# Capítulo 4

# Desarrollo de la Asignatura

Este capítulo se encuentra formado por una serie de prácticas en las cuales el estudiante pondrá a prueba los conocimientos teóricos y prácticos adquiridos en las materias que conforman el módulo de Redes y Seguridad. De tal manera que se busca mediante el planteamiento de casos prácticos, que el alumno estimule su razonamiento para proponer soluciones con el fin de resolver los problemas planteados en cada práctica.

Los laboratorios se proponen semanalmente, cada uno cuenta con distintas prácticas, en las cuales se toman lo puntos más relevantes de cada tema expuesto, estos servirán para dar solución a los problemas presentados.

Las prácticas están conformadas por los siguientes puntos:

- **Objetivo**: Se plantean en general las actividades que se pretenden cubrir

- **Material**: En lista los dispositivos, software y cables de red a utilizar para la elaboración de la práctica.

- **Introducción**: Se presenta algunos conceptos básicos que el alumno debe tener en consideración para dar solución a los problemas planteados. Los temas planteados se han revisado en las materias que conforman en módulo de Redes y Seguridad.

- **Problemática**: Los problemas abordados en las prácticas, esta diseñados para que emulen circunstancia, que los egresados de la carrera de Ingeniería en Computación, encuentran frecuentemente en el ámbito laboral.

Cabe señalar que en los escenarios propuestos, se plantean una serie de soluciones, las cuales pueden ser mejoradas u optimizadas por el alumno o el profesor, ya que para solucionar un problema pueden existir distintas soluciones.

# Laboratorio 1.- Configuración básica de dispositivos que interconectan la red

## Laboratorio 1.1 Configuración Básica del Switch

### Objetivo

El alumno investigará y aplicará los procedimientos básicos necesarios para efectuar la configuración de un Switch capa 2, sin importar el fabricante de éste. Cabe resaltar que cada fabricante utiliza un sistema operativo propietario y por tal motivo cambia la forma de configuración y ejecución.

Entre las configuraciones básicas se encuentran:

- Configurar nombre y dirección IP que sirva para la administración del equipo.
- Configurar las contraseñas para garantizar el acceso seguro al modo de configuración.
- Configurar la seguridad básica en los puertos del Switch.

### Materiales y Equipo

- Switch capa 2 administrable
- 3 Cables directos y 1 de consola.
- 2 Computadoras o más.
- Simulador de red (Si no se tiene físicamente los dispositivos).

### Introducción

Un Switch es un dispositivo que tiene como objetivo principal unificar redes entre sí sin la necesidad de examinar a fondo las tramas enviadas y recibidas, debido a que sólo examina la dirección MAC de destino, creando puentes que tienen la posibilidad de dividir la red en varios dominios de colisión además de proporcionar una alta velocidad de retransmisión. El Switch originalmente es un equipo que opera en la capa 2 del modelo OSI, el cual tiene como característica principal aprender y almacenar las direcciones MAC de los dispositivos conectados en una tabla, por lo que el tráfico de datos irá desde el puerto origen únicamente al puerto destino evitando colisiones y bucles de información.

Existe una gran variedad de empresas que fabrican este tipo de dispositivos, los cuales se pueden clasificar en administrados y no administrados.

- El Switch no administrado funciona de forma automática y no permite realizar configuraciones internas que ayuden a mejorar el desempeño del mismo. Este tipo de equipos son utilizados frecuentemente en redes pequeñas.

- El Switch administrable permiten su configuración. Éstos proporcionan una gran flexibilidad debido a que puede ser supervisado y además configurados de tal forma que se obtenga su máxima funcionalidad.

Para llevar a cabo la administración de los Switch existen dos formas de hacerlo vía web y vía línea de comandos, por lo regular la forma más confiable y segura de configurar un dispositivo es vía comandos, debido a que presenta una mayor estabilidad. En la actualidad existen distintos fabricantes de dispositivos, cada uno de ellos desarrolla un OS con lenguaje y estructura propia, por ejemplo los dispositivos Cisco utilizan el Cisco IOS (*Cisco* Internet working Operating System) el cual ofrece funciones de enrutamiento y comunicación, además de presentar acceso confiable y seguro a los recursos de la red. Juniper utiliza JUNOS que es un sistema operativo de red fiable y de alto rendimiento con funciones de enrutamiento, conmutación y seguridad.

## Problemática

Una consultoría fue contratada por la empresa BOX, para solucionar un problema que se tiene en la red, el dueño de la empresa identificó que se presenta una enorme latencia al enviar la información, así como la pérdida de ésta. El dueño le proporcionó al ingeniero asignado el diagrama de red que se muestra en la Figura 4.1.

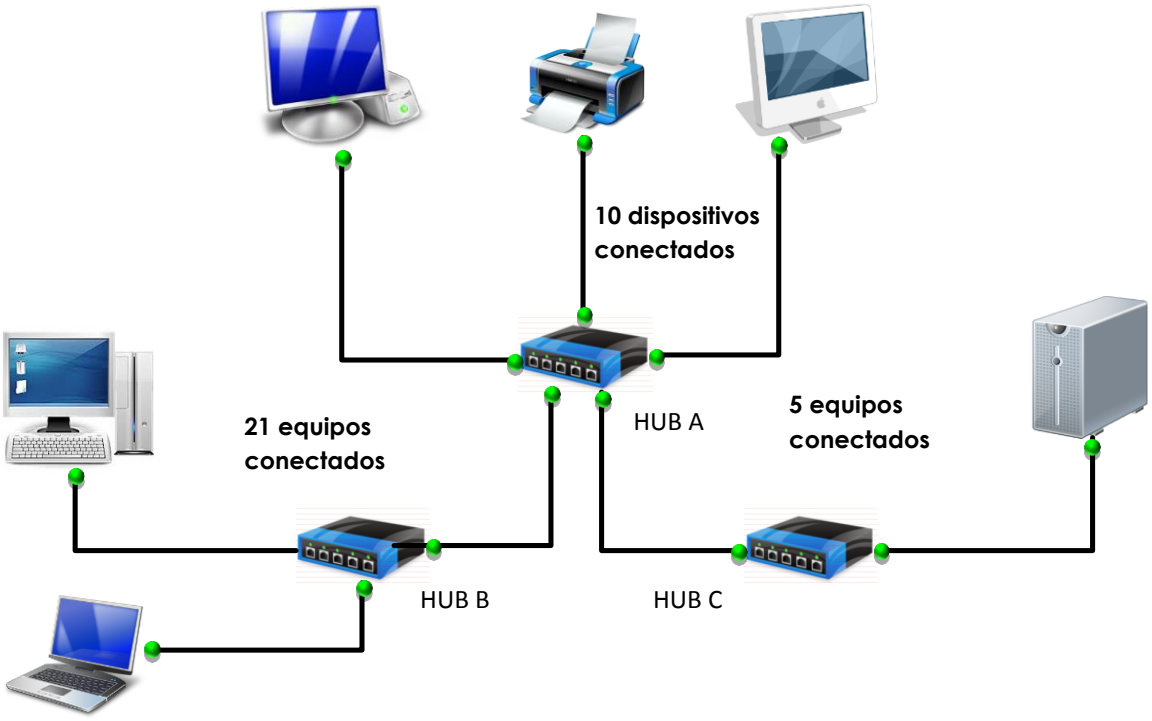



**Figura 4.1- Diagrama de Red Hub**

El ingeniero observa que la red utiliza Hubs para realizar la conexión entre los distintos dispositivos que conforman la red, la utilización de estos implica que existe un dominio de colisión, por lo que decide brindar una posible solución al problema presentado. De acuerdo a lo expuesto, proponga una posible arquitectura para dar solución al problema planteado.

**Respuesta esperada:**

- Actualizar la red utilizando dispositivos que separen los dominios de colisión (Switch) en donde cada interfaz es un propio dominio de colisión.

- Para saber el número de Switches que van a ser utilizados se debe tomar en cuenta el número de dispositivos conectados y la velocidad de sus interfaces así mismo debe cerciorarse de que cuente con un sistema operativo que le permita configurarlo.

Diseñe un diagrama de red el cual brinde una posible solución a este requerimiento, utilizando un equipo que cuente con las características necesarias para soportar la red actual así como el crecimiento futuro de ésta con un rango de 20%.

**Respuesta esperada:**

Con la finalidad de hacer estos laboratorios de forma dinámica, el profesor deberá utilizar su experiencia para validar los escenarios propuestos por el alumno y de ser posible utilizar equipos de diferentes fabricantes.

Posteriormente de haber investigado qué Switch cumple con los requerimientos necesarios para solucionar el problema planteado, el ingeniero necesita configurar y poner a punto el Switch. Para realizar esta tarea será necesario realizar las siguientes configuraciones:

- Configuración de contraseñas , mensajes de inicio y nombre de Dispositivo
- Configuración de seguridad en Puertos del Switch de forma estática y dinámica(Si el dispositivo lo soporta)
- Entre otras.

## Actividad a realizar

Para realizar la configuración del Switch, es necesario investigar que comandos realizan las siguientes tareas:

- Configurar el nombre del dispositivo.
- Configurar la contraseña para entrar en modo configuración.
- Configurar direcciones de DNS.
- Configurar mensajes de inicio de sesión.
- Habilitar el acceso remoto a través de los protocolos SSH, Telnet y FTP.
- Configurar el puerto de administración.
- Configurar una interfaz de administración.
- Crear dos usuarios, uno con todos los privilegios y el otro de sólo lectura.

**Respuesta esperada:**

En el anexo A práctica 1.1 se observa las posibles configuraciones que pueden realizar en los dispositivos, así como los diagramas de red propuestos para este laboratorio.

Cabe señal que las configuraciones mostradas pueden variar dependiendo los criterios y actividades que el maestro plantee.

Una vez concluida la configuración es necesario probar que existe comunicación entre los dispositivos así como validar los parámetros de seguridad empleados. El checklist de pruebas a ejecutar para determinar que la implementación fue exitosa es la siguiente:

- Ejecutar el comando ping desde dos dispositivos diferentes
- Obtener la tabla de direcciones MAC conectadas a los Switch
- Realizar las pruebas necesarias para validar la seguridad en los puertos del equipo (si el equipo utilizado lo permite).

# Laboratorio 1.2 Configuración Básica del Router

## Objetivo

El alumno investigara y llevara a cabo los procedimientos básicos para realizar la configuración de un Router el cual podrá ser implementado en una red. Entre las configuraciones elementales se encuentran:

- Configurar nombre, dirección IP que sirva para la administración del equipo.
- Configura las contraseñas para garantizar el acceso seguro al modo de configuración.
- Configuración de direcciones IP en los puertos del Router.
- Configuración del Router para que funcione como DCE o DET.

## Materiales y Equipo

- 2 Router.
- 3 Cables Ethernet, 1 cable seria V.35 DTE, 1 cable serial v.35 hembra y 1 de consola.
- Aplicación de Hyperterminal.
- 2 Computadoras o más.
- Simulador de red (Si no se tiene físicamente los dispositivos).

## Introducción

El Router es un dispositivo que opera en la capa 3 del modelo OSI, su objetivo principal es encaminar las tramas que se envían entre redes distintas, éstos se emplean fundamentalmente en la construcción de redes WAN y LAN, en la Figura 4.2 se muestra como los Routers son utilizados para interconectar distintas redes.

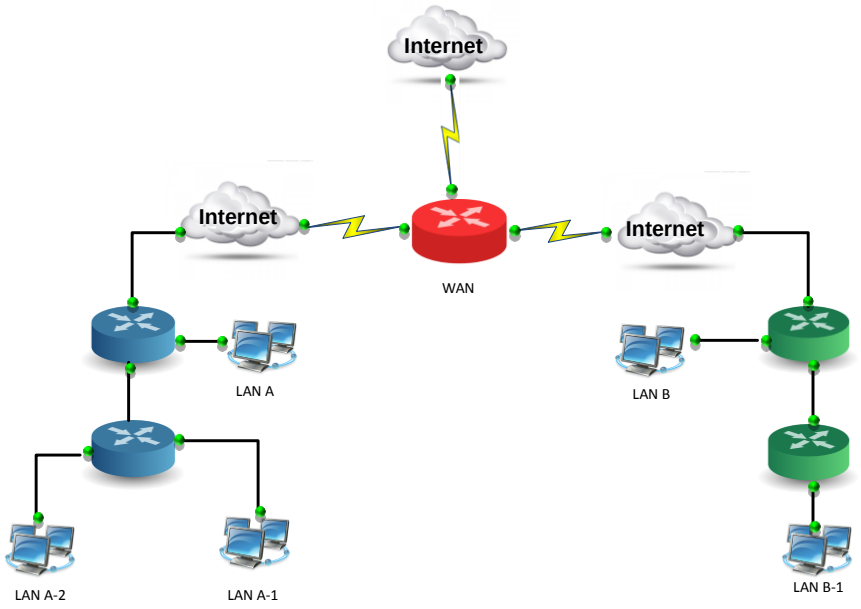



**Figura 4.2 – Interconexión de redes a través de un Router**

Estos dispositivos realizan la función de encaminamiento, es decir, son capaces de elegir la ruta más eficiente que debe seguir un paquete para llegar a su destino final, esta operación la realiza consultando las tablas de enrutamiento que contiene así como la de los Routers vecinos. En la Figura 4.3 se explica la forma en la que un Router envía los paquetes a través de una red LAN o WAN.

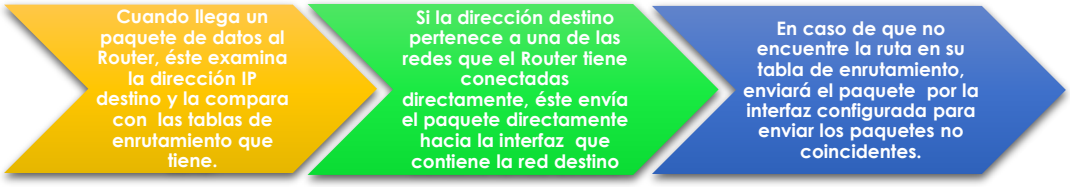



**Figura 4.3 – Forma en la que traba un Router**

Un Router posee las siguientes características.

- Toman sus decisiones basadas en direcciones de red.
- Sirven para dividir las redes LAN en dominios de difusión (broadcast) separados.
- Se utilizan para conectar redes: WAN y LAN.
- Determina las mejores rutas para los paquetes de datos entrantes basado en métricas.
- Se basa en la construcción de tablas de enrutamiento y en el intercambio de la información de red que contiene otros Routes.

Los enlaces WAN son proporcionados por los proveedores de servicios de internet, los cual entregan los paquetes a su destino final a través de la red. Para llevar a cabo el envío es necesario contar con un dispositivo que sincronice los datos para que viajen a través de la red, este dispositivo es conocido como DCE (Equipo terminal del circuito de datos), el cual es utilizado para convertir los datos del Router (DTE) en una forma aceptable para el proveedor de servicios WAN. El equipo terminal de datos (DTE) es el responsable de generar los datos y enviárselos al DCE para su transmisión. Cuando la información llega a su destino el proceso se realiza en sentido inverso y el DCE convierte la señal entrante para que el dispositivo DTE pueda transmitirlo a su destino final.

Cuando se interconectan dos Routers dentro de una Red LAN es necesario que uno de éstos funcione como un DCE, para ello es necesario configurar algunos parámetros que hagan que éste lleve a cabo la sincronización.

## Problemática

A principios de año una empresa decidió actualizar su infraestructura de red debido a que el personal de trabajo aumentó considerablemente, teniendo así que expandir sus oficinas abriendo una sucursal más la cual se encuentra en un edificio continuo. Este cambio conlleva a adquirir equipo de comunicación que soporte y lleve a cabo la comunicación entre ambos sitios. Para hacer estos cambios, es necesario rediseñar el esquema de red en el cual existan distintas subredes, las cuales serán asignadas de acuerdo al área y al número de usuarios que la conforman. La empresa proporciona la siguiente información:

- Área de contabilidad y recursos humanos 20 nodos de red.
- Área de marketing 80 nodos de red.
- Área de dirección y gerencia 20 nodos de red.
- Área de ingeniería 10 nodos de red.

El área de ingeniería necesita realizar una propuesta para este proyecto, la cual incluya el dispositivo que mejor se adecue a las necesidades de ésta, así como el diagrama de red. Después de haber analizado las propuestas presentadas por los ingenieros de Redes, el director del área de ingeniería decidió utilizar el siguiente esquema (Figura 4.4).

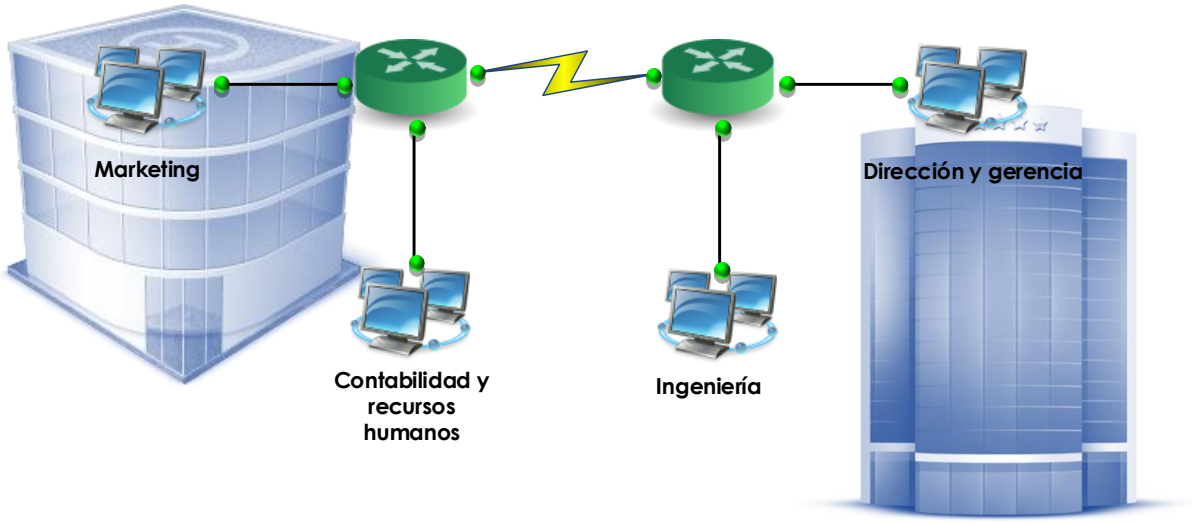



**Figura 4.4 – Diagrama de red empresa**

Para llevar a cabo el direccionamiento de la red se decidió utilizar el método de VLSM, el segmento de red a utilizar es el siguiente 192.168.0.0/24. Dentro de este segmento de red se debe segmentar el intervalo de red para tener subredes por cada una de las áreas.

Calcule y divida el segmento de red de acuerdo a los requerimientos solicitados, ingresa la información en la Tabla 4.1

**Respuesta esperada:**

**Tabla 4.1 – Direccionamiento propuesto para la empresa**

| Nombre de Subred | ID de red | Gateway | Broadcast |
|---|---|---|---|
| Marketing | 192.168.0.0/25 | 192.168.0.126 | 192.168.0.127 |
| Contabilidad | 192.168.0.128/27 | 192.168.0.158 | 192.168.0.159 |
| Dirección | 192.168.0.160/27 | 192.168.0.190 | 192.168.0.191 |
| Ingeniería | 192.168.0.192/28 | 192.168.0.206 | 192.168.0.207 |
| Enlace WAN | 192.168.0.252/30 | 192.168.0.254 | 192.168.0.255 |

## Actividad a realizar

Después de haber realizado la segmentación del direccionamiento por áreas, es necesario hacer las configuraciones adecuadas en los Routers para establecer la comunicación entre las sucursales.

Para realizar la configuración de los Routers, es necesario realizar las siguientes configuraciones en cada uno de éstos:

- Configurar el nombre del dispositivo.
- Configurar la contraseña para entrar en modo administración.
- Configurar direcciones de DNS.
- Configurar mensajes de inicio de sesión.
- Habilitar el acceso remoto a través de los protocolos SSH, Telnet y FTP.
- Configurar el puerto de administración.
- Configurar una interfaz de administración.
- Configurar cada una de las interfaces que serán conectadas a las subredes.
- Configurar el enlace serial ya sea DTE o DCE.
- Crear dos usuarios, uno con todos los privilegios y el otro de sólo lectura.

**Respuesta esperada:**

En el anexo A práctica 1.2 se observa una de las configuraciones que se pueden realizar en los dispositivos. Cabe señal que las configuraciones ejemplo pueden variar dependiendo los criterios y actividades que el maestro plantee.

Después de haber configurado cada uno de los Routers es necesario realizar pruebas de comunicación entre cada una de las subredes. Elabore un set de pruebas el cual valide que la configuración realizada sea la correcta y analice los resultados.

**Respuesta esperada:**

Realizar pruebas de conectividad entre subredes tales como: ping, tracert, traceroute. Las subredes no serán capaces de comunicarse debido a que los Routers necesitan tener configurado rutas estáticas o algún protocolo de enrutamiento.

Realice las configuraciones necesarias para que la implementación de la red sea funcional.

**Respuesta esperada:**

En la configuración mostrada en el anexo A práctica 1.2 se utilizó el protocolo de enrutamiento dinámico RIPV2, el cual permitirá realizar la comunicación entre las subred.

# Laboratorio 1.3 Configuración básica de un Access Point

## Objetivo

El alumno investigará los principales componentes físicos y lógicos que conforman un Access Point o Router inalámbrico, así como las características de seguridad que lo integran. En este laboratorio los alumnos Configurarán:

- Nombre de la red (SSID)
- Contraseña de seguridad
- Filtrado por dirección MAC
- Configuración de Firewall
- Filtrado de URLs
- Monitoreo de los logs de seguridad

## Materiales y Equipo

- Access Point o Router inalámbrico.
- Conexión a Internet
- Dispositivo electrónico con conexión a Wi-Fi.
- Cable Ethernet

## Introducción

La comunicación inalámbrica está regida por una serie de estándares que sirven para asegurar la interoperabilidad entre dispositivos fabricados por diferentes proveedores. Las tres organizaciones principales que administran los estándares WLAN alrededor del mundo son:

- **ITU-R** Regula la asignación de frecuencias de las bandas del espectro radioeléctrico.
- **IEEE** Especifica cómo se realiza la modulación de la señal de radiofrecuencia (RF) para transportar la información de una forma eficiente y segura.
- **Wi-Fi:** Impone a los distintos fabricantes la necesidad de realizar dispositivos que sean compatibles para asegurar una interoperabilidad de los mismos.

Para que exista una homogeneidad en la forma de transmitir la información entre dispositivos inalámbricos fue necesario crear el estándar 802.11 el cual define la forma en que trabajan las dos primeras capas del modelo OSI, este estándar establece las mismas funcionalidades que se presentan en el estándar 802.3 como el tipo de canal de transmisión, las características de la señal que transporta y el tipo de acceso al medio.

Un punto importante que se debe considerar al momento de crear un red WLAN es que los dispositivos estén certificados por WI-FI, la cual es una marca comercial que adopta y certifica los equipos con los estándares 802.11, con el objetivo de facilitar la compatibilidad entre éstos.

Entro los dispositivos que son utilizados para crear redes inalámbrica se encuentran:

**WAP (Wireless Access Point)**: Es un dispositivo que conecta diferentes equipos de comunicación inalámbricos para formar una red. Algunas de las ventajas que ofrece es la comunicación entre dispositivos que se encuentran en la red alámbrica e inalámbrica, así como la facilidad para ampliar una red LAN geográficamente. Los Wireless Access Point son dispositivos que pueden ser administrados para mejorar su funcionamiento, así como el de la red. En la Figura 4.5 se ilustra la forma en la que puede ser implementado un WAP.

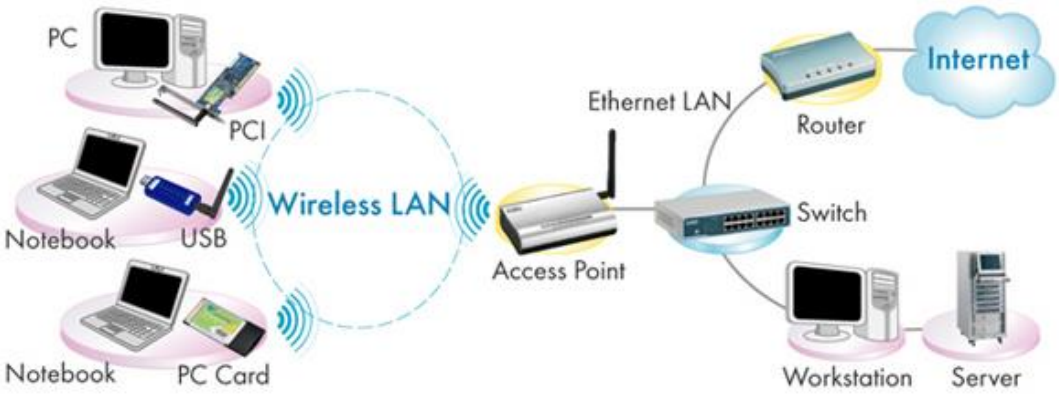



**Figura 4.5 – Implementación de Access Point**

Los **Routers inalámbricos:** Es el dispositivo encargado de recibir la señal ofrecida por un ISP (Proveedor de Servicios de Internet). El Router tiene la tarea de repartir la señal a los elementos que forman la red inalámbrica, en éste se pueden llevar a cabo distintas configuraciones de seguridad, calidad de servicios y demás. Este tipo de dispositivos son categorizados dentro de la denominada línea SOHO (Small Office-Home Office), y está destinado a usuarios finales y pequeñas empresas donde el número de usuarios a conectar no es muy alto. En la Figura 4.6 se observa un esquema general de un Router inalámbrico.


**Figura 4.6 – Esquema general Router inalámbrico**

Estos dispositivos operan en la capa 2 del modelo OSI, su funcionamiento consiste en extender la red local cableada a lugares donde la red Ethernet no puede llegar, este dispositivo trabaja mediante sistemas de radio frecuencia y se encarga de recibir y transmitir la información generada por dispositivos inalámbricos hacia su destino final. Los principales componentes de este equipo son 4: Las antenas, el puerto Ethernet, el Puerto consola o de administración y el cable de alimentación. En la Figura 4.7 se muestran los componentes físicos que componen a Router inalámbrico.

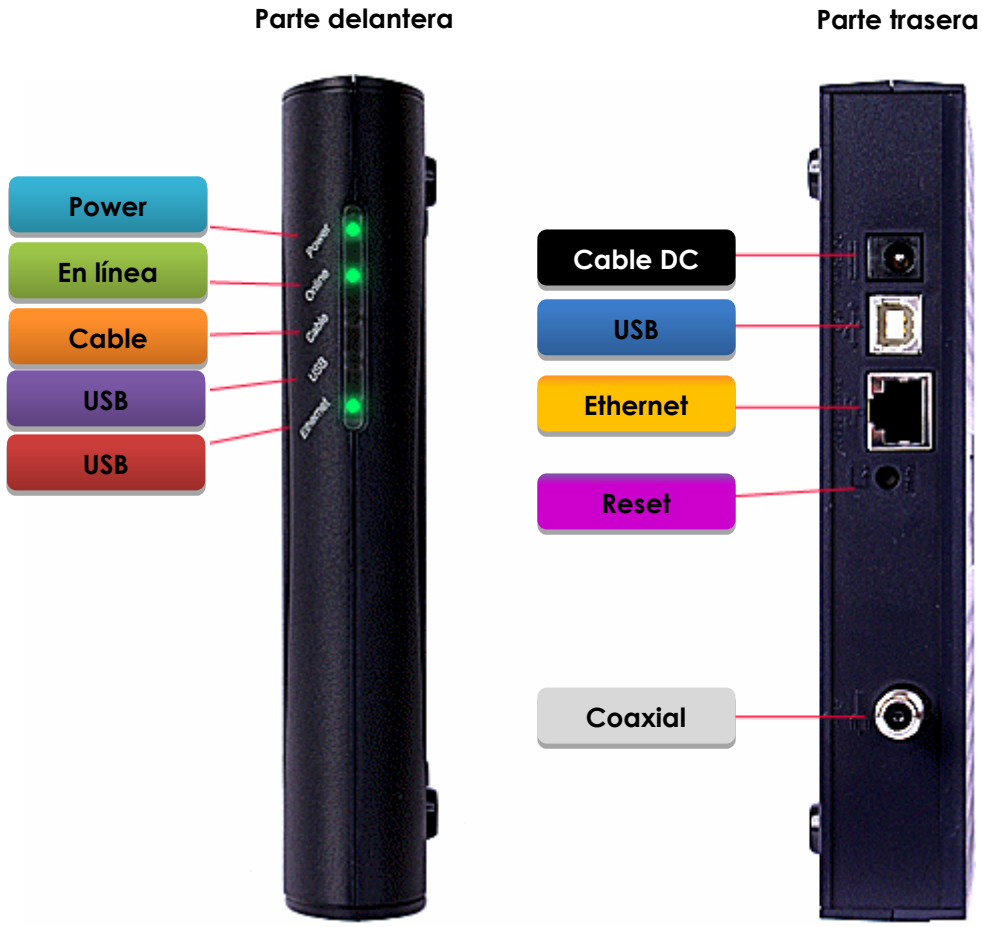



**Figura 4.7 – Componentes físicos del Router inalámbrico**

## Problemática

El departamento de redes y seguridad de una universidad actualizó su infraestructura y realizó la expansión de su red Wireless, integrando Routers inalámbricos los cuales fueron colocados en distintos salones. Para tener un control más preciso de las personas que se conectan a la red, los administradores decidieron brindarle al personal autorizado contraseña las cuales son válidas a lo largo del cuatrimestre.

Sin embargo, han recibido varios reportes referentes a la lentitud para navegar en la red e internet, ¿Cuáles son las posibles causas por la cuales se vea afectado el rendimiento de la red?

**Respuesta esperada:**

Las posibles causas por las cuales se ve afectada la navegación son:

- Exceso de sesiones hacia los Routers.
- Problemas en el cableado utilizado para conectar la Router a la red.
- Problemas de Hardware o software en los Routers.
- Degradación del performance del equipo utilizado para realizar la conexión de los Routers a la red.
- Acceso a páginas de Internet o aplicaciones que demanda un gran ancho de banda.

Después de analizar los logs que entregan los equipos, tal y como se muestra en la Tabla 4.2 y hacer troubleshooting en los Routers, los administradores de la red se dieron cuenta que existía un exceso de conexiones de equipos a los Routers, así como el acceso a demasiadas páginas que demandan demasiado ancho de banda de la red.

**Tabla 4.2 - Log de autenticación**

| IP Address | Host Name | MAC Address |
|---|---|---|
| 192.168.2.4 | gateway-675320d | 0c:60:76:68:8b:32 |
| 192.168.2.5 | IKRK-PC | 1c:65:9d:da:74:10 |
| 192.168.2.35 | android_86ce489 | 20:54:76:58:d4:f3 |
| 192.168.2.7 | iKary | 28:37:37:73:2f:4d |
| 192.168.2.24 | iPod-Princ | 28:37:37:d2:46:68 |
| 192.168.2.38 | Kary-14 | 64:27:37:25:2e:d0 |
| 192.168.2.42 | unknown | 84:00:d2:ac:cc:f4 |

En base a lo detectado ¿Cuáles serían las posibles soluciones para resolver el problema?

**Respuesta esperada:**

La respuesta varía dependiendo del equipo utilizado para llevar a cabo la práctica. Es necesario llevar a cabo las siguientes acciones:

- Método de autenticación.
- Acceso mediante la dirección MAC.
- Filtrado de páginas Web.
- Contraseñas seguras.

## Actividad a Realizar

Para realizar la configuración de los equipos es necesario identificar las características de seguridad lógica con las que cuenta los dispositivos a configurar. A continuación se presentan algunos parámetros que pueden ser configurados en todo dispositivo:

- SSID.
- Método de autenticación.
- Control de acceso mediante la dirección MAC.
- Filtrado de URL.

# Laboratorio 2.- Diseño e implementación de una red

## Laboratorio 2.1 Subnetting

### Objetivo

El alumno llevará a cabo el diseño y configuración de una red mediante subnetting, así mismo identificará las ventajas y desventajas que tiene al utilizar este método. En este laboratorio el alumno realizará:

- Diseño de la red mediante Subnetting.
- Configuración de Routers.
- Configuración del Switch.

### Materiales y Equipo

- Switch capa 2 administrable.
- Router.
- Cables red y 1 de consola.
- 2 Computadoras o más
- Simulador de red (Si no se tiene físicamente los dispositivos).

### Introducción

El método de subnetting consiste en dividir una red física en subredes lógicas más pequeñas, las cuales trabajan a nivel de envío y recepción de paquetes como una red independiente, aunque todas pertenezcan a la misma red física.

Tener segmentada la red mediante subnetting permite tener una mejor administración, seguridad y control del tráfico, además de mejorar el performance de la red, sin embargo, una de las grandes desventajas que se tiene al utilizar este método es el desperdicio considerable de direcciones IPs, ya que todas las subredes utilizan la misma máscara de red sin importar el número de host que contengan.

Para realizar la segmentación de las redes es necesario tomar en cuenta que existen 5 clases de redes, las cuales se muestran en la tabla 4.3, esto con el objetivo de tener una mejor planeación de la red:

Tabla 4.3 – Clase de redes

| Clase | Direcciones Disponibles | | N° de Sub-Redes | N° de Host | Tamaño de la red |
|---|---|---|---|---|---|
| | Inicio | Final | | | |
| A | 0.0.0.0 | 127.255.255.255 | 128 | 16 777 214 | Redes grandes |
| B | 128.0.0.0 | 191.255.255.255 | 16 384 | 65 534 | Redes medianas |
| C | 192.0.0.0 | 223.255.255.255 | 2 097 152 | 254 | Redes pequeñas |
| D | 224.0.0.0 | 239.255.255.255 | No aplica | No aplica | Multicast |
| E | 240.0.0.0 | 255.255.255.255 | No aplica | No aplica | Investigación |

## Problemática

De acuerdo a una actualización en las políticas de la organización se ha decretado realizar una organización de la red de datos, en la cual se tenga distribuido el espacio de direcciones otorgado conforme a la sucursal a la que pertenece, ésta se encuentra compuesta por 11 sucursales distribuidas por todo el país y se piensa que en un futuro se inauguren 4 oficinas más.

Para ello la empresa Engineering & Design 21 ha decidido convocar al departamento de sistemas para que los ingenieros presenten sus propuestas en la cual deben justificar por qué han elegido **Subnetting** como el método a emplear.

ENGINEERING & DESIGN

**Propuesta de direccionamiento**

El segmento de red otorgado es:

**132.100.0.0/16**

**Se necesita utilizar un método de direccionamiento en el cual se tenga un buen aprovechamiento del espacio de red otorgado.**

| Sucursal | # de direcciones IP a utilizar |
|---|---|
| **Distrito Federal** | 1100 |
| **Querétaro** | 1000 |
| **Puebla** | 800 |
| **Toluca** | 900 |
| **Monterrey** | 2030 |
| **Cancún** | 1000 |
| **Durango** | 800 |
| **Sonora** | 1200 |
| **Oaxaca** | 700 |
| **Chiapas** | 650 |
| **Quintana Roo** | 1413 |

| Nuevas Tiendas | # de direcciones IP a utilizar |
|---|---|
| **Nueva Tienda 1** | 1515 |
| **Nueva Tienda 2** | 500 |
| **Nueva Tienda 3** | 2021 |
| **Nueva Tienda 4** | 780 |

| Enlaces WAN | # de direcciones IP a utilizar |
|---|---|
| **WAN 1** | 2 |
| **WAN 2** | 2 |

Al haber analizados la información obtenida, la empresa publicó también el diagrama de red que se muestra en la Figura 4.8, éste se utilizará para implementar la red.

