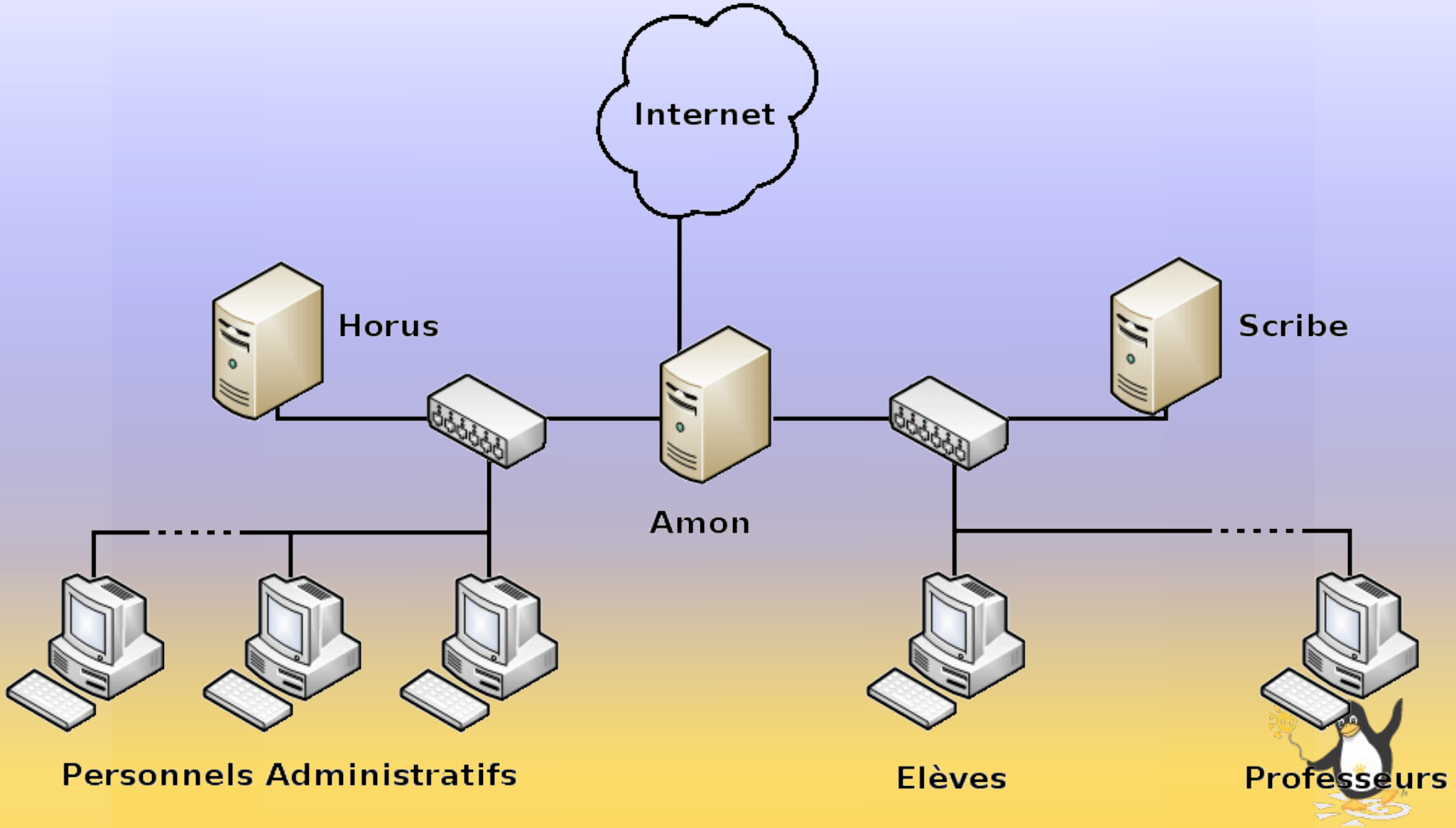
Séminaire EOLE
DIJON
23 et 24 Octobre 2008

802.1x et RADIUS

Introduction (1)

- Actuellement, chaque groupe d'utilisateur doit utiliser un ensemble d'ordinateurs précis.
  - Personnels administratifs, professeurs, élèves.
  - Bâtiments administratifs, salle des professeurs, CDI ou salle de cours de Technologie.
- L'accès aux ressources est géré de manière géographique.
- D'où vient l'utilisateur ?

