**PRÁCTICA FINAL ARQUITECTURA DE REDES**

3ºB GITT+BA Ignacio García Santamaría 30/04/2022

**Índice**

[**Introducción** 3](#_Toc102237296)

[**1.** **Sistema Autónomo A** 3](#_Toc102237297)

[**1.1.** **Descripción del AS** 3](#_Toc102237298)

[**1.2.** **Descripción de OSPF y de las ACL** 3](#_Toc102237299)

[**1.3.** **Topología de la red** 3](#_Toc102237300)

[**1.4.** **Router-on-a-stick** 5](#_Toc102237301)

[**1.5.** **Implementación del protocolo de encaminamiento de OSPF** 5](#_Toc102237302)

[**1.6.** **Análisis de las tablas de rutas** 6](#_Toc102237303)

[**1.7.** **Listas de acceso (ACL)** 7](#_Toc102237304)

[**2.** **Sistema Autónomo B** 10](#_Toc102237305)

[**2.1.** **Descripción del AS** 10](#_Toc102237306)

[**2.2.** **Descripción de RIP V1** 10](#_Toc102237307)

[**2.3.** **Topología de la red** 10](#_Toc102237308)

[**2.4.** **Implementación del protocolo de encaminamiento de RIP V1** 11](#_Toc102237309)

[**2.5.** **Análisis de las tablas de rutas** 12](#_Toc102237310)

[**2.6.** **Listas de acceso (ACL)** 13](#_Toc102237311)

[**3.** **Sistema Autónomo C** 16](#_Toc102237312)

[**3.1.** **Descripción del AS** 16](#_Toc102237313)

[**3.2.** **Descripción de RIP V2** 16](#_Toc102237314)

[**3.3.** **Topología de la red** 16](#_Toc102237315)

[**3.4.** **Implementación del protocolo de encaminamiento de RIP V2** 17](#_Toc102237316)

[**3.5.** **Análisis de las tablas de rutas** 18](#_Toc102237317)

[**4.** **Sistema Autónomo D** 20](#_Toc102237318)

[**4.1.** **Descripción del AS** 20](#_Toc102237319)

[**4.2.** **Descripción de una interfaz virtual** 20](#_Toc102237320)

[**4.3.** **Topología de la red** 20](#_Toc102237321)

[**4.4.** **Análisis de las tablas de rutas** 20](#_Toc102237322)

[**5.** **Interconexión de los Sistemas Autónomos** 22](#_Toc102237323)

[**5.1.** **Interconexión de los AS’s** 22](#_Toc102237324)

[**5.2.** **Descripción de BGP** 22](#_Toc102237325)

[**5.3.** **Topología de la red** 22](#_Toc102237326)

[**5.4.** **Implementación del protocolo de encaminamiento de RIP V1** 23](#_Toc102237327)

[**5.5.** **Análisis de las tablas de rutas** 23](#_Toc102237328)

[**ANEXO AS A** 25](#_Toc102237329)

[**Router-on-a-stick** 25](#_Toc102237330)

[**OSPF** 25](#_Toc102237331)

[**ANEXO AS B** 27](#_Toc102237332)

[**RIP V1** 27](#_Toc102237333)

[**Configuración telnet** 28](#_Toc102237334)

[**ANEXO AS C** 29](#_Toc102237335)

[**RIP V2** 29](#_Toc102237336)

[**ANEXO Interconexión de los Sistemas Autónomos** 31](#_Toc102237337)

[**BGP** 31](#_Toc102237338)

# **Introducción**

En este informe se va a dar conectividad a cuatro AS’s diferentes mediante el uso de diferentes protocolos de enrutamiento y diferentes directivas de filtrado de tráfico. Para cada AS se va a realizar una breve descripción del protocolo de enrutamiento y de las directivas que se emplean, un esquema de la red, las políticas de tráfico aplicadas y el procedimiento seguido para asegurarme de que se cumplen con los requerimientos exigidos.

Dentro de la red que debe ser creada, cada AS tendrá un identificador y una relación de vecindad específica con el resto de AS de la cual se hablará más adelante. La manera de proceder en este informe va a ser primero un repaso por cada AS en particular, y posteriormente se analizará la interconexión de los diferentes Sistemas Autónomos.

1. **Sistema Autónomo A**
   1. **Descripción del AS**

En este AS se usa el protocolo de direccionamiento Open Shortest Path First (OSPF). En la red habrá cuatro routers: Un router frontera, un router interno, y un router asignado a cada una de las dos empresas que hay presentes. La empresa E1 tiene 4 departamentos, cada uno perteneciente a una VLAN, y con 256 direcciones públicas cada uno. Haciendo uso de un único interfaz físico debemos dar soporte a las redes distintas de cada departamento. La empresa E2 no se divide en departamentos y tiene 2048 direcciones IP. Las restricciones de tráfico presentes en este AS las tiene el departamento 1, el cual solo puede cursar tráfico WEB hacia internet, pero puede tener comunicación total con los otros departamentos.

* 1. **Descripción de OSPF y de las ACL**

OSPF es un protocolo de encaminamiento de estado de enlaces, óptimo para redes medianas y grandes. Cada router tiene conocimiento completo de la topología de la red, no obstante, las tablas de rutas se muestran igual que en cualquier otro procedimiento. Las actualizaciones en OSPF se transmiten de manera inmediata cuando hay cambios en la topología de la red, y el protocolo tiene soporte CIDR y permite la agregación de direcciones para resumir la información transmitida. Adicionalmente, en OSPF contamos con un router designado y con un router de backup para transmitir la información de la red. Para este caso en particular se va a hacer uso de OSPF en área única, y como el encaminamiento en todas las redes debe ser óptimo en cuanto al número de saltos, no he modificado el ancho de banda de referencia en ninguno de los routers del sistema.

Las Access Control List (ACL) son una serie de instrucciones que permiten a los routers controlar el tráfico por sus interfaces de manera selectiva. Cada ACL contiene una serie de sentencias que pueden permitir o denegar el tráfico y se asigna de entrada (los paquetes se inspeccionan antes de ser enrutados) o de salida de un interfaz (los paquetes entrantes se enrutan al interfaz de salida donde son inspeccionados). En mi caso voy a hacer uso de listas de acceso extendidas, las cuales se pueden identificar mediante un nombre descriptivo, en lugar de mediante un número. La principal razón por la cual he decidido usar la ACL extendidas es porque además especificar un protocolo específico después de la condición de permitir o denegar, permiten editar las instrucciones existentes.

* 1. **Topología de la red**

En la Ilustración I se muestra la topología de la red del SA A. La topología se ha hecho de tal manera para cumplir con los requerimientos iniciales. Cada interfaz de los routers pertenece a redes diferentes. En el router exterior he establecido una red adicional que no se menciona en las especificaciones del proyecto, he establecido esta red para comprobar si el permiso de tráfico WWW que restrinjo mediante las ACL ha sido asignado correctamente. La presencia de este servidor también me va a permitir comprobar las restricciones de tráfico de otros sistemas autónomos.

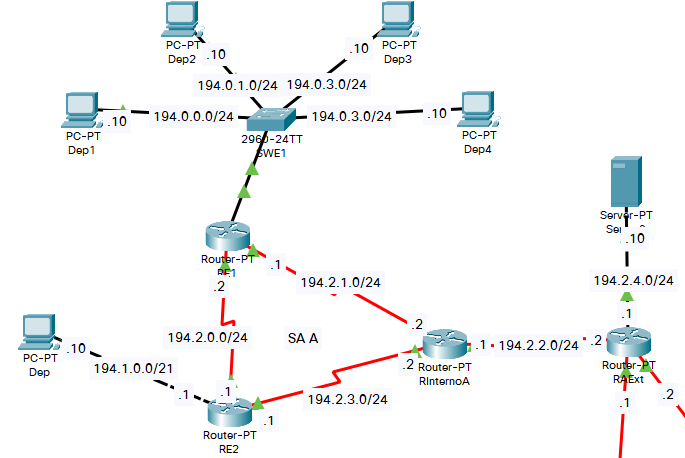


Ilustración : Topología de la red del AS A

Con el fin de comprobar la conectividad en cada una de las redes establecidas, he decidido poner un sistema final representativo del resto de la red. A la hora de asignar direcciones IP a cada una de las empresas, en la empresa E2 la máscara de red es /21 para así incluir las 2048 direcciones IP que necesita la LAN. Cada departamento de la empresa E1 requiere de 256 direcciones IP, es por eso que su máscara de red es /24, adicionalmente, se les han asignado a los departamentos redes contiguas y agregables para que así el router de la empresa E1 presente la información de manera resumida al resto del AS’s.

