

Sécurité informatique

INF36207

Systèmes d'authentification, d'autorisation et de traçabilité.

Kerberos, NTLM, Radius, TACACS, LDAP, AD et AzureAD. Protocoles OAUTH & SAML. Protocole EAP/PAP/CHAP.

Martin Arsenault, ing., MBA, MGP

Hiver 2023



Pour ce soir...

- Retour sur le TP#3 déposé ce weekend
- Théorie sur AAA



Qu'est-ce que le AAA ?

- AAA est un acronyme couramment utilisé dans le domaine de la sécurité informatique pour décrire les trois éléments clés de l'authentification, de l'autorisation et de la comptabilité (en anglais, Authentication, Authorization, and Accounting).
- C'est un cadre architectural permettant d'accéder aux ressources informatiques, d'appliquer des politiques, d'auditer l'utilisation, de fournir les informations essentielles requises pour la facturation des services et d'autres processus essentiels à la gestion et à la sécurité du réseau.
- Ce processus est principalement utilisé pour que les ressources du réseau et des applications logicielles soient accessibles aux utilisateurs légitimes (via l'authentification) pour ce qu'ils sont autorisés à faire (via l'autorisation) et capturer les actions effectuées (via la comptabilité).
- Dans l'ensemble, le concept AAA est essentiel pour la sécurité informatique car il permet de garantir que seuls les utilisateurs autorisés ont accès aux ressources, et que leurs activités peuvent être surveillées et contrôlées pour éviter les atteintes à la sécurité.

Implémentation du AAA

- La fonction AAA peut être implémentée en utilisant une base de données locale ou en utilisant un serveur de contrôle d'accès sécurisé (ACS).
 - Base de données locale sur le système :
 - Système de gestion d'utilisateurs directement intégré au système gérant l'accès.
 - Serveur ACS :
 - Méthode la plus couramment utilisée en entreprise.
 - Un ACS est utilisé pour la fonction AAA (ou une partie) sur lequel une configuration le liant au système à accéder est réalisée.
 - L'ACS est donc désigné comme système de référence pour assurer les fonctions de contrôle d'accès et garantie que l'utilisateur est la bonne personne.

Authentication / Authentification

- L'authentification fait référence au processus de vérification de l'identité d'un utilisateur ou d'un système.
- Le processus implique généralement un nom d'utilisateur, des mots de passe, des cartes d'identité ou d'autres méthodes pour confirmer l'identité de la personne ou du système qui accède aux données ou aux ressources.
- L'authentification afin d'être plus robuste peut être garantie par une méthode de double authentification (2FA, MFA, etc.)
- Ces méthodes incluent l'utilisation d'une base de données locale sur l'appareil même ou l'envoi de demandes d'authentification à un serveur externe tel que le serveur ACS.



Authorization / Autorisation

- L'autorisation fait référence aux règles et aux politiques qui déterminent ce que les utilisateurs ou les systèmes sont autorisés à faire une fois qu'ils ont été authentifiés.
- Cela peut inclure des autorisations d'accès à des fichiers ou des ressources spécifiques, ou des restrictions d'accès à certaines zones ou fonctions du système.
- Cette fonction peut également appliquer des politiques sur des ressources ou sur l'utilisateur en fonction des privilèges qui lui sont conférés.

ACCESS DENIED

ACCESS GRANTED

Accounting / Comptabilité (Traçabilité)

- La comptabilité fait référence au suivi des activités des utilisateurs et des systèmes, y compris les tentatives d'authentification, les autorisations accordées ou refusées, et l'utilisation des ressources.
- La comptabilité permet de détecter les activités suspectes ou non autorisées et de fournir des informations sur l'utilisation du système pour la gestion et la planification.
- Cette fonction fournit des moyens de surveiller et de capturer les événements effectués par l'utilisateur lors de l'accès aux ressources. Elle peut même surveiller la durée d'accès aux ressources.



AAA → Avantages et inconvénients

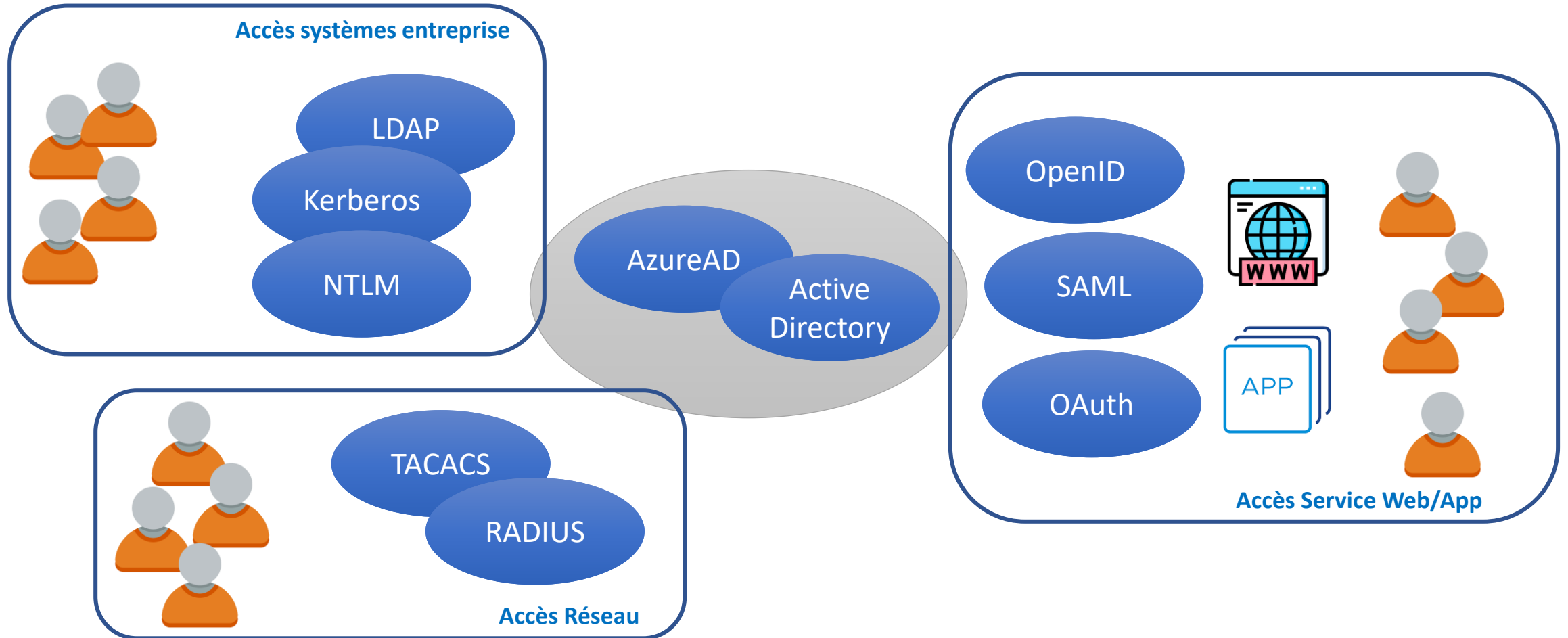
- Avantages

- AAA augmente l'évolutivité d'un réseau, soit la propriété d'un système de gérer une quantité croissante de travail en ajoutant des ressources au système.
- Cela entraîne une flexibilité accrue et un meilleur contrôle du réseau.
- Il aide à maintenir les protocoles standard dans le réseau en permettant le maintien d'informations d'identification uniques pour chaque utilisateur.
- Les administrateurs informatiques disposeront d'un point central pour l'authentification des utilisateurs et du système.

- Inconvénients

- Sur les ACS, la configuration et l'installation initiale peuvent être compliquée et chronophage.
- Il est très difficile de déterminer quel est le meilleur outils AAA à implémenter dans une organisation en raison des différents systèmes en place et de leur intégration.
- La maintenance peut être difficile et chronophage pour le matériel sur site.

Interactions des différents protocoles et systèmes d'authentification



Active Directory

- Un **répertoire d'entreprise** est une structure hiérarchique qui stocke des informations sur les objets du réseau. Un répertoire, au sens le plus générique, est une liste complète d'objets.
 - Ex : Un annuaire téléphonique est un type de répertoire qui stocke des informations sur les personnes, les entreprises et les organisations gouvernementales. Les annuaires téléphoniques enregistrent généralement les noms, les adresses et les numéros de téléphone.
- Active Directory (AD) est une technologie Microsoft utilisée pour gérer des ordinateurs et d'autres appareils sur un réseau. Il s'agit d'une fonctionnalité principale de Windows Server, un système d'exploitation qui exécute à la fois des serveurs locaux et basés sur Internet.
- **Avantages**
 - Structure organisationnelle hiérarchique permettant un point d'accès unique aux ressources du réseau.
 - Authentification et réplication multiples systèmes avec possibilité de créer des relations de confiance avec des réseaux externes.
 - Fournit un emplacement centralisé pour la gestion des comptes d'utilisateurs et d'ordinateurs, ce qui peut faire gagner du temps et accroître l'efficacité des administrateurs informatiques. Cela permet également une application cohérente des politiques de sécurité et des autorisations.
 - Il fournit une gamme de fonctionnalités de sécurité, notamment des stratégies de mot de passe, des stratégies de groupe et des contrôles d'accès, qui peuvent aider à protéger le réseau contre les accès non autorisés et les activités malveillantes.
 - Conçu pour prendre en charge de grands réseaux avec de nombreux utilisateurs et appareils, et peut facilement évoluer pour répondre aux besoins des organisations en pleine croissance. Cela inclut la possibilité d'ajouter des contrôleurs de domaine et des serveurs supplémentaires selon les besoins.
 - Facilite le partage de ressources telles que des fichiers et des imprimantes sur le réseau et la gestion de l'accès à ces ressources via des autorisations et des paramètres de sécurité.
 - Des fonctionnalités complètes d'audit et de création de rapports, qui peuvent aider les organisations à suivre les modifications et l'activité sur le réseau, et à identifier les problèmes de sécurité potentiels.

Active Directory

- **Service d'annuaire** – Un service d'annuaire est un arrangement hiérarchique d'objets structurés de manière à en faciliter l'accès. Cependant, fonctionner comme un service de localisation n'est pas l'objectif exclusif d'AD. Il aide également les organisations à disposer d'une administration centrale sur toutes les activités menées dans leurs réseaux. Essentiellement un service d'annuaire réseau :
 - Fournit des informations sur les objets utilisateur, les ordinateurs et les services du réseau.
 - Stocke ces informations dans une base de données sécurisée et fournit des outils pour gérer et rechercher le répertoire.
 - Permet de gérer les comptes d'utilisateurs et les ressources, d'appliquer les politiques de manière cohérente selon les besoins d'une organisation.
 - Active Directory fournit plusieurs services différents, regroupés sous l'égide des « services de domaine Active Directory », ou AD DS. Ces prestations comprennent :
- **Services de domaine** – Stocke des données centralisées et gère la communication entre les utilisateurs et les domaines. Comprend également l'authentification de connexion et la fonctionnalité de recherche
- **Services de certificats** – Il génère, gère et partage des certificats. Un certificat utilise le cryptage pour permettre à un utilisateur d'échanger des informations sur Internet en toute sécurité avec une clé publique.
- **Services d'annuaire légers** – Prend en charge les applications d'annuaire utilisant le protocole ouvert (LDAP).
- **Répertoire de fédération** - Fournit une authentification unique (SSO) pour authentifier un utilisateur dans plusieurs applications Web en une seule session.
- **Gestion des droits** - Il contrôle les droits et la gestion des informations. AD chiffre le contenu, tel que les e-mails ou les documents Word, sur un serveur pour limiter l'accès.

Ce que contient un AD

Contrôleurs de domaine – Un serveur qui exécute AD DS est appelé contrôleur de domaine. Les contrôleurs de domaine hébergent et répliquent la base de données du service d'annuaire à l'intérieur de la forêt. Le service d'annuaire fournit également des services de gestion et d'authentification des ressources dans la forêt. Ces serveurs hébergent des services essentiels dans AD DS, notamment : – Kerberos Key Distribution Center (kdc) – NetLogon (Netlogon) – Windows Time (W32time) – Intersite Messaging (IsmServ)

Schéma – Un ensemble de règles, le schéma, qui définit les classes d'objets et d'attributs contenus dans l'annuaire, les contraintes et limites sur les instances de ces objets, et le format de leurs noms.

Catalogue global – Un catalogue global qui contient des informations sur chaque objet du répertoire. Cela permet aux utilisateurs et aux administrateurs de trouver des informations sur l'annuaire, quel que soit le domaine de l'annuaire qui contient réellement les données. Pour plus d'informations sur le catalogue global, voir Rôle du catalogue global

Domaine racine de la forêt – Le premier domaine installé dans une forêt Active Directory est appelé domaine racine

Sites – Les sites dans AD DS représentent la structure physique, ou topologie, de votre réseau. AD DS utilise les informations de topologie du réseau, qui sont stockées dans l'annuaire en tant qu'objets de site, de sous-réseau et de lien de site, pour créer la topologie de réplication la plus efficace

Protocole d'accès à l'annuaire léger - AD est basé sur le protocole LDAP (Lightweight Directory Access Protocol). Ce protocole fournit un langage commun permettant aux clients et aux serveurs de se parler.

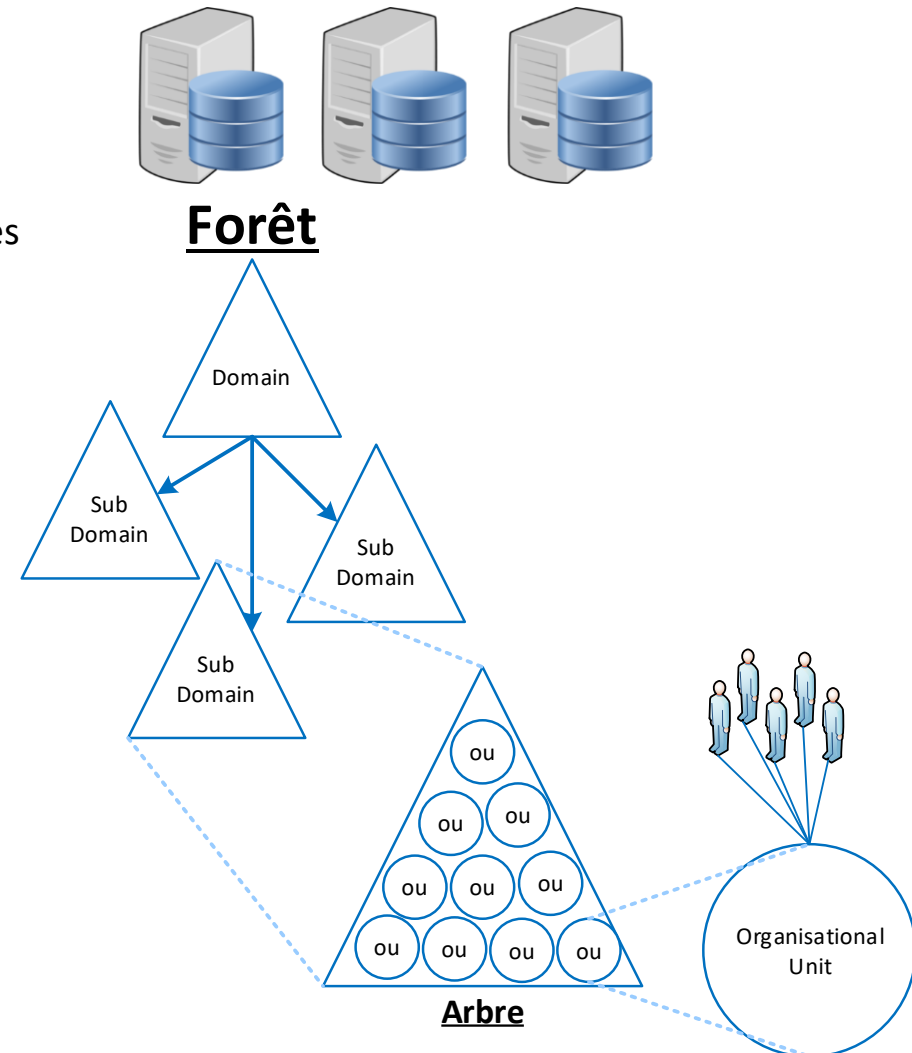
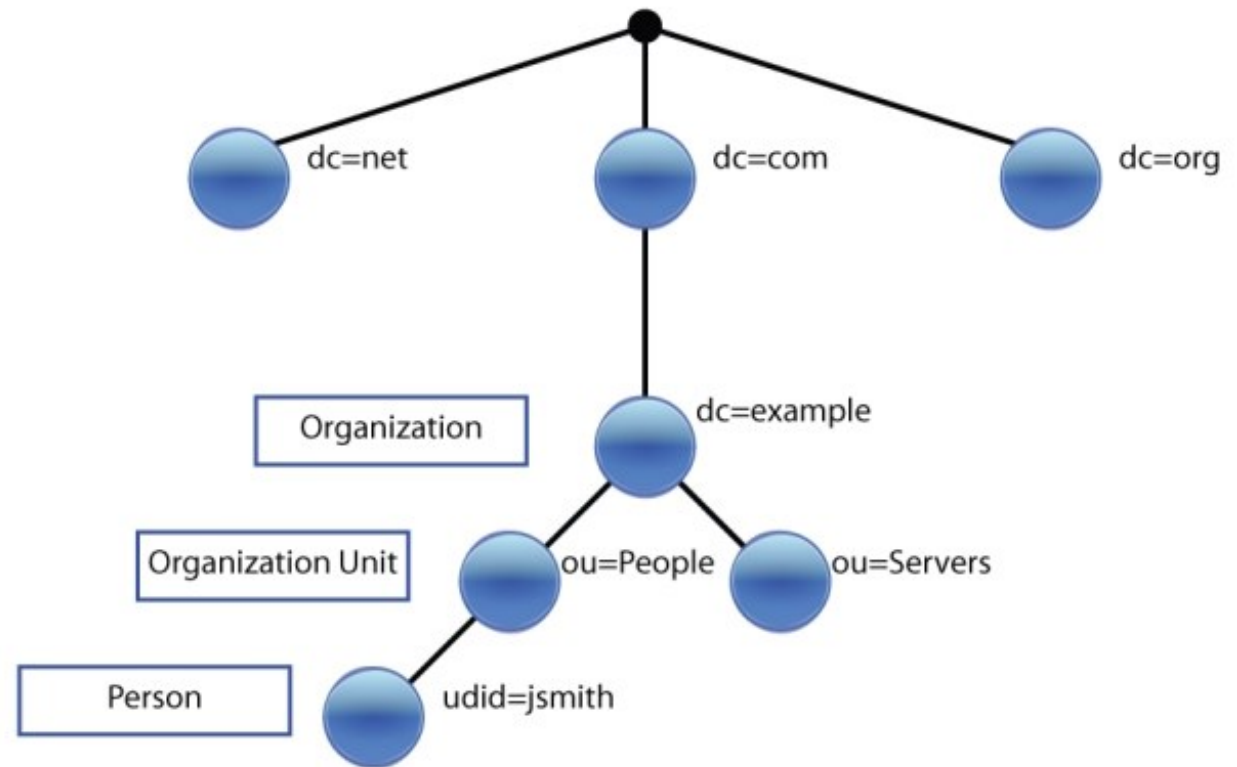


Schéma d'un AD



Comment sécuriser l'AD ?

