GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Seguridad en Redes TCP/IP

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)

Plan

- 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)

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 al menos 40 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

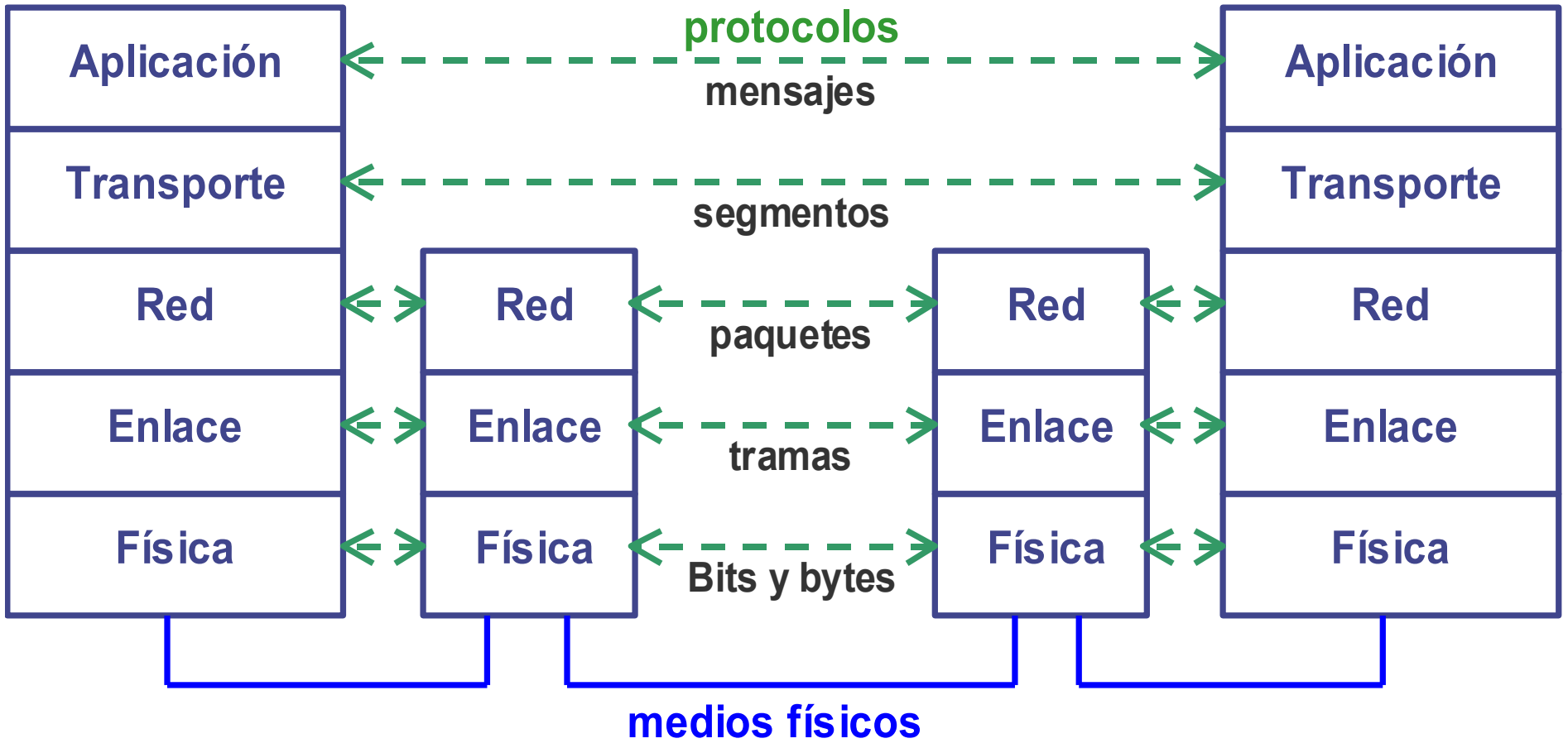
Internet

- 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.fing.edu.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.fing.edu.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