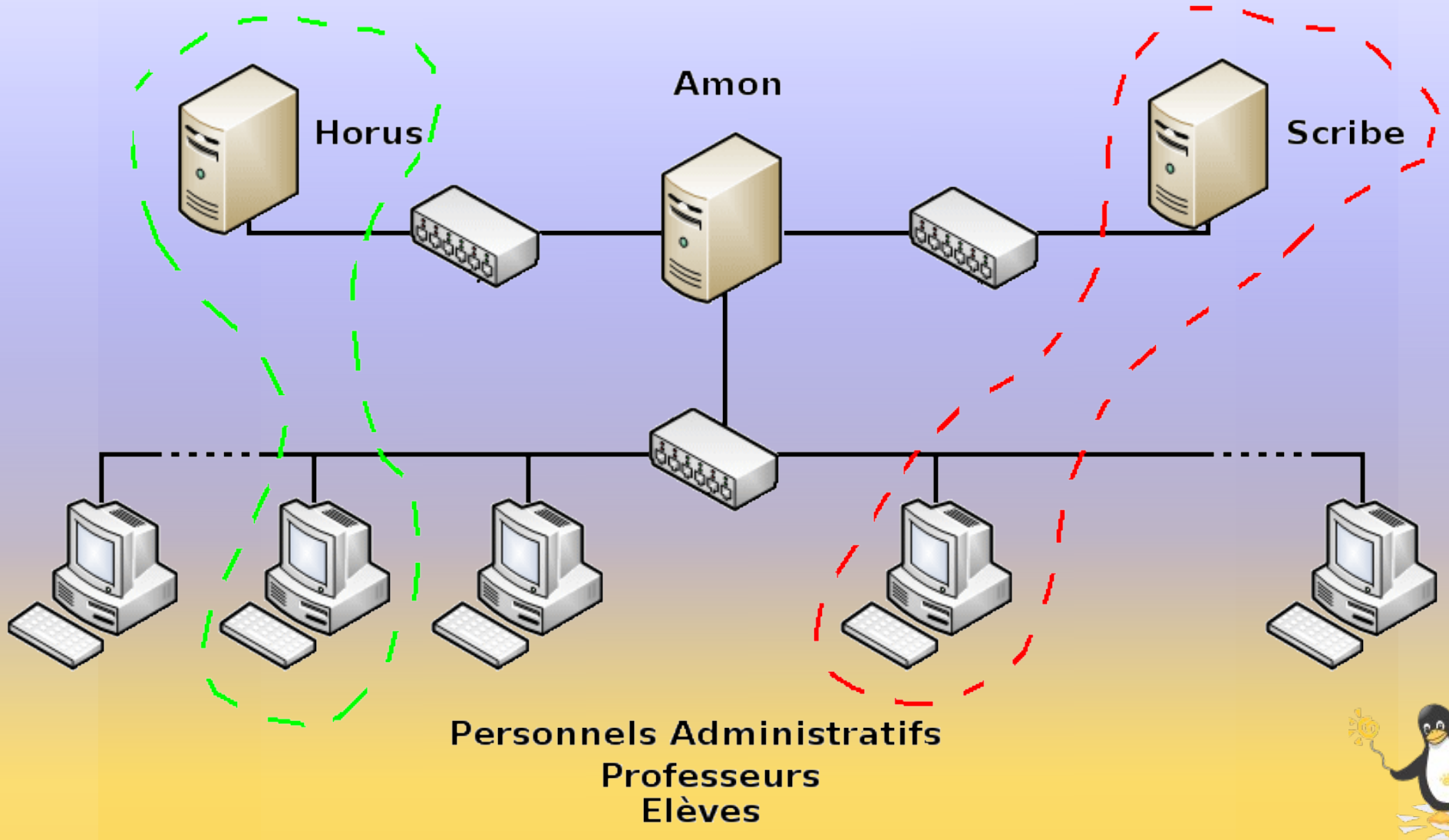
Introduction (2)



Introduction (3)

- Objectif : permettre le nomadisme entre les postes de l'établissement.
  - Un ordinateur doit pouvoir être utilisé par n'importe quel membre de l'établissement.
- Pour cela, une des solutions est de mettre en place un attribution dynamique des VLAN.
  - Chaque type d'utilisateur est sur un réseau différent.
  - Les accès aux ressources sont simplifiés.
- Qui est l'utilisateur ?

