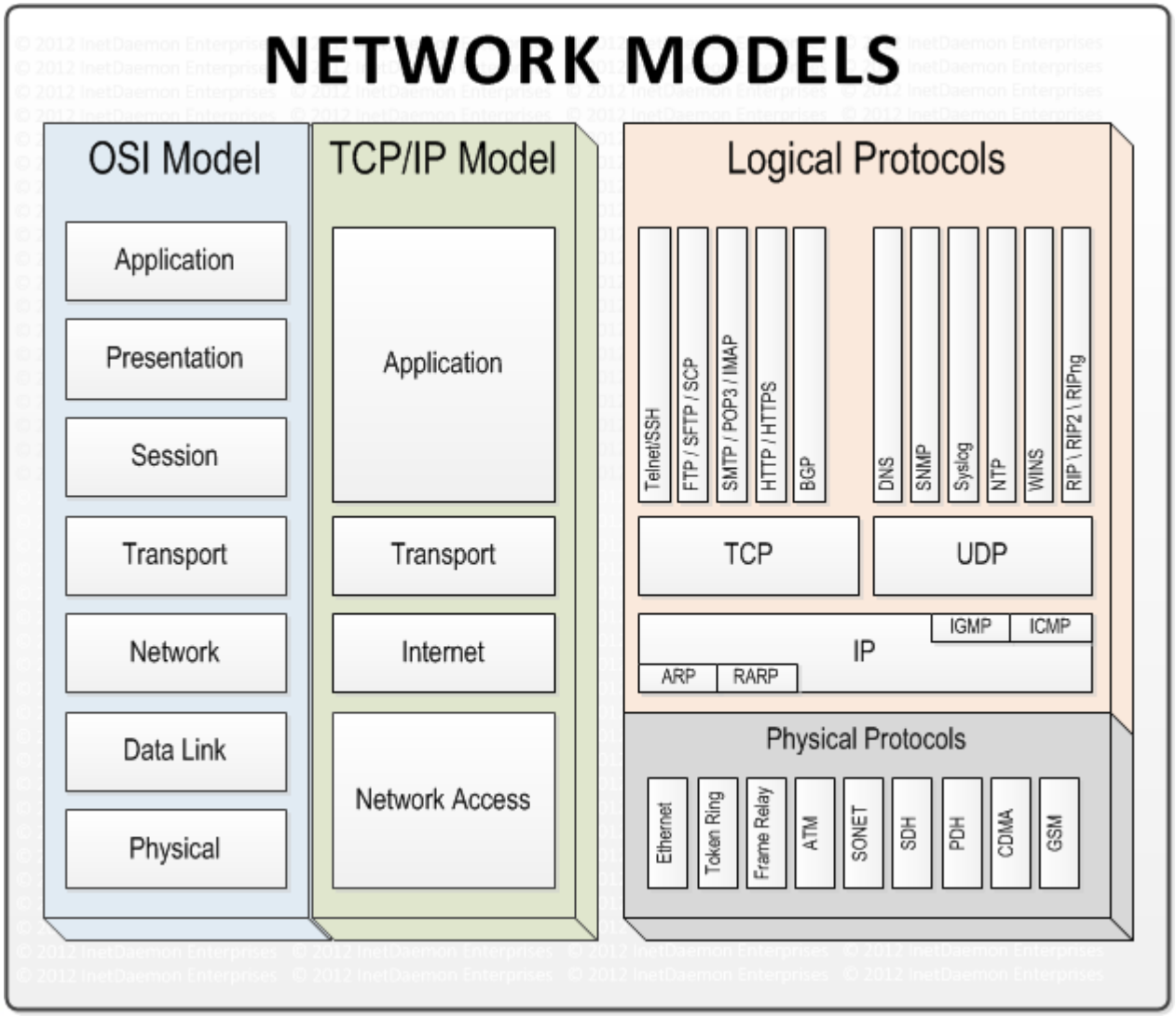
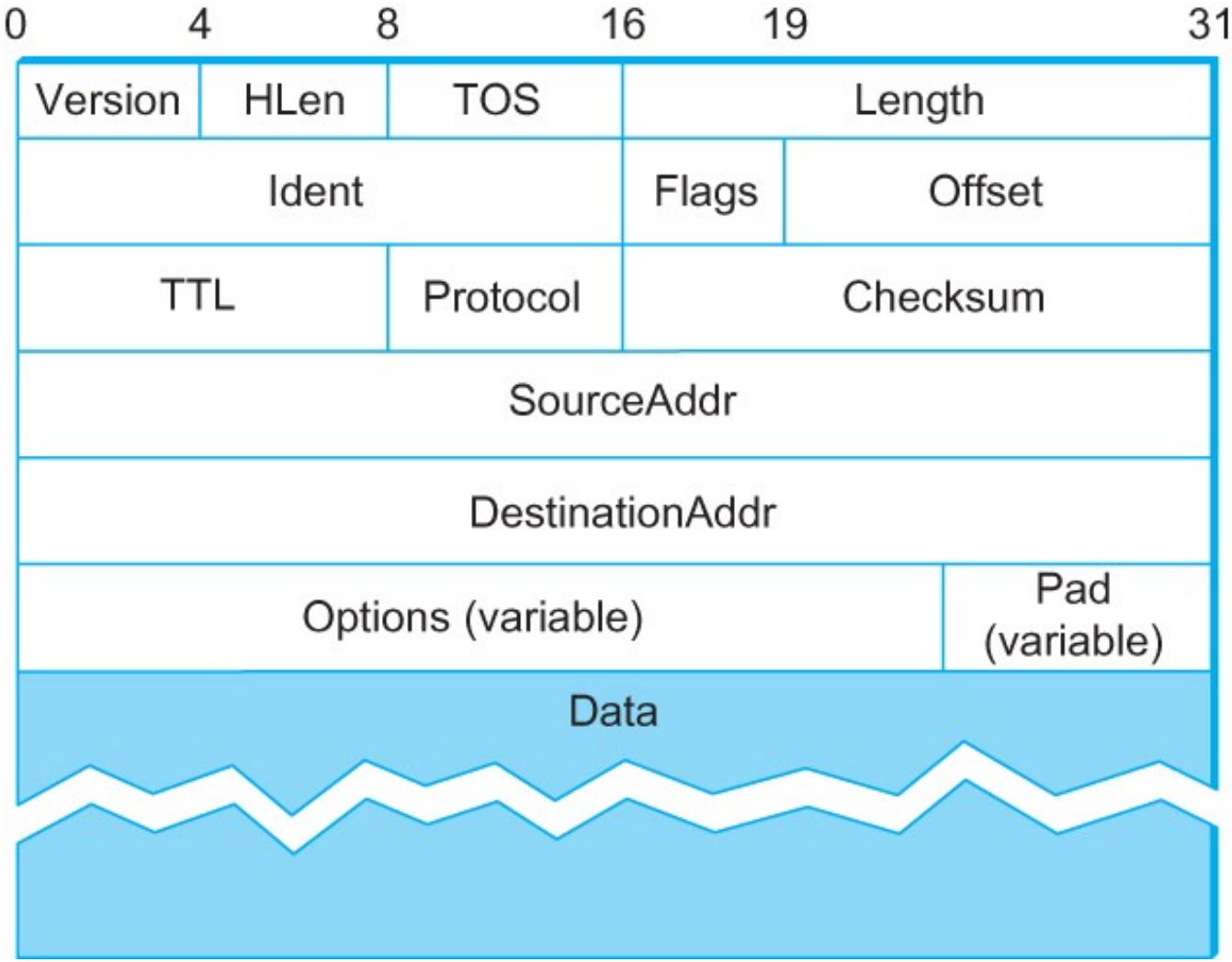
Unidad 5

Seguridad en Redes

Stack TCP/IP


NETWORK MODELS
OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
TCP/IP Model
Application
Transport
Internet
Network Access
Logical Protocols
Telnet\SSH
FTP / SFTP / SCP
SMTP / POP3 / IMAP
HTTP / HTTPS
BGP
DNS
SNMP
Syslog
NTP
WINS
RIP \ RIP2 \ RIPng
TCP
UDP
IGMP
ICMP
IP
ARP
RARP
Physical Protocols
Ethernet
Token Ring
Frame Relay
ATM
SONET
SDH
PDH
CDMA
GSM

Datagrama IPv4



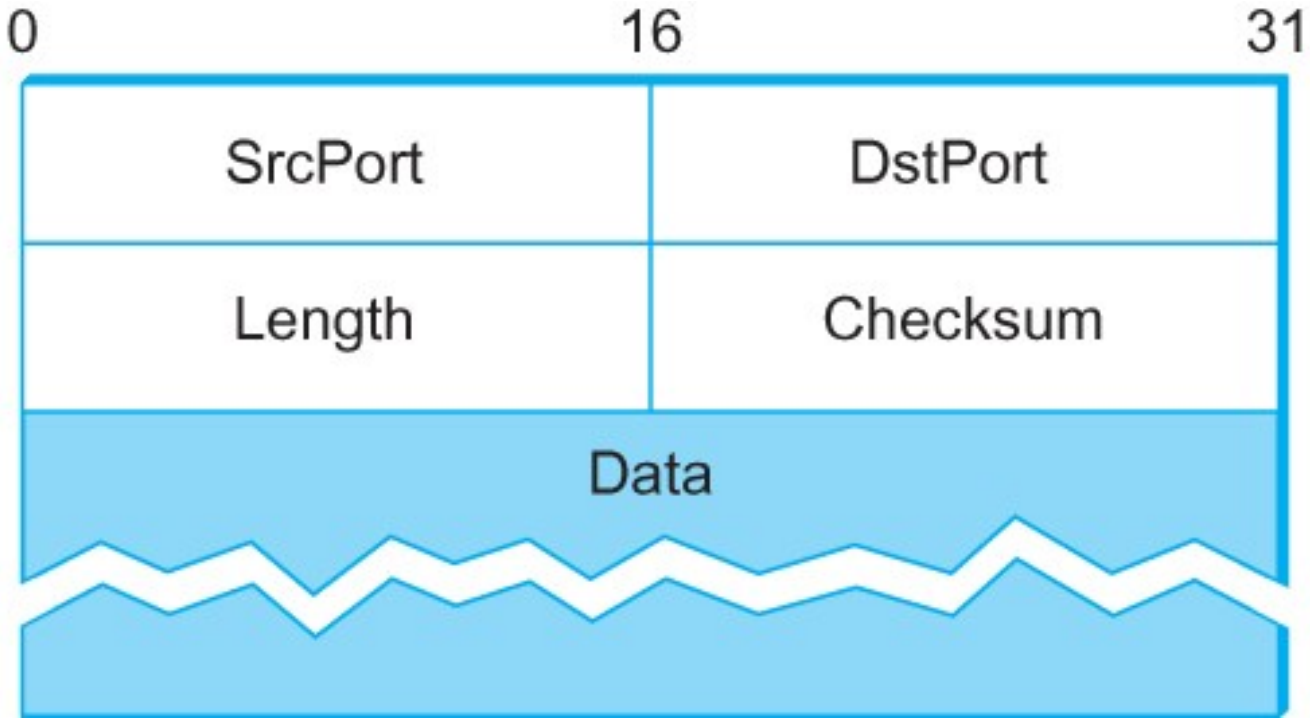
TCP , UDP, ICMP

- **TCP: Transmission Control Protocol.** Protocolo orientado a la conexión. Provee control de flujo, recuperación de errores y confiabilidad.

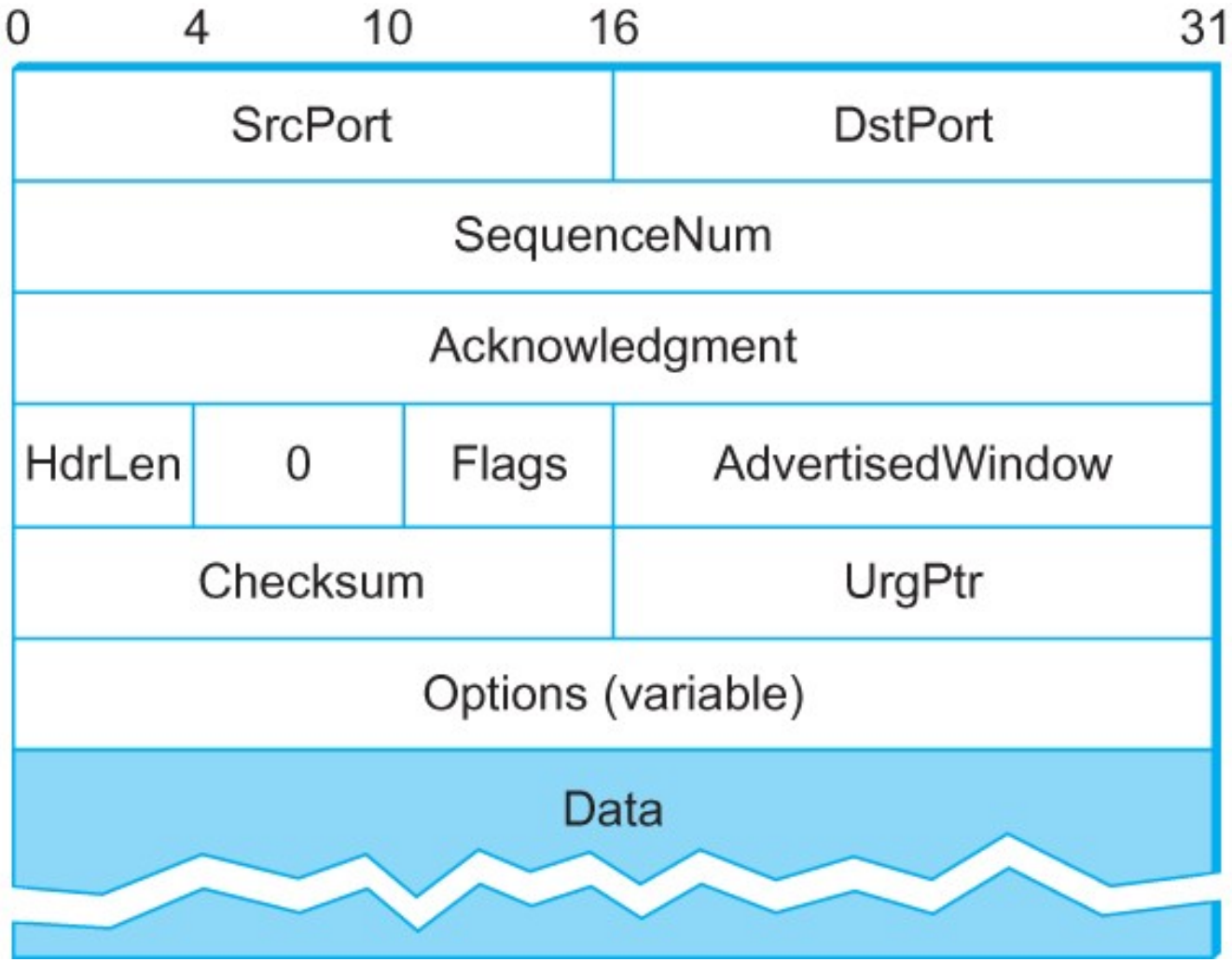
- **UDP: User Datagram Protocol.** Muy sencillo, no provee garantías. La recuperación de errores es responsabilidad de la aplicación.

