UNIVERSIDAD PRIVADA BOLIVIANA

APLICACIONES CON REDES

PROYECTO FINAL
Redes Empresariales

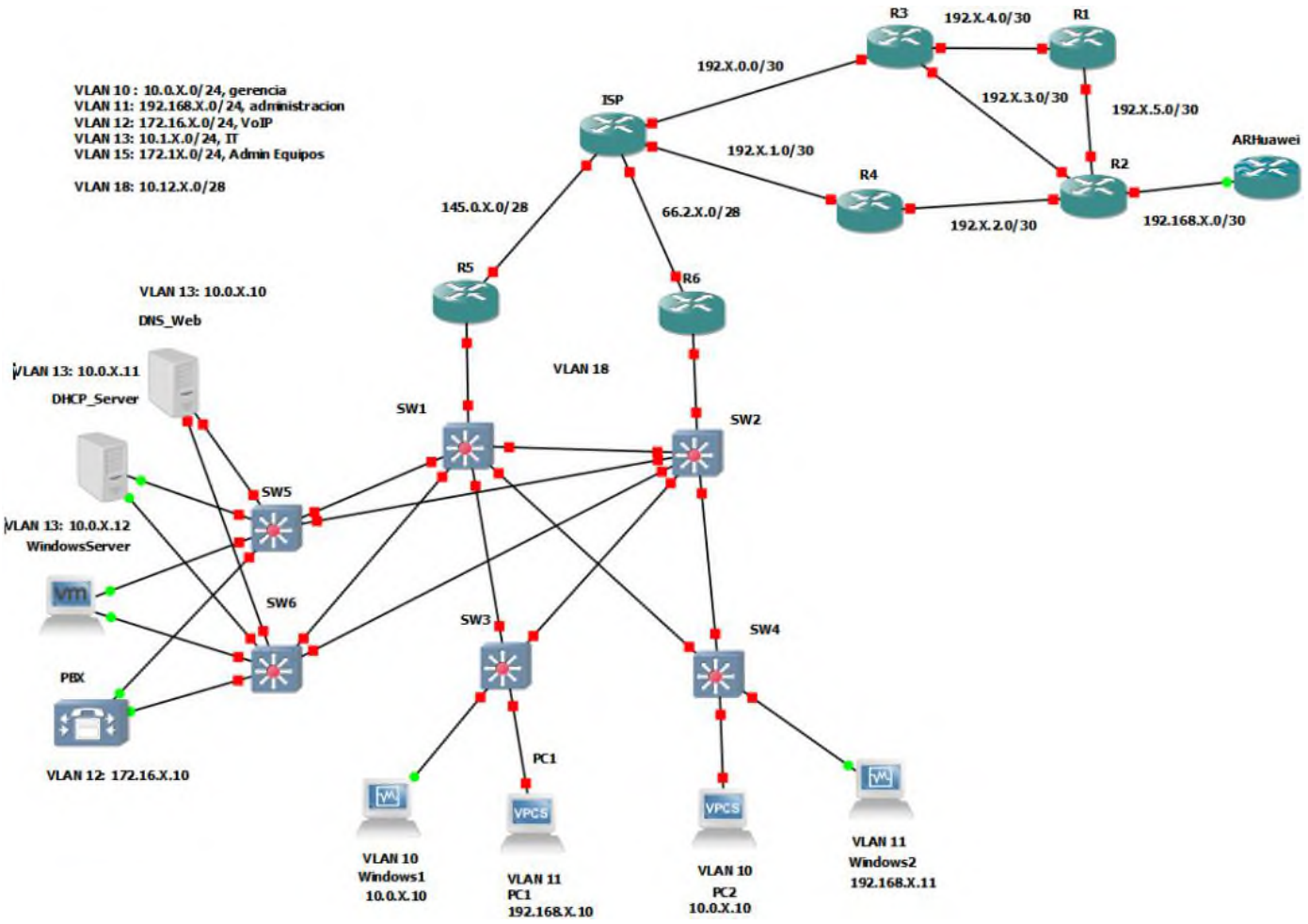
Docente: Ing. Hermann Medrano Larraín

Integrantes:
Fecha:

Cochabamba Bolivia

El proyecto consta de armar las siguientes topologías físicas mostradas en las imágenes de abajo. Donde se configurarán los servicios requeridos en los enunciados.
El esquema físico de la red de la central es:

RED GNS3



Configurar los siguientes servicios:
VTP: Configurar los switches de capa 3 SW1 y SW2 como servidores, el dominio VTP debe de ser cisco.com. El password de VTP será: cisco.
Los switches SW3, SW4 y SW5 deben trabajar como clientes.

