

**Universidad Nacional de La Matanza**

Departamento de Ingeniería e Investigaciones Tecnológicas

**Redes de Computadoras**

**TP Nº 5**

**LAN Switch y Ruteo de VLAN**

Profesor: Ing. Binker, Carlos

JTPs: Ing. Federiconi, Alejandro

Ing. Fernández, Diego

Ing. Vilarino, Martín

Alumnos: Andrade, Cristian Martín

Cuassolo, Facundo Gonzalo

Lorenz Vieta, Germán

González, Diego Andrés

**Switch LAN y VLANs**

**Objetivo y descripción general.**

Esta práctica pretende familiarizar al alumno con la configuración y gestión de una red local basada en switches LAN y redes locales virtuales (VLANs). Aunque los detalles concretos de cómo se realizan este tipo de tareas dependen del equipo utilizado, los aspectos básicos son similares en todos los fabricantes.

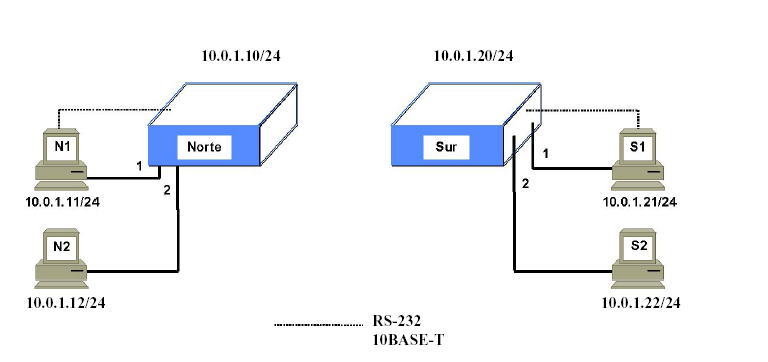
La práctica simula el establecimiento de una red local que abarca dos edificios, que denominamos Norte y Sur. En cada edificio se dispone de un switch, de un conjunto de ordenadores o hosts y de un router (utilizado en la segunda sesión).

***Por cada prueba que se realice se deberan realizar la captura de pantallas***

**PRIMERA SESIÓN.**

**Parte 1.1: Conectarse al switch por la interfaz de consola.**

En primer lugar procederemos a realizar las conexiones que aparecen en el esquema de la figura 1 (las direcciones IP que aparecen en la figura se configurarán más adelante). Los switch utilizados son los CISCO 1900.



**Figura 1: Interconexión de los equipos**

**Familiarizarse con la interfaz de comandos del switch**

Al abrir la interfaz de comandos, se muestra la pantalla de bienvenida que tiene el siguiente aspecto:

**Catalyst 1900 Management Console**

**Copyright (c) Cisco Systems, Inc. 1993-1998**

**All rights reserved.**

**Enterprise Edition Software**

**Ethernet Address: 00-50-F0-49-13-C0**

**PCA Number: 73-3124-01**

**PCA Serial Number: FAA03059JPK**

**Model Number: WS-C1924C-EN**

**System Serial Number: FAA0308J03U**

**Power Supply S/N: PHI024800YV**

**Power Supply P/N:**

**PCB Serial Number:**

**1 user(s) now active on Management Console.**

**User Interface Menu**

**[M] Menus**

**[K] Command Line**

**Enter Selection**: \_

En la pantalla de bienvenida tecelaremos una **‘K’** para elegir la interfaz de línea de comandos por ser más general, ya que la de menús es específica de los CISCO 1900, mientras que la de línea de comandos se puede utilizar, con algunas diferencias, en casi todos los equipos de la marca Cisco (switches, routers, etc.).

Al entrar en la interfaz de línea de comandos veremos aparecer el prompt **‘>’**, que indica acceso no privilegiado. Podemos hacer uso del comando **‘?’**, que nos muestra la lista de comandos que podemos utilizar en este entorno. Por ejemplo uno de esos comandos es **‘show’**; tecleando **‘show ?’** nos aparece una lista de los argumentos que admite el comando **show**. Ahora teclearemos el comando **‘show version’** que nos muestra una información resumida del switch: la versión de software que tiene, el tiempo que lleva encendido, etc.

#show version

Cisco Catalyst 1900/2820 Enterprise Edition Software

Version V9.00.04

Copyright (c) Cisco Systems, Inc. 1993-1999

1900Switch uptime is 1day(s) 22hour(s) 32minute(s) 44second(s)

cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory

Hardware board revision is 5

Upgrade Status: No upgrade currently in progress.

Config File Status: No configuration upload/download is in progress

15 Fixed Ethernet/IEEE 802.3 interface(s)

Base Ethernet Address: 00-30-80-C7-BE-C0

La interfaz de línea de comandos del switch dispone de varios entornos o modos, cada uno de ellos identificado por un prompt diferente. El prompt **‘>’** identifica el llamado modo Usuario, que es el modo no privilegiado. Mediante el comando **‘enable’** podemos pasar al modo Privilegiado, con lo que el prompt cambia a **‘#’**; dependiendo de la configuración que tenga el switch es posible que al pasar a modo Privilegiado nos pida una password de acceso.