- **ICMP: Internet Control Message Protocol.** Es usado para mensajes de control, mensajes de error, etc. El Ping utiliza ICMP. Algunos tipos de ICMP: Echo request, Echo Reply, Destination Unreachable, Time Exceeded, Timestamp, Timestamp Reply, Redirect Message, etc.

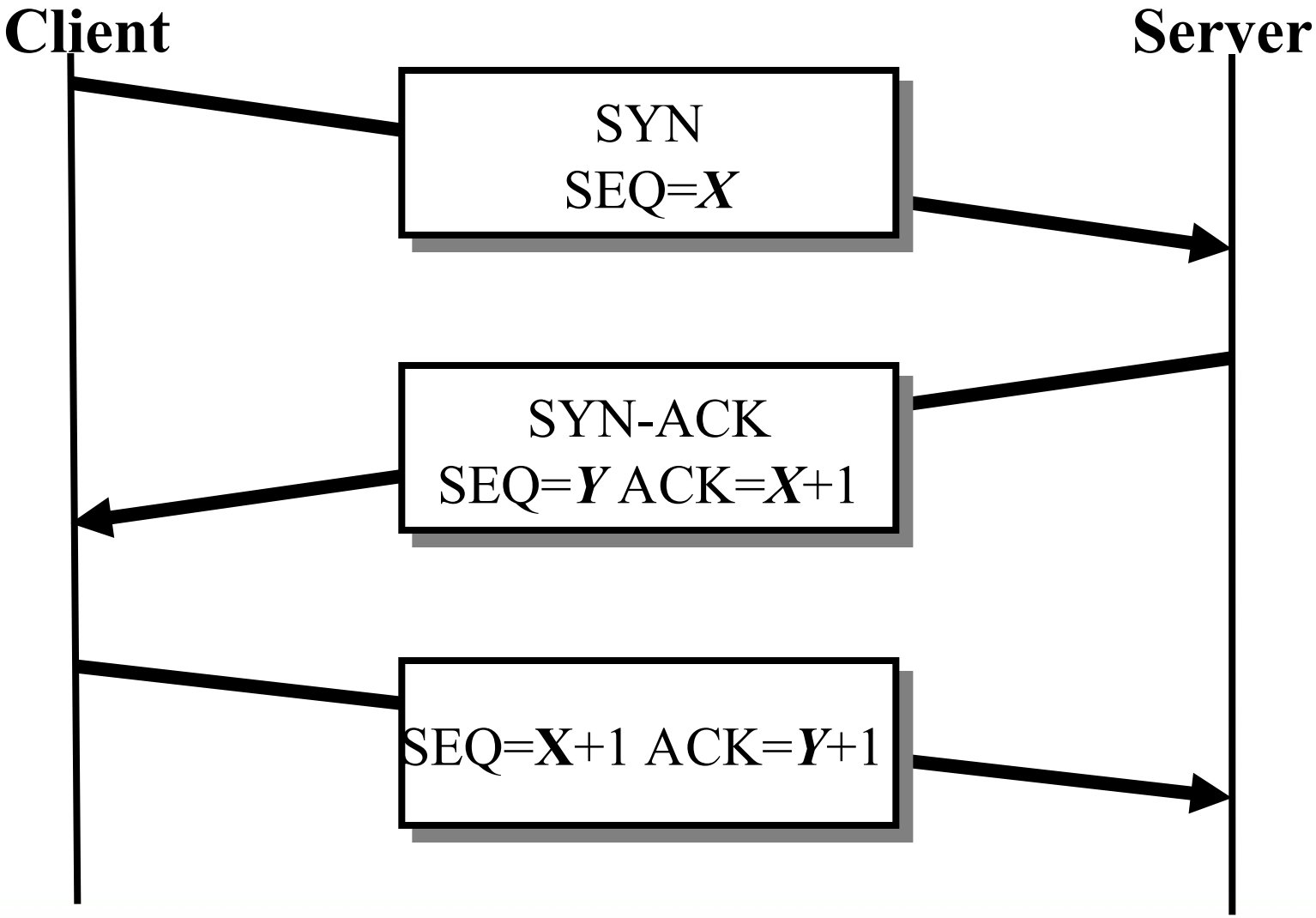
Paquete UDP



Paquete TCP


0
4
10
16
31
SrcPort
DstPort
SequenceNum
Acknowledgment
HdrLen
0
Flags
AdvertisedWindow
Checksum
UrgPtr
Options (variable)
Data

Three-way handshake

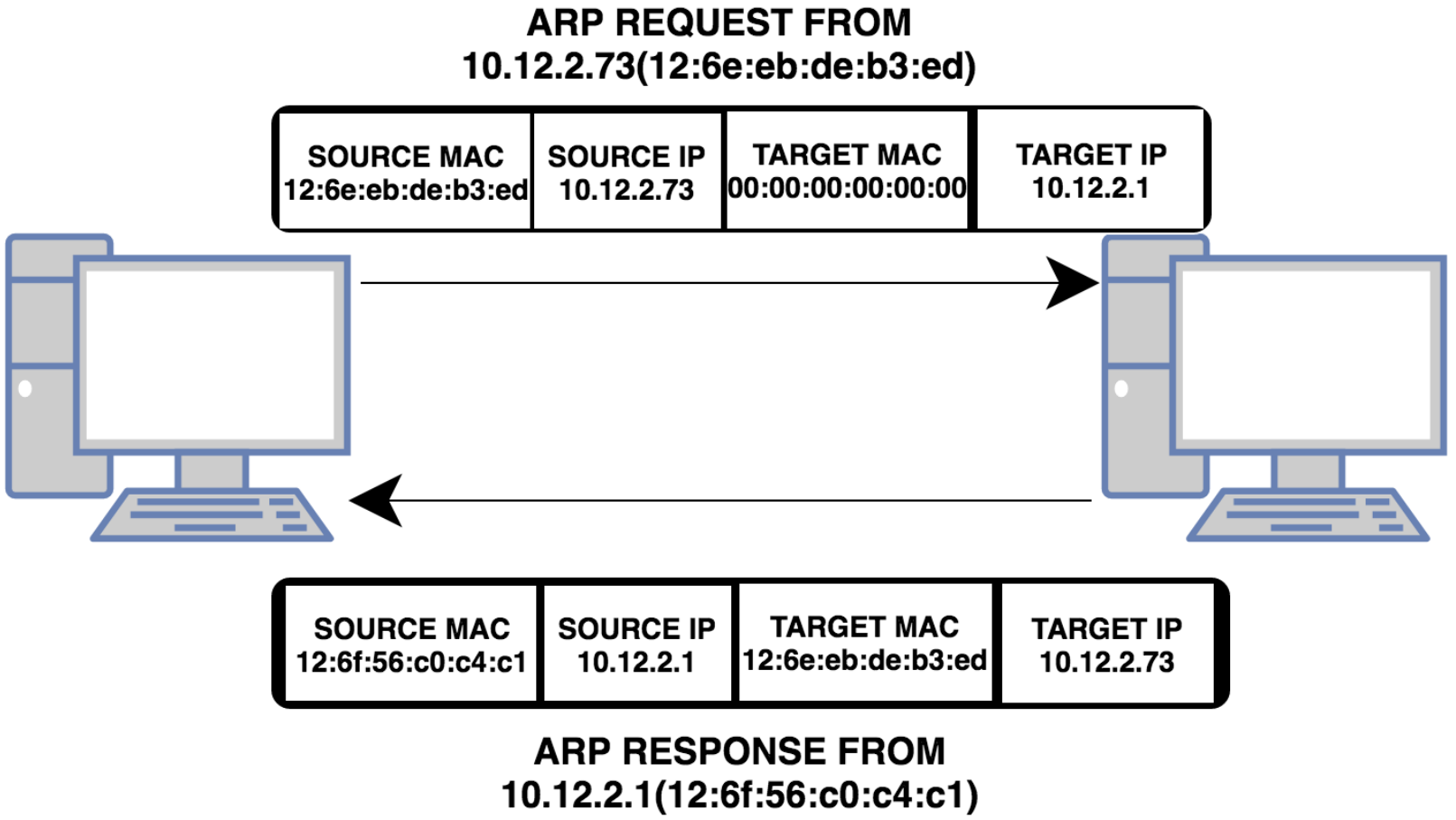


Address Resolution Protocol (RFC 826)

Protocolo responsable de encontrar la dirección de hardware (MAC) que corresponde a una determinada dirección IP.

Cada equipo tiene una tabla ARP en la que guarda un cache temporal de los resultados obtenidos.

ARP


ARP REQUEST FROM
10.12.2.73(12:6e:eb:de:b3:ed)
SOURCE MAC
12:6e:eb:de:b3:ed
SOURCE IP
10.12.2.73
TARGET MAC
00:00:00:00:00:00
TARGET IP
10.12.2.1
SOURCE MAC
12:6f:56:c0:c4:c1
SOURCE IP
10.12.2.1
TARGET MAC
12:6e:eb:de:b3:ed
TARGET IP
10.12.2.73
ARP RESPONSE FROM
10.12.2.1(12:6f:56:c0:c4:c1)

Sniffers

Los Sniffers (husmeadores) de paquetes son programas de software o hardware que pueden “ver” y registrar el tráfico que pasa sobre una red digital. Mientras el flujo de datos viaja por la red, el sniffer captura cada paquete y opcionalmente lo decodifica y lo analiza en base a reglas, estandares y especificaciones.

Dependiendo de la infraestructura de comunicaciones, uno puede sniffear todo o sólo una parte del tráfico de red desde un sólo equipo dentro de esa red.

Se dice que opera en “modo promiscuo” porque escucha todo lo que pasa por el medio, y no sólo lo que está destinado al equipo adonde se ejecuta la herramienta.

Pueden ser usados para:

- Analizar problemas en la red.
- Detectar intentos de intrusión a través de la red.
- Obtener información para luego hacer una intrusión.
- Monitorear el uso de la red.
- Reportar estadísticas de la red.
- Espiar a otros usuarios de la red y obtener información sensible como passwords.
- Hacer ingenieria reversa de protocolos usados en la red.

- Ejemplos: Tcpdump, wireshark (ethereal), ngrep, dsniff, Kismet (wireless)

Ejemplo: Establecimiento de la conexión

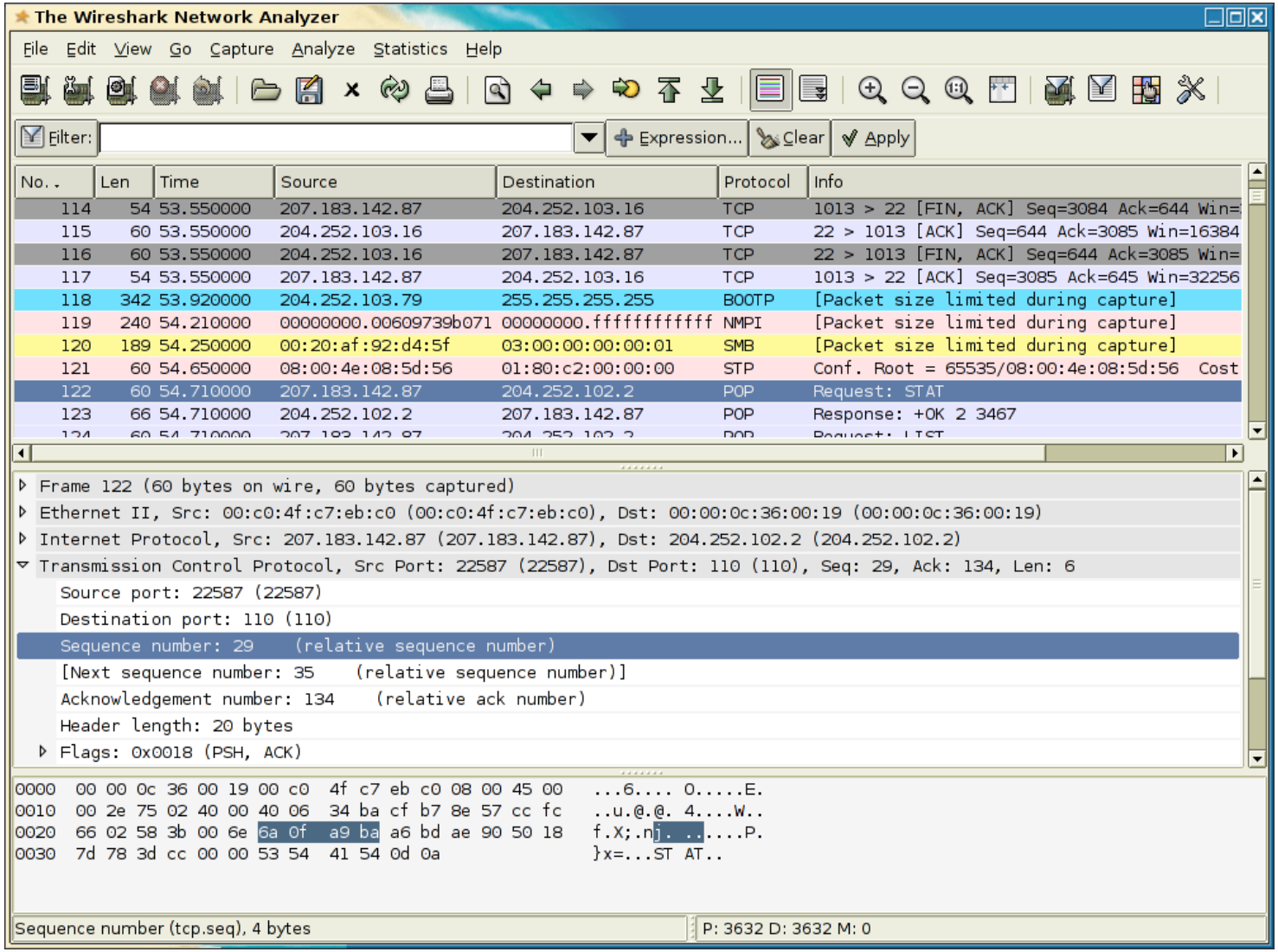
 # tcpdump -n -i eth0 -S port 9 (servicio discard)

