Imagen que contiene exterior, cielo, nieve, agua

Descripción generada con confianza muy alta

**ESCUELA SUPERIOR POLITÉNICA DEL LITORAL**

**PROYECTO DE CONMUTACIÓN Y ENRUTAMIENTO**

**MANUAL TÉCNICO**

SISTEMA DE CONFIGURACIÓN DEL PROTOCOLO DEL ENRUTAMIENTO BGP PARA LA INTERCONEXIÓN ENTRE EMPRESAS O ISP

**MG. ADRIANA COLLAGUAZO**

**GRUPO #2**

OCHOA OCHOA ARIANA

CRUZ OCHOA ALBERTO

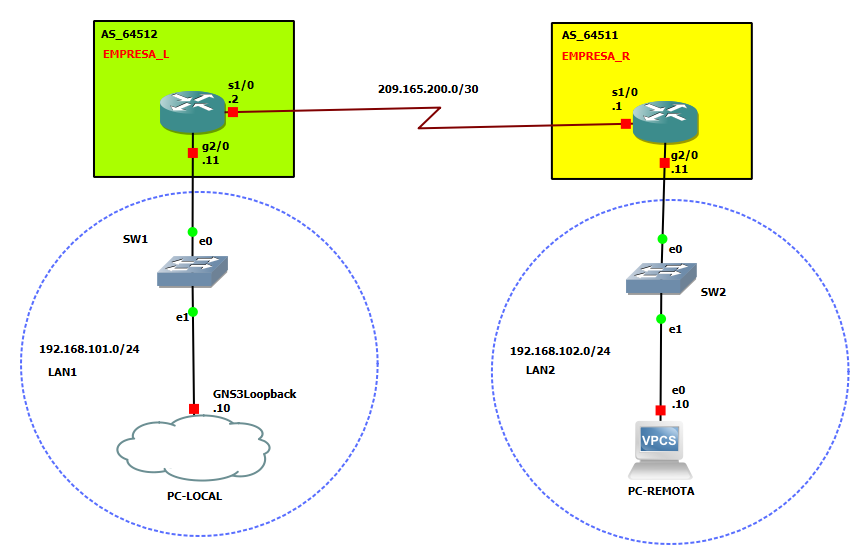
SÁNCHEZ VALVERDE JOSUÉ

SOLEDISPA CARRASCO ALDAIR

**PARALELO 1**

2T – 2018

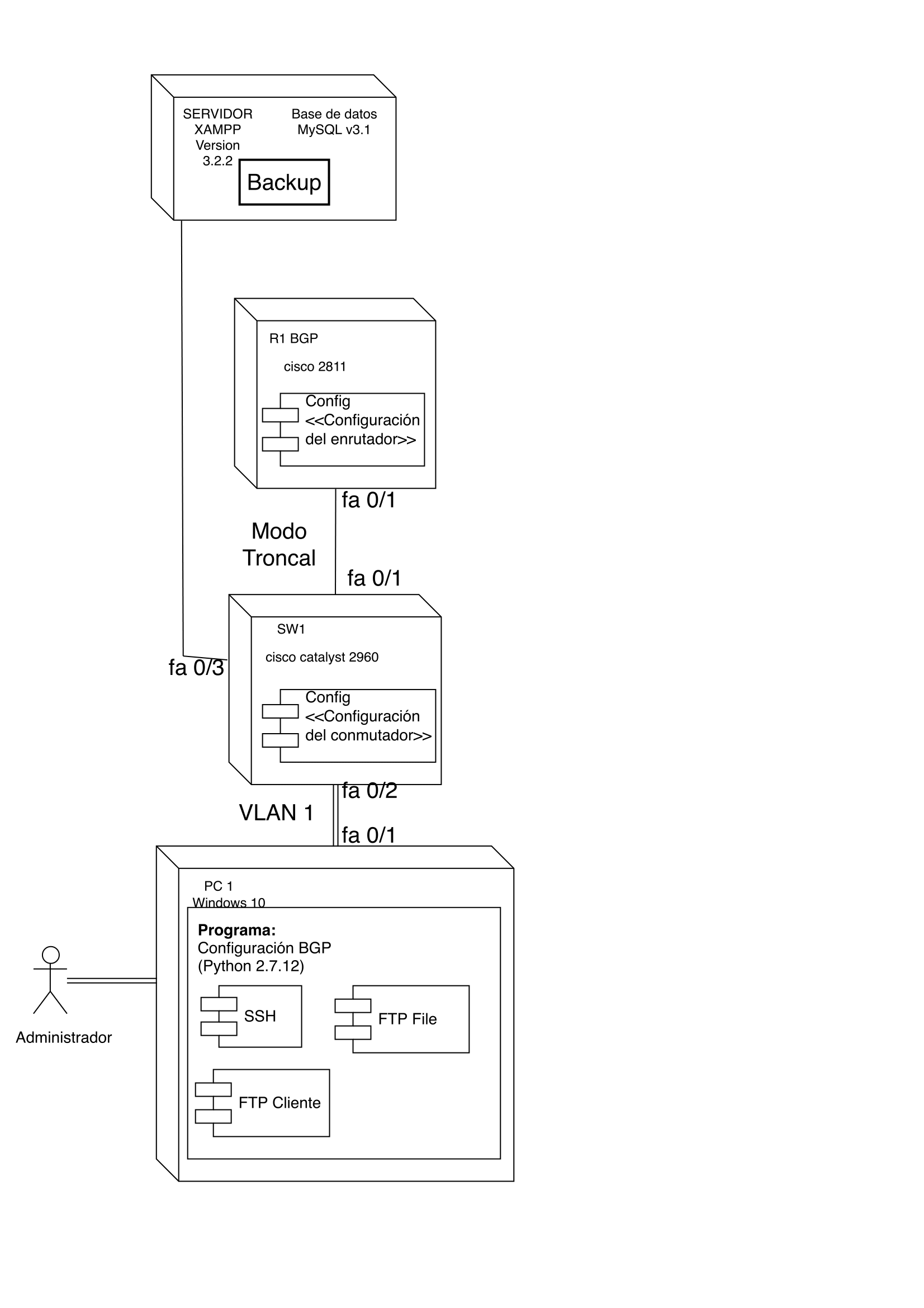
**Diagrama de red**



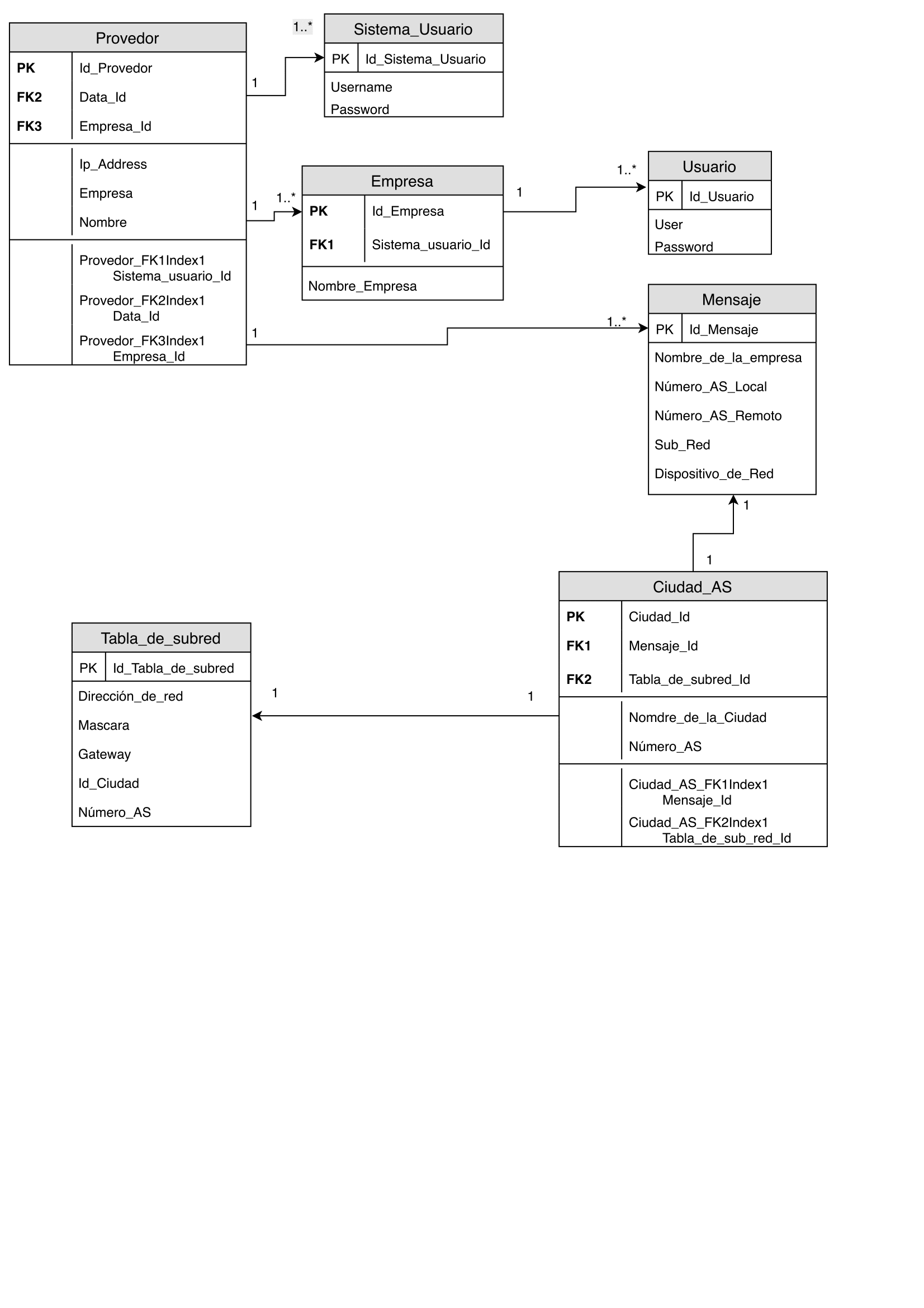
**Recursos**

|  |  |
| --- | --- |
| Hardware | Software |
| 2 enrutadores Cisco | GNS3 version 2.1.2 para Windows (64-bit) |
| Dos Computadores portátiles | Python 2.7.12 con las librerías: Telnetlib, easygui, wxPython, wx |
|  | WxFormBuilder versión 3.5 |
|  | Plataforma de desarrollo colaborativo GitHub |
|  | Aplicación web Asana |

**Diagrama de Despliegue**



**Modelo de entidad-relación de la base de datos.**

****

**Campos y tipos de datos creados en la base de datos**

A continuación se presenta en detalle los campos con sus respectivos tipos de datos creados en la base de datos del proyecto:

El campo ***PROVEEDOR*** corresponde al ISP, en donde presenta como datos el id\_proveedor que representa un ID único otorgado al ISP, además la Data\_Id que indica información acerca del proveedor de internet, Empresa\_Id indica el ID de la empresa para la posterior interconexión entre las mismas. Presenta como datos del campo la dirección IP, la empresa y el nombre de la misma.

