Trabajo Practico 6

Colazo, Agustín

Passaglia, Nicolás

Aimaretto, Lucas

Leonhardt, Elisabeth

Facultad de Ciencias Exactas, Físicas y Naturales.

Universidad Nacional de Córdoba

31/10/2017

Ejercicio 1

¿Que es lo que se ve en cada capa?

El protocolo resolución de direcciones (ARP) es un protocolo de capa de enlace, este protocolo sirve para encontrar la dirección MAC que se asocia con una determinada dirección ip. Ademas, este protocolo funcione a nivel de la red local.

En Wireshark solo vemos dos capas y el protocolo ARP que va por encima de la capa de enlace. En estos mensajes no hay capa de red.

En la capa de enlace se observa que se utiliza el protocolo ARP, se observa la MAC origen de la trama, y la MAC destino.

El mensaje transportado ARP tiene la MAC origen y la ip origen. En caso de conocer la MAC destino, hay un campo que la contiene. Si no se conoce, este campo lleva 00.00:00.00:00.00. Y la ip destino.

```
> Frame 125: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: Apple_77:29:8b (60:92:17:77:29:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: Apple_77:29:8b (60:92:17:77:29:8b)
      Type: ARP (0x0806)
v Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: Apple_77:29:8b (60:92:17:77:29:8b)
      Sender IP address: 10.0.0.34
      Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Target IP address: 10.0.0.2
```

¿Que se puede decir con respecto a la frecuencia con la que aparecen los mensajes?

Los mensajes ARP aparecen cada 40-50 segundos preguntando por la ip del host 10.0.0.110. Esto se relaciona con el tiempo de vida en cache de la tabla ARP en el router de la red local. El funcionamiento de cuando vuelve a hacer un pedido en el protocolo ARP difiere de router a router.

En este caso el router que utilizado es un router/modem de Arnet.

Antes de que se venza el plazo de vida de la entrada en la tabla ARP, el router enviá un mensaje a la MAC que aparece en la tabla, que se corresponde con esa dirección ip. Si este host sigue conectado a la red, y tiene la misma ip, responderá al router con un mensaje ARP. En este caso no se utiliza la dirección de broadcast de MAC.

La ip del host es 10.0.0.110 y la ip del router es 10.0.0.2.

arp

No.	Time	Source	Destination	Protocol	Length	Info
713	42.077149	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
714	42.077197	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
1801	91.794824	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
1802	91.794870	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
2260	141.731320	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
2261	141.731373	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
2339	180.094805	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
2340	180.094855	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
2409	220.324307	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
2410	220.324352	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
2458	255.731115	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
2459	255.731165	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
2593	292.029375	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
2594	292.029415	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
2666	339.496836	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
2667	339.496883	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f
3730	394.539309	AdbBroad_05:66:5d	RivetNet_e7:8e:4f	ARP	42	Who has 10.0.0.110? Tell 10.0.0.2
3731	394.539354	RivetNet_e7:8e:4f	AdbBroad_05:66:5d	ARP	42	10.0.0.110 is at 9c:b6:d0:e7:8e:4f

Cuando no se conoce la dirección física del destino, se enviá el mensaje por broadcast. Y aquel que tenga esa dirección ip, responderá con su MAC.

¿Cuales son las entradas en la tabla ARP del host?

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\tin>arp -a

Interface: 10.0.0.110 --- 0xe
  Internet Address      Physical Address      Type
  10.0.0.2              74-88-8b-05-66-5d     dynamic
  10.0.0.202            00-56-cd-31-93-1b     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Las entradas estáticas no tienen tiempo de vida en cache, mientras que las entradas dinámicas si.

10.0.0.2 es la dirección ip del gateway. Y 10.0.0.202 corresponde a otro host conectado en la red local.

¿Es posible ver la tabla ARP del router? ¿Como se ve dicha tabla?

En el router de la red local a la que se esta conectado no se puede acceder a la tabla ARP del router. El router que se esta utilizando es un router/modem de Arnet.

Pero en un router Cisco si se puede ver la tabla del mismo usando el comando “show arp”.