16:38:21.644505 IP 192.168.0.1.1912 > 192.168.0.99.9: S 3617094593:3617094593(0) **win 65535 <mss 1460,nop,nop,sackOK>**

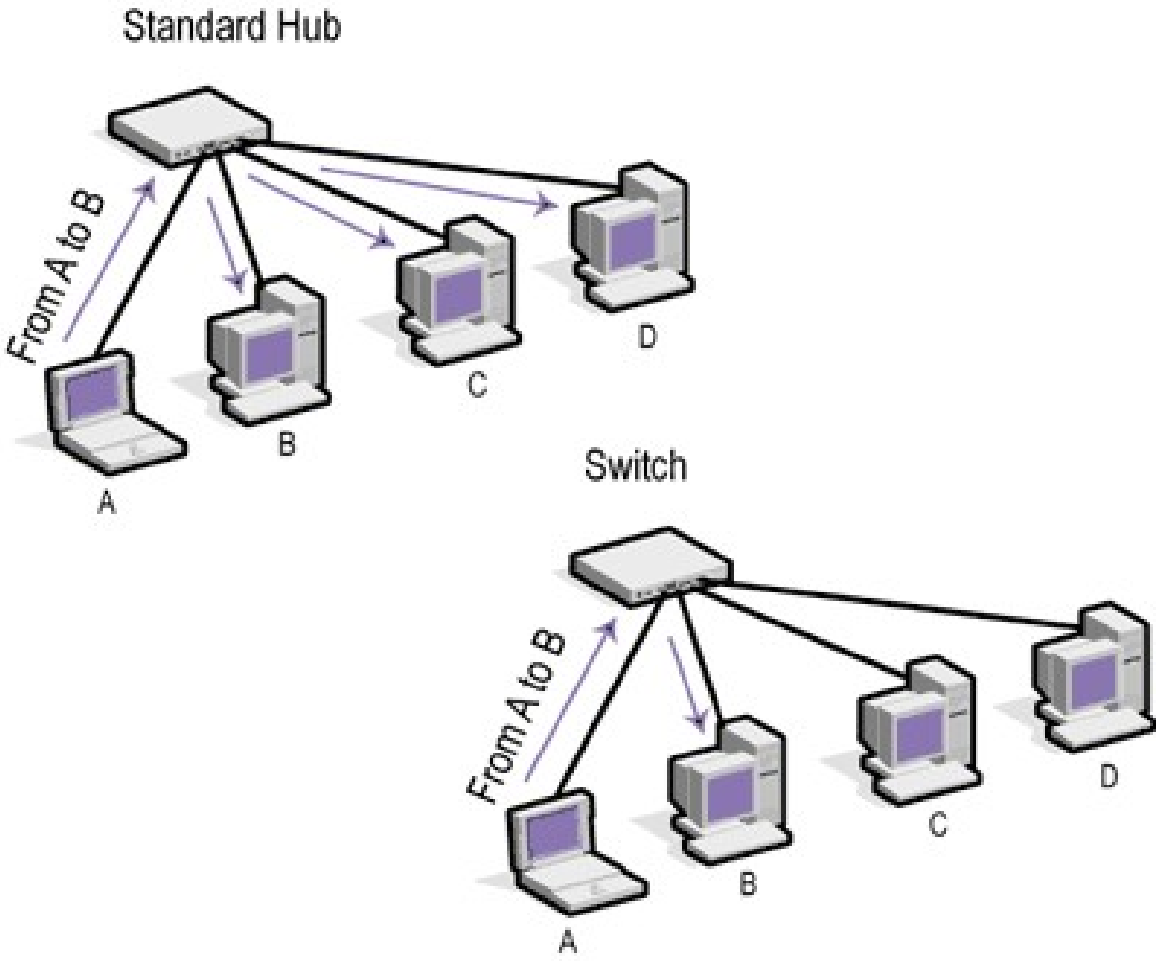
16:38:21.644603 IP 192.168.0.99.9 > 192.168.0.1.1912: S 3448904776:3448904776(0) ack 3617094594 **win 5840 <mss 1460>**

16:38:21.644720 IP 192.168.0.1.1912 > 192.168.0.99.9: . ack 3448904777 **win 65535**

Wireshark

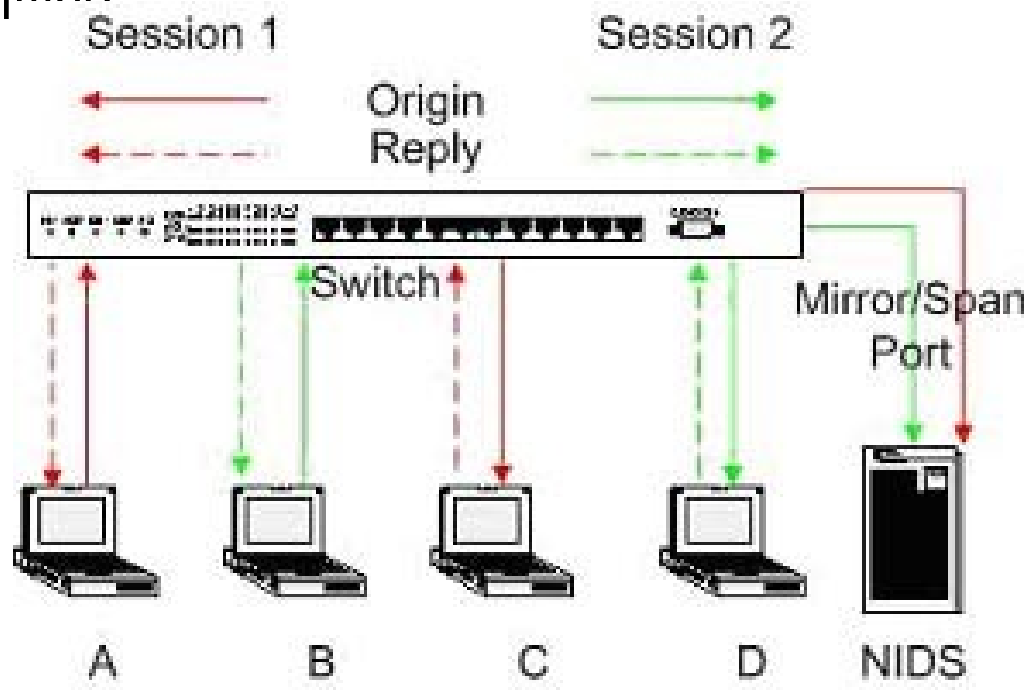

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Len Time Source Destination Protocol Info
114 54 53.550000 207.183.142.87 204.252.103.16 TCP 1013 > 22 [FIN, ACK] Seq=3084 Ack=644 Win=
115 60 53.550000 204.252.103.16 207.183.142.87 TCP 22 > 1013 [ACK] Seq=644 Ack=3085 Win=16384
116 60 53.550000 204.252.103.16 207.183.142.87 TCP 22 > 1013 [FIN, ACK] Seq=644 Ack=3085 Win=
117 54 53.550000 207.183.142.87 204.252.103.16 TCP 1013 > 22 [ACK] Seq=3085 Ack=645 Win=32256
118 342 53.920000 204.252.103.79 255.255.255.255 BOOTP [Packet size limited during capture]
119 240 54.210000 00000000.00609739b071 00000000.ffffffffffff NMPI [Packet size limited during capture]
120 189 54.250000 00:20:af:92:d4:5f 03:00:00:00:00:01 SMB [Packet size limited during capture]
121 60 54.650000 08:00:4e:08:5d:56 01:80:c2:00:00:00 STP Conf. Root = 65535/08:00:4e:08:5d:56 Cost
122 60 54.710000 207.183.142.87 204.252.102.2 POP Request: STAT
123 66 54.710000 204.252.102.2 207.183.142.87 POP Response: +OK 2 3467
Frame 122 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:c0:4f:c7:eb:c0 (00:c0:4f:c7:eb:c0), Dst: 00:00:0c:36:00:19 (00:00:0c:36:00:19)
Internet Protocol, Src: 207.183.142.87 (207.183.142.87), Dst: 204.252.102.2 (204.252.102.2)
Transmission Control Protocol, Src Port: 22587 (22587), Dst Port: 110 (110), Seq: 29, Ack: 134, Len: 6
Source port: 22587 (22587)
Destination port: 110 (110)
Sequence number: 29 (relative sequence number)
[Next sequence number: 35 (relative sequence number)]
Acknowledgement number: 134 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
0000 00 00 0c 36 00 19 00 c0 4f c7 eb c0 08 00 45 00 ...6.... O.....E.
0010 00 2e 75 02 40 00 40 06 34 ba cf b7 8e 57 cc fc ..u.@.@. 4....W..
0020 66 02 58 3b 00 6e 6a 0f a9 ba a6 bd ae 90 50 18 f.X;.nj. ......P.
0030 7d 78 3d cc 00 00 53 54 41 54 0d 0a }x=...ST AT..
Sequence number (tcp.seq), 4 bytes
P: 3632 D: 3632 M: 0

Hub vs Switch



Monitoreo de redes switcheadas

•La mayoría de los switch que tienen funcionalidades de administración, pueden definir un puerto de monitoreo (port mirroring o switch port analyzer (span)). En este puerto se copia todo el tráfico de y hacia uno o varios puertos para que pueda ser monitoreado mediante sniffing

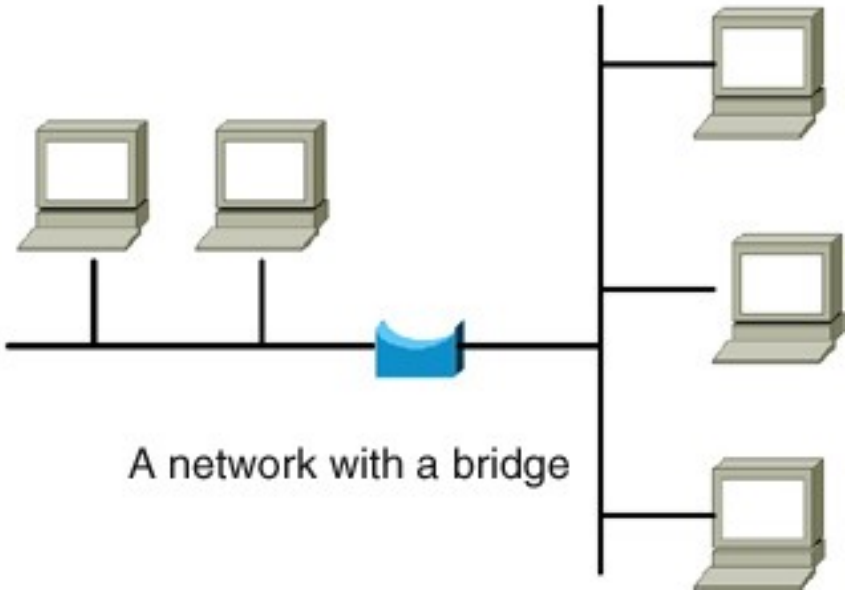


Network Tap

•Dispositivos de hardware que se insertan en un segmento de red y envían copia del tráfico que pasa por ellos a una estación de monitoreo. Ejemplo:

