INGENIERÍA TELEMATICA EXAMEN DE ARS
PRIMER PARCIAL. FEBRERO 2005

Primera Parte. Teoría y Laboratorio

Tiempo: 1 hora 45 minutos

Esta parte debe realizarse sin material de consulta. Puede utilizar una calculadora.

1 Pregunta 1 (3 puntos):

Responda en la hoja adjunta.

En cada una de las afirmaciones o preguntas marque la respuesta correcta. Solo debe marcar una respuesta en cada caso; si cree que hay varias respuestas correctas debe elegir la que a su juicio mejor se ajuste a la pregunta. Lea los enunciados con atención.

Forma de puntuación:

Respuesta correcta: 1 punto positivo
Respuesta incorrecta: 1/(n-1) puntos negativos (siendo *n* el número de respuestas posibles)
Ausencia de respuesta: 0 puntos

La nota final de esta pregunta no podrá ser negativa.

1.1 La afirmación que dice: "En una LAN conmutada (sin VLANs) el tráfico broadcast se propaga por toda la red sin excepciones, es decir por todas las interfaces activas de todos los conmutadores, es:

A) Verdadera
B) Falsa. Solo se envían por las que tienen hosts, no por las que tienen routers u otros conmutadores
C) Verdadera si y sólo si los conmutadores están en modo promiscuo.
D) Verdadera si y sólo si todas las estaciones (conmutadores, hosts y routers) están en modo promiscuo.

1.2 ¿Qué campos se modifican en una trama Ethernet DIX cuando entra en un conmutador por un puerto de 10 Mb/s y sale por uno de 100 Mb/s?:

A) Ninguno
B) La dirección MAC de origen y el CRC
C) La dirección MAC de origen, la de destino y el CRC
D) El TTL y el CRC

1.3 Si tenemos que instalar una red local y solo disponemos de conmutadores que no soportan Spanning Tree ¿Qué limitación tendremos?:

A) No podremos hacer bucles
B) No podremos crear VLANs
C) No podremos realziar conexiones full duplex
D) Todas las anteriores

1.4 En una red local basada en hubs se sustituyen éstos por conmutadores, sin modificar el tráfico generado en la red. ¿De que forma cambiará el consumo de CPU en los hosts debido al proceso de las tramas recibidas?:

A) Aumentará
B) Disminuirá
C) No se modificará
D) Puede aumentar o disminuir, dependerá de la proporción de tráfico broadcast respecto al tráfico total

1.5 La necesidad de etiquetar en una LAN conmutada las tramas Ethernet indicando la VLAN a la que pertenecen surge cuando:

A) Se configuran VLANs en los conmutadores
B) Se configuran VLANs en los conmutadores y se conectan éstas mediante routers
C) Se configuran VLANs en los conmutadores y se establecen enlaces trunk entre ellos
D) Se configuran VLANs en los conmutadores, se establecen enlaces trunk entre ellos y se interconectan las VLANs mediante routers

1.6 ¿Que tratamiento reciben, a efectos de spanning tree, los enlaces serie de una red con puentes remotos?

A) Se ignoran. Los puentes remotos no ejecutan el spanning tree
B) La línea serie se considera equivalente a una LAN que solo conectara dos equipos (los puentes remotos)
C) Los dos puentes unidos pro la línea serie se consideran dos 'medios puentes' es decir se les trata como si fueran uno solo
D) Los puentes remotos ejecutan en sus interfaces serie una instancia de spanning tree diferente de la que realizan para las interfaces LAN

1.7 Con que situación se asocia el denominado problema 'de la cuenta a infinito'?

A) Con el routing dinámico
B) Con el routing basado en el vector distancia
C) Con el routing basado en el estado del enlace
D) Con el routing jerárquico

1.8 El control de admisión es:

A) Un mecanismo de decubrimiento de rutas óptimas en todo tipo de redes
B) Un mecanismo de control de congestión aplicable solo a redes CONS
C) Un mecanismo de control de congestión aplicable a todo tipo de redes
D) Un mecanismo de control de congestión aplicable solo a redes CLNS

1.9 ¿En que situación sería menos recomendable utilizar un protocolo de routing?:

A) En una red mallada y estable (es decir en la que los enlaces permanecen siempre operativos)
B) En una red mallada e inestable
C) En una red no mallada y estable
D) En una red no mallada e inestable

1.10 ¿Quién recibe los LSPs (Link State Packets) que envía un router en una red?

