****

**Redes de Computadoras**

Proyecto Integrador

Alumnos:

Campos Alan

Dores Joaquin

Comisión 1 Grupo 13

**Índice temático**

Introducción

Marco Teórico

Desarrollo

Tabla de IPs estáticas

Diseño capa física

Diseño capa de enlace

Diseño capa de red

Diseño capa de transporte

Diseño capa de aplicación

Conclusión

**1.Introducción**

A lo largo de este informe se busca detallar la implementación y desarrollo de un proyecto de red para la petrolera “PetroGlobal S.A.”, la cual tiene múltiples sedes, cada una con sus especificaciones y requerimientos de servicios. Se diseñó la red considerando sus 3 sedes, la principal ubicada en CABA, otra ubicada en San Juan, y una última en Mendoza, siguiendo las especificaciones proporcionadas por el cliente y añadiendo ciertas características para mejorar la precisión y funcionalidad de dicha red.

Comenzando con la sede de CABA, contamos con la disponibilidad de 4 pisos del edificio, el piso 10, el piso 7, el piso 2 y el piso 1. En el décimo piso se encuentra el Centro de Datos, con 10 Racks y capacidad para alojar hasta 100 servidores; entre ellos tenemos el Local Resolver, el Servidor Web principal de la petrolera, 1 servidor de Correo y un servidor Web seguro delegado a la Intranet del departamento de administración, entre otros. En este piso también se encuentra el departamento de distemas, que dispone de 23 puestos de trabajo; el directorio,con 10 puestos de trabajo; el departamento de prensa, con otros 10 puestos de trabajo, el departamento de diseño, con 5 puestos de trabajo; el departamento de ingeniería, con 7 puestos de trabajo y el departamento de contabilidad, con unos 9 puestos de trabajo disponibles.

Pasando al séptimo piso, contamos con gerentes que posee 6 puestos de trabajo, departamento de marketing con 5 puestos de trabajo, facturación y liquidaciones con 6 puestos y el departamento de RRHH con 4 puestos de trabajo.

Además, el segundo piso cuenta con el departamento de mantenimiento, el cual dispone de 5 puestos de trabajo y el departamento de compras con 5 puestos de trabajo.

Por último, en el primer piso se encuentra la sala de reuniones, con 8 puestos de trabajo, un SUM con 30 puestos de trabajo y un departamento de atención al público con 5 puestos de trabajo.

En la sede de San Juan tenemos 2 pisos, en el primero se encuentran el SUM, con una capacidad para 20 puestos de trabajo; también se encuentra el departamento de atención al público, que dispone de 5 puestos de trabajo. Luego, en el 2do piso se encuentra el departamento de administración, con 4 puestos de trabajo, el departamento de comercio, con 3 puestos de trabajo y por último, se encuentra el cuarto de servidores, que almacena el servidor DNS primario y el secundario de prensa, el servidor Web de San Juan y un servidor destinado a DHCP.

En la sucursal de Mendoza se dispone únicamente del 2do piso del edificio, allí encontramos un SUM, con 10 puestos de trabajo, un Departamento comercial, que dispone con 3 puestos de trabajo, un departamento de administración, con 2 puestos de trabajo, el departamento de tráfico, con 5 puestos de trabajo y por último una sala de servidores con 4 servidores.

Las sucursales de Mendoza y de San Juan poseen ambas un solo segmento de red, mientras que la sede de CABA las redes se encuentran segmentadas en redes virtuales (VLANs) de acuerdo a los siguientes grupos de pertenencia:

1. Administración: Facturación y Liquidaciones, Departamento de Contabilidad, Atención al Público, Departamento de RRHH y Departamento de Compras
2. Logística: Departamento de Prensa, Departamento de Diseño, Departamento de Ingeniería y Departamento de Mantenimiento.
3. Gerencia: Directorio, Gerentes, Departamento de Marketing, Sala de Reuniones y SUM.
4. Departamento de Sistemas y Centro de Datos: Tienen su VLAN propia.

La planificación y el desarrollo de la red fue llevado a cabo en el emulador de Cisco Packet Tracer, donde pudimos implementar todos los detalles de la red de forma más simple y tener una visión gráfica y completa de esta, desarrollando todas las características necesarias de cada elemento importante de la red, dejando de lado los elementos a repetir, como podría ser por ejemplo, la cantidad de puestos de trabajo de cada área, dejando de manera graficada una cantidad representativa de estos por cada sala.

Por último, por una cuestión de organización, decidimos modificar la cantidad de PCs y servidores en los diferentes departamentos. Por ejemplo, el departamento SUM correspondiente a la sede de CABA posee 30 puestos de trabajo, pero, para simplificarlo, únicamente se muestra el primer y el último puesto de trabajo.