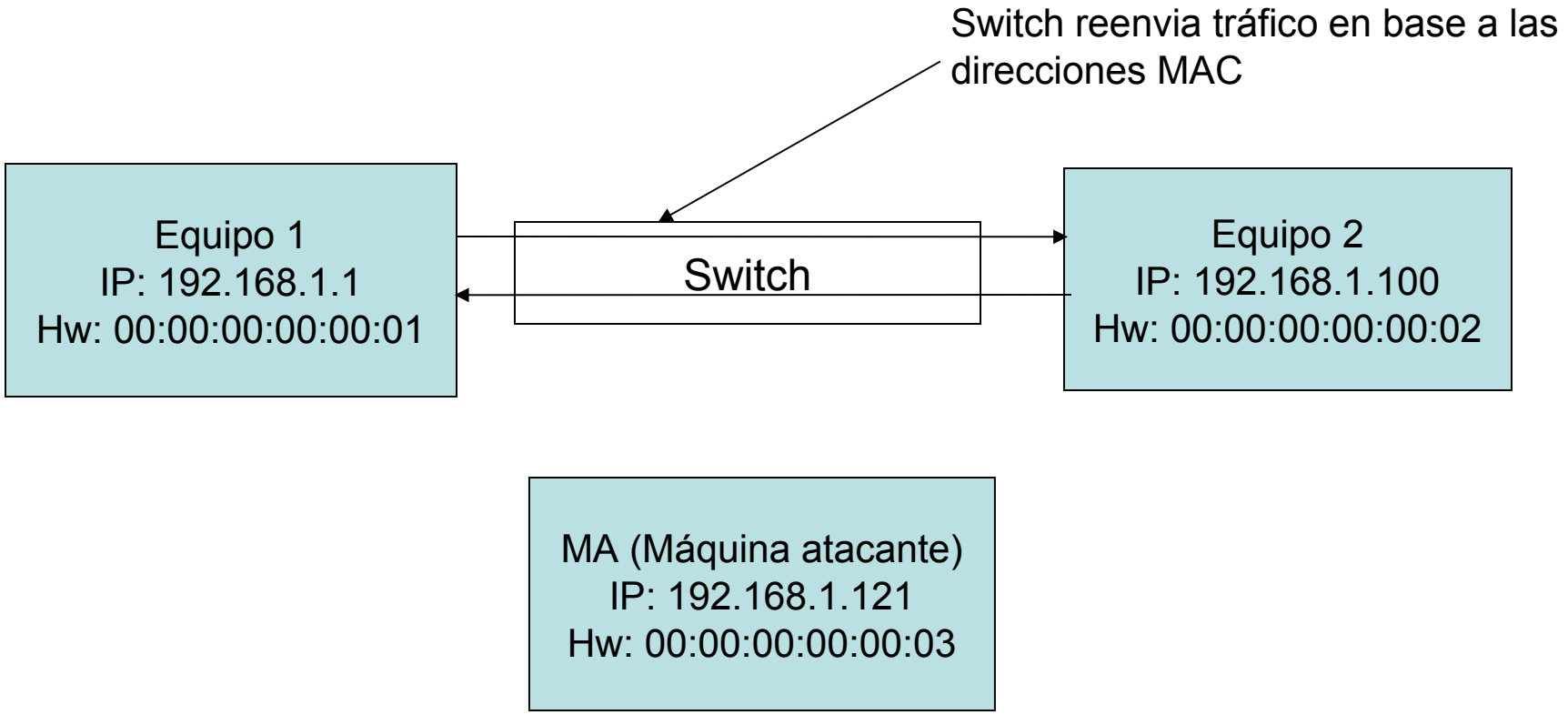
Dispositivos inline

- **Se puede utilizar una estación de trabajo con 2 placas de red (sin IP) para armar un bridge transparente. Se suele agregar una tercer placa con IP para acceder y administrar el equipo en forma remota.**



A network with a bridge

ARP Spoofing



Antes del ataque……..

ARP Spoofing

Antes del ataque, E1 y E2 se comunican entre ellos. Las tablas ARP de cada equipo son:

E1(192.168.1.1):

192.168.1.100	00:00:00:00:00:02
192.168.1.123	00:00:00:00:00:14

E2(192.168.1.100):

192.168.1.1	00:00:00:00:00:01
192.168.1.123	00:00:00:00:00:14

El switch trabaja a nivel de direcciones MAC y reenvia paquetes a la máquina correcta basandose en dicha dirección. ¿Qué pasa si manipulamos la tabla de ARP (también llamado ARP poisoning) en E1 y E2 para que la dirección MAC de destino en todos los paquetes que intercambian sea la dirección de la máquina atacante? Entonces, el switch reenvia los paquetes a dicha maquina atacante.

Después del ataque, la tabla queda así:

E1:

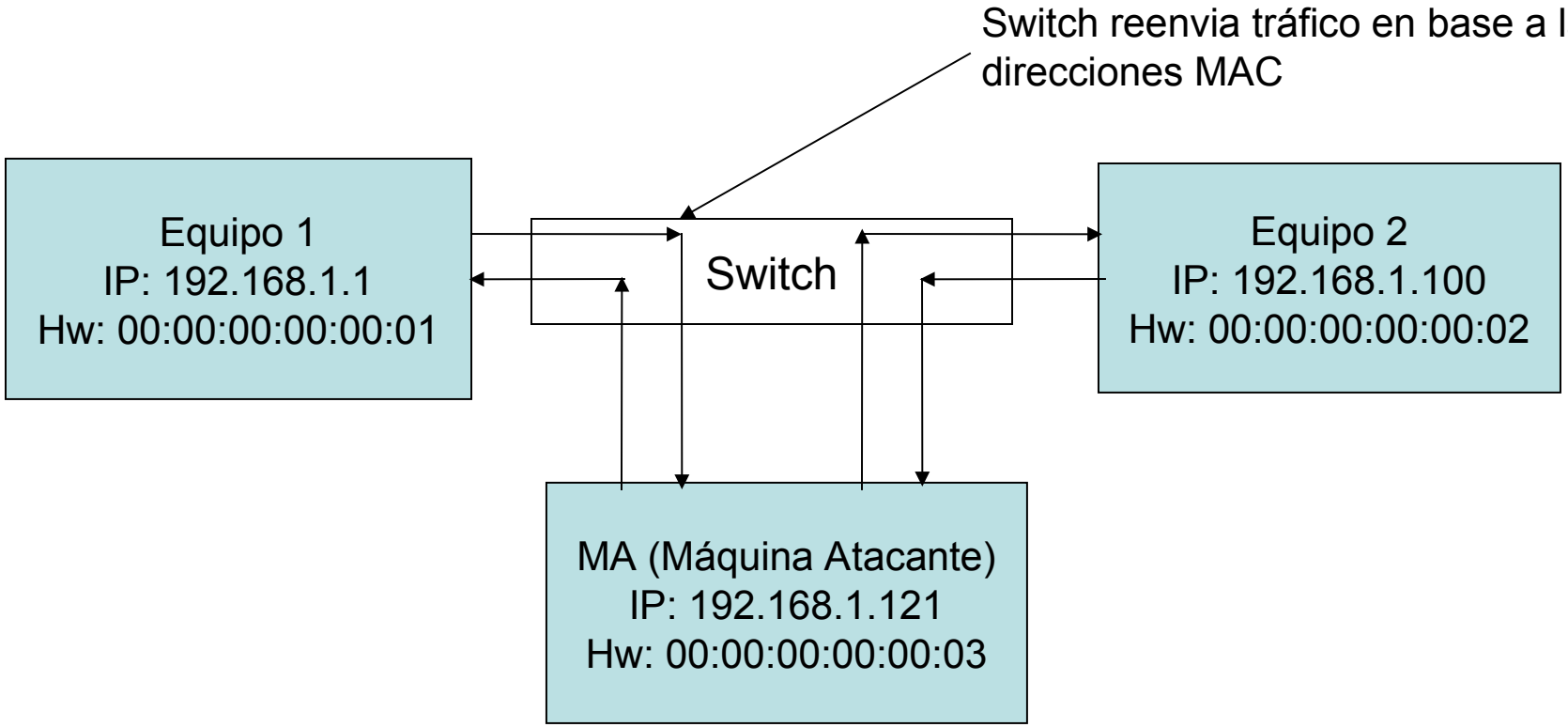
192.168.1.100	00:00:00:00:00:03
192.168.1.123	00:00:00:00:00:14

E2:

192.168.1.1	00:00:00:00:00:03
192.168.1.123	00:00:00:00:00:14

Donde 00:00:00:00:00:03 es la dirección MAC de la máquina atacante.

ARP Spoofing



Después del ataque……..

Nota: Hay que habilitar ip_forwarding en la máquina atacante o si no se romperá la comunicación entre las máquinas atacadas.

IP Spoofing

- **El host que recibe un paquete confía en que el remitente está diciendo la verdad con respecto a su dirección IP de origen.**

- **¿Por que querría mentir?**
  - Esconder el origen de un ataque
  - Secuestrar una sesión abierta.
  - Aprovecharse de aplicaciones que autentican basandose en la dirección IP de origen.
- **¿Cómo se hace?**
  - Se crean paquetes con IP de origen falsificada.

Ataques de Denegación de Servicio

- **Ataque TCP RST.**
- **Ataque ICMP contra TCP.**
- **Ataque de SYN Flooding.**

Estos ataques usan IP Spoofing.

Reset de Conexiones

- **Un host X envia un paquete RST reseteando la conexión cuando:**
  - Un host Y solicita una conexión a un puerto cerrado de X.
  - Por cualquier razón (sin uso por un cierto tiempo, condición anormal) desea cerrar la conexión.

- **El RESET es unilateral!**

Ataque TCP RST

- **Enviar un paquete RST (TCP RESET flag) con la dirección IP origen "spoofeada" a cualquier extremo de la conexión.**

- **Debo conocer SRC_IP, SRC_PORT, DST_IP, DST_PORT, número de secuencia en ventana de uso:**

  - Se puede intentar "adivinar" los parámetros desconocidos.
  - O sniffear el tráfico y obtener todos los parámetros.

Ref: Ignoring the great firewall of China, Robert Clayton
https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

Ataques ICMP contra TCP

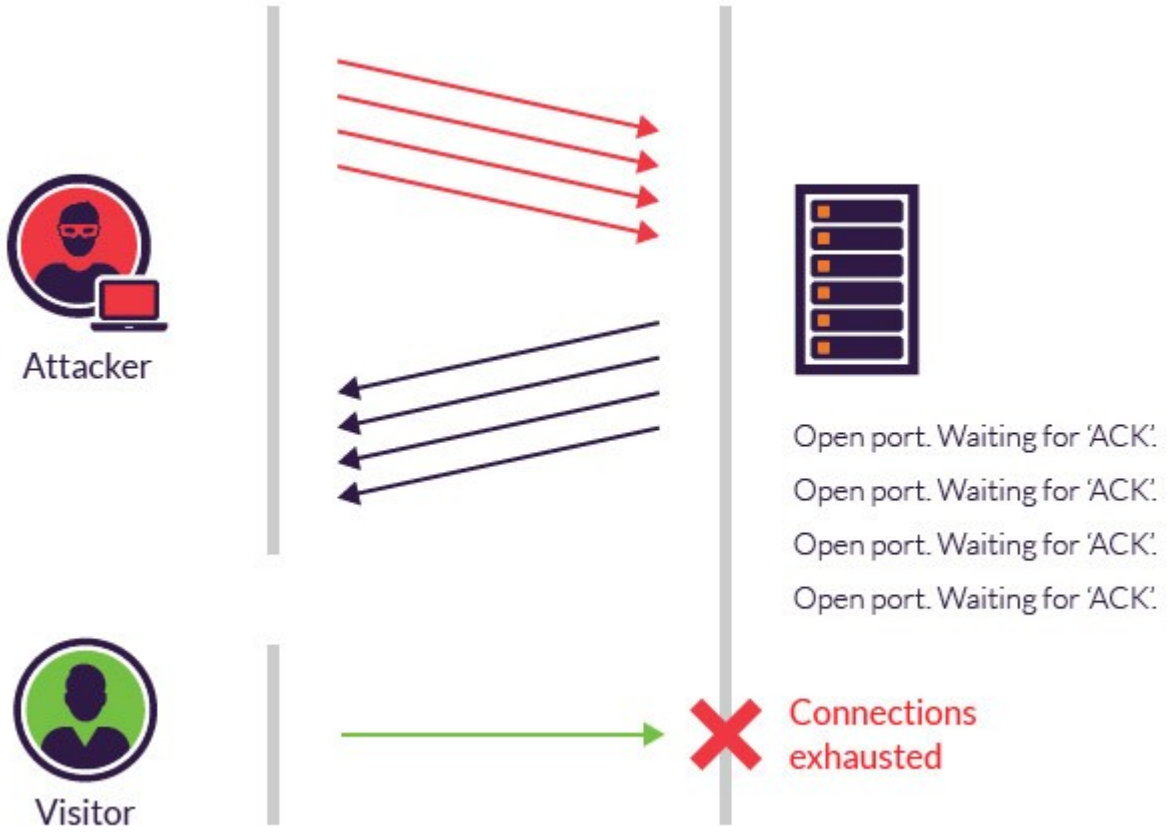
Existen variantes que utilizan ICMP para finalizar una conexión, sin necesidad de conocer los números de secuencia.

Tipos de mensajes involucrados:

- Protocol Unreachable.
- Port Unreachable.
- Fragmentation Needed and DF set.

