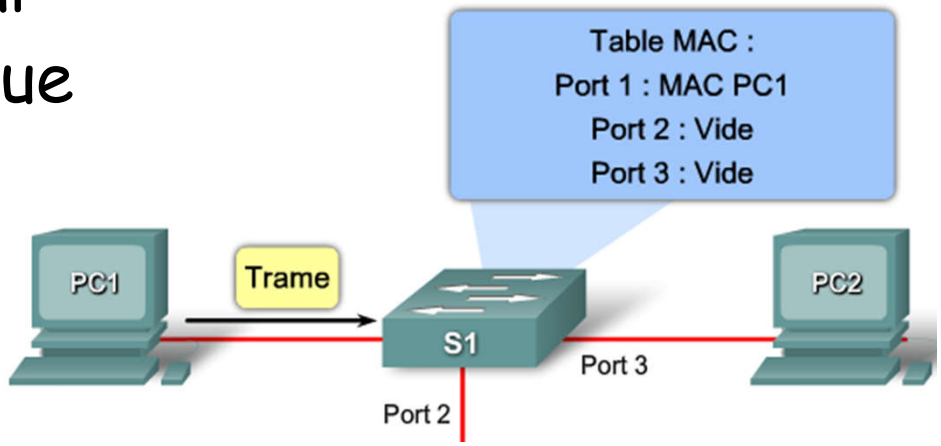
2-Sécurisation des équipements réseaux

Techniques de sécurisation

- Sécurisation des équipements réseaux
  - Filtrage par adresse MAC
  - Gestion des mots de passe
  - Recouvrement des mots de passe oubliés
  - Protection des lignes de commandes
  - Désactivation des services inutilisés
  - Sauvegarde TFTP
  - Connexions distantes TELNET et SSH
  - Sécurisation des accès WLAN
  - Authentification
  - Protocoles AAA

Filtrage par adresses MAC

- En théorie l'@MAC est unique
- Table MAC commutateur
- Le commutateur effectue une association **@MAC source / port**



- Filtrage par adresse MAC
  - Permet d'autoriser ou de refuser l'accès au réseau aux équipements définis dans une liste d'accès. L'@MAC est analysée par le commutateur et est comparée à la liste des autorisations

Filtrage par adresses MAC

- Lorsqu'un PC se connecte sur un port d'un Switch il est capable de récupérer l'ensemble du trafic passant par ce port du Switch
  - Il faut donc sécuriser l'accès à ses ports
- On peut donc protéger certains ports en restreignant l'accès à une ou plusieurs @MAC spécifiques
  - Utiliser le mode access
  - Autoriser la connexion qu'à une seule adresse MAC
  - Spécifier la seule adresse MAC autorisée à se connecter sur ce port précis
  - Apprentissage dynamique de l'adresse autorisée
  - Désactiver le port en cas de violation

Configuration

- Elle se fait en plusieurs étapes
  - 1. Mettre le port en mode access
    - **Switch(config-if)# switchport mode access**
  - 2. Activer la **sécurité globale** sur un ou plusieurs ports
    - **Switch(config-if)# switchport port-security**
  - 3. Indiquer le **nombre maximum** d'adresses MAC qui peuvent se connecter sur ce port (dans l'exemple 2)
    - **Switch(config-if)# switchport port-security max 2**
- Il existe deux cas pour le filtrage
  - **Filtrage statique** : la liste des adresses mac autorisées est spécifiée de manière statique
  - **Filtrage dynamique** : la liste des adresses mac autorisées est apprise dynamiquement

Configuration

- Filtrage statique
  - 4. Pour spécifier les seules adresses MAC autorisées
    - **Switch(config-if)#switchport port-security mac-address 0001.424B.6502**
    - **Switch(config-if)#switchport port-security mac-address 00a1.b2cB.def2**

