



GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Seguridad en Redes (parte 1)





Introducción

- Las redes conectan computadoras.
¿Que problemas se presentan?
- Mayor interacción es posible, a costa de interacciones no deseadas
- Veremos los retos y problemas específicos de las redes, y como contribuye y depende de la seguridad de las computadoras
- En particular hablaremos de redes TCP/IP (Internet)



- Conceptos básicos redes TCP/IP
- Problemas de seguridad en redes TCP/IP
- Mecanismos de mitigación
 - Seguridad IP (IPSec)
 - Redes privadas virtuales (VPN)
 - Virtual LAN (VLAN)
 - Firewalls
 - Sistemas de detección de intrusos (IDS)



GRUPO DE SEGURIDAD INFORMÁTICA

Conceptos Básicos de redes TCP/IP





Redes de datos TCP/IP

- Pequeñas o grandes, su objetivo es llevar información de un computador a otro
- La mayor red de datos pública, **Internet**, funciona sobre protocolos e ideas de hace 30 años.
- Para simplificar su estudio, las redes se modelan separando su funcionalidad en “capas”
- Nos basaremos en el modelo OSI modificado para adaptarse a la arquitectura de TCP/IP



Internet

- Internet es el resultado de la interconexión de múltiples redes de computadoras que utilizan un mismo conjunto de protocolos
- Utiliza la tecnología de conmutación de paquetes (unidades de datos con un formato definido)

