Trabajo Práctico de
Integración de conocimientos

Interconexión de sistema de estaciones meteorológicas.

Bruno Crisafulli

Universidad Nacional de Luján
Lic. en Sistemas de Información
Administración y Gestión de Redes

Trabajo Práctico Integrador.

Interconexión de sistema de estaciones meteorológicas.

El trabajo final del curso consiste en demostrar habilidades para diseñar, instalar, configurar y administrar una solución de conectividad, equipamiento y servicios aplicada al caso de estudio planteado en clase.

Su tarea será definir:

1. La topología lógica para todas las redes de la organización.

2. El esquema de direccionamiento IP.

3. Los dispositivos físicos requeridos para la interconectividad solicitada.

4. Los enlaces necesarios para la conectividad a Internet y la conectividad con las distintas locaciones, indicando los requerimientos de nivel de servicio (SLAs) de contratación para cada enlace.

5. Los servicios requeridos con sus respectivas implementaciones de software para cada uno de los roles, por ejemplo: Servidor Web, DNS, etc. Brinde al menos una implementación alternativa para cada uno y justifique su elección.

6. Las configuraciones particulares necesarias para la implementación de una central telefónica VoIP para las comunicaciones con locaciones remotas, tales como: Características de QoS, configuración de cortafuegos y otras opciones de seguridad.

7. La configuración de las herramientas de monitoreo manual y automatizado de servicios, indicando qué aspectos de la gestión de red se deberían monitorizar (fallas, contabilidad, etc.). En función de ello, señale qué elementos de la red selecciona para monitorizar, qué parámetros de éstos, y defina acciones mínimas para determinados eventos que desea controlar. Por ejemplo, notificación al administrador ante umbrales de carga superados en el servidor de bases de datos, etc.

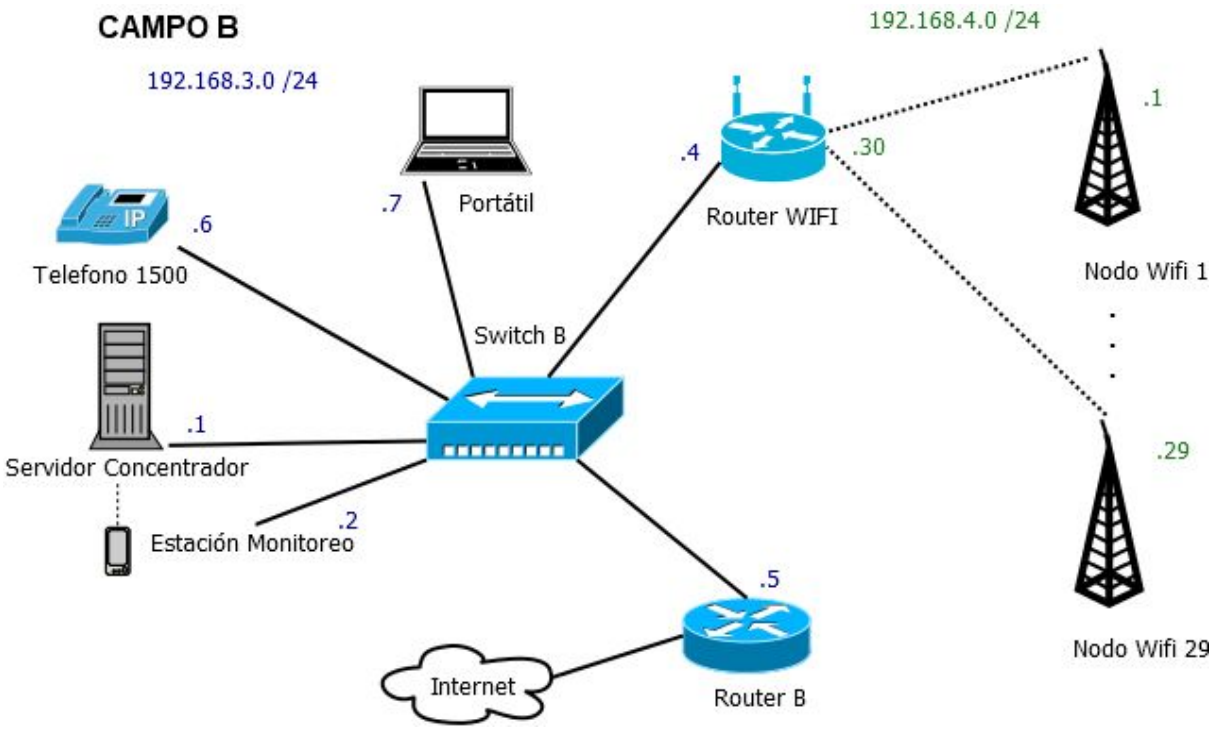
8. Las configuraciones necesarias para garantizar la prestación de los servicios mencionados, incluyendo la regulación de las tasas de transferencia por servicio y prioridades utilizando jerarquías basadas en clases de tráfico.

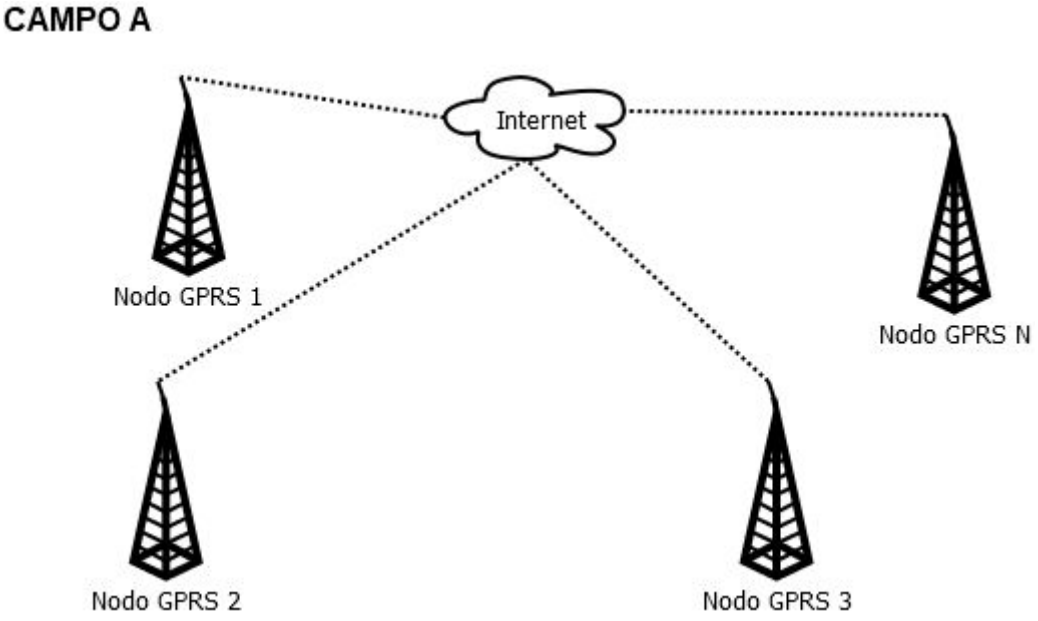
9. Las herramientas de protección de confidencialidad e integridad del tráfico de red y la gestión de las mismas, teniendo en cuenta política de cortafuegos, separación de redes en capa 2 y capa 3, seguridad en acceso remoto y gestión de certificados. Además, indique qué alternativa de seguridad debería considerarse en el servidor Web, en el Servidor de recolección principal y en el nodo Master del Cluster, en función de los requerimientos de la organización.

