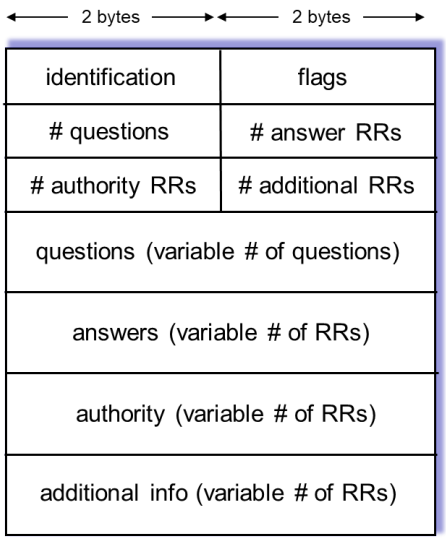
**Redes de Computadoras**
**Letra y Soluciones – 25 de julio de 2022**

## Pregunta 1 (12 puntos)

a) Muestre el formato de los mensajes consulta y respuesta de DNS y la utilidad de cada uno de sus campos. En particular, explique la utilidad de al menos 4 banderas (*flags*).
b) ¿Es posible que un mensaje de respuesta de DNS contenga sólo la cabecera? Justifique.

## Solución Pregunta 1

a) Ambos mensajes tienen el mismo formato. Este es:




Los primeros 12 bytes constituyen la sección de cabecera, la cual contiene una serie de campos.
El primero de estos campos es un número de 16 bits que **identifica** la consulta. Este identificador se copia en el mensaje de respuesta a la consulta, lo que permite al cliente establecer las correspondencias correctas entre las respuestas recibidas y las consultas enviadas.
En el campo **Flags** se incluyen una serie de banderas. A continuación se mencionan y describen las básicas.
Una flag **consulta/respuesta** (**qr**) de 1 bit informa si el mensaje es una consulta (0) o una respuesta (1).
Una bandera **autoritativa** (**aa**) de 1 bit se activa en un mensaje de respuesta cuando el servidor DNS que genera la respuesta es un servidor autoritativo para el nombre solicitado.
La bandera **recursión-deseada** (**rd**), también de 1 bit, se activa cuando un cliente (host o servidor DNS) desea que el servidor DNS realice una recursión cuando no disponga del registro.
En un mensaje de respuesta, la flag de **recursión-disponible** (**ra**) de 1 bit se activa si el servidor DNS que responde soporta la recursión.
En la cabecera también se incluyen cuatro campos **"número de"** (**#...**), que indican el número de apariciones de los cuatro tipos de secciones de datos que siguen a la cabecera.
El resto de mensaje tiene por tanto un largo variable, pudiendo contener 4 campos distintos (cada uno de largo variable): **consultas** (**questions**), **respuestas** (**answers**), **autoridad** (**authority**) y **información adicional** (**additional information**).
La sección **consultas** (**questions**) contiene información acerca de la consulta que se va a realizar. Esta sección incluye un campo de nombre que contiene el nombre que se va a consultar y un
campo de tipo que especifica el tipo de cuestión que se plantea acerca del nombre; por ejemplo, la
dirección del host asociada con un nombre (tipo A) o el servidor de correo para un nombre (tipo
MX).
En una respuesta de un servidor DNS, la sección **respuestas** (**answers**) contiene los registros del recurso para el nombre que fue consultado originalmente. En cada registro de recurso (RR) existe un parámetro Tipo (por ejemplo, A, NS, CNAME y MX), un parámetro Valor y el parámetro TTL. Una respuesta puede devolver varios registros de recursos, ya que un nombre de host puede tener asociadas varias direcciones IP.

La sección **autoridad** (**authority**) contiene información autoritativa relacionada con la consulta realizada.
La sección **información adicional** (**additional information**) contiene otros registros útiles. Por ejemplo, el campo de respuesta en un mensaje de respuesta a una consulta MX contiene un registro de recurso que proporciona el nombre de host canónico de un servidor de correo. Esta sección de información adicional contiene un registro de tipo A que proporciona la dirección IP para el nombre de host canónico del servidor de correo.

b) Si la consulta que motiva dicha respuesta está bien formada, no, no es posible, pues en la respuesta siempre se incluye en la sección **consultas** (**questions**), la query realizada.

