IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE: INGENIERO EN COMUNICACIONES Y ELECTRONICA

NOMBRE DEL SEMINARIO: INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD

VIGENCIA: DES/ESIME-CUL/5052005/23/12

DEBERA DESARROLLAR: BELLO DIAZ JESUS ALEJANDRO
HERNANDEZ PALMARES ISRAEL
LUNA MIRANDA JOAQUIN
MIGUEL GARCIA GIULIANI
UREÑA REYES ROSA MARIA

NOMBRE DEL TEMA

"CONFIGURACIÓN DEL CRECIMIENTO DE LA RED DE DATOS DE LA EMPRESA OMEGA"

INTRODUCCIÓN

La seguridad en una red es el principal factor que se debe contemplar en su implementación, debido a un gran incremento en los ataques cibernéticos provocados por la creciente necesidad de comunicación a través de medios electrónicos y la gran cantidad de datos personales que fluyen en la red.

CAPITULADO

I. INTRODUCCION A LAS REDES
II. ETHERNET
III. SWITCHEO
IV. CONFIGURACION DEL CRECIMIENTO DE LA RED DE DATOS DE LA EMPRESA OMEGA

México D.F. Junio de 2012

M. EN C. RAYMUNDO SANTANA ALQUICIRA
Coordinador del Seminario

ING. PEDRO AVILA BUSTAMANTE
Instructor del Seminario

M. EN C. ANTONIO ROMERO ROJANO
Jefe de la carrera de I.C.E

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD PROFESIONAL CULHUACAN

“Configuración del crecimiento de la red de datos de la empresa OMEGA”

T E S I N A

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

POR OPCIÓN DE SEMINARIO

PRESENTAN:

BELLO DIAZ JESUS ALEJANDRO
HERNANDEZ PALMARES ISRAEL
LUNA MIRANDA JOAQUIN
MIGUEL GARCIA GIULIANI
UREÑA REYES ROSA MARIA

México D.F JUNIO 2012

Índice temático.

Capítulo 3 Switcheo

Capítulo 4 "Configuración del crecimiento de La red de datos de la empresa OMEGA"

Anexos

- **Objetivo.**

Realizar las configuraciones estándar de seguridad del corporativo para los switches de la red y dar servicio a los nuevos usuarios.

- **Problemática.**

Debido a que la red es de reciente implementación, no cuenta con ningún servicio configurado en los equipos de la red LAN, por ello se necesita darlos de alta para que los nuevos usuarios trabajen con los estándares del corporativo, así como brindar criterios de seguridad a los usuarios de los diferentes departamentos laborales.

- **Justificación.**

Con las configuraciones de los switches de la red se establecerá la comunicación y los servicios necesarios para los administradores de la nueva red.

- **Alcance.**

Únicamente se configuraran los switches de la etapa de acceso de la red para dar los servicios de internet, almacenamiento, seguridad y correo electrónico a los usuarios finales.

Introducción.

La seguridad en una red es el principal factor que se debe contemplar en la implementación de esta, debido a un gran incremento en los ataques cibernéticos provocados por la creciente necesidad de comunicación a través de medios electrónicos y la gran cantidad de datos personales que fluyen en la red.

En la actualidad no basta con implementar tecnologías que faciliten una conexión cada vez más rápida a la red, si no se tienen las más mínimas medidas de seguridad, los datos estarán expuestos a toda persona con conocimientos de informática e intenciones maliciosas.

Existen diversas herramientas que van desde las más básicas hasta herramientas sofisticadas que protegen los datos a través de la red interna de una empresa o a través de internet. El saber implementarlas garantiza cumplir con el compromiso de proteger los datos de los usuarios de nuestra red y con esto impulsar un mayor crecimiento de la productividad de los usuarios.

Las herramientas de seguridad no solo basta con instalarlas y/o activarlas, se debe llevar todo un proceso de monitoreo que permita una completa revisión del funcionamiento de estas con el fin de garantizar una seguridad eficiente.

Las herramientas de seguridad que se tratan en este proyecto van encaminadas a demostrar que con una correcta planeación del control del tráfico de datos generado por una área laboral se puede cumplir con una condición de seguridad la cual evita que una persona ajena a estos datos pueda llegar a interceptarlos y comprometer las funciones laborales de quien los genero.

Capítulo 1

INTRODUCCIÓN A LAS REDES

1.1 Modelo OSI.

A principios de la década de 1980 el desarrollo de redes sucedió con desorden en muchos sentidos. Se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. Para mediados de la década de 1980, las empresas comenzaron a sufrir las consecuencias de la rápida expansión. Las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de conexiones privadas o propietarias. Las tecnologías de conexión que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de conexión a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes llamado “modelo de referencia de Interconexión de Sistemas Abiertos” OSI por sus siglas en inglés (Open System Interconnection) (Figura 1.1).

Figura 1.1 Modelo OSI

1.1.1 Capa 1 (Física).

Esta capa es la encargada de los aspectos mecánicos de los componentes de la red, incluyendo la interpretación de las señales eléctricas/electromagnéticas, sistemas de tierra física, velocidades de transmisión y demás elementos físicos de la red mediante las normas y estándares creados por los diferentes organismos involucrados en resolver los problemas de incompatibilidad en redes tales como ISO, IEEE y la TIA/EIA.

Otra de sus funciones es la de transmitir los bits de información a través del medio utilizado, el cual puede ser un medio guiado o no guiado, es decir, un medio cableado o inalámbrico, así como el modo de transporte de estos bits que puede ser:

- SIMPLEX: donde la información viaja en un solo sentido de emisor a receptor.
- HALF DUPLEX: donde la información viaja en ambos sentidos pero no al mismo tiempo alternando el emisor y el receptor sus posiciones durante la transmisión.
- FULL DUPLEX: donde la información viaja en ambos sentidos y al mismo tiempo de emisor a receptor.

1.1.2 Capa 2 (Enlace De Datos).

Esta capa se ocupa del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Esta capa del modelo OSI se subdivide en dos subcapas con el fin de proporcionar un mayor control para el acceso a la red dado que una subcapa es para enlace lógico (LLC Logical Link Control) y la otra subcapa es para enlace físico (MAC Media Access Control) (Figura 1.2).

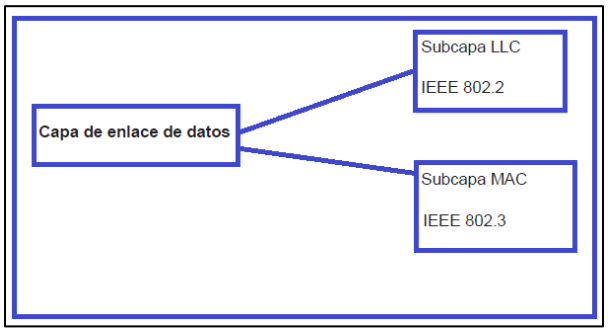


Figura 1.2 Capa De Enlace y Subcapas LLC y MAC

1.1.3 Capa 3 (Red).

Esta capa se ocupa de que la información llegue desde el origen al destino, aun si ambos extremos no están conectados directamente, esto quiere decir que, los datos pueden llegar desde un origen situado en una ciudad en un extremo del mundo hasta otra cuidad destino del otro lado del mundo sin la necesidad de tener un solo cable o un solo dispositivo que conecte ambos puntos.

Cubrir grandes distancias se consigue gracias a los protocolos de ruteo RIP, OSPF, EIGRP y BGP y dispositivos llamados routers que logran tener una interconexión entre ellos de tal manera que logran cubrir grandes distancias y la información fluye entre ellos como si fuese una carrera de relevos.

1.1.3.1 IP (Internet Protocol).

El protocolo de internet es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes. Existen dos versiones de direcciones IP, la versión 4 y 6. Las IPs versión 6 están fuera del alcance de este proyecto por lo que solo se tratan las direcciones versión 4.

Las direcciones IPv4 están compuestas por 32 bits en 4 octetos de 8 bits cada uno separados por un punto (Figura 1.3).

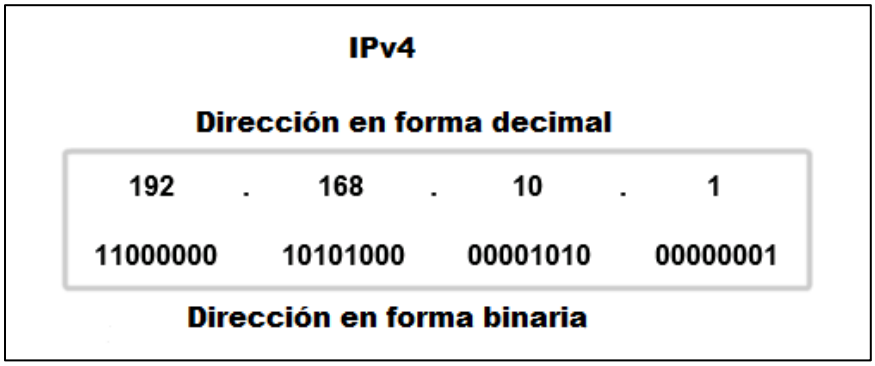


Figura 1.3 Dirección IPv4

Expresado en formato decimal el rango de direcciones IPv4 es de 0.0.0.0 a 255.255.255.255 y este rango está dividido en direcciones públicas y privadas. Las direcciones públicas son designadas para uso en redes a las que accedemos atreves de internet tales

como los sitios web. Las direcciones privadas son utilizadas para redes internas y no son enrutables en internet.

Los bloques de direcciones privadas son:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Existe una agrupación de los rangos de direcciones IP llamadas clases, las cuales se clasifican de acuerdo al valor del primer octeto en la tabla 1.1 se muestran las características de las clases de direccionamiento IPv4.

Clase de red IP	1er rango del octeto	Parte de Red (N) y Host (H)	Máscara de subred	Número de Host por red
A	1-127	N.H.H.H	255.0.0.0	16,777,214
B	128-191	N.N.H.H	255.255.0.0	65,534
C	192-223	N.N.N.H	255.255.255.0	254
D	224-239	ND (Multicast)		
E	240-255	ND (Experimental)		

Tabla 1.1 Clases De Direcciones IPv4

1.1.4 Capa 4 (Transporte).

Esta capa se encarga de la confiabilidad del transporte de datos estableciendo sesiones entre los host origen y destino con el fin de detectar fallas en la comunicación esta capa funciona con dos protocolos base. TCP que es un protocolo orientado a conexión el cual se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de la red estableciendo una sesión entre los host implicados en la trasmisión y UDP un protocolo no orientado a la conexión que proporciona que las aplicaciones envíen sus datagramas sin antes iniciar una sesión con el host destino.

TCP y UDP incluyen un número de puerto origen y destino en sus segmentos y datagramas respectivamente (Figura 1.4). Este número de puerto permite que los datos sean direccionados a la aplicación correcta que se ejecuta en el host destino.

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos (Contacto)
De 1024 a 49151	Puertos registrados
De 49152 a 65535	Puertos privados y/o dinámicos

Figura 1.4 Número de Puertos de Aplicaciones TCP.

1.1.5 Capa 5 (Sesión).

Esta capa establece, gestiona y finaliza las conexiones procesos o aplicaciones entre usuarios finales utilizando protocolos de conexión segura SSL, TLS y RPC que proporcionan comunicaciones seguras por una red, comúnmente Internet.

1.1.6 Capa 6 (Presentación).

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible. Esta capa es la primera en trabajar más el contenido de la comunicación que en cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos.

1.1.7 Capa 7 (Aplicación).

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidores de ficheros (FTP) y páginas web (HTTP). Existen tantos protocolos como aplicaciones y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece exponencialmente.

1.1.8 Proceso de Encapsulamiento y Des encapsulamiento.

El proceso de encapsulamiento se refiere a la forma en que la información viaja a través del modelo OSI desde las capas superiores hasta la capa física en un origen y el destino tendrá el proceso inverso es decir, desde la capa física hasta las capas superiores.

Este proceso de encapsulamiento se dará siempre que un usuario acceda a la red utilizando cualquier aplicación ya sea un navegador web, enviar y recibir un correo, bajar o subir archivos a un servidor y demás aplicaciones que requieran acceder a una red ya sea interna o externa a través de internet (Figura 1.5).

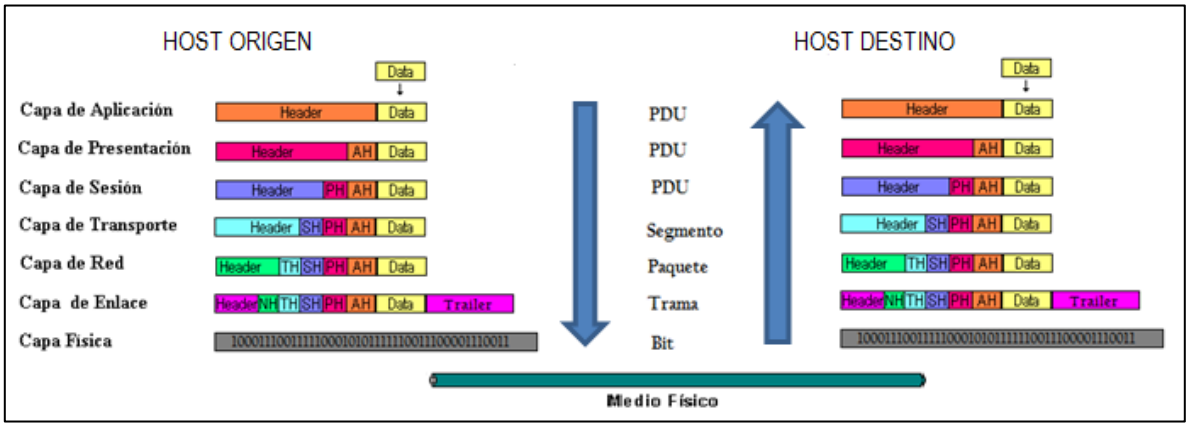


Figura 1.5 Proceso De Encapsulamiento y Des encapsulamiento.

1.2 Estándares IEEE.

La IEEE (Instituto de Ingenieros Eléctricos y Electrónicos por sus siglas en inglés) es el organismo internacional encargado de regular los estándares relacionados con el área de la electrónica y de publicarlos. Gran parte de los estándares de redes provienen de la IEEE.

El estándar IEEE 802 para redes de área local es ampliamente difundido y seguido. En la tabla 1.2 podemos observar los diferentes estándares de IEEE.