**2. Marco Teórico**

**DNS**

El DNS, o Sistema de Nombres de Dominio, es una tecnología esencial en Internet que traduce los nombres de dominio que usamos a diario, como www.ejemplo.com, en direcciones IP numéricas que las computadoras pueden entender y utilizar para comunicarse entre sí. Funciona como una agenda telefónica de Internet, permitiéndonos acceder a sitios web y servicios en línea mediante nombres fáciles de recordar, permitiendo que las personas accedan a sitios web y recursos en línea a través de nombres de dominio en lugar de tener que recordar direcciones IP numéricas complejas. Gracias al DNS, navegar por Internet, enviar correos electrónicos y realizar otras actividades en línea es mucho más sencillo y eficiente.

**HTTP**

HTTP o HyperText Transfer Protocol es un protocolo de comunicación utilizado en la World Wide Web (WWW) y en otros sistemas de información hipermedia.

Fue diseñado para permitir la transferencia de datos, especialmente documentos web y recursos relacionados, entre un cliente (por lo general, un navegador web) y un servidor web. HTTP es un protocolo sin estado, lo que significa que cada solicitud y respuesta entre el cliente y el servidor es independiente, sin conocimiento de interacciones anteriores.

HTTP es esencial para la navegación web y el intercambio de información en línea. A lo largo del tiempo, ha evolucionado con nuevas versiones, como HTTP/1.1 y HTTP/2, para mejorar el rendimiento y la eficiencia en la transferencia de datos en la web.

**HTTPS**

HTTPS o Hypertext Transfer Protocol Secure es una extensión del protocolo HTTP diseñada para proporcionar seguridad y privacidad en las comunicaciones en línea. HTTPS se utiliza ampliamente en la World Wide Web para garantizar que los datos transmitidos entre el cliente (por ejemplo, un navegador web) y el servidor web estén cifrados y protegidos

contra posibles amenazas de seguridad.

La implementación de HTTPS es esencial para proteger la privacidad y la seguridad de los usuarios en línea

**DHCP**

El Protocolo de Configuración Dinámica de Host (DHCP) se encarga de asignar automáticamente direcciones IP, máscaras de subred y otros parámetros de configuración de red a los dispositivos que se conectan a una red. Su función principal es simplificar la administración de redes, eliminando la necesidad de configurar manualmente los parámetros descritos en cada dispositivo, y disminuyendo la posibilidad de errores ya que se adapta a dispositivos que se conectan y desconectan con frecuencia.

**SMTP**

SMTP, o Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol), es un protocolo estándar de Internet utilizado para enviar y recibir correos electrónicos. Se encarga principalmente del envío de mensajes desde el cliente de correo electrónico del remitente hasta el servidor de correo del destinatario. SMTP define cómo se comunican los servidores de correo entre sí para transmitir mensajes de manera confiable y eficiente. Este protocolo funciona en conjunto con otros protocolos, como IMAP o POP3, que se utilizan para la recuperación de correos electrónicos desde el servidor al cliente del usuario final.

**POP**

El Protocolo de Oficina de Correos, conocido como POP (Post Office Protocol), es un protocolo de Internet utilizado para recuperar correos electrónicos desde un servidor remoto al cliente de correo electrónico del usuario. La versión más comúnmente utilizada es POP3 (Post Office Protocol version 3).

POP3 permite a los usuarios descargar sus mensajes de correo electrónico a su dispositivo local y, generalmente, elimina los correos del servidor una vez descargados, aunque muchas configuraciones permiten mantener una copia en el servidor. Este protocolo es útil para acceder a los correos sin necesidad de estar siempre conectado a Internet, ya que los mensajes se almacenan localmente en el dispositivo del usuario.

**UDP**

UDP, o Protocolo de Datagrama de Usuario (User Datagram Protocol), es uno de los principales protocolos de la suite de protocolos de Internet. UDP se utiliza para enviar mensajes, conocidos como datagramas, entre computadoras en una red. A diferencia de TCP (Transmission Control Protocol), UDP es un protocolo sin conexión, lo que significa que no establece una conexión previa entre el emisor y el receptor antes de enviar datos.

Las principales características de UDP incluyen:

Sin Conexión: No establece una conexión antes de enviar datos, lo que permite una comunicación más rápida.

No Fiable: No garantiza la entrega de los paquetes de datos ni su recepción en el orden correcto. No realiza retransmisiones de datos perdidos.

Ligero: Tiene una sobrecarga mínima en comparación con TCP, lo que lo hace ideal para aplicaciones que requieren velocidad y eficiencia.

Usos Comunes: Es frecuentemente utilizado en aplicaciones donde la velocidad es crítica y se pueden tolerar algunas pérdidas de datos, como en transmisión de video y audio en tiempo real, juegos en línea, y consultas rápidas de red.

