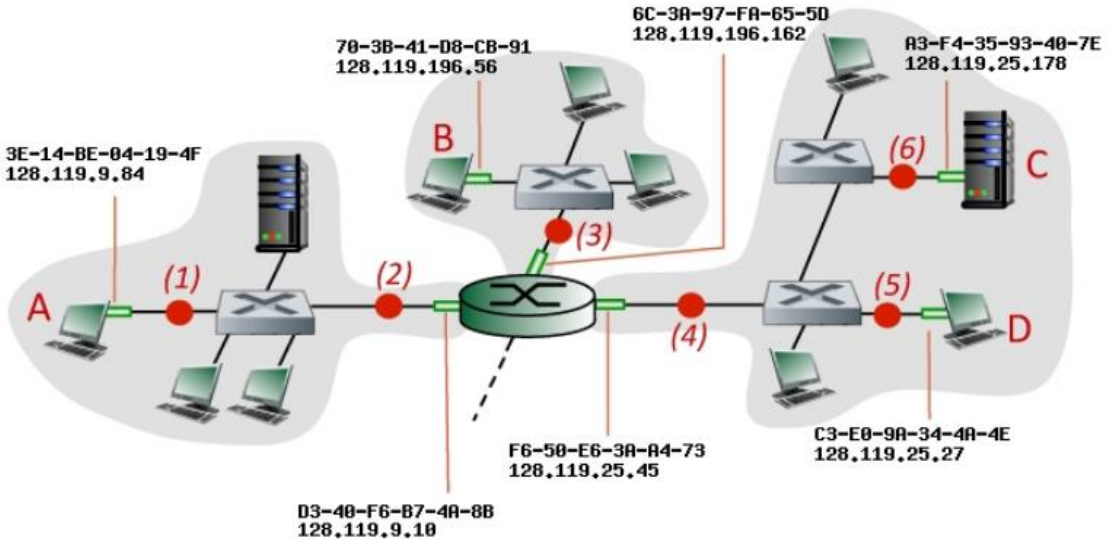
GII TDRC
TEMA 3: Arquitecturas y Servicios de Redes Corporativas (Capa de Enlace)
- Relación de Problemas -

1) Considere la topología de la figura, en la que se muestran las **direcciones IP y MAC** de los interfaces de los nodos (hosts) A, B, C y D, así como las de los interfaces del router. Las Tablas ARP (hosts y routers) y las Tablas de Conmutación (Switches) están completas.
   a) Suponga que se envía un datagrama desde A hasta B. Indique las direcciones IP y Ethernet origen y destino consideradas en los puntos (1), (2) y (3).
   b) Indique las mismas direcciones si se envía un datagrama desde C hasta B en los puntos (6), (4) y (3).
   c) Indique las mismas direcciones si se envía un datagrama desde D hasta C en los puntos (5) y (6).



Las Tablas ARP están completas, por lo que se sabe enviar tramas a todos los equipos de las subredes (se conocen sus MAC).
Las Tablas de Conmutación de los switches están completas, por lo que se sabe por qué puerto enviar las tramas con destino a una MAC.

La trama Ethernet incluye información de dirección Ethernet (MAC) de origen y destino, así como las direcciones IP de origen y destino de la capa de red (encapsuladas en los datos de la trama).
Las IPs origen y destino se mantienen en todos los saltos (van en capsuladas y sólo se pueden ver en el destino).

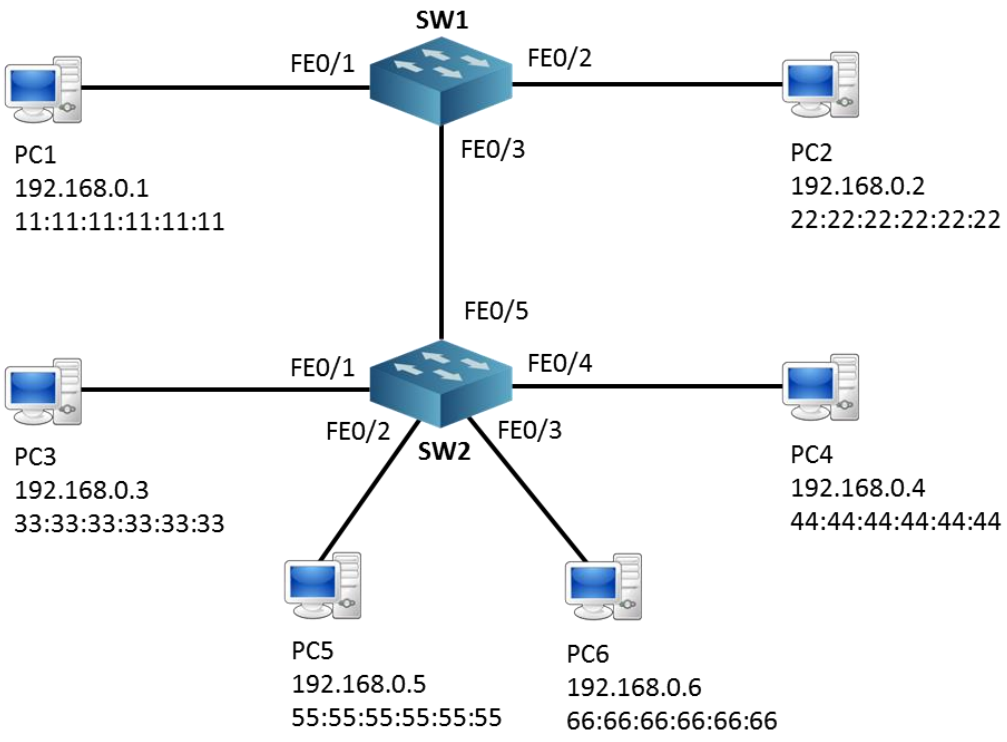
a) Envío desde A a B
A nivel de cada de red, se sabe que la IP de destino está en otra subred, así que A se lo enviaría a su Default Gateway para el reenvío a la otra subred.
En el punto *(1)*:
Ethernet origen: 3E-14-BE-84-19-4F, Ethernet destino: D3-40-F6-B7-4A-8B
IP origen: 128.119.9.84, IP destino: 128.119.196.56
En el punto *(2)*:
Lo mismo que en el punto (1)
El swich es “transparente”, no cambia nada en las tramas.

