Trabajo Práctico
Integración de conocimientos

Interconexión de Sistema de Estaciones Meteorológicas.

Beron Federico - 122190
Diciembre 2017

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

Contenido

Consignas

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).

Sobre el caso de estudio.

Se requiere diseñar 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 y ofrecer parte de los datos obtenidos al público en general. Para realizar esta tarea hay que tener en cuenta que el sistema estará distribuido en cuatro localizaciones distintas, que cuentan además con distintas características.

En la localización denominada “Campo A” (Figura 1) las estaciones meteorológicas utilizadas cuentan con un módulo de comunicación por GPRS, por lo que se comunicarán a la estación central a través de Internet.

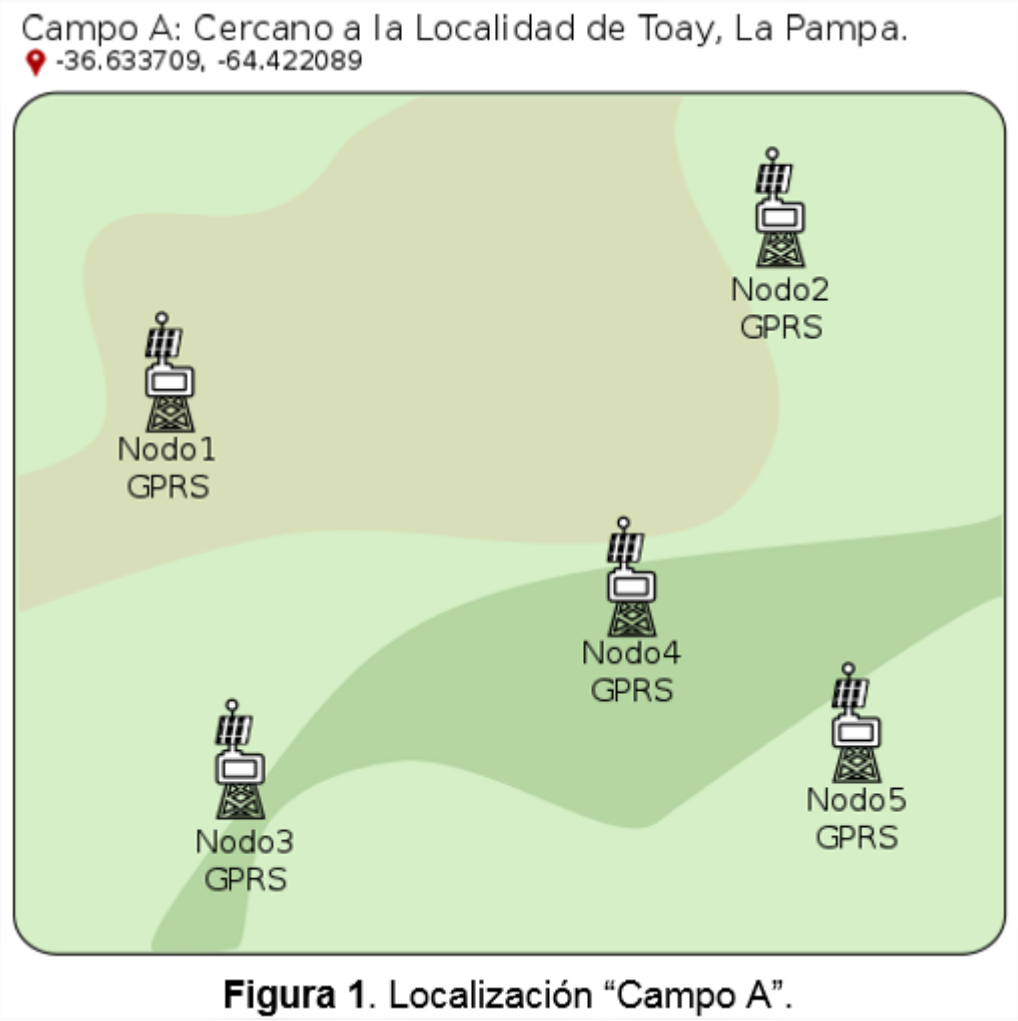


Figura 1. Localización “Campo A”.

El segundo campo, denominado “Campo B” (Figura 2), se encuentra a considerable distancia de cualquier centro urbano y no existen antenas de comunicación celular que permitan utilizar el módulo GPRS de las estaciones. Se necesitará por ello, contar con otra tecnología para lograr la conexión de datos. La organización ha optado por crear una estación concentradora que dispondrá de una conexión a Internet satelital. Esta estaciónconcentradoratendrá la tarea de recolectar los datos de las estaciones meteorológicas adyacentes a través de una red WIFI de largo alcance (las estaciones se encuentran en un radio de 20 km de la estación concentradora). Cada 20 minutos, laestación concentradora, enviará los datos al servidor de recolección principal, ubicado en la estación central. De no contar con conexión a Internet en ese momento, sea debido a interferencias o por factores climatológicos, el servidor de la estación concentradora retendrá los datos y volverá a enviarlos al momento de retomar la conectividad.

En la estación concentradora se dispondrá además de un teléfono VoIP con acceso a los restantes internos de la organización, que será de utilidad para la persona que deba llegar a

esa localización remota a realizar una tarea de configuración o mantenimiento (recuerde que no existe cobertura de señal celular). Se requiere además una boca de red disponible para conectar una portátil para realizar dichas tareas. Además, el servidor concentrador debe poder ser accedido remotamente, utilizando SSH en el puerto no estándar 10022.

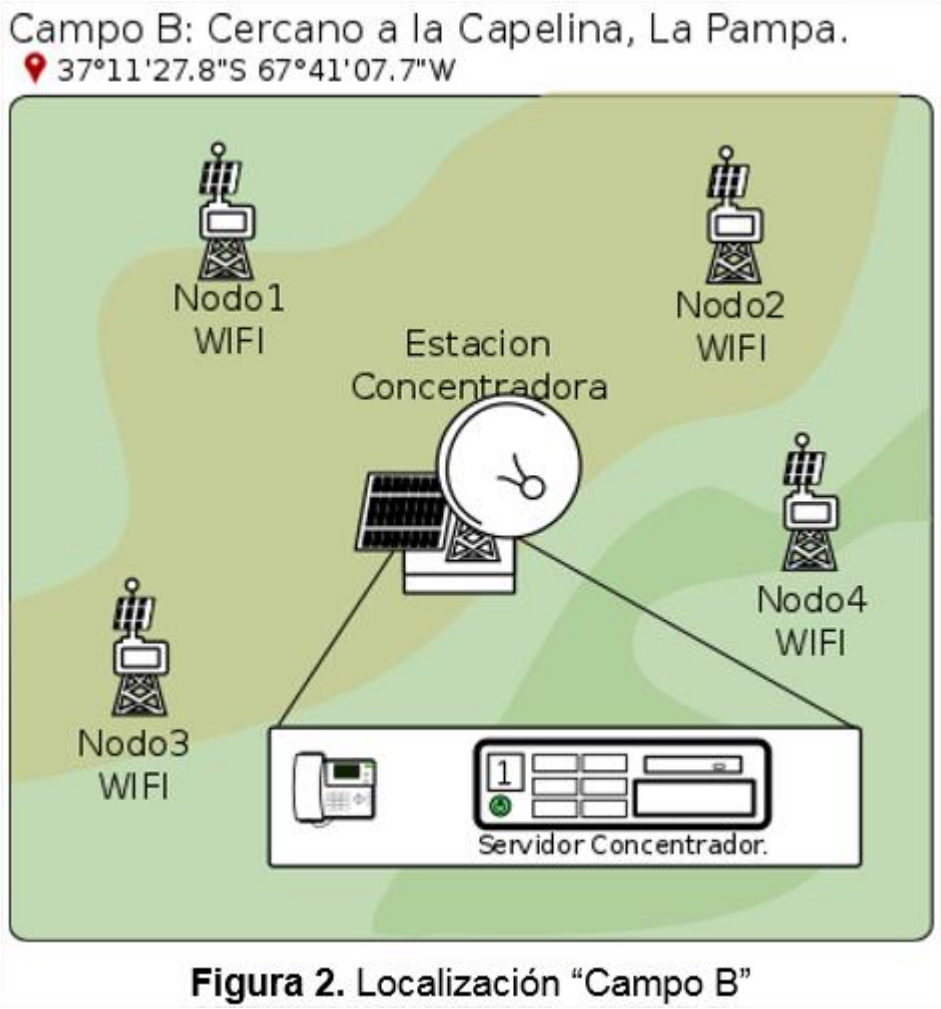


Figura 2. Localización “Campo B”

