UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Seguridad y Alta Disponibilidad

Virtual Private Networks

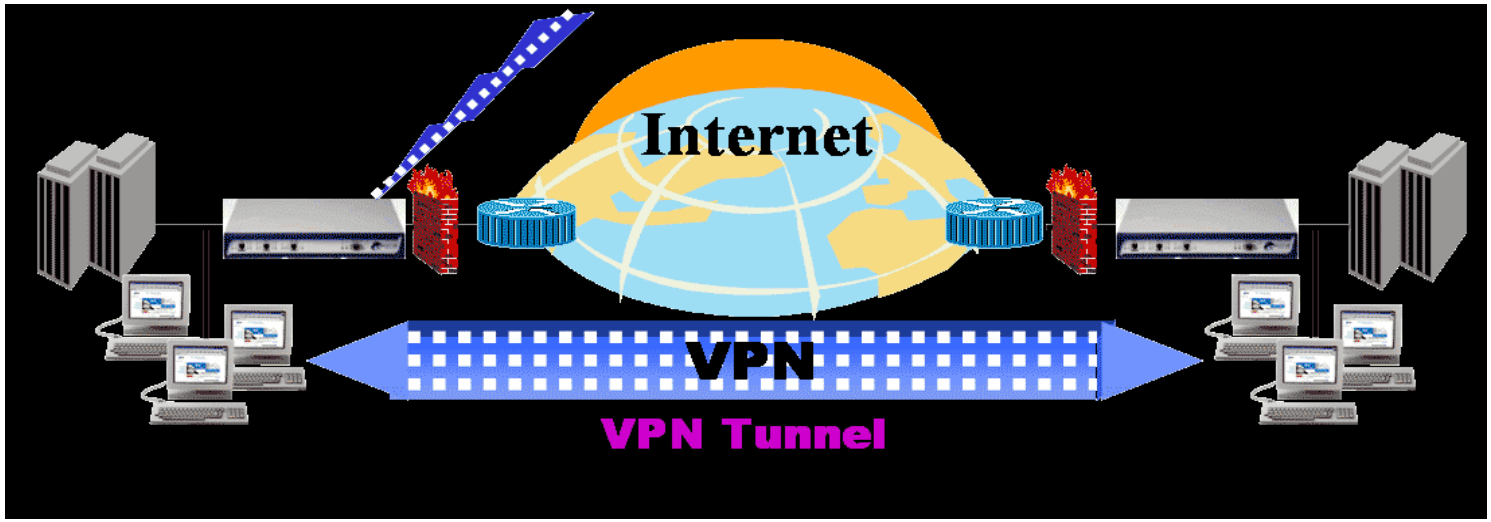
Félix Villanueva Molina
Escuela Superior de Informática
Universidad de Castilla-La Mancha

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Introducción

- Definición:
  - Transportar datos privados sobre una infraestructura de red pública
    - Ejemplo: Conectar dos sedes de una misma empresa a través de internet
      - El acceso a los datos sólo puede realizarse si formas parte de la VPN
    - Extiendes la red local
  - Generalmente, los datos de la VPN que viajan por la red pública van encriptados.
  - Desde el punto de vista del usuario/aplicación se da la visión de una única red.

Introducción



Fuente:
http://www.taringa.net/posts/ebooks-tutoriales/5492417/firewall-y-redes-privadas-virtuales_.html

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Clasificación

- Encriptadas vs no encriptadas
  - Encriptadas: utilizan encriptación para asegurar el tráfico a través de la red publica
  - No encriptadas: ejemplo MPLS VPN, deben confiar en el ISP para el tema de seguridad.
- Las VPN encriptadas predominan.

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Clasificación

- Nivel OSI:
  - Enlace: Las redes privadas que forman la VPN se conectan a través de la capa de enlace.
    - Muchos protocolos de la capa de enlace no proveen encriptación
  - Red: se crean túneles a nivel de red
    - Ejemplo IPSec
  - Aplicación: se conectan a través de la capa de aplicación
    - Ejemplo SSH o SSL

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Clasificación

- VPN de acceso remoto
  - Los usuarios se conectan con la empresa a través de Internet desde cualquier sitio
    - Ej. Cuando nos conectamos con nuestro banco.
  - Conectan a internet y mediante un software VPN utilizan protocolos para establecer un túnel (normalmente encriptado) con protocolos como PPTP o L2TP/IPSec
- VPN sitio-a-sitio
  - Utilizan la infraestructura pública (Ej. Internet) para establecer una red global que cubra una empresa o institución
    - Se unen las sedes “extendiendo” la red local

Clasificación

- VPN interna
  - Estructurar la red interna en la gestión de la entidad, usa la red local.
    - Por ejemplo solo los responsables de pedidos pueden manejar el presupuesto.
  - Generalmente puede ir asociado al uso de VLAN
  - Los AP wifi suelen ir en su propia VLAN y tambien se conectan mediante una vpn.

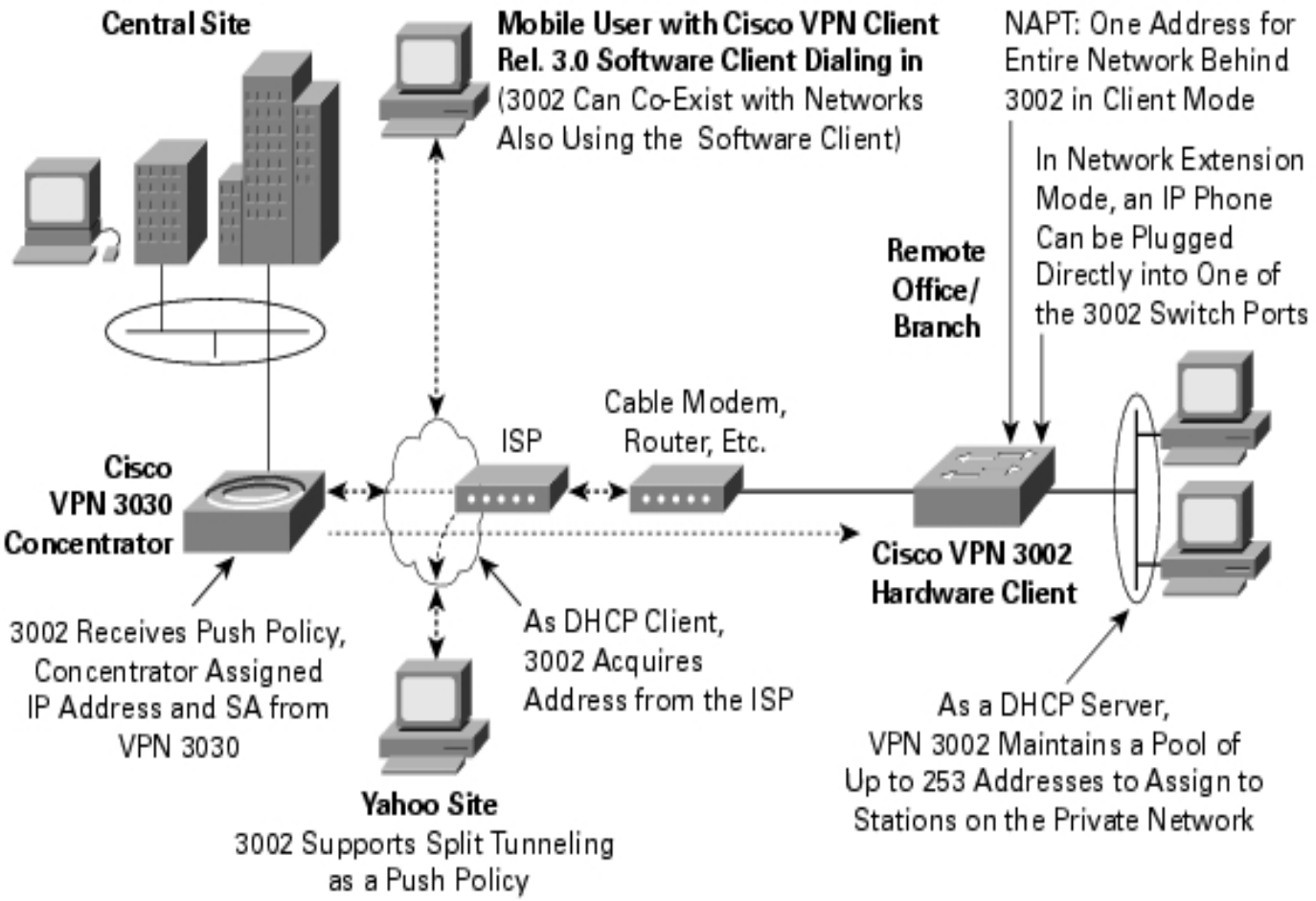
UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Implementaciones

