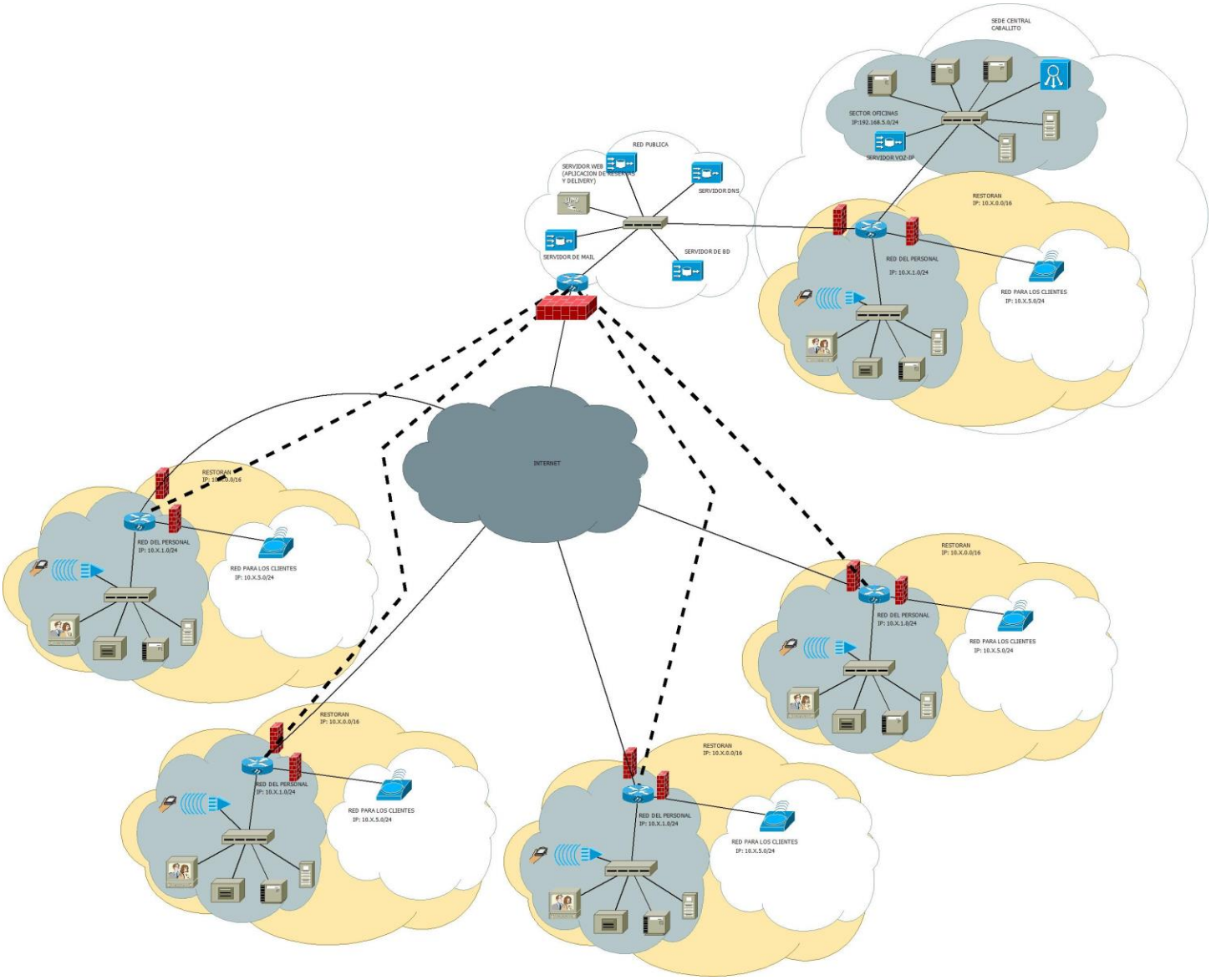
# Trabajo Práctico de Integración de Conocimientos

FECHA DE ENTREGA: 2/12/2015

Lucas Mufato. Legajo: 117780

# Índice:

# Topología y direccionamiento básico de la red



## Descripción general:

La red interconecta distintas restaurantes de una misma cadena mediante una VPN montada sobre enlaces dedicados (líneas punteadas) que unen las sedes con la central.