A) El router raíz
B) Solo sus vecinos
C) Todos los routers
D) Sus vecinos y el router raíz

1.11 ¿Cual de los siguientes protocolos no utiliza datagramas IP para enviar su información?:

A) RARP
B) ICMP
C) DHCP
D) OSPF

1.12 ¿Qué ocurre cuando el campo TTL de la cabecera IP vale cero?

A) Se descarta y se envía mensaje de error al emisor
B) Nada. El paquete sigue su curso.
C) Se descarta
D) Se envía mensaje de error al emisor

1.13 ¿Cuántas direcciones útiles obtendremos si creamos subredes con máscara 255.255.255.240 a partir de la red 200.200.200.0/25? Suponga que se aplica CIDR y subnet-zero

A) 112
B) 84
C) 128
D) 224

1.14 ¿Que denominación reciben las entidades encargadas de asignar direciones IP al máximo nivel (es decir de rango más alto) en Internet?

A) NOCs (Network Operation centers)
B) ISPs (Internet Service Providers)
C) RIRs (Regional Internet Registries)
D) AAOs (Address Asignment Organizations)

1.15 Al enrutar un paquete en un router se encuentra que hay varias rutas utilizables con diferentes métricas, máscaras y distancias administrativas. Una de ellas se ha configurado como ruta estática, mientras que el resto han sido obtenidas por OSPF o por IS-IS. Diga cual de todas se utilizará en primer lugar:

A) La de métrica más baja
B) La de distancia administrativa menor
C) La de máscara más larga
D) La ruta estática, independientemente de su métrica, máscara o distancia administrativa

1.16 A efectos del protocolo BGP los routers se agrupan por:

A) Áreas
B) Sistemas Autónomos (Autonomous Systems)
C) Zonas
D) Sistemas Pares (Peer Systems)

1.17 ¿Que tipo de mensaje ICMP recibe normalmente un host cuando utiliza el mecanismo denominado 'descubrimiento de la MTU del trayecto'?

A) Time Exceeded
B) Destination Unreachable
C) Size Exceeded
D) Source quench

1.18 El host 10.10.10.10/8, que se acaba de encender, ejecuta el comando 'ping –c 1' (1 paquete) hacia las direcciones IP 10.10.10.11, 90.10.10.10 y 90.10.10.11, recibiendo tres respuestas. ¿Cuantas tramas capturaremos si seguimos el tráfico con el Ethereal en ese host en modo no promiscuo?:

A) Tres
B) Diez
C) Seis
D) Ocho

1.19 El campo 'fragment offset', utilizado al fragmentar datagramas IP, cuenta los bytes en grupos de ocho. Esto significa que:

A) La longitud de la parte de datos de los datagramas siempre ha de ser múltiplo de ocho
B) Solo se pueden fragmentar los datagramas cuyos datos tienen una longitud total múltiplo de ocho
C) El datagrama puede tener cualquier longitud, pero la parte de datos de los fragmentos (excepto posiblemente el último) ha de ser multiplo de ocho
D) Cuando se fragmenta un datagrama se añade un relleno para que sus datos tengan una longitud múltiplo de ocho

1.20 Los acuerdos que realizan los ISP para intercambiar tráfico en un punto neutro (normalmente sin compensaciones económicas,) se denominan:

A) Acuerdos de conectividad
B) Acuerdos de intercambio
C) Acuerdos de peering
D) Acuerdos de visibilidad

1.21 ¿Cuál de los campos siguientes de la cabecera IPv4 no existe, ni tiene equivalente, en IPv6? :

A) Checksum
B) Tiempo de vida
C) Protocolo
D) Dirección de origen

1.22 La principal diferencia de BGP respecto del resto de protocolos de routing es que:

A) Permite establecer restricciones para impedir el tráfico de tránsito
B) BGP no puede funcionar en entornos 'classless' (CIDR)
C) Emplea una mética más sofisticada que la mayoría de los protocolos de routing
D) Con BGP no está permitido crear topologías malladas

