REDES

VPN, NAT y SNMP

VPN

- Virtual Private Network
- Se utiliza para interconectar redes o equipos a través de otras redes.
- Si se atraviesa redes de terceros
  - Aplicar encripción de datos
- Normalmente se lo denomina túnel porque encapsula la comunicación entre las dos puntas

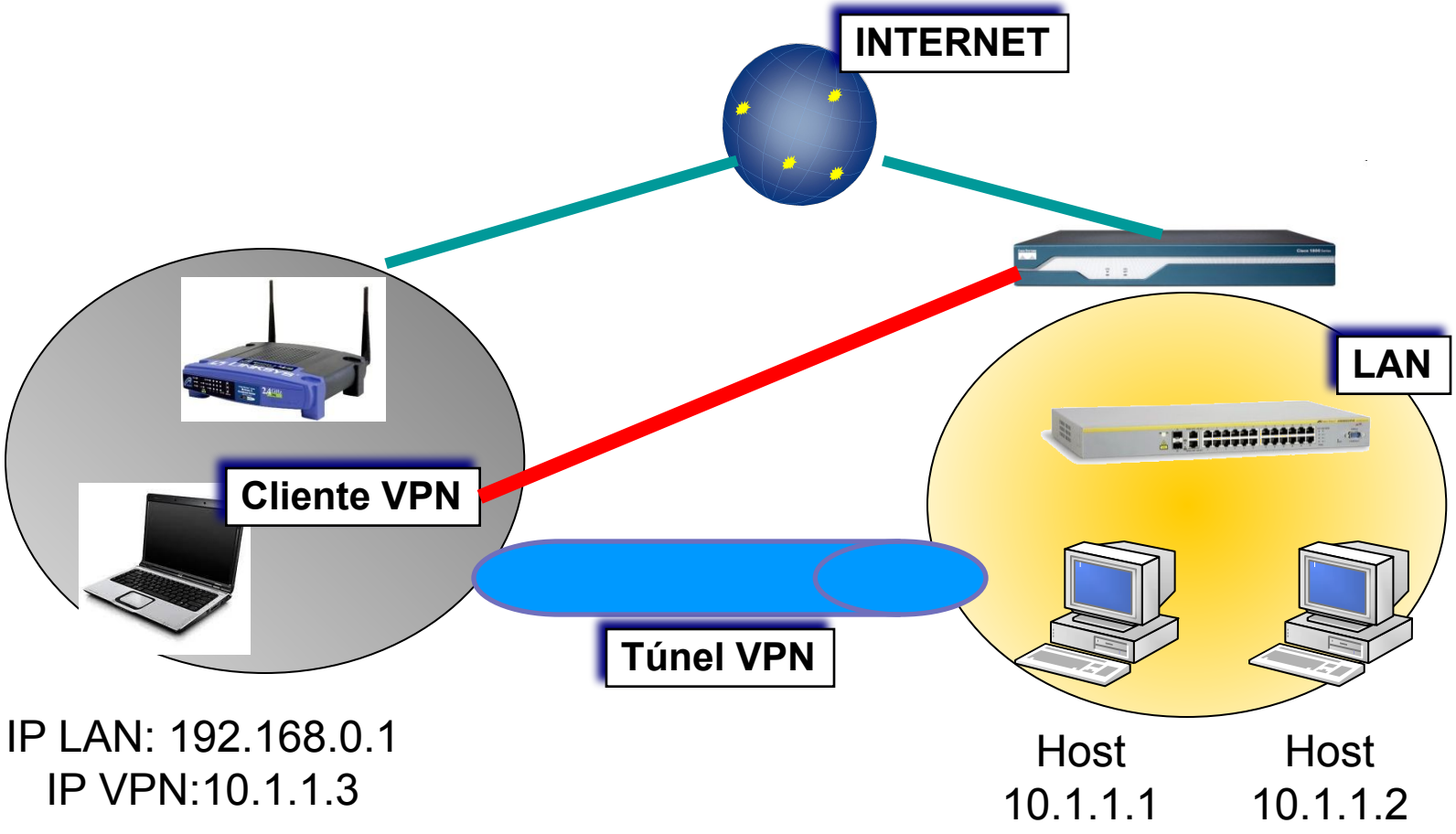
VPN

- Modos de conexión más comunes
  - Cliente a Sitio
  - Sitio a Sitio
- Tipos soluciones
  - Hardware (Firewall)
  - Software (Cliente – servidor)
  - Mixtas

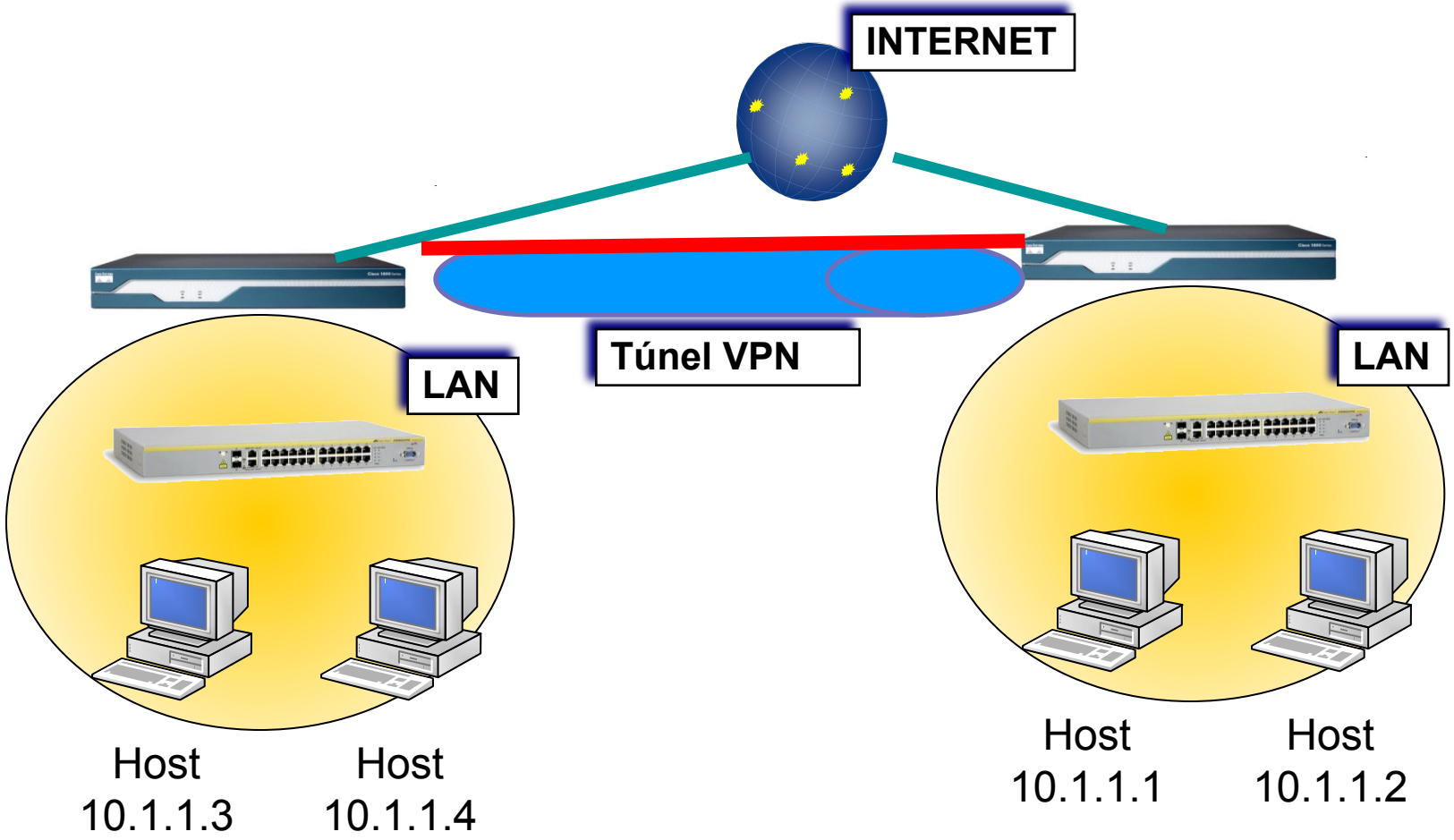
Tipos de VPN

- Cliente a Sitio
  - Uso común:
    - Usuarios móviles
  - Licencias
    - Suele ser por cliente/usuario
- Sitio a Sitio
  - Uso común:
    - Sucursales a través de Internet
    - Interconexión entre empresas
  - Licencias
    - Suele ser por sitio