En el modo Privilegiado se pueden usar todos los comandos del modo Usuario más otros solo accesibles en modo Privilegiado. Del modo Privilegiado podemos volver en cualquier momento al modo Usuario con el comando **‘exit’**. Del modo Privilegiado también podemos pasar a otro modo llamado Configuración Global mediante el comando ‘**configure**’ que se caracteriza por el

prompt ‘**(config)#**’. Como su nombre indica el modo Configuración Global permite hacer cambios globales en la configuración del equipo, para lo cual dispone de un conjunto de comandos completamente diferente al modo Privilegiado. Se puede volver del modo Configuración Global al modo Privilegiado mediante el comando **‘exit’**, o también pulsando **CTRL/Z.** El último modo que necesitamos conocer para realizar esta práctica es el modo Configuración de Interfaz que también dispone de un conjunto de comandos propio. Se llega a él desde el modo Configuración Global mediante el comando **‘interface int’** donde **‘int’** corresponde al nombre de alguna interfaz existente en el equipo (por ejemplo Ethernet0/1), como veremos más tarde. El modo Configuración de Interfaz se utiliza para configurar características de una interfaz específica del equipo y se identifica por el prompt **‘(config-if)#’.** Se puede volver de este al modo Configuración Global mediante el comando **‘exit’**.

Esquemáticamente la conmutación de modos se desarrolla según la siguiente secuencia:

**enable**. **configure**. **interface *int***.

Usuario <-----------> Privilegiado <--------------------> Configuración <-----------------------> Configuración

.**exit** . **exit** o **CTRL/Z** Global .**exit** de Interfaz

Algunas características interesantes del intérprete de línea de comandos, aplicables a todos los modos, son las siguientes:

. • En cualquier modo se puede utilizar el comando ‘?’ para solicitar ayuda sobre los comandos

permitidos.

. • La tecla **CTRL/P** (o flecha hacia arriba . ) recupera el último comando tecleado.

. • Todos los comandos admiten abreviaturas siempre y cuando no haya ambigüedad en su

significado. Si se escribe un comando o argumento incompleto y se pulsa la tecla tabulador el sistema termina de escribir el comando o argumento que corresponde. Esto permite al usuario asegurarse de que ha utilizado la abreviatura correcta para el comando que desea utilizar.

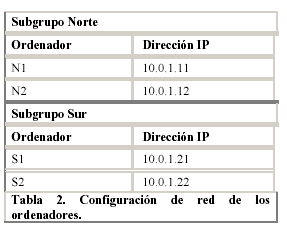
**#?**Exec Commands:  
 clear Reset functions  
 configure Enter configuration mode  
 copy Copy configuration or firmware  
 delete Reset configuration  
 disable Turn off privileged commands  
 enable Turn on privileged commands  
 exit Exit from the EXEC  
 help Description of the interactive help system  
 menu Enter menu interface  
 ping Send echo messages  
 reload Halt and perform warm start  
 session Tunnel to module  
 show Show running system information  
 terminal Set terminal line parameters  
 vlan-membership VLAN membership configuration

**Parte 1.2: Familiarizarse con el funcionamiento del switch y realizar pruebas básicas.**

Armar un laboratorio de red como el de la figura 1.

Configuración de los ordenadores y prueba básica de conectividad

Cada alumno deberá asignar una dirección IP a los ordenadores de acuerdo con lo que se indica en la tabla 2.



**Configuración IP de los switches, asignación de password y conexión vía telnet**

Configurar mediante el comando *hostname* los nombres de los Switch. Ahora asignaremos una dirección IP al switch. Una vez en modo Privilegiado tecleamos el comando **‘configure’** para pasar al modo Configuración Global, cosa que reconoceremos porque el prompt cambia ahora a **‘(config)#’**. En el modo de Configuración Global tecleamos **‘?’** y veremos que aparece en la lista el comando **‘ip’**; tecleando **‘ip ?’** averiguaremos qué parámetros admite dicho comando. Uno de ellos es **‘address’**, que sirve para asignar una dirección IP y máscara al switch. Utilizaremos este comando para introducir la configuración IP correspondiente, de acuerdo con la relación que aparece en la Tabla 3 (por ejemplo para el switch Norte el comando a teclear será **‘ip address 10.0.1.10 255.255.255.0’**. Una vez hecho esto saldremos del modo

Configuración Global tecleando **CTRL/Z**. Al salir de este modo volvemos al modo Privilegiado, por lo que el prompt vuelve a ser **‘#’**. La secuencia completa de comandos para el switch Norte sería por ejemplo la siguiente:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**ip address 10.0.1.10 255.255.255.0**

(config)#**CTRL/Z**

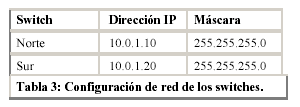
#

(config)#hostname Norte

Norte(config)#ip address 10.0.1.10 255.255.255.0

(config)#hostname Sur

Sur(config)#ip address 10.0.1.20 255.255.255.0



Una vez le hemos asignado una dirección IP al switch ya podemos comunicarnos con él desde cualquier ordenador conectado a la red, como podemos comprobar lanzándole paquetes de prueba mediante el comando **ping**. En principio esto nos debería permitir configurarlo vía telnet desde cualquier ordenador. Sin embargo, por razones de seguridad no se permite el acceso vía telnet cuando el equipo no tiene password, por lo que lo siguiente que haremos será asignarle una password. La password que utilizaremos es **‘password’** (sin las comillas). Para introducirla teclearemos por consola en modo Configuración Global el comando **‘enable password level 15 password’** (como antes entraremos en el modo Configuración Global con el comando **‘configure’** y saldremos con **‘CTRL/Z’**). La secuencia completa es la siguiente:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**enable password level 15 password**

(config)#**CTRL/Z**

#

Sur(config)#enable password level 15 password

Sur(config)#exit

**El password usado es: password**

A partir de este momento podremos acceder vía telnet al switch desde cualquier ordenador conectado a él.

Ahora nos conectaremos desde los dos ordenadores al switch vía telnet, para acceder como consola remota.

**Uso del comando ‘show interface’**

En primer lugar pasaremos al modo Privilegiado mediante el comando **‘enable’** (password **‘password’**) y teclearemos el comando **‘show interfaces’** para ver las características y forma de numerarse de las diferentes interfaces del equipo. La salida generada por este comando ocupa varias pantallas, quedándose el Terminal boqueado cuando se completa la primera, lo cual viene indicado por el texto ‘more’ al final de la pantalla.