En el punto *(3)*:
Ethernet origen: 6C-3A-97-FA-65-5D, Ethernet destino: 70-3B-41-D8-CB-91
IP origen: 128.119.9.84, IP destino: 128.119.196.56

b)
En el punto *(6)*:
Ethernet origen: A3-F4-35-93-40-7E, Ethernet destino: F6-50-E6-3A-A4-73
IP origen: 128.119.25.178, IP destino: 128.119.196.56
En el punto *(4)*:
Lo mismo que en punto (6)
En el punto *(3)*:
Ethernet origen: 6C-3A-97-FA-65-5D, Ethernet destino: 70-3B-41-D8-CB-91
IP origen: 128.119.25.178, IP destino: 128.119.196.56

c)
En el punto *(5)*:
Ethernet origen: C3-E0-9A-34-4A-4E, Ethernet destino: A3-F4-35-93-40-7E
IP origen: 128.119.25.27, IP destino: 128.119.25.178
En el punto *(6)*:
Lo mismo que en punto (5)

2) En la red mostrada en la figura en la que se indican las direcciones IP y MAC de los diferentes hosts, el PC3 hace una petición *ARP Request* para enviar un paquete a la IP 192.168.0.2 (PC2). Suponiendo que las Tablas ARP de todos los hosts están vacías:
   a) Indique la **secuencia de tramas ARP** que se producen en toda la red en cada instante, puede rellenar una tabla como la que se incluye.
   b) Si después de esa petición, se hace otro *ARP Request* desde PC1 para averiguar la MAC de PC4, muestre las **Tablas de Conmutación** de los switches una vez recibida la respuesta (*ARP Reply*) en PC1.



Tramas ARP generadas en cada instante:

Instante	MAC origen	MAC destino	IP origen	IP destino
1	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a SW2	192.168.0.3	192.168.0.2
2	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 44:44:44:44:44:44	192.168.0.3	192.168.0.2
2	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 55:55:55:55:55:55	192.168.0.3	192.168.0.2
2	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 66:66:66:66:66:66	192.168.0.3	192.168.0.2
2	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a SW1	192.168.0.3	192.168.0.2
3	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 11:11:11:11:11:11	192.168.0.3	192.168.0.2
3	33:33:33:33:33:33	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 22:22:22:22:22:22	192.168.0.3	192.168.0.2
4	22:22:22:22:22:22	Ethernet(33:33:33:33:33:33) ARPReply(22:22:22:22:22:22) Llega a SW1	192.168.0.2	192.168.0.3
5	22:22:22:22:22:22	Ethernet(33:33:33:33:33:33) ARPReply(22:22:22:22:22:22) Llega a SW2	192.168.0.2	192.168.0.3
6	22:22:22:22:22:22	Ethernet(33:33:33:33:33:33) ARPReply(22:22:22:22:22:22) Llega a PC3	192.168.0.2	192.168.0.3

a) PC3 intenta obtener la MAC del equipo PC2 (192.168.0.2).
Para la secuencia hay que tener en cuenta que el ARP Request se envía por broadcast, por lo que los switches lo envían por todos sus puertos excepto por el que les llegó.

Instante 1 → PC3 envía el ARP Request
Instante 2 → SW2 envía por broadcast a todos los demás (PC5, PC6, PC4) y a SW1.
El destino sigue siendo broadcast, por lo que los PCs que lo reciban y no sean destino, simplemente descartan los paquetes.
Instante 3 → SW1 envía por broadcast a todos los demás (PC1, PC2).
El destino sigue siendo broadcast, por lo que los PCs que lo reciban y no sean destino, simplemente descartan los paquetes.
PC2 recibe el paquete que lleva su IP.
Apunta la MAC de origen en su tabla ARP.
Instante 4 → PC2 envía su ARP Reply.
Va dirigido a la MAC de PC3.
Llega a SW1

Instante 5 → SW1 se lo pasa a SW2 (de forma transparente)
Instante 6 → SW2 se lo pasa a PC3.
Apunta la respuesta en su tabla ARP.

En las Tablas ARP sólo apuntan los que son destinatarios de las tramas.
Se añade un TTL a cada entrada.

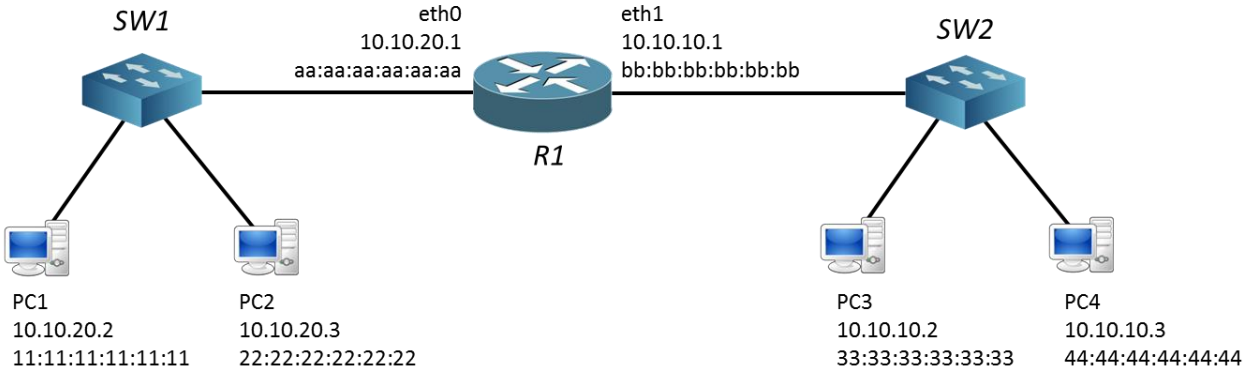
b) Las tablas de conmutación al principio están vacías y se manda todo por broadcast, pero cuando van recibiendo tramas por puertos, apuntan la MAC de origen de las mismas y el puerto por el que llegan.
Después de las dos peticiones y respuestas, las Tablas de Conmutación serían:

