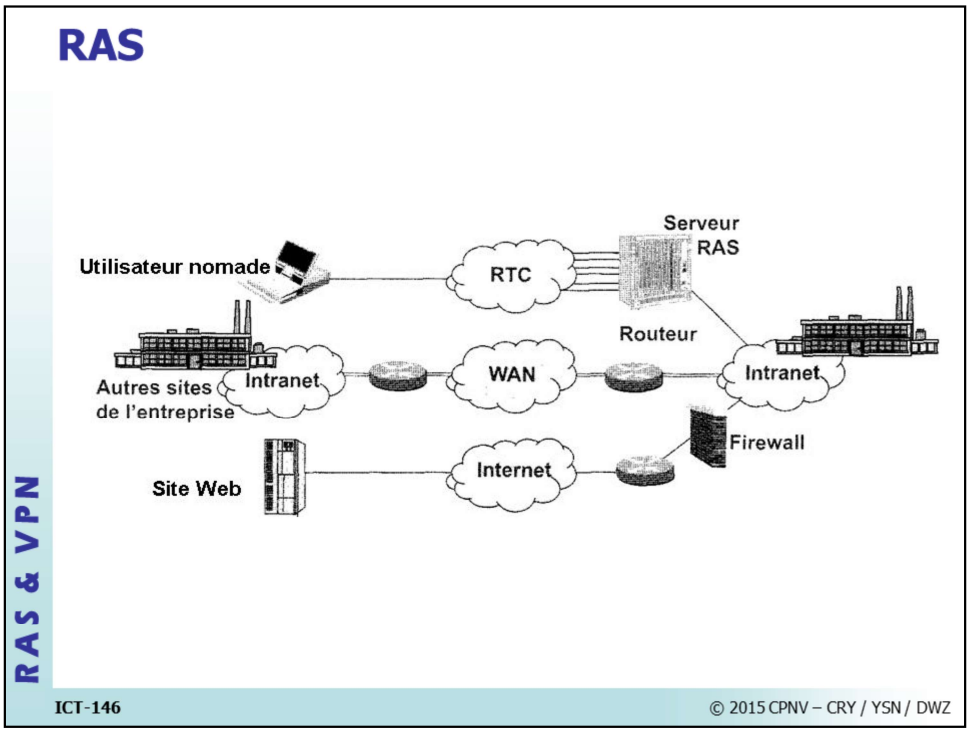

ICT-146
Relier une entreprise à Internet
4 – RAS & VPN
© 2015 CPNV – CRY / YSN / DWZ

146 – Relier une entreprise à Internet

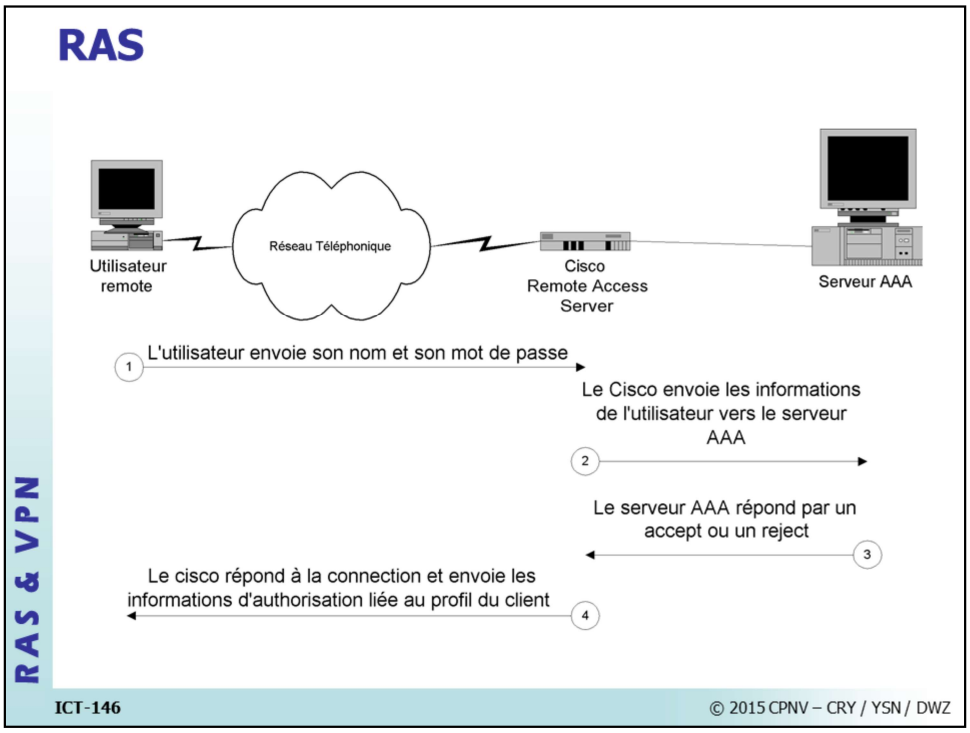


Les **réseaux locaux d'entreprises** (LAN ou RLE) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent **reliés à Internet** par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via Internet.