1.23 La principal diferencia entre BOOTP y DHCP es que

A) BOOTP no puede asignar dirección IP a un host con una dirección MAC desconocida y DHCP sí
B) Los mensajes BOOTP no pueden atravesar los routers y los de DHCP sí
C) BOOTP no puede enviar la máscara de subred, DHCP sí
D) Ninguna de las anteriores

1.24 En el caso que los servidores DNS de una red dejen de funcionar

A) Fallan todas las conexiones IP
B) Falla la conectividad IP interna
C) Ninguna de las anteriores
D) Falla la conectividad IP externa

1.25 Los certificados para clave pública se caracterizan por:

A) Proteger con el certificado la clave privada
B) Estar firmados con la clave pública de la autoridad de certificación
C) Comprobar la integridad de los datos que contiene
D) Estar escritos en lenguaje C

Pregunta 2.1 (1,5 punto):

Una empresa de ordenadores ofrece sus productos por Internet. Para ello dispone de un certificado que entrega a sus clientes cuando quieren realizar alguna operación de compra. Los clientes disponen de sus propios certificados. No todos los certificados son firmados por la misma Autoridad de Certificación.

Responda a las siguientes preguntas de forma concisa, para que las operaciones puedan tener la máxima garantía:

Cuando un nuevo cliente entrega su certificado a la empresa de ordenadores:

1. ¿Qué información se puede obtener de dicho certificado?

Identidad del usuario, su clave pública, la CA, periodo de validez y el compendio de todo ello firmado por la clave privada de la CA

2. ¿Qué hace la empresa para fiarse de este certificado?¿y cómo lo hace?

Obtener el certificado raíz de la CA y comprobar que la firma del certificado por parte de la CA es correcto, es decir que comprobamos si MD5(Certificado) es igual a $E_{CA}(D_{CA}(MD5(Certificado)))$.

Cuando ambas partes disponen de los certificados y de las claves públicas, utilizando la notación $E_x()$ para cifrar con la clave pública de X y $D_x()$ para cifrar con la clave privada de X, indique:

3. Si el mensaje a mandar es P, desde el cliente a la empresa, ¿cómo codifica el mensaje para que éste permita comprobar simplemente la identidad de quien lo envía? Justifíquelo.

Una vez tenemos certificados y claves públicas, si el cliente firma con su privada, permite identificarse. Para comprobarlo, la empresa le aplica la clave pública del cliente, obtenida del certificado, es decir $E_{Cliente}(D_{Cliente}(P))$.

4. Si el mensaje a mandar es P, desde el cliente a la empresa, ¿cómo codifica el mensaje para que éste lo envíe cifrado a la empresa? Justifíquelo.

Como tenemos la clave pública de la empresa, como cliente podemos mandar $E_{empresa}(P)$, de forma que el único que lo puede leer es la empresa con su clave privada, con $D_{empresa}(E_{empresa}(P))$.

5. Si el mensaje a mandar es P, desde el cliente a la empresa, ¿cómo codifica el mensaje para que éste vaya cifrado y permita comprobar la identidad? Justifíquelo.

Hacemos una combinación de los 2 anteriores, por tanto el cliente manda $E_{empresa}(D_{Cliente}(P))$ y para descifrarlo, la empresa aplica $E_{Cliente}(D_{empresa}(E_{empresa}(D_{Cliente}(P))))$.

Pregunta 2.2 (1,5 punto):

Una empresa quiere conectarse a Internet. Para ello compra a la autoridad competente dos clases C, 200.200.6.0/24 y 200.200.7.0/24 y el dominio "ars.es.". Sin embargo la empresa dispone de más de 508 ordenadores, concretamente 2000. Parte de este rango de IP comprado, se utiliza por un servidor de túneles VPN para asignar IP a los empleados de la empresa que desde el exterior realizan una conexión VPN al servidor, de forma que les permita obtener una IP interna de la empresa para poder acceder a diferentes servicios.

La conexión a Internet se realizar desde nuestro router de salida por un enlace serie al router del ISP. Este enlace utiliza direccionamiento privado con la subred 172.16.10.4/30, siendo la primera dirección IP asignada al ISP y la segunda al router de salida.

