WALLONIE-BRUXELLES  
ENSEIGNEMENT

WIL

400

**HEHbe Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment

Permet de configurer la manière dont une analyse identifie les vulnérabilités

Scan Type Custom

Scan Type Custom

Default

Scan for known web vulnerabilities

Scan for all web vulnerabilities (quick)

Scan for all web vulnerabilities (complex)

Custom

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

- General
- Brute Force
- Web Applications
- Windows
- Databases

REPORT

ADVANCED

Accuracy

- Override normal accuracy
- Avoid potential false alarms
- Show potential false alarms
- Perform thorough tests (may disrupt your network or impact scan speed)

Effectue des tests approfondis (par ex. un plugin peut analyser plusieurs niveaux de répertoire SMB au lieu d'un seul)  
Plus intrusif, meilleurs résultats mais peut perturber le réseau.

Si l'option Report Paranoïa est réglée sur Show potential false alarms, une faille est signalée à chaque fois, même s'il y a un doute sur le fait que l'hôte distant soit affecté.

Avoid potential false alarms indique à Nessus de ne signaler aucune faille s'il y a un soupçon d'incertitude que l'hôte soit affecté.

• • • 401

**HEHbe Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment (suite)

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

- General
- Brute Force
- Web Applications
- Windows
- Databases

General Settings

Only use credentials provided by the user

Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.

Oracle Database

Test default accounts (slow)

Hydra

Des options pour utiliser Hydra sont disponibles si celui-ci est installé sur la même machine que Nessus

• • • 402

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment (suite)

Lors du scan, Nessus se fait passer pour ce navigateur

URL de la première page testée par Nessus.  
Syntaxe pour tester plusieurs page /:mypage:/test

Nombre de liens que Nessus suit pour chaque page de démarrage.

Nessus suit les liens dynamiques et peut dépasser la limite Max depth.

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network > Assessment (suite)

Application Test Settings

- Enable generic web application tests
- Abort web application tests if HTTP login fails → ne fait aucun test s'il n'arrive pas à se loguer.
- Try all HTTP methods → Utilise des requêtes POST, pas seulement GET
- Attempt HTTP Parameter Pollution
- Test embedded web servers
- Test more than one parameter at a time per form
  - Test random pairs of parameters
  - Test all pairs of parameters (slow)
  - Test random combinations of three or more parameters (slower)
  - Test all combinations of parameters (slowest)
- Do not stop after the first flaw is found per web page
  - Stop after one flaw is found per web server (fastest)
  - Stop after one flaw is found per parameter (slow)
  - Look for all flaws (slowest)

URL for Remote File Inclusion: http://rfi.nessus.org/rfi.txt  
If the target(s) being scanned cannot reach the Internet, the default URL can be replaced by an internally hosted file. The file must contain PHP source code that displays "NessusCodeExecTest" when executed.

Maximum run time (minutes): 5

### – Basic Network Scan > Assessment (suite)

- **Attempt HTTP Parameter Pollution**
  - Essaye de contourner les mécanismes de filtrage en injectant du contenu dans une variable tout en fournissant à cette même variable un contenu valide.
- **Test embedded web servers**
  - Les serveurs web intégrés sont souvent statiques et ne contiennent pas de scripts CGI personnalisables.
  - Ils peuvent avoir tendance à se bloquer ou à ne plus répondre lorsqu'ils sont analysés.
  - Tenable recommande d'analyser les serveurs Web intégrés séparément des autres serveurs Web.
- **Test more than one parameter at a time per form**
  - Par défaut, un paramètre est testé à la fois.
  - Cette option permet de tester plusieurs paramètres ainsi que de gérer la combinaison des valeurs des arguments utilisés dans les requêtes HTTP.

### – Basic Network Scan (suite)

- **Do not stop after first flaw is found per web page**
  - Si cette option est désactivée, dès qu'une faille est trouvée sur une page web, l'analyse passe à la page web suivante.
- **URL for Remote File Inclusion (RFI)**
  - Certaines applications web incluent dynamiquement des fichiers ou des scripts externes.
  - Une attaque RFI est possible lorsqu'une application reçoit un chemin d'accès à un fichier en entrée d'une page web et qu'elle ne l'analyse pas correctement. Cela permet à une URL externe d'être fournie à la fonction d'inclusion.

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment (suite)

The screenshot shows the Nessus configuration interface under the 'ASSESSMENT' tab. In the 'General' section, there is a checkbox labeled 'Request information about the SMB Domain'. In the 'User Enumeration Methods' section, three checkboxes are checked: 'SAM Registry', 'ADSI Query', and 'WMI Query'. A red box highlights the 'RID Brute Forcing' button, which is currently set to 'OFF'. Arrows point from the text descriptions to the respective configuration items.

Nessus interroge les utilisateurs du domaine au lieu des utilisateurs locaux.

Tente d'enumérer les comptes d'utilisateurs  
Risque de bloquer les comptes utilisateurs.

**Remarque :** Il existe des solutions spécifiques pour découvrir les vulnérabilités et les mauvaises configurations Active Directory, par exemple *Tenable Identity Exposure*.

• • • 407

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan (suite)

The screenshot shows the Nessus configuration interface under the 'ASSESSMENT' tab. In the 'Databases' section, there is a checkbox labeled 'Use detected SIDs'. A note below it states: 'If host and database credentials are specified, Nessus will attempt to authenticate to the database with SIDs detected locally.' A red box highlights the 'Use detected SIDs' checkbox.

- **Nécessite d'avoir configuré des identifiants d'hôte et Oracle.**
  - Le scanner s'authentifie auprès des cibles, puis tente de détecter localement les identifiants de système Oracle (SID).
  - L'analyseur tente ensuite de s'authentifier à l'aide des informations d'identification de la base de données Oracle et des SID détectés.

• • • 408

## Basic Network Scan Template

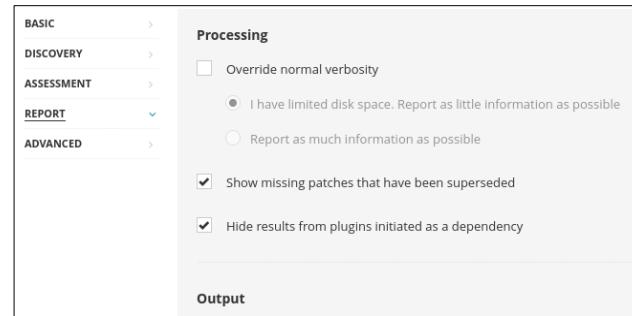
### – Basic Network Scan > Report

- **Superseeded patch**

- Un correctif remplacé est un correctif qu'il n'est pas nécessaire d'installer parce qu'un correctif ultérieur est disponible et corrige la même vulnérabilité.

- **Plugin dependency**

- Les plugins dépendent souvent des résultats d'autres plugins pour exécuter leurs fonctions.
- Ne pas mentionner les plugins utilisés rend le rapport plus lisible.



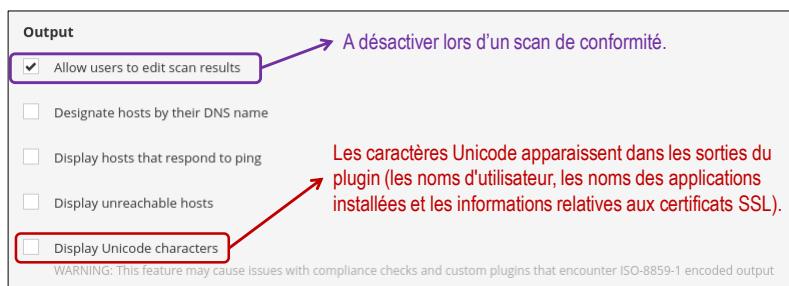
The screenshot shows the 'Processing' tab under the 'REPORT' section of the NetworkMiner interface. It includes the following settings:

- Override normal verbosity
- I have limited disk space. Report as little information as possible
- Report as much information as possible
- Show missing patches that have been superseded
- Hide results from plugins initiated as a dependency

At the bottom right of the window, there are three red dots and the number 409.

## Basic Network Scan Template

### – Basic Network Scan > Report (suite)



The screenshot shows the 'Output' tab under the 'REPORT' section of the NetworkMiner interface. It includes the following settings:

- Allow users to edit scan results
- Designate hosts by their DNS name
- Display hosts that respond to ping
- Display unreachable hosts
- Display Unicode characters

A purple arrow points to the first checkbox with the text: "A désactiver lors d'un scan de conformité." (Disable during a compliance scan).

A red arrow points to the last checkbox with the text: "Les caractères Unicode apparaissent dans les sorties du plugin (les noms d'utilisateur, les noms des applications installées et les informations relatives aux certificats SSL)." (Unicode characters appear in plugin outputs (user names, application names installed and SSL certificate information)).

Below the checkboxes, a warning message reads: "WARNING: This feature may cause issues with compliance checks and custom plugins that encounter ISO-8859-1 encoded output."

At the bottom right of the window, there are three red dots and the number 410.

**HEHbe** Sciences et technologies

## Basic Network Scan Template

– Basic Network Scan > Advanced

**BASIC**

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

General

**General Settings**

Enable safe checks

Stop scanning hosts that become unresponsive during the scan

Scan IP addresses in a random order

Automatically accept detected SSH disclaimer prompts  
This will automatically attempt to agree to prompts in SSH connections that Tenable products are configured to recognize.

Scan targets with multiple domain names in parallel

Create unique identifier on hosts scanned using credentials

Trusted CAs

CA certificates listed here will be considered as trusted CAs by the scan

• • • 411

**HEHbe** Sciences et technologies

## Basic Network Scan Template

– Basic Network Scan > Advanced (suite)

- **Enable Safe Checks**
  - Lorsque cette option est activée, elle désactive tous les plugins susceptibles d'avoir un effet néfaste sur l'hôte distant.
- **Stop scanning hosts that become unresponsive during the scan**
  - Un hôte pourrait ne plus répondre suite à l'utilisation d'un plugin DoS, parce qu'un système de protection bloque le scan ou juste parce qu'un utilisateur a éteint son PC.
- **Scan IP addresses in a random order**
  - Peut être utile pour répartir le trafic réseau lors du scan d'une grande étendue d'IP.
- **Automatically accept detected SSH disclaimer**
  - S'il est désactivé et que la cible présente un disclaimer, celui-ci ne sera pas accepté et le scan accrédié ssh login fail
- **Scan targets with multiple domain names in parallel**
  - Désactivé, pour empêcher de submerger un hôte par plusieurs scans simultanés lorsque plusieurs noms renvoient vers une même adresse IP.
- **Trusted CA**
  - Liste des autorités de certification reconnues par Nessus.