- Réduction de la surface d'attaque (comptes/groupes haut privilège, postes spécifiques, etc.)
- Surveillance des signes de compromission
- Anti-virus et anti-programme malveillant
- Mise à jour (OS + Applicatives)
- Logiciel de gestion des vulnérabilités
- Configuration complète et correcte
- Contrôleurs de domaine sécurisé
- Limiter les privilèges excessifs
- Comptes privilégiés permanents / VIP
- Évitez les comptes attrayants (i.e.: admin)
- Avoir un compte de secours

10 lois immuables en sécurité

Loi n° 1 : Personne ne croit que quelque chose de mal peut lui arriver, jusqu'à ce que cela se produise

Loi n° 2 : la sécurité ne fonctionne que si le moyen sécurisé est également le moyen le plus simple

Loi n° 3 : si vous ne suivez pas les correctifs de sécurité, votre réseau ne vous appartiendra pas longtemps

Loi n°4 : Il ne sert à rien d'installer des correctifs de sécurité sur un ordinateur qui n'a jamais été sécurisé au départ

Loi n°5 : La vigilance éternelle est le prix de la sécurité

Loi #6 : Il y a vraiment quelqu'un qui essaie de deviner vos mots de passe

Loi #7 : Le réseau le plus sécurisé est un réseau bien administré

Loi n°8 : La difficulté de défendre un réseau est directement proportionnelle à sa complexité

Loi #9 : La sécurité n'est pas une question d'évitement des risques ; c'est une question de gestion des risques

Loi #10 : La technologie n'est pas une panacée

Azure Active Directory

- Azure Active Directory (Azure AD) est un service de gestion des identités et des accès dans le **cloud**. Cette solution **facilite l'accès à des milliers d'applications SaaS supplémentaires**, au portail Azure et à des **ressources externes** telles que Microsoft 365 pour les membres de votre personnel. Ils peuvent également accéder à des **ressources internes** telles que des applications sur le réseau intranet de votre entreprise et toutes les applications cloud créées par votre propre entreprise grâce à Azure Active Directory.
- Vous pouvez également maintenir votre implémentation Active Directory sur site avec l'aide d'Azure AD. Expliqué simplement, Azure AD permet aux utilisateurs de s'inscrire à divers services et d'y accéder depuis n'importe quel endroit via le cloud en utilisant un seul nom d'utilisateur et mot de passe.
- **Pourquoi Azure AD ?**
 - Supposons que vous ayez une grande organisation avec de nombreux utilisateurs. Certains services Azure doivent être disponibles pour tous les utilisateurs pour qu'ils puissent s'acquitter de leurs responsabilités. Lorsque l'administrateur leur donne un nom d'utilisateur et un mot de passe uniques pour chaque service, ils peuvent accéder à des services tels que des systèmes et des services web, internes et externes. Il peut être difficile pour les administrateurs et les employés de gérer plusieurs connexions d'utilisateurs à la fois.
 - Azure Active Directory (AD) peut alors être utilisé. Les administrateurs peuvent facilement gérer de nombreuses connexions d'utilisateurs avec Azure AD. Pour accéder à chaque service, les administrateurs doivent fournir un identifiant et un mot de passe uniques.

Azure Active Directory

- **Authentification** : Pour accéder aux différents services, une vérification d'identité est nécessaire. L'inclusion de fonctionnalités telles que l'authentification multifacteur et la réinitialisation de mot de passe en libre-service fait également partie d'Azure AD.
- **Authentification unique** : Avec l'authentification unique (SSO), vous pouvez vous connecter à diverses applications avec un seul identifiant et un seul mot de passe.
- **Gestion des applications** : à l'aide d'Azure AD, vous pouvez gérer à la fois vos applications locales et basées sur le cloud.
- **Gestion des appareils** : Azure AD fournit l'enregistrement des appareils en plus des comptes pour des individus spécifiques. Il permet également des restrictions d'accès conditionnel basées sur l'appareil pour limiter les tentatives d'accès à celles provenant d'appareils connus.
- Bref, c'est l'implémentation infonuagique de l'Active Directory classique.



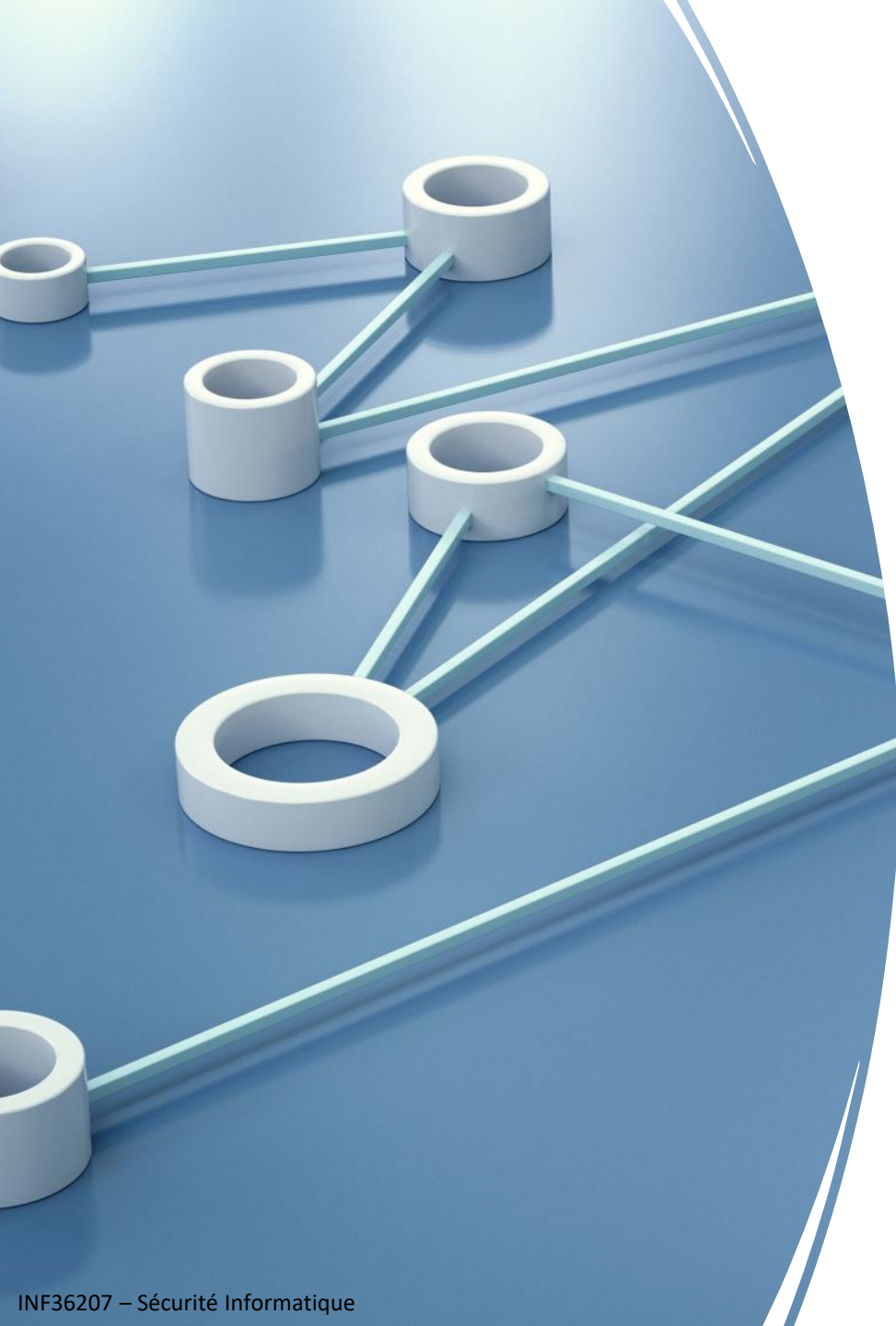
Azure Active Directory

SSO – Single Sign-On

(authentification unique)

- C'est une méthode d'authentification qui permet à l'utilisateur de se connecter une fois à un système et de réutiliser sa session active pour se rendre sur d'autres systèmes nécessitant une authentification.
- Assure une meilleure sécurité et une meilleure expérience pour l'utilisateur en rehaussant l'efficience et sa productivité.
- Il permet également de sauver des coûts et d'avoir un seul système centralisé d'authentification.



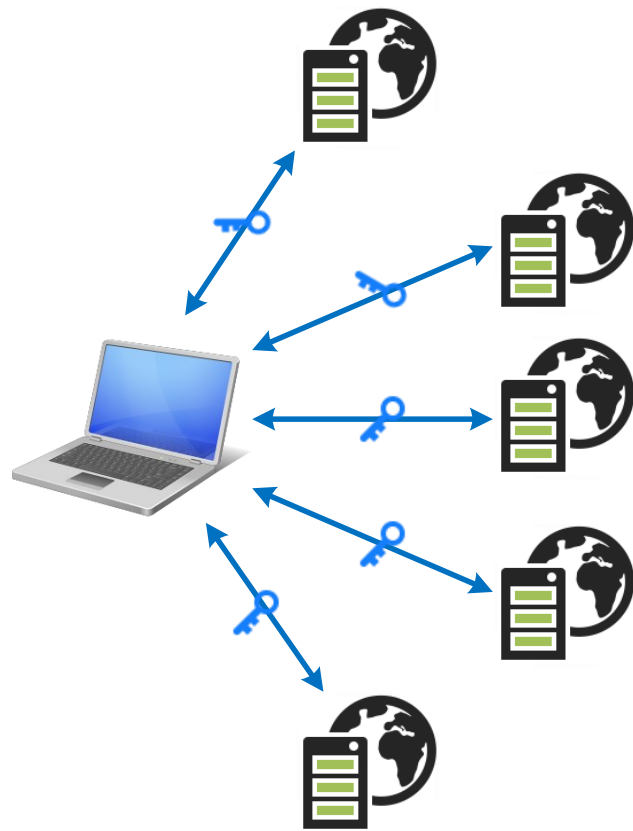


Fédération d'accès Fédération d'identité

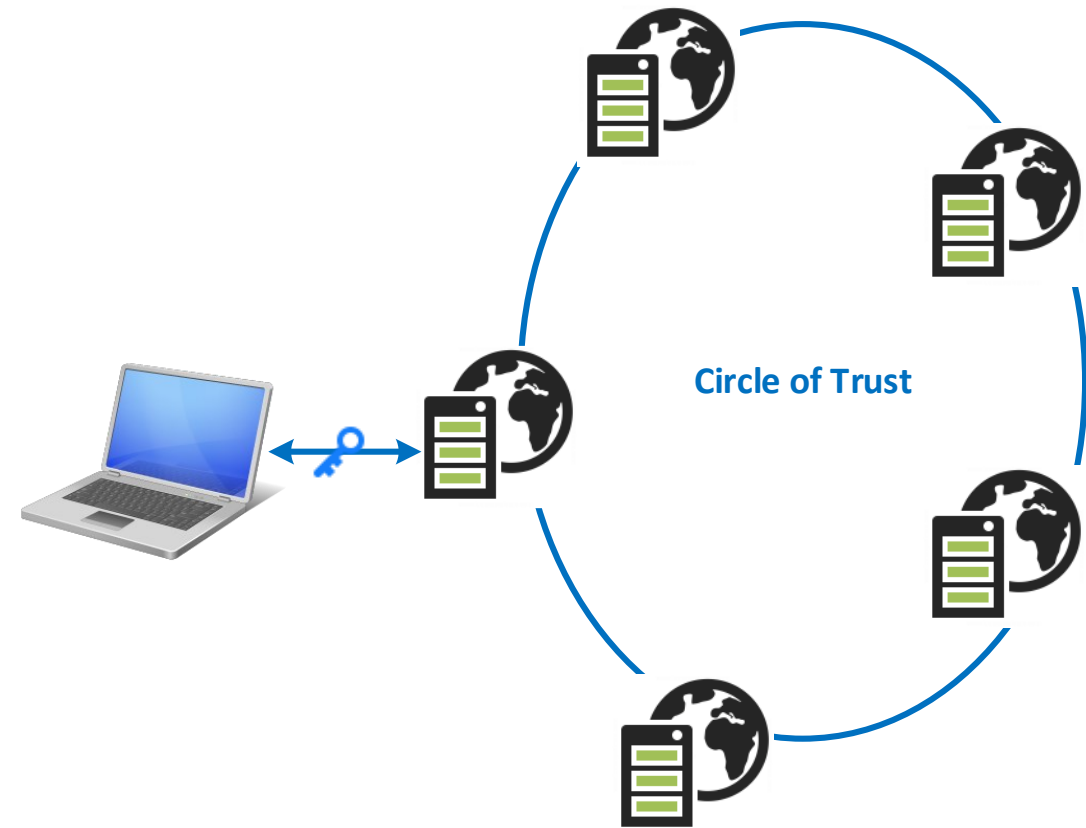
- Il s'agit d'un regroupement de confiance de plusieurs système d'authentification.
- Ceci permet à un utilisateur qui doit accéder à un système ou des systèmes qui ne sont pas géré par lui de s'y raccorder en ayant recours à ses identifiants et cela, même s'il est sur les infrastructures d'une autre organisation.
- Un bel exemple de cette mise en commun des systèmes est le réseau sans fil Eduroam

https://monitor.eduroam.org/map_service_loc.php

Fédération d'accès



Avec la fédération d'accès
5 accès 5 systèmes

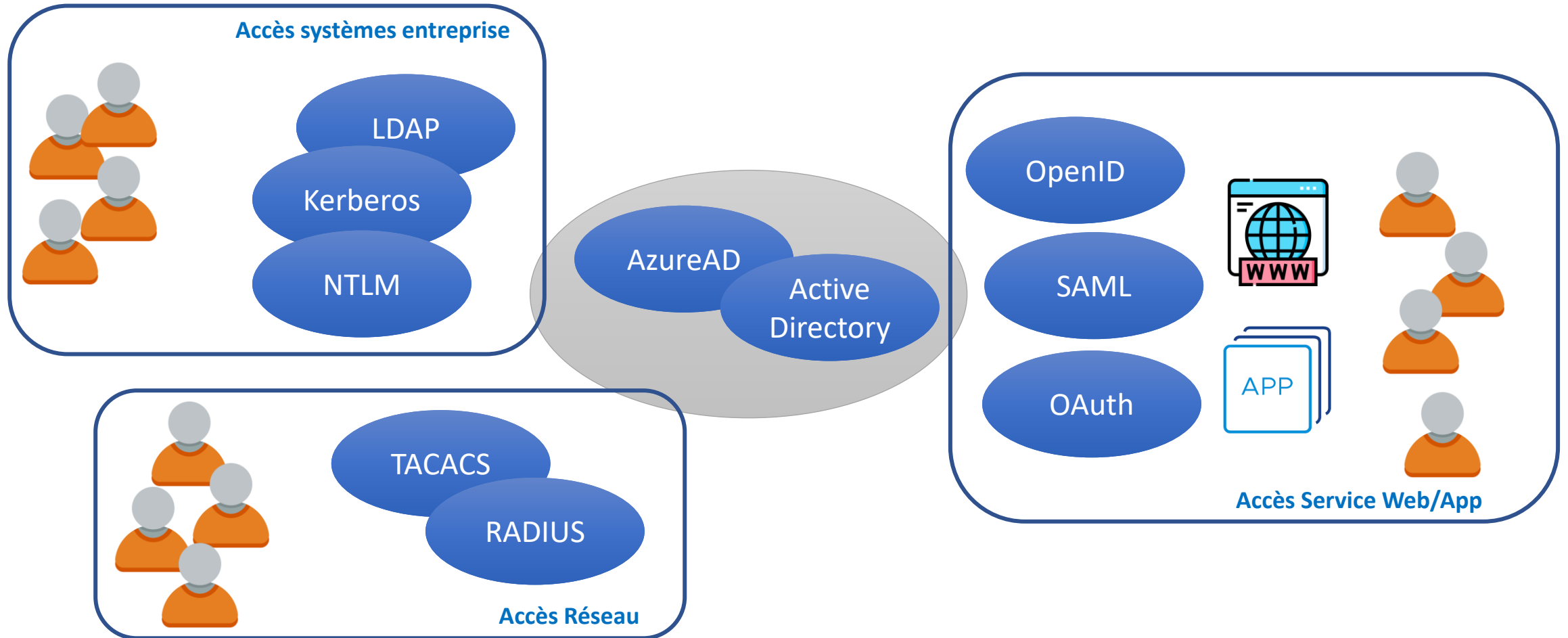


Avec la fédération d'accès
1 accès 5 systèmes

The image features three server racks in the foreground, each filled with various electronic components and displays. The background is a dark blue field with a complex, glowing white circuit board pattern. The title 'Systèmes et protocoles' is centered over the image in a large, white, serif font.