En resumen, UDP es un protocolo rápido y eficiente para la transmisión de datos, adecuado para situaciones donde la baja latencia es más importante que la fiabilidad.

**TCP**

TCP, o Protocolo de Control de Transmisión, es uno de los principales protocolos de la suite de protocolos de Internet, utilizado para garantizar la entrega confiable y ordenada de datos entre aplicaciones que se ejecutan en diferentes dispositivos. TCP establece una conexión antes de transmitir datos, asegurando que tanto el emisor como el receptor estén listos para comunicarse. Este protocolo garantiza la entrega sin errores y en el orden correcto, retransmitiendo paquetes si es necesario, y gestionando el flujo y la congestión de datos para evitar sobrecargas en la red.

Gracias a su fiabilidad, TCP es fundamental para aplicaciones que requieren una transferencia de datos segura y precisa, como la navegación web, el correo electrónico y la transferencia de archivos. Además, TCP divide los datos en segmentos manejables para su envío y los vuelve a ensamblar en el destino, asegurando una comunicación efectiva y ordenada en la red.

**IP**

IP, o Protocolo de Internet, es el protocolo central en la suite de protocolos de Internet, responsable de enviar y recibir datos entre dispositivos en una red. Cada dispositivo tiene una dirección IP única que permite identificarlo y dirigir los datos correctamente. IP encapsula los datos en paquetes, fragmenta aquellos demasiado grandes y los reensambla en el destino. Además, IP determina la ruta que los paquetes deben seguir a través de la red, utilizando routers para dirigir el tráfico. Existen dos versiones principales de IP: IPv4, con direcciones de 32 bits, e IPv6, con direcciones de 128 bits, que soporta una mayor cantidad de dispositivos.

**Cable de Fibra Óptica**

Cable de transmisión mediante una onda de luz en fibra de vidrio. Estos dispositivos y tecnologías se encargan del transporte correcto de información a lo largo de las diferentes sedes, conectando así los equipos a los diferentes DNS y servidores alojados o solicitados en la red.

**Cable de Cobre Directo (FastEthernet)**

Un cable de cobre directo es un cable Ethernet diseñado para conectar dispositivos que requieren una comunicación directa, como un computador a un switch.

**Conexión Directa:**

Este tipo de cable se utiliza para conectar dispositivos del mismo tipo, como un computador a un switch, sin necesidad de un dispositivo intermedio como un concentrador o un router.

**Cable de Cobre Cruzado**

Un cable de cobre cruzado es un tipo de cable Ethernet diseñado para conectar dispositivos del mismo tipo, como dos computadoras o dos switches, sin necesidad de un dispositivo intermedio como un concentrador o un router.

Propósito: Facilita la comunicación directa entre dispositivos idénticos al intercambiar las señales de transmisión y recepción, permitiendo una conexión punto a punto.

**VLAN**

VLAN es una forma de crear redes lógicas independientes dentro de una red física. Permite agrupar dispositivos en la misma red, aunque no estén físicamente conectados.

Objetivo: Mejorar la administración de la red, la seguridad y el rendimiento al segmentar el tráfico en grupos lógicos.

Cómo funciona: Se asignan etiquetas a los paquetes de datos para identificar a qué VLAN pertenecen. Los dispositivos en la misma VLAN pueden comunicarse directamente, incluso si están en ubicaciones físicas diferentes.

Beneficios:

* Segmentación: Permite dividir la red en grupos lógicos para mejorar el rendimiento y la seguridad.
* Administración eficiente: Facilita la gestión de la red al organizar dispositivos lógicamente en lugar de depender de la topología física.
* Seguridad mejorada: Limita la comunicación entre dispositivos a la misma VLAN, reduciendo la exposición a posibles amenazas.

Para no tener que establecer un enlace diferente por cada VLAN se pueden configurar enlaces ‘trunk’ entre los diferentes Switches, junto al router.

**NAT (Dinámico / Estático)**

NAT es una técnica que permite traducir direcciones IP en un paquete de datos mientras se mueven a través de un enrutador o firewall, cambiando las direcciones de origen y/o destino.

Propósito: Permite conservar direcciones IP públicas, ya que múltiples dispositivos internos pueden compartir una única dirección IP pública.

Tipos de NAT:

* Estático: Asigna una dirección IP privada específica a una dirección IP pública.
* Dinámico: Asigna direcciones IP privadas de un grupo compartido a medida que se necesitan.

**PAT**

PAT es una extensión de NAT que utiliza números de puerto para permitir que varios dispositivos internos compartan una única dirección IP pública, optimizando la gestión de direcciones en redes.