Ref: "ICMP attacks against TCP", RFC5927

Ataque de Syn Flooding



Ref: "TCP SYN Flooding Attacks and Common Mitigations", RFC4987

Una solución: Syn cookies

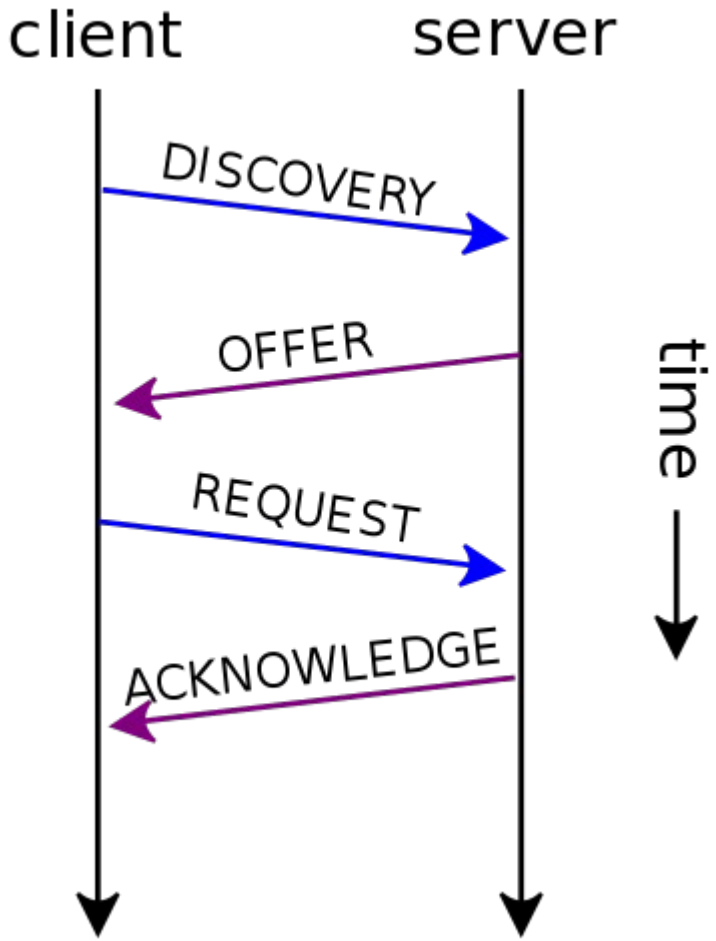
- **Las SYN cookies son elecciones particulares del número de secuencia inicial (ISN) por parte del servidor.**

- **Se almacena el estado en el ISN, no en el servidor.**

- **El ISN se elige utilizando un hash que incluye parte de la hora, un secreto del servidor y los datos de ip y puerto origen y destino.**

Ref: https://cr.yp.to/syncookies.html

DHCP - Dynamic Host Configuration Protocol



Protocolos de aplicación

- **Comandos r**
- **Ident**
- **Telnet y SSH**
- **Tftp**
- **Web**
- **Mail**
- **DNS**
- **SNMP**
- **NTP**
- **Autenticación en Windows**

Comandos r

- **Hace un tiempo, la gente quería acceder fácilmente a equipos remotos, sin tener que loguearse con usuario y clave.**

- **Surgen los comandos r**
  - rcp – Copia de archivos remotos (TCP/514)
  - rlogin – login remoto (TCP/513)
  - rsh - Shell remoto (TCP/514)
  - rwho – Usuarios logueados en el equipo remoto (UDP/513)

Autenticación

- **Los archivos /etc/hosts.equiv y .rhosts proveen el mecanismo de autenticación para rlogin, rsh y rcp**
- **Estos archivos especifican qué equipos remotos y usuarios son considerados "confiables"**
  - Los usuarios confiables pueden acceder al sistema local sin proveer una password.
  - El archivo /etc/hosts.equiv aplica a todo el sistema, mientras que cada usuario puede mantener su propio .rhost en su directorio home.

- **Estos mecanismos saltean los mecanismos standard basados en usuario-password.**

Identd (TCP/113)

- Definido en RFC 1413. También conocido como auth.
- Sirve para identificar el usuario remoto de una conexión TCP determinada.
- Cuando un usuario o programa en la computadora A hace un pedido ident a la computadora b, solo puede preguntar por la identidad de los usuarios de las conexiones entre A y B. El cliente especifica los números de puertos usados en ambos extremos, y el servidor B devuelve una cadena con el nombre del usuario.

Telnet (TCP/23)

- Permite login remoto.
- Todo el tráfico viaja en claro.
- Utiliza user y password para loguearse.
- Muy utilizado para administración de routers, switches, etc.
- Posibilidad de MitM, Session Hijack, etc

SSH (TCP/22)

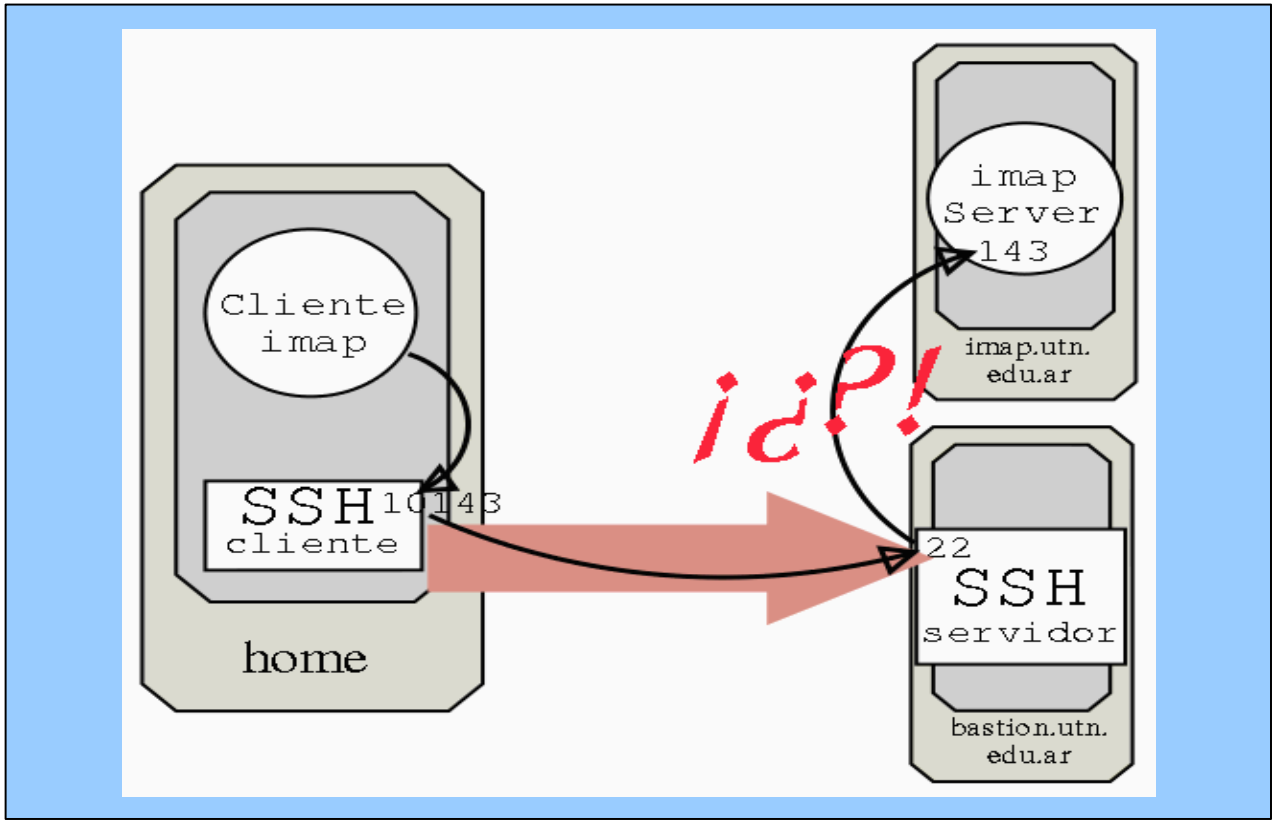
- Secure shell es un protocolo para comunicaciones seguras, permite login remoto, transferencia de archivos y tunneling de conexiones.
- SSH cifra todo el tráfico (incluidas las contraseñas) para eliminar de un modo efectivo las "escuchas", los secuestros de las conexiones y otros ataques a nivel de red.
- Además, puede utilizar mecanismos de pares de claves en vez de username/password.

De que tipo de cosas protege SSH

- Man-in-the-Middle (MitM) attack / Spoofing
- Session hijacking
- Sniffing
- Data modification

Túneles SSH - Local a otro servidor

```
home:~$> ssh -L 10143:imap.utn.edu.ar:143 bastion.utn.edu.ar
```



TFTP (UDP/69)

- Trivial FTP. Protocolo muy simple de transferencia de archivos.
- Usado para arrancar estaciones de trabajo sin disco rígido o transferir configuraciones de dispositivos de red como por ejemplo routers. Es usado por PXE (Preboot Execution Environment)
- No usa usuario ni clave
- Útil para copiar archivos en equipos comprometidos.

HTTP (TCP/80)

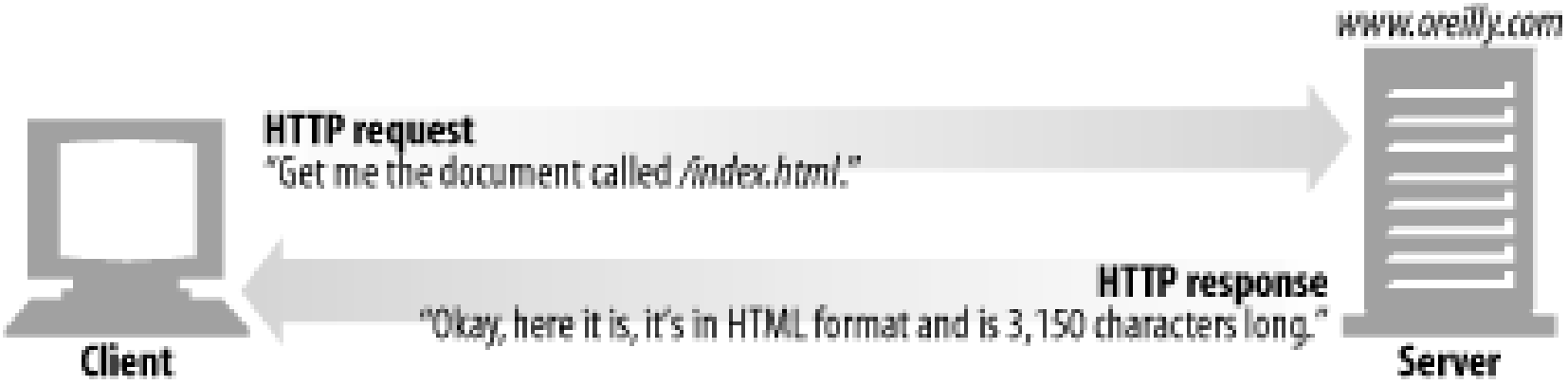
El HyperText Transfer Protocol es un protocolo de aplicación para sistemas de información hipermediales, distribuidos y colaborativos. Es el lenguaje que utilizan los clientes y servidores web para comunicarse entre sí. Es un protocolo simple, basado en texto, que no maneja estados. Esto significa que cada solicitud que el cliente envía al servidor es independiente de las solicitudes anteriores.

La versión HTTP/2 es un protocolo binario, donde los encabezados van comprimidos, permite multiplexar transmisiones en una misma conexión, etc.

Y se viene HTTP/3, basado en quick

https://daniel.haxx.se/http3-explained/

Protocolo cliente servidor



HTTP Request

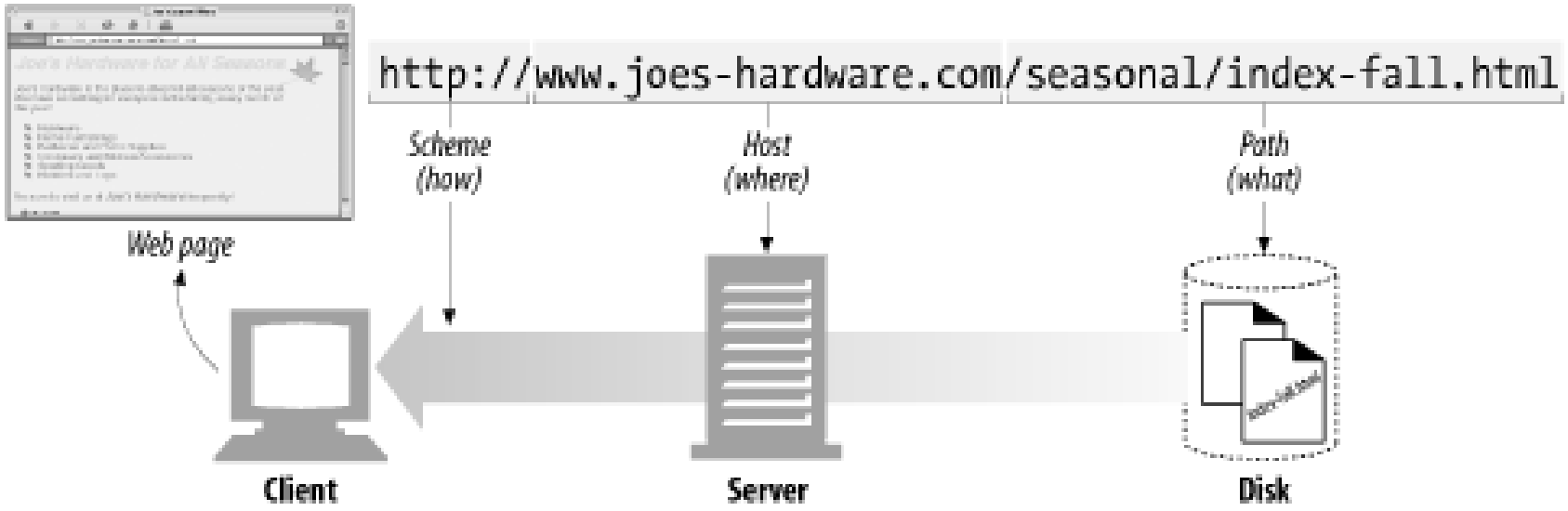
El protocolo HTTP es un protocolo de pedido/respuesta. Un cliente envía una solicitud a un servidor. En dicha solicitud incluye un método, URI y versión de http. Luego incluye una serie de encabezados y modificadores. Opcionalmente, puede incluir un cuerpo adicional con contenidos.

URI y URL

Las URIs proveen una forma de localizar un recurso en internet.

Diferencia: URI es un concepto genérico, URL es un concepto informal (no se usa más en las especificaciones técnicas) asociado con algunos esquemas populares como HTTP, FTP, MAILTO, etc.