**Pregunta 2 ( 12 puntos)**
Suponga que hay dos programas, un emisor y un receptor, transfiriendo datos sobre Internet usando transporte TCP.
a) ¿Qué mecanismo entra en acción si el transmisor genera datos a una tasa mayor de la que la red es capaz de transportar? Describa brevemente el principio de funcionamiento del mecanismo.
b) ¿Qué mecanismo entra en acción si el transmisor genera datos a una tasa mayor de la que el receptor es capaz de recibir? Describa brevemente el principio de funcionamiento del mecanismo.

**Solución Pregunta 2**

a) Control de congestión. El mecanismo consiste en ajustar la cantidad de paquetes sin confirmar que el emisor está permitido generar. Esta cantidad se ajusta respondiendo a eventos que son interpretados como síntomas de congestión, tales como la llegada de ACKs duplicados o eventos de *timeout*. Mientras estos eventos no se dan, el emisor intenta aumentar esta cantidad. Este ajuste se realiza controlando el tamaño de la ventana de congestión, que luego tiene impacto en el tamaño de la ventana de transmisión.

b) Control de flujo. En ese mecanismo el receptor notifica al emisor de la cantidad de buffer local disponible, usando los mensajes ACK. Esto permite al emisor ajustar la emisión de datos de forma de no desbordar al receptor. Para esto ajusta la ventana de recepción del emisor con la cantidad máxima de datos que puede soportar el receptor.

**Pregunta 3 (8 puntos)**
Indique y describa brevemente las dos funciones principales de la capa de red y como funcionan en conjunto.

**Solución Pregunta 3**

**a) Reenvío (forwarding)**: mover paquetes entre puertos de entrada y salida del router.
**Enrutamiento (routing)**: determinar la ruta de los paquetes desde origen a destino. Para ello existen los algoritmos de enrutamiento.
**Interacción:** Cada router intercambia con sus pares, mediante al menos un protocolo de enrutamiento, información que se utiliza, en al menos un algoritmo de enrutamiento, para poblar sus tablas de forwarding. Dichas tablas, en su formato más básico contienen para un valor de dirección contenido en la cabecera de los paquetes que llegan al router, el enlace de salida. De esta forma, para cada paquete que arriba a un router por cualquiera de sus

interfaces, el router examina la tabla de forwarding (en el caso de IP a partir de la dirección IP destino contenida en el encabezado IP) y a partir del “longest match” determina por qué interfaz debe ser enviado (además de determinar cuál es el “next hop”, lo que determina en el caso más genérico, la dirección destino de capa de enlace que deberá contener la trama que lo lleve a su próximo salto).

**Pregunta 4 (8 puntos)**

a) Describa el algoritmo *CSMA/CD* de acceso al medio utilizado en *Ethernet*.

b) Describa el mecanismo de *backoff* exponencial binario ejecutado luego de una colisión.

**Solución Pregunta 4**

*a)*

*1. El adaptador de red obtiene un datagrama de la capa de red, prepara una trama de capa de enlace y la coloca en el buffer del adaptador.*
*2. Si el adaptador detecta que el canal está inactivo (es decir, no hay señal de energía entrando al adaptador desde el canal), comienza a transmitir la trama. Si, por otro lado, el adaptador detecta que el canal está ocupado, espera hasta que detecta que no hay señal, y luego comienza a transmitir la trama.*
*3. Mientras transmite, el adaptador monitoriza la presencia de energía de señales provenientes de otros adaptadores que usan el canal de transmisión.*
*4. Si el adaptador transmite la trama completa sin detectar señales de otros adaptadores, la trasmisión de la trama se da por finalizada. Si, por el contrario, el adaptador detecta señales de otros adaptadores mientras transmite, aborta la transmisión (es decir, deja de transmitir su trama).*
*5. Después de parar la trasmisión, el adaptador espera una cantidad de tiempo aleatoria y luego regresa al paso 2.*

*b)*

*La espera aleatoria se implementa mediante el algoritmo de backoff exponencial binario. Cuando al transmitir una trama se experimentan n colisiones, el nodo elige un valor de K al azar entre {0, 1, 2, . . . . 2exp(n) - 1}. De este modo, cuantas más colisiones experimente una trama, mayor será el intervalo desde el cual K es elegido. Para Ethernet, la cantidad real de tiempo que espera un nodo es K veces la cantidad de tiempo necesario para enviar 512 bits a Ethernet) y n está topeado en 10.*

**Problema 1 (30 puntos)**

Suponga un escenario con dos host de red A y B donde B desea enviar a A un conjunto de mensajes de datos que ya tiene disponibles. El envío de mensajes debe cumplir los siguientes requisitos:

- La capa superior es la que solicita en el host A un nuevo dato. Cuando en A se recibe una solicitud de la capa superior para obtener el siguiente mensaje de datos (D) de B, A tiene que enviar un mensaje de solicitud (R) a B a través del canal que va de A a B.
- Solo cuando B recibe un mensaje R puede devolver un mensaje de datos (D) a A a través del canal de B a A.
- A tiene que entregar exactamente una copia de cada mensaje D a la capa superior.
- Los mensajes R se pueden perder (pero no corromper) en el canal de A a B.
- Los mensajes D, una vez enviados, siempre son correctamente entregados.
- El retardo a lo largo de ambos canales es desconocido y variable.