- Basadas en hardware
  - Escalan mejor
  - Mas eficientes
  - La configuración y el despliegue se suele hacer desde un punto central
  - Transparente desde el punto de vista de las aplicaciones y el sistema operativo
  - Se suelen usar en VPN sitio-a-sitio
    - Siempre suelen estar activas

Implementaciones

- Hardware



Fuente:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_data_sheet09186a00801089cf.html

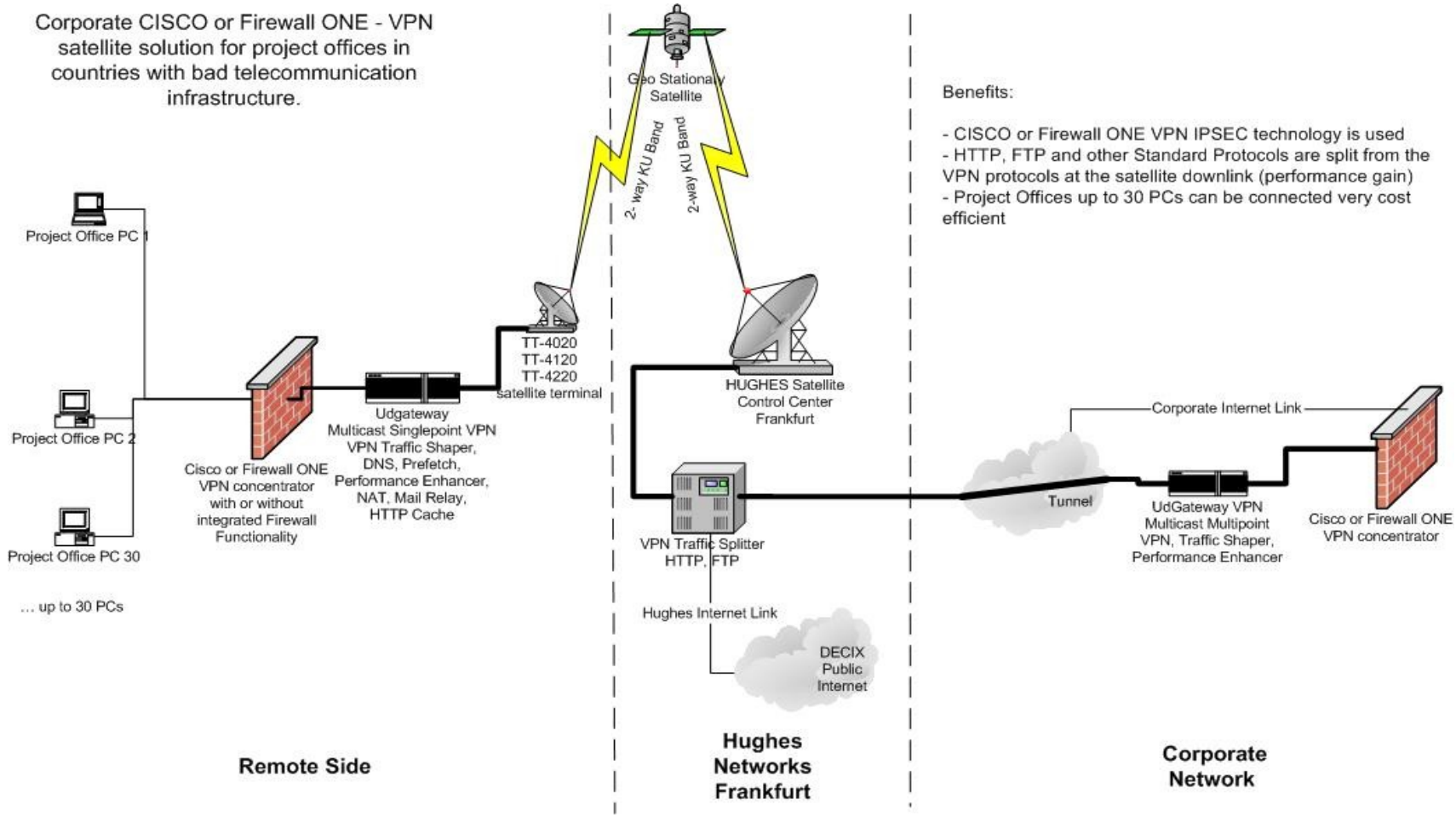
UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Implementaciones

- Basadas en firewall
  - Los firewalls modernos incluyen el software necesario para establecer VPN
  - Pueden ser utilizados en VPN sitio-a-sitio o en VPN de acceso-remoto