Ejemplo URL


http://www.joes-hardware.com/seasonal/index-fall.html
Scheme
(how)
Host
(where)
Path
(what)
Web page
Client
Server
Disk

Métodos HTTP

- GET - Solicita la entidad identificada por el URI incluido en el pedido.
- HEAD - De funcionalidad similar al GET, pero el servidor debe devolver solo los headers, y no el contenido.
- POST - Para que el servidor destino reciba la entidad incluida en el request, subordinada al URI indicado.
- PUT - Para que el servidor almacene en el URI indicado, la entidad incluida en la solicitud.
- OPTIONS - Solicita información acerca de los mecanismos de comunicación disponibles, métodos habilitados, etc.
- DELETE - Para borrar del servidor el URI indicado.
- TRACE - Para que el servidor responda con la solicitud, tal cual la recibió. Se utiliza para debugging.

HTTP Request


```
GET http://www.ejemplo.edu.ar HTTP/1.1
Host: www.ejemplo.edu.ar
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1;
   en-US; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;
   q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Content-length: 0
```

HTTP Response

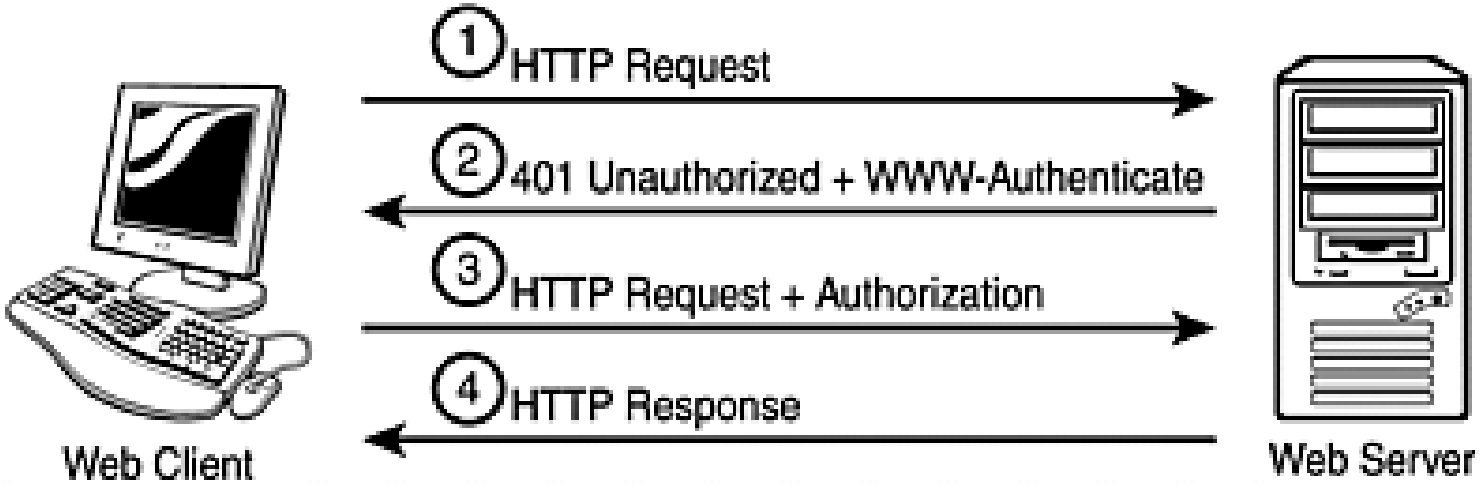

```
HTTP/1.1 200 OK
Date: Tue, 16 Sep 2008 20:53:07 GMT
Server: Apache/1.3.32 (Unix) PHP/5.2.4 Chili!Soft-ASP/3.6.2
    mod_ssl/2.8.21 OpenSSL/0.9.7
Last-Modified: Fri, 22 Sep 2006 15:54:45 GMT
ETag: "b1c03a-523c-45140745"
Accept-Ranges: bytes
Content-Length: 21052
Content-Type: text/html

<HTML><HEAD><TITLE>Web interno de la universidad</TITLE>
<BODY bgcolor="#CCCC66">
<p><img src="arcert.jpg" width="400" height="40"> </p>
<font face="Verdana, Arial, Helvetica, sans-serif">

<p><b>Web Interno de la universidad</b></p>
```

HTTP Basic Auth

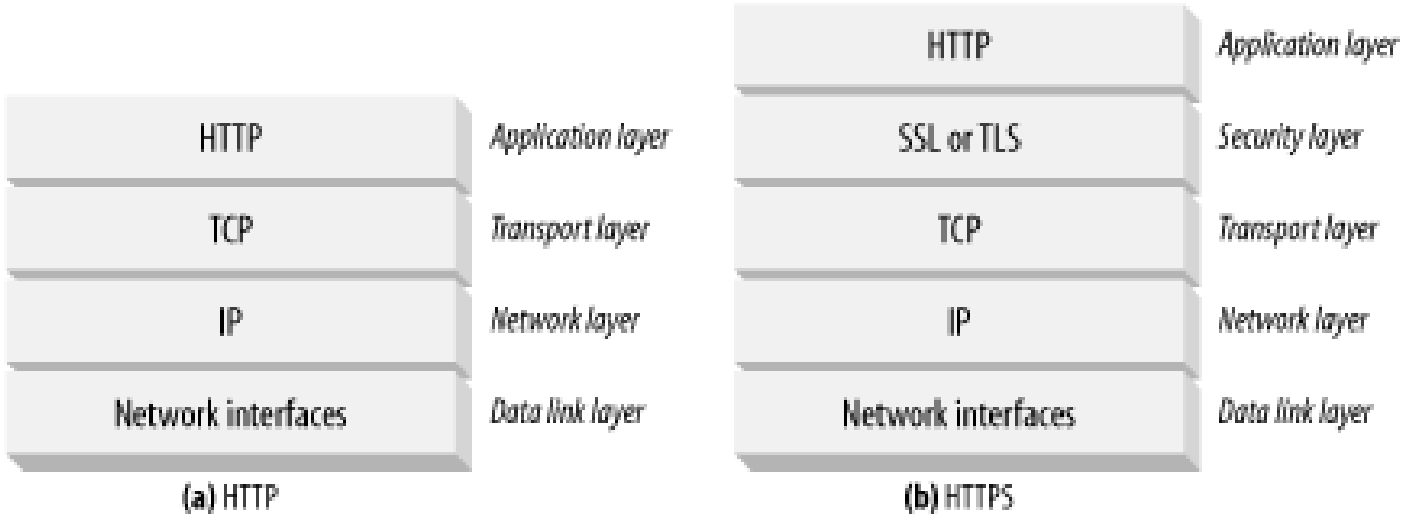
Mecanismo de autenticación Definido en RFC 2617



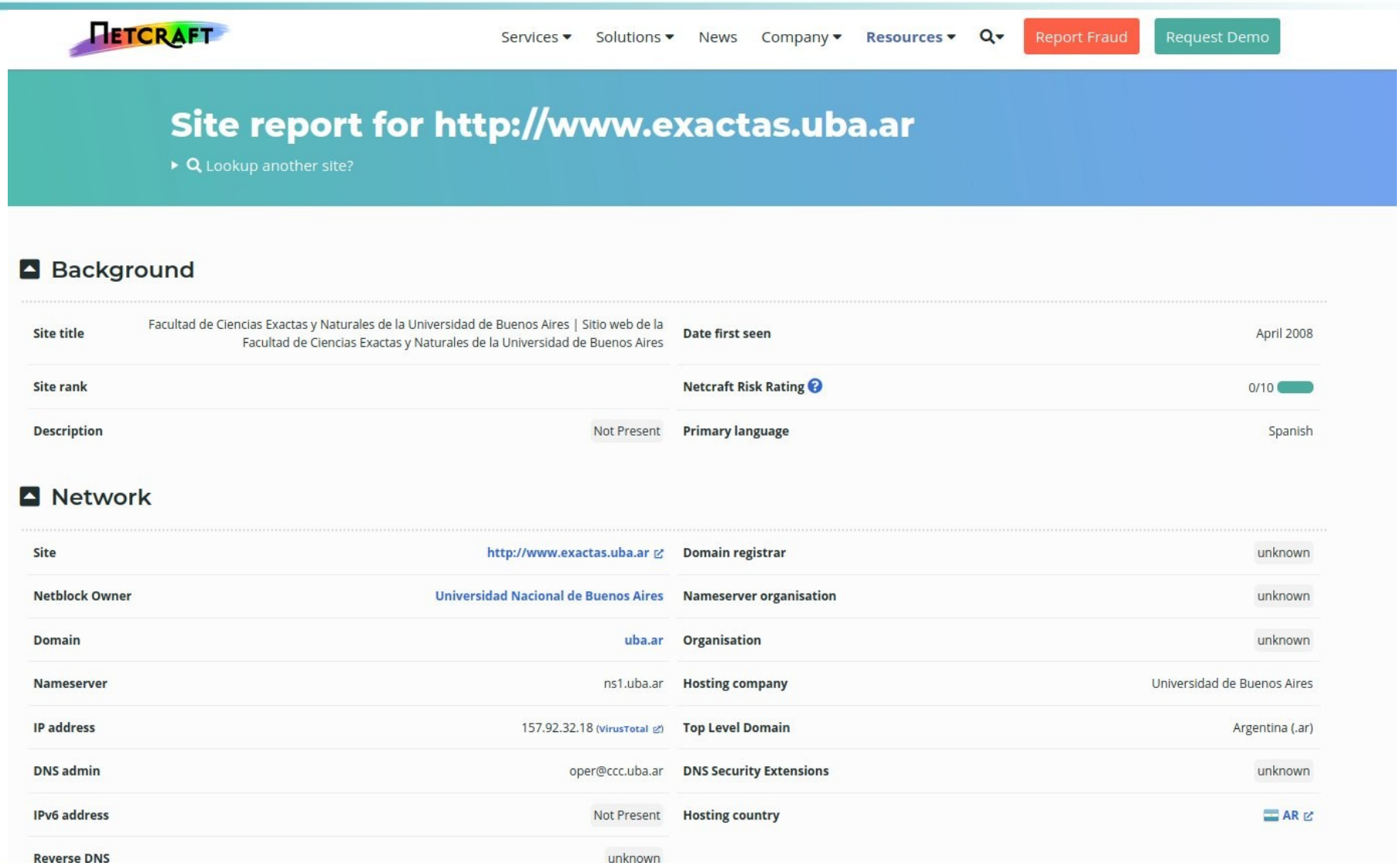
HTTPS

HTTP + TLS

Comunicación con canal encriptado utilizando TLS. Bien implementado, no permite el robo de información en tránsito. Además, permite identificar fehacientemente al servidor y, en algunos casos, al cliente. Port 443/TCP



Netcraft – www.exactas.uba.ar



Correo Electrónico

- **Protocolos**
  - SMTP (TCP/25), POP3 (TCP/110), IMAP4(TCP/143)
- **Se pueden usar sobre SSL: 465, 995, 993**
- **Exchange, Postfix, Exim, Sendmail, Qmail**

Ejemplo Correo Electrónico

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Return-Path: <xxx@xxx.com.ar>

Delivered-To: rbaader@ejemplo.edu.ar

Received: from unknown (HELO me) (200.x.x.x)

by mail.ejemplo.edu.ar with SMTP; 29 Oct 2004 14:00:16 -0000

Received: from ecosport.xxx.com.ar ([127.0.0.1])

by localhost (chatarra [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 28182-02 for <rbaader@ejemplo.edu.ar>

Received: from of123c (of123_1-T_rbaader.xxx.com.ar [10.1.1.51])

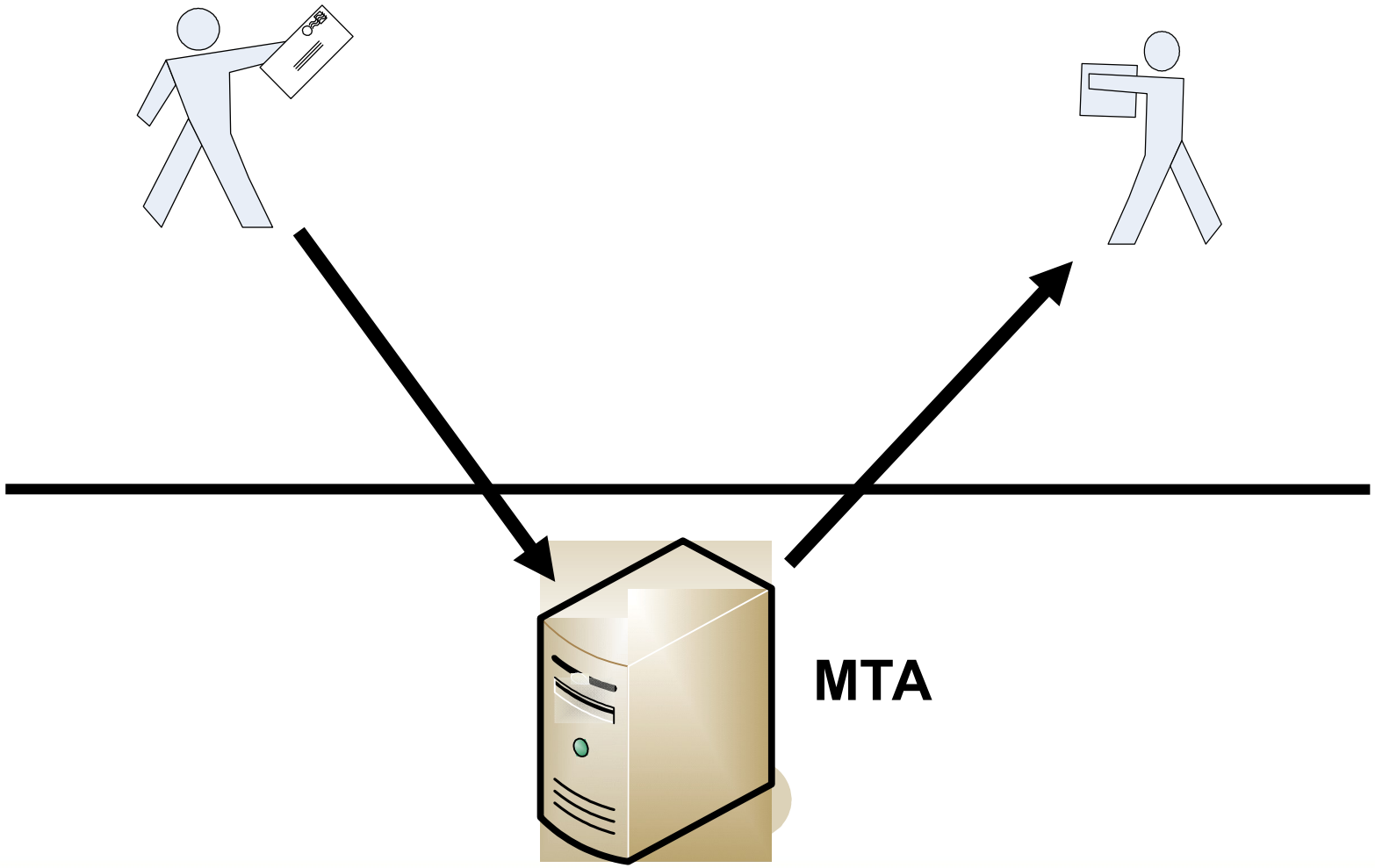
by chatarra.xxx.com.ar (Postfix) with SMTP id C2AA5204F6A for <rbaader@ejemplo.edu.ar>

