

Seguridad de Sistemas

Clase 10: Cracking a la Autenticación

Introducción

ATRIBUTO

CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

NO REPUDIO

AUTENTICACION



CONTROL

CIFRADO

FUNCION HASH

HA, RESPALDO

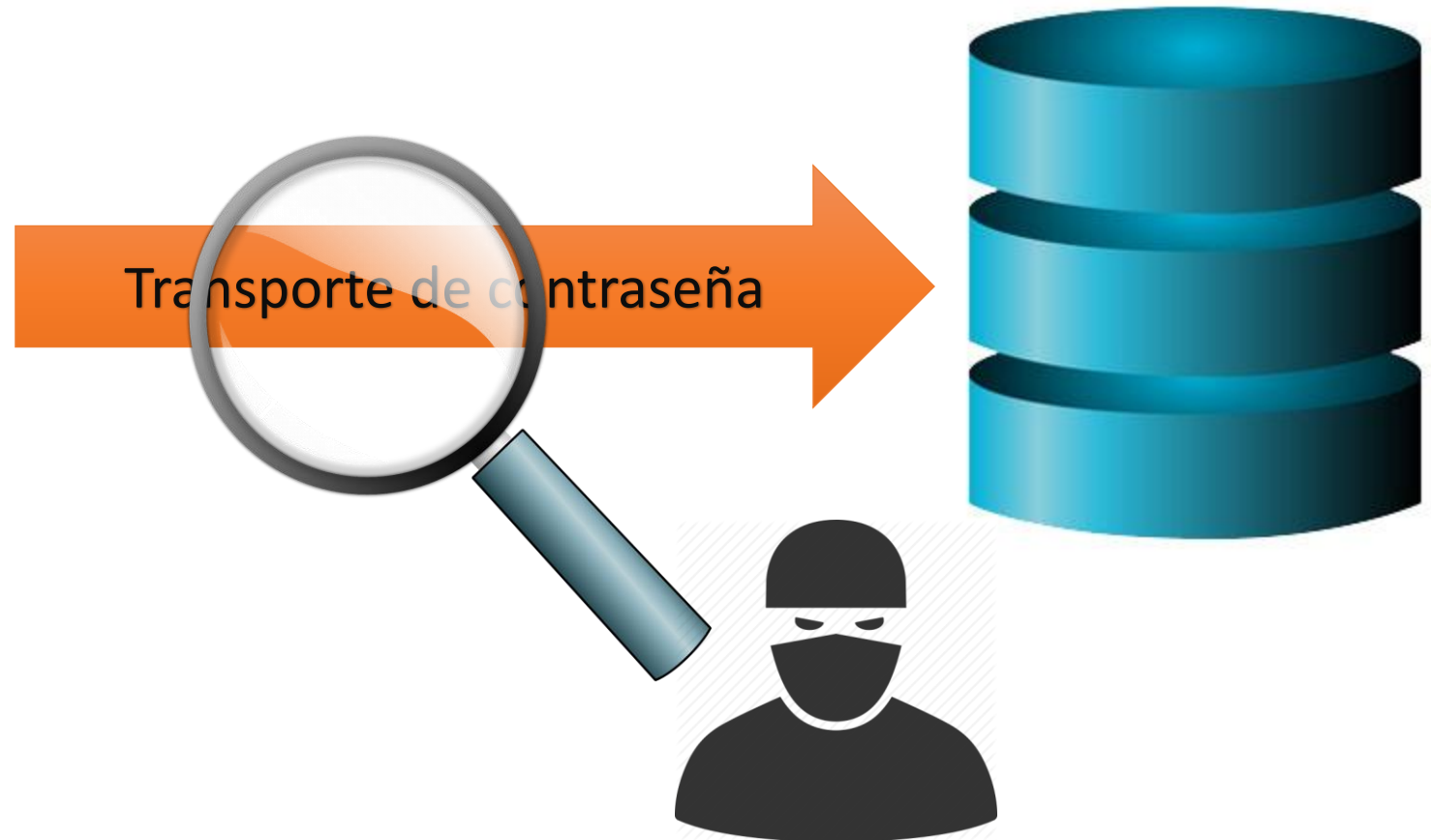
FIRMA DIGITAL

FUNCION HASH *

Introducción

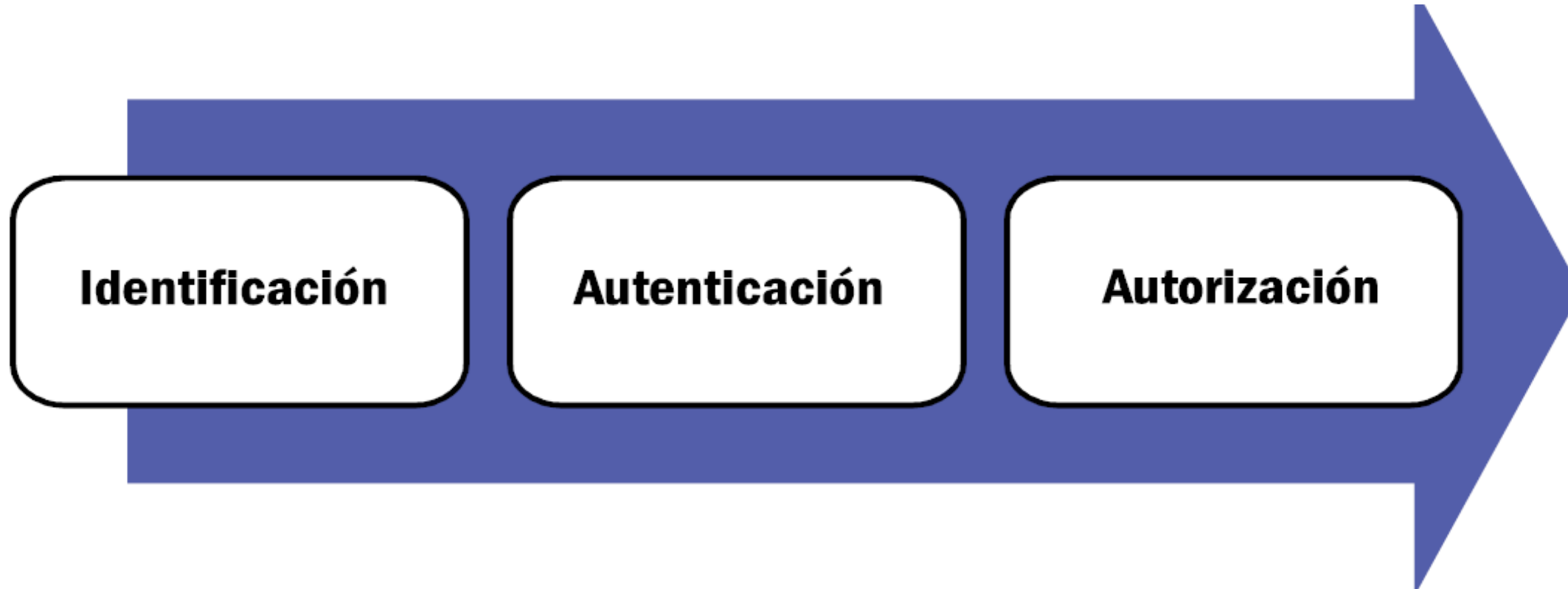
- ¿Qué es el control de acceso?
- Cuando hablamos de control de acceso nos referimos a la capacidad de permitir acceso a un sistema o recursos solamente a entidades autorizadas (usuarios, programas y procesos), buscando proteger datos y sistemas. En la implementación de un sistema de control de accesos hay distintas fases, que podemos resumir en establecimiento, mantenimiento, revocación y auditoría.