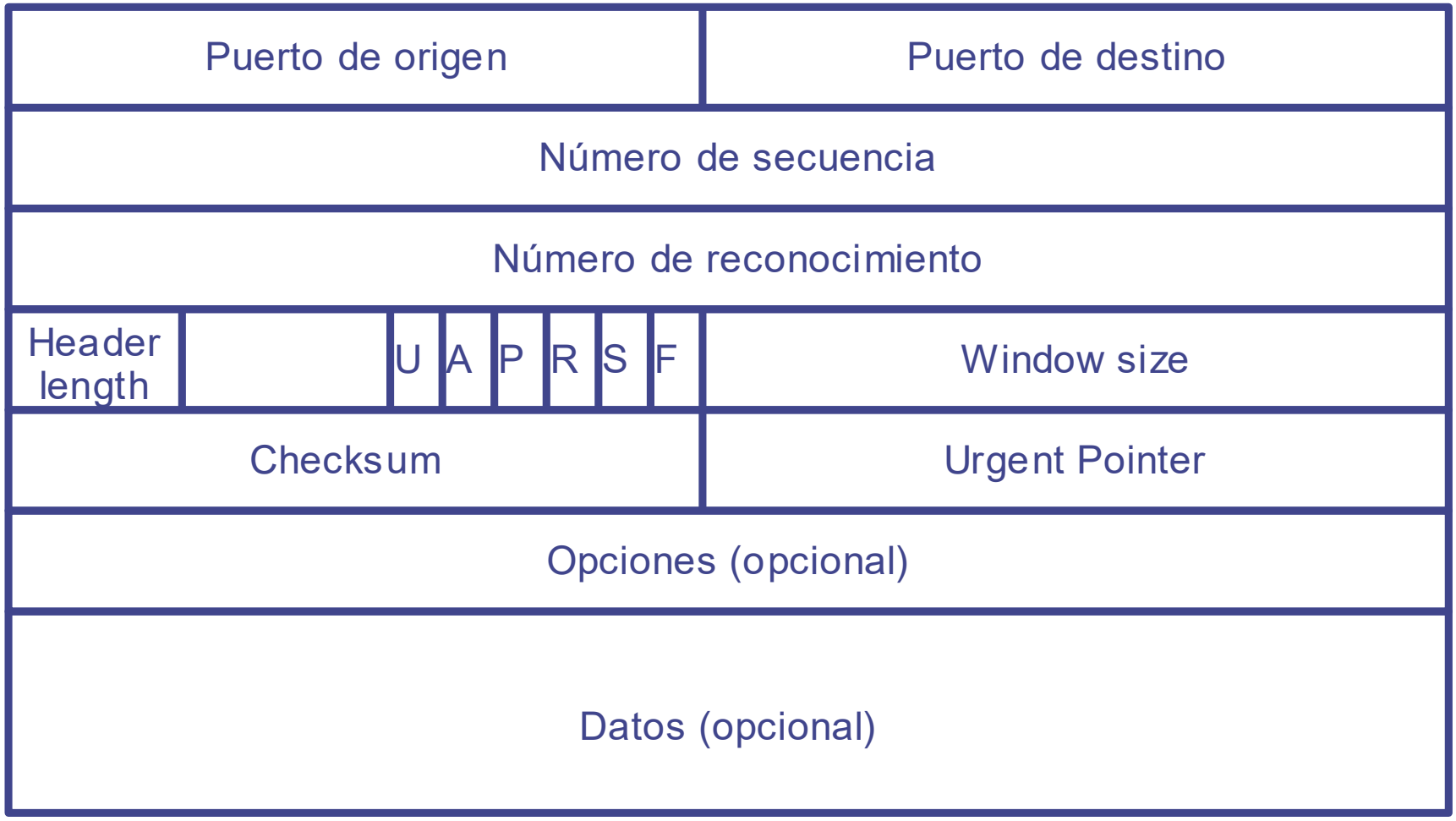
Capa de aplicación

- 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**

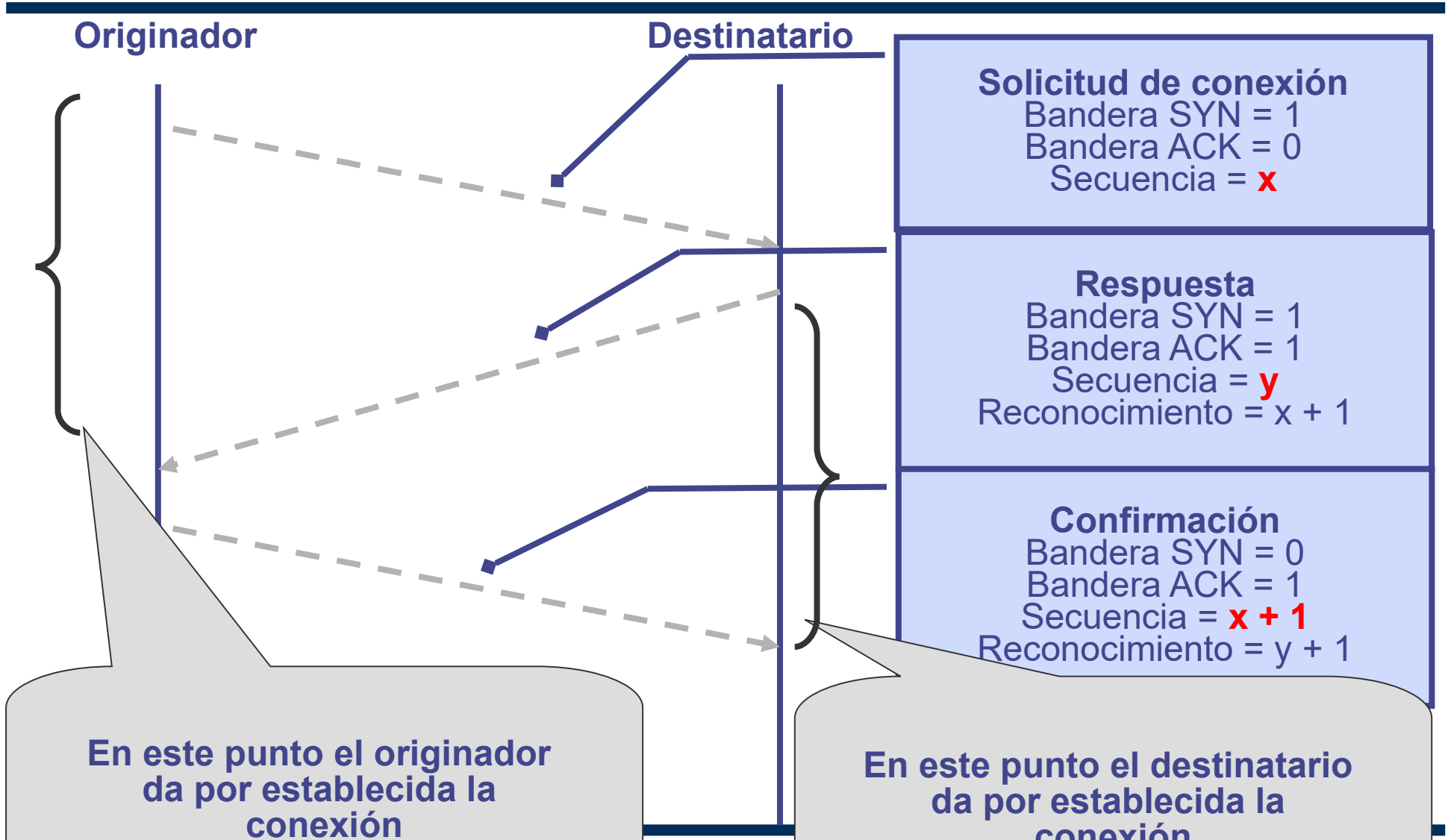
Capa de transporte

- En Internet, 2 protocolos:
  - TCP: Orientado a conexión, confiable
    - Garantiza un flujo confiable de información entre dos entidades
    - Usado por http, ftp, correo electrónico (SMTP), 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

