

Taller de Wiretapping

Teoría de las Comunicaciones

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

6 de Septiembre 2023

Objetivo

- Tomar dimensión de lo que implica conectarse y usar Internet.
- ARP
- Aprender a usar herramientas de Wiretapping para ver “en vivo” lo que sucede dentro de una red.
- Trabajo Práctico.



Primer acercamiento

¿Qué sucede cuando accedo a <http://www.dc.uba.ar/> desde el navegador?

Accedamos a una URL

- Accedo *http://dc.uba.ar*:
 - ➊ Se “dispara” una consulta para traducir *dc.uba.ar* a una **IP**.

Accedamos a una URL

- Accedo *http://dc.uba.ar*:
 - ➊ Se “dispara” una consulta para traducir *dc.uba.ar* a una **IP**.
 - ➋ Genera 3 mensajes para generar una conexión **TCP**.

Accedamos a una URL

- Accedo *http://dc.uba.ar*:
 - ① Se “dispara” una consulta para traducir *dc.uba.ar* a una **IP**.
 - ② Genera 3 mensajes para generar una conexión **TCP**.
 - ③ Hace un GET por **HTTP** para obtener el **HTML** de la web *dc.uba.ar*.

Accedamos a una URL

- Accedo *http://dc.uba.ar*:
 - ① Se “dispara” una consulta para traducir *dc.uba.ar* a una **IP**.
 - ② Genera 3 mensajes para generar una conexión **TCP**.
 - ③ Hace un GET por **HTTP** para obtener el **HTML** de la web *dc.uba.ar*.
 - ④ Envía otros 4 mensajes para cerrar la conexión **TCP**.

Accedamos a una URL

- Accedo *http://dc.uba.ar*:
 - ① Se “dispara” una consulta para traducir *dc.uba.ar* a una **IP**.
 - ② Genera 3 mensajes para generar una conexión **TCP**.
 - ③ Hace un GET por **HTTP** para obtener el **HTML** de la web *dc.uba.ar*.
 - ④ Envía otros 4 mensajes para cerrar la conexión **TCP**.
- No estamos teniendo en cuenta:
 - Mensajes entre nodos de la red para avisar que están disponibles.
 - Todos los mensajes que implican la consulta del punto 1.
 - Todo esto cambia si hacemos **stream de video**, **descargamos un archivo** o **subimos un fichero**.

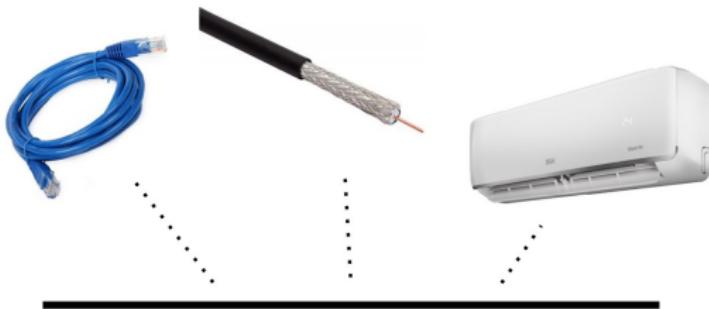
Accedamos a una URL

The screenshot shows the homepage of the Department of Computer Science (DC) at the University of Buenos Aires (UBA). The header features social media icons (Facebook, Twitter, YouTube, Instagram) and links for 'NOVEDADES' and 'AGENDA'. Below the header is a navigation bar with links for 'INICIO', 'INSTITUCIONAL', 'CARRERAS', 'INVESTIGACIÓN', 'EXTENSIÓN', 'COMUNIDAD DC' (which is highlighted in green), and 'CONTACTO'. The main content area has a dark blue background with a network-like pattern. A large white 'Ciencia' logo is centered, with the text 'Conocé nuestro Instituto de Investigación UBA/CONICET' below it. A green button labeled 'VISITAR SITIO' is present. At the bottom left, there is a link to the website: <https://www.dc.uba.ar/>.

Red de redes

¿Cómo hacemos para que el pedido viaje de nuestra máquina hasta el servidor de *dc.uba.ar*?

