TRABAJO PRÁCTICO DE INTEGRACIÓN DE CONOCIMIENTOS

Administración y gestión de Redes (11085)

Luz Bárcena 118124
mluzbarcena@gmail.com

Contenido

Situación 2
Topología de las redes de la organización 2
Esquema de direccionamiento IP 4
Detalle de Sede Central 4
Detalle de sucursales 5
Detalle de servidores 6
Dispositivos físicos requeridos 6
Sede central 6
Sucursales 7
Servidores 7
Requerimientos de nivel de servicios (SLAS) 7
Métricas en la conectividad a Internet 7
Métricas en la conectividad entre las sucursales 7
Implementaciones de software 7
Configuraciones para la implementación de una central telefónica VoIP 8
Configuración de Firewall 8
Monitoreo 8
QoS 9
Seguridad en el servidor 11
VPN 12
Suposiciones 12

Situación

Cadena de restaurantes, con sede central en Caballito y sucursales en Pilar, La Plata, San Antonio de Areco y Junin (la idea es expandirse).

Rubro de gastronomía.

La gente debe poder ver por Internet los menús que hay en cada una de las sucursales. En cada ciudad puede cambiar el menú. Pueden ver la disponibilidad si hay mesas, pueden hacer reservas en cualquier localidad en las que hay restaurantes y pueden hacer pedidos de delivery por Internet.

Va a haber Wi-Fi en todos los restaurantes sin contraseña.

Los mozos levantan desde un smartphones (con una aplicación enlatada) los pedidos directamente de la mesa, que van apareciendo en la cocina (terminales), y después en la caja (terminal).

Telefonía IP entre las sucursales, y que los mozos tengan su propio interno en el celular.

Ya tienen telefonía tradicional.

Va a tener un servidor de mail también, porque se mandan promociones por mail a los clientes.

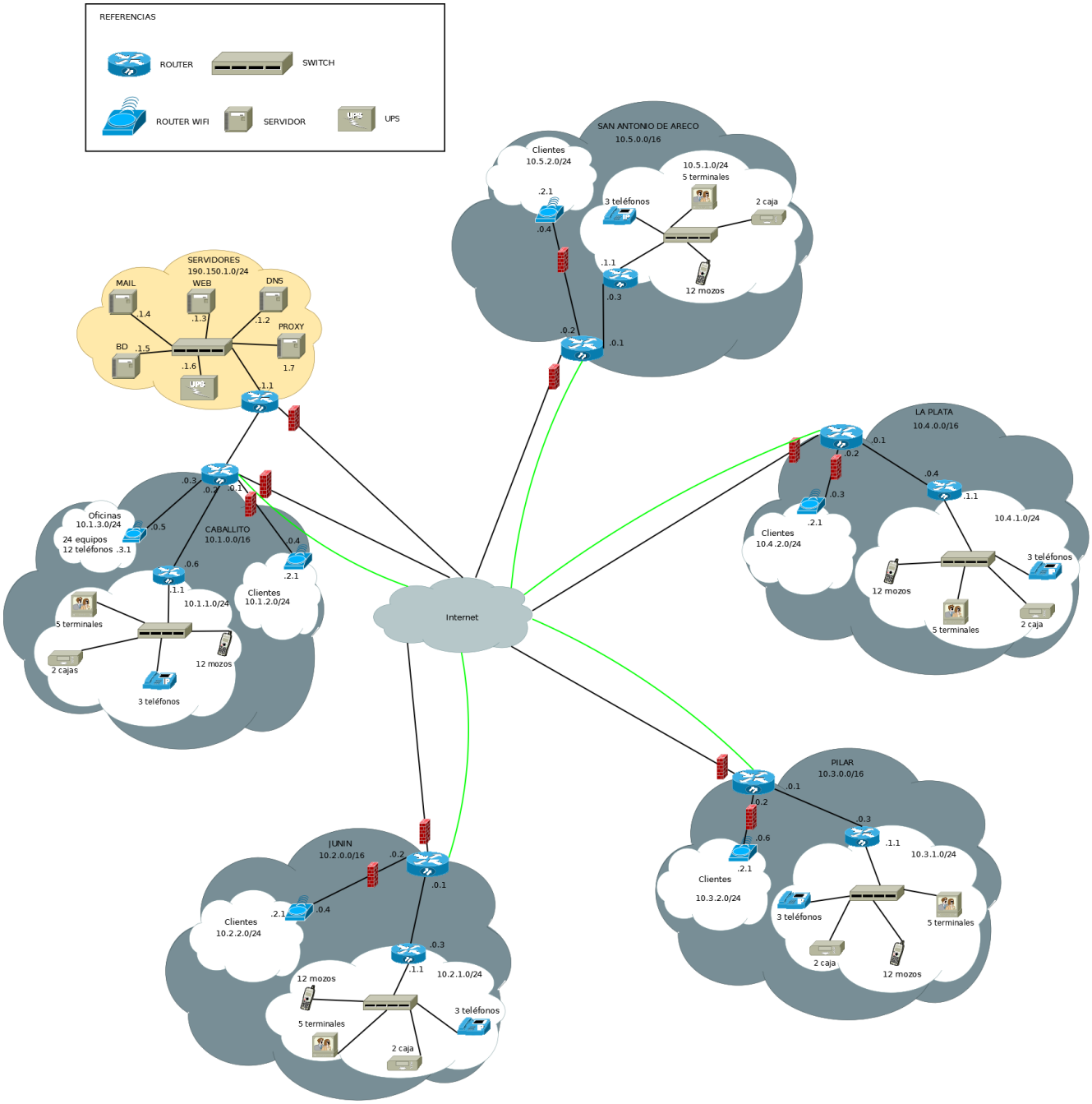
La sede central va a contar con el restorán mismo, y arriba unas oficinas grandes. En estas hay 24 computadoras y 12 teléfonos.