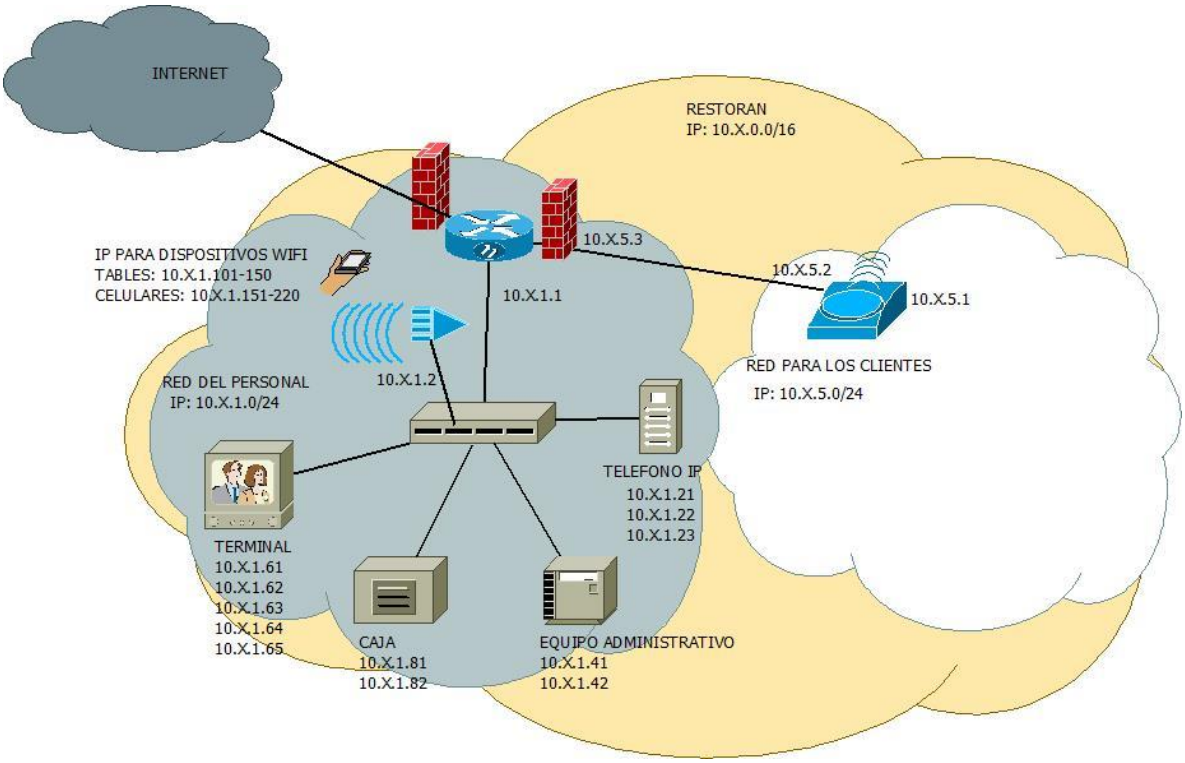
Estas sedes a su vez tienen otra conexión distinta a internet para brindar acceso tanto a los clientes, como a las necesidades de esa sede.
Todas los restaurantes de distintas sedes tiene la misma topología y configuración, la sede central tiene además del restaurant, una red de oficinas y una red pública con los servidores.

Direcciones IP de las sedes:

- Sede central (restaurant): 10.0.0.0/16
- Sede Junin: 10.1.0.0/16
- Sede La Plata: 10.2.0.0/16
- Sede Areco: 10.3.0.0/16
- Sede Pilar: 10.4.0.0/16
- Red de oficina de la sede central: 192.168.5.0/24
- Red pública para servidores: 200.127.211.0/28

# DIRECCIONAMIENTO

## Descripción del direccionamiento en los restaurantes




Todos los restaurantes tendrán un dominio de red dentro del 10.0.0.0/8, cada uno tendrá un subred del tipo /16 que se definirá de manera general como 10.X.0.0/16, siendo X un número que represente a cada sede (descripto en la sección “Descripción general”).

La red /16 de cada restaurant tendrá 2 redes /8, una red para los clientes y una red para el personal.

La red para los clientes será accesible a través del wifi, este no tendrá contraseña, y su dominio será el 10.X.5.0/24. Las direcciones IP para los clientes se asignaran dinámicamente entre las direcciones 10.X.5.5 y 10.X.5.254.

La red para el personal contendrá un switch (de 48 bocas) que conecta a todos los dispositivos que necesiten una conexión cableada, estos dispositivos y su rango de direcciones ip son:

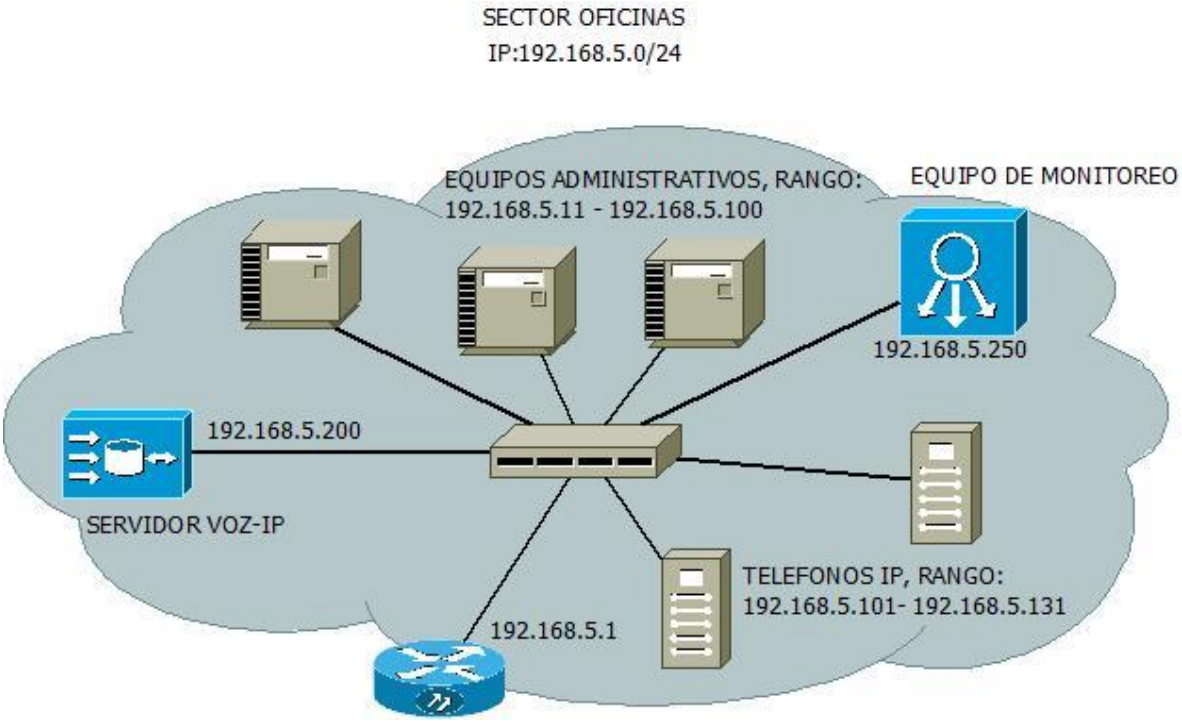
- Gestión de red: dentro del rango 10.X.1.1 – 10.X.1.20
- Teléfono IP: dentro del rango 10.X.1.21 – 10.X.1.40
- Equipo Administrativo: dentro del rango 10.X.1.41-10.X.1.60
- Terminal: dentro del rango 10.X.1.61 – 10.X.1.80
- Caja: dentro del rango 10.X.1.81 – 10.X.1.100