Tabla de Conmutación SW2:
33:33:33:33:33:33 – FE0/1 – Instante 1
22:22:22:22:22:22 – FE0/5 – Instante 5
-
11:11:11:11:11:11 – FE0/5
44:44:44:44:44:44 – FE0/4

Tabla de Conmutación SW1:
33:33:33:33:33:33 – FE0/3 – Instante 2
22:22:22:22:22:22 – FE0/2 – Instante 4
-
11:11:11:11:11:11 – FE0/1
44:44:44:44:44:44 – FE0/3

Se apunta el tiempo en el que llegó, porque las entradas se van borrando pasado un tiempo sin que se hayan actualizado.

3) Dada la topología de red mostrada, en la que se indican las direcciones IP y MAC de los diferentes interfaces y suponiendo que las Tablas ARP de todos los nodos (hosts y router) están vacías. Las tablas de enrutamiento están completas y todos los PCs tienen como *Default Gateway* a R1 (interfaz en su subred).
   a) Indique en una tabla todas las tramas ARP generadas para poder realizar un envío de un paquete ICMP (ping) desde PC1 hasta PC3. Incluya un número que indique el instante de tiempo en el que se producen (considere instantes numerados secuencialmente comenzando en 1).
   b) Muestre las tablas ARP de cada nodo al finalizar esta transmisión del paquete.
   c) En la situación actual, indique de nuevo las tramas ARP generadas antes del envío de un paquete IP entre PC3 y PC2.



a)
Tramas ARP generadas en cada instante ANTES DEL ENVÍO DEL PAQUETE ICMP:

Hay que hacer PROXY ARP:
PC1 tendrá como default gateway a R1
En el instante 1 se enviará la trama ARP preguntando por la MAC del router (MAC destino sería FFFFFFFFFF a nivel de Ethernet y 000000000 en la trama ARP.

Instante	MAC origen	MAC destino	IP origen	IP destino
1	11:11:11:11:11:11	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a SW1	10.10.20.2	10.10.20.1
2	11:11:11:11:11:11	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 22:22:22:22:22:22	10.10.20.2	10.10.20.1
2	11:11:11:11:11:11	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a aa:aa:aa:aa:aa:aa (R1)	10.10.20.2	10.10.20.1
3	aa:aa:aa:aa:aa:aa	Ethernet(11:11:11:11:11:11) ARP Reply(aa:aa:aa:aa:aa:aa) Llega a SW1	10.10.20.1	10.10.20.2
4	aa:aa:aa:aa:aa:aa	Ethernet(11:11:11:11:11:11) ARP Reply(aa:aa:aa:aa:aa:aa) Llega a PC1	10.10.20.1	10.10.20.2

** Se envía el paquete ICMP de PC1 a R1 (destino PC3)

Tramas ARP generadas en cada instante TRAS EL ENVÍO DEL PAQUETE ICMP de PC1 a R1:

El router recibirá el paquete ICMP con destino PC3 (10.10.10.2).
Deberá hacer un ARP Request para averiguar la MAC de PC3.

Instante	MAC origen	MAC destino	IP origen	IP destino
1	bb:bb:bb:bb:bb:bb	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a SW2	10.10.10.1	10.10.10.2
2	bb:bb:bb:bb:bb:bb	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 33:33:33:33:33:33	10.10.10.1	10.10.10.2
2	bb:bb:bb:bb:bb:bb	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 44:44:44:44:44:44	10.10.10.1	10.10.10.2
3	33:33:33:33:33:33	Ethernet(bb:bb:bb:bb:bb:bb) ARPReply(33:33:33:33:33:33) Llega a SW2	10.10.10.2	10.10.10.1
4	33:33:33:33:33:33	Ethernet(bb:bb:bb:bb:bb:bb) ARPReply(33:33:33:33:33:33) Llega a R1	10.10.10.2	10.10.10.1

*** ICMP funciona sobre IP. La transmisión del paquete ICMP se hará como datos encapsulados dentro de una trama Ethernet, que PC1 enviará a R1 en primera instancia (a su MAC a nivel de enlace).
R1 desencapsulará el datagrama IP (ICMP) y lo interpretará, viendo su destino (PC3). Lo

encapsulará de nuevo y lo enviará a nivel de enlace a PC3 (a su dirección MAC), que lo desencapsulará y lo interpretará. ***

El router enviará el paquete ICMP a PC3 el paquete que viene de PC1. Luego recibirá la respuesta y la enviará a PC1.
Las tablas ARP ya están rellenas con todas las MAC, y las tablas de Conmutación de los Switches también, por lo que se puede hacer la transmisión de forma directa.

b) Tras el envío del paquete ICMP, habrá llegado el ARP Reply de R1 a PC1 y el de PC3 a R1.