- Filtrage dynamique
  - 4. Les adresses mac autorisées sont apprises dynamiquement par ordre d'arrivée jusqu'à atteindre le nombre maximum fixée
    - **Switch(config-if)#switchport port-security mac-address sticky**

Configuration

- Etapes suivantes
  - 5. En cas de violation action à entreprendre
    - **Switch(config-if)# switchport port-security violation ?**
- Il existe deux méthodes en cas de violation
  - **shutdown** : le port est totalement désactivé
  - **restrict** : le port est activé mais tous les paquets de la machine non autorisée sont bloqués. Le Switch garde en mémoire le nombre de violations
- Remettre le port dans l'état initial non sécurisé
    - **Switch#clear port-security [options]**
  - Réactiver un port désactivé par le filtrage
    - Faire **no shutdown** et ensuite **shutdown**

Gestion des mots de passe

- Mot de passe d'accès à la console
  - **Routeur(config)#line console 0**
  - **Routeur(config-line)#password cisco**
  - **Routeur(config-line)#login**
- Mot de passe administrateur
  - Deux manières de le définir
    - **Routeur(config)#enable password class1**
    - **Routeur(config)#enable secret class2**
  - Le mot de passe secret est prioritaire sur le mot de passe password
- Cryptage et taille minimale des mots de passe
  - **Routeur(config)#service password-encryption**
  - **Routeur(config)#security passwords min-length [0-16]**

Suppression des mots de passe

- Permet de supprimer les mots de passe console et administrateur
- **Routeur>show version**
  - Notez la valeur du registre de configuration
  - « Configuration register is `0x2102` »
  - Redémarrez le routeur
  - Pendant le chargement appuyez sur CTRL+C
  - Sous windows CTRL + Pause
  - Mode **rommon** de démarrage basic sans l'IOS
- **rommon 1> confreg 0x2142**
- **rommon 2> reset**

Protection des lignes inactives

- Les lignes console et vty peuvent être inactives pendant un intervalle de temps
- Déconnexion automatique au bout d'un temps
  - **R1(config)#line console 0**
  - **R1(config-lin)#exec-timeout 5 0 (5 minutes 0 secondes)**
  - **R1(config)#line vty 0 4**
  - **R1(config-lin)#exec-timeout 5 0**
- Empêcher les tentatives de connexion par force brute
- Bloquer les tentatives de connexion pendant 5 minutes si un utilisateur effectue 2 tentatives de connexion sans y parvenir au bout de 2 minutes.
  - **R1(config)#login block-for 300 attempt 2 within 120**

Désactivation des services

- Désactiver les services inutilisés qui fonctionnent par défaut au démarrage du routeur
  - Suivant les versions de l'IOS les services ne sont pas les mêmes
  - **R1(config)#no service timestamps**
  - **R1(config)#no service nagle**
  - **R1(config)#no cdp run (Equipements cisco voisins)**
  - **R1(config)#no service ?**
- Désactiver les protocoles UDP qui ne doivent pas être routés
  - **R1(config)#no ip forward-protocol udp ?**
- Fonction de sécurité globale du routeur
  - **R1#auto secure**