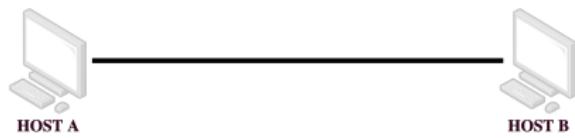
Medio físico



FISICA

- Nos abstraemos y le decimos *link* o *enlace*.
- ruido, señal, delay, ancho de banda, etc.

Red Punto-a-Punto

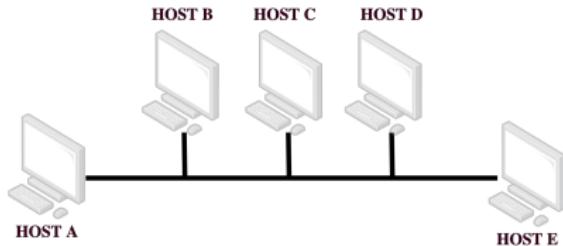


ENLACE

FISICA

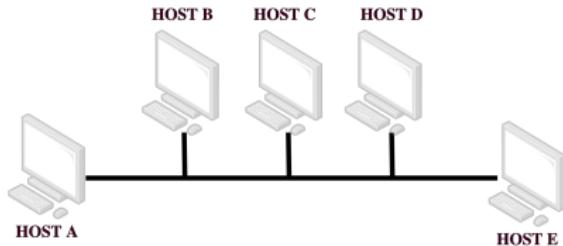
- Lo más básico: dos computadoras conectadas.
- A las computadoras las llamamos *hosts*.
- Cuando son 2: Red punto a punto
- Direccionamiento: MAC

Red de medios compartidos



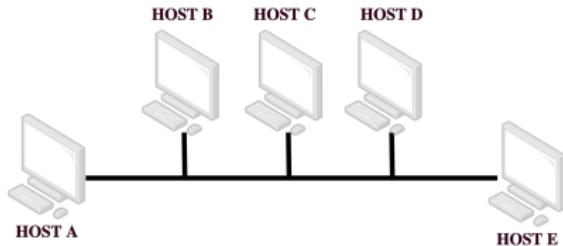
- Cuando son más: Medios compartidos.
- ¿Qué podemos encontrar acá?

Red de medios compartidos



- Cuando son más: Medios compartidos.
- **¿Qué podemos encontrar acá?**
 - Ethernet, WiFi.

Red de medios compartidos

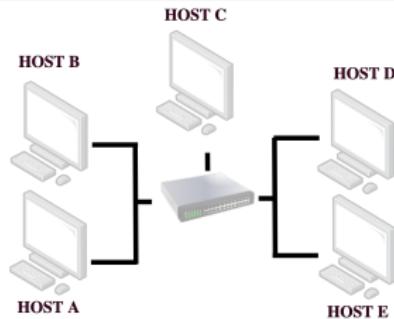


ENLACE

FISICA

- Cuando son más: Medios compartidos.
- ¿Qué podemos encontrar acá?
 - Ethernet, WiFi.
 - MAC Address
- Problema: Límite de hosts, de distancia.
- ¿Posibles soluciones?

Switches



ENLACE

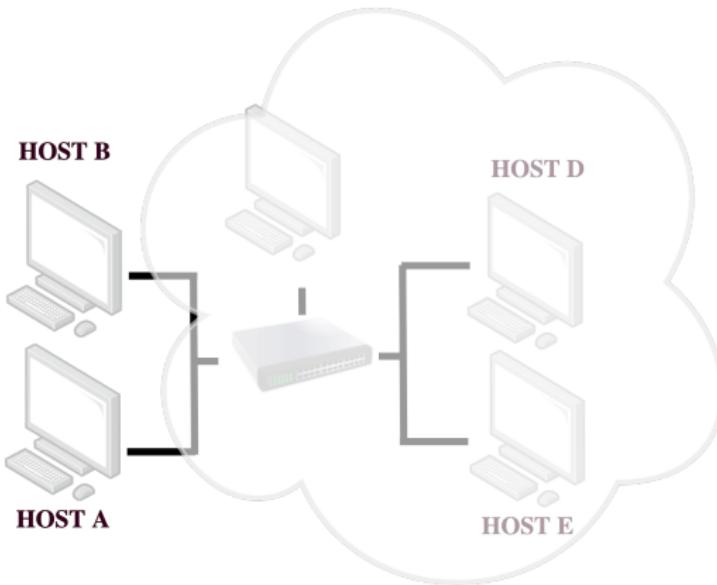
FISICA

- Dispositivos intermedios, **switches**.
- Reciben información por una entrada (*puerto*) y la **reenvían** (*forwarding*) por una salida (*puerto*).
- Tipo de redes “switcheadas” :
 - Circuito.
 - Paquetes.
- BPDU, ARP, etc.