Troncales: Configurar todos los enlaces de los switches como troncales estáticas. Donde se permita todas las VLANS y que se maneje la encapsulación con el estándar 802.1Q.

VLANS: Crear las VLANS mostradas en la topología física. Asignar las VLANS de acceso tal como se muestra en la topología física.

PVST: Las VLANS 10, 11 y 12 deberán estar como root bridge en el SW1 y como backup bridge en el SW2.
La VLANS 13 y 15 deberán estar como root bridge en el SW2 y como backup bridge en el SW1.

SVIs: Se deberán implementar interfaces SVI, en los switches de capa 3 SW1 y SW2. Para ello se deben usar la segunda y tercera dirección IP de cada subred y asignar a las interfaces SVI correspondiente.

HSRP: Configurar un grupo HSRP para cada VLAN, de modo que se tenga alta disponibilidad de la dirección IP de la puerta de enlace predeterminada para poder acceder a Internet y otras redes remotas.
En el caso de los routers, configurar dos direcciones IPs para que trabajen con HSRP, y siempre estén disponibles. Asegurando la alta disponibilidad de acceso a Internet.

Redundancia de enlace en servidores: Instalar una máquina virtual con Windows Server, configurar redundancia con dos enlaces en active backup, que se conecten a los dos switches de datacenter. Lo mismo hacer con el servidor DHCP, DNS WEB y PBX.

DHCP: Montar un servidor DHCP en un router Mikrotik. Configurar pools para todas las VLANs excepto para las VLANs de servidores y administración de equipos, en las cuales se debe asignas las IPs de manera estática. Previamente probar la conectividad de los PCs poniendo IPs estáticas. Se deben amarrar las direcciones IPs en el servidor DHCP en Mikrotik, según el esquema de red.
Configurar el relay dhcp en las interfaces SVI.

Administración de equipos: Configurar una IP en la interface VLAN 15 de administración de equipos, switches, y proveer al equipo de acceso remoto. Configurar seguridad en las interfaces virtuales VTY con usuario y password; y habilitar SSH.

ACLS: Bloquear con un ACL extendido el acceso de todas las redes, excepto la red de la VLAN 13, a la red de administración de equipos (VLAN 15).

Enrutamiento: Configurar rutas por defecto en los switches de capa 3 SW1 y SW2. En los routers R1 y R2.
Para el tráfico de vuelta hacia las redes de las VLANS se deberá crear rutas estáticas desde los routers R1 y R2.

NAT: Configurar NAT estático para el servidor Web puerto 80 y servidor DNS puerto 53. Esta configuración debe realizarse en ambos routers, para redundancia en los servicios.
Configurar PAT para todas las VLANs en ambos routers R1 y R2.

Red WAN: Se configurarán las direcciones IP públicas en cada interface de los routers, acorde al diagrama topológico.
Configurar OSPF en todos los routers de la red WAN. De tal manera que todas las direcciones públicas puedan ser aprendidas en toda la red de routers que están con OSPF.
En la red WAN configurar direcciones públicas conocidas, como ser 8.8.8.8, 8.8.4.4.4, para poder simular el acceso a Internet. Estas direcciones públicas deben ser aprendidas por todos los routes en la red WAN, incluso en eNSP.

Windows Server: Configurar Directorio Activo y añadir las computadoras con windows 7 al directorio activo.

DNS: Instalar Debian 12, instalar los paquetes de Bind, donde se configurará un servidor DNS autoritativo como local, para ello usar vistas y access lists, permitiendo el acceso a

los registros locales y públicos en el servidor DNS. Crear un nombre de dominio, ejemplo: dominio.com.
Crear registros A para el servidor DNS, página web (www y FQDN) y central telefónica, de manera local.
Crear registros públicos para el DNS y la página web (www y FQDN).

