Interconexión de sistema de estaciones meteorológicas

Administración y Gestión de Redes - 11085
Universidad Nacional de Luján 2017

Juran, Martín Tomás - 143191 - tomasjuran96@gmail.com

Índice 1

Objetivos y alcance 2

Topología de red
- Campo A y Campo B 3
- Estación Central, Santa Rosa 4
- Estación de Administración Remota, CABA 5

Direccionamiento - Capa de red 6
Tablas de rutas 9
Tablas de traducción de direcciones (NAT) 13
Direccionamiento - Capa de enlace 14
Direccionamiento - red privada virtual (VPN) 16
Clasificación y priorización del tráfico 17
Enlaces contratados - Acuerdos de nivel de servicio (SLA) 19

Software y Servicios
- Resumen 21
- Voz sobre IP (VoIP) 22
- Portal Web 22
- Servicio de resolución de nombres (DNS) 22
- Monitoreo y control 23
- Acceso remoto 26
- Seguridad - Red Privada Virtual (VPN) 26
- Seguridad - Firewall 26
- Virtualización 30
- Base de Datos 30

Mecanismos de redundancia y tolerancia a fallos 31

Dispositivos físicos 33

Anexo - Bibliografía 34

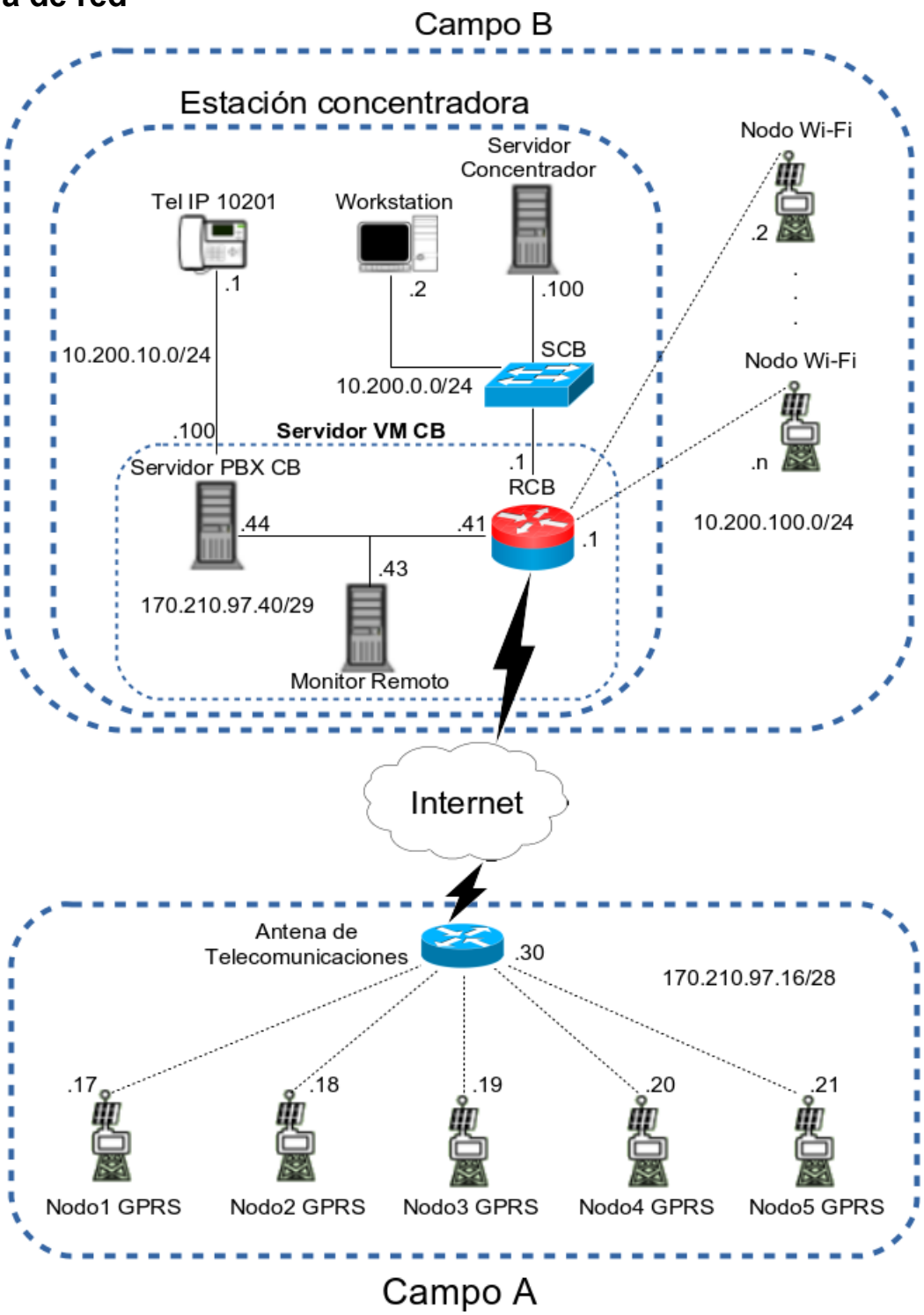
Objetivos y alcance

Este documento propone el diseño de una infraestructura de red para poder recolectar la información de un sistema de sensores distribuidos en la provincia de la Pampa, procesarlos en un datacenter en una estación central en la ciudad de Santa Rosa y ofrecer parte de los datos obtenidos al público en general.

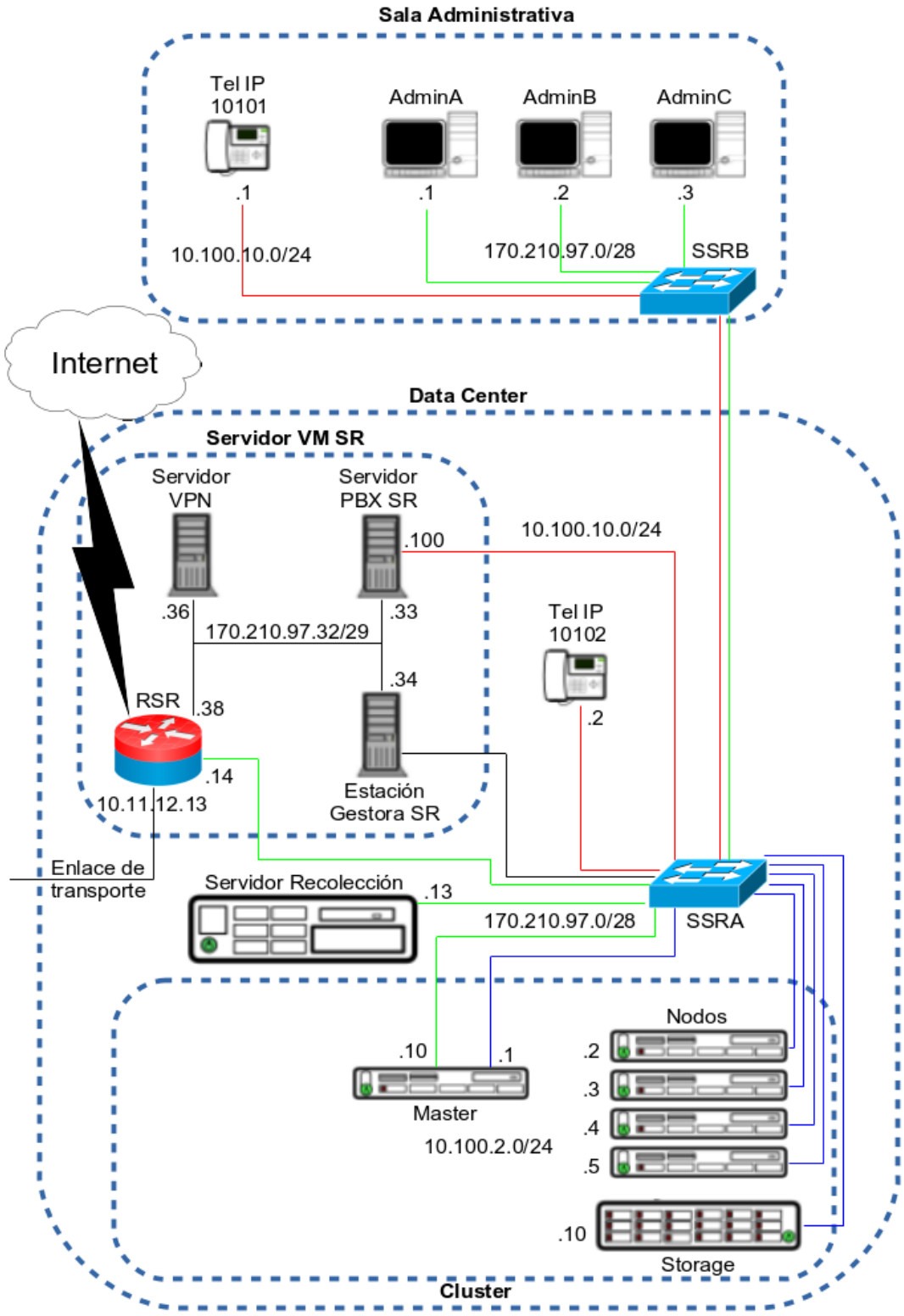
Están definidos en este documento:
- La topología lógica para todas las redes de la organización.
- El esquema de direccionamiento IP.
- Los dispositivos físicos requeridos para la interconectividad propuesta.
- Los enlaces necesarios para la conectividad a Internet y la conectividad con las distintas locaciones, indicando los requerimientos de nivel de servicio (SLAs) de contratación para cada enlace.
- Los servicios requeridos con sus respectivas implementaciones de software para cada uno de los roles, por ejemplo: Servidor Web, DNS; con al menos una implementación alternativa para cada uno.
- 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.
- 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.), qué elementos de la red monitorizar, qué parámetros de éstos y definiendo acciones mínimas para determinados eventos que se desean controlar.
- Las configuraciones necesarias para garantizar la prestación de los servicios mencionados, incluyendo la regulación de las tasas de transferencia por servicio y prioridades utilizando jerarquíasbasadas en clases de tráfico.
- 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.
- Los mecanismos para garantizar la disponibilidad y tolerancia a fallas de los servicios, tales como: suministro eléctrico y refrigeración.