Para avanzar a la siguiente debemos pulsar la barra espaciadora y así sucesivamente hasta agotarlas todas. La salida por pantalla puede abortarse en cualquier momento pulsando **CTRL/C**.

El comando **‘show interfaces’** puede utilizarse con argumentos, con lo que podemos obtener información sobre una interfaz en particular. Esto resulta útil cuando sólo se quiere obtener información sobre una o unas pocas interfaces. Por ejemplo el comando **‘show interface Ethernet 0/2’** (que podemos abreviar a **‘s in e 0/2’**) nos muestra información sobre la interfaz número 2 únicamente. Ahora haremos un **‘show interface’** de la interfaz donde está conectado nuestro ordenador (Ethernet 0/1 ó Ethernet 0/2) y nos fijaremos en la información que aparece.

Sur#show interface

**Ethernet 0/1 is Enabled**

**(Esta informacion la da por cada interface del switch de 1 a 12, la 26 y 27)**

Hardware is Built-in 10Base-T

Address is 00b0.af91.67b8

MTU 1500 bytes, BW 10000 Kbits

802.1d STP State: Forwarding Forward Transitions: 1

Port monitoring: Disabled

Unknown unicast flooding: Enabled

Unregistered multicast flooding: Enabled

Description:

Duplex/Flow Control setting: Half duplex

Enhanced Congestion Control: Disabled

Receive Statistics Transmit Statistics

------------------------------------- -------------------------------------

Total good frames 215 Total frames 581

Total octets 20906 Total octets 40585

Broadcast/multicast frames 215 Broadcast/multicast frames 581

Broadcast/multicast octets 20906 Broadcast/multicast octets 40585

Good frames forwarded 44 Deferrals 0

Frames filtered 171 Single collisions 0

Runt frames 0 Multiple collisions 0

No buffer discards 0 Excessive collisions 0

Queue full discards 0

Errors: Errors:

FCS errors 0 Late collisions 0

Alignment errors 0 Excessive deferrals 0

Giant frames 0 Jabber errors 0

Address violations 0 Other transmit errors 0

Ethernet 0/2 is Enabled

Hardware is Built-in 10Base-T

Address is 00b0.af92.6818

MTU 1500 bytes, BW 10000 Kbits

802.1d STP State: Forwarding Forward Transitions: 1

Port monitoring: Disabled

Unknown unicast flooding: Enabled

Unregistered multicast flooding: Enabled

Description:

Duplex/Flow Control setting: Half duplex

Enhanced Congestion Control: Disabled

**Verificación y cambio del tipo de conexión.**

Ahora haremos una prueba de los problemas de rendimiento que se producen cuando se tiene una configuración mixta half-full en una conexión Ethernet. Las interfaces 10BASE-T del switch no negocian el modo half-full y tienen por defecto configuración half-dúplex. En cambio las tarjetas de los ordenadores sí negocian el modo half-full en el momento de conectarse. Por tanto los ordenadores al conectarse al switch se han puesto a trabajar en modo half-duplex.

Cambiar a modo full dúplex la interfaz Ethernet 0/1 en la que se conecta el ordenador 1. Para ello utilizaremos el comando **‘duplex full’** en el modo Configuración de Interfaz de la interfaz que queremos cambiar. La secuencia de comandos es la siguiente:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**int eth0/1**

(config-if)#**duplex full**

(config)# **CTRL/Z**

#

Norte(config)#interface ethernet0/1

Norte(config-if)#duplex full

Norte(config-if)#exit

Norte(config)#exit

Una vez hecho el cambio a full lo comprobaremos con el comando **‘show interfaces ethernet 0/1’** (o **‘s in e 0/1’)** y buscaremos el sitio donde ponga ‘Duplex setting: Full duplex’.

**Parte 2.1: Crear dos VLANs y comunicarlas**

En esta parte de la práctica se crearán dos VLANs en cada switch y se asignarán los puertos a una u otra. A continuación conectaremos entre sí ambos switches , primero en una VLAN y luego en la otra.

A las VLANs las llamaremos ‘pares’ y ‘impares’ y les asignaremos los números 2 y 3 respectivamente (el número 1 está reservado para la VLAN ‘default’, que es la que viene por defecto configurada en el equipo). Para crear las VLANs entraremos en consola del switch y utilizaremos en modo Configuración Global el comando **‘vlan’** según se muestra a continuación:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**vlan 2 name pares**

(config)#**vlan 3 name impares**

(config)#**CTRL/Z**

#

Ahora podemos utilizar el comando **‘show vlan’** para comprobar que las definiciones se han realizado correctamente. Lo que aparece por pantalla debe ser similar a esto:

#**show vlan**

Norte#show vlan

VLAN Name Status Ports

--------------------------------------

**1 default Enabled 1-12,A,B,AUI (todas por defecto….)**

**2 pares Enabled**

**3 impares Enabled**

1002 fddi-default Suspended

1003 token-ring-defau Suspended

1004 fddinet-default Suspended

1005 trnet-default Suspended

--------------------------------------

VLAN Type SAID MTU Parent RingNo BridgeNo Stp Trans1 Trans2

---------------------------------------------------------------------------

1 Ethernet 100001 1500 0 0 0 Unkn 0 0

2 Ethernet 100002 1500 0 0 0 Unkn 0 0

3 Ethernet 100003 1500 0 0 0 Unkn 0 0

1002 FDDI 101002 1500 0 0 0 Unkn 0 0

1003 Token-Ring 101003 1500 0 0 0 Unkn 0 0

1004 FDDI-Net 101004 1500 0 0 0 IEEE 0 0

1005 Token-Ring-Net 101005 1500 0 0 0 IBM 0 0

---------------------------------------------------------------------------

#conf

Enter configuration commands, one per line. End with CNTL/Z

Norte(config)#vlan 2 name pares

Norte(config)#vlan 3 name impares **(hacer esto por cada switch)**

Una vez creadas las VLANs debemos asignar los puertos a ellas. Si un puerto no lo asignamos a ninguna de las dos quedará en la VLAN ‘default’ (la 1) que es en la que se encuentran todos inicialmente.