Systèmes et protocoles

Interactions des différents protocoles et systèmes d'authentification



Qu'est-ce que LDAP ?

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole Internet fonctionnant sur TCP/IP, utilisé pour accéder aux informations des répertoires(AD). Le protocole LDAP est essentiellement utilisé pour accéder à un répertoire actif.

Simple d'utilisation :

- Le modèle fonctionnel de LDAP est plus simple car il omet les fonctionnalités en double.
- Il est facile à comprendre et à mettre en œuvre.

LDAP définit les opérations d'accès et de modification des entrées d'annuaire telles que :

- Recherche de critères spécifiés par l'utilisateur
- Ajout d'une entrée
- Suppression d'une entrée
- Modification d'une entrée
- Modification du nom distinctif ou du nom distinctif relatif d'une entrée
- Comparer une entrée

Fonctions supportées par LDAP ?

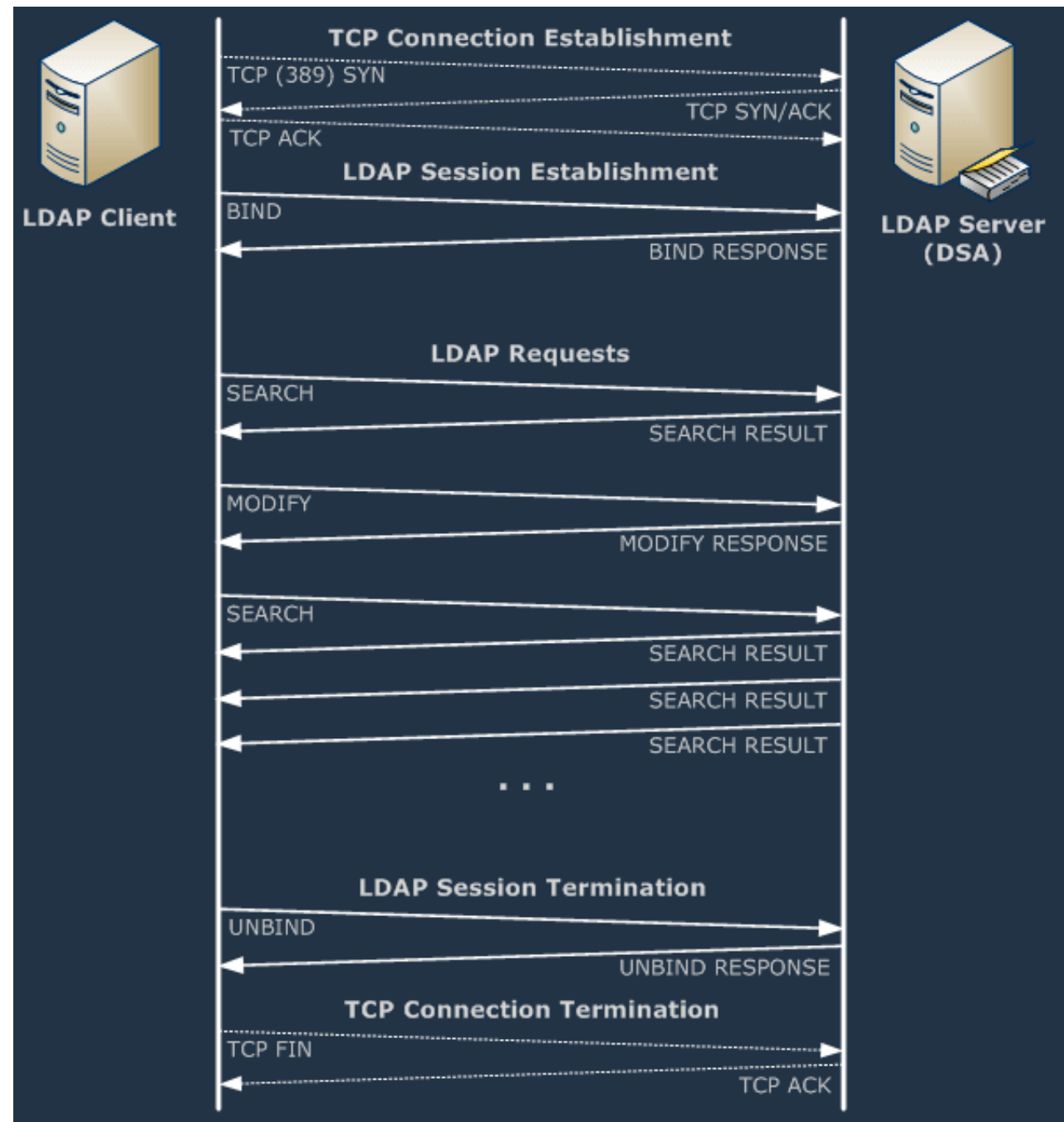
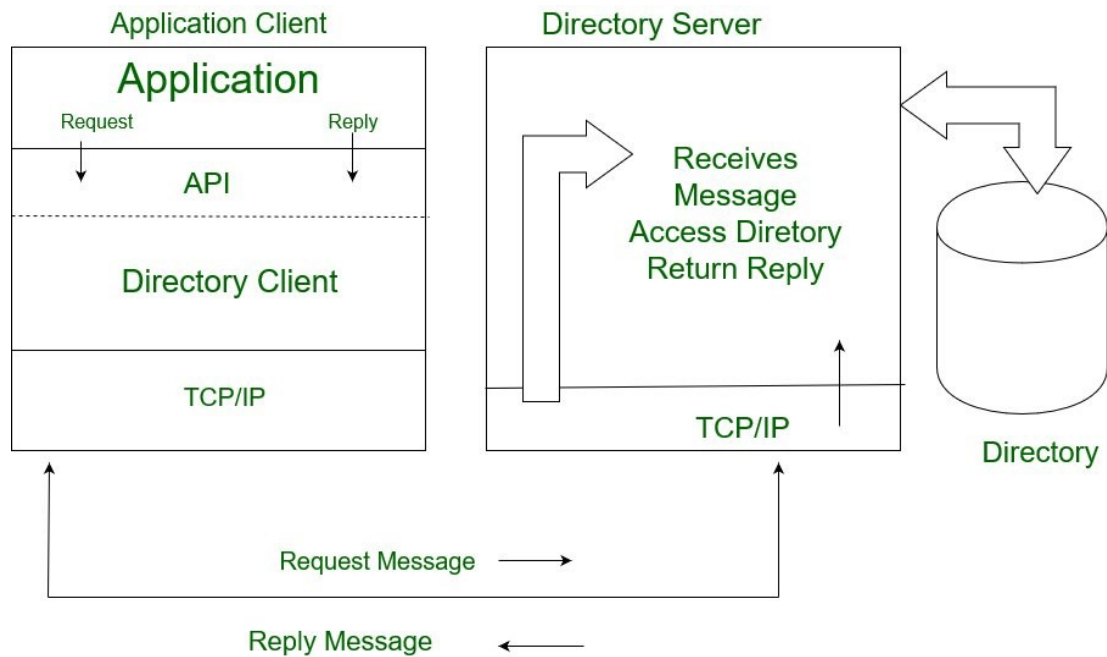
Connexion client/serveur :

1. Le client établit une session BIND avec le serveur en utilisant le nom d'hôte/IP/et le numéro de port. Pour des raisons de sécurité, l'utilisateur définit l'authentification basée sur l'ID UTILISATEUR et le mot de passe.
2. Le serveur effectue des opérations telles que la lecture, la mise à jour, la recherche, etc.
3. Le client met fin à la session à l'aide de la fonction UNBIND ou Abandon.

Interaction client-serveur LDAP :

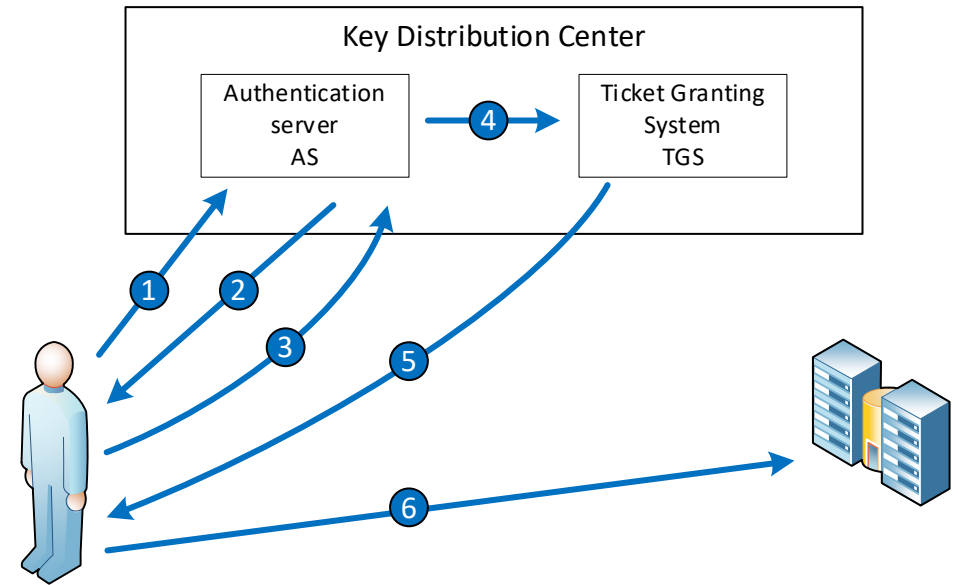
Elle est assez similaire à toute autre interaction client-serveur:

1. Une demande par le protocole LDAP est envoyée au serveur par le client.
2. Le serveur effectue des opérations sur le répertoire telles que la recherche, la mise à jour, la suppression, etc.
3. La réponse est renvoyée au client.



Qu'est-ce que l'authentification Kerberos ?

- Kerberos est un protocole d'authentification réseau développé au MIT, qui utilise une technique de chiffrement à clé symétrique. Il inclut également un centre de distribution de clés.
- Kerberos est largement utilisé dans les systèmes sécurisés basés sur des fonctionnalités de test et de vérification fiables. Kerberos est utilisé dans l'authentification Posix, ainsi que dans Active Directory, NFS et Samba. Et c'est un autre système d'authentification pour SSH, POP et SMTP.
- Cela fonctionne sur le modèle basé sur le client-serveur. Kerberos utilise la cryptographie à clé symétrique et un centre de distribution de clés (KDC) pour authentifier et vérifier les identités des consommateurs. La clé symétrique utilisée est la même pour le chiffrement et le déchiffrement. Un KDC est une base de données de toutes les clés secrètes. Un KDC comporte 3 aspects :
 - Un serveur d'octroi de tickets (TGS) qui connecte le consommateur au serveur de service (SS).
 - Une base de données Kerberos qui stocke le mot de passe et l'identification de tous les utilisateurs testés.
 - Un serveur d'authentification (AS) qui joue l'authentification préliminaire.



1. L'utilisateur envoie un message à KDC, demandant des clés afin que l'utilisateur puisse prouver son authenticité et accéder aux services .
2. AS renvoie un ticket à l'utilisateur sous forme cryptée.
3. L'utilisateur décryptera le message et obtient le code de hachage qu'il renvoie au AS. Maintenant, AS vérifiera l'authenticité.
4. Si l'utilisateur est autorisé, AS donne un ticket de service (clé secrète) au serveur d'octroi de tickets.
5. TGS le remet à l'Utilisateur.
6. À l'aide de ce Ticket, le client communique avec un serveur.

Kerberos infailible ?

- Il n'y a pas de niveau de protection infailible à 100 %
 - Création de faux ticket
 - Tentatives répétées de brute force sur les mots de passe
 - Programme informatique malveillant pour réduire le cryptage
- Kerberos est toujours le meilleur protocole d'accès sécurisé disponible aujourd'hui. Il est suffisamment flexible pour utiliser des algorithmes de cryptage robustes pour aider à lutter contre les nouvelles menaces.
- **Avantages de Kerberos :**
 - **Contrôle d'accès :** Contrôle d'accès puissant. Les utilisateurs bénéficient d'un point unique pour le suivi de toutes les connexions et l'application des politiques de protection.
 - **Authentification mutuelle :** Permet aux structures de transport et aux clients de s'authentifier mutuellement.
 - **Durée de vie limitée du ticket :** Chaque ticket dans Kerberos possède des horodatages et des données à vie.
 - **Authentification réutilisable :** Authentification est durable et réutilisable.
 - **Sécurité :** Plusieurs clés secrètes, l'autorisation de tiers et la cryptographie font de Kerberos un protocole de vérification sécurisé. Les mots de passe ne sont pas envoyés sur les réseaux et les clés secrètes sont cryptées, ce qui rend difficile pour les attaquants de se faire passer pour des utilisateurs ou des services.
 - **Performances :** Conserve une trace des informations client après vérification. En outre, Kerberos peut transférer des informations client d'un serveur Web de bout en bout vers d'autres serveurs d'arrière-plan tels que SQL Server.

Kerberos 4 vs 5

- **Kerberos version 4 :**
 - Logiciel d'authentification basé sur le Web qui est utilisé pour l'authentification des informations des utilisateurs lors de la connexion au système par la technique DES pour le cryptage. Il a été lancé à la fin des années 1980.
- **Fonctionnalités de Kerberos V4 :**
 - Authentification : fournit des services d'authentification et de chiffrement aux clients et serveurs du réseau.
 - Cryptage : utilise un algorithme de cryptage simple qui est moins sécurisé que le cryptage utilisé dans Kerberos V5.
 - Service d'octroi de tickets (TGS) : utilise un seul TGS pour tous les services réseau, ce qui signifie que le TGS doit gérer un grand nombre de requêtes.
 - Pas de prise en charge des horodatages : ne prend pas en charge les horodatages, ce qui le rend vulnérable aux attaques par relecture.
- **Kerberos version 5 :**
 - version plus récente du logiciel Kerberos, développée pour améliorer la sécurité de l'authentification. Kerberos version 5 fournit un service d'authentification unique dans un réseau qui est distribué sur une entreprise. Il a été lancé en 1993.
- **Fonctionnalités de Kerberos V5 :**
 - Authentification : fournit des services d'authentification, de chiffrement et d'autorisation aux clients et serveurs du réseau.
 - Cryptage : utilise un algorithme de cryptage plus sécurisé que Kerberos V4, ce qui le rend moins vulnérable aux attaques.
 - Service d'octroi de tickets (TGS) : utilise plusieurs serveurs TGS pour gérer les demandes de différents services réseau. Cela améliore l'évolutivité et réduit la charge sur les serveurs TGS individuels.
 - Prise en charge des horodatages : prend en charge les horodatages, ce qui le rend moins vulnérable aux attaques par relecture.
 - Prise en charge des tickets renouvelables : prend en charge les tickets renouvelables, ce qui permet aux utilisateurs d'étendre leur authentification sans avoir à ressaisir leurs mots de passe.

Kerberos 4 vs 5

- **Similitudes entre les deux versions de Kerberos :**

- Utilisent un processus d'authentification similaire qui implique un client, un serveur et un serveur d'authentification tiers de confiance (TAS) qui émet des tickets pour le client.
- Utilisent le cryptage pour protéger les données sensibles et empêcher les écoutes clandestines.
- Utilisent l'authentification par mot de passe, ce qui oblige les utilisateurs à entrer leurs mots de passe pour accéder aux ressources réseau.
- Utilisent l'authentification basée sur les tickets, qui permet aux utilisateurs de s'authentifier auprès de plusieurs ressources réseau sans avoir à saisir leur mot de passe plusieurs fois.
- Utilisent un centre de distribution de clés (KDC) pour distribuer les clés secrètes aux clients et serveurs du réseau.
- Conçus pour être compatibles avec une large gamme de systèmes d'exploitation et de protocoles réseau, ce qui les rend adaptés à une utilisation dans des environnements réseau hétérogènes.

Kerberos version 4

La version 4 de Kerberos a été lancée à la fin des années 1980.

Il fournit un support de ticket.

La version 4 de Kerberos fonctionne sur le système de codage Receiver-makes-Right.

Il ne prend pas en charge l'authentification interdomaine transitive.

Il utilise la technique Data Encryption Standard pour le cryptage.

Dans Kerberos version 4, la durée de vie du ticket doit être spécifiée en unités pour une durée de vie de 5 minutes.

Kerberos version 5

La version 5 de Kerberos a été lancée en 1993.

Il fournit une prise en charge des tickets avec des fonctionnalités supplémentaires pour le transfert, le renouvellement et la postdatation des tickets.

Kerberos version 5 fonctionne sur le système de codage ASN.1.

Il prend en charge l'authentification interdomaine transitive.

Il utilise toutes les techniques de chiffrement car le texte chiffré est étiqueté avec un identifiant de chiffrement.