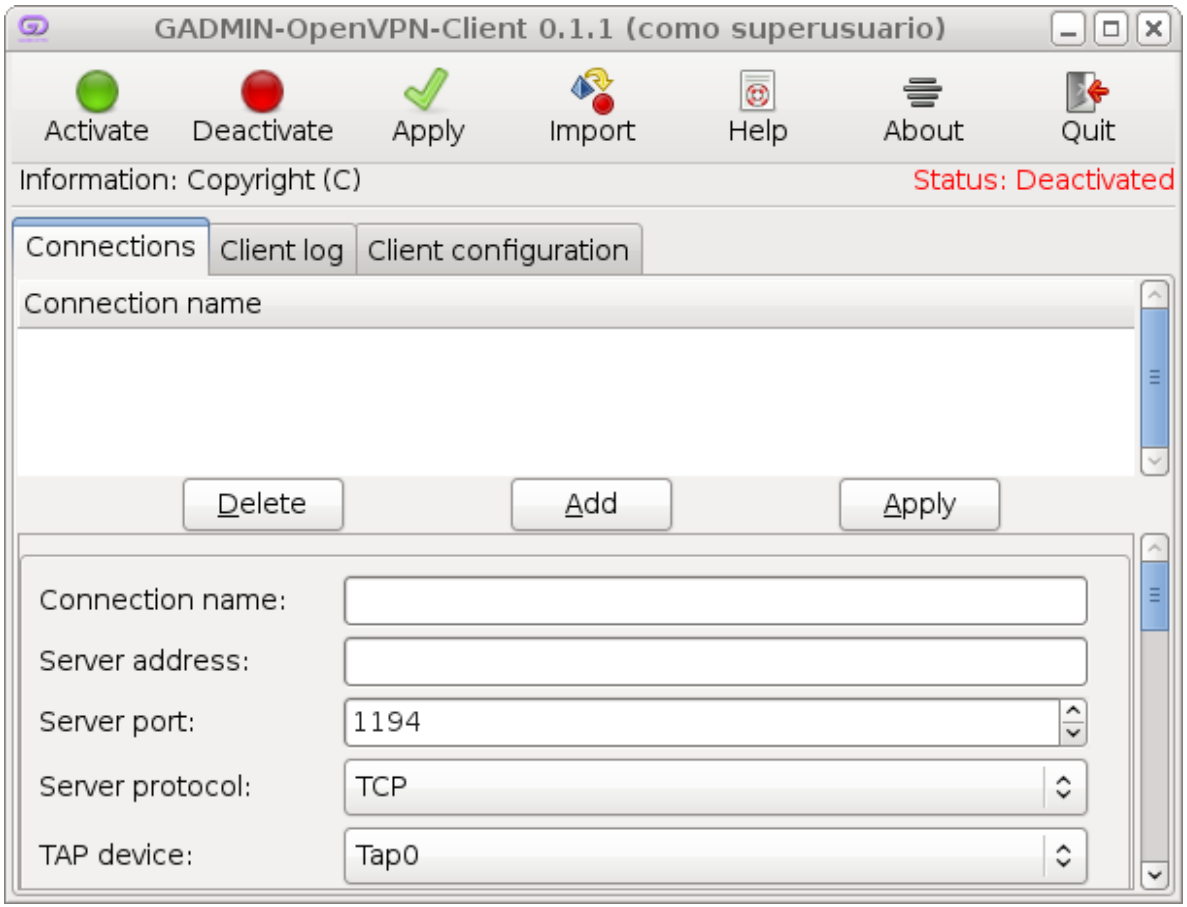
Implementaciones

- Basadas en firewall



Implementaciones

- Basadas en software
  - En VPN acceso-remoto
  - Mas configurables



UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Shell seguras SSH

- Substituto del clásico telnet
- Permite establecer una shell en una máquina remota a través de la red.
- Todo ello de forma segura
- Establecer túneles seguros para otras aplicaciones.
- No permite que las contraseñas viajen en claro.

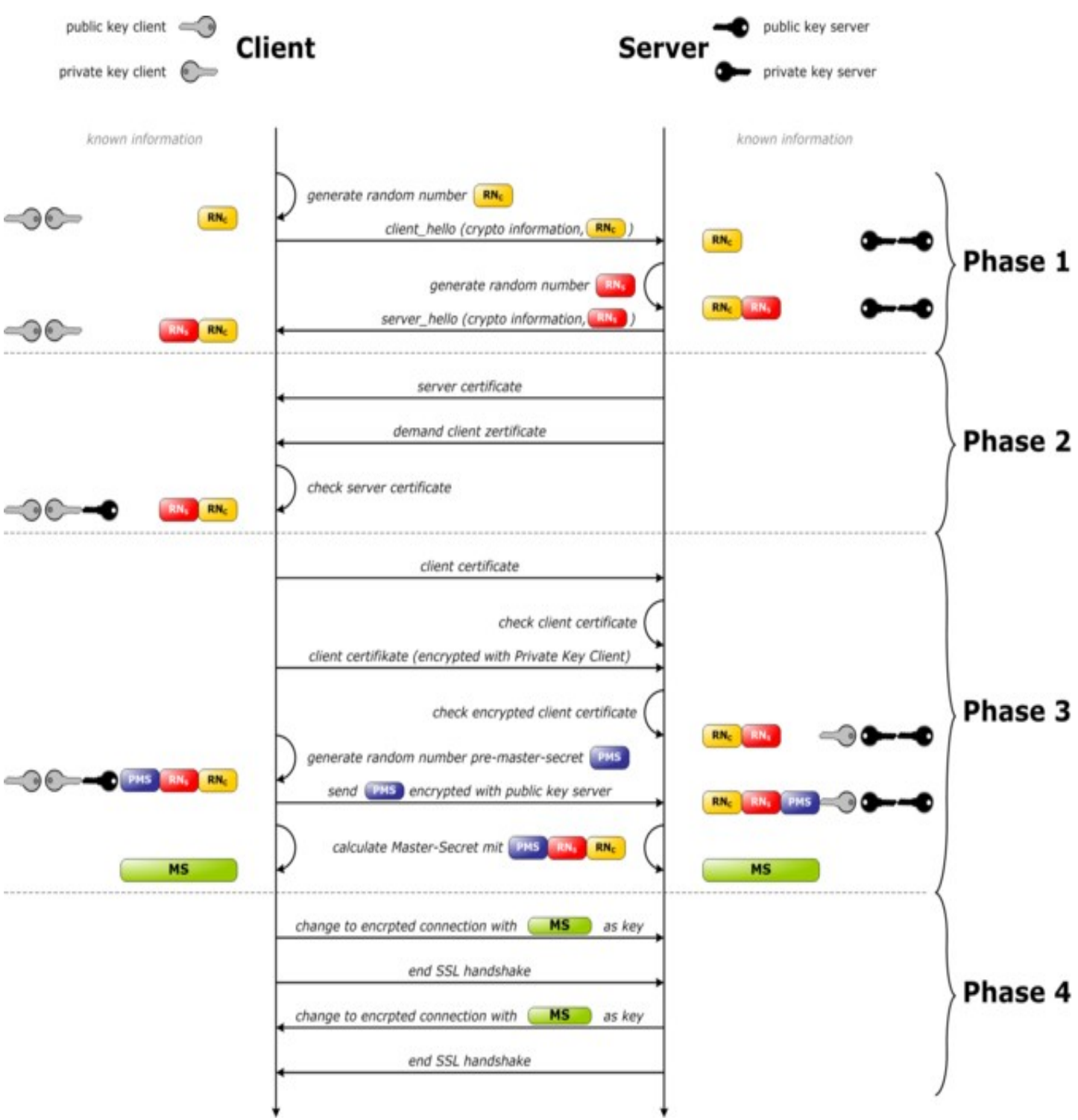
FUENTE: http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a0080088716.html

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Características SSH.

- Encriptación en la capa de transporte
- Autenticación entre el cliente y el servidor
- Interacción encriptada.
- Se pueden configurar varios métodos de autenticación
- Se negocian en la fase inicial.

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA



Autor:

Christian Friedrich

OpenSSH: configuración

- sh_config: Archivo de configuración del sistema cliente SSH por defecto que se sobreescribe si hsay alguno ya presente en el directorio principal del usuario (~/.ssh/config)
- sshd_config: Archivo de configuración para el demonio sshd
- ssh_host_dsa_key: Clave privada DSA usada por el demonio sshd
- ssh_host_dsa_key.pub: Clave pública DSA usada por el demonio sshd
- ssh_host_key: Clave privada RSA usada por el demonio sshd para SSH v1
- ssh_host_key.pub: Clave pública RSA usada por el demonio sshd para SSH v1
- ssh_host_rsa_key: Clave privada RSA usada por el demonio sshd para SSH v2
- ssh_host_rsa_key.pub: Clave pública RSA usada por el demonio sshd para SSH v2

Fuente:
José Raúl López Medina
“Protocolo SSH”

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

OpenSSH: configuración

- Directorio principal del usuario ~/.ssh/:
- authorized_keys: Lista de claves públicas "autorizadas". Cuando un cliente se conecta al servidor, el servidor valida al cliente chequeando su clave pública firmada almacenada dentro de este archivo
- id_dsa: Clave privada DSA del usuario
- id_dsa.pub: Clave pública DSA del usuario
- id_rsa: Clave RSA privada usada por ssh para SSH v2
- id_rsa.pub: La clave pública RSA usada por ssh para SSH v2
- identity: La clave privada RSA usada por ssh para SSH v1
- identity.pub: La clave pública RSA usada por ssh para SSH v1
- known_hosts: Claves de host DSA de los servidores SSH accedidos por el usuario. Este archivo es muy importante para asegurarse de que el cliente SHH está conectado al servidor SSH correcto

Fuente:
José Raúl López Medina
“Protocolo SSH”

Configuración servidor.