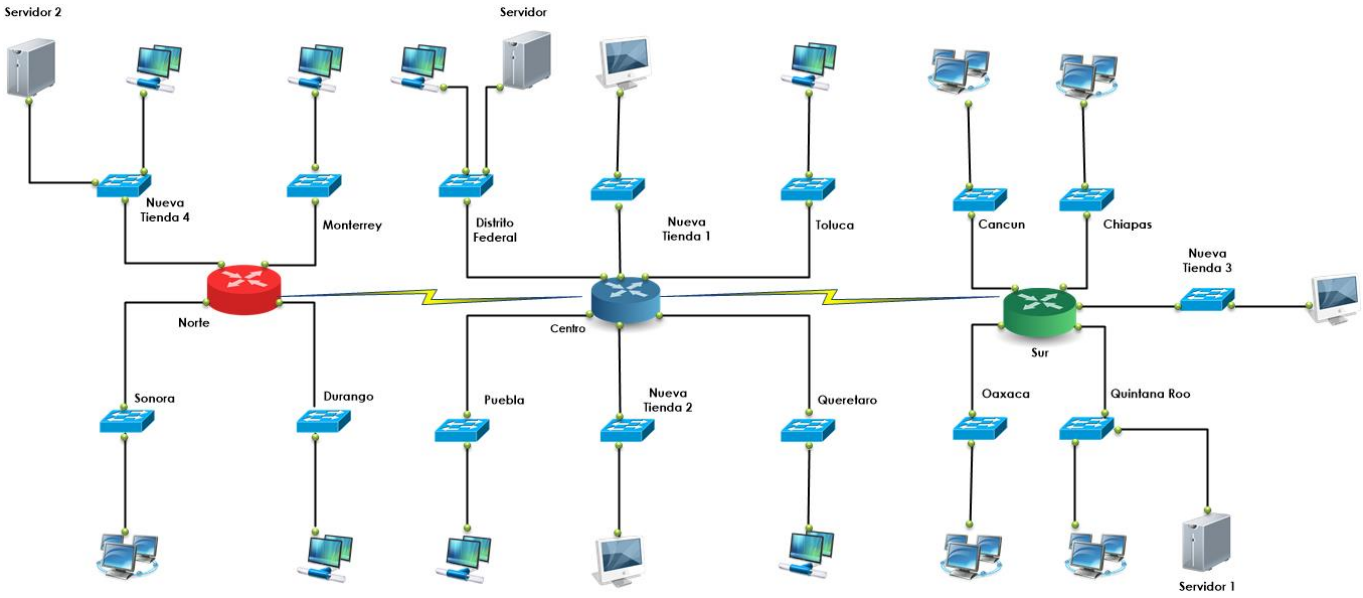



**Figura 4.8 – Diagrama de red empresa Engineering & Design**

Después de haber diseñado el diagrama de red, los ingenieros realizaron los cálculos necesarios para obtener el direccionamiento que se utilizará en la implementación. Calcule y divida el segmento de red de acuerdo a los requerimientos solicitados, ingrese la información en la Tabla 4.4

**Tabla 4.4 – Direccionamiento Subnetting**

| Nombre de Subred | ID de red | Gateway (Ideal) | Broadcast |
|---|---|---|---|
| No utilizable | 132.100.0.0/21 | 132.100.7.254 | 132.100.7.255 |
| Distrito Federal | 132.100.8.0/21 | 132.100.15.254 | 132.100.15.255 |
| Querétaro | 132.100.16.0/21 | 132.100.23.254 | 132.100.23.255 |
| Puebla | 132.100.24.0/21 | 132.100.31.254 | 132.100.31.255 |
| Toluca | 132.100.32.0/21 | 132.100.39.254 | 132.100.39.255 |
| Monterey | 132.100.40.0/21 | 132.100.47.254 | 132.100.47.255 |
| Cancún | 132.100.48.0/21 | 132.100.55.254 | 132.100.55.255 |
| Nueva tienda 1 | 132.100.56.0/21 | 132.100.63.254 | 132.100.63.255 |
| Nueva tienda 2 | 132.100.64.0/21 | 132.100.71.254 | 132.100.71.255 |
| Nueva tienda 3 | 132.100.72.0/21 | 132.100.79.254 | 132.100.79.255 |
| Nueva tienda 4 | 132.100.80.0/21 | 132.100.87.254 | 132.100.87.255 |
| Durango | 132.100.88.0/21 | 132.100.95.254 | 132.100.95.255 |
| Sonora | 132.100.96.0/21 | 132.100.103.254 | 132.100.103.255 |
| Oaxaca | 132.100.104.0/21 | 132.100.111.254 | 132.100.111.255 |
| Chiapas | 132.100.112.0/21 | 132.100.119.254 | 132.100.119.255 |
| Quintana Roo | 132.100.120.0/21 | 132.100.127.254 | 132.100.127.255 |
| WAN | 132.100.128.0/21 | 132.100.135.254 | 132.100.135.255 |
| WAN 1 | 132.100.136.0/21 | 132.100.143.254 | 132.100.143.255 |
| No utilizable | 132.100.144.0/21 | 132.100.143.254 | 132.100.151.255 |

## Actividad a Realizar

Se deben de realizar las configuraciones necesarias, para que la red propuesta, trabaje de manera correcta. En base a sus conocimientos determine, ¿Qué configuraciones se deben realizar?

**Respuesta esperada:**

De acuerdo a lo aprendido en las prácticas pasadas, las configuraciones mínimas necesarias para que la red trabaje adecuadamente son:

- Configurar los parámetros necesarios para identificar al dispositivo, así como habilitar los parámetros de seguridad en cuanto a la administración se refiere.
- Asignar las direcciones IP a cada uno de los dispositivos en las interfaces utilizadas.
- A nivel de capa 2 realizar las configuraciones de seguridad necesarias, para asegurar que algún dispositivo ajeno a la red pueda conectarse.
- Configuración el enrutamiento necesario para que todas las localidades se comuniquen.

Después de haber realizado las configuraciones necesarias para que la red trabaje adecuadamente, es necesario realizar las pruebas de conectividad, Registre la evidencia necesaria para comprobar que ésta trabaje adecuadamente.

Dentro de las pruebas que el alumno debe realizar se encuentran:

- Pruebas de ping, tracert.
- Mostrar las tablas de enrutamiento que son generadas en los Routers.

# Laboratorio 2.2 VLSM

## Objetivo

El alumno investigará y diseñará un esquema de direccionamiento basándose en el método de VLSM. En este laboratorio los alumnos realizarán las siguientes actividades:

- Diseñar un esquema de direccionamiento utilizando VLSM.
- Implementar el direccionamiento en un segmento de red.
- Empleará los conocimientos para resolver problemas relacionados con VLSM tales como la Segmentación de red,
- Utilizará los conocimientos adquiridos en laboratorios preliminares para realizar la configuración de Switch y Router.

## Materiales y Equipo

- Routers
- Switch capa 2 administrable
- 3 Cables directos y 1 de consola
- 2 Computadoras o más
- Simulador de red (Si no se tiene físicamente los dispositivos).

## Introducción

El método de direccionamiento denominado: "Máscaras de subred de tamaño variable *(Variable Length Subnet Mask, VLSM)"* representa una de las opciones que se desarrollaron para solucionar el problema de agotamiento de direcciones IPv4, esta técnica consiste en diseñar un esquema de direccionamiento usando varias máscaras en función de la cantidad de hosts, es decir, la cantidad de hosts determina la longitud de la máscara o longitud del prefijo de red.

El método que emplea VLSM es el resultado del proceso por el cual se divide una red en subredes más pequeñas cuyas máscaras de red son de diferente longitud, justo como su nombre lo indica se determina según las necesidades de hosts por subred. La implementación de VLSM maximiza la eficiencia del direccionamiento. A continuación en la Tabla 4.5 se ejemplifica la manera en que VLSM calcula la máscara a utilizar.

**Tabla 4.5 – Método de máscara de longitud variable VLSM**

| Sufijo | Host | Prefijo | 2^n=host | Binario=>Decimal |
|---|---|---|---|---|
| .255 | 1 | /32 | 2^0 | ....11111111 |
| .254 | 2 | /31 | 2^1 | ..... 11111110 |
| .252 | 4 | /30 | 2^2 | .....11111100 |
| .248 | 8 | /29 | 2^3 | ..... 11111000 |
| .240 | 16 | /28 | 2^4 | ..... 11110000 |
| .224 | 32 | /27 | 2^5 | ..... 11100000 |
| .192 | 64 | /26 | 2^6 | ..... 11000000 |
| .128 | 128 | /25 | 2^7 | ..... 10000000 |

VLSM es utilizado por algunos protocolos de enrutamiento como RIPv2, OSPF, IGRP, EIGRP, lo cual permite a los administradores de red organicen y utilicen con libertad distintas máscaras redes que se encuentran dentro de un sistema autónomo de red, Cabe mencionar que le uso de este esquema de direccionamiento, depende de la capacidad de los Routers para soportar este tipo de direccionamiento.

## Problemática

De acuerdo a una actualización en las políticas de la organización se ha decretado llevar a cabo una organización en la red de datos en la cual se tenga distribuido el espacio de direcciones otorgado conforme a la sucursal a la que pertenece, ésta se encuentra compuesta por 11 sucursales distribuidas por todo el país y se piensa que en un futuro se inauguren 4 oficinas más Para ello la empresa Engineering & Design 21 ha decidido convocar al departamento de sistemas para que los ingenieros presenten sus propuestas en la cual deben justificar por qué han elegido **VLSM** como el método a emplear.


**Propuesta de direccionamiento**

El segmento de red otorgado es:

**132.100.0.0/16**

**Se necesita utilizar un método de direccionamiento en el cual se tenga un buen aprovechamiento del espacio de red otorgado.**

| Sucursal | # de direcciones IP a utilizar |
|---|---|
| **Distrito Federal** | 1100 |
| **Querétaro** | 1000 |
| **Puebla** | 800 |
| **Toluca** | 900 |
| **Monterrey** | 2030 |
| **Cancún** | 1000 |
| **Durango** | 800 |
| **Sonora** | 1200 |
| **Oaxaca** | 700 |
| **Chiapas** | 650 |
| **Quintana Roo** | 1413 |

| Nuevas Tiendas | # de direcciones IP a utilizar |
|---|---|
| **Nueva Tienda 1** | 1515 |
| **Nueva Tienda 2** | 500 |
| **Nueva Tienda 3** | 2021 |
| **Nueva Tienda 4** | 780 |

| Enlaces WAN | # de direcciones IP a utilizar |
|---|---|
| **WAN 1** | 2 |
| **WAN 2** | 2 |

Al haber analizado la información obtenida, la empresa publicó también el diagrama de red que se observa en la Figura 4.9, el cual se utilizará para implementar la red.

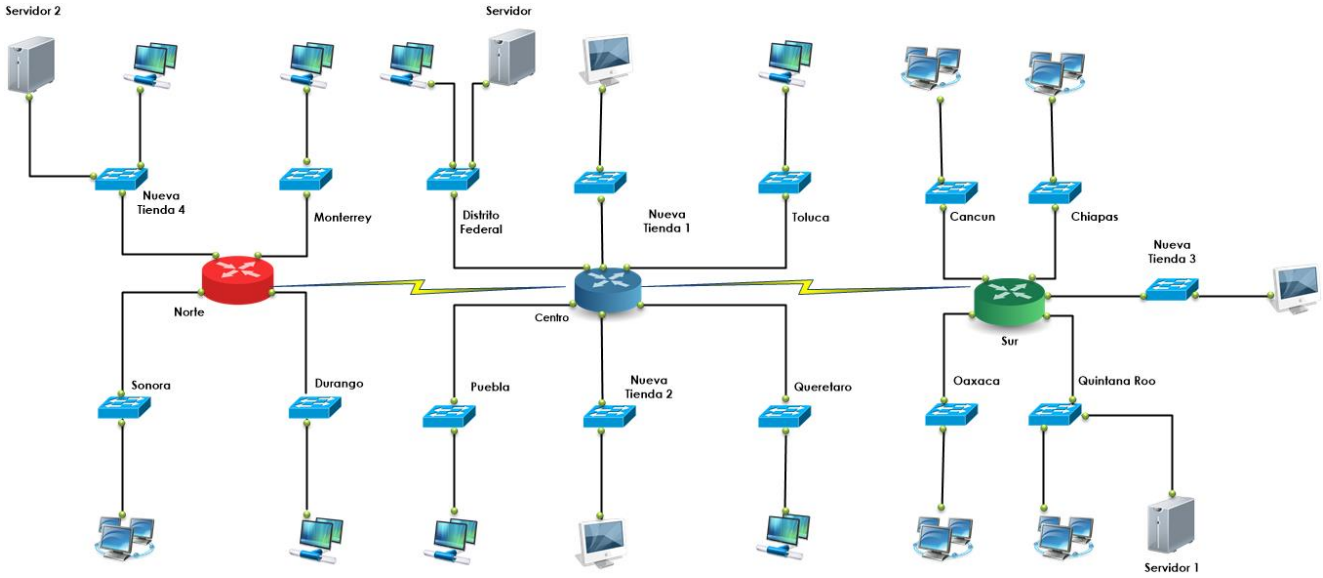



**Figura 4.9 – Diagrama de red empresa Engineering & Design VLSM**

Después de haber diseñado el diagrama de red, los ingenieros realizaron los cálculos necesarios para obtener el direccionamiento que se utilizará en la implementación. Calcule y divida el segmento de red de acuerdo a los requerimientos solicitados, ingrese la información en la Tabla 4.6

**Respuesta esperada:**

Los alumnos con base en su experiencia deben de realizar la segmentación de las direcciones mediante el método de VLSM.

**Tabla 4.6 – Direccionamiento VLSM**

| Subred | N° Host requeridos | ID de red | Broadcast | Máscara |
|---|---|---|---|---|
| **Monterrey** | 2030 | 132.100.0.0 | 132.100.7.255 | /21 |
| **Nueva Tienda 3** | 2021 | 132.100.8.0 | 132.100.15.255 | /21 |
| **Nueva Tienda 1** | 1515 | 132.100.16.0 | 132.100.23.255 | /21 |
| **Quintana Roo** | 1413 | 132.100.24.0 | 132.100.31.255 | /21 |
| **Sonora** | 1018 | 132.100.32.0 | 132.100.35.255 | /22 |
| **D.F.** | 1015 | 132.100.36.0 | 132.100.39.255 | /22 |
| **Querétaro** | 1000 | 132.100.40.0 | 132.100.43.255 | /22 |
| **Cancún** | 1000 | 132.100.44.0 | 132.100.47.255 | /22 |
| **Toluca** | 900 | 132.100.48.0 | 132.100.51.255 | /22 |
| **Puebla** | 800 | 132.100.52.0 | 132.100.55.255 | /22 |
| **Durango** | 800 | 132.100.56.0 | 132.100.59.255 | /22 |
| **Nueva Tienda 4** | 780 | 132.100.60.0 | 132.100.63.255 | /22 |
| **Oaxaca** | 700 | 132.100.64.0 | 132.100.67.255 | /22 |
| **Chiapas** | 650 | 132.100.68.0 | 132.100.71.255 | /22 |
| **Nueva Tienda 2** | 500 | 132.100.72.0 | 132.100.73.255 | /23 |
| **WAN 1** | 2 | 132.100.74.0 | 132.100.74.3 | /30 |
| **WAN 2** | 2 | 132.100.74.4 | 132.100.74.7 | /30 |

## Actividad a Realizar

Para la presentación de la propuesta se debe realizar una simulación de la red con el diseño de direccionamiento que se propuso anteriormente, es necesario llevar a cabo las configuraciones en los equipos intermedios para realizar la propuesta sea exitosa. Con base en sus conocimientos determine, ¿Qué configuraciones se deben realizar?

**Respuesta esperada:**

- Configurar los equipos con el nombre de la sucursal para identificar al dispositivo, y habilitar los parámetros de seguridad en cuanto a la administración se refiere.
- Asignar las direcciones IP a cada uno de los dispositivos en las interfaces utilizadas.
- A nivel de capa 2 realizar las configuraciones de seguridad necesarias, para asegurar que algún dispositivo ajeno a la red no pueda conectarse.
- Realice el enrutamiento necesaria para que todas las localidades se comuniquen.

Después de haber realizado las configuraciones necesarias para que la red trabaje adecuadamente, es necesario realizar las pruebas de conectividad, Registre la evidencia necesaria para comprobar que ésta trabaje correctamente.

Dentro de las pruebas que el alumno debe realizar se encuentran:

- Pruebas de ping, tracert.
- Mostrar las tablas de enrutamiento que son generadas en los Routers.

# Laboratorio 2.3 Configuración de direccionamiento

## Objetivo

El alumno ejecutará las pruebas y tareas necesarias para realizar la configuración de las tarjetas de red, sin importar el sistema operativo y tecnología que sean utilizados en los equipos de cómputo.

Entre las actividades a efectuar se encuentran:

- Configurar tarjetas de red alámbricas e inalámbricas de manera gráfica.
- Configurar tarjetas de red alámbricas e inalámbricas en modo consola.
- Ejecutar comandos para la identificación de problemas.

## Materiales y Equipo

- Router
- Switch
- Equipos de cómputo con los siguientes características:
    - Equipo con S.O Windows Server
    - Equipo con S.O MAC OS
    - Equipo con S.O Ubuntu o cualquier distribución Linux.
    - Instalar sobre el equipo con Ubuntu un servidor FTP.
    - Instalar sobre el equipo con Windows Server un servidor Web.

## Introducción

Una tarjeta de red o adaptador de red es un dispositivo de Hardware, el cual tiene como función principal convertir la información que se envía y recibe a través de la red en señales que son enviadas por algún medio de comunicación, ya sea por un medio terrestre o vía inalámbrica. También son utilizadas para compartir recursos entre dos o más computadoras (discos duros, CD-ROM, impresoras, etc). A este dispositivo se le conoce como NIC (Network Interface Card), cada tarjeta tiene un identificador denominado dirección MAC, el cual es único e irrepetible. La dirección MAC consta de 48 bits escritos en sistema hexadecimal, donde los seis primeros números (OUI) son el identificador del fabricante que son asignados por la IEEE, y los últimos seis números son determinados por el fabricante de forma consecutiva.

## Componentes de tarjetas de red

En la actualidad existen dos tipos de tarjetas de red:

- **Alámbricas:** Este tipo de tarjetas utilizan cable UTP o fibra óptica para conectarse a la red cableada, en la Figura 4.10 se muestra estos dos modelos.

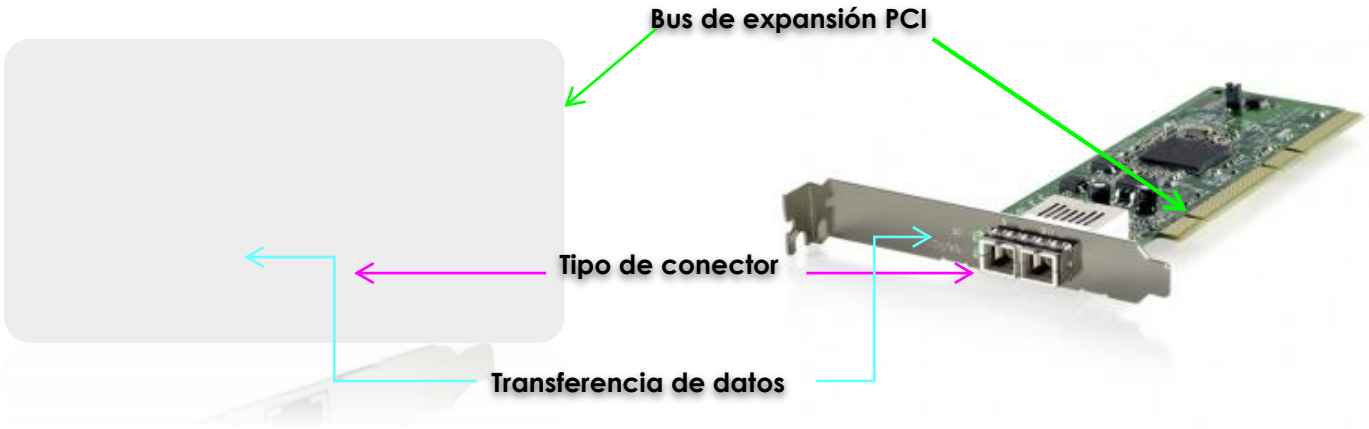



**Figura 4.10 – Tarjetas de red**

- **Inalámbricas:** Son utilizadas por lo regular por dispositivos móviles los cuales envía la información mediante ondas electromagnéticas. Existen distintos tipos de tarjetas los cuales se muestra en la Figura 4.11

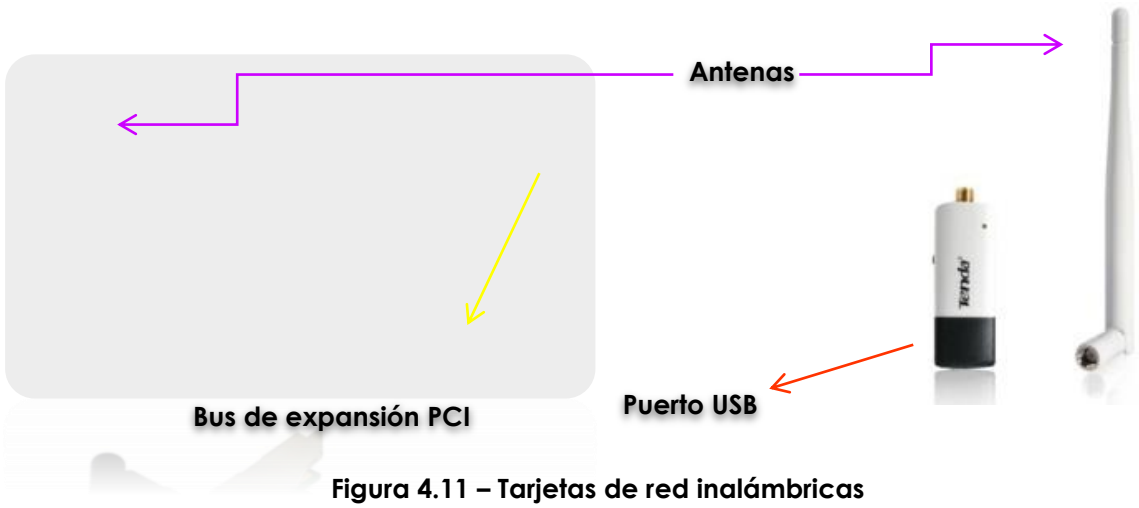



**Figura 4.11 – Tarjetas de red inalámbricas**

Las tarjetas de red independientemente del tipo que se trate ya sea inalámbrica o alámbrica utilizan el protocolo TCP/IP el cual proporciona una transmisión confiable de paquetes de datos entre equipos de sistemas operativos distintos que se encuentran en una red. El protocolo TCP/IP proviene de dos protocolos importantes, el TCP (Protocolo de Transmisión de Control) e IP (Protocolo de Internet), éste es el responsable de direccionar los paquetes para que lleguen a su destino, esta dirección IP puede ser asignada estáticamente o dinámicamente por un servidor central.

## Problemática

El departamento de redes de una importante empresa de autotransportes ha recibido 3 solicitudes urgentes, las cuales se describen a continuación:

- El equipo de cómputo del director de ventas no tiene acceso a Internet.
- Se acaba de publicar una nueva página Web de ventas por Internet y desde la red interna los usuarios no pueden ingresar a dicho sitio.
- El departamento de finanzas tiene fuera de producción el servidor FTP donde se almacenan las facturas diarias.

De acuerdo al siguiente diagrama de red de la Figura 4.12, los ingenieros de soporte deben analizar y resolver la situación.

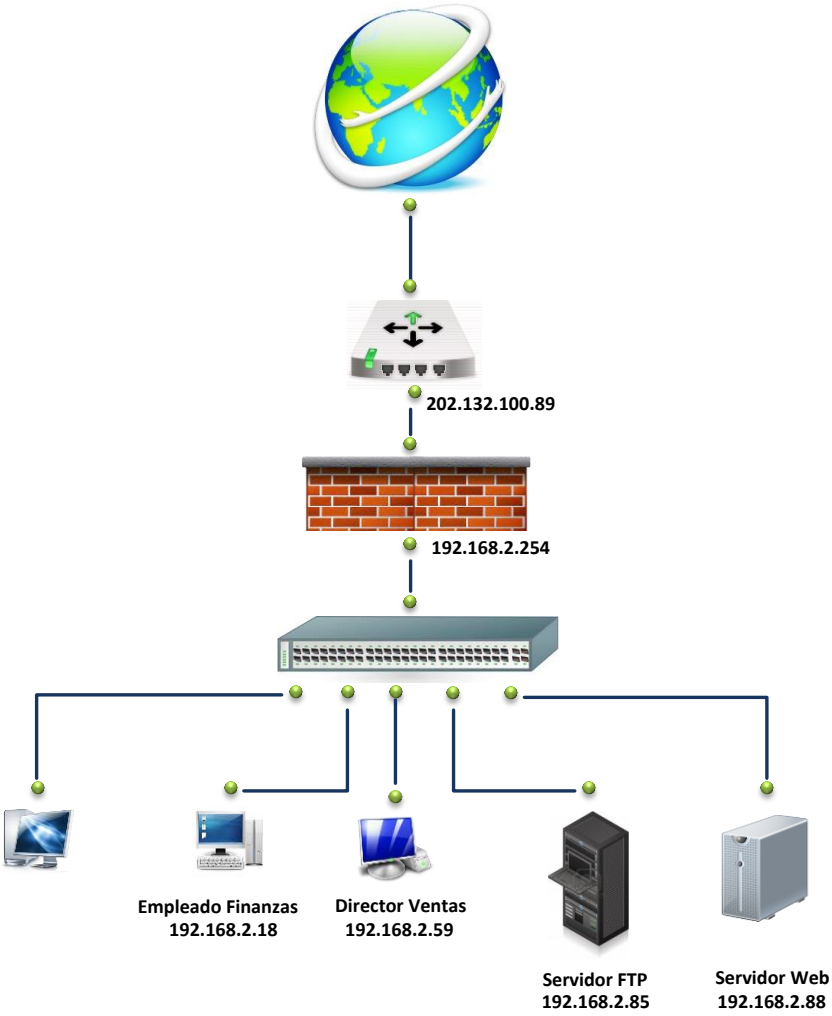



**Figura 4.12 – Diagrama de red empresa autotransportes**

Realiza todas las pruebas de conectividad que permitan obtener la información necesaria para resolver el problema, muestre los resultados obtenidos y brinde una explicación de cada uno de ellos.

**Respuesta esperada:**

Ejecutar los siguientes comandos para validar que existe comunicación con todos los puntos de la red.

- Ping de todos los host hacia el Gateway 192.168.2.254
- Ping del empleado de finanzas hacia el Servidor FTP
- Ping de todos los host hacia Internet
- Traceroute de los host hacia el servidor FTP y Web
- Traceroute hacia Internet

Los alumnos deben mostrar las pantallas de los resultados obtenidos.

Una vez analizadas las pruebas de conectividad, los ingenieros deben entregar una serie de actividades propuestas para identificar cuál es la falla por la cual los servicios no están disponibles, debido a que serán evaluadas para otorgarles un tiempo determinado para efectuar los cambios.

**Respuesta esperada.**

- Verificar el direccionamiento de cada dispositivo, el cual debe coincidir con el diagrama de red proporcionado.
- Verificar el tipo de direccionamiento utilizado en cada uno de ellos y determinar qué método es el adecuado para el servicio.
- Validar que todos los equipos tengan salida a Internet.
- Investigar qué Sistema Operativo tiene instalado cada equipo de cómputo y también cómo se lleva a cabo la configuración de la tarjeta de red inalámbrica o alámbrica en esas plataformas.
- Solicitar la información adicional.
  - Máscaras de red
  - Gateway configurado
  - Servidores DNS

## Actividad a realizar

Una vez recopilada y organizada toda la información que el equipo de soporte proporcionó, la compañía les brinda únicamente 30 minutos para realizar las configuraciones. Para considerar que el problema fue resuelto es necesario presentar pruebas de conectividad de los siguientes equipos.

**Servidor FTP**

- Realizar las configuraciones propuestas y validar que tenga salida a Internet.
- Validar que el servicio al que deben ingresar esté disponible.
- Verificar que el departamento de finanzas pueda realizar la carga y descarga de archivos en el servidor FTP.

**Servidor Web**

- Realizar las configuraciones propuestas y validar que tenga salida a Internet.
- Validar que el servicio al que deben ingresar esté disponible.
- Verificar que desde la red interna se tenga acceso al portal Web de ventas en línea.

**Equipo del Director de Ventas**

- Realizar las configuraciones necesarias y brindarle salida a Internet.

Una vez concluida la configuración, los ingenieros realizaran la entrega de un reporte de las actividades realizadas.

# Laboratorio 3.- Configuración de redes Virtuales (VLANs)

## Laboratorio 3.1 Configuración básica de VLANs

### Objetivo

El alumno investigará y aplicará los procedimientos necesarios para realizar las configuraciones de VLANs en un Switch, sin importar el fabricante del dispositivo que se esté configurando.

### Materiales y Equipo

- Switch capa 2 administrable
- Cables para realizar la interconexión de los dispositivos.
- Simulador de red (Si no se tiene físicamente los dispositivos).

### Introducción

Una VLAN es una red de área local que agrupa un conjunto de equipos de manera lógica y no física, Los administradores de red configuran las VLANs mediante software en lugar de hardware lo que las hace más flexibles, si se llega a presentar un nuevo requerimiento de crecimiento de la red.

La tecnología de VLANs basa su funcionamiento en la utilización de Switches, de tal manera que estos permiten un control más inteligente del tráfico de la red ya que trabajan a nivel de capa 2, además permite el aislamiento del tráfico entre distintas subredes, para que de ésta manera la eficiencia de la red se incremente. Existen distintos tipos de VLANs, las cuales se clasifican dependiendo su uso, a continuación se enlistas éstas:

- VLAN de datos: Este tipo es configurado para enviar tráfico de datos generados por los usuarios, a este tipo de VLANs también se lo conoce como VLAN de usuarios.

- VLAN predeterminada: Es la VLAN a la cual pertenecen todos los puertos de Switch por defecto cuando se enciende el Switch.

- VLAN Nativa: Esta asignada a un puerto troncal 802.1Q, este tipo de puertos admiten tráfico que llega de distintas VLAN.

- VLAN de administración: Es una VLAN que sirve para realizar la administración de los Switch, por defecto la VLAN 1 sirve para llevar a cabo esta tarea en el caso que no se defina otra para este uso, es aconsejable no utilizar la VLAN de administración por defecto.

Algunas de las ventajas que conlleva utilizar VLANs son:

- Aumento en la Seguridad: Cuando se tiene información sensible y que solamente es manejada por algunas personas, es posible manejar subredes independientes, para que el personal autorizado solo pueda tener acceso a ésta.

- Mayor rendimiento: la división de redes planas en múltiples grupos lógicos de trabajo, disminuyen el tráfico innecesario en la red, aumentando así el rendimiento de la red.

- Eliminación de dominios de broadcast: Al dividir una red en VLANs, reducirá en gran medida el número de dispositivos que pertenecen a un dominio de broadcast.

- Flexibilidad en la administración: Brinda una mayor administración en los cambios que se realizan sobre la red, ya que la arquitectura puede cambiarse usando los parámetros de los Switches.

Las VLANs se pueden clasificar según la forma de asignación de los puertos de un Switch. Sin embargo otra manera de clasificar las VLANs dependerá del tipo de información que utilice el Switch para agrupar los dispositivos de una manera lógica. De acuerdo a lo explicado anteriormente se pueden clasificar en:

- VLAN estáticas: Se definen de manera permanente la relación entre los puertos del Switch y la VLAN a la cual pertenece.

- VLAN dinámicas: Los puertos del Switch determinan de manera automática su asignación a una VLAN. Esto es cuando un equipo se conecta a un puerto que no pertenece a ninguna VLAN y transmite una trama, el Switch detecta la dirección MAC y busca a qué VLAN pertenece en su base de datos y automáticamente configura el puerto con las características de la VLAN correspondiente.

- VLAN basada en el puerto o protocolo: El Switch utilizará los números de puertos para hacer la agrupación lógica de usuarios. Es decir, el Switch clasificará el tráfico recibido según el tipo de protocolo del paquete de nivel de red que reciba.

Las VLANs son asociadas a un ID para su identificación, y algunos dispositivos tienen la opción de colocarles un identificador o nombre. Los ID que pueden ser utilizados para asignar a una VLAN son:

- Rango Normal: Son utilizadas en redes de tamaño pequeño a medinas, su rango de ID se encuentra entre 1 al 1001.

- Rango extendido: éstas son utilizadas por los Proveedores de servicios, para que amplíen su infraestructura para brindar servicios a más clientes, los ID utilizados están entre 1006 al 4094.

- ID reservados: ID 1 (Utilizada como VLAN predeterminada) y 1002 al 1005 (Esta reservada para las VLAN Token Ring y FDDI).

## Problemática

La Escuela Secundario No. 8, ha pedido al maestro encargado de la Red, una nueva restructuración de la red, ya que se ha presentado lentitud en la red, así como problemas de seguridad. Para ello el maestro Contrató a un consultor para que proponga una solución al problema que se presenta y le explica el problema que se tiene, después de la junta para realizar el levantamiento de la información, identifica que existen 3 grupos principalmente que ocupa la red los cuales son:

- Maestros.
- Alumnos.
- Administrativos.

Además existen algunos servidores a los cuales solo pueden tener acceso algunas áreas tales como:

- Servidor de calificaciones, solo tiene acceso profesores.
- Servidores de Historial académico, acceso habilitado para profesores.
- Base de datos de Información de alumnos y personal, el cual está limitado a personal administrativo.

Después de haber analizado la información recopila, el consultor propone una solución, la cual consiste en dividir la red en tres segmentos distintos uno para alumnos, profesores y personal administrativo, cada uno tendrá un direccionamiento y una VLAN asignada, en la Figura 4.13 se observa el diagrama de red presentado, así como en la Tabla 4.7 el direccionamiento propuesto.

**Respuesta esperada:**

El direccionamiento de red y el diagrama de red propuesto, puede ser modificado por el profesor dependiendo de las actividades y criterios utilizados en la práctica.

**Tabla 4.7 – Direccionamiento VLAN**

| Nombre | ID | ID de red | Broadcast |
|---|---|---|---|
| Alumnos | 8 | 192.168.10.0/24 | 192.168.10.255 |
| Profesores | 9 | 192.168.20.0/24 | 192.168.20.255 |
| Administrativos | 10 | 192.168.30.0/24 | 192.168.30.255 |

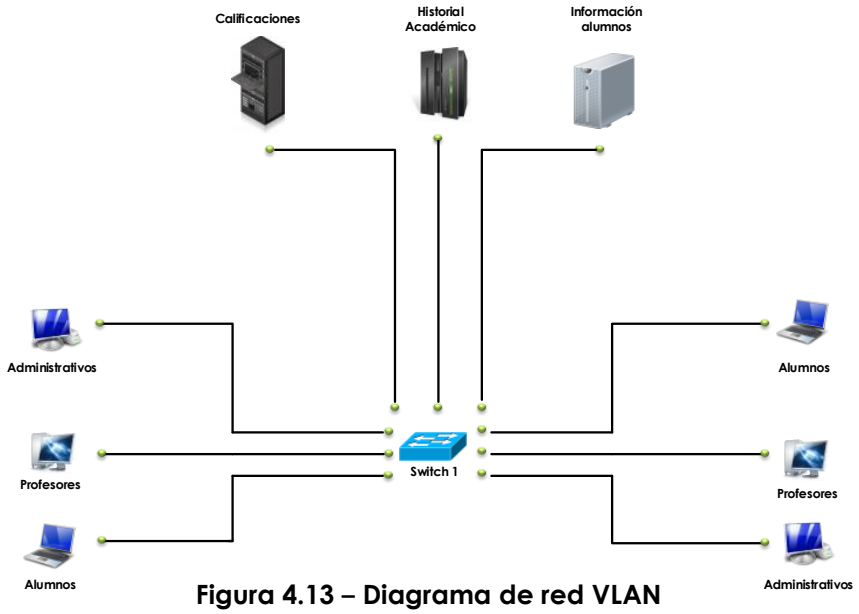



**Figura 4.13 – Diagrama de red VLAN**

## Actividad a Realizar

Antes de realizar las configuraciones pertinentes, comente en grupo la solución propuesta y qué acciones realizaría para aumentar la seguridad en la red.

Después de haber validado y comentado la propuesta, es preciso realizar las configuraciones necesarias para que la red sea total mente funcional. Para ello es necesario investigar cómo realizar éstas.

**Respuesta esperada:**

La forma en la que los equipos sean configurados dependerá del fabricante del dispositivo en cuestión, sin embargo se deben de realizar las siguientes configuraciones:

- Realizar las configuraciones básicas en el Switch tales como nombre, configuración de contraseñas de administración, mensajes, seguridad en puertos, entre otros.
- Creación de VLANs, así como la asignación a cada interfaces.
- Configuración de parámetros de red, tanto en los servidores como en los equipos.

Una vez realizadas las configuraciones, es necesario realizar pruebas de conectividad para garantizar que exista comunicación entre los dispositivos. ¿Cuáles realizarías? ¿En caso de que exista algún problema con la comunicación que haría para solucionar el problema?

**Respuesta esperada:**

El alumno deberá investigar, con qué comandos u opciones gráficas, cuentan los dispositivos utilizados en esta práctica para realizar troubleshooting.

# Laboratorio 3.2 Configuración de enrutamiento entre VLANs

## Objetivo

El alumno investigará y realizará las configuraciones necesarias para proporcionar comunicación entre distintas VLANs, sin importar el fabricante del dispositivo que se utilice. Además pondrá en práctica los conocimientos adquiridos en prácticas pasadas.

## Materiales y Equipo

- Switches capa 2 administrable.
- Router.
- Cables para realizar la interconexión de los dispositivos, así como su para configuración.
- Simulador de red (Si no se tiene físicamente los dispositivos).

## Introducción

Como se explicó en la práctica pasada las VLANs son redes lógicas que ayudan a tener un mayor control sobre la red, así como el eliminar dominios de broadcast, aumenta la seguridad y facilita la administración de la red y más, sin embargo al hablar de VLAN también tenemos que tomar en cuenta otros concepto tales como Enlaces troncales.

Cuando un puerto del Switch pertenece a una VLAN predeterminada es llamada puerto de acceso, mientras que un puerto que envía información de distintas VLANs a través de un enlace punto a punto se le conoce como enlace troncal o puerto troncal.

La principal función de los enlaces troncales es transmitir información de distintas VLANs sobre un mismo cable, sin la utilización de éstos sería necesario contar con distintos puertos del Switch dedicados a cada una de las VLANs que transmiten tal y como se muestra en la Figura 4.14.

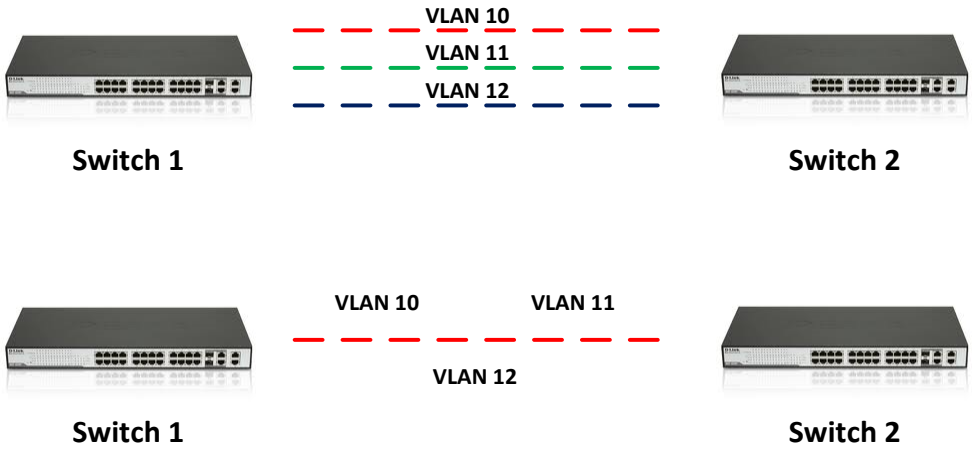



**Figura 4.14 – Enlace Troncales**

Los enlaces troncales se rigen bajo el protocolo 802.1Q, el cual fue desarrollado como un mecanismo que permita a múltiples redes interconectadas a través de Switches o Routers compartir transparentemente el mismo medio físico de transmisión sin problema de interferencia éntrelas redes que comparten el medio.