En todas las sedes habrá:

- 5 terminales en todas las cocinas, 2 en las cajas
- 12 mozos por sucursal.
- 3 teléfonos: 1 cocina, 1 adm, 1 caja.

En cada restorán se estima que va a haber 150 personas como máximo.

Topología de las redes de la organización



La red conecta cuatro sucursales y una sede central a través de una red VPN para que el tráfico sea seguro entre ellas.

La sede central (Caballito) cuenta con tres redes para diferenciar tres grupos de usuarios o aplicaciones. Una de ellas es la red Wi-Fi que utilizarán los clientes del restaurante con la que accederán a Internet, otra para las oficinas y la tercera es la que involucra a los mozos y las terminales. A su vez, también está conectada a una red pública en la que se encuentran los servidores: web, mail, BD, proxy y DNS.

Las cuatro sucursales cuentan con la misma topología; una red Wi-Fi a la que se conectan los clientes para acceder a Internet y la red de mozos y terminales.

Esquema de direccionamiento IP

Sede central Caballito: 10.1.0.0/16

Sucursal Junín: 10.2.0.0/16

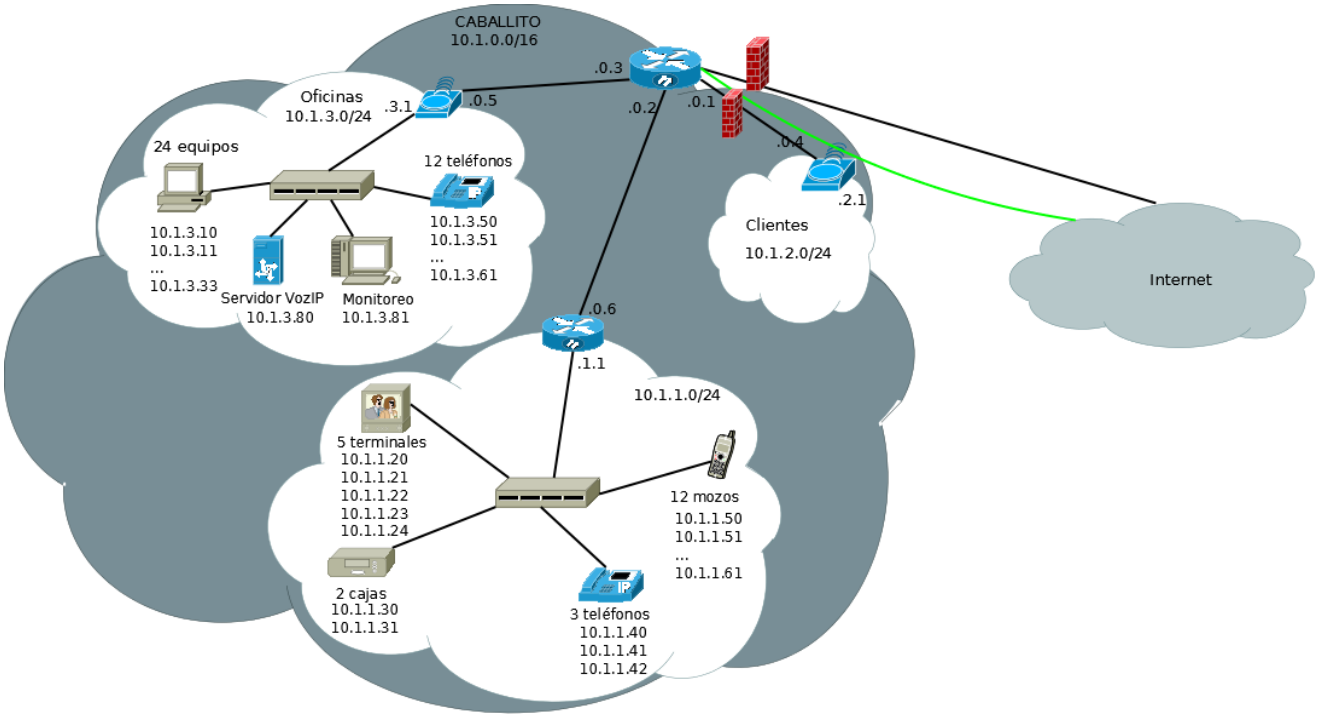
Sucursal Pilar: 10.3.0.0/16

Sucursal La Plata: 10.4.0.0/16

Sucursal San Antonio de Areco: 10.5.0.0/16

Red de servidores: 190.150.1.0/24

Detalle de Sede Central

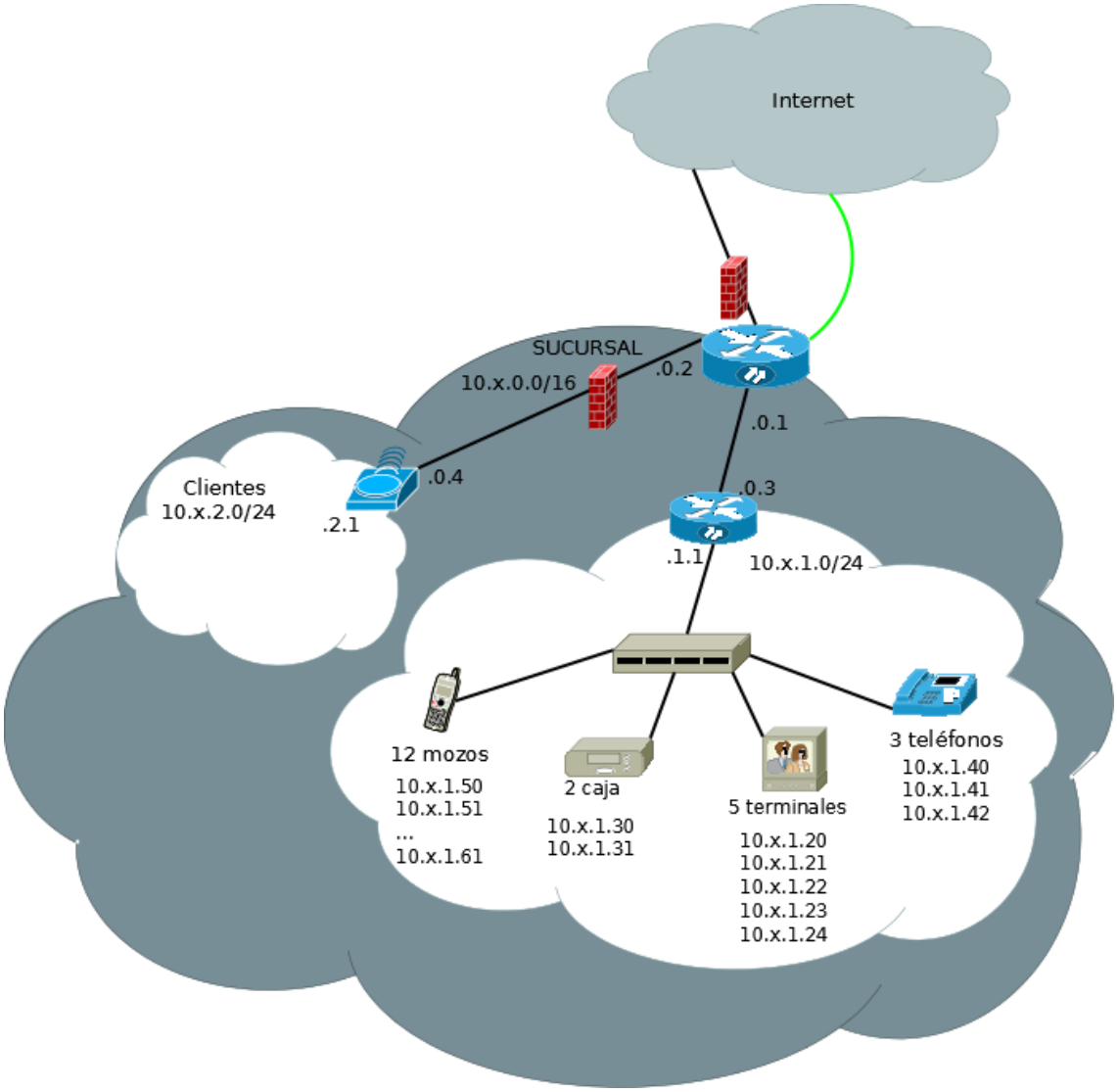


Dentro de la sede central entonces se encuentran tres redes.