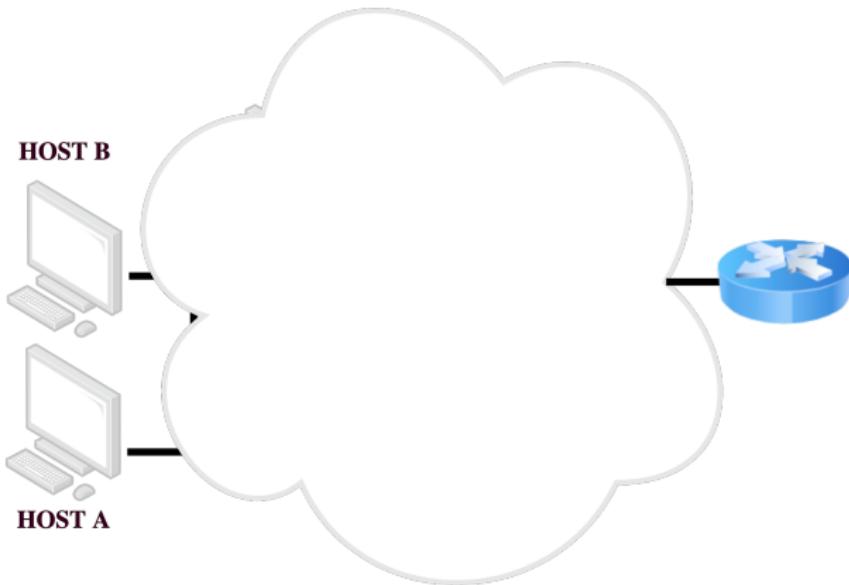
Red de redes

¿Cómo hacemos para conectar redes de cierto tipo (WiFi, Ethernet) con redes de tipos distintos o iguales?

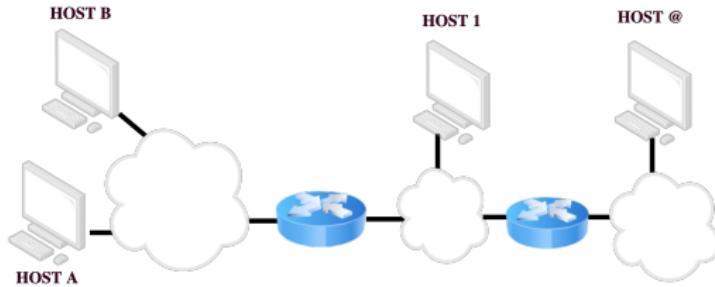
Red de redes



Red de redes



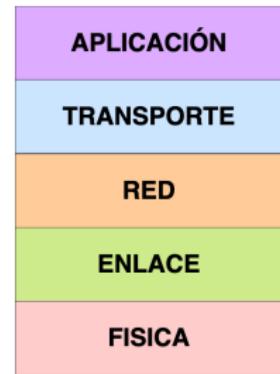
Red de redes



- Routers o gateways, reenvían paquetes.
- Direccionamiento: **IPs**.
- Red de redes, internetworking, Internet.

Red de redes

Finalmente..



Red de redes

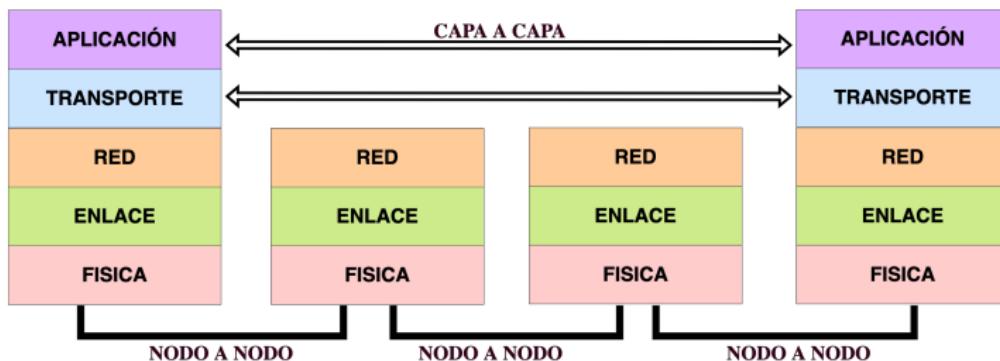
¿Pero cómo un dispositivo como un **switch** puede interpretar lo que manda un dispositivo como un **router**? ¿El router entiende HTTP? ¿El switch entiende TCP?