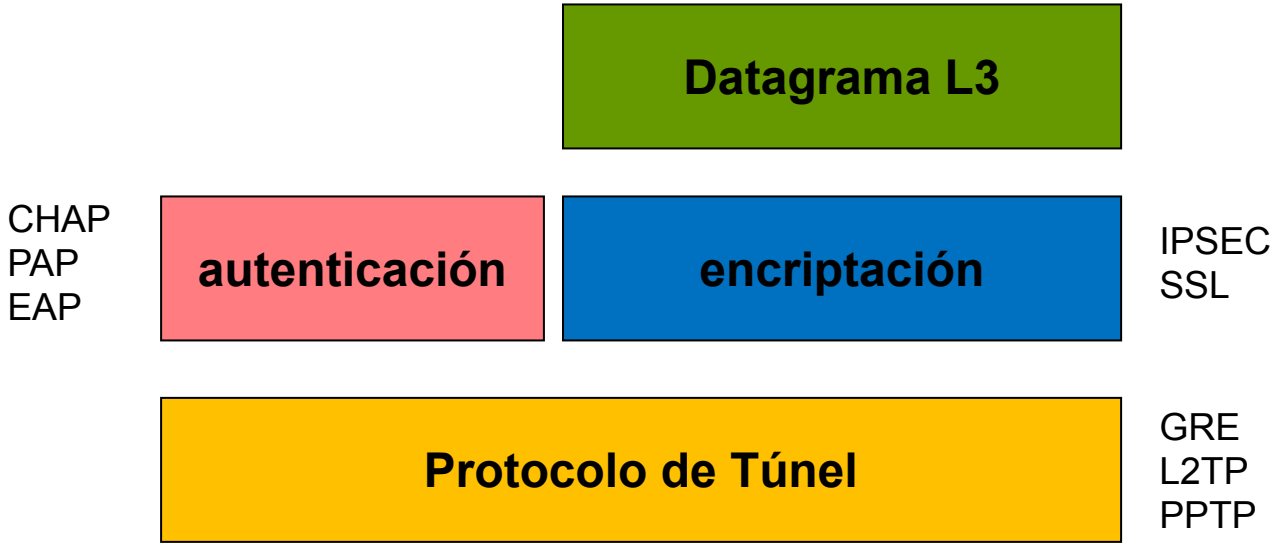
VPN – Cliente a sitio



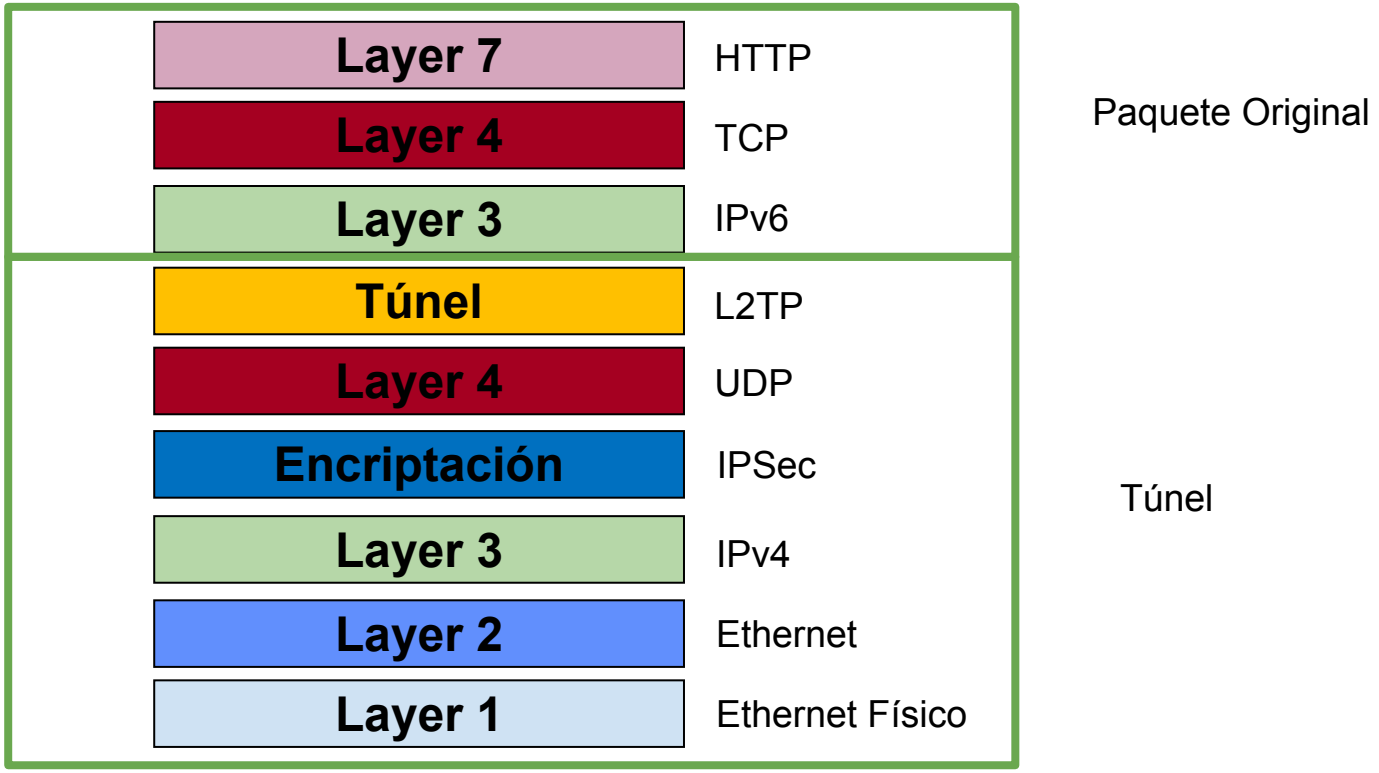
VPN – Sitio a sitio



Capas de una VPN

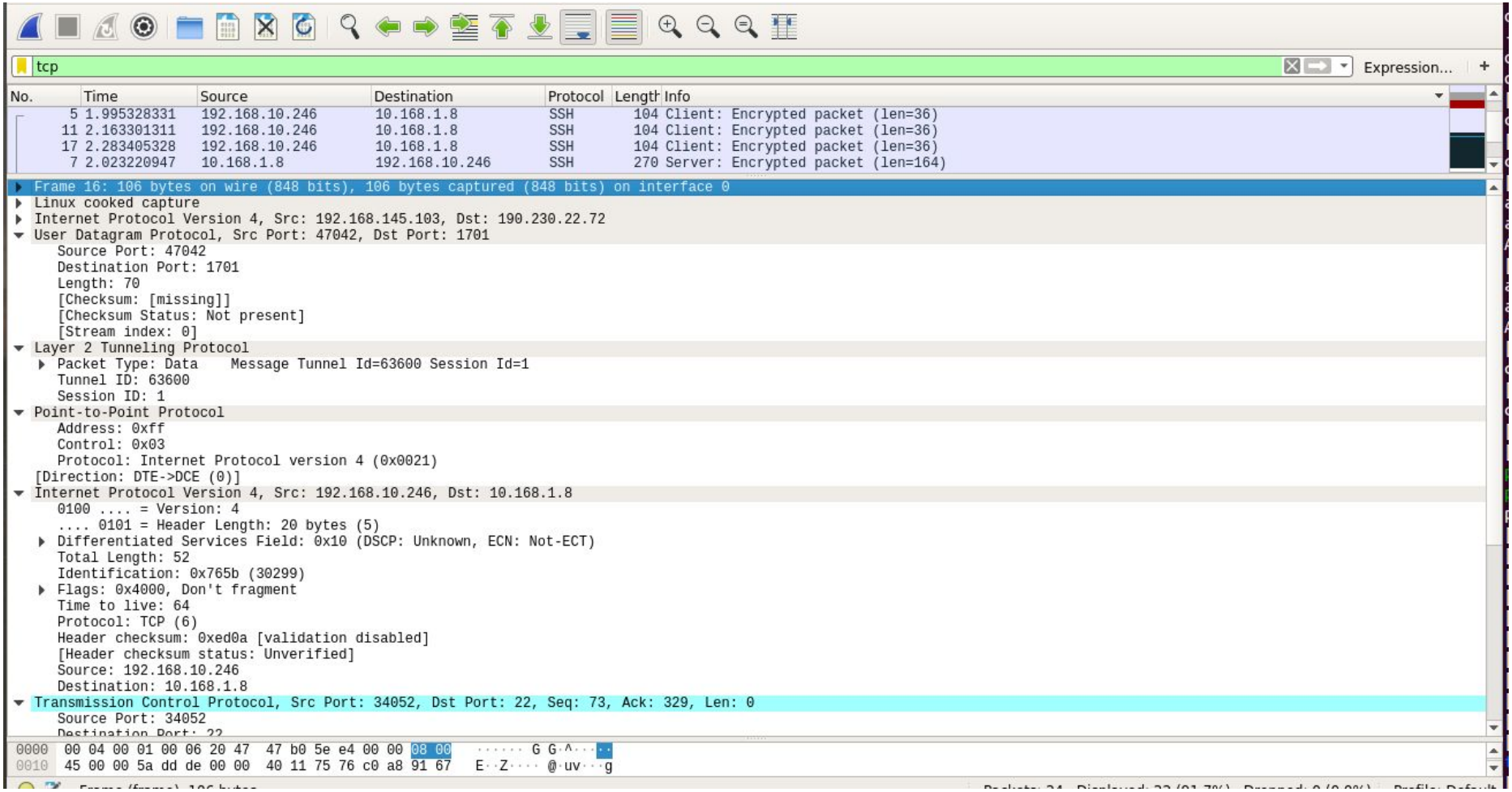


Ejemplo de capas de una VPN



- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)
- PPTP (Peer to Peer Tunneling protocol)

Captura de paquetes con VPN



Soluciones de software

- Sistemas operativos

- OpenVPN
  - Licencia GPL
  - Permite crear VPN SSL
  - Usa un solo puerto UDP
  - Pasa a través de Proxy y Firewall
  - No tiene problemas con NAT

Soluciones de Hardware

- Firewalls
  - Soportan VPN Cliente-Sitio y Sitio-Sitio
  - Proveen cliente propietario
  - Permiten conexión por VPN SSL (el navegador necesita un plug-in que se instala en la PC)

IPSec

- En 1998 la IETF define los RFC's para las VPN
- IPSec es un conjunto de protocolos para crear VPNs
  - RFC 2401 (IPSec)
  - RFC 2402 (Authentication Header)
  - RFC 2406 (Encapsulating Security Payload)
  - RFC 2408 (ISAKAMP)
  - RFC 2409 (IKE – Internet Key Exchange)