## Problemática

Una empresa transnacional decide expandir sus oficinas, y hacer una restructuración de su red interna debido a que actualmente todos sus trabajadores comparten un mismo segmento de red. El departamento de Networking identificó que es necesario dividir la red por departamento, así como tener un segmento especial para los servidores. Desafortunadamente les fue asignado poco presupuesto para realizar las modificaciones, por tal motivo el directo de Networking decide elaborar un inventario y saber con qué recursos cuentan para hacer la restructuración, al llevar a cabo el inventario obtiene la siguiente información:

- 1 Router de 4 puertos FastEthernet 10/100/1000.
- 3 Switches con 50 puertos FastEthernet 10/100/1000.
- 1 Firewall con módulo de UTM.

Después de haber obtenido el inventario se realizó una reunión para estructurar la red con base en los dispositivos con los que cuentan así como los requerimientos que se presentan. La información recopilada con base en los usuarios y áreas se muestra en la tabla 4.8.

**Tabla 4.8 – Número de usuarios por Área**

| Área | Número de Usuarios |
|---|---|
| **Bodega** | 20 (+20) |
| **Recursos Humanos (RH)** | 10(+10) |
| **Contaduría** | 15(+10) |
| **Desarrollo** | 30(+10) |
| **Managers** | 20(+10) |
| **TI** | 20(+10) |
| **Servidores** | 10(+10) |

Al haber analizado la información, se estableció que solo ciertos departamentos deberían tener la posibilidad de comunicarse con el servidor de base de datos tales como managers, contaduría, recursos humanos y desarrollo, el área de TI debe ser capaz de comunicarse con todas las áreas, así mismo todas las área deben ser capaces de comunicarse con el servidor de correos.

Para realizar el direccionamiento se utilizó el segmento de red 192.168.10.0/23. Tomando como base el número de host por cada área, realice los cálculos necesarios para obtener el direccionamiento utilizando el método VLSM y complete la tabla 4.9.

**Respuesta esperada:**

El direccionamiento de red propuesto, puede ser modificado por el profesor dependiendo de las actividades y criterios utilizados en la práctica.

| Tabla 4.9 –Direccionamiento propuesto empresa transnacional. | | | |
|---|---|---|---|
| **Nombre** | **ID VLAN** | **ID de red** | **Broadcast** |
| Bodega | 56 | 192.168.10.0/26 | 192.168.10.63 |
| Desarrollo | 55 | 192.168.10.64/26 | 192.168.10.127 |
| Managers | 54 | 192.168.10.128/27 | 192.168.10.159 |
| TI | 53 | 192.168.10.160/27 | 192.168.10.191 |
| Contaduría | 52 | 192.168.1.192/27 | 192.168.10.223 |
| Recursos humanos | 51 | 192.168.10.224/27 | 192.168.10.255 |
| Servidores | 50 | 192.168.11.0/27 | 192.168.11.31 |

Una vez realizado el análisis de la información y haber obtenido el direccionamiento que será utilizado en cada departamento, es necesario realizar el diagrama de red, en la Figura 4.15 se presenta el diagrama de red propuesto.

**Respuesta esperada:**

El diagrama de red propuesto, puede ser modificado por el profesor dependiendo de las actividades y criterios utilizados en la práctica.

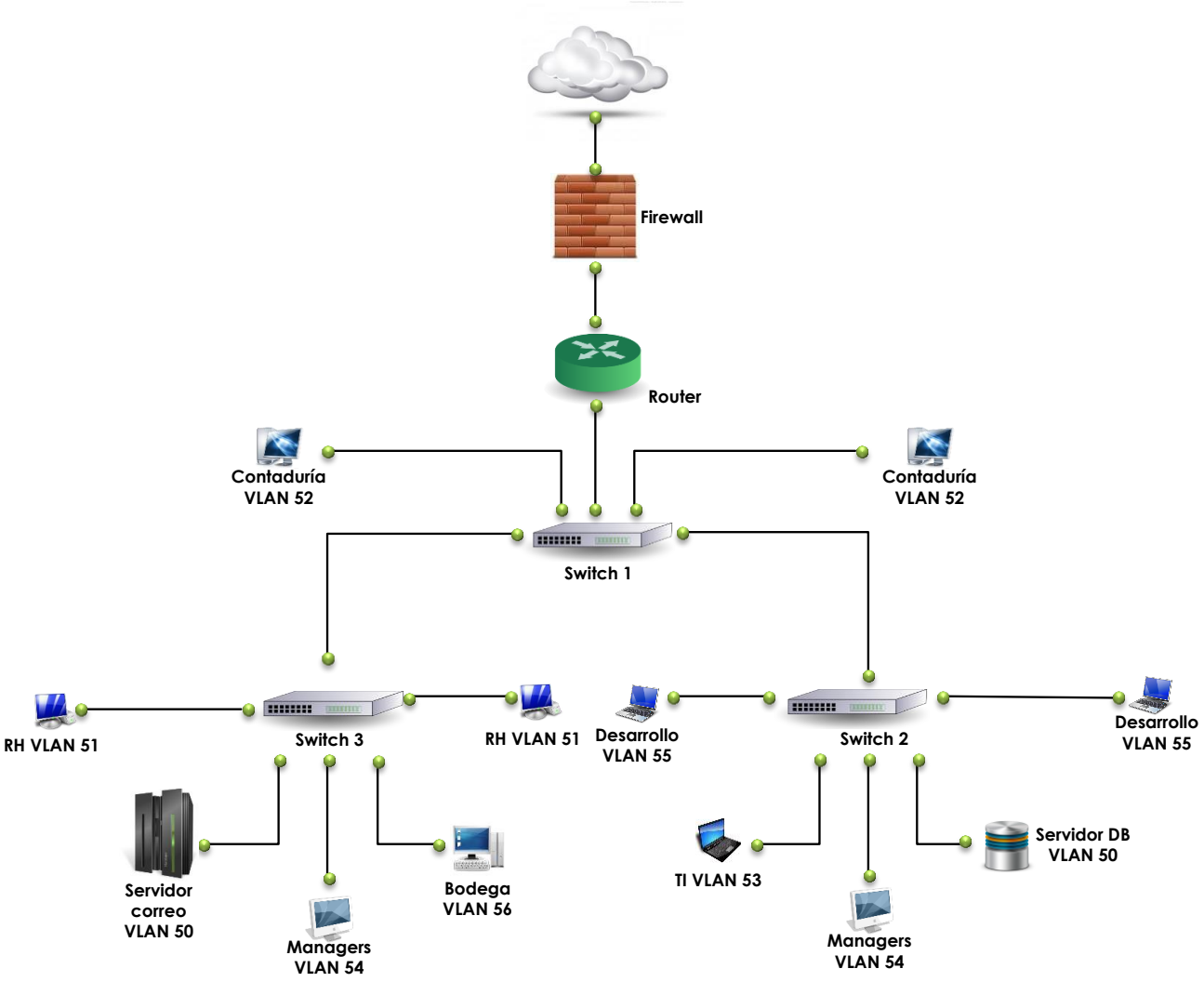



**Figura 4.15 – Diagrama de red empresa transnacional**

## Actividad a Realizar

Antes de realizar las configuraciones necesarias, comente si el diagrama propuesto es el óptimo o qué cambios realizaría para optimizarlo.

**Respuesta esperada:**

Las respuestas pueden variar dependiendo los conocimientos del alumno

Después de haber validado y comentado la propuesta, es preciso realizar las configuraciones necesarias para que la red sea total mente funcional. Para ello es necesario investigar cómo realizar éstas.

**Respuesta esperada:**

La forma en la que los equipos sean configurados dependerá del fabricante del dispositivo en cuestión, sin embargo se deben de realizar las siguientes configuraciones:

- Realizar las configuraciones básicas
- Creación de VLANs y creación de enlaces troncales
- Configuración de parámetros de red, tanto en los servidores como en los equipos.

Una vez realizadas las configuraciones, es necesario realizar pruebas de conectividad para garantizar que exista comunicación entre las VLANs existentes tal y como se pide en los requerimientos. ¿Cuáles realizarías? ¿En caso de que exista algún problema con la comunicación que realizarías para solucionar el problema?

**Respuesta esperada:**

El alumno deberá investigar, con qué comandos u opciones gráficas, cuentan los dispositivos utilizados en esta práctica para realizar troubleshooting. Para que exista comunicación entre las distintas VLANs, es necesario hacer configuraciones en los Routers para que estos sepan cómo hacer la comunicación entre VLANs.

# Laboratorio 4.- Configuración de protocolos de enrutamiento

## Laboratorio 4.1 RIP

### Objetivo

El alumno analizará y llevará a cabo la configuración del protocolo de enrutamiento RIP V1 o RIP V2, para establecer la comunicación entre distintas redes las cuales se encuentran en distintos Routers.

### Materiales y Equipo

- Routers.
- Cables para realizar la interconexión de los dispositivos, así como para su configuración.
- Simulador de red (Si no se tiene físicamente los dispositivos).

### Introducción

La función principal de un Router es realizar el encaminamiento de paquetes hacia su dirección destino, para realizar esto el Router necesita consultar una tabla de enrutamiento la cual posee almacenada la información de las rutas sobre las redes que están conectadas directamente a él así como las remotas. Las tablas de enrutamiento contienen asociaciones, estas le indican al Router que cierto destino puede ser alcanzado con una mayor facilidad enviándolo a un Router en particular.

Los protocolos de enrutamiento se clasifican de acuerdo a su método de enrutamiento ya sea dinámico o estático, protocolos de Gateway interior o exterior y demás. Dentro de los protocolos dinámicos se encuentra RIP V1 y RIP V2, estos protocolos tienen las características que son protocolos de Gateway interior y vector distancia.

RIP V1 es un protocolo de enrutamiento con clase, esto quiere decir que basa su funcionamiento en las clases de la IP ya sea tipo A, B o C, al tener esta característica, este tipo de enrutamiento no envía información de la máscara de subred en las actualizaciones de las tablas de enrutamiento. RIP V2 al contrario de la versión 1 es un protocolo de enrutamiento sin clase, el cual incluye la máscara de red en las actualizaciones de las tablas de enrutamiento.

Dentro de las características principales que presenta RIP en sus dos versiones se encuentran:

- Utiliza como métrica el conteo de saltos para seleccionar la mejor ruta.
- Si el conteo de saltos excede o es mayor a 15, el protocolo no es capaz de proveer una ruta para la red destino.

- Envía las actualizaciones de los enrutamientos cada 30 segundos a través de broadcast o multicast dependiendo la versión.

Entre las mejoras que se introdujeron para el protocolo RIPV2 se encuentran:

- Dentro de las actualizaciones de enrutamiento se incluye la máscara de subred.
- Posee un mecanismo de autenticación para la seguridad de la actualización de las tablas de enrutamiento
- Admite VLSM.
- Utiliza direcciones multicast en vez de broadcast.
- Admite sumarización manual de rutas.

Una de las desventajas de este protocolo es que solo puede ser utilizado en redes de tamaño pequeño, aun así es uno de los más utilizados debido a su fácil implementación.

## Problemática

Una empresa automotriz desea estructurar de nuevo su red ya que lo consideran obsoleta y poco funcional, para ello llevó a cabo un concurso para seleccionar a la consultoría que llevará a cabo la implementación de la red. Después de calificar a cada participante, la empresa PEER fue seleccionada para realizar el proyecto.

Durante la junta inicial se identificó que la red consta de 4 sucursales, cada una de ellas con distintos departamentos, en la Tabla 4.10 se muestran los departamentos existentes por cada sucursal.

**Tabla 4.10 – Departamentos existentes por localidad**

| Sucursal | Departamento | Empleados |
|---|---|---|
| Corporativo México | Presidencia | 80 |
| | Ingeniería | 50 |
| | Contabilidad | 30 |
| | Recursos Humanos | 10 |
| | Servidores | 40 |
| Corporativo Guadalajara | vicepresidencia | 30 |
| | Diseño automotriz | 20 |
| | Contabilidad | 5 |
| | Recursos Humanos | 5 |
| | Servidores | 20 |
| Planta Puebla | Ensamble 1 | 50 |
| | Ensamble 2 | 30 |
| Planta Querétaro | Ensamble 1 | 50 |
| | Ensamble 2 | 30 |

Dentro de los requerimientos obtenidos durante la junta inicial, se pidió que la red estuviera dividida en distintas subredes, cada una con direccionamiento distinto, con base en lo aprendido y desarrollado en prácticas pasadas, proponga el direccionamiento a utilizar en la red y presente un diagrama de red de cómo quedaría implementada.

### Respuesta esperada:

El direccionamiento de red y el diagrama esperados serán variable debido a que el alumno será el encargo de proponer la solución, a continuación se observa en la Figura 4.16 y en la Tabla 4.11 una posible solución.

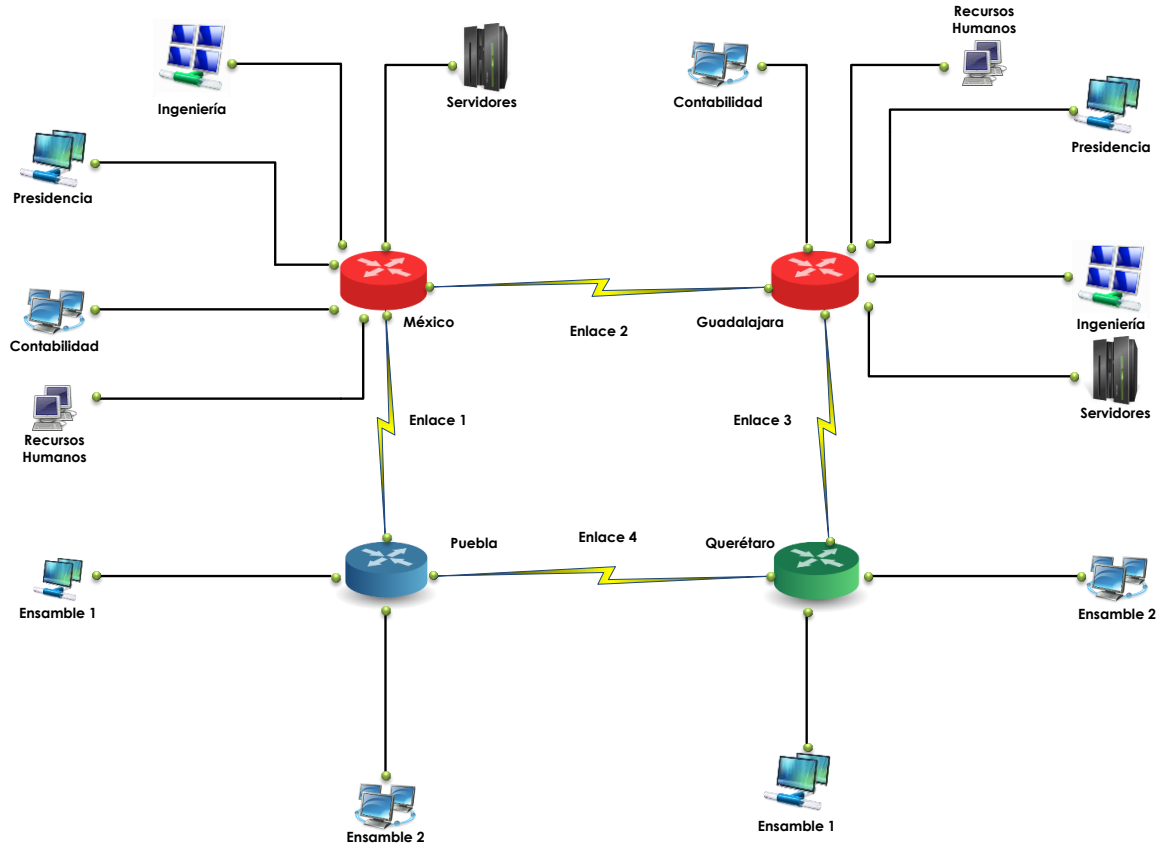



**Figura 4.16 – Diagrama de red Propuesto empresa automotriz**

**Tabla 4.11 – Direccionamiento de red propuesto empresa automotriz**

| Sucursal | Departamento | ID de Red | Broadcast |
|---|---|---|---|
| Corporativo México | Presidencia | 192.168.10.0/25 | 192.168.10.127 |
| | Ingeniería | 192.168.10.128/26 | 192.168.10.191 |
| | Contabilidad | 192.168.11.0/27 | 192.168.11.31 |
| | Recursos Humanos | 192.168.11.32./28 | 192.168.11.47 |
| | Servidores | 192.168.10.192/26 | 192.168.10.225 |
| Corporativo Guadalajara | Vicepresidencia | 192.168.200.0/27 | 192.168.20.31 |
| | Diseño automotriz | 192.168.20.32/27 | 192.168.20.63 |
| | Contabilidad | 192.168.20.96/29 | 192.168.20.103 |
| | Recursos Humanos | 192.168.20.104/29 | 192.168.20.111 |
| | Servidores | 192.168.20.64/27 | 192.168.20.95 |
| Planta Puebla | Ensamble 1 | 10.150.44.0/26 | 10.150.44.63 |
| | Ensamble 2 | 10.150.44.64/27 | 10.150.44.95 |
| Planta Querétaro | Ensamble 1 | 10.200.200.0/26 | 10.200.200.63 |
| | Ensamble 2 | 10.200.200.64/27 | 10.200.200.95 |
| Enlace 1 | - | 172.16.80.40/29 | 172.16.80.47 |

| | | | |
|---|---|---|---|
| Enlace 2 | - | 172.16.70.96/29 | 172.16.70.103 |
| Enlace 3 | - | 172.120.90.144/29 | 172.120.90.151 |
| Enlace 4 | - | 172.160.10.8/29 | 172.160.10.15 |

## Actividad a Realizar

Antes de realizar las configuraciones necesarias exponga el diagrama diseñado, así como el direccionamiento realizado para dicho diagrama. Comenten y validen cuál de los diagramas propuestos es el más óptimo.

**Respuesta esperada:**

Las respuestas pueden variar dependiendo los conocimientos del alumno

Después de haber validado y comentado la propuesta, es preciso realizar las configuraciones necesarias para que la red sea total mente funcional. Para ello es necesario investigar cómo realizar éstas.

**Respuesta esperada:**

La forma en la que los equipos sean configurados dependerá del fabricante del dispositivo en cuestión, sin embargo se deben de realizar las siguientes configuraciones:

- Configuraciones básicas en el Router
- Configuración de protocolo de enrutamiento RIPV1 o RIPV2

Una vez realizadas las configuraciones, es necesario realizar pruebas de conectividad para garantizar que exista comunicación entre los distintos segmentos de red.

**Respuesta esperada:**

El alumno deberá investigar, con qué comandos u opciones gráficas, cuentan los dispositivos utilizados en esta práctica para realizar troubleshooting. Algunos comandos que serán utilizados, son los proporcionados por el fabricante y deben ser ejecutados desde los Routers, otros comandos tales como ping y tracert o traceroute, serán ejecutados desde los equipos que se encuentran en la red.

# Laboratorio 4.2 OSPF

## Objetivo

El alumno investigará en qué consiste el Protocolo de ruteo OSPF, además analizará y llevará a cabo las configuraciones necesarias para establecer la comunicación entre distintas redes.

## Materiales y Equipo

- Routers.
- Cables para realizar la interconexión de los dispositivos, así como para su configuración.
- Simulador de red (Si no se tiene físicamente los dispositivos).

## Introducción

El protocolo OSPF (Open Shortes Path First), fue desarrollado por el Interior Gateway Protocol working group del IETF, este grupo fue creado en 1988 para realizar el diseño de un protocolo de Gateway interior, basado en el algoritmo del camino más corto. OSPF fue creado debido a que RIP era incapaz de servir a un gran número de redes heterogéneas. Este protocolo, fue el resultado del esfuerzo de distintas personas la cuales crearon el algoritmo SPF (Shortest Path First) conocido como algoritmo de Dijkstra.

OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red mediante tablas de enrutamiento la cual contiene información sobre sistemas locales y vecinos. De esta manera es capaz de calcular que distancia hay para cada posible ruta y luego escoge que ruta es la más corta para acceder a su destino. Para calcular que ruta es la más rápida también se tiene en cuenta por donde pasa y el estado de los enlaces, cosa que por ejemplo, en el caso de RIP se calcula sólo la distancia y no el tráfico del enlace, por esta causa OSPF es un protocolo de encaminamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de encaminamiento distribuida y de rápida propagación.

Algunas características que presenta OSPF son:

- Rápida detección de cambios en la topología de la red
- División de tráfico para varios rutas equivalentes
- Autenticación
- Acepta VLSM

## Problemática

Una universidad actualmente se encuentra localizada en un edificio de 4 pisos, debido a la alta demanda a la que se está enfrentando decidió mudarse a un conjunto de 3 edificios. Durante la migración, se contrató a una compañía especializada en la instalación y configuración de redes. Durante las juntas se dieron a conocer los

requerimientos con los cuales debe de cumplir la red. El líder de proyecto encargado de la implementación identificó lo siguiente:

- Existen distintos departamentos, cada uno tendrá un direccionamiento propio.
- Se debe contar con un segmento especial para servidores.
- La convergencia de la red debe ser lo más rápido posible.

Después de haber analizado los requerimientos solicitados, el equipo de ingenieros asignados para realizar el proyecto, decidió utilizar OSPF como protocolo de enrutamiento, así como el diagrama de red mostrado en la Figura 4.17.

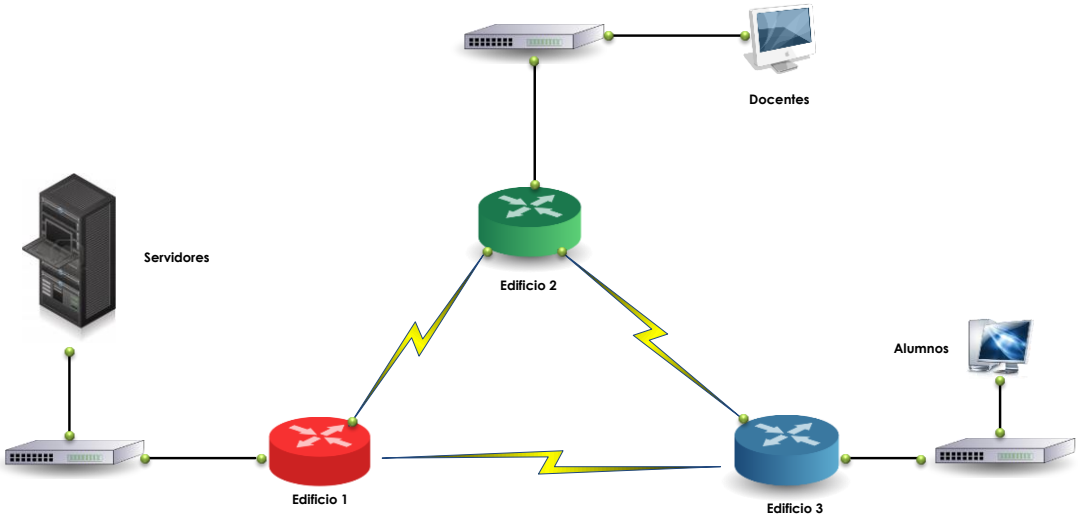



**Figura 4.17 – Diagrama de red OSPF**

## Actividad a Realizar

Antes de realizar las configuraciones necesarias, analice el diagrama de red presentado y comente qué acciones realizaría para llevar a cabo el enrutamiento.

**Respuesta esperada:**

El alumno propondrá la forma en la que debe ser configurado OSPF, configurando los parámetros necesarios que utiliza el fabricante del dispositivo.

Realice las configuraciones necesarias en los Routers para configurar el enrutamiento con OSPF y haga pruebas de comunicación entre las diferentes subredes.

**Respuesta esperada:**

Las configuraciones y comandos utilizados dependerán de la marca del dispositivo que se esté utilizando. En principio todos los dispositivos trabajan bajo el mismo principio, lo que difiere es la forma en la que se configuran.

Después de haber configurado y realizado las pruebas de comunicación, desconecte uno de los enlaces entre lo Routers y anote que es lo que sucede cuando realiza esto, ¿Sigue existiendo comunicación entre las red?, ¿Cuál es la ruta que sigue para llegar a las redes después de haber desconectado el enlace?

**Respuesta esperada:**

Aunque se desconecte uno de los enlaces los Routers, estos encontrarán alguna ruta por la cual establecer la comunicación entre las redes. El comando tracert o tracerout, puede indicar el camino que sigue un paquete hasta su destino.

# Laboratorio 5.- Instalación y configuración de servicios

## Laboratorio 5.1 Configuración de un servidor FTP

### Objetivo

El alumno realizará la instalación y configuración de un servidor FTP en distintos sistemas operativos, además de hacer pruebas para verificar su correcto funcionamiento.

### Materiales y Equipo

- Máquinas Virtuales con diversos sistemas Operativos.
- Software para instalar servidor FTP.
- Analizador de protocolos.

### Introducción

FTP es un protocolo que permite la transferencia de archivos entre dos equipos, éste se encuentra definido en el RFC 959. La arquitectura que sigue este servicio es cliente/ servidor, esto quiere decir que es necesario tener dos programas los cuales trabajan de la siguiente manera:

- El cliente FTP se encarga de la conexión y la descarga o subir archivos al servidor
- El Servidor FTP ejecuta las peticiones recibidas por el cliente FTP

Cuando el cliente establece la conexión con el servidor FTP lo realiza mediante el puerto 21, este puerto es utilizado como control y el servidor crea el canal de datos a través del puerto 20. La principal desventaja de este protocolo es que el tráfico entre el cliente y el servidor no se encuentra cifrado, esto da pie a que cualquier persona pueda utilizar un sniffer para capturar el nombre y clave utilizadas para autenticarse sobre el servidor. Para solucionar este problema existe la aplicación SFTP (Secure File Transfer Protocol), el cual es un protocolo que proporciona la funcionalidad para transferir y manipular archivos de manera fiable.

### Problemática

Un despacho de contadores tiene un problema el cual tiene que ver con el almacenamiento de la información que maneja cada uno de sus empleados. Se dieron cuenta que los empleados almacenaban toda la información de sus clientes en sus computadoras, sin embargo esta información debe ser consultada por distintas personas que pertenecen a otras áreas.

El dueño de la empresa decidió contratar a un especialista que le ayudara a resolver este problema, pero al exponer su necesidad, el dueño puso en claro que no contaba con los recursos económicos necesarios para realizar una implementación costosa.

Con base en las necesidades y los recursos con los que cuenta el despacho el especialista decide realizar la publicación de un servidor el cual servirá para cumplir con las necesidades planteadas, en la Figura 4.18 se observa un esquema de la solución.

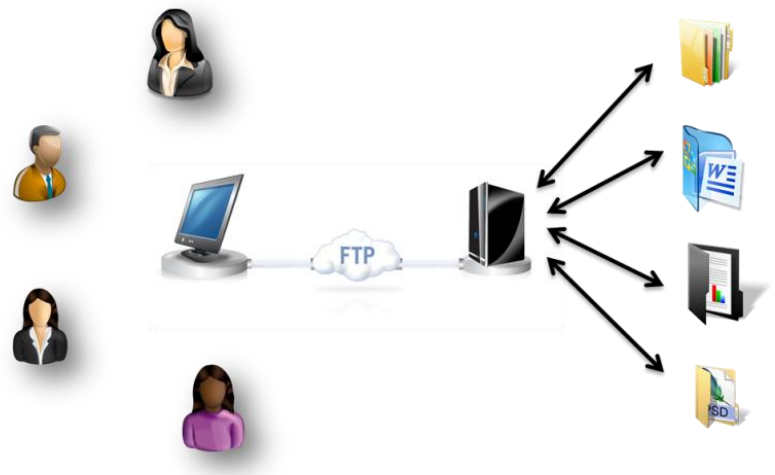



**Figura 4.18 – Implementación servidor FTP**

¿Qué solución daría con base en los requerimientos y limitantes con los que se presenta?

**Respuesta esperada:**

Una posible respuesta es instalar sobre un sistema operativo un servidor FTP en el cual mediante los nombres de usuarios se les brinden niveles de privilegios y acceso a las carpetas que requieren.

## Actividad a Realizar

Realice la instalación y configuración de un servidor FTP, así como la creación de distintos usuarios con diferentes niveles de privilegios. Efectúe diversas pruebas para validar su correcto funcionamiento y anote sus comentarios.

Instale un analizador de protocolos y realice capturas del tráfico que se establece al realizar la conexión con el servidor FTP. Al analizar las capturas ¿qué es lo que puede identificar? Muestra evidencia.

**Respuesta esperada:**

Al analizar todo el tráfico que se genera al establecer la comunicación con el servidor FTP es posible visualizar las credenciales de acceso, esto lo convierte en un servicio vulnerable, por lo que se recomienda utilizar un protocolo seguro, como el SFTP.

Después de haber instalado el servidor FTP y haber analizado el flujo de información entre el cliente y el servidor. ¿Qué realizaría para que la comunicación entre los dos se lleve a cabo de manera segura?

**Respuesta esperada:**

Es necesario utilizar contraseñas seguras, así como utilizar software que garantice la seguridad al momento que se envié la información entre cliente y servido.

# Laboratorio 5.2 Configuración de un servidor Web

## Objetivo

El alumno investigará qué software existe para realizar la publicación de páginas Web, ejecutará la instalación y configuración de un servidor Web en distintos sistemas operativos, además efectuará la publicación de una página Web básica en el servidor instalado.

## Materiales y Equipo

- Máquinas Virtuales con diversos sistemas Operativos.
- Software para instalar servidor Web.
- Una Página Web básica.

## Introducción

Un servidor Web es un programa que está diseñado para publicar páginas web. Este se ejecuta continuamente, esperando que se realicen peticiones por parte del cliente, una vez realizada la petición éste responderá a través de una página web la cual se mostrará en el navegador.

Existen distintos programas que pueden ser utilizados para montar un servidor Web, la elección de estos dependerá de los requerimientos o recursos con los cuales cuente la empresa en donde se llevará a cabo la instalación del servidor. Algunos de los servidores Web que existen son:

-Apache Web Server
-WampServer
-Nginx Web Server
-Microsoft ISS
-XAMPP
-Cherokee Web Server
-Tomcat
-Abyss Web Server

## Problemática

Un Hospital solicita al departamento de sistemas una solución para que los doctores desde su consultorio ingresen a un portal donde se almacena el historial médico de los pacientes, así como hacer modificaciones a éste. Los ingenieros después de analizar los requerimientos y necesidades que surgen, plantean una solución, la cual consiste en realizar una publicación de una página web donde los doctores realicen las tareas solicitadas. Sin embargo en estos momentos el departamento no cuenta con los recursos necesarios para invertir en nueva tecnología la cual ayude a solucionar el problema.

Al realizar una búsqueda dentro de los recursos con los que cuenta el departamento, se obtuvo un servidor con los recursos necesarios de Hardware para publicar el servidor Web.

## Actividad a Realizar

Realice la instalación y configuración de un servidor Web y lleve a cabo la publicación de una página Web, efectúe pruebas de conexión para validar que se tenga acceso correcto a la página publicada.

Con base en sus conocimientos ¿qué haría para mejorar la seguridad en la página y qué haría para optimizar el correcto funcionamiento de la página Web?

**Respuesta esperada:**

Para aumentar la seguridad en la página publicada, lo mejor es utilizar el protocolo https, además de esto incorporar un sistema de autenticación para que solo el personal autorizado tenga acceso a la información.

# Laboratorio 6.- Servicios de autenticación y administración de usuarios

## Laboratorio 6.1 Servicios de directorio activo

### Objetivo

El alumno investigará sobre herramientas y mecanismos manejados para brindar el servicio de identificación de usuarios por directorio activo y realizará las acciones que se requieren para la implementación de éste.

### Materiales y Equipo

- Servidor físico o virtual con mínimo 2 GB en RAM y 40 GB en disco duro.
- Sistema operativo Windows Server 2008 R2 o superior (versión evaluación).
- 2 computadoras con sistema operativo Windows versión profesional.

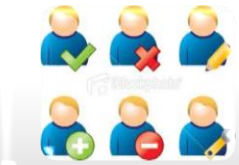
### Introducción

El proceso de autenticación es un componente crítico en la actividad de cualquier red de computadoras, ya que los usuarios deben de autenticarse para hacer huso de algún recurso que la red proporcione. Acceder a una computadora individual o a un sitio web requiere un protocolo de autenticación confiable para ejecutar un proceso de fondo para establecer la verificación del usuario. Estos servicios de autenticación y administración de usuarios se han convertido en un mecanismo de seguridad utilizado en las redes de datos para brindar un mayor control sobre los permisos y recursos a los cuales tiene acceso cada uno de ellos. En gran parte de las organizaciones se tiene la identificación de usuarios implementada principalmente sobre los protocolos que se observan en la Figura 4.19.

En el ámbito de la redes existen diversos programas e implementaciones basadas en estos protocolos para la identificación de usuarios, uno de los más utilizado es el llamada directorio activo (Active Directory) de la compañía Microsoft®. Investigue al menos otros cinco programas existentes para realizar la identificación de usuarios:

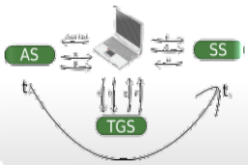
**Respuesta Esperada**

- Novell Directory Services
- iPlanet - Sun ONE Directory Server
- OpenLDAP
- Red Hat Directory Server
- Apache Directory Server
- Open DS
- FreeRADIUS
- Cistron
- GNU Radius
- ICRADIUS



**LDAP**

- **Protocolo Ligero de Acceso a Directorios (LDAP)** es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.




**Kerberos**

- Identifica usuarios implementando una biblioteca grande y compleja de claves encriptadas que sólo asigna la plataforma Kerberos. Estas claves no pueden ser leídas o exportadas fuera de Kerberos.

**RADIUS**

- **De las siglas Remote Authentication Dial-In User Service**. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión

**Figura 4.19 – Servidores de autenticación**

El directorio activo (Active Directory) de Microsoft® actúa como una capa de gestión entre los usuarios y los recursos compartidos el cual trabaja con distintos protocolos entre los que están LDAP, DNS, DHCP y Kerberos es decir, éste se considera como un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas para cada uno de ellos.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso. La estructura de un directorio activo incluye los conceptos que se muestran en la Figura 4.20

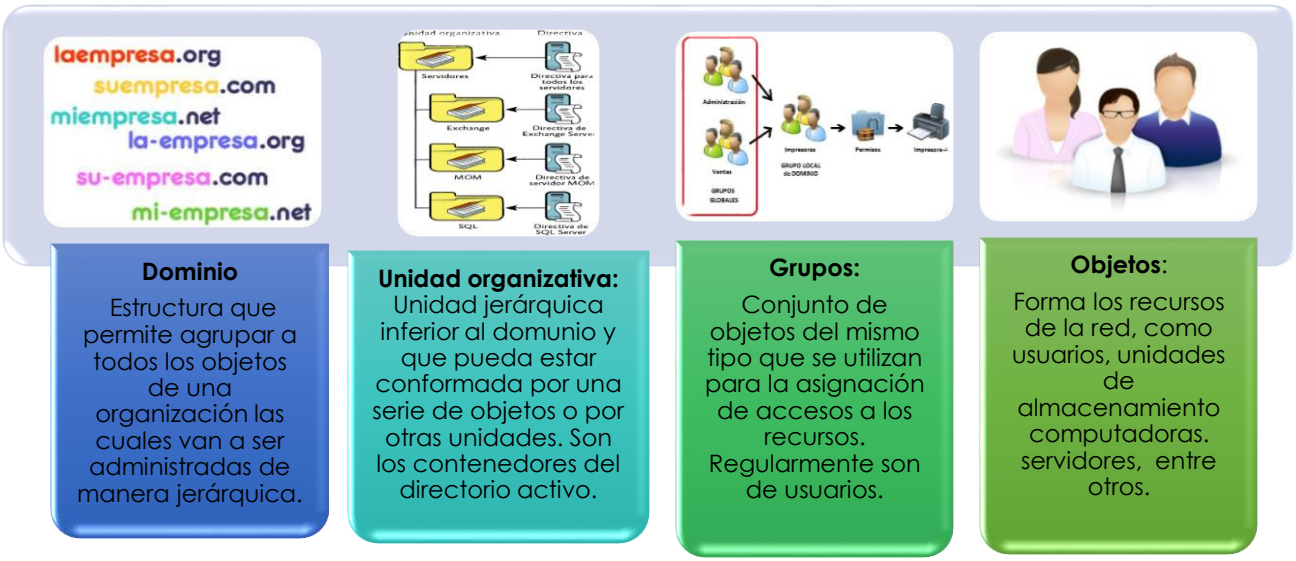



**Figura 4.20 – Estructura directorio activo**

La arquitectura de un directorio activo se basa en árboles de manera jerárquica. Un ejemplo de ello se muestra en la Figura 4.21

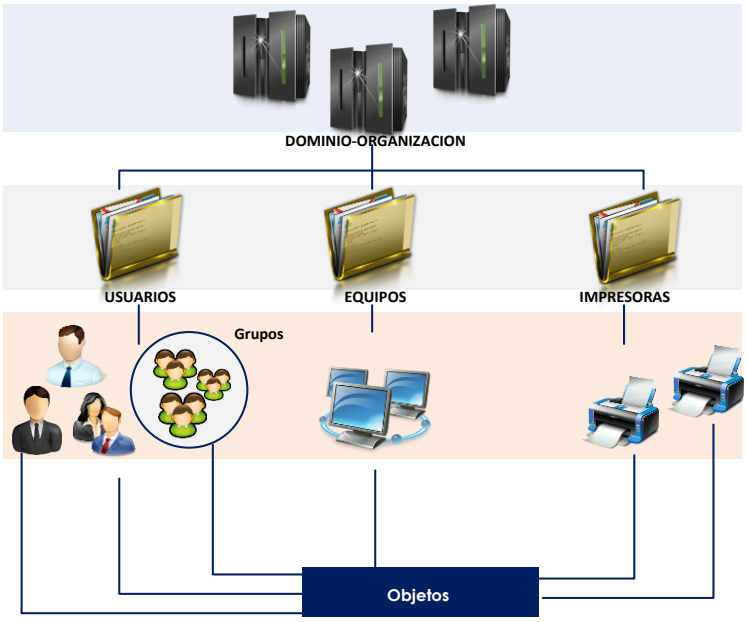



**Figura 4.21 – Arquitectura directorio activo**

## Problemática

El colegio de ingenieros de Monterrey tiene basada su estructura de red únicamente en direccionamiento IP, últimamente le ha ocasionado una gran carga administrativa ya que incrementó a 400 el número de usuarios y su infraestructura de seguridad está basada de acuerdo a la IP asignada. Por tal motivo se necesita cambiar este modelo a uno que le permite identificar a los usuarios, en donde se tenga información como nombre, puesto, departamento, organización por áreas, así como controlar el acceso a los recursos de la organización.