Ejercicio 2

Protocolo	MAC origen en trama	MAC destino en trama	IP origen en datagrama	IP destino en datagrama	Contenido
ARP	2FE8:A101:B1E1	FFFF:FFFF:FFFF	-	-	Who has 192.168.1.20? Tell 192.168.1.10
ARP	2FE8:A102:B1F1	2FE8:A101:B1E1	-	-	192.168.1.20 is at 2FE8:A102:B1F1
ICMP	2FE8:A101:B1E1	2FE8:A102:B1F1	192.168.1.10	192.168.1.20	Ping request
ICMP	2FE8:A102:B1F1	2FE8:A101:B1E1	192.168.1.20	192.168.1.10	Ping reply

Ejercicio 3

a)

Protocolo	MAC origen en trama	MAC destino en trama	IP origen en datagrama	IP destino en datagrama	Contenido
ARP	0026:183A:3B3C	FFFF:FFFF:FFFF	-	-	Who has 10.0.0.1? Tell 10.0.0.10
ARP	0040:0B4C:2701	0026:183A:3B3C	-	-	10.0.0.1 is at 0040:0B4C:2701
ICMP	0026:183A:3B3C	0040:0B4C:2701	10.0.0.10	10.0.3.10	Ping request
ARP	0040:0B4C:2701	FFFF:FFFF:FFFF	-	-	Who has 10.0.3.10? Tell 10.0.3.1
ICMP	0040:0B4C:2701	0026:183A:3B3C	10.0.0.1	10.0.0.10	Destination Host Unreachable

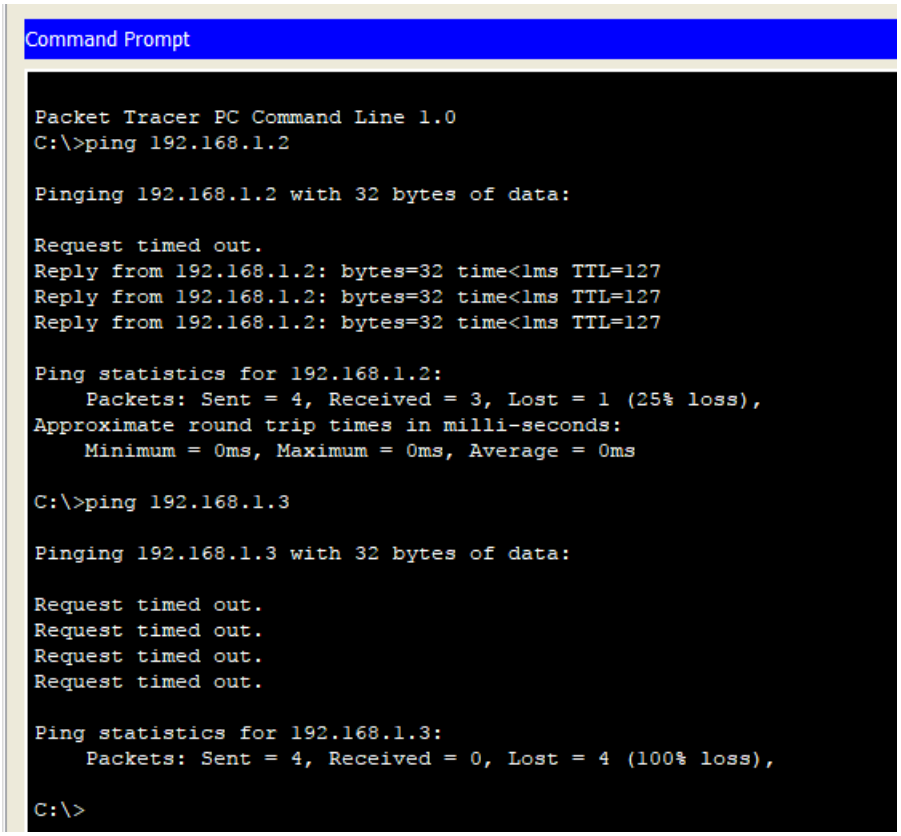
Algunos routers de Cisco descartan los paquetes que van a un destino cuando no hay ninguna entrada ARP en la tabla que se asocie con esa dirección ip. Este comportamiento es para evitar que el router se quede esperando una respuesta ARP que posiblemente no vaya a llegar. La RFC 1812 dice que el router no debe responder con un ICMP Destination Unreachable solo porque no haya una entrada en la tabla ARP.

Es posible que esta RFC haya sido actualizada por otra. Pero el router 1841 que se uso en la simulación de Cisco Packet Tracer tiene este comportamiento o similar.

Fuente

Este es un caso análogo simulado en Packet Tracer que muestra esta situación. Si bien las direcciones ip no son las mismas, el caso es igual.