Únicamente asignaremos los puertos 1, 2, 5, 6, 7 y 8 en el SWITCH Norte y 1, 2, 5 y 6 en el Sur, los pares a la VLAN ‘pares’ y los impares a la VLAN ‘impares’. Para ello utilizaremos en el modo Configuración de Interfaz, el comando **‘Switchport**.. La secuencia de comandos a utilizar, por ejemplo en el switch Norte, es la siguiente:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**interface ethernet 0/1**

(config-if)#**switchport access vlan 3**

(config-if)#**i e 0/2**

(config-if)# **switchport access vlan 2**

(config-if)#**i e 0/5**

(config-if)# **switchport access vlan 3**

(config-if)#**i e 0/6**

(config-if)# **switchport access vlan 2**

(config-if)#**i e 0/7**

(config-if)# **switchport access vlan 3**

(config-if)#**i e 0/8**

(config-if)# **switchport access vlan 2**

(config-if)#**exit**

(config)#**CTRL/Z**

#

Norte(config)#interface ethernet0/1

Norte(config-if)# switchport access vlan3

Norte(config-if)#interface ethernet0/2

Norte(config-if)#switchport access vlan2

Norte(config-if)#interface ethernet0/5

Norte(config-if)# switchport access vlan3

Norte(config-if)#interface ethernet0/6

Norte(config-if)# switchport access vlan2

Norte(config-if)#interface ethernet0/7

Norte(config-if)# switchport access vlan3

Norte(config-if)#interface ethernet0/8

Norte(config-if)# switchport access vlan2

Norte(config-if)#exit

Recordemos que la tecla **CTRL/P** (o flecha arriba) repite el comando anterior, lo cual facilita la introducción repetida de un mismo comando, algo especialmente útil en este caso. Si repetimos ahora el comando **‘show vlan’** obtendremos un resultado como el siguiente:

#**show vlan**

Norte#show vlan

VLAN Name Status Ports

--------------------------------------

**1 default Enabled 3-4,9-12,A,B,AUI**

**2 pares Enabled 2,6,8 (configuradas las pares)**

**3 impares Enabled 1,5,7 (configuradas las impares)**

1002 fddi-default Suspended

1003 token-ring-defau Suspended

1004 fddinet-default Suspended

1005 trnet-default Suspended

--------------------------------------

VLAN Type SAID MTU Parent RingNo BridgeNo Stp Trans1 Trans2

---------------------------------------------------------------------------

1 Ethernet 100001 1500 0 0 0 Unkn 0 0

2 Ethernet 100002 1500 0 0 0 Unkn 0 0

3 Ethernet 100003 1500 0 0 0 Unkn 0 0

1002 FDDI 101002 1500 0 0 0 Unkn 0 0

1003 Token-Ring 101003 1500 0 0 0 Unkn 0 0

1004 FDDI-Net 101004 1500 0 0 0 IEEE 0 0

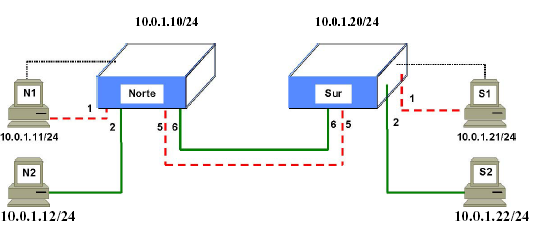
1005 Token-Ring-Net 101005 1500 0 0 0 IBM 0 0

---------------------------------------------------------------------------

**Verificar y capturar lo configurado**

A continuación realizaremos una conexión entre ambos switch mediante la interfaz 6 . Pero ahora esa interfaz pertenece a la VLAN pares, por lo que con esa conexión solo podrán comunicarse entre los dos Switch los ordenadores de la VLAN pares. Los alumnos deberán comprobar que en efecto la comunicación entre los ordenadores N2 y S2 es posible, pero no entre N1 y S1.

Para conseguir comunicación entre N1 y S1 uniremos la interfaz 5 de ambos switches mediante otro patch ‘crossover’ (figura ) . Una vez hecho esto comprobaremos que hay comunicación N1-S1. Sin embargo sigue sin haber comunicación N1-S2 ni N2-S1.



**Figura . Conexión independiente de las VLANs ‘pares’ y ‘impares’**

Nota: en el simulador un cable crossover (cruzado en sus pares 1-3 y 2-6) figurara como una conexión en otro color.

Como uniría en un switch real ambas VLAN? Como lo haria en el caso del simulador?

Vamos a proceder ahora a interconectar de los dos switch a 100 Mb/s. Como disponemos de dos interfaces de este tipo (A y B) (estas interfaces son las FastEthernet, puertos 26 y 27) bastaría con asignar una a la VLAN pares y otro a la impares y conectar ambas entre los dos switch, como hemos hecho antes.

Realizar esta prueba asignando estos puertos a las VLAN

**Parte 2.2: Configuración de un enlace ‘trunk’.**

El ejercicio anterior presenta tres inconvenientes:

. • Requiere utilizar dos cables para la conexión de los switch.

