3º GRADO EN INGENIERÍA INFORMÁTICA
Examen de Interconexión de Redes de Computadores
Convocatoria de Febrero. Curso: 2017 – 2018

NOMBRE:

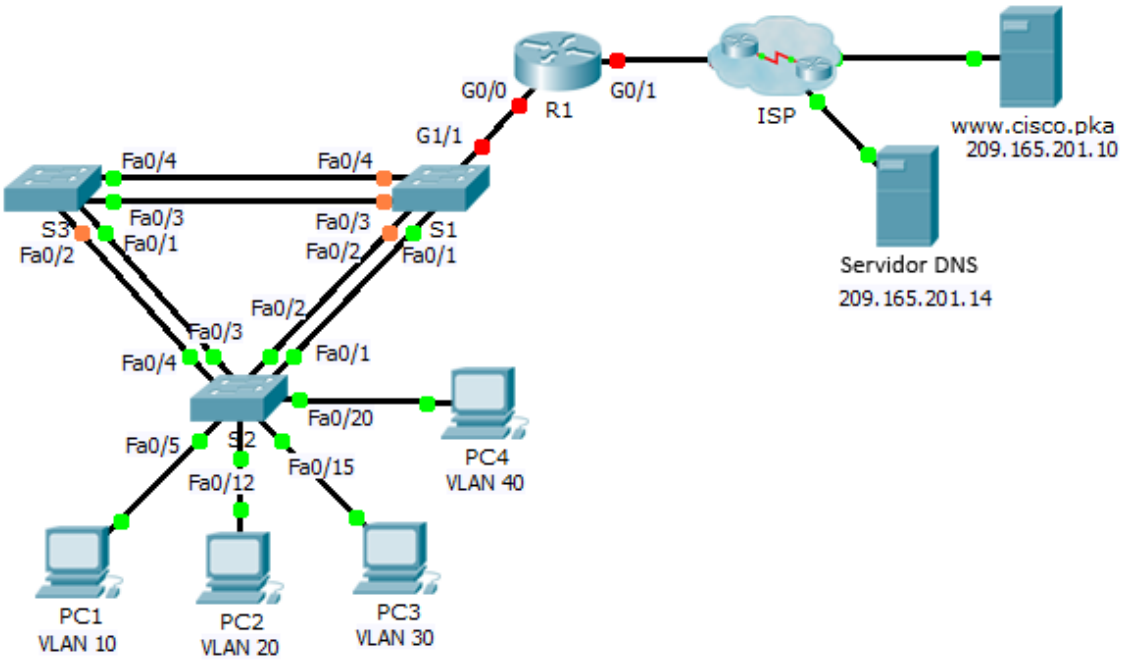
TEORÍA (2 PUNTOS):

CUESTIÓN	V/F
Un switch construye su tabla CAM para la conmutación de tramas con la siguiente información obtenida de una trama recibida: dirección origen e interfaz sobre la que se recibió la trama.	V
Si en una topología con varios switches y VLANs implementadas, lanzamos un mensaje "arp request" desde un PC, sólo los dispositivos conectados físicamente al mismo switch que el PC podrán verlo.	F
En la autoconfiguración de direcciones IPv6 por parte del propio equipo, juega un papel importante la dirección física impresa en la NIC.	V
En IPv6 la fragmentación en ruta está prohibida por lo que debe realizarse en el origen tras el descubrimiento de la MTU mínima del trayecto.	V
Para poder acceder de forma segura a un switch de capa 2, debemos asignarle una dirección IP a una de las interfaces físicas del equipo y configurar el acceso a las líneas vty mediante SSH.	F
Cuando configuramos las líneas vty de un switch para acceder a él de forma remota mediante SSH, la función del comando**: crypto key generate rsa** es generar una par de claves (pública y privada).	V
Para configurar un router como *DHCP relay* hay que indicarle la dirección del servidor DHCP mediante el comando **ip helper address** dentro del modo configuración de interfaz, sobre la interfaz destinada a capturar los mensajes *DHCP-request*.	V
Con el comando: **ip route 150.200.30.0 255.255.255.0 s0/0/0 200** creamos una ruta hacia la red 150.200.30.0 que sólo se utilizará en el caso de que no se reciban actualizaciones de los protocolos de routing anunciando dicha red (RIP, OSPF y/o EIGRP).	V
Dado que HTTP es un protocolo sin estado, es necesario guardar fragmentos de información (cookies) en el equipo del cliente a petición del servidor de la página que serán utilizadas por el servidor en posteriores conexiones.	V
UDP es el protocolo de transporte utilizado en la transmisión de vídeo y voz IP.	V
Cuando un switch recibe una trama sin etiquetar (IEEE.1q) en un enlace troncal, se la envía a la VLAN nativa.	V
En el enrutamiento entre VLANs, la interfaz de entrada y salida de los paquetes enrutados por el "router-on-a-stick" es la misma.	V
Los protocolos de routing en IPv6 utilizan las direcciones link-local como dirección de siguiente salto en las rutas hacia las distintas redes.	V
Las rutas IPv6 aparecen en la misma tabla de rutas que las rutas IPv4.	F
Para verificar la firma digital, el receptor aplica la función hash a la información original recibida (mensaje sin cifrar) y descifra la firma con la clave privada del emisor. El resultado debe ser el mismo en ambas operaciones.	F
En un router "Dual Stack", con OSPF activado tanto para IPv4 e IPv6, los mensajes OSPFv2 (IPv4) que envía llevan dirección origen la dirección IPv4 de la interfaz de salida. Mientras que los mensajes OSPFv3 (IPv6) que envía llevan dirección origen la dirección link-local de la interfaz de salida.	V
Cuando una interfaz de un switch ha sufrido una violación de seguridad, se debe emitir un comando de interfaz *shutdown / no shutdown* para volver a habilitar el puerto.	V
Durante el establecimiento de una conexión segura con un servidor, éste responde con un certificado digital que contiene su clave pública firmada digitalmente por una Autoridad de Certificación fiable.	V