Acá se observa que el router 1841 no envía el mensaje ICMP de error, sino que el ping request vence por time-out.



b)

Protocolo	MAC origen en trama	MAC destino en trama	IP origen en datagrama	IP destino en datagrama	Contenido
ICMP	0026:183A:3B3C	0040:0B4C:2701	10.0.0.10	10.0.3.5	Ping request
ARP	0040:0B4C:2701	FFFF:FFFF:FFFF	-	-	Who has 10.0.3.5? Tell 10.0.3.1
ARP	0026:183B:3D3C	0040:0B4C:2701	-	-	10.0.3.5 is at 0026:183B:3D3C
ICMP	0040:0B4C:2701	0026:183B:3D3C	10.0.0.10	10.0.3.5	Ping Request
ICMP	0026:183B:3D3C	0040:0B4C:2701	10.0.3.5	10.0.0.10	Ping Reply
ICMP	0040:0B4C:2701	0026:183A:3B3C	10.0.3.5	10.0.0.10	Ping Reply

Ejercicio 4

1)

	SW1	SW2	SW3	SW4	SW5
BRIDGE ID	0003.E4A0.BEC5	0060.3ECB.A65A	000B.BEC5.07C7	00E0.F752.4236	00E0.F702.0CAC
ROOT ID	0003.E4A0.BEC5	0003.E4A0.BEC5	0003.E4A0.BEC5	0003.E4A0.BEC5	0003.E4A0.BEC5

2)

El ROOT ID de esta red es 0003.E4A0.BEC5 (dirección MAC del switch). Cabe destacar que cada interfaz del switch tiene su propia mac, pero a los propósitos del algoritmo spanning tree, solo importa el bridge id que es único para cada switch.

Todos los switches tienen el mismo costo, y la prioridad de los switches no se modifico. Por tanto se selecciona como Root Bridge el switch con menor numero de Bridge ID. Esto se observa en la tabla.

No puede haber dos Root Bridge en una misma red local.

Si hay varias VLAN en una misma red local física, si pueden haber distintos Root Bridge. Pero un solo Root Bridge por VLAN.

Para cada LAN o VLAN, el Root Bridge es el switch que tiene el bridge priority mas bajo. En caso de conflicto, se elige el switch con menor numero de MAC.

3) Mencione los estados que atraviesa un puerto.

Los puertos atraviesan cinco estados: Bloqueando, escuchando, aprendiendo, reenviando y deshabilitado.

- Bloqueo: En este estado, la interfaz de capa 2 no participa en el reenvió de mensajes, pero se pueden recibir BPDU's. Las tramas de datos se descartan. Los switch comienzan en este estado ya que sino podrían generarse bucles en la red. No se guardan las direcciones MAC en la tabla.
- Escucha: Este estado es el primero luego de la fase de bloqueado cuando el algoritmo spanning tree determina si la interfaz de capa 2 debe participar en el reenvió de mensajes. En caso de que no sea así, este vuelve al estado de bloqueo. En este estado se procesan las BPDU. No se guardan las direcciones MAC en la tabla.
- Aprendizaje: En este estado, la interfaz de capa 2 se prepara para el reenvió de mensajes. Se descartan las tramas de datos pero se guardan las direcciones MAC en la tabla. Se procesan la BPDU.
- Reenvió: En este estado, la interfaz recibe y enviá datos. Se procesan las BPDU. También se actualiza la tabla de direcciones MAC.

- Deshabilitado: En este estado, la interfaz no participa en el spanning tree y no reenviá mensajes. No se procesan BPDU. Se llega a este estado cuando se deshabilita la interfaz o esta falla.

Esta información se tomo de las siguientes fuentes:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/spantree.html#61228

https://es.wikipedia.org/wiki/Spanning_tree

4) Que es un puerto designado?

Los puertos designados, son los puertos de un switch que otros switches utilizan (o podrían utilizar) para alcanzar el Root Bridge. El puerto designado de un segmento es el que tiene el menor costo de camino para alcanzar el Root Bridge.

En un switch puede haber varios puertos designados. Todas los puertos del Root Bridge son designados.

En un segmento donde hay un puerto designado, el otro puerto del segmento sera un puerto no designado o root.

5) Que es un puerto root?

Un puerto root es el puerto de un switch que tiene el menor costo desde el switch hasta el Root Bridge. En un switch hay un solo puerto root. El único switch sin puertos root es el Root Bridge.

En un segmento donde hay un puerto root, el otro puerto del segmento sera un puerto designado.

6) Que es un puerto bloqueado?

Los puertos bloqueados o no designados son puertos que siempre estarán en el estado de bloqueo, para asi evitar los bucles en la red. Los puertos bloqueados son también puertos alternativos. En caso de que falle un enlace, proveen rutas alternativas.

Cuando un switch puede elegir varios puertos root, elige el de menor costo, y el resto de los puertos candidatos a root se bloquean.

En un segmento donde hay un puerto bloqueado, el otro puerto sera un puerto designado.