  - Muy complejo de implementar !
  - Corre en espacio Kernel en los SO

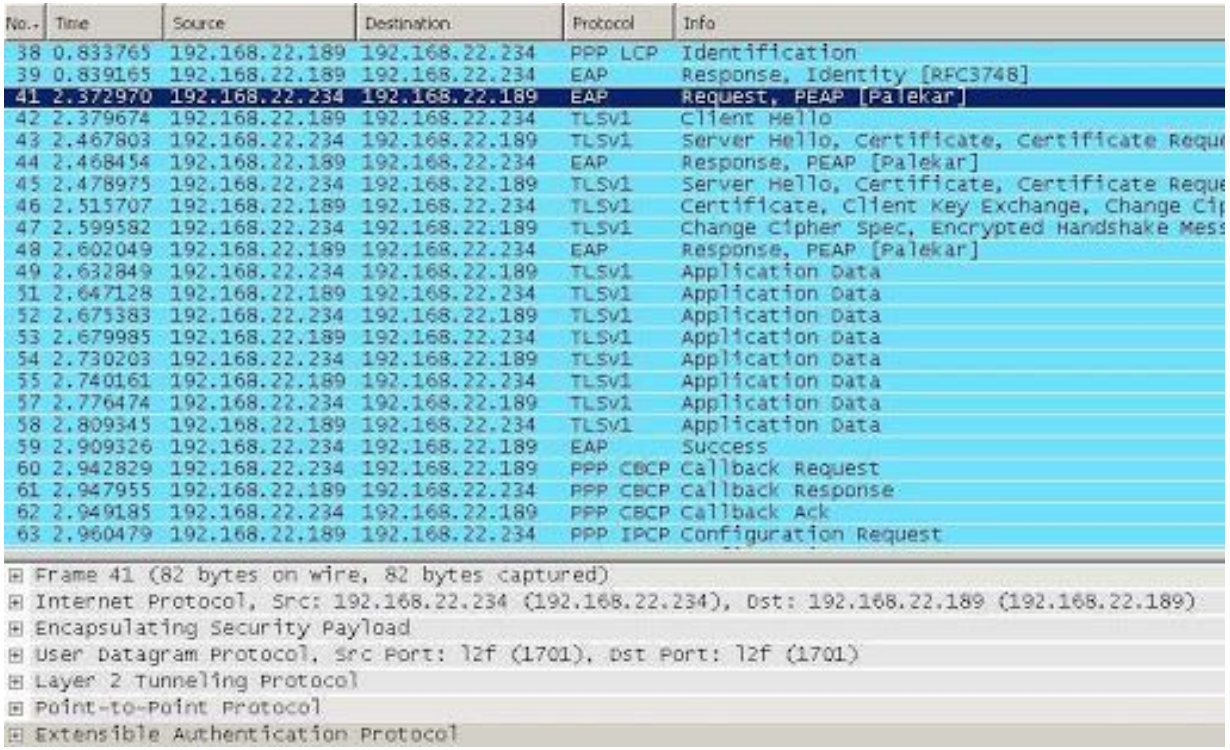
VPN SSL

- El cliente se conecta a URL
  - Ej: https://vpn.miempresa.com.ar
  - El navegador suele pedir instalación de un plug-in
  - Autentificación
  - Crea interfaz virtual
  - Genera la misma VPN que “Cliente a sitio”

  - Ventajas
    - Usa puerto común (443)
    - No requiere instalación de cliente

  - La licencia suele ser por cliente

Captura de paquetes con VPN



No.	Time	Source	Destination	Protocol	Info
38	0.833765	192.168.22.189	192.168.22.234	PPP LCP	Identification
39	0.839165	192.168.22.189	192.168.22.234	EAP	Response, Identity [RFC3748]
41	2.372970	192.168.22.234	192.168.22.189	EAP	Request, PEAP [Palekar]
42	2.379674	192.168.22.189	192.168.22.234	TLSv1	Client Hello
43	2.467803	192.168.22.234	192.168.22.189	TLSv1	Server Hello, Certificate, Certificate Requ
44	2.468454	192.168.22.189	192.168.22.234	EAP	Response, PEAP [Palekar]
45	2.478975	192.168.22.234	192.168.22.189	TLSv1	Server Hello, Certificate, Certificate Requ
46	2.515707	192.168.22.189	192.168.22.234	TLSv1	Certificate, Client Key Exchange, Change Ci
47	2.599582	192.168.22.234	192.168.22.189	TLSv1	Change Cipher Spec, Encrypted Handshake Mes
48	2.602049	192.168.22.189	192.168.22.234	EAP	Response, PEAP [Palekar]
49	2.632849	192.168.22.234	192.168.22.189	TLSv1	Application Data
51	2.647128	192.168.22.189	192.168.22.234	TLSv1	Application Data
52	2.675383	192.168.22.234	192.168.22.189	TLSv1	Application Data
53	2.679985	192.168.22.189	192.168.22.234	TLSv1	Application Data
54	2.730203	192.168.22.234	192.168.22.189	TLSv1	Application Data
55	2.740161	192.168.22.189	192.168.22.234	TLSv1	Application Data
57	2.776474	192.168.22.234	192.168.22.189	TLSv1	Application Data
58	2.809345	192.168.22.189	192.168.22.234	TLSv1	Application Data
59	2.909326	192.168.22.234	192.168.22.189	EAP	Success
60	2.942829	192.168.22.234	192.168.22.189	PPP CBCP	Callback Request
61	2.947955	192.168.22.189	192.168.22.234	PPP CBCP	Callback Response
62	2.949185	192.168.22.234	192.168.22.189	PPP CBCP	Callback Ack
63	2.960479	192.168.22.189	192.168.22.234	PPP IPCP	Configuration Request

⊞ Frame 41 (82 bytes on wire, 82 bytes captured)
⊞ Internet Protocol, Src: 192.168.22.234 (192.168.22.234), Dst: 192.168.22.189 (192.168.22.189)
⊞ Encapsulating Security Payload
⊞ User Datagram Protocol, Src Port: l2f (1701), Dst Port: l2f (1701)
⊞ Layer 2 Tunneling Protocol
⊞ Point-to-Point Protocol
⊞ Extensible Authentication Protocol

Protocolos de Autenticación de VPN

- EAP (Extensible Authentication Protocol) - Más Seguro
- CHAP (Challenge Handshake Protocol)
- PAP (Password Authentication Protocol) - Menos seguro

- Intercambian credenciales entre el cliente y el servidor VPN
- Handshake e intercambio de claves o shared secret

Ejemplo de conexión (1)

- Interface Eth0 de Notebook
  - IP: 192.168.0.49
  - GW: 192.168.0.1
  - MASK: 255.255.255.0
  - Serv DNS: 8.8.8.8

IPv4 Tabla de enrutamiento

Rutas activas:

Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.49	55
192.168.0.0	255.255.255.0	En vínculo	192.168.0.49	311
192.168.0.49	255.255.255.255	En vínculo	192.168.0.49	311
192.168.0.255	255.255.255.255	En vínculo	192.168.0.49	311
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331
255.255.255.255	255.255.255.255	En vínculo	192.168.0.49	311

Ejemplo de conexión (2)

- Conexión a empresa
  - Host: vpn.miempresa.com.ar (181.22.33.44)
  - Sabemos que dentro de la empresa están las redes:
    - 10.4.0.0/16
    - 10.50.50.0/24
    - 10.40.1.0/24
    - 192.168.0.0/16

Ejemplo de conexión (2)

- Creamos la conexión de VPN

- Interface Eth0 de Notebook (no cambió)
  - IP: 192.168.0.49
  - GW: 192.168.0.1
  - MASK: 255.255.255.0
  - Serv DNS: 8.8.8.8

- Interface Eth1 de Notebook
  - IP: **10.50.50.152**
  - GW: (no tiene)
  - MASK: 255.255.255.0

Ejemplo de conexión (3)

- Nueva tabla de ruteo luego de la conexión VPN

IPv4 Tabla de enrutamiento

Rutas activas:

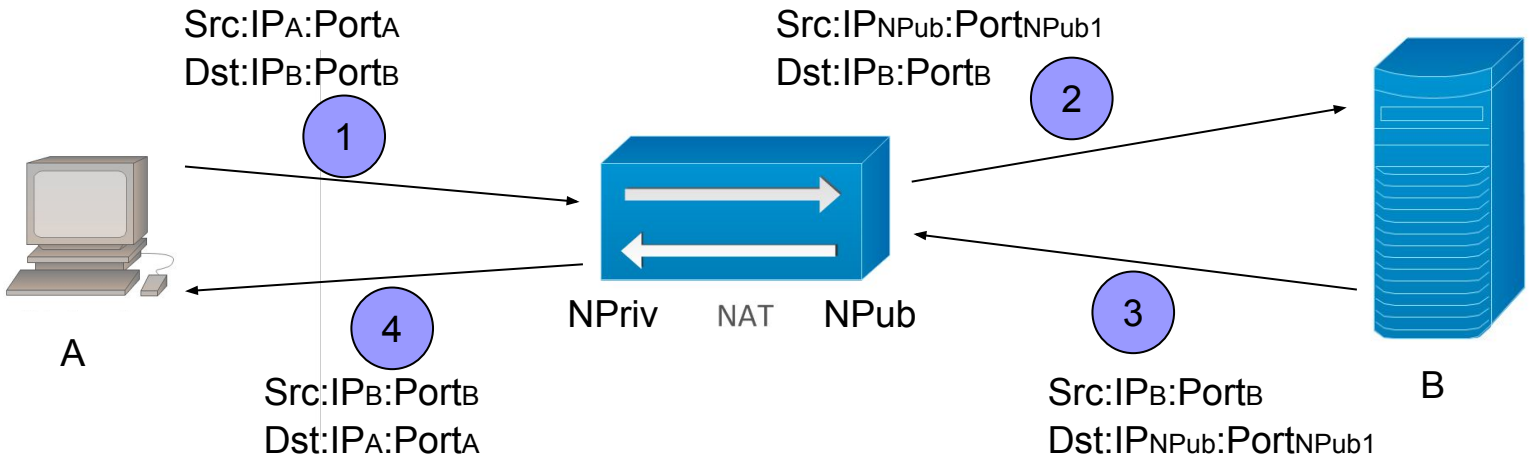
Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.49	55
10.4.0.0	255.255.0.0	En vínculo	10.50.50.152	2
10.40.1.0	255.255.255.0	En vínculo	10.50.50.152	2
181.22.33.44	255.255.255.255	192.168.0.1	192.168.0.49	55
192.168.0.0	255.255.0.0	En vínculo	10.50.50.152	2
192.168.0.0	255.255.255.0	En vínculo	192.168.0.49	311
192.168.0.49	255.255.255.255	En vínculo	192.168.0.49	311
192.168.0.255	255.255.255.255	En vínculo	192.168.0.49	311
255.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331
255.255.255.255	255.255.255.255	En vínculo	192.168.0.49	311

NAT

- No está estandarizado
- El NAT tradicional no acepta conexiones entrantes a menos que hayan sido salientes.
- Fue diseñado para el concepto cliente/servidor
- NAT no desaparece con IPv6 porque siguen existiendo los firewalls (¿será así ?)