Se supone que a usted le contratan como consultor, dado que usted les informó que está muy metido en la materia. Le preguntan:

1. En el router de salida de la empresa, ¿qué ruta estática debemos configurar para acceder al exterior? Tome como formato para indicar la ruta estática "`ip route red máscara next-hop`"

ip route 0.0.0.0 0.0.0.0 172.16.10.5

2. El router del ISP que nos ofrece conectividad a Internet, ¿qué ruta estática debe incluir para que nos lleguen los paquetes de nuestro rango de IP?

ip route 200.200.6.0 255.255.254.0 172.16.10.6

3. ¿Qué solución propondría para conseguir que todos los ordenadores de la empresa pudieran conectarse a Internet simultáneamente?

NAT extendido, también conocido como NAPT, PAT o NAPT es decir con multiplexación de IP a nivel de puerto.

4. Una vez comprado el dominio "ars.es.", le piden que indique de forma simplificada cuales son los siguientes pasos para configurar el DNS de la empresa.

Por orden: configurar los 2 servidores (primario y secundario para que haga transferencia de zona del primario), registrar e inventariar todos los elementos de la empresa (tanto con resolución directa como inversa, para los servicios que se deseen), avisar a ".es" que los servidores están preparados con sus IP respectivas.

5. Los gerentes han oído algo sobre "DNS Spoofing" y la verdad que estos temas le merecen respeto. Le piden que brevemente les explique en qué consiste y cómo se puede solucionar.

Es un ataque, que intercepta la petición al DNS y la contestación la realiza un tercero dando una contestación de forma que se asigna a un nombre, una IP que no corresponde. La solución es utilizar certificados con el DNS.

6. Respecto a la configuración del DNS, le piden que defina los registros (indicando su tipo) que permiten resolver el nombre para el servidor web de la empresa (www.ars.es, con IP 200.200.6.2), el servidor FTP (ftp.ars.es, con IP 200.200.6.3), el servidor de túneles (vpn.ars.es, con IP 200.200.6.4).

Suponiendo que tenemos configurado el SOA, por tanto debemos introducir los siguientes registros tipo A:

www	**A**	**200.200.6.2**
ftp	**A**	**200.200.6.3**
vpn	**A**	**200.200.6.4**

7. Le piden que indique una forma de centralizar las cuentas y las contraseñas de los empleados de la empresa, de forma más estructurada y flexible posible. ¿Qué protocolo y/o tecnología propone?

LDAP es la mejor opción. Otras opciones pueden ser X.500, Kerberos, Radius, ...

Los empleados que se conectan desde casa, realizan una conexión VPN con el servidor de túneles. Tras autenticarse obtienen una IP pública del rango de la empresa, concretamente del rango 200.200.6.128/25. En el caso que el empleado en su casa tenga la IP asignada por su ISP local 147.156.100.1 y siendo la IP del servidor de túneles 200.200.6.4, si el usuario ejecuta "ping –n –c 1 200.200.6.1" siendo 200.200.6.1 la IP asignada a la Ethernet del router de la empresa, indique:

8. las cabeceras IP del paquete enviado desde el usuario al servidor de túneles, especificando direcciones origen y destino.

Aquí tenemos IP dentro de IP.
Primera cabecera (más externa): Destino 200.200.6.4 Origen 147.156.100.1
Segunda cabecera: Destino 200.200.6.1 Origen 200.200.6.129

9. la cabecera IP del paquete enviado desde el servidor de túneles al destino especificado.

Es el paquete que llevaba encapsulado antes, es decir Destino 200.200.6.1 Origen 200.200.6.129