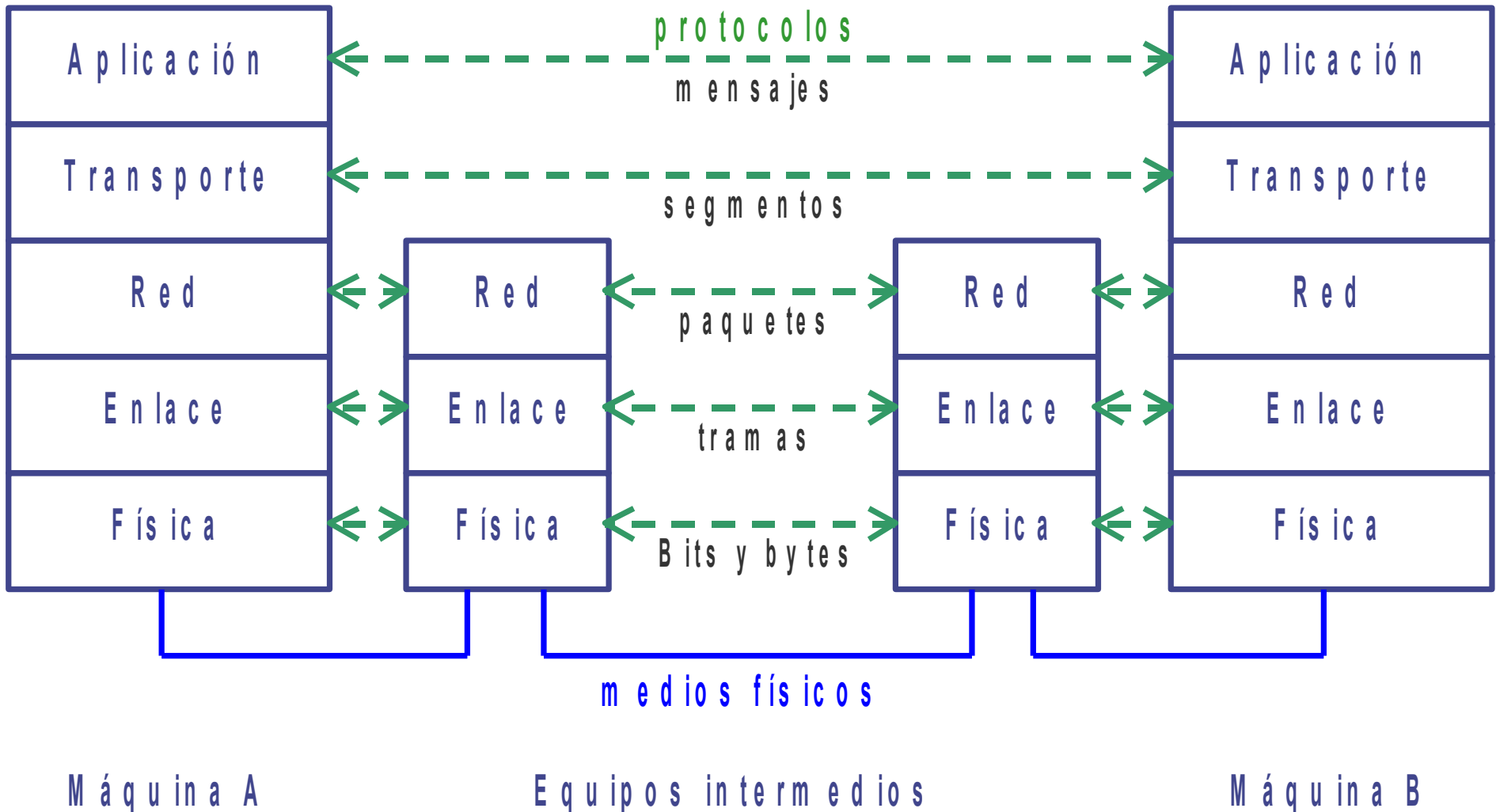


Modelo de capas

- Se utiliza un modelo organizado en capas para el diseño y análisis de las redes de datos
- Se trata de atacar el problema complejo mediante la división en problemas de menor complejidad
- Cada capa debe resolver un problema específico y dar servicios a las capas superiores



Modelo de capas en Internet





Funciones principales

- Aplicación (http, ftp, ssh, telnet, pop3, imap, ...)
 - Clientes y servidores de aplicaciones concretas
 - Ej: transferencia de archivos, correo electrónico, navegación...
- Transporte (tcp, udp)
 - Comunicación de datos entre cliente y servidor
 - Diferentes tipos de servicio y calidades
- Red (ip)
 - Encaminamiento de paquetes a través de la red para alcanzar el destino



Funciones principales (cont.)

- Enlace de datos (ethernet, ppp, hdlc, ...)
 - Transmisión de datos entre equipos directamente conectados. Ej: Ethernet, PPP, HDLC. También se pueden considerar ATM, FrameRelay cuando se usan como redes de transporte de IP
- Física (par telefónico, fibra óptica, coaxial, wireless)
 - Transmisión de datos en cada medio físico particular



Ejemplo: Navegación

- En mi navegador escribo:
 - <http://www.antel.com.uy>
- Se despliega en mi pantalla un conjunto de textos, imágenes, animaciones
- ¿Qué funciones son necesarias para que esto funcione?



Ejemplo: Navegación

- Los usuarios se manejan mejor con nombres (www.antel.com.uy), pero las computadoras no
- Hay que transformar esa etiqueta en una dirección de máquina. Protocolo de capa de aplicación: DNS
- Para intercambiar información entre el cliente y el servidor necesito un protocolo de capa de transporte: TCP en el ejemplo
- Para transportar los paquetes a través de la red uso el protocolo de capa de red: IP
- En las capas inferiores depende de la tecnología de conexión a la red en cada extremo



Capa de aplicación

- Múltiples protocolos: smtp, pop3, imap, http, https, ftp, etc.
 - Vulnerabilidades en protocolos e implementaciones
- Servicio **DNS: Domain Name system**
 - Servicio de capa de aplicación usado por las demás aplicaciones
 - Se implementa como una base de datos distribuida a nivel mundial
 - Opera con un mecanismo de consultas y respuestas
 - Es un **servicio crítico para el usuario de Internet**