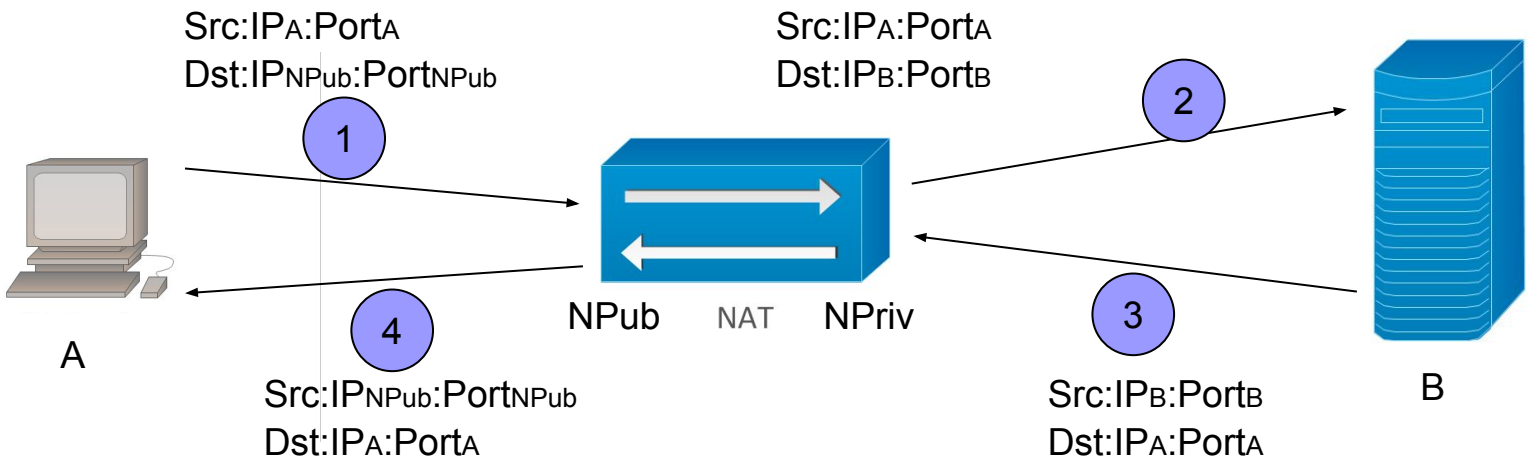
SNAT (Source NAT)

- Utilizado cuando un dispositivo en una red privada contacta a otro en una red pública
- Típicamente el de la red pública es un servidor de algún tipo



DNAT (Destination NAT)

- Utilizado cuando un dispositivo en una red pública quiere iniciar una conexión hacia uno que se encuentra en una red privada
- Típicamente el de la red privada es un servidor de algún tipo

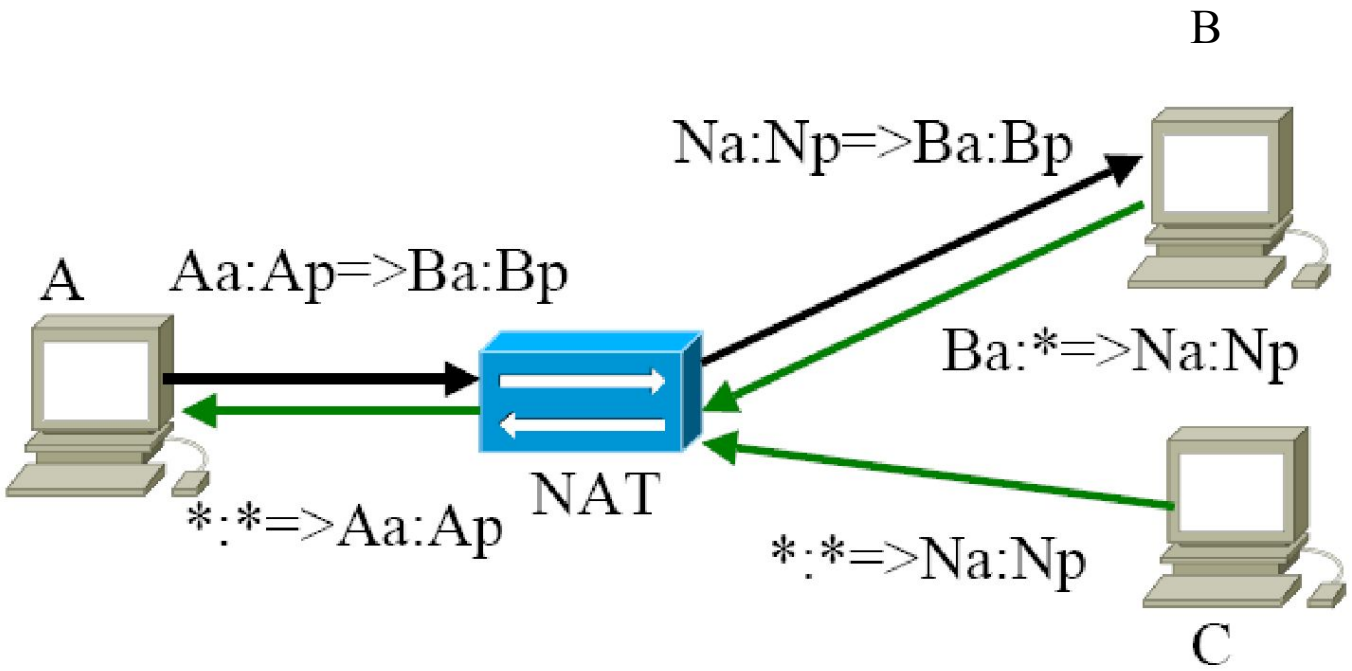


Tipos de NAT

- Tipos de NAT
  - Full Cone
  - IP Restricted NAT
  - Port restricted NAT
  - Symmetric

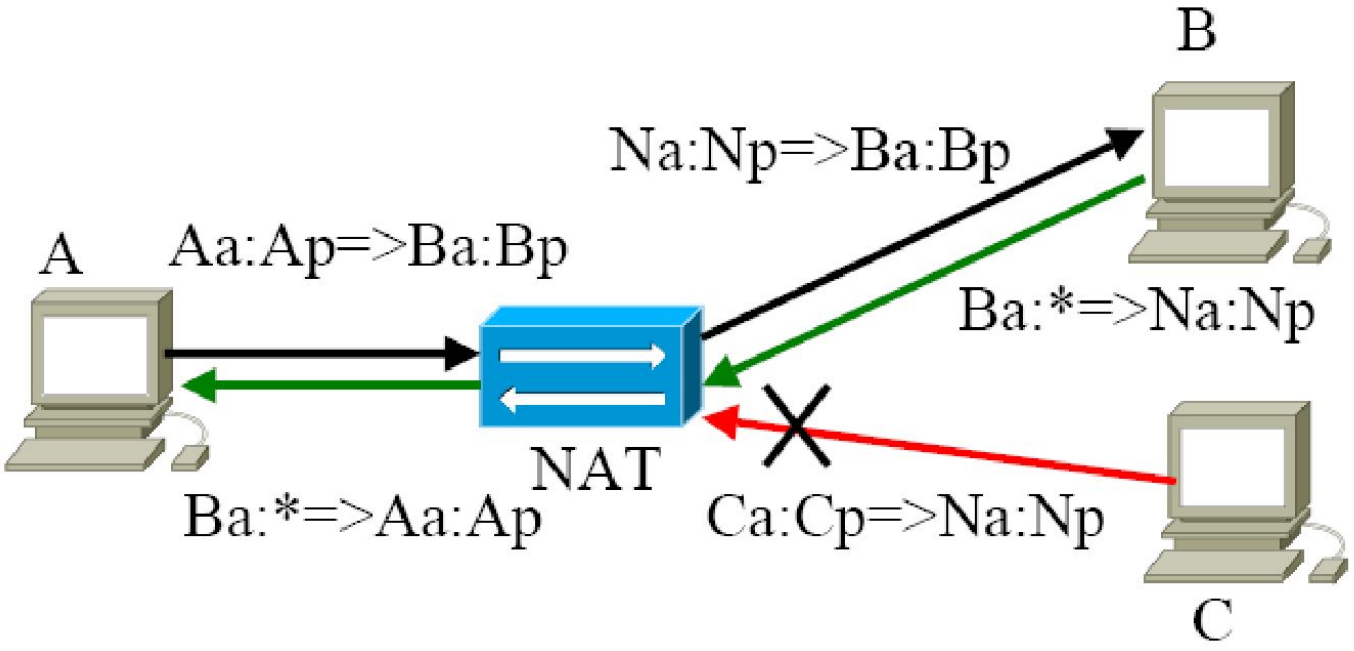
NAT – Full Cone (Static NAT)

- a=address, p=port
- Muy poco restrictivo para conexiones entrantes
- Mapeo estático para servidores