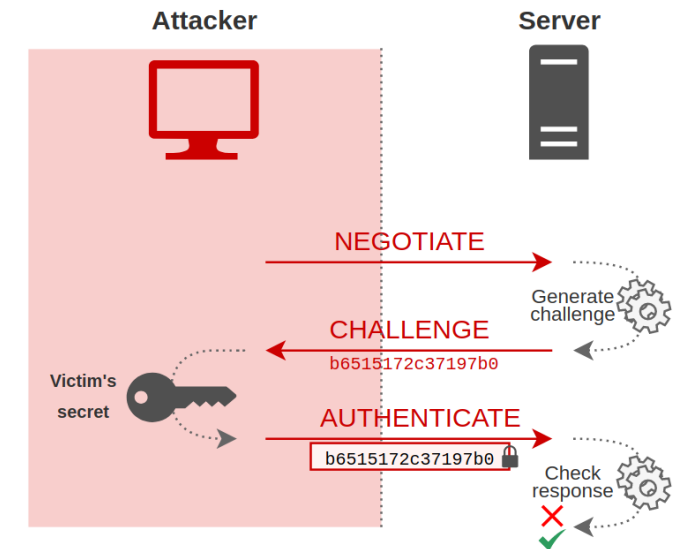
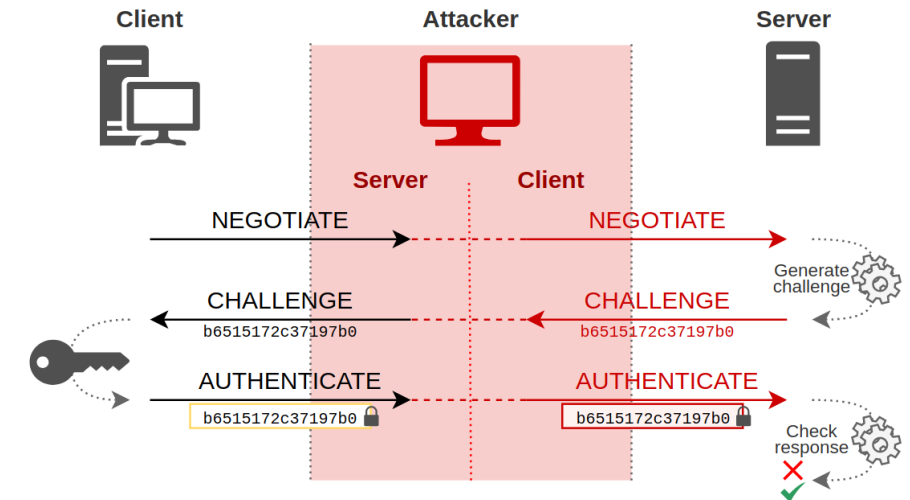
Dans Kerberos version 5, la durée de vie du ticket est spécifiée avec la liberté d'un temps arbitraire.

Authentication NTLM

- Windows NT LAN Manager (NTLM) est un protocole d'authentification challenge-réponse utilisé pour authentifier un client auprès d'une ressource sur un domaine Active Directory. Lorsque le client demande l'accès à un service associé au domaine, le service envoie un défi au client, exigeant que le client effectue une opération mathématique à l'aide de son jeton d'authentification, puis renvoie le résultat de cette opération au service. Le service peut valider le résultat ou l'envoyer au contrôleur de domaine (DC) pour validation. Si le service ou le contrôleur de domaine confirme que la réponse du client est correcte, le service autorise l'accès au client.
- NTLM est un type d'authentification unique (SSO) car il permet à l'utilisateur de fournir le facteur d'authentification sous-jacent une seule fois, lors de la connexion.
- NTLM est largement déployé, même sur de nouveaux systèmes, pour maintenir la compatibilité avec les systèmes plus anciens, mais n'est plus recommandé pour une utilisation par Microsoft car NTLM ne prend pas en charge les méthodes cryptographiques actuelles, telles que AES ou SHA-256. Microsoft a adopté Kerberos comme protocole d'authentification préféré pour Windows 2000 et les domaines Active Directory ultérieurs.
- NTLM est généralement considéré comme non sécurisé car il utilise une cryptographie obsolète qui est vulnérable à plusieurs modes d'attaques. NTLM est également vulnérable à l'attaque pass-the-hash et aux attaques par force brute.

Attaque de type NTLM Relay

- Type d'attaque rendu possible lorsqu'un agent malicieux intercepte les informations d'identification d'un utilisateur qui se connecte à un système.
- L'agent malicieux relaye les informations d'identification vers un autre ordinateur sur le même réseau, en utilisant une attaque de type « passe le relais ». L'ordinateur cible accepte ces informations d'identification permettant à l'agent malicieux de prendre le contrôle de l'ordinateur cible et d'y lancer des commandes.
- Peut être utilisé pour obtenir un accès non autorisé à des systèmes sensibles, tels que des serveurs de fichiers ou des contrôleurs de domaine.
- Peut être particulièrement dangereuses dans un environnement de réseau d'entreprise.
- Pour se protéger, il faut désactiver l'authentification NTLM qui n'est pas sécuritaire et utiliser des protocoles plus robuste tel que Kerberos.



Kerberos VS NTLM

- Kerberos est un système d'authentification basé sur des tickets qui est utilisé pour l'authentification des informations des utilisateurs lors de la connexion au système. Kerberos est basé sur la cryptographie à clé symétrique et dépend d'un tiers fiable et fonctionne sur le chiffrement à clé privée lors des phases d'authentification. Différentes versions de Kerberos sont développées pour améliorer la sécurité de l'authentification. Kerberos est généralement implémenté dans les produits Microsoft tels que Windows 2000, Windows XP et les versions ultérieures de Windows.
- **Avantages de Kerberos :**
 - Sécurité renforcée : Kerberos utilise la cryptographie à clé symétrique, qui est considérée comme plus forte que l'authentification basée sur le hachage de NTLM.
 - Authentification unique (SSO) : Kerberos active l'authentification unique, ce qui signifie que les utilisateurs n'ont besoin d'entrer leurs informations d'identification qu'une seule fois pour accéder à plusieurs ressources.
 - Prise en charge multiplateforme : Kerberos est une norme ouverte et peut être utilisé sur diverses plateformes, notamment Unix et Linux.
- **Inconvénients de Kerberos :**
 - Complexité : Kerberos nécessite plus de configuration et d'installation que NTLM, ce qui peut compliquer son déploiement et sa maintenance.
 - Nécessite une synchronisation de l'heure : Kerberos s'appuie sur une synchronisation précise de l'heure entre les serveurs, ce qui peut être un défi dans les grands environnements distribués.
 - Problèmes de compatibilité : certaines applications et certains systèmes plus anciens peuvent ne pas être compatibles avec Kerberos, ce qui peut limiter son utilisation dans certains environnements.



Kerberos VS NTLM

- NTLM (New technology LAN Manager) est un protocole d'authentification propriétaire de Microsoft. NTLM est également basé sur la technologie de chiffrement à clé symétrique et nécessite des serveurs de ressources pour fournir l'authentification, l'intégrité et la confidentialité aux utilisateurs. NTLM ne prend pas en charge la délégation d'authentification et l'authentification à deux facteurs. NTLM est généralement implémenté dans les versions antérieures de Windows telles que Windows 95, Windows 98, Windows ME, NT 4.0.
- **Avantages de NTLM :**
 - Simplicité : NTLM est plus facile à configurer et à configurer que Kerberos.
 - Largement pris en charge : NTLM est pris en charge par de nombreuses applications et systèmes, y compris les anciennes versions de Windows.
 - Non dépendant de la synchronisation de l'heure : NTLM ne nécessite pas de synchronisation de l'heure entre les serveurs, ce qui peut faciliter sa mise en œuvre dans certains environnements.
- **Inconvénients de NTLM :**
 - Sécurité plus faible : NTLM utilise une authentification basée sur le hachage, qui est considérée comme plus faible que la cryptographie à clé symétrique de Kerberos.
 - Prise en charge SSO limitée : NTLM ne prend pas en charge SSO, ce qui signifie que les utilisateurs peuvent avoir besoin de saisir leurs informations d'identification plusieurs fois pour accéder à différentes ressources.
 - Vulnérable à certaines attaques : NTLM est vulnérable à certaines attaques, telles que les attaques pass-the-hash et pass-the-ticket, qui peuvent compromettre la sécurité.



Kerberos VS NTLM

- **Similitudes :**
- Les deux protocoles fournissent une authentification pour les utilisateurs essayant d'accéder aux ressources du réseau.
- Les deux protocoles reposent sur l'utilisation de hachages pour stocker et comparer les informations d'identification.
- Les deux protocoles prennent en charge l'authentification mutuelle, où le client et le serveur s'authentifient mutuellement.
- Les deux protocoles prennent en charge les clés de session, qui sont utilisées pour sécuriser la transmission des données après authentification.
- Les deux protocoles ont été inclus dans les systèmes d'exploitation Windows et sont largement utilisés dans les environnements Windows.

Différence entre Kerberos et NTLM :

- Kerberos et NTLM sont des protocoles d'authentification importants utilisés dans les environnements windows.
- Cependant, Kerberos est plus sécurisé, évolutif et compatible avec les systèmes modernes, tandis que NTLM est plus simple à configurer et à gérer et fonctionne bien avec les systèmes plus anciens.
- Le choix entre les deux protocoles dépend finalement des besoins spécifiques de l'organisation et des ressources dont elle dispose.

Kerberos	NTLM
Kerberos est un logiciel open source et propose des services gratuits.	NTLM est le protocole d'authentification propriétaire de Microsoft.
Kerberos prend en charge la délégation d'authentification dans les applications multiniveaux.	NTLM ne prend pas en charge la délégation d'authentification.
Kerberos prend en charge l'authentification à deux facteurs telle que la connexion par carte à puce.	NTLM ne fournit pas de connexion par carte à puce.
Kerberos a la fonction d'authentification mutuelle.	NTLM n'a pas la fonction d'authentification mutuelle.
Kerberos offre une sécurité élevée.	Alors que NTLM est moins sécurisé que Kerberos.
Kerberos est pris en charge par Microsoft Windows 2000, Windows XP et les versions ultérieures de Windows.	NTLM est également pris en charge dans les versions antérieures de Windows telles que Windows 95, Windows 98, Windows ME, NT 4.0.

Kerberos VS LDAP

- **Avantages de LDAP :**

- Gestion centralisée : LDAP fournit un système de gestion centralisé pour l'authentification des utilisateurs, ce qui facilite la gestion de l'accès des utilisateurs sur plusieurs serveurs et services.
- Léger : LDAP est un protocole léger, ce qui signifie qu'il peut gérer un grand nombre d'utilisateurs et de services sans causer de problèmes de performances.
- Extensible : LDAP est extensible et peut être personnalisé pour répondre à des exigences d'authentification spécifiques. Cela en fait un protocole polyvalent pour divers environnements.
- Intégration : LDAP peut être intégré à d'autres protocoles d'authentification, tels que Kerberos et SAML, ce qui en fait un protocole flexible et adaptable.

- **Inconvénients de LDAP :**

- Sécurité : LDAP n'offre pas le même niveau de sécurité que Kerberos. LDAP ne prend pas en charge le cryptage par défaut, ce qui signifie que des informations sensibles peuvent être transmises en texte brut.
- Complexité : LDAP peut être complexe à configurer et à gérer, en particulier pour les déploiements à grande échelle.
- Évolutivité : LDAP n'est pas aussi évolutif que Kerberos, en particulier dans les environnements à fort trafic.

Kerberos VS LDAP

- **Avantages de Kerberos :**
 - Sécurité : Kerberos est un protocole plus sécurisé que LDAP, offrant des capacités de cryptage et d'authentification renforcées.
 - Évolutivité : Kerberos est un protocole évolutif, ce qui le rend adapté aux déploiements à grande échelle et aux environnements à fort trafic.
 - Authentification unique : Kerberos prend en charge l'authentification unique (SSO), ce qui le rend plus convivial et efficace.
 - Intégration : Kerberos peut être intégré à d'autres protocoles d'authentification, tels que LDAP et SAML, ce qui en fait un protocole flexible et adaptable.
- **Inconvénients de Kerberos :**
 - Complexité : Kerberos peut être complexe à configurer et à gérer, en particulier pour les déploiements à grande échelle.
 - Compatibilité : Kerberos n'est pas compatible avec les systèmes d'exploitation plus anciens, ce qui peut être un défi pour les systèmes hérités.
 - Surdébit : l'authentification Kerberos peut ajouter un surcoût au réseau, en particulier lorsqu'il s'agit d'un grand nombre d'utilisateurs et de services

Kerberos VS LDAP

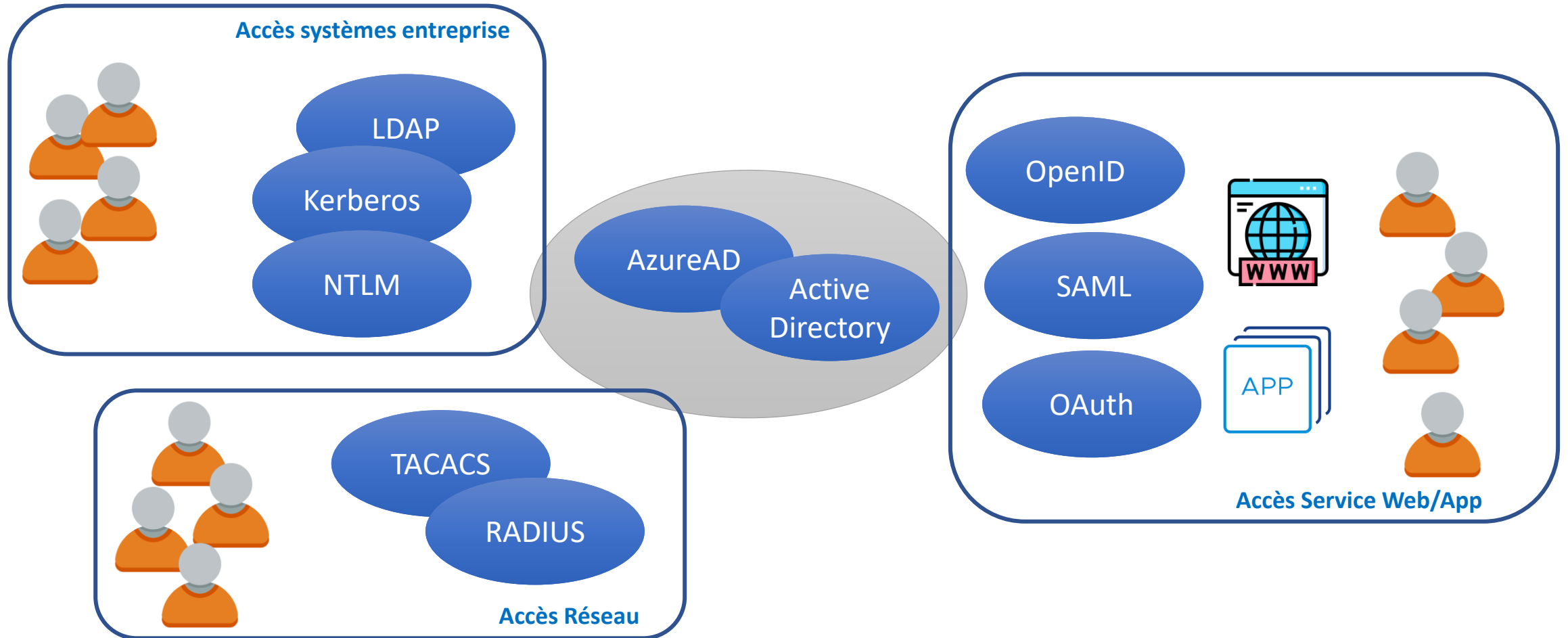
- **Similitudes entre LDAP et Kerberos :**
 - Authentification : LDAP et Kerberos sont utilisés à des fins d'authentification. Ils fournissent tous deux un moyen de vérifier l'identité d'un utilisateur avant d'accorder l'accès aux ressources.
 - Modèle client/serveur : LDAP et Kerberos utilisent tous deux un modèle client/serveur, dans lequel un client envoie une demande à un serveur pour accéder aux ressources.
 - Gestion centralisée : les deux protocoles prennent en charge la gestion centralisée des données d'authentification des utilisateurs. LDAP stocke les données d'authentification des utilisateurs, y compris les noms d'utilisateur et les mots de passe, dans un répertoire. Kerberos utilise un serveur d'authentification centralisé pour gérer l'authentification des utilisateurs.
 - Sécurité : LDAP et Kerberos offrent tous deux une sécurité à des fins d'authentification. LDAP peut utiliser des protocoles sécurisés tels que SSL/TLS pour crypter les données transmises entre le client et le serveur. Kerberos utilise la cryptographie à clé symétrique pour authentifier les utilisateurs et protéger les données transmises sur le réseau.
 - Intégration : LDAP et Kerberos peuvent être intégrés à d'autres systèmes et applications. LDAP peut être utilisé pour authentifier les utilisateurs pour diverses applications et services. Kerberos peut être utilisé pour l'authentification unique (SSO) sur plusieurs applications et services.
 - Largement utilisé : LDAP et Kerberos sont largement utilisés dans les environnements d'entreprise. LDAP est utilisé pour gérer les données d'authentification et d'autorisation des utilisateurs dans divers services d'annuaire, y compris Active Directory. Kerberos est utilisé à des fins d'authentification dans les environnements Windows et est intégré à divers services et applications Microsoft.

Différence entre LDAP et Kerberos :

LDAP	Kerberos
LDAP est utilisé pour autoriser les détails des comptes lors de l'accès.	Kerberos est utilisé pour gérer les informations d'identification en toute sécurité.
Ce n'est pas une source ouverte mais il a une implémentation telle que Open LDAP qui sont open-source.	C'est un logiciel open source qui fournit des services gratuits.
Il prend en charge l'authentification à deux facteurs avec le protocole RADIUS.	Il prend en charge l'authentification à deux facteurs.
LDAP ajoute l'authentification en deux options SASL ou authentification anonyme.	Kerberos ajoute une sécurité élevée et offre une authentification mutuelle.
Il fournit une authentification dans les applications multiniveaux.	Il fournit une authentification dans les applications multiniveaux.

- LDAP et Kerberos sont tous deux des protocoles d'authentification utilisés dans les environnements d'entreprise, mais ils ont des objectifs différents.
- LDAP est principalement utilisé pour gérer et accéder aux répertoires, tandis que Kerberos est conçu pour fournir une authentification sécurisée pour les applications client/serveur.
- LDAP utilise un mécanisme d'authentification simple, tandis que Kerberos utilise la cryptographie à clé symétrique.
- Alors que LDAP est compatible avec une large gamme de services d'annuaire et peut être utilisé dans divers environnements, Kerberos est principalement conçu pour être utilisé dans des environnements Windows.
- En fin de compte, le choix entre LDAP et Kerberos dépendra des besoins et des exigences spécifiques d'une organisation.