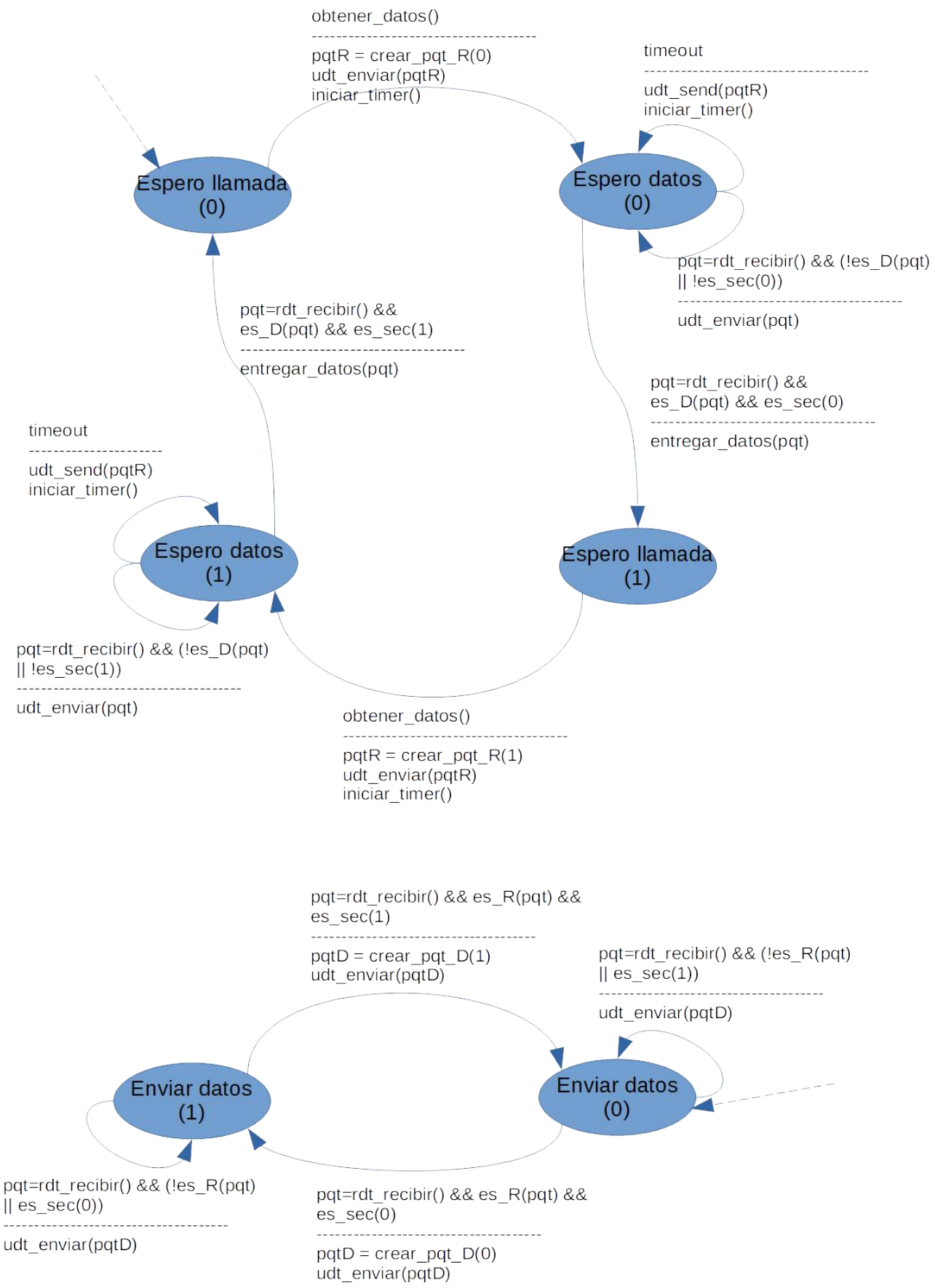
**Se pide:**

a) Diseñe y describa mediante máquinas de estados el protocolo que refleje el comportamiento de las dos entidades descrito anteriormente. Debe dar la máquina de estados de A y de B.
b) Explique brevemente las decisiones tomadas en el diseño de su protocolo.