• • • 412

**HEHbe** Sciences et technologies Basic Network Scan Template

– Basic Network Scan > Advanced (suite)

**Performance Options**

- Slow down the scan when network congestion is detected
- Network timeout (in seconds): 5
- Max simultaneous checks per host: 5
- Max simultaneous hosts per scan: 30
- Max number of concurrent TCP sessions per host: [ ]
- Max number of concurrent TCP sessions per scan: [ ]

**Unix find command Options**

Exclude Filepath	Add File
Filepaths to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.	
Exclude Filesystem	Add File
Filesystems to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.	
Include Filepath	Add File
Filepaths to include from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.	

**Windows file search Options**

Windows Exclude Filepath	Add File
Filepaths to exclude from any use of search on Windows systems excludes which include \Windows\WinSxS and \Windows\servic	
Windows Include Filepath	Add File
Filepaths to include from any use of Recursive search on Windows hosts tests are enabled. Use of this setting will replace the de	

• • • 413

**HEHbe** Sciences et technologies Basic Network Scan Template

– Basic Network Scan > Advanced (suite)

**Debug Settings**

- Log scan details  
Logs the start and finish time for each plugin used during a scan to nessusd.messages.
- Always report SSH commands  
Attaches all SSH commands run on target hosts irrespective of debug settings.
- Enable plugin debugging  
Attaches available debug logs from plugins to the vulnerability output of this scan.

Debug Log Level: Level 1: Basic Debugging

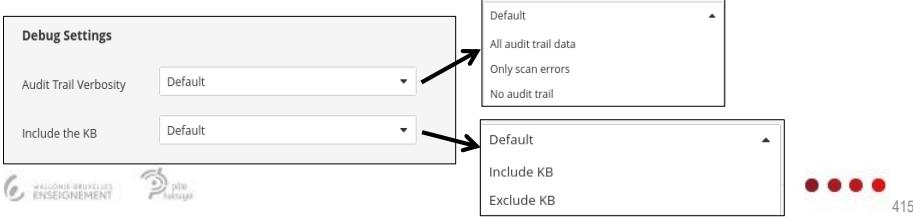
Level 1: Basic Debugging  
Level 1: Basic Debugging  
Level 2: Advanced Debugging  
Level 3: Full Debugging  
Level 4: Unrestricted Debugging

• • • 414

## Basic Network Scan Template

### – Basic Network Scan > Advanced (suite)

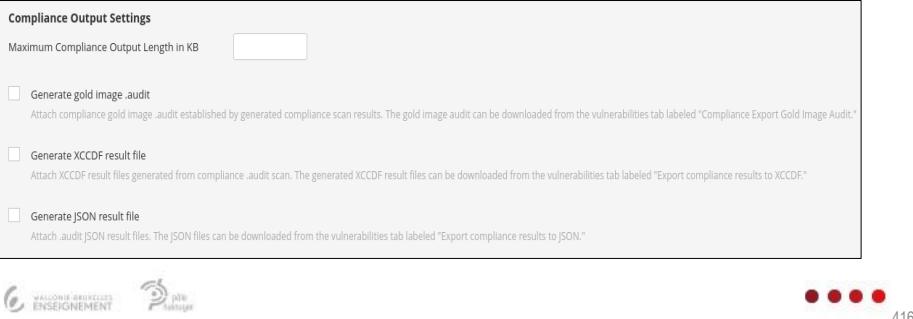
- **Audit trail**
  - Fonction qui renseigne pourquoi un plugin a eu tel comportement
  - Par exemple, pourquoi il ne renvoie pas de résultat, bien qu'il soit en cours d'exécution.
- **Include the KB**
  - Une base de connaissances (KB : Knowledge Base) est créée pour chaque cible au cours d'un scan Nessus.
  - Lorsqu'un plugin collecte des informations qui doivent être "partagées" avec d'autres plugins, elles sont stockées dans la base de connaissances de cet hôte.
  - Fournit plus de données de débogage en incluant les données de la KB dans les résultats du scan.



## Basic Network Scan Template

### – Basic Network Scan > Advanced (suite)

- Contrôle la longueur maximale de chaque contrôle de conformité individuel renvoyée par la cible.
- Permet de choisir les plugins à utiliser pour formater les résultats de scan conformité dans des formats de données que d'autres outils (Tenable et tiers) peuvent utiliser.





Sciences  
et technologies

## Basic Network Scan Template

### • Onglet « Plugins »

		PLUGIN NAME	PLUGIN ID
CGI abuses : XSS	703		
CISCO	2322	Debian DLA-100-1 : mutt security update	82084
Databases	944	Debian DLA-1000-1 : imagemagick security update	101031
Debian Local Security Checks	9020	Debian DLA-1001-1 : exim4 security update (Stack Clash)	101032
Default Unix Accounts	172	Debian DLA-1002-1 : smb4k security update	101033
Denial of Service	110	Debian DLA-1003-1 : unrar-nonfree security update	101065
DNS	231	Debian DLA-1004-1 : drupal7 security update	101092
FS Networks Local Security Checks	1294	Debian DLA-1005-1 : mercurial security update	101121
Fedora Local Security Checks	17687	Debian DLA-1006-1 : libarchive security update	101173
Firewalls	400	Debian DLA-1007-1 : icedove/thunderbird security update	101208
FreeBSD Local Security Checks	5382	Debian DLA-1008-1 : libxml2 security update	101174
FTP	271	Debian DLA-1009-1 : apache2 security update	101175
Gain a shell remotely	282	Debian DLA-1011-1 : jasper security update	82085
General	354	Debian DLA-1010-1 : vorbis-tools security update	101209
Gentoo Local Security Checks	3441	Debian DLA-1011-1 : sudo security update	101210



417



Sciences  
et technologies

## Basic Network Scan Template

### – Basic Network Scan > Advanced (suite)

#### Debug Settings

Log scan details  
Logs the start and finish time for each plugin used during a scan to nessusd.messages.

Always report SSH commands  
Attaches all SSH commands run on target hosts irrespective of debug settings.

Enable plugin debugging  
Attaches available debug logs from plugins to the vulnerability output of this scan.

Debug Log Level

Enumerate launched plugins  
Adds a list of plugins that were launched during the scan.

Audit Trail Verbosity

Include the KB



418

**HEHbe Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport

My Scans

Import New Folder + New Scan

Search Scans 4 Scans

Name	Schedule	Last Scanned
test	On Demand	✓ October 6 at 9:05 AM

test

Back to My Scans

Hosts 1 Vulnerabilities 1 Remediations 1 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.1	22 13 42

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0

419

**HEHbe Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport (suite)

Filter ▾ Search Vulnerabilities 34 Vulnerabilities

Sev	CVSS	VPR	Nam... Family	Count	⋮
Mixed	...	...	QMisc.	30	ⓘ
Mixed	...	...	IEGeneral	2	ⓘ
Mixed	...	...	MWindows	2	ⓘ
Mixed	...	...	SSGeneral	9	ⓘ
Mixed	...	...	TLService detection	4	ⓘ
Mixed	...	...	SMisc.	2	ⓘ
Info	...	...	HWeb Servers	10	ⓘ
Info	...	...	SWindows	10	ⓘ
Info	...	...	SWindows : User management	2	ⓘ

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: October 6 at 9:16 AM  
End: October 6 at 9:41 AM  
Elapsed: 24 minutes

Vulnerabilities

420

**HEH.be Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport (suite)

The screenshot shows a 'Filters' dialog box with a dropdown menu set to 'All' and a condition 'Severity is equal to Critical'. Below it is a 'Vulnerabilities' report card showing one critical vulnerability (CVSS 9.8) from host 192.16. A navigation bar at the bottom includes icons for 'Back to My Scans', 'Hosts', 'Vulnerabilities', 'Remediations', 'History', 'Configure', 'Audit trail', 'Launch', 'Report' (which is highlighted with a red box), and 'Import'.

**Vulnerabilities**

Severity	CVSS	VPR	Name Family	Count
Critical	9.8	Q...	Misc.	2

Host: 192.16 | CVSS: 9.8 | Q... | Misc.: 2

421

**HEH.be Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport (suite)

The screenshot shows a 'Report' section with a red box around the 'Report' button in the top right. Below it is a 'Generate Report - 1 Host Selected' dialog. The 'Report Format' is set to 'HTML'. Under 'Select a Report Template', there are several options: 'Complete List of Vulnerabilities by Host' (selected), 'Detailed Vulnerabilities By Host', 'Detailed Vulnerabilities By Plugin', and 'Vulnerability Operations'. A 'Template Description' box states: 'This report provides a summary list of vulnerabilities for each host detected in the scan.' At the bottom of the dialog, a red box highlights the 'Filters Applied' section which says 'Severity is equal to Critical'. Navigation icons at the bottom include 'Back to My Scans', 'Hosts', 'Vulnerabilities', 'Remediations', 'History', 'Configure', 'Audit trail', 'Launch', 'Report' (highlighted with a red box), and 'Import'.