ESTANDAR	GRUPO DE TRABAJO
802.0	Comité Ejecutivo Patrocinador
802.1	Interfaces De Red De Área Local De Alto Nivel
802.2	Control De Enlace Lógico
802.3	CSMA/CD (ETHERNET)
802.4	Token Bus
802.5	Token Ring
802.6	MAN (Red De Área Metropolitana)
802.7	Banda Ancha (Transmisión General)
802.8	Fibra Óptica (Grupo Técnico De Recomendación)
802.9	Red De Área Local ISDN
802.10	Seguridad De Interoperación De Redes De Área Local
802.11	Redes De Área Local Inalámbrica
802.12	Prioridad De Demanda

802.14	Redes De Cable De Comunicaciones De Banda Ancha
802.15	Redes Personales Inalámbricas WPAN
802.16	Acceso Inalámbrico De Banda Ancha BWA

Tabla 1.2 Estándares IEEE

1.3 Topologías De Red.

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que se es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los host acceden a los medios para enviar datos. Las topologías físicas más usadas son:

- Topología de Bus.
- Topología de Anillo.
- Topología en Estrella.
- Topología en Estrella Extendida.
- Topología Jerárquica.
- Topología de Malla.

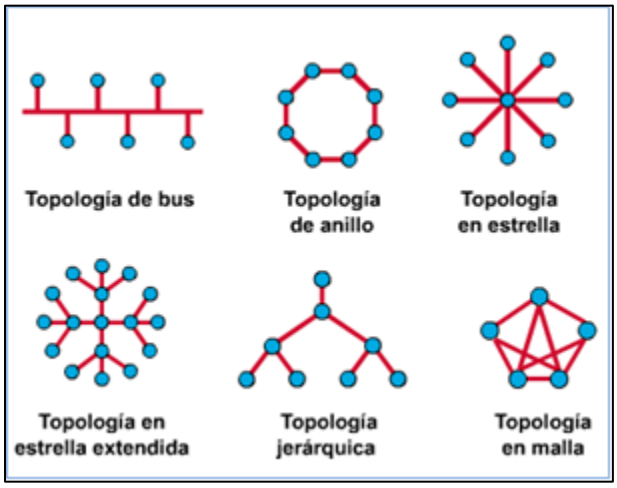


Figura 1.6 Topologías

La topología lógica de una red es la forma en que los host se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son Ethernet y Token ring.

1.4 Modelo De Redes Jerárquicas.

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico.

En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo (core)(Figura 1.7).

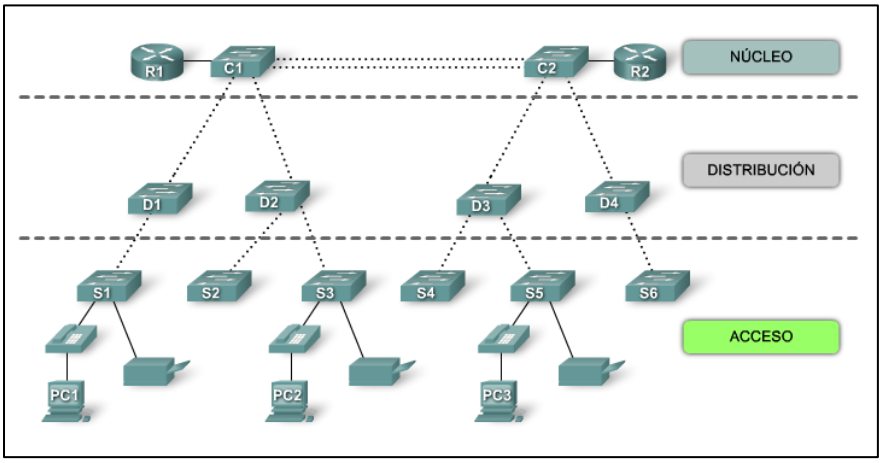


Figura 1.7 Modelo Jerárquico De Redes

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos.

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso.

La capa núcleo del diseño jerárquico es el backbone (columna vertebral) de alta velocidad de la internetwork. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. En redes muy pequeñas, es usual que se implemente un modelo de núcleo colapsado, en el que se combinan la capa de distribución y la capa nucleó en una sola capa.

Capítulo 2

ETHERNET

2.1 Estándar IEEE 802.3.

El estándar para Ethernet es el 802.3 y opera en las dos capas inferiores del modelo OSI: la capa de enlace de datos en su subcapa MAC y la capa física.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC. El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

La subcapa MAC de Ethernet tiene dos responsabilidades principales:

- Encapsulamiento de datos: el cual proporciona tres funciones.
    - ❖ Delimitación de la trama
    - ❖ Direccionamiento
    - ❖ Detección de errores
- Control de acceso al medio.

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibirla. El proceso de encapsulación también posibilita el direccionamiento de la capa de Enlace de datos. Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.

Una función adicional de la encapsulación de datos es la detección de errores. Cada trama de Ethernet contiene un tráiler con una comprobación cíclica de redundancia (CRC) de los contenidos de la trama. Una vez que se recibe una trama, el nodo receptor crea una CRC para

compararla con la de la trama. Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

Por su parte el control de acceso al medio por medio de la subcapa MAC controla la colocación de tramas en los medios y el retiro de tramas de los medios. Como su nombre lo indica, se encarga de administrar el control de acceso al medio. Esto incluye el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones.

La topología lógica subyacente de Ethernet es un bus de multi acceso. Esto significa que todos los host (dispositivos) en ese segmento de la red comparten el medio. Esto significa además que todos los nodos de ese segmento reciben todas las tramas transmitidas por cualquier nodo de dicho segmento.

Ethernet ofrece un método para determinar cómo comparten los host el acceso al medio. El método de control de acceso a los medios para Ethernet clásico es el Acceso múltiple con detección de portadora con detección de colisiónes (CSMA/CD).

La topología física de Ethernet es una topología en estrella utilizando hubs (Figura 2.1). Los hubs concentran las conexiones al tomar un grupo de host y permitir que la red los trate como una sola unidad. Cuando una trama llega a un puerto, la copia a los demás puertos para que todos los segmentos de la LAN reciban la trama.

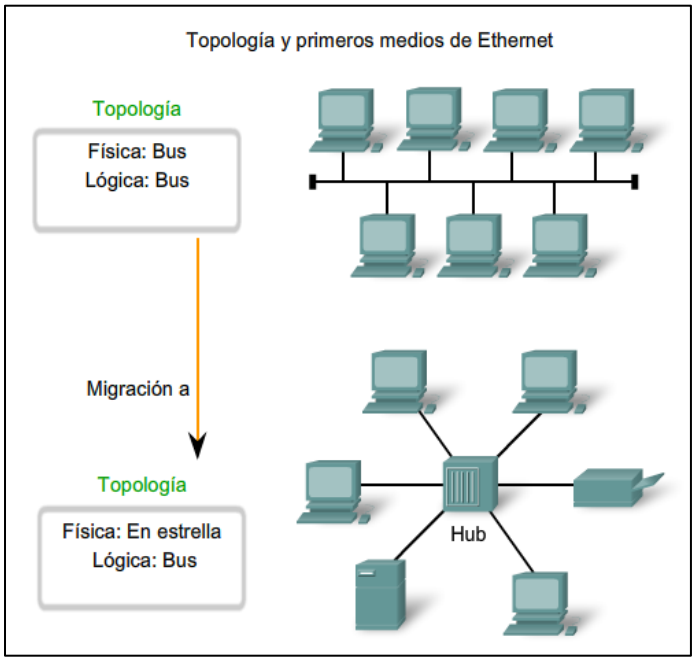


Figura 2.1 Topología Bus a Estrella

A medida que se agregaban más dispositivos a una red Ethernet, la cantidad de colisiones de tramas aumentaba notablemente. Durante los períodos de poca actividad de comunicación, las pocas colisiones que se producían se administraban mediante el CSMA/CD, con muy poco impacto en el rendimiento, en caso de que lo hubiera. Sin embargo, a medida que la cantidad de dispositivos y el consiguiente tráfico de datos aumentan, el incremento de las colisiones puede producir un impacto significativo en la experiencia del usuario.

Un desarrollo importante que mejoró el rendimiento de la LAN fue la introducción de los switches para reemplazar los hubs en redes basadas en Ethernet (Figura 2.2). Este desarrollo estaba estrechamente relacionado con el desarrollo de Ethernet 100BASE-TX. Los switches pueden controlar el flujo de datos mediante el aislamiento de cada uno de los puertos y el envío de una trama sólo al destino correspondiente (en caso de que lo conozca) en lugar del envío de todas las tramas a todos los dispositivos.

El switch reduce la cantidad de tramas que recibe cada host, lo que a su vez disminuye o minimiza la posibilidad de colisiones. Esto, junto con la posterior introducción de las comunicaciones full-duplex permitió el desarrollo de Ethernet de 1 Gbps.

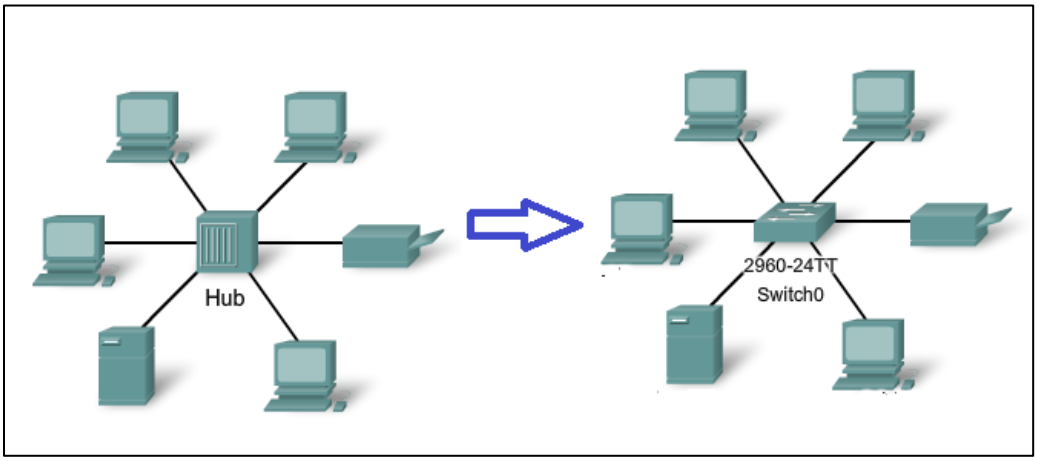


Figura 2.2 De Hub a Switch

2.2 Tramas de Ethernet.

Existen dos estilos de tramas de Ethernet: el IEEE 802.3 original y el IEEE 802.3 revisado (Ethernet II). Las diferencias entre los estilos de tramas son mínimas. La diferencia más significativa entre el IEEE 802.3 original y el IEEE 802.3 revisado es el agregado de un

delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud (Figura 2.3).

El estándar Ethernet original definió el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Esto incluye todos los bytes del campo Dirección MAC de destino a través del campo Secuencia de verificación de trama (FCS). Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama. El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN).

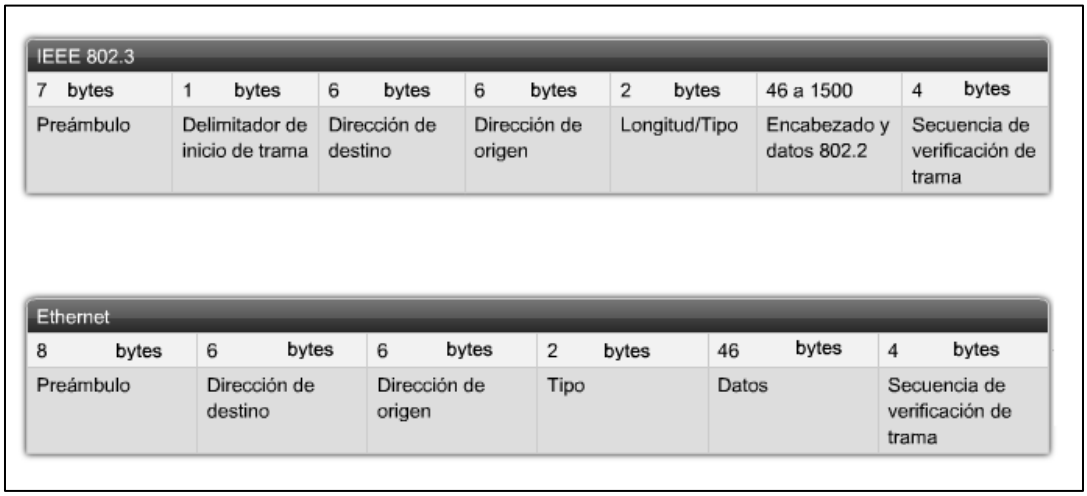


Figura 2.3 Tramas Ethernet y 802.3

El campo Dirección MAC de destino (6 bytes) es el identificador del receptor deseado. La Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama. El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz que origina la trama.

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo receptor recibe la trama y genera una CRC para detectar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama.

2.3 Direcciones MAC.

La dirección de Control de Acceso al Medio (MAC), fue creada para ayudar a determinar las direcciones de origen y destino dentro de una red Ethernet. Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales.

El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet. Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE, este le asigna a cada proveedor un código de 3 bytes, denominado Identificador Único Organizacional (OUI).

El IEEE obliga a los proveedores a que todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor en los 3 primeros bytes más el código del fabricante en los últimos 3 bytes (Figura 2.4).

La dirección MAC se encuentra grabada en la ROM (Memoria de sólo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente (el software no puede cambiarla). Sin embargo, cuando se inicia una PC la NIC copia la dirección a la RAM (Memoria de acceso aleatorio). Cuando se examinan tramas se utiliza la dirección que se encuentra en la RAM como dirección de origen para compararla con la dirección de destino.

Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers (cualquier dispositivo que pueda originar o recibir datos en la red).

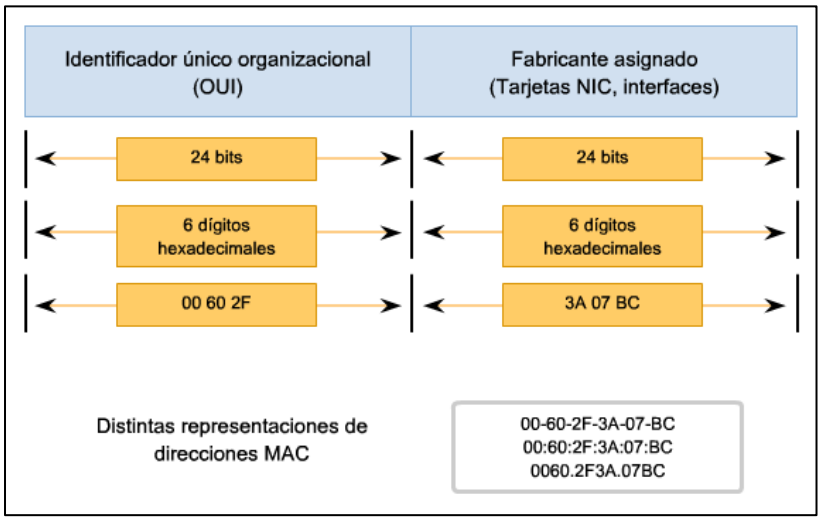


Figura 2.4 Estructura de la dirección MAC

2.4 Unicast.

Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único.