Las estaciones meteorológicas recopilan 15 variables, de tipo long int, que son enviadas cada 10 minutos al servidor que tengan configurado, adicionando además 6 bytes para un número de identificación de estación. En el caso del “Campo A” las estaciones se comunican directamente al servidor de recolección principal mientras que en el caso del “Campo B”, las estaciones meteorológicas se comunican con el servidor concentrador, y es este último quien envía los datos al servidor de recolección principal. Tanto el servidor concentrador como las estaciones meteorológicas utilizarán un protocolo propio, que implementa cifrado de clave pública y privada, sobre UDP. El overhead en promedio del protocolo de aplicación es de 32 bytes por datagrama. El puerto utilizado por los servidores que recepcionan datos es el 1410. En la ciudad de Santa Rosa, La Pampa, se encuentra localizada la estación central (Figura 3), en ella habrá dos salas diferentes. En una de ellas, habrá 3 puestos de administración que deberán contar con acceso tanto a las redes internas como a Internet y a un teléfono IP. La sala restante es un data center, denominado Data Center Santa Rosa.

En el Data Center Santa Rosa estará el servidor de recolección principal, un servidor de máquinas virtuales, un teléfono IP, y un pequeño cluster de cómputo. El cluster cuenta con un nodo “master” que tendrá acceso a tres redes distintas, la pública para permitir acceso remoto (utilizando ssh), una red interna mediante la que se comunicará solamente con sus cuatro nodos ycon el servidor de almacenamiento, y la tercera, la red privada de la organización. El

master obtendrá los datos de procesamiento del servidor de recolección principal, a través de la red privada de la organización y los almacenará en su servidor de almacenamiento.

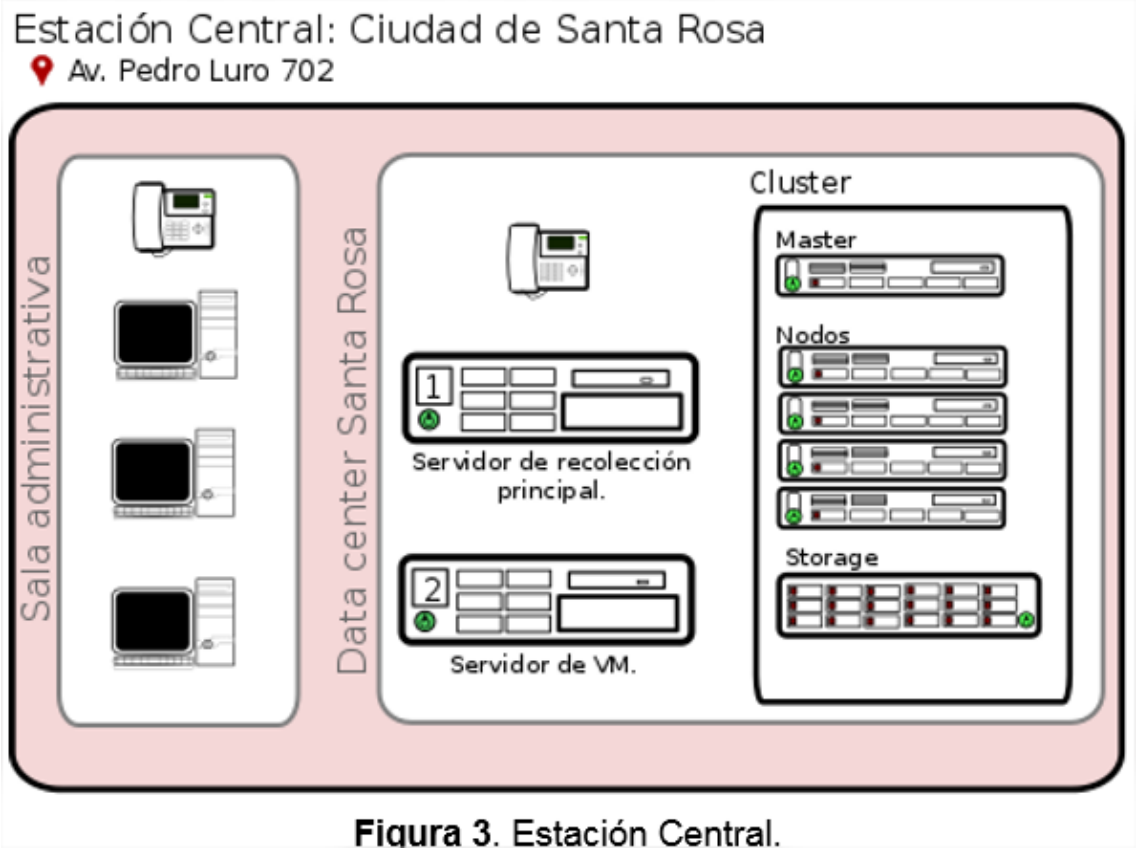


Figura 3. Estación Central.

Finalmente, la última localización será en CABA y será denominada Estación de Administración Remota (Figura 4) en Buenos Aires. Allí habrá un pequeño datacenter con un Servidor de Máquinas Virtuales, y se proveerá el servicio al público a través de un portal web. Contará además con dos teléfonos IP y 3 puestos administrativos. El Servidor Web tomará los datos desde una red privada con la que se comunicará con el "master" del cluster Data center Santa Rosa. El servidor Web utilizará la herramienta rsync para realizar el transporte de los datos, mediante el uso de un script que se actualizará cada 10 minutos. El tamaño promedio de las imágenes transportadas es de 10Mb.