- La primera de ellas es la red 10.1.1.0/24 en la que se encuentran 12 mozos, 3 teléfonos, 2 cajas, 5 terminales en la cocina y el servidor VozIP, pero también queda un rango en la red para utilizar si se necesitan agregar más dispositivos.
- La segunda es la red Wi-Fi de clientes 10.1.2.0/24 en la que los clientes se conectarán sin necesitar clave para poner acceder a Internet.
- La tercera de las redes es la de las oficinas 10.1.3.0/24 en la que se encuentran 24 equipos de administración con salida a Internet y 12 teléfonos IP.

La sede central también estará conectada a la red pública de servidores de la organización a través de un router.

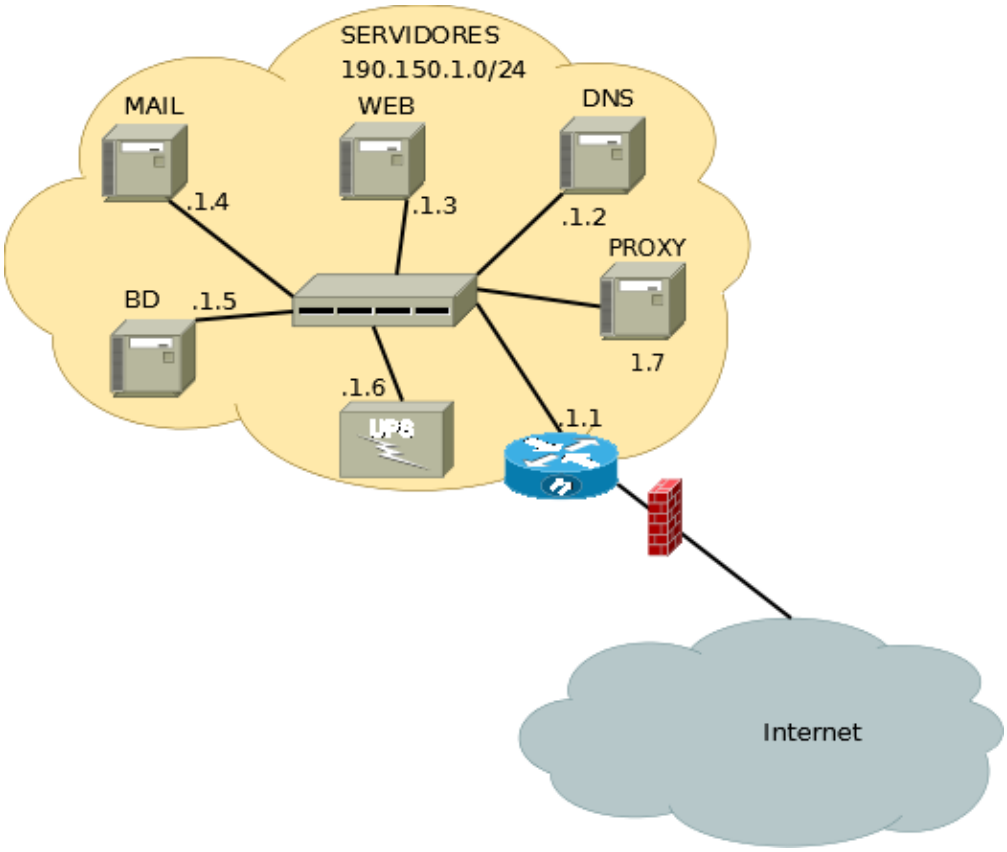
Detalle de sucursales



Las sucursales van a tener el mismo tipo de red 10.x.0.0/16 donde x es el número que va variando. Todas ellas tendrán la misma topología, teniendo dos redes internas.

- La primera red es 10.x.1.0/24 donde se encontrarán los dispositivos de los 12 mozos, 2 cajas, 5 terminales y 3 teléfonos, también contemplando una posible expansión por si se necesitaran más dispositivos.
- La segunda red es la red Wi-Fi de clientes 10.x.2.0/24 a la que se conectarán los clientes sin necesidad de clave para acceder a Internet.

Detalle de servidores



La red de servidores tendrá un IP pública y brindará servicios al exterior e interior de la organización, por lo que saldrá a Internet sin incovenientes.