En el ejemplo que se muestra en la figura 2.5, un host con una dirección IP 192.168.1.5 (origen) solicita una página Web del servidor en la dirección IP 192.168.1.200.Para que se pueda enviar y recibir un paquete unicast, el encabezado del paquete IP debe contener una dirección IP de destino. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. La dirección IP y la dirección MAC se combinan para enviar datos a un host de destino específico.

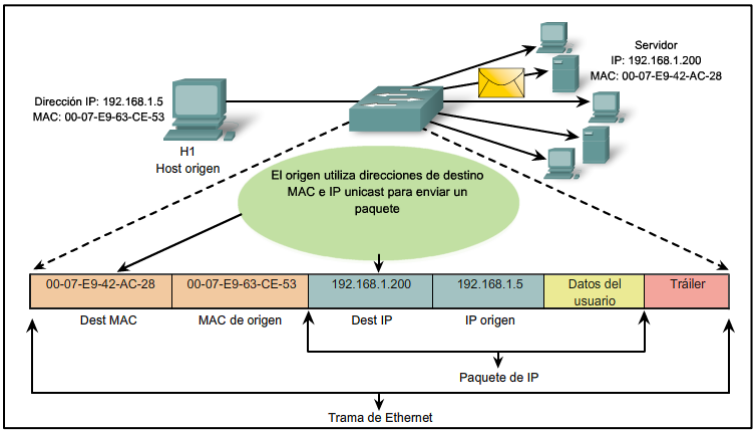


Figura 2.5 Unicast

2.5 Broadcast.

Con broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete. Una gran cantidad de protocolos de red utilizan broadcast, como el Protocolo de configuración dinámica de host (DHCP) y el Protocolo de resolución de direcciones (ARP).

Tal como se muestra en la figura 2.6, una dirección IP de broadcast para una red necesita una dirección MAC de broadcast correspondiente en la trama de Ethernet. En redes Ethernet, la dirección MAC de broadcast contiene 48 unos que se muestran como el hexadecimal FF-FF-FF-FF-FF-FF.

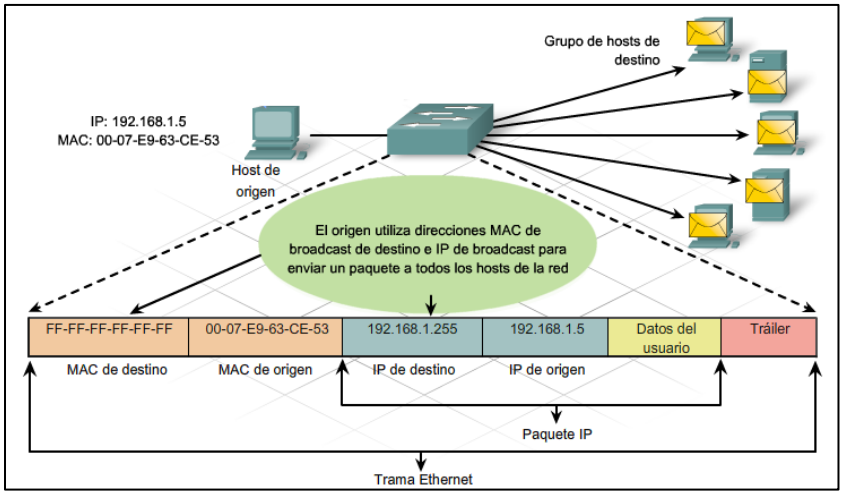


Figura 2.6 Broadcast

2.6 Multicast.

Las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. El intervalo de direcciones multicast es de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast (Figura 2.7).

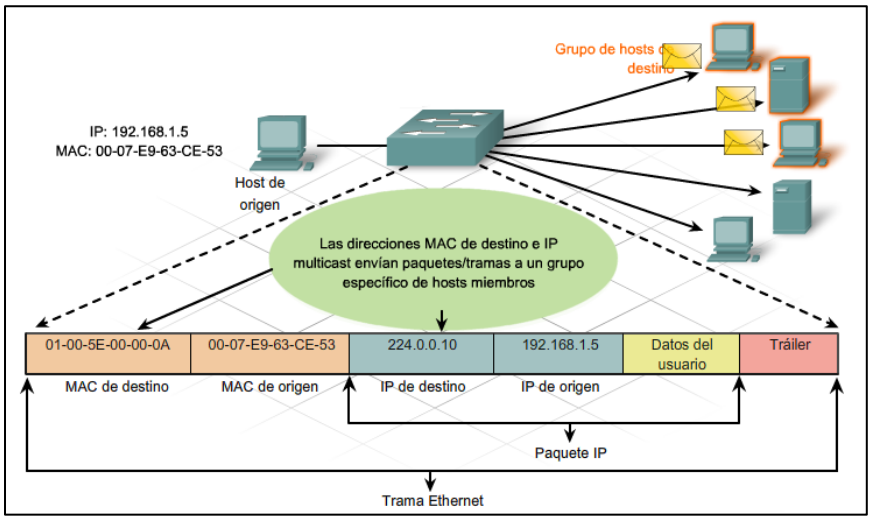


Figura 2.7 Multicast

2.7 Control De Acceso Al Medio.

En un entorno de medios compartidos, todos los dispositivos tienen acceso garantizado al medio, pero no tienen ninguna prioridad en dicho medio. Si más de un dispositivo realiza una transmisión simultáneamente, las señales físicas colisionan y la red debe recuperarse para que pueda continuar la comunicación.

Ethernet utiliza el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) para detectar y manejar colisiones y para administrar la reanudación de las comunicaciones.

Debido a que todas las computadoras que utilizan Ethernet envían sus mensajes en el mismo medio, se utiliza un esquema de coordinación distribuida (CSMA) para detectar la actividad eléctrica en el cable. Entonces, un dispositivo puede determinar cuándo puede transmitir. Cuando un dispositivo detecta que ninguna otra computadora está enviando una trama o una señal portadora, el dispositivo transmitirá en caso de que tenga algo para enviar.

Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión. Esta señal interferente se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que éstos invocarán un algoritmo de postergación. Este algoritmo de postergación hace que todos los dispositivos dejen de transmitir durante un período aleatorio, lo que permite que las señales de colisión disminuyan.

Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones. Un dominio de colisiones también se denomina segmento de red. Por lo tanto, los hubs y repetidores tienen el efecto de aumentar el tamaño del dominio de colisiones. Por lo tanto, se requiere de otros mecanismos cuando existen grandes cantidades de usuarios que quieren tener acceso y cuando se necesita un acceso a la red más activo los switches son la principal solución.

2.8 Tipos De Ethernet.

Las diferencias que existen entre Ethernet estándar, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet tienen lugar en la capa física. La figura 2.8 muestra algunas de las características de Ethernet.

Tipo de Ethernet	Ancho de banda	Tipo de cable	Duplex	Distancia máxima
10Base-5	10 Mbps	Coaxial thicknet	Half	500 m
10Base-2	10 Mbps	Coaxial thinnet	Half	185 m
100Base-TX	10 Mbps	UTP Cat3/Cat5	Half	100 m
100Base-TX	100 Mbps	UTP Cat5	Half	100 m
100Base-TX	200 Mbps	UTP Cat5	Full	100 m
100Base-TX	100 Mbps	Fibra multimodo	Half	400 m
1000Base-T	200 Mbps	Fibra multimodo	Full	2 km
1000Base-TX	1 Gbps	UTP Cat5e	Full	100 m
1000Base-SX	1 Gbps	UTP Cat6	Full	100 m
1000Base-LX	1 Gbps	Fibra multimodo	Full	550 m
10GBase-CX4	1 Gbps	Fibra monomodo	Full	2 km
10GBase-T	10 Gbps	Twinaxial	Full	100 m
10GBase-LX4	10 Gbps	UTP Cat6a/Cat7	Full	100 m
10GBase-LX4	10 Gbps	Fibra multimodo	Full	300 m
10 Mbps	10 Gbps	Fibra monomodo	Full	10 km

Figura 2.8 Tipos De Ethernet

Capítulo 3

SWITCHEO

3.1 Switches LAN Ethernet.

Los switches son una parte fundamental de la mayoría de las redes. Los switches permiten la segmentación de la LAN en distintos dominios de colisiones. Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto (Figura 3.1).

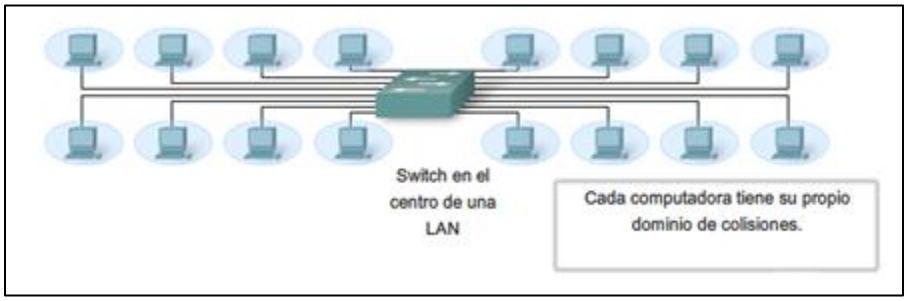


Figura 3.1 Switch

Cada nodo dispone del ancho de banda de los medios completo en la conexión entre el nodo y el switch. Ejemplo si se tiene un switch con 10 nodos, todos tienen el ancho de banda completo de 100 Mbps disponible.

Una conexión punto a punto dedicada a un switch también evita contenciones de medios entre dispositivos, lo que elimina las colisiones (Figura 3.2).

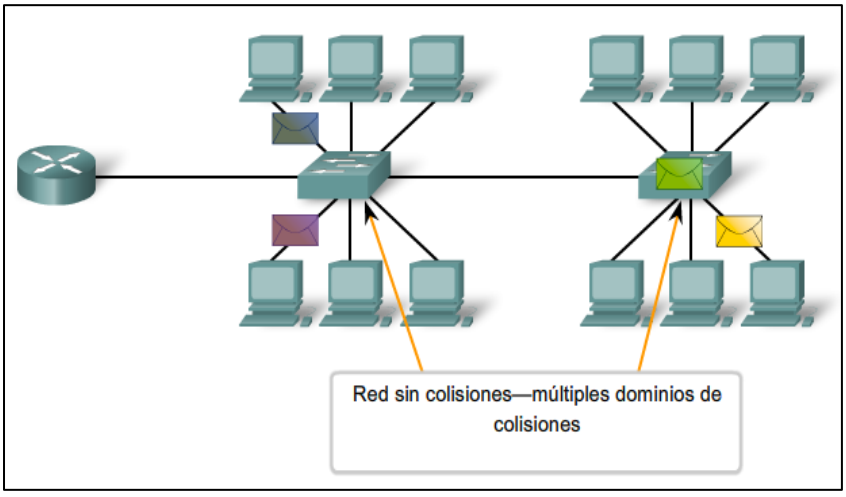


Figura 3.2 Switch Sin Colisiones

3.1.1 Densidad de puerto.

En un switch para las capas de acceso, de distribución y núcleo, se debe considerar la capacidad del switch para admitir los requerimientos de densidad de puerto, tasas de reenvió y agregado de ancho de banda de la red.

La densidad de puerto es el número de puertos disponibles en un switch único. Los switches de configuración fija habitualmente admiten hasta 48 puertos en un único dispositivo. Los switches modulares pueden admitir densidades de puerto muy altas mediante el agregado de tarjetas de línea de puerto de switch múltiples (Figura 3.3).

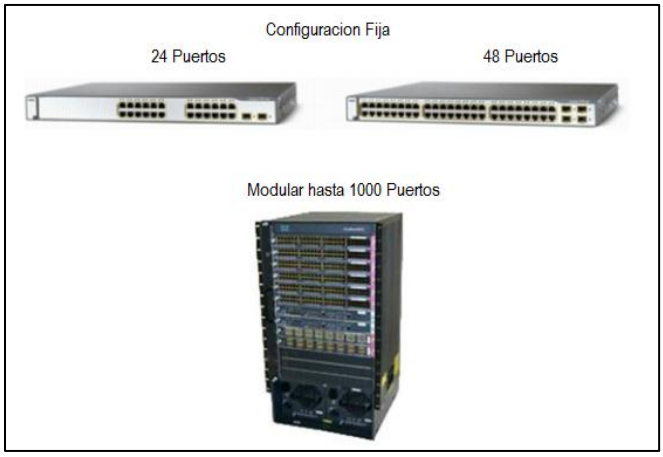


Figura 3.3 Densidad De Puertos

3.1.2 Interfaz De línea De Comandos (CLI).

La interfaz de comandos de un switch permite introducir las sentencias de configuración para la administración de seguridad, creación redes LAN virtuales, administración a distancia y todas la configuraciones que llegue a requerir el switch para un óptimo funcionamiento.

Una vez terminado el proceso de arranque del switch, se tiene acceso a la CLI en su condición de EXEC, donde, se puede comenzar con las configuraciones del switch.

Como característica de seguridad, el software IOS de Cisco divide las sesiones de EXEC en los siguientes niveles de acceso:

- EXEC usuario: Permite que una persona tenga acceso solamente a una cantidad limitada de comandos básicos de monitoreo. El modo EXEC del usuario es el modo

predeterminado al que se ingresa después de iniciar sesión en un switch desde la CLI. El modo EXEC del usuario se identifica con la indicación >.

- EXEC privilegiado: Permite que una persona tenga acceso a todos los comandos del dispositivo, como aquellos que se utilizan para la configuración y administración, y es posible protegerlo por contraseña para que tengan acceso al dispositivo sólo los usuarios autorizados. El modo EXEC privilegiado se identifica con la indicación #.

Para pasar del modo EXEC de usuario al modo EXEC privilegiado, se debe ingresar el comando *enable*. Y para pasar del modo EXEC privilegiado al modo de configuración global, se debe ingresar el comando *configure terminal*.

Cuando se realiza una configuración en el switch esta se guarda en la DRAM y la configuración de inicio se almacena en la sección NVRAM de la memoria Flash. Al introducir el comando *copy running-config startup-config*, el software IOS de Cisco copia la configuración en ejecución en la NVRAM, de modo que cuando el switch arranque, la configuración de inicio se cargue con la nueva configuración (Figura 3.4).

Sintaxis del comando de CLI IOS de Cisco	
Versión formal del comando copy de IOS de Cisco. Confirmar el nombre de archivo de destino. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy system:running-config flash:startup-config** Destination filename [startup-config]?
Versión informal del comando copy. Se supone que running-config se está ejecutando en el sistema y que el archivo startup-config se almacenará en NVRAM flash. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy running-config startup-config** Destination filename [startup-config]?
Hacer una copia de respaldo de startup-config en un archivo almacenado en NVRAM flash. Confirmar el nombre de archivo de destino. Presionar la tecla Enter para aceptar y usar la combinación de teclas Crtl+C para cancelar.	S1#**copy startup-config flash:config.bak1** Destination filename [config.bak1]?