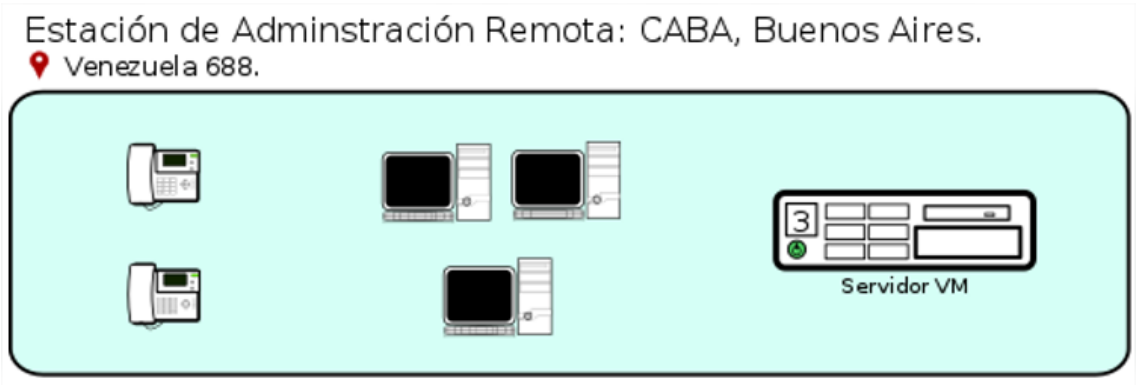


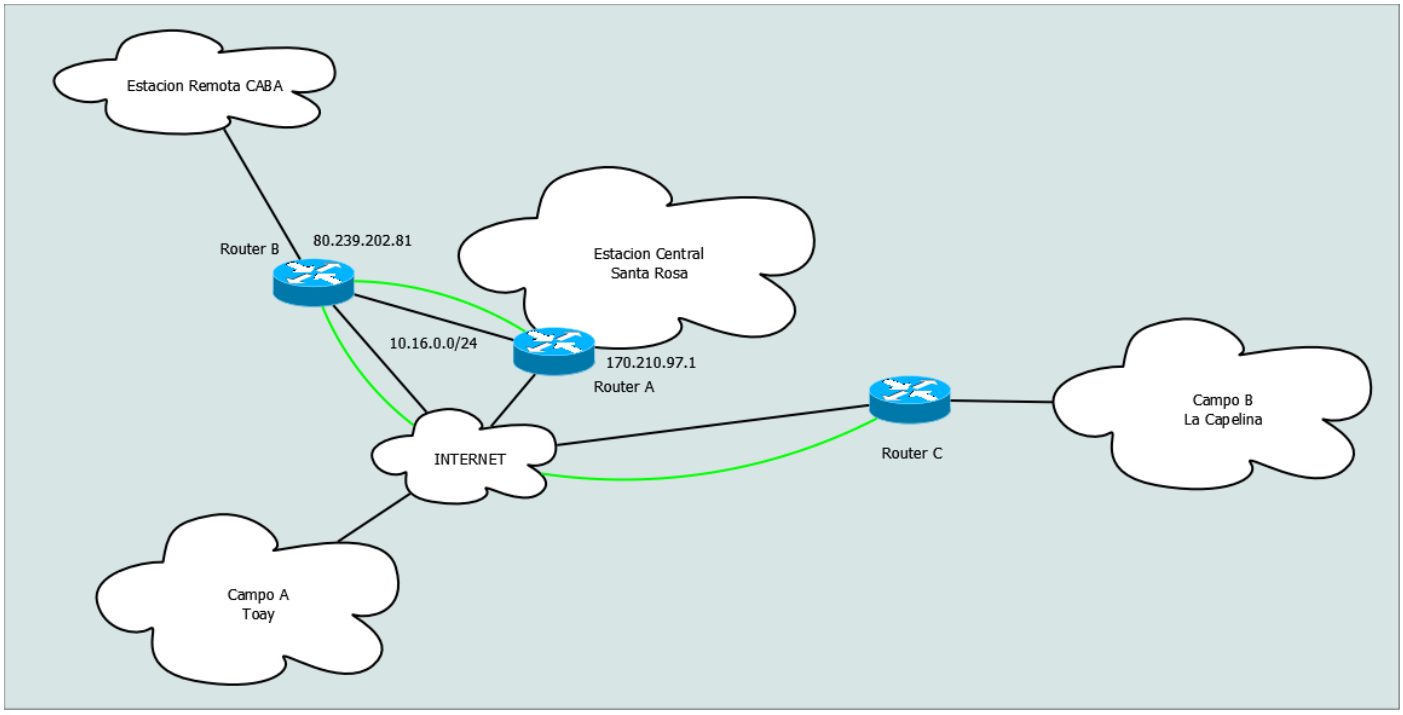
Figura 4. Estación de administración remota.

La estación de administración remota contará con un enlace a Internet, y un enlace a una red privada organizacional, ya que se contratará un enlace de transporte que unirá esta estación con la estación central en La Pampa.

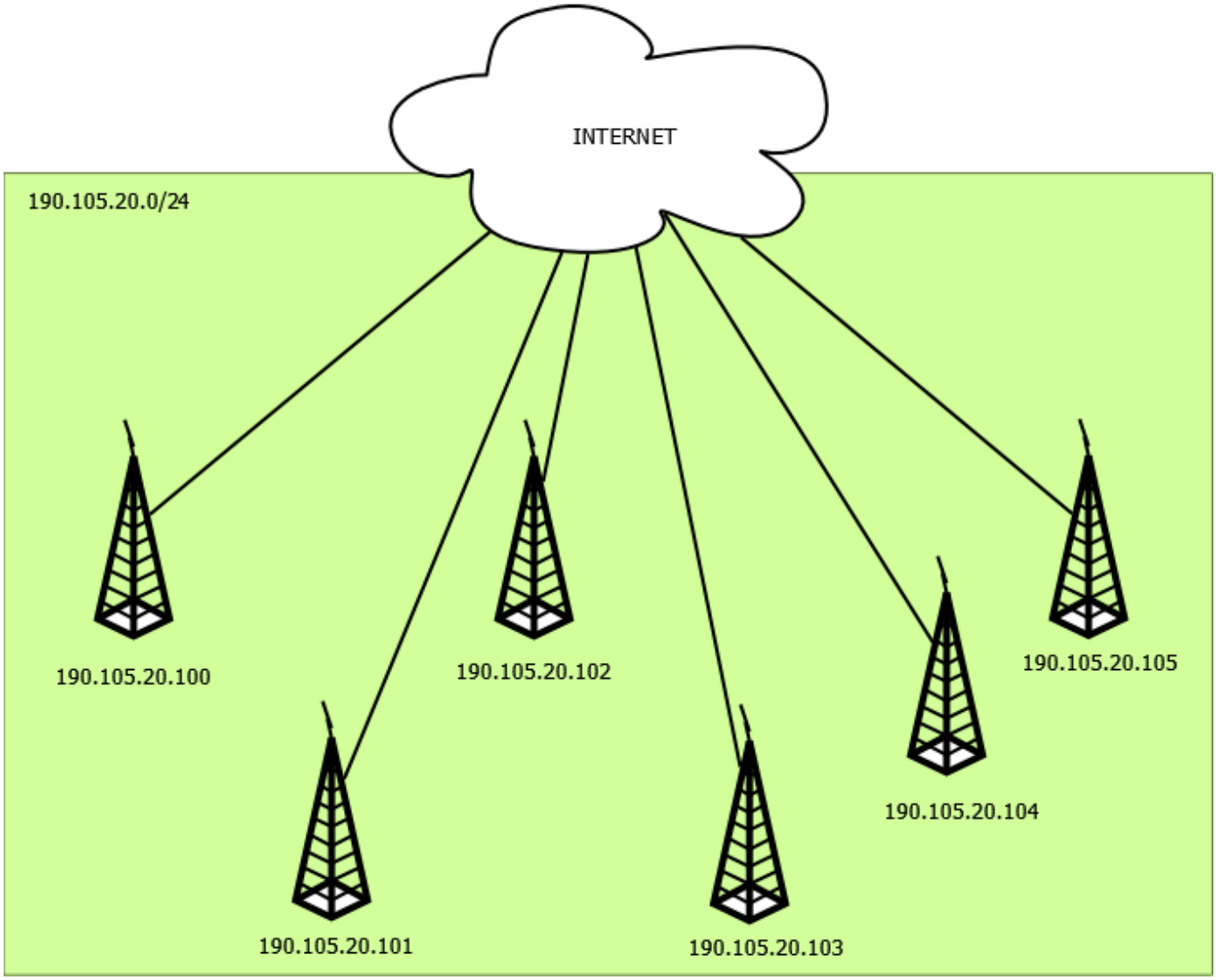
En cuanto al direccionamiento IP público se cuenta con la red 170.210.97.0/26 para la estación central en Santa Rosa, la Pampa, y la red 80.239.202.80/27 para la estación de administración remota en CABA.

Es muy importante considerar que hay que realizar un monitoreo del estado de las estaciones meteorológicas, por lo que debe aplicar al menos una estrategia para conocer el estado de las mismas.