Si desde un aula del Campus del Carmen, invocamos al servidor DNS y le pedimos que nos resuelva www.netacad.com, nos dará la respuesta y nos indicará que es “no autoritativa”	**V**
Las VPNs implementadas mediante IPsec ofrecen conectividad simple desde máquinas de escritorio no controladas por la compañía, poco o nulo mantenimiento del software en ellas y portales web personalizados para el usuario tras identificarse.	**F**

PROBLEMA 1. (1 punto)

Considera la topología dada en la figura:



1. Asignar direcciones IP a cada uno de los elementos (sobre el dibujo de la topología), teniendo en cuenta que la dirección de red asignada a la organización es: **209.164.0.0/30**. El reparto de direcciones ha de hacerse teniendo en cuenta:

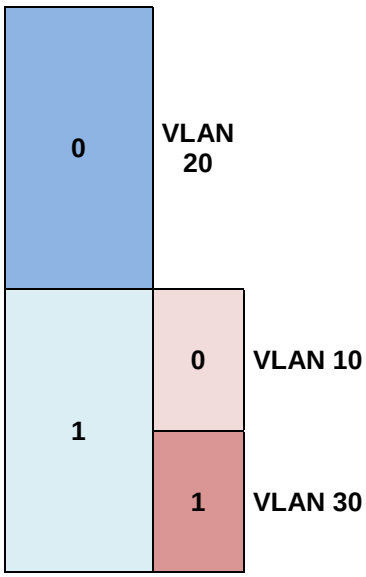
    a. La VLAN 10 tendrá 50 equipos.
    b. La VLAN 20 tendrá 63 equipos.
    c. La VLAN 30 tendrá 46 equipos.
    d. La VLAN 40 tendrá 37 equipos
    e. La red que conecta el R1 al router del ISP tiene 2 equipos.

    Las cantidades anteriores reflejan los equipos ya presentes en el dibujo.

RED	Nº HOSTS
VLAN 10	50
VLAN 20	63
VLAN 30	46
VLAN 40	37
R1-ISP	2

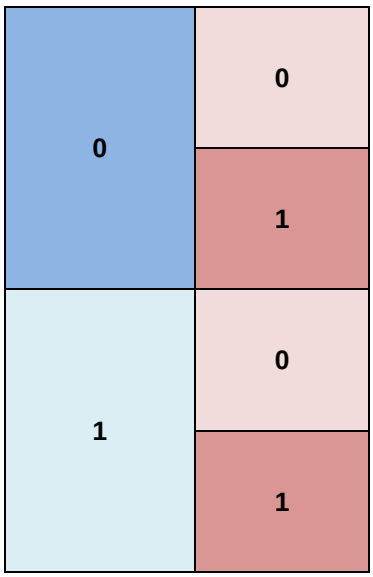
Red	Dirección de red	Máscara	Dir. Broadcast	Rango válido
VLAN 20	192.168.0.0	255.255.255.128	192.168.0.127	.1 - .126
VLAN 10	192.168.0.128	255.255.255.192	192.168.0.191	.129 - .190
VLAN 30	192.168.0.192	255.255.255.192	192.168.0.255	.193 - .254
VLAN 40	192.168.1.0	255.255.255.192	192.168.1.63	.1 - .62
R1-ISP	**209.164.0.0**	255.255.255.252	209.164.0.3	.1- .2

192.168.0.0/24



Máscara:	/25	/26
Nº IP válidas	126	62

192.168.1.0/24



Máscara:	/25	/26
Nº IP válidas	126	62

2. Indica, brevemente, la configuración que deberían tener S1, S2, S3 y R1 para que cualquier equipo de las VLANs 10, 20, 30 y 40 tenga plena conectividad.

