Basic Routing Lab

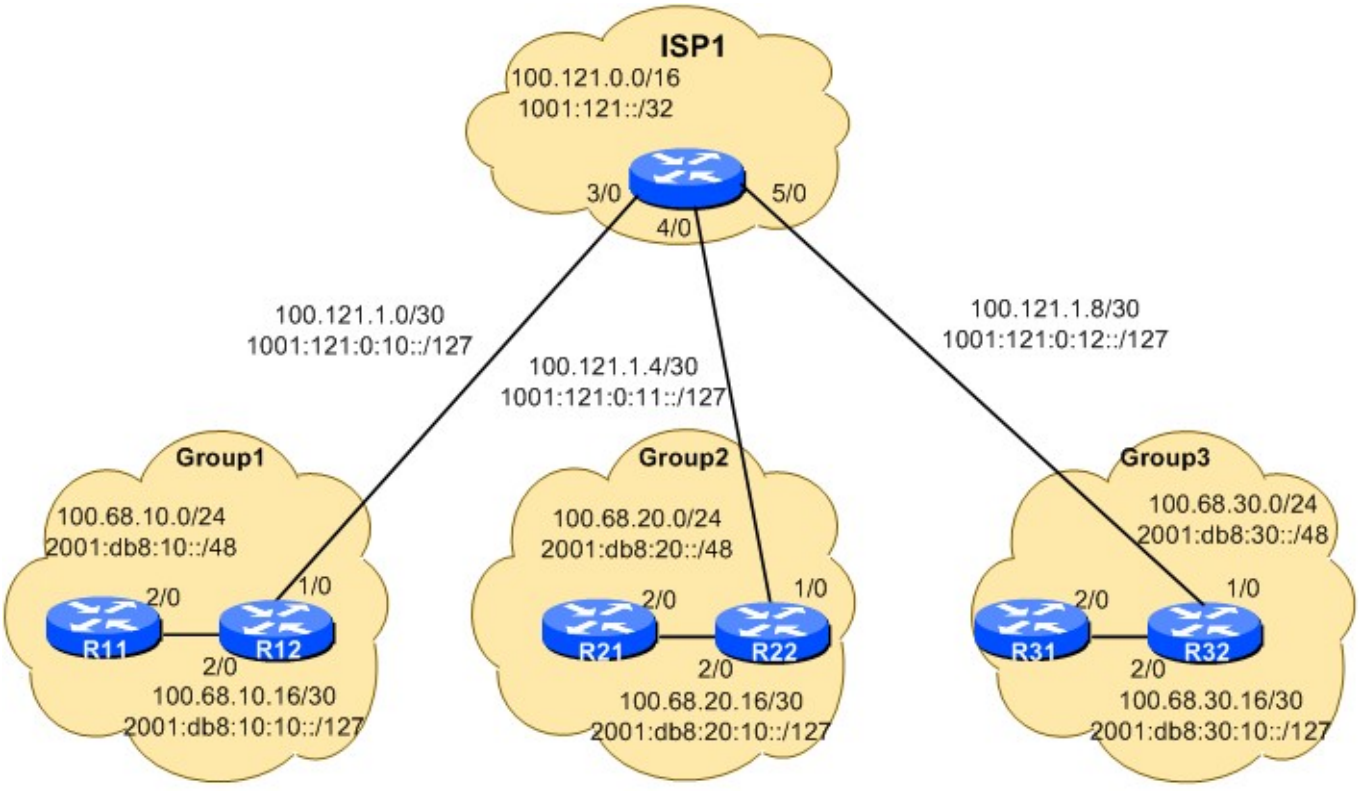
Introduction

El propósito de este ejercicio es introducir a los participantes a los requerimientos de la configuración básica de un enrutador Cisco.

La topología de la red esta diseñada de forma modular y permite que el laboratorio crezca cuando sea necesario, dependiendo del número de participantes. Cada modulo en este laboratorio tiene un (1) ISP y tres (3) redes de clientes (Universidades, Institutos, etc.). Los módulos pueden ser interconectados.