El departamento de seguridad y redes proponen la siguiente arquitectura teniendo a todos los usuarios dentro de la red corporativa asociada a su dominio.

| Dominio: INGENIEROSMTY.COM | |
|---|---|
| **Finanzas (80 usuarios)** | Desarrollo y proyectos (45 usuarios) |
| **Compras (30 usuarios)** | Recursos Humanos (90 usuarios) |
| **Sistemas (50 usuarios)** | Contabilidad (70 usuarios) |
| **Seguridad (40 usuarios)** | Servicios (5 usuarios) |

La información a configurar por DHCP o IP estática a cada usuario se muestra en la Tabla 4.11.

**Segmento de Red: otorgado: 172.16.30.0/23**

**Tabla 4.11 Direccionamiento colegio de ingenieros**

| Usuario | Departamento | IP | Máscara | Gateway | DNS |
|---|---|---|---|---|---|
| Ingmty/usuario1 | Finanzas | 172.16.30.2 | 255.255.254.0 | 172.16.30.1 | 172.16.30.80 |
| Ingmty/usuario2 | Compras | 172.16.30.3 | 255.255.254.0 | 172.16.30.1 | 172.16.30.80 |
| … | …. | …. | … | … | … |
| Ingmty/usuario400 | Sistemas | 172.16.31.254 | 255.255.254.0 | 172.16.30.1 | 172.16.30.80 |

## Actividad a Realizar

Teniendo la información de la propuesta, realice un diagrama en donde se proponga la arquitectura del dominio. Además es necesario investigar y proponer algunas configuraciones de seguridad que puedan realizarse en el servidor de dominio configurado. Anote las configuraciones y justifique.

### Respuesta esperada

Un ejemplo de diagrama de dominio para el colegio de ingenieros se observa en la figura 4.22 conformarse de la siguiente manera

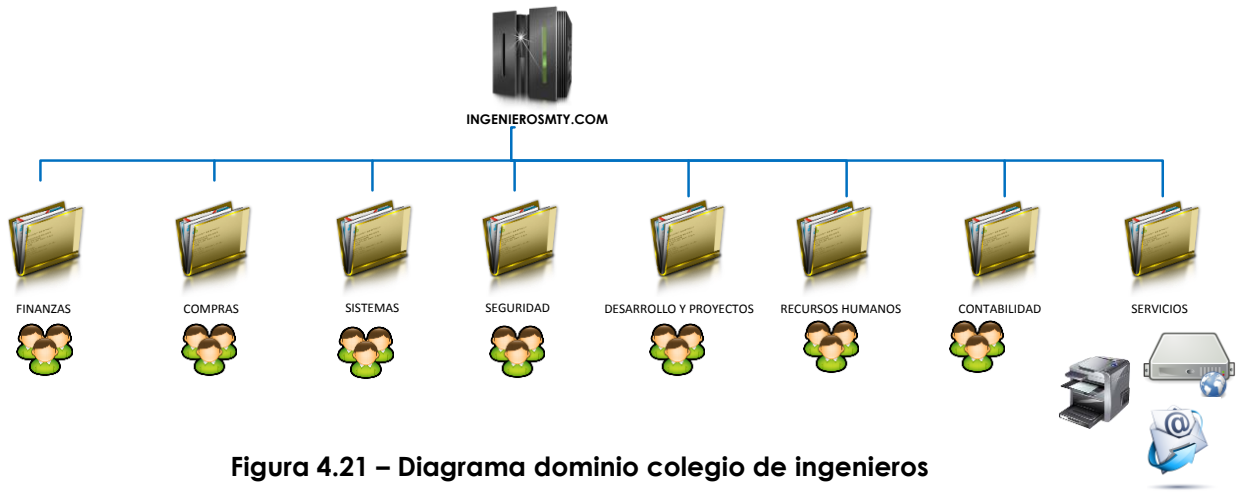



**Figura 4.21 – Diagrama dominio colegio de ingenieros**

En donde a los grupos para los usuarios se les asignará una IP dinámica mediante el protocolo DHCP mientras que a los equipos que conforman el grupo de "Servicios" se les otorgará una IP estática.

Las medidas de seguridad implementadas propuestas son las siguientes:

| Área | Medidas de seguridad |
|---|---|
| Finanzas | Ejemplo: No será posible cambiar la configuración de red ni de proxy, tiene asignado un papel tapiz por área, no será |

| | |
|---|---|
| | posible instalar ni desinstalar programas y habrá cambio de contraseña cada mes. |
| Compras | Ejemplo: No será posible cambiar la configuración de red, tiene asignado un papel tapiz por área, será posible instalar pero no desinstalar programas y habrá cambio de contraseña cada mes. |
| Sistemas | Diseñar permisos de acuerdo a su departamento. |
| Seguridad | Propuesto |
| Desarrollo y Proyectos | Propuesto |
| Recursos Humanos | Propuesto |
| Contabilidad | Propuesto |
| Servicios | Propuesto |

# Laboratorio 6.2 Configuración de servidor RADIUS

## Objetivo

El alumno investigará sobre herramientas y mecanismos utilizados para brindar el servicio de autenticación de usuarios a través del protocolo RADIUS, así como los pasos a seguir para realizar la implementación del mismo.

## Materiales y Equipo

- Servidor o equipo con Sistema Operativo Linux.
- Access Point o Router Inalámbrico.
- Computadora o equipo con Wi-Fi.

## Introducción

RADIUS (Remote Authentication Dial-In User Server) es un protocolo que permite llevar a cabo la autenticación, autorización y registro de usuarios remotos sobre algún recurso en particular, dicho término es conocido como "AAA", el cual se explica a continuación:

- Autenticación: proceso por el cual se determina si un usuario tiene permiso para tener acceso a un recurso en específico que se encuentra en la red, este proceso se lleva a cabo mediante el nombre de usuario y un password.

- Autorización: se refiere cuando a un determinado usuario se le conceden permisos sobre un recurso en específico, basándose para ello en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Los métodos de autorización soportados habitualmente por un servidor RADIUS incluyen bases de datos LDAP, bases de datos SQL e incluso archivos de configuración locales del servidor.

- Registro: se refiere a realizar un registro en el consumo de los recursos por parte de los usuarios. El registro suele incluir aspectos como la identidad de usuarios, la naturaleza del servicio prestado, además de hora de inicio y termino de los servicios utilizados por el usuario.

Una de las principales utilidad de un servidor RADIUS, es integrarse con algún dispositivo o aplicación que necesite de algún método de autenticación para brindar algún servicio, como por ejemplo Firewall, Access Point, servidor FTP, páginas Web, entre otros.

A continuación se muestra en la Figura 4.22 un diagrama general de cómo se realiza la integración de un servidor RADIUS en una red de datos.

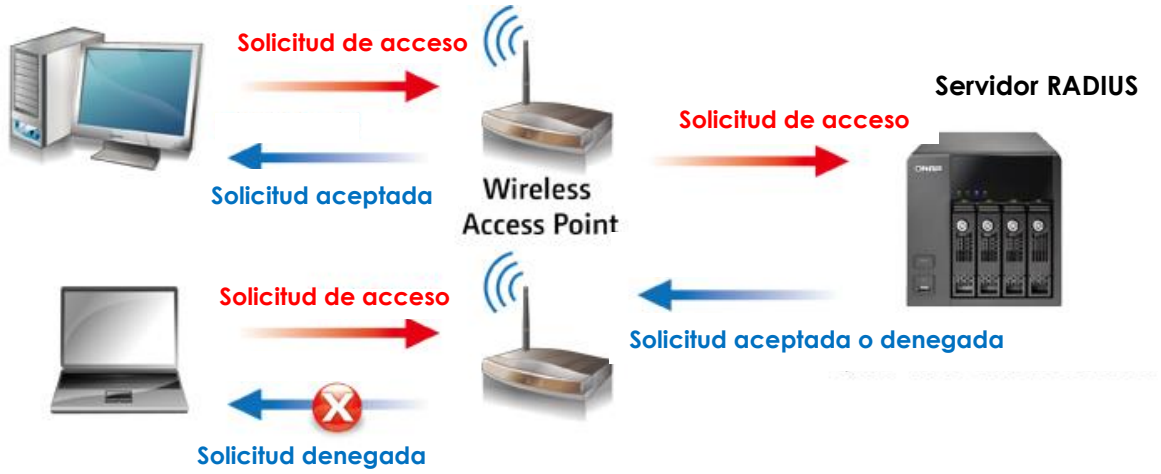



**Figura 4.22 - Integración de servidor Radius**

## Problemática

En una escuela de gastronomía se ha instalado Accesss Point en cada una de las aulas para ingresar a la red inalámbrica. Para este proyecto la directiva ha solicitado un control de usuarios para que sólo el personal autorizado tenga acceso a los servicios que necesita. Para llevar a cabo la implementación se ha lanzado una convocatoria para el diseño y arquitectura de este requerimiento, el cual tiene como requisito apegarse a estas características:

- Utilizar protocolo RADIUS.
- Sistema operativo Linux.
- Se debe utilizar un software que no requiera licenciamiento.
- Se cuenta con un servidor físico con 512 MB en RAM, 80 GB en Disco Duro y 2 tarjetas de red Ethernet.
- Distribución de usuarios por dirección MAC y por nombre de usuario.
- Se requiere realizar una distribución de usuarios por departamento.

El diagrama de red proporcionado es el que se muestra en la Figura 4.23:

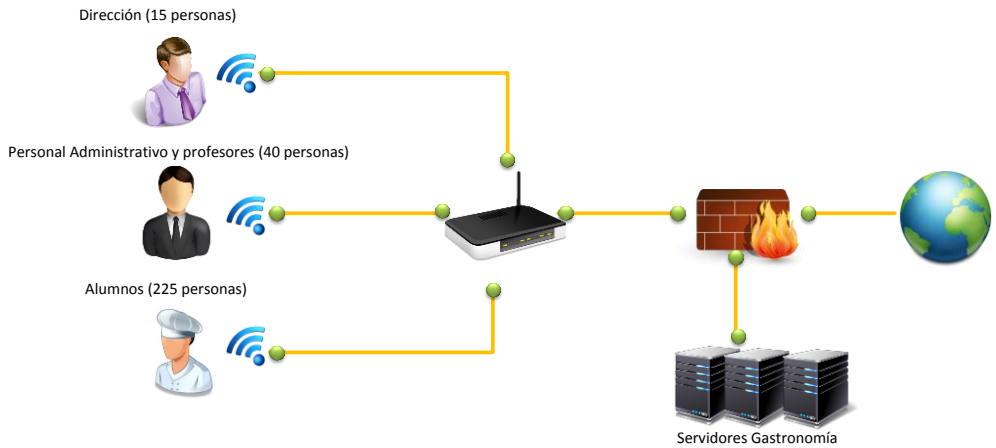



**Figura 4.23 - Diagrama de red escuela de gastronomía**

## Actividades a realizar

De acuerdo al proyecto presentado se debe entregar una propuesta técnica detallada en el cual se describa y diseñe una solución de implementación de un servidor RADIUS, con base en la información proporcionada investigue qué software deberá utilizarse y realice un breve informe de los beneficios que éste presenta.

***Respuesta esperada:***

Uno de los softwares que podrían utilizar es **"FreeRADIUS"** es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como: una biblioteca BSD para clientes, módulos para soporte en Apache, y un servidor de RADIUS.

El servidor FreeRADIUS es modular, escalable y fácil de implementar, entre sus principales características se encuentran:

- Para realizar las tareas de AAA puede almacenar y acceder a la información por medio de múltiples bases de datos: LDAP (AD, OpenLDAP), SQL (MySQL, PostgreSQL, Reales Oracle,…) y ficheros de texto (fichero local de usuarios, mediante acceso a otros, fichero de sistema /etc/passwd).
- Soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, mod_auth_radius, pam_auth_radius, Pyrad, extensiones php de RADIUS, etc).
- Se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, SUSE, Mandriva, Fedora Core, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.
- Soporta el uso de servidores Proxy.

Una vez determinado qué servidor se utilizará, elabore la propuesta técnica de integración con el servidor RADIUS para la autenticación de usuarios, esta debe contener un nuevo diagrama de red donde se observe el servidor.

### Respuesta esperada

El diagrama de integración con el servidor de autenticación se muestra en la Figura 4.24:

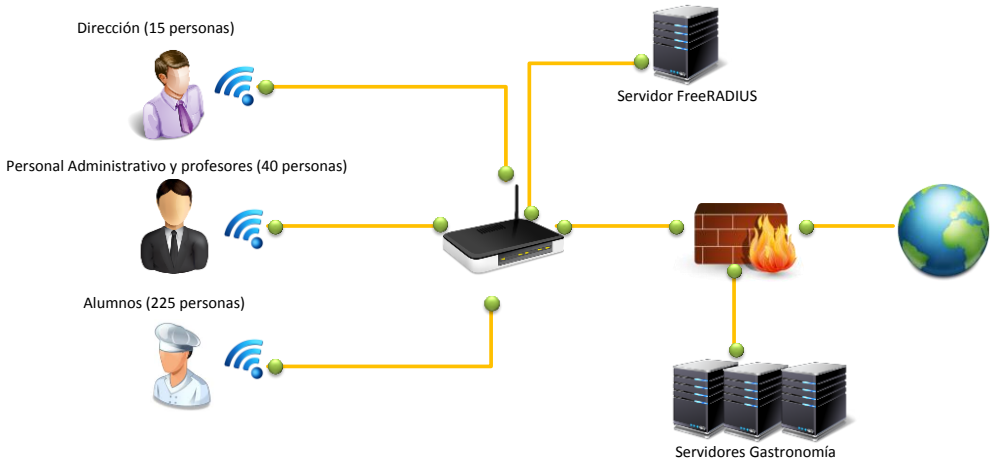



**Figura 4.24 - Diagrama de red con servidor RADIUS**

En donde la distribución de usuarios se muestra en la Tabla 4.12:

**Tabla 4.12 - Distribución de usuarios**

| Departamento | Usuario | Método de autenticación | Descripción |
|---|---|---|---|
| **Dirección** | Dirección | Por dirección MAC | Para los usuarios del departamento de dirección se les realizará una autenticación basada en la dirección MAC de sus dispositivos para no solicitarle las credenciales y con ello garantizar que tengan los servicios que necesitan en el colegio. Son los usuarios más importantes. |
| **Personal Administrativo y profesores** | Depto_adm | Por usuario y password también con dirección MAC | En este departamento se dividirán los usuarios de administración y serán identificados por dirección MAC y que utilizan equipos fijos y los profesores mediante un nombre de usuario y contraseña otorgados. |
| **Alumnos** | Alumno_iniciales_grado | Por usuario y password | Para los alumnos la técnica a utilizar será ingresando un nombre de usuario y password los cuales serán actualizados cada periodo escolar. |

Una vez concluida la propuesta lleve a cabo la implementación de este servicio y realice la memoria técnica con todo el desarrollo que realizó para llevar a cabo la instalación del servidor RADIUS.

**Respuesta esperada:**

La instalación del servidor RADIUS se realiza en un sistema operativo basado en Linux. En el Anexo B, se muestra paso a paso la configuración del servidor.

# Laboratorio 7.- Configuración básica de dispositivos de seguridad

## Laboratorio 7.1 Configuración básica de firewalls

### Objetivo

El alumno investigará y realizará las configuraciones necesarias para llevar a cabo la implementación de un firewall, el cual será utilizado para brindar seguridad perimetral a una red LAN.

### Materiales y Equipo

- Firewall
- Cables para realizar las conexiones

### Introducción

En la actualidad gran parte de las empresas, necesitan conectarse a internet para realizar sus tareas cotidianas tales como son consultan en distintas páginas, tramites gubernamentales, transferencias bancarias y demás. Sin embargo al conectarse a una zona no segura corren el riesgo de ser blanco de múltiples amenazas, tales como virus, ataques de denegación de servicios, hackeo y más. Para reducir este tipo de amenazas, las organizaciones implementan distintos sistemas de seguridad, entre los que se encuentran los firewalls.

Un firewall es un dispositivo de Software o Hardware el cual es utilizado para separar una zona segura de una no segura tal como se muestra en la figura 4.26. La mayoría de las veces las organizaciones implementan estas tecnología antes de su salida a internet, su tarea principal es examinar los paquetes que pasan a través de él y bloquear aquella que no cumple con los criterios de seguridad establecidos por el administrador.

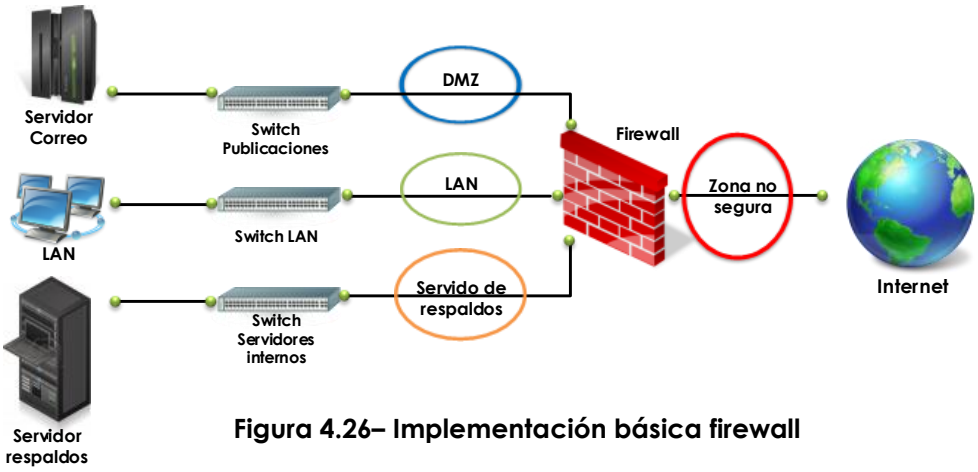



**Figura 4.26– Implementación básica firewall**

El firewall se puede considerar el componente de infraestructura de seguridad de red más importante y estratégico, ya que visualiza todo el tráfico y, como tal, se encuentra en la ubicación más efectiva para imponer las políticas de seguridad establecidas por la empresa. Desafortunadamente, los firewall tradicionales trabajan analizando la dirección IP origen, IP destino, puerto y protocolo para clasificar el tráfico, lo que permite a las aplicaciones y a los usuarios expertos en tecnologías esquivarlos con facilidad mediante saltos de puertos, el uso de ssl, el acceso a través del puerto 80 o el uso de puertos no estándar.

La pérdida de visibilidad y control resultante coloca a los administradores de la red en desventaja y expone a la empresa a tiempos de inactividad originados de un ataque, el aumento de los gastos operativos y una posible pérdida de información confidencial. Para atacar los problemas que se tiene al utilizar firewalls tradicionales, los administradores de red se apoyan de distintas herramientas dedicadas tales como filtrado de contendido, antivirus, IPS, DLP, entre otros.

La tendencia en la actualidad es el uso de firewalls de nueva generación, los cuales ofrecen distintas tecnologías tales como, filtrado de URL, detección de aplicaciones, antivirus, antiSpyware, detección de vulnerabilidades, así como las características habituales de un firewall, todos estos módulos, ayudan a tener una mayor seguridad sobre la red, así como una administración centralizada.

Para llevar a cabo la configuración de cualquier tipo de firewall es necesario familiarizarse con algunos conceptos, investigue y comente los términos que a continuación se presentan:

- **DMZ:** Es una red o parte de una red, separada de otros sistemas por un cortafuegos, que permite que sólo entren o salgan ciertos tipos de tráfico de red. El objetivo principal, es que todo el tráfico externo se comunique solamente con la DMZ. La DMZ no se puede comunicar con la red interna, previniendo posibles ataques en caso de algún intruso gane control de la DMZ.

- **Políticas de seguridad:** Es un conjunto de criterios de seguridad establecidos por el administrador del firewall, los cuales permiten o deniegan el tráfico a través del firewall.

- **NAT:** Network Address Traslation por su singlas en inglés, es la acción de traducir una dirección IP de una red a otra red distinta, como por ejemplo cuando se navega a internet, la dirección IP que tiene la máquina pertenece a un segmento privado, pero cuando se navega a través de internet el proveedor de servicios de internet ISP asigna una IP pública.

- **Gateway:** Conocido también como puerta de enlace es un sistema de la red que permite, a través de sí mismo acceder a otra red, o dicho de otra manera sirve como enlace entre dos o más redes. Un ejemplo es un Router el cual tiene como objetivo realizar el enrutamiento entre distintas redes.

- **Qué es IPs Públicas y Privadas:** Una IP pública es aquella que nos ofrece el ISP la cual poder ser asignada de manera dinámica o estática, las IPs públicas son utilizada únicamente para navegar a través de internet y es únicas e irrepetible en el mundo. Las IPs privadas sirve para brinda direccionamiento dentro de una red LAN, estas IPs a comparación de las IPs públicas pueden repetirse y ser utilizadas por distintas organizaciones.

- **Protocolos de enrutamientos:** Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes Routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto.

## Problemática

El despacho de contadores DCA, contrató a una consultoría de seguridad para rediseñar su red de una forma más segura, durante la junta de levantamiento de requerimientos, el ingeniero encargo de realizar el proyecto identificó lo siguiente:

- Cuenta con 25 usuarios, los cuales se encuentran divididos en 4 áreas, 10 auxiliares contables, 5 cobranzas, 5 finanzas y 5 contadores.

- Tienen 4 servidores para los cuales solo algunas áreas pueden tener acceso, a continuación se muestra en la Tabla 4.13 las áreas que tiene permisos de conexión a ciertos servidores.

**Tabla 4.13 - Permisos de conexión de servidores**

| | Correo | Respaldos | Datos clientes | Facturación |
|---|---|---|---|---|
| Auxiliares contables | | | | |
| Cobranza | | | | |
| Finanzas | | | | |
| Contadores | | | | |

**Acceso permitido** **Acceso denegado**

- El ISP proveerá al despacho de contadores con una IP pública Estática.

- El direccionamiento otorgado dentro de la red se realiza de forma estática, esto es para llevar un control más estricto de quien navega en la red, debido a que no se cuenta con una herramienta para realizar la identificación o autenticación de usuarios.

- Se está pensando en contrata a nuevo personal para cada área, sin embargo todavía no cuentan con un número definido.

- El número de sesiones que genera un usuario en promedio es de 90 PPS.

Además de la información antes recopilada, el dueño del despacho entregó el diagrama de red que se muestra en la Figura 4.27.

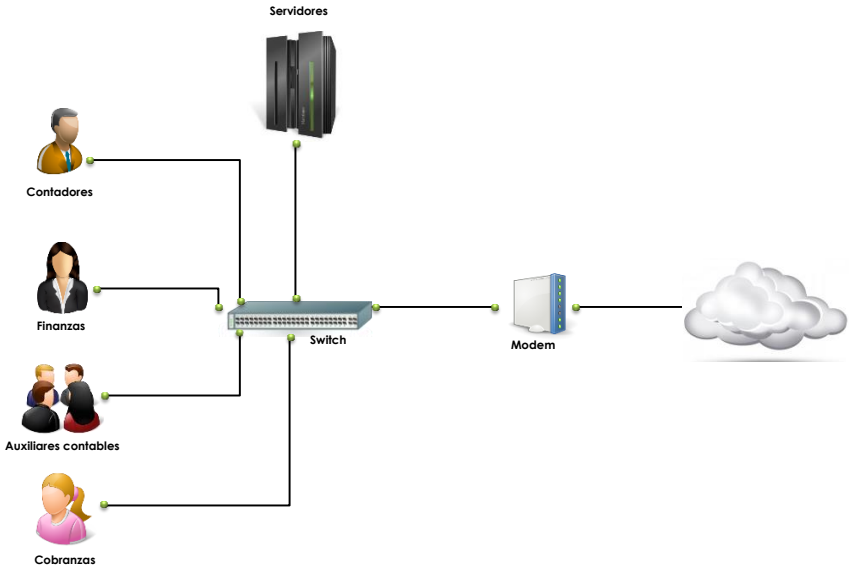



**Figura 4.27 – Diagrama de red Actual despacho contadores**

Durante el transcurso de la junta, el dueño comentó que desea convertirse en un despacho que otorgue servicios a nivel nacional. Para ello, se debe considerar brindar un alto nivel de seguridad dentro de su red, debido a que manejan información confidencial de distintos clientes.

## Actividad a Realizar

Con base a sus conocimientos adquiridos durante la carrera, proponga un diagrama de red y una solución para cumplir con los requerimientos obtenidos durante la junta de levantamiento, anote y justifique su respuesta.

**Respuesta esperada:**

Se debe tomar en cuenta que la solución planteada no es la única y puede variar dependiendo de los conocimientos de cada alumno. La posible solución que a continuación se presenta, se realiza tomando en cuenta los objetivos planteados para la práctica.

Como primera actividad, se debe asignar un segmento de red a cada una de las áreas, el direccionamiento puede ser realizado a través de VLSM. Para cada una de las áreas contempladas, se deberá tomar en cuenta un crecimiento del 50% aproximadamente, en la Tabla 4.14 se muestra el direccionamiento propuesto.

| Tabla 4.14 – Direccionamiento propuesto despacho contadores | | | | |
|---|---|---|---|---|
| Área | Host Requeridos | ID de red | ID broadcast | Mascara |
| Auxiliares | 15 | 172.16.14.0 | 172.16.14.31 | /27 |
| Servidores | 8 | 172.16.14.32 | 172.16.14.47 | /28 |
| cobranza | 8 | 172.16.14.48 | 172.16.14.63 | /28 |
| Contadores | 8 | 172.16.14.64 | 172.16.14.79 | /28 |
| Finanzas | 8 | 172.16.14.80 | 172.16.14.95 | /28 |

Para solventar el problema de permisos entre las distintas áreas, se propone dividir la red en distintas zonas de seguridad, esto permitirá tener un mayor control sobre el tráfico que circula a través de la red, en la figura 4.28 se muestra una propuesta del diagrama de red.

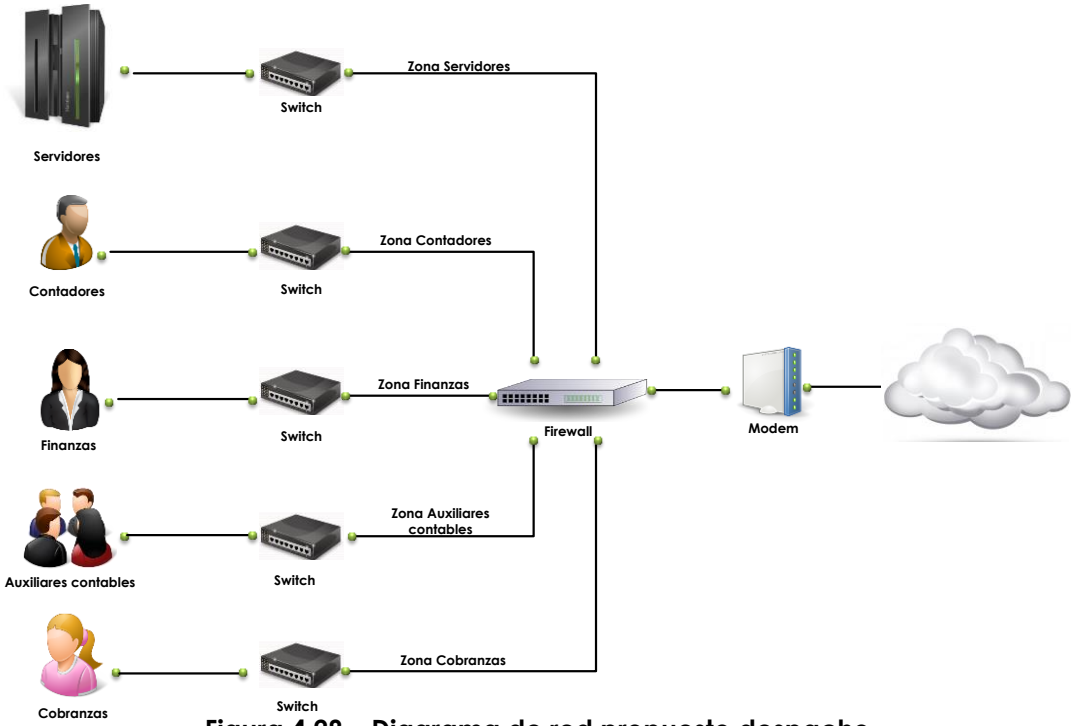



**Figura 4.28 – Diagrama de red propuesto despacho**

Además realice el dimensionamiento del firewall que debe utilizar para la implementación, consulte al menos dos fabricantes y justifique técnicamente qué firewall seleccionaría para la implementación, tome en cuenta la información recolectada durante el levantamiento de información.

**Respuesta esperada:**

De acuerdo a los requerimientos dados por el cliente, una posible solución para el firewall es el modelo PAN-500 del fabricante Palo Alto Networks, este firewall tiene 8 interfaces Ethernet 10/100/1000, tiene un throughput de 250 Mbs y 7500 sesiones por segundo y un

máximo de sesiones concurrentes de 64 000. A continuación se muestra en la Figura 4.29 el firewall propuesto.

**Figura 4.29 – Firewall propuesto despacho contadores**

Realice las configuraciones necesarias para que la solución propuesta, sea funciona y en liste las actividades a realizar para llevar a cabo esto. Después de haber hecho las configuraciones, haga pruebas de comunicación entre las distintas zonas, adjunte evidencia.

**Respuesta esperada:**

Dentro de las actividades a realizar se encuentran:

- Creación de zonas
- Asignación de IPs a interfaces
- Rutas estáticas
- Nat
- Políticas de seguridad

Las pruebas de comunicación deben ser realizadas con los comandos básicos de comunicación, tal es el caso del Ping y el tracert.

# Laboratorio 7.2 Publicación de servicios

## Objetivo

El alumno investigará y realizará la publicación de un servidor Web y un servidor FTP a través de un firewall, estos servicios serán consultados por distintos usuarios, dentro y fuera de la red LAN.

## Materiales y Equipo

- Firewall.
- Servidor Web y un servidor FTP.
- Cables para realizar las conexiones.

## Introducción

Hoy en día muchas de las empresas, necesitan publicar distintos servicios, los cuales deben ser consultados por sus clientes o por sus empleados, para realizar distintas tareas, tales como consulta de correo electrónico, respaldo, consulta de información, consulta de páginas web, entre otras. Todos éstos se encuentran alojados dentro de distintos servidores, que están localizados dentro de distintas zonas de la red LAN.

Para que los clientes y empleados puedan utilizar estos servicios, muchas de las empresas deciden publicarlos a través de internet, esto garantiza que si un usuario no se encuentra dentro de la red de la empresa pueda hacer uso de los servicios que necesitan.

Al realizar la publicación de los servicios a través de internet, quedan vulnerables a distintos ataques que pueden ser perpetrados por un hacker o una persona que desee atentar contra la integridad del servicio. Para evitar estas acciones, existen diversos sistemas de seguridad que ayudar a mantenerlos íntegros, uno de estos sistemas son los firewall, los cuales ayudará minimizar las vulnerabilidades, así como aumentar la seguridad para ingresar a las aplicaciones publicadas.

## Problemática

El despacho de contadores DCA, ha aumentado su cartera de clientes, por tal motivo necesita realizar algunas modificaciones en su red para solventar algunas tareas que son realizadas por los clientes, para ello es necesario efectuar la publicación de una página web donde se enlistará información vital para los tramites contables. Además de esto necesitan publicar un sitio donde los clientes realicen el respaldo de toda su contabilidad y otra información importante.

La consultoría que administra la cuenta del despacho de contadores, asignó a un ingeniero para realizar lo solicitado por el cliente, éste revisa las memorias técnicas que han hecho anteriormente para el cliente y encuentra lo siguiente:

- La red se encuentra dividida en distintas zonas de seguridad, cada una con un direccionamiento de red distinto

- Se cuenta con 4 servidores dedicados, para correo, respaldos, datos clientes y facturación.

Dentro de la información analizada se encuentra el diagrama de red que se muestra en la Figura 4.30

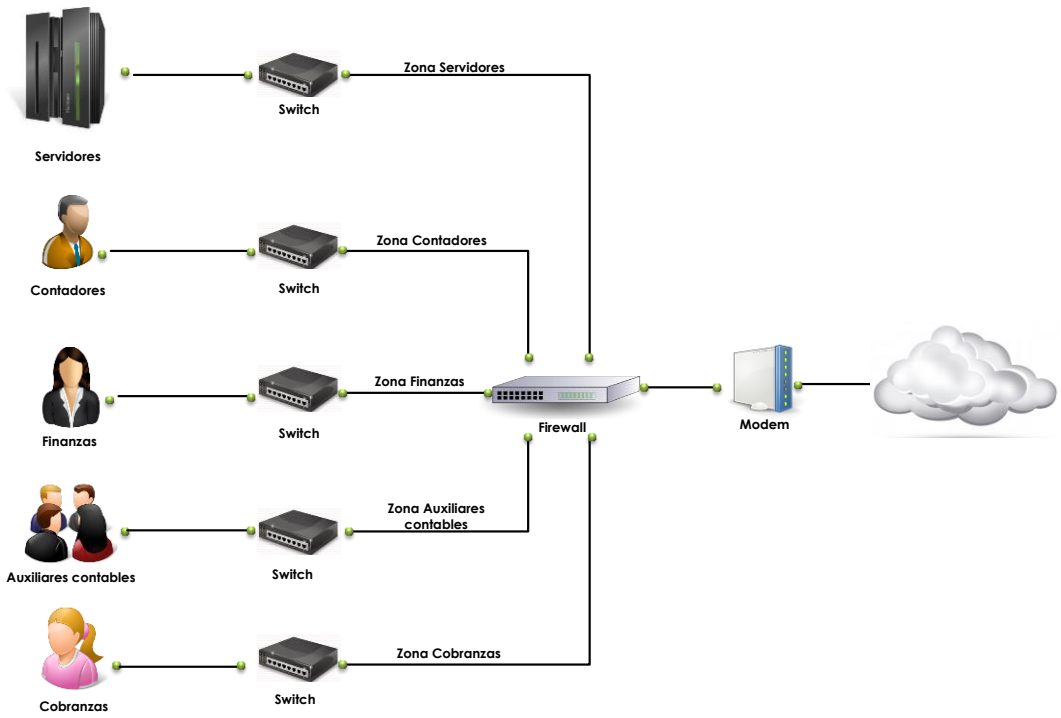



**Figura 4.30 – Diagrama red publicación**

## Actividad a Realizar

**Nota:** Se utilizará el mismo direccionamiento y diagrama de red, que se planteó en el laboratorio 7.1 Configuración básica de Firewall.

Realice las configuraciones necesarias, para efectuar la publicación de los servicios requeridos, y establezca las políticas de seguridad necesarias para garantizar la seguridad de los servicios.

**Respuesta esperada:**

Para llevar a cabo la publicación de los servicios es necesario realizar configuraciones tales como NATs, ruteos y políticas de seguridad. La forma en que se configuran dependerá del

fabricante del firewall utilizado, sin embargo los conceptos utilizados son los mismos. A continuación se muestran una serie de pasos genéricos que deben ser seguidos para configurar la publicación de servicios.

- Configuración de NATs: Se deben realizar dos NATs, el primero deberá ser de destino, éste debe traducir la dirección pública a la IP privada del servicio o del servidor que se desea publicar, en el caso que se cuente con sola una IP pública y distintos servicios publicados se debe publicar el servicio con un puerto. El segundo NAT debe ser realizado como de origen, esto quiere decir que la IP del servidor donde reside el servicio deberá trasladar su dirección privada a la IP pública, si se tiene una sola IP será necesario realizar el NAT con el puerto correspondiente.

- Rutas: Las rutas deberán ser creadas para establecer la comunicación entre los clientes y el servidor que contiene la publicación.

- Políticas de seguridad: Las políticas de seguridad deberán ser creada para que únicamente permita el tráfico por el puerto por el cual se publicó el servicio o en el caso que el firewall detecte aplicaciones, será permitida la aplicación.

Durante la publicación del servicio indique qué dificultades se presentaron al momento de realizar la publicación y explique cómo dio solución a los problemas suscitados. Una vez que se haya realizado la publicación, adjunte evidencia que valide el correcto funcionamiento de los servicios. Explique y documente cada una de las pruebas realizadas.

**Respuesta esperada:**

Entre las pruebas que debe realizar el alumno para validar el correcto funcionamiento se encuentra:

- Pruebas de Networking tales como Ping, Telnet, Tracert.
- Tráfico Capturado por el firewall, en este se debe observar las peticiones realizadas por un usuario que se encuentra fuera de la red.
- Imagines que demuestren la correcta visibilidad de los servicios.

# Laboratorio 7.3 Creación de VPNs

## Objetivo

El alumno investigará y realizará las configuraciones necesarias para establecer VPNs sitio a sitio o de acceso remoto, sin importar el fabricante del firewall utilizado.

## Materiales y Equipo

- Firewall.
- Cables para realizar las conexiones.

## Introducción

En la actualidad muchas de las empresas necesitan que otras sucursales o usuarios localizados en espacios geográficos distintos se conecten a su red corporativa, de forma rápida, segura y a bajo costo. Para ello muchas empresas contratan enlaces dedicados de internet los cuales aseguran una alta disponibilidad en cuanto a la comunicación entre sucursales se refiere, sin embargo el uso de esta tecnología es costosa y sólo empresas con los recursos económicos suficientes pueden adquirirla. Afortunadamente el crecimiento exponencial de Internet, ha permitido el uso de este medio de comunicación para realizar conexiones rápidas y seguras, a través de la tecnología conocida como VPN.