Interactions des différents protocoles et systèmes d'authentification



Qu'est-ce que RADIUS ?

- RADIUS signifie Remote Authentication Dial-In User Service, est un protocole de sécurité utilisé dans le cadre AAA pour fournir une authentification centralisée aux utilisateurs qui souhaitent accéder au réseau.
- Si un seul administrateur souhaite accéder à 100 routeurs et utiliser pour le nom d'utilisateur et le mot de passe (authentification), l'administrateur doit créer le même compte d'utilisateur sur l'ensemble des équipements. De plus, s'il souhaite changer son mot de passe, il doit le faire pour tous les appareils de façon manuelle. Bien sûr, c'est une tâche ardue.
- Un serveur ACS (Access Control Server) peut être utilisé. ACS fournit un système de gestion centralisé dans lequel la base de données de nom d'utilisateur et de mot de passe est conservée. De plus, la fonction d'autorisation peut être configurée. C'est donc deux fonction en un seul système : Authentification et autorisation.
- **Fonctionnalités :**
 1. Protocole standard ouvert pour le cadre AAA, c'est-à-dire qu'il peut être utilisé entre n'importe quel appareil de fournisseur et le serveur Cisco ACS.
 2. Il utilise UDP comme protocole de transmission.
 3. Il utilise le numéro de port UDP 1812 pour l'authentification et l'autorisation et 1813 pour la comptabilité.
 4. Si le périphérique et le serveur ACS utilisent RADIUS, seuls les mots de passe des paquets AAA sont chiffrés.
 5. Aucune autorisation de commande explicite ne peut être mise en œuvre.
 6. Il fournit un support comptable plus étendu que TACACS+.
 7. Dans RADIUS, l'authentification et l'autorisation sont couplées.

Qu'est-ce que RADIUS ?

- **Fonctionnement :**
 - Lorsque d'autres périphériques souhaitent accéder au serveur d'accès réseau, il enverra un message de demande d'accès au serveur ACS pour faire correspondre les informations d'identification. En réponse à la demande d'accès du client, le serveur ACS fournira un message d'acceptation d'accès au client si les informations d'identification sont valides et un rejet d'accès si les informations d'identification ne correspondent pas.
- **Avantages :**
 - Comme il s'agit d'un standard ouvert, il peut également être utilisé entre les autres appareils.
 - Support comptable plus étendu que TACACS+
- **Désavantages :**
 - Comme RADIUS utilise UDP, il est donc moins fiable que TACACS+.
 - Aucune autorisation de commande explicite ne peut être mise en œuvre.
 - RADIUS chiffre uniquement les mots de passe. Il ne protège pas d'autres données telles que le nom d'utilisateur.

Qu'est-ce que TACACS+ ?

- TACACS+, qui signifie Terminal Access Controller Access Control Server, est un protocole de sécurité utilisé dans le cadre AAA pour fournir une authentification centralisée aux utilisateurs qui souhaitent accéder au réseau.
- **Fonctionnalités :**
 - Protocole développé par Cisco pour le cadre AAA, c'est-à-dire qu'il peut être utilisé entre l'appareil Cisco et le serveur Cisco ACS.
 - Il utilise TCP comme protocole de transmission.
 - Il utilise le numéro de port TCP 49.
 - Si le périphérique et le serveur ACS utilisent TACACS+, tous les paquets AAA échangés entre eux sont chiffrés.
 - Il sépare AAA en éléments distincts, c'est-à-dire que l'authentification, l'autorisation et la comptabilité sont séparées.
 - Il offre un contrôle plus granulaire (que RADIUS) car les commandes autorisées à être utilisées par l'utilisateur peuvent être spécifiées.
 - Il fournit un support comptable mais est moins étendu que RADIUS.


Qu'est-ce que TACACS+ ?

- **Fonctionnement :**
 - Le client du TACACS+ est appelé Network Access Device (Nad) ou Network Access Server (NAS). Le périphérique d'accès au réseau contactera le serveur TACACS+ pour obtenir une invite de nom d'utilisateur via le message **CONTINUER** . L'utilisateur entre alors un nom d'utilisateur et le périphérique d'accès au réseau contacte à nouveau le serveur TACACS+ pour obtenir une invite de mot de passe (message Continuer) affichant l'invite de mot de passe à l'utilisateur, l'utilisateur entre un mot de passe, et le mot de passe est ensuite envoyé au serveur TACACS+.
- Le serveur peut répondre avec l'un des messages de réponse suivants :
 - Si les informations d'identification saisies sont valides, le serveur TACACS+ répondra par un message ACCEPTER.
 - Si les informations d'identification saisies ne sont pas valides, le serveur TACACS+ répondra par un message REJETER.
 - Si le lien entre le serveur TACACS+ et le serveur NAS ou TACACS+ ne fonctionne pas correctement, il répondra par un message ERROR.
 - Si l'autorisation TACACS+ est requise, le serveur TACACS+ est à nouveau contacté et il renvoie une réponse d'autorisation ACCEPT ou REJECT. Si le message ACCEPT est renvoyé, il contient des attributs qui sont utilisés pour déterminer les services qu'un utilisateur est autorisé à faire.
 - Pour la comptabilisation, le client enverra un message REQUEST au serveur TACACS+ auquel le serveur répond par un message RESPONSE indiquant que l'enregistrement est reçu.
- **Avantage :**
 - Fournit un contrôle plus granulaire que RADIUS. TACACS+ permet à un administrateur réseau de définir les commandes qu'un utilisateur peut exécuter.
 - Tous les paquets AAA sont chiffrés plutôt que simplement des mots de passe (dans le cas de Radius).
 - TACACS+ utilise TCP au lieu d'UDP. TCP garantit la communication entre le client et le serveur.
- **Désavantage -**
 - Comme il est propriétaire de Cisco, il ne peut donc être utilisé qu'entre les appareils Cisco. TACAS+ est une norme ouverte RFC8907
 - Prise en charge de la comptabilité moins étendue que RADIUS.

TACACS

VS

RADIUS



- **Avantages (TACACS+ sur RADIUS) :**

- Comme TACACS+ utilise TCP donc plus fiable que RADIUS.
- TACACS+ fournit plus de contrôle sur l'autorisation des commandes tandis que dans RADIUS, aucune autorisation externe des commandes n'est prise en charge.
- Tous les paquets AAA sont cryptés en TACACS+ alors que seuls les mots de passe sont cryptés en RADIUS c'est à dire plus sécurisé.

- **Avantages (RADIUS sur TACACS+) :**

- Comme il s'agit d'une norme ouverte, RADIUS peut donc être utilisé avec des appareils d'autres fournisseurs, tandis que TACACS+ étant la propriété de Cisco, il ne peut être utilisé qu'avec des appareils Cisco.
- Il dispose d'un support comptable plus étendu que TACACS+.

TACACS+	RADIUS
Protocole propriétaire Cisco	protocole standard ouvert
Il utilise TCP comme protocole de transmission	Il utilise UDP comme protocole de transmission
Il utilise le numéro de port TCP 49.	Il utilise le numéro de port UDP 1812 pour l'authentification et l'autorisation et 1813 pour la comptabilité.
L'authentification, l'autorisation et la comptabilité sont séparées dans TACACS+.	L'authentification et l'autorisation sont combinées dans RADIUS.
Tous les paquets AAA sont cryptés.	Seul le mot de passe est crypté tandis que les autres informations telles que le nom d'utilisateur, les informations comptables, etc. ne sont pas cryptées.
de préférence utilisé pour ACS.	utilisé lorsque ISE est utilisé
Il fournit un contrôle plus granulaire, c'est-à-dire qu'il peut spécifier la commande particulière pour l'autorisation.	Aucune autorisation externe de commandes n'est prise en charge.
TACACS+ offre une prise en charge multiprotocole	Pas de support multiprotocole.
Utilisé pour l'administration de l'appareil.	utilisé pour l'accès au réseau

TACACS vs RADIUS - Similitudes

- Le processus est démarré par Network Access Device (NAD – client de TACACS+ ou RADIUS). NAD contacte le serveur TACACS+ ou RADIUS et transmet la demande d'authentification (nom d'utilisateur et mot de passe) au serveur. Tout d'abord, NAD obtient l'invite de nom d'utilisateur et transmet le nom d'utilisateur au serveur, puis à nouveau le serveur est contacté par NAD pour obtenir l'invite de mot de passe, puis le mot de passe est envoyé au serveur.
- Le serveur répond par un message d'acceptation d'accès si les informations d'identification sont valides, sinon envoie un message de refus d'accès au client. En outre, l'autorisation et la comptabilité sont différentes dans les deux protocoles car l'authentification et l'autorisation sont combinées dans RADIUS.

Différences entre Kerberos et RADIUS

- **Caractéristiques de Kerberos :**

- Il inhibe diverses attaques d'intrusion.
- Il implémente l'authentification sur Internet pour les applications Web.
- Fournit une confiance unique à la racine et réduit les scénarios de maillage complet.
- Accorde l'interopérabilité avec d'autres domaines de passage.

- **Caractéristiques de RADIUS :**

- Son serveur peut agir en tant que client proxy pour d'autres serveurs Radius.
- Communication entre client et serveur authentifiée par une clé partagée
- Il prend en charge les protocoles PPP, PAP et CHAP à des fins d'authentification.
- Il fonctionne avec UDP et est un protocole sans état.

KerberosName	RADIUS
Il est utilisé pour gérer les informations d'identification des utilisateurs en toute sécurité.	Il est utilisé pour l'authentification centralisée, la comptabilité et l'autorisation des informations de l'utilisateur.
Kerberos est un logiciel open source qui fournit de nombreux services gratuits.	Ce n'est pas open-source mais il possède une implémentation telle que Free RADIUS qui est open-source.
Il fournit une authentification à deux facteurs.	Il ne fournit pas d'authentification bidirectionnelle mais peut définir deux niveaux de privilèges.
Kerberos associe haute sécurité et authentification mutuelle.	RADIUS fournit une authentification par client RADIUS également appelé NAS.
Il fournit une authentification dans les applications multiniveaux.	Il fournit une authentification dans les applications multiniveaux.

Différence entre LDAP et RADIUS

- **Fonctionnalités de LDAP :**
 - Il implémente un protocole open-source avec une architecture flexible.
 - Fonctionne directement sur TCP/IP et SSL.
 - LDAP est un protocole auto-automatisé.
 - Fournit une assistance étendue dans tous les secteurs.
- **Avantages de LDAP :**
 - Gestion centralisée : LDAP fournit un système de gestion centralisé pour l'authentification des utilisateurs, ce qui facilite la gestion de l'accès des utilisateurs sur plusieurs serveurs et services.
 - Léger : LDAP est un protocole léger, ce qui signifie qu'il peut gérer un grand nombre d'utilisateurs et de services sans causer de problèmes de performances.
 - Extensible : LDAP est extensible et peut être personnalisé pour répondre à des exigences d'authentification spécifiques. Cela en fait un protocole polyvalent pour divers environnements.
 - Intégration : LDAP peut être intégré à d'autres protocoles d'authentification, tels que Kerberos et SAML, ce qui en fait un protocole flexible et adaptable.
- **Inconvénients de LDAP :**
 - Sécurité : LDAP n'offre pas le même niveau de sécurité que RADIUS. LDAP ne prend pas en charge le cryptage par défaut, ce qui signifie que des informations sensibles peuvent être transmises en texte brut.
 - Complexité : LDAP peut être complexe à configurer et à gérer, en particulier pour les déploiements à grande échelle.
 - Évolutivité : LDAP n'est pas aussi évolutif que RADIUS, en particulier dans les environnements à fort trafic.

Différence entre LDAP et RADIUS

- **Caractéristiques de RADIUS :**
 - Son serveur peut agir en tant que client proxy pour d'autres serveurs Radius.
 - Communication entre client et serveur authentifiée par une clé partagée.
 - Il prend en charge les protocoles PPP, PAP et CHAP à des fins d'authentification.
 - Il fonctionne avec UDP et est un protocole sans état.
- **Avantages de RADIUS :**
 - Sécurité : RADIUS offre un niveau de sécurité supérieur par rapport à LDAP. RADIUS prend en charge le chiffrement et fournit des capacités d'authentification fortes, ce qui le rend idéal pour protéger les informations sensibles.
 - Évolutivité : RADIUS est un protocole évolutif, ce qui le rend adapté aux déploiements à grande échelle et aux environnements à fort trafic.
 - Flexibilité : RADIUS peut être utilisé pour authentifier une large gamme d'appareils, notamment des points d'accès sans fil, des VPN et des pare-feu.
 - Authentification centralisée : RADIUS fournit une authentification et une autorisation centralisées, ce qui facilite la gestion de l'accès des utilisateurs sur plusieurs appareils.
- **Inconvénients de RADIUS :**
 - Complexité : RADIUS peut être complexe à configurer et à gérer, en particulier pour les déploiements à grande échelle.
 - Intégration : RADIUS n'est pas aussi flexible que LDAP lorsqu'il s'agit d'intégrer d'autres protocoles d'authentification.
 - Surcharge de performances : l'authentification RADIUS peut augmenter la surcharge du réseau, en particulier lorsqu'il s'agit d'un grand nombre d'utilisateurs et de services.
- **Similitudes:**
 - Authentification centralisée : LDAP et RADIUS fournissent une authentification et une autorisation centralisées, ce qui facilite la gestion de l'accès des utilisateurs sur plusieurs appareils.
 - Base de données d'utilisateurs : LDAP et RADIUS utilisent tous deux une base de données d'utilisateurs pour stocker les informations d'identification et d'autorisation des utilisateurs.
 - Personnalisation : LDAP et RADIUS peuvent être personnalisés pour répondre à des exigences d'authentification spécifiques, ce qui en fait des protocoles polyvalents pour divers environnements.
 - Contrôle d'accès au réseau : LDAP et RADIUS peuvent être utilisés pour le contrôle d'accès au réseau, garantissant que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques.
 - Intégration tierce : LDAP et RADIUS peuvent s'intégrer à des protocoles d'authentification tiers, tels que SAML et Kerberos, pour fournir une solution d'authentification et d'autorisation plus complète.



Différences entre LDAP et RADIUS

LDAP et RADIUS sont tous deux des protocoles d'authentification utilisés dans les environnements d'entreprise, mais ils ont des objectifs différents.

LDAP est principalement utilisé pour gérer et accéder aux répertoires, tandis que RADIUS est conçu pour fournir des services centralisés d'authentification, d'autorisation et de comptabilité dans des scénarios d'accès à distance.

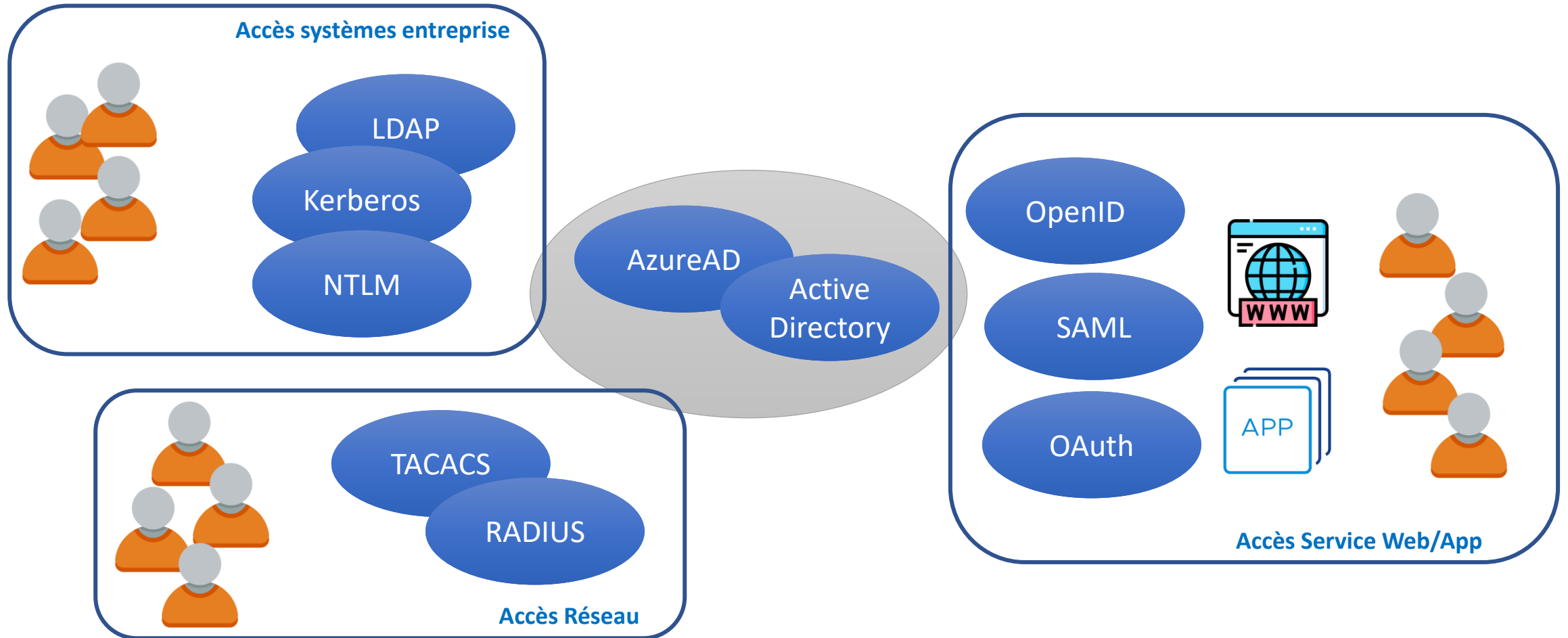
LDAP utilise un mécanisme d'authentification simple, tandis que RADIUS utilise un mécanisme d'authentification plus sécurisé impliquant un secret partagé. RADIUS offre une sécurité renforcée grâce à l'utilisation d'un secret partagé et offre des services de comptabilité, contrairement à LDAP.