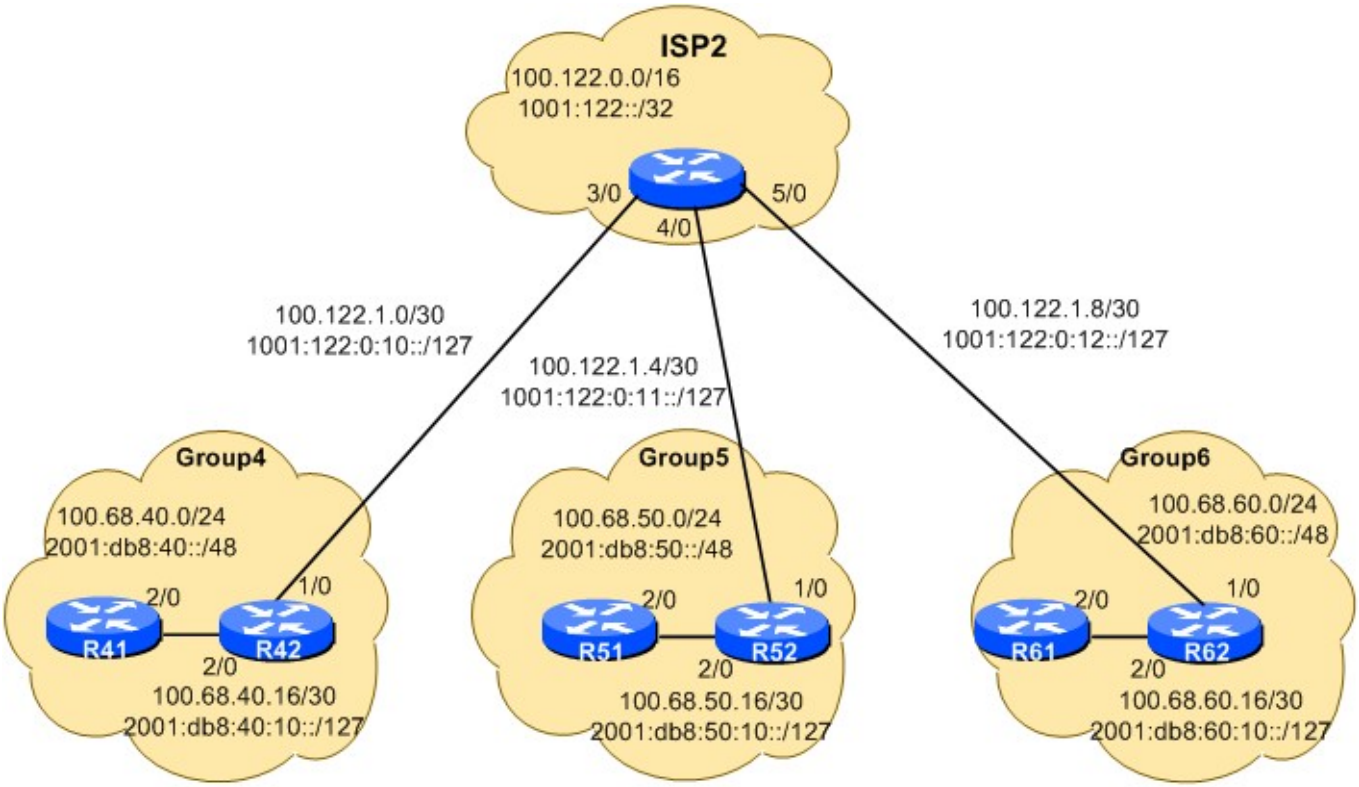
Topología del Modulo 1

El modulo uno está compuesto de tres grupos (1,2,3), y su ISP. A medida que avancemos en el taller, agregaremos un NREN a este modulo también.