Hay que considerar por qué nodos pasa la petición y la respuesta y se apuntan en las tablas.
Habría un TTL de 20 minutos por defecto, aunque no será relevante en este ejercicio.
Las consultas se utilizan para crear entradas con la MAC e IP de origen en los destinos solamente (no en los nodos por los que se va pasando, que simplemente descartan los paquetes). Esto es así para no crear tablas gigantes a las que no se les daría uso (muchas entradas innecesarias), según el RFC (https://tools.ietf.org/html/rfc826).

Tabla ARP de PC1:
aa:aa:aa:aa:aa:aa – 10.10.20.1 – TTL=20 (ARP Request PC1→R1)

Tabla ARP de R1:
11:11:11:11:11:11 – 10.10.20.2 – TTL=20 (ARP Request PC1→R1)
33:33:33:33:33:33 – 10.10.10.2 – TTL=20 (ARP Request R1→PC3)

** La primera entrada se rellenó cuando se recibió el ARP Request de PC1 a R1

Tabla ARP de PC3:
bb:bb:bb:bb:bb:bb – 10.10.10.1 – TTL=20 (ARP Request R1→PC3)

** Esta entrada se rellenó cuando se recibió el ARP Request de R1 a PC3

c)

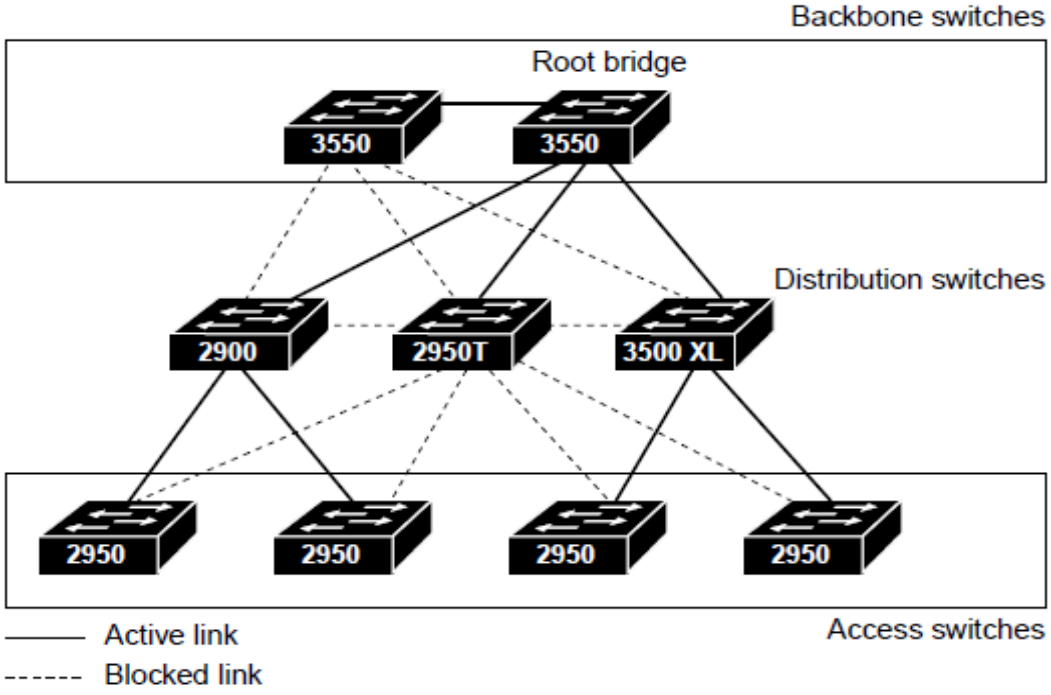
** PC3 sabrá que PC2 está en otra subred, hará Proxy ARP, pero ya conocerá la MAC de R1 (está en su tabla ARP).
De modo que enviará el paquete IP directamente a R1

R1 al recibirlo tendrá que hacer un ARP Request de la MAC de PC2, teniendo en cuenta su IP.

Instante	MAC origen	MAC destino	IP origen	IP destino
1	aa:aa:aa:aa:aa:aa	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a SW1	10.10.20.1	10.10.20.3
2	aa:aa:aa:aa:aa:aa	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 11:11:11:11:11:11 (PC1)	10.10.20.1	10.10.20.3
2	aa:aa:aa:aa:aa:aa	Ethernet(FF:FF:FF:FF:FF:FF) ARP Request (000000000) Llega a 22:22:22:22:22:22 (PC2)	10.10.20.1	10.10.20.3
3	22:22:22:22:22:22	Ethernet(aa:aa:aa:aa:aa:aa) ARP Reply (22:22:22:22:22:22) Llega a SW1	10.10.20.3	10.10.20.1
4	22:22:22:22:22:22	Ethernet(aa:aa:aa:aa:aa:aa) ARP Reply (22:22:22:22:22:22) Llega a aa:aa:aa:aa:aa:aa (R1)	10.10.20.3	10.10.20.1

Una vez rellena la tabla ARP de R1 con esta nueva entrada (la del PC2), enviará el paquete IP a nivel de enlace (como una trama Ethernet en la que irá encapsulado) a su MAC.

4) Dada la siguiente topología en una red en la que se reflejan los enlaces activos actualmente y los inactivos (bloqueados) tras haber ejecutado STP. Asigne identificación a todos los switches de acuerdo para que encajen con los criterios del protocolo. Asuma que todos tienen la prioridad por defecto. Para cada puerto, indique si se trata de *Designated Port*, *Root Port* o *Blocked*. Asuma que el ancho de banda de los enlaces es decreciente desde *Backbone* hasta *Access*.