**Ruteo (Estático)**

Ruteo es la determinación de la ruta óptima que los paquetes de datos deben seguir desde un dispositivo de origen hasta un dispositivo de destino a través de una red.

Objetivo: Garantizar la entrega eficiente de datos al seleccionar el camino más eficaz entre redes interconectadas.

Tabla de Ruteo: Los routers mantienen tablas de ruteo que almacenan información sobre las redes disponibles y las rutas hacia ellas. Estas tablas se utilizan para tomar decisiones de reenvío de paquetes.

Rutas Estáticas: Configuradas manualmente por el administrador de red.

Métricas de Ruteo: Los routers utilizan métricas, como la distancia administrativa y el costo, para determinar la mejor ruta entre redes.

**Subneteo**

Subneteo es el proceso de dividir una red IP en subredes más pequeñas para mejorar la eficiencia en el uso de direcciones IP y optimizar el rendimiento de la red.

Objetivo: Maximizar el número de redes disponibles y reducir el tamaño de las mismas para mejorar la gestión de direcciones IP y limitar el tráfico de la red.

Cómo funciona: Se toma una red IP grande y se divide en segmentos más pequeños llamados subredes. Cada subred tiene su propia gama de direcciones IP y se gestiona como una red independiente.

Máscara de subred: Se utiliza una máscara de subred para determinar qué parte de la dirección IP pertenece a la red y qué parte está reservada para identificar dispositivos dentro de la subred.

Notación CIDR: Se utiliza la notación CIDR (Classless Inter

* Domain Routing) para representar direcciones IP y máscaras de subred de manera más eficiente.

Beneficios:

* Eficiencia en el uso de direcciones IP: Permite asignar direcciones de manera más precisa, evitando el desperdicio de direcciones IP.
* Control de tráfico: Facilita la gestión del tráfico al limitar la propagación de broadcasts y mejorar la seguridad al segmentar la red.

**Firewall IPv4**

Un firewall IPv4 monitorea y controla el tráfico de red, permitiendo o

bloqueando paquetes según reglas predefinidas.

Reglas de Filtrado: Las reglas determinan qué tráfico se permite o se

bloquea según criterios como direcciones IP, puertos y protocolos.

**Redes Wireless**

Las redes inalámbricas son fundamentales para la conectividad sin cables,

ofreciendo movilidad y acceso remoto a diversos dispositivos y servicios.

**3.Desarrollo**

El proyecto consta del desarrollo de una red para la empresa Petro Global.S.A. que contemple sus 3 sedes en el país, por lo que el primer paso fue dividir la sucursal en sus respectivas sedes, y comenzamos a poner todos los equipos y medios físicos necesarios para la red, según el cliente lo pidió; teniendo en cuenta lo previamente realizado en la sede de San Juan, hecho en el proyecto inicial.

Diseño capa física

Comenzamos por colocar un router en cada sede y conectandolos para ya establecer una comunicación interna entre las sedes; del router de CABA, que pasa a ser la sede central de la empresa, sale la conexión a Internet mediante la conexión a un router ISP previamente establecido por el proveedor de Internet, que a su vez conecta a los servidores DNS de root, ar, y edu.ar.

Las conexiones punto a punto entre los routers de las tres sedes y la conexión con el proveedor de internet la hicimos con cable de fibra óptica para que pudieran conectarse los 3 sniffers que se usarían para monitorear el tráfico de las redes. Para los vínculos verticales de la red utilizamos cableado de fibra óptica para disminuir los errores a capa de enlace, ya que no son afectados por ondas electromagnéticas aumentando así la confiabilidad de nuestra red. Las conexiones entre los switches y los dispositivos se realizaron con cables Fast Ethernet.

Luego de conectar los routers, seguimos con la distribución de la red mediante los switches; para ello, cada una de las oficinas en cada sede cuenta con un switch correspondiente dependiendo de la cantidad de equipos necesarios(y con ello según la necesidad de equipos de trabajo se usaron switchs vacíos con 10 bocas o de 24 bocas Fast Ethernet más 2 Gigabyte Ethernet para comunicar los routers). Considerando la distribución de las oficinas, los switchs de oficinas se vinculan en cascada al que se encuentra en el rack principal del piso.

En el centro de datos ubicado en CABA, buscamos representar la cantidad de espacio necesario para los servidores con 3 switches numerados del 1 al 96 (la idea era hacerlo con los equipos Cisco 3660-24 por su conexión de Gigabyte Ethernet, pero por una dificultad con las VLAN no llegamos a poder configurarlos).

Para la maquetación de los equipos de trabajo, se usaron 2 equipos por oficina para representar el primer y último equipo, conectados a su vez en el los respectivos switches, dejando espacios para los que se utilizarían en caso de completar cada cuarto.