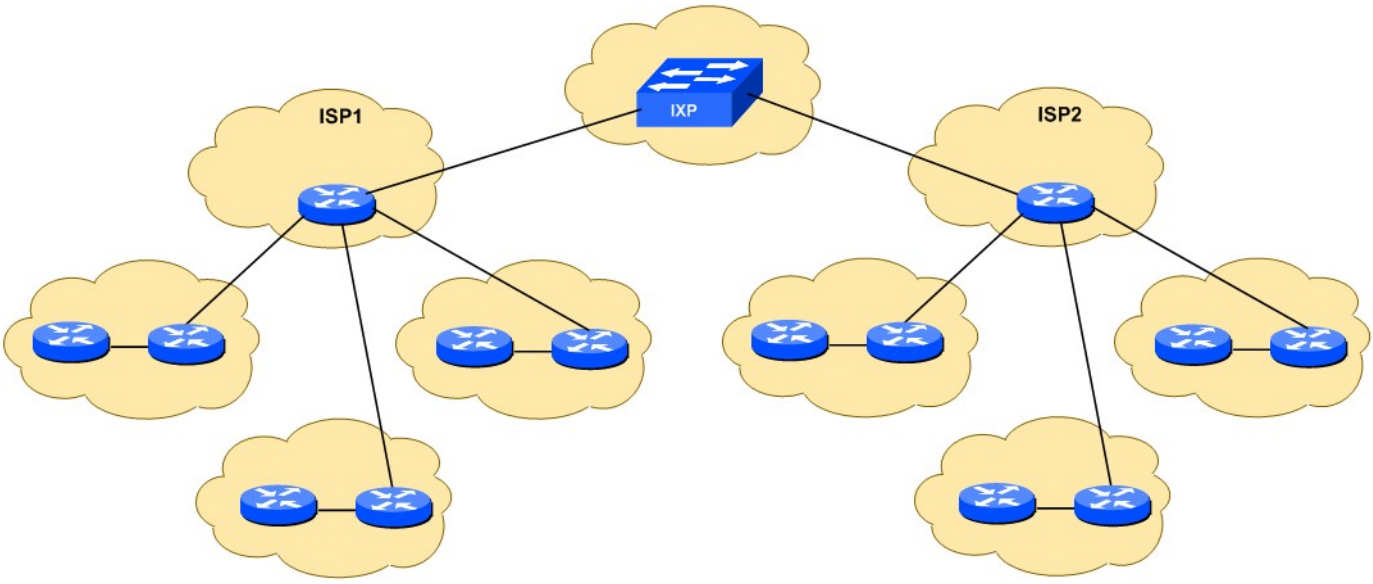
Topología del Modulo 2

El modulo dos está compuesto de tres grupos (4,5,6), y su ISP. A medida que avancemos en el taller, agregaremos un NREN a este modulo también.



Topología Completa del Laboratorio

Todo el laboratorio del taller está interconectado como se muestra en el diagrama de más abajo – los ISPs tienen una relación de intercambio de rutas a través un Punto de Intercambio de Internet (IXP).



Logística

A cada participante se le asignará una red. Dependiendo del número de participantes, una persona o un grupo será responsable de la configuración de uno de los enrutadores. Durante el transcurso del laboratorio es posible que los participantes roten entre los diferentes enrutadores para que puedan apreciar y entender la red desde otro punto de vista.

A medida que avance en los ejercicios, usted verá ejemplos de configuraciones para uno o más de los enrutadores. **Asegúrese de tomar los ejemplos y adaptarlos a su propio enrutador, topología de red y plan de direccionamiento. Use los diagramas como una guía para ayudarlo a entender con que enrutador y red está trabajando.**

Refiérase al documento con Instrucciones de Acceso al Laboratorio para información de cómo conectarse y entrar a los enrutadores que han sido asignados a usted y/o su grupo.

Asignación del Espacio de Direcciones

Refiérase al documento del Plan de Direccionamiento de IP para información sobre el esquema de direccionamiento para la infrastructura de redes de los laboratorios.

Configuración Básica de un Enrutador

Los siguientes ejemplos de configuración muestran la configuración sugerida y recomendada para los enrutadores en cada grupo. Remplace la **X** en los ejemplos, con su número de grupo.

Nombre del Enrutador

```
enable
config terminal
hostname RX1
```

Configure la Autenticación

```
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
username nsrc secret lab-PW
enable secret lab-EN
service password-encryption
line vty 0 4
 transport preferred none
line console 0
 transport preferred none
```

Configure el Sistema de Bitácora

```
no logging console
logging buffered 8192 debugging
```

Deshabilite la Resolución de DNS

```
no ip domain-lookup
```

Activar Enrutamiento para IPv6

Activar el enrutamiento de IPv6 y habilita el uso de CEF para IPv6 (no vienen habilitados por defecto en Cisco IOS)

```
ipv6 unicast-routing
ipv6 cef
```

Deshabilite Enrutamiento Basado en el Origen para IPv4/IPv6

```
no ip source-route
no ipv6 source-route
```

Descubrimiento del Path MTU

Habilite el descubrimiento del Path MTU en el enrutador – esta función no está habilitada para la conexión al plano de control del enrutador (pero está habilitada por defecto para BGP).

```
ip tcp path-mtu-discovery
```

Salga del Modo de Configuración y Guárdela

```
end
write memory
```

Configuración de las Interfases

Enlaces a otros Enrutadores

Configure sus interfaces de acuerdo al diagrama.