. • Consume todos los puertos Fast Ethernet de los switch, por lo que ya no sería posible

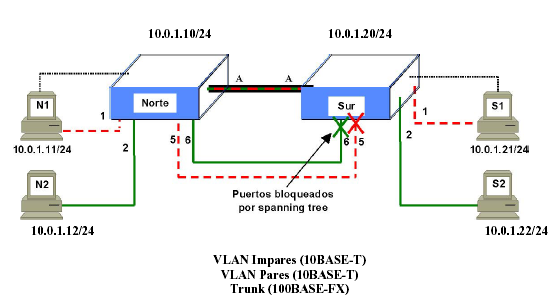
realizar otras conexiones a 100 Mb/s en ellos.

. • No se podría utilizar si hubiera más de dos VLANs en los switches.

Para evitar esos problemas utilizaremos un enlace **trunk**, que permite enviar por un solo enlace el tráfico de varias VLANs.

Para enviar por un enlace tráfico de varias VLANs sin riesgo de mezclarlas es preciso etiquetar las tramas que se envían de alguna manera. Actualmente el estándar IEEE 802.1Q establece una forma estándar de realizar ese etiquetado (también llamado encapsulado) pero los Cisco 1900 son anteriores a dicho estándar por lo que no lo soportan. En su lugar utilizan un encapsulado propietario de Cisco que se denomina ISL (Inter Switch Link). Como en nuestro caso los dos switch son del mismo modelo esto no plantea ningún problema de interoperabilidad, pero podría serlo si quisiéramos integrar en la red equipos de otros fabricantes que no soportaran ISL.

En esta parte de la práctica configuraremos la interfaz A (FastEthernet 0/26) de cada switch como un enlace trunk . Esta interfaz no estará asignada a ninguna VLAN en particular sino a todas a la vez y podrá redirigir tramas pertenecientes a cualquiera de las VLANs existentes en ambos switch. De esta forma un enlace será suficiente para la conexión de los dos switch, independientemente del número de VLANs que se configuren en ellos.



**Creación de un enlace ’Trunk’**

Para configurar una interfaz en modo trunk utilizamos el comando **‘trunk’** dentro del modo Configuración de Interfaz correspondiente a la interfaz que se quiere modificar. La secuencia de comandos en nuestro caso es la siguiente:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**i f 0/26**

(config-if)#**trunk on**

(config-if)#**exit**

(config)#**CTRL/Z**

#

Sur(config)#int f0/26

Sur(config-if)#trunk on

Sur(config-if)#exit

Sur(config)#exit

Sur#

con el trank hecho en los 2Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-1999 Microsoft Corp.

Norte#show trunk A

DISL state: On, Trunking: On, Encapsulation type: ISL

C:\>ping 10.0.3.21

Pinging 10.0.3.21 with 32 bytes of data:

Reply from 10.0.3.21 ;bytes=32 time=22ms TTL=254

Reply from 10.0.3.21 ;bytes=32 time=22ms TTL=254

Reply from 10.0.3.21 ;bytes=32 time=22ms TTL=254

Reply from 10.0.3.21 ;bytes=32 time=22ms TTL=254

Ping Statistics for 10.0.3.21:

Packets Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 22ms, Maximum = 23ms, Average = 22ms

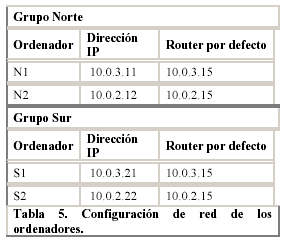
Podemos comprobar que la configuración se ha realizado correctamente tecleando el comando en modo Privilegiado **‘show trunk A’**(A corresponde al puerto 26). Una vez hecho el cambio en ambos switches los conectaremos por el puerto A

**Parte 2.3: Interconexión de las VLANs mediante routers**

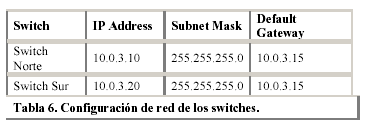
**Conexión de las VLANs mediante un router**

A continuación interconectaremos las dos VLANs mediante un router, que como ya hemos comentado es la manera normal de hacer dicha interconexión.

Pero antes de conectarlas mediante un router debemos separar nuestras dos VLANs en dos redes IP diferentes. Antes hemos utilizado direcciones de la red 10.0.1.0/24 (máscara 255.255.255.0) para todos los ordenadores; esta red abarca todas las direcciones desde la 10.0.1.1 hasta la 10.0.1.254. Esto era lo lógico cuando todos los ordenadores pertenecían a la misma VLAN, y también cuando estando en VLANs diferentes las uníamos mediante un cable puente. Pero como ahora queremos que las dos VLANs se unan mediante un router debemos asignarles direcciones de redes diferentes. Usaremos pues la red 10.0.2.0/24 (máscara 255.255.255.0) para la VLAN pares y la 10.0.3.0/24 (máscara 255.255.255.0) para la VLAN impares. Estas redes abarcan las direcciones 10.0.2.1-254 y 10.0.3.1-254, respectivamente. Además le asignaremos a cada host un router por defecto, que será el que utilizará para comunicar con otros hosts que no pertenezcan a su misma red IP (es decir a su misma VLAN). Los valores que debemos asignar ahora a los hosts son los que figuran en la tabla 5:



Ahora debemos modificar las direcciones IP de los switch, y asignarles también un router por defecto. Recordemos que hemos elegido que la VLAN impares actúe como VLAN de gestión de los switches, por lo que les debemos asignar direcciones que pertenezcan a dicha VLAN. Para asignar las direcciones IP utilizamos el comando **‘ip address’**, mientras que para asignar el router por defecto emplearemos el comando **‘ip default-gateway’**, ambos en modo Configuración Global. Los datos a introducir son los siguientes:



Por ejemplo la secuencia de comandos para el Switch Sur será la siguiente:

#**config**

Enter configuration commands, one per line. End with CNTL/Z

(config)#**ip address 10.0.3.20 255.255.255.0**

(config)#**ip default-gateway 10.0.3.15**

(config)#**CTRL/Z**

Sur(config)#ip address 10.0.3.20 255.255.255.0

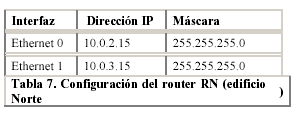
Sur(config)#ip default-gateway 10.0.3.15

Sur(config)#exit

Para la interconexión de los switch se deberá colocar en el Switch Norte un router (RN) con dos interfaces Ethernet.