Arquitectura de red



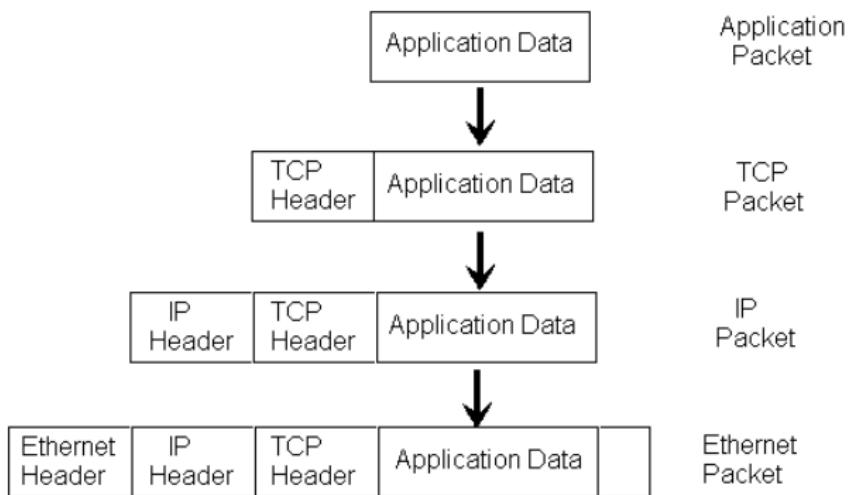
- Cada capa abstrae un nivel más al nivel físico.
- Cada capa define un **protocolo**.
- Cada capa provee servicios a su capa superior.

Arquitectura de red

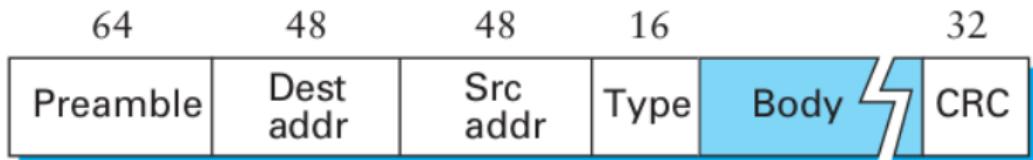


Encapsulamiento

Data Encapsulation into the Protocol Layers

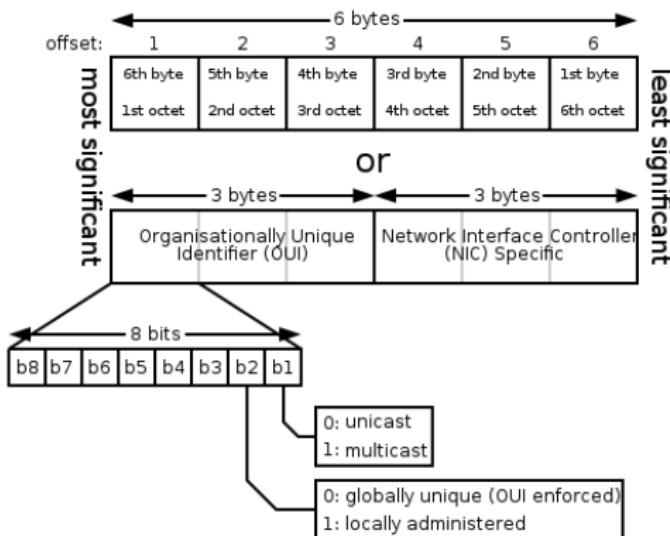


Ethernet



- Preamble: Sincronizar clocks.
- Type: A qué protocolo superior debería ser destinado.

Ethernet - MAC Address



Motivaciones

Cuáles son las capas que necesitan direccionamiento?