Una VPN (Red Privada Virtual) es una red privada construida dentro de una infraestructura de red pública. Las organizaciones pueden usar una VPN para reducir sus costos de ancho de banda de WAN, a la vez que aumentan la velocidad de conexión, así como proporcionar un máximo nivel de seguridad a través de protocolos IPsec (seguridad IP cifrada) o túneles SSL (VPN Secure Socket Layer). Algunos algoritmos, funciones y protocolos tales como MD5, SHA, 3DES, Diffie-Hellman y más, son utilizados para realizar el cifrado e integridad de la información que viaja a través de los túneles. Las VPN ayudan a proteger los datos que se transmiten a través de una red no segura como lo es internet, de todo acceso no autorizado, el cual atenta con la confidencialidad, disponibilidad e integridad de la información.

Las VPNs pueden ser clasificadas en dos tipos principalmente, de acceso remoto y sitio a sitio. En entornos corporativos las VPNs de acceso remoto permiten a los empleados ingresar a la intranet de su compañía desde su casa o mientras se encuentran fuera de su oficina. Las VPNs sito a sitio permiten a los empleados en oficinas separadas geográficamente compartir recursos tales como base de datos, servidores FTP, Servidores Web, aplicaciones y más. En la Figura 4.31 se muestra un ejemplo de VPNS sitio a sitio y de acceso remoto.

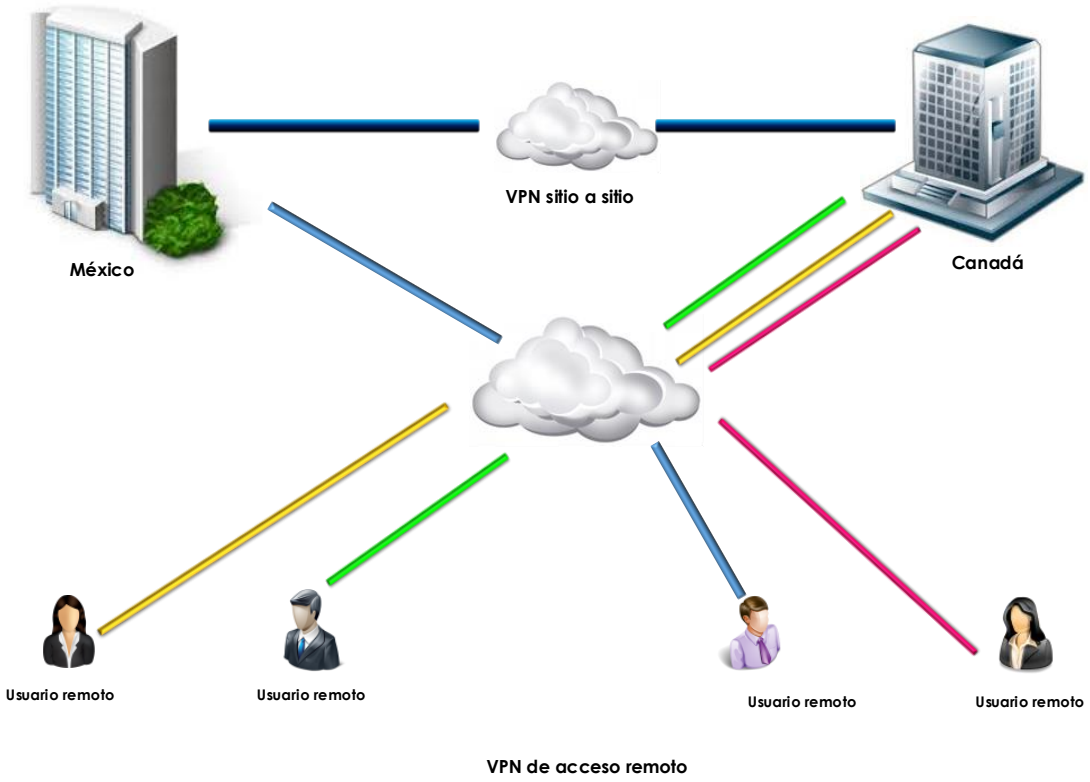



**Figura 4.31 – VPNs Acceso remoto y VPNs sitio a sitio**

Las VPN de acceso remoto, son implementadas mediante el uso de VPN SSL, ésta consiste en uno o más dispositivos conectados generalmente mediante un navegador de internet, una aplicación dedicada o un Gateway (Punto fina en donde se conectan los usuarios), el tráfico entre el usuario remoto y el Gateway es encriptado con el protocolo SSL. Este tipo de VPN es utilizada por gente que trabaja remotamente, en dispositivos móviles, computadoras personales, Smartphones, y demás.

Durante la configuración de VPN, es necesario tener claro algunos términos los cuales son utilizados para la configuración y puesta a punto de las VPNs, investigue lo siguiente:

**Protocolo IPSec:** Es un conjunto de protocolos cuyas funciones es asegurar las comunicaciones sobre el protocolo de internet, autenticando y cifrando cada paquete IP en un flujo de datos. IPSec incluye protocolos para el establecimiento de claves de cifrado. El protocolo IPSec trabaja en la capa 3 del modelo OSI, esto hace que sea más flexible, ya que puede ser utilizado para proteger protocolos de Capa 4 como son TCP y UDP.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad.

**Encabezado de autenticación (AH):** Es un protocolo de seguridad que es utilizado para realizar la autenticación del origen de un paquete IP, así como verificar la integridad de su contenido. Éste autentica el paquete a través DE la suma de comprobación calculada mediante un código de autenticación de mensaje basado en hash, mediante una clave secreta y funciones MD5, SHA-1, SHA-512, SHA-384 y más.

**Carga de seguridad encapsulada (ESP):** Proporciona un medio para garantizar la privacidad, la autenticación del origen y la integridad del contenido. El protocolo en modo túnel encapsula el paquete y adjunta nuevos encabezados, este nuevo encabezado IP contiene la dirección de destino necesaria para enrutar los datos protegidos a través de la red. Con el protocolo ESP es posible cifrar o autenticar, o los dos al mismo tiempo, para la el cifrado es posible contar con métodos criptográficos como son DES, 3DES, AES128, AES 265 y más.

**Asociación de seguridad (SA):** Es un acuerdo unidireccional entre los participantes de la VPN en lo que tiene que ver con los métodos y parámetros utilizados para garantizar la seguridad de un canal de comunicación. Una asociación de seguridad está conformada por los siguientes componentes los cuales garantiza la seguridad de las comunicaciones:

- Claves y algoritmos de cifrado.
- Modo de protocolo transporte o túnel.
- Método de admiración de claves, ya sean manuales o Autokey IKE.
- Periodo de vigencia de SA.
- IP destino.
- Protocolo de Seguridad AH o ESP.
- Valor del índice de parámetros de seguridad..

**Intercambio Diffie-Hellman:** Permite a los participantes elaborar un valor secreto compartido. El punto fuerte de esta técnica es que permite a los participantes crear el valor secreto a través de un medio no seguro sin tener que transmitir este valor a través de un medio inseguro, existen distintos grupos de Diffie-Hellman los cuales son:

- Grupo DH 1: Módulo de 768 bits.
- Grupo DH 2: Módulo de 1024 bits.
- Grupo DH 5: Módulo de 1536 bits.

Para llevar a cabo el establecimiento de un túnel IPSec AuthoKey IKE, es necesario que se lleven a cabo dos fases, explique cada uno de las fases.

**IKE Fase 1:** Esta fase es la encargada de establecer un canal autenticado de comunicación. Para esto utiliza el Algoritmo de Diffie-Hellman el cual es asimétrico y permite el intercambio seguro de llaves simétricas como DES, 3DES, AES o SEAL las cuales son utilizada para encriptar el tráfico entre los pares en la fase 2. La autenticación para este protocolo se puede realizar por medio de claves Pre-Compartidas (Pre-Shared Key) o de Certificados.

Parámetros disponibles para IKE ph1:

- Authentication: Pre-Shared Keys, RSA-Encryption, RSA-Signature.
- Encryption Algorithm: DES, 3DES, AES [128, 192, 256].
- Key Exchange: DH-Group1 [768-bit], DH-Group 2 [1024-bit], DH-Group 5 [1536-bit].
- Hashing: MD5, SHA-1.

**IKE Fase 2:** En esta fase los pares hacen uso del canal seguro establecido en la fase 1 para compartir las claves simétricas con las cuales se realiza el cifrado del tráfico.

Parámetros disponibles para IKE ph2:

- Encryption Algorithm: esp-des, esp-3des, esp-aes [128, 192, 256], esp-seal, esp-null.
- Authentication: ah-md5-hmac, ah-sha-hmac, esp-md5-hmac, esp-sha-hmac.

## Problemática

El despacho de contadores DCA, ha aumentado su cartera de clientes exponencialmente, y por tal motivo ha tenido que instalar diversas sucursales a lo largo del país. El dueño del despacho mando llamar a la consultoría que administra la red, para indicarles los nuevos requerimientos a los que se está enfrentado.

Durante la junta para el levantamiento de información, se explicó que con base al reciente crecimiento de la empresa todas las sucursales necesitan tener acceso a diversos servicios que únicamente deben existir dentro de la red corporativa, tales servicios son programas de facturación y bases de datos, éstos contienen información confidencial de los clientes, esto servicios actualmente se encuentran en las oficinas centrales localizadas en el Distrito Federal.

Otro de los requerimientos planteados, fue el ingreso a los servicios de facturación y base de datos, por parte de contadores que viajan para visitar a clientes donde no se tiene oficinas remotas. Después de la junta, el ingeniero que se encuentra a cargo de la cuenta, revisó la información de implementaciones anteriores y observo lo siguiente:

- Solo se tiene documentados 25 usuarios en 4 distintas áreas y 4 servidores, esta información fue obtenida de la primera implementación. Actualmente el número de usuarios subió a 100 solo en las oficinas centrales, y 25 en promedio en oficinas remotas, el direccionamiento que actualmente se tiene se observa en la Tabla 4.15.

**Tabla 4.15 – Direccionamiento existente despacho contadores**

| Área | Host Requeridos | ID de red | ID broadcast | Mascara |
|---|---|---|---|---|
| **Auxiliares** | **15** | **172.16.14.0** | **172.16.14.31** | **/27** |
| **Servidores** | **8** | **172.16.14.32** | **172.16.14.47** | **/28** |
| **cobranza** | **8** | **172.16.14.48** | **172.16.14.63** | **/28** |
| **Contadores** | **8** | **172.16.14.64** | **172.16.14.79** | **/28** |
| **Finanzas** | **8** | **172.16.14.80** | **172.16.14.95** | **/28** |

Las demás direcciones en las oficinas centrales son asignadas a través de DHCP en un segmento192.168.100.0/24. Este segmento fue asignado para solventar momentáneamente el actual crecimiento de la red. Dentro del firewall que se tiene este segmento tiene permiso de ingresar a todo dentro de la red.

- Se tienen 3 sucursales y una oficina central.
- El direccionamiento que se tiene en las oficinas remotas es entregado vía DHCP por el módem que otorga el proveedor de servicios de internet.
- Los usuarios que se deben conectar en dispositivos móviles cuando se encuentran fuera de la oficina central son 50, las conexiones no son concurrentes.
- La oficina central es la única que cuenta con una IP pública estática.

Después de analizar toda la información que recopiló el ingeniero encargado de la cuenta, realizó un esbozo de la red que actualmente se tiene, éste se puede observar en la Figura 4.33

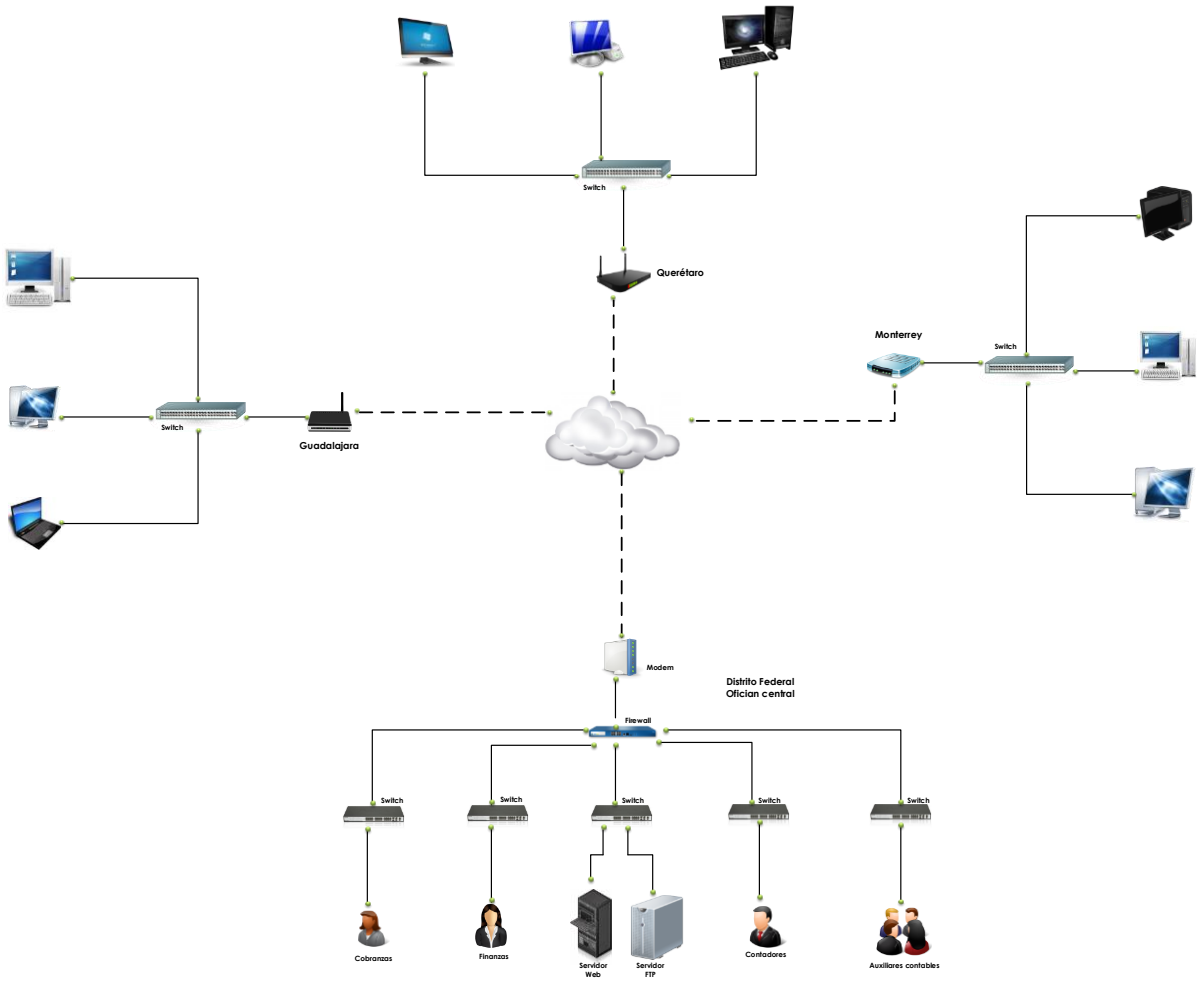



**Figura 4.33 – Diagrama de red de VPN para sucursales despacho**

## Actividad a Realizar

Con base en la información expuesta anteriormente, proponga una solución a los requerimientos del despacho de contadores, si es necesario realice más preguntas al maestro para dar una solución completa. Además dimensione y elija los equipos que serán utilizados para la implementación, justifique los equipos propuestos.

**Respuesta esperada:**

Con la información que se proporcionó en la problemática, el alumno deberá de dar una solución a las necesidades que presenta el despacho, hay que tomar en cuenta que la información proporcionada, no es suficiente para que el alumno proponga un escenario que cumpla con las necesidades del negocio y por tal motivo tendrá que realizar distintas preguntas para diseñar una arquitectura.

En esta práctica el maestro tendrá que proporcionar la información faltante para dar solución al problema presentado. Entre la información adicional que proporcionará, se encuentra:

- Número de usuarios por localidad.
- Velocidad de internet que tiene contratado por localidad.
- Segmentos de red que serán utilizados en cada localidad.
- Posibilidad de contratar IPs privadas para cada una de las sucursales.
- Sistemas operativos utilizados en dispositivos que se conectaran por la VPNs de acceso remoto.
- Permisos de acceso a recursos.
- Pedir que los servidores, utilice un segmento de red distinto por cuestiones de seguridad.
- Método de autenticación de usuarios con acceso a VPN de acceso remoto.

El dimensionamiento de los equipos a utilizar dependerá de la información adicional que proporcione el maestro.

Proponga un diagrama de Red, de acuerdo a la solución propuesta, este debe incluir.

- Direccionamiento utilizado.
- Equipos que formarán parte de la solución.
- Zonas existentes.
- VPNs a utilizar.

**Respuesta esperada:**

El diagrama de red dependerá de la arquitectura propuesta por cada alumno, lo importante de este diagrama es como el alumno realizará la implementación de las VPNs.

De acuerdo a su diagrama propuesto realice las configuraciones necesarias para que éste funcione correctamente. Una vez realizado lo anterior realice las siguientes pruebas de comunicación.

- Ping de las sucursales a los servicios que se necesitan ingresar
- Tracert para verificar los saltos desde la IP origen hacia los servicios requeridos.
- Dentro de los firewall utilizados en la implementación, realizar una captura del tráfico generado al momento de realizar pruebas.
- Logs que validen el establecimiento de la VPN.

**Respuesta esperada:**

Las pruebas presentadas para validar el correcto funcionamiento del escenario propuesto por el alumno, dependerán de cada uno de los direccionamiento presentado.

# Laboratorio 8.- Tendencias en la tecnología

## Laboratorio 8.1 Control de la Web 2.0

### Objetivo

El alumno investigará las herramientas que existe para realizar el control de la Web 2.0, así mismo llevará a cabo la implementación de una herramienta dedicada para realizar el control de la misma.

### Materiales y Equipo

- Firewall de nueva generación
- Computadora o laptop
- Cables para realizar las conexiones necesarias
- Navegadores Internet Explorer, Mozilla y Chrome

### Introducción

La Word Wide Web, ha cambiado la forma en la que las personas realizan sus actividades cotidianamente, éstas pueden ir desde realizar transacciones bancarias, hasta comunicarse con otras personas, compartir video y más. Desde su creación en la década de los 90´s las páginas web que conformaba la Word Wide Web eran del tipo estáticas, esto quiere decir que contenían únicamente texto fijo y por tal motivo no permitía la interacción del usuario con la información que contenía. Hoy en día el diseño de las páginas Web es cada vez más dinámico, en éstas se pueden encontrar distintas tipos de aplicaciones embebidas con las cuales el usuario puede realizar distintas tareas.

La Web 2.0 se caracteriza principalmente por el uso de aplicaciones dinámicas que permiten al usuario participar en la organización, creación y contribución de contenido en los sitios Web, un ejemplo claro de la Web 2.0 es Facebook, éste ofrece distintos tipos de contenido con el cual puede interactuar el usuario.

Para las empresas que llevan un control de lo que pueden y no pueden consultar sus usuario en internet dentro de sus instalaciones, la Web 2.0 se ha convertido en un desafío, esto es debido a que no es sencillo realizar un control del contenido dinámico que contiene las páginas web que visitan sus usuarios. Otro punto que hace que cada vez se mas difícil el filtrado de las páginas Web es la utilización del protocolo SSL, éste es utilizado para cifrar toda la información que viaja a través un red no segura como lo es internet. El uso de este protocolo hace que algunas herramientas dedicadas al filtrado Web sean ineficaces para realizar el filtrado. Para solventar este problema los fabricantes han hecho uso de certificados digitales, estos permiten realizar el descifrado de todo el tráfico que es cifrado a través del protocolo ssl, al realizar esto se tiene una mayor visión de todo información que transmite y así ser capaz de realizar el filtrado web eficientemente.

## Problemática

La empresa GSC, ha identificado que la mayoría de sus usuarios pasan la mayor parte de su tiempo visitando y utilizando aplicaciones que no son permitidas para realizar sus actividades laborales. El uso de estas aplicaciones hace que el uso ancho de banda utilizado se vea afectado. Por tal motivo el gerente de TI, ha decidido adquirir una tecnología que ayude a solucionar el problema presentado. Para ello ha contactado a distintos proveedores para que le brinde una solución, cada uno tendrá que presentar una prueba de concepto con el objetivo de enseñarle porqué su solución cumple mejor con las necesidades presentadas.

La consultoría 8Net, solicito a su ingeniero de preventa que realizara la prueba de concepto, con la solución que se adecuara más a las necesidades presentadas. El ingeniero decidió presentar un firewall de nueva generación como solución para filtrado Web y de aplicaciones, esto debido a su fácil implementación y fácil administración.

Dentro de la junta inicial, el gerente de TI dejo en claro que la solución propuesta no debe de presentar ningún cambio en la infraestructura de la red y por ningún motivo deben realizarse configuraciones adicionales en los dispositivos de los usuarios. Bajo la anterior premisa y después de haber elegido la solución, el ingeniero analizó el diagrama de red que se muestra en la Figura 4.34 y que fue proporcionado por el gerente de TI.

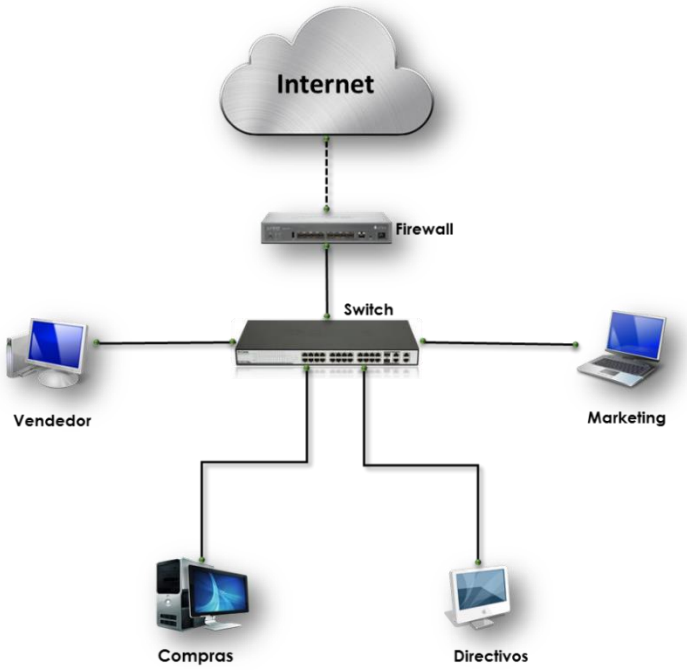



**Figura 4.34 – Diagrama de red GCO**

Para realiza las pruebas de filtrado se ocuparán tres tipos de perfiles, el primero es para altos directivos, en este se permitirá la mayoría de las páginas de internet excepto aquellas que tengan que ver con contenido de adultos o páginas que pueden afectar la integridad del

usuario. El segundo perfil está dirigido hacia el área de Marketing y compras, en este perfil solo se permitirá el acceso a redes sociales pero sin la opción de utilizar las aplicaciones contenidas en estas, también se dará permiso a todas las páginas que tengan que ver con tiendas departamentales y correo electrónico. El último perfil de filtrado será el más restrictivo, debido a que solo tendrá ingreso a correo electrónico y páginas de consulta general.

## Actividad a Realizar

Con base a los requerimientos que se presentan para la prueba de concepto, proponga un diagrama de red basado en el original, que satisfaga las necesidades presentadas, justifique su diagrama de red propuesto.

**Respuesta esperada:**

El diagrama de red propuesto no debe de modificar la arquitectura del diagrama original, debido a que en la configuración no debe de realizar configuraciones de capa 3, a continuación se muestra en la Figura 4.35 una posible solución al escenario propuesto. El firewall de nueva generación es colocado entre el firewall existente y el Switch debido a que por este punto pasa todo le tráfico de internet, el cual quieres ser filtrado.

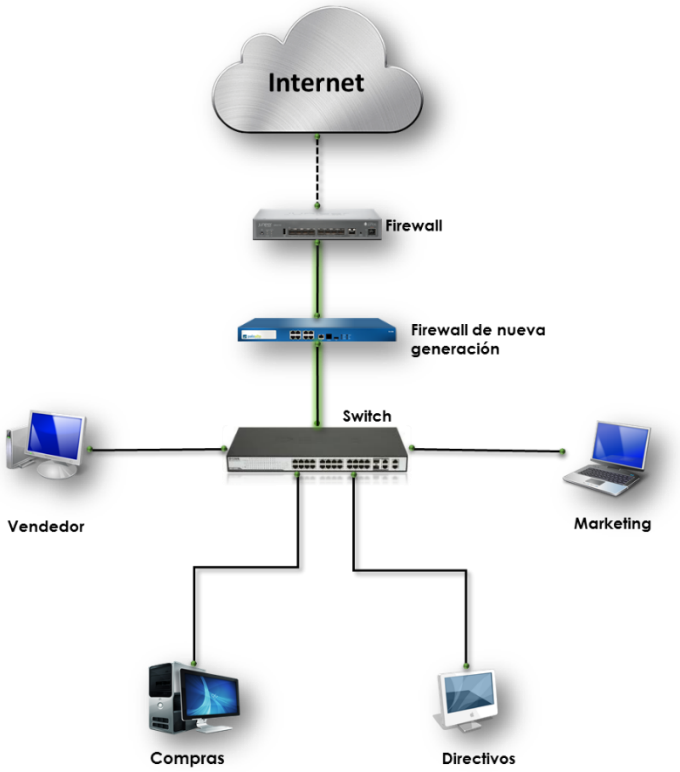



**Figura 4.35 – Diagrama de red propuesto GCO**

Una vez propuesta la arquitectura de red, es necesario configurar el firewall de nueva generación para integrarlo a la red, realice las configuraciones necesarias para que la integración sea de forma transparente y valide su correcto funcionamiento. Para realizar la

validación es necesario que adjunte evidencia del tráfico que pasa a través del firewall así como pruebas de comunicación desde un equipo a internet.

**Respuesta esperada:**

El firewall de nueva generación utilizado tiene la posibilidad de ser configurado en un modo llamado virtual Wire, esta configuración permite que se pueda ingresarse el firewall a cualquier parte de la red sin la necesidad de hacer modificaciones en esta, además de utilizar los distintos módulos con los que cuenta. Dentro de las configuraciones que deben ser realizadas para que el firewall opere en modo Virtual Wire son:

- Creación de zonas de seguridad
- Configuración de interfaces a utilizar, en modo Virtual Wire
- Creación de políticas de Seguridad las cuales contendrán los perfiles de Filtrado, estas políticas deberán permitir el tráfico entre las zonas que serán utilizadas.

Las pruebas de comunicación, deben realizarse desde un equipo que se encuentre en una de las zonas configuradas, entre las pruebas realizar se encuentran:

- Ping: Este puede realizar se a cualquier dirección IP tal como el Gateway de la red o un DNS público 8.8.8.8
- Tracert: En este se observará que el firewall no interfiere en los saltos que se deben hacer para llegar a una IP.

Otra de las evidencias que deben de presentar, es el tráfico que pasa a través de firewall en este se observará toda las aplicaciones utilizadas.

Después de haber validado la correcta comunicación y la salida de internet, se deberán de crear los perfiles de filtrado Web y grupos de aplicaciones de acuerdo a lo planteado durante la junta de requerimientos. Realice pruebas para validar el correcto funcionamiento del filtrado Web y muestre evidencia de que han sido los bloqueados los accesos a las páginas no permitidas.

**Respuesta esperada:**

El alumno deberá de presentar una imagen en la cual se muestra una página de bloque tal y como se observa en la Figura 4.36 adicionalmente tendrá que colocar el tráfico observado en el firewall.

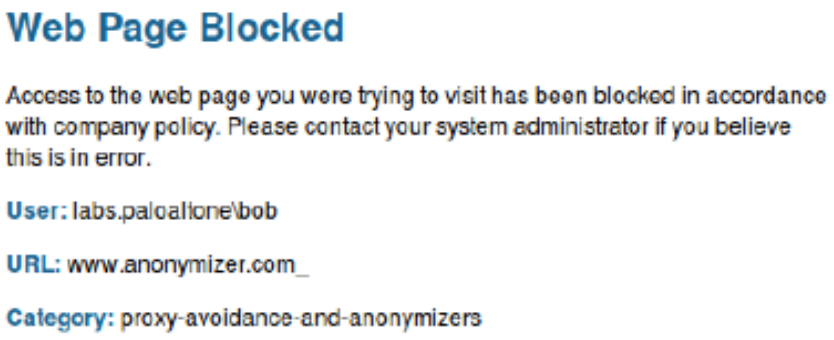



**Figura 4.36 – Página de Bloqueo**

De acuerdo a las pruebas realizadas, ¿Qué pasa cuando utiliza el protocolo https para ingresar a algunas páginas?, Explique qué es lo que sucede, plantee una solución y llévela a cabo. Documente la solución propuesta y muestre capturas de pantallas donde se muestre el bloqueo de las página Web que utilizan el protocolo https y también analice el tráfico observado en el firewall.

**Respuesta esperada:**

Cuando se trata de navegar utilizando el protocolo http, el filtrado Web funciona correctamente y es posible bloquear las páginas que no están permitidas, pero cuando se ocupa https se observa que no es posible bloquear la navegación web, esto sucede debido a que todo el tráfico que viaja a través del protocolo https se encuentra cifrado y para el firewall de nueva generación es imposible descifrarlo sin algún método que lo ayude a visualizar el tráfico. Para solucionar este problema es necesario crear un certificado de seguridad que ayude a descifrar todo el tráfico https que pasa por el firewall.

El alumno tendrá que crear un certificado de seguridad que será instalado en las máquinas en donde se realicen las pruebas, este certificado será creado desde el firewall de nueva generación.

# Laboratorio 8.2 Prevención de pérdida de la información

## Objetivo

El alumno investigará sobre las tecnologías, herramientas y nuevas técnicas que en el ámbito de redes y seguridad se están utilizando para combatir la fuga de información.

## Materiales y Equipo

- Equipo de cómputo, revistas, libros, y todo aquel material de investigación.

## Introducción

Una de las mayores amenazas que actualmente han sido de gran impacto para las organizaciones es la fuga o robo de información, sin embargo, de acuerdo con el más reciente Informe Global sobre Fraude de Kroll 2013/2014 realizado con el apoyo del Economist Intelligence Unit, la cantidad de compañías que fueron víctimas de fraude por robo de información aumentó considerablemente en los últimos años. Este tipo de fraude se encuentra sólo atrás del robo de activos físicos. El resultado de este análisis se muestra en las Tablas 4.16 y 4.17.

**Tabla 4.16- Compañías afectadas por fraude**

| | 2013 | 2012 |
|---|---|---|
| Robo de activos físicos | 28% | 24% |
| Robo de información | 22% | 21% |
| Conflicto de intereses de la gerencia | 20% | 14% |
| Fraude de vendedores, proveedores o adquisiciones | 19% | 12% |
| Fraude financiero interno | 16% | 12% |
| Infracción regulatoria o de cumplimiento | 16% | 11% |
| Corrupción y soborno | 14% | 11% |
| Robo de PI | 11% | 8% |
| Colusión de mercado | 8% | 3% |
| Malversación de fondos de la compañía* | 8% | — |
| Lavado de dinero | 3% | 1% |

*No cubierto en la encuesta de 2012

**Tabla 4.17- Compañías que se describen vulnerables**

| | 2013 | 2012 |
|---|---|---|
| Robo de información | 21% | 7% |
| Corrupción y soborno | 20% | 10% |
| Robo de activos físicos | 18% | 6% |
| Robo de PI | 18% | 7% |
| Fraude de vendedores, proveedores o adquisiciones | 18% | 5% |
| Infracción regulatoria o de cumplimiento | 18% | 5% |
| Conflicto de intereses de la gerencia | 17% | 4% |
| Colusión de mercado | 14% | 5% |
| Malversación de fondos de la compañía* | 13% | — |
| Lavado de dinero | 11% | 4% |

* No cubierto en la encuesta de 2012

El robo de información, al igual que casi todos los tipos de fraude, habitualmente es un delito perpetrado internamente; no obstante, cada vez son más las personas ajenas a las empresas que aprovechan huecos de seguridad para obtener información y lucrar con ella.

Debido a esto, se vuelve importante saber cómo la organizaciones se preparan y hacen frente a esta situación, qué tan vulnerables se consideran ante esta amenaza y cómo les afectaría un incidente de esta índole. Diversos fabricantes de seguridad informática han detectado y desarrollado mecanismos que brindan protección de fuga de información que generalmente los denominan "Data Loss Prevention (DLP)".

DLP es un término de seguridad informática que se refiere a los sistemas que identifican, supervisan y protegen los datos en uso, los datos en movimiento, y los datos estáticos, sin importar el lugar donde se almacene o se utilice. Los sistemas están diseñados para detectar, prevenir el uso no autorizado y la transmisión de información confidencial de acuerdo a las reglas o políticas establecidas en cada organización.

Actualmente las entidades gubernamentales y privadas a nivel mundial están dando mayor importancia al manejo de la información, por lo que han establecido políticas, procedimientos, normas internas e inclusive en algunos países ya existen leyes que la regulan.

## Problemática

El corporativo de una prestigiosa tienda departamental sospecha que su información confidencial y datos de sus clientes han salido de su red, por lo que solicitó a su área de Seguridad Informática que le brinde una propuesta para identificar y dar solución a este requerimiento.

La información que ellos consideran crítica y que desean proteger es:

- Datos personales de sus clientes (nombre, dirección, número de cliente, RFC, e-mail, entre otras).
- Números de tarjetas de crédito
- Palabras claves que deseen proteger.

El departamento actualmente no cuenta con presupuesto para adquirir e implementar una herramienta especializada, sin embargo pide a sus ingenieros que hagan un análisis de los diversos fabricantes que lo ofrecen y que investiguen si su infraestructura actual puede solucionar temporalmente el requerimiento solicitado.

## Actividad a Realizar

Una vez identificado el problema, el corporativo de la tienda departamental solicita lo siguiente:

- Informe de herramientas especializadas en Data Loss Prevention, señalando lo que principalmente ofrece cada una de ellas ya que se realizará un estudio de mercado para elegir cuál de ellas cumple con sus expectativas.

- Validar si con la infraestructura actual se puede mitigar este problema y realizar el diseño e implementación de la solución para aminorar la fuga de información en la compañía. Presentar cómo se llevó a cabo dicha prueba.

La infraestructura actual de la empresa se muestra en la Figura 4.37.

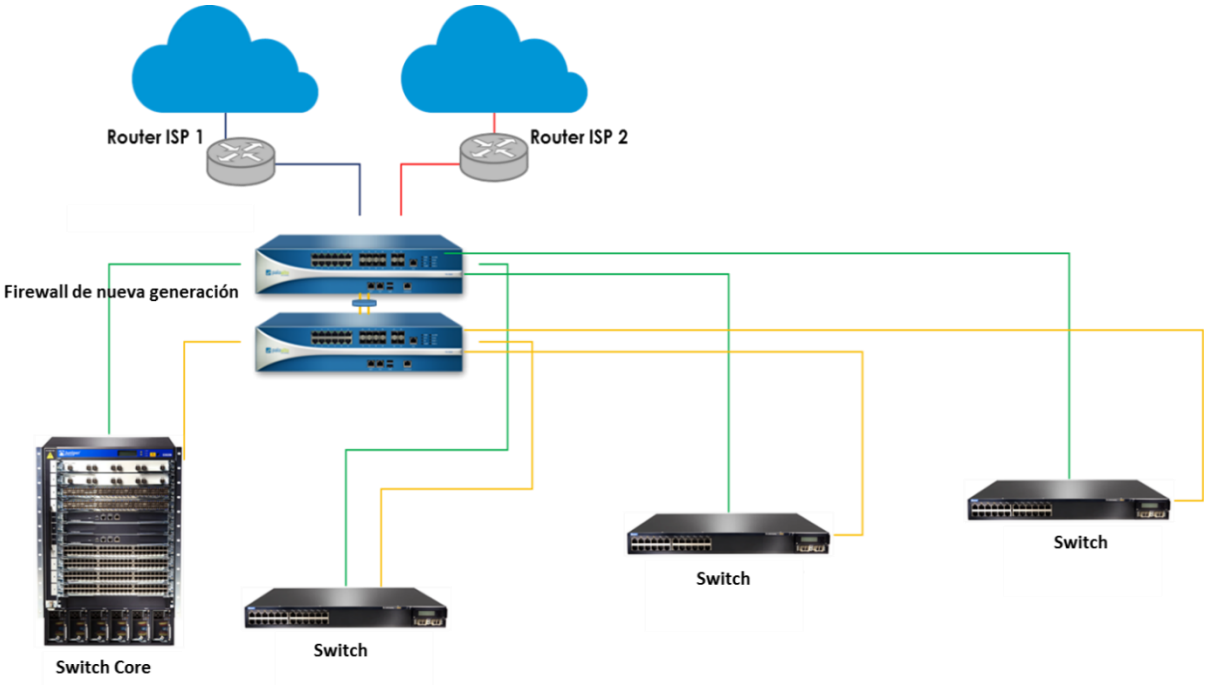



**Figura 4.37- Diagrama de red tienda departamental**

### Respuesta esperada:

El informe de alguna de las herramientas de Data Loss Prevention que los alumnos pueden entregar debe contener las características principales de cada una de ellas y mencionar que ventajas ofrece. Algunos ejemplos de fabricantes se presentan a continuación en la Tabla 4.18

**Tabla 4.18 Fabricantes herramientas Data Lost Prevention**

| Fabricante | Nombre de producto | Enlace con información |
|---|---|---|
| **Websense** | Data Security Suite | https://es.websense.com/content/data-security-suite-features.aspx |
| **Symantec** | Data Loss Prevention | http://www.symantec.com/es/mx/data-loss-prevention |
| **McAfgee** | Total Protection for Data Loss Prevention | http://www.mcafee.com/us/products/total-protection-for-data-loss-prevention.aspx |
| **EgoSecure** | EgoSecure EndPoint Protección de datos | http://egosecure.com/es/soluciones/ |
| **RSA-EMC** | Data Loss Prevention Suite | http://www.emc.com/data-protection/index.htm?nav=1 |

El estudio de Gartner muestra a los fabricantes líderes de este campo publicado el pasado Diciembre de 2013. (Véase Figura 4.38)

Fuente: http://www.gartner.com/technology/reprints.do?id=1-1O3ZIKF&ct=131213&st=sb


**Figura 4.38 – Cuadrante Gartner 2013 DLP**

## Respuesta esperada:

Analizando y buscando las características de cada dispositivo que conforma la red de la compañía se observa que en el Firewall Next Generation Palo Alto Networks contiene un módulo denominado "Data Filtering"

Data Filtering permite realizar mediante la utilización de expresiones regulares, palabras clave, o condiciones que se definen en reglas y perfiles para detectar y controlar la información que circule a través de esa red.