Alors que RADIUS est compatible avec une large gamme d'équipements réseau et peut être utilisé dans divers environnements, LDAP est principalement utilisé dans les environnements Windows.

En fin de compte, le choix entre LDAP et RADIUS dépendra des besoins et des exigences spécifiques d'une organisation.

LDAP	RADIUS
Il est court appelé Lightweight Directory Access Protocol.	Il est l'abréviation de Remote Authentication Dial-In User Service.
LDAP est utilisé pour autoriser les détails des enregistrements lors de l'accès.	Il est utilisé pour l'authentification centralisée, la comptabilité et l'autorisation des informations de l'utilisateur.
Il n'est pas open-source mais il possède une implémentation telle que Open LDAP qui sont open-source.	Ce n'est pas open-source mais il possède une implémentation telle que Free RADIUS qui est open-source.
Il prend en charge l'authentification à deux facteurs avec le protocole RADIUS.	Il ne fournit pas d'authentification bidirectionnelle, mais peut définir deux niveaux de privilèges.
LDAP ajoute l'authentification en deux options SASL ou authentification anonyme.	RADIUS fournit une authentification par client RADIUS également appelé NAS.
Il rend l'authentification dans les applications multiniveaux.	Il fournit une authentification dans les applications multiniveaux.

Interactions des différents protocoles et systèmes d'authentification



OAuth

- **OAuth (Open Authorization)** est un protocole standard ouvert pour l'autorisation d'une application pour l'utilisation des informations de l'utilisateur, en général, il permet à une application tierce d'accéder aux informations relatives à l'utilisateur telles que le nom, la date de naissance, l'e-mail ou d'autres données requises à partir d'une application comme Facebook, Google etc. sans donner le mot de passe de l'utilisateur à l'application tierce. Il se prononce **oh-auth** .
- Vous avez peut-être vu un bouton "Connexion avec Google" ou "Connexion avec Facebook" sur la page de connexion/inscription d'un site Web qui facilite l'utilisation du service ou du site Web en vous connectant simplement à l'un des services et en accordant l'autorisation de l'application cliente pour accéder à vos données sans donner de mot de passe. Cela se fait avec OAuth.
- Il est conçu pour fonctionner avec HTTP et permet l'émission de jetons d'accès à l'application tierce par un serveur d'autorisation avec l'approbation du propriétaire.

OAuth

- Il y a 3 composants dans le mécanisme OAuth :
 1. Fournisseur OAuth - Il s'agit du fournisseur OAuth, par exemple. Google, Facebook, etc.
 2. Client OAuth - Il s'agit du site Web sur lequel nous partageons ou authentifions l'utilisation de nos informations. Par exemple. Geeks pour Geeks etc.
 3. Propriétaire – L'utilisateur dont la connexion authentifie le partage d'informations.
- OAuth peut être implémenté via la console Google pour permettre une connexion Google sur une application Web.
- Modèle à suivre :
 1. Obtenir l'ID client OAuth 2.0 à partir de la console d'API Google
 2. Ensuite, obtenez un jeton d'accès auprès du serveur d'autorisation Google pour accéder à l'API.
 3. Envoyez la requête avec le jeton d'accès à une API.
 4. Obtenez un jeton d'actualisation si un accès plus long est requis.

Authentication SAML

SAML est un framework basé sur XML qui signifie **Security Assertion Markup Language** . Voyons comment SAML est utilisé pour activer le SSO (Single-Sign-On).

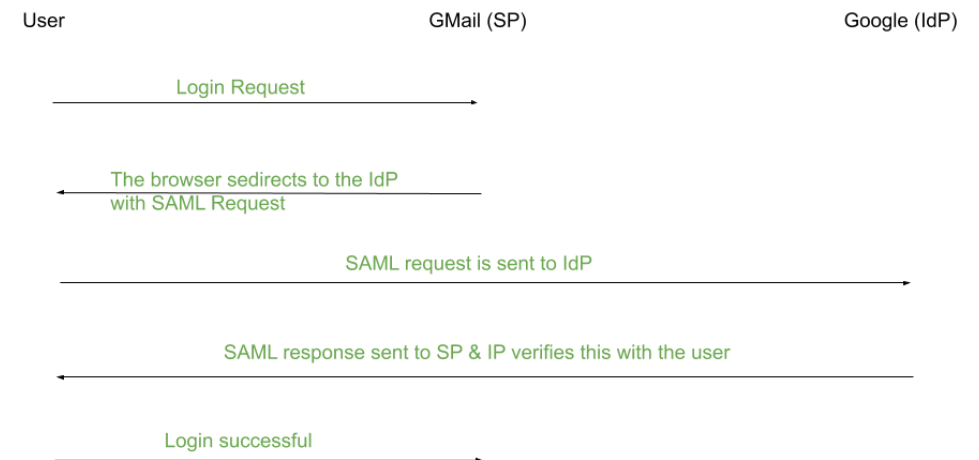
Exemple - Lorsqu'une personne se connecte sur gmail.com, elle peut visiter YouTube, Google Drive et d'autres services Google sans avoir à se connecter à chaque service séparément.

Le flux d'authentification SAML est basé sur deux entités -

1.Fournisseurs de services (SP) - Le SP reçoit l'authentification de l'IdP et accorde l'autorisation à l'utilisateur.

2.Fournisseurs d'identité (IdP) - L'IdP authentifie un utilisateur et envoie ses informations d'identification avec ses droits d'accès au service au SP.

Dans l'exemple ci-dessus, SP sera Gmail et IdP sera Google. SAML active l'authentification unique et, comme expliqué ci-dessus, un utilisateur peut se connecter une seule fois et les mêmes informations d'identification seront utilisées pour se connecter à d'autres SP.



Authentication SAML

- **Flux de travail d'authentification SAML :**
 - Un utilisateur essaie de se connecter à Gmail.
 - Gmail génère une requête SAML.
 - La requête SAML est envoyée à Google par le navigateur, qui analyse cette requête, authentifie l'utilisateur et crée une réponse SAML. Cette réponse SAML est codée et renvoyée au navigateur.
 - Le navigateur renvoie cette réponse SAML à Gmail pour vérification.
 - Si l'utilisateur est vérifié avec succès, il est connecté à Gmail.
- **Demande SAML :**
 - Certains des termes importants de la requête SAML sont définis ci-dessous :
 1. **ID** – Identifiant d'une requête SAML particulière.
 2. **Émetteur** – Le nom du fournisseur de services (SP).
 3. **NameID** – Le nom d'utilisateur/adresse e-mail ou numéro de téléphone utilisé pour identifier un utilisateur.
 4. **AssertionConsumerServiceURL** – L'interface URL SAML du SP où l'adresse IP envoie le jeton d'authentification.
- **Réponse SAML :**
 - Une réponse SAML se compose de deux parties :
 1. **Assertion** -
C'est un document XML qui contient les détails de l'utilisateur. Celui-ci contient l'horodatage de l'événement de connexion de l'utilisateur et la méthode d'authentification utilisée (par exemple, authentification à 2 facteurs, Kerberos, etc.)
 2. **Signature** -
Il s'agit d'une chaîne encodée en Base64 qui protège l'intégrité de l'assertion. (Si un attaquant essaie de changer le nom d'utilisateur dans l'assertion en nom d'utilisateur de la victime, la signature empêchera le pirate de se connecter en tant qu'utilisateur).
- **Génération de clé :**
 - Le fournisseur d'identité (IdP) génère une clé privée et une clé publique. Il signe l'assertion avec la clé privée. La clé publique est partagée avec le fournisseur de services (SP) qui l'utilise pour vérifier la réponse SAML, puis connecter l'utilisateur.

Vulnérabilités SAML

- Signature non vérifiée :
 - Si quelqu'un est en mesure de modifier l'identifiant de nom (nom d'utilisateur) dans la réponse SAML et de se connecter en tant que quelqu'un d'autre en raison de l'absence de processus de vérification de signature.
- Signature vérifiée uniquement lorsqu'elle existe :
 - Si quelqu'un modifie la valeur de l'identifiant du nom et supprime la signature avant que la réponse ne soit reçue par le navigateur et qu'il soit toujours en mesure de se connecter en tant que victime.
- Comment Injection :
 - Un utilisateur peut être enregistré avec un commentaire XML dans le nom d'utilisateur comme suit :
 - email : prerit<!--notprerit-->@test.com
 - Lors du traitement de la réponse SAML, le SP ignorera le commentaire et nous connectera en tant que victime. L'intégralité de la réponse SAML peut être interceptée à l'aide d'un proxy tel qu'une suite burp. Notez qu'il doit d'abord être décodé par le format URL puis par le format Base64 pour être visualisé.
- SAML Replay :
 - L'attaquant capture la réponse SAML et l'utilise plusieurs fois pour se connecter en tant que victime.

Différence entre OAuth et LDAP

- **Avantages de LDAP :**

- LDAP est un protocole standardisé d'accès et de maintenance des informations d'annuaire, ce qui facilite son intégration à une large gamme de systèmes et d'applications.
- LDAP est largement utilisé et bien établi, avec de nombreuses ressources disponibles pour le dépannage et le support.
- LDAP offre un moyen sécurisé de gérer les identités des utilisateurs et des appareils dans une organisation, permettant un contrôle et une gestion centralisés.

- **Inconvénients de LDAP :**

- LDAP peut être complexe à configurer et à gérer, en particulier pour les grandes organisations avec des structures de répertoires plus complexes.
- LDAP peut être vulnérable aux attaques s'il n'est pas correctement sécurisé, car il repose sur des noms d'utilisateur et des mots de passe pour l'authentification.
- LDAP peut ne pas convenir à toutes les applications ou à tous les cas d'utilisation, en particulier ceux qui nécessitent un contrôle d'accès plus granulaire ou une intégration avec des services basés sur le cloud.

- **Avantages d'OAuth 2 :**

- OAuth 2 est un protocole flexible qui prend en charge un large éventail de cas d'utilisation et de scénarios, y compris les applications Web, les applications mobiles et les API.
- OAuth 2 est largement utilisé et bien établi, avec de nombreuses ressources disponibles pour le dépannage et l'assistance.
- OAuth 2 offre un moyen sécurisé d'authentifier et d'autoriser les utilisateurs et les applications, avec des mécanismes intégrés de contrôle d'accès et de délégation.

- **Inconvénients d'OAuth 2 :**

- OAuth 2 peut être complexe à configurer et à gérer, en particulier pour les organisations ayant des exigences de sécurité complexes ou des systèmes hérités.
- OAuth 2 peut être vulnérable aux attaques s'il n'est pas correctement sécurisé, comme les attaques de phishing ou le vol de jetons.
- OAuth 2 peut ne pas convenir à toutes les applications ou à tous les cas d'utilisation, en particulier ceux qui nécessitent un contrôle d'accès plus granulaire ou une intégration avec des systèmes hérités.

Différence entre OAUTH et LDAP

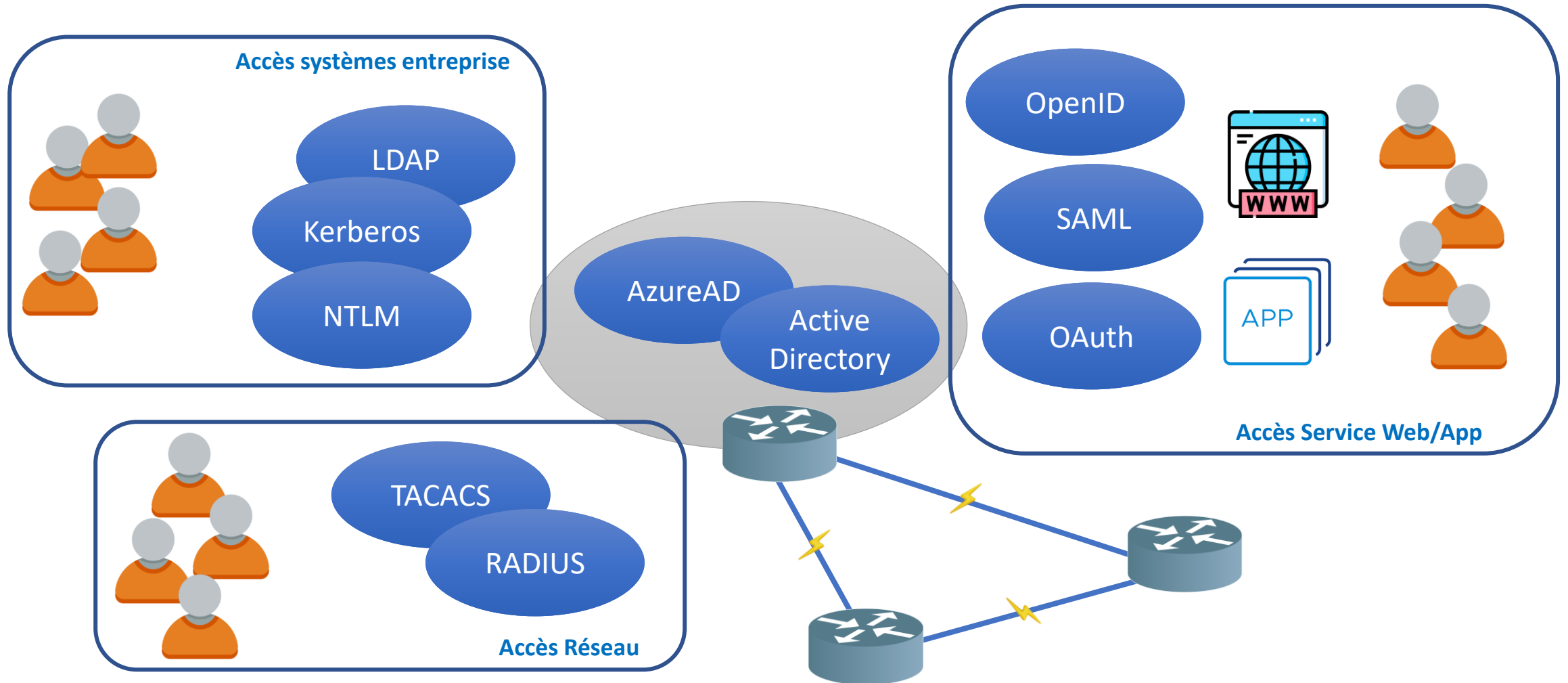
- **Similitudes :**
 - LDAP et OAuth 2 sont largement utilisés dans les environnements d'entreprise pour l'authentification et l'autorisation des utilisateurs.
 - Les deux protocoles utilisent des jetons pour gérer l'authentification et l'autorisation, LDAP utilisant une combinaison de nom d'utilisateur et de mot de passe, et OAuth 2 utilisant des jetons d'accès et des jetons d'actualisation.
 - Les deux protocoles prennent en charge la gestion centralisée des identités, permettant aux organisations de gérer les identités des utilisateurs et l'accès à plusieurs applications et systèmes.
 - LDAP et OAuth 2 offrent tous deux un moyen standardisé de gérer et d'accéder aux identités et aux autorisations des utilisateurs, ce qui facilite l'intégration des applications à ces systèmes.
 - Les deux protocoles fournissent des mécanismes de contrôle d'accès et de délégation, permettant aux organisations de gérer l'accès des utilisateurs aux ressources en fonction de règles et de politiques prédéfinies.

Différences entre LDAP et OAuth

- LDAP et OAuth 2 sont utilisés à des fins d'authentification et d'autorisation, mais ils ont des objectifs différents et ont des approches différentes.
- LDAP est utilisé pour l'authentification et le contrôle d'accès aux répertoires et aux ressources.
- OAuth 2 est utilisé pour l'autorisation et permet aux applications tierces d'accéder aux ressources au nom d'un utilisateur.
- Alors que LDAP fournit la sécurité grâce au cryptage et aux protocoles sécurisés, OAuth 2 utilise des jetons d'accès pour accorder l'accès aux ressources.
- En fin de compte, le choix entre LDAP et OAuth 2 dépendra des besoins et des exigences spécifiques d'une organisation.

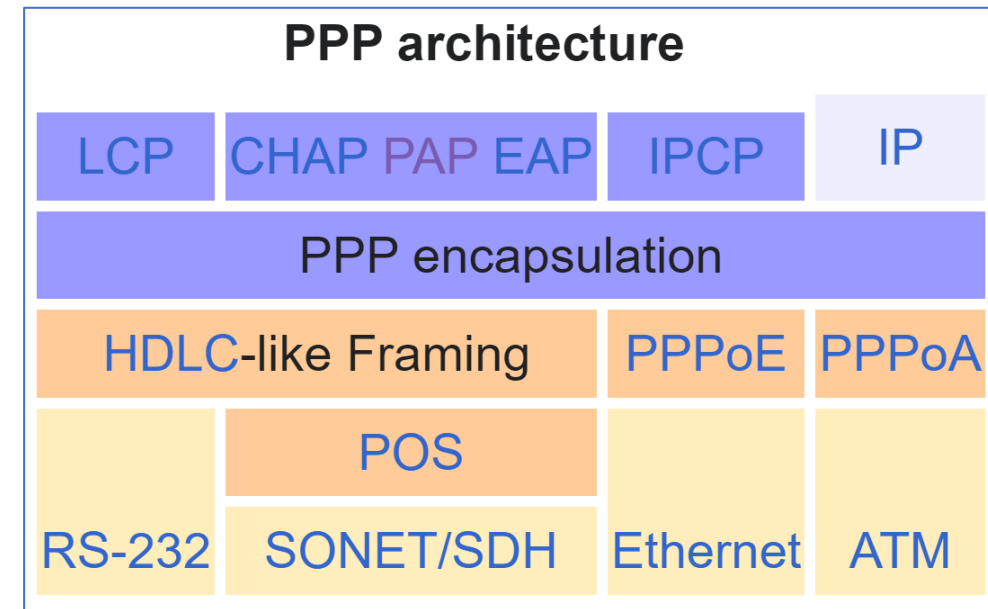
LDAP	OAuth 2
LDAP est utilisé pour autoriser les détails des enregistrements lors de l'accès.	Il est utilisé pour l'authentification des informations d'identification de l'utilisateur comme côté serveur.
Il n'est pas open-source mais il possède une implémentation telle que Open LDAP qui sont open-source.	Il s'agit d'un standard ouvert pour la délégation d'accès.
Il prend en charge l'authentification à deux facteurs avec le protocole RADIUS.	Il fournit une authentification bidirectionnelle et peut vous indiquer le nombre d'attributs de l'utilisateur.
LDAP ajoute l'authentification en deux options SASL ou authentification anonyme.	OAuth fournit une authentification par jeton d'accès appelé jetons réseau.
Il rend l'authentification dans les applications multiniveaux.	Il fournit une authentification dans les applications multiniveaux.