Tendrá:

- **Un servidor de mail:** 190.150.1.4
- **Un servidor web:** 190.150.1.3
- **Un servidor DNS:** 190.150.1.2
- **Un servidor Proxy:** 190.150.1.7
- **Un servidor de BD:** 190.150.1.5, y
- **Una UPS:** 190.150.1.6 para tener un sistema de fallas en ocasiones en que por ejemplo haya problemas eléctricos con los equipos.

Dispositivos físicos requeridos

Sede central

- 2 switchs
- 2 routers Wi-Fi
- 2 routers
- Una PC para ser Servidor de VozIP
- Una PC para monitoreos
- 15 teléfonos
- 24 equipos
- 7 terminales

Sucursales

- 1 switch
- 1 router Wi-Fi
- 2 routers
- 7 terminales
- 3 teléfonos

Servidores

- 1 switch
- 1 router
- 1 UPS
- 5 servidores

Requerimientos de nivel de servicios (SLAS)

Métricas en la conectividad a Internet

- Retardo delay: 400ms máximo.
- Jitter: 200ms máximo.
- Throughput-Bandwidh: 6Mbps.
- Pérdida de paquetes: no debe ser superior a 1% de los paquetes transmitidos.
- Disponibilidad: superior a 98%.
- Preservación de secuencia por flujo:
- Calidad de experiencia:

Métricas en la conectividad entre las sucursales

- Retardo delay: 200ms máximo.
- Jitter: 100ms máximo.
- Throughput-Bandwidh: 3Mbps.
- Pérdida de paquetes: no debe ser superior a 1% de los paquetes transmitidos.
- Disponibilidad: superior a 98%.
- Preservación de secuencia por flujo: paquetes ordenados, ya que un mal ordenamiento trae muchos problemas con VOIP por ejemplo.
- Calidad de experiencia:

Implementaciones de software

- **Servidor BD:** PostgreSQL 9.5 porque es gratuito y libre y es considerado uno de los motores de BD más avanzados en la actualidad. Segunda opción MySQL, también software libre.
- **Servidor Mail:** PostFix 3.1 por su sencillez y seguridad. Segunda opción Exim4.
- **Servidor DNS:** Bind 9.10.4 porque es el servidor más utilizado en Internet ya que es multiplataforma. Segunda opción OpenDNS.
- **Servidor Web:** Apache porque es software libre, con mucho soporte y muchas funcionalidades. Segunda opción TomCat 8.
- **Servidor VoIP:** AsteriskNow porque es una solución simple utilizando Asterisk. Segunda opción Elastix.
- **Servidor Proxy:** Squid.

Configuraciones para la implementación de una central telefónica VoIP

Para la central telefónica en la sede central se instalará en una computadora ubicada en la oficina, el software AsteriskNOW.

Como se cuenta con un solo servidor ubicado en la sede central, en caso de problemas con el servidor, no estará disponible la opción de hacer llamadas con los teléfonos IP o los smartphones.

Si no hay una buena configuración y una buena calidad de servicio asegurada, va a haber muchos problemas y poca eficiencia en las comunicaciones por este medio. Por eso se necesita asegurar que:

- No haya pérdidas de paquetes significativas, ya que esto puede causar que, en la espera por éstos, incrementen los retardos. Si aumentan los retardos de algunos paquetes, y en otros no, esto causa que haya una variación de ellos (jitter) y que la comunicación no sea buena.
- No haya paquetes fuera de orden porque también aumentan la latencia.

Configuración de Firewall

Mediante la configuración de ciertos firewalls se filtrará el tráfico entre las redes de la organización (Internas) e Internet (externas) para prevenir intrusiones, como así también el tráfico entre las redes de clientes y las redes de oficinas y del restaurante.

Para esto, en las sucursales y sede central, se configurarán:

- Los routers que rutean a Internet.
- Router Wi-Fi de la red de clientes.

En la red de servidores se configurará en el router con salida a Internet.

Tendrán una política permisiva, o sea que no se filtrará nada que no esté explícitamente configurado.

Monitoreo

Las herramientas a utilizar son:

SmokePing: Es una herramienta para medir el retardo de un punto a otro. Es una herramienta simple, que genera gráficos para la interpretación de los retardos. Esta herramienta va a medir el retardo todo el día, es decir que va a estar siempre activa.

Iperf: Es una herramienta para medir el throughput y la calidad del enlace. Se utilizará para medir la calidad del enlace VPN.

Ntop: Es una herramienta para el monitoreo y análisis del tráfico en la red, con la cual se podrán observar por ejemplo la actividad de la red en un espacio de tiempo o la actividad por protocolos.