Un ejemplo de configuración y resultado de la implementación se observa en las Figuras 4.39 y 4.40:

| | Name | ID | Repeat Count |
|---|---|---|---|
| 1 | ZIP | 52004 | 1.0 M |
| 2 | Windows Executable (EXE) | 52020 | 7.7 K |
| 3 | Windows Dynamic Link Library (DLL) | 52019 | 3.8 K |
| 4 | RAR | 52015 | 187 |
| 5 | Windows Batch (BAT) | 52009 | 51 |
| 6 | Windows BAT | 52128 | 29 |

**Figura 4.39- Registros de control de Archivos**

| Receive Time | File Name | Name | From Zone | To Zone | Destination | To Port | Application | Action |
|---|---|---|---|---|---|---|---|---|
| 09/29 17:34:23 | | ZIP | outsidea | insideat | 10.12.62.61 | 59319 | web-browsing | alert |
| 09/29 17:34:10 | SharePane.swf | ZIP | outsidea | insideat | 10.1.137.57 | 61152 | flash | alert |
| 09/29 17:34:07 | | ZIP | outsidea | insideat | 10.11.171.131 | 52865 | web-browsing | alert |
| 09/29 17:34:04 | AF102430631.WAT | Windows Dynamic Link Library (DLL) | outsidea | insideat | 10.11.57.124 | 50738 | sharepoint-base | alert |
| 09/29 17:34:02 | | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64232 | web-browsing | alert |
| 09/29 17:34:01 | | ZIP | outsidea | insideat | 10.1.137.57 | 61152 | web-browsing | alert |
| 09/29 17:34:01 | Setup.exe | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64223 | web-browsing | alert |
| 09/29 17:33:55 | EasySpeedPC.exe | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64208 | web-browsing | alert |
| 09/29 17:33:55 | | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64219 | web-browsing | alert |
| 09/29 17:33:55 | setup_mbot_mx.exe | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64214 | web-browsing | alert |
| 09/29 17:33:54 | GenesisInstaller.exe | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64120 | web-browsing | alert |
| 09/29 17:33:54 | setup.exe | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64210 | web-browsing | alert |
| 09/29 17:33:53 | | Windows Executable (EXE) | outsidea | insideat | 10.3.198.165 | 64216 | web-browsing | alert |
| 09/29 17:33:51 | ith1167715478112490038.D2.pd.ipa | ZIP | outsidea | insideat | 10.1.137.27 | 54930 | apple-appstore | alert |
| 09/29 17:33:44 | | ZIP | outsidea | insideat | 10.11.174.20 | 64267 | web-browsing | alert |
| 09/29 17:33:34 | pad-builtin-wallpaper-1.jpg | ZIP | outsidea | insideat | 10.1.137.27 | 54917 | apple-appstore | alert |
| 09/29 17:33:33 | mzps6573205229973649199.ipa | ZIP | outsidea | insideat | 10.1.139.239 | 57367 | apple-appstore | alert |
| 09/29 17:33:28 | ModernNavigationAddButtonIcon.png | ZIP | outsidea | insideat | 10.1.137.27 | 54917 | apple-appstore | alert |

**Figura 4.40- Registros de actividad con control de archivos**

# Laboratorio 8.3 Servicios en la nube

## Objetivo

El alumno investigará en distintas fuentes de información cuales son los servicios que se proporcionan en la nube, así como los requisitos para la contratación de éstos.

## Materiales y Equipo

- Equipo de cómputo pare realizar la investigación.
- Artículos de periódicos, revistas, libros y otras fuentes que proporcionen información relacionados con el tema a abordar.

## Introducción

Día a día las necesidades de las personas y empresas cambian constantemente a un ritmo acelerado, para solventar esta necesidad las empresas y prestadores de servicios deben tener la posibilidad de brindar servicios de manera eficiente, rápida, segura y sobre todo que estén disponibles. Para realizar todas estas tareas, la mayor parte de las empresas gastan fuertes sumas de su presupuesto en actualizaciones de tecnológicas que permitan el funcionamiento continuo del negocio además de brindar servicios de alta Calidad.

Las aplicaciones comerciales tradicionales han sido siempre demasiado complicadas y caras implementarlas, la cantidad y la variedad necesaria de Software y Hardware requerido para ejecutarlas son inmensas y por tal motivo se necesita a todo un equipo de especialistas para que las puedan instalar, configurar, probar, ejecutar y actualizarlas. Cuando se multiplica este esfuerzo por años de trabajo y por cientos de aplicaciones, es fácil comprender por qué las empresas más grandes con los mejores departamentos de TI no están consiguiendo los resultados esperados.

Gracias a la tecnología conocida como Cloud Computing, las empresas pueden olvidarse de todas las inversiones en Hardware o Software y pueden contratar todo esto con un proveedor de servicios, éste tendrá la responsabilidad de proporcionar el Hardware y Software necesario para que todas las aplicaciones funciones de manera correcta. Las aplicaciones basadas en la Nube pueden implementarse y ejecutarse en cuestión de días o semanas a un menor costo. Con una aplicación en la Nube, solo es necesario bajar una aplicación en algún dispositivo móvil o abrir un explorador de Internet.

El Cloud Computing, es un concepto que se utiliza para hacer referencia a un conjunto de herramientas o servicios a los que se ingresan únicamente a través de Internet, Esta plataforma permite conectarse desde distintos dispositivos y aplicaciones, para acceder a información que se puede crear, compartir, almacenar y demás. El uso cada vez más frecuente de este servicio indica que se está atravesando por una transición en la que se abandona el uso exclusivo de la computadora de escritorio para ingresar a servicios, para sustituirla de manera gradual por diferentes dispositivos que permiten acceder a la información en cualquier momento y desde cualquier lugar.

Anteriormente el guardar archivos significaba almacenarlo en la computadora o en dispositivos de almacenamiento tal como una USB o discos duros externos. Si se necesitaba compartirlo con alguien más algún archivo o documento se hacía a través de correo electrónico o algún medio de almacenamiento externo. El uso de las aplicaciones que viven en la nube, ha permitido acceder a documentos desde cualquier dispositivo que tenga conexión a Internet, con la posibilidad de editarlo directamente en el navegador.

Entre las principales ventajas de utilizar la nube se encuentran:

- Bajo costo para implementación de nuevas aplicaciones.
- Disponibilidad de las aplicaciones e información
- Se puede utilizar en cualquier dispositivo que tenga acceso a Internet
- Las aplicaciones en la nube no dependen de un sistema operativo en específico para funcionar correctamente.
- No es necesario contar con algún dispositivo de almacenamiento para guardar la información.

Una de las grandes desventajas de utilizar los servicios en la nube es que es necesario contar con una conexión a Internet para ingresar a ellos.

## Problemática

Una empresa de electrodomésticos, cuenta con distintas aplicación que deben ser utilizadas por todos sus empleados desde cualquier dispositivo móvil. El área de TI encargada del proyecto, estuvo planeando la implementación del nuevo servicio y observo que necesita realizar una inversión considerable para sacarlo adelante. Revisando los presupuestos asignados para ese año, el llevar acabo la implementación del proyecto rebasa por mucho el tope presupuestal asignado para a el área de TI. Al encontrarse con esta situación, el área de IT propone llevar todos los servicios a la Nube y así bajar el costo del proyecto.

## Actividad a Realizar

Investigue más acerca de la Cloud Computing y comente entre el grupo lo encontrado, exponga sus puntos de vista y enliste cuales son las ventajas y desventajas de utilizar esta tecnología.

**Respuesta esperada:**

La respuesta dependerá de la información recolectada por cada alumno.

Realice una investigación con cualquier proveedor de servicios en la nube y adjunte la información en la cual se muestre los requisitos y servicios proporcionados por éste.

**Respuesta esperada:**

La respuesta dependerá del proveedor con el cual se haya investigado o contactado.

# Laboratorio 9.- Detección de amenazas y análisis de vulnerabilidades

## Laboratorio 9.1 Sistema de detección y prevención de intrusos

### Objetivo

El alumno explicará las diferencias que existen entre un sistema de detección de intrusos y un sistema de prevención de intrusos, así mismo realizará las configuraciones necesarias para implementar un IPs.

### Materiales y Equipo

- 1 firewall de nueva generación con módulo de IPs
- 2 Computadoras

### Introducción

Durante los últimos años las organizaciones han hecho cada vez más uso de dispositivos móviles, computadoras portátiles y nuevas tecnologías que se presentan para facilitar su trabajo y comunicarse con cualquier persona, esto es, aunado con el creciente uso de Internet hace que el trabajo de los administradores de las redes de datos se vuelva cada vez más complejo, debido a que tiene que mantener la red funcionando correctamente y también brindar un alto nivel seguridad. Por este motivo y debido a la importancia que han tomado las redes de datos, es necesario desarrollar políticas de seguridad cada vez más restrictivas que proporcionen un alto nivel de seguridad, pero sin interferir en las actividades que se realizan cotidianamente.

Es común escuchar noticias sobre algunas empresas a nivel mundial que han sufrido ataque de hackers en los cuales alguna o toda la información de sus clientes ha sido sustraída o que algún componente de su infraestructura ha sido afectado. En este contexto es donde surgen nuevos conceptos referentes a la seguridad en las redes, tales como: las vulnerabilidades y los ataques, dichas actividades se presentan tanto internamente como externamente en las organizaciones.

La diferencia entre estos términos, es que la vulnerabilidad tiene que ver con errores de software o de configuraciones que permiten a un intruso tener acceso a un sistema y comprometerlo, mientras que un ataque es un intento de explotar una vulnerabilidad en ese sistema. Las vulnerabilidades son los caminos para llevar a cabo un ataque, por eso es importante contar con herramientas dedicadas que ayuden a los administradores de la red a descubrir y proteger las vulnerabilidades que existen dentro de ésta, así como tener la posibilidad de detener cualquier ataque dirigido. Entre las tecnologías utilizadas para realizar estas tareas se encuentran los IDS e IPS.

Los sistemas de detección de intrusos (IDS) son sistemas que detectan y alertan las intrusiones suscitadas en un sistema o una red, éstos se encuentran constantemente vigilando, e incorporando mecanismos de análisis de tráfico, análisis de sucesos en sistemas operativos y aplicaciones, los cuales le permiten descubrir si existe algún evento intrusivo en tiempo real. Un IDS puede ser un dispositivo de Hardware o Software, el cual está conectado a una o varias redes; o bien una aplicación que se ejecuta en una o varias máquinas las cuales analizan el tráfico de red que sus interfaces capturan, los elementos generados por el sistema operativo y las aplicaciones locales.

Existen dos tipos de IDS, los cuales son:

- NIDS (Sistema de detección de intrusos de red): Estos sistemas disponen de una o varias interfaces de red conectadas a puntos estratégicos de la red, éste monitorea el tráfico que pasa por dichos puntos en busca de tráfico malicioso.

- HIDS (Sistemas de detección de intrusos de Host): Éstos se instalan en las maquinas que componen la red tales como estaciones de trabajo o servidores. Los HIDS tiene acceso a los archivos, por lo que pueden conocer de manera más fiable si un ataque fue exitoso o no.

Los IDS ofrecen un interesante servicio para el análisis forense después de la consumación de ataques. Es posible que un IDS no haya sido capaz de detener la acción de un atacante, pero si puede haber guardado un registro de los mensajes que transitaron por la red y así realizar una investigación más a fondo de lo sucedido durante el ataque.

Los IPS tiene varias formas de detectar el tráfico malicioso, algunas técnicas en los que basa su funcionamiento es:

- Detección basada en firmas
- Detección basa en políticas: El IPS requiere que se declaren específicamente las políticas de seguridad.
- Detección basada en anomalías: funciona como un patrón de comportamiento normal de tráfico, el cual es comparado permanente con el tráfico en línea, éste enviara una alarma o notificación cuando el tráfico real varíe respecto del patrón considerado como normal.

La diferencia entre un IPS y un IDS, es que el IDS es una herramienta reactiva pues alerta al administrador ante la detección de un posible intruso, mientras que un sistema de prevención de intrusos es proactivo, debido a que establece políticas de seguridad para proteger los equipos o la red de un posible ataque.

## Problemática

Una organización gubernamental en recientes días ha sido blanco de distintos ataques informáticos, los cuales comprometieron la disponibilidad de algunos equipos, así como el ingreso de código sobre distintas base de datos. Durante la junta para saber qué fue lo que sucedió, se observó que el firewall con el que cuenta, no fue capaz de detectar o detener

los ataques realizados, debido a que el módulo de UTM con el que cuenta no estaba correctamente configurado, además de presentar un mal diseño sobre la arquitectura de red la cual se observa en la Figura 4.41.

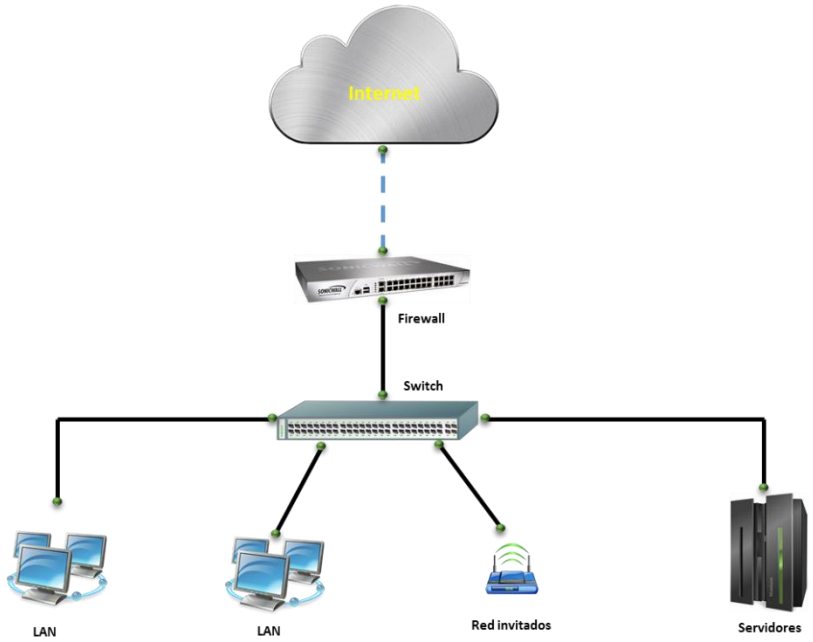



**Figura 4.41 – Diagrama de red organización gubernamental**

Revisando la forma en la que esta implementada la red, se observó que es plana, esto quiere decir que tiene un mismo direccionamiento para toda la red sin importar si son invitados, servidores o host de los empleados de la institución. Las direcciones IP son asignadas a través del Firewall mediante su servidor DHCP y también se cuenta con un rango de direcciones estáticas pertenecientes al mismo segmento para asignarla a los servidores. Después de analizar las debilidades con las que cuenta su red, las áreas encargadas de la administración y la seguridad, decidieron realizar una nueva arquitectura y diseño en su red corporativa. Para ello lanzaron una convocatoria en la cual se requiere la adquisición de nuevos dispositivos de red para fortalecer la seguridad.

Dentro de la convocatoria se solicitan los siguientes puntos:

- Filtrado de aplicaciones y contenido en la Web.
- Descifrado de contenido sobre protocolo SSL
- Equipo con módulo de IPS (Antivirus, Antispyware, Protección de vulnerabilidades).
- Bloqueo de archivos.
- Filtrado de datos (A nivel de expresiones regulares).
- Consola de administración basada en Web.
- Clientes de VPN SSL.
- 100 VPN IPSec.
- Creación de reportes personalizados.
- 8 interfaces 10/100/1000.
- Puerto consola e interfaz de administración.

- 250 Mbps Firewall throughput.
- 7 500 nuevas sesiones por segundo.
- 1 000 usuarios.

## Actividad a Realizar

Con base a lo explicado en la problemática, enliste cuales son las vulnerabilidades que presenta la red y proporcione sus recomendaciones.

**Respuesta esperada:**

La respuesta del alumno variará de acuerdo a los criterios de cada uno. A continuación se presenta en la Tabla 4.19 algunas posibles respuestas así como su solución.

**Tabla 4.19 - Vulnerabilidades presentadas en la red**

| Vulnerabilidades | Solución |
|---|---|
| **Único direccionamiento de red** | Creación de varios segmentos de red para las distintas áreas o la creación de VLANs |
| **Políticas de seguridad** | Creación de políticas de seguridad más restrictivas. |
| **Configuración correcta en UTM** | Definición de perfiles dependiendo la aplicación o servicio que se quiera proteger. |
| **Políticas de filtrado Web y de aplicaciones** | Se deben crear políticas de control de aplicaciones y filtrado Web para cada una de las áreas que componen la empresa. |
| **Normas de seguridad** | Se deben instaurar normas a los usuarios, en cuestión del uso de las computadoras, así como el uso de dispositivos de almacenamiento externos. |

De acuerdo a las especificaciones solicitadas durante la convocatoria, investiga distintos modelos y marcas, que tengan dichas características y elige uno que consideres que será el que mejor cumple con las expectativas para la nueva arquitectura.

**Respuesta esperada:**

La propuesta del o los equipos solicitados dependerá de la arquitectura que el alumno proponga, sin embargo por motivos de la práctica el equipo que debe ser propuesto deberá contar con todos los módulos solicitados.

Con base al equipo elegido realiza una presentación de la tecnología y describe como llevarías a cabo la protección ante vulnerabilidades y ataques, incluyendo el diseño de una nueva arquitectura de red para la institución gubernamental y exponga ante el salón de clases por qué su propuesta sería la mejor para llevar a cabo la implementación y justifique por qué su diseño aumenta la seguridad de la red.

**Respuesta esperada:**

La arquitectura propuesta, dependerá de los equipos que el alumno haya utilizado para su diseño, sin embargo se debe tomar en cuenta que la practica deberá ser realizada con el equipo con el que cuenta el laboratorio. A continuación se propone una arquitectura de red basada en un firewall de nueva generación, el cual cumple con las características solicitadas en la problemática. Así mismo se explica la forma en la que la arquitectura propuesta ayudará a aumentar la seguridad en la red.

Una de las principales medidas de seguridad a tomar es el separar en distintas subredes las áreas tal y como se muestra en la Tabla 4.20.

**Tabla 4.20 - zonas de seguridad**

| **Red** | Zona | Subred | VLAN |
|---|---|---|---|
| **Servidores** | Servidores | 192.168.200.0/24 | - |
| **Red LAN** | LAN | - | 192.168.10.0/24 |
| **Invitados** | LAN | - | 192.168.20.0/24 |

Otro punto a tomas en cuenta es el crear distintos perfiles de seguridad entre los cuales se encuentran:

- **Antivirus:** Este tipo de Perfil únicamente bloqueará, alertará o permitirá todo aquel virus que viaje a través de los siguientes protocolos: FTP, HTTP, IMAP, POP3, SMB y SMTP.

- **Spyware:** El perfil identificara todo Spyware que contenga en su Base de datos, este clasifica en distintos niveles de severidad, lo más recomendable es bloquear todo aquella firma que sea considerado como de un nivel Crítico, Alto y Medio.

- **Vulnerabilidades:** Ésta basa su funcionamiento en una serie de firmas que son actualizadas constantemente con las últimas amenazas detectadas, además de ser catalogadas con un nivel de criticidad información, bajo, medio, alto y crítico. Entre las acciones que se realizan en este perfil se encuentran permitir, alertar y Bloquear. Por buenas prácticas se recomienda colocar los niveles de criticidad alto, medio y crítico en Bloquear.

Cada uno de estos perfiles debe ser integrado a una política de seguridad la cual analizará el tráfico, revisando si existe alguna coincidencia con las firmas de cada uno de los perfiles configurados.

La arquitectura de red propuesta tiene como objetivo separar la red en distintas zonas de seguridad, esta división aumentará en gran medida la seguridad del tráfico que viaja a través de la red. En la Figura 4.42 se muestra una posible arquitectura.

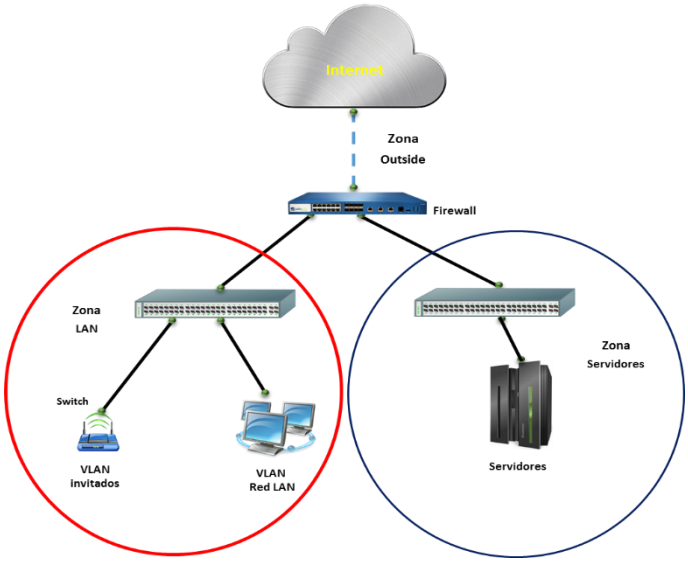



**Figura 4.42 – Diagrama de red propuesto organización gubernamental**

Se recomienda que por cada una de las zonas a proteger se realicen distintos perfiles de seguridad en donde se determine cuáles de ellos deben estar con un nivel de seguridad más alto y tomar todas las medidas preventivas necesarias.

Después de haber discutido en grupo las distintas arquitecturas, así como las medidas de seguridad a tomar, realice las configuraciones necesarias para que el escenario propuesto sea funcional.

**Respuesta esperada:**

El alumno deberá realizar las siguientes configuraciones para que el escenario propuesto quede completamente configurado:

- **Salida a internet**: El alumno realizarás las configuraciones necesarias, para que la red de invitados y la red LAN tengan salida a internet.

- **Creación de perfiles y políticas de seguridad**: Se deberán crear políticas de seguridad las cuales permitan el ingreso a los servicios publicados. Los perfiles de seguridad deberán de ser configurados de tal manera que la seguridad del tráfico que pasa a través de la red sea completa.

- **Creación de perfiles de seguridad** (AntiVirus, Anti-Spyware y Vulnerability Protection) para cada una de las zonas teniendo diferentes niveles de protección entre ellas.

Una vez realizadas la configuración investigue y realice ataques dirigidos al escenario creado, se debe probar que la red se encuentra protegida ante ataques mediante malware, código malicioso o vulnerabilidades. Realice las pruebas ante el profesor y muestre los resultados obtenidos.

**Respuesta esperada.**

El alumno instalará y ejecutará un programa que lleve a cabo un escaneo de vulnerabilidades, algunos programas que están disponibles para realizar esto son Nexpose, Acunetix o Nessus. Además debe mostrar evidencia del escaneo realizado, así como de lo detectado por el IPS, a continuación se presenta en la Figura 4.43 y 4.44 un ejemplo de lo que el alumno debe entregar.

**Top de Vulnerabilidades y Ataques.**

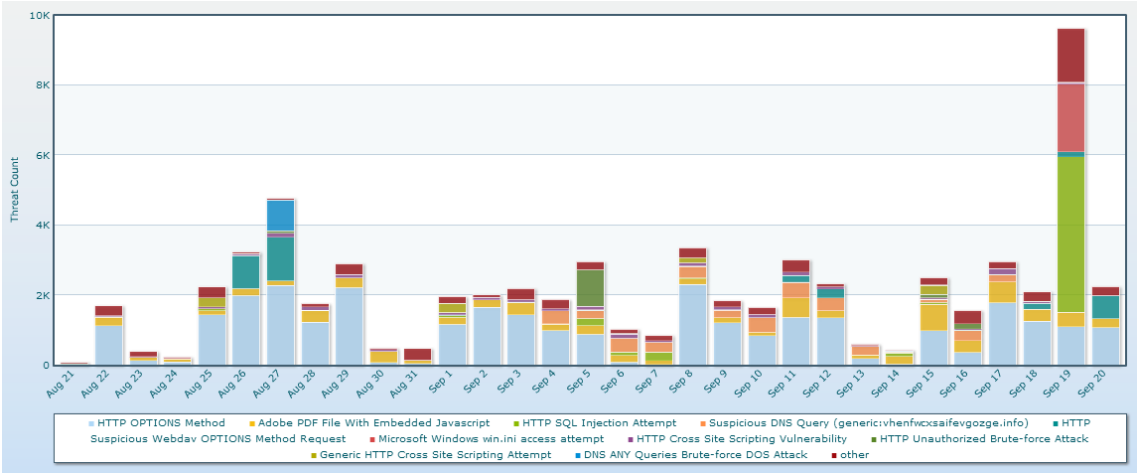



**Figura 4.43 – Top vulnerabilidades y ataques**

**Registro de tráfico y validar que se encuentre bloqueado.**

| | | Receive Time | Type | Name | ID | From Zone | To Zone | Attacker | A... N... | Victim | To Port | Application | Action | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 09/20 18:51:44 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 186.109.86.227 | | | 40702 | unknown-udp | drop-all-packets | critical |
| | | 09/20 18:21:16 | spyware | Win32.Conficker.C p2p | 12544 | outsidea | DMZ1 | 213.98.71.253 | | | 19435 | unknown-udp | drop-all-packets | critical |
| | | 09/20 18:11:37 | vulnerability | HTTP /etc/passwd access attempt | 35107 | outsidet | DMZ1 | 190.120.7.14 | | | 80 | web-browsing | drop-all-packets | high |
| | | 09/20 17:56:19 | vulnerability | SMB: User Password Brute-force Attempt | 40004 | insideat | DMZ1 | 10.1.80.221 | ... | | 445 | ms-ds-smb | drop-all-packets | high |
| | | 09/20 17:27:14 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 218.111.97.205 | | | 31493 | unknown-udp | drop-all-packets | critical |
| | | 09/20 12:31:59 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 85.32.99.202 | | | 34822 | unknown-udp | drop-all-packets | critical |
| | | 09/20 09:50:12 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 82.104.56.137 | | | 49085 | unknown-udp | drop-all-packets | critical |
| | | 09/20 09:10:43 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 210.75.15.50 | | | 40218 | unknown-udp | drop-all-packets | critical |
| | | 09/20 08:42:19 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 93.139.157.87 | | | 43225 | unknown-udp | drop-all-packets | critical |
| | | 09/20 05:45:01 | vulnerability | Microsoft ASN.1 Library Heap Overflow Vulnerability | 30780 | outsidet | DMZ1 | 62.133.26.34 | | | 445 | ms-ds-smb | drop-all-packets | critical |
| | | 09/20 01:31:21 | spyware | Win32.Conficker.C p2p | 12544 | outsidet | DMZ1 | 177.101.232.131 | | | 58819 | unknown-udp | drop-all-packets | critical |
| | | 09/19 21:55:29 | vulnerability | SMB: User Password Brute-force Attempt | 40004 | insideat | DMZ1 | 10.1.80.221 | ... | | 445 | ms-ds-smb | drop-all-packets | high |
| | | 09/19 21:05:56 | vulnerability | Internet Explorer Improper URL Canonicalization Domain Spoofing Vulnerability | 30140 | outsidea | insideat | 205.185.216.42 | | | 54157 | web-browsing | drop-all-packets | high |
| | | 09/19 20:37:02 | vulnerability | Internet Explorer Improper URL Canonicalization Domain Spoofing Vulnerability | 30140 | outsidea | insideat | 205.185.216.10 | | | 34316 | web-browsing | drop-all-packets | high |
| | | 09/19 20:23:26 | vulnerability | Internet Explorer Improper URL Canonicalization Domain Spoofing Vulnerability | 30140 | outsidea | insideat | 205.185.216.42 | | | 49398 | web-browsing | drop-all-packets | high |

**Figura 4.44 – Registro de tráfico de vulnerabilidades**

# Laboratorio 9.2 Análisis de vulnerabilidades

## Objetivo

El alumno investigará y analizará todo lo que se necesita para llevar a cabo un análisis de vulnerabilidades en diferentes equipos de cómputo, utilizando herramientas que ayuden a detectar cualquier vulnerabilidad que se presente.

## Materiales y Equipo

- Equipo de cómputo
- Software libre o versión prueba para el análisis de vulnerabilidades.
- Sistema operativo que se compatible con las herramientas de análisis de vulnerabilidades.

## Introducción

La palabra vulnerabilidad en seguridad informática hace referencia a una brecha de un sistema que permite a un perpetrador comprometer la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema, de sus datos o aplicaciones. Las vulnerabilidades son el resultado de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas. Las vulnerabilidades se clasifican en 6 tipos las cuales son:

- **Física:** Este tipo de vulnerabilidades se refiere al control de acceso físico al sistema.
- **Natural:** la vulnerabilidad natural se refiere a que grado puede verse afectado el sistema por desastres naturales o ambientales.
- **Hardware:** el no revisar las características de los dispositivos así como la falta de mantenimiento de estos, presenta una vulnerabilidad del tipo Hardware.
- **Software:** El que un programa presente fallas o debilidades hace más fácil acceder a ellos y por lo tanto lo hace más vulnerable ante algún tipo de ataque que se puede presentar.
- **Red:** el mal planeamiento de una red no siguiendo los estándares de cableado estructurado y otro tipo de estándares, presentan una amenaza de riesgo potencialmente alta.
- **Humana:** Las vulnerabilidades de este tipo suelen ser las más comunes y las que menos se puede evitar ya que por más que se trate de evitarlas no se puede cubrir la mayoría, algunos ejemplos de este tipo de vulnerabilidades pueden ser:

- Ingeniería social
- Mala comunicación con el personal
- Contratar personas sin un perfil psicólogo y ético
- El descuido

Los tipos de vulnerabilidades que con mayor frecuencia son explotadas en el ámbito de redes y seguridad son las de software, red y hardware ya que se descubren vulnerabilidades constantemente en todo tipo de sistemas y aplicaciones, y el hecho de que se publiquen rápidamente hace que existan más probabilidades para que los atacantes quieran aprovecharse de ellas.

Una de las preocupaciones más importantes del área de seguridad informática en las organizaciones es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas de información así como en los componentes de la infraestructura de las redes de datos, las cuales son el objetivo principal de herramientas de software cada vez más sofisticadas en su capacidad de ocasionar daños a los sistemas de información así como a la infraestructura que los soporta. Con el fin de incrementar la seguridad en las empresas es necesario realizar un análisis de vulnerabilidades para identificar aquellos huecos de seguridad que se encuentran expuestas en la red que se quiere proteger.

Lo anterior muestra que es crucial contar con un plan de acción efectivo donde se deban de identificar y mitigar los riesgos a los que se encuentra expuesta la empresa, de tal modo que se esté preparado para superar cualquier eventualidad que interrumpa, dañe o perjudique las actividades habituales de las organizaciones y que se definan las medidas de seguridad adecuadas con la finalidad de reducir los riesgos a los que pueda estar sometida, evitando que se efectúe una amenaza.

## Problemática

En una empresa de reclutamiento y selección de personal que tiene más de 20 años en el mercado cuenta con una gran cantidad de información recabada a lo largo de ese tiempo, ésta se tiene resguardada en un sistema de información centralizada en su Data Center de la Ciudad de México, sin embargo, hace algunas semanas se suscitó un incidente de seguridad en donde alteraron su base de datos con información sensible de sus clientes y de las empresas para las que trabaja, este acontecimiento provocó que la organización tomara las medidas necesarias para que ataques de este tipo no pasen nuevamente, para ello solicitaron a una empresa encargada de seguridad informática que realizara un análisis de vulnerabilidades de la situación actual en todos sus servidores, así como la implementación de soluciones que les brinde protección.

A continuación se muestra en la Figura 4.45 el diagrama de red, así como en la Tabla 4.21 la cantidad de los servidores que integran su red de Data Center.

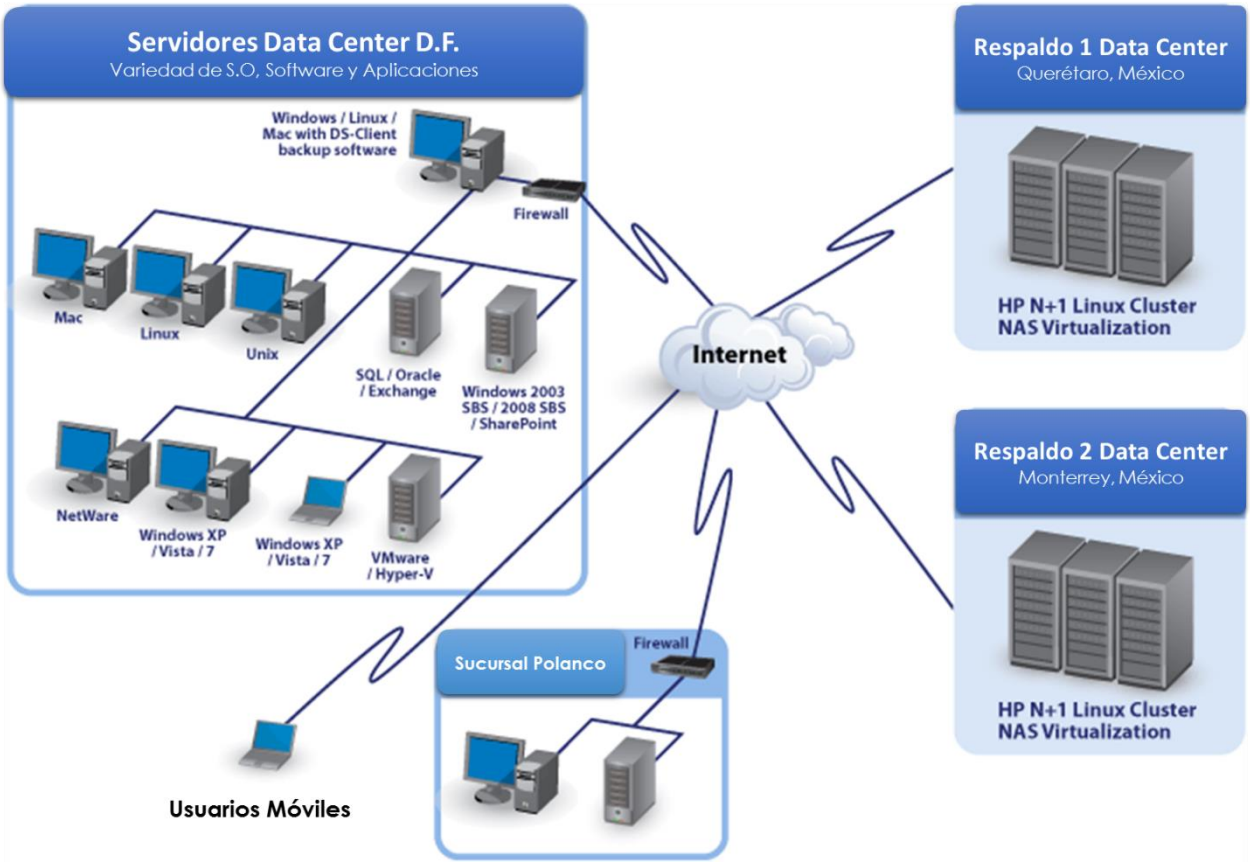



**Figura 4.45 diagrama de red Data Center**

| Tabla 4.21 Componentes Data Center | | | |
|---|---|---|---|
| Servidores Linux | 4 | SQL / Oracle / Exchage | 53 |
| Windows XP/ Vista/ Windows 7 | 10 | Windows 2005 / SSB5 / 2008 | 44 |
| Mac | 8 | VMware / Hyper-V | 10 |
| Usuarios Móviles | 150 | HP N+1 Linux Cluster NAS Virtualization | 2 |
| Firewall | 1 | | |

## Actividad a Realizar

Con base a la información presentada por la empresa, el grupo de ingenieros que fue contratado para realizar el análisis de vulnerabilidades, deberá realizar una lista de todos los dispositivos que existen dentro de la red, la cual ayudará a decidir en conjunto con la empresa, qué servicios son considerados como de alta criticidad.

### Respuesta esperada

El alumno deberá de realizar esta actividad en conjunto de su profesor, para que cada equipo tenga un escenario distinto se les indicarán cantidades y sistemas operativos

diferentes a analizar. Un ejemplo del resultado de este listado de componentes se muestra en la Tabla 4.22.

| Tabla 4.22 – Propuesta componentes de Data Center | | |
|---|---|---|
| **Componente** | **Número de servidores** | **Criticidad** |
| Servidores Linux | 4 | Todos son nivel críticos |
| Windows XP/ Vista/ Windows 7 | 10 | 5 nivel críticos<br>5 nivel alto |
| Mac | 8 | 4 nivel crítico<br>3 nivel alto<br>1 nivel medio |
| Usuarios Móviles | 150 | 150 nivel medio |
| Firewall | 1 | No se le hará análisis |
| SQL / Oracle / Exchage | 53 | 45 nivel critico<br>8 nivel alto |
| Windows 2005 / SSB5 / 2008 | 44 | 25 nivel critico<br>18 nivel alto |
| VMware / Hyper-V | 10 | 10 nivel critico |
| HP N+1 Linux Cluster NAS Virtualization | 2 | 2 nivel critico |

Una vez organizada y determinada la información para este análisis, el grupo de especialistas considera que el análisis de vulnerabilidades se aplicará en primera fase únicamente a los servidores que estén categorizados como de nivel crítico para que los servicios y los datos resguardados en estos dispositivos sean los principales activos a proteger, para ello se deberán de entregar un análisis detallado de las vulnerabilidades que se hayan encontrado y brindar la descripción de cada una de ellas, buscando si se tiene un registro en CVE (Common Vulnerability & Exposures).