Prioridad por defecto 32768.
RB debe tener una MAC menor si tienen todos la misma prioridad

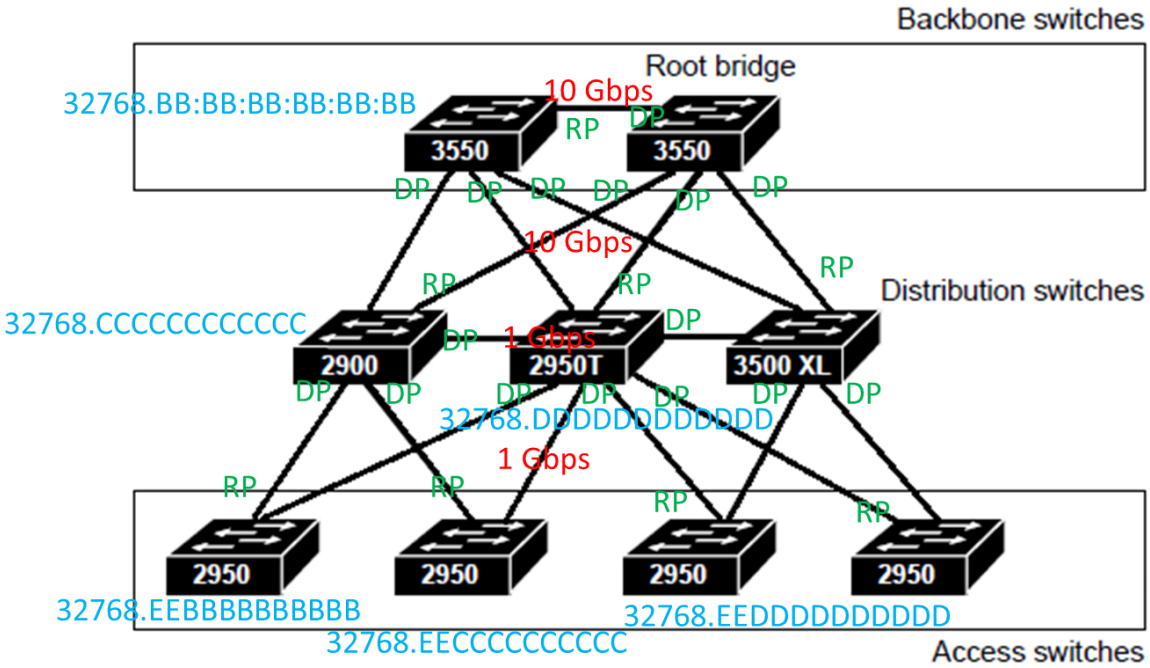
Asignar capacidades según tabla:

Link Bandwidth	STP Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

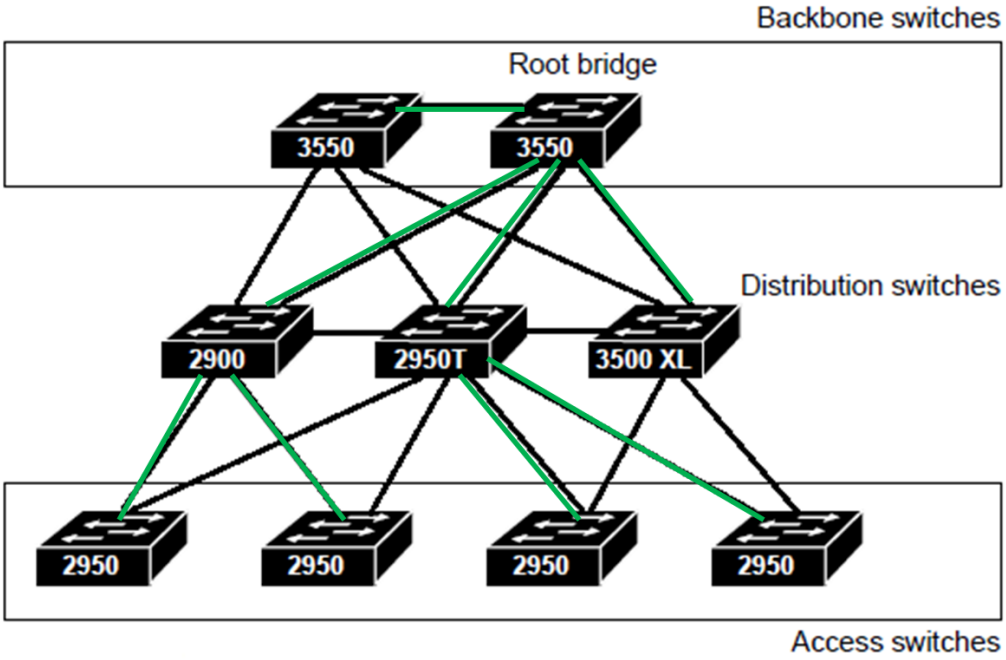
RP → Más cercano al RB

DP:
Todos los puertos del RB son DP

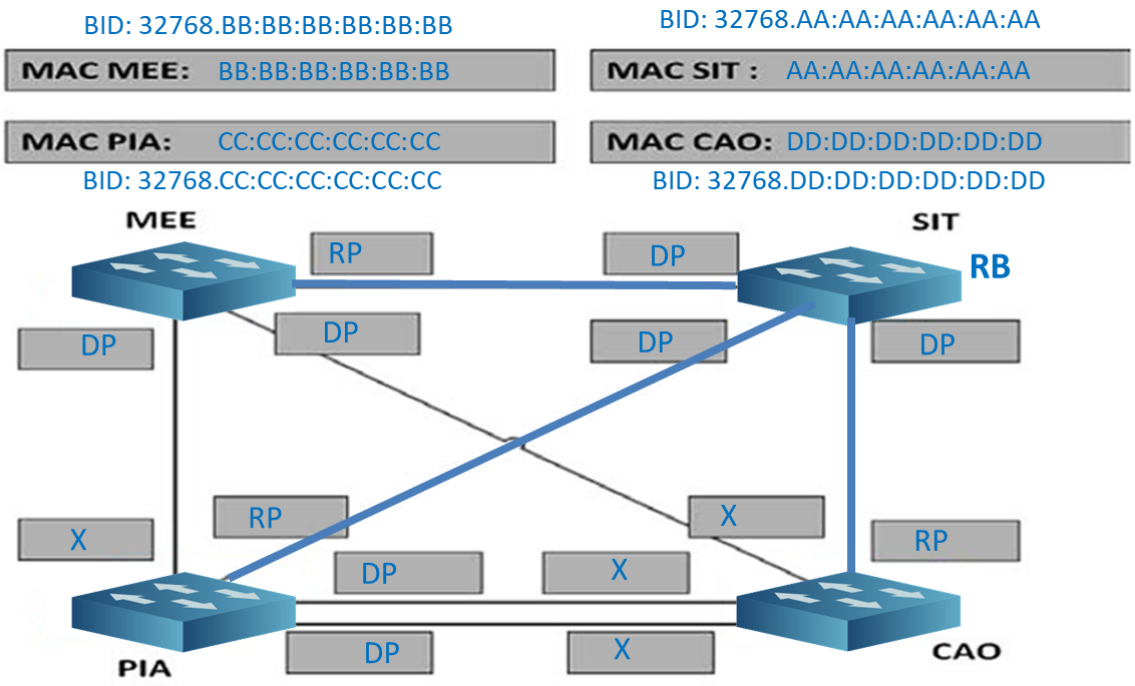
Las reglas para decidir en cada segmento de red cuál es la BPDU de mayor calidad son:
1) Más bajo Root Bridge Id
2) Más bajo Root Path Cost
3) Más bajo Sender Bridge Id (el switch que ha transmitido la BPDU al enlace)
4) Más bajo Sender Port Id (prioridad del puerto.puerto, Ejemplo: 128.4)



El árbol de expansión sería:



5) En la topología mostrada, STP está habilitado y ha provocado que algunos enlaces estén bloqueados. Considerando que todos los enlaces son FastEthernet (100 Mbps) y que todos los switches están configurados con la prioridad por defecto:
   a) Asigne una identificación (BID) a cada switch y haga que SIT sea el RB.
   b) Indique, para cada Puerto, si éste es RP, DP o si su estado es *blocking* (X)



a) La identificación será **Prioridad.MAC**. Si queremos que SIT sea el RB, su BID debe ser el menor.
Podríamos poner prioridad 4096, pero nos dicen que todos tienen la prioridad por defecto, por lo que todos tendrían BID = 32768.MAC. Y la MAC de SIT deberá ser la menor.

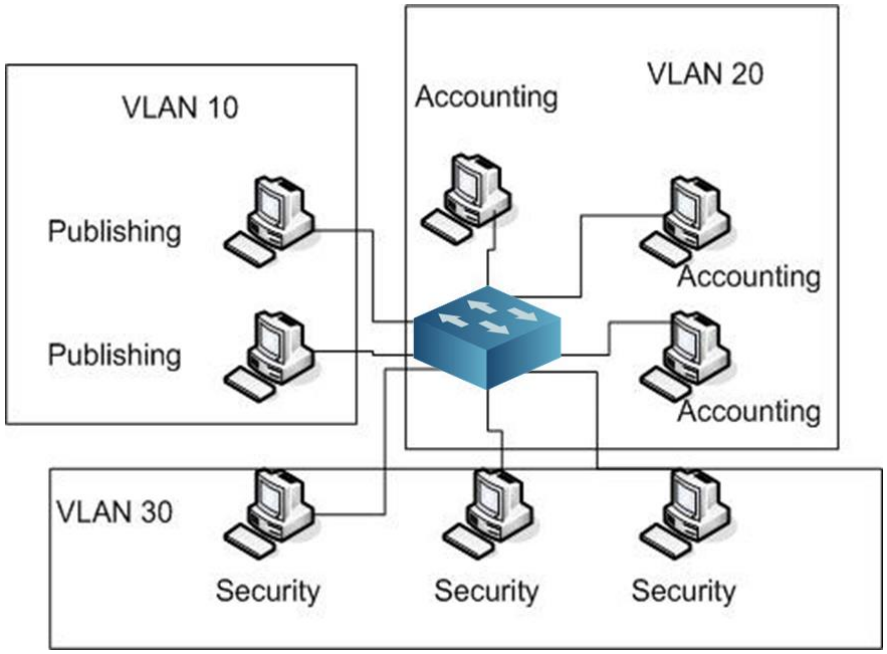
b) Root Port → los más cercanos al Root Bridge (según el Root Path Cost, que depende de la calidad del enlace)
Como todos son FastEthernet, el coste de cada enlace será 19.

Designated Port → el que une al switch con el enlace de mayor "calidad"