10. Los mecanismos para garantizar la disponibilidad y tolerancia a fallas de los servicios, tales como: suministro eléctrico, conectividad, refrigeración, entre otras.

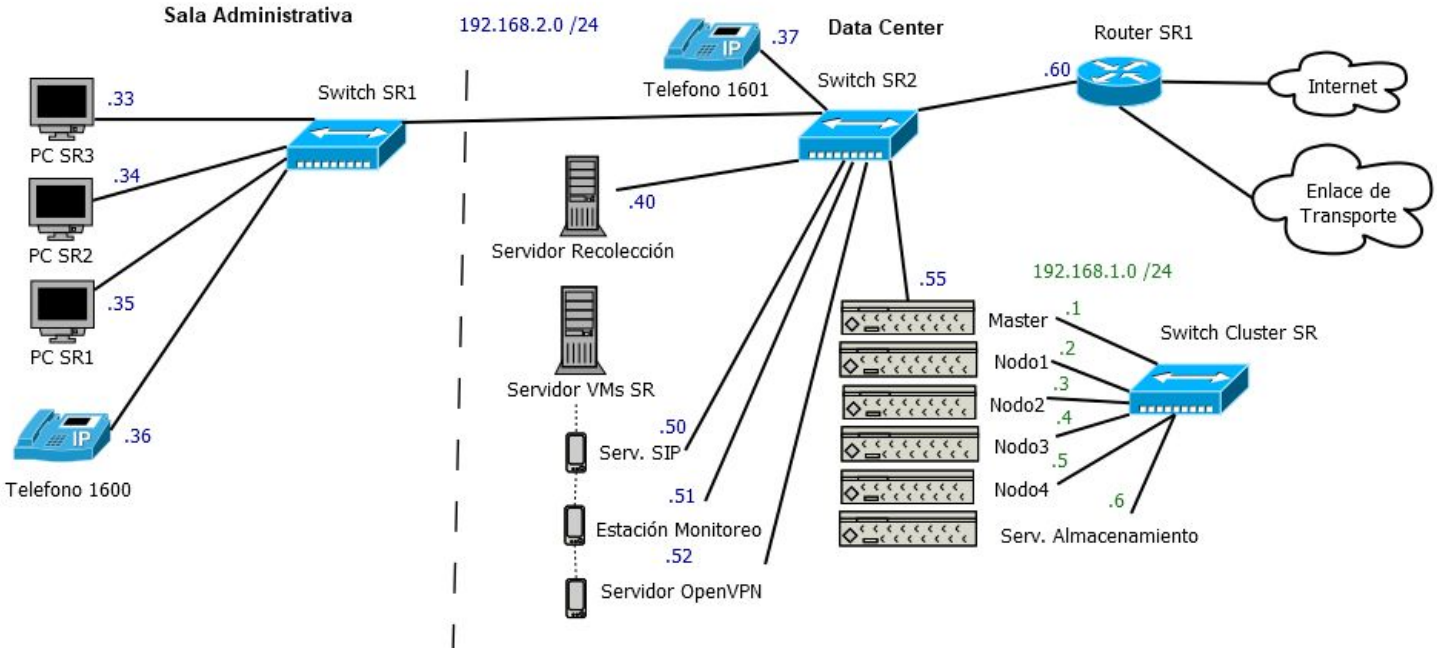
11. Indique y justifique cualquier otra configuración y/o suposiciones realizadas (o restricciones impuestas).