Figura 3.4 Comandos Copy

El puerto consola de los dispositivos de red provee el acceso físico a la interfaz lógica del dispositivo. Como parte de la seguridad de la red esta terminal debe estar protegida por una

contraseña para evitar el acceso no autorizado. En la figura 3.5 se muestran los comandos para configurar la contraseña de la terminal.

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1#**configure terminal**
Cambio del modo de configuración global a modo de configuración de línea para la consola 0.	S1(config)#**line con 0**
Establece **cisco** como contraseña para la línea de la consola 0 del switch.	S1(config-line)#**password cisco**
Establece la línea de consola para que solicite el ingreso de la contraseña antes de conceder el acceso.	S1(config-line)#**login**
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	S1(config-line)#**end**

Figura 3.5 Contraseña Puerto Consola

Los puertos vty de un switch permiten obtener acceso remoto al dispositivo. Es posible llevar a cabo todas las opciones de configuración mediante los puertos de terminal vty. No se necesita acceso físico al switch para obtener acceso a los puertos vty. Por ello, es muy importante que estén protegidos. Cualquier usuario con acceso de red al switch puede establecer una conexión remota de terminal vty. Si no se aseguran los puertos vty en forma adecuada, usuarios malintencionados podrían comprometer la configuración del switch (Figura 3.6).

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	S1#**configure terminal**
Cambio del modo de configuración global a modo de configuración de línea para la consola 0.	S1(config)#**line vty 0 4**
Establece **cisco** como contraseña para la línea de la consola 0 del switch.	S1(config-line)#**password cisco**
Establece la línea de consola para que solicite el ingreso de la contraseña antes de conceder el acceso.	S1(config-line)#**login**
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	S1(config-line)#**end**

Figura 3.6 Contraseña VTY

Proteger el modo EXEC privilegiado es importante dado que es donde se introducen los comandos de configuración global del switch. El comando de configuración global *enable*

password permite especificar una contraseña para restringir el acceso al modo EXEC privilegiado (Figura 3.7).

Sintaxis del comando de CLI IOS de Cisco	
Cambio de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Configura la **contraseña de habilitación** para ingresar al modo EXEC privilegiado.	`S1(config)#enable password password`
Configura la **contraseña de habilitación** secreta para ingresar al modo EXEC privilegiado.	`S1(config)#enable secret password`
Sale del modo de configuración de línea y vuelve al modo EXEC privilegiado.	`S1(config)#end`

Figura 3.7 Contraseña EXEC Privilegiado

3.1.3 Seguridad en el Switch.

Un switch que no cuenta con seguridad de puerto permite que un atacante se conecte al switch por un puerto habilitado en desuso, que recopile información o que genere ataques. Un switch puede configurarse para actuar como un hub, lo que significa que todos los sistemas conectados al switch pueden ver de manera potencial todo el tráfico de la red que pasa a través de él y llega a todos los sistemas conectados a él. Además, un atacante puede recopilar tráfico que contiene nombres de usuario, contraseñas o información de configuración acerca de los sistemas de la red.

La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Cuando se asignan direcciones MAC seguras a un puerto seguro, el puerto no envía paquetes con direcciones origen que se encuentren fuera del grupo de direcciones definidas.

Existen varias formas de configurar la seguridad de puerto:

- Direcciones MAC seguras estáticas: Las direcciones MAC se configuran manualmente mediante el comando de configuración de interfaz *switchport port-security mac-address*. Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch.

- Direcciones MAC seguras dinámicas: Las direcciones MAC se aprenden de manera dinámica y se almacenan sólo en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia.

- Direcciones MAC seguras sin modificación: Se puede configurar un puerto para que aprenda de manera dinámica las direcciones MAC y luego guardarlas en la configuración en ejecución.

Las direcciones MAC seguras sin modificación poseen las siguientes características:

- Cuando se habilita el aprendizaje sin modificación en una interfaz mediante el comando de configuración de interfaz *switchport port-security mac-address sticky*, la interfaz convierte todas las direcciones MAC seguras dinámicas, incluyendo aquellas que se aprendieron de manera dinámica antes de habilitar el aprendizaje sin modificación.

- Cuando se configuran direcciones MAC seguras sin modificación mediante el comando de configuración de interfaz *switchport port-security mac-address sticky mac-address*, éstas se agregan a la tabla de direcciones y a la configuración en ejecución. Si se deshabilita la seguridad de puerto, las direcciones MAC seguras sin modificación permanecen en la configuración en ejecución.

- Si se guardan las direcciones MAC seguras sin modificación en el archivo de configuración, cuando se reinicia el switch o cuando se cierra la interfaz, esta última no necesita volver a aprender estas direcciones. Si no se guardan las direcciones seguras sin modificación, éstas se pierden.

Se puede configurar la interfaz para uno de tres modos de violación, en base a la acción a tomar en caso de que se produzca dicha violación.

- Protección.
- Restricción.
- Desactivación.

La figura 3.8 muestra la forma de habilitar la seguridad de puerto sin modificación en el puerto Fast Ethernet 0/18 del switch S1. Como se mencionó con anterioridad.

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global. Use este comando del IOS de Cisco:	S1#**configure terminal**
Especificar el tipo y número de interfaz física a configurar. Use este comando del IOS de Cisco:	S1(config)#**interface fastEthernet 0/18**
Establecer el modo de interfaz como acceso. Use este comando del IOS de Cisco:	S1(config-if)#**switchport mode access**
Activar la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security**
Establecer el número máximo de direcciones seguras en 50. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security maximum 50**
Activar el aprendizaje sin modificaciones. Use este comando del IOS de Cisco:	S1(config-if)#**switchport port-security mac-address sticky**
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	S1**(config-if)#end**

Figura 3.8 Seguridad De Puerto Sin Modificación

3.2 VLAN.

Una LAN Virtual (VLAN) permite crear grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Cuando se configura una VLAN, se le asigna un nombre para describir la función principal de los usuarios de esa VLAN. Estas VLAN permiten implementar las políticas de acceso y seguridad para grupos particulares de usuarios.

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLAN y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso. Si dos computadoras están conectadas físicamente en el mismo switch no significa que se puedan comunicar. Los dispositivos en dos redes y subredes separadas se deben comunicar a través de un router (Capa 3).

Los principales beneficios de utilizar las VLAN son los siguientes:

- Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- Reducción de costo: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.
- Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.
- Mitigación de la tormenta de broadcast: la división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast. La segmentación de LAN impide que el broadcast se propague a toda la red.
- Administración de aplicación o de proyectos más simples: las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea más fácil. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.

El acceso a las VLAN está dividido en un rango normal o un rango extendido.

- VLAN de rango normal
    - ❖ Se utiliza en redes de pequeños y medianos negocios y empresas.
    - ❖ Se identifica mediante un ID de VLAN entre 1 y 1005.
    - ❖ Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
    - ❖ Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.
    - ❖ El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN.
- VLAN de rango extendido
    - ❖ Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo

suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.

- Se identifican mediante un ID de VLAN entre 1006 y 4094.
- Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan en el archivo de configuración en ejecución.
- VTP no aprende las VLAN de rango extendido.

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. La VLAN predeterminada para los switches de Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se puede volver a denominar y no se puede eliminar. El tráfico de control de Capa 2 se asociará siempre con la VLAN 1.

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). Una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal. Es una optimización de seguridad usar una VLAN diferente de la VLAN 1 como la VLAN nativa.

La figura 3.9 revisa los comandos IOS de Cisco utilizados para agregar una VLAN a un switch.

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	`S1(config)#vlan vlan id`
(Opcional) Especificar un único nombre de VLAN para identificar la misma. Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	`S1(config-vlan)#name Nombre de VLAN`
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo vlan.dat y para que la configuración entre en vigencia.	`S1(config-vlan)#end`

Figura 3.9 Configuraciones VLAN

Después de crear una VLAN, se le debe asignar un puerto o más. Cuando se asigna un puerto de switch a una VLAN en forma manual, se lo conoce como puerto de acceso estático. Un puerto de acceso estático puede pertenecer a sólo una VLAN por vez.

En la figura 3.10 se muestran los comandos del IOS para asignar un puerto a una VLAN

Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	`S1#configure terminal`
Ingresar la interfaz para asignar la VLAN.	`S1(config)#interface` *interface id*
Definir el modo de asociación de VLAN para el puerto.	`S1(config-if)#switchport mode access`
Asignar el puerto a una VLAN.	`S1(config-if)#switchport access vlan` *vlan id*
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Figura 3.10 Asignar Un Puerto A Una VLAN

Para verificar que las VLAN se crearon de forma correcta así como los puertos asociados a estas se utiliza el comando *show vlan brief*, el cual muestra los contenidos del archivo vlan.dat.

3.2.1 Dominio De Broadcast.

En funcionamiento normal, cuando un switch recibe una trama de broadcast en uno de sus puertos, envía la trama a todos los demás puertos. En la figura 3.11, toda la red está configurada en la misma subred, 172.17.40.0/24. Como resultado, cuando la computadora del cuerpo docente, PC1, envía una trama de broadcast, el switch S2 envía esa trama de broadcast a todos sus puertos. La red completa la recibe finalmente; la red es un dominio de broadcast.

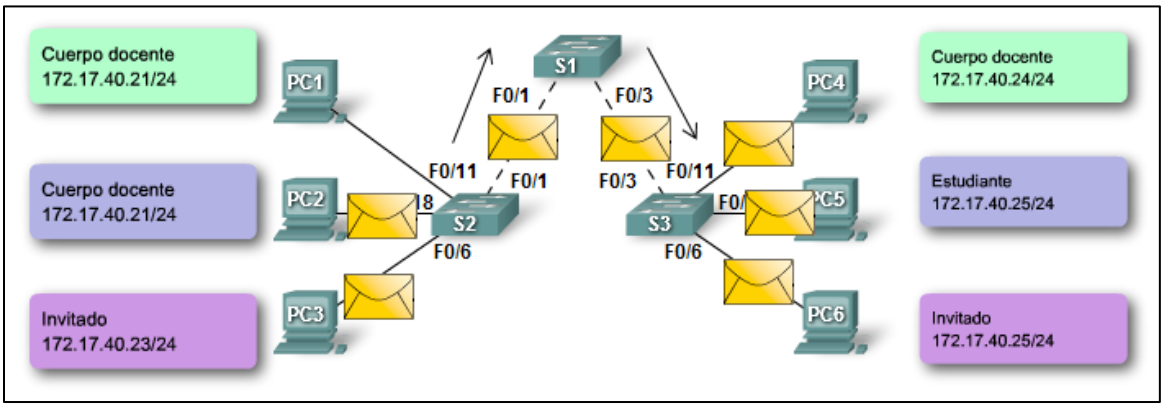


Figura 3.11 Dominio De Broadcast

En la figura 3.12, se dividió la red en dos VLAN: Cuerpo docente como VLAN 10 y Estudiante como VLAN 20. Cuando se envía la trama de broadcast desde la computadora del cuerpo docente, PC1, al switch S2, el switch envía esa trama de broadcast sólo a los puertos de switch configurados para admitir VLAN 10. Los puertos que componen la conexión entre los switches S2 y S1 (puertos F0/1) y entre S1 y S3 (puertos F0/3) han sido configurados para admitir todas las VLAN en la red. Esta conexión se denomina enlace troncal.

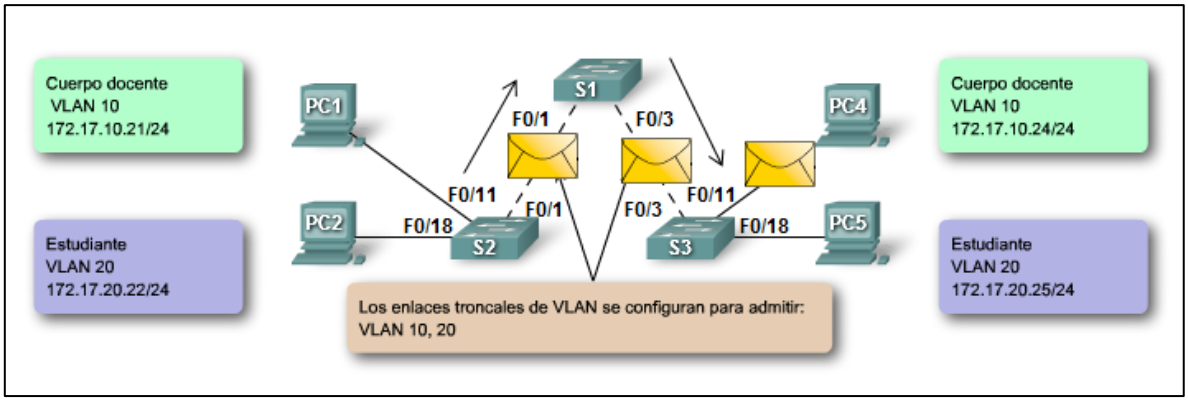


Figura 3.12 División Del Dominio De Broadcast

La fragmentación de un gran dominio de broadcast en varias partes más pequeñas reduce el tráfico de broadcast y mejora el rendimiento de la red. La fragmentación de dominios en VLAN permite además una mejor confidencialidad de información dentro de una organización. La fragmentación de dominios de broadcast puede realizarse con las VLAN (en los switches) o con routers. Cada vez que dispositivos en diferentes redes de Capa 3 necesiten comunicarse, es necesario un router sin tener en cuenta si las VLAN están en uso.

3.2.2 Troncales.

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN permite extender las VLAN a través de toda una red.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

Los switches de capa 2 solo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que indique a qué

VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama de Ethernet original y específica la VLAN a la que pertenece la trama.

El campo de etiqueta de la VLAN consiste de un campo EtherType, un campo de información de control de etiqueta y del campo de FCS (Figura 3.13).

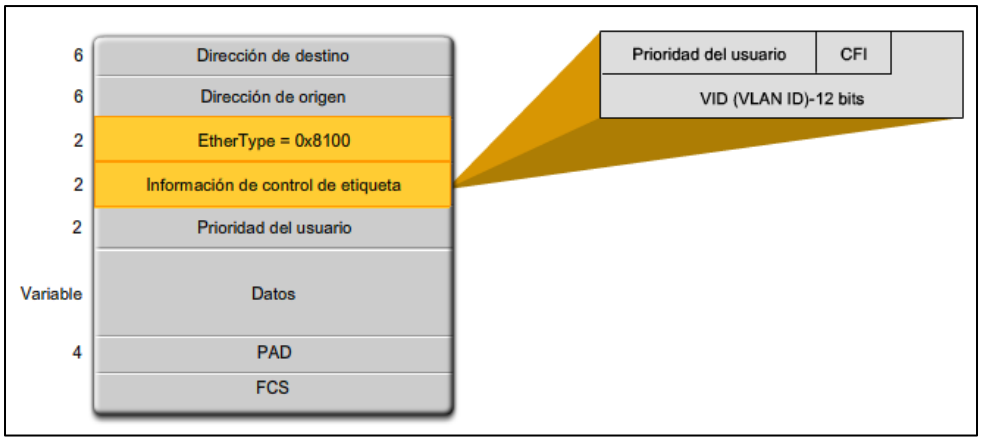


Figura 3.13 Encabezado de Encapsulación 802.1Q

En la Figura 3.14 se muestran las configuraciones para habilitar un puerto como troncal.