Esta propuesta no contempla la definición del financiamiento, instalación ni pruebas del diseño.

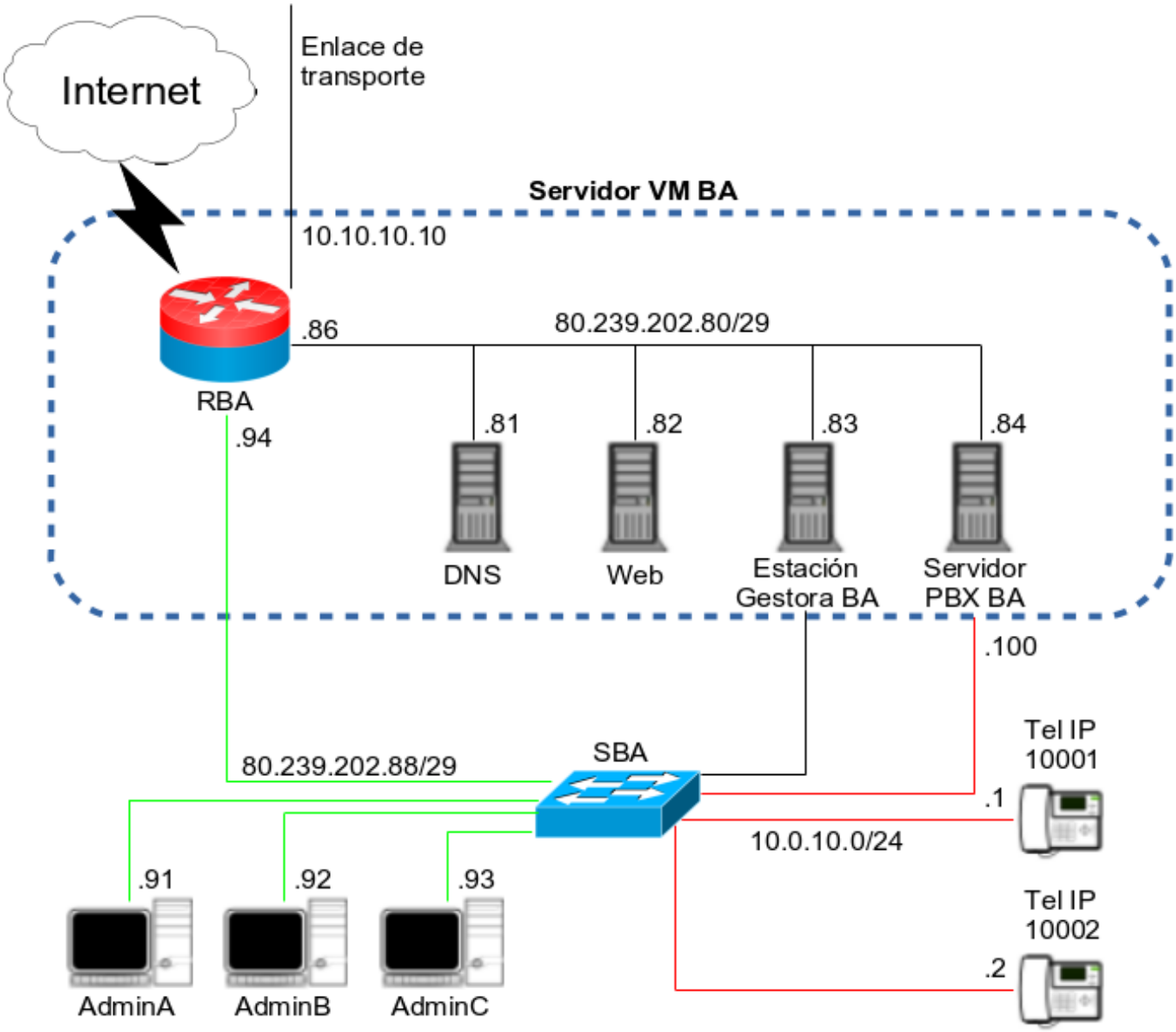
Topología de red



Estación Central, Santa Rosa



Estación de Administración Remota, Ciudad Autónoma de Buenos Aires



Direccionamiento - Capa de red

Las redes de interconexión con los ISP están marcadas con la dirección “X.X.X.X”.

Redes

Descripción	Dirección de red	Máscara	Primer host	Último host	Dir. de host disponibles	Hosts actuales
Nodos GPRS	170.210.97.16	255.255.255.240	.17	.30	14	6
Nodos Wi-Fi	10.200.100.0	255.255.255.0	.1	.254	254	5
Servidor Concentrador	10.200.0.0	255.255.255.0	.1	.254	254	3
Telefonía Campo B	10.200.10.0	255.255.255.0	.1	.254	254	2
Servidor VM Campo B	170.210.97.40	255.255.255.248	.41	.46	6	3
Telefonía Santa Rosa	10.100.10.0	255.255.255.0	.1	.254	254	3
Servidor VM Santa Rosa	170.210.97.32	255.255.255.248	.33	.38	6	4
Administración Santa Rosa	170.210.97.0	255.255.255.240	.1	.14	14	6
Red de cómputos	10.100.2.0	255.255.255.0	.1	.254	254	6
Telefonía Buenos Aires	10.0.10.0	255.255.255.0	.1	.254	254	3
Servidor VM Buenos Aires	80.239.202.80	255.255.255.248	.81	.86	6	5
Administración Buenos Aires	80.239.202.88	255.255.255.248	.89	.94	6	4