Topología

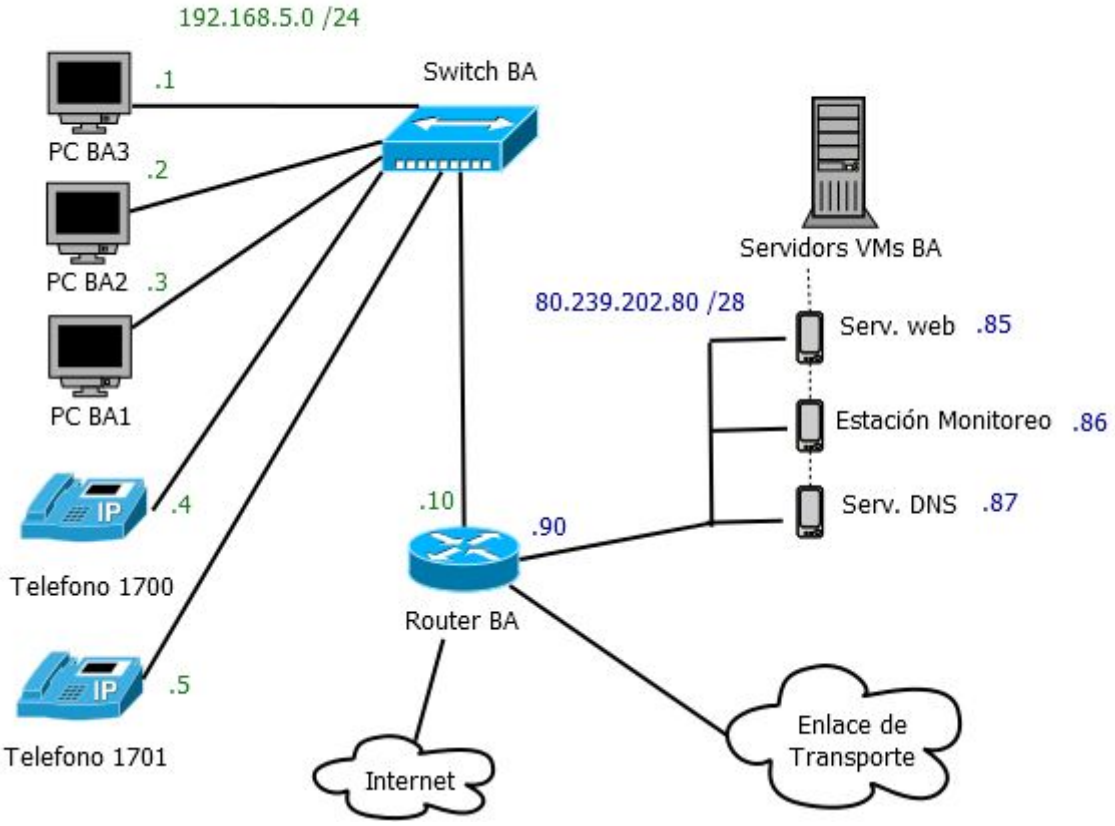

CAMPO B
192.168.3.0 /24
192.168.4.0 /24
.7
Portátil
.4
.30
.1
Router WIFI
Nodo Wifi 1
IP
.6
Telefono 1500
Switch B
.1
Servidor Concentrador
.29
.2
Estación Monitoreo
.5
Internet
Router B
Nodo Wifi 29


CAMPO A
Internet
Nodo GPRS 1
Nodo GPRS N
Nodo GPRS 2
Nodo GPRS 3

ESTACIÓN CENTRAL: SANTA ROSA



ESTACIÓN AMD. REMOTA: BUENOS AIRES



Direccionamiento - Capa de red

Redes

Red	Dirección de red	Mask	Dir. de Host disponibles	Dir. Utilizadas
Nodos Wifi (B)	192.168.4.0	/24	254	5
Estación Concentradora (B)	192.168.3.0	/24	254	5
Nodos GPRS (A) *				
Estación Central (SR)	192.168.2.0	/24	254	11
Cluster (SR)	192.168.1.0	/24	254	6
Estación Adm. Remota Red Administrativa (BA)	192.168.5.0	/24	254	6
Estación Adm. Remota Red Datacenter (BA)	80.239.202.80	/28	14	4

*Dependerá de las direcciones asignadas por el ISP que provea el servicio.

Tablas de Rutas

Nodos Wifi - Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.4.0	/24	wlan0	*	Red local
default		wlan0	192.168.4.30	Router Wifi

Router WIFI - Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.4.0	/24	wlan0	*	Red local
192.168.3.0	/24	eth0	*	Red local

Notese que no posee *default*, ya que las antenas solo necesitan comunicarse normalmente con el servidor concentrador y de monitoreo o a lo sumo con la portátil.

Teléfono - Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.3.0	/24	eth0	*	red local
default		eth0	192.168.3.5	Router B

Servidor Concentrador y de monitoreo y Portátil- Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.3.0	/24	eth0	*	red local
192.168.4.0	/24	eth0	192.168.3.4	Comunicación con Nodos wifi
default		eth0	192.168.3.5	Router B

Router B - Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.3.0	/24	eth0	*	red local
192.168.4.0	/24	eth0	192.168.3.4	Comunicación con Nodos wifi
192.168.2.0	/24	tun1	*	Túnel OpenVPN con Santa Rosa
default		satelital	x.x.x.x	ISP - Conexión a Internet

Teléfonos - Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.2.0	/24	eth0	*	red local

PCs, Servidor de Recolección y Máquinas Virtuales - Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.2.0	/24	eth0	*	red local
default		eth0	192.168.2.60	Router SR1

Master - Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.2.0	/24	eth0	*	red local
192.168.1.0	/24	eth1	*	Red local Cluster
default		eth0	192.168.2.60	Router SR1

Nodos y Serv. Almacenamiento del Cluster - Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.1.0	/24	eth0	*	red local

Router SR1 - Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.2.0	/24	eth0	*	red local privada Santa Rosa
192.168.3.0	/24	tun1	*	Túnel OpenVPN con campo B
28.239.202.80	/28	tun2	*	Túnel OpenVPN con Buenos Aires sobre el Enlace contratado
x.x.x.x	x	eth1	x.x.x.x	red del Enlace contratado
default		eth2	y.y.y.y	ISP - Conexión a Internet

Teléfonos y PCs - Buenos Aires

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.5.0	/24	eth0	*	red local
default		eth0	192.168.5.10	Router BA

Máquinas Virtuales - Buenos Aires

Destino	Máscara	Interfaz	Gateway	Descripción
80.239.202.80	/28	eth0	*	red local
default		eth0	80.239.202.80	Router BA

Router BA - Buenos Aires

Destino	Máscara	Interfaz	Gateway	Descripción
192.168.5.0	/24	eth0	*	red local privada
80.239.202.80	/28	eth1	*	red local
192.168.3.0	/24	tun1	*	Túnel OpenVPN con Santa rosa sobre el enlace contratado
x.x.x.x	x	eth2	x.x.x.x	red del Enlace contratado
default		eth3	y.y.y.y	ISP - Conexión a Internet

Dispositivos Físicos requeridos

A continuación se muestran algunos dispositivos de recomendación y referencia necesarios para implementar la conectividad deseada:

Campo A

Comunicador Gprs 3g - Gs 2060

Ganancia de Antena: 2dB
Temperatura de operación: 5º - 40º
Precio Unidad: $3300 ARS
https://articulo.mercadolibre.com.ar/MLA-674516409-comunicador-gprs-3g-gs-2060-dsc-_JM

Campo B

Antenas WIFI de largo alcance

Dependiendo de si hay obstrucciones menores tales como arboledas, utilizar un rango de frecuencia más bajo tiene mejor rendimiento:

900mHz NLOS Wireless Bridge System

Soporte POE.
802.11N
Frecuencia de Operación: 902-928 MHz
Throughtput en condiciones ideales: 150 Mbps
Precio por par: $500 USD
http://www.radiolabs.com/products/wireless/900-mhz-wireless-bridge-link.php

Router Wifi Cisco SRP521W
802.11N / G
Access Control List (ACL) support
Stateful Packet Inspection (SPI)
Syslog support
DHCP server
Precio unitario: $100 USD

Switch Cisco Sg110-16
16 puertos 10/100/1000Base-T + 2 puertos SFP
Apto para Rack
802.3af PoE
Temperatura de Operación: de 0º a 40º C
Precio unitario: $3400 ARS

Router Linksys LRT224
OpenVPN Server Support
Integrated Firewall
802.1q VLAN
Puertos: un 10/100/1000 RJ45 WAN, un 10/100/1000 RJ45 WAN/DMZ y cuatro 10/100/1000 RJ45 LAN
Precio unitario $260 USD

Santa Rosa

3 Switch Cisco Sg110-16 anteriormente mencionado.
1 router Linksys LRT224 anteriormente mencionado.

Buenos Aires

1 Switch Cisco Sg110-16 anteriormente mencionado.
1 router Linksys LRT224 anteriormente mencionado.

Enlaces - Acuerdos a Nivel de Servicio (SLAs)

A continuación se detallarán los SLAs que deben cumplis los enlaces contratados:

Campo B

Se deberá contratar un enlace satelital a internet, cuyos requisitos son:

- Tasa de transferencia de subida mínima de 4 Mbps.
- Tasa de transferencia de bajada mínima de 2 Mbps.
- Disponibilidad mínima mensual de 70%.
- Tiempo mínimo entre fallas de 30 hs.
- Tiempo máximo de restauración de servicio de 24Hs.
- Delay máximo de 800 ms al servidor DNS de google ip 8.8.8.8 .
  y un Jitter máximo de 200 ms
- Perdida de paquetes máxima mensual de 12%.