Para que la información presentada quede más clara, a continuación, se presenta dos tablas con información más detallada que la que se presenta en la Ilustración 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara | Gateway de salida | Empresa |
| Dep1 | Fa0/0 | 194.0.0.10 | /24 | 194.0.0.1 | E1 |
| Dep2 | Fa0/0 | 194.0.1.10 | /24 | 194.0.1.1 | E1 |
| Dep3 | Fa0/0 | 194.0.2.10 | /24 | 194.0.2.1 | E1 |
| Dep4 | Fa0/0 | 194.0.3.10 | /24 | 194.0.3.1 | E1 |
| Dep | Fa0/0 | 194.1.0.10 | /21 | 194.1.0.1 | E2 |
| Server0 | Fa0/0 | 194.2.4.10 | /24 | 194.2.4.10 | Testing |

Tabla : Información sobre los dispositivos finales

|  |  |  |  |
| --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara |
| RE1 | Serial2/0 | 194.2.1.1 | /24 |
| Serial3/0 | 194.2.0.2 | /24 |
| Fa0/0.5 | 194.0.0.1 | /24 |
| Fa0/0.10 | 194.0.1.1 | /24 |
| Fa0/0.20 | 194.0.2.1 | /24 |
| Fa0/0.30 | 194.0.3.1 | /24 |
| RE2 | Fa0/0 | 194.1.0.1 | /21 |
| Serial2/0 | 194.2.3.1 | /24 |
| Serial3/0 | 194.2.0.1 | /24 |
| RInternoA | Serial2/0 | 194.2.2.1 | /24 |
| Serial3/0 | 194.2.1.2 | /24 |
| Serial6/0 | 194.2.3.2 | /24 |
| RExtA | Fa0/0 | 194.2.4.1 | /24 |
| Serial2/0 | 194.2.2.2 | /24 |

Tabla : Información sobre los routers[[1]](#footnote-1)

* 1. **Router-on-a-stick**

Tal y como se mencionó en el enunciado de la práctica, para la empresa E1 debemos de dar soporte a cuatro redes diferentes mediante un único interfaz físico. Esto es únicamente posible mediante el uso de interfaces virtuales y de VLAN.

En el switch SWE1 debo asignar a cada departamento una VLAN diferente, de este modo, la única manera de que se comuniquen los departamentos entre sí es a través del router (esto nos beneficia adicionalmente para poder efectuar las restricciones de tráfico mencionadas en las especificaciones). Adicionalmente, el enlace entre el router y el switch debe estar en modo troncal para que se propague la información por dicho enlace.

En la Tabla 3 se muestra se muestra de forma esquemática la asignación de las VLAN a los interfaces del router para así poder realizar Router-on-a-stick.

|  |  |  |
| --- | --- | --- |
| Interfaz | VLAN | Departamento |
| Fa0/0 | Troncal | - |
| Fa0/2 | VLAN 5 | Dep1 |
| Fa0/3 | VLAN 10 | Dep2 |
| Fa0/4 | VLAN 20 | Dep3 |
| Fa0/5 | VLAN 30 | Dep4 |

Tabla : Interfaces del switch SWE1

A la hora de configurar el router, una vez accedemos a los interfaces virtuales, además de configurar su IP correspondiente, es necesario configurar la subinterfaz para que funcione en una VLAN específica.[[2]](#footnote-2)

* 1. **Implementación del protocolo de encaminamiento de OSPF**

Tras comprobar que la asignación de las redes que están directamente conectadas se comunican entre sí, incluyendo los diferentes departamentos de la empresa E1, procedí a implementar el protocolo de direccionamiento OSPF para tener conectividad entre redes que no están conectadas directamente al mismo router. Dado que dicho protocolo se emplea en todo mi sistema autónomo, debo configurar todos los routers de mi red.

En primer lugar, establecí el identificador de los routers para establecer el router designado, como dicho router es el encargado de comunicar la información de la red. Decidí que fuese el router RInternoA el que tuviese el menor router-id, ese router también tiene acceso tanto a los dos routers de las empresas como al router exterior.

En segundo lugar, anuncié ya dentro del interfaz del proceso de OSPF las redes del AS a las que estaban directamente conectados cada uno de los routers. Posteriormente establecí como interfaz pasivo aquellos interfaces de los routers que no interconectan redes, de esta manera no les llegan notificaciones OSPF a los dispositivos finales. Por último, en el router RInternoA puse como ruta por defecto de manera estática el enlace que le conecta con el RExtA y la propagué al resto de routers del AS mediante OSPF, de este modo cualquier dirección IP de otros AS me aseguro de que ser direccionada a los routers que se encargan de comunicar los diferentes AS’s.[[3]](#footnote-3)

* 1. **Análisis de las tablas de rutas**

Una vez implementado el protocolo de enrutamiento y comprobada la conectividad entre todos los dispositivos, procedo a analizar las tablas de rutas para comprobar que he implementado adecuadamente el protocolo de OSPF.

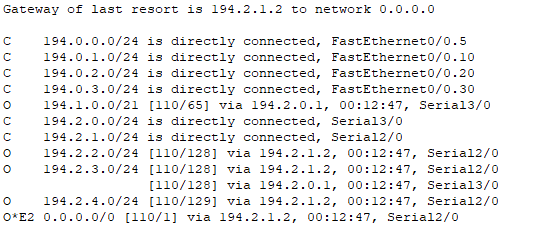


Ilustración : Tabla de rutas del router RE1

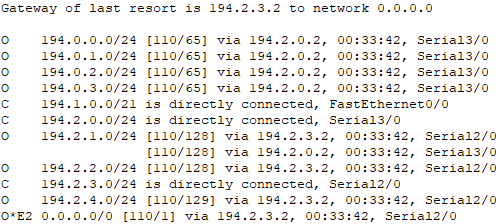


Ilustración : Tabla de rutas del router RE2

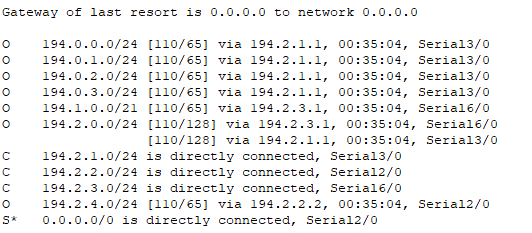


Ilustración : Tabla de rutas del router RInternoA

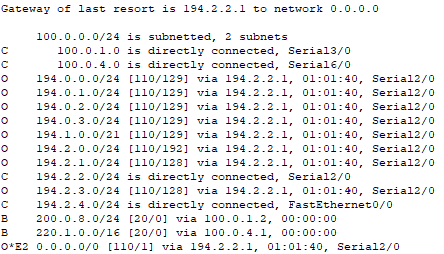


Ilustración : Tabla de rutas del router RAExt

Como se puede apreciar en las Ilustraciones 2, 3, 4 y 5. Se ha propagado en todos los routers la información de OSPF, por tanto, tengo comunicación total dentro de mi AS. La información no vinculante presentada sobre router RAext la voy a analizar cuando estudie la comunicación entre los sistemas autónomos.

* 1. **Listas de acceso (ACL)**

El objetivo de esta lista de acceso es permitir al Departamento 1 el tráfico WWW con el resto de internet, no obstante, se debe permitir la comunicación con el resto de departamentos. Es por eso que he aplicado la ACL en el interfaz virtual del Departamento 1, como se puede apreciar en la Ilustraciones 5 y 6 he aplicado la lista de acceso a la entrada a dicho interfaz. He aplicado la lista de acceso en el interfaz más próximo al departamento que quiero restringir para no tener tráfico innecesario en mi red. Adicionalmente, en la lista de acceso he permitido el tráfico WWW del departamento 1 con el resto de la red, he permitido el tráfico IP del departamento 1 con los otros departamentos, y he denegado el tráfico del departamento 1 con el resto de internet.