Introducción



Introducción

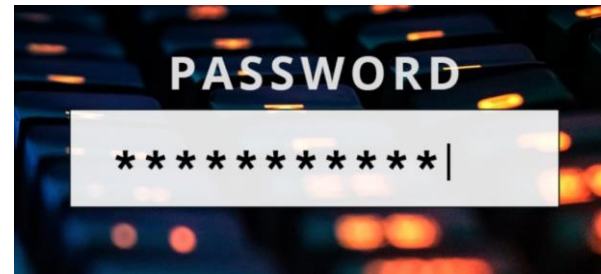
- Proceso de autenticación



Introducción

- Factores de autenticación

- Algo que uno sabe



- Algo que uno tiene



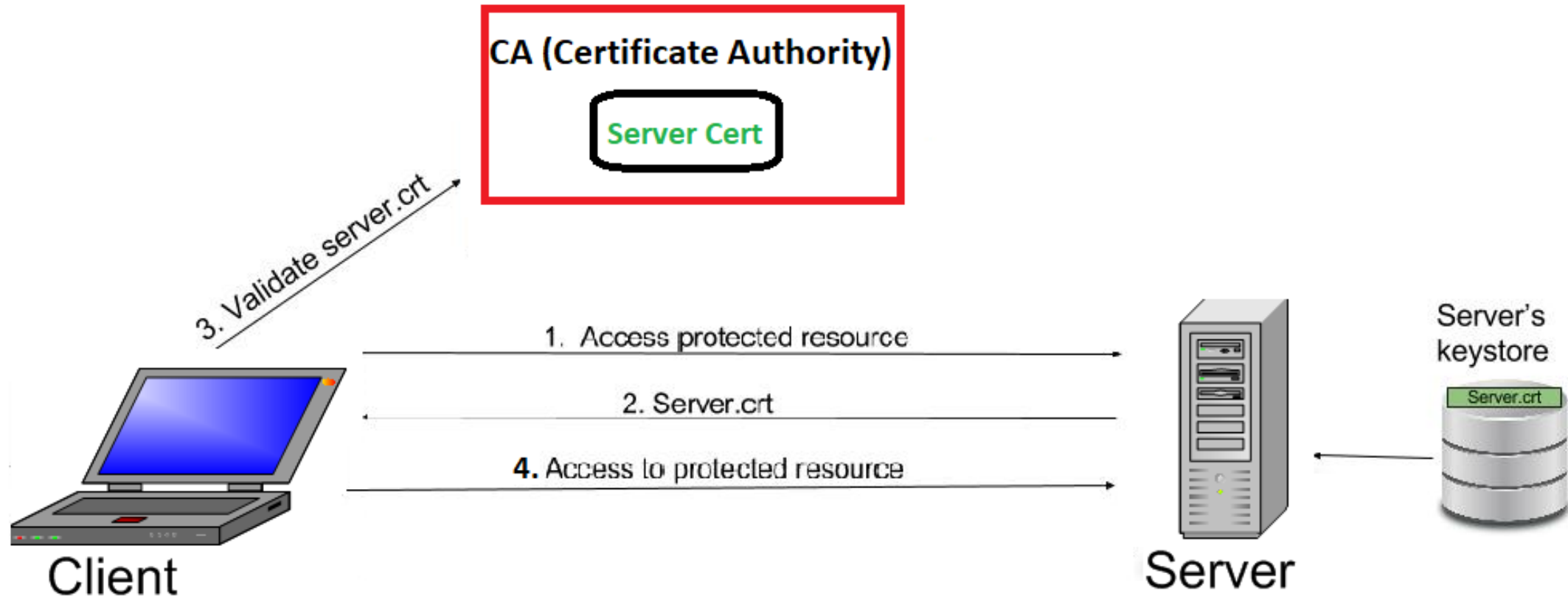
- Algo que uno es



Tipos de autenticación

- **One-way authentication**
- En esta modalidad de autenticación, sólo el cliente valida al servidor para asegurarse de que recibe datos del servidor previsto o viceversa. Esta es la forma más simple de autenticación y se utiliza cuando sólo es necesario validar a uno de los integrantes de la comunicación.
- Este modelo es susceptible a ataques de suplantación dado que es posible que uno de los dos integrantes, cliente o servidor no se valide adecuadamente.
- Ejemplo: autenticación en portales web

Introducción



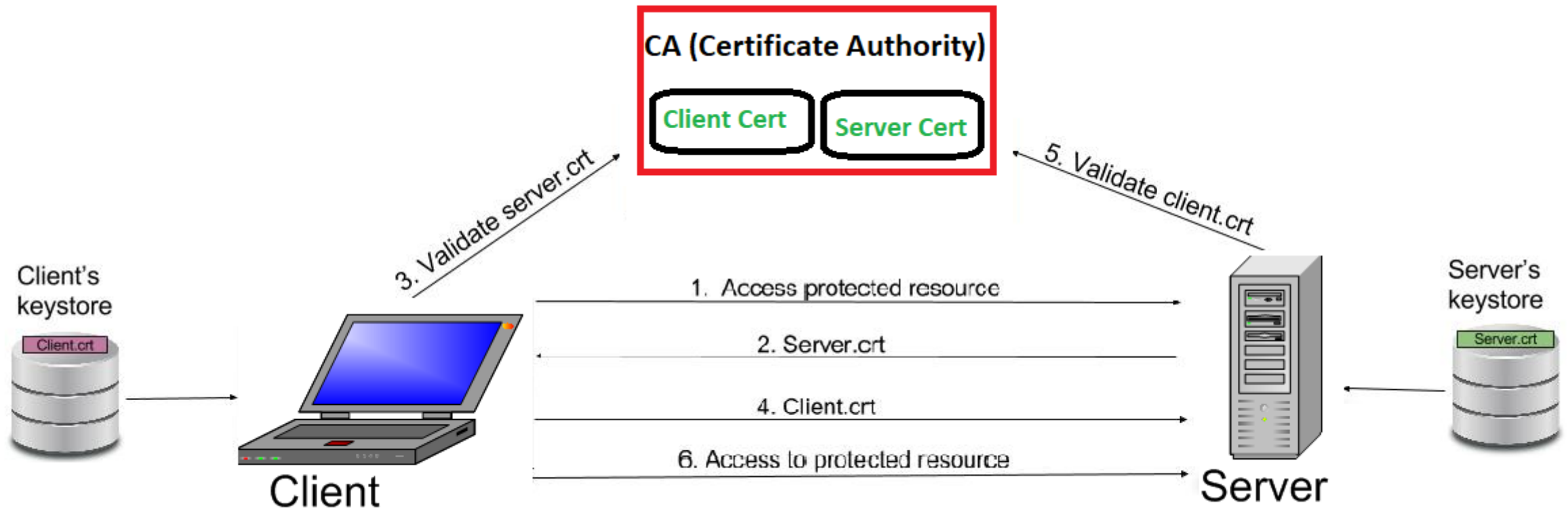
Esquema de one-way authentication

Tipos de autenticación

- **Mutual Authentication**

- La autenticación mutua, también llamada autenticación bidireccional, es un proceso o tecnología en el que ambas entidades en un enlace de comunicaciones se autentican entre sí. En un entorno de red, el cliente autentica el servidor y viceversa. De esta manera, los usuarios de la red pueden estar seguros de que están haciendo negocios exclusivamente con entidades y servidores legítimos, y pueden estar seguros de que todos los posibles usuarios están intentando obtener acceso con fines legítimos. La autenticación mutua está ganando aceptación como una herramienta que puede minimizar el riesgo de fraude en línea en el comercio electrónico.

Introducción

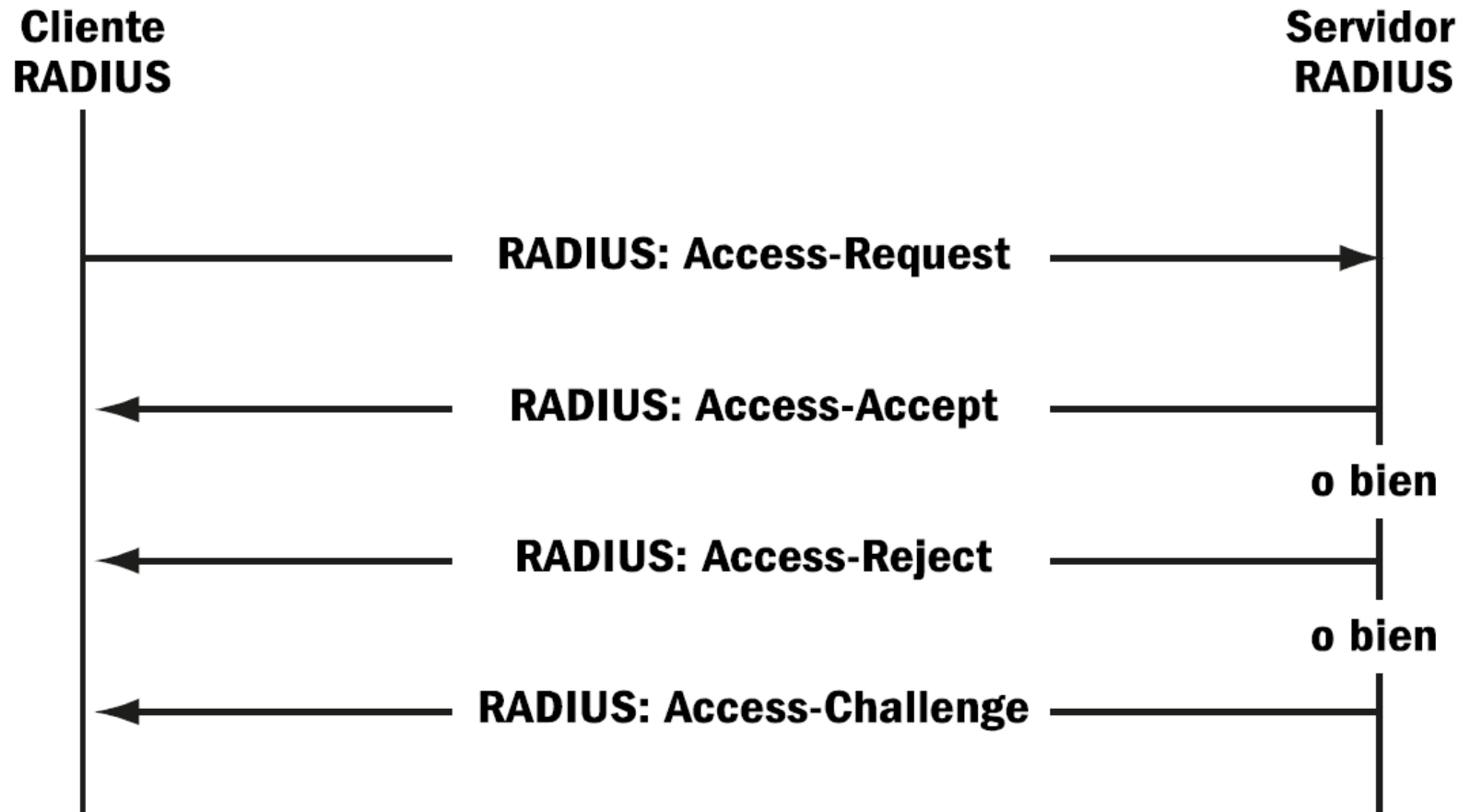


Esquema de mutual authentication

Sistemas AAA

- **RADIUS (Remote Authentication Dial-In User Service)**
- Protocolo de autenticación y autorización que trabaja sobre el puerto UDP 1812, estandarizado en 1991 por Living Enterprises y se rige por el RFC 2866.
- Se utiliza principalmente en conexiones de Internet mediante módem, DSL, cablemódem, Ethernet o Wi-Fi.
- Utiliza los esquemas de autenticación como PAP, CHAP o EAP.
- Puede entregar configuración de red al cliente aceptado, tales como conexiones L2TP o dirección IP.