En la sede de Mendoza, al tener un solo piso, simulamos el rack principal de la sede con un switch conectado directamente al router en el cuarto de servidores, por lo que se conecta directamente a los 4 servidores de la sede. A su vez, se conecta a otros 4 switches, 1 por cada respectivo departamento del piso como en el resto de sucursales.

La sede de San Juan (perteneciente al trabajo inicial), fue modificada para usar aumentar la velocidad de las interconexiones en la sala de servidores, utilizando un switch Cisco 3660, que tiene hasta 28 puertos de Gigabit Ethernet. Este switch es usado además a modo de rack principal que conecta con cada uno de los servidores de la sala y también hacia los switches de los departamentos en los pisos.

Diseño capa de enlace

Las sedes de Mendoza y San Juan cuentan con un único segmento de red, siendo 192.168.145.0/26 y 192.168.145.64/26 respectivamente.

En la sucursal de CABA, se han creado cuatro VLANs (Redes de Área Local Virtual) para segmentar la red y mejorar la seguridad, el rendimiento y la gestión del tráfico:

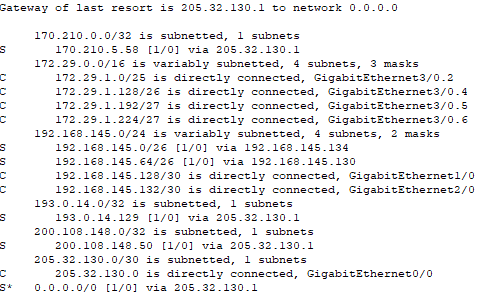
| **VLAN** | **Nombre** | **Cantidad de equipos** | **Red** |
| --- | --- | --- | --- |
| 2 | VLAN CENTRO DE DATOS y SISTEMAS | 123 EQUIPOS | 172.29.1.0/25 |
| 4 | VLAN GERENCIA | 59 EQUIPOS | 172.29.1.128/26 |
| 5 | VLAN LOGÍSTICA | 27 EQUIPOS | 172.29.1.192/27 |
| 6 | VLAN ADMINISTRACIÓN | 29 EQUIPOS | 172.29.1.224/27 |

Como el enunciado del trabajo integrador daba ubicación a las VLAN por oficinas, configuramos los switches de tal forma que las conexiones troncales fueran las esperadas, lo cual es una práctica para reducir el tráfico de la red según el envío de información. El router de la sede es el encargado de conectar las subredes en los casos que se comunican, en el cual se usaron los comandos de encapsulación para que en la interfaz queden las VLAN como sub-interfaces separadas.

Diseño capa de red

Para la conexión de las redes de las sedes de Mendoza y San Juan y los enlaces punto a punto entre los routers de las 3 sedes se nos proporcionó el bloque de IPs 192.168.145.0/24. Hicimos un subneteo teniendo en cuenta la cantidad de host de cada sede por lo que a la sede de San Juan le asignamos la red IP 192.168.145.64/26 y a Mendoza le asignamos la red IP 192.168.145.0/26.

Tabla de Ruteo del router CABA:



La sede de CABA cuenta con 4 redes, como se explicó anteriormente,la red de Administración: 172.29.1.224/27 donde todas las máquinas deben tener IP estática ya que acceden a un firewall para el servidor Web seguro de administración.

Las otras redes son la de Logística: 172.29.1.192/27, la de Gerencia: 172.29.1.128/26 y la de datos y sistemas: 172.29.1.0/25.

Además del subneteo de la red de CABA(conectada a uno de los enlaces Gigabit Ethernet del router) configuramos a dicho router de la sede, la ruta estatica 192.168.145.0/24, subneteada como se aprecia en la tabla de enrutamiento de la imagen.

Con el subneteo de la red 192.168.145.0/24 logramos una conexión con las otras dos sedes.

Por último tiene configurada una tercera ruta estática 0.0.0.0/0 vía 205.32.130.1 que permite conectar las 6 redes internas con internet.

En la sede de San Juan se cuenta con un único segmento de red con disponibilidad de 62 host de los cuales 11 serán estáticos(dpto. de administración y servidores) y el resto serán dinámicos.

En el router de San Juan configuramos la ruta 192.168.145.0/24 subneteada en 192.168.145.64/26, directamente conectada y 192.168.145.128/30 también directamente conectada.

Tambien agregamos la ruta 0.0.0.0/0 via 192.168.145.129 que

conecta San Juan con CABA y por ende con internet.

En la sede de Mendoza, así como en San Juan, tenemos 62 hosts, de los cuales 6 son estáticos y el resto dinámicos.

En el router de Mendoza configuramos la ruta 192.168.145.0/24 subneteada en 192.168.145.0/26, directamente conectada y 192.168.145.132/30 también directamente conectada.