**Respuesta esperada**

El profesor indicará a los alumnos que busquen herramientas o algún tipo de software que sean capaces de determinar qué vulnerabilidades se han encontrado en los servidores seleccionados.

Una herramienta ejemplo que podrían utilizar es Deep Security de Trend Micro con el módulo Intrusion Prevention. Este se encarga de realizar un escaneo de vulnerabilidades personalizado en los equipos, brindándoles la opción de protegerlos ante ella.

El análisis en cada equipo aparecerá como se muestra en la figura 4.46, por lo que el alumno hará un breve listado de las vulnerabilidades críticas o altas que encuentre y brindará un mayor detalle de cada una de ellas.

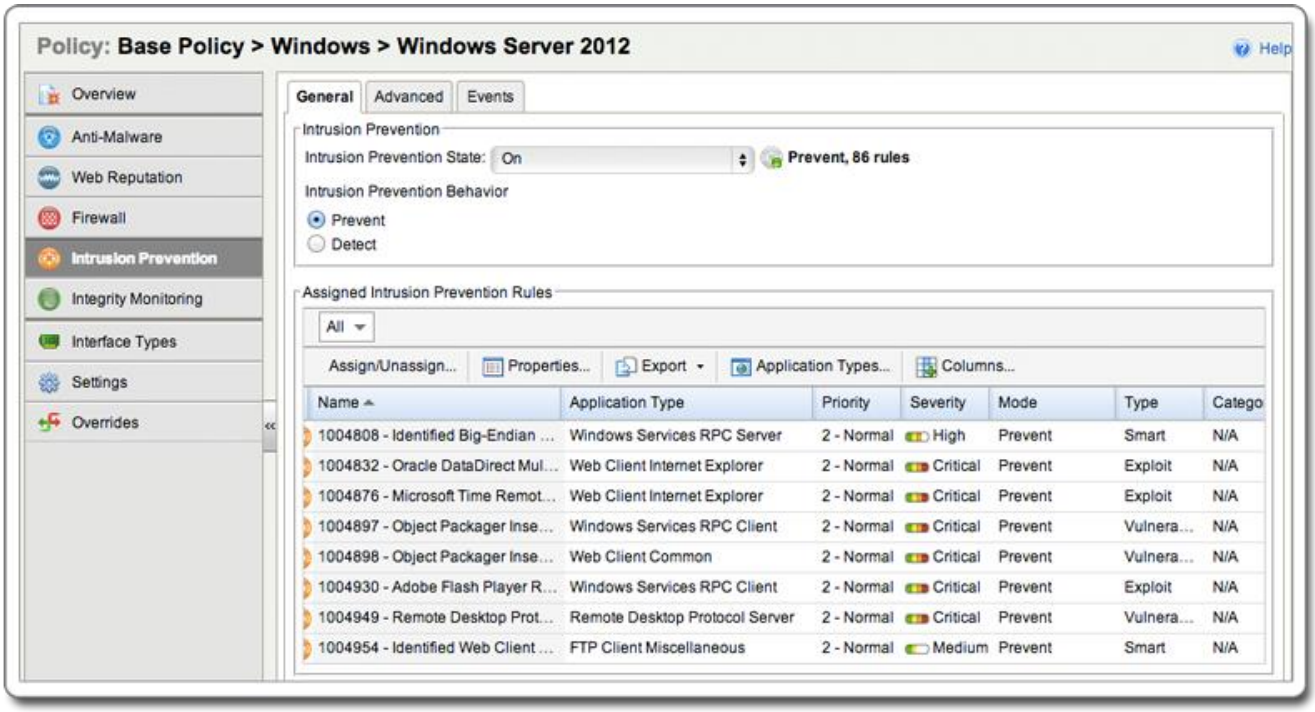



**Figura 4.46 Análisis de vulnerabilidades**

### Ejemplo de vulnerabilidades

El alumno investigará sobre las vulnerabilidades que considere que son más críticas, y entregará una tabla con la información obtenida, tal y como se observa en la Tabla 4.23

**Tabla 4.23 Vulnerabilidades críticas**

| Nombre | Sistema Operativo | Vulnerabilidad |
|---|---|---|
| Servidor1 | Windows XP | Nombre: *MS08-067* - Se trata de una vulnerabilidad calificada como crítica en el servicio de servidor porque permite ejecutar remotamente código arbitrario en el sistema vulnerable. El servicio de servidor permite compartir los recursos locales de un usuario, como discos e impresoras, para que otros usuarios de la red puedan tener acceso a los mismos. Tiene el *CVE*-2008-4250 |
| Servidor2 | Windows Server 2003 | Nombre MS12-004 – Se trata de una vulnerabilidad que permite la ejecución remota de código si un usuario abre un archivo multimedia con Windows Media especialmente diseñado. Un atacante que explote exitosamente la vulnerabilidad podría conseguir el mismo nivel de derechos de usuario que el usuario local |

Después de haber realizado el análisis en los dispositivos críticos y la investigación de ellas, tome las medidas necesarias para que se realice la protección del equipo. Indique qué

actividades realizó para asegurar que están protegidos ante estas vulnerabilidades antes detectadas.

### Respuesta esperada

El alumno elegirá el método que considere más adecuado de acuerdo a su investigación de las vulnerabilidades halladas, entre las actividades que se realizará se encuentran las siguientes:

- Actualización de Sistemas Operativos
- Aplicaciones de parches
- Aplicación de fixes
- Instalación de Anti-Virus
- Implementar herramientas de seguridad que brinden protección ante las vulnerabilidades encontradas.
- Entre otras.

Finalmente, compruebe a través de un nuevo análisis, que los servidores anteriormente escaneados ya no presentan las vulnerabilidades antes descubiertas.

### Respuesta esperada

El alumno deberá realizar nuevamente el análisis de vulnerabilidades y en dicho reporte no deberán de aparecer los mismos registros un ejemplo se observa en la Figura 4.47

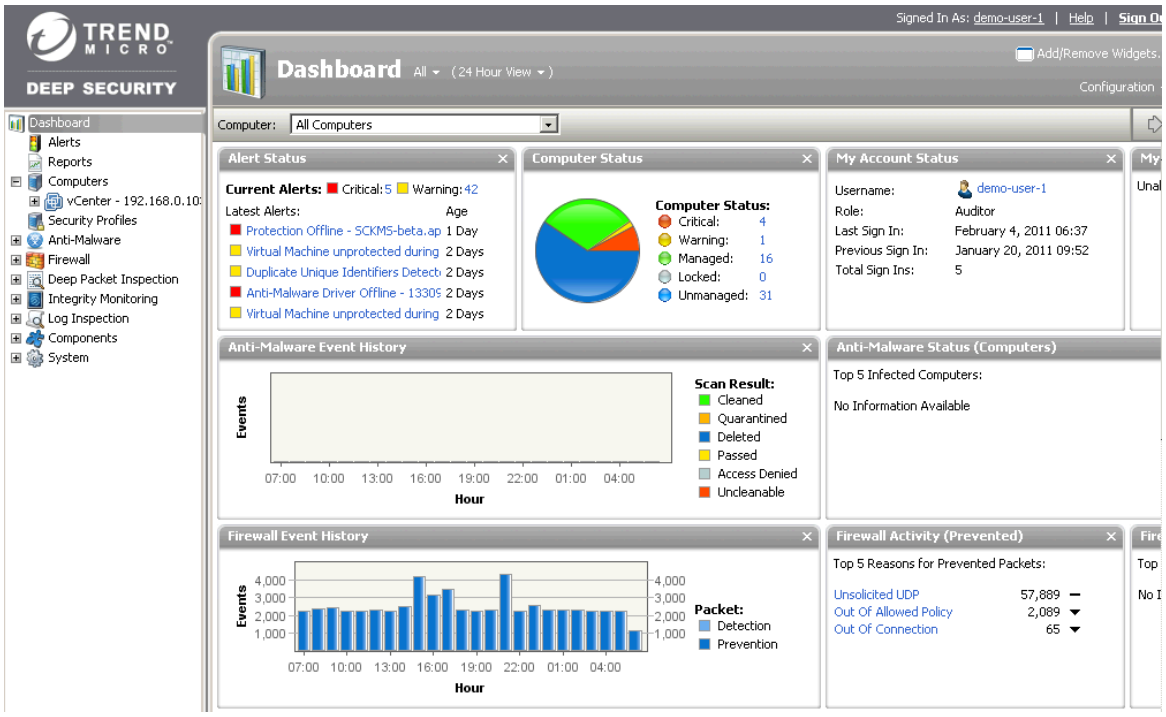



**Figura 4.47 – Escaneo de vulnerabilidades**

Opcionalmente el alumno tratará de explotar alguna de las vulnerabilidades identificadas mediante un ataque dirigido, el resultado de éste deberá ser la nula ejecución de éste.

# Laboratorio 10.- Monitoreo de dispositivos y aplicaciones de red

**Laboratorio** **Trazas de monitoreo de Networking**

## Objetivo

El alumno investigará que protocolos son utilizados para llevar a cabo el monitoreo en las redes de datos, así como las herramientas que son utilizadas para hacer esta actividad. Además tendrá que realizar la configuración y puesta a punto de un herramienta de monitoreo, la cual permitirá el monitoreo de un dispositivo de red.

## Materiales y Equipo

- Equipo de cómputo
- Dispositivos de redes de datos que soporten protocolo SNMP
- Software libre o versión prueba para el monitoreo de red.
- Sistema operativo que se compatible con las herramientas de monitoreo.

## Introducción

Las empresas hoy en día requieren de un proceso de monitoreo de red, el cual es considerado como fundamental y que en la gran mayoría de las veces es ignorado, por falta de presupuesto, por lo que la ausencia del monitoreo en la mayoría de los casos trae como consecuencia:

- Aumento de costos no previstos
- Bajo nivel de servicio organizacional, y
- Deterioro de la infraestructura de red.

La función de monitoreo de la red de una organización debe ser una labor continua ya que la infraestructura que la conforma es un organismo que necesita de una permanente supervisión de todos sus componentes, a fin de conocer oportunamente las interrupciones de servicios, el tráfico que puede soportar un dispositivo, caídas en los servicios por parte de los proveedores de Internet, ataques suscitados que atenten contra la disponibilidad de los dispositivos y comportamiento anómalo dentro de la red, entre otras situaciones que requieran de la intervención de los ingenieros de la red para evitar el colapsos o saturaciones que ponen en riesgo la continuidad de la operación.

El área encargada del monitoreo de los dispositivos de red es el NOC ("Network Operations Center") o Centro de Operación de Red, el cual tiene como función monitorear todo el ambiente de TI con el que cuenta la empresa a fin de asegurar que el servicio de tecnología ofrecido en todos los niveles, corresponda a lo necesario para las

actividades de la organización. El monitoreo que realiza el NOC abarca distintos componentes de la infraestructura, tales como:

- Computadoras
- Routers
- Switches
- Conmutadores telefónicos
- Servidores
- Firewalls
- Servicios en la nube
- Enlaces de Internet
- Redes MPLS

El NOC lleva a cabo el monitoreo utilizando dos enfoques que son:

- ***Monitoreo activo:*** *Este monitoreo se lleva a cabo mediante el envío de paquetes de prueba a la red o a determinadas aplicaciones, midiendo sus tiempos de respuesta. Este monitoreo tiene la característica de agregar tráfico en la red y es comúnmente utilizado para medir el rendimiento en una red. Algunas de las técnicas que son utilizadas para este monitoreo son:*

  - ***Basado en ICMP***

    - *Se detectan problemas en la red.*
    - *Detecta retardos y pérdidas de paquetes.*
    - *Verifica la disponibilidad de host y elementos de red.*

  - ***Basado en TCP***

    - *Tasa de transferencia*
    - *Diagnosticar problemas a nivel de aplicación.*

  - ***Basado en UDP***

    - *Pérdida de paquetes en un sentido*

- ***Monitoreo pasivo:*** *Se basa en la obtención de datos a partir de recolección y análisis el tráfico que circula por la red, se emplean diversos dispositivos para llevar a cabo este monitoreo como: sniffers, equipo que interconectan a la red (Switch, Router, Hub) y computadoras que tienen instalado algún software para el análisis de tráfico y que soporten los protocolos SNMP, NETFLOW y RMON. A diferencia del monitoreo activo este no agrega tráfico, y es utilizado principalmente para contabilizar el uso de la red.*[1]

[1] Ing. Carlos Alberto Vicente Altamirano, Seminario ADMIN-UNAM "Seguridad Perimetral" Tema: Monitoreo de Recursos de Red, UNAM 2005.

## Problemática

Una aerolínea tiene publicado su sistema de venta de boletos por Internet, en varias ocasiones han sufrido percances al no tener disponibles sus servicios, teniendo como consecuencia grandes pérdidas económicas y el disgusto de sus usuarios, por esta situación la directiva necesita que se tomen las medidas necesarias para que esto no vuelva a suceder. La directiva solicitó a los gerentes de las áreas de redes implementar un centro de monitoreo el cual tendrá la función de visualizar la disponibilidad de todos los componentes que conforman la red de dicha organización en tiempo real, además de identificar de manera proactiva cualquier incidente que se suscite.

Los gerentes de cada área establecieron una lista de los equipos y aplicaciones que consideran críticos para la operación de la aerolínea, en la Tabla 4.24 se enlistan los dispositivos que serán integrados al centro de monitoreo de red (NOC).

| Tabla 4.24 - Dispositivos a monitorear | | |
|---|---|---|
| **Listado de equipos** | | |
| 2 Firewall | 1 Gateway VoIP | 5 Servidores DNS |
| 3 Enlaces de Internet | 1 IP / PBX | 2 Túnel VPN |
| 2 Switch Core | 25 Servidores Web Windows | 12 Servidores FTP |
| 4 Switch DMZ | 3 Servidores de correo | 40 Servidores BD |

Ademas de establecer los dispositivos a monitorear, en la Figura 4.48, se presenta el diagrama de red con el que cuenta la aerolinea

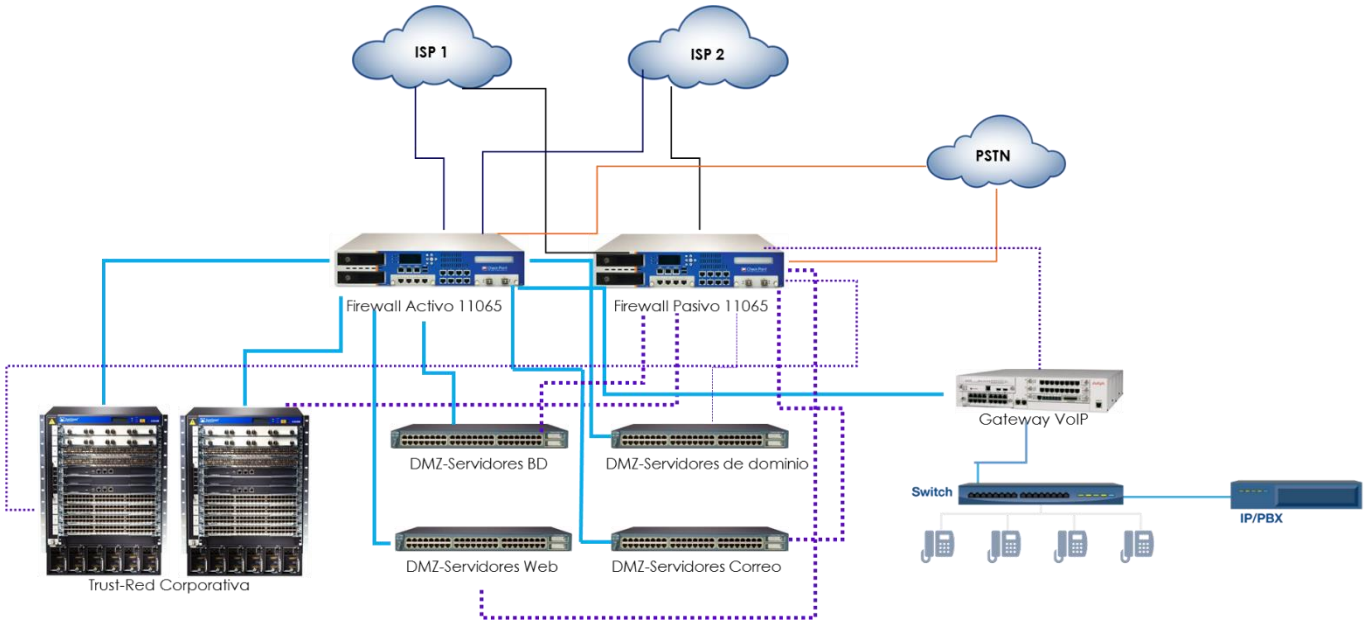



**Figura 4.48 - Diagrama de red aerolínea**

## Actividad a Realizar

Una vez identificados los equipos a monitorear, se les asignó a los gerentes que llevaran a cabo la implementación y el diseño del NOC, y para ello se les pidió que presentaran un documento justificando qué herramienta van a utilizar y como estará conformado. Los requisitos mínimos que debe cumplir la herramienta a implementar son los siguientes:

### Monitoreo pasivo

- Herramienta basada en protocolo SNMP.
- Que monitoree la disponibilidad y el desempeño, analice el uso del tráfico y administre las configuraciones de los Routers, Switches, firewalls, aceleradores WAN y puntos de acceso inalámbrico.
- **Que lleve a cabo el monitoreo del estado general de un dispositivo de red.**
- **Que permita realizar análisis de red mediante el registro de tendencias.**
- **Tener un sistema de notificaciones de alertas mediante correo electrónico o SMS.**
- Que monitoree el desempeño de los servidores en múltiples sistemas operativos

### Monitoreo activo

- Monitoreo de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
- Monitoreo de los recursos de un host
- Monitoreo remoto, a través de túneles SSL cifrados o SSH.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Interfaz web opcional, para observar el estado de la red actual, notificaciones, historial de problemas, archivos de registros, etc.
- Reportes y estadísticas del estado cronológico de disponibilidad de servicios

### Respuesta esperada

Alguna de las posibles herramientas que el alumno propodrá para realizar el monitoreo solicitado se describen en la Tabla 4.25.

**Tabla 4.25 Herramientas de monitoreo**

| Herramienta de Monitoreo | Características |
|---|---|
| **Nagios (Monitoreo activo)** | Nagios es un sistema de monitorización de equipos y de servicios de red, escrito en C y publicado bajo la GNU General Public License, el lenguage con el cual está desarrollado asegura una rápida ejecución y su licencia que lo determina como Software Libre hace que siempre tenga actualizaciones disponibles y que hay una gran comunidad de desarrolladores soportándolo. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP, entre otros) el monitoreo de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria,), independencia de sistemas operativos. |

| | |
|---|---|
| **OpManager(Monitoreo Pasivo)** | Esta herramienta ofrece a través del protocolo SNMP, una funcionalidad avanzada de gestión de fallas y desempeño, en todos los recursos críticos de TI tales como enrutadores, enlaces WAN, conmutadores, firewalls, rutas de llamada VoIP, servidores físicos, servidores virtuales, controladores de dominio y otros dispositivos de infraestructura de TI. Además, combina una interfaz que le permite implementar, así como aplicar las políticas de monitoreo en múltiples dispositivos. Entre las principales características se encuentran:<br>- Paneles de monitoreo y detección de redes<br>- Mapa automático de redes<br>- Mapas personalizados<br>- Vista de Google Maps<br>- Análisis de tráfico de red<br>- Gestión de configuración de redes |

Una vez presentado el documento con las herramientas que se eligieron para el NOC, se debe llevar a cabo la implementación y entregar la memoria técnica en donde se describa:

- Cómo se implementó
- Los elementos adicionales que se necesitan
- Las configuraciones realizadas
- Las pruebas realizadas para lograrlo

**Respuesta esperada**

En la memoria técnica se deben incluir los siguientes 4 elementos para que el profesor valide que el alumno realizó e investigó todo lo que solicita para que ambas herramientas realicen las funciones esperadas.

- Cómo se implementó: Se instalaran las 2 herramientas en dos servidores por separado.

    - El OpMaager puede ser en un servidor Windows
    - El Nagios se instala sobre S.O Linux

- Los elementos adicionales que se necesitan Para que el monitoreo se lleve a cabo se necesita:

- Revisar que los dispositivos a monitorear soporten el protocolo SNMP v1, v2 o v3.
- Tener la MIB (Management Information Base) de cada uno de los elementos a monitorear.
- Tener o establecer una comunidad para el protocolo SNMP.
- En caso de tener un firewall o dispositivo de seguridad, brindar permisos para que la herramienta de monitoreo pueda realizar las consultas a los equipos.

- Configuraciones:

Tanto en la consola de la herramienta de monitoreo como en los dispositivos que se van a integrar al NOC, es necesario configurar el protocolo SNMP con los mismos parámetros: Versión SNMP, Comunidad de tal manera que ambos obtengan y brinden la información que se les está solicitando.

- Pruebas

El alumno debe lograr con las herramientas monitorear el dispositivo y visualizar diversos elementos que le ayudarían al administrador de red a detectar algún problema que se presente en los dispositivos que están siendo monitoreados. Deberá de Mostrar en la consola de administración los parámetros que se están monitoreando, tal y como se observa en las Figuras 4.49 y 4.50.

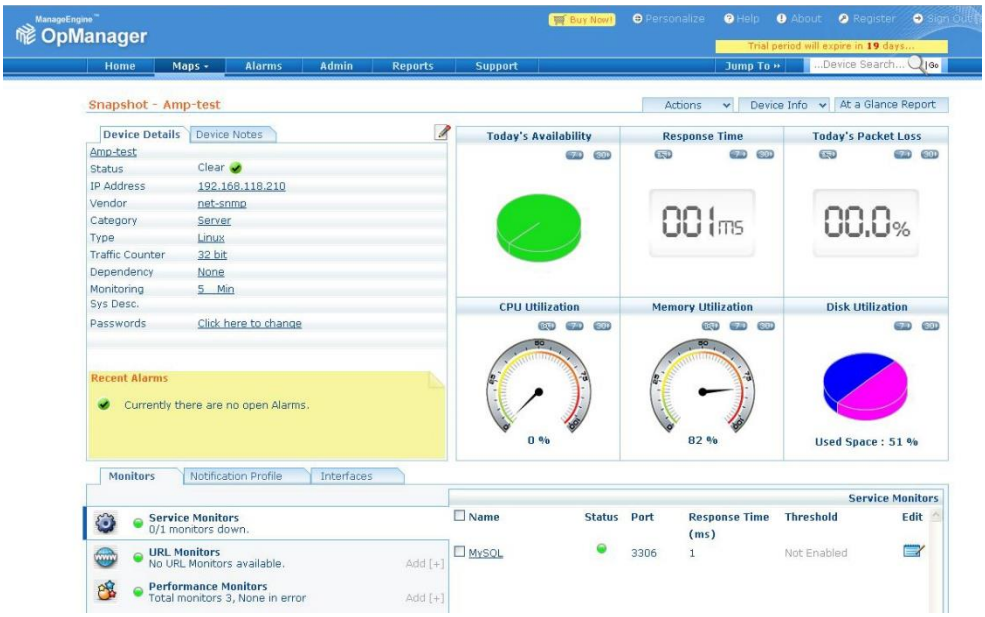



**Figura 4.49- Monitoreo Pasivo (OpManager)**

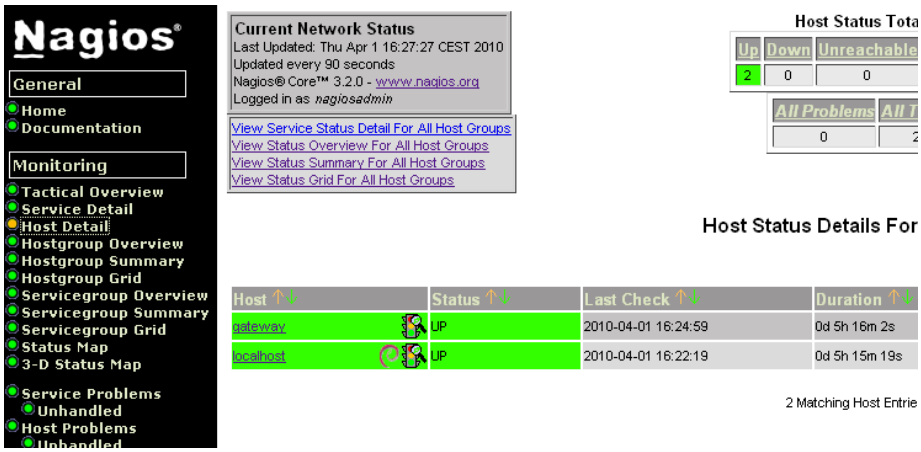



**Figura 4.50- Monitoreo Activo (Nagios)**

# Laboratorio 10.2 Análisis de Tráfico

## Objetivo

El alumno llevará a cabo una evaluación de distintos analizadores de protocolos, así como el análisis de algunas capturas realizadas.

## Materiales y Equipo

- Computadora con S.O compatible con las herramientas de análisis de tráfico a utilizar.
- Analizadores de Protocolos.
- Puerto Espejo.
- Cable de Red.

## Introducción

Un analizador de protocolos o Sniffer, es una herramienta que se emplea para visualiza los mensajes de comunicación que se intercambian entre dos equipos en una red. El Sniffer captura las tramas a nivel de la capa de enlace datos, que se envían y reciben a través de las interfaces de red de los equipos. Un punto importante a resaltar es que este tipo de herramientas son elementos pasivos o no invasivos, esto quiere decir que únicamente observa los mensajes que intercambian las aplicaciones y protocolos, sin interferir en ningún momento con el contenido del mismo. Las tramas capturadas son siempre una copia exacta a la que envía o recibe un equipo.

Su principal funcionamiento consiste en capturar una copia de los paquetes que pasan a través de la red, para posteriormente realizar un análisis de ellos. Existe distintos de tipos de análisis entre los que se encuentran los gráficos y los estructurales. Cuando se realiza un análisis estructural es común ver la composición del Paquete tales como el contenido de las cabeceras, protocolo, datos del cuerpo del mensaje y más. Con el análisis estadístico podemos observar estadísticamente la utilización de un protocolo, un puerto, el tiempo de respuesta, entre otros muchos reportes que las Sniffers o analizadores de protocolos traigan preconfigurados.

Hoy en día existen distintos analizadores de protocolos tanto gratuitos como con licencia, todos estos trabajan bajo el mismo principio de analizar las tramas que viaja sobre la red. Sin embargo la gran diferencia se ve reflejada en los módulos con los que cuentan los Sniffers con licencia, estos van desde la reconstrucción de llamadas telefónicas y videos, visitas de páginas Web, hasta la visualización de tráfico encriptado (Siempre y cuando se cuente con las claves para realizar este tipo de tarea).

## Problemática

Una empresa departamental decidió adquirir un analizador de Protocolos debido a que están presentado un gran número de fallas en su red, para ello solicitó al área de TI evaluar distintos productos tanto de software libre así como con licencia. Al finalizar las pruebas deberán entregar un informe explicando cuales son las principales ventajas y desventajas de cada uno de los analizadores de protocolos examinados. Con base a este reporte se decidirá que producto adquirir.

Dentro de las necesidades por la cuales se necesita adquirir un Sniffer se encuentran:

- Latencia en algunas aplicaciones internas de la red.
- Caídas de aplicaciones internas.
- Detección de tráfico mal intencionado que viaja a través de la red.
- Obtención de reportes en los cuales se observe de manera sencilla el comportamiento de la red.
- Reconstrucción de llamadas telefónicas.
- Visualización de correo electrónico de la empresa.
- Análisis de distintos segmentos de red.

Para realizar las pruebas, se proporcionó el diagrama de red de la empresa el cual se muestra en la Figura 4.51, con base a éste, los encargados de realizar la evaluación decidirán cual es el mejor lugar para integrar el analizador de protocolos y así entregar el reporte lo más completo posible.

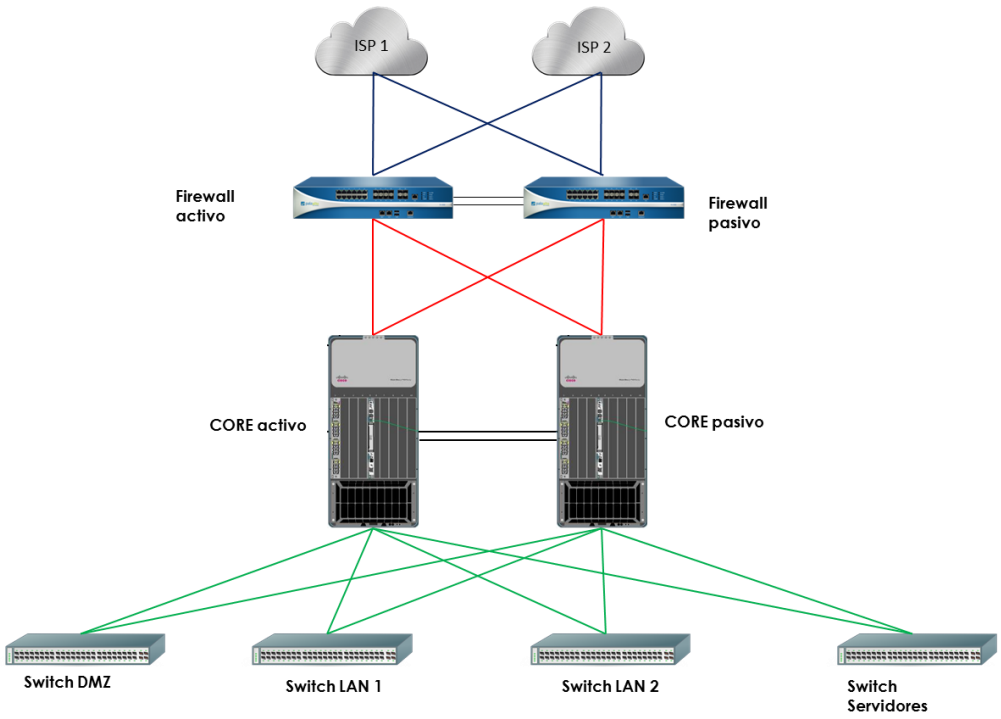



**Figura 4.51 – Diagrama de red empresa departamental**

## Actividad a Realizar

Investigar que analizadores de protocolos existen tanto de software libre como los que requieren licencia y realizar una tabla comparativa de las características con las que cuentan cada uno de ellos.

**Respuesta esperada:**

El alumno deberá de entregar una tabla en la cual se observen las características que cada uno de los analizadores de protocolos presentan, tal y como se muestra en la Tabla 4.26

**Tabla 4.26 – Características analizadores de protocolos**

| | Características | | | | | |
|---|---|---|---|---|---|---|
| **Producto** | **Análisis en tiempo real** | **Gráficas** | **Reportes predefinidos** | **Creación de Reportes** | **Reconstrucción de aplicaciones** | **Fácil Administración** |
| **Wireshark** | Si | Si | No | No | No | Si |
| **Ethereal** | Si | Si | No | No | No | Si |
| **Colasoft Capsa Network Sniffer** | Si | Si | Si | Si | No | Si |
| **ClearSight Analyzer** | Si | Si | Si | Si | Si | Si |
| **Miiksun** | Si | Si | Si | Si | Si | Si |

De acuerdo al diagrama de red proporcionado por la empresa, sugiera una posible integración del analizador de protocolos en la red y exponga ante el grupo porqué es el lugar más adecuado para su instalación.

**Respuesta esperada:**

Para realizar la integración del analizador de protocolos a la red, el alumno deberá realizarse distintas preguntas por ejemplo:

- ¿Qué subredes se desea monitorear?
- ¿Qué tipo de tráfico se desea monitorear?
- ¿Sobre qué equipos se quiere realizar el monitoreo?
- ¿Qué dispositivo puedo configurar para que todo el tráfico que deseo analizar sea visible?
- ¿Cuál es el comportamiento del tráfico sobre la red a analizar?
- ¿Qué se espera obtener del tráfico analizado?

Después de haber identificado y justificado el lugar en donde se colocará el analizador de protocolos, realice las configuraciones necesarias para que los analizadores ocupados para laboratorio, sean capaces de empezar a recibir tráfico. Adjunte evidencia del tráfico Capturado.

**Respuesta esperada:**

Para realizar la configuración y puesta a punto de la solución es necesario realizar las siguientes actividades.

- Configurar del puerto espejo en el Switch.
- Configurar la interfaz del equipo donde se vaya a realizar las capturas en modo promiscuo.
- Instalación del analizador de protocolos.
- Selección de la interfaz de red que será utilizada para recibir el tráfico.

Ahora que ya se encuentra configurados e instalados los analizadores de protocolos, realice las siguientes actividades:

- Capture el siguiente tráfico:

  - Visitas distintas páginas de internet
  - Realizar pruebas de ping a algún DNS público.
  - Envíe un correo electrónico

- Detenga la captura y guárdela en formato PCAP.
- Analice e interprete el tráfico capturado con ambos analizadores de protocolos y explique por lo menos 2 de las tramas capturadas.

**Respuesta esperada:**

Para el tráfico capturado, el alumno deberá explicar cómo está conformado uno de los frames, a continuación se presenta un ejemplo, en el cual se observa la consulta a una página de internet a través del protocolo http, el análisis se realizará utilizando el analizador de protocolos Wireshark.

El analizador de protocolos Wireshark está conformado principalmente por 3 ventanas, la primer ventana es llamada Packet list, en esta se encuentra un listado de todas las tramas capturadas independientemente del protocolo capturado. En la ventana central es conocida como Packet Detail, la cual muestra en mayor detalle la trama capturada y seleccionada, los detalles de la trama son mostradas en un menú en forma de árbol, cuyas ramas pueden expandirse o contraerse para tener una visión más general o una visión más detallada. Por último se encuentra la ventana inferior llamada Packet Bytes, en esta se puede observar el mismo contendió de la venta central pero en forma hexadecimal estos están organizados en filas de 16 Octetos. Por comodidad, este panel inferior nos muestra también, en su parte derecha, una copia de los octetos de la trama pero en formato ASCII, es decir, cada octeto es traducido al carácter equivalente según el código ASCII. A continuación en la Figura 4.52 se observa un ejemplo de captura realizada, seguida una breve explicación.

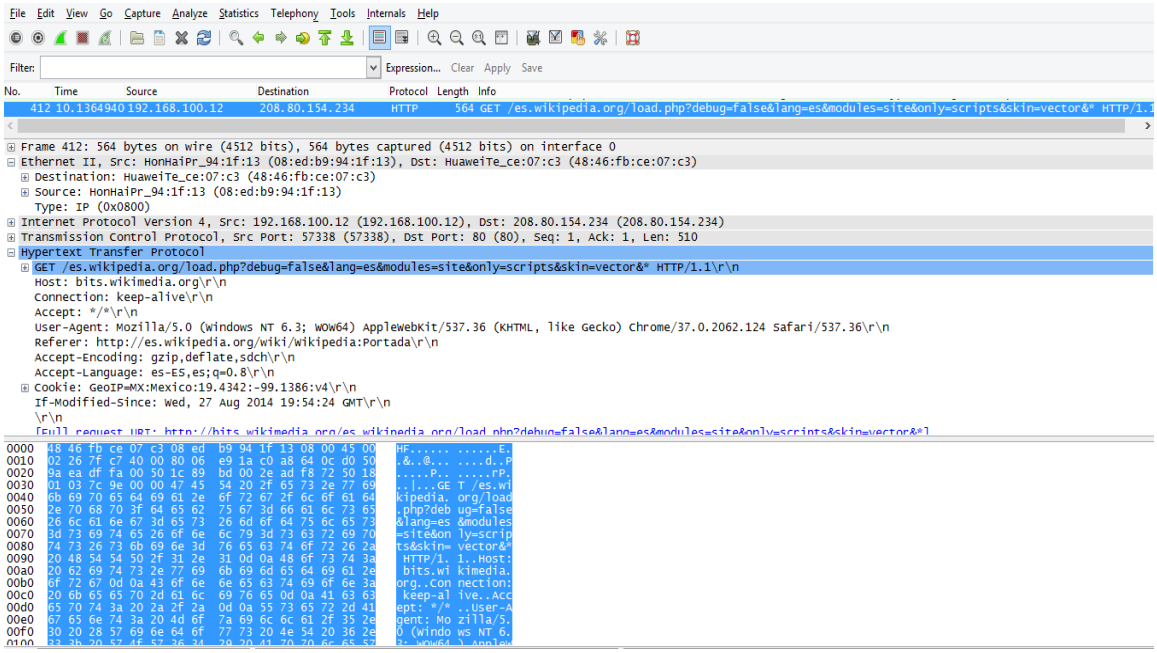



**Figura 4.52 – Captura de Tráfico HTTP mediante Wireshark**

En la parte superior como anteriormente se comentó se observan las tramas capturadas, para el ejemplo se seleccionó la trama número **412** a simple vista se observa que se está realizada con una petición a la página es.wikipedia.org. En el panel central se observa los detalles relativos al contenido del frame seleccionado, en la primera rama se visualiza información relacionada con el instante en el que la trama fue capturada tal como: fecha y hora de la captura, número de los octetos que se han capturado, numero de orden y más. Esta rama en específico es colocada por Wireshark. Las ramas subsecuentes son el número de cabeceras con las que cuenta el frame.

En este caso, la segunda rama nos indica que es una cabecera del tipo Ethernet versión 2, esta muestra tres campos, los dos primeros indican las direcciones MAC orígenes y destino de las maquinas que entablan la comunicación y el campo Type indica que se trata de una cabecera del tipo Ethernet versión 2.