10. Cuando contesta el router, ¿qué pasa con el paquete de vuelta, es decir el ICMP Echo Reply?

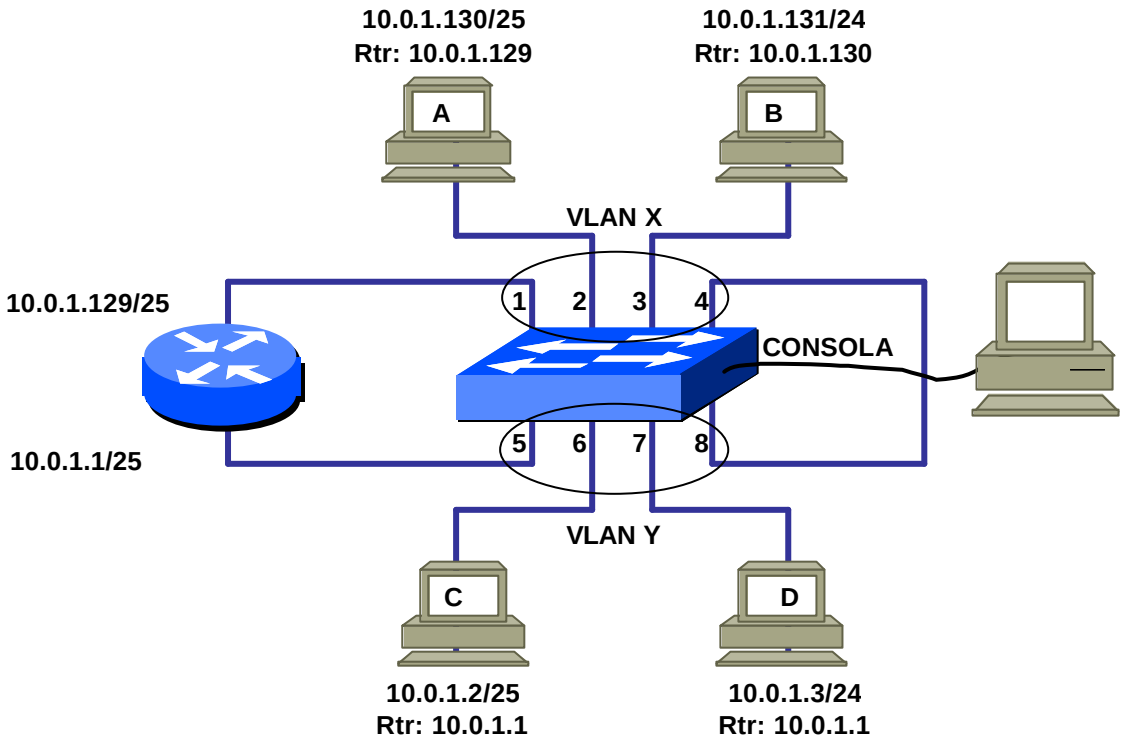
Que lo captura el servidor de túneles para encapsularlo en el tunel, pues la contestación se realiza a 200.200.6.129 y el servidor de túneles actúa como proxy de sus IP asignadas.

INGENIERÍA TELEMATICA. EXAMEN DE ARS.
PRIMER PARCIAL, FEBRERO 2005
PROBLEMAS

Para resolver estos problemas el alumno puede utilizar todo el material auxiliar que desee (apuntes, libros, etc.) y calculadoras, pero no ordenadores personales.

Problema 1 (1,5 puntos):

En la red de la figura adjunta:



se ejecuta en el host A el comando '`ping -n -c 1 10.0.1.2`'. A continuación se ejecuta en la consola del conmutador el comando 'show interfaces' para observar el número de tramas transmitidas y recibidas en cada interfaz del conmutador. Rellene la siguiente tabla indicando los valores se obtendrán para cada interfaz:

Interfaz	Tramas recibidas	Tramas transmitidas
1		
2		
3		
4		
5		
6		
7		
8		

Suponga que todos los equipos se acaban de encender y que no existe ninguna actividad en la red aparte de la originada por la ejecución del comando ping descrito. En particular el router no está ejecutando ningún protocolo de routing y el conmutador no tiene activado spanning tree ni protocolos de gestión

SOLUCION:

La opción –n indica que no se haga uso del servidor de nombres, por lo que no tendremos que preocuparnos por posibles mensajes enviados al DNS. La opción -c 1 indica que se enviará un solo paquete ICMP Echo request del tamaño por defecto, por lo que en caso de funcionar las cosas nomrlamente recibiremos también un solo mensaje ICMP Echo reply.

Como el enunciado nos dice que se supone que todos los equipos se acaban de encender vamos a suponer que las tablas ARP cache de los equipos (hosts y router) están en blanco y también las tablas de direcciones MAC del conmutador.