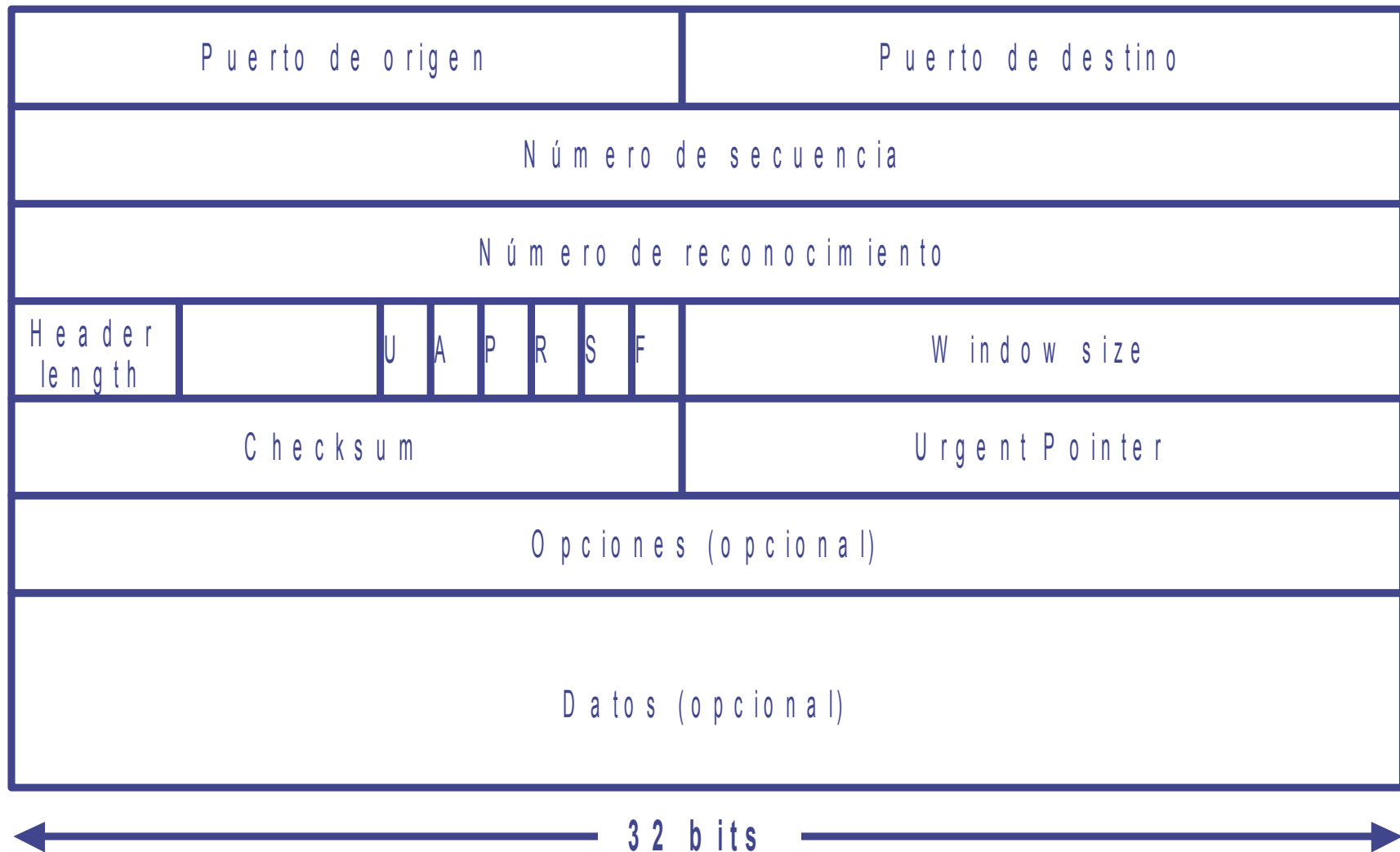


Capa de transporte

- En Internet, 2 protocolos:
 - TCP: Orientado a conexión, confiable
 - Garantiza un flujo confiable de información entre dos entidades
 - Usado por http, ftp, correo electrónico, etc.
 - UDP: No orientado a conexión, no confiable
 - Usado por DNS, VoIP,