Sistemas AAA

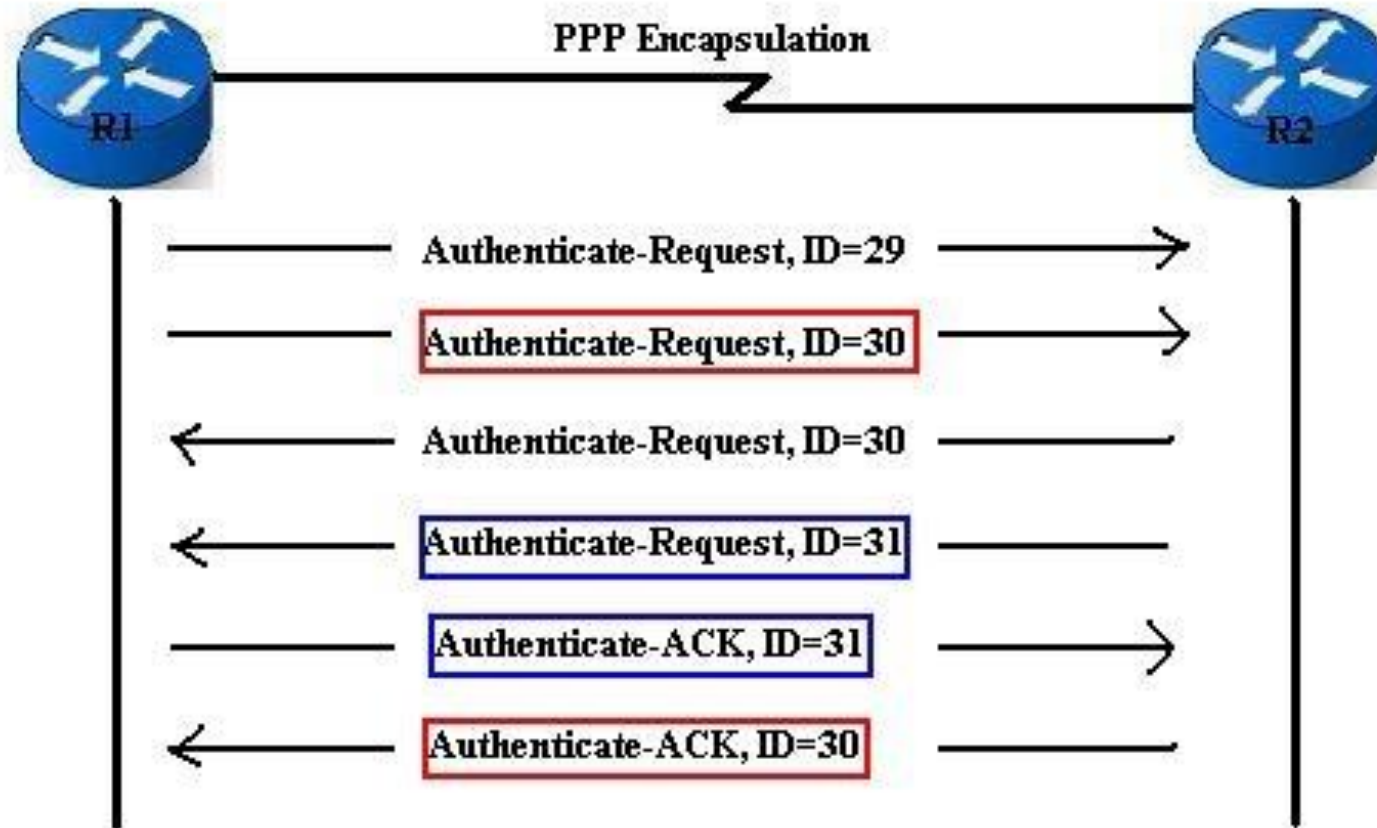


Esquema de operación del protocolo RADUS

Servidores AAA

- **Protocolos de RADIUS**
- PAP (Password Authentication Protocol)
- Es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. PAP es un subprotocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o passwords en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

Servidores AAA

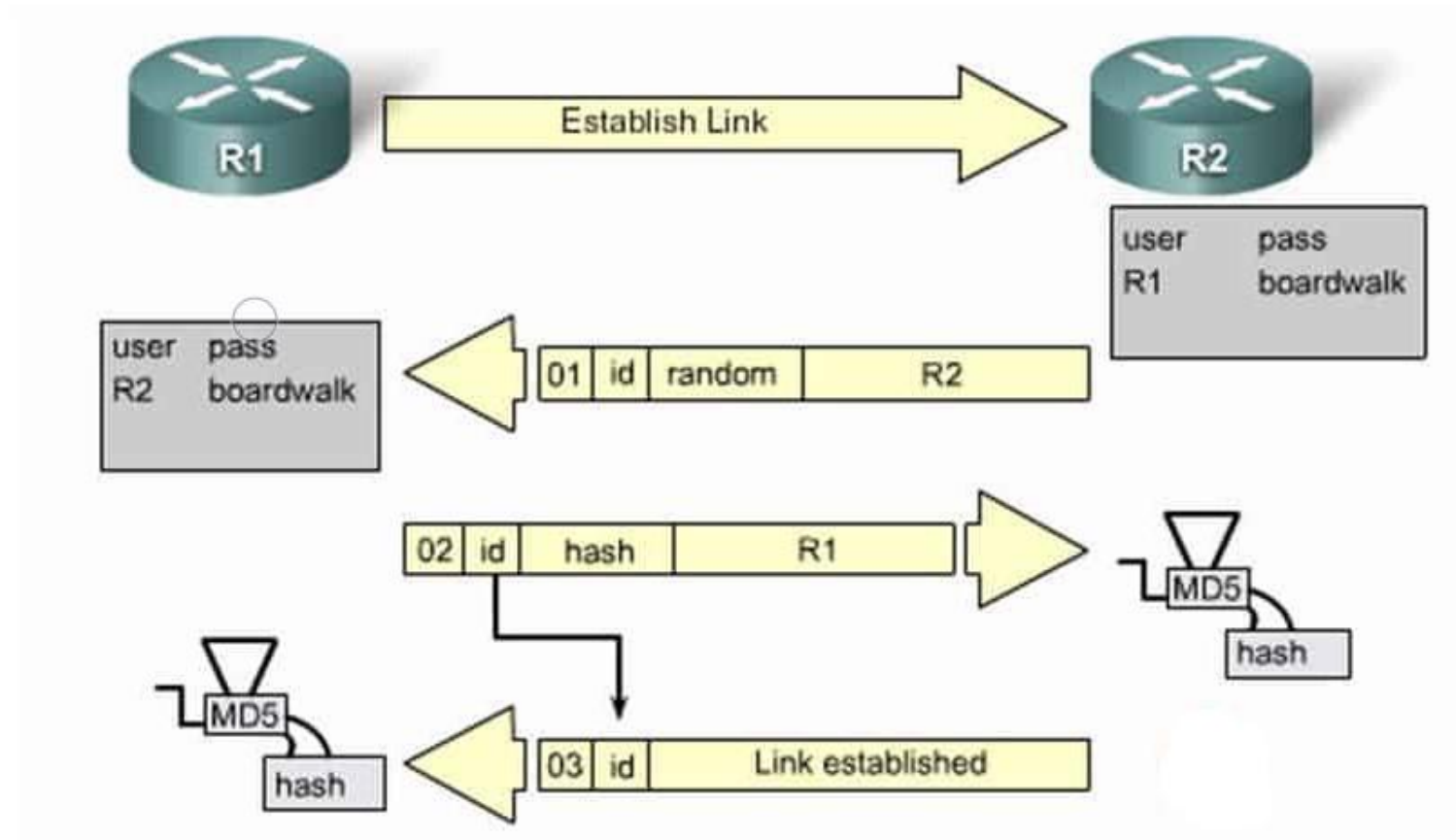


Esquema de operación de PAP

Servidores AAA

- **Protocolo RADIUS**
- CHAP (Challenge Handshake Authentication Protocol)
- Es un método de autenticación usado por servidores accesibles vía PPP. A través de él se verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación.
- La verificación se basa en una contraseña compartida.