Ejemplo práctico: SSH.pdf

Fuente:
Http://sopa.dis.ulpgc.es/ii-aso/portal_aso/leclinux/seguridad/ssh/ssh.pdf

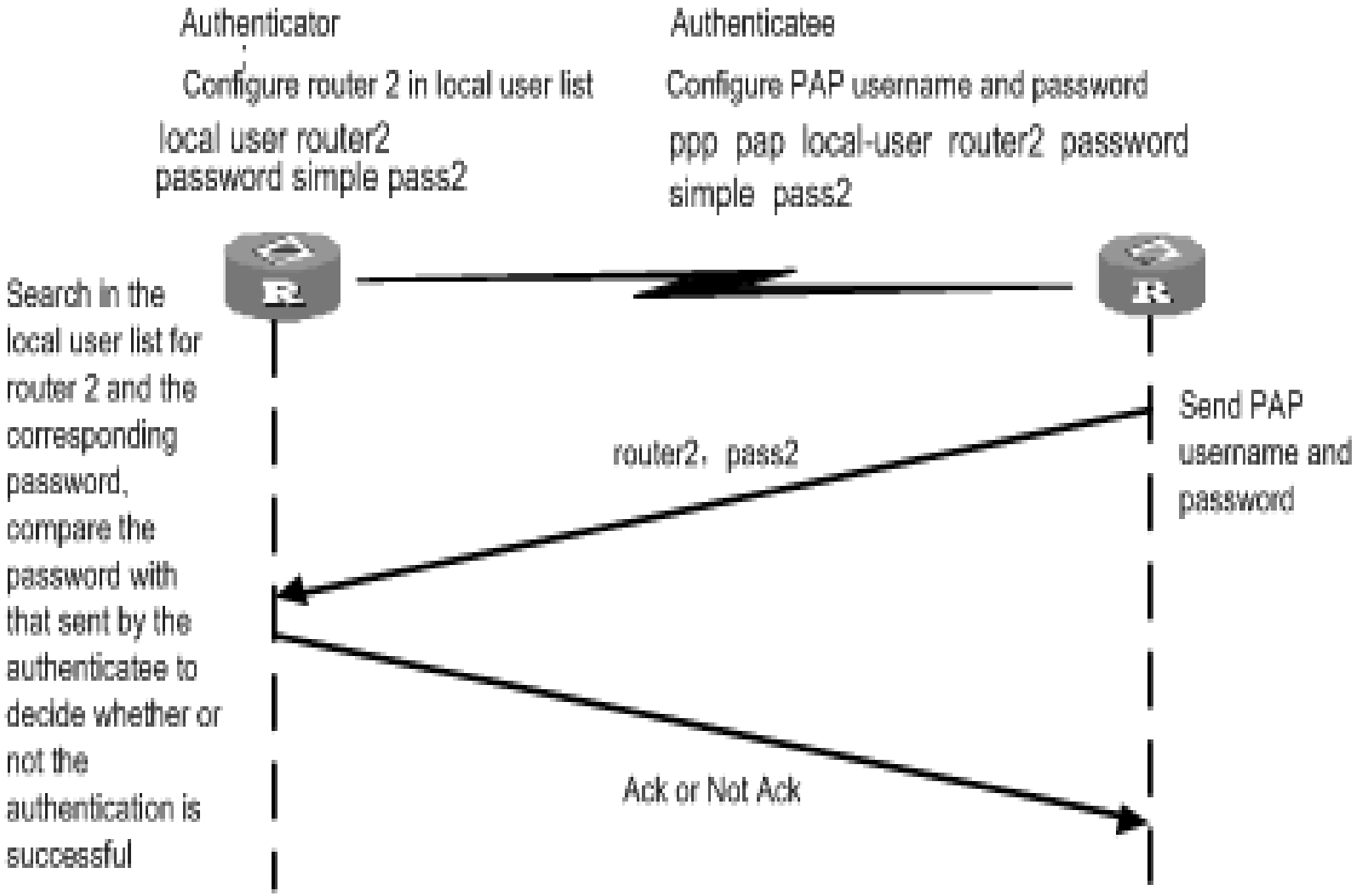
Protocolos/Esquemas de autenticación

- Los protocolos de autenticación permiten verificar la identidad de la persona/servicio que desea acceder a un recurso.
- Son el primer paso en todos los procesos seguros
- Multitud de opciones
  - Protocolo de autenticación de contraseña (PAP)
  - Protocolo de autenticación por desafío mutuo (CHAP)
  - Protocolo de autenticación extensible(EAP)

Protocolo de autenticación de contraseña

- Nombre de usuario y contraseña se envían sin cifrar
- No es seguro
  - Una captura del PPP permite ver la contraseña