Pour autant, les données transmises sur Internet sont beaucoup **plus vulnérables** que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit **écouté** par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de **liaisons spécialisées**. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.

Cette approche traditionnelle, en multipliant les modes d'accès, complexifie la maintenance du système et le fragilise en terme de sécurité.



Principe de fonctionnement

Le client (PC, portable ou autre) muni d'un équipement modem ou terminal adapter ISDN se connecte au serveur d'accès RAS par le biais d'une liaison RTC Analogique ou Numérique.

Les données d'authentification fournies par le client sont relayées par le serveur d'accès au serveur AAA. Ce dernier contrôle les autorisations contenues dans sa base de données et retourne sa validation au serveur d'accès.

Si l'utilisateur est authentifié avec succès, il se verra attribuer des paramètres de connexion qui lui sont propres; les droits d'accès aux différents équipements lui seront accordés en fonction de son identité.

Le serveur d'accès maintien les informations de connections afin de pouvoir générer des rapports d'utilisation (accounting).

Access server

Le concentrateur d'accès réseau est équipé d'un port Ethernet et d'un port E1 configuré pour accéder à un PRI (*Primary Rate Interface*) ISDN. Une telle connexion permet l'établissement de 30 appels téléphoniques modem simultanés.

Pour satisfaire aux connections distantes d'origine analogique, l'Access server doit être équipé d'un module qui lui permet de fournir des connections d'origine analogiques par le biais du PRI.

Serveur AAA

Une bonne solution pour le service d'Authentication, d'Authorization et d'Accounting (AAA) est basée sur le protocole RADIUS.

Le dialogue entre le serveur RAS et le serveur AAA se fait par le protocole IP en utilisant des datagrammes UDP sur les ports 1812 pour les requêtes d'authentification et 1813 pour les requêtes d'accounting.

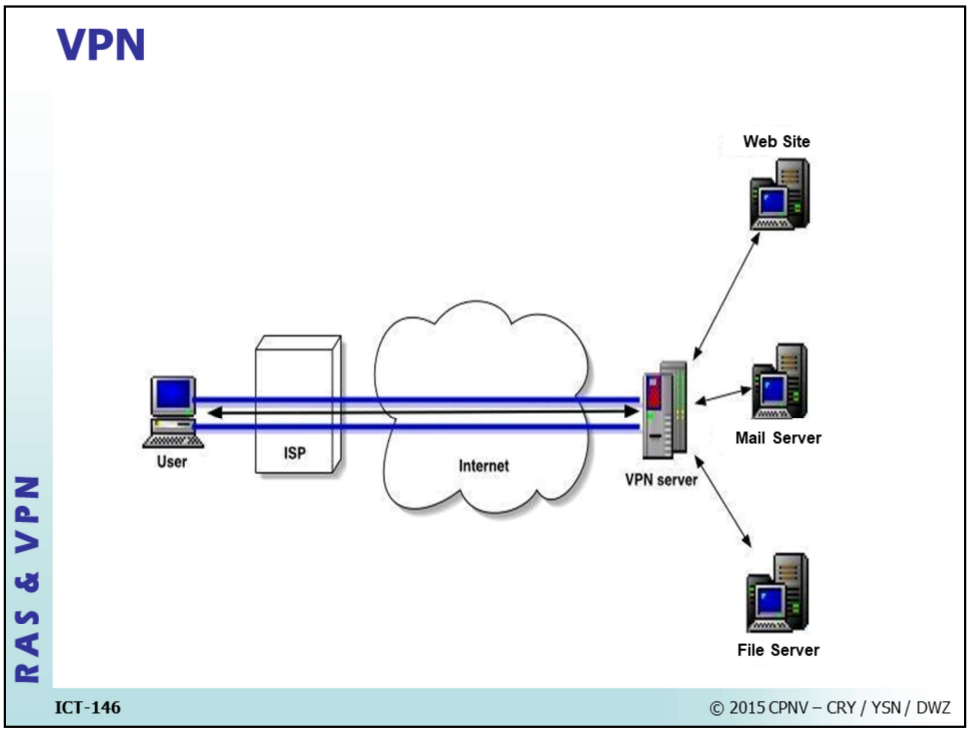
Les spécifications relatives aux mécanismes d'authentification et d'accounting de radius sont définies dans les RFC2138 et 2139.