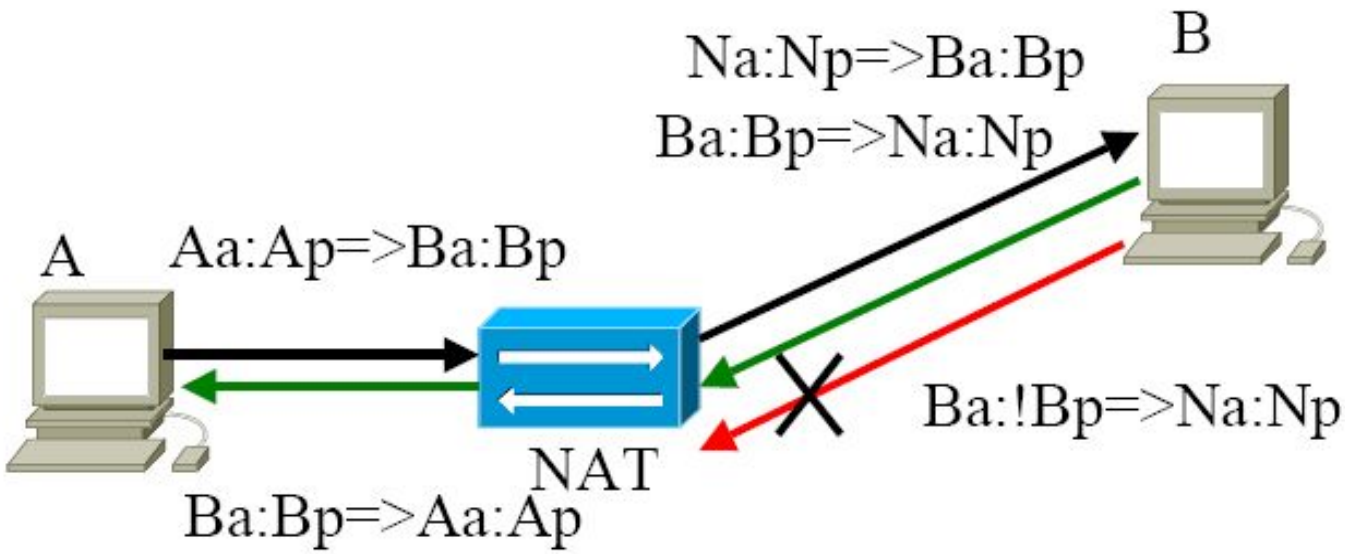
NAT – IP Restricted

- a=address, p=port
- Solo restringe la IP entrante no el puerto



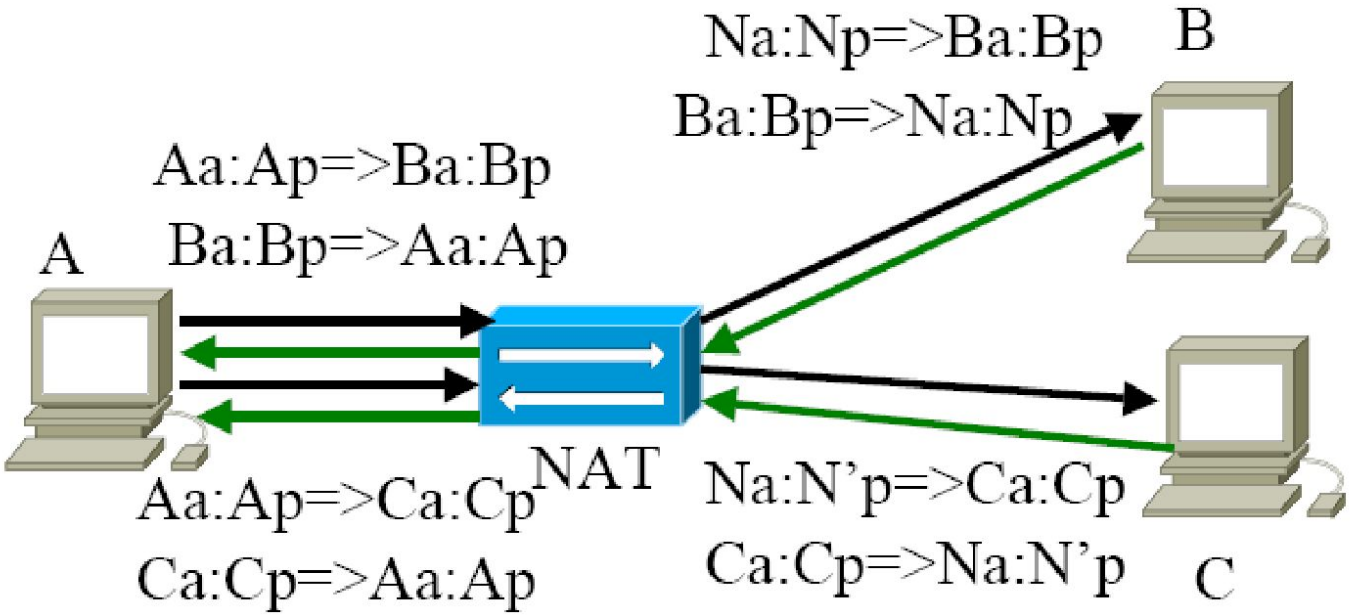
NAT – Port Restricted

- a=address, p=port
- Restringe la IP entrante y el puerto



NAT – Symmetric

- a=address, p=port
- Cada nueva conexión genera un nuevo puerto

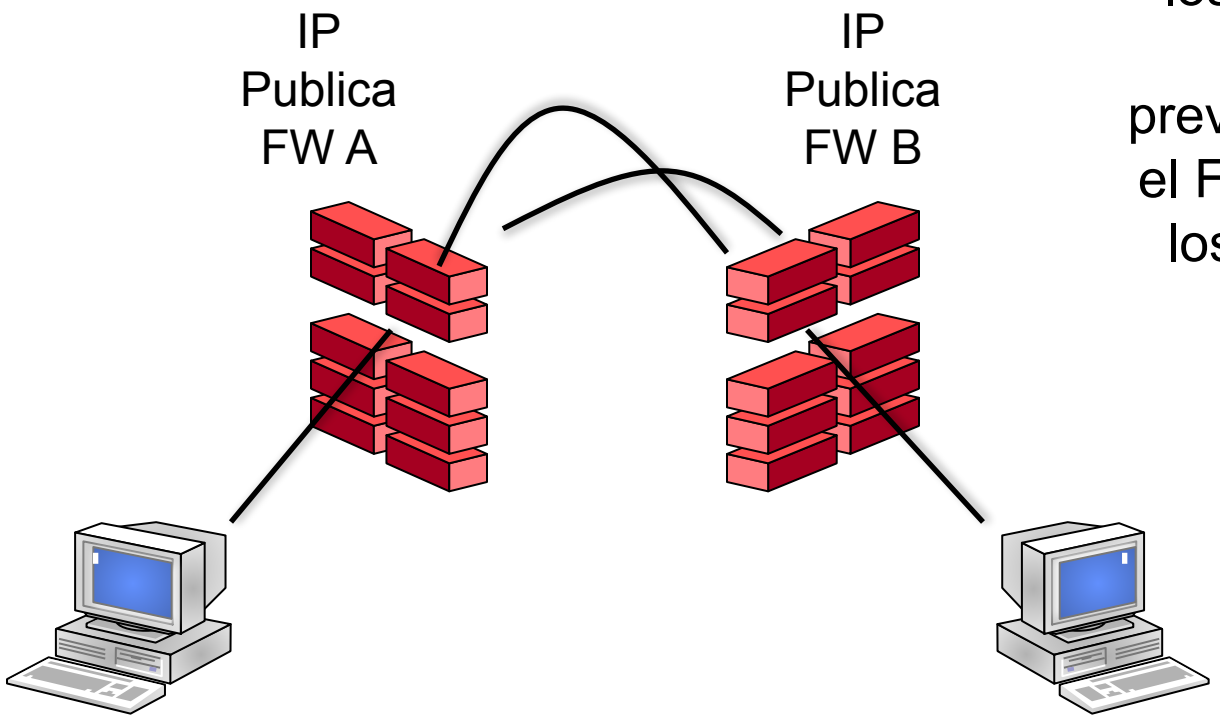


NAT Traversal

- Se debe buscar una solución para servicios del tipo P2P o VOIP
- No es posible crear reglas de NAT entrantes para todos los clientes posibles

- Soluciones
  - UDP Hole Punching
  - STUN
  - TURN
  - ICE

UDP Hole (sin servidor)