Campo A

Se deberá contratar múltiples enlaces GPRS a un mismo proveedor. Las pruebas se realizarán para cada antena y el promedio entre todas para cada parámetro deberá corresponderse a:

- Tasa de transferencia de subida mínima de 1 Mbps.
- Tasa de transferencia de bajada mínima de 1 Mbps.
- Disponibilidad mínima mensual de 95%.
- Tiempo mínimo entre fallas de 24 hs.
- Tiempo máximo de restauración de servicio de 18Hs.
- Delay máximo de 500 ms al servidor DNS de google ip 8.8.8.8 y
  un jitter máximo de 100 ms.
- Perdida de paquetes máxima mensual de 5%.

Santa Rosa

Se deberá contratar un enlace a internet de fibra óptica cuyos requisitos son:

- Tasa de transferencia de subida mínima de 10 Mbps.
- Tasa de transferencia de bajada mínima de 10 Mbps.
- Disponibilidad mínima mensual de 98%.
- Tiempo mínimo entre fallas de 18 Hs.
- Tiempo máximo de restauración de servicio de 10Hs.
- Delay máximo de 500 ms al servidor DNS de google ip 8.8.8.8 y
  un jitter máximo de 100 ms.
- Perdida de paquetes máxima mensual de 2%.

Buenos Aires
Se deberá contratar un enlace a internet de fibra óptica cuyos requisitos son:

- Tasa de transferencia de subida mínima de 30 Mbps.
- Tasa de transferencia de bajada mínima de 15 Mbps.
- Disponibilidad mínima mensual de 99%.
- Tiempo mínimo entre fallas de 8 hs.
- Tiempo máximo de restauración de servicio de 4Hs.
- Delay máximo de 200 ms al servidor DNS de google ip 8.8.8.8 y
un jitter máximo de 50 ms.
- Perdida de paquetes máxima mensual de 0.5%.

Enlace dedicado Santa Rosa - Buenos Aires
Deberá contratarse un servicio de enlace de transporte dedicado entre la estación central de Santa Rosa y la Estación de adm. remota de Buenos Aires que deberá cumplir con los siguientes requisitos:

- Throughput mínimo simétrico de 10Mbps
- Disponibilidad mínima mensual de 99%.
- Tiempo mínimo entre fallas de 14 hs.
- Tiempo máximo de restauración de servicio de 6Hs.
- Delay máximo de 200 ms entre ambos extremos y
un jitter máximo de 50 ms.
- Perdida de paquetes máxima mensual de 0.1%.

Para monitorear el cumplimiento de los requisitos se utilizarán las herramientas *iperf* y *ping.*

Servicios a implementar

A continuación se detallarán los servicios brindados por el sistema y el software utilizado para implementarlos.

Sistemas Operativos

Se ha tomado la decisión de utilizar en todos los dispositivos (exceptuando los casos en que estos traen software específico del fabricante como los switches y routers) software libre, por lo que los host poseerán como Sistema Operativo a **Ubuntu,** las máquinas virtuales en su totalidad **Debian** y para el cluster dada su arquitectura se usará **Debian-Beowulf.**

Virtualización

Habrá dos servidores de máquinas virtuales para alojar distintos servicios como está especificado en el diagrama: Uno en Santa Rosa y otro en Buenos Aires. El software recomendado para implementar la virtualización en el dispositivo físico es **XenServer 4.8** o como alternativa, KVM. Ambas son elegidas por ser Software libre ampliamente utilizado comercialmente.

Servicio de consulta Web

Se brindará un servicio de consulta al público de los datos meteorológicos a través de los protocolos HTTP 2.0 y HTTPS. Para esto se cuenta con un servidor web alojado en la Estación de Buenos Aires cuya IP será 80.239.202.85. El software recomendado para su implementación es **Apache 2.4** o como alternativa Nginx, los cuales ambos se caracterizan por ser Software Libre ampliamente utilizado comercialmente de manera que está comprobado su buen funcionamiento.
Particularmente para el caso de HTTPS es necesario obtener un certificado de tipo X.509 de una autoridad certificadora, pero su adquisición y configuración exceden el alcance de este documento.

Servicio de resolución de nombres

El sistema contará con un servidor que responde consultas de resolución de nombres o DNS, ubicado en la Estación de Buenos Aires cuya IP será 80.239.202.87. El software recomendado para su implementación es **BIND 9.12** por ser el más utilizado en Internet y ser software libre, como alternativa se puede elegir Unbound, de similares características.

Trabajo de Monitoreo y Control

Para el trabajo de monitoreo y control sobre todos los dispositivos de la red se utilizará el protocolo **SNMP v3**, a través de la herramienta **Nagios 4** (como alternativa puede utilizarse Munin 2). Este software de monitoreo estará instalado en las tres máquinas virtuales destinadas a dicho fin, una en la estación B, una en la estación de Buenos Aires y la principal en Santa Rosa. Cada una abarcará los

dispositivos respectivos de su edificio/área. La estación de Santa Rosa monitoreará además las antenas del campo A; las estaciones B y Buenos Aires darán reportes y alertas a la de Santa Rosa.
La función de que haya una estación de monitoreo en cada edificio, aunque la principal sea la de Santa Rosa, es que se sigan recopilando los datos de monitoreo por más de que se caiga la conectividad entre las áreas. Existe la alternativa de encargar la recopilación “offline” a cada dispositivo monitoreado, pero esto requeriría asegurar que todos implementen RMON y lo soporten.
Es necesario que todos los dispositivos monitoreados posean instalado el servicio **snmpd** y sean configurados para generar alertas asincrónicas específicas para cada equipo (se detallaran más adelante). Puede contemplarse también el uso de la MIB **RMON2** y de las MIB propietarias en dispositivos específicos como en el caso de los router Cisco para extender la capacidad de control sobre estos.