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global en el switch S1.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz.	`S1(config)#interface F0/1`
Definir la interfaz F0/1 como un enlace troncal IEEE 802.1Q.	`S1(config-if)#switchport mode trunk`
Configurar la VLAN 99 para que sea la VLAN nativa.	`S1(config-if)#switchport trunk native vlan 99`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Figura 3.14 Configurar Puerto Troncal

Para verificar los enlaces troncales de un switch se utiliza el comando *show interfaces trunk.*

3.2.3 VTP (VLAN Trunking Protocol).

El VTP permite configurar un switch de modo que propagué las configuraciones de una VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID

de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP.

VTP minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. VTP permite separar una red en dominios de administración más pequeños para reducir la administración de las VLAN. Un beneficio adicional de configurar los dominios del VTP es que limita hasta qué punto se propagan los cambios de configuración en la red si se produce un error (Figura 3.15).

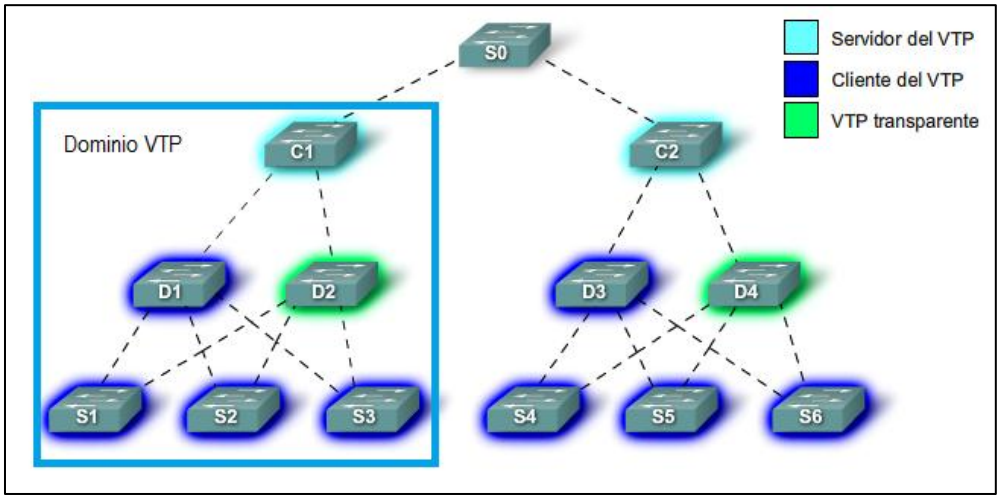


Figura 3.15 VTP

Capítulo 4

“Configuración Del Crecimiento De La Red De Datos De La Empresa OMEGA”

4.1 Estado Actual.

Este proyecto surge de la ampliación de la red de la empresa OMEGA, concretamente la sección de administración de la nueva sucursal de puebla, donde, desde la ciudad de México en el edificio matriz se da soporte para el área de distribución y ventas.

Esta nueva red del edificio matriz se encuentra dividida en 7 subredes una para cada departamento laboral, los cuales son:

- Departamento de Ventas
- Departamento de Distribución
- Departamento de Gerencia
- Departamento de Recursos Humanos
- Área para Visitantes
- Sala de Juntas

La nueva red consta de 80 host distribuidos en 4 switches de acceso cisco catalyst 2960 de 24 puertos cada uno, ubicados en el IDF del 5° piso.

La tabla 4.1 muestra las direcciones IP de subred de cada uno de los departamentos laborales.

Subred/Departamento	No. Host	192.168.0.0/24	Host	Broadcast y Mascara de subred
Ventas	30	192.168.0.0/26	.1 - .62	.63 Broadcast 255.255.255.192
Distribución	25	192.168.0.64/27	.65 - .94	.95 Broadcast 255.255.255.224
Visitantes	10	192.168.0.96/28	.97 - .110	.111 Broadcast 255.255.255.240
Gerencia	5	192.168.0.112/28	.113 - .126	.127 Broadcast 255.255.255.240
RH	3	192.168.0.136/29	.137 - .142	.143 Broadcast 255.255.255.248
Juntas	3	192.168.0.144/29	.145 - .150	.151 Broadcast 255.255.255.248

Tabla 4.1 Subredes IP

Los 80 host están distribuidos en los 4 switches de acceso como se muestra en la tabla 4.2

Switch	Cantidad de Host
Acceso1	10 Ventas, 10 Distribución
Acceso2	10 Ventas, 5 Distribución, 5 Gerencia
Acceso3	10 Ventas, 10 Visitantes
Acceso4	10 Distribución, 3 RH, 3 Juntas, 4 Libres

Tabla 4.2 Distribución de Host

En la tabla 4.3 se muestra la distribución física de los host en los puertos con su respectiva dirección IP.

Puerto	Acceso1	Acceso2	Acceso3	Acceso4
1	192.168.0.1	192.168.0.11	192.168.0.21	192.168.0.80
2	192.168.0.2	192.168.0.12	192.168.0.22	192.168.0.81
3	192.168.0.3	192.168.0.13	192.168.0.23	192.168.0.82
4	192.168.0.4	192.168.0.14	192.168.0.24	192.168.0.83
5	192.168.0.5	192.168.0.15	192.168.0.25	192.168.0.84
6	192.168.0.6	192.168.0.16	192.168.0.26	192.168.0.85
7	192.168.0.7	192.168.0.17	192.168.0.27	192.168.0.86
8	192.168.0.8	192.168.0.18	192.168.0.28	192.168.0.87
9	192.168.0.9	192.168.0.19	192.168.0.29	192.168.0.88
10	192.168.0.10	192.168.0.20	192.168.0.30	192.168.0.89
11	192.168.0.65	192.168.0.75	192.168.0.97	192.168.0.137
12	192.168.0.66	192.168.0.76	192.168.0.98	192.168.0.138
13	192.168.0.67	192.168.0.77	192.168.0.99	192.168.0.139
14	192.168.0.68	192.168.0.78	192.168.0.100	192.168.0.145
15	192.168.0.69	192.168.0.79	192.168.0.101	192.168.0.146
16	192.168.0.70	192.168.0.113	192.168.0.102	192.168.0.147
17	192.168.0.71	192.168.0.114	192.168.0.103	
18	192.168.0.72	192.168.0.115	192.168.0.104	
19	192.168.0.73	192.168.0.116	192.168.0.105	
20	192.168.0.74	192.168.0.117	192.168.0.106	

Tabla 4.3 Distribución en puertos

Todo lo anterior provoca un buen funcionamiento de la red, sin embargo, la seguridad es totalmente deficiente desde los usuarios hasta los dispositivos. Esto es porque los switches no presentan ninguna configuración de seguridad para el acceso y el tráfico generado por los usuarios de la red provoca dominio de broadcast, lo cual produce un aumento en el consumo

de ancho de banda de los enlaces, así como la posibilidad de que los datos generados por un departamento laboral pueda ser capturado por otro usuario de otro departamento laboral.

En la Figura del anexo 1 se muestra el dominio de broadcast que provoca la actual configuración de la red con la ayuda del programa de simulación Packet Tracer™ de CISCO Systems Inc. Este broadcast provoca un consumo de ancho de banda y la posibilidad de que otro usuario capture ese tráfico y pudiera robar información, todo esto a pesar de ser un ping fallido debido a que las PC pertenecen a diferentes subredes, sin embargo, el mismo problema se presenta si las PC implicadas pertenecieran a la misma subred.

Otro de los factores de riesgo que presenta esta red es con respecto a los servidores de trabajo para los departamentos de ventas y distribución, ya que el tráfico generado por los usuarios de los demás departamentos podría llegar a conectarse a dichos servidores.

Los departamentos que presentan mayor sensibilidad son Gerencia y Visitantes. El departamento de gerencia alberga a los jefes de secciones y los datos generados no deben de poder ser interceptados por otros departamentos. El área de visitantes es un área destinada para personal de otras compañías que por motivos comerciales visiten la compañía OMEGA y requieran conexión de red, por lo tanto, esta área no representa relación directa con la compañía OMEGA, por ende el tráfico generado de visitas no puede llegar a interceptar tráfico de los departamentos de ventas, gerencia y distribución.

Los switches utilizados en la red presentan falta de seguridad en el acceso y sus puertos, de esta forma cualquier usuario de la red podría llegar a tener acceso remoto a ellos, además la falta de seguridad de los puertos podría llegar a presentar un riesgo en la seguridad de la red, en el anexo 1 se puede apreciar que los switches no cuentan con contraseñas de las terminales virtuales vty, la terminal de consola y el modo EXEC Privilegiado del CLI y los puertos no tienen habilitada su función de seguridad de direcciones MAC. **(Ver anexo 1)**

4.2 Propuesta.

Para solucionar la problemática presentada se propone la creación de las VLAN necesarias para cubrir las subredes existentes más una VLAN de administración y nativa, así como habilitar las contraseñas en los switches y la seguridad de los puertos.

Se propone la creación de 7 VLAN nombradas de acuerdo al departamento laboral a la cual pertenecerá, la numeración de las VLAN será del número 2 al número 8 (Tabla 4.4).

Departamento	VLAN
Ventas	2
Distribución	3
Visitantes	4
Gerencia	5
RH	6
Juntas	7
Admin&Native	8

Tabla 4.4 VLAN Propuestas

Los servidores de trabajo pertenecerán a sus respectivas VLAN. La distribución de las VLAN en los puertos de los switches de acceso se presenta en la tabla 4.5.

Puerto	Acceso1	Acceso2	Acceso3	Acceso4
1	Ventas	Ventas	Ventas	Distribución
2	Ventas	Ventas	Ventas	Distribución
3	Ventas	Ventas	Ventas	Distribución
4	Ventas	Ventas	Ventas	Distribución
5	Ventas	Ventas	Ventas	Distribución
6	Ventas	Ventas	Ventas	Distribución
7	Ventas	Ventas	Ventas	Distribución
8	Ventas	Ventas	Ventas	Distribución
9	Ventas	Ventas	Ventas	Distribución
10	Ventas	Ventas	Ventas	Distribución
11	Distribución	Distribución	Visitantes	RH
12	Distribución	Distribución	Visitantes	RH
13	Distribución	Distribución	Visitantes	RH
14	Distribución	Distribución	Visitantes	Juntas
15	Distribución	Distribución	Visitantes	Juntas

16	Distribución	Gerencia	Visitantes	Juntas
17	Distribución	Gerencia	Visitantes	Libre
18	Distribución	Gerencia	Visitantes	Libre
19	Distribución	Gerencia	Visitantes	Libre
20	Distribución	Gerencia	Visitantes	Libre

Tabla 4.5 Distribución en puertos VLAN

Al crear las VLAN es necesario que los enlaces entre los switches de acceso y el switch de distribución sean habilitados como troncales. En la tabla 4.6 se presenta el número de puerto que será habilitado como troncal en cada uno de los switches.

Switch	Puertos Troncales	Conexión Hacia
Acceso1	24 y 23	Distribución y Acceso2
Acceso2	24 y 23	Acceso1 y Acceso3
Acceso3	23 y 24	Acceso2 y Acceso4
Acceso4	23 y 24	Acceso3 y Distribución

Tabla 4.6 Puertos Troncales

Para configurar el VTP para la administración de las VLAN se proponen los siguientes valores:

- Dominio - AdministradoresPuebla
- Contraseña - vlanomega

El VTP server será el switch de distribución y los VTP clients los 4 switches de acceso. Otra medida de seguridad propuesta es cambiar la VLAN nativa de la 1 a la 8.

En materia de la seguridad de los switches, en la tabla 4.7 se muestran las contraseñas propuestas para su configuración.

Terminal	Password
Consola	Omega
VTY 0 4	Omega
EXEC Privilegiado	Omega

Tabla 4.7 Contraseñas

Para la seguridad de los puertos de los switches se propone una configuración de Direcciones MAC seguras sin modificación de máximo 2 direcciones MAC por puerto y para los

puertos correspondientes a la VLAN Visitas una configuración de Direcciones MAC seguras dinámicas máximo de 1 dirección MAC y en caso de violación, la acción del puerto será la desactivación.

4.3 Desarrollo.

El primer paso a realizar es la configuración de las contraseñas en los switches de la red de acuerdo con la tabla 4.7, mediante los siguientes comandos. **(Ver Anexo 2)**

Distribucion>enable /Nos permite entrar a la configuración en modo EXEC privilegiado.
Distribucion#configure terminal /Nos permite ingresar al modo de configuración global.
Distribucion (config)#enable secret omega /Se establece la contraseña para el EXEC privilegiado.
Distribucion (config-line)#line vty 0 4 /Líneas de acceso remoto disponibles.
Distribucion (config-line)#pass omega /Ingreso de password.
Distribucion (config-line)#login /Solicita el ingreso de la contraseña antes de conceder el acceso.
Distribucion (config-line)#exit /Salir de la configuración.
Distribucion (config)#service password-encryption /Encriptado de las contraseñas
Distribucion (config)#end

El segundo paso es la configuración del VTP en los 5 switches de acuerdo con el dominio y las contraseñas propuestas en el cual utilizamos los siguientes comandos.

Distribucion (config)#vtp mode server /Configura el modo VTP que trabajara en el switch como servidor.
Distribucion (config)#vtp domain AdministradoresPuebla /Establece el nombre del dominio.
Distribucion (config)#vtp password vlanomega /Aplica una contraseña al dominio.

El tercer paso es configurar los enlaces troncales como tal como se propuso en la tabla 4.6, los comandos son como sigue. **(Ver Anexo 3)**

Distribucion (config)#interface range fa0/1 – 2 /Aplica en la interfaz fast Ethernet 1-2
Distribucion (config-if-range)#switchport mode trunk /Habilita el puerto como enlace troncal 802.1Q
Distribucion (config-if-range)#switchport trunk native vlan 8 /Realiza el cambio de la VLAN nativa a la VLAN 8

El cuarto paso es declarar las VLAN en el VTP Server tal como se propuso en la tabla 4.4 con los comandos siguientes. **(Ver Anexo 4)**

Distribucion (config)#vlan 2 /Creación de la VLAN
Distribucion (config-vlan)#name Ventas /nombre de la VLAN.

El quinto paso es asignar los puertos de los switches de acceso a su respectiva VLAN de acuerdo a la tabla 4.5 en el cual utilizamos los comandos siguientes. **(Ver Anexo 5)**

Acceso1 (config)#interface range fa0/1 – 10 /Prepara la interfaz disponible
Acceso1 (config-if-range)#switchport mode Access /Pone en modo acceso al puerto del switch.
Acceso1 (config-if-range)#switchport access vlan 2 /Asigna el Puerto a la VLAN correspondiente
Acceso1 (config-if-range)#no shutdown /Levanta o pone en funcionamiento la interfaz.