- Configurar el direccionamiento IP (dirección., máscara, puerta enlace y servidor DNS) en cada equipo, según la VLAN a la que pertenece. Podremos configurarlo mediante DHCP.
- Configuración del router
  - como router on a stick: la interfaz troncal debe tener subinterfaces que serán las puertas de enlace de cada VLAN y debemos configurarle el protocolo de etiquetado 802.1q.
  - configurar la dirección IP estática que nos da el ISP en la interfaz WAN y salida por defecto al R_ISP o configurarlo como cliente DHCP
  - NATP
  - ACL (Firewall)
  - Acceso remoto SSH
- Configuración los switches de la topología:
  - Crear las VLAN 10, 20, 30 y 40 en todos los switches, una VLAN de administración y otra nativa
  - Asignar como puertos de acceso a las diferentes VLANs los que correspondan.
  - Configurar los enlaces troncales entre switches y con el Router
  - IP en la VLAN administrativa y puerta de enlace
  - Acceso remoto SSH
  - Seguridad de puerto

PROBLEMA 2 (1 punto)

En la topología anterior el servidor www.cisco.pka en un instante determinado, debe enviar 4380 bytes (datos de aplicación) a un cliente de la VLAN 10. Suponiendo que:

a. La MTU de todas las redes desde el servidor hasta el R ISP es: 1500 bytes.
b. La MTU del enlace entre R ISP y R1 es de 576 Bytes.
c. La MTU de la Intranet (de R1 a cada una de las VLANs) es: 1500 Bytes.

- Indica cómo y dónde se llevaría a cabo el proceso de fragmentación así como la longitud total de los datagramas originales y, para cada fragmento que se genere, el valor de los campos de la cabecera IP: ID, flag MF, Offset y Longitud total.

Bytes a enviar en la capa de aplicación:	4380
MTU red origen	1500
Nº de datagramas que salen del origen:	3

R_ISP debe fragmentar cada uno de los 3 datagramas:

MTU nueva	576
Datos IP en MTU nueva/8	69,5
Espacio para datos IP en nueva trama	552
Nº de fragmentos por cada datagrama:	2,68115942

Fragmentos por cada datagrama:	2	de tamaño total	572
	1	el último, de tamaño total	396

Datagrama	ID	MF	Offset	LT
Orig 1	1	0	0	1500
Frag 1.1	1	1	0	572
Frag 1.2	1	1	69	572
Frag 1.3	1	0	138	396
Orig 2	2	0	0	1500
Frag 2.1	2	1	0	572
Frag 2.2	2	1	69	572
Frag 2.3	2	0	138	396
Orig 3	3	0	0	1500
Frag 3.1	3	1	0	572
Frag 3.2	3	1	69	572
Frag 3.3	3	0	138	396

PROBLEMA 3 (1 punto)

Representar la secuencia de envío a nivel de transporte entre los servidores y el cliente del ejercicio anterior:

1. La entidad de transporte del cliente envía una petición **DNS request** a la entidad de transporte del servidor DNS (Puerto cliente: 1040, puerto del servidor: 53) para preguntar por la dirección IP correspondiente a **www.cisco.pka**.

2. La entidad de transporte del servidor DNS envía un **DNS response** con la dirección correspondiente a **www.cisco.pka**: 209.165.201.10.

3. Una vez conocida la IP de la máquina que aloja al servidor **www.cisco.pka ,** la entidad de transporte del Cliente establece conexión con la entidad de transporte del Servidor HTTP **www.cisco.pka** (Puerto cliente: 1030, puerto del servidor: 80).

4. El cliente envía la orden "**GET**" para solicitar la transferencia de la página web del Servidor **www.cisco.pka** .

5. El servidor **www.cisco.pka** envía al cliente: 4380 Bytes de datos (página web en formato MIME), mediante TCP.

6. La entidad de transporte del servidor **www.cisco.pka** cierra la conexión.

Consideraciones:

- Las entidades de transporte del Cliente y Servidor negocian un tamaño máximo de datos en cada segmento (MSS) acorde a la MTU de las redes en las que se encuentran conectados.
- La entidad de transporte del Cliente anuncia un tamaño de ventana inicial de 8760 Bytes.
- El número de secuencia inicial de la entidad de transporte del Cliente es 3000 y la del Servidor www.cisco.pka es 0.
- Sólo se transmiten segmentos TCP y/o datagramas UDP al principio de un tic de reloj y tardan en llegar al destino medio tic de reloj, si no se pierden.
- El temporizador para las retransmisiones de segmentos TCP es de 3 tics de reloj.
- Suponer que **no se pierde ningún segmento de datos.**
- La aplicación lee datos del buffer del RX cuando está a la mitad de su capacidad inicial.

Dibuja cómo se llevaría a cabo la transmisión UDP y TCP, incluyendo el establecimiento y el cierre de la conexión TCP y las ventanas de recepción de B y trasmisión de A.

NOTA: suponer que los segmentos de acuse de recibo "puros" no gastan números de secuencia, mientras que los segmentos involucrados en el inicio y cierre de la conexión (que tengan activado el bit SYN o el bit FIN) gastan 1 número de secuencia.

La MTU de las redes en las que se encuentran el servidor HTTP y el cliente es de 1500 Bytes. De modo que negociarán un
MSS=MTU-cab. IP-cab. TCP.
Es decir, MSS=1500-20-20=1460 Bytes

El servidor HTTP deberá enviarle al cliente la página web de 4380 Bytes en 4380/1460 = 3 segmentos con datos

La ventana inicial del cliente es de 8760 Bytes, por lo que cabrían 8760/1460 = 6 segmentos de 1460 Bytes de datos