Protocolo de autenticación de contraseña



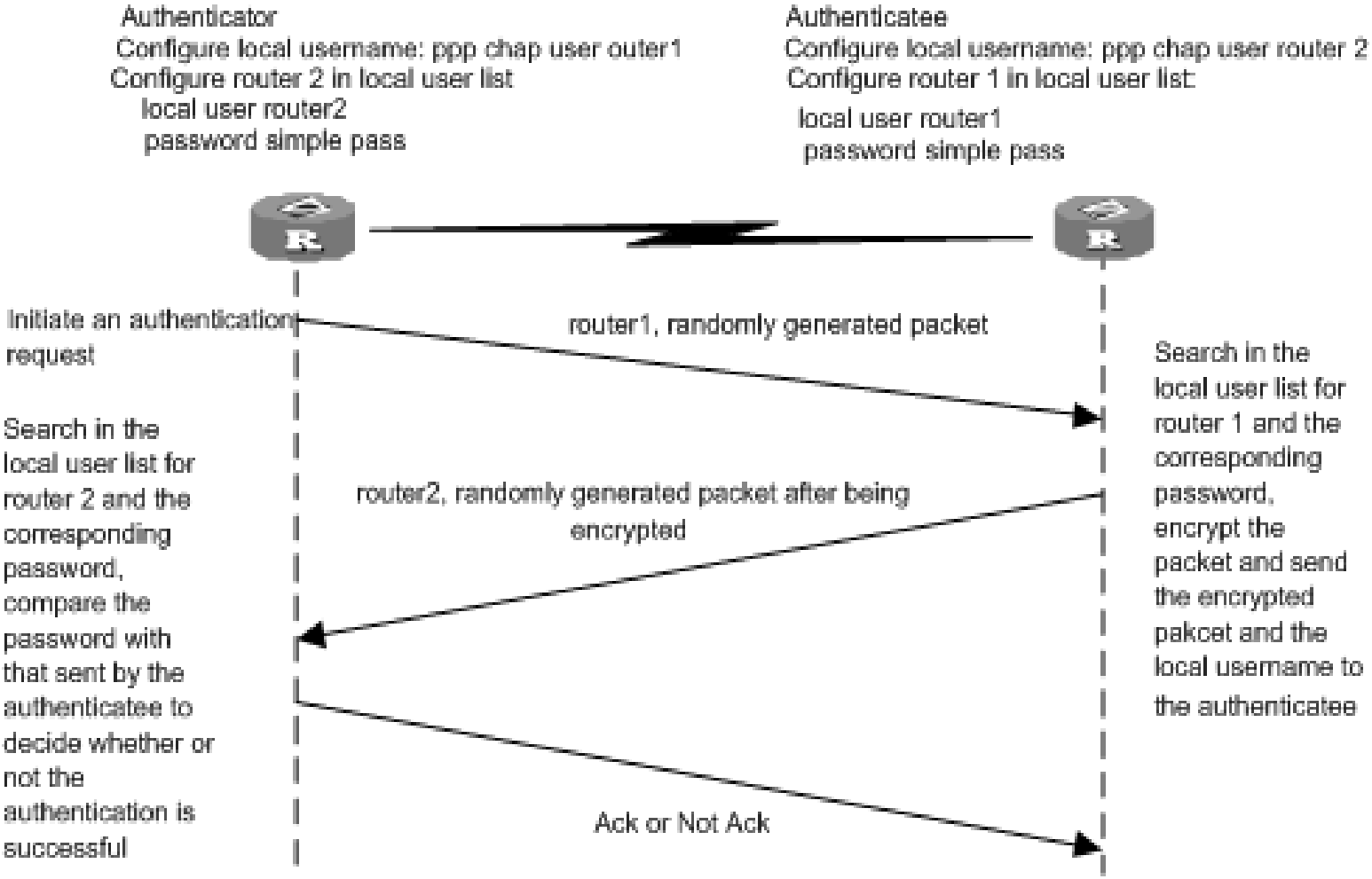
Fuente:
http://www.h3c.jp/jp/Products___Solutions/Technology/WAN/PPP/200701/200808_6666_0.htm

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Protocolo de autenticación por desafío mutuo

- El cliente envía una petición de acceso
  - Un hash con su contraseña (no la contraseña en si mismo)
- El servidor manda un desafío
- El cliente utiliza un algoritmo hash (MD5) para calcular un resultado con su contraseña y el desafío
  - Lo envía al servidor
- El servidor compara y permite o no el acceso

Protocolo de autenticación por desafío mutuo



Fuente:
http://www.h3c.jp/jp/Products___Solutions/Technology/WAN/PPP/200701/200808_6666_0.htm

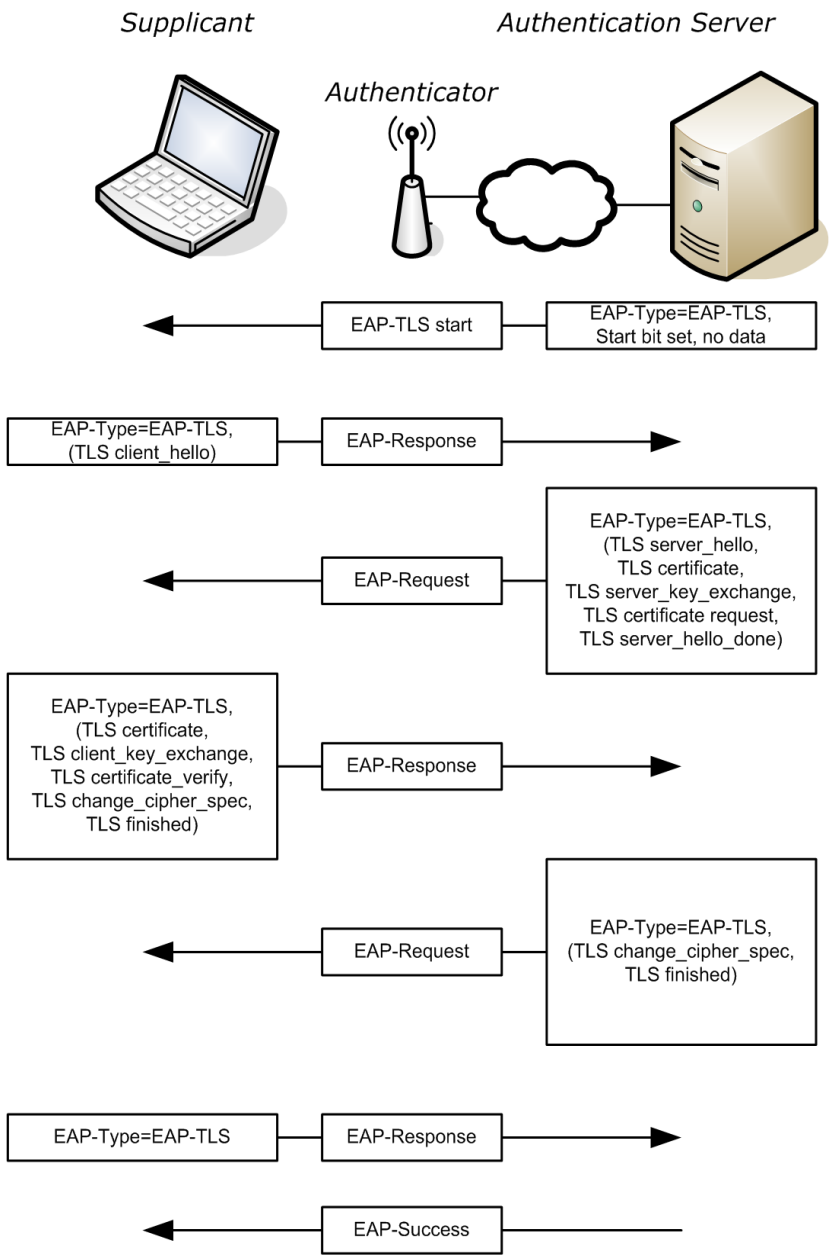
UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Protocolo de autenticación extensible

- Admite varios métodos de autenticación
  - Es mas una arquitectura que un protocolo
  - Generalmente se usan los basados en certificados
  - Muy usado en redes inalámbricas y conexiones punto a punto
  - Usado en WPA2 y WPA
    - Permiten 5 esquemas de EAP:
      - EAP-TLS, EAP-SIM, EAP-AKA, etc.
  - También existen problemas:
    http://www.infosecwriters.com/text_resources/pdf/SSotillo_EAP.pdf

EAP-TLS

- Transport-Layer-Security
- RFC 5216
- Uno de los mas seguros
- Habitual en dispositivos inalámbricos



