Protocolos de la Capa de Aplicación

Ing. Norberto Gaspar Cena
Redes de Información
4to Año Ingeniería en Sistemas de Información

World Wide Web

- Fue la primera aplicación de Internet que atrajo al publico en general (1990)
- La web opera bajo demanda
  - Muy diferente a la radio o a la televisión donde los operadores tienen “disponible el contenido”
- HyperText Tranfer Protocol (HTTP) [RFC 1945 y RFC 2616]
- Utiliza el modelo cliente/servidor
  - HTTP define la estructura de mensajes de como interactúan el cliente y el servidor
- La web consta de objetos
  - Objetos: html, jpg, clip de audio/video, etc

World Wide Web - HTTP

- Utiliza TCP como protocolo de transporte
  - Se inicia la conexión TCP (*3-way handshake*)
  - Los procesos del cliente y del servidor acceden a través de sus sockets
  - Los mensajes se envían y se reciben a través de los sockets
  - HTTP no se preocupa por la perdidas de datos
- Del lado del servidor se envía información sin almacenar información acerca de los clientes
  - Un objeto se puede mandar muchas veces al mismo cliente
  - HTTP es un protocolo sin memoria de estado
- Debería cada par solicitud/respuesta ir por una conexión TCP separada?
  - Conexiones persistentes/Conexiones no persistentes

HTTP – No persistente y Persistente

http://www.frvm.utn.edu.ar/

- Se inicia la conexión
- El cliente envía un mensaje de solicitud HTTP a través de su socket
- El proceso servidor recibe el mensaje, recupera el objeto de su medio de almacenamiento, encapsula el objeto y envía al cliente
- El proceso HTTP indica a TCP que cierre la conexión (TCP realmente no termina la conexión)
- El cliente HTTP recibe el mensaje de respuesta. La conexión TCP termina. El cliente HTTP extrae el objeto, examina el archivo HTML y localiza las referencias a los demás objetos
- Los primero cuatro pasos se repiten para cada uno de los objetos que contenga la web

Se generan tantas conexiones TCP como objetos contenga la web

HTTP – Formato de los mensajes

Mensaje de solicitud HTTP

- GET /unadirección/pagina.html
- Host: www.frvm.utn.edu.ar
- Connextion: close
- User-agent: Mozilla/4.0
- Accept-language: es

Mensaje de respuesta HTTP

- HTTP/1.1 200 OK
- Connection: close
- Date: Mon, 13 May 2013 12:30:14 GMT
- Server: Apache/1.3.0 (Linux)
- Last-Modified: Sun, 6 May 2013 09:34:14 GMT
- Content-length: 6821
- Content-Type: text/html
- (datos)