Hosts

Host	Dirección	Interfaz
Nodo1_GPRS	170.210.97.17	gi0
Nodo2_GPRS	170.210.97.18	gi0
Nodo3_GPRS	170.210.97.19	gi0
Nodo4_GPRS	170.210.97.20	gi0
Nodo5_GPRS	170.210.97.21	gi0
Antena de Telecomunicaciones	170.210.97.30	gi0
Antena de Telecomunicaciones	X.X.X.X	eth0
Router Campo B	10.200.100.1	wlan0
Router Campo B	10.200.0.1	eth0
Router Campo B	170.210.97.48	eth1
Router Campo B	X.X.X.X	eth2
Nodo1_Wi-Fi	10.200.100.2	wlan0
Nodo2_Wi-Fi	10.200.100.3	wlan0
Nodo3_Wi-Fi	10.200.100.4	wlan0
Nodo4_Wi-Fi	10.200.100.5	wlan0
Servidor Concentrador	10.200.0.100	eth0
Workstation	10.200.0.2	eth0
Teléfono IP 10201	10.200.10.1	eth0
Servidor PBX Campo B	10.200.10.100	eth0
Servidor PBX Campo B	170.210.97.44	eth1
Monitor Remoto	170.210.97.43	eth0
Teléfono IP 10101	10.100.10.1	eth0
Teléfono IP 10102	10.100.10.2	eth0
Servidor PBX Santa Rosa	10.100.10.100	eth0
Servidor PBX Santa Rosa	170.210.97.33	eth1
Estación Gestora Santa Rosa	170.210.97.34	eth0
Servidor VPN	170.210.97.36	eth0
Router Santa Rosa	170.210.97.38	eth1
Router Santa Rosa	10.11.12.13	eth2

Router Santa Rosa	X.X.X.X	eth3
Router Santa Rosa	170.210.97.14	eth0
AdminA Santa Rosa	170.210.97.1	eth0
AdminB Santa Rosa	170.210.97.2	eth0
AdminC Santa Rosa	170.210.97.3	eth0
Servidor Recolección	170.210.97.13	eth0
Servidor Recolección	10.100.1.2	eth1
Servidor de Cómputos Master	170.210.97.10	eth0
Servidor de Cómputos Master	10.100.1.1	eth1
Servidor de Cómputos Master	10.100.2.1	eth2
Nodo de Cómputos 1	10.100.2.2	eth0
Nodo de Cómputos 2	10.100.2.3	eth0
Nodo de Cómputos 3	10.100.2.4	eth0
Nodo de Cómputos 4	10.100.2.5	eth0
Servidor Storage	10.100.2.10	eth0
Teléfono IP 10001	10.0.10.1	eth0
Teléfono IP 10002	10.0.10.2	eth0
Servidor PBX Buenos Aires	10.0.10.100	eth0
Servidor PBX Buenos Aires	80.239.202.84	eth1
Estación Gestora Buenos Aires	80.239.202.83	eth0
Servidor Web	80.239.202.82	eth0
Servidor DNS	80.239.202.81	eth0
Router Buenos Aires	80.239.202.86	eth1
Router Buenos Aires	10.10.10.10	eth2
Router Buenos Aires	X.X.X.X	eth3
Router Buenos Aires	80.239.202.94	eth0
AdminA Buenos Aires	80.239.202.91	eth0
AdminB Buenos Aires	80.239.202.92	eth0
AdminC Buenos Aires	80.239.202.93	eth0

Tablas de rutas

Campo A

Nodos GPRS

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.16	255.255.255.240	gi0	-	Red local
default	-	gi0	170.210.97.30	

Antena de Telecomunicaciones

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.16	255.255.255.240	gi0	-	Red local
X.X.X.X	255.255.255.252	eth0	-	Red entre routers con ISP
default	-	eth0	X.X.X.X	Enlace a ISP

Campo B

Nodos Wi-Fi

Destino	Máscara	Interfaz	Gateway	Descripción
10.200.100.0	255.255.255.0	wlan0	-	Red local
default	-	wlan0	10.200.100.1	

Servidor Concentrador / Workstation

Destino	Máscara	Interfaz	Gateway	Descripción
10.200.0.0	255.255.255.0	eth0	-	Red local
default	-	eth0	10.200.0.1	

Teléfonos IP

Destino	Máscara	Interfaz	Gateway	Descripción
10.200.10.0	255.255.255.0	eth0	-	Red local
default	-	eth0	10.200.10.100	

Servidor PBX Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
10.200.10.0	255.255.255.0	eth0	-	Red local (Tel IP)
170.210.97.40	255.255.255.248	eth1	-	Red local (Virtual)
default	-	eth1	170.210.97.48	

Monitor Remoto

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.40	255.255.255.248	eth0	-	Red local (Virtual)
default	-	eth0	170.210.97.48	

Router Campo B

Destino	Máscara	Interfaz	Gateway	Descripción
10.200.0.0	255.255.255.0	eth0	-	Red local
170.210.97.40	255.255.255.248	eth1	-	Red local (Virtual)
10.200.100.0	255.255.255.0	wlan0	-	Red local (Nodos)
10.200.10.0	255.255.255.0	eth1	170.210.97.44	Red Telefonía IP
X.X.X.X	255.255.255.252	eth2	-	Red entre routers con ISP
default	-	eth2	X.X.X.X	Enlace a ISP

Estación Central Santa Rosa

Teléfonos IP

Destino	Máscara	Interfaz	Gateway	Descripción
10.100.10.0	255.255.255.0	eth0	-	Red local
default	-	eth0	10.100.10.100	

Administradores

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.0	255.255.255.240	eth0	-	Red local
default	-	eth0	170.210.97.14	

Servidor VPN y Estación Gestora Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.32	255.255.255.248	eth0	-	Red local (Virtual)
default	-	eth0	170.210.97.38	

Servidor PBX Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
10.100.10.0	255.255.255.0	eth0	-	Red local (Tel IP)
170.210.97.32	255.255.255.248	eth1	-	Red local (Virtual)
default	-	eth1	170.210.97.38	

Servidor Recolección

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.0	255.255.255.240	eth0	-	Red local
10.100.1.0	255.255.255.0	eth1	-	Red local (Master)
default	-	eth0	170.210.97.14	

Servidor de cómputos Master

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.0	255.255.255.240	eth0	-	Red local
10.100.1.0	255.255.255.0	eth1	-	Red local (Recolección)
10.100.2.0	255.255.255.0	eth2	-	Red local (Nodos y Storage)
default	-	eth0	170.210.97.14	

Nodo de cómputos y Storage

Destino	Máscara	Interfaz	Gateway	Descripción
10.100.2.0	255.255.255.0	eth0	-	Red local

Router Santa Rosa

Destino	Máscara	Interfaz	Gateway	Descripción
170.210.97.0	255.255.255.240	eth0	-	Red local
170.210.97.32	255.255.255.248	eth1	-	Red local (Virtual)
10.100.10.0	255.255.255.0	eth1	170.210.97.33	Red Telefonía IP
10.11.12.X	255.255.255.252	eth2	-	Red entre routers (enlace de transporte contratado)
80.239.202.80	255.255.255.240	eth2	10.11.12.X	Enlace de transporte contratado
X.X.X.X	255.255.255.252	eth3	-	Red entre routers con ISP
default	-	eth3	X.X.X.X	Enlace a ISP

Estación de Administración Remota CABA

Teléfonos IP

Destino	Máscara	Interfaz	Gateway	Descripción
10.0.10.0	255.255.255.0	eth0	-	Red local
default	-	eth0	10.0.10.100	

Servidor PBX Buenos Aires

Destino	Máscara	Interfaz	Gateway	Descripción
10.0.10.0	255.255.255.0	eth0	-	Red local (Tel IP)
80.239.202.80	255.255.255.248	eth1	-	Red local (Virtual)
default	-	eth1	80.239.202.86	

Servidores DNS, Web y Estación Gestora Buenos Aires

Destino	Máscara	Interfaz	Gateway	Descripción
80.239.202.80	255.255.255.248	eth0	-	Red local (Virtual)
default	-	eth0	80.239.202.86	

Administradores

Destino	Máscara	Interfaz	Gateway	Descripción
80.239.202.88	255.255.255.248	eth0	-	Red local
default	-	eth0	80.239.202.94	