Sauvegarde TFTP

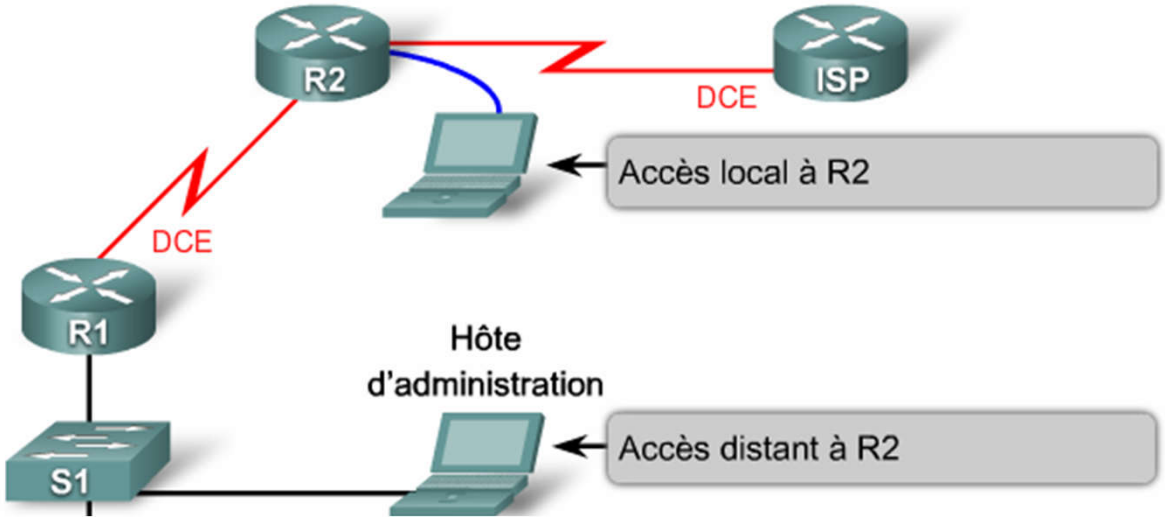
- Protocole de transfert des fichiers légers fonctionnant en UDP sur le port 69
- Sauvegarde de la configuration des routeurs
  - Nécessité d'un client et d'un serveur TFTP
  - Vérifier la connexion entre client et serveur (ping)
- Sauvegarde de la mémoire flash (Images IOS)
  - **Router#copy flash tftp:**
- Sauvegarde de la configuration actuelle du routeur
  - **Router#copy running-config tftp:**
- Chargement de la configuration depuis le serveur TFTP vers le routeur
  - **Router#copy tftp: [running-config | flash]**

Mise à jour (upgrade) IOS

- **Switch Catalyst 2960 IOS 12.2 → IOS 15.0**
- Pré-configuration
  - Adresse IP du serveur TFTP, du switch (vlan 1)
  - Vérification version IoS et de l'image IoS 15 (TFTP)
- Mise à jour IOS depuis le serveur TFTP
  - **Switch#copy tftp flash:**
  - **Address or name of remote host []? 10.0.0.1**
  - **Source filename [ ]? c2960-lanbasek9-mz.150-2.SE4.bin**
- Installation de la nouvelle image IOS
  - **Switch(config)#boot system flash:c2960-lanbasek9-mz.150-2.SE4.bin**
  - **Switch#write**
  - **Switch#reload**
- Vérification
  - **Switch#version**

Gestion des accès à distance

- Accès à distance
  - Facilite l'administration des équipement sur des grands réseaux
- Nécessité de protocoles d'accès distants
  - **TELNET** → Les informations circulent en clair
  - **SSH** → Chiffrement des informations



Configuration SSH

- Configuration d'un accès SSH sur le routeur
  - **Router(config)# hostname Nomrouteur**
  - **Router(config)# ip domain-name info.ut.sn**
  - **Router(config)# ip ssh version 2**
  - **Router(config)# ip ssh time-out 120 (120 secondes)**
  - **Router(config)# ip ssh authentication-retries 2**
    (Fermeture après deux tentatives sans succès)
  - **Router(config)# crypto key generate rsa (taille 1024 bits)**