Interactions des différents protocoles et systèmes d'authentification



Architecture PPP

- PPP permet à plusieurs protocoles de couche réseau de fonctionner sur le même lien de communication. Pour chaque protocole de couche réseau utilisé, un protocole de contrôle de réseau (NCP) distinct est fourni afin d'encapsuler et de négocier des options pour les multiples protocoles de couche réseau. Il négocie les informations de la couche réseau, par exemple l'adresse réseau ou les options de compression, une fois la connexion établie.
- Les NCP suivants peuvent être utilisés avec PPP :
 - IPCP pour IP ([RFC1332](#))
 - le protocole OSI Network Layer Control Protocol (OSINLCP) pour les différents protocoles de couche réseau OSI
 - le protocole de contrôle AppleTalk (ATPP) pour AppleTalk
 - le protocole IPXCP (Internetwork Packet Exchange Control Protocol) pour l'échange de paquets Internet
 - le protocole DECnet Phase IV Control Protocol (DNCP) pour le protocole DNA Phase IV Routing (DECnet Phase IV)
 - le NetBIOS Frames Control Protocol (NBFCP) pour le protocole NetBIOS Frames (ou NetBEUI comme on l'appelait auparavant)
 - le protocole de contrôle IPv6 (IPV6CP) pour IPv6



État d'un lien PPP

- Lien mort
 - Déconnexion de la liaison, volontaire ou suivant l'ordre de se déconnecter (par exemple, un utilisateur a terminé sa connexion commutée.)
- Phase d'établissement de liaison
 - Négociation du protocole de contrôle de liaison. En cas de succès, le contrôle passe soit à la phase d'authentification, soit à la phase du protocole de couche réseau, selon que l'authentification est souhaitée ou non.
- Phase d'authentification
 - Il permet aux parties de s'authentifier mutuellement avant qu'une connexion ne soit établie. En cas de succès, le contrôle passe à la phase de protocole de couche réseau. Cette phase est facultative.
- Phase de protocole de couche réseau
 - Protocoles de contrôle de réseau sont activés. Par exemple, IPCP est utilisé pour établir un service IP sur la ligne.
 - Le transport de données pour tous les protocoles qui sont démarrés avec succès avec leurs protocoles de contrôle de réseau se produit également dans cette phase. La fermeture des protocoles réseau se produit également dans cette phase.
- Phase de terminaison de liaison
 - Cette phase ferme cette connexion. Cela peut se produire en cas d'échec d'authentification, s'il y a tellement d'erreurs de somme de contrôle que les deux parties décident de supprimer automatiquement le lien, si le lien échoue soudainement ou si l'utilisateur décide de raccrocher une connexion.

Protocoles d'authentification

Protocole d'authentification :

Les protocoles d'authentification demandent simplement de valider l'identité de l'utilisateur qui veut avoir accès aux ressources. Ces protocoles authentifient également les terminaux simplement pour les utilisateurs de services.

•Protocole d'authentification extensible (EAP) :

Il existe plusieurs protocoles d'authentification initiés par le client, c'est-à-dire l'homologue, mais l'authentification EAP est généralement initiée par le serveur. Il s'agit d'un protocole qui prend essentiellement en charge un large éventail de protocoles d'authentification.

•Protocole d'authentification de mot de passe (PAP) :

Ce protocole est particulièrement nécessaire pour vérifier l'identité et le mot de passe de l'homologue ou du client, ce qui peut entraîner un succès ou un échec. Il est également symétrique et n'autorise même pas les paramètres asymétriques avec l'authentificateur et l'homologue.

•Challenge Handshake Authentication Protocol (CHAP) :

Ce protocole est particulièrement nécessaire pour vérifier l'identité du pair ou du client à l'aide d'une poignée de main à trois voies. C'est asymétrique.

Protocole PAP

Protocole d'authentification de mot de passe (PAP) –

PAP est un protocole d'authentification de mot de passe utilisé par les liens PPP pour valider les utilisateurs. L'authentification PAP nécessite que l'appareil appelant envoie le nom d'utilisateur et le mot de passe. Si les informations d'identification correspondent à la base de données locale de l'appareil appelé ou dans la base de données AAA distante, l'accès est autorisé sinon refusé.

Fonctionnalités -

Certaines des fonctionnalités de PAP sont :

- Le mot de passe est envoyé en clair.
- Tous les systèmes d'exploitation réseau prennent en charge PAP.
- Il utilise un protocole de prise de contact bidirectionnel.
- Il n'est pas interactif.
- PAP prend en charge à la fois l'authentification unidirectionnelle (unidirectionnelle) et l'authentification bidirectionnelle (bidirectionnelle).

Protocole PAP

- PAP est généralement utilisé dans les scénarios suivants :
 1. Lorsque l'application ne prend pas en charge CHAP.
 2. Circonstances où il est nécessaire d'envoyer un mot de passe en texte clair pour simuler une connexion à l'appareil appelé (hôte distant).
 3. En cas d'incompatibilités entre différents fournisseurs de CHAP.
- **Avantage de CHAP sur PAP :**
 1. CHAP est plus sécurisé que PAP.
 2. CHAP peut fournir une authentification périodiquement pour reconnaître si l'utilisateur accédant au lien PPP est le même ou non.
 3. Dans CHAP, les vrais mots de passe ne sont jamais partagés sur le lien, mais une valeur de hachage de celui-ci est calculée et transférée.
- **Avantage de PAP sur CHAP :**

Le seul avantage de PAP sur CHAP est qu'il est pris en charge par tous les fournisseurs de systèmes d'exploitation réseau, on peut donc dire que PAP est utilisé là où CHAP n'est pas pris en charge. Mais si CHAP est pris en charge, il est recommandé d'utiliser CHAP car il est plus sécurisé.

Protocole CHAP

- Le protocole CHAP (Challenge Handshake Authentication Protocol) est un protocole d'authentification point à point (PPP) développé par l'IETF (Internet Engineering Task Force). Il est utilisé au démarrage initial du lien. En outre, il effectue des vérifications périodiques pour vérifier si le routeur communique toujours avec le même hôte.
 - Il utilise le protocole d'établissement de liaison à 3 voies. Tout d'abord, l'authentificateur envoie un paquet de défi au pair, puis le pair répond avec une valeur en utilisant sa fonction de hachage à sens unique. L'authentificateur fait alors correspondre la valeur reçue avec sa propre valeur de hachage calculée. Si les valeurs correspondent, l'authentification est confirmée, sinon la connexion sera interrompue.
 - Il utilise une fonction de hachage unidirectionnelle.
 - Il s'authentifie également périodiquement pour vérifier si la communication a lieu avec le même appareil ou non.
 - En outre, il offre plus de sécurité que PAP (Password Authentication Procedure) car la valeur utilisée (découverte par la fonction de hachage) est modifiée de manière variable.
 - CHAP nécessite de connaître le texte en clair du secret car il n'est jamais envoyé sur le réseau.

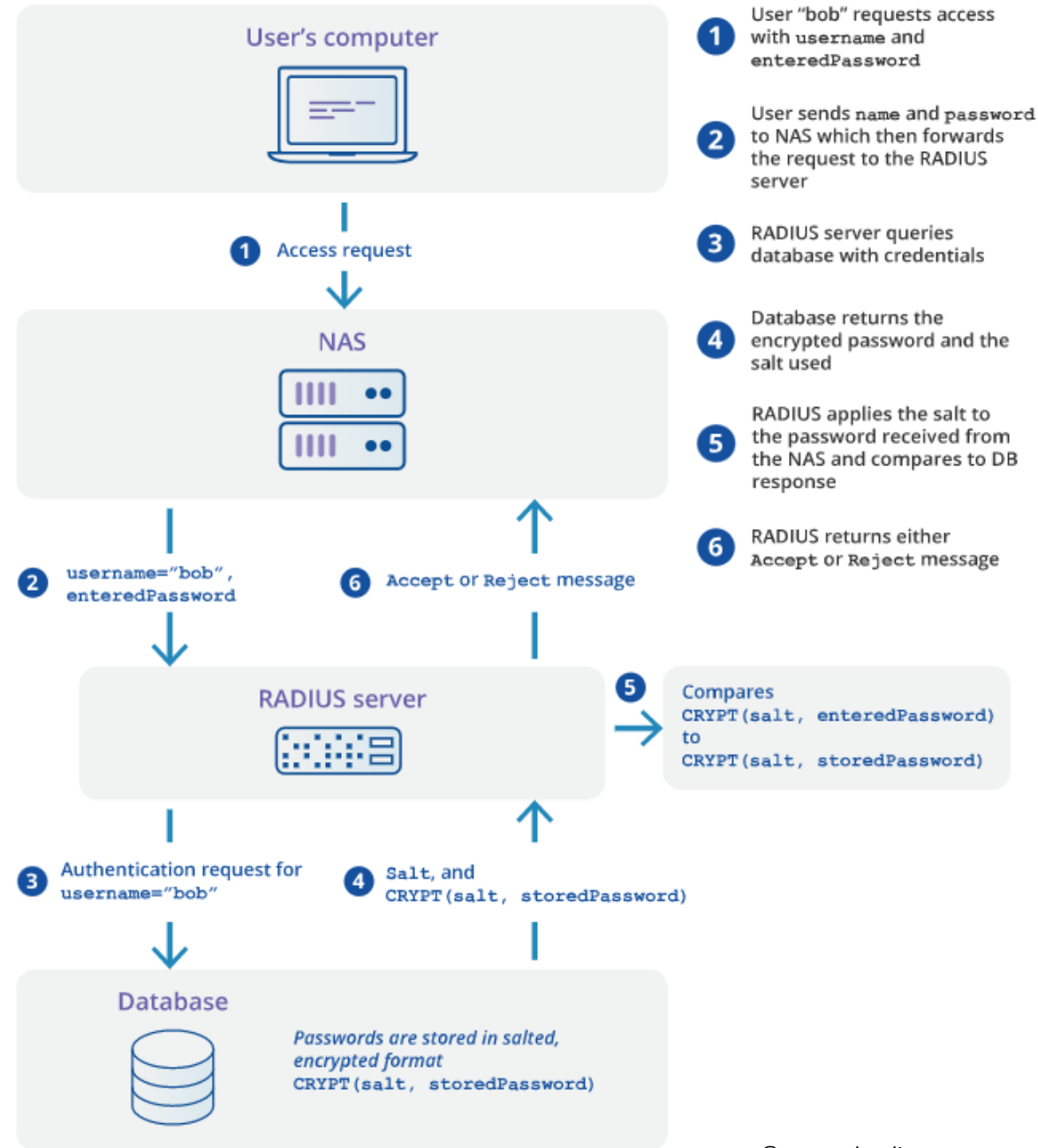
Protocole CHAP

- Il existe 4 types de paquets CHAP :
 - **Challenge packet** : C'est un paquet envoyé, par l'authentificateur au peer, au début du CHAP 3-way Handshake. Le paquet Challenge est également envoyé périodiquement pour vérifier si la connexion n'est pas altérée. Il contient la valeur de l'identifiant, le champ de valeur qui contient une valeur aléatoire et contient également le champ de nom qui contient le nom de l'authentificateur. Le champ de nom est utilisé pour la recherche de mot de passe. Le champ de nom est également transmis au générateur de hachage MD5 et une valeur de hachage unidirectionnelle est générée.
 - **Response Packet** : Il est utilisé pour répondre au paquet challenge. Il contient le champ Valeur qui contient la valeur de hachage unidirectionnelle générée, la valeur de l'identifiant et le champ de nom. Le champ Nom du paquet de réponse est défini sur le nom d'hôte du routeur homologue. Maintenant, le champ Nom du paquet Challenge est recherché pour le mot de passe. Le routeur recherche une entrée qui correspond au nom d'utilisateur dans le champ Nom du paquet Challenge et obtient le mot de passe. Ensuite, ce mot de passe est haché en le transmettant au générateur de hachage MD5 et une valeur de hachage unidirectionnelle est générée. Cette valeur est insérée dans le champ de valeur du paquet de réponse et envoyée à l'authentificateur.
 - **Paquet de réussite** : Maintenant, l'authentificateur effectue également la même chose en recherchant dans le champ de nom (s'il a une entrée pour ce nom d'utilisateur) du paquet de réponse et en l'utilisant, il génère une valeur de hachage. Si la valeur générée est la même que celle de l'homologue, le paquet de réussite est envoyé.
 - **Paquet d'échec** : Si la valeur générée est différente, le paquet d'échec est envoyé au pair.

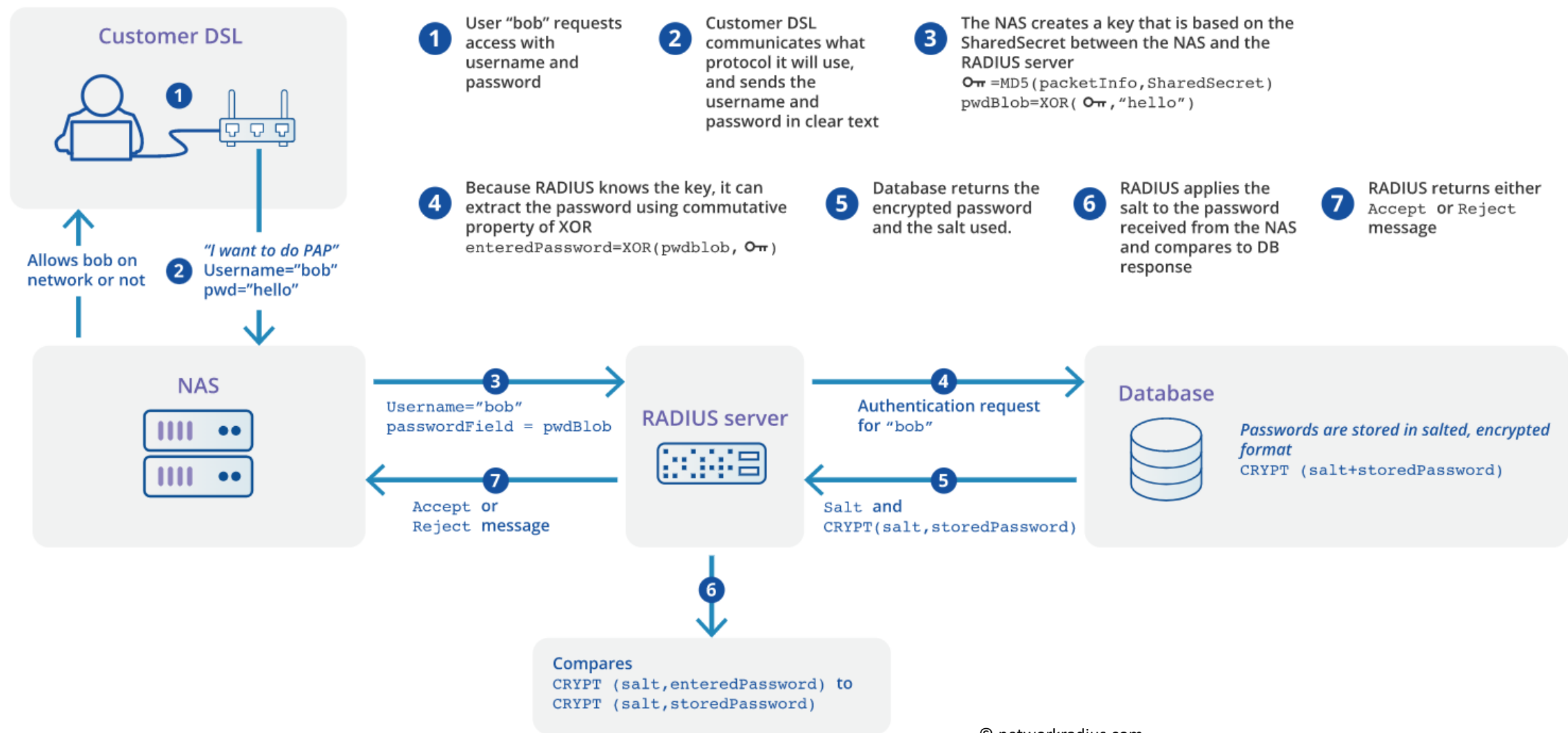
Autres protocoles

- Quatre types de méthodes d'authentification EAP (Extensible Authentication Protocol) :
 - **Protocole d'authentification extensible léger (LEAP)** - Afin d'éliminer la faiblesse du WEP, CISCO introduit une méthode d'authentification sans fil propriétaire appelée LEAP. Pour s'authentifier, le client doit fournir des informations d'identification de nom d'utilisateur et de mot de passe, puis le client et le point d'accès (AP) échangent une phrase de défi cryptée. L'accès est fourni au client si la phrase de défi cryptée correspond. LEAP utilise une clé dynamique pour crypter la phrase contrairement au WEP qui utilise une clé statique. Mais plus tard, il a été trouvé vulnérable, donc LEAP a depuis été déprécié. De nos jours, bien que les appareils sans fil puissent offrir LEAP, vous ne devriez pas l'utiliser.
 - **EAP-FAST** - En outre, CISCO a introduit une méthode plus sécurisée que LEAP appelée EAP Flexible Authentication with secure Tunneling (EAP-FAST). Dans cette méthode, les identifiants d'authentification sont sécurisés en transmettant un identifiant d'accès protégé (PAC) entre l'AS et le client. PAC est une sorte de secret partagé généré par le serveur d'authentification, utilisé pour l'authentification mutuelle. C'est une série de trois phases.
 - Phase-1** : PAC est généré et installé sur les clients.
 - Phase 2** : lors de l'authentification mutuelle, le client et le serveur d'authentification négocient un tunnel de sécurité de la couche de transport (TLS).
 - Phase-3** : Pour plus de sécurité, les clients sont ensuite authentifiés via le tunnel TLS.
 - **EAP protégé (PEAP)** - PEAP est une amélioration supplémentaire par rapport à EAP-FAST. Il utilise également l'authentification externe et interne. L'étape supplémentaire de cette méthode est le certificat numérique. Le serveur d'authentification présente un certificat numérique (DC) aux clients dans l'authentification externe, si les clients sont satisfaits du DC, un tunnel TLS est construit pour l'authentification interne. Le DC se compose de données sous une forme standard qui identifie le propriétaire. Il est validé par une tierce partie appelée autorité de certification (CA). L'autorité de certification est connue et approuvée par les clients et le serveur d'authentification.
 - **EAP-TLS** – PEAP est encore amélioré par EAP-TLS. Dans celui-ci, le certificat numérique est installé à la fois sur l'AS et sur le client. Ils échangent tous les deux un certificat, puis le tunnel TLS est construit pour échanger le matériel de clé de chiffrement. EAP-TLS est considéré comme le plus sécurisé mais la mise en œuvre est un peu complexe. L'installation manuelle du certificat numérique sur des centaines de clients peut s'avérer peu pratique. Une infrastructure à clé publique (PKI) est utilisée pour fournir un certificat en toute sécurité au client et le révoquer lorsque le client ou l'utilisateur n'a plus accès au réseau. EAP-TLS est utilisé uniquement lorsque les clients sans fil peuvent accepter et utiliser des certificats.