Host: 192.16 | CVSS: 9.8 | Q... | Misc.: 2

Scan Details

Policy: Basic Network Scan  
Status: Compiled  
Severity Base: CVSS v3.0

Generate Report - 1 Host Selected

Report Format:  HTML  CSV

Select a Report Template:

Complete List of Vulnerabilities by Host (Selected)  
Detailed Vulnerabilities By Host  
Detailed Vulnerabilities By Plugin  
Vulnerability Operations

Template Description:

This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:  
Severity is equal to Critical

422

**HEH.be**  
Sciences  
et technologies

## Configuration de Nessus

### Advanced Scan template

**Advanced Scan**  
Configure a scan without using any recommendations.

WALLONIE-BRUXELLES  
ENSEIGNEMENT

423

**HEH.be**  
Sciences  
et technologies

### Advanced Scan template

Les onglets, host discovery et port scanning sont les mêmes que pour un « basic network scan »

Settings    Credentials    Plugins

BASIC  
DISCOVERY  
\* Host Discovery  
Port Scanning  
Service Discovery

Identity  
ASSESSMENT  
REPORT  
ADVANCED

Remote Host Ping  
Ping the remote host

General Settings  
 Test the local Nessus host  
 Use fast network discovery

Ping Methods  
 ARP  
 TCP  
 ICMP  
 UDP

Destination ports: built-in  
 Assume ICMP unreachable from the gateway means the host is down  
 Maximum number of retries: 2

WALLONIE-BRUXELLES  
ENSEIGNEMENT

424

**HEH.be Sciences et technologies**

## Advanced Scan template

- Setting > discovery > Service Discovery

**BASIC**

**DISCOVERY**

- Host Discovery
- Port Scanning
- Service Discovery**
- Identity

**ASSESSMENT**

**REPORT**

**ADVANCED**

**General Settings**

Probe all ports to find services

Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.

Search for SSL/TLS/DTLS Services

Search for SSL/TLS on

Search for DTLS on

Identify certificates expiring within x days

Enumerate all SSL/TLS ciphers

When selected, Nessus ignores the list of ciphers advertised by SSL/TLS services, and enumerates them by attempting to establish connections using all possible ciphers.

Enable CRL checking (connects to the Internet)

• • • 425

**HEH.be Sciences et technologies**

## Advanced Scan template

- Setting > Discovery > Identity
- Collect Identity Data from Active Directory

- Permettre à Nessus de collecter des objets d'utilisateur, d'ordinateur et de groupe dans l'Active Directory.
- Nécessite d'avoir configuré les identifiants pour l'accès à l'AD.

**General Settings**

Collect Identity Data from Active Directory

Checking this box will enable collection of identity information from Active Directory using Domain User credentials.

• • • 426

## Advanced Scan template

- Setting > Discovery > Assessment > General

Voir « Basic Network Scan »

Par défaut, Nessus considère que les signatures sont périmées, quel que soit le temps écoulé depuis la mise à jour. Vous pouvez autoriser une période de grâce jusqu'à 7 jours avant de signaler qu'une signature est périmée.

Nessus tente d'envoyer du spam à l'adresse indiquée.

• • • 427

## Advanced Scan template

- Setting > Discovery > Assessment > Malware

Par défaut, Nessus utilise le cloud pour comparer les résultats du scan avec des malwares connus

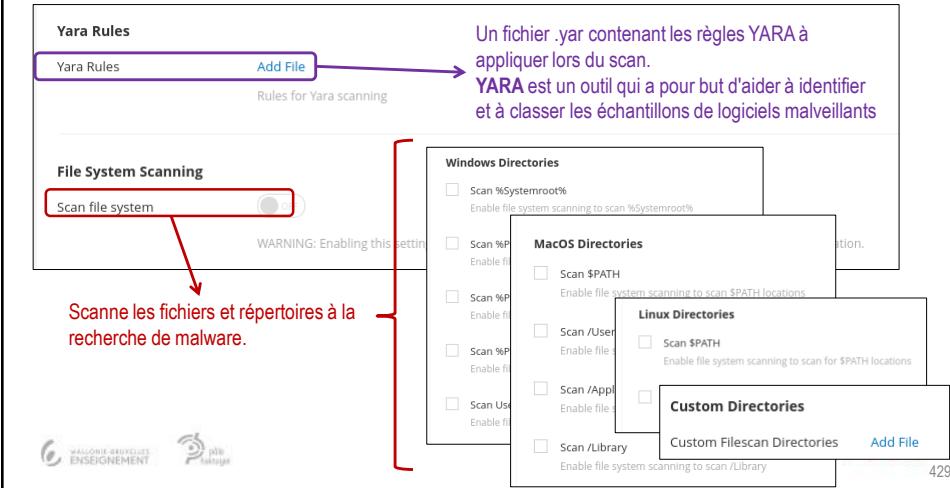
Fournir un fichier texte contenant une liste d'adresses IP connues comme étant malicieuses que vous souhaitez détecter.

Liste d'IP et de noms d'hôtes que Nessus ignorera pendant le scan.

• • • 428

## Advanced Scan template

- Setting > Discovery > Assessment > Malware (suite)



**Yara Rules**

Add File → Un fichier .yar contenant les règles YARA à appliquer lors du scan.  
**YARA** est un outil qui a pour but d'aider à identifier et à classer les échantillons de logiciels malveillants

**File System Scanning**

Scan file system → Scanne les fichiers et répertoires à la recherche de malware.

WARNING: Enabling this setting will scan all files and folders on your system.

**Windows Directories**

- Scan %Systemroot% → Enable file system scanning to scan %Systemroot%
- Scan %P% → Enable file system scanning to scan %P%
- Scan %P% → Enable file system scanning to scan %P%
- Scan %P% → Enable file system scanning to scan %P%
- Scan %User% → Enable file system scanning to scan %User%
- Scan %App% → Enable file system scanning to scan %App%
- Scan %Library% → Enable file system scanning to scan %Library%

**MacOS Directories**

- Scan \$PATH → Enable file system scanning to scan \$PATH locations
- Scan /User → Enable file system scanning to scan /User
- Scan /App → Enable file system scanning to scan /App
- Scan /Library → Enable file system scanning to scan /Library

**Linux Directories**

- Scan \$PATH → Enable file system scanning to scan for \$PATH locations

**Custom Directories**

Custom Filescan Directories Add File → 429

## Advanced Scan template

- Exemple YARA

- La règle ci-dessous indique à YARA que tout fichier contenant l'une des trois chaînes doit être signalé comme « silent\_banker ».

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

source : <https://yara.readthedocs.io/en/latest/>

## Autres templates

- Advanced Dynamic Scan template

- Dynamique

- Au fur et à mesure que Tenable publie de nouveaux plugins, tous les plugins qui correspondent à vos filtres sont automatiquement ajoutés à l'analyse ou à la politique au lieu de sélectionner manuellement des familles de plugins.

- Plugins : <https://www.tenable.com/plugins>

- Familles de Plugins : <https://www.tenable.com/plugins/families/about>

Advanced Dynamic Scan  
Configure a dynamic plugin scan without recommendations.

Match: All of the following:

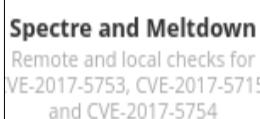
CVE is equal to CVE-YYYY-ID (or CVE-2011-XXXX)

Preview Plugins

Save Cancel

CERT Advisory ID  
CERT Vulnerability ID  
CORE Exploit Framework  
CPE  
CVE  
CVSS v2.0 Base Score

## Autres templates

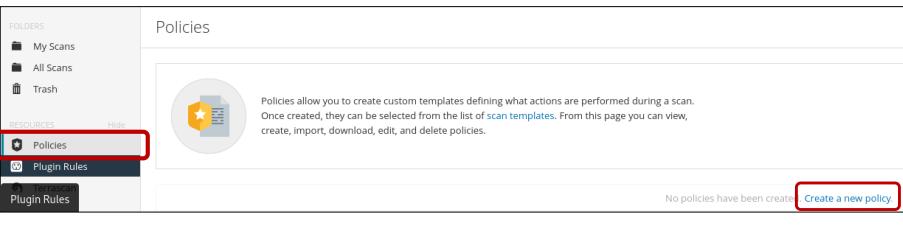


PLUGIN FAMILY	TOTAL	PLUGIN NAME	PLUGIN ID
AIX Local Security Checks	7	CentOS 6 / 7 : firefox (CESA-2018:0122)	106317
Amazon Linux Local Security Checks	3	CentOS 6 / 7 : microcode_ctl (CESA-2018:0093) (Spectre)	106107
CentOS Local Security Checks	12	CentOS 6 : kernel (CESA-2018:0008) (Meltdown) (Spectre)	105589
Debian Local Security Checks	5	CentOS 6 : libvirt (CESA-2018:0030) (Spectre)	105594
Fedora Local Security Checks	14	CentOS 6 : microcode_ctl (CESA-2018:0013) (Spectre)	105590
Firewalls	1	CentOS 7 : kernel (CESA-2018:0007) (Meltdown) (Spectre)	105588
FreeBSD Local Security Checks	1	CentOS 7 : kernel (CESA-2018:0151) (Meltdown) (Spectre)	106353
General	2	CentOS 7 : libvirt (CESA-2018:0029) (Spectre)	105593
Huawei Local Security Checks	8	CentOS 7 : linux-firmware (CESA-2018:0014) (Spectre)	105591
MacOS X Local Security Checks	5	CentOS 7 : linux-firmware (CESA-2018:0094) (Spectre)	106108
Misc.	8	CentOS 7 : microcode_ctl (CESA-2018:0012) (Spectre)	105556
Oracle Linux Local Security Checks	21	CentOS 7 : qemu-kvm (CESA-2018:0023) (Spectre)	105592
Red Hat Local Security Checks	58		
Scientific Linux Local Security Checks	14		
Settings	4		

**HEH.be Sciences et technologies**

## Nessus policies

- **Nessus policies**
  - Une « policy » est un ensemble d'options de configuration prédéfinies liées à l'exécution d'une analyse.
  - Après avoir créé une « policy », vous pouvez la sélectionner comme modèle lors de la création d'un scan.
  - **Créer une « policy »**



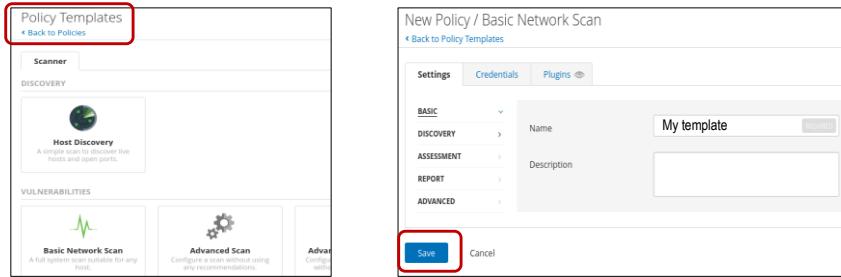
No policies have been created. [Create a new policy](#).