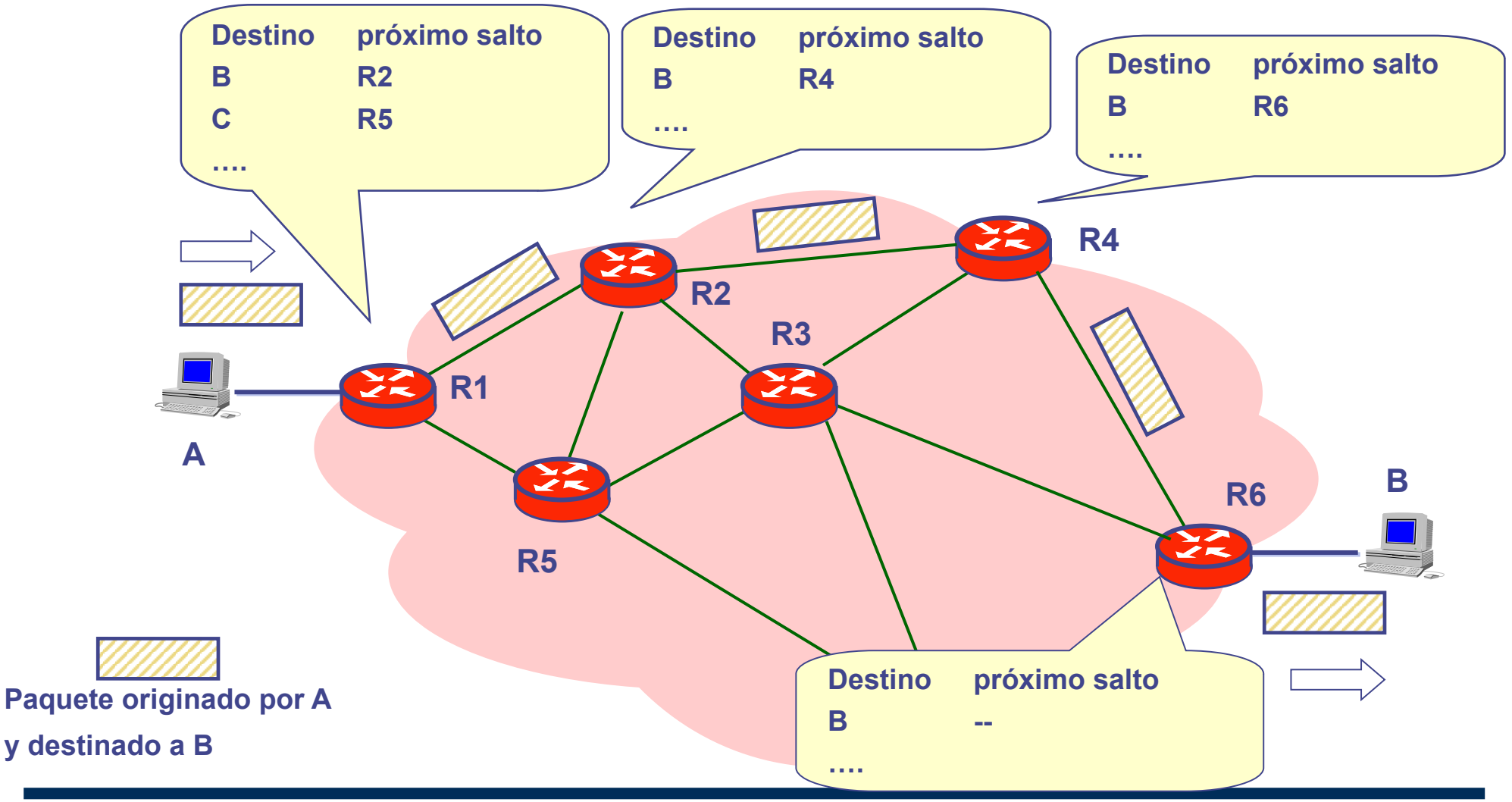
UDP

- 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

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.