El router dispone además de interfaces serie que no se utilizan en esta práctica. El modelo de router puede variar en función del material disponible en cada momento. En algunos equipos las interfaces Ethernet se identifican exteriormente como **‘Ethernet 0’** y **‘Ethernet 1’** o FastEthernet 0 y FastEthernet 1 A nivel de configuración las interfaces se denominan **‘Ethernet 0’** y **‘Ethernet 1’** respectivamente en todos los modelos.

Configurar el router con los siguientes datos



Utilizar los siguientes comandos

Router1#conf t

Router1(config)#interface Fast0/0

Router1(config-if)#encap dot1q 2

Router1(config-if)#ip address 10.0.2.15 255.255.255.0

Router1(config-if)#exit

Router1(config)#interface Fast0/1

Router1(config-if)#encap dot1q 3

Router1(config-if)#ip address 10.0.3.15 255.255.255.0

Poner operativas las interfaces.

RN(config)#interface Fast0/0

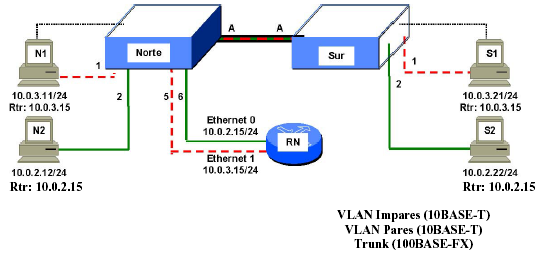
RN(config-if)#encap dot1q 2

RN(config-if)#ip address 10.0.2.15 255.255.255.0

RN(config-if)#exit

La configuración del router está preparada para conmutar paquetes entre las dos redes. Los alumnos deben ahora conectar el router según se muestra en el esquema de la figura 10, es decir la interfaz Ethernet 0 (o AUI 0) a la interfaz 6 del Switch Norte, y la Ethernet 1 (AUI 1) a la interfaz 5.

**10.0.3.10/24 (impares) 10.0.3.20/24 (impares)**



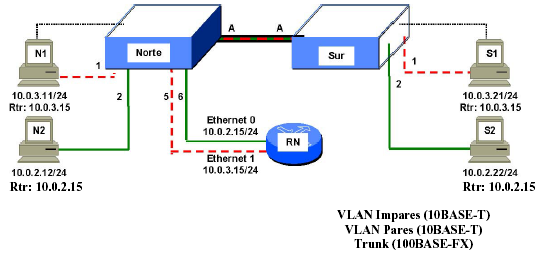
**Figura. Interconexión física de las dos VLANs mediante un router**

Ahora los alumnos deberán comprobar que es posible la comunicación entre cualquier par de hosts. En caso de problemas se puede probar a hacer un ping a la interfaz del router que se encuentra en nuestra misma VLAN, por ejemplo si es un ordenador de la VLAN impares haremos ping a 10.0.3.15.

Los hosts que se encuentran en la misma VLAN se comunican directamente, mientras que los que están en VLANs diferentes lo hacen a través del router.

**Parte 2.4: Interconexión de las VLANs mediante routers con una sola interface**

**OBJETIVO**:  Aprender a configurar un router con subinterfaces y rutear distintas vlans de un switch conectado al mismo con una sola interface en modo TRUNK.

” 

Se necesita habilitar el TRUNK en la interface Fast Ethernet del Switch que está conectada al Router.

Nota: Los links configurados como Trunk se utilizan para transportar varias vlans entre dispositivos de la red. El Trunking solamente puede ser soportado por las interfaces Fast Ethernet. También el Trunking tiene dos tipos de métodos de encapsulacion, ISL y 802.1q.

(config)#interface Fast 0/5

(config)#Trunk on

En este momento el switch ya está configurado, por lo tanto este transporta los paquetes de ambas vlans hasta el Router. Lo que se debe hacer ahora es enseñarle al router como aceptar esos paquetes.

Para ello ingresar al Router RN y configurar en la subinterface FastEthernet 0/0.2 “encapsulación dot1q con la vlan2” y en la subinterface FastEthernet 0/0.3 “encapsulación dot1q con la vlan3.”

RouterRN#conf t

RouterRN(config)#interface Fast0/0.2

RouterRN(config-if)#encap dot1q 2

RouterRN(config-if)#ip address 10.0.2.15 255.255.255.0

RouterRN(config-if)#exit

RouterRN(config)#interface Fast0/0.3

RouterRN (config-if)#encap dot1q 3

RouterRN(config-if)#ip address 10.0.3.15 255.255.255.0

Completa la configuración necesaria se debe comprobar que ahora “si” se puede pinguear cualquier equipo de la red.

Habiendo podido realizar los “pings” solicitados en los puntos anteriores, se determinó que existe comunicación entre cada una de las redes o “áreas de la empresa”. Esto se logra ya que el Router es un dispositivo capaz de manejar distintas redes y realizar el ruteo necesario para que haya visibilidad entre dichas redes, es decir que se puedan comunicar entre sí.