WALLONIE-BRUXELLES ENSEIGNEMENT [All subjects](#) 433

**HEH.be Sciences et technologies**

## Nessus policies

- **Créer une « policy » (suite)**
  - Choix d'un template de départ
    - Pour ne pas devoir configurer tous les paramètres, vous pouvez sélectionner un « template » à partir duquel commencer votre configuration.



Back to Policy Templates

Scanner

DISCOVERY

Host Discovery

A quick scan to discover live hosts and open ports

VULNERABILITIES

Basic Network Scan

A full port and service scan for any host

Advanced Scan

Continuous scanning using any recommendations

Advanced Options

New Policy / Basic Network Scan

Back to Policy Templates

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: My template

Description

Save Cancel

WALLONIE-BRUXELLES ENSEIGNEMENT [All subjects](#) 434

The screenshot shows the Nessus policies interface. At the top left is the HEH.be logo with the text "Sciences et technologies". To the right, the title "Nessus policies" is displayed. Below the title, a sub-section title "- Crée une « policy » (suite)" is shown. The main area is titled "Policies" and contains a table with one row. The table columns are "Name", "Template", and "Last Modified". A single row is present with the name "My template", the template "Basic Network Scan", and the last modified date "Today at 1:49 PM". A red box highlights the "Import" button and the "New Policy" button. A red arrow points from the "User Defined" button in the "Scan Templates" section of the "My scan > New scan" interface to the "User Defined" button in the "Scan Templates" section of the "Policies" interface. Another red arrow points from the "Export" button in the "Scan Templates" section of the "Policies" interface to the text "Export (backup, réutilisation, ...)".

The screenshot shows the Nessus policies interface. At the top left is the HEH.be logo with the text "Sciences et technologies". To the right, the title "Nessus policies" is displayed. Below the title, a sub-section title "• Plugins rules" is shown, followed by a sub-sub-section title "- Redéfinir les gravités (severity)". A bulleted list explains that these rules allow modifying plugin severity levels to fit organizational security profiles. The main area is titled "Plugin Rules" and contains a table with one row. The table columns are "FOLDERS", "RESOURCES", and "Plugin Rules". A single row is present with the folder "My Scans", the resource "Policies", and the rule "Plugin Rules". A red box highlights the "New Rule" button and the "Create a new plugin rule" link. A red arrow points from the "Plugin Rules" link in the "RESOURCES" section of the "Plugin Rules" interface to the "Plugin Rules" link in the "RESOURCES" section of the "Policies" interface.



Sciences  
et technologies

## Nessus policies

- Plugins rules (suite)

New Rule

Host: Leave empty for all hosts.

Plugin ID: Number

Expiration Date: Optional

Severity: Hide this result

Add Cancel

Ce plugin n'apparaîtra pas dans les résultats de scan

Hide this result

Info  
Low  
Medium  
High  
Critical

WALLONIE-BRUXELLES  
ENSEIGNEMENT

437



## Nessus policies

- Terrascan

- Analyseur de code statique pour IaC (Infrastructure as Code).

- L'analyse statique est un processus d'analyse du code source dans le but de trouver des bogues et d'évaluer la qualité du code sans avoir besoin de l'exécuter.

Terrascan

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Terrascan

**Terrascan**

Terrascan is a static code analyzer for Infrastructure as Code. It can be installed and run in a number of different ways, and is most commonly used in automated pipelines to identify policy violations before insecure infrastructure is provisioned. Refer to [Docs](#) for more information.

**Terrascan Installation**

Terrascan

Enabling this option will auto-install the Terrascan executable onto this Nessus host. Disabling this option will remove Terrascan from Nessus.

**Details for the Terrascan executable:**

Status:	Not Installed
Version:	N/A
Path:	N/A

Save Cancel

WALLONIE-BRUXELLES  
ENSEIGNEMENT

438

**HEH.be** Sciences et technologies

Bug bounty

- Amusez-vous à chercher des vulnérabilités

**bugcrowd** OUT HACK THEM ALL™ Who We Are Products Resources Customers CrowdStream Programs About Learn More

**Tesla** Accelerating the world's transition to sustainable energy

\$100 – \$100,000 per vulnerability Partial safe harbor

Submit report

Program details Announcements 2 CrowdStream Hall of Fame

**Overview**

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting.

Vulnerabilities rewarded 729

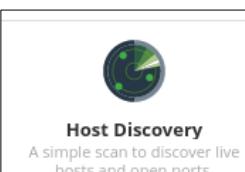
WALLONIE-BRUXELLES ENSEIGNEMENT Pôle de l'Innovation

• • • 439

**HEH.be** Sciences et technologies

## Configuration de Nessus

### Host Discovery Scan

 Host Discovery A simple scan to discover live hosts and open ports.

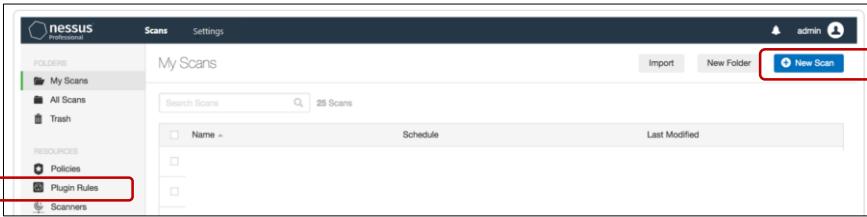
WALLONIE-BRUXELLES ENSEIGNEMENT Pôle de l'Innovation

• • • 440

**HEH.be Sciences et technologies**

## Host Discovery Template

- Découverte d'hôtes
  - Scan
    - Avant de pouvoir créer votre premier scan, vous devez attendre la fin de la compilation des plugins.
  - Scan template
    - Lorsque vous créez une analyse (New scan) ou une politique (Policies) pour la première fois, la section *scan template* apparaît.



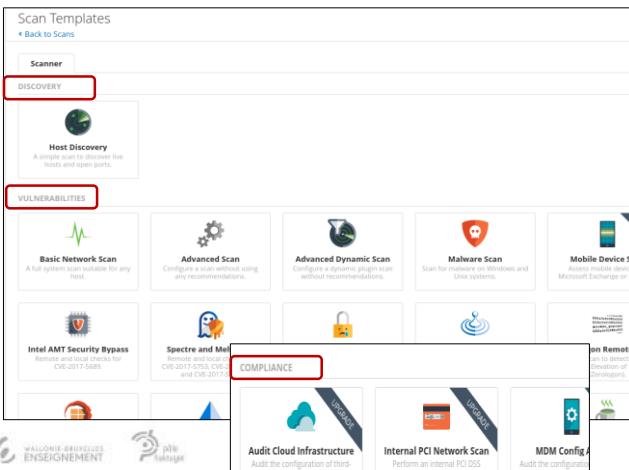
WALLONIE-BRUXELLES  
ENSEIGNEMENT

441

**HEH.be Sciences et technologies**

## Host Discovery Template

- Découverte d'hôtes (suite)
  - Affichage des modèles (*scan templates*)



WALLONIE-BRUXELLES  
ENSEIGNEMENT

442

**Trois types de modèles**

- Discovery
- Vulnérabilités
- Compliance

Certains ne sont pas disponibles dans la version « Essentials » de Nessus

**HEH.be Sciences et technologies**

## Host Discovery Template

- Découverte d'hôtes (suite)

New Scan / Host Discovery

Back to Scan Templates

Settings Plugins

BASIC

General (highlighted)

Schedule

Notifications

DISCOVERY

REPORT

ADVANCED

Name: Host-Discovering

Description:

Folder: My Scans

Targets: 192.168.0.0/24

Upload Targets Add File

Save Cancel

Save or launch

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle de l'enseignement

443

**HEH.be Sciences et technologies**

## Host Discovery Template

- Programmation des scans
  - Choisir des horaires pendant lesquels le réseau/hôtes ne sont pas déjà surchargés.

BASIC

General (highlighted)

Schedule

Notifications

DISCOVERY

REPORT

ADVANCED

Enabled: On

NOTE: Only one schedule can be enabled. Any other scheduled scans will be disabled. Upgrade to Nessus Professional

Frequency: Once

Starts: 14:00 2023-10-09

Timezone: Europe/Brussels

Summary: Once on Monday, October 9th, 2023 at 2:00 PM

Once

Daily

Weekly

Monthly

Yearly

Save Cancel

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle de l'enseignement

444

**HEH.be Sciences et technologies**

## Host Discovery Template

- Notification des scans
  - Un serveur SMTP doit être configuré

Filtres les informations notifiées par mail

445

**HEH.be Sciences et technologies**

## Host Discovery Template

- Configuration du serveur SMTP

446

**HEH.be Sciences et technologies**

## Host Discovery Template

- Discovery

Settings Plugins

BASIC

**DISCOVERY**

REPORT ADVANCED

Scan Type: Host enumeration

General Settings:

Always test the local Nessus host

Use fast network discovery

Ping hosts using:

TCP  
ARP  
ICMP (2 retries)

Host enumeration  
Host enumeration  
OS Identification  
Port scan (common ports)  
Port scan (all ports)  
**Custom**

Si désactivé, Nessus tente d'éviter les faux positifs en effectuant des tests supplémentaires pour vérifier que la réponse ne provient pas d'un proxy ou d'un équilibreur de charge.