Servidores AAA

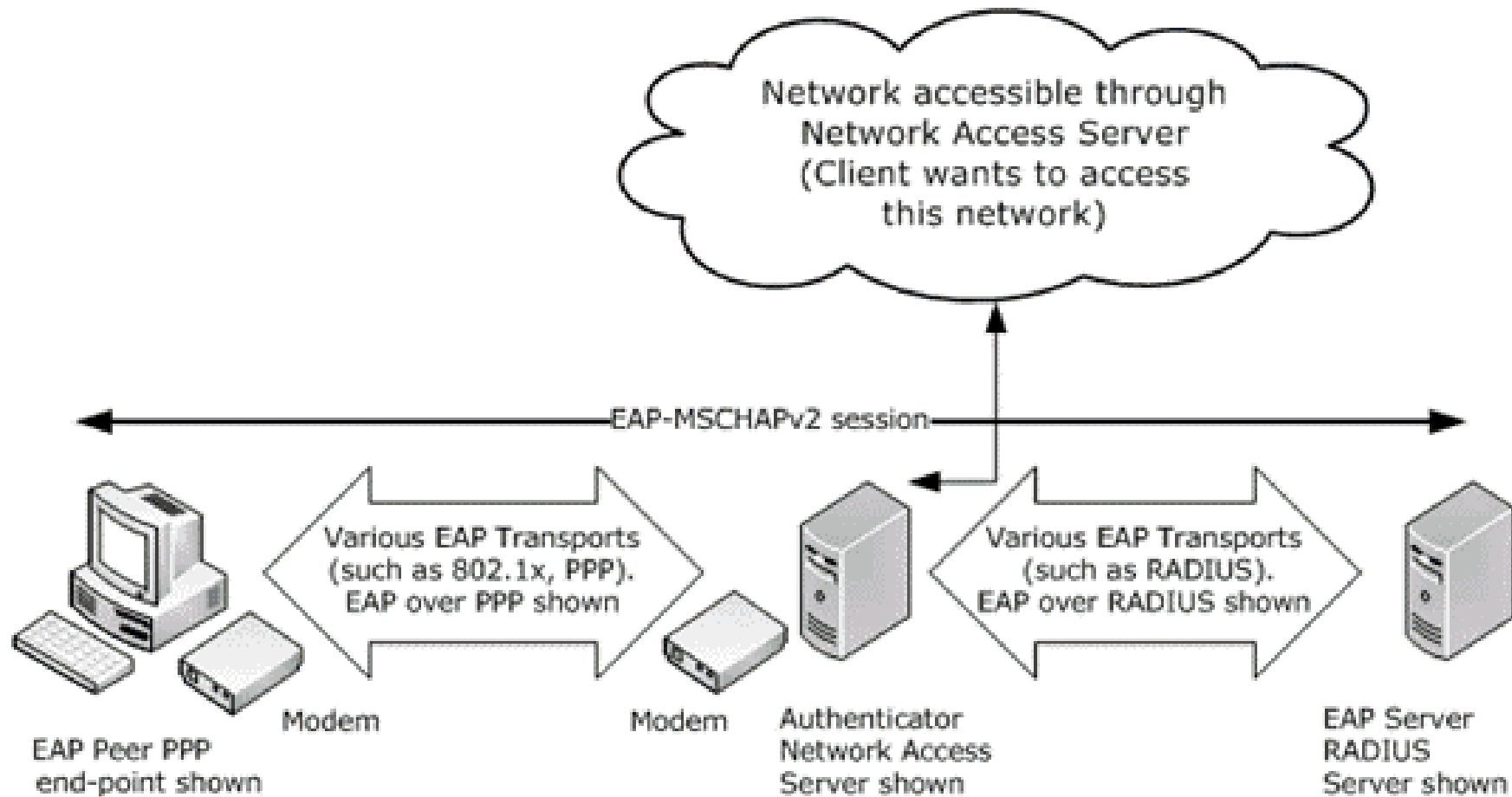


Esquema de operación de CHAP

Servidores AAA

- **MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)**
- Es la versión de Microsoft del protocolo de autenticación de contraseñas de cifrado por desafío mutuo, el cual es irreversible. Se encuentra actualmente en la versión MS-CHAPv2, definida en el RFC 2759.
- Sus principales ventajas son:
 - proporciona un mecanismo de cambio de contraseña controlado por autenticador
 - proporciona un mecanismo de reintento de autenticación controlado por autenticador
 - define los códigos de falla devueltos en el campo de mensaje de paquete de falla

Servidores AAA

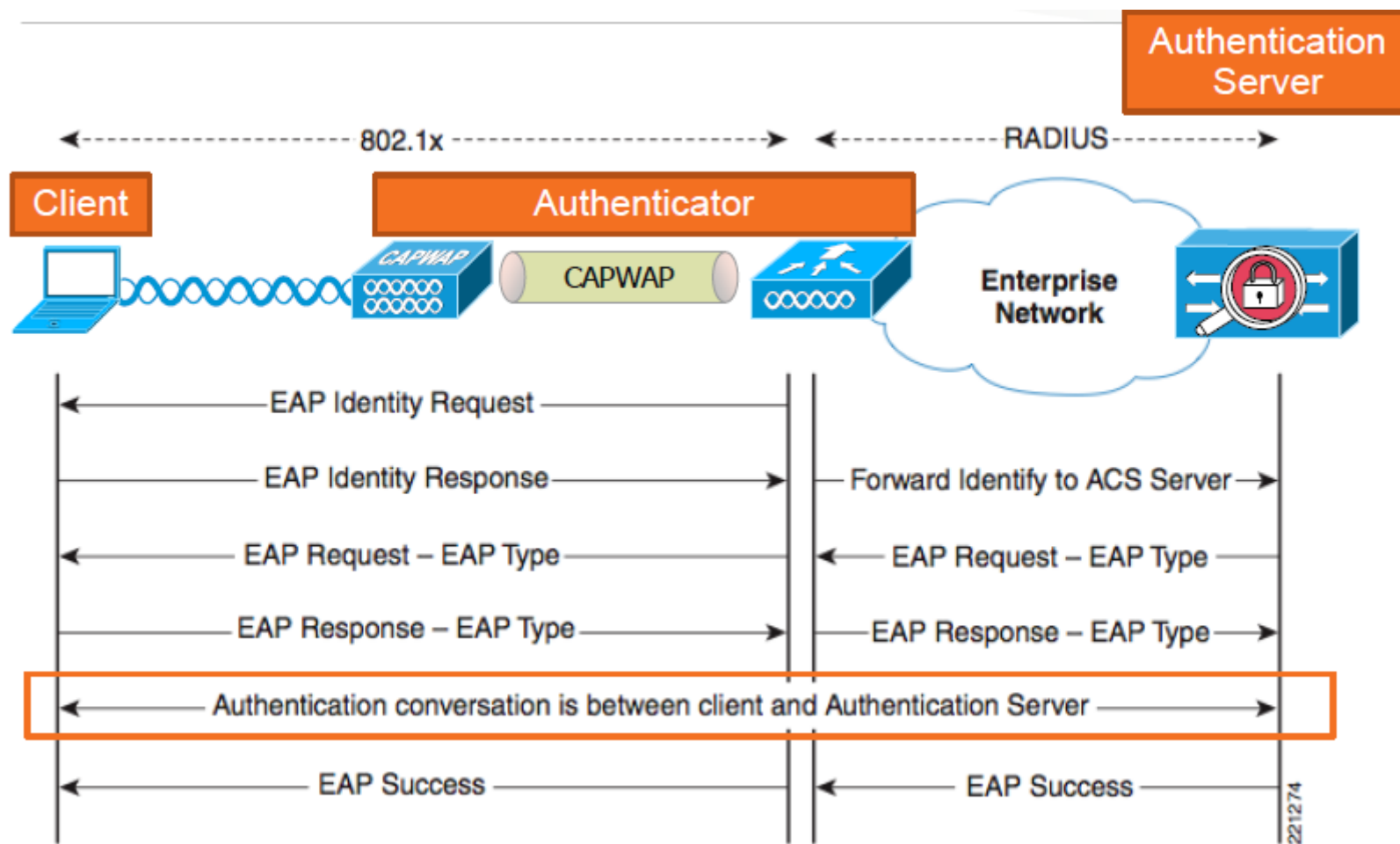


Autenticación usando MS-CHAP

Servidores AAA

- **Protocolo RADIUS**
- EAP (Extensible Authentication Protocol)
- Corresponde a un framework de autenticación usado habitualmente en redes WLAN y LAN. Actualmente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.
- EAP fue diseñado para utilizarse en la autenticación para acceso a la red, donde la conectividad de la capa IP puede no encontrarse disponible. Dado que EAP no requiere conectividad IP, solamente provee el suficiente soporte para el transporte confiable de protocolos de autenticación.