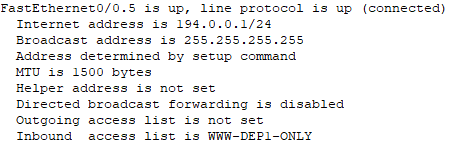


Ilustración : Aplicación de la ACL en el interfaz virtual

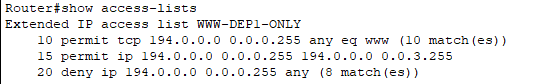


Ilustración : ACL implementada AS A

A continuación, compruebo que he aplicado adecuadamente las ACL. He intentado hacer ping desde el departamento 1 y el departamento 4 al Server0, el cual se encuentra fuera del sistema autónomo. Posteriormente he comprobado la conexión al servidor Web desde los mismos departamentos.

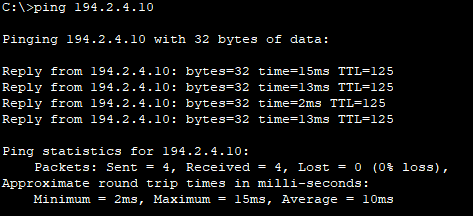


Ilustración : Ping desde departamento 4 al Server0

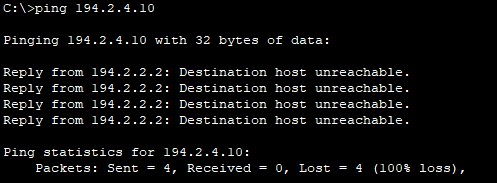


Ilustración : Ping desde departamento 1 al Server0

Me está denegando la comunicación el interfaz donde he implementado la ACL, mientras que desde el departamento 4, donde no he implementado ninguna restricción de tráfico sí que tengo comunicación.

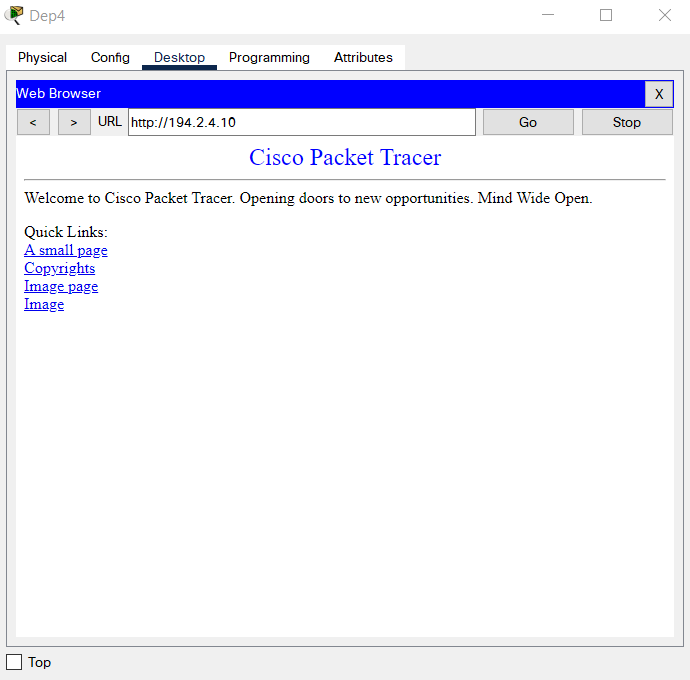


Ilustración : Conexión al servidor desde el departamento 4

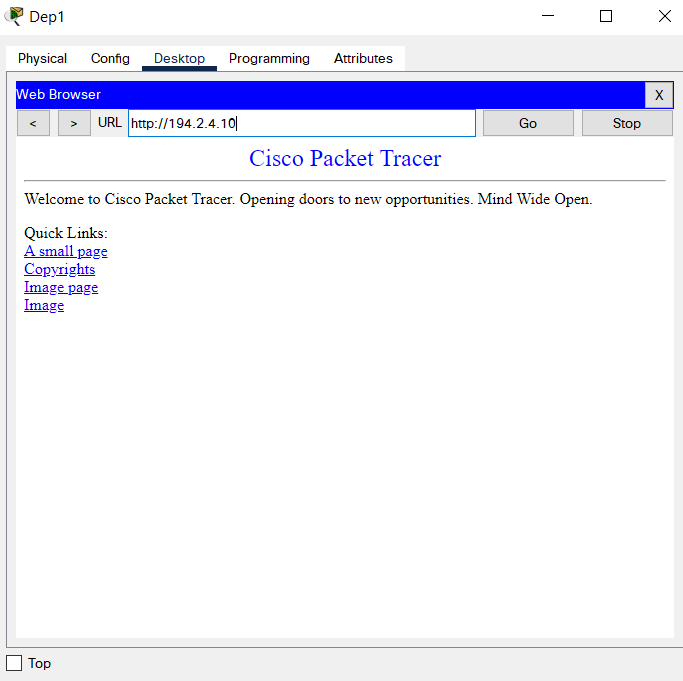


Ilustración : Conexión al servidor desde el departamento 1

Desde ambos departamentos tengo comunicación WWW, es lógico que en el departamento 4 la haya, no obstante, que también tenga dicha comunicación desde el departamento 1 indica que sí que he implementado adecuadamente la ACL.

1. **Sistema Autónomo B**
   1. **Descripción del AS**

En este AS se usa el protocolo de direccionamiento Routing Information Protocol (RIP V1). En esta red habrá 6 routers: Un Router Frontera, un Router Interno, un Router principal (el cual se conecta con el router interior y tiene conectada una LAN), y 3 routers adicionales que, al igual que el Router Principal, tiene cada uno conectado una LAN con 32 direcciones IP. En este AS se utilizan direcciones de clase C, con el rango comprendido entre 200.0.0.0 y 200.0.127.0, y esta empresa tiene asignada internamente la red 200.0.8.0. El AS tiene adicionalmente un firewall, por tanto, se deberá hacer uso de las ACL para restringir el tráfico, que únicamente permite el tráfico http y telnet.

* 1. **Descripción de RIP V1**

Es un protocolo de encaminamiento vector-distancia, por tanto, los dispositivos de encaminamiento no saben la topología completa de la red. Es necesario que las redes en las que son implementadas sean pequeñas, porque los valores de las distancias deben ser inferiores a 15. La implementación de RIP, tanto de V1 como de V2 es relativamente sencilla, únicamente hay que anunciar las redes a las que estás un router RIP directamente conectado. No obstante, la diferencia entre las versiones es que en la V1 solo admite VLMS en una situación específica. Para que las redes se propaguen adecuadamente permitiendo el uso de máscaras en lugar de clases, las redes conectadas a los router RIP deben de pertenecer a la misma clase y la misma máscara.

* 1. **Topología de la red**

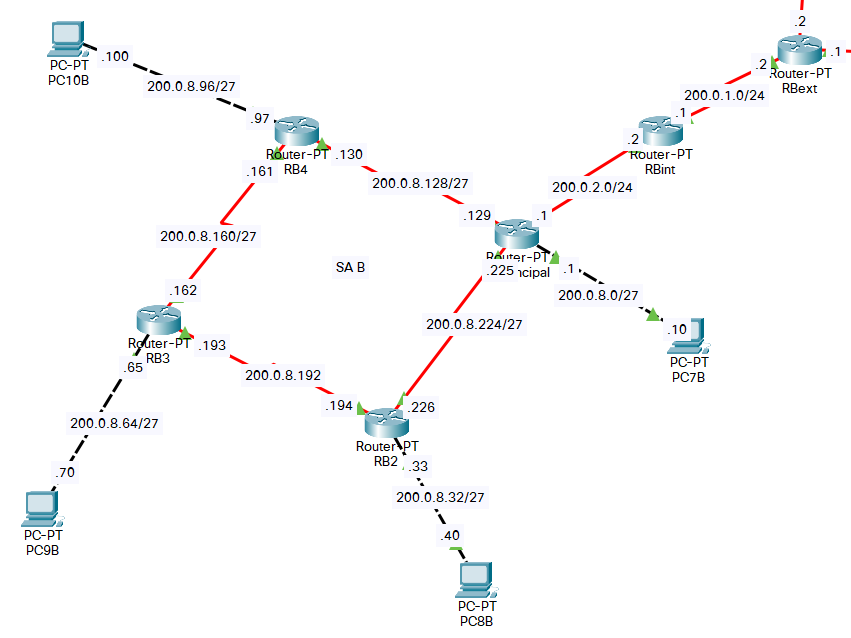


Ilustración : Topología de la red del AS B

En la Ilustración 12 se muestra la topología de la red del SA B. La topología se ha hecho de tal manera para cumplir con los requerimientos iniciales. Cada interfaz de los routers pertenece a redes diferentes. Dada esta topología, debido al protocolo que se debe aplicar y la red IP que se nos ha sido asignada, para que se propaguen las LAN necesitamos que las redes que interconectan los routers a las que están conectadas dichas LAN pertenezcan a la misma clase y tengan la misma máscara. Es por eso que todas las direcciones IP con las que cuento son /27, y como ya he asignado todas las direcciones para poder usar RIP V1 dentro de la empresa, he decidido que para los enlaces RBPrincipal-RBInterior y RBInterior-RBExterior usar dos redes IP con las que contaba el AS.