WALLONIE-BRUXELLES ENSEIGNEMENT

447

**HEH.be Sciences et technologies**

## Host Discovery Template

- Host Discovery

BASIC

**DISCOVERY**

Host Discovery

Port Scanning

REPORT ADVANCED

Remote Host Ping

Ping the remote host

General Settings

Test the local Nessus host

Use fast network discovery

Ping Methods

ARP → Ne fonctionne que sur le réseau local

TCP

Destination ports: **built-in**

ICMP

Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries: 2

UDP

TCP built-in ports	
139	1029
135	79
445	497
80	548
22	5000
515	1917
23	53
21	161
6000	9001
1025	49000
25	443
111	993
1028	8080
9100	2869

448

**HEH.be** Sciences et technologies

## Host Discovery Template

- Port scanning

**BASIC**

**DISCOVERY**

**Host Discovery**

**Port Scanning**

**REPORT**

**ADVANCED**

**Ports**

Consider unscanned ports as closed

Port scan range: default

**Network Port Scanners**

TCP → Full TCP 3-way handshake

Override automatic firewall detection

Use soft detection

Use aggressive detection

Disable detection

SYN → TCP SYN scan

Override automatic firewall detection

Use soft detection

Use aggressive detection

Disable detection

UDP

Due to the nature of the protocol, it is generally not possible for a port scanner to use the netstat or SNMP port enumeration options instead if possible.

• • • 449

**HEH.be** Sciences et technologies

## Host Discovery Template

- Host Discovery (suite)
  - Fragile devices

- Le balayage des ports est connu pour provoquer le dysfonctionnement de certains dispositifs dit « fragiles ».
- Par exemple, le balayage des ports d'une imprimante peut causer l'impression d'une grande quantité d'informations (probablement dénuée de sens) provenant de chaque port au fur et à mesure du balayage.

**Fragile Devices**

Scan Network Printers

Scan Novell Netware hosts

Scan Operational Technology devices

**Wake-on-LAN**

List of MAC addresses

Boot time wait (in minutes)

Indique à quelles adresses envoyer un paquet magique afin d'allumer le périphérique.

• • • 450

## Host Discovery Template

- Report

The screenshot shows the 'Output' section of the 'REPORT' settings. It includes three checkboxes:

- Allow users to edit scan results
- Designate hosts by their DNS name
- Display hosts that respond to ping
- Display unreachable hosts
- Display Unicode characters

A warning at the bottom states: "WARNING: This feature may cause issues with some..."

Permet de supprimer des éléments du rapport. Doit être désactivé en cas de scan de conformité.

Les hôtes qui n'ont pas répondu à la requête ping sont inclus dans le rapport de sécurité en tant qu'hôtes morts. A ne pas activer pour de larges étendues d'IP à scanner.

Les caractères Unicode apparaissent dans la sortie du plugin

- Par exemple, les noms d'utilisateur et les noms des applications installées.

## Host Discovery Template

- Advanced

The screenshot shows the 'ADVANCED' section with the following configuration:

- Performance Options**
  - Slow down the scan when network congestion is detected
  - Network timeout (in seconds): 5
  - Max simultaneous checks per host: 5
  - Max simultaneous hosts per scan: 256
  - Max number of concurrent TCP sessions per host: [empty]
  - Max number of concurrent TCP sessions per scan: [empty]
- Unix find command Options**
  - Exclude Filepath: Add File (Filepaths to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.)
  - Exclude Filesystem: Add File (Filesystems to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -fs-type argument.)
  - Include Filepath: Add File (Filepaths to include from any use of the find on Unix systems. One entry per line.)

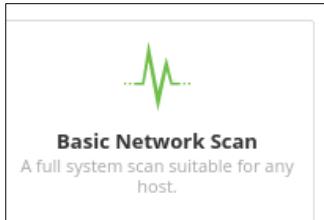
### Windows file search Options

Windows Exclude Filepath	Add File
	Filepaths to exclude from thorough test
Windows Include Filepath	Add File
	Filepaths to include from any use of the find on Unix systems. One entry per line.

**HEH.be**  
Sciences  
et technologies

## Configuration de Nessus

### Vulnerabilities Scan

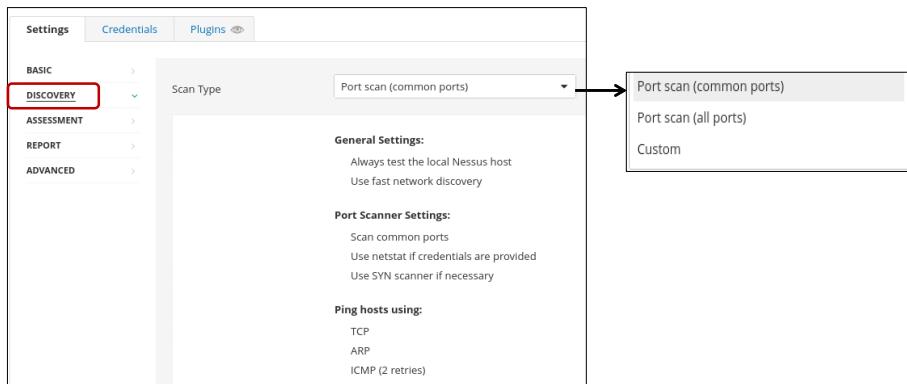


The screenshot shows a slide from a presentation. At the top is the HEH.be logo. Below it is the title "Configuration de Nessus" and the subtitle "Vulnerabilities Scan". A central image is a screenshot of a web-based configuration interface for a "Basic Network Scan". The interface includes a green heart rate monitor icon, the title "Basic Network Scan", and the description "A full system scan suitable for any host.". At the bottom of the slide are logos for Wallonie-Bruxelles Enseignement, Pôle de l'Innovation, and three red dots followed by the number 453.

**HEH.be**  
Sciences  
et technologies

### Basic Network Scan Template

- Scan de vulnérabilités (Onglet « Settings »)
  - Basic Network Scan > Discovery
  - Effectue un scan de vulnérabilités avec « tous » les plugins de Nessus activés.



The screenshot shows a detailed view of the Nessus Settings interface. The left sidebar has tabs for "Settings", "Credentials", and "Plugins". The "DISCOVERY" tab is highlighted with a red box. The main panel shows the "Scan Type" dropdown set to "Port scan (common ports)". To the right, a dropdown menu for "Scan Type" is open, showing options: "Port scan (common ports)" (highlighted), "Port scan (all ports)", and "Custom". Below the dropdown are sections for "General Settings" (Always test the local Nessus host, Use fast network discovery) and "Port Scanner Settings" (Scan common ports, Use netstat if credentials are provided, Use SYN scanner if necessary). At the bottom are settings for "Ping hosts using": TCP, ARP, ICMP (2 retries). At the very bottom are logos for Wallonie-Bruxelles Enseignement, Pôle de l'Innovation, and three red dots followed by the number 454.

**HEHbe Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment

Permet de configurer la manière dont une analyse identifie les vulnérabilités

Scan Type Custom

Scan Type Custom

Default

Scan for known web vulnerabilities

Scan for all web vulnerabilities (quick)

Scan for all web vulnerabilities (complex)

Custom

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

- General
- Brute Force
- Web Applications
- Windows
- Databases

REPORT

ADVANCED

Accuracy

- Override normal accuracy
- Avoid potential false alarms
- Show potential false alarms
- Perform thorough tests (may disrupt your network or impact scan speed)

Effectue des tests approfondis (par ex. un plugin peut analyser plusieurs niveaux de répertoire SMB au lieu d'un seul)  
Plus intrusif, meilleurs résultats mais peut perturber le réseau.

Si l'option Report Paranoïa est réglée sur Show potential false alarms, une faille est signalée à chaque fois, même s'il y a un doute sur le fait que l'hôte distant soit affecté.

Avoid potential false alarms indique à Nessus de ne signaler aucune faille s'il y a un soupçon d'incertitude que l'hôte soit affecté.

• • • 455

**HEHbe Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment (suite)

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

- General
- Brute Force
- Web Applications
- Windows
- Databases

General Settings

Only use credentials provided by the user

Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.

Oracle Database

Test default accounts (slow)

Hydra

Des options pour utiliser Hydra sont disponibles si celui-ci est installé sur la même machine que Nessus

• • • 456

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment (suite)

Lors du scan, Nessus se fait passer pour ce navigateur

URL de la première page testée par Nessus.  
Syntaxe pour tester plusieurs page `/:mypage:/test`

Nombre de liens que Nessus suit pour chaque page de démarrage.

Nessus suit les liens dynamiques et peut dépasser la limite Max depth.

457

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network > Assessment (suite)

Application Test Settings

- Enable generic web application tests
- Abort web application tests if HTTP login fails → ne fait aucun test s'il n'arrive pas à se loguer.
- Try all HTTP methods → Utilise des requêtes POST, pas seulement GET
- Attempt HTTP Parameter Pollution
- Test embedded web servers
- Test more than one parameter at a time per form
  - Test random pairs of parameters
  - Test all pairs of parameters (slow)
  - Test random combinations of three or more parameters (slower)
  - Test all combinations of parameters (slowest)
- Do not stop after the first flaw is found per web page
  - Stop after one flaw is found per web server (fastest)
  - Stop after one flaw is found per parameter (slow)
  - Look for all flaws (slowest)

URL for Remote File Inclusion `http://rfi.nessus.org/rfi.txt`

If the target(s) being scanned cannot reach the Internet, the default URL can be replaced by an internally hosted file. The file must contain PHP source code that displays "NessusCodeExecTest" when executed.

Maximum run time (minutes) 5

458

### – Basic Network Scan > Assessment (suite)

- **Attempt HTTP Parameter Pollution**
  - Essaye de contourner les mécanismes de filtrage en injectant du contenu dans une variable tout en fournissant à cette même variable un contenu valide.
- **Test embedded web servers**
  - Les serveurs web intégrés sont souvent statiques et ne contiennent pas de scripts CGI personnalisables.
  - Ils peuvent avoir tendance à se bloquer ou à ne plus répondre lorsqu'ils sont analysés.
  - Tenable recommande d'analyser les serveurs Web intégrés séparément des autres serveurs Web.
- **Test more than one parameter at a time per form**
  - Par défaut, un paramètre est testé à la fois.
  - Cette option permet de tester plusieurs paramètres ainsi que de gérer la combinaison des valeurs des arguments utilisés dans les requêtes HTTP.