HTTP – Códigos de Estado

200 OK: La solicitud se ha ejecutado con éxito

301 Moved Permanently: El objeto solicitado ha sido movido de forma permanente. Location: especifica el nuevo URL

400 Bad Request: Error genérico indicando que la solicitud no ha sido entendida por el servidor

404 Not Found: El objeto solicitado no existe en el servidor

500 HTTP version Not Supported: La versión de HTTP solicitada no es soportada por el servidor

HTTP – Cookies

HTTP no mantiene estados

A menudo es deseable poder identificar a los usuarios

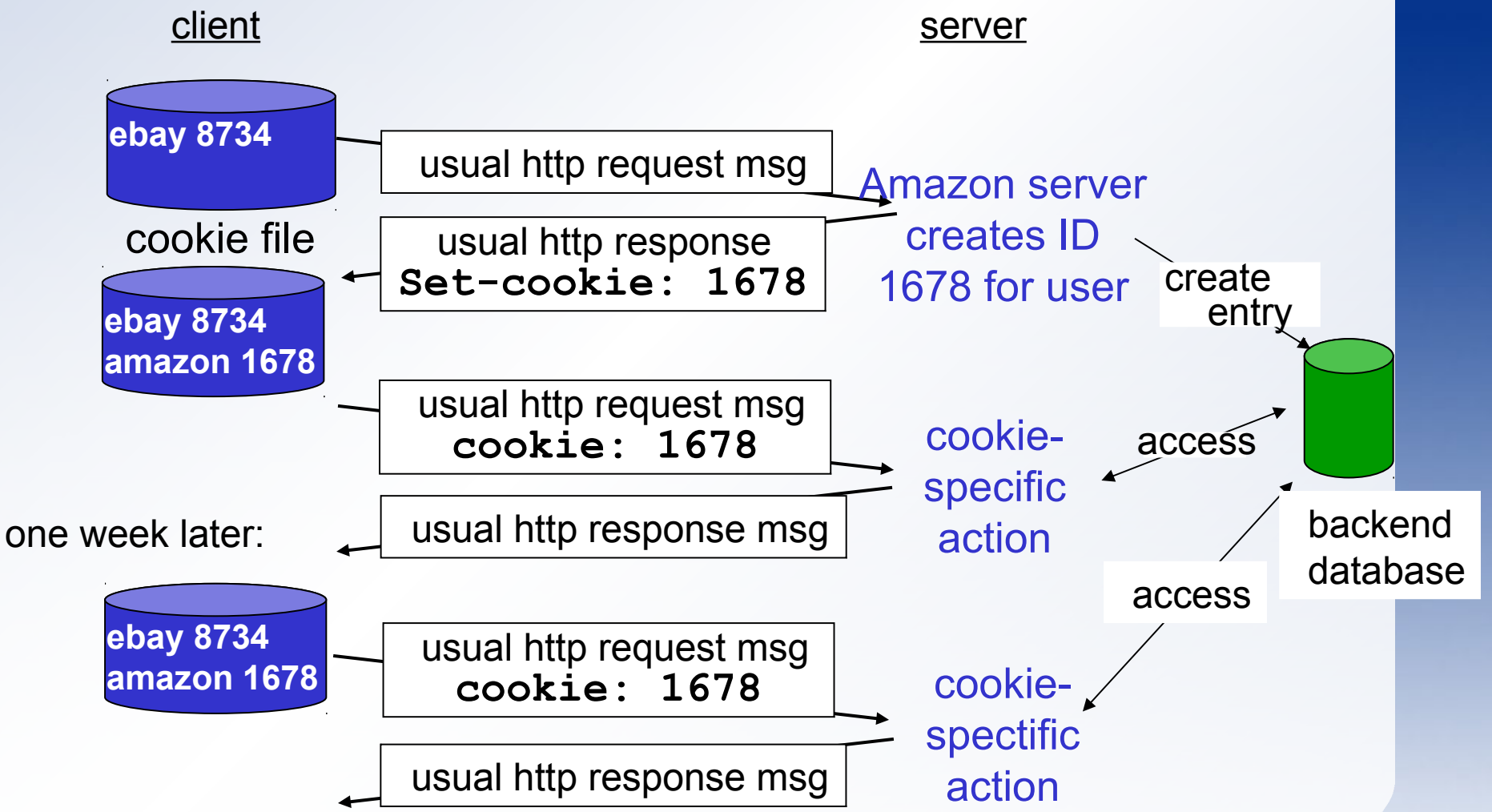
Para estos fines HTTP cookies [RFC 2965]

De esta manera se logra realizar un seguimiento de los usuarios

Son algo controvertidas

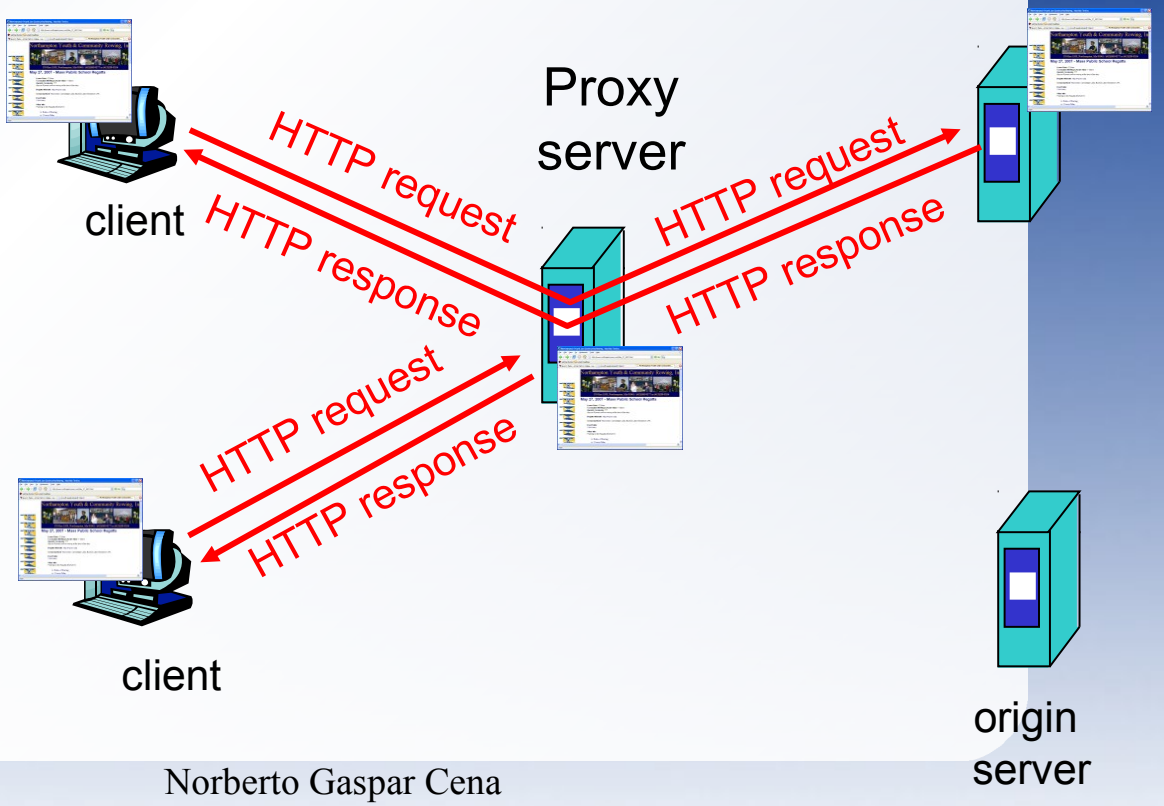
- Puede considerarse como una invasión a la privacidad del usuario