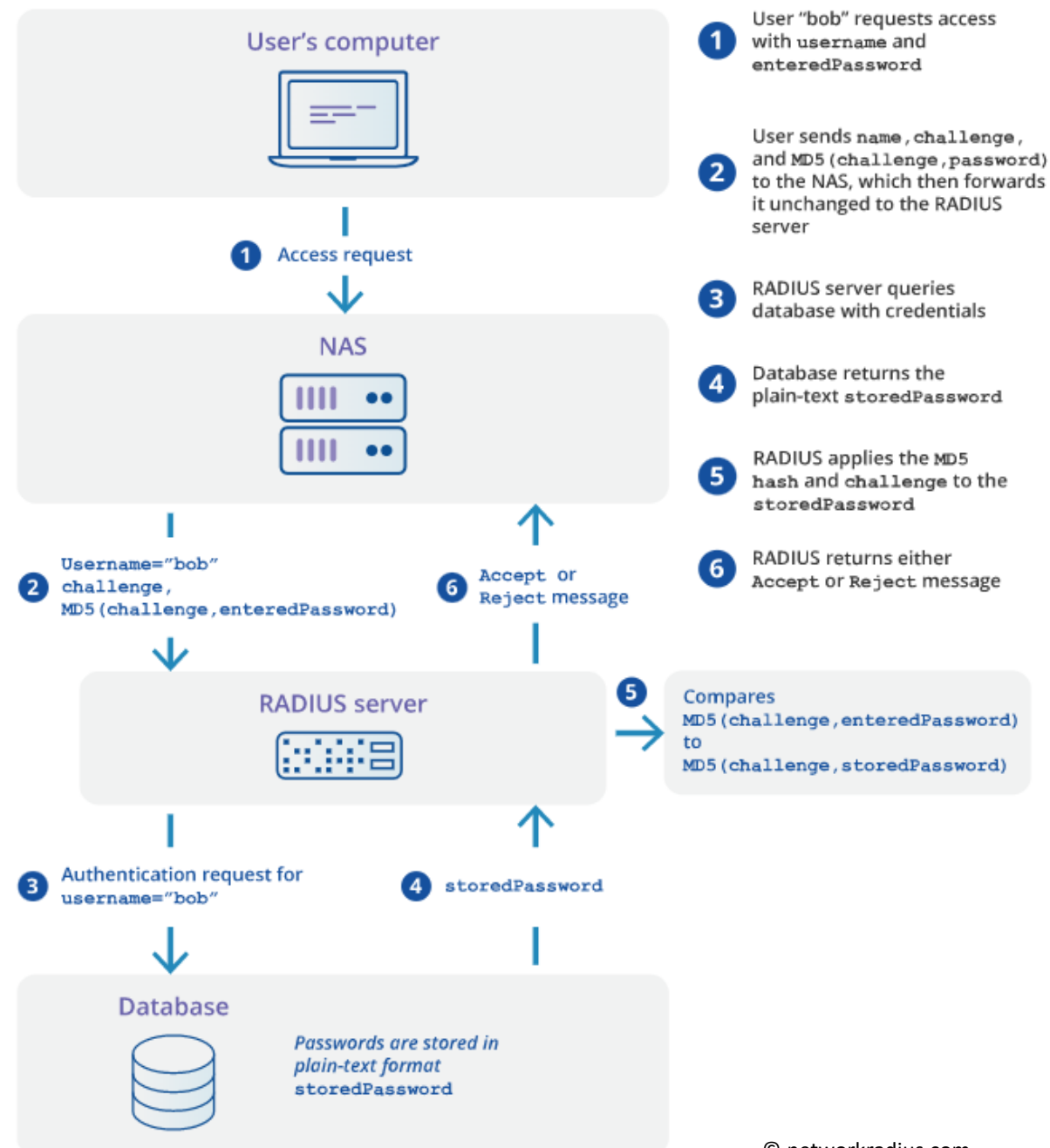
How PAP Works



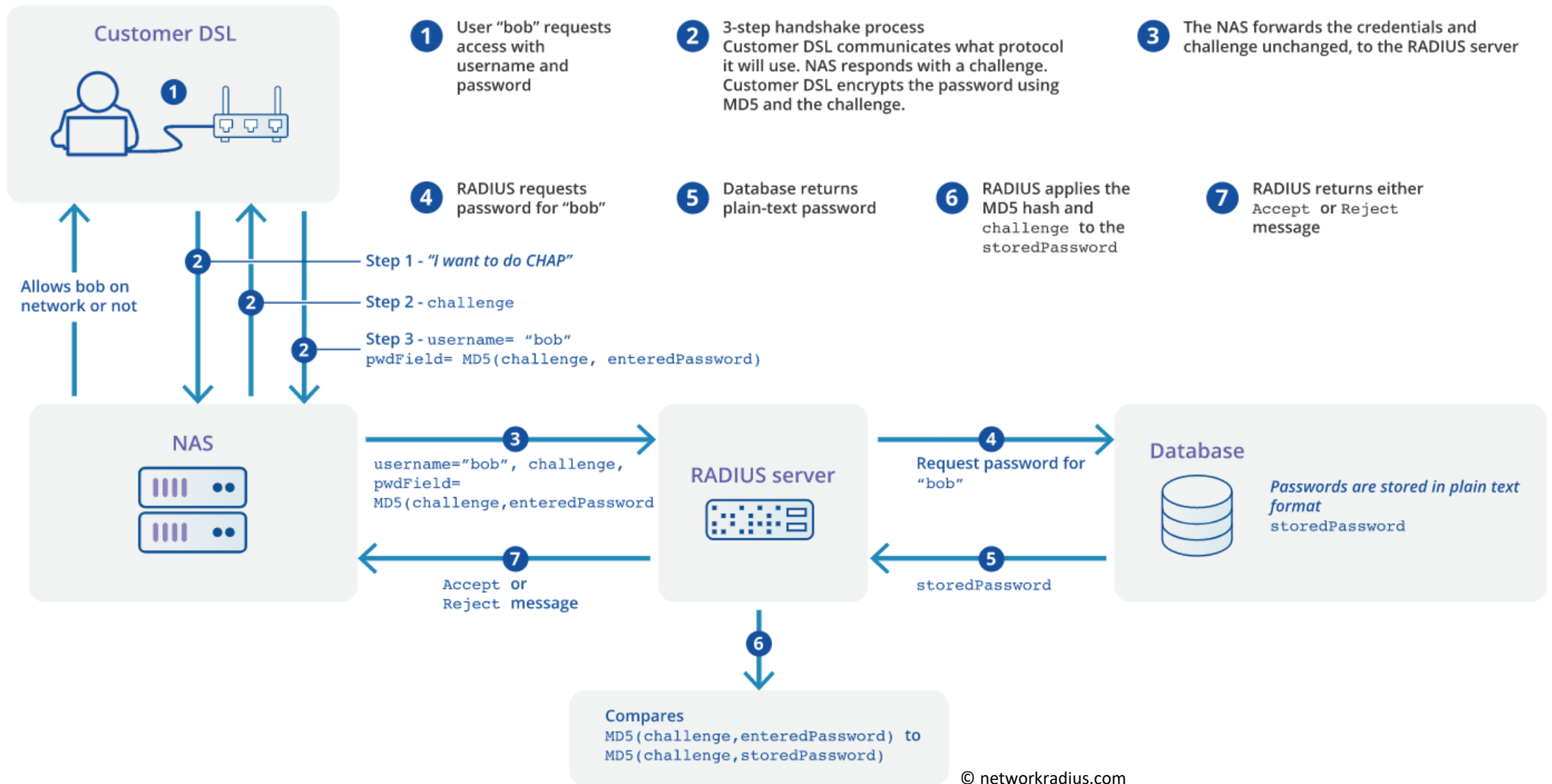
How PAP works



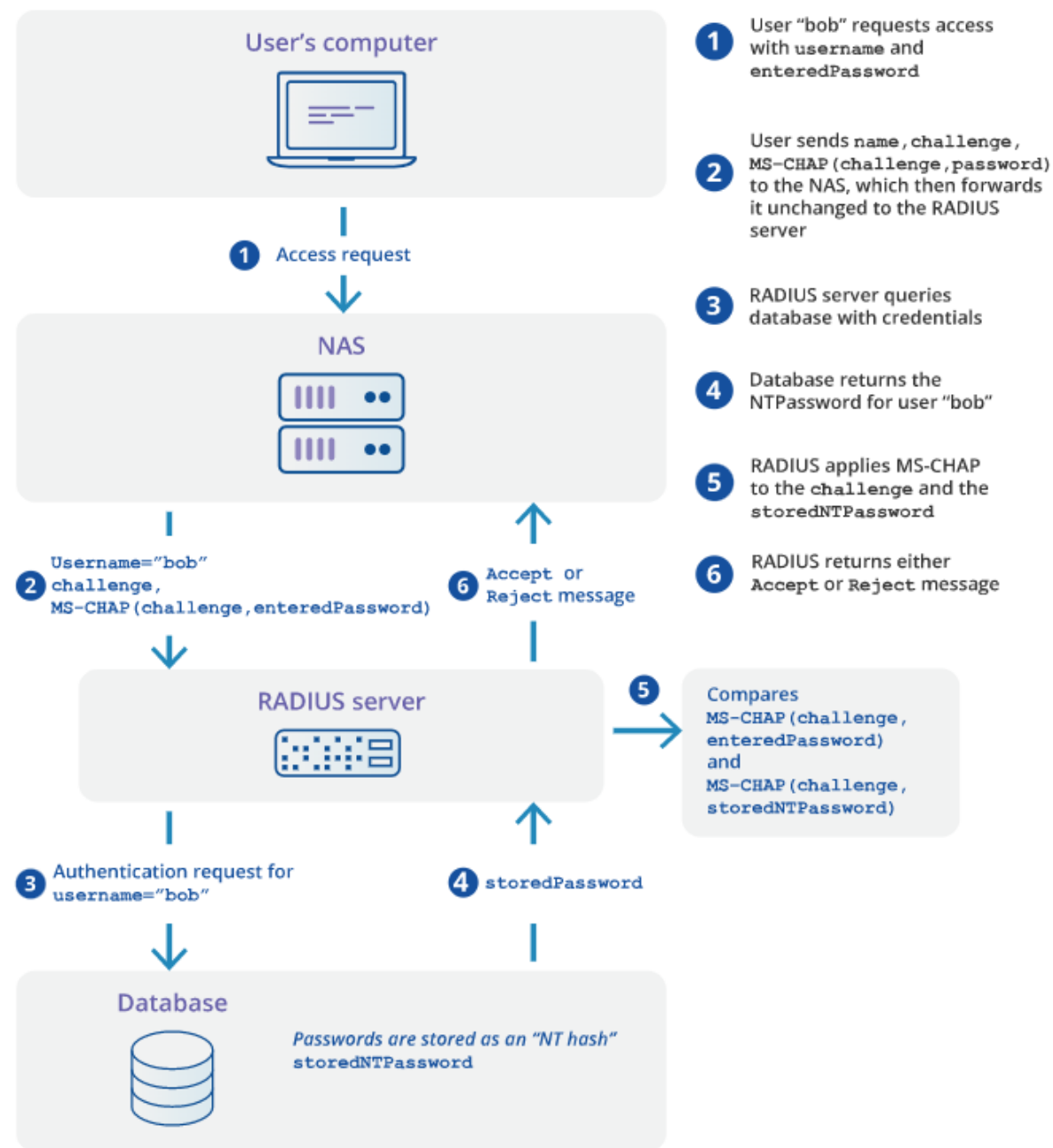
How CHAP Works



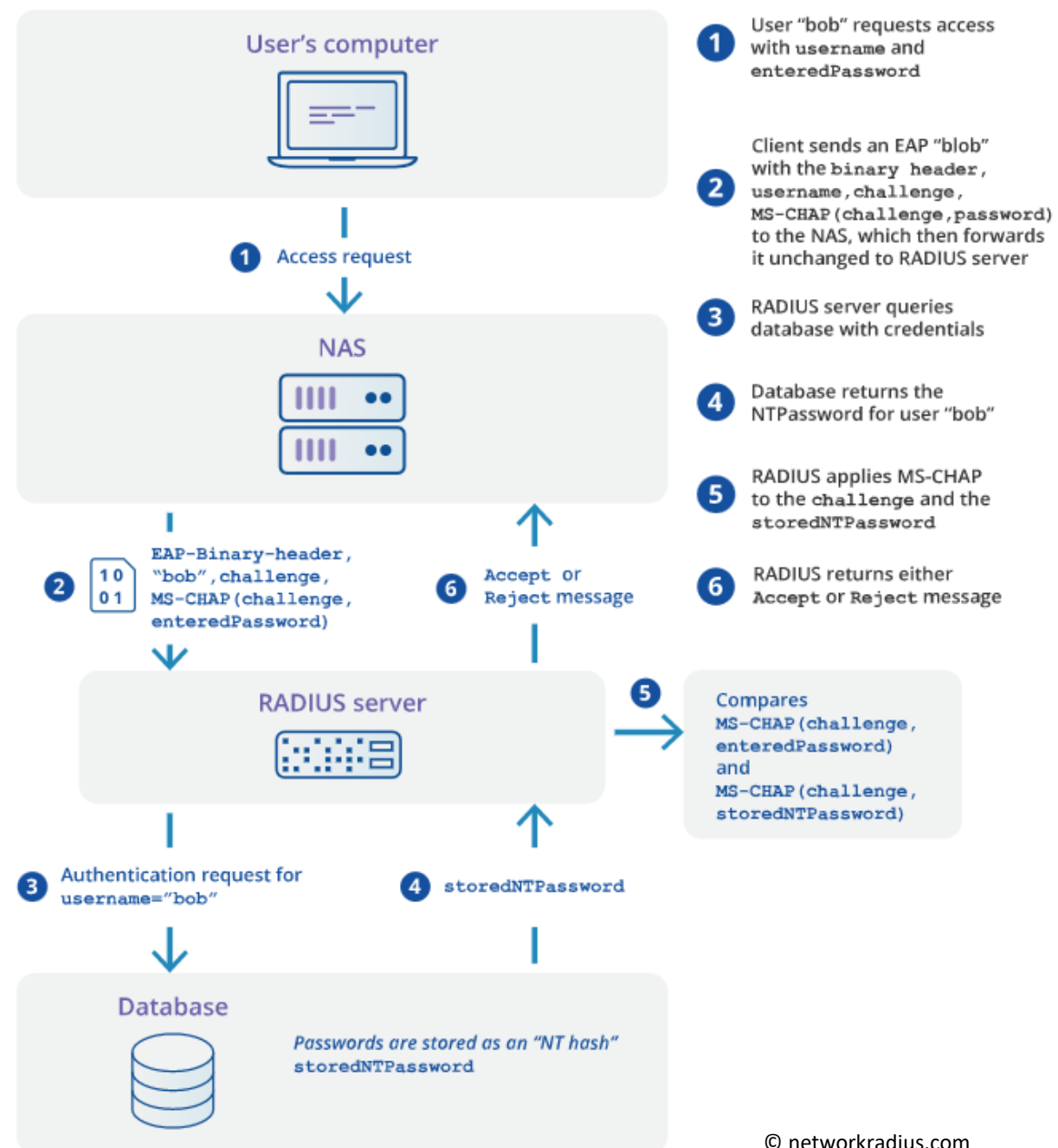
How CHAP works



How MS-CHAP Works



How EAP MS-CHAP Works



WPA2 & WPA3 Enterprise Common Protocols	Level of Encryption	Authentication Speed	Directory Support	Credentials
EAP-TLS	Public-Private Key Cryptography	Fast - 12 Steps	Universal	Passwordless
PEAP-MSCHAPv2	Bad Encryption (MD4, Compromised since 1995)	Slow - 22 Steps	Active Directory	Passwords
EAP-TTLS/PAP	No Credential Encryption	Slowest - 25 Steps	Non-AD LDAP Servers	Passwords

© networkradius.com