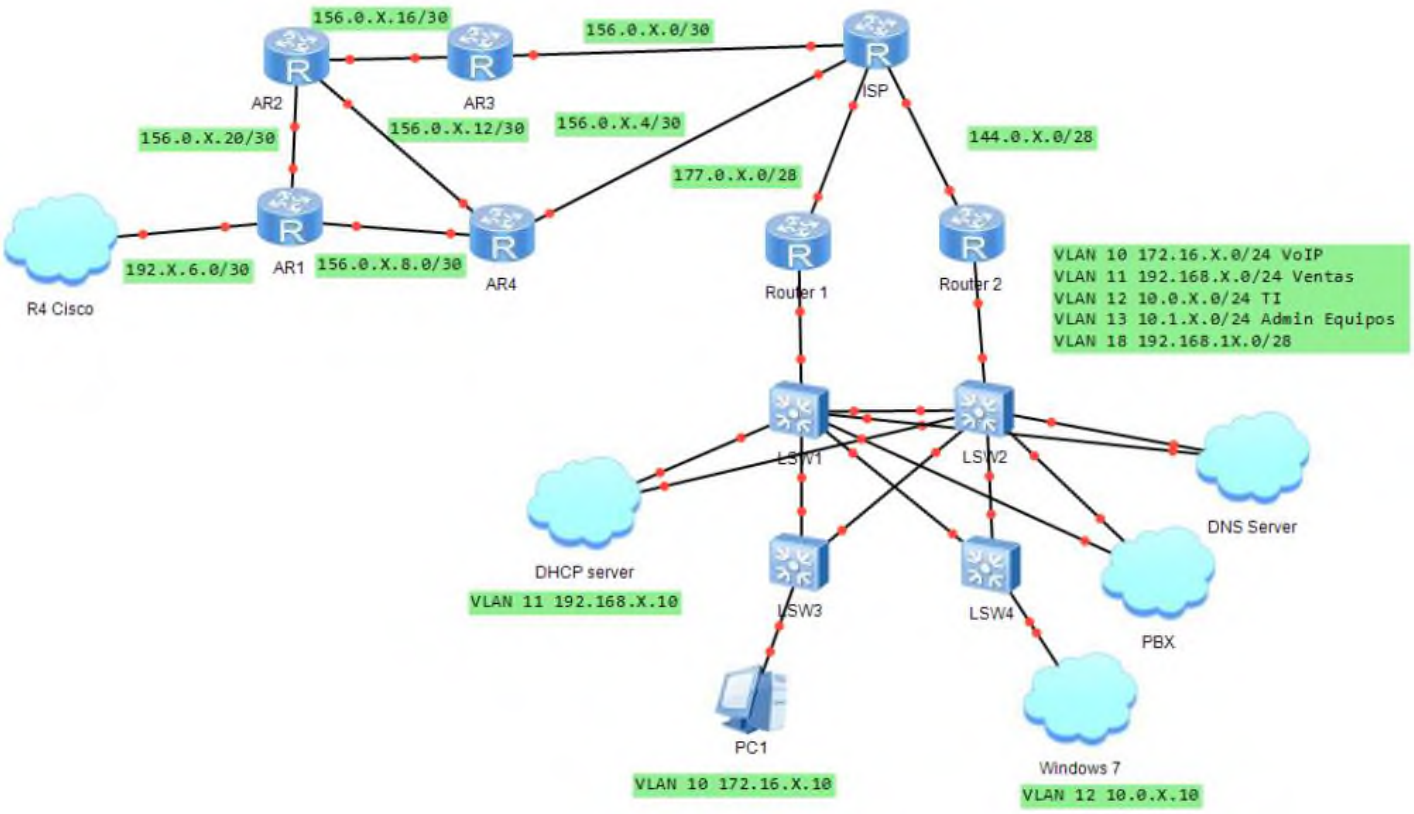
Web: En el servidor Debian montado, instalar NGINX. Configurar un bloque para la pagina web de la empresa.

PBX: Instalación y configuración de un servidor PBX con Issabel PBX, configurar internos y probar llamadas. Se tendrán los números de Internos (número de usuario)XX para la PBX en GNS3 y (número de usuario)XX para la PBX en eSNP.
En las máquinas virtuales con Windows 7, registrar el softphone con la PBX.
Configurar un enlace punto a punto, donde se enrutará el tráfico de la red VoIP, la conexión será entre el Router 1 de eSNP y el R5 de GNS3, simulando así una conexión VPN. Configurar una Troncal IAX, para que se puedan realizar llamadas entre la PBX de GNS3 y eSNP. Para ello, configurar las rutas estáticas necesarias.

Pruebas: Al finalizar, se debe tener los siguientes resultados:

- Ping entre equipos de distintas redes.
- Ping direcciones públicas de GNS3 y eSNP.
- Desde el cmd de Windows comprobar la resolución de registros DNS.
- Acceder a la página web del servidor WEB, desde un Windows 7.
- Que las redes públicas se publiquen mediante OSPF entre la red OSPF de Cisco y la red OSPF de Huawei.
- Que el acceso a Internet se mantenga constante cuando se apaga un equipo. Un router o un switch de capa 3. Ping a una publica de un router Huawei constante.
- Realizar llamadas entre los softphones, dentro la misma PBX. Llamadas entre PBXs, a través de la troncal IAX.