El campo  ***SISTEMA\_USUARIO*** es aquel que se encarga de administrar la Id\_Sistema\_Usuario, es decir que tiene como datos la identificación del usuario para el ingreso al sistema, el username y el password.

El campo ***EMPRESA*** presenta como tipos de datos creados el ID\_Empresa el cual es la identificación única de la empresa a tratar para la interconexión, y el Sistema\_usuario\_Id que representa la identificación del usuario, datos como usuario y clave del mismo para el acceso.

El campo  ***USUARIO*** presenta la identificación única del usuario, user y password como reconocimiento del usuario.

El campo ***MENSAJE*** presenta un ID\_Mensaje, este campo se encarga de mostrar cuando exista la interconexión entre empresas tanto la local como la remota, con ayuda de la información de la misma como Nombre\_de\_la\_empresa, Número\_AS\_local correspondiente al AS de la empresa local, Número\_AS\_remoto que corresponde al AS de la empresa remota, sub\_Red que representa la dirección de la red en la cual se encuentran al momento ambas empresas y Dispositivo\_de\_Red que representa el equipo el cual se encuentra teniendo la conexión al momento.

El campo ***CIUDAD\_AS*** es aquel que se encarga de mostrar según sus tipos de datos las empresas que se desean interconectar mostrando sus respectivos AS, posee como dato el Nombre\_de\_la\_ciudad, y número\_de\_AS.

