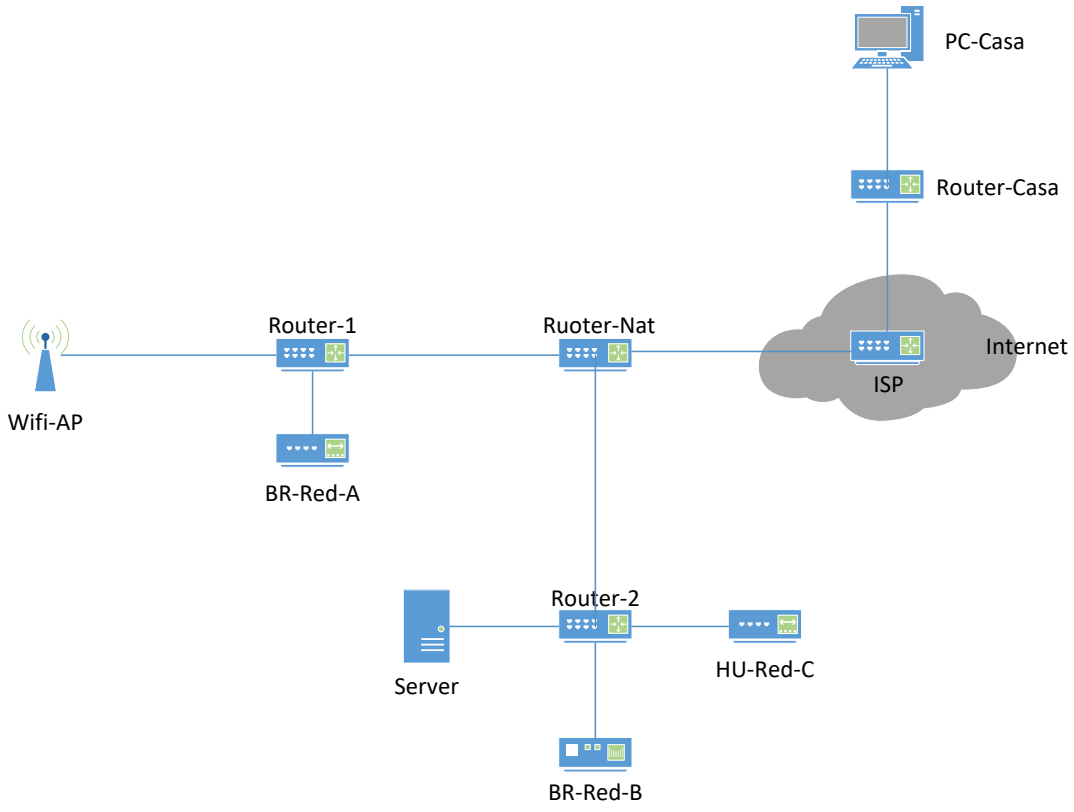
Comunicación de Datos 1

Trabajo Práctico Especial 2016

Consideraciones Generales

- La aprobación del Trabajo Práctico Especial es condición necesaria para aprobar la materia.
- El trabajo se puede hacer en grupos de hasta 3 personas.
- Los integrantes de los grupos con las direcciones de mail de cada integrante se deben enviar a fermayorano@gmail.com hasta el 25/08/2016
- A cada grupo se le asignará un ayudante al que se le deben realizar las consultas que considere necesarias.
- La fecha límite de entrega del trabajo es 20/10/2016.
- Para la entrega del TPE se debe enviar por correo electrónico el archivo IMN que se genera en Core, y un informe en formato PDF al ayudante correspondiente. Dicho informe debe contener todos los comandos ingresados en cada inciso, las capturas de pantalla con los resultados obtenidos, y el análisis de las capturas obtenidas con la herramienta Wireshark.
- Luego de la fecha de entrega, cada ayudante coordinará con sus grupos la defensa del TPE.

Topología de red



La red tiene las siguientes características:

- En el BR-Red-A hay actualmente 3 PC conectadas y la cantidad de conexiones que soporta el Bridge es 48
- En el BR-Red-B hay actualmente 2 PC conectadas y la cantidad de conexiones que soporta el Bridge es 64
- En el HU-Red-C hay actualmente 2 PC conectadas y la cantidad de conexiones que soporta el Bridge es 12
- Al Wifi-Ap tiene 2 Laptop conectadas y prevé que se conectarán hasta 20 equipos.

Ejercicios

1- Para la cantidad de conexiones proyectadas para cada una de las redes, realice una asignación de direcciones IP utilizando VLSM. Considere que las direcciones privadas se encuentren en el rango 192.168.X.0 a 192.168.X.255, donde X es el número de grupo que se les asignó.

2- Realice una tabla en donde se indiquen cada una de las subredes resultantes, indicando el nombre de cada red, su dirección base, la máscara, y el rango que incluye cada bloque.

3- Implemente la red propuesta en el emulador CORE con la disposición de equipos que actualmente se tienen conectados. Considere la asignación IP realizada en el ejercicio 1, y la colocación de direcciones públicas en donde corresponda.

4- Configurar todas las interfaces y rutas de los routers, minimizando la cantidad de entradas en las tablas de ruteo (considere el uso de rutas por defecto).
Cabe desatacar que los comandos correspondientes deben estar cargados en la opción User Defined -> Startup Commands de cada dispositivo, y que dentro de los servicios sólo deben quedar habilitados el IP FORWARD y User Defined.
Tenga en cuenta que el router del ISP no lleva ruta por defecto.

5- Consultar las tablas ARP de un dispositivo en particular. Eliminar una entrada a la tabla y generar un ping de manera que se generen paquetes ARPRequest y ARP Reply. En el informe agregar las capturas de pantalla correspondientes en donde se demuestre el funcionamiento del protocolo.

6- Configurar NAT en el Router–Nat para que los equipos conectados a la Red-A y al Wifi-Ap puedan acceder a la parte pública mediante el proceso de MASQUERADE.
Configure el Router-Casa para que PC-Casa pueda acceder a la parte pública mediante el proceso de MASQUERADE.
Configure DNAT en el puerto 8080 del Router-Nat para que los equipos externos puedan acceder al puerto 8000 del Server.

7- Realizar pruebas utilizando el comando ping entre los siguientes puntos:
   - Desde un equipo conectado a la Red-A hasta el Server
   - Desde un equipo conectado al Wifi-AP a la interfaz pública del Router-Casa

Mediante la utilización de Wireshark, analice el camino seguido por los paquetes generados, adjuntando al informe las capturas de pantalla correspondientes.

8- Ejecute el comando hping3 con la opción –S[IP_Destino] –p [Puerto_Destino] desde la PC-Casa a la ip pública del Router-Nat. Analizar los resultados obtenidos con capturas de pantalla de Wireshark.

9- Analizar el tráfico de paquetes en la red conectada a través de un hub (HU-Red_C) y de un switch (BR-Red-B). Observar las diferencias entre el comportamiento de ambos casos. Justificar con la captura de las pantallas de Wireshark correspondientes.

10- **Generar distintos errores en la configuración de los routers** de la red de manera de generar paquetes ICMP con los siguientes códigos de error:
- Destination network unreachable
- Destination host unreachable
- Time Exceeded

11- Realice un traceroute desde un equipo conectado a la Red-A a la interfaz pública del Router-Casa. Observe con Wireshark los paquetes que se genere, analizando la información relevante de cada uno de los ellos.