RED eSNP



Troncales: Configurar todos los enlaces de los switches como troncales estáticas. Donde se permita todas las VLANs y que se maneje la encapsulación con el estándar 802.1Q.

VLANS: Crear las VLANs mostradas en la topología física. Asignar las VLANs de acceso tal como se muestra en la topología física.

MSTP: Cambiar el modo de STP de PVSTP a MSTP, donde se tendrán tres instancias. La primera instancia abarcará a las VLANs 10 y 11; la segunda instancia abarcará a las VLANs 12 y 13.
La primera instancia deberá estar como root bridge en el SW1 y como backup bridge en el SW2.
La segunda instancia deberá estar como root bridge en el SW2 y como backup bridge en el SW1.

SVIs: Se deberán implementar interfaces SVI, en los switches de capa 3 SW1 y SW2. Para ello se deben usar la segunda y tercera dirección IP de cada subred y asignar a las interfaces SVI correspondiente.

VRRP: Configurar un grupo VRRP para cada VLANs, de modo que se tenga alta disponibilidad de la dirección IP de la puerta de enlace predeterminada para poder acceder a Internet y otras redes remotas.
En el caso de los routers, configurar dos direcciones IPs para que trabajen con VRRP, y siempre estén disponibles. Asegurando la alta disponibilidad de acceso a Internet.

Redundancia de enlace en servidores: Instalar una máquina virtual con Mikroitk, configurar redundancia con dos enlaces en active backup, que se conecten a los dos switches de datacenter.

DHCP: Montar un servidor DHCP en un router Mikrotik. Configurar pools para todas las VLANs. Configurar el relay dhcp en las interfaces SVI.

Enrutamiento: Configurar rutas por defecto en los switches de capa 3 SW1 y SW2. En los routers R1 y R2.
Para el tráfico de vuelta hacia las redes de las VLANs se deberá crear rutas estáticas desde los routers R1 y R2.

NAT: Configurar PAT para todas las VLANs en ambos routers R1 y R2.

Red WAN: Se configurarán las direcciones IP públicas en cada interfaz de los routers, acorde al diagrama topológico. Ver que las

Protocolo de enrutamiento: Se trabajará con el protocolo de enrutamiento OSPF. Para que todos los routers de la red WAN aprendan las redes públicas de manera dinámica.

DNS: Montar un DNS local con Bind. Configurar un subdominio, por ejemplo dominio.subdominio.com. Crear registros DNS para el servidor DNS y para la PBX.

PBX: Instalación y configuración de un servidor PBX con Issabel PBX, configurar internos y probar llamadas. Se tendrán los números de Internos (número de usuario)XX para la PBX en GNS3 y (número de usuario)XX para la PBX en eSNP.
En las máquinas virtuales con Windows 7, registrar el softphone con la PBX.
Configurar un enlace punto a punto, donde se enrutará el tráfico de la red VoIP, la conexión será entre el Router 1 de eSNP y el R5 de GNS3, simulando así una conexión VPN. Configurar una Troncal IAX, para que se puedan realizar llamadas entre la PBX de GNS3 y eSNP. Para ello, configurar las rutas estáticas necesarias.

Pruebas: Al finalizar, se debe tener los siguientes resultados:

- Ping entre equipos de distintas redes.
- Ping direcciones públicas de GNS3 y eSNP.
- Acceder a la página web del servidor web de GNS3, desde un Windows 7 desde la red eSNP.
- Que las redes públicas se publiquen mediante OSPF entre la red OSPF de Cisco y la red OSPF de Huawei.
- Que el acceso a Internet se mantenga constante cuando se apaga un equipo. Un router o un switch de capa 3. Ping a una publica de un router Cisco constante.
- Registrar el softphone de Windows 7 con la PBX. Probar llamadas entre centrales PBXs, a través de la troncal IAX.
- Resolución DNS de los registros configurados.

Investigar:

- Alta disponibilidad funcionando en los servidores. Usando agregación de enlace Active Backup.

NOTAS

- Las X, representan el numero de lista de cada estudiante en la lista de acceso a las máquinas virtuales, con lo que cada estudiante configurará las redes IPs acorde al numero de lista. Esto se incluye en la configuración de los números de interno en las PBXs.