El sexto paso es habilitar la seguridad de los puertos tal como se propuso con un máximo de 2 direcciones MAC y para los puertos correspondientes a la VLAN Visitas máximo de 1 dirección, así como la desactivación en caso de violación. **(Ver Anexo 6)**

Acceso1 (config-if-range)#switchport port-security /Habilita la seguridad de puerto
Acceso1 (config-if-range)#switchport port-security maximum 2 /Indica que seran max. 2 direcciones MAC
Acceso1 (config-if-range)#switchport port-security mac-address sticky /Configura la seguridad de puerto en Direcciones MAC seguras sin modificación
Acceso1 (config-if-range)#switchport port-security violation shutdown /Indica la desactivación en caso de violación.

4.4 Pruebas.

La primera prueba consiste en verificar la correcta función de las contraseñas configuradas mediante el comando IOS *show running config.* En la Figura del anexo 2 se muestra el resultado para el switch Acceso1, siendo el mismo resultado para todos los demás switches.

La segunda prueba es la comprobación de los enlaces troncales y el cambio de la VLAN Nativa a la VLAN 8 mediante el comando IOS *show interfaces trunk.* El anexo 3 muestra el resultado para el switch Acceso2, siendo el mismo resultado para todos los demás switches.

La tercera prueba a realizar es la confirmación de la creación de las VLAN por medio del VTP y la correcta asignación de los puertos a su respectiva VLAN mediante el comando de IOS *show vlan brief.* En la figura del anexo 5 se muestra el resultado para el switch Acceso3, teniendo un resultado exitoso en todos los demás switches.

La cuarta prueba es confirmar la correcta habilitación de la seguridad en los puertos de los switches mediante el comando *show running config*. El anexo 6 muestra el resultado para el switch Acceso4, teniendo el mismo resultado exitoso en los demás switches.

4.5 Resultados.

Con base a las pruebas realizadas de la nueva configuración se puede establecer un nuevo funcionamiento de la red con un mayor nivel de seguridad.

La creación de las VLAN provoca una segmentación del dominio de broadcast, lo que produce una reducción en el consumo de ancho de banda y disminuye la posibilidad de que otro usuario que no pertenezca a la misma VLAN capture tráfico de datos y pudiera robar información, ya que ahora el broadcast solo tiene lugar en las PC que pertenezcan a la misma VLAN.

Como parte de los resultados exitosos de la nueva configuración de la red se puntualiza que el acceso a los servidores ahora es más seguro ya que solo los usuarios de las VLAN de Ventas y Distribución pueden tener acceso a sus respectivos servidores. **(Ver anexo7)**

4.6 Conclusiones.

Con base a las pruebas y resultados se puede concluir que el nivel de la seguridad de la red aumentó considerablemente. Ahora existe un mayor control de los datos generados por un usuario, de tal forma que los datos ya no podrían ser interceptados tan fácilmente por otros usuarios ajenos tanto a la red, como a los departamentos laborales.

Las VLAN son una herramienta de seguridad lógica presente en la gran mayoría de las redes en el mundo gracias a su fácil implementación y administración. Esta herramienta debe de ir de la mano de una adecuada planeación que permita delimitar claramente las zonas, subredes y departamentos laborales que deban estar debidamente delimitados y cuyos datos generados contengan información crítica tanto para la empresa como para el usuario.

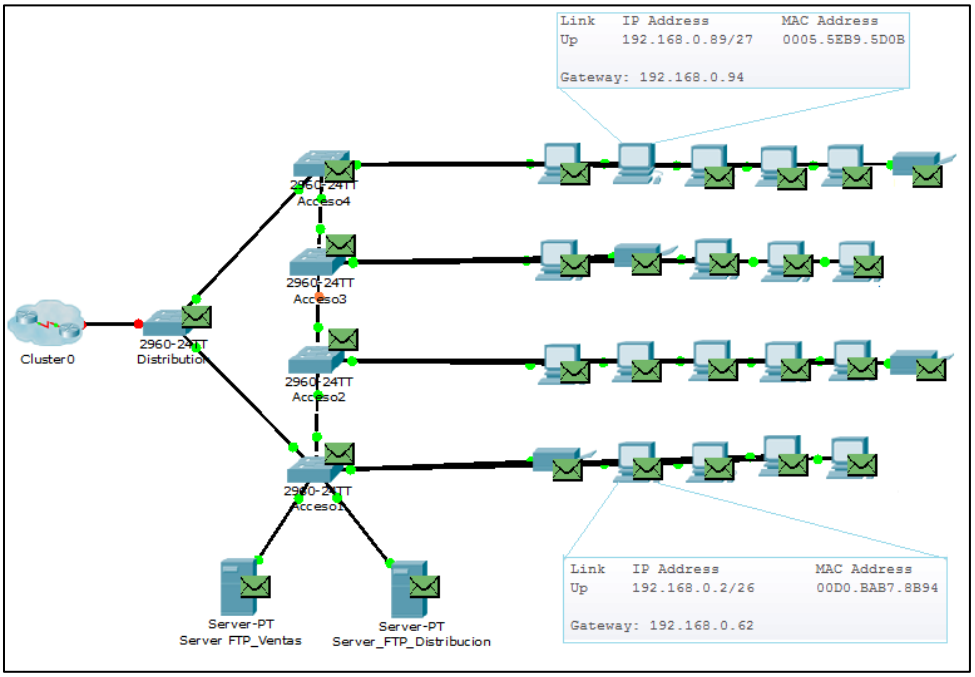
La correcta implementación de las herramientas de seguridad debe de llevar un correcto seguimiento y una constante actualización que garanticen una protección de los datos del usuario ante las crecientes amenazas de seguridad, no basta con las mínimas condiciones de seguridad en una red ya que estas condiciones deben de estar un paso delante de los riesgos existentes.

En este proyecto se propusieron con éxito condiciones de seguridad a nivel de switcheo, sin embargo existen otras herramientas a otros niveles tanto en software como en hardware que deben siempre estar presentes para complementar la seguridad de la red. Estas

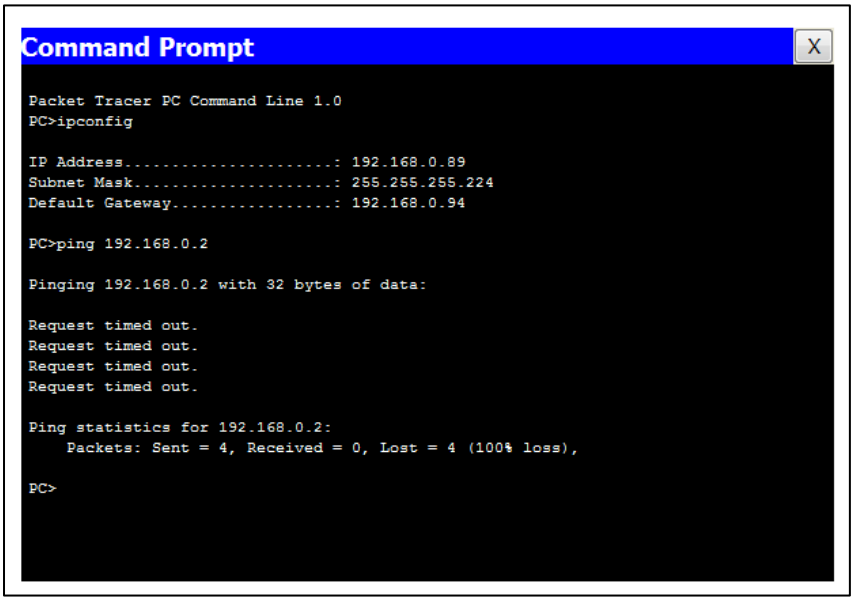
herramientas son a nivel de ruteo con listas de control de acceso (ACL) a nivel de software tales como Firewalls, Servidores Proxy, Sistemas de Detección de Intrusos (IDS) y otros sistemas especializados para las aplicaciones de red, tales como Antivirus, certificados de seguridad en internet para https y encriptaciones de textos.

ANEXO 1

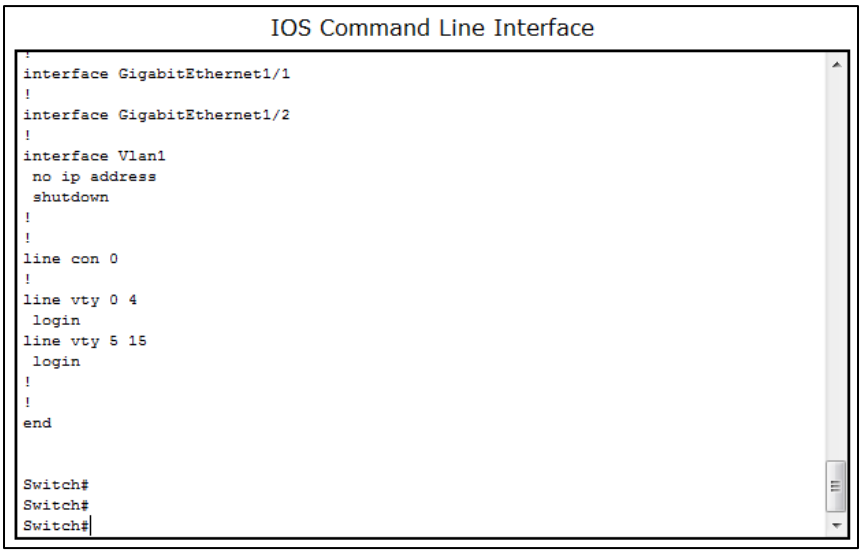
La figura muestra un ejemplo en el cual se envía un ping de la PC de la subred de distribución con dirección 192.168.0.89 a la PC de la subred de ventas con dirección 192.168.0.2. La figura muestra el estado actual que se encuentra la red.



La siguiente figura muestra el resultado del ping entre las dos PC, en donde nos indica que no hay respuesta, debido a que pertenecen a distintas subredes.



En la figura se muestran las configuraciones actuales de los switches donde se muestra que no existe una configuración de contraseñas y por lo tanto la red puede estar en riesgo, se observa que los switches no cuentan con contraseñas vty, del modo EXEC privilegiado del CLI ni los puertos tienen habilitada su función de seguridad de dirección MAC.

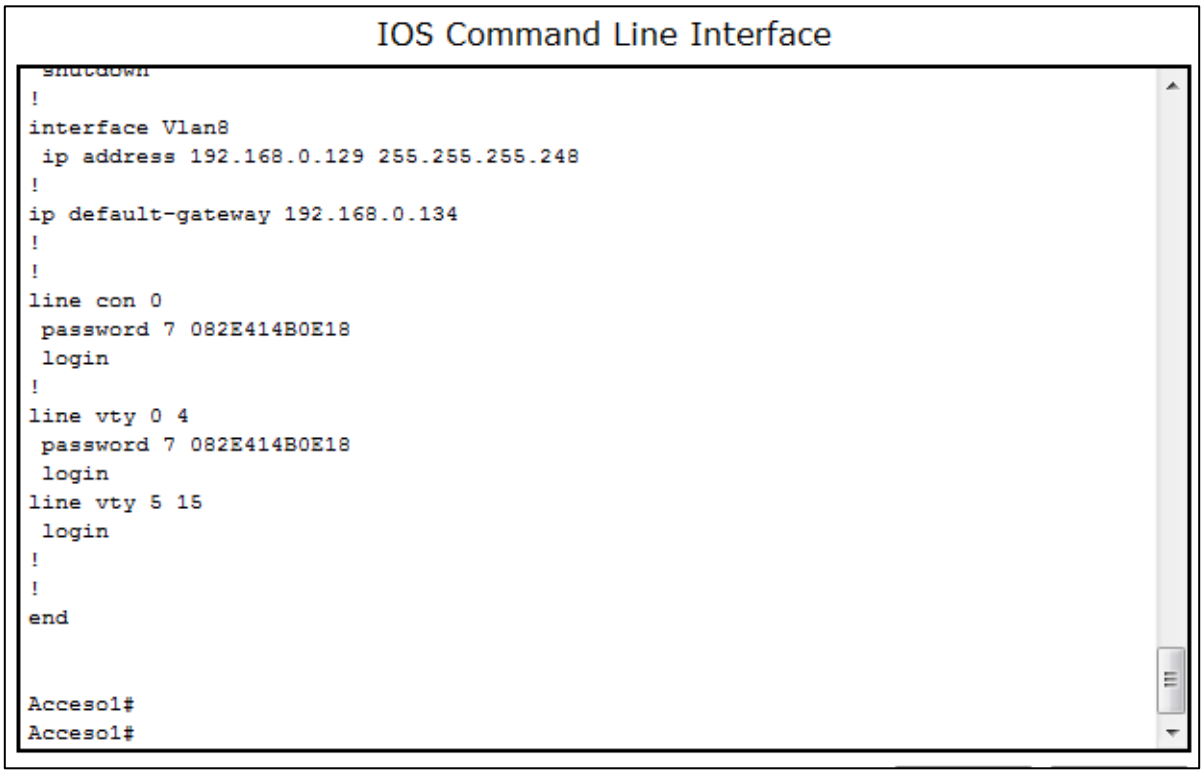


ANEXO 2

Se muestran las configuraciones para el switch Distribución y Acceso1, para los demás switches son los mismos comandos.

```
Distribucion>enable
Distribucion#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Distribucion (config)#enable secret omega
Distribucion (config)#line con 0
Distribucion (config-line)#pass omega
Distribucion (config-line)#login
Distribucion (config-line)#line vty 0 4
Distribucion (config-line)#pass omega
Distribucion (config-line)#login
Distribucion (config-line)#exit
Distribucion (config)#service password-encryption
Distribucion (config)#end

%SYS-5-CONFIG_I: Configured from console by console
Distribucion#exit

Acceso1>enable
Acceso1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Acceso1 (config)#enable secret omega
Acceso1 (config)#line con 0
Acceso1 (config-line)#pass omega
Acceso1 (config-line)#login
Acceso1 (config-line)#line vty 0 4
Acceso1 (config-line)#pass omega
Acceso1 (config-line)#login
Acceso1 (config-line)#exit
Acceso1 (config)#service password-encryption
Acceso1 (config)#end

%SYS-5-CONFIG_I: Configured from console by console
Acceso1#exit
```

En la figura podemos observar que se realizaron las configuraciones de las contraseñas de acceso para los inicios de sesión. Las contraseñas se encuentran encriptadas.