Helpdesk y Sistema de Tickets
El sistema brindará además un sistema de tickets para que los usuarios internos a la organización puedan abrir un ticket en caso de algún problema o falla y que haya un seguimiento de esto. El software recomendado para su implementación es OTRS v6 (Opensource Ticket Request System) que es integrable a la herramienta Nagios anteriormente mencionada.

Servicio de Acceso Remoto Seguro
El sistema brindará un servicio de acceso o login remoto seguro a través de internet a los siguientes dispositivos: El Servidor concentrador y la estación de monitoreo en el campo B; El servidor Master en Santa Rosa (desde donde a su vez puede interactuar con los demás dispositivos del edificio); Las máquinas virtuales del servidor de Buenos Aires.
Para esto se utilizará el protocolo **SSH** (Secure Shell) y el software recomendado para implementarlo es **OpenSSH v7.6**. Esta herramienta sigue un formato Cliente-Servidor, por lo que se requiere que en los dispositivos mencionados se tenga instalada y en escucha la versión servidor de la herramienta.
Además también es necesario que los dispositivos posean claves públicas correspondientes a los usuarios autorizados para el login remoto en el mismo, esto quedará a cargo del Administrador de Red.

Almacenamiento de Datos

El sistema contará con Bases de Datos Locales para el Servidor Concentrador (Campo B), el Servidor de Recolección (Santa Rosa), el Servidor de Almacenamiento (Santa Rosa) y el Servidor Web (Buenos Aires). Estas serán implementadas de manera relacional y se recomienda el uso del motor **PostgreSQL**, debido a que es software libre con muchas utilidades y herramientas además de gran cantidad de documentación, como alternativa, se sugiere MySQL por ser de características similares.

Comunicación entre edificios segura

El sistema se valdrá del uso de túneles VPN para lograr una comunicación segura a través de los medios de terceros que comunican los edificios. Por lo tanto habrá dos túneles VPN, uno entre Santa Rosa y Buenos Aires, a través del enlace dedicado, y otro entre Santa Rosa y el Campo B, a través de internet. Para su implementación se utilizará **OpenVPN 2.4** soportado por los Router Linksys especificados previamente. Para su configuración será necesario crear, almacenar y mantener certificados de autenticidad que serán autofirmados en el Servidor openVPN alojado en Santa Rosa para dicho fin, cuya IP es 192.168.2.52. Los primeros certificados que se creen deberán ser transferidos entre los edificios de manera segura sin contar con los túneles VPN, lo que quedará a cargo del administrador de red. Los certificados tendrán fecha de vencimiento y serán renovados cada 30 días (plazo modificable).

Servicio de telefonía

El sistema brindará también, servicio de voz sobre IP, valiéndose de los teléfonos IP de los edificios, la red, el servidor de registro (demarcado como *servidor SIP* en el diagrama) y del protocolo de señalización SIP/SDP. El software recomendado para implementar el servidor SIP es **Asterisk**, o como alternativa Kamailio 4. La codificación de la voz a binario se hará con el codec **Opus** (RFC 6716) o como alternativa G.722, pero siempre de manera homogénea dentro de la organización para evitar el transcoding y de esta forma permitir que los teléfonos puedan realizar el streaming de audio de forma más directa.

Tabla de registro de los dispositivos
Los teléfonos se valdrán de un mnemónico para referirse al SIP server para poder registrarse. Dicho mnemónico queda a definirse y será resuelto luego a una IP efectiva a través de DNS (servidor de la organización).

Host	Interno	Register Serv.	Descripción
192.168.3.6	1500	192.168.2.51	Teléfono Campo B
192.168.2.36	1600	192.168.2.51	Teléfonos Santa Rosa
192.168.2.37	1601	192.168.2.51	
192.168.5.4	1700	192.168.2.51	Teléfonos Buenos Aires
192.168.5.5	1701	192.168.2.51	

Configuración
El servidor Asterisk requerirá ser configurado para que brinde el correcto funcionamiento que se espera del servicio. Sus archivos de configuración más importantes son *Sip.conf* y *Extensions.conf*.

Quality of Service (QoS)
El sistema aplicará técnicas de control de flujo en los router de borde que permitirán ofrecer mínimas características de QoS para VoIP (que se detallan más adelante) pero los factores más importantes que son la Latencia, el Jitter y la pérdida de paquetes, están sujetos a los SLAs establecidos para cada enlace, por lo que, por ejemplo, entre los edificios de Santa Rosa y Buenos Aires el sistema asegura buena calidad en la comunicación pero con el Campo B en cambio, por ser un enlace satelital, la comunicación será mala.

No se ha dado mayor relevancia al servicio de telefonía porque se entiende que el objetivo del sistema se centra en la recolección, procesado y distribución de datos meteorológicos.

Gestión de la Red

La gestión de la red se verá plasmada en su mayoría en la estación de monitoreo de Santa Rosa, donde se recopilarán los datos de la actividad de la red y realizarán los ajustes dinámicamente para mejorar las prestaciones, además de llevar registro de el uso de los recursos de red por usuarios o tipos de usuarios.

La siguiente tabla señala los parámetros básicos a monitorear de los que se llevará registro y, si se les configurará una alerta automática, (*Trap*) se indica el umbral y la acción a tomar:

Dispositivo	Recurso	Umbral	Acción
Todos a los que aplique	Conectividad	No disponible	Notificar al Adm.
	tiempo de respuesta		
	packets in		
	packets out		
	up time		
Servidores	Espacio disco utilizado	80% de espacio total	Notificar al Administrador
	Temperatura Cpu	80% de la máxima operacional	Notificar al Adm.
		95% de la máxima operacional	Apagar el servidor durante 15 min.
	Uso de Disco		
	Uso de Cpu		
Aires Acondicionados	Estado	no disponible	Notificar al Administrador
	Temperatura de Operación		
Termostatos de ambiente	Temperatura	mayor a 30°C	Notificar al Administrador

Switches	Congestión en las colas		
	Mac de dispositivos		
Routers de Borde	Tasa de Paquetes por interfaz		
	Perdida de Paquetes		
	Conectividad del enlace contratado	no disponible	Notificar al Adm.
Web Server	Cantidad de Conexiones	15 Conexiones desde misma IP	Bloquear IP y Log del alerta

Clasificación y priorización de tráfico

Se hará una clasificación del tráfico en los router de borde de manera que se priorice la transferencia de datos meteorológicos y de monitoreo además de asegurar el throughput necesario para el servicio de VoIP. Para esto se utilizará la herramienta TC (Traffic Control) y se empleará la técnica de Token Bucket Jerárquico. Las políticas de encolado y priorización serán las siguientes:

Campo B

Clase	Filtro	Característica
VoIP	IP destino u origen 192.168.3.6 (Telefono 1500)	Tasa de Transferencia asegurada de 1 Mbps Encolado de Alta prioridad
Datos meteorológicos y de monitoreo	UDP Puerto destino 1410 o UDP Puerto destino 161 o UDP Puerto destino 162	Tasa de transferencia asegurada de 1 Mbps Encolado de prioridad media
Default	*	Encolado de baja prioridad y prioridad de dropeo

Santa Rosa

Clase	Filtro	Característica
VoIP	IP destino u origen 192.168.2.36 (Telefono 1600) o IP destino u origen 192.168.2.37 (Telefono 1601)	Tasa de Transferencia asegurada de 2 Mbps Encolado de Alta prioridad
Datos meteorológicos y de monitoreo	UDP Puerto destino 1410 o UDP Puerto destino 161 o UDP Puerto destino 162	Tasa de transferencia asegurada de 1 Mbps Encolado de prioridad media
Default	*	Encolado de baja prioridad y prioridad de dropeo

Buenos Aires

Clase	Filtro	Característica
VoIP	IP destino u origen 192.168.5.4 (Telefono 1700) o IP destino u origen 192.168.5.5 (Telefono 1701)	Tasa de Transferencia asegurada de 1 Mbps Encolado de Alta prioridad
Datos meteorológicos y de monitoreo	UDP Puerto destino 1410 o UDP Puerto destino 161 o UDP Puerto destino 162	Tasa de transferencia asegurada de 1 Mbps Encolado de prioridad media
Default	*	Encolado de baja prioridad y prioridad de dropeo

Seguridad

Firewall

La política de seguridad que se eligió para el sistema es de lineamiento prudente, por lo que los firewall droppearán todo aquello que no esté explícitamente definido para pasar. Esto se implementará en los router de borde de los edificios, utilizando la herramienta Netfiler. Las reglas de firewall quedarían inicialmente como sigue:

Router B (Campo B)

Ip origen	Ip Dest.	Puerto Origen	Puerto Destino	Protoc-olo	Acción	Descrip.
192.168.3.6	162.168.2.50	*	5060	TCP / UDP	ACCEPT	Telefono - Sip Serv
162.168.2.50	192.168.3.6	5060	*	TCP / UDP	ACCEPT	Sip Serv - Teléfono
IP Router B **	IP Router SR **	*	1194	UDP	ACCEPT	VPN Campo B - Santa Rosa
IP Router SR **	IP Router B **	*	1194	UDP	ACCEPT	VPN Santa Rosa - Campo B
192.168.3.1	192.168.2.40	*	1410	UDP	ACCEPT	Serv Concentrador - Serv Recolec.
192.168.2.40	192.168.3.1	1410	*	UDP	ACCEPT	Serv Recolec. - Serv Concentrador
192.168.3.2	192.168.2.51	*	161	UDP	ACCEPT	Monitoreo Campo B - Santa Rosa
192.168.2.51	192.168.3.2	*	161	UDP	ACCEPT	Monitoreo Santa Rosa - Campo B
192.168.3.6	192.168.2.0 /24	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Santa Rosa
192.168.2.0 /24	192.168.3.6	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Santa Rosa

192.168.3.6	192.168.5.0 /24	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Buenos Aires
192.168.5.0 /24	192.168.3.6	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Buenos Aires
192.168.3.1	*	22	*	TCP	ACCEPT	SSH a Serv. Concentrador
*	192.168.3.1	*	22	TCP	ACCEPT	SSH a Serv. Concentrador
192.168.3.2	*	22	*	TCP	ACCEPT	SSH a Estación Monitoreo
*	192.168.3.2	*	22	TCP	ACCEPT	SSH a Estación Monitoreo

** IPs dadas por el ISP

*** Requiere inspección profunda

Router SR - Santa Rosa

Ip origen	**Ip Dest.**	**Puerto Origen**	**Puerto Destino**	**Protoc-olo**	**Acción**	**Descrip.**
192.168.2.50	192.168.3.6	5060	*	TCP / UDP	ACCEPT	Sip Serv - Teléfono Campo B
192.168.3.6	192.168.2.50	*	5060	TCP / UDP	ACCEPT	Teléfono Campo B - Sip Serv
192.168.5.4 / .5	192.168.2.50	*	5060	TCP / UDP	ACCEPT	Teléfonos BA - Sip Serv
192.168.2.50	192.168.2.37	5060	*	TCP / UDP	ACCEPT	Sip Serv - Teléfonos BA
IP Router B **	IP Router SR **	*	1194	UDP	ACCEPT	VPN Campo B - Santa Rosa
IP Router SR **	IP Router B **	*	1194	UDP	ACCEPT	VPN Santa Rosa - Campo B
IP Router BA **	IP Router SR **	*	1194	UDP	ACCEPT	VPN Buenos Aires - Santa Rosa

IP Router SR **	IP Router BA **	*	1194	UDP	ACCEPT	VPN Santa Rosa - Buenos Aires
192.168.3.1	192.168.2.40	*	1410	UDP	ACCEPT	Serv Concentrador - Serv Recolec.
192.168.2.40	192.168.3.1	1410	*	UDP	ACCEPT	Serv Recolec. - Serv Concentrador
192.168.2.55	80.239.202.85	*	1410	UDP	ACCEPT	Master - Serv. Web
80.239.202.85	192.168.2.55	1410	*	UDP	ACCEPT	Serv. Web - Master
IPs Campo A **	192.168.2.40	*	1410	UDP	ACCEPT	Campo A - Serv Recolección
192.168.2.40	IPs Campo A **	1410	*	UDP	ACCEPT	Serv Recolección - Campo A
IPs Campo A **	192.168.2.51	*	162	UDP	ACCEPT	Traps Campo A - Estación Monitoreo
192.168.2.51	IPs Campo A **	*	161	UDP	ACCEPT	Estación Monitoreo - Campo A
IPs Campo A **	192.168.2.51	*	161	UDP	ACCEPT	Campo A - Estación Monitoreo
192.168.3.2	192.168.2.51	*	161	UDP	ACCEPT	Monitoreo Campo B - Santa Rosa
192.168.2.51	192.168.3.2	161	*	UDP	ACCEPT	Monitoreo Santa Rosa - Campo B
80.239.202.86	192.168.2.51	*	161	UDP	ACCEPT	Monitoreo BsAs - Santa Rosa
192.168.2.51	80.239.202.86	161	*	UDP	ACCEPT	Monitoreo Santa Rosa - BsAs
192.168.3.6	192.168.2.36	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Campo B
192.168.2.36	192.168.3.6	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Campo B