Ejercicio 5

1) Si tuviera que usar diagramas de Venn para explicar la diferencia entre un dominio de colisión (DC) y un dominio de broadcast (DB). Como seria tal explicacion?

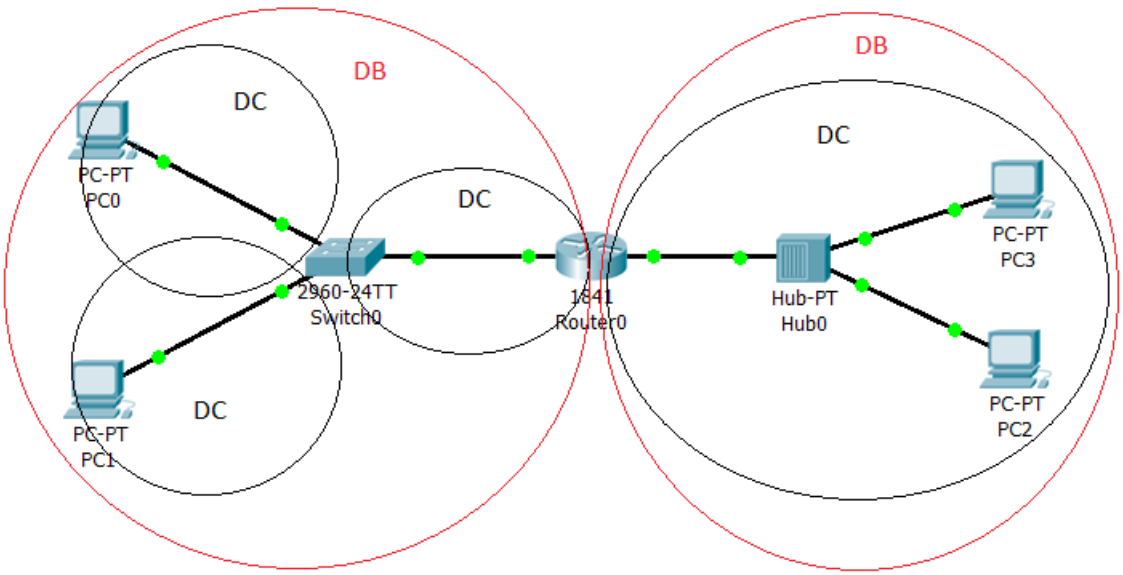
Un dominio de colisión es un segmento físico de una red de computadoras donde las tramas pueden colisionar. Los dominios de colisión se dan en una red física. La red física puede ser un dominio de colisión o puede tener varios dominios de colisión. Esta red física puede ser una LAN o varias VLAN.

Un dominio de difusión es el área lógica de una red en que todas las computadoras se pueden enviar mensajes directamente. Los dominios de difusión se encuetran en una LAN o VLAN, comparten una subred y una dirección de difusión.

Los hubs extienden el dominio de colisión, mientras que los switches lo limitan. Esto es porque el hub repite los mensajes que le llegan a una interfaz por todos los otros puertos. Mientras que los switches aprenden los puertos a los que están conectados los distintos dispositivos, a través de su dirección física. Cuando llega un mensaje a un puerto, actualizan la tabla con esa dirección MAC. Cuando reenvían un mensaje, buscan en la tabla la interfaz correspondiente y envían el mensaje por ahí. Si no se encuentra en la tabla, envían el mensaje por todas las otras interfaces.

Por otro lado los routers limitan el dominio de broadcast. Puede haber varias subredes conectadas directamente a un router, donde cada subred es un dominio de broadcast.

En el siguiente diagrama podemos ver un hub, un switch y un router. El switch divide los dominios de colisión, cada dominio de colisión pasa a ser el segmento que conecta al switch, y a la computadora o router. Mientras que el hub extiende el dominio de colisión, todos los elementos conectados directamente al hub pasan a ser parte del dominio de colisión. Cada LAN es un dominio de difusión, ya que cualquier computadora puede enviar un mensaje directamente a otra computadora en la LAN. En este caso los dominios de colisión están contenidos en el dominio de broadcast. Cuando NO se utiliza VLANS, los dominios de colisión están contenidos o son igual al dominio de broadcast. Pero cuando se



utiliza VLAN’s este no es el caso, y los dominios de colisión pueden contener a los dominios de difusión.

Otro caso en que se usan diagramas de Venn es en el ejercicio siguiente. En esa imagen solo se dibujan los dominios de colisión y de broadcast de interés, aunque hay otros presentes:

- Dominio de colisión y broadcast en el segmento entre routers, o entre routers y switches.
- Dominio de colisión entre cada computadora y la interfaz del switch a la que esta conectada.
- En el caso de hubs, el dominio de colisión es también un dominio de broadcast.