Router Buenos Aires

Destino	Máscara	Interfaz	Gateway	Descripción
80.239.202.88	255.255.255.248	eth0	-	Red local (Administradores)
80.239.202.80	255.255.255.248	eth1	-	Red local (Virtual)
10.0.10.0	255.255.255.0	eth1	80.239.202.84	Red Telefonía IP
10.10.10.X	255.255.255.252	eth2	-	Red entre routers (enlace de transporte contratado)
170.210.97.0	255.255.255.192	eth2	10.10.10.X	Enlace de transporte contratado
X.X.X.X	255.255.255.252	eth3	-	Red entre routers con ISP
default	-	eth3	X.X.X.X	Enlace a ISP

Tablas de traducción de direcciones (NAT)

Router Campo B - Source NAT

Pre-NAT			Post-NAT	
Dirección Origen	**Puerto Destino**	**Protocolo**	**Dirección Origen**	**Puerto Destino**
10.200.0.2	80	TCP	170.210.97.48	80
10.200.0.2	443	TCP	170.210.97.48	443
10.200.0.2	53	UDP	170.210.97.48	53
10.200.0.100	1410	UDP	170.210.97.50	1410

Router Campo B - Destination NAT

Pre-NAT			Post-NAT	
Dirección Destino	**Puerto Origen**	**Protocolo**	**Dirección Destino**	**Puerto Origen**
170.210.97.48	80	TCP	10.200.0.2	80
170.210.97.48	443	TCP	10.200.0.2	443
170.210.97.48	53	UDP	10.200.0.2	53
170.210.97.50	1410	UDP	10.200.0.100	1410

Direccionamiento - Capa de enlace

El direccionamiento en capa de enlace está basado en la creación de VLANs para la segmentación del dominio de broadcast, estando cada una contenida en una subred IP.

Las dos Estaciones Gestoras, ubicadas en la Estación Central de Santa Rosa y la Estación de Administración Remota de Bs. As., tienen un enlace promiscuo (marcado en negro) que monitorea todo el tráfico que pasa por los switches.

Estación Central Santa Rosa

Etiqueta	Subred	Descripción	Cantidad de hosts
100 (verde)	170.210.97.0/28	Red administrativa	6
200 (roja)	10.100.10.0/24	Telefonía IP	3
300 (azul)	10.100.2.0/24	Cluster de cómputo	6

Origen	Destino	Etiqueta	Tipo
Administradores	SSRB	100 (verde)	Tag
Cómputos Master	SSRA	100 (verde)	Tag
Servidor Recolección	SSRA	100 (verde)	Tag
RSR	SSRA	100 (verde)	Tag
SSRA	SSRB	100 (verde), 200 (roja)	Trunk
Tel IP 10101	SSRB	200 (roja)	Tag
Tel IP 10102	SSRA	200 (roja)	Tag
Servidor PBX	SSRA	200 (roja)	Tag
Cómputos Master	SSRA	300 (azul)	Tag
Cómputos Nodos	SSRA	300 (azul)	Tag
Cómputos Storage	SSRA	300 (azul)	Tag

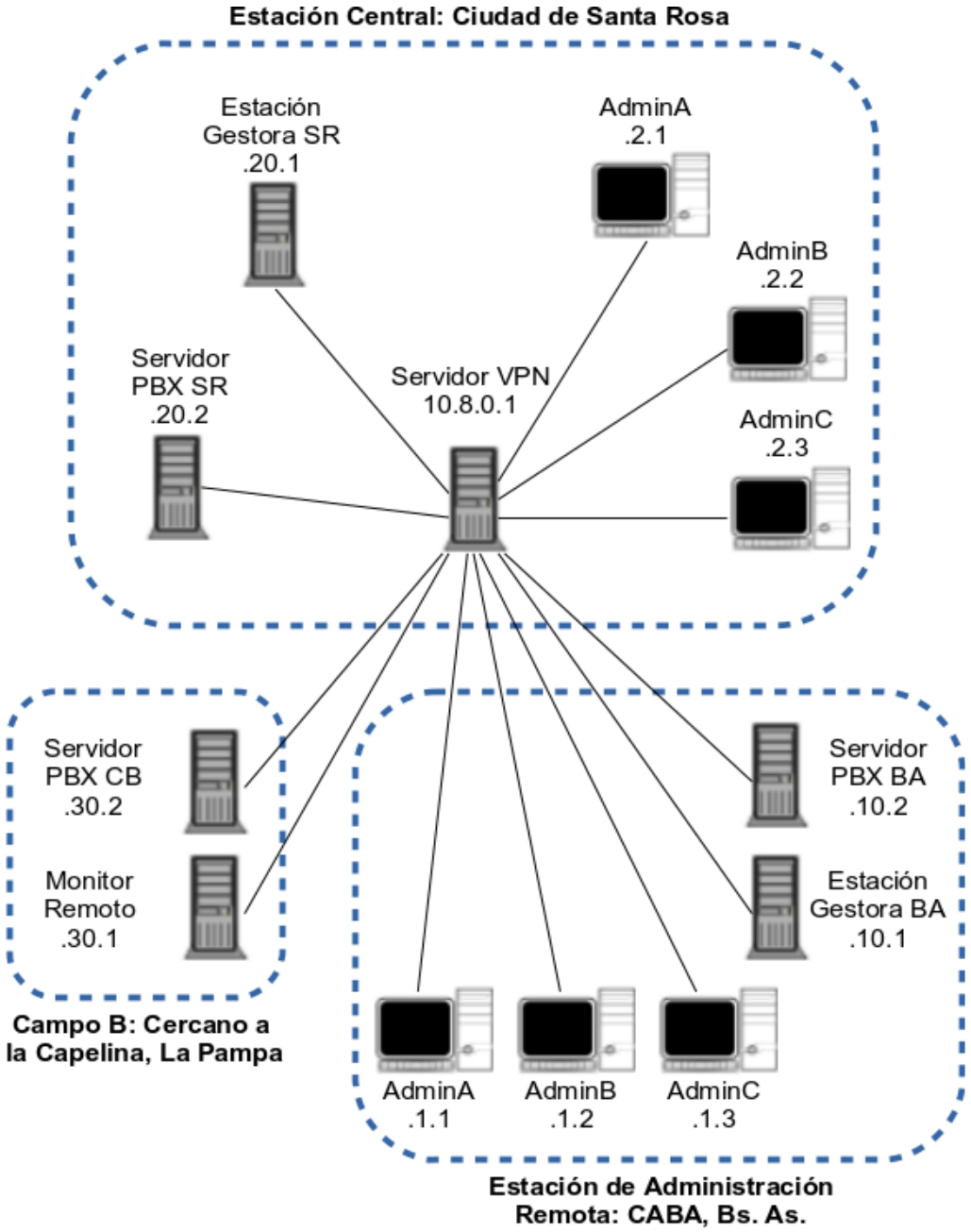
Estación de Administración Remota Buenos Aires

Etiqueta	Subred	Descripción	Cantidad de hosts
100 (verde)	80.239.202.88/29	Red administrativa	4
200 (roja)	10.0.10.0/24	Telefonía IP	3

Origen	Destino	Etiqueta	Tipo
Administradores	SBA	100 (verde)	Tag
RBA	SBA	100 (verde)	Tag
Teléfonos IP	SBA	200 (roja)	Tag
Servidor PBX	SBA	200 (roja)	Tag

Direccionamiento - Red privada virtual (VPN)

El principal objetivo de la red privada virtual (VPN) planteada es permitir transmitir los datos de voz, monitoreo y control a través de las redes extraorganizacionales de manera segura. Para esto se configura un servidor OpenVPN que generará un certificado autofirmado, claves pública y privada para sí mismo y claves para cada uno de los hosts de la VPN. Los administradores también tienen acceso a la VPN con el fin de comunicarse entre sí (más allá de por los teléfonos IP) y acceder a los datos de monitoreo remotamente.



Clasificación y priorización del tráfico

Los Servidores PBX deberán clasificar el tráfico VoIP utilizando el campo DSCP en IPv4, marcándolo Expedited Forwarding para su posterior priorización en la red del ISP.