Estos rangos de direcciones son meramente para identificar distintos tipos o funciones de los dispositivos. Y no afecta su funcionamiento.

También hay un rango definido para los dispositivos inalámbricos, que se verán conectados mediante un Access Point, que serían las Tablet de los mozos que utilizan la aplicación enlatada para tomar pedidos, y los celulares de estos, que permitan realizar llamadas por la red de VOZ-IP de la empresa. Este rango será de:

- Tablet: dentro del rango: 10.X.1.101 – 10.X.1.150
- Celulares: dentro del rango: 10.X.1.151- 10.X.1.220

## Descripción  del direccionamiento en la oficina




La sección de oficina tendrá 24 equipos administrativos, 12 teléfonos IP, 1 servidor de VOZ-IP y 1 equipo que será el encargado del monitoreo de esta y el resto de las redes de la empresa.
Esta red tiene el dominio 192.168.5.0/24, los equipos administrativo ocuparan los rangos entre 192.168.5.11 – 192.168.5.100.

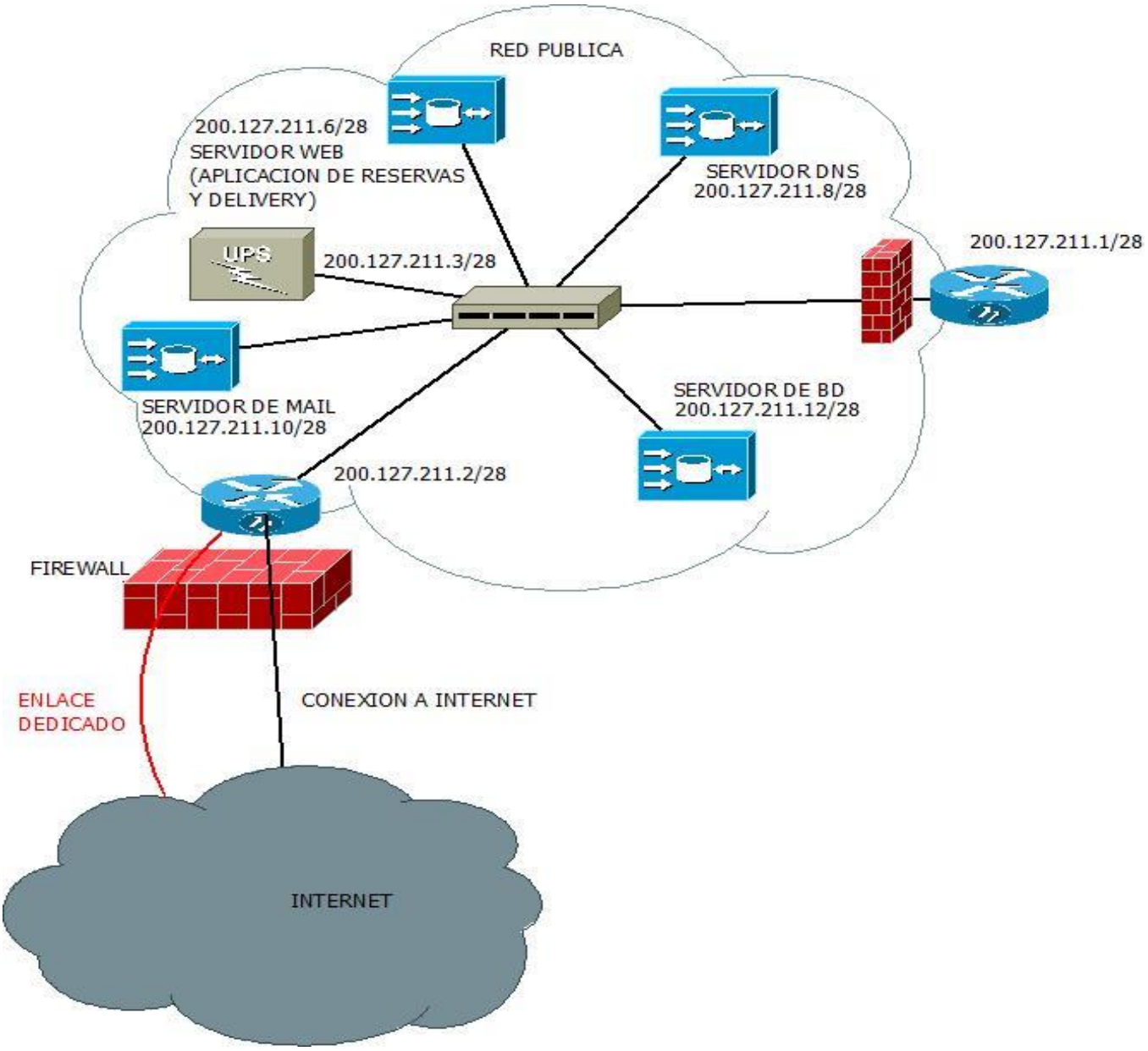
Los teléfonos IP ocuparan los rangos entre 192.168.5.101 – 192.168.5.131.

