Redes Virtuales (VLAN)

Capa 2

LOVE PURPLE
LIVE GOLD

WALC 2013
Managua, Nicaragua
14 al 18 de octubre
Organización General:
16°
Taller sobre
Tecnologías de Redes Internet
para América Latina y el Caribe
Fundación
EsLaRed

INTRODUCCION

Virtual LANs (VLANs)

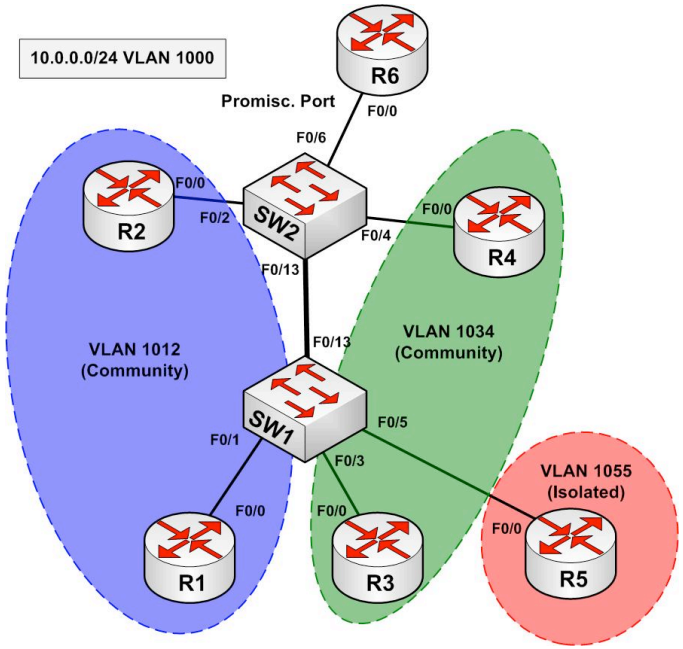
- Nos permiten separar los switches en varios switches virtuales.
- Sólo los miembros de una VLAN pueden ver el tráfico de dicha VLAN.
  - Tráfico entre VLANs debe pasar por un enrutador.

NSRC
Network Startup Resource Center

LOVE PURPLE
LIVE GOLD

Virtual LANs (VLANs)

- Nos permiten utilizar una sola interfaz de enrutador para llevar tráfico de varias subredes.
  - Ejemplo: Sub-interfaces en Cisco

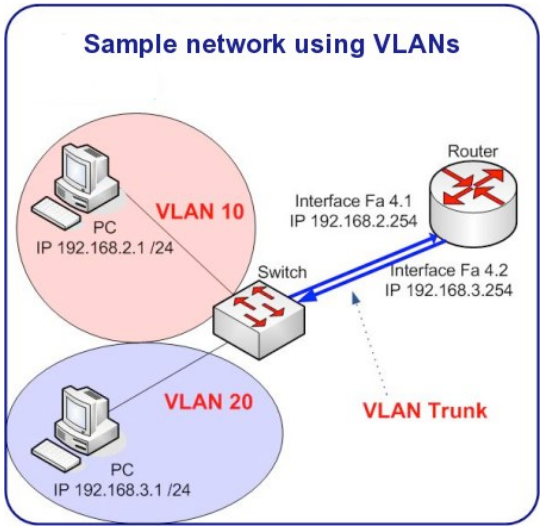


NSRC
Network Startup Resource Center

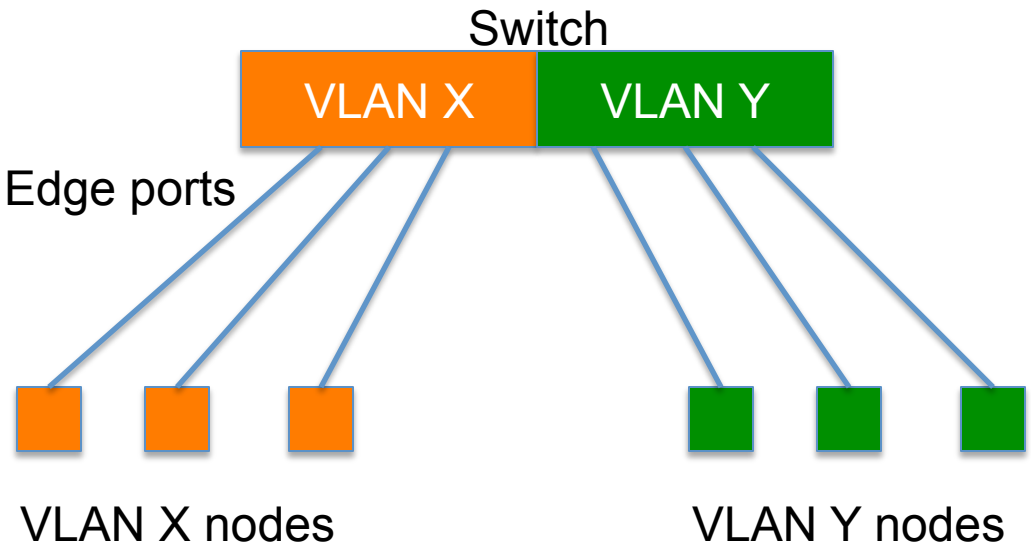
Love Purple
Live Gold

VLANs Locales

- Dos o más VLANs dentro de un mismo switch.
- ***Los Puertos de usuario (Edge)***, donde las máquinas se conectan, se configuran como miembros de la VLAN.
- El switch se comporta como varios switches separados, enviando tráfico solamente entre miembros de la misma VLAN.



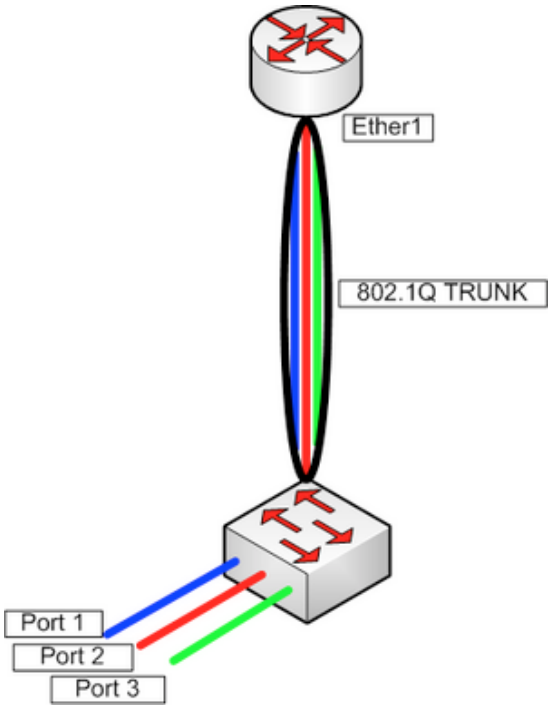
VLANs Locales



VLAN TRUNKS

VLANs Entre Switches

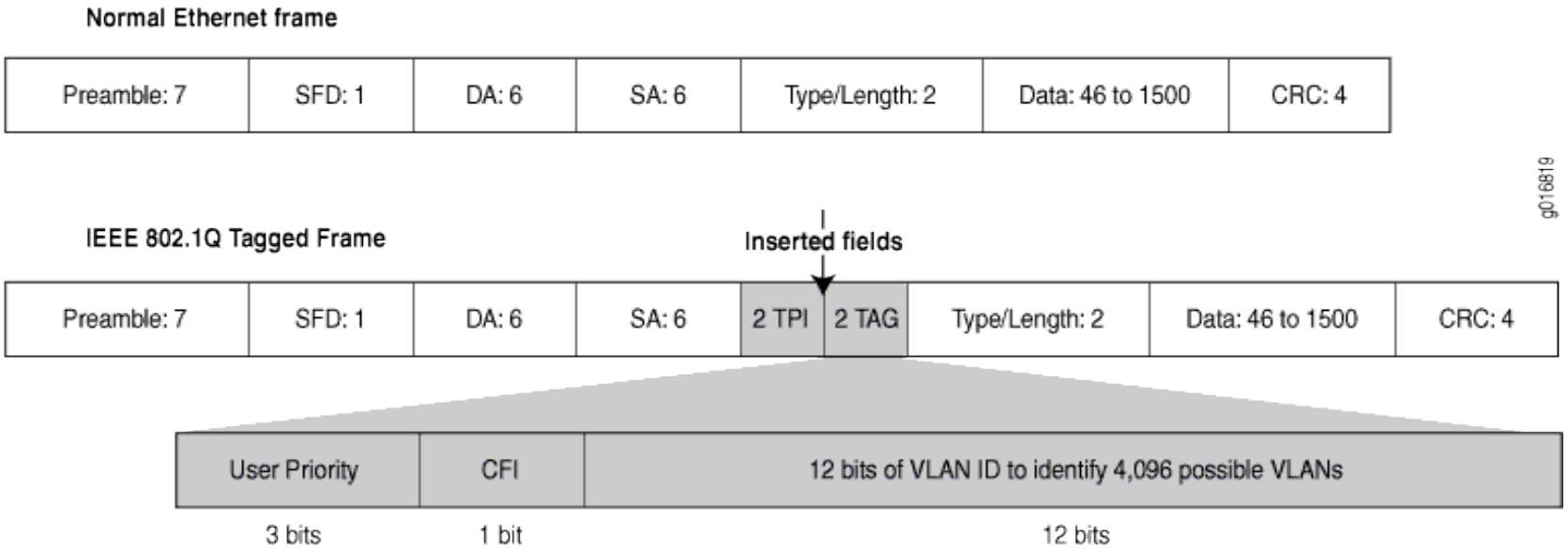
- Dos o más switches pueden intercambiar tráfico de una o más VLANs
- Los enlaces inter-switch se configuran como ***troncales (trunks)***, transportando tramas de todas o una parte de las VLANs de un switch
- Cada trama lleva una **etiqueta** (***tag)*** que identifica la VLAN a la que pertenece



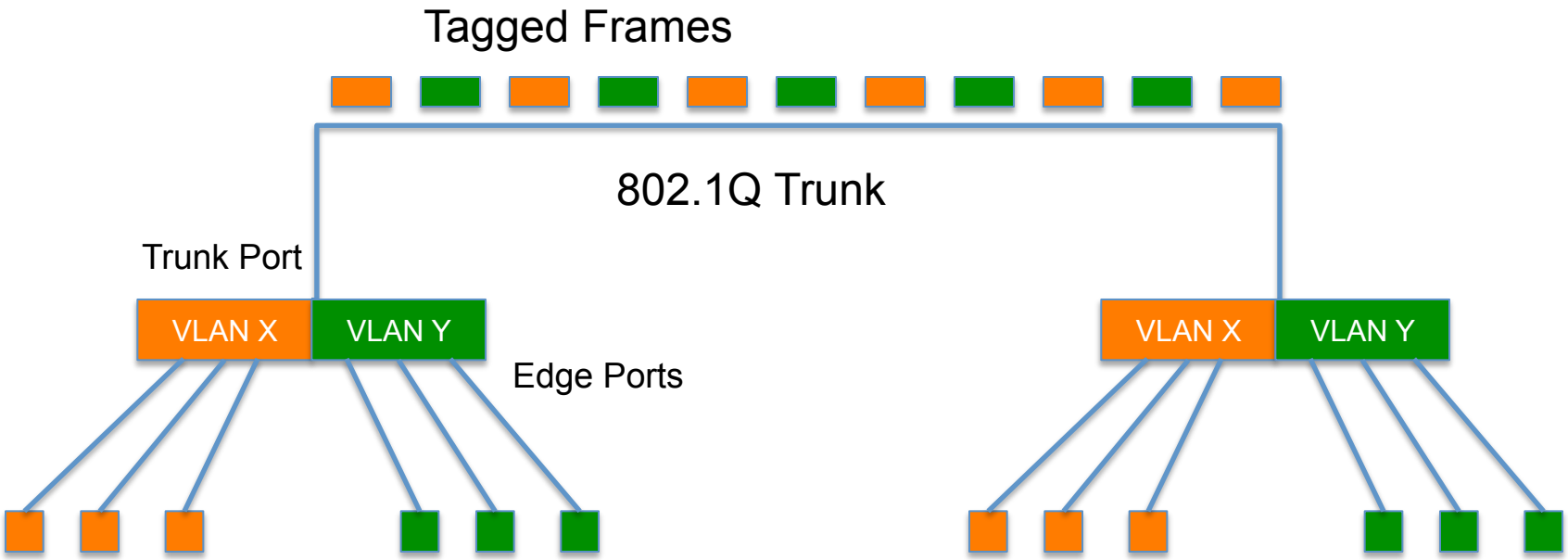
802.1Q

- El estándar de la IEEE que define cómo las tramas ethernet deberían ser etiquetadas ***tagged*** cuando viajan a través de troncales.
- Esto implica que switches de **diferentes vendedores** son capaces de intercambiar tráfico entre VLANs.

802.1Q tagged frame



VLANs Entre Switches



Esto se conoce como “VLAN Trunking”

Tagged vs. Untagged

- Los puertos de usuarios no se etiquetan, sólo se hacen “miembros” de una VLAN.
- Sólo es necesario etiquetar tramas en puertos entre switches (*trunks*), cuando éstos transportan tráfico de múltiples VLANs.
- Un *trunk* puede transportar tráfico de VLANs *tagged* y *untagged.*
  - Siempre que los dos switches estén de acuerdo en cómo manejar éstas.

Los VLANs y Complejidad

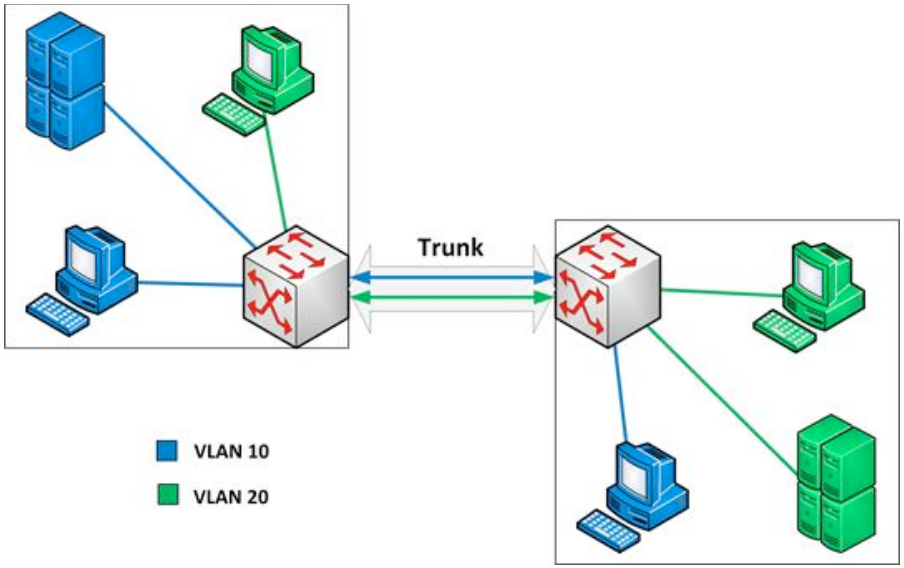
- Ya no se puede simplemente “reemplazar” un switch.
  - Ahora hay una configuración de VLANs que mantener.
  - Los técnicos de campo necesitan más formación.
- Hay que asegurarse de que todos los enlaces troncales están transportando las VLANs necesarias.
  - Recordar cuando se esté agregando o quitando VLANs.

Buenos Usos de VLANs

- Hay que segmentar la red en varias subredes, pero no hay suficientes switches.
- Separar los elementos de infraestructura como teléfonos IP, controles automáticos, etc.
- Separar el plano de control:
  - Sugerencia: Restringir quiénes puden acceder a la dirección de gestión del switch.

Malos Usos de VLANs

- Porque es posible, y le hace sentir “cool” ☺
- Porque le darán seguridad absoluta para sus usuarios (o así parece).
- Porque le permiten extender la red IP hasta otros edificios remotos.
  - De hecho esto es muy común, pero es muy mala idea.



No Hacer un “VLAN spaghetti”

- Extender una VLAN a través de múltiples edificios o todo el campus.
- Mala idea porque:
  - El tráfico broadcast viaja a través de todas las troncales, de un extremo al otro de la red.
  - Una tormenta de broadcast se propagará a través de toda la extensión de la VLAN, y afectará las otras VLANS!
  - Una pesadilla para el mantenimiento y la resolución de problemas

PORT AGGREGATION

Agregación de Enlaces

- Conocido como *port bundling, link bundling.*
- Se pueden usar varios enlaces en paralelo como si fueran un enlace único virtual.
  - Para mayor capacidad del canal.
  - Para redundancia (tolerancia a fallos).

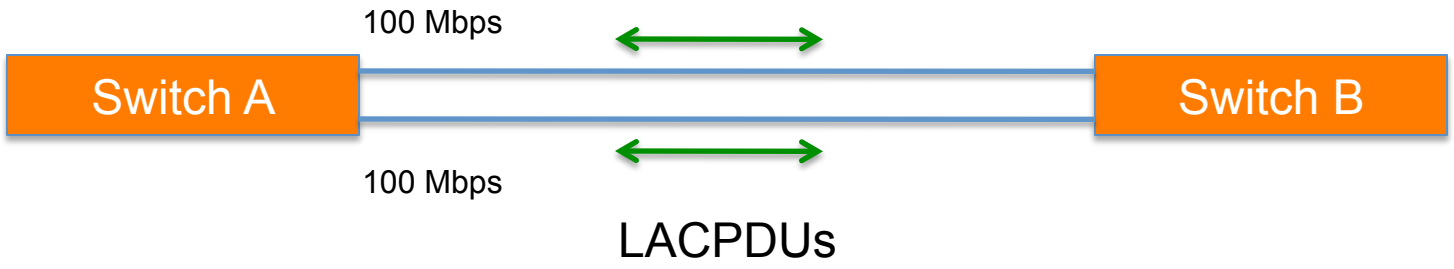
- LACP (Link Aggregation Control Protocol) es un método estándar para negociar estos enlaces agregados entre switches.

Operación de LACP

- Dos switches conectados via múltiples enlaces enviarán paquetes LACPDU, identificándose a sí mismos y a los puertos que los enlazan.
- Entonces construirán los enlaces agregados y empezarán a pasar tráfico por ellos.
- Los puertos se pueden configurar como pasivos o activos.

Protocol	Mode	Description
None	On	Forces the port to channel mode without negotiation.
PAgP	**Auto**	Port will passively negotiate to become an EtherChannel. Port will NOT initiate negotiations.
	Desirable	Port will passively negotiate to become an EtherChannel. Port will initiate negotiations.
LACP	**Passive**	Port will passively negotiate to become an EtherChannel. Port will NOT initiate negotiations.
	Active	Port will passively negotiate to become an EtherChannel. Port will initiate negotiations.

Operación de LACP

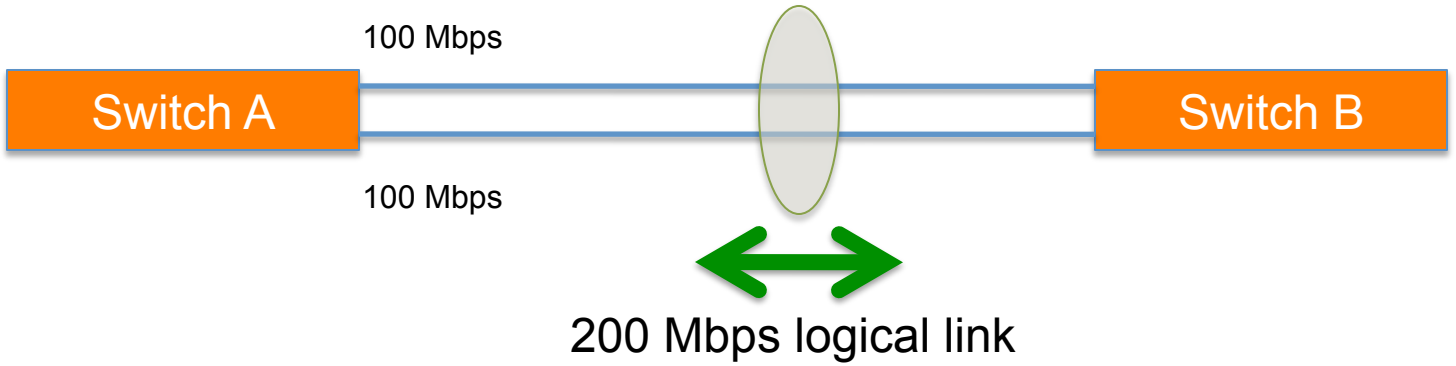


- Los switches A y B se conectan entre sí mediante dos pares de puertos Fast Ethernet.

- LACP se habilita y los puertos se activan.

- Los switches empiezan a enviar LACPDUs y negocian cómo establecer en enlace virtual.

Operación de LACP



- El resultado es un enlace virtual agregado de 200 Mbps.

- El enlace es también tolerante a fallos: Si uno de los enlaces miembro falla, LACP automáticamente quitará a ese enlace del grupo y seguirá enviando tráfico a través del enlace disponible.

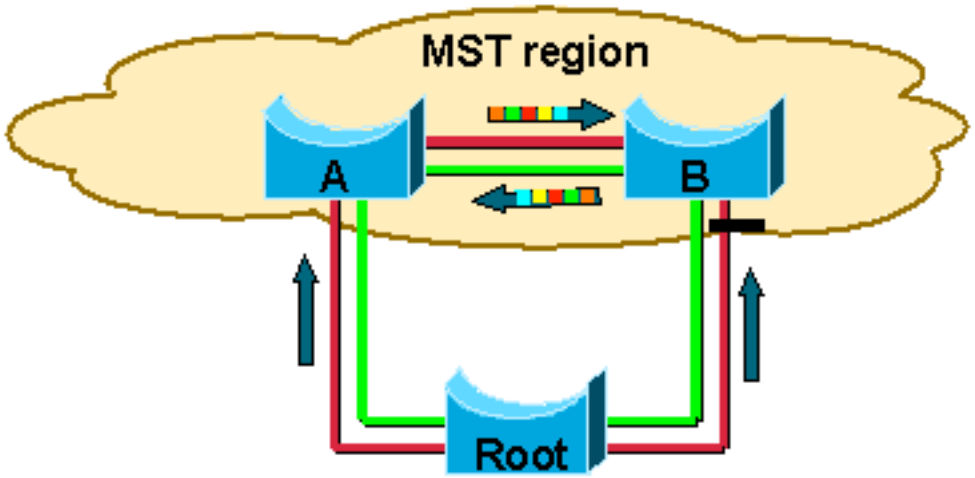
Distribución del tráfico (LACP)

- Los enlaces agregados distribuyen las tramas gracias a un algoritmo, basado en:
  - Dirección MAC origen y/o destino.
  - Dirección IP origen y/o destino.
  - Números de puerto origen y/o destino.
- Dependiendo de la naturaleza del tráfico, esto puede resultar en tráfico desbalanceado.
- Siempre elija el método de balanceo de carga que provea la distribución máxima.

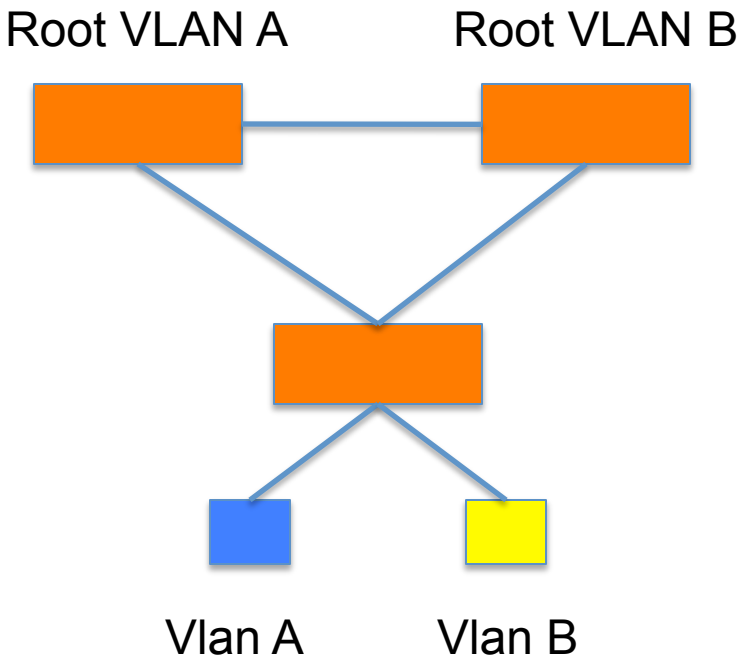
SPANNING TREE

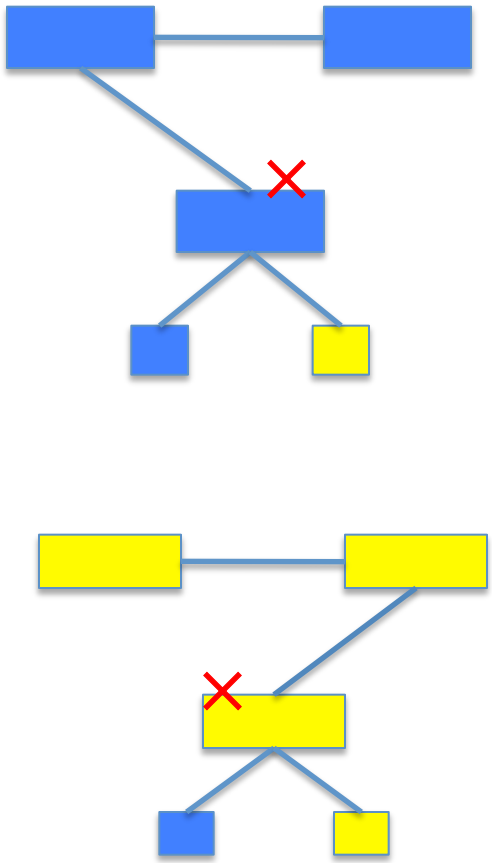
Multiple Spanning Tree (802.1s)

- Permite crear “instancias” de Spanning Tree por cada grupo de VLANs.
  - Las múltiples topologías permiten el balanceo de carga a través de diferentes enlaces.
- Compatible con STP y RSTP.



Multiple Spanning Tree (802.1s)



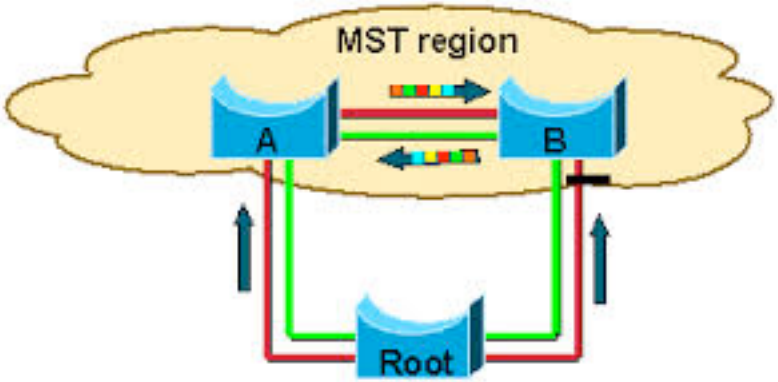


Multiple Spanning Tree (802.1s)

- Región MST:
  - Los switches son miembros de una misma región si coinciden en sus parámetros:
    - Nombre de configuración MST.
    - Número de revisión de la configuración MST.
    - Mapeo de VLANs a instancias.
  - Un resumen hash de estos atributos se envía dentro de las BPDUs para su rápido análisis en los switches.
  - Una región es generalmente suficiente.

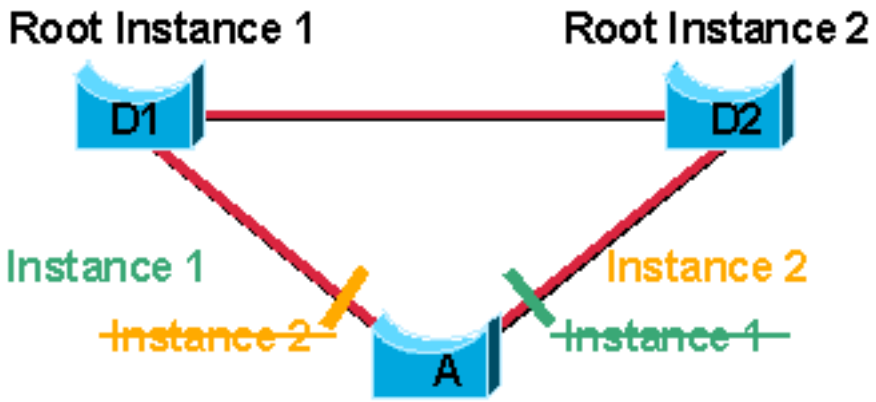
Multiple Spanning Tree (802.1s)

- IST = Internal Spanning Tree.
  - Interno a la región.
  - Presenta toda la región como un switch virtual único al CST externo.



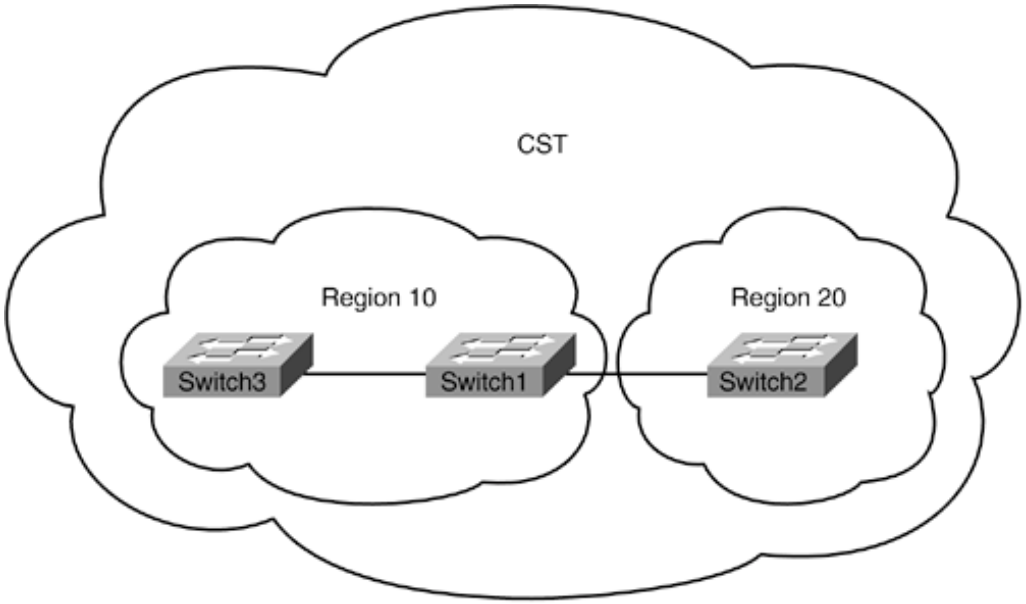
Multiple Spanning Tree (802.1s)

- Instancias MST:
  - Grupos de VLANs se mapean a distintas instancias de MST.
  - Estas instancias representarán cada topología alternativa, o caminos de reenvío alternativos.
  - Se especifica un switch raíz y uno alternativo para cada instancia.

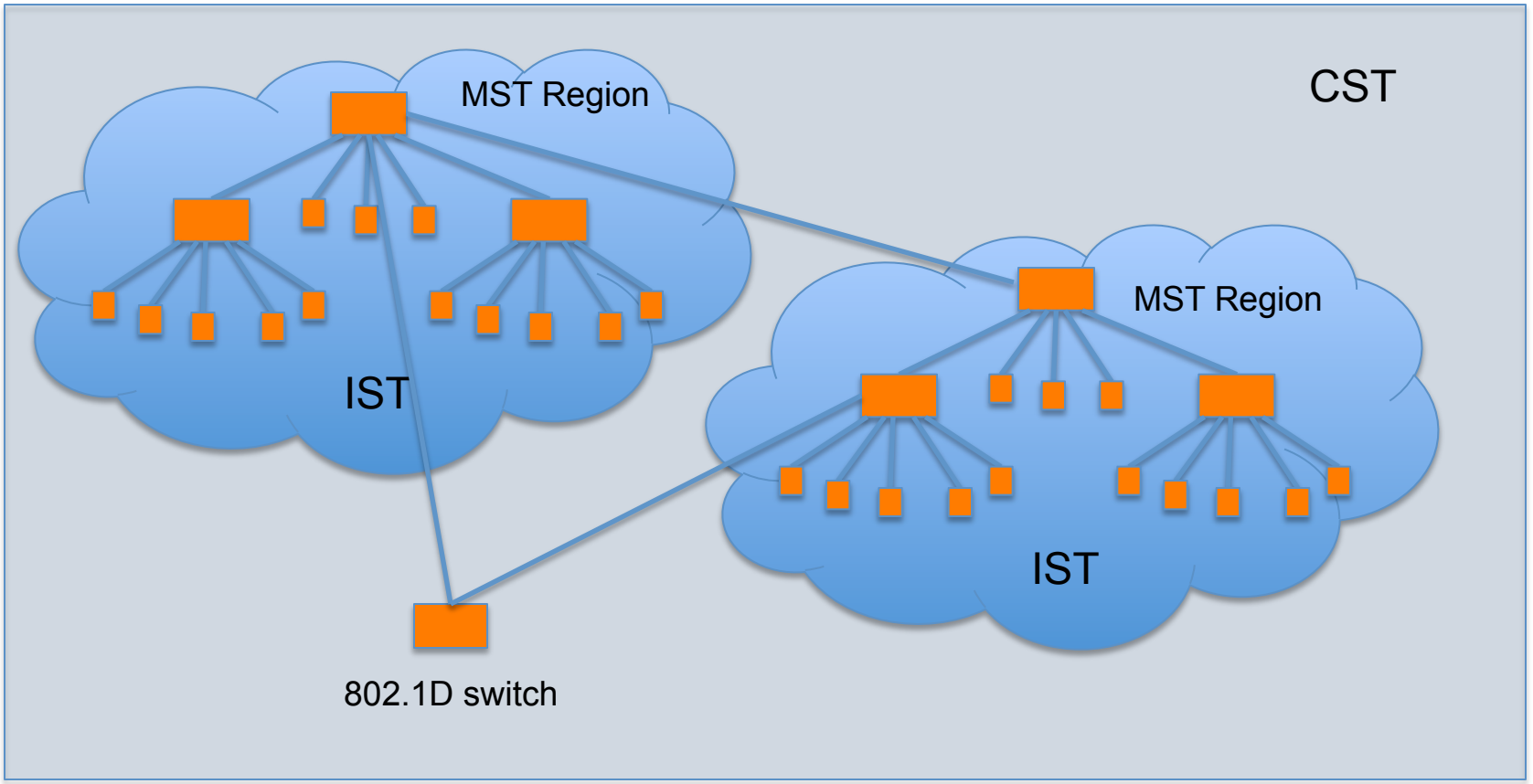


Multiple Spanning Tree (802.1s)

- CST = Common Spanning Tree
  - Para interoperar con otras versiones de Spanning Tree, MST necesita un spanning tree común que contenga todas las demás “islas”, incluyendo otras regiones MST.



Multiple Spanning Tree (802.1s)



Multiple Spanning Tree (802.1s)

- Pautas de diseño”
  - Determinar los caminos de reenvío relevantes y distribuir las VLANs de manera equitativa entre las instancias correspondientes a cada uno de estos caminos.
  - Designar los switches raíz y alternativo para cada instancia.
  - Asegurarse de que todos los switches concuerdan en sus parámetros.
  - No asignar VLANs a la instancia 0, ya que ésta es utilizada por el IST.

QUE BUSCAR EN UN SWITCH

NSRC
Network Startup Resource Center

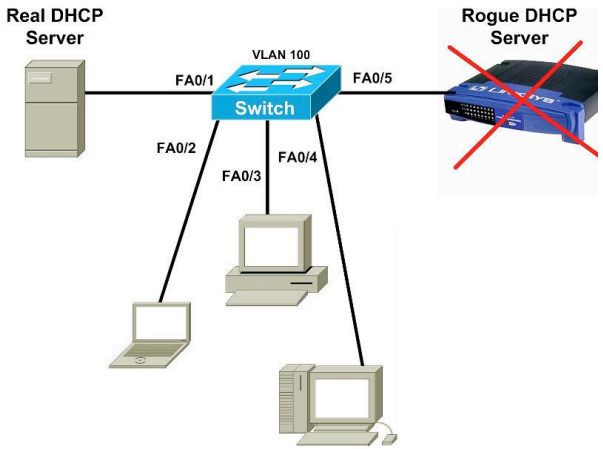
Love Purple
LIVE GOLD

Elección de Switches

- Funcionalidades mínimas:
  - Conformidad con los estándares
  - Gestión cifrada (SSH/HTTPS)
  - VLAN trunking
  - Spanning Tree (por lo menos RSTP)
  - SNMP
    - Por lo menos versión 2 (v3 tiene mejor seguridad)
    - Traps

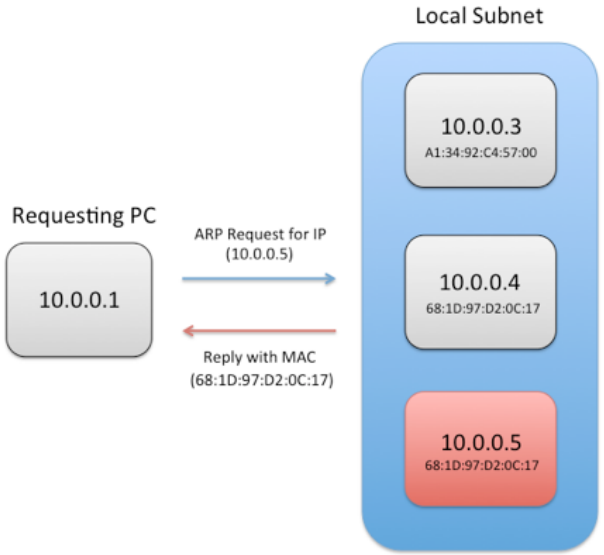
Elección de Switches

- Otras funcionalidades recomendadas:
  - DHCP Snooping
    - Evitar que sus usuarios activen un servidor DHCP ilegítimo
      - Ocurre mucho con los enrutadores wireless de bajo coste (Netgear, Linksys, etc) enchufados al revés.
    - Los puertos que suben hasta el servidor DHCP legítimo se designan como “trusted”. Si hay DHCPOFFERs originadas desde puertos no confiados, son descartadas.



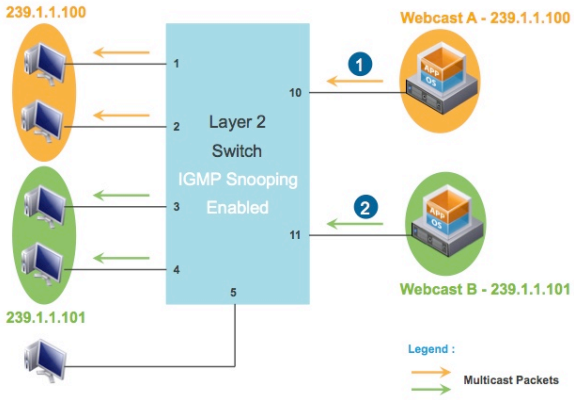
Elección de Switches

- Otras funcionalidades recomendadas:
  - Inspección de ARP dinámica
    - Un nodo malicioso puede realizar un ataque “man-in-the-middle” al enviar respuestas ARP ilegítimas
    - Los switches pueden mirar dentro de los paquetes ARP y descartar los que no sean legítimos.



Selección de Switches

- Otras funcionalidades recomendadas:
  - IGMP Snooping:
    - Los switches por defecto reenvían las tramas multicast a través de todos sus puertos.
    - Al “husmear” el tráfico IGMP, el switch puede aprender cuáles máquinas son miembros de un grupo multicast, y enviar las tramas a través de los puertos necesarios solamente.
    - Muy importante cuando los usuarios utilizan Norton Ghost, por ejemplo.

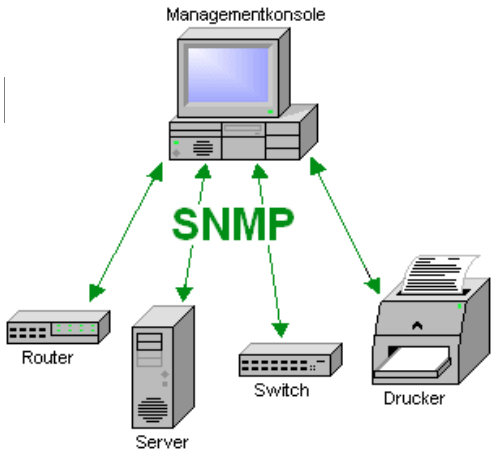


NSRC
Network Startup Resource Center

Love Purple
Live Gold

Gestión de Red

- Habilite los SNMP traps y/o Syslog:
  - Reunir y procesar en un servidor central
    - Cambios de Spanning Tree.
    - Discordancias de Duplex.
    - Problemas de cableado.
- Monitorizar las configuraciones
  - Usar RANCID para reportar todos los cambios que ocurran en la configuración del switch.

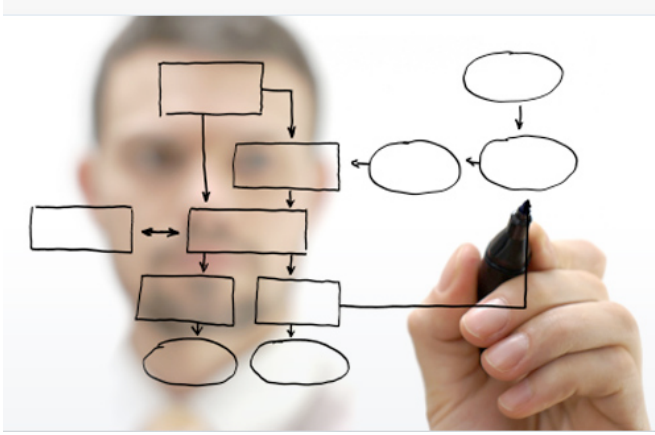


Gestión de Red

- Reuna y guarde las tablas de reenvío usando SNMP periódicamente.
  - Esto permite encontrar las direcciones MAC en su red de forma rápida.
  - Puede usar archivos de texto simple y buscar con ‘grep’, o usar una herramienta con interfaz web y una base de datos.
- Active LLDP (o CDP o similar):
  - Le muestra cómo los switches están interconectados entres sí, y a otros dispositivos.

Documentación

- Documente la ubicación de sus switches.
  - Nombre el switch basado en su ubicación:
    - E.g. edificio1-sw1
  - Mantenga un récord de la ubicación física:
    - Nivel, número de clóset, etc.
- Documente las conexiones a las tomas de red:
  - Número de salón, número de toma, nombre del servidor, printer, etc.



¡Gracias!

Jeffry Handal

jhandal@lsu.edu

NSRC
Network Startup Resource Center

Love Purple
Live Gold