Se conocen los puertos UDP previamente y el Firewall no los cambia

Pc A

Conexión a FB:40001

Desde 40000

Pc B

Conexión a FA:40000

Desde 40001

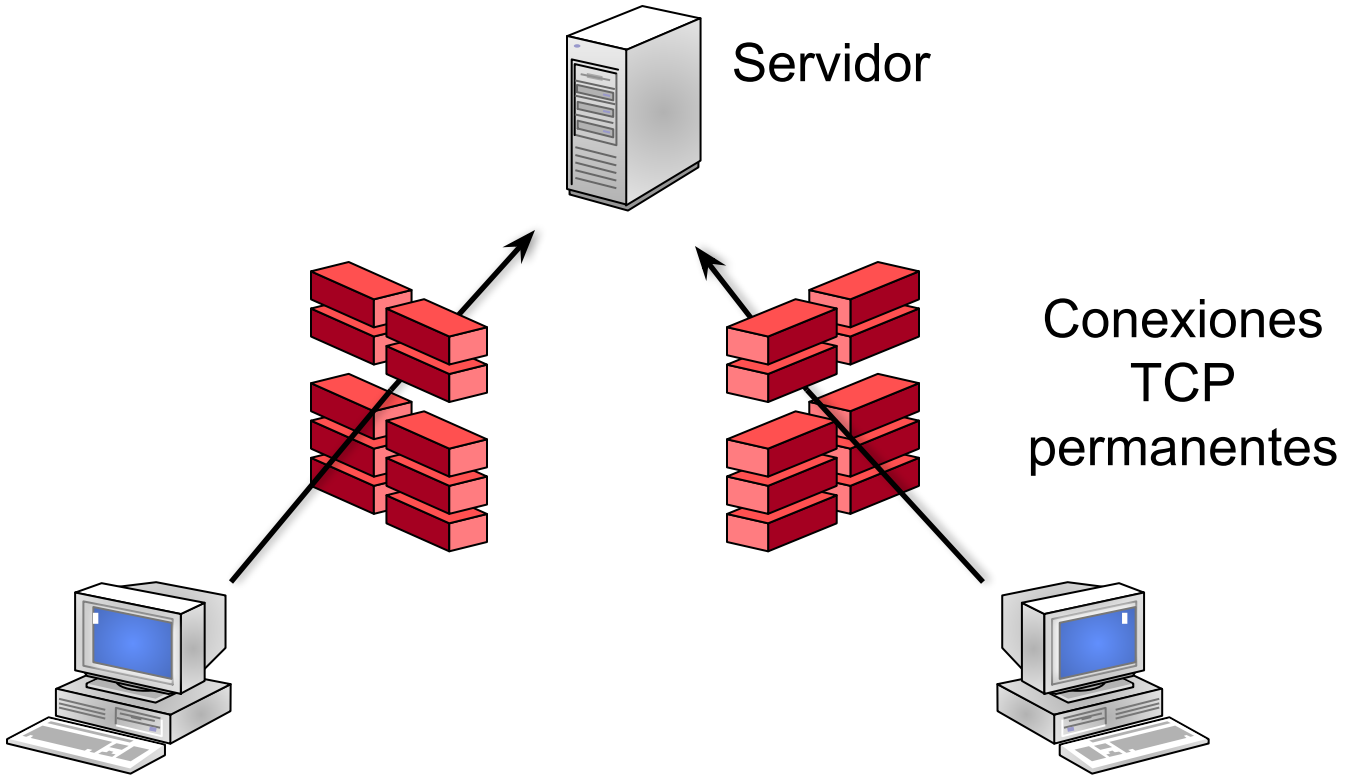
UDP Hole (sin servidor)

```
srv@srv-nb:~$ sudo tcpdump udp -i eth2 | grep 4000
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
00:57:43.481685 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:57:45.482073 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:57:47.482508 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:57:49.482922 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:57:51.483405 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:57:53.483781 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:59:09.492181 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:59:11.064525 IP pampero.it.itba.edu.ar.40000 > srv-nb.local.40001: UDP, length 20
00:59:11.492727 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
00:59:12.062764 IP pampero.it.itba.edu.ar.40000 > srv-nb.local.40001: UDP, length 20
00:59:12.492940 IP srv-nb.local.40001 > pampero.it.itba.edu.ar.40000: UDP, length 20
```

user1@left $ nat-traverse 40001:pampero.itba.edu.ar:40000

user2@pampero $ nat-traverse 40000:ejemplo.dyndns.com:40001

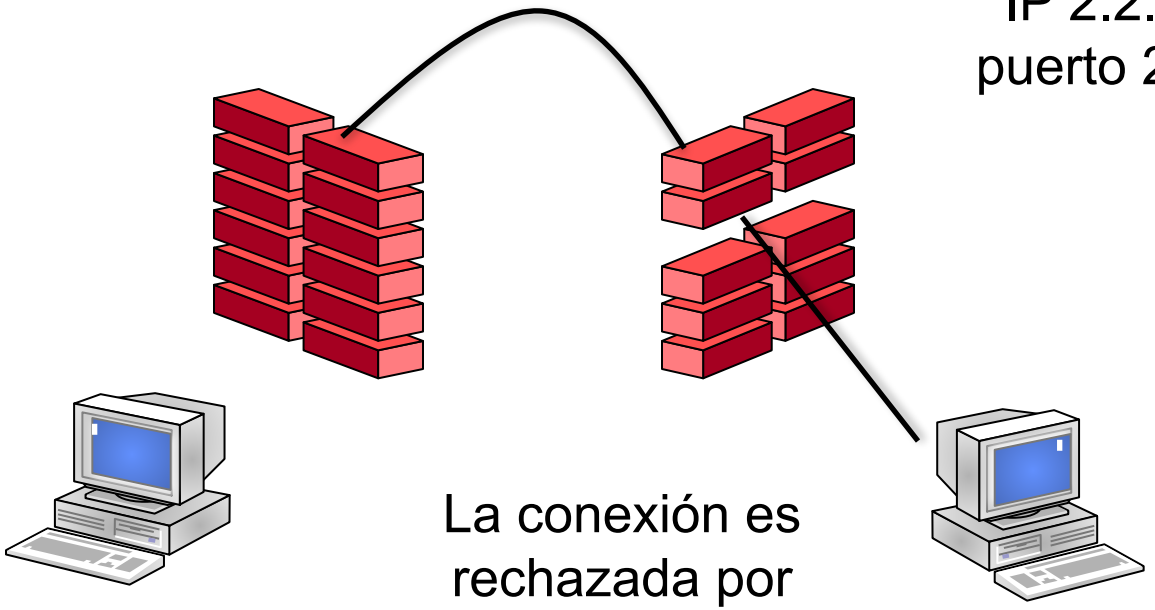
UDP Hole punching (con servidor)



UDP Hole punching (con servidor)