- Connexion à partir d'un poste client SSH
  - **PC> ssh –l username IProuteur**

- Visualiser les connexions SSH actives
  - **Router# show ssh**

Filtrage Telnet ou SSH

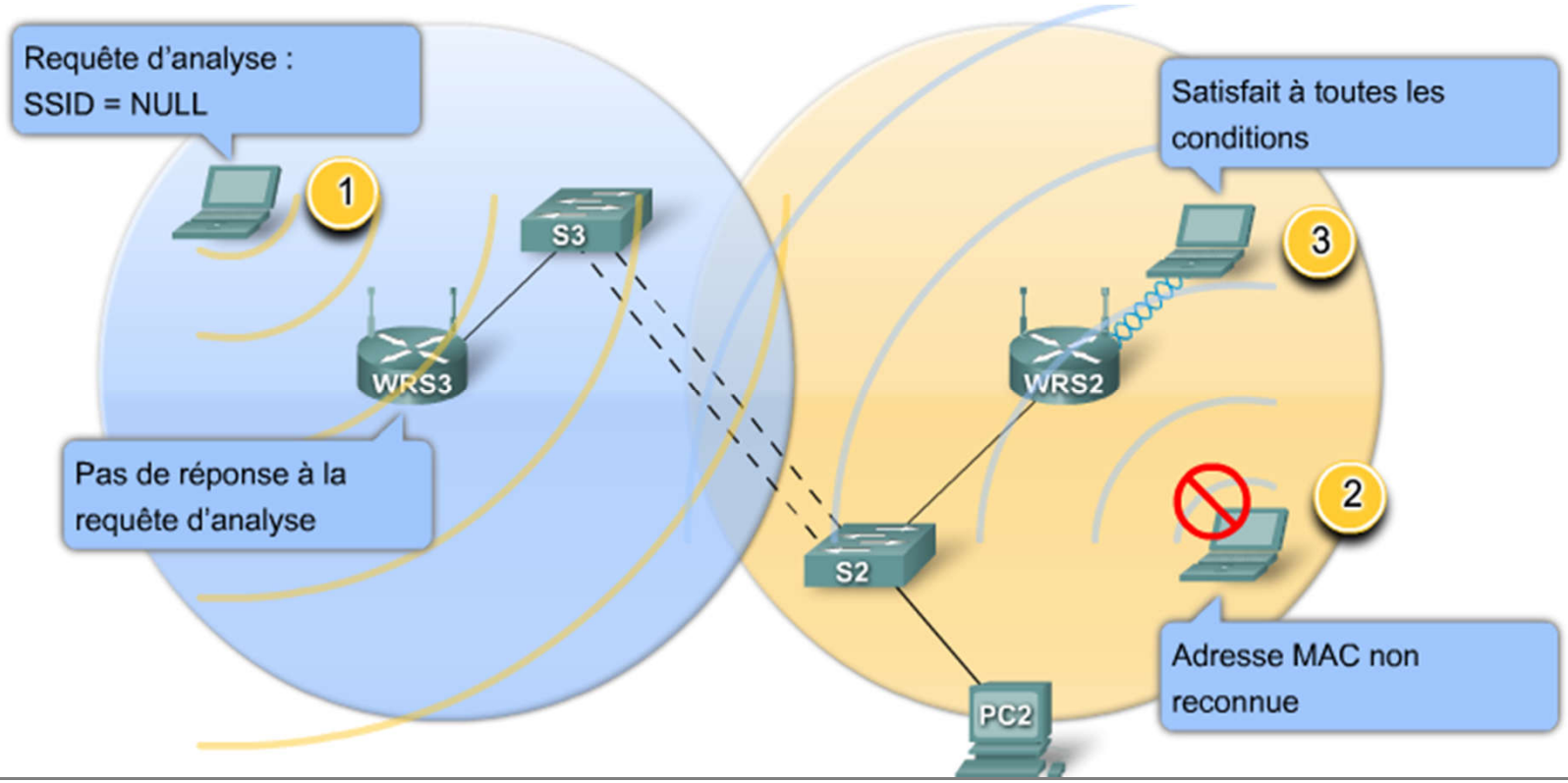
- Activer les lignes vty pour les connexions distantes
  - **Router(config)# line vty 0 4**
  - **Router(config-line)# password cisco**
  - **Router(config-line)# login**

- Filtrage du protocole de connexion distante
  - **Router(config-line)# transport input ?**