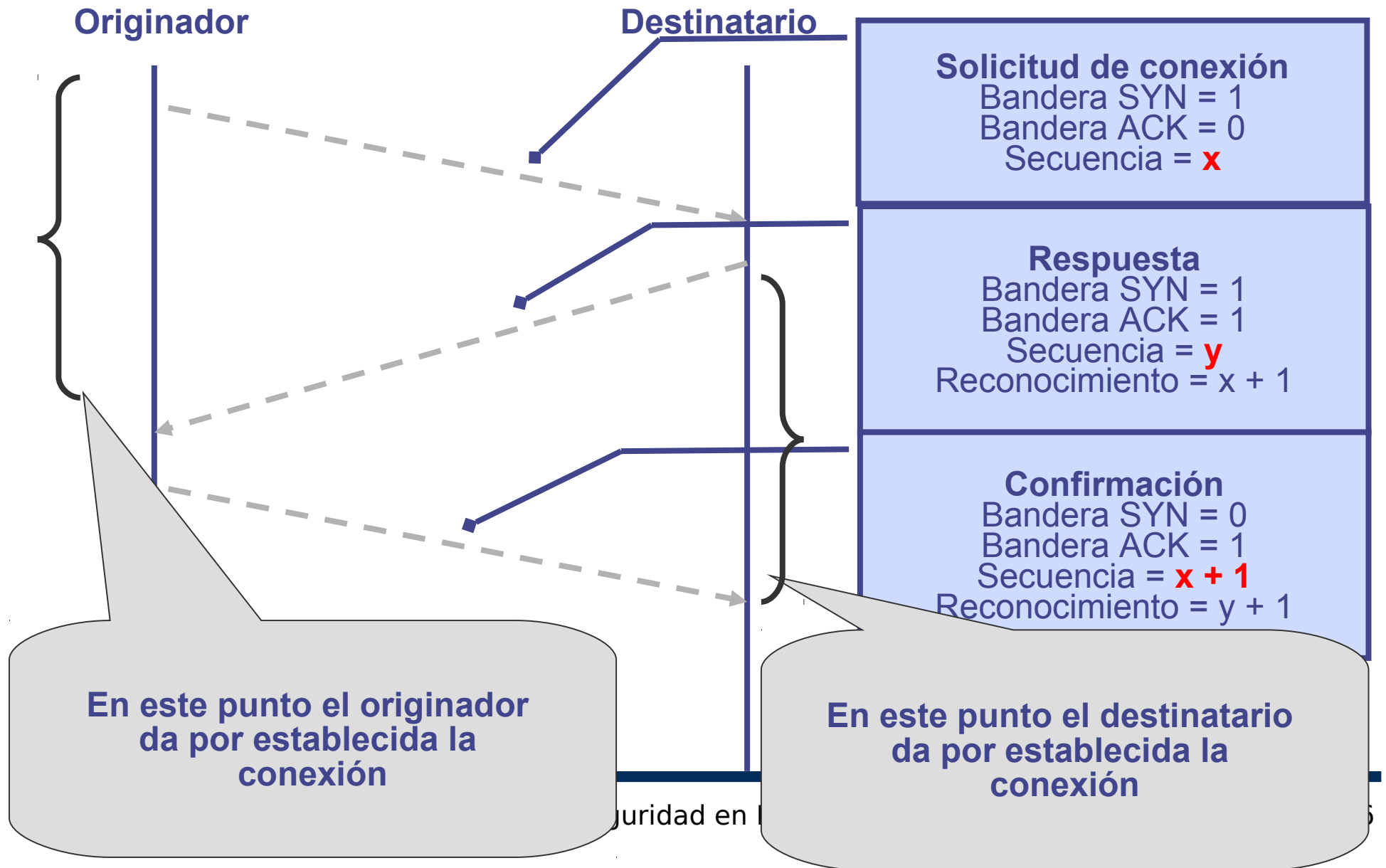


Encabezado TCP





Establecimiento de conexión en TCP





Algunos problemas de TCP

- Por cada conexión establecida o en proceso de establecerse el equipo consume recursos
 - Ataques de negación de servicio (SYN Flooding)
- Si el número de secuencia es predecible, podría establecer una conexión “ciega” o insertar datos en otra conexión
 - Session Hijacking



- Muy sencillo. Básicamente puertos origen y destino
- No ofrece garantías de entrega en destino
- No tenemos ningún campo que nos permita reconocer una solicitud válida de una inválida
 - Muy fácil realizar solicitudes “a nombre de otro”