ANEXO 3

Se muestran las configuraciones para el switch Distribución y Acceso2, para los switches Acceso1, Acceso3 y Acceso4 son los mismos comandos que Acceso2.

```
Distribucion>enable
Password:
Distribucion #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Distribucion (config)#vtp mode server
Setting device to VTP SERVER mode.
Distribucion (config)#vtp domain AdministradoresPuebla
Changing VTP domain name from NULL to AdministradoresPuebla
Distribucion (config)#vtp password vlanomega
Setting device VLAN database password to vlanomega
Distribucion (config)#interface range fa0/1 – 2
Distribucion (config-if-range)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Distribucion (config-if-range)#switchport trunk native vlan 8
Distribucion (config-if-range)#end

%SYS-5-CONFIG_I: Configured from console by console
Distribucion #exit


Acceso2>enable
Password:
Acceso2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Acceso2 (config)#vtp mode client
Setting device to VTP CLIENT mode.
Acceso2 (config)#vtp domain AdministradoresPuebla
Changing VTP domain name from NULL to AdministradoresPuebla
Acceso2 (config)#vtp password vlanomega
Setting device VLAN database password to vlanomega
Acceso2 (config)#interface range fa0/23 - 24
Acceso2 (config-if-range)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
```

Acceso2 (config-if-range)#switchport trunk native vlan 8
Acceso2 (config-if-range)#end

%SYS-5-CONFIG_I: Configured from console by console
Acceso2#exit

La figura nos muestra la configuración de los enlaces troncales. En la figura se muestra el número de puerto habilitado como troncal, el protocolo de encapsulamiento 802.1q y el cambio correcto de la VLAN nativa de la 1 a la 8. Otra de las configuraciones mostradas son las VLAN permitidas en la troncal.

IOS Command Line Interface

```
User Access Verification

Password:

Acceso2>enable
Password:
Acceso2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      8
Fa0/24      on           802.1q         trunking      8

Port        Vlans allowed on trunk
Fa0/23      1-1005
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/23      1,2,3,4,5,6,7,8
Fa0/24      1,2,3,4,5,6,7,8

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      1,2,3,4,5,6,7,8
Fa0/24      1,2,3,4,5,6,7,8
Acceso2#
```

ANEXO 4

Se muestran las configuraciones para el switch Distribución, dado que es el VTP Server y se encargara de propagar las VLAN por los switches VTP Clients.

```
Distribucion>enable
Password:
Distribucion#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Distribucion (config)#vlan 2
Distribucion (config-vlan)#name Ventas
Distribucion (config-vlan)#vlan 3
Distribucion (config-vlan)#name Distribucion
Distribucion (config-vlan)#vlan 4
Distribucion (config-vlan)#name Visitantes
Distribucion (config-vlan)#vlan 5
Distribucion (config-vlan)#name Gerencia
Distribucion (config-vlan)#vlan 6
Distribucion (config-vlan)#name RH
Distribucion (config-vlan)#vlan 7
Distribucion (config-vlan)#name Juntas
Distribucion (config-vlan)#vlan 8
Distribucion (config-vlan)#name Admin&Native
Distribucion (config-vlan)#end

%SYS-5-CONFIG_I: Configured from console by console
Distribucion#exit
```

ANEXO 5

Se muestran las configuraciones para los switches Acceso3 y Acceso4, para los switches Acceso1 y Acceso2 son los mismos comandos.

```
Acceso3>enable
Password:
Acceso3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Acceso3 (config)#interface range fa0/1 - 10
Acceso3 (config-if-range)#switchport mode access
Acceso3 (config-if-range)#switchport access vlan 2
Acceso3 (config-if-range)#no shutdown
Acceso3 (config-if-range)#exit
Acceso3 (config)#interface range fa0/11 - 20
Acceso3 (config-if-range)#switchport mode access
Acceso3 (config-if-range)#switchport access vlan 4
Acceso3 (config-if-range)#no shutdown
Acceso3 (config-if-range)#end

%SYS-5-CONFIG_I: Configured from console by console
Acceso3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Acceso3#exit

Acceso4>enable
Password:
Acceso4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Acceso4 (config)#interface range fa0/1 - 10
Acceso4 (config-if-range)#switchport mode access
Acceso4 (config-if-range)#switchport access vlan 3
Acceso4 (config-if-range)#no shutdown
Acceso4 (config-if-range)#exit
Acceso4 (config)#interface range fa0/11 - 13
Acceso4 (config-if-range)#switchport mode access
Acceso4 (config-if-range)#switchport access vlan 6
Acceso4 (config-if-range)#no shutdown
Acceso4 (config-if-range)#exit
Acceso4 (config)#interface range fa0/14 - 17
Acceso4 (config-if-range)#switchport mode access
Acceso4 (config-if-range)#switchport access vlan 7
Acceso4 (config-if-range)#no shutdown
Acceso4 (config-if-range)#end
```

%SYS-5-CONFIG_I: Configured from console by console
Acceso4#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Acceso4#exit

En la figura mediante el comando *show vlan brief* nos muestra el número y el nombre de las VLAN creadas por medio del VTP así como el estatus en el que se encuentran y puerto asignado a cada una de las VLAN, como podemos observar nos indica que existen 4 puertos asignados a la VLAN por default, 10 puertos en la VLAN ventas, y 10 en la VLAN visitantes esto es solo para el acceso 3, y el resultado es satisfactorio para los demás accesos.

IOS Command Line Interface

```
Acceso3>enable
Password:
Acceso3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Gig1/1, Gig1/2
2    Ventas                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
3    Distribucion                      active
4    Visitantes                        active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
5    Gerencia                          active
6    RH                                active
7    Juntas                            active
8    Admin&Native                      active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Acceso3#
```

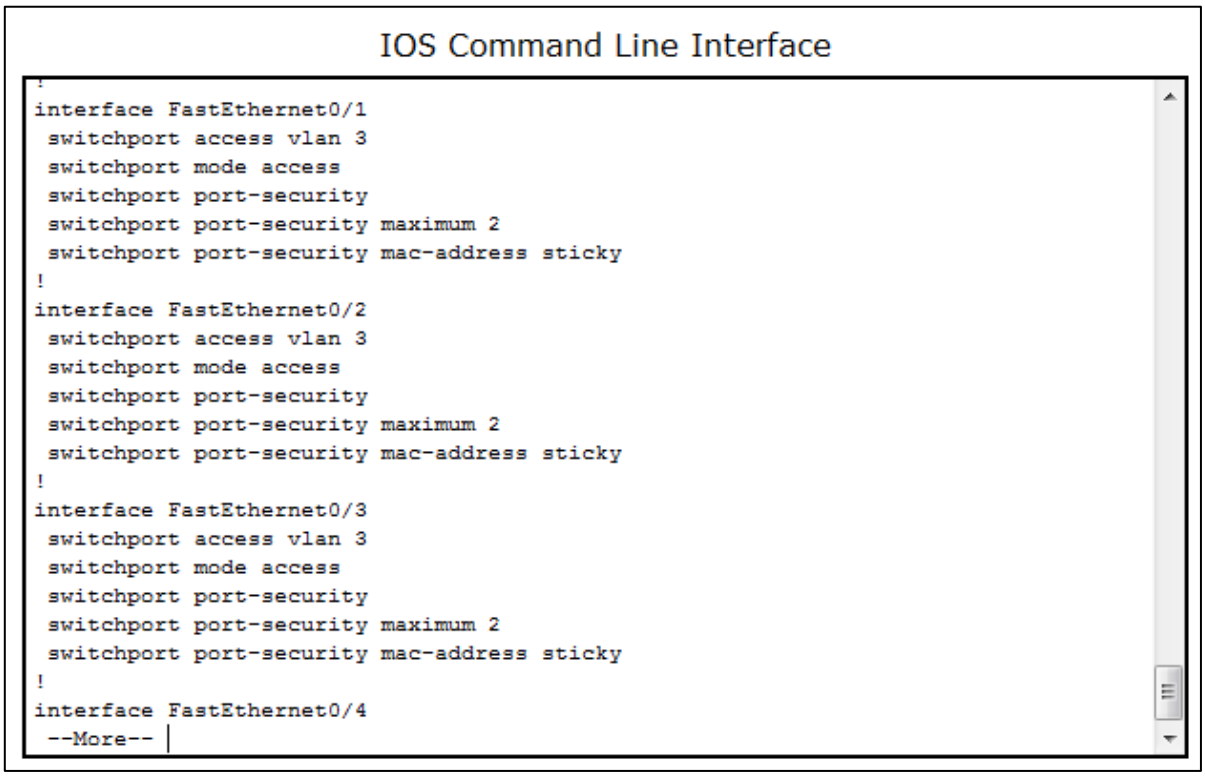
ANEXO 6

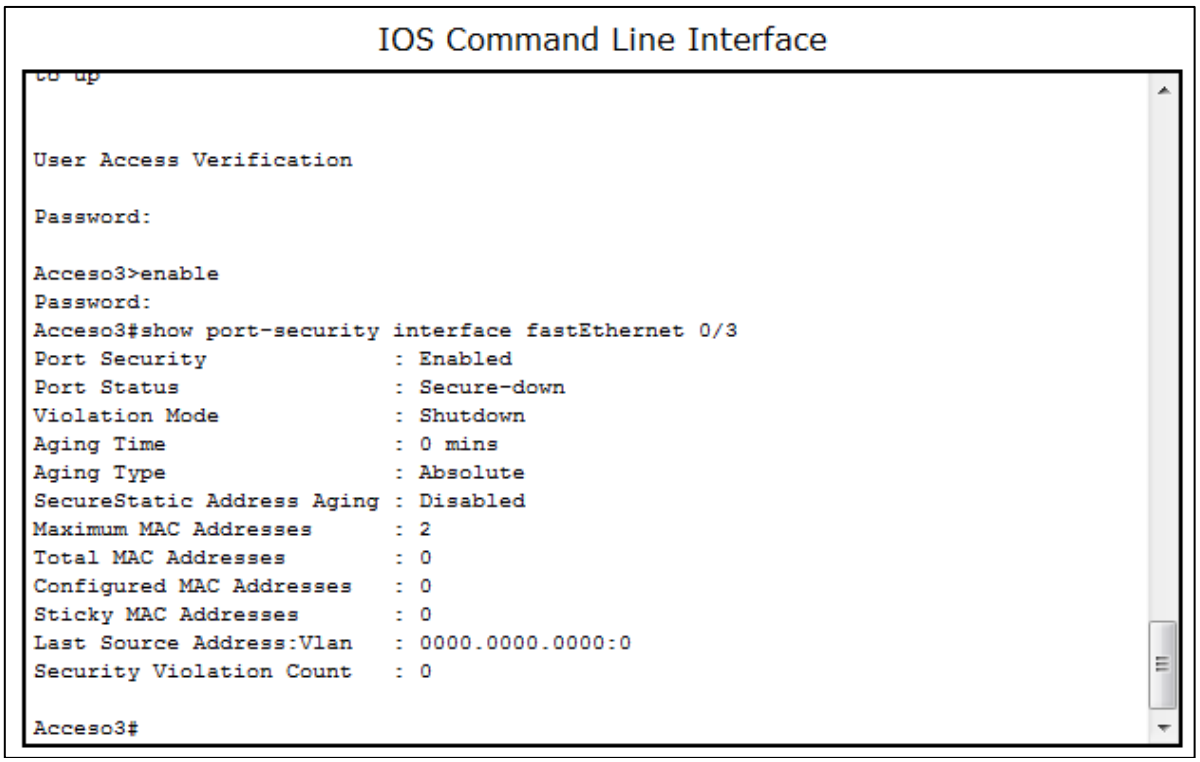
Se muestran las configuraciones para los switches Acceso1 y Acceso3, para los switches Acceso2 y Acceso4 son los mismos comandos.

```
Acceso1>enable
Password:
Acceso1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Acceso1 (config)#interface range fa0/1 - 20
Acceso1 (config-if-range)#switchport port-security
Acceso1 (config-if-range)#switchport port-security maximum 2
Acceso1 (config-if-range)#switchport port-security mac-address sticky
Acceso1 (config-if-range)#switchport port-security violation shutdown
Acceso1 (config-if-range)#end

%SYS-5-CONFIG_I: Configured from console by console
Acceso1#exit

Acceso3>enable
Password:
Acceso3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Acceso3 (config)#interface range fa0/1 - 10
Acceso3 (config-if-range)#switchport port-security
Acceso3 (config-if-range)#switchport port-security maximum 2
Acceso3 (config-if-range)#switchport port-security mac-address sticky
Acceso3 (config-if-range)#switchport port-security violation shutdown
Acceso3 (config-if-range)#exit
Acceso3 (config)#interface range fa0/11 - 20
Acceso3 (config-if-range)#switchport port-security
Acceso3 (config-if-range)#switchport port-security maximum 1
Acceso3 (config-if-range)#switchport port-security violation shutdown
Acceso3 (config-if-range)#end

%SYS-5-CONFIG_I: Configured from console by console
Acceso3#exit
```

Mediante el comando *show running config* podemos observar en la figura la correcta habilitación de la seguridad en los puertos en el Acceso3, siendo el mismo resultado para los demás switches de acceso.

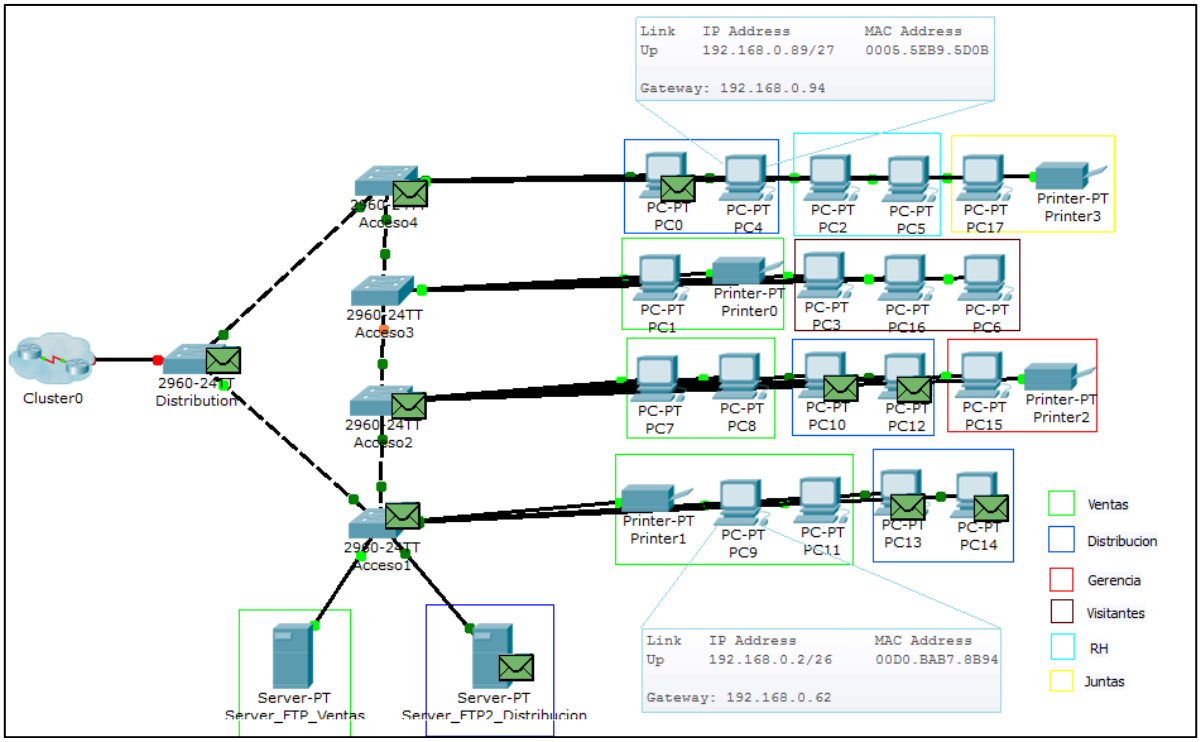
En la siguiente figura se muestra otro de los comandos que se pueden utilizar, el cual es *show port-security interface interface-id*, el cual despliega una información más detallada para un puerto en específico.