Introduction (4)



802.1x ?

- Décrit le contrôle d'accès à un réseau.
- Mis au point en 2001 par le groupe de travail IEEE 802
- Permet de réguler les accès aux réseaux depuis des ports libres, en restreignant l'accès de clients non identifiés ou non autorisés.
- Repose sur l'utilisation d'EAP (Extended Authentication Protocol) pour transporter les informations d'identification des utilisateurs.

Objectif de 802.1x

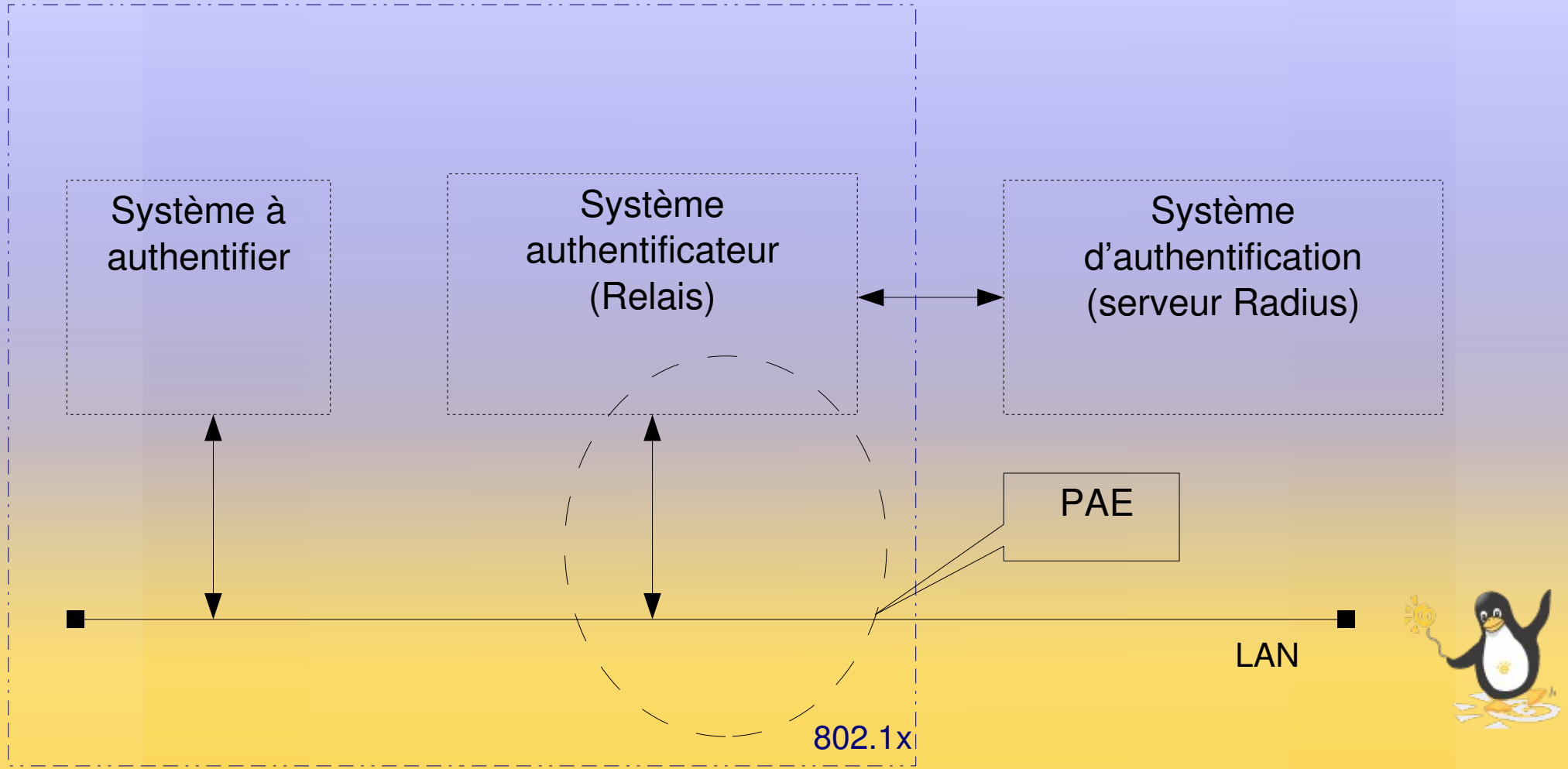
- Sécuriser l'accès au réseau, dès la connexion d'un client sur l'un des équipements d'extrémité.
- Standardiser un mécanisme de relais d'authentification au niveau 2
  - Pour les accès via des interfaces IEEE 802{.3 .5 .11}
  - Pour permettre un contrôle d'accès aux ressources
  - Même si l'accès physique au réseau n'est pas contrôlable
  - Exemples
    - Accès Internet depuis une aire publique
    - Affectation à un VLAN donné en fonction de l'authentification