En los routers deberán definirse disciplinas de encolado, por ejemplo con la herramienta **tc**, utilizando la técnica **token bucket jerárquico**, como se define a continuación:

Router Campo B

Puerto Origen	Puerto Destino	Protocolo	Características
1194	*	UDP	Encolado de alta prioridad
*	1194	UDP	Encolado de alta prioridad
1410	*	UDP	Encolado de media prioridad
*	1410	UDP	Encolado de media prioridad
22	*	TCP	Encolado de media prioridad
*	22	TCP	Encolado de media prioridad
10022	*	TCP	Encolado de media prioridad
*	10022	TCP	Encolado de media prioridad
*	*	*	Default: Encolado de baja prioridad. Tasa de transferencia limitada a 1 Mbps. Prioridad de drop.

Router Santa Rosa

Puerto Origen	Puerto Destino	Protocolo	Características
1194	*	UDP	Encolado de alta prioridad
*	1194	UDP	Encolado de alta prioridad
1410	*	UDP	Encolado de media prioridad
*	1410	UDP	Encolado de media prioridad
22	*	TCP	Encolado de media prioridad
*	22	TCP	Encolado de media prioridad
*	*	*	Default: Encolado de baja prioridad. Tasa de transferencia limitada a 2 Mbps. Prioridad de drop.

Router Buenos Aires

Puerto Origen	Puerto Destino	Protocolo	Características
1194	*	UDP	Encolado de alta prioridad. Tasa de transferencia limitada a 3 Mbps
*	1194	UDP	Encolado de alta prioridad. Tasa de transferencia limitada a 3 Mbps
22	*	TCP	Encolado de media prioridad
*	22	TCP	Encolado de media prioridad
*	*	*	Default: Encolado de baja prioridad. Tasa de transferencia limitada a 3 Mbps. Prioridad de drop.

IP Origen	IP Destino	Características
80.239.202.81	*	(DNS) Encolado de alta prioridad. Tasa de transferencia limitada a 0,5 Mbps
*	80.239.202.81	(DNS) Encolado de alta prioridad. Tasa de transferencia limitada a 0,5 Mbps
80.239.202.82	*	(Web) Encolado de media prioridad
*	80.239.202.82	(Web) Encolado de media prioridad

Enlaces contratados - Acuerdos de nivel de servicio (SLA)

Enlace a Internet satelital Campo B

Este enlace se utilizará principalmente para la transferencia de los datos meteorológicos y VoIP. Las pruebas se realizarán desde el **Servidor Concentrador** al **Servidor de cómputos Master** en la Estación Central de Santa Rosa. Los requisitos son:

- Disponibilidad mínima mensual: 70%
- Tiempo mínimo entre fallas: 24 hs
- Tiempo máximo de restauración del servicio: 18 hs
- Pérdida de paquetes máxima: 30% mensual. Las pruebas se harán con **iperf**.
- Delay máximo: 1000 ms. Las pruebas se harán con **ping**.
- Jitter máximo: 200 ms. Las pruebas se harán con **ping**.
- Capacidad: Tasa de transferencia mínima de 3 Mbps simétricos. Las pruebas se harán con **iperf**.

Enlace a Internet Campo A

Este enlace se utilizará para la transferencia de datos meteorológicos y el eventual monitoreo de las estaciones. Las pruebas se harán desde cada uno de los **Nodos GPRS** hasta el **Servidor Recolección** en la Estación Central de Santa Rosa. Los requisitos son:

- Disponibilidad mínima mensual: 98%
- Tiempo mínimo entre fallas: 24 hs
- Tiempo máximo de restauración del servicio: 18 hs
- Pérdida de paquetes máxima: 2% mensual. Las pruebas se harán con **iperf**.
- Delay máximo: 500 ms. Las pruebas se harán con **ping**.
- Jitter máximo: 50 ms. Las pruebas se harán con **ping**.
- Capacidad: Tasa de transferencia mínima de 1 Mbps simétrico. Las pruebas se harán con **iperf**.

Enlace a Internet Estación Central Santa Rosa

Este enlace se utilizará para la transferencia de datos meteorológicos, tanto con la **Estación Concentradora** en el Campo B como los **Nodos GPRS** en el Campo A. Las pruebas se harán contra ambos. Los requisitos son:

- Disponibilidad mínima mensual: 99%
- Tiempo mínimo entre fallas: 15 hs
- Tiempo máximo de restauración del servicio: 4 hs
- Pérdida de paquetes máxima: 1% mensual. Las pruebas se harán con **iperf**.

- Capacidad: Tasa de transferencia mínima de 5 Mbps simétricos. Las pruebas se harán con **iperf** contra los lugares establecidos de manera concurrente, de manera que la suma de las tasas de transferencia cumpla con el requisito.

Enlace a Internet Estación de Administración Remota Buenos Aires

Este enlace se utilizará para dar servicios web y DNS al público. Los requisitos son:

- Dispinibilidad mínima mensual: 99,5%
- Tiempo mínimo entre fallas: 15 horas
- Tiempo máximo de restauración del servicio: 4 hs
- Número máximo de microcortes por hora: 3
- Pérdida de paquetes máxima: 0,5% mensual.
- Round Trip Time máximo: 200 ms para usuarios en Argentina, 400 ms para el resto.
- Capacidad: Tasa de transferencia mínima de 50 Mbps simétricos. Las pruebas se harán con **ftp** contra http://security.debian.org, http://ar.archive.ubuntu.com y ftp.microsoft.com.

Enlace de transporte contratado

Este enlace se utilizará para transportar los datos del **Servidor de cómputos Master** en la Estación Central de Santa Rosa al **Servidor Web** en la Estación de Administración Remota de Buenos Aires, además de cursar tráfico VoIP. Las pruebas se harán entre los dos servidores mencionados. Los requisitos son:

- Disponibilidad mínima mensual: 99,8%
- Tiempo mínimo entre fallas: 12 hs
- Tiempo máximo de restauración del servicio: 4 hs
- Número máximo de microcortes por hora: 3
- Pérdida de paquetes máxima: 0,1% diario. Las pruebas se harán con **iperf**.
- Delay máximo: 30 ms. Las pruebas se harán con **ping**.
- Jitter máximo: 10 ms. Las pruebas se harán con **ping**.
- Capacidad: Tasa de transferencia mínima de 10 Mbps simétrico. Los paquetes marcados como Expedited Forwarding deberán tener una tasa asegurada de 2 Mbps. Las pruebas se harán con **iperf**.
- Preservación de secuencia por flujo: No se admite el reordenamiento de paquetes dentro de un mismo flujo. Cualquier paquete transferido fuera de orden se contabilizará como perdido.

Software y Servicios

Resumen
Todo el software elegido pertenece a la categoría **Software Libre** y es utilizado ampliamente en el mercado, ya que está más que comprobado su buen funcionamiento. La mayoría de las alternativas propuestas también cumplen con esto, pero presentan menos funcionalidades o son más difíciles de configurar.