192.168.3.6	192.168.2.37	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Campo B
192.168.2.37	192.168.3.6	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Campo B
192.168.2.36	192.168.5.0 /24	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Buenos Aires
192.168.5.0 /24	192.168.2.36	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Buenos Aires
192.168.2.37	192.168.5.0 /24	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Buenos Aires
192.168.5.0 /24	192.168.2.37	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Buenos Aires
192.168.2.55	*	22	*	TCP	ACCEPT	SSH a Master
*	192.168.3.55	*	22	TCP	ACCEPT	SSH a Master
192.168.2.33 / .34 / .35	*	*	25/53/80/ 443/110/ 143	TCP / UDP	ACCEPT	Salida a internet de hosts
*	192.168.2.33 / .34 / .35	25/53/80/ 443/110 /143	*	TCP / UDP	ACCEPT	Salida a internet de hosts

** IPs dadas por el ISP

*** Requiere inspección profunda

Router BA - Buenos Aires

Ip origen	Ip Dest.	Puerto Origen	Puerto Destino	Protoc-olo	Acción	Descrip.
192.168.5.4 / .5	192.168.2.50	*	5060	TCP / UDP	ACCEPT	Teléfonos BA - Sip Serv
192.168.2.50	192.168.2.37	5060	*	TCP / UDP	ACCEPT	Sip Serv - Teléfonos BA
IP Router BA **	IP Router SR **	*	1194	UDP	ACCEPT	VPN Buenos Aires - Santa Rosa
IP Router SR **	IP Router BA **	*	1194	UDP	ACCEPT	VPN Santa Rosa - Buenos Aires
192.168.2.55	80.239.202.85	*	140	UDP	ACCEPT	Master - Serv. Web
80.239.202.85	192.168.2.55	*	1410	UDP	ACCEPT	Serv. Web - Master
80.239.202.86	192.168.2.51	162	*	UDP	ACCEPT	Monitoreo BsAs - Santa Rosa
192.168.2.51	80.239.202.86	*	161	UDP	ACCEPT	Monitoreo Santa Rosa - BsAs
80.239.202.85	*	80 / 443 / 25	*	TCP	ACCEPT	Servicio web
*	80.239.202.85	*	80 / 443 / 25	TCP	ACCEPT	Servicio web
80.239.202.87	*	53	*	UDP / TCP	ACCEPT	Servicio DNS
*	80.239.202.87	*	53	UDP / TCP	ACCEPT	Servicio DNS
192.168.3.6	192.168.5.4 / .5	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Campo B
192.168.5.4 / .5	192.168.3.6	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Campo B

192.168.2.36 / .37	192.168.5.4 / .5	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Santa Rosa
192.168.5.4 / .5	192.168.2.36 / .37	*	*	UDP / RTP / RTCP ***	ACCEPT	Comunicación telefónica con Santa Rosa
80.239.202.85 / .86 / .87	*	22	*	TCP	ACCEPT	SSH a Servidores
*	80.239.202.85 / .86 / .87	*	22	TCP	ACCEPT	SSH a Servidores
192.168.5.1 / .2 / .3	*	*	53/80/ 443 / 25 / 110 / 143	TCP / UDP	ACCEPT	Salida a internet de hosts
*	192.168.5.1 / .2 / .3	53/80/ 443 / 25 / 110 / 143	*	TCP / UDP	ACCEPT	Salida a internet de hosts

** IPs dadas por el ISP

*** Requiere inspección profunda

Otras consideraciones de Seguridad

El firewall de filtro de paquetes es insuficiente como medida de seguridad, sobretodo en un sistema que brinda servicios al público. Es responsabilidad del Administrador de Red y su equipo de trabajo, velar por la seguridad del sistema y estar alerta a intrusiones y cambios bruscos en el comportamiento del tráfico.

El servidor web y el de DNS deben tener una configuración adecuada y actualizada para ofrecer servicios abiertamente a la internet, previniendose en lo posible a los ataques comunes o conocidos como:

- Denegación de Servicio (DoS)

Específicos del servicio Web:

- Slow Loris Attack
- SQL Injection
- Cross-Site Scripting
- Fuerza Bruta sobre los Controles de Acceso
- Spam

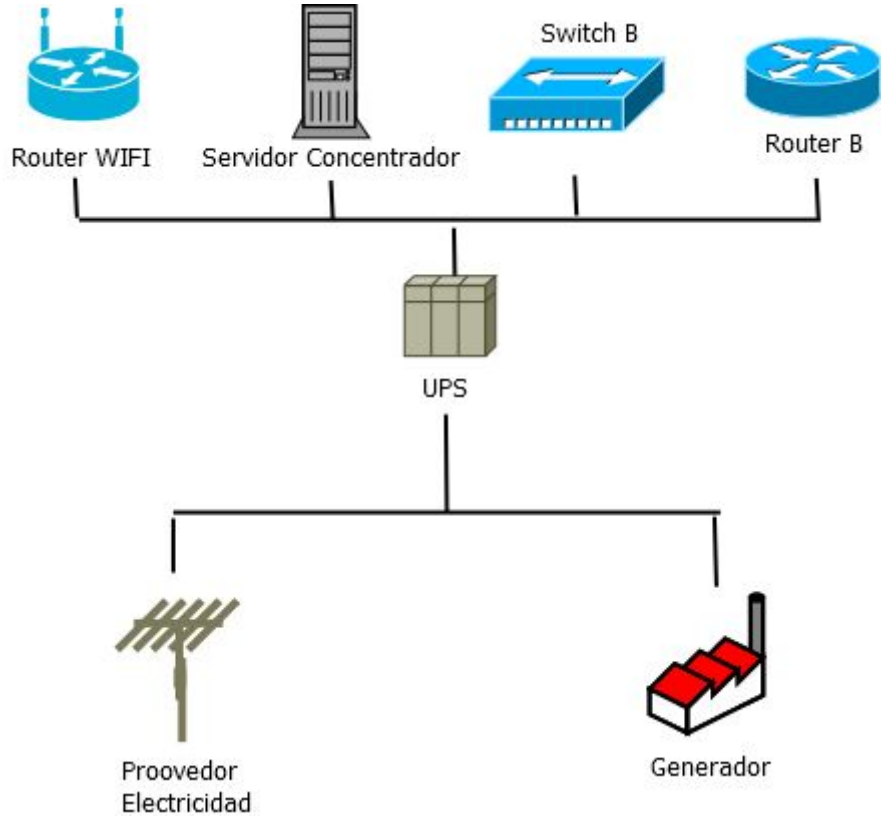
Disponibilidad y Tolerancia a fallas

Para que el sistema pueda asegurar cierta disponibilidad en todos sus servicios es necesario que las salas donde se encuentren los Servidores y equipos de interconexión principales en cada edificio estén adecuadamente acondicionadas.