El campo ***TABLA\_DE\_SUBRED*** presenta el ID\_Tabla\_de\_subred como tipo de dato el cual se encarga de mostrar la identificación respectiva a la red de cada empresa ya sea la local o remota con su respectivo AS, en el presente campo se muestra la dirección\_de\_red, máscara, gateway, Id\_Ciudad y Número\_AS como parámetros principales para ordenar una tabla de subred para la respectiva interconexión y el correcto funcionamiento del proyecto.

**Configuraciones de los dispositivos de red utilizados.**

Configuración de router *Empresa Local*

|  |  |
| --- | --- |
|  | conf t |
|  | hostname EMPRESA\_L |
|  | ip domain-name fiec.espol.edu.ec |
|  | no ip domain lookup |
|  | crypto key generate rsa |
|  | 1024 |
|  |  |
|  | banner motd #SOLO ACCESO A PERSONAL AUTORIZADO# |
|  | username admin privilege 15 secret admin |
|  | username alberto privilege 15 secret alberto |
|  | username aldair privilege 15 secret aldair |
|  | username ariana privilege 5 secret ariana |
|  | line console 0 |
|  |  |
|  |  |
|  | exec-timeout 3 3 |
|  | login local |
|  | exit |
|  | line vty 0 15 |
|  |  |
|  | exec-timeout 3 3 |
|  | login local |
|  | transport input all |
|  | exit |
|  | service password-encryption |
|  | int f0/0 |
|  | des Conectado a LAN1 |
|  | ip address 192.168.101.11 255.255.255.0 |
|  | no sh |
|  | int f0/1 |
|  | des Conectado a RED\_REM\_2 |
|  | ip address 192.168.100.1 255.255.255.0 |
|  | no sh |
|  | int s0/2/0 |
|  | des Enlace serial BGP hacia AS\_64511 |
|  | ip address 209.165.200.2 255.255.255.252 |
|  | no sh |
|  | end |