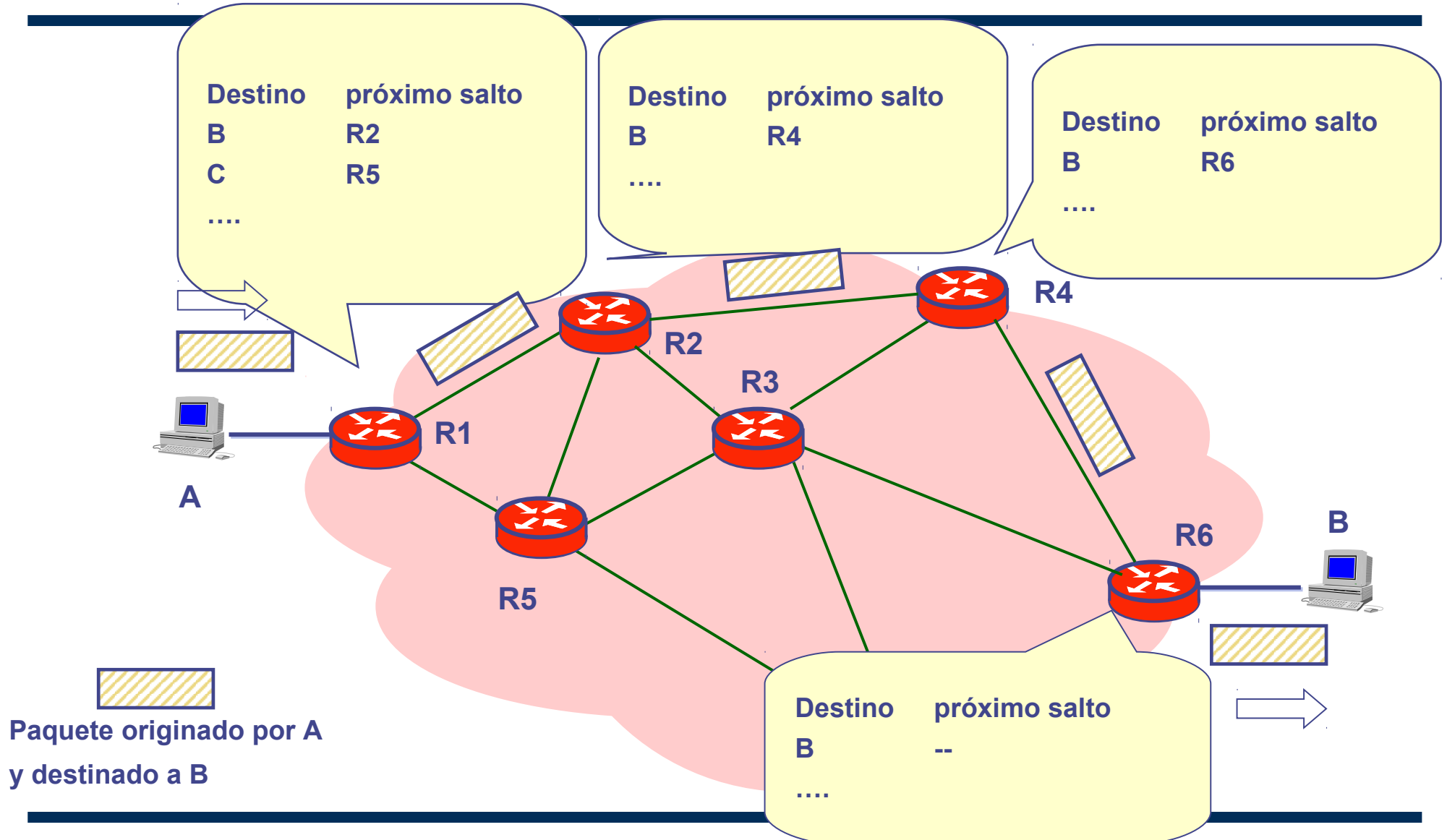


Capa de Red IP

- Arquitectura de datagramas
- Cada datagrama contiene en su encabezado la dirección del destino
- Es un servicio “mejor esfuerzo”. No hay garantía de entrega, ni de retardos, ni de orden
- La decisión de enrutamiento se realiza paquete a paquete en base a dirección de destino
- La red no mantiene información de estado de los flujos de paquetes que circulan por ella



Encaminamiento de datagramas (forwarding function)





Direcciones IP

- Identificador “único” en la red
- En IP versión 4: 32 bits (164.73.38.2)
- En IP versión 6: 128 bits (2001:1328:6::5)
- Asignadas por “Registros de Internet”
 - Hay rangos de direcciones para uso privado
- Cada paquete lleva dirección de origen y destino
- Típicamente se puede enviar paquetes con cualquier dirección de origen



Enrutamiento

- Cada enrutador en el camino de origen a destino debe conocer como llegar al destino
- Rutas estáticas: configuradas manualmente
- Rutas dinámicas: protocolos de ruteo
- Los enrutadores e información de ruteo son targets atractivos para un atacante
 - Negación de servicio
 - Redirección de tráfico
- No hay indicación del origen real del paquete



GRUPO DE SEGURIDAD INFORMÁTICA

Problemas de Seguridad en Redes TCP/IP



GSI - Facultad de Ingeniería - 2013



Capa 3 en internet

- IPv4 e IPv6
- Muy similares en sus características de seguridad
- IPSec es obligatorio (de implementar) en IPv6
- Servicio de datagramas. No hay garantías de entrega/duplicados/retardos. No hay garantías de origen
 - Cualquier equipo puede enviar un paquete con IP de origen arbitraria
 - Algunos proveedores filtran, otros no



- Salvo en ambientes muy controlados, no puede garantizarse la relación IP <-> máquina
 - En Internet, ni siquiera IP <-> empresa
- Es muy difícil rastrear un ataque proveniente de Internet con direcciones origen modificadas



Interacción de IP y la capa MAC

- ARP - Mapeo de dirección de capa 3 a dirección de capa MAC
- Protocolo muy sencillo.
 - A envía consulta por Broadcast pidiendo MAC correspondiente a la IP B
 - “B” responde
- Cualquiera puede responder
- Idea: modificar el mapeo en cache



ARP spoofing

- La mayoría de los sistemas aceptan respuestas a preguntas que no hicieron, o actualizan su cache ante un pedido
- Si lo “refresco” suficientemente seguido, no hará un nuevo pedido broadcast
- Permite ataques Man In The Middle, escuchas, Negación de servicio, etc.
- Es lo que se utilizó en el primer laboratorio



ARP Spoofing “Soluciones”