Servidores AAA



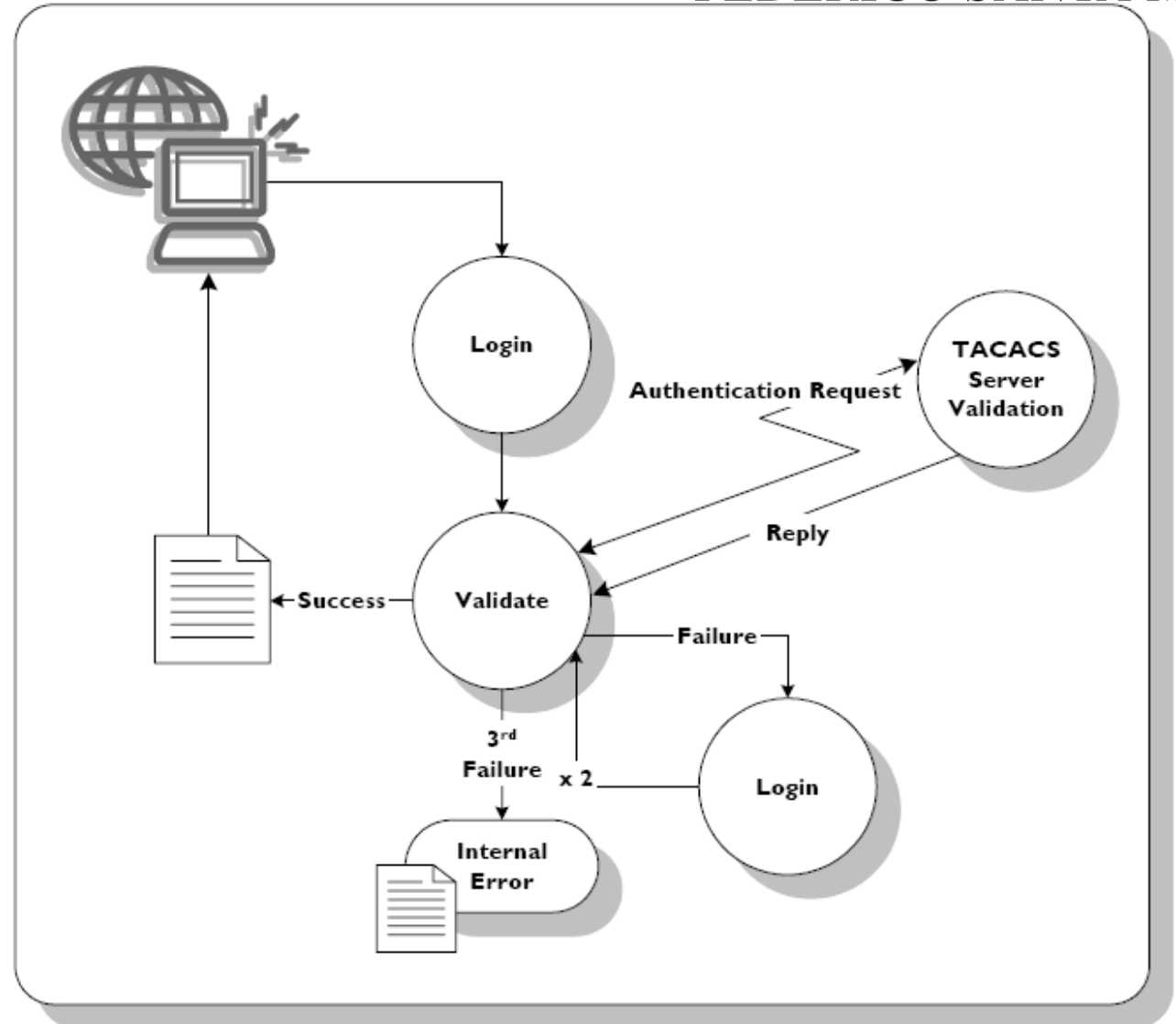
Esquema de operación de EAP

Servidores AAA

- **TACACS (Terminal Access Controller Access Control System)**
- Es un sistema de AAA creado en 1984 para los viejos servidores UNIX. TACACS permite a un servidor de acceso remoto (RAS) comunicarse con un servidor de autenticación para determinar si un usuario debe tener o no acceso a la red, administrando las contraseñas de forma centralizada en una base de datos.
- Esta definido en el RFC 1492y utiliza el puerto TCP 49.
- Cisco creo una versión propietaria llamada TACACS+ que incluye autenticación de doble factor.

Servidores AAA

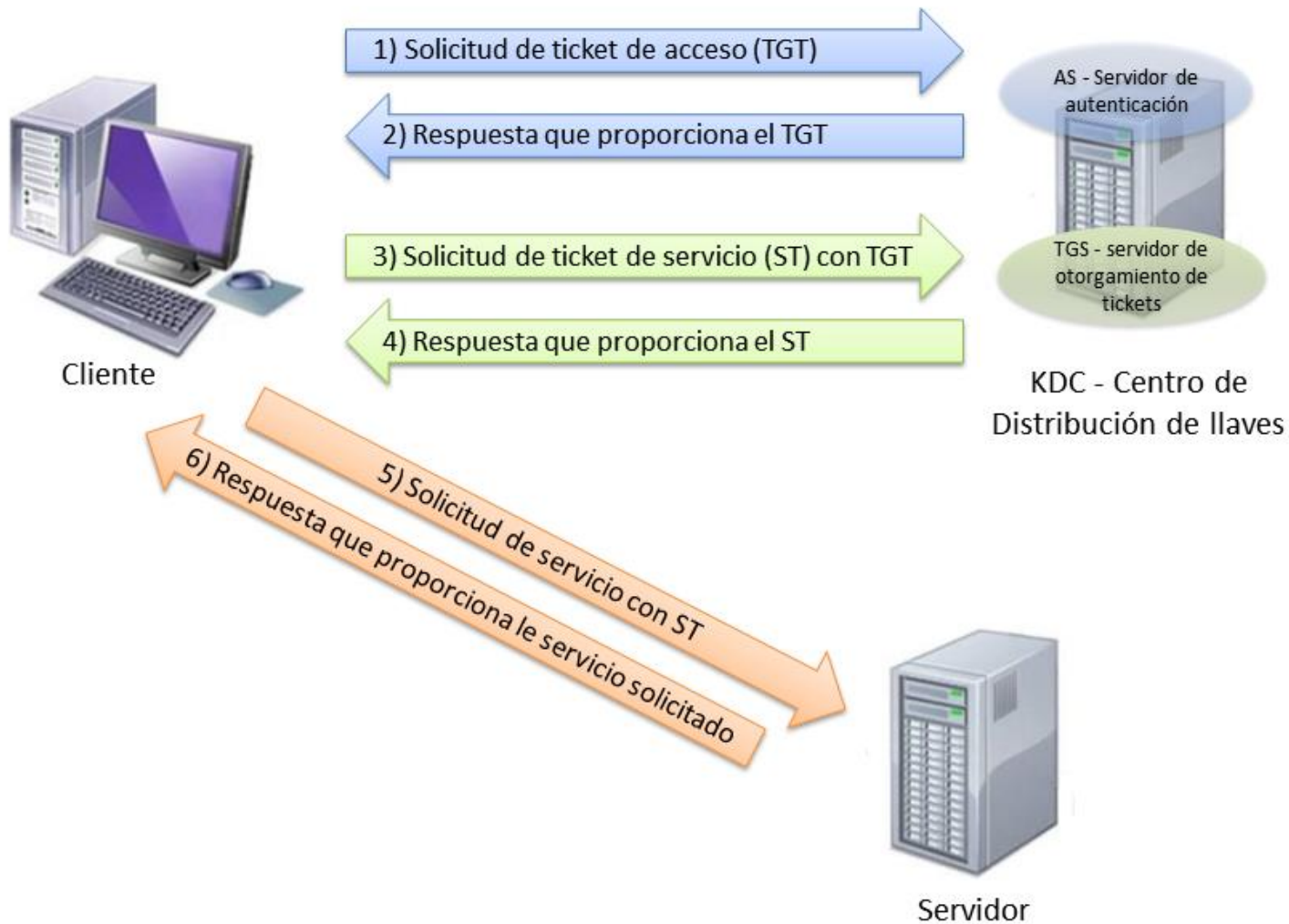
Esquema de autenticación utilizando TACACS



Servidores AAA

- **Kerberos**
- Es un estándar y un protocolo de autenticación para redes, cuya última versión es de junio de 2013. Posibilita la comunicación entre partes sobre un canal inseguro permitiendo que cada una demuestre su identidad a la otra.
- Utiliza un modelo cliente-servidor donde ambos verifican la identidad del otro, posibilitando la autenticación del inicio de la conexión y los mensajes individuales. El modelo está basado en la criptografía simétrica

Servidores AAA



**Autenticación usando
Kerberos**

Protocolos de autenticación MS

- **LM (LAN Manager)**
- Desarrollado por Microsoft en los año 80 para las primeras versiones de Windows NT.
- En 1990 se lanza la versión LMv2, bajo soporte TCP/IP, dado que la anterior sólo funcionaba sobre NetBIOS.
- Hoy en día esta función esta obsoleta por sus múltiples fallas de seguridad.