Ejemplo:
http://www.dartmouth.edu/~pkilab/pages/EAP-TLSwFreeRadius.html

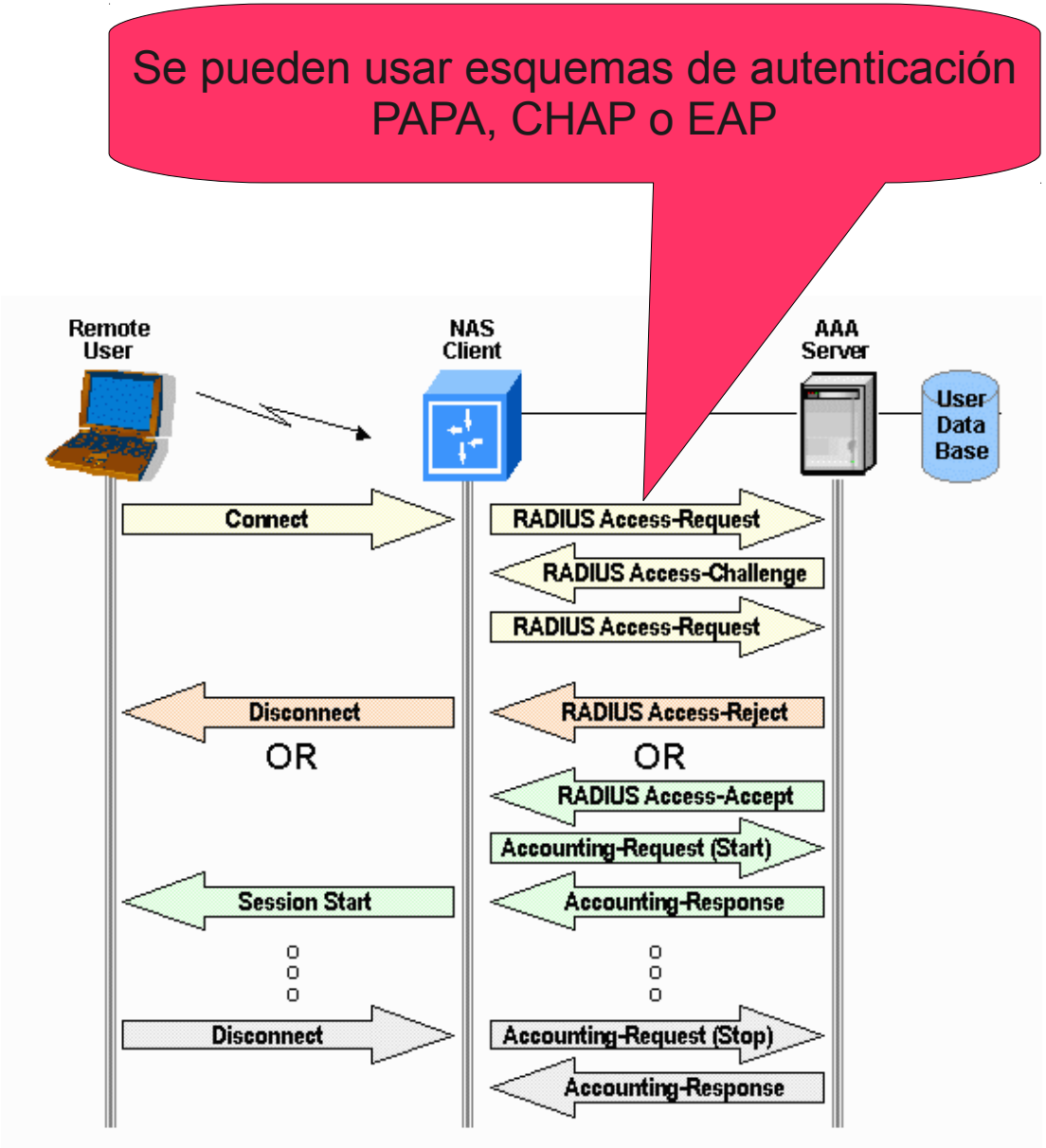
UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

RADIUS

- Remote Authentication Dial In User Service
- Servidores de control de acceso
  - Los servicios de red delegan en ellos la autorización
- Otros ejemplos de servicios de control de acceso es TACACS+ (Terminal Access Controller Access System)
  - RFC 1492

RADIUS

- RFC 2138
- Es mas que un protocolo de Autenticación
  - Es un protocolo AAA (Autenticación, Autorización y Administración)



Fuente:
http://www.wi-fiplanet.com/tutorials/article.php/3114511/Using-RADIUS-For-WLAN-Authentication-Part-I.htm

RADIUS

- Usado por el estándard de seguridad 802.11x
- Comparativa:

Protocol	Authentication			Authorization			Accounting		
	Tunnel access	Console access	Cut-through Proxy	Tunnel access	Console access	Cut-through Proxy	Tunnel access	Console access	Cut-through Proxy
Local	X	X	X	X	X*				
RADIUS	X	X	X	X		X	X	X	X
TACACS+	X	X	X		X	X	X	X	X
SDI	X								
NT	X								
Kerberos	X								
LDAP				X					