Tambien agregamos la ruta 0.0.0.0/0 via 192.168.145.133 que

conecta San Juan con CABA y por ende con internet.

El router ISP fue configurado de tal forma que con él conectan los servidores raíz de DNS que para la maquetación fueron uno de los server ROOT llamado k.root-servers.net de IP 193.0.14.129, el servidor de nic.ar de IP 200.108.148.50 y el servidor Edu.ar de dirección IP 170.210.5.56 (que dejamos a modo de ejemplo), y el servidor de google cuya IP es 64.223.190.94

Tablas de IP estática

En las tablas de ip estática no se anotaron las ip de las impresoras, a pesar que están debidamente configuradas.

Sede San Juan:

| Dispositivo | IP |
| --- | --- |
| Router Borde(conexión Interna) | 192.128.145.65 |
| Router Borde(conexión con CABA) | 192.128.145.128 |
| Servidor Web San Juan | 192.168.145.68 |
| Servidor Web Prensa | 192.168.145.69 |
| Servidor DNS Prensa | 192.168.145.78 |
| Servidor DNS Prensa secundario | 192.168.145.79 |
| Servidor DHCP | 192.168.145.72 |
| Servidor Correo | 192.168.145.67 |
| Local Resolver | 192.168.145.66 |
| PC ADM 1 | 192.168.145.80 |
| PC ADM 2 | 192.168.145.81 |
| PC ADM 4 | 192.168.145.83 |

Sede Mendoza:

| Dispositivo | IP |
| --- | --- |
| Router-Borde(conexión interna) | 192.168.145.1 |
| Router-Borde(conexión a CABA) | 192.168.145.132 |
| Servidor DHCP | 192.168.145.2 |
| Servidor MAIL | 192.168.145.3 |
| Servidor Local Resolver | 192.168.145.4 |
| Servidor M4 | 192.168.145.5 |

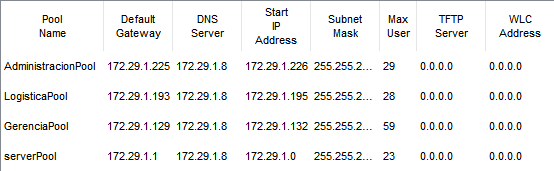
Sede CABA:

| Dispositivo | IP |
| --- | --- |
| Router a ISP | 205.32.130.2 |
| Router a Mendoza | 192.168.145.133 |
| Router a San Juan | 192.128.145.129 |
| Router a VLAN admin | 172.29.1.1 |
| Router a VLAN logística | 172.29.1.129 |
| Router a VLAN gerencia | 172.29.1.193 |
| Router a VLAN datos y sistemas | 172.29.1.225 |
| Server DHCP | 172.29.1.3 |
| Server HTTP Principal pgsa | 172.29.1.2 |
| Server HTTPS  Administración | 172.29.1.4 |
| Server SMTP | 172.29.1.5 |
| Local Resolver | 172.29.1.8 |
| Server DNS Primario | 172.29.1.6 |
| Server DNS Secundario | 172.29.1.7 |
| PCs administración | 17 2.29.1.226-254 |

Para la configuración de DHCP creamos 3 servidores distribuidos en las distintas sucursales, para asignar las IP de los equipos que no necesitaban objetivamente mantener una dirección estática. En cada servidor se crearon los grupos necesarios (pool) para la distribución, a los cuales se les debía especificar un nombre, una puerta de enlace predeterminada, un servidor DNS, una dirección IP de inicio, su máscara de subred, y el número máximo de usuarios.

| Sede | Nombre | Gateway | Servidor DNS | Direccion IP inicial | Mascara de subred | Número máximo de usuarios |
| --- | --- | --- | --- | --- | --- | --- |
| Mendoza | serverPool | 192.168.145.1 | 172.29.1.8 | 192.168.145.9 | 255.255.255.192 | 51 |
| San Juan | serverPool | 192.168.145.65 | 192.168.145.66 | 192.168.145.84 | 255.255.255.192 | 43 |

Para asignar IP por DHCP en CABA, necesitamos crear varios pool para lograr que todas las subredes tuvieran su segmentación adecuada.



Diseño capa de transporte

En la capa de transporte, utilizamos los 2 protocolos de esta:

TCP para los servidores HTTP, HTTPS, email entre las sedes (POP3 y SMTP) y DNS (para las consultas entre los servidores de las sedes).

Y UDP para las consultas de host a los servidores DNS y DHCP.

Diseño capa de aplicación

Servidores DNS

Los servidores DNS, como mencionamos anteriormente, tienen como principal función la resolución de dominios de los dispositivos de una red.

En este proyecto utilizamos para la sede de San Juan los servidores DNS de prensa, primario y secundario y un Local Resolver para la asignación de IPs a los respectivos dominios.