El servidor pasa las coordenadas de la Pc A a la Pc B

La Pc B Intenta una conexión a la IP 2.2.2.2 puerto 2828



La conexión es rechazada por el Firewall de A

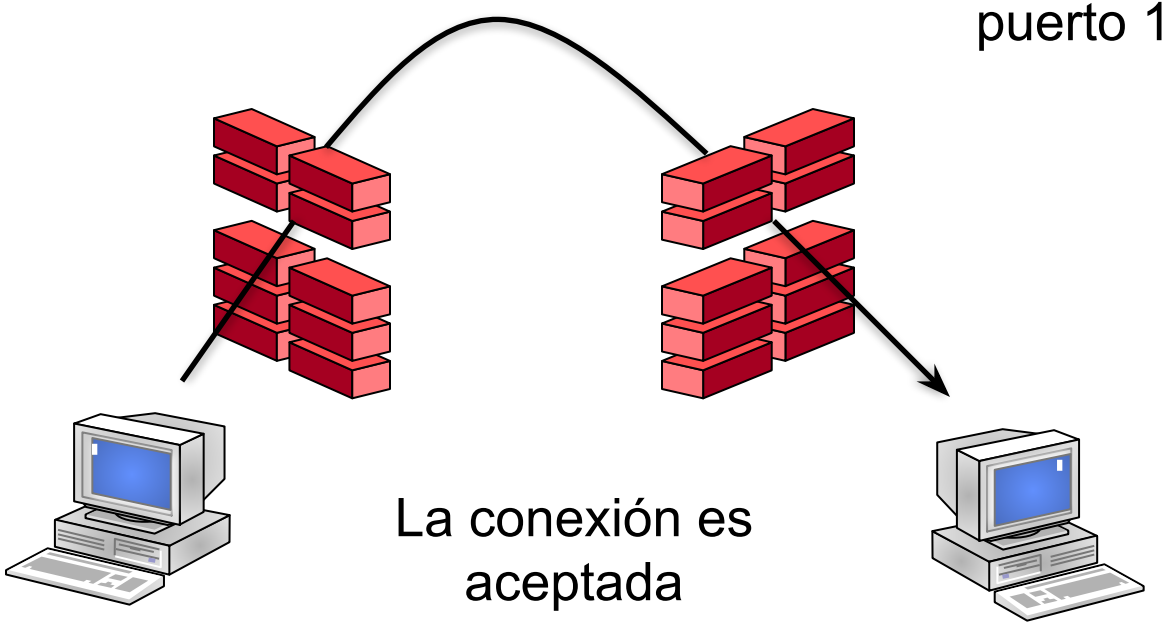
Pc A

IP:2.2.2.2
Puerto 2828

UDP Hole punching

El servidor pasa las coordenadas de la Pc B a la Pc A

La Pc A intenta una conexión a la IP 1.1.1.1 puerto 1414



La conexión es aceptada porque es esperada por el firewall de B

Pc A

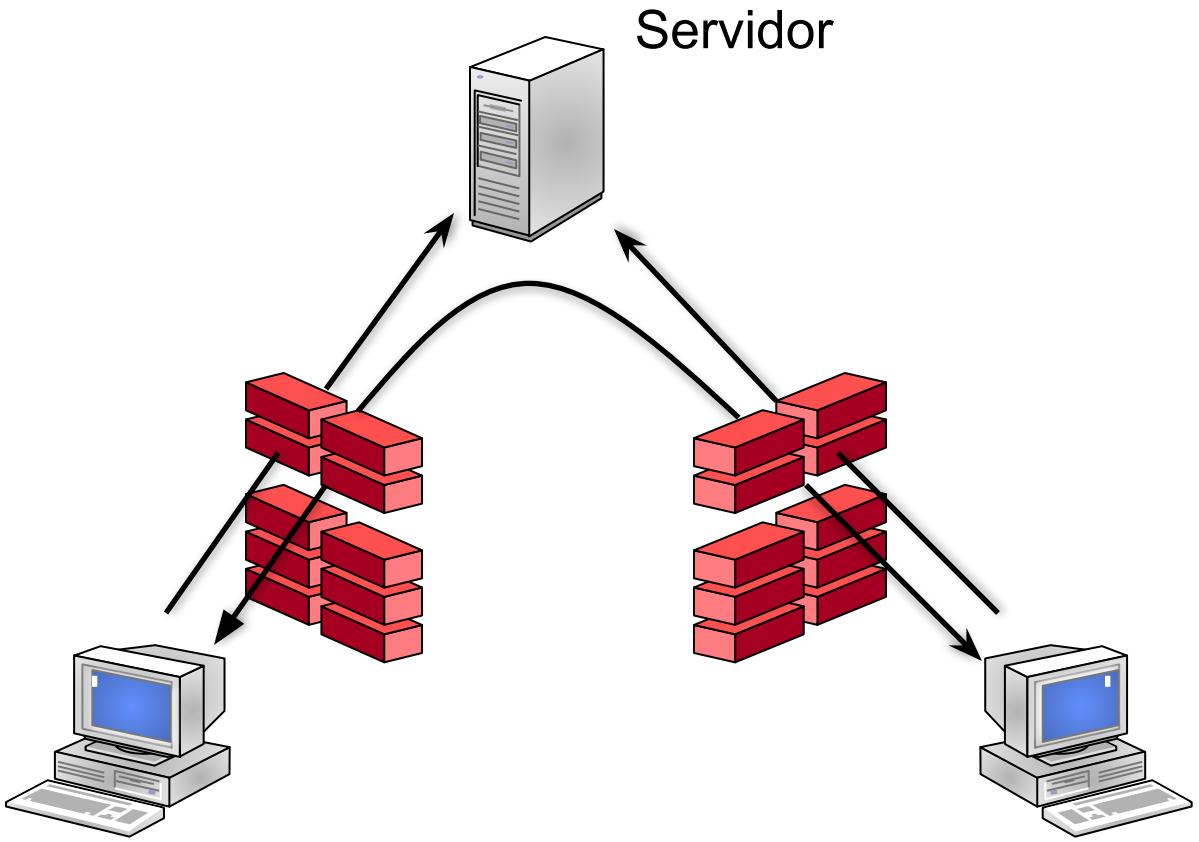
IP:2.2.2.2
Puerto 2828

Pc B

IP:1.1.1.1
Puerto 1414

UDP Hole punching

Se mantienen las conexiones TCP por posibles cambios



Pc A

IP:2.2.2.2
Puerto 2828

Pc B

IP:1.1.1.1
Puerto 1414

UDP Hole Punching

- Esta técnica no esta estandarizada
- Si no funciona esta técnica se debe pasar los datos a través del sever (relay)
  - Alto uso de recursos de hardware
  - Limitaciones de ancho de banda y latencia

STUN

- Session Traversal Utilities for NAT
- RFC 5389 (antes RFC 3489)
- Protocolo para descubrir distintos tipos de NAT
- Define los pasos a seguir y tipos de mensajes a enviar
- Permite a los clientes conocer la IP publica y puerto con los que salen sus datos.
- Chequea conectividad entre dos endpoints

STUN

- Existen servidores gratuitos en Internet
  - stun.ekiga.net
  - stun.xten.com
  - stun.voipbuster.com
  - …….
- No suelen ofrecer relay

TURN

- Traversal Using Relay NAT
- RFC 5766
- Debería ser la segunda opción en caso que no funcione STUN
- Protocolo para hacer relay de UDP y TCP detrás de NAT
- Única solución para Symmetric NAT

ICE

- Interactive Connectivity Establishment
- Evalua todos los cantidatos de conexión
  - STUN / TURN / IPs Locales
- Los ordena por prioridad
- Chequea conectividad
- Una vez que se establece la conexión deja de operar

Monitoreo y administración de redes

- Problemas frecuentes
  - Caída o mal funcionamiento de servicios. Nos avisa el usuario !
  - Cortes de energía en sitio central y remoto.
  - Enlace saturado. ¿Quién esta generando ese trafico ?
  - Servidor remoto encendido pero no responde ping. ¿ Tengo que ir hasta allá ?

Monitoreo y administración de redes

- Se busca lograr administración preventiva y proactiva
- Único sistema de monitoreo, todas las capas
- Reportes, Estadísticas y toma de decisiones
- Seguridad
- Acuerdo de niveles de servicios (SLA)
- Se usa principalmente SNMP

SNMP
Simple Network Management Protocol

- Herramienta sencilla para la gestión de red
- Define una base de información de gestión (MIB: Management Information Base) limitada y fácil de implementar
- Define un protocolo para permitir a un gestor obtener y establecer variables MIB y para permitir a un agente emitir notificaciones no solicitadas (traps)

SNMP

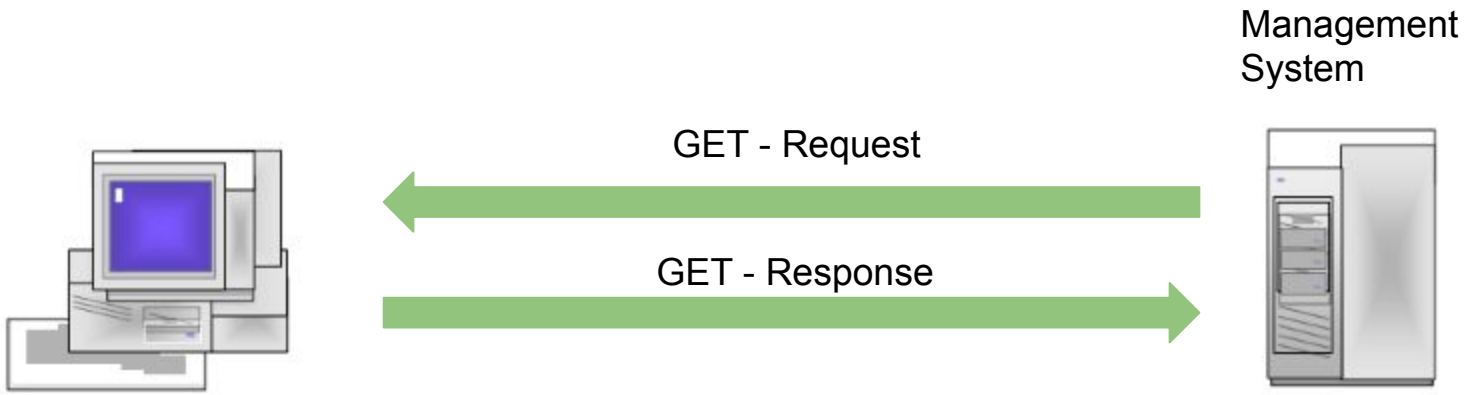
Dispositivos que lo soportan

- Switches
- Sistemas Operativos
- Routers
- Impresoras
- Centrales Telefonicas (PABX)
- Otros

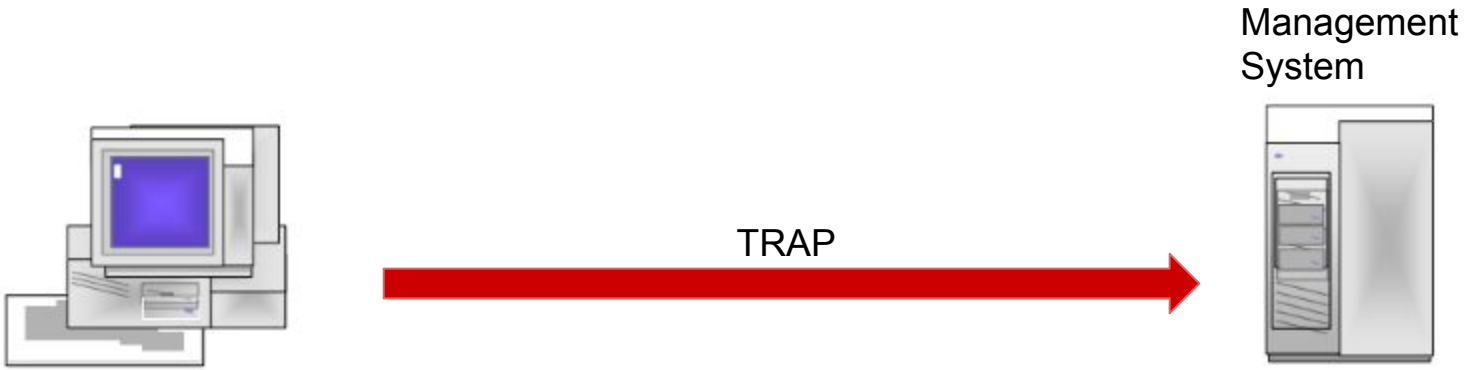
SNMP Mensajes

- **Get**, para obtener información
- **Set**, para asignarle valores a los objetos
- **Notify,** le permite a los agentes informar a la estacion de management.
- **Trap**, cuando ocurren eventos no planeados , los agentes que notan que un evento significativo ha ocurrido informan a todas las estaciones de management.

Tipos de eventos SNMP



Se realizan GET periódicos para chequear estado (ej: cada 60 seg)