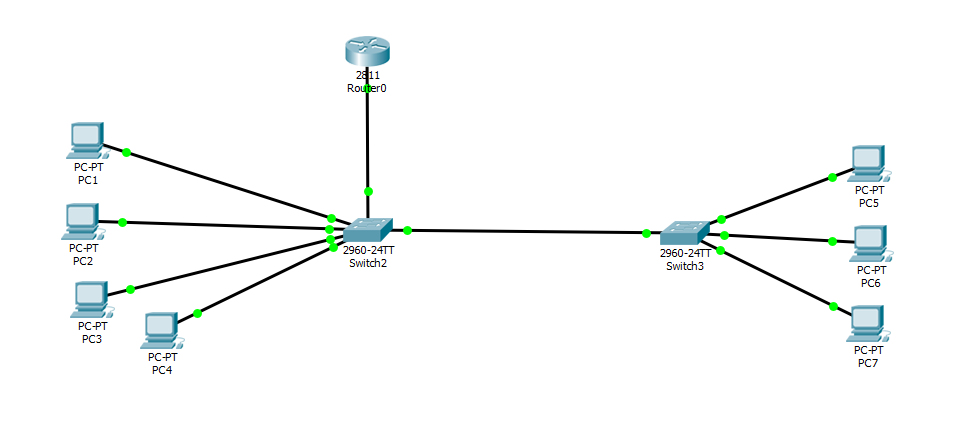
Por último, ingresando al Switch, se podrán ver las vlans asignadas en cada uno de los ports del equipo utilizando los siguientes comandos, *“show vlan”* y *“show vlan-membership”.*

(config-if)#end

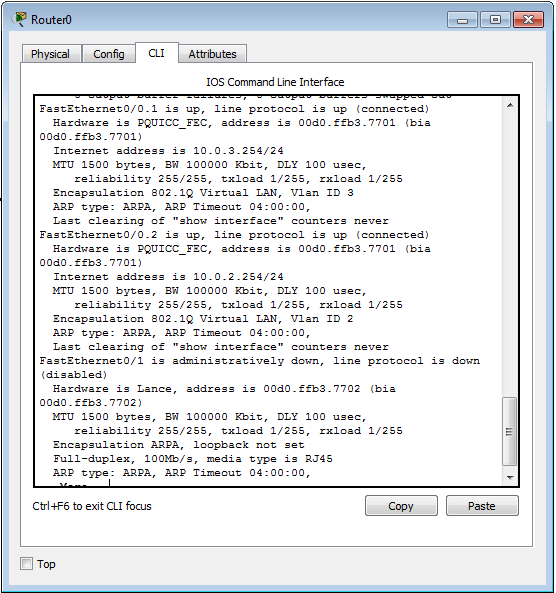
#show vlan

#show vlan-membership

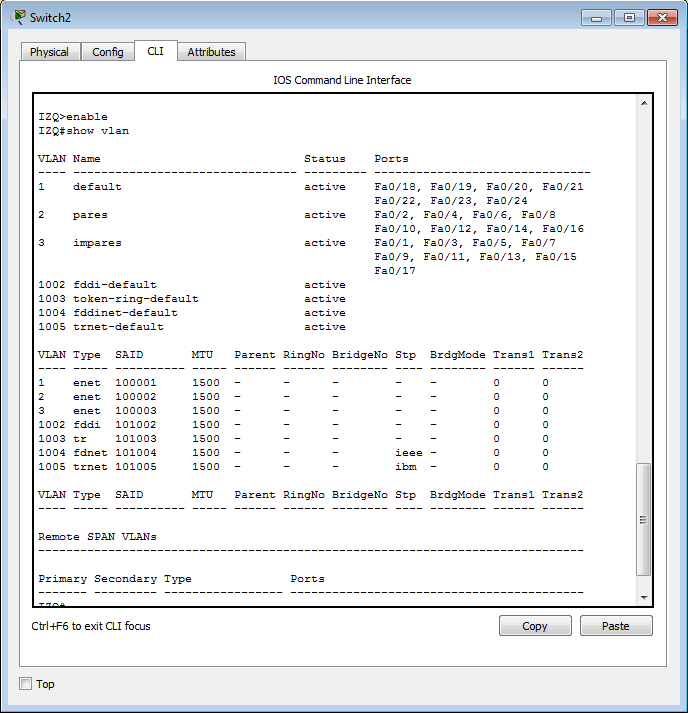
Capturas del funcionamiento:



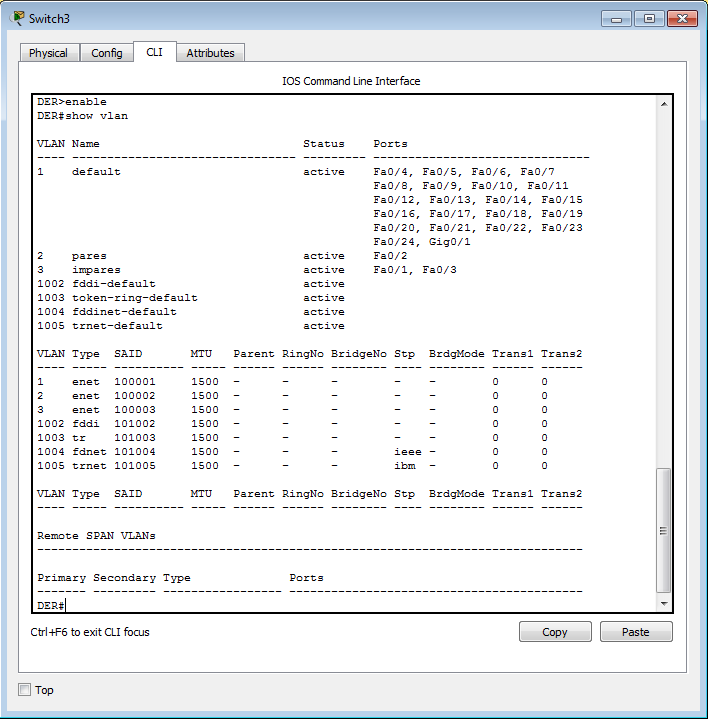
Ejemplo de topología finalizada y en funcionamiento.