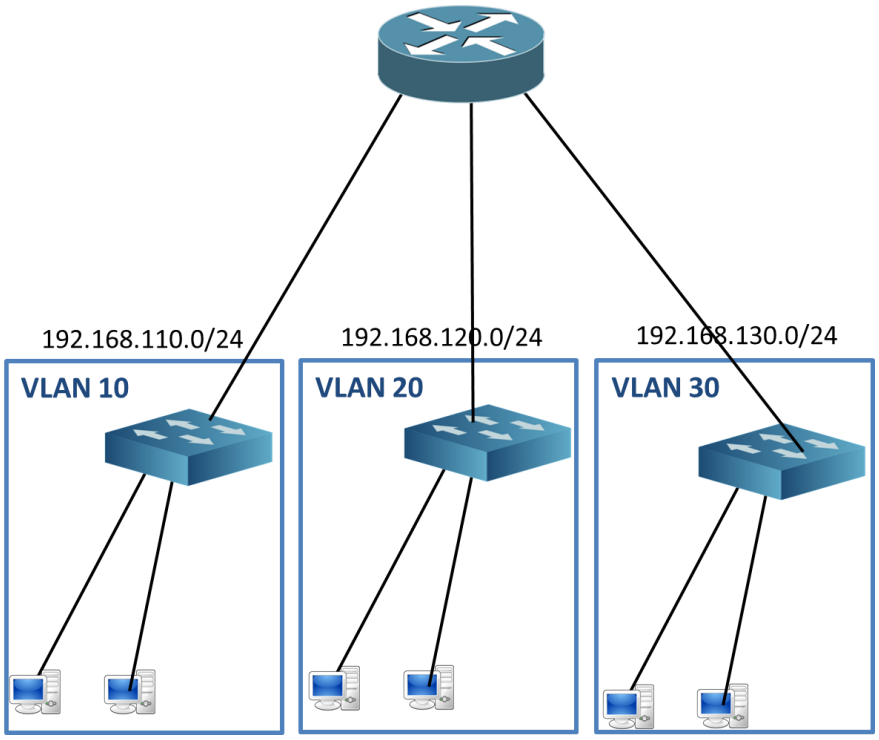
BPDU de mayor calidad son:
1) Más bajo Root Bridge Id
2) Más bajo Root Path Cost
3) Más bajo Sender Bridge Id (el switch que ha transmitido la BPDU al enlace)
4) Más bajo Sender Port Id (prioridad del puerto.puerto, Ejemplo: 128.4)

Todos los puertos del RB son DP.

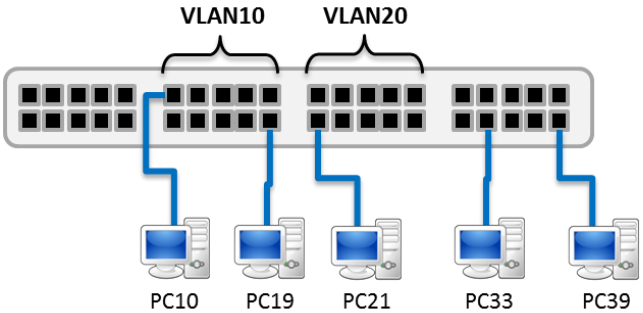
6) La topología de la figura muestra una división en distintas LANs virtuales (VLANs) realizada con la configuración del switch. Dibuje la topología virtual de red a la que equivaldría esta distribución real. Asigne direcciones IP a las redes, así como lo necesario para que haya conectividad total.



- Switches separados (independientes) formando 3 subredes
- Tres subredes independientes: 192.168.100.0/24, 192.168.101.0/24, 192.168.102.0/24
- Añadir un router para conectarlas



7) En el siguiente switch gestionable SW1 se han creado las **VLANs 10 y 20**. La asignación de puertos a estas VLANs ha sido FE10-FE19 y FE20-FE29 respectivamente.
   a) Indique si los hosts PC10, PC21 y PC33 enviasen un ***ARP Request***, ¿quiénes lo recibirían y quiénes no?
   b) ¿Qué hosts pueden hacerse **ping entre ellos**? ¿Qué haría falta añadir en la topología para que todos pudieran hacerse ping entre ellos?
   c) ¿Qué hosts podrían hacer **ping o telnet a SW1**?
   d) ¿Cuántas entradas podría haber como mucho en..
      Tabla ARP de PC10
      Tabla ARP de PC21
      Tabla ARP de PC30
   e) Escriba la **Tabla de Conmutación** de SW1 una vez todos los hosts se han comunicado entre sí.



DIRECS. MAC
PC10 - 10:10:10:10:10:10
PC19 - 19:19:19:19:19:19
PC21 - 21:21:21:21:21:21
PC33 - 33:33:33:33:33:33
PC39 - 39:39:39:39:39:39

a) PC10 → ARP Request : Lo recibiría solamente PC19 (las VLAN restringen el broadcast)
PC21 → ARP Request : No lo recibiría ninguna de estas máquinas (no hay nadie más en VLAN20)

PC33 → ARP Request : Lo recibiría solamente PC39 (está en la misma VLAN1, la definida por defecto)

b) En la topología actual se podrán hacer ping entre ellos los que estén en la misma VLAN

Para que todos pudieran hacerse ping entre sí sería necesario añadir un router que conectase las diferentes VLANs.

c) Para hacer ping o telnet se debe acceder a través de la VLAN1 (la que hay para Gestión del Switch). Por tanto, sólo PC33 o PC39 podrían hacerlo.