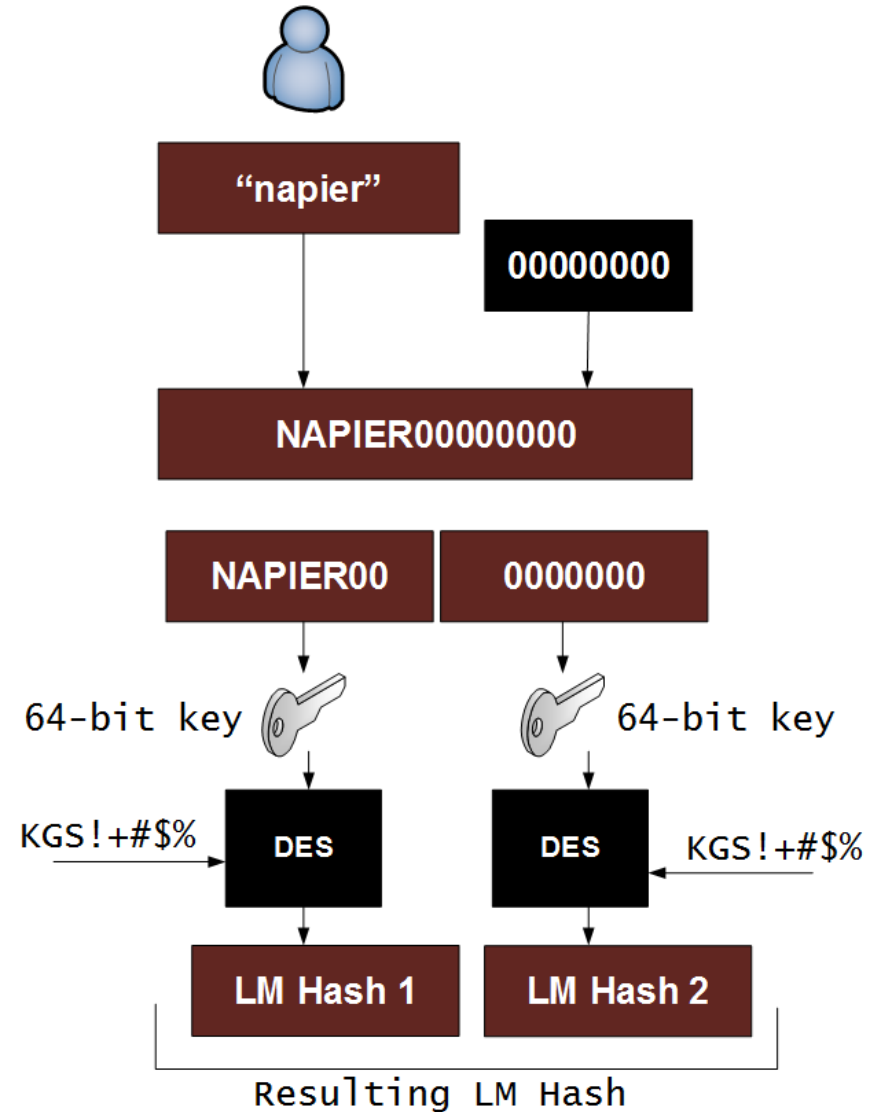
Protocolos de autenticación MS

- **Principales características de LAN Manager**

- La contraseña del usuario está restringida a un máximo de catorce caracteres
- La contraseña del usuario se convierte a mayúsculas.
- Esta contraseña está rellena con caracteres nulos a 14 bytes.
- La contraseña de "longitud fija" se divide en dos mitades de 7 bytes.
- Cada una de las dos claves se utiliza para encriptar DES la cadena ASCII constante "KGS! @ # \$%", que da como resultado dos cadenas de 8 bytes cada una.
- Estos dos valores de texto cifrado se concatenan para formar un valor de 16 bytes, que es el hash LM

Protocolos de autenticación MS

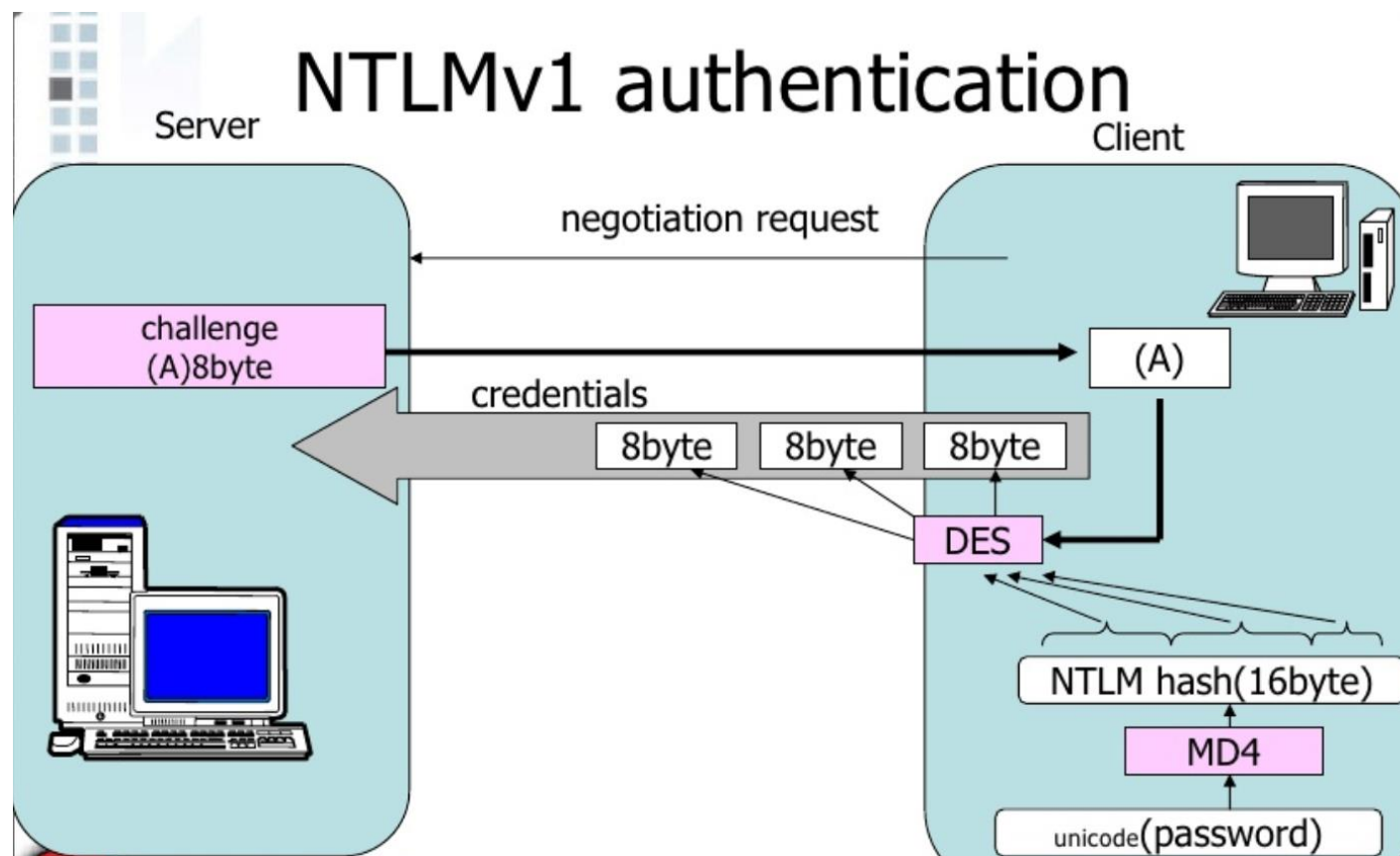
Fórmula de calculo de HASH LM en Sistemas Microsoft



Protocolos de autenticación MS

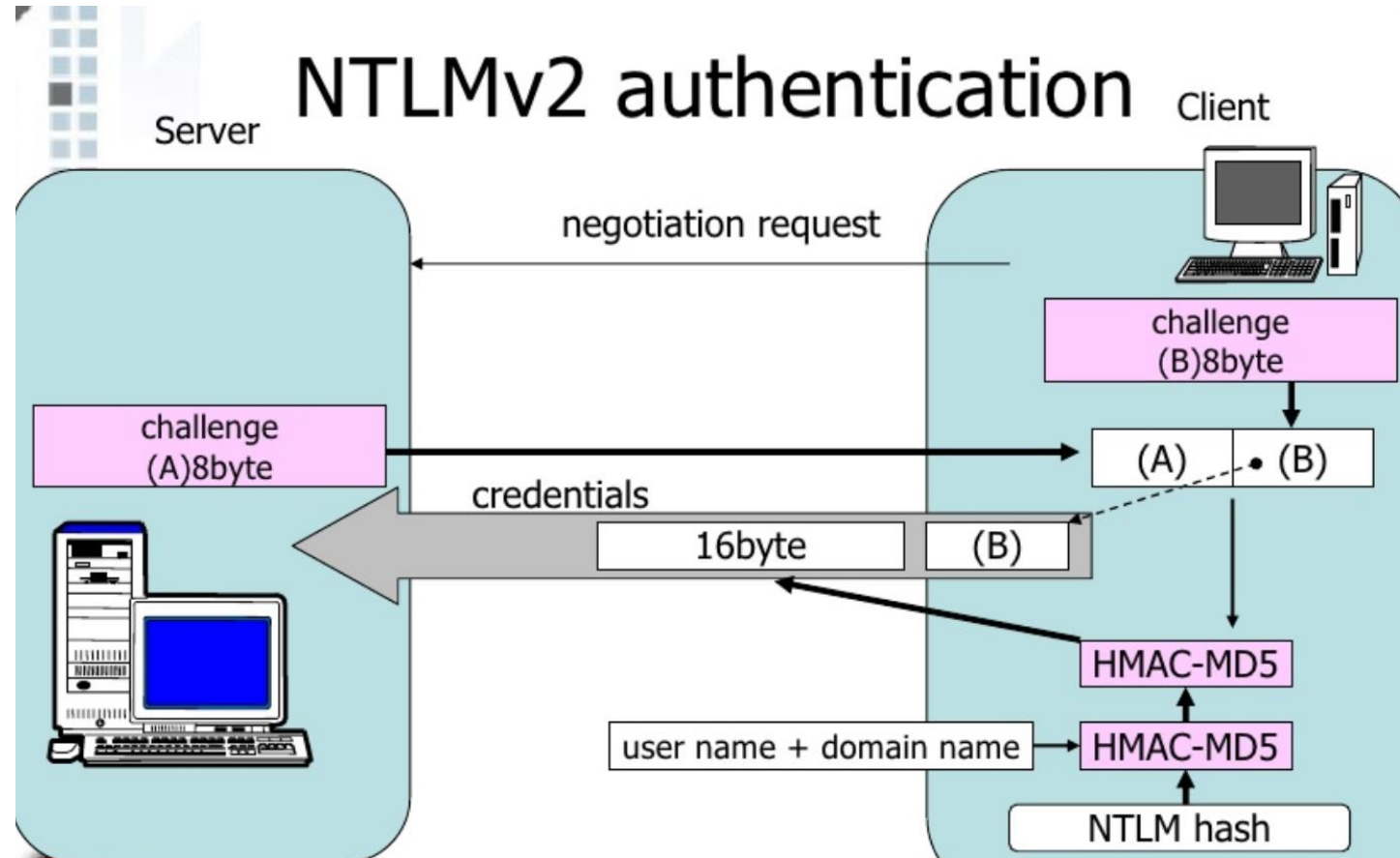
- **NTLM (New Technology LAN Manager)**
- Es el sucesor de LM, protocolo de autenticación de desafío-respuesta que utiliza tres mensajes para autenticar a un cliente en un entorno orientado a la conexión y un cuarto mensaje adicional si se desea integridad.
 - Primero, el cliente establece una ruta de red al servidor y envía un *NEGOTIATE_MESSAGE* anunciando sus capacidades.
 - Luego, el servidor responde con *CHALLENGE_MESSAGE* que se usa para establecer la identidad del cliente.
 - Finalmente, el cliente responde al desafío con un *AUTHENTICATE_MESSAGE*

