Fase 4 – Activitat 6.2: Enllaços troncals

0- Identificació del grup i activitat:

Curs: ASIX2
Projecte: PJ7 Disseny i simulació de LANs
Fase: 4
Activitat: 6.2
Grup/Individual: Individual

1.- Objectiu de l'activitat

a) Configuració de VLANs
b) Configuració de ports troncals
c) Configuració de VLANs nadiues
d) Estudi del protocol IEEE802.1q
e) Filtres de VLANS.

2.- Conceptes sobre ports troncals, etiquetatge de trames i tipus de VLANs

2.1.- Definició bàsica de VLAN

- Una VLAN (Virtual Local Area Network) permet segmentar una xarxa física en diferents xarxes lògiques independents.
- Això permet separar dispositius dins del mateix switch com si estiguessin en xarxes diferents.

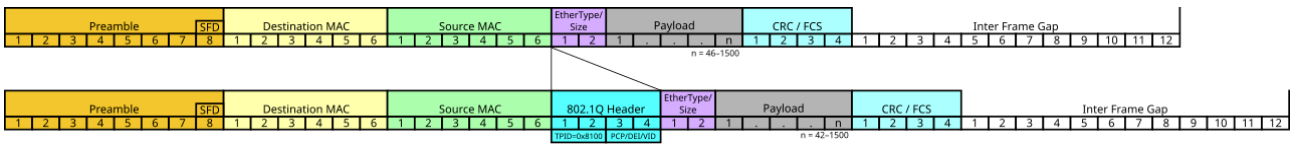
2.2.- Avantatges de les VLANs

- Millora de la seguretat separant el trànsit.
- Reducció del domini de broadcast.
- Millor organització de la xarxa.
- Facilitat d'administració.

2.3.- Norma IEEE 802.1Q

- La norma IEEE 802.1Q defineix el sistema d'etiquetatge de trames Ethernet per identificar a quina VLAN pertany cada paquet.
- Afegeix un camp de 4 bytes dins la trama Ethernet amb l'identificador de VLAN.
- Estructura d'una trama Ethernet amb IEEE 802.1Q:
    - MAC Destí (6 bytes)
    - MAC Origen (6 bytes)
    - TPID - Tag Protocol Identifier (2 bytes, valor 0x8100)
    - TCI - Tag Control Information (2 bytes) que inclou:
        - PCP (3 bits) Prioritat
        - DEI (1 bit)
        - VLAN ID (12 bits)
    - EtherType (2 bytes)
    - Dades (46–1500 bytes)
    - FCS (4 bytes)

La inserció del camp 802.1Q incrementa la mida de la trama en 4 bytes respecte a una trama Ethernet estàndard.



- Captures IEEE802.1q: https://wiki.wireshark.org/uploads/__moin_import__/attachments/SampleCaptures/vlan.cap.gz

2.4.- Tràfic etiquetat i no etiquetat

- El tràfic etiquetat (tagged) inclou una etiqueta VLAN dins la trama Ethernet.
- El tràfic no etiquetat (untagged) és una trama Ethernet normal sense cap camp VLAN.

2.5.- Equips que treballen amb tràfic etiquetat i que no utilitzen tràfic etiquetat

- Treballen amb tràfic etiquetat: switches gestionables, routers, firewalls i servidors amb VLAN configurades.
- No utilitzen etiquetes: ordinadors, impressores i dispositius finals connectats a ports tipus access.

2.6.- Port mode access
- Un port en mode access només pertany a una única VLAN.
- El tràfic surt i entra sense etiqueta cap al dispositiu final.

2.7.- Port mode trunk
- Un port en mode trunk pot transportar múltiples VLANs simultàniament.
- El trànsit circula etiquetat segons la norma 802.1Q.

2.8- VLAN de gestió
- La **VLAN de gestió** és una VLAN dedicada exclusivament per a la **gestió de dispositius de xarxa** (switches, routers, firewalls, APs).
- No hauria d'utilitzar-se per trànsit d'usuaris ni trànsit de dades ordinari pels següents motius:
    - Seguretat
    - Control i organització
    - Fiabilitat
- Bones pràctiques:
    - Crear una VLAN exclusiva, per exemple **VLAN 99** o **VLAN 200**.
    - No utilitzar la VLAN nadiua ni VLANs d'usuari per gestió.
    - Limitar l'accés a aquesta VLAN només des de subxarxes de gestió o VPN segures.
    - Configurar ports d'equip de gestió com a **access port** dins d'aquesta VLAN.
    - Utilitzar protocols segurs (SSH, SNMPv3, HTTPS) per accedir als equips.

2.9.- VLAN nadiua
- La VLAN nadiua és la VLAN que, en un enllaç trunk, envia i rep el trànsit sense etiqueta.
- Si un port troncal rep trànsit sense etiquetar, per defecte l'envia a la VLAN nadiu
- És important que coincideixi als dos extrems del trunk.

2.10.- VLAN per defecte
- La VLAN per defecte és habitualment la VLAN 1 en molts switches.
- Tots els ports solen estar assignats inicialment a aquesta VLAN.
- No es pot modificar

2.11.- VLAN nadiua per defecte
- En la majoria de switches (especialment Cisco), la VLAN nadiua per defecte és la VLAN 1.
- El trànsit de VLAN 1 viatja sense etiqueta per defecte.
- La VLAN nadiua per defecte es pot modificar.
- Problemes de seguretat si no es modifica:
    - VLAN Hopping (Double Tagging) → Permet a un atacant arribar a una VLAN a la qual no hauria de tenir accés.
    - Si VLAN 1 està activada i utilitzada pels usuaris pot permetre capturar el trànsit de gestió (STP, VTP,,,) i permet a més usuaris poder fer atacs.
- Solució als problemes de seguretat:
    - No utilitzar VLAN 1
    - Crear una VLAN dedicada (ex: 999) com a nadiua
    - No assignar ports d'usuari a la VLAN nadiua
    - Coincidència exacta de VLAN nadiua als dos costats del trunk
    - Altres mesures no estrictament relacionades amb la problemàtica de la VLAN nadiua per defecte:
        - Desactivar DTP si no és necessari. DTP permet al switch configurar automàticament el mode d'un port (troncal o access). Si aquesta configuració es fa de manera manual es millora la seguretat.
        - Deshabilitar ports no utilitzats

3- Activitat

1- Descarrega el fitxer amb captures **IEEE802.1q** i a continuació:
- Fes un filtre **ICMP**.
- Comprova dins del primer missatge ICMP el format de la trama Ethernet
- Troba si és una trama etiquetada o no ho és
- Indica dins de quina VLAN es troba la trama capturada

2- Realitza la següent activitat → Configuració d'enllaços troncals amb packet tracer