El servidor VOZ-IP tendrá la IP 192.168.5.200/24.

El equipo de monitoreo de redes tendrá la dirección 192.168.5.250/24.

Las direcciones de todos los equipos son estáticas y están conectados mediante un Switch de 48 bocas.

## Descripción del direccionamiento en la red pública




La red pública de la empresa es la 200.127.211.0/28, en esta se alojaran los servidores que brindan servicios al exterior como hacia dentro de la misma empresa. Estos servidores son:

- Servidor Web, IP: 200.127.211.6/28
- Servidor DNS, IP: 200.127.211.8/28
- Servidor de Correo, IP: 200.127.211.10/28
- Servidor de Base de Datos, IP: 200.127.211.12/28

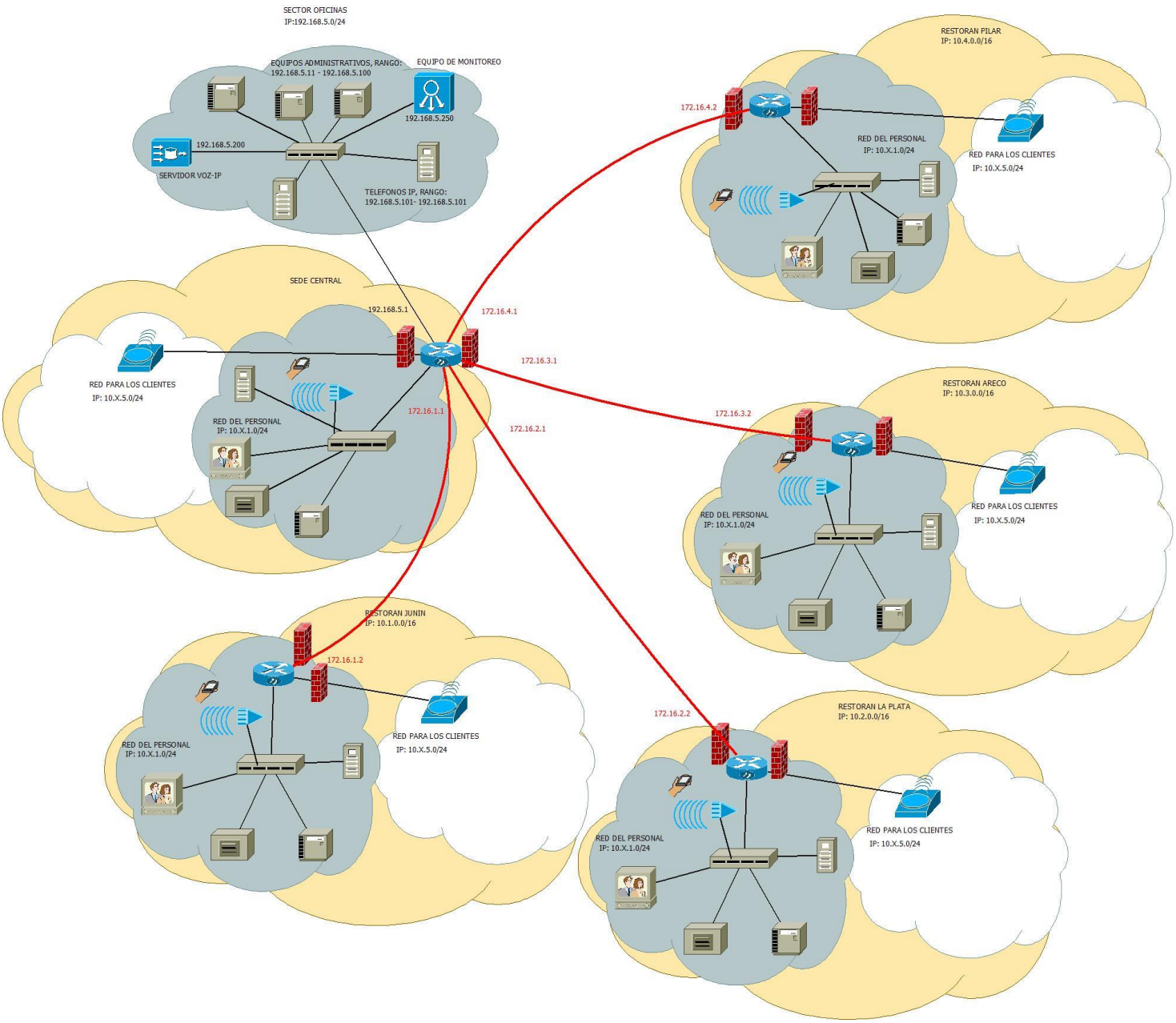
Cada servidor físico contendrá 2 máquinas virtuales, cada una actuara como servidor lógico (por ejemplo: servidor web).