From: "Fernando X" <xxx@xxx.com.ar>

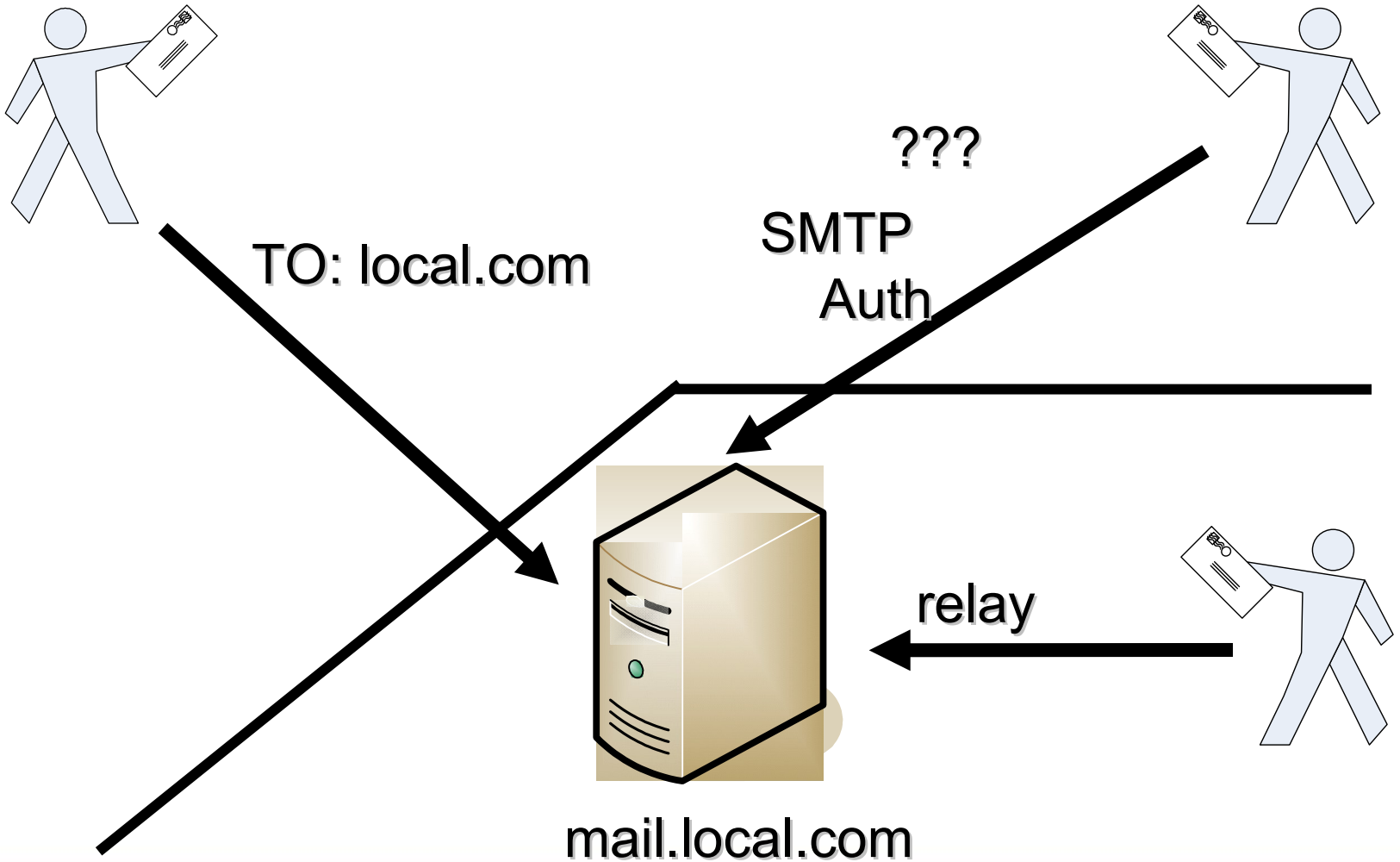
To: “Rodolfo Baader" <rbaader@ejemplo.edu.ar>

Subject: Re: Un favor!

Problema: Open Relay



Open Relay



SMTP-AUTH (RFC 2554)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

```
220-mail.xxxxxxxx.com ESMTP Exim 4.34 #1 Wed, 23 Jun 2004
    17:35:13 -0700
EHLO mail.myserver.com
250-mail.xxxxxxxx.com Hello mail.myserver.com [192.168.0.156]
250-SIZE 52428800
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
bXl1c2VybmFtZQ==
334 UGFzc3dvcmQ6
bXlwYXNzd29yZA==
235 Authentication succeeded
```

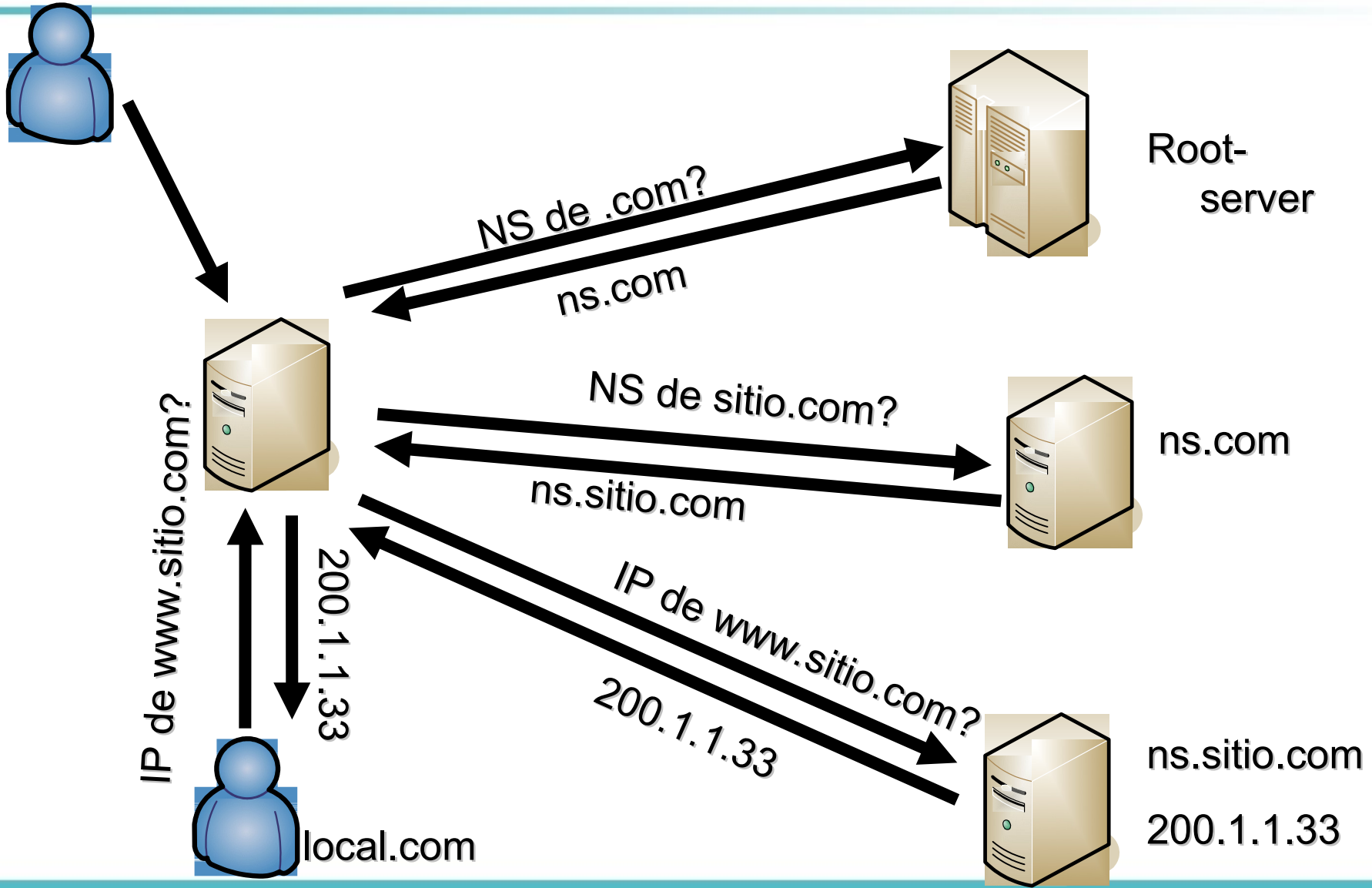
SMTP-AUTH CRAM-MD5

S: 220 smtp.example.com ESMTP server ready
C: EHLO jgm.example.com
S: 250-smtp.example.com
S: 250 AUTH CRAM-MD5 DIGEST-MD5
C: AUTH FOOBAR
S: 504 Unrecognized authentication type.
C: AUTH CRAM-MD5
S: 334
PENCeUxFREJoU0NnbmhNWitOMjNGNndAZWx3b29kL
mlubm9zb2Z0LmNvbT4=
C: h
S: 235 Authentication successful.

DNS (UDP/53, TCP/53)

- **Domain Name System**
- **Esquema jerárquico de resolución de nombres.**
- **Servidores primarios y secundarios, comunicación entre ellos.**

DNS


Root-server
NS de .com?
ns.com
NS de sitio.com?
ns.sitio.com
ns.com
IP de www.sitio.com?
200.1.1.33
IP de www.sitio.com?
200.1.1.33
ns.sitio.com
200.1.1.33
local.com

DNS

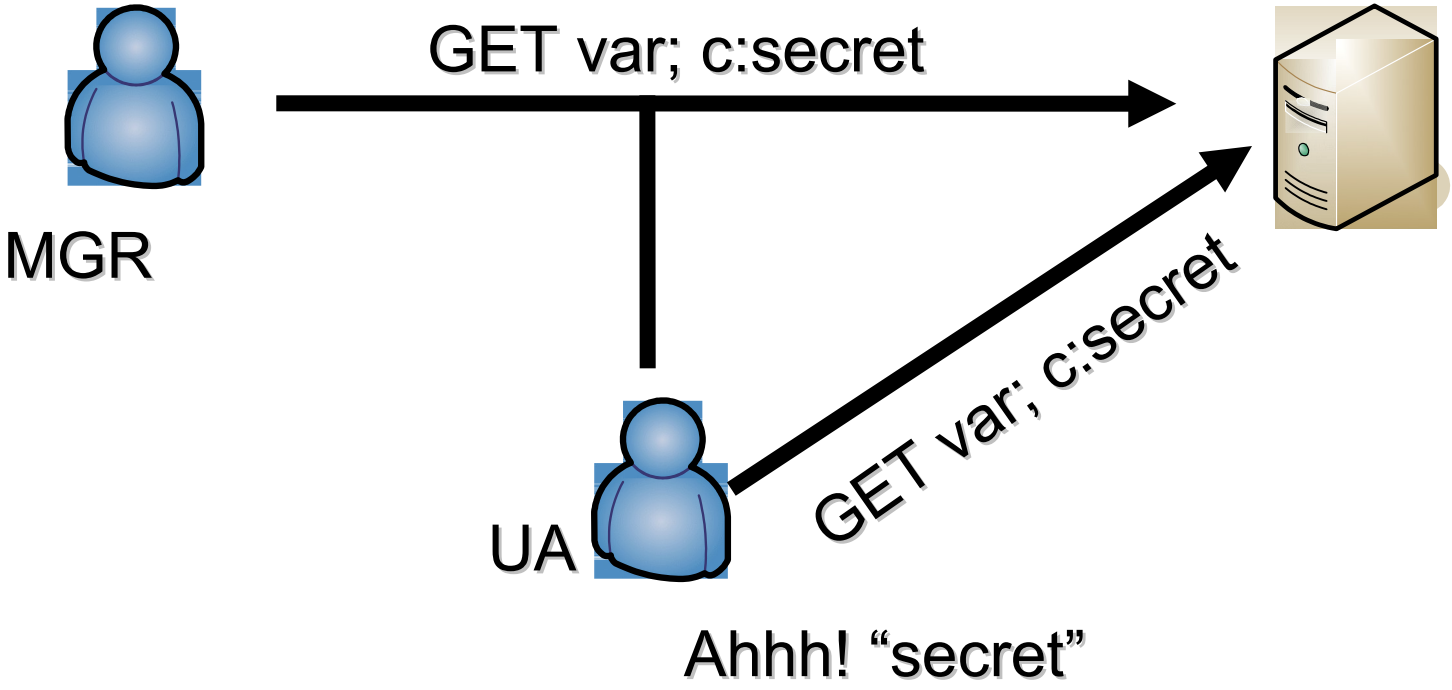
- **No permitir consultas recursivas**
- **Retacear información**
  - No permitir transferencia de zonas.
  - Cuidar los nombres de los hosts.
- **Actualizaciones**