El servidor/router/dispositivo informa un TRAP ante un evento

SNMP -MIB

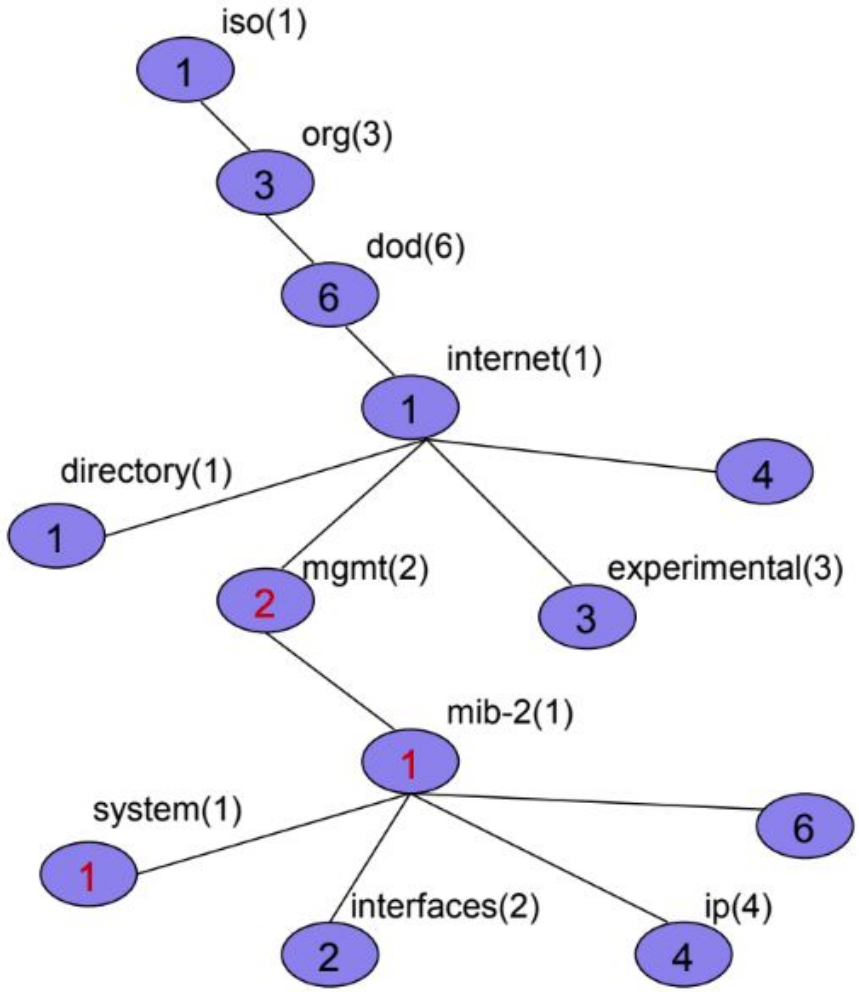
- Management Information Base
- Existen bases estandarizadas para dispositivos
- Otros utilizan bases privadas que proveen con el producto
- Archivos .MIB

SNMP -MIB

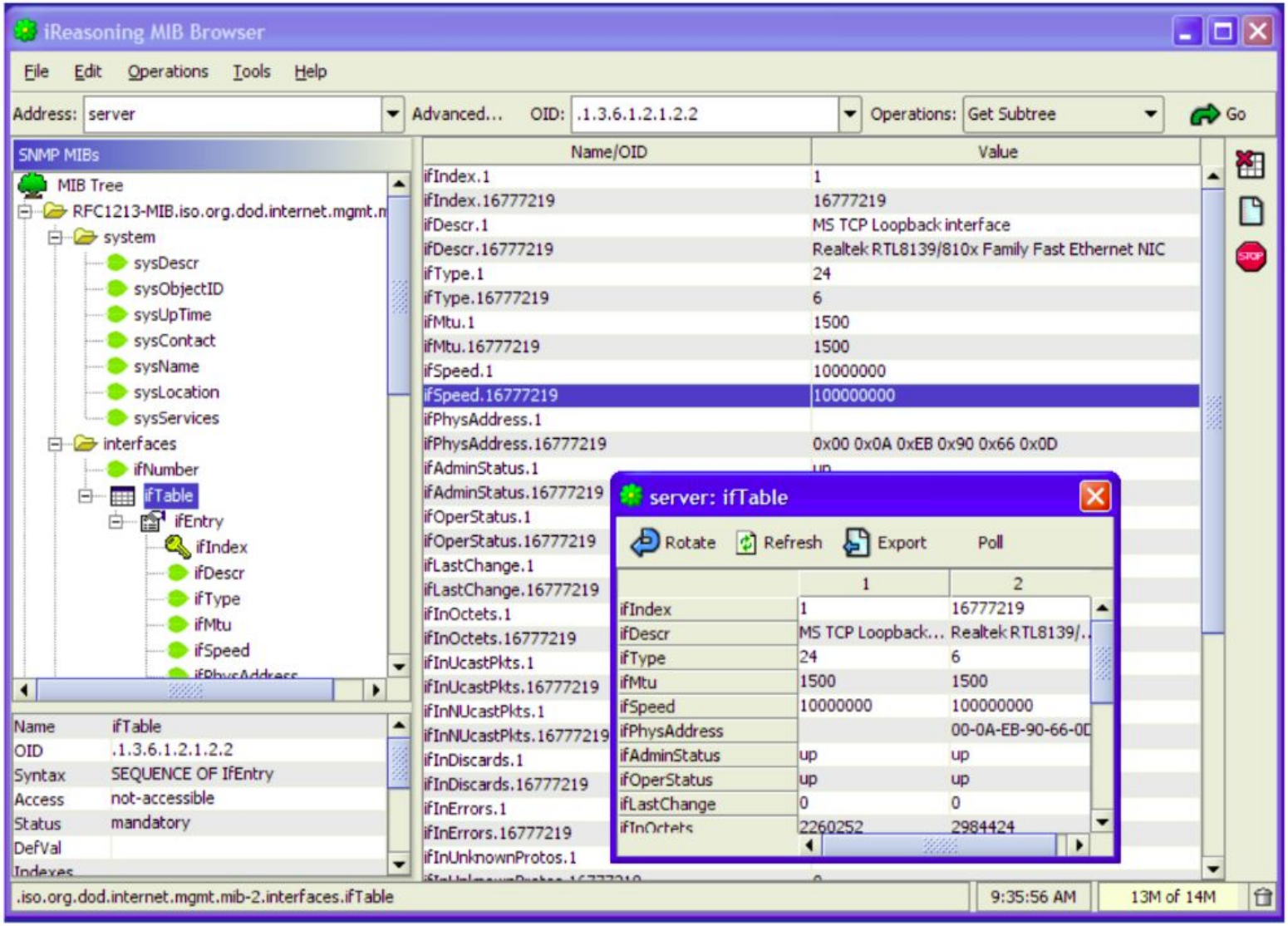
Object IDentifier (OID)

Ejemplo .1.3.6.1.2.1.1

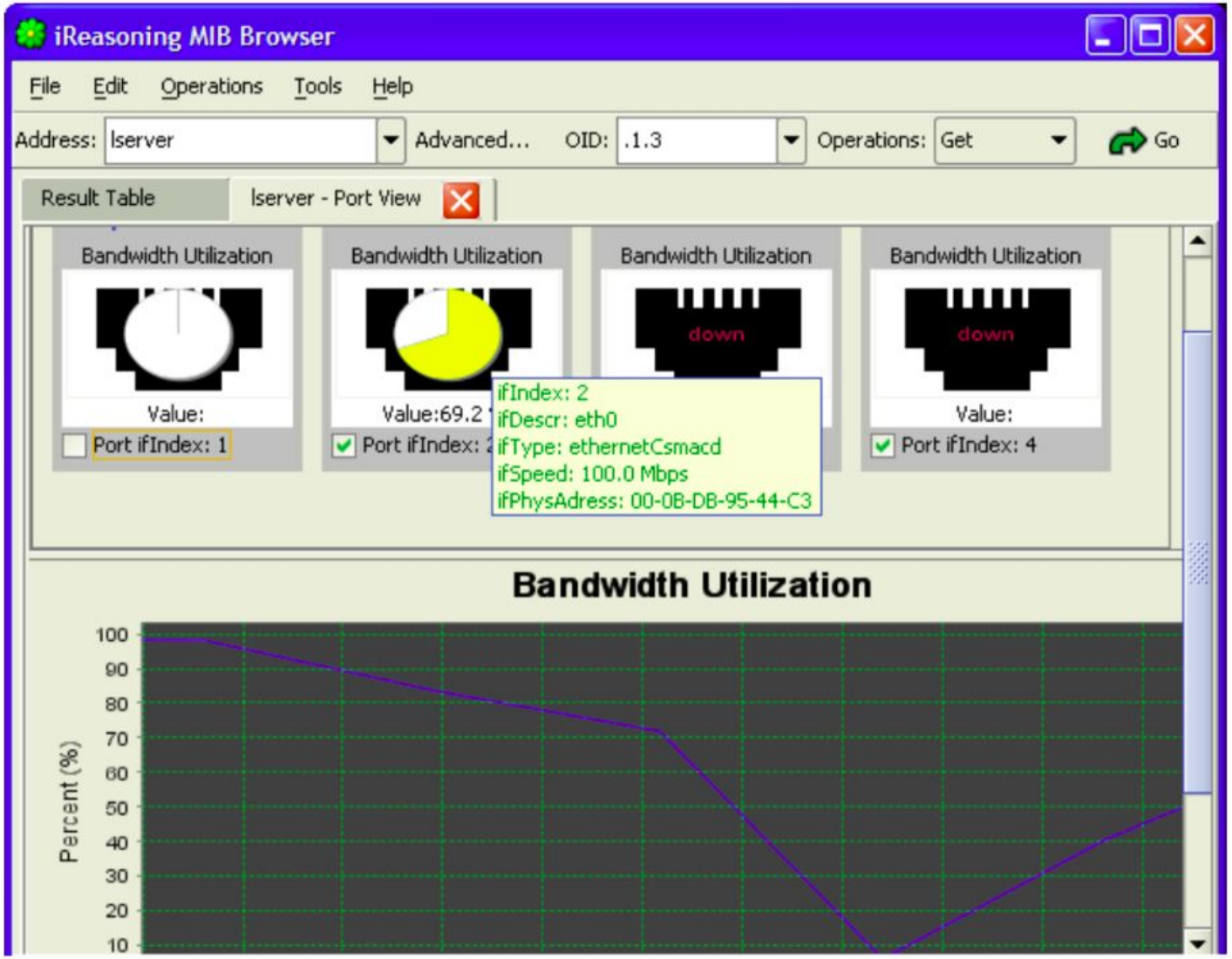
.iso.org.dod.internet.mgmt.mib-2.system



MIB Browser (1)



MIB Browser (2)



Aplicaciones para Monitoreo

- HP OpenView
- IBM Tivoli
- CA
- Nagios

Administración remota

- Servidor con fallas puede no aceptar conexiones remotas.
- Soluciones
  - HP iLO
  - Dell DRAC
  - Intel V-pro

Administración remota

- Placa de red extra o única
- Se configura la dirección IP en el BIOS (estática o dinámica)
- Se puede tomar gestión remota
- Se puede observar desde el arranque del servidor.