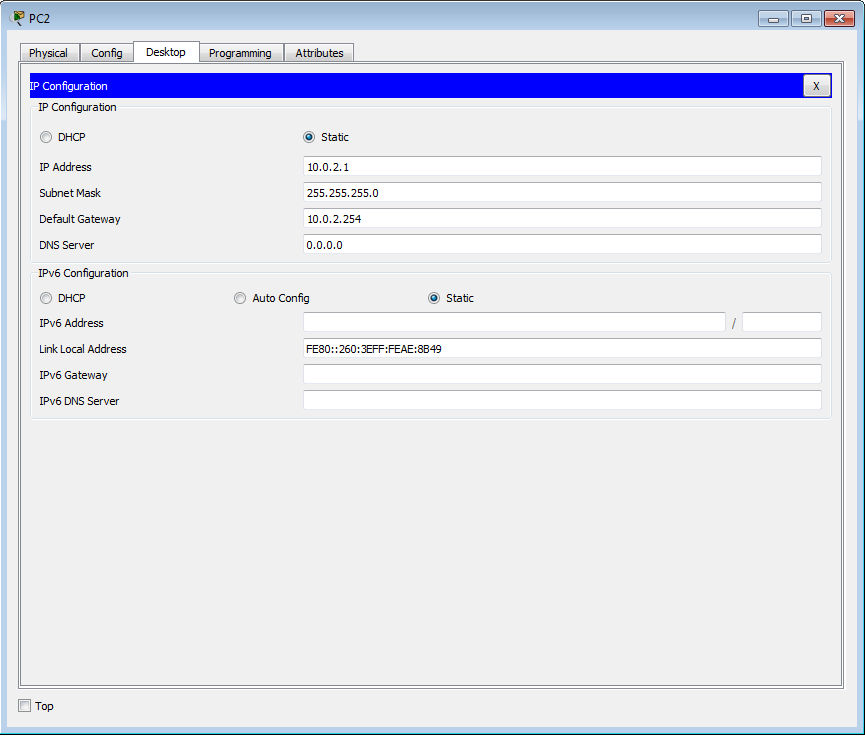
Captura de configuracion de subinterfaces 0/0.2 y 0/0.3



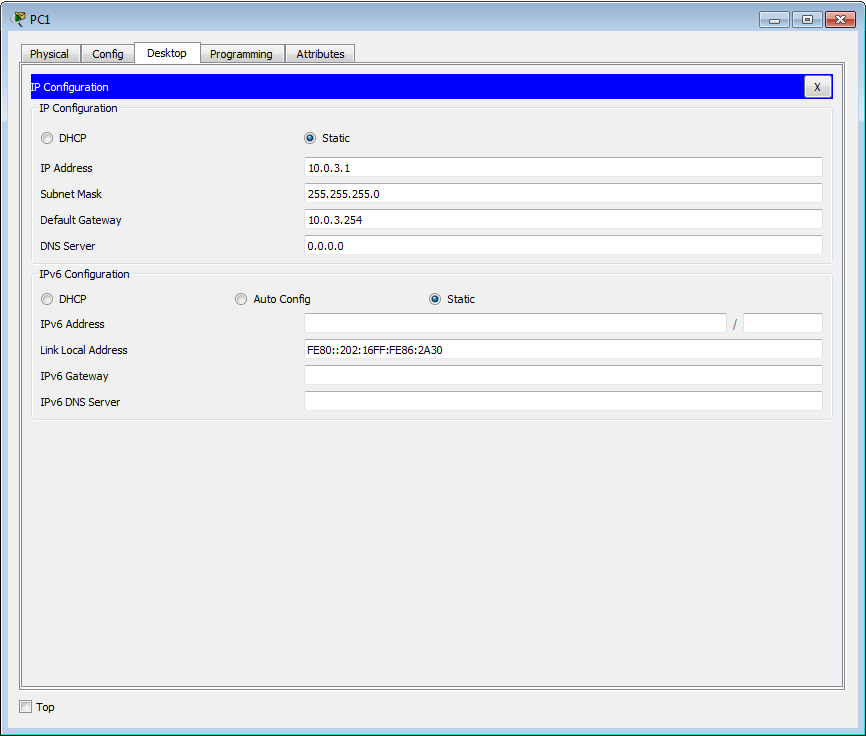
Configuracion de vlan 2 y 3 del primer switch, junto con los puertos asignados.



Configuracion de vlan 2 y 3 del segundo switch, junto con los puertos asignados.



Ejemplo de host miembro de vlan 2.



Ejemplo de host miembro de vlan 3.

**CONCLUSIONES**:

Suponiendo que cada una de las PCs representan distintas áreas dentro de una empresa se puede decir que en la red tenemos mucho trafico interno. Parte de ese trafico se concentra en el área “A” y otra parte se concentra en el área “B”.

Separando las vlans pudimos lograr también separar el trafico. (Recordar que las vlans separan dominos de broadcast dentro de los Switch de layer 2). De esta forma el trafico del área “A” no es escuchado por el área “B”.

El único problema es que cuando alguien de una de las área quiere comunicarse con alguien de otra área, ambas redes se ven imposibilitadas de hacerlo.

Para poder hacerlo se debió utilizar un router. En el router se crearon subinterfaces (una por cada subnet/vlan) y se configuro cada una de ellas de forma tal que encapsulen los paquetes con ISL (esto nos permitió comunicar el puerto Fast Ethernet del router con el puerto Fast Ethernet del switch configurado como trunk).

De esta forma se logra tener al switch separando dominios de broadcast y al router administrando las vlans para que puedan comunicarse unas con otras.