- Medios compartidos (MAC)
 - Dispositivos directamente conectados

Motivaciones

Cuáles son las capas que necesitan direccionamiento?

- Medios compartidos (MAC)
 - Dispositivos directamente conectados
- Red (IP)
 - Dispositivos **indirectamente** conectados

Motivaciones

Necesitamos traducir direcciones de capa de Red a direcciones físicas (ej. MAC address).

Primer approach - estático

- Se crea una tabla por host, dado una dirección IP nos dice su MAC.
- El administrador de red las actualiza por cada nueva IP en cada dispositivo.
- Que pasa si cambian las IPs?
 - Cualquier modificación implica mucho tiempo. Aunque se genera menos tráfico.

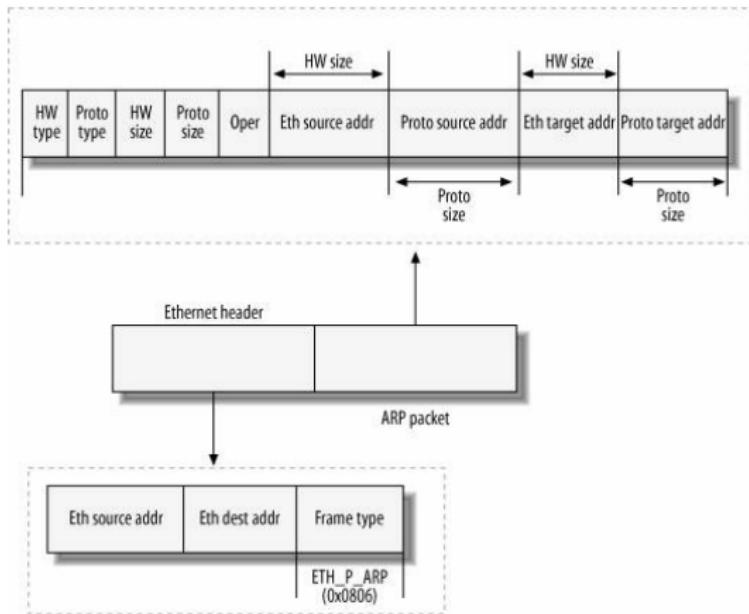
Segundo approach: ARP - dinámico

- La sigla: *Address Resolution Protocol*.
- Es un protocolo que, en esencia, permite mapear direcciones de nivel de red a direcciones físicas.
- Clave e indispensable en el funcionamiento de las redes modernas.
- Especificado en el RFC 826 (circa 1982).
- No está limitado a IP + Ethernet: la especificación es general.

Tecnicismos varios

- La pregunta ARP consiste en un mensaje **broadcast** sobre la red local.
 - Recordar que no se propaga más allá de la red local!
- La respuesta, en cambio, es **unicast**.
- Optimización: se implementa una caché (ARP table) para guardar las direcciones resueltas (o conocidas).
 - Las entradas se agregan al resolver o bien al observar un pedido de otra máquina.
 - Cada entrada tiene un tiempo de expiración para evitar problemas.

Pormenores del paquete



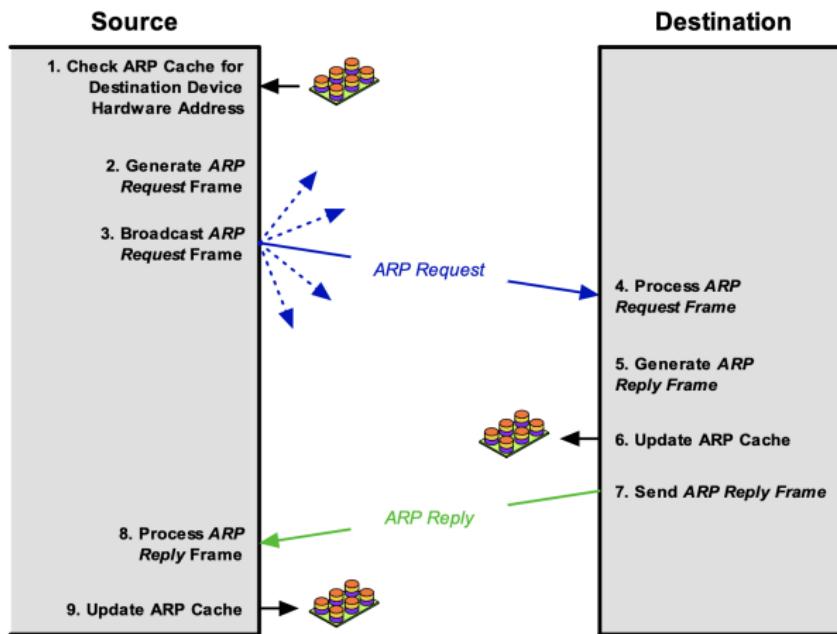
Pormenores del paquete (cont.)