Utilice las siguientes funciones como base para su diseño, puede modificarlas y/o agregar nuevas si lo considera necesario:
`obtener_dato()` (llamada de capa superior), `pqtR=crear_pqt_R()`, `pqtD=crear_pqt_D()`, `es_R(pqt)`, `es_D(pqt)`, `udt_enviar(pqt)`, `pqt=rdt_recibir()`, `entregar_datos(pqt)` (entrega datos de pqt a la capa superior)

**Solución 1**

Debido a que el canal A-B puede perder mensajes de solicitud, A necesitará un tiempo de espera y retransmitir sus mensajes de petición (para poder recuperarse de la pérdida). Dado que los retrasos del canal son variables y desconocidos, es posible que A envíe solicitudes duplicadas (es decir reenviar un mensaje de solicitud que ya ha sido recibido por B). Para poder detectar mensajes de solicitud duplicados, el protocolo utilizará números de secuencia. Un número de secuencia de 1 bit será suficiente para un protocolo de solicitud/respuesta del tipo "stop and wait".
En el caso de B, no se consideran retransmisiones ya que el canal de B a A no pierde mensajes.


obtener_datos()
---
pqtR = crear_pqt_R(0)
udt_enviar(pqtR)
iniciar_timer()
timeout
---
udt_send(pqtR)
iniciar_timer()
Espero llamada (0)
Espero datos (0)
pqt=rdt_recibir() && (!es_D(pqt) || !es_sec(0))
---
udt_enviar(pqt)
pqt=rdt_recibir() && es_D(pqt) && es_sec(1)
---
entregar_datos(pqt)
pqt=rdt_recibir() && es_D(pqt) && es_sec(0)
---
entregar_datos(pqt)
timeout
---
udt_send(pqtR)
iniciar_timer()
Espero datos (1)
Espero llamada (1)
pqt=rdt_recibir() && (!es_D(pqt) || !es_sec(1))
---
udt_enviar(pqt)
obtener_datos()
---
pqtR = crear_pqt_R(1)
udt_enviar(pqtR)
iniciar_timer()
pqt=rdt_recibir() && es_R(pqt) && es_sec(1)
---
pqtD = crear_pqt_D(1)
udt_enviar(pqtD)
pqt=rdt_recibir() && (!es_R(pqt) || es_sec(1))
---
udt_enviar(pqtD)
Enviar datos (1)
Enviar datos (0)
pqt=rdt_recibir() && (!es_R(pqt) || es_sec(0))
---
udt_enviar(pqtD)
pqt=rdt_recibir() && es_R(pqt) && es_sec(0)
---
pqtD = crear_pqt_D(0)
udt_enviar(pqtD)

**Problema 2 (30 puntos)**

Sea una empresa con 4 grupos de trabajo *Administración*, *Ventas*, *Servicio técnico* y *Desarrollo*. La empresa contrata un servicio de acceso a Internet que le proporciona el rango de direcciones IP 193.91.90.0/24, donde el primer prefijo /30 del rango es utilizado para la conexión con el ISP (*Proveedor de Servicios de Internet*).

Se desea que todos los equipos de la empresa cuenten con una dirección IP pública y que cada grupo utilice una subred definida exclusivamente para el grupo.
La cantidad de equipos que utilizará cada grupo son: *Administración* 6 equipos; *Ventas* 12 equipos; *Servicio técnico* 60 equipos; *Desarrollo* 125 equipos.

El equipamiento de conectividad de la empresa es, un *router* con 8 puertos de conexión Ethernet, del cual uno de ellos se utiliza para la conexión con el ISP. Además se dispone de 5 *switches* de 48 puertos (*sw48_1*, *sw48_2*, *sw48_3*, *sw48_4* y *sw48_5*) y dos *switches* de 24 puertos (*sw24_1* y *sw24_2*).
Se pide:

a) Asigne el prefijo de subred a utilizar por cada grupo de trabajo.
b) Suponiendo que todos los equipos de un grupo se encuentran cercanos entre si, genere un mapa de conexión del *router* y los *switches*, con una distribución de los dispositivos y la conexión entre ellos, indicando que subred atienden, que permita soportar la red planteada.
c) Suponiendo ahora que el *router* y los *switches* manejan VLANs (norma IEEE 802.1Q), modifique su solución anterior para permitir la instalación de equipos de cualquier grupo en cualquier puerto del los distintos *switches*.
    i. Indique el esquema de conexión requerido, indicando el protocolo de capa 2 utilizado en cada enlace y configuración requerida.
    ii. ¿Es posible reutilizar su asignación de la parte a) para este escenario? Justifique.