HTTP – Cookies



Almacenamiento Cache web

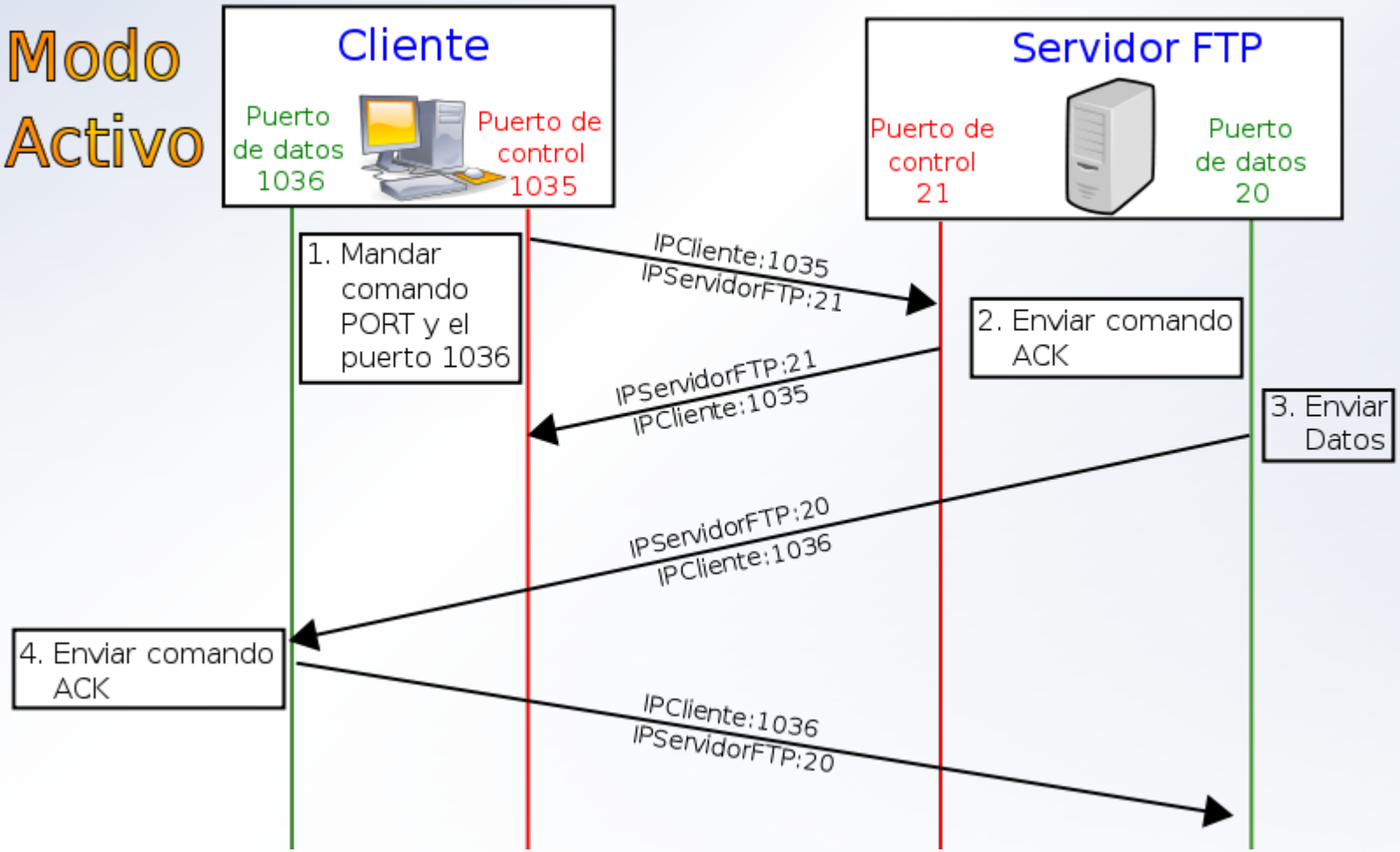
Servidor Proxy
Dispone de su propio espacio en disco
Mantiene copias de objetos solicitados
Utiliza la cabecera
HTTP para obtener
la fecha de
ultima modificación
ISA Server/Squid



