Fundamentos de Redes (Grado en Ingeniería Informática y Doble Grado en Ingeniería Informática y Matemáticas)

Seminario 6: Resolución de problemas de los Temas 4 y 5

Curso 2023/2024

Profesora: Julia Caleya Sánchez, jcaleyas@ugr.es

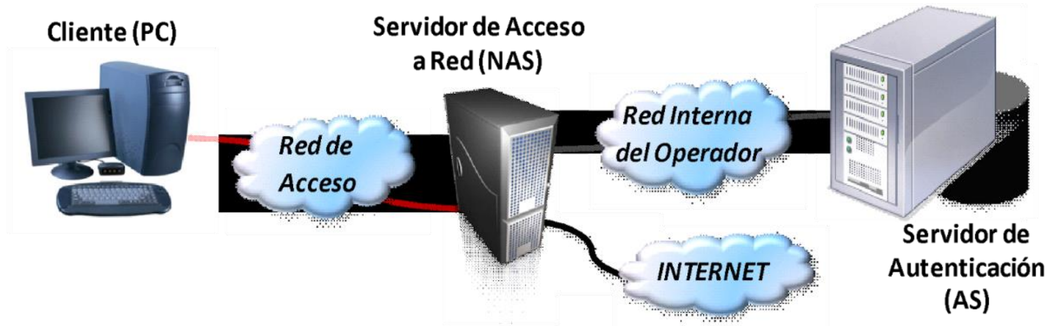
UNIVERSIDAD DE GRANADA

DPTO. TEORÍA DE LA SEÑAL, TELEMÁTICA Y COMUNICACIONES

Ejercicio 1

SEGURIDAD

La figura y mensajes siguientes describen un hipotético protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



Aceptadas la disponibilidad y validez de las claves públicas involucradas en base a la existencia de una entidad superior confiable, responda razonadamente:

a) **¿Qué servicios de seguridad se proporcionan en el protocolo descrito?**

b) **¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?**

PC -> NAS: $Kpub_{NAS}$(petición acceso + usuario)

NAS -> PC: desafío

PC -> NAS: $Kpub_{NAS}$(MD5(usuario + K_{PC-AS} + desafío))

NAS -> AS: petición autenticación + usuario + desafío + MD5(usuario + K_{AS-PC} + desafío)

AS -> NAS: petición aceptada + $Kses_{PC-NAS}$ + K_{PC-AS}($Kses_{PC-NAS}$) o petición rechazada

NAS -> PC: $Kpriv_{NAS}$(petición aceptada + K_{PC-AS}($Kses_{PC-NAS}$)) o $Kpriv_{NAS}$(petición rechazada)

PC -> NAS: $Kses_{PC-NAS}$(datos a enviar)

NAS -> Internet: datos a enviar

Internet -> NAS: datos de respuesta

NAS -> PC: $Kses_{PC-NAS}$ (datos de respuesta)

Siendo:

$Kpub_X$: cifrado con la clave pública de X

$Kpriv_X$: cifrado con la clave privada de X

K_{X-Y}: la clave secreta entre X e Y

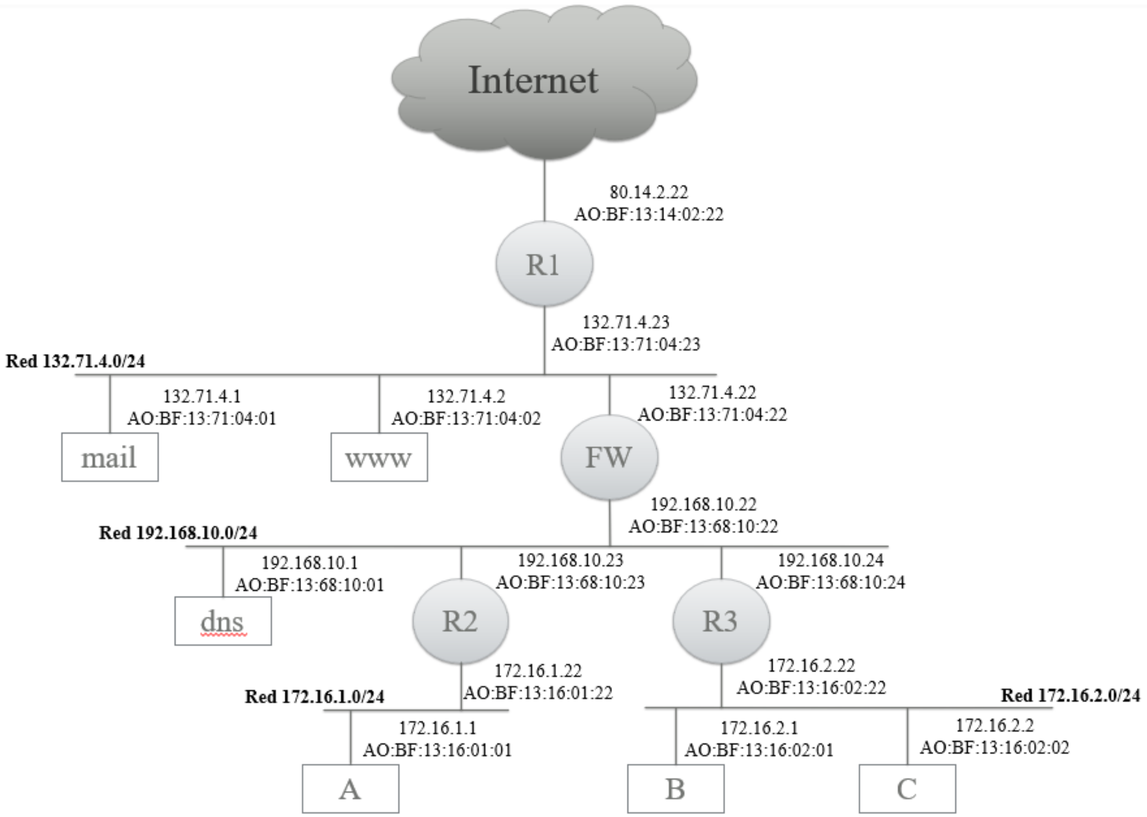
$Kses_{X-Y}$: la clave secreta de sesión entre X e Y

MD5 una función hash

Ejercicio 2

DNS Y SMTP

Dada la topología adjunta correspondiente a una red corporativa, en la que se especifican tanto las direcciones IP como las MAC de cada uno de los dispositivos que la forman, analice el tráfico generado al hacer un acceso de correo electrónico desde el host "C" al servidor "mail", especificando en una tabla, y para cada trama Ethernet generada:



a) **Las direcciones hardware (físicas) origen y destino.**

b) **Las direcciones IP origen y destino contenidas en el paquete IP encapsulado.**

c) **En su caso, los puertos origen y destino de la unidad de datos del protocolo (PDU) de transporte, así como los flags activos y campos de secuencia y ACK.**

d) **El tipo de mensaje de que se trata.**

NOTA: suponga todas las tablas ARP son conocidas y, por simplicidad utilice sólo los dos últimos de los 6 octetos de las direcciones físicas de las NIC (interfaces o tarjetas de red).

Ejercicio 3

VELOCIDAD DE TRANSMISIÓN EN SERVICIOS TELEMÁTICOS

Una sucursal con 50 empleados en Granada tiene una red interna basada en *FastEthernet* (100 Mbps) que se conecta a Internet con una red de acceso ADSL de 0,5 Mbps de subida y 1,5 Mbps de bajada. Cada empleado, en el desempeño de su trabajo, realiza un promedio de 2000 solicitudes de información a la hora a un servidor de Base de Datos ubicado en la central del banco, en Madrid, donde cada solicitud supone el envío por parte del servidor de un promedio de 10 registros de 1 KB cada uno. Adicionalmente, la modificación de datos tras algunas de estas solicitudes supone el envío promedio de 100 actualizaciones, de 10 registros de media, a la hora desde la sucursal al servidor. El resto de los servicios telemáticos se restringe. Calcule el promedio de la velocidad de transmisión requerida. ¿Es la velocidad del enlace de acceso suficiente?

Ejercicio 4

HTTP

Compare el rendimiento en términos temporales de HTTP persistente y no persistente considerando los siguientes parámetros:

- **Descarga de una página web con 10 objetos incrustados**
- **Tiempo de Establecimiento de conexión TCP: 5 ms**
- **Tiempo de Cierre de conexión TCP: 5 ms**
- **Tiempo de solicitud HTTP: 2 ms**
- **Tiempo de respuesta HTTP (página web u objeto): 10 ms**

Ejercicio 5

ESPECIFICACIONES PARA APLICACIONES TELEMÁTICAS

Discuta las características de las siguientes aplicaciones en términos de su tolerancia a la pérdida de datos, los requisitos temporales, la necesidad de rendimiento mínimo y la seguridad:

- **La telefonía móvil.**
- **WhatsApp.**
- **YouTube.**
- **Spotify.**
- **Comercio electrónico.**