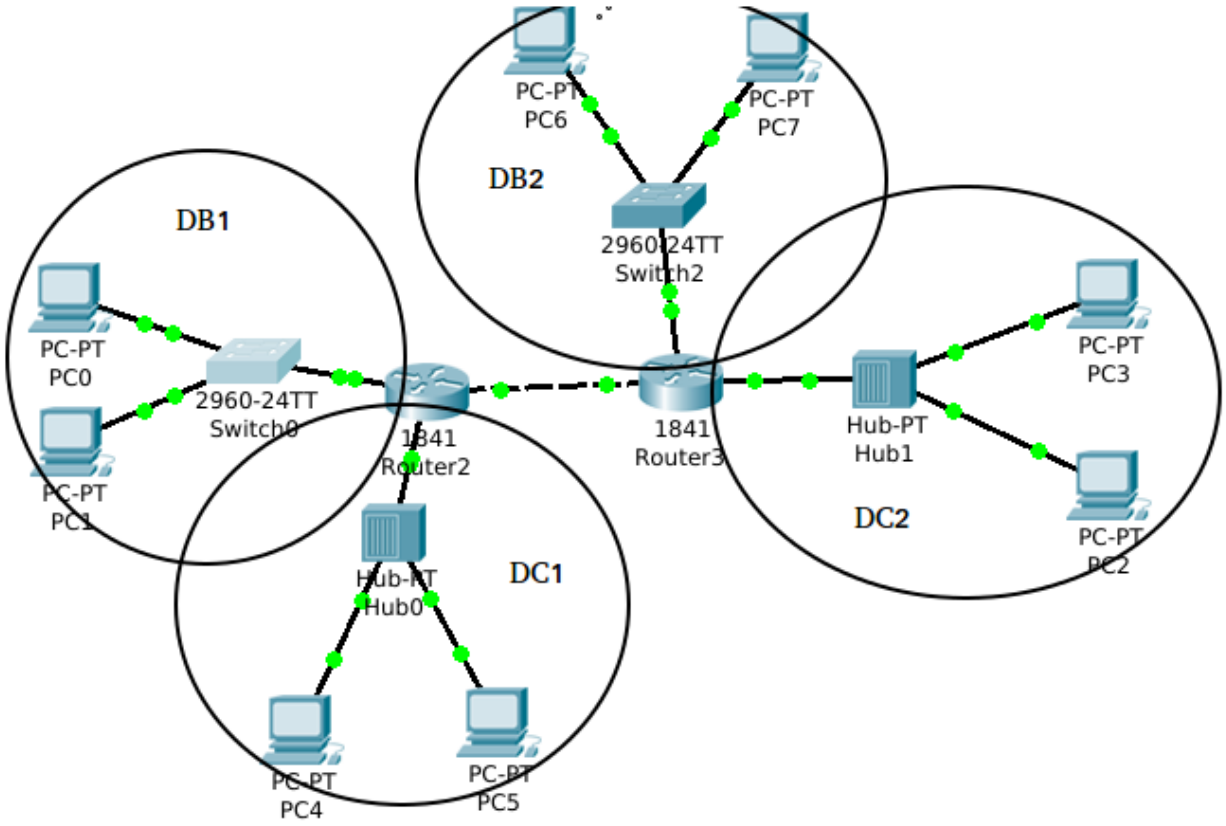
2) Diagrame una red de 8 computadoras de tal forma que:

a. 2 PCs en un DC1

b. 2 PCs en un DB1

c. 2 PCs en un DC2

d. 2 PCs en un DB2



Bibliografía

https://technet.microsoft.com/en-us/library/cc958841.aspx

https://technet.microsoft.com/en-us/library/cc754761(v=ws.11).aspx

https://learningnetwork.cisco.com/thread/24460

https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones

https://learningnetwork.cisco.com/thread/61454

http://blog.e2h.net/2009/12/01/analisis-de-red-con-wireshark/

http://www.omnisecu.com/cisco-certified-network-associate-ccna/how-spanning-tree-protocol-stp-select-root-port.php

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/spantree.html#61228

http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-a-designated-port.php

https://supportforums.cisco.com/t5/lan-switching-and-routing/stp-root-port-vs-designated-port/td-p/1517842

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/spantree.html#pgfId-1083116

https://seguinfo.wordpress.com/2012/09/02/dominio-de-colision-y-dominio-de-broadcast/

https://es.wikipedia.org/wiki/Dominio_de_difusi%C3%B3n

https://es.wikipedia.org/wiki/Dominio_de_colisi%C3%B3n