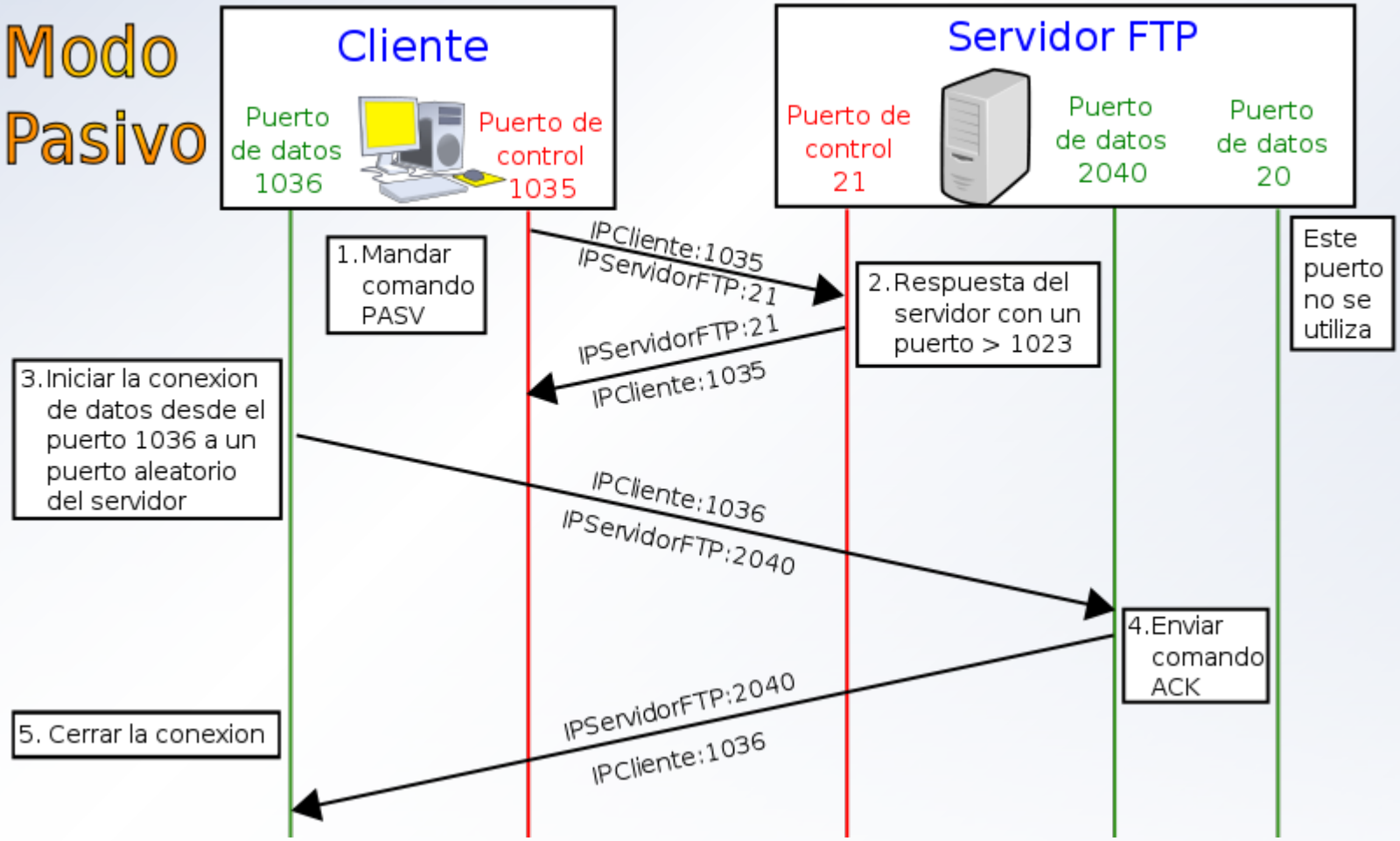
Transferencia de Archivos – FTP

- Proporciona servicio de autenticación
  - Además de permisos de escritura/lectura/ejecución
- Funciona sobre TCP
- Utiliza dos conexiones TCP paralelas
  - Conexión de control
  - Conexión de datos
- Se establece una conexión TCP al servidor al puerto 21
  - Por defecto el puerto para el envío de datos es el 20
  - FTP activo / FTP pasivo
- El lado cliente envía identificación y contraseña
- A través de este puerto se envían comandos para modificar el directorio remoto
  - Las conexiones de datos son abiertas y cerradas por cada archivo enviado
  - La conexión de control permanece abierta durante la sesión del usuario

Transferencia de Archivos – FTP