* Command authorization by privilege level only

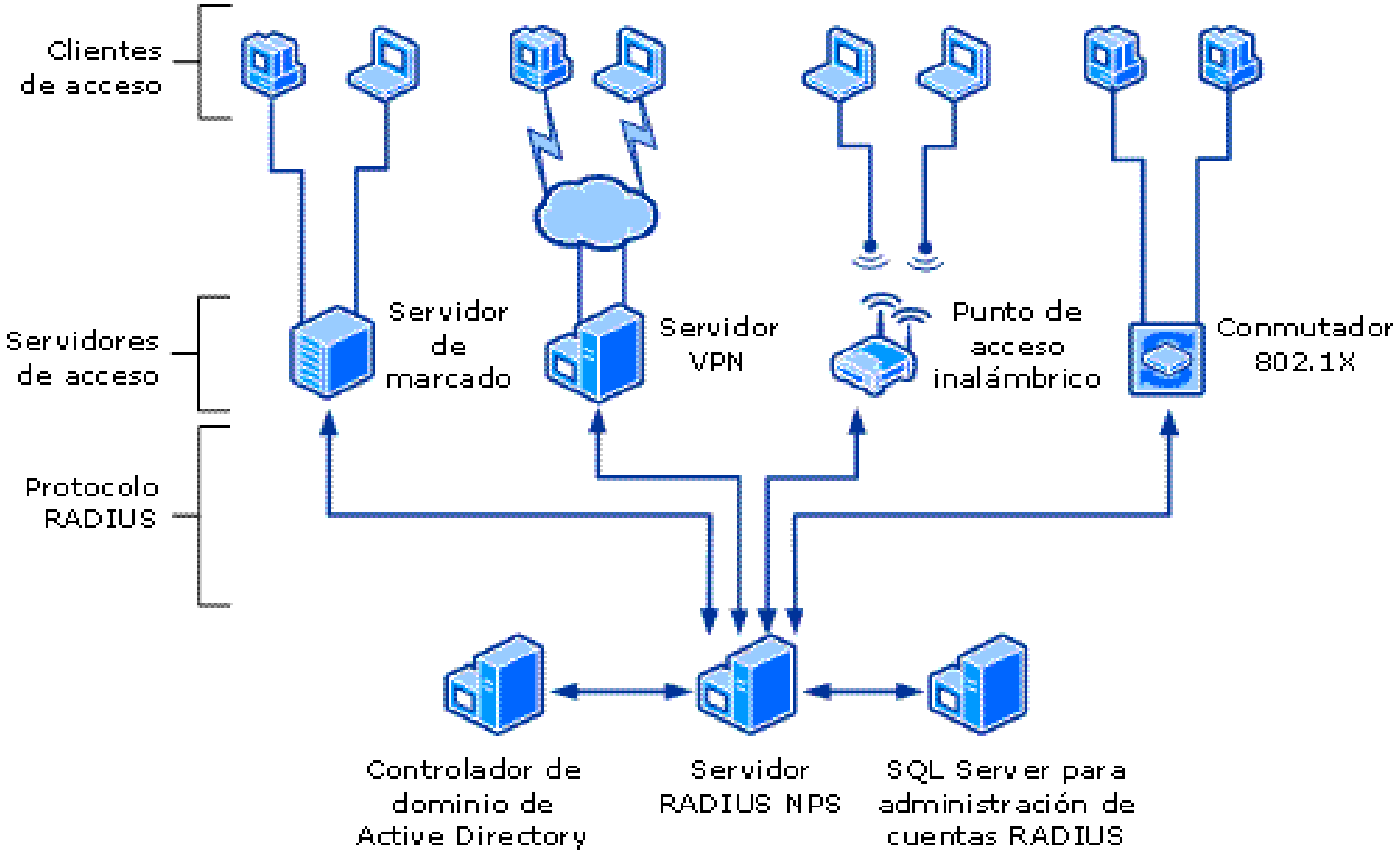
Fuente: Cisco

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

RADIUS

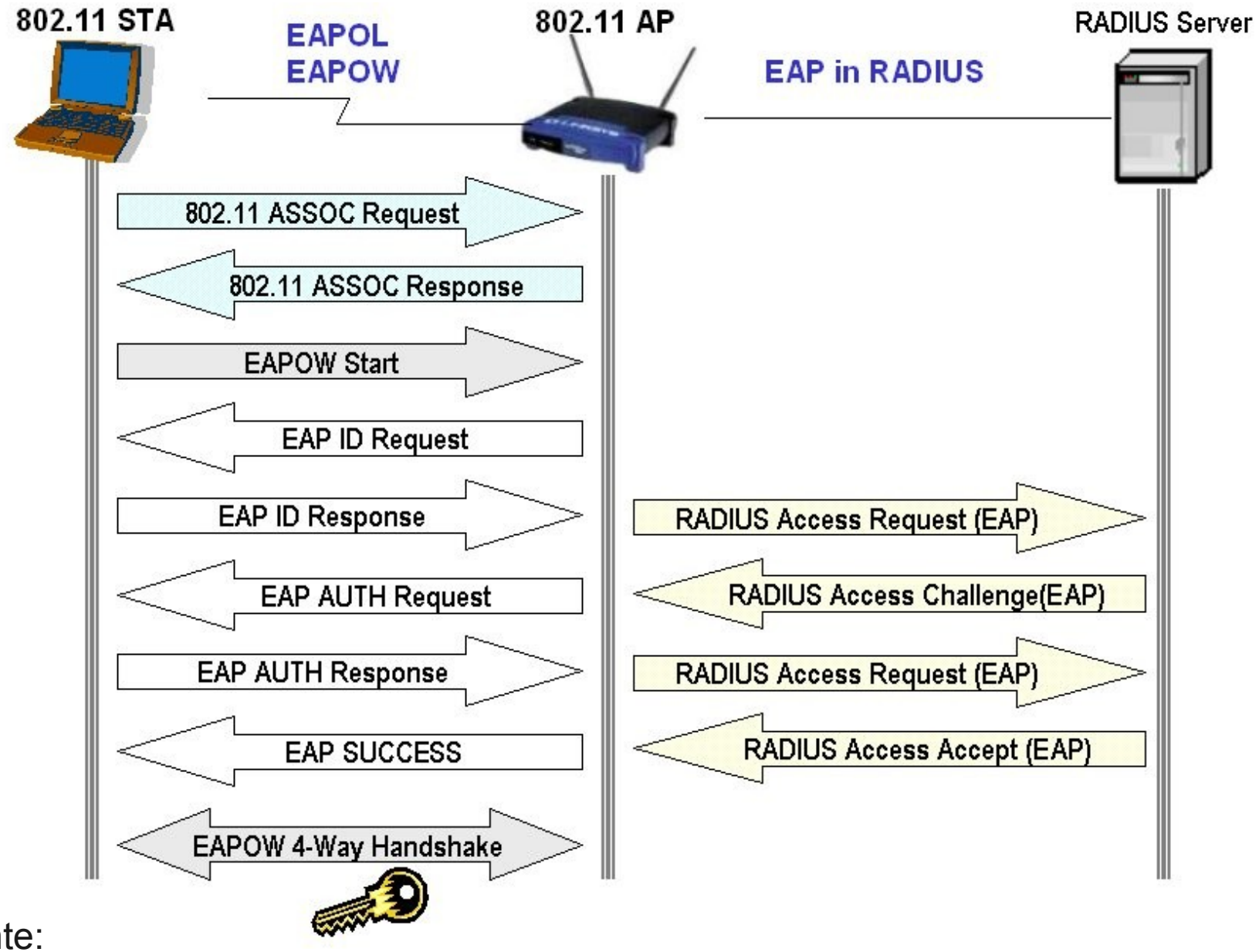
- Utiliza UDP
  - Autenticación: Puerto 1812
  - Administración de cuentas: Puerto 1813
- 6 tipos de mensajes:
  - Acceso
  - Rechazo/Aceptación Acceso
  - Desafío de Acceso
  - Administración de cuenta / respuesta de administración de cuenta.

RADIUS



Fuente: http://technet.microsoft.com/es-es/library/cc755248%28WS.10%29.aspx

RADIUS



Fuente:
http://astrophysics.gsfc.nasa.gov/eudcomp/wireless/wireless_intro.html

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

KERBEROS

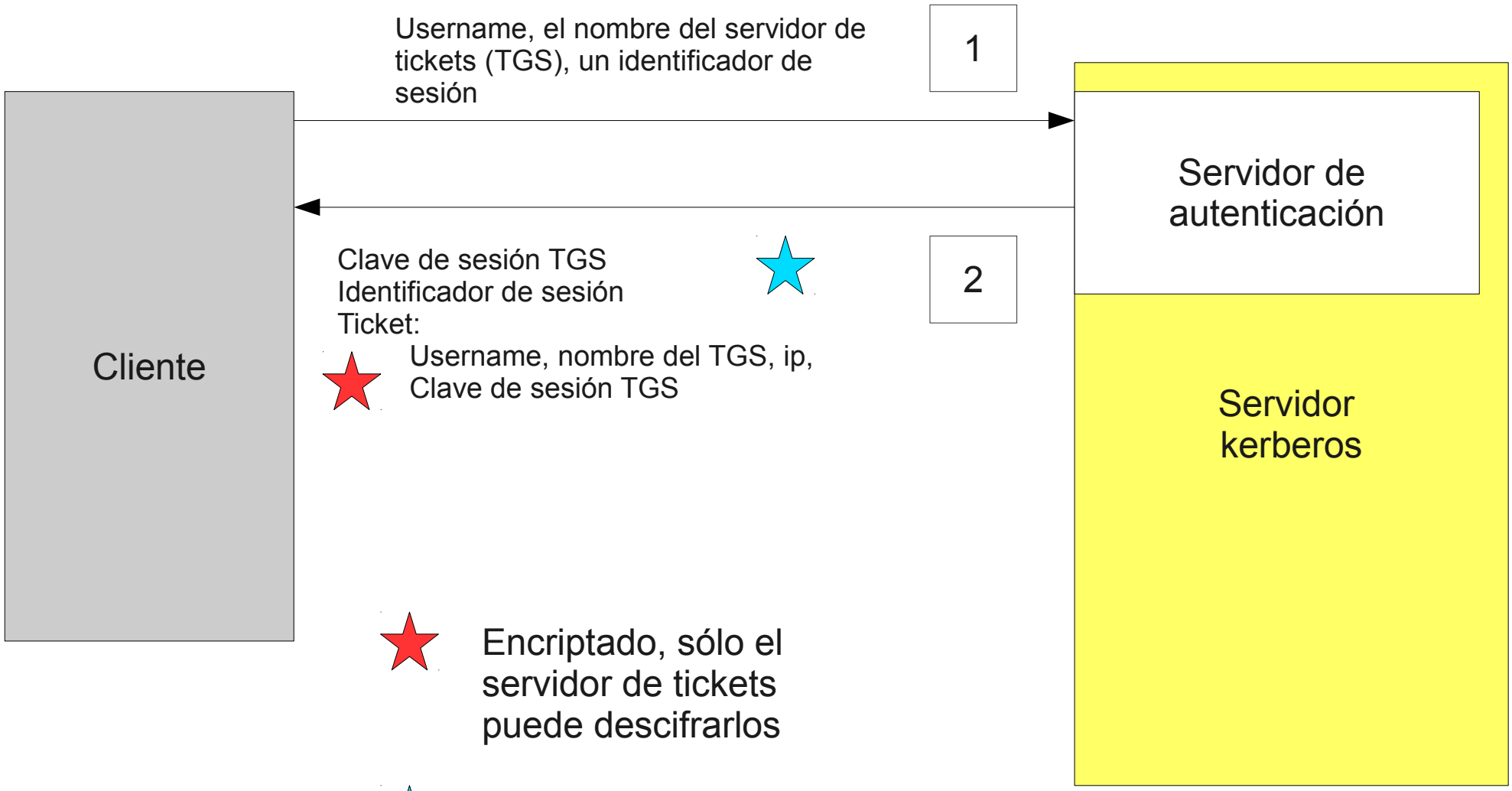
- Creado por el instituto Tecnológico de Massachusetts (MIT)
- Autentifica a el cliente y al servidor
- RFC 4120
- Características:
  - Cifrado AES (RFC 3962)
  - API de servicios de seguridad genérico (RFC 4121)