Note que para los enlaces hacia el ISP utilizaremos direcciones del espacio de direcciones del ISP, mientras que para los enlaces internos utilizaremos direcciones de nuestro propio espacio de direcciones..

En RX1:

```
interface GigabitEthernet2/0
 description Enlace PaP a RX2
 ip address 100.68.X0.17 255.255.255.252
 no ip directed-broadcast
 no ip redirects
 no ip proxy-arp
 ipv6 address 2001:db8:X0:10::0/127
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress
 no shutdown
!
```

En RX2:

```
interface GigabitEthernet1/0
 description P2P Link to ISP1
 ip address 100.121.1.2 255.255.255.252
 no ip directed-broadcast
 no ip redirects
 no ip proxy-arp
 ipv6 address 1001:121:0:10::1/127
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress
 no shutdown
!
interface GigabitEthernet2/0
 description Enlace PaP a RX1
 ip address 100.68.10.18 255.255.255.252
 no ip directed-broadcast
 no ip redirects
 no ip proxy-arp
 ipv6 address 2001:db8:10:10::1/127
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress
 no shutdown
```

Descripción de Algunos de los Comandos Usados

no ip directed-broadcast

Un paquete IP de Difusión Dirigida es un paquete IP cuya dirección de destino es una dirección valida de broadcast en una subred de IP, pero que se origina desde un nodo que no es parte de ese segmento de red.

Debido a que las difusiones dirigidas, y especialmente las difusiones dirigidas de ICMP, han sido abusadas por personas maliciosas, recomendamos deshabilitar el comando de difusiones dirigidas en todas las interfaces que no lo necesitan (posiblemente en todas las interfaces).

no ip proxy-arp

Proxy ARP es una técnica en la que un dispositivo, usualmente un enrutador, responde a solicitudes

de ARP que estaban destinadas a otro dispositivo. Cuando el enrutador enmascara su identidad y responde a las solicitudes de ARP, el enrutador se hace responsable de hacer llegar los paquetes de IP al destino “real”. Proxy ARP puede ayudar en el caso de que maquinas quieran comunicarse con subredes remotas sin la necesidad de configurar y proceso de enrutamiento o definir un enrutador por defecto.

Desventajas de usar Proxy ARP:

- Incrementa el impacto de los ataques de spoofing con ARP, en los que una máquina se identifica como si fuera otra para interceptar los paquetes
- Hace difícil el identificar configuraciones equivocadas en los dispositivos
- Los dispositivos tendrán tablas de ARP más grandes

no ip redirects

Paquetes ICMP de re-direccionamiento pueden ser enviados a dispositivos cuando un enrutador sabe que hay otro enrutador en la misma subred con un mejor camino hacia la dirección de destino. Si un hacker logra instalar un enrutador en una red que cause que los enrutadores legítimos aprendan sobre caminos ilegítimos, el enrutador del hacker terminaría desviando el tráfico legítimo gracias los mensajes ICMP de re-direccionamiento. Por esta razón, es recomendado que este técnica sea deshabilitada en todas las interfaces.

ipv6 nd ra suppress

Anuncios de enrutadores IPv6 son enviados periódicamente por los enrutadores para informar a todos los dispositivos que el está presente en el segmento, y ayudar a los dispositivos que generen sus propias direcciones de IPv6 utilizando los mecanismos de auto-configuración sin estado. Este comando no es necesario en interfaces con un enlace punto-a-punto.

ipv6 nd prefix default no-advertise

Previene que el enrutador envíe prefijos de IPv6 como parte de los anuncios de enrutador de IPv6, y de esta forma los clientes no pueden auto-configurarse con direcciones globales de IPv6. Este comando es de utilidad en versiones de IOS donde no se puede suprimir los mensajes de solicitud de anuncio de enrutador (RA).