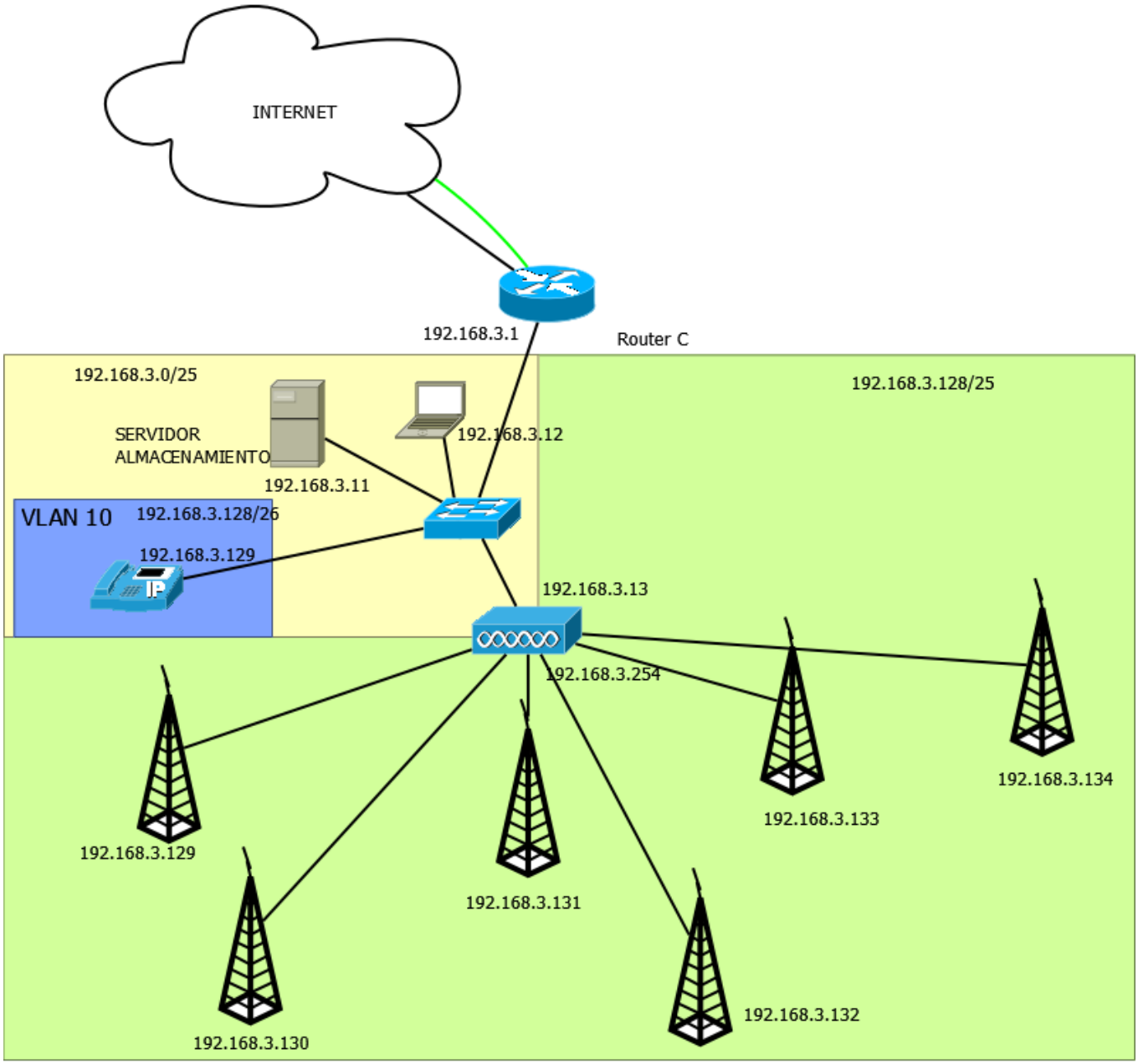
1. Topología Lógica y esquema de direccionamiento



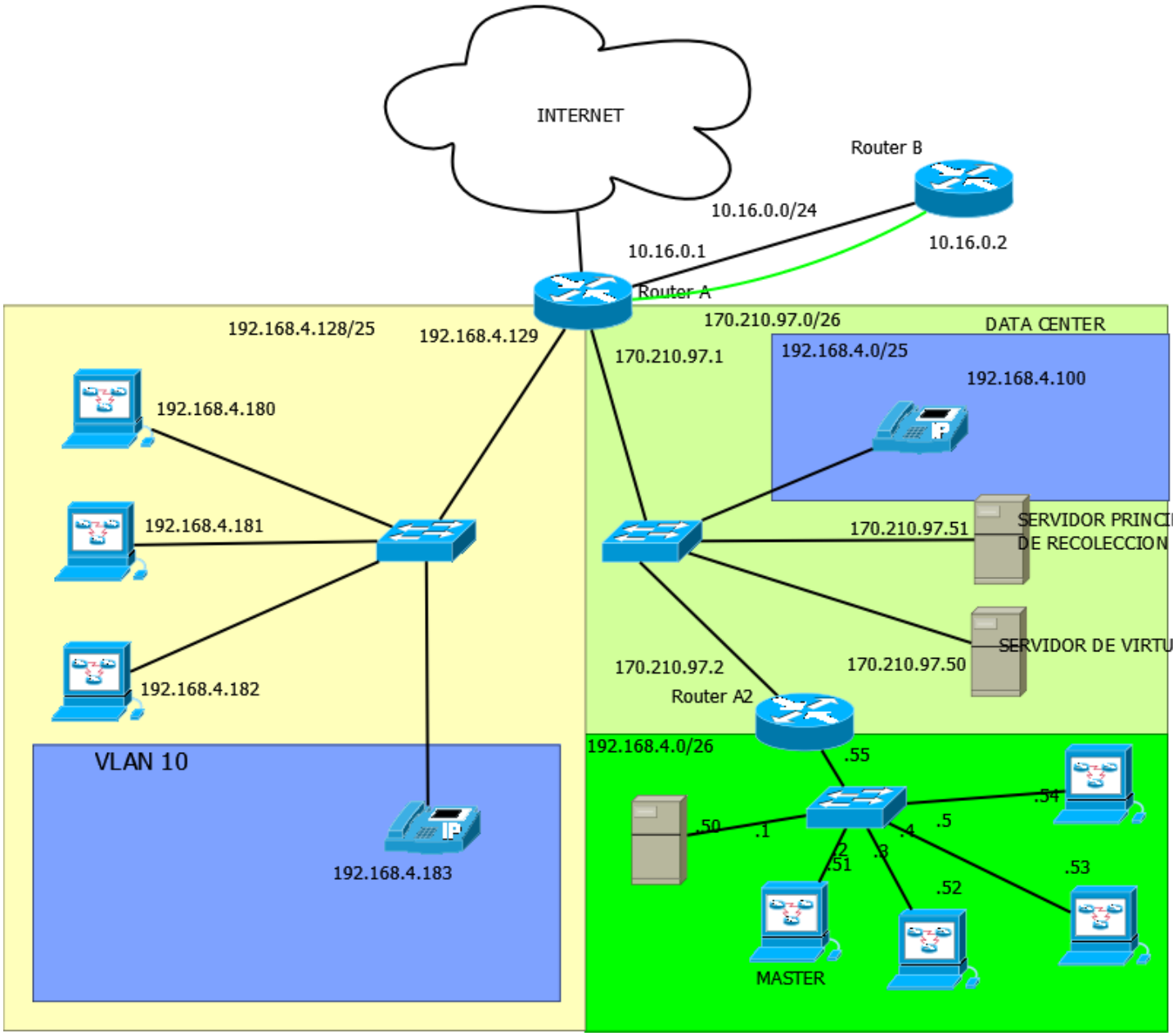
1 Diagrama generico de la interconexion entre las sedes