Nmap: Es una herramienta para escaneo de puertos y exploración de redes. Puede no ser segura ya que brinda información de los equipos de la red y de los puertos que se encuentran abiertos o cerrados. Se usará en algunas ocasiones para verificar que los puertos de los diferentes servicios estén abiertos y sean correctos.

Los aspectos más importantes a analizar con estas herramientas son el uso de la red, el retardo que hay y si hay en un lapso de tiempo una cantidad significativa de descarte de paquetes.

Utilizando **Nagios** (sistema de monitorización) se mandarán las alertas sobre situaciones no normales en software o hardware al administrador. Las razones pueden ser, por ejemplo:

- Un alto porcentaje de uso de disco.
- Logueos indebidos.
- Mucha carga en el procesador.
- Caída de un servidor.
- Corte de luz, y en consecuencia la UPS quede sin conexión con corriente.
- Un alto número de descarte de paquetes.
- Temperatura alta en un servidor.

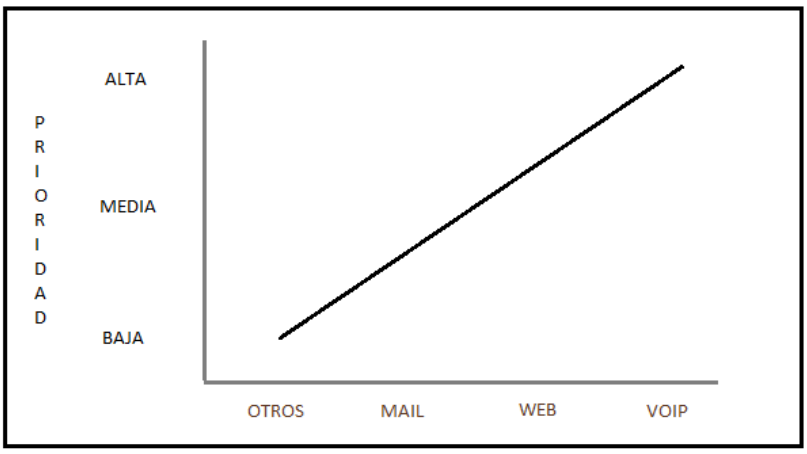
Esto puede ser mediante correo electrónico.

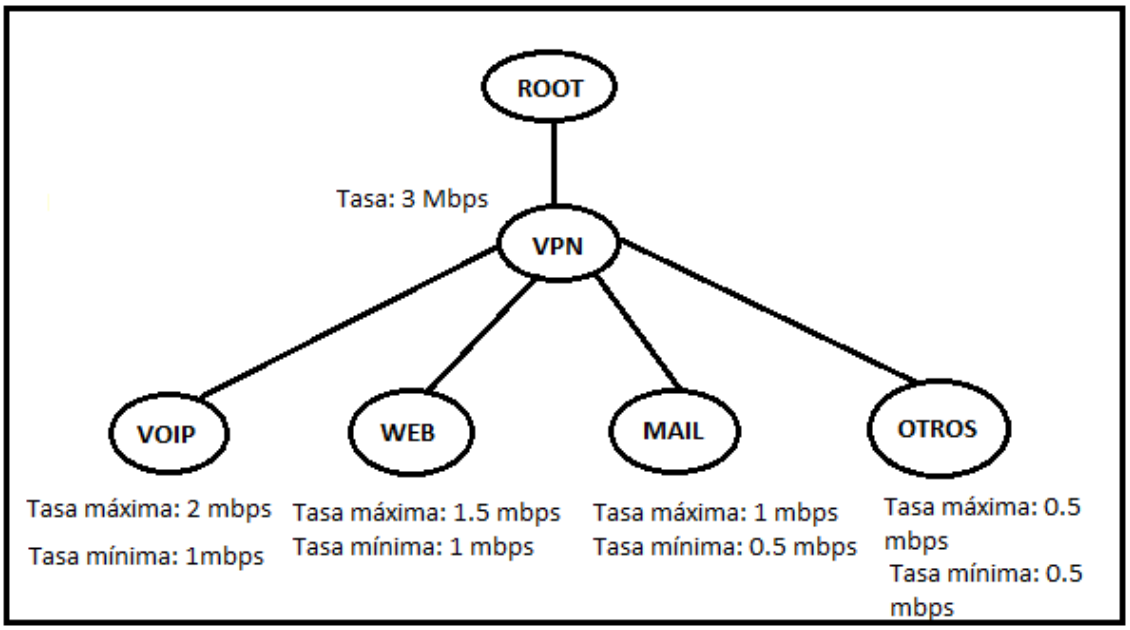
También es una herramienta que permite ver el estado de la red mediante una herramienta web y crear ciertos informes con respecto a la necesidad.