Utilité de 802.1x

- Sécuriser les réseaux.
  - Assure une validation de l'accès au médium.
  - Limite en amont les intrusions sur le réseau.
  - Enregistre éventuellement les opérations de chaque utilisateur.
- Faciliter la gestion pour les administrateurs.
- Permettre la mobilité des utilisateurs.
  - Banalisation des postes.
  - Intégration des postes nomades (portables, terminaux, etc.)
  - Prise en compte des connexions sans fil.

Principes (1)

- Interaction entre 3 acteurs



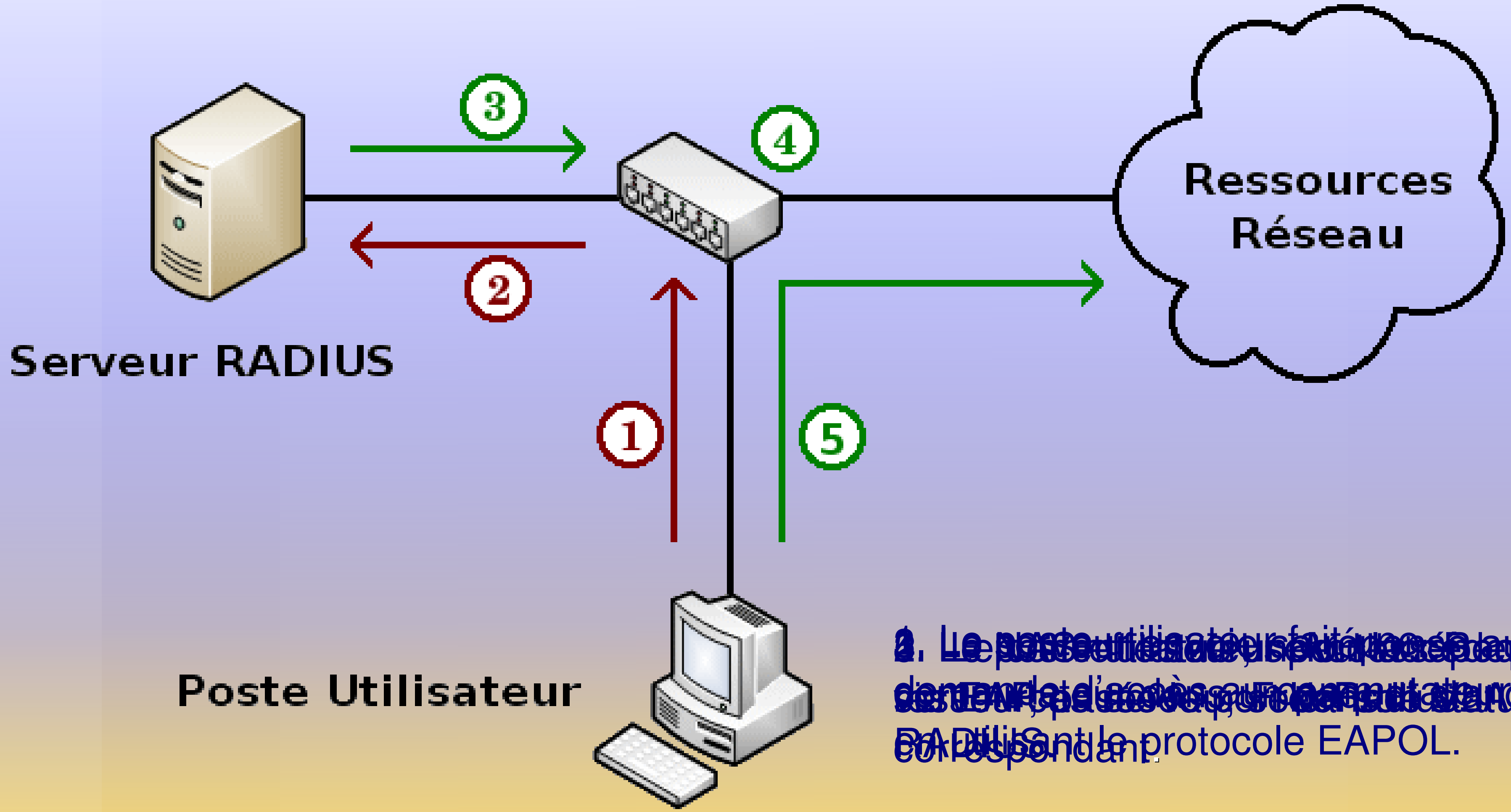
Principes (2)