Servicio	Software	Tipo de flujo de tráfico de red	Protocolo utilizado	Usuarios	Servidores	Tasa de transferencia requerida	Calidad de Servicio
VoIP	Asterisk, Elastix	Peer-to-peer	SIP / SDP, RTP, RTCP	Teléfonos IP	PBX	2 Mbps simétricos	Expedited Forwarding (la más alta prioridad)
Web	Nginx, Apache	Cliente / Servidor	HTTP, HTTPS	Externos	VM CABA	50 Mbps simétricos	Tasa asegurada
DNS	Unbound, BIND	Cliente / Servidor	DNS	Externos	VM CABA	-	Delay mínimo
Agente de monitoreo	Nagios, Munin	Cliente / Servidor	SNMP	Administradores	VM CABA, VM Santa Rosa	-	Alta prioridad
Acceso remoto	OpenSSH	Cliente / Servidor	SSH	Administradores	-	-	Alta prioridad
Transferencia al Servidor Web	rsync, OpenSSH	Cliente / Servidor	SSH	-	VM CABA, Master Santa Rosa	10 Mbps a la Estación Remota	Alta prioridad
Red Privada Virtual	OpenVPN	Peer-to-peer	-	Administradores	Servidores VM	-	-
Firewall	pfSense, netfilter	-	-	-	-	-	-
Virtualización	KVM, XenServer	-	-	-	Servidores VM	-	-
Base de Datos	PostgreSQL, MySQL	-	-	-	Servidores de almacenamiento	-	-

Voz sobre IP (VoIP)

El servicio de Voz sobre IP (VoIP) se implementará utilizando los protocolos de señalización SIP / SDP. El CODEC para audio utilizado será G.711. Se recomienda que los servidores PBX corran Asterisk o en su defecto Elastix, pero que todos usen el mismo software.
El servicio de VoIP se brindará a tres lugares geográficamente distantes. Para esto, a cada estación se le ha asignado un servidor que actuará como **proxy** y **registrar**, comunicándose con los otros servidores a través de la VPN de la organización, a modo de mantener la confidencialidad en las llamadas. El esquema de registro es el siguiente:

Host	Cuenta	Registrar	IP Registrar
Tel IP 10201	10201	Servidor PBX CB	10.200.10.100
Servidor PBX CB	-	Servidor PBX SR	10.8.20.2 (VPN)
Tel IP 10101	10101	Servidor PBX SR	10.100.10.100
Tel IP 10102	10102	Servidor PBX SR	10.100.10.100
Servidor PBX BA	-	Servidor PBX SR	10.8.20.2 (VPN)
Tel IP 10001	10001	Servidor PBX BA	10.0.10.100
Tel IP 10002	10002	Servidor PBX BA	10.0.10.100

Portal Web

La organización cuenta con un servidor web para disponer de los datos meteorológicos al público utilizando los protocolos HTTP (versiones 1.0, 1.1 y 2.0) y HTTPS. En el caso de HTTPS será necesario adquirir un **certificado X.509** de una autoridad de certificación. La obtención de este certificado y la configuración del servidor están fuera del alcance de este documento.
El software recomendado para su implementación es **Nginx**, o en su defecto **Apache WebServer**.

Servicio de resolución de nombres (DNS)

La organización cuenta con un servidor que atiende consultas de resolución de nombres (DNS). Para ello, el servidor DNS deberá poder recibir consultas y hacerlas a los servidores **root** correspondientes.
Los software recomendados para su implementación son **Unbound** o **BIND**.

Monitoreo y control

Para el monitoreo y control se utilizará el protocolo SNMP (puertos UDP 161 y 162) y se dispondrán tres servidores: las **estaciones gestoras** en Santa Rosa y Bs. As. y un **monitor remoto** en la ubicación Campo B, que implementará **rmon**. Las estaciones gestoras deberán utilizar una herramienta gráfica de monitoreo (se recomienda **Nagios** o **Munin**, pero que ambas estaciones utilicen la misma). Los dispositivos monitoreados deberán correr el servicio **snmpd** y ser configurados para generar las alertas que se detallarán más adelante.
El monitor remoto responderá a la estación gestora de Santa Rosa. Todo el tráfico SNMP entre dos ubicaciones geográficamente distantes (aquellas que utilicen un enlace de terceros) transitará a través de la VPN organizacional, con la excepción del monitoreo de la estación gestora Santa Rosa y los Nodos GPRS, que utilizarán el protocolo SNMP sobre DTLS en los puertos no estándar 10161 y 10162 (Traps), para lo cual se hará uso de un certificado autofirmado.
Los parámetros a monitorear deberán ser consultados al menos cada 10 minutos. Estos se detallan a continuación.

Monitor Remoto

Dispositivo	Parámetro	Umbral	Alerta
Servidor Concentrador	Uso de disco	75% de espacio superado	Notificar al administrador
Servidor PBX	Estado del servicio PBX	No disponible	Reiniciar servicio, notificar al administrador
Nodos Wi-Fi	Conectividad	No disponible	Notificar al administrador, enviar logs
RCB	Tasa de paquetes del enlace a Internet	Supera 80% de capacidad del Router	Deshabilitar interfaz, notificar al administrador, generar logs
RCB	Pérdida de paquetes	Supera el 30% mensual	Generar logs

Estación Gestora Santa Rosa

Dispositivo	Parámetro	Umbral	Alerta
Servidor Recolección	Uso de disco	75% de espacio superado	Notificar al administrador
Servidor Master	Uso de disco	75% de espacio superado	Notificar al administrador

Servidor Storage	Uso de disco	75% de espacio superado	Notificar al administrador
Servidor PBX	Estado del servicio PBX	No disponible	Reiniciar servicio, notificar al administrador
Servidor VPN	Estado del servicio VPN	No disponible	Reiniciar servicio, notificar al administrador
SSRA	Congestión (uso de buffers de encolado)	80% de espacio superado	Notificar al administrador, enviar logs
Nodos GPRS	Conectividad	No disponible	Notificar al administrador, enviar logs
RSR	Tasa de paquetes del enlace contratado	Supera 80% de capacidad del Router	Deshabilitar interfaz, notificar al administrador, generar logs
RSR	Tasa de paquetes del enlace a Internet	Supera 80% de capacidad del Router	Deshabilitar interfaz, notificar al administrador, generar logs
RSR	Delay a la Estación Concentradora en Campo B	Mayor a 1000 ms	Generar logs
RSR	Delay a los Nodos GPRS	Mayor a 500 ms	Generar logs
RSR	Pérdida de paquetes del enlace contratado	Supera el 0,1% diario	Generar logs
RSR	Pérdida de paquetes del enlace a Internet	Supera el 1% mensual	Generar logs

Estación de Administración Remota Buenos Aires

Dispositivo	Parámetro	Umbral	Alerta
Servidor PBX	Estado del servicio PBX	No disponible	Reiniciar servicio, notificar al administrador
Servidor DNS	Estado del servicio DNS	No disponible	Reiniciar servicio, notificar al administrador
Servidor DNS	Delay	-	Mantener logs
Servidor Web	Estado del servicio Web	No disponible	Reiniciar servicio, notificar al administrador
Servidor Web	Delay	-	Mantener logs
Servidor Web	Cantidad de datos transmitidos	-	Mantener logs
SBA	Congestión (uso de buffers de encolado)	80% de espacio superado	Notificar al administrador, enviar logs
RBA	Tasa de transferencia del enlace contratado	Menor a 9 Mbps (90% del contratado)	Notificar al administrador, enviar logs
RBA	Tasa de transferencia del enlace a Internet	Menor a 45 Mbps (90% del contratado)	Notificar al administrador, enviar logs
RBA	Tasa de paquetes del enlace contratado	Supera 80% de capacidad del Router	Deshabilitar interfaz, notificar al administrador, generar logs
RBA	Tasa de paquetes del enlace a Internet	Supera 80% de capacidad del Router	Deshabilitar interfaz, notificar al administrador, generar logs
RBA	Delay al Master de Cómputos en Santa Rosa	Mayor a 30 ms	Notificar al administrador

RBA	Pérdida de paquetes del enlace contratado	Supera el 0,1% diario	Notificar al administrador
RBA	Pérdida de paquetes del enlace a Internet	Supera el 0,5% diario	Notificar al administrador

Acceso remoto

Para el acceso remoto se utilizará el protocolo **ssh**. El software para su implementación será **OpenSSH**, que deberá funcionar como servicio en los lugares de acceso remoto y estar instalado en los dispositivos que quieran acceder. Para la autenticidad será necesario que los lugares de acceso remoto tengan las claves públicas de los hosts autorizados, generadas manualmente por un administrador, permitiendo **solamente** a estos la conexión. El puerto a utilizar será el estándar 22 TCP, excepto en el **servidor concentrador** que escuchará en el puerto no estándar 10022 TCP.
Como alternativa para el acceso remoto podría utilizarse la red privada virtual, aunque esto supondría un grave costo en el servidor VPN.