Habrá 2 servidores físico, uno contendrá al servidor web y al servidor de Base de Datos, el otro al servidor DNS y al servidor de Correo.

## Redundancia y resistencia a fallos:

En esta red habrá un UPS. Los servidores y equipos de ruteo estarán enchufados en este para no sufrir problemas por variaciones en la tensión o cortes de luz. Al mismo tiempo, cada servidor tendrá una copia de respaldo en otro servidor, de esta manera si se produce un fallo en un servidor, otro podrá tomar su lugar. (Una arquitectura maestro-esclavo)

# Descripción de la VPN




La VPN interconectara las redes de los restaurants de las distintas sedes con la central, tendrá una topología del tipo ESTRELLA, dado que todas las sedes se conectaran con la central mediante los enlaces dedicados.

El objetivo de la VPN es simular un canal directo entre las sedes y la centra, de modo que las distintas redes privadas se puedan comunicar entre ellas de modo seguro (cifrando los paquetes)

## Descripción general de la conexión en la red

Todas las redes de los clientes tendrán acceso a internet, pero no podrán acceder a otras redes de la empresa, ni a otras redes de clientes.

En cambio las redes del personal de los restaurants podrán comunicarse entre ellas mediante la VPN, también con la con red de oficina.

# Dispositivos necesarios y requerimientos de los enlaces

## Dispositivos necesarios:

- Router WIFI (LINKSYS WRT1900ACS)
- Switch grande (Tp-link Tl-sf1048 48 Puertos)
- Switch mediano (Tp-link Tl-sg1024 24 Puertos)
- Teléfonos IP ( Gigaset A510IP )
- UPS (Smart UPS SRC 2000 XLI)
- Servidores (Intel Xeon E3 V3)
- Equipo Router (Sera una computadora o servidor con un Debian configurado para routear)

## Numero de dispositivos necesarios:

- Router WIFI: 2 por cada restorán. Total: 12.
- Switch grande: 1 por cada restorán + 1 por oficina. Total 7.
- Switch mediano: 1 para la red de los servidores. Total 1.
- Teléfonos IP: 3 por cada restorán + 12 por oficina. Total: 27.
- UPS: 1 para la red de los servidores. Total: 1.
- Servidores: 2 para la rede de los servidores + 1 para oficinas. Total: 3
- Equipo Router: 1 por cada restorán + 1 para la red de servidores. Total: 6

## Requerimientos de conexión a internet y enlaces dedicados:

Las sedes contaran con las siguientes características en cuestión de acuerdo de nivel de servicio:

- Retardo: un máximo de 400ms con cualquier dispositivo ubicado en la Argentina
- Jitter: un promedio de retardo de 200ms
- Capacidad del canal: 3 Mbps asimétricos, 2 Mbps de bajada y 1 Mbps de subida.
- Perdida de paquetes: no mayor al 0,5% diario y 1% mensual.
- Disponibilidad: de 95% mensual, siendo no menor a un 98% anual
- Preservación de secuencia de flujo:  no se deberá preservar la secuencia del flujo
- Calidad de experiencia: no se tomara en cuenta esta característica.

El enlace hacia internet de la sede central contara con las siguientes características:

- Retardo: un máximo de 200ms con cualquier dispositivo ubicado en Argentina
- Jitter: un promedio de retardo de 100ms
- Capacidad del canal: 3 Mbps simétricos
- Perdida de paquetes: no mayor al 0,3% diario y 0,5% anual.
- Disponibilidad: de 98% mensual, siendo no menor a un 99,9% anual
- Preservación de secuencia de flujo: no se deberá preservar al secuencia de flujo
- Calidad de experiencia: no se tomara en cuenta esta característica.

Los enlaces dedicados entre las sedes y la centra tendrán las siguientes características:

- Retardo: un máximo de 100ms
- Jitter: un promedio de retardo de 50ms, con una varianza máxima de 30ms
- Capacidad del canal: 1 Mbps simétricos
- Perdida de paquetes: no mayor al 0,1% diario y 0,5% anual.
- Disponibilidad: de 98% mensual, siendo no menor a un 99,9% anual

- Preservación de secuencia de flujo: se deberá preservar la secuencia de flujo(importante para el servicio de VOZ-IP)
- Calidad de experiencia: no se tomara en cuenta esta característica.

## Implementaciones en software

Servidor web: APACHE 2.4.17, ya que es software libre, potente, multiplataforma y muy configurable. Alternativa: TOMCAT.

Servidor de mails: POSTFIX 3.0, dado que también es software libre y corre en sistemas Unix, alternativa: SMTP EXCHANGE

Servidor de Base de datos: POSTGRES 9.4, ya que es multiplataforma y software libre. Alternativa: MYSQL.

Servidor DNS: BIND 9.4, ya que es multiplataforma. Alternativa: NSD3

Servidor VOZ-IP: ASTERIKS 12.2.0, porque es software libre. Alternativa: ELASTIX

Firewall: IPTABLES, simple y potente, fácil de configurar.