- Configuración de entradas ARP estáticas
- Separación de redes críticas
- Monitoreo de cambios en las entradas de ARP
- Encriptación en capas superiores
- Algunos equipos, al recibir un ARP donde cambia un mapeo existente IP-MAC, mandan una consulta ARP a la vieja MAC. Solo funciona si la entrada aún está en cache



Otros problemas en capa 3

- **Ataques** a los protocolos de **ruteo**
 - Si puedo modificar la información de ruteo, puedo encaminar tráfico importante por donde no debería
 - Es común que los protocolos de ruteo interno se ejecuten sin medidas de seguridad (aunque estas estén disponibles)
 - Con ruteo externo (BGP), el mayor peligro son publicaciones a través de proveedores que no filtren adecuadamente a sus clientes
- Ataques con paquetes de control (**ICMP**)



Capa 4 en internet

- UDP (servicio de datagrama): junto con IP, muy fácil hacer spoofing de solicitudes (ej. DNS)
- Muy difícil distinguir solicitudes válidas de inválidas. No hay estado en las solicitudes



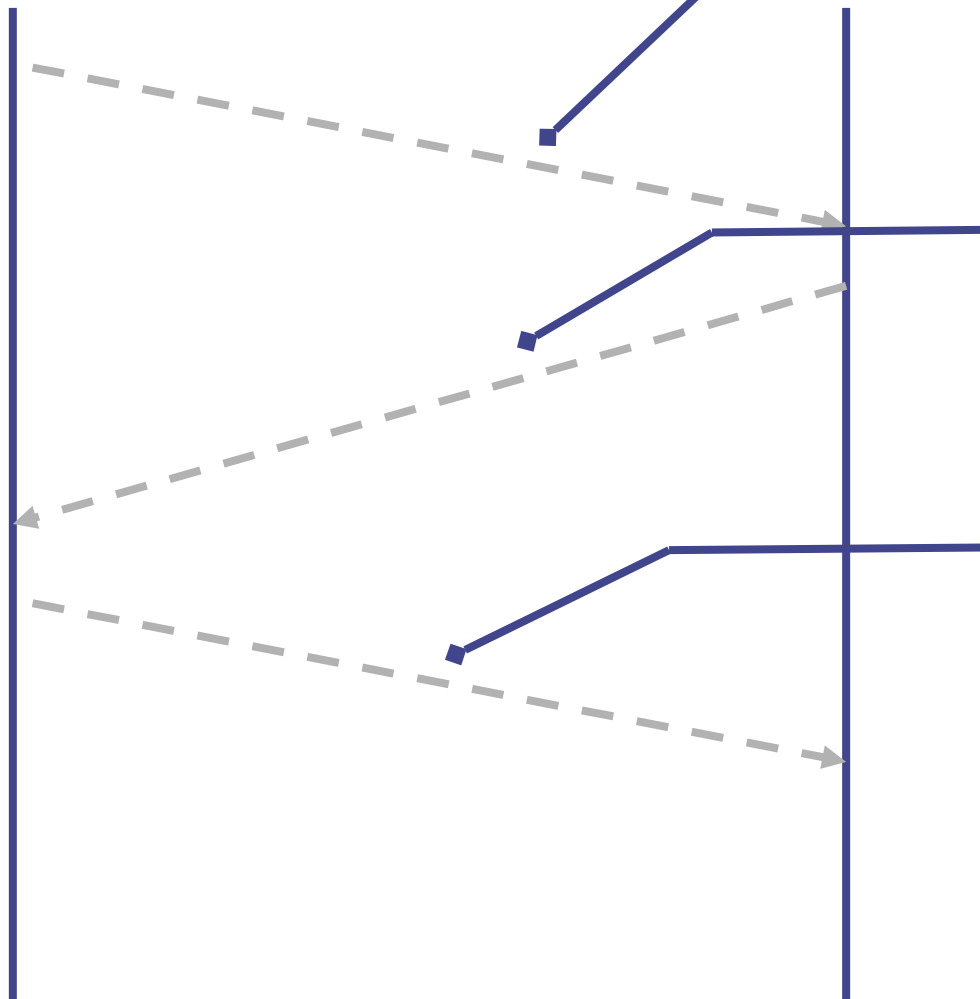
- Orientado a conexión, confiable
 - Número de secuencia para detectar segmentos duplicados, faltantes, reordenados, fuera de secuencia
 - Suma de comprobación para detectar errores de transmisión
 - No sirve para detectar modificación maliciosa
- Establecimiento de conexión de 3 vías