Para que la información presentada quede más clara, a continuación, se presenta dos tablas con información más detallada que la que se presenta en la Ilustración 11.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara | Gateway de salida |
| PC7B | Fa0/0 | 200.0.8.10 | /27 | 200.0.8.1 |
| PC8B | Fa0/0 | 200.0.8.40 | /27 | 200.0.8.33 |
| PC9B | Fa0/0 | 200.0.8.70 | /27 | 200.0.8.65 |
| PC10B | Fa0/0 | 200.0.8.100 | /27 | 200.0.8.97 |

Tabla : Información sobre los dispositivos finales

|  |  |  |  |
| --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara |
| RBprincipal | Serial2/0 | 200.0.1.1 | /24 |
| Serial3/0 | 200.0.8.129 | /27 |
| Serial7/0 | 200.0.8.255 | /27 |
| Fa0/0 | 200.0.8.1 | /27 |
| RB2 | Fa0/0 | 200.0.8.33 | /27 |
| Serial2/0 | 200.0.8.226 | /27 |
| Serial3/0 | 200.0.8.194 | /27 |
| RB3 | Fa0/0 | 200.0.8.65 | /27 |
| Serial2/0 | 200.0.8.193 | /27 |
| Serial3/0 | 200.0.8.162 | /27 |
| RB4 | Fa0/0 | 200.0.8.97 | /27 |
| Serial2/0 | 200.0.8.130 | /27 |
| Serial3/0 | 200.0.8.132 | /27 |
| RBInterno | Serial2/0 | 200.0.1.2 | /24 |
| Serial3/0 | 200.0.2.1 | /24 |
| RBExt | Serial2/0 | 194.2.4.1 | /24 |

Tabla : Información sobre los routers

* 1. **Implementación del protocolo de encaminamiento de RIP V1**

A la hora de implementar RIP V1 es más sencillo aun que OSPF, en cada uno de los routers en los que va a ser implantado (RBPrincipal, RB2, RB3 y RB4) basta con encontrarnos en el interfaz de RIP y declarar las redes a las que estamos directamente conectados y queremos que se propaguen gracias al protocolo. Adicionalmente, al igual que en el protocolo anterior, establecí en los interfaces de las redes LAN que la información RIP no se propague por los mismos porque no es de nuestro interés que los dispositivos finales reciban actualizaciones del protocolo de enrutamiento. Por último, propagué como ruta por defecto del RBPrincipal para que propaguen al router RBExt las direcciones que no pertenezcan a las 4 LAN asignadas.

Para poder conectar a la empresa con el exterior del sistema autónomo, podría haber empleado otra red distinta dentro de las que pertenecen al SA cuya máscara y clase fuese la misma que las que he asignado a la empresa. No obstante, para poder presentar la información de la red agregada me decante establecer la tabla de rutas manualmente para poder enrutar desde dentro de la empresa hasta el exterior y viceversa.

* 1. **Análisis de las tablas de rutas**

Una vez implementado el protocolo de enrutamiento y comprobada la conectividad entre todos los dispositivos, procedo a analizar las tablas de rutas para comprobar que he implementado adecuadamente el protocolo de RIP V1 y que la asignación de las rutas estáticas la he hecho de manera correcta.[[4]](#footnote-4)

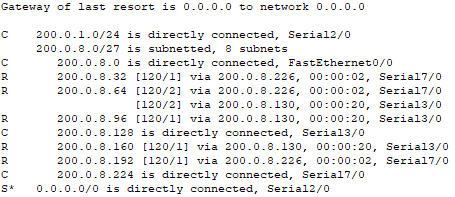


Ilustración : Tabla de rutas del router RBPrincipal

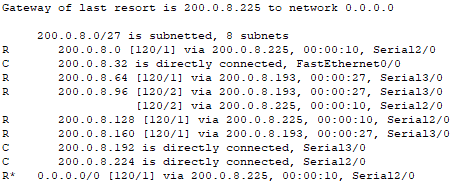


Ilustración : Tabla de rutas del router RB2

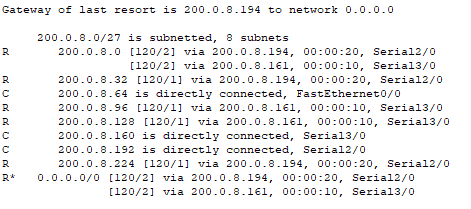


Ilustración : Tabla de rutas del router RB3

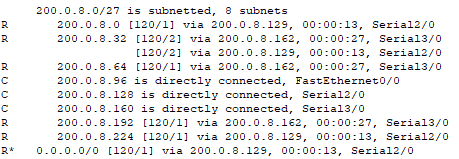


Ilustración : Tabla de rutas del router RB4

Como se puede apreciar en las Ilustraciones anteriores, se ha implementado adecuadamente el protocolo RIP. Los routers pertenecientes a la empresa conocen todas las redes que interconectan todos los routers diferentes y también conocen las LAN donde se encuentran los dispositivos finales. Adicionalmente, la ruta por defecto, que fue implementada estáticamente en el router principal, también se ha propagado al resto de routers.

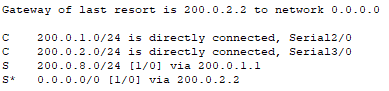


Ilustración : Tabla de rutas del router RBInt

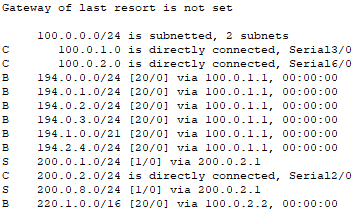


Ilustración : Tabla de rutas del router RBExt

En las Ilustraciones 17 y 18, si nos fijamos exclusivamente en la información relativa a este AS, al ver las tablas de rutas se justifica en mayor medida porque he implantado estáticamente las rutas desde la empresa al exterior y viceversa. En router interno solo he incluido la ruta por defecto y la ruta de la empresa resumidas (se pueden resumir porque todo el rango de direcciones ha sido asignado), mientras que en RBExt solo he introducido manualmente como direccionar a la empresa.

* 1. **Listas de acceso (ACL)**

El objetivo de esta lista de acceso es que únicamente se admita tráfico http y telnet desde el interior de la empresa hacia el exterior, dentro de la empresa no hay restricciones de tráfico. He aplicado una ACL en el interfaz Serial2/0 de manera saliente, de este modo no condicionaba el tráfico dentro de mi empresa. Al implementar la lista de manera saliente me aseguro que no hay tráfico innecesario entre los diferentes AS. En las Ilustraciones 19 y 20 muestro la ACL establecida y la implementación de la ACL en el interfaz.

Todas las restricciones o permisos que doy en la lista de acceso los implemento independientemente del dispositivo que los transmita o los reciba, esto se debe a que si algún mensaje sale del interfaz donde la ACL ha sido implementada, necesariamente debe provenir de la empresa. En la lista de acceso permito el tráfico telnet, permito el tráfico http y deniego cualquier otro tipo de tráfico, tal y como indican las especificaciones del proyecto.



Ilustración : ACL implementada AS B

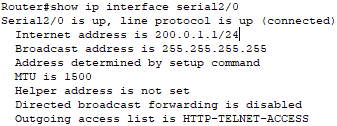


Ilustración : Aplicación de la ACL en el interfaz Serial2/0

A continuación, compruebo que he aplicado adecuadamente las ACL. He hecho un ping desde el PC7B (podría haberlo hecho desde cualquier otra red de mi empresa) al servidor web que ya empleé para comprobar las ACL del AS A. Posteriormente intenté conectarme a dicho servidor desde el PC y por último traté de hacer telnet al RAExt donde tengo conectado el Server0 que he hecho las dos comprobaciones anteriores.