Dialogue entre le client et le serveur d'accès

Phase	Protocole(s)	Description
1	Etablissement de la connexion ISDN ou analogique	Détection de la signalisation et adaptation de la vitesse de transmission.
2	Etablissement de la liaison Point à Point selon la couche Data Link LCP du protocole PPP	Acquisition des informations d'authentification selon les protocoles PAP, CHAP ou MS-CHAP et négociation des paramètres tels que : Compression de l'en-tête des paquets Callback
3	Couche réseau NCP du protocole PPP	Négociation du "Network Protocol" : TCP/IP, IPX/SPX ou NetBEUI
4	L'étape finale de l'établissement du protocole PPP sur TCP/IP est la négociation des paramètres nécessaires au client RAS par le biais du sous protocole IPCP.	Le client reçoit les informations suivantes : Adresse IP Serveur DNS Serveur WINS Définition des routes Listes d'accès etc.

PAP : *Password Authentication Protocol*. protocole conçu par Cisco. C'est l'un des plus simples dispositifs d'authentification. Le problème est que le client envoie le nom de l'utilisateur et le mot de passe en clair.

CHAP : *Challenge-Handshake Authentication Protocol*. renforce les lacunes de sécurité par le cryptage des informations d'accès (nom et mot de passe) en utilisant un challenge émis par le serveur d'accès. Le protocole **MS-CHAP** est une adaptation de CHAP faite par la société Microsoft.



Le concept de réseau privé virtuel

Un bon compromis aux méthodes traditionnelles d'accès à distance consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation (en anglais ***tunneling***), c'est-à-dire en encapsulant les données à transmettre de façon **chiffrée** à l'intérieur d'une transmission non sécurisée. On parle alors de réseau privé virtuel (noté RPV ou ***VPN***, acronyme de ***Virtual Private Network***) pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit *virtuel* car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.

Le système de VPN permet donc d'obtenir une **liaison sécurisée** à moindre coût, si ce n'est la mise en oeuvre des équipements terminaux. En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.

Fonctionnement d'un VPN

Un réseau privé virtuel repose sur un protocole, appelé **protocole de tunnelisation** (*tunneling*), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un *VPN* établi entre deux machines, on appelle *client VPN* l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et *serveur VPN* (ou plus généralement **serveur d'accès distant**) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur.

Les protocoles de tunnelisation

Les principaux protocoles de tunneling sont les suivants :

- **PPTP** (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2F** (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- **L2TP** (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'*IETF* (RFC 2661) pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

Le protocole PPTP

Le principe du protocole PPTP (*Point To Point Tunneling Protocol*) est de créer des trames sous le protocole PPP et de les encapsuler dans un datagramme IP.

Ainsi, dans ce mode de connexion, les machines distantes des deux réseaux locaux sont connectés par une connexion point à point (comprenant un système de chiffrement et d'authentification, et le paquet transite au sein d'un datagramme IP.

De cette façon, les données du réseau local (ainsi que les adresses des machines présentes dans l'en-tête du message) sont encapsulées dans un message PPP, qui est lui-même encapsulé dans un message IP.

Le protocole L2TP

Le protocole L2TP est un protocole standard de tunnelisation très proche de PPTP. Ainsi le protocole L2TP encapsule des trames du protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS).

Le protocole IPSec

IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir l'authentification, l'intégrité et la confidentialité des échanges.

Le protocole IPSec est basé sur trois modules :

IP Authentification Header (**AH**) qui fournit l'authentification et l'intégrité.

Encapsulating Security Payload (**ESP**) qui fournit l'authentification, l'intégrité et la confidentialité.

Security Assocation (**SA**) qui définit l'échange des clés et des paramètres de sécurité.

IPSec fonctionne selon deux modes : **tunnel** et **transport**. Dans le cadre du mode transport, seules les données des protocoles de niveaux supérieurs sont protégées. Dans le cadre du mode tunnel, il crée un nouveau paquet IP encapsulant celui qui doit être transporté. Les deux modes peuvent utiliser la sécurisation par AH, par ESP ou les deux.