La empresa PetroGlobal S.A posee el dominio pgsa.com.ar, para este dominio primero configuramos la delegación del dominio com.ar a través del servidor DNS a.dns.ar que es el que maneja estos dominios.

Se le asignó al resolver la IP 192.168.145.66 al local resolver y lo configuramos para que pueda llegar el root server.

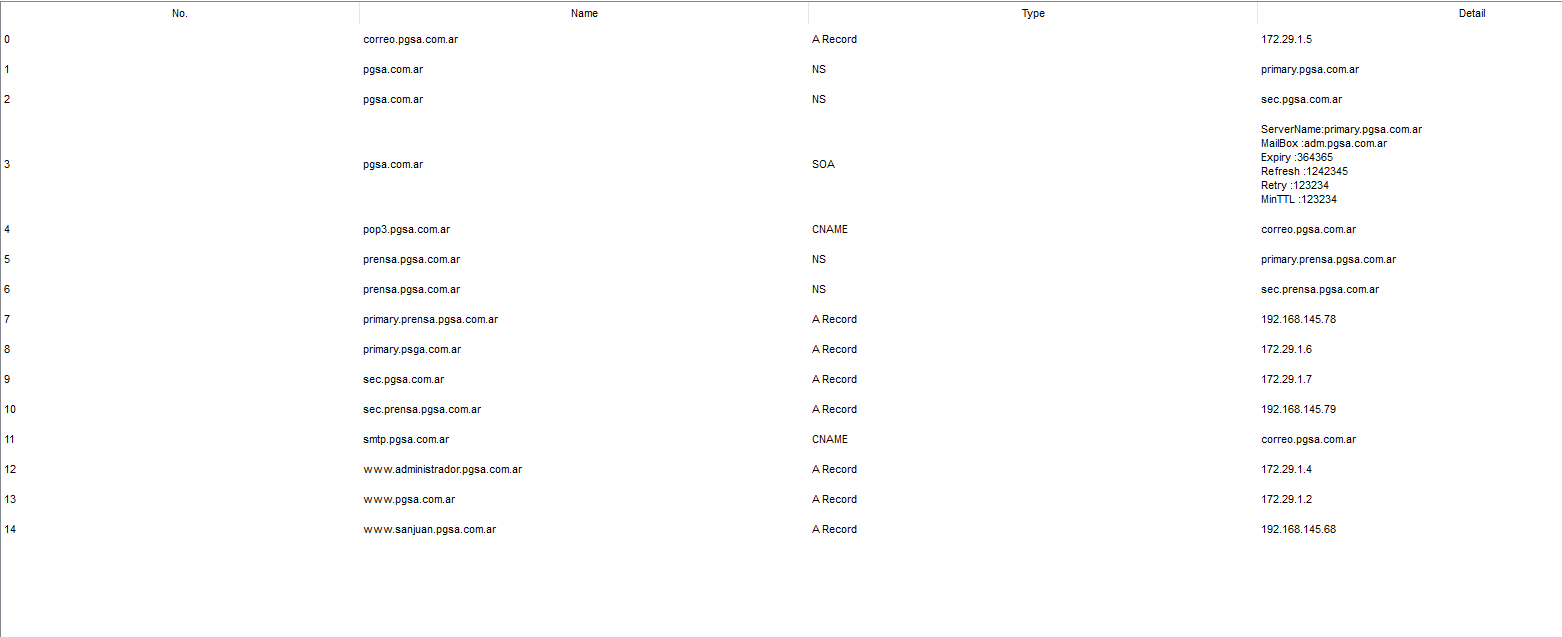
Se asignó como NS (. -> k.root-servers.net) y como registro Address ( k.root-servers.net -> 193.0.14.129)

Lo mismo hicimos con el Local Resolver de CABA que tiene la IP 172.29.1.8.

Además de este, los servidores DNS de CABA serían:

* DNS primario pgsa
* DNS secundario pgsa

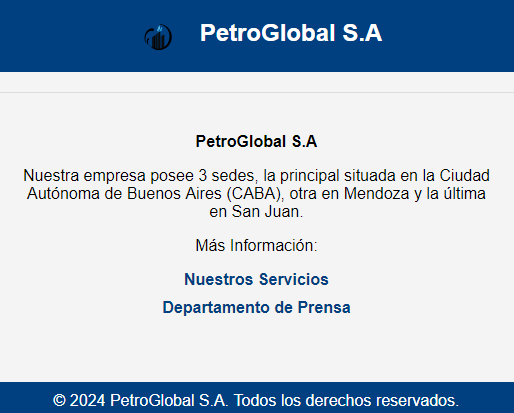
La configuración DNS de estos es:



Servidores Web

En la sede de CABA,colocamos el servidor HTTP principal de pgsa y el servidor web seguro de administración que estaban previamente en la sede de San Juan. Allí quedo el servidor Web de prensa y un nuevo servidor Web exclusivo de San Juan.