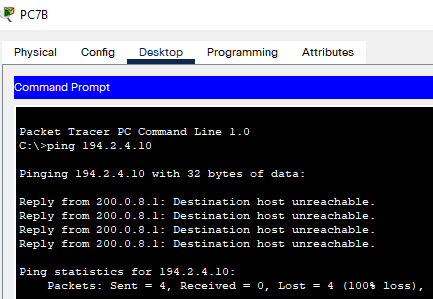


Ilustración : ping PC7B-Server0

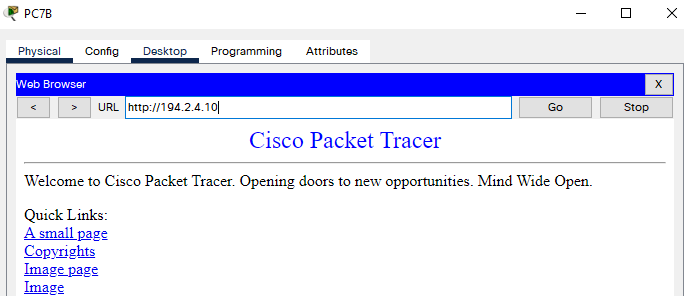


Ilustración : Comprobación de conexión WWW PC7B-Server0

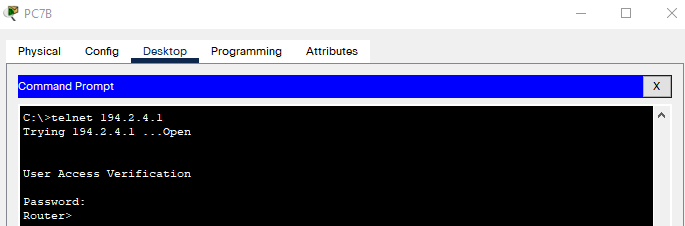


Ilustración : Comprobación de conexión telnet PC7B-RAExt

En la Ilustración 21 me están denegando la comunicación el interfaz donde he implementado la ACL. En la Ilustración 22 puedo apreciar que sí que tengo conexión WWW desde el mismo PC al mismo servidor. En la Ilustración 23, tras habilitar las líneas virtuales en router RAExt[[5]](#footnote-5), traté de establecer una conexión telnet desde el PC7B al interfaz de este router que va conectado al servidor (es la única red de este router que ha sido anunciada entre diferentes AS).

1. **Sistema Autónomo C**

## **Descripción del AS**

En este AS se usa el protocolo de direccionamiento Routing Information Protocol (RIP V2). El esquema de conexiones es el mismo que el usado en el AS B, no obstante, entre los routers de la empresa se hará uso de la red 10.0.0.0. Adicionalmente, uno de los routers estará conectado a un punto de acceso que soportará una red WI-FI con 256 direcciones privadas. En este caso no se deberá aplicar ninguna restricción de tráfico.

* 1. **Descripción de RIP V2**

RIP V2 es un protocolo de direccionamiento vector-distancia sin clases. El modo de funcionamiento es muy similar al RIP V1, empero, podemos anunciar las redes sin preocuparnos ni de su clase principal ni de la máscara de subred empleada.

* 1. **Topología de la red**

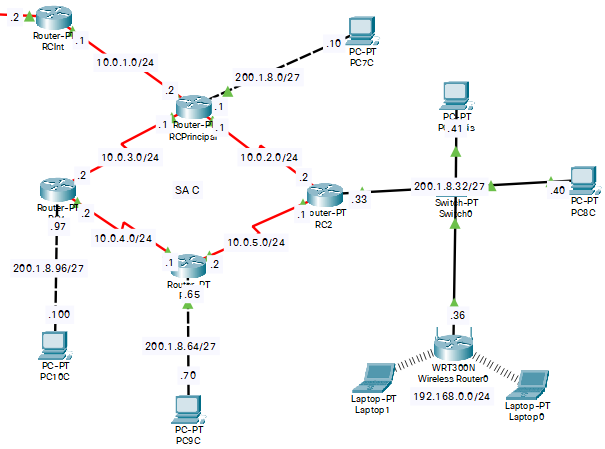


Ilustración : Topología de la red del AS C

En la Ilustración 24 se muestra la topología de la red del SA C. Como se puede apreciar en la Ilustración, el esquema de conexiones no se ha modificado. En las redes que interconectan los routers se ha hecho uso de la red 10.0.0.0. Mientras que para las diferentes LAN de esta empresa he hecho uso de la 200.0.1.8.0/25, de manera análoga a la misma distribución seguida en el SA B. Dentro de una de las LAN, con el objetivo de no crearme una red nueva a la que enrutar desde el exterior, he incluido un router WIFI donde me crearé una red con 256 direcciones privadas.

Para que la información presentada quede más clara, a continuación, se presenta dos tablas con información más detallada que la que se presenta en la Ilustración 24.

En la Tabla 6 no se presenta información sobre los dispositivos pertenecientes a la red privada porque dichos dispositivos no se dan a conocer al exterior. Se hace uso de NAT para que los datagramas que provienen o van hacia la red privada puedan ser direccionados.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara | Gateway de salida |
| PC7C | Fa0/0 | 200.1.8.10 | /27 | 200.1.8.1 |
| PC8C | Fa0/0 | 200.1.8.40 | /27 | 200.1.8.33 |
| PC9C | Fa0/0 | 200.1.8.70 | /27 | 200.1.8.65 |
| PC10C | Fa0/0 | 200.1.8.100 | /27 | 200.1.8.100 |

Tabla : Información sobre los dispositivos finales

|  |  |  |  |
| --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara |
| RCprincipal | Serial2/0 | 10.0.1.2 | /24 |
| Serial3/0 | 10.0.3.1 | /24 |
| Serial6/0 | 10.0.2.1 | /24 |
| Fa0/0 | 200.1.8.1 | /27 |
| RC2 | 200.1.8.3 | 200.0.8.33 | /27 |
| Serial2/0 | 100.0.2.2 | /24 |
| Serial3/0 | 10.0.5.1 | /24 |
| RC3 | Fa0/0 | 200.1.8.65 | /27 |
| Serial2/0 | 10.0.5.2 | /24 |
| Serial3/0 | 10.0.4.1 | /27 |
| RC4 | Fa0/0 | 200.1.8.97 | /27 |
| Serial2/0 | 10.0.4.2 | /24 |
| Serial3/0 | 10.0.3.2 | /24 |
| RCInt | Serial2/0 | 10.0.1.1 | /24 |
| Serial3/0 | 10.0.0.2 | /24 |
| RCExt | Serial2/0 | 10.0.0.1 | /24 |
| Wireless Router0 | Internet | 200.1.8.36 | /27 |
| LAN | 192.168.0.1 | /24 |

Tabla : Información sobre los routers

* 1. **Implementación del protocolo de encaminamiento de RIP V2**

La implantación de RIP V2 fundamentalmente es igual que la de RIP versión 1, cada router declara las rutas a las que está directamente conectado. La propagación de la ruta por defecto también se hace de la misma manera que la versión original de RIP. Sin embargo, hay que indicar también al router donde estamos implementando el protocolo de enrutamiento que estamos trabajando con la versión 2 de RIP. Por último, por defecto RIP resume las tablas de rutas, en nuestro caso esto no es óptimo porque necesitamos que los routers sepan direccionar de manera óptima a la red de destino, y si tienen la red resumida, en muchas ocasiones le será indistinto el interfaz por el que son enviados los datagramas, por tanto, quité la auto-sumarización en todos los dispositivos de mi red.

A diferencia que en el AS B, en este caso como es un protocolo de enrutamiento sin clases, no necesito implementar una red estática para que todos mis datagramas lleguen desde el interior de la empresa al exterior y viceversa. Con implementar RIP V2 en todo mi sistema autónomo, ya sabrán los dispositivos intermedios encaminar los datagramas al exterior.

Para poder implementar la red WIFI, tuve que asignarle a un router una dirección pública, pero la red a la que dicho router da soporte debía ser privada. Dentro de este router, entre otras medidas, se puede configurar el tamaño de la red WIFI e incluso introducir una contraseña para prevenir la conexión automática al mismo por parte de los dispositivos. Tras establecer la red WIFI, comprobé la conectividad entre dos dispositivos de la misma red, y la comunicación de dicha red con el resto del sistema autónomo.