- El campo **Oper** puede tomar los valores 1 (*who-has*) o 2 (*reply*).
- **HW type** y **Proto type** indican los protocolos de nivel de enlace y de nivel de red respectivamente involucrados en la comunicación.
- Observar que la cantidad de bits asignada a las direcciones depende del valor que tomen los campos **HW size** y **Proto size**.
- Dichos campos tienen un largo de 8 bits (i.e., direcciones con un máximo de $2^8 - 1 = 255$ bits).

Algoritmo

- Emisor manda un mensaje ARP broadcast con Oper = who-has
- Cada dispositivo que reciba el mensaje:
 - Si la IP no coincide, lo descarta.
 - Si la IP coincide, completa la MAC address y la envía al emisor con Oper = reply
 - El emisor de mensaje recibe el mensaje ARP y guarda en su tabla las direcciones (IP, MAC)
- La tabla ARP se limpia cada cierta cantidad de tiempo

Algoritmo



Algunas definiciones

- ¿NIC? Network Interface Controller (wlan0, eth0, lo, prueben haciendo ifconfig).

```
$ ifconfig
eth0:      flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
ether 3c:92:0e:33:4b:01  txqueuelen 1000  (Ethernet)
RX packets 0  bytes 0 (0.0 B)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 0  bytes 0 (0.0 B)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Algunas definiciones, cont.

Modo promiscuo

Los paquetes con MAC destino ajena no se descartan. Suben hasta el kernel para que podamos consumir las tramas. **Igual veríamos mensajes broadcast, multicast y unicast.**

Modo monitor

Permite capturar tráfico por medio del Wireless NIC, estando o no asociados con el AP o la red Ad-Hoc. En este modo se puede escuchar todo el tráfico de una red wireless.

Wireshark

- Es un analizador de paquetes.
- Nos permite observar la red o wiretappear la red.

Momento DEMO

[**GOTO Wireshark**]

¿Qué es Scapy?

- Scapy es un paquete de python para la manipulación de paquetes.
- Puede crear y descifrar paquetes de un gran número de protocolos.
- Puede enviar paquetes, capturarlos, analizarlos, unir pedidos con respuestas, y mucho más.
- Amplia funcionalidad que permite reemplazar otras herramientas (nmap, arping, tcpdump, etc.).
- Multiplataforma, libre, abierto, gratis y hecho en python
- Más info ⇒ <http://www.secdev.org/projects/scapy/>

Cómo instalar Scapy

Para python 3.*:

```
pip3 install scapy  
sudo apt-get install python3-scapy  
conda install -c conda-forge scapy
```

Taller time!

Nobody:
Bugs right before a demo:



Introducción

ARP

Sniffing

Scapy

Trabajo Práctico 1: Wiretapping

Tips

Más material

Trabajo práctico

CONSIGNA

Trabajo práctico

- 10K tramas POR red.
- Es importante la manera de exponer los resultados
 - Gráficos
 - Tablas
 - Referencias

NO “el gráfico de la página anterior”
SI “Como se observa en la Figura X”
- No dar cosas por obvias. Explicar.
- Plantear hipótesis.

Referencias

- Wireshark (página web oficial) <http://www.wireshark.org>
- Scapy (página web oficial) <http://www.secdev.org/projects/scapy/>
- Scapy Doc <https://scapy.readthedocs.io/en/latest/>
- Berkeley Packet Filter <http://biot.com/capstats/bpf.html>
- Tutoriales de Scapy <https://thepacketgeek.com/scapy-p-01-scapy-introduction-and-overview/>
- Troubleshooting modos NIC <https://www.wireshark.org/faq.html#q6.1>