Seguridad - Red Privada Virtual (VPN)

Como se planteó anteriormente, la organización contará con una red privada virtual. El software para su implementación será **OpenVPN**, utilizando un esquema de cliente / servidor. El servidor VPN, ubicado en la Estación Central Santa Rosa, deberá generar las claves de todos sus clientes para la autenticidad y utilizar un certificado autofirmado. La forma de transferir estas claves y certificado de manera segura queda a cargo del administrador.

Seguridad - Firewall

Todos los routers que actúan como Firewall deberán ser configurados en forma **prudente**, es decir, droppear todo lo que no esté explícitamente definido para pasar. Además deberán poder dejar pasar paquetes de conexiones ya establecidas. Las reglas para el protocolo TCP sólo afectan a los segmentos que lleven la bandera SYN en 1.
El software recomendado para su implementación es **pfSense**, o en su defecto **netfilter** en Linux.

Router Campo B

Chain	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Protocolo	Acción
FORWARD	10.200.100.0/24	10.200.0.100	*	1410	UDP	ACCEPT
FORWARD	10.200.0.100	10.200.100.0/24	1410	*	UDP	ACCEPT
Nodos Wi-Fi con Servidor Concentrador						
FORWARD	170.210.97.40/24	170.210.97.36	*	1194	UDP	ACCEPT
FORWARD	170.210.97.36	170.210.97.40/24	1194	*	UDP	ACCEPT
Servidores PBX y Monitoreo Remoto con el Servidor VPN						
FORWARD	10.200.0.0/24	*	*	80, 443, 53	TCP	ACCEPT
FORWARD	10.200.0.0/24	*	*	53	UDP	ACCEPT
FORWARD	*	10.200.0.0/24	53	*	UDP	ACCEPT
Acceso web al Administrador (Workstation)						
FORWARD	10.200.0.100	170.210.97.13	*	1410	UDP	ACCEPT
FORWARD	170.210.97.13	10.200.0.100	1410	*	UDP	ACCEPT
Servidor Concentrador con Servidor Recolección						
FORWARD	170.210.97.43	*	*	161	UDP	ACCEPT
FORWARD	*	170.210.97.43	161	*	UDP	ACCEPT
FORWARD	170.210.97.43	*	162	*	UDP	ACCEPT
FORWARD	*	170.210.97.43	*	162	UDP	ACCEPT
SNMP y SNMPTrap para el Monitor Remoto						
FORWARD	*	10.200.0.100	*	10022	TCP	ACCEPT
Acceso remoto al Servidor Concentrador						
FORWARD	10.200.0.0/24	10.200.10.0/24	*	*	*	ACCEPT
FORWARD	10.200.0.0/24	10.200.100.0/24	*	*	*	ACCEPT
FORWARD	10.200.0.0/24	170.210.97.40/29	*	*	*	ACCEPT
FORWARD	10.200.10.0/24	10.200.0.0/24	*	*	*	ACCEPT
FORWARD	10.200.100.0/24	10.200.0.0/24	*	*	*	ACCEPT
FORWARD	170.210.97.40/29	10.200.0.0/24	*	*	*	ACCEPT
Acceso administrativo a redes internas						

Router Santa Rosa

Chain	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Protocolo	Acción
FORWARD	170.210.97.16/28	170.210.97.13	*	1410	UDP	ACCEPT
FORWARD	170.210.97.13	170.210.97.16/28	1410	*	UDP	ACCEPT
Nodos GPRS con Servidor Recolección						
FORWARD	170.210.97.50	170.210.97.13	*	1410	UDP	ACCEPT
FORWARD	170.210.97.13	170.210.97.50	1410	*	UDP	ACCEPT
Servidor Concentrador con Servidor Recolección						
FORWARD	170.210.97.34	*	*	161	UDP	ACCEPT
FORWARD	*	170.210.97.34	161	*	UDP	ACCEPT
FORWARD	170.210.97.34	*	162	*	UDP	ACCEPT
FORWARD	*	170.210.97.34	*	162	UDP	ACCEPT
SNMP y SNMPTrap para la Estación Gestora						
FORWARD	170.210.97.40/29	170.210.97.36	*	1194	UDP	ACCEPT
FORWARD	170.210.97.36	170.210.97.40/29	1194	*	UDP	ACCEPT
FORWARD	170.210.97.0/28	170.210.97.36	*	1194	UDP	ACCEPT
FORWARD	170.210.97.36	170.210.97.0/28	1194	*	UDP	ACCEPT
FORWARD	80.239.202.88/29	170.210.97.36	*	1194	UDP	ACCEPT
FORWARD	170.210.97.36	80.239.202.88/29	1194	*	UDP	ACCEPT
FORWARD	80.239.202.80/29	170.210.97.36	*	1194	UDP	ACCEPT
FORWARD	170.210.97.36	80.239.202.80/29	1194	*	UDP	ACCEPT
Servidor VPN con sus clientes						
FORWARD	170.210.97.34	170.210.97.16/28	*	10161	UDP	ACCEPT
FORWARD	170.210.97.16/28	170.210.97.34	10161	*	UDP	ACCEPT
FORWARD	170.210.97.34	170.210.97.16/28	10162	*	UDP	ACCEPT
FORWARD	170.210.97.16/28	170.210.97.34	*	10162	UDP	ACCEPT
Estación Gestora con Nodos GPRS (SNMP sobre DTLS)						
FORWARD	*	170.210.97.0/28	*	22	TCP	ACCEPT
Acceso remoto al Master de cómputos y Administración						
FORWARD	170.210.97.0/24	*	*	80, 443,	TCP	ACCEPT

				53		
FORWARD	170.210.97.0/24	*	*	53	UDP	ACCEPT
FORWARD	*	170.210.97.0/24	53	*	UDP	ACCEPT
Acceso web a Administradores						
FORWARD	170.210.97.0/28	10.100.10.0/24	*	*	*	ACCEPT
FORWARD	170.210.97.0/28	170.210.97.32/29	*	*	*	ACCEPT
FORWARD	10.100.10.0/24	170.210.97.0/28	*	*	*	ACCEPT
FORWARD	170.210.97.32/29	170.210.97.0/28	*	*	*	ACCEPT
Acceso administrativo a redes internas						

Router Buenos Aires

Chain	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Protocolo	Acción
FORWARD	80.239.202.80/29	170.210.97.36	*	1194	UDP	ACCEPT
FORWARD	170.210.97.36	80.239.202.80/29	1194	*	UDP	ACCEPT
Servidores PBX y Estación Gestora con el Servidor VPN						
FORWARD	*	170.210.97.10	*	22	TCP	ACCEPT
Acceso remoto al Master de cómputos						
FORWARD	*	80.239.202.81	*	53	TCP	ACCEPT
FORWARD	*	80.239.202.81	*	53	UDP	ACCEPT
FORWARD	80.239.202.81	*	53	*	UDP	ACCEPT
Responder a consultas DNS						
FORWARD	80.239.202.81	*	*	53	TCP	ACCEPT
FORWARD	80.239.202.81	*	*	53, 123	UDP	ACCEPT
FORWARD	*	80.239.202.81	53, 123	*	UDP	ACCEPT
Hacer consultas DNS y NTP (Servidor DNS)						
FORWARD	*	80.239.202.82	*	80, 443	TCP	ACCEPT
Servidor Web						
FORWARD	80.239.202.88/29	*	*	80, 443	TCP	ACCEPT
FORWARD	80.239.202.88/29	*	*	53	UDP	ACCEPT
FORWARD	*	80.239.202.88/29	53	*	UDP	ACCEPT

Acceso web a Administradores						
FORWARD	*	80.239.202.88/29	*	22	TCP	ACCEPT
Acceso remoto a Administradores						
FORWARD	80.239.202.88/29	80.239.202.80/29	*	*	*	ACCEPT
FORWARD	80.239.202.88/29	10.0.10.0/24	*	*	*	ACCEPT
FORWARD	80.239.202.80/29	80.239.202.88/29	*	*	*	ACCEPT
FORWARD	10.0.10.0/24	80.239.202.88/29	*	*	*	ACCEPT
Acceso administrativo a redes internas						

Virtualización

Los siguientes servidores tendrán máquinas virtuales brindando servicios:
Servidor VM Campo B: Servidor PBX, Monitor Remoto, Router Virtual.
Servidor VM Santa Rosa: Servidor PBX, Servidor VPN, Estación Gestora, Router Virtual.
Servidor VM Buenos Aires: Servidor PBX, Estación Gestora, Servidor Web, Servidor DNS, Router Virtual.