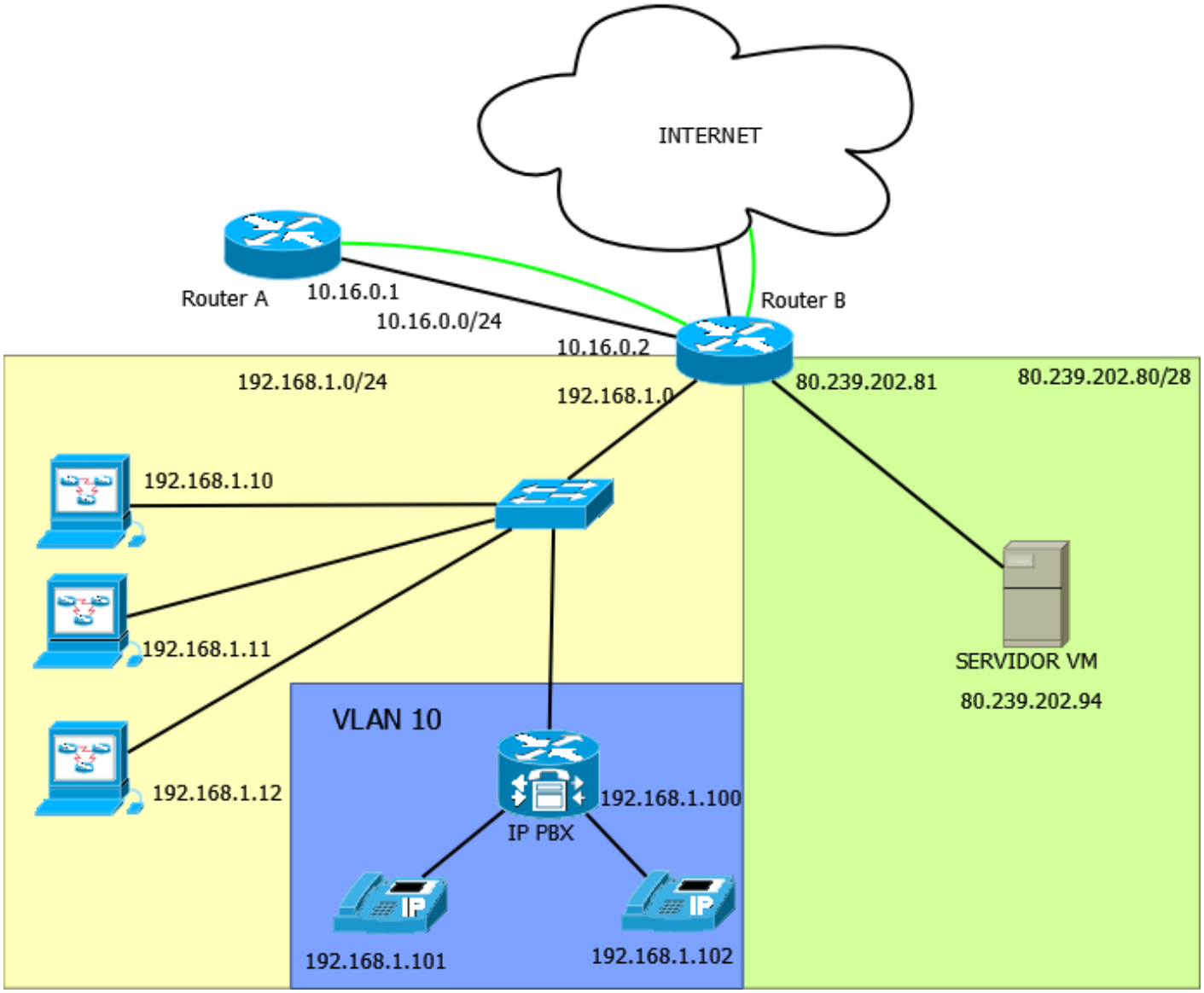
2 Diagrama Campo , Toay



3 Diagrama Logico Campo B, La Capelina



4 Diagrama Logico Estacion Central, Santa Rosa



5 Diagrama Lógico Estación Remota, CABA

2. Esquema de Direccionamiento

Campo A:

Nodos	Dir Red destino	Mascara	Gateway	Descripcion
	170.210.97.0	255.255.255.192	-	Conexión directa con el Servidor de Almacenamiento Principal

Campo B:

Estacion, estacion remota	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.3.0	255.255.255.128	-	Red Local
	default	-	192.168.3.1	

Router C	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.3.0	255.255.255.0	-	Red Local
	10.10.10.0	255.255.255.0	-	Enlace VPN
	default		x.x.x.x	Enlace ISP

Nodos	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.3.128	255.255.255.128	-	Red Local
	default	-	192.168.3.254	

Tel IP	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.3.128	255.255.255.192	-	Red Local
	192.168.1.100	255.255.255.0	192.168.3.1	VLAN CABA
	192.168.4.128	255.255.255.192	192.168.3.1	VLAN Estacion Central

Estacion Central:

Estaciones de trabajo	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.4.128	255.255.255.128	-	red local
	default	-	192.168.4.129	

Tel IP (.101)	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.4.128	255.255.255.128	-	red local
	192.168.4.0	255.255.255.128	192.168.4.129	VLAN Estacion Central
	192.168.1.0	255.255.255.0	192.168.4.129	VLAN CABA
	192.168.3.128	255.255.255.192	192.168.4.129	VLAN campo B

Tel IP (.100)	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.4.0	255.255.255.128	-	red local
	192.168.4.128	255.255.255.128	170.210.97.1	VLAN Estacion Central
	192.168.1.0	255.255.255.0	170.210.97.1	VLAN CABA
	192.168.3.128	255.255.255.192	170.210.97.1	VLAN campo B

Nodos esclavos y servidor de almacenamiento temporal	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.4.0	255.255.255.128	-	red local

Nodo Master	Dir Red destino	Mascara	Gateway	Descripcion
	192.168.4.0	255.255.255.128	-	red local
	170.210.97.0	255.255.255.128	192.168.4.55	red interna
	default	-	192.168.4.55	

Servidor Principal y Servidor de VM	Dir Red destino	Mascara	Gateway	Descripción
	170.210.97.0	255.255.255.192	-	red local
	192.168.4.0	255.255.255.192	-	red de cluster
	default	-	170.210.97.1	

Router A	Dir Red destino	Mascara	Gateway	Descripción
	192.168.4.128	255.255.255.128	-	red local
	170.210.97.0	255.255.255.192	-	red local
	192.168.4.0	255.255.255.192	170.210.97.2	red de nodos
	10.10.11.0	255.255.255.0	-	VLAN

	10.16.0.0	255.255.255.0	-	red de interconexión con router B
	192.168.4.0	255.255.255.128	-	VLAN
	80.239.202.80	255.255.255.240	10.16.0.2	servidor web
	default	-	X.X.X.X	internet

Router A2	Dir Red destino	Mascara	Gateway	Descripción
	192.168.4.0	255.255.255.128	-	red local
	170.210.97.0	255.255.255.192	-	red interna
	80.239.202.80	255.255.255.240	10.16.0.2	servidor web
	default	-	X.X.X.X	internet

CABA:

Servidor VM	Dir Red destino	Mascara	Gateway	Descripcion
	80.239.202.80	255.255.255.240	-	red local
	default	-	80.239.202.81	

Estaciones de trabajo	Dir Red destino	Mascara	Gateway	Descripción
	192.168.1.0	255.255.255.0	-	red local
	80.239.202.80	255.255.255.240	192.168.1.0	red de VM
	default	-	192.168.1.0	internet

Tel IP	Dir Red destino	Mascara	Gateway	Descripción
	192.168.1.0	255.255.255.0	-	red local
	192.168.3.128	255.255.255.192	192.168.1.100	VLAN campo B
	192.168.4.0	255.255.255.128	192.168.1.100	VLAN Estación Central
	192.168.4.128	255.255.255.128	192.168.1.100	VLAN Estación Central

IP PBX	Dir Red destino	Mascara	Gateway	Descripción
	192.168.1.0	255.255.255.0	-	red local
	192.168.3.128	255.255.255.192	192.168.1.0	VLAN campo B
	192.168.4.0	255.255.255.128	192.168.1.0	VLAN Estación Central

	192.168.4.128	255.255.255.128	192.168.1.0	VLAN Estación Central

Router B	Dir Red destino	Mascara	Gateway	Descripción
	192.168.1.0	255.255.255.0	-	red local
	80.239.202.80	255.255.255.240	-	red local
	10.16.0.0	255.255.255.0	-	red de interconexión con router A
	192.168.4.0	255.255.255.192	10.16.0.1	red de nodos
	default	-	X.X.X.X	internet

3. Dispositivos Físicos Requeridos

Campo A:
Módulos de comunicación por GPRS:
http://www.todomicro.com.ar/
SIM800L-GPS-MODULE
390 ARS por unidad.

Campo B:
Antenas WIFI de largo alcance, hasta 30KM:
Modelo: Ubiquiti Rocket M2
Memoria: 64MB SDRAM, 8MB flash
Interface de red: 1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface
Frecuencia de operación: 5470MHz – 5825 MHz
Máximo poder de consumo: 8 watts
Soporte POE
Temperatura de operación: -30C a 75C
Precio por unidad: 235 US

Access Point Inalámbrico:
Modelo: Cisco Aironet 35021
300 Mbps
802.11ac y 802.11n
Precio 139 US

Switches (4):
Modelo: MikroTik CSS326-24G-2S
24 puertos
Permite gestionar el reenvío de puerto a puerto, aplicar filtro MAC, configurar VLAN, duplicar el tráfico, aplicar limitación de ancho de banda e incluso ajustar algunos campos de encabezado MAC e IP.
Precio 139 US

Router A2, B, C:
Modelo Cisco RV325 Dual Gigabit
Velocidad: 10/100/1000Base-T
14 puertos
Soporta encriptación y Firewall SPI
SSL e IPCsec
Alto rendimiento en VPNs
Precio 280 US

Router A:
MikroTik CCR1036-12G-4S
12 puertos Gigabit Ethernet
4 puertos SFP

Hasta 16Gbit/s de throughput
Precio por unidad 995 US

4. SLA para cada enlace

Sera necesario contratar un ISP que cumpla con los requerimientos de servicio que se listan a continuación. Obviamente se elegirá el que los provea al menor precio:

-Un enlace dedicado simétrico con un throughput de 1Gbps medidos en capa de red para brindar todos los servicios que requiera la organización.