Transferencia de Archivos – FTP



FTP – Comandos y Respuestas

Comandos

- user nombre_de_usuario
- pass contraseña
- ls
- mput/put nombre_archivo/s
- mget/get nombre_archivo/s
- del nombre_archivo
- pwd
- cd

Respuestas

- 331 Username OK, password required
- 125 Data connection already open; transfer starting
- 425 Can't open data connection
- 425 Error writing file

RFC [959]

Correo electrónico en Internet

Esta compuesto por

- Agentes de usuario
- Servidores de correo
- Protocolo simple de transferencia de correo (SMTP)

Los agentes de correo se utilizan para leer/responder/reenviar/guardar/escribir correos

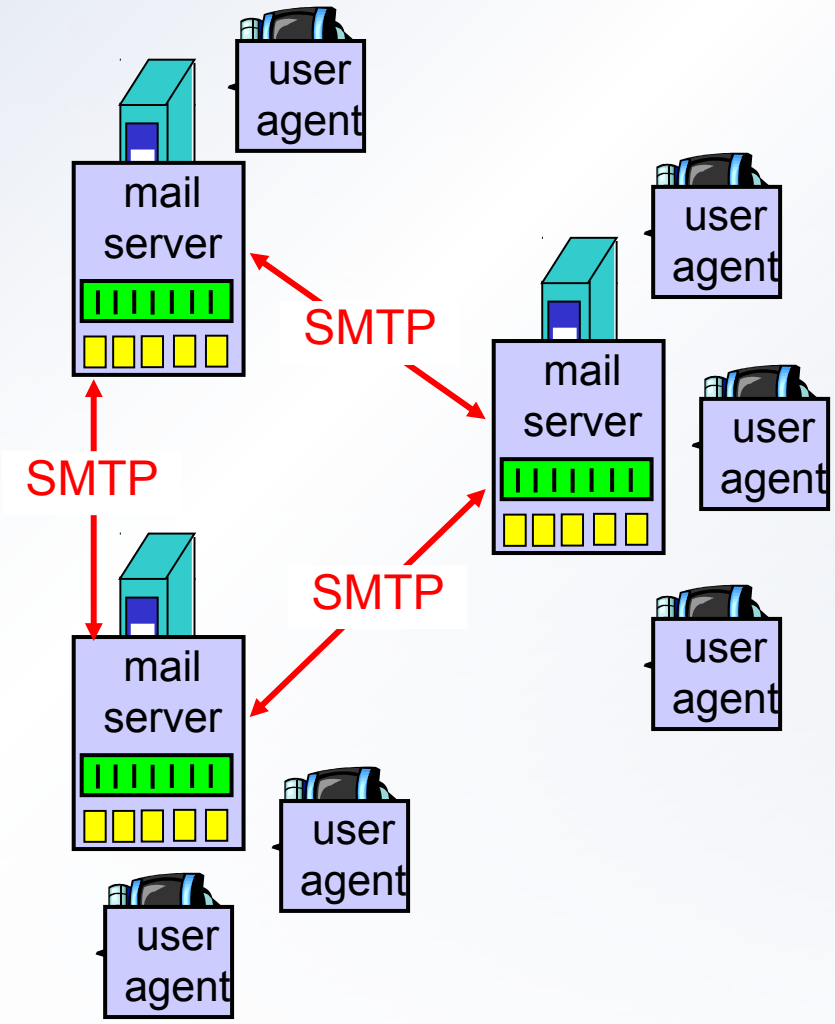
Los servidores de correo forman el núcleo de la infraestructura