Establecimiento de conexión en TCP

Originador

Destinatario



Solicitud de conexión

Bandera SYN = 1
Bandera ACK = 0
Secuencia = x

Respuesta

Bandera SYN = 1
Bandera ACK = 1
Secuencia = y
Reconocimiento = x + 1

Confirmación

Bandera SYN = 0
Bandera ACK = 1
Secuencia = x + 1
Reconocimiento = y + 1



Establecimiento de conexión en TCP

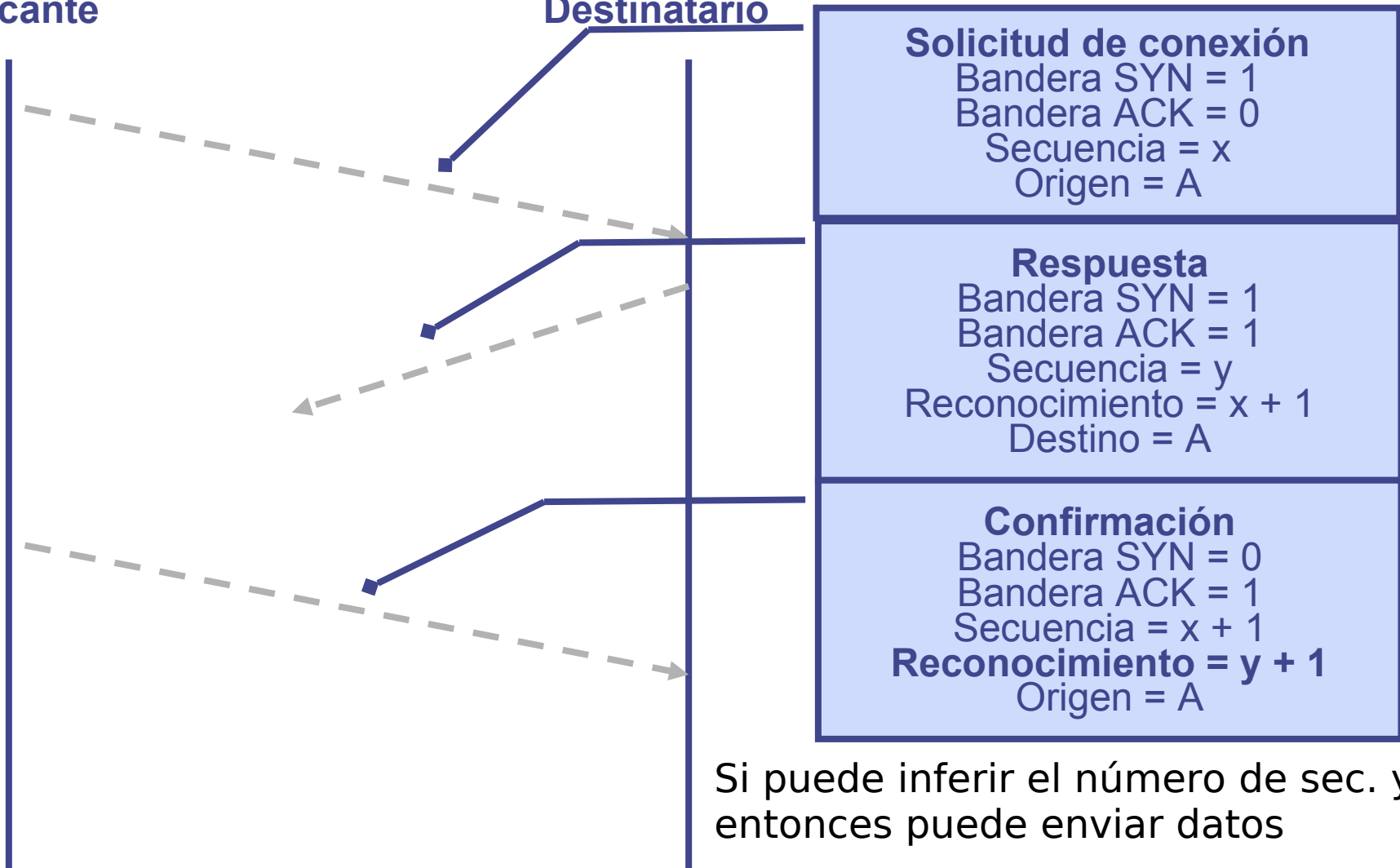
- Si yo quiero insertar datos en una conexión, debo conocer:
 - puertos origen y destino
 - IP origen y destino
 - Números de secuencia dentro de la ventana del receptor
- Idem para establecer una conexión “a ciegas”
- El número de secuencia inicial se elige “aleatoriamente”, no solo en base a un reloj como se hizo inicialmente