- Système à authentifier (supplicant) :
  - Client, équipement qui a besoin de se faire authentifier sur le réseau.
  - Utilise EAP pour dialoguer avec l'Authenticator.
- Système authentificateur (Authenticator)
  - Équipement (de niveaux 2 ou 3) qui assure la sécurité 802.1x sur l'interface et l'accès au réseau.
  - Gère un PAE (Port Access Entity) qui permettra au Supplicant d'accéder ou non aux ressources du réseau.
  - Fait la transition des informations du Supplicant au serveur d'authentification.

Principes (3)

- Système d'authentification (Authentication Server)
  - Équipement qui valide ou non les informations fournies par l'Authenticator.
  - Fournit les informations relatives au compte de l'utilisateur authentifié (VLAN, ACL, DHCP).
  - Différents serveurs d'authentification :
    - En local dans l'authenticator.
    - TACAC, TACAC+.
    - RADIUS (le plus utilisé).
    - DIAMETER (successeur de RADIUS).

Fonctionnement (1)



1. Le poste utilisateur fait une demande d'accès au commutateur en utilisant le protocole EAPOL.

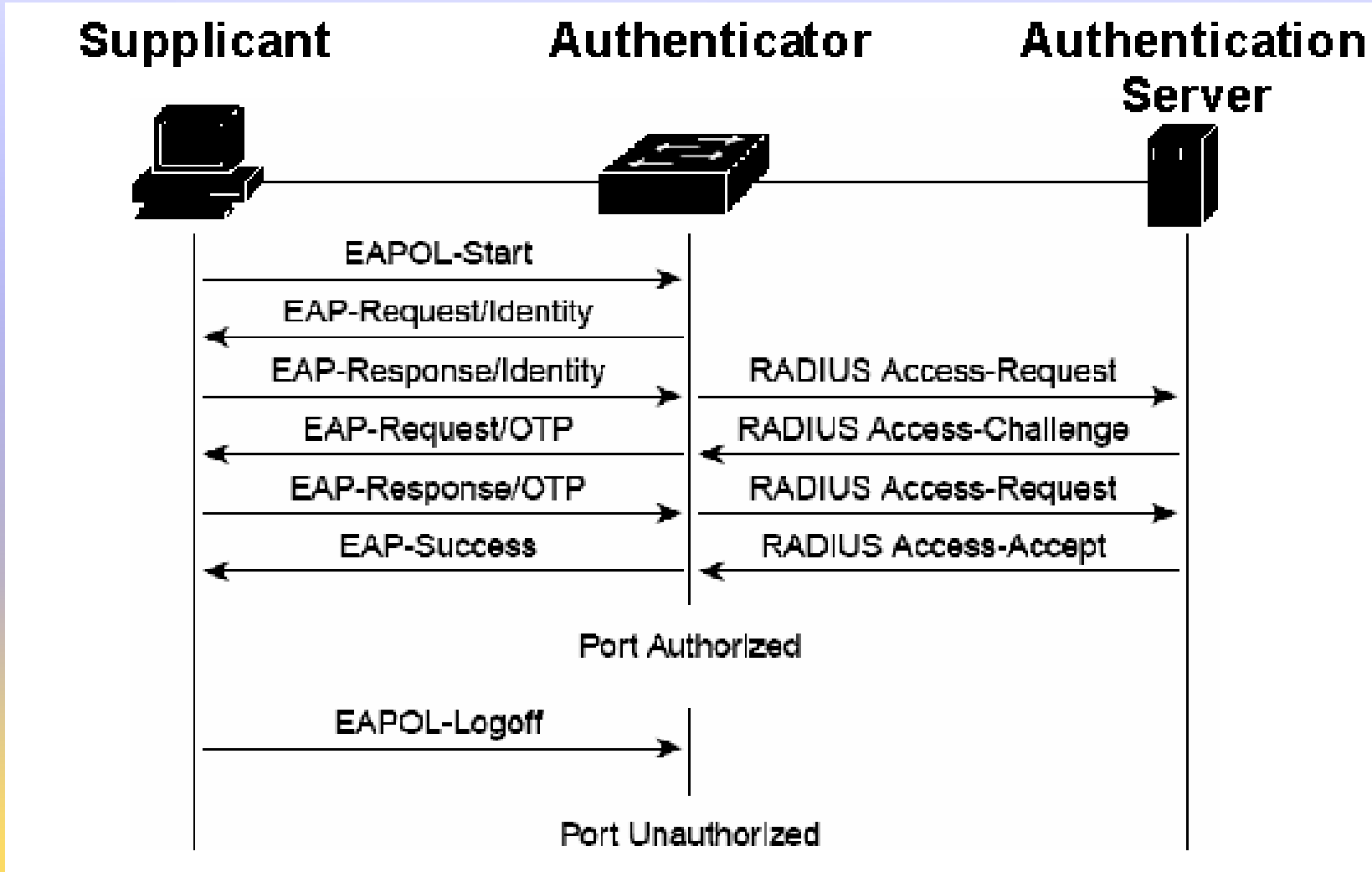
Fonctionnement (2)

- Phase 1 :
  - Connexion d'une station à l'équipement d'accès.
  - Par défaut, le port de l'équipement est fermé.
- Phase 2 :
  - Demande d'authentification du client de la part de l'équipement d'accès.
- Phase 3 :