Al lanzar el ping de A hacia la dirección 10.0.1.2, como se trata de una dirección que pertenece a otra subred A intentará hacer uso de su router por defecto para enviar el datagrama. Pero como A no sabe cual es la dirección MAC de su router por defecto mandará en primer lugar un 'ARP request' buscándolo. Este ARP request se enviará a la dirección broadcast, por lo que entrará por la interfaz 2 y saldrá por 1, 3 y 4. al salir por 4 entrará por 8 y saldrá por 5, 6 y7. El conmutador habrá anotado en sus interfaces 2 y 8 la MAC de A.

El router responderá con un mensaje 'ARP reply' que irá dirigido a la dirección MAC de A, que entrará al conmutador por la interfaz 1 y saldrá por 2 (al tener el conmutador anotada la MAC de A la respeusta solo sale por este puerto). La respeusta permitirá al conmutador anotar la dirección MAC correspondiente a esa interfaz del router.

Una vez averiguada la MAC del router el host A le enviará el mensaje ICMP Echo Request en un paquete IP que irá en una trama unicast que entrará por 2 y saldrá por 1.

EL router procesará el paquete IP y descubrirá que su destinatario está en la subred en la que se encuentra su otra interfaz Ethernet, por lo que enviará por esa interfaz un 'ARP Request' a la dirección broadcast en una trama que entrará por 5, saldrá por 6, 7 y 8, entrará por 4 y saldrá por 1, 2 y 3. El conmutadro anotará esa dirección MAC en sus interfaces 5 y 4.

El 'ARP Reply' de B entrará por 6 y saldrá por 7.

El 'ICMP Echo Request' entrará entonces por 5 y saldrá por 6.

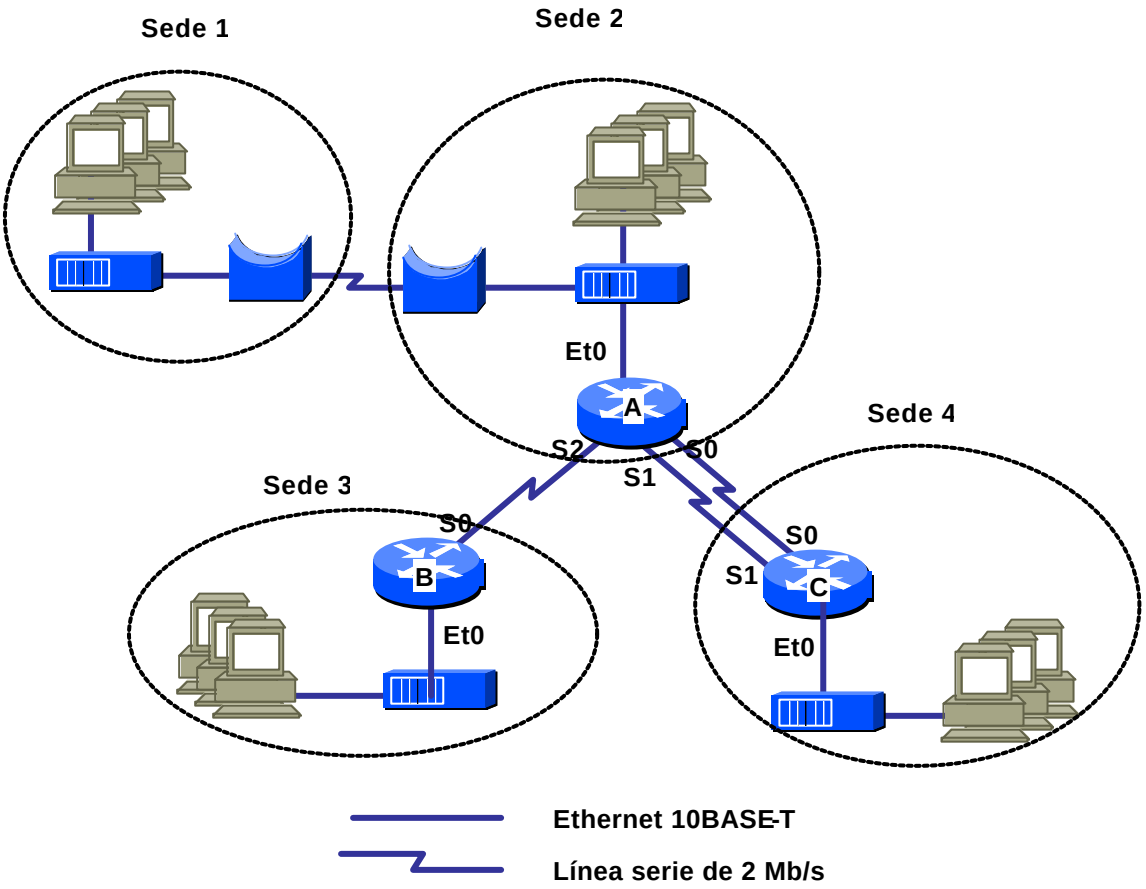
El host C generará entonces su 'ICMP Echo Reply' que entrará por 6 y saldrá por 5. Después el paquete hará la última parte de su viaje saliendo por 1 y entrando por 2.