Por último, el panel inferior muestra, sin ninguna información extra, los octetos ("bytes") de los que está compuesta la trama que se seleccionó en el panel superior y cuyos detalles se observaron en el panel central. Esos octetos se muestran en hexadecimal organizados en filas de 16 octetos. Como ayuda se observa que cada fila de 16 octetos se encuentra precedida de un número en hexadecimal que indica la posición que ocupa el primero octeto de la fila en la trama. Por ejemplo, la primera fila viene precedida por el número 0000 (hexadecimal) lo que quiere decir que el primer octeto de esa fila es el que estaba en la primera posición de la trama (la cero). La segunda fila está etiquetada con el número 0010 (hexadecimal), que es el 16 en decimal. Por comodidad, este panel inferior muestra también en su parte derecha, una copia de los octetos de la trama pero en formato ASCII.

Después de haber realizado un análisis de algunas de las tramas capturadas, realice un reporte comparativo de los dos analizadores de protocolos utilizados y justifique cual sería la mejor opción que cubre con las necesidades planteadas en la problemática.

**Respuesta esperada:**

El alumno deberá de entregar un documento donde realice una comparación entre los analizadores de protocolos utilizados, así como enlistar los beneficios y desventajas que presenta cada uno. También presentará una conclusión en la cual justifique cual es el mejor analizador que cumple con las necesidades plasmadas en la problemática.

# Laboratorio 10.3 Trazas de Auditoria/Monitoreo

## Objetivo

El alumno investigará en distintas fuentes de información cuáles son las herramientas consideradas como SIEMs. Así mismo expondrá ante el grupo cual son los principales componentes que lo conforman, su funcionamiento y qué beneficios se obtienen de él.

## Materiales y Equipo

- Equipo de cómputo pare realizar la investigación.
- Artículos de periódicos, revistas, libros y otras fuentes que proporcionen información relacionados con el tema a abordar.

## Introducción

Hoy en día el entender lo que realmente pasa sobre en una red corporativa es una tarea compleja para los administradores de las red, debido a que no es fácil llevar un control sobre todo lo que se hace, sucede o afecta a todos los dispositivos, aplicaciones y demás componente que la conforman.

Una manera de saber qué es lo que está sucediendo es recolectar los eventos que genera cada uno de los componentes de la red, sin embargo esta es una tarea complicada, ya que se genera un evento por cada actividad realizada, por ejemplo:

- Ingreso al equipo.
- Cambio en la configuración.
- Falla en un procesador.
- Creación de una cuenta.
- Fallas en la autenticación.
- Establecimiento de las fases de una VPN.
- Reinicio de un servicio.

Cabe señalar que cada componente de la red genera y entrega de manera distinta la información. Los orígenes de estos eventos son diversos tales como:

- **Sistemas operativos**: Eventos de los diferentes sistemas operativos que operan en la red.

- **Orígenes de TI referenciales**: El software utilizado para mantener y seguir activos, revisiones, configuración y vulnerabilidad.

- **Eventos de aplicaciones**: Los eventos generados de las aplicaciones instaladas en la red.

- **Control de acceso de usuarios**: Los eventos generados de las aplicaciones o dispositivos que permiten a los usuarios acceder a los recursos de la compañía.

- **Perímetro de seguridad**: Dispositivos y software utilizados para crear un perímetro de seguridad.

Para ayudar a que el administrador de red tenga una visión de lo que está sucediendo de una manera clara y sencilla, se han diseñado distintas soluciones tales como:

- Security Information Management (SIM).
- Security Event Management (SEM).

Un SIM es el encargado de almacenar una gran cantidad de eventos (logs) a largo plazo, para posteriormente ser utilizados. El SEM se encuentra enfocado al análisis y correlación en tiempo real de los datos obtenidos de los orígenes de eventos, este tiene la posibilidad de detecta problemas e iniciar una respuesta a un incidente en tiempo real, basado en configuraciones realizadas por el administrador. Sin embargo el tener estas dos tipos de tecnologías por separado a veces se volvía difícil de administrar. Por tal motivo en 1995 surgió un nuevo concepto denominado SIEM (Security Information and Event Management), el cual se encuentra conformado por un SIM y un SEM, entre las características con las que esta tecnología cuenta son:

- **Recolección de datos**: Esta debe ser capaz de recolectar información de diferentes orígenes de eventos los cuales incluyen dispositivos de red, seguridad, servidores, bases de datos, aplicaciones y demás dispositivos que sean capaces de proporcionar logs.

- **Correlación**: Valida atributos específicos de la información, y a través de una base de datos de eventos puede correlaciones múltiples eventos brindando un resultado integrado.

- **Alertas**: A través del análisis automatizado de la información recibida, tiene la capacidad de generar alertas por diferentes medios, ya sea correo electrónico o menaje de texto.

- **Reportes**: Permite visualizar la información recolectada en tiempo real así como realizar reportes personalizados.

- **Cumplimiento**: Permite colectar información para auditoría y cumplimiento, permitiendo adaptarse a la norma en curso.

- **Retención/Cifrado**: tiene la capacidad de guardar la data recibida y cifrarla en diferentes métodos, esto facilita la búsqueda de información histórica con fines de auditoria o investigación forense.

Hoy en día existen distintos fabricantes que ofrecen este tipo de soluciones, pero en principio la arquitectura y la forma en la que funcionan son similares. La diferencia entre

cada fabricante dependerá de la forma en la que presentan la información, así como características propias del producto.

## Problemática

La empresa de transportes Gateway, desea llevar un control más estricto de todo lo que pasa en su red, para ello decidió adquirir la solución SIEM, sin embargo antes de elegir cual adquirir les gustaría saber cuál es la que mejor se ajusta a sus necesidades, así como a su presupuesto. Entre los principales requerimientos que se presentan se encuentran:

- Monitoreo en tiempo real de todos los eventos de configuración y autenticación de los equipos a monitorear.
- Generación de alertas en base a un cátalo de eventos.
- Creación de reportes personalizados.
- Fácil análisis de la información recolectada.
- Gráficas en las cuales se observe de una manera más clara los eventos analizados.
- Almacenamiento de evento de por lo menos 6 meses y posibilidad de almacenarlos en un repositorio fuera de la solución.
- Posibilidad de enviar notificaciones a través de correo electrónico.

El área TI será la encargada de realizar la evaluación para la adquisición de la solución, como primera etapa deben investigar qué soluciones existen y cuál de ellas se encuentran mejor posicionadas en el cuadrante de Gartner, la segunda consistirá en plantear una posible arquitectura para llevar a cabo la implementación de un SIEM y por último tendrá que entregar un reporte con la solución que cumple con los requerimientos deseados.

## Actividad a Realizar

Con base a lo planteado en la problemática, investigue cuales son las soluciones SIEM que ofrece el mercado, así como una breve explicación de cada una de ellas, además averigüe cuáles son las mejores posicionadas en el cuadrante de Gartner.

**Respuesta esperada:**

El alumno deberá investigar y realizar una tabla en la cual se observen algunos ejemplos de las distintas soluciones que existen en el mercado, en la Tabla 4.27 se observa una posible respuesta.

**Tabla 4.27 – soluciones SIEMs**

| Solución | Fabricante | Descripción |
|---|---|---|
| **IBM QRadar Security Intelligent Platform** | IBM | IBM QRadar Security Intelligence Platform ofrecen una arquitectura unificada en la que se integran la gestión de sucesos e información de seguridad, la gestión de registros, la detección de anomalías, la investigación de incidentes y la gestión de la configuración y de las vulnerabilidades |

| | | |
|---|---|---|
| **HP ArcSight** | HP | Es el gestor de eventos de seguridad que analiza y correlaciona cada evento con el fin de ayudar a los administradores con la detección de eventos de seguridad, de cumplimiento de normas y de gestión de riesgos para operaciones de inteligencia y seguridad. |
| **NetIQ Sentinel** | Novell | Sentinel es una solución de gestión de información de seguridad y eventos (SIEM) y de supervisión del cumplimiento, la cual supervisa automáticamente los entornos TI más complejos y ofrece la seguridad requerida para protegerlos. Sentinel actúa como el sistema nervioso central para la seguridad de la empresa, Recolecta eventos de toda la infraestructura, los Analiza y establece correlaciones entre estos. |

De acuerdo a la última evaluación realizada para las soluciones SIEM, el cuadrante de Gartner para el año 2014 muestra los mejores productos en este ramo, en la Figura 4.53 se observa el cuadrante.


**Figura 4.53 – Cuadrante de Gartner SIEMs**

Después de haber investigado y observado que existen distintos fabricantes que ofrecen este tipo de soluciones, exponga de forma gráfica la forma en la que trabaja in SIEM.

**Respuesta esperada:**

El objetivo de exponer la forma en la que trabaja un SIEM, es que el alumno entienda en forma general el cómo funciona este tipo de herramientas, entre los principales puntos que debe contener la exposición se encuentran los siguientes:

- Diagrama de red genérico con cada uno de los componentes que conforman el SIEM.
- Descripción del funcionamiento de cada uno de los componentes.
- Flujo del tráfico desde la generación del evento hasta el procesamiento de este por parte del SIEM.

En la Figura 4.54 se observa un diagrama genérico con cada uno de los componentes que conforman un SIEM.

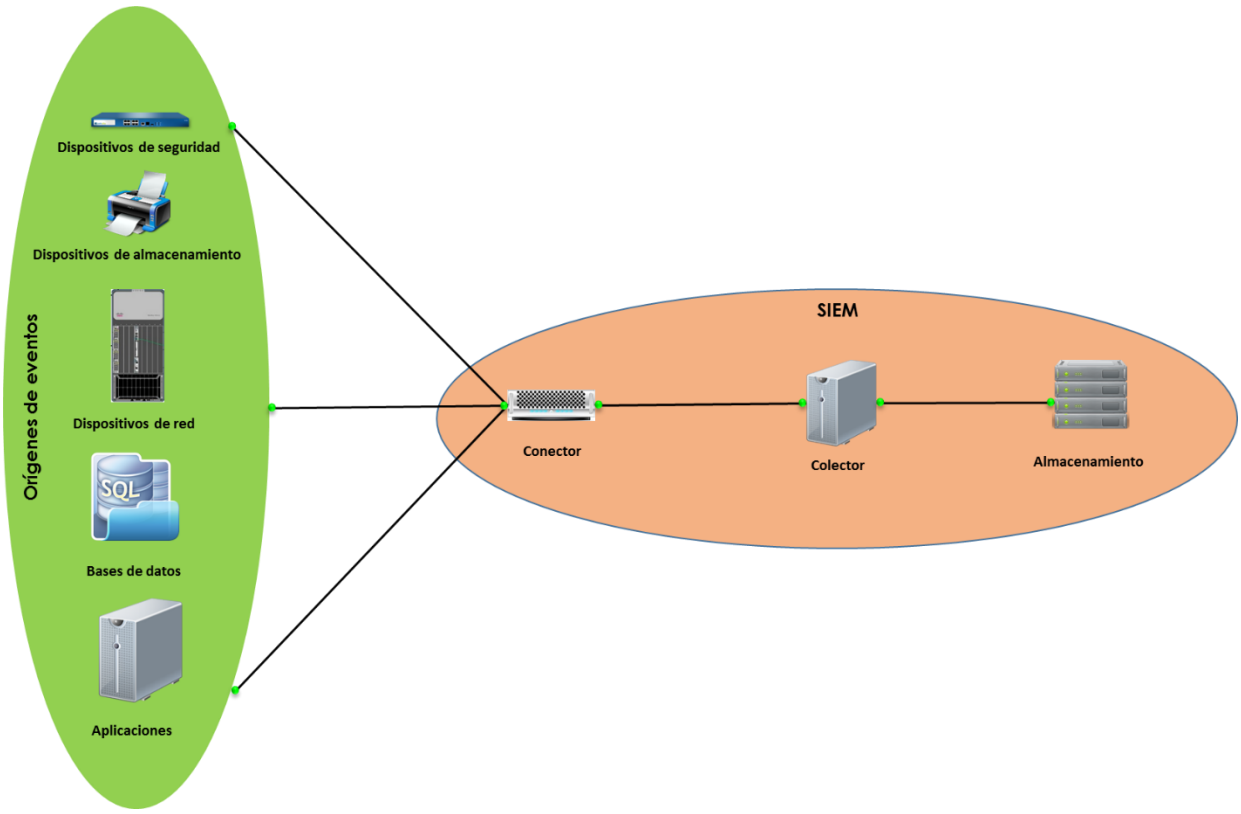



**Figura 4.54 – Arquitectura SIEM**

Descripción de componentes que conforman la arquitectura:

- Origenes de eventos: Los origenes de eventos es todo aquel elemento que conforma la red y es capaz de crear eventos que pueden ser monitorieados por el SIEM.

- Conectores: Ofrecen conexiones desde los orígenes de eventos al sistema SIEM. Utilizando protocolos estándar de la industria para obtener los eventos, como por

ejemplo syslog, JDBC para leer tablas de la base de datos y WMI para leer los registros de eventos de Windows. Los conectores proporcionan:

  - Transporte de datos de eventos en bruto desde los orígenes de eventos al recopilador.
  - Filtrado específico de conexión.
  - Gestión de errores de conexión.

- Colector: Es el encargado de realizar la parte operativa del SIEM, entre sus principales funciones se encuentra:

  - Analizar y normalizar los datos.
  - Analiza los datos en busca de eventos que disparen las alertas configuradas por el administrador.
  - Encargado de traducir los eventos recopilados para mostrarlo en forma gráfica.
  - Catalogar los datos para la elaboración de reportes.

- Alamacenamiento de evetos: los SIEM ofrece múltiples opciones para almacenar los datos recopilados. Por defecto, recibe dos cadenas de datos independientes pero similares desde los conectores: los datos del evento y los datos en bruto. Estos datos se almacenan en el sistema de archivos local del servidor o en su defecto son enviados a una storage para su almacenamiento.

Una vez concluida las actividades anteriores, elabore un reporte en el cual justifique cuál de los SIEMs investigados cumple con las características solicitadas durante la problemática.

**Respuesta esperada:**

El reporte que el alumno entregará, debe justificar de manera clara y concisa porque es la mejor opción para cumplir con los requerimientos establecidos.

# Laboratorio 11.- Integración de los conocimientos adquiridos

## Laboratorio 11.1 Resolución de problemas y demostración de conocimientos en Redes

### Objetivo

El alumno pondrá en práctica los conocimientos adquiridos durante el semestre y realizará la configuración y puesta a punto del escenario propuesto.

### Materiales y Equipo

- Routers.
- Switches.
- Computadoras.
- Cables para realizar las configuraciones entre los distintivos.
- Simulador de red (Si no se tiene físicamente los dispositivos).
- Aplicación de Hyperterminal.

### Problemática

Una empresa de construcción ha seleccionado a la empresa 5-Consulting, para realizar la implementación y configuración de su red LAN y WAN, la constructora tiene como sede los estados de Querétaro, Cancún, Monterrey y Distrito Federal. Para la implementación se le ha dado la libertar de proponer el direccionamiento IP bajo ciertos parámetros exigidos por la constructora, adicionalmente se solicita tener en cuenta las siguientes variables.

1. Propuesta de Equipos a ser utilizados, para la implementación.

2. Deberá entregar una tabla con las características de cada equipo que será utilizado.

3. Configurar los enlaces WAN entre las diferentes sedes, tomando en cuenta lo siguiente:

    a. Debe de existir redundancia entre los enlaces WAN para evitar que alguna de las sedes se quede incomunicada con las demás.
    b. El enrutamiento a utilizar debe ser fácil de implementar y administrar.
    c. El segmento de la red WAN debe contemplar 12 Host para su utilización.

4. La empresa 5-Consulting deberá de entregar todo el direccionamiento.

5. Las sucursales cuentan con diferentes VLANs, las cuales tiene distintos número de host, en la Tabla 4.28 se observa la distribución de host por localidad.

| Tabla 4.28 - Número de host por sucursal | | | | |
|---|---|---|---|---|
| **VLAN** | Distrito Federal | Querétaro | Monterrey | Cancún |
| **VIP** | 30 | 10 | 15 | 10 |
| **COMPRAS** | 15 | 2 | 5 | 2 |
| **PROVEEDORES** | 15 | 15 | 15 | 15 |
| **USUARIOS** | 70 | 40 | 40 | 40 |
| **VISITAS** | 20 | 20 | 20 | 20 |
| **SERVIDORES** | 50 | 5 | 5 | 5 |
| **RESPALDOS** | 50 | 0 | 0 | 0 |
| **INGENIERÍA** | 10 | 2 | 2 | 2 |

6. Debe existir la comunicación entre todas las VLAN, con excepción de la VLAN de respaldos, los únicos que deben comunicarse con esta es la de Ingeniería y servidores.

7. En la VLAN de servidores debe de existir un servidor FTP y un servidor Web.

8. Implementará algunos mecanismo de seguridad tales como:

    a. La seguridad en los puertos de los Switch
    b. Control de acceso al servidor ftp.
    c. Control sobre el tráfico que ingresa a la VLAN de Servidores y respaldos.

9. Deberá entregar una memoria técnica en la cual se plantee paso a paso la metodología utilizada para realizar la implementación de la red.

Después de haber escuchados y enlistado las características solicitadas por la contractura, los ingenieros plantearon el diagrama de red que se muestra en la Figura 4.55.

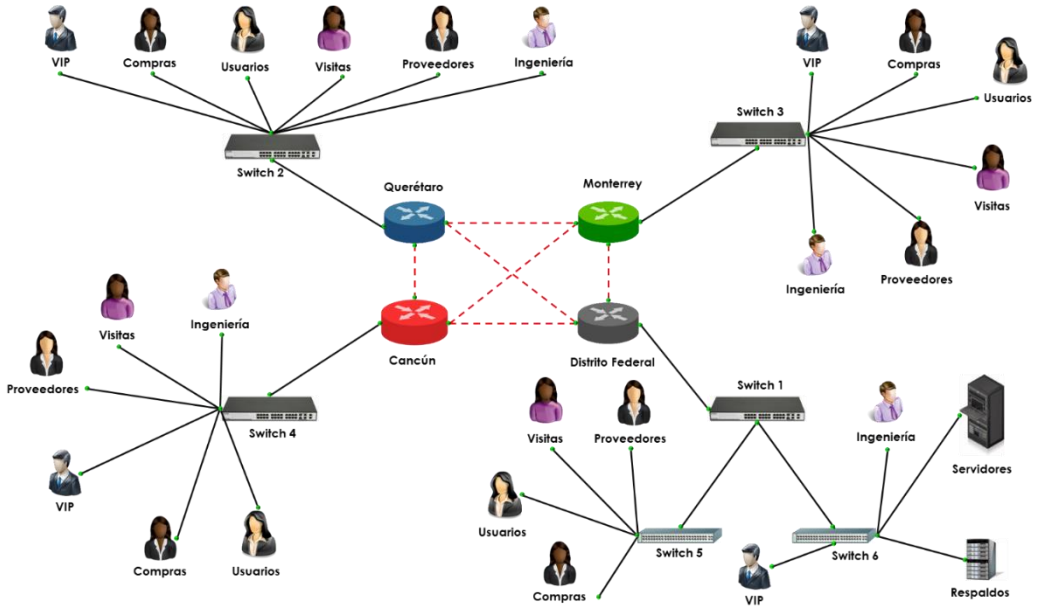



**Figura 4.55 – Diagrama de red Propuesto para la constructora.**

## Actividad a Realizar

Con base a lo planteado en la problemática Investigue que equipos cumplen con las características para dar solución al escenario que se presenta y realice una tabla en la cual se en liste las características de los equipos propuestos.

**Respuesta esperada:**

El alumno tendrá que investigar cuantos y que dispositivos cumplen con las necesidades planteadas durante la problemática propuesta. Para hacer un correcto dimensionamiento de los equipos a utilizar el alumno deberá tomar en cuenta distintos aspectos tales como:

- Número de usuarios, con base a esto se dimensionará el número de Switch necesarios para realizar la implementación. Se debe tomar en cuanta siempre un crecimiento del 30%.
- Velocidad de las interfaces.
- Tipos de Tecnologías que son soportadas en cada uno de los dispositivos, se debe tomar en cuenta que los dispositivos seleccionados deben soportar las características planteadas durante la problemática.

Proponga un direccionamiento de acuerdo al número de usuarios, tome en cuenta los parámetros solicitados durante la problemática y entregue una tabla en la cual se observe el direccionamiento propuesto.

**Respuesta esperada:**

El direccionamiento propuesto por cada alumno será variable, debido a que pueden utilizar distintos segmentos de red para realizarlo. Sin embargo se debe tomar en cuenta que debe hacerse a través del método VLSM.

En la problemática se propone un diagrama de red por parte de los ingenieros, de acuerdo a su criterio indique si éste cumple con las necesidades de la constructora, además proponga un diagrama de red opcional al planteado en la problemática.

**Respuesta esperada:**

El diagrama propuesto en la problemática cumple con los requerimientos plasmados, sin embargo el alumno deberá plantear un diagrama de red opcional, tomando en cuenta principalmente la redundancia entre los enlaces WAN.

Después de haber planteado el diagrama de red, realice las configuraciones necesarias para que el escenario propuesto sea totalmente funcional, haga pruebas de conexión entre las distintas VLAN de acuerdo a lo plasmado en la problemática y obtenga evidencia de las mismas.

**Respuesta esperada:**

El alumno deberá realizar las configuraciones necesarias para que la red propuesta sea totalmente funcional, entre la evidencia que deberá entregar se encuentra:

- Comunicación entre las diferentes VLANs.
- Prueba de comunicación entre los servidores y los usuarios de cada VLAN.
- Validar que la redundancia entre las enlaces WAN funcione correctamente.
- Correcto funcionamiento de la seguridad aplicada en la red, tales como:
    - Seguridad en los puertos de los Switches.
    - Autenticación al ingresar en el servidor FTP.
    - Control del tráfico que ingresa en la VLAN de servidores y respaldos.

Posterior a la validación del correcto funcionamiento de la red, elabora una memoria técnica la cual constará de lo siguiente:

a) Introducción.
b) Diagrama de red propuesto.
c) Direccionamiento planteado.
d) Configuraciones realizadas para llevar a cabo la implementación de la red propuesta.
e) Pruebas realizadas para la validación de la funcionalidad del escenario.
f) Conclusiones.

**Respuesta esperada:**

El alumno deberá de presentar una memoria técnica la cual contendrá los puntos solicitados anteriormente. Se debe tomar en cuenta que la presentación de ésta debe contener todos los aspectos vistos durante el curso en lo que respecta a la parte de Networking.

**Nota:** La problemática propuesta cumple con los aspectos vistos durante el curso en la parte de Networking. Sin embargo, el maestro puede proponer otra problemática y distintos escenarios con el fin de evaluar lo visto a lo largo del curso.

# Laboratorio 11.2 Resolución de problemas y demostración de conocimientos en Seguridad Informática

## Objetivo

El alumno pondrá en práctica los conocimientos adquiridos durante el semestre y realizará la configuración y puesta a punto del escenario propuesto.

## Materiales y Equipo

- Firewalls.
- Switches.
- Equipos de cómputo.
- Máquinas virtuales con distintos sistemas operativos.
- Cables para realizar las interconexiones.
- Software para monitoreo de equipos.
- Analizador de Protocolos
- Servidor Radius, FTP Y Web.
- Servidor de Directorio Activo y máquinas que pertenezcan al dominio.

**Nota:** Los servicios solicitados como Máquinas virtuales, Software para realizar el monitoreo de equipos, analizadores de protocolos y servicios de autenticación, fueron utilizados y configurados a lo largo de curso por los alumno. Estos mismos serán utilizados y adaptados para realizar el examen final.

## Problemática

Una empresa de publicidad decidió contratar a una Consultoría para llevar la administración y configuración de los equipos que conforman su red. Dentro de la junta inicial el ingeniero encargado de la administración de la red explicó cómo se encuentra actualmente estructurada y cuál es el plan de crecimiento a su nueva sucursal localizada en Canadá. Para la red actual se obtuvo la siguiente información:

- Se tiene un segmento para toda la red.
- Se utilizan IPs reservadas para los servidores.
- El firewall que actualmente se tiene únicamente sirve para realizar la publicación de servicios y permitir algunos servicios desde la red interna.

Entre los planes para realizar el mejoramiento y crecimiento de la red se encuentra:

- Crear segmentos de red distintos para cada una de las áreas existentes, estas serán colocadas en VLANs.
- Establecer perfiles de filtrado de contenido web y de aplicaciones para cada una de las áreas o por usuarios en específico.

- Inspección de tráfico SSL.
- Dividir la red en distintas zonas de seguridad.
- Realizar las publicaciones de servicios.
- Implementar una solución de IPS, la cual sirva para proteger la red de cualquier tipo de ataque.
- Instalar un analizador de protocolos en algún lugar estratégico la red, el cual tendrá como objetivo observar parte del tráfico que pasa a través de la red de México.
- La consultoría deberá monitorear la disponibilidad de algunos elementos que conforman la red.
- Conexión remota de usuarios a través de VPNs SSL, utilizando un servidor free RADIUS como método de autenticación.
- Comunicación entre las distintas sucursales a través de VPNs.
- Actualmente se cuenta con los siguientes componente de red localizados en México:
    - Un firewall de nueva generación.
    - Dos Switches configurables
    - Dos servidores los cuales son utilizados para realizar las publicaciones y los respaldos.
    - Servidor de Directorio Activo
    - Una IP Pública estática.

Al finalizar la junta, la consultoría encargada del proyecto convocó a una segunda junta para proponer una posible solución, así como realizar algunas preguntas adicionales para completar la información requerida para llevar a cabo la implementación.

## Actividades a realizar

De acuerdo a lo estipulado en la junta inicial indique si la información proporcionada, es suficiente para dar una solución al escenario que se presenta en la problemática, en caso de no ser suficiente, elabore una serie de preguntas para completar la información que requiere para llevar a cabo la configuración y puesta a punto del escenario presentado.

**Respuesta esperada:**

Para llevar a cabo esta práctica será necesario la intervención del maestro, debido a que él proporcionará la información adicional que necesita el alumno para proponer una posible solución a la problemática planteada, así como realizar las configuraciones necesarias para el correcto funcionamiento del escenario propuesto.

A continuación se presenta en la Tabla 4.27 algunas posibles preguntas que el alumno realizará, así como su respuesta, cabe señal que las respuestas pueden ser modificadas por el maestro.

**Tabla 4.29 - preguntas a realizar**

| *Preguntas* | Respuesta |
|---|---|
| ¿Cuál será el direccionamiento utilizado en la red? | El direccionamiento será propuesto por cada uno de los alumnos de acuerdo a las indicaciones dadas por el maestro. |
| ¿Cuantas áreas existen y cuantos usuarios hay en cada una de ellas? | El número de áreas existentes pueden ser variables de acuerdo a lo propuesto por el maestro. |
| ¿Cuantas zonas de seguridad existirán? | Las zonas de seguridad serán propuesta por el alumno, el único requisito es que la parte de respaldos y servidores quede separa de las demás zonas de seguridad. |
| ¿Los dispositivos con los que se cuentan actualmente que funcionalidades tienen? | El firewall de nueva generación cuanta con los siguientes módulos activos: IPS, Filtrado URL y filtra de aplicaciones, cliente para la utilización VPNs ssl. |
| Para la sucursal localizada en Canadá ¿Cuántos usuarios son?, ¿Será implementado filtrado de URL y de aplicaciones?, ¿Se aplicaran algún perfil de IPS? | El número de usuarios, será asignado por el profesor. La sucursal de Canadá también contar con filtrado URL y de aplicaciones, así como perfil de IPS. |
| ¿Qué segmento de red, VLAN o usuarios tendrán permitido ingresar a la zona de servidores? | El profesor definirá que grupos de usuarios tendrán acceso a la zona de servidores. |
| ¿Cuántos perfiles de filtrado Web y aplicaciones existirán? Y ¿Qué tendrá permitido cada perfil? | Por lo menos se definirán tres perfiles de filtrado de aplicaciones y web, entre los cuales se encuentran: Global, VIP y visitantes. |
| ¿Los perfiles de Filtrado Web y de aplicaciones serán asignados por usuario, IP o segmentos de IPs? | Los perfiles serán asignados de acuerdo a lo especificado por el maestro. |
| ¿Qué tipo de publicaciones se realizarán? | Los servicios que se publicarán serán los utilizados en las prácticas realizadas durante el semestre, los cuales son servidor FTP y servidor Web. |
| ¿Se crearán perfiles de IPS para cada na de las publicaciones y navegación a internet? | Se crearán perfiles de IPS, uno será para las publicaciones y el otro el utilizado para la navegación a internet. |
| ¿Qué parámetros se desea que monitoreo el NOC? | Dentro de los parámetros que se desea monitorear se encuentra: |

| | |
|---|---|
| | • Disponibilidad de los equipos<br>• Estado de las interfaces<br>• Performance del equipo<br>• Utilización de memoria |
| ¿Qué tipo de comunicación se permitirá entre las distintas sucursales? | Se permitirá el tráfico entre los distintos departamentos. Solo se tomara en cuenta que se debe restringir el ingreso a los servidores y a los servidores de respaldo de acuerdo a las aplicaciones que utilice cada uno. |
| ¿Se debe de cumplir con alguna especificación para realizar las VPNs site to site? | Los parámetros utilizados para la creación de las VPN serán establecidos por el alumno. |
| ¿Los usuarios que se conecten utilizando clientes VPNs ssl, a que recursos dentro de la empresa podrán ingresar? | Los usuarios que se conecten a la red, solo tendrán acceso al segmento de Servidores. |

Después de haber clasificado y analizado la información proporcionada, proponga un escenario que cumpla las necesidades establecidas y realice un plan de trabajo en el cual se describan todas las actividades que realizará para configurar la solución propuesta.

**Respuesta esperada:**

El alumno deberá plantear un diagrama de red que cumpla con los requerimientos planteados durante las juntas, en la Figura 4.56 se presenta una posible solución. También deberá de presentar un plan de trabajo con todas las actividades que se realizarán durante la implementación.

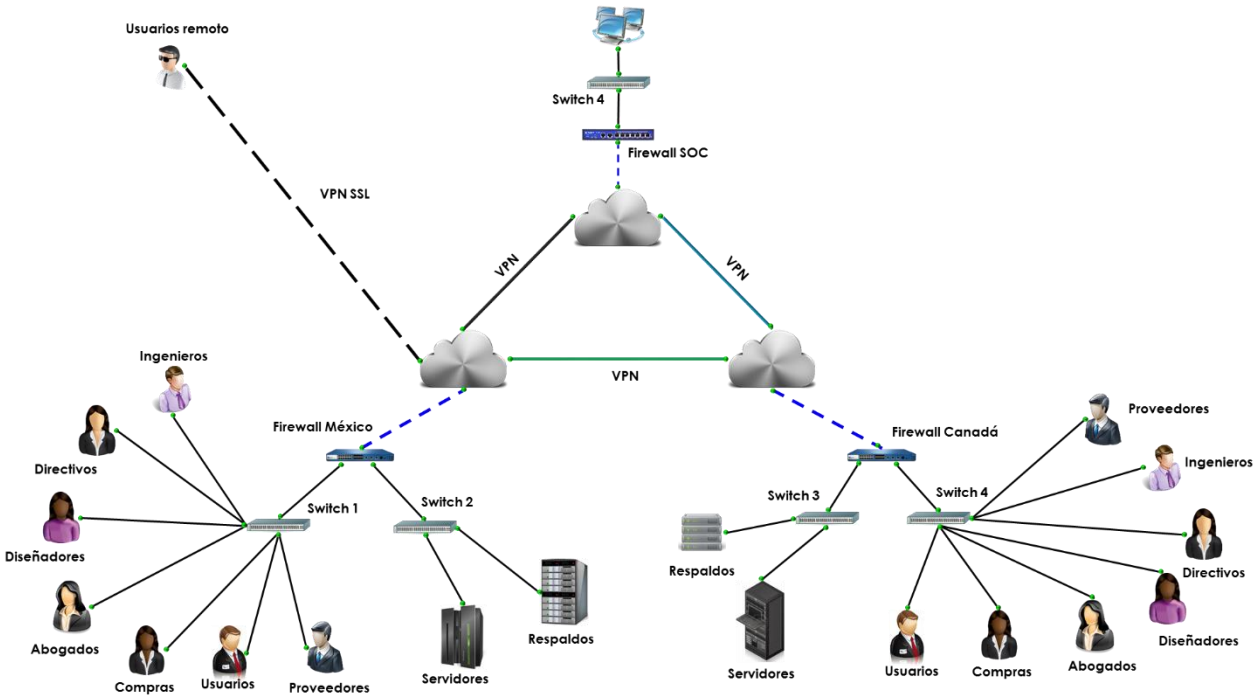



**Figura 4.56 - Diagrama de red propuesto para empresa de publicidad**

Dentro los campos que debe contener el plan de trabajo se encuentran:

- Actividad a realizar.
- Responsable de la actividad.
- Tiempo estimado de ejecución.
- Porcentaje del avance.

Ahora que se tiene un plan de trabajo y una arquitectura para la red de la empresa de publicidad, implemente el diagrama de red que propuso y realice las configuraciones necesarias para que el escenario sea funcional.

**Respuesta esperada:**

Se deberán realizar las configuraciones pertinentes para que el escenario planteado por el alumno funcione correctamente, entre los principales puntos que debe de realizar se encuentran:

1. Direccionamiento de la red.
2. Publicación de servicios.
3. Comunicación entre VLANs y zonas.
4. Creación de políticas de seguridad y de filtrado de aplicaciones.
5. Creación de VPN site to site.
6. Creación de VPN ssl.
7. Configuraciones necesarias para que el analizador de protocolos observe el tráfico que pasa a través de la red.
8. Creación de políticas de IPS para proteger la red y los servidores.

Al finar la configuración deberá presentar un reporte donde se observe evidencia de cada una de los puntos planteados durante la problemática, entre los puntos que debe contener este documento se encuentran:

1. Diagrama de red.
2. Direccionamiento propuesto.
3. Comunicación entre las distintas VLANs.
4. Logs de tráfico en los distintos Firewall.
5. Evidencia de que el filtrado por URL y de aplicaciones funcione correctamente.
6. Evidencia del establecimiento entre las VPNs.
7. Correcta autenticación de usuarios a través de la VPN SSL y logs en el firewall donde se observe el correcto ingreso.
8. Validación de la disponibilidad de los equipos monitoreados de acuerdo con la herramienta de monitoreo utilizada.
9. Muestra del trafico observado sobre el analizador de protocolos.
10. Correcto funcionamiento de los perfiles de IPS creados, para este punto deberá de realizar un escaneo de vulnerabilidades sobre alguno de los servicios publicados.

**Respuesta esperada:**

El documento entregado por el alumno deberá contener evidencia de todas las pruebas realizadas para la validación del correcto funcionamiento del escenario propuesto.

# Bibliografía

## Capítulo 4 Antecedentes de redes y seguridad

Rincon Jaime. (2010). TIPOS DE SERVIDORES. 15 de Julio del 2014, de Scribs Sitio web: http://es.scribd.com/doc/26694127/TIPOS-DE-SERVIDORES.

Brodkin John . (2009). Green IT, virtualization top of mind at IT Roadmap. 20 de Julio del 2014, de NetworkWorld Sitio web: http://www.networkworld.com/article/2262342/virtualization/green-it--virtualization-top-of-mind-at-it-roadmap.html

S.A.M Rizvi, V.K. Sharma. (2011). Introduction to computer networks.United Kindon: Oxford

O´Flaherty Christian.(2009). IPv6 para Todos: Guía de uso y aplicación para diferentes entornos. Buenos Aires Argentina. Capitulo Argentina de ISOC

Iñigo Jordi, Barceló José María, Cerdá Llorenc, Peig Enric, Abella Jaume. (2008). Estructura de redes de computadores. Barcelona: UOC

STALLINGS William (2000). Comunicaciones y Redes de Computadores. España: Prentice Hall

DAVIES LEE, Joseph & Thomas (2003) Microsoft WINDOWS SERVER 2003 Protocolos, Y servicios TCP/IP (España): Referencia Técnica McGraw-Hill.

# Conclusiones

A lo largo del presente trabajo se abarcaron distintos temas que el alumno egresado de la carrera de Ingeniería en Computación del Módulo de Redes y Seguridad aprendió en las materias que componen el modulo. Estos conocimientos son la base para que el alumno enfrente los retos que día a día se presentan en el mundo laboral. Sin embargo el contar con estos conocimientos no garantiza que el alumno tenga la capacidad de utilizarlos para la resolución de problemas.

Por tal motivo el trabajo realizado, específicamente en el Capítulo 4, plantea una serie de escenarios prácticos donde el alumno se enfrenta a algunos problemas que en el campo laboral se presentan. Estos laboratorios fueron elaborados con base en investigaciones y reportes realizados por entidades de consultoría y de investigación de las tecnologías de información a nivel internacional, entre las que destacan: Gartner, IDC, NSS Labs, InfoSec Institute, así como en la participación en distintos proyectos a lo largo de la experiencia laboral por parte de nosotros.

Durante el periodo comprendido del 2 al 6 de Diciembre del 2014, se llevó a cabo el curso "Praxis de rede y seguridad", en el laboratorio de redes y seguridad de la facultad de ingeniería, con alumnos del último semestre de la carrera de Ingeniaría en computación, en el área de Redes y Seguridad. Este tuvo como objetivo poner a aprueba algunas prácticas planteadas en el capítulo 4, y así ver el impacto que estas causa en los alumnos.

El resultado obtenido fue el esperado, los alumnos contaba con los conocimientos teóricos, pero al momento de realizar las configuraciones en un dispositivo físicos empezaron a tener algunas dificultades, ya que no sabían cómo transformar esos conocimientos a algo práctico. Conforme fue avanzando el curso los alumno fueron desarrollando aptitudes tales como el razonamiento y el trabajo en equipo, esto factores ayudaron a que concluyeran los laboratorios satisfactoriamente.

De acuerdo a lo planteado en el objetivo y con base en los resultados obtenidos durante la realización del curso inter-semestral, consideramos que se debe contar una materia práctica donde el alumno ponga a prueba los conocimientos adquiridos a lo largo del Módulo de Redes y Seguridad, así como tener un lugar donde pueda realizar la manipulación y configuración de algunos dispositivos que conforman una red.