Protocolos de autenticación MS



Esquema de operación de NTLMv1

Protocolos de autenticación MS



Esquema de operación de NTLMv2

Protocolos de autenticación MS

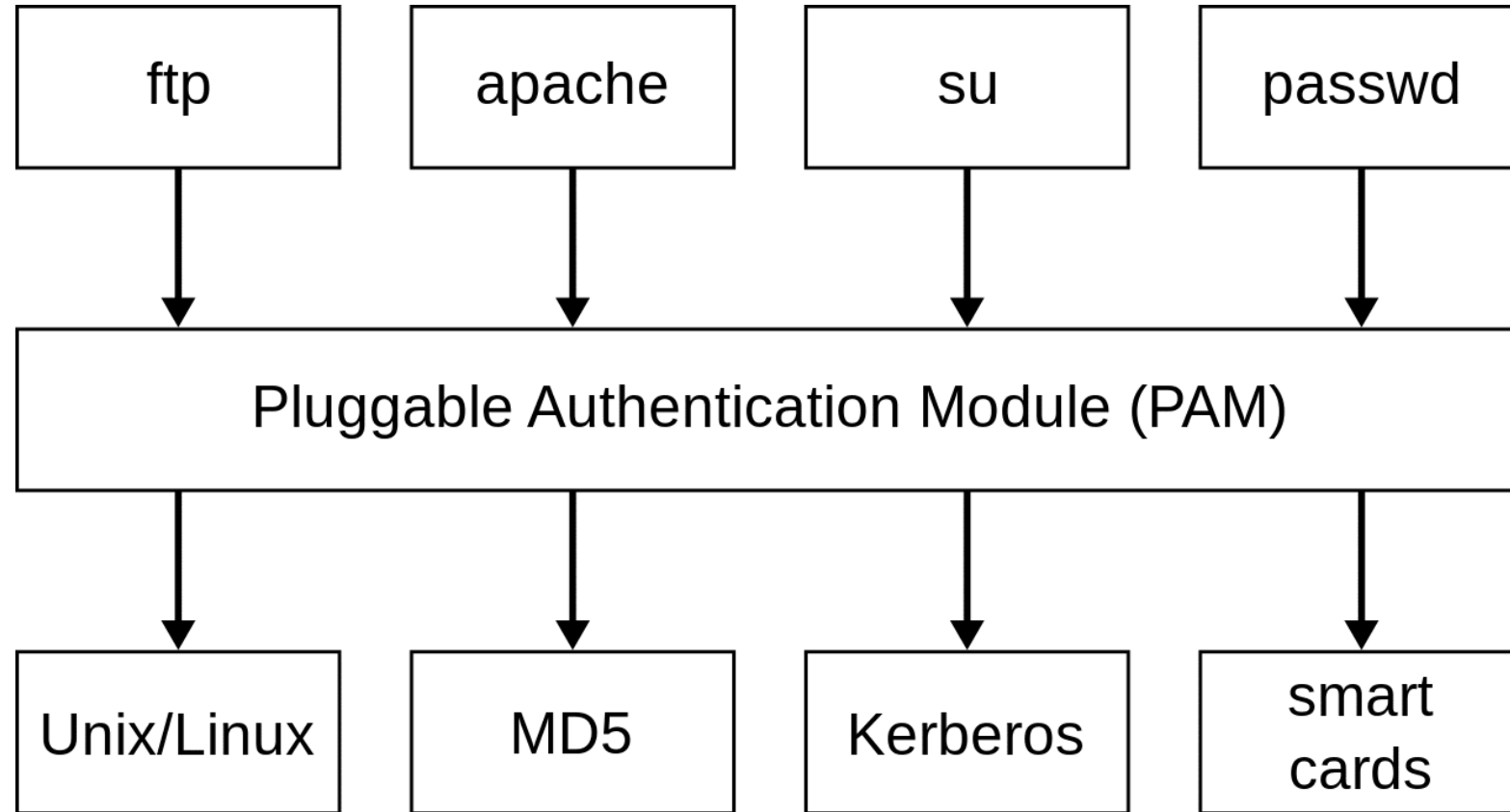
- Resumen

	LM	NTLMv1	NTLMv2	Kerberos
Password case sensitive	NO	YES	YES	YES
Client challenge	NO	NO	YES	YES
Password hash algorithm	DES (ECB mode)	MD4	MD5	MD4
Hash value length	64 + 64 bit	128 bit	128 bit	128 bit
C/R key lenght	56 + 56 + 16 bit	56 + 56 + 16 bit	128 bit	128 bit
C/R algorithm	DES (ECB mode)	DES (ECB mode)	HMAC-MD5	HMAC-MD5 & RC4
C/R value lenght	64 + 64 + 64 bit	64 + 64 + 64 bit	128 bit	36 byte

Protocolos de autenticación Linux

- **Autenticación en Linux**
- Existe un módulo llamado PAM (Pluggable Authentication Modules) el cual establece una interfaz entre los programas de usuario y distintos métodos de autenticación. De esta forma, el método de autenticación, se hace transparente para los programas. Contiene los siguientes submódulos:
 - Módulo de cuentas
 - Módulo de autenticación
 - Módulo de contraseñas
 - Módulo de sesión

Protocolos de autenticación Linux

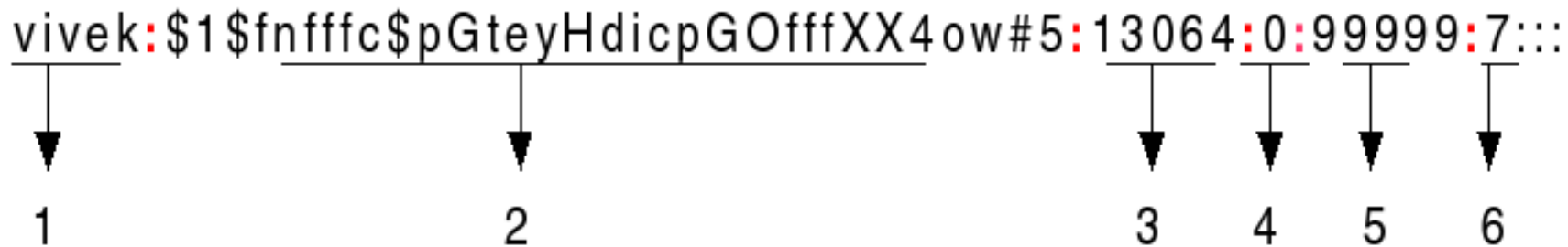


Esquema de autenticación en servidores Linux

Protocolos de autenticación Linux

- En los sistemas Linux, la contraseñas de usuarios del Sistema Operativo, se almacenan en el archivo `/etc/shadow`, el cual tiene la siguiente estructura:

vivek:\$1\$fnfffc\$pgteyHdicpGOfffXX4ow#5:13064:0:99999:7:::



1 2 3 4 5 6 7

Algoritmos de hash

- \$1\$ is MD5
- \$2a\$ is Blowfish
- \$2y\$ is Blowfish
- \$5\$ is SHA-256
- \$6\$ is SHA-512