### – Basic Network Scan (suite)

- **Do not stop after first flaw is found per web page**
  - Si cette option est désactivée, dès qu'une faille est trouvée sur une page web, l'analyse passe à la page web suivante.
- **URL for Remote File Inclusion (RFI)**
  - Certaines applications web incluent dynamiquement des fichiers ou des scripts externes.
  - Une attaque RFI est possible lorsqu'une application reçoit un chemin d'accès à un fichier en entrée d'une page web et qu'elle ne l'analyse pas correctement. Cela permet à une URL externe d'être fournie à la fonction d'inclusion.

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan > Assessment (suite)

The screenshot shows the Nessus configuration interface under the 'ASSESSMENT' tab. In the 'General' section, there is a checkbox labeled 'Request information about the SMB Domain'. In the 'User Enumeration Methods' section, three checkboxes are checked: 'SAM Registry', 'ADSI Query', and 'WMI Query'. A red box highlights the 'RID Brute Forcing' button, which is currently set to 'OFF'.

Nessus interroge les utilisateurs du domaine au lieu des utilisateurs locaux.

Tente d'enumérer les comptes d'utilisateurs  
Risque de bloquer les comptes utilisateurs.

**Remarque :** Il existe des solutions spécifiques pour découvrir les vulnérabilités et les mauvaises configurations Active Directory, par exemple *Tenable Identity Exposure*.

• • • 461

**HEH.be Sciences et technologies**

## Basic Network Scan Template

– Basic Network Scan (suite)

The screenshot shows the Nessus configuration interface under the 'ASSESSMENT' tab. In the 'General' section, there is a checkbox labeled 'Use detected SIDs' with a note: 'If host and database credentials are specified, Nessus will attempt to authenticate to the database with SIDs detected locally.'

- Nécessite d'avoir configuré des identifiants d'hôte et Oracle.
  - Le scanner s'authentifie auprès des cibles, puis tente de détecter localement les identifiants de système Oracle (SID).
  - L'analyseur tente ensuite de s'authentifier à l'aide des informations d'identification de la base de données Oracle et des SID détectés.

• • • 462



## Basic Network Scan Template

### – Basic Network Scan > Report

- **Superseeded patch**

- Un correctif remplacé est un correctif qu'il n'est pas nécessaire d'installer parce qu'un correctif ultérieur est disponible et corrige la même vulnérabilité.

- **Plugin dependency**

- Les plugins dépendent souvent des résultats d'autres plugins pour exécuter leurs fonctions.
- Ne pas mentionner les plugins utilisés rend le rapport plus lisible.

The screenshot shows the 'Processing' tab under the 'REPORT' section of the NetworkMiner interface. It includes the following settings:

- Override normal verbosity
- I have limited disk space. Report as little information as possible
- Report as much information as possible
- Show missing patches that have been superseded
- Hide results from plugins initiated as a dependency

At the bottom right of the window, there are three red dots and the number 463.



## Basic Network Scan Template

### – Basic Network Scan > Report (suite)

The screenshot shows the 'Output' tab under the 'REPORT' section of the NetworkMiner interface. It includes the following settings:

- Allow users to edit scan results
- Designate hosts by their DNS name
- Display hosts that respond to ping
- Display unreachable hosts
- Display Unicode characters

A purple arrow points to the first checkbox with the text: "A désactiver lors d'un scan de conformité." (Disable during a compliance scan).

A red arrow points to the last checkbox with the text: "Les caractères Unicode apparaissent dans les sorties du plugin (les noms d'utilisateur, les noms des applications installées et les informations relatives aux certificats SSL)." (Unicode characters appear in plugin outputs (user names, application names installed and SSL certificate information)).

Below the checkboxes, a warning message reads: "WARNING: This feature may cause issues with compliance checks and custom plugins that encounter ISO-8859-1 encoded output."

At the bottom right of the window, there are three red dots and the number 464.

**HEHbe** Sciences et technologies

## Basic Network Scan Template

– Basic Network Scan > Advanced

BASIC >  
DISCOVERY >  
ASSESSMENT >  
REPORT >  
ADVANCED >  
General

**General Settings**

- Enable safe checks
- Stop scanning hosts that become unresponsive during the scan
- Scan IP addresses in a random order
- Automatically accept detected SSH disclaimer prompts  
This will automatically attempt to agree to prompts in SSH connections that Tenable products are configured to recognize.
- Scan targets with multiple domain names in parallel
- Create unique identifier on hosts scanned using credentials

Trusted CAs

CA certificates listed here will be considered as trusted CAs by the scan

WALLONIE-BRUXELLES  
ENSEIGNEMENT

ULB  
Université de Louvain

• • • 465

**HEHbe** Sciences et technologies

## Basic Network Scan Template

– Basic Network Scan > Advanced (suite)

- **Enable Safe Checks**
  - Lorsque cette option est activée, elle désactive tous les plugins susceptibles d'avoir un effet néfaste sur l'hôte distant.
- **Stop scanning hosts that become unresponsive during the scan**
  - Un hôte pourrait ne plus répondre suite à l'utilisation d'un plugin DoS, parce qu'un système de protection bloque le scan ou juste parce qu'un utilisateur a éteint son PC.
- **Scan IP addresses in a random order**
  - Peut être utile pour répartir le trafic réseau lors du scan d'une grande étendue d'IP.
- **Automatically accept detected SSH disclaimer**
  - S'il est désactivé et que la cible présente un disclaimer, celui-ci ne sera pas accepté et le scan accrédié ssh login fail
- **Scan targets with multiple domain names in parallel**
  - Désactivé, pour empêcher de submerger un hôte par plusieurs scans simultanés lorsque plusieurs noms renvoient vers une même adresse IP.
- **Trusted CA**
  - Liste des autorités de certification reconnues par Nessus.

WALLONIE-BRUXELLES  
ENSEIGNEMENT

ULB  
Université de Louvain

• • • 466

**HEHbe** Sciences et technologies Basic Network Scan Template

– Basic Network Scan > Advanced (suite)

**Performance Options**

- Slow down the scan when network congestion is detected
- Network timeout (in seconds): 5
- Max simultaneous checks per host: 5
- Max simultaneous hosts per scan: 30
- Max number of concurrent TCP sessions per host: [ ]
- Max number of concurrent TCP sessions per scan: [ ]

**Unix find command Options**

Exclude Filepath	Add File
Filepaths to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.	
Exclude Filesystem	Add File
Filesystems to exclude from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.	
Include Filepath	Add File
Filepaths to include from any use of the find on Unix systems. One entry per line. Format as used by the -path argument.	

**Windows file search Options**

Windows Exclude Filepath	Add File
Filepaths to exclude from any use of search on Windows systems excludes which include \Windows\WinSxS and \Windows\servic	
Windows Include Filepath	Add File
Filepaths to include from any use of Recursive search on Window tests are enabled. Use of this setting will replace the de	

• • • 467

**HEHbe** Sciences et technologies Basic Network Scan Template

– Basic Network Scan > Advanced (suite)

**Debug Settings**

- Log scan details  
Logs the start and finish time for each plugin used during a scan to nessusd.messages.
- Always report SSH commands  
Attaches all SSH commands run on target hosts irrespective of debug settings.
- Enable plugin debugging  
Attaches available debug logs from plugins to the vulnerability output of this scan.

Debug Log Level: Level 1: Basic Debugging

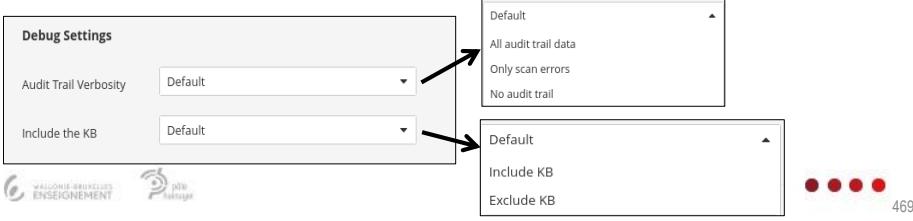
Level 1: Basic Debugging  
Level 2: Advanced Debugging  
Level 3: Full Debugging  
Level 4: Unrestricted Debugging

• • • 468

## Basic Network Scan Template

### – Basic Network Scan > Advanced (suite)

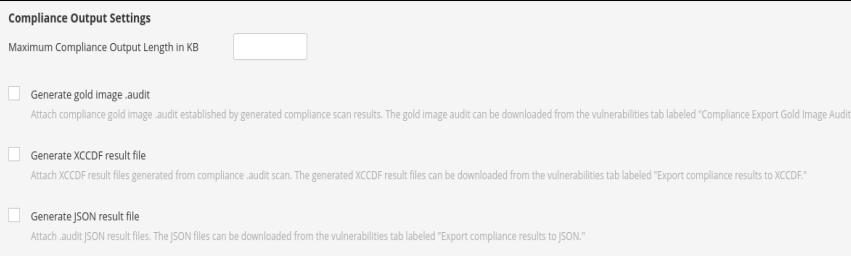
- **Audit trail**
  - Fonction qui renseigne pourquoi un plugin a eu tel comportement
  - Par exemple, pourquoi il ne renvoie pas de résultat, bien qu'il soit en cours d'exécution.
- **Include the KB**
  - Une base de connaissances (KB : Knowledge Base) est créée pour chaque cible au cours d'un scan Nessus.
  - Lorsqu'un plugin collecte des informations qui doivent être "partagées" avec d'autres plugins, elles sont stockées dans la base de connaissances de cet hôte.
  - Fournit plus de données de débogage en incluant les données de la KB dans les résultats du scan.



## Basic Network Scan Template

### – Basic Network Scan > Advanced (suite)

- Contrôle la longueur maximale de chaque contrôle de conformité individuel renvoyée par la cible.
- Permet de choisir les plugins à utiliser pour formater les résultats de scan conformité dans des formats de données que d'autres outils (Tenable et tiers) peuvent utiliser.



### • Onglet « Plugins »

		PLUGIN NAME	PLUGIN ID
CGI abuses : XSS	703		
CISCO	2322	Debian DLA-100-1 : mutt security update	82084
Databases	944	Debian DLA-1000-1 : imagemagick security update	101031
Debian Local Security Checks	9020	Debian DLA-1001-1 : exim4 security update (Stack Clash)	101032
Default Unix Accounts	172	Debian DLA-1002-1 : smb4k security update	101033
Denial of Service	110	Debian DLA-1003-1 : unrar-nonfree security update	101065
DNS	231	Debian DLA-1004-1 : drupal7 security update	101092
FS Networks Local Security Checks	1294	Debian DLA-1005-1 : mercurial security update	101121
Fedora Local Security Checks	17687	Debian DLA-1006-1 : libarchive security update	101173
Firewalls	400	Debian DLA-1007-1 : icedove/thunderbird security update	101208
FreeBSD Local Security Checks	5382	Debian DLA-1008-1 : libxml2 security update	101174
FTP	271	Debian DLA-1009-1 : apache2 security update	101175
Gain a shell remotely	282	Debian DLA-1011-1 : jasper security update	82085
General	354	Debian DLA-1010-1 : vorbis-tools security update	101209
Gentoo Local Security Checks	3441	Debian DLA-1011-1 : sudo security update	101210

### – Basic Network Scan > Advanced (suite)

**Debug Settings**

Log scan details  
Logs the start and finish time for each plugin used during a scan to nessusd.messages.

Always report SSH commands  
Attaches all SSH commands run on target hosts irrespective of debug settings.

Enable plugin debugging  
Attaches available debug logs from plugins to the vulnerability output of this scan.

Debug Log Level

Enumerate launched plugins  
Adds a list of plugins that were launched during the scan.

Audit Trail Verbosity

Include the KB

**HEHbe Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport

My Scans

Name	Schedule	Last Scanned
test	On Demand	October 6 at 9:05 AM

test

Vulnerabilities

Scan Details

Hosts: 1 | Vulnerabilities: 473 | Remediations: 0 | History: 0

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0

473

**HEHbe Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport (suite)

Filter ▾ Search Vulnerabilities 34 Vulnerabilities

Sev	CVSS	VPR	Nam...	Family	Count
Mixed	...	...	QMisc.		30
Mixed	...	...	IEGeneral		2
Mixed	...	...	MWindows		2
Mixed	...	...	SGeneral		9
Mixed	...	...	TLService detection		4
Mixed	...	...	SMisc.		2
Info	...	...	HWeb Servers		10
Info	...	...	SWindows		10
Info	...	...	SWindows : User management		2

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: October 6 at 9:16 AM  
End: October 6 at 9:41 AM  
Elapsed: 24 minutes

Vulnerabilities

Critical: 3 | High: 10 | Medium: 10 | Low: 2 | Info: 9

474

**HEH.be Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport (suite)

The screenshot shows a 'Filters' dialog box with a dropdown menu 'Match All of the following' and a condition 'Severity is equal to Critical'. Below it is a 'Vulnerabilities' summary table with one critical vulnerability found on host 192.16.

Severity	CVSS	VPR	Name Family	Count
Critical	9.8	Q...	Misc.	2

Below the interface are logos for Wallonie-Bruxelles Enseignement and Pôle de l'Innovation, followed by a red navigation bar with dots and the number 475.

**HEH.be Sciences et technologies**

### Basic Network Scan Template

- Afficher les résultats et le rapport (suite)

The screenshot shows a 'Hosts' overview with 34 vulnerabilities found across 1 host. A red box highlights the 'Report' button in the top right. Below it is a 'Generate Report - 1 Host Selected' dialog with options for HTML or CSV format, and a 'Filters Applied' section indicating 'Severity is equal to Critical'.

Scan Details:

- Policy: Basic Network Scan
- Status: Compiled
- Severity Base: CVSS v3.0

Below the interface are logos for Wallonie-Bruxelles Enseignement and Pôle de l'Innovation, followed by a red navigation bar with dots and the number 476.

**HEH.be**  
Sciences  
et technologies

## Configuration de Nessus

### Advanced Scan template

Advanced Scan  
Configure a scan without using any recommendations.

WALLONIE-BRUXELLES  
ENSEIGNEMENT

477

**HEH.be**  
Sciences  
et technologies

### Advanced Scan template

Settings    Credentials    Plugins

BASIC  
DISCOVERY  
\* Host Discovery  
Port Scanning  
Service Discovery

Identity  
ASSESSMENT  
REPORT  
ADVANCED

Remote Host Ping  
Ping the remote host

General Settings

Test the local Nessus host  
This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.

Use fast network discovery  
If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Fast network discovery bypasses those additional tests.

Ping Methods

ARP  
 TCP  
 ICMP

Destination ports

Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries

UDP

WALLONIE-BRUXELLES  
ENSEIGNEMENT

478

**HEH.be Sciences et technologies**

### Advanced Scan template

- Setting > discovery > Service Discovery

General Settings

Probe all ports to find services

Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.

Search for SSL/TLS Services

Search for SSL/TLS on: All TCP ports

Search for DTLS on: None

Identify certificates expiring within x days: 60

Enumerate all SSL/TLS ciphers

When selected, Nessus ignores the list of ciphers advertised by SSL/TLS services, and enumerates them by attempting to establish connections using all possible ciphers.

Enable CRL checking (connects to the Internet)

479

**HEH.be Sciences et technologies**

### Advanced Scan template

- Setting > Discovery > Identity
- Collect Identity Data from Active Directory

- Permettre à Nessus de collecter des objets d'utilisateur, d'ordinateur et de groupe dans l'Active Directory.
- Nécessite d'avoir configuré les identifiants pour l'accès à l'AD.

General Settings

Collect Identity Data from Active Directory

Checking this box will enable collection of identity information from Active Directory using Domain User credentials.

480

## Advanced Scan template

- Setting > Discovery > Assessment > General

Voir « Basic Network Scan »

Par défaut, Nessus considère que les signatures sont périmées, quel que soit le temps écoulé depuis la mise à jour. Vous pouvez autoriser une période de grâce jusqu'à 7 jours avant de signaler qu'une signature est périmée.

Nessus tente d'envoyer du spam à l'adresse indiquée.

• • • 481

## Advanced Scan template

- Setting > Discovery > Assessment > Malware

Par défaut, Nessus utilise le cloud pour comparer les résultats du scan avec des malwares connus

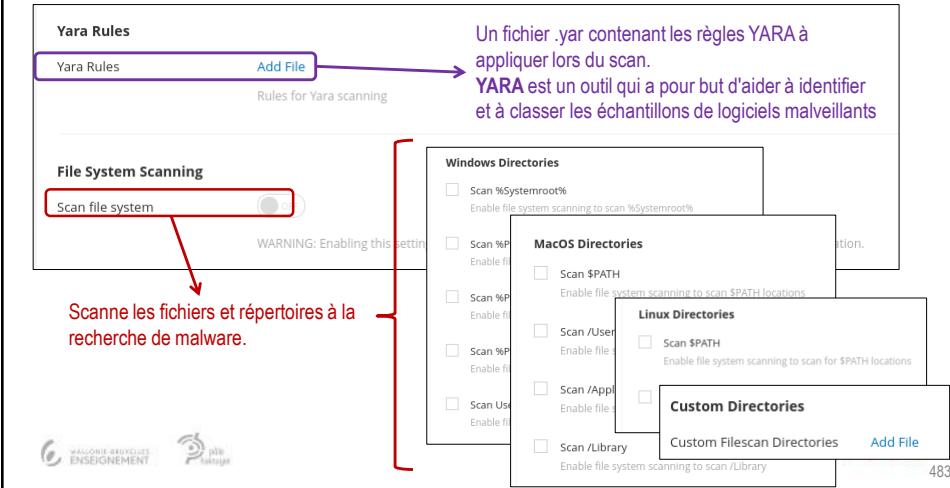
Fournir un fichier texte contenant une liste d'adresses IP connues comme étant malicieuses que vous souhaitez détecter.

Liste d'IP et de noms d'hôtes que Nessus ignorera pendant le scan.

• • • 482

## Advanced Scan template

- Setting > Discovery > Assessment > Malware (suite)



**Yara Rules**

Add File → Un fichier .yar contenant les règles YARA à appliquer lors du scan.  
**YARA** est un outil qui a pour but d'aider à identifier et à classer les échantillons de logiciels malveillants

**File System Scanning**

Scan file system → Scanne les fichiers et répertoires à la recherche de malware.

WARNING: Enabling this setting will scan all files and folders on your system.

**Windows Directories**

- Scan %Systemroot% → Enable file system scanning to scan %Systemroot%
- Scan %P% → Enable file system scanning to scan %P%
- Scan %P% → Enable file system scanning to scan %P%
- Scan %P% → Enable file system scanning to scan %P%
- Scan %User% → Enable file system scanning to scan %User%
- Scan %App% → Enable file system scanning to scan %App%
- Scan %Library% → Enable file system scanning to scan %Library%

**MacOS Directories**

- Scan \$PATH → Enable file system scanning to scan \$PATH locations
- Scan /User → Enable file system scanning to scan /User
- Scan /App → Enable file system scanning to scan /App
- Scan /Library → Enable file system scanning to scan /Library

**Linux Directories**

- Scan \$PATH → Enable file system scanning to scan for \$PATH locations

**Custom Directories**

Custom Filescan Directories → Add File → 483

## Advanced Scan template

- Exemple YARA

- La règle ci-dessous indique à YARA que tout fichier contenant l'une des trois chaînes doit être signalé comme « silent\_banker ».

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

source : <https://yara.readthedocs.io/en/latest/>

## Autres templates

- Advanced Dynamic Scan template

- Dynamique

- Au fur et à mesure que Tenable publie de nouveaux plugins, tous les plugins qui correspondent à vos filtres sont automatiquement ajoutés à l'analyse ou à la politique au lieu de sélectionner manuellement des familles de plugins.