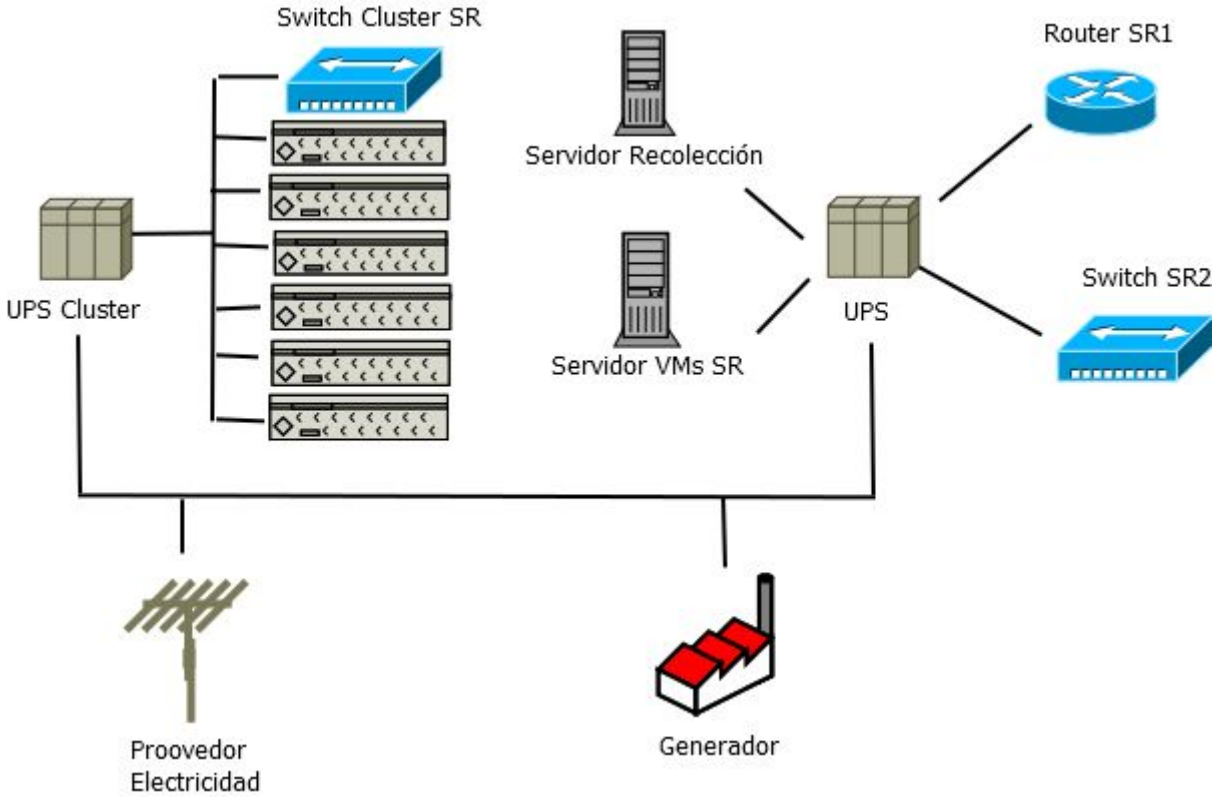
Se requiere que haya dos equipos de aire acondicionado en cada sala de servidores, de manera que se intercalen en su funcionamiento y en el caso de que uno falle el otro puede mantener las condiciones de ambiente hasta la reparación.

Otro factor de gran impacto en la disponibilidad es el suministro eléctrico. Lo ideal sería poder conseguir suministro de dos proveedores, cuyas fuentes y redes de distribución sean distintas, pero es muy difícil o imposible en la Argentina. Por lo tanto se utilizarán generadores a combustible de back up, y UPS para maximizar el tiempo que se mantiene la operatividad cuando haya una caída de energía:

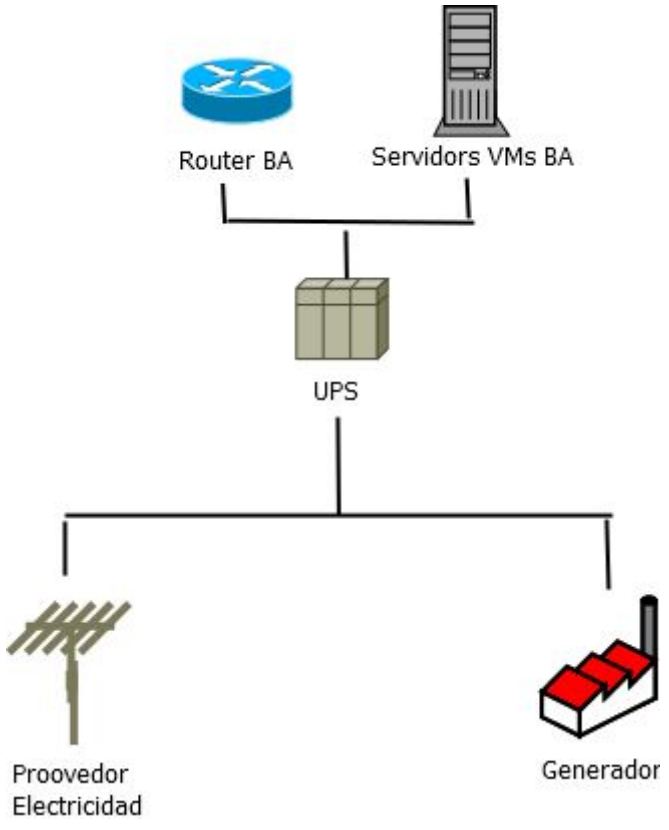
Campo B



Santa Rosa



Buenos Aires



Si se desease aumentar la disponibilidad del servicio web y DNS, existe la posibilidad de contratar un enlace más a internet para el edificio de Buenos Aires, de manera de aportar redundancia en caso de que falle el enlace ya contratado. Esto está soportado por el router utilizado, permitiendo hacer el cambio en caliente o incluso hacer balanceo de carga.

Bibliografía

Oppenheimer Priscilla, “Top-Down Network Design” Third Edition. Cisco Press 2011

RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3418: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)