Para la implementación se recomiendan **KVM** o **XenServer**, preferiblemente eligiendo una opción o la otra de manera homogenea.

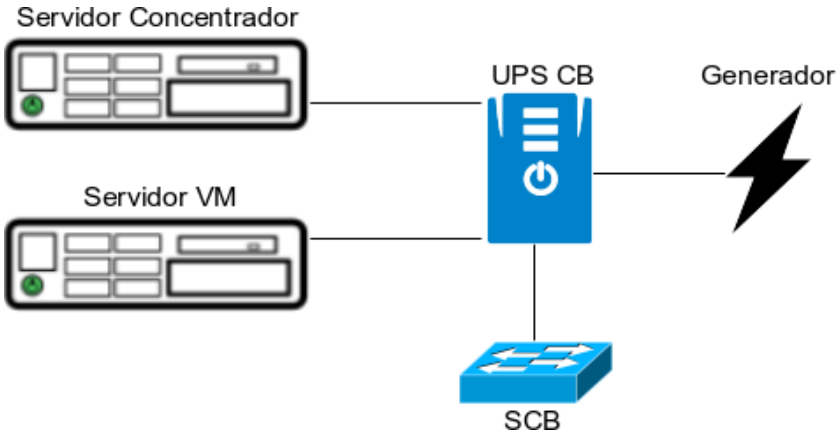
Base de Datos

Los servidores que requieran almacenamiento (en particular los servidores de **Recolección**, **Concentrador** y **Storage**) lo harán a través de una Base de Datos local. Los motores de Bases de Datos recomendados son **PostgreSQL** y **MySQL/MariaDB**

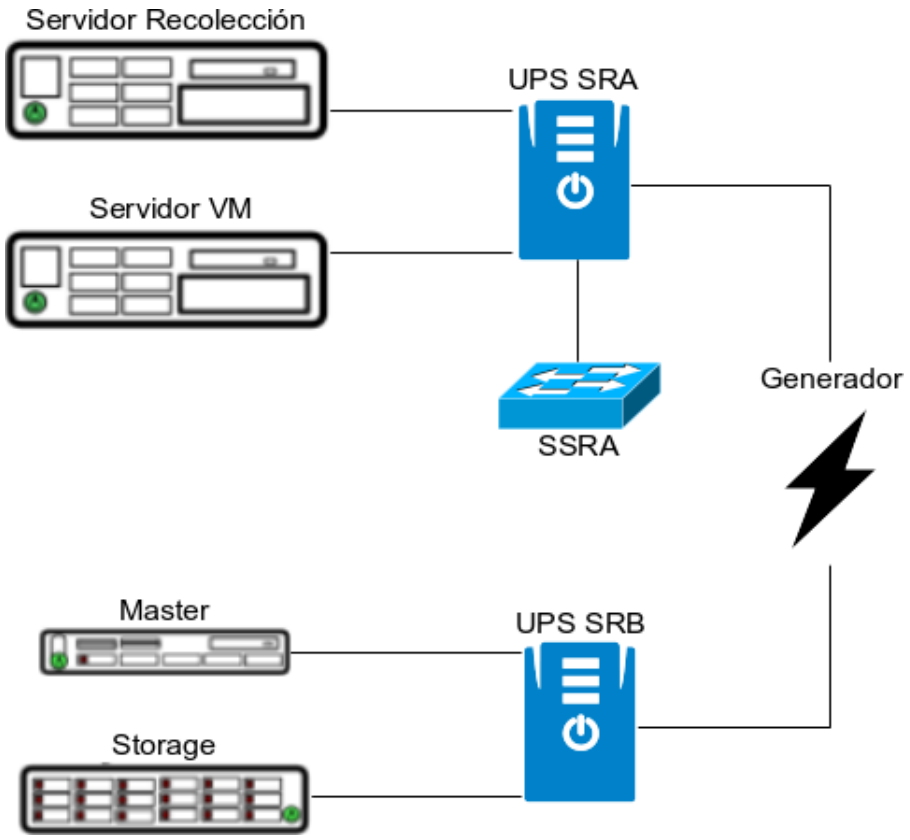
Mecanismos de redundancia y tolerancia a fallos

Para mantener en servicio a los sistemas críticos ante fallos en el suministro eléctrico se recomienda mantener a los servidores y dispositivos intermedios con una fuente eléctrica alternativa. Además, es vital para evitar el sobrecalentamiento de servidores que estos se hallen en un cuarto con temperatura regulada. Para esto se recomiendan al menos dos acondicionadores que funcionen por turnos, de modo de mantener la temperatura las 24 horas.
Se asume que las estaciones meteorológicas (Nodos Wi-Fi y GPRS) son autosustentables, o al menos poseen su propio mecanismo de regulación ante fallas.
El uso de generadores eléctricos es opcional para aumentar la disponibilidad de los sistemas críticos. Se proponen los siguientes diagramas para obtener tolerancia a fallos:

Estación Concentradora Campo B



Estación Central Santa Rosa



Estación de Administración Remota Buenos Aires

Dispositivos físicos

Nombre	Descripción	Características
Servidor VM CB	Servidor de Máquinas Virtuales, Estación Concentradora	Procesador Dual Core 1,6 GHz. 16 GB RAM. 1 TB almacenamiento. 4 puertos Gigabit Ethernet
Servidor Concentrador	Servidor Concentrador, Estación Concentradora	Procesador Dual Core 1,6 GHz. 8 GB RAM. 1 TB almacenamiento. 2 puertos Gigabit Ethernet
Servidor VM BA	Servidor de Máquinas Virtuales, Estación de Administración Remota	Procesador Dual Core 2,4 GHz. 16 GB RAM. 1 TB almacenamiento. 6 puertos Gigabit Ethernet
Servidor VM SR	Servidor de Máquinas Virtuales, Estación Central	Procesador Dual Core 2,4 GHz. 16 GB RAM. 1 TB almacenamiento. 6 puertos Gigabit Ethernet
Servidor Recolección	Servidor de Recolección, Estación Central	Procesador Dual Core 1,6 GHz. 8 GB RAM. 10 TB almacenamiento. 2 puertos Gigabit Ethernet
Servidor Storage	Servidor Storage, cluster de cómputos, Estación Central	Procesador Dual Core 1,6 GHz. 8 GB RAM. 10 TB almacenamiento. 2 puertos Gigabit Ethernet
Servidor Master	Servidor Master, cluster de cómputos, Estación Central	Procesador Dual Core 1,6 GHz. 8 GB RAM. 1 TB almacenamiento. 2 puertos Gigabit Ethernet
Servidor Nodo x4	4 Servidores Nodos, cluster de cómputos, Estación Central	Procesador Quad Core 2,2 GHz. 32 GB RAM. 1 TB almacenamiento. 2 puertos Gigabit Ethernet
SCB	Switch, Estación Concentradora	24 puertos Gigabit Ethernet
SSRA	Switch A, Estación Central	36 puertos 10 Gigabit Ethernet, Soporte para VLANs
SSRB	Switch B, Estación Central	24 puertos Gigabit Ethernet, Soporte para VLANs
SBA	Switch, Estación de Administración Remota	24 puertos Gigabit Ethernet, Soporte para VLANs

UPS CB	UPS, Estación Concentradora	1400 W / 2000 VA
UPS SRA	UPS A, Estación Central	1400 W / 2000 VA
UPS SRB	UPS B, Estación Central	1400 W / 2000 VA
UPS BA	UPS, Estación de Administración Remota	1000 W / 1500 VA
-	Cableado	Gigabit Ethernet Categoría 6

Anexo - Bibliografía

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

RFC 6353: Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)