Para cada uno se implementó una página web con HTML.



Además, creamos un servidor HTTP para internet (Google), desde el cual se puede acceder a todas las páginas de la empresa.

**Servidor de Correo:**

El protocolo de aplicación SMTP es utilizado para la transferencia y POP3 para visualización (utilizado para correos electrónicos). El cliente envía un Email al servidor (el cual distribuye el mensaje) utilizando el protocolo SMTP y es obtenido mediante el protocolo POP3.

En el caso del servidor de correo de esta red, comenzamos configurando las ips de cada servidor SMTP y la puerta de enlace (gateway), que corresponde a la dirección IP de cada servidor para cada router. Y luego seguimos por configurar los 3 usuarios:

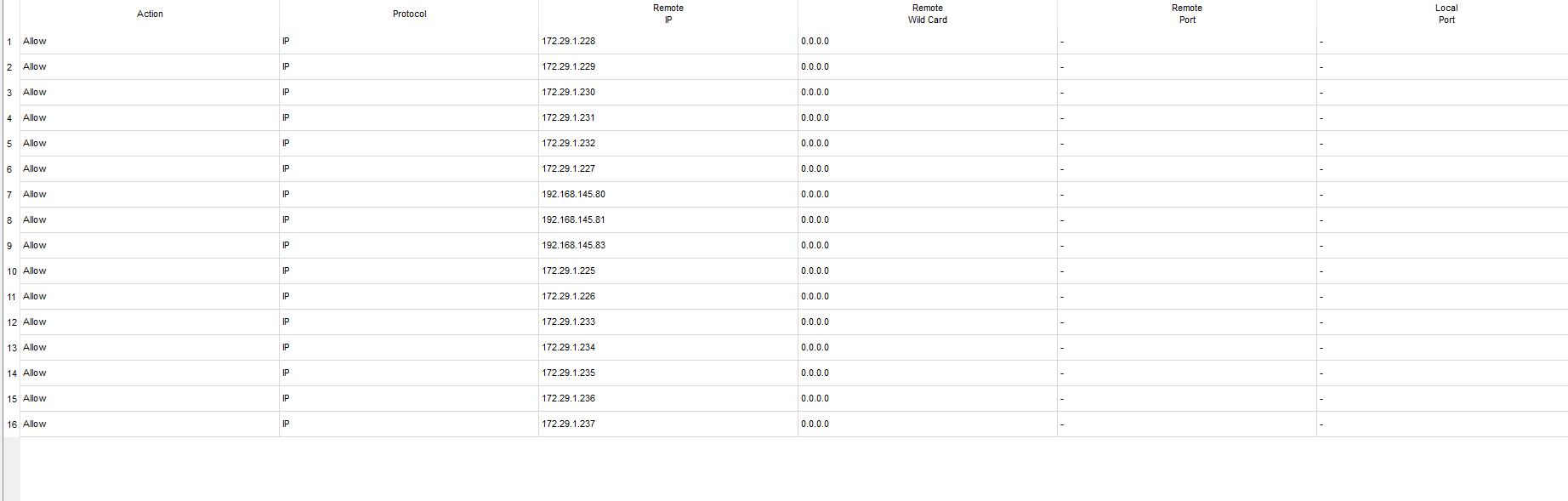
* [alancampos@pgsa.com.ar](mailto:alancampos@pgsa.com.ar)
* [joaquindores@pgsa.com.ar](mailto:joaquindores@pgsa.com.ar)
* [joaquinvillalba@pgsa.com.ar](mailto:joaquinvillalba@pgsa.com.ar)

La contraseña de los 3 usuarios es “redes”.

Estos pueden intercambiar mensajes en sus respectivas PCS de las 3 sedes. Se puede observar en las computadoras de San Juan y en CABA, con algunos mensajes.

**Firewall:**

El servidor Web HTTPS correspondiente al sistema administrativo posee un servicio de Firewall, con el fin de que solo se le permita el acceso a las PCs del departamento de administración de cada sede y a toda la VLAN de administración de CABA. Para esto, se configuró la acción “allow “con la IP de cada PC de administración con la wildcard 0.0.0.0 con el protocolo IP.



Conclusión

En resumen, este trabajo nos permitió aplicar todos los laboratorios realizados y los temas estudiados previamente. A lo largo del proceso, enfrentamos diversas problemáticas que nos ayudaron a entender ciertos conceptos mediante la simulación de la red. Este proyecto fue muy útil para consolidar los conocimientos adquiridos y reforzar nuestra comprensión de los temas tratados anteriormente.