* 1. **Análisis de las tablas de rutas**

Una vez implementado el protocolo de enrutamiento y comprobada la conectividad entre todos los dispositivos, procedo a analizar las tablas de rutas para comprobar que he implementado adecuadamente el protocolo de RIP V2.[[6]](#footnote-6)

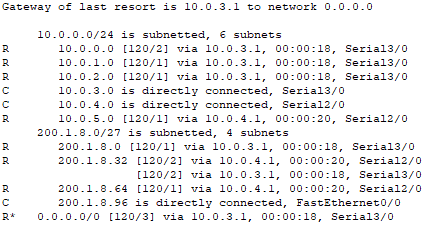


Ilustración : Tabla de rutas del router RC4

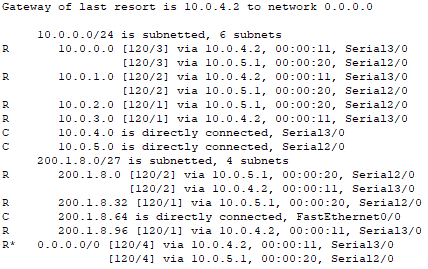


Ilustración : Tabla de rutas del router RC3

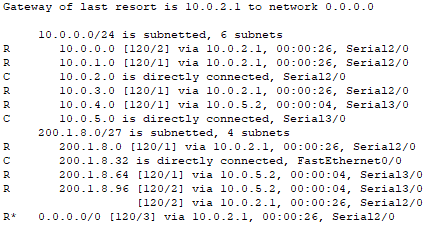


Ilustración : Tabla de rutas del router RC2

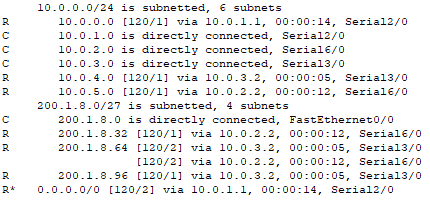


Ilustración : Tabla de rutas del router RCPrincipal

Como se puede apreciar en las tablas de rutas de los routers de dentro de la empresa, la información en estas no se presenta de manera resumida porque sino no sabríamos direccionar los datagramas a los dispositivos finales. Como se había mencionado anteriormente, la red WIFI no se propaga porque estas direcciones acceden al exterior realizando NAT. RIP V2 ofrece balanceo de cargas porque hay varias opciones de rutas cuando el costo para llegar a la red de destino es idéntico. La ruta por defecto se ha propagado adecuadamente en todos los dispositivos de mi red.

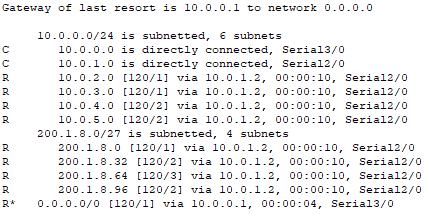


Tabla : Tabla de rutas del router RCInt

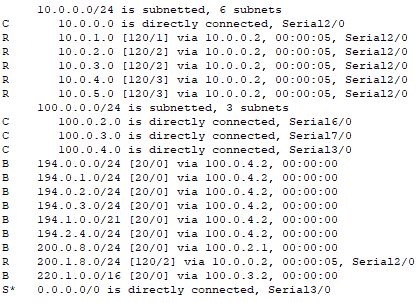


Tabla : Tabla de rutas del router RCExt

En este solamente haciendo uso del protocolo de enrutamiento RIP V2 en todo mi AS he conseguido direccionar tanto los paquetes de la empresa como los paquetes del router interior y exterior sin necesidad de la implementación estática de las rutas.

1. **Sistema Autónomo D**
   1. **Descripción del AS**

Este el sistema autónomo más sencillo, únicamente contamos con dos routers (el exterior y el interno). En el router interno habrá una interfaz virtual por la que se accede a una red de 65536 direcciones IP. El protocolo de enrutamiento a utilizar será de manera estática y se usará la red 220.0.0.0/30 para conectar los dos routers del AS.

* 1. **Descripción de una interfaz virtual**

Una interfaz de loopback es una interfaz lógica interna del router que no se asigna a un puerto físico, por tanto, nunca se puede conectar a otro dispositivo. La interfaz de loopback es útil para probar y administrar un dispositivo intermedio, para simular redes detrás del router o para comprobar procesos internos de routing. En este caso, la red que asignemos al interfaz virtual (220.1.0.0/16) deberá ser propagada al exterior.

* 1. **Topología de la red**

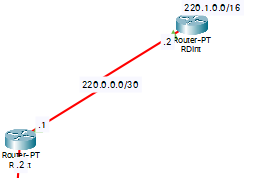


Ilustración : Topología de la red del AS C

Tal y como mencionan las especificaciones del enunciado, asigné la red 200.0.0.0/30 a la conexión entre los dos routers. Adicionalmente, asigné al interfaz de LoopBack0 la red 220.1.0.1/16 para que así perteneciese a una red con el suficiente número de conexiones que especifica el enunciado. A la hora de configurar el enrutamiento, lo realicé de manera estática, teniendo que establecer la ruta por defecto en el router interior, y anunciando en el router exterior la presencia de la red del interfaz de LoopBack.

Dada la simplicidad de este sistema autónomo por el bajo número de conexiones y la ausencia de implementación de protocolos de encaminamiento, voy a analizar directamente las tablas de rutas.

* 1. **Análisis de las tablas de rutas**

Si nos fijamos en la información de la tabla de rutas que solamente hace referencia a este sistema autónomo, podemos apreciar lo que he mencionado en el párrafo anterior:

El router RDInt, si desconoce cualquier mensaje que le llegue, lo enruta hacia el router RDExt. Por otra parte, si al router RDExt le llega un mensaje de la red 220.1.0.0/16, lo direccionará al router RDInt, el cual hará llegar el datagrama al interfaz de LoopBack.

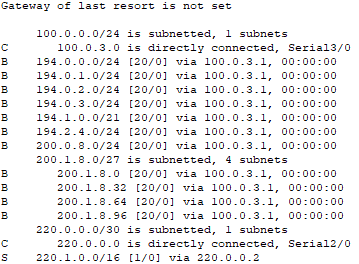


Ilustración : Tabla de rutas de RDExt

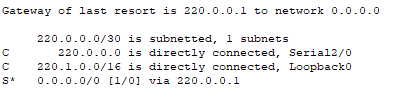


Ilustración : Tabla de rutas del router RDInt

1. **Interconexión de los Sistemas Autónomos**
   1. **Interconexión de los AS’s**

Cada Sistema autónomo debe de tener un identificador asignado. Y la vecindad entre los routers exteriores de los AS’s debe ser la siguiente: A -> B, C; B -> A, C; C -> A, B, D; D -> C. Dado que el enrutamiento debe realizarse respecto al menor número de saltos y que necesitamos comunicar Sistemas Autónomos diferentes, el protocolo de enrutamiento que va a ser empleado es el Boarder Gateway Protocol (BGP).

* 1. **Descripción de BGP**

Es el principal protocolo de encaminamiento de internet. BGP percibe internet como un conjunto de AS’s que se comunican gracias a este protocolo de direccionamiento vector-distancia. Los mensajes intercambiados por los routers frontera de los AS’s, además de incluir origen y destino, incluye los sistemas autónomos que han atravesado, evitando de este modo problemas como el de conteo al infinito.

A diferencia de otros protocolos, los routers se conocen entre sí mediante definición administrativa. En nuestro caso, como queremos comunicar sistemas autónomos diferentes, se va a hacer uso de EBGP. BGP admite tanto CIDR como agrupación de IP’s (lo cual reduce el tamaño de las tablas de rutas y del tráfico de mantenimiento), no obstante, para que una red sea propagada al resto de routers externos, es necesario que esta aparezca en la tabla de rutas.

Los routers vecinos intercambian información entre sí mediante conexiones TCP. Estos vecinos se pueden enviar: mensajes abiertos (para establecer conexiones con vecinos), keepalives (para mantener la conexión y verificar las rutas), mensajes de actualización (con las rutas de las redes de destino y los atributos de la ruta).

Para implementar EBGP es necesario:

1. Habilitar BPG dándole un identificador al router frontera de cada AS: A -> 10, B -> 20, C -> 30 y D -> 40 en nuestro caso.
2. Establecer administrativamente una relación de vecindad con los otros routers frontera.
3. Anunciar las redes que quiero compartir, las cuales deben de estar incluidas en las tablas de rutas.
   1. **Topología de la red**

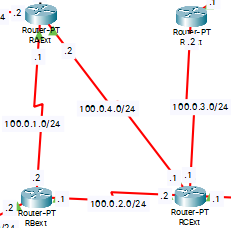


Ilustración : Red de interconexión de los diferentes AS's

En este caso solamente se va a analizar y explicar la red establecida para comunicar los diferentes sistemas autónomos. Dentro de los 4 enlaces establecidos, tal y como indican las especificaciones, he decidido emplear direcciones públicas con máscara /24 para que me resultara más fácil la asignación de IPs dentro de las nuevas redes creadas.