TCP Session Hijacking

Atacante

Destinatario



Solicitud de conexión Bandera SYN = 1 Bandera ACK = 0 Secuencia = x Origen = A
Respuesta Bandera SYN = 1 Bandera ACK = 1 Secuencia = y Reconocimiento = x + 1 Destino = A
Confirmación Bandera SYN = 0 Bandera ACK = 1 Secuencia = x + 1 Reconocimiento = y + 1 Origen = A

Si puede inferir el número de sec. y, entonces puede enviar datos



Algunas debilidades

- Por cada conexión, se debe guardar estado (incluso antes de completarse)
 - Syn flood: inundación de paquetes de establecimiento de conexión. Se ocupan recursos en conexiones que nunca se terminarán de establecer. Hay paliativos
 - Llenado de la tabla de conexiones establecidas
- Ataques con TCP reset (DOS)
- Ataques con ICMP unreachable
- Ataques con ICMP must-fragment



Capa de aplicación

- Donde se encuentran los servicios que le interesan al usuario
- Miles de potenciales servicios
 - Muchos de ellos sin ninguna consideración por la seguridad en su diseño
 - Otros mal implementados
- Algunos servicios se consideran parte de la infraestructura
 - DNS



Capa de aplicación

- Para conectarse a un determinado servicio, se utiliza el puerto de capa de transporte del mismo
 - Servicios bien conocidos. Ejemplos: http(80), smtp(25), pop3(110), ntp(123), dns (53), etc.
 - Otros. Pueden tener puertos fijos o algún servicio de directorio
- Portscan: búsqueda de servicios abiertos en una dirección o rango de direcciones
 - Intento de conexión a muchos puertos



- Resolución de nombres
- Sistema distribuido
 - Zonas de autoridad, con sus servidores autoritativos
 - Servidores recursivos que guardan cache
- Las consultas utilizan UDP
- 13 servidores “raiz” (13 direcciones IP), necesarios para comenzar cualquier búsqueda



Por qué es crítico

- Si no funciona, la mayoría de los servicios serían inalcanzables por la mayoría de los usuarios
- Si se modifican datos maliciosamente, se puede redirigir tráfico de un sitio legítimo o negar servicio
 - Phishing y otros ataques



Problemas del DNS

- Bugs de seguridad en los servidores antiguos (BIND y otros)
- Cache corruption: ante una pregunta, el servidor devuelve datos relevantes para otra consulta, falsos. Versiones viejas de servidores recursivos caían en esta trampa
- No hay ninguna autenticación de las respuestas
- Bugs en los clientes
 - Aceptar respuestas a consultas que no se hicieron



Problemas del DNS

- Puede brindar información sobre los servicios brindados externamente (e internamente si los ponemos en el DNS)
 - Es común utilizar “split dns” (visiones distintas según desde donde o a qué servidor consultemos)
- Separar servidores internos (recursivos) de los externos, para evitar intentos de cache poisoning desde afuera
- Problemas de seguridad en los registros de nombres de dominio



Otras aplicaciones

- Cualquier aplicación accesible a través de una red es susceptible de ser atacada si tiene bugs en su implementación
- Históricamente, la cantidad de bugs de seguridad en servidores de todo tipo es alta
- A veces nos olvidamos que, por ejemplo, una impresora con conexión de red es tan vulnerable como nuestros servidores
- Algunos ejemplos se verán la semana que viene



Ataque comunes en redes

- Pruebas y escaneos: intentos de obtener información de sistemas remotos. Típicamente como precursores de futuros ataques
- Envío de paquetes que exploten vulnerabilidades en las implementaciones de los protocolos o las aplicaciones
- Captura de paquetes (packet sniffing) – capturar paquetes que pasan por la red y obtener información sensible



Más tipos de ataque

- Negación de servicio (denial of service) – generar peticiones que carguen excesivamente o hagan colapsar un equipo o enlace
- Spoofing – hacerse pasar por otra máquina (u otro usuario)



Portscans

- Típicamente ataque “de reconocimiento”
- Búsqueda de servicios disponibles
- Detección de versiones
- “Fingerprint” del Sistema Operativo, parches



Ataques de negación de servicios

- Hemos visto que pueden ser causados por problemas en varias capas
 - ARP spoofing
 - Ataques a los protocolos de ruteo
 - Llenado de tablas de información de conexiones
 - Modificación de entradas en el DNS



Bibliografía y referencias

- **A. Tanenbaum.** *Redes de Computadoras.* 4Ta ed. Prentice Hall, 2003.
- **R. Anderson,** *Security Engineering – A Guide to Building Dependable Distributed Systems,* Wiley, 2001.
- **D. Gollman,** *Computer Security,* Wiley, 2006.