- **DNS over TLS y Dns Over HTTPS (ver cuestiones de privacidad)**

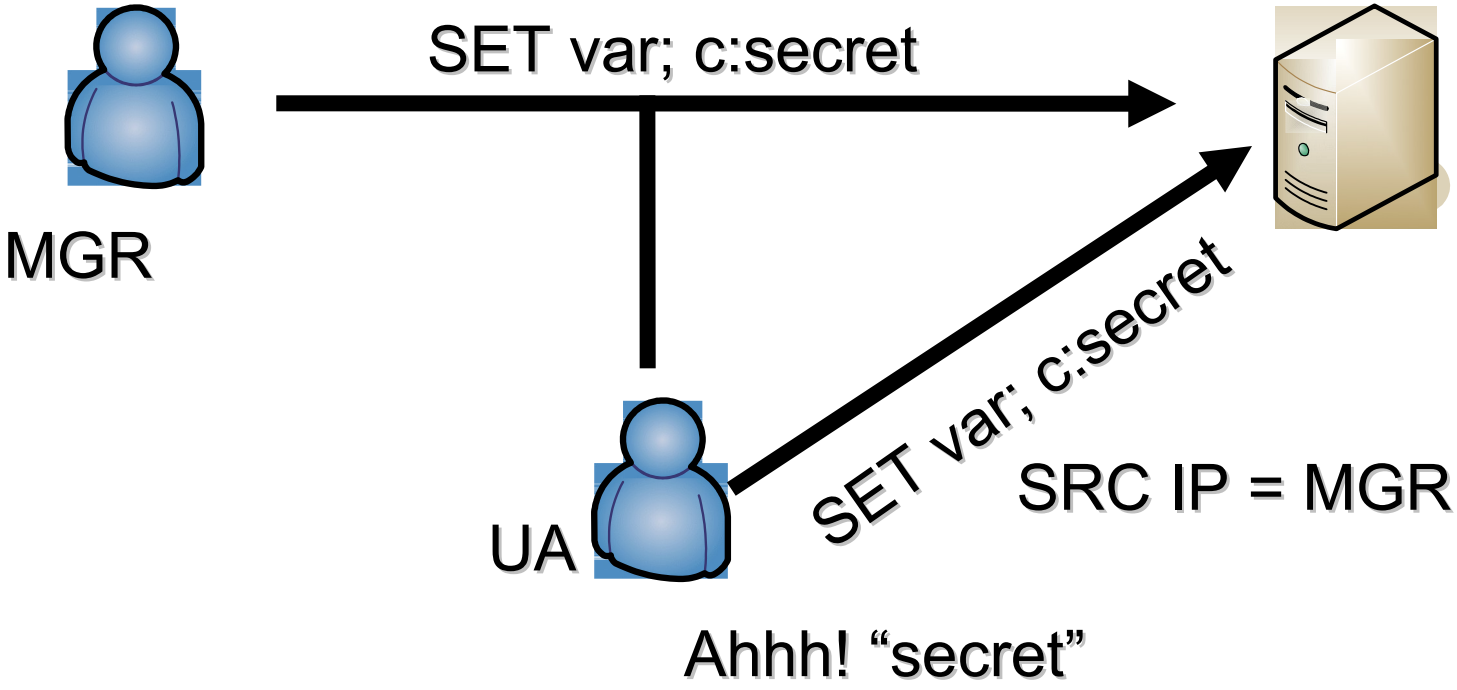
SNMP (UDP 161 y 162)

- **Simple Network Management Protocol**
- **Versiones v1, v2 y v3**
- **Sólo v3 sirve en un ambiente no asegurado**

SNMP

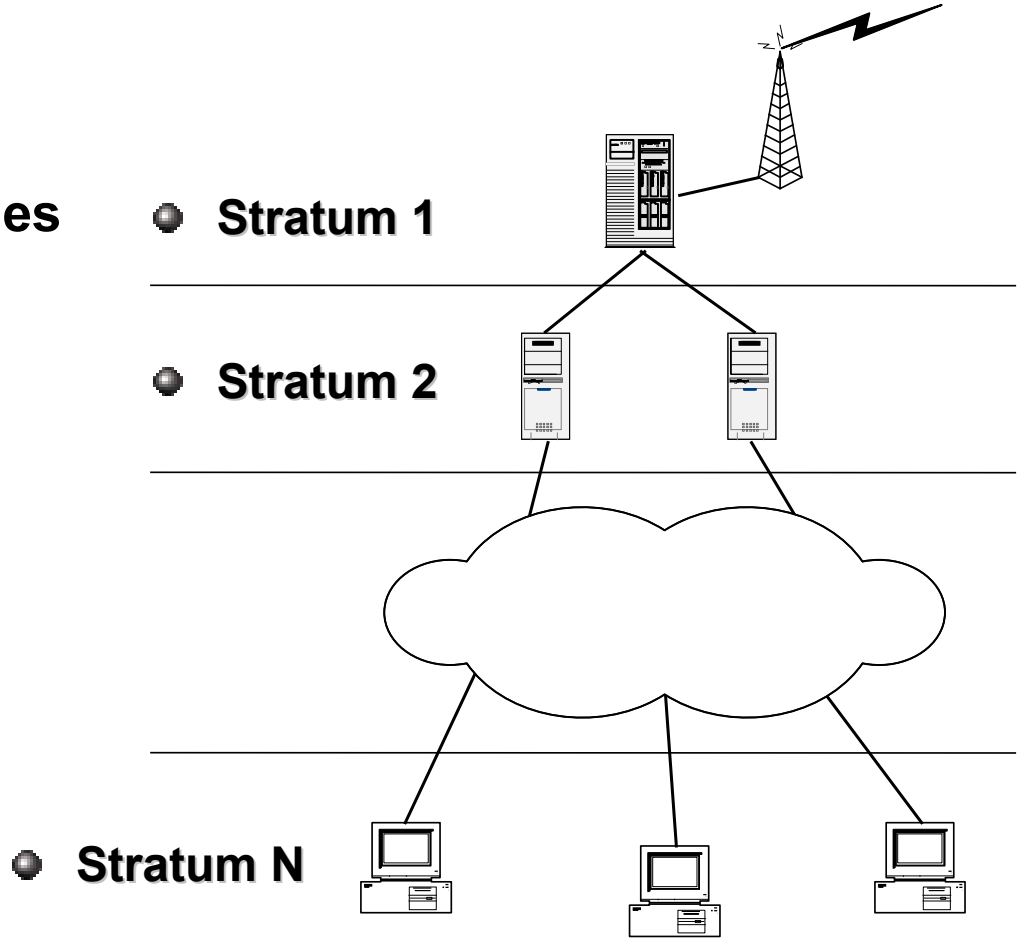


SNMP



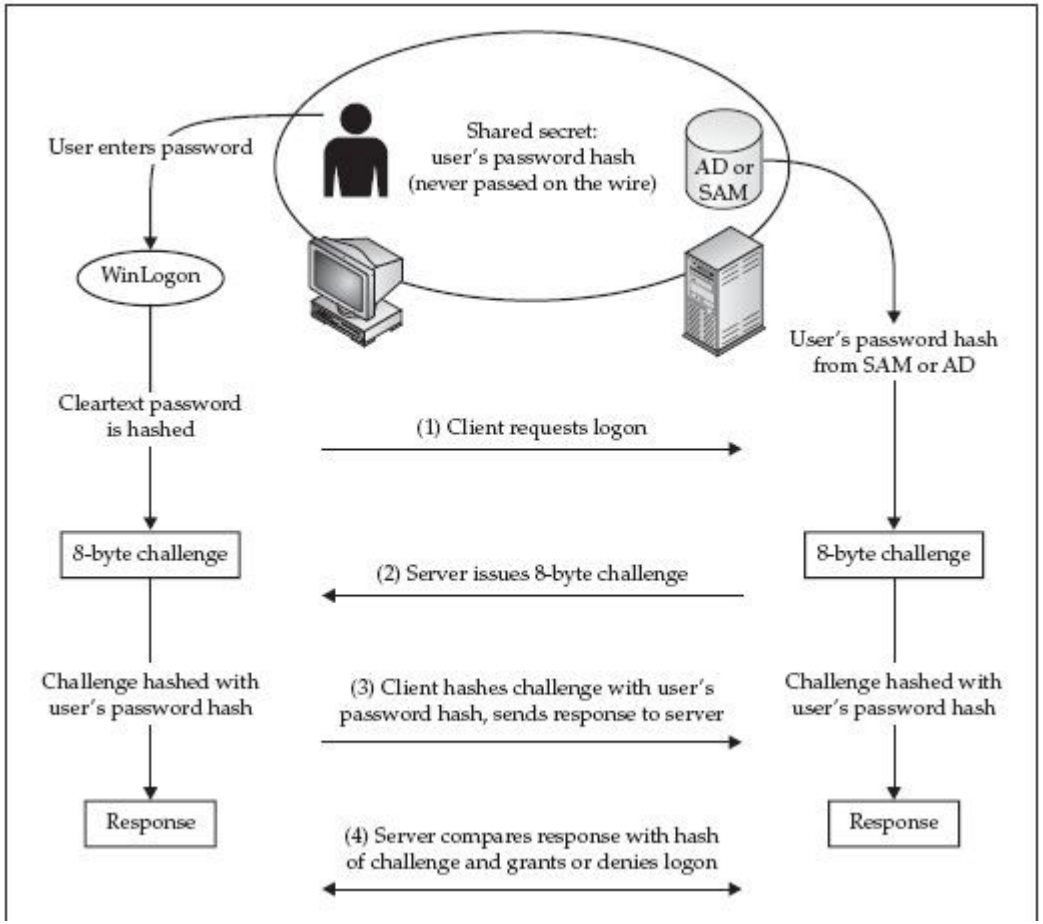
NTP (UDP/123)

- **Network Time Protocol**
- http://www.ntp.org
- **Permite sincronizar relojes**



Autenticación en Windows vía Red

MSV1_0 – Mecanismo pre-Kerberos



Ejemplo captura

AuthType	LM Hash	NT Hash	NT Serv-Chall	LM Cli-Chall	NT Cli-Chall
LM & NTLMv1	087B5B51531EE75983C6EFD966462706	8A923847309A...	F49FC03EB1C7DF68	69AD1B2DF0F4...	07756D654613
LM & NTLMv1	FD1FDDF9D58BD888DD263737E88F9C9F	4C02E5EDD99B...	3A5B76E314612A9A	E5E5EA7785B4...	E56D9D8055F1
LM & NTLMv1	7466F995B694D1AB192EF69A336921A6	115767781107...	CB7C7E82FBDD0FF4	7ADBA44A06E6...	C5639AA8416D
LM & NTLMv1	A91555B318E9559AA512BD877DD6C77C	C0A6D474B155...	0E0412D789643500	266EC72B3C53...	C1917F2483C6
LM & NTLMv1	7C1500C8B9EED8680EA08C2DAC7C930B	6243D8DB3A56...	1F12B6AAEEFE173B	B25475DB358A...	192FC9FF584E
LM & NTLMv1	C5A2E43D377FA8C2089FE84EBB7286A0	9BA1663D9414...	062B38CEADF87405	7A6016269196...	80E425AF6E81
LM & NTLMv1	A1F836199D6866CDAE89A67B78DD4950	FE67E078E313...	E803A629F3BAC8D6	96DB5DA146A1...	9F31CD332B10
LM & NTLMv1	752C0F327F198C61BF8E5C98B61D1157	B51E87F65090...	E79349190A3CAE5F	5996A9AC5F1C...	8D808A115619
LM & NTLMv1	9B4D439EEC8436E798F1BACC2B3F67E5	B0665CCE6206...	6FF825DCECE318F6	C2D7BD06FFF0...	5A771D165103
LM & NTLMv1	873F39F55EEAC889CE28035E420A0A54	37F7D7C84024...	C49D1826373476B8	9E4B01968513...	0A3037B0C802
LM & NTLMv1	27CB72C50130DF94F4D11FD67780C21F	8757476CD807...	AB136BB36D11192D	F4E11C696B87...	DA4AEC1E0EFE
LM & NTLMv1	F9880E29CD5DD8807D030CB2F21A5197	36B540646143...	3CBA646E8274A889	F7390D5DA289...	F2A980653748
LM & NTLMv1	8339FDD2B94A9141BCEB657F34048533	86B21425CA54...	566199AE10C5E0D7	26F2EA870F30...	3231BC4D4A69
LM & NTLMv1	921E9E5DD29A7DA3A9F28FD6B9A8EF59	43468FFC7F0E...	252E713393B3ACD6	AA92E3045E09...	B47FB278F042
LM & NTLMv1	78E494CF85C47BC5138741EC2A1EBD02	FD252A00B7FD...	318F5D9D35D1DECC	95EC75E72A19...	48AB36035B6F
LM & NTLMv1	ACA936F2799F00B7B6AD8ED76B4677F7	18FA980700A6...	658A97AD3FC10EED	7F4CF87237ED...	EF5617D4DE52