Para que la información presentada quede más clara, a continuación, se presenta una tabla con información más detallada que la que se presenta en la Ilustración 32.

|  |  |  |  |
| --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara |
| RAExt | Serial3/0 | 100.0.1.1. | /24 |
| Serial6/0 | 100.0.4.2 | /24 |
| RBExt | Serial3/0 | 100.0.1.2 | /24 |
| Serial6/0 | 100.0.2.1 | /24 |
| RCExt | Serial3/0 | 100.0.4.1 | /24 |
| Serial6/0 | 100.0.2.2 | /24 |
| Serial7/0 | 100.0.3.1 | /24 |
| RDExt | Serial3/0 | 100.0.3.2 | /24 |

Tabla : Información sobre los routers

* 1. **Implementación del protocolo de encaminamiento de RIP V1**

Siguiendo los pasos que he mencionado en la introducción teórica del protocolo, tras asignarle el identificador a cada sistema autónomo y de establecer la relación de vecindad entre los routers exteriores, procedí a propagar las rutas de cada AS.

Como se ha podido apreciar en las tablas de rutas de los routers exteriores presentadas anteriormente en cada AS, en función del protocolo de enrutamiento utilizado, la información presente en dichas tablas de rutas salía resumida o no. Sin embargo, para que BGP anuncie las redes al exterior, es necesario que dichas redes aparezcan en la tabla de rutas, es por eso que, si la información no se presenta resumida en estos routers, no va a poder propagarse a los otros routers exteriores resumida.

* 1. **Análisis de las tablas de rutas**

Una vez implementado el protocolo de enrutamiento y comprobada la conectividad entre todos los dispositivos, procedo a analizar las tablas de rutas para comprobar que he implementado adecuadamente el protocolo de BGP.[[7]](#footnote-7)

Como se puede apreciar en las Ilustraciones siguientes, solamente he anunciado aquellas redes donde tengo conectados dispositivos finales, incluyendo la red auxiliar creada para comprobar el tráfico WWW. De este modo me aseguro que mis tablas de rutas no sean excesivamente largas y, además, me protejo de que dispositivos ajenos a los sistemas autónomos puedan acceder a routers que exclusivamente enrutan a otros routers.

En las tablas de ruta podemos observar que todos los routers exteriores saben encaminar datagramas a todos los sistemas autónomos. Todos los AS’s salvo el A presentan al exterior la información de manera resumida, no obstante, esto no es culpa del protocolo BGP, sino que dicha información no se ha resumido al hacer uso de OSPF.

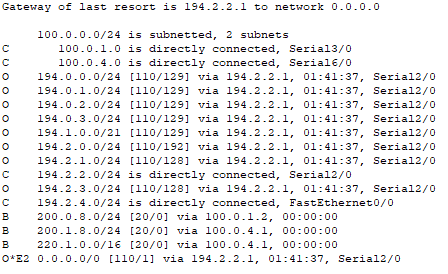


Ilustración : Tabla de rutas del router RAExt

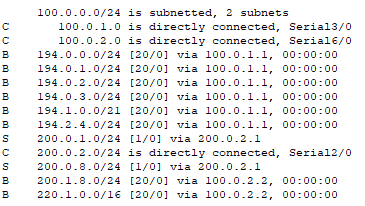


Ilustración : Tabla de rutas del router RBExt

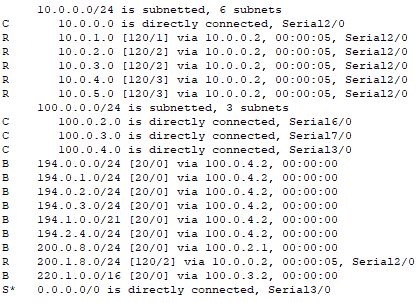


Ilustración : Tabla de rutas del router RCExt

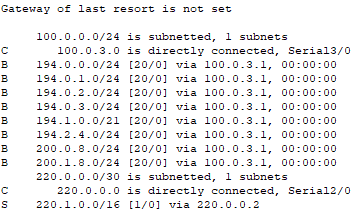


Ilustración : Tabla de rutas de RDExt

**ANEXO AS A**

**Router-on-a-stick**

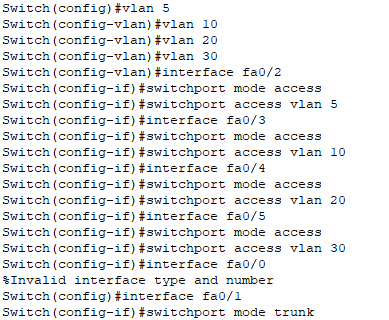


Ilustración : Comandos introducidos en el switch SWE2

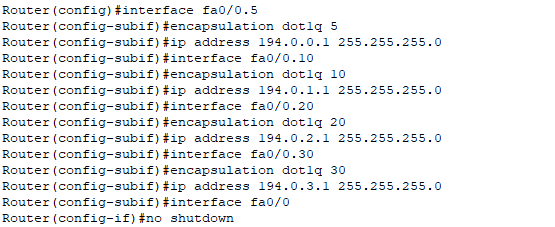


Ilustración : Comandos introducidos en el router RE1

**OSPF**

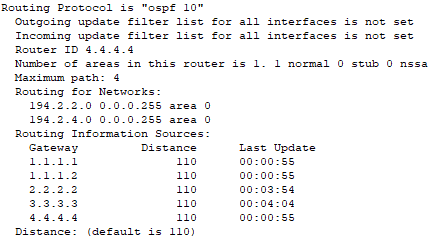


Ilustración : Redes declaradas e id del router para RAExt en protocolo OSPF

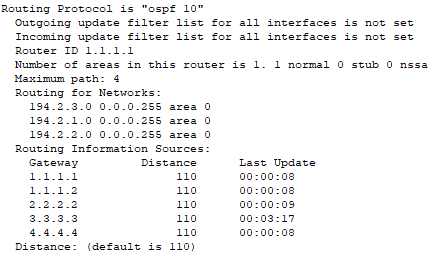


Ilustración : Redes declaradas e id del router para RInternoA en protocolo OSPF

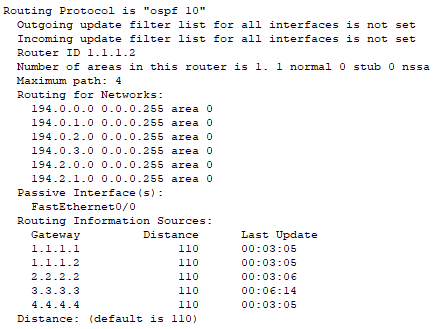


Ilustración : Redes declaradas e id del router para RE1 en protocolo OSPF

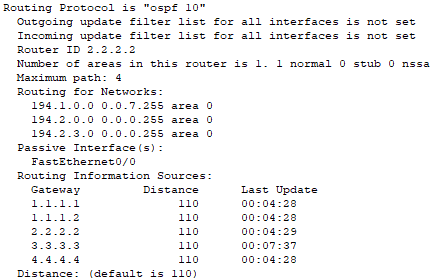


Ilustración : Redes declaradas e id del router para RE2 en protocolo OSPF

**ANEXO AS B**

**RIP V1**

Como se puede observar en las Ilustraciones presentadas a continuación, los routers declaran las redes sin máscaras. Adicionalmente en dichas Ilustraciones podemos ver con quien tiene comunicación RIP cada router. Por último, podemos apreciar la versión de RIP que estamos empleando en este sistema autónomo.