  - Le client fournit son certificat d'authentification à l'équipement.

Fonctionnement (3)

- Phase 4 :
  - L'équipement propage ce certificat jusqu'au serveur d'authentification.
- Phase 5 :
  - Le serveur d'authentification vérifie le profil de l'utilisateur, valide (ou non) le certificat, autorise (ou non) l'accès au réseau puis renvoi sa réponse à l'équipement.
- Phase 6 :
  - Si le serveur d'authentification accepte le certificat, alors l'équipement ouvre son port et le trafic peut être diffusé.
  - Le client peut accéder aux ressources réseau.
  - Sinon, le port reste dans son état initial et le trafic est bloqué.

Fonctionnement (4)



Fonctionnement (5)

État d'un port :

- L'état d'un port varie en fonction du résultat de la requête d'accès.
- Le port contrôlé peut prendre deux états :
  - Authorized : dans ce cas le port est passant pour tout le trafic.
  - Unauthorized : dans ce cas le port est bloquant pour tout le trafic.

Fonctionnement (6)

État d'un port :

- Par défaut, port en mode unauthorized.
- Connexion, requête d'authentification :
  - Port en mode authorized si authentification valide.
  - Port en mode unauthorized si authentification pas valide.
- Déconnexion, port en mode unauthorized.
- Client ne supportant pas le 802.1x, port en mode unauthorized (possibilité d'activation du port avec accès restreint).