- Cada destinatario tiene un buzón de correo
- Los servidores mantienen colas de mensajes
- Reintentos de envío y mensajes de error

SMTP [RFC 822]

- Puerto 25

Esquema Global



SMTP

Utiliza TCP para las conexiones

Realiza conexiones persistentes

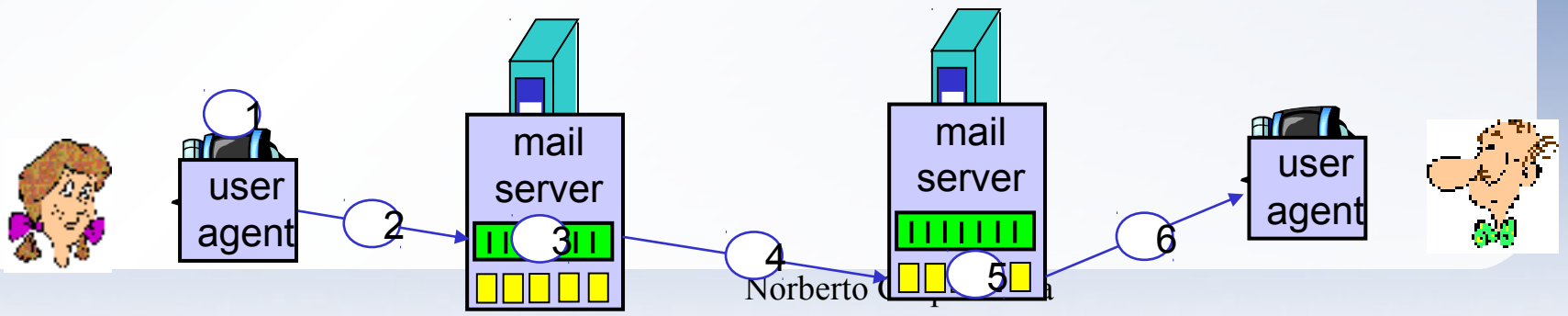
Comandos

- HELO / MAIL FROM / RCPT TO / DATA

SMTP nativo solo acepta mensajes US ASCII

- Para solucionarlo se implemento Multiporpose Internet Mail Extensions
- Version de MIME: Content-Type

MIME [RFC 2045] a [RFC 2049]



POP3

Post Office Protocol Version 3 (pop3)

- Funciona sobre TCP
- Protocolo de correo simple
- Utilizado solo para descargar correos
- Puerto 110

Comandos

- user usuario
- pass contraseña
- list
- retr 1
- del 1

IMAP

Internet Mail Access Protocol (IMAP) [RFC 3501]

- Funciona sobre TCP
- Protocolo de correo complejo
- Puerto 143

Viene a resolver el problema de la portabilidad de los correos

Permite crear/borrar/mover los mensajes

Permite realizar búsquedas en carpetas remotas

Permite bajar solo parte de los mensajes (Cabecera)

Funcionamiento de los correos electrónicos web

Administración de la red - SNMP

Administra (consulta u otras operaciones) de diferentes dispositivos (*routers, switches, hubs, hosts, modems, impresoras, etc*)

Cada equipo conectado a la red ejecuta procesos (agentes)

Ejemplo:

- en un **router**: interfaces activos, la velocidad de sus enlaces serie, número de errores, bytes emitidos, bytes recibidos, etc
- en una **impresora**: *que se terminó el papel, cantidad de trabajos, etc*
- en un **switch**: *bocas conectadas, tráfico de cada una, etc*

Administración de la red - SNMP

La forma normal es mediante el sondeo (pooling)

- Pregunta: la estación administradora envía una solicitud a un agente (proceso que atiende petición SNMP) pidiéndole información o mandándole actualizar su estado
- Respuesta: la información recibida del agente es la respuesta o la confirmación a la acción solicitada

El Problema: muchos nodos = mucho tráfico

La solución: trap

- Un agente manda la información al nodo administrador puntualmente, ante una situación predeterminada