-Un enlace de 1Gbps medido en capa de enlace para la intercomunicación entre los distintos centros.

-Disponibilidad mensual no inferior a 99,1% .

-Un RTT entre las sucursales inferior a 50ms y a cualquier parte del mundo inferior a 400ms. El objetivo principal es tener un correcto funcionamiento de Voip aunque es bueno para cualquier aplicación tener menor RTT.

-Jitter inferior a 10%. Como el principal objetivo de la red es la transferencia bulk de datos, no resulta de vital importancia ésta métrica.

-Pedida de paquetes inferior al 0.1. No resulta una métrica tan importante porque el principal objetivo de la red no es la comunicación vía VOIP.

- Para los enlaces entre sedes, como en el caso del Router A con el Router B, será necesario la utilización de un enlace de fibra.

- Y en cuanto a los enlaces dentro de cada cede, deberán ser de tipo Gigabit Ethernet Categoría 6, para permitir el la rápida transferencia de los datos crudos y los procesados hasta 1Gbps.

Puede controlarse las tasas de transferencia del enlace a internet en capa 3 con la herramienta Iperf. El RTT puede ser medido con la herramienta Smokeping seleccionando servidores ubicados en distintas partes del mundo y terminales en otras sucursales. Y se las tasas de trasferencia de los enlaces entre las sedes puede controlarse en capa 2 con la herramienta VNSTAT.

5. Servicios Requeridos

Servidor de Base de Datos

Deberá ser desplegado en la Estación Central en Santa Rosa. Las opciones propuestas son MySQL y PostgreSQL. Ambas elegidas por ser herramientas gratuitas y de reconocido rendimiento y robustez.

Servidor DNS

Para la administración de los subdominios de la organización. La implementación recomendada es BIND, por ser una herramienta robusta, multiplataforma y que se ajusta a las necesidades de la organización. Y como alternativa PowerDNS.

Servidor Web

Se propone la utilización de Apache por ser software libre, por contar con una gran comunidad que da soporte y aporta funcionalidades nuevas constantemente. Como segunda opción puede recomendarse TomCat 8.

Servidor VOIP

Los teléfonos ip distribuidos en la organización se comunicaran utilizando SIP en el puerto UDP 5060. Se propone la utilización de AsteriskNOW implementado sobre Asterisk, el cual es una solución simple y completa que provee las funcionalidades de una PBX.

Servidor Proxy

Se propone la utilización de Squid por ser una herramienta de comprobada robustez y funcionalidad.

Servidor de SSH

Será necesario la implementación de este ser servicio para permitir el acceso remoto al servidor concentrador en el puerto 10022. Y también para acceder al nodo master del cluster.

Servidor de Virtualización

Se propone la utilización del Virtual Machine Monitor “Xen” por proveer aislamiento seguro, control de recursos, garantías de calidad de servicio y migración de máquinas virtuales en caliente. Además de ser de código abierto. Y como alternativa, aunque paga, VMWare ESX. Ambos son virtualizadores de tipo I.

Servidor VPN

Sera necesario la implementación de un servidor VPN para permitir la conexión remota a los host especificados, estos son la Estación Concentradora ubicada en La Capelina y al cluster ubicado en el DataCenter en la Estación Central. Para la implementación se sugiere utilizar OpenVPN.

6. Configuraciones para Implementar VOIp

La central telefónica VOIP será implementado en la estación de monitoreo remoto en CABA. Con lo que debe permitir el registro de los teléfonos ip localizados en las distintas sedes.

Los 2 archivos de configuración más importantes para Asterisk son:

Sip.conf: que define los canales SIP, se configura los clientes SIP

Extensions.conf: que define el comportamiento de las llamadas, los servicios brindados

Para definir nuevas extensiones, en el archivo sip.conf se deben agregar las siguientes líneas:

[Nombre de la extensión]

Parámetro=valor

Por ejemplo, para los teléfonos IP situados en CABA:

```
[101]
 context=default
 type=friend
 callerid="user1.101"
 username=1.101
 secret=pass1101
 nat=no
 canreinvite=yes
 host=dynamic
 qualify=yes

[102]
 context=default
 type=friend
 callerid="user1.102"
 username=1.102
 secret=pass1102
 nat=no
 canreinvite=yes
 host=dynamic
 qualify=yes
```

Luego en el archivo extensión.conf se deben agregar las siguientes líneas, para configurar el DialPlan:

```
exten => 101, 1, Dial(SIP/102,30,Ttm) //permite llamar al 102
exten => 101,1,Hangup //permite terminar la llamada cuando cuelga
exten => 3000,102,Voicemail(3000) //salta el contestador si el destina no está accesible
```

Donde el significado de los parámetros es:

exten => extensión, prioridad, Comando(parámetros)

Estas líneas deberían repetirse para cada teléfono definido en el archivo sip.conf. Es decir para cada uno de los teléfonos IP de la organización.

Para garantizar características de QoS se requiere configurar los routers con con la herramienta Traffic Control (TC), para que prioricen el trafico correspondiente a VOIP. Además es necesario solventar los principales problemas de QoS de una una red de VoIP, que son la Latencia, el Jitter la pérdida de paquetes y el Eco.
En cuanto al jitter y a la latencia, como los enlaces internos en la organización van a ser sobre Gigabit Ethernet Cat6, se espera que dichos parámetros se mantengan en valores aceptables sin mayores complicaciones. Para solventar los posibles problemas de eco, es necesario que el retardo o latencia sea menor a 10ms.
Los routers deberán actuar como firewalls, con lo que deberán clasificar el trafico correspondientes a los dispositivos de comunicación IP con la clase Expedited Forwarding (EF):

```
iptables --append PREROUTING –source
192.168.3.129,192.168.4.100,192.168.4.183,192.168.1.102,192.168.1.101 -j DSCP --set-dscp-class EF
```

Aunque se vuelve sobre este último tema más adelante en el apartado *9. Servicios de Seguridad.*

7. Herramientas de monitoreo

Dispositivos	Parámetros	Herramienta	Umbral	Acción
Servidor WEB	Tasa de transferencia	iperf	18 Mbits/Seg	Notificar via mail al administrador
	Test de estrés	ab	Tiempo promedio de respuesta 200 ms para el 95% de las peticiones	Notificar via mail al administrador
Routers	Latencia, entre los routers.	SmokePing	100ms promedio	Notificar via mail al administrador
	Tasa de transferencia	iperf	18 Mbits/Seg	Notificar via mail al administrador
Cluster A	Tasa de transferencia	iperf	18 Mbits/Seg	Notificar via mail al administrador
Servidor Principal	Latencia, desde los diferentes campos	SmokePing	100ms promedio	Notificar via mail al administrador
	Tasa de transferencia	iperf	18 Mbits/Seg	Notificar via mail al administrador
Servidor de BD	Utilización de disco	script	80%	Notificar via mail al administrador
	Estado del servicio	script	Estado Caído	Reiniciar, servicio y notificar via mail al administrador
Servidor DNS	Estado del servicio	script	Estado Caído	Reiniciar, servicio y notificar via mail al administrador
Servidor VPN	Estado del servicio	script	Estado Caído	Reiniciar, servicio y notificar via mail al administrador

Lo descripto arriba se recomienda ejecutarse sobre un Servidor de monitoreo independiente del resto de dispositivos de la organización. Este es con alimentación eléctrica independiente, sistema de refrigeración también independiente. Es importante mencionar que dicho servidor debe contar con un 99.99% de disponibilidad mínima mensual.
El resto de los dispositivos se comunicaran con el servidor de monitoreo (Managing Entity) utilizando SNMP. Para que éste tome las medidas necesarias. El/Los administradores de red utilizaran NAGIOS para realizar consultas desde el servidor de montioreo. Las estadisticas de monitoreo consultadas de las MIB de los SNMP Agent permitirán determinar anomalías de consumo o de funcionamiento para tomar acciones en consecuencia.