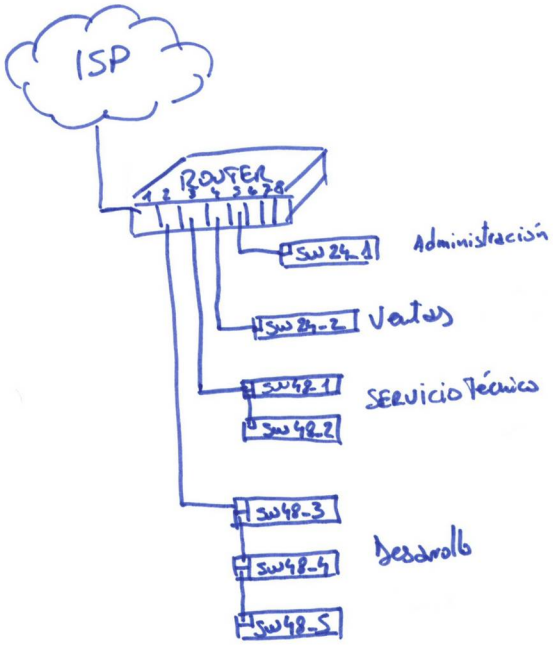
**Solución 2**

a) Cada grupo posee los siguientes requerimientos:

Administración: 6 equipos + router + dir. LAN + dir Broadcast → 9 direcciones → /28
Ventas: 12 equipos + router + dir. LAN + dir Broadcast → 15 direcciones → /28
Servicio Técnico: 60 equipos + router + dir. LAN + dir Broadcast → 63 direcciones → /26
Desarrollo: 125 equipos + router + dir. LAN + dir Broadcast → 128 direcciones → /25
ISP: 1 router + router ISP + LAN + dir Broadcast → 4 direcciones → /30

Administración: 193.91.90.32/28
Ventas: 193.91.90.48/28
Servicio Técnico: 193.91.90.64/26
Desarrollo: 193.91.90.128/25
ISP: 193.91.90.0/30 (pues: “el primer /30 del rango de IPs es utilizado para la conexión con el ISP”)

b)




Se configuran 5 de las 8 bocas con cada una de las redes definidas. En cada subred se configura la primer dirección a la interfaz correspondiente del router.
La boca 1 se conecta al ISP
La boca 2, asignada a Desarrollo, se conecta a un equipo de 48 bocas, conectado a otros dos equipos de 48 bocas “en cascada”. A éstos se conectan los 125 equipos y quedan 14 bocas libres (48x3-5-125).
La boca 3, asignada a Servicio Técnico, se conecta a un equipo de 48 bocas, conectado a otro “en cascada”. A éstos se conectan los 60 equipos y quedan 33 bocas libres (48x2-3-60)
La boca 4, asignada a Ventas, se conecta a un equipo de 24 bocas. Se le conectan los 12 equipos y quedan 11 bocas libres (24-1-12).
La boca 5, asignada a Administración, se conecta a un equipo de 24 bocas. Se le conectan los 6 equipos y quedan 17 bocas libres (24-1-6).

c) Hay 2 topologías válidas: conectar un switch al router y luego cada switch a este router (donde todos los enlaces son trunk) o conectar el router y todos los switches en serie con enlaces trunk.
Veamos el caso donde se conectan los 7 switches y el router en serie.
La boca 1, de conexión al ISP, mantiene la configuración anterior. Se definen 4 VLANs para desarrollo, servicio técnico, ventas y administración con tags 100, 101, 102 y 103 respectivamente. Se definen 4 interfaces virtuales en la boca 2 del router, configurándolas con las direcciones IP de las interfases físicas anteriores.
La boca 2se configuran en modalidad de trunk y se pasan todas las VLANs taggeadas.
A los switches se les configuran las VLANs 100, 101, 102 y 103. Se les configura el puerto 1 y 2 de cada switch como trunk y el resto de las bocas como acceso.