Puerto UDP/161 sondeo

Puerto UDP/162 trap

Administración de la red - SNMP

- Nodos administrados que ejecutan agentes SNMP
- Estación administradora o consola de administración encargados de hacer el pooling o recibir el trap de los agentes
- Mantienen una base de datos MIB
- MIB: Management Information Base. Base de datos relacional (organizada por objetos y sus atributos o valores) que contiene información del estado de un nodo administrado y es actualizada por los agentes SNMP

Administración de la red - SNMP

Grupo	Variable	Significado
system	sysUpTime	Tiempo desde el último arranque
interfaces	ifNumber	Número de interfaces de red
interfaces	ifInErrors	Número de paquetes entrantes en los que el agente ha encontrado error
ip	ipInReceives	Número de paquetes recibidos
icmp	icmpInEchos	Número de solicitudes de Echo ICMP recibidas
tcp	tcpInSegs	Número de paquetes TCP recibidos
udp	udpInDatagrams	Número de datagramas UDP recibidos

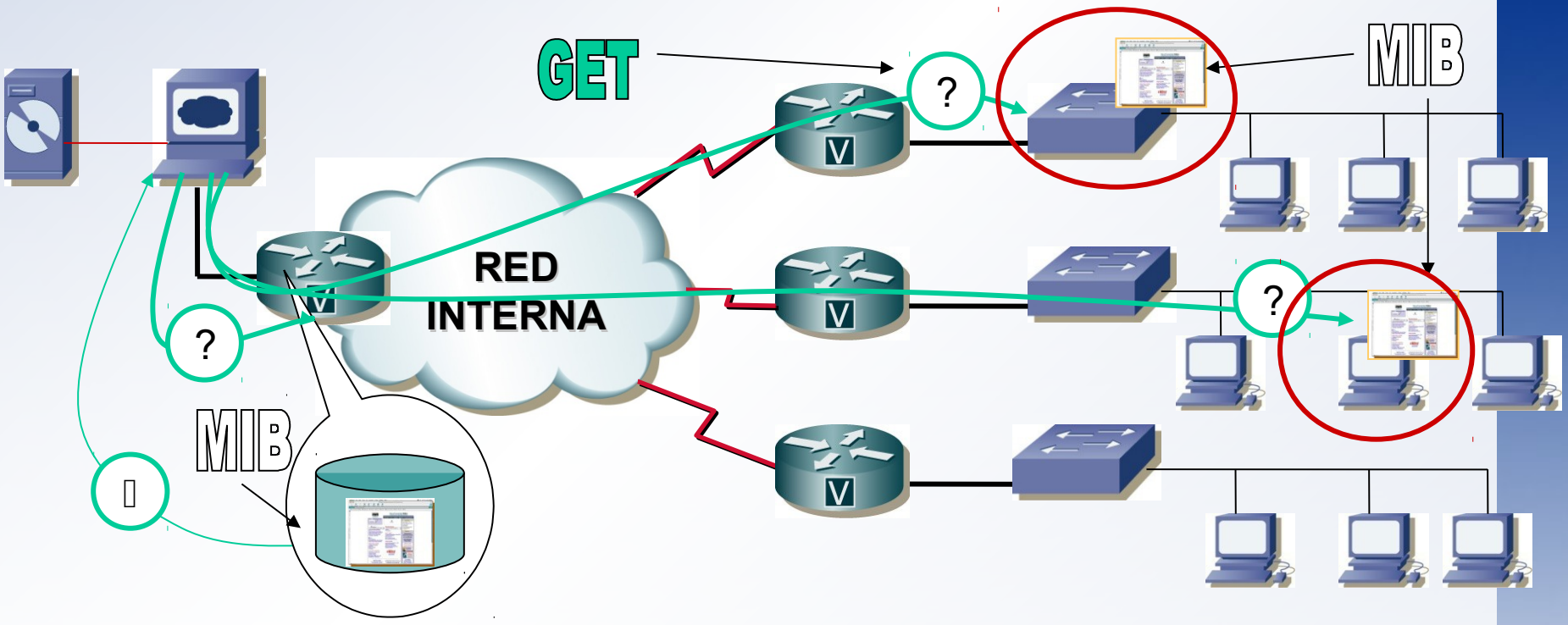
SNMP – Comandos Básicos

GET: Implica que la consola de administración recupera datos del agente

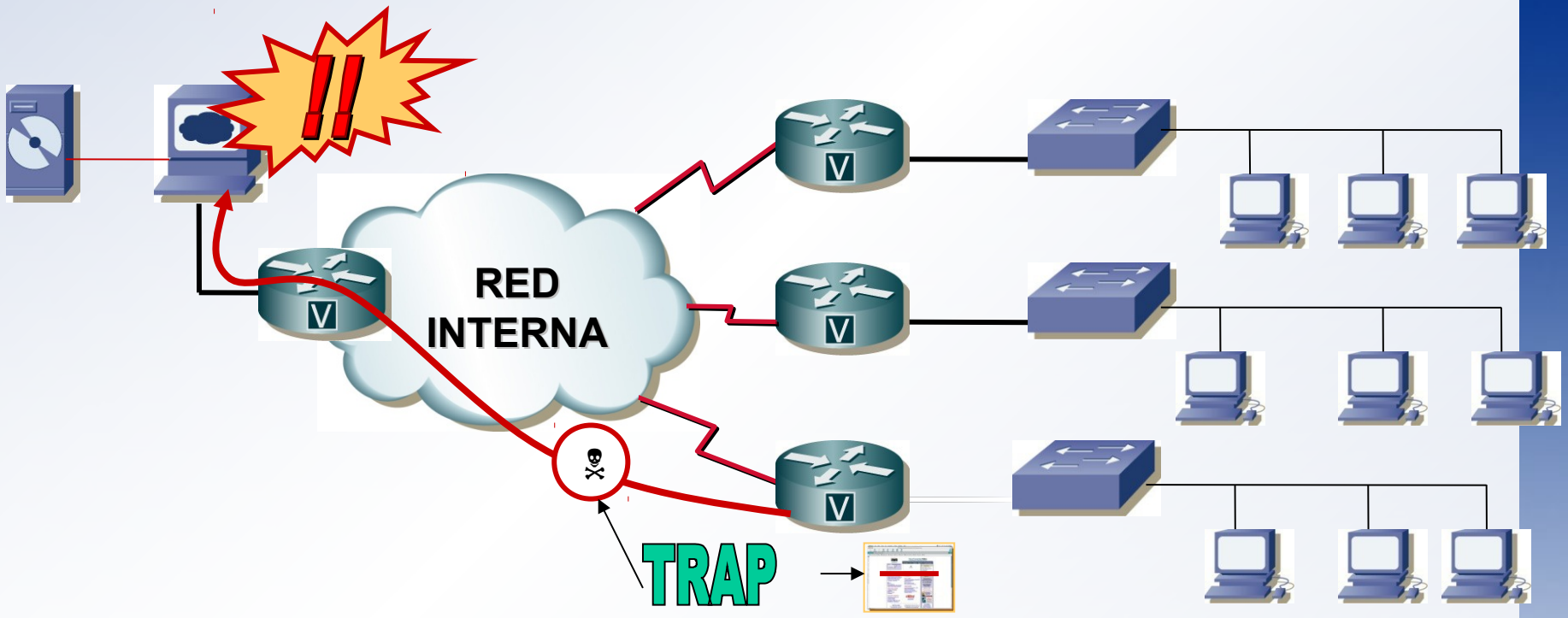
SET: Implica que la consola de administración establece los valores de los objetos en el agente

TRAP: Implica que el agente notifica a la consola de administración acerca de los sucesos de importancia por interrupción