Fonctionnement (7)

Configuration dynamique.

- Mise en place de services supplémentaires grâce à la centralisation des profils au niveau d'un serveur RADIUS.
  - Affectation dynamique de VLAN
  - Association dynamique à un pool DHCP
  - Affectation dynamique de règles de sécurité (Access List - ACL)
  - ...

Fonctionnement (8)

Configuration dynamique de VLANs.

- Un port peut être placé de façon dynamique dans un vlan en fonction de la réussite ou de l'échec de l'authentification.
- L'affectation dynamique des VLANs se configure sur le serveur RADIUS.
- 3 comportements d'attribution sur un port 802.1x :
  - Pas de VLAN (échec d'authentification, etc.)
  - Guest VLAN (Connexion d'un client ne supportant pas l'authentification).
  - VLAN spécifique à l'utilisateur (authentification réussi et affectation d'un VLAN par radius).

RADIUS(1)

- Remote Access Dial In User Service.
- Conçu pour répondre aux problème d'authentification des accès distants par liaison téléphonique.
- Permet l'application du protocoles AAA (Authentication, Authorization, Accounting).
- Offre une sécurité avancée pour des systèmes de points d'accès au réseau.
- Deux sortes d'authentification RADIUS :
  - Basée sur l'adresse MAC de la carte Ethernet.
  - Basée sur le protocole 802.1x.

RADIUS(2)

- Principe de base :
  - Fournir un modèle d'échange d'information de l'authentification
  - Permettre le transport des données d'authentification MAC ou EAP.
- Va être utilisé entre deux acteurs :
  - Le serveur Radius qui délivre ou non une autorisation au client.
  - Le client Radius (NAS: Network Autorisation System) qui est le commutateur qui demande s'il doit, ou non autoriser l'entité distante a se connecter au réseau.
- L'entité qui se connecte sur le réseau n'a pas a connaître le protocole Radius.
- Le serveur Radius peut identifier les entités grâces à la une base d'utilisateur dans un annuaire LDAP.

RADIUS(3)

- Authentification Radius 802.1x
  - L'entité qui se connecte fournit des informations au commutateur au travers du protocole EAP.
  - Le dialogue qui s'instaure entre l'entité et le serveur se fait indirectement par l'intermédiaire du NAS via le protocole Radius.
  - Cela implique l'utilisation d'un logiciel spécifique sur le client qui saura parler 802.1x.

Mise en place(1)

- Sur le Supplicant :
  - Activation de 802.1x
  - Choix de la méthode EAP.
- Sur l'Authenticator :
  - Activation du 802.1x sur les ports.
  - Redirection vers l'Authentication Server.
  - Règles de sécurité sur les ports ou la borne.

Mise en place(2)

- Sur l'Authentication Server
  - Création des profils.
  - Mise en place des règles de sécurités sur les profils.
  - Liens externes (LDAP, DHCP).

Principal inconvénients

- Nécessite une configuration spécifique sur chacun des postes client (installation des certificats et configuration de la méthode d'authentification).
- Nécessite des équipements réseau compatibles avec ce protocole (mineur puisque la plupart d'entre eux le sont désormais).
- Difficulté de fournir une configuration clef en main car une partie est spécifique au type d'équipement.

Perspectives Eole(1)

- Phase 1 :Réalisation d'une maquette.
  - Installation et configuration de RADIUS sur Amon.
  - Couplage RADIUS avec l'annuaire LDAP de Scribe.
  - Affectation des VLANs en fonction des utilisateurs.
  - Début de templatisation des fichiers de configurations.

Perspectives Eole(2)

- Phase 2 : Mise en place dans un établissement pilote.
  - Dans un premier temps, sur le réseau pédagogique afin d'affecter des ressources différentes en fonction des communautés.
  - Prise en compte de réseaux WIFI et des postes nomades.
  - Par la suite, banalisation du poste client.
- Phase 3 : Mise à disposition sur les modules Eole.

Merci de votre attention