## Descripción del firewall y priorización de tráfico

### Firewall:

Se configurara un firewall en cada router de cada sede que se conecte a internet, en el caso de la sede central, será el que se conecte a la red pública de la empresa. También el router que conecta esta red pública con internet tendrá una configuración de firewall.

Todos estos Firewalls contara con una **POLITICA PERMISIVA**, una configuración básica que tendrán es no permitir el paso de paquetes desde una red 10.X.5.0/24(red de los clientes) a una red 10.X.X.0/24 (red del personal) o a una red 192.168.X.0/24(red de oficinas).

Ejemplo de configuración en IPTABLES:

*Iptables –a forward –s 10.X.5.0/24 –d 10.x.0.0/16 –J reject*

(Este comando impide a cualquier dispositivo de la red 10.X.5.0 enviar mensaje a alguno de la red 10.X.0.0/16)

*Iptables –a forward –s 10.X.5.0/24 –d 192.168.0.0/16 –j reject*

(Este comando impide a cualquier dispositivo de la red 10.X.5.0 enviar mensaje a alguno de la red 192.168.0.0/16)

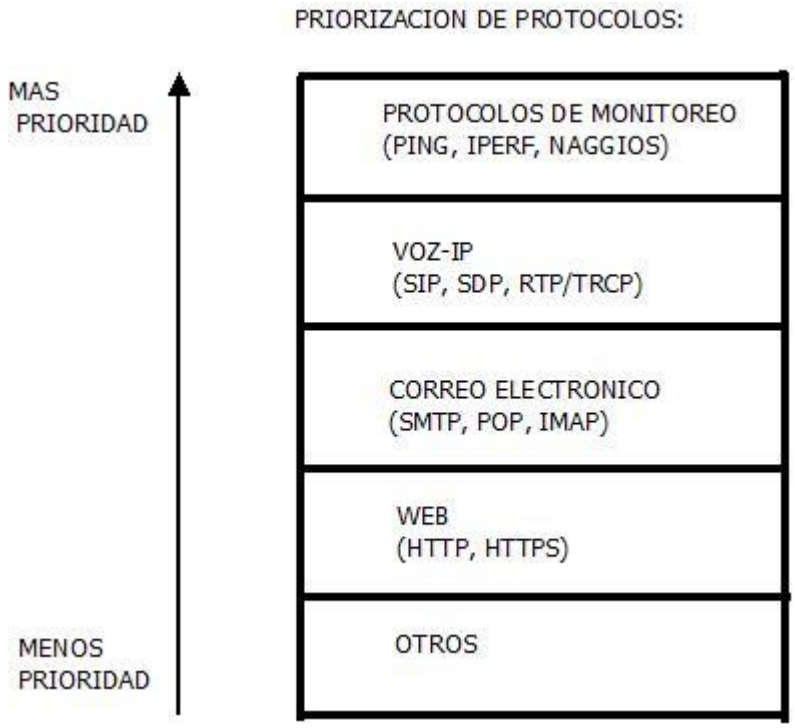
*Iptables –a forward –d 10.X.5.0/24 –s 192.168.0.0/16 –j reject*

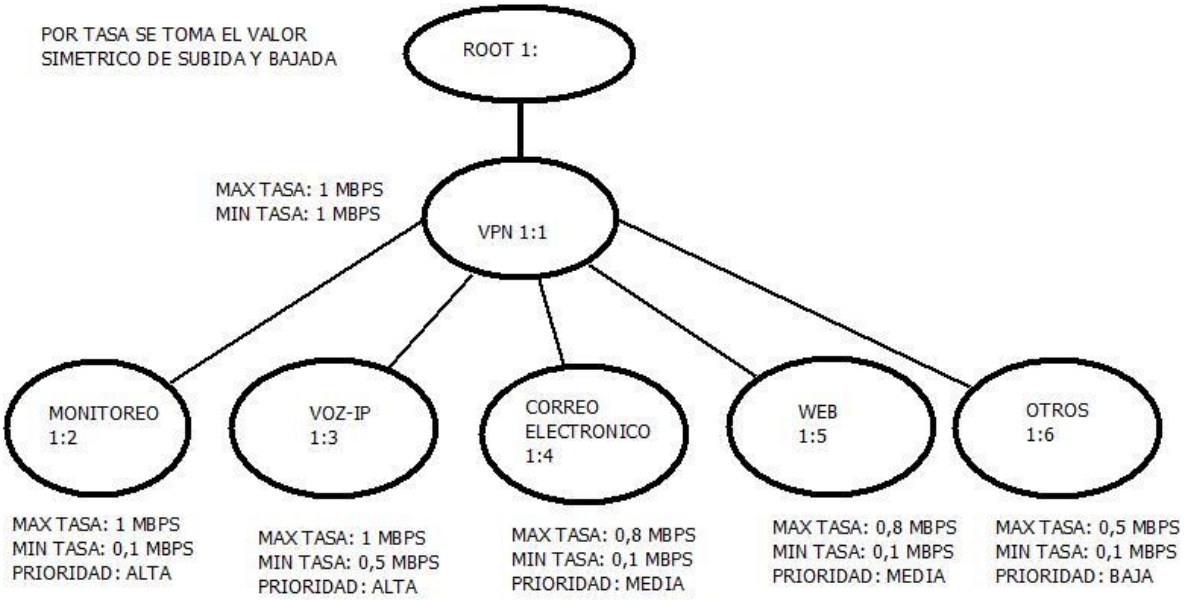
*Iptables –a forward –d 10.X.5.0/24 –s 10.x.0.0/16 –j reject*

(Estos últimos 2 comandos impiden a dispositivos de las redes 192.168.0.0/16 y 10.X.0.0/16 enviar mensaje a cualquier dispositivo de la red 10.X.5.0/24).