SNMP – Ejemplos de Funcionamiento



SNMP – Ejemplos de Funcionamiento



SNMP – Versiones

Versión 1

- La seguridad se basa en comunidades (que usan passwords comunes sobre texto plano)
- A pesar de que es la versión inicial es la que se distribuye en muchos equipos

Versión 2

- Reduce la carga de tráfico adicional para la monitorización. SNMPv2 puede leer SNMPv1

Versión 3

- Para evitar la falta de seguridad en las transmisiones (con cifrado y autenticación)

Si no se dispone de seguridad suficiente, con carácter general es aconsejable deshabilitar la ejecución de comandos SET

SNMP – Monitorización Inteligente

Ejemplo 1:

- Mediante SNMP, un router puede reportar **un incremento de la carga cada 10%.**
- *"Si utiliza un sondeo dirigido por interrupción y se conoce la **carga del sondeo regular**, puede dar instrucciones al router para enviar una interrupción cuando se experimente un incremento significativo en la carga,10%"*
- Después de recibir un mensaje de interrupción, el servidor puede seguir sondeando al dispositivo para mayores detalles.

Ejemplo 2:

- **Otro caso de configuración,** cuando el router de salida tiene tráfico de salida superior a 34 Mbps, que mande al administrador de la red notificación o alerta

Palabras Claves

- HTTP
- FTP
- SMTP
- POP3/IMAP
- SNMP