**Configuración de router *Empresa Remota***

|  |  |
| --- | --- |
|  | enable |
|  | conf t |
|  | hostname EMPRESA\_R |
|  | ip domain-name fiec.espol.edu.ec |
|  | no ip domain lookup |
|  | crypto key generate rsa |
|  | 1024 |
|  | enable secret cisco |
|  | banner motd #SOLO ACCESO A PERSONAL AUTORIZADO# |
|  | username admin privilege 15 secret admin |
|  | username alberto privilege 15 secret alberto |
|  | username aldair privilege 15 secret aldair |
|  | username ariana privilege 5 secret ariana |
|  | line console 0 |
|  | logging synchronous |
|  | exec-timeout 3 3 |
|  | login local |
|  | exit |
|  | line vty 0 15 |
|  | logging synchronous |
|  | exec-timeout 3 3 |
|  | login local |
|  | transport input all |
|  | exit |
|  | service password-encryption |
|  | int f0/0 |
|  | des Conectado a LAN2 |
|  | ip address 192.168.102.11 255.255.255.0 |
|  | no sh |
|  | int s0/2/0 |
|  | des Enlace serial BGP hacia AS\_64512 |
|  | ip address 209.165.200.1 255.255.255.252 |
|  | no sh |
|  | end |

**Explicación del código fuente desarrollado con los comentarios correspondientes**

Durante la realización del proyecto se logró efectuar de manera correcta las respectivas historias de usuario planteadas en la rúbrica, con ayuda de un programa ingresando códigos y validando todos los posibles casos con ayuda de una base de datos, finalizando y obteniendo el resultado esperado.

* En el caso de la primera historia de usuario donde se menciona que se requiere ingresar a un dispositivo que se encuentre activo en la red, accediendo a la base de datos donde el dispositivo se encuentra asociado a una dirección IP, se presenta parte del código para el correcto funcionamiento y acceso al dispositivo para establecer una sesión remota:

Imagen que contiene captura de pantalla

Descripción generada con confianza alta

El presente código se establece para realizar la conexión a la base de datos de MySQL, definiendo a servidor como nombre del servidor, nombre de usuario, contraseña del usuario y bd como nombre de la base de datos.

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

La función all\_empresas hace una consulta a la BD, y retorna una tupla de listas paralelas con las id, nombre y ASNs de las empresas .

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

La función consultar\_interfaces se encarga realizar una consulta de todas las interfaces de un dispositivo siempre y cuando la conexión sea exitosa.

* En cuanto a la segunda historia de usuario, se menciona que se requiere realizar una configuración el sistema autónomo, seleccionando a la vez el nombre de la empresa, nombre de dispositivo que se requiere interconectar usando el protocolo BGP, seleccionando el número de AS respectivo de cada dispositivo.

A continuación, se presenta breve parte del código donde se realiza a cabalidad cada uno de los criterios de aceptación para el resultado final de la segunda historia de usuario.

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

La función consultar\_empresas se encarga de realizar la consulta de todas las empresas siempre y cuando la conexión en la base de datos sea exitosa, donde retorna la lista de empresas existentes determinan el Id de la misma, el nombre y ASN de la empresa.

Imagen que contiene captura de pantalla

Descripción generada con confianza alta

La función buscar\_id\_dispositivo busca el dispositivo según el nombre y el id de la empresa siempre y cuando la conexión que se tenga en la base de datos sea exitosa. A su vez también se presenta una función denominada buscar\_ip\_dispositivo, la misma realiza la misma función anterior pero la diferencia es que determina la ip del dispositivo a seleccionar.

Imagen que contiene texto, captura de pantalla

Descripción generada con confianza alta

Esta función habilita el protocolo BGP mediante una conexión ssh, donde determina en los parámetros el dispositivo a configurar y el AS del mismo que desea ingresar.

* En cuanto a la tercera historia de usuario, se requiere crear redes para los dispositivos seleccionados de la empresa local y remota, indicando el nombre del dispositivo y determinando los prefijos de red en la sesión BGP.

Imagen que contiene texto, captura de pantalla

Descripción generada con confianza alta

La función configurar\_Network anuncia las redes que son ingresadas como parámetro de entrada, en la variable lista\_Network se presenta lista de strings de IP y máscara de red que corresponden al grupo de networks a configurar en el router.

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

La función config\_Vecino configura el enrutador vecino con su AS, teniendo como parámetros el objeto que se conectará por ssh, la dirección IP del dispositivo vecino, SA del router de la empresa local, SA del router de la empresa remota, y finalmente una lista de strings que corresponden al grupo de redes a configurar en el router. En la presente función se realiza la configuración BGP de ambos dispositivos local y remoto.