Prueba de Conectividad

Haga algunas pruebas de PING

```
R12# ping 100.68.10.17        <- R11
R12# ping 2001:db8:10:10::0   <- R11
R12# ping 100.121.1.1         <- ISP1
R12# ping 1001:121:0:10::0    <- ISP1
```

y analice el resultado de los siguientes comandos:

```
show arp                      : Muestra la cache de ARP
show interface <int>          : Muestra el estado y configuración de la
                                interfaz
show ip interface <int>       : Muestra el estado y configuración IP de las
                                interfaces
show ipv6 neighbors           : Muestra los vecinos de IPv6
show ipv6 interface <int>     : Muestra el estado y configuración IPv6 las
                                interfaces
show cdp neighbors            : Muestra los vecinos aprendidos vía CDP
```

Haga un PING a dispositivos en otros grupos (recuerde remplazar RX en los ejemplos, con su propio número de grupo):

- Desde RX2, trate un ping a las IP de las interfaces en los enrutadores en los otros grupos.
- Desde RX1, trate un ping a las IP de las interfaces en los enrutadores en los otros grupos.

Que pasa? Por qué?

Examine las tablas de enrutamiento y de reenvío

```
show ip route
show ipv6 route
```

Para ver las tablas de renvío:

```
show ip cef
show ipv6 cef
```

Puede ver caminos para los otros grupos y el ISP en las tablas de enrutamiento?

… Y en las tablas de reenvío?

Que necesita para que pueda llegar hacia los otros grupos (y los ISPs)?

Que necesitan los otros grupos para que puedan llegar hacia su grupo?

Creando Rutas Estáticas

En sus enrutadores RX1, y RX2, neceseitará crear rutas estáticas para:

- Todos los otros grupos
- El espacio de direcciones de los IPS (si, para ambos ISP)
- Todos los enlaces que interconectan los otros grupos al ISP

Hacia donde apuntan (próximo salto) las rutas en RX2?

Hacia donde apuntan (próximo salto) las rutas en RX1?

Recuerde que la sintaxis para añadir rutas es:

```
ip route SUBNET MASK NEXT-HOP
```

Por ejemplo, en R12, para llegar al Grupo 2:

```
R12(config)# ip route 100.68.20.0 255.255.255.0 100.121.1.1
R12(config)# ipv6 route 2001:db8:20::/48 1001:121:0:10::0
```

Basado en la información del ejemplo de mas arriba, cree las rutas estáticas necesarias para llegar a todos los grupos, los enlaces de interconexión y el espacio de direcciones del ISP.

Grabar la Configuración

Verifique y salve la configuración.

```
show running-config
write memory
```

Apéndice A – Ejemplo de Configuración del ISP1

Este es un ejemplo de la configuración para el enrutador de ISP1. La configuración del ISP2 será muy similar. Los grupos que operarán el ISP1 e ISP2 deberán construir su configuración basada en el ejemplo de más abajo.

```
hostname ISP1
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
username nsrc secret nsrc-PW
enable secret nsrc-EN
service password-encryption
line vty 0 4
 transport preferred none
line console 0
 transport preferred none
no logging console
logging buffered 8192 debugging
no ip domain-lookup
ipv6 unicast-routing
ipv6 cef
no ip source-route
no ipv6 source-route
!
interface Loopback0
 ip address 100.121.0.1 255.255.255.255
 ipv6 address 1001:121::1/128
!
interface GigabitEthernet1/0
 description Enlace al IXP
 ip address 100.127.1.1 255.255.255.0
 no ip directed-broadcast
 no ip redirects
 no ip proxy-arp
 ipv6 address 2001:db8:ffff:1::1/64
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress
 no shutdown
!
! Enlace al Grupo 1 (repita para los Grupos 2 y 3 en GigE4/0 and G5/0)
interface GigabitEthernet3/0
 description Enlace PaP a R12
 ip address 100.121.1.1 255.255.255.252
 no ip directed-broadcast
 no ip redirects
```

```
 no ip proxy-arp
 ipv6 address 1001:121:0:10::/127
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress
 no shutdown
!
! Rutas hacia el Grupo 1 (repita para los grupos 2 y 3)
ip route 100.68.10.0 255.255.255.0 100.121.1.2
ipv6 route 2001:db8:10::/48 1001:121:0:10::1
!
! Rutas hacia el Grupo 4 (repita para los grupos 5 y 6)
ip route 100.68.40.0 255.255.255.0 100.127.1.2
ipv6 route 2001:db8:40::/48 2001:db8:ffff:1::2
!
! Rutas al espacio de direcciones del ISP2
ip route 100.122.0.0 255.255.0.0 100.127.1.2
ipv6 route 1001:122::/32 2001:db8:ffff:1::2
!
! Rutas fijas para los bloque de direcciones del ISP1
ip route 100.121.0.0 255.255.0.0 null0
ipv6 route 1001:121::/32 null0
!
```