  - **all :** tous les protocoles autorisés
  - **none :** aucun protocole autorisé
  - **telnet :** seul le protocole telnet est autorisé
  - **ssh :** seul le protocole ssh est autorisé

Sécurité des WLAN

- SSID non diffusé
- Filtrage des adresses MAC
- Authentification distante



Sécurité WLAN

- **WEP (Wired Equivalent Privacy) 1997**
  - Clé statique variant de 64 à 128b (Hexadecimal)
- **WPA (Wifi Protected Access) 2003**
  - Clé statique variant de 8 à 63 caractères ASCII
- **WPA Entreprise**
  - Authentification distante par des serveurs AAA
- Evolution vers **WPA2 et WPA2 Enterprise**

Authentification

- Critère de sécurité : **Confidentialité**
- Garantie que les seuls personnes autorisées ont accès à l'information
- Deux grands types d'authentification :
  - **Authentification locale** : les informations d'authentification sont stockées sur le périphériques où l'on doit s'authentifier
  - **Authentification distante** : les informations d'authentification sont stockées sur des serveurs distants où l'on doit s'authentifier à l'aide de protocoles

Authentification locale

- Création d'un compte utilisateur/mot de passe
  - **Routeur(config)#username test secret cisco**
  - **Routeur(config)#username test1 secret cisco1**
- Configuration des listes d'authentification locales
  - Activer globalement l'authentification
  - Créer une liste d'authentification **LOCAL_AUTH**
  - Authentifier les connexion sur les lignes **console** et **vty** en utilisant la bases de données locales :
  - **R1(config)#aaa new-model**
  - **R1(config)#aaa authentication login LOCAL_AUTH local**
  - **R1(config)#line console 0**
  - **R1(config-lin)#login authentication LOCAL_AUTH**
  - **R1(config-lin)#line vty 0 4 (5 connexions simultanées)**
  - **R1(config-lin)#login authentication LOCAL_AUTH**

Types et authentification

- Possibilités d'authentification
  - **R1(config)#aaa authentication login LOCAL_AUTH ?**

`local`	Uses the local username database for authentication.
`local-case`	Uses case-sensitive local username authentication.
`none`	Uses no authentication.
`group radius`	Uses the list of all RADIUS servers for authentication.
`group tacacs+`	Uses the list of all TACACS+ servers for authentication.

- Authentification de secours
  - Choisir par ordre de priorité la méthode d'authentification
  - **R1(config)#aaa authentication login LOCAL_AUTH local group radius**

Les protocoles AAA

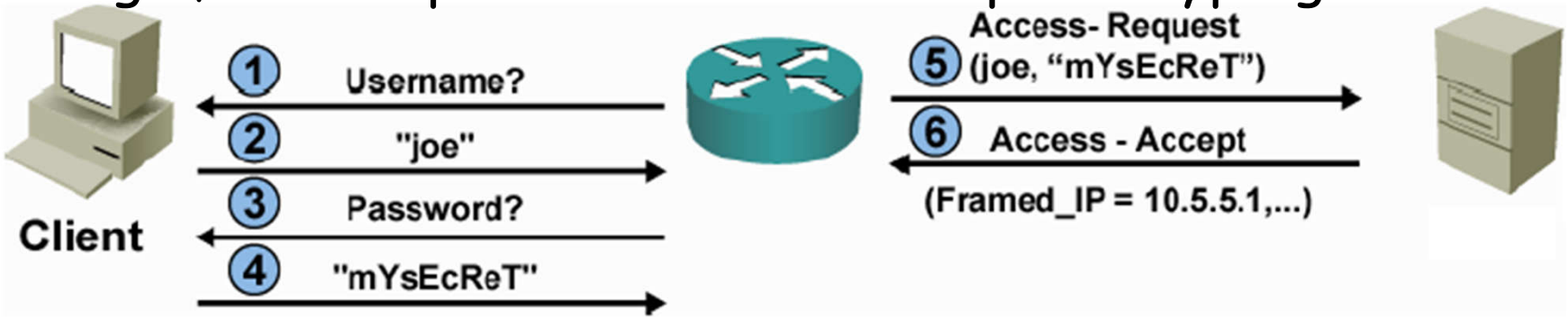
- Le terme AAA englobe trois notions
  - **Authentication** : Authentification des utilisateurs
  - **Authorization** : Autorisation (droits d'accès)
  - **Accounting** : Traçabilité
- Les routeurs peuvent utiliser leurs bases de données locales pour accomplir ces fonctions ou d'autres protocoles associés à des serveurs
- Les protocoles AAA les plus utilisés sont
  - Radius (*Remote Authentication Dial-In User Service*)
  - Tacacs (*Terminal Access Controller Access-Control System*), propriétaire de Cisco
- Nous verrons le protocole Radius dans le cadre de ce cours (standard)

