Repaso de teoría

1. ¿Qué es y para qué sirve STP? ¿Cuáles fueron sus evoluciones?

STP (Spanning Tree Protocol) es un protocolo de nivel 2 (enlace de datos) definido por el estándar IEEE 802.1D que evita bucles de red en topologías conmutadas. Sirve para garantizar que en una red Ethernet exista una única ruta activa entre dos nodos, desactivando enlaces redundantes si es necesario.

En una red Ethernet sin control:

* Si hay caminos redundantes, un paquete puede circular indefinidamente → **tormentas de broadcast**.
* Los switches aprenden direcciones MAC incorrectas al recibir múltiples copias de una misma trama.
* **Congestión** en la red → caída total del servicio.

STP crea una topología lógica en forma de árbol libre de bucles, desactivando enlaces redundantes de forma temporal. Para esto:

1. Se elige un Root Bridge (el switch con menor Bridge ID).
2. Se calcula el camino más corto (de menor costo) desde cada switch al Root.
3. Se definen roles:
   * Root Port (RP): el mejor puerto de un switch para llegar al Root Bridge.
   * Designated Port (DP): el mejor puerto en un segmento LAN para reenviar tráfico hacia el Root.
   * Otros puertos se bloquean si generan bucles.

IEEE 802.1D – STP (Spanning Tree Protocol clásico)

El protocolo original, definido por el estándar IEEE 802.1D, fue creado para prevenir bucles en redes conmutadas mediante la construcción de una topología lógica en forma de árbol sin ciclos. Para ello, designa un switch raíz (Root Bridge) y calcula los caminos más cortos hacia él, bloqueando enlaces redundantes que podrían causar bucles. Cada switch clasifica sus puertos en estados como Blocking, Listening, Learning, y Forwarding, lo cual permite determinar si un puerto puede reenviar tráfico. Sin embargo, su principal desventaja es su lenta convergencia, ya que puede tardar entre 30 y 50 segundos en estabilizar la red ante un cambio de topología.

IEEE 802.1w – RSTP (Rapid Spanning Tree Protocol)

Esta evolución reemplaza a STP clásico y se enfoca en reducir drásticamente los tiempos de convergencia en caso de fallos o cambios en la red. RSTP fusiona tres de los estados anteriores en uno solo llamado Discarding, simplificando la transición de los puertos. A diferencia del STP, donde solo el Root Bridge envía BPDUs periódicos, en RSTP todos los switches intercambian BPDUs activamente, permitiendo detectar rápidamente cambios en la topología. Además, introduce dos nuevos tipos de puertos: Alternate Port, que ofrece un camino alternativo hacia el Root Bridge, y Backup Port, que actúa como respaldo de un enlace en el mismo segmento. Gracias a estas mejoras, RSTP permite una recuperación casi instantánea de la red.

IEEE 802.1s – MSTP (Multiple Spanning Tree Protocol)

MSTP fue diseñado para abordar las limitaciones del STP y RSTP en entornos con múltiples VLANs. En lugar de crear una instancia de árbol por cada VLAN, lo cual genera consumo de recursos y tráfico innecesario, MSTP permite agrupar varias VLANs bajo una misma instancia de spanning tree, reduciendo el uso de CPU y la cantidad de BPDUs circulando por la red. Esto no solo mejora el rendimiento, sino que también habilita el balanceo de carga al permitir que diferentes VLANs usen distintos caminos activos en la red. Esta flexibilidad lo convierte en la mejor opción para redes empresariales medianas y grandes con segmentación lógica avanzada.

IEEE 802.1aq – SPB (Shortest Path Bridging)

SPB representa una evolución completa de los protocolos anteriores. En lugar de bloquear puertos para evitar bucles, como hacen STP, RSTP y MSTP, utiliza todos los enlaces disponibles gracias a un enfoque basado en el conocimiento completo de la topología de red. Esto se logra mediante un plano de control distribuido, que permite a los switches calcular las rutas más cortas hasta todos los destinos (similar al enrutamiento en redes IP). SPB ofrece altísima escalabilidad, recuperación rápida ante fallos, y mayor eficiencia en el uso del ancho de banda. Soporta dos modos: SPBV (basado en VLAN ID) y SPBM (basado en MAC). Es especialmente útil en grandes redes metropolitanas o de centros de datos.

1. Dentro de las variantes de STP cual o cuales pueden usarse para un entorno con vlans

 **IEEE 802.1s (MSTP)** es la **variante específica para redes con VLANs**, ya que permite manejar múltiples VLANs sobre una sola instancia de árbol lógico.

 **SPB (IEEE 802.1aq)** también puede usarse en redes con VLANs, y lo hace con mayor eficiencia, especialmente en redes complejas o grandes.

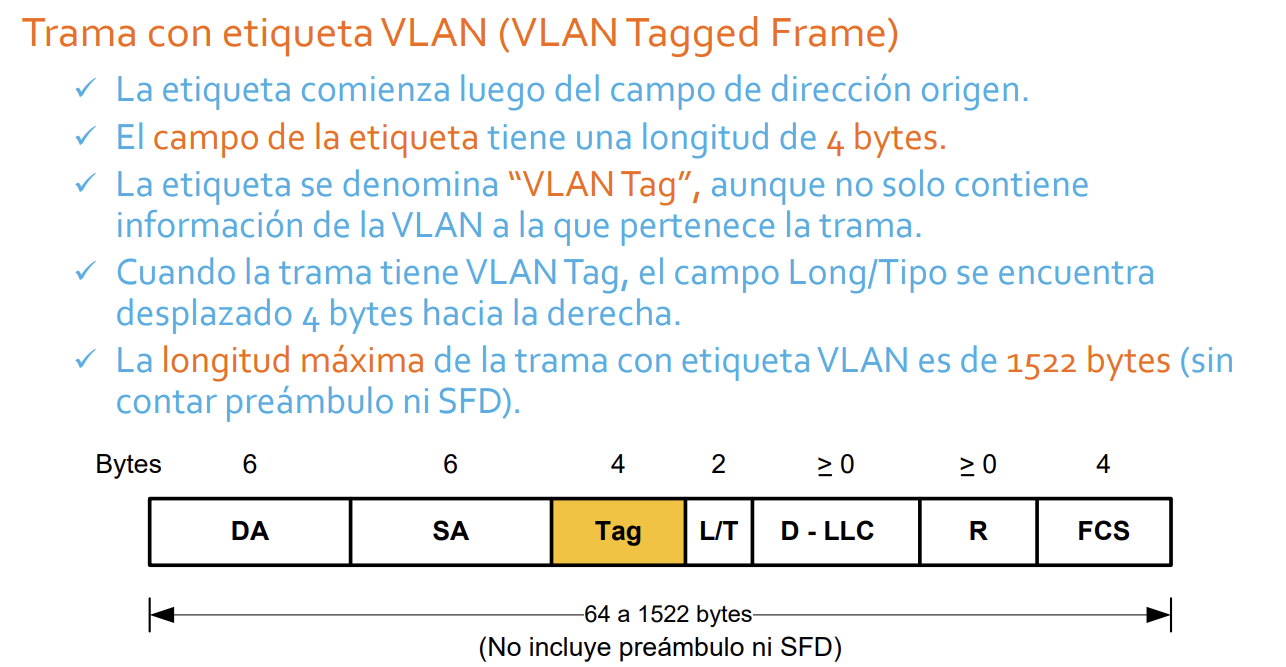
1. Describa los distintos mecanismos de retransmisión de tramas usados en switch

Los **switches** pueden operar con los siguientes modos de retransmisión de tramas:

* **Store and Forward (Almacenamiento y envío)**: Almacena toda la trama, verifica errores con CRC, y solo retransmite si no hay errores. Más seguro, pero con más latencia.
* **Cut Through (Rápido)**: Lee solo los primeros 6 bytes (dirección destino) y reenvía la trama inmediatamente. Menor latencia, sin verificación de errores.
* **Modified Cut Through (Rápido modificado)**: Lee 64 bytes antes de reenviar. Considera que la mayoría de errores ocurren en esos primeros bytes. No realiza control de errores.

1. ¿Qué estándar debe soportar un switch para que soporte vlans?

El switch debe cumplir con el estándar IEEE 802.1Q, que define el etiquetado de tramas VLAN en redes Ethernet. Esto permite segmentar lógicamente una red física en múltiples redes virtuales



1. ¿Qué es link aggregation y para qué sirve?

**Link Aggregation** es una técnica que permite **combinar múltiples enlaces físicos** entre switches en un único enlace lógico para:

* Aumentar el ancho de banda total.
* Proveer redundancia (si un enlace falla, los demás siguen activos).
* Balancear la carga de tráfico entre enlaces.

Es útil tanto para mejorar el rendimiento como la disponibilidad de la red. Se basa en el estándar **IEEE 802.3ad**

Agregar aquí tipos de switches con info extra, puerto uplink, switch administrable y copiar lo de VLAN Tagged y Untagged del power.

1. Investigue acerca de la placa de 10 Gb modelo DXE-820T y conteste las siguientes preguntas:
   1. ¿La placa soporta conexión de fibra óptica multimodo?

No. La placa soporta los estándares 100BASE-TX, 1000BASE-T, 10GBASE-T. Todos ellos trabajan sobre cables de cobre. Está diseñada para utilizarse con cables de cobre de par trenzado, como los Cat 6, Cat 6a o superiores.

* 1. ¿Soporta autonegociación? ¿Se puede conectar a un switch Ethernet 802.3?

Sí, la D-Link DXE-820T **soporta autonegociación**, lo que le permite adaptarse automáticamente a la velocidad y modo de operación del dispositivo al que se conecta. Es compatible con los estándares IEEE 802.3 a partir de 100 Mbps, 100BASE-TX, 1000BASE-T y 10GBASE-T. Por lo tanto, no se puede conectar a un switch Ethernet 802.3 pues no negocia ni opera en la velocidad de 10 Mbps.

* 1. ¿Si tuviera oficinas cableadas con cable UTP Cat. 5e, podría instalar esta placa en un servidor y conectarlo a la red?

Sí, es posible instalar la DXE-820T en un servidor y conectarlo a una red cableada con UTP Cat. 5e. Sin embargo, es importante tener en cuenta que, para alcanzar velocidades de 10 Gbps, se recomienda el uso de cables Cat. 6a o superiores. Con cables Cat. 5e, la tarjeta funcionará a velocidades de 100 Mbps o 1 Gbps, dependiendo de la calidad del cableado y la distancia.

* 1. ¿Por qué soporta Jumbo Frames?

La DXE-820T **soporta Jumbo Frames** para mejorar la eficiencia de la red al permitir el envío de tramas de mayor tamaño que las estándar (hasta 9.6 KB). Esto reduce la sobrecarga de procesamiento en la CPU y mejora el rendimiento en aplicaciones que manejan grandes volúmenes de datos, como servidores de archivos o bases de datos.

* 1. ¿Qué característica del funcionamiento de la placa favorece a su criterio a los procesos que se ejecutan en un servidor?

Una característica destacada de la DXE-820T es su capacidad de **offloading de checksum** para los protocolos TCP, UDP e IP. Esto significa que la tarjeta puede encargarse del cálculo y verificación de sumas de verificación, liberando a la CPU del servidor de estas tareas y mejorando el rendimiento general del sistema.

* 1. ¿Es posible instalar más de una placa en un servidor y trabajar en forma eficiente, ampliando el ancho de banda del mismos, de forma tal que las consultas de las aplicaciones sean respondidas en forma eficiente?

Sí, la DXE-820T **soporta la configuración de múltiples adaptadores en un servidor** mediante técnicas como el **teaming** o **Smart Load Balancing™**. Esto permite combinar varias interfaces de red para aumentar el ancho de banda disponible y proporcionar tolerancia a fallos, asegurando una respuesta eficiente a las consultas de las aplicaciones.

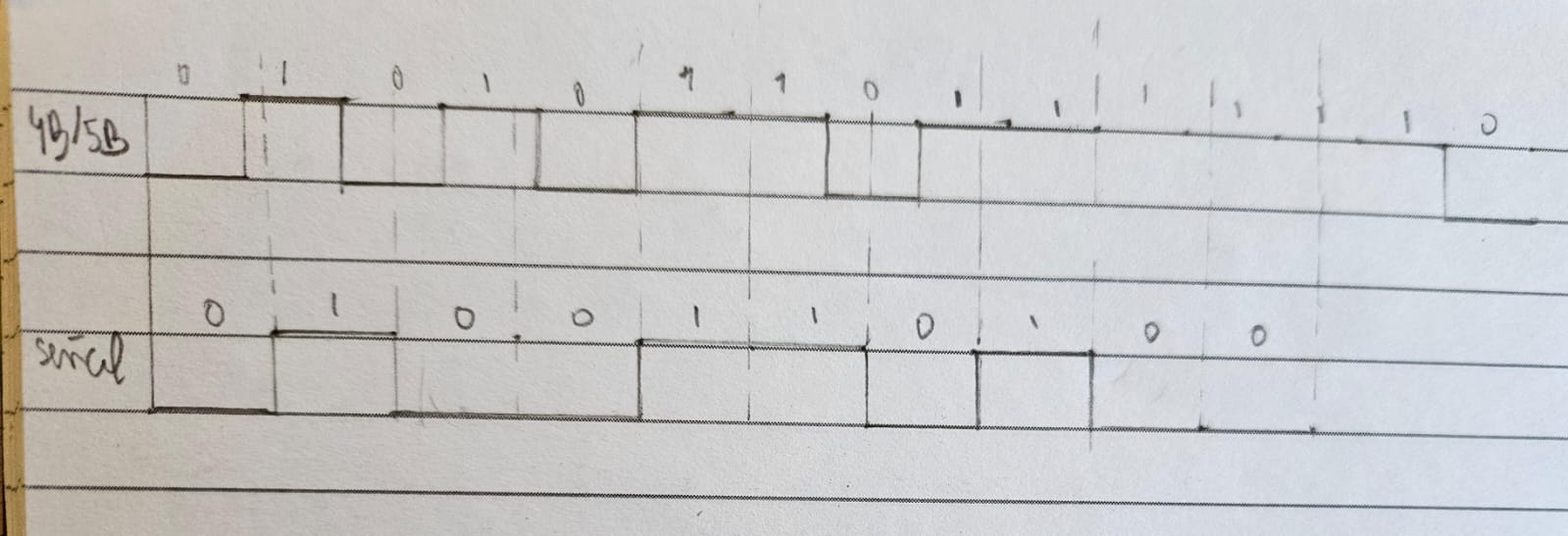
**NIC Teaming** (también llamado “Bonding” en Linux o “Adapter Teaming”) es la técnica de agrupar dos o más placas de red físicas (NICs) en un solo adaptador lógico, que actúa como una única interfaz para el sistema operativo.

Smart Load Balancing™ es una implementación propietaria de teaming inteligente, ofrecida por algunos fabricantes como Broadcom o D-Link. Tiene las siguientes características:

🔄 1. Balanceo de carga de salida (Outbound Load Balancing)

Distribuye dinámicamente el tráfico saliente entre las NICs del equipo según el uso actual, sin requerir cambios en el switch.

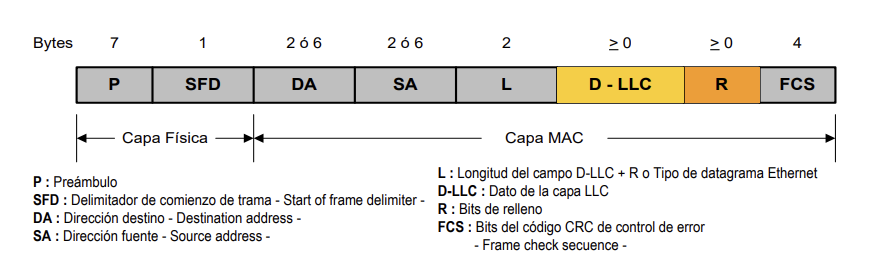
1. Dado el siguiente string 0100110100 codificar usando 4B/5B.



1. Ud. está diseñando la cabecera de un protocolo MAC y dispone de los siguientes campos: MAC origen, MAC destino, Tipo, Control, de 6,6,2 y 4 Bytes respectivamente.

¿En qué orden ubicaría los campos dentro de la cabecera MAC para mejorar la perfomance de los puentes transparentes? ¿Cómo lo hace Ethernet?

En primer lugar, colocaría la MAC destino ya que es lo que el puente debe inspeccionar para saber dónde reenviar la trama. Luego, colocaría la dirección MAC origen ya que el puente la utiliza para el aprendizaje de direcciones. Luego, el tipo que indica a capa superiores el protocolo de capa superior (no lo utiliza el puente). Y finalmente el código de control ya que es el que verifica la integridad de la trama completa.





1. Compare el overhead que producen el preámbulo (8 bytes) más un espacio interframe de 12 Bytes, en una red Fast Ethernet y el tamaño mínimo de paquete (64 bytes) y una red Giga Ethernet y el tamaño mínimo de paquete (512 bytes).

En una red Fast Ethernet, siendo el tamaño mínimo de paquete igual a 64 bytes y sumando a la trama el preámbulo de 8 bytes y espacio interframe de 12 bytes, obtenemos una trama de 84 bytes.

Luego, el overhead del paquete es igual a

overhead = (Longitud de preámbulo + interframe) / Longitud del paquete = 20 Bytes/84 bytes = 0,238 = 23,8 %

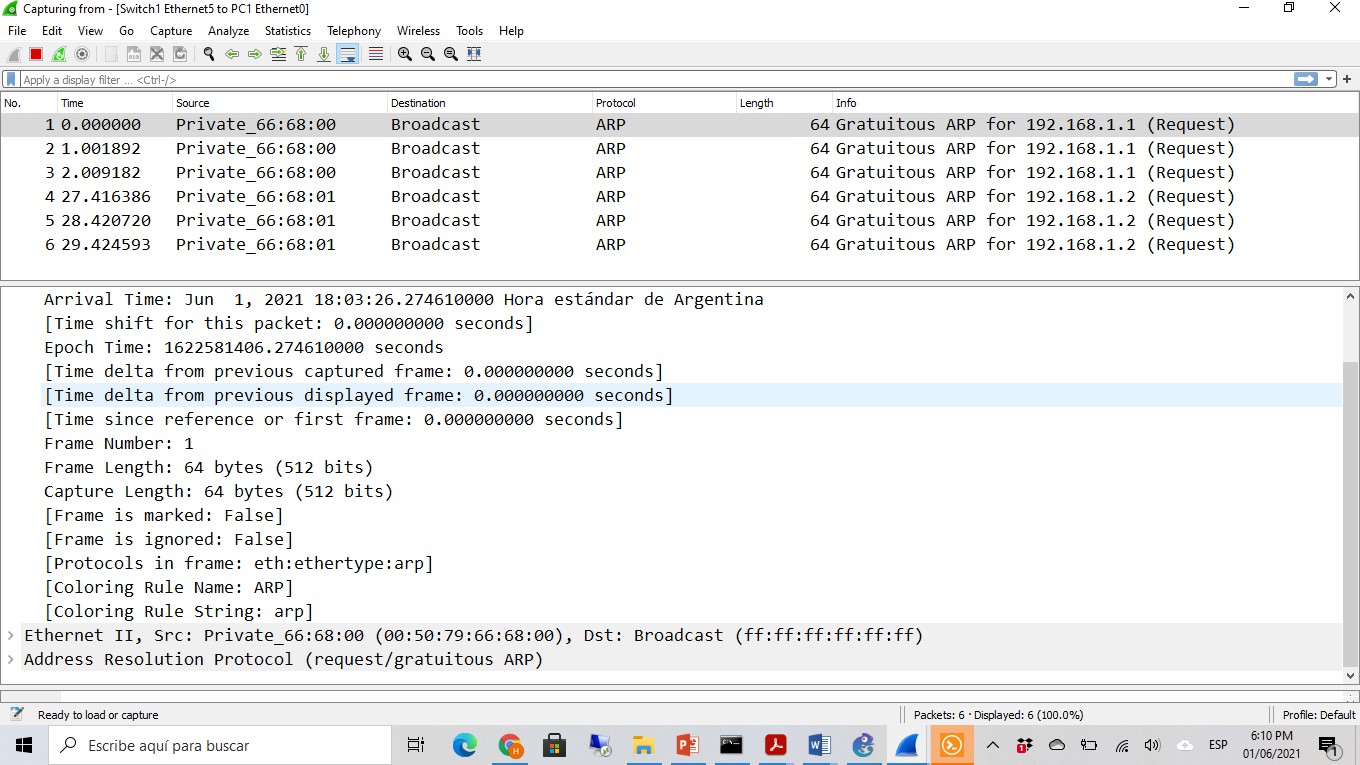
En una red Giga Ethernet, siendo el tamaño mínimo de paquete igual a 512 bytes y sumando a la trama el preámbulo de 8 bytes y espacio interframe de 12 bytes, obtenemos una trama de 532 bytes.

Luego, el overhead del paquete es igual a

overhead = (Longitud de preámbulo + interframe) / Longitud del paquete =

20 Bytes/532 bytes = 0,0375 = 3,75 %

1. Usando GNS3 (el profesor la enviará un proyecto GNS3 llamado frame ethernet)
   1. Abra el proyecto de una pequeña red compuesta de dos pc’s (use VPCS, que viene por default) y conecte esas dos pc’s a el Switch Ethernet que viene por defecto, la pc1 la conecta al puerto 5 y a la pc 2 la conecta al puerto 6.
   2. Encienda la red.
   3. Active el monitoreo en el enlace entre la pc 1 y el switch (Wireshark).
   4. Configure con la consola de la pc 1 la dirección ip con este comando: “ip 192.168.1.1/24” y presione Enter.
   5. Configure con la consola de la pc 2 la dirección ip con este comando: “ip 192.168.1.2/24” y presione Enter.
   6. Vaya a la consola de la pc1 y ejecute el comando “ping 192.168.1.2”.
   7. Abra el Wireshark y tendrá los siguientes paquetes capturados



Cuál es la longitud del frame: 64 Bytes

Cuál es la longitud capturada: 64 Bytes

La longitud mínima del Frame era para redes: Ethernet y Fast Ethernet Qué tipo de Frame es: Ethernet II

Cual es la Destination Address y que significa: es FF:FF:FF:F:F:F y significa que es un paquete de broadcast dirigido a todas los dispositivos conectados al switch

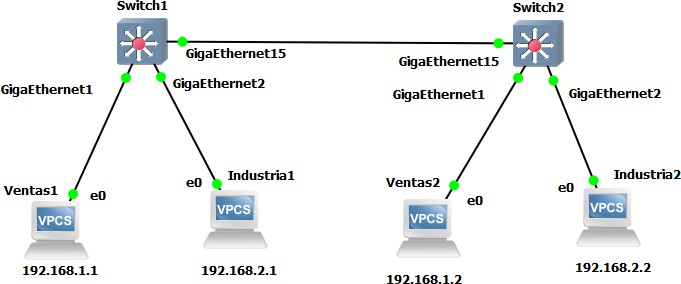
Cual es la Source Address y qué significa: 00:50:79:66:68:00, es la dirección MAC de la pc 1

El campo Longitud /Tipo que rol juega y que significa su valor: el campo se un campo Tipo, dado que el Frame es Ethernet II, y tiene un valor igual 0 x 0806, lo que significa que el campo de datos tiene encapsulado un protocolo ARP

Cuál es la MAC Address del computador destina y qué tipo de MAC es: la MAC Address del computador destino es 00:50:79:66:68:01, es una dirección MAC Unicast

1. Usando GNS3 (el profesor le enviará un proyecto que se llama “lan vlan práctica 8” y una imagen de un switch L2, que se llama vIOS.vmdk)
   1. Abra el GNS3 e instale la imagen en la opción “Edit”, “Preferences”, QEMU VM, añadiendo el archivo vIOS.vmdk (en la pestaña General Settings, en la opción Category, elija Switch y en RAM configure 512 Mb, en la pestaña “Network”, configure “adapters” = 16)
   2. Si usa Windows 10 y tuviera problemas para abrir el proyecto, desactive el firewall de la red interna o privada

Abra el proyecto que le envía la cátedra (lan vlan): el escenario es el siguiente:



A configurar la vlan “ventas” (vlan 100) y la vlan “industria” (vlan 200) en ambos switches. El enlace trunk va a transportar las VLAN 100 y VLAN 200 para poder comunicar las pc’s “ventas 1” con “ventas 2”, y las pc’s “industria 1” con “Industria 2”

# SWITCH 1

Creación de las VLAN en el Switch 1:

Abrir una consola sobre el SW1

vIOS-L2-01> enable (ingresa el modo administración)

vIOS-L2-01#vlan database (ingresa al modo de administración de VLAN) vIOS-L2-01(vlan)#vlan 10 name prof

vIOS-L2-01(vlan)#vlan 20 name alum vIOS-L2-01(vlan)#exit

vIOS-L2-01#show vlan brief (muestra las vlan’s configuradas) Configura los puertos de acceso a cada VLAN en el switch 1:

vIOS-L2-01# config terminal (ingresa al modo configuración)

vIOS-L2-01(config)#interface GigabitEhternet 0/1 (ingresamos al modo configuración específica)

vIOS-L2-01(config-if)#switchport access vlan 100 (configura el puerto de “Ventas 1”)

vIOS-L2-01(config)#interface GigabitEthernet 0/2 (ingresamos al modo configuración específica)

vIOS-L2-01(config-if)#switchport access vlan 200 (configura el puerto para “Industria 1”

Configura el dominio de VLAN (en el switch 1 porque el switch 1 es el Server)

vIOS-L2-01(config-if)#exit (salimos del modo configuración configuración específica y volvemos al modo configuración)

vIOS-L2-01 (config)#vtp mode server (configuramos el server del modo VLAN) vIOS-L2-01 (config)#vtp domain local (configuramos el dominio del modo VLAN) Configura el enlace Trunk en el puerto 15 (en el switch 1)

vIOS-L2-01 (config)#interface GigabitEthernet 3/3 vIOS-L2-01 (config-if)#switchport mode trunk

vIOS-L2-01 (config-if)#switchport trunk allowed vlan 1-1005

# SWITCH 2

Configura al Switch 2 con el modo cliente en el dominio de VLAN vIOS-L2-02 (config)#vtp mode client

vIOS-L2-02 (config)#vtp domain local Configura el puerto trunk

vIOS-L2-02 (config)#interface GigabitEthernet 3/3 vIOS-L2-02 (config-if)#switchport mode trunk

vIOS-L2-02 (config-if)#switchport trunk allowed vlan 1-1005

Configura puertos de Acceso

vIOS-L2-02 (config)#interface GigabitEthernet 0/1 vIOS-L2-02 (config-if)#switchport access vlan 100 vIOS-L2-02 (config)#interface GigabitEthernet 0/2 vIOS-L2-02 (config-if)#switchport access vlan 200

PARA VER LA CONFIGURACIÓN EJECUTAR EN AMBOS SWITCHES LOS SIGUIENTES COMANDO (EN MODO ADMINISTRACIÓN)

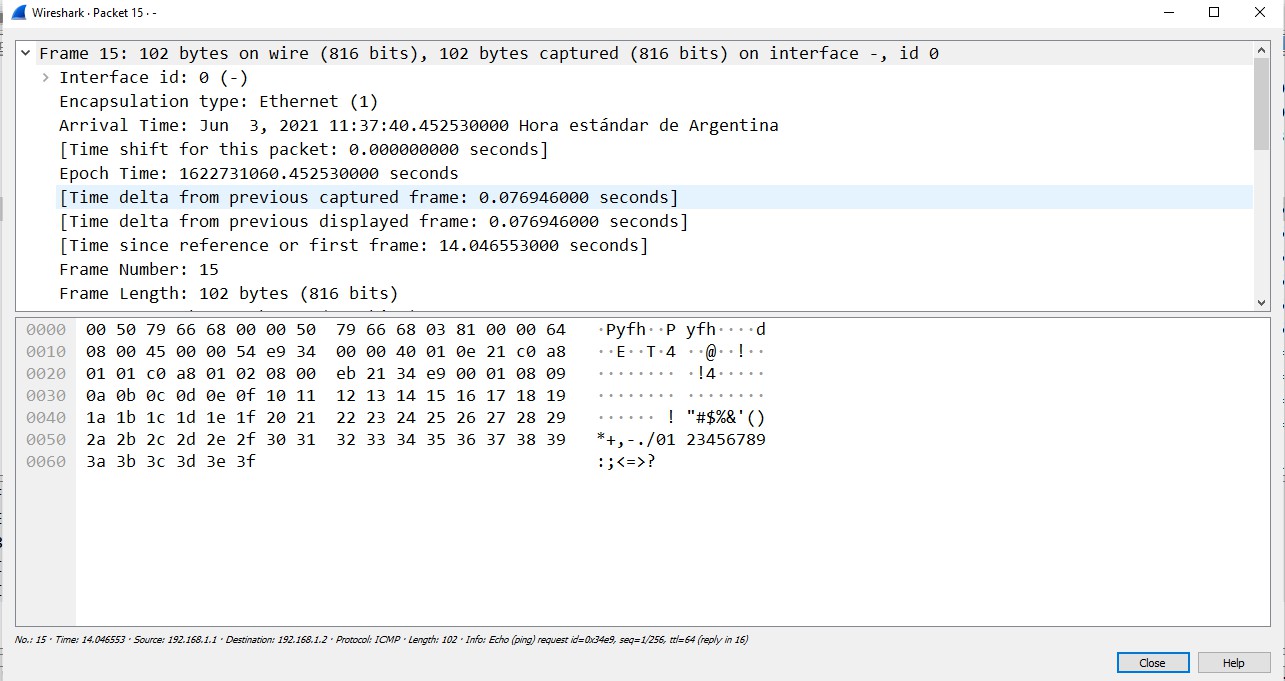
vIOS-L2-02 # show vlan brief (muestra las vlan’s)

vIOS-L2-02 # show interface trunk (muestra los enlaces trunk)

vIOS-L2-01 # show vlan brief (muestra las vlan’s)

vIOS-L2-01 # show interface trunk (muestra los enlaces trunk)

* 1. Inicie la captura con Wireshark sobre el enlace trunk
  2. Haga un ping desde la pc ventas 1 a las pc ventas 2
  3. Responda las siguientes preguntas, en base a los paquetes capturados, se muestra el ejemplo de un Frame capturado:



* 1. Abra el primer Frame del comando ping . ¿Cuál es la longitud del Frame?:
  2. ¿Qué protocolos están encapsulados en el Frame?:
  3. ¿Tipo de Frame? :
  4. ¿Cómo sabe el switch que es un Frame de 802.1Q?
  5. Describa los valores que observa a nivel 802.1q