IOS Command Line Interface
!
interface FastEthernet0/1
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 --More--


IOS Command Line Interface
up
User Access Verification
Password:
Acceso3>enable
Password:
Acceso3#show port-security interface fastEthernet 0/3
Port Security : Enabled
Port Status : Secure-down
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
Acceso3#

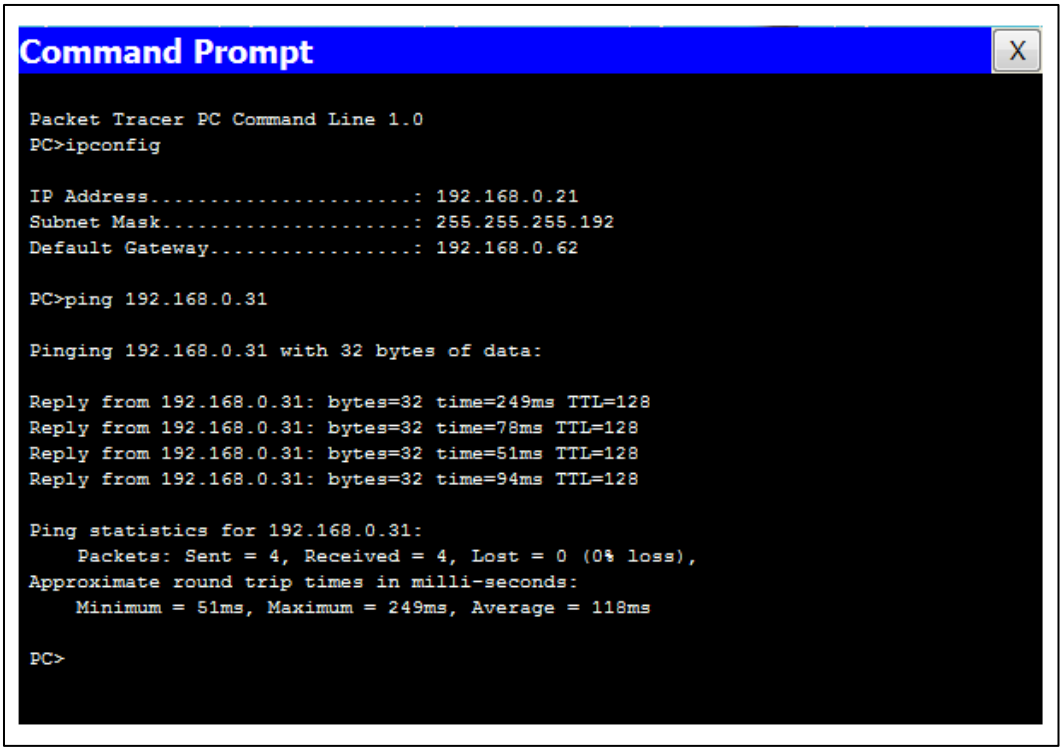
ANEXO 7

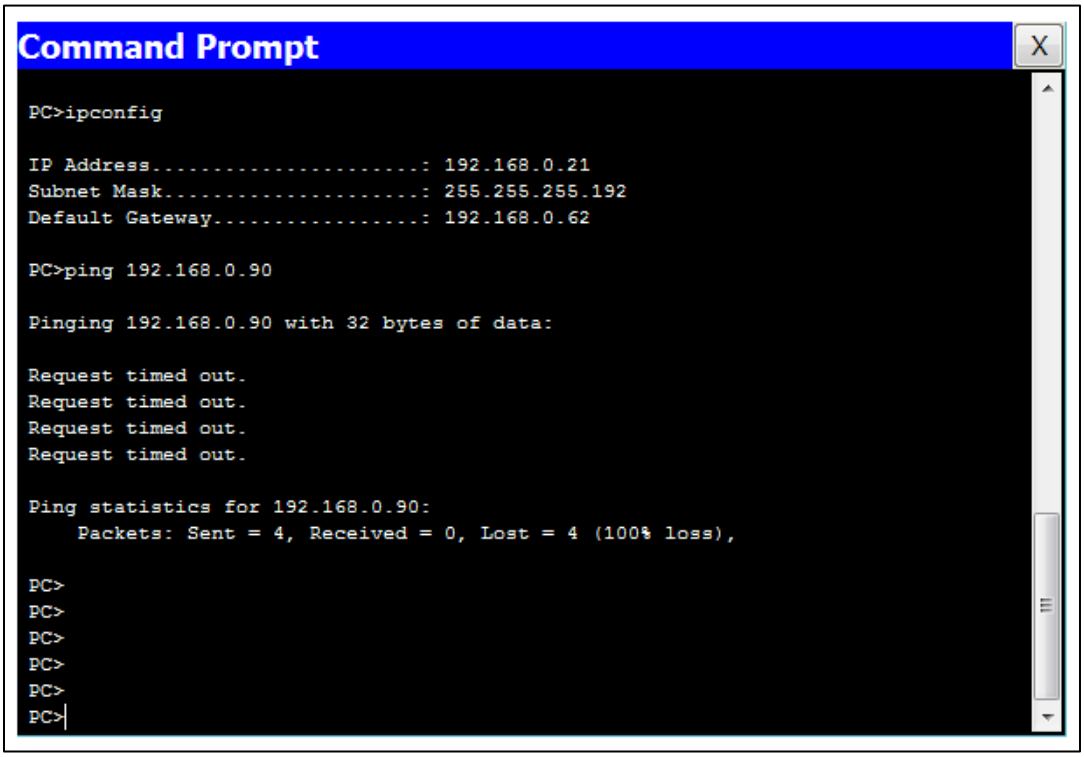
En la Figura se muestra la segmentación de los dominios de broadcast provocado por el resultado satisfactorio de la nueva configuración de la red con la ayuda del programa de simulación Packet Tracer™ de CISCO Systems Inc, observamos también la asignación de VLANS por cada área.



En las siguientes figuras se muestran los resultados de dos pings entre la PC de la VLAN 2 Ventas con dirección 192.168.0.21 a su servidor de trabajo con dirección 192.168.0.31 y a al servidor de trabajo de la VLAN 3 Distribución con dirección 192.168.0.90.

El resultado del ping exitoso muestra que solo la VLAN 2 Ventas puede tener acceso a su servidor de trabajo. La otra figura muestra que una VLAN distinta a la VLAN 3 Ditribucion no puede tener acceso al servidor de esta VLAN.


Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ipconfig
IP Address.....: 192.168.0.21
Subnet Mask.....: 255.255.255.192
Default Gateway.....: 192.168.0.62
PC>ping 192.168.0.31
Pinging 192.168.0.31 with 32 bytes of data:
Reply from 192.168.0.31: bytes=32 time=249ms TTL=128
Reply from 192.168.0.31: bytes=32 time=78ms TTL=128
Reply from 192.168.0.31: bytes=32 time=51ms TTL=128
Reply from 192.168.0.31: bytes=32 time=94ms TTL=128
Ping statistics for 192.168.0.31:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 51ms, Maximum = 249ms, Average = 118ms
PC>


Command Prompt
X
PC>ipconfig
IP Address.....: 192.168.0.21
Subnet Mask.....: 255.255.255.192
Default Gateway.....: 192.168.0.62
PC>ping 192.168.0.90
Pinging 192.168.0.90 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.90:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
PC>
PC>
PC>
PC>
PC>

Índice de figuras.

Glosario.

Agrupación de direcciones.- En IP para móviles, conjunto de direcciones designadas por el administrador de red principal para que lo utilicen los nodos móviles que necesitan una dirección permanente.

Algoritmo de postergación.- Cuando se detecta una colisión, cada emisor tendrá un retardo antes de volver a transmitir. Cada emisor elige un retardo aleatorio entre o y d (d es un valor de retardo estándar). Si se produce otra colisión, cada host duplica el intervalo del cual se elige el retardo, es decir, el retardo aleatorio ahora estará entre 0 y 2d. Si se produce otra colisión, el intervalo estará entre 0 y 4d y así sucesivamente. Luego de cada colisión, el intervalo aleatorio aumenta.

Autoconfiguración.- Proceso mediante el cual un host configura automáticamente su dirección IPv4 a partir del prefijo del sitio y la dirección MAC local.

Base de datos de directivas de seguridad (SPD).- Base de datos que determina el nivel de protección que debe aplicarse a un paquete. La SPD filtra el tráfico de IP para establecer si se debe descartar un paquete, autorizarle el paso o protegerlo con IPsec.

Carga útil.- Los datos que se transportan en un paquete. La carga útil no incluye la información de encabezado que se necesita para que el paquete llegue a su destino.

Cortafuegos.- Cualquier programa o dispositivo que aísle la intranet o red de una organización particular de Internet, con lo cual queda protegida de intrusiones externas. Un cortafuegos puede abarcar filtrado de paquetes, servidores proxy y NAT (Network Address Translation, traducción de direcciones de red).

Descubrimiento de vecinos.- Mecanismo de IP que permite a los host encontrar otros host que residen en un vínculo conectado.

Detección de errores.- Proceso en el que se detecta que deja de funcionar una interfaz o la ruta de una interfaz a un dispositivo de capa de Internet. IPMultipathing para redes presenta dos clases de detección de errores: detección en vínculos (predeterminada) o en sondeos (opcional).

Detección de reparaciones.- Proceso en el que se detecta si una tarjeta de interfaz de red o la ruta de dicha tarjeta a un dispositivo de capa 3 comienza a funcionar correctamente después de un fallo.

Dirección de datos.- Dirección IP que puede utilizarse como origen o destino de datos. Las direcciones de datos forman parte de un grupo IPMP y se pueden usar para enviar y recibir tráfico en cualquier interfaz del grupo. Además, el conjunto de direcciones de datos de un grupo IPMP se puede utilizar continuamente siempre que funcione una interfaz en el grupo.

Ethernet PHY.- Es el transceptor de interfaz física, lo que significa que trata con la capa 1 (la capa física, de ahí el PHY) de Ethernet.

Gateway.- Puerta de enlace por defecto, es una dirección IP utilizada en las interfaces Ethernet de un router para percibir el tráfico de la subred LAN.

Host.- Sistema que no reenvía paquetes. En general, un host tiene una interfaz fisica, aunque también puede constar de varias interfaces.

ICMP.- Siglas inglesas de Internet ControlMessage Protocol (protocolo de mensajes de control de Internet). Se utiliza para administrar e intercambiar mensajes de control.

Índice de parámetros de seguridad.- Valor entero que indica la fila de la base de datos de asociaciones de seguridad (SDAB) que debe utilizar un destinatario para descifrar un paquete recibido.

IP.- El protocolo de internet es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

IPv4.- Internet Protocol version 4. IPv4 en ocasiones se denomina IP. Esta versión admite un espacio de direcciones de 32 bits.

IPv6.- Internet Protocol version 6. IPv6 admite espacio de direcciones de 128 bits.

Latencia.- Es el retraso entre el momento en que comienza un proceso y el momento en que se detectan sus efectos. Por ejemplo, al transmitir datos, la latencia es el tiempo que se tarda en enviar los datos del emisor al receptor

Lista de revocación de certificados (CRL).- Lista de certificados de claves públicas revocados por una autoridad de certificación. Estas listas se almacenan en la base de datos de CRL que se mantiene con IKE.

Nodo.- En IPv4, cualquier sistema compatible con IPv4, ya sea host o enrutador.

Nodo móvil.- Host o enrutador capaz de cambiar su punto de conexión de una red a otra y mantener todas las comunicaciones utilizando su dirección IP permanente.

Paquete.- Grupo de información que se transmite como una unidad a través de líneas de comunicaciones. Contiene un encabezado IP y una carga útil.

Red principal.- Red cuyo prefijo coincide con el prefijo de red de una dirección permanente de nodo móvil.

Router.- Sistema que en general tiene más de una interfaz, ejecuta protocolos de encaminamiento y reenvía paquetes. Un sistema se puede configurar con una sola interfaz como enrutador si el sistema es el punto final de un vínculo PPP.

SA (Security Association).- Asociación que establece las propiedades de seguridad entre un primer host y un segundo.

Servidor proxy.- Servidor que se emplaza entre una aplicación cliente, por ejemplo un navegador de web, y otro servidor. Se utiliza para filtrar solicitudes, por ejemplo para impedir el acceso a determinados sitios web.

Tabla de enlace.- En IP para móviles, tabla de agentes internos que asocia una dirección permanente con una auxiliar, incluyendo la vida útil de que dispone y el tiempo que se otorga.

Tarjeta de interfaz de red.- Tarjeta de adaptador de red que actúa como interfaz de una red. Algunas tarjetas de interfaz de red pueden tener varias interfaces físicas.

TCP/IP.- (Transmission Control Protocol/Internet Protocol) es el protocolo o lenguaje de comunicaciones básico de Internet. También se usa como protocolo de comunicaciones en redes privadas (tanto intranets como extranets).

Traducción de la dirección de red.- También se conoce como NAT (del inglésNetwork Address Translation). Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red. Se utiliza para limitar la cantidad de direcciones IP globales que se necesitan.

Vínculo IP.- Infraestructura o medio de comunicación que permite a los nodos comunicarse en la capa de vínculo. La capa de vínculo es la inmediatamente inferior a IPv4/IPv6. Ejemplos son las redes Ethernet (simple o con puente) o ATM. Se asignan uno o más números o prefijos de subred IPv4 a un vínculo IP.

Bibliografía.

- Ethernet Networks from 10Base-T to Gigabit
  Gilbert Held
  Wiley computer publishing
  2005

- Cisco Networking Academy CCNA Exploration 4.0
  CISCO Systems INC.
  2007 - 2008

- Laboratorio de redes de datos
  Héctor Oswaldo Gonzáles Kaempfer
  Universidad Austral de Chile
  2005

- Guía de Administración del Sistema: Servicios IP
  ORACLE INC.
  2010

- Manual de HP para Servidores
  Hewlett-Packard México
  2010

- http://informaticamoderna.com
- http://support.microsoft.com
- http://neutron.ing.ucv.ve/revista-e/No1/SERRANO2.html
- http://www.e-advento.com/tecnologia/lan_intro.php