8. Configuración de Servicios

Priorización de tráfico

Para la priorización del trafico correspondiente a VOIp se recomienda la utilización de netfliter (iptables) descripto más adelante en la sección *9. Servicios de Seguridad*, junto a las reglas de control de acceso y filtrado de trafico.
Para definir las disciplinas de encolado se recomienda la utilización de TC (Traffi Control), el método de encolado será Hierarchical Token Bucket (HTB).

NOTA: se toma la interfaz eth0 como la correspondiente a la interfaz de salida para cada paquete.
Para los enlaces a internet correspondientes al router C, router B, y router A. Como para el enlace de interconexión entre los routers A y B:

```
# tc qdisc add dev eth0 root handle 1: htb default 1
# tc class add dev eth0 parent 1: classid 1:1 htb rate 15Mbit ceil 15Mbit
# tc class add dev eth0 parent 1: classid 1:2 htb rate 20Mbit ceil 20Mbit
```

Luego las reglas de clasificación en dichos routers:

```
iptables -t mangle -A POSTROUTING -i eth2 -p udp --dport 5060 -o eth0 \-j CLASSIFY --set-class 1:2
```

Una vez configurado la priorización de tráfico y los mecanismos de encolado, puede verificarse su desempeño utilizando la herramienta netem de TC.

VLAN

Sera necesario la implementación de VLANs en los switches para separar el dominio de broadcast de los teléfonos IP de los demás dispositivos de la red. Permitido asi entre otras cosas reducir el tráfico de la red. Implementado mediante VLANs de nivel 1 o basadas en *port witching*.
Por otro lado, como de momento no existe una gran cantidad de terminales de trabajo, ni se especifica grupos de trabajo o áreas en la que se divide la organización no se ve la necesidad de la creación de más VLANs. Aunque queda planteada la situación para futuras expansiones o reestructuraciones, ya que es una solución escalable.
Tampoco se hace referencia a distintas categorías de usuarios, con lo que si sería aplicable la implementación de VLANs para permitir la comunicación directa en capa 2 a los usuarios de la misma categoría, pero forzarlos a pasar por un router en caso de solicitar la comunicación entre grupos. Dando así una capa más de seguridad a la protección de la información sensible.

9. Servicios de Seguridad

Seguridad SSH

Para las conexiones remotas mediante SSH se deben tomar en cuenta varias cuestiones de seguridad a configurar en el servidor SSH:

- Elegir un puerto de escucha al azar, no el seleccionado por defecto.
- Limitar el tiempo que se muestra la pantalla de login, mediante el parámetro
  LoginGraceTime
- Quitarle al usuario root los permisos sobre SSH
- Limitar la cantidad de intentos fallidos por usuario, mediante el parámetro
  MaxAuthTries
- Limitar la cantidad de conexiones simultaneas
  MaxStartups
- Indicar los usuarios que tiene permitido la conexión mediante SSH
  AllowUsers pedro@<host o red de acceso>

Configuración de Firewall

Por otro lado no es necesario, ni recomendable que se pueda acceder al Servidor de Almacenamiento Principal ni al cluster de propcesamiento ubicados en el datacenter, a través de internet, ni que tenga salida hacia allí. Por lo que se propone configurar un Firewall en el Router A para que filtre el contenido.

Para todos los routers:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
192.168.4.3
############################################################################ #
Eliminar todas las reglas existentes
############################################################################
iptables -F
iptables -X
iptables -Z

## Aceptar paquetes de conexiones ya establecidas
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

## SMTP, POP3, IMAP
```

```
iptables -A FORWARD -i eth0 -s 170.210.97.0/26 -p tcp -m multiport --dports 25,110,143 --syn -j ACCEPT

## DNS
iptables -A FORWARD -i eth0 -s 172.210.97.0/26 -d 172.210.96.1 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth1 -d 172.210.97.0/26 -s 172.210.96.1 -p udp --sport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 172.210.97.0/26 -d 172.210.96.1 -p tcp --dport 53 --syn -j ACCEPT

## NTP
iptables -A FORWARD -i eth0 -s 172.210.97.0/26 -d 172.210.96.1 -p udp --dport 123 -j ACCEPT
iptables -A FORWARD -i eth1 -d 172.210.97.0/26 -s 172.210.96.1 -p udp --sport 123 -j ACCEPT

## HTTP/S
iptables -A FORWARD -i eth0 -s 172.210.97.0/26 -p tcp -m multiport --dports 80,443 --syn -j ACCEPT

############################################################################## #
Permitir hacer pring desde cualquier ubicación interna de la organización
##############################################################################
iptables -A OUTPUT -p icmp -j ACCEPT
iptables -A INPUT -s 172.210.96.0/26 \ 192.168.4.128/25 \ 192.168.4.0/26 \ 80.239.202.80/28 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -s 172.210.96.0/26 \ 192.168.4.128/25 \ 192.168.4.0/26 \ 80.239.202.80/28 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -s 172.210.96.0/26 \ 192.168.4.128/25 \ 192.168.4.0/26 \ 80.239.202.80/28 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -s 172.210.96.0/26 \ 192.168.4.128/25 \ 192.168.4.0/26 \ 80.239.202.80/28 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -p icmp --icmp-type echo-reply -j ACCEP

##############################################################################
###Permitir que el servidor de VoIP provea servicio a teléfonos en las redes 192.168.4.0/25, 192.168.4.128/25, 192.168.1.0/24 y 192.168.3.0/25. El servidor VOIP se encuentra en 192.168.1.100 en CABA
##############################################################################

iptables -A FORWARD -s 192.168.4.0/25 \ 192.168.4.128/25 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25  -d 192.168.1.100 --dport 5060 -p tcp --syn -j ACCEPT
iptables -A FORWARD -d 192.168.4.0/25 \ 192.168.4.128/25 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -s 192.168.1.100 --dport 5060 -p tcp --syn -j ACCEPT
iptables -A FORWARD -s 192.168.4.0/25 \ 192.168.4.128/25 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -d 192.168.1.100 --dport 5060 -p udp -j ACCEPT
iptables -A FORWARD -d 192.168.4.0/25 \ 192.168.4.128/25 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25 -s 192.168.1.100 --sport 5060 -p udp -j ACCEPT

# permitir el tráfico entre las redes locales
iptables -A FORWARD -s 172.210.96.0/26 \ 192.168.4.128/25 \ 192.168.4.0/26 \ 80.239.202.80/28 \ 192.168.1.0/24 \ 192.168.3.0/25 \ 192.168.3.128/25  -j ACCEPT
```

```
## SSH
iptables -A FORWARD -d 92.168.4.0/26 --dport 22 -p tcp --syn -j ACCEPT
iptables -A FORWARD -d 192.168.3.11 --dport 10022 -p tcp --syn -j ACCEPT
```

Router A:

```
## permitir la entrada de datos de los campos de recolección
iptables -P INPUT –d 170.210.97.51 –s 192.168.3.0/25 \ 192.168.3.128/25  \ 190.105.20.0/24 –j
ACCEPT

## DNS
iptables -A OUTPUT -d 192.168.4.3 -p udp --dport 53 -j ACCEPT
iptables -A INPUT -s 192.168.4.3 -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 192.168.4.3 -p tcp --dport 53 --syn -j ACCEPT

## NTP
iptables -A OUTPUT -d 192.168.4.183 -p udp --dport 123 -j ACCEPT
iptables -A INPUT -s 192.168.4.183 -p udp --sport 123 -j ACCEPT

## SMTP
iptables -A OUTPUT -d 192.168.4.3 -p tcp --dport 25 --syn -j ACCEPT

## HTTP/S
iptables -A FORWARD -i eth2 -d 170.210.97.50 -m multiport --dport 80,443 -p tcp --syn -j
ACCEPT
iptables -A INPUT -i eth2 -d 170.210.97.50 -m multiport --dport 80,443 -p tcp --syn -j ACCEPT
iptables -A OUTPUT -i eth2 -d 170.210.97.50 -m multiport --dport 80,443 -p tcp --syn -j
ACCEPT
```

Router B:

```
## DNS
iptables -A OUTPUT -d 80.239.202.94 -p udp --dport 53 -j ACCEPT
iptables -A INPUT -s 80.239.202.94 -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 80.239.202.94 -p tcp --dport 53 --syn -j ACCEPT

## NTP
iptables -A OUTPUT -d 80.239.202.94 -p udp --dport 123 -j ACCEPT
iptables -A INPUT -s 80.239.202.94 -p udp --sport 123 -j ACCEPT

## HTTP/S
iptables -A FORWARD -i eth2 -d 80.239.202.94 -m multiport --dport 80,443 -p tcp --syn -j
ACCEPT
iptables -A INPUT -i eth2 -d 80.239.202.94 -m multiport --dport 80,443 -p tcp --syn -j ACCEPT
iptables -A OUTPUT -i eth2 -d 80.239.202.94 -m multiport --dport 80,443 -p tcp --syn -j
ACCEPT

##########################################################################Permitir
mensajes ICMP Echo Request y Echo Reply desde Internet hacia el Servidor Web, limitando
las peticiones a un máximo de 10 por segundo.
##########################################################################
```

```
iptables -A FORWARD -d 80.239.202.94 -i eth2 -p icmp --icmp-type echo-request -m limit --limit 10/s -j ACCEPT
iptables -A FORWARD -d 80.239.202.94 -i eth2 -p icmp --icmp-type echo-reply -m limit --limit 10/s -j ACCEPT
iptables -A FORWARD -d 80.239.202.94 -o eth2 -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A FORWARD -d 80.239.202.94 -o eth2 -p icmp --icmp-type echo-request -j ACCEPT
```

Router A2:

A este dispositivo solo será accedido por el servidor web y por un administrador de manera remota para su administración.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
192.168.4.3
############################################################################ #
Eliminar todas las reglas existentes
############################################################################
iptables -F
iptables -X
iptables -Z

## permitir conexión con el servidor web de la organización
iptables -P INPUT –d 192.168.4.51 –s 80.239.202.94 –j ACCEPT
iptables -P OUTPUT –d 192.168.4.51 –s 80.239.202.94 –j ACCEPT

## permitir comunicación con el servidor de almacenamiento principal
iptables -P INPUT –d 192.168.4.0/26 –s 170.210.97.51 –j ACCEPT
iptables -P OUTPUT –d 192.168.4.0/26 –s 170.210.97.51–j ACCEPT
iptables -P FORWARD –d 192.168.4.0/26 –s 170.210.97.51 –j ACCEPT
```

Una vez configurado todos los firewalls se recomienda validar dichas configuraciones con iptraf. Intentar acceder desde afuera, e intentarlo desde una estación interna. Para validar todas las reglas creadas.

VPN

Esta red conecta usuarios fuera de la organización de manera remota a la Estación Concentradora y a al cluster de procesamiento a través de una red pública (Internet), pero asegurando los servicios de seguridad: autenticidad, confidencialidad e integridad ya que opera sobre TLS.
En el diagrama, puede verse dicha red virtual marcada con una línea verde.
La red virtual a crear será la 10.10.10.0/24 para el acceso a la Estación Concentradora, y la ip del servidor será la 10.10.10.1. Y la red 10.10.11/24 para el acceso al cluster de la Estación Central, cuyo servidor tendrá la ip 10.10.11.1.
Por otro lado como la VPN se implementa con el objetivo de soportar la conexiones remotas mediante SSH, ya de por si por la utilización de éste protocolo obtendremos autenticidad e integridad de los datos, ya que utiliza claves públicas para la autenticación en la maquina remota, y además la conexión viaja cifrada.

10. Mecanismos de disponibilidad y tolerancia a fallos

Para garantizar el servicio de disponibilidad es de imperiosa necesidad la implementación de servicios y equipos redundantes. Para que ante la falla de algún dispositivo de la red, la performance de la misma no se vea mermada, o que directamente quede inutilizada.

Por lo dicho es recomendable implementar:

- Servidores redundantes para cada servicio activo en la organización: tener servicios redundantes de DNS, Web Server, Server VOIP, y demás servicios necesarios.

- Base de datos replicadas en uno o varios nodos esclavos para proveer el mayor grado de disponibilidad posible.

- En el cluster, contar con mecanismos de protección de datos ante posibles fallas y contar con servidor de almacenamiento replicado. Así como un balanceador de carga entre ambos nodos maestros (el principal y el replicado).

- Por cada dispositivo de interconexión y cada dispositivo critico en el funcionamiento de la organización, como ser el Servidor de Almacenamiento Principal, Servidor Concentrador, Servidor Web, los Servidores de Virtualización y el cluster de procesamiento, se recomiendo contar con fuentes de alimentación redundantes, por ejemplo con unidades UPS. Y generadores eléctricos en el caso de fallas eléctricas que afecten a una sede por completo, y alimenten a dichas UPS.

- Se recomienda que los lugares físicos donde se encuentra el datacenter cuente con:

    - Espacio adecuado para la correcta distribución de los dispositivos
    - Mecanismos de ventilación para mantener la temperatura a valores recomendados. Al igual que en casos anteriores, también es recomendable que los mecanismos de ventilación sean redundantes, para que ante la falla de uno de ellos los servicios puedan seguir funcionando.
    - Contar con mecanismos de seguridad que restrinjan el acceso al mismo. Lo mismo puede sugerirse para el Servidor Concentrador ubicado en La Capelina. Para ello es recomendable la elaboración de un documento con las políticas de seguridad de la organización, donde se especifique por ejemplo las normativas a seguir para permitir conexiones VPN a la organización.

11. Configuraciones y suposiciones realizadas

Es requisito que el Routers C cuente con una dirección IP pública, no especificada, para permitir el ruteo a través de internet. Por esta razón será necesario que dicho router junto con el router A implementen mecanismos para hacer NAT.
Utilizaremos un mecanismo de NAT dinámico:

NAT Router A:

Source NAT:

Pre-NAT		Post-NAT	
Puerto	IP origen	Puerto	IP origen
80	192.168.3.128/25	80	x.x.x.x
443	192.168.3.128/25	443	x.x.x.x
53	192.168.3.128/25	53	x.x.x.x
25	192.168.3.128/25	25	x.x.x.x
123	192.168.3.128/25	123	x.x.x.x
110	192.168.3.128/25	110	x.x.x.x
10022	192.168.3.128/25	10022	x.x.x.x
5060	192.168.3.128/25	5060	x.x.x.x

Destination NAT:

Pre-NAT		Post-NAT	
Puerto destino	IP destino	Puerto destino	IP destino
80	192.168.3.128/25	80	x.x.x.x
443	192.168.3.128/25	443	x.x.x.x
53	192.168.3.128/25	53	x.x.x.x
25	192.168.3.128/25	25	x.x.x.x
123	192.168.3.128/25	123	x.x.x.x
110	192.168.3.128/25	110	x.x.x.x
10022	192.168.3.128/25	10022	x.x.x.x
5060	192.168.3.128/25	5060	x.x.x.x

NAT Router C:

Source NAT:

Pre-NAT		Post-NAT	
Puerto	IP origen	Puerto	IP origen
80	192.168.3.0/24	80	x.x.x.x
443	192.168.3.0/24	443	x.x.x.x

53	192.168.3.0/24	53	x.x.x.x
25	192.168.3.0/24	25	x.x.x.x
123	192.168.3.0/24	123	x.x.x.x
110	192.168.3.0/24	110	x.x.x.x
10022	192.168.3.0/24	10022	x.x.x.x
5060	192.168.3.0/24	5060	x.x.x.x

Destination NAT:

Pre-NAT		Post-NAT	
Puerto destino	IP destino	Puerto destino	IP destino
80	192.168.3.0/24	80	x.x.x.x
443	192.168.3.0/24	443	x.x.x.x
53	192.168.3.0/24	53	x.x.x.x
25	192.168.3.0/24	25	x.x.x.x
123	192.168.3.0/24	123	x.x.x.x
110	192.168.3.0/24	110	x.x.x.x
10022	192.168.3.0/24	10022	x.x.x.x
5060	192.168.3.0/24	5060	x.x.x.x

Por otro lado las estaciones meteorológicas del campo A, se conectan directamente a internet, por lo que se asume que cuentan con direcciones IP públicas, asumiendo que se asignó el bloque de direcciones: 190.105.20.0/24.