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

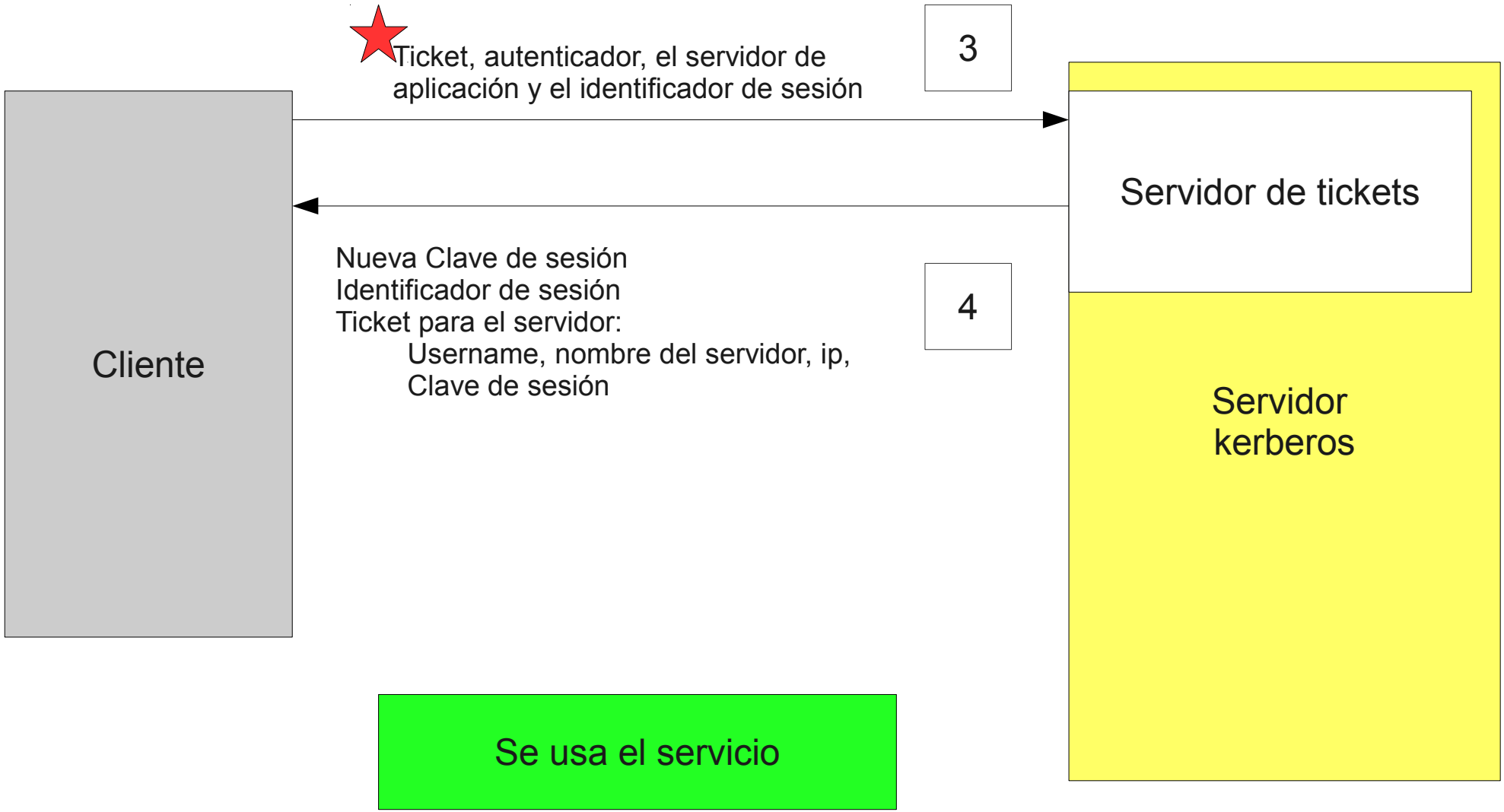
KERBEROS

- Servidor y usuario/servicio dispone de una clave
- Base de datos unificada
- Se requiere de un registro previo donde se negocian las claves.
  - Kerberos tiene las claves del cliente y del servidor
  - Nunca viajan por la red.
- En principio el usuario/servicio confían en el servidor kerberos
  - Se establecen tickets por sesión

Kerberos


Username, el nombre del servidor de tickets (TGS), un identificador de sesión
1
Cliente
Servidor de autenticación
Clave de sesión TGS
Identificador de sesión
Ticket:
Username, nombre del TGS, ip,
Clave de sesión TGS
2
Servidor kerberos
Encriptado, sólo el servidor de tickets puede descifrarlos
Encriptado con la contraseña Del cliente.

Kerberos


Ticket, autenticador, el servidor de aplicación y el identificador de sesión
3
Servidor de tickets
Nueva Clave de sesión
Identificador de sesión
Ticket para el servidor:
Username, nombre del servidor, ip,
Clave de sesión
4
Cliente
Servidor kerberos
Se usa el servicio

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

GSSAPI

- Kerberos v5 usa una interfaz genérica de servicios de seguridad
- Se está convirtiendo en un estándar de facto
  - Implementaciones de RADIUS y SSH tambíen lo usan.
- *Generic Security Services Application Program Interface*. (RFC 2743 y RFC 2744)

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

GSSAPI

- Entorno a 45 llamadas:
  - Para obtener credenciales
  - Generar/contestar retos
  - Encriptar/desencriptar datos de usuario/aplicación
  - Etc.
- Existen versiones para C y Java