- Plugins : <https://www.tenable.com/plugins>

- Familles de Plugins : <https://www.tenable.com/plugins/families/about>

The screenshot shows the Tenable.io interface with the 'Dynamic Plugins' configuration dialog open. On the left, there's a card titled 'Advanced Dynamic Scan' with the sub-instruction 'Configure a dynamic plugin scan without recommendations.' Below the card are logos for Wallonie Bruxelles Enseignement and the University of Namur. The configuration dialog has tabs for 'Settings', 'Credentials', and 'Dynamic Plugins'. In the 'Dynamic Plugins' tab, there's a dropdown menu labeled 'Match' with 'All' selected, followed by 'of the following'. A red arrow points from the 'Advanced Dynamic Scan' card to this dropdown. To the right of the dropdown is a search bar containing 'CVE' and a dropdown menu with 'is equal to' selected. A placeholder 'CVE-YYYY-ID (or CVE-2011-1234)' is shown in the search bar. Below the search bar are buttons for 'Preview Plugins', 'Save', and 'Cancel'. To the right of the main dialog is a sidebar with options: CERT Advisory ID, CERT Vulnerability ID, CORE Exploit Framework, CPE, CVE, and CVSS v2.0 Base Score.

485

## Autres templates



**Spectre and Meltdown**  
Remote and local checks for  
CVE-2017-5753, CVE-2017-5715  
and CVE-2017-5754

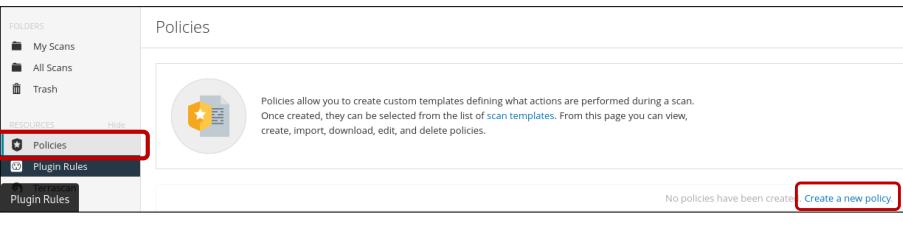
PLUGIN FAMILY	TOTAL	PLUGIN NAME	PLUGIN ID
AIX Local Security Checks	7	CentOS 6 / 7 : firefox (CESA-2018:0122)	106317
Amazon Linux Local Security Checks	3	CentOS 6 / 7 : microcode_ctl (CESA-2018:0093) (Spectre)	106107
CentOS Local Security Checks	12	CentOS 6 : kernel (CESA-2018:0008) (Meltdown) (Spectre)	105589
Debian Local Security Checks	5	CentOS 6 : libvirt (CESA-2018:0030) (Spectre)	105594
Fedora Local Security Checks	14	CentOS 6 : microcode_ctl (CESA-2018:0013) (Spectre)	105590
Firewalls	1	CentOS 7 : kernel (CESA-2018:0007) (Meltdown) (Spectre)	105588
FreeBSD Local Security Checks	1	CentOS 7 : kernel (CESA-2018:0151) (Meltdown) (Spectre)	106353
General	2	CentOS 7 : libvirt (CESA-2018:0029) (Spectre)	105593
Huawei Local Security Checks	8	CentOS 7 : linux-firmware (CESA-2018:0014) (Spectre)	105591
MacOS X Local Security Checks	5	CentOS 7 : linux-firmware (CESA-2018:0094) (Spectre)	106108
Misc.	8	CentOS 7 : microcode_ctl (CESA-2018:0012) (Spectre)	105556
Oracle Linux Local Security Checks	21	CentOS 7 : qemu-kvm (CESA-2018:0023) (Spectre)	105592
Red Hat Local Security Checks	58		
Scientific Linux Local Security Checks	14		
Settings	4		

486

**HEH.be Sciences et technologies**

## Nessus policies

- **Nessus policies**
  - Une « policy » est un ensemble d'options de configuration prédéfinies liées à l'exécution d'une analyse.
  - Après avoir créé une « policy », vous pouvez la sélectionner comme modèle lors de la création d'un scan.
  - **Créer une « policy »**



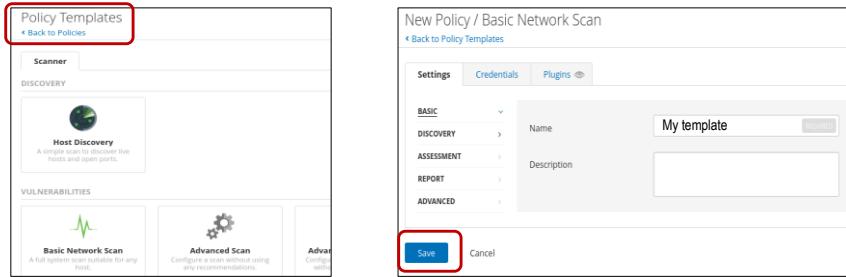
WALLONIE-BRUXELLES  
ENSEIGNEMENT

487

**HEH.be Sciences et technologies**

## Nessus policies

- **Créer une « policy » (suite)**
  - Choix d'un template de départ
    - Pour ne pas devoir configurer tous les paramètres, vous pouvez sélectionner un « template » à partir duquel commencer votre configuration.



WALLONIE-BRUXELLES  
ENSEIGNEMENT

488

The screenshot shows the Nessus policies interface. At the top left is the HEH.be logo. To its right, the title "Nessus policies" is displayed. Below the title, a sub-section title "- Crée une « policy » (suite)" is shown. The main area displays a "Policies" page with a table listing one policy: "My template". A red box highlights the "Import" button at the top right of the table. A red arrow points from the "User Defined" tab in the "Scan Templates" section of the "New scan" dialog to the "User Defined" tab in the "Scan Templates" list on the right. Another red arrow points from the "Export" icon in the "Scan Templates" list to the text "Export (backup, réutilisation, ...)".

The screenshot shows the Nessus policies interface. At the top left is the HEH.be logo. To its right, the title "Nessus policies" is displayed. Below the title, a sub-section title "• Plugins rules" is shown, followed by a sub-sub-section title "- Redéfinir les gravités (severity)". A bulleted list explains that these rules allow modifying plugin severity levels to fit organizational security profiles. The main area displays a "Plugin Rules" page with a table showing no rules have been created. A red box highlights the "Create a new plugin rule" button at the bottom right. A red arrow points from the "Plugin Rules" tab in the navigation bar to this button.



Sciences  
et technologies

## Nessus policies

- Plugins rules (suite)

New Rule

Host

Plugin ID

Expiration Date

Severity  Hide this result

Add Cancel

Ce plugin n'apparaîtra pas dans les résultats de scan

Info  
Low  
Medium  
High  
Critical

• • • 491



## Nessus policies

- Terrascan

- Analyseur de code statique pour IaC (Infrastructure as Code).

- L'analyse statique est un processus d'analyse du code source dans le but de trouver des bogues et d'évaluer la qualité du code sans avoir besoin de l'exécuter.

TERRASCAN

Terrascan

Details for the Terrascan executable:

Status:	Not Installed
Version:	N/A
Path:	N/A

Save Cancel

• • • 492

**HEH.be** Sciences et technologies

Bug bounty

- Amusez-vous à chercher des vulnérabilités

**bugcrowd** OUT HACK THEM ALL™ Who We Are Products Resources Customers CrowdStream Programs About Learn More

**Tesla** Accelerating the world's transition to sustainable energy

\$100 – \$100,000 per vulnerability Partial safe harbor

Submit report

Program details Announcements 2 CrowdStream Hall of Fame

**Overview**

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting.

Vulnerabilities rewarded 729

• • • 493

## Bibliographie

### Ouvrages

ACISSI, *Sécurité informatique. Ethical Hacking 6<sup>e</sup> édition*, ENI, 2022

HUCABY D., *CCNA Wireless 200-355*, Cisco Press, 2015

SANTOS O., STUPPI J., *CCNA Security 210-260 Official Cert Guide*, Cisco Press, 2015.

VIJAY KUMAR VELU, *Mastering Kali Linux for advanced penetration testing 4<sup>ème</sup> édition*, Packt, 2022

### Sources électroniques

BAUDU H., LE BOURHIS F., *La propagation des ondes*, [en ligne]  
<http://dept.navigation.enmm.free.fr/propagation.swf>, 2006.

BEST MONITORING TOOLS, *Configure SNMP v3 on Cisco Devices*, [en ligne]  
[https://bestmonitoringtools.com/configure-snmpv3-on-cisco-router-switch-asa-nexus-a-step-by-step-guide/#SNMPv2\\_is\\_so\\_easy\\_-\\_why\\_do\\_we\\_need\\_SNMPv3](https://bestmonitoringtools.com/configure-snmpv3-on-cisco-router-switch-asa-nexus-a-step-by-step-guide/#SNMPv2_is_so_easy_-_why_do_we_need_SNMPv3)

CISCO SYSTEM, INC, *Antenna Patterns and Their Meaning*, [en ligne]  
[http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod\\_white\\_paper0900aecd806a1a3e.pdf](http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.pdf), 1992–2007.

CISCO SYSTEMS, INC, *Catalyst 2960-X Switch Network Management Configuration Guide*, [en ligne] [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0\\_2\\_EX/network\\_management/configuration\\_guide/b\\_nm\\_15ex\\_2960-x\\_cg/b\\_nm\\_15ex\\_2960-x\\_cg\\_chapter\\_0100.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/network_management/configuration_guide/b_nm_15ex_2960-x_cg/b_nm_15ex_2960-x_cg_chapter_0100.html)

CISCO SYSTEMS, INC, *Introduction to Cisco IOS NetFlow - A Technical Overview*, [en ligne]  
[http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod\\_white\\_paper0900aecd80406232.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html), 2012.

CISCO SYSTEMS, INC, *IP SLAs Configuration Guide, Cisco IOS Release 15M&T*, [en ligne]  
[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla\\_overview-0.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_overview-0.html), 2022.

CISCO SYSTEMS, INC, *NetFlow Configuration Guide, Cisco IOS Release 15M&T*, [en ligne]  
<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/get-start-cfg-nflow.html>, 2016.

CISCO SYSTEMS, INC, *SNMP Configuration Guide*, [en ligne]  
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html>, 2020.

GORDON LYON, *The Nmap Project*, [en ligne] <https://nmap.org/>, 2023.

MEDIAWIKI, *The Penetration Testing Execution Standard*, [en ligne] <http://www.pentest-standard.org>, 2023.

Cisco Networking academy, Ethical Hacker, [en ligne]  
<https://www.netacad.com/courses/ethical-hacker?courseLang=en-US>, 2023