Protocolos de autenticación Linux

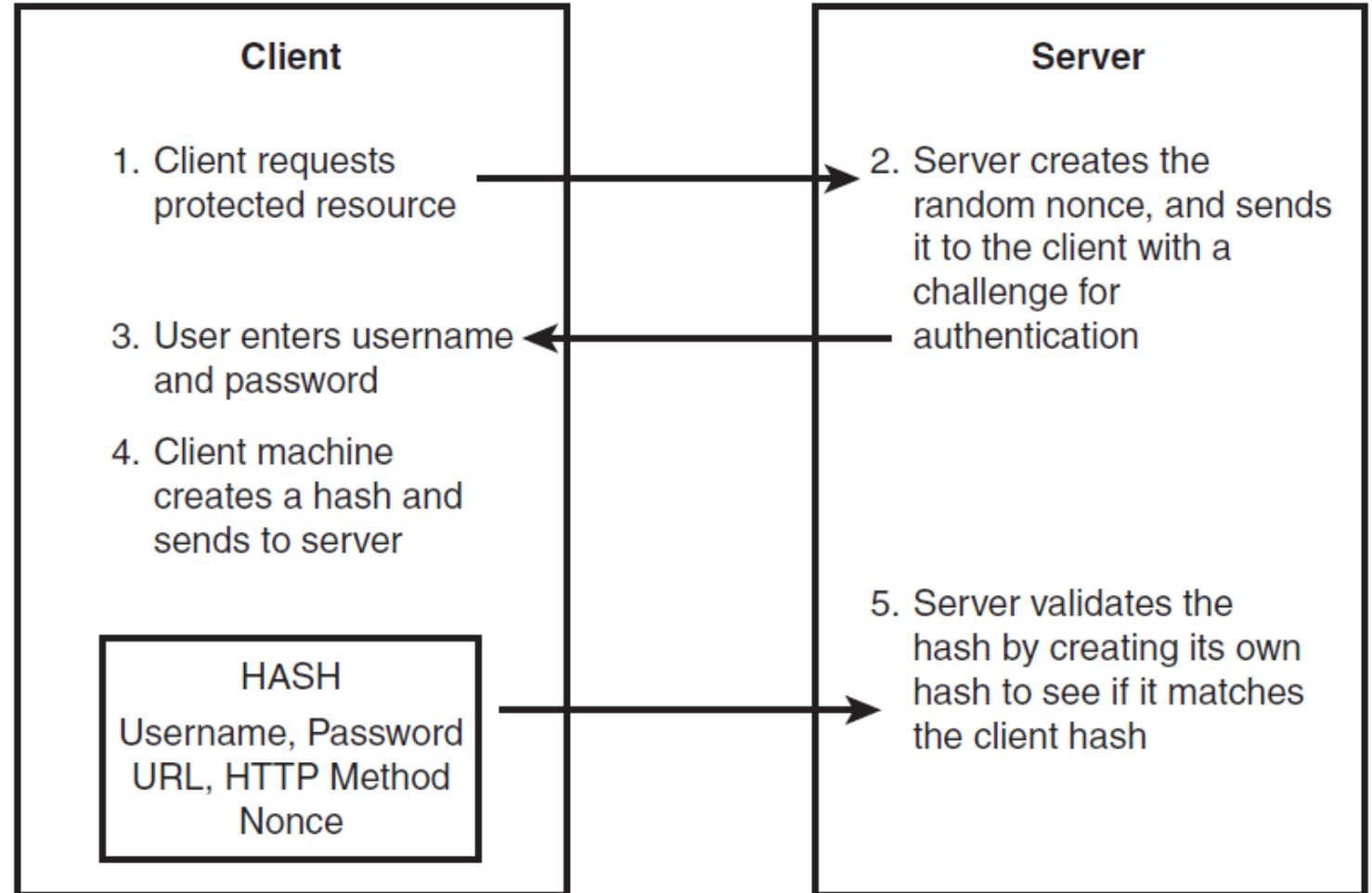
- Estructura del archivo /etc/shadow
- 1.- Username: id del usuario.
- 2.- Password: contraseña en formato HASH.
- 3.- Last password change (lastchanged): Días desde 1 enero de 1970 que la contraseña ha cambiado.
- 4.- Minimum: Días que deben transcurrir para el cambio de contraseña.
- 5.- Maximum: Días durante los cuales la contraseña es válida.
- 6.- Warn: Días a los que el usuario será avisado para cambiar la contraseña.
- 7.- Inactive: Días a los que se deshabilita la contraseña después que caduque.
- 8.- Expire: Días a los que se deshabilita la cuenta 1 enero de 1970.

Autenticación aplicaciones web

- Hoy en día existen diversas formas de implementar sistemas de autenticación en aplicaciones web.
- Una de las que utiliza criptografía es la llamada “Digest access authentication”, definida en el RFC 2069 que utiliza funciones HASH para el envío de las contraseñas y/o id de usuarios.
- Aplica una función hash al nombre de usuario y contraseña antes de enviarlos a través de la red.
- De esta forma se protegen los datos confidenciales dado que la contraseña en texto plano nunca viaja a través de la red.

Autenticación aplicaciones web

Operación de Digest Authentication en aplicaciones web

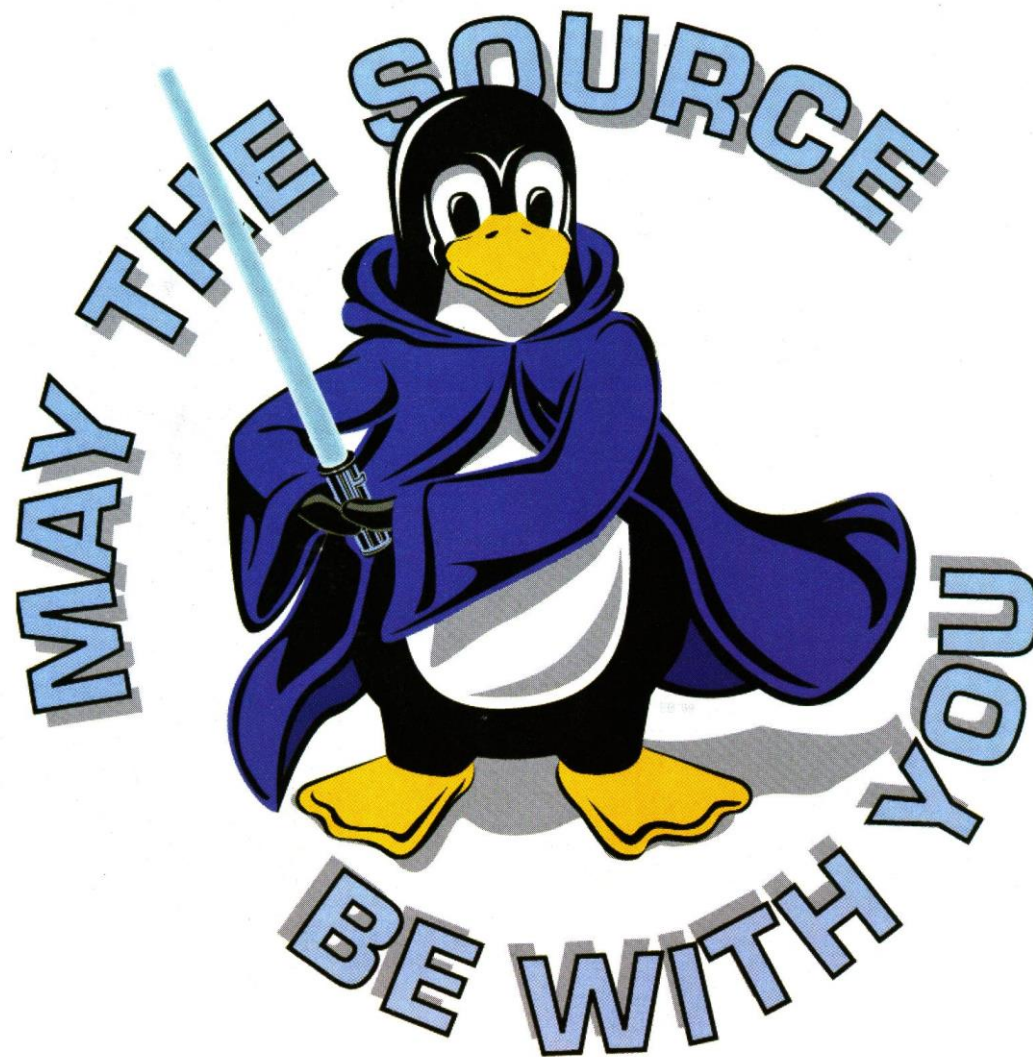


Cracking de contraseñas

- Diccionario: se utiliza un base de contraseñas conocidas y se aplica a la autenticación del servicio que se desea vulnerar.
- Fuerza bruta: se intenta reconstruir la contraseña o el digest de esta a través de generación de caracteres a alta velocidad, este tipo de ataques requiere gran capacidad de procesamiento.
- Vulnerabilidades: es posible realizar bypass de los sistemas de autenticación a través de algunas vulnerabilidades como SQLi o Padding

Resumen

- Control de acceso
- Tipos de autenticación
- Sistemas AAA
- Protocolos de Autenticación Microsoft
- Protocolos de Autenticación en Linux
- Autenticación en aplicaciones web
- Cracking de contraseñas



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA