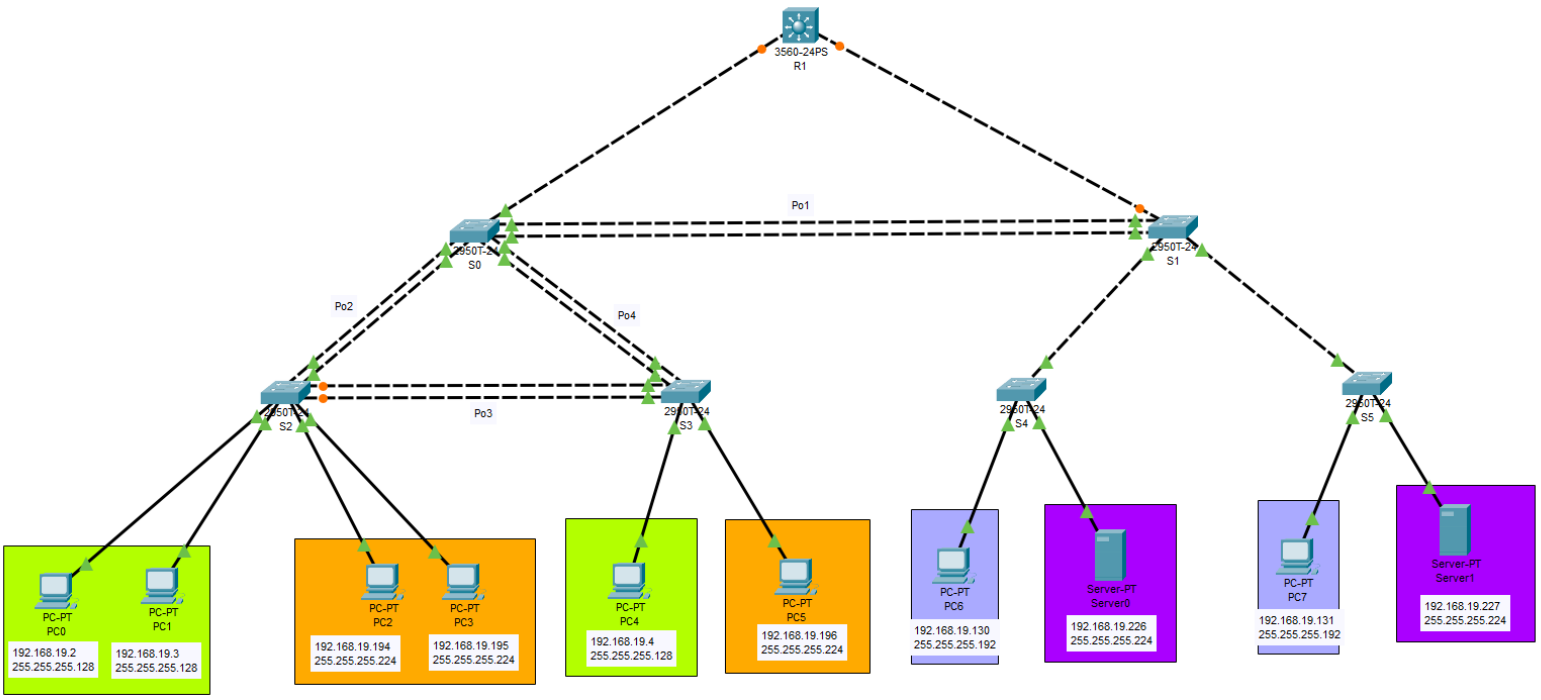
Practica 1

Nombre	Carnet
Santiago Gilberto Antonio Rivadeneira Ruano	201313722
Javier Oswaldo Miron Cifuentes	201602694
Edwin Alfredo Lopez Gomez	201314007

Grupo 18

19 de febrero 2022

TOPOLOGÍA

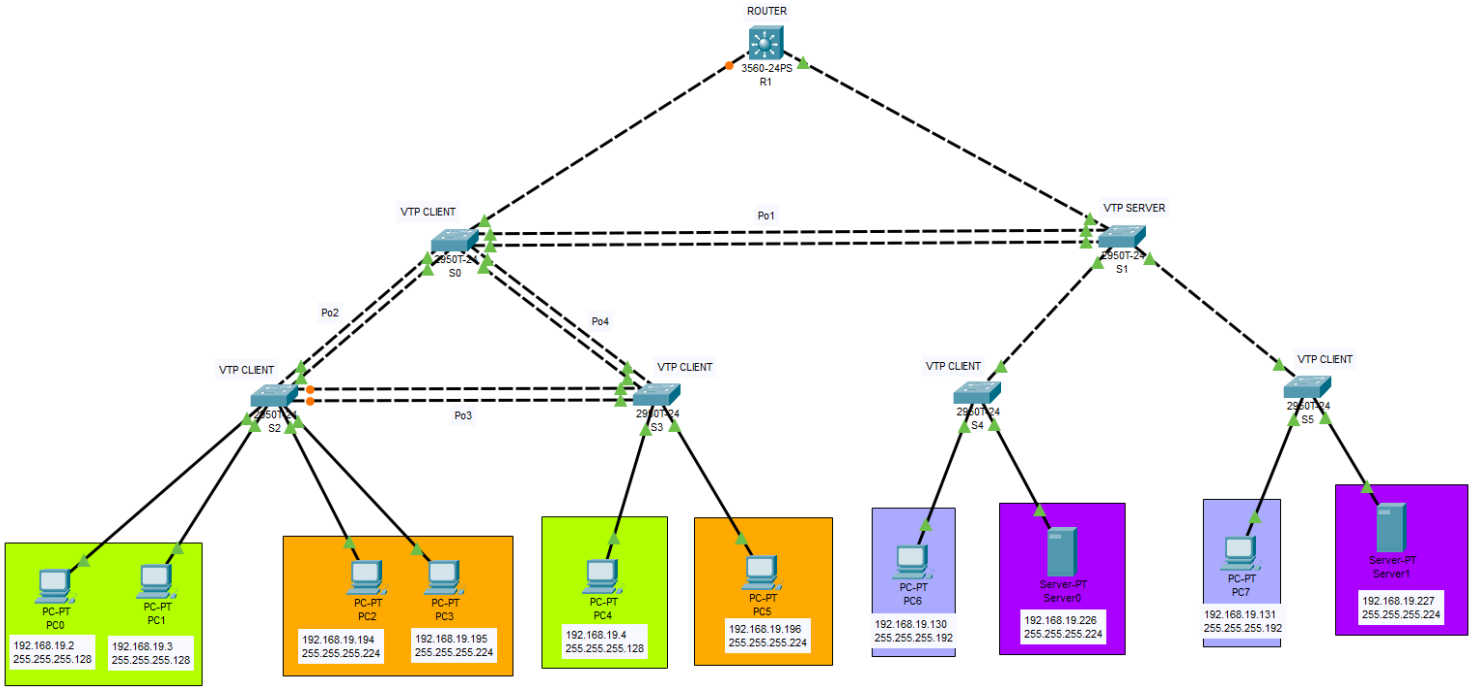

3560-24PS
R1
Po1
2950T-24
S0
2950T-24
S1
Po2
Po4
2950T-24
S2
Po3
2950T-24
S3
2950T-24
S4
2950T-24
S5
PC-PT
PC0
192.168.19.2
255.255.255.128
PC-PT
PC1
192.168.19.3
255.255.255.128
PC-PT
PC2
192.168.19.194
255.255.255.224
PC-PT
PC3
192.168.19.195
255.255.255.224
PC-PT
PC4
192.168.19.4
255.255.255.128
PC-PT
PC5
192.168.19.196
255.255.255.224
PC-PT
PC6
192.168.19.130
255.255.255.192
Server-PT
Server0
192.168.19.226
255.255.255.224
PC-PT
PC7
192.168.19.131
255.255.255.192
Server-PT
Server1
192.168.19.227
255.255.255.224

CONFIGURACIÓN VTP

Se definió el siguiente conjunto de VLANS con base a los departamentos solicitados:

NOMBRE VLAN	NÚMERO VLAN
Ventas	19
Distribución	29
Administración	39
Servidores	49
Management&Native	99
BlackHole	999

Topologia de VTP



Vtp domain: g18

Vtp password: g18

Vtp version: 2

Comandos de configuración VTP

- **VTP SERVER**

  $ S1(config)# vtp domain g18

  $ S1(config)# vtp password g18

  $ S1(config)# vtp version 2

  $ S1(config)# vtp mode server

- **VTP CLIENT**

  $ S0(config)# vtp domain g18

  $ S0(config)# vtp password g18

  $ S0(config)# vtp version 2

  $ S0(config)# vtp mode client

  La configuración de vtp client se aplicó para S0,S2,S3,S4,S5

Configuración VLAN Nativa

$ configure terminal

$ interface f#/#

switchport trunk native vlan ID

Configuración Ethernet Channel

- **LACP**

  $ configure terminal

  $ interface range f0/# - # ➔ rango

  $ channel-protocol lacp

  $ channel-group # mode active/passive

- **PAGP**

  $ configure terminal

  $ interface range f0/# - # ➔ rango

  $ channel-protocol pagp

  $ channel-group # mode desirable/auto

Configuración STP

$ configure terminal

$ spanning-tree mode pvst/rapid-pvst

Pruebas de convergencia

Escenario	Tipo Ethernet Channel	Protocolo Spanning-Tree	Tiempo de Convergencia
1	Ethernet Channel LACP	STP	00:00:37.90
2	Ethernet Channel LACP	RSTP	00:00:07.90
3	Ethernet Channel LACP	PVSTP	no disponible
4	Ethernet Channel PAgP	STP	00:01:11.95
5	Ethernet Channel PAgP	RSTP	00:00:14.73
6	Ethernet Channel PAgP	PVSTP	no disponible

Mediante la realización de pruebas experimentales de protocolos de redundancia se logró determinar que el protocolo más rápido en converger fue el Rapid Spanning Tree Protocol (RSTP), utilizando el protocolo de control de agregación de enlaces (LACP).

Subnetting

Por medio de un análisis de los departamentos, se logró determinar que la distribución de los departamentos es diferente, algunos requieren de una mayor cantidad de host que otros. Por lo que se distribuyeron los host asumiendo la capacidad de crecimiento de cada departamento.

Para realizar dicha distribución se utilizó una estrategia de diseño de subred denominada Variable Length Subnet Mask (VLSM). La cual nos permitió llevar a cabo una administración de subredes dependiendo la cantidad de host necesarios por subred.

Distribución de Host VLSM

A continuación se presenta la distribución de las vlan implementadas:

- Ventas: 126
- Administración: 62
- Distribución: 30
- Servidores: 30

Para el área de **ventas** se colocó la mayor cantidad de hosts, esto debido a que usualmente estas áreas tienen a tener una mayor demanda de hosts por la cantidad de empleados que se pueden necesitar. Para el área de **administración**, se colocaron 62, ya que el área administrativa puede ser lo suficientemente grande para cubrir con las necesidades de la empresa. Por último, a distribución y servidores se les coloca la misma cantidad de hosts, ya que usualmente este tipo de actividades no suelen ser demasiado demandantes en cuanto a capacidad de red.

Subred	Nº de Hosts	IP de red	Máscara	Primer Host	Último Host	Broadcast
Ventas	126	192.168.19.0 /25	255.255.255.128	192.168.19.1	192.168.19.126	192.168.19.127
Administracion	62	192.168.19.128 /26	255.255.255.192	192.168.19.129	192.168.19.190	192.168.19.191
Distribucion	30	192.168.19.192 /27	255.255.255.224	192.168.19.193	192.168.19.222	192.168.19.223
Servidores	30	192.168.19.224 /27	255.255.255.224	192.168.19.225	192.168.19.254	192.168.19.255

Intervlan

Se configuraron las interfaces VLAN utilizando los siguientes comandos:

$ R1(config)# Interface vlan X

$ R1(config)# ip address 192.168.18.X 255.255.255.X

$ R1(config)# description nombreVlan

$ R1(config)# exit

Esta configuración se aplicó para cada una de las diferentes VLAN de ventas, distribución, administración,servidores, management&native y blackhole.

Luego de crear las interfaces vlan es necesario crear las vlan en el switch de capa 3 para poder realizar comunicación y direccionamiento entre ellas.

$ R1(config)# vlan X

$ R1(config)# name “nombreVlan”

$ R1(config)# exit

DTP

Se desactivo el protocolo DTP de los puertos troncales, utilizando los siguientes comandos:

Para desactivar el protocolo en Interfaces:

$ SX(config)#interface fastethernet X/X

$ SX(config)#switchport nonegotiate

$ SX(config)#exit

Para desactivar el protocolo en Port-Channel:

$ SX(config)#interface port-channel X

$ SX(config)#switchport nonegotiate

$ SX(config)#exit

Esta configuración se realizó ya que los switch vienen por defecto con este protocolo activado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking en los enlaces Ethernet.

PORT-SECURITY

Se aplicaron las políticas de seguridad en las interfaces de los equipos de capa 2, a continuación se muestran los comandos utilizados:

Comandos de configuración para el área de ventas:

$ SX(config)#interface fastethernet X/X

$ SX(config-if)#switchport port-security

$ SX(config-if)#switchport port-security mac-address sticky

$ SX(config-if)#switchport port-security maximum 5

$ SX(config-if)#switchport port-security violation shutdown

Comandos de configuración para el área de distribución, administración y servidores:

$ SX(config)#interface fastethernet X/X

$ SX(config-if)#switchport port-security

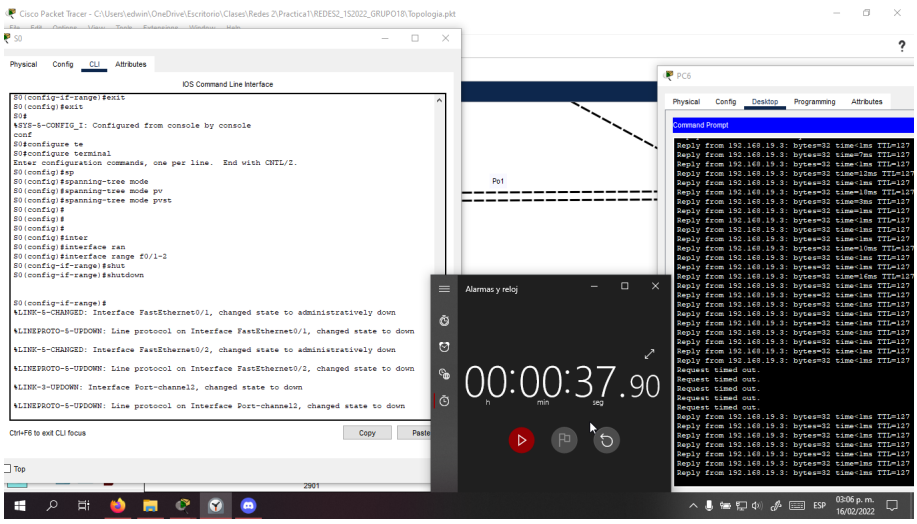
$ SX(config-if)#switchport port-security mac-address sticky

$ SX(config-if)#switchport port-security maximum 1

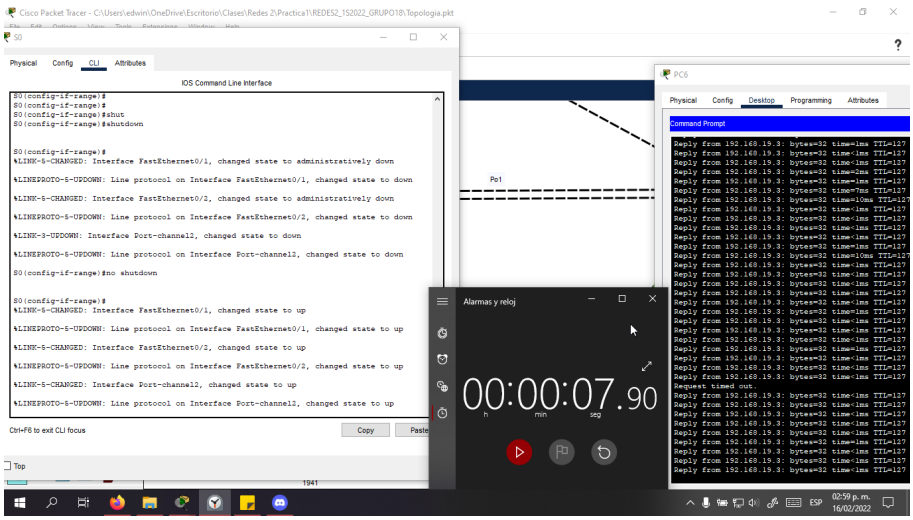
$ SX(config-if)#switchport port-security violation shutdown

ANEXOS

Escenario 1



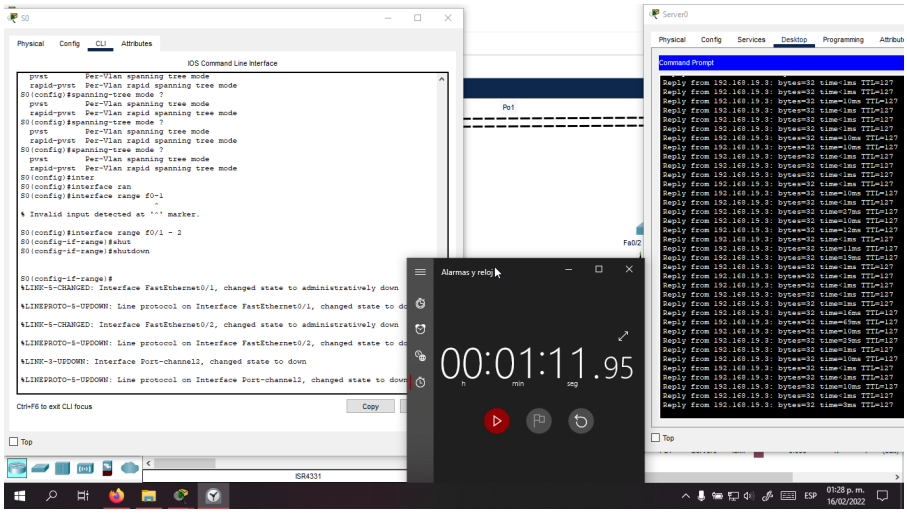
Escenario 2



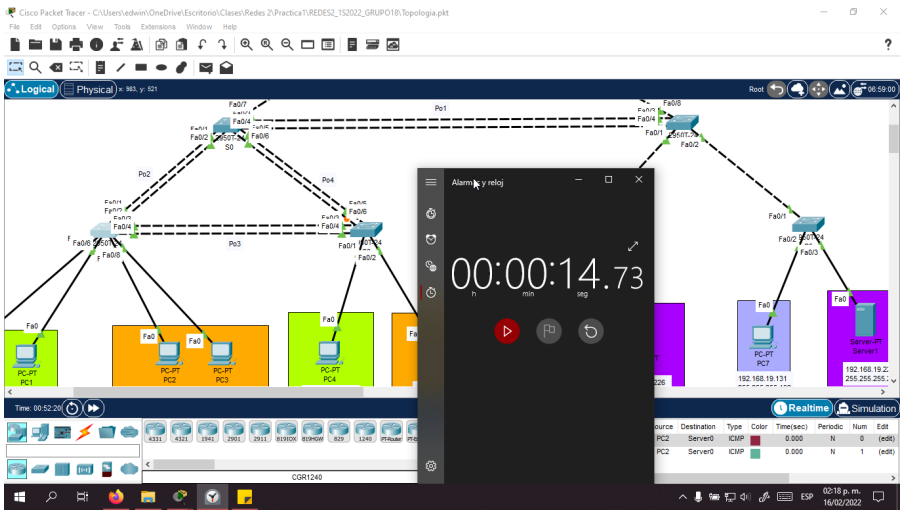
Escenario 3

No disponible

Escenario 4



Escenario 5



Escenario 6

no disponible