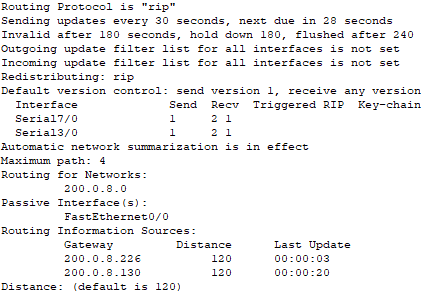


Ilustración : Información acerca de RIP V1 en RBPrincipal

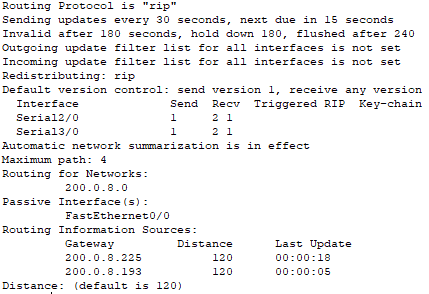


Ilustración : Información acerca de RIP V1 en RB2

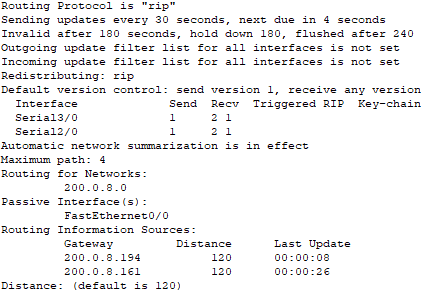


Ilustración : Información acerca de RIP V1 en RB3

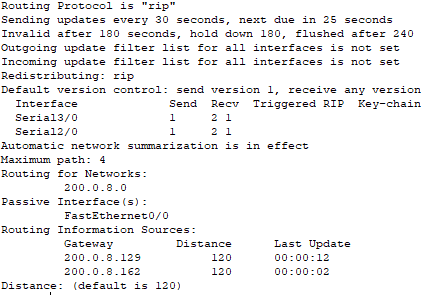


Ilustración : Información acerca de RIP V1 en RB4

**Configuración telnet**

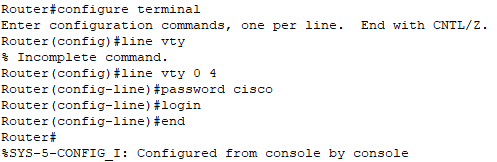








Ilustración 46: Configuración línea virtual en RExtA

**ANEXO AS C**

**RIP V2**

Como se puede observar en las Ilustraciones presentadas a continuación, los routers declaran las redes sin máscaras. Adicionalmente en dichas Ilustraciones podemos ver con quien tiene comunicación RIP cada router. Además, podemos apreciar la versión de RIP que estamos empleando en este sistema autónomo. Por último, podemos apreciar que la auto-sumarización ha sido deshabilitada para que los datagramas puedas ser enrutados.

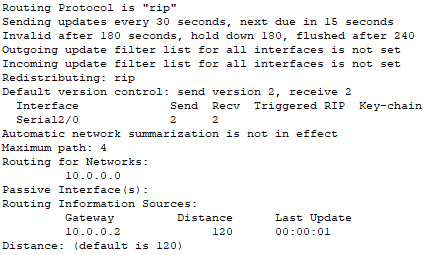


Tabla : Información acerca de RIP V2 en RCExt

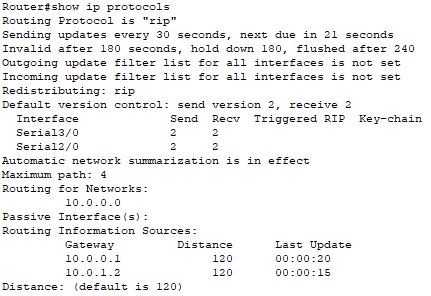


Tabla : Información acerca de RIP V2 en RCInt

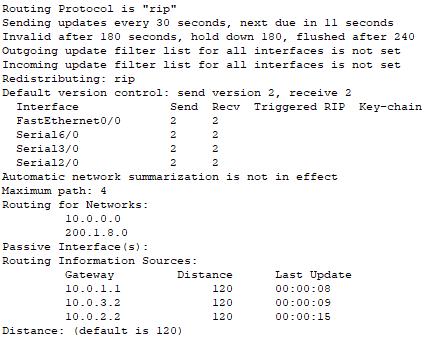


Tabla : Información acerca de RIP V2 en RCPrincipal

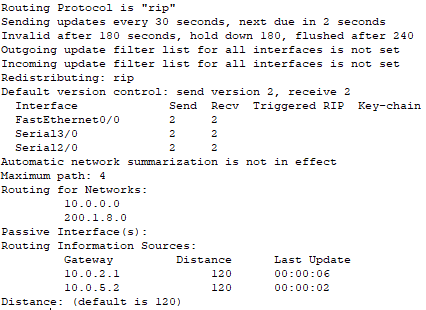


Tabla : Información acerca de RIP V2 en RC2

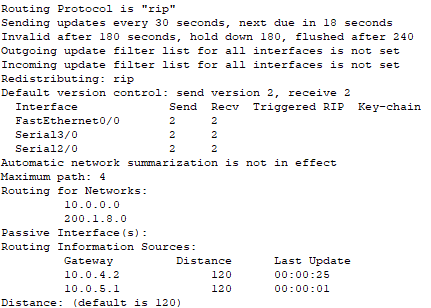


Tabla : Información acerca de RIP V2 en RC3

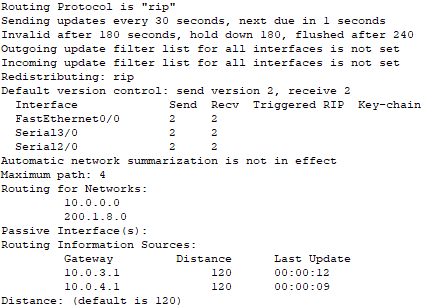


Tabla : Información acerca de RIP V2 en RC4

**ANEXO Interconexión de los Sistemas Autónomos**

**BGP**

Al analizar el protocolo BDGP implementado en cada router podemos distinguir además del identificador del router externo del sistema autónomo, las redes con las que hemos establecido relación de vecindad. Las redes propagadas y anunciadas por los routers se podrán observar en la tabla de rutas.

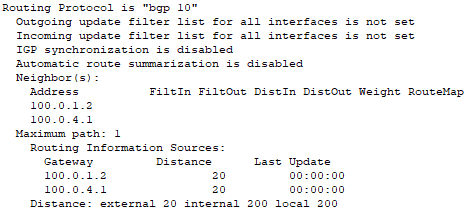


Tabla : Información acerca de BGP en RAExt

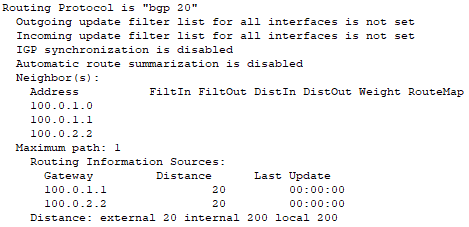


Tabla : Información acerca de BGP en RBExt

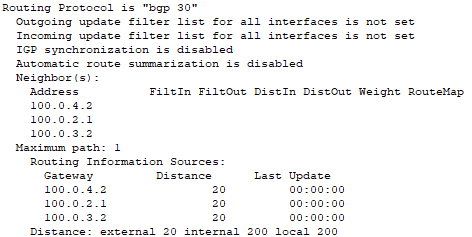


Tabla : Información acerca de BGP en RCExt

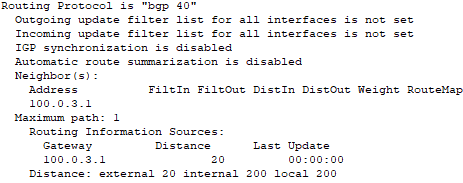


Tabla : Información acerca de BGP en RDExt

1. La información presentada en la tabla hace referencia al AS A. Los interfaces del RExtA con el resto de routers exteriores se analizará más adelante. [↑](#footnote-ref-1)
2. En el Anexo AS A: Router-on-a-stick se incluyen los comandos introducidos. [↑](#footnote-ref-2)
3. En el Anexo AS A: OSPF se incluye información relativa a las rutas propagadas y al identificador de los routers. [↑](#footnote-ref-3)
4. En el Anexo AS B: RIP V1 se incluye información relativa a las rutas propagadas mediante el protocolo de enrutamiento. [↑](#footnote-ref-4)
5. En el Anexo AS B: Configuración telnet se incluyen los comandos introducidos para habilitar la línea de telnet en dicho el router exterior RAExt. [↑](#footnote-ref-5)
6. En el Anexo AS C: RIP V2 se incluye información relativa a las rutas propagadas mediante el protocolo de enrutamiento. [↑](#footnote-ref-6)
7. En el Anexo Interconexión de los Sistemas Autónomos: BGP se incluye información relativa a las rutas propagadas mediante el protocolo de enrutamiento. [↑](#footnote-ref-7)