QoS

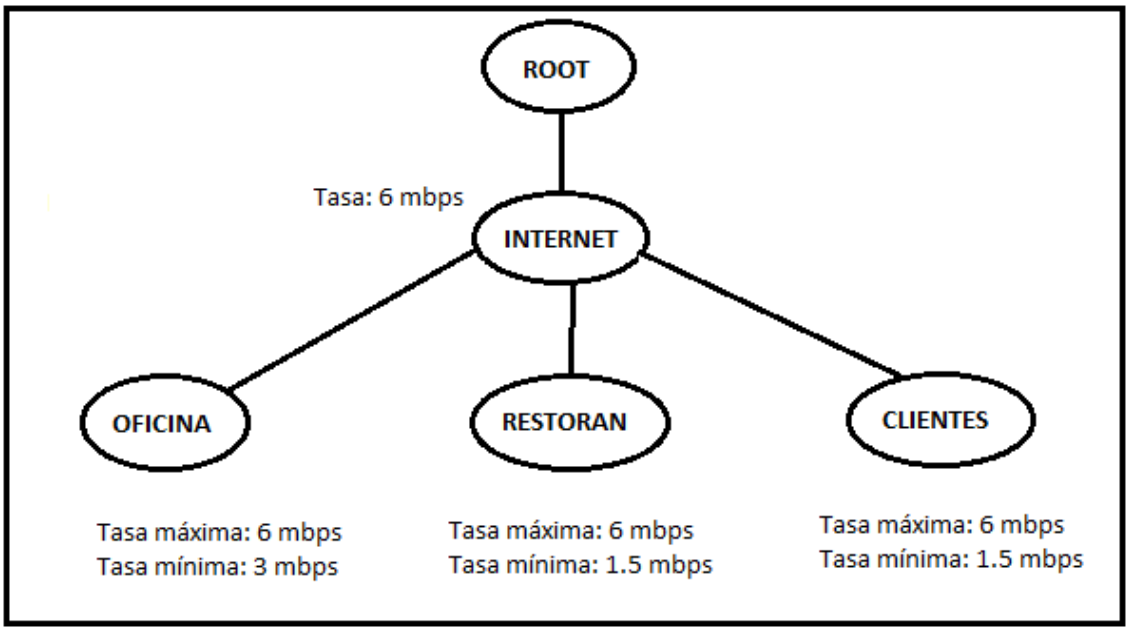
VOIP necesita tener prioridad en el tráfico. No puede tener una latencia superior a 200ms ya que en caso contrario las conversaciones no serían fluidas.

- Por eso es que, **en la red VPN** que une a las sucursales y la sede central, se dará prioridad de la siguiente manera:



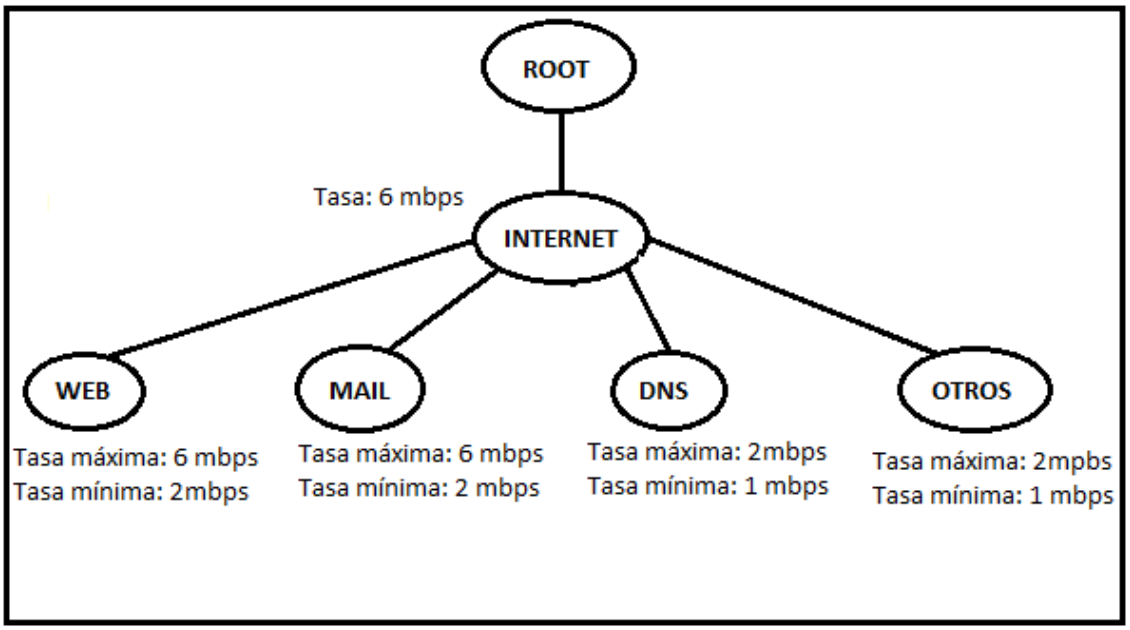


- Mientras que el tráfico **dirigido a Internet** tendrá las siguientes características:

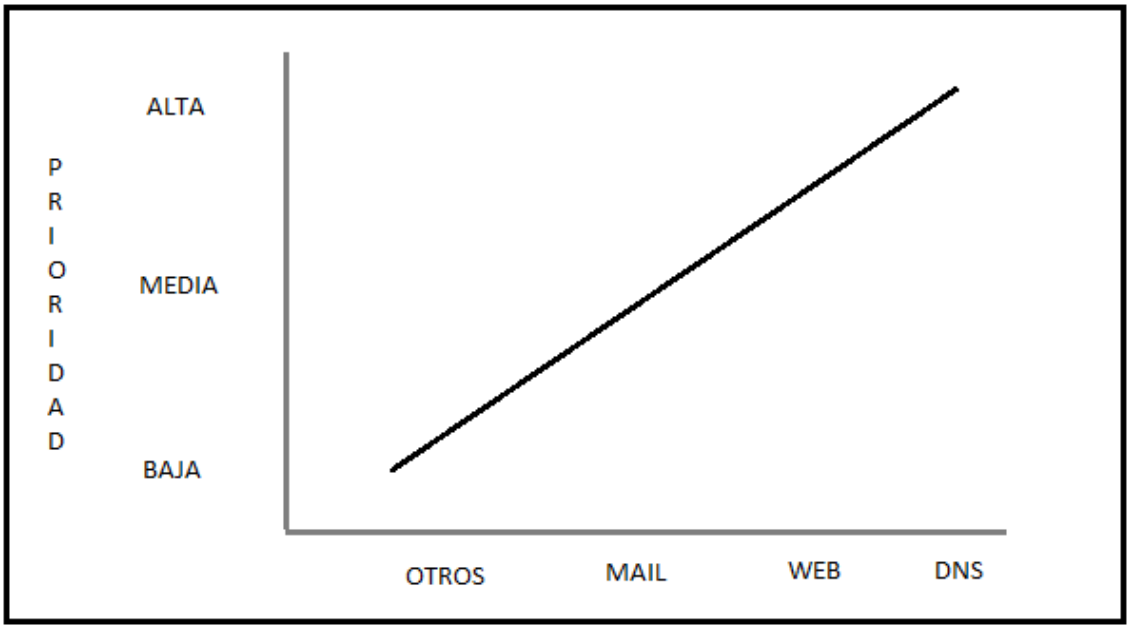


Como se puede ver, las oficinas tienen una prioridad más alta que la red del restaurante y que la de los clientes.

- La situación del tráfico a Internet desde la **red de servidores** es:



Y la prioridad que tienen es:



Seguridad en el servidor

Una buena medida para tener seguridad en el servidor web si es que, por ejemplo, se manejan datos importantes del usuario, es usar un certificado digital.

SLL permite encriptar los datos que circulan entre el servidor y el cliente, porque de otro modo viajan en texto plano.

Para tener un certificado digital se necesita tener una clave pública y una privada. Primero que todo la clave privada estará en el servidor web. Luego hay que generar una solicitud de firma de certificado con todos los datos de la organización y paso siguiente se le agregará la clave pública, pero se firmará con la clave privada.

Es posible utilizar un certificado autofirmado, pero para más seguridad la solicitud de firma de certificado debe ir a una Autoridad de Certificados. Ésta devolverá un certificado que será utilizado por el servidor web ahora sí brindando seguridad.

VPN

En el diagrama, marcado con una línea verde.

Esta red conecta las sucursales con la sede central utilizando una red pública, pero con seguridad ya que hay autenticación de usuarios y cifrado de datos.

Suposiciones

- Como se cuenta con telefonía tradicional aparte de la telefonía IP, supuse que no hará falta que se pueda utilizar telefonía IP para comunicarse con la tradicional. Caso contrario se necesitaría un dispositivo aparte (gateway).
- En las redes internas como se supone que como máximo habrá 150 clientes a la vez la red 10.x.2.0/24 alcanza para ellos.