El resultado de todo lo anterior es el siguiente:

Interfaz	Tramas recibidas	Tramas transmitidas
1	2	3
2	2	3
3	0	2
4	1	1
5	2	3
6	2	3
7	0	2
8	1	1

Problema 2 (2,5 puntos):

Una empresa dispone de una red informática repartida en cuatro sedes que se interconectan según la siguiente topología:



Cada una de las sedes tiene 50 ordenadores.

Se quiere utilizar el protocolo IP para comunicar todos los ordenadores entre sí, empleando direccionamiento privado pues la red no se conecta al exterior.

- Realice la asignación de subredes correspondiente.
- Diga cual deberá ser la configuración de los tres routers, A, B y C, indicando para cada interfaz la dirección IP y la máscara.Indique las rutas estáticas que deberán definirse en cada caso. Se quiere que entre el router A y el C el tráfico se reparta por igual entre ambos enlaces.
- ¿De qué forma cambiaría el tráfico en las líneas serie si se sustituyeran los hubs por conmutadores?
- ¿Cambiaría el tráfico en el enlace serie entre las sedes 1 y 2 si se sustituyeran por routers los puentes transparentes que las unen?

Explique sus respuestas.

SOLUCION

Como el enunciado nos dice que utilicemos direccionamiento privado sin imponer más requisitos vamos a asignar subredes /24 consecutivas. Como las sedes 1 y 2 se encuentran en la misma subred aquí necesitaremos dar cabida a 100 ordenadores más el router, pero con una subred /24 podemos tener hasta 254 direcciones útiles por lo que no tendremos ningún problema. Además en el caso de las sedes 1 y 2 podemos asignar la mitad inferior de las direcciones a la sede 1 y la mitad superior a la sede 2, de forma que si en un futuro se quisiera dividir la subred entre ambas sedes colocando routers en vez de puentes transparentes se podría hacer sin modificar las direcciones de los hosts (aunque habría que modificar sus máscaras). Para las líneas serie entre los routers utilizaremos subredes /30 de un rango diferente para mejorar la claridad de la configuración.