## Priorización del tráfico:

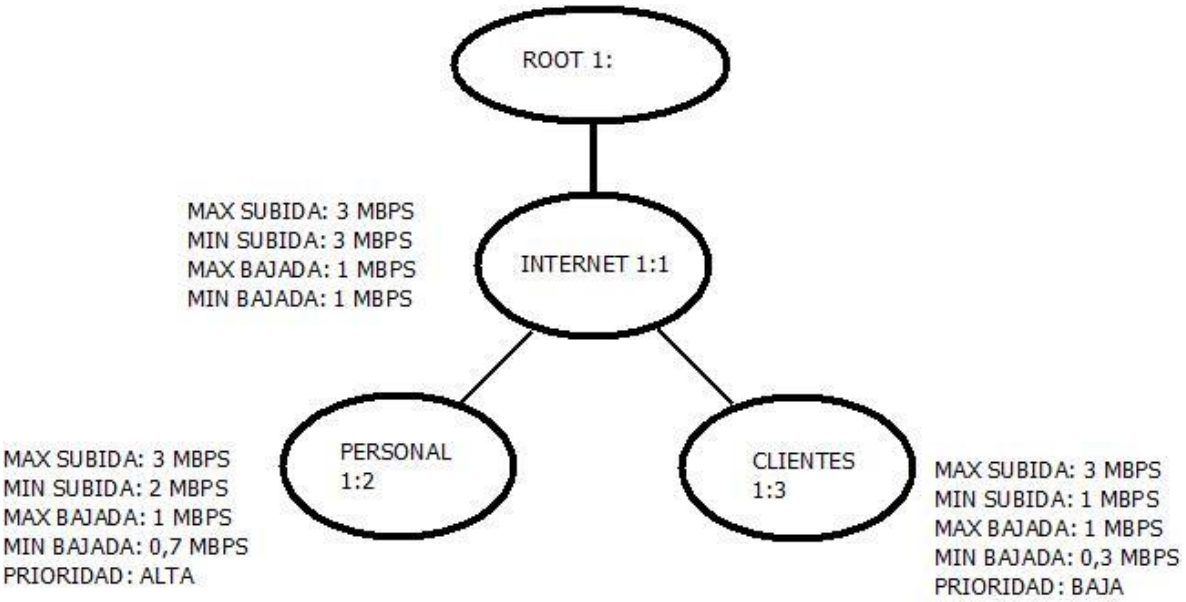
El tráfico de las VPN será priorizado por su tipo de la siguiente manera:





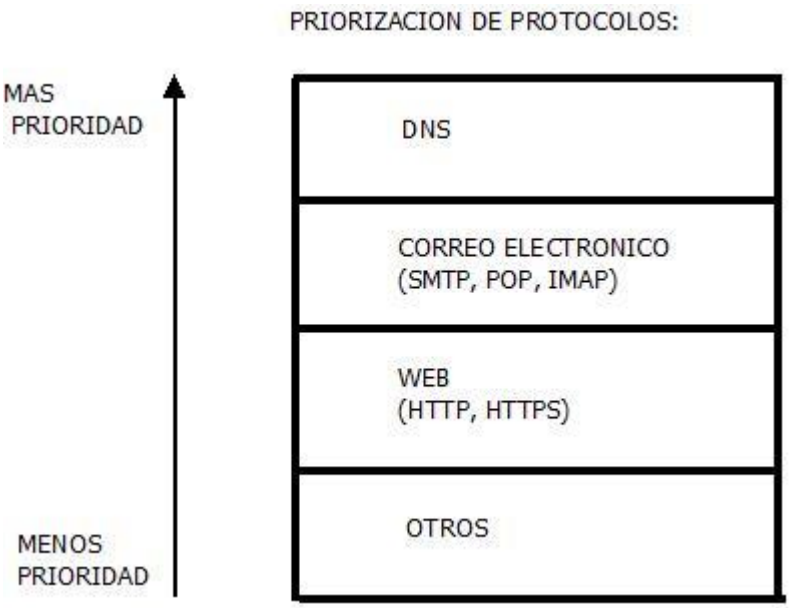

El tráfico saliente hacia internet será priorizado por su origen:

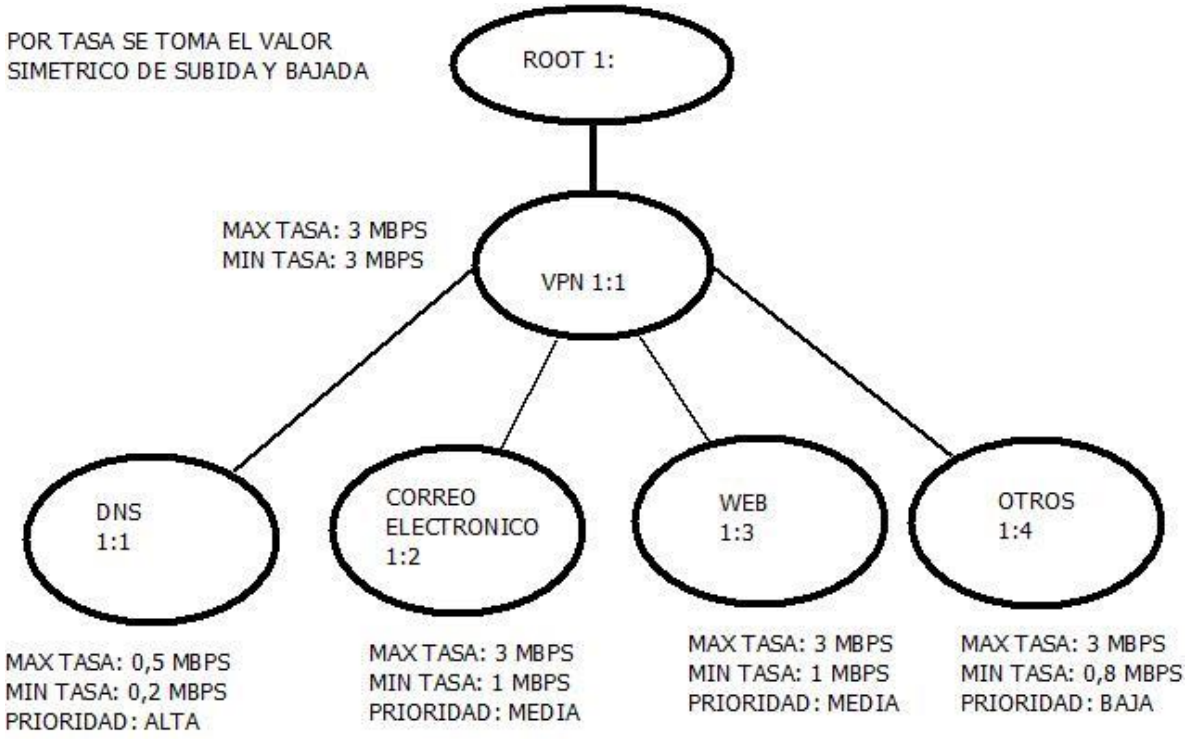
- Se dividirá en el tráfico de los clientes y el tráfico del personal, ambos tendrán la posibilidad de utilizar como máximo todo el canal, pero como mínimo la clase del personal usara 2/3 del canal mientras que la clase del cliente usara 1/3




Este caso también incluye al router de la sede central que envía la información a la red pública de la empresa.

En la sede central, el tráfico desde la red pública hacia internet se priorizara  por protocolo:



# Herramientas de monitoreo

## Monitoreo desde equipo de gestión (en la red de oficinas):

Este equipo contara con varios programas instalados para medir diversos servicios, funcionamientos, etc. Estos programas son:

**Smokeping**: se utilizara para medir el delay y el jitter con cada sede constantemente para verificar que se cumple el SLA en los enlaces dedicados. Esta herramienta estará activa todo el tiempo.

**Iperf**: se utilizara para medir la capacidad del canal en los enlaces dedicados en que forman la VPN, el cliente será el equipo de gestión y el/los servidores serán los routers de "borde" en las sedes. Esta herramienta se utilizara en momentos determinados.

**Nagios:** se utilizara para monitorizar equipos y servicios, preferentemente los servidores de la red pública. Un ejemplo de la configuración de las alertas que el programa emitirá serian en los siguientes casos:

- Capacidad del disco es mayor del 75% en cualquiera de los servidores se enviara un mail a la administrador de red.
- Si un Servidor no responde, se enviara un mail y al administrador de red.
- Si la temperatura en un servidor supera los 120 grados se enviara un mail al administrador de red.
- Si un firewall descarta más de 1000 paquetes en un minuto o tiene un porcentaje de descarte mayor al 70% se enviara un mail al administrador de red.
- Si el uso de CPU de algún servidor es mayor del 90% por más de 20 minutos se enviara un mail al administrador de red.
- Si el uso de memoria RAM es superior al 90% por 20 minutos se enviara un mail al administrador de red.
- Si la UPS detecta un corte en la energía, se enviara un mail al administrador de red.

## Monitoreo desde los routers en las sedes:

**Ntop**: se utilizara para realizar estadísticas del uso de las redes conectadas al router, de esta manera se detectaran anomalías como: un dispositivo que use demasiado la red, que transmiten en un protocolo que no deberían, etc. Esta herramienta estará activa todo el tiempo.

**Nmap**: se utilizara para verificar que en todos los dispositivos, solamente estén abiertos los puertos para procesos necesarios, y no haya procesos indeseados escuchando en algún puerto de algún dispositivo. Esta herramienta se utilizara en momentos determinados.

# Gestión de Certificados y Seguridad

## Servidor Web

La empresa contara con un par de claves públicas y privadas, en el servidor web se instalara la clave privada, se generara un solicitud de firma de certificado, en la cual se encontrara la clave pública e información de identidad de la empresa, esta solicitud será enviada a una Autoridad de Certificados. Esta firmara la solicitud, devolviendo un certificado, el cual será utilizado por el servidor web para autenticarse con los clientes brindando confiabilidad.

La Autoridad de Certificados será una de las siguientes entidades:

- Comodo
- Symantec
- GoDaddy
- GlobalSign
- DigiCert

## VPN

Para la implementación de VPN se utilizara el software *openvpn,* con el cual se crearan un par de claves públicas y privadas, las que deberán estar en ambos extremos de los equipos conectados. De esta manera se consigue una comunicación cifrada de manera simétrica.