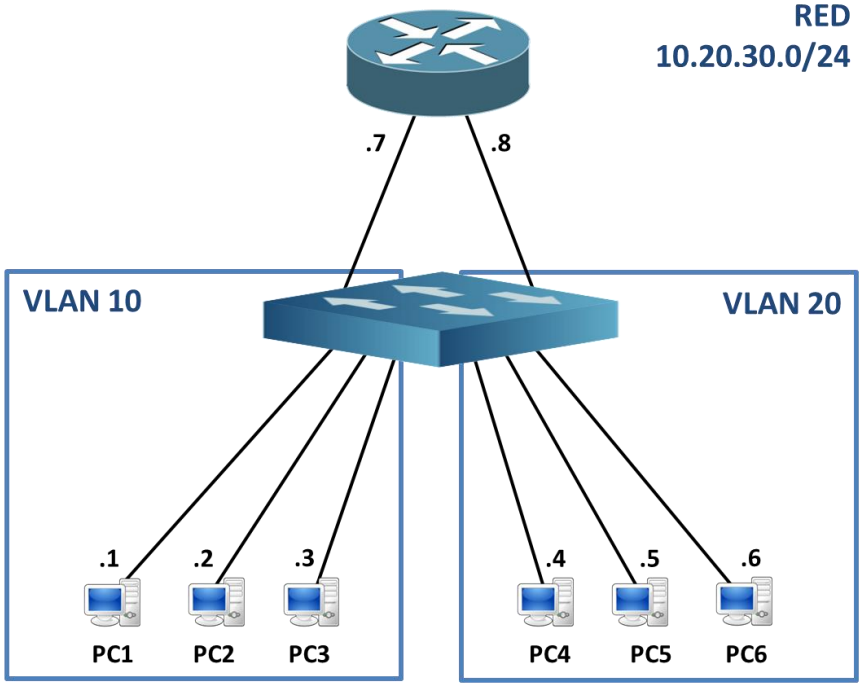
d) En la topología actual (con esos equipos), podría haber únicamente:
Tabla ARP de PC10 → 1 entrada para PC19
Tabla ARP de PC21 → ninguna entrada
Tabla ARP de PC30 → 2 entradas para PC33 y PC39

e) Tabla de conmutación de SW1:
33:33:33:33:33:33 – FE33 – VLAN1
39:39:39:39:39:39 – FE39 – VLAN1
10:10:10:10:10:10 – FE10 –VLAN10
19:19:19:19:19:19 – FE19 – VLAN10
21:21:21:21:21:21 – FE21 – VLAN20

** Se añadirían las entradas para el Router (MAC – FE – VLAN)

8) Dibuje la topología y razone qué problemas podría haber en cada uno de estos casos:
a) Si los equipos de una misma red real estuvieran divididos en dos VLANs.
b) Si una VLAN albergara dos redes diferentes.

a) Una sola red, dos VLAN



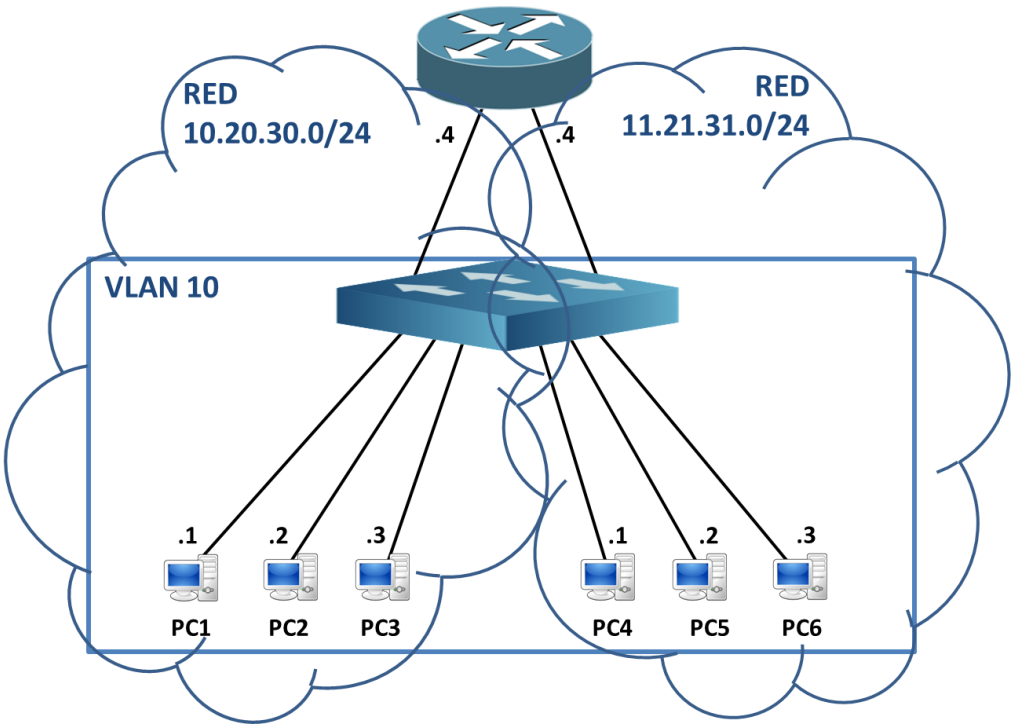
En este caso:

Si por ejemplo, el PC1 intenta comunicarse con PC5, sabrá que está en su misma red (por la IP), así que no será necesario hacer un Proxy ARP (no habrá que pasar por el router).

PC1 hará un ARP Request con la IP de PC5, que se enviará por broadcast.
El Switch sólo transmitirá ese broadcast a los equipos en la VLAN 10 (la del PC1), el broadcast llegará a PC2, PC3 y al router, que no lo propaga (los routers aíslan dominios de difusión).

De modo que NO LLEGARÁ a PC5 y no se podrán comunicar.

b) Una sola VLAN, dos redes



En este caso:

Si por ejemplo, el PC1 intenta comunicarse con PC5:

- PC1 vería que no está en su misma subred ➔ tendrá que hacer un proxy ARP a través del router.
- El router le respondería con la MAC asociada a PC5.
- PC1 enviaría un paquete a PC5 usando su IP destino y la MAC del router.
- El router enviaría el paquete a PC5 (IP de destino).
- **El paquete llegaría.**

El **problema** de este escenario es cuando se quiere hacer un **broadcas**t:

- Los mensajes enviados por PCs de las distintas redes llegarían a los de la otra red, porque el Switch los transmitiría al estar en la misma VLAN.
- De forma que no conseguiríamos aislar los dominios de broadcast, como es deseable al dividir en subredes.

*** La solución a ambos escenarios sería desplegar dos VLANs diferentes y dos subredes, una en cada VLAN.