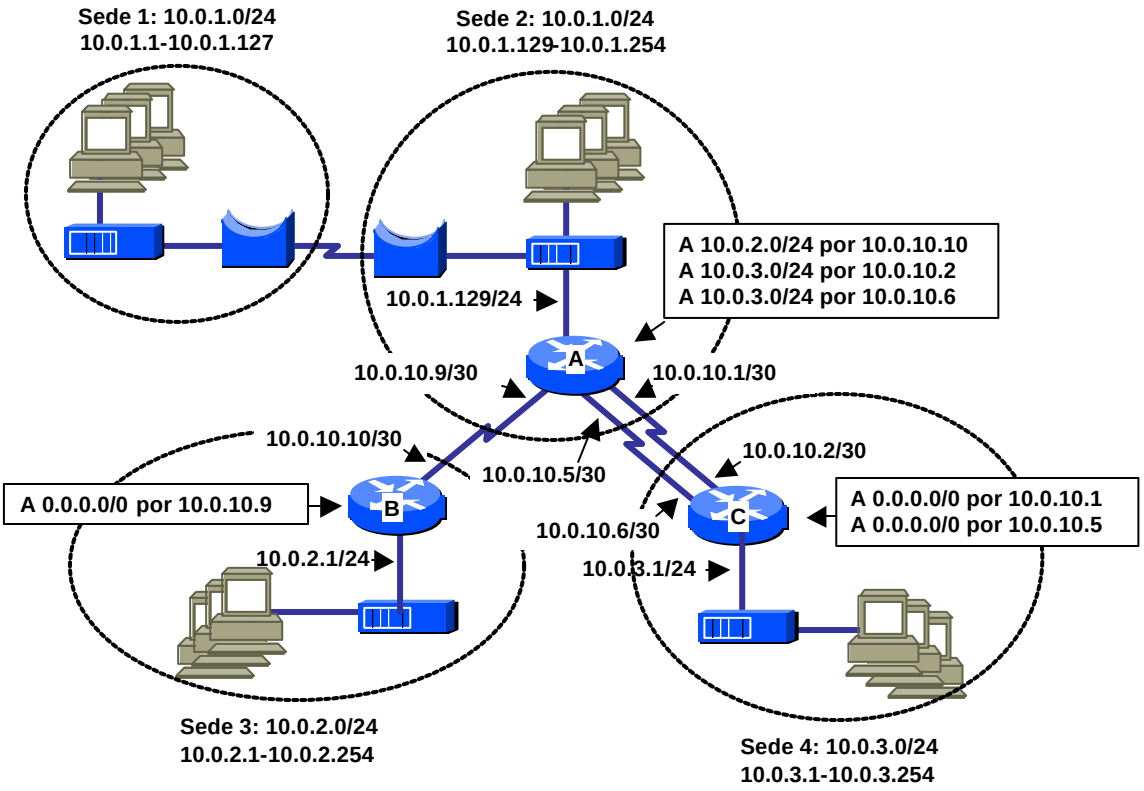
El reparto de subredes será pues el siguiente:

Subred	Subred/máscara	Rango asignable
LAN Sede 1	10.0.1.0/24	10.0.1.1-10.0.1.127
LAN Sede 2	10.0.1.0/24	10.0.1.129-10.0.1.254
LAN Sede 3	10.0.2.0/24	10.0.2.1-10.0.2.254
LAN Sede 4	10.0.3.0/24	10.0.3.1-10.0.3.254
Línea serie 0 Sede 2-Sede 4	10.0.10.0/30	10.0.10.1-10.0.10.2
Línea serie 1 Sede 2-Sede 4	10.0.10.4/30	10.0.10.5-10.0.10.6
Línea serie Sede 2 – Sede 3	10.0.10.8/30	10.0.10.9-10.0.10.10

Obsérvese que la Sede 1 y la Sede 2 comparten la misma subred aun cuando se les asigna rangos diferentes.

A la línea serie entre la Sede 1 y la Sede 2 no se le asigna subred pues al tratarse de dispositivos a nivel 2 no disponen de direcciones IP en sus interfaces. A lo sumo se asignaría una dirección IP a cada puente, en cuyo caso recibirían direcciones de la LAN en la que se encuentran.

La siguiente figura muestra resumida las interfaces y rutas correspondiente al reparto de subredes de la tabla anterior:



Al sustituir los hubs por conmutadores el tráfico unicast en las interfaces Ethernet de los routers se reduciría, pero no se modificaría de ninguna forma el tráfico en las líneas serie. Ni siquiera habría modificación en la línea serie entre la Sede 1 y la Sede 2, ya que los puentes transparentes ya estaban aislando el tráfico unicast innecesario entre ambas sedes.

Si se sustituyeran los puentes transparentes por routers en la línea serie entre la sede 1 y la sede 2 se reduciría el tráfico en la línea al suprimir el tráfico broadcast (por ejemplo el generado por mesnaejs ARP request). Esto debería ir acompañado de una subdivisión de la subred correspondiente en dos subredes. Si se ha hecho (como en este caso) un reparto inteligente de las direcciones en ambas sedes se puede realizar esta subdivisión con un mínimo impacto para los usuarios, sin necesidad de renumerar los equipos (aunque sí sería preciso modificar la máscara de subred a todos ellos).