Radius

- Protocole standard (**RFC 2865**) largement utilisé par les FAI pour authentifier les utilisateurs (ADSL)
- Assure le transport des données d'authentification de façon normalisée entre le client et le Serveur
- **Serveur Radius**
  - Relié à une base données d'identification locale ou externe (BD SQL, Annuaire LDAP)
  - Utilise le port **UDP 1645**
  - Transactions entre serveur et client chiffrées et authentifiées grâce à une **clé secrète partagée**
- **Client Radius**
  - NAS (Network Access Server)
  - Équipement établissant la connexion au serveur

Architecture client serveur

- Client NAS (Network Access Server)
  - Equipement qui désire s'authentifier et bénéficier des autorisation nécessaires
- Serveur Radius
  - Permet l'authentification et ensuite procure les autorisations nécessaires au NAS
- Paramètres de la transaction
  - Login, mot de passe et clé secrète pour cryptage



Fonctionnement de l'identification

- Fonctionnement par étapes
  - Le client radius (NAS) demande au poste deux paramètres (login et ensuite mot de passe)
  - Le client génère une requête ***Access-Request*** contenant les informations d'authentification
    - Mot de **passe crypté** mais **login en clair**
  - Le serveur consulte sa base et donne une des réponses
    - **ACCEPT** : l'identification a réussi
    - **REJECT** : l'identification a échoué
    - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge ») ;
  - Le serveur retourne ensuite les autorisations spécifiques à l'utilisateur authentifié

Autorisations et traçabilité

- Centralisation des paramètres de sécurité
- Autorisations : permet d'enrichir les identifications avec d'autres paramètres
  - Adresse IP fixe
  - Temps de connexion
  - Temps d'inactivité
- Accounting
  - Journalisation (logs des accès)
  - Facturation
- RADIUS est très utilisé pour l'identification des clients ADSL d'un fournisseur d'accès
  - Permet leur authentification et la facturation

Limitations de radius

- Radius est utilisé avec UDP
  - Utiliser UDP pour un débit plus important
  - Utiliser TCP pour plus de sécurité
- Radius base son identification login+mot de passe
  - Avec les mobiles d'autres numéros (IMEI)
- Radius utilise un transport en clair ou seul le mot de passe est crypté
  - Pris en compte dans TACACS
- RADIUS n'assure pas de mécanisme d'identification du serveur
  - Une machine peut se faire passer pour un serveur Radius et détourner le trafic du NAS

Configuration de Radius

- Configurer préliminaires du serveur RADIUS
  - @IP du routeur NAS
  - Port 1645
  - Comptes utilisateurs et clé secrète partagée
- Configuration du routeur pour RADIUS
  - **Router(config)# aaa new-model**
  - **Router(config)# aaa authentication login lprt3 group radius**
- Indiquer l'adresse IP du serveur radius et la clé
  - **Router(config)# radius-server host 192.168.10.2 auth-port 1645 key macle1**
- Activer les connexions à distance sur le NAS
  